2005 Version

IPv6 Depolyment Guideline

A Case Study for a Local Government to Implement an IPv6 Multicast Distribution System in Their Network

March 2005

IPv6 Promotion Council of Japan
DP-WG Large Enterprise, Local Government and SOHO SWG

Table of Contents

1. Network Configuration in Applicable Area

Basic Information on Applicable Local Government

Introduced to the reader here is an outline of the local government envisaged as an object of the case study reported hereinbelow.

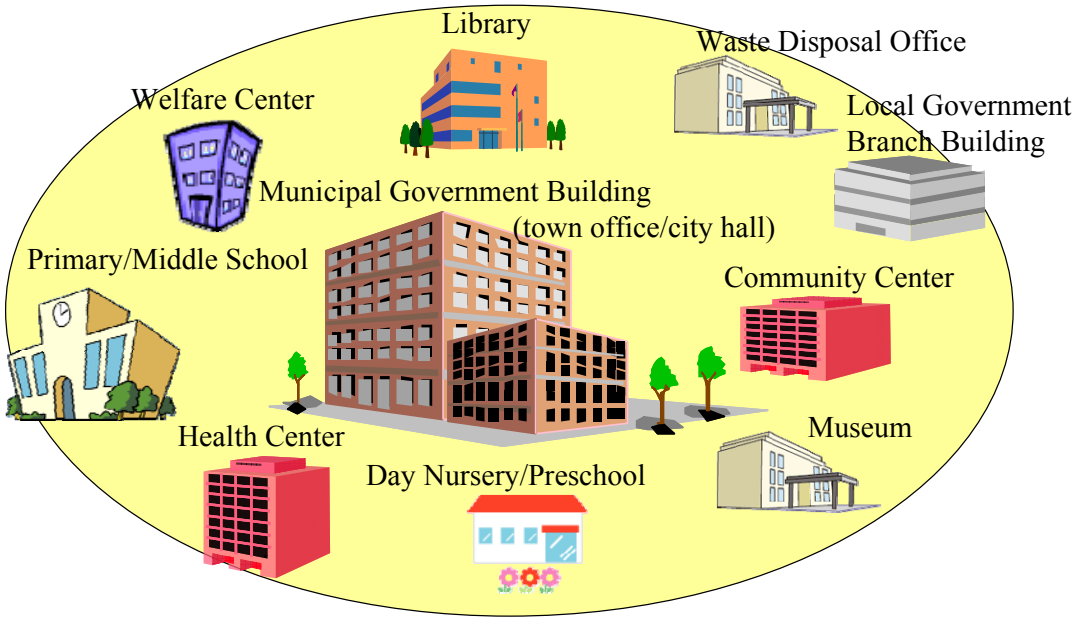
The local government covered by the present report is one of the basic municipalities (not a prefecture but a city, including towns and villages), or a medium-sized city with a population of about 120,000 citizens. In this local government, approximately 1,000 municipal office workers are serving the citizens.

The local government has had a local government network (an OA-oriented network that the personnel are authorized to use in their general services) formed within an area under jurisdiction of the local government. This is a star-shaped network linking 20 medium-sized bases (local government branch buildings, libraries, museums, health centers, etc.) and 40 small-sized bases (community centers, tourism centers, unmanned facilities, etc.), with the local government building (city hall) positioned at the center. The bases, including the local government building, are located centrally in a specific region (as connected by a wide LAN, CATV network and the like).

This local government network is connected with the Internet at a single point (at a level of approximately 1.5Mbps). And the municipal personnel are using email, web access, groupware, file-sharing service and so on (with an accounting service also available in some cases). In principle, the network is not authorized to make remote access.

An Image of Local Government and its Associated Facilities

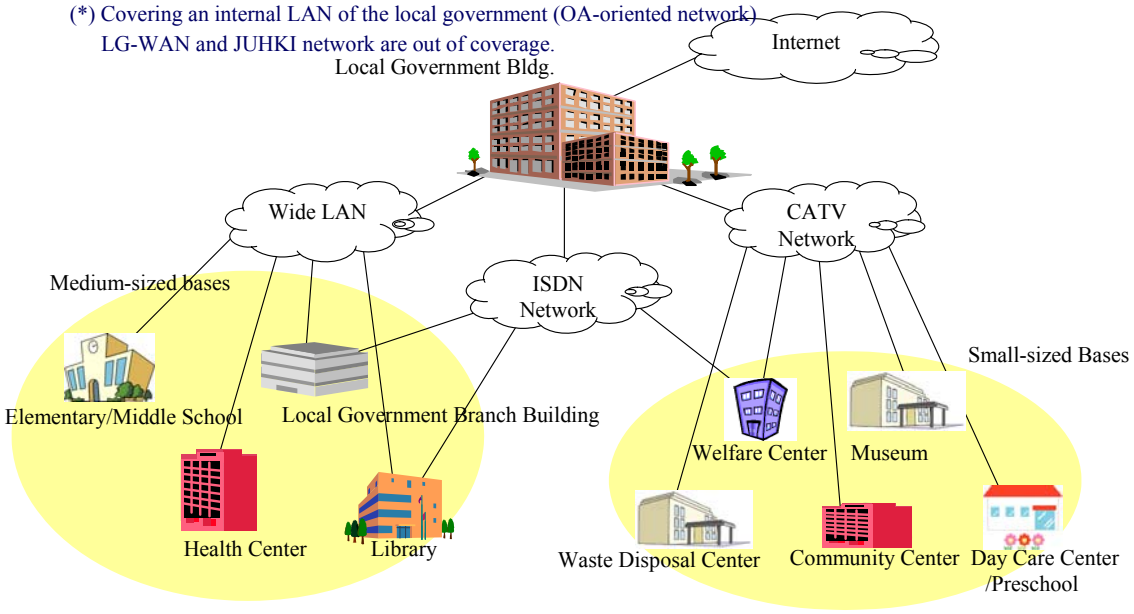
- Associated facilities exist concentratedly within a specific area.



As envisaged also in this case, a local government network (neither LGWAN nor Basic Residents' Registration Network <<JUHKI Net>> but an OA-oriented internal LAN here). Normally, it is connected with associated facilities in a star-shaped formation. And an inter-base connection circuit is used, with a wide LAN and a local CATV line applied. As tailored to a specific purpose, moreover, a backup system may be provided sometimes, using an ISDN line.

Local Government Network

- Local government network (*) is star-connected with associated facilities.
- A wide LAN and a local CATV circuit are used to inter-connect bases.
- Sometimes, an ISDN line may be used to provide a backup circuit.



Features of Local Government Network

In the case envisaged here, a 1.5Mbps private circuit is employed on the external (Internet) access line. It has no redundancy.

As far as security is concerned, the network has any internal terminals inhibited from communicating with the Internet, in principle, with the network firewall taken for the boundary. A public server (email and web) and proxy are arranged in DMZ.

The firewall has an access policy "Deny Any Access, in Principle."

Exterior → DMZ: Services other than specific ones (open web, email, etc.) are to be denied, in principle.

DMZ → Exterior: Services other than specific ones by specific servers are to be denied in principle.

DMZ → Interior: Denied

Interior → DMZ: Services other than specific ones (web proxy, email, etc.) are to

be denied, in principle.

Exterior → Interior： Denied

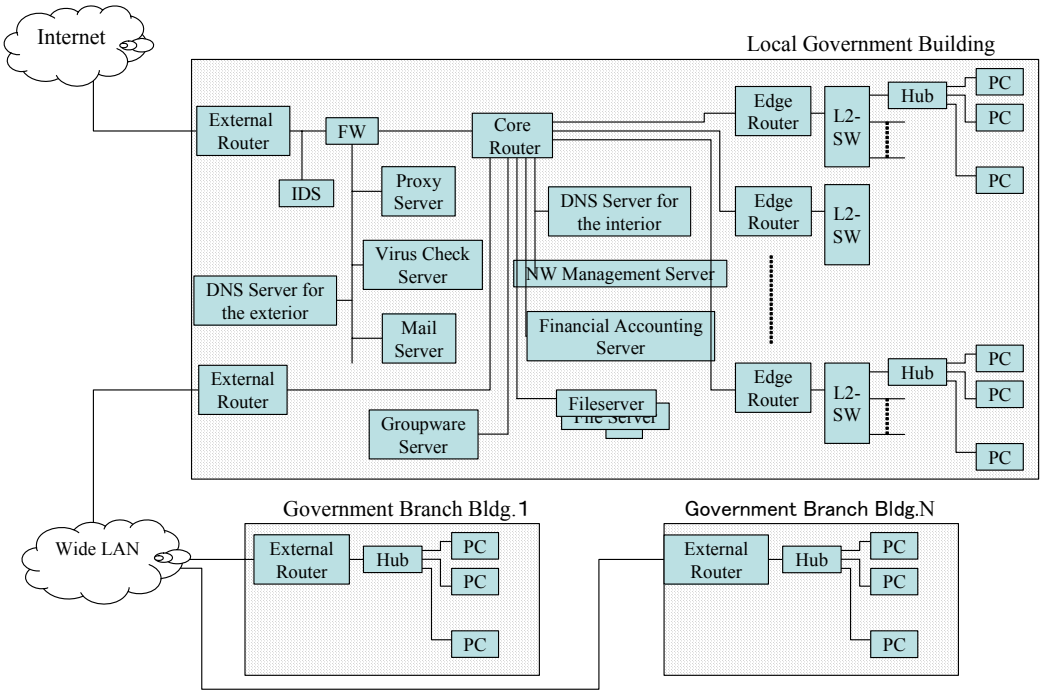
Interior → Exterior： Denied, in principle

Being NATted with the firewall, the internal network (IPv4) makes use of private addresses. (The NAT feature is not required unless a direct access is made from the interior to the exterior.)

In addition, an illegal access detector feature is implemented in linkage with IDS. A monthly summary is managed and reported as a result of daily monitoring with IDS.

Within the local government building, clients are interconnected to form subnets by floor and by department. Small-/medium-sized bases are connected with the local government, using a wide LAN and/or CATV network. Some bases have these networks backed up with an ISDN circuit.

Exemplar Local Government Network Configuration



2. IPv6 Deployment Scenario

An enterprise has its activities conducted mainly in pursuit for direct profits. A local government, however, is more strongly called for a social contribution, such as welfare, education, public activities and the like.

Administrative objectives common to such a local government are to establish environments for closer communications between inhabitants and administration and for faster and more efficient services, to make towns more vigorous and to transmit the administration information.

Especially as an IPv6 effective use case, the video distribution network infrastructure is effectively usable to relay a local government assembly. We should create an environment where the municipal personnel are able to attend the local government assembly so as to know what is discussed there. In the future, it should be widely opened to regional inhabitants so that an open administration may be materialized.

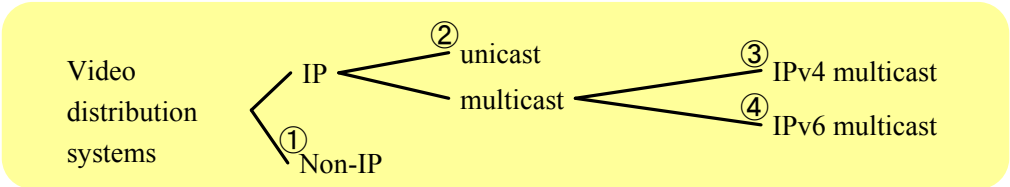
Now, an implementation of video distribution in a local government will be discussed here.

Comparing Video Distribution Systems

Video distribution is available in a few system alternatives as illustrated below. They may be roughly divided into two systems: one is to apply IP and the other not. IP-applied systems include the IPv4/IPv6 unicast, IPv4 multicast and IPv6 multicast. These systems are compared here.

Studying Video Distribution Systems

<System Classification>



<System Comparison>

System / Evaluation item	①Non-IP	②IPv4/IPv6 unicast	③IPv4 multicast	④IPv6 multicast
Efficiency (general distribution)	A	B(※1)	A	A
Cost	C(※2)	B	A	A
Extensibility/potential	C(※3)	A	B	A

※1: Suitable for on-demand distribution, but a general distribution, such as live-relay, to many terminals, however, would increase load on distribution server .

※2: Unlike universal infrastructure, such as IP, it is prerequisite to set up exclusive network distribution infrastructure.

※3: To extend distribution size, it is necessary to newly provide private circuit. In the future, moreover, it is difficult to publicize distributed information to the exterior

Comparing IP with Non-IP

The IP-applied video distribution is, first of all, compared with the non-IP video distribution.

For the IP-applied video distribution, an existing IP-based LAN environment is used to add a distributing server and receiving clients so that a video distribution system may be materialized.

Using the IP would permit us to implement the video distribution system at a relatively low implementation and operation cost. It is necessary, however, to study applying an appropriate priority control of either existing IP application's communication band or video distribution.

For the non-IP distribution, video data is distributed through an exclusive distribution private analog-line network, wired TV network or the like. The non-IP distribution provides a relatively stable image quality. Since it is an exclusive distribution network system, it has its applications limited. In addition, it is difficult to expand the distribution coverage.

Conclusively, the IP-based distribution is more advantageous unless the legacy infrastructure is available.

Comparing Unicast with Multicast

A comparison is made between unit cast and multicast.

As an advantage of the unicast, it may be pointed out that the unicast allows for on-demand streaming and downloading. The multicast, on the other hand, allows for saving the communication band in case where contents with a large capacity are live-relayed and generally distributed to a large number of terminals.

The multicast is more advantageous when relaying a municipal assembly on a real-time basis.

Comparing Video Distribution Systems (continued)

- Unicast vs. Multicast
  - Advantage of Unicast
    - Capability of handling on-demand streaming and downloading is advantageous.
  - Advantage of Multicast
    - Capable of saving the communication band when live-relaying or generally distributing contents with a large capacity to many terminals. (Refer to the following)

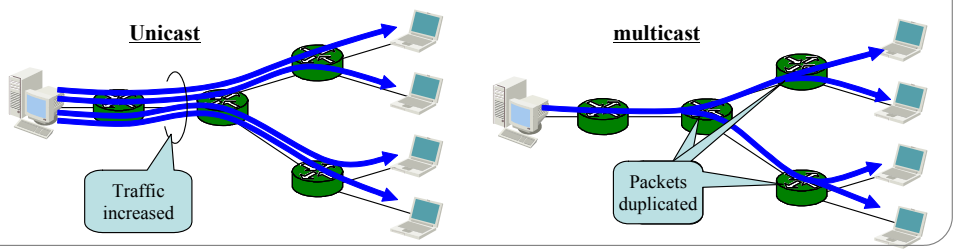
Band of Circuit Required for General Distribution of Video Contents to Many Terminals

(Example) Prerequisites:

- Rate of transferring video contents to be distributed: 3Mbps
- Number of terminals to receive contents live-relayed and generally distributed: 50 units

Circuit band required:

150Mbps for unicast and 3Mbps for multicast



Conclusion: Multicast is more advantageous, if aimed at relaying a local government assembly on a real time basis.

Comparing Multicasts between IPv4 and IPv6:

IPv4 and IPv6 multicasts do not differ in functional and/or implemental advantages.

In multicast communications, both routing and group management protocols are nearly identical functionally between Pv4 and IPv6.

In existing systems, moreover, IPv4 products compatible with the multicast have been scarcely implemented. Even the IPv4 multicast, therefore, requires routers to be renewed. In this sense, it cannot be safely said that the IPv6 multicast is more disadvantageous.

Applications, such as Windows Media Service and MediaPlayer, exclusively used to transfer and playback videos, are compatible with both IPv4 and IPv6 multicasts.

The IPv6, however, has a multicast address space abundantly available. A group ID can be generated out of a global address prefix for the unicast so that a global multicast address can be obtained with ease.

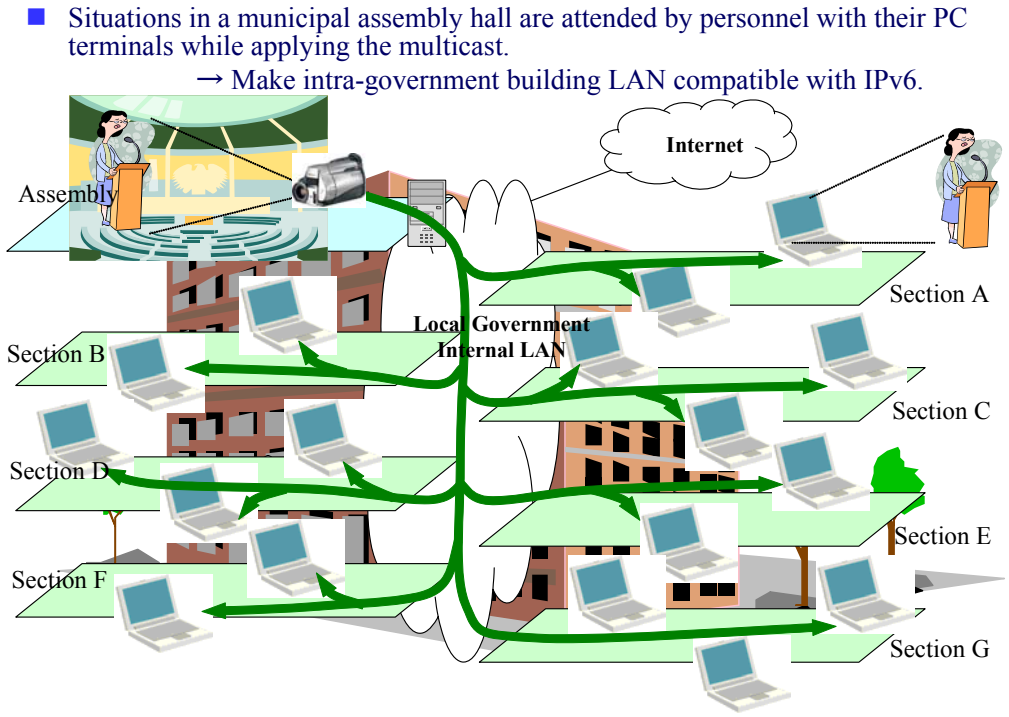
Some small-sized router products currently available, moreover, are compatible with the multicast in IPv6 only.

Thus, an evaluation from the viewpoint of a future network setup would allow us to expect that the IPv6 will have higher cost-effectiveness in the future.

We may safely come to the conclusion, therefore, that the IPv6 multicast is more advantageous.

Local Government Assembly Relay Image

As illustrated below, what is making progress in a local government assembly hall can be monitored in real time at a PC terminal by the personnel once the LAN in a local government has been made compatible with IPv6 and with the IPv6 multicast.



Outline of IPv6 Multicast Implementation

For multicast-compatible related equipment, Windows Media Service plus Camera（IEEE1394 or USB）should be implemented in a server. Router/Layer 3 Switch is made compatible with IPv6 and changed over to a broader band (by upgrading the software version or replacing the equipment). A client should make use of Windows XP + Windows Media Player10.

For a size of changes, it is necessary that to make compatible with IPv6 such Layer 3 Processor as main switch, WAN-applicable router, firewall and so on in addition to the installation of a new multicast server (liking with a camera). According to the situations, Layer 3 equipment is revoked (changed over to Layer 2).

Although it is necessary to make the user terminal compatible with IPv6, Windows XP is to be used here. In the first phase, 50 units (5%) out of total 1,000 user terminals are to be renewed into IPv6 terminals. Subsequently, IPv6 terminals will be sequentially implemented.

A distribution to the exterior is considered to involve too many issues, such as firewall, external circuit and so on at this time.

Issues to be Studied, Coupled with IPv6 Multicast Implementation

To implement the IPv6 multicast, it is necessary to study the following points:

A switch on the LAN need have the MLD Snooping feature mounted so that the multicast traffic may not flow into an unnecessary port. For distribution, there is a problem to make a connection between branch government building and WAN compatible with IPv6. To make the network openly available in the exterior, furthermore, it is necessary to review the distribution system.

In the initial phase, the distribution is to be limited to the services for the internal LAN of the local government and to provide an IPv6 circuit with a tunnel and dual stack.

- Video Band/Format
  - Is approximately 1M acceptable or should it be broader?
  - Windows Media Video (wmv format) is readily applicable.
  - Number of frames (fps) and of pixels
- Traffic Evaluation
  - Effects on another user who shares the switching hub (necessity of MLD snooping)
  - Necessity of band control and priority control with routers (effects of a burst load due to other applications)
- How about distribution to government branch buildings?
  - Review circuit band and external router.
  - Use IPv6 over IPv4 tunnel to take temporary measure.
- Distribution Coverage Setting
  - It is necessary to study distribution coverage according to each municipality policy.
  - What distribution method should be used when making the network open to the exterior of a municipality?
- External Circuit
  - In initial stages, limit circuitry to internal LAN services of the local government.
  - Provide external line as IPv6 circuit composed of tunnel, dual stack, etc.
  - Broaden circuit band, coupled with implementation of IPv6 (1.5M → 10M or 100M).

What be Noted on Security

Introduced to you hereinbelow are the precautions to taken in relation to the security policy you should adopt when implementing the IPv6 multicast distribution. (Refer to Chapter 4 Local Governments (BCP), Security Guidelines.)

BCP

First of all, a decision to limit distributees to the interior of an intra-net system only in initial stages of implementation without distribution to the exterior would be supportable enough from a security point of view. More specifically, the following measures are to be taken:

- Expressly isolate the distribution coverage by setting the multicast and/or filter in edge routers.
- Apply a log management setup at an application level in the distribution server.

And the IPv6 services available at each terminal, moreover, are to be used on a limited basis. The IPv6 services at terminals are to be limited as follows:

- Support the IPv6 transport at the minimum required level. Since a global address is not required for the IPv6 multicast service, we may use a method in which no RA is set at the edge router.
- Some other methods available are to limit the use of the IPv6 applications that may fall outside the coverage of management by the organization, to restrict the installation itself of applications or to generate an independent segment (using VLAN).

Future

In the future, security is to be secured by applying authentication to stream data. This will permit us to properly use the contents open and limitedly open to the public. To make contents limitedly open to the public, an implementation is to be studied so that the DRM and/or access can be authenticated.

For protection against a false distribution server (to identify the distribution source), a countermeasure is to be taken by setting a filer in the multicast router.

What be Noted on Performance/Operation

Once the services have been put into full-fledged operation, MLD Snooping is required. It is Layer 2 Switching feature to send a multicast packet to those terminals only, which desire it to be distributed. It is necessary to provide Layer 2 Switch allowing for that function.

In addition, it is necessary to have the services segregated from others by setting priority

control and band control.

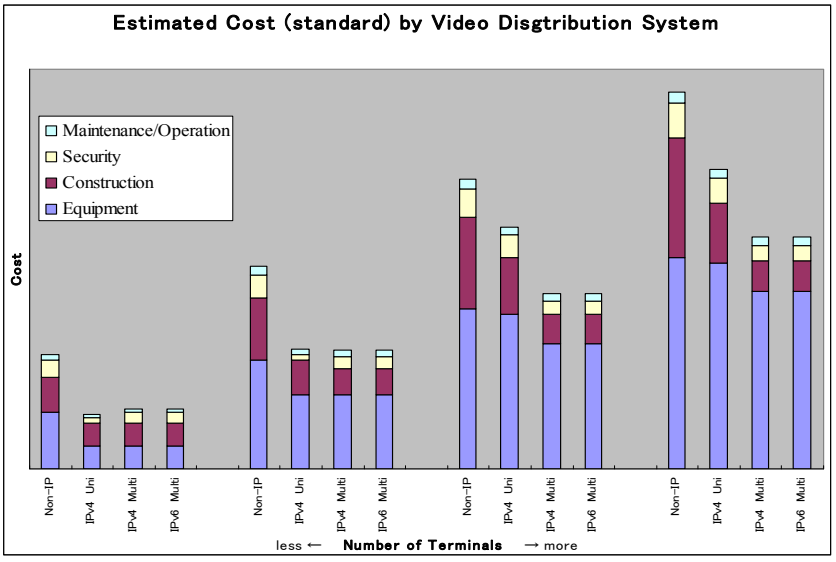
It is necessary, furthermore, to take into consideration the control that should be available in the event of a multicast service oversupply. In the future, there are possibilities that multicast sessions (channels) may be generated. In such event, the number of sessions will be called upon to be limited so that they can avoid being ruined together.

In preparation for a possible communication fault, moreover, it is necessary to arrange in order the methods of analyzing and separating such fault and of taking corrective action. Maintenance/operation tools specializing in the multicast are demanded so that a line occupancy status and a failed part can be managed.

Cost Assessment

The cost required to make the network applicable to the multicast could be roughly estimated (standardized) as referred to below.

■ Roughly Estimated Cost Required to Make Multicast Applicable (Standard)



Breakdown of Cost for Equipment in IPv6 Multicast（equipped with 50 receiving terminals）

- Servers: PC Server＋Windows Server 2003 license＋camera ＝ 0.3＋ 0.6＋ 0.1≒ 1.0 in million yen
- Clients: PC (Windows XP) x 50 units ≒ 9.0 million yen
- Main SW: IPv6-applicable L3-SW ≒ 3.0 million yen

3. Network Configuration on Deployment to IPv6

Multicast-applicable Network

To set up the IPv6 multicast applicable network for the purpose of distributing contents within a closed coverage of the internal LAN of the government, it is necessary to carry out the operations required as follows:

Main Switch

Replace with Layer 3 Switch applicable to IPv6.

Set a IPv6-applicable configuration (addressing and routing).

Set a IPv6-applicablemulticast.

Multicast Server

Install a multicast server plus a video camera at the point where the contents to be distributed are to be transmitted (local government assembly hall).

Connect as the IPv6-applicable server to a segment in the internal LAN of local government.

Client

Implement a PC provided with the OS (Windows XP) applicable to IPv6.

Install IPv6 in the PC and update Windows Media Player.

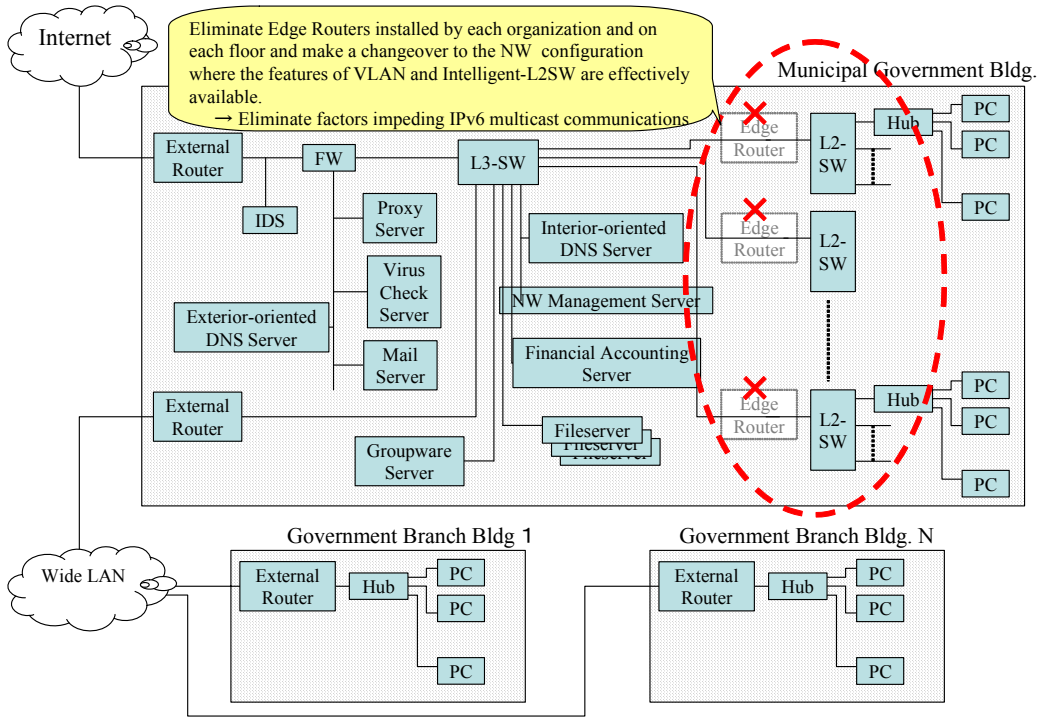
Disuse unnecessary edge routers

Delete those edge routers, which might impede IPv6 communications and reduce the Layer3-oriented stratum as illustrated below.

Distribute to a remote base

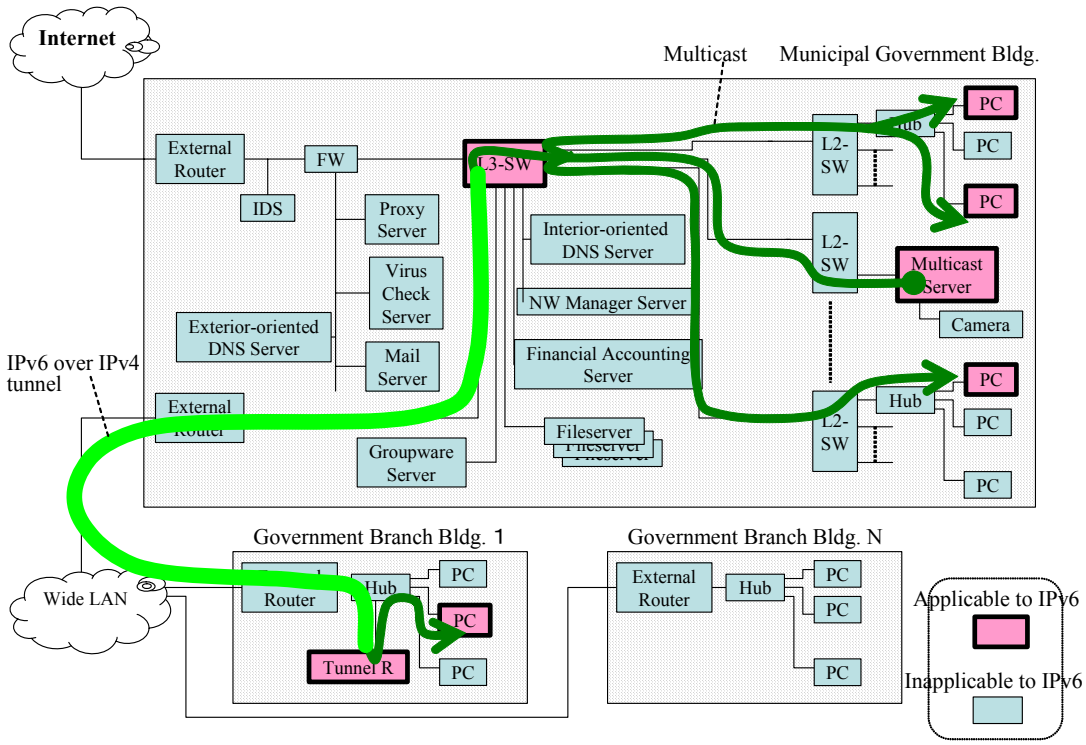
With tunnel connections employed, it is necessary to provide a multicast-applicable tunnel- terminating router.

Network Simplified



The local government building is to be changed over to Layer 2 as far as practicable in the interior. Then, the IPv6 multicast is to be distributed to PCs. IPv6 over IPv4 tunneling is implemented on the circuit between a branch and the local government building so that the IPv6 multicast distribution will be performed by way of the existing IPv4 infrastructure.

Multicast-applicable Network



Future Issues on Multicast-applicable Network

In the future, the distribution in the internal LAN of local government will be extended into a large scale so that contents will be distributed to the exterior, too. In that stage, it is necessary to take the following into consideration:

Internet-connected Circuit

Contract to use a IPv6-applicable circuit (dual/tunnel), with distribution band taken into account.

Regarding the feasibility of implementing a multicast distribution, it is necessary to consult with a connection provider.

It is also necessary to take a possible changeover of the distribution server to ASP into consideration.

Multicast Server

A multicast server for external distribution is to be installed in DMZ.

Firewall, IDS

The security equipment applicable to IPv6 multicast communications is to be implemented. (At present, the existing firewall has remained inapplicable to IPv6 multicast communications)

DNS

To make the external distribution server open to the public, DNS is to be also applicable to IPv6. (This is not directly influential over the multicast.)

Client

An IPv6-applicable PC (Windows XP or the like) is to be implemented in full scale.

Layer 2 Switch

The Layer-2 switch applicable to MLD Snooping is to be implemented, coupled with the multicast communications being put into substantial operation.

The IPv6 network implemented, with the multicast video distribution requirement taken for the turning point, is to have the network infrastructure effectively utilized so that miscellaneous IPv6 applications may be efficiently implemented.

4. Supplements

IPv6 Multicast

What is multicast?

Multicast is a technology, which permits one terminal transmitter to efficiently transfer the information to N terminal receivers, with one packet duplicated into two or more by a router in the relay mode. It may be efficiently applied to live-relay and generally distribute broadband contents.

Multicast System

To implement the multicast, it is necessary to select an applicable system out of either “Route Control System” or “Group Management System.

Route Control System

Protocol to be used by routers to each other to implement multicast communications:

PIM-SM

Protocol most popularly employed at the present to exchange the multicast route information:

PIM-SSM

A receiver participates in a multicast group after the receiver has selected a transmitter. It is possible to protect multicast communications against their possible impediment by an illegal transmitting terminal.

Group Management System

Protocols to be used between router and host to materialize multicast communications:

MLD (Multicast Listener Discovery)

MLDv1： PIM-SM-applicable multicast group management protocol

MLDv2： PIM-SSM-applicable multicast group management protocol

What is an appropriate multicast system currently available?

Judging from the aspects of practical usability and popularity for the time being, PIM-SM/MLDv1 is advantageous. From the viewpoint of packet transfer efficiency and security, however, PIM-SSM/MLDv2 is superior. For the time being, therefore, it is realistic to implement the IPv6 multicast with PIM-SM and MLDv1 and to make a deployment to PIM-SSM and MLDv2 in the future, coupled with a buildup of applicable products.

BSR and RP in PIM-SM:

RP

Point where a router is available to send a participation message so that the transmitting/receiving host will take part in the multicast: PIM-SM usually has a multicast packet transferred via RP.

BSR

RP and BSR have their own information (IPv6 address, etc.) notified to all PIM-SM routers.

Multicast Address

Address Space

ff00:: /8 is provided as the address space for the IPv6 multicast.

<Reference> In case of IPv4:

224.0.0.0～239.255.255.255 (Class D)

(Example) Where the user who owns 2001:db8:1234::/48 generates a multicast address:

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

x: Scope specified

*: Group ID specified

Special IPv6 Multicast Addresses

The following two addresses are available as special IPv6 multicast addresses:

ff02::/16 : Link local scope multicast address and

ff0e::/16 : Global scope multicast address

SWG Members of Large Enterprise/Local Government Segment, DP-WG

（titles omitted）

SWG Chair

Tsukioka (Hitachi, Ltd.)
Sakauchi (NEC Corporation)

Members

Arano (Inter NetCore, Inc.)
Ito (Canon)
Inomata (Fujitsu Limited)
Oikawa (Microsoft)
Ota (NTT East)
Ohira (Ricoh Company, Ltd.)
Kato (NTT)
Kanayama (Intec W&G)
Kokubu (RINT)
Suzuki (Hitachi, Ltd.)
Tachibana (aniani.com)
Tatsuki (NEC Corporation)
Tokushige (NTT Communications Corporation)
Nakai (NTT Communications Corporation)
Nakahara (NEC Corporation)
Nishida (Ricoh Company, Ltd.)
Shirota (Hitachi, Ltd.)
Hashimoto (MRI)
Hiroumi (Intec NetCore, Inc.)
Yamazaki (NTT Communications Corporation)
Yamamoto (NTT East)
Yoshioka (Toyota InfoTechnology Center Co., Ltd.)

SWG Members of SOHO Segment, DP-WG

(titles omitted)

SWG Chair

Inomata (Fujitsu Limited)
Tsukioka (Hitachi, Ltd.)
Bannai (NEC Corporation)

Members

Arano (Inter NetCore, Inc.)
Nakai (NTT Communications Corporation)
Nakahara (NEC Corporation)
Kanaumi (NEC Corporation)
Ohira (Ricoh Company, Ltd.)
Ito (Canon)
Yamamoto (Shimizu Construction)
Yoshioka (Toyota)
Ozaki (Fujitsu Limited)

Inquiries

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

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