2005 Version

IPv6 Deployment Guideline

Tips for Design and Operation of IPv6

March 2005

IPv6 Promotion Council of Japan
DP-WG

Table of Contents

Network Management

Address Management Database

Status of IPv6 support by the various management databases of providers

It is now a common concern for operation side such as ISP and IDC what a good management method for IPv6 address is. This issue is basically depends on providers. If the scale is small, it is possible to support forcibly using Excel, etc., but if the scale is large, bankruptcy occurs unless RDBMS is used fully.

There are no package products of various management DBs at present. Each provider customizes them, and it is considered that this state without general-use package products will continue even if IPv6 becomes most popular. Therefore, it may be necessary to research the IPv6 supporting status of RDBMS as well.

IPv6 Promotion Council of Japan publishes the IPv6 address management tool.

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

IPv6 supporting status of management tools

Open source type

The following open source type management tools support IPv6.

Nagios (http://www.nagios.org/)

ping6, Port monitoring (nagios-plugins-1.4.0alpha1)

Argus (http://argus.tcp4me.com/)

ping6, Port monitoring

AS Path Tree (http://carmen.ipv6.tilab.com/ipv6/tools/ASpath-tree/)

Management tool for BGP4+ (Indicate topology based on routing table of BGP4+)

MRTG (SNMP over IPv6)

net-snmp (SNMP over IPv6)

Some satisfactory ones are now available.

Commercial type

The following commercial type products support IPv6.

HP OpenView

Eden

Ciscoworks (planned to support)

IPv4/IPv6 translator type

The existing IPv4 monitoring tool now supports IPv6 by using a translation function. This method is not recommended because there is a concern about stability.

IPv6 Management Gateway

http://www.ipv6.man.poznan.pl/6net/mg6-frame/index.html)

IPv6/IPv4 translation of ICMP and SNMP

Yokogawa Electric Corporation TTB, etc.

Reference URL

http://6nettools.dante.net/cgi-bin/moin/moin.cgi/WortIndex

http://tools.6net.org/toolsList/

http://www.idg.co.jp/nw/service/service.html

Network Design

Addressing of Router, Communication Devices

It is recommended to set the address of router and server manually. Because, in the address auto configuration using EUI-64, when NIC is changed, address is changed.

In order to reduce trouble with DNS registration and filtering setting, it is effective to devise a naming rule that is easy to understand.

Expression of port No. or name by combining 0~9 and a~f such as ::1, ::53, ::80, ::cafe freely.

Expression of ATM link between Tokyo 03-Hiroshima 082 using :c726:a00:3:82, etc.

However, it should be remembered that this sort of easily understandable address can also be easily targeted by attacks.

Renumbering Method

It is possible to renumber through the coexisting process of new and old addresses using the fact that it is possible to assign multiple IPv6 addresses to the same interface.

As the procedure, the new address shall be acquired at first and then connectivity (routing) shall be set using the new address. Then the new address shall be assigned to IPv6 node (router and terminal). At this time, old address shall be left without deleting. At the terminal level, address auto configuration is used. Along with this procedure, DNS registration shall be changed as well. Next, the old address shall be deleted and connectivity of old address (routing) shall be deleted.

According to the procedure shown above, it becomes possible to carry out staged renumbering with less influence of discontinuance of service, compared with renumbering of IPv4.

The following Internet Draft is available.

Procedures for Renumbering an IPv6 Network without a Flag Day

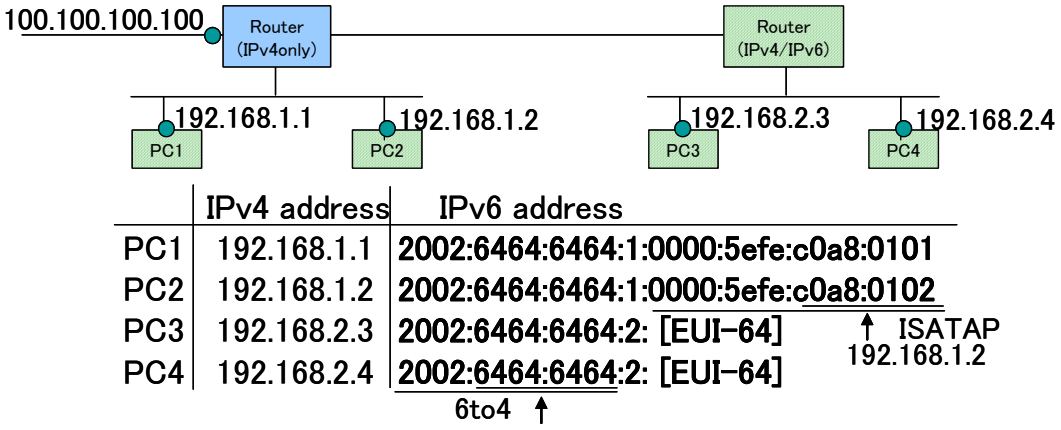
（Draft-ietf-v6ops-renumbering-procedure-01.txt）

IPv6 Local Address Assignment Method Inside Enterprise

It has been officially decided not to use “site local address” that was considered as the address that was earmarked for usage in private IPv6 networks. If so, what can we assign as an IPv6 address when we deploy IPv6 experimentally in the closed area network?

(1) Usage of global IPv4 address and 6to4 address creation rule

Under this rule, address will not be duplicated even if IPv6 local address setting information remains after official IPv6 address is acquired when the target network is connected to the Internet in the future. In the case of 6to4, combination of 2002:: and IPv4 address of 6to4 relay router expressed in hexadecimal is used as a network prefix. As shown in the Fig. below, it becomes possible to realize communication between IPv4/IPv6 dual stack terminals in the organization under addressing based on the rule of 6to4 using IPv4 address of router.



2) Global unique local address (fc00::/8, fd00::/8)

Global unique local address is assigned for private network as a sole address in the world, as an alternate to site local address. However, the discussion about this has just started at IETF, so it is not recommended to use it at this stage.

Network Topology of Dependent SOHO

It is considered that the communication form between dependent SOHO and headquarters will change along with the progress in deployment of IPv6.

Along with migration to IPv6, it is expected that the number of cases using not only application of former client server type but also P2P application such as IP phone will increase in SOHO that depends on IP network for all communication.

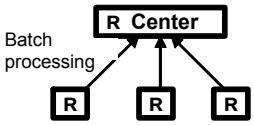
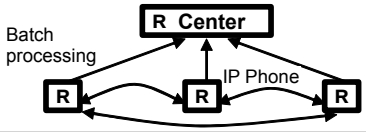
In the case of former star type connection, when P2P application is used, communication is concentrated on one place and there is a risk of deterioration of quality.

Mesh type connection that enables P2P connection between bases becomes necessary, so the connection form is required to enable usage of star type and mesh type simultaneously.

Change of topology by deployment of IPv6

- Change of topology in dependent SOHO
  - Along with increase in communication between bases, mesh type is used at the same time taking into account of quality.

Phenomenon	Present	BCP	Future
Center (HQ or ISP)	Connection from bases is concentrated by client server type communication.	Along with usage of broadband at bases, processing load on machines at Center increases.	Only acquisition of information held at Center is provided to the bases.
SOHO base (dependent SOHO side)	Communication is made only with Center.	Communication between bases increases along with usage of IP phone and P2P application. In the case of star type, Center becomes bottle neck.	Communication can be made freely among bases apart from the when connection to Center is necessary. VPN connection is used between bases.

Change of network topology	Star (hub & spoke) type	Mixture of star type and mesh type	
Change of application usage style	Base accesses only a server situated at Center.	VoIP or P2P communication is used frequently after deployment of IPv6.	Sensor network, etc. (communicate information to bases mutually and directly in order to acquire).
Change of VPN termination (when IPsec is used)			

(12/9) Migration period from Star type →Mesh type is set at the middle of "Next". ⇒ is added to express the state of migration.

Multi Homing of Company

The main purpose of multi homing in company is to utilize lines for each purpose (dedicated line is for SNA and ADSL line is for web or mail, etc.) and to secure backup communication route (ADSL, ISDN, etc. as a candidate). Moreover, distribution of the load and optimization of performance will be the objective.

The following are the requirements of multi homing summarized for each purpose.

Utilization of lines for each purpose

In this case, it is necessary to be able to choose different lines for each purpose (application). If it is the same application regardless of whether it is pull or push, the same line shall be used for coming and going.

Securing backup communication route

This is a method of using another line if one line is no longer usable. Therefore, when

the main line is usable, the other line (for both directions) should be set not to be used. It is also necessary to avoid cutting off the session when switching lines.

Multi homing technology/technique (outbound)

The following techniques are available for outbound multi homing.

Setting different gateways for each terminal

This is a method of separate lines being used for each terminal.

Allocation by a terminal

One of them is a method where terminal itself allocates according to the destination address. In this case, terminal has other paths than default gateway.

The other method is that terminal carries out policy routing (allocation by application).

Allocation by gateway (router, load distribution device)

Allocation method according to destination address, policy routing (allocation by application and sender address) and random load distribution such as ECMP are included in this category.

Inbound DNS

This is the method to change the responding address (dependent SOHO) according to the purpose (FQDN). Multiple number of addresses can be set for backup or distribution of load.

VRRP, HSRP, ESRP, etc.

These are the protocols used to secure redundancy of network devices used for backup. There are routers to which extension function such as dummy down of router at disconnection of line is installed.

Multi homing technology/technique (inbound)

The following techniques are available for inbound multi homing.

BGP

In this case, the number of paths increases, therefore this is used only on large scale networks.

Supporting ISP individually

Paths are fed to each other between ISPs locally.

Technology to change address at the middle of network

NAT, proxy and tunneling is considered for this technology.

Outbound DNS

This is used to change the responding address according to purpose (FQDN). It is

possible to set multiple addresses for backup or distribution of load.

Multi prefix

This is a method to set multiple prefixes in the same link (interface). Multiple addresses are a precondition for IPv6, therefore this method can be used widely. It is possible for the terminal to choose source address according to usage.

Mobile IP

There is a method to dare to apply Mobile IP to a non-mobile terminal as well in order to utilize care-of-address.

Multi Homing of IPv6

With regard to SOHO, NAT is the only multi homing technique that can be used for IPv4 at present.

Because, it is not possible for SOHO to receive AS, and “punching hole” is viewed with suspicion. It is not common to set multiple addresses for the same terminal. To begin with, NAT is already performed even without multi homing.

However, this will cause a problem making usage of P2P application difficult.

On the other hand, multi prefix can be considered effective as a method for IPv6. The method of using RFC3178 (using secondary link) increases the cost.

This seems to be efficient for operation in dependent SOHO in particular by utilizing addresses for each service. In the case of pull type application, the function of source address selection becomes important.

Usage of multi prefix is currently investigated in multi6 WG of IETF, and the purposes alone have already been made into an RFC (RFC3582).

Source address selection for IPv6

Source address selection for IPv6 is made into RFC as “RFC3484 Default Address Selection for Internet Protocol version 6 (IPv6)”. Here, the following 8 points are defined as rules for selecting source address.

1. Same address as destination takes priority
2. Address close to destination in the sense of scope takes priority
3. Non-deprecated address takes priority
4. Home address takes priority over care-of address
   *Mechanism capable of turning back with application should be provided (SHOULD)
5. Address of interface sending the packet takes priority

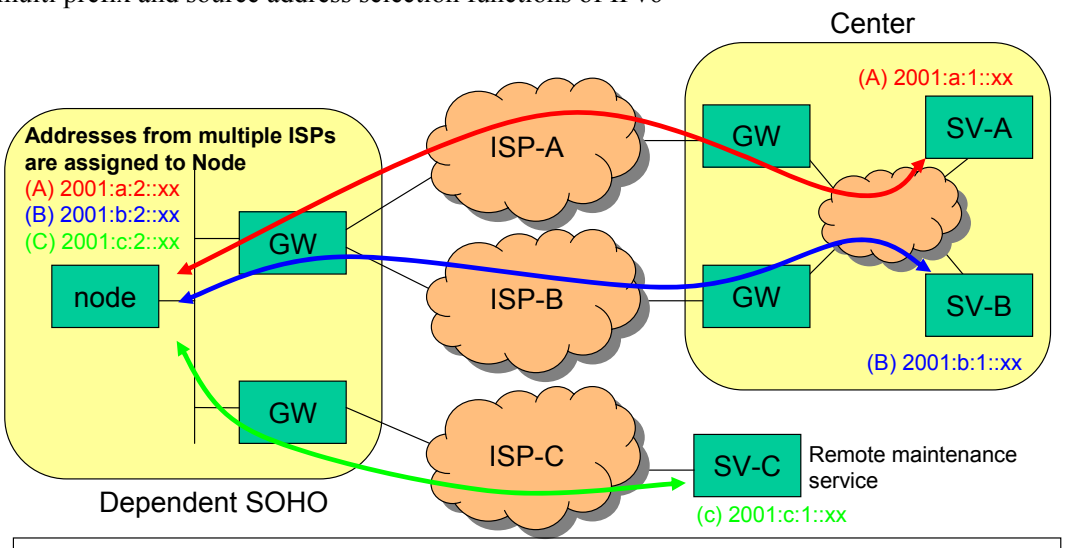
6. Address with the same label as that of destination on the policy table takes priority
7. Public address takes priority over temporary address
   *Mechanism capable of turning back with application should be provided (MUST)
8. Address with long consistencies with destination takes priority (longest match)

Among the 8 rules mentioned above, rule 8 can be used in the present state to utilize for each application. However, it becomes necessary to design address systematically. The disadvantage of rule 6 is that all terminals need to be set.

Configuration example of multi prefix/ multi homing

In the Fig. shown below, addresses from multiple ISPs are assigned to single terminal in dependent SOHO, and this terminal selects the sender address using “source address selection” and communicates data.

□ Example of Multi homing configuration of SOHO network using multi prefix and source address selection functions of IPv6



- When accessing from base node to center server, sender address is determined according to source address selection function.
- Response from center server to base node is sent to the address of sender of node as it is.
- Possible to control communication path from base node to each server in both coming and going directions.

Issues of multi prefix /multi homing

Multi prefix and multi homing has issues mainly on selection of default router and switching the line.

Default router selection

There is a problem that if default router is separated for each line, it is unknown to which line data is sent. No standard is defined for RFC2461 (Neighbor Discovery) in particular.

If a router transfers communication to a line as it is, there is a possibility that the usage doesn't match and ingress filter of ISP catches it.

As a countermeasure, the improvement of implementation of terminal and incorporation of a system such as draft-ietf-ipv6-router-selection-02.txt (extension in which path is fed by RA) in which data is sent to a corresponding origin router of sending RA referring to source address can be considered. However, till then the only method we can use is to redirect on the router side.

Behavior at switching a line

If the address is not switched immediately when switching a line, ingress filter may catch the address of different line and communication may be discontinued. If breakage of a line is detected by a router, it is ideal if it is incorporated in RA, however, End-End is separate.

This is the same as the case when NAT is used for IPv4, but if the address is changed according to switching of line, session is cut off. The mechanism to maintain the session such as Mobile IP, etc. for instance is required.

Server System Control

Setting Method of DNS in Company

Setting of DNS server

Setting of normal resolution

IPv4

・A record

www IN A 1.2.3.4

IPv6

・AAAA record

www IN AAAA 2001:db8::80

・It is better not to use A6 record.

Setting of reverse resolution

IPv4

・ in-addr.arpa domain

4.3.2.1.in-addr.arpa IN PTR www.hogehoge.jp

IPv6 （→refer to Security Guideline）

・ip6.arpa domain

・It's better to set ip6.int for compatibility in the past.

0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6

.arpa IN PTR www.hogehoge.jp

<The idea of IPv6 address registration>

When the existing service in which IPv4 address is registered with DNS is made to support IPv6 additionally, following 2 methods can be considered.

(1) to register the same domain name as A record with AAAA record as well.

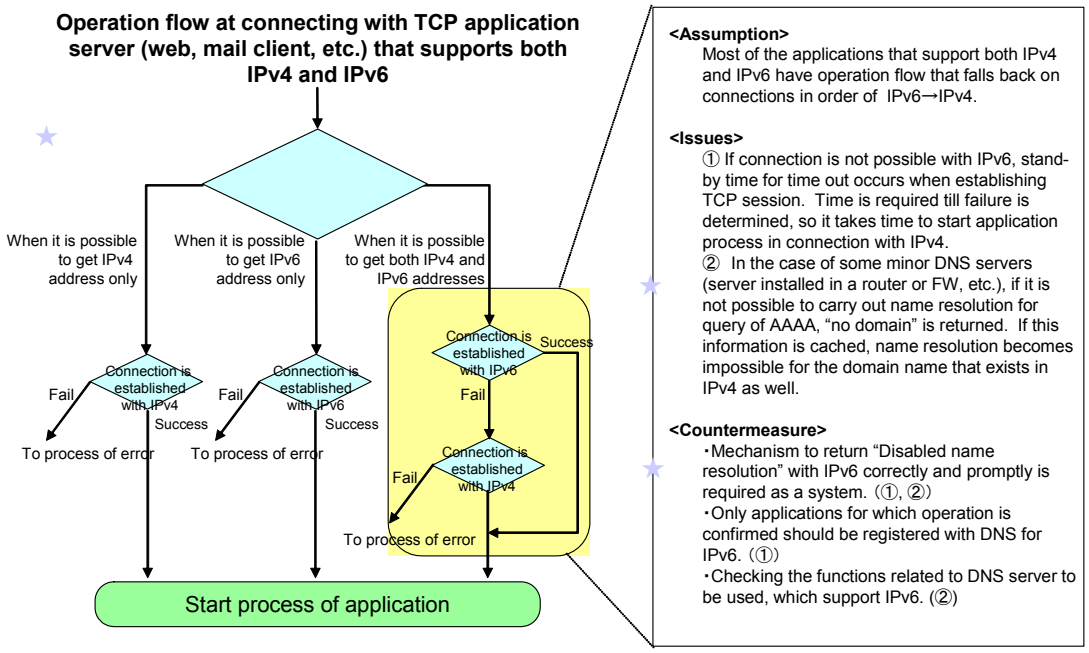
(2) to register different domain name from A record with AAAA record.

Generally speaking, when migrating from IPv4 to IPv6, it is better to use the method that doesn't require a user to utilize different domain names for IPv4 and IPv6 (1), but when continuing IPv4 service as well intentionally, it is possible to select (2).

Nonconformities caused by making DNS support IPv6

Most of the applications that support IPv4/IPv6 fall back on connection in the order of IPv6 →IPv4. The problem here is that time is required to time out with IPv6, therefore it takes time to start processing with IPv4. Moreover, some DNS servers return “no domain” if it is not possible to perform name resolution of IPv6, and disturb name resolution with IPv4.

<Nonconformity of DNS caused by deployment of IPv6>



Name Management of Information Home Equipment

Naming

For naming, equipment in the home needs to have functions to discover DNS server, perform registration and name resolution. The issue here is the how to discover DNS server, sending method of query and how to use transport protocol.

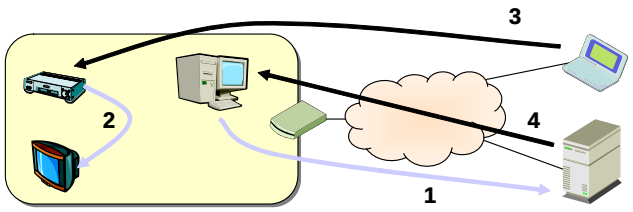
It is also necessary to clarify who should be capable of resolution (normal resolution) of whose name (for instance, whether it is necessary to be able to tell the address of the terminal inside home from arbitrary terminal outside of home).

Naming (continued)

- Functions: Registration/resolution, DNS server discovery, naming method
- Methods: Sending method of query, discovery method of DNS server, Transport protocol

- Classification according to purpose of name resolution

Case	Who	Solves whom?
1	Node at home	Node at home
2	Node at home	Node at home
3	Node at home (with confidential relationship)	Node at home
4	Node at home (without confidential relationship)	Node at home



- Case 2 is associated closely with Service Discovery.
- For Case 3 and 4, it is necessary to discuss the provision method of information to node at home and the safety of provision.

Issues of name resolution at home (Case 2)

- When node at home wants to resolve node at home, the following matters should be investigated.

◆DNS server discovery process
- ➢Multicast
- ➢Anycast
- ➢Auto setting protocol
- ➢Manual setting
- ➢Server unnecessary method

◆Registration of machine information
- ➢Name of machien
  - – Framework of DNS
  - – Framework of other than DNS
- ➢IP address
- ➢Other additional information

◆Query model
- ➢Multicast
- ➢Anycast
- ➢Unicast
- ➢ICMPv6 Node Information Query

◆Domain name
- ➢When framework of DNS is used
  - – Which domain should home use?
    - » To be assigned by ISP?
- ➢Users name randomly?

Countermeasure plan for name resolution at home (Case 2)

DNS server discovery process

In order to use DNS, a terminal needs to know the address of DNS by some means. However, there is equipment that doesn't have interface to be set at home, therefore it is necessary to set this information automatically.

There are some methods of auto setting. When well-known Anycast or Multi cast is used, it is necessary to consider security issues.

In the IETF draft, Router Advertisement, DHCP and well-known multicast are listed up.

There is a possibility that a method that does not use DNS server may appear.

- DNS server discovery process
  - Existence of machine that has no I/F to be set⇒necessity of auto setting
  - Possible to omit setting by using "Well-known Anycast and Multicast"
    - Necessary to investigate security.
  - Discussion by IETF (draft-ietf-dnsop-ipv6-dns-configuration)
    - the following 3 methods are listed up, and not limited to one.
    - Advantages and disadvantages of each method are sorted.
    - RA
    - DHCP
    - Well-known multicast
- There is a possibility that a different method that doesn't depend on DNS server appears
  - When a scenario for IPv6 deployment driven by non-PC is made

Query model

In the case of multicast DNS, it becomes necessary to support at individual node level and to have a server for external inquiries. ICMP Node Information Query (NIQ) is not DNS for a start, therefore program needs to be revised. Anycast DNS and Multicast DNS have security issues.

- Query model
  - Unicast
    - The same as existing DNS.
  - Anycast
    - Possible to use inside and outside servers together by using a server that supports recursive inquiries.
    - It is OK to distribute Anycast address with DHCP or it is OK to define “Well-Known” address (not defined at present)
  - Multicast
    - Each node needs to support muticast name resolution.
    - Server for resolving name through external DNS server is required.
      - Because inquiry is not transferred in the case of Multicast DNS.
  - ICMPv6 Node Information Query
    - Not DNS
      - Program needs to be corrected.
        - » Inquiry side: Necessry to modify a resolver so that it becomes possible to use as a regular name resolution mechanism on OS
        - » Response side: Necessary to support Node Information Query
  - Security issues related to Anycast and Multicast DNS
    - It is not guaranteed which server receives or which server sends a response in terms of protocol.

Registration of equipment information

Even for a PC, registration of IPv6 addresses is a hard job, and it is considered that there is equipment that has no mechanism to display or input. Therefore an auto registration mechanism is requisite.

In this case, even at home it is necessary to control the range where the registered information is disclosed. It is assumed that the machine model name is used for the name, however, if there are more than two items of the same model at home, there may be an issue as to how to distinguish them.

- Registration of machine information
  - It is difficult to register IPv6 address with DNS (or equivalent means)
    - Existence of machine that doesn't have display or input device.
    - It is possible that many nodes are connected in the world of 5:5.
    - ⇒ Automatic registration method is necessary.
      - Linkage of detection of connection (change of address) and auto registration.
        - » DNS UPDATE, etc.
  - Physical position and supporting relationship
    - When considering the convenience of the user, it is preferable to use with a sense of "a camera at the entrance", rather than "camera01".
      - "camera01" is OK as information to be registered with DNS, but it is necessary to change in order to show the user.
  - Issues
    - To what extent can information be disclosed?
      - Handling of privacy.
    - Naming method: If there are multiple items of the same model, how are they distinguished?

Issue of name resolution from outside of home (Case 3, 4)

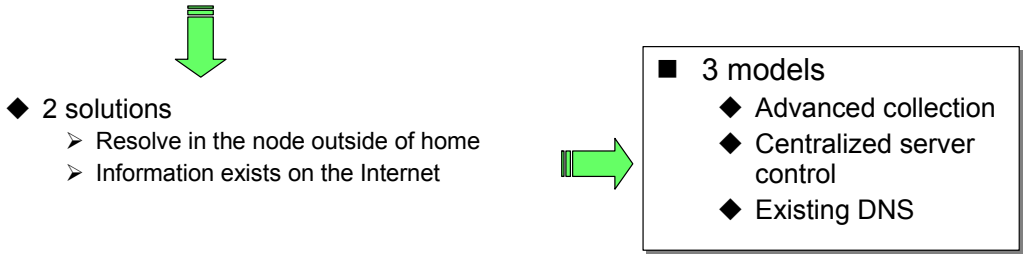
With regard to name resolution of terminal at home using terminal outside of home (equivalent to Case 3 and Case 4 in the table of "Classification according to purpose of name resolution" mentioned previously), it is possible to use the existing mechanism of dynamic DNS or DNS update for registration, however, the problem is what should be set as the registration destination. Moreover, it is necessary to set rules for registration information and target equipment for registration. From the view point of privacy protection, disclosure destination of information and disclosed contents are extremely important issues.

- When node outside of home wishes to resolve node at home
  - Registration
    - DDNS, DNS update
    - Registration destination
      - Server provided by ISP
      - Server provided by machine vendor
      - Server provided by a third person
    - Registration information
      - Determination of registration information/target machines for registration
    - Disclosure destination of information/disclosed contents
    - Securing privacy

Countermeasures for name resolution from outside of home (Case 3, 4)

It is not possible to operate a DNS server in regular home. Therefore, there are only 2 ways; whether it is resolved inside the terminal or there is information on the Internet. So, it is expected that 3 models will be used; advanced collection, centralized server control and existing DNS according to the usage.

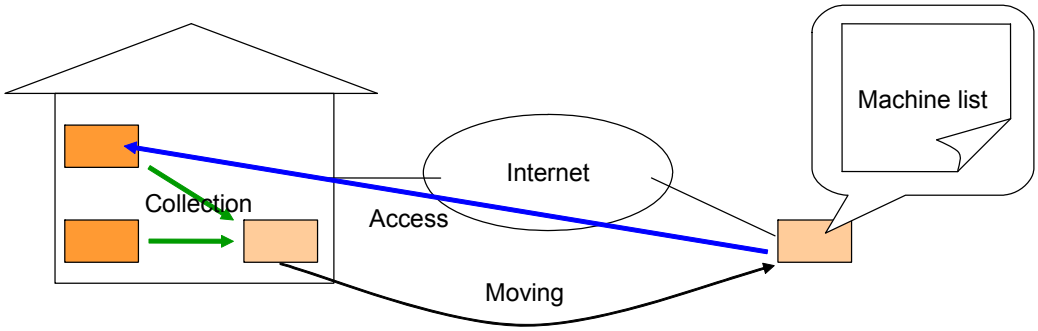
- Precondition: It is impossible to operate DNS server (for external disclosure) at a regular home
  - Transfer problem of domain name
  - Not possible to control
  - Relay of DNS query, simple DNS server for inside is used



Advanced collection model

In the case of the advanced collection model, it is considered that the equipment moving inside and outside of the home collects information of for instance /etc/hosts while it is at home and carries out name resolution using such information when it is taken outside. In this case, information exists only inside the equipment taken out, so it is safe. But, it is necessary to set each equipment. It is not possible to follow up a change of address after setting (after taken out).

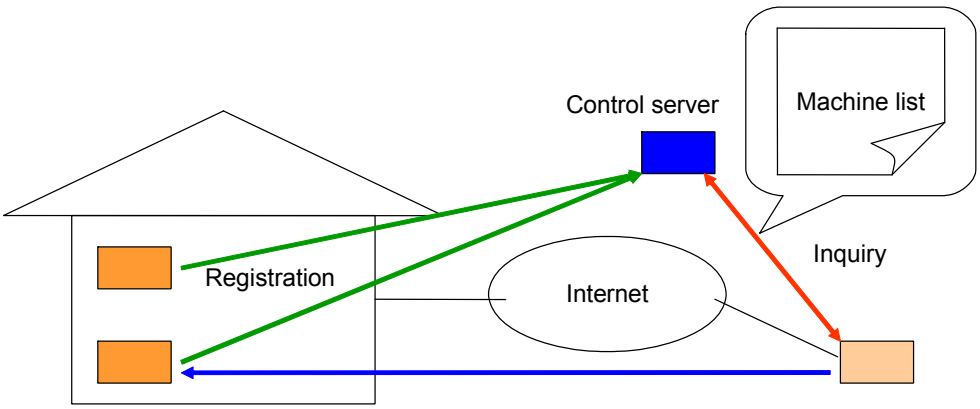
- Advanced collection model
  - For example, to have /etc/hosts.
  - Information exists only inside of node, so it's safe
    →It's necessary to set for each node.
  - Not possible to follow up a change of address after setting (after item is taken out).



Centralized server control model

In this case, DNS information is managed on the server set on the Internet based on some kind of contract. To this DNS server, only registered node is able to access. Registration may be carried out using dedicated software.

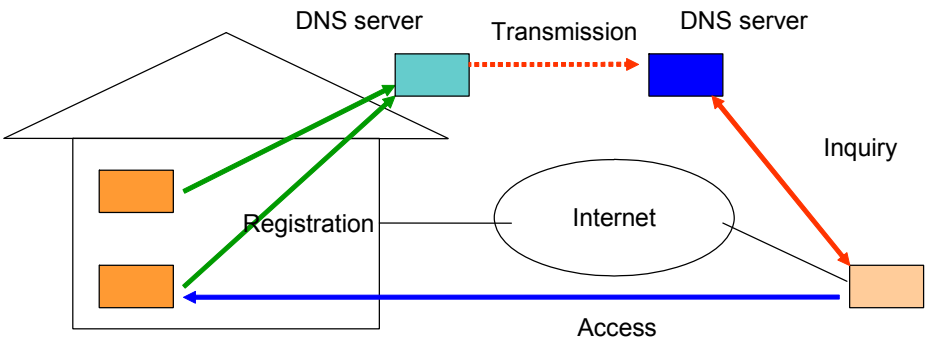
- Centralized server control model
  - Control on a server based on a contract
  - Only registered nodes are able to access
  - Dedicated software is used for registration?



Existing DNS model

In this model, registration is made with existing DNS server, and only registered node is able to access. However, the problems of how to automate the registration method (possibility of using dedicated software) and how to process the disclosure range of information and privacy problems are issues.

- Existing DNS model
  - Registration with DNS server
  - Only registered node is able to access.
  - Registration method (auto registration using dedicated software?)
  - Disclosure range of information/privacy issue



Other Naming issues

One of the other issues is how to treat transport protocol used for DNS related matters. Dual stack is preferable for this. Because, there will almost certainly be names that can be resolved only with IPv4 or IPv6. When considering about installation to a router for home, dual stack has no problems.

Another issue is a multi prefix / multi home environment. In the case of IPv6, multiple network prefixes may be assigned to one terminal. However, there are no clarified answers for how to utilize them by end node in order to select source address for application.

Moreover, DNSSEC is discussed for assuring security of communication related to DNS, but the discussion has not reached a conclusion yet.

Naming: other issues

- Selection of transport protocol

  ⇒Dual stack after all
  - It is desirable for server to support a wide range.
    - When considering installation on a router (for home), there is no problem with dual stack.
- Multi prefix / Multi home environment
  - PPPoE multi session is carried out for IPv4
    - A method to route DNS query properly is implemented.
      - Setting is carried out statically in many cases.
    - Because there is NAT, no problem is actualized.
      - End node doesn't need to consider multi home.
  - In the case of IPv6, selection of source address becomes important.
    - If DNS doesn't return appropriate response, selection of source address may not function properly.
- DNSSEC

With regard to automatic naming of non-PC equipment, it is an issue as to how to distinguish equipment if there are more than two items of the same model. Moreover, it is preferable to use names that are easy for users to understand, for instance when the names are displayed in the list with application. It is required to automate up to around this point.

- Naming of non-PC equipment
  - If there are more than two items of the same model (in the case there is more than one TV or video/DVD machine), how are they distinguished?
  - Easy naming is preferable for a user when names are displayed in a list using an application.
    - It is preferable to maintain correlation with the position of the equipment in the home.
      - Camera at entrance
      - Air conditioner in living room, etc.
  - If it is possible, automation is preferable.

Usage Model

Remote Monitoring, Remote Control

Demand for device monitoring and remote control

There is a demand for outsourcing of IT control including remote support for printers and software maintenance of PC terminals. In the case of SOHO in particular, it is often necessary to outsource these control operations, and the control level is improved by outsourcing.

For remote monitoring and control, communication with machines inside LAN and external machines becomes necessary.

Form of machine monitoring, remote monitoring

There are Pull type and Push type remote monitoring and control.

Pull type

In this case, only the machines inside the LAN can be initiators. It is an advantage that this type can be realized using the former security framework, however, there are disadvantages such as occurrence of delay in communication and wasteful consumption of band width.

Push type

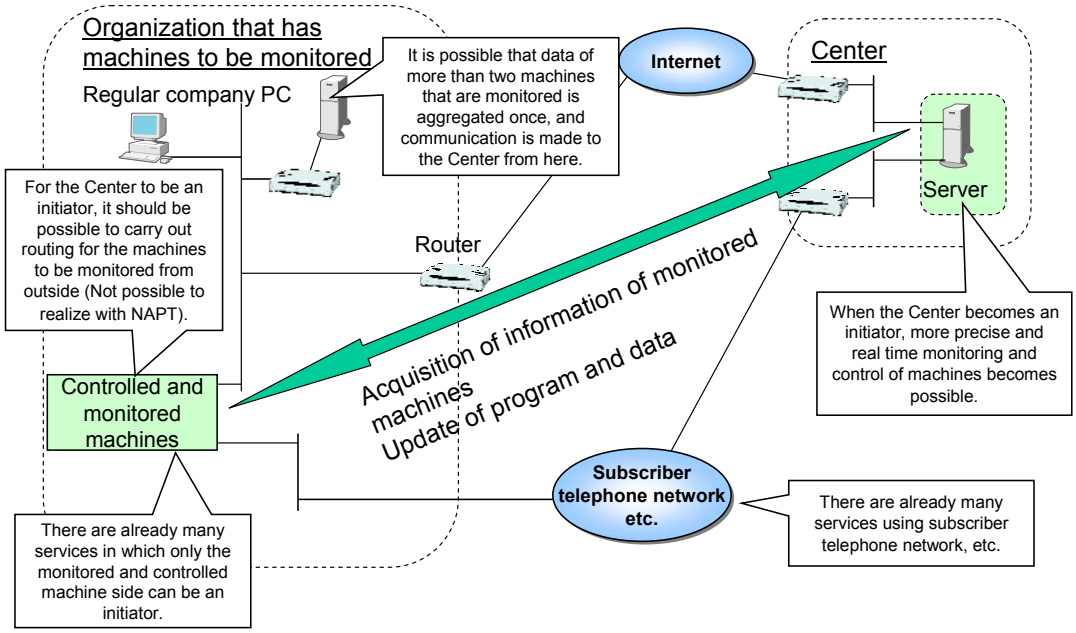
In the case of this type, not only machines inside LAN but also external machines can be initiators. This type has higher implementability when it is used for IPv6 to which routing can be done from outside. This type provides the possibility of various new businesses.

Concept of machine control and remote control

The Fig. shown below illustrates remote monitoring and control.

There are many remote monitoring and control services using telephone lines. When the Internet is used, only pull type machines, i.e., target machines for monitoring and control can be initiators in many services. If the control center becomes an initiator, secure service with excellent real time performance can be provided.

Concept of machine control and remote control (continued)



Example of problems of Pull type and advantages of Push type

As shown in the present Windows Update, delay in execution of countermeasures or non execution of countermeasures can be pointed out as disadvantages of Pull type. This is shown by the fact that there are still Blasters and Nimda.

Well then, what will be the state if Windows Update is Push type? You will be able to communicate with a communication partner without delay and the items that are not updated are controlled by the center, besides, it will be possible to take measures such as sending update CDs free of charge in environments where update could not be performed.

As described above, when using real time control service, outsider has to be an initiator. Outsourcing of server control (“telnet” of a server from outside) falls into this category.

Network used for monitoring

Various networks are used for remote monitoring and remote control.

Non-IP network (phone, etc.)

This network has high value, but also has the problem that it is difficult to carry out transparent communication using IP.

Dedicated line, wide area Ether network, IP-VPN network, etc.

In these cases, cost vs effect is low unless the scale is large and control is troublesome.

Internet VPN network

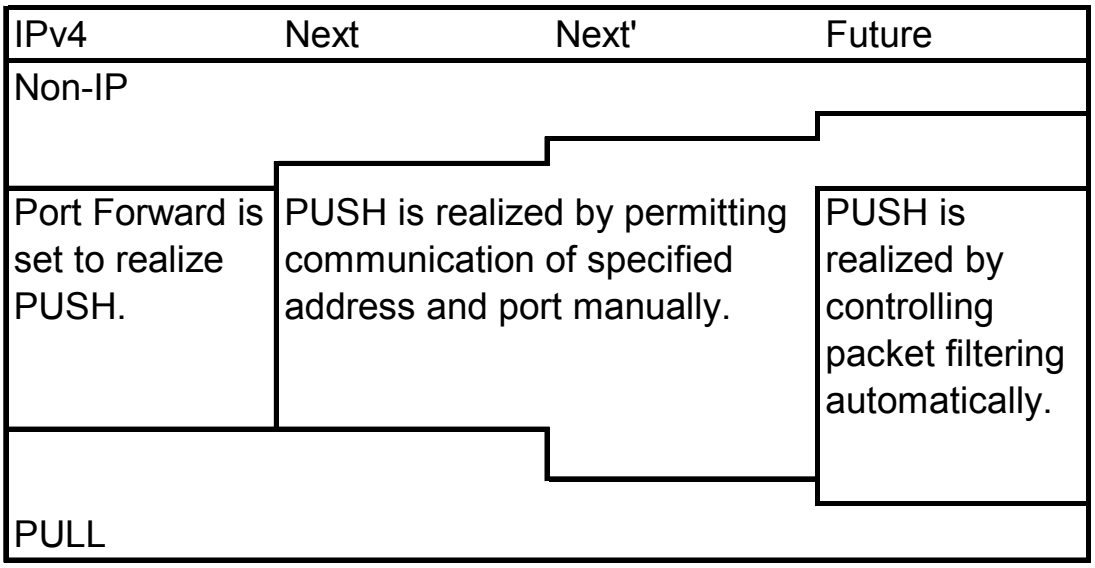
Price is low, but it has the disadvantage of tunneling and cost is incurred for devices.

Monitoring communication in IPsec transport mode

Price is low, but Push type communication becomes necessary. However, if there is E2E communication, control is easy.

Technology for construction of machine monitoring path

Pull type is mainly used in the present world of IPv4. However, by applying the technology to create a monitoring path gradually, it becomes possible to deploy to Push type service with IPv6. At first port transfer shall be set, and then, you move to the stage where communication of port is permitted manually, and in the end it should be possible to realize Push by automatic control of packet filtering.



Former technology using IPv4

The former method using IPv4 has the characteristics shown below.

Pull type

Initiators should always be machines inside the LAN, and no external machine can be an initiator. It is easy to realize this type.

Push type

Non-IP line, dedicated line and IP-VPN network are used. Different network is connected only for the sole purpose of monitoring the terminal. Therefore, cost is high, and this type can be used only in an environment with a large scale monitoring system (difficult to use in SOHO).

There is Push by port mapping. With this port forward is carried out for relevant internal node. It is necessary to consider scalability. Moreover, skill above a certain level is required to control a network.

Change of former technology by deployment to IPv6 (BCP)

Pull type

The same as in the case of usage of IPv4.

Push type

Push is carried out via non-IP line, dedicated line or IP-VPN network. This is the same as in the case of using IPv4. It is possible to use on the Internet without special setting (P2P communication performance of IPv6). It is necessary to consider security of packet filter setting, etc. For this, you can limit reachability from outside, or so on.

However, scalability is low, and skill over a certain level is required for control. IPsec transport mode communication of E2E can be used as well.

Desirable technology for the future

Desirable technology for the future is one that realizes Push with a high degree of freedom. This technology is required to have a function to automate realization of limited reachability, which used be carried out manually by BCP, to authenticate the other part, to punch a filter and to recover the hole automatically after completion of usage. With this technology, it will be possible to carry out control according to the other party (result of authentication) or communication state. Technically speaking, this will be a similar protocol to SIP.

However, it is required to standardize the procedure of this sort of protocol. If the procedure is not standardized, standards unique to each manufacturer will be scattered, and cost will increase for both manufacturers and users. Moreover, with this method, the necessity for other methods will decrease.

Factors of Problems and Countermeasures

v6fix, Name Resolution

v6fix

As one of the WIDE projects, a project called v6fix (http://v6fix.net/) started.

This project is to resolve various problems related to IPv6, and name resolution issue is handled as the most important topic for this project.

As an effort towards documentation, “InternetDraft” was written.

draft-ietf-dnsop-misbehavior-against-aaaa-02

This will be RFC soon.

Guideline for execution is under preparation for publication at http://v6fix/net/. It is planned to start the research into the actual state inside Japan, and to reinforce it later. It is planned to request vendors and domain administrators to make an improvement as a result of research.

It is also planned to provide a library of BSD in order to handle on the implementation client side.

Present state of matters related to name resolution

Implementation state of IPv6

IPv6 is already implemented in many DNS servers and clients.

On the server side, BSD, Linux and Mac OS X support IPv6 as OS, and in the case of DNS, versions after bind9 and bind8.4 support IPv6.

In the case of client, Windows XP, MacOS X, BSD and Linux support IPv6 as OS, and in the case of browser, Internet Explorer, Safari, Mozilla and Firefox support IPv6.

Regardless of connectivity with IPv6, inquiries of AAAA occur on a daily basis.

Operation state of DNS

With regard to IPv6 implementation state of DNS, more than half of ccTLD servers (135/243 countries) support IPv6. The JP domain already started to support it a few years ago. gTLD (.com, .net) started to support it in October, 2004 as well. Support with root servers is also in progress.

Issue of DNS server that doesn't react to AAAA correctly

This issue relates to the response of a DNS when an inquiry about AAAA RR is made to a domain that has only A RR (typical domain that does not use IPv6).

Correct response (RFC1034)

The correct response is to return an empty response (no error) or to respond stating that other RR is available though AAAA RR is not available. According to this response, a client is able to make an of A RR inquiry separately and communicate with IPv4.

Incorrect response

There are DNS servers that ignore an AAAA inquiries. Due to this response, a long time out occurs (from a few tens of seconds to more than a minute).

Some DNSs return NXDOMAIN error. This indicates that there is no RR, so communication even with IPv4 will no longer be possible. Moreover, NXDOMAIN will remain in DNS cache of resolver, so a client that doesn't draw AAAA will be forcibly involved. This causes a denial of service attack in some cases (CERT recommendation).

Others

Handling of tunnel usage by ISP users

There is an issue for ISPs about how to handle usage of a tunnel by a user. Concretely speaking, it is an issue about the handling method of IPv4 Protocol No.41 packet (IPv6 capsuled packet).

First of all, when a tunneling service is provided, this packet is not filtered in the ISP network. Even if a tunnel service is not provided, it is recommended to avoid using filtering as much as possible because it will interfere with usage of 6to4, etc.

However, in this case, there is a weak part in terms of security as indicated in the Internet draft shown below.

Security Considerations for 6to4

（http://www.ietf.org/internet-drafts/draft-ietf-v6ops-6to4-security-04.txt）

The issue here shall be filtering with a tunnel router, for example putting IPv6 capsuled packet through only to the destination at the end of tunnel.

MTU discovery

In the case of IPv4 packet, it is possible to carry out Fragment even in the middle of path for delivery of packets, and no ICMP such as ICMPv6 Type2 is used. Therefore, ISP, etc. carries out filtering ICMP packet in some cases.

However, in the case of IPv6, no Fragment is carried out at the middle of the path for delivery of packets. When packet side becomes “Too Big” at the router in the middle of the path, the router returns Type 2 “Packet Too Big Message” of ICMPv6 to the sender. The sender receives this message, stores it in a packet of adequate size and sends it.

Therefore, this case should be handled carefully because if ICMPv6 message (Type2 at least) is not delivered to the end node on the IPv6 Internet, communication performance will be damaged.

It is necessary to carry out through operation including ISP, not to filter the ICMPv6 Type2 message (refer to Security Guideline).

Internet Related Technical Information

Historical Circumstances of sTLA Allocation

In the initial policy regarding allocation of sTLA (1999), the minimum size of initial allocation was /35. However, after it was revised (Jul. 1, 2002), it became /32. Along with this change, sTLA holders who have already acquired /35 became eligible to upgrade to /32, however, shifting to /32 is voluntary, so there are still some sTLAs that have /35 after the new policy is enacted. Therefore, at present, sTLAs with /32 and /35 exist together (Note: the word “sTLA” is not used at present, but here it is used for convenience in order to indicate the organization that receives allocation of address directly from RIR).

IPv6 Multicast

Multicast is a technology that enables transferring information efficiently from a sender on one machine to receivers of n machines by a router reproducing more than 2 packets at relay of packet.

This technology is effectively used for live broadcast of broadband content or simultaneous distribution.

At deployment of multicast, it is necessary to choose “Path control method” or “Group control method” to be used.

Path control method

Protocol used between routers in order to realize multicast communication.

PIM-SM

Most common protocol as of now, which is used for exchange of multicast path information.

PIM-SSM

With this, a receiver is able to join the multicast group after specifying a sender, and it will be possible to prevent multicast communication disturbance from illegal transmission terminals.

Group control method

The protocol used between router and host in order to realize multicast communication.

MLD(Multicast Listener Discovery)

−MLDv1: Multicast group control protocol supporting PIM-SM

−MLDv2: Multicast group control protocol supporting PIM-SSM

What are appropriate multicast methods as of now?

PIM-SM / MLDv1 is considered appropriate from the view point of practicability and diffusion. However, PIM-SSM / MLDv2 is excellent in terms of packet transfer efficiency and security.

Therefore, it is realistic to achieve IPv6 multicast using PIM-SM and MLDv1 for now and shift to PIM-SSM and MLDv2 in the future when the lineup of supporting products is enriched.

BSR and RP in PIM-SM

RP: A certain point of a router to which a transmission host sends a participation message to participate in multicast. In the case of PIM-SM, multicast packet is normally transferred via RP.

BSR: The router that notifies information of RP or BSR itself (IPv6 address, etc.) to all PIM-SM routers.

Multicast address

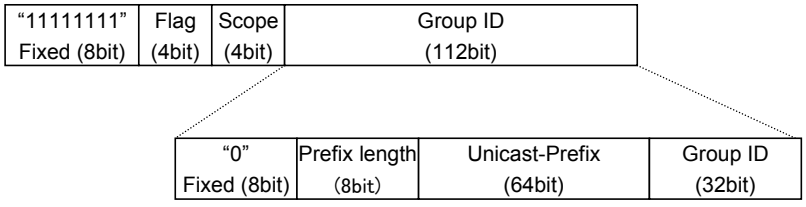
In the case of IPv6, as address space for multicast, ff00::/8 is prepared. For an example, in the case of IPv4, 224.0.0.0～239.255.255.255 (Class D) is an address for multicast.

Usage method of this address space shall be as shown below, for example when a user with 2001:db8:1234::/48 creates multicast address.

ff3x:30:2001:db8:1234::****:****

x: Specification of scope

*: Specification of group ID



The following is are special IPv6 multicast addresses.

ff02::/16: Multicast address of link local scope

ff0e::/16: Multicast address of global scope

Communication Quality Assurance of IP Network

As communication quality assurance measures of IP network, it is possible to use the following methods.

- Physical measures (increase in the band area, limitation of housing quantity)
- Realization using functions of network devices in ATM, SONET, Ethernet, etc. (scheduling of queuing, TDM (ATM, SONET), rejection of priority packet)
- For dynamic setting of devices, VLAN function, signaling (RSVP, etc.) or setting from control server (COPS, etc.) shall be used.

Communication quality assurance can be classified largely into QoS and CoS. Standard of quality varies (rejection of packet, delay, band area, jitter, etc.).

QoS：Quality of Service

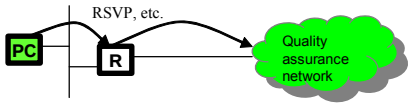
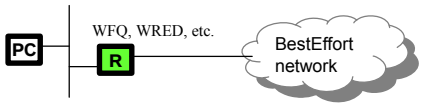
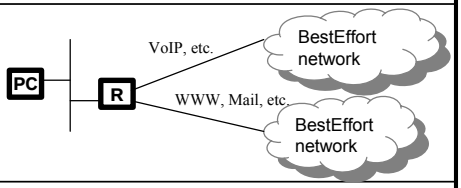
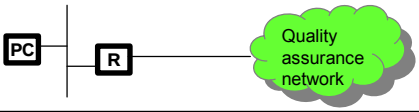
This service secures resources (band, etc.) for communication and assures communication quality. Real time application, etc. are the targets.

CoS：Class of Service

This service assures communication quality using priority order. Business applications, etc. are the targets.

Communication quality assurance pattern of SOHO

Communication quality assurance shown in the Table below is expected to be used in SOHO. It is not necessary to use methods independently, it is also possible to use them in combination.

Item	Contents	Outline diagram
Terminal	Terminal driven communication quality assurance system is used.	
Connection line	Quality assurance setting is carried out by a router (priority transfer, rejection of packet). Increase of connection line band is included as well.	
Multiple connection lines	Load is dispersed using multiple connection lines.	
Communication quality assurance network	Carrier prepares a network that assures communication quality.	

Above mentioned pattern shall be used independently or as a combination.

Communication quality assurance of SOHO

LAN

In LAN, it is possible to use sufficient band areas by reduction of prices of Gigabit Ethernet devices, so it is considered that there will be no large amount of demand for quality assurance technology.

WAN

Line speed of WAN connection is around a few Mbps - 100 Mbps, which is slow compared with a LAN and causes deterioration of quality easily. To handle this problem, it is possible to incorporate traffic spread method of inbound and outbound using multi-home.

The internal network of carrier is basically “Best Effort”, therefore quality is not assured. However, as a method to assure quality, it is possible to control outbound traffic at CE (customer edge) or, to construct network with communication quality assureable devices and provide function.

Features of quality assurance of IPv6

Header format of IPv6

2 fields regarding quality assurance are set in the IPv6 header.

Traffic Class field (8bit)

This is used for classification of class such as priority control. This is ToS (Type of Service)(8bit) in the case of IPv4.

Flow Label field (20bit)

This is used by a sender to specify processing method in units of flow.

Avoidance of packet division on network side

In the case of IPv6, packet is not divided by machines on a communication path. However, there are some caution points about this matter.

When a sending terminal sends a packet in a non-rejectable size, it is required that “Too-Big-Message” of ICMP reaches the sender from the machine on the path to which smaller MTU is set.

In this case, it is required to investigate the condition that ISP, etc. controlling machines on a path doesn’t block a relevant message or the decrease in security caused by the absence of blocking.

Features of each event of IPv6

IPv6 has features regarding quality assurance as shown in Table below when compared with IPv4. In general, more detailed and higher freedom of control is possible.

Item	IPv4	IPv6
Communication quality assurance of application	Possible to control 8bit (ToS) type on IP layer.	Possible to control 8+24bit (Traffic Class and Flow Label) type on IP layer.
Communication quality assurance in units of terminal (VoIP, remote maintenance, etc.)	Difficult to assure QoS of E2E due to concealment of address using NAT.	Easy to assure QoS of E2E by using global address.
Resource induction by terminal itself	Static resource induction that sets path for resource beforehand, or signaling of RSVP, etc. is used.	Dynamic resource induction using source address selection with multi prefix.
Avoidance of delay in processing by dividing packet	Because packet is divided or reconstructed on communication path, the number of delays in processing increases.	Packet is divided only by a sender, the number of delays in processing on path decreases.

- With IPv6, particle of QoS assurance can be more segmented and setting with higher degree of freedom (mapping of QoS of E2E, etc.) becomes possible.

Conclusions for communication quality assurance

Communication quality assurance of IP depends largely on the physical network configured. When deploying from IPv4 to IPv6, no change occurs in the physical network, therefore, it is considered that there will be no difference in quality assurance technology itself.

However, compared with IPv4, IPv6 has superiorities in terms of quality assurance such as particle segmentation, E2EQoS, resource derivation and packet division. When IPv6 is used, quality assurance targeting E2E will be easier including VoIP or remote maintenance in particular. Therefore, it will be possible to assure quality interlocking all configuration factors on E2E.

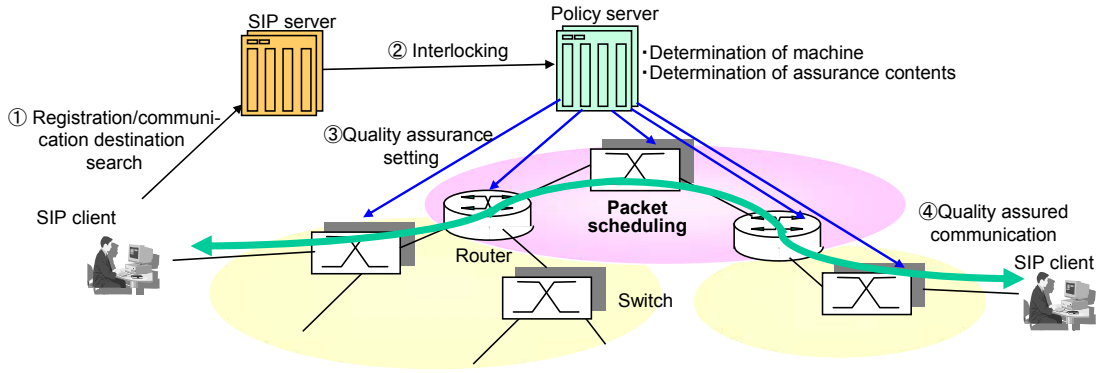
However, the problem is that there is no administrator who carries out design, setting and operation of quality assurance in the case of SOHO.

Communication quality guideline

Along with deployment to IPv6, it will be crucial to carry out quality assurance by discriminating mission critical communication from other communication in the case of SOHO that depend for all their communications on the IP network.

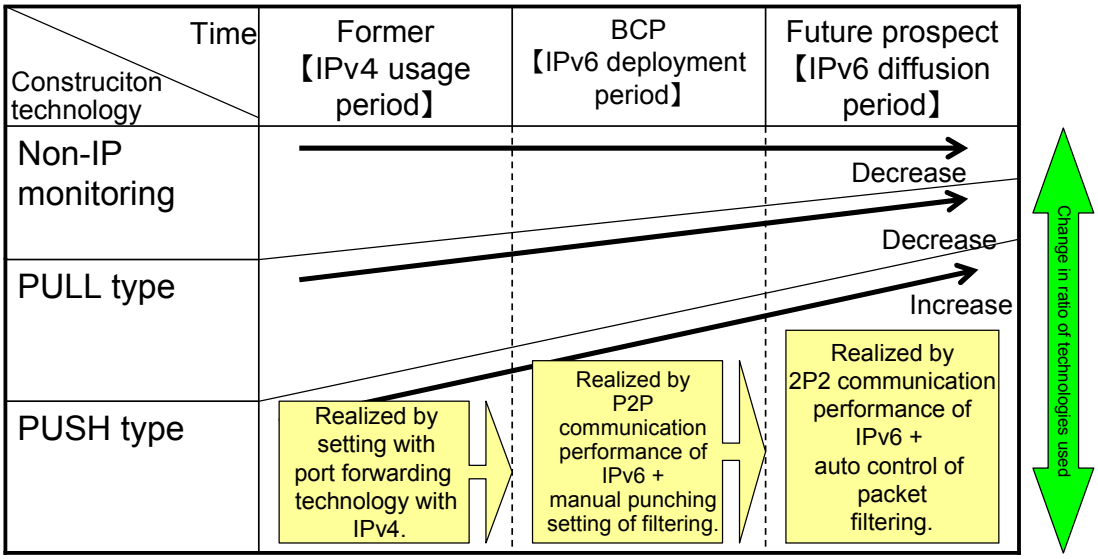
When IPv6 is used, segmentation of quality assurance will improve. However, in SOHO where there is no administrator, though quality assurance using LAN can be performed relatively easily, it will be difficult to assure quality of WAN.

Therefore, it is necessary to provide automated communication quality assurance to SOHO (Note: it depends on the usage method whether pay-as-you-go accounting or quantitative accounting is used for quality assurance service).



Change in Technology that Constructs Device Monitoring Path

Technology that constructs monitoring path of devices is explained in the section of remote monitoring and remote control, but it is considered that Push type device monitoring will increase gradually as shown in the Table below.



IPv6 Supporting State of Internet System

Classification of servers

Servers of ISP can be classified as shown below.

Service server

Application server that users actually use for web and mail. It is customized in various ways according to usage. For instance, there the web for advertisement of ISP, hosting, web or mail bundled to connection service.

Infrastructure server

This server is required commonly for usage of service, and DNS and Radius are included in this category. This server is required to have the highest reliability.

Operation server

This server is required for operation of ISP and NMX and SNMP are included in this category. This is not a target for users to access directly, therefore, it is not crucial to support IPv6.

IPv6 support of server

As the present state of server support for IPv6, many OSs used as a server are capable of dual stack configuration (Linux, FreeBSD, Solaris, etc.). Most of the existing IPv4 applications (web, mail, DNS, etc.) support IPv6. With regard to DNS and the web, results have already been achieved in provision of commercial and experimental service of ISP.

IPv6 supporting method

As configuration method of server, 2 methods can be considered; making IPv4 service server dual, and addition of new server dedicated to IPv6 service. If there is even a little anxiety over the influence of dual on performance of IPv4, the latter method should be selected. This is the same when the influence from discontinuance of service due to updating OS and application versions is large in the case that the dual method is selected.

Server shall be set at new dual segment dedicated to IPv6 service. This is because, if IPv6 server and IPv4 server that may have different supporting speed for vulnerability, etc. are stored in the same segment, IPv4 server will be affected. This doesn't require a large cost compared with backbone.

It is necessary to pay attention to filtering of ICMPv6 at IPv6 server segment. Fragment processing using IPv6 is not carried out at the middle node, but sender terminal divides it into deliverable size using Path MTU Discovery (ICMPv6 Type2 message is used), therefore it is not permitted to filter ICMPv6 Type 2 message with a router at the middle.

DNS

In the case of DNS supporting IPv6, it is required to be able to resolve IPv6 address and to execute it via IPv6. There are 2 kinds of name resolutions with IPv6; resolution of IPv6 address from host name (normal resolution, AAAA record) and resolution of host name from IPv6 address (reversal resolution, ip6.arpa.domain).

We recommend using BIND9 for DNS implementation. BIND9 supports IPv6 completely. Actual results are made through commercial provision. However, the same thing has become possible with BIND8 now. If it is just for name resolution, it is OK to use BIND4 (via IPv4).

As a method for ISP to support IPv6, because it is the most important server and is not allowed to disconnect a service, 2 new dual servers shall be prepared for IPv6 (primary, secondary). A server for controlling resolver and zone can be used by sharing.

This shall be provided as a resolver dedicated to IPv6. Inquiries via IPv4 should be made

thorough existing server. Moreover, according to requests of customers, transfer of reversal resolution or provision of DNS controlled by a customer as a secondary is carried out.

Web

The web server is classified into web for advertisement of ISP, web to be bundled to connection service and web hosting. Software supports IPv6 from Apache2.0 as standard, and there usage results with ISP have been obtained as well.

Support should start from the web for advertisement of ISP. There are no critical ones compared with DNS, however, if safety is very important, a new server of dual stack can be set up. If it is of a version after Apache2.0, it is possible to make an existing server dual as well.

It seems that it will take a little while for the web bundled to ISP service and web hosting to be made dual. This is because, in the case of middle and small ISPs, service of hosting provider is used in many cases and hosting providers have not changed to dual yet.

As a resolution at your own discretion, it is possible to set a new dual server, however, there are many servers and operation is required for moving contents, besides mirroring of content and a synchronization system become necessary, so the operation man-hours will increase.

On the other hand, as a realistic resolution, it is possible to set reverse proxy, which is made dual stack. With this, it becomes possible to provide access to an existing server of IPv4 from IPv6, and moreover, it will not be necessary to consider moving contents, which makes this a good solution at the stage when the number of accesses to IPv6 is still small.

Mail

Software of mail server supports IPv6 as a standard from Sendmail8.1. Qpopper is a patch supporting IPv6. However, compared with DNS and web, the usage results are limited.

With regard to the present BCP, anti-virus software has not supported IPv6 yet, therefore it’s better not to provide it as ISP service. Which means that the measures taken at present are avoiding making SMTP and POP servers support IPv6, or avoiding giving IPv6 addresses to MX record host name of DNS.

When the above mentioned issues have been cleared, there are 2 methods to support IPv6. First of all, when existing mail account is used, new dual server shall be set up and disc of existing IPv4 server shall be shared with NFS, etc. When a new mail account is used, a

new dual server shall be set.

Monitoring (NMS, SNMP)

With regard to IPv6 support of operation server (NMS, SNMP), based on the idea that a dual stack network is a precondition (ISP in particular), the number of products that support IPv6 completely is still small. IPv6 transport of SNMP in particular is implemented with very few managers and clients. However, if it is possible to get IPv6 MIB via IPv4, the problem will not be so serious.

Regarding reachability check, it is necessary to monitor connectivity (ping) with IPv6, therefore commercial tools already support IPv6.

It is necessary to carry out service check with IPv6, but commercial tools do not yet support this as of now. There are some tools that can be used free of charge. (Nagios)

Many ISPs have set new dual servers for IPv6 service now.

Inquiry

Please send mail to the address shown below for inquiries regarding this guideline.

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