Report
Study Group on Internet's Smooth Transition to IPv6
(Tentative Translation)

★June 2008

Study Group on Internet's Smooth Transition to IPv6

● Introduction

In Japan, Internet users exceeded 87 million at the end of 2006 ("Survey for trend to Telecommunications Services in 2006", Ministry of Internal Affairs and Communications). The number of permanent connection broadband service contracts exceeded 28.3 million at the end of 2007 (investigation by Ministry of Internal Affairs and Communications). Additionally, the market size of business-to-business electronic commerce through the Internet reached 148 trillion yen ("Market survey on electronic commerce, 2006", Ministry of Economy, Trade and Industry). The Internet is now indispensable for the social economy and the lives of Japanese citizens.

On the other hand, a quarter of a century has passed since the basic technology to provide Internet services, Internet Protocol version 4 (henceforth "IPv4"), was established in 1981. It is estimated that IPv4 addresses for the Internet connections will soon run short. Thus, difficulties in supporting further development of the Internet began to emerge.

In consideration of this situation, this study group examined the measures that are needed to overcome such restrictions in IPv4 and realize further development of the Internet, mainly from the technical perspective.

This study group met four times from August 2007 to April 2008, and the workgroup formed for examination of technical details convened 11 meetings. Between the meetings, the volunteer members of the workgroup held several brainstorming sessions. Thus, technical actions against IPv4 addresses exhaustion were examined in detail.

This report brings together the examination of these many meetings. It is the world's first report that comprehensively describes the actions that are necessary from a variety of related players to IPv4 addresses exhaustion. We hope that, based on this report, the parties involved in the Internet all over the world and in Japan will tackle the shortage in IPv4 addresses to ensure further development of the Internet.

Contents

1 Present Status of IPv4 address consumption

1.1 IPv4 addresses

At present, the Internet is realized based on a communication method (protocol) called IPv4 (Internet Protocol version 4). IPv4 transmits packets from the node (device) with the source address assigned to the node with the destination address assigned. The packets consist of the header section that contains information necessary for communication control, such as the source and destination addresses, and the payload section containing data. The addresses to assign to these nodes are called "IPv4 addresses." Because they are 32 bits of binary numbers, a maximum of 2^32 (4,294,967,296) addresses are available for use. Therefore, the network using IPv4 cannot connect 430 million or more nodes in principle. This means that, as long as the Internet continues to use IPv4 as basic technology, the number of nodes connectable to the Internet is limited.

IPv4 addresses are usually divided into 4 sets of 8-bit numbers, which are displayed in decimal numbers (0-255) (e.g. 192.168.255.0). To show a series of addresses, usually, several higher-order bits are fixed and lower-order bits are arbitrary (for example, top 16 bits are set as 192.168 and lower 16 bits can be used freely). RFC 4632 specifies that the size of the series must be indicated as "/x" using the number of fixed bits (for example, "/16" indicates that top 16 bits are fixed, thus showing a series of 65,536 addresses.) IPv4 addresses are basically divided into units of "/8" (the top 8 bits are fixed, showing a series of 16,777,216 addresses). A large number of addresses are represented in the unit of "/8." For example, the whole IPv4 addresses consist of 256 in "/8" units.

1.2 Current use of IPv4 addresses

There are almost 4,300 million IPv4 addresses, but about 610 million (more than 36 of "/8" units) of them are allocated for specific use by the standard. Furthermore, according to the rule before starting the general use of the Internet, 94 of the "/8" units were allocated by 1995 (four of them have been returned). The addresses allocated before defining the current allocation rule for IPv4 addresses are called the "historical PI (provider independent) addresses." Many of them have been assigned to U.S. government agencies and companies involved in the development of ARPANET, the precursor to the Internet (see Reference 1). The current allocation rule for IPv4 addresses was defined in 1996. By March 2008, 89 in "/8" units were allocated. The remaining IPv4 addresses are 41 in "/8" units.

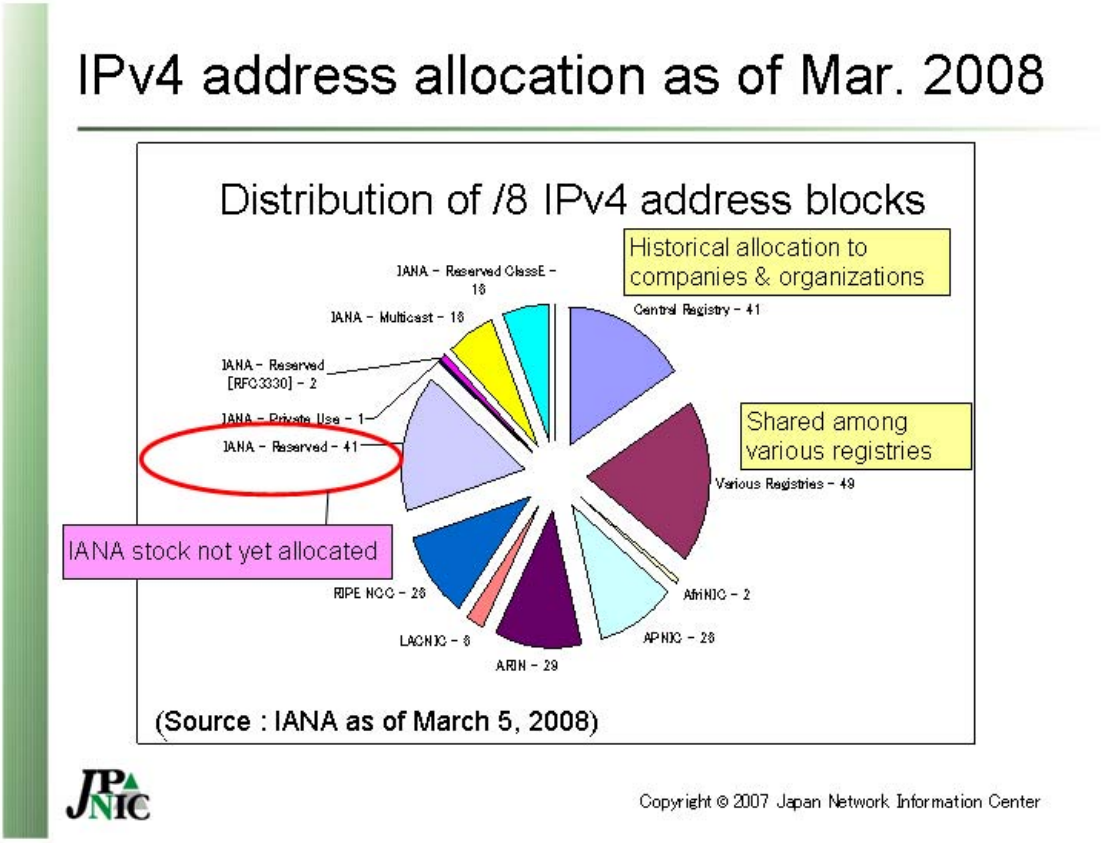


Fig. 1 - 1　Current IPv4 address distribution
(Based on the material from Japan Network Information Center)

１．３　New demands of IPv4 addresses

IPv4 addresses have been consumed 5 in /8 units from 1999 to around 2003 every year. However, the consumption increased rapidly from around 2004, now about 10 in "/8" units have been consumed every year. Because the remaining IPv4 addresses are consumed with the new demands of IPv4 addresses, they will run out in about four years if they are used at the current pace.

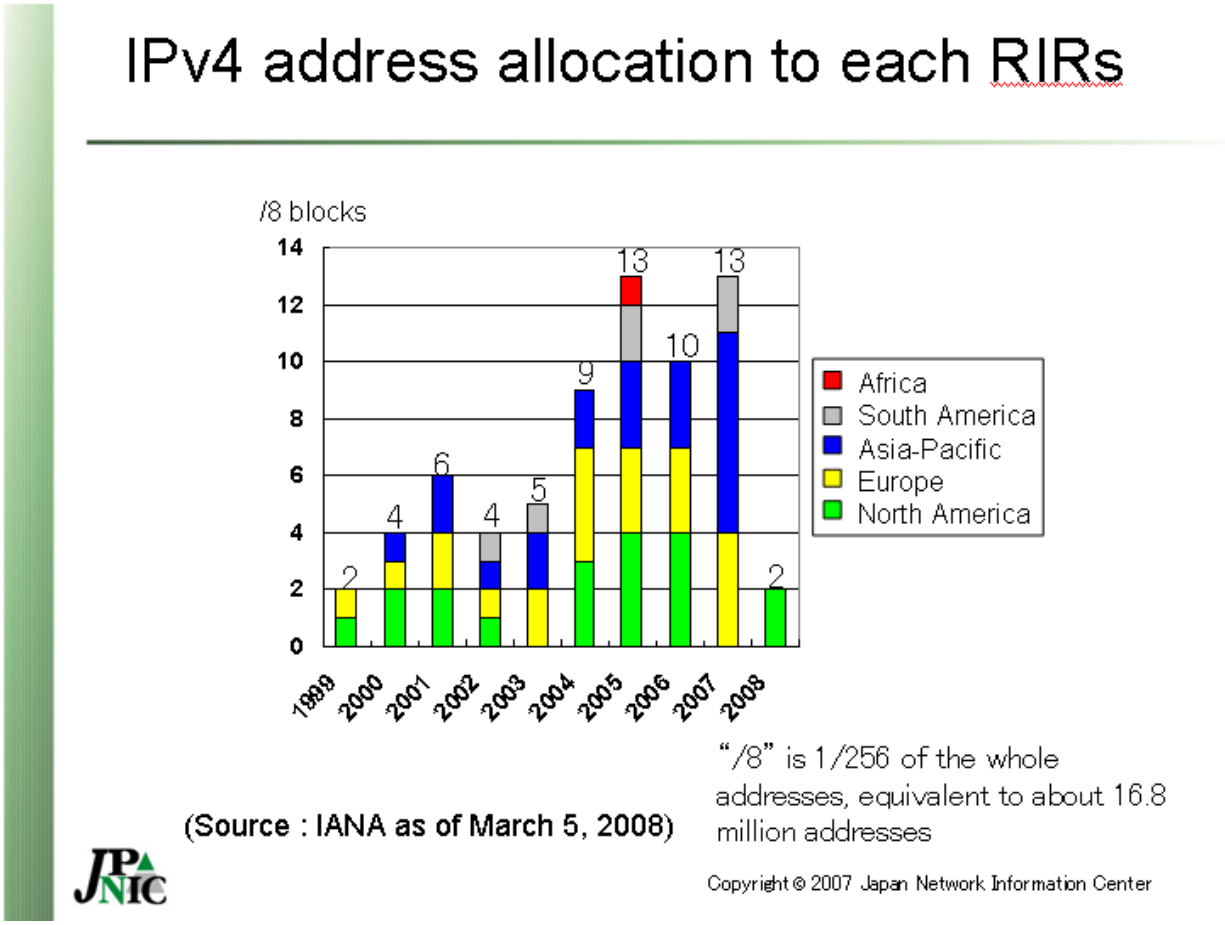


Fig. 1 - 2 IPv4 address allocation to each RIRs
(Based on the material from Japan Network Information Center)

2 Influence of address exhaustion and estimate exhaustion date

2.1 Influence of address exhaustion

When IPv4 addresses are exhausted, the Internet at that point can be maintained, but its further development will be impossible. Because IPv4 addresses required to connect devices to the Internet will run short, it will have an enormous amount of negative influence as shown below (for details, see Reference 3).

- Impossible or difficult new entry/use
  - Companies, organizations and individuals that have no addresses will be hardly able to enter a new market, or new services that require a large number of IP addresses will be hardly able to be started.
  - Many services will be hardly able to accept new users.
- Difficulty in providing services
  - Services where addresses are assigned to users for each service in order to achieve access from the Internet to users will be hardly able to be started or expanded.
  - Optimization of the service/architecture using the uniqueness of the IP addresses will become difficult.
- Difficult operation/Increase in cost/Restricted services
  - Difficult operation/Increase in cost/Restricted services will arise owing to save the addresses such as sharing of the addresses.

It will influence not only ISPs that provide the Internet access services but also service providers, system integrators, and ICT-related device manufacturers and vendors. It will also have great influence on the services that users employ through the Internet. Thus, the exhaustion of IPv4 address will disturb the use of ICT itself. If it is not responded properly, it is likely to have a great negative influence on socioeconomic activities in Japan, such as slowdown of the economic growth driven by the improved productivity by using ICT. Therefore, it is very important to implement measures by the time IPv4 addresses are exhausted that will enable continuous development of the Internet even when IPv4 addresses are exhausted.

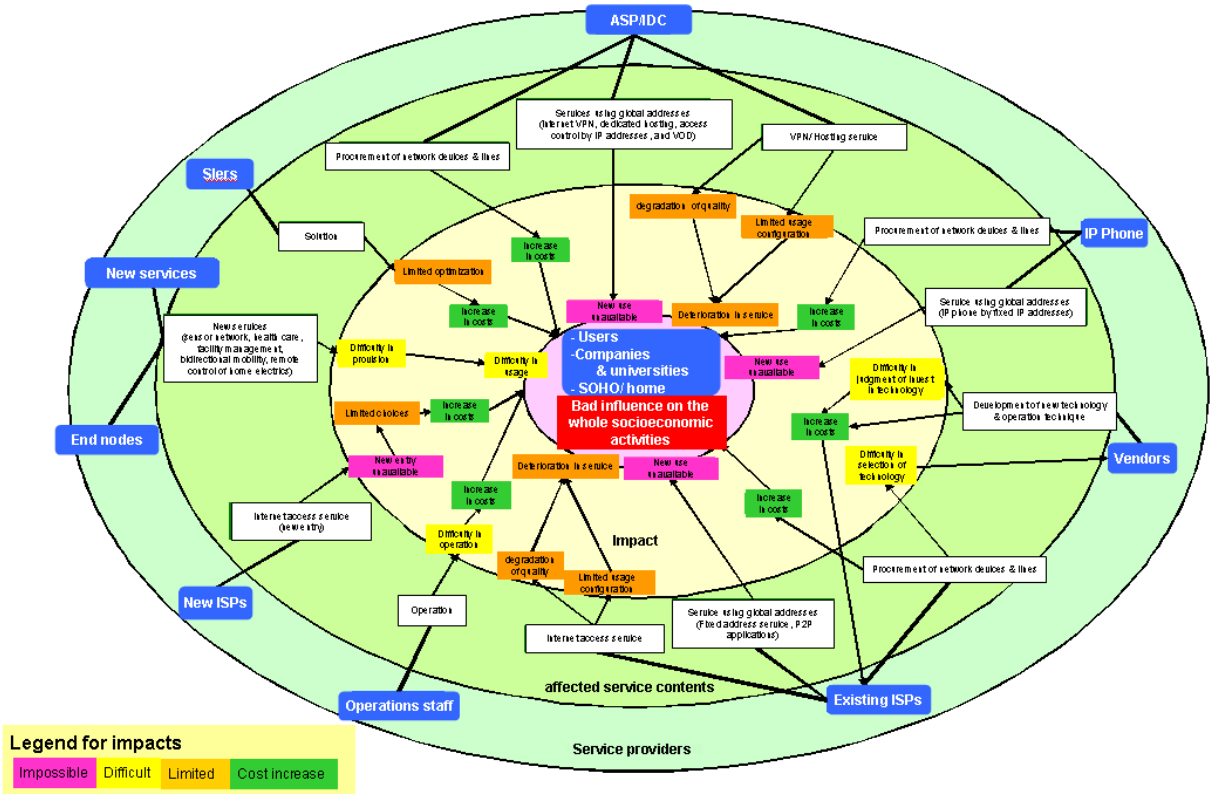


Fig. 2-1 Propagation image of influence by IPv4 address exhaustion

2.2 IPv4 address exhaustion date

2.2.1 Estimate of new demands for IPv4 addresses

As shown in Fig. 1-2, current new demand for the IP addresses is concentrated on Europe, Asia-Pacific region, and South America. Therefore, an overall trend can be grasped by predicting the trend of the new demand for IPv4 addresses in these areas.

(1) Asia-Pacific region and South America

These regions include the countries that have accomplished remarkable economic development, including BRICs (Brazil, India, China, and Russia in the European area). In these areas, the population diffusion rate of the Internet is only 12.3% of Chinese population and 21% of Brazilian. On the other hand, the annual rate of increase shows 20%-30% in China about 20% in Brazil. In Japan, the diffusion rate of the Internet in population is 68.5%. Considering that in G6 countries except Japan the diffusion rate of the Internet in population has reached to 53.7 to 68.0%, it is expected that the rapid spread of the Internet will continue in these areas.

In China, most Internet users have a broadband connection, but 18.2% of users

in South America use broadband connections (65.0% in Japan). This means that the Internet will spread, and the broadband connection users will increase as well as Internet in South America.

According to the report from a work group member of this study group, the number of IPv4 addresses required per user in the permanent connection broadband connection is about 10 times greater than for dialup connections. Therefore, even if Internet users do not increase in number, the new demand for IPv4 addresses will be generated when the rate of broadband connection users increases. Thus, it is reasonable to expect that the new demand for IPv4 addresses in the Asia-Pacific region and South America will be as great as or greater than the present conditions.

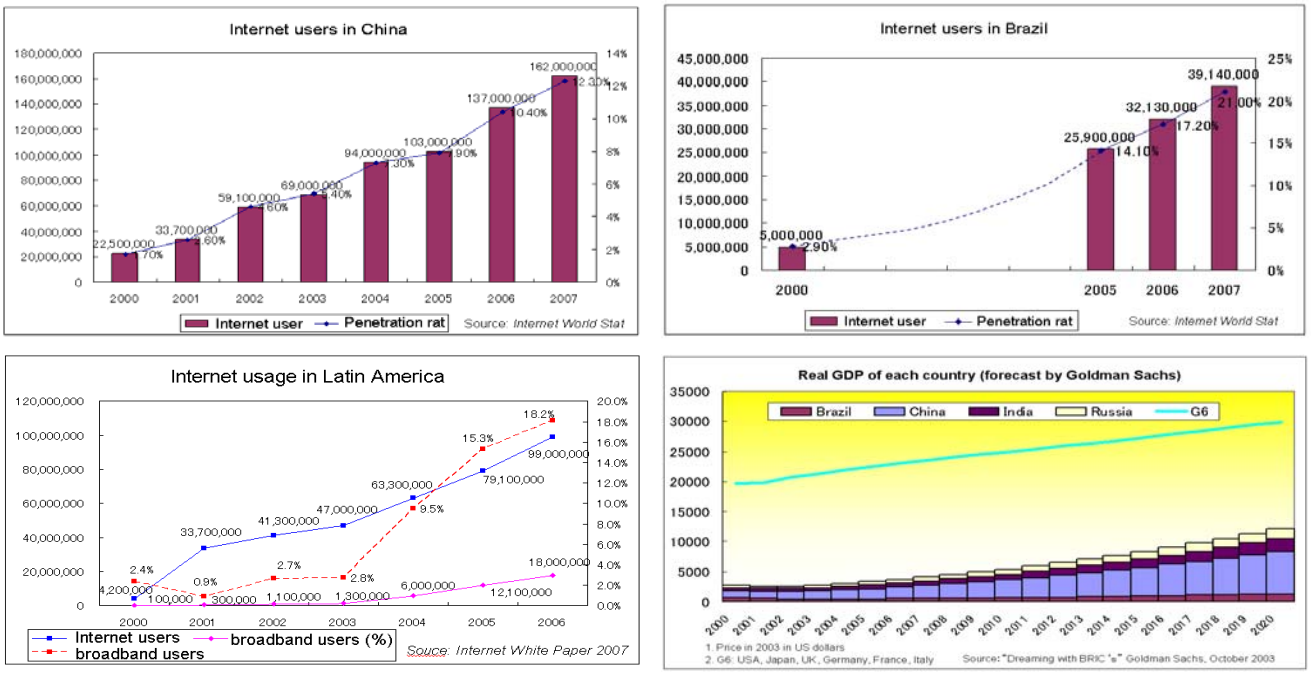


Fig. 2-2 Internet usage in Asia and South America, such as China and Brazil

(2) Europe

In Europe, the diffusion rate of the Internet in population is almost over 50%. It is inappropriate to assume that the population diffusion rate of the Internet in population will continue. However, because only 15%-23% of the population (30%-40% of users) uses broadband connections in each country, the transition from dialup connections to broadband connections will continue steadily. Then, it is reasonable to expect that the new demand for IPv4 addresses in Europe will be

as great as or greater than the present status.

Internet users in Europe (2007)

	Population	Internet user	Internet user (%)
France	61,350,009	32,925,953	53.70%
Germany	82,509,367	50,426,117	61.10%
UK	60,363,602	38,512,837	63.80%
Italy	59,546,696	32,190,658	54.10%
Spain	45,003,663	21,772,334	48.40%

Source: Broadband Scorecard Q1 - 2007 (ECTA)

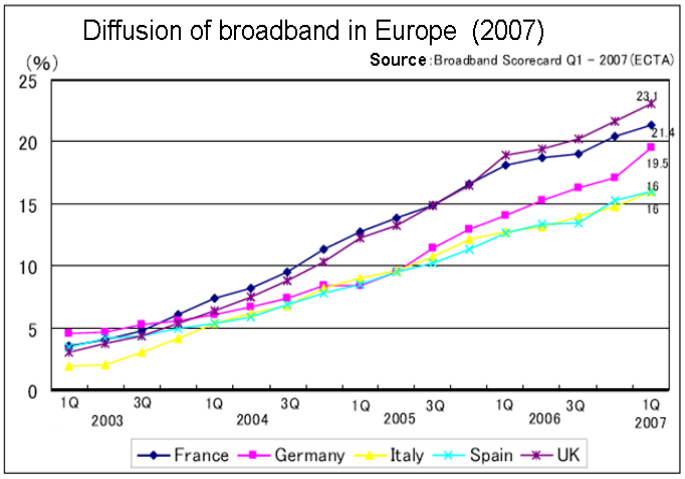
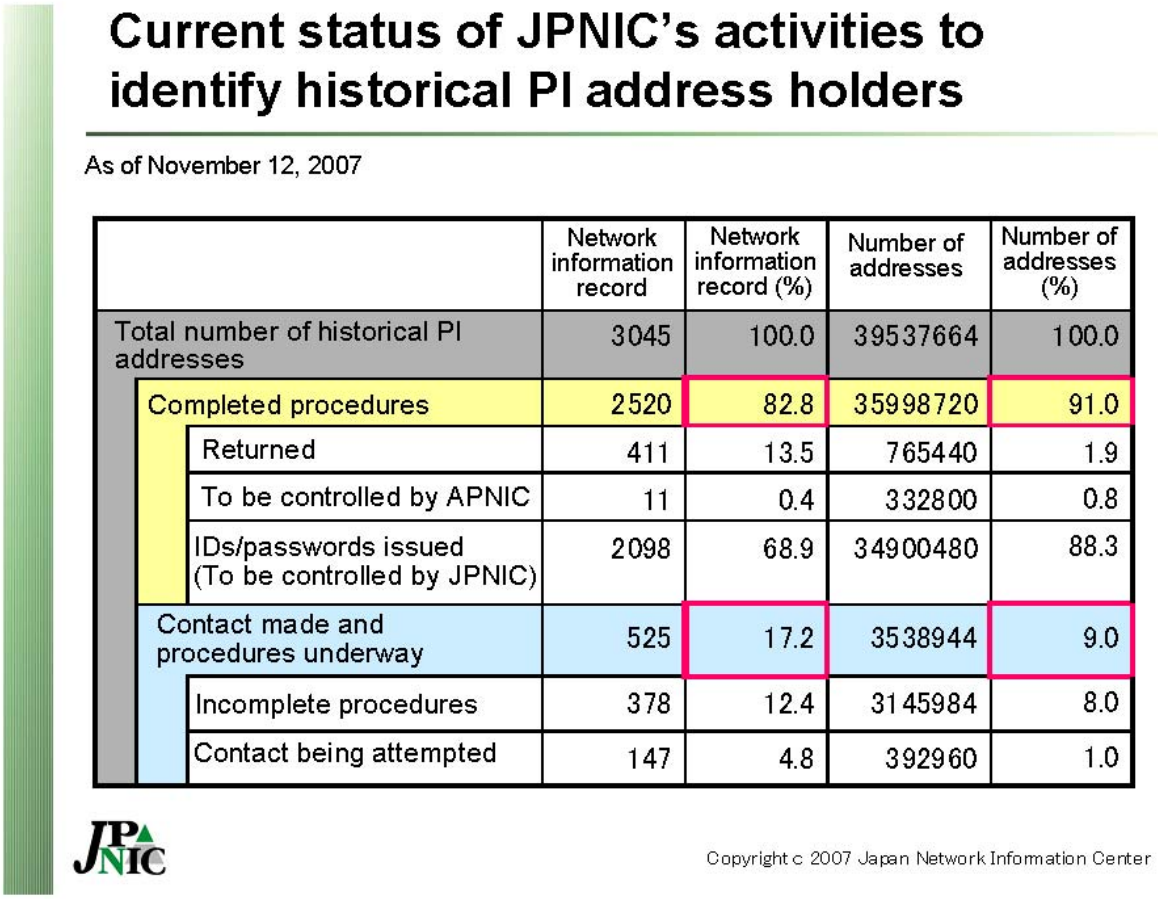


Fig. 2-3 Increase of the Internet use in Europe

2.2.2 Possibility of return of IPv4 addresses

In Section 2.2.1, the trend of the new demand for IPv4 addresses was examined. On the other hand, because IPv4 addresses are not consumer appliances, they can be returned when they are no longer necessary. This may increase the stock of IPv4 addresses. However, once IP addresses are allocated, systems are generally configured under the premise that those who received the addresses can use all of them. Even if there are unused IP addresses in an organization, the information system must be reconstructed for the addresses return and huge amounts of cost is needed in many cases. Therefore, IPv4 addresses are hardly returned. For example, the "historical PI addresses" allocated before the current IP address allocation rule has reached 94 in "/8" blocks, only four blocks were returned to the international stock. The historical PI addresses assigned in Japan are about 2 in "/8" units. Although Japan Network Information Center continues to try to contact those to which these addresses are allocated, the returned addresses occupy only 1.9% of the historical PI addresses allocated to those who were contacted (as of November 2007). Therefore, it is unlikely that the amount of returned IPv4 addresses that already allocated will increase.



Current status of JPNIC's activities to identify historical PI address holders

As of November 12, 2007

	Network information record	Network information record (%)	Number of addresses	Number of addresses (%)
Total number of historical PI addresses	3045	100.0	39537664	100.0
Completed procedures	2520	82.8	35998720	91.0
Returned	411	13.5	765440	1.9
To be controlled by APNIC	11	0.4	332800	0.8
IDs/passwords issued (To be controlled by JPNIC)	2098	68.9	34900480	88.3
Contact made and procedures underway	525	17.2	3538944	9.0
Incomplete procedures	378	12.4	3145984	8.0
Contact being attempted	147	4.8	392960	1.0

JPNIC

Table 2-1 Advance of procedure about the historical PI addresses
(Based on the material from Japan Network Information Center)

2.2.3 Expected IPv4 address exhaustion date

Based on the examination in Section 2.2.1 and Section 2.2.2, it is appropriate to think that IPv4 address consumption will be as great as or greater than the present status. In order to eliminate uncertainties in predicting the exhaustion date of IPv4 address stock, it is most appropriate to apply regression analysis based on the past data of IPv4 address consumption for the estimate of the future consumption, assuming that there will be no significant changes in the situation, namely, there will be no change in the rule concerning international address allocation or address maintenance, and that those to whom addresses are allocated will not try to retain surplus addresses arbitrarily. The details of the forecast method are shown in Reference 4. According to the analysis, the following is expected:

- International stock of IPv4 addresses will be exhausted in the middle of 2010 - at the beginning of 2012.

・ The addresses used in Japan will not be able to be replenished at the beginning of 2011 - in the middle of 2013.

If there is no change in the rules concerning international address allocation or address maintenance, and those to whom addresses are distributed will not try to retain surplus addresses arbitrarily, the following is forecast:

- Exhaustion of IANA pool in the middle of 2010 to the beginning of 2012
- No more allocation of the addresses used in Japan at the beginning of 2011 to the middle of 2013

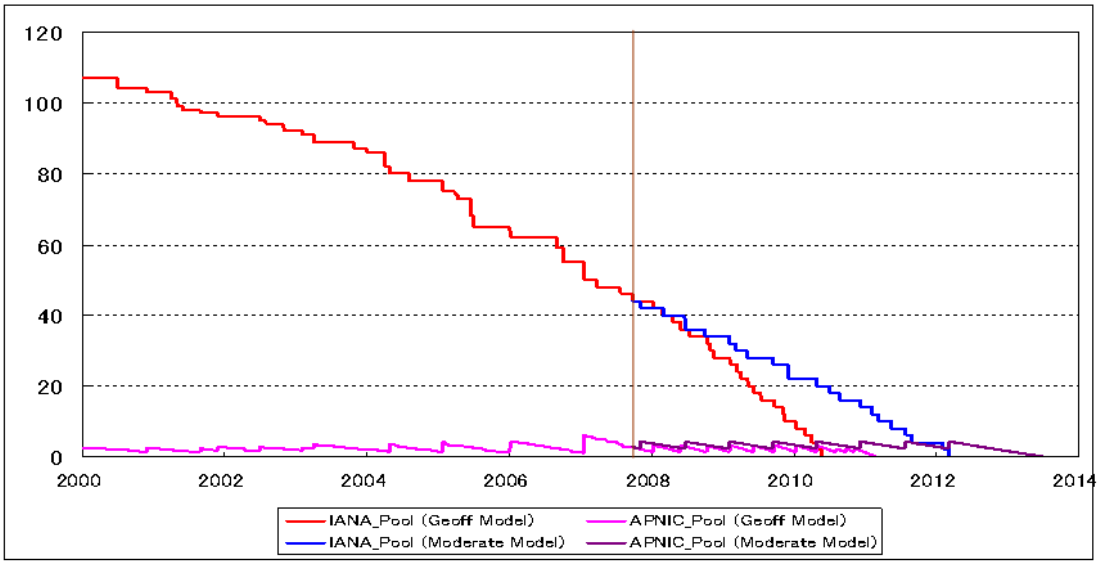


Fig. 2 - 4 Estimated date of IPv4 address exhaustion

3 Actions against address exhaustion

As shown in Chapter 2, the supplement of IPv4 addresses will be likely to be difficult in Japan as early as the beginning of 2011. Therefore, in order to ensure the continuous development of the Internet and its use, the preliminary actions must be completed for enabling successive acceptance of users for three years by the beginning of 2011. Because the development of radical new technology, such as the development of a new communication method compatible with IPv4, is very unlikely to finish in time, actions that can be basically supported by the existing technology should be inquired.

IPv4 addresses are resources whose total number is strictly determined at 2^32 (=4,294,967,296). Therefore, in case we continue to use IPv4, there are only two measures as shown below:

(1) Share one address among two or more nodes (saving of IP addresses)

(2) Use all addresses until none is left unused (maximum density of IP address use)

On the other hand, if we decide to use a system other than IPv4, the following option can be selected:

(3) Utilization of new address resources

Therefore, in this section, after extracting specific technical measures from the viewpoint of the feasibility of the above three measures with the existing technology, which measure to choose against the exhaustion of IPv4 addresses is examined.

3.1 Examination of specific measures

3.1.1 Saving of IPv4 addresses

In principle, if one address is shared among two or more nodes, an infinite number of nodes can be connected to the Internet. In this case, the node that the shared address is assigned is the source of communication, the connection through NAT (Network Address Translation)/NAPT (Network Address Port Translation) is widely recognized and established technically.

On the other hand, when the node that the shared address is assigned is the destination of communication, it is necessary to indicate a specific node among two or more nodes that share one address in some way. This can be solved by defining the port number of TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) used in the specific node beforehand, using NAPT. Therefore, it is appropriate to examine the use of NAT/NAPT as a method for saving IP addresses.

3.1.2 Most efficient use of IPv4 address

Although, theoretically speaking, only 4,300 million of IPv4 addresses exist, IPv4 address exhaustion date can be postponed by using the addresses until none is left unused. However, only 41 in /8 units (680 million) are left in the present international stock, and the other addresses:

- are preserved for specific use (private address, multicast address, etc.) (a little more than 36 units, about 610 million)
- have already been allocated (a little less than 179 units, about 300 million).

Because the current allocation rule assigns /21 units (in unit of 2,048 addresses), which are as little as the demand for one year, it is expected that more efficient use will be sought in future assignments. In order to use IPv4 addresses more efficiently, it is important to attain more efficient use of IPv4 addresses which is already allocated to users or specific use. Therefore, as a means for maximum density of IP address use, it is appropriate to examine the reallocation of the allocated IPv4 addresses.

3.1.3 Utilization of new address resources

Even if IPv4 addresses are exhausted, by the migration to a protocol that uses addresses different from the 4,300 million IPv4 addresses, new address resources can be exploited for future development of the Internet. As a communication method for the Internet that uses different addresses from IPv4 addresses, IETF (Internet Engineering Task Force), which standardized IPv4, has standardized IPv6 (Internet Protocol version 6) as a succeeding protocol of IPv4.

The address administration organization, ICANN (The Internet Corporation for Assigned Names and Numbers), and local address administration organizations also recommend the transition to the IPv6 network against IPv4 exhaustion. Because IPv6 is the only standardized communication method that can coexist with IPv4 without using the function of other protocols, it is appropriate to examine the transition to IPv6 as new address resources.

The need for the transition to IPv6 has been mentioned since the beginning of the 2000s, assuming that IPv4 addresses will be exhausted someday. However, according to "IPv6 diffusion rate investigation" by Internet Association Japan, the traffic of IPv6 in the Internet as of March 2007 amounts to only about 0.1% of the traffic by IPv4. This may result in the doubt whether the transition to IPv6 is a good way to avoid the exhaustion of IPv4 addresses.

However, IPv6 has already been used to distribute emergency earthquake reports through the Internet. Besides the Internet, they are also used in video delivery and the next-generation network in the local IP network provided by NTT East/West. Its use is beginning to spread (refer to Reference 5). Although IPv6 has

been reached to practical use technically, since the research and development for practical application. However, the reason come from the situation that IPv4 addresses are assigned as required and users have abundant experience in utilization and system construction Ipv4, so there is no need to use IPv6.Therefore, it is expected that the transitions to IPv6 will work effectively for supporting continuous development of the Internet, when it become difficult to receive assignment of the new IPv4 addresses.

3.2 Outline and evaluation of each method

3.2.1 Utilization of NAT/NAPT

In this method a network is divided two parts into LAN (local area network) and WAN (wide area network) at first. Then it shares one global IP address among multiple nodes by using one global IP address on the WAN side and private IP addresses on the LAN side.

Conversion between a global IP address and a private IP address is generally performed with the following two methods:

- Static conversion according to the predefined rule
- Dynamic conversion according to the latest communication.

Therefore, in trying access from the node in LAN to WAN, communication can be established successfully. On the other hand, when access is tried from the WAN side to the node in the LAN, because the technical mechanism for offering the above predefined rule to third parties does not exist, access is possible from those who know the rule in advance, but access from those who do not know the rule, i.e., public access, is very difficult. The information about an IP address etc. may be included in the payload section, in some communication protocols or applications. In this case, the introduction of ALG (Application Level Gateway) is required for each communication protocol and application by the introducer of NAT/NAPT.

NAT/NAPT is used widely to share IP addresses in homes or offices, but large-scale NAT/NAPT is employed only at part of cable Internet. It should be noted that the operation expertise is totally different from the utilization in homes and offices.

Based on this premise, the evaluation of utilization of NAT/NAPT as a strategy against IPv4 address exhaustion is as follows (for details, see Reference 6-1).

（1） Effect as a countermeasure

－ If it applies to the Internet users , such as consumers, a certain effect for saving addresses can be expected.

- If it applies to the nodes installed for providing services on the Internet, such as websites, there is a possibility that general services, which is the original purpose, cannot be provided.
- Therefore, its applicable area and its effect as a countermeasure are limited.

（２） Items that should considered in choosing as a countermeasure

- Addresses can be saved in Internet access service providers for consumers, but addresses continue to be required by service providers and data centers.
- Because we have little experience in the operation of large-scale NAT used as part of Internet access service, there is a possibility that expertise must be constructed.
- We cannot estimate how massive aggregation will be technically possible at the present moment.
- Because cost increases as aggregation is advanced, we cannot estimate the entire cost required.

（３） Problems that will occur when it is selected as a countermeasure

- Those who introduces NAT/NAPT or ALG will inevitably limit communication that can be passed. Therefore, all communications cannot be passed theoretically, and a limit. Theoretically, it is impossible to pass the all communications providing Internet access services must be limited.
- In case of a problem, the failed node cannot be specified from the WAN side, because one address is shared among several nodes.

３.２.２ Reallocation of assigned IPv4 addresses

This is a method that collects the addresses allocated to organizations or the addresses for specific purposes except those that are truly required, and reallocates them to other organizations. This countermeasure needs the change of the address allocation policy, which is international agreement in IETF or ICANN, besides expecting that the addresses will be returned voluntarily. The following international agreement needs to be made for that:

- In IETF, reexamination of the way the IP addresses for particular use should be and their necessary quantity
- In ICANN, how the addresses other than those truly required are returned from those who have already received allocation of the addresses
- In ICANN, how to estimate the truly required addresses

Because the network system using IPv4 is generally designed and built, assuming that all the allocated IP addresses can be used, therefore returning the addresses may result in system modification requiring significant cost. Based on

this premise, the evaluation of reallocation of assigned IPv4 addresses as a strategy against IPv4 address exhaustion is as follows (for details, see Reference 6-2).

（１） Effect as a countermeasure

- The number of nodes connectable with the Internet will not increase.
- Although Japan Network Information Center has tried to recover the addresses assigned in the past, at most about 2% of the addresses have been collected. The new demand for addresses in the world (13 in /8 units in 2007, among which seven of them were demanded in the Asia-Pacific region) amounts to about 5% of the whole addresses. Voluntary return will suffice only for the demand for at most several months.
- Therefore, when international agreement is not made about policy change of address allocation, any effect can hardly be expected.
- Even if compulsory recovery is performed, 1/3 of the currently assigned addresses must be recovered to meet the address demand for five years, for example. Thus, it cannot be a countermeasure by itself.

（２） Items that should considered in choosing as a countermeasure

- At present, the schedule of change in the address allocation policy, which is an essential condition for recovery, cannot be estimated. It cannot be selected as a countermeasure without a guarantee that the policy will be changed within at least three years
- When the address allocation policy is changed, it is required to be able to check with certainty comparable as the present condition who the IP addresses is allocated to. It is required to renew the information for guaranteeing the justification of judgment about where the communication addressed to a certain IP address should be relayed to with considerable accuracy.
- When compulsory address recovery is performed, there is a possibility that fragmentation of address allocation may be encouraged. If it is about 2 times fragmented, the existing routers probably cannot deal with the route information that the routers must store, because the amount of information exceeds the memory space in a router.

（３） Problems that will occur when it is selected as a countermeasure

- When fragmentation of address assignment occurs, whether receiving address replenishment, all the Internet operators' cost will increase. Thus,

beneficiaries and defrayers do not match.

- Because required cost depends on the address assignment policy, the entire cost required cannot be estimated.

3.2.3 Transition to IPv6

This is a method that transition to an incompatible communication protocol that can coexist with IPv4 (they cannot communicate mutually without sometreatments). IPv4 and IPv6 are usually regarded as different communication protocols within communication devices. Even if they are not treated as different communication methods, it is guaranteed that flow of IPv6 packets in the existing network dose't cause problems, because IPv4 and IPv6 are distinguished at the first 4 bits (version section) of the packet header. Because IPv6 provides 21^28 (3.4 x 1038) addresses (if 10 billion people use 100 million addresses per second, the addresses will be available for 10 trillion years), it will be effective enough as a countermeasure against address exhaustion.

On the other hand, IPv6 is a comparatively new technology that is not widely used. Therefore, there are some difficulties in starting a large-scale utilization: the products are crude, and the operation expertise and support tools are insufficient. Based on this premise, the evaluation of the transition to IPv6 as a strategy against IPv4 address exhaustion is as follows (for details, see Reference 6-3).

(1) Effect as a countermeasure

- It can be a permanent measure.

(2) Items that should considered in choosing as a countermeasure

- Without a certain additional action, communication cannot be established between IPv4 network and the IPv6 network. Using a translator (translation equipment of a communication protocol that connects IPv4 network and the IPv6 network) can solve some problems, but it cannot be guaranteed that all communications are relayed successfully.
- Especially for the communication protocol and application that include the information about the IP address in the payload section, communication between IPv4 network and the IPv6 network cannot be relayed, unless those who introduces the translator install ALG for each communication protocol/application.
- The devices or services that are used now may be unable to deal with IPv6. These devices or their software needs to be replaced. Therefore, it is very difficult for all existing IPv4 users and services to migrate to IPv6 within

three years. A bridging action is also required.

- Experience in operation is generally scarce and operation support tools are insufficient.
- Because addresses do not need to be saved, there is a possibility that communication pathway may explode.

（３） Difficulties that will occur when it is selected as a countermeasure

- Until IPv4 network can be suspended, it is necessary to operate two logically different networks, IPv4 network and the IPv6 network simultaneously. That results in an increase in operation cost. It is estimated that the operation cost must increase up to as twice as the current operation cost.

３.３ Selection of Countermeasure

This examination is intended to continuous development and utilization of the Internet, even after replenishment of IPv4 addresses is difficult in Japan. Therefore, the countermeasure to be selected must complete initial response in about three years, i.e. by the beginning of 2011, at that time supplying of IPv4 addresses may be difficult. There are some problems that must be solved in the three countermeasures mentioned above. In choosing one of them, it is necessary to consider that the relevant problems can be solved in about three years (feasibility within a time limit) as a matter of highest priority. It is also desirable that the currently realizable use in the Internet can also be provided, from a viewpoint of continuous development of the Internet and its utilization (continuity of service).

It is inevitable that general users will be influenced, whichever measure we may select. Therefore, it must be remembered that, once it starts, it is difficult to change to another measure along the way (continuance of effect). Three countermeasures are compared based on these three viewpoints.

３.３.１ Comparison of feasibility within the time limit

First, utilization of NAT/NAPT can be realized by installing additional devices. There are some problems that cannot be solved immediately: service will be Restricted and operation experience is insufficient. However, this can be started immediately in principle.

On the other hand, for reallocation of the assigned IPv4 addresses, it is doubtful that the problems can be solved within three years. In this countermeasure, the change of the address allocation policy is indispensable. Three years in not long enough to establish international agreement about policy change. Especially, about recovery of the assigned addresses, standpoints are extremely different

among the countries that have received many historical PI addresses and comparatively abundant in IPv4 addresses (U.S. and part of Europe), and the countries that started to receive allocation of the IP addresses after the general utilization of the Internet is started and the newly emerging countries where the spread of the Internet started after the Internet is widely used all over the world (the Asia-Pacific region including China, South America including Brazil and Africa). Therefore, it is appropriate to think that there are hardly any chances that change of the policy will take place within three years so that sufficient number of IPv4 addresses can be collected to meet the demand for some years to come.

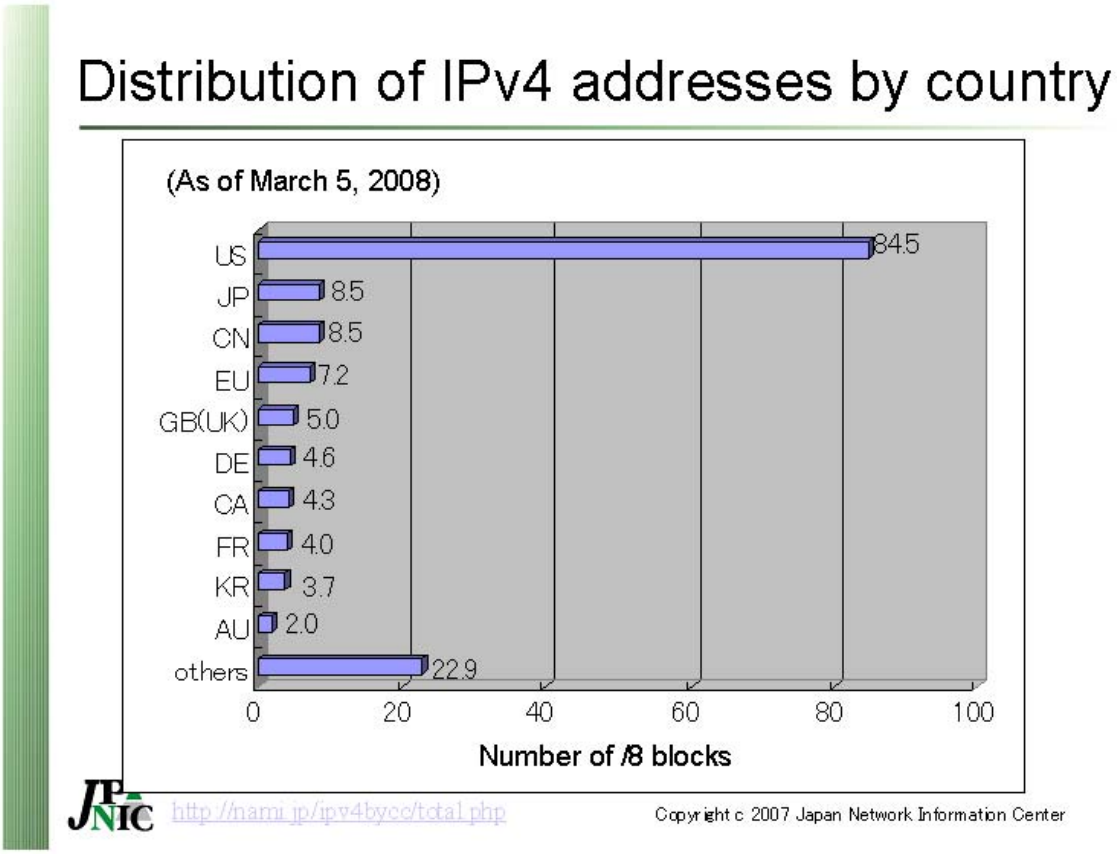


Fig. 3-1 Distribution of IPv4 addresses by country
(Based on the material from Japan Network Information Center)

It is very difficult to guarantee that the problems can be solved within three years to the transition to IPv6. Because it will take time in product development. Devices and softwares replacement might be necessary.

3.3.2 Comparison of continuity of service

First, in utilization of NAT/NAPT, it is inevitable that access from the WAN side to the nodes in LAN is restricted, so, if it is selected as a measure, the continuity of the present service cannot be guaranteed. On the other hand, if reallocation of the assigned IPv4 addresses is selected, it will not affect the services because there will be no technical change. When the transition to IPv6 is selected, if all devices, software, and services support IPv6, all the things that are provided in the current Internet are abailable.

3.3.3 Comparison of continuity of effect

In utilization of NAT/NAPT, because there exist those who can save the addresses (Internet connection providers that accommodate many general users), and those who have difficulty (such as service providers in the Internet asking for access from the general etc.), so there is a question about continuity of effect. It is judged that continuity of effect is limited in reallocation of the assigned IPv4 addresses, because it does not increase the number of nodes that can access the Internet. On the other hand, in transition to IPv6 the effect is permanent, because a large number of addresses are available.

3.3.4 Choice of measure

The examination from Section 3.3.1 to Section 3.3.3 is summarized as below.

Table 3-1 Comparison of countermeasures

	Utilization of NAT/NAPT	Reallocation of the assigned IPv4 addresses	Transition to IPv6
Feasibility within a time limit	○	Doubtful	Extremely difficult
Service continuity	Restricted	○	○
Permanent effect	Doubtful	×	○

Based on this, the following is possible:

- Three viewpoints cannot be fulfilled with only one measure.
- There is only one combination to fulfill three viewpoints by two measures: utilization of NAT/NAPT and the transition to IPv6.
- Three viewpoints can be fulfilled if all three measures are combined.

Because large cost is expected in enforcement of each measure, fewer measures to implement are desired. Therefore, as an action against IPv4 address exhaustion,

the following is considered to be the most appropriate:

- Because only transition to IPv6 can maintain the continuity of the effect without a restriction in providing services, it should be performed as an essential measure.
- However, because it is difficult to complete the transition to IPv6 by IPv4 address exhaustion date, NAT/NAPT should be used in the beginning.

Although reallocation of the assigned IPv4 addresses is not denied, the address allocation policy needs to be changed with consideration for the problems stated in Section 3.2.

4 Procedures to introduce measures for address exhaustion

The examination up to Chapter 3 indicates that, in order to deal with IPv4 address exhaustion, one measure cannot meet three viewpoints (solution within a time limit, service continuity, and permanent effect). Therefor it is required to save IPv4 addresses by utilization of NAT/NAPT and transit to IPv6 at the same time.

However, when two measures with different characteristics are combined, only both of their disadvantages will be observed, and they will not work well as measures if an introduction procedure is inappropriate. Because the Internet is not intensively managed by specific persons, the response to IPv4 address exhaustion requires all the stakeholders' cooperation. Therefore, the procedures for introduction of measures against IPv4 address exhaustion are examined, and the procedure for introducing these measures to function effectively is shown below. Common understanding will be developed about changes of the Internet communication environment by IPv4 address exhaustion.

4.1 Overview of the introduction of the measures

4.1.1 Basic elements that build the Internet

The Internet roughly consists of nodes (devices) connected to the Internet, and the network that connects the devices. The utilization of devices is roughly divided in the *service side* that offers benefits through the Internet and the *user side* that receives the benefits. It is appropriate to think that the Internet is the system that can offer various benefits through circulation of the information as shown below.

```
Users  <=> User side devices
                <=> Network <=>
                            Service side devices <=> Service providers
```

Therefore, the procedures to introduce measures against address exhaustion will be examined by dividing the Internet into three elements of users, networks, and services and considering the characteristics of each element.

In this case:

- "Users" are those who receive the services provided through a network or perform direct communication between users.
- "networks" bridges communications between the users and service providers, or between the users.
- "Services" are the benefits offered to the users through "networks".

It must be noted that each existing organization does not always fit in only one of the elements. For example, a general Internet access service consists of the following sections:

- The network section, which offers the connectivity and information delivery to other nodes to users.
- The service section, which offers e-mail, website hosting, and portal sites to users.

It should be noted that the companies that have a website have both of the following aspects:

- Aspect as network users
- Aspect as service providers that provide services to consumers

4.1.2 Basic characteristics of each three elements and their influence exerted by the introduction procedure for measures

(1) Characteristics of users

For users, the Internet is only an instrument to receive benefits. After users compare the benefits received only through the Internet and the obstacles in using the Internet, or the benefits and obstacles generated in the Internet and by the means other than the Internet (for example, service provided by actual stores), they have chosen receiving benefits through the Internet, and they use the Internet only as the means. Therefore, when the obstacles in the introduction of the measures are great, users may choose not to use the Internet instead of introducing the measures. Particularly, individual users may have to give up using the Internet against their will, if the measures are complicated in some cases.

At the same time, if many users give up using the Internet to avoid the introduction of the measures, the goal for the measures against address exhaustion, i.e. continuous development of the Internet, cannot be achieved. Therefore, the procedure for introducing measures must not require special efforts by most of the users. Consequently, the procedure for introducing measures must not require an active response from the users during the transition stage of the introduction.

(2) Characteristics of services

For services, the positioning of the Internet varies greatly with the types of benefits offering. There are benefits that can be offered only through the Internet (for example, portal sites), and benefits that can be offered also with the means other than the Internet (for example, mail order).

For the former, the Internet is the only way to offer benefits. Thus, if a change of the environment for communication to users in necessary they would be receptive to the measure for the change.

it can be expected that the response to the change would be flexible even if the environment for communication among users must be changed. On the other hand, for the latter, the Internet is used as a way of offering benefits easily, inexpensively, and promptly to many users compared with other means. If the barrier is very high because of the change in the communication to users, they may stop using the Internet. However, because both of them are exposed to severe competition, an active response can be expected accordingly if the response to the change in the Internet communication environment is proved to be indispensable for the future business growth.

（3） Characteristics of networks

For “networks”, the response to address exhaustion is indispensable for continuous development. If “networks” do not introduce the measures, however hard “users” and “services” endeavor to address exhaustion, there is a possibility that they cannot communicate through the Internet. Therefore, “networks” must complete the initial response until address exhaustion, and bear the most important responsibility to make the environment where an essential measure can be taken by “users” and “services”. Thus, it is desirable that, when introducing measures, the network plays as active a role as possible and responses by “services” and “users” are asked for only if the response by “networks” is logically impossible or irrational.

4.1.3 Characteristics of measures and influence on the introduction procedure

（1） Characteristics of NAT/NAPT

a） Difficulty in bidirectional access

As described in Chapter 3, when NAT/NAPT is used, the IP addresses that are distributed to each node are private IPv4 addresses, and their uniqueness cannot be maintained any longer. The nodes accommodated under NAT/NAPT can access the nodes to which the global IPv4 addresses are distributed, but the opposite is difficult. Therefore, the nodes that expect access from any person, i.e. “services”, still require global IPv4 addresses. At the same time, global addresses must be distributed to “users” when they want to use the P2P communication. This limits adaptation of NAT/NAPT only to “users”, and global addresses must be distributed in some way at least to users to whom NAT/NAPT is applied.

b） Difficulty in user distinction depending on the address

As described in Chapter 3, when NAT/NAPT is used, the IP address

distributed to each node is a private IPv4 address, and its uniqueness is no longer maintained. Therefore, when services distinguish users, if the addresses distributed to user nodes or the source address of communication from "users" is the global IPv4 address, there is a possibility that user distinction may no longer be executed properly. Thus, "services" need to be provided, considering a possibility that the "users" are accommodated under NAT/NAPT.

c) Limit in the number of simultaneous sessions

As described in Chapter 3, NAT/NAPT relays the response from the WAN side to an appropriate node by grasping the history of what node on the LAN side communicates with what address on the WAN side. Then it is inevitable that the number of communication sessions that can be relayed simultaneously is limited. Therefore, when the communication volume from the LAN side increases substantially all at once, the data may not be relayed properly (when the computer virus called MS_Blaster was diffused in the summer of 2003, communications that tried to infect other PCs were generated by PCs infected by the virus, in some cable Internet providers, the NAT/NAPT equipment failed). This means that "services" must be provided, bearing in mind the possibility that users under NAT/NAPT have a limit to the number of simultaneous sessions.

d) NAT/NAPT is not involved in the payload section of an IP packet

As described in Chapter 3, NAT/NAPT only converts the source address or the destination address described in the header section of an IP packet. Therefore, when the information based on an IP address is indicated in the data accommodated in the payload of an IP packet, it is necessary to change the information with ALG separately, in principle. However, because ALG is necessary for every each "services", it is impossible to install ALG supporting all the services on the network. Therefore, considering that NAT/NAPT exists on "networks", "services" must be provided without describing the information based on an IP address in the data accommodated in the payload section of an IP packet, or ALG for exclusive use must be distributed to "users".

(2) Characteristics of IPv6

a) Cannot communicate with an IPv4 network

As described in Chapter 3, because IPv6 is incompatible with IPv4, a translator is required for communication from the node where only IPv6 was distributed to the node where only IPv4 was distributed, or from the node where only IPv4 was distributed to the node where only IPv6 was distributed. However, a translator is necessary for every each application provided through

the network. Therefore, to install the translators supporting all the services on a network is impossible. Because of this, “services” must support both IPv4 and IPv6, support one of them and use a translator installed for the other, or support one of them and distribute dedicated translators to “users” to support the other.

The display of a simple Web page can be supported generally by the simple translator that converts only the IP packet headers for IPv4 and IPv6, but, because offering such a translator is equivalent to “services” according to the classification in this section, a translator will not be installed on a network anyway. Because there is a possibility that the address conversion by this translator may be abused as anonymous activities such as attacks, it should be noted that the access analysis function must be enhanced when this translator is installed.

４.２ Introduction procedure for measures

Based on the view described in Section ４.１, it is appropriate to introduce the measures in the following three steps:

- Before IPv4 address exhaustion (up to 2010)
- Early stage of IPv4 address exhaustion (from the beginning of 2011)
- Middle stage of IPv4 address exhaustion (beginning of 2012 at the earliest)

It is then appropriate to end IPv4 support by “networks” and “services”, and to transit to IPv6 when the need for using IPv4 is sufficiently decreased (the final stage of IPv4 address exhaustion). The middle stage of IPv4 address exhaustion will come at the beginning of 2012 at the earliest, because additional allocation of the current IPv4 addresses will be sufficient for the demand for one year.

４.２.１ Before IPv4 address exhaustion

The stage before IPv4 address exhaustion is the period of preparation for enabling acceptance of new users, even after new IPv4 addresses are unavailable. This is a period to maintain the Internet connection environment with the existing IPv4 and to set the environment where “users” and “services” can transit to IPv6. Therefore, basically the three basic elements of the Internet should take the following actions.

（１） Networks

Both of IPv4 and IPv6 networks will be built, and connection by IPv6 will be included in a basic service before IPv4 address exhaustion at the latest.

（２） Services

"Services" must support both IPv4 and IPv6 before IPv4 address exhaustion as much as possible. And it is desirable that IPv4 section will support "users" accommodated under NAT/NAPT. IPv6 can be introduced through system change or using a translator.

（３） Users

It is desirable that "users" will support both IPv4 and IPv6 as much as possible when the devices connecting to the Internet and software introduced to these devices are procured, renewed, or modified.

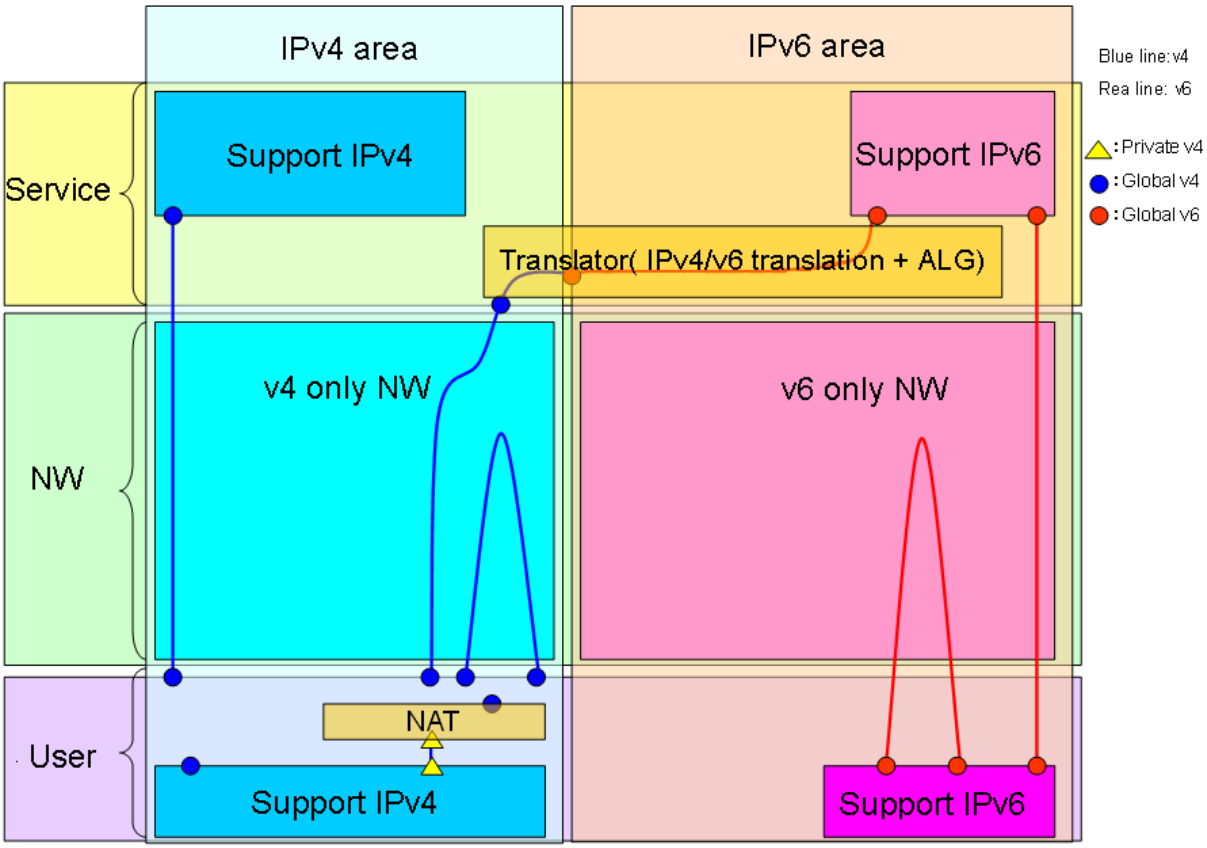


Fig. 4 - 1 Model of the Internet immediately before IPv4 address exhaustion

4.2.2 Early stage of IPv4 address exhaustion

In this time, the new unallocated IPv4 addresses will run out and it will be difficult to distribute the global IPv4 addresses to new “users”. These “users” will be accommodated under NAT/NAPT. Therefore, three basic elements of the Internet should take the measures as follows basically.

（1） Networks

“Networks”, will accommodate new “users” under NAT/NAPT, as offering IPv4 addresses becomes difficult. The global IP addresses can be provided to all the users will be IPv6 only.

（2） Services

“Services” will support both IPv4 and IPv6, and the IPv4 support section will also support “users” accommodated under NAT/NAPT.

It should be noted that, in case “services” cannot realize this, they cannot be connected from the “users” connecting to the “networks” after the early stage of IPv4 address exhaustion, resulting in a gradual increase of “users” that cannot connect to the “services”.

（3） Users

“Users” should introduce the devices connectiong to the Internet and the softwares installed in these devices that support IPv4/IPv6 as soon as possible.

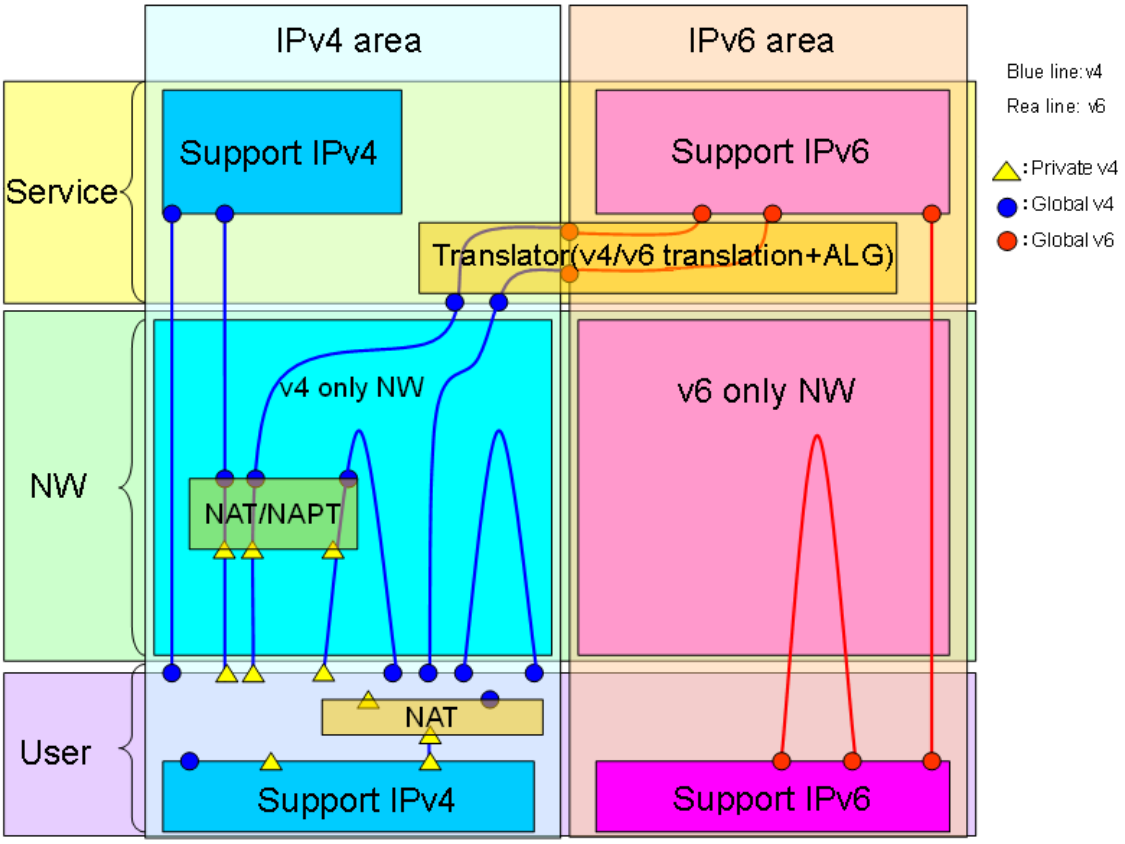


Fig. 4-2 Model of the Internet in the early stage of IPv4 address exhaustion

4.2.3 Middle stage of IPv4 address exhaustion

In this method there will be few global IPv4 addresses that can be distributed to "services" requiring global IP addresses, and the existing "users" will be accommodated under NAT/NAPT. Therefore, basically the three basic elements of the Internet should take the following actions.

(1) Network

On "networks", the existing users will also start to be accommodated under NAT/NAPT. Basically, IPv6 will be a basic connection service by "networks".

(2) Services

"Services" will be basically provided using IPv6, and "services" using IPv4 will continue to be provided for remaining devices/software at the "users" that support only IPv4s. In case "services" cannot realize this, the number of the "users" who cannot connect their "services" will increase further, and the number of the "users" who can connect will approach zero quickly.

(3) Users

"Users" should use IPv6 if possible.

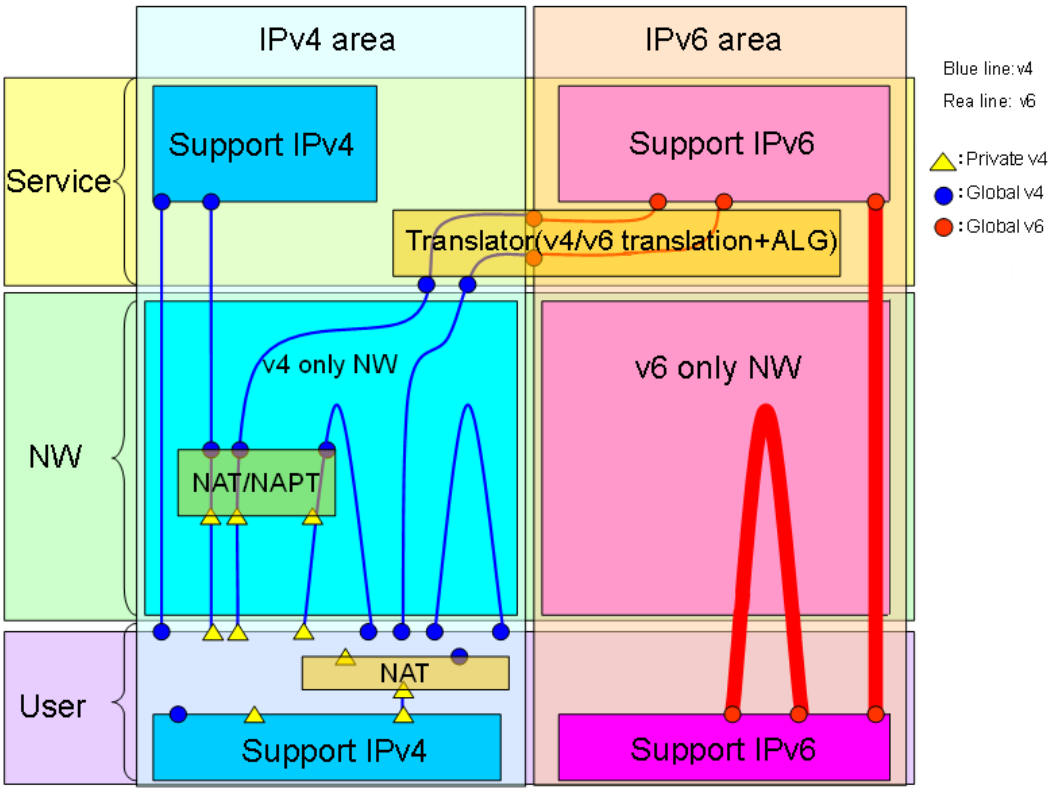


Fig. 4-3 Model of the Internet in the middle stage of IPv4 address exhaustion

4.3 Introduction of measures in the network

Now, in Japan, a large number of ISPs provide Internet access service to “users”. When users use the Internet access service from these ISPs, they often use the access networks that are provided by a relatively small number of providers. Therefore, how to provide the Internet access service by IPv6 through an access network also needs to be examined in the transition to IPv6.

4.3.1 Players

With an Internet access service or service of an access network, the function that should be provided will change significantly depending on the connection method between them. In order to guarantee the versatility of the examination, it is most appropriate to examine how to accommodate users after choosing only the most fundamental functions for both sides.

First, the fundamental function of the Internet access service is to offer connectivity to the Internet. On the other hand, when communication from a user reaches another node, it generally passes through multiple networks. Therefore, the definition must be established that uniquely decides which network provider offered connectivity to the Internet. In this case, it is thought that only distribution of IP addresses to users is essential for “offering connectivity to the Internet” and an element “offered by only one provider”. Therefore, in this report, offering of connectivity to the Internet is defined as “distribution to users of the IP addresses for which the provider has responsibility in utilization”, and this is called the offering of “reachability”.

The fundamental function of the service of an access network is to pass user communication to the “reachability” provider and to pass the communication destined for a user that is provided by “reachability” to the user. This is called offer of “connectivity” in this report.

It should be noted that “reachability” and “connectivity” do not mean any specific business form. For example, “reachability” and “connectivity” are usually provided by one entity on the cable Internet.

4.3.2 Specific methods

If connectivity is connected only to one reachability, special technical consideration is unnecessary. However, when one connectivity is connected with multiple reachabilities, to which “reachability” a user communication should be passed must be decided in the connectivity to relay it. Therefore, “reachability” and

“connectivity” need to be connected, so that a user can decide to which "reachability” to relay.

In considering technical methods regarding this, because the provision of “reachability” is distribution of IP addresses to users, there are four available systems, depending on in which layer in the OSI reference model the distinction is performed.

c

（1） Distinction in Layer 1 (physical layer)

Users are distinguished on the physical line level, and they are connected to the “reachability” to which they should be connected physically. This includes jumpers which connect the metal line in a user's home to the accommodation equipment for “reachability” to connect. In this case, because “connectivity” is not involved in the IP layer, “reachability” can employ IPv4 and IPv6 arbitrarily.

（2） Distinction in Layer 2 (data link layer)

Users are distinguished by the device ID (MAC Address in case of Ethernet) attached to the equipment installed on the user's premises (CPE: Customer Premises Equipment). They are connected to appropriate “reachability” on the Layer 2 level.

PPP (Point to Point Protocol), TAG-VLAN, MPLS, etc. can be used. In this case, CPE is indispensable. Because “connectivity” is not involved in the IP layer, the “reachability” can employ IPv4 and IPv6 arbitrarily.

（3） Distinction with an IP address

In this method, the IP address distributed to the user is decided after considering the distinction of “reachability” and delivery of communication to a user with “connectivity”. In this case, the IP address distributed to a user cannot be determined only by the “reachability” side. Therefore, a certain rule about what kind of IP address should be distributed to a user must be established.

（4） Distinction using tunneling technology

In this case, after IP addresses are distributed to the equipment installed in the user premise (CPE) in “connectivity”, and the connection with the accommodation equipment in “reachability” is attained, the IP addresses are again distributed to the users from the accommodation equipment in “reachability”.

IP in IP technology, such as IP-VPN, MIP (Mobile IP), and NEMO (Network Mobility), and L2TP are possible. In this case, CPE and the terminal supporting tunneling technology are indispensable, and the technical overhead exists for accommodating IP packets to other packets.

4.3.3 Considerations

(1) Cost

The entire cost for realization of four systems described in Section 4.3.2 cannot be estimated at present, because it greatly depends on the implementation. On the other hand, the burden on the side of "connectivity" is greater, and the burden on the side of "reachability" is smaller in order from (1) to (4). However, because the cost for "connectivity" and "reachability" will eventually be passed on to users, it should be noted that the difference in the burden does not affect the selection of which system is better. At the same time, it also should be noted that higher performance and complicated equipment must be installed on the user premises (CPE) as the technical overhead for user accommodation is greater in the order from (1) to (4).

(2) Risk of specific communication environment accompanied by system utilization

Except for system (1) described in Section 4.3.2, a certain communication method is used to distinguish users. In this case, when a different system from the international trend is chosen, the communication environment for Japanese users may be different from that of general users in the world, resulting in disadvantages in receiving of services and selection of devices.

However, it is necessary to examine which system to choose, considering the international standardization trend, because the international standardization about the connection method of the "connectivity" and "reachability" in IPv6 and the devices required for its realization has not been advanced sufficiently.

(3) Decision of the connection method

Because the connection method for "connectivity" and "reachability" is related to the definition of the business boundary between them, it is appropriate that it will be decided with discussions between both parties.

However, in order for the Internet connection by IPv6 to be available by 2010, it must be remembered that three processes (development of required devices by manufacturers, introduction of the equipment to the network, and the network verification) will take much time after the decision on the connection method. The period required depends on the connection method, but it is expected that about half a year to one year is required for each process. Thus, about two years and a half are required to secured in total. Therefore, considering Section 4.3.2 (1) and (2), the parties involved in "connectivity" and "reachability" must promptly begin to examine how to connect them and reach agreement at an early stage.

In deciding the connection method for "connectivity" and "reachability" related to the Internet connection by IPv6, not only the viewpoint on the side of

“networks”, such as domestic and international trends of the technology and product, but also the viewpoint of users and services, which are components of the network connection, are required. As shown in Section ５.２ Players , it is necessary to pay attention to the wide-ranging trends in environment for the usage of the players, the market environment, business conditions, and overseas Internet businesses.

5 Action plan towards the response to address exhaustion

In order to realize the measure introduction procedure shown in Chapter 4, various problems shown in Reference 7 must be solved. For the solution, all the stakeholders concerning the Internet must cooperate. Therefore, an action plan must be created of what each player should do by when, and promote it all over Japan. The action plan shown here only assumes standard actions. It is most important for each player to decide on the specific action plan toward IPv4 address exhaustion, getting the devices, software, and services in perspective.

5.1 Examination policy of the action plan

Basic elements of the Internet, networks, services, and users, should primarily respond to IPv4 address exhaustion, respectively. However, in the introduction of the measures against IPv4 address exhaustion, there are many technical problems that cannot be solved by the above three elements all by themselves. Therefore, cooperation from other elements and other relevant parties is indeispensable (see Reference 7 for the details of the technical problems). The action plan will be examined one by one as shown below:

- According to the introduction procedure, the action plan for the “networks”, “services”, and “users” (henceforth "immediate parties") will be examined.
- The action plan for the indirect parties about the cooperation will be examined so that immediate parties solve the itmes which they cannot solve by themselves, under the cooperation of the relevant parties and other elements (henceforth "indirect parties").

In the examination, the kind of relevant parties involved must be checked because the characteristics and capacity are different between immediate or indirect parties.

5.2 Players

5.2.1 Immediate parties

Because each “networks”, “services”, and “users” have some elements whose characteristic is significantly different from others, it is appropriate to examine them after further fragmentation as shown below.

（1） Network

As shown in Section 4.3, it must be examined after dividing it into “reachability” and “connectivity”.

（2） Services

The form and technical competence of “services” are extremely diverse. It is

difficult to indicate the characteristics of each player, whatever classification is used. On the other hand, the items to perform can be summarized in two items: that services can be provided through the IPv6 network, and to enable to provide services through IPv4 network to the users accommodated under NAT/NAPT. There is no major difference between the action plans. Therefore, this examination is performed without further fragmentation.

（３） Users

The form and technical competence of “users” are extremely diverse. “Users” must basically support IPv6 in their own system. Therefore, the indirect parties can be examined through fragmentation of users according to the characteristics of their devices or software. From this viewpoint, it is appropriate to subdivide “users” into three categories as shown below for examination, based on the characteristics of the device/software they own.

- "Consumers", who have high probability of using special protocols, such as communication with information appliances and games, because they use the Internet for amusement;
- "Middle-scale users," who have high probability of using package products in combination;
- "Large-scale users," who have high probability of building their own information system with independent development and advanced customization.

５.２.２ Indirect parties

It is appropriate to examine the following four types of indirect parties in addition to the above immediate parties:

- "Government," which is involved in the whole system;
- "Address administration organizations," which are the Internet-related organizations, such as the address administration organizations involved in allocation of IP addresses, and industry organizations;
- "Manufacturers and vendors," which develop and manufacture the fundamental devices and software that constitute the Internet;
- "SIer's (System Integrators) and outsourcing service providers," which develop specific products including services on the Internet.

５.３ Action plan for immediate parties

５.３.１ Action plan towards address exhaustion

（１） Action plan concerning networks

At the exhaustion of IPv4 address, which is estimated to occur at as early as

the beginning of 2011, networks must provide both the connection service using private IPv4 addresses using NAT/NAPT for the users who desire access by IPv4, and the connection service using IPv6 addresses for the users who desire global reachability. From these viewpoints, networks need to take the following actions towards the early stage of address exhaustion.

a) Action plan concerning networks ("reachability" and "connectivity")

- With the considerations described in 4.3.3 in mind, in order to enable the Internet connection using IPv6 by 2010, it is necessary to reach a fundamental agreement about the connection method of “reachability” and “connectivity” by the summer of 2008. Therefore, concerted examination must be started immediately.
- Based on the above agreement about the connection method, networks should support both IPv4 and IPv6 by 2010. In this case, not only the supporting IPv4/IPv6 in communication facilities, such as routers and switches, should be realized, but also the operation of devices and applications that are needed for stable operation of networks, such as monitoring devices and network operation systems, should be enabled to use in the IPv6 network.

  Devices and applications will need to be developed by manufacturers and vendors, and the verification of the networks also takes time. Therefore, while creating the plan for the transition to IPv6 by the end of 2008, operation skill must be improved by the start of operations.

b) Action plan for networks (reachability)

- The IP address distribution mechanism to users must be able to distribute the addresses in both IPv4/IPv6 by 2010. In this case, it is required to build the system, assuming that some users use both IPv4 and IPv6, while the other users employ only IPv6.

  Devices and applications will need to be developed by manufacturers and vendors, and the verification of the networks also takes time. Therefore, while creating the plan for the transition to IPv6 by the end of 2008, operation skill must be improved by the start of operations.
- IPv4 section in the networks must be able to introduce NAT/NAPT by 2010. In the transition to NAT/NAPT, it is assumed that anonymity in the network will increase, and it will be difficult to locate attackers. It should be noted that the access analysis feature must be enhanced, including the installation of the log storage equipment.

  Devices and applications will need to be developed by manufacturers and vendors, and the verification of the networks also takes time. Therefore, while creating the plan for the introduction of NAT/NAPT to IPv4 section in the

networks by the end of 2008, operation skill must be improved by the start of operations.

c） Action plan for networks (reachability or connectivity)

● User networks should be accommodated in both IPv4 and IPv6 by 2010. In this case, considering that users are likely to use only IPv6 for connection since 2010, it is required that user authentication will support both IPv4 and IPv6.

Devices and applications will need to be developed by manufacturers and vendors, and the verification of the networks also takes time. Therefore, while creating the plan for the transition to IPv6 by the end of 2008, operation skill must be improved by the start of operations.

● The cache DNS must support the inquiries through IPv4/IPv6 and the inquiries of IPv4/IPv6 relevant records from users by 2010.

Devices and applications will need to be developed by manufacturers and vendors, and the verification of the networks also takes time. Therefore, while creating the plan for the transition to IPv6 by the end of 2008, operation skill must be improved by the start of operations.

d） Action plan for networks (connectivity)

● Users should be able to access ISPs using IPv6 by 2010.

In this case, it is required to build the system, assuming that some users use both IPv4 and IPv6, while the other users use only IPv6.

Devices and applications will need to be developed by manufacturers and vendors, and the verification of the networks also takes time. Therefore, while creating the plan for the transition to IPv6 by the end of 2008, operation skill must be improved by the start of operations.

（2） Action plan for services

For the transition of services to IPv6, not only communication facilities, such as routers and switches, but also the service provision method must support IPv6. Additionally, the back-end system supporting service may also need to support IPv6. After the exhaustion of IPv4 address, which is estimated to start as early as the beginning of 2011, the global IPv4 addresses cannot be distributed, and some users can access only with the private addresses of IPv4 addresses. Therefore, by then, the services must enable the users under NAT/NAP to access. From these viewpoints, the services must support the following towards the early stage of address exhaustion.

● By 2010, the services on IPv4 must be able to be provided to the users accommodated under NAT/NAPT and to whom only the private addresses will

be distributed.

In changing the service provision method, changes and modifications, and verification of devices and software that are used for providing the services will be required and it is assumed that it will take time. Therefore, it is necessary to verify by the end of 2008 whether the change in the service provision method is necessary or not and to create the plan for enabling to provide their services to the users under NAT/NAPT immediately.

● Services will transit to IPv6 by 2010.

In this case, not only communication devices, such as routers/switches, but also the service provision method must support IPv6.

When in enabling to receive communication using IPv6 from the outside, the supporting IPv6 communication in security-related products such as firewall, intrusion detection/prevention devices, anti-virus gateways, and formulation of a security policy concerning IPv6 communication will be needed. Examination of the communication distribution policy using load balancer in IPv6 communication will also be needed. Therefore, the service provision method will need to be revised thoroughly. Thus, taking advantage of the renewal time of devices and the opportunity of addition of functions to the services, the transition to IPv6 must be advanced steadily.

Especially when the transition of the services to IPv6 is realized using translators, a dedicated translator is basically required for every application. We must remember that it will take time for its development and verification.

Therefore, by the end of 2008, while checking IPv4 dependability of the system concerning service provision, it is necessary to create a plan for transitioning to IPv6 immediately.

（3） Action plan for users

For users, there will be no immediate environment change before the exhaustion of IPv4 address. However, a long-term plan will often be needed for replacement of devices. From these viewpoints, it is desirable for users to take the following actions toward the early stage of address exhaustion.

a） Consumers

● It is desirable to choose the products that support IPv6 in purchasing PCs or software.

● If the special-purpose devices (network connected home appliances and game machines) with a built-in communications function do not support IPv6 when they are used for the Internet connection function, it is necessary to remember that, after the first stage of IPv4 address exhaustion, there is a possibility that

their services will be restridted.

- When purchasing communication devices, such as broadband routers, it is desirable that they support IPv6. When purchasing the devices that do not support IPv6, it is necessary to remember that, after the first stage of IPv4 address exhaustion, there is a possibility that they cannot be used.

b) Middle-scale users

- It is desirable to choose the products that support IPv6 in procurement of PCs, servers and software that communicate via the Internet with the outside world. It is desirable that the products that support IPv6 will be used for the devices and software that are likely to receive communications from the outside, such as mail servers, by 2010.
- In the introduction/renewal of relay appliances, such as routers/switches, VPN devices, and proxy servers, which may relay communication with the outside, it is desirable to choose the products that support IPv6.
- It is desirable to start the examination of a plan to transition to IPv6, bearing in mind that the information systems, including database systems and file sharing systems, will transit to IPv6 after the first stage of address exhaustion.
- Communication using IPv6 through the Internet will be started after completing the transition of security-related products, such as firewall, intrusion detection/prevention devices and anti-virus gateways, to IPv6 communication.

c) Large-scale users

- It is desirable to choose the products that support IPv6 in procurement of PCs, servers and software that communicate via the Internet with the outside world. It is desirable that the products that support IPv6 will be used for the devices and software that are likely to receive communications from the outside, such as mail servers, by 2010.
- In the introduction/renewal of relay appliances, such as routers/switches, VPN devices, proxy servers, and bandwidth control devices that may relay communication with the outside, it is desirable to choose products that support IPv6.
- It is desirable to start the examination of a plan to transition to IPv6, bearing in mind that the entire information system will transit to IPv6 after the first stage of address exhaustion. Especially, in independent development or customized systems, such as database systems and authentication systems, it is necessary to detect the implementation that depends on IPv4 promptry, and supporting IPv6 must be advanced according to modification or system

renewal. Therefore, an immediate estimate of how much time it takes for the transition to IPv6 is required.

- Communication by IPv6 through the Internet will be started after completing the transition of security-related products, such as firewall, intrusion detection/prevention devices and anti-virus gateways, to IPv6 communication.

5.3.2 Action plan in the early stage of address exhaustion

(1) Action plan for networks

- Access using IPv4 will be offered by the connection service using private IPv4 addresses with NAT/NAPT when addresses are exhausted.

(2) Action plan for services

Particular responses will be unnecessary if the change to the service provision method supporting the users to whom only the private IPv4 addresses are distributed, and the support IPv6 in the services are completed according to Section 5.2.1.

(3) Action plan concerning users

Transition to IPv6 should be promoted, because, in the Internet access service, it will be difficult to receive new distribution of IPv4 global addresses. Especially when the networks and services support IPv6, the PCs supporting IPv6 will automatically use IPv6 rather than IPv4 in communication, without users even being aware. Thus, the availability of IPv6 will increase quickly and the Internet access service using IPv4 may be reduced. On the other hand, because it takes time for the devices owned by users to support IPv6, it is desirable to take early actions if possible. From these viewpoints, users must take the following actions towards the middle stage of address exhaustion.

a) Consumers

- The products that support only IPv4 should not be selected in the purchase of PCs or software.
- The dedicated devices with built-in communication function (network connected home appliances and game machines) that support only IPv4 will be lent, not purchased. Basically, the products that support IPv6 should be selected.
- In purchasing communication devices, such as broadband routers, the products that support IPv6 should be selected.

b) Middle-scale users

- The products that support IPv6 should be selected in procurement of PCs,

servers and software that communicate via the Internet with the outside world.

- In the introduction/renewal of relay appliances, such as routers/switches, VPN devices, and proxy servers, which may relay communication with the outside, it is desirable to choose the products that support IPv6.
- The transition of security-related products, such as firewall, intrusion detection/prevention devices and anti-virus gateways, to IPv6 communication should be completed as soon as possible to enable to use IPv6.
- The planning of transition of information systems to IPv6 must be promoted.

c) Large-scale users

- The products that support IPv6 should be selected in procurement of PCs, servers and software that communicate via the Internet with the outside world.
- For relay appliances, such as routers/switches, VPN devices, proxy servers, and bandwidth control devices that may relay communication with the outside, it is desirable to choose the products that support IPv6.
- The transition of security-related products, such as firewall, intrusion detection/prevention devices and anti-virus gateways, to IPv6 communication should be completed as soon as possible to enable to use IPv6.
- The planning of transition of information systems to IPv6 must be promoted.

5.4 Spillover action plan accompanied with the actions by immediate parties

5.4.1 Action plan towards address exhaustion

(1) Action plan for networks

- As basic information for examination of a plan to transit to IPv6 by users, and to promote the transition of the services to IPv6 and their adoption of NAT/NAPT, a plan to transition to IPv6 and introduction of NAT/NAPT to IPv4 section in the networks must be released as soon as it is created. Especially, it should be notified to the customers of connection services thoroughly.

(2) Action plan for service providers

- As basic information for examination of a plan to transit to IPv6 by users, a plan to transit to IPv6 and support the users under NAT/NAPT to use IPv6 must be released as soon as it is created.
- When dedicated devices are required on the user side in providing the services and they support only IPv4, they should be lent rather than sold. If they are sold, it should be fully explained to the purchasers that they may not work after the first stage of IPv4 address exhaustion.

（３） Manufacturers and vendors of devices and software

- The information concerning the situation of support IPv6 in their products should be widely publicized so that the users of the devices and software and SIer's can use it to help to create a plan to trainsit to IPv6.
- Development of required devices, software, and operation tools should be accelerated, based on the plan of the transition of the networks and services to IPv6 and the introduction of NAT/NAPT in their network IPv4 section.

  Especially, sufficient scalability of performance must be provided, considering the increasing tendency of traffic and connection nodes.
- The devices for users should support IPv6 as soon as possible. When the devices that support only IPv4 are sold, it should be fully explained to the purchasers that they may not work after the first stage of IPv4 address exhaustion.
- The authentication logos including IPv6 Ready Logo Program by IPv6 Forum should be actively utilized so that purchasers can understand whether the devices and software support IPv6 or not.
- Research on the attack method in communication using IPv6 should be advanced, and the security-related products for IPv6 should be expanded at an early stage.

（４） SIer's and outsourcing service providers

- It should be actively notified to customers, including "large-scale users" and "services", that transition to IPv6 is required because IPv4 address will be exhausted, and that it will take time for the transition to IPv6.
- Sufficient support system should be organized to help the networks, services, and users to create the plan of the transition to IPv6.
- Because it is expected that the migration of databases will take time, it should be reported that the plan of transition to IPv6 must be created at an early stage if possible by taking advantage of system renewal.
- It should be notified widely that examination of security policies and selection of required devices/software take considerable time because the attack method in communication using IPv6 has not been sufficiently studied at present.
- After the investigation about the support in IPv6 in commercial application software, middleware, operating systems, and network devices, the necessary environment should be provided in cooperation with manufacturers and vendors if the support is insufficient.
- The outsourcing service providers should transit their services (network monitoring services and hosting services) to IPv6 by 2010.

（５） Address management organizations etc.

- It should be widely publicized that continuous utilization of IPv4 has a limit, and that it will affect the stable growth of Japanese economy, requiring the transition of the Internet to IPv6 and some actions by the users.
- This report should be widely publicized at the meetings of the international examination/adjustment concerning the Internet so that an international trend will match the policy in Japan.
- Especially, the information relevant to IPv6 should be sufficiently exchanged with the organizations of other countries, so that the communication environment of Japanese users will not differ from the that of general users in the world as a result of migration of the Internet to IPv6.

（６） Government

- This report should be widely publicized at the meetings of the international examination/adjustment concerning the Internet so that an international trend will match the policy in Japan.
- In cooperation with relevant companies and organizations, it should be widely publicized that continuous utilization of IPv4 has a limit, and that it will affect the stable growth of Japanese economy, requiring the transition of the Internet to IPv6 and some actions by the users.
- The progress of the action plan should be paid attention to, an environment should be created to facilitate smooth adjustment and negotiation between the players.
- While paying attention to the adjustment by the network-related parties especially about the action to the networks described in Section ５．２．１（１）, in case it takes a long time to consensus building , immediate solution will be urged.
- Product development should be activated including peripheral products, such as communication facilities and security-related products that will be needed for the utilization of NAT/NAPT as a temporary action and the migration of the Internet to IPv6 as a permanent action. In case the essential products that have sufficient performance and capability for the action against IPv4 address exhaustion do not exist, the budget action and the taxation system action should be examined.
- In cooperation with related organizations, support measures should be discussed about the initial cost in actions against IPv4 address exhaustion.
- The IPv6 educational program for engineers for technical skills, such as the maintenance of test beds, should be supported, so that the network-related parties, service-related parties, manufacturers and vendors, SIer's, and

outsourcing service providers can ensure the transition to IPv6 on the Internet.

- The creation of tests for engineers on the development capability for IPv6-compatible systems should be examined to offer the basis of selection to users, services, and SIer's.

5.4.2 Action plan in the early stage of address exhaustion

(1) Action plan for networks

- Schedules, such as accommodation of new customers under NAT/NAPT based on the plan of NAT/NAPT implementation in IPv4 section, and the accommodation of the existing customers under NAT/NAPT, should be released as required as the basic information in promoting the transition to IPv6 by users. While thoroughly notifying them especially to the customers of connection services, the limitation in using IPv4 for services should be widely publicized.
- The support system should be built to facilitate the utilization of IPv6 by users.

(2) Action plan for service providers

- The limitation in using IPv4 for service provision should be publicized widely to the users under NAT/NAPT.

(3) Manufacturers and vendors of devices and software

- Support IPv6 in the devices for users should be promoted.

  The devices that only support IPv4 should be lent rather than sold. If they are sold, it should be fully explained to the purchasers that they may not work in the near future.

(4) SIer's and outsourcing service providers

- Transition of user-owned systems to IPv6 should be supported.

(5) Address management organizations etc.

- It should continue to be widely publicized that continuous utilization of IPv4 has a restriction, and that it will affect the stable growth of Japanese economy, requiring the transition of the Internet to IPv6 and some actions by the users.
- This report should continue to be widely publicized at the meetings of the international examination/adjustment concerning the Internet so that an international trend will match the policy in Japan.
- Especially, the information relevant to IPv6 should be sufficiently exchanged with the organizations of other countries, so that the communication environment of Japanese users will not differ from that of general users in the world as a result of migration of the Internet to IPv6.

（６） Government

- This report should continue to be widely publicized at the meetings of the international examination/adjustment concerning the Internet so that an international trend will match the policy in Japan.
- In cooperation with relevant companies and organizations, it should continue to be widely publicized that continuous utilization of IPv4 has a restriction, and that it will affect the stable growth of Japanese economy, requiring the transition of the Internet to IPv6 and some actions by the users.
- The progress of the action plan should be paid attention to, and an environment should be created to facilitate smooth adjustment and negotiation between the players.

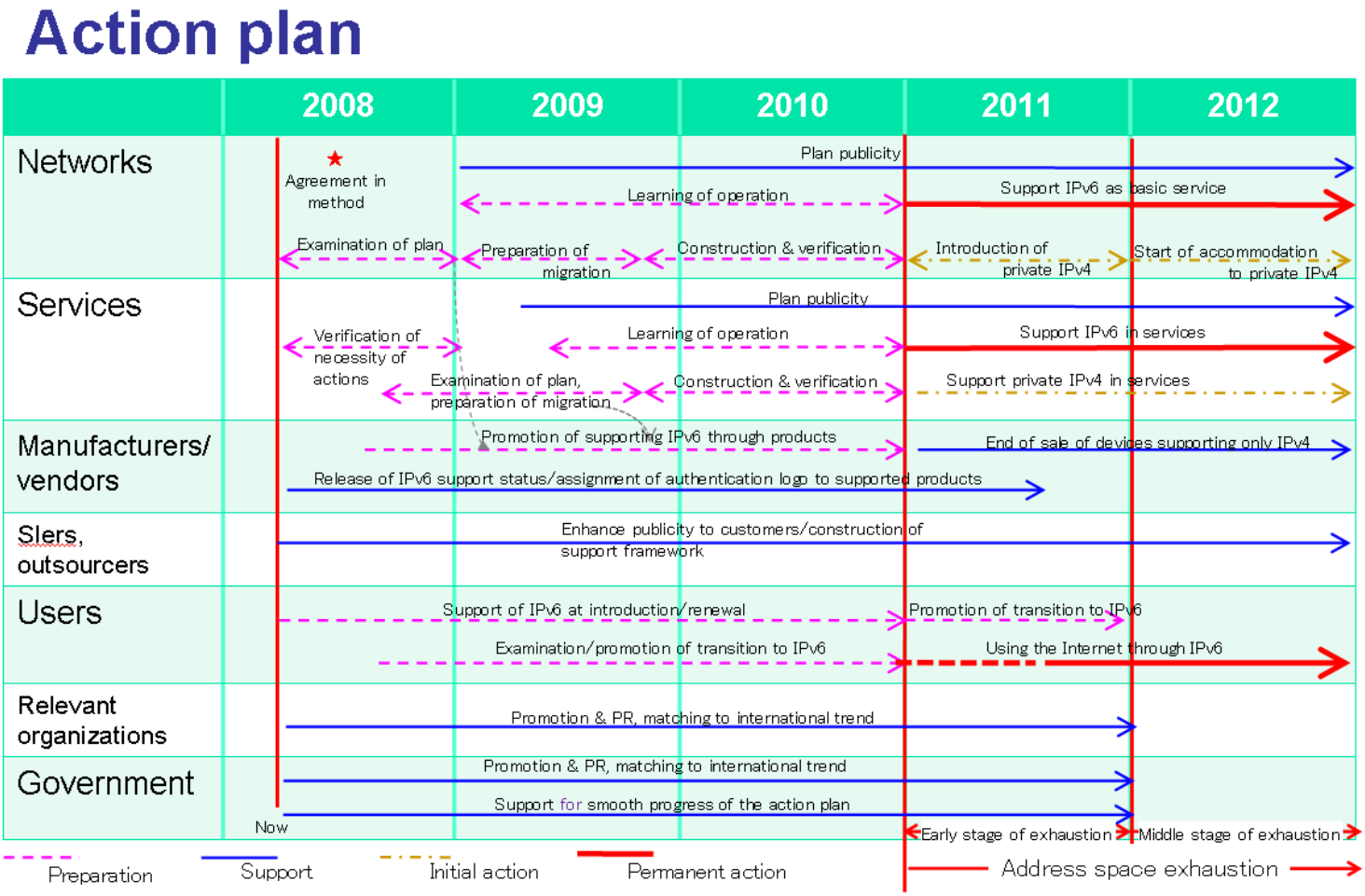


Fig. 5 - 1 Overview of the action plan

５.５ Construction of the action plan promotion framework

Not only the government but many private organizations, companies, etc. must promote the action plan shown in Section ５.４. The government will not force each player to perform what is described in the action plan. It is extremely important that each player recognizes its role and promote the actions for itself. However, the introduction method of the actions must be shared broadly. To grasp the progress, a framework is required to urge those who are behind the schedule to take actions. Therefore, it is necessary to build the promotion organization in cooperation of the government and the private sector for promoting this action plan.

On the other hand, it is not appropriate to establish separately the promotion organization to promote the transition of the Internet to IPv6, because the IPv6 Promotion Council already exists for that purpose. It is appropriate to reconstruct the council to the promotion framework of the whole country for the actions against IPv4 address exhaustion in the Internet by strengthening the function of the following IPv6 Promotion Council:

- Grasping the progress of the action plan and the transition of the Internet to IPv6
- Information sharing in action plan promotion
- Improvement of knowledge by related parties through construction, employment, etc. of the test bed
- Examination of amendment of the action plan as required

● Conclusion

As shown in this report, a true countermeasure for international exhaustion of IPv4 address is the transition of the Internet from IPv4 to IPv6, which is standardized as a successor of IPv4. The necessity of the transition of the Internet to IPv6 has been repeatedly maintained since the beginning of the 2000s, but, at present, IPv6 is used only with the services that only IPv6 can provide, assuming that IPv4 will continue to be used for the time being. However, all the international IP address management organizations, such as ICANN, have warned about international exhaustion of IPv4 addresses. Therefore, countermeasures must be taken with a sense of urgency that it is already impossible to continue to use IPv4.

Unless the Internet access services and the Internet service providers create a plan to transition to IPv6 by the end of this year, it will be difficult to tackle after the international exhaustion of IPv4 addresses. Therefore, this study group expects that all relevant parties will understand what to do and initiate the appropriate action based on this report. We also expect that the government will check whether these actions are progressing steadily and urge appropriate actions as required.

As shown at the beginning, this report is the world's first report comprehensively describing the actions to be taken by a variety of players relevant to the Internet with regard to the shortage of IPv4 addresses. It should be presented to international meetings by the government and address management organizations as a model of the transition of the Internet to IPv6 and for use as the basis for development of the Internet all over the world. We expect that this will help improvement of the presence of our country in international meetings for the Internet policy examination and strengthening of the global competitiveness of the Japanese Internet-related industries.

Reference 3: Influence of the IPv4 address exhaustion

No.	Target	Specific influence	Secondary impact	
			Target	Influence
01-01	ASP/IDC companies	Because global IP addresses are required for VPN services via the Internet, new VPN services via the Internet will be impossible. New VPN services are restricted to the IP-VPN service in closed networks.	Users Companies Universities	The VPN service through the Internet cannot be received. As a result, IP-VPN depending on the specific company's lines must be used. Therefore the introduction cost will increase.
01-02		It will be difficult to offer new hosting services. Although virtual hosts are possible, it will be impossible to meet the demand for separating the resource completely for every customer.	Users	New users can receive only shared hosting services. Flexible site management will be limited because the security policy must be adjusted, and flexible resource changes will be difficult.
01-03		Data centers/web hosting businesses can continue to provide services via virtual hosts, but the cost of providing services will be higher because of load distribution.		
01-04		Access control using IP addresses for security will be difficult to offer because of increase in users who has no global address. The authentication and access control method must be changed, resulting in a restriction of embodiment.		
01-05		New services that use many global IP addresses, such as the VOD service, cannot be developed or provided.	Companies Users	Because the ASP/SaaS type services will be restricted, improvements in productivity and the creation of new businesses utilizing them will be limited.
02-01	ISP's (existing)	It will be impossible to increase the address pool for dynamic address assignment, resulting is growing address occupancy. Therefor the failure in address acquisition will occur with increasing frequency. The quality of Internet access services will be limited. Providing new services will also be limited.	New users	Subscription to an ISP will be difficult.
			Users	The service quality will be limited for users using dynamic address services.
02-02		Services using global IP addresses (fixed address service, service that identifies a device by an IP address through the Internet, such as IP phone, etc.) cannot be developed or provided.	Users	The new utilization of fixed address services will be impossible. The new utilization of convenient services will be impossible.
02-03		It will arise that the reorganization of network configuration including the relocation of global and private addresses and the increase of routing information that is caused by the fragmentation of address space. The throughput of routers currently used may be exceeded. In this case, CPU and memory upgrades or model exchanges will be needed, leading to cost increases.		
02-04		Because both users using private addresses and users using global addresses will exist on a network provied by a company, ingenuity in the access path to servers and applications provided by the company and authentication will be needed, leading to cost increases.	Users	The users who have only private addresses will be limited availability of some applications.

02-05		Depending on the number of remaining IPv4 addresses that, the urgency of the need for the action against IPv4 address exhastion is different amang ISPs. Some ISPs may continue services for the moment, and others will need prompt action. However, even if action is taken, the service content will be restricted in some cases.	Users	When the services provided by an ISP change, users must cope with the change or migrate to other ISP. As a result, service quality will be restricted or costs will increase.
02-06		Wholesale companies must take action, resulting in cost increases. Continuity of business will be difficult, depending on the timing and the specific action.		
03-01	ISP's (new)	It will be difficult to start new ISP business because a new connection to the IPv4 Internet will be impossible. Only the commission for upper ISPs will be possible, and business expansion will be limited.	Users	The competitive activation by new entries will not be expected. Therefore the cost will increase in the long term.
04-01	Corporate networks University networks	Because a new utilization of Internet VPN will be impossib le, utilization via the Internet will be impossible with a WAN connection between the existing corporate network (university network) and any new base (branch, branch school). The connection using IP-VPN and dedicated lines will be indispensable, so that costs will increase.		
04-02		Because a new company, university, or other entity will not be able to obtain a global address, providing services and activities on a self-managed network will be restricted. An R&D-type organization will have difficulty in producing results because of insufficient flexibility in activities.		
05-01	SOHO networks Home networks	They usually depend heavily on services by ISPs because they are connected to the external network via the ISP. Use of the Internet will be restricted because of the restrictions on services by ISPs.		
06-01	End nodes (Non-PC equipment, sensors, etc.)	Utilization and provision of sensor networks will be difficult.	Users	New network services expected to appear in the future, such as remote sensing and remote control, will be impossible.
07-01	Operation staff	Operation loads will increase because ISP networks will become more complex, and it will be difficult to maintain labor conditions.	ISP's Users	System operation costs will increase. These costs will also affect service charges, resulting in higher total costs.
08-01	SIers	Because available network configurations and the variety of proposals will be restricted, it will be impossible to offer an optimum solution in a network utilization system.	Users Companies	In a network utilization system, available solutions will be limited.
08-02		The advantages or disadvantages of ASP/SaaS type services will depend on the offering of addresses rather than the content of the service, and the price system will be distorted. Therefore, solutions will be sought for a closed system rather than using a shared service. Thus, the supply formats of solutions will be restricted and costs will increase.	Users Companies	Utilization of a platform-type shared service will be difficult. The overhead for business continuity and costs will increase in small companies.
09-01	Vendors	It is necessary to develop a new design method that assumes the shortage of addresses in offering new functions and device maintenance using the network, Therefor cost will increase.	Users Companies	It will be necessary to perform the introduction, operation, and maintenance, considering the utilization format assuming the address shortage for new functions and device maintenance, leading to cost increases.
09-02		New technical development will be needed for maintenance and operations of address translation and redundancy. Therefor cost will increase.		

09-03		It is uncertain that how long does the prevention technology for address shortage is efficient . (it is difficult to estimate when it will be unnecessary by introducing IPv6) The risk of development and the adoption of such technology is high. Therefore, decision-making by management will be difficult.		
10-01	Users	It will be impossible to use some services and applications via the Internet, for example applications that require P2P connections and server system services in a new field. In some cases, even if the communication sender is provided the services, it will be impossible to connect to the receiver depending on receiver's environment.	Users Economy	By restricting information exchange between users on the Internet, the buying motivation through the Internet currently maintained with substantial information will be discouraged. Therefore expansion of the Internet economy will be difficult.
10-02		Technical and cost burdens will be passed on to users, and the cost paid by users will increase.		
11-01	IP phone	Expansion of the use of Internet telephones using global IP addresses will be impossible. The network configuration for a carrier with regard to Internet telephones will be complicated because of the combined use of private addresses, and costs will increase for maintenance and operation.	Companies ISP's	Although private addresses will be possible, the costs will increase in small and medium-sized companies because gateways will have to be installed. The costs will also increase in ISPs because of the increase in the overhead costs caused by utilization of Centrex.
11-02		The expansion of usage of VoIP applications that require global addresses, such as Internet TV conference systems will be impossible.		
12-01	New services	Industries and regions that have not used the Internet until now but will try to use it, will not be able to enter the market with services that support health, medical treatment, welfare, nursing, and management services, such as production, facilities, city management, security services, and two-way services for content delivery and games.	Users	It will be impossible to provide new Internet services by the businesses.
			Macroeconomy	Because it will be impossible to provide new services via the Internet, the migration to the Internet economy will not advance. The Internet economy that is supposed to continue expanding will be unable to develop.
12-02		In future network services with high mobility, including onboard networks, the assumed service content will be restricted.		
12-03		In home networks, the services that control or monitor electric appliances at home externally via HGW will be restricted.		
13-01	Macroeconomy	The potential growth rate generated by productivity growth using ICT will be restricted because the Internet utilization service will hit the ceiling.	Macroeconomy	The companies that receive substantial benefit from the expansion of the Internet economy will have a difficulty in sustention of stock prices because of the uncertainty of growth.
14-01	Other	When the black market that trades in IPv4 addresses appears, an address area that cannot ensure reachability to the whole Internet may be generated because the authentication of address utilization cannot be proved. It will be difficult to maintain reachability and reliability for the whole IPv4 Internet.		
14-02		The diffusion rate of the current Internet will be fixed, and regional differences will occur. The Internet will be continuously used in urban areas, but expansion of Internet use will be difficult in rural areas.		

Reference 6:
Evaluation results of three measures for IPv4 address space exhaustion

Reference 6-1

Utilization of NAT/NAPT

	Positive opinions	Negative opinions
Utilization style	(1) It functions as part of security countermeasures, because the restriction of access from outside is caused.	(1) Communication between users who are assigned only private IP addresses is difficult. [Reason] It is difficult to specify the nodes inside LAN side from the WAN side beyond NAT/NAPT. However, it can be solved partly by relaying data via a server assigned a global IP address. (2) Decrease of the transmission speed occurs because of address translation. [Reason] It is necessary to manage the information for address translation in NAT/NAPT. When large-scale operation were done, the relevant information becomes huge and the required time taken for address translation increases. (3) Communication using a protocol that includes address information in payload needs to be managed individually. [Reason] NAT/NAPT traversal communications with protocols that have data transport including address information in themselves, such as SIP and IPsec, or the protocols having difficulty to convert by GW require individual ALG for each . However, support for all communication applications is practically impossible. (4) Duplication of the address occurs [Reason] There are chances that the communication between nodes accommodated under different NAT/NAPT becomes impossible depending on the communication applications. Because there is a possibility that two or more nodes may use a same private IP address in such a case. (5) Anonymity grows in negative meaning. [Reason] The logged data has to be discarded after a short term because of very high storage cost for NAT/NAPT. Therefore, it is difficult to specify the user who acts maliciously among the users who are sharing the same global IP address.

Network configuration	(1) The current devices can be used as it is. [Reason] Because Current devices are going on to use IPv4 addresses as usual, adding equipments for NAT/NAPT or modifications to the settings is possible measure.	(6) The IP addresses assigned for the current existing appliance must be renumbered. [Reason] The addressing architecture must be changed with the introduction of NAT/NAPT. (7) Extension of private IPv4 address space need to be considered. [Reason] Considering the large scale usage of NAT/NAPT, it is expected to consider the extension private IPv4 address space beforehand.
Operation	(2) There is much technical knowledge that has been accumulated. [Reason] Because NAT/NAPT is used widely at present.	(8) The operability when NAT/NAPT is used in a large-scale network is uncertain. [Reason] It is mostly used in comparatively small-scale networks such as CATV and business enterprise networks, and operational experience in large-scale networks is scarce. Therefore, it is uncertain how massive aggregation of networks by using NAT/NAPT would be possible at present moment, and expertise must be established. (9) Operability of multi-stage NAT is uncertain. [Reason] Because the operation experience using multi-stage NAT in a large-scale network is scarce, feasibility is uncertain. (10) Some can save addresses, while others cannot. [Reason] It is impossible to use NAT/NAPT by who wants to receive public access, such as operators of websites, and they can't save addresses. On the other hand, Internet service providers may be able to produce a surplus of many global IPv4 addresses by using NAT/NAPT. (11) Caution about patents must be considered. [Reason] Because it is necessary to use NAT/NAPT in combination with ALG for individual communication applications, it may conflict with unknown patents as a result of technical patches.

Cost	(3) The cost to change protocols is unnecessary. [Reason] Because IPv4 addresses will be used for operations in the same way as in the present operation.	(12) Investment of network supplier companies will be greater. [Reason] It is necessary to install equipment for each of a certain number of users. And cost also increases as the aggregation advances, it is difficult to estimate the entire cost that would be required.

Reference 6-2

Reallocation of the assigned IPv4 addresses

	Positive opinions	Negative opinions
Utilization style		
Network configuration	(1) The current devices can be used as it is. [Reason] Because IPv4 addresses will be used for operations in the same way as in the present operation..	(1) The mechanism for notifying proper address users must be established. [Reason] New mechanism to guarantee identifying address user will be required to guarantee the correct data transport.
Operation	(2) The available addresses may increase with changes in the address allocation policy.	(2) The capability of measure for address demand is not enough. [Reason] New address demand at present throughout the world has reached 5% of all IPv4 addresses. It will be difficult to fulfill even immediate demand. Because considerable system recovery costs will be required especially for returning surplus addresses, a fairly powerful incentive or compelling force for doing it will be required. (3) When consensus will be built concerning changes in address allocation policy is uncertain. (4) The addresses will run out someday at all. [Reason] New address demand at present throughout the world has reached 5% of all addresses. The addresses will run out someday, no matter how efficient distribution may be. (5) Management of the routing path will be difficult. [Reason] If the addresses are fragmented and assigned regardless of the area, management of routing information will be difficult.

Cost	(3) The cost to change protocols is unnecessary. [Reason] Because IPv4 addresses will be used for operations in the same way as in the present operation.	(6) Management of the routing path will be difficult. [Reason] If the addresses are fragmented and assigned regardless of the area, management of routing information is difficult, resulting in cost increase in all network operators.

Reference 6-3

Transition to IPv6

	Positive opinions	Negative opinions
Utilization style	(1) Abundant IP addresses can be used. [Reason] Because there are a huge number (2^{128}) of IPv6 addresses. (2) Transition to IPv6 facilitates usage of devices/applications which assume end-to-end operations.	(1) There are devices and applications that do not support IPv6 [Reason] Many old devices and applications support only IPv4. Some devices that support IPv6 have basic functions, but they often have no functions that are required in real-world networks such as redundancy. (2) Implementation of IPv6 is unstable yet.
Net configuration	(4) Efficient and easy-to-use networks suitable for current use can be built when the IPv6 would be introduced. [Reason] The IPv4 network was built by patching conventional technology. In the migration to new technology, the network suitable for current use can be created. (5) Network design (address design) becomes easy. [Reason] Because there are abundant IPv6 addresses. (6) Development into larger-scale network usage becomes easy. [Reason] Because address and routing management will be simplified.	(3) The networks must be redesigned. [Reason] Appropriate network resizing will be necessary to decrease burden that comes from adding IPv6 function into network devices. (4) IPv4 will continue to be indispensable on the server side. [Reason] As long as IPv4 exists on the client side, global IPv4 will continue to be required on the server side.
Operation	(7) Network management becomes easy. [Reason] In IPv6 network, we can use abundant addresses. It is possible to take advantage of its functions to build easy operation network.	(5) Both IPv4 and IPv6 networks must be operated concurrently for a certain period. [Reason] It cannot be assumed that IPv4 addresses will transit to IPv6 addresses instantly. The transition period will last for a few years to some decades. During the transition period, ISPs will need to consider whether to operate the IPv4/IPv6 dual stack network or to use translators for connecting the IPv4 and IPv6 networks. When employing an IPv4/IPv6 dual stack network, the design, construction, and testing will take some time (even if it does not double).

Operation		(6) Because the influence on users will be the greatest, providers will need to take action. [Reason] The actions by companies providing network services are also required in proportion to the burden on users. But supporting IPv6 may not advance because the companies cannot expect to recover the costs of supporting IPv6 under the present circumstances. (7) It is necessary to consider how to introduce IPv6. [Details] There are two options that must be considered: transit to IPv6 with actively eliminating the existing IPv4 network, or as long as users demand keep refining IPv4 network. (8) Accumulation of technical expertise is scarce, and the number of engineers is few. [Reason] Because the operation of IPv6 is not widespread, operational experience is insufficient. Even if there is operations management engineers who can design and construct a IPv4/IPv6 network, very few of them can isolate faults of networks. Therefore, it will be necessary to educate engineers. (9) User support will take much time and effort. [Reason] Current users do not recognize that they are using IPv4. Therefore, it is necessary to explain the change to IPv6 and provide technical support after the change. (10) Aspects of operations and securities will take much time. [Reason] With regard to the idea of network security, maintenance and operation, in some areas there are the big difference in IPv6 from IPv4 rather than the IP transport itself. Therefore, it will take much time to disseminate the information of this recognition and construct the environment for fitting above.

Operation		(11) The consideration is necessary not to bring any differences in our services. [Reason] From a management perspective, it is necessary to ensure that there are no differences between the services provided to IPv6 users and IPv4 users.
Cost		(12) The prices of network devices are expensive compared with IPv4. [Reason] Because the devices that support IPv6 also support IPv4, these devices are more expensive than devices that support only IPv4. (13) Migration costs are enormous. [Reason] Introduction and modification of equipment and verification during the introducing devices cost a great deal of money, depending on the conformance with IPv6 specifications of the devices and applications.

Reference 7:

List of problems with measures for IPv4 address exhaustion

Reference 7-1: Problems accompanying the transition to IPv6 of the Internet

Category a No particular problems.
b Although there are products, there is no operational capability, or the operational experience is insufficient.
c Although there are products, operational tools are insufficient.
d Although there is technology, there are no products.
e There is no technology.

Note: The existence of the above products are restricted as far as known to the members.
Regarding non general purpose product including self developed one, the term "products" above may be interpreted to "objects" and "There is no" may be interpreted to "Modification should be for".

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Consumer users	Devices	PC	a/b	-Possible if the newest software including OS is used. Example: In the case of Windows, Vista or later is necessary (Windows XP does not support DNS and file sharing using IPv6). -The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.	a/b	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.	a/b	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.
		Network connected home appliances	a/d	-Many of the devices including DLNA device are supporting only IPv4. -IPv4 may be going to continue to be indispensable, because some devices have difficulty in updating after shipment.	a/d	-Few devices are supporting IPv6 now. -Uncertainty about the state synchronization at backup redundancy (may be lacking in stability). -Enough performance may not be obtained for video.	a/d	-Few devices are supporting IPv6 now. -Uncertainty about the state synchronization at backup redundancy (may be lacking in stability). -Enough performance may not be obtained for video.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Consumer users	Devices	Devices, such as game machines, that are likely to use special ports	a/d	-Many of the devices are supporting only IPv4. -IPv4 may be going to continue to be indispensable because some devices have difficulty in updating after shipment.	a/d	-Few devices are supporting IPv6 now. -Uncertainty about the state synchronization at backup redundancy (may be lacking in stability). -Simultaneity in communication may	a/d	-Few devices are supporting IPv6 now. -Uncertainty about the state synchronization at backup redundancy (may be lacking in stability). -Simultaneity in communication may
		CPE	a/b/c/d	-Required functions are dependent on the network architecture. -There are some products including DSL modems that do not support IPv6 and have no development plan. -Remote monitoring functions using IPv6 must be developed. -Most equipments at the present are supporting only IPv6 pass-through and cannot perform IPv6 routing. Therefore, it is difficult to manage the devices supporting IPv6. -IPv6 is inferior in throughput to IPv4. -NAT which practically functions as a firewall will be removed. -The existing devices are inferior in the security related functions (packet filter, SPI, IDS, and firewall). -The function to upgrade the old devices at home that support only IPv4 to IPv6-enable may be required.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Consumer users	Applications	E-mail	a/b	-Generally possible if the newest software is used. Example: Thunderbird, Becky!, Winbiff, etc. -Fall back may be occurred, although it depends on the DNS.	a/b		a/b	
		Web browsing	a/b	-Generally possible if the newest software is used. Example: Internet Explore, Firefox, Opera, etc. -Fall back may be occurred, although it depends on the DNS.	a/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	a/d	-The service side must provide a translator for each application.
		VoIP	a/b/d	-Depends on products. -The network must provide DNS that support each of IPv4/v6.	a/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	a/d	-The service side must provide a translator for each application.
		Streaming	a/d	-Depends on products. -The network must provide DNS that support both IPv4/v6.	a/d		a/d	-The service side must provide a translator for each application.
		Dynamic DNS	d					
		P2P application	a/d	-Depends on applications.	a/d	-Depends on applications. -There may be much content that cannot be supported by a translator (those are including the address in the payload section).	a/d	-Depends on applications. -The service side must provide a translator for each application
		NTP	a		a	-Simultaneity in communication may not be ensured.	a	-Simultaneity in communication may not be ensured.
		Personal firewall	a	-Generally possible if the newest software is used				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Middle scale users	Devices	PC	a/b	-Possible if the newest software including OS is used. Example: In the case of Windows, Vista or later is necessary (Windows XP does not support DNS and file sharing with IPv6). -The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient. -Remote maintenance tools are insufficient.	a/b	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.	a/b	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.
		Servers	a/b/d	-Possible if the newest software including OS is used. Example: In the case of Windows Server, 2008 or later is necessary. -Software upgrage is needed in many cases. -Kind of middleware may need to be modified. -The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient. -Remote maintenance tools are insufficient.	a/b/d	The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.	a/b/d	The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Middle scale users	Devices	Routers/switches	a/b/c	-The management function using IPv6 must be developed. -Remote maintenance tools are insufficient. -Many existing devices do not support IPv6 and they are likely to be replaced. -Even if the devices are supporting IPv6, stability may decrease. Especially in the case of old devices, throughput with IPv6 may decrease significantly as compared with IPv4. -Some routers/switches accommodating servers have problems in the redundancy (ALAXALA, NEC, and Nokia have completed implementation). -Being careful with setup of the security related functions (packet filter, SPI, IPSec, etc.) may be difficult, because the address length is long in IPv6.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Middle scale users	Devices	Firewall	b/c	-Few products are supporting IPv6. -In some products, coverage of supporting level is unclear, which including whether the policy rule depending on the address can be created under the IPv6 environment. -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed. -There may be some problems in controlling the IPv6 extended header (RFC 4942). -Difficulty in state synchronization at redundancy. -Throughput with IPv6 may decrease significantly as compared with IPv4. -Operation expertise must be reconstructed.	b	-It is uncertain whether the address-based policy can be described properly.	b	-It is uncertain whether the address-based policy can be described properly.
		IDS/IPS	b/c/d	-Few products are supporting IPv6. -In some products, coverage of supporting level is unclear, which including whether the policy rule depending on the address can be created under the IPv6 environment. -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed. -Difficulty in state synchronization at redundancy. -Throughput with IPv6 may decrease significantly as compared with IPv4.	b	-It is uncertain whether the address-based policy can be described properly.	b	-It is uncertain whether the address-based policy can be described properly.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Middle scale users	Devices	Antivirus gateways	b/c/d	-Few products are supporting IPv6. -In some products, coverage of supporting level is unclear, which including whether the policy rule depending on the address can be created under the IPv6 environment. -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed. -Some DNS-based Black hole lists do not support IPv6. -Difficulty in state synchronization at redundancy. -Throughput with IPv6 may decrease significantly as compared with IPv4.	d	-It is uncertain whether the address-based policy can be described properly.	d	-It is uncertain whether the address-based policy can be described properly.
		Proxy servers	b/c/d	-Standalone proxy servers are provided. -Some Web servers have the proxy function. Example: Apache, IIS2003 -Many proxy servers with embedded appliance do not support IPv6. -Difficulty in state synchronization at redundancy. -Throughput with IPv6 may decrease significantly as compared with IPv4. -Filtering conditions may not be able to specified carefully.	b/c/d	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.	b/c/d	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Middle scale users	Devices	VPN devices	a/b	-Operation expertise must be reconstructed.	a/b	-Improper operation may be occurred. -SSL VPN is possible. -IPsec VPN is unavailable when using automatic key management (because it negotiates with a traffic selector at key exchange), but it is available with manual key management.	a/b	-Improper operation may be occurred. -SSL VPN is possible. -IPSec VPN is unavailable when using automatic key management (because it negotiates with a traffic selector at key exchange), but it is available with manual key management.
		Office equipment	b	-Few products are supporting IPv6.	b		b	
	Applications	E-mail (including content DNS)	a/b	-Generally possible if the newest software is used. Example: Sendmail, bind -Whole DNS tree must support both IPv4 and IPv6. -Operation expertise must be reconstructed. -DNS must support each of IPv4/v6. -DNS may cause a fall back to the other side of communication.	a/b		a/b	
		Web browsing	a/b/d	-Generally possible if the newest software is used. Example: IE, Firefox, Opera -Operation expertise must be reconstructed. -DNS must support each of IPv4/v6.	a/b	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	a/b	-Depends on applications. -The service side must provide a translator for each application.
		VoIP	a/b/d	-Operation expertise must be reconstructed. -DNS must support each of IPv4/v6.	a/b	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	a/b	-Depends on applications. -The service side must provide a translator for each application.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Middle scale users	Applications	DHCP	a/b/c/d	-Generally possible if the newest software is used. Example: Windows Vista, ISC-DHCP, WIDE-DHCPv6, Dibbler -However, no products support full specifications. -Operation expertise must be reconstructed..				
		Authentication	a/b/d	-Some RADIUS products support IPv6 Example: Fullflex RADIUS -Active Directory authentication does not support IPv6. -The quarantine network and the filtering by the L2 switch may not function. -Operation expertise must be reconstructed.	a/b/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section). -Man-in-the-middle problems may occur.	a/b/d	-Depends on applications. -The service side must provide a translator for each application. -Man-in-the-middle problems may occur.
		DB	b/d	-Generally possible if the newest DMBS is used. Example: DB2, PostgreSQL, and IBM DB2 (Oracle have not supported IPv6 yet) -Though DBMS support IPv6, individual databases may need to be modified. -It is possible to support IPv6 only in the DB front. -Operation expertise must be reconstructed.	b/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	b/d	-Depends on applications. -The service side must provide a translator for each application.
		NTP	a	-Example: ntpd	a	-Simultaneity in communication may not be ensured.	a	-Simultaneity in communication may not be ensured.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Devices	PC	a/b	-Possible if the newest software including OS is used. Example: In the case of Windows, Vista or later is necessity (Windows XP does not support DNS and file sharing with IPv6). -The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient. -Remote maintenance tools are insufficient.	a/b	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient	a/b	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient
		Servers	a/b/d	-Possible if the newest software including OS is used. Example: In the case of Windows Server, 2008 or later is required. -Software upgrade is needed in many cases. -It is likely that middleware must be modified. -The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient -Remote maintenance tools are insufficient.	a/b/d	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient	a/b/d	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Devices	Routers/switches	a/b/c	-The management function using IPv6 must be developed. -Remote maintenance tools are insufficient. -Many existing devices do not support IPv6 and they are likely to be replaced. -Even if the devices are supporting IPv6, stability may decrease. Especially in the case of old devices, throughput with IPv6 may decrease significantly as compared with IPv4. -Some devices accommodateing server have problems in the redundancy of routers/switches accommodated in servers (ALAXALA, NEC, and Nokia have completed implementation). -Being careful with setup of the security related functions (packet filter, SPI, IPSec, etc.) may be difficult because the address length is long in IPv6.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Devices+	Firewall	b/c	-Few products are supporting IPv6 -In some products, support coverage of supporting level is unclear, which including whether the policy rule depending on the address can be created under the IPv6 environment -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed -There may be some problems in controlling the IPv6 extended header (RFC 4942) -Difficulty in state synchronization at redundancy -Throughput with IPv6 may decrease significantly as compared with IPv4 -Operation expertise must be reconstructed	b	-It is uncertain whether the address-based policy can be described properly.	b	-It is uncertain whether the address-based policy can be described properly.

		Field	When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Devices+	IDS/IPS	b/c/d	-Few products are supporting IPv6 -In some products, coverage of supporting level is unclear, which including whether the policy rule depending on the address can be created under the IPv6 environment. -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed -Difficulty in state synchronization at redundancy -Throughput with IPv6 may decrease significantly as compared with IPv4 -Operation expertise must be reconstructed	b	-It is uncertain whether the address-based policy can be described properly.	b	-It is uncertain whether the address-based policy can be described properly.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Devices	Antivirus gateways	b/c/d	-Few products are supporting IPv6. -In some products, it is unclear whether the policy rule depending on the address can be created under the IPv6 environment. -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed. -Some DNS-based black hole lists do not support IPv6 -Difficulty in state synchronization at redundancy -Throughput with IPv6 may decrease significantly as compared with IPv4 -Operation expertise must be reconstructed	d	-It is uncertain whether the address-based policy can be described properly.	d	-It is uncertain whether the address-based policy can be described properly.
		Proxy servers	b/c/d	-Standalone proxy servers are provided. -Some Web servers have the proxy function. Example: Apache, IIS2003 -Many proxy servers with embedded appliance do not support IPv6. -Difficulty in state synchronization at redundancy. -Throughput with IPv6 may decrease significantly as compared with IPv4. -Filtering conditions may not be able to specified carefully. -Compared with IPv4, there is difficulty in using IPv6 in large scale usage.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Devices	Bandwidth control equipment	b/c/d	-Some products exists, but dedicated products are rare. Example: PureFlow, as a dedicated product. -This function is implemented in many routers. -The management function using IPv6 must be developed.				
		VPN devices	a/b/d	-Operation expertise must be reconstructed. -Throughput with IPv6 may decrease significantly as compared with IPv4. -In many cases, multicast is supported only for IPv4.	a/b	-Improper operation may be occurred. -SSL VPN is possible. -IPsec VPN is unavailable when using automatic key management (because it negotiates with a traffic selector at key exchange), but it is available with manual key management.	a/b	-Improper operation may be occurred. -SSL VPN is possible. -IPsec VPN is unavailable when using automatic key management (because it negotiates with a traffic selector at key exchange), but it is available with manual key management.
		Office equipment	b	-Few products are supporting IPv6.	b		b	
	Applications	E-mail (including content DNS)	a/b	-Generally possible if the newest software is used. Example: Sendmail, bind -Whole DNS tree must support both IPv4 and IPv6. -DNS must support each of IPv4/v6. -Throughput with IPv6 may decrease significantly as compared with IPv4. -Filtering conditions may not be able to specified carefully. -DNS may cause a fall back to the other side of communication. -Operation expertise must be reconstructed.	a/b		a/b	

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Applications	Web browsing	a/b	-Generally possible if the newest software is used. Example: IE, Firefox, Opera -Operation expertise must be reconstructed. -DNS must support each of IPv4/v6. -Throughput with IPv6 may decrease significantly as compared with IPv4. -Changing of the proxy setting according to a destination address may not be specified.	a/b	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	a/b	-Depends on applications. -The service side must provide a translator for each application
		VoIP	a/b/d	-DNS must support each of IPv4/v6. -Call agents must be reconstructed -Throughput using IPv6 may decrease significantly as compared with IPv4.	a/b	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	a/b	-Depends on applications. -The service side must provide a translator for each application
		DHCP	a/b/c/d	-Generally possible if the newest software is used. Example: Windows Vista, ISCDHCP, WIDEDHCPv6, Dibbler -However, no products support full specifications. -Operation expertise must be reconstructed -Throughput using IPv6 may decrease significantly as compared with IPv4.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Large scale users	Applications	Authentication	a/b/d	-Active Directory authentication does not support IPv6. -Some RADIUS products support IPv6. Example: Fullflex RADIUS -However, standardization of some parameters required as RADIUS is being discussed. -Operation expertise must be reconstructed. -Throughput using IPv6 may decrease significantly as compared with IPv4. -The quarantine network and the filtering by the L2 switch may not function.	a/b/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section). Man-in-the-middle problems may occur	a/b/d	-Depends on applications. -The service side must provide a translator for each application. -Man-in-the-middle problems may occur.
		DB	b/d	-Generally possible if the newest DMBS is used. -Though DBMS support IPv6, individual databases may need to be modified. -It is relatively easy to support IPv6 only in the DB front. -Operation expertise must be reconstructed. -Throughput using IPv6 may decrease significantly as compared with IPv4.	b/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	b/d	-Depends on applications. -The service side must provide a translator for each application
		Business applications	d	-It is likely that modification is required.	d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	d	-Depends on applications. -The service side must provide a translator for each application
		NTP	a		a	-Simultaneity in communication may not be ensured.	a	-Simultaneity in communication may not be ensured.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Network（Internet）	Devices	Routers/switches	a/b	−Although operation experience is insufficient in many cases, some scientific systems and ISPs are already under operation − There is a possibility that operations such as emergency update may increase, because the bugs and vulnerabilities relating IPv6 have not been sufficiently corrected. −Operation expertise must be reconstructed −Some old devices must be replaced −Remote maintenance tools are insufficient −Stability may decrease −In the case of old devices and those for small and medium scale users, throughput using IPv6 may decrease significantly as compared with IPv4. −Some devices have problems in the redundancy of routers/switches accommodated in servers (ALAXALA, NEC, and Nokia have completed implementation) −Being careful with setup of the security related functions (packet filter, SPI, IPSec, etc.) may be difficult because the address length is long in IPv6.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Network（Internet）	Devices	Accommodation equipment	a/d	−Depends on architecture . −The products that do not support IPv6 must be renewed. −The products authorized by Cable Labs (DOCSIS3.0) are required in the CATV industry.				
		Servers	a/b/d	−Operation experience is insufficient in many cases. −Operation expertise must be reconstructed. −The products that do not support IPv6 must be renewed. −The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient. −Throughput using IPv6 may decrease significantly as compared	a/b/d	−The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.	a/b/d	−The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.
		Monitoring devices	d	−The function of the product is insufficient −The products that do not support IPv6 must be renewed. −The monitoring function using IPv6 must be developed.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Network（Internet）	Applications	Cache DNS	b/c	-Generally possible if the newest software is used. -Operation experience is insufficient in many cases. -Operation expertise must be reconstructed. -The whole DNS tree must support IPv6 -Throughput using IPv6 may decrease significantly as compared with IPv4. -DNS is likely to cause fall back to the other side of communication.	b		b	
		Maintenance/operation tools	c/d	-The monitoring function using IPv6 needs to be developed. -The reporting function etc. will be limited (flow information).				
		Authentication	c/d	-Some products support IPv6. Example: Fullflex RADIUS -However, standardization of some parameters required as RADIUS is being discussed -Operation expertise must be reconstructed -Throughput using IPv6 may decrease significantly as compared with IPv4.	a/b/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section). Man-in-the-middle problems may occur	a/b/d	-Depends on applications. -The service side must provide a translator for each application. -Man-in-the-middle problems may occur.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Network (Internet)	Applications	DHCP	b/c/d	– Generally possible if the newest software is used. Example: Windows Vista, ISCDHCP, WIDEDHCPv6, Dibbler – However, no products support full specifications. –Operation expertise must be reconstructed –Throughput using IPv6 may decrease significantly as compared with IPv4.				
		Access analysis	b/c/d/e	–The access analysis–based on reverse DNS lookup is almost impossible. –The access analysis–based on a database is technically possible.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Devices	Routers/switches	a/b	−Although operation experience is insufficient in many cases, some scientific systems and ISPs are already under operation − There is a possibility that operations such as emergency update may increase, because the bugs and vulnerabilities relating IPv6 have not been sufficiently corrected. −Operation expertise must be reconstructed −Some old devices must be replaced −Remote maintenance tools are insufficient −Stability may decrease −In the case of old devices and those for small and medium scale users, throughput using IPv6 may decrease significantly as compared with IPv4. −Some devices have problems in the redundancy of routers/switches accommodated in servers (ALAXALA, NEC, and Nokia have completed implementation) −Being careful with setup of the security related functions (packet filter, SPI, IPSec, etc.) may be difficult because the address length is long in IPv6.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Devices	Servers	a/b/d	-Possible if the newest software including OS is used Example: In the case of Windows Server, 2008 or later is required -Middleware/contents accommodated in servers must be verified individually. -Operation experience is insufficient in many cases -Operation expertise must be reconstructed -The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient -Remote maintenance tools are insufficient	a/b/d	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.	a/b/d	-The mechanism of selecting a suitable communication method under the v4/v6 mixed environment is insufficient.
		Load balancers	b/d	-There are only a few products. Example: BIGIP -The management function using IPv6 must be developed. -Operation expertise must be reconstructed. -Remote maintenance tools are insufficient. -Throughput using IPv6 may decrease significantly as compared with IPv4.				

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Devices	Firewall	b/c	-Few products are supporting IPv6 -In some products, support coverage of supporting level is unclear, which including whether the policy rule depending on the address can be created under the IPv6 environment -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed -There may be some problems in controlling the IPv6 extended header (RFC 4942) -Difficulty in state synchronization at redundancy -Throughput with IPv6 may decrease significantly as compared with IPv4 -Operation expertise must be reconstructed	b	-It is uncertain whether the address-based policy can be described properly.	b	-It is uncertain whether the address-based policy can be described properly.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Devices	IDS/IPS	b/c/d	'-Few products are supporting IPv6 -In some products, coverage of supporting level is unclear, which including whether the policy rule depending on the address can be created under the IPv6 environment. -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed -Difficulty in state synchronization at redundancy -Throughput with IPv6 may decrease significantly as compared with IPv4 -Operation expertise must be reconstructed	b	-It is uncertain whether the address-based policy can be described properly.	b	-It is uncertain whether the address-based policy can be described properly.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Devices	Antivirus gateways	b/c/d	-Few products are supporting IPv6. -In some products, it is unclear whether the policy rule depending on the address can be created under the IPv6 environment. -Filtering conditions may not be able to specified carefully. -The management function using IPv6 must be developed. -Some DNS-based black hole lists do not support IPv6 -Difficulty in state synchronization at redundancy -Throughput with IPv6 may decrease significantly as compared with IPv4 -Operation expertise must be reconstructed	d	-It is uncertain whether the address-based policy can be described properly.	d	-It is uncertain whether the address-based policy can be described properly.
		Translator (NATPT) (This deals with the interconversion of IPv4 and IPv6 in			d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).		
		Translator (ALG) (This deals with the interconversion of IPv4 and IPv6 by referencing Layer 5 or above)					d/e	-A translator must be provided for each application.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Applications	Contents DNS	a/b	-Generally possible if the newest software is used. Example: bind -Operation experience is insufficient in many cases. -Operation expertise must be reconstructed. -The whole DNS tree must support IPv6. -The web for registration of registrars must support IPv6. -There are few domain registration companies that provide the interface to register the AAAA records to the NS server in a domain. -Throughput with IPv6 may decrease significantly as compared with IPv4.	a/b		a/b	
		E-mail (including content DNS)	a/b	-Generally possible if the newest software is used. Example: Sendmail -Operation expertise must be reconstructed. -Access controls, such as junk emails, cannot be performed. -Throughput with IPv6 may decrease significantly as compared with IPv4. -DNS must support each of IPv4/v6. -DNS is likely to cause fall back to the other side of communication.	a/b		a/b	

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Applications	Authentication	a/b/d	-Some products are supporting IPv6. Example: Fullflex RADIUS -However, standardization of some parameters required as RADIUS is being discussed -Operation expertise must be reconstructed -Throughput using IPv6 may decrease significantly as compared with IPv4.	a/b/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section). Man-in-the-middle problems may occur	a/b/d	-Depends on applications. -The service side must provide a translator for each application. -Man-in-the-middle problems may occur.
		html/file	a/b	-Generally possible if the newest server software is used. Example: IIS, Apache -Though the server software supports IPv6, the contents may need to be modified. -Operation expertise must be reconstructed. -Throughput with IPv6 may decreas significantly as compared with IPv4. -It may be impossible that the region for contents distribution is limited-based on the user's IP address.	a/b/d	-There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	a/b/d	-Depends on applications. -The service side must provide a translator for each application

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Applications	DB	b/d	−Generally possible if the newest DMBS is used. −Even though DBMS support IPv6, individual databases may need to be modified. −Operation expertise must be reconstructed. −It must be examined whether the IPv6 support is really necessary or not (the backend may be used even if it only supports IPv4). −Throughput with IPv6 may drop significantly as compared with IPv4.	b/d	−There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	b/d	−Depends on applications. −The service side must provide a translator for each application
		Application servers	b	−Generally possible if the newest server software is used. −Though the server software supports IPv6, applications may need to be modified individually. −Throughput with IPv6 may decrease significantly as compared with IPv4.	b	−Development is required. −There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	b	−Development is required. −Depends on applications. −The service side must provide a translator for each application
		Streaming	a/b/d	−Depends on products. −Operation experience is insufficient in many cases. −Operation expertise must be reconstructed. −Throughput with IPv6 may decrease significantly as compared with IPv4. −It may be impossible that the region for contents distribution is limited−based on the user's IP address.	a/b/d	−There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section). −Uncertainty about the state synchronization at backup redundancy (lacking in stability). −Enough performance may not be obtained for video.	a/b/d	−Uncertainty about the state synchronization at backup redundancy (lacking in stability). −Enough performance may not be obtained for video.

Field			When separate communications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available. (No communication between IPv4 and IPv6).		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (IPv4 to/from IPv6 translation) is provided.		When the intercommunications between IPv4 and IPv6 are realized in the environment where both IPv4 and IPv6 are available and translator service (ALG) is provided.	
			Category	Remarks	Category	Remarks	Category	Remarks
Service providers	Applications	VoIP	b/d	-Operation expertise must be reconstructed. -Call agents must be reconstructed. -Throughput with IPv6 may decrease significantly as compared with IPv4.	b/d	-Call agents must be reconstructed. -There may be much content that cannot be supported by a translator (In case the content has the address information in the payload section).	b/d	-Call agents must be reconstructed. -Depends on applications -The service side must provide a translator for each application
		NTP	a	-Example: ntpd, the SEIKO Precision time server	a	-Simultaneity in communication may not be ensured.	a	-Simultaneity in communication may not be ensured.

Reference 7-2: Problems accompanying the introduction of NAT into the network

Categ a Possible
b Although there are products, there is no operational capability, or the operational experience is insufficient
c Although there are products, operational tools are insufficient
d Although there is technology, there are no products
e There is no technology

Note: The existence of the above products are restricted as far as known to the members.
Regarding non general purpose product including self developed one, the term "products" above may be interpreted to "objects" and "There is no" may be interpreted to "Modification should be for".

Field			When the user accommodated under NAT communicates with another user who has a global IP address		When the user accommodated under NAT communicates with another user under NAT	
			Category	Remarks	Category	Remarks
Consumer users	Devices	PC	a	-Depends on applications	a/b	-Depends on applications
		Network connected home appliances	a/b	-Functions will be limited because controls are performed using DDNS, port forwarding or CPE -If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable.	a/b/c/d/e	-Functions will be more strictly limited than when the other side of communication has a global IP address, because controls are performed using DDNS and port forwarding or CPE - If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable.
		Devices, such as game machines, that are likely to use special ports	a/b	-Functions will be limited because controls are performed using DDNS, port forwarding or CPE -If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable.	a/b/c/d/e	-Functions will be more strictly limited than when the other side of communication has a global IP address, because controls are performed using DDNS and port forwarding or CPE -If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable.
		CPE	a/b	-It is necessary that wholesale providers can allocate private addresses to end users from ISPs	a/b/c/d/e	-Depends on protocol and architecture -It is necessary that wholesale providers can allocate private addresses to end users from ISPs
	APP	E-mail	a/b		a/b	-No particular problems will occur if the mail server has a global IP address. -In order to access to the server under NAT, a relay server with static NAT or a global IP address is required.

Field			When the user accommodated under NAT communicates with another user who has a global IP address		When the user accommodated under NAT communicates with another user under NAT	
			Category	Remarks	Category	Remarks
Consumer users	Applications	Web browsing	a/b	-If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable.	a/b	-If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable. -In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address.
		VoIP	a/b/c	-Depends on the products to be used and their combination -Depends on the compatibility between SIP and NAT (timer), the support of the SIPNAT function.	a/b/c	-Depends on the products to be used and their combination -Depends on compatibility between SIP and NAT (timer etc.), the support of the SIPNAT function. -Service stability may decrease.
		Streaming	a/b		a/b	-In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address. -Service stability and transfer performance may decrease.
		Dynamic DNS	a/d		a/d	
		P2P application	a/b		a/b	-Depends on applications
		NTP	a/b		a/b	-In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address.
		Personal firewall	a/b		a/b	
scale users Middle	Devices	PC	a		a/b	-Depends on applications
		Servers	a		a/b/c	-The server under NAT may cause problems in operation such as port forwarding, scale, and stability
		Routers/switches	a		a/b/c	-The product that offers the NAT function must be replaced because of its functions and scale
		Firewall	a		a/b/c	-Reexamination of operation may be required
		IDS/IPS	a		a/b/c	-Reexamination of operation may be required
		Antivirus gateways	a		a/b/c	-Reexamination of operation may be required
		Proxy servers	a		a/b/c	-The server under NAT may cause problems in operation such as port forwarding, scale, and stability

Field			When the user accommodated under NAT communicates with another user who has a global IP address		When the user accommodated under NAT communicates with another user under NAT	
			Category	Remarks	Category	Remarks
Middle scale users	Devices	VPN devices	a/d/e	– Initiation from a user is possible. –User have to be under static NAT, if the communication is initiated from the other side. –In case of IPsec, the NAT traversal function must be supported. –In case of IPsec, it is dependent on a device whether multiple devices under NAPT can be handled. –IPsec (AH) cannot be used.	b/c/d/e	–Initiation from a user is possible. –User have to be under static NAT, if the communication is initiated from the other side. – In case of IPsec, the NAT traversal function must be supported. –In case of IPsec, it is dependent on a device whether multiple devices under NAPT can be handled. –IPsec (AH) cannot be used.
		Office equipment	a/b	–It may be impossible to use some functions that do not assume the intermediation of NAT.	a/b/c	–It may be impossible to use some functions that do not assume the intermediation of NAT.
	Applications	E-mail (including content DNS)	a		a/b/c	–In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address. –The server under NAT may cause problems in operation such as port forwarding, scale, and stability
		Web browsing	a		a/e	–If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable. –In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address.
		VoIP	b/c/d	–Depends on the products to be used and their combination –Depends on the compatibility between SIP and NAT (timer), the support of the SIPNAT function.	b/c/d	–Depends on the products to be used and their combination –Depends on the compatibility between SIP and NAT (timer), the support of the SIPNAT function. –Service stability may decrease.
		DHCP	a		a/b	–DHCP relay etc. is required
		Authentication	d	–Depends on protocol and architecture	d	–Depends on protocol and architecture
		DB	a	–Depends on protocol and architecture	a	–Depends on protocol and architecture
		NTP	a		a/b/c	–In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address.

Field			When the user accommodated under NAT communicates with another user who has a global IP address		When the user accommodated under NAT communicates with another user under NAT	
			Category	Remarks	Category	Remarks
Large scale users	Devices	PC	a		a/b	-Depends on applications
		Servers	a		a/b/c	-The server under NAT may cause problems in operation such as port forwarding, scale, and stability
		Routers/switches	a		a/b/c	-The products that offer the NAT function may need to be replaced because of their functions and scale
		Firewall	a		a/b/c	-Reexamination of operation may be required
		IDS/IPS	a		a/b/c	-Reexamination of operation may be required
		Antivirus gateways	a		a/b/c	-Reexamination of operation may be required
		Proxy servers	a		a/b/c	-The server under NAT may cause problems in operation such as port forwarding, scale, and stability
		Bandwidth control equipment	a/b/c		a/b/c/e	-It is very doubtful whether the bandwidth control expected by the operator will be provided due to the influence of multi-stage NAT
		VPN devices	a/d/e	-Initiation from a user is possible. -User have to be under static NAT, if the communication is initiated from the other side. -In case of IPsec, the NAT traversal function must be supported. -In case of IPsec, it is dependent on a device whether multiple devices under NAPT can be handled. -IPsec (AH) cannot be used.	b/c/d/e	-Initiation from a user is possible. -User have to be under static NAT, if the communication is initiated from the other side. -In case of IPsec, the NAT traversal function must be supported. -In case of IPsec, it is dependent on a device whether multiple devices under NAPT can be handled. -IPsec (AH) cannot be used.
		Office equipment	a/b	-It may be impossible to use some functions that do not assume the intermediation of NAT.	a/b/c	-It may be impossible to use some functions that do not assume the intermediation of NAT.
		NTP	a		a/b/c	-In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address.
	Applications	E-mail (including content DNS)	a		a/b/c	-In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address. -The server under NAT may cause problems in operation such as port forwarding, scale, and stability
		Web browsing	a		a	-If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable. -In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address.

Field			When the user accommodated under NAT communicates with another user who has a global IP address		When the user accommodated under NAT communicates with another user under NAT	
			Category	Remarks	Category	Remarks
Large scale user	Applications	VoIP	b/c/d	-Depends on the products to be used and their combination -Depends on the compatibility between SIP and NAT (timer), the support of the SIPNAT function.	b/c/d	-Depends on the products to be used and their combination -Depends on the compatibility between SIP and NAT (timer), the support of the SIPNAT function. -Stability in servises may decrease.
		DHCP	a		a/b	-DHCP relay etc. is required
		Authentication	d	-Depends on protocol and architecture	d	-Depends on protocol and architecture
		DB	a	-Depends on protocol and architecture	a	-Depends on protocol and architecture
		Business applications	a	-Depends on protocol and architecture	a	-Depends on protocol and architecture
Network（Internet）	Devices	Routers/switches	a/b	-Scaling problems with NAT router may occur	a/b/c	-The server under NAT may cause problems in operation such as port forwarding, scale, and stability
		Accommodation	a	-The existing devices supporting IPv4 are available.	a/b	
		Servers	a	-It is assumed that the server will distribute global IPv4	a/b/c	-In order to access to the server under NAT, it is required to use the Static NAT or the relay servers with global IP address. -The server under NAT may cause problems in operation such as port forwarding, scale, and stability.
		Monitoring devices	a/b/c	-There is a possibility that the equipment accommodated under NAT cannot be monitored	b/c/e	-There is a possibility that the equipment accommodated under NAT cannot be monitored
		NAPT	d/e	-Although there are fundamental NAT technology and products, the enabling technology and products for large scale NAT suitable for carriers do not exist.	d/e	-Although there are fundamental NAT technology and products, the enabling technology and products for large scale NAT suitable for carriers do not exist.
	Applications	Cache DNS	a		a/b/c	-There is actual achievement in the system in a company -The server under NAT may cause problems in
		Maintenance/operation tools	a	-There is a possibility that the equipment accommodated under NAT cannot be monitored	a/b/c/e	-There is a possibility that the equipment accommodated under NAT cannot be monitored
		Authentication	a/d	-Depends on protocol and architecture	b/d	-Depends on protocol and architecture
		DHCP	a		a/b	
		Access analysis	a/d/e	-It is assumed that the log analysis in large scale NAT will be difficult	a/b/c/e	-There is a possibility that the equipment accommodated under NAT cannot be monitored -Because anonymity increases, analysis will be impossible in many cases.

Field			When the user accommodated under NAT communicates with another user who has a global IP address		When the user accommodated under NAT communicates with another user under NAT	
			Category	Remarks	Category	Remarks
Service providers	Devices	Routers/switches	a		a/b/c	-The products that are used as a NAT box may need to be replaced because of their functions and scale
		Servers	a/d/e	-Difficulty in dealing with DoS attacks	a/b/c	-When servers are installed under NAT, it is assumed that access from the outside will be difficult
		Load balancers	a		a/b	-It is necessary to place the load balancers just before servers.
		Firewall	a/e	-Because it is possible that many users access using the same address, some king of problems may occur.	a/b/c	-Reexamination of operation may be required -Because it is possible that many users access using the same address, some king of problems may occur.
		IDS/IPS	a/e	-Because it is possible that many users access using the same address, some king of problems may occur.	a/b/c/e	-Reexamination of operation may be required -Because it is possible that many users access using the same address, some king of problems may occur.
		Antivirus gateways	a		a/b/c	-Reexamination of operation may be required
	Applications	Contents DNS	a/d	-Scaling problems may occur -The method to support DDNS is not established.	a/b/c	-When servers are installed under NAT, it is assumed that access from the outside will be difficult
		E-mail (including content DNS)	a	-Scaling problems may occur	a/b/c	-When servers are installed under NAT, it is assumed that access from the outside will be difficult
		Authentication	a/d	-Depends on protocol and architecture -Scaling problems may occur	a/d	-Depends on protocol and architecture
		html/file	a	-If IP addresses are used in Layer 4 or above, the devices that belong to this category are unavailable. -Scaling problems may occur	a/b/c	-When servers are installed under NAT, it is assumed that access from the outside will be difficult
		DB	a	-Depends on protocol and architecture. -Scaling problems may occur.	a	-Depends on protocol and architecture
		Application servers	a	-Scaling problems may occur	a	-When servers are installed under NAT, it is assumed that access from the outside will be difficult
		Streaming	a	-Scaling problems may occur	a/d	-When servers are installed under NAT, it is assumed that access from the outside will be difficult
		VoIP	a/b/c/d	-Depends on the products to be used and their combination -Depends on the compatibility between SIP and NAT (timer), the support of the SIPNAT function. -Scaling problems may occur	a/b/c/d	-Depends on the products to be used and their combination -Depends on the compatibility between SIP and NAT (timer), the support of the SIPNAT function. -Scaling problems may occur -Stability in servises may decrease.
		NTP	a	-Scaling problems may occur	a/b/c	-When servers are installed under NAT, it is assumed that access from the outside will be difficult