2005 Version
IPv6 Deployment Guideline

Home Segment

March 2005

IPv6 Promotion Council of Japan
DP-WG Home SWG

Table of Contents

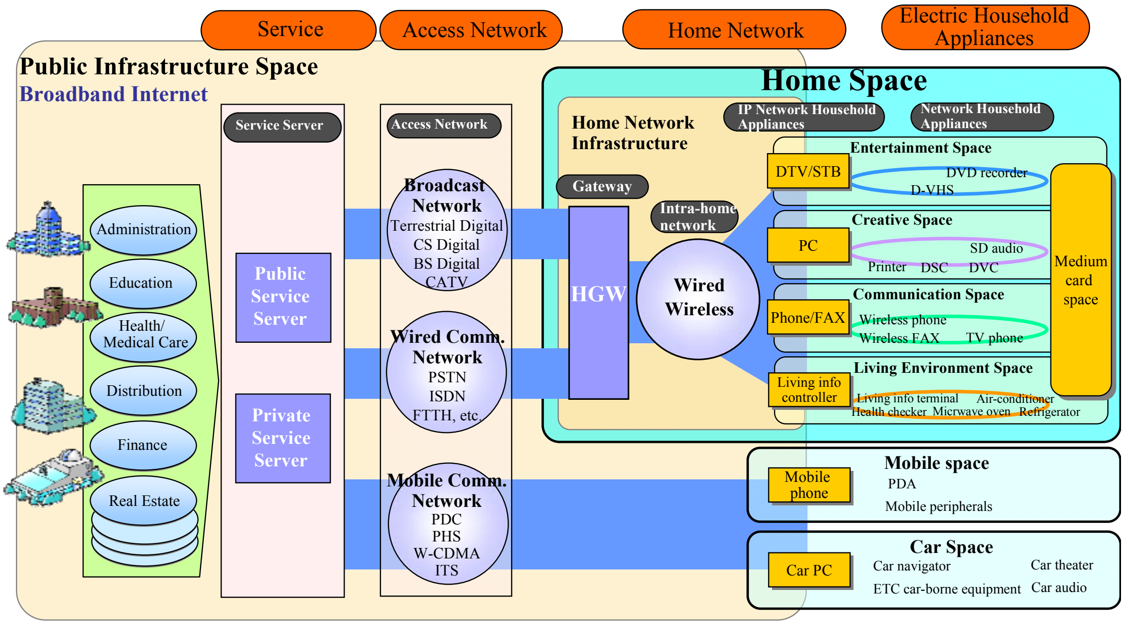
1. Segment Features

Overall Picture

A home network is expected to comprise a variety of media, protocols and equipment components.

As far as the services offered through the Internet, including public ones, are concerned, their diversification will make further and further progress so that the information will be delivered to homes by way of terrestrial digital broadcasting, satellite broadcasting, ADSL, optical fiber, wireless access technology, mobile communications and so on. Even in the home, two or more transmission technologies either wired or wireless may be sometimes used properly to establish a linkage among a set top box, AV household appliances, white goods, PCs, telephone sets and so on.

A wide diversity of media, protocols and equipment are expected to compose a home network.



More specifically, a home gateway (household router) undertakes a connection between Internet access and home networks. Intra-home network equipment has its space classified by objective and connected device into spaces, such as entertainment, creative, communication and living environment. In each group of the equipment composing each space, various protocols (IEEE1394, USB, ECHONET, etc.) are used. In some cases, moreover, each equipment group may have the equipment for conversion between IP and individual protocols (IP network household appliance). Initially, many IP network household appliances may employ a protocol compatible with the network other than IP. In the future, however, non-IP equipment is expected to change progressively over to IP.

Features of Home Segment

From the present to the future, the home segment may well be considered featured as follows:

- **Network configuration and working equipment vary from home to home**
  Especially in the future, a home network is expected to go on having an increasing number of not only PCs but also non-PC equipment (white goods and AV equipment).
- **Person able to manage the network is unavailable**
  The home user could not be expected to carry out setting in detail. It is likely that the home network will continue being used on a default basis or without being reset once set up In addition, there are possibilities that the equipment emerging from now on, especially electric household appliances, may not have an interface for setting.
- **Use ISP connection services**
  ISP is connected in a variety of forms in the home. Nevertheless, a home network is assumed to have one subnetwork. Though segmented into wired and wireless LANs, the home network uses ISP services as one subnetwork on an overall basis.

This guideline is intended to study a deployment of the home segment, covering the IP-terminating equipment while putting the changeover of non-IP equipment (ECHONET and IEEE1394) to IPv6 out of scope hereof. In other words, it is assumed that non-IP equipment should be connected by way of an IP appliance.

Classification of Players

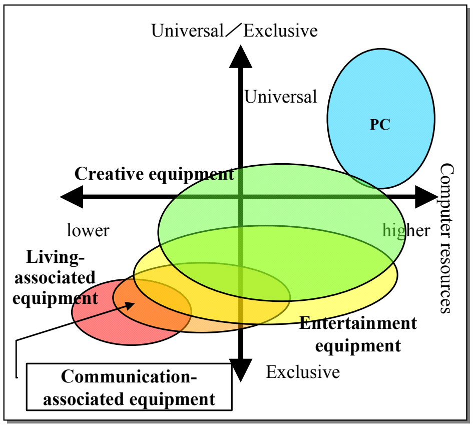
Now, the term, “Player,” is to be introduced here. The term, “Player,” as used herein, means a provider of the products and services used in the home. The reader of the present Guideline should be a player anyway. More specifically, an end-equipment provider, a network equipment provider, a communication network provider and a service provider are to fall in a range of “Players” as defined herein.

End Equipment Provider

The existing first player is an end equipment provider. The term, “end equipment,” means the terminal equipment that should finally connect to the network. Existing mixedly in an intra-home network are various types of equipment, including but not being limited to, entertainment equipment, such as PCs, video recorders, etc., creative equipment, such as digital cameras, etc., living-associated equipment, such as air-conditioners, etc., and communication-related equipment, such as telephone sets, etc.

Such equipment may be described in two categories by form of using the network: one is the equipment to be used with the lead taken by the user and the other used by the service provider. From a computer resource size point of view, the equipment may be divided into three: small-sized built-in type, large-sized built-in type and PC.

- End equipment means
  - PC,
  - Entertainment equipment,
  - Creative equipment,
  - Living-associated equipment, and
  - Communication equipment.
- Various types of equipment exist mixedly
  - Network using form
    - Use with the lead taken by the user.
    - Service providers employ.
  - Computer resources/equipment diversity
    - Small built-in equipment
    - Large built-in equipment
    - PC



PC

The PC is one of the end equipment. Both hardware and OSs are available in a range of variants, such as AT-compatible machines, Macintosh and so on. The PC is featured by the computer resource volume abundantly available. It has a product service life of about three years and a potential of becoming the center of a home network. Especially, a PC, which could not be described properly within the framework of an existing PC, does exist. A debut has been already made by such PC as equipped with the interface called “10 feet UI,” remotely controllable at a more or less distance just like a TV set.

The PC is an appliance, which has few requirements for a network. In other words, the PC is capable of coping flexibly with any network.

Entertainment Equipment

Entertainment equipment includes such appliances as TV sets, HDD (video) recorders, component stereo systems, STBs, various types of tuners, game machines, etc.

Computer resources have their volume diversified from product to product and could not be expressed unconditionally. Game machines, for example, have a large volume of computer resources while TV sets have a little. A game machine usually has a product service life of 3 thru 10 years.

It is one of the entertainment equipment's features that a machine is often provided with a user interface. In many cases, the user interface is often equipped with both input and output systems. The entertainment equipment may be sometimes provided with a user interface controllable by way of a network.

Various problems involved in the management of contents are seriously inherent to the entertainment equipment, trading off its convenience.

In terms of the requirements for a network, the entertainment equipment should show a low delay and should have an appropriate band (several Mbps, a level enough to distribute an MPEG2 class but an HD class in the future).

Creative Equipment

PC peripherals, digital cameras, digital video cameras and the like may be classified as creative equipment.

A volume of computer resources are available in the creative equipment, which, however, has a product service life of 3 thru 5 years generally. Most of the creative equipment allows for an equipment design on the assumption that it is connected to and operates in collaboration with a PC. Nevertheless, the creative equipment may have a non-PC-operated design for its sales feature.

How the user interface should designed depends upon the concept of an individual product. It may be envisaged so that the equipment can be operated either with a PC or independently (cooperating with a digital camera, printer or the like).

For network requirements, the creative equipment is called upon to provide positive connectivity. In addition, it is required to have an appropriate band (several Mbps, resorting to the working data traffic).

Living-associated Equipment

The living-associated equipment includes white goods or electric household appliances and living sensors (electric appliance operation sensor, pressure sensor, light sensor, etc.). For features, the living-associated equipment has a computer resource volume limited in a great measure (in the world of kilobytes) with a product service life of 5 years or more. In some cases, it may not have a user interface, or even if any, very poor (e.g., 2 buttons plus 1 LED or the like).

As far as such equipment is concerned, the user may continue to have consciousness of the equipment as one of electric household appliance components. The vendor hopes that such consciousness should be implanted in the user. The feeling is just like, "Plug its power cable in a power outlet and the equipment will operate."

The living-associated equipment includes an air-conditioner, a cooking appliance, a water heater and the like, all of which might physically injure the user or endanger the life in the event of their malfunctioning. A burglar alarm sensor is included also in the living-associated equipment, involving a criminal event. And it may be practically used as built in a building, too.

From the viewpoint as referred to above, the living-associated equipment calls upon the network to have secure connectivity and to attain the integrity of data. If possible, moreover, it is required to have the concealability of communications.

Network Equipment Provider

It is the network equipment provider that could be taken up as player next to the end equipment provider. The term, "network equipment," as used herein, means the "equipment except for the end nodes composing an intra-home network." These may be subdivided by layer under charge.

The equipment up to Layer 2 includes an xDSL modem, an optical medium converter, etc. The equipment of Layer 3 and above includes a router, etc. And they are combined into a composite product comprising an xDSL modem + a router + an IP telephony.

Network Equipment of Layer 2 and below:

The network equipment of Layer 2 and below may be divided by application into equipment for isolated houses and for collective housing and intra-home appliances.

The network equipment for a detached house (equipment to connect the home with the exterior) includes an ADSL modem, an optical medium converter and a cable modem (bridge type).

For features, the network equipment of Layer 2 and below is generally leased by an access undertaking or from an ISP. ADSL modems, optical medium converters and cable modems, all to be interconnected, are generally available as designated product. Such equipment has media converted between WAN and Ethernet.

The equipment for collective housing includes an Ethernet switch (for inter-home division), VDSL concentrator, and home PNA switch.

For features, the equipment of Layer 2 and below is considered to have a function of combining two or more media and data link technologies. And it is expected to provide us with a function of connecting a wireless LAN access point (802.3, 802.11), a Bluetooth access point (802.3, Bluetooth), a small-power wireless (Small Power Wireless 802.3), electric light wiring, power line, TV antenna coaxial cable, etc. They may be provided in a building as its ancillaries, too in some cases.

A number of subscriber lines are intensively provided in the equipment while it is normally inhibiting subscribers from communicating directly to each other.

The intra-home equipment includes an Ethernet switch (for intra-home use), wireless LAN access point, Bluetooth access point and so on.

Network Equipment of Layer 3 and above

The network equipment at this level includes a router and an authentication server (installed in collective housing).

The router secures a lowest limit of security with NAPT. In this case, the network equipment may be protected to some extent against an attack from the exterior unless the server is open to the public. It is the model in which the router serves as a security boundary. There is a trend for security features, such as a firewall and a simplified IDS, to be generally mounted more and more. Some products have emerged partially, allowing for a virus check and updating a pattern. Nevertheless, it may be safely said that they have still remained unprotected against a pest or worm, such as, “Trojan Horse” and spyware.

As the features mounted in the router, VPN and Mobile IP (Home Agent) have come to show a higher and higher level of demand.

To implement IPv6 in a network, a router falling in a price range of more 30 thousand yen has been forerunning, first of all. A budget model priced at ten thousand yen or less has encountered with difficulties in getting more popular unless specific advantages and use scenes have been established, considering that development expenses have been being strained.

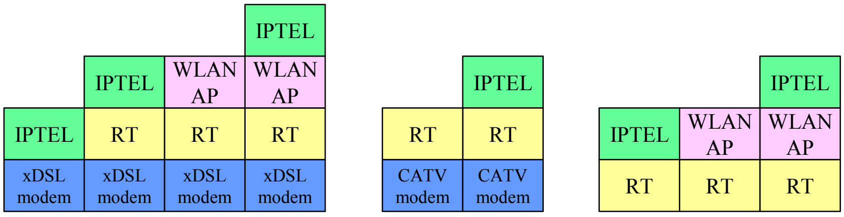
The IPv6 services currently available have their methodology vary from provider to provider. Consequently, a provider-specified router is employed. The authentication server installed in collective housing may require a consensus of the residents for its changeover to IPv6.

Composite Equipment

Composite equipment has come to be widely employed since it permits multiple functions to be provided in a simple configuration. It is a form relatively readily acceptable to the user. From the viewpoint of popularizing the IPv6, the composite equipment should be desirably changed over to IPv6. It may be safely pointed out, however, that the equipment of this type, if equipped with a modem and IP telephony, need often employ an access provider-specified product or ISP- designated. In addition, there is a product whose specific services are limited to an xDSL modem plus IP telephony or the like. Products of this type are significantly influential over a home network configuration.

- Composite Equipment

【Example】



【Features】

- Generally employed owing to the demand for a multifunctional but simple configuration:
  - Relatively readily acceptable to the user.
  - Changeover to IPv6 is expected to popularize IPv6.
- A modem and IP telephony, if mounted, have their models often designated by the access provider or in ISP (to assure connectivity).
- Some existing products have their specific services limited to an xDSLmodem + IP telephony or the like.
- Significantly influential over a home network configuration.

Communication Network Provider

For another player, the communication network provider is available. The term, as used herein, signifies the undertaking to provide the IPv6/IPv4 network (IPv6/IPv4 connected to the Internet). And two functions are available: one is to provide the ISP core network (providing a function of connecting IPv6/IPv4 to the Internet) and the other to provide an access network (providing a home network with a function of connection to an ISP core network). Exemplar access networks available are as follows:

xDSL, FTTH

Often provided by an access provider (There is a case where ISP may provide this feature.)

CATV

Provided by a CATV undertaking

Wireless LAN

Often provided by a wireless LAN access provider or ISP

Mobile phone/PHS

Provided by a mobile phone/PHS communication carrier

IPv6 tunnel connection

Provided often by ISP

Usually, an ISP core network and an access network are often set up separately. As seen in CATV Internet services, however, an identical network provider may set up both ISP core and access networks.

Access networks are available in two types: site type and host type.

The site type means a home network formed as a site. CPE (router) of Layer 3 exists in the home network of this type.

The host type means a formation where a home network is connected directly with an access network on a Layer-3 basis. Layer-2 CPE (modem) exists in the home network of this type.

A communication service provider normally provides a home with the following network functions:

Addressing:

Distributes to a home network an address required for the network to connect with the Internet.

Routing:

Routes a packet for IPv6 and IPv4 Internet connections.

Normally, routes a packet fixedly to the ISP on a default basis (standard routing normally established in the network equipment → a tact understanding)

The presupposition above, however, may crumble due to multi-homing or the like.

The communication network provider has a significant impact on the formation of a home network. They are decisive of the following points, for example: Which is the WAN connection method, site type or host type? Is one address only delivered or two or more deliverable? Is the address global or private? Is the number of machines connectable at a time limited to one or are two or more acceptable by way of NAT?

The communication network provider, furthermore, is also influential over a development of equipment. For example, they are decisive of whether or not NAT Traversal be available (whether or not NAT be provided) and of whether or not an end node be provided with security mechanisms (whether or not security mechanisms be provided). The communication network provider is influential over the functions implemented especially in the network equipment (CPE).

Service Provider

On the home network infrastructure as referred to above, a wide variety of network services could be envisaged to be deployed over each equipment group. The following examples are conceivable:

《PC》

Internet applications conventionally available (Web, FTP, Mail, ...)
Services for other equipment are also available

《Entertainment Equipment》
Content distribution, network games and video record booking

《Living Equipment》
Home security, living aids, welfare and remote maintenance

《Communication Equipment》
IP telephony and TV telephony

《Creative Equipment》
Printing and video/music editing

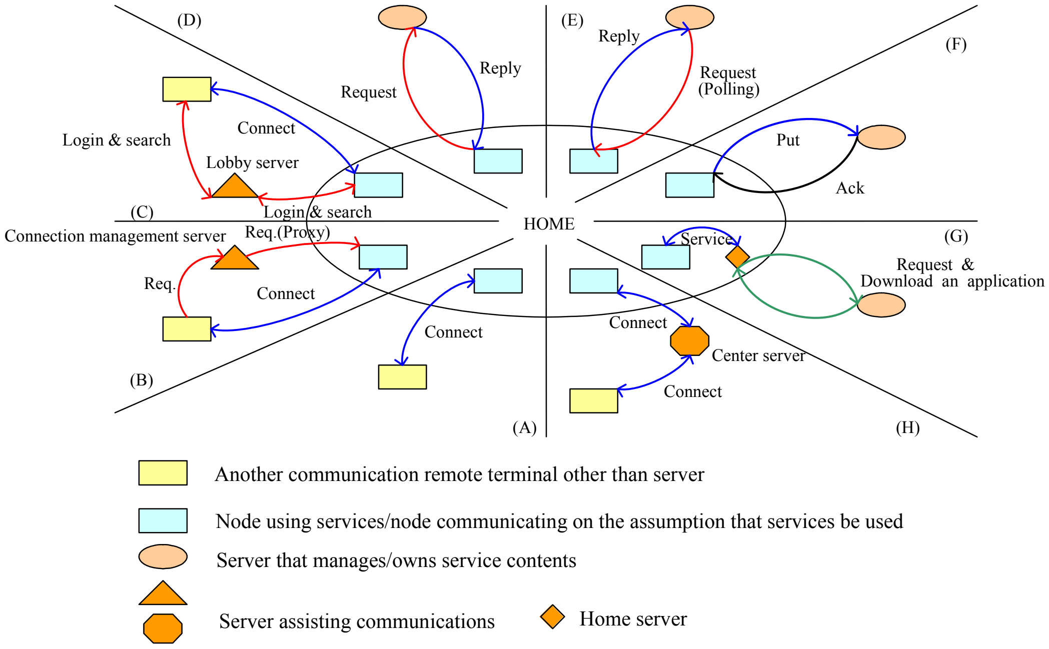
Such “services” as referred to above are closely related with the end equipment. An end device essential to a specific service does exist indeed while some applications and systems are also available subject to the presumption that they must cooperate with a server and/or an intra-home terminal. These services, furthermore, are conceivable in two categories: one is offered by an end equipment provider and the other by the one other than the end equipment provider. These services’ requirements for a network vary with the type of a service and with the form in which the service is rendered. There are possibilities that the services common to ASP may be available (with B2B2C applied to cooperate with another portal site, too). Exemplar cases are, for instance, charging management, user authentication management, security management, job management and so on.

These services may be classified by communication form as follows:

(A) Completely P2P type
(B) P2P + Connection Management Server type
(C) P2P + Lobby Server type
(D) Client/Server type
(E) Client/Server (ASP Poling) type
(F) Client/Server (Client Post) type
(G) Home Server type
(H) Via Center Server type

A method of classifying services by their type or requirement for a network is also conceivable. Such method, however, is considered incapable of covering all the services diversified more and more. A classification by communication form, therefore, has applied here.

■ A Graphically Shown Classification of Services by Form of Communications



(D)
(E)
(F)
(C)
(G)
(B)
(A)
(H)
HOME
Request
Reply
Reply
Request (Polling)
Login & search
Connect
Lobby server
Login & search
Put
Ack
Connection management server
Req.(Proxy)
Service
Req.
Connect
Request & Download an application
Connect
Connect
Center server
Connect
Another communication remote terminal other than server
Node using services/node communicating on the assumption that services be used
Server that manages/owns service contents
Server assisting communications
Home server

Let's see various forms of communications by service in detail here.

(A) Completely P2P type

This is a formation of communications, in which an end node finds out a remote station directly to perform the P2P communications. DNS or a service discovery protocol is used to find out the remote station.

Exemplar Uses: self-contained file exchange software and intra-home cooperation.

Service Provider's Role: To provide application software.

Traffic: Starting point – P2P participant node, Ending point - P2P participant node, and Route – direct communication.

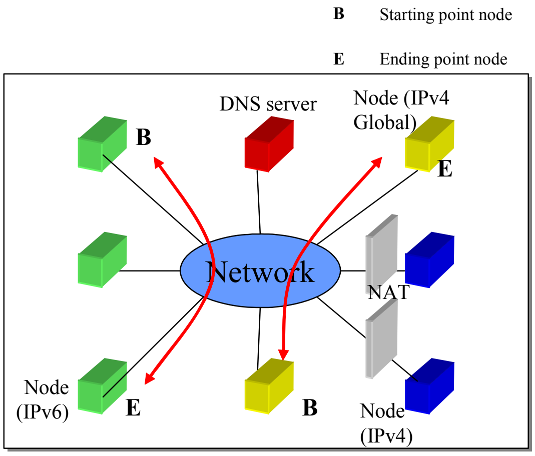
Features: Free from an overconcentration in one station because no server is employed, though dependent upon a node.

Miscellaneous: Necessary to set a port forward, DMZ and the like so that the IPv4 node behind NAT can communicate.

- Communication Forms in detail

  (A) Completely P2P Type

  - A form of communications in which an end node directly finds out a remote terminal and performs P2P communications.
    - To find out the remote terminal, use DNS or service discovery protocol.
  - Exemplar Uses
    - Self-contained file exchange software
    - Intra-home cooperation
  - Service provider's role
    - Provide application software
  - Traffic
    - Starting point:P2P participant node
    - Ending point: P2P participant node
    - Route: direct communication
    - Features
      - Not concentrated in one station because there is no server, through depending upon a node
  - Miscellaneous
    - Necessary to set a port forward, DMZ, etc. so that the IPv4 node behind NAT may communicate.



(B) P2P +Connection Management Server type

This is a form of P2P communications performed, with an end node discovering a communicating remote station by way of the connection management server where communication policies and connections are limited.

Exemplar Uses: IP telephony and SIP-based applications whose connections are managed.

Service Provider's Role: Provide application software. Operate connection management server.

Traffic: Starting point - P2P participant node, Ending point - P2P participant node, Route - Via server for initial communications.

Normally, communications are performed directly. Traffic will concentrate in the management server, coupled with an increase in number of nodes.

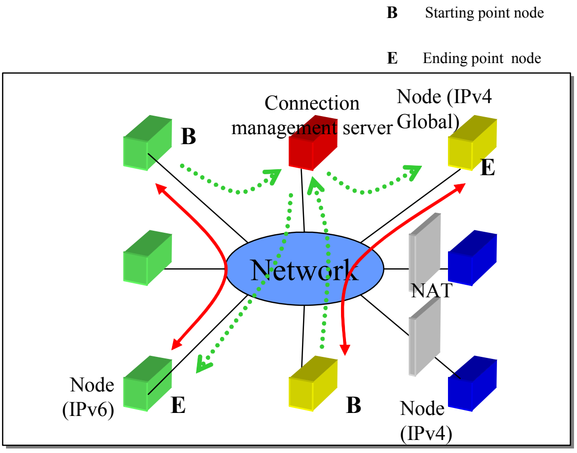
Miscellaneous: Similarly to (A), the NAT issue is found.

- Communication Forms in Detail

  (B) P2P ＋ connection management server type

  - Form in which P2P comms are performed, with comm remote terminal discovered by end node via comm policy and connection management server limiting comms.
  - Exemplar Uses
    - IP telephony
    - SIP-based application connected and managed
  - Service Provider's Role
    - Provide application software
    - Operate connection management server
  - Traffic
    - Starting point P2P participant node
    - Ending point P2P participant node
    - Route via server for initial comm.

      direct for normal comm.
    - Feature
      - Traffic concentrated on management server, coupled with an increase in number of nodes
  - Miscellaneous
    - NAT issue remains unchanged.



(C) P2P + Lobby Server type

This is a form of P2P communications performed, with a remote station to communicate with discovered by way of the lobby server that has presence information. It differs from (B) in the sense that neither does a policy apply nor is a connection limited.

Exemplar Uses: P2P type Internet game, and broadcast type application (P2P with a list of broadcasting stations taken for the starting point).

Service Provider’s Role : Provide application software and operate a lobby server.

Traffic: Starting point - P2P participant node, Ending point - P2P participant node, Route - via server for initial communications.

Normally, communications are performed directly.

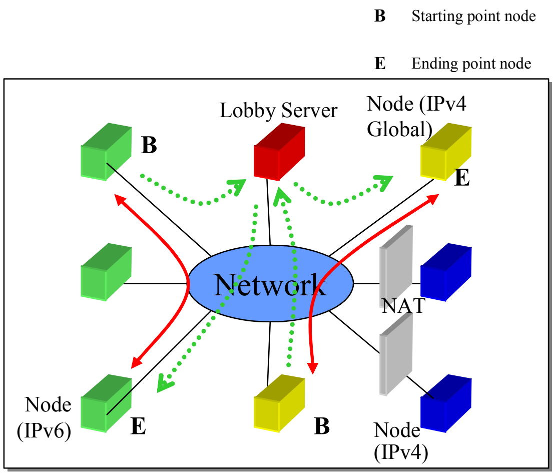
Feature: Refer to (B).

Miscellaneous: For the NAT issue, refer to (A).

- Communication Forms in Detail

  (C) P2P + lobby server type

  - Form of comms in which P2P comms are performed, with comm remote terminal discovered via Lobby Server holding presence information.
    - This type differs from (B) in the sense that neither does policy apply nor are connections limited.
  - Exemplar Uses
    - P2P type Internet game
    - Broadcast type application (in case of P2P with broadcasting station list as starting point)
  - Service Provider's Role
    - Provide application software
    - Operate lobby server
  - Traffic
    - Starting point P2P participant node
    - Ending point P2P participant node
    - Route via server for initial comm.
      direct for normal comm.
    - Feature
      - See (B).
  - Miscellaneous
    - NAT issue remains unchanged.



(D) Client/Server type

This is a form of communications, which will function, with a client obtaining certain information from a server.

Exemplar Uses: Existing Internet applications, such as Web, FTP, Mail, etc. Broadcast type application, such as VoD or the like, and C/S type instant message and C/S type Internet games (MMOG, etc.).

Service Provider’s Role : Provide application software. Operate the server.

Traffic: Starting point - Client, Ending point Server, Route - All communications are directed toward the server.

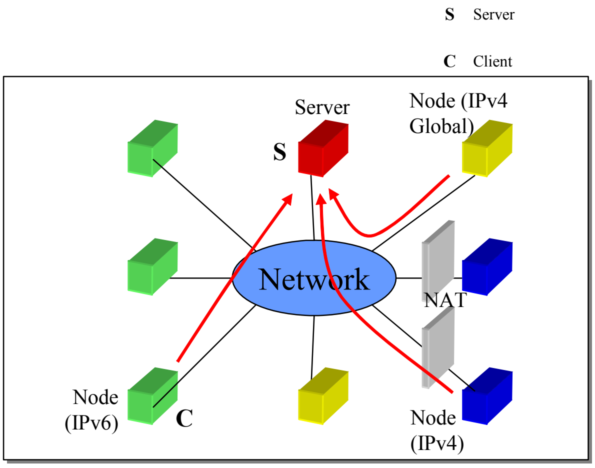
Feature: Traffic concentrates in the server.

Miscellaneous: Usable even behind NAT.

- Communication Forms in Detail

  (D) Client/Server type

  - Form of comms, which will function, with client obtaining certain information from server
  - Exemplar Uses
    - Existing Internet applications, such as Web, FTP, Mail, etc.
    - Broadcast type application, such as VoD or the like
    - C/S type instant message and C/S type Internet game (MMOG, etc.)
  - Service Provider's Role
    - Provide application software.
    - Operate server.
  - Traffic
    - Starting point   Client
    - Ending point   Server
    - Route   All comms are directed toward Server
    - Feature
      - Traffic concentrates on Server.
  - Miscellaneous
    - Usable even behind NAT



(E) Client/Server (ASP Polling) type

This is a form of communications, which will function when an ASP Client obtains certain information from an intra-home server.

Exemplar Uses: Telemetering and remote monitoring and remote maintenance (operation periodically checked by ASP).

Service Provider's Role: Sell applicable equipment. Provide applications. Operate nodes in ASP and arrange in order/manage information collected.

Traffic: Starting point - ASP (Client), Ending point - Intra-home (server), Route - All comms start from ASP.

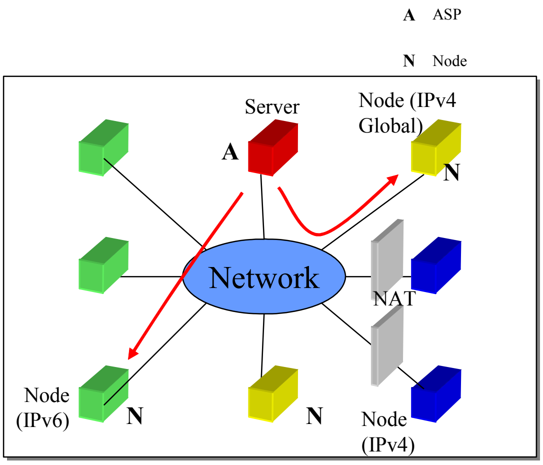
Feature: ASP capable of controlling traffic.

Miscellaneous: Incapable of reaching behind NAT.

- Communication Forms in Detail

(E) Client/Server (ASP polling) type

- From of comms, which will function, with ASP Client obtaining certain information from intra-home server.
- Exemplar Uses
  - Telemetering and remote monitoring
  - Remote maintenance (operation periodically checked by ASP)
- Service Provider's Role
  - Sell applicable equipment.
  - Provide applications.
  - Operate nodes in ASP and arrange in order/manage information collected.
- Traffic
  - Starting point ASP (Client)
  - Ending point Intra-home (server)
  - Route All comms start from ASP.
  - Feature
    - ASP capable of controlling traffic
- Miscellaneous
  - Incapable of reaching behind NAT



(F) Client/Server (Client Post) type

This is a form of communications, which will function when an intra-home client notifies the ASP server of certain information. It differs from (D) in the sense the Client notifies the Server of information.

Exemplar Uses: Remote monitoring (Images being monitored, etc, are periodically uploaded), remote maintenance (information periodically notified by sensor nodes) and home security (information notified, based on events).

Service Provider’s Role: Sell applicable equipment. Provide applications. Operate nodes in ASP and arrange in order/manage information collected.

Traffic: Starting point - intra-home, Ending point - ASP, Route - All comms concentrate in ASP.

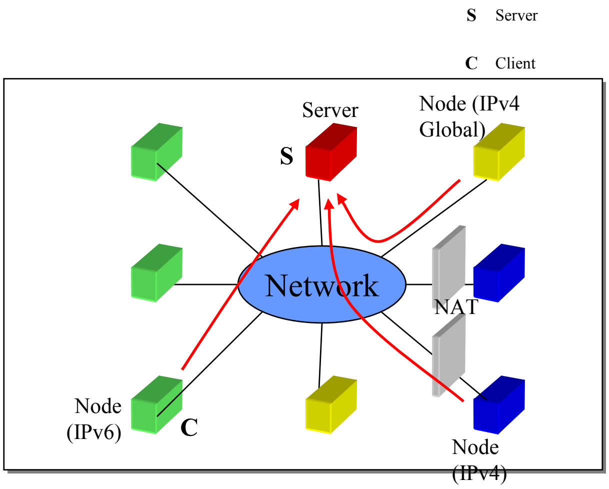
Feature: Often uncontrollable by ASP (dependent upon equipment).

Miscellaneous Usable even behind NAT.

- Communication Forms in Detail

(F) Client/Server (client post) type

- Form of comms, which will function, with intra-home client notifying ASP server of certain information
  - This type differs from (D) in the sense that Client notifies Server of information
- Exemplar Uses
  - Remote monitoring (Images being monitored, etc, are periodically uploaded)
  - Remote maintenance (information periodically notified by sensor nodes)
  - Home security (information notified, based on events)
- Service Provider's Role
  - Sell applicable equipment.
  - Provide applications
  - Operate nodes in ASP and arrange in order/manage information collected
- Traffic
  - Starting point intra-home
Ending point ASP
  - Route All comms concentrate in ASP
  - Feature
    - Often uncontrollable by ASP (dependent upon equipment)
- Miscellaneous Usable even behind NAT



(G) Home Server type

This is a form of communications composed of the intra-home communications invoked, with application being run after downloaded from ASP. It may be taken for a composite model composed of (D) and (A).

Exemplar Uses: Not existing under the current situation?

Service Provider's Role: Provide applications being downloaded and at linked nodes. Sell equipment applicable (as running platform).

Traffic: Starting point - intra-home (as downloaded), Ending point - ASP (as downloaded), Route - Normally closed in the home though concentrated in server only as downloaded

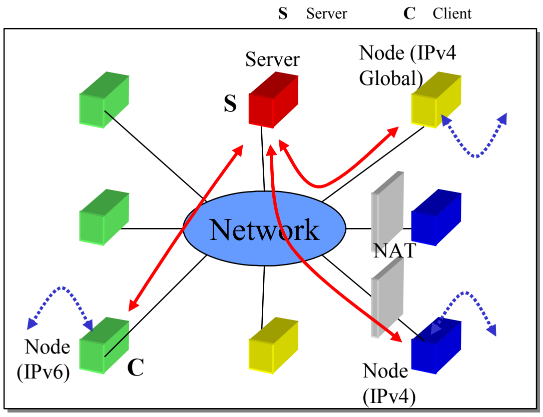
Feature: Possibly downloading may rapidly concentrate when upgrading version.

Miscellaneous: Usable even behind NAT.

- Communication Forms in Detail

(G) Home server type

- Form of intra-home comms invoked, with application being run after downloaded from ASP
  - This may be taken for composite model composed of (D) and (A).
- Exemplar Uses
  - Not existing under the current situation?
- Service Provider's Role
  - Provide applications being downloaded and at linked nodes.
  - Sell equipment applicable (as execution platform)
- Traffic
  - Starting point intra-home (as downloaded)
  - Ending point ASP (as downloaded)
  - Route Normally closed in the home though concentrated in server only as downloaded
  - Feature
    - Possibly downloading may rapidly concentrate when upgrading version
- Miscellaneous Usable even behind NAT



(H) Via Center Server type

This is a form of communications, all of which are performed via the Center Server.

Exemplar Uses: Provide some remote access services and additional functions, such as virus check, etc. for communication route.

Service Provider's Role: Sell application software. Operate the server.

Traffic: Starting point - intra-home, Ending point - Server (essentially opposing node), Route - All traffic does not fail to flow via server.

Feature: Traffic will increase rapidly, coupled with an increase in number of users.

Miscellaneous Usable even behind NAT.

Analysis of Current Situation

Statistical Information

According to “a Time-Series of Changes in Number of Internet Connection Service Users, etc.(as of August 2004)” published by the Ministry of Internal Affairs and communications, Internet connection services in Japan are currently used in household as referred to below.

How to connect with Internet

Number of dial-up subscribers: approx. 18.62 million contracts

Direct dial-up through PC (modem) (PSTN)

Dial-up router (ISDN)

Number of subscribers in an environment normally connected to the Internet:

approx. 16.92 million contracts: ADSL (12.55), FTTH (1.6) and CATV (2.77) in million

Number of mobile-phone Internet service subscribers: approx. 71.93 million contracts

(Total number of households in Japan for 2000: approx. 46 million)

Network connection forms

Described here are the forms in which networks for general detached houses and collective housing are connected.

Network for a detached house:

The network in a detached house is featured by its capability of getting a circuit served in from the outside of the house at an individual discretion though costly.

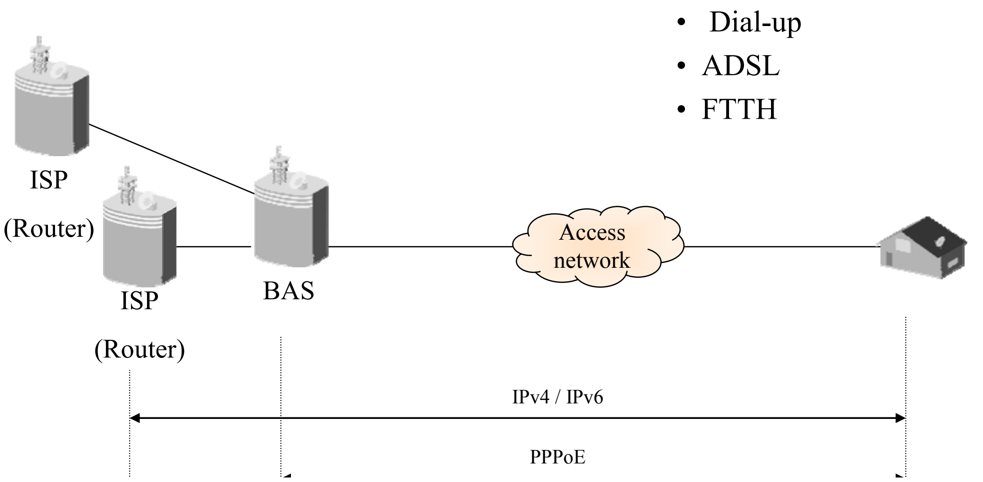
Network for collective housing:

A network for collective housing is available at low cost but requires a consensus among its residents (when newly laying out the network). And it is provided as an infrastructure facility, such as the equipment for the collective housing.

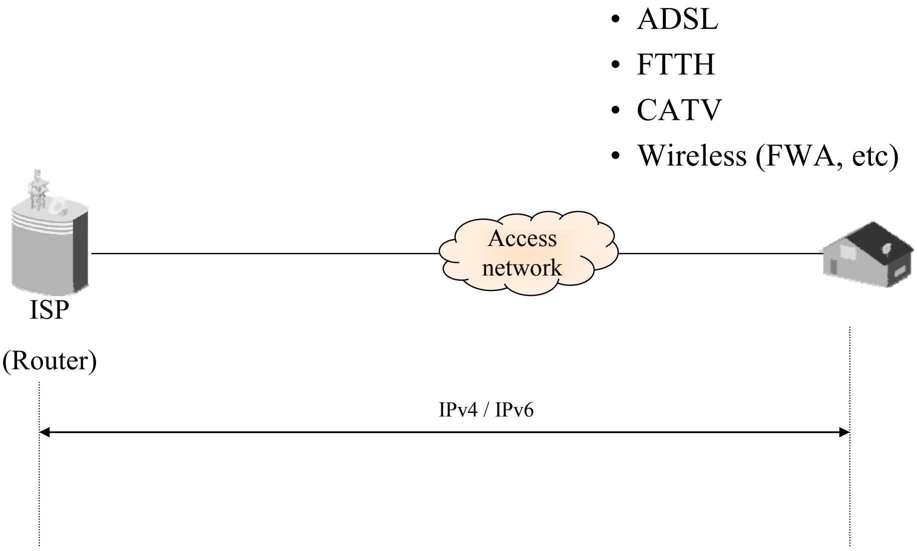
A network in a detached house may be described in two categories: PPP connection type and IP connection type as illustrated below. In the PPP connection type, the PPPoE session is extended so that either IPv4 or IPv6 will be threaded. The IP connection type, on the other hand, provides a simple configuration, in which an access network is connected directly with a router on the ISP side.

■ Form of Network Connections for Detached Houses

Case 1: PPP Connection type



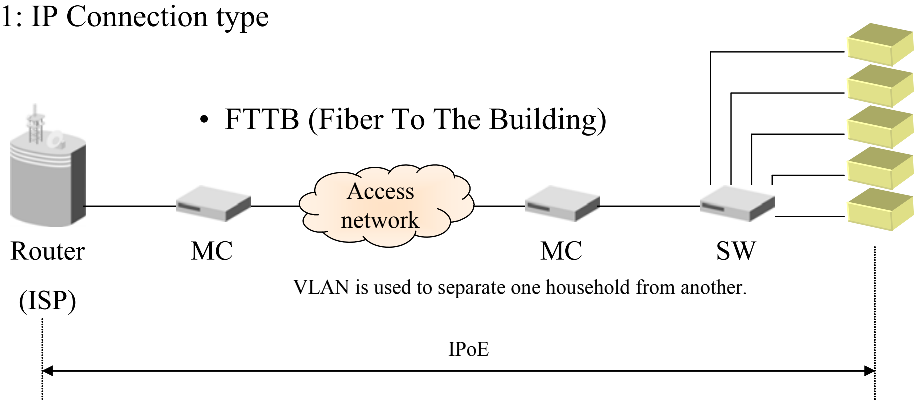
Case 2: IP Connection type



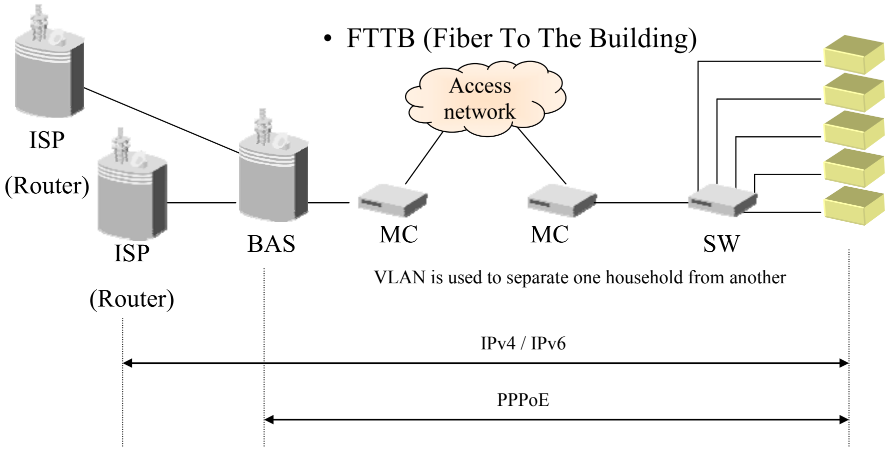
A collective housing network may be also described in two categories by connection: IP connection type and PPP connection type. In either case, a switch is placed in the collective housing and each household is separated with a VLAN so that it cannot communicate directly with another household in the collective housing. In some cases, moreover, an authentication server also serving as router may be installed in the collective housing.

Form of Networks for Collective Housing

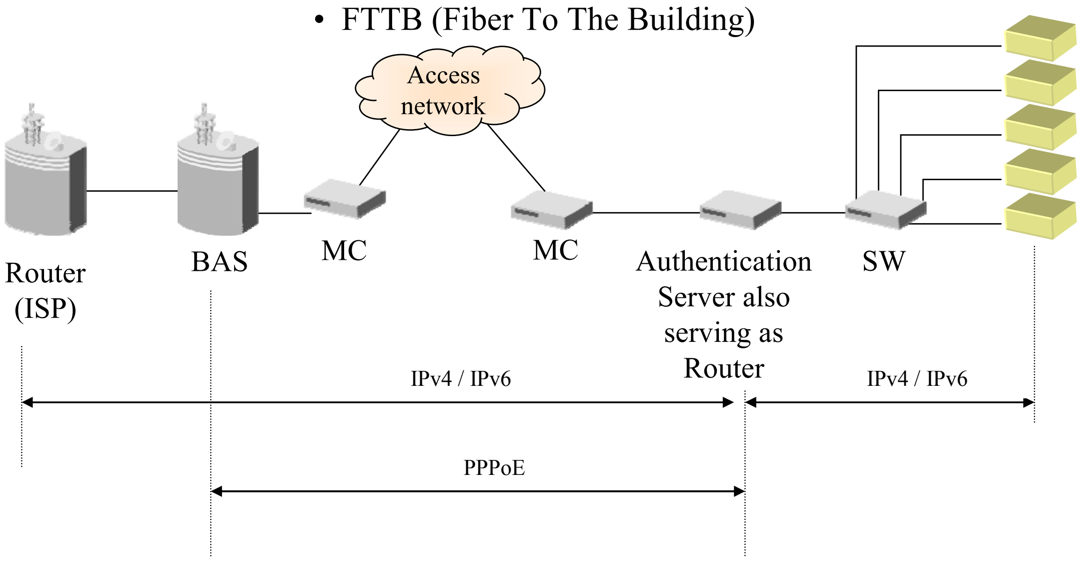
Case 1: IP Connection type


• FTTB (Fiber To The Building)
Access network
Router
(ISP)
MC
MC
SW
VLAN is used to separate one household from another.
IPoE

Case 2: PPPoE Connection type


• FTTB (Fiber To The Building)
Access network
ISP
(Router)
ISP
(Router)
BAS
MC
MC
SW
VLAN is used to separate one household from another
IPv4 / IPv6
PPPoE

Case 3: Collective Housing Authentication Server Installed type

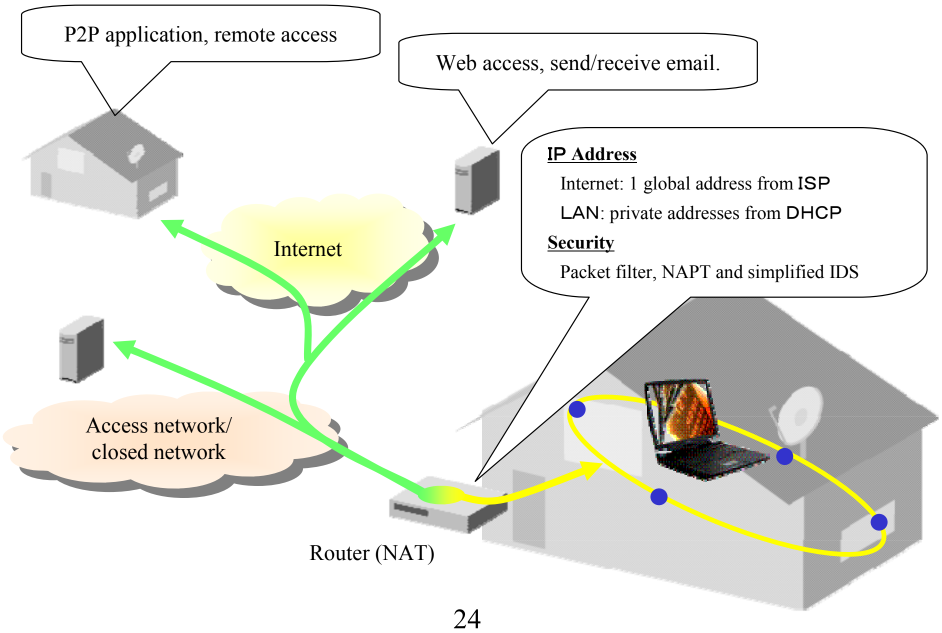


• FTTB (Fiber To The Building)
Access network
Router (ISP)
BAS
MC
MC
Authentication Server also serving as Router
SW
IPv4 / IPv6
IPv4 / IPv6
PPPoE

Typical Example

The IPv4 home network currently available is configured in a typical form as illustrated below. A router is located on the boundary between home and Internet. ISP assigns one global address to the interface to the Internet side and the router's DHCP Server feature assigns private addresses to the interface on the LAN side so that addresses can be exchanged mutually between LAN and Internet (NAT). The home network is making effective use of P2P applications and remote access in addition to basic tools, such as web, FTP, email and so on by way of the Internet. Some access networks are connected to a closed network.

Typical Example of IPv4 Home Network



P2P application, remote access
Web access, send/receive email.
IP Address
Internet: 1 global address from ISP
LAN: private addresses from DHCP
Security
Packet filter, NAPT and simplified IDS
Internet
Access network/ closed network
Router (NAT)

Outline of Intra-home Situations

At present, game machines and AV equipment have come to be used as entertainment equipment in addition to a PC. A network player has emerged, enabling the data on a PC to be played back on a TV set. And compatibility with the DLNA guidelines has made progress. Consequently, the equipment and software, which are capable of cooperating to each other, have begun emerging. As a result, interconnections are going to be available not only from a PC to a non-PC but also between non-PCs to each other so that they can operate cooperatively.

For living-associated equipment, some vendors have released on a trial basis those white goods, which are compatible with a network. These products, however, are considered to have a certain long period of time ahead before coming into general use. Network-compatible cameras and network-applicable sensors have been also released but they have not shown a large quantity sold yet in reality. There are some users really, who are making use of a camera installed in a nursery center or the like.

The creative equipment has not so significantly growing quantitatively while the communication equipment has been rapidly coming into wide use with IP telephony. And it is expected to develop into IP TV telephony.

Intra-home wiring is implemented on both wired and wireless (802.11a/b/g) basis.

For network equipment, the access network terminating devices generally available include a home gateway, a medium converter, a router and so on.

User services include web, email (used in the Client’s position of), messenger systems (using P2P), intra-home email. Web server (used in the Server’s position: by a very limited number of users only), remote video booking (service-in but partially).

As far as security is concerned, a firewall feature in a router (mainly packet filter and NAPT function, but in some cases, stateful packet inspection feature, simplified IDS, etc.), a personal firewall function in a PC (mainly virus check of emails) and ISP-offered services (virus check etc.) are currently available.

The fundamental security, however, is to restrict incoming packets with a packet filter/NAT. It should be noted anyway that most of users are unable to do anything other than default settings.

2. Deployment Scenario in Home Network

Principles of Deployment Scenario in Home Network

Principles of Deployment Model and of Deployment Scenario

The home situations generally seen at present may be summarized into three cases: the first is where two or more machines are connected with a router, the second where a single machine only is connected (on a bridge basis) with a modem (dial-up, ADSL modem and medium converter) and the third where there is neither network nor applicable equipment.

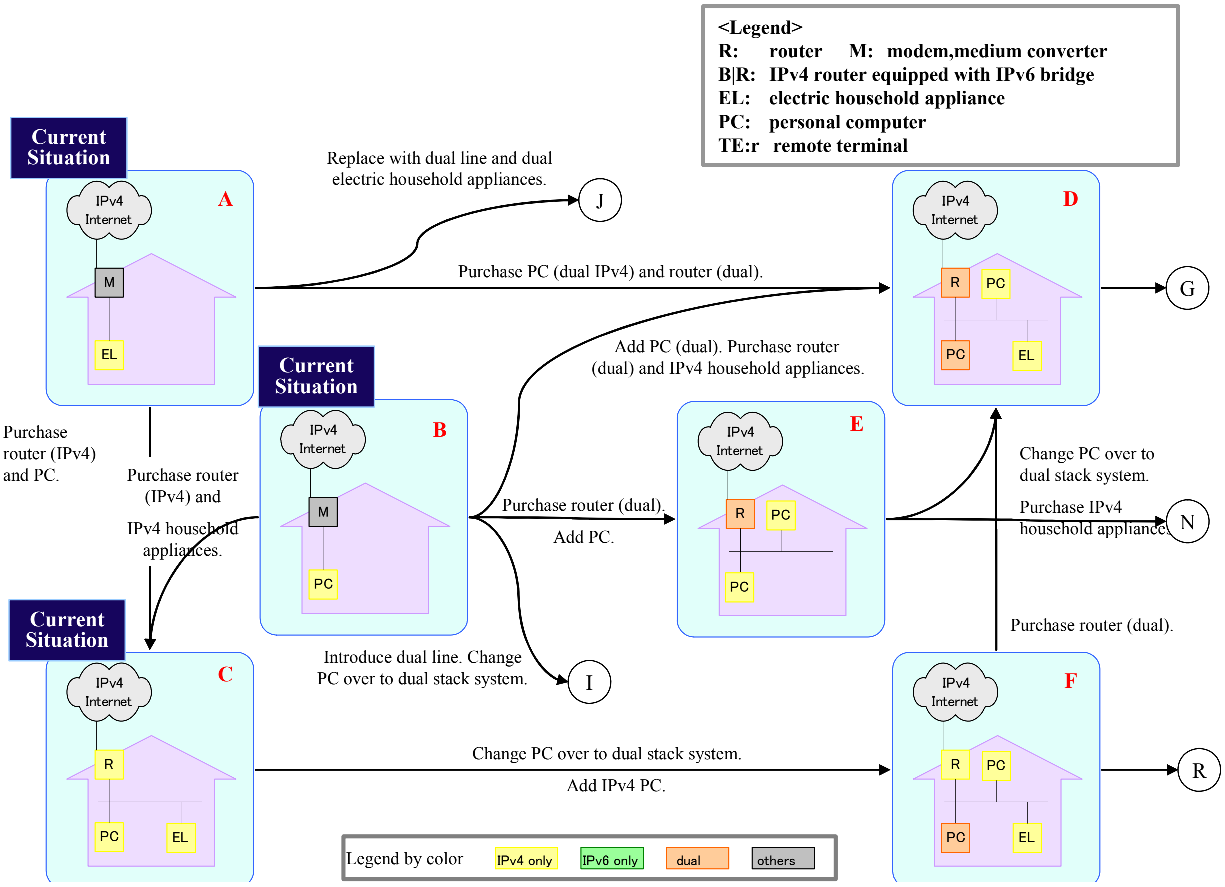
Envisaged here is an IPv6 deployment scenario where a PC and a non-PC mixedly exist. There are a lot of issues common to those in the SOHO segment. It is necessary, however, to take into consideration an environment where nothing but a non-PC does exist, or scenario that we could not expect anywhere other than household.

Envisaged below are the household models that fall in a range of homes currently existing and in the BCP and IPv6 popularization phases. And the issues involved in deployment are to be arranged in order by clarifying the differences between the models.

Deployment Scenario in Home Network (Outline of Deployment Model)

From the current situation of a home network, a deployment process from today to BCP/IPv6 popularization phases might well be summarized into the following three illustrations:

Overview (from Current Situation to BCP)



<Legend>
R: router M: modem,medium converter
B|R: IPv4 router equipped with IPv6 bridge
EL: electric household appliance
PC: personal computer
TE:r remote terminal

Replace with dual line and dual electric household appliances.

Purchase PC (dual IPv4) and router (dual).

Add PC (dual). Purchase router (dual) and IPv4 household appliances.

Purchase router (IPv4) and PC.

Purchase router (IPv4) and IPv4 household appliances.

Purchase router (dual). Add PC.

Introduce dual line. Change PC over to dual stack system.

Change PC over to dual stack system.

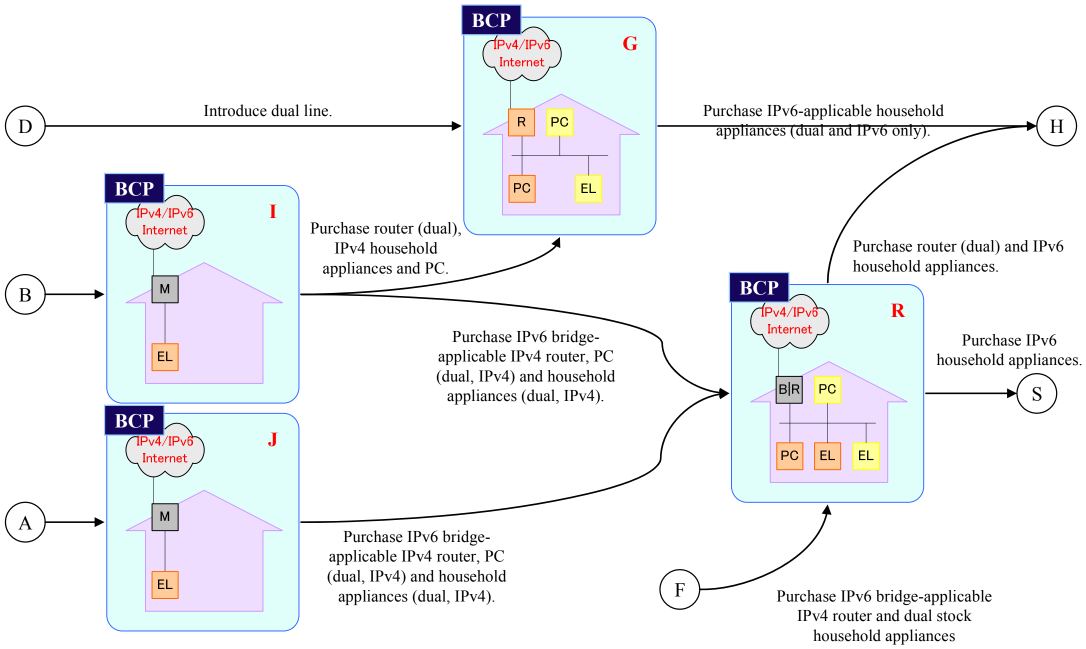
Purchase IPv4 household appliances.

Purchase router (dual).

Change PC over to dual stack system. Add IPv4 PC.

Legend by color: IPv4 only, IPv6 only, dual, others

Overview (BCP)



Introduce dual line.

Purchase IPv6-applicable household appliances (dual and IPv6 only).

Purchase router (dual), IPv4 household appliances and PC.

Purchase IPv6 bridge-applicable IPv4 router, PC (dual, IPv4) and household appliances (dual, IPv4).

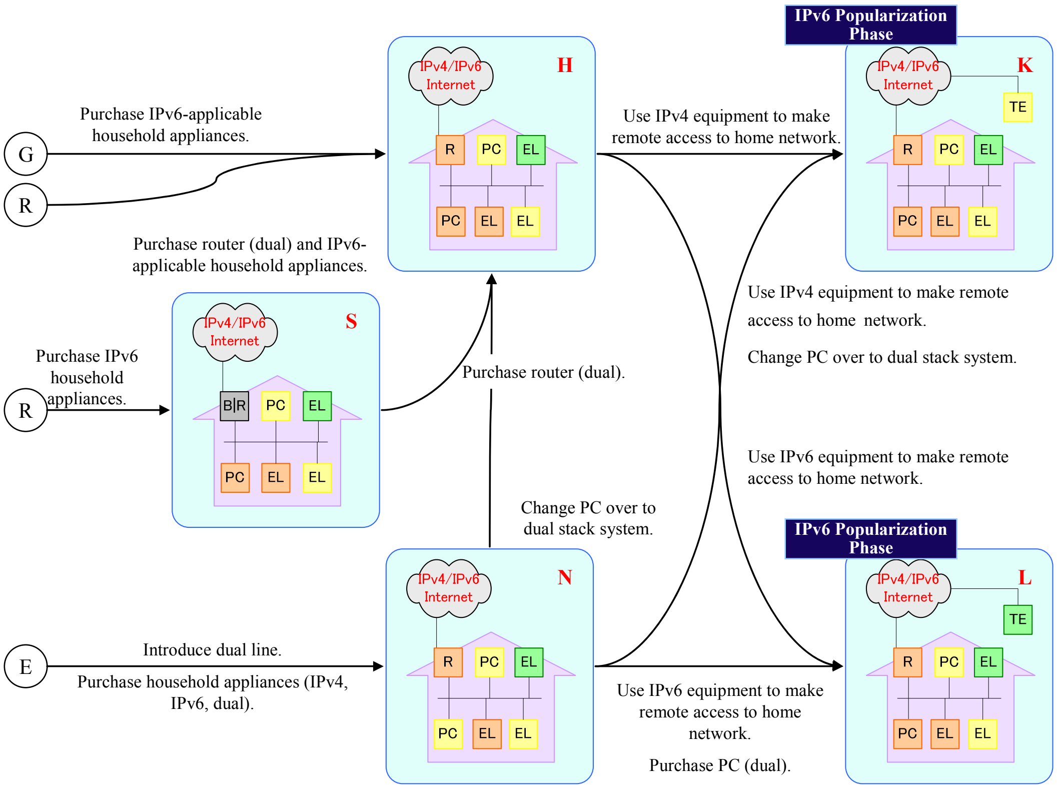
Purchase router (dual) and IPv6 household appliances.

Purchase IPv6 household appliances.

Purchase IPv6 bridge-applicable IPv4 router, PC (dual, IPv4) and household appliances (dual, IPv4).

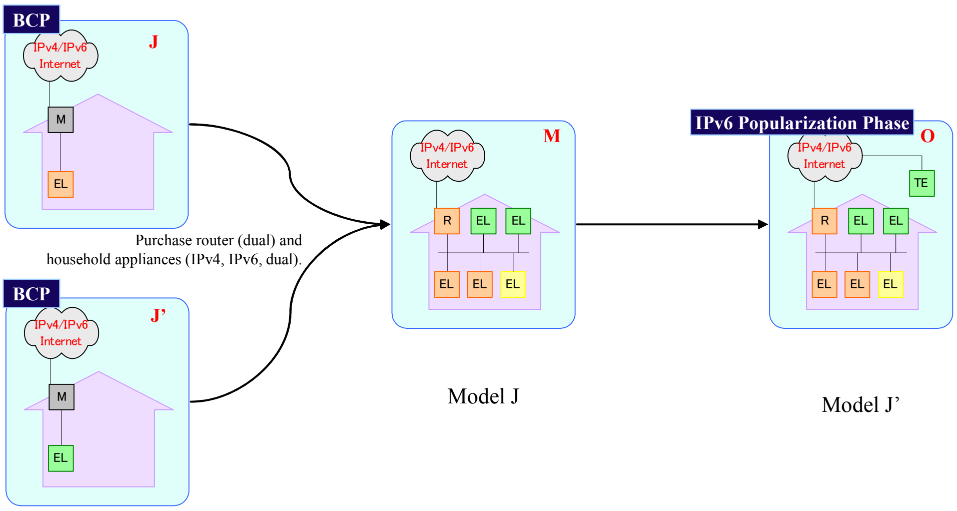
Purchase IPv6 bridge-applicable IPv4 router and dual stack household appliances

Overview (from BCP to IPv6 Popularization)


IPv6 Popularization Phase
IPv6 Popularization Phase
H
K
S
N
L
G
R
R
E
IPv4/IPv6 Internet
R
PC
EL
B|R
TE
Purchase IPv6-applicable household appliances.
Purchase router (dual) and IPv6-applicable household appliances.
Purchase IPv6 household appliances.
Use IPv4 equipment to make remote access to home network.
Purchase router (dual).
Use IPv4 equipment to make remote access to home network.
Change PC over to dual stack system.
Use IPv6 equipment to make remote access to home network.
Change PC over to dual stack system.
Introduce dual line.
Purchase household appliances (IPv4, IPv6, dual).
Use IPv6 equipment to make remote access to home network.
Purchase PC (dual).

A scenario, where the deployment to IPv6 is making progress, coupled with the utilization of non-PCs while making no use of a PC at all, may be envisaged as illustrated below.

Overview (non-PC)


BCP
BCP
IPv6 Popularization Phase
J
J'
M
O
IPv4/IPv6 Internet
M
R
EL
TE
Purchase router (dual) and household appliances (IPv4, IPv6, dual).

Model J

Model J'

Deployment Scenario in Home Network (Studying a Scenario)

Illustrations given above do not cover all models conceivable. It is unnecessary to follow intermediate stages sequentially.

In principle, however, the scenario considered most deployable begins with Models A, B and C (current situation) and goes to Models K and L (IPv6 popularization stage) by way of Model G (BCP). As an instance practically served, moreover, another deployment scenario is also available, where it starts from Models A, B and C and reaches K and L by way of R.

Another scenario that need be taken into consideration for the home segment is for a household without having any PC to make a deployment of J/J'→ M → O by owning electric household appliances and game machines only. In addition, a deployment of P → M/H → K, L and O may be considered available as a development of the case where the home is networked in the interior only.

Each model envisaged is to be defined as itememized below:

- Configuration (access network, point of connection with the Internet and equipment in the home network)
- Working applications (applications used in the home)
- Address architecture (addresses allocated from ISP and assigned to the home in the interior)
- Naming (how to query and register)
- Security measures (encryption, protection against illegal access, virus countermeasures and DoS measures)
- How to set (how to set equipment)

Models Envisaged: Current Situation

For the current situations in the home, the following three models are envisageable:

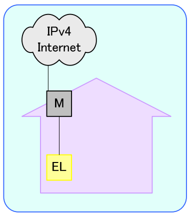
A: Modem/medium converter + non-PC (game machine, HDD recorder, etc.)
This is a case where one non-PC, such as a game machine or the like, is connected without any PC.

B: Modem/medium converter + PC
This is the case where one PC only is connected.

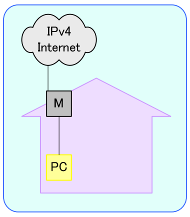
C: Router + intra-home LAN is configured
This is a case where a router is placed with an intra-home LAN built so that two or more units of equipment are really connected with the Internet.

Home Network Examples in Current Situation (IPv4)

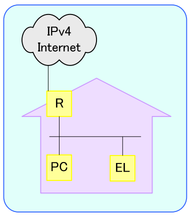
- A Modem/MC + non-PC (game machine, HDD recorder, etc.)
- B Modem/MC + PC
- C Router + intra-home LAN built



Model A



Model B



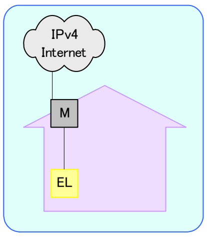
Model C

Model A has features as illustrated below. A single non-PC terminal only is connected by bridge-connecting a modem and a converter. This terminal is given a global IP address by PPP and DHCP. Should it be necessary to make access to the intra-home equipment from the exterior, a dynamic DNS service will be used.

Models Envisaged: Current Situation (Model A's Features)

Model		A : Mono-functional Model
Description		One machine in the home
Configuration	Boundary with Network	Modem and medium converter (bridge connection)
	Equipment connected	Game machine, non-PC equipment (AV equipment, IP camera, IP telephony, etc.), including case where two or more appliances are selectively connectable
Working application		Network game software, remote (mobile phone) VTR booking
Addressing	Internet	Global IP addressing with DHCP/PPP
	Local	---
Naming	Query	(Inside → outside) DNS server selected in ISP (Outside → inside) Use DDNS services and a private server provided by a vendor
	Registration	For the outside: DDNS and private server provided by vendor (A registration technique is dependent upon the services employed).
How to set		Nil
Miscellaneous		

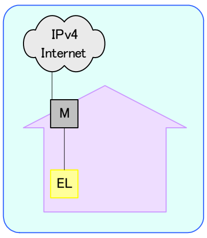
Model A



As far as security measures are concerned, Model A has encrypted communications and has been protected against illegal access, using different methods from machine model to machine model. Besides, there are many cases where no security measure has been taken at all. No countermeasures have been taken against a possible virus attack.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problems and so on
	Encryption	Resorts to equipment. Encryption systems, such as ▪ IPsec ▪ SSL ▪ Unique, etc. are implemented ,or not implemented	▪ SSL generally applied as long as equipment is TCP-based, such as HTTP or the like ▪ A few types of IP security-applied equipment are available.	✧ There is a fear that communications may be tapped. ✧ There is a fear that communications may be falsified. ■ UI getting complicated more and more ■ Key setting when using IP security
	Illegal access protection	Resorts to equipment, ▪User authentication ▪Server authentication ▪Client authentication ▪Access restricted on an address basis Or no countermeasure is taken.	▪ An appropriate authentication is implemented to protect offered services against illegal use or abuse. ▪ Access is restricted on an IP address basis.	✧ There is a feature that services may be illegally used. ✧ A camera or the like might lead to a disclosure of privacy. ■ Not regarded as a problem in equipment/services without taking any measure because their probability of encountering a threat is low.
	Virus protection	No protective measure is taken.	—	■ It is considered that there is no virus threat. ■ Effectiveness of measures is not seen.

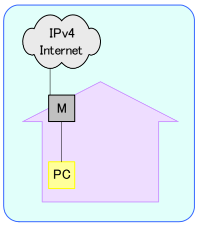
Model A



Now, Model B has features as illustrated below. In this case, a single PC terminal only is connected with a modem and a converter on a bridge connection basis. PPP and DHCP have given this terminal a global IP address. Whenever it may be necessary to make access to the equipment inside the home from the exterior, the dynamic DNS service is used.

Models Envisaged: Current Situation (Model B's Features)

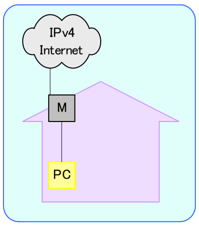
Model		B: Model with PC only
Description		One PC in the home
Configuration	Boundary with network	Modem and medium converter (bridge connection) including the case where two or more appliances are connected selectively
	Equipment connected	PC
Working application		Mail, Web, network game, connection with a corporate intra-network
Address	Internet	Global IP addressing with DHCP/PPP
	Local	---
Naming	Query	(Inside → outside) DNS server designated by ISP (Outside → inside) Use DDNS services and private server offered by vendor
	Registration	For the exterior: DDNS and private server offered by vendor (Registration techniques are dependent upon services used.)
How to set		Windows applications, unique setting methods by application, automatic setting/updating
Miscellaneous		



Model B

For security measures taken in Model B, communication encryption resorts to the OS or application while virus protection and illegal access countermeasures are left to the user under the current situations.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Resorts to OS/application. Systems, such as ■ IPsec ■ SSL, and ■ Unique are implemented or not implemented	■ Cope individually. ■ Grain sizes are varied: ■ By application ■ By protocol ■ By address ■ SSL employed generally if on a TCP basis ■ Measure flexibly changeable according to remote terminal to be connected	✧ There is a fear that communications may be tapped ✧ There is a fear that communications may be falsified. ■ IPsec difficult to be used generally in the home ■ It is often offered, however, as private application for corporate intra-access. ■ The user has pushed "OK" button without making certain of various dialog boxes.
	Illegal access protection	Resorts to the user.	Personal firewall	✧ There is a fear that a security hole on PC may be attacked. ■ Many users stop using personal firewall on a blanket basis if there should be any application not working.
	Virus protection	Resorts to the user.	･Virus checker ･ISP services	✧ Inflected with virus/spreading infection ✧ Virus may cause information to flow out. ■ Some users may put virus checker out of place because of performance degradation.



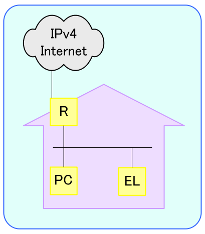
Model B

Model C is the home that has the so-called broadband environment using a router. At present, the home of this type is mostly provided with the network services using IPv4 only. Nevertheless, the router is used to connect an intra-home LAN, to which two or more PCs and non-PC equipment are connected. The LAN has private addresses distributed with DHCP. Dynamic DNS services or the like are used for connection from the exterior to the equipment linked with the intra-home LAN.

Models Envisaged: Current Situation (Model C's Features)

Model		C: IPv4-aided Network
Description		Two or more PCs/equipment in the home
Configuration	Boundary with network	Router connection
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		Mail, web, network game and connection with corporate intra-network
Address	Internet	Global IP addressing with DHCP/PPP
	Local	DHCP
Naming	Query	(Inside → outside) Use ISP-designated DNS server while relaying to intra-home node with router . (Outside → inside) Use DDNS services and private server offered by vendor. (Some settings, however, are essential to implementation of access beyond router) (Inside → inside) NetBIOS, etc.
	Registration	For the exterior: Use DDNS services and vendor-offered private server. (Registration techniques are dependent upon working services.)
How to set		Windows application, unique setting methods by application, automatic setting/updating
Miscellaneous		

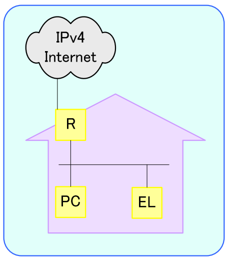
Model C



Model C has security measures resort to the equipment, OS and an application as far as communication encryption is concerned. For protection against illegal access, a router is used but how to use the router resorts to the user. Security at the end-terminal level resorts to the equipment or to the user. The router is not provided with any virus protection but it resorts to the user as far as an end terminal is concerned.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Resorts to equipment, OS and application. Systems, such as ■ IPsec ■ SSL and ■ Unique system are implemented, or not implemented	■ Router: ■ Termination with PPTP/IPsec ■ Pass-through ■ End node: ■ Encrypted separately in equipment/application ■ Measures vary with remote terminal to be connected. ■ Router, if able to take over end node, may be used in some cases.	Refer to Models A and B. ■ Manual settings will be required if router protects end node communications (because there is no tool of informing router what communications end node wants to protect).
	Illegal access protection	■ Router ■ Countermeasure already taken ■ Implementation, however, resorts to the user. ■ End node ■ Resorts to equipment and to user	■ Router ■ Packet filter ■ Simplified IDS ■ End node ■ Personal firewall	Refer to Models A and B.
	Virus protection	■ Router ■ No countermeasure taken ■ End node ■ Resorts to the user.	■ Router ■ Virus checker (Packets passing by are checked.) ■ End node ■ Virus checker ■ ISP services are used.	Refer to Models A and B. ✧ Threats to household appliances have not been rooted out completely. ✧ Possibilities that virus may proliferate from NAS or the like. ✧ Virus may enter external storage if it is connected to household appliance. ✧ Possibilities that virus if entering household appliance may remain unaware. ■ (It is considered) virus that may threaten the router does not exist.

Model C



Models Envisaged: First Step

As the formation that has made a step forward from the three Current Situation models referred to above, the equipment capable of using IPv6 has made debut. It is likely, however, that the user has persistently bought the IPv4-applicable equipment, which is found in turn to be accompanied by IPv6 after purchase. For a dial-up user to use two or more appliances, they have been progressively employing a router, which is in many cases found to be compatible with IPv6. In this stage, the IPv6 feature has just entered the home. It does not always mean that IPv6 is being used popularly.

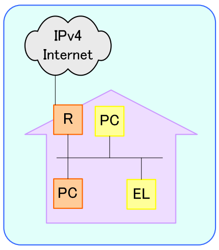
It is Models D, E and F that are implemented in the formation advanced a step forward as referred to above. They, respectively, signify the cases as follows:

Model D: Both router and PC were found to be compatible with dual stack.

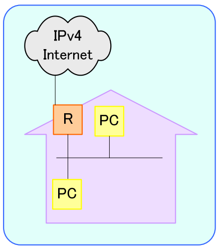
Model E: Router purchased was found to be compatible with dual stack.

Model F: With PC purchased, the OS was found to be compatible with dual stack. (Windows XP, etc.)

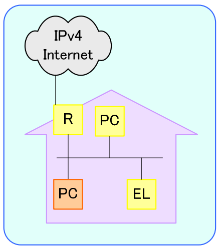
- Make a step forward from the current situation and then …
  - Equipment applicable to IPv6 has appeared, too.
    - IP telephony
    - Network camera, etc.
  - To make use of two or more appliances, it is recommended to use a router.
- Model
  - D: Both router and PC were compatible with dual stack.
  - E: Router purchased was found to be compatible with dual stack.
  - F: With a PC purchased, the OS was found to be compatible with dual stack.



Model D



Model E



Model F

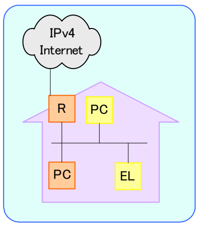
Models D, E and F's Features are basically identical. Explained here, therefore, is Model D only while omitting the explanations about Models E and F herefrom. Model D has a PC, plus two or more non-PC appliances existing in the home. A router is used to connect them to the exterior. The router has global IP addresses allocated by DHCP/PPP on the interface to the Internet side. Private addresses are allocated by DHCP in the home.

Models Envisaged: First Step (Model D's Features)

Models E and F basically identical with Model D are omitted.

Model		D: IPV4 is persistently used though router and PC are of dual type.
Description		Two or more PCs/equipment in the home
Configuration	Boundary with network	Router connection
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		Mail, web, network game and connection with corporate intra-network, remote VTR booking/video recording
Address	Internet	Global IP addressing with DHCP/PPP
	Local	DHCP
Naming	Query	Refer to Model C.
	Registration	Refer to Model C.
How to set		Windows applications, unique setting means by application, automatic setting/updating
Miscellaneous		

Model D

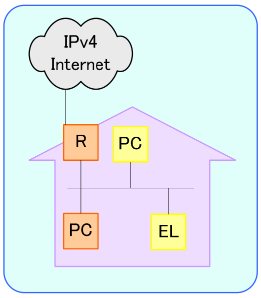


Model C has security measures resort to the equipment, OS and an application as far as communication encryption is concerned. For protection against illegal access, a router is used but how to use the router resorts to the user. Security at the end-terminal level resorts to the equipment or to the user. The router is not provided with any virus protection but it resorts to the user as far as an end terminal is concerned.

Models E and F basically identical with Model D are omitted.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Resorts to equipment, OS and application. Systems, such as ■ IPsec ■ SSL ■ Unique, etc. are implemented, or not implemented	■ Router ■ Termination with PPTP/IPsec ■ Pass-through ■ End node ■ Individually encrypted in equipment/application ■ Measures vary with remote terminal to be connected. ■ Router, if able to take over end node, may be used in some cases.	✧ There is a fear that communications may be tapped ✧ There is a fear that communications may be falsified. ■ Either is compatible with IPv4 only. ■ IPv6 does not have a scene where it is usable since it is not provided with any external connection.
	Illegal access protection	■ Router ■ Countermeasure already taken ■ Implementation, however, resorts to the user. ■ End node ■ Resorts to the user/equipment.	■ Router ■ Packet filter ■ Simplified IDS ■ End node ■ Personal firewall	✧ There are possibilities that services may be illegally used. ✧ A camera or the like might lead to disclosure of privacy. ✧ There is a fear that a security hole on PC may be attacked. ■ Either is compatible with IPv4 only.
	Virus protection	■ Router ■ No countermeasure taken ■ End node ■ Resorts to equipment and to user ■ ISP services are used.	■ Router ■ Virus checker (Packets passing by are checked.) ■ End node ■ Virus checker ■ ISP services	✧ Inflected with virus/spreading infection ✧ Virus may cause information to flow out. ■ Either is compatible with IPv4 only. ■ There is a fear that virus, which has invaded by way of IPv4, may spread in the home by way of IPv6 normally put out of use.

Model D



Models Envisaged: BCP

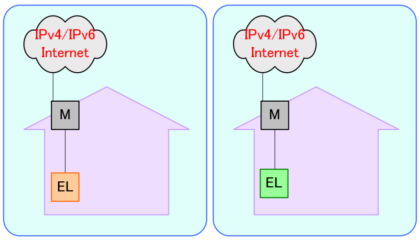
Subsequently, BCP in IPv6 is taken up. In this phase, even some appliances only will start using services as IPv6. Now, the home user will newly subscribe with the provider who has IPv6 services available, or will change over to the IPv6 services available in the existing provider. IPv4 remains serviceable as usual.

Unless an IPv6 router is available, an option conceivable is to use the IPv6 bridge feature available in the existing IPv4 router. This is Model R as illustrated below.

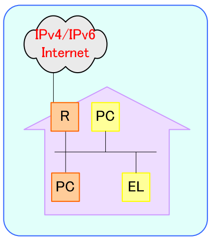
A scenario with the lead taken by the non-PC equipment, on the other hand, is also conceivable. In some cases, it may be assumed, for example, that the Internet starts being connected for the purpose of using the IP telephony and a set-top box only and that telephone has been found to be compatible with IPv6. Such a case will begin with Models J and J'.

- Partially changed over to IPv6: BCP Model to popularize IPv6
  - Even some appliances only start using services as IPv6.
  - Newly subscribe with a provider for IPv6 services/change the existing service over to IPv6.
    - IPv4 remains usable as usual.
  - Unless an IPv6 router is available, an alternative available is to use the IPv6 bridge feature (Model R)
- In some cases, Model J or J' may start being used without following an established procedure.
  - Scenario with the lead taken by non-PC
  - Service-unified type IPv6 household appliance (IP telephony and,STB), etc.

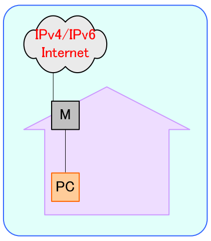
BCP with the lead taken by non-PC



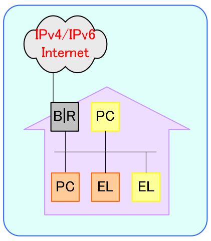
Model J Model J'



Model G



Model I



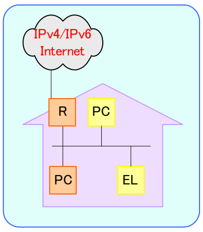
Model R

In Model G, a PC on the intra-home LAN only uses IPv6 while IPv4 only is applied in others.

Models Envisaged: BCP (Model G's Features)

(IPv4 zone identical with that in Models C/D is omitted.)

Model		G: Network with PC only using IPv6 and others IPv4.
Description		Two or more PCs/equipments in the home: with PC applicable to dual stack in some cases
Configuration	Boundary with network	Router (dual stack) connected
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		As usual (web, corporate intra-network connected, etc.), IP telephony, IP broadcasting, etc.
Address	Internet	Links local only
	Local	Prefixes used in the LAN: ▪ Obtain from ISP with DHCPv6-PD and DTCP (with /48 and /64 allocated) ▪ Generate with automatic tunnel protocol ▪ Statically allocate. RA is used to notify a prefix as locally linked.
Naming	Query	Windows XP has IPv6 incapable of transferring a DNS packet. Stacks up to Windows XP SP1 may fail to communicate due to a problem in AAAA and CNAME processing.
	Registration	
How to set		Windows applications, unique setting means by application, automatic setting/updating
Miscellaneous		Even with OS applicable to IPv6, IPv6 usage may be limited, if application is incompatible with IPv6.

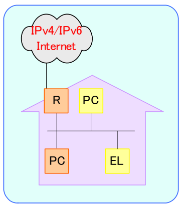


Model G

Model G has IPv6 security measures resort to the equipment, OS and an application as far as communication encryption is concerned. For protection against illegal access, a router is used but how to use the router resorts to the user. Security at the end-terminal level resorts to the equipment or to the user. As far as virus is concerned, IPv6 is not provided with any countermeasures under the current situation.

(IPv4 zone identical with that in Models C/D)

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Resorts to equipment, OS and application. Encryption systems, such as ■ IPsec ■ SSL and ■ Unique are implemented, or not implemented.	■ Router ■ IPsec termination ■ End node ■ Individually encrypted in equipment/application ■ Router, if capable of taking over an end node, may be employed in some cases (IPsec Tunnel mode, etc.)	■ Windows XP cannot be encrypted with IPv6 ESP (as of OCT/01/04) ■ Mechanisms for end node to ask router for encryption are required (or, manual settings are required). ■ For end node to use IPsec, UI will get complicated. (Skill requirements will level up remarkably.)
	Illegal access protection	■ Router ■ Countermeasures already taken ■ Implementation resorts to the user-dependent. ■ End node ■ Resorts to the user/equipment.	■ Router ■ Packet filter ■ End node ■ Personal firewall	✧ Direct access to an end node from the Internet might never be made before connecting and using IPv6 . (Security hole with countermeasures not taken yet is visualized) ✧ There is a fear of illegal access to a home IPv4 node via the dual stack host. ■ Personal firewall products compatible with IIPv6 are unavailable . (Windows XP SP2 standard products only)
	Virus protection	No countermeasure taken in IPv6	—	✧ Encrypted contents in packets cannot be checked with a router or the like. There is a fear of probably passing through an ISP virus check, etc. ■ Virus checker is incompatible yet with IPv6 (Disk I/O check only). ■ Communications cannot be checked. ■ A fear of slipping by even if the user should think "Countermeasures have been already taken."

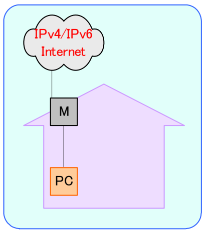


Model G

Model I has an environment of Model B but with one PC, which has been replaced with a PC applicable to the dual stack. If the application you want to use is compatible with IPv6 only, Model I is significant. Otherwise, it would be serviceable with IPv4 connected only.

Models Envisaged: BCP (Model I's Features)

Model		I: Model B whose PC has been replaced with a dual-compatible PC.
Description		One PC in the home, being compatible with dual stack
Configuration	Boundary with network	Modem and medium converter (bridge connection)
	Equipment connected	PC
Working application		Connected with the Internet and a closed network (regional IP network) Web, connected with corporate intra-network, IP broadcasting, etc.
Address	Internet	Obtain global prefix by either one of the following methods: ■ Use DHCPv6-PD, DTCP, etc. to obtain from ISP (/48 or /64 allocated) ■ Use automatic tunnel protocol to generate. ■ Statically allocate. ■ Receive RA directly from ISP.
	Local	- (Concept "Local" does not exist, since one machine only is provided).
Naming	Query	DNS server designated by ISP, with DDNS used from the exterior.
	Registration	For the exterior: Use DDNS and server provided by vendor. (Registration techniques depend on working services.)
How to set		Windows applications, unique setting means by application, automatic setting/updating
Miscellaneous		A model is significant if the application you desire to use is compatible with IPv6. Otherwise, it is serviceable with IPv4 connected only.

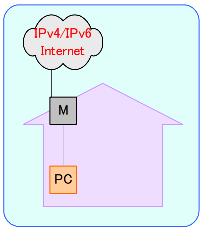


Model I

Model I has IPv6 security measures resort to the equipment, OS and an application as far as communication encryption is concerned. Its protection against illegal access resorts to the user. As far as virus is concerned, IPv6 is not provided with any countermeasures at the present.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Resorts to OS and application. System, such as ▪ IPsec ▪ SSL and ▪ Unique are implemented, or not implemented.	Encrypted individually in OS and application	▪ Windows XP does not allow IPv6 ESP to encrypt (as of OCT/01/04) . ▪ If end node should use IPsec, UI will be complicated (with skill requirements rapidly leveled up).
	Illegal access protection	Resorts to the user.	▪ Personal firewall ▪ Already proven to be compatible with Windows XP SP2	▪ IPv6-applicable personal firewall is commercially unavailable. ▪ Windows XP has packet filter feature only implemented.
	Virus protection	No countermeasure is available in IPv6.	-	▪ Virus checker remains inapplicable to IPv6 yet (with Disk I/O only checked). ▪ Comms cannot be checked. ▪ A fear of slipping by even if the user should think "Countermeasures have been already taken."

Model I

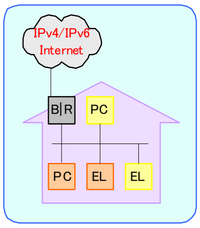


Model R is the same as Model B but its PC replaced with the one compatible with dual stack. Although a router applicable to IPv6 is not introduced, the IPv6 brigade feature available in the IPv4 router is used to lead IPv6 in the intra-home LAN.

Models Envisaged: BCP (Model R's Features)

Model		R: IPv6–applicable PC/equipment without using an IPv6 router have been implemented.
Description		One or more PCs in the home; PC/equipment compatible with dual stack or IPv4 only
Configuration	Boundary with network	IPv4 router, IPv6 bridge
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		Connected with the Internet and a closed network (regional IP network). Web, connected with corporate intra-network, IP broadcasting, etc.
Address	Internet	RA that has passed through IPv6 bridge allows for addressing, as it is. (IPv6 bridge has eliminated a distinction between WAN and LAN.)
	Local	-
Naming	Query	DNS server designated by ISP, with DDNS used from the exterior.
	Registration	For the exterior: use DDNS and server provided by vendor.
How to set		Windows applications, unique setting means by application, automatic setting/updating
Miscellaneous		A model is significant if the application you desire to use is compatible with IPv6. Otherwise, it is serviceable with IPv4 connected only.

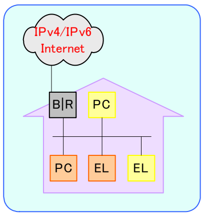
Model R



Model R has IPv6 security measures resort to the equipment, OS and an application in the PC as far as communication encryption is concerned. For protection against illegal access, no countermeasure is available so long as the IPv6 bridge is used. An RA proxy-compatible product would be helpful in protecting the home network against illegal access but whether or not it should be used would be left to the user.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Resorts to OS and applications. Systems, such as ■ IPsec ■ SSL and ■ Unique are implemented, or not implemented.	Individually encrypted in OS and applications	■ Windows XP is incapable of encrypting with IPv6 ESP(as of OCT/01/04) ■ When an end node uses IPsec, UI will get complicated (with skill requirements leveled up remarkably).
	Illegal access protection	■ No countermeasure taken in IPv6 bridge ■ RA Proxy-compatible products have already had countermeasures taken. ■ Resorts to the user.	End node ■ Personal firewall ■ Windows XP SP2 already made compatible ■ Firewall products commercially available have not been changed over to IPv6 yet. IPv6 Bridge ■ Packet filtering	■ IPv6 bridge, which transfers all IPv6 packets, has difficulties in keeping security at a level equal to that of IPv4. ■ Personal firewall software applicable to IPv6 is commercially unavailable. ■ Firewall provided on a standard basis in Windows XP has an only function of filtering packets.
	Virus protection	No countermeasure taken in IPv6	-	■ Virus checker remains inapplicable to IPv6 yet (but checks Disk I/O only.) ■ Comms cannot be checked. ■ A fear of slipping by even if the user should think “Countermeasures have been already taken.”

Model R

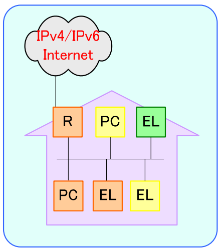


Models Envisaged: Before Dawn of IPv6 Popularization Phase

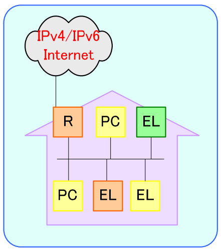
Models H, N and S have made a step forward into the IPv6 popularization phase, getting rid of the BCP status. In this phase, some equipment applicable to IPv6 only has emerged. Since the end user remains unaware of the difference between IPv6 and IPv4, an IPv4-to-IPv6 protocol translator feature is essential to Models H, N and S, any of which may require for a communication with the IPv4 equipment.

■ Make a Step Forward ahead BCP.

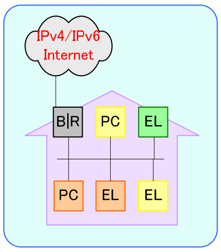
- Equipment applicable to IPv6 only has made debut.
  - From a viewpoint of the user, the difference is unknown between the equipment applicable to IPv6 only and to IPv4 only.
    - The more universally applicable the equipment, the more strongly it is called upon to be capable of communicating with the IPv4 equipment, too.
  - Translator Feature Required
    - In Model N, the PC is applicable to IPv4 only while household appliances are of IPv6/dual type.



Model H



Model N



Model S

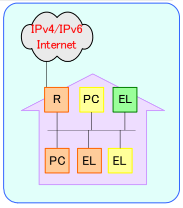
Model H is a variant of Model G, in which the equipment compatible with IPv6 only is implemented. It is connected with ISP by way of a dual stack-applicable router.

Models Envisaged: Before Dawn of IPv6 Popularization Phase (Model H's Features)

(For the IPv4 zone, refer to Model C/D.)

Model		H: Purchase Model G + equipment applicable to IPv6 only.
Description		Two or more PCs/equipment in the home; some PCs are of dual stack type and others are compatible with IPv6.
Configuration	Boundary with network	Router (dual stack) connected
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		Web, connected with corporate intra-network, IPv6 equipment intercommunications in the home, and IP broadcasting
Address	Internet	Obtain global prefix by either one of the following methods: ■ Obtain from ISP with DHCPv6-PD, DTCP, etc. (with /48 and /64 allocated) ■ Use automatic tunnel protocol to generate. ■ Statically allocate. ■ Receive RA directly from ISP.
	Local	Notify RA prefix. Link local
Naming	Query	(Outside → inside) Nodes are individually registered in DDNS server. (Inside → inside) IPv6-applicable version UPnP (not finalized yet), multicast DNS, etc.
	Registration	
How to set		Translators need be set translator system by translator system as far as translator settings are concerned. ■ Case were exclusive prefix must be provided for conversion ands ■ Where it may be necessary to relate IPv4 addresses with IPv4 addresses.
Miscellaneous		It is necessary to review the translator position.

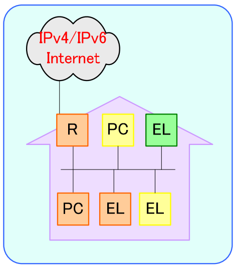
Model H



As far as IPv6 security is concerned in Model H, security products at terminals should be desirably compatible with IPv6 for protection against illegal access and/or virus attack.

(For the IPv4 zone, refer to Model C/D.)

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Both implementation level and system resort to OS, equipment and applications. ■ IPsec ■ SSL and ■ Unique are implemented, or not implemented.	■ Router ■ IPsec termination (tunnel transport mode) ■ Pass through IPsec, etc. ■ End node ■ Provided with IPsec, SSL and Unique individually by equipment/by application ■ Router, if able to take over end node, may be used in some cases.	■ Translator and IPsec are coexisting.
	Illegal access protection	■ Router Countermeasure already taken ■ End node resorts to the user. ■ Personal firewall should be compatible with IPv6 (desirably).	■ Router ■ Packet filter ■ End node ■ Personal firewall	✧ Vulnerability has emerged due to disagreement on security policy between household appliances and PCs. ✧ A fear of illegal access to IPv4 nodes in the home by way of dual stack. ✧ Establish unexpected access route, using translators.
	Virus protection	■ Virus checker should be compatible with IPv6 (desirably). ■ Virus check by ISP should be desirably compatible with IPv6.	■ Router ■ Virus checker (Packets passing by are checked.) ■ End node ■ Virus checker ■ ISP services	■ May same policy be established in IPv4 and IPv6? ■ Is any end user burden-free method available? ■ Possibilities some points may have to be set differently between IPv4 and IPv6 ■ Discrepancies of default policy from appliance to appliance might invite confusion.



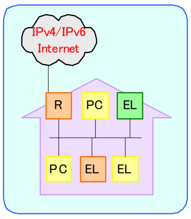
Model H

Model N is a derivative of Model C whose equipment is of dual stack type, with some appliances applicable to IPv6 only although the PC in the home is compatible with IPv4 only.

Models Envisaged: Before Dawn of Ipv6 Popularization Phase (Model N's Features)

(For the IPv4 zone, refer to Model C.)

Model		H: Model C + dual/equipment applicable to IPv6 only purchased
Description		Two or more PCs/equipment in the home, with PCs applicable to IPv4 only and equipment to IPv6, with some appliances applicable to dual stack.
Configuration	Boundary with network	Router (dual stack) connected
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		Web, connected with corporate intra-network, IPv6 equipment intercommunications in the home, and IP broadcasting
Address	Internet	Obtain global prefix by either one of the following methods: ▪ Obtain from ISP with DHCPv6-PD, DTCP, etc. (with /48 and /64 allocated) ▪ Use automatic tunnel protocol to generate. ▪ Statically allocate. ▪ Receive RA directly from ISP.
	Local	Notify RA prefix. Link local
Naming	Query	(Outside → inside) Nodes are individually registered in DDNS server. (Inside → inside) IPv6-applicable version UPnP (not finalized yet), multicast DNS, etc.
	Registration	
How to set		Translators need be set translator system by translator system as far as translator settings are concerned. ▪ Where an exclusive prefix must be provided for conversion, ▪ Where it is necessary to establish relations with IPv4 addresses in advance
Miscellaneous		It is necessary to review the translator position.

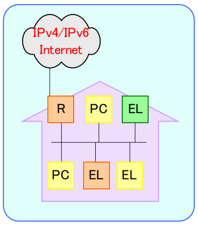


Model N

As far as the IPv6 security is concerned, Model N requires end terminal security products to be compatible with IPv6 similarly to Model H.

(For the IPv4 zone, Refer to Model C.)

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Both implementation level and system resort to OS, equipment and applications. ▪ IPsec ▪ SSL ▪ Unique are implemented, or not implemented.	▪ Router ▪ IPsec termination (tunnel transport mode) ▪ Pass through IPsec, etc. ▪ End node ▪ Provided with IPsec, SSL and Unique individually by equipment/by application ▪ Router, if able to take over end node, may be used in some cases.	▪ Translator coexisting with IPsec.
	Illegal access protection	▪ Router Countermeasure already taken ▪ End node resorts to the user. ▪ Personal firewall should be compatible with IPv6 (desirably).	▪ Router ▪ Packet filter ▪ End node ▪ Personal firewall	✧ Vulnerability has appeared due to disagreement on security policy between household appliances and PCs. ✧ A fear of illegal access to IPv4 nodes in the home by way of dual stack. ✧ Establish unexpected access route, using translators.
	Virus protection	▪ Virus checker should be compatible with IPv6 (desirably). ▪ Virus check by ISP should be desirably compatible with IPv6.	▪ Router ▪ Virus checker (Packets passing by are checked.) ▪ End node ▪ Virus checker ▪ ISP services	▪ May same policy established in IPv4 and IPv6? ▪ Is any end user burden-free method available? ▪ Possibilities some points may have to be set differently between IPv4 and IPv6 ▪ Discrepancies of default policy from appliance to appliance might invite confusion.



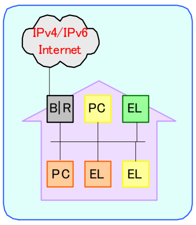
Model N

Model S is a variant of Model R, to which the equipment applicable to IPv6 only has been added. As far as their connection with the Internet is concerned, IPv4 is routed and IPv6 is bridged.

Models Envisaged: Before Dawn of IPv6 Popularization Phase (Model S's Features)

(For the IPv4 zone, refer to Models C/D.)

Model		S: Purchase Model R + equipment applicable to IPv6 only.
Description		Two or more PCs/equipment in the home; with some PCs of dual stack type and some appliances applicable to IPv6 only.
Configuration	Boundary with network	IPv4 router with IPv6 bridge
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		Web, connected with corporate intra-network and IPv6 equipment intercommunications in the home
Address	Internet	Directly addressed with RA that has passed though IPv6 bridge (IPv6 bridge does not discriminate WAN/LAN.)
	Local	—
Naming	Query	(Outside → inside) Nodes are individually registered in DDNS server. (Inside → inside) IPv6-applicable version UPnP (not finalized yet), multicast DNS, etc.
	Registration	
How to set		Translators need be set translator system by translator system as far as translator settings are concerned. ■ Where an exclusive prefix must be provided for conversion, ■ Where it is necessary to establish relations with IPv4 addresses in advance
Miscellaneous		It is necessary to review the translator position.



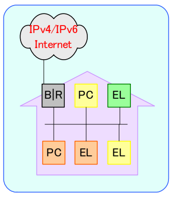
Model S

As far as the IPv6 security is concerned, the same as Model G holds true in Model S. At the same time, it is necessary to cover the security weak point that will arise when using a translator.

(For the IPv4 zone, refer to Models C/D.)

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Both implementation level and system resort to OS, equipment and applications. ■IPsec ■SSL ■Unique are implemented, or not implemented	■ Router ■ IPsec termination (tunnel transport mode) ■ Pass through IPsec, etc. ■ End node ■ Provided with IPsec, SSL and Unique individually by equipment/by application ■ Router, if able to take over end node, may be used in some cases.	■ Translator coexisting with IPsec.
	Illegal access protection	■ No countermeasure taken in IPv6 bridge ■ countermeasure already taken in RA proxy ■ End node resorts to the user. ■ Personal firewall should be compatible with IPv6 (desirably).	■ IPv6 Bridge ■ Packet filter ■ End node ■ Personal firewall	✧ Vulnerability has appeared due to disagreement on security policy between household appliances and PCs. ✧ A fear of illegal access to IPv4 nodes in the home by way of dual stack. ✧ Establish unexpected access route, using translators.
	Virus protection	■ Virus checker should be compatible with IPv6 (desirably). ■ Virus check by ISP should be desirably compatible with IPv6.	■ Router ■ Virus checker (Packets passing by are checked.) ■ End node ■ Virus checker ■ ISP services	■ May same policy established in IPv4 and IPv6? ■ Is any end user burden-free method available? ■ Possibilities some points may have to be set differently between IPv4 and IPv6 ■ Discrepancies of default policy from appliance to appliance might invite confusion.

Model S



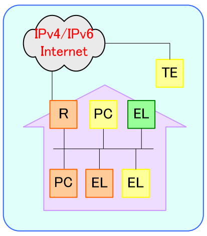
Models Envisaged: IPv6 Popularization Phase

In the IPv6 popularization phase, both IPv4 and IPv6 are available in a coexisting environment without being aware which is serviceable.

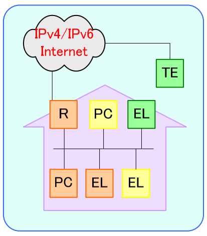
Under such circumstances, the equipment may be classified according to the protocol that it will use when it is making access to the home.

Models Envisaged: IPv6 Popularization Phase (continued)

- Let's enter an IPv4/IPv6 unconscious environment while coexisting with IPv4.
  - K: A remote access source is IPv4 equipment.
    - K' : A remote access source is dual-stack equipment (with IPv4 applied) .
  - L: A remove access source is IPv6 equipment.
    - L' : A remote access source is dual-stack equipment (with IPv6 applied) .



Model K



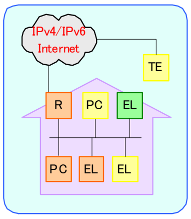
Model L

Model K is a variant of Model H, to which the case where IPv4 is used to make access to an intra-home LAN remotely from the outside. It is recommended to mount the translator feature on the router.

Models Envisaged: IPv6 Popularization Phase (Model K's Features)

Model		K: Model H + IPv4 equipment making access to an intra-home appliance from the exterior
Description		Two or more PCs/equipment in the home, with a coexistence of equipment applicable to dual stack, IPv4 only and IPv6 only. External equipment has IPv4 applied.
Configuration	Boundary with network	Router (dual stack) connected
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliances, IP camera and IP telephony) V4 external equipment (mobile phone and PC(PDA))
Working application		Booking VTR from mobile phone and viewing an image in an intra-home camera, on external equipment
Address	Internet	Obtain global prefix by either one of the following methods: ▪ Obtain from ISP with DHCPv6-PD, DTCP, etc. (with /48 and /64 allocated) ▪ Use automatic tunnel protocol to generate. ▪ Statically allocate. ▪ Receive RA directly from ISP.
	Local	Use RA to notify prefix. Link local
Naming	Query	Refer to Model H.
	Registration	
How to set		Windows applications, unique setting means by application, automatic setting/updating
Miscellaneous		It is recommended to install the translator function on the router. To connect up to the router with IPv4, it is necessary to set the router in detail.

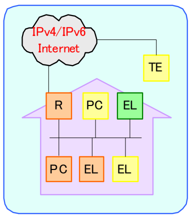
Model K



As far as the security is concerned, it is necessary to take appropriate countermeasures against the threat that will newly arise from such remote access.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Both implementation level and system resort to OS, equipment and applications. ■IPsec ■SSL ■Unique are implemented, or not implemented	■ Router ■ IPsec termination (tunnel transport mode) ■ Pass through IPsec, etc. ■ End node ■ Provided with IPsec, SSL and Unique individually by equipment/by application ■ Router, if able to take over end node, may be used in some cases.	✧ An incoming route for a remote terminal might lead to vulnerability. ■ A possible disclosure of encryption key, etc.
	Illegal access protection	■ Router Countermeasure already taken ■ Implementation, however, resorts to the user. ■ End node resorts to the user.	■ Router ■ Packet filter ■ End node ■ Personal firewall	✧ An incoming route for a remote terminal might lead to vulnerability. ■ An appropriate method of managing and authenticating the password is required. ✧ An introduction of translators aimed at remote access might invite vulnerability. (Even a zone inaccessible with IPv4 could be accessed.)
	Virus protection	■ Virus checker should be compatible with IPv6 (desirably). ■ Virus check by ISP should be desirably compatible with IPv6.	■ Router ■ Virus checker (Packets passing by are checked.) ■ End node ■ Virus checker ■ ISP services	✧ A remote terminal might not be properly protected while you are out. ✧ A remote terminal might become a virus source while you come back home.

Model K



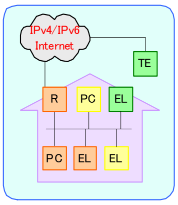
In Model L, remote access is made with IPv6.

Models Envisaged: IPv6 Popularization Phase (Model L's Features)

Model		L: Model H + IPv6 equipment making access to intra-home equipment remotely
Description		Two or more PCs/equipment in the home: with equipment applicable to dual stack, to IPv4 only and to IPv6 only coexisting. External equipment employs IPv4.
Configuration	Boundary with network	Router (dual stack) connected
	Equipment connected	PC, game machine, non-PC equipment (AV, household appliances, IP camera and IP telephony) IPv6 external equipment (PC(PDA))
Working application		Booking VTR from mobile phone and viewing images in intra-home camera with external equipment
Address	Internet	Obtain global prefix by either one of the following methods: ▪ Obtain from ISP with DHCPv6-PD, DTCP, etc. (with /48 and /64 allocated) ▪ Use automatic tunnel protocol to generate. ▪ Statically allocate. ▪ Receive RA directly from ISP.
	Local	Use RA to notify prefix. Link local
Naming	Query	Refer to Model H.
	Registration	
How to set		Windows applications, unique setting means by application, automatic setting/updating
Miscellaneous		Translator feature is recommended to be mounted on router. How to get a list of appliances in the home is a key point.

(Basically identical to Model K)

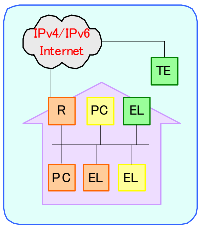
Model L



For security, it is also necessary here to take appropriate countermeasure against a terminal make remote access.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Both implementation level and system resort to OS, equipment and applications. ■IPsec ■SSL ■Unique are implemented, or not implemented	■ Router ■ IPsec termination (tunnel transport mode) ■ Pass through IPsec, etc. ■ End node ■ Provided with IPsec, SSL and Unique individually by equipment/by application ■ Router, if able to take over end node, may be used in some cases.	✧ An incoming route for a remote terminal might lead to vulnerability. ✧ A possible disclosure of encryption key, etc.
	Illegal access protection	■Router Countermeasure already taken ■ Implementation, however, resorts to the user. ■ End node resorts to the user.	■ Router ■ Packet filter ■ End node ■Personal firewall	✧ An incoming route for a remote terminal might lead to vulnerability. ■An appropriate method of managing and authenticating the password is required. ✧An introduction of translators aimed at remote access might invite vulnerability. (Even a zone inaccessible with IPv4 could be accessed.)
	Virus protection	■ Virus checker should be compatible with IPv6 (desirably). ■ Virus check by ISP should be desirably compatible with IPv6.	■ Router ■ Virus checker (Packets passing by are checked.) ■ End node ■ Virus checker ■ ISP services	✧ A remote terminal might not be properly protected while you are out. ✧ A remote terminal might become a virus source while you come back home.

(Basically identical to Model K)



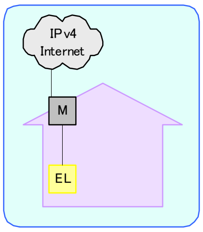
Model L

Models Envisaged: Non-PC Model

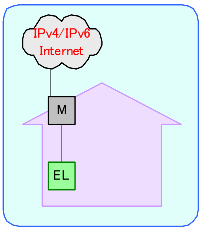
As far as the deployment to IPv6 is concerned, there are some formations peculiar to the home segment. It is a deployment of the world where non-PC equipment only is connected in the home without any PC.

In the illustration below, A is an example of the current situations. J is a formation where specific household appliance services are used on a dual stack basis. J' has no protocol but IPv6. In some cases, however, specific household appliance services may well be considered available. M is an intra-home formation where two or more non-PC appliances are connected, being made progressively applicable to IPv6. O is a remote access made by an IPv6 terminal to the non-PC equipment. And a remote access from dual-stack equipment is conceivable as O'.

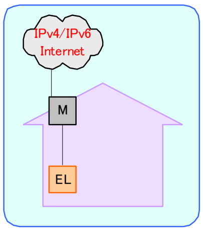
- Environments that must be taken into consideration in the home segment:
  - A: Current Situations
  - J: A default package of dual stack household appliances
  - J': A default package of IPv6 household appliances
  - M: IPv6 household appliances have emerged; household appliances free from a PC
  - O: Remote access (Make remote access from an IPv6 terminal.)
    - O' Remote access (Make remote access from a dual stack.)



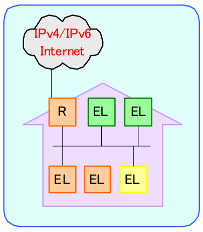
Model A



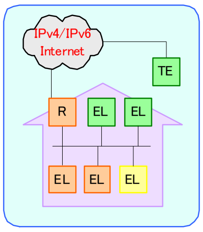
Model J



Model J'



Model M

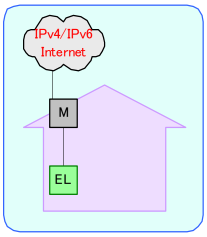


Model O

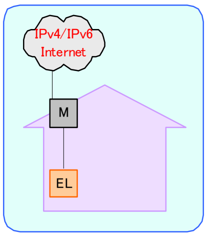
Model J is the case where a single non-PC appliance applicable to dual stack or to IPv6 only does exist in the home. To connect it with the Internet, a modem or a medium converter is used to make a bridge connection. In this case, a network connection is used for a kit of services that are set with household appliances.

Models Envisaged: Non-PC Model/BCP (Model J's Features)

Model		J,J': Default packages of household appliances
Description		Dual stack (Model J) household appliances in the home/one IPv6 household appliance (Model J')
Configuration	Boundary with network	Modem and medium converter (bridge connection)
	Equipment connected	Dual stack-compatible household appliances (Model J)/IPv6 household appliance (Model J')
Working application		Telephone, video booking and IP broadcasting
Address	Internet	Receive RA directly from ISP. (RA is most simply made applicable because of household appliances though any other tools may be conceivable.)
	Local	-
Naming	Query	DNS server designated by ISP, with DDNS used from the exterior.
	Registration	For the exterior: Use DDNS and private server provided by vendor. (For IP telephony, use SIP server provided by vendor or carrier.)
How to set		There are high possibilities that a service provider may offer setup services.
Miscellaneous		Use phone/VTR booking, etc. as xSP services available in a kit of household appliances. End equipment addressing as xSP service available



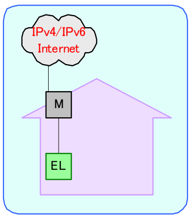
Model J'



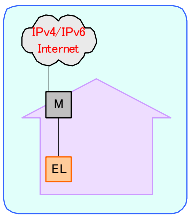
Model J

For security in Model J, it may be pointed out that non-implementation of an authentication feature would be risky, considering that an electric household appliance has a long service life.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Resorts to equipment.	▪ Provided with IPsec, SSL and Unique individually by equipment/by application ▪ Countermeasure varies with remote terminal to communicate.	▪ To what extent could measure be taken? ▪ Low-margin nodes make it difficult to encrypt hardware ▪ Difficult to take any countermeasures if implemented encryption itself should be vulnerable (especially hardware).
	Illegal access protection	Resorts to equipment and to user	▪ Authentication ▪ User authentication ▪ Server authentication ▪ Client authentication ▪ Access restriction ▪ Address basis ▪ Domain name basis	▪ (Equipment unprotected against illegal access) It may be considered to have no fear of being attacked with IPv6. ▪ Risky if authentication feature should be unavailable, with equipment service life taken into consideration
	Virus protection	No countermeasure taken		▪ Household appliances are considered free from risk of receiving virus attack.



Model J



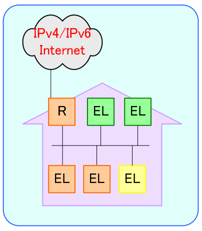
Model J’

Model M referred to in a table below is an evolved version of Model J. Two or more non-PC appliances are connected and a dual-stack applicable router is used for connection with the Internet. Naming solutions employed include UPnP or multicast DNS and the like.

Models Envisaged: Non-PC Model/Before Dawn (Model M's Features)

Model		M: Evolve from Model J.
Description		Two or more appliances in the home, with some applicable to IPv4 only and others to IPv6 only Router (dual stack) will be required.
Configuration	Boundary with network	Router (dual stack) connected
	Equipment connected	Game machine and non-PC equipment (AV, household appliance, IP camera and IP telephony)
Working application		TV and video: viewing intra-home camera images on TV set.
Address	Internet	Obtain global prefix by either one of the following methods: ▪ Obtain from ISP with DHCPv6-PD, DTCP, etc. (with /48 and /64 allocated) ▪ Use automatic tunnel protocol to generate. ▪ Statically allocate. ▪ Receive RA directly from ISP.
	Local	Use RA to notify prefix. Link local
Naming	Query	UPnP, multicast DNS, etc.
	Registration	Node that has functions equivalent to DNS server closed in the home: naming involves some issues.)
How to set		Without PC, router and equipment should be set with browser on TV or the like.(Some browsers may disturb setting screen.)
Miscellaneous		

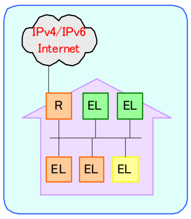
Model M



For security, it will be necessary, for example, to encrypt communications. Since it is the world where electric household appliances only are available, however, a complicatedness-free implementation is essentially required.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Both implementation level and system resort to equipment and applications. ▪ IPsec ▪ SSL and ▪ Unique are implemented, or not implemented	▪ Router ▪IPsec termination (tunnel transport mode) ▪Pass through IPsec, etc. ▪ End node ▪Provided with IPsec, SSL and Unique individually by equipment/by application ▪ Router, if able to take over end node, may be used in some cases.	✧ An incoming route for a remote terminal might lead to vulnerability. ▪ A possible disclosure of encryption key, etc. ▪ Appropriate setting means are essential to household appliances only.
	Illegal access protection	▪Router Countermeasure already taken ▪ Implementation, however, resorts to the user. ▪ End node resorts to the user.	▪ Router ▪ Packet filter ▪ End node ▪Personal firewall ▪Various types of authentication	✧ Appropriate setting means are essential to household appliances only.
	Virus protection	▪ Expect ISP and ASP services. ▪ End nodes are also expected to be protected against visrus attack.		▪ Virus threats to household appliances have not been identified clearly.

Model M

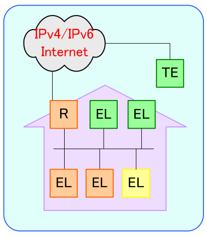


A further progress would bring about the stage on which the IPv4 equipment making access to an intra-home appliance from the exterior will emerge in addition to the situations of Model H. It is recommended that the translator feature should be implemented on the router.

Models Envisaged: Non-PC Model/IPv6 Popularization Phase (Model O's Features)

Model		O: Model H + IPv4 equipment making access to intra-home appliances remotely
Description		Two or more appliances in the home; with equipment applicable to dual stack, to IPv4 only and to IPv6 only coexisting External equipment has IPv6 applied.
Configuration	Boundary with network	Router (dual stack) connected
	Equipment connected	Game machine and non-PC equipment (AV, household appliance, IP camera and IP telephony) IPv6 external equipment (mobile phone and PC(PDA))
Working application		Booking VTR from mobile phone and viewing images in intra-home camera with external equipment
Address	Internet	Obtain global prefix by either one of the following methods: ■ Obtain from ISP with DHCPv6-PD, DTCP, etc. (with /48 and /64 allocated) ■ Use automatic tunnel protocol to generate. ■ Statically allocate. ■ Receive RA directly from ISP.
	Local	Use RA to notify prefix. Link local
Naming	Query	Refer to Model H. It should be duly noted that there are household appliances only.
	Registration	
How to set		Separate consideration is essential to setting in translator.
Miscellaneous		Translator feature is recommended to be mounted on router.

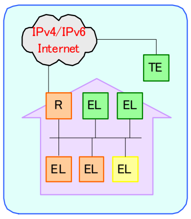
Model O



As far as security is concerned, an illegal access protection feature must be intensified but communication encryption is equally essential.

Security Measures	Measure	Status of Measure	Methodology	Threat, Problem, etc.
	Encryption	Both implementation level and system resort to equipment and applications. ■IPsec ■SSL ■Unique are implemented, or not implemented	■ Router ■IPsec termination (tunnel transport mode) ■Pass through IPsec, etc. ■ End node ■Provided with IPsec, SSL and Unique individually by equipment/by application ■ Router, if able to take over end node, may be used in some cases.	◇ An incoming route for a remote terminal might lead to vulnerability. ■A possible disclosure of encryption key, etc. ■ Appropriate setting means are essential to household appliances only.
	Illegal access protection	■Router Countermeasure already taken ■ Implementation, however, resorts to the user. ■ End node resorts to the user.	■ Router ■ Packet filter ■ End node ■Personal firewall ■Various types of authentication	◇ An incoming route for a remote terminal might lead to vulnerability. ■A possible disclosure of encryption key, etc. ■ Appropriate setting means are essential to household appliances only.
	Virus protection	■ Expect ISP and ASP services. ■ End nodes are also expected to be protected against visrus attack.	？？	■ Virus threats to household appliances have not been identified clearly.

Model O



Points in Deployment from Current Situation to BCP:

Generalizing what has been referred to above would permit us to recognize that some points need be followed when making a deployment from the current situation to BCP as referred to below.

Configuration

If possible, the user should be guided to a router-applied formation.

With the IPv6 bridge feature applied, the user should be urged to secure security at an end node.

It is strongly recommended to use a personal firewall.

For the sake of security, it is recommendable to employ a product equipped with an RA Proxy feature.

Application

In the BCP phase, it is desirable to provide an attractive IPv6 application.

The user is satisfied with IPv4.

A wider popularization of IP telephony and IP-applied multicast broadcasting might gather momentum on the deployment to IPv6.

The existing IPv4 applications will continue being used as they are.

Address Naming

An address name used in IPv4 is also used in IPv6.

For a transport protocol for DNS, IPv4 is to apply mainly.

Security

Encryption (IPsec and PPTP(?)) is to be implemented in the router.

Encryption at an SSL or application level is also to continue applying, too.

A personal firewall (commercially available)is expected to become compatible with IPv6.

Miscellaneous

Various methods of setting in non-PC equipment should be desirably automated. This automation, however, involve difficulties in the phase of deployment from the current situation to BCP.

Intra-home communication systems have been being studied, with IPv4 forerunning. In the BCP environment, IPv4 is prominent.

Non-PC-led Deployment Scenarios

A deployment to the IPv6 non-PC only environment also involves the issues similar to the PC-led one, in principle.

For the requirements specific to a non-PC IPv6 environment, the following points may be taken up:

・ A security feature is expected to be available with the router.

(Implementing this feature at a small-sized node might invite an increase in unit pricing for nodes. It is undesirable for a small node to process an extra packet, because it would lead to an increase in power consumption and to a decrease in response performance.)

・ Under the current situations, it is impossible to set a non-PC appliance nor a router without a PC (browser feature).

The browser feature borne by a digital TV set should try to be used. In this stage, it is necessary to be fully attentive to the HTML compatibility. It is also necessary to be attentive to the use of a script in HTML.)

・ Necessary to popularize automatic setup feature

It is necessary to automate the procedure for setting an access network/ISP-led modem, router, etc.

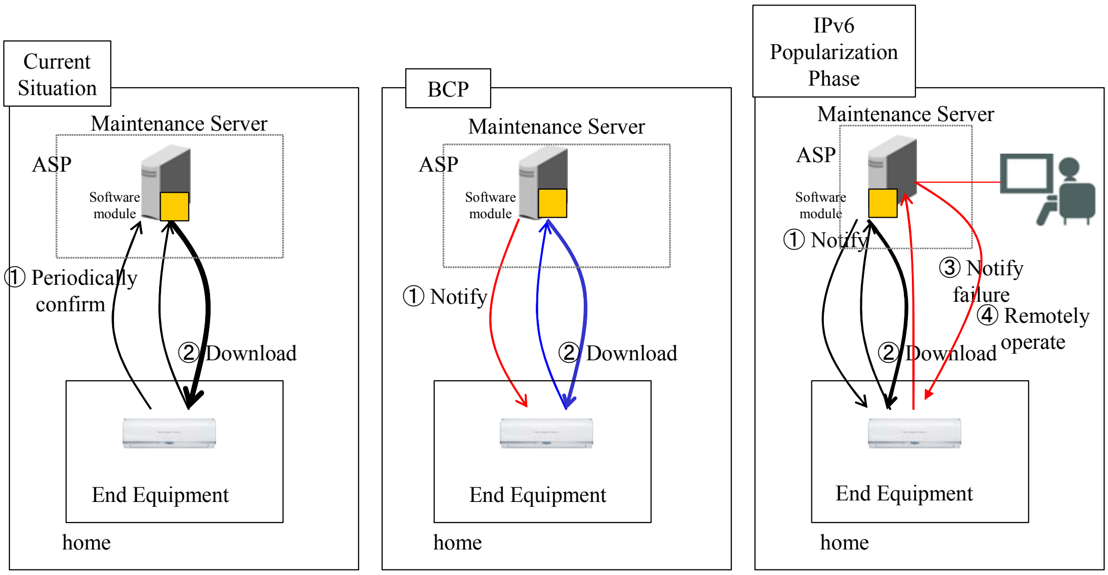
3. Deployment Scenario in Player

Implementation from Service Deployment Scenario

Here, specific services (an envisaged scenario) are assumed so that a deployment scenario is introduced in a player. Remote maintenance and network games are discussed hereunder.

Remote Maintenance Scenario

- Remote Maintenance Service Image



Thought out here is an implementation of the more timely and positive remote maintenance on a certain end appliance. Under the current situations, it is assumed that the end appliance itself checks the software for its update through the Internet, and that the updated software, if any, will be downloaded and installed.

To materialize more positive and faster updating, a deployment is to be made to the mechanisms where the maintenance server will notify the end appliance once the software module updated is ready to be provided. In response, the end appliance will download the updated module.

In addition, a further deployment is to be made to the mechanisms where a maintenance staff upon receipt of a failure notice from the end appliance will remotely operate it to do the related operation in the IPv6 popularization phase.

- Network Game Scenario
  - Outline of scenario functions
    - Current Situation
      - Inter-user communications are performed via a server and a game is played between homes.
    - BCP
      - The server provides user registration/search and a P2P type game is played on an inter-home basis.
    - IPv6 Popularization Phase
      - In a P2P type game, a real-time content, such as a video chat or the like, is used on an inter-home basis.
      - Should a game occupy a large CPU capacity, the grid feature is used so that the CPU in another game machine will be used on an inter-home basis.

This scenario is considered to provide both service provider and user with the following advantages:

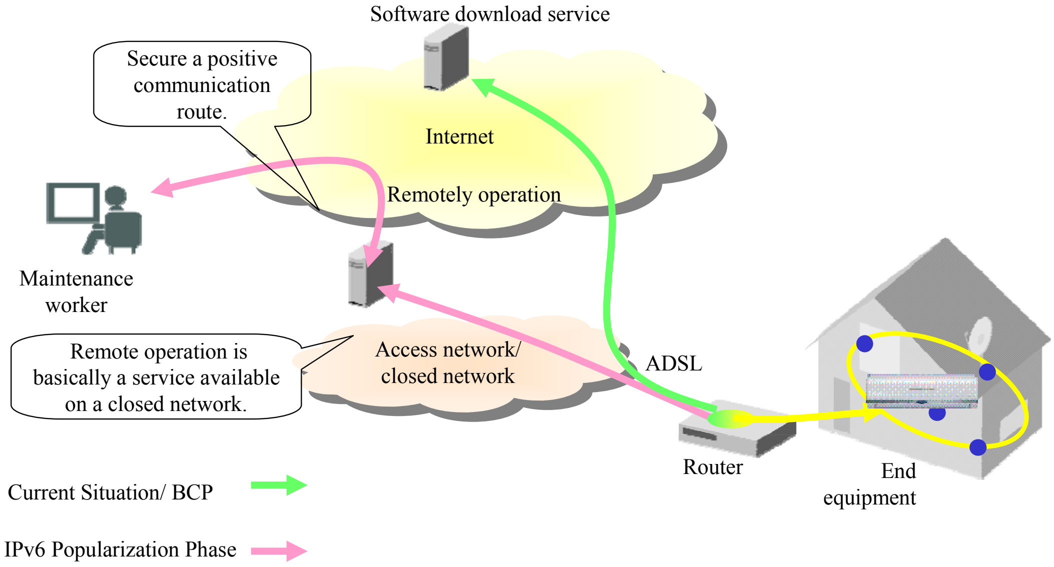
- Remote Maintenance Scenario
  - Advantages of the scenario for service provider and user:
    - Current Situation
      - Service provider: may reduce software maintenance cost .
      - User : may use the updated software.
    - BCP
      - Service provider: may control a load on the server and reduce the operational cost.
      - User : may use the updated software earlier as a result of its automatic installation.
    - IPv6 Popularization Phase
      - Service provider: may save the cost to dispatch a maintenance worker at the site.
      - User : may reduce the equipment downtime because a failure will be discovered and repaired earlier.

This scenario has its services implemented in such a formation as classified below.

- Classification of Services in Remote Maintenance
  - Current Situation
    - Periodically check. (F) Client/Server (Client Post) type
    - Download software. (D) Client/Server type
  - BCP
    - Periodically check. (E) Client/Server (ASP polling) type
    - Upgrade software. (D) Client/Server type
  - IPv6 Popularization Phase
    - Periodically check. (E) Client/Server (ASP polling) type
    - Download software. (D) Client/Server type
    - Remotely operate. (D) Client/Server type + (F) Client/Server (Client post)

From a network point of view, the updated module is provided and obtained on an open network. The remote operation to be performed in the IPv6 popularization phase, however, is to be implemented by way of a closed network.

- Network Configuration


Software download service
Secure a positive communication route.
Internet
Remotely operation
Maintenance worker
Remote operation is basically a service available on a closed network.
Access network/ closed network
ADSL
Router
End equipment
Current Situation/ BCP
IPv6 Popularization Phase

Current Situation

In the current situation of this scenario, all maintenance communications are performed with IPv4. And the end equipment in the home always start communicating.

For a status of each player in this stage, see the related section in the “Scenario in Player” referred to later.

- Current Situation
  - Feature
    - Communicate in the IPv4 environment.
    - Start communicating from the home as transmitting source.
  - Links with which each player is related.
    - End equipment provider
      - Built-in equipment edition: current situation
    - Network equipment provider
      - L3 and above equipment (including composite one) edition: current situation
    - Communication Network (general)
      - ISP SWG
    - Service provider
      - (D) Client/Server type: current situation
      - (F) Client/Server (Client post) type: current situation

BCP

IPv6 is used in BCP. Using IPv6 will permit the exterior to communicate with the home arbitrarily. It will be newly necessary, however, to take security into consideration.

- BCP
  - Features
    - Communicate in the IPv6 environment.
    - Communications from the exterior to the home take place.
    - It is necessary to take security into consideration.
  - Links with which each player is related.
    - End equipment provider
      - Built-in equipment edition: BCP
    - Network equipment provider
      - L3 and above equipment (including composite one) edition: BCP
    - Communication network provider
      - ISP SWG
    - Service provider
      - (D) Client/Server type: BCP
      - (E) Client/Server (ASP polling) type: BCP
    - Miscellaneous
      - Security SWG

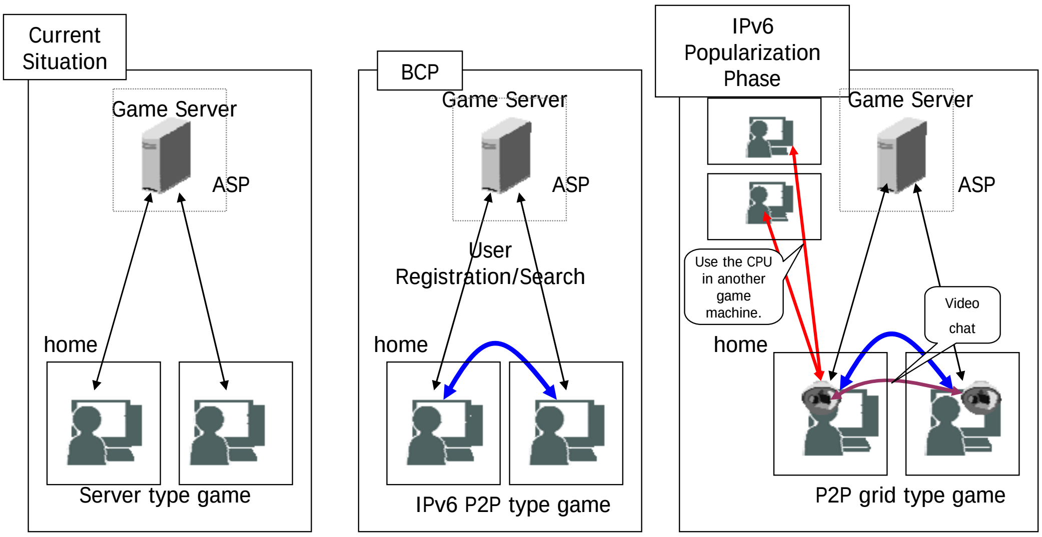
IPv6 Popularization Phase

In the IPv6 popularization phase, IPv6 will be effectively used not only to communicate from the exterior to the home but also to remotely operate the end equipment. In this phase, strict security measures are called upon.

- IPv6 Popularization Phase
  - Feature
    - Communicate in the IPv6 environment.
    - Communications from the exterior to the home take place.
    - Firm security is required to operate the end equipment available in the home.
  - Links with which each player is related.
    - End equipment provider
      - Built-in equipment edition: BCP/IPv6 Popularization Phase
    - Network equipment provider
      - L3 and above equipment (including composite one) edition: BCP/IPv6 Popularization Phase
    - Communication network provider
      - ISP SWG
    - Service provider
      - (D) Client/Server type: BCP/IPv6 Popularization Phase
      - (E) Client/Server (ASP polling) type: BCP/IPv6 Popularization Phase
      - (F) Client/Server (Client post) type: BCP/IPv6 Popularization Phase
    - Miscellaneous
      - Security SWG

Network Game Scenario

Network Game Service Image



This scenario is to intensify the functions available in a network game. At present, a network fighting-game has all of its functions controlled by the server. BCP has the user registration/ management executed by the server. For actual fighting, however, BCP provides a peer-to-peer (P2P) type game, which is really fought through direct communications between users' end terminals. In the IPv6 popularization phase, moreover, an application, such as real-time video chat or the like, is developed while trying to materialize the grid computing that would enable a far more highly loaded game to be fought by making effective use of a CPU cycle in surplus in another end equipment connected with the network.

- Network Game Scenario
  - Outline of scenario functions
    - Current Situation
      - Inter-user communications are performed via a server and a game is played between homes.
    - BCP
      - The server provides user registration/search and a P2P type game is played on an inter-home basis.
    - IPv6 Popularization Phase
      - In a P2P type game, a real-time content, such as a video chat or the like, is used on an inter-home basis.
      - Should a game occupy a large CPU capacity, the grid feature is used so that the CPU in another game machine will be used on an inter-home basis.

This scenario provides a service provider with a chance of offering a new form of games at lower cost. At the same time, it provides the user with the possibility of enjoying a game of such type as difficult to materialize so far.

- Network Game Scenario
  - Advantages of scenario for service provider and user:
    - Current Situation
      - Service provider: may provide a new form of games via a server.
      - User : may enjoy a game in cooperation with another user.
    - BCP
      - Service provider: may suppress a load on the server so that investments may be controlled.
      - User : can avoid a server congestion and enjoy a game in cooperation with another user.
    - IPv6 Popularization Phase
      - Service provider: may provide a game at a large CPU capacity and a new game using video contents.
      - User : may use a new form of games.

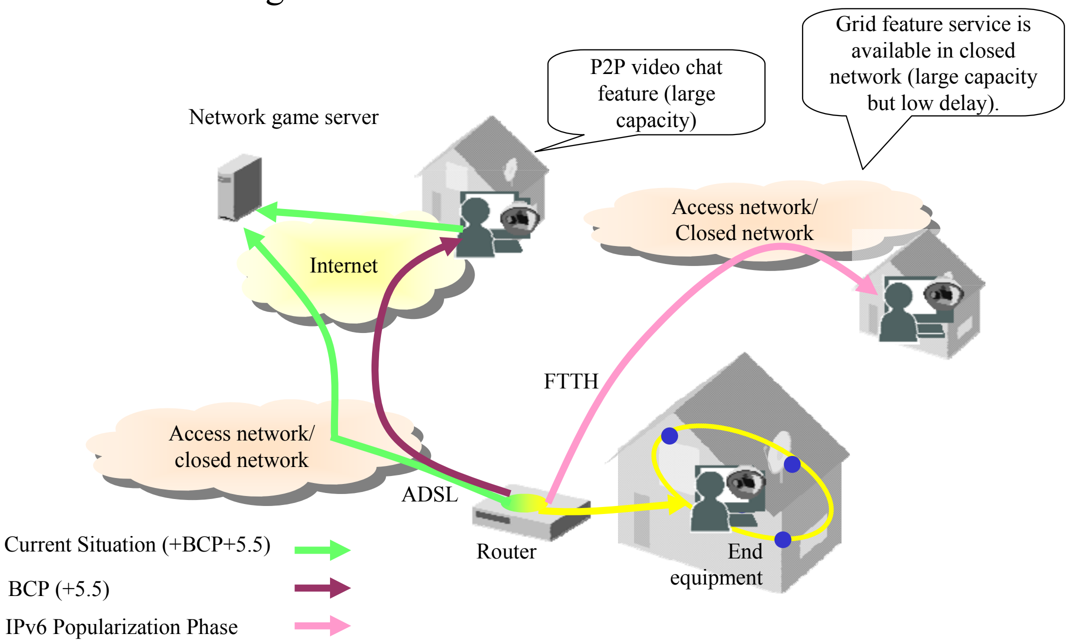
In this scenario, a network game has a network usage form evolved as referred to below.

Classification of Services in Network Game

- Current Situation
  - Server type network game (D) Client/Server type
- BCP
  - Server type network game (D) Client/Server type
  - P2P type network game (C) P2P + Lobby Server type
- IPv6 Popularization Phase
  - Server type network game (D) Client/Server type
  - P2P type network game (C) P2P + Lobby Server type
    - Add a P2P video chat feature.
  - Grid type network game (B) P2P + connection management server

From a network point of view, large-capacity communications, such as a video chart or the like, will go on increasing on an open network. In addition, grid computing will come to be performed on a closed network by making effective use of large capacity and low delay.

Network Configuration


Grid feature service is available in closed network (large capacity but low delay).
P2P video chat feature (large capacity)
Network game server
Access network/ Closed network
Internet
FTTH
Access network/ closed network
ADSL
Router
End equipment
Current Situation (+BCP+5.5)
BCP (+5.5)
IPv6 Popularization Phase

Current Situation

Under the current situations, a network game is based on IPv4 communications, which will not fail to be started by the end equipment in the home. The status of each player is shown at the related section as referred to below in the “Scenario in Player” later.

- Current Situation
  - Feature
    - IPv4
    - Communications are sent by the home as transmission source.
  - Links with which each player is related.
    - End equipment provider
      - Built-in equipment edition: current situation
    - Network equipment provider
      - L3 and above equipment (including composite one) edition: current situation
    - Communication network provider
      - ISP SWG
    - Service provider
      - (D) Client/Server type: current situation

BCP

In BCP, IPv6 inter-home communications will come to be performed. Coupled with this, the security feature will become important for a game to secure fairness, too. In addition, it will become necessary to cope with the delay and QoS issues in P2P communications.

- BCP
  - Feature
    - IPv6
    - Inter-home communications take place.
    - Security functions to protect user information and maintain fairness.
    - Extend a network to a large capacity/low delay, covering QoS.
  - Links with which each player is related.
    - End equipment provider
      - Built-in equipment edition: BCP
    - Network equipment provider
      - L3 and above equipment (including composite one) edition: BCP
    - Communication network provider
      - ISP SWG
    - Service provider
      - (B) P2P+Connection management server: BCP
      - (C) P2P + Lobby Server type: BCP
      - (D) Client/Server type: BCP
    - Miscellaneous
      - Security SWG

IPv6 Popularization Phase

In this phase, it is naturally necessary to cope with the issues in BCP. In addition, the end equipment will be called on to be applicable to the multi-home/multi-prefix mode so that using the closed network for grid computing may coexist with playing a game on an open network.

- IPv6 Popularization Phase
  - Feature
    - IPv6
    - Inter-home communications take place.
    - Security functions to protect user information and maintain fairness.
    - Extend a network to a large capacity/low delay, covering QoS.
    - CPE, End Equipment applicable multi-home/multi-prefix
  - Links with which each player is related.
    - End equipment provider
      - Built-in equipment edition: BCP/IPv6 Popularization Phase
    - Network equipment provider
      - L3 and above equipment (including composite one) edition: BCP/IPv6 Popularization Phase
    - Communication network ISP provider
      - ISP SWG
    - Service provider
      - Service (C) P2P + Lobby Server type: BCP/IPv6 Popularization Phase
      - Service (D) Client/Server type: BCP/IPv6 Popularization Phase
    - Miscellaneous
      - Security SWG

Scenario of Deployment in Each Player

In the beginning of this document, the players involved in the deployment of a network to IPv6 were analyzed. Arranged in order below are the steps that each player to take in deployment/implementation, including precautions and problems involved. If the deployment should be available in two or more options, their respective advantages and disadvantages will be defined.

The Service Provider edition, furthermore, does not specialize in IPv6 but contains a general description of IP-applied goods.

Scenario in Player: End Equipment Provider

Here, the end equipment will be described as classified into three categories: PC (OS and middleware), PC (applications) and built-in equipment.

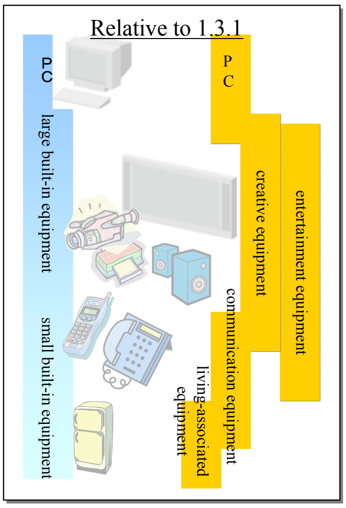
The reason why such a classification has applied rather than by type of equipment is because a working use does not always agree with the working equipment in terms of those network functions which should be performed. A network function is largely dependent upon the capability of a network-borne CPU. Between a PC and built-in equipment, in particular, there is a significant difference in their requirements, such as user interface availability, computer resources serviceable enough to operate security mechanisms, universal type or custom-made and so on.

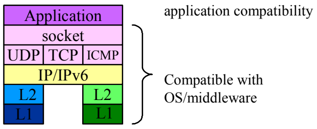
Between an on-PC OS/middleware development and an applied software development, furthermore, there is a difference in the protocol level to be achieved in a network/transport layer or in an application layer.

Player Deployment Scenario (End Equipment Provider Edition)

- End Equipment Provider Edition classifies and sorts equipment as follows:
  - PC (OS and middleware)
  - PC (applications)
  - Built-in equipment
- Classified because:
  - An actual application classification does not always coincide with what should be materialized by equipment.
    - Rather influenced more significantly by computer resources
  - Requirements differ between PC and built-in equipment.
    - User interface availability
    - Computer resources usable in security mechanisms
    - Universal/exclusive
  - Requirements differ between OS/middleware development on PC and applied application development.
    - Compatilibity at network layer/transport layer protocol level
    - Compatilibity at application layer level

Classification





Current Situations of Built-in Equipment

There are a lot of IPv6 stacks, including various types of ITRON OS, Linux and Windows CE .NET for a small-sized machines and Windows XP Embedded/CE for a large-sized machine.

As far as their implementation is concerned, the IPv6 Ready Logo program (http://www.ipv6ready.org/) and its specifications are helpful for your reference.

Most of the built-in equipment commercially available, however, is not compatible with IPv6. In many cases, IPv4 has been used to extend functions, bringing about a harmful influence of complicating the communication steps or setting up a closed network with a unique protocol applied.

The built-in equipment compatible with IPv6 is currently available from several vendors, such as a network camera, a sensor centralized management device, an IP telephony set, a set-top box (expected to be released on a blanket basis on the assumption that the services be used), etc.

An application protocol working in the built-in equipment normally varies from field to field. A variety of protocol systems have been discussed and employed in the built-in equipment. A certain time is required to standardize them. A standard protocol system specializing in IPv6 does not exist, indeed. IP-compatible equipment has been really moving to extend an IPv4-compatible system to an IPv6-compatible type.

BCP in Built-in Equipment

Requirements (essential)

The essential requirements to the built-in equipment are as follows:

1. Making a stack compatible with IPv6 (a changeover to a dual stack)

To this end, two choices are available: one is to purchase an IPv6 stack already developed and the other to newly develop a stack for a specific OS.

Essential requirements are to provide a stack with an IPv6 base protocol (address automatic setting specified in IPv6 Ready Logo Phase-1 <including NDP> and packet-sending/receiving specification). In this sense, I-D (draft-ietf-ipv6-node-requirements), TACA Project (www.taca.jp), would be helpful for your reference.

2. User Interface

The user should be allowed to display and set the IPv6-associated information. The “Plug and Play” principle , however, should apply to the user interface basically.

3. Tailoring Appropriate Applications to an IPv6 Stack

It is necessary to carry out programming independently available to an address family (socket, address, etc.) and to properly decide a communication receiving address or sending address (so as not to downgrade the user friendliness). In the event of failure to use IPv6, moreover, it is necessary to materialize a smooth fall-back.

4. Naming Solution

For naming solution, it is called upon to take measures as follows:

DNS query AAAA record compatible
DNS transport is not required to be compatible with IPv6 (in dual-stack mode)

DDNS registration The registration protocol is compatible with AAAA records.
(Compatible with AAAA records to the DDNS server side)

Miscellaneous Implementation peculiar to the vendor (→ It is desirable to act on vendors for standardization.)

5. Security Mechanisms

Access restriction:

Access restriction systems conceivable include user/password authentication and restriction based on a node (Unique ID), on an address and on a domain name.

A stack compatible with the IPv4 mapped address would require caution. Using the IPv6 socket might establish an IPv4 connection. Besides, a reverse dictionary-based access restriction cannot or should not be used.

Methodologically, an access restriction should be tailored at an application level or addressed at a built-in equipment level. Without a user interface, however, a problem would still be left behind, or difficult to establish a security mechanism. Available also as a solution to the problem are a method of deciding an appropriate policy beforehand (authorizing an identical prefix only or otherwise) and a means of physically dissolving the problem (proximity device authentication, joint use of infrared ray communications or the like).

A system or a method need be selected according to the characteristics of development equipment.

Requirements (optional)

“Desirably Materialize Safe Communications”

Compatibility with IPsec and with SSL is available a means of materializing safe communications.

IPsec may be implemented in either software or hardware.

Software implementation is advantageous for low cost while having disadvantages pointed out, including possibilities that it may lead to a degradation of performance and to an induction of vulnerability.

Hardware implementation is advantageous for high performance. Its disadvantages include high cost and necessity to modify the OS/protocol stack more or less.

IPsec as a whole has a disadvantage that it separately requires key-exchange mechanisms, such as IKE, IKEv2, static, etc. And an initialization of IKE remains problematical. The IPv6 IPsec stack, Windows XP (including SP2), moreover, would not allow ESP to be used for encryption.

SSL, on the other hand, is advantageous in the sense that there are a plenty of compatible clients (with a web browser available) , with its disadvantage lying in the incapability of using any applications other than TCP-based ones.

“Desirably Automate Settings”

Automation except for NDP (address/default settings) remains unavailable on a standard basis. It is necessary, therefore, to implement a unique method of automating settings. It might well be considered as one of the advantages that the usability could be improved by implementing a unique system. Nevertheless, a vendor-unique system would bring about a disadvantage of losing interconnectivity.

“Desirably Use IPv6 even if IPv6 Router is Unavailable”
“Desirably Use IPv6 even if Access Circuit does not Support IPv6”

To meet these requirements, it is necessary to implement an IPv6 termination feature. Methodologically, two means are available: tunnel termination and access circuit termination. The disadvantage as a whole could be pointed out as the high possibility of pressing computer resources if IPv6 should be implemented in a signal appliance.

・ Tunnel Termination

In this case, the access circuit is terminated with an IPv6 tunnel established on IPv4 by using the existing terminator (router or the like). The advantage is that the access circuit would not always need to be changed over to IPv6. The equipment manufacturer/vendor, furthermore, is in a position to act also as a tunnel server/ASP, too. The disadvantage is the fact that tunnel systems are disorderly available and that any tunnel system, which could be called a “de-facto” standard, is unavailable. Since systems vary from tunnel connection provider to tunnel connection provider, their implementation involves difficulties. Besides, using a tunnel will bring about a difference in connectivity between IPv4 and IPv6. This may downgrade usability while confusing the user with high probability. In addition, it will increase the implementation cost, too.

・ Access Circuit Termination

It is conceivable to have a feature built in the access terminator (originally built-in or retrofitted) . The advantage is its capability of allowing the user to communicate on an IPv6 basis without fail while the disadvantage pointed out is high cost. It is naturally premised on a changeover of the access circuit to IPv6.

"Desirably Perform Setting Operations with GUI"
"Desirably Set Details at a Higher Level than that on a Plug and Play basis."

To this end, it is conceivable to provide and/or apply the universal user interface that has neither controls nor displays. Using the web browser available on a PC or in a digital TV set will fall in a range of options available.

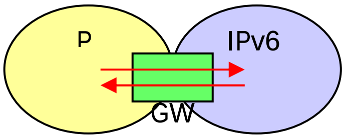
IPv6 Popularization Phase for Built-in Equipment

Requirements (essential)

The essential requirements to the built-in equipment in the IPv6 popularization phase are as follows:

1. Standardize the technologies for a gateway to a specific application protocol/network

It will be necessary that the protocol composing a closed network be combined with the IPv6 network. Ideally, interchangeability should be established between Unique Protocol P and IPv6 to each other. Though dependent upon how a protocol and an application will operate, the one-way interchangeability may be considered acceptable, too (including a status notice with a sensor, etc.)



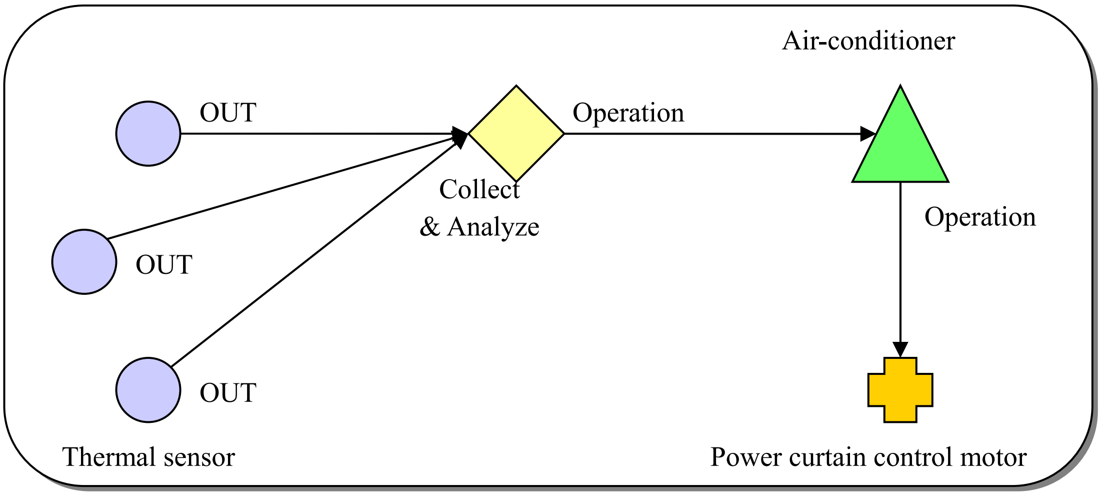
This should be preferably proceeded with while standardizing IPv6-compatible application protocols at a time.

2. Standardize IPv6-compatible application protocols

It is desirable to make both application protocol transport and application protocol-exchanging information compatible with IPv6. More specifically, they include service discovery/notice/control protocols and the address information contained in a protocol.

3. Desirably Materialize Flexible Cooperation among Two or More Appliances

To this end, it will be necessary to define an operation sequence (nodes, events, and conditions involved) and to materialize its operations. The advantage is a potential to materialize a highly advanced feature by letting two or more appliances cooperate. In other words, a cooperation among different vendors, once materialized, would allow ISP and a vendor to control the equipment on a blanket basis so that the usability may be upgraded. The disadvantage is a fear that corralling may take place since a standardized mechanism remains unavailable. There is another fear, on the other hand, of the delay in dissolving the problems, coupled with the standardization work.



4. Intensify security

As far as security is concerned, all the equipment cannot be addressed identically.

・ Where security is available at a local node:

In this case, the node is to be provided with an appropriate one of various security mechanisms, such as IPsec, SSL, dynamic key exchange, encrypt/hash algorithm and so on.

・ Where security is unavailable at a local node:

It is necessary to build up those mechanisms, which would ask CPE (router and bridge) for an appropriate protection. Some measures must be additionally taken by disabling the network to communicate with any remote terminals other than those designated through prior restriction.

In addition, it is called upon to establish a security measure technique.

An on-line automatic updating function is available in two types; push type and pull type. Either function, however, is subject to a prior agreement with the user. Off-line updating is offered in such a way of sending the updating software to the user as far as the built-in equipment is used under a service contract or the like.

5. Naming Solution/Equipment Discovery Mechanism

To manage the equipment on a blanket basis and to display a list of appliances, it is necessary to provide a mechanism of detecting two or more appliances existing in the home. And a naming mechanism is also required so that the user may readily detect and identify a name (naming in a natural language and relating it to a location in the home). De facto standards should desirably make debut in IPv6.

Requirements (optional)

“Desirably Materialize Safer Communications”

In this sense, it is called upon to make effective use of new security mechanisms, such as Trusted 3rd Party Model or the like, as a means of establishing access restriction and secure data channeling. This model has an advantage of allowing settings to be simplified. It has disadvantages, such as a relying on third party’s becoming a Single Point of Failure, a delay taking place when trying to communicate, necessity of addressing application by application and needs for cooperation in business aspects (or put all in your chest).

“Desirably Protect Equipment More Safely”

To control the network equipment, especially the firewall located at the entrance to the home, it is expected that a control mechanism, such as IPv6-compatible UPnP IGD or the like, should make debut sooner. It has an advantage of improving the safety since the system may shut off the exterior so long as communications are put out of scope. The disadvantage is its incapability of properly handling the communications independently starting in the exterior.

“Desirably Protect More Equipment with Priority”

In this sense, it will be necessary to manage intra-home security polices and settings on a blanket basis. It has an advantage of allowing possible misoperations to be reduced by avoiding individual settings. Even in the event of a new threat, the security may be modified with ease. (ISP or the vendor may manage security on a blanket basis, too.)

The disadvantage is a possible event of corralling because standard mechanisms do not exist. Even if a standardization work should be performed, a delay could be predicted in dissolving those problems, if any, which may arise, coupled with the standardization work.

“Desirably Materialize Communications with Consideration Given to Privacy”

Making a private extension will allow you to dynamically change the least 64 digits of an IPv6 address (interface ID). Under the current situations, however, it is difficult to materialize a higher level of concealability in communications, Nevertheless, a few suggestions have been made at a research level and could be expected to evolve technologically in the future while hoping a significant progress of standardization from now on. Studies have been being made on a method of encrypting communications while both server and user are maintaining the concealability of a communication core.

Current Situation of PC (OS/Middleware)

The compatibility with IPv6 has been already established in most of the operating systems, such as Windows series, Mac OS X, Linux, BSD family OSs, Solaris and so on.

Basically, these operating systems secure interconnectivity. Nevertheless, there are some discrepancies, which may be mainly pointed out as follows:

- Implementing the Advanced API,
- Resolver's behaviors varying from implementation to implementation,
- Implementing the Node Information Query,
- Methods of implementing Privacy Extension and of determining a sender address,
- IPv6 transport in DNS,
- DNS UPDATE and
- IPsec

Some problems have been pointed out in implementing IPv6 in an OS. That is, a certain period of time is required to accomplish the connection or it is impossible to connect. (Under the WIDE Project, an activity called, "IPv6 Fix" has started: http://www.v6fix.net/)

Whether IP is valid or invalid with an OS in its initial conditions varies from OS to OS. It is valid in Mac OS X and invalid in Windows. And Linux has IP valid or invalid, depending upon its distribution.

BCP in PC (OS/Middleware)

Once IPv6 has been validated, IP is serviceable and it is unnecessary to take drastically corrective action.

Nevertheless, BCP involves problems in virus protection software, personal firewall, DNS/resolver, applications, etc.

Problem in Virus Protection Software

Out of the existing virus protection software, a network protocol analyzer type has remained incompatible with IPv6 (as of OCT/01/04).

(Example) When an email message is read via IPv6 POP3, a virus cannot be detected before a disk not checked for virus has started being written in.

Problem in Personal Firewall

Personal Firewall has still remained incompatible with IPv6 (as of OCT/01/04 for package products). Windows XP (SP1 + Advanced Network Pack, SP2) has IPv6 Firewall capable of operating statefully but it has no GUI.

Problem in DNS/Resolver

There are some stacks existing, which would not process though the DNS server has returned CNAME or Record A.

Problem in Applications

There is a problem that even a network unconnectible with IPv6 will unconsciously try to connect IPv6 once AAAA has been obtained in DNS response. A case, moreover, has been reported where a fall-back to IPv4 was imperfect and time-consuming.

IPv6 Popularization Phase for PC (OS/Middleware)

Requirements (essential)

1. Dissolve the operational problem arising from a restriction on implementation
2. Completely support IPsec
   In this sense, it is called upon to support ESP for encryption and dynamic key-exchange protocols, such as IKE and IKEv2.
3. Support an intra-home node management feature
   To this end, it is necessary to implement those applications which will manage a necessary protocol (UPnP, Rendezvous, Multicast DNS or the like).

Requirements (optional)

In the IPv6 popularization phase, optional requirements include an implementation of Mobile IPv6 (Client and Home Agent), IPv6 transport in DNS and new security mechanisms (SEND and DNSSEC), and a support of other new specifications.

Current Situation of PC (applications)

Famed applications are now in the process of getting dual stack compatible. Some problems, however, have been pointed out. For example, “a network unconnectible with

IPv6 will unconditionally try to connect IPv6 once AAAA has been obtained as DNS response. This involves two problems: one is attributable to the library offered by the OS and the other attributable to a unique connection logic. Pointed out also, furthermore, are such problems as, "A fall-back to IPv4 is imperfect but time-consuming," and "It is impossible to directly enter an IPv6 address."

The applications that could be taken up as usable examples include a web browser (HTTP Client), FTP Client, Email Client, VoIP, SSH (Remote Log-in) and Instant Message.

It has been also pointed out that there are some applications not confirming to the style peculiar to Address Family. A case, for example, does not use Socket API (getaddrinfo()) to the RFC2553 format, which has had AF_INET, AF_INET6 hard-coded.

In some cases, satisfactory security measures have not been taken, especially insufficient to take countermeasures against a variety of virus software.

BCP in PC (applications)

Requirements (essential)

1. Promoting Changeover to Dual Stack

It is necessary to enlighten the user on the programming technique peculiar to Address Family. Though not related with the operation of a program, the enlightenment is an important step to the establishment of a better code. This should be promoted with the imitative taken by OS vendors and development environment vendors. Socket Level API could be concealed with Application Library.

In addition, it is also necessary to introduce a fall-back mechanism so as to reduce the case where IPv4 only is easier to use. So long as an OS remains unmodifiable, the corrective action should be taken on the application side as far as practicable. Fall-back mechanisms should be expected to be standardized.

2. In a working scene where the OS and applications have been frequently found to be vulnerable, their positive use should be refrained from

Since there is a fear that you may suffer from a problem of possibly assuming a security-related responsibility, there are some cases where you should not dare to recommend an OS and/or an application or applications. For any applications free from vulnerability, however, you should positively recommend to use them so as popularize their usage.

3. User Interface Standardized

It may be safely said that a user interface could be preferably handled identically even if an application, such as how to enter an IPv6 address or the like, were changed. Entering "." (period) will cause a shift to the next box in Ipv4. A method equivalent thereto should be introduced in IPv6, too.

The IPv6 terms used to compose a user interface, moreover, should be of standard type. For recommendable terms relating to IPv6, please refer to the terms made open to the public by the IPv6 Terms Work Group, Internet Association (http://www.iajapan.org/ipv6/v6termwg.html).

Requirements (optional)

1. Support the IPv6 addresses (literal) in a block, where FQDN, etc. should be entered for URL

This feature is effective to cut and divide a problem. Nevertheless, it may be considered acceptable if it is applicable to a fault detector application only.

2. Support IPv6 for auxiliary functions

Action should be desirably taken on an application by application basis, including a script to automatically set proxy in a web browser and an improvement of the support statuses in various macros and script languages.

Scenario in Players: Network Equipment Providers

Network equipment providers will be discussed, with network equipment classified as follows:

- Layer 1/Layer 2 equipment
- Layer 3 and higher equipment (including composite equipment)
- Equipment for collective housing (Layer 1 and higher equipment located in common space)

Composite equipment, which is a combination of Layer 3 and higher equipment, is not treated separately. The equipment for collective housing is independently handled since functional requirements vary from equipment to equipment.

Current Situation of Layer 1/Layder 2 Equipment

The equipment discussed here covers a switching hub, a wireless LAN access point, an xDSL modem, a cable modem (bridge type), a medium converter and ONU. These devices are not conscious, in principle, of the compatibility with IPv6.

A wireless LAN access point, however, does exist, which will check a setup layer (Layer 3 or higher). In such a case, IPv6 may disable you to communicate since the unique authentication process is provided on the premise that IPv4 should apply. And there is a wireless access point not allowing for a passage of multicast. There are possibilities that communications may be unavailable since IPv6 multicast (which is to begin with MAC Address 33:33) could not pass through the access point.

BCP in Layer 1/Layder 2 Equipment

Requirements (essential)

1. IPv6 Transmitting Process

A corrective action need be taken for the equipment incapable of transmitting IPv6. This is basically dependent upon the hardware. So, the corrective action is hard to take. An only solution to this problem is to replace such equipment. Even a filtering function, using EtherType, need support IPv6 securely.

Requirements (optional)

“Multicast Traffic Localization”

While listening to and watching a contents-distributing service, there may be some instances where the IP telephony and data communications are pressed. Consequently, it is necessary to localize the MLD Snooping-applied multicast traffic. From a cost point of view, the economy would not permit the localization to be implemented in an inexpensive appliance.

“Desirably Secure QoS”

To assure the quality of a highly real-time-oriented application, such as IP telephony, etc. by absolute priority control, it is called upon to provide an absolute priority control feature with COS/TOS/TC/DSCP. The cost, however, makes it economically difficult to implement the feature in inexpensive equipment.

IPv6 Popularization Phase for Layer 1/Layder 2 Equipment

Requirements (essential)

1. Localize Multicast Traffic

Making MLD Snooping feature available allows for localization of multicast traffic

2. Secure QoS

By making a priority control feature available with COS/TOS/TC/DSCP, it is necessary to assure the quality of a highly real-time-oriented application, such as IP telephony , etc. At the same time, it is also necessary to assure the quality of those applications, which may require a certain band for video traffic, etc. under the band warranty.

Current Situation of Layer 3 and Higher Equipment (including composite equipment)

Some of the high-end model broadband routers commercially available have been already made compatible with IPv6 and with dual stack, too. Budget models involve a cost-inhibitive factor. The equipment working as connected with the host has been made applicable to IPv6 by means of an IPv6 bridge feature.

In a trade rental case, some of the router-built-in modems have been made applicable to dual stack. This is an IPv6-applicable broadband router most readily obtainable by the user in general at the present. It is being implemented in such a way as if the user said, "The equipment furnished after subscribing the service is found to be compatible with IPv6."

IP telephony has not been making progress in being compatible with IPv6 because the existing IP telephony services are subject to the prerequisite that IPv4 should apply. In a closed network, the IPv6-applied TV telephony services are available, indeed. Their connectivity with general IP telephony, subscribed telephones and mobile phones, however, has not been provided.

BCP in Layer 3 and Higher Equipment (including composite equipment)

Requirements (essential)

1. Compatibility with IPv6 in Broadband Routers

It is desirable to make a commercial available budget model (inexpensive model) compatible with IPv6.

First of all, it is called upon to implement a basic stack equivalent to IPv6 Ready Logo (Phase-1).

In addition, it is necessary for a site type connection to implement DHCPv6-PD, a promising IPv6 service system.　A PPPoE connection would require IPv6CP.

In the case of a host type connection, it is called upon to apply RA Proxy so as to process filtering with a broadband router without passing through a packet.

It is essentially necessary to make a firewall feature compatible with IPv6, too.　Static and dynamic packet filters are called upon to be implemented. Caution is essential to setting the ICMPv6 filter (problems, such as Path MTU Discovery, etc.).

In this stage, a naming solution is materialized in the IPv4 transport.　It is called upon to make the DNS Proxy feature compatible with AAAA records.　DDNS-compatible equipment is called upon to be compatible with AAAA records upon registration in DDNS.

Requirements (optional)

“Compatibility with IPv6 in Broadband Routers”

It is desirable to make a broadband router compatible with IPv6 from the following points of view:

- IPsec (to be used for remote access and for VPN communications with a specific remote terminal)
- Firewall Traversal (equivalent to NAT Traversal in IPv4, with UPnP promising: standardization is awaited.)
- Compatibility of security feature in security routers with IPv6,
- Implement an IPv6 over IPv4 tunnel.　(DTCP, Configured, 6to4, TSP, ISATAP, Teredo, etc.　Tunnel systems should be desirably standardized.　For services, a system with an authentication feature is desirable.)
- Implement an IPv4/IPv6 translator feature (NAT-PT, SIIT, etc.; case where you desire to enjoy IPv6 services at an IPv4 terminal, or vice versa.)
- MLD Proxy (Multicast traffic can be localized.　It will accelerate the popularization of multicast-applied low-cost live distribution/ VOD services.)
- Functions materialized by IPv4 are to be gradually made compatible with IPv6 (changeover to dual stack).
- Make priority control available with COS/TOS/TC/DSCP (to assure the quality of a highly real-time-oriented application, such as IP telephony or the like, and of those applications, which require a certain band for video traffic under the band warranty, and to establish a QoS policy in cooperation with trade services.)

IPv6 Popularization Phase for Layer 3 and Higher Equipment (including composite equipment)

Requirements (essential)

1. Implement the VPN protocol (IPsec, etc/)

   This is essentially necessary so as to make remote access and use VPN communications with a specific remote terminal to communicate with.
2. Firewall Traversal (UPnP)
3. Compatibility of Transport with IPv6

   This covers DNS and UPnP. The compatibility is required for communications at a terminal where nothing but IPv6 is serviceable. The IPv6 transport, moreover, is called upon to be compatible with GUI, such as WWW or the like, and with CLI, such as console/telnet, etc.
4. Compatibility of the security feature in a security router with IPv6
5. Compatibility of IP telephony with IPv6
6. Multi-homing

   IPv6 is required to employ a route selection method according to services (source address routing, Layer 4 and higher routing, etc.). It is necessary, moreover, to study a naming solution means (selecting DNS server according to services to be used). It is necessary to employ a starting point address selecting system as tailored to the form in which services are rendered (RFC3484 method, decide a starting point address according to the services).
7. MLD Proxy
8. Compatibility with priority control with COS/TOS/TC/DSCP

   The absolute priority control feature is used to assure the quality of a highly real-time-oriented application, such as IP telephony or the like, and of those applications, which demand a certain band, such as video traffic under a band warranty, to limit a band and to warrant a minimum band. It is called upon to establish a QoS policy in cooperation with the provider’s services and terminal equipment (to implement UPnP QoS).

Requirements (optional)

It is called upon to implement VPN in the Trusted 3rd Party model (it is possible to simplify settings and to manage an access list on a blanket basis) and to implement the Home Agent feature in Mobile IPv6.

Current Situation of Equipment for Collective Housing

As long as Layer 1/Layer 2 equipment is concerned, IPv6 is, in principle, out of consciousness. The equipment of this type includes a medium converter, a switching hub, a VDSL concentrator, a Home PNA switch, ONU, etc. Refer to the section relating to Layer 1/Layer 2 Equipment.

Layer 3 equipment involves a problem, such as authentication server, etc. See the explanation given above in relation to Layer 3 and Higher Equipment.

BCP in Equipment for Collective Housing

Requirements (essential)

1. Change Authentication Server over to IPv6

It is essentially necessary that the authentication server in DHCPv6-PD and IPv6CP be made compatible with dual stack.

2. Separate a user site with Layer 2/Layer 3 equipment (Refer to “Security SWG”)

It is necessary to separate RA, DHCPv6, etc. by IPv6 packet filtering. In the case of a host type, the setup router is required to take either of the actions referred to below so that residents living within an identical link may communicate to each other.

NDP Proxy

→ In case of communications between two terminals in the home, the sending terminal receives NA from two. If implemented in accordance with RFC2461, however, the content of NA from the proxy side is give priority because an override flag goes 0 (zero) for NA on the proxy side.

Put off on-link in RA , with ICMPv6 Redirect off in the router

→ Terminals in the home communicate to each other via a router.

Requirements (optional)

“Multicast Traffic Distribution: Layer 2 Equipment”

Making MLD Snooping available allows for a distribution of multicast traffic from user (room) to user (room).

“Desirably Secure QoS: Layer 2/Layer 3 Equipment”

Making priority control available with COS/TOS/TC/DSCP permits the absolute priority control feature to assure the quality of a highly real-time-oriented application, such as IP telephony or the like, and of those applications, which demand a certain band, such as video traffic under a band warranty. It is desirable to establish a QoS policy in cooperation with the provider’s services.

IPv6 Popularization Phase of Equipment for Collective Housing

Requirements (essential)

1. Remote Access Covered by Authentication Server

To terminate a remote access in the authentication server, it is necessary to provide a feature of distributing remote access communications to the home of each user. To terminate the remote access in each user home, it is necessary to provide a feature of authenticating remote-access communications after identifying them in the authentication server.

2. MLD Snooping Compatible : L2 Equipment

In this stage, it is necessary for every user to become able to distribute the multicast traffic.

3. Priority Control with COS/TOS/TC/DSCP: Layer 2/Layer 3 Equipment

In IPv6 Popularization Phase, it is called upon to assure the quality of a highly real-time-oriented application, such as IP telephony or the like, and of those applications, which demand a certain band, such as video traffic under a band warranty, to limit a band and to warrant a minimum band. It is necessary to establish a QoS policy in cooperation with the provider’s services.

Deployment Scenario in Players: Communication Network Provider

For the deployment scenario of a communication network provider, refer to the ISP SWG’s deployment scenario.

Deployment Scenario in Players: Service Provider

According to a classification by player, service providers are classified by form of communications as follows:

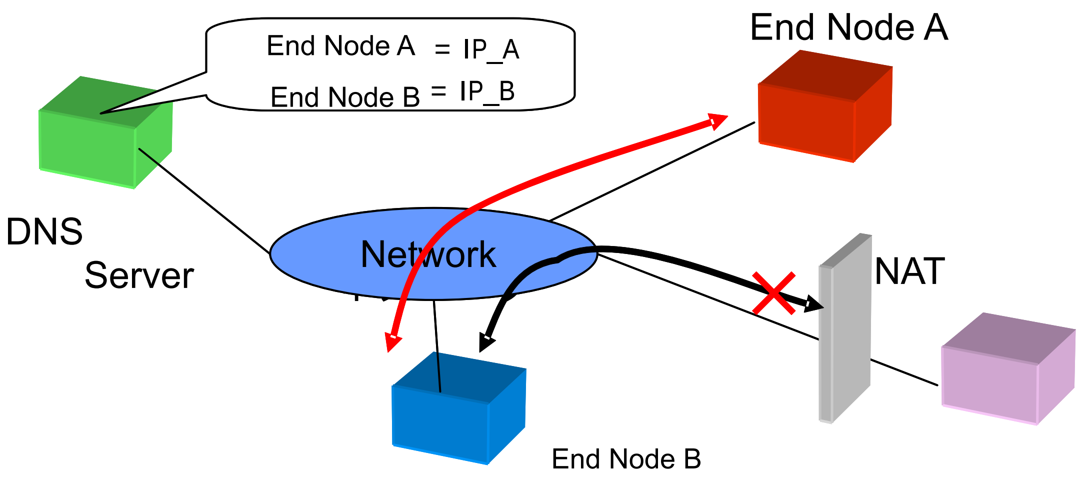
(A) Complete P2P type
(B) P2P+ Connection Management Server type
(C) P2P + Lobby Server type
(D) Client/Server type
(E) Client/Server (ASP Polling) type
(F) Client/Server (Client Post) type
(G) Home Server type
(H) Via Center Server type

Discussed hereinbelow are the deployment scenarios for various service providers according to the classification referred to above.

Current Situation of Service (A): Complete P2P type

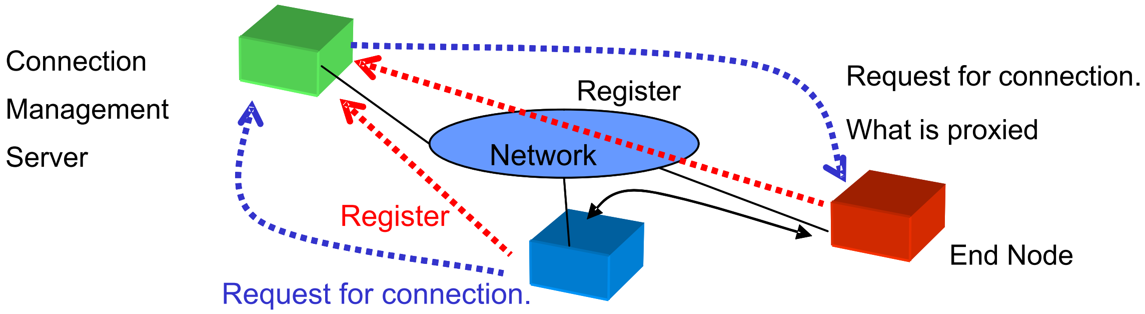
Under the current situations, the user behind NAT is disabled to make a direct connection, making it difficult to make use of P2P. Complete P2P type services, therefore, employ the mechanisms beyond NAT, such as static port forward and via-server (Service H types).

In this case, the address to which access be made is open to the public in DNS, etc.



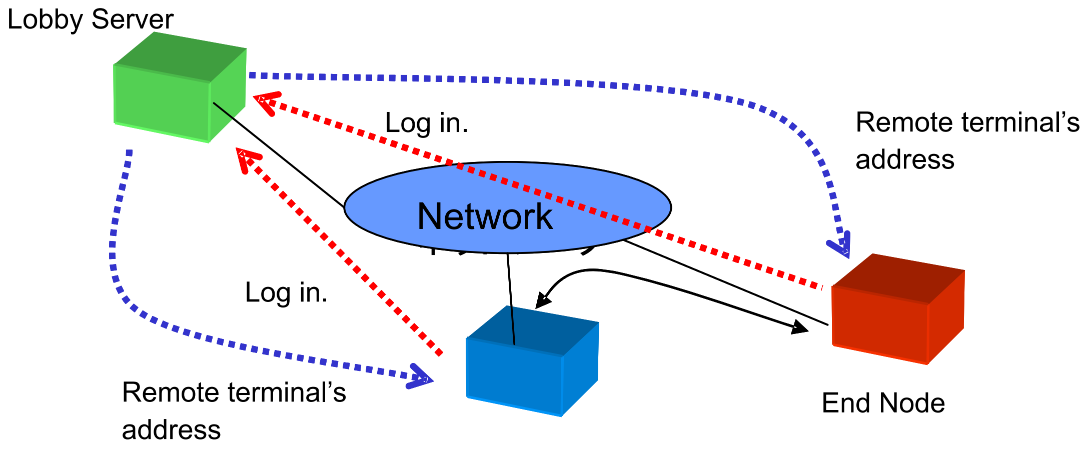
Current Situation of Service (B): P2P + Connection Management Server type

In services of this type, the Connection Management Server is used as a means of searching for a remote terminal to communicate with. In other words, it provides a function of judging the connectivity with a lobby server. As tailored to the current situation (IPv4), a back-end system (policy management, membership management, charging, support, etc.) is built up in full scale. With IPv4 services mainly rendered, some IPv6-applied services make debut in VoIP.



Current Situation of Service (C): P2P + Lobby Server type

In this service type, the lobby server is used as a means of readily finding out a remote terminal to communicate with. It may provide additional services, such as chat, storage and the like. And they are widely used in P2P type network games. The NAT problem does exist similarly to Complete P2P type.



Current Situation of Service (D): Client/Server type

Under the current situations, this is the network service form most commonly employed. The existence of NAT does not affect (in principle) communications.

A changeover of the server software to IPv6 has been already completed as far as famed software is concerned, such as WebServer, Mail (SMTP) Server, FTP Server and DNS server.

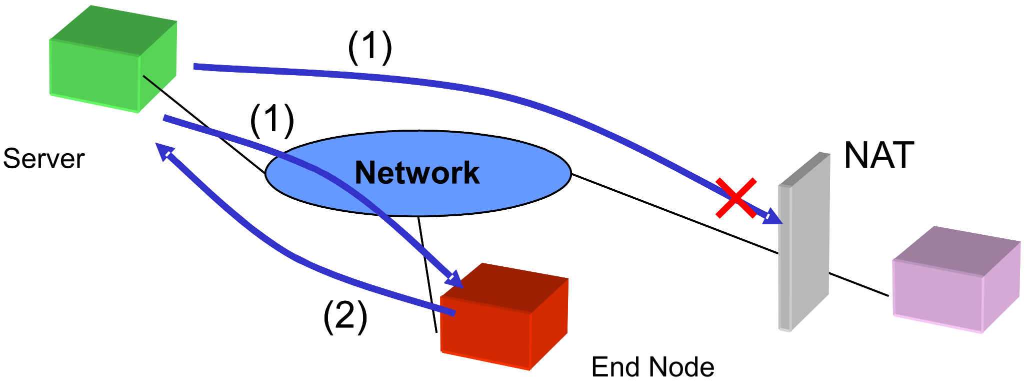
A changeover of the client software to IPv6 has been making progress in famed software, such as Web Browser, FTPClient, Mail (SMTP, POP and IMAP) Client and Remote Access.

What has been awaiting a solution by the infrastructure includes the connectivity with IPv6 on the client side of the network, DNS response issue (A and AAAA), and route problem (difference between IPv4 Route and IPv6 Route).

It has been pointed out that the software has compatibility deficiencies (unsatisfactory fall-back, access list nor properly functioning).

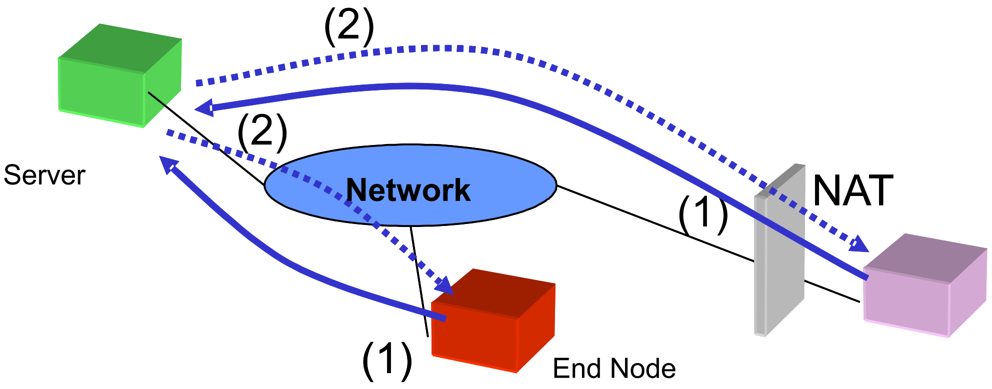
Current Situation of Service (E): Client/Server (ASP Polling) type

With NAT existing, it has been impossible to secure the direct reachability from ASP to a polling object node.　Consequently, this service type has been being scarcely used.



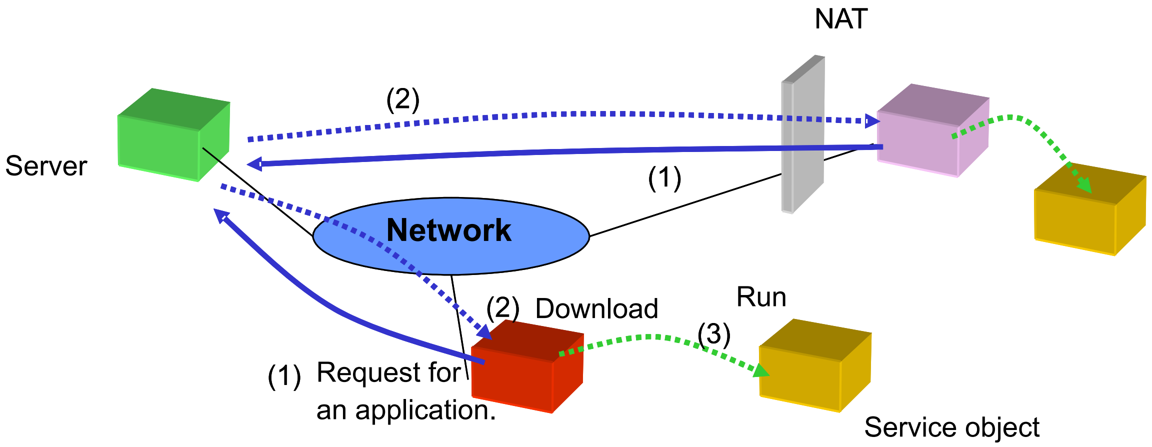
Current Situation of Service (F): Client/Server (Client Post) type

This service type is used in some application services making use of a network. In some cases, it is used to transmit information from a sensor or from a monitor camera. Since data can be sent to ASP without fail even with NAT existing, the Client Server type service is used as a substitute for Server Polling type.



Current Situation of Service (G): Home Server type

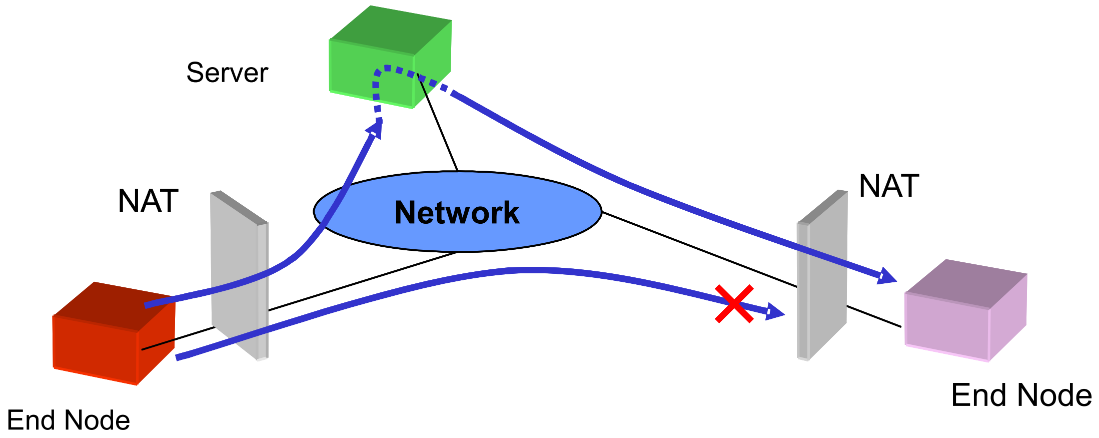
This is a composite form of Client Server type + communications closed in the home. Under the current situations, the service has been used scarcely. To ensure safety for an application platform, it is mostly incapable of communicating with any address other than a download source. It may well be considered that the service type is popularly used in such a form where no communications with any other node will follow the process of downloading as seen in a mobile phone application and in updating the firmware.



Current Situation of Service (H): Via Center Server type

This service type is used unless direct communications between end nodes are unavailable.

If both end nodes should be inside NAT in VoIP, for example, Service (H) is used as final substitute means. In some cases, moreover, a center node may be essentially required in VPN services from a protocol point of view. It may be safely said that the service type is often used to support the main services to be originally provided.



BCP Common to Services

Requirements (essential)

1. Make a protocol compatible with dual stack

To add IPv6 compatibility, it is necessary to reconfirm the protocol used in the service. To exchange the address information in the protocol, its modification will be required so that it will be compatible with both IPv4 and IPv6. The closest attention is essential to the use of a unique protocol, if any.

2. Make the server software compatible with dual stack

For compatibility with a server, two measures need be taken: one is to allow for IPv6 communications at the front end and the other to permit the IPv6 information to be handled as data at the back end.

3. Make (Client) applications compatible with dual stack

Unless either IPv6 or IPv4 turns unserviceable, a provision should be provided so that you may try an appropriate alternative method. The same applies to an application, which may perform P2P type communications, too. The service-related software, moreover, should allow for updating after shipment. This is because there are possibilities that the specification for the IPv6 base protocol may need to be reviewed in the BCP phase. It is essentially necessary to update the software that covers a bug fix and security. A delay or failure to take action might lead to a decline in evaluating the product. Action need be taken with consideration given to the Product Liability law.

In the following description about BCP, services will be analyzed model by model in the form referred to below.

Advantages of Selection

The advantages that the service provider could take by selecting the model are enumerated below.

Implementation Difficulty Level: Assessment in Five Grades 1 (Easy) - 5(Difficult):

A difficulty level is to be determined, with the following points comprehensively assessed:

- Technological difficulty (Difficult unless technologies required for services have been established yet)
- Work required to be done, coupled with a changeover to IPv6 (deployment/new implementation) (the more work, the more difficult the implementation will be)

- Size of external factors on environments at the lowest level upon start of services (the larger the size, the more difficult the implementation will be)
- Size of revenue sources envisaged (the smaller the size, the more difficult the implementation will be)

Requirements

To start up services in the BCP phase, arrange requirements in order.
(Enumerate the requirements for services as a whole, not from a network-oriented point of view only.)

Problems

About the problems involved upon startup of services in the BCP phase

To make a step forward

A description will be given about the points that must be improved before making a step forward (IPv6 Popularization Phase).

Outline of BCP Phase

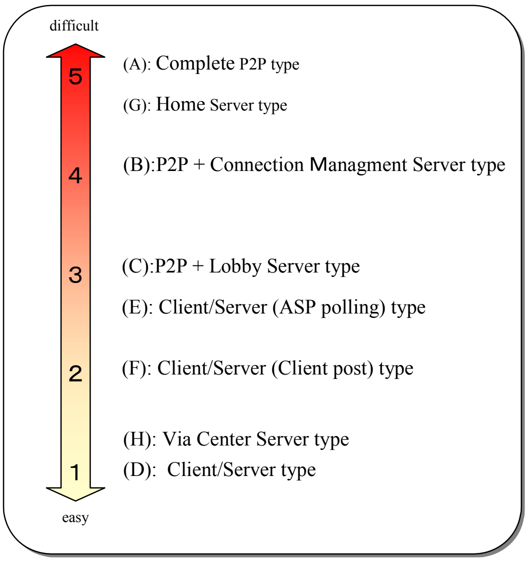
In this phase, it is difficult to rapidly start up services available from nothing but IPv6 while pushing them to the front.

Because a materialization of complete P2P services will be accompanied by technological difficulties (safe communications, naming solution, etc.) and a business model for services has not been found out yet. To materialize Home Server type services, the absence of a universal platform will turn out to be an issue awaiting solution. Multicast will limit usable access networks. In addition, it could not avoid jointly using the unicast tunnel. If software and hardware can be provided on a blanket basis, another approach, such as Client/Server (ASP Polling type) service, etc., will be available.

A changeover of the existing IPv4-provided services to dual stack could be materialized with ease. This holds true in all of the types, Client/Server, Via Center Server and Client/Server (Client Post).

Player Deployment Scenario （Service provider Edition)

- BCP Phase Overview



difficult

5 (A): Complete P2P type

(G): Home Server type

4 (B):P2P + Connection Managment Server type

3 (C):P2P + Lobby Server type

(E): Client/Server (ASP polling) type

2 (F): Client/Server (Client post) type

(H): Via Center Server type

1 (D): Client/Server type

easy

- It is difficult to rapidly start up services available from nothing but IPv6 while pushing them to the front.
  - Complete P2P Service
    - Technological difficulties (safe communications, naming solution, etc.)
    - No business model is available for service.
  - Home Server type service
    - Universal platform does not exist.
  - Multicast
    - Network is restricted
      - Access network is restricted.
      - Unicast tunnel is used jointly.
  - Where software and hardware may be provided on a blanket basis, another approach is available.
    - Client/Server (ASP Polling type) service
- A changeover of the existing IPv4-provided services to dual stack could be materialized with ease.
  - Client/Server type
  - Via Center Server type
  - Client/Server (client post) type

Service (A): Complete P2P type BCP

Advantages of Selection

Selecting this service type has an advantage of materializing the communications free from any influence of a third party or parties. It is possible to secure the reliability independent of any third parties and to materialize a low delay in end-to-end communications.

Implementation Difficulty Level: 5

○ The software development difficulty is at a low level.

× There are a lot of technological problems involved in the network, more specifically, naming solution (inquiry and registration), cooperation with the firewall, access control (in case where existing services are available) and coexistence with the IPv4 user.

× There are a lot of external factors required to implement this service, including the above-mentioned technological problems, IPv6 access to the Internet and so on.

○ Considering that a business model for services has not been established yet under the current situation, it is inevitable to resort to the sales of software and to some support services. Since it has a narrow scope of deployment, however, the service type may be taken for a system easy to implement in any aspects other than business.

Requirements

A requirement is to operate a dynamic DNS server.

Problems

Inevitably DNS is used to disclose an IP address to the public. It involves a fear of developing into a privacy issue. Besides, the software will be cut and sold. And it will raise another problem that the income sources are scarce.

To make a step forward

Some technological issues are called upon to be dissolved, including the compatibility of publicized naming solution technology, such as dynamic DNS or the like, with privacy, security in P2P communications (employing a universal encryption system and an easy restriction on access) and so on.

In addition, it is necessary to secure an income source other than the software sales. A conceivable business model would be to earn the income by providing a kit of hardware, software and support services necessary to use the service.

Service (B): P2P + Connection Management Server type BCP

Advantages of Selection

The advantages arising from selecting this system are as follows:

- Able to dissolve the problems involved in naming solution since Connection Management Server is used to determine a remote terminal to communicate with,
- Able to improve the safety because the Connection Management Server controls communications and intervenes in exchanging encrypted keys, and
- Able to expect a continuous income of membership fees through the Connection Management Server.

Implementation Difficulty Level: 4

○ This system will improve safety because a management server intervenes. In a combination with the Trusted 3rd Party Model, the system will further improve the safety.

○ It may be safely said that the system shows a low level of the difficulty in developing the P2P software.

× (With the existing services available), there are some difficulties for IPv6 and IPv4 to coexist.

× Connection Management Server and Back-end Server (data) need be made compatible with IPv6.

× (Under an IPv6 environment), it is necessary to accumulate the know-how in operating the Management Server and managing and applying the Connection Policy.

△ It may be safely said that there are a relatively small number of technological problems except for cooperation with the firewall.

△ It may be said that there are a slightly large number of external factors required, such as technological problems referred to above, IPv6 access to the Internet, etc.

○ A continuous income may be expected to arise from providing members with the Connection Management Server.

Requirements

Requirements are to operate an IPv6-compatible Connection Management Server and to make the working internal data format compatible with IPv6.

Problems

In case where services have been offered in IPv4, it will raise a problem to coexist the user who has been already using the IPv4 environment. Even if applications and the server are made compatible with dual stack, it is still difficult to communicate with the IPv4 NAT user.

Since the Connection Management Server and the Back-end Server will become a single point of failure, it may be said that the running cost is high.

To make a step forward

Toward the next step, it is called upon to:

- Enhance the affinity with IPv4 . (Provide a translator feature, using the form of Service (H) or otherwise.)
- Secure the safety of communications (especially in the zones of P2P communication and of communications with the Connection Management Server)
- Improve the quality of the P2P communication zone (quality improvement all over the network, such as backbone, access, etc., including QoS)
- Implement a large size by introducing all-in-one packages (a changeover of the access circuit to IPv6, and hardware/software support)

Service (C): P2P+ Lobby Server type BCP

Advantages of Selection

This system is to use the Lobby Server to determine a remote terminal to communicate with so that the naming solution-related problems can be dissolved. The user need not be strongly conscious of P2P communications.

An opposing node has its IPv6 address notified by the Lobby Server. There are possibilities, therefore, that the system may be applied to the firewall control in the future.

In addition, a continuous membership fee income could be expected by way of the Lobby Server.

Implementation Difficulty Level: 3

○ It may be safely said that the P2P software development shows a low difficulty level.

× (With the existing services available), there are some difficulties for IPv6 to coexist with IPv4.

× Lobby Server and Back-end Server (data) need be made compatible with IPv6.

○ It may be safely said that there are a relatively small number of technological problems except for cooperation with the firewall.

△ There are a slightly large number of external factors required, such as technological problems referred to above, IPv6 access to the Internet, etc.

○ A continuous income may be expected to arise from providing members with the Lobby Server.

Requirements

This system is required to operate an IPv6-compatible Lobby Server and to make the working internal data format compatible with IPv6.

Problems

(In case where services have been offered in IPv4,) the system will raise a problem of coexistence with the user who has been already using the IPv4 environment. Even if applications and the server are made compatible with dual stack, it is still difficult to communicate with the IPv4 NAT user.

Since the Lobby Server will become a single point of failure, the running cost will be apt to be high.

To make a step forward

Toward the next step, it is called upon to:

・ Enhance the affinity with IPv4 . (Provide a translator feature, using the form of Service (H) or otherwise.)

・ Improve the ability to attract customers thanks to additional features available with the Lobby Server.

・ Secure the safety of communications (especially in the zones of P2P communication and of communications with the Lobby Server)

・ Improve the quality of the P2P communication zone (quality improvement all over the network, such as backbone, access, etc., including QoS)
・ Implement a large size by introducing all-in-one packages (a changeover of the access circuit to IPv6, and hardware/software support)

Service (D): Client/Server type BCP

Advantages of Selection

This system allows for an implementation of IPv6 without the necessity to change most of the existing services.

Implementation Difficulty Level: 1

○ There are few technological problems. Since the communication form is identical with that of IPv4, the same technologies as those for IPv4 are applicable as they are.
○ An open-source family of server software has been almost completely made compatible with IPv6. A unique server, if employed, however, need make its software compatible with IPv6.
○ The infrastructure (data center, etc.) have made progress in its buildup.
* Refer to the section relating to “Data Center,” too.

【NOTE】

This service type would not allow for direct recovery of the cost incurred on a changeover to IPv6.

▶ Because the current situation (IPv4) has already achieved what is identical with IPv6.
▶ To recover the cost for a changeover to IPv6, it is necessary to implement those services which would uniquely make effective use of the advantages available in IPv6. Services (B) and (E), for example, may be considered jointly usable. This form might well be taken for a transition step to that end.
▶ A relatively minor advantage, such as elimination of NAT Traversal, is available. Nevertheless, it is considered insufficient to recover the transition cost.

Requirements

An IPv6-compatible front-end server need be operated. It is necessary that the internal data format to be used for the service should be made compatible with IPv6.

Problems

Challenges to be tackled with are operator training and log management. It will be necessary to make a deployment of the large-scale back-end database. Especially when making a deployment of actually working data, the closest attention is necessary.

To make a step forward

Toward the next step, it is called upon to make directly effective use of the advantages available in IPv6 in addition to an improvement of reliability on the Server and to an establishment of log management techniques.

Service (E): Client/Server (ASP Polling) type BCP

Advantages of Selection

The existing (back-end) server equipment may be applied so that the initial cost requirements can be suppressed. This system allows ASP to provide information in arbitrary timing. In addition, it permits us to grasp a network band, which will be used for polling from ASP.

Implementation Difficulty Levels: 2 - 4

△ It may be said that there are a slightly large number of technological problems. Since the small built-in equipment is expected to make debut, problems peculiar to such equipment will take place.

△ To make a deployment from the existing service of C/S type, it is necessary to make a deployment of the back-end server and data.

△ It is necessary to install a private appliance (or software) applicable to polling on the user side. If software and hardware can be provided on a blanket basis, however, it may well be taken for an advantage. It is difficult for BCP to adopt a formation where software only or additional service only are provided.

○ It is possible to let the user unconsciously make use of IPv6. Telemetering, for example, can deploy as a total solution, which contains an access circuit and equipment.

Requirements

A deployment to IPv6 would require us to provide the IPv6 polling-compatible equipment and software and to operate ASP stably (to mange collected data). To make a deployment from the existing services, moreover, it is necessary to make a deployment of the back-end server, too.

Problems

First of all, the balance between polling interval and service quality will turn out to be a problem. Narrowing the interval will require a band more.

It will be a challenge of ours, moreover, to secure the reachability of equipment installed in the home, especially to cooperate with the firewall.

To make a step forward

Toward the next step, it will be called upon to accumulate the know-how to gather data by polling (to manage both polling interval and band), to reduce the size of a node to be polled, to save electric power and to lower the price. In addition, it will be a challenge to secure a safe path of communications.

Service (F): Client/Server(Client Post) type BCP

Advantages of Selection

This service type allows for an implementation of IPv6 without the necessity of changing most of the existing services. Since the initial operation is left to the customer, it is easy to let an IPv4 node coexist with an IPv6 node. In the future when the IPv6 user population increases, there is a likelihood that Service (F) may make a deployment to ASP Polling type. Then, it will be able to enjoy the advantages available in ASP Polling type.

Implementation Difficulty Level: 2

○ Service (F) has a small number of technological problems only. Since it has the same communication form as that in IPv4, the same technologies as those in IPv4 may be applied as they are. Since the small built-in equipment is expected to make debut, problems peculiar to such equipment will take place.

△ To make a deployment from the existing services of C/S type, it is necessary to make a deployment of the back-end server and data.

○ It is possible to let the user unconsciously make use of IPv6. Once the equipment has been made compatible with dual stack, IPv4 can provide services likewise. After the home network has been connected to IPv6, furthermore, Service (F) may be switched over to Polling type.

○ It is possible to draw such a deployment scenario as “IPv4 Post type → IPv6 Post type →IPv6 Polling type.”

Requirements

What is required includes the equipment and software that have a function of posting information under IPv6, including a stable supply of software. To make a deployment from the existing service, moreover, it is necessary to make a deployment of the back-end server.

Problems

How to balance the post interval to be set by the client with the service quality is a problem awaiting solution. Too narrowed an interval would consume the larger band.

If event-driven (coupled with an increase in number of nodes), it is undeniable that DoS may be generated by nature. An event-driven case, moreover, has a feature that the traffic pattern may be assumed.

To make a step forward

Toward the next step, it is called upon to accumulate the know-how to gather data using a lot of nodes, to control the interval of data posted by the client, to manage the band on the ASP side, to reduce the size of a node in which data be posted, to save electric power, to lower the price and to secure a safe path of communications.

Service (G): Home Server type BCP

Advantages of Selection

This system has an advantage that a downloaded portion of applications will be covered by C/S type services. With a monthly rating system introduced, a continuous income may be expected to come in. Besides, it is a form, with which the user has been familiarized, such as a mobile phone application or the like.

Implementation Difficulty Level: 5

× Neither interface nor protocol has been established yet to let two or more nodes cooperate to each other in the home.

× No method has been established yet to secure the safety when a downloaded application communicates with another node.

Requirements

It is called upon to establish a platform for the home server to run, and an application platform , such as an interface to control intra-home nodes, etc. It is necessary to supply the platform with a downloaded application.

Problems

Problems may be pointed out as follows:

- How an application has safety assured is a problem. More specifically, is there any means that permits to make certain how the safety of applications is ensured while allowing an accessed node to be sure that access is made by the application whose safety has been assured.
- It has been also pointed out as a problem that too small a number of application platforms/software would fail to make business. Specifications need be made commonly applicable (example: mobile phone application) . If a closed platform should be acceptable, the service may be started at once.

To make a step forward

Toward the next step, it is called upon to provide a safely running environment. To this end, there is a method of communicating by means other than IP/IPv6 at a downloading site (infrared rays?, for example).

It is called upon, furthermore, to establish the common specifications of application platforms, too.

Service (H): Via Center Server type BCP

Advantages of Selection

This service type has advantages of its selection as follows:

- Since each communication is of simple C/S type, the existing technologies may be applied.
- A server is used to provide communication control so that safety can improve.
- A reliable server intervenes in exchanging the encrypted key so that safety will improve.
- A server performs the translator function so that an IPv4 node and an IPv6 node can materialize intercommunications.
- The center server conceals a communicating remote terminal so that privacy can be protected at a high level.
- The center server, which does not fail to intervene, may be used for charging.

Implementation Difficulty Level: 1 - 2

○ Service (H) involves a very small number of technological problems and provides a form of communications identical with IPv4. The same technologies as those under IPv4 may be used as they are. The translator, moreover, is relaying at an application level, so that it can

securely relay.
△ To make a deployment from the existing services, it is necessary to make a deployment of the back-end server and data, too
○ It is possible to easily materialize the coexistence with IPv4.
○ Server subscription fees allow a continuous income to be secured.

Requirements

It is called upon to make relay servers compatible with IPv6, especially at the front end where a connection from subscribers are processed and at the translator unit where the subscribers using IPv4 are interconnected with those using IPv6.

It is necessary, moreover, to make the back-end server able to handle IPv6 information as data.

Problems

What could be taken up as a problem may be described in two aspects: one is a rapid increase in traffic and sever load according as the number of users increases, and the other is the server that will turn out to be a single point of failure.

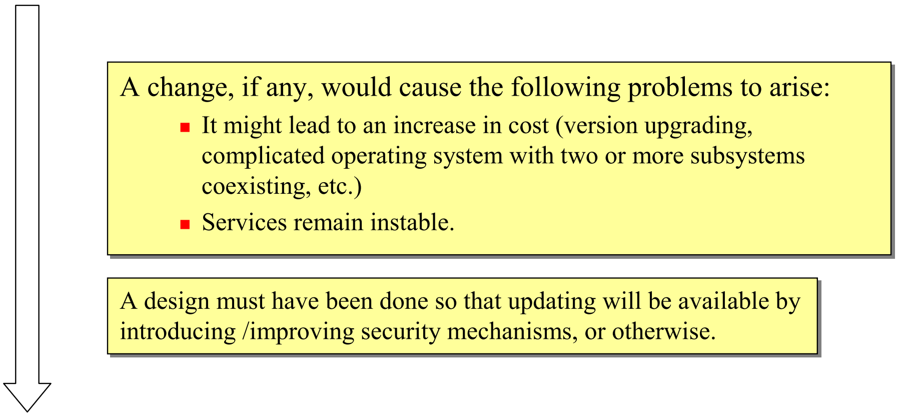
To make a step forward

Toward the next step, it is called upon to establish a safe relay-operating server (to be provided as the server, on which subscribers may rely together). It is called upon, furthermore, to accumulate the operational know-how to avoid a concentration of traffic.

What has been referred to hereinabove is the BCPs by service form. As far as service providers are concerned, it may be generally pointed out that once the BCP phase has been reached, what is contained in the services rendered during the phase does not have so significant discrepancies from those to be provided in the IPv6 popularization phase. If these discrepancies should be significant, to the contrary, the cost will increase all the more. And the services rendered will turn instable. During the BCP phase, therefore, it is necessary to fully verify such discrepancies and to accumulate the know-how involved.

Player Deployment Scenario (Service Provider Edition)

Service providers' IPv6 Popularization Phase (Transition Completion Phase) is considered not so significantly different from the BCP phase.



A change, if any, would cause the following problems to arise:

- It might lead to an increase in cost (version upgrading, complicated operating system with two or more subsystems coexisting, etc.)
- Services remain instable.

A design must have been done so that updating will be available by introducing /improving security mechanisms, or otherwise.

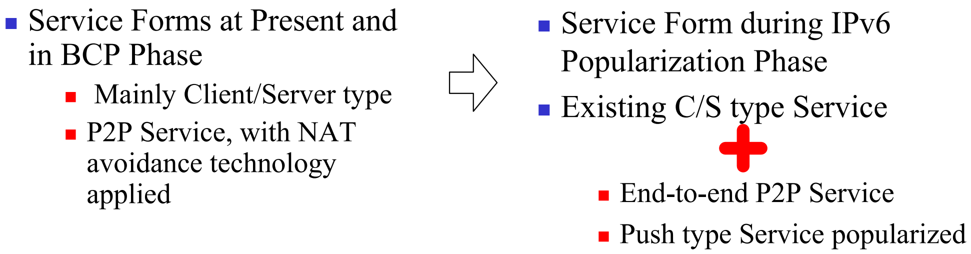
It is important to perform a plenty of simulations, tests and trials (Beta service) during the BCP phase fully repetitively.

Regarding the changes in service form, the following may be pointed:

Predominantly prevailing at present and in the BCP phase are the existing C/S type services and those P2P services, which are using a variety of NAT avoidance techniques. In the IPv6 popularization phase, however, end-to-end type P2P services and push type services will come to be popularized.

During the period when such new forms of services are being diffused together with IPv6, there are some points to be noted duly. In other words, it is called upon to establish a scheme capable of rendering services fully for an immense number of terminals in addition to an accumulation of the operating know-how in a new form of services.

For such a new form of services, moreover, it is necessary to fully study in advance whether or not an IPv4 terminal be supported and how the user support be provided.



- Service Forms at Present and in BCP Phase
  - Mainly Client/Server type
  - P2P Service, with NAT avoidance technology applied

- Service Form during IPv6 Popularization Phase
- Existing C/S type Service

+

  - End-to-end P2P Service
  - Push type Service popularized

<u>Rise of New Service Forms</u>

- For a new service form.
  - Importantly, create a system capable of rendering services to an immense number of nodes, and
  - Accumulate the operational know-how.
- Desriably, define a procedure for addressing an IPv4 node expressly.
  - Whether or not you should support, including its time duration,
  - In the event of fault, when supporting the user, and so on

Requirements for Service Provider in the Pv6 Popularization Phase

The IPv6 popularization phase is considered to come up with “Services are expected to deploy laterally,” including an expansion of sensor uses, etc.

In the BCP phase, for example, a burglar sensor has been communicating with a private ASP only. In the IPv6 popularization phase, it will come to send data to a universal appliance, such as PC, intra-home controller or the like. As a result, it will be possible to materialize centralized monitoring in the home.

For another deployment conceivable in the IPv6 popularization phase, furthermore, the sensor capable of communicating during the BCP phase with the ASP, which offers a security service only, furthermore, will come to supply data to the ASP, which offers a home health care service.

Consequently, the following technological requirements will come up:

- Standardize service (application) protocols.
- Establish a technology to convert service (application) protocols to each other.
- Establish techniques for service discovery and naming (refer to the section titled “Naming”) in the home. (Strictly speaking, these are not to be offered by a service provider.
- Thoroughly protect the collected information for private information protection.

The IPv6 popularization phase will be the times for “what is being communicated will be closely related with the user’s life,” far more than ever.

Sensors will far more widely cover the information to be collected. This will bring about the feasibility of effective using the characteristics of an end node with an IPv6 address. And letting such information cooperate to one another will permit more significant services to be offered. To that end, it is called upon to employ an interconnectible authentication/ encryption mechanism, which will be also associated with the lateral deployment as already referred to. In this sense, a safe and easy technique is expected to appear.

For a technological requirement, an easy or user-skill-free encrypt authentication system must be employed. There are two essential requirements: one is an encryption mechanism capable of securely protecting information, and the other is an authentication mechanism capable of limiting information users.

Impact of Service Providers on Network Infrastructure during Deployment: BCP → IPv6 Popularization Phase

Deployment from C/S to P2P

This deployment brings about a reduction of the traffic flowing into service providers (ASP). Nevertheless, there are possibilities that such traffic reduction may not arise if lobby and connection management servers come to provide additional features (chat, bulletin board, etc.) because such additional features are of C/S type.

If a server should offer an IPv4-to-IPv6 converter feature in the deployment phase, moreover, there are possibilities that the traffic flowing via the server may show a rapid increase. In this sense, special attention must be paid to the initial stages of the deployment from BCP to the IPv6 popularization phase (after the service has been recognized by the user in general).

And such an increase in inter-user traffic will be followed by a change in pattern of the backbone traffic.

Popularization of Small Built-in Nodes with IPv6-applied

To render the Client Post type service, it is important to correctly grasp its inflow traffic, frequency and regularity. A service of this type is incapable of controlling the nodes requesting for a connection. Consequently, the Client Post type service is inherently inclined to make the problem far more serious than the ASP Polling type service.

The back-end server (database and administration system) is considered to be built up and modified sufficiently, based on the know-how accumulated in the IPv4 currently available.

4. Challenges to be Tackled toward IPv6 Popularization Phase

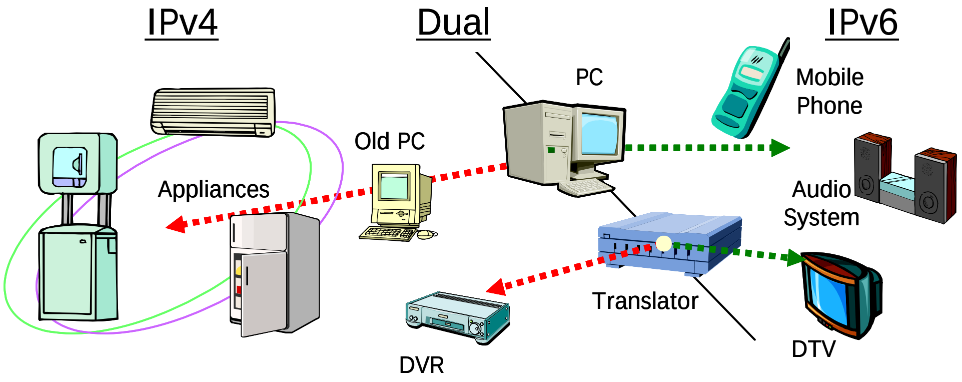
Challenges toward IPv6 Popularization Phase

Translator Feature

The term, translator feature, means the technology to materialize a conversion between IPv6 and IPv4. NAT-PT, ALG and TCP Relay, for example, may be taken up. For NAT-PT, it is scheduled to provide "IPv6 Ready Logo Program Phase-2."

The translator has its advantages depend upon the necessity to let the equipment applicable to IPv6 only cooperate with the one applicable to IPv4 only. Especially an implementation of the translator in the home is dependent upon a status of each home. It may be safely said that, if there are a larger number of IPv4 appliances in the home, the translator will work effectively, but if not, it will be less effective.

Nevertheless, the translator should be implemented if its usage is expressly defined or if the vendor desires to secure an intercommunication with a ready-made product.

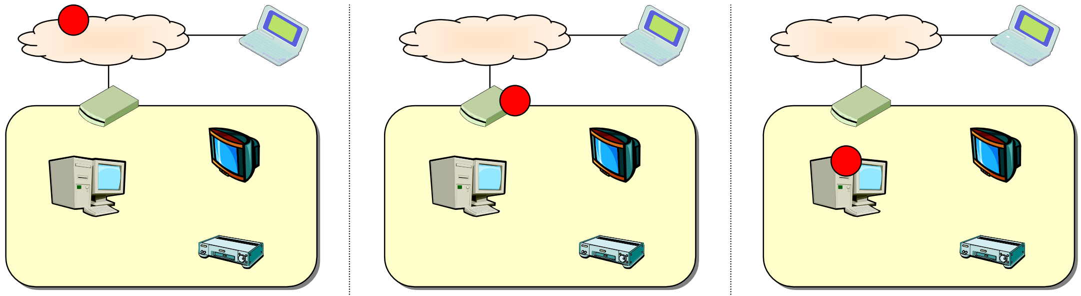


Where to locate the translator feature is application-dependent.

The illustration below shows the advantages and disadvantages of three translators classified by location: outside the home, on a router, and on a PC,

Translator Functions

- Location: Dependent upon application



Located outside the home

- Provided as part of remote access services

【Advantage】

- Complicated settings not required in the home

【Disadvantages】

- IPv4⇔IPv6 inconvertible in the home
- Unavailable to make access to IPv4 node in the home

Located on a Router

- Provided as one of the functions available in a broadband router.

【Advantage】

- Bilaterally convertible IPv4⇔IPv6 (with router having global IPv4 address)

【Disadvantages】

- Router settings complicated
- Security downgraded due to a mistake in design

Located on a PC

- Provided as one of software on a PC

【Advantage】

- Easy to implement since it is a PC application.

【Disadvantages】

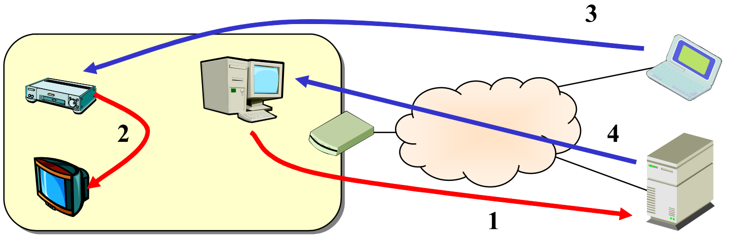
- PC settings complicated (as related with Personal firewall, etc.)
- Difficult to use from another appliance

Naming

“Naming” is a general term used to express a functional method relating to registration/ solution and DNS server discovery, including how to give a name. Methodologically, naming requires a query sending procedure, a DNS server discovery means and a transport protocol. Naming is classified by naming solution purpose as follows:

- Functionally ･･･ Registration/solution, DNS server discovery and naming technique
- Methodologically ･･･ How to transmit a query, how to find out DNS server, and transport protocol
- Classification by Objective of Naming Solution

	Who?	Whom to dissolve?
1	Node inside the home	Node outside the home
2	Node inside the home	Node inside the home
3	Node outside the home (w/reliable relationships)	Node inside the home
4	Node outside the home (w/ reliable relationships)	Node inside the home



- Case 2 is closely related with a service discovery
- Cases 3 and 4 necessitate arguments about how to furnish a node outside the home with information, including safety involved.

Issues on Naming Solution in the Home

If an intra-home node desires a solution to another intra-home node, it is necessary to study the following items:

DNS Server Discovery Process

This process prompts you to judge which you desire to use, Multicast or Anycast, Automatic Setting Protocol or Manual Setting one, and Sever-free System or Server-working one.

Information Equipment Registration

To register an equipment name, it is necessary to study which you desirably use, DNS framework or non-DNS one, and how you desirably register an IP address and other additional information.

Query Model

For an inquiry form, you must study some choices, such as Multicast, Anycast, Unicast and ICMPv6 Node Information Query.

Domain Name

To use the DNS framework to decide a domain name, the following points must take into consideration: which domain the home should use, whether or not it should be transferred by ISP, and whether or not the user should give an appropriate domain name.

Proposed Action for Naming Solution in the Home

The issues to be studied as referred to above should be addressed as proposed below:

DNS Server Discovery Process

Automatic settings are essential to this process, considering that the equipment without any setting interface does exist.

Using the well-known Anycast and Multicast will allow you to omit a setting operation. Nevertheless, it is necessary to study some aspects associated with security.

In the argument (draft-ietf-dnsop-ipv6-dns-configuration) by IETF, three methods, RA, DHCP and well-known Multicast, are enumerated and have not yet narrowed down into one. This draft has arranged in order the advantages and disadvantages involved in each of the three methods.

If an IPv6 popularization scenario with the lead taken by the non-PC equipment should be drawn up, there are possibilities that another method may emerge without resorting to the DNS server.

Query Model

Unicast remains unchanged from the existing DNS.

Anycast will permit inside and outside servers to be shared by using the server that supports recurrent inquiries. An Anycast address may be distributed in DHCP, or it is also possible to define an address in well-known (undefined under the current situation).

For Multicast, individual nodes need be compatible with multicast naming solution. In addition, it is necessary to provide a server for naming solution through an external DNS server because Multicast DNS does not transfer an inquiry.

ICMPv6 Node Information Query is not a DNS. The program, therefore, need be modified. On the query side, first of all, the resolver should be modified so that it will be available as an ordinary naming solution mechanism on the OS. On the response side, it will be also necessary to respond to a node information query.

Anycast/Multicast DNS involves a security problem. In other words, it does not provide any warranty on the protocol in relation to which server should receive and from which server the response should return.

Registering the Equipment Information

It is a difficult job to register an IPv6 address in DNS (or a remote terminal means) because some equipment does not have a display unit and/or an input device. In addition, an automatic registration means is required, considering that the world in the IPv6 popularization phase may have a number of nodes connected. Consequently, the connection detector (address changer) feature, such as DNS UPDATE or the like, is called upon to cooperate with the automatic registration.

For a correlation with a physical location, it is desirable to make access as if it were felt like an “entrance camera” rather than “camera01,” with the user-friendliness taken into consideration. “camera01” may be acceptable as the information to be registered on DNS. To make it visible for the user, however, the information need be converted.

Problems to be taken up in relation to the equipment registration are “to what range the registered information be open to the public, that is, how to treat the privacy” and “How naming be discriminated if there should be two or more appliances under an identical model number.

Issues on Solution to Naming from Outside the Home

Solutions to naming in the home have been discussed as referred to above. In case where a node outside the home desires to solve naming inside the home (i.e., Cases 3 and 4 according to the classification already referred to), the issues involved include the following registration-related points:

- How to use DDNS and/or DNS update.
- Where to register has some choices, such either server provided by ISP, by an equipment vendor or by a third party.
- Necessary to determine the information and equipment to be registered.
- Necessary to define where and what information be open to.
- Must secure the privacy.

Solutions to Naming from outside the Home

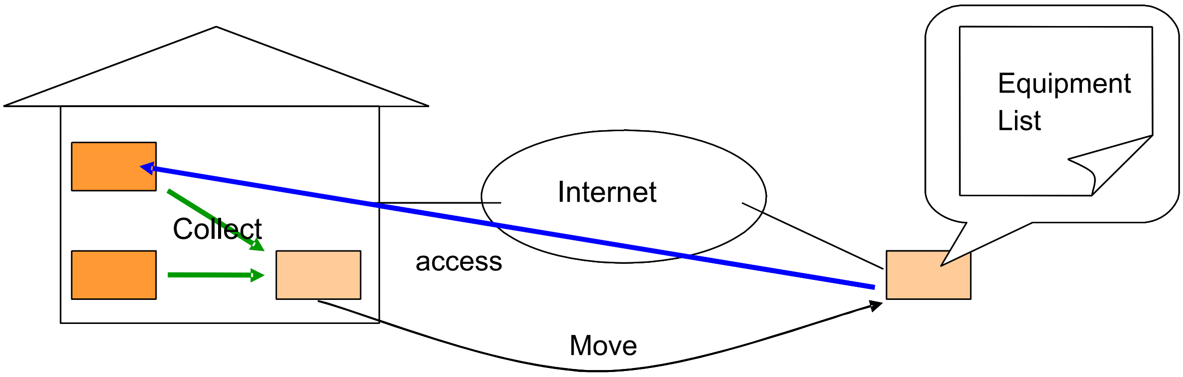
As a prerequisite to any countermeasures you may take, there is a fact that the home at large cannot operate a DNS server (to make information open to outside the home).

There is a domain name assignment issue, too. Naturally, the home is unable to manage a DNS server. Nevertheless, the home is relaying a DNS query while using a simplified DNS server indeed.

A policy fundamental to the solution should be either of the two: a solution found out in nodes inside the home, or information resident on the Internet. More specifically, the following models are conceivable:

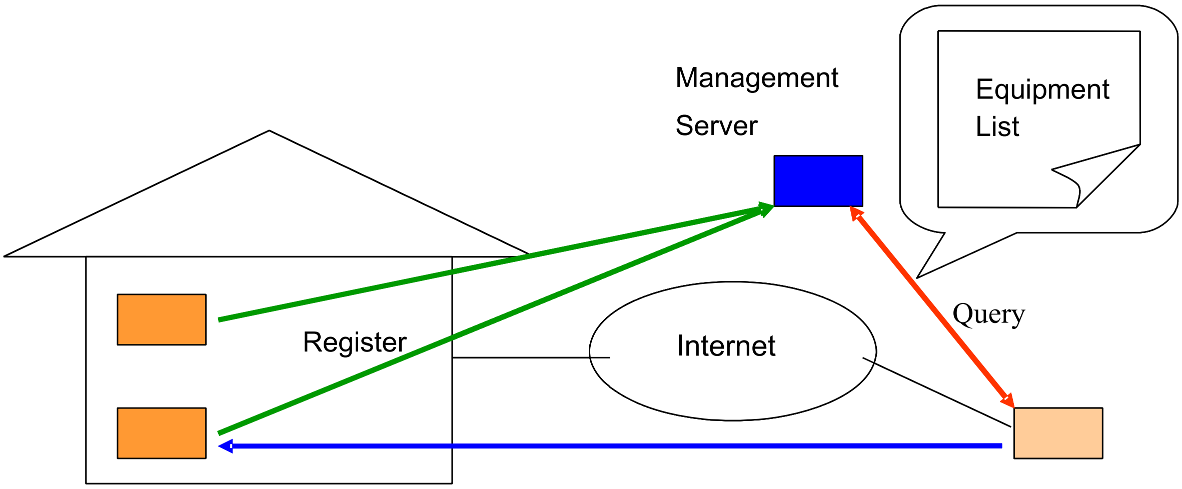
Prior Collection Model

For example, each terminal is assumed to have /etc/hosts. In this case, the information exists inside the node only and safe enough. It is necessary to set node by node. An alternation of address could not follow the completion (delivery) of setting.



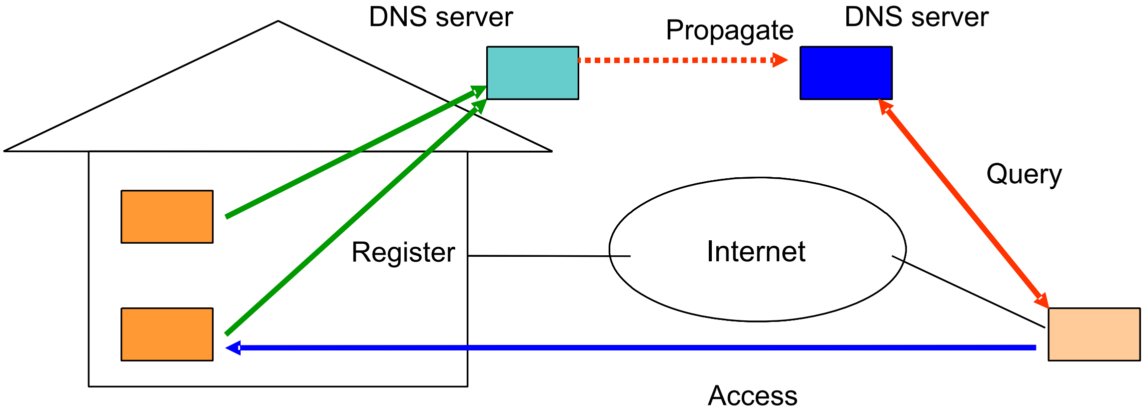
Centralized Server Management Model

This is a model where a contracted sever is used for management. An already registered node only allows for access. A registration may be made under the software for the exclusive use.



Existing DNS Model

This is a technique for registering in a DNS server as usual. An already registered node only allows for access. A registration may be made under the software for the exclusive use. In this case, however, there are some challenges to tackle: i.e. information disclosure and privacy issues.



Other Issues on Naming

The following points may be taken up as miscellaneous issues on naming:

Select a transport protocol

Anyway, the dual stack is desirable. It is considered desirable that at least the server side provides a wide coverage. Considering that a router (for household) will be equipped with the dual stack sooner or later, the dual stack is problem-free.

Multi prefix/Multihome Environment

In IPv4, the PPPoE multi-session is used to implement the multihome. In addition, a means of properly routing a DNS query has been also implemented. Nevertheless, it is often set statically. In IPv4 that has NAT, any multihome related issues have never been visualized yet. An end node was not required to be concerned about the multihome.

For IPv6, however, it becomes important to select a source address. Unless DNS responds properly, there is a fear that the source address selector may not operate properly.

DNSSEC

To secure the security for DNS, moreover, it remains unknown how DNSSEC will come to be used in the future.

Naming the non-PC Equipment

There is another challenge: if there are two or more non-PC appliances under an identical model number (there are two or more TV sets and video/DVD recorders), how could we discriminate each of them? It is called upon to give naming intelligible for the user in case of listing equipment names in an application. Especially, each equipment name should be desirably correlated with its location in the home by naming like “entrance camera,” “living room air-conditioner” and so on. It is called upon, moreover, to automate such naming process, if possible.

Revision Records

Year 2004 Version

Newly published

Year 2005 Version

Revisions

- Added a deployment scenario in the home network.
- Renamed “based on events” → “in the home network”
- Added B｜R : IP Bridge-borne IPv4 Router.
- Detailed security items.
- Added “Scenario in Players.”

Members of Home Segment, DP-WG

(titles omitted)

FY’03 Members

SWG Chair

Koji Kubota (Matsushita Electric)

Study Members (titles omitted in kana order)

Arano (Intec NetCore, Inc.)
Ishihara (Toshiba)
Ozawa (Matsushita Electric)
Onoue (Matsushita Electric)
Kawashima (NEC Access Technica)
Kikuyama (Matsushita Electric)
Sadata (NTT Communications)
Shimada (Matsushita Electric)
Suzuki (Matsushita Electric)
Segawa (Panasonic Communications)
Nakai (NTT Communications)
Nakamura (Matsushita Electric)
Murata (Panasonic Communications)
Yamatani (Arise)

FY’04 Members

SWG Chair

Mitsuaki Oka (Toshiba Solution)
Koji Kubota (Matsushita Electric)

Study Members (titles omitted in kana order)

Satoru Akiyama (NTT East)
Takashi Arano (Intec NetCore, Inc.)
Kiyoteru Ishihara (KDDI)
Jyoji Isihara (Toshiba)
Kenichi Kanayama (Intec NetCore, Inc)
Masanobu Kawashima (NEC Access Technica)
Kuniyasu Goto (Fujitsu)
Yuichi Shimada (Fujitsu Access)
Takumi Segawa (Panasonic Communications)
Motoyuki Takizawa (Fujitsu Access)
Takahiro Furukawa (Fujitsu Access)

Inquires

For information relating to these Guidelines, please inquire by emailing to:

wg-dp-comment@v6pc.jp
IPv6 Promotion Council of Japan DP-WG