2005 Version

IPv6 Deployment Guideline

Data Center, IX Edition

March 2005

IPv6 Promotion Council of Japan
DP-WG Data Center SWG

Table of Contents

Introduction

This document is created for use by service providers and vendors who are involved in Data Center and IX, and describes general items, guidelines and methods that should be investigated when deploying IPv6 in Network service at Data Center and IX.

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

1. Features of Segments

Features of Data Center Segment

In this section, the deployment state to IPv6 at Data Center and IX is described, present issues for vendors are analyzed, the deployment model is verified and issues at deployment are discussed.

Connection with ISP vendors has a close connection with the operation at Data Center and IX, but the connection status with ISP varies widely.

In the following pages, the present status of the Data Center and IX is analyzed.

Analysis of Present Status at Data Center

Definition of Data Center

The Data Center is the name of the business that offers a housing service to house content distribution server firms such as content distribution vendors and connectivity services with the Internet.

Targets for this guideline

The word “Data Center” is also used in the broad sense to indicate an existing data center that includes computer centers, etc., however, here Data Center is used to indicate an Internet Data Center (iDC) that offers connectivity to the Internet.

iDC provider

Business of iDC provider can be classified into 2 large categories;

- The case where a provider offers a service as part of Internet Service Provider (ISP) business,
- The case where an independent provider that doesn’t develop ISP business (carrier type provider, foreign affiliated provider) offers a service.

In the former case, network devices that are the backbone for an ISP are often installed, therefore in such cases it is sometimes called a Network Operation Center (NOC). Not only user facilities, but also a backbone server of Data Center provider is installed. For

instance, there are servers related to additional service for connectivity service, backbone server composed for hosting service (DNS, etc.) and monitoring related server (SNMP, etc.).

Major Service of Data Center

The following are the major services of the Data Center.

Housing Service

This service provides a rack for housing server or network equipment. Air conditioning control and power supply are also provided. Primary maintenance is also provided for devices to be housed in most cases (OFF/ON of power supply, checking the state of lamp, etc.). Biometrics technology (fingerprint or vein authentication, etc.) is used for entry and exit control. However, this service does not relate to deployment to IPv6, therefore, it is not covered in this guideline.

Connectivity Service

This service provides connectivity to the Internet for a rack contracted with housing service. This service is often provided with 100Mbps or 1Gbps, however, there is also a narrow band service using a band control device, etc. (service of less than 10Mbps, etc.).

Hosting Service

This service provides web and mail service from the server facility of the Data Center provider. Users do not need to operate or monitor the server themselves, and operation and monitoring are performed uniformly on the provider side. This is a sort of outsourcing type service.

This guideline handles deployment to IPv6 for connectivity service and hosting service.

IPv6 Supporting State of Data Center

IPv6 supporting state

Though there are differences in the form, 33 companies, which is approx. 30% of 101 iDC providers throughout the country provide IPv6 service. (source: Impress Internet Data Center comparison/investigation/deployment guide, 2004 autumn edition) Main services are IPv6 connection service and IPv6 hosting service, and tunneling service is provided in some cases. Some iDCs provide IPv6 connection service as a charge paying service.

State of IPv6 service of Data Center

It is not known how the backbone network in the Data Center migrates to dual stack. At present most of providers construct separate IPv6 networks and in most cases a double investment is made, therefore additional cost is required for operation. The cost for full route transit of IPv6 is also too expensive at present.

There is also the consideration that it is difficult to set the price (apparently the cost will be more than existing service). It is difficult to deploy to IPv6 if the IPv6 traffic for consumers does not flow, and if the timing to renew facilities is missed, there is a possibility that introduction will be delayed a few years.

Analysis of Present Status of IX

We can define that IX provides network connection environment for ISPs to connect to each other. Basic service forms are GbE connection and FE connection, and there is 10GbE connection as well.

At present, IPv6 connection service is provided for IX service users of existing IPv4 at experimental and commercial IXs inside the country.

In this guideline, Layer 2-IX is covered.

IX can be classified into 2 broad categories; Mutual connection demonstration experimental IX of academic NW and commercial NW (WIDE project), and IX specialized provider (JPIX, JPNAP, local IX provider, etc.)

Service of IX is provided with port connection of layer 2 switch in order to secure connectivity between ISP providers. The main stream is shifting from 100Mbps to 1Gbps, and now there is a service of 10Gbps available. A monitoring type server is installed to monitor a network and notify problems.

IPv6 Supporting State of IX

The following is the support status of IX for IPv6.

NSPIXP6 (WIDE project, http://www.wide.ad.jp/)

A provider that is a member of NSPIXP Society (DIX-IE, NSPIXP3) is able to connect to NSPIXP6 free of charge. DIX-IE already supports dual stack.

JPIX (Japan Internet Exchange, http://www.jpix.co.jp/)

If you are a provider using JPIX, you are able to use the service with free of charge.

JPNAP6 (Internet Multi feed, http://www.mfeed.co.jp/)

Anybody is able to use JPNAP6 (Tokyo) service free of charge during the trial service period as long as they receive allotment of sTLA. If the provider uses JPNAP Osaka service, only the dual stack service can be used free of charge during the trial period.

State of IPv6 Service of IX

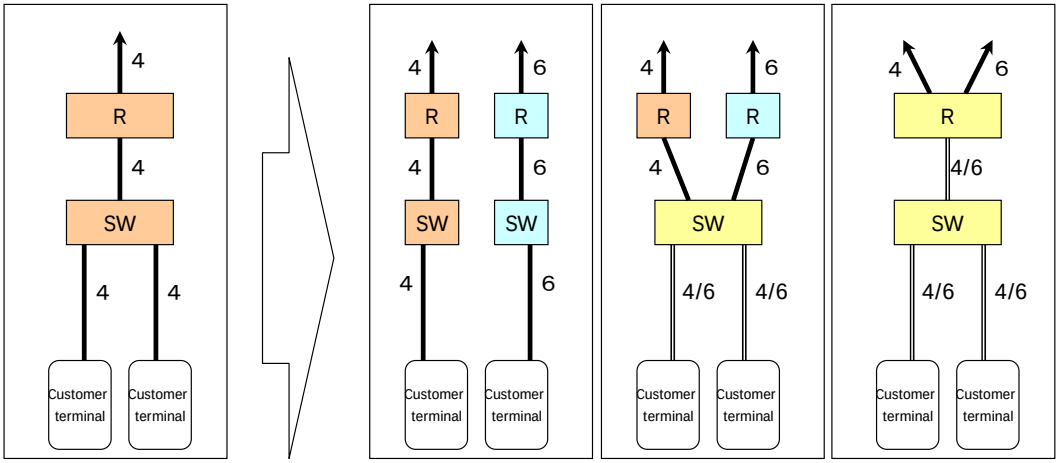
Most providers provide the service for the purpose of verification or experiment. Many of them support the service so that they are not left behind from a trend of industry. With regard to operation, monitoring and redundancy of equipment, service is provided with degraded quality. It is easy to change to dual stack, however, it is difficult for IX providers alone to carry out deployment to IPv6, so that those providers are required to carry out deployment through listening to ISP providers, etc. in order to make a close relationship with ISP providers.

It is also not easy to decide to move to IPv6, moreover, it can be pointed out that the price setting can only be carried out in units of port and it is affected considerably by the timing of renewal of ISP facilities.

2. Deployment Model and Introduction Scenario

Deployment Model for Data Center

Deployment model for Data Center Network can be illustrated as shown in the Fig. below.



Present state | Native method | Dual stack method (Edge driven type) | Dual stack method (Full replace type)

The following is an explanation of deployment model of Data Center from 3 view points; addressing, routing and provision method to users.

Addressing

Initial allocation size of address

sTLA has a big advantage in flexibility of path control compared with NLA. Moreover, it is not a very high hurdle to acquire and operate sTLA, so it is recommended to carry out the procedure towards acquiring sTLA.

There is a condition, which is that “you should have a plan to allocate /48 of 200 at least within 2 years” when you acquire sTLA, so it is recommended to devote sufficient consideration to the allocation condition.

Securing IPv6 address space

There is a method to acquire over /32 IPv6 address trees independently from APNIC, and a method to acquire a part of IPv6 address of upper ISP. We recommend using the method to acquire IPv6 address over /32 independently.

Because, when you acquire /32 independently, you will have more freedom to secure redundancy and control paths, and if you acquire IPv6 addresses from upper ISP, renumbering always occurs when you transfer to a different ISP from the upper ISP.

Please refer to the material of ISP SWG for concrete application method.

IPv6 address to be provided to a customer

Under the present address policy, the IPv6 address to be provided to a customer is connected in /64 when connecting to the edge switch directly, and it is connected in /64 and /48 is formed underneath when connecting to a router.

Addressing (200pcs., /48, 2-year problem)

When acquiring IPv6 address over /32 from APNIC, the conditions shown below apply. (http://www.nic.ad.jp/ja/translation/ipv6/20040714-01.html).

- You should be LIR.
- You should not be the end site.
- You should have a plan to provide connectivity with IPv6 Internet to the organization to which /48 is allocated. At this time, the path advertisement for the Internet should be integrated to one allocated address.
- You should have a plan to allocate 200 pcs. of /48 at least within 2 years.

Data Center providers seem to think the 4th condition is a problem, however, if you consider the case shown below, you will be able to solve the problem very easily.

- Allocate one of /48 to one user (one rack).
- Many sharing type hosting services use the method to save IPv4 addresses (name based virtual hosting), however, it is not necessary to save the address space forcibly in the case of IPv6.

Allocation of address to infrastructure and users

Following matters are shown in http://www.nic.ad.jp/ja/translation/ipv6/20040714-01.html.

Normally /48 is allocated, excluding extremely large scale applicants.

E.g.) /48 to one user (one rack)

/64 is allocated when it is known that the sole subnet is required according to specification.

E.g.) /64 to a server segment.

E.g.) /64 between router and router

/128 when it is clearly known that a sole device is to be connected.

E.g.) /128 to loop back of a router

The same description is made in ISP SWG, so please refer to that as well.

Routing

As a basic policy, it is better to choose a method that doesn't affect the existing IPv4 network. It is also better to select a method that uses tunnels as little as possible, and it is also recommended not to make devices route IPv4 if such devices have already routed IPv6.

For EGP, GBP4+ is used. However, under the current state, there is some concern about stability when a routing table of both IPv4 and IPv6 is held.

For, IGP, OSPFv3 is recommended. RIPng is acceptable at the initial stage, but when the number of routers to be handled increases, it is better to move to OSPFv3. ISP SWG has the same description, so please refer to that as well.

Provision Method to a User

In the provision scenario of IPv6 for a user, it is considered that IPv6 native method or IPv4/IPv6 dual stack method (edge-driven type) is used at first and then IPv4/IPv6 dual stack method (full replace type) is used. The following is an explanation of each method.

Network (provision method to a user)

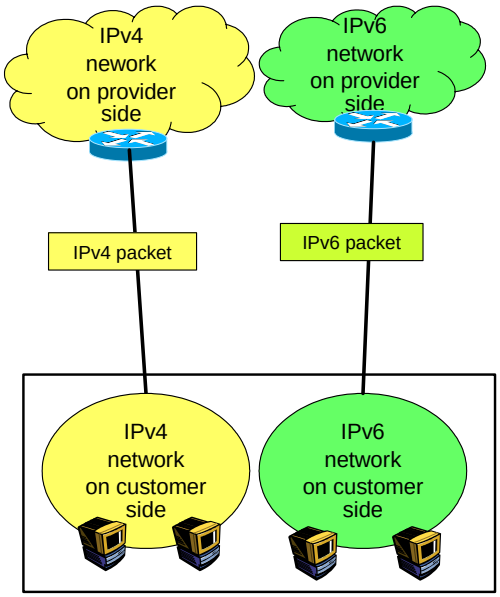
- Small start
- Goal is IPv6/IPv4 dual stack (Full replace type)

Time	Point	EGP	IGP	Network form, usage method, etc.
Start	Construction of external connection	BGP4+	static RIPng	Experiment, validation
n mohths time	Construction of small scale IPv6 network	BGP4+	RIPng OSPFv3	Provision to a customer with IPv6 native method
	Deployment to dual stack network	BGP4+	OSPFv3 RIPng	Edge part is made dual stack
n years time	Completed form in present situation	BGP4+	OSPFv3	Overall netwok is made dual stack

IPv6 Native Method

Connectivity for IPv6 is prepared separately and provided to a user.

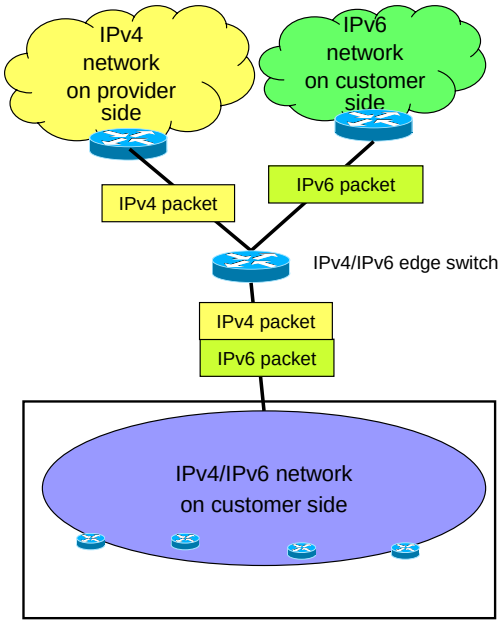
- Connectivity for IPv6 shall be prepared separately and provided to a user. (it shall be a single stack as a service viewing from iDC)
- Merits for provider
  - It is possible to construct without affecting existing IPv4 network.
  - It is possible to start from small scale IPv6 network, so the hurdle is low.
- Demerits for provider
  - Cost is incurred. Increase in cost along with growth of IPv6 network.
- Caution points
  - Attention is required because there is a possibility of making dual stack environment or L2 loop through connecting connectivity of existing IPv4 and connectivity of IPv6 on L2.



IPv6/IPv4 dual stack method (Edge-driven type)

Edge switch shall be enabled to route IPv6/lit and it is provided to a user as dual stack.

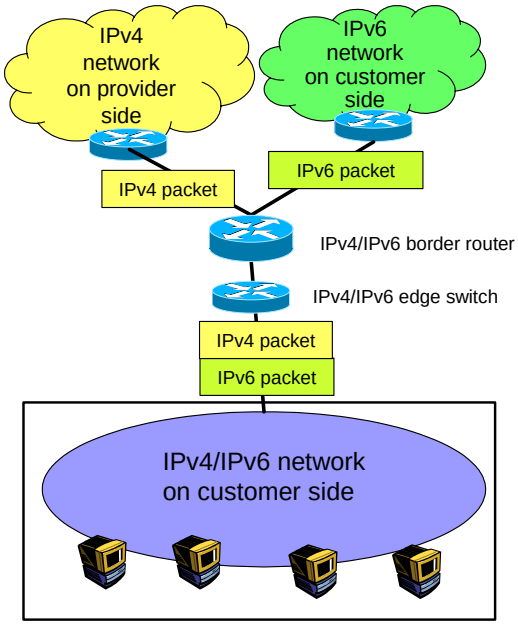
- Edge switch shall be capable of IPv6/IPv4 routing, and it is provided to a user as dual stack. Upper from edge switch shall be made into different network. Edge switch can be either of L2 or L3.
- Merit for provider
  - It is possible to provide dual stack to a customer at low cost without creating whole network again.
- Issues considered by provider
  - Design that doesn't affect IGP of existing IPv4 network
  - Design that prevents flow of IPv6 packet to IPv4 network side
  - Whether protocol used currently for redundancy operates properly in this case.



IPv6/IPv4 dual stack method (full replace type)

Whole network shall be made into IPv4/IPv6 dual stack.

- Overall network shall be changed to IPv4/IPv6 dual stack.
- Major type in IPv6 diffusion period ~ 5:5
- This method is recommended when constructing whole iDC network from the start.



Tunnel method

It is possible to consider tunneling between the routers of the Data Center and the customer, however, this method is not recommended.

- Tunnel method in premises
  - IPv6/IPv4 tunnel router shall be prepared in Data Center and tunnel is used with router on customer side.
  - This method is available, but quality is doubtful and it is difficult to separate when problem occurs, so this method is not recommended.

- Idea about tunnel
  - Network shall be designed without using a tunnel as a basic rule.
  - If a tunnel is used, it should be used after taking into account issues such as usage of closed tunnel on ones own network or quality.

Notes related to Auto-configuration

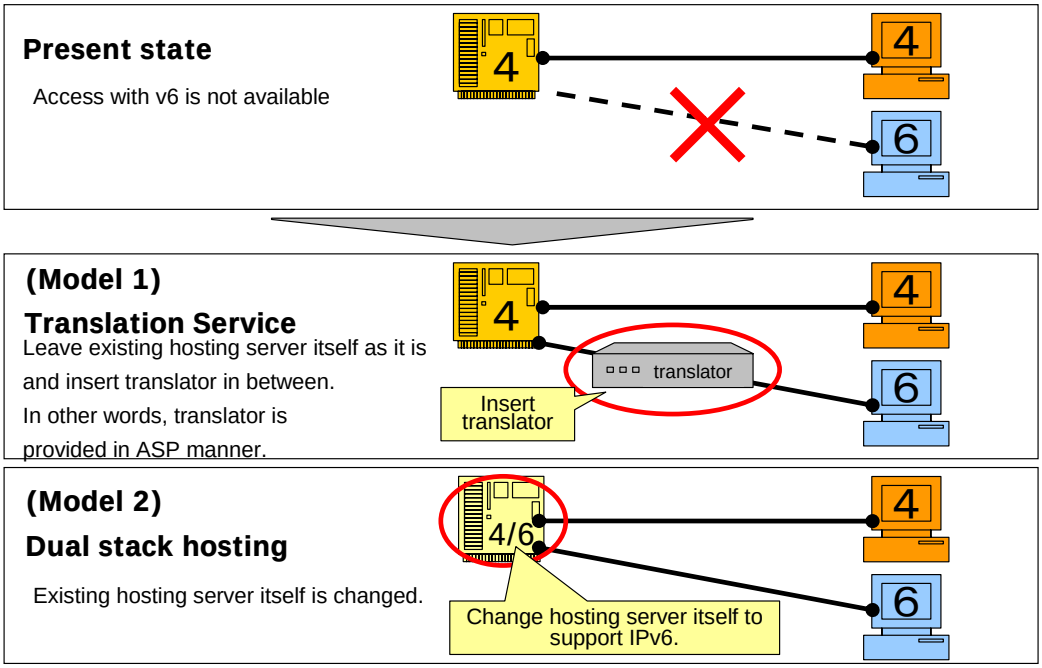
Auto-configuration technology such as Router Advertisement (RA, DHCPv6), etc., which is used for IPv6 should be set very carefully after considering the influence on the server firm and network. It is sometimes necessary to set in such a manner that these packets are destroyed.

You need to think whether the RA used in your own company is discharged outside or whether unpredictable IPv6 address is assigned by RA discharged from customer side.

Deployment Model of Hosting Service

Deployment of Hosting Service

When making a hosting service support IPv6, service should be a dual stack hosting service in the end, however, as a service during a deployment period, there is an IPv6 deployment model using translation service, in which inquiries of Ipv6 are translated by protocol and replay is made as proxy to IPv4 communication.



Hosting services can be classified into 4 broad categories.

High grade hosting

1-1: Dedicated hosting

1-2: Shared hosting

Modest price hosting

2-1: Shared hosting

2-2: Shared hosting using IA server

The following is an explanation of each hosting.

1-1: High grade dedicated hosting

It is called hosting, but actually it is almost the same as housing + customer server. Dedicated server is used, and installation, setting and operation are all handled individually. Deployment to dual stack hosting is used as deployment procedure.

1-2: High grade shared hosting

It is shared, but the contents are independent from each other in this service. It is independent at PF level such as VMWare, and is independent at OS level such as chroot-jail.

IP address is assigned individually. It is possible to install a unique application.

Operation is also handled individually to a certain extent in many cases.

The issues of this hosting for deployment to IPv6 are how to handle the state if the application installed independently by a user doesn't support IPv6 and whether it is possible to deploy only some users to IPv6 (case of chroot-jail in particular).

2-1: Modest price shared hosting

This is the service shared at the application (setting) level. Virtual_host of apache or sendmail.cw of sendmail are used. Services available for web site and mail are regulated.

In this case, IP address is also shared. CNAME is used for FQDN and HTTP HostHeader is used for application level. It is not allowed to install application independently, and usage of CGI is limited in some cases.

The issues of this type for deployment to IPv6 are that it is impossible to deploy only some users to IPv6 and that it is desired to assign IPv6 address to each user after deployment.

2-2: Modest price shared hosting using IA server

This is basically the same as 2-1. Hosting providers develop tools for control independently in many cases.

The issues related to this type of deployment to IPv6 are that it is impossible to deploy only some users to IPv6, that it is desired to assign IPv6 address to each user after deployment and how GUI tools developed independently can support IPv6.

Translation Service

In the translation service, an existing hosting server is used as it is and a IPv4/IPv6 protocol translator is sandwiched in-between. This is the service for provision of a protocol translator in the manner of an ASP. This service is used during the deployment period, and it is assumed that it will be replaced with dual stack method in the future.

Protocol translators are classified into 3 categories; NAT-PT type, TRT type and application proxy type. Here, name resolution is assumed to be performed separately, so that it is not the type using so called DNS proxy (totd, etc.).

Each protocol translator is explained in the following.

NAT-PT type

NAT-PT is short for Network Address Translator - Protocol Translator. This is an extension of NAT and carries out procedure up to protocol translation. Translation is

performed in 3 layers (IP layer), and overheads are low, but no window control or resending control is performed.

TRT type

TRT is short for Transport Relay Translator, and as the name suggests, it carries out translation on a transport layer (4 layers, TCP/UDP layer). Overheads are larger than NAT-PT, however, not as large as application proxy type. Window control and resending control are performed.

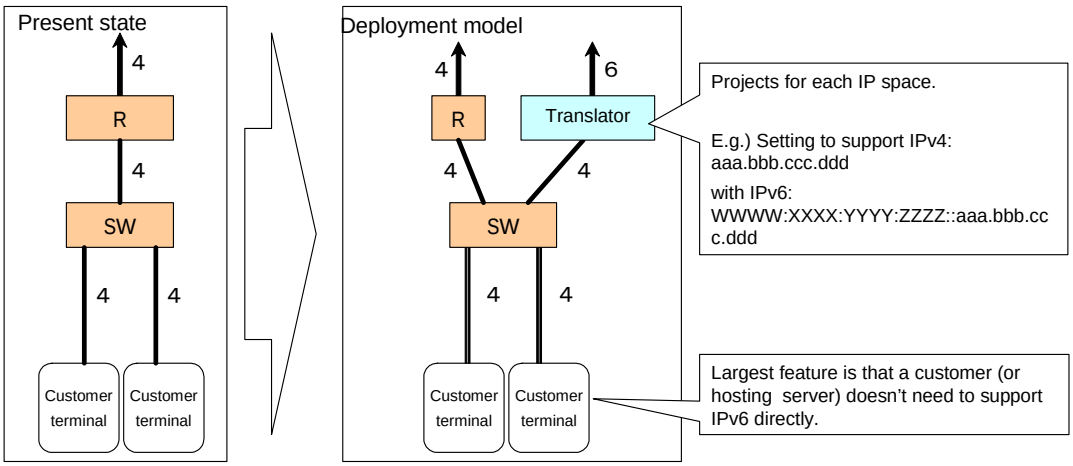
Application Proxy type

Translation is carried out at the application level. It is necessary to prepare this for each application (http/https, smtp, etc.). It's not necessarily the case that all required protocols are available, and overheads are large. However, this method has the highest translation performance and compatibility.

Translation service: introduction pattern (1)

In this pattern, a translator is set at a higher level.

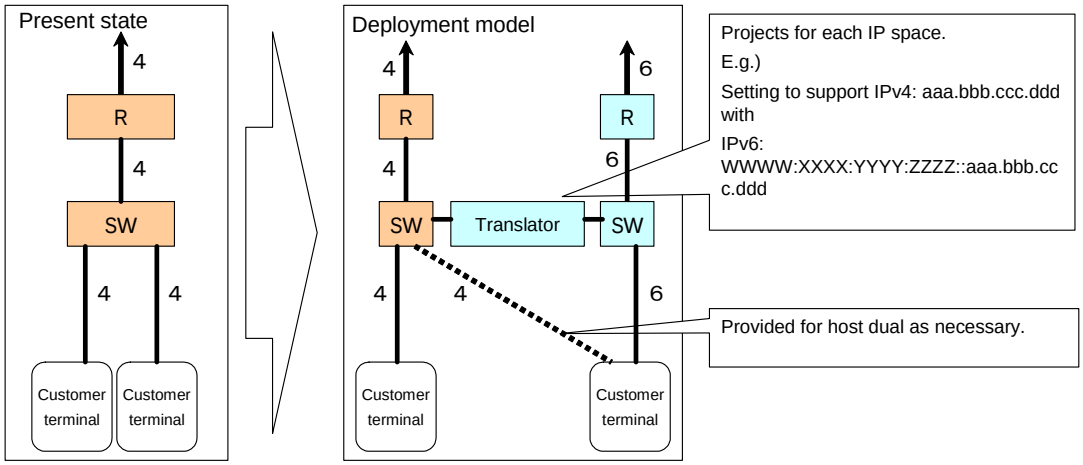
- Pattern that translator is set at upper level (STEP1)
  - Large amount of translation is made at upper in this pattern
  - Simple support at an extremely early stage (exactly the present BCP)



Translation service: introduction pattern (2)

This is the pattern that appears when the number of dual hosts starts to increase, and actually this is the first step.

- Pattern where translator is sandwiched in-between (STEP2)
  - This pattern appears when the number of dual hosts increases
  - STEP1 is actually the extreme logic, and this model will be the first step.

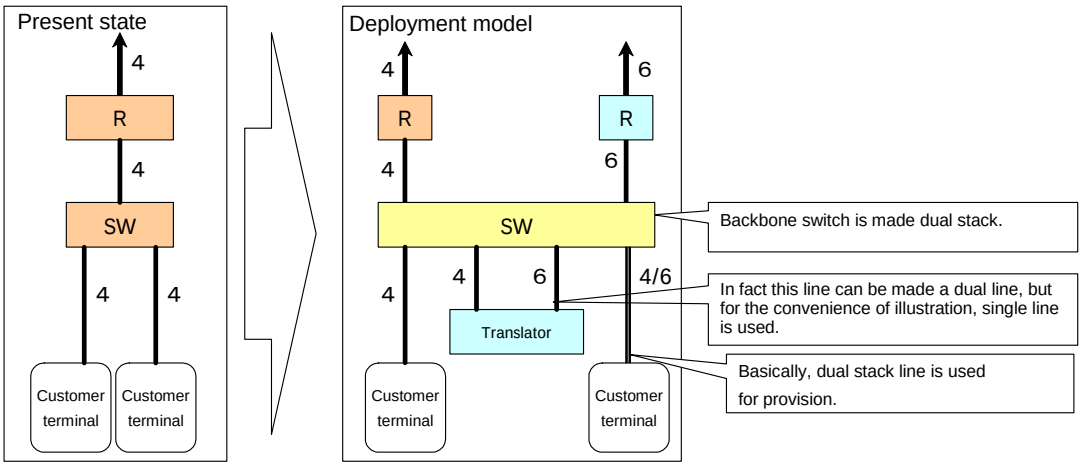


Translation service: introduction pattern (3)

This pattern appears when dual host is used at full scale.

■Translator is used in this pattern (STEP3)

□This pattern appears when the dual host is used full scale.



Dual stack hosting

Dual stack hosting means to make iDC hosting servers into a dual stack. Transfer is made from the necessary part, and the entire system is transferred to iDC in the end. This is done at renewal timing in most cases.

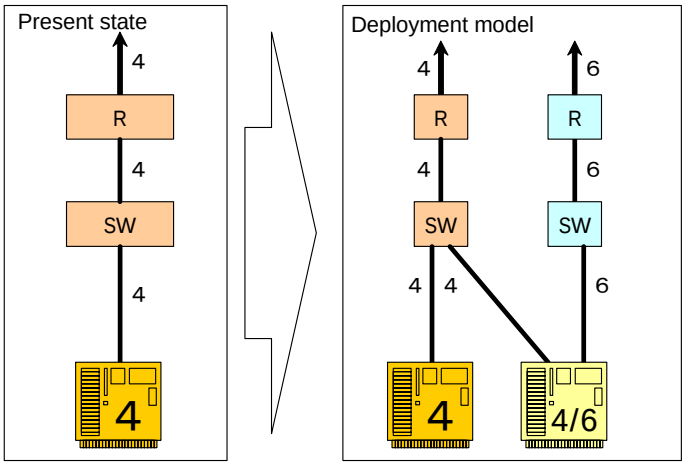
Dual stack hosting: introduction pattern (STEP 1)

This is the method called host dual stack hosting.

■Host dual stack hosting

□Simplest network configuration

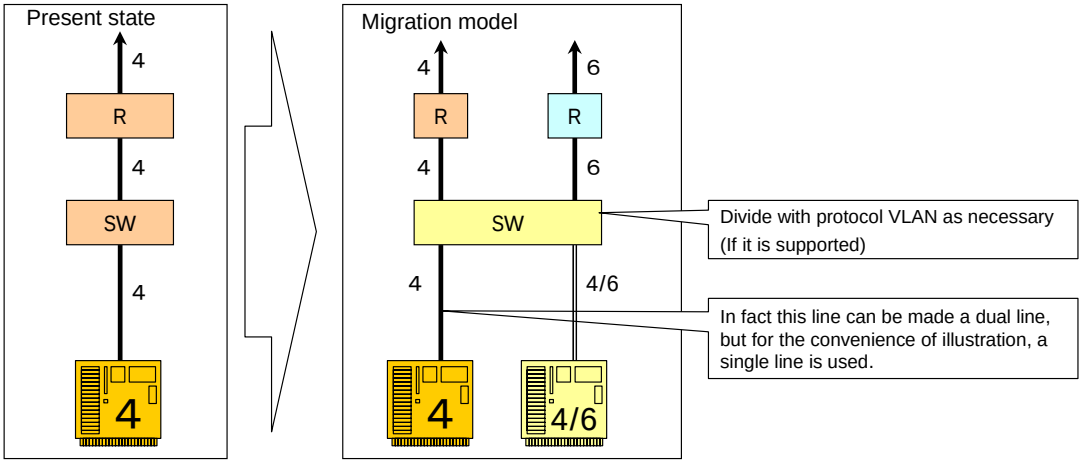
□However, a little high in cost



Dual stack hosting: introduction pattern (STEP2)

This is the method called cable dual stack hosting.

- Cable dual stack hosting
  - This is also good for the fist step.
  - Caution is required if there is extremely old equipment on a user terminal.



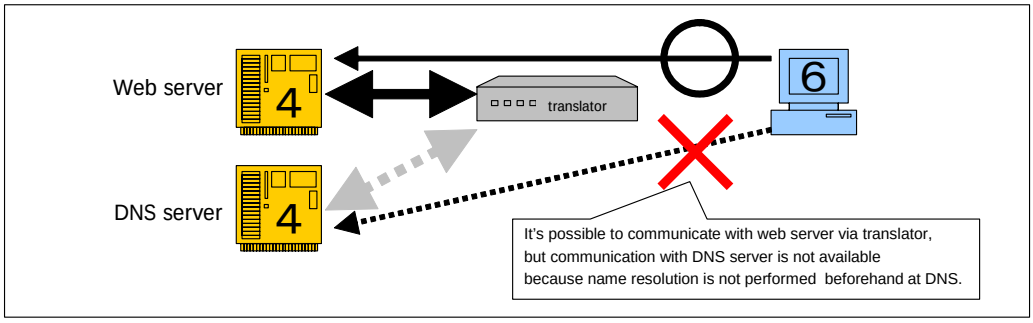
Issues

Common issues in deploying to IPv6

One issue common to translation service and dual stack hosting is that name resolution will not be available when deployment is carried out partially.

Common issues for deployment to IPv6

- Issue of DNS
  - In the case of deployment only part of existing system to IPv6, and if DNS is not included in the IPv6 deployment range, there is a possibility that IPv6 name resolution is not available.
  - This issue occurs easily when “simple deployment” is performed using Application Proxy type translator.



  - Countermeasure:
    (1) First of all, include DNS in IPv6 deployment targets.
    (2) Arrange a dual stack DNS service, which will be the base.

Another possible issue will be that when the implementation does not comply with the OSI model, if a translator is simply installed, a problem occurs. A direct example is the pattern where raw IP address (3 layer information) is written in 7 layer information.

Typical cases are that <A HREF=http://1.2.3.4/hogehoge.html> is written in HTML source, or that information indicating a sender is written in SNMP_TRAP using IP address.

It is not impossible to handle this problem using equipment that translates 7 layer, however, it is not a fundamental solution. It is necessary to write with FQDN thoroughly.

Issues of translation service

The translation service has the issues shown below.

・Whether all protocols can be translated.
・Whether the communication for which a path is encrypted can be translated as well.
・Dealing with host authentication
・L4-7 switch’s state of supporting v6
・Possibility to be used as a platform (concealment of access origin)
・Access log problem
・Whether the service is economically possible (revenue and expenditure balance)

The following is an explanation of the above mentioned issues.

Whether all protocols can be translated

There is no problem as a basic rule, as long as the device is NAT-PT type or TRT type translator. Basic protocols including http, smtp and ssh are supported. Streaming protocols such as mms and rtsp are also supported. Application proxy type translator is also furnished with necessary protocols. As a product example, reverse proxy of apache is available for web and nameproxy (Windows) is available for DNS.

When protocol is not regulated, it is possible to define and create individually. This will be a merit in that “deployment is possible selectively”, for application proxy type. In conclusion, it is OK to say that it is almost supported.

Whether the communication for which a path is encrypted can be translated as well

It is simply a matter of passing through from right to left as a basic rule, therefore there is no problem (payload is not taken into account). However, attention is required for cases such as HTTPS, where host authentication comes as a set. (refer to the following section.)

In conclusion, there is no problem even if it is just encryption.

Dealing with host authentication

There is no problem in communication with NAT-PT type and TRT type. However, if a raw IP address is used for authentication or a different FQDN is allocated, problems may occur (the name and content of certificate conflict each other). Application proxy type is not supported. It is necessary to install a certificate for a different server from the target server for deployment to the protocol translator.

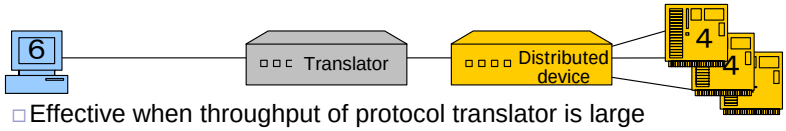
In conclusion, attention is necessary because a problem of different certificates occurs if the same FQDN is not used at deployment.

L4-7 switch’s state of supporting v6

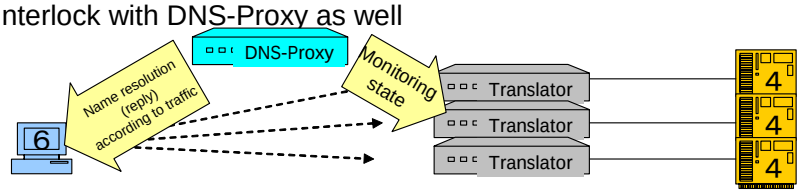
In general, there are only a few products in this genre that support IPv6 at present.

Issues of Translation Service

- V6 supporting state of L4-7SW
  - There are still only a few load balancers that support IPv6 (F5 BIG-IP, etc.)
  - There are several reverse proxy types.
    - (NetCache, Apache, Orenosp Secure Reverse Proxy, etc.)
  - Alternative method
    - Usage of protocol translator and load balancer together



  - Effective when throughput of protocol translator is large
    - Interlock with DNS-Proxy as well



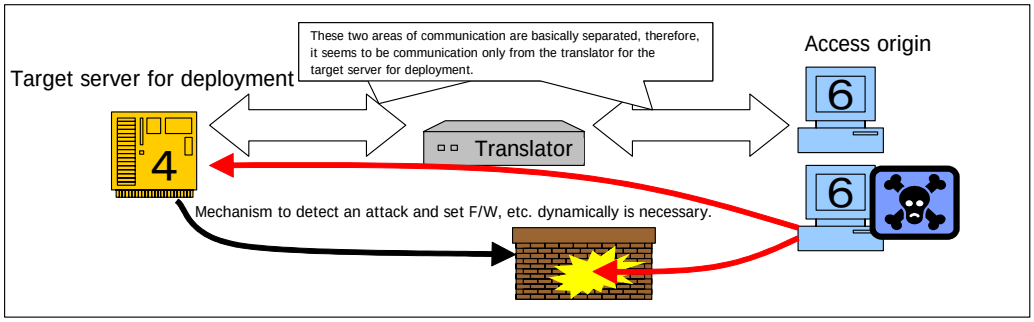
- Conclusion: Implementation by vendor is not realized yet, it is a future task.

Possibility to be used as a platform (concealment of access origin)

Translation has the problem that the true access origin is concealed by the translator.

Issues of translation service

- Possibility to be used as a platform (concealment of access origin)
  - In any form, target server for deployment can see only the address of translator
  - Actual access origin is concealed in the translator



- Conclusion: Concealment always occurs without exception.
- Countermeasures: (1) Acquisition/control of log using translator (next item)
  (2) Implementation of dynamic filtering

Access log problem

Because the access origin is concealed, it is impossible to analyze access only with the log on the target server for deployment. Therefore, it is crucial to acquire and control log on the translator (time synchronization is also required in this case).

Moreover, there is a slight problem in the format of acquirable log. Here, “combined_log of apache” is assumed as the necessary log (web access analysis used for marketing, etc. is assumed). In the case of application proxy, it is possible to acquire the same log as that of target application for deployment as a basic rule. In the case of NAT-PT type and TRT type, it becomes either “NAT result only” or “capture of all packets”, so it is necessary to check up with log on the target server for deployment or to analyze capture.

In conclusion, in the case of NAT-PT/TRT, there is a slight problem. In order to handle this problem, it is necessary to develop NAT-PT/TRT with which log in necessary format can be acquired.

Whether the service is economically possible (revenue and expenditure balance)

The translation service doesn’t seem very complicated technology for general users, however, for providers, it requires additional investment in necessary equipment. There is a method available to form using free software, however, it is not very secure from the view of commercial use. There is a possibility that the revenue you can expect is low despite the detailed work required.

Therefore in conclusion, you must investigate the business model in a cautious manner. You must consider the point of whether a customer will find value in IPv6 and whether additional value will be improved when it is installed in the base.

Issues of dual stack hosting service

The following are the issues of dual hosting service.

- The issue of the hosting service itself (not limited to IPv6)
- Possibility of only partial deployment
- Influence on firewall
- Whether the service is economically possible (revenue and expenditure balance)

The following is an explanation of these issues.

The issues of hosting service itself (not limited to IPv6)

The issues related to hosting service itself are whether it is possible to form hosting in the narrow sense (uniformed service) and if it is not possible, whether it is possible to operate. However, in this section, deployment of existing hosting service to IPv6 is explained on the basis that the above mentioned issues are already resolved.

Apart from “only partial user deployment” (next item), this problem will not occur by deployment to IPv6 as a new problem.

Possibility of only partial deployment

In the case that applications used by some users don’t support IPv6 in shared hosting, the issue of whether it is possible to choose not to deploy such users to IPv6. This may be possible under the specification assumed for high grade shared hosting. If not, it becomes necessary to reassemble sharing for supporting and non-supporting IPv6.

However, in the case of modest price shared hosting, “installation of unique application by some users” will not occur in the first place.

In conclusion, it is considered as possible to support.

Influence on firewall

You need to take great care with a firewall when it is shared. Because there is a possibility of decrease in throughput by adding IPv6 process, regardless of whether hosting is dedicated or shared.

However, it is not necessary to change firewall to dual stack forcibly. A deployment form of rising host dual type can be used. However, you must be aware of the initial cost.

Whether the service is economically possible (revenue and expenditure balance)

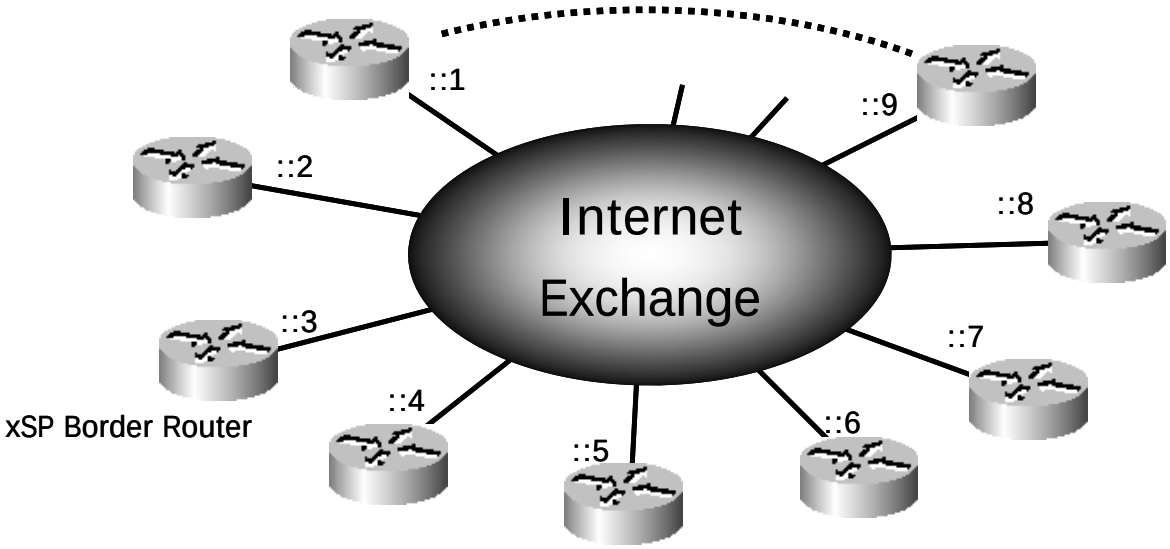
The current price of modest price hosting is ¥3,000 per month. It is considered that there are no users who want to have IPv6 in the present circumstances. Which means that it is very difficult to increase the price at present.

In the case of high grade hosting, the present price is ¥100,000 per month, and this will be the nearest target. However, it is doubtful whether it is possible to increase this price.

In conclusion, the service may be carried out as an additional value service for high grade hosting.

Deployment Model of IX

IPv6 address for IX



In the case of IX, a router for external connection is connected for each ISP on the same LAN segment. An address in the same subnet (A:B:C:D::/64 in Fig. mentioned above), which is allocated according to the policy of IX operator is assigned to connection interface of each router to IX.

Requirements of IPv6 address for IX

In the case of allocated addresses such as for an ISP, it is not necessary to assign an address block to an organization downstream. With regard to required size, (some of)/64 is sufficient for existing IX, so the size allocated to ISP (/32) is not suitable for allocation to IX.

However, due to the original nature of IX, IX address should be neutral and independent without depending on specified ISP, therefore it is preferable to assign directly from RIR.

If it is allocated by LIR of specified ISP, etc., neutrality will be impaired and address for IX is advertised globally as a part of the address space of the ISP. Which is a problem.

Assignment of IPv6 address for IX

At present, an IPv6 address of the address space (/48) of the appropriate size is assigned directly from RIR to IX. In Japan, assignment is made by APNIC, but JPNIC carries out the application work as an agency. The application method is indicated on the home page of

JPNIC.
http://www.nic.ad.jp/ja/translation/apnic/apnic-portable-assignment-request-form-j.html

RIR secures a certain amount of address spaces to be used for assignment to IX.

E.g.) APNIC 2001:07FA:: /32
RIPE 2001:07F8:: /32
ARIN 2001:0504:: /30

It is possible to filter using these figures based on the appropriate policy.

Advertisement of address for IX

With regard to the advertisement of address used for IX commonly in the case of IPv4 and IPv6, it is used only for the BGP session of adjacent routers on IX, therefore the necessity for advertisement is only slight.

From the view point of neutrality, it is not preferable to be advertised by a specified ISP. Moreover, if a specified ISP advertises from other than IX, there is a risk of routing trouble and a risk of attack/defense to a router on IX from out of IX segment (sending RST packet attacking vulnerability of TCP). For the above mentioned reasons, advertisement globally is generally suspended.

With regard to the advertisement of IPv6 addresses for IX, addresses are sometimes assigned for IX from each RIR under the condition that they are not advertised globally, so advertisement on a global Internet path table is “prohibited”.

Issues of IPv6 address for IX

There is an issue of link local address vs global unicast address for IX. As explained previously, the necessity to advertise addresses for IX globally is only minor, and because communication is normally made on the same link, the usage of link local addresses is investigated. In this case, the transfer of packets sent to a link local address by a router is prohibited; therefore problems caused by advertising the address for IX can be strictly avoided.

On the other hand, there is a problem that it is difficult for the management entity to control addresses for IX responsibly. Moreover, it can be pointed out that the old implementation doesn’t support BGP+ using link local address. In the case a connection is made by a multiple number of BGP+ using the same router, there is a possibility of overlap according to the design of address. Besides, reachability of a node neighboring IX is lost, so it is difficult to carry out life-or-death monitoring.

Due to these issues, it is left to the discretion of the management entity of IX in many cases, which should be used.

Deployment Model Pattern of IX

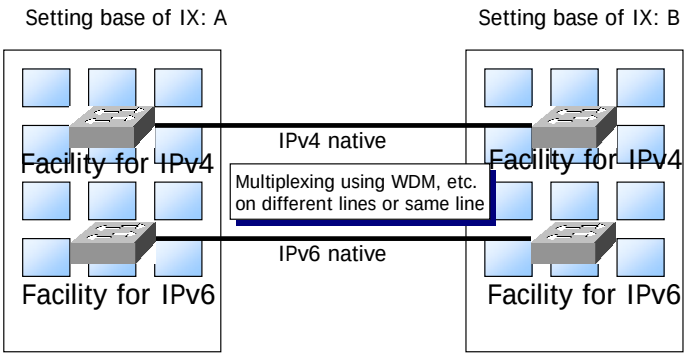
IX provider facility (switch)

As deployment models for IX providers, there are different line (dedicated to IPv6 service) type deployment, VLAN separation type deployment and dual type deployment.

Different line (dedicated to IPv6 service) type deployment

In this type, different equipment and lines are used for IPv4 and IPv6 separately.

IX provider: Different line (dedicated to IPv6 service) type deployment

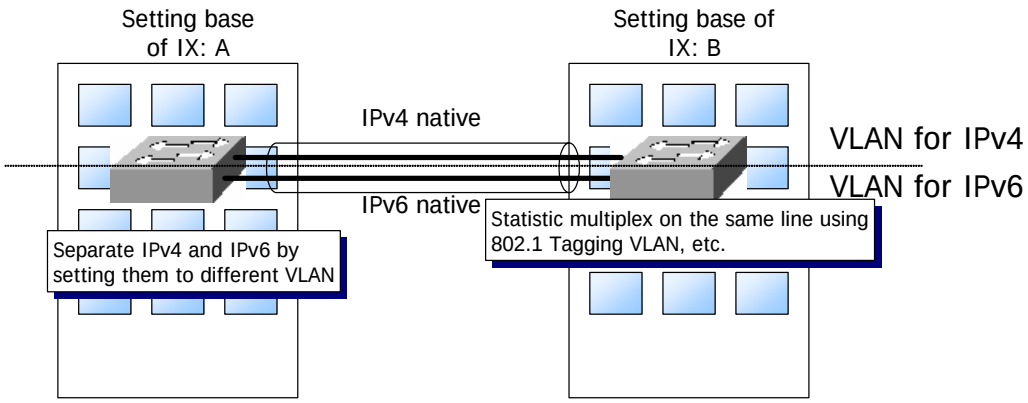


- In this form, different equipment and different lines are used for IPv4 and IPv6.
- Because it becomes necessary to prepare a cabinet (switch) and lines between bases separately from existing facility, additional facility cost is incurred by IX provider.
- IPv4 and IPv6 are not mixed, therefore there is no need to worry about influence of IPv6 traffic.
- Operation and cost are separated from existing IPv4, too.
- Dual stack is not possible, therefore, additional facility cost is incurred by xSP providers as well.

VLAN separation type deployment

IPv4 and IPv6 are connected using the same equipment and line, but 2 protocols are separated by VLAN.

IX provider: VLAN separation type deployment

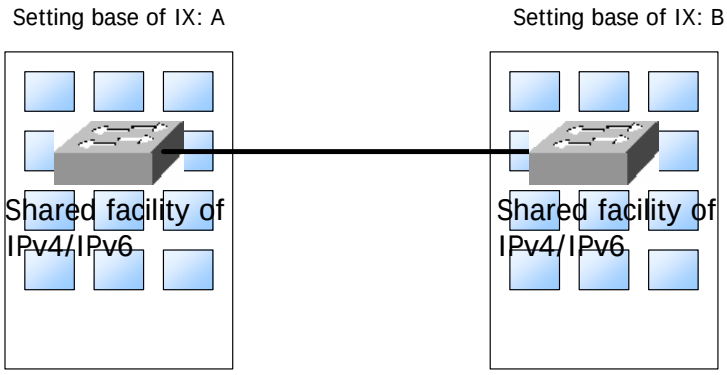


- In this form, Ipv4 and IPv6 are separated in VLAN using same equipment and line.
- Existing cabinet (switch) and line between bases are used, therefore no additional facility cost is incurred by IX provider.
- Additional task occurs for management of VLAN, etc.
- Because traffic of IPv4 and IPv6 is not mixed, there is no need to worry about influence of IPv6 traffic.
- Fee is separate from existing IPv4.
- Dual stack is not possible, therefore, additional facility cost is incurred by xSP providers as well.

Dual type deployment

In this case, IPv4 and IPv6 are not separated. Both are put through as dual stack.

IX provider: Dual type deployment



- IPv4 and IPv6 are provided without separation using the same equipment and same line.
- No additional facility cost is incurred by IX provider.
- Distinguishing operation and fees for each becomes difficult.
- There is a possibility of influence of IPv6 traffic on IPv4 traffic.
- Provision as dual stack is possible, therefore no load of additional port is incurred by xSP provider.

Deployment scenario of IX provider facilities

"Different line type" requires capital investment, however, it is possible to provide IPv4 and IPv6 services considering the operation and cost of each separately. Moreover, it is not necessary to worry about the influence of IPv6 traffic, therefore, this is suitable for initial provision such as experimental service.

However, if you want to avoid additional capital investment, you may consider introducing it in the form of "VLAN separation type".

When a substantial amount of traffic occurs in the period between diffusion period of IPv6 - 5:5, it is assumed that it will be provided using the "Dual type" form due to cost and various other reasons.

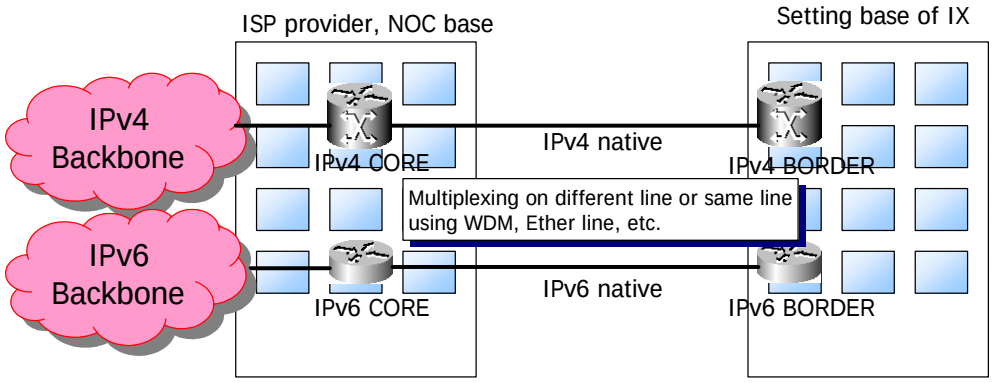
xSP providers

Deployment scenario of xSP providers for IX connection can be classified into 4 broad categories; different line (dedicated to IPv6 service) type, shared line (L2 separation) type, tunnel type and dual type.

Different line (dedicated to IPv6 service) type and shared line (L2 separation) type

In these types IPv6 and IPv4 are prepared as separate services.

xSP provider: Different line (dedicated to IPv6 service) type/shared line (L2 separation) type

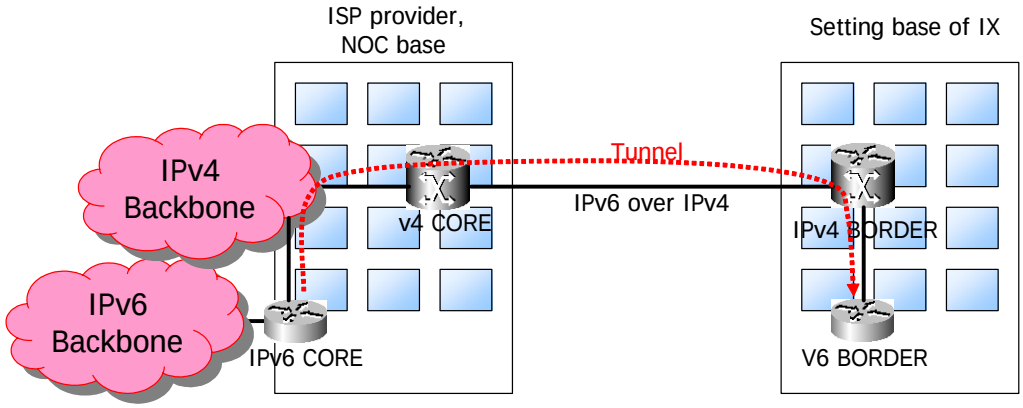


- In this form, IPv6 line is prepared separately from IPv4 line.
- It is possible to multiplex on the same line using L2 (VLAN) service or WDM device in order to reduce line cost.
- Even if the facility is set at the setting base of IX in order to connect to IX of IPv4, additional capital investment occurs.
- It is possible to avoid influence of IPv6 traffic on IPv4.
- This form is used in many cases at present.

Tunnel type

In this type, IPv6 is put through an IPv4 line using tunneling.

xSP provider: Tunnel type

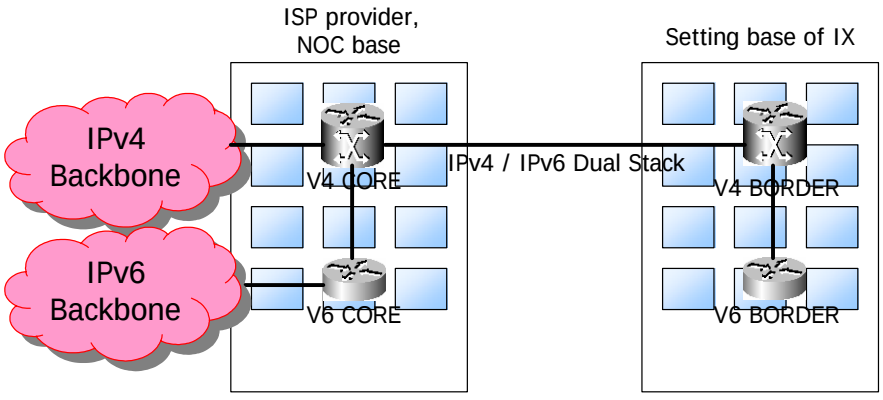


- In this form, IPv6 connection routers are connected using “IPv6 over IPv4” tunnel.
- It is possible to share access line.
- This is not recommended strongly because if the influence of trouble in IPv4 network is received, it becomes difficult to separate.

Dual type

This type is used to put through IPv4 and IPv6 in the form of dual stack.

xSP provider: Dual type



- In this form, IPv6 connection routers are connected using dual stack line.
- In the case of former type equipment, it is unknown how the state where IPv6 and IPv4 coexist affects, therefore, this is passed intentionally in some cases.
- It is assumed that this form will be used after diffusion period of IPv6 and period of 5:5.

Deployment scenario of xSP provider

When an xSP provider connects with IX for IPv6, they need to extend IPv6 network to the point of the facility set by IX provider.

However, the present IPv4 network is an important infrastructure, therefore it can not cease operation. So the network is constructed separately for IPv4 and IPv6 at the initial stage in order to avoid a risk. In order to reduce the cost for access lines, it is possible to use Ether line or wave length multiplexing. It is possible to use a tunnel, but this method is not recommended because separation will be complicated.

When a substantial amount of traffic occurs in the period between the diffusion period of IPv6 - 5:5, it is assumed that it will be provided in the form of “Dual type” as in the case of IX provider facilities.

When xSP providers renew the facilities, they are required to select facilities based on these deployment scenarios.

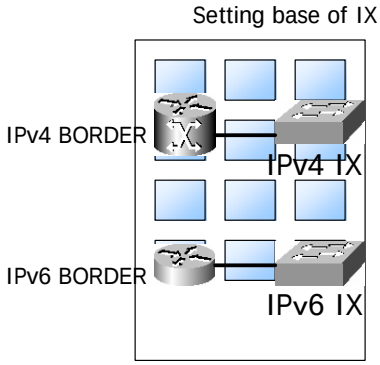
IX connection facilities of xSP provider

As in the scenario for deploying connection facilities of xSP at IX, different line type (different router), different line type (different interface) and dual type may be considered.

Different line type (different router)

In this type, different routers are prepared for IPv4 and IPv6.

IX connection facility of xSP provider: Different line type (different router)

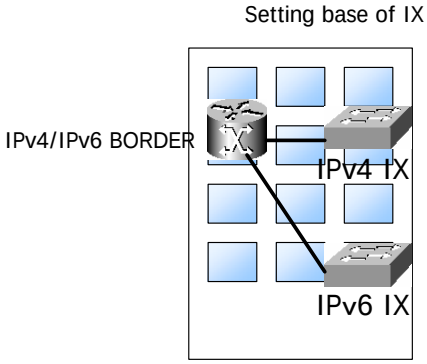


- In this form, xSP router is prepared separately for IPv4 and IPv6.
- Because IPv4 and IPv6 don’t coexist, there is no need to worry about the influence of IPv6 traffic.
- It is possible to operate separately from existing IPv4 network.
- It is necessry to prepare routers that support BGP double for IPv4 and IPv6.

Different line type (different interface)

In this case, there is just one router, but different interfaces are used.

IX connection facility of xSP provider: Different line type (different interface)

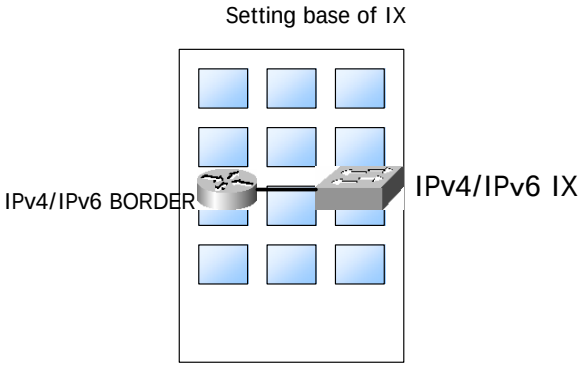


- In this form, one xSP router is used for both IPv4 and IPv6, however, different interfaces are used for connection.
- It becomes necessary to prepare interfaces individually, but it is possible to control traffic of IPv4 and IPv6 individually.

Dual type

In this case, the connection of IPv4 and IPv6 is made using one router and one interface.

IX connection facility of xSP provider: Dual type



- In this form, one xSP router is used for both IPv4 and IPv6 and one interface is used for connection.
- It is crucial that IX supports dual stack. At present, most IX provider facilities don't support dual stack, therefore, the number of connections in this form is very small.
- Facility cost depends on total amount of traffic of IPv4 and IPv6.
- It is difficult to control traffic by separating IPv4 and IPv6.

Scenario of xSP providers for deploying facilities for IX connection

The deployment scenario is almost the same as the one described in the previous section, and the connection of IPv4/IPv6 using different routers is mainly used so that risk is avoided at the initial stage. In the period between diffusion period of IPv6 - 5:5, it is assumed that the “IPv4/IPv6 dual stack” connection form will be used.

However, if IPv4 and IPv6 coexist in the same interface, management of traffic becomes difficult, therefore, the “same router/different interface” form may be used in some cases. It is also necessary to establish a method to acquire traffic for IPv4 and IPv6 separately.

3. Assumed Issues in the Diffusion Period

Deployment Issues (general statement)

There is a possibility that support for IPv6 is justified in the diffusion period, but some difficulties for deployment will remain.

The following are the reasons why deployment should be made.

- In order to discriminate from other companies, or in order not to be left behind other companies
- Appearance of xSP that provides service only to IPv6

On the other hand, the following are the reasons why you may not want to deploy.

- Increase in cost (additional equipment is required along with deployment of IPv6, purchase of additional full route for iDC, etc.)
- Address problem (It becomes difficult to change IPv6 addresses if there is upstream dependence, address numbering of server type is actually impossible in iDC or hosting service)
- Stability (In the case of iDC, Middle Box is included in configuration factors apart from router and switch, so it becomes difficult to ensure their mutual connectivity and operability)
- Operation (cost of operation of v4 and v6, distribution of human resources)

Assumed Issues for Data Center in Diffusion Period

Deployment timing of IPv6 for Data Center

Enthusiasm for efforts on IPv6 varies according to the type of iDC.

In the case of a government affiliated iDC or an iDC that works closely with local public organizations (third sector iDC), deployment of IPv6 will be requisite. It depends on the trend related to electronic government, but it is highly probable that deployment of IPv6 will be requisite.

In the case of a carrier type or ISP type iDC, or large scale iDC that has a backbone, it is relatively easy to deploy to IPv6. When deployment of backbone to IPv6 is promoted, it is

easy for the iDC itself to deploy to IPv6. This depends on the form, but provision of simple IPv6 connectivity to a customer can be easily achieved.

However, in the case of independent and relatively small or middle sized iDC with extended hosting, it is difficult to deploy IPv6.

If upstream of these iDCs has already deployed to IPv6, address comes from upstream, therefore it becomes difficult to cheat on. Deployment of IPv6 will be put into practice when it becomes inevitable to do so due to rational request to deploy IPv6 from a customer, etc., or when it becomes possible to manage the cost or deploying IPv6.

Which means that, in the case of iDC, deployment depends on a request by a customer and surrounding circumstances. It is considered that customers of iDC don't need to deploy themselves to IPv6 if the end user access system is not deployed to IPv6. But if a service that is provided only to IPv6 appears, there will be another scenario.

Deployment Issues for Data Center (general statement)

In conclusion, it is still difficult for iDCs and their end users to justify deployment of IPv6. It requires additional cost, so you can not deploy to IPv6 actively unless there are enough merits to meet additional cost. There will be technical merits, but for iDC, the merits are rather small. The following are the deployment issues.

- Current allocation rules for IPv6 address
- Increase in the amount of equipment for which mutual connectivity must be checked (classification of the cases to check mutual connectivity will increase to more than double)
- Deployment of various tools provided to customers for IPv6 (tools to provide information including traffic information and contact address information, tool for updating information on customer side including customer information, contact address information, DNS and mail)

Assumption of diffusion period

In the diffusion period, how will the situation for iDC change?

iDC with IPv4 only	A reasonable number of relatively small sized iDCs exist
iDC with IPv4 and IPv6 as dual stack	Most of iDCs will be this form
iDC with IPv6 only	It is assumed there will be almost none of them

The following are the assumed form of iDC's customers.

Customer with IPv4 only	Longtime service provider
Customer with IPv4 and IPv6 as dual stack	Majority of xSP
Customer with IPv6 only	It is possible to assume that there will be xSP for new business development

Process to IPv6 Ready Data Center

It is relatively easy to deploy a backbone to IPv6. It is also relatively easy to deploy customer edge to IPv6, though it depends on the form of realization (provision of native, provision by tunnel).

On the other hand, deployment of IPv6 on the customer side depends on the implementation of customer (equipment of edge on customer side, Middle Box in particular).

Problem is for edge routers, firewalls and load balancer to support IPv6.

Assumed issues related to diffusion period

Increase in the amount of IPv6 traffic

The following are the problems for dual stack router in particular.

・Handling ever increasing routing tables
・IPv6 routing is processed by software in the case of certain equipment.
・Whether it is possible to carry out routing of IPv4 stably in the case of burst traffic of IPv6.

It is not clarified yet which redundant protocol can operate stably with IPv6 among OSPFv3, VRRP IPv6, ESRP and HSRP.

Traffic pattern may possibly change from the present pattern in which most of the traffic is from Data Center to users (E.g.: traffic pattern will be different between IPv4 and IPv6, or traffic pattern will change due to appearance of new application).

SLA issue

In the case that SLA is defined for a customer, it becomes a problem whether it is possible to provide SLA without making a change even if backbone, etc. on Data Center side deploys to dual stack network. It is also necessary to think about usage of appropriate redundancy and about whether different SLA is necessary for both IPv6 and IPv4.

Fusion of broadcast and communication, Internet usage by non-PC equipment

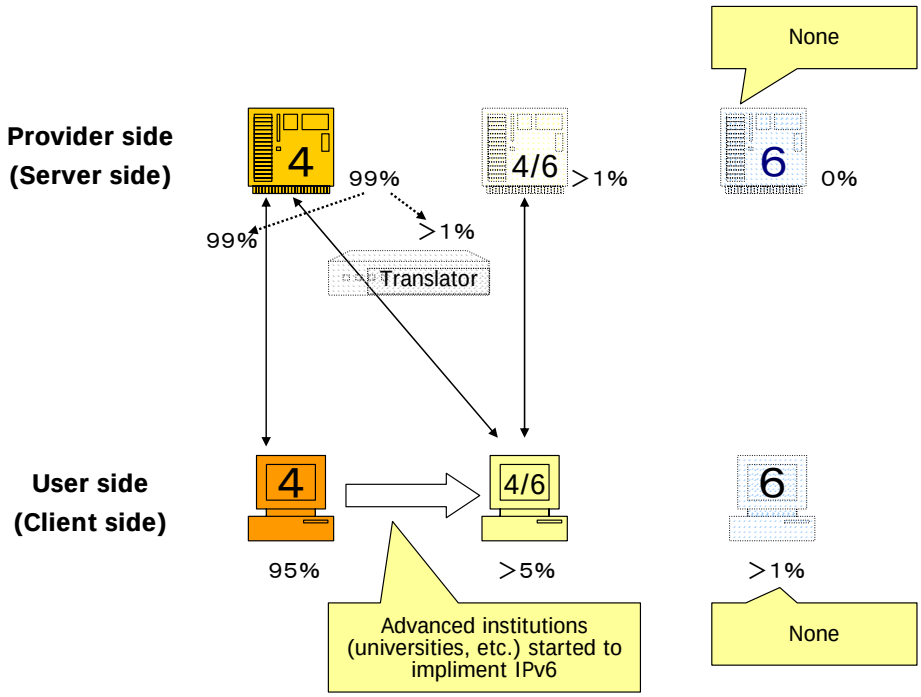
When the number of providers who set a server in Data Center increases along with the increase in the number of devices linked with broadcast and the number of information household equipment due to fusion of communication and broadcast, it is assumed that the role of the Data Center will expand further.

Assumed scenario for hosting service

The following are the assumed contents of the hosting service at present and in the diffusion period.

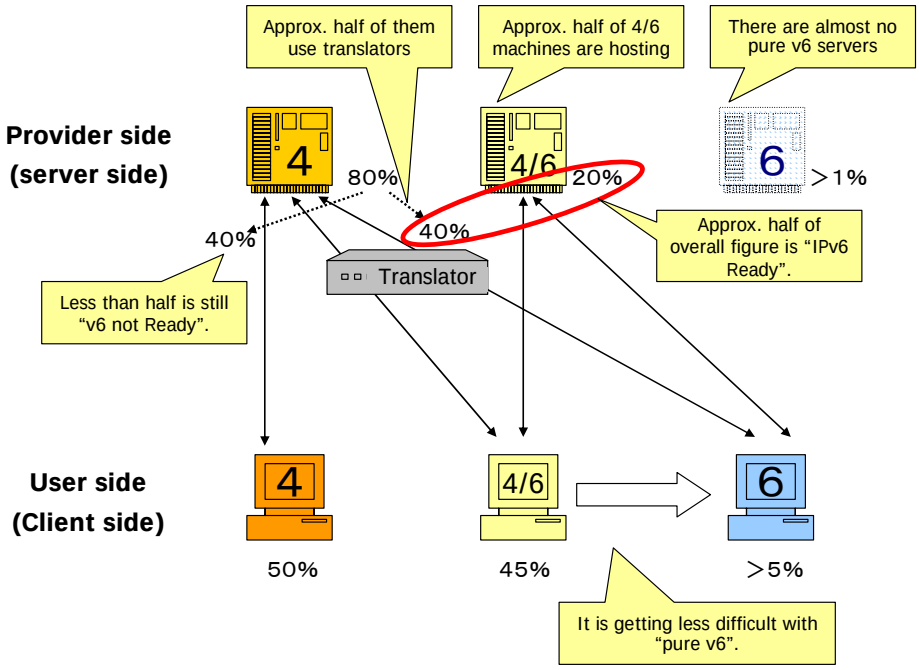
Present model

Provider side	Almost all servers are IPv4 only
User side	Almost all users are IPv4 only
	Some advanced users are in IPv4/IPv6 dual environment



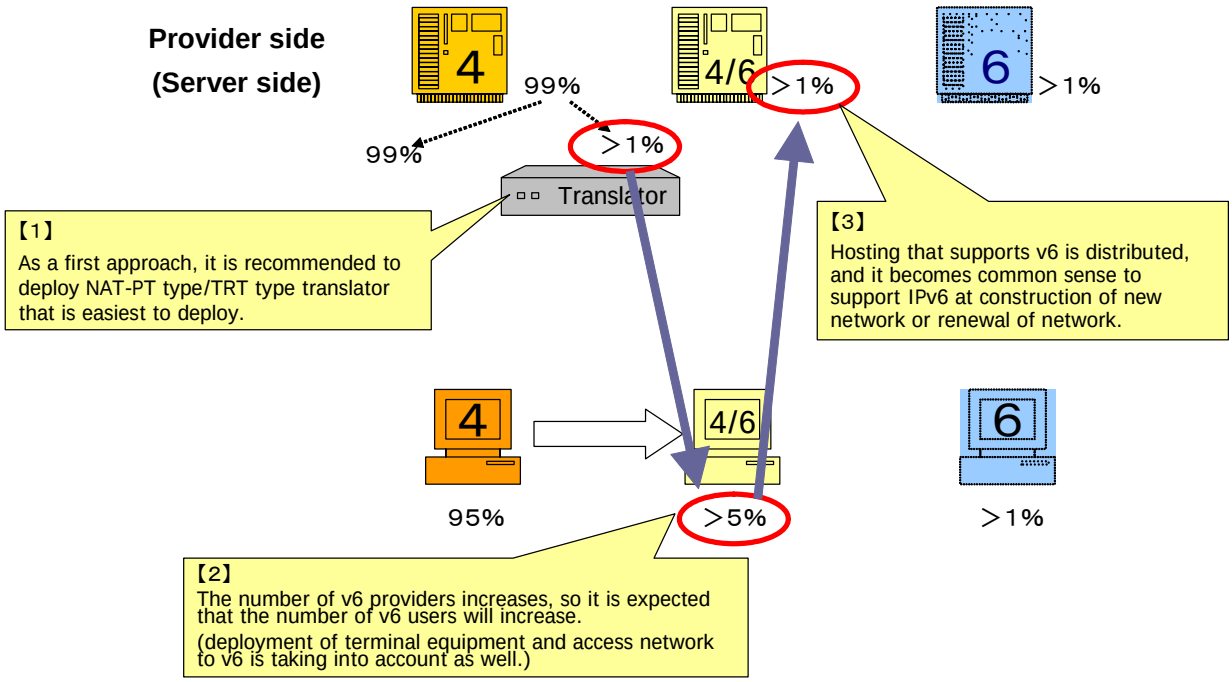
Assumed model in diffusion period

Provider side	v6 Ready rate is 50% “Simple deployment” rate by translator is relatively high. When a new site is created, v6 is supported in most cases.
User side	Number of cases of dual usage of v4/v6 is increasing. v6 Ready rate is approx. 50%. At the stage of considering deployment to pure v6.



Deployment scenario

In the deployment scenario, deployment to IPv6 affects server and user as shown below.



Technical issues for deployment of hosting service

The following are the technical issues for hosting service deployment in the diffusion period.

Common issues

Supporting a system that is not based on the OSI reference model becomes a problem. It is possible to avoid the problem with “contents filter” if it is at the level of HTML file, but if the product is created uniquely, the problem may possibly be more complicated.

With regard to the problem of DNS, you just deploy DNS as the first thing, so there is no problem. DNS lease service is provided by any ISP, because there are almost no cases of supporting IPv6 only.

In the case of translation service

There is a trade off of host authentication issues and log control issues. However, this problem can be resolved when NAT-PT type translator with which control of log is easy is

released.

Anxiety towards a platform attack can be solved by implementation of a dynamic filter. This is the same system as the F/W linked iDS.

In the case of a dual stack hosting service

There are no technical problems for this particular subject.

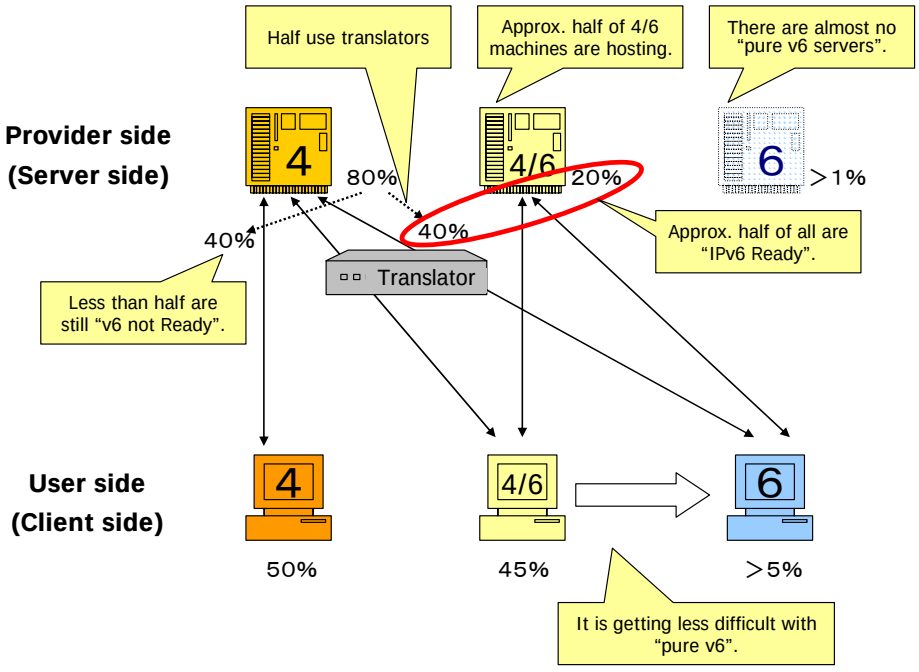
Next step in the diffusion period

Most of the cases assumed in the scenario for diffusion period described above for simple deployment. In order to move on to the next stage, the problems shown below remain.

・Method of moving from simple deployment (translation service) to full scale deployment (dual stack hosting service)
・Method of deploying (simply) a server that has not deployed
・The road to pure v6 (how to abandon v4)

Assumed scenario

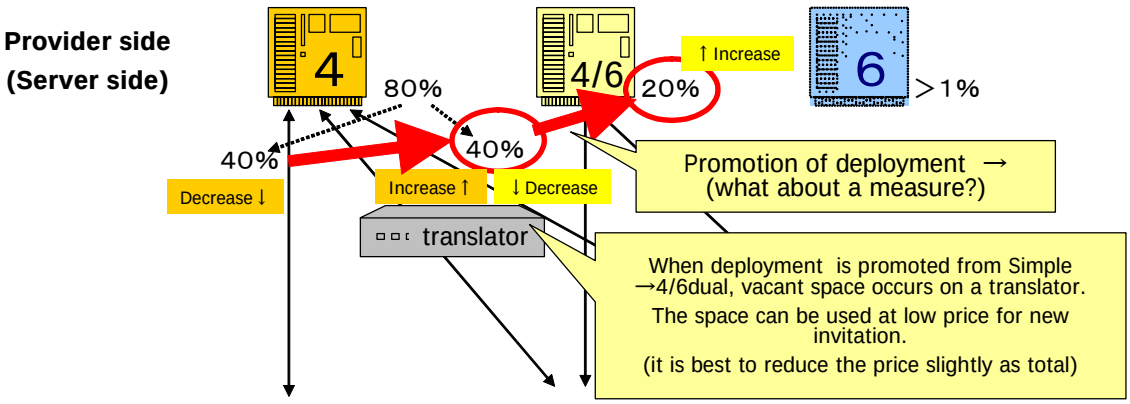
The following situation can be assumed as the next step in the diffusion period.



In order to solve the issues (1)

It is possible to consider that ISP or iDC bundles translator service as a method to deploy a server that has not deployed in the diffusion period, however, there is still a problem of how to justify the cost.

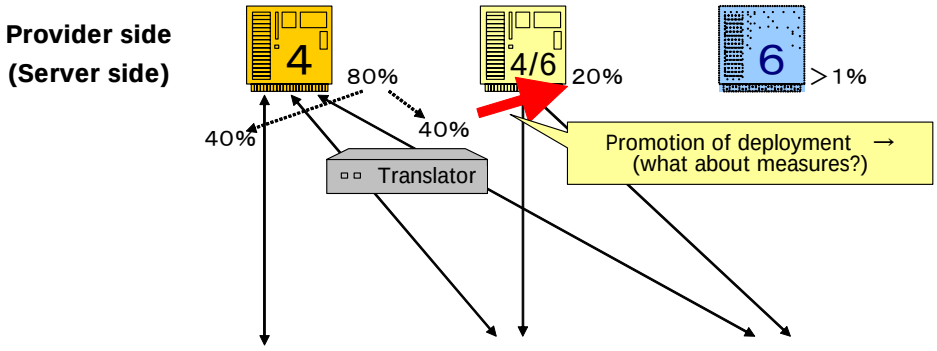
- How to deploy a server that has not deployed yet
  - ISP-iDC bundles translator service
    - a part of translator that becomes less crowded after a peak of usage shall be provided free of charge or at extremely low price.
    - It is possible to provide at low price if the cost is collected at the initial investment, but what about resource?



In order to solve the issues (2)

For the timing to shift to simple deployment to full scale deployment, renewal of the system becomes the key.

- How to shift simple deployment to full scale deployment
  - Renewal of the system is the key for timing.
    - It is a common sense to have new server as dual stack (assumption)
  - Reduction of dual stack hosting fee based on accumulation of know-how and competition principle.

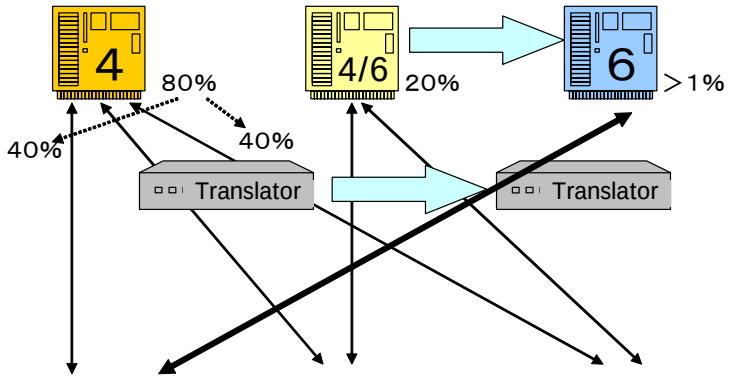


In order to solve the issues (3)

In order to abandon IPv4 in the end and promote changing servers to pure v6, it is possible to consider the method of using a translator in reversal direction as an option.

- How to abandon v4
  - Use a translator in reversal direction and promote deployment of server to “pure v6”.
    - It is more favorable if it is possible to use a translator, which becomes vacant along with promotion of deployment.
    - It is v6 > v4, so projection address is not usable (it is necessary to set each time manually such as static NAT), but the number will be small at this time.

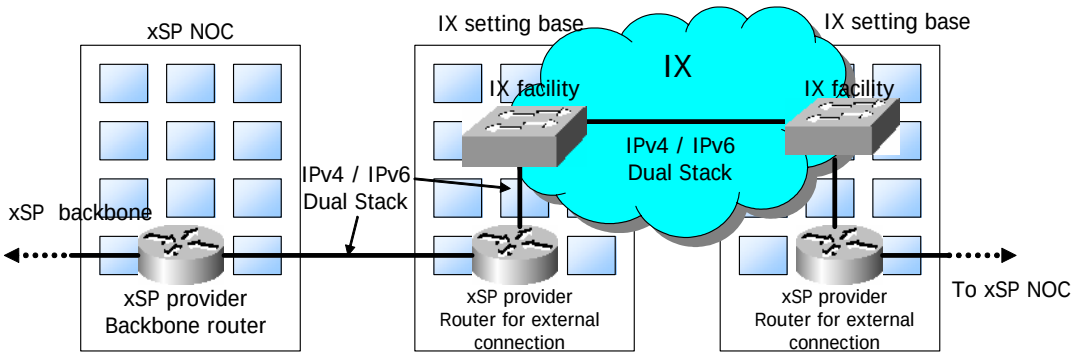
Provider side
(Server side)



Assumed Issues of IX in Diffusion Period

Configuration of IX in diffusion period

In the diffusion period, both IX providers and xSP providers use facilities and line as dual stack.



- In diffusion period, IX providers provide a service as dual stack of both facilities and lines without discriminating/separating IPv4 and IPv6.
- xSP providers who are the users of IX shall prepare facilities and lines as dual stack likewise.

Assumed issues of IX towards diffusion period

Distribution of IPv6 load at link aggregation

For IX in diffusion period, distribution of IPv6 load at link aggregation becomes an issue.

In the case that link aggregation (LAG) is used to configure between IX switches, there are devices that perform distribution of traffic according to MAC address for IPv6 communication.

This is not a problem now because there is little IPv6 traffic, but when the amount of traffic increases in the future, the traffic of connection between IX switches may be concentrated on one line and overflow of traffic may occur.

Handling of users who need only a single protocol

There is another problem as to how you can handle the protocol filter if you are told that IPv6 (v4) is not necessary. It is possible that an IX user will say that IPv6 (or IPv4) is not necessary due to reasons of their own convenience, even if it is dual stack IX. Some of the

present IX switches are not able to perform protocol filtering, therefore there will be cases where the request of such users are not complied with.

Performance issue of switch

There are devices that don't show sufficient performance in processing of IPv6 compared with IPv4. In order to solve this issue, it is necessary to request that the vendor improve it.

Issue of the possibility of communication even with an address other than those assigned by IX

BGP peer can be established with other link local addresses than those assigned by IX to a user. This is a problem, which is difficult to monitor on IX side.

Deployment of 6bone address (pTLA/pNLA)

It has been decided to discontinue using experimental address (3ffe::/16) allocated by 6bone or 6bone-jp from June 6, 2006, so if a path exchanged on IX includes these addresses, renumbering of address becomes necessary.

Reference literature

RFC3701 6bone (IPv6 Testing Address Allocation) Phaseout
（http://www.ietf.org/rfc/rfc3701.txt ）

⇒It is recommended to renumber by manual setting as deployment method. Please refer to Tips in ISP-SWG material for the deployment procedure.

Assumed issues on user side

Improvement of performance of router

There are devices that don't show sufficient performance in processing of IPv6 compared with IPv4. In order to solve this issue, it is necessary to request that a vendor improve it.

Appearance of IPv6 only users

If IPv4 address is not assigned, router ID may cause batting. Therefore, it is necessary to assign and operate IPv4 addresses comprehensively.

Members of DP-WG Data Center Segment

(titles omitted)

Chair

Okimoto (NTT West)

Members (titles omitted, in the order of the Japanese syllabary)

Arano (Intec NetCore, Inc.)
Ishii (Internet Multi Feed)
Ishida (MEX)
Ishihara (KDDI)
Ue (NTT Smart Connect)
Katayama (NTT West)
Tanizaki (NTT Smart Connect)
Nishino (JPIX)
Hirao (JPIX)
Furukawa (NTT West)

Inquiries

Please contact the address shown below by mail for inquiries regarding this guideline.

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