IPv6 Multi-service Networking Technologies

Takaaki Moriya[†], *Hiroyuki Ohnishi, Yasuhiro Seki, and Tadashi Ito*

Abstract

This article reports our study on connecting IPv6 (Internet protocol version 6) equipment in user networks to multiple service networks. With the spread of various information appliances and devices, e.g., digital televisions and DVD recorders, there is a growing need to provide a way to connect them to network services. This will lead to a lot of equipment using multiple services over the network. Therefore, in the near future, as IPv6 addresses are widely deployed in a large number of devices, it will be important to consider connectivity models suitable for the future expansion of network access with IPv6.

1. What is a multi-service network?

Today, personal computers (PCs) at home can easily connect to the Internet through broadband access like ADSL (asymmetric digital subscriber line) and FTTH (fiber to the home), which are widely available. The spread of the broadband environment is expected to increase the number of devices connected to IP networks. PCs and other information appliances and devices should be connected to the network because they will then be able to utilize various network-based services, such as remote maintenance and remote control.

Since the Japanese government's IT Strategy Headquarters adopted the e-Japan strategy in 2003, IPv6 (Internet protocol version 6) technology has been considered a necessary step to enhance and upgrade the network infrastructure (IT: information technology). IPv6, which has been developed as the next-generation Internet protocol, has a much larger address space, security features, automatic network configuration, guaranteed communication quality, and many other features. It is assumed that IPv6 functions will be deployed in a large number of devices in homes or buildings in the near future. Service providers need IPv6 equipment to be controlled flexibly because they want to deploy attractive services suitable for the characteristics of each device. End users, on the other hand, should connect devices they own to the IP network and simultaneously use various network services depending on each device's type and purpose. For example, a user could simultaneously use multiple services via a PC: she could watch a movie at home by accessing a streaming service while monitoring her children via a live camera installed in the kindergarten by a security service provider; she could also access her company's internal server in order to work from home. In another example, a home appliance could be controlled by multiple service providers: a refrigerator could be remotely maintained by the manufacturer and simultaneously controlled remotely by the user to check the amount of juice and vegetables via an information appliance service. Thus, large numbers of mixed IPv6 devices such as computers and sensors with different functions will be connected. Furthermore, such devices will be independently connected to the network to obtain appropriate services. To accommodate the increasing number of IPv6 devices and the variety of services, we must consider IPv6 connectivity models for discriminating between different types of network use at a particular location and simultaneously connecting to several destinations.

To meet such requirements, NTT Network Service

[†] NTT Network Service Systems Laboratories
Musashino-shi, 180-8585 Japan
E-mail: moriya.takaaki@lab.ntt.co.jp

Systems Laboratories is studying a new platform that supports easy connection between service networks and user networks. Service networks are ones belonging to service providers who offer network services, e.g., a security service. User networks are expected to be an IPv6 environment in a home or apartment building, where a lot of equipment including non-PC devices will be connected to network services. In our platform, we assume the user network is simultaneously connected to multiple service networks. We examined if such a model is feasible, effective, and practical. NTT Network Service Systems Laboratories is studying network control technologies to create a platform called a multi-service network (**Fig. 1**). This article reports our study on connecting IPv6 equipment in user networks to multiple service networks.

2. Requirements for a multi-service network

2.1 Identifying each device

Every user device must be identified by service networks because remote control and maintenance services are based on push-type communication from the service provider to the devices in the user network. IPv4 (Internet protocol version 4), which is currently used on the Internet, does not provide enough global addresses and needs network address translation, so it is difficult for IPv4 to provide push-type communication from outside the user network. However, IPv6, which has been developed based on IPv4 as a protocol for the next-generation Internet, has a huge number of addresses and can assign a global address to each device, making it easy for a service provider to manage user equipment. Thus, the multi-service platform should be based on IPv6 technology because IPv6 has the advantage of easy deployment of push-type communication service.

2.2 Assigning the IP address space

For service providers in particular, systematic assignment of network addresses to equipment belonging to the service network makes it possible to manage many devices efficiently, considering a device's type, location, user name, and so on. If providers and users independently obtained IP address spaces from an Internet service provider (ISP) and assigned those IP addresses to the users' devices, then the service provider would have to manage a lot of "scattered" addresses of equipment belonging to its service network. It would be troublesome for the service provider to control the user's devices flexibly and manage the network.

To avoid this, we need a mechanism for assigning unified and coordinated addresses to both service and user networks in order to enable service providers to easily control equipment in the user network. For example, a service provider can set static filtering to control access to its server by assigning specific addresses to the user network.

2.3 Supporting access to multiple service providers

To achieve simultaneous access to multiple services and apply push-type service, multiple IP address spaces of service providers should be assigned to the

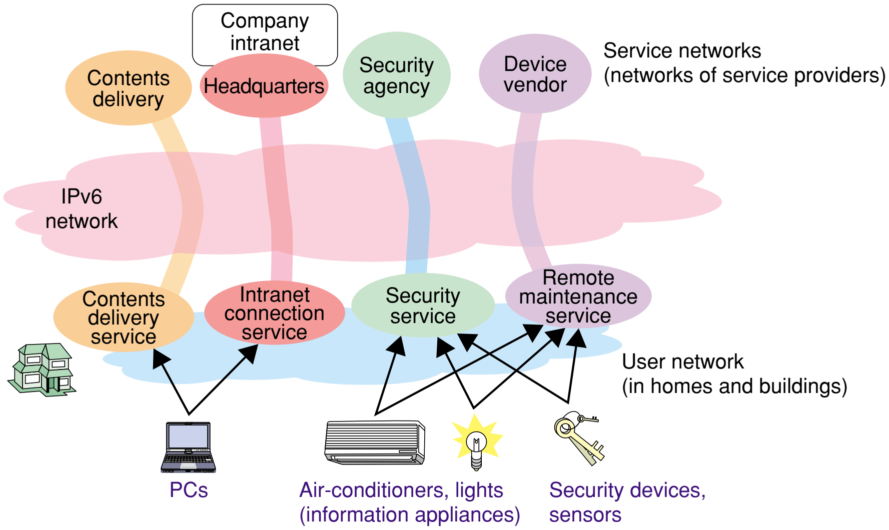

Company intranet
Contents delivery
Headquarters
Security agency
Device vendor
Service networks (networks of service providers)
IPv6 network
Contents delivery service
Intranet connection service
Security service
Remote maintenance service
User network (in homes and buildings)
PCs
Air-conditioners, lights (information appliances)
Security devices, sensors

Fig. 1. IPv6 multi-service network.

user's network. Of course, those assigned IP addresses must be properly chosen when a device accesses the service provider. In addition to the address assignment, access by a device that has not been authenticated and authorized to use its service must be rejected.

3. Solutions

To meet the above three requirements, we have developed two techniques: virtual network construction and multi-path distribution [1] (**Fig. 2**).

3.1 Virtual network construction

This technique expands part of the service network into the user network in a virtual manner. It also enables secure IPv6 address prefix assignment from the service provider to the user network. The technique consists of i) dynamic IPv6 prefix assignment with authentication and ii) dynamic IPv6 prefix acquisition and IPv6 prefix advertisement using a service profile. These two functions are achieved as follows.

The user and service networks are connected via a virtual tunnel, provided between the multi-homing function (MHF) on the user network and the service network delegating function (SNDF) on the service network. MHF and SNDF are expected to be implemented in gateway routers of the user network and service provider, respectively. The virtual tunnel between MHF and SNDF is not established until after SNDF has verified that MHF is authorized to access the service network. Using the virtual tunnel, SNDF dynamically assigns part of the provider's address space to MHF. Then MHF broadcasts the information about all of the acquired address spaces, and the user equipment automatically configures multiple IPv6 addresses by using every prefix announced by MHF. Dynamic assignment is effective because it prevents the address space from being used wastefully. In this way, part of the IP address space of the service network is assigned to a user's devices so that the service provider can directly access and control them. This technique can not only assign a systematic IP address to each user device, but can also enable the service provider to identify devices related to its service.

3.2 Multi-path distribution

This technique provides simultaneous/selective access to multiple service networks. It consists of i) an IP routing function based on the source address and ii) an access control function. These functions are cooperatively achieved by both MHF and the user equipment, as shown in **Table 1**. As mentioned in section 3.1, the user equipment acquires multiple addresses of service providers. To resolve the host name in the service provider, a DNS (domain name system) proxy is implemented in MHF.

When accessing a host in the service network, a user's device can select a source address among multiple addresses using the source address selection mechanism [2] that can choose the longest-matching

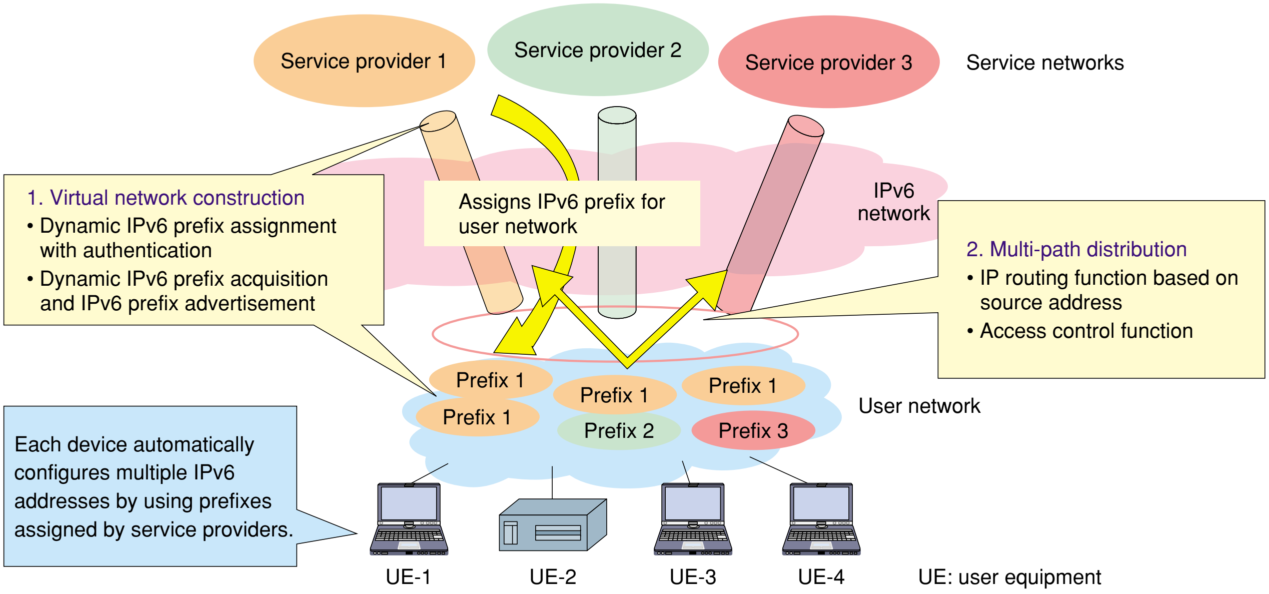

Service provider 1
Service provider 2
Service provider 3
Service networks
1. Virtual network construction
• Dynamic IPv6 prefix assignment with authentication
• Dynamic IPv6 prefix acquisition and IPv6 prefix advertisement
Assigns IPv6 prefix for user network
IPv6 network
2. Multi-path distribution
• IP routing function based on source address
• Access control function
Prefix 1
Prefix 1
Prefix 1
Prefix 2
Prefix 1
Prefix 3
User network
Each device automatically configures multiple IPv6 addresses by using prefixes assigned by service providers.
UE-1
UE-2
UE-3
UE-4
UE: user equipment

Fig. 2. Multi-service networking technologies.

Table 1. Deployment of functions.

	Function	Deployment of functions		
		User equipment	MHF	SNDF
Virtual network construction	Dynamic IPv6 prefix assignment with authentication	—	—	√
	Dynamic IPv6 prefix acquisition and IPv6 prefix advertisement	—	√	√
Multi-path distribution	IP routing based on source address	√	√	—
	Access control function	—	√	—
IPv6 basic technology	DNS	√	√	—
	Tunneling	—	√	√

prefix with respect to the destination address. When the device communicates using the source address selected by the above function, MHF checks whether the source address was assigned by the proper service provider and authorized to use the service. If this verification fails, the communication is filtered out by MHF. Then, MHF chooses an appropriate route for connecting the user's device to an appropriate service provider.

However, we have not yet concluded that this is the best approach. In the current approach, access filtering is executed after the device configures the IP address. Another approach would be to have MHF refer to the service access policy before the service network address space is assigned. MHF would authenticate devices and permit only authenticated ones to configure the IP address. Investigating which approach is the best for a multi-service network is a topic for future study.

4. Implementation

NTT Network Service Systems Laboratories implemented the MHF/SNDF model and evaluated both the feasibility and effectiveness of the technologies. **Figure 3** shows the prototype network for eval-

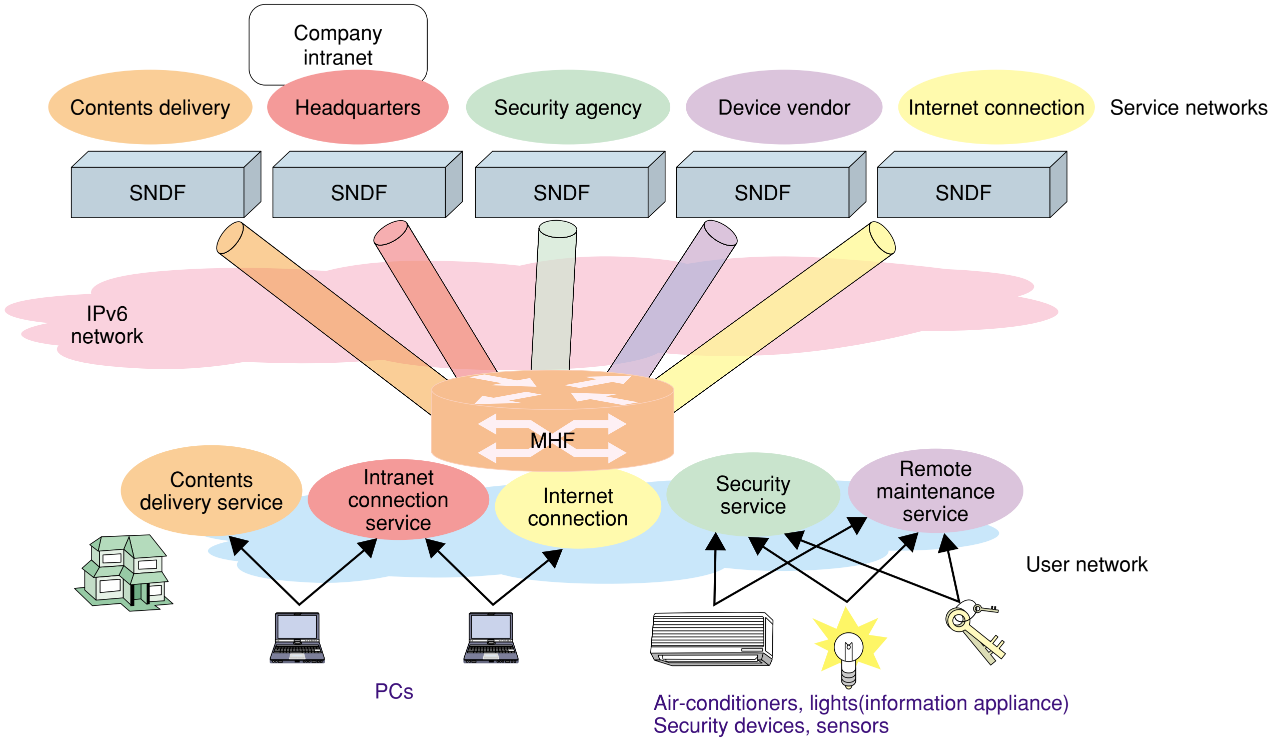


Fig. 3. Prototype network.

uating our multi-service networking technologies with five service networks and one of the six user networks, in which IPv6 equipment and applications are allocated. The results show that multiple IPv6 addresses were correctly assigned to user equipment and the equipment could connect to appropriate service providers depending on type of application. For example, **Fig. 4** shows an ordinary Windows XP computer in a user network connecting to three service providers: a contents delivery service provider (provider 1) and two remote-camera service providers (providers 2 and 3). This means that a commonly used PC supporting IPv6 can simultaneously connect to three services. In fact, by capturing forwarded packets in the user network, we showed that source addresses assigned by multiple service providers were correctly distinguished and chosen. This evaluation showed that the multi-service networking technologies made it possible to connect between multiple user networks and multiple service networks with the required performance. Therefore, the multi-service network platform is feasible for connectivity models suitable for the future expansion of IPv6 equipment and services.

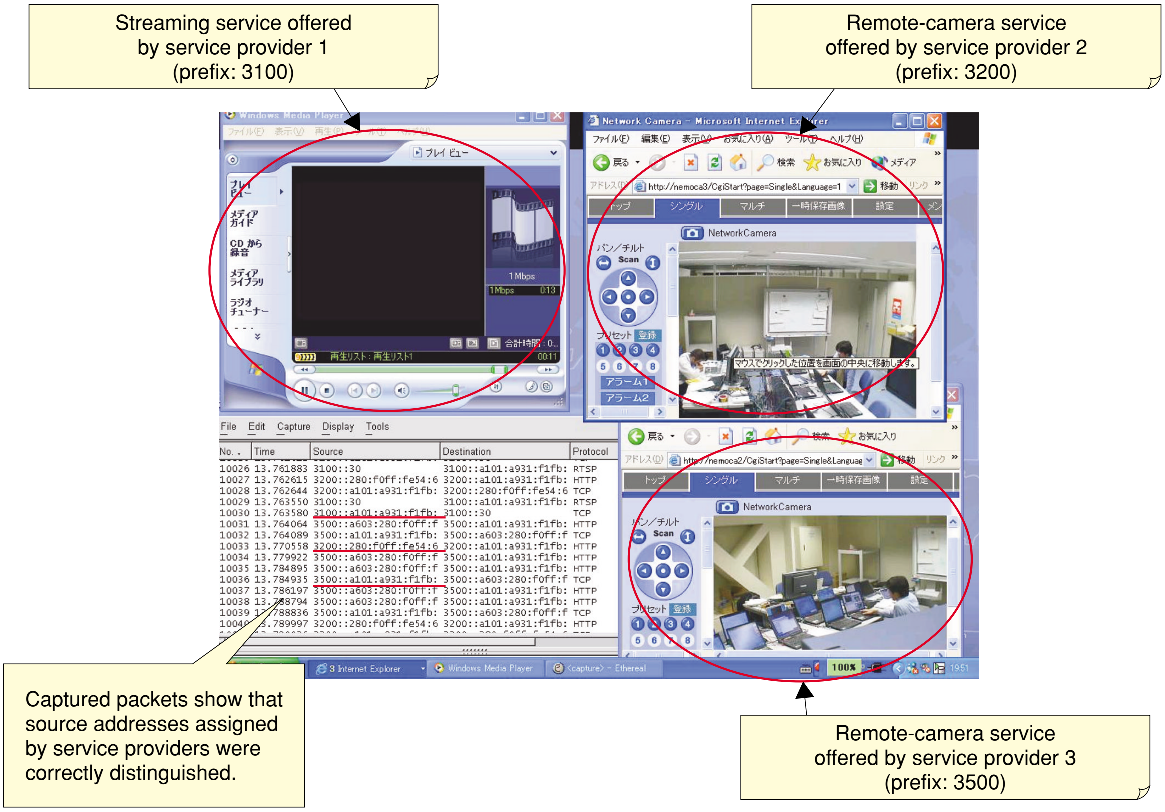
5. Future work

Our future work will be focused on creating network services with our platform. The multi-service networking technologies introduced in this report were applied to an IPv6 deployment field trial sponsored by the Ministry of Internal Affairs and Communications with the participation of NTT East in 2004. During this trial, which is still continuing, we will not only examine the feasibility of cooperation between various service providers, but also continue to gain knowledge about multi-service networks. In addition to the functions mentioned in this report, we will study the functions needed for network service, such as QoS (quality of service) control for service providers and applications.

References

[1] H. Ohnishi, T. Moriya, T. Jocha, and Y. Seki, “A path selection method in IPv6 multi-homing network,” IEICE Society Conference, Sep. 2004.

[2] R. Draves, “Default Address Selection for Internet Protocol version 6 (IPv6),” RFC3484, Feb. 2003.



Streaming service offered
by service provider 1
(prefix: 3100)

Remote-camera service
offered by service provider 2
(prefix: 3200)

```
File  Edit  Capture  Display  Tools

No. .  Time       Source                Destination           Protocol
10026 13.761883 3100::30              3100::a101:a931:f1fb: RTSP
10027 13.762615 3200::280:f0ff:fe54:6 3200::a101:a931:f1fb: HTTP
10028 13.762644 3200::a101:a931:f1fb: 3200::280:f0ff:fe54:6 TCP
10029 13.763550 3100::30              3100::a101:a931:f1fb: RTSP
10030 13.763580 3100::a101:a931:f1fb: 3100::30              TCP
10031 13.764064 3500::a603:280:f0ff:f 3500::a101:a931:f1fb: HTTP
10032 13.764089 3500::a101:a931:f1fb: 3500::a603:280:f0ff:f TCP
10033 13.770558 3200::280:f0ff:fe54:6 3200::a101:a931:f1fb: HTTP
10034 13.779922 3500::a603:280:f0ff:f 3500::a101:a931:f1fb: HTTP
10035 13.784895 3500::a603:280:f0ff:f 3500::a101:a931:f1fb: HTTP
10036 13.784935 3500::a101:a931:f1fb: 3500::a603:280:f0ff:f TCP
10037 13.786197 3500::a603:280:f0ff:f 3500::a101:a931:f1fb: HTTP
10038 13.788794 3500::a603:280:f0ff:f 3500::a101:a931:f1fb: HTTP
10039 13.788836 3500::a101:a931:f1fb: 3500::a603:280:f0ff:f TCP
10040 13.789997 3200::280:f0ff:fe54:6 3200::a101:a931:f1fb: HTTP
```

Captured packets show that source addresses assigned by service providers were correctly distinguished.

Remote-camera service
offered by service provider 3
(prefix: 3500)

Fig. 4. Simultaneous connection to three service providers.

Takaaki Moriya

Emerging Communication Architecture Project, NTT Network Service Systems Laboratories.

He received the B.E. degree in electronics engineering and the M.S. degree in frontier informatics from the University of Tokyo, Tokyo in 2001 and 2003, respectively. In 2003, he joined NTT Network Service Systems Laboratories, Tokyo, Japan. His research interests include mobile *ad hoc* networks, ubiquitous networks, and network measurement technology. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan and the Information Processing Society of Japan (IPSJ).

Hiroyuki Ohnishi

Emerging Communication Architecture Project, NTT Network Service Systems Laboratories.

He received the B.E. and M.E. degrees in mechanical engineering from Waseda University, Tokyo in 1996 and 1998, respectively. In 1998, he joined NTT Network Service Systems Laboratories, Tokyo, Japan. His research interests include ubiquitous and mobile networks. He has played an active role in IETF (The Internet Engineering Task Force) in developing and disseminating mobile networking technology. He received the Switching System Research Award from IEICE in 1999. He is a member of IEICE.

Yasuhiro Seki

Senior Research Engineer, Emerging Communication Architecture Project, NTT Network Service Systems Laboratories.

He received the B.E. and M.E. degrees in information sciences from the University of Tsukuba, Tsukuba, Ibaraki in 1988 and 1990, respectively. In 1990, he joined NTT Switching Systems Laboratories, Tokyo, Japan. He has been engaged in R&D of switching software for ISDN packet, ATM, and IMT-2000 systems. His research interests are now focused on mobile networking and ubiquitous networking. He is a member of IPSJ.

Tadashi Ito

Senior Research Engineer, Supervisor, Group Leader, Emerging Communication Architecture Project, NTT Network Service Systems Laboratories.

He received the B.E. and M.E. degrees in mechanical engineering from Keio University, Tokyo in 1985 and 1987, respectively. Since joining NTT Network Service Systems Laboratories in 1987, he has been engaged in research on ATM-LAN systems and MPLS systems. His research interests are now focused on ubiquitous networking. He is a member of IEICE and IEEE.