2005 Version

IPv6 Deployment Guideline

ISP Segment

March 2005

IPv6 Promotion Council of Japan
DP-WG ISP SWG

Table of contents

Introduction

This document is created for use by middle and small sized ISPs and Operators/SIers who are involved in the construction and management of access networks, and describes general items, guidelines and methods that should be investigated when middle and small ISPs and access network providers introduce IPv6 in the future.

The contents described here indicate only some examples of the concept, and they are not the only solution. This document is meant to be used as a reference when readers introduce IPv6 according to their own management policies and restriction conditions.

Outline

Features of segment

- Features of middle and small ISP segments are analyzed and described.
- Features of connection methods between access networks and customers/ISPs are analyzed and described.

Connection between access networks and customers	Site type, Host type
Connection between access networks and ISPs	P2P, PTA, LAA

Deployment made by middle and small ISPs

- Deployment methods for network, routing and addressing in middle and small sized ISP backbones are described.

Deployment in access network

- Deployment method in the form of access network shown below has been investigated.
  ADSL/FTTH, CATV, wireless LAN, mobile, tunnel access

IPv6 deployment case study of middle/small sized ISP

- Case study is included, in which it is assumed that the middle and small sized IPv4 ISPs carry out the IPv6 test service.

1. Features of Segment

Targets

Provision targets: Wholesale (Flet's, eAccess, ACCA, etc.), retail (OCN, ODN, DION, @Nifty, BIGLOBE, Yahoo! BB, etc.)
Geographical range: Global (UUNET, VERIO, etc.), national (OCN, ODN, DION, @Nifty, BIGLOBE, Yahoo! BB, etc.), regional (local ISP)
Contents of service: IP connectivity, application (ASP), operation management agency service (MSP)

In this document, the discussion is made targeting general middle/small sized ISPs with the following features.

- Those that purchase part of their configuration factors from another provider and have general consumers as their customers (retail)
- Those that are semi major enterprises that have not yet reached national scale (national ~ regional)
- Those that provide IP connectivity and basic applications (DNS, Web, Email)

Target Access Networks

The target access networks of this guideline provide a connection with ISP core networks in order for customer networks to obtain connectivity with the Internet.
This guideline classifies connections according to the physical form (ADSL, FTTH, CATV, wireless LAN, mobile, connection by IPv6 tunneling on IPv4 Internet). PSTN and FWA are not included as targets for investigation in this guideline.

What is IPv6 Deployment for Middle/Small ISPs and Access Network Providers

The motivations for middle/small sized ISPs and access network providers to deploy to IPv6 are;

- to cope with advanced service at an early stage
- to cope with the release of equipment and applications that attract users
- to cope with national measures and changes in the ISP industry

Therefore, as an easy deployment plan for those providers to use, it is better to consider starting a new service, rather than replacing the existing service. If the new service is a good one, users will automatically shift to it as a consequence (E.g.: Dial up ⇒ ADSL, regular phone ⇒ regular phone/IP phone).

The following are the points that middle and small ISPs and access network providers must consider when they start a new service.

- Costs related to a new service (IPv6 service) (small scale start is preferable as of now, where it is difficult to predict the time to pay)
- Operation cost
- Upgrading cost of equipment
- User support cost, etc.
- Influence on the existing service (IPv4 service) (influence on the existing service (IPv4 service) should be avoided. Compared with ISP, hurdle to deploy to IPv6 is higher for access network providers due to the unique conditions of each network, therefore, it is required to investigate thoroughly before deployment in their case.)
- Necessary resources for new service (personnel, know-how)(Many middle/small sized ISPs run their business with a small number of people, therefore they will need to utilize the outsource menu of other companies, educate personnel required for full-scale operation through experimental services, etc. and to accumulate know-how.)

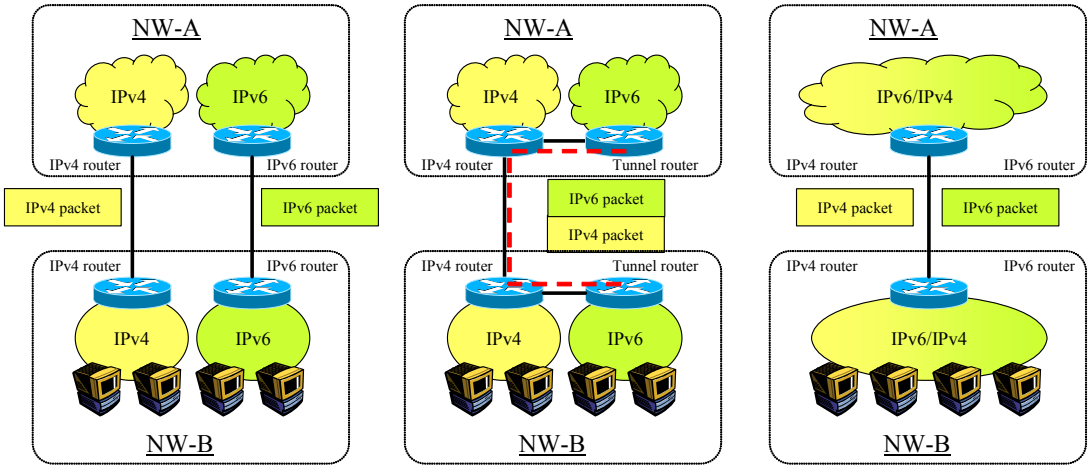
3 Methods of Supporting IPv6

There are 3 types of connection method for supporting IPv6, which are Native, Tunnel and Dual. When an ISP deploy IPv6, they must use these methods (single or multiple) and realize IPv6 communication for upper connection and connection with the backbone of own company and users.

When Native is used, it is possible to introduce IPv6 without affecting the IPv4 environment at all, however, the deployment cost is the largest of the 3 for ISPs. This method is suitable for critical cases where the IPv4 environment is stable.

When Tunnel is used, it is possible to introduce IPv6 almost without affecting the IPv4 environment. Cost is about the middle level, and this is suitable for ISPs who wish to keep using the existing IPv4 environment and to avoid a large influence on the IPv4 environment.

Dual is the ideal method, with which it is possible to use both protocols of IPv6 and IPv4 together. Cost is considered to be the smallest of three. However, it becomes necessary to make all L3 nodes including router and firewall used inside ISP support IPv6/IPv4 dual.



Native

- Possible to deploy IPv6 without giving any influence to IPv4 environment
- Largest cost
- For the case where stability of IPv4 environment is critical

Tunnel

- Possible to deploy IPv6 without having hardly any influence on IPv4 environment.
- Cost is middle scale
- For the case where existing IPv4 environment is used and influence on it is desired to be as small as possible.

Dual

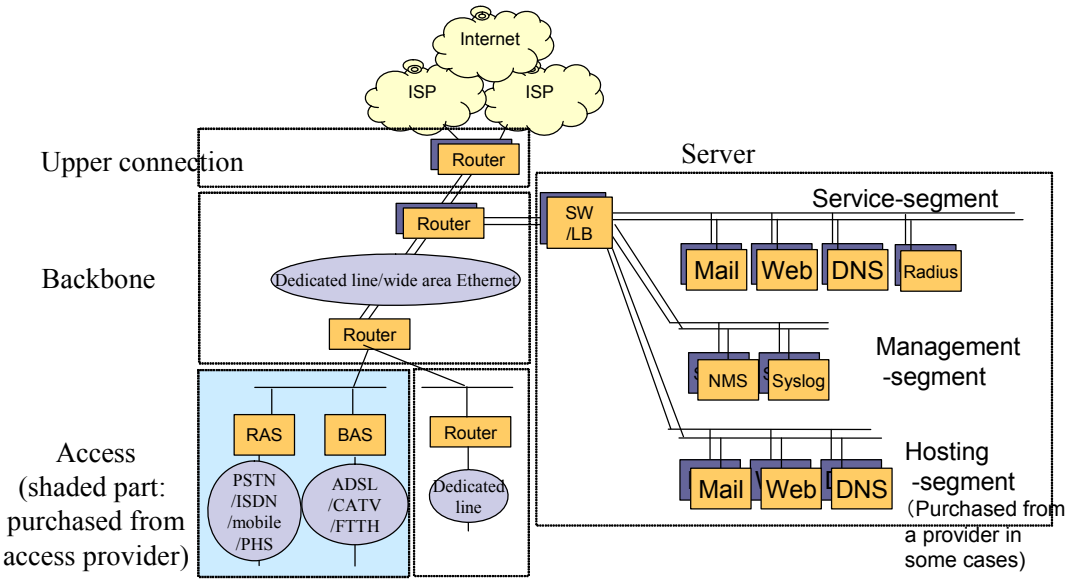
- Ideal method where both IPv6/IPv4 protocols can be used together.
- Smallest cost
- For the case where it is possible to shift all L3 nodes including router/ firewall to support IPv6/IPv4 Dual.

2005.1

Configuration Factors for Middle/Small Sized ISP

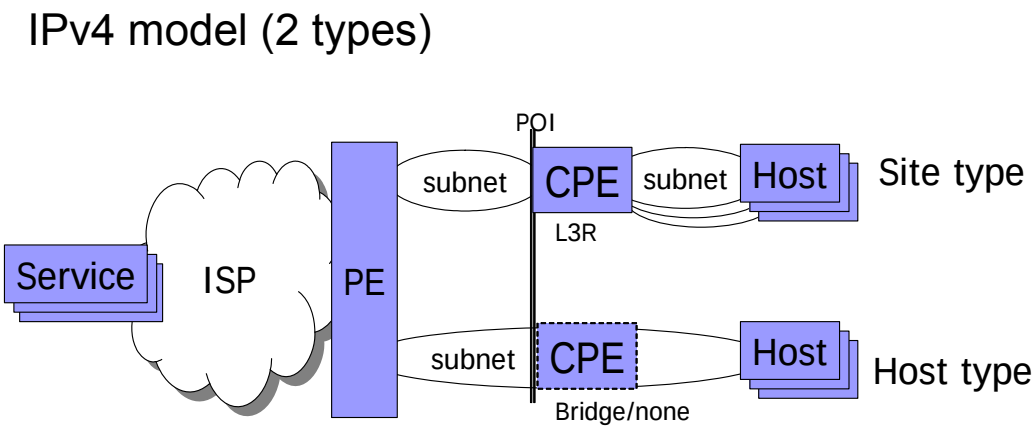
The Fig. shows the general network configuration of middle/small sized ISPs. They purchase access service such as Dial up, ADSL and FTTH from an access provider, connect it to the network backbone of their own company configured with dedicated line or wide area Ethernet together with a direct dedicated line from a user and then connect to the Internet via upper SIP.

The server segment is connected to a backbone, and this server segment is configured with DNS and Email server of which the target is the overall service, the service segment in which web server is installed, management segment in which network management system or syslog server is installed and the hosting segment that operates the web server, Email server and DNS for hosting service oriented to users.



Configuration of Access Network

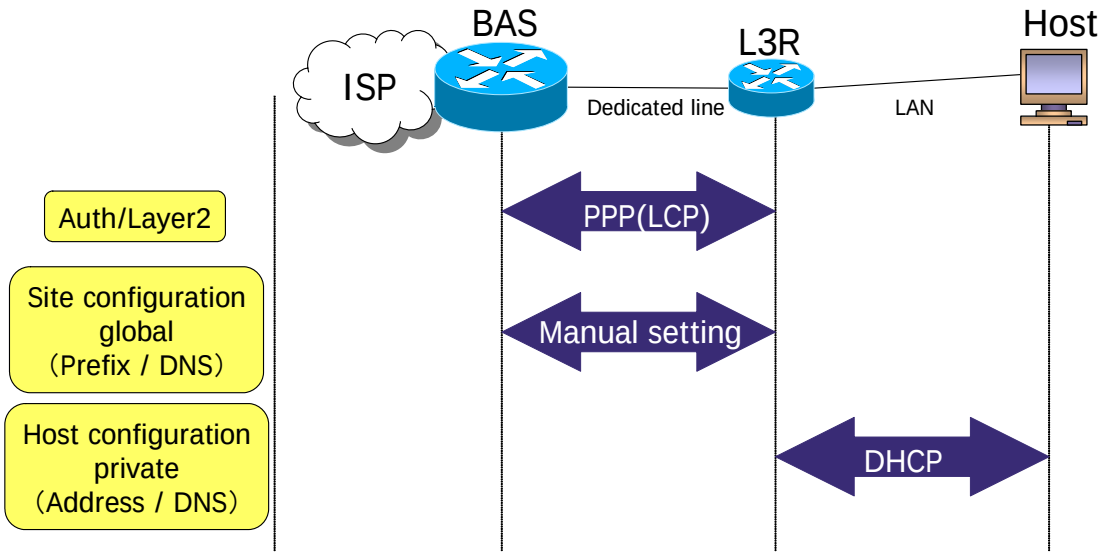
Access networks of the present IPv4 service can be categorized into 2 broad forms, Site type and Host type according to the connection form of the customer.



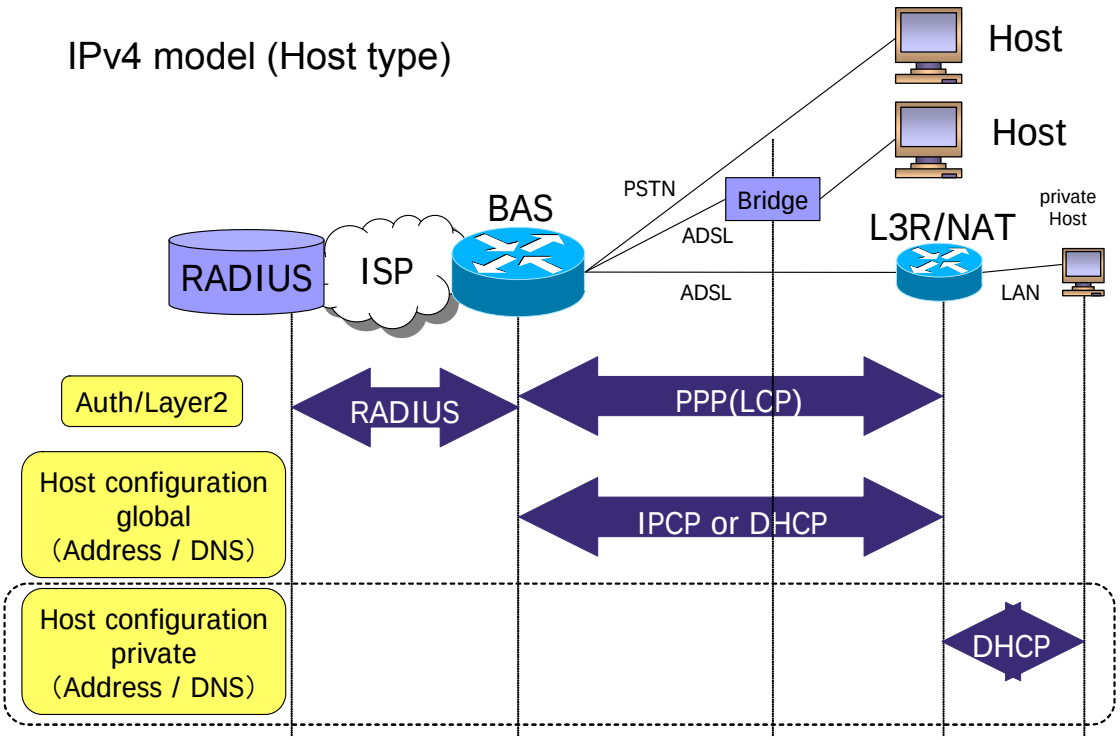
	CPE type	Example
Site type	L3R(Router)	Economy type service, Dedicated line for enterprise type service
Host type	L2 Bridge/ none	Many Dial up connection type services and ADSL /FTTH services use this model, (Host=NAT/Router), Hotspot

In the case of Site type, a router is installed on the user base. This form is used for the line service used by an enterprise. Authentication or layer 2 connection is performed through PPP.

IPv4 model (Site type)



Host type is a provision form of a service for most consumers, including ADSL, FTTH and wireless LAN.


IPv4 model (Host type)
Host
Host
PSTN
Bridge
BAS
ADSL
L3R/NAT
private
Host
RADIUS
ISP
ADSL
LAN
Auth/Layer2
RADIUS
PPP(LCP)
Host configuration
global
（Address / DNS）
IPCP or DHCP
Host configuration
private
（Address / DNS）
DHCP

2. Best Current Practice

Range and investigation policy of BCP

In the following, best current practice (BCP) is discussed. The method (experimental, commercial) by which middle/small sized ISPs and access network providers are able to use with their own ability immediately is described.

Target ISPs are those who provide connectivity to external Internet and application services (DNS, Web, Mail) at present. It is assumed that the access provider provides connectivity to ISP.

Investigation policy is to consider the influence on the IPv4 service, consider cost reasonableness, illustrate merits and demerits of options and illustrate deployment model cases.

Current State of IPv6 Connectivity Service

IPv6 connection services provided at present are as shown below.

ISP service (for company)

Dedicated line (ATM, STM): Native, Dual, Tunnel

LAN(DC): Tunnel, Native

ISP service (for individual)

ADSL: Tunnel, Dual

FTTH: Tunnel, Dual

CATV: Dual (experimental), Native (experimental)

Wireless LAN: Dual (experimental)

PSTN: Dual (experimental)

Mobile (PHS): Dual (experimental)

Tunnel ASP service as others

2.1 Deployment for Middle/Small ISPs

Outline of recommended deployment method

In the following, recommended deployment methods are described from the 3 view points of addressing, routing and networking. At first an outline of these methods is mentioned.

Addressing

It is recommended to get sTLA.

/48 Prefix shall be allocated to a site.

Routing

It is recommended to use routing protocol used for IPv4.

It shall be possible to construct routing topology of IPv6 and IPv4 separately.

When ISIS is used, it is sometimes necessary to match routing topology of IPv6 and IPv4.

Network

It causes less impact at the introduction period when IPv6 is constructed independently from IPv4.

Networks of IPv6 and IPv4 shall be integrated at the expansion period of IPv6 network.

Addressing

Initial allocation size of address

There are 2 usage purposes of address for a provider:

・Address space distributed to a customer (for a user)

・Address space for operation and management of own network (for infrastructure)

Address space acquisition varies according to acquisition method.

	Size	Acquisition methods
sTLA	/32(/35)	Allocation by APNIC
NLA	/33～/47 /32	Re-allocation by a holder

Each provider chooses either sTLA or NLA depending on network scale, connection requirements and ease of operation/management.

Note: the expressions sTLA and NLA are not used any more, but they are used in this document for convenience.

Comparison of sTLA and NLA

The table below compares the merits and demerits of address space between sTLA and NLA for ISPs.

	sTLA	NLA
BGP4+	●Possible to control paths with Internet (Multihome) ▲Some conditions to apply for acquisition ▲ISPs including lower ISPs have a duty to register /48 ▲Duty to control DNS reverse resolution of acquisition space	●Acquisition and operation are easy according to distribution condition of upper ISP ●Peer (exchange of paths for address space of adjacent ISPs) is possible. ▲It is restricted to secure redundancy path with Internet ▲Man hours for deployment to sTLA are large
nonBGP4+	●Operation is easy (Possible to use BGP4+ later) ▲Some conditions to apply for acquisition ▲Difficult to secure redundancy path with Internet ▲ ISPs including lower ISPs have a duty to control /48 ▲Duty to control DNS reverse resolution of acquisition space	●Acquisition and operation are easy according to distribution condition of upper ISP ●Operation is easy ▲Difficult to secure redundancy path with Internet ▲Man hours for deployment to sTLA are large

- The hurdles to acquire/operate sTLA are not high, and it will be common for middle and small sized ISPs to acquire sTLA.

Address acquisition conditions

The address acquisition conditions of sTLA and NLA are described below. The hurdles for acquiring and operating sTLA are not high, so middle and small sized ISPs will get sTLA in many cases.

<u>sTLA</u>

It is necessary to be a member of APNIC or be a specified provider of JPNIC address management, and it is also necessary to comply with the APNIC address policy shown below.

Qualification for initial allocation of IPv6 addresses (sTLA)

a) You should be an LIR.
b) You should not be an end site.
c) You should have a plan to provide connectivity with IPv6 Internet for the organization to which /48 is assigned. At this time, path advertisement for the Internet should be aggregated to one allocated address.
d) You should have a plan to allocate 200 /48 at least within 2 years.

NLA

NLA is the address acquired from the upper ISP. It becomes a condition to comply with the allocation policy of upper ISP (ISP with /32, etc.) to acquire this address. Normally this forms a set with usage of IPv6 connection service of upper ISP.

Address space to be allocated seems to be based on the planned number of /48 in one year's time (or 2 years' time) in many cases, though it depends on the policy of upper ISP. Therefore, it is necessary to determine the upper ISP taking into account the address space to be allocated, connection requirements and so on.

Path control method with sTLA

In the case of sTLA, there are 2 kinds of routing protocol available; BGP4+ and Static.

With BGP4+, it is possible to control the path with IPv6 Internet. When there is just one upper ISP, Static is sufficient, but it is necessary to prepare for usage of BGP4+ in the future.

Duty of a holder of sTLA

When you acquire and use sTLA, the following duties are imposed.

Report of allocation of a Prefix to a customer

When you allocate a Prefix space of /48 to a customer, you are obliged to register the information with APNIC. Report of /48 to APNIC is made by mail. (registering Person Object for Tech-c and Admin-c, and registering inet6num Object)

Reverse resolution of sTLA space DNS

You are obliged to control the DNS reverse resolution space of acquired sTLA.

Acquisition method of NLA

Address of NLA is acquired from the upper ISP (sTLA, NLA). Address is normally assigned as an asset with usage of IPv6 connection service of upper ISP. The upper ISP for the IPv6 connection doesn't have to be the same upper ISP as for IPv4.

The size of address space to be assigned is often based on the planned number of /48 for a year's time (and 2 years' time) of the target for assignment, though it depends on the policy of the upper ISP. It is considered better to determine the upper ISP taking into account address space to be assigned and connection requirements.

Path control method with NLA

In the case of NLA, connectivity to the IPv6 Internet is acquired from the upper ISP from which NLA is acquired.

At present in Japan, filtering of prefixes longer than /35 is generally carried out at many ASs from the view point of aggregating paths of the overall Internet. However, in RFC2772 (6Bone Backbone Routing Guidelines) that regulates the usage rules of IPv6 experimental network 6bone, punching holes is prohibited.

Routing varies as well, according to a policy of upper ISP. There are cases where setting default path to the upper ISP with Static and when IPv6 full path can be received with BGP4+. It is possible to make the path for specified ISP redundant through Internet Exchange (IX) or Private Peering. If the implied consensus between ASs is destroyed in the future, it is a concern that there may be an effect from an expanding number of paths caused by punching holes.

Deployment from NLA to sTLA

As an opportunity for an ISP that has started with NLA to deploy to sTLA, there are 2 cases assumed; the case where multihome is introduced for stability of paths and the case where larger address space (sTLA) is required because consumption of NLA addresses is promoted.

When deploying, for instance, sTLA is acquired at first, then connection is made with the upper ISP or IX, sTLA path is advertised and renumbering work is carried out. At this time, deployment work of address should be performed not only in the network of ones own company but also at the site of a customer. Refer to Tips in Section 4 for concrete work.

Addressing Method

Addressing to a customer

Address should be assigned to end users according to the IPv6 address policy of RIR (APNIC) (http://ftp.apnic.net/apnic/docs/ipv6-address-policy). Under this address policy, /48 shall be assigned to one connection as a basic rule, however, it is also mentioned as an option in the policy to assign /64 in cases where the environment of a customer is only 1 segment or to assign /128 in the case of just one terminal. Under the present IPv6 connection service, normally /48 or /64 is assigned to a connection for a consumer (ADSL, etc.).

It should be noted that it is necessary to register whois with RIR in the case of /48 and that it is required to handle additional assignment process to an end user (paperwork, aggregation of paths) in the case of /64.

Addressing in network infrastructure

Address space of IPv6 is huge compared with IPv4, so it becomes possible to make a plan with a margin easily. First of all, you don't need to think about the number of hosts, so all subnets are generally configured with /64. Moreover, ISP is able to assign /48 for each POP as an infrastructure. In general, it is possible to consider giving priority to aggregation of paths inside ISP over address usage efficiency.

In the case of sTLA (/32), if 7132 pcs. of /48 (usage rate 10.9%) are assigned, it becomes possible to receive additional allocation (from HD-Ratio (in the case of usage rate 0.8)).

ISP needs to register with APNIC database for each /48, however, if the registered number exceeds HD-Ratio: 0.8, it will be possible to receive additional allocation (double the address space) immediately after the application is made.

It is considered preferable to assign addresses for customers by aggregating them for each connection POP so that it becomes possible to aggregate paths (the idea is the same as that of IPv4). In the case that a tunnel for a customer terminates at the server of the center at first, it is necessary to consider renumbering when a customer deploys to dual service (change of accommodation to edge).

Addressing in server segment

In order to secure the address space for the server segment, /64 shall be assigned to one LAN segment. It is also considered effective to secure multiple /64 in one LAN segment so that it becomes possible to handle the assumed method of usage for the future (source

address selection, etc.).

Routing

EGP

For EGP, BGP4+ (eBGP, iBGP) is used. It is possible to use the same technology as IPv4 BGP such as full-mesh, route reflector and confederation.

BGP routing topology

External connection (eBGP) shall follow the policy of the connection destination whether lines should be separated for each protocol (IPv6 Native link is added) or peering shall be performed on different routers for IPv4 and IPv6 on Dual segment. It is also possible to set peer topology for the internal connection (iBGP) independently from that of IPv4.

Notes for implementation of BGP of IPv6 router

In the case of middle and small ISPs, the same AS is generally used for both IPv6 and IPv4 except in special cases, however, if it is different, it is not possible to start BGP process of 2AS with the same router in the case of some routers.

When it is implemented to change IPv4 and IPv6 paths in one BGP4+ process, the following points should be noted in the configuration of iBGP.

- It is necessary to use the same AS number for IPv6 and IPv4.
- It is necessary to have the same configuration of RR for IPv6 and IPv4 (Route Reflector Cluster-ID is the same).
- It is necessary to have the same configuration of SubAS for IPv4 and IPv6 (Confederation SubAs is the same).

BGP Peer

With regard to BGP Peer, the following two points should be noted.

Reception of NLRI (Network Layer Reachability Information)

We recommend that you do not handle IPv6 NLRI with IPv4 Peer because dependence on the reachability of information on other protocols should be avoided. Which means that

IPv4 routing should be peered with IPv4 address and IPv6 routing should be peered with IPv6 address.

Peer address

Global addresses and link local address are considered for peer addresses. eBGP should follow the policy of IX and connection destination as a basic rule, however, in the address policy, it is determined that it is possible to assign the non-routable global address for IX to IX. It is sometimes difficult to maintain stable operation with link local address due to specification of eBGP, therefore we recommend the use of global addresses if it is possible to choose. For iBGP, global addresses are used.

BGP routing policy

With regard to routing filter, prefix filter should be introduced for the setting of each peer and others than s/pTLA should be filtered out. Moreover it is desirable to use AS Path filter simultaneously. It is OK to pass 6to4 prefix (2002::/16), but performing punching holes of /35 should be prevented at ISPs that have /32. Communication of site local address for which usage has already terminated should preferably be filtered with the external connection interface to make sure.

In order to check legitimacy of prefix in IPv6, information of s/pTLA or database of each RIR or 6bone shall be checked.

Reception of full path

It is possible to receive IPv6 full path by using IPv6 connection service (commercial, experimental) of the upper ISP or by connecting with experimental and research organizations such as WIDE. When you would like to keep a certain level of connection service from the viewpoint of stability of the path, we recommend using the commercial IPv6 service as one of them.

IGP

There are OSPFv3, i/IS-ISv6, RIPng and Static as options for IGP, however, for IGP that becomes a core, we recommend using the same Link State method dynamic routing as IPv4 (OSPFv3 already has usage results by major ISPs). Because Link State method has 2 advantages; convergence of path is quick and aggregation of paths is possible.

However, in the case of small scale at the initial stage of introduction (tunnel only) or so on, Static or RIPng can be used. It is also possible to start with Static or RIPng and change to OSPFv3 when the number of HOPs or routers handled increases in the future.

Selection of IGP

With regard to select IGP in IPv6, it is better to select IPv6 versions of protocols used for IPv4 from the view point of usage experience. Which means selecting RIPng when RIP is used for IPv4 and OSPFv3 when OSPFv2 is used.

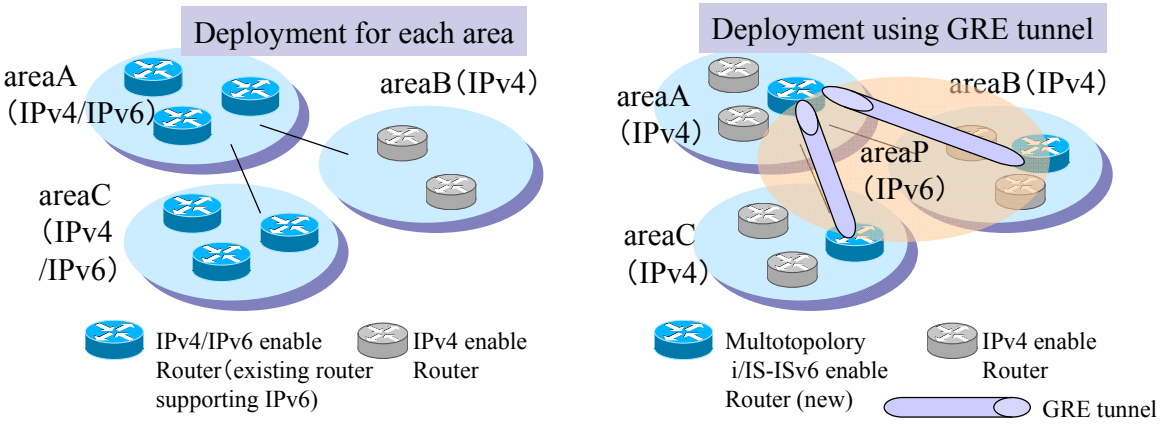
However, in the case of i/IS-IS → i/IS-ISv6, there are 2 restrictions, therefore it isn't suitable for phased deployment.

- In order to set IPv6 routing topology and IPv4 routing topology independently within the same area, it is necessary to adopt multitopology i/IS-IS (in order to support IPv6 using i/IS-IS, it is necessary to operate all i/IS-IS routers of IPv4 that operate within the same area in IPv6 as well).
- Transport of routing information is OSI protocol, so it is not handled for IPv6 over IPv4 tunnel. Therefore, it becomes necessary to use tunneling technology that doesn't depend on IP protocol, such as GRE tunnel, but in such cases, triple stack of IPv6, GRE and IPv4 is formed and overheads increase.

If the above mentioned point becomes a problem, it is better to use i/IS-IS → OSPFv3.

Routing topology of IGP

Routing topology of RIPng and OSPFv3 can be designed independently for IPv4 and IPv6. In the case of i/IS-ISv6, the following 2 patterns can be used as a phased deployment procedure according to the conditions described previously.



Control of path with end users

In the case of IPv6, the number of cases where end users have prefixes increases compared with IPv4, therefore, the ratio of requirement to control path increases.

When dynamic routing is used, it is necessary to filter to avoid a path advertised by user having an affect inside the ISP.

Moreover, when using RA on a segment shared by multiple users, it is necessary to filter using a switch or modem so that even if a certain user outputs RA by mistake, it doesn't spread to other users, or, even though this is not a perfect countermeasure, it is necessary to set router-preference of the upper router to high.

Network

Upper connection

Menu provided by the upper ISP can be classified as shown below.

Connection method: Tunnel type, Native type, L2 shared type, Dual type
Routing protocol: BGP4+, Static

Router for connection with upper can be configured in a dedicated manner for IPv6 service, or in a shared manner between IPv4 service and v6 service. "Dedicated" here means not to place traffic of IPv4 service users, and doesn't mean to operate the router only for IPv6. There is no other choice but to operate a dedicated router for IPv6 service as Dual Stack for

the time being for the sake of router management (SNMP, etc.).

Explanation of each upper connection pattern

Provision menus of upper ISP have various features shown below.

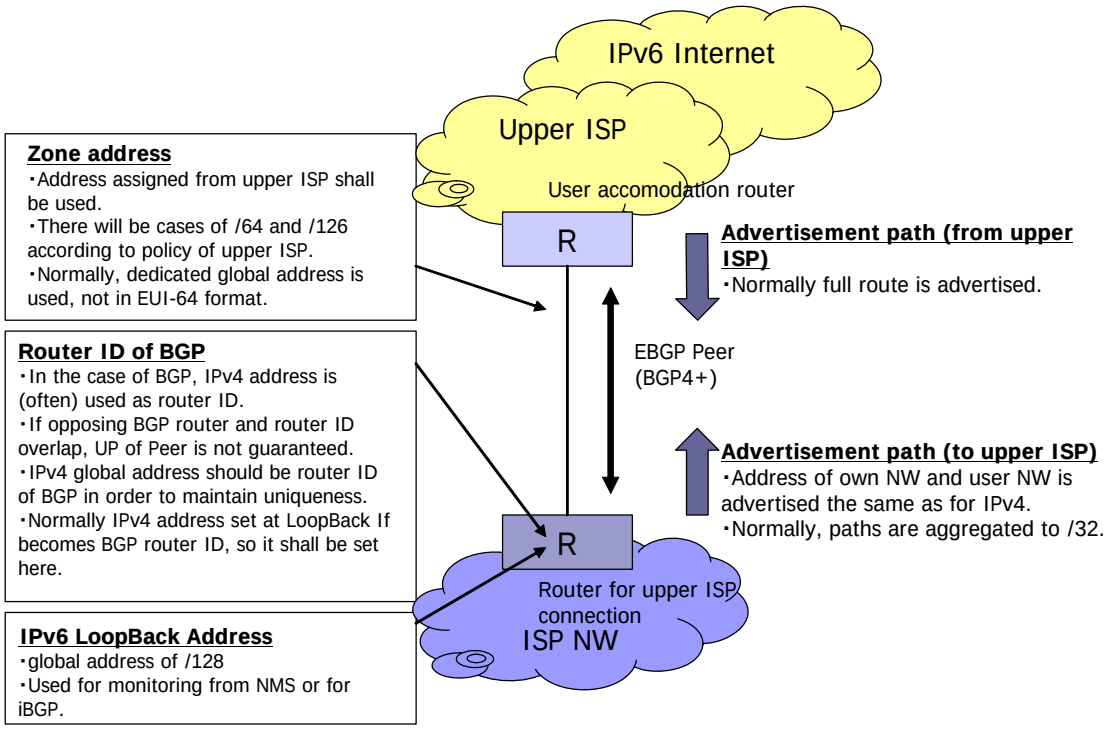
- Tunnel type, L2 shared type
  Fee is charged as an additional service of IPv4 in many cases.
- Dual type
  No new line is necessary, and it is cheaper than purchasing both IPv4 and IPv6 services.
- Native type
  A line is necessary for IPv6, therefore cost increases if the contact point with the upper ISP is geographically distant.

In addition to the above mentioned points, usable routing protocol (BGP4+, Static), fees and dealing with changes in menu in the future should be considered when selecting the upper ISP.

With regard to a router on the ISP for connecting with the upper, defect of a router for connection with upper affects all existing services, therefore it is safer (possible with types other than Dual type) when routers are separated for the existing service (IPv4) where stable operation is requisite and for new service (IPv6). When setting a router dedicated to IPv6 service, the capital investment is pointed out as a disadvantage.

Configuration example of upper connection (BGP4+)

Fig. shows a configuration example of connection with upper in the case of middle and small ISPs.



Peer connection

Peer connection is carried out with BGP4+.

In the case of public peers (peer via IX), connection is generally made to Layer 2 switch. It is not common to connect to Layer 3 (router) IX, or to connect to IX via tunnel.

On the other hand, in the case of private peers (peer directly connected between ISPs), peer can be formed by tunnel.

Therefore, 3 kinds; Native, Dual stack and Tunnel are considered as configuration patterns for peer connection.

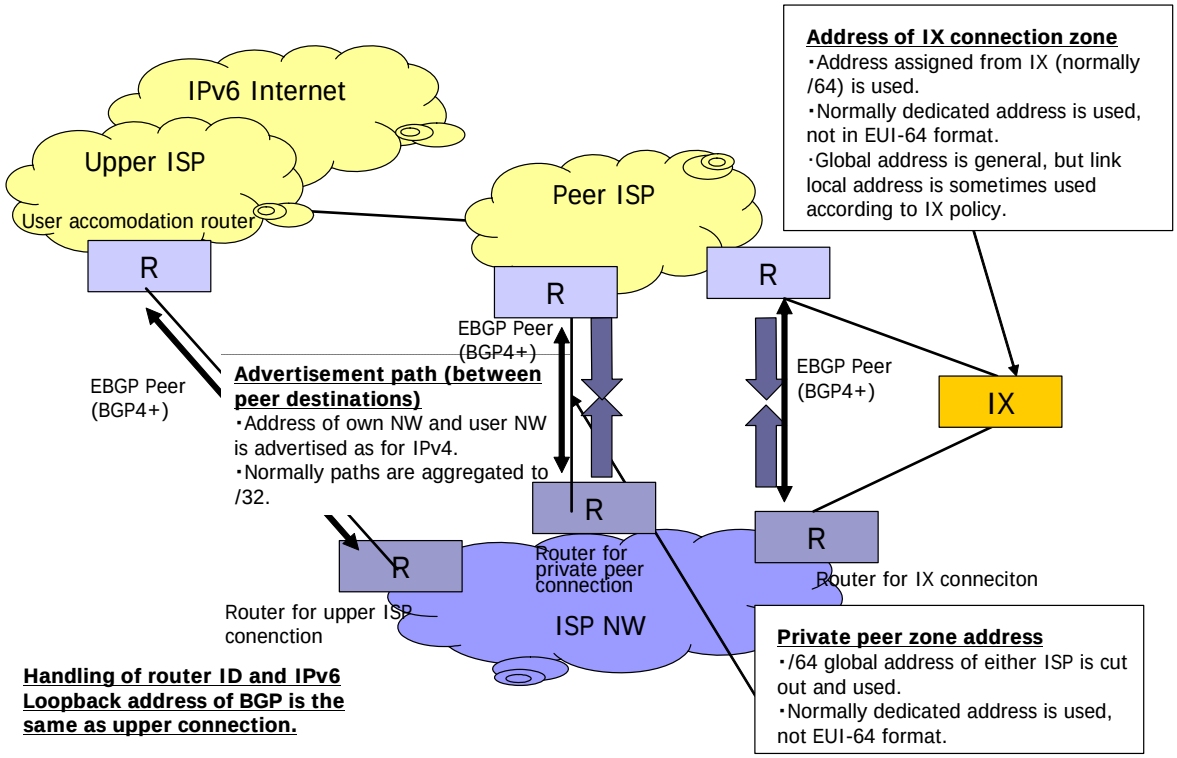
Peer connection method using tunnel is sometimes used for private peers. This method is probably used for IPv6 peers with ISP connected directly under IPv4.

As “Direct connection” of this case, there are IPv4 private peers, IPv4 public peers and IPv4upper/customer connections.

We don’t recommend setting a tunnel peer across other ISP networks. Because, if any trouble occurs in reachability of tunnel, it becomes difficult to monitor and handle the state.

Configuration example of peer connection (BGP4+)

Fig. shows a configuration example of peer connection in the case of middle and small sized ISPs.



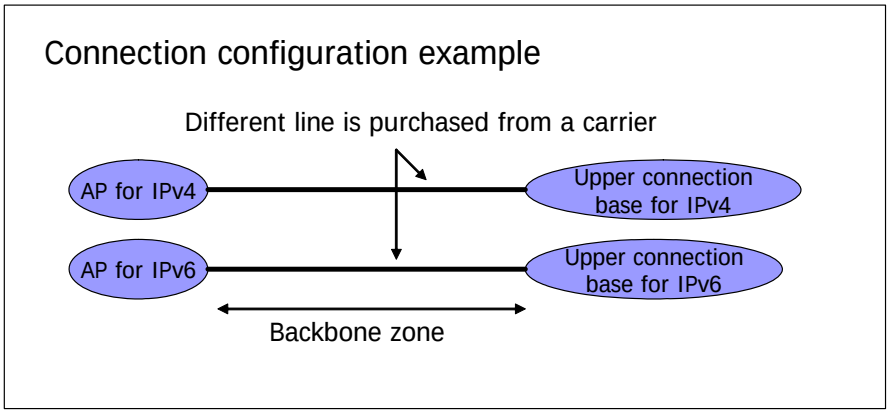
Backbone

Backbone of middle/small sized ISPs can be defined as “line used to connect the setting base of a router for connecting with the upper and the access point”. “Access point” here means the connection point with the access line provider. In this case, it is not always the case that there is a router at an access point. Middle/small sized ISPs buy backbone line from other communication providers. These days, may of them buy the wide area Ethernet service. Purchase of lines for backbone is sometimes used with the same meaning as construction of backbone.

Backbone configuration can be classified into 4 types; separate line (dedicated for IPv6 service) type, Tunnel type, Shared line (L2 separation) type and Dual type.

Separate line (dedicated for IPv6 service) type

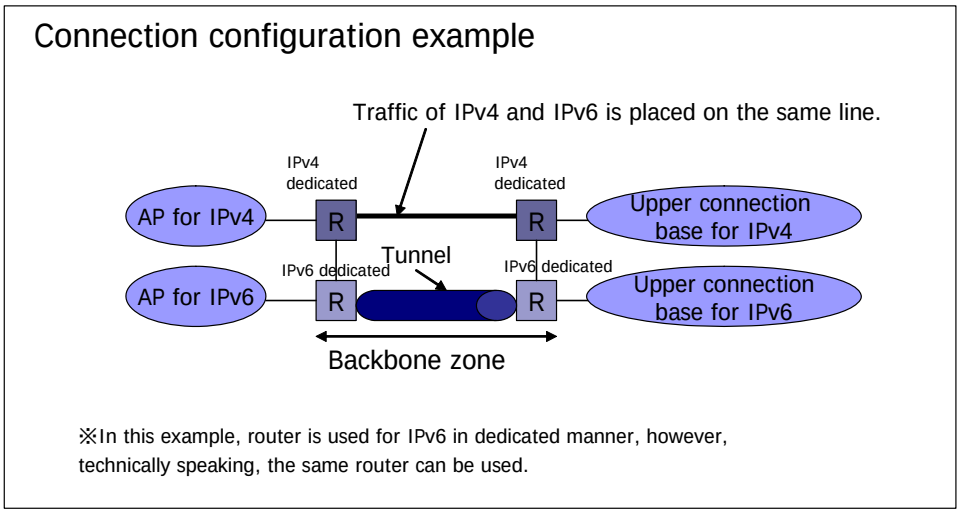
In this case a separate line is purchased for IPv6, and the merit is that no influence is received from traffic of other service. However, the disadvantage is that the line cost increases because a new line is required.



Tunnel type

This configuration at deployment has been referred to frequently, but there are problems shown below when the target of this type is a middle/small sized ISP.

- Router isn't always set at the access point in the case of middle/small ISP.
- Even if there is a router, it doesn't always support IPv6.
- Even if luckily it supports IPv6, it is necessary to estimate the influence on the existing service.
- This depends on the number of access points, but a substantial amount of capital investment is required to set a new router for tunnel.



Notes at constructing a network with tunnel

MTU size

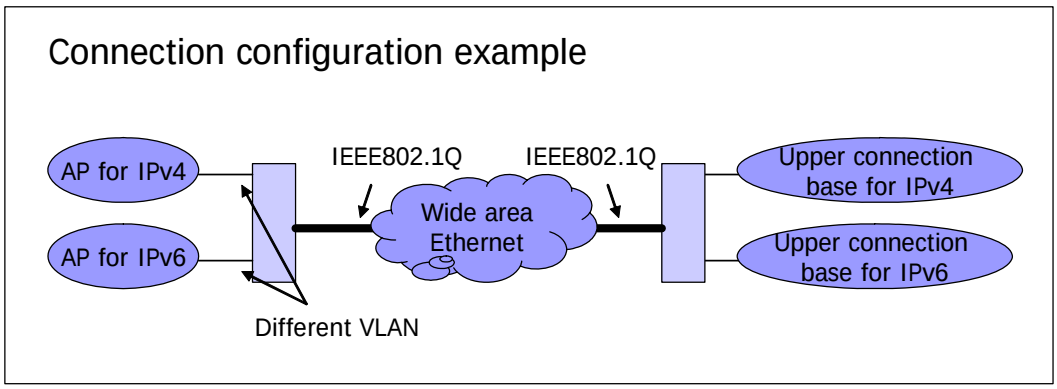
It is recommended to match MTU size of tunnel interface at the both ends. If Path MTU size in a tunnel zone is unknown, MTU of tunnel interface should be set at 1280 byte. When Path MTU value is known, it is OK to adjust MTU size of tunnel interface according to such a value.

Life/death observation of tunnel interface

Under general implementation, life/death of tunnel interface doesn't link with life/death of IPv4 address, which is a terminal point of tunnel. Even if reachability of tunnel terminal to IPv4 address disappears, tunnel interface itself doesn't collapse. Particular care must be taken in the case that reachability of tunnel to IPv4 address is secured by setting path statically, because it is not possible to handle dynamically. It is desirable to observe life/death of IPv4 address at the terminal point of tunnel.

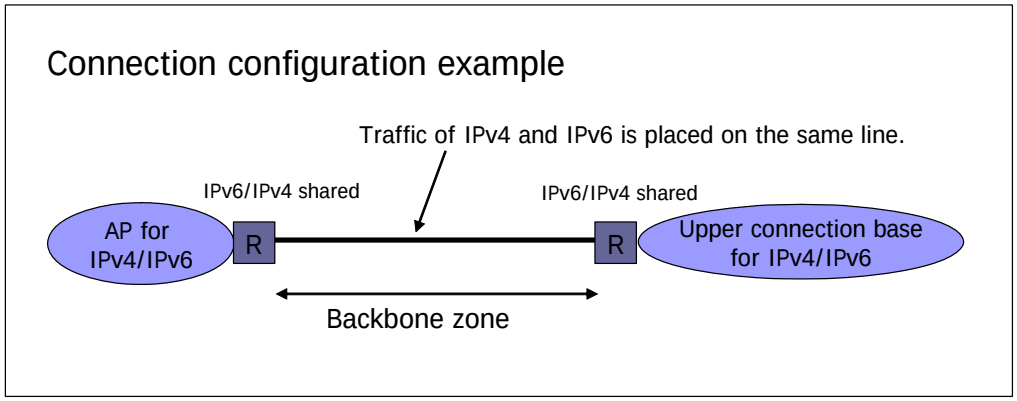
Shared line (L2 separation) type

In this type, existing service of IPv4 and IPv6 service are separated logically using technology of Layer 2, and in the case of Ethernet, VLAN is used and VP/VC is used for ATM. The advantage of this type is that it is possible to keep the line cost at low level by sharing backbone line with IPv4 service and IPv6 service.



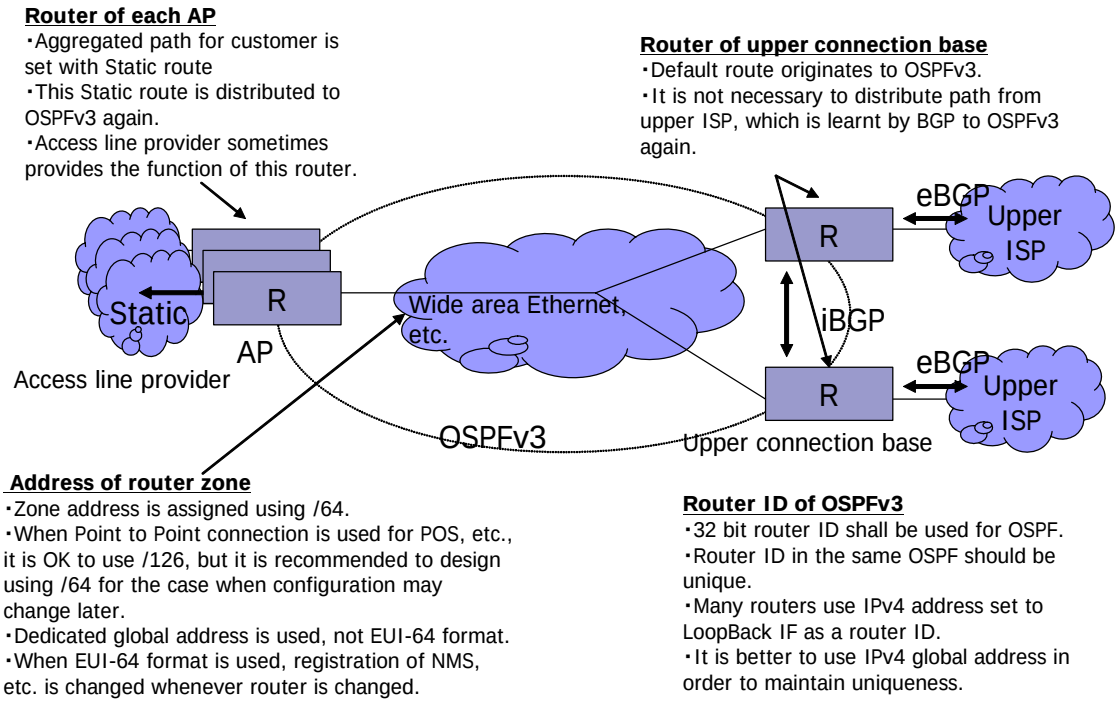
Dual type

IPv4 service and IPv6 service are provided in an integrated manner. Backbone line can be shared, therefore line cost can be kept at a low level. Moreover the router is shared as well, so this is the method with the highest cost merit. The influence on the IPv4 service is a concern, but some major ISPs have already started to use this configuration. However, in the case of middle/small sized ISPs, a router doesn't always exist at the access point, so it is impossible to form this configuration in some cases.



Configuration example of backbone

Backbone of middle/small sized ISP can be configured into the form shown in Fig.



2.2 Deployment of Access Network

Outline

Addressing of access network is basically the same as IPv4, but it is necessary to investigate about the dedicated Prefix distribution method.

Routing is the same as IPv4 as a basic rule.

Network configuration is the same as IPv4 as a basic rule, but Site type configuration is recommended. However, in the case that usage outside of the company is assumed (wireless LAN, mobile), Host type is recommended.

In order to support IPv6, it is necessary to promote configuration equipment to support IPv6/IPv4 dual stack. ADSL/FTTH and wireless LAN are used for this.

If dual stack supporting state of equipment is not promoted, connection is made using tunnel. For instance, CATV and mobile (tunnel access).

Access network

As access line of IPv6 service provided by middle/small sized ISP, ADSL or FTTH is assumed. Middle/small sized ISPs generally purchase this service from access line providers and provide the service, and this general case is used as a target in this document as well.

Contents

Contents described with regard to deployment of access network are shown below.

Common items

Network

- Connection model with a customer
- Connection model with ISP

Addressing, routing

- Address design
- Routing design
- Discussion related to dedicated Prefix distribution

Individual items

"Requirement of each equipment" and "Connection method" are described for each access network form of ADSL/FTTH, CATV, wireless LAN, mobile and tunnel access.

Common Items

Outline

Network

There are 2 types of connection with customer; Site type and Host type. It is desirable to use Site type from the viewpoint of assuring the security of the network inside customer's home.

With regard to ISP connection, there are 3 types; P2P, PTA and LAA. It is recommended to use the same method as that for IPv4.

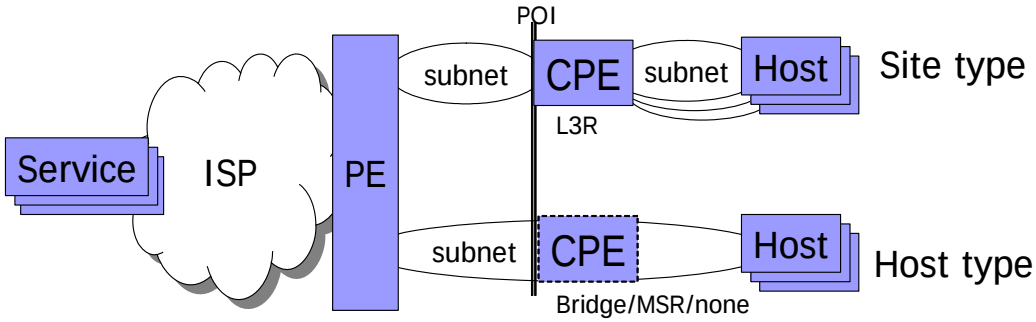
Addressing, routing

These are the same as IPv4 as a basic rule. It is necessary to consider when assigning dedicated Prefix.

Network

Connection model between IPv6 customer and access network

The Fig. shown below is a model to make a connection from access network to end user using Site or Host type.



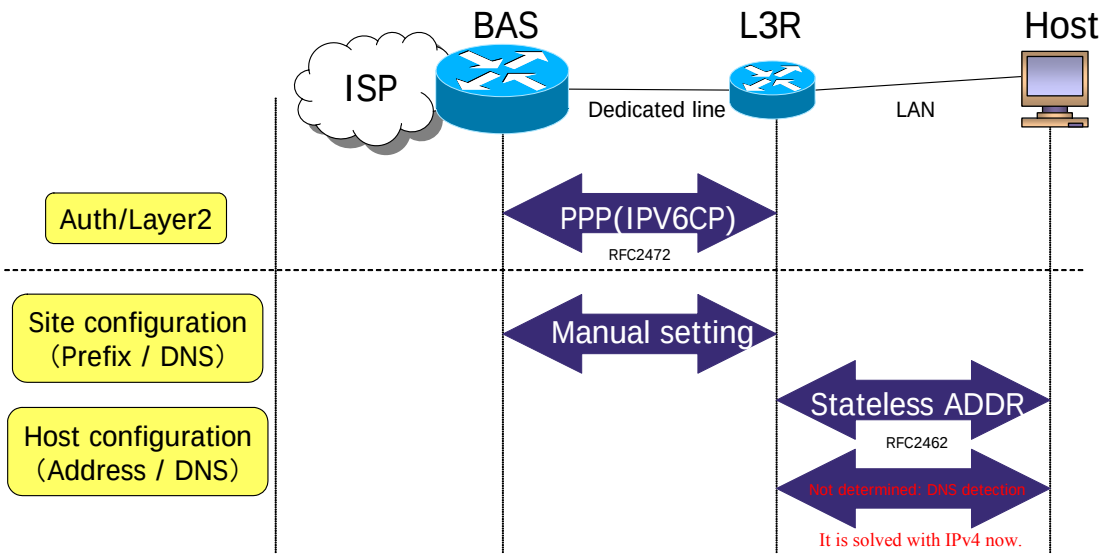
	CPE type	Prefix	Example
Site type	L3R(Router)	/48,/64	Dedicated line for enterprise type service, ADSL/FTTH service
Host type	L2 Bridge/MSR/none	/64	Dial up connection type service, 3G mobile data service, ADSL/FTTH service (limited to /64), Hotspot

MSR=Multi-link Subnet Router

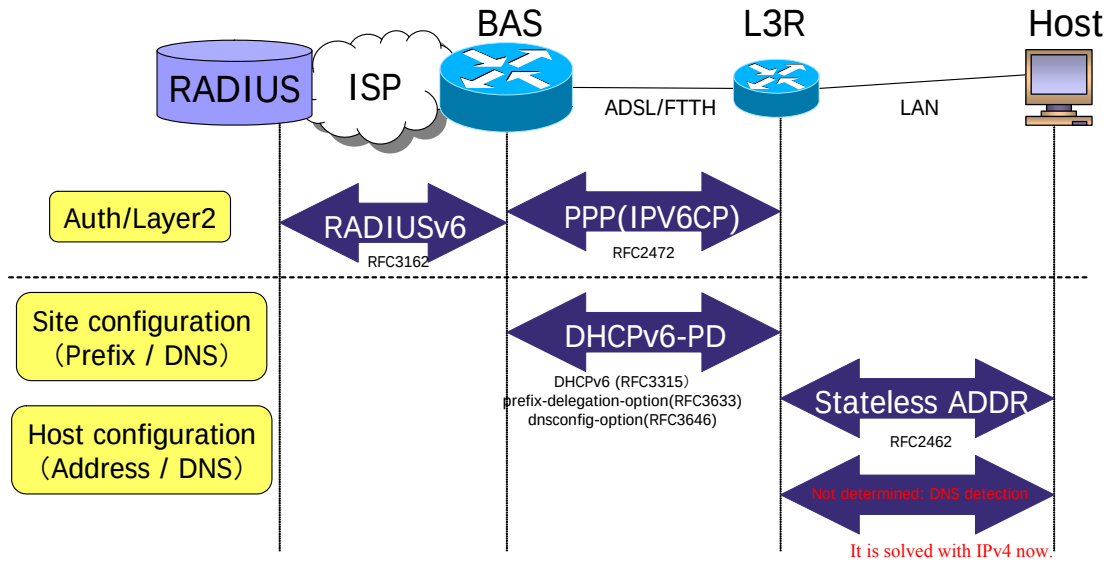
Configuration of Site type

2 forms are considered as Site type. The difference between these forms is whether the base of the user is configured manually or by using DHCPv6.

Site type No.1

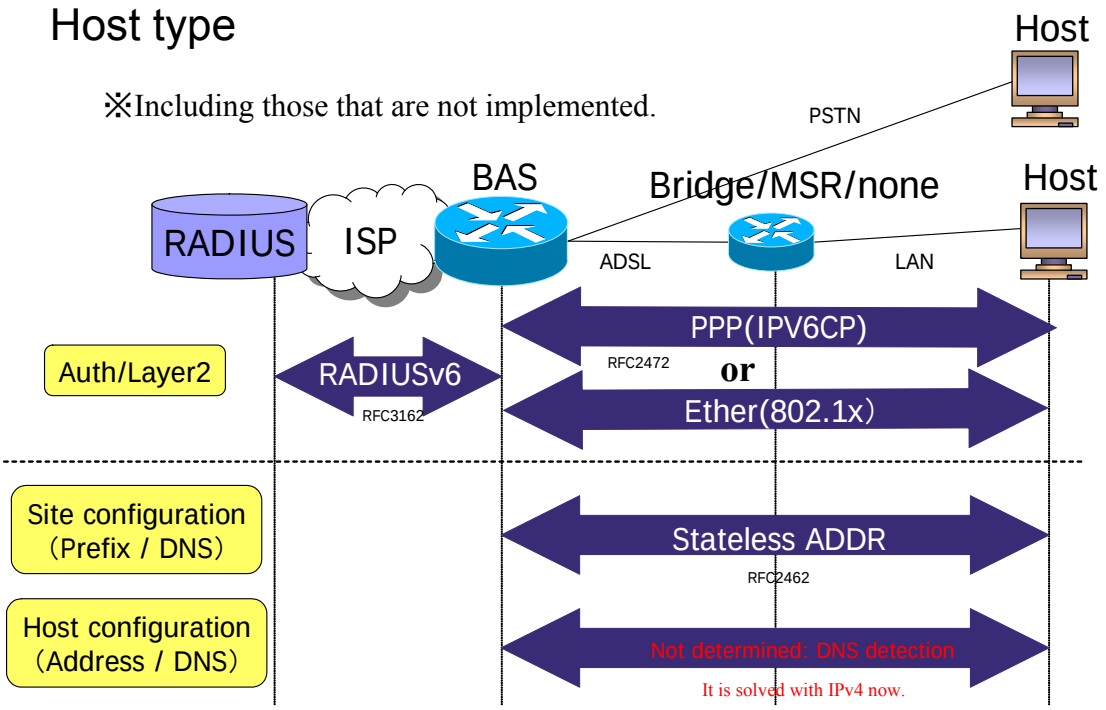


Site type No.2



Host type

The Fig. below shows the configuration of Host type.



Connection model between IPv6 access network and ISP

Connection between access network and ISP network is classified into the 3 broad categories shown below according to the connection method of customer traffic.

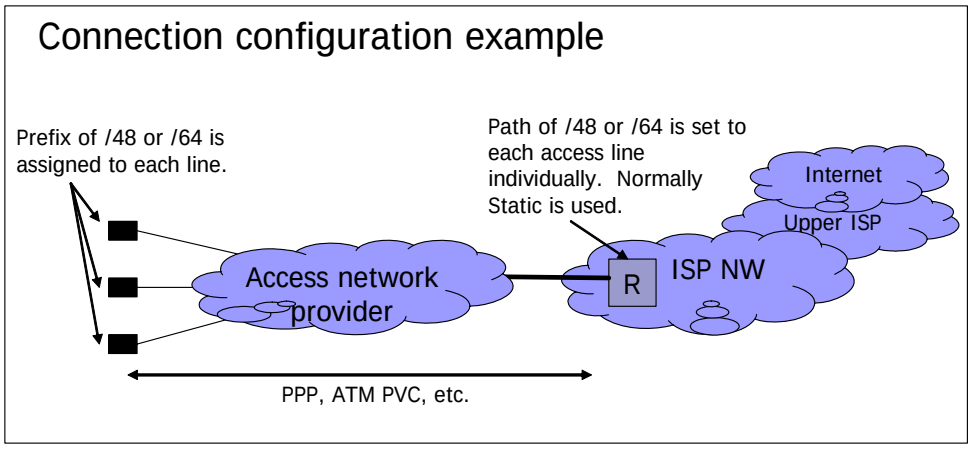
- Point-to-Point (P2P) type
- PPP Termination Aggregation (PTA) type
- L2TP Access Aggregation (LAA) type

It's better to use the same connection method for both IPv6 and IPv4 in order to reduce load of operation method for each protocol, but in some cases it is the only choice to use different type for IPv6 and IPv4 depending on the development policy of access network provider (and ISP).

Generally ISP network provides user authentication and network connectivity, but in some cases authentication and connectivity are separated and network connectivity is outsourced to another provider.

Point-to-Point connection type

In this case, access network is used as Layer 2 network for a stack of IP packets. Each line (PPP, ATM PVC, etc.) is terminated directly by ISP. Inside access network is configured with Layer 2, therefore it is not necessary to do routing in IP layer.

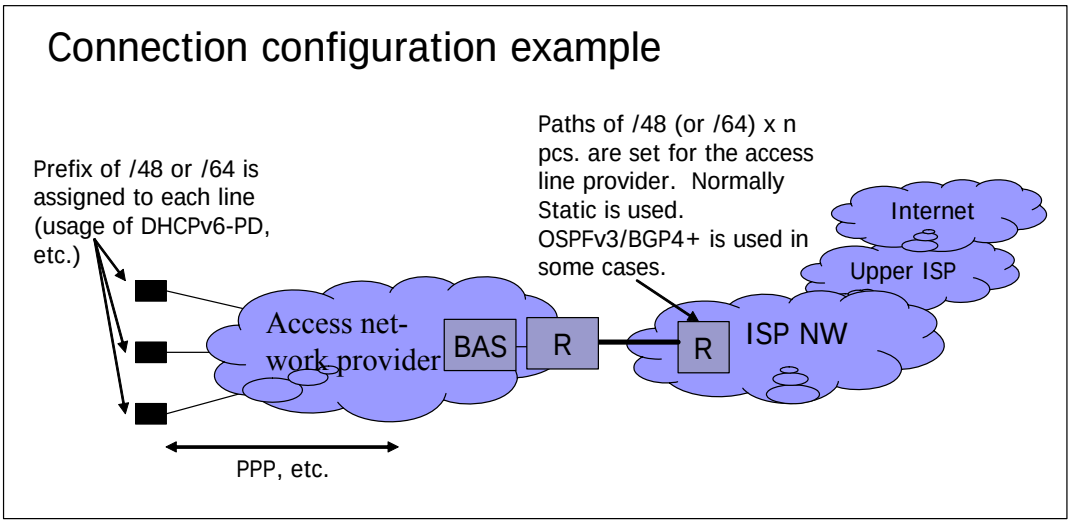


PPP Termination Aggregation type

In this case, each line (PPP, etc.) is terminated in the access network, and IPv6 and IPv4 packets are handed over to ISP. L2TP configuration is formed within access network taking into account scalability, etc.

Routing should be made between equipment that terminates PPP (BAS in general) in access network and ISP network. When L2TP configuration is formed within the access network, routing of L2TP packet is necessary as well.

This is the usage form generally used at present.

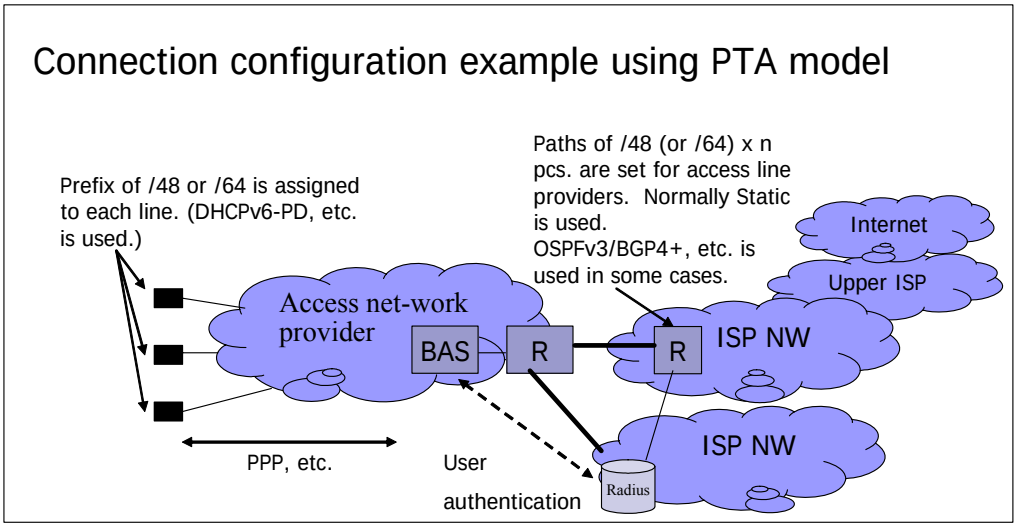


L2TP Access Aggregation type

This method encapsulates each access line (PPP, etc.) to L2TP and hands it over to ISP. PPP terminates at ISP. IPv4 transport is sufficient for L2TP and it is not necessary to form routing of customer traffic in access network. However, routing is necessary for L2TP packet.

Outsourcing form of network connection

It is possible for ISP to carry out only authentication of customers by RADIUS and to outsource IPv6 and IPv4 connectivity of a customer to another ISP (or access provider). Even if the company doesn't have IPv6 connectivity, it is possible to start IPv6 service.



Connection configuration between IPv6 access network and ISP network

The following points are pointed out for physical connection method between access network and ISP under IPv6.

P2P type and LAA type

- The same as IPv4 as a basic rule because it doesn't depend on protocol of customer traffic
- In the case of LAA type, connection is made with IPv4 L2TP for both IPv6/IPv4 packets of customer.

PTA type

- Consideration is required because IPv6 packet is exchanged directly.
- Native, Dual and Tunnel are the divisions of Layer3 type connection method.
- Single home connection and multihome connection are the divisions of Layer 2 type connection method.

Notes for each connection are the same as those for connection between ISP core network and upper ISP.

Configuration of network in access provider

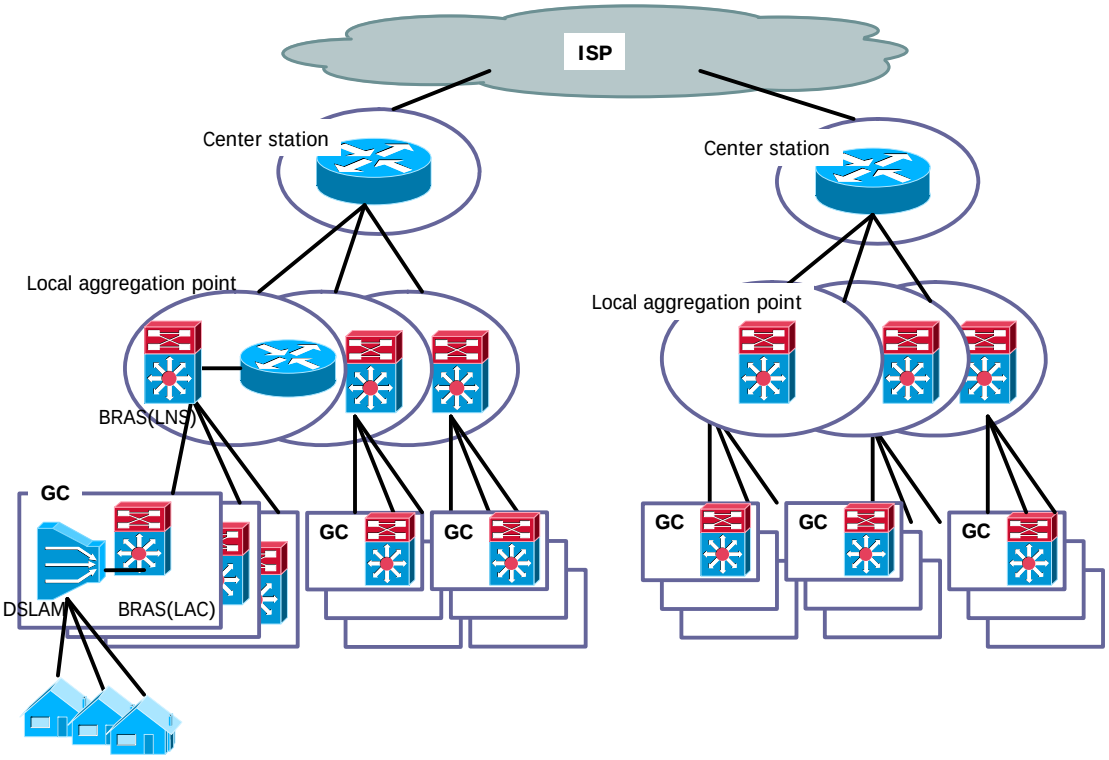
Network configuration inside the access provider is the same as IPv4 as a basic rule.

Features of the network of broadband providers (regular wholesale type ADSL providers) are that subscribers are aggregated for each area and PPP termination is made with BRAS (LAC/LNS), and that after PPP termination, mutual connection is made with ISP at the center station using IP routing.

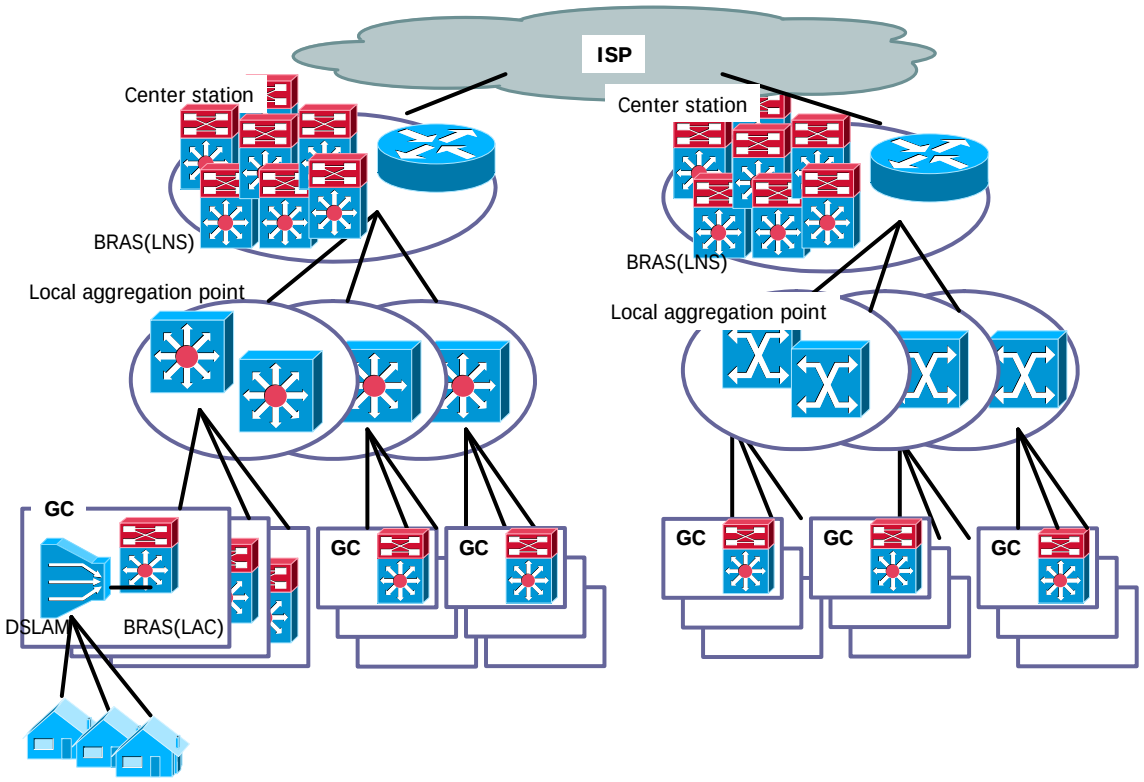
The following 2 configurations are used for the network from PPP termination point to the center station that has ISP mutual connection point.

- NW configuration in which PPP terminates at multiple bases throughout the country and IP routing is carried out to the center station → multiple LNSs are set throughout the country.
- NW configuration in which PPP terminates intensively at the center station and mutual connection is made with ISP within the station → LNS is set only at the center station.

Network configuration in which multiple LNS s are set throughout the country



Network configuration in which LNS is set only at the center station



Addressing, Routing

Address design

In this section, the design of address used for customers and for the infrastructure of the provider, and design of address for access network providers and ISP providers are discussed.

Definition of distribution method of address for a customer

Three kinds of distribution method of address for a customer are considered; Variable, Dedicated and Completely dedicated methods.

Variable

IPv6 Prefix is pooled at BAS, etc. and address is discharged from a pool for each connection, and it is possible that Prefix is changed for each connection.

Dedicated

This is a method in which connection is made using the same Prefix every time, however, the Prefix is changed when the connection location is changed.

Completely dedicated

Same Prefix can be used anywhere you go.

Distribution method of address for a customer

We recommend using “Dedicated” Prefix distribution as BCP with regard to distribution of address for a customer.

Under the present access service, “Dedicated” method is commonly used and “Completely dedicated” is not common.

There will be “Variable” Prefix distribution in the future, however, it is necessary to examine and discuss provision cost by provider, ASP service and users’ needs for “Variable” Prefix distribution.

Address design in access network

Address design in access network is the same as IPv4 as a basic rule.

Address for a customer

Connection address is provided by ISP. Prefix bundle is handed over from ISP for each connection line, and IPv6 address is provided by distribution Prefix and RA.

One point for consideration in network configuration is that Prefix can be aggregated by LNS of center station in the network configuration in which LNS is set only at the center station. In the network configuration in which multiple LNSs are set throughout the country, it is possible to aggregate Prefix for each regional base. When carrying out dedicated Prefix distribution service, it is necessary for ISP to understand what size the Prefix bundle from ISP is divided into.

Address for infrastructure of provider

Address for infrastructure of entrepreneur shall comply with ISP backbone. In a network that deals with IPv6 packets, it is necessary to assign IPv6/IPv4 addresses (network between BRAS ~ IPS connection routers, etc.).

Address design viewed from ISP network

Address design viewed form ISP network is basically the same as for IPv4.

Address for a customer

Necessary amount of Prefix pool for each connection shall be given.

One point of consideration when a dedicated Prefix is provided is that it is necessary to design Prefixes taking into account the network configuration the access provider. Prefix aggregation for each LNS is basic, and it is required to plan Prefixes considering the setting location of LNS.

Address for infrastructure of provider

Refer to the item on Address of Backbone for this item.

Routing between IPv6 access network and ISP network

The basic idea is the same as the connection between ISP core network and upper ISP network. From the ISP network, an access network looks like a customer, and from the access network, the ISP network looks like an upper ISP network.

It is assumed that paths are aggregated for each connection in order to control paths (when Prefixes are pooled to BAS through dynamic Prefix distribution). If there is a path that can not be aggregated, it is necessary to consider dynamic routing, etc.

In the case of a single home, Static routing is used for connection. When connecting with multiple links, it becomes necessary to consider automatic switching at trouble, redundancy and distribution of load.

In the case of multihome, dynamic routing is necessary. Care for multiple links is handled with dynamic routing + α .

ADSL/FTTH

Recommended deployment method

An outline of the recommended deployment method is for IPv6 to be supported for CPE inside the home of the customer and BAS (LNS BAS) of access network provider. Connection shall be by IPv6/IPv4 Dual Stack, and traffic of customer shall be terminated at the same BAS for both IPv4 and IPv6.

Site type is common for a connection method with a customer. When using Host type, it is necessary to consider packet filtering of IPv6 communication, etc.

Requirements of each equipment

・ Requirements for BAS to support IPv6

BAS is short for Broadband Access Server and BRAS is Broadband Remote Access Server.

This equipment aggregates lines of broadband connection. In general, PPP is terminated. According to the function, it is divided into LNS (L2TP Network Server) and LAC (L2TP Access Concentrator).

Requirements for LNS BAS to support IPv6 are as shown below.

L2 layer
PPPoE/oA shall be terminated.
L2TP should be supported (LNS function when handling IPv6).
PPP IPv6NCP (IPV6CP) should be supported.

L3 layer
Supporting IPv6 addressing, routing
RA and DHCPv6-PD are sent to the PPP link connection destination.

Upper layer
Authentication
PPP authentication is the same as IPv4.
RADIUS IPv6 Attribute should be handled (IPv6 Prefix).
After IPv6 link (IPV6CP) is up, RA and DHCPv6-PD shall be sent to PPP link connection destination based on account and IPv6 Prefix information.
Requirements of BAS to support IPv6 (continued)

Requirements of LAC BAS to support IPv6 are as shown below.

L2 layer
PPPoE/oA shall be handled.
L2TP LAC function should be supported.
L2TP shall be set to appropriate LNS BAS for user account suffix (suffix information is set manually by LAC or function such as RADIUS shall be used).
Not necessary to support IPV6CP (because PPP is tunneled).

L3 layer
Not necessary to support IPv6 (because L3 layer data of user is not handled).

Upper layer
PPP authentication if necessary.
Linkage with RADIUS (as necessary)

BAS connection configuration

When (LNS) BAS supports IPv6, rest of BAS connection network can be configured in the same manner as for IPv4 as a basic rule (L2TP topology, etc.).
Routing is configured as shown below.
At upper ISP, static or dynamic routing is used. It depends on the network policy of the access provider. When connecting to an ISP directly, it is desirable to use routing that enhances redundancy. It is desirable to aggregate paths with BAS, but please refer to the section on Address design.
On the Host side, static routing is used for each CPE link (PPP, etc.).

Requirements of CPE to IPv6

With regard to the requirements for CPE to support IPv6, it should be considered for each model; Site type model, Host type model and Host type model (with additional functions).
Implementation of Path MTU Discovery for CPE should be considered as a point of notice. CPE is required to have a function to support multicast, and it is also necessary to consider authentication of connection.

■CPE of Site type model

• IPv6 packet transfer

IPv6 network shall be terminated and routed.

• Address assignment

Address shall be assigned to equipment within a home.

For network → CPE, DHCPv6 PD and RA are used.

CPE→home equipment generate RA from DHCPv6PD Prefix information. When /48 Prefix is notified, one arbitrary /64 shall be cut out with CPE, RA Prefix shall be generated and RA on network side shall be proxied (RA Proxy).

Address on network side of CPE is set by link local connection, RA, etc.

• Routing

Static default routing to the ISP network shall be carried out as routing. It shall be static routing (Connected) to Prefix on Home side, and dynamic routing on Home side is an option. Dynamic routing to ISP network is generally not carried out.

• Security

The same filtering as for IPv4 shall be carried out.

■CPE of Host type model

• IPv6 packet transfer

Only IPv6 packets shall be bridged (IPv4 functions as a router). However, this is not preferable from the viewpoint of connection of information home appliances. A router that supports RA Proxy is desirable (described later).

• Address assignment

RA shall be transferred from a network, so address is not assigned.

• Routing

There is no routing (passing through as it is).

• Security

Filtering is not performed.

■CPE of Host type model (with additional function)

This enhances function of CPE of Host type model. CPE shall be RA Proxy implementation router. Security shall be secured with CPE according to the requirements to support information home appliances.

• IPv6 packet transfer

IPv6 network shall be terminated (in a pseudo manner) and IPv6 routing shall be carried out. It is seen as the same network from the network side, and from the Home side it is seen as though it is segmented.

Address assignment

RA Proxy is performed in the order of network → terminal (and CPE).

Routing

Routing is the same as that of Site type.

Security

General filtering is carried out.

Path MTU Discovery (PMTUD) on CPE

IPv6 PMTUD is a function implemented for a device that handles IP (CPE, (LNS) BAS, etc. in the case of broadband network). PMTUD is not handled (can not be handled) in the lower layer.

In the network of broadband providers, configuration of PPPoE or L2TP is common, and the MTU size becomes smaller than the general size (1500 byte) on Ethernet due to overheads of PPP or L2TP header. MTU information is notified from network (BAS) to CPE with PPP, and MTU shall be set to CPE interface (LCP MRU option).

However, when notification of MTU information or setting of MTU size with CPE fails, difference occurs on handling of MTU between CPE and ADSL network. Packet is put through in the case of CPE and packet is rejected as oversize packet in the case of ADSL network. If it is rejected, MTU can not ever be learnt, so that packets can not be put through.

Therefore it is necessary to notify information of MTU size at negotiation of PPP. It is recommended to use MRU option and implement appropriate interface MTU size setting from MRU information.

Moreover, it is required to implement appropriately to handle ICMP Packet Too Big

Message. It is necessary not to filter the ICMP Message packet.

Moreover, in the case that the connection is not PPP connection, and MTU size changes in the lower layer on network side between CPE and IPv6 router, it is necessary to furnish a function to notify appropriate MTU size to CPE (appropriate implementation of general PMTUD is required).

Supporting of multicast by CPE

According to the network model, the following 2 types are considered.

- Model to aggregate with BAS (in the case of Site type or Host type PPP connection, etc.)
  Multicast packet is aggregated to the device (BAS) that terminates L3. Availability generally depends on performance of BAS.

- Flat model (in the case of Host type L2 connection, etc.)
  When setting VLAN, the same problem as above occurs. In the case of flat space, coexistence of PrivateVLAN and multicast is required, and handling method of multicast at ND will become a problem.

According to the device, it is possible to discriminate whether CPE needs to handle IPv6.

- When CPE handles IPv6
  CPE shall support MLD/IPv6 multicast routing and MLD proxy.

- When CPE doesn't /can't handle IPv6
  It is necessary to support MLD at the connection destination of L3 (BAS, etc.).

Connection authentication

Authentication shall be carried out with PPP LCP, etc. at connecting a link. Authentication is not carried out again when discharging the address.

- Site type
  With regard to authentication of communication between CPE and BAS, PPP authentication is common for user authentication and user specification. After PPP authentication, there is no authentication for a user. Authentication is not carried out again at discharging the address.

• Host type

Connection authentication between terminal and BAS is authenticated by attaching a string physically or by PPP authentication on a terminal.

Connection method

Site type (No.1)

This is IPv6 connection that is realized when provider router (including BAS) supports IPv6. This is not common for a service for individuals, but it can be used for SOHO connection, etc. Physical line is attached to a router that accommodates a customer, so it is easy to provide a service of dedicated address.

CPE - provider router shall be connected using some kind of earthen pipe type connection method such as PPPoA/PPPoE, (dedicated line, ATM).

Setting of IPv6 for CPE is generally carried out manually.

Ethernet connection (IPv6 over Ethernet) is generally used between CPE and terminal, and IPv6 auto address setting is used. The issue shall be the method for a terminal to detect IPv6 DNS Cache address (DNS address notification, etc.).

With regard to authentication, a user is specified when dedicated setting of line, etc. is used, so there is no sequence for authentication.

Site type (No.2)

This type realizes when (LNS) BAS supports IPv6. This is a common form for services for individuals.

Connection between BAS and CPE shall be made by PPP NCP (IPV6CP). The method to start IPCP and IPV6CP on the same LCP at the same time is common.

For distribution of Prefix, DHCPv6 Prefix Delegation Option is used. As for size, /64 and /48 are generally distributed. It is possible to notify DNS Cache address, etc. under the same scheme.

The CPE and terminal are generally connected by Ethernet (IPv6 over Ethernet). IPv6 auto address setting is used. The issue is the method for the terminal to detect IPv6 DNS Cache address (DNS address notification, etc.).

For authentication, PPP authentication (account setting with CPE) is carried out. The regular authentication is used between BAS and RADIUS. If a dedicated Prefix is necessary, IPv6 Prefix is required to support “Attribute”.

With regard to (LNS) BAS supporting IPv6, in the case of L2TP form, LAC BAS doesn’t

have to support IPv6.

Accounts are used for connection authentication in the same way as in IPv4. Separate accounts should be used for IPv4 service and IPv6 (or Dual Stack) service. That is to say, BAS accommodation supporting IPv6 and BAS accommodation supporting IPv4 shall be separated by Suffix.

Host type L2 connection

• Between BAS and CPE

In this case, between BAS and CPE on network side looks like the same Ethernet segment when viewing from terminal side.

Address shall be assigned by sending RA from BAS, but the assignment method varies according to the segment form between BAS and CPE.

When BAS and CPE is LAN of one segment, RA shares one. With this method, the terminal accommodated in the same BAS is able to communicate directly, however, this method usually causes many nonconformities. Some kind of countermeasure (PrivateVLAN, etc.) is required.

When there are different segments for each user between BAS and CPE, VLAN or so on shall be set between BAS and CPE. RA shall be separated for each user. Communication between the terminals accommodated in the same BAS should always made via BAS.

• Between CPE and terminal

Generally speaking, Ethernet connection (IPv6 over Ethernet) is used between CPE and terminal. IPv6 auto address setting is used, however, the issue will be the method to detect IPv6 DNS Cache address (DNS address notification, etc.) on the terminal.

There are 2 forms; the form in which all Ethernet frames are bridged by CPE and the other one in which only Ethernet frame of IPv6 packet is bridged. In the latter case, IPv4 packet is terminated by a modem.

When viewing from the terminal side, the network side looks like the same segment of Ethernet.

• Authentication mechanism with L2 connection model

There is no authentication for address assignment, and it depends on connection authentication in lower layer. If there is no CPE, switch to accommodate a customer takes

the role of CPE such as termination of VLAN. There is no authentication in particular, so if it is necessary, L2 shall be authenticated between CPE and network. Line and Prefix shall be connected with a string.

Host type PPPoE connection

• Between BAS and CPE

In this case connection is made by PPP NCP (IPV6CP). The method to start IPCP and IPV6CP on the same LCP is generally used. User authentication is performed when connecting PPP.

RA is used for Prefix distribution, and /64 is distributed to each user. Communication between terminals accommodated in the same BAS should always go through BAS.

It doesn't depend on the segment form between BAS and CPE.

• Between CPE and terminal

Between CPE and terminal is generally connected with Ethernet (IPv6 over Ethernet). There are 2 forms; the form in which all Ethernet frames are bridged by CPE and the other one in which only Ethernet frame of IPv6 packet is bridged. In the latter case, IPv4 packet is terminated by a modem.

When viewing from the terminal side, network side looks like the same segment of Ethernet. IPv6 auto address setting is carried out by RA from BAS.

The method to detect IPv6 DNS Cache address (DNS address notification, etc.) on the terminal shall be the issue.

With regard to the case where there is no CPE, between BAS and terminal is connected directly with PPP regarding L2, therefore it doesn't depend on the presence of CPE.

• Authentication

At PPP authentication, account setting is performed on a terminal.

Regular authentication is used between BAS and RADIUS. If dedicated Prefix is necessary, it is required for IPv6 Prefix to support Attribute.

Problems in Home network

Multi prefix in Home

There are 2 kinds of multi prefix used inside the home; multi prefix between ISPs and multi prefix within ISP.

Multi prefix between ISPs is the multihome for different upper ISPs. It is relatively easy to use when the number of connections with ISP (CPE) is just one, however, if the number of ISP connections (CPE) becomes multiple, it is necessary to have a mechanism to select the appropriate exit.

As investigation matters, it becomes necessary to check whether there is a demand from SOHO, etc., and the relationship with address filtering. It is also necessary to pay attention to trends in standardization of multihome (IETF multi6 WG).

Multi prefix within an ISP is assumed to be used as the method to segregate services in the same ISP (Internet connection, VoIP, broadcasting type streaming and connection with information household appliances).

It is possible to change the requirements of a network such as the presence of external connection, presence of dedicated address and presence of QoS according to Prefix.

There are 2 ways of handing Prefixes; handing as multiple Prefixes or handing it as a batch of Prefixes and segregating them inside the network. In the latter case, it is necessary for the CPE to understand the meaning of a Prefix, however, the segregation method varies according to the service model, therefore it is considered difficult for a CPE to handle.

Technically, address selection/routing selection is a problem. Source address selection is considered as using RFC. Address selection can be carried out using name resolution, therefore it is necessary to consider the necessity for source routing technology.

It is also required to consider whether it is possible for information household appliances to handle multi prefixes.

Prefix management and policy at Home

With regard to management of prefixes used inside the home, the investigation issue shall be how to handle prefix notifications made from a network. Which means, whether prefixes are received as a large bundle (/48) and divided inside the home or whether a multiple number of /64 is received. In either way, it becomes necessary for CPE to handle multi prefixes.

The other issue about usage of prefixes is whether they should be divided into subnets for each usage purpose. If the usage purposes overlap, it becomes meaningful to discharge multiple prefixes to the same link.

Mutlilink inside Home

Another investigation issue is dynamic routing support inside the Home. However, this becomes an issue when Home becomes multilink. Therefore, first of all it is necessary to consider the possibility that Home becomes multilink and ISP supports it. The standpoint of ISP and standpoint of user lie within this problem.

From the standpoint of the ISP, it is difficult for the ISP to control more than two links inside the Home, therefore ISP shall distribute multi prefixes and ask Home to divide and use them under Home's responsibility.

From the standpoint of the user, in the case of the general user in particular, if it is a service, they require support as a matter of course. Therefore the focus point shall be whether the ISP is required to have a system that supports multilink.

In such cases, it is requested to link up information between each router (for distribution of addresses in particular), and in this very case MSR (Multilink Subnet Router) is required.

Function required for CPE that supports information household appliances

Supplementing the functions related to networks, which are missing from information household appliances is one of the important issues to be solved in the future.

We can not expect that the function of information household appliances as a network device will improve dramatically at least for a while. Secure communication and name resolution methods are included in these functions. Therefore, it is expected for the network to supplement these functions.

If so, CPE that exists inside the home as a network device becomes a key device. It is required to realize secure communication between external terminal and household network (CPE) and to implement the method to support name resolution of information household appliances (DDNS/SIP, etc.).

Security realized by CPE

Security functions with the CPE is required to realize include packet filtering and coping with secure communication.

Packet filtering that is the same function as IPv4 has already been handled by BCP. Therefore, the point is whether there is a function required as a unique function for IPv6. For instance, there is a possibility of linking up with information household appliances. It is considered to exchange information between information household appliances and CPE such as UPnP.

With regard to demand for secure communication, IPsec or SSL/TLS can be implemented to CPE.

In the case of IPsec, the infrastructure for exchanging keys becomes a problem. In the case of SSL/TLS, the issuance of certificates to each CPE and installation become a problem.

For these problems, it is required to handle in an ASP manner.

CATV

Recommended deployment method

As an outline for CATV, it is recommended to use the form of tunnel connection between routers at home and center under the present circumstances. In this model, Dual Stack (tunnel) router is installed inside the home and a Tunnel termination router is installed at the center.

Site type is generally used as the customer connection method. Standardization of CATV Internet to support IPv6 is currently promoted.

IPv6 deployment model of CATV Internet

With regard to CATV Internet support for IPv6, DOCSIS is currently investigated for use in supporting IPv6, and at present there are only a few CATV Internet facilities that support IPv6.

The issues for CATV networks to support IPv6 are the problem of ND action on CM or Bridged CMTS (handling of multicast, ND Proxy) and Classification of IPv6 traffic (IPv6 is all handled by BestEffort, therefore it is impossible to carry out preferential control of IPv6

phone packet, etc.).

Under the above mentioned restrictions, many CATVs currently provide IPv6 using Tunnel. It is expected that DOCSIS will support IPv6 as soon as possible.

As deployment models, the following two cases are considered;

- Bridged CMTS
- Routed CMTS

In both models, CM and CMTS have some L3 functions according to the management purpose.

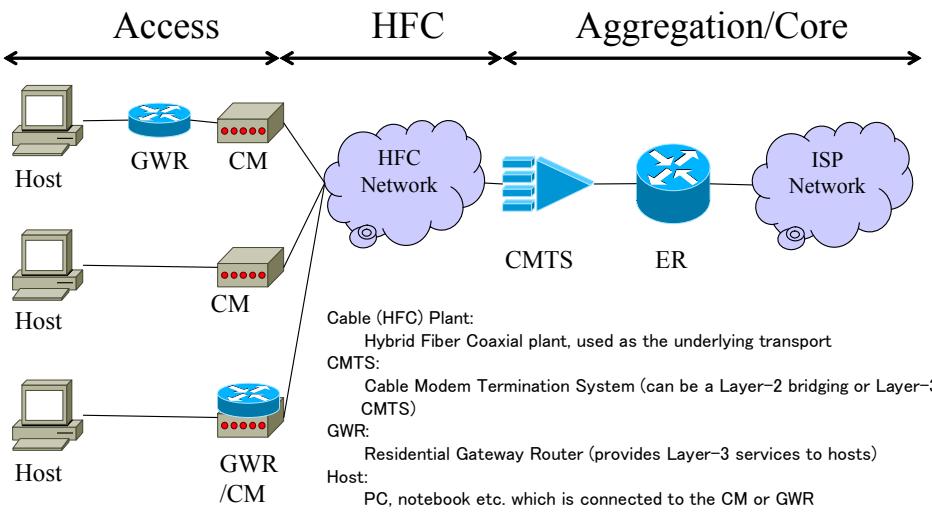
Requirements for each equipment

The following are the configuration factors for CATV Internet.

- Edge Router (ER)
- CMTS (Cable Modem Termination System)
- CM (Cable Modem)
- GWR (Residential GateWay Router)

Factors that affect deployment to IPv6 can be illustrated as shown in the Fig. below.

Influential cable network factors



Cable (HFC) Plant:
Hybrid Fiber Coaxial plant, used as the underlying transport
CMTS:
Cable Modem Termination System (can be a Layer-2 bridging or Layer-3 routing CMTS)
GWR:
Residential Gateway Router (provides Layer-3 services to hosts)
Host:
PC, notebook etc. which is connected to the CM or GWR
CM:
Cable Modem
ER:
Edge Router
Data Over Cable Service Interface Specification (DOCSIS):
The standards defining how data should be carried over cable networks.

50

Connection method

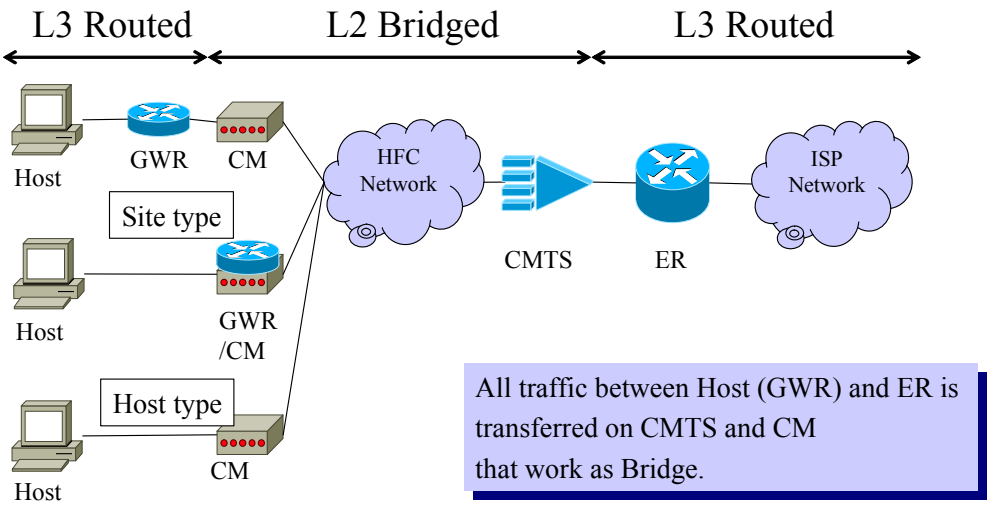
In the following, the requirements for each equipment are described with regard to the connection method shown below.

- Bridged CMTS
  - Site type
  - Host type
- Routed CMTS
  - Site type
  - Host type

A CATV Internet network is generally a unified network of access network and ISP network as it is called in this document, however, in this section, connection between customer and access network is discussed. Please refer to the item on upper connection of ISP for the connection with upper ISP.

Supporting IPv6 under Bridged CMTS

Model



Supporting IPv6 under Bridged CMTS (Site type)

・Infrastructure

For infrastructure, Host, GWR (GWR/CM) and ER are required to support IPv6 routing. CM and CMTS don't need to support IPv6 routing, but they need a bridge for IPv6 Packet. Please refer to the item on Data Transfer for this issue. Moreover, IPv6 Unicast/Multicast packet needs to be transferred between this Bridge division (CMTS-CM).

・Addressing

With regard to addressing, IPv4 address is assigned to CM by DHCPv4 for the purpose of management. With regard to Host, /64 or over (/48 in general) shall be assigned to GWR by DHCP-PD. In the case of discharging a dedicated address, MAC address authentication of DHCPv6-PD is available.

・Data Transfer

Under CMTS, IPv6 packet is bridged. In the case of CMTS, it is necessary to transfer ND packet or implement ND Proxy. Communication between different sites depends on whether CMTS and CM transfer Multicast IPv6 ND properly. For ND, Link Local Multicast is used. Whichever is used, it is necessary to support IPv6 Link Local Multicast.

For CM, IPv6 packet shall be bridged as well. Host under different CMs should have communication through CMTS. For CM, it is required to transfer ND packet or implement ND Proxy as well. When using IPv6 Multicast application across DOCSIS Cable Network, CMTS and CM need to support Snooping of IGMPv3/MLDv2.

・Routing

With regard to routing, default routing shall be set at ER statically on Host side. On ER side, static routing setting is carried out for Host. When using DHCP-PD, Static route for Prefix transferred to Host is defined.

For control of path to upper, IGP shall be used. It is desirable to aggregate Host paths for upper, and ER shall handle iBGP according to upper path control.

Supporting IPv6 under Bridged CMTS (Host type)

・Infrastructure

Host and ER need to support IPv6 routing. On the other hand, CM/CMTS don't need to support IPv6 routing, but IPv6 Packet Bridging is required. Please refer to the item on Data Transfer for this issue. IPv6 Unicast/Multicast packet need to be transferred between this Bridge division (CMTS-CM).

• Addressing

With regard to addressing, IPv4 address is assigned to CM by DHCPv4 for the purpose of management. For Host, /64 is assigned under CM by RA or DHCPv6. When discharging dedicated address, dedicated RA+dedicated terminal (dedicated MAC address) method and MAC address authentication of DHCPv6-PD are available.

• Data transfer

Under CMTS, IPv6 packet is bridged. It is necessary to transfer ND packet or implement ND Proxy. Communication between different sites depends on whether CMTS and CM transfer Multicast IPv6 ND properly. For ND, Link Local Multicast is used. Whichever is used, it is necessary to support IPv6 Link Local Multicast.

For CM, IPv6 packet shall be bridged as well. Hosts under different CMs should have communication through CMTS. For CM, it is required to transfer ND packet or implement ND Proxy as well. When using IPv6 Multicast application across DOCSIS Cable Network, CMTS and CM must support Snooping of IGMPv3/MLDv2.

• Routing

With regard to routing, default routing shall be set at ER statically on Host side. On ER side, static routing setting is carried out for Host. When using DHCP-PD, Static route for Prefix transferred to Host is defined.

For control of path to upper, IGP shall be used. It is desirable to aggregate Host paths for upper, and ER shall handle iBGP according to upper path control.

Common matters for Bridged CMTS

One common matter for Bridged CMTS is that it is possible to use the existing authentication method for connection authentication. DHCP authentication using MAC address of CM is normally used.

Supporting IPv6 by CM that uses Proxy ARP

For CM to carry out MAC address authentication of a terminal, Proxy ARP may possibly be used. Applicable cases are where CM acts as a bridge and carries out MAC address authentication. It is judged to put through a frame by looking at issued Mac address of Ethernet frame. CM uses Ethernet frame transmission, so CM receives a frame once and then sends it to the opposite interface again. When CM has Ethernet MAC address and it doesn't act as a router, Proxy ARP operation is carried out. It is possible to apply the same procedure to Bridged CMTS as well.

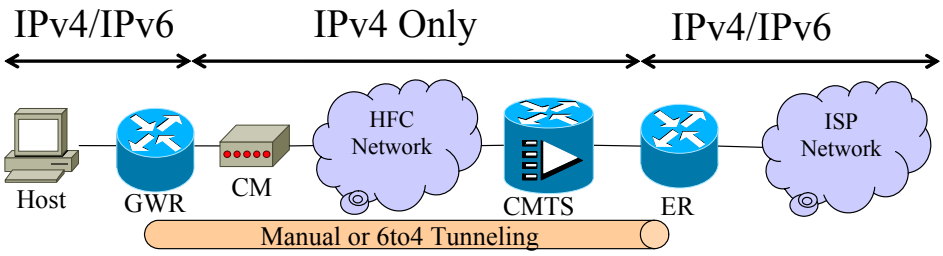
In this case, in order to support IPv6, CM receives an Ethernet frame that includes IPv6 packets from a terminal. It is received by CM once and then sent to a router again. MAC address of IPv6 packet addressed to a router needs to be translated to Ethernet MAC address of CM. Therefore, it is necessary to support IPv6 ND Proxy, etc.

Supporting IPv6 under Routed CMTS (Site type)

• Tunnel connection between GWR and Routed CMTS

For CM and CMTS, IPv4 device is used as it is and ER, Host and GWR must support Dual Stack.

Site type: Tunnel connection between GWR and Routed CMTS

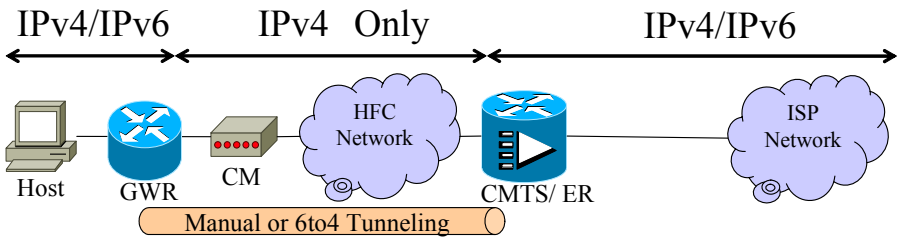


- IPv6 target equipment
  - Host, GWR, ER
- Addressing
  - Between GWR~ER
    - /64 RA form ER for a link
    - Prefix distribution by DHCPv6 PD
  - Between GWR ~ Host
    - RA
- Data transfer
  - Tunnel between GWR ~ ER
  - For CM and CMTS, it is sufficient to handle just IPv4.
- Routing
  - Host
    - Default setting with RA
  - GWR
    - RA or static default setting
    - Prefix routing on LAN side
  - ER
    - IGP, etc.
    - Aggregation of paths

• Tunnel connection between GWR and Routed CMTS/ER

CMTS and GWR support IPv6. CM doesn't need to go through IPv6. In order for CMTS and GWR to support IPv6, HW and SW will need to be upgraded.

Site type: Tunnel connection between GWR and Routed CMTS/ER

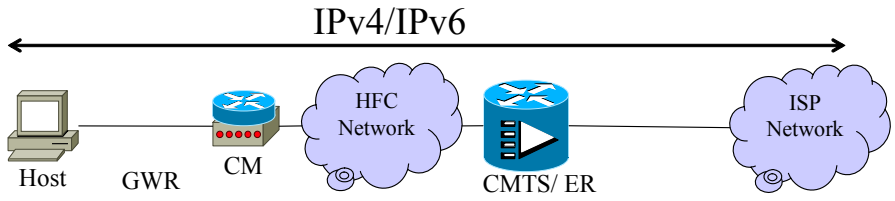


- IPv6 target equipment
  - Host, GWR, CMTS/ER
- Addressing
  - Between GWR ~ CMTS/ER
    - /64 RA from CMTS/R for a link
    - Prefix distribution by DHCPv6 PD
  - Between GWR and Host
    - RA
- Data transfer
  - Tunnel between GWR ~ ER
  - For CM, it is sufficient to handle just IPv4.
- Routing
  - Host
    - Default setting with RA
  - GWR
    - RA or static default setting
    - Prefix routing on LAN side
  - ER
    - IGP, etc.
    - Aggregation of paths

• GWR/CM ~ Routed CMTS/ER Native connection

GWR and CM support IPv6 as a unified type and CMTS supports IPv6 as well. Change of embedded CM/GWR and CMTS occurs, so it is difficult to deploy at present. It becomes necessary to change specification of DOCSIC to embedded CM/GWR as well.

Site type: GWR/CM ~ Routed CMTS/ER Native connection



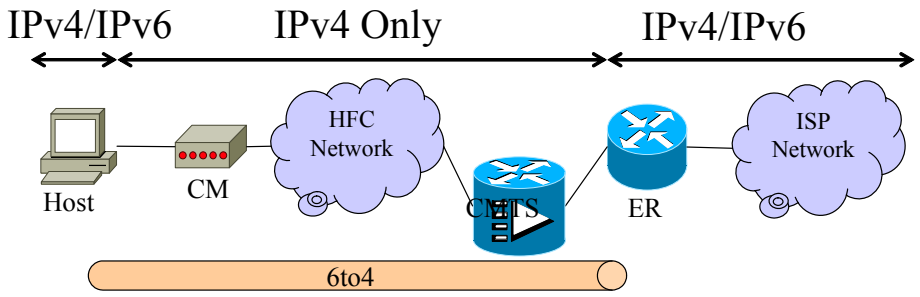
- IPv6 target equipment
  - Host, CM/GWR, CMTS/ER
- Addressing
  - Between CM/GWR~CMTS/ER
    - /64 RA from ER for a link
    - Prefix distribution with DHCPv6 PD
    - CMTS/ER is required to support DHCPv6 Relay.
  - Between CM/GWR ~ Host
    - RA
- Data transfer
  - IPv6 Native transfer
  - CM/CMTS carries out IPv6 routing, so ND or Multicast shall support as a router.
- Routing
  - Host
    - Default setting by RA
  - CM/GWR
    - RA or static default setting
    - Prefix routing on LAN side
  - CMTS/ER
    - IGP, etc.
    - Aggregation of paths

Supporting IPv6 under Routed CMTS (Host type)

• Tunnel connection between Host and ER

For CM and CMTS, IPv4 device is used as it is, and only ER and Host are changed to support Dual Stack.

Host type: Tunnel connection between Host and ER

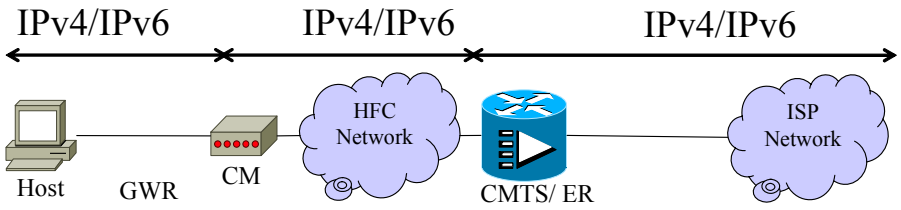


- IPv6 target equipment
  - Host, ER
- Addressing
  - Static or RA/DHCPv6
- Data transfer
  - Tunnel between Host ~ ER
  - For CM and CMTS, it is sufficient to handle only IPv4.
- Routing
  - Host
    - Static default setting
  - ER
    - IGP, etc.
    - Aggregation of paths

• Native connection between Host and CMTS/ER

CMTS shall support IPv6 and CM shall bridge IPv6 Unicast/Multicast. This indicates that DOCSIS supports IPv6, therefore it is not easy to do. For CMTS to support IPv6, hardware and software will need to be upgraded.

Host type: Native connection between Host and CMTS/ER



- IPv6 target equipment
  - Host, CMTS/ER
  - CM is IPv6 bridge
- Addressing
  - Between CMTS/ER ~ Host
    - RA
    - When distributing using DHCPv6, CMTS/ER is required to support DHCP Relay.
- Data transfer
  - IPv6 Native transfer
  - It is necessary for CM to implement ND (including RS/RA) Proxy, etc.
- Routing
  - Host
    - Default setting by RA
  - CMTS/ER
    - IGP, etc.
    - Aggregation of paths

Behavior of DHCP Relay in CMTS

With regard to handling of DHCP packet relay, MAC address of CM is assigned to DHCP Discover packet as an option and relayed. It is considered preferable to assign MAC address of CM to Unicast DHCP packet as well when re-releasing.

Common issues for Bridged/Routed CMTS

• IPv6 Multicast

CM and bridged CMTS must support IGMPv3/MLDv2 snooping. Implementation of present CM seems to have a problem with Multicast passing. Implementation to handle Multicast properly is required, and it becomes necessary to encourage DOCSIS to state the handling of IPv6 Multicast clearly.

• IPv6 QoS

At present, DOCSIS has not defined the streaming of IPv6. It becomes necessary to classify Unicast/Multicast traffic of IPv6 properly on DOCSIS network. For the items shown below, it is necessary to support IPv6 address of 128 bit.

- IP source address
- IP source mask
- IP destination address

• IP destination mask
• IP traffic class (DSCP)

The following 2 new classifications are also required for IPv6.
• IP version
• Flow label (optional)

• Security

Security is provided by BLP+ (Baseline Privacy Plus) within DOCSIS. Only the encrypted Multicast depends on the IP address. In order to support encrypted Multicast of IPv6, it is necessary to expand specification of DOCSIS properly.

Another method is to use IPsec, which is crucial for implementing to IPv6, however, the system of key distribution is an issue that must be investigated.

• Packet filtering

IPv6 packet filtering shall be carried out with CM or CMTS. It is possible to set filtering across layers (IP packet filtering with CM/CMTS that carries out bridge performance).

Packet filtering is normally carried out by CM. Types of packets to be filtered are File sharing (Windows/AppleTalk), Anti virus, Unintended (distributed intentionally to the network) RA or DHCPv6 response. The number of user terminals to be connected using MAC addresses is also limited according to DOCSIS regulation.

It is possible to carry out packet filtering using L3 equipment (GWR, Host, Routed CMTS, ER) that supports IPv6, but it becomes necessary to maintain consistency with CM (/CMTS) filter. Anonymous address is used on Host as necessary.

• Handling of internal attack, etc.

In the case of CMTS Bridged Model, Host of other customer accommodated in the same CMTS is accommodated as the same segment. Therefore, it becomes impossible to control packet on the network side, and it is not possible to protect from internal attack made by malicious users. In this case, filtering using CM (/CMTS) is effective.

It is possible to carry out packet filtering using L3 device that supports IPv6 (GWR, Host, Routed CMTS, ER). However, it becomes necessary to maintain consistency of CM (/CMTS) filter.

• IPv6 network control

DOCSIS, PacketCable and CableHome MIB have already considered supporting IPv6. The objects that identify IP version and InetAddressType are related to all SNMP objects. In this way, it becomes possible to observe the state of customer's CM through SNMP.

However, it doesn't always have to mean that SNMP protocol must support IPv6. It is possible for CATV providers to control it together with CM/SNMP manager server. It doesn't mean that IPv6 traffic of a customer is placed on it.

With regard to traffic for controlling CM, when DOCSIS supports operation, it is may possibly be controlled using different wave length from the user data (address assignment to CM by DHCP, tftp, SNMP, etc.).

• Provisioning

Setting of customer CM shall be updated remotely using tftp. This is regulated by DOCSIS. Setting shall be updated properly at starting IPv6 service using this procedure.

However, it isn't necessary for tftp protocol to support IPv6. It is possible for CATV providers to control both CM/tftp servers, and it doesn't mean that IPv6 traffic of a customer is placed on it.

Reference material

ISP IPv6 Deployment Scenarios in Broadband Access Networks
(Draft-asadullah-v6ops-bb-deployment-scenarios-00.txt)

5. Broadband Cable Networks

Wireless LAN

Recommended deployment method

The following is an outline of IPv6 deployment for wireless LAN.

For street box, existing wireless LAN equipment is used as it is. It is necessary to check handling of IPv6 packets of existing wireless LAN AP. With regard to connection with backbone, it is possible to point out that impact would be smaller on the existing network if IPv6 and IPv4 were constructed separately at Introduction.

Customer connection method is Host type when viewing from a customer.

Features of wireless LAN

Wireless LAN consists of street box and wireless LAN access system.

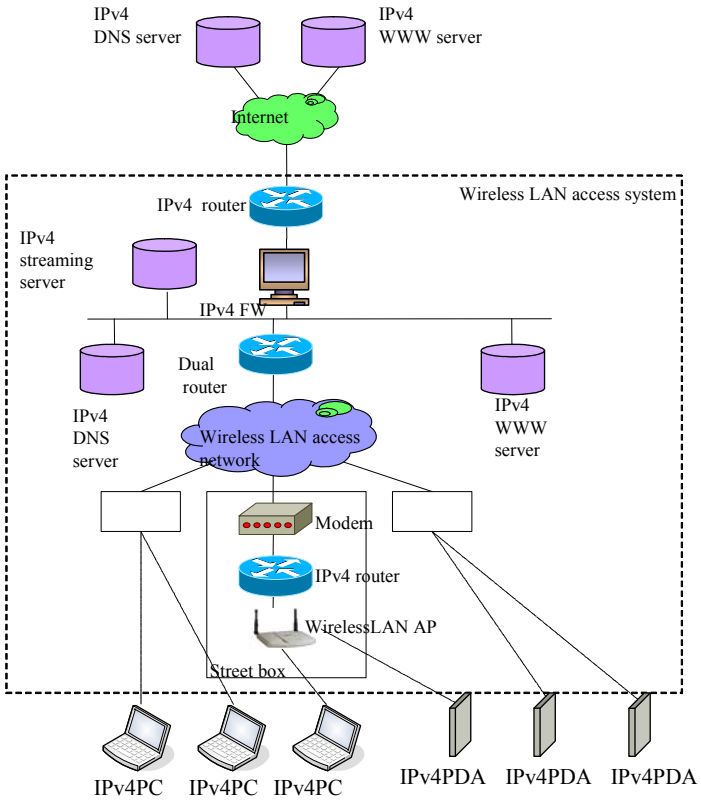
Street box consists of a modem (connected to wireless LAN access system using ADSL, etc.), router and wireless LAN access point.

On the other hand, wireless LAN access system consists of internal router (for

accommodating street box, etc.), external connection router and a group of servers (WWW server, DNS server, streaming server, firewall).

In the wireless LAN network that supports IPv4, general users connect to a wireless LAN access system that supports IPv4 using IPv4 terminal and service provider connects using IPv4 server.

Features of wireless LAN network



Requirements for each equipment

Street box

In the case of street box, existing modem is used as it is. Router is required to support IPv6. Existing wireless LAN access point is used as it is as well, but it is necessary to check the handling of IPv6 packet (discussed later).

Backbone

Deployment is made to a network that is able to handle IPv6. Deployment shall be carried out by separating IPv6 and IPv4 due to the reasons shown below.

• Firewall

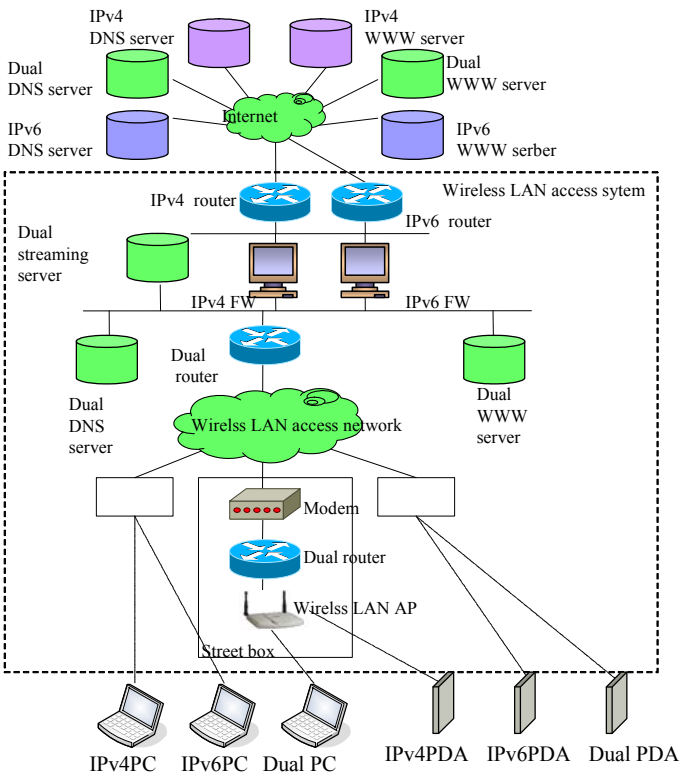
In an IPv4 network, it is difficult to distribute global address to all terminals and network address translation (NAT) is carried out, but in the case of an IPv6 network, it is possible to distribute all unique global addresses, therefore it is not necessary to translate addresses. In the case of an IPv4 network, the address for a terminal of a general user is masked by NAT equipment, therefore direct connectivity from the Internet can be shut off, but in the case of IPv6, connectivity from the Internet can be provided to all terminals, therefore, description of security policy including filtering may possibly become complicated. Therefore, in order to eliminate the influence of IPv4 service on the performance, separation shall be used.

• Router

Defects of upper connection router affect everything, so it should be separated from IPv4 router of the existing service, for which stable operation is crucial.

When the above mentioned issues are resolved, deployment is made to the network in which the same equipment/network supports IPv6 (Dual Stack).

Features of wireless LAN network - IPv6 introduction



Connection method (between terminal and backbone)

Outline

Site type connection is generally used. Information box is set at the wireless LAN Spot, and modem, router and access point are set inside the information box. Router shall support IPv6. This is the Layer2 segment based on the Ethernet frame, therefore generally there is no problem for IPv6 communication.

Distribution of address

For address distribution to each street box, IPv6 address auto setting (RS/RA) can be used as it is. Normally dedicated /64 Prefix is assigned as Site type connection of Ethernet 1 segment. Address on WAN side of street box shall be set statically or using RA from a center router.

Address is distributed to Host using dedicated Prefix + RA from a router inside each street box. Normally addresses are dedicated addresses inside the same AP, but it is allowable to use variable address using anonymous address. However, due to terminal implementation and setting dependence, it is difficult to force the use of dedicated/variable from wireless LAN provider.

Authentication at address distribution, countermeasure, etc.

With regard to MAC address filter authentication, it is not possible to carry out IPv6 communication before authentication terminates, and function of address auto setting based on IPv6 communication can not be used either before authentication terminates.

To authenticate RADIUS, it is necessary to support IPv6 Attribute. RADIUS transport itself is able to use IPv4.

Routing

The following is IPv6 routing after IPv6 connection is realized.

Default routing (RA/static) to a router is used for Host, and street box router is static. With regard to the router, static routing shall be used for IGP, and it is necessary to aggregate access point paths.

Connection method (between backbone and ISP)

There are 2 ways of connection to ISP; Native and Dual Stack.

Moreover, static routing and dynamic routing are considered for routing configuration, but dynamic routing is desirable in order to secure redundancy. BGP is used for IGP.

In the case of Tunnel, tunnel router is set and tunneling with ISP shall be carried out. Same routing as mentioned above is used, but it is also possible to create 2 tunnels and maintain redundancy using routing.

The following are the points that need to be confirmed.

Handling of IPv6 Ethernet frame

It is necessary to check whether wireless LAN access point and wireless LAN card put through IPv6 Ethernet frame (protocol No. 0x86DD). With regard to Unicast, if the equipment is certified for general Wi-Fi, there is no problem.

It is necessary to check the handling of IPv6 ND in particular. It is necessary to confirm support of IPv6 ND (Ethernet Multicast frame) or ND Proxy. This is very important particularly when MAC authentication is carried out at the access point.

When handling Multicast, it is necessary to check the handling of Multicast Ethernet frame. It is considered there will be an access point that puts through only Broadcast frame and not Multicast frame.

Countermeasure of a liar RA/DHCP

Increasing the priority degree of router RA is being considered as a countermeasure. Handling of DHCP is to be considered as an issue of IPv4.

Countermeasure of “liar” RA/MLD terminal in access point/segment is required

Increasing the priority degree of router RA is being considered for this case as well, however, it is not a perfect countermeasure.

Countermeasure for access points that use Proxy ARP

When MAC address authentication is carried out at the access point, Proxy ARP may possibly be used. It is possible that such access points are not able to support IPv6 ND. Countermeasures including ND Proxy are required, so it should be checked beforehand.

Countermeasure of access point that puts through Broadcast frame and doesn’t put through Multicast frame

In this case, it is probably not possible to use IPv6 ND, so it is necessary to check about putting through necessary Multicast frame beforehand.

Packet drop problem in the wireless zone

If ND or MLD packet is caught, it becomes a problem. It is pointed out in “Transmission of IPv6 Packets over 802.11/WLAN Networks (Draft-daniel-ipv6-over-wifi-01.txt)”.

With regard to the handling of DAD (Section 4.), it is said in this explanation that “Source

Address Based Packet Filtering At Layer2" is requisite for WLAN. Which means that filtering for cases where MAC address of own node becomes a source, filtering is carried out in an L2 manner at the access point.

The issue here is that it is not possible to receive a packet that has the same Link Local Address (=same MAC address) at DAD, so address overlaps.

As a resolution, it is difficult to omit Source Address Filtering, but it maybe possible to set all Source MAC addresses of DAD packet (NS/NA) as unspecified (All 0).

The following points are considered as investigation items.

Network security

It is possible to use the existing system as it is for the authentication to connect with wireless LAN network. This is because connection authentication is not carried out in IP protocol layer.

SSID

Only the wireless LAN terminal to which the same SSID is set, among IDs used to specify the access point of the connection destination can be connected.

IEEE802.1x authentication

Authentication and access control are carried out for each user connected on the wireless LAN through coordination between Radius server set on the center side and wireless access point, therefore, it becomes possible to ensure high security. Authentication using shared key beforehand such as WPA and authentication based on certificates can be used as an authentication method.

VLAN authentication

Connection is provided only to users who are authenticated on the wireless LAN access point to connect to VLAN, which permits access to specified servers and specified networks, therefore it becomes possible to provide a service to limited users.

Multicast

For multicast, the existing system can be used with MLD or multicast routing (PIM-SM, etc.).

However, it is necessary for the IPv6 router to support multicast. When wireless LAN segment uses ADSL provider's line in particular, it is likely that IPv6 facilities (normally BAS)

don’t support IPv6 multicast transmission. In such cases, some kind of measure is required such as connecting multicast packet to upper multicast network directly using IPv6 tunnel, etc.

It is desirable for L2 equipment attached to the wireless LAN segment to support MLD Snoop, etc.

Moving permeability in the wireless LAN network

When moving in the same wireless LAN segment, moving permeability is secured including address. However, connectivity is cut off temporarily at the point where it is not possible to supplement electric waves of wireless LAN. Therefore, countermeasures are required for re-authentication and time-out.

When moving between different wireless LAN networks, it is necessary to apply MobileIPv6. In this case, it is necessary to investigate the timing of re-authentication of connection, equipment status of supporting MobileIPv6 and the location to set HA .

Investigation issues in IPv6 distribution period

In the distribution period of IPv6, changing the infrastructure for provision of IP service to Dual Stack becomes an issue. Because in this period, integration of IPv4 facilities and IPv6 facilities is promoted.

Reference literature

ISP IPv6 Deployment Scenarios in Broadband Access Networks
(Draft-asadullah-v6ops-bb-deployment-scenarios-00.txt 8. Wireless LAN)

Transmission of IPv6 Packets over 802.11/WLAN Networks
(Draft-daniel-ipv6-over-wifi-01.txt)

Mobile

Recommended deployment method

Outline of mobile's support status of IPv6 is shown below.

First of all, connection is made by tunnel using PC to which a mobile data card is connected. PC with OS that supports IPv6 is used, however, it depends on support of OS and service style which tunnel methods (Configured / ISP Provisioned / Automatic Tunnel) are used.

Connection method of a customer is generally Host type. For IPv6 Native connection using mobile data card, facilities of mobile providers are required to support IPv6 connection. For IPv6 connection of a mobile phone terminal itself, the terminal is also required to support IPv6.

In this section, IPv6 deployment of mobile user is discussed, not the support of IPv6 by the mobile network itself. Which means that, with regard to network, the interface between terminal and mobile network and interface between mobile network and ISP are discussed. We are not discussing how to create the mobile network itself (excluding the part of interface).

The configuration of terminal is PC (Notebook PC) + mobile (card or mobile terminal), and OS of PC is used for IPv6 Stack. We are not discussing the supporting of IPv6 by the mobile terminal itself.

We recommend as Best Current Practice to investigate making a terminal (of PC, etc.) to which a mobile is connected support IPv6. Making a connection mobile terminal itself support IPv6 will be an issue in the IPv6 distribution period.

When a mobile network is used for connection, Host type connection is generally used.

As connection methods between terminal and mobile network, there are Tunnel connection and Native connection.

Features of segment

Equipment

The following equipment is used.

Terminal	PC + card for mobile connection
Network	PPP termination equipment
	IPv4 router
	Authentication system

Connection model

As connection model, PTA model and LAA model are considered.

- PTA (PPP Terminated Aggregation) model

  PPP (IPCP NCP) connection is used between terminal and mobile network, PPP is terminated with PPP termination device in the mobile network.

  Between mobile network and ISP is IPv4 connection.

- LAA (L2TP Access Aggregation) model

  PPP (IPCP NCP) connection is used between terminal and mobile network. PPP Packet is capsuled with L2TP in a mobile network.

  Between mobile network and ISP is IPv4 connection. PPP packet capsuled with L2TP is handed to ISP. PPP is terminated by PPP termination device in ISP.

Addressing

For addressing, one IPv4 address is discharged by PPP. Both dedicated and variable addresses are possible.

Address pool

Address is discharged from ISP using RADIUS, etc. Address pool is assigned in dedicated manner form ISP and discharged from a mobile network authentication facility.

Authentication

General PPP authentication is carried out. When discharging dedicated address, PPP authentication is used to specify a user as well.

Routing

For between terminal and mobile network, static default routing is used.

Dynamic routing is generally used inside a mobile network.

Between mobile network and ISP is static or dynamic routing.

Security

IP packet filtering is carried out using mobile connection card, etc. Filtering of file shared packet is checked using port No. of TCP/UDP. Check function across layers can also be used. It is possible to carry out IP packet filtering on a terminal.

Tunnel connection

Equipment

Network equipment is the equipment necessary for IPv4 connection and IPv6 tunnel termination router.

Connection model

IPv4 connection shall be PPP connection (same as the present state).

With regard to IPv6 connection, there are 2 models at the termination position of tunnel; mobile network tunnel termination model and ISP tunnel termination model.

• Mobile network tunnel termination model

It is required for (a part of) the mobile network to be capable of handling IPv6.

IPv6 tunnel is carried out between terminal and mobile network on terminal side. Mobile network prepares tunnel termination router and terminates a tunnel. When using IPv4 dedicated address, Configured Tunnel is used as a tunneling method, and when using IPv4 variable address, ISP Provisoned Tunnel or Automatic Tunnel is used.

The use of Dual Stack connection (same link for IPv6/IPv4), IPv6 Native connection (different link for IPv6/IPv4) or Tunnel connection between mobile network and ISP is considered.

• ISP tunnel termination model

This model is used when mobile network is not able to handle IPv6.

IPv6 tunnel is carried out between terminal and mobile network on terminal side. When using IPv4 dedicated address, Configured Tunnel is used and when using IPv4 variable address, ISP Provisioned Tunnel or Automatic Tunnel is used.

Between mobile network ~ ISP, regular IPv4 connection is used, and ISP shall prepare tunnel termination router and terminate tunnel.

Addressing

In the case of IPv4, one IPv4 address is discharged with PPP (IPCP NCP).

In the case of IPv6, address distribution depends on specification of tunnel.

6to4	/48
ISATAP, Teredo	/64+IPv4 address
Others	Arbitrary

In the case of IPv6, it becomes important to suppress unnecessary signaling (in order to use the wireless zone effectively).

Authentication

In the case of IPv4, regular PPP authentication is carried out.
n the case of IPv6, authentication is performed for ISP Provisioned Tunnel, but it is not normally performed for other tunnel.

Routing

Routing between terminal and mobile network depends on specification of tunnel. Normally static default routing is used for mobile network. Routing between mobile network and ISP is the same for both IPv6 and IPv4. Dynamic routing must support IPv6.

Security

With regard to security, IP packet filtering is carried out on a terminal.

Native connection

Equipment

The form of the equipment is the same in the network.

Connection model

IPv4 connection shall be PPP connection, which is the same as the present connection. Under IPv6 connection, the same method is used for IPv4 (PPP).
Under 3GPP specification, interface ID notified from mobile network side shall be used and controlled on network side so that overlap of interface ID can be avoided. With this procedure, it is assured that ID is unique in a link, therefore no DAD is performed (precisely speaking, DAD is ignored).

• PTA (PPP Terminated Aggregation) model
Between terminal and mobile network, PPP (IPV6CP NCP) connection is used.
In the mobile network, PPP is terminated by PPP termination device.

Between mobile network and ISP, Dual Stack connection (same link for IPv6/IPv4), IPv6 Native connection (different link for IPv6/IPv4) or Tunnel connection is used.

• LAA (L2TP Access Aggregation) model

Between terminal and mobile network, PPP (IPV6CP NCP) connection is used.
PPP packet is capsuled with L2TP in a mobile network.

Between mobile network and ISP, IPv4 connection is used, and PPP packet capsuled with L2TP is handed to ISP, and PPP is terminated by PPP termination device in ISP.

Addressing

For addressing, one IPv4 address is discharged by PPP (IPCP NCP).

With regard to IPv6, /64 Prefix is notified with RA. In this case sending timing of Unsolicited RA becomes a problem. It is necessary to control to prevent discharge of a large amount, therefore, sending intervals and optimization of Prefix survival period become issues of concern.

In the case of 3GPP specification, the problem is that it doesn't support multi prefix as of now. There is a regulation to use one address for one link.

We recommend the use of anonymous address (Privacy Extension), however, we don't recommend changing the address frequently. This is to avoid the problems caused in usage of SIP signaling, etc.

DHCPv6 can also be used. This can be used under normal usage method, and it is required to handle properly by using DHCP Proxy/Relay on network side.

Address pool shall be discharged with RA from a mobile network in a static (or dynamic) manner according to information of RADIUS, etc. of ISP. It is also possible to assign address pool on mobile network side in a dedicated manner and discharge it dynamically with RA.

Authentication

With regard to authentication, general PPP authentication is carried out. It is used to specify a user as well in the case that dedicated address is charged. PPP LCP authentication is carried out using the same system as IPv4.

Routing

Same routing is used for IPv4 and IPv6. Dynamic routing is required to support IPv6.

Static routing to default router is used between terminal and mobile network.

It is common to use dynamic routing between mobile network and ISP.

Security

IP packet filtering is carried out using mobile connection card, etc. It is desirable that IPv6 and IPv4 have the same system. Moreover, IP packet filtering is carried out on a terminal.

Assumed form and issues in the IPv6 distribution period

The issue is that mobile terminal supports IPv6. Whether PPP of mobile terminal network stack supports IPv6 (IPV6CP NCP) becomes a problem. In the case of 3GPP, it is necessary to make PPP stack support to a certain extent.

Tunnel Access

Recommended deployment method

Outline

For tunnel access used by companies, Configured Tunnel is used. This is a commonly used method.

For tunnel access used by individuals, it is recommended to use ISP Provisioned Tunnel (TSP, DTCP, etc.). In this case, CPE terminates a tunnel. This method has the feature that it is possible to manage user connections and control addressing.

Site type is commonly used as customer connection method for both cases. In the case of tunnel access for individuals, terminal terminates a tunnel directly (Host type) in some cases.

Features of segment

Generally, whole IPv4 connection becomes a target.

All of global IPv4 address connection (IPv4 address dedicated, IPv4 address variable) and private IPv4 address connection (inside home, inside company) are included.

Best Current Practice

In this section, best current practice is discussed according to the realization method of tunnel (Configured Tunnel, ISP Provisioned Tunnel and Automatic Tunnel).

The following is an outline of each realization method.

• Configured Tunnel

This is mainly used for Site type connection. This is effective when IPv4 tunnel termination is dedicated address. This is generally used as a service for corporate users (who use dedicated address). As a feature, it is possible to carry out user provisioning on ISP side.

• ISP Provisioned Tunnel

In this case, both Site type and Host type connection can be used. TSP or DTCP protocol is used. Both individual users and corporate users can be the target. It is possible to set up a tunnel by user authentication and to carry out user provisioning on ISP side.

• Automatic Tunnel

This is mainly used for Host type connection. 6to4, ISATAP or Teredo protocol can be used. Generally this is for individual users, and authentication mechanism is not normally furnished. This is effective when uniform provision is made to all users inside ISP, but it has a problem when finding out who uses IPv6 or when caring for users who don't want to use IPv6.

<u>Configured Tunnel</u>

• Supporting network equipment

User side is required to have Configured Tunnel termination router. It is not impossible for Host that supports IPv6 to terminate a tunnel, but this is not a normal method.

ISP is required to have tunnel termination router. It is necessary to connect to IPv6/IPv4 network at the same time.

• Addressing

Address shall be set beforehand, and Prefix is assigned in dedicated manner (normally /48 for each connection).

• Routing

Static (default setting to a tunnel interface) or external routing (BGP4+) is used on user side.

On ISP side, static or external routing is used to assign address in such a manner that paths can be aggregated. For upper (core) connection, static/IGP/iBGP is used.

ISP Provisioned Tunnel

• Supporting network equipment

On user side, in the case of Site type, tunnel is terminated by router, and in the case of Host type, tunnel is terminated by terminal.

On ISP side, tunnel termination system is used. In this case, it is required to connect to IPv6/IPv4 networks at the same time. Servers are divided according to function such as a server for tunnel termination or server for authentication function in many cases.

• Addressing

Dedicated Prefix is provided for each user account.

In the case of Host type, /128 Prefix or /64 is distributed, and random address inside Prefix is used on terminal side. When user authentication is used, it becomes possible to put a string between user information and Prefix information.

• Routing

Static (default setting to tunnel interface) routing is used on a user side. External routing (BGP4+) is not common.

On ISP side, static routing is used to assign address in such a manner that paths can be aggregated. For upper (core) connection, static/IGP/iBGP is used.

Automatic Tunnel

• Supporting network equipment

On user side, it is required that only each tunnel termination host supports it. However, in the case of 6to4, it is possible to use a router as well.

On ISP side, tunnel termination router/system is used. In this case, it is required to connect to both IPv6/IPv4 networks at the same time.

• Addressing

IPv6 address is generated from IPv4 address, therefore addressing depends on IPv4 address. If IPv4 address is a dedicated address, IPv6 address shall be dedicated. If IPv4

address is dedicated, Configured Tunnel is normally used.

• Routing

Static (default setting to a tunnel interface) is used on user side. External routing is not common.

On ISP side, static routing is used for a user. Address is assigned in a manner that paths can be aggregated. For upper (core) connection, static/IGP/iBGP is used.

• Others

When limiting connection users, ACL shall be set for tunnel termination.

Tunnel connection in private network

• Connection between sites

This is carried out mainly in the company. Configured tunnel connection is normally used, and both ends use IPv4 dedicated address.

As VPN connection, IPsec-VPN, IP-VPN service supporting IPv6 (MPLS 6PE, etc.) and wide area Ethernet service are considered.

• Host connection inside site

This is used in both the company and at home. ISATAP and Teredo are the typical types.

In the case of ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), ISATAP router shall be set on the boundary of external network.

When Teredo is used, IPv6 packet is capsuled using UDP over IPv4 packet and tunnel is made from inside of NAT.

• Remote access (connection from outside of site to specified site)

This is mainly used in companies at present, however, it is considered for use at home in the future. IPsec-VPN and SSL-VPN are the typical types. In both cases, it is necessary to support IPv6 transport, so it is required to solve the problems unique to IPv6.

• Others

As others, L2TP can be used.

IPv6 address dedicated/variable

The following is a classification of tunnel methods mentioned above according to the fact of whether IPv6 address is dedicated or variable.

Dedicated
Configured Tunnel
ISP Provisioned Tunnel (depends on ISP policy)

Variable
ISP Provisioned Tunnel (depends on ISP policy)
Automatic Tunnel (depends on dedicated/variable IPv4 address)

Assumed form and issues in IPv6 distribution period

In this section, supplemental explanation is made for the deployment to Native/Dual Stack network from a network that has used a tunnel.

Motivation for deployment is to avoid overheads of tunnel processing along with increase inIPv6 traffic.

As Tips, handling of IPv4 Protocol No.41 packet (IPv6 capsuled packet) is explained.

When tunnel service is performed, this packet is not filtered in ISP network. Even if the service is not performed, we recommend not carrying out filtering wherever possible because it helps to prevent using 6to4, etc.

However, because filtering is not performed, it becomes necessary to consider security. There is a risk of attack on internal network or DoS attack on tunnel router through a tunnel. Refer to Security SWG (I1)/(I2) for this matter.

Server Operation Management

Please refer to Data Center SWG for this matter.

3. Assumed Form and Issues in the IPv6 Distribution Period

Assumed Form and Issues in the IPv6 Distribution Period

The following state and issues are considered in the IPv6 distribution period.

1. Increase in the ratio of Dual equipment

Stable operation as dual system is required, and it is also necessary that fall back operation from IPv6 to IPv4 of application is performed with no problem (under investigation in WIDE IPv6Fix Project).

Countermeasures for the matters that can be carried out in IPv4 and can not be carried out in IPv6 at present are also issues to be solved, such as DNS auto detection method, support of IPv6 transport by SNMP, support of IPv6 by virus soft, stateful AutoConfiguration (DHCPv6), multihome connection of end site, multihome connection using IP address and filtering of ICMPv6.

2. Increase in IPv6 traffic

It is required to improve processing performance of router, switch, IDS, firewall and load distribution device.

3. Release of IPv6 only equipment

If equipment that talks only with IPv6 is released, it becomes necessary to check presence of communication with IPv4 only equipment and communication method. Though this is described later, it is also considered to deploy IP phone to IPv6. If translator becomes necessary, it is necessary to consider the type and setting location.

4. Usage of Internet by non-PC equipment

It is necessary to consider arrangement of the contents of Zero-conf and achievement method, and at the same time it is necessary to consider simple methods of ensuring security.

5. Access from outside to inside

For accessing from outside to inside, it is expected to standardize dynamic punching protocol. Moreover, it is also expected to improve mutual connectivity of IPsec and establish security management method by ISP (described later). It is also necessary to find a protection method for important control type traffic, which is necessary for maintenance and measurement remotely, though it is a narrow band area.

6. Increase in P2P traffic

Along with the expansion of P2P traffic, traffic control method (file exchange, segregation from IP phone, etc.) will be more and more required.

7. Fusion of broadcasting and communication

It is necessary to consider a phased plan for making multicast to home default. It will also be necessary to establish the method to discriminate quality (QoS, policy routing (described later), etc.) from Best Effort Service.

8. IP communication with mobile equipment

Seamless Mobile IPv6 operation is required when changing links in particular.

9. Others

Name resolution technology (DNS, UPnP, SIP, etc.), their usage method (for each purpose), usage method of Privacy Extension and forming of consensus between ISP about problems occurring in the operation process (establishment of standard for punching holes, recommendation of Ingress filter at provider edge, etc.) will be issues. Moreover, it is required for ISP to cope with the form assumed by each segment (Home, Unmanaged, Managed).

Technical Issues in IPv6 Distribution Period

In the following, we discuss deployment issues of IP phone to IPv6, achievement issues of MultiPrefix, supporting issues of IPv6 Multicast and achievement issues of QoS on IPv6.

Deployment Issues of IP Phone to IPv6

With regard to deployment of phones to IPv6, ISP has 2 issues to consider; deployment of IP phone service that ISP provides and mutual connection with enterprise IP Centrex.

Concretely speaking, the point of issue varies according to the fact of whether dual phone machine is able to exist in the process of deployment of IP phone service.

When dual phone machine is released, it will be an issue whether operation including protocol selection mechanism between SIP server and client and fall-back has sufficient reliability or not.

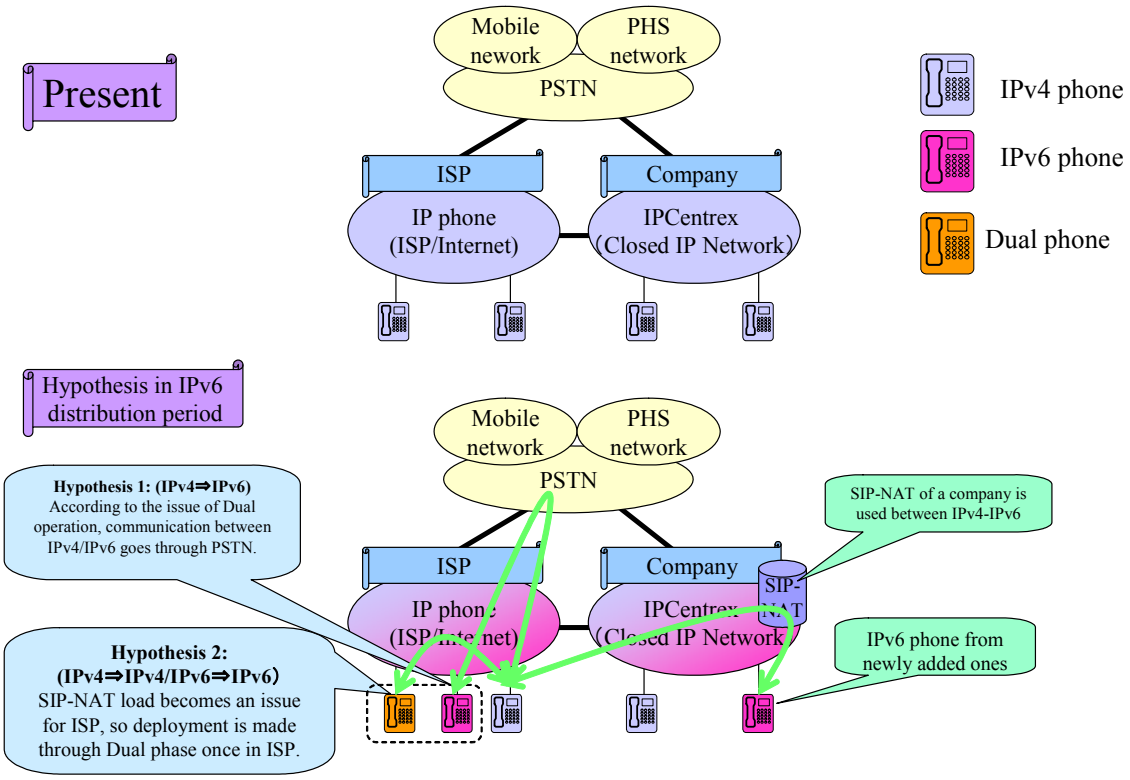
If IPv6 only phone is released, connection method with IPv4 equipment will be a problem, and the point of whether a translator such as SIP-NAT has sufficient durability against load

will be a particular issue.

At present, many middle and small sized ISPs have purchased IP phone service of major ISPs (SIP server is outsourced), so it is considered that the number of cases where middle and small sized ISPs consider deployment of IP phone to IPv6 will not be great.

However, there will be cases where it is required to secure QoS in access network for ISP's quality preservation of IP phone service.

Hypothesis of deployment in IPv6 distribution period



Target

In this section we discuss deployment of protocol stack of IP phone to IPv6, usage of SIP and application of SIP for other uses than IP phone, as name resolution protocol of equipment in particular.

Present state

In this section, we discuss the system in which SIP protocol is used. H. 323/MEGACO, etc. is used as well, but we don't discuss them here.

As application area, company and public (regular home) are considered.

The purpose of IP phone for a company is mainly replacement of extension phone. Usage of IPv6 is partially promoted. Dedicated terminal for IP phone functions as a SIP terminal. SIP server shall be individual for each enterprise, or shall be outsourced to ISP, etc. It is connected to the outside via PSTN and mutual connection with other IP phone system is not normally considered.

The purpose of IP phones for the public (regular home) is replacement of the home phone. As SIP terminal, CPE implements SIP client, and this CPE is used as a VoIP terminal. With this, it is aimed to avoid IPv4 global address problem.

With regard to SIP server, SIP mutual connection between ISPs becomes an issue. There is a problem of SIP dialect. It is a problem whether it is possible to absorb using interface between SIP servers. ISP that is not aligned or general PSTN phone terminal is avoided by communication via PSTN.

Deployment to IPv6

In deployment from IPv4 to IPv6, one of the turning points will be whether there is a Dual Stack period or not.

IPv4 → IPv4/IPv6 → IPv6

IPv4 → IPv6

It depends which deployment form is used, but in the latter case, difference between protocols may be absorbed by the system. However, in any case, it is necessary to check UUI mutual connection (communication between SIP terminals, RTP, etc.). There is a possibility that it is not possible to make communication between IPv6 and IPv4 protocols.

It is possible to absorb mutual connection of IPv6 and IPv4 with the system in the case it is between servers. However, mutual connection of UUI mentioned above is a problem. Dual Stack will probably be hard to do.

With regard to the problem of mutual connection (between ISP systems), it is possible to absorb SIP dialect with SIP server. Moreover, with regard to promotion of mutual connection, various activities are performed. For IPv6, there have been deployment demonstration experiments made by the Ministry of Internal Affairs and Communications, IPv6 CerWG/THAI, etc. However, it is considered that the problem of mutual connection will remain in the age of IPv6. It is necessary to check whether there are particular problems for deployment to IPv6.

Required implementations include, terminal, CPE, router and other SIP server systems.

Issues to Realize MultiPrefix (Source Address Selection)

MutiPrefix on IPv6

Motivation to MultiPrefix

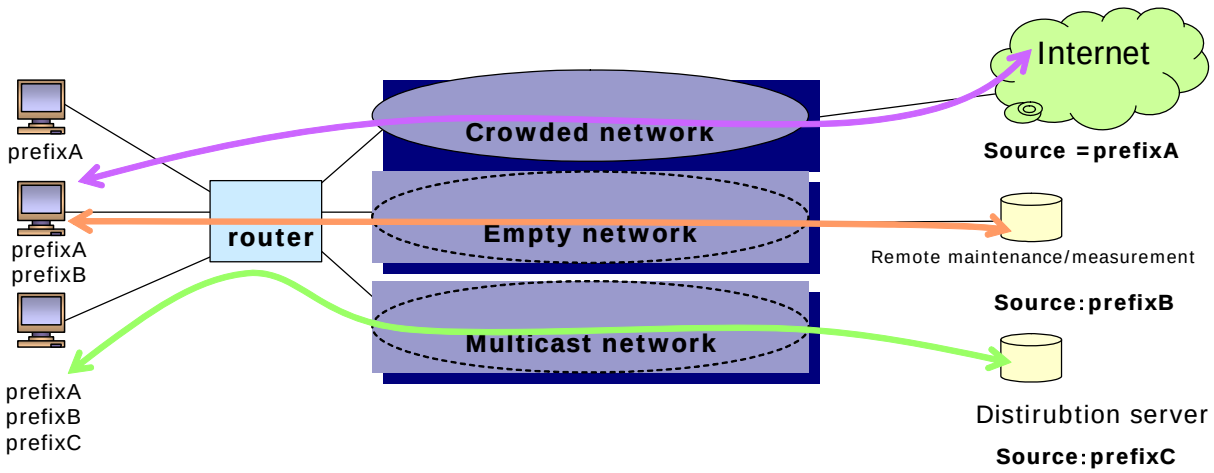
Realization of QoS (separation of QoS by Prefix, etc. Refer to the item of QoS as well), overlapped service (coexistence of IPv6 global connection service and ISP IPv6 private network connection service) and site multihome are considered as needs of MultiPrefix.

Related technology

Related technologies are IPv6 addressing (it is assumed to handle multiple IPv6 addresses using one interface in IPv6), routing selection (policy routing) and source address selection (RFC3484). MultiPrefix depends largely on these technologies.

Policy routing

It is considered to use a method to divide IP sides that go through by using the fact that communication origin terminal selects a “longest-match” source address for the destination address and carries out communication under MultiPrefix environment, which is a characteristic of IPv6.



Terminal support to realize MultiPrefix

There are 2 cases of MultiPrefix considered, depending on the fact of whether terminal supports it or not.

• When terminal provides support

It is possible that a highly functional terminal (PC terminal in general) supports it. It is considered that support is provided at OS level.

• When terminal is not able to provide support

It is not a large problem to assign multiple addresses, but information household appliances are considered as terminals that are probably not able to carry out address selection and routing selection properly.

When terminal provides support

・Items should be supported on terminal side

In the case of a highly functional terminal (PC in general), capability to assign multiple addresses and address selection function should be supported.

・Items should be supported by CPE

CPE should be able to receive information from account server, and appropriate address distribution, appropriate routing and filtering should be achieved. Here the method of taking up MAC information and registration method become a problem.

・Items that should be supported by network

In a network, appropriate routing and filtering should be performed using account server.

・Source address selection of application on a terminal

This is the function that allows the selection of a correct address in the end after failure to establish a connection, even if incorrect address is selected once. If application allows retry for connection using Getaddrinfo(), it is OK. However, a system to notify the application that establishment of connection failed is required. If ICMPv6 Error is picked up by a network, it takes time to acknowledge that establishment failed.

When terminal is not able to provide support

・Items that should be supported on terminal side

Even if a terminal is not able to support MultiPrefix (information household appliances, etc.), it is necessary to support regular address setting and routing.

・Items that should be supported by CPE

Information from account server is received via DHCP. Information received includes Prefix corresponding to MAC address, etc.

It is considered to receive beforehand or when receiving RS as a receiving timing, however, there will be a problem on how to treat Unsolicited RA.

Appropriate address distribution shall be carried out based on MAC address. However, handling of ND is complicated. For appropriate routing, it is possible to select routing using source address. Packet process from unappropriate address is performed for filtering.

In this series of procedures, the issue is how to take up and register MAC information.

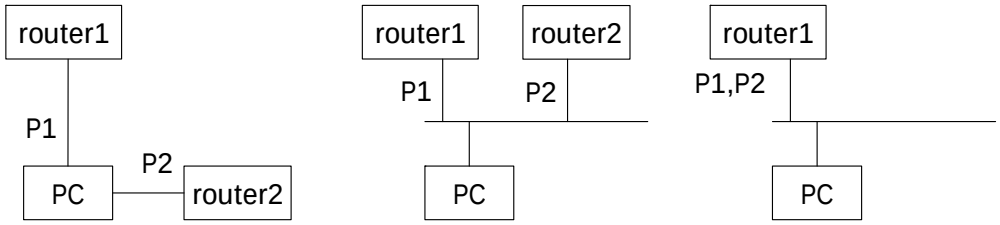
・Items that should be supported by network

Account server is managed based on DHCPv6. Source routing shall be used according to the case. Filtering is cared for by router or server.

Source Address Selection in MultiPrefix environment

Conditions for terminal to have multiple Prefixes

There are 2 patterns for the case; when a terminal with multiple interfaces functions practically and when a router advertises multiple Prefixes. In the following, “terminal accommodated in multiple routers” is included in “the case when a router advertises multiple Prefixes”.



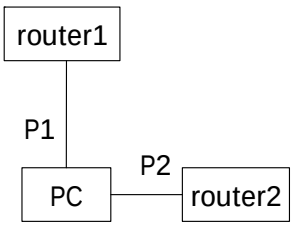
Terminal with multiple I/F

Terminal accommodated in multiple routers (this is excluded from the target of investigation this time.)

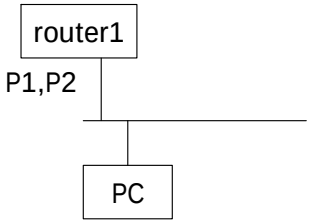
Router advertises multiple Prefixes

Conditions to fail Source Address Selection

- It is assumed that Nexthop Selection is performed successfully.



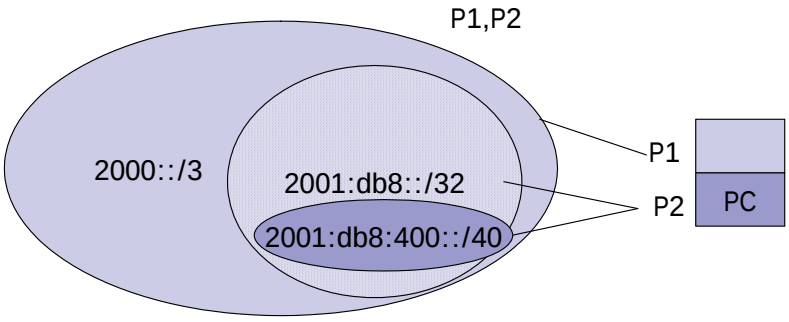
Successful at all times
(RFC3484 Rule.5
"Prefer outgoing interface")



Successful with RFC3484 Rule 8 in most cases
("Using the longest matching prefix")
But if it is not successful, Rule 6 is necessary.
("Prefer Same label")

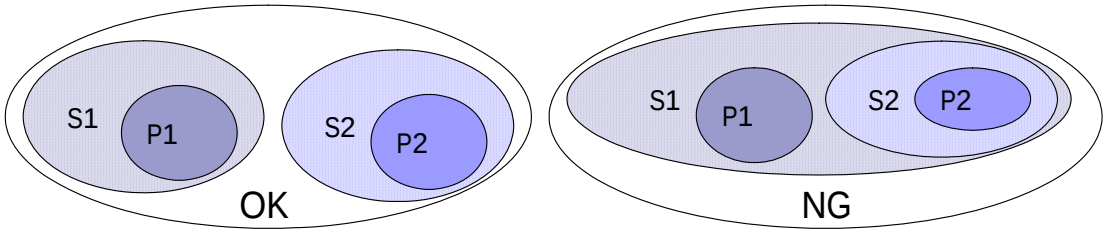
Example of failed Source Address Selection

- e.g.)
  - P1=2001:db8:420:1::/64
  - P2=2001:0:165:10::/64
  - P2 is used for Internet (2000::/3) communication, and P1 is used for Intranet (2001:db8:400::/40) communication.
  - When communicating with 2001:db8::1, Intranet Prefix P1 is used.



What should we do to avoid failing Source Address Selection

- Preconditions
  - Communication destination $\forall x1 \in S1$ to which P1 should be used for communication
  - Communication destination $\forall x2 \in S2$ to which P2 should be used for communication
  - $P1 \subseteq S1$, $P2 \subseteq S2$
- Conditions
  - It will be successful when using $S1 \cap S2 = \phi \Leftrightarrow$RFC3484 Rule 8(Longest Match Prefix).
  - If this is not assured, RFC3484 Rule 6 (Prefer Same Label) is necessary.



Issues to Support IPv6 Multicast

Handling of Multicast

The basic idea is the same as IPv4. Multicast is used to signal participation/removal of Multicast group to/from a terminal. In the case of IPv4, IGMP is used and in the case of IPv6, ICMPv6 and MLD are used.

Protocol of multicast routing is the same (PIM-SM/SSM/DM, etc.).

IPv6 Multicast

With IPv6 Multicast, it is possible to realize multicast distribution to the end terminal simply, utilizing globalness (usage of PIM-SSM). The issue is how to utilize this merit, such as exceeding NAT of Multicast.

Dual stack Multicast

In the case of Dual Stack, it should be possible to construct different tables for IPv4 and IPv6 with multicast routing.

In the case of a protocol that depends on RPF (Reverse Path Forwarding) of Unicast routing table such as PIM in particular, IPv4/IPv6 Unicast routing topology doesn't have to be the same, so the Multicast routing tables in both cases shall have different topologies.

With regard to Multicast group, there are differences in group space and scope, so it is necessary to check what they affect.

IPv6⇔IPv4 mutual connectivity

Between IPv6 and IPv4, there is a difference of address first of all. There is an issue of whether mutual translation of address → Multicast Translation should be carried out or not.

With regard to mutual connection of routing, it is necessary to check the necessity first of all.

With regard to the difference of group space, there is an issue of whether group mutual translation should be carried out or not.

Implementation of Multicast function to equipment

Terminal

MLD is used as a terminal. Many PCs have implemented it.

CPE

CPE carries out Static Multicast routing. There is a possibility that it is not realistic to create an internal environment of the user of individual service in order to carry out dynamic routing.

With regard to MLD and/or MLD Proxy, it may be requested that it be able to handle MLD on MLD Proxy + ISP side.

Router

It is required to support Multicast routing and MLD, however, there are already many implementations (PIM-SM).

L2 switch

MLD Snooping function is required.

Issue to Realize QoS on IPv6

Range of QoS in this document

QoS discussed in this document is a traffic discrimination mechanism on the same network. For discrimination in the same network, queuing of interface, Diffserv can be used.

However, we discriminate by constructing different sides here. Physical side shall be separated using different side by MultiPrefix. Then, handling shall be separated according to Prefix, and policy routing, etc. shall be used.

As an application example, there is preferential control of stream type traffic; for instance, IP phone and image streaming.

Handling of QoS

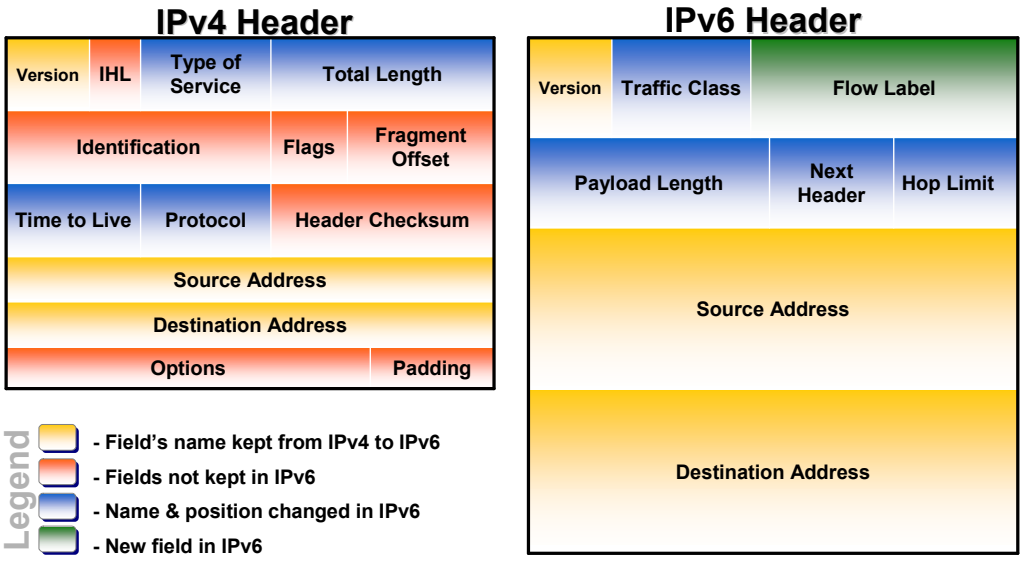
Comparison diagram of IPv4 Header and IPv6 Header is shown below.

Handling of IPv6 Traffic Class field is the same as that of IPv4 ToS field. Difference from IPv4 is “FlowLabel”. Therefore, in order to demonstrate uniqueness of IPv6, it is necessary to realize application of FlowLabel.

With regard to mapping with Layer2 QoS, the same as with IPv4, it is possible to consider the relation with MPLS, etc.

For mutual compatibility of IPv6⇔IPv4 QoS, it is required to consider whether it is necessary and when it would be necessary.

Reference: Comparison of IPv4 header and IPv6 basic header



Expected QoS function on equipment

CPE

For CPE, handling of Traffic Class field and Queuing functions are required.

Router

For router, handling of Traffic Class field and Queuing

Others

QoS policy control system, etc.

4. Tips

Matters Related to Address

The addresses of routers and servers should be set manually. In the case of EUI-64, if NIC is changed, address is changed, so a dedicated address should be used in order to reduce the trouble of DNS registration and filtering setting.

The following are convenient naming rule examples.

- ::1 , ::53 , ::80 , ::cafe
- :c726:a00:3:82 This shall be allocated to ATM link between Tokyo 03- and Hiroshima 082.

However, it should be noted that these addresses may easily become a target for attack.

Renumbering Method

The following is an explanation of a manual renumbering method that is easy to carry out. This method uses the fact that it is possible to assign multiple IPv6 addresses to the same interface.

The procedure is as shown below.

1. Acquisition of new address
2. Setting of new address connectivity (routing)
3. Assignment of new address to IPv6 node (router and terminal)
   - Former address shall be assigned as well without deleting it.
   - It is automatically set with AddressAutoConfiguration at terminal level.
4. DNS registration change work shall be carried out as well.
5. Former address shall be deleted.
6. Former address connectivity (routing) shall be deleted.

In IPv6, when renumbering is carried out using this method, there will be less influence of disconnection of service compared with renumbering of IPv4 and phased renumbering is possible.

This procedure is included in the draft shown below.

Procedures for Renumbering an IPv6 Network without a Flag Day

(Draft-ietf-v6ops-renumbering-procedure-01.txt)

Historical Circumstances of sTLA Allocation

First of all (1999), the initial allocation was /35.

After revision (Jul. 1, 2002), the initial allocation became /32. But, it is optional for an sTLA holder who has already acquired /35 to upgrade to /32, therefore there are sTLAs that have /35 even after a new policy is enforced. At present, sTLAs of /32 and sTLAs of /35 coexist.

Appendix

IPv6 Deployment Case Study of Middle/Small Sized ISP

Purpose and Assumed ISP Form

In this section, typical IPv6 Introduction models for middle/small ISPs is discussed based on the description of guideline. The purpose of this discussion is to accumulate operational experience and to give a guide for service support.

Assumed form of middle and small sized ISPs is as shown below.

Network

It constructs IPv4 network and provides ISP service.

Address

It receives IPv4 address allocation from JPNIC as an address specified provider.

Routing

It acquires AS No. (from JPNIC, etc.) and carries out external connection of IPv4 with BGP. It uses OSPFv2 for internal routing. Internal BGP (iBGP) doesn't use Confederation or RR.

It is assumed for this section that the former method is used in order to secure connectivity of IPv4. And only the part specialized to IPv6 is discussed in this section.

IPv6 Network Introduction Policy

Address

Address shall be acquired independently for IPv6 (/32 Prefix space). Address of IPv4 and connectivity are secured for management, however, IPv4 traffic of user is not handled. As an IPv6 test service, it is assumed to provide /48 Prefix to a customer.

Network

Different network for IPv6 shall be constructed independently from existing network. The basic idea of configuration is the same for IPv6/IPv4. There is concern regarding the ease of deployment to the Dual Stack network in the future using backbone, external connection,

access connection and server segment.

Backbone uses tunnel in some cases. As an IPv6 test service, it is assumed to provide tunnel connection to customers.

Routing

Consistency shall be taken with the existing network as much as possible. Here, routing is considered taking into account integration of IPv6 and IPv4 networks in the future. IPv6/IPv4 routing protocols shall be consistent and IPv4/IPv6 routing topology shall be consistent. As an IPv6 test service, it is assumed to set static routing to a customer.

Reference: When Acquiring the Address From Upper ISP

In the following, difference from the case when address is acquired independently is shown.

Network

External connection shall normally be made only to upper ISP. It is difficult to connect to more than 2 upper ISPs. However, it is possible to connect to several upper ISPs in order to secure redundancy.

Address

IPv6 address space shall be acquired from the upper ISP. In this case, address space shall be smaller than the case when it is acquired from APNIC (/32 minimum). The size of acquirable address space varies according to the policy of the upper ISP.

Routing

Normally Static connection is used with upper ISP as default network. It is possible to connect using dynamic routing (BGP4+, etc.) in order to secure redundancy or for peering with other ISP.

When carrying out Peer, it is not permitted to advertise own path from Peer destination to the external network (in order to avoid IPv6 Prefix punching hole). When using private AS, it is necessary to adjust AS No. used with Peering destination. (Normally this form is not recommended.)

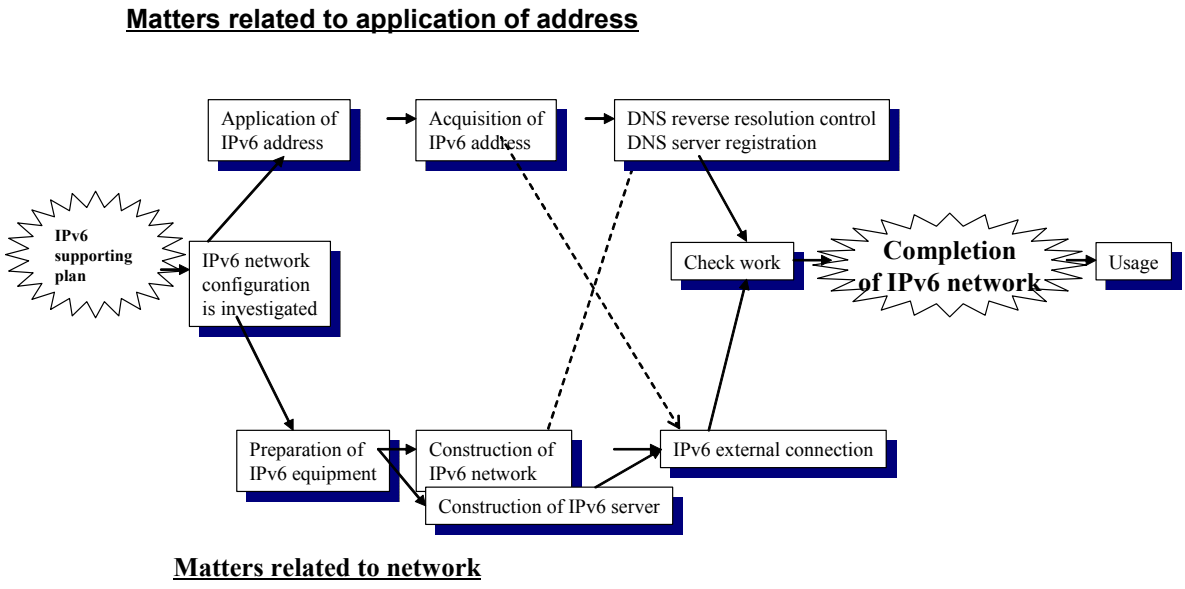
Introduction Procedure

Introduction procedure is explained in the following using the points shown below.

1. Investigation of network configuration (Physical configuration, Logical configuration)
2. Acquisition of address
3. Preparation of equipment
4. Construction of network
5. Usage

Duty associated with acquisition of address (registration of RIR database along with assignment of address, control of DNS reverse resolution setting for acquired address)

Construction Chart Diagram



1. Investigation of network configuration

You are sometimes asked about IPv6 network development plan when you acquire an address, so it should be thought through first.

Physical configuration

Configuration is network, backbone, external connection, access and server segment.

At the test network stage, it is not necessary to duplicate networks and facilities, however, it is desirable to construct the same network as the one you will use for the service.

Logical configuration

Addressing design

Prefix plan complying with the usage; for customer, POP shall be made. It should be noted to secure large Prefix area for each POP so that it becomes easier to aggregate paths.

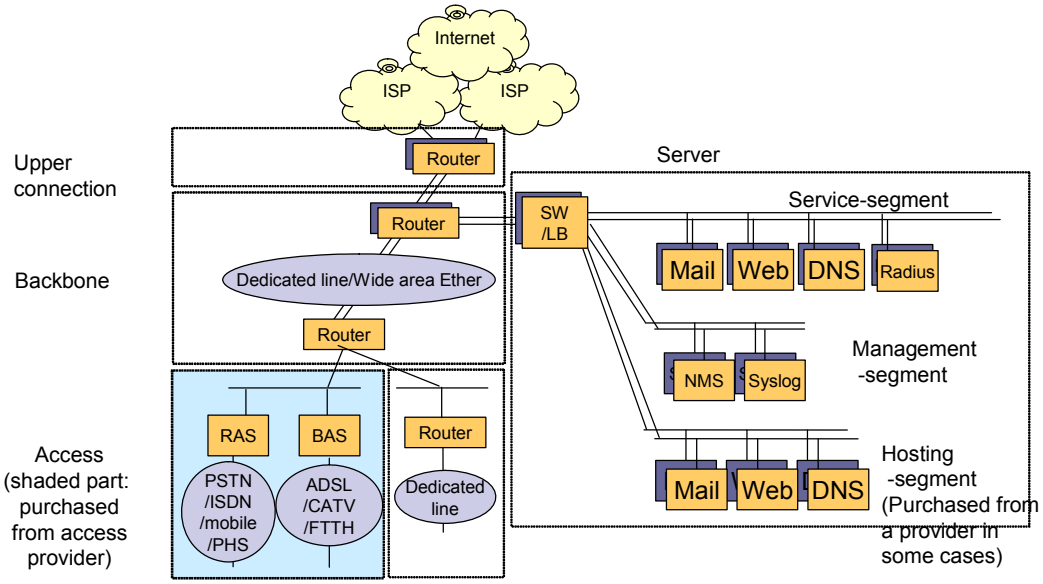
Even if carrying out only data transfer of IPv6, IPv4 address should always be assigned to each interface. This is done for the operation on the existing system.

Routing design

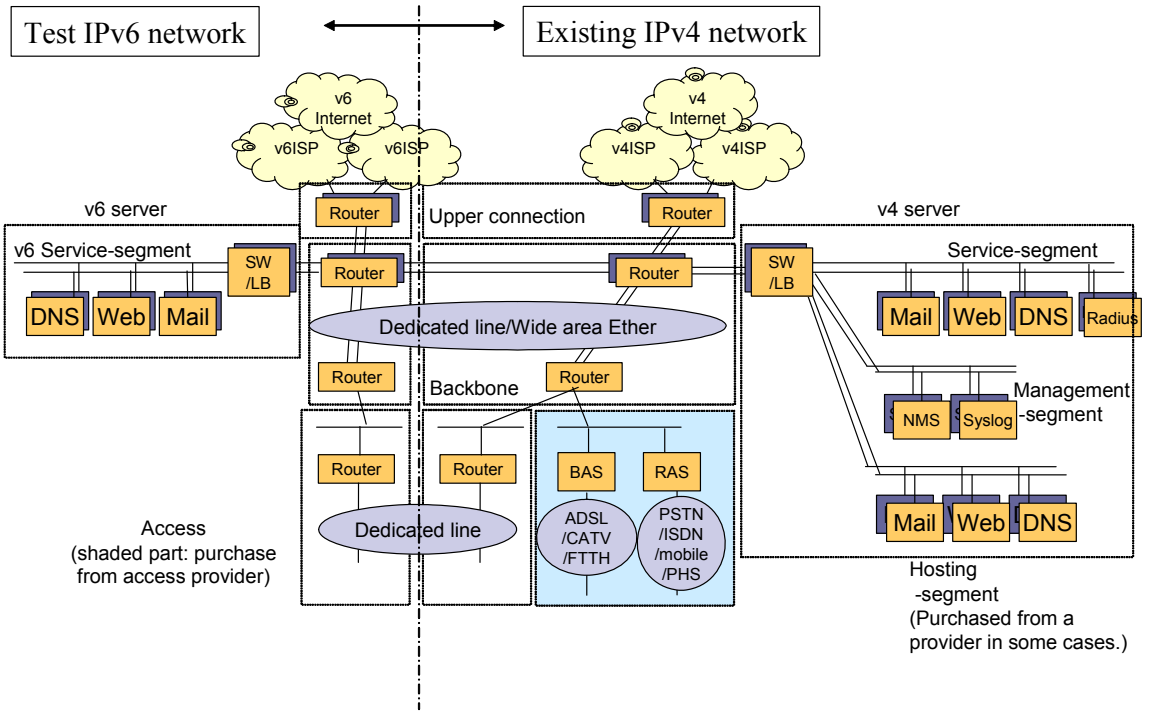
For external path, BGP Mulitprotocol Extension is used and for internal path, OSPFv3 is used.

As for setting of customer path, static routing and re-distribution to internal path are carried out.

Re-publication: Configuration Factors of Middle/Small Sized ISP



Configuration Example of IPv6 Test Network



2. Acquisition of address

In the case of provider specified by JPNIC, application for address is carried out using "JPNIC IPv6 address application introduction service".

Please refer to http://www.nic.ad.jp/ja/ipv6/index.html (JPNIC).

Necessary contents for application

Refer to http://www.nic.ad.jp/doc/ipv6-alloc-process.html for procedure of application for IPv6 address.

Contents to be filled out in application

Refer to the example of application shown below for the contents.

Fee

IPv6 address allocation fee

- ¥4.2 (tax included) per site (/48)
- In the case of /32, it shall be ¥29,954 (tax included) by adjusting and calculating as 7,132 sites.

IPv6 address maintenance fee

- In the case of /32, ¥262,500/year (tax included)

  When address over IPv4 /20 is controlled (when receiving allocation), /32 IPv6 address maintenance fee is exempted. (the higher of either IPv4 address maintenance fee or IPv6 address maintenance fee is applied.)

Refer to JPNIC document, JPNIC-00937 "Rules for IP address allocation, etc." for details. (http://www.nic.ad.jp/doc/ip-rule.html)

Around one month after JPNIC and APNIC complete checking work of the application contents, IPv6 Prefix shall be allocated.

Application of IPv6 address

IPv6 address application (example is mentioned later *) shall be created and sent by mail to request@ipv6.nic.ad.jp (subject, etc. shall be arbitrary).

*Extracted from the material of regular explanatory meeting of specified IP address management providers.

(http://www.nic.ad.jp/ja/materials/ip/4beginers20040910.pdf)

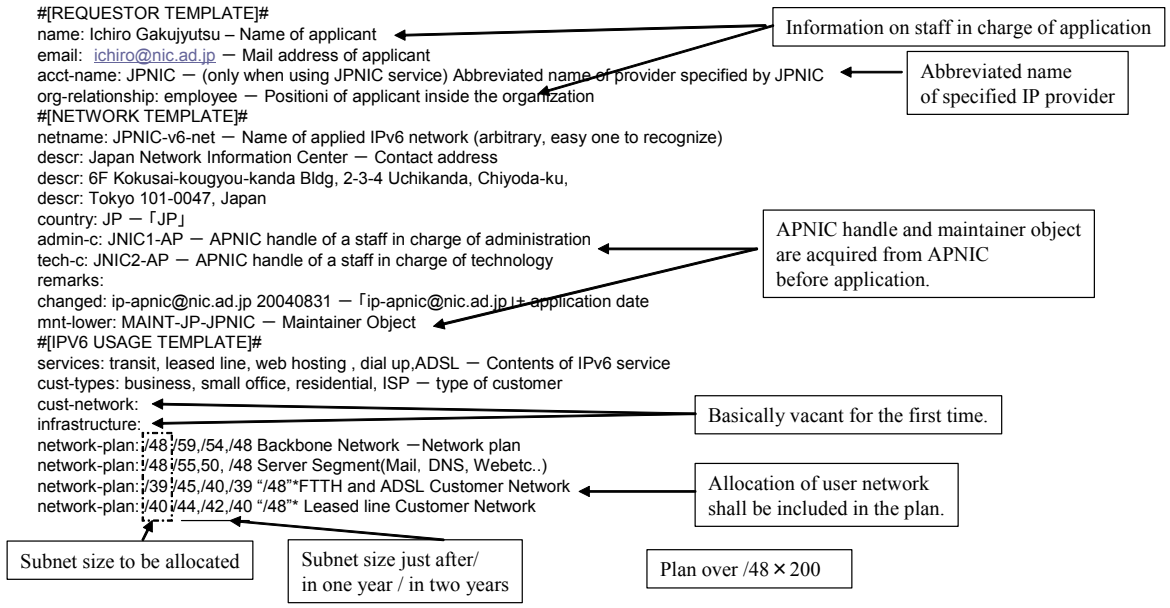
Application shall be sent to APNIC after it is checked by JPNIC. During checking work of the contents, you may receive questions from JPNIC or APNIC (via JPNIC) in some cases.

Refer to theguideline shown below for the description according to individual network state.

http://www.nic.ad.jp/ja/translation/ipv6/ipv6-alloc-form-guide.html

Before applying for IPv6 address, you shall apply for and acquire Maintainer Object (network information) and Person Object (network administrator information) from APNIC. Application method is described in the following.

Description example of IPv6 address application



It is better to prepare a plan to develop IPv6 service as a supplemental information for the application mentioned above.

Maintainer Object, Person Object application method

You shall apply for Maintainer Object (network information) and Person Object (network administrator information) required for application of IPv6 address.

You shall create Maintainer/Person Object application (example is mentioned later) and send it to maint-request@apnic.net (Maintainer Object application address) by mail. APNIC account shall be included in the subject. In the case of a provider specified by JPNIC, "JPNIC-JP" should always be included in the subject.

Refer to the following sites for an explanation of application method (and changing method

of the contents).

http://www.nic.ad.jp/ja/translation/apnic/apnic-102-j.html

http://www.nic.ad.jp/ja/translation/apnic/20021217.html

If there is no problem, you will be informed of an APNIC NIC handle that shows Maintainer Object approval/registration and Person Object registration information by mail within a few days.

Description example of Maintainer Object, Person Object application

```
#[MAINTAINER TEMPLATE V:3.0]#

mntner: MAINT-JP-JPNIC              ― MAINT-JP-[name of organization], Name of organization is arbitrary (recommended to use abbreviated name of specified provider)
descr: Maintainer for JPNIC         ― Simple outline of organization
descr: Webhosting, dialup, leased line
descr: Japan
admin-c: AUTO-1                     ― When applying for Person and Object at the same time, [AUTO-numeric figure] shall be filled in to match the description of Person
                                      Object
tech-c: AUTO-2                      ― It is OK to write the same person in columns of admin-c and tech-c.
                                      Possible to register multiple number for Admin-c and Tech-c.  In such cases, necessary amount should be written.
upd-to: noc@nic.ad.jp               ― Contract address of information related to Maintainer Object (Person Object or Domain Object (described later) update information is
                                      sent)
auth:  CRYPT-PW JPNIC-v6v6          ― Authentication method when using Maintainer Object
                                      Plaintext authentication - "CRYPT-PW" + Plaintext password
remarks:                            ― Notes (not necessary in particular)

[PERSON TEMPLATE V:4.0]#

Person: Ichiro Gakujyutsu           ― Name
address: 6F Kokusai-kougyou-kanda Bldg, 2-3-4 Uchikanda, Chiyoda-ku,  ― Address
address: Tokyo 101-0047, Japan
country:  JP                        ― Country of location, "JP" in the case of provider specified by JPNIC
phone:  +81-3-1234-5678             ― Telephone number of contact
fax-no:  +81-3-1234-9876            ― Facsimile number of contact (voluntary)
e-mail: ichiro@nic.ad.jp            ― e-mail address
nic-hdl: AUTO-1                     ― NIC handle
                                      When applying for Person and Object at the same time, [AUTO-numeric figure] shall be filled in to match the description of Person
                                      Object
remarks:                            ― Notes (not necessary in particular)

#[PERSON TEMPLATE V:4.0]#

person: Hanako Gakujyutsu
address: 6F Kokusai-kougyou-kanda Bldg, 2-3-4 Uchikanda, Chiyoda-ku,
address: Tokyo 101-0047, Japan
country:  JP
phone:  +81-3-1234-5678
fax-no: +81-3-1234-9876
e-mail: hanako@nic.ad.jp
nic-hdl: AUTO-2
remarks:

#[TEMPLATES END]#
```

3. Preparation of equipment

The main equipment required is the server and router.

Router

Router is used for external connection (upper connection, Peer connection of IX or privatepeer, backbone, access and accommodation of customer). In this case study, it is assumed to use tunnel termination router.

Server

It is crucial to set DNS server to carry out reverse resolution control of the acquired address.

It is necessary to use a server that handles AAAA. It doesn't always have to support IPv6 transport, however, it is desirable to support it.

As others, it is desireable to construct a server that supports IPv6 for basic mail or web site in order to accumulate experience as well. It is desirable to prepare a server for daily control of IPv6 network or IPv6 terminal. This is used to control Ping6 or traceroute6.

Selection of equipment, server application

Selection of equipment

If the equipment you currently use supports IPv6, we recommend that you use the same equipment if possible. This is to facilitate deployment to Dual Stack network.

Necessary functions

It is required to furnish IPv6 function equivalent to IPv6 Logo Phase I. We recommend the use of equipment that has acquired IPv6 Logo Mark if possible. A list of equipment that has acquired the IPv6 Logo Mark shall be indicated later.

In the case of router, apart from the points mentioned above, it is required to support necessary routing protocol (BGP4+, OFPFv3, Static in this case).

Selection of server application

If the server OS you currently use supports IPv6, we recommend that you use the same OS if possible (BSD, Linux (application of USAGI is recommended), Solaris, HP-UX, etc.).

If the server application you currently use supports IPv6, we recommend using the same application if possible.

Examples of server applications that support IPv6 are Bind9 for DNS, Apache2 for web, and in the case of E-mail, SMTP server shall be Sendmail, postfix or qmail, and POP3 server shall be qpopper, cyrus-IMAPd (as IMAP server as well), etc.

Information on OSs and application servers that support IPv6 is included in "IPv6 Style".

http://www.ipv6style.jp/jp/statistics/ipv6unix/index.shtml

Authentication of equipment

For the purpose of equipment authentication, there is an IPv6 Ready Logo program (http://cf.v6pc.jp/frames.html). This is a qualified program, which is used as a guideline for Introduction of equipment and sponsored by the IPv6 Forum. A pass standard is established, and at present, a Phase I program and a partial Phase II program are established.

Target equipment includes routers, terminals and special devices. We recommend using

IPv6 Ready Log qualified items if possible.

Latest list of IPv6 Logo Mark qualified items is indicated at the URL shown below.

http://cf.v6pc.jp/logo_db/approved_list.php

4. Construction of network

Construction method of network is the same as that of existing network. It is desirable to construct in the same form as the existing network as far as possible for the sake of deployment to Dual Stack network.

• External connection

In order to secure stable connection, it is desirable to use the IPv6 gateway service, etc. of an ISP for securing IPv6 connection. Even with only upper connection, connectivity inside the country shall be secured.

It is considered better to secure the connectivity of IPv6 with domestic ISP by carrying out Peer using IX that supports IPv6.

• Customer connection

Static path setting shall be used for connection. Static path of customer shall be re-distributed to inner path of ISP in order to secure connectivity. Setting of Configured Tunnel shall be made with tunnel router of customer.

Moreover, router shall be set and server shall be set (construction of server segment, construction of server).

Construction of router

As IPv6 addressing, /64 Prefix shall normally be assigned to a link. /126 Prefix is acceptable, however, we don't recommend using /127. We also don't recommend setting "unnumbered" from the viewpoint of life and death monitoring of a link.

IPv6 address to be assigned to router interface shall normally be dedicated. RA, etc. is not used. Link local address can be used as it is with no problem (fe80::(EUI-64)).

IPv4 addressing shall follow the existing policy.

Example of external connection – Connection to IX (NSPIXP6) that supports IPv6

NSPIXP6 is IX that supports IPv6 and is operated by WIDE Project.

It must be understood that it is not a production level such as DIXIE, but it is an experimental level. It has connection points in KDDI Otemachi Building, NTT Otemachi Building and NTT Dojima Building. Refer to the URL shown below for details.

http://www.wide.ad.jp/nspixp6/

Example of connection procedure to NSPIXP6

With regard to connection to NSPIXP6, you should consult with professor Kato of Tokyo University (by mail or at NSPIXP meeting). There is no regulated format, but the information shown below will make it easier for you make a judgement.

- Organization
- Outline of organization
- Purpose of connection
- AS
- IPv6 Prefix (if you have one)
- Connection location, etc.

Connection with NSPIXP6 shall be carried out after connection is permitted. It is requested to inform NSPIXP6 operation section of the work time, etc. beforehand.

Normally connection is made with FastEthernet (100BASE-TX/FX). IPv6 Peer address is assigned under certain rules. It shall be fe80::ASN:ID or (NSPIXP6 IPv6 Prefix) ::ASN:ID. Refer to http://www.wide.ad.jp/nspixp6/peering-address.txt.

After connection work is complete, you connect to NSPIXP6, and then you contact the operation section to inform them of the following information.

Connection location, connection switch port No., IPv6 Prefix, name of organization, AS No. (decimal, hexadecimal), Peer address, implementation of IX connection router, contact address

With this procedure, addition to the contact list is carried out.

Negotiation and setting of Peer

After connecting to NSPIXP6, you contact each Peer contact address to ask about Peer. When making a contact, it is preferable to inform them of the following connection information.

• IPv6 address (address created according to the policy mentioned above)
• AS Path to be advertised (Own AS, AS Path underneath as well if any)
• Prefix to be advertised (Own Prefix, Prefix underneath as well if nay)
• Contact point regarding operation (mail, telephone No., Fax No., etc.)
• MD5 password, exchange of memorandum, etc. if necessary

After Peer is agreed, setting of Peer shall be input to IX connection router. You shall check that Peer session starts and paths are exchanged properly.

Tips for construction of network

Access list for ICMPv6 packet

In the case of IPv6, even if an ICMPv6 packet is passed through, it will not be a big security threat. For PMTUD action, it is definitely necessary to pass Type2 (Packet Too Big) packet through in particular. It is considered better to pass through Type1 (Destination Unreachable), Type3 (Time Exceeded) and Type4 (Parameter Problem) as well.

In IPv6, there is no worry of attack on inner segment using broadcast ICMP packet from outside, which occurs in IPv4. ICMPv6 packet related to Neighbor Discovery is used only with link local.

ICMPv6 packet filter shall be set according to network policy as necessary (blocking of Type129/130 (Echo Request/Reply) packet, Type138 (Router Renumbering) and Type139/140 (Node Information Query) for checking the presence of inner host).

IPv6 address registered with database of APNIC should be able to reach (IPv6 address of DNS server, etc.).

Filtering for tunnel

In IPv4 segment where IPv6 tunnel packet passes through, it is necessary to pass IP Protocol No. 41 packet.

Construction of server segment network

• Addressing

Addressing in sever segment shall be carried out as shown below.

In the case of IPv6, /64 Prefix is allocated to a segment. Server address shall normally be allocated as dedicated address, and RA is not used. It is possible to allocate with RA in some cases.

In the case of IPv4, Prefix of the size necessary for connection shall be allocated. Server address shall normally be allocated as dedicated address.

• Routing

Normally for both IPv4 and IPv6, static routing is used as default. Dynamic routing or VRRP can be set in order to secure redundancy in some cases.

Construction of server

DNS server

DNS server shall be constructed as Dual Stack.

In the case of DNS that controls reverse resolution zone information, it is set to compete SOA record of reverse resolution zone.

When 2001:db8::/32 → 8.b.d.0.1.0.0.2.ip6.arpa

Registration record shall be created as necessary. This is because upper server doesn't always support inquiries of IPv6. Route server in particular doesn't support inquiries of IPv6 at present.

Mail server

SMTP server shall normally be constructed as Dual Stack. This is because, it is possible to be connected for both IPv6 and IPv4 by a server of connection origin, but the server of connection destination may receive connection of only IPv4. Moreover, it is not possible to register MX record by separating into IPv6 and IPv4.

POP3/IMAP server, etc. shall depend on client's status of support for IPv6.

Example of DNS Zone information setting (bind 9)

- named.conf
  - Normal resolution

```
zone “test.com” {
type master;
file “test.com.zone”
};
```

  - Reverse resolution

```
zone “8.b.d.0.1.0.0.2.ip6.arpa” {
type master;
file “8.b.d.0.1.0.0.2.ip6.arpa.rev”;
};
```

- test.com.zone

```
@       IN      SOA     ns.test.com. Admin.test.com. (
                                2004122101
                                3600
                                900
                                3600000
                                3600 )
        IN      NS      ns.test.com.
ns      IN      A       192.168.0.1
        IN      AAAA    2001:db8::53
```

- 8.b.d.0.1.0.0.2.ip6.arpa.rev

```
@       IN      SOA     ns.test.com. Admin.test.com. (
                                2004122101
                                3600
                                900
                                3600000
                                3600 )
        IN      NS      ns.test.com.
3.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   IN   PTR   ns.test..com.
```

Connection test

The following are the points that should be checked at connection test.

· Connectivity to IPv6 Internet

Checking routing table

Checking reachability from inside to external IPv6 network

Reachability from inner router, etc. shall be checked using Ping6 or traceroute6. As a target host, it is possible to use www.v6pc.jp (IPv6 Promotion Council of Japan) and www.kame.net (KAME Project).

Checking reachability from outside to inner IPv6 network

Reachability shall be checked with the state of own IPv6 Prefix advertisement, ping6 to the inner network (IPv6 address of inner router, etc.) or traceroute6 using Looking Glass that supports external IPv6.

http://www.v6.mfeed.ad.jp/ipv6/lg.html
http://query.freak.ne.jp/
http://www.v6.dren.net/lg/index.html, etc.

Dummy customer environment shall be prepared and IPv6 network connectivity from customer's network shall be checked.

It shall be checked that PMTUD works properly inside a network by changing (enlarging) the packet size of Ping6.

Checking by setting the value over the max. MTU value (1500 bytes) on regular Ethernet, etc.

• Action of server

DNS shall be set and application to transfer IPv6 address space reverse resolution control right shall be made to APNIC.

Application method is described later.

Check the action of Web and Mail servers.

• Control

Whether it is possible to control IPv6 equipment using the existing system.

It is preferable to be able to control with both IPv4 and IPv6.

Checking of reachability from login server.

Registration of RIR database of IPv6 Prefix DNS reverse resolution information

When registration is made, Internet connectivity of DNS server (address, DNS server action) and reverse resolution zone information (SOA record) are checked by the system of APNIC, so DNS server shall be constructed and reverse resolution zone information shall be set beforehand.

Person Object application (example is shown later) for person in charge of administration of allocated Prefix (admin-c), person in charge of technical operation (tech-c) and zone administrator (zone-c) shall be created and sent by mail to auto-dbm@apnic.net (normally the same as Maintainer Object).

If there is no problem, APNIC NIC handle showing Person Object registration information is received within a few days.

Then, domain Object application (example is shown later) of DNS reverse resolution information shall be created and sent by mail to auto-dbm@apnic.net.

Refer to URL shown below for an explanation of application method (and changing method

of the contents).

http://www.nic.ad.jp/ja/translation/apnic/apnic-database-update-info.html

If there is no problem, completion of registration is received by mail within a few days.

Description example of Person Object registration application

Person: Ichiro Gakujyutsu	—	Name
Address: 6F Kokusai-kougyou-kanda Bldg, 2-3-4 Uchikanda, Chiyoda-ku,		
Address: Tokyo 101-0047, Japan	—	Address
Country: JP	—	Country of location (“JP” in the case of Japan)
Phone: +81-3-1234-5678	—	Telephone number for contact
Fax-no: +81-3-1234-9876	—	Facsimile number for contact (voluntary)
e-mail: ichiro@nic.ad.jp	—	e-mail address
nic-hdl: AUTO-1	—	NIC handle (this is not determined, so write “AUTO-1”.)
Remarks:	—	Note (not necessary in particular)
Notify:	—	Contact address (not necessary if it is the same as e-mail)
mnt-by: MAINT-JP-JPNIC	—	Description of maintainer Object of ISP
Changed: noc@nic.ad.jp	—	Address of ISP staff in charge of application Normally upd-to: of Maintainer Object is written
Source: APNIC	—	Information source shall be written. “APNIC” in the case of provider specified by JPNIC

Description example of IPv6 Prefix DNS reverse resolution information registration application

Domain: 8.b.d.0.1.0.0.2.ip6.arpa	—	Name of reverse resolution domain
descr: Reverse Delegation of 2001:db8::/32	—	Desciption of domain
admin-c: IG100-AP	—	NIC handle of admnistrator
tech-c: HG200-AP	—	NIC handle of operator
zone-c: HG200-AP	—	NIC handle of zone administrator
nserver: dns-ipv6-1.nic.ad.jp	—	Name of DNS server (FQDN) that controls reverse resolution zone.
Nserver: dns-ipv6-2.nic.ad.jp		OK to write multiple number of DNS server names. There is no registration of database of DNS server name, so it shall be set beforehand so that it is possible to carry out normal resolution.
sub-dom:		Sub-domain list (not necessary for IPv6 reverse resolution registration)
dom-net:		Address list in domain (not necessary for IPv6 reverse resolution registration)
Remarks:	—	Note (not necessary in particular)
notify: noc@nic.ad.jp	—	Address of ISP staff in charge of application Normally upd-to: of Maintainer Object shall be written.
mnt-by: MAINT-JP-JPNIC	—	Maintainer Object of ISP shall be written.
mnt-lower:	—	Lower Maint. Object when it is not authenticated with mnt-by. (not necessary in particular)
Refer:	—	Reference to DNS server (not necessary for IPv6 reverse resolution registration)
Changed	—	Address of person who changes information Normally upd-to: of Maintainer Object shall be written.
Source:	—	Registration database name shall be written. “APNIC” in the case of provider specified by JPNIC

5. Operation

• Daily management

For network monitoring, equipment interface life and death monitoring shall be carried out using IPv6 ICMPv6. NMS that supports IPv6, etc. shall be used.

Moreover, life and death monitoring of equipment interface (ICMPv4), process monitoring (syslog) and traffic state monitoring (snmp) are carried out from the existing IPv4 management system as well.

• Provisioning

This is a duty accompanying acquisition of address.

Registration of RIR database accompanying allocation of address shall be carried out (registration method is described later).

Moreover, DNS reverse resolution setting of acquired address shall be carried out. As necessary, transfer of the rights of allocated Prefix reverse resolution zone shall be set.

As provisioning at accommodating a customer, there are tunnel setting and static path setting.

・External connection

Peering information shall be updated.

Registration of RIR database of IPv6 address allocation information

Person Object application (example is shown above) for person in charge of allocated Prefix management (admin-c) and person in charge of technical operation (tech-c) shall be created and sent by mail auto-dbm@apnic.net. If there is no problem, APNIC NIC handle showing registration method of Person Object is received via mail within a few days.

inet6num Object application (example is mentioned later) of allocated Prefix information shall be created and sent by mail to auto-dbm@apnic.net.

Refer to the following site for explanation of application method (changing method of the contents).

http://www.nic.ad.jp/ja/translation/apnic/apnic-database-update-info.html

If there is no problem, notification of completion of registration is received by mail within a few days.

Description example of inet6num Object registration application

inet6num: 2001:db8:1::/48	― IPv6 Prefix
netname: JPNICTESTNET	― Name of network (voluntary, with capital)
descr: JPNIC IPv6 Test Network	― Description of network
country: JP	― Country of location (“JP” in the case of Japan)
admin-c: IG100-AP	― NIC handle of administrator
tech-c: HG200-AP	― NIC handle of operator
ev-srv:	― Name of DNS server (not necessary for inet6num in particular)
status: ALLOCATED NON-PORTABLE	― State of network “ALLOCATED NON-PORTABLE” in the case of allocation of address
remarks:	― Note (not necessary in particular)
notify: noc@nic.ad.jp	― Address of ISP staff in charge of application Normally upd-to: of Maintainer Object shall be written.
mnt-by: MAINT-JP-JPNIC	― Maintainer Object of ISP shall be written.
mnt-lower: mnt-by. (Not necessary in particular)	― Lower Maint. Object when it is not authenticated with
mnt-irt: of now)	―Computer Security Incident Response Team (CSIRT) For security incident (not necessary in particular as
changed: noc@nic.ad.jp	― Address of a person who changes information Normally upd-to: of Maintainer Object shall be written
source: APNIC	― Name of registration database “APNIC” in the case of provider specified by JPNIC

IPv6 address management tool for LIR

This is a management tool that supports the procedure from acquisition of IPv6 address to management in the IPv6 address acquisition organization (LIR). This is developed by IPv6 Promotion Council of Japan, and is useful for organizations that will acquire IPv6 address and need to control IPv6 in the future.

A document that covers the matters related to application of address from application method of address to registration with database of /48 Prefix site is attached. This is useful for organizations that already have an IPv6 address management system or that carry out IPv6 address management using the system already set (IPv4 management system).

Refer to URL shown below for details.

http://www.v6nic.net/system/index.html

Trouble shooting

Routing

Q: What shall we do for a path used to advertise to peer?

A: Normally, AS that is aggregated with /32 Prefix is advertised (some AS have /35 Prefix due to historical circumstances, or some AS have shorter Prefix than this). It is normally recommended to cut out /48 or /64 Prefix from Prefix held by own AS and to flow them randomly.

Q: Unknown /48 or /64 is flowed from the neighbor ISP…

A: As a special usage, APNIC or so on sometimes allocate a Prefix like this. You can research database of RIR using whois, and if it is not a suspicious route, there is no particular problem.

You can find information on allocation state of IPv6 Prefix at each RIR including special usage at the URL shown below as well;

http://www.ripe.net/ripencc/mem-services/registration/ipv6/ipv6allocs.html

If fine Prefix apparently cut out from /32 is flown, you can filter relevant Prefix on In side of BGP setting.

Addressing

Q: We have a problem of addressing allocation.

A: When controlling data center in units of /56 for instance, if 2001:DB8:0:0000::/56 is set

for a segment of network equipment and 2001:DB8:0:0A00::/56 is set for a segment for server, management table of/64 doesn't become too large, and it will be easily recognizable whether it is server or router by reading the first part.

In the case of IPv6, management of IPv6 Prefixes in a phased manner is important know-how. It has an advantage that trouble shooting is easy to carry out.

Operation

Q: If trouble is suspected, when the operator checks the normality of the service, where should the operator try Ping or HTTP Get?

A: We recommend selection taking into account the connection point with Peer. Generally, www.v6pc.jp or www.kame.net is used.

Ping for general web site doesn't require the operator to have special technology, but it has the disadvantage that it is difficult to detect path trouble. It is important to check the normality of the service while considering where your own network carries out Peer. We recommend checking using traceroute as well.

However, you need to pay attention to HTTP Get because it is not possible to specify address directly using literal format (*) in many cases in the world of IPv6.

In the case of a browser that uses engine of Internet Explorer, it is not possible to access in literal format at present. However, this format is sometimes supported, such as in Firefox1.0, which is a browser using Mozilla engine.

(*) Literal format is the format of http://[IPv6 address]/ (e.g.: http://[2001:DB8::1]].

APNIC registration

Q: I can not register reverse resolution DNS server.

A: For reverse resolution domain registration of APNIC, behavior of DNS shall be checked using a script. If registration is not complete to the end, check the following items of DNS server.

- Is it possible to draw IP address for FQDN of DNS server?
- Is there any Internet connectivity to DNS server?
- Has DNS server started?
- Is SOA record for reverse resolution domain set?

Contents are mentioned in the error message as well, so check the comment and treat it, then carry out registration work again.

Investigation Members of DP-WG ISP segment

(Titles omitted)

Members of 2003

Chair of SWG

Tetsuya Nakai (NTT Communications)

Reader

Address & Routing

Ishihara (KDDI)

Network

Ishikawa (NTTPC Communications)

Matsudaira (Fujitsu)

Server

Tachibana (Aniani.com)

Investigation members (titles are omitted/in the order of Japanese syllabary)

Aramo (Intec NetCore, Inc.)

Ishihara (Toshiba)

Inomata (Fujitsu)

Okamoto (eAccess)

Kanayama (Intec NetCore, inc.)

Kunitake (RINT)

Suzuki (Hitachi)

Suda (Chita medias network)

Takeyama (eAccess)

Nakahara (NEC)

Nanba (Furukawa Electric CO, Ltd.)

Matsuoka (NTT PF)

Member of 2004

Chair of SWG

Kiyoteru Ishihara (KDDI)

Investigation members (titles are omotted, in the order of Japanese syllabary)

Araki (Japan Telecom)

Arano (Intec NetCore, Inc.)

Iizuka (Poweredcom)

Ishii (Internet Multifeed)

Ishihara (Toshiba)

Ito (IPv6 Promotion Council of Japan)

Inaba (TOKAI)

Ota (NTT East)

Otsuka (NTT West)

Oka (Toshiba Solution)

Okimoto (NTT West)

Kawashima (NEC Access Technica)

Kawashima (Cisco Systems)

Kitamura (NTT West)

Kitou (Allied Telesis)

Kunitake (Anchor Technology)

Gotou (Fujitsu)

Koyama (Kurashiki Cable Television)

Sato (Allied Telesis)

Sato (NTT East)

Suzuki (IIJ Technology)

Suzuki (NTT Communications)

Suzuki (Hitachi)

Suda (Chita Medias Network)

Tomikawa (IIJ Technology)

Nakai (NTT Communications)

Nakahara (NEC)

Nanba (Furukawa Electric CO, Ltd.)

Nishino (eAccess)

Nishimoto (eAccess)

Hiromi (Intec NetCore, Inc.)

Hosono (NTT East)

Matsumoto (Intec NetCore, Inc.)

Matsumoto (Japan Telecom)
Mizutani (Cisco Systems)
Minato (Fujitsu Access)
Mouri (NTT Communications)
Yamamoto (NTT East)

Inquiry

Please direct any inquiries about this guideline to the following address.

IPv6 Promotion Council of Japan DP-WG / e-mail: wg-dp-comment@v6pc.jp