2005 Version

IPv6 Deployment Guideline

Large Enterprise/Local Government Edition

March 2005

IPv6 Promotion Council of Japan
DP-WG Large Enterprise/Local Government SWG

About this document

This document is created for use by network administrators and Slers who construct and manage the networks of large enterprises and local governments, and describes general items, guidelines and methods that should be investigated when large enterprises and local governments introduce IPv6 in the future.

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

Table of Contents

1. Features of Segments 4

Features of Large Enterprise/Local Government Networks 4

Classification Factors of Large Enterprise/Local Government Networks, Relationship with IPv6 4

2. BCP (things that can be done immediately) 5

2.1 Advanced Deployment of IPv6 Network Environment 8

2.2 Deployment of IPv6 along with Deployment of New Application 22

3. The Target NW & System Form + Application in the IPv6 Distribution Period 31

4. Issues for IPv6 Distribution Period 37

Investigation Members 40

Revision of this Guideline 40

1. Features of Segments

Features of Large Enterprise/Local Government Networks

The following are the features of the networks of large enterprises and local governments, which are the target for deliberation in this document.

- The overall network is controlled by a specified full-time division.
- Relatively large scale network with more than several tens of users
- An Intranet is used inside the organization.
- Mail and web application services are provided inside and outside of the organization.
- Cost: Cost efficiency in particular is a strong consideration.
- Security: Network division maintains and controls the security policy in a strict manner.
- Stability: If a defect occurs on a network facility, a large influence is exerted on society and the organization (redundant configuration, regular update of facilities).

Classification Factors of Large Enterprise/Local Government Networks, Relationship with IPv6

(1) Number of connection points with the Internet
- 1 location **→Multihome routing**
- Multiple locations

(2)Type of Internet connection lines
- Dedicated line **→ISP service menu**
- xDSL, CATV, FTTH

(3) Number of users (access amount to shared server) **→Load distribution device**
- 100 persons and under
- 100 persons and over

(4) No. of bases **→Connection method between bases**
- Single base
- Multiple bases

(5) Base connection method **→Connection method between bases**
- Mesh type (IP-VPN, wide area Ethernet)
- Star type (Internet VPN, dedicated line)

(6) Server access method
- ASP type **→ASP service menu, load distribution**
- 1 location concentration type
- Base distribution type

(7) Redundant configuration (ISP connection line, backbone device, etc.)
- Present **→VRRP, OSPF**
- Absent

(8) Remote access
- Present **→Remote access service**
- Absent

(9) Address usage
- Global **→NAT**
- Private

(10) Deployment of Volp
- Present **→SIP, NAT**
- Absent

2. BCP (things that can be done immediately)

Basic policy

Basic idea

The object is to establish the same network environment for IPv6 as that of IPv4 (IPv4 will continue to be used as before for the time being).

Existing applications shall be used continuously in the existing IPv4 network system, and the new applications will actually be used in the new IPv6 network system after a trial operation.

Deployment method

At first, IPv4/IPv6 dual stack network shall be constructed within the minimum necessary range. If IPv6 is introduced partially, the networks shall be mutually connected by “IPv6 over IPv4” tunneling.

Then, according to the occurrence of regular update and the usage needs of the network, the support range of IPv6 will be gradually expanded.

BCP as security

It is crucial to ensure network security strictly in large enterprise/local government networks. The following is an explanation of tentative idea about security for the time being.

Modification model

Settings that support IPv6 shall be added to the F/W settings based on the present IPv4 at the same level, and moreover as additional settings, individual IPv6 accesses shall be permitted in a limited way.

At the first stage, partial segments shall be migrated to IPv6 (including tunneling connection), and regarding P2P access to IPv6 applications, it will be determined whether minimal holes should be made on the firewall after special investigation is held.

Strict model

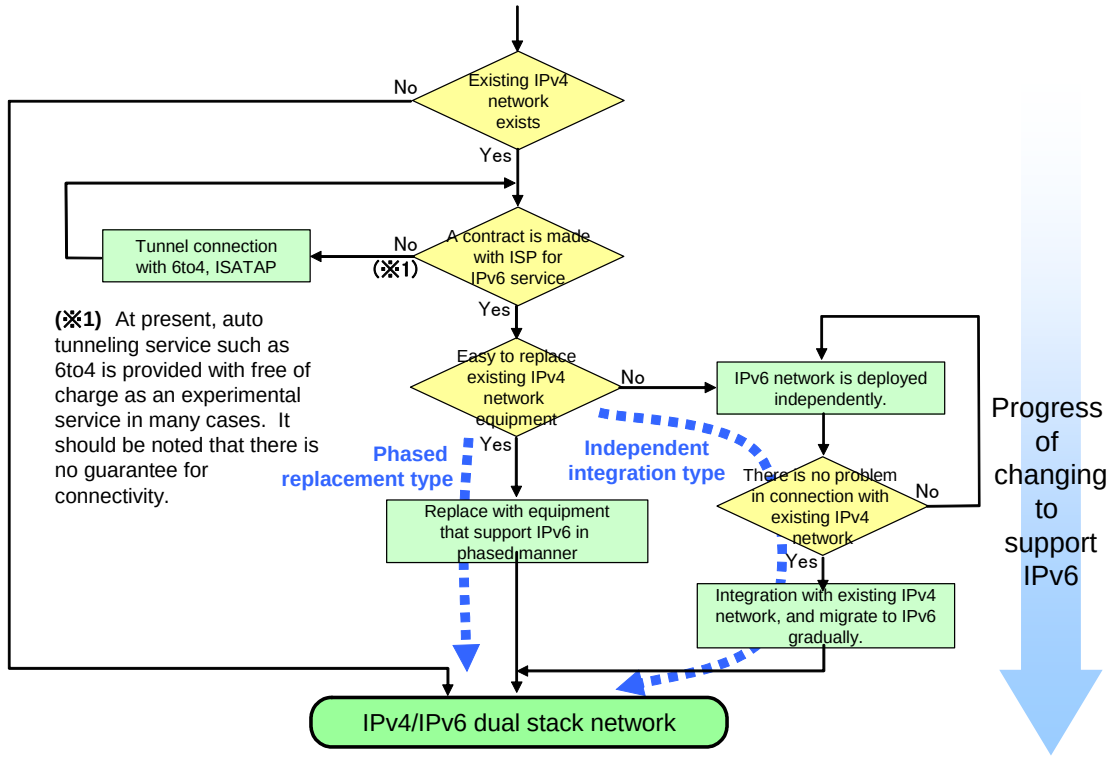
This model doesn't approve the connection of the existing network and new IPv6 network. At the first stage, the IPv6 network shall be constructed independently from the existing network.

Before the IPv6 security policy for large enterprise/local government is established for the further practical level, company confidential information and personal information are not handled in the IPv6 network or on the terminals connected to this network.

"The proper organization of IPv6 security policy is an immediate and most important issue!"

Flow of IPv6 network construction

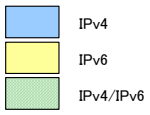
For deployment to the IPv6 network in the case of large enterprises and local governments, 2 types of patterns: the phased replacement pattern and independent integration pattern are considered.

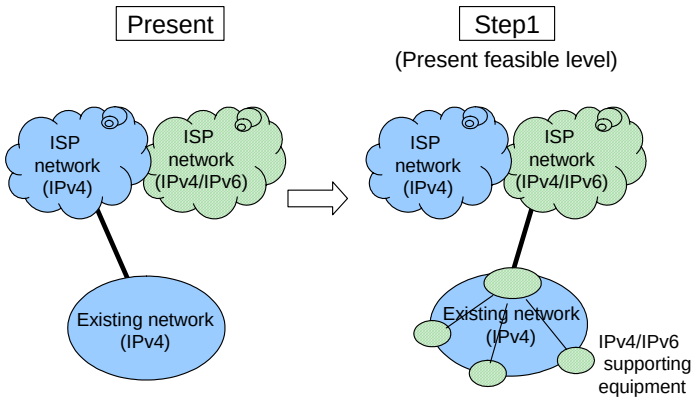


(※1) At present, auto tunneling service such as 6to4 is provided with free of charge as an experimental service in many cases. It should be noted that there is no guarantee for connectivity.

Deployment pattern of phased replacement type

Existing network shall be deployed to IPv6 in a phased manner and the backbone networks all support IPv4/IPv6 dual stack.

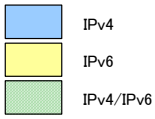


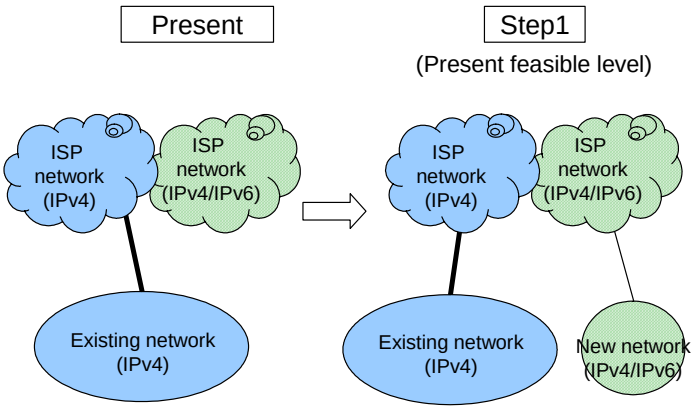


・Part of existing IPv4 network shall be replaced with equipment supporting IPv6 in a phased manner.

Deployment pattern of independent integration pattern

Independent IPv4/IPv6 dual stack network shall be integrated with the existing network, and traffic shall be deployed gradually.





・IPv4/IPv6 network shall be constructed independently from existing IPv4 network.

Reasons to introduce IPv6 “now”

The following are the presumed reasons for large enterprises to try to introduce IPv6 at the present stage.

(1) Advanced deployment of IPv6 network environment

To secure future network applications in advance by deployment of IPv6 in advance based on a long-term facility plan.

(2) Deployment of IPv6 along with deployment of new applications (VoIP, etc.)

For improvement of business efficiency for business trips, conferences, etc. Possibility of working at home.

Security management in units of organization → individual.

(3) Arrangement of environment for development of IPv6

Development of the products related to IPv6 is the main purpose.

(4) Improvement of company image/presence, sales capability/appeal to customers

It is plausible to expect the company image to be improved through deployment of cutting-edge technology.

2.1 Advanced Deployment of IPv6 Network Environment

IPv6 supporting service/equipment

“Fundamental environment for IPv6 (factor technology) is already furnished.”

ISP connection line

Major ISPs have already started providing commercial services via three types of methods; Tunneling method, Dual stack method, Native method.

Among these 3 methods, the Tunneling method is the most suitable to experience IPv6. Because the influence on the existing IPv4 network is the smallest with this method. However, it is necessary to prepare for overhead by capsuling. If you are considering full-scale deployment of IPv6, you need to choose a Dual stack method. In the case of the Native line method, which is for IPv6 only, there are many restrictions in usage at present

because DNS and SNMP have not completed support of IPv6 yet. It is better to think of Native line is a service for small scale ISPs.

Router

Most middle and large-scale routers already support IPv6 (processing of hardware is making progress as well). Mutual connectivity between vendors is high and verification of mutual connection with protocols such as RIPng, OSPFv3 and PIM-SM is also promoted. On the other hand, the support of small routers for IPv6 has not been promoted sufficiently. When considering that IPv4 and IPv6 can be configured independently, it is a requisite condition for routers to support IPv6 now.

Firewall

In the case of major firewalls, basic packet filtering function supports IPv6 now. Additional functions for practical usage are becoming enriched. However, it is necessary to investigate security policy for P2P applications and IPsec communication between client terminals, tunneling and multicast (→Refer to I-1~2 and J-1~4 in Security Guideline).

Furthermore, you need to be aware that there are no products that support multicast routing protocol as of now.

DNS server

If you use BIND, it is possible to change to IPv6 through standard upgrade of a version. If the network is dual stack type, you don’t need to adhere to the concept of migrating query packets to IPv6 (supporting AAAA records is important).

As a tentative method, it is possible to refer to external DNS that supports IPv6.

Root DNS servers now support IPv6 (.jp, .kr, etc.) with gTLD (Generic Top-Level Domains) and ccTLD (Country Code Top-Level Domain).

Some DNS implemented to a router and FW cause undesirable movement, therefore it is necessary to check them (→Refer to Section 6, Tips “Setting of DNS server”).

Other servers

With regard to web and mail (*1), major software already supports IPv6.

In the case of network control server, MIB supports IPv6 (SNMP is based on IPv4).

PC/PDA

Most major OSs already support IPv6 (but, the functional support level varies). IPv6 is deployed along with purchasing new OS and updating OS. It is necessary to take thorough security measures at the terminal level taking into account E2E communication.

(*1): With regard to deployment of IPv6 for mail server, it is necessary to check the support state of virus check applications separately and investigate support with consideration of security measure.

Acquisition of IPv6 global address

Acquisition method of IPv6 address

It is possible to receive allocation of a global prefix by making a contract with an ISP that provides IPv6 services (there are many ISPs including commercial and test services). (*)

Under the present effective address policy, one or multiple /48 sized addresses are allocated from the upper ISP with which a contract is made as an address space allocated to an enterprise and local government.

However, when the scale of an enterprise is large or an Intranet is configured within group companies and the enterprise controls/uses an enterprise network that is capable of configuring a large scale network, which has more than 200 sites to allocate /48, such enterprise complies with the initial assignment standard of address policy, therefore they are eligible to apply for a RIR (Regional Internet Registry, Japan is under jurisdiction of APNIC) for independent address space of /32 and to acquire address through review.

In the case of local governments, on the other hand, it is considered necessary to maintain independence of address space at the review according to the public utility of the service provided by an local government and the bylaws of the organization, so that even if the scale of such organization is not large enough to allocate /48 to more than 200 sites, it is possible to receive assignment of /32 address. However, when /32 space is acquired from APNIC, as in the case of an ISP, it becomes a duty to perform control of allocation of /48 space and report to APNIC.

(*): For the address assignment method in the case to introducing IPv6 in a closed area as a trial at the initial deployment stage before actually acquiring global address from ISP, refer to Section 6 Tips “IPv6 Local address assignment method”.

Detailed information with regard to acquisition of IPv6 address

Site of JPNIC:
http://www.nic.ad.jp/ja/translation/ipv6/20040714-01.html
Site of IPv6 Promotion Council of Japan Remote Control Node Address SWG:
http://www.v6pc.jp/jp/wg/remoteSWG/index.html

Design of IPv6 global address

Basic idea

Global prefix of /48 is sufficient address space (*) for most large enterprise/local government networks, however, the following points should be considered taking into account development in the future.

- Simple and efficient (easy to see) allocation of address
- Schematic address allocation assuming recombination/expansion of network configuration in the future
- Address allocation accommodating geographical/organizational configuration in the target network

(*) In the case of IPv4, it is necessary to design address when dividing segments after devoting close consideration to the number of terminals anticipated to be connected in the future. In the case of IPv6, on the other hand, it is actually possible to connect an infinite number of terminals by interface identifier of lower 64-bit, therefore, when the global address of /48 is acquired, it becomes possible to design addresses for segment division using 16-bit without consideration for the number of terminals.

Routing

The present supporting status of equipment

Most routers that support IPv6 support RIPng. Some upper models support OSPFv3. Compatibility with the products of other companies is also verified, therefore there are no practical problems.

IPv6 routing protocol in large enterprise/local government networks

At the initial stage of deployment of IPv6, static routing is sufficient. RIPng or OSPFv3 can be introduced along with an expansion of the scale.

When using dual stack, it is probably easier to understand if it is used with routing protocol of IPv4.

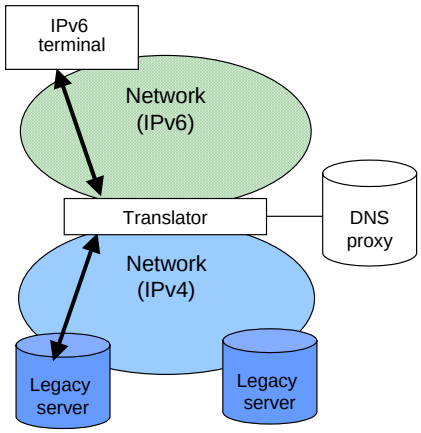
When using multicast for a service of live reporting or broadcasting, equipment supporting multicast routing protocol such as PIM-SM shall be selected.

Translator

Features

NAT-PT method and TRT method are commercialized. Communication between IPv4 host and IPv6 host is realized by translating protocol at the middle of communication.

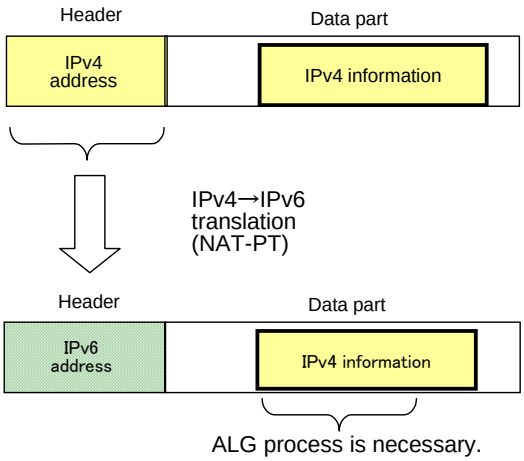
It is possible to specify the communication partner with FQDN (Fully Qualified Domain Name) using DNS proxy. It is possible to support IPv6 without changing server settings of legacy system (possible to use the huge assets of IPv4 the system as it is).



Problems

ALG (Application Level Gateway) is required for an application with hierarchy violation (refer to Fig. below). When translating packets from IPv4 to IPv6, it is necessary to pay attention on setting of MTU (Maximum Transmission Unit). FQDN is necessary for the communication partner.

Moreover, it is required to use with protocol translation using reverse proxy.



Tunneling

Fixed tunneling

IPv6overIPv4 tunnel shall be created in a fixed manner between specified IPv6 supporting routers.

Auto tunneling

DTCP (Dynamic Tunnel Configuration Protocol)

When this method is used, it becomes possible to create tunnel dynamically from client side (E.g., experiment of free bit Feel6 Farm IPv6 connection).

6to4

IPv6 address shall be created automatically from a global IPv4 address (*1), and tunnel is created in between with 6to4 relay router provided by the major ISP. It is not guaranteed that the outward and inward paths become the same.

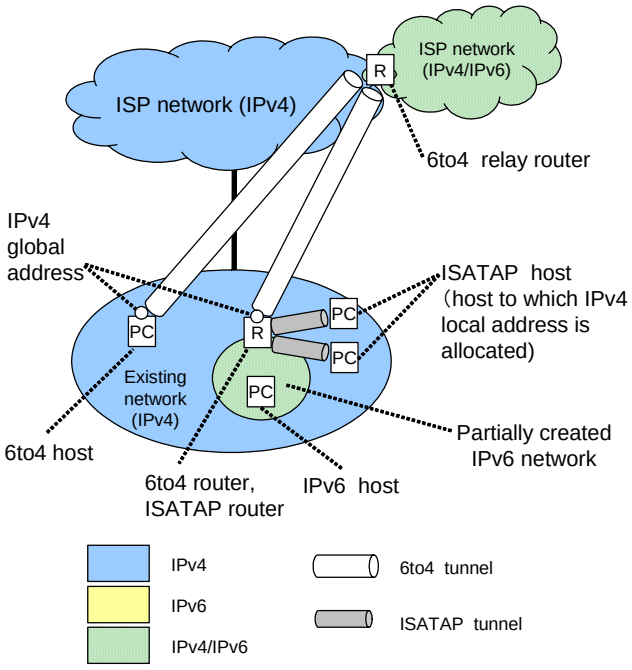
ISATAP

It is possible to create a tunnel in a LAN where local IPv4 addresses are used.

Teredo

It is possible to use tunnel technology in an environment where a NAT device intervenes.

IPv6 deployment image using auto tunneling protocol (6to4, ISATAP, etc.)



6to4 tunnel shall be created between disclosed 6to4 relay router and router/host that has IPv4 global address. Between ISATAP router (IPv4 global and local boundaries) and host that does not have IPv4 global address, ISATAP tunnel shall be created.

When there is F/W in the tunnel creation zone, it is necessary to make settings so that IPv6toIPv4 packet (IP protocol No.41 packet) can pass through.

It is relatively easy to introduce IPv6, but there are problems with performance, reliability and security. However, in the case of 6to4 tunnel, it is not guaranteed that the outward and inward paths of the packet to be transferred become the same.

Deploying the boundary part to IPv6

Functions required for the boundary part in the existing network are filtering, logging, NAT (address translation), virus checking, remote access and IDS.

In IPv4, the firewall and NAT realize the above-mentioned functions (functions are required for IPv6 as well, except address translation function).

When introducing IPv6, it is desirable to introduce a router that supports IPv4 and IPv6 (firewall if possible) as an addition, without changing the existing IPv4 part. The new router that supports IPv4/IPv6 processes only the IPv6 traffic, and the same filtering (*1) is set as in

IPv4 as a basic rule.

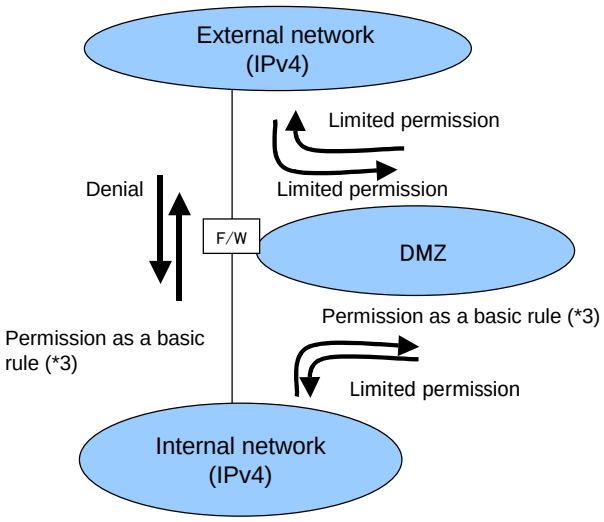
IPv4 traffic is processed at the existing IPv4 part (*2).

(*1) In the case that high functional filtering equivalent to IPv4 is not supported, denial shall be set as a basic rule. Refer to “MTU Discovery” in “Section 6 Design Usage Guideline (tips)” for the filtering settings regarding ICMP.

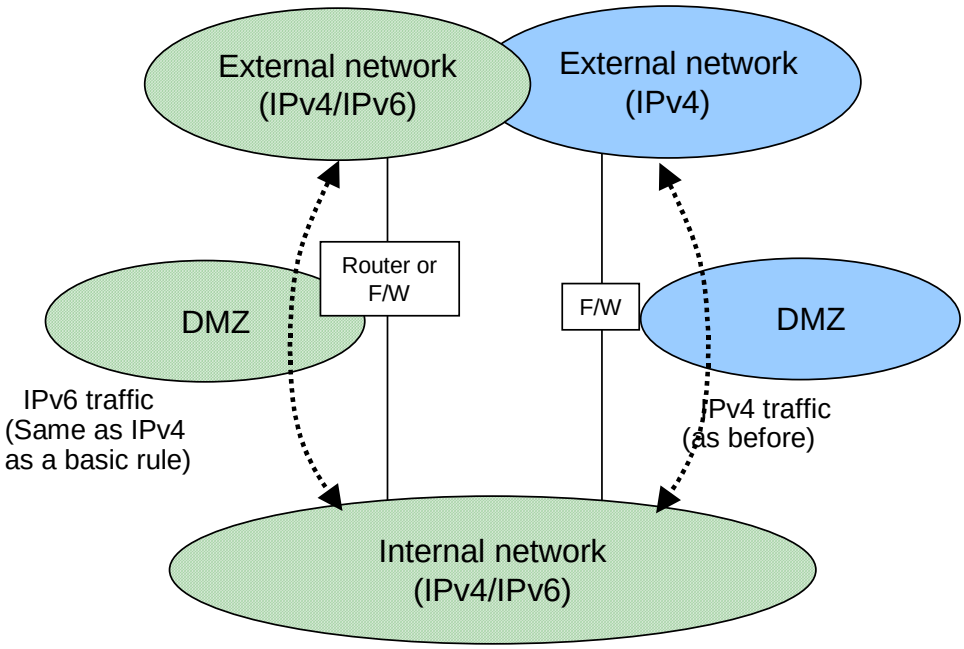
(*2) The reasons that a router supporting IPv4/IPv6 doesn’t process IPv4 traffic are to prevent degradation of an existing security level and to continue providing existing service even if the trouble occurs on the IPv6 side. The same way of thinking applies to logging, virus check and IDS function as well.

(*3) Filtering settings as a large enterprise/local government network are set at “limited permission (basically denial)” according to the security policy of each organization in many cases.

<Former configuration>



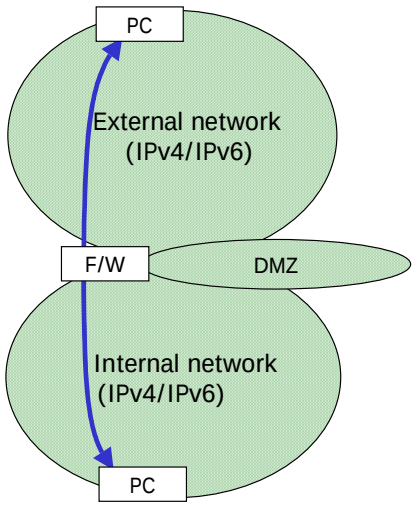
<Configuration at deployment of IPv6>



Filtering

<u>In the case of F/W that supports IPv6</u>

At present, it is a basic concept to maintain (or to avoid degradation) the same security policy for both IPv4 and IPv6.



・E2E communication

When permitting E2E communication that is via a firewall, only the specified accesses (filtering with IP address and port No.) should be put through the limited terminals (→Refer to Security Guideline: A-1~3).

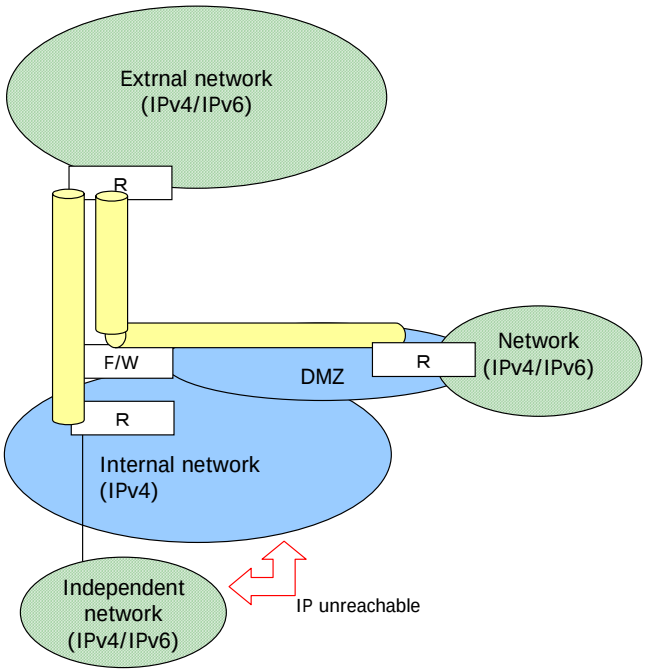
E2E communication based on IPsec, which goes through firewall is an issue to be investigated in the future. When permitting on a trial basis, only the specified accesses (filtering with IP address) should be put through the limited terminals. At this time, security measures including personal F/W should be used on the terminal device (→Refer to Security Guideline: A-4).

<u>In the case of a F/W that doesn't support IPv6</u>

・IPv6overIPv4 tunnel

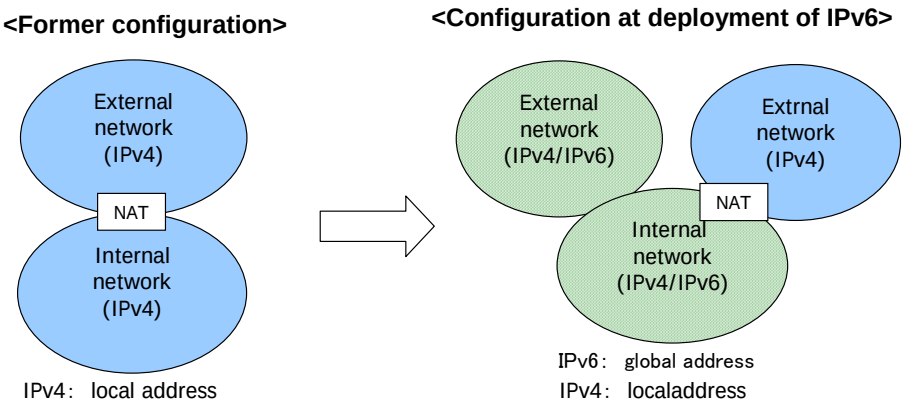
Basically, IPv6overIPv4 tunneling access is permitted for DMZ (passing of IP protocol No. 41 is permitted), and a partial IPv6 supporting segment shall be created in DMZ. In this IPv6 supporting segment, connection hosts should be limited and special security control should be used.

When permitting IPv6overIPv4 tunnel connection to the internal network (IP protocol No.41 passes), it should be performed using the network (IP unreachable) separated from the existing network for the time being.



NAT

In IPv4, NAT was frequently used (*1) in order to save address space. However, in IPv6, local address using NAT is not used as a basic rule.



・Keeping address information confidential

In the former IPv4 network, address information inside an Intranet was kept confidential as a result of usage of NAT. Therefore, if any error occurred on a communication with outside, troubleshooting was a hard job. The necessity for keeping address information confidential (*2) is an issue to be investigated in the future.

(*1) In some cases of IPv4, NAT is used for the connection between private networks (duplicate NAT) due to integration of companies.

(*2) In the case of IPv6, it is possible to keep interface identifier (host part) confidential using Privacy Extension (RFC3041), however, it is necessary to investigate the usage method from the view point of network management (→Refer to Security Guideline: D-1).

Remote access

The following are the remote access methods used at present.

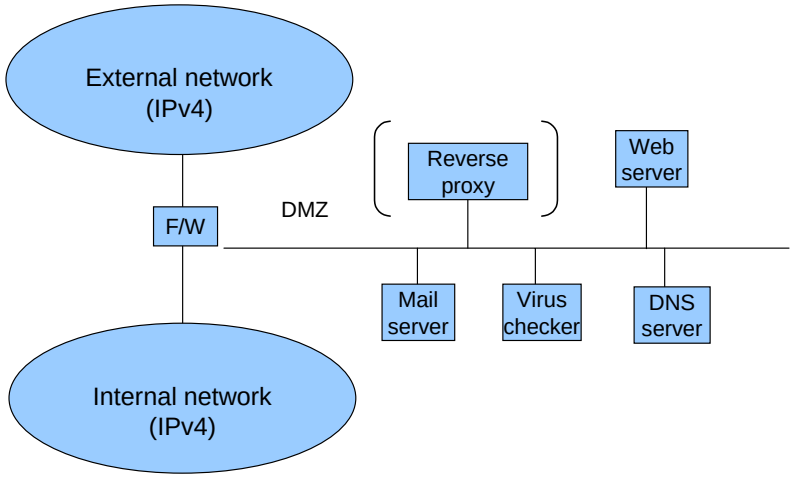
(a) To make a phone call to NAS (held by a company).
(b) To make a phone call to NAS (held by a provider) and access from there using L2TP as a batch.
(c) Internet VPN (tunnel mode)
(d) SSL-VPN

It is most realistic to form an IPv6 tunnel in a remote access of IPv4 at present. However, it shall be “IPv6 over IPv4 over IPv4 (security tunnel)”, therefore, it becomes necessary to consider fragmentation problems in particular.

Deploying DMZ to IPv6

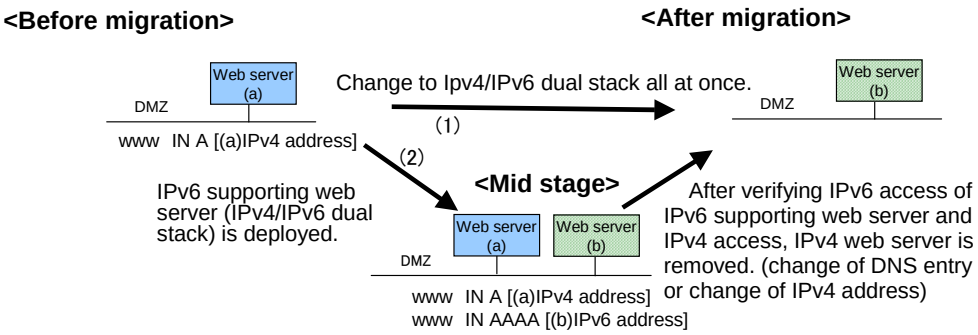
Web server

Fig. shows a configuration example of DMZ configured using Firewall (F/W). It is considered that web server (reverse proxy, instead), mail server, DNS server, virus checker and SSL accelerator are set in DMZ.



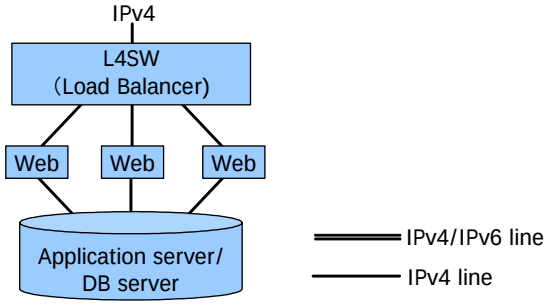
・Deploying Web server to IPv6

Deploying web server to IPv6 is relatively easy to realize through upgrading version including Apache 2.0. Two IPv6 deployment patterns for web servers in actual use are considered; (1) changing to IPv4/IPv6 dual stack all at once and (2) using IPv4 web server and IPv6 supporting web server (IPv4/IPv6 dual stack) together for a certain period.



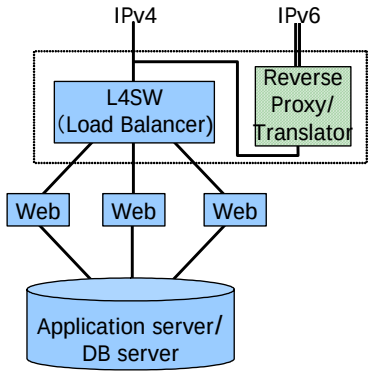
In the case of large scale system

Fig. shows the device configuration example of a large scale system in which load is distributed over multiple web (front end) servers using a load balancer. <Configuration 1> - <Configuration 3> shown below are considered as the deployment patterns to support IPv6.



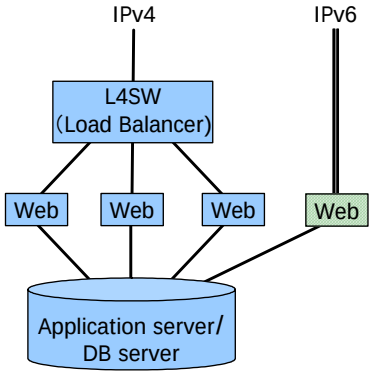
<Configuration 1>

Access based on IPv6 is translated by protocol using Reverse Proxy and processed in the same handling manner as access based on the existing IPv4.



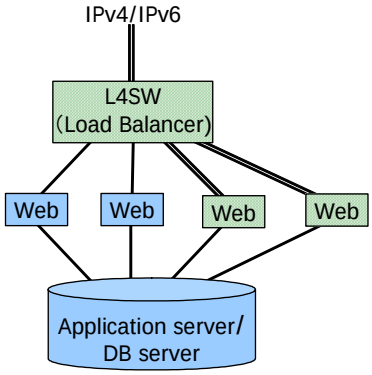
<Configuration 2>

Load of access based on IPv6 is not distributed, and web server that supports IPv6 is set individually.



<Configuration 3>

L4SW and web servers shall be made to support IPv6.



Connection method between bases

Relationship of connection method between bases and availability of dual and tunnel is shown in Table below.

	Dual (IPv6/IPv4)	Tunnel (IPv6 over IPv4)
Frame relay	○ (*1)	○
Dedicated line	○ (*1)	○
IP-VPN	- (*2)	○
Wide area Ethernet	○ (*1)	○

(*1) OK to use when terminal device is made to support IPv6 (should be IP independent. But it's necessary to check with service provider).
(*2) There is no service that supports IPv6 at present.

At the initial stage of deployment of IPv6, it is realistic to do so using a tunnel. It is all right to think about a new service menu that supports dual stack when the load of traffic, etc. becomes extreme.

With regard to QoS maintenance/control of new IPv6 application or existing IPv4 application along with deployment of IPv6, it is necessary to check with line providers for each connection service between each base.

Terminal control

Control of terminal address information and DNS information

The following are the address setting method for the terminal and notification method of DNS address with IPv4 and IPv6.

	Address setting to terminal	Notification of DNS address
IPv4	DHCPv4/Static	DHCPv4/Static
IPv6	RA (*1)/Static	DHCPv4/Static

(*1) When it is necessary to specify a terminal from a log, it becomes possible to control as for MAC address by creating interface identifier using EUI-64. However, in this case, it is not possible to control completely, and it is a precondition not to use Privacy Extension. In order to realize more strict terminal control, it becomes necessary to consider using

authentication system or VLAN (refer to “Network access control” in Section 4, Issues for IPv6 distribution period).

(*2) It is not possible to set DNS information automatically to a client terminal only with RA function (RFC2461, 2462) of IPv6. Provision method of DNS information to a terminal in IPv6 (RFC3315, 3646, etc.) has just been standardized; therefore, it is realistic to use DHCPv4 at the present stage.

- Possible to set IPv6 address and other information on UNIX type terminals in a static manner
- Possible to set IPv6 address on Windows type terminals in a static manner
  (query of DNS is IPv4 only).
- When using DHCPv6 after DHCPv6 is distributed, it is necessary to investigate the usage method again.
  (In order to avoid inconsistency of setting information due to mixture of DHCPv4 and v6.)

2.2 Deployment of IPv6 along with Deployment of New Application

How to promote applications supporting IPv6

New applications shall support IPv4/IPv6 dual stack as a basic rule.

It is not necessary to make existing applications support IPv6 forcibly. They can be changed to support IPv6 (*1) when software version is upgraded. When there is a front application, it should take priority to be changed to support IPv6.

(*1) However, as of now, for instance when migrating mail servers to IPv6, it is necessary to check anti virus application’s status of support for IPv6 separately and consider security measures as well.

For developers Applications shall be developed in a framework independent from protocol. It is desirable to investigate the usage of an interface that doesn’t depend on the application, such as RPC.

What is an application suitable for IPv6

As applications suitable for IPv6, various P2P applications are considered first of all.

Type of P2P applications	Inside Intranet	Outside (specified)	Outside (not specified)
VoIP	○	○	○
IM (Instant Messenger)	○	○	○
Groupware	○	○	-
Serverless File sharing	○	○	-
Maintenance/Monitoring	○	○	-
Multicast streaming	○	-	-
Dedicated address (Mobile IP)	○	○	-
TV conference	○	○	-

VoIPv6 solution

This is a solution to reduce costs related to external connection of IP phone. It is just to make a contract for IPv6 and punch a hole in a firewall for the necessary traffic. It is possible to reduce cost using external connection of IPv6 phones, compared with external connection of IPv4 phone, which is considered as likely to spread in the future.

The presumed effects would be, reduced load on external line GW (SIP-NAT), reduced cost for acquiring global address and simplified IP phone traffic (concentrated on a center can be avoided).

In the meantime, security shall be ensured by only permitting passage of traffic related to IPv6 phone (specifying protocol ID and address) using a firewall. At the actual deployment, independent integration type or phased replacement type is selected according to security policy of each company.

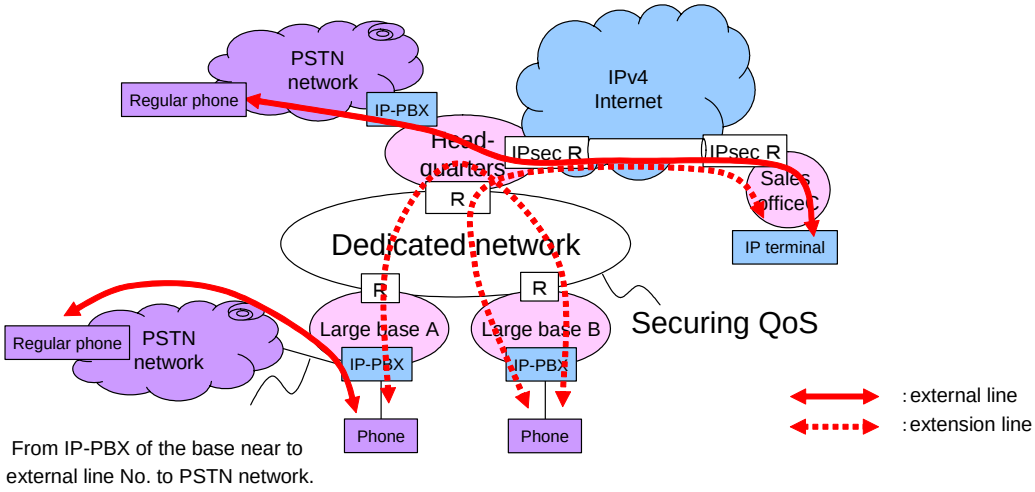
When the load on GW becomes a bottleneck for some kind of APL, not limited to IP phone, it is possible to construct as ○○ solution using the same logic.

In June, 2004, an example case applying VolPv6 service to approx. 300 bases and approx. 20,000 terminals was reported.

Present IP phone deployment pattern

At present, IP phones are mainly used as an extension phone. Usage of IP phones for external lines will be realized in the future. At large scale bases, connection equivalent to dedicated line shall be carried out in order to secure QoS. Sales offices and branches are connected with Internet VPN.

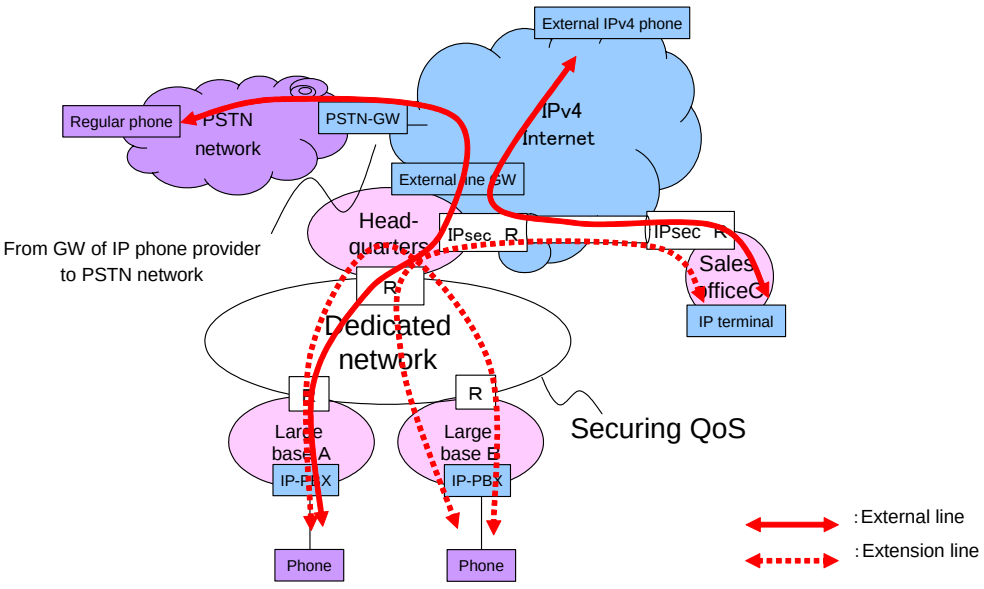
The problem is in the complication of communication traffic for sales offices and branches.



Expansion of IP phone by IPv4 (external connection)

External line gateway (SIP-NAT) is crucial for connection with external IP phone. All external line traffic should go through external line gateway (PSTN calls, too).

It is requisite to secure capacity of external line gateway according to the demand for external line. Additional cost is required to secure quality of call.



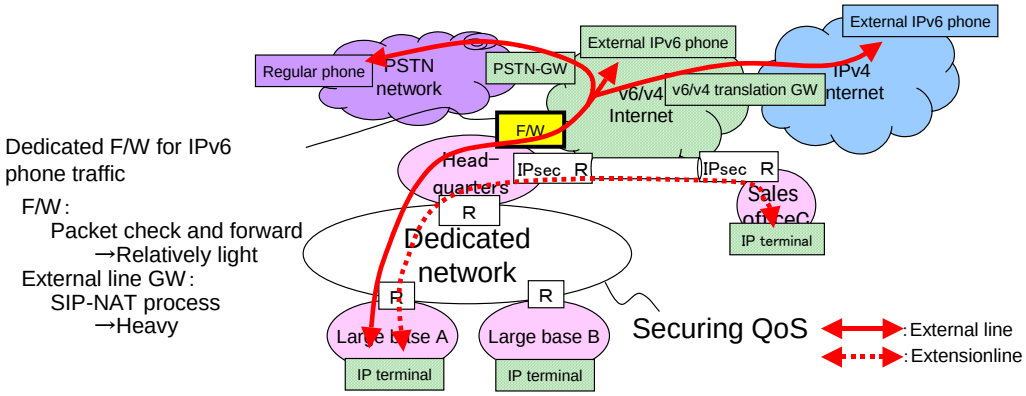
VoIPv6 solution ~ For large scale bases ~

Load of external line gateway, which is considered necessary to connect IP phone with external line should be reduced.

<u>IPv6 external line doesn't go through external line gateway → goes through firewall</u>

An exit to the Internet that allows only traffic of IPv6 phone to go through shall be held. Exit firewall shall be controlled by the information control division.

The merits of this method are that the load of HQ and external line gateway is reduced and cost is reduced.

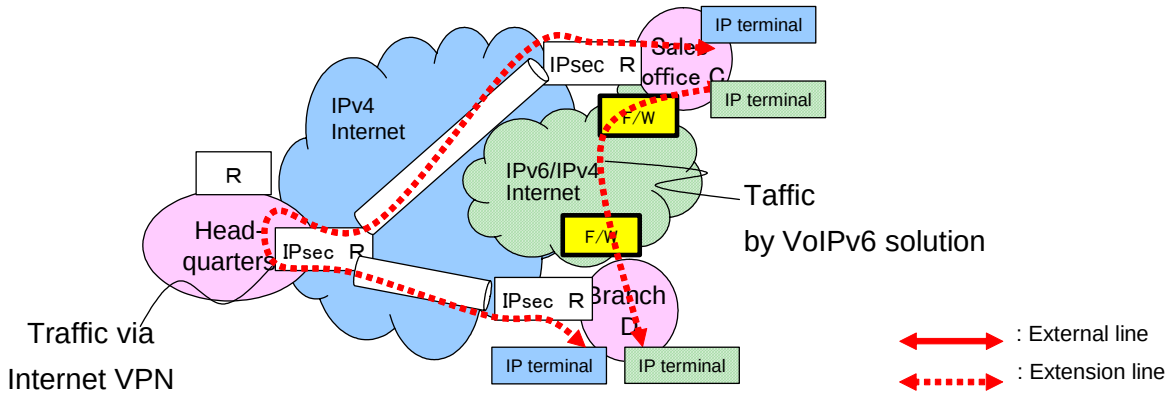


VoIPv6 solution ~ For sales office/branch ~

Traffic via Internet VPN to sales offices and branches should be simplified.

Firewall of the base shall have an exit to the Internet that allows only traffic of IPv6 phone to go through. Firewall at exit shall be controlled by the information control division.

The merit of this method is that new IPv4 addresses are not required and cost can be reduced (when the same configuration is used for IPv4, new global address is required). Another advantage is that calling traffic via Internet VPN can be simplified.



VoIPv6 solution ~ Another merit ~

When IP extension phones are distributed, nearly double the number of addresses becomes necessary.

Example: In the case of a work place with 100 employees

For server/router/printer/wireless AP (dedicated allocation) : 50 pcs.

For PC (DHCP allocation) : 150 pcs. (operation is possible with total 200 pcs. = /24)

120 IP extension phones are added → Total 320 addresses are required (overflow with /24)

In the case of IPv4, subnet needs to be designed again, so subnet mask shall be changed. Or different segment shall be added (= IP phone shall be defined as a different segment).

In any case, cost for re-design becomes large.

In the case of IPv6, on the other hand, re-design required for IPv4 (re-design of subnet due to increase in the number of terminals) is not necessary.

2.3 Concrete IPv6 introduction concept

Classification factors of large enterprise/local government network: Pattern A

(1) Number of connection points with Internet
- (●) 1 location
- Multiple locations

(2) Type of Internet connection lines
- (●) Dedicated line
- xDSL, CATV, FTTH

(3) Number of users (access amount to shared server)
- (●) 100 persons and under
- 100 persons and over

(4) No. of bases
- (●) Single base
- Multiple bases

(5) Base connection method
- Mesh type (IP-VPN, wide area Ethernet)
- Star type (Internet VPN, dedicated line)

(6) Server access method
- ASP type
- 1 location concentration type
- Base distribution type

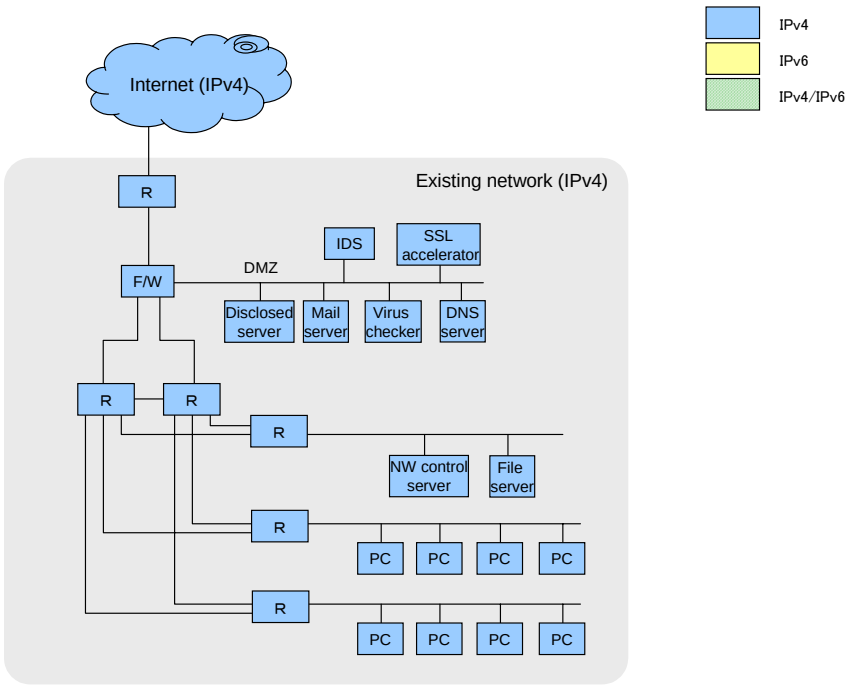
(7) Redundant configuration (ISP connection line, backbone device, etc.)
- (●) Present
- Absent

(8) Remote access
- Present
- (●) Absent

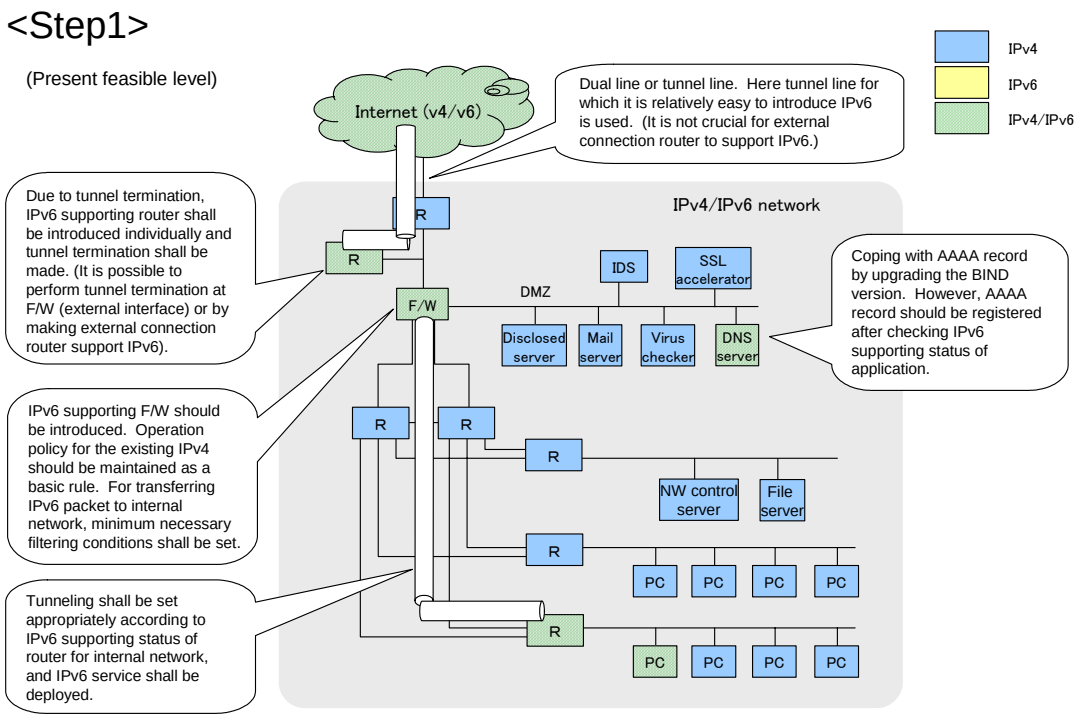
(9) Address usage
- Global
- (●) Private

(10) Introduction of VoIP
- Present
- (●) Absent

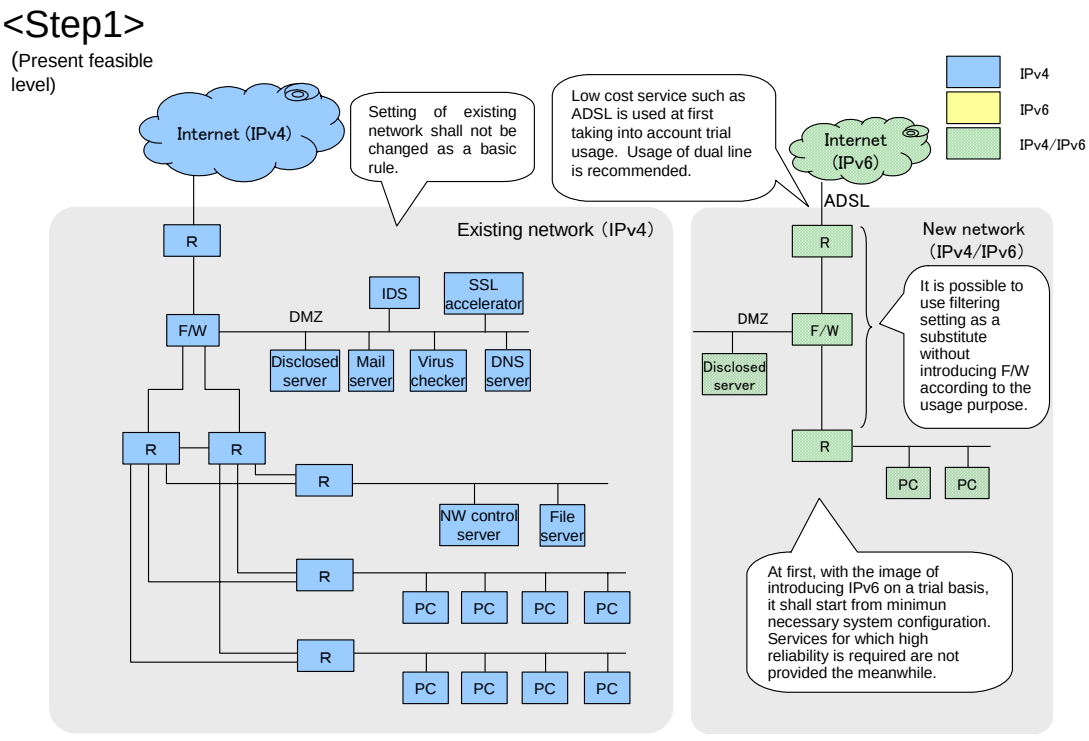
Example of large enterprise/local government network: Pattern A



Phased replacement type: Pattern A



Independent integration type: Pattern A



Classification factors of large enterprise/local government network: pattern B

(1) Number of connection points with Internet
- 1 location
- ◉ multiple locations

(2) Type of Internet connection lines
- ◉ Dedicated line
- xDSL, CATV, FTTH

(3) Number of users (access amount to shared server)
- 100 persons and under
- ◉ 100 persons and over

(4) No. of bases
- Single base
- ◉ Multiple bases

(5) Base connection method
- ◉ Mesh type (IP-VPN, wide area Ethernet)
- Star type (Internet VPN, dedicated line)

(6) Server access method
- ASP type
- ◉ 1 location concentration type
- ◉ Base distribution type

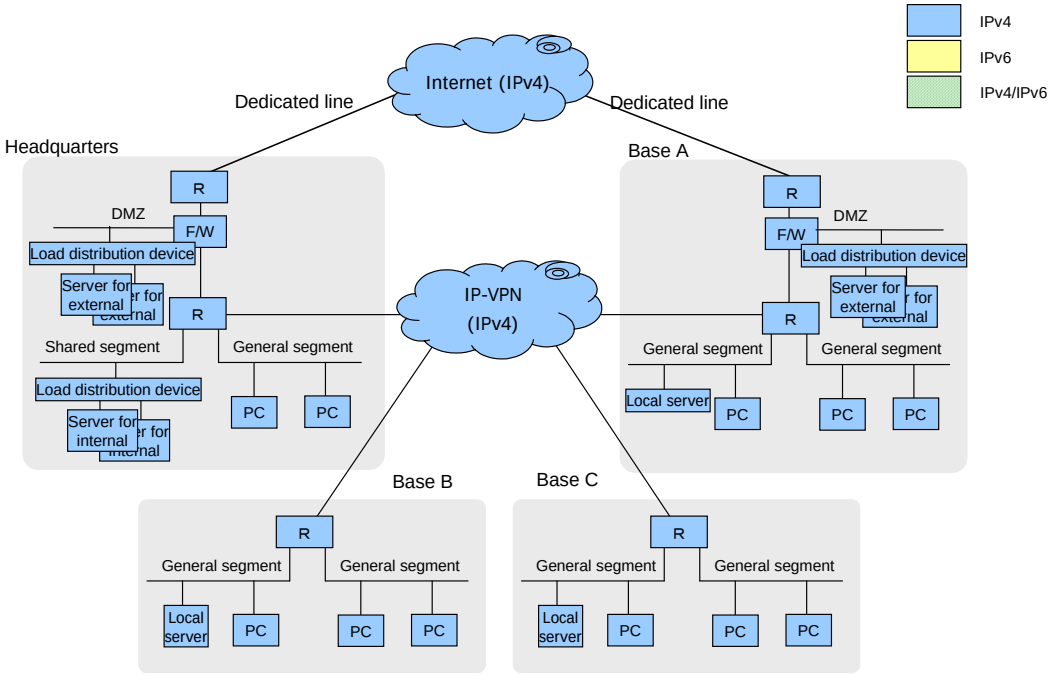
(7) Redundant configuration (ISP connection line, backbone device, etc.)
- Present
- ◉ Absent

(8) Remote service
- Present
- ◉ Absent

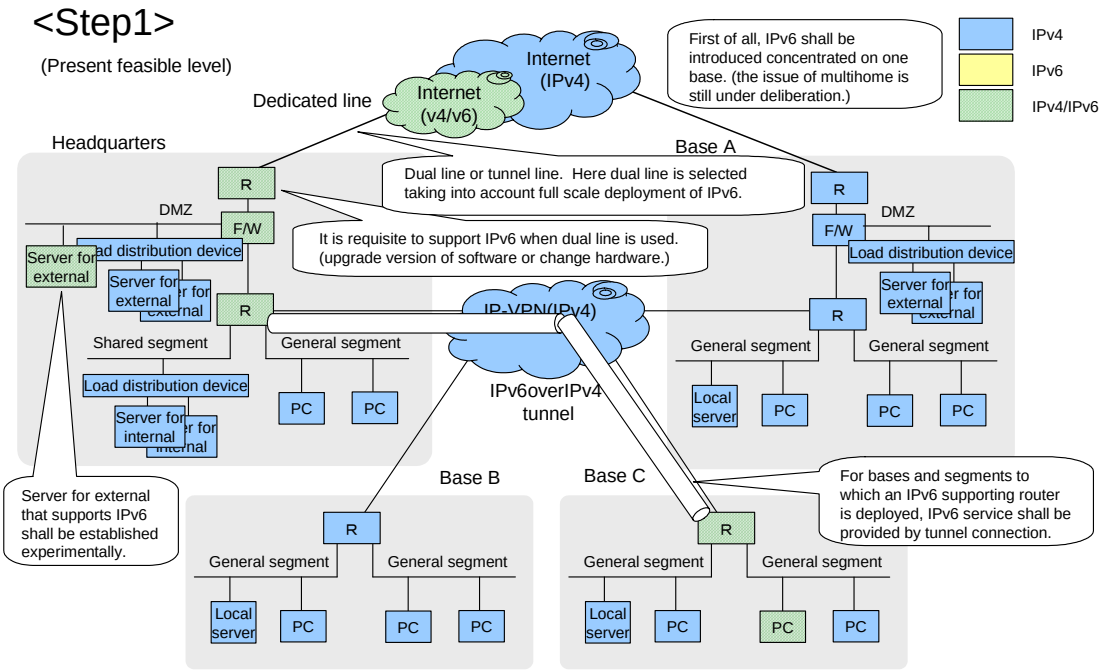
(9) Address usage
- Global
- ◉ Private

(10) Introduction of VoIP
- Present
- ◉ Absent

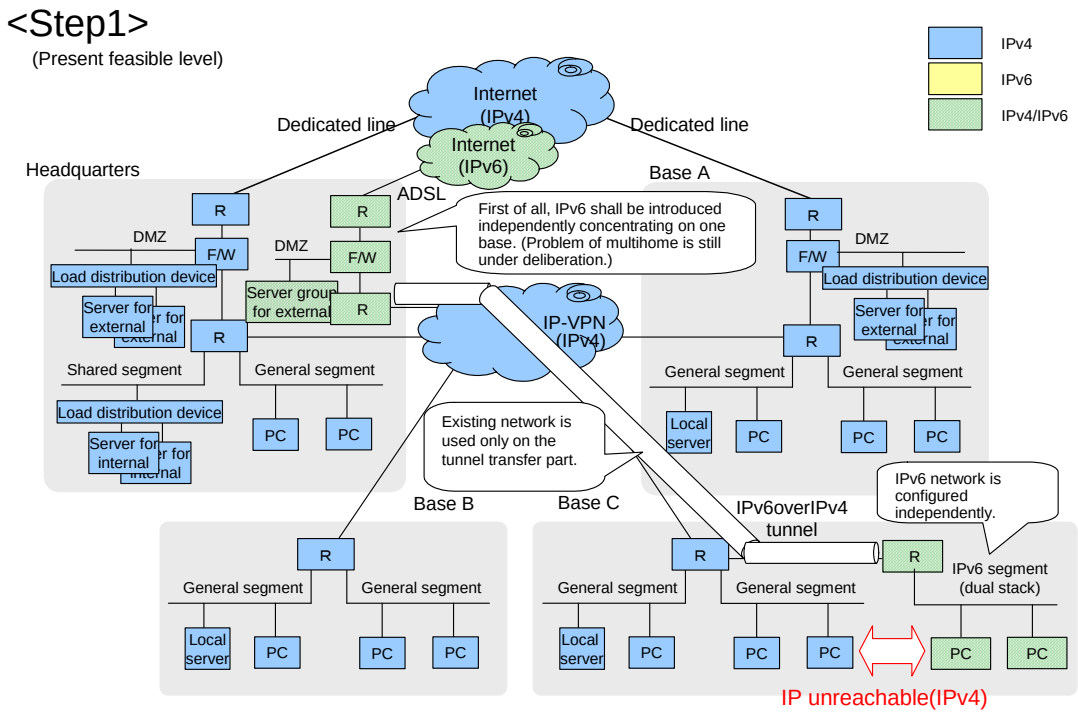
Example of large enterprise/local government network: Pattern B



Phased replacement type: Pattern B



Independent integration type: Pattern B



3. The Target NW & System Form + Application in the IPv6 Distribution Period

Assumed IPv6 usage environment and fundamental policy in IPv6 distribution period

Assumed IPv6 usage environment

The following is the assumed usage environment in the IPv6 distribution period.

Enrichment of IPv6 network environment

- IPv6 line service by middle and small scale ISP (dual stack, tunnel)
- Enrichment of product variation of large ~ small routers
- Full scale support of IPv6 functions by basic OSs (mobile, IPsec)
- Various application soft that supports IPv6 will be distributed.
- Enrichment of products with security measures such as firewall and IDS

Distribution of new network framework

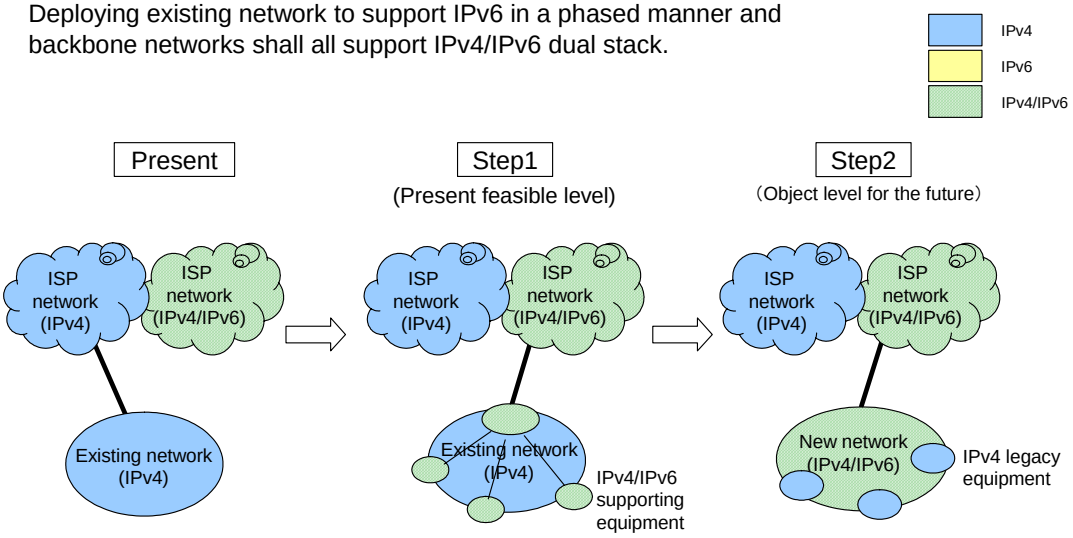
- Non-PC network connection. (progress of changing to ubiquitous)
- From security control in units of organizations to security control in units of individuals

Security policy is established in the IPv4/IPv6 dual environment.

- Applications utilizing features and merits of IPv6 will start to be distributed under new security policy.
- Illegal action based on IPv6 will become common?

Deployment pattern of phased replacement type

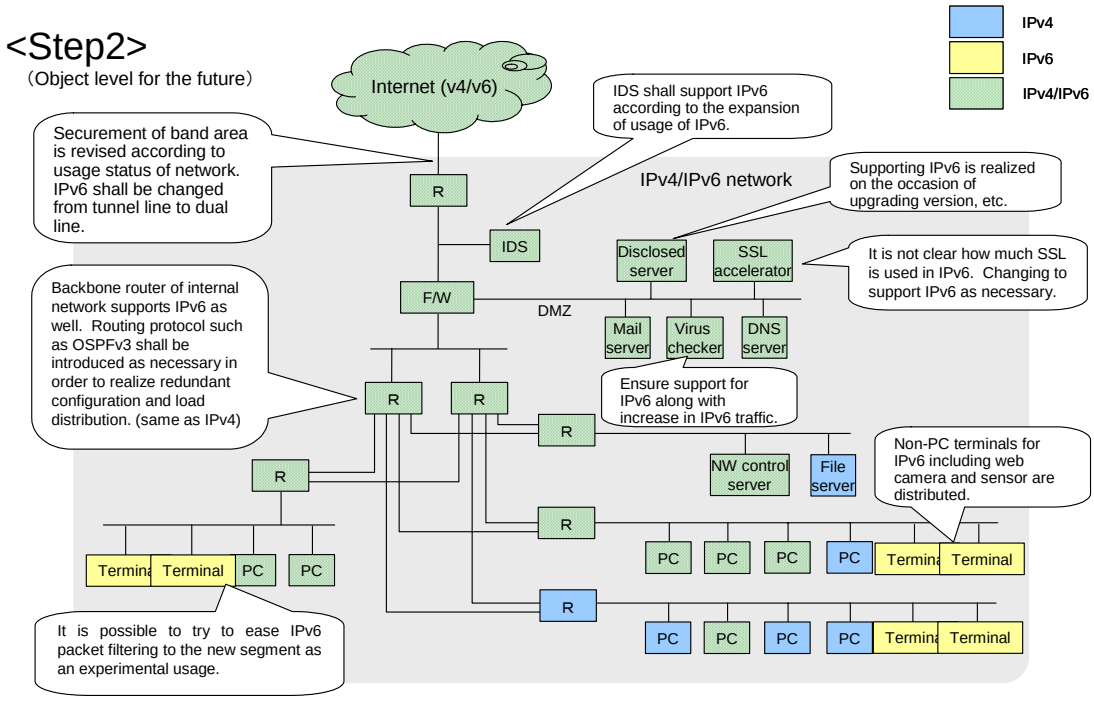
Deploying existing network to support IPv6 in a phased manner and backbone networks shall all support IPv4/IPv6 dual stack.



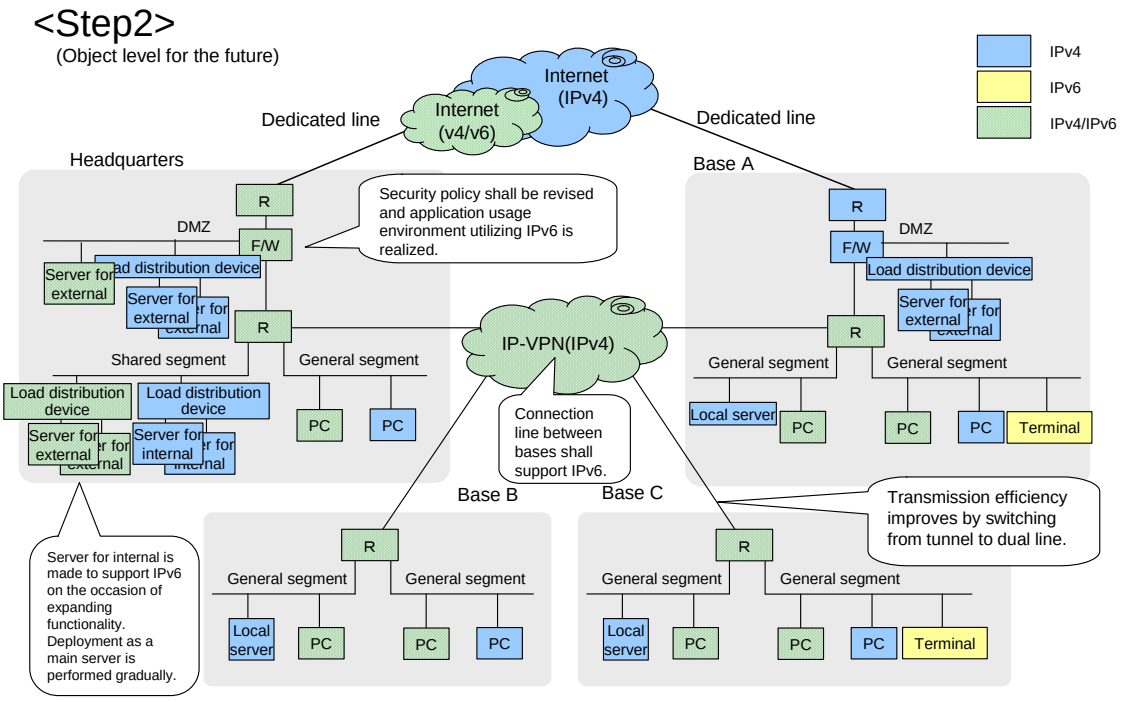
・Replace part of existing IPv4 network with IPv6 supporting equipment in a phased manner.

・Progress of deployment from IPv4 to IPv6.
・IPv4 legacy facility remains.

Phased replacement type: Pattern A

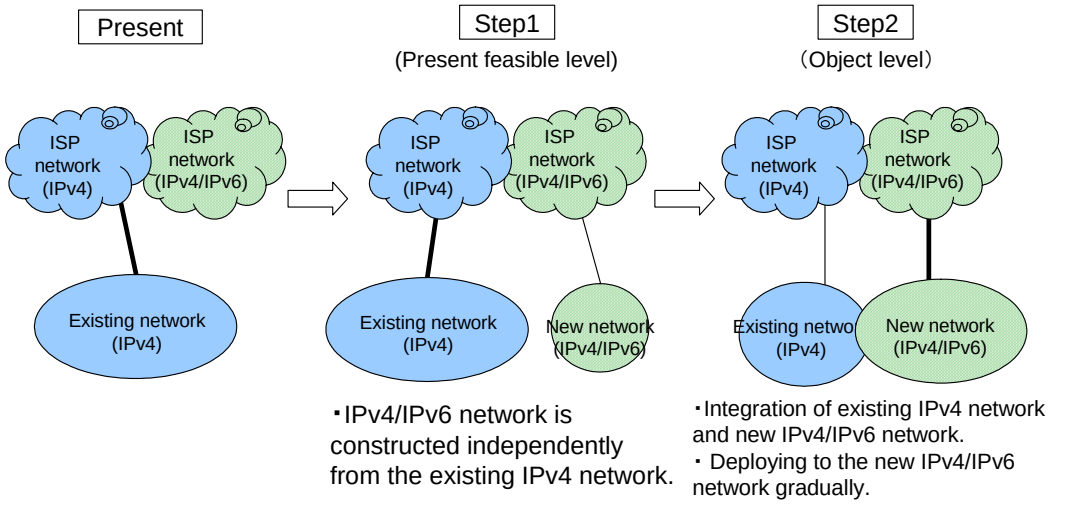


Phased replacement type: Pattern B

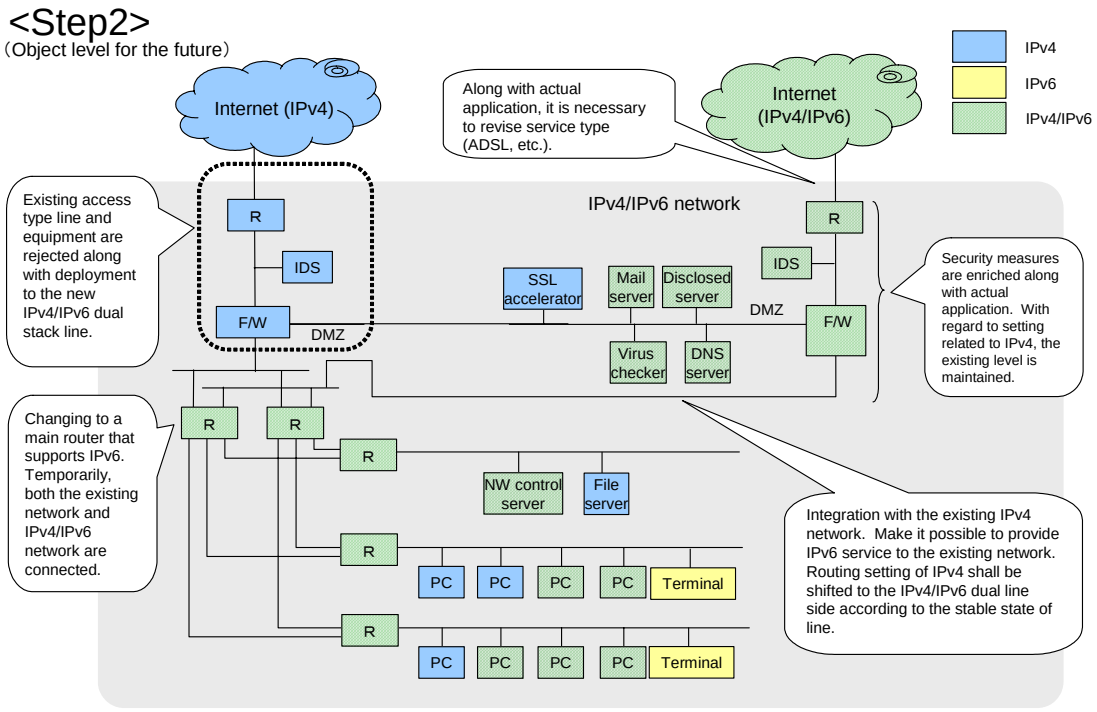


Deployment pattern of independent integration type

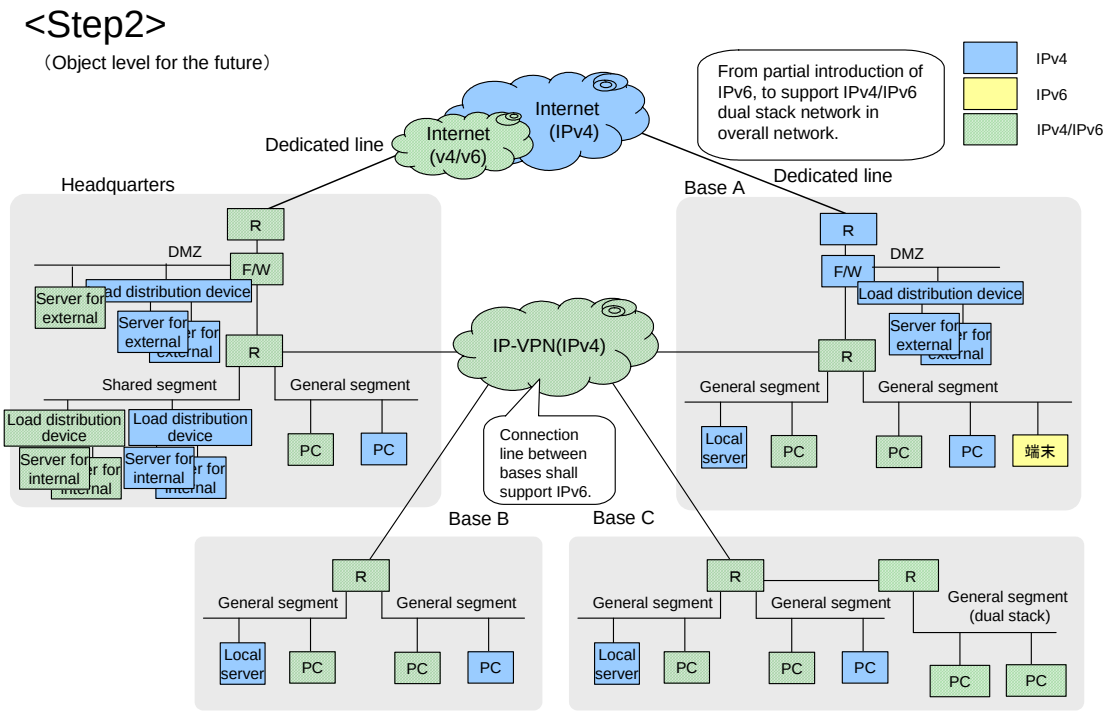
Independent IPv4/IPv6 dual stack network is integrated to the existing network and traffic is deployed gradually.



Independent integration type: Pattern A



Independent integration type: Pattern B



Application: Things to realize with IPv6

“Plug & Play + Secure + Manageable network”

Ideal IPv6 environment

- End users are able to communicate only with appropriate partners safely without settings once they connect the terminals.
- Administrators are able to identify owner/location of the terminal easily.
- Administrators are able to control settings of end users as a batch.

Network configuration

- There is no special change in network topology.
- Location of a terminal can be changed frequently.

Protocol stack

- Dual stack is a basic rule.
- Pure-IPv6 (only +legacy server has reverse proxy)

*Operation cost of IPv4+IPv6 vs deployment of applications to IPv6

Trade off of cost

* IPv6-only terminals will be released someday in the future.

Security

- Authentication method for each terminal and access control method when permitting E2E communication.
- Limitation method related to encryption of E2E with outside.
- Administrators favorably limit and check communications flexibly based on the security policy of the organization.

Requirements for realization of suitability for IPv6

- Handling of mobility
- Dynamic name registration (Dynamic DNS or SIP)
- MIPv6

E2E communication (usage of SIP, etc.)

- VoIP (extension line, external line)
- TV conference
- File sharing
- IM

Access limitation method from other terminal

- Personal Firewall
- Access from outside
- External access by employees (IPsec, F/W)
- Equipment maintenance access (separate line)

- Security for internal access
- Source spoofing attack measure
- Filtering with terminal housed directly in a terminal
- Layer 2 switch that filters abnormal RA
- Privacy Extension measure

→Which one, and to what extent should it be admitted?

4. Issues for IPv6 Distribution Period

Multihome

Merits of multihome

Redundancy of connection to the Internet is secured in multihome. Moreover, It is possible to set to optimize paths and distribute load. Under IPv4 network, many users were able to use somehow.

Address policy of IPv6

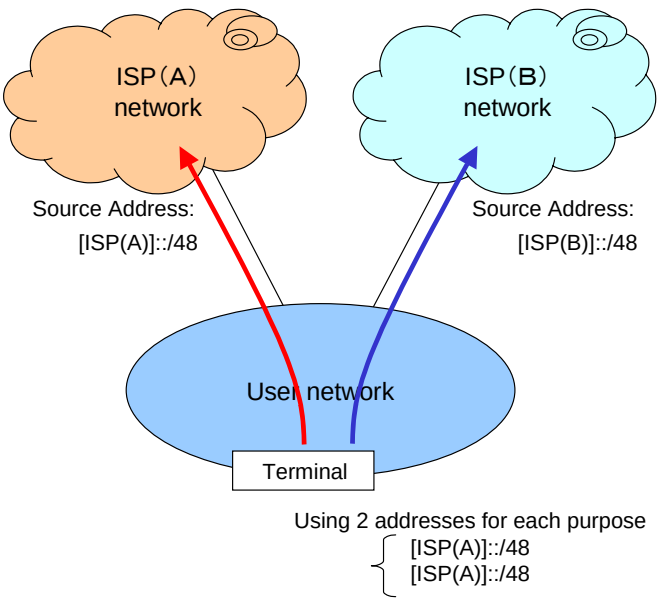
It is emphasized to aggregate paths for routing, so addresses are controlled in a hierarchy (tree) structure. All general users acquire addresses from unique ISP.

→More than 2 kinds of paths don't occur as a basic rule.

Issues

Multi prefix is allocated to each terminal and Source Address Selection is used to handle. Intellectual address selection algorithm is required for the terminal, and it is difficult to process the situation when an ISP line has trouble.

When punching hole is set on the ISP side, path information increases.



Network access control

It is expected that various kinds of equipment are connected to the network under IPv6 network.

Member PC, printer, non-member PC/PDA, white board, copy machine, lighting, air conditioner, sensor, monitoring camera, TV….

There will be needs:

To set access control on different levels for each equipment.

Not to control all equipment at the same level.

Solutions

Some segments shall be made using VLAN and equipment shall be connected to appropriate segments using IEEE802.1x authentication. Access limitation shall be set for each segment (→Refer to Security Guideline: G-3).

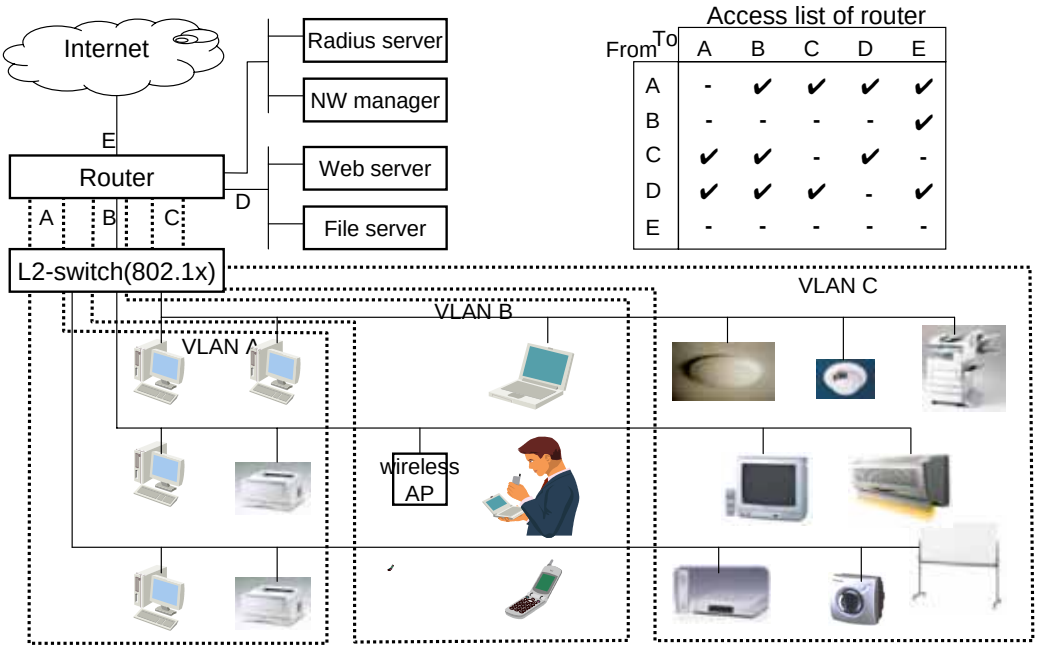
<Example of access policy>

Member PC: All accesses are permitted

Other PC: Only limited accesses are permitted (guest account is used)

Other equipment: Only internal access is permitted

<Concept of access control using IEEE802.1x and VLAN>



Other issues for IPv6 distribution period (excluding matters related to security)

Base for provision of IPv6 service

Not only ISP but also IDC and wholesaler need to support IPv6.

Address re-numbering

Address re-numbering shall occur in the cases shown below.

- When switching from IPv4 to IPv4/IPv6 dual stack under the line connection contract with ISP
- When switching main external connection line from existing network line to new network line

It becomes necessary to consider a measure to minimize man hours required for the change mentioned above.

Various application relations

- DNS
  DNS discovery, DNS registration procedure, new naming procedure
- Mail/Web
  Virus checker/contents checker to support IPv6
- Groupware
  Dedicated client software to support IPv6 (including web service)
  Deployment technology to IPv6 for a server (reverse proxy, translator, etc.)
- File sharing
  Name, signaling, security assurance
- Market place
  Various dedicated software to support IPv6

Investigation Members

Suzuki (Hitachi)
Tachibana (Aniani.com)
Tatsuki (NEC)
Tokushige (NTT Communications)
Nakai (NTT Communications)
Nakahara (NEC)
Nishida (Ricoh)
Shirota (Hitachi)
Hashimoto (MRI)
Hiromi (Intec NetCore, Inc.)
Yamazaki (NTT Communications)
Yamamoto (NTT East Japan)
Yoshioka (Toyota IT Development Center)

Revision of this Guideline

This guideline will incorporate revisions occasionally by the DP-WG.
History of major changes is shown below.

May, 2004: Initial version

March, 2005: Revised version

The changes shown below are incorporated along with establishment of Security SWG.

Section 5 “Security model” is deleted.
Destination to quote Security Guideline is added in the description related to security.
Information in Clause 2.1 “Service/equipment that supports IPv6” is updated.
Information of Clause 2.1 “Acquisition of IPv6 global address” is added.
Contents of Clause 2.2 “IPv6 introduction along with introduction of new application” are updated and added.
Contents of Section 3 “Independent integration type: pattern A” are updated.
Section 6 Issues related to “DNS” is added.