IPv6 Home Router Guideline (Translated Version)

[Ver.2.0]

7 - 29 - 2010

(Translated: 12 - 1 - 2012)

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

Table of contents

1 Introduction

This section is not translated to English.

2 Connection Model for IPv6 Internet Service

This section is not translated to English.

3 Address Assignment Function

This chapter describes methods for assigning addresses to a terminal to be connected to the WAN side, LAN side, and LAN side segments of a router.

3.1 Prefix Assignment

This section describes requirements for a router when a service provider assigns a prefix to a user.

3.1.1 Prefix Information Distributed to a Home Network

Requirement 1 : A router can get prefix information for home network from the connected service provider using DHCPv6-PD.

Necessity : Mandatory（MUST）

Reason : DHCPv6-PD is the standard protocol for automatic prefix assignment. It eliminates wrong configuration due to manual inputting by a user.

Requirement 2 : Prefix information for home network can be manually configured.

Necessity : Mandatory（MUST）

Reason : The connected service provider may not support prefix distribution using DHCPv6-PD.

3.1.2 Size of a Prefix Assigned to a Home Network

Requirement 3 : A router can receive the prefix assigned by a service provider in the range of /48 - /64.

Necessity : Mandatory（MUST）

Reason : It is required that a prefix in the range of /48 - /64 is assigned to an end site by “IPv6 Address Allocation and Assignment Policy at JPNIC”[8].

Remarks : As it is conceivable that segments are separated between wireless and wired or deployment of DMZ, distribution of multiple segments (prefix length shorter than /64) is desirable. The assigned prefix size, however, is to be decided by a service provider.

Though the prefix length may be shorter than /48 in enterprise network, enterprise network is out of the scope in this section.

3.2 WAN Side Address

This section describes address assignment to the WAN side of a Home Router (link

with service provider) in a service model described in Section 1.4.3.1.

3.2.1 Global Address Assignment Method (Automatic)

Requirement 4 : A global address can be assigned automatically to the WAN side interface.

Necessity : Mandatory（MUST）

Reason : This is mandatory for realizing automatic setting without user intervention.
Both of the following methods are mandatory.
[a] SLAAC（Stateless Address Auto configuration）
[b] DHCPv6

Remarks : It depends on a service provider which method — SLAAC or DHCPv6 — is used in assigning an IP address. To support both services, a router has to implement both functions.
It is also considered possible to have it automatically determined whether SLAAC or DHCPv6 is used without letting a user configure this [59].
If SLAAC is used, a service provider cannot know the assigned address unless it is used in combination with a mechanism for informing the provider of the assigned address (DDNS etc.).
The following elements also need to be taken into account in selecting the function.

- Technical trends: as of July 2010, with DHCPv6, prefix length distribution needs to be used in combination with a router advertisement/prefix option etc.
- The fact that, for an IPv6 global unicast address, the interface identifier is specified as 64-bit length [46].
- The requirements concerning address prefix size to be assigned to WAN side and problems that can arise in this regard (Section 7.1).

3.2.2 Global Address Assignment Method (Manual)

Requirement 5 : A global address can be assigned manually to the WAN side interface.

Necessity : Mandatory（MUST）

Reason : Although automatic configuration is presumed, manual configuration is also necessary.

3.2.3 Response to the Absence of Global Address Assignment

Requirement 6 : A router can communicate using an address in assigned prefix range to LAN side network if no address is assigned to WAN side interface.

Necessity : Mandatory (MUST)

Reason : This is mandatory as a router is required to send and receive packets under a service model in which a global address is not assigned to the WAN side.

Remarks : This function is necessary when a router acts as a DNS proxy, etc.

Using a LAN side address or assigning an address to a virtual interface is conceivable, but this document does not specify how to generate an address to be used.

3.3 LAN Side Address

This section describes address assignment to the LAN side of a Home Router (link with user's home network).

3.3.1 Prefix Re-distribution

Requirement 7 : On the basis of a prefix received using DHCPv6-PD from a service provider, a router can generate a /64 prefix and re-distribute it to the LAN side.

Necessity : Mandatory (MUST)

Reason : This is mandatory as a means for automatically redistributing a prefix distributed to user's home network by a service provider to user's home equipment.

Remarks : With regard to the protocol for redistribution, see Section 6.1.

The method is not specified for deriving a /64 prefix from a prefix larger than /64 received using DHCPv6-PD. For example, if a /48 prefix has been received using DHCPv6-PD, it is necessary to determine the values in the range of 49 to 64 bits when redistributing it to the LAN side. The method for determining those values is not specified in this document.

3.3.2 Multiple Prefix Reception

A router can select which prefix is to be redistributed to the LAN side if multiple prefixes have been received using DHCPv6-PD from one or more service providers.

Necessity : Optional (MAY)

Reason : This requirement is intended to support environments where multiple upstream service providers exist or where the service provider distribute

different multiple prefixes. Because an environment with a number of upstream service providers is considered to be exceptional for a Home Router, this should be treated as optional.

Remarks : A connection service is conceivable which distributes one fixed prefix and one unfixed prefix.

Since fixed and unfixed prefixes each have its own advantages, it is preferable for a user to be able to select either.

An attention should be paid to a conceivable case in which the choice of one type of prefix precludes an access to a specific network.

If multiple prefixes are assigned by multiple service providers, a problem can arise with terminal's behavior [17].

3.3.3 Change in Distributed Prefix

Requirement 8 : If the prefix distributed using DHCPv6-PD by the service provider changes due to WAN side reconnection or other reasons, a router can properly change the prefix to be distributed to the LAN side.

Necessity : Mandatory（MUST）

Reason : It is necessary to minimize such impacts on communication in a user's network as resulting from the use of a service which varies a prefix assigned to a user with time.

Remarks : This document does not specify a method for changing an assigned prefix. See Section 6.1.2 for renumbering terminals in a home network upon a change in the distributed prefix.

3.3.4 Generation and Distribution of a ULA Prefix

Requirement 9 : A router can generate a ULA prefix and distribute it to the LAN side if prefix information is not assigned by the service provider.

Necessity : Recommended (SHOULD)

Reason : This is to guarantee communication in the home network when a global address is not assigned in IPv6-only environment. It is classified as Recommended (Not Mandatory), since home networks are usually expected to be dual stack.

Remarks : Specifications of ULA should be based on RFC4193.

In the reference [59], the use of ULA is Mandatory (MUST).

Renumbering is required if prefix information is assigned by the service provider after the distribution of a ULA prefix.

4 Security Function

This chapter describes security functions that are considered to be minimally necessary for the protection of a user's home network. Functions dealt with here are minimally necessary elements for realizing integrity (prevention and detection of data tampering, recovery of tampered data, etc.), confidentiality (encryption, etc.), and availability (convenience in configuration, etc.). While enhancing users' awareness of security, it is necessary to take a flexible approach by combining these elements [60][61].

4.1 Access Control Function

4.1.1 Restriction of Access from Outside

As a prerequisite, security functions employed for IPv4 (including direct non-reachability from an outside network to a home network owing to NAT/NAPT) are also necessary for an IPv6 Home Router.

4.1.1.1 Basic Setting for Access Restriction

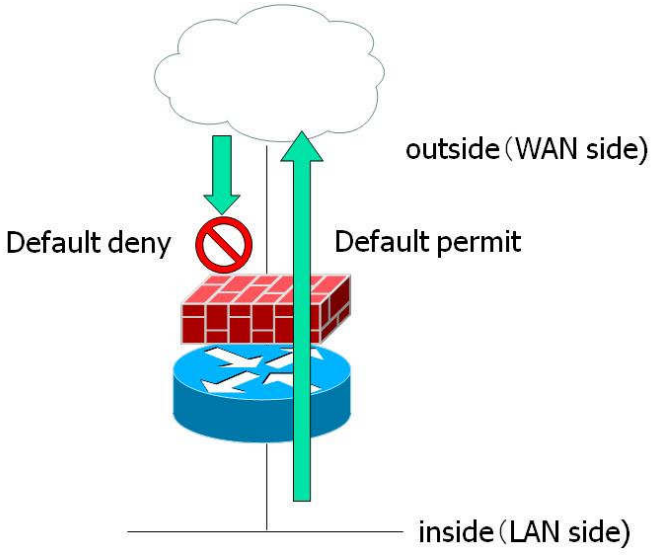

Figure 4-1 Function of Access Control from Outside

Requirement 10 : A router can perform access restriction that allows communication from inside (LAN side) to outside (WAN side) and blocks communication from outside to inside.

Necessity : Mandatory (MUST)

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

Remarks : Although the default behavior blocks communication from outside to inside, it is also necessary to enable a setting that allows such communication (see also Section 4.1.2.).

4.1.1.2 Access Restriction by Static Filter

Requirement 11 : A router can restrict access by static filter.

- Traffic is passed through by default from inside to outside.
- With TCP, SYN from outside to inside is dropped by default.
- With UDP, communication from outside to inside is blocked by default.
  Note: The mandatory protocols for services, such as DNS, telephony, TV, etc. need to be allowed.
- With ICMPv6, only mandatory messages [9] from outside to inside are passed through, while others are blocked by default.

Necessity : Mandatory（MUST）

Reason : To maintain the minimally necessary level of network security achieved in current IPv4 networks by NAT restriction in IPv6 network.

Remarks : Whether an IPv6 address on a WAN side interface should be configured or not should be determined in light of its necessity in service provision and security.

In implementing access control, it is necessary to take reassembling of fragmented packets into account. (See Section 4.1.3 also.)

Even a traffic from inside is recommended to be blocked if its source address is any of the following.

- Global address other than one assigned by the service provider
- Link-local address（fe80::/10）
- Site-local address（fec0::/10, deprecated in RFC3879）
- ULA（fc00::/7）
- Multicast address（ff00::/8）
- Well-known anycast address

  Subnet-router anycast address, etc.
- IANA reserved address（::/8）

  loopback address, unspecified address, IPv4-compatible address, IPv4-mapped address, etc.
- Documentation address（2001:db8::/32）

4.1.1.3 Access Restriction by Dynamic Filter (Stateful Packet Inspection: SPI)

Requirement 12 : A router can restrict access by a dynamic filter (SPI).

- Traffic is passed through by default from inside to outside.
- Connections from inside to outside are recorded, and returned traffic of this connection from outside to inside is passed.

Necessity : Recommended（SHOULD）

Reason : This is intended to maintain a security level equivalent to the current IPv4 NAT in IPv6 as well. It is, however, classified as recommended as a static filer can ensure the minimally necessary level of security.

It is classified as Recommended also because it is an important function for maintaining the security level in IPv6.

As regards SPI, see the descriptions in RFC 4787 also [47].

Such implementation of SPI state control is classified as Recommended that

takes into account control using a timer.

4.1.2 Functions Configurable for Access Control and their Level of Necessity

Requirement 13 : A router can configure access control functions indicated in Table 4-1.

Necessity : Mandatory (MUST)

Table 4-1 Functions Configurable for Access Control and their Level of Necessity

Function	Necessity
A router can control access by IPv6 source/destination address.	Mandatory (MUST)
A router can recognize the next header (protocol). (See Section 7.2.3)	Mandatory (MUST)
A router can control access by protocol type. (Extended header type etc.)	Recommended (SHOULD)
A router can trace the next header chain.	Mandatory (MUST)
A router can control access by ICMP Type and Code [9].	Recommended (SHOULD)
A router can control 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 : This document does not specify the degree of depth to which the next header chain needs to be traced.

In realizing a communication using a tunnel, it is required to consider the implementation of access control corresponding to addresses inside a tunnel such as DPI (Deep Packet Inspection).

4.1.3 Access Control of Fragmented Packets

Requirement 14 : A router can reassemble fragmented packets and control their access based on the settings for control of access from outside.

Necessity : Optional (MAY)

Reason : This is required because access control needs to be performed for fragmented packets. Since, however, reassembling and maintaining fragmented packets consume equipment resources, this is classified as Optional.

Remarks : A UDP packet is often used for DNS communication, and the size of UDP packet is expected to increase due to an increase in the size of DNS response packet caused by the spread of DNSSEC and other reasons. If the size of a packet exceeds the path MTU size, the original packet is fragmented and sent as fragmented packets. In this case, unfragmentable parts of the original packet are included in every fragmented packet, but fragmentable parts exist only in the fragmented packet into which they are divided. Therefore, under the condition that this function is not implemented, if the upper layer protocol header, etc. exist only in fragmentable parts, access control is possible only for a leading packet of a fragment and impossible for other fragmented packets.

4.1.4 Access Restriction to the Device itself

Requirement 15 : Access control is possible with communications to the device itself. Access control is likewise possible with functions controlling the device itself.

Necessity : Mandatory (MUST)

Reason : Because it is necessary to ensure security for service functions provided by the device itself as an IPv6 host.

4.2 Other security functions

Requirement 16 : A router is equipped with such security functions as warning against configuration changes.

- It has a safe initial configuration for protecting itself from internal and external security risks and gives warning if such a change in configuration is made as is vulnerable.
- It is equipped with anti-virus and anti-tampering functions.
- It has functions for logging, notifying, disaster recovery, etc.
- It has safe initial configuration for communication transiting it.
- It can warn against and notify a change entailing security risk.
- It can be configured for address conversion, etc.
- If wireless LAN is to be used, a router is required to have a strong encryption function.

Necessity : Optional（MAY）

Reason : This requirement is intended to inform a user unfamiliar with security of safety and risk of a given configuration as well as to support such a user. This is classified as Optional, however, since functions given here are wide ranging, which makes it difficult to define the minimum functions required.

5 DNS Proxy/Resolver Function

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

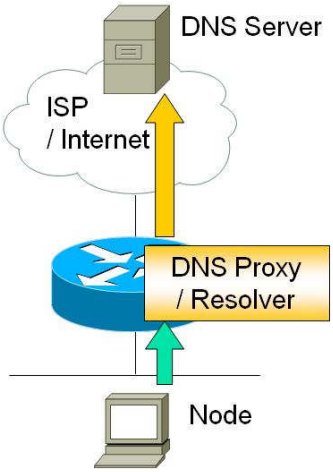

Figure 5-1 Conceptual Diagram for DNS Proxy/Resolver Function

Although opinions are divided as to the necessity of DNS Proxy/Resolver function for a home router, cache can mitigate the load of DNS server if it is implemented in home router.

In addition, if it is not implemented, there is a possibility that problems such as a delay or communication failure arise due to incorrect selection of DNS server at the terminal side. Furthermore, the direct input of IP address, instead of FQDN, will then be necessary for access to a router's Web-GUI. Since the direct input of IPv6 address is difficult, this will degrade users' convenience.

http://setup.example.jp/ → http://[2001:db8:1234:5678::1]/

This guideline summarizes requirements for implementing DNS Proxy/Resolver functions under the following preconditions.

- Queries from a terminal and responses from DNS server are handled as transparently as possible without changing a flag or data.
- Cases involving a conversion process such as translator or ALG (application-level gateway) are not discussed in this document since the function in question will then be included in the functions of translator or ALG. Since there is a risk that a terminal receives an unintended response if such a conversion process is involved, an individual case needs to be examined.
- DNS Resolver functions are described to be considered regardless of IPv4 or

IPv6.

5.1 Transport

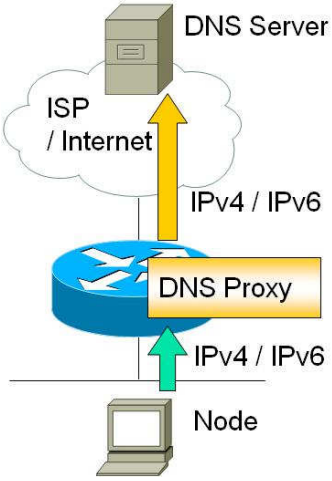

Figure 5-2 Selection of Transport Used

5.1.1 Transport protocol

Requirement 17 : Both IPv6 transport and IPv4 transport are supported as transport over which a query to a DNS server is made.

Necessity : Mandatory（MUST）

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

5.1.2 Transport Conversion Function

Requirement 18 : A router can convert a query from the terminal in whatever transport to a one in transport required by the service provider.

Necessity : Mandatory（MUST）

Reason : Because capability for DNS communication is required even in the transition period to IPv6.

5.1.3 Prioritized Transport

Requirement 19 : If a query from the terminal is made over the same transport as the one used by the DNS server designated by the service provider, a proxy action is performed over the same transport as the one over which a query from the terminal is made.

Necessity : Optional（MAY）

Reason : If the transport is not changed, it is more likely that the requesting terminal obtains the expected result [15]. This requirement is Optional, since

there is no guarantee that the DNS server beyond the home router (DNS proxy) uses the same transport.

Remarks : If the DNS server supports only IPv4 transport even though a query from the terminal to the DNS Proxy is made over IPv6 transport, the DNS Proxy needs a transport conversion function. Unless the terminal chooses transport intentionally, it is meaningless for the DNS Proxy to use the same transport.

When a proxy action is performed over the same transport, the DNS Proxy needs a function to record the transport over which the terminal has made a query.

As some DNS servers in the IPv4 Internet are configured to give different responses based on the source address, using the same transport does not necessarily result in the same response. Using the same transport, however, makes it more likely that a more appropriate response is obtained. In addition, the terminal may make a transport specific query. Using the same transport is thus more likely to result in a more appropriate response.

The necessity for this requirement will be reexamined when a need arises in the future to use the same transport.

5.2 Type of Address on which DNS Proxy Listens

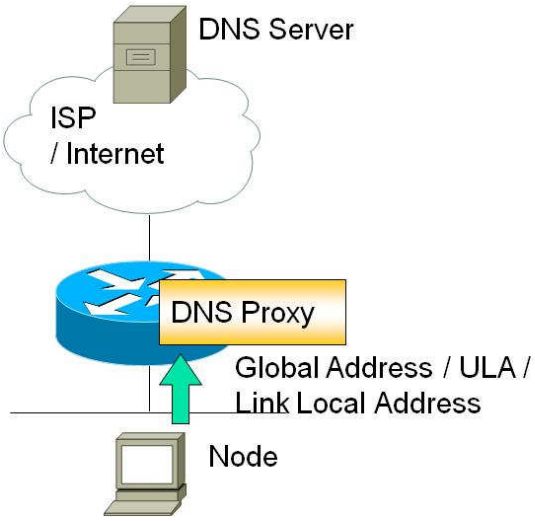

Figure 5-3 Type of Address Listened On

5.2.1 Type of Address on which DNS Proxy Listens

Requirement 20 : A router can listen on a unicast address (any of global address, ULA, or link-local address).

Necessity : Mandatory (MUST)

Reason : Because it is necessary to be able to listen on a unicast address at least.

Remarks : ULAs need to be defined in advance for the DNS Proxy if it listens on ULAs. It should be noted that, if a ULA has been already used on the LAN, a mechanism is required to generate a different ULA that does not conflict with it.

When the DNS Proxy listen on a global address in case upstream connection is dropped or where setup is incomplete, it is conceivable that there is no global address assigned to the DNS Proxy. Such a case should be paid attention to, because a query packet does not reach the DNS Proxy. Some additional considerations are also required including not to accept queries from the WAN side in order not to become a DNS Open Resolver which is used in a DNS amplification attack.

When the DNS Proxy listens on a link local address, queries from other segments do not reach the DNS Proxy. Attention also needs to be paid for a possibility that some hosts don't accept link-local address as a DNS server's address.

5.3 DNS Server selection

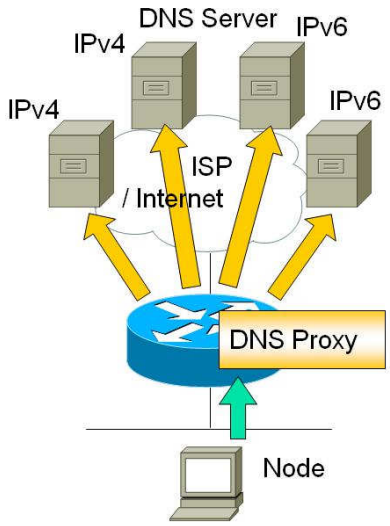

Figure 5-4 DNS Server Selection

5.3.1 Sequential Selection

Requirement 21 : A router can handle a list of DNS servers and select one sequentially.

Necessity : Mandatory (MUST)

Reason : To increase reachability to the destination.

5.3.2 Policy based Selection

Requirement 22 : A router can handle a policy based on a domain name, and select a DNS server according to a domain name specified by a user's query.

Necessity : Optional (MAY)

Reason : With this function, service providers such as access providers can provide policy based on domain name. It is classified as Optional, however, since this function largely depends on service provided by service providers.

Remarks : Although both sequential selection mechanism and domain name based selection mechanism can be a solution for the DNS server selection issue for each service network in a multi-prefix environment, both mechanisms should be based on the consideration of their advantages and disadvantages since neither of them provides an almighty solution [17].

There is no standard that prioritizes DNS query transports (IPv6 or IPv4). Some argue that IPv4 should be used because there is concern about the

stability of current IPv6 DNS servers, while others argue that IPv6 should be used considering migration to IPv6 in the near future. Currently this issue is under discussion. At this moment, resolvers of many operating systems favor IPv6 transport. It is assumed that the same result should be returned from the DNS server regardless of transport. [16]

5.4 Cache

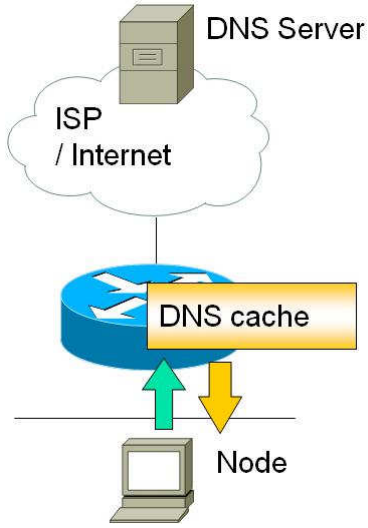

Figure 5-5 DNS Cache Function

5.4.1 Cache Function

Requirement 23 : The responses returned to a query from the terminal should be cached, and the cached information should be returned upon subsequent and similar queries.

Necessity : Optional（MAY）

Reason : This is required because it enables the load mitigation (suppression of query/response packets) of the service provider's DNS server. It is Optional, however, as there are many things to be considered in its implementation.

Remarks : As a prompt action is required if a DNS-related vulnerability such as a Kaminsky Attack [18] is found, the implementation of this function needs to be based on the consideration of its advantages and disadvantages.

It should be noted that caching large records such as RRSIG is required to support DNSSEC.

5.5 Resolver Function

Although the following functions required of a DNS resolver are not IPv6-specific, they are more relevant to IPv6 than to IPv4. They are hence recommended to be considered as a part of the specifications to be implemented in a Home Router.

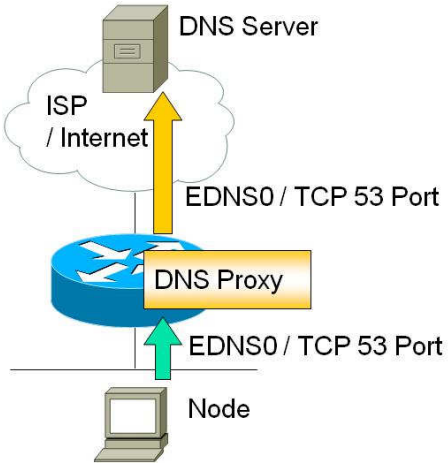

Figure 5-6 DNS Resolver Function

5.5.1 Supported Resource Records

Requirement 24 : Queries from a host should all be processed transparently regardless of resource record (RR) type.

Necessity : Mandatory (MUST)

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

Remarks : A reverse query for a ULA must not be made, however (except when a ULA is used within a service provider).

5.5.2 Unexpected Flag and Data

Requirement 25 : Received flags and data that cannot be interpreted must not be changed or deleted.

Necessity : Mandatory (MUST)

Reason : To maintain transparency between a terminal and the DNS server.

5.5.3 EDNS0

Requirement 26 : A router can process EDNS0-compliant [19] query packets

(including OPT RRs) transparently and send a response exceeding 512 bytes to a terminal. In addition, a router must forward fragmented response packets without modification or after reassembling them.

Necessity : Mandatory（MUST）

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

5.5.4 Support of TCP Port 53

Requirement 27 : A query can be processed transparently even if the terminal (after receiving DNS Header TC=1 [20], [21]) falls back to TCP connection. (A router must listen not only on UDP Port 53 but also TCP Port 53.)

Necessity : Mandatory（MUST）

Reason : In order not to influence the query-related behaviors of a terminal.

5.5.5 DNSSEC

Requirement 28 : A router can process packets supporting DNSSEC transparently [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 : Mandatory（MUST）

Reason : In order not to influence the query-related behaviors of a terminal.

Requirement 29 : DNSSEC-compliant recursive processing (validator) including signature verification is implemented as a DNS Proxy/Resolver function [22][23][24].

Necessity : Optional（MAY）

Reason : This requirement is intended to process queries from a terminal appropriately. It is classified as Optional, however, since realization is possible as a single function Proxy with an IP address conversion function only.

Remarks: This needs to be considered as Windows 7 supports DNSSEC although it is currently not implemented in Windows XP or Windows Vista.

It depends on implementation whether to implement recursive processing (validator) including signature verification as a Home Router's DNS Proxy/Resolver function or to operate as a single function Proxy with an IP address conversion function only.

6 Information Distribution Function to Home Networks

This chapter describes the distribution function of address/prefix information and server information from the Home Router to hosts.

6.1 Distributing Address/Prefix Information

6.1.1 Distribution Using RAs

Requirement 60： A router has a function to inform a host of the prefix to be assigned to it through router advertisement (RA).

Necessity：Mandatory（MUST）

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

Remarks：See Section 3.3.2 about the policy for prefix information distribution within LAN upon obtaining multiple prefixes from service providers.

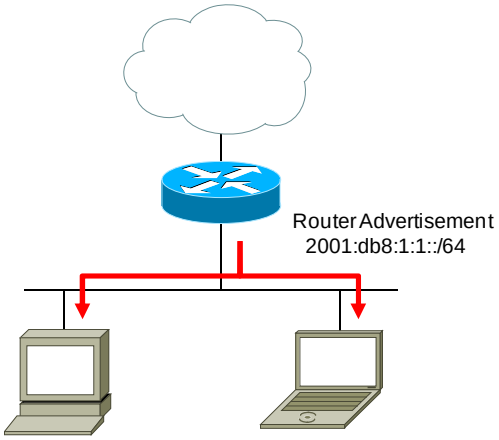

Figure 6-1 Distribution of Prefix Information Using RA

Requirement 61： The length of a prefix notified by RA should be /64 by default.

Necessity：Mandatory（MUST）

Reason：Many implementations use the last 64 bits of an address as the interface ID in stateless address auto configuration.

Remarks：It should be noted that, when a prefix whose length other than /64 is distributed, the address for a device in a LAN sometimes may not be set correctly. For example, in Windows Vista SP1, an address cannot be generated from a prefix other than /64 .

According to SLAAC (RFC 4862) specifications, if the sum of the prefix length in the Prefix Information Option of RA and the length of an interface ID that a

terminal itself has does not equal 128 bits, the Prefix Information Option MUST be ignored [29][48]

Requirement 62 : A router has a function to send an RA such that Preferred Lifetime in its Prefix Information option is set to 0.

Necessity : Recommended (SHOULD)

Reason : This is a function required to minimizing the impact on communication by a terminal in such cases as switching the service provider. The requirement should be classified as Recommended, however, since this function needs to be implemented by taking into account occasions on which it is performed.

Remarks : If an address A whose Preferred Lifetime is 0 and an address B whose Preferred Lifetime is not 0 are assigned to a terminal, the address B is preferred as a source address for a communication initiated by the terminal [15].

One conceivable occasion on which this function is performed is, for instance, when a change in a prefix assigned by the service provider is detected due to service provider switching or other reasons. In this case, if a RA is sent which has a preferred lifetime field set to 0 for the old prefix, a terminal which receives the RA ceases to use an address which has the old prefix in subsequent communications, enabling a smooth change in (renumbering of) the address of a home terminal. If an RA which has a preferred lifetime field set to 0 for the old prefix is not sent, it is possible that an address generated from the old prefix is used as a source address for communication initiated until the preferred lifetime for the old prefix is changed to 0 at the terminal, which may conceivably cause a problem in communication.

Another occasion conceivable is when a disconnection is detected in the WAN side link. (Since reachability is then lost to a global prefix assigned to a home network, that prefix becomes invalid.) In this case, however, it is possible that home network communication beyond a router, in particular, is disabled at the point of time when a global address inside the home network becomes invalid (when valid lifetime becomes 0). Consequently, such measures are required to be taken as ensuring communication in a home network by advertising a ULA prefix. (See Section 3.3.4.)

Requirement 63 : A router has a function to send an RA with Router Lifetime set to 0.

Necessity : Recommended（SHOULD）

Reason : This is effective when a terminal is not preferred to select itself as the default route. This requirement is classified as Recommended, however, since this function needs to be implemented by taking into account occasions on which it is performed.

Remarks : A terminal receiving an RA with Router Lifetime set to 0 does not select the router sending the RA as the default route.

One conceivable occasion on which this function is performed is, for instance, when a disconnection is detected in the WAN side link. In this instance, if an RA with Router Lifetime set to 0 is sent, the terminal receiving it ceases to select the router sending the RA as the default route. The terminal, consequently, will no longer send such packets to the router that are bound for any destination other than the LAN segment it belongs to (Internet-bound packets).

Attention should be paid to a case where multiple LAN segments are connected to a router. Since, in this case, sending only an RA with Router Lifetime set to 0 disables communication from one LAN segment to another LAN segment, such countermeasures as route distribution through more-specific routes [35] are required.

6.1.2 Distribution using DHCPv6

Requirement 64 : A router has a function to inform hosts of an address by DHCPv6.[27]

Necessity : Optional（MAY）

Reason : It is effective when assigning a specific address to a home network terminal. This requirement is Optional, however, as SLAAC is generally used for address configuration on the terminal side.

Remarks : If this function is enabled, advertise an RA with M flag set to 1 to a LAN segment.

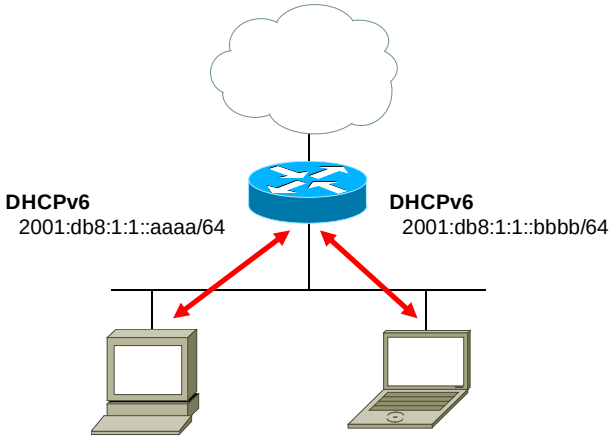

Figure 6-2 Distribution of Address Information by DHCPv6

Requirement 65： A router has a function to send a Reconfigure message with the msg-type of its Reconfigure Message Option set to 5 (Renew message).

Prerequisite：Requirement 35 has been implemented.

Necessity：Recommended（SHOULD）

Reason：This is effective for prompting a terminal to reacquire an address quickly via DHCPv6 when its address is changed. This requirement is classified as Recommended, however, since this function needs to be implemented by taking into account occasions on which it is performed.

Remarks：One conceivable occasion which this function is performed is, when a change in the prefix assigned by the service provider is detected due to service provider switching or other reasons.

Requirement 66： A router has a function for distributing a prefix to another router in a home via DHCPv6-PD[30] and a function that can specify, for the router in a home, the prefix to be distributed.

Necessity：Optional（MAY）

Reason：This is effective for distributing the prefix to be assigned to the terminal connected to the relevant router when multiple routers exist in a home network. This requirement is classified as Optional since there are conceivably not so many users who install multiple routers in their home network.

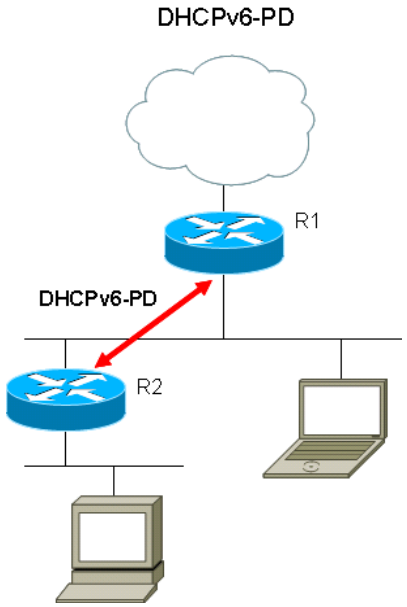

Figure 6-3 Distribution of Prefix Information by DHCPv6-PD

6.2 Distributing Server Information

6.2.1 Distribution using RA

Requirement 67： A router has a function for distributing a DNS server address to a LAN segment RA.

Necessity：Optional（MAY）

Reason：Implementation is expected at a terminal [31] for obtaining a DNS server information from RA (as DNS information distribution through RA is going through standards track [31]). This requirement is classified as Optional, however, since this function is currently not standardly implemented in Windows XP/Vista/7 or MacOS.

Remarks：If the DNS server address is changed due to service provider switching or other reasons, it is preferable to advertise an RA message with RDNSS option's Lifetime field set to 0 for the old DNS server address in order to have the old DNS server address deleted from the DNS server list that a terminal has.

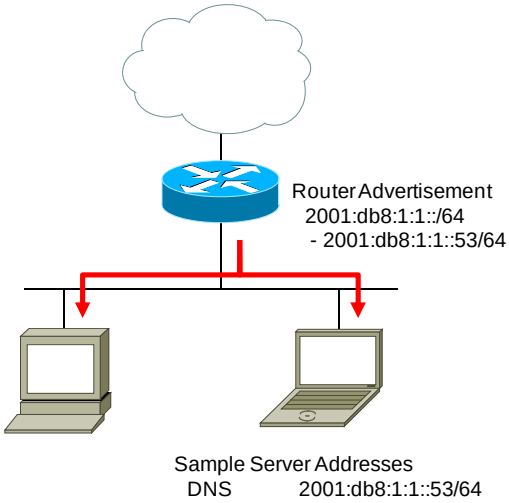

Figure 6-4 Distribution of Server Information by RA

6.2.2 Distribution using DHCPv6

Requirement 68： A router has a function for distributing DNS server address to a LAN segment DHCPv6 .

Necessity：Mandatory（MUST）

Reason：DHCPv6 is commonly used as the method to obtain DNS server information in implementation at the host side.

Remarks : If this function is rendered effective, advertise an RA message with O flag set to 1 to a LAN segment.

In terms of standardization, whereas DHCPv6 (RFC 3646) is in the category of Standards Track, RA (RFC 5006) is in the category of Experimental [32]. IETF, however, is presently considering the promotion of RFC5006 to the category of Standards Track.

Requirement 69 : A router has a function for distributing other server addresses (SIP, NTP etc.) to a LAN segment DHCPv6.

Necessity : Optional (MAY)

Reason : This requirement is intended to avoid configuration errors due to manual inputting by a user. It is classified as Optional, however, as it largely depends on the service by a service provider whether any of other servers is used.

Remarks : If this function is rendered effective, advertise an RA message with O flag set to 1 to a LAN segment.

It depends on service specifications of a service provider which server address to distribute.

Server addresses distributable by DHCPv6:

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

List of DHCPv6 parameters:

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

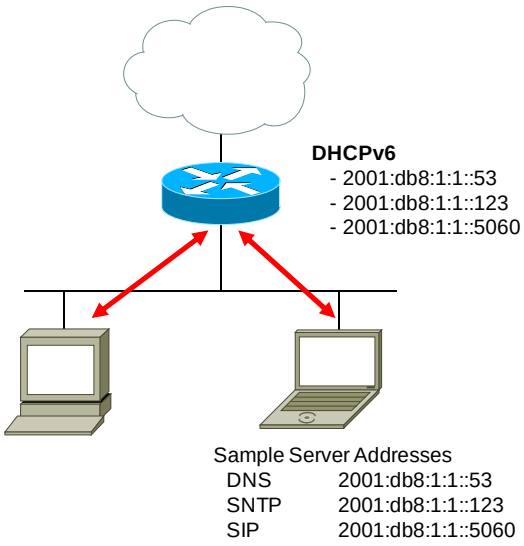

Figure 6-5 Distribution of Server Information by DHCPv6

Requirement 70 : A router has a function to send a Reconfigure message with the msg-type of its Reconfigure Message option set to 11 (Information-request message).

Prerequisite : Requirement 40 has been implemented.

Necessity : Recommended (SHOULD)

Reason : This requirement is intended to prompt a terminal to reacquire server information quickly via DHCPv6 when the server address distributed is changed due to service provider switching and other reasons. This requirement is classified as Recommended, however, since a change in server information depends on service by a service provider.

6.3 Distribution of Other Information

6.3.1 Distribution of MTU Information

Requirement 71 : A router has a function advertise the MTU value of the access line to a LAN segment RA. The MTU value of the access line to be advertised should be configurable.

Necessity : Recommended (SHOULD)

Reason : This is effective for changing the MTU values of all nodes in a home network. This requirement is classified as Recommended, however, since setting the MTU to a small value can degrade the performance of intra-LAN communication.

Remarks : Due to filtering of the "ICMPv6 Packet Too Big" message and other reasons, a terminal may fail to find the optimal MTU in path MTU discovery, resulting in loss of communication(See Section 7.4.). In such a case, making the MTU of the terminal interface smaller recovers communication.

Although there is a method for manually changing the MTU of the terminal interface, configuring it takes time if multiple hosts are connected to the LAN. If a router advertises link MTU to a LAN segment, this MTU is reflected on all terminals connected to the LAN, saving time and efforts for configuring the MTU at each terminal.

7 Routing/Multicast Function

This chapter describes the minimum requirements of routing and multicast function for the Home Router to be connected to IPv6 service.

7.1 Communications to Unused Address/Network

Requirement 43 : A router has a function not to forward traffic destined for the assigned prefix to upstream.

Necessity : Mandatory（MUST）

Reason : To prevent packets ping-pong between the Homer Router and service provider's router until Hop Limit becomes 0.

Remarks : Packets destined to an unused address space need to be dropped without being forwarded to the default route.

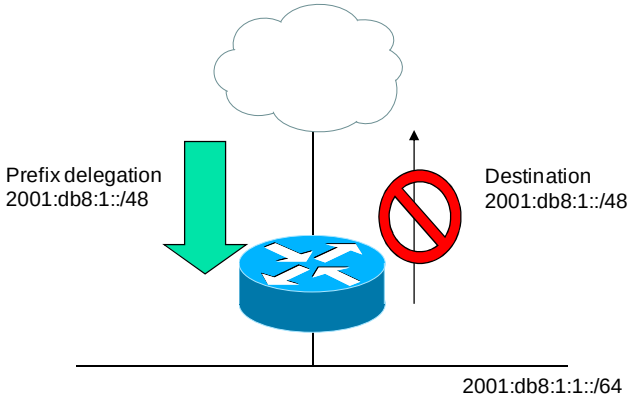

Figure 7-1 Service that assigns an address prefix by DHCPv6-PD

Requirement 44 : On a Point-to-Point link, When the router receives packets destined for an address other than its own interface address prefix, it must send the ICMPv6 Destination Unreachable message with Code 3 (Address unreachable), and not forward the packets [33].

Necessity : Mandatory（MUST）

Reason : To prevent packets ping-pong between the Home Router and service provider's router until Hop Limit becomes 0.

Remarks : This feature was undefined in RFC2463 but was defined in RFC4443.

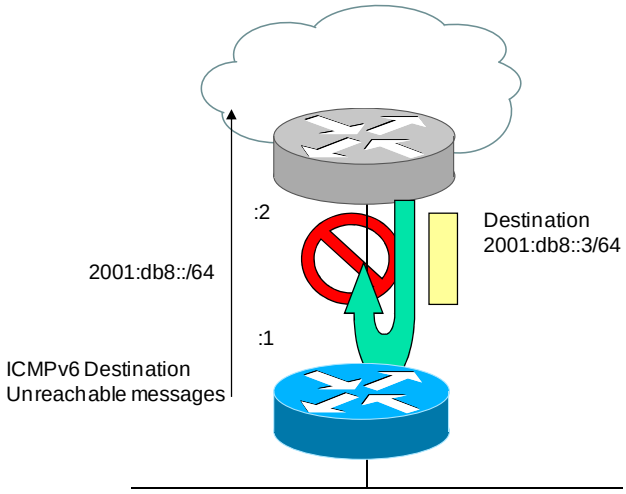

Figure 7-2 Service Providing a Point-to-Point Link as the WAN uplink

7.2 Routing Information and Extension Header

7.2.1 WAN Side Routing

Requirement 45 : A router has a function to configure static routes for the WAN side.

Necessity : Mandatory（MUST）

Reason : The router is minimally required to have a function for explicitly configuring routing information, such as default route.

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.

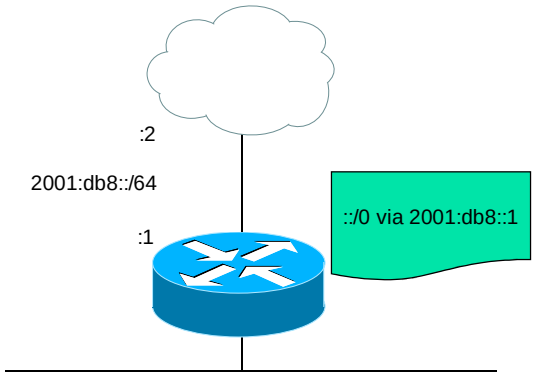

Figure 7-3 Static Route Setting for the WAN side

Requirement 46 : A router supports default route auto configuration by RA. .

Necessity : Mandatory（MUST）

Reason : Consideration is necessary for a service which configures IPv6 address by RA.

Remarks : Although a router in general does not support default route auto configuration by RA, it is important for a Home Router to perform configuration for a service provider without user's manual intervention [48]. Also, when multiple WAN interfaces exist and multiple RA's are received, it is necessary to decide which default route should be preferred. This should be treated as an item for further study. (See Section 10.2)

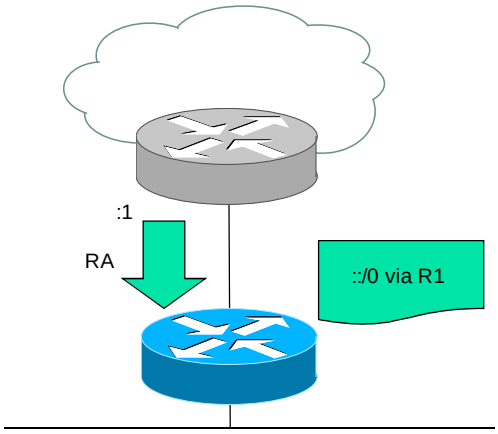

Figure 7-4 The Default Route Auto configuration Using RA

7.2.2 LAN Side Routing

Requirement 47 : A router supports route distribution to the LAN side by RIPng [34].

Necessity : Optional（MAY）

Reason : This function is expected to be used for controlling the route to the network connected to a router's LAN side. This requirement is classified as Optional, however, since there are conceivably not so many users who install multiple routers in their home network.

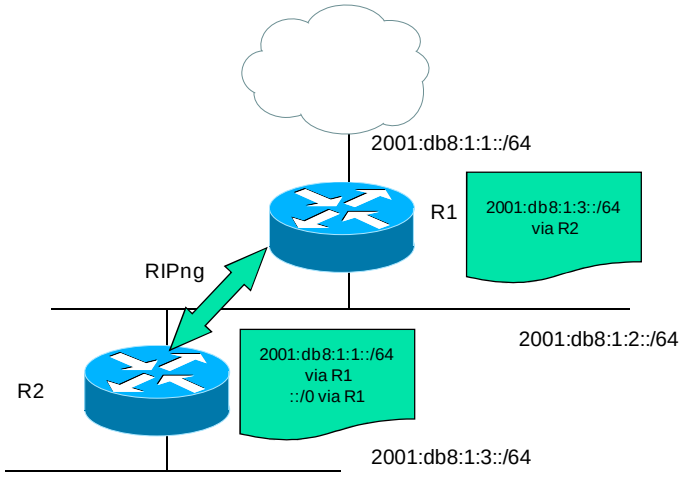

Figure 7-5 Route Control by RIPng

Requirement 48 : A router supports route distribution to the LAN side by more specific routes [35].

Necessity : Optional（MAY）

Reason : This function is expected to be used for controlling routes for the network connected to a router's LAN side. This requirement is classified as Optional, however, since it depends on the service by a service provider.

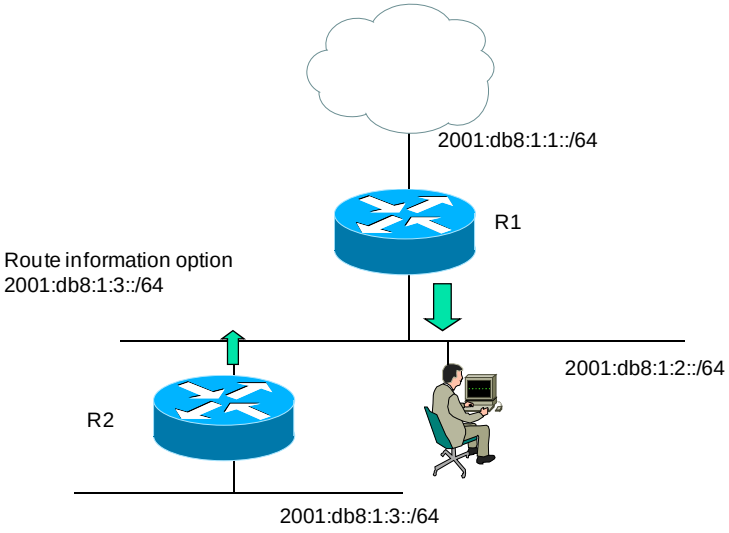

Figure 7-6 Use of More-Specific Routes

7.2.3 Extension Header

Requirement 49 : A router has a function to prohibit RH0 (Type 0 routing headers) packet forwarding.

Necessity : Mandatory (MUST)

Reason : Because its use is prohibited in the current specification, given the need to take account of a DoS attack by IPv6 source routing [11].

Remarks : Rather than implementation that prohibits any routing header, implementation is necessary that can recognize the type correctly and prohibit only Type 0.

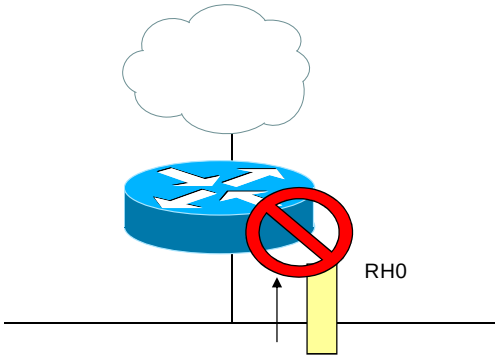

Figure 7-7 RH0 Packet Forwarding Prohibited

7.3 IPv6 Multicast

In IPv6, many multicast messages are used in control packet such as NDP. Multicast support is a mandatory function for IPv6 equipment. The description of multicast in this chapter discusses a multicast routing function.

Requirement 50 : A router supports multicast routing

Necessity : Optional (MAY)

Reason : To support a service using multicast. This function is classified as Optional since it largely depends on the service by a service provider.

7.3.1 IPv6 multicast function

Two patterns of connection to an IPv6 multicast service are conceivable depending on the protocol used upstream from a Home Router (toward the WAN side). The functions required for each connection configuration are shown below.

7.3.2 Connection by PIM

Joining/Leaving a multicast group is notified to a service provider using PIM.

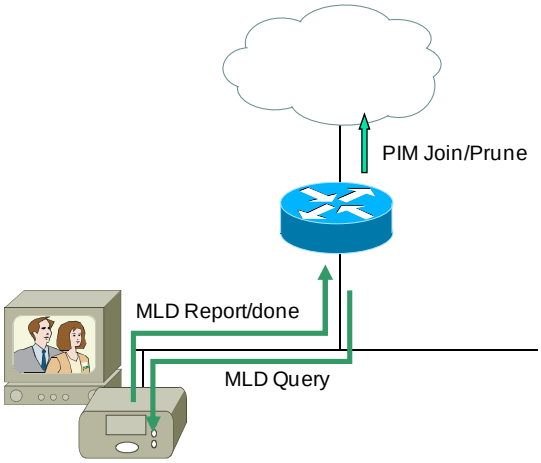

Figure 7-8 Multicast Connection Using PIM

Requirement 51 : A router has a multicast routing function by PIM [36][37][38].

Prerequisite : Requirement 50 has been implemented.

Necessity : Optional（MAY）

Reason : To support services using PIM as a WAN side protocol. This requirement is classified as Optional, however, since it largely depends on the service by a service provider.

Remarks : Many optional functions exist in the specification of PIM-SM/SSM, and optional functions required to ensure connectivity largely depend on the service specification of a service provider. Furthermore, under a simple tree structure that needs to be supported by a Home Router, implementation by MLD Proxy costs less and is considered to be easier to be introduced than a complex PIM protocol.

Requirement 52 : A router has an MLD (v1/v2) router function[39][40][41].

Prerequisite : Requirement 50 has been implemented.

Necessity : Optional（MAY）

Reason : Because support for MLD router function is necessary on a router for a terminal to participate in a multicast network during PIM connection. Optional functions required to ensure connectivity, however, are Optional since they largely depend on the service by a service provider.

Remarks : Many optional functions exist in the specification of PIM-SM/SSM, and

optional functions required to ensure connectivity largely depend on the service specification of a service provider. Furthermore, under a simple tree structure that needs to be supported by a Home Router, implementation by MLD Proxy costs less and is considered to be easier to be introduced than a complex PIM protocol.

7.3.3 Connection by MLD Proxy

Joining/Leaving a multicast group is notified to a service provider using MLD.

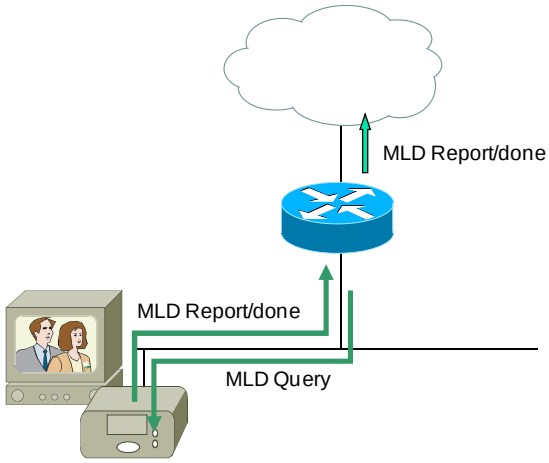

Figure 7-9 Multicast Connection Using MLD Proxy

Requirement 53 : A router has an MLD (v1/v2) Proxy function [42].

Prerequisite : Requirement 50 has been implemented.

Necessity : Mandatory (MUST)

Reason : A function for notifying joining/leaving a multicast group to a service provider is minimally necessary for using multicast service.

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 function [43] as well if a Home Router has a switching function.

Requirement 54 : A router has an MLD (v1/v2) snooping function [43].

Prerequisite : Requirement 50 has been implemented.

Necessity : Optional (MAY)

Reason : Because this is necessary to restrict unnecessary multicast traffic. This function, however, is Optional since its use is expected only if a router has a switching function.

Remarks : It is preferable for a Home Router to have this function if it has a wireless LAN function.

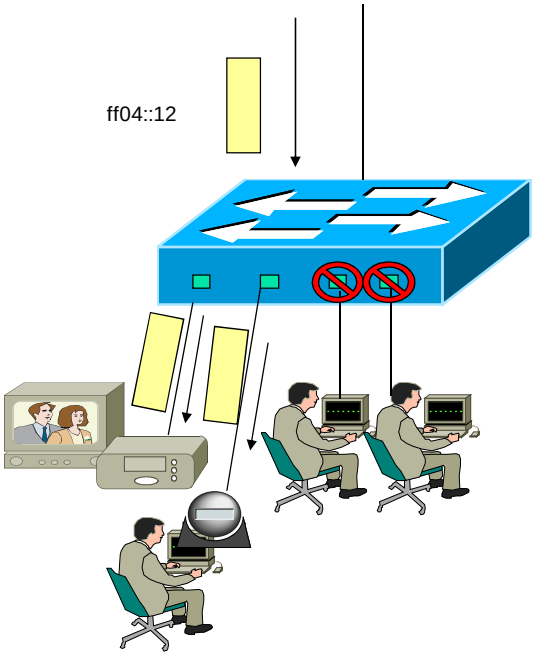

Figure 7-10 MLD Snooping Function

7.4 Special Forwarding

Requirement 55 : A router has a function for appropriately adjusting the MSS (Maximum Segment Size) option of TCP communication through a Home Router.

Necessity : Optional（MAY）

Reason : Because, if the MTU value of the access line is smaller than that of a home network, path MTU discovery is performed every time TCP communication is initiated, reducing communication efficiency. This function, however, is Optional since it can be substituted by the function for distributing MTU information specified in the Section 6.3.1.

Remarks : The value of MSS option field contained in a TCP SYN packet sent by a device in a home network is determined on the basis of the network MTU value. Therefore, if the MTU value of the access line is smaller than that of a home network, the size of TCP segment transmitted from a TCP connection host to a device in the home network is greater than the MTU value of the access line, resulting in path MTU discovery.

The implementation of this function is preferable in order to avoid problems in path MTU discovery resulting from the load on routers in the access network caused by the frequent performance of path MTU discovery.

The appropriate MSS value can be calculated from the MTU/MRU value of the access line.

8 Configuration Function for the Service Side

This chapter describes the configuration method and items to be configured for a Home Router. Note that it is the service provider who is to perform configuration.

8.1 Configuration Method

Requirement 56 : A Home Router has a function that enables the service provider to provide it with required configurations. (A Home Router supplied by the service provider is subject to this requirement.)

Necessity : Recommended (SHOULD)

Reason : A Home Router needs to obtain information required for home network devices to use the service by the service provider by some means. This requirement is classified as Recommended, since it depends on the service of the service provider which method is to be used and since distributing preconfigured Home Routers is also conceivable.

Remarks : It is necessary to prohibit anyone other than the service provider to provide a Home Router with configurations and to make invalid the methods other than the one used by the provider. (See Section 4.1.4.)

Specific methods for configuration are illustrated below.

8.1.1 Auto configuration

This section illustrates the method by which a Home Router obtains the necessary configuration information autonomously, without direct configuration of a Home Router by the service provider.

- A Home Router has a SLAAC function.

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

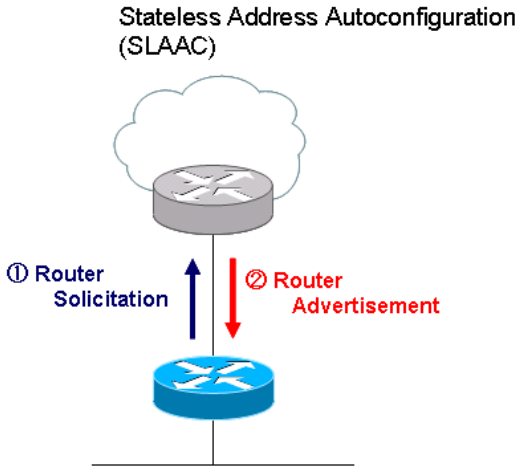

Figure 8-1 Auto configuration by SLAAC

- A Home Router has a DHCPv6 client function.

  A DHCPv6 client function refers to a function for requesting information such as IPv6 address to a DHCPv6 server and reflecting the information obtained in its configuration..

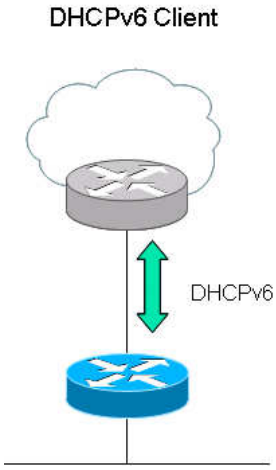

Figure 8-2 Remote Configuration by DHCPv6

- A Home Router can be configured by TR-069

  Configuration method using TR-069, a remote configuration protocol defined by Broadband Forum for CPE.

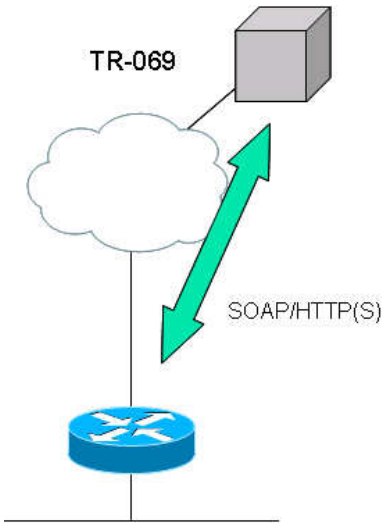

Figure 8-3 Remote Configuration by TR-069

- A Home Router can be configured by UPnP.

  Configuring method using UPnP: automatic equipment registration mechanism defined by UPnP Forum.

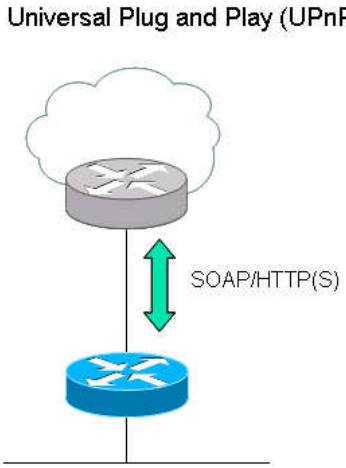

Figure 8-4 Configuration by UPnP

8.1.2 Manual Configuration

Because it is conceivable that the service provider manually configures a Home Router directly, the router needs to be equipped with the interface for it. Specifically, Web interface, telnet, ssh, etc. will be used.

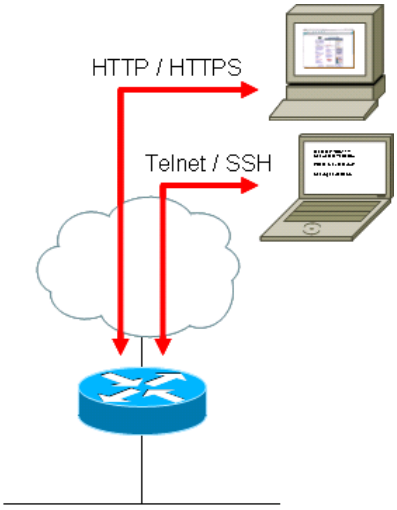

Figure 8-5 Conceptual Diagram for Manual Configuration

8.2 Configuration Items

This section describes specific items to be configured for a Home Router by the configuration methods mentioned in Section 8.1.

8.2.1 Address Configuration

See Chapter 3.

8.2.2 Security-related Configuration

8.2.2.1 Access control from outside

Requirement 57 : A router has a function to turn on and off its remote configuration mechanism.

Necessity : Recommended (SHOULD)

Reason : This requirement is intended to enable providing such service that even users unfamiliar with security setting can maintain the necessary security level for using the service. The requirement is classified as Recommended, since this function depends on the service by the service provider.

Remarks : It needs to be possible for a user to disable this function if it is not used.

Requirement 58 : A router has a function to control access to its configuration mechanism from a certain network or by certain operators.

Necessity : Optional (MAY)

Reason : This is intended to restrict unauthorized access from outside when a global address is assigned. This function is Optional, since it largely depends on the

service by the service provider.

8.2.2.2 Firmware Updating Function

Requirement 59 : A Home Router's firmware can be updated.

Necessity : Recommended（SHOULD）

Reason : This is intended for cases where new functions are added to a Home Router or where it is required to eliminate a newly-discovered vulnerability. This function is classified as Recommended, since depends on the service by the service provider.

Remarks : Although it is primarily used by the service provider, this function may sometimes be used by the user of a Home Router.

8.2.3 DNS Configuration

This section describes the method of configuring a DNS server address for a Home Router when DNS Proxy function is available. See Chapter 5 for other DNS functions.

8.2.3.1 DNS Server Address for DNS Proxy Function

Requirement 60 : A Home Router can use DNS server information obtained through DHCPv6 and so on.

Necessity : Mandatory（MUST）

Reason : Automatic configuration makes setup easy for end users.

Requirement 61 : DNS server information can be configured manually.

Necessity : Mandatory（MUST）

Reason : Automatic distribution of DNS server information may not be supported by the service provider.

8.2.4 Home Network Configuration

This section describes the method of configuring information required for a Home Router to configure home network equipment.

8.2.4.1 Prefix Distributed to the LAN Side

See Chapter 3.

8.2.4.2 Server Addresses Distributed to the LAN Side

Requirement 62 : A Home Router can obtain various server addresses from the service provider as a DHCPv6 client and distribute them to LAN side as a DHCP server.

Necessity : Mandatory（MUST）

Reason : Since server information distributed to a Home Router generally differ depending on the service provided, it is preferable to enable selective distribution of necessary information.

Requirement 63 : A router has a function to configure various kinds of server address manually.

Necessity : Mandatory（MUST）

Reason : Automatic distribution of server information may not be supported by the service provider.

8.2.5 Routing/Multicast Configuration

See Chapter 7.

9 User Interface Function

This chapter describes a user interface provided to Home Router users. The necessity of support of IPv6 used in the user interface is indicated relative to the case where the function provided in IPv4.

9.1 Web-GUI（Graphical User Interface）

Requirement 64 : IPv6 is supported by a router's Web-GUI using protocols shown in Table 9-1 for accepting configuration by users.

Necessity : Recommended（SHOULD）

Table 9-1 Protocols Used for Web-GUI

Protocol	Necessity
HTTP（80/tcp）	Recommended（SHOULD）
HTTPS（443/tcp）	Optional（MAY）

Reason : Because supporting IPv6 transport enhances convenience in configuration by users. This requirement is classified as Recommended, since the minimum functions can be provided by IPv4 transport.

Remarks : A Home Router is generally configured by accessing its Web-GUI from a Web browser installed in a PC or other devices.

It is preferable to use https for the security perspective.

9.2 CLI（Command Line Interface）

Requirement 65 : IPv6 is supported by a router's CLI using protocols shown in Table 9-1 for accepting configuration by users.

Necessity : Optional（MAY）

Table 9-2 Protocols Use for CLI

Protocol	Necessity
TELNET（23/tcp）	Optional（MAY）
SSH（22/tcp）	Optional（MAY）

Reason : Because supporting IPv6 transport enhances convenience in configuration by users. This requirement is classified as Recommended, since the implementation of this function in IPv4 transport is not Mandatory either.

Remarks : It is preferable to use ssh for the security perspective.

9.3 Entry of IPv6 Address/Prefix

Requirement 66 : If a user enters an IPv6 address/prefix, it must be possible to enter it with the notation specified in RFC4291.

Necessity : Recommended（SHOULD）

Reason : Because it enhances convenience in configuration by a user to enable entry in either abbreviated or unabbreviated notation. This function is classified as Recommended, since the absence of its implementation does not affect IPv6 communication.

9.4 Text Representation of IPv6 Address/Prefix

Requirement 67 : It is recommended by IETF [63] for text representation of an IPv6 address/prefix. A router supports the text representation of an IPv6 specified in RFC5952..

Necessity : Recommended（SHOULD）

Reason : Because an IPv6 address may be expressed different notations. This requirement is classified as Recommended, since the absence of its implementation does not affect IPv6 communication.

Remarks : Unifying notation of IPv6 addresses helps correct recognition.

10 Conclusion

10.1 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 10-1. 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.

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

Requirement Assumption	Contents	Necessity	Section	Delta from v1
Requirement 1	A router can obtain prefix information from the connected service provider using DHCPv6-PD.	Mandatory	3.1.1	—
Requirement 2	Prefix information can be manually configured.	Mandatory	3.1.1	—
Requirement 3	A router can receive the prefix assigned by a service provider in the range of /48 - /64.	Mandatory	3.1.2	—
Requirement 4	A global address can be allocated automatically to the WAN side interface.	Mandatory	3.2.1	—
Requirement 5	A global address can be allocated manually to the WAN side interface.	Mandatory	3.2.2	—
Requirement 6	A router can communicate using an address in the prefix assigned to a user if a global address is not allocated to a WAN side interface.	Mandatory	3.2.3	New
Requirement 7	On the basis of a prefix received using DHCPv6-PD from a service provider, a router can generate a /64 prefix and re-distribute it to the LAN side.	Mandatory	3.3.1	—
Requirement 8	A router can select which prefix is to be redistributed to the LAN side if multiple prefixes have been received using DHCPv6-PD from one or more service providers.	Optional	3.3.2	—
Requirement 9	If the prefix distributed using DHCPv6-PD by the service provider changes due to WAN side	Mandatory	3.3.3	Changed Necessity to

	reconnection or other reasons, a router can properly change the prefix to be distributed to the LAN side.			Mandatory
Requirement 10	A router can generate a ULA prefix and distribute it to the LAN side if prefix information is not obtained from the service provider.	Recommended	3.3.4	New
Requirement 11	A router can perform access restriction that allows communication from inside (LAN side) to outside (WAN side) and blocks communication from outside to inside.	Mandatory	4.1.1.1	—
Requirement 12	A router can restrict access by static filter.	Mandatory	4.1.1.2	—
Requirement 13	A router can restrict access by a dynamic filter (SPI).	Recommended	4.1.1.3	—
Requirement 14	A router can configure access control functions indicated in Table 4 1.	Mandatory	4.1.2	Changed a sentence in Table-4.1
Requirement 15	A router can reassemble fragmented packets and control their access based on the requirements for restriction of access from outside.	Optional	4.1.3	New
Requirement 16	Access control is possible with communications to the device itself. Access control is likewise possible with functions controlling the device itself.	Mandatory	4.1.4	—
Requirement 17	A router is equipped with such security functions as warning against configuration changes.	Optional	4.2	New
Requirement 18	Both IPv6 transport and IPv4 transport are usable as transport over which a query to a DNS server is made.	Mandatory	5.1.1	—
Requirement 19	A router can convert a query from the terminal in whatever transport to a one in transport required by the service provider.	Mandatory	5.1.2	New
Requirement 20	If a query from the terminal is made over the same transport as the one used by the DNS server designated by the service provider, a proxy action is performed over the same transport as the one over which a query from the terminal is made.	Optional	5.1.3	Changed a sentence at requirement
Requirement 21	A router can listen on a unicast address (any of	Mandatory	5.2.1	—

	global address, ULA, or link-local address).			
Requirement 22	A router can use multiple DNS servers and select one by sequential search.	Mandatory	5.2.1	Changed a sentence at requirement
Requirement 23	In case there is any function such as a domain identification method which selects a DNS server arbitrarily according to a specific policy, the rules set by such a function should be followed.	Optional	5.3.2	—
Requirement 24	The responses returned to a query from the terminal should be cached, and the cached information should be returned upon subsequent and similar queries.	Optional	5.4.1	—
Requirement 25	Queries from a terminal should all be processed transparently regardless of resource record (RR) type.	Mandatory	5.5.1	—
Requirement 26	Flags and data received that cannot be interpreted must not be changed or deleted.	Mandatory	5.5.2	New
Requirement 27	A router can process EDNS0-compliant query packets (including OPT RRs) transparently and send a response exceeding 512 bytes to a terminal. In addition, a router must forward fragmented response packets without modification or after reassembling them.	Mandatory	5.5.3	—
Requirement 28	A query can be processed transparently even if the terminal (after receiving DNS Header TC=1) falls back to TCP connection. (A router must listen not only on UDP Port 53 but also TCP Port 53.)	Mandatory	5.5.4	—
Requirement 29	A router can process packets supporting DNSSEC transparently.	Optional	5.5.5	Separated requirement
Requirement 30	DNSSEC-compliant recursive processing (validator) including signature verification is implemented as a DNS Proxy/Resover function.	Optional	5.5.5	Separated requirement
Requirement 31	A router has a function to inform a home network terminal of the prefix to be assigned to it through router advertisement (RA).	Mandatory	6.1.1	—
Requirement 32	The length of a prefix notified by RA should be /64	Mandatory	6.1.1	—

Assumption 31	by default.			
Requirement 33 Assumption 31	A router has a function to send an RA such that Preferred Lifetime in its Prefix Information option is set to 0.	Recommended	6.1.1	New
Requirement 34 Assumption 31	A router has a function to send an RA with Router Lifetime set to 0.	Recommended	6.1.1	New
Requirement 35	A router has a function to inform a home network terminal of an address by DHCPv6.	Optional	6.1.2	—
Requirement 36 Assumption 35	A router has a function to send a Reconfigure message with the msg-type of its Reconfigure Message Option set to 5 (Renew message).	Recommended	6.1.2	New
Requirement 37	A router has a function for distributing a prefix to a home device (including another router) via DHCPv6-PD and a function that can specify, for each device, the prefix to be distributed.	Optional	6.1.2	New
Requirement 38	A router has a function for distributing a DNS server address to a LAN segment using RA.	Optional	6.2.1	—
Requirement 39	A router has a function for distributing DNS server address to a LAN segment by DHCPv6	Mandatory	6.2.2	—
Requirement 40	A router has a function for distributing other server addresses (SIP, NTP etc.) to a LAN segment by DHCPv6.	Optional	6.2.2	—
Requirement 41	A router has a function to send a Reconfigure message with the msg-type of its Reconfigure Message option set to 11 (Information-request message).	Recommended	6.2.2	New
Requirement 42	A router has a function to advertise the MTU value of the access line to a LAN segment through RA. The MTU value of the access line to be advertised should be configurable.	Recommended	6.3.1	New
Requirement 43	A router has a function not to forward traffic addressed to the assigned prefix upstream.	Mandatory	7.1	—
Requirement 44	When a router receives packets for an address other than its own interface address on a Point-to-Point link, it must send the ICMPv6 Destination Unreachable message with Code 3	Mandatory	7.1	—

	(Address unreachable) and not forward the packets.			
Requirement 45	A static route for the WAN side can be configured.	Mandatory	7.2.1	—
Requirement 46	Default route auto configuration using RA is possible.	Mandatory	7.2.1	—
Requirement 47	Route distribution to the LAN side by RIPng is possible	Optional	7.2.2	—
Requirement 48	Requirement 48 : It is possible to distribute a route to the LAN side by more specific routes.	Optional	7.2.2	—
Requirement 49	It is possible to prohibit RH0 (Type 0 routing headers) packet forwarding.	Mandatory	7.2.3	—
Requirement 50	Multicast routing function.	Optional	7.3	Summarized assumption
Requirement 51 Assumption 50	A router has a multicast routing function by PIM.	Optional	7.3.2	—
Requirement 52 Assumption 50	A router has a MLD (v1/v2) router function.	Optional	7.3.2	Changed to Optional
Requirement 53 Assumption 50	A router has a MLD (v1/v2) Proxy function.	Mandatory	7.3.3	—
Requirement 54 Assumption 50	Requirement 54 : A router has MLD (v1/v2) snooping function.	Optional	7.3.4	—
Requirement 55	Requirement 55 : A router has a function for appropriately adjusting the MSS (Maximum Segment Size) option of TCP communication through a Home Router.	Optional	7.4	New
Requirement 56	A Home Router is equipped with a function that enables the service provider to provide it with required configurations. (Home Routers supplied by the service provider are subject to this requirement.)	Recommended	8.1	—
Requirement 57	It is possible to configure the access restricting function of a device.	Recommended	8.2.2.1	—
Requirement 58	There is a means for accessing Home Router’s administration interface from the administration segment of a service provider on the WAN interface	Optional	8.2.2.1	—

	side.			
Requirement 59	The router’s firmware can be updated.	Recommended	8.2.2.1	New
Requirement 60	A router can use DNS server information obtained through means such as DHCPv6.	Mandatory	8.2.3.1	—
Requirement 61	DNS server information can be configured manually.	Mandatory	8.2.3.1	—
Requirement 62	A router can obtain server addresses of various kinds from the connected service provider through DHCPv6.	Mandatory	8.2.4.2	—
Requirement 63	Server addresses of various kinds can be manually configured.	Mandatory	8.2.4.2	—
Requirement 64	IPv6 is supported by a router’s Web-GUI using protocols shown in Table 9 1 for accepting configuration by a user.	Recommended	9.1	New
Requirement 65	IPv6 is supported by a router’s CLI using protocols shown in Table 9 2 for accepting configuration by a user.	Optional	9.2	New
Requirement 66	If a user is to be required to enter an IPv6 address/prefix, it must be possible to enter an expression in the notation specified in RFC4291.	Recommended	9.3	New
Requirement 67	The notation recommended by IETF is used for text representation of an IPv6 address/prefix.	Recommended	9.4	New
—	Prefix for distribution to user is fixed.	—	—	Deleted
—	Prefix for distribution to user varies with time.	—	—	Deleted
—	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.	—	—	Deleted
—	A router has a DHCPv6 Relay function.	—	—	Deleted

10.2 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.

10.2.1 Items Not Studied

- Number of supported headers of extension header chain
- Support for transport protocol other than TCP, UDP
- Recommended value for filtering
  - Usable applications list etc.
- 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 address handing
- IPv4/IPv6 inter-conversion function
- Local name resolution/node discovery/service discovery function
  - mDNS (zeroconf), LLMNR, uPnP etc.
- 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.

10.3 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)	IT Holdings Corporation
FUJISAKI, Tomohiro (co-chair)	Nippon Telegraph and Telephone Corporation
NAKAGAWA, Akira (co-chair)	Japan Internet Exchange (JPIX)
INNAMI, Tetsuya (co-chair)	Cisco Systems G.K.
KITAGUCHI, Yoshiaki	Kanazawa University
SHIMADA, Yasuharu	IO Data Device, Inc.
ATARASHI, Yoshifumi	Alaxala Networks Corporation
KASIMURA, Yasuo	Alcatel-Lucent
ASHIDA, Hiroyuki	IS Consulting G.K.
SAHARA, Tomoyuki	Internet Initiative Japan Inc.
KAWASHIMA, Masanobu	NEC AccessTechnica, Ltd.
SUZUKI, Sousuke	NTT Communications Corporation
TOMOCHIKA, Takeshi	NTT Communications Corporation
MIZUKOSHI, Ichiro	Nippon Telegraph and Telephone East Corporation
OKADA, Shingo	Nippon Telegraph and Telephone Corporation
HEI, Yuuichiro	KDDI R&D Laboratories
TSUCHIYA, Shishio	Cisco Systems G.K.
KOHNO, Miya	Juniper Networks
TSUJI, Akira	Century Systems Co., Ltd.
NAKATA, Munehiro	Century Systems Co., Ltd.
KAMINE, Yoshiaki	So-net Entertainment Corporation
MURAKAMI, Makoto	SoftBank Telecom Corp.
SUGANUMA, Makoto	CRUST INC..
HANAYAMA, Hiroshi	Net One Systems Co., Ltd.
IDA, Yoshihiro	Panasonic Communications Co., Ltd.
MOTOHASHI, Atsushi	Fujitsu Limited
ONODA, Mitsuhiro	Yamaha Corporation
TSUKUNI, Takeshi	Mitsubishi Research Institute, Inc. (secretariat)
FUKUSHIMA, Nao	Mitsubishi Research Institute, Inc. (secretariat)

10.4 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
[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] draft-mrw-behave-nat66-02: IPv6-to-IPv6 Network Address Translation (NAT66)
[13] DOCSIS 3.0 specification http://www.cablelabs.com/specifications/doc30.html
[14] RFC 5625: DNS Proxy Implementation Guidelines
[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-client.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 Auto configuration
[49] RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
[50] RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for

IPv6 (DHCPv6)
[51] RFC 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] draft-ietf-softwire-ipv6-6rd-08: IPv6 via IPv4 Service Provider Networks "6rd"
[54] draft-shirasaki-nat444-isp-shared-addr-03: NAT444 with ISP Shared Address
[55] draft-ietf-softwire-dual-stack-lite-04: Dual-stack lite broadband deployments post IPv4 exhaustion
[56] draft-ymbk-aplusp-05: The A+P Approach to the IPv4 Address Shortage
[57] Issues with Port-Restricted IPs
http://www.ietf.org/proceedings/09nov/slides/aplusp-3.pdf
[58] draft-ietf-behave-v6v4-xlate-stateful-11: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
[59] draft-ietf-v6ops-ipv6-cpe-router-04: Basic Requirements for IPv6 Customer Edge Routers
[60] IPv6 Migration Guidelines (2005) Security Segment
http://www.v6pc.jp/jp/archive/index.phtml
[61] draft-ietf-v6ops-cpe-simple-security-11: Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service
[62] RFC 5571: Softwire Hub and Spoke Deployment Framework with Layer Two Tunneling Protocol Version 2 (L2TPv2)
[63] draft-ietf-6man-text-addr-representation-07: A Recommendation for IPv6 Address Text Representation
[64] RFC 3041: Privacy Extensions for Stateless Address Auto configuration in IPv6

These references would have possibly been updated.