IPv6 Home Router Guideline (Translated Version)

[Ver.1.0]

2009-06-22

IPv6 Promotion Council
IPv4/IPv6 Coexistence WG　IPv6 Home Router SWG

Revision History

Ver.	Revised on:	Summary
0.9	2009-05-22	Public Comment Version
1.0	2009-06-22	Ver. 1.0 Some modification, unstudied items preparation

Acknowledgement

We would like to thank Yasuo Kashimura from Alcatel Lucent in translating the guideline document, which is originally written in Japanese.

Original Guideline in Japanese is available at:
http://www.v6pc.jp/jp/upload/pdf/v6hgw_Guideline_1.0.pdf

Table of Contents

1 Introduction

1.1 Background and Purpose of this Document

In recent years, the issue of IPv4 address exhaustion has always been on the agenda for discussion, and network operators have naturally been expected to support IPv6 at an early stage.

It was under these circumstances that, in September 2008, the IPv4/IPv6 Co-Existence Working Group (WG) under the IPv6 Promotion Council[1] set up the "IPv6 Home Router Sub-Working Group (SWG)."[2] The purpose of this SWG is to bring together the minimum common functions of the "Home Router" that are necessary for ISPs to provide IPv6 Connection services, so that it becomes possible for Internet users to use the IPv6 environment smoothly. "Minimum common functions" in this context means that discussions were held not only from the viewpoint of Internet users, but also from the viewpoints of Home Router-developing vendors and IPv6 connection service providers.

This document summarizes the content of studies conducted so far at "IPv6 Home Router SWG" in a tangible output titled "IPv6 Home Router Guideline." Note that it has no compelling force over Home Router implementation or ISP's IPv6 service specification.

[1] IPv6 Promotion Council: http://www.v6pc.jp/

[2] IPv6 Home Router SWG: http://www.v6pc.jp/jp/wg/coexistenceWG/v6hgw-swg.phtml

1.2 Environment Assumed and Readers Targeted by this Guideline

This Guideline assumes an environment in which a home network is connected to an ISP through a Home Router (compact router deployed inside a user's home) as the Internet connection topology. Also, as the IPv6 connection service assumes a dual-stack environment, our studies should be conducted under the assumption that IPv4 equipment should communicate using IPv4. Further, those functions that become necessary due to changes in the IPv4 environment, such as Large Scale NAT (LSN), caused by IPv4 address exhaustion are also out of scope.

Examples of networks that are out of scope are listed below:

<Network Environment out of scope>

- Enterprise networks
- Public networks such as hot spots
- Networks to which client terminals are directly connected
- Networks in which middle boxes such as multi-stage NAT are also employed

The assumed IPv6 Home Router would have extensibility fully considered and possess the minimum-required functions.

This Guideline is to be read primarily by the following readers:

- People designing/developing a Home Router
- People providing Internet connectivity services, such as those working for ISPs

1.3 Glossary of Terms and Notation

The terms used in this Guideline have the meanings defined in “IPv6-related Glossary”[3] compiled by Internet Association Japan (IAjapan). For details, please refer to the Glossary. Other terms not described in the Glossary are explained below:

Table 1-1 Explanation of Terms Used in This Guideline

Term	Description
ULA (RFC 4193)	Unique Local IPv6 Unicast Addresses. IPv6 unicast address defined for use in local communication such as within a site. Equivalent to IPv4 private address (RFC 1918), it is specified that part of the prefix should be generated randomly, contributing to the enhanced uniqueness of an address.
TR-069	Technical Report 069. One of the technical specifications defined by BroadBand Forum, it defines the application layer protocol for remotely controlling CPE equipment. More specifically, it defines communication between CPE and Auto Configuration Server (ACS) using SOAP/HTTP [44].
UPnP	Universal Plug and Play. Generic term for the technical specification defined by UPnP Forum with the purpose of making it possible to join a network just by plugging in the equipment. More specifically, it describes in XML such information as how to control the behavior and functions of equipment, with such information being communicated using existing protocols such as SOAP/HTTP [45].

The expression “IPv4/IPv6” is used to communicate that there are both an IPv4 address and an IPv6 address present. Also, “(Prefix length is) short/long” is used to represent a comparison of IPv6 address prefix size, the definition of which is given below:

・Shorter than /35: means prefix length is shorter than 35 bits E.g.) /32
Indicates, as prefix size, the address space is large

・Longer than /35: means prefix length is longer than 35 bits E.g.) /64
Indicates, as prefix size, the address space is small

[3] IPv6-related Glossary (IAJapan): http://www.iajapan.org/ipv6/v6term/glossary_01.html

1.4 Preparation of Guideline

This section gives an overview of the functions of the Home Router discussed in this Guideline, and explains the structure of this Guideline.

1.4.1 Basic Functions Provided by ISP

An ISP's IPv6 connection service model assumed in this Guideline can primarily be categorized into the four functions shown in Figure 1-1:

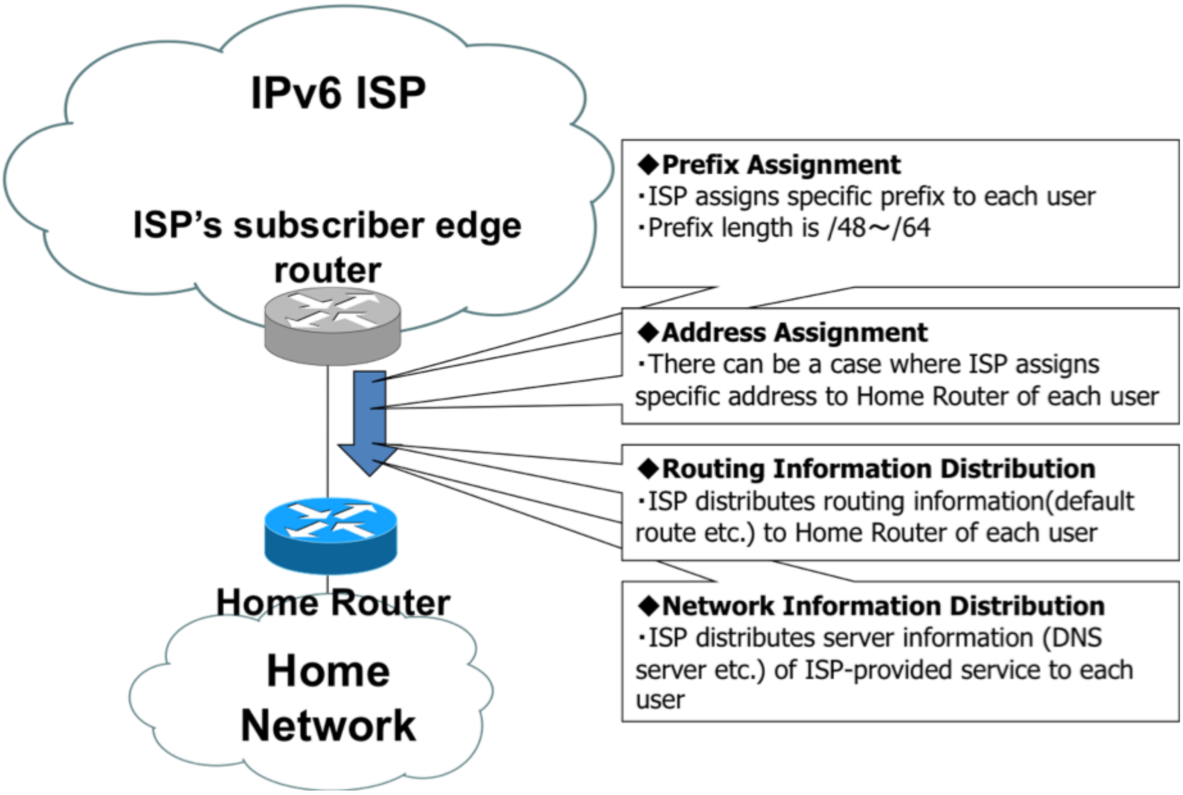
IPv6 ISP
ISP's subscriber edge router
Home Router
Home Network
◆Prefix Assignment
・ISP assigns specific prefix to each user
・Prefix length is /48～/64
◆Address Assignment
・There can be a case where ISP assigns specific address to Home Router of each user
◆Routing Information Distribution
・ISP distributes routing information(default route etc.) to Home Router of each user
◆Network Information Distribution
・ISP distributes server information (DNS server etc.) of ISP-provided service to each user

Figure 1-1 Summary of ISP's Service Model

・Prefix Assignment

In IPv6, unlike the IPv4 connection service, address assignment per prefix is necessary. The assigned prefix size differs depending on the service, but is assumed to be approximately between /64 and /48 of prefix length [8].

・Address Assignment

A case may be assumed in which the address is assigned from the ISP-side to the WAN-side interface of the IPv6 Home Router for the purpose of monitoring if the connection is dead or alive.

・Routing Information Distribution

Similar to the IPv4 case in principle, the default route is set from the ISP to the user-side.

- Network Information Distribution

  It is normal for server information provided by the ISP to the user not only to be communicated as static text information but also distributed using DHCP etc.

Assuming an environment with the mechanism above, we tried to organize the functions a Home Router needs.

1.4.2 Home Network Summary

A Home Router needs to re-distribute and assign information on each network (as described earlier and provided by the ISP side) to the home network. This Guideline discusses the following router functions regarding network setting for a home network.

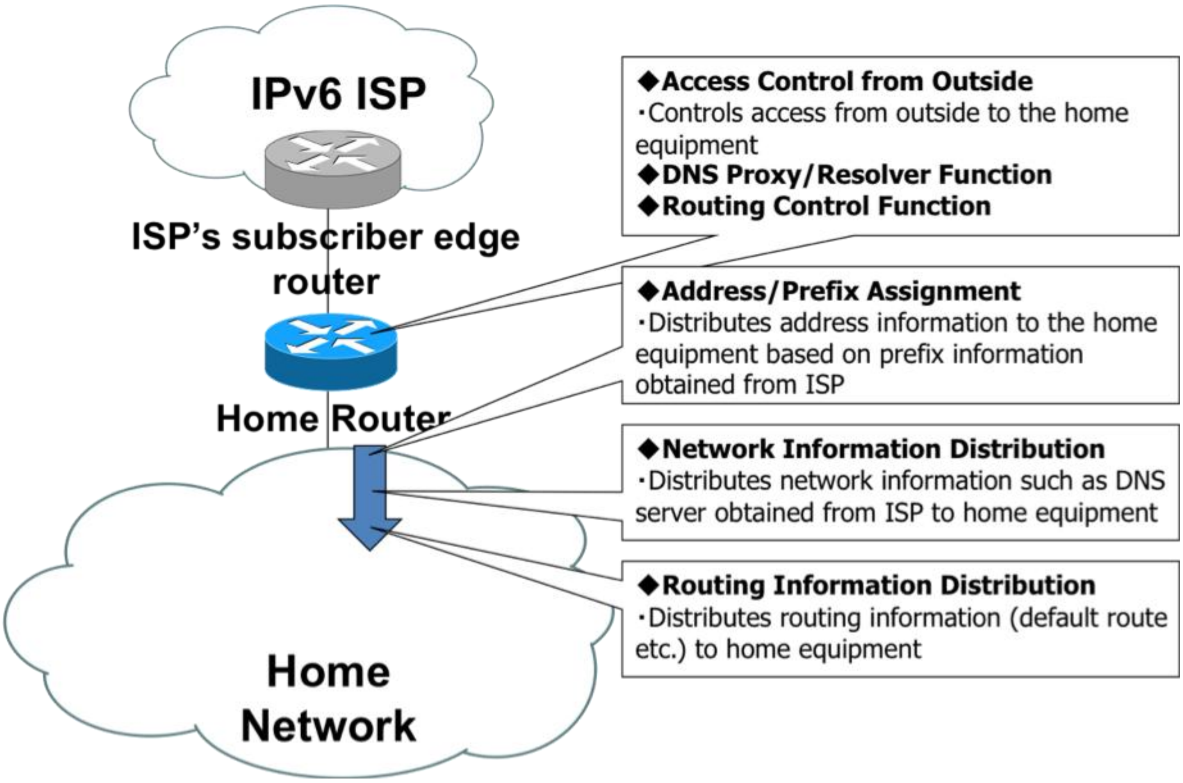
IPv6 ISP
ISP's subscriber edge router
Home Router
Home Network
◆Access Control from Outside
・Controls access from outside to the home equipment
◆DNS Proxy/Resolver Function
◆Routing Control Function
◆Address/Prefix Assignment
・Distributes address information to the home equipment based on prefix information obtained from ISP
◆Network Information Distribution
・Distributes network information such as DNS server obtained from ISP to home equipment
◆Routing Information Distribution
・Distributes routing information (default route etc.) to home equipment

Figure 1-2 Home Network Setting Overview

- Address/Prefix Assignment

  Function for assigning prefix and address to the client terminal in the home LAN using the address space assigned by the ISP-side. Various schemes can be considered such as dynamic and static.

- Network Information Distribution

  Function to distribute information about DNS server etc. to a client terminal.

Some standardized methods exist.

・Routing Information Distribution

Regarding routing information to a client terminal, a method that distributes only the default route is considered normal.

・Access Control from Outside

In IPv6, similar to the IPv4 case, it is necessary to control communication to the home. Especially in IPv6, as it is highly likely that a home network will be configured with a global address, controlling access from outside is regarded to be important.

・DNS Proxy/Resolver Function

Although it is possible to use the DNS server provided by an ISP directly from the client terminal, a case can be assumed in which, similar to the IPv4 case, the DNS function is there.

・Routing Control

Unlike the IPv4 case, proper implementation is needed given the fact that the assigned address space is large and unused space may appear. Depending on the service provided, a case in which implementation for multicast becomes necessary can be assumed.

1.4.3 Functions Required of Home Router

Based on the services/functions listed in Sections 1.4.1 and 1.4.2, we sorted the functions required for the Home Router discussed in this Guideline as shown in Table 1-2.

Table 1-2 List of Functions Required of Home Router and Corresponding Chapter Numbers

Major Item	Medium Item	Chapter Number
Address／Prefix Setting Function	Prefix Information Reception	3.1
	Address／Prefix Information Distribution	3.3, 5.3, 6.1
	WAN-side Address Setting	3.2, 8.1.1
Routing Control Function	Routing Setting	7.2
	Not Reachable Address/Prefix Control	7.1
	Multicast Function	7.3
Access Control Function	Access Control to Router Itself	4.2
	Access Control to Home Network	4.1, 7.2.3

	Control Rule Setting	4.1(4.1.2)
Server Function	DNS Proxy Function	5.2, 5.3, 5.4, 5.5
	DNS Resolver Function	5.6
	Network Information Acquisition and Distribution	6.2, 8.2.4.2 , 8.2.4.3
	Setting Function of Router Itself	8.1, 8.2

In this Guideline, these functions are described in the following chapters.

In Chapter 2, we organize the functions that are necessary when connecting to the ISP that provides an IPv6 connection service. Given that the format of the IPv6 connection service provided by an ISP is unclear as of Fiscal Year 2008, we address only the IPv6 connection service format in this version.

In Chapter 3, we organize the functions focusing on use of the address space assigned by ISP. Specifics about the protocols used are described in Chapter 6 and Chapter 8.

In Chapter 4, we summarize the necessary functions for access control from outside. As end-to-end connection will be possible with IPv6, the importance of this function is assumed to increase.

In Chapter 5, we summarize DNS service-related functions. Similar to the IPv4 case, we organize the points requiring care when implementing DNS Proxy etc.

In Chapter 6, we organize things from the viewpoint of the home network setting.

In Chapter 7, we summarize routing information-related functions, and also discuss the use of multicast.

In Chapter 8, we organize the necessary functions at the ISP side that provides the IPv6 connection service. As most of the functions will have already been summarized by then, pointers are listed.

The functions required of the Home Router are organized as indicated above, and detailed functions are organized according to the items listed in Table 1-3 to summarize needs.

Table 1-3 Legend for Description of Detailed Functions (Minor Items)

Item	Meaning
Assumption:	Assumptions for the requirement discussed are described.
Requirement:	Overview of detailed functions required of Home Router is described.
Necessity:	The degree to which the requirement under discussion is required is represented by: “Mandatory/Recommended/Optional.”

	Mandatory (MUST): It is mandatory to implement the function. Recommended (SHOULD): It is recommended to implement the function. Optional (MAY): Implementation is left up to the vendor because the function may provide added value to the router (service-dependent function etc.)
Reason:	Reasons that led us to consider the function listed as a requirement are given.
Remarks:	Reference information etc. discussed before deciding necessity is given.

2 Functions for Connecting to ISP

In this chapter, the purpose is to summarize the necessary connection functions when a router uses an ISP service. Given that an ISP's method of providing IPv6 network reachability was unclear when conducting research for this Guideline, it is limited to identifying what connection formats may exist. As a result, the functions required of a home router are not defined in this chapter. Authentication technology in each connection configuration is also out of scope.

2.1 Native Connection

2.1.1 Connection Configuration

Requirement: To provide IPv6network reachability via a native connection with no tunnel termination at the Home Router

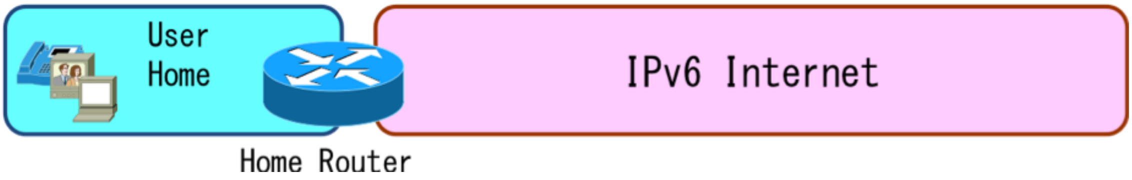

Figure 2-1 Native Connection

2.2 PPPoE/PPPoA

2.2.1 Connection Configuration

Requirement: To provide IPv6network reachability to a user's home on PPP [1][2][3].

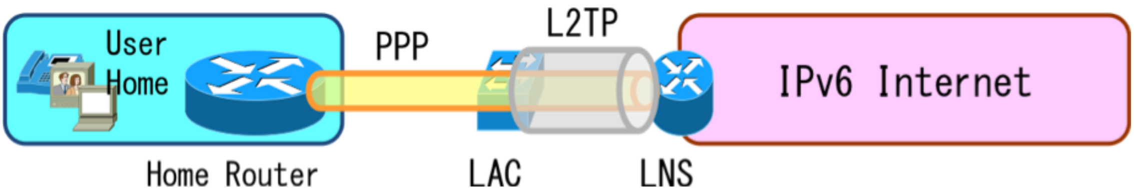

Figure 2-2 PPPoE/PPPoA Connection

2.3 IP-based Tunnel (IPv6 over IPv4・IPv6 over IPv6 etc.)

2.3.1 Connection Configuration

Requirement: To capsulate with IP and provide IPv6network reachability to a user's home [4][5][6][7].

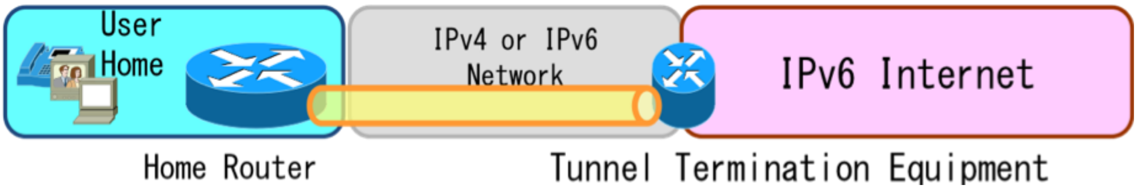

Figure 2-3 IP-based Tunnel Connection

3 Address Assignment Method

In this chapter, various address assignment methods for a terminal to be connected to the WAN-side, LAN-side, and LAN-side segments of a router are described.

3.1 Prefix Assignment

Router requirements when a service provider assigns a prefix to a user are described in the following.

3.1.1 Prefix Information Distributed to a Home Network

Requirement: Router can obtain prefix information from connected ISP using DHCPv6-PD.

Necessity: Mandatory (MUST)

Reason: DHCPv6-PD is the standard protocol for performing IPv6 prefix assignment automatically. Implementation is mandatory to eliminate configuration errors due to manual inputting by a user.

Requirement: Manual configuration should be possible.

Necessity: Mandatory (MUST)

Reason: Mandatory to respond to cases in which a connected ISP has no support for prefix distribution using DHCPv6-PD.

3.1.2 Prefix Size Assigned to Home Network

Requirement: Router can receive the prefix assigned by service provider in the range of /48 - /64.

Necessity: Mandatory (MUST)

Reason: In "IPv6 Address Allocation and Assignment Policy at JPNIC" [8], as assignment primarily of /48 - /64 is required to be done at the end site, the ability to handle a prefix within this range is mandatory.

Remarks:

- When considering separation of wireless/wired segments, or deployment of DMZ, distribution of multiple segments (prefix length shorter than /64) is desirable, but the assigned prefix size is to be decided by the service provider.
- When considering SOHO etc., there is a possibility that a prefix length shorter than /48 will be assigned.

3.1.3 Assignment of Prefix

The prefix distributed by a service provider to a user can be either assigned in a fixed manner or vary with time.

Requirement: Prefix for distribution to user is fixed.

Necessity: Recommended (SHOULD)

Reason: There are many limitations/constraints such as node requirements. (re-numbering when a prefix is changed, level of ongoing communication to be guaranteed during the change, etc., to achieve variable prefix assignment) In the current situation, when considering stable operability of user networks, fixed prefix assignment is more desirable than variable. Hence, fixed assignment is recommended.

Remarks: Even if fixed assignment is the primary concern, considering privacy concealment etc., responding to a prefix change request from the user side should be possible.

Requirement: Prefix for distribution to user varies with time.

Necessity: Optional (MAY)

Reason: Some people have the opinion that this is necessary to guarantee a user's communication privacy. In addition, in the current situation, non-fixed assignment is the mainstream for IPv4 and a user might require an equivalent function. However, given the issue that a user's home equipment can follow a prefix change when online, and given that operation of a Home Router becomes complicated during a prefix change, this is treated as an option in the current situation.

Remarks:

- If a prefix is specified to be unfixed, the router should be able to detect a prefix change (i.e., it should remember prefixes assigned in the past and function properly when a change occurs). In addition, consideration needs to be given to the handling of sessions during ongoing communication, and to support re-numbering of a user's home equipment during the change (also see 3.3.3).
- Whether an address should be fixed or varied with time depends on the service of the service provider; there are advantages and points for consideration with each (see Table 3-1).

Table 3-1　Impact of Fixed/Unfixed Assigned Address

	Category	Specific Image	Occasion	Security/Privacy
Fixed	Address changes every time contract with ISP is terminated	Case in which user changes contract from ISP-A to ISP-B	Operation and management is easy	User not subjected to attack can have advantages of fixed address
	Address changes every time location is changed	Case in which user relocates home to another place		Privacy issue involved
↕	Address changes every time operational event happens	About once every several years, such as ISP backbone design change etc.		
	Address changes every time user makes a request	Case in which user wants to change address after experiencing DoS attack	Possibility that all the addresses in a home may change	User subjected to attack can avoid attack
Unfixed	Address changes every time connection is made	Address changes every time Home Router or PC booted up (to a degree not noticed by the user)	- During link down - During Home Router replacement	

3.2　WAN-side Address

In this section, address allocation to the WAN-side of a Home Router (link with service provider) is described.

3.2.1　Allocation of Global Address

Requirement:　Global address can be allocated to the WAN-side of Home Router. The address to be allocated is not to be from the address space assigned to the user, but rather from a different space owned by the service provider.

Necessity:　Recommended (SHOULD)

Reason:　Due to the service provider's requirement for the ability to perform dead or alive monitoring of a user, and to make it easier for the service provider to implement a service on the router, allocation of the address to the WAN-side of the Home Router should be possible.

Remarks:

- Operation only with a link local address, without allocation of a global address, can also be considered.
- Given that use by the service provider is assumed, it is desirable that the service provider assigns it not from the user-assigned space but rather from a different one. However, if an address managed by the service provider is allocated, it could be beyond user management (beyond recognition). If this address is not managed properly, a security issue may arise, such as allowing unauthorized access to the address that is not expected by the user.

3.2.1.1 Global Address Allocation Method (Automatic)

Assumption: For a case in which global address is allocated to the WAN-side.

Requirement: Global address can be allocated automatically to the WAN-side interface.

Necessity: Mandatory (MUST)

Reason: This is mandatory to achieve automatic setting with no user intervention.

Either of the methods below is mandatory:

[a] SLAAC (Stateless Address Auto Configuration)

[b] DHCPv6

Remarks:

- When using SLAAC, unless in combination with a separate mechanism for informing the configured address (DDNS etc.), the service provider will not be able to know the allocated address.
- For method selection, technical trends (as of April 2009, in DHCPv6, prefix length distribution needs to be used in combination with a separate router advertisement/prefix option etc.), need to be considered. The fact that, in an IPv6 global unicast address, the interface identifier is specified as 64-bit length [46] and should balance with other requirements (address prefix size to be assigned to WAN-side, and issues that might arise (Section 7.1)) also need to be considered.

3.2.1.2 Global Address Allocation Method (Manual)

Assumption: For a case in which a global address is allocated to the WAN-side.

Requirement: Global address can be allocated manually to the WAN-side interface.

Necessity: Mandatory (MUST)

Reason: Although automatic configuration is a prerequisite, manual configuration is also necessary.

3.3 LAN-side Address

In this section, address allocation to the LAN-side of the Home Router (link with user's home network) is described.

3.3.1 Prefix Re-distribution

Requirement: On basis of a prefix received using DHCPv6-PD from ISP, the router can generate a /64 prefix and re-distribute it to the LAN-side.

Necessity: Mandatory (MUST)

Reason: A method to automatically re-distribute a prefix distributed to a user's home equipment by the ISP is mandatory.

Remarks:

- With regard to the protocol for re-distribution, see Section 6.1.
- The method for deciding the /64 prefix if a prefix larger than /64 has been received using DHCPv6-PD is not specified. For example, if a /48 prefix has been received using DHCPv6-PD, it is necessary to decide the value within the range of 49 to 64 bits when re-distributing to the LAN-side. The method for making this decision can be implementation-dependent; it is not specified in this document.

3.3.2 Multiple Prefix Reception

Requirement: Multiple prefixes have been received using DHCPv6-PD from one or more ISPs, and the router can select which prefix is to be re-distributed to the LAN-side.

Necessity: Optional (MAY)

Reason: This function supports environments where a number of upstream ISPs exist and where the ISP may distribute a number of different prefixes. Because an environment with a number of upstream ISPs is considered to be exceptional for a Home Router, this should be treated as optional.

Remarks:

- A connection service whereby distribution of one each of a fixed prefix and a dynamic prefix is assumed.
- Fixed prefix and dynamic prefixes each have their own advantages, so it is

desirable for a user to be able to select either.

- Although a case can be anticipated in which access to a specific network may become impossible after having selected a prefix of either type, that kind of prefix is not specified in this document.

3.3.3 Change of Distributed Prefix

Assumption: The case of a service whereby a user-assigned prefix is varied with time.

Requirement: In case the prefix distributed using DHCPv6-PD by ISP changes due to re-connection of the WAN-side connection, changing the prefix to be distributed to the LAN-side properly should be possible.

Necessity: Recommended (SHOULD)

Reason: In case a service whereby a user-assigned prefix is varied with time is selected, it is necessary to minimize the effects of a service-provider-initiated change of prefix on communication in a user network. As the situation is unclear regarding support provided by home equipment for a change of prefix, this should be treated as a recommended function.

Remarks: Many specific methods are specified (see Sections 3.1.3 and 6.1.2).

4 Access Control Function from Outside

In this chapter, the access control mechanism that is considered to be the minimum requirement for protecting the user home network is described. As a precondition, security functions employed for IPv4 (including the point at which direct reachability from an outside network to the home network is lost due to NAT/NAPT) should also be necessary for an IPv6 Home Router.

4.1 Access Control Function from Outside

4.1.1 To Restrict Access from Outside

4.1.1.1 Basic Setting for Access Restriction

Requirement: Router can perform access restriction at a point where there is communication from inside (LAN-side) to outside (WAN-side), while communication from outside to inside is dropped.

Necessity: Mandatory (MUST)

Reason: Access control equivalent to the initial behavior of the current IPv4 Home Router is considered to be mandatory.

Remarks: Although the default behavior is to restrict communication from outside to inside, it is also necessary to have that communication by setting it at the same time (see also Section 4.1.2).

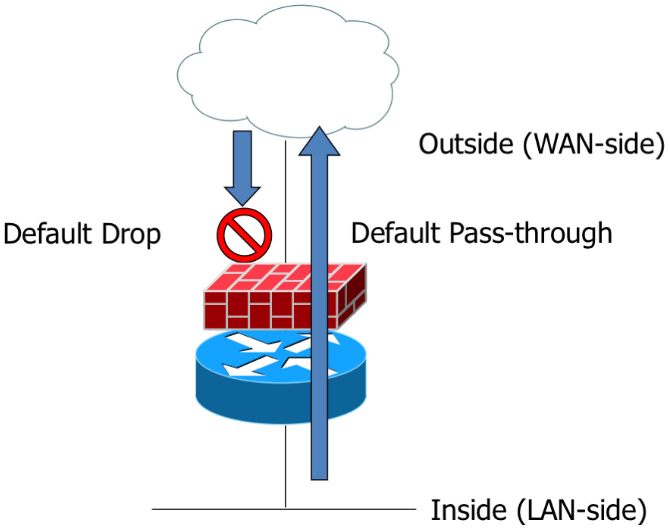

Figure 4-1 Access Control from Outside Function

4.1.1.2 Detailed Setting of Access Restriction

Requirement: Router can restrict access with static filter.

- Traffic is passed through by default from inside to outside.
- For TCP, SYN from outside to inside is dropped by default.
- For UDP, only specific protocols from outside to inside are allowed through, while other protocols are dropped by default.

  Specific protocol: DNS or other service-dependent mandatory protocols (TV, telephony etc.).
- For ICMPv6, only a mandatory message [9] from outside to inside is allowed through, while others are dropped by default.

Necessity: Mandatory (MUST)

Reason: Maintaining the minimum network security level considered necessary in IPv6 is mandatory.

Remarks:

- There are cases in which control of traffic from the inside will be necessary from a security viewpoint. For example, communication with a source address other than the address assigned by the service provider may be restricted.
- Access control must be implemented with consideration given to the re-configuration of fragmented packets.

4.1.1.3 Extended Functions of Access Restriction

Requirement: Router can restrict access with a dynamic filter (SPI).

- Traffic passes through by default from inside to outside.
- Connections through which communications took place from inside to outside should be remembered, and for these connections, traffic passes through from outside to inside.

Necessity: Recommended (SHOULD)

Reason:

- Because this is also an important function to maintain a security level equivalent to the current IPv4 NAT in IPv6 as well, this should be treated as Recommended.
- With regard to SPI, also see the descriptions of RFC 4787 [47].

4.1.2 Setting Criteria for Restricting Access from Outside

Requirement: Router can have criteria on the basis of which access from outside is passed through or dropped.

Necessity: Mandatory (MUST)

Function	Necessity
Router can restrict access by IPv6 source/destination address.	Mandatory (MUST)
Router can recognize the next header (protocol) (See Section 7.2.3)	Mandatory (MUST)
Router can restrict access by protocol type (extended header type etc.)	Recommended (SHOULD)
Router can trace the next header chain	Mandatory (MUST)
Router can restrict access by ICMP Type and Code [9]	Recommended (SHOULD)
Router can restrict access by TCP/UDP source/destination port number	Mandatory (MUST)

Reason: To maintain the security level of the current IPv4 network in IPv6 as well [10].

Remarks: When tracing the next header chain, the degree of depth to which it needs to be traced is implementation-dependent (Currently, there is no specification).

4.2 Restricting Access to the Device Itself

Requirement: Access control of communications to the device itself is possible.

Necessity: Mandatory (MUST)

Reason: Achieving security for service functions provided by equipment itself as an IPv6 host is necessary.

5 DNS Proxy/Resolver Function

In this chapter, the DNS Proxy function that is implemented in many current IPv4 Home Routers and other DNS-related functions such as Resolver function are described. Also see [14].

5.1 Assumptions

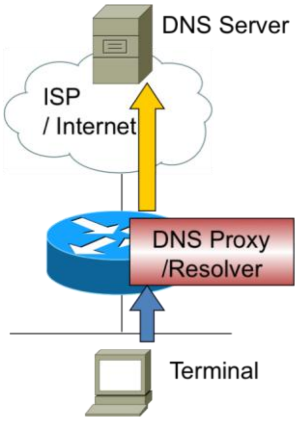

Figure 5-1 DNS Proxy/Resolver Function Concept Figure

Reason for DNS Proxy/Resolver Needed

Benefits of Implementation

DNS server load mitigation (when using cache)

In an environment with no upstream connection, setting the DNS server to the client will be possible.

Local name resolution will be possible.

Drawbacks of Non-implementation

Due to incorrect selection of DNS server at the terminal side, it is possible for problems such as a delay or communication failure to occur.

For access to Web-GUI, direct input of IP address will be necessary instead of FQDN (User convenience lowered). ※Input of IPv6 address will be difficult

http://web.setup/ → http://[2001:db8::1]/

Assumptions for Implementing DNS Proxy/Resolver Functions

The principle is to handle a request from a terminal transparently.

In case a conversion process such as translator or ALG is involved, because this function will be in the functional domain of translator or ALG, it is outside the scope of our current studies.

In case the conversion process above is involved due to implementation at the DNS side, independent studies will be necessary because there is a risk that a terminal may get an unintended query result.

DNS Resolver part is described as an item that should be considered regardless of IPv4 or IPv6.

5.2 Transport

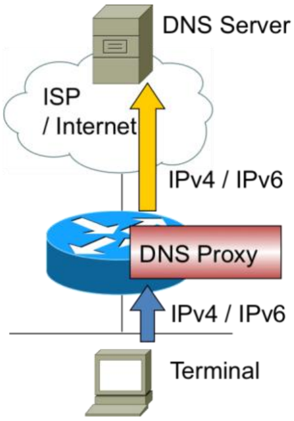

Figure 5-2 Selection of Used Transport

5.2.1 Usable Transport

Requirement: At the upstream side of DNS Proxy (DNS server-side of ISP), both IPv6 transport and IPv4 transport can be usable.

Necessity: Mandatory (MUST)

Reason: To be able to support both cases when the DNS server address specified by ISP etc. may be either IPv4 or IPv6.

5.2.2 Prioritized Transport

Requirement: Proxy operation can be performed with the same transport as a DNS request from a terminal.

Necessity: Optional (MAY)

Reason: Because there is a possibility that, due to a change of transport, the requesting terminal may not be able to get the expected result [15].

Remarks: The reason why Proxy operation with the same transport is not MUST/SHOULD but MAY is because it will be necessary to change transport if there is a cache server beyond a Home Router (DNS Proxy). For example, in case even if the query from a terminal to the DNS Proxy is made with IPv6 transport, a cache server supports IPv4 transport only, so the DNS Proxy will need a transport conversion function.

When performing a Proxy operation with the same transport, the DNS Proxy will need the function to remember the transport requested by the terminal.

As there is an operation in the IPv4 Internet whereby a reply from the DNS server may differ depending on the query source address, alignment of transport does not necessarily get us the same reply. Nevertheless, it is recommended that transport be aligned in terms of probability.

5.3 Type of Address with which DNS Proxy to Listen

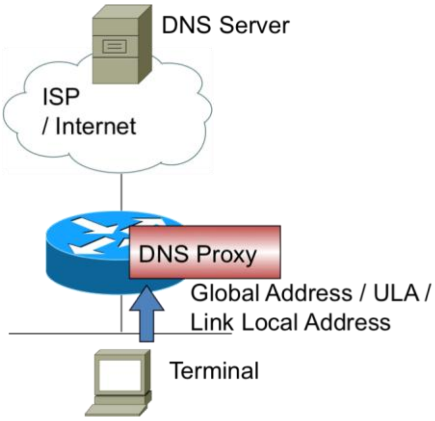

Figure 5-3 Type of Address to listen

5.3.1 Type of Address with which DNS Proxy to Listen

Requirement: Router can listen with a unicast address (any global address, ULA, or link local address).

Necessity: Mandatory (MUST)

Reason: It is necessary to be able to listen with a unicast address at a minimum.

Remarks: When listening with ULA, the DNS Proxy needs to have defined the ULA to be used in advance. Further, when the ULA was already in use on the LAN, a mechanism to generate another ULA that does not conflict will be necessary.

- When the DNS Proxy listens for a query with an ULA, implementation is allowed whereby it is not shown to the outside as an interface and reply is possible only from inside.
- When the DNS Proxy listens for a query with a global address, a situation may exist in which no global address is assigned to the DNS Proxy, such as during upstream connection failure or when setup is not complete. In this case, attention is required as a query packet cannot reach the DNS Proxy.

Further, in order not to become a DNS Open Resolver that may serve as a factor in a DNS amplified attack, consideration such as not accepting queries from the WAN-side is required.

- When the DNS Proxy listens for a query with a link local address, queries from other segments cannot reach the DNS Proxy. Moreover, as it is possible for problems to exist, such as a terminal Resolver not being able to specify link local address etc., attention is required.
  Also, implementing DNS (RFC 4795) [53] can also be considered.

5.4 Selection Method when Multiple DNS Servers Exist

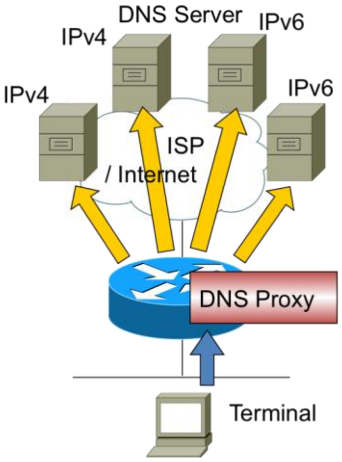

Figure 5-4 Selection of DNS Server

5.4.1 Selection by Sequential Search Method

Requirement: Router can use multiple DNS servers and perform DNS selection by Sequential Search Method.

Necessity: Mandatory (MUST)

Reason: To increase reachability to communication destination.

5.4.2 Arbitrary Selection Function

Requirement: In case there is any function such as Domain Identification Method whereby a DNS server is selected arbitrarily according to a specific policy, the rules set by such function should be followed.

Necessity: Optional (MAY)

Reason: To prioritize the intention of user or ISP.

Remarks:

- Although both Sequential Search Method and Domain Identification Method can be a solution for the DNS server selection issue per service network in a multi-prefix environment, they cannot solve all related problems. Implementation should be done after evaluating benefits and drawbacks [16][17].

- There is no specification regarding priority for the case in which the DNS server exists respectively for IPv6 transport and IPv4 transport.
- There are different opinions such as IPv4 should be used because there is concern about the current IPv6 DNS server, or IPv6 should be used considering migration to IPv6 in the near future. Opinions are divided and this is an issue for further study.
- Among Resolvers of various OS's, there are many that prioritize IPv6.
- In DNS, the assumption is that the same reply should be made regardless of transport.

5.5 Cache

5.5.1 Cache Function

Requirement: The results obtained by a DNS request from a terminal should be cached, and such cached information should be returned in subsequent and similar DNS requests.

Necessity: Optional (MAY)

Reason: Because ISP's DNS server load mitigation (suppression of request/reply packet) is possible.

Remarks: As a prompt response will be required in case a DNS-related vulnerability such as a Kaminsky Attack [18] is found, implementation needs to be done after evaluating benefits and drawbacks.

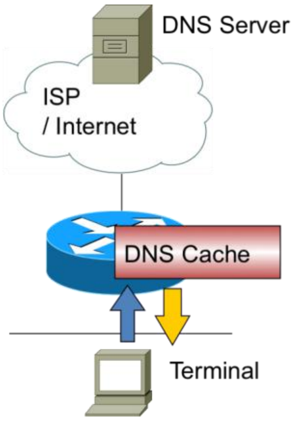

Figure 5-5 DNS Cache Function

5.6 Resolver Function

Although the following functions required of a Resolver are not IPv6-specific, they are more relevant than in IPv4. Hence, it is recommended that they are considered to be part of the specification to be implemented in a Home Router.

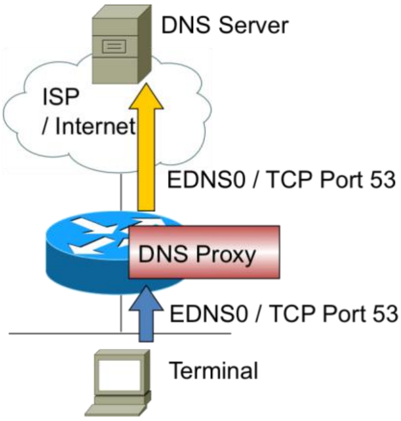

Figure 5-6 DNS Resolver Function

5.6.1 Supported Resource Record

Requirement: DNS request from a terminal should all be processed transparently regardless of resource record (RR) type.

Necessity: Mandatory (MUST)

Reason: Because the requesting terminal cannot get the expected result if RR type is limited.

5.6.2 EDNS0

Requirement: Router can process EDNS0[19]-supported request (including OPT RR) packet transparently, and send a reply exceeding 512 bytes to a terminal.

Necessity: Mandatory (MUST)

Reason: Because situations are arising in which a DNS reply packet exceeds 512 bytes, due to use of AAAA or PTR, SPF, SRV, TXT, DNSSEC etc.

5.6.3 TCP Port 53 Support

Requirement: In case the terminal (after receiving DNS Header TC=1 [20][21]) falls back to TCP connection, the DNS request can be processed transparently.

Listening not only at UDP Port 53 but also at TCP Port 53.

Necessity: Mandatory (MUST)

Reason: In order not to impact the DNS request-related behavior of a terminal.

5.6.4 DNSSEC (Reference)

Requirement: Router can process the following packets that support DNSSEC transparently or properly [22][23][24].

EDNS0 (OPT RR) DO bit set.

RRSIG, DNSKEY, DS, NSEC, NSEC3, NSEC3PARAM RR used.

For DNS Header Bit, CD (checking disabled) or AD (authentic data) is used.

Necessity: Optional (MAY)

Reason: In order not to impact the DNS request-related behavior of a terminal.

Remarks: Currently, this is not implemented in Windows XP or Windows Vista; Urgency seems to be not so great. As DNSSEC implementation is planned for Windows 7, and use in combination with IPSec is assumed, it may become necessary to look into IPsec support [25].

As a Home Router's DNS Proxy/Resolver function, whether to implement recursion process including signature verification, or to operate as single-function Proxy with IP address conversion only is implementation-dependent.

6 Information Distribution Function to Home network

In this chapter, the distribution method of address/prefix information and server information from the Home Router to the home terminal are described.

6.1 Distributing Address/Prefix Information

6.1.1 Distribution Using RA

Requirement: Router has a function to inform by RA the prefix to be assigned to home network terminal.

Necessity: Mandatory (MUST)

Reason: This function is mandatory for an IPv6 router [28].

Remarks: For distribution policy within LAN in case multiple prefix has been obtained from ISP etc., see Section 3.3.2.

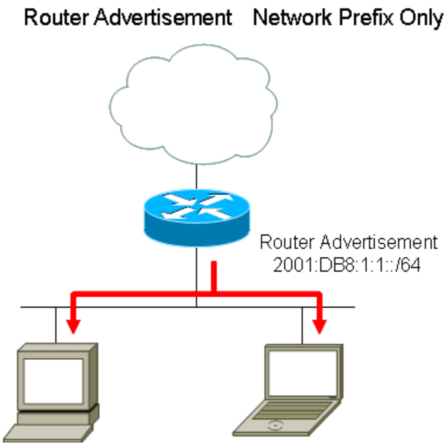

Figure 6-1 Distribution of Prefix Information Using RA

Requirement: Prefix length informed by RA should be /64 by default.

Necessity: Mandatory (MUST)

Reason: Because many implementations have the last 64 bit of the address as the interface ID in a stateless address automatic configuration in the terminal.

Remarks: Take note of the fact that, when distribution is done with a prefix length other than /64, there are cases in which the address does not get set properly to equipment in a LAN. For example, address generation cannot be done with a prefix other than /64 in Windows Vista SP1.

In SLAAC (RFC 4862) specification, it is specified that, in case the sum of the prefix length in the Prefix Information Option of RA and interface ID length held by the node itself is not 128, the Prefix Information Option is ignored (MUST) [29][48].

6.1.2 Distribution Using DHCPv6

Requirement: Router has a function to inform an address to a home terminal by DHCPv6 [27].

Necessity: Optional (MAY)

Reason: Because it is effective when assigning a specific address to a home network terminal.

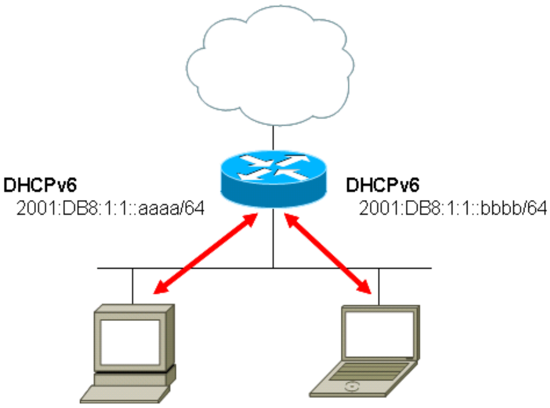

Figure 6-2 Distribution of Address Information by DHCPv6

Requirement: There should be a function for distributing a prefix to home equipment (router) by DHCPv6-PD [30]. There should be a function that enables specification of the prefix to be distributed per equipment.

Necessity: Optional (MAY)

Reason: In case multiple routers exist at a home, to distribute the prefix to be assigned to the terminal connected to the relevant router.

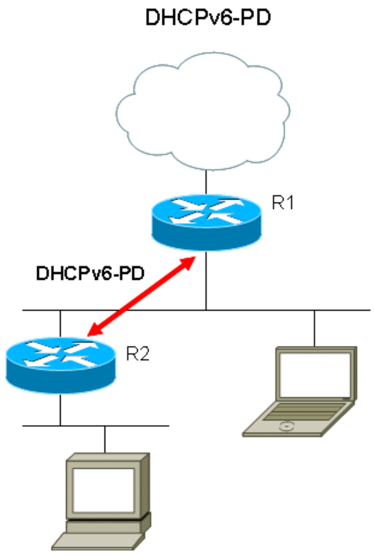

Figure 6-3 Distribution of Prefix Information by DHCPv6-PD

6.2 Distributing Server Information

6.2.1 Distribution using RA

Requirement: Router has a function for distributing DNS server address to the LAN segment.

Necessity: Optional (MAY)

Reason: Because implementation [31] to get a DNS server information from RA is expected at a terminal.

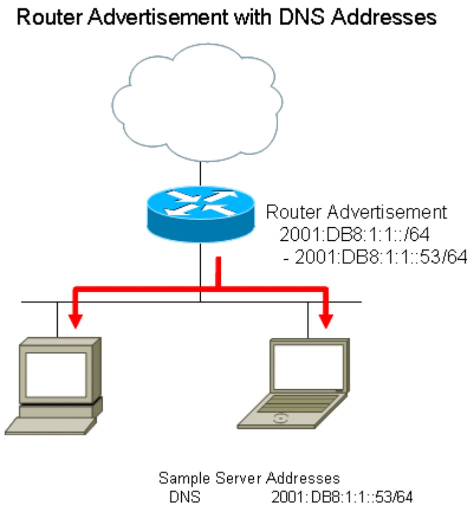

Figure 6-4 Distribution of Server Information by RA

6.2.2 Distribution using DHCPv6

Requirement: Router has a function for distributing DNS server address by DHCPv6 to a LAN segment.

Necessity: Mandatory (MUST)

Reason: Because the method to get DNS server information by DHCPv6 is common with implementation at the terminal side.

Remarks: With standardization, DHCPv6 is Standard Track (RFC 3646), while RA is Experimental (RFC 5006) [32].

Requirement: Router has a function for distributing other server addresses (SIP, NTP etc.) by DHCPv6 to a LAN segment.

Necessity: Optional (MAY)

Reason: To automatically set to the terminal the server information required for a user to use various services.

Remarks: Which server address is to be distributed depends on the specification of an ISP's service.

Server address distributable by DHCPv6:

SIP server [49], DNS server [50], NIS server [51], SNTP server [52] etc.

DHCPv6 parameter list:

http://www.iana.org/assignments/dhcpv6-parameters/

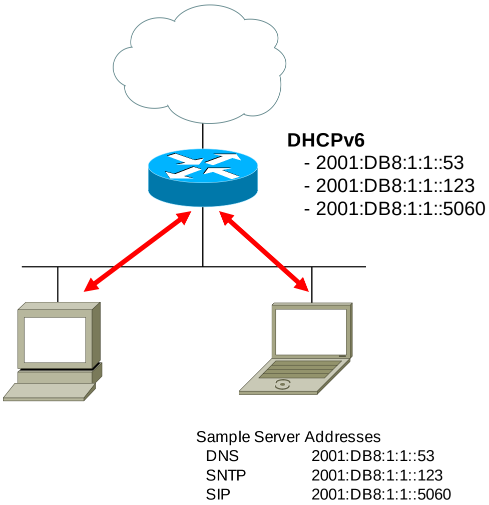

Figure 6-5 Distribution of Server Information by DHCPv6

6.2.3 DHCPv6 Relay Function

Requirement: Router has a DHCPv6 Relay function.

Necessity: Optional (MAY)

Reason: Because the case in which an ISP manages a home network setting is anticipated.

Remarks: DHCPv6 server function and DHCPv6 relay function are not concurrently used on same equipment.

- When the DHCPv6 Relay function is enabled, the DHCPv6 Server function should be disabled (In case the DHCPv6 Server function has been implemented).
- When the DHCPv6 Server function is enabled, the DHCPv6 Relay function should be disabled.

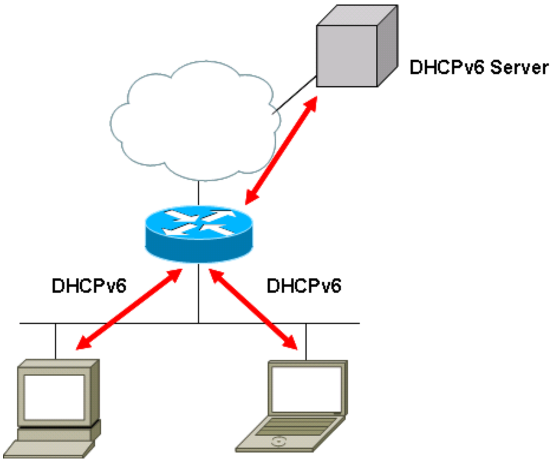

Figure 6-6 DHCPv6 Relay Function

7 Routing/Multicast Function

In this chapter, the minimum-required routing function/multicast function for the Home Router to get connected to a service using IPv6 is described.

7.1 Handling Communications to Unused Address/Network

Assumption: Service to perform address assignment by DHCPv6-PD.

Requirement: Router has a function not to forward traffic addressed to the assigned prefix upstream.

Necessity: Mandatory (MUST)

Reason: If packets addressed to an unused address space are forwarded to a default route, such packets get ping-ponged between a Home Router and an ISP router until TTL gets to 0. This ping-pong behavior should be prevented.

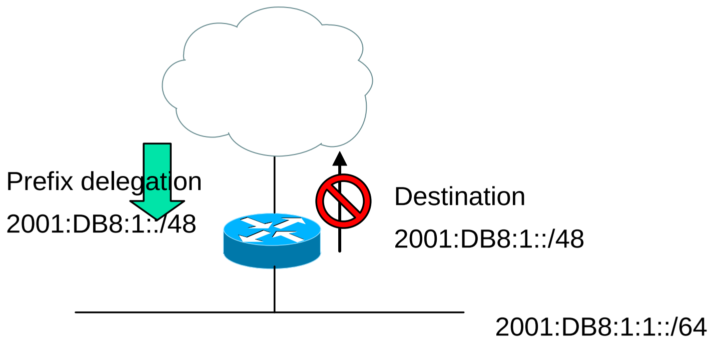

Figure 7-1 The Service To Do Address Assignment by DHCPv6-PD

Assumption: Service to perform connection with the WAN-side as a Point-to-Point link.

Requirement: When the router receives packets for an address other than own interface address on a Point-to-Point link, ICMPv6 Destination Unreachable messages, Code 3 (Address unreachable) should be sent out, and packets should not be forwarded [33].

Necessity: Mandatory (MUST)

Reason: To prevent packets from getting ping-ponged between Home Router and ISP Router until TTL gets to 0.

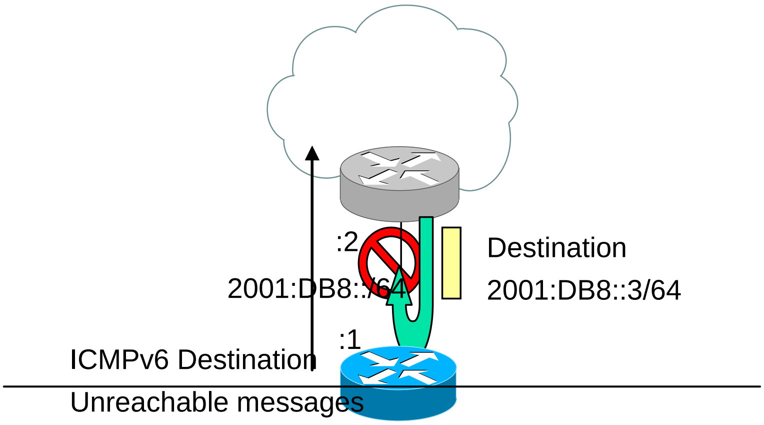

Figure 7-2 Service To Connect with WAN-side as a Point-to-Point Link

7.2 Routing Information/Extension Header

7.2.1 Routing Control on WAN-side

Requirement: Static route for WAN-side can be configured.

Necessity: Mandatory (MUST)

Reason: Because at least the function for explicitly setting a default route etc. in a router is required.

Remarks: Because the ICMPv6 redirect function will not work properly if a link local address cannot be specified to the next hop address, it is also necessary to be able to specify the link local address.

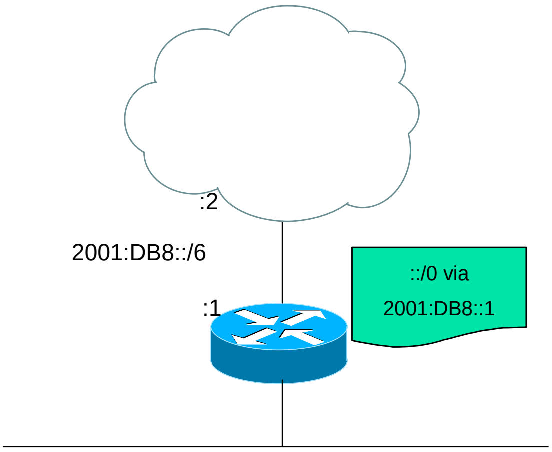

Figure 7-3 Static Route Setting for WAN-side

Requirement: Automatic configuration of default route using RA should be possible.

Necessity: Mandatory (MUST)

Reason: Because consideration is necessary for a service whereby IPv6 address is configured by RA.

Remarks: Although a router in general does not support automatic configuration of a route by RA, it is important for a Home Router to perform setting for a service provider without the user's manual intervention [48]. Also, when multiple WAN interfaces exist and multiple RA's are received, attention is called for as it is necessary to decide which default route should be prioritized. This should be treated as an item for further study (see Section 9.2).

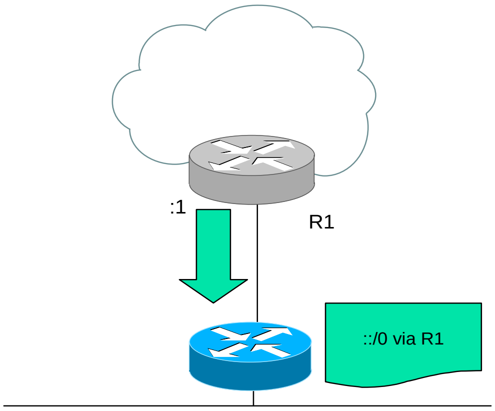

Figure 7-4 Automatic Configuration of Default Route Using RA

7.2.2 Route Control to LAN-side

Requirement: Route distribution to the LAN-side by RIPng [34] is possible.

Necessity: Optional (MAY)

Reason: Because its use is anticipated when controlling the route to the network connected to a router's LAN side.

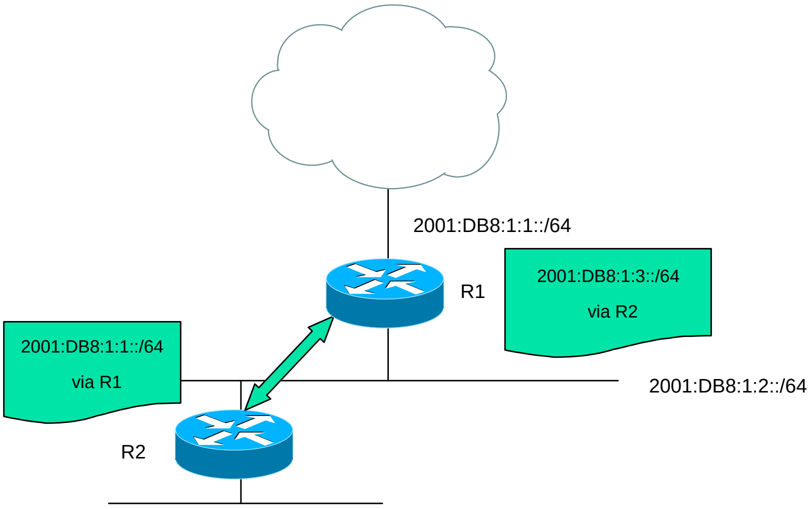

Figure 7-5 Route Control by RIPng

Requirement: It is possible to distribute a route to the LAN-side by More-Specific Routes [35].

Necessity: Optional (MAY)

Reason: Because its use is anticipated when controlling routes to a network connected to a router's LAN-side.

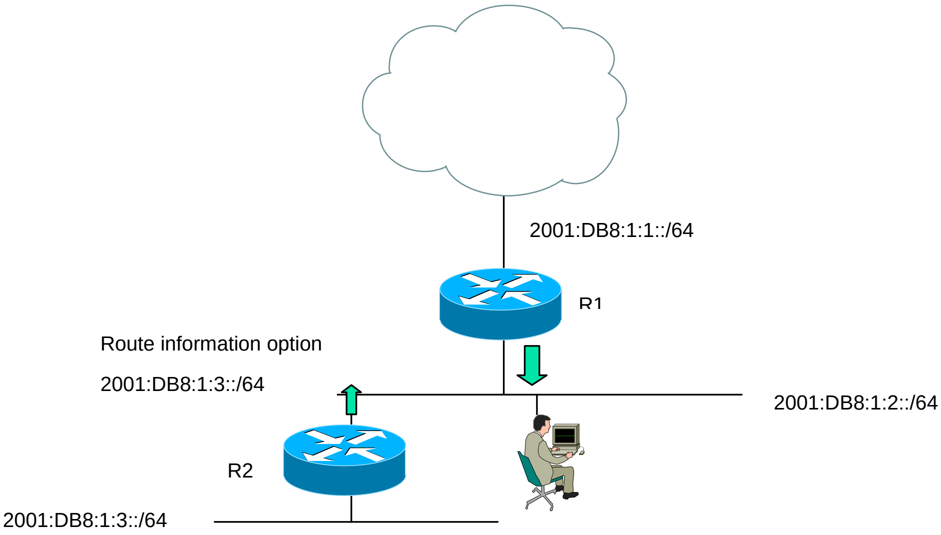

Figure 7-6 Use of More-Specific Route

7.2.3 Extension Header

Requirement: It is possible to prohibit RH0 (Type 0 routing headers) packet forwarding.

Necessity: Mandatory (MUST)

Reason: Because consideration of a DoS attack by IPv6 source routing [11] is necessary, and its use is prohibited in the current specification.

Remarks: Rather than implementation whereby routing header is completely prohibited, it is necessary to be able to look at the type accurately and prohibit Type 0 only.

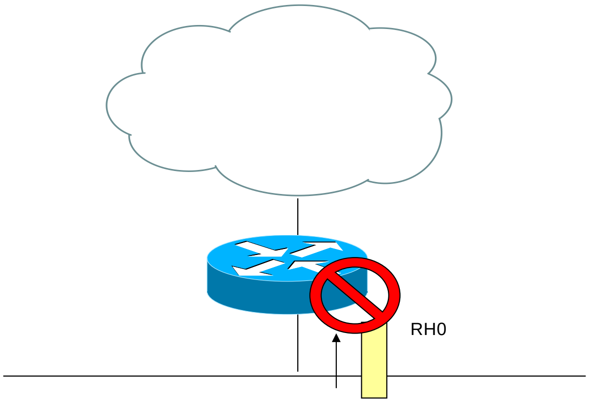

Figure 7-7 RH0 Packet Forwarding Prohibited

7.3 IPv6 Multicast

Because a Home Router's support for the IPv6 Multicast function largely depends on an ISP's service, the overall function should be treated as Optional (MAY).

7.3.1 Function per IPv6 Multicast Connection Configuration

For connection to an IPv6 multicast service, two connection patterns can be considered depending on the protocol used upstream from a Home Router (to WAN-side). The functions required for each connection configuration are shown below.

7.3.2 Connection by PIM

Join/Leave for Multicast group is informed to ISP using PIM.

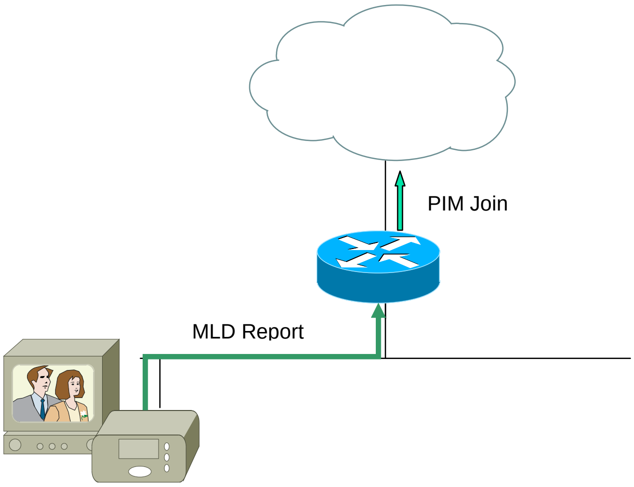

Figure 7-8 Multicast Connection Using PIM

Assumption: The case of connecting to Multicast service by PIM

Requirement: Router has Multicast routing function by PIM [36][37][38].

Necessity: Mandatory (MUST)

Reason: To support services using PIM as the WAN-side protocol.

Remarks: Many optional functions exist in the specification of PIM-SM/SSM, and depending on the implementation status of equipment, problems may occur in terms of inter-operability. Due to this, care should be taken during implementation. This is treated as an item for further study (See Section 9.2).

Assumption: The case of connecting to Multicast service using PIM.

Requirement: Router has MLD (v1/v2) router function [39][40][41].

Necessity: Mandatory (MUST)

Reason: Because support for MLD router function is necessary for terminal to participate in a Multicast network during PIM connection.

7.3.3 Connection by MLD Proxy

Join/Leave Multicast group is informed to ISP using MLD.

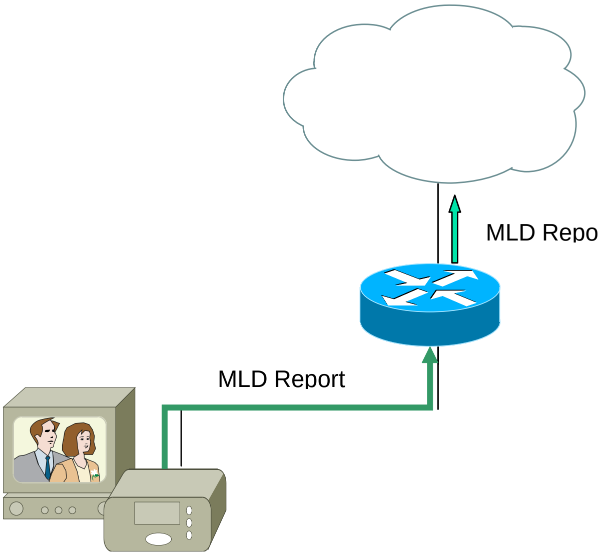

Figure 7-9 Multicast Connection Using MLD Proxy

Assumption: Case of connecting to Multicast service using MLD Proxy.

Requirement: Router has MLD (v1/v2) Proxy [42] function.

Necessity: Mandatory (MUST)

Reason: To inform Join/Leave Multicast group to ISP-side by MLD.

7.3.4 MLD Snooping

In any of the connection configurations described in Section 7.3.1, it is desirable to implement the following MLD snooping [43] function as well if a Home Router has a switch function. Also, if a Home Router has a wireless LAN function, it is desirable to have a function equivalent to MLD snooping that restricts the flow of unnecessary Multicast traffic to a wireless LAN-connected node.

Requirement: Router has MLD (v1/v2) snooping [43] function.

Necessity: Optional (MAY)

Reason: Because its use is anticipated only when a router has a switching function.

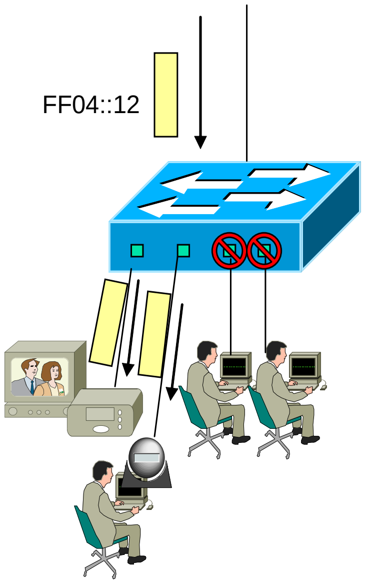

Figure 7-10 MLD Snooping Function

8 Configuration Method on Service-side

In this chapter, the configuration method and items to be configured for a Home Router are described. Note that the agent who does the setting is the service provider.

8.1 Configuration Method

Overview: A Home Router is equipped with a function for the service provider to feed the necessary setting to it.

Necessity: Mandatory (MUST)

Reason: Because users who are not familiar with the security configuration can get a service with a certain level of security.

Remarks: Specific setting methods are listed with examples below.

8.1.1 Automatic Configuration

In this section, the method whereby a Home Router gets the necessary setting information autonomously, with no direct operation of a Home Router by the service provider, is listed with examples below.

- Router has SLAAC function.

  Method of setting an IPv6 address by RA without using a DHCPv6 server.

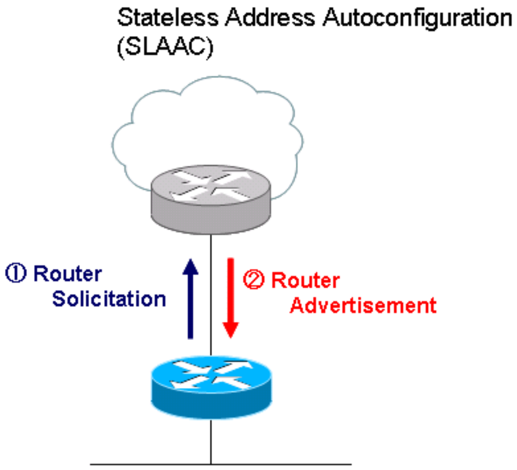

Figure 8-1 Automatic Configuration by SLAAC

- Router has DHCPv6 client function.

DHCPv6 client function is a function for requesting information such as IPv6 address to a DHCPv6 server and configuring the information obtained to become a host.

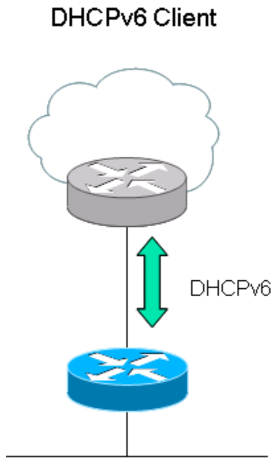

Figure 8-2 Address Configuration by DHCPv6

- Router can use TR-069 for address configuration.

Setting method using TR-069: protocol for remotely controlling CPE defined by BroadBand Forum.

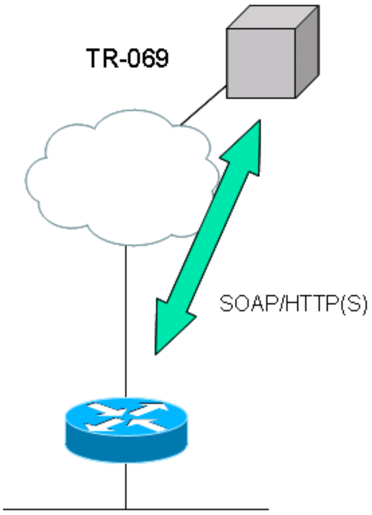

Figure 8-3 Address Configuration by TR-069

- Router can be configured by UPnP.

Method of configuring an address using UPnP: automatic equipment registration mechanism defined by UPnP Forum.

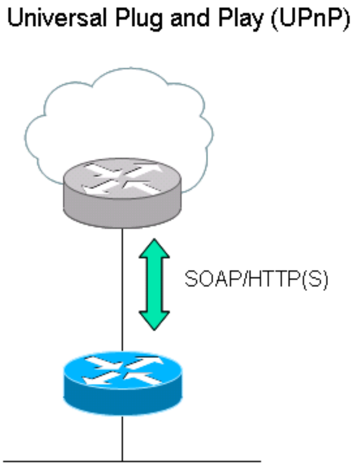

Figure 8-4 Address Configuration by UPnP

8.1.2 Manual Configuration

Because a case is anticipated in which a service provider manually sets a Home Router directly, the interface for that needs to be implemented. Specifically, Web interface or telnet, ssh etc. will be used.

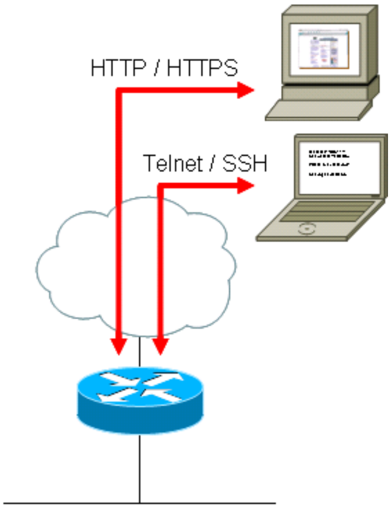

Figure 8-5 Manual Configuration Concept Figure

8.2 Configuration Items

In this section, specific items to be configured for a Home Router by the configuring methods mentioned in Section 8.1 are described.

8.2.1 Address Configuration

See Chapter 3.

8.2.2 Security-related Configuration

Requirement: It should be possible for a user to make setting changes to the Access Restricting function of equipment directly, and, setting should also be possible from the operator-side such as the ISP.

Necessity: Recommended（SHOULD）

Reason: To enable services to be provided whereby even users not familiar with security setting can maintain the necessary security level while being serviced.

Remarks: Because this is a service-dependent function, it should be possible for the user to disable the function when it is not being used.

Requirement: There should be means for accessing a Home Router's administration interface from an ISP's administration segment at the WAN interface-side.

Necessity: Optional (MAY)

Reason: To restrict unauthorized access from outside when a global address is assigned and monitored.

8.2.3 DNS Configuration

In this section, the method of configuring a DNS server address for a Home Router if the Home Router uses a DNS Proxy function is described. For other items, see Chapter 5.

8.2.3.1 DNS Server Address for DNS Proxy Function

Requirement: Router can use DNS server information obtained through means such as DHCPv6.

Necessity: Mandatory (MUST)

Reason: To eliminate setting errors by automation.

Requirement: Manual setting is possible.

Necessity: Mandatory (MUST)

Reason: Because there may be a case in which automatic configuration by an ISP is not possible.

8.2.4 Home Network Configuration

In this section, the method of configuring necessary information when a Home Router performs setting for Home equipment is described.

8.2.4.1 Prefix Distributed to LAN-side

See Chapter 3.

8.2.4.2 Various Server Address Distributed to LAN-side

Requirement: Router can get it from the connected ISP by DHCPv6.

Necessity: Mandatory (MUST)

Reason: Because it is generally the case that a variety of server information distributed to a router differs depending on the service provided, and a method that enables selective distribution of necessary information is desirable.

Requirement: Manual setting is possible.

Necessity: Mandatory (MUST)

Reason: Because there may be a case in which automatic configuration by an ISP is not possible.

8.2.4.3 DHCPv6 Server Address for DHCPv6 Relay Function

Assumption: Case using DHCPv6 Relay function

Requirement: Manual setting is possible.

Necessity: Mandatory (MUST)

Reason: Because an automatic method for assigning a DHCPv6 server address is not provided.

Remarks: By making Multicast routing work between the DHCPv6 server and a Home Router, it is also possible to make explicitly setting the DHCPv6 server address unnecessary.

8.2.5 Routing/Multicast Configuration

See Chapter 7.

9 Conclusion

9.1 Summary of Functions Required of IPv6 Home Router

“Minimum-required Common Functions for IPv6 Home Router” described up to the preceding chapter are summarized in Table 9-1. Although this Guideline does not cover all the functions of the IPv6 Home Router, implementation considering at least the functions listed here is desired for an IPv6 Home Router. Note that items not studied and treated for further discussion are summarized in the next section (Section 9.2).

Table 9-1 List of Functions Needed for IPv6 Home Router

Num	Minor Item		Necessity	Section
1	It is possible to get prefix information distributed to a home network from the connected ISP using DHCPv6-PD.		Mandatory	3.1.1
2	Manual setting of prefix information distributed to a home network is possible.		Mandatory	3.1.1
3	It is possible to receive the prefix assigned by service provider in the range of /48～/64.		Mandatory	3.1.2
4	Prefix for distribution to user is fixed.		Recommended	3.1.3
5	Prefix for distribution to user varies with time.		Optional	3.1.3
6	It is possible to allocate a global address to the WAN-side of a Home Router. The address to be allocated is not from the address space assigned to user, but rather from a different space owned by the service provider.		Recommended	3.2.1
7	Assumption 6	It is possible to allocate WAN-side global address dynamically.	Mandatory	3.2.1.1
8	Assumption 6	It is possible to allocate WAN-side global address manually.	Mandatory	3.2.1.2
9	Based on the prefix received using DHCPv6-PD from ISP, it is possible to generate /64 prefix and re-distribute it to the LAN-side.		Mandatory	3.3.1
10	In case multiple prefixes have been received using		Optional	3.3.2

	DHCPv6-PD from one or multiple ISPs, it is possible to select which prefix to re-distribute to the LAN-side.			
11	Assumption 5	In case the prefix distributed using DHCPv6-PD by an ISP changes due to re-connection of the WAN-side connection, it is possible to change the prefix to be distributed to the LAN-side properly.	Recommended	3.3.3
12	It is possible to restrict access where there is communication from inside (LAN-side) to outside (WAN-side), while communication from outside to inside is restricted by default.		Mandatory	4.1.1.1
13	It is possible to restrict access with a static filter.		Mandatory	4.1.1.2
14	It is possible to restrict access with a dynamic filter (SPI).		Recommended	4.1.1.3
15	It is possible to set up criteria by which access from outside is allowed or restricted.		Mandatory	4.1.2
16	It is possible to set up a filter to control access of communications to the router itself.		Mandatory	4.2
17	At the upstream side of DNS Proxy (DNS server-side of ISP), both IPv6 transport and IPv4 transport are usable.		Mandatory	5.2.1
18	Proxy operation is performed with the same transport as DNS request from terminal.		Optional	5.2.2
19	For DNS Proxy, listen for unicast address (any global address, ULA, or link local address) is possible.		Mandatory	5.3.1
20	It is possible to use multiple DNS servers, and perform DNS selection by Sequential Search Method.		Mandatory	5.4.1
21	In case there is any function such as Domain Identification Method whereby a DNS server is selected arbitrarily according to a specific policy, the rules set by such function are followed.		Optional	5.4.2
22	The results obtained by a DNS request from		Optional	5.5

	terminal are cached, and such cached information is returned in a subsequent and similar DNS request.		
23	DNS request from terminal is processed transparently regardless of resource record (RR) type.	Mandatory	5.6.1
24	It is possible to process an EDNS0-supported request (including OPT RR) packet transparently, and send a reply exceeding 512 bytes to terminal.	Mandatory	5.6.2
25	The case in which terminal (after receiving DNS Header TC=1) does fallback to TCP connection and makes a DNS request is processed transparently. Listening should be performed not only at UDP Port 53 but also at TCP Port 53.	Mandatory	5.6.3
26	It is possible to process the following packets that support DNSSEC transparently or properly.	Optional	5.6.4
27	It has a function to inform the prefix to be assigned to a home network terminal by RA.	Mandatory	6.1.1
28	Prefix length informed by RA is /64 by default.	Mandatory	6.1.1
29	It has a function to inform an address to a home terminal by DHCPv6.	Optional	6.1.2
30	It has a function for distributing a prefix to home equipment (router) by DHCPv6-PD. It has a function that enables the prefix distributed to be specified per item of equipment.	Optional	6.1.2
31	It has a function for distributing a DNS server address to a LAN segment.	Optional	6.2.1
32	It has a function for distributing a DNS server address by DHCPv6 to a LAN segment.	Mandatory	6.2.2
33	It has a function for distributing another server address (SIP, NTP etc.) by DHCPv6 to a LAN segment.	Optional	6.2.2
34	It has a DHCPv6 Relay function.	Optional	6.2.3
35	Assumption 30 It has a function not to forward traffic addressed to the assigned prefix upstream.	Mandatory	7.1

36	When the router receives packets for addresses other than own interface address on a Point-to-Point link, ICMPv6 Destination Unreachable messages, Code 3 (Address unreachable) should be sent out, and packets should not be forwarded.		Mandatory	7.1
37	It is possible to configure a static route for a WAN.		Mandatory	7.2.1
38	Automatic configuration of default route at the WAN-side using RA is possible.		Mandatory	7.2.1
39	Route advertisement to the LAN-side by RIPng is possible.		Optional	7.2.2
40	It is possible to distribute a route to the LAN-side by More-Specific Routes.		Optional	7.2.2
41	It is possible to prohibit RH0 (Type 0 Routing Headers) packet forwarding.		Mandatory	7.2.3
42	IPv6 Multicast function		Optional	7.3
43	Assumption 42	Multicast using PIM is usable.	Optional	7.3
44	Assumption 43	It has a Multicast routing function by PIM.	Mandatory	7.3.2
45	Assumption 43	It has a MLD (v1/v2) router function.	Mandatory	7.3.2
46	Assumption 42	It is possible to use a MLD Proxy and connect to Multicast service.	Optional	7.3
47	Assumption 46	It has a MLD (v1/v2) Proxy function.	Mandatory	7.3.3
48	Assumption 42	It has a MLD (v1/v2) snooping function.	Optional	7.3.4
49	Home Router is equipped with the function for the service provider to feed the necessary setting to that Home Router.		Mandatory	8.1.1
50	It is possible for the user to change the setting of the Access Restriction function of equipment directly, and setting is possible from the operator-side such as the ISP.		Recommended	8.2.2
51	It has a means for accessing Home Router's		Optional	8.2.2

<table>
<tr><td></td><td colspan="2">administration interface from ISP's administration segment at the WAN interface-side.</td><td></td><td></td></tr>
<tr><td>52</td><td colspan="2">It is possible to use DNS server information obtained through means such as DHCPv6.</td><td>Mandatory</td><td>8.2.3.1</td></tr>
<tr><td>53</td><td colspan="2">Manual configuration of DNS server address is possible.</td><td>Mandatory</td><td>8.2.3.1</td></tr>
<tr><td>54</td><td colspan="2">It is possible to get various server addresses from the connected ISP by DHCPv6.</td><td>Mandatory</td><td>8.2.4.2</td></tr>
<tr><td>55</td><td colspan="2">Manual configuration of various server addresses is possible.</td><td>Mandatory</td><td>8.2.4.2</td></tr>
<tr><td>56</td><td>Assumption 34</td><td>Manual configuration of DHCPv6 server address is possible.</td><td>Mandatory</td><td>8.2.4.3</td></tr>
</table>

9.2 Study Items for Next Edition

In this Guideline, not all of the functions of the Home Router could be covered in definitions of functions, so further studies are required in the future. The items that need further study are summarized below.

9.2.1 Items that Require Review/Detailed Studies

- Necessity of WAN-side global address
- Fragment process during filtering
- Number of supported headers of extension header chain
- Support for transport protocol other than TCP, UDP
- Recommended value for filtering
  - ➢ Usable applications list etc.
- Sorting of DNS transport discussion
- Re-consideration regarding PIM implementation

9.2.2 Items Not Studied

- Issues during DNS service
  - ➢ Source port randomization, DNSSEC support etc.
- Provider connection function (service support per provider)
  - ➢ Point-to-Multipoint connection, ISP service automatic distinction function etc.
- Multi-prefix support (Multiple ISP connection)

  - Multi-session, default route handling, 66NAT etc.
- Subnet/router/anycast handing
- Tunnel connection function
- IPv4/IPv6 inter-conversion function
- Unfixed prefix support function
- uPnP
- Bonjour
- Node discovery function
- mDNS
- Other unstudied router functions (for reference)

QoS function, dynamic DNS registration, static NAT, bridge function, equipment access control (MAC address authentication etc.), home gateway individual authentication (individual identification), 802.1x authentication, Wireless function (802.11, BlueTooth), setup-related function (initial setting function, setting by Web), various media support (Wireless, Ether, USB, IEEE1394, telephony, ISDN) etc.

9.3 Study Members

Study members are listed below. Members other than those in charge of forum duties are listed according to the Japanese syllabary of their organization name.

Name	Organization
ARANO, Takashi(WG chair)	Intec NetCore Inc.
KITAGUCHI, Yoshiaki(chair)	Intec NetCore Inc.
FUJISAKI, Tomohiro(co-chair)	Nippon Telegraph and Telephone Corporation
NAKAGAWA, Akira(co-chair)	KDDI Corporation
INNAMI, Tetsuya(co-chair)	SoftBank BB Corp.
ATARASHI, Yoshifumi	Alaxala Networks Corporation
KASHIMURA, Yasuo	Alcatel-Lucent
ASHIDA, Hiroyuki	its communications Inc.
SAHARA, Tomoyuki	Internet Initiative Japan Inc.
KAWASHIMA, Masanobu	NEC Access Technica, Ltd.
SUZUKI, Sousuke	NTT Communications Corporation
UEMATSU, Takashi	Nippon Telegraph and Telephone West Corporation
SHIBATA, Takumi	Nippon Telegraph and Telephone West Corporation
MIZUKOSHI, Ichiro	Nippon Telegraph and Telephone East Corporation
OKADA, Shingo	Nippon Telegraph and Telephone Corporation
KAWASHIMA, Michio	KDDI Corporation
HEI, Yuuichiro	KDDI R&D Laboratories
TSUCHIYA, Shishio	Cisco Systems G.K.
KOHNO, Miya	Juniper Networks
KAMINE, Yoshiaki	So-net Entertainment Corporation
SAKODA, Hiroshi	So-net Entertainment Corporation
YAMAGUCHI, Takuya	So-net Entertainment Corporation
MURAKAMI, Makoto	SoftBank Telecom Corp.
KOBAYASHI, Takeki	SoftBank BB Corp.
SUGANUMA, Makoto	Densan Co., Ltd.
HANAYAMA, Hiroshi	Net One Systems Co., Ltd.
IDA, Yoshihiro	Panasonic Communications Co., Ltd.
MOTOHASHI, Atsushi	Fujitsu Limited
ONODA, Mitsuhiro	Yamaha Corporation

9.4 Reference List

[1] RFC 5072: IP Version6 over PPP

[2] RFC 5172: Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol

[3] RFC 1994: PPP Challenge Handshake Authentication Protocol (CHAP)

[4] RFC 3056: Connection of IPv6 Domains via IPv4 Clouds (6to4)

[5] RFC 4380: Tunneling IPv6 over UDP through Network Address Translations (Teredo)

[6] RFC 2784: Generic Routing Encapsulation (GRE)

[7] Draft-kuwabara-softwire-ipv6-via-l2tpv2-00: A Model of IPv6 Internet Access Service via L2TPv2 Tunnel (softwire)

[8] IPv6 Address Allocation and Assignment Policy at JPNIC
http://www.nic.ad.jp/doc/jpnic-01078.html

[9] RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls

[10] RFC 4864: Local Network Protection for IPv6

[11] RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

[12] NAT66 IPv6-to-IPv6 Network Address Translation

[13] DOCSIS 3.0 specification http://www.cablelabs.com/specifications/doc30.html

[14] DNS Proxy Implementation Guidelines　(draft-ietf-dnsext-dnsproxy-03)[work in progress]

[15] RFC 3484: Default Address Selection for Internet Protocol version 6 (IPv6)

[16] RFC 4477: Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues

[17] A Study into the Construction of IPv6 Multi-Prefix Environment
http://www.v6pc.jp/pdf/v6pc-mp-1.0.pdf

[18] Kaminsky Attack-related Information
http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning.html

[19] RFC 2671: Extension Mechanisms for DNS (EDNS0)

[20] RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

[21] RFC 1123: Requirements for Internet Hosts—Application and Support

[22] RFC 4033: DNS Security Introduction and Requirements

[23] RFC 4034: Resource Records for the DNS Security Extensions

[24] RFC 4035: Protocol Modifications for the DNS Security Extensions

[25] DNSSEC on Windows 7 DNS client
http://blogs.technet.com/sseshad/archive/2008/11/11/dnssec-on-windows-7-dns-clien

t.aspx

[26] RFC 4294: IPv6 Node Requirements

[27] RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

[28] RFC 4294: IPv6 Node Requirements

[29] RFC 4861: Neighbor Discovery for IP version 6 (IPv6)

[30] RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6

[31] RFC 5006: IPv6 Router Advertisement Option for DNS Configuration

[32] RFC 4339: IPv6 Host Configuration of DNS Server Information Approaches

[33] RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

[34] RFC 2080: RIPng for IPv6

[35] RFC 4191: Default Router Preferences and More-Specific Routes

[36] RFC 4601: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)

[37] RFC 2362: Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification

[38] RFC 4607: Source-Specific Multicast for IP

[39] RFC 2710: Multicast Listener Discovery (MLD) for IPv6

[40] RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6

[41] RFC 4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast

[42] RFC 4605: Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")

[43] RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

[44] TR-069 http://www.broadband-forum.org/technical/download/TR-069Amendment2.pdf

[45] UPnP http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf

[46] RFC 4291: IP Version 6 Addressing Architecture

[47] RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP

[48] RFC 4862: IPv6 Stateless Address Autoconfiguration

[49] RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers

FC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

FC 3898: Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

[52] RFC 4075: Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6

[53] RFC 4795: Link-Local Multicast Name Resolution (LLMNR)