

Network Control Technology to Realize the NetroSphere Concept

Kenta Kawakami, Masahiro Kobayashi, Kazufumi Yogo, Kenzo Okuda, Masayuki Sekiguchi, Toshiyuki Kurahashi, Seisuke Arai, Toshiaki Tsuchiya, and Nobuya Shirai

Abstract

NTT has announced its NetroSphere concept, which was developed with the objective of promptly, reliably, and economically supplying services required by network users and middle B operators (the second B in the B2B2X (business-to-business-to-X) business model). NTT Network Technology Laboratories is conducting research on network control technologies to respond to the needs of diverse middle B operators flexibly and efficiently and to provide high-quality services with the aim of achieving the NetroSphere concept. This article examines the progress of these initiatives.

Keywords: network configuration and control, resource optimization, security

1. Introduction

NTT has announced its NetroSphere concept [1], which is being developed in order to promptly, reliably, and economically supply services required by network users and middle B operators (service operators). In this article, we introduce three network control technologies that enable us to respond flexibly and efficiently with high-quality service to the needs of various middle B operators. These technologies consist of *network abstraction* to implement network design and configuration, *network resource optimal control* to enable responses to temporary changes in demand, and *cyber-attack suppression control* that achieves stable service during cyber-attacks.

2. Key changes affecting the networks

First, the positioning and relevance of the technologies mentioned above are explained (**Fig. 1**). To realize the NetroSphere concept, it is necessary to respond to two kinds of changes: business models and traffic that is difficult to predict.

2.1 Changes to business models

Changes to business models means shifting from a standardized supply service model where carriers provide services through individual networks such as NGN (Next Generation Network), to a B2B2X (business-to-business-to-X) business model where middle B operators can build businesses and services according to their needs by freely incorporating original value-added functions to the base functions supplied by the carriers. Accommodating these changes requires networks that can respond flexibly to various middle B operator needs and that can promptly offer services. The technology to achieve this is network abstraction technology.

2.2 Unpredictable traffic changes

Network traffic up to now has been uniform and predictable, as service traffic has been dominated by services provided by carriers, for example, phone, Internet, and video services. However, in the NetroSphere era, we envisage an increase in the unpredictability of traffic changes. This may be caused by various elements such as rapid changes to traffic flow due to the start of new services from middle B operators with the previously mentioned business model

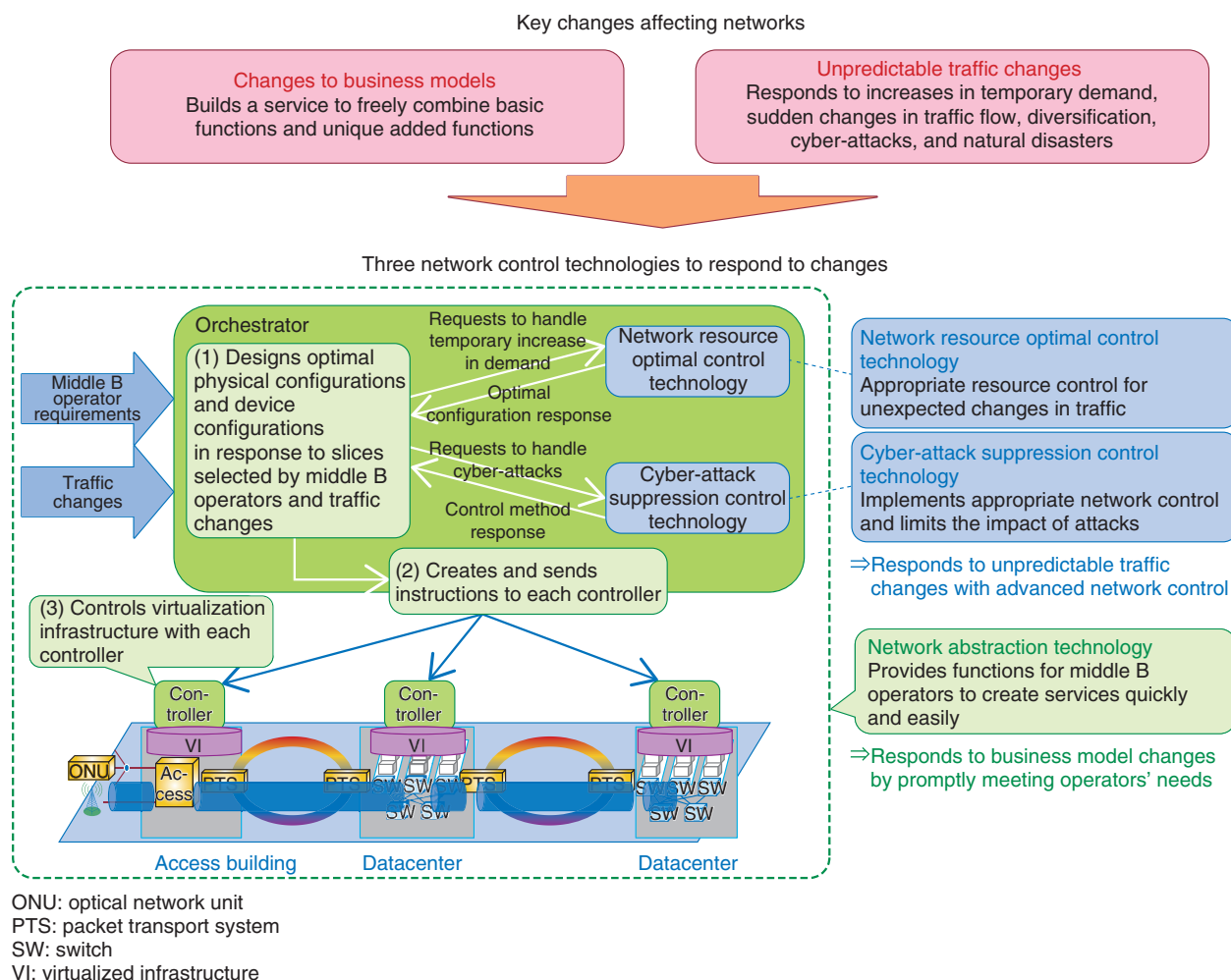


Fig. 1. Three network control technologies to respond to changes.

changes; diversification of traffic characteristics due to the spread of numerous services, especially IoT (Internet of Things) services; temporary increases in demand due to large-scale events; and rapid responses to major disasters and cyber-attacks. For the unpredictable traffic changes above, network resource optimal control technology makes it possible to respond to temporary changes in demand, and cyber-attack suppression control technology can achieve stable service quality during a cyber-attack. These two kinds of technology are used as network configuration algorithms within the network abstraction technologies, and are capable of handling unpredictable traffic changes.

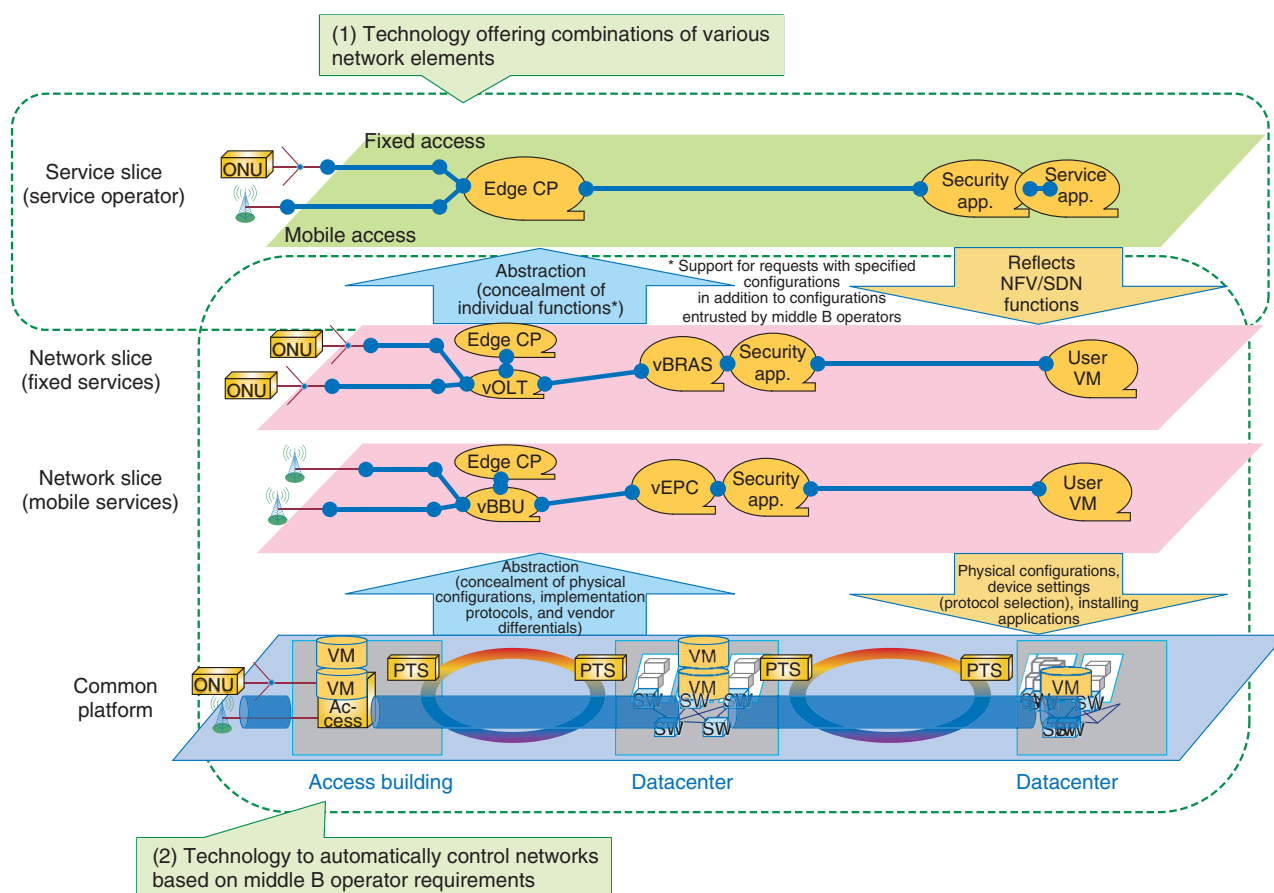
3. Network abstraction technologies

With network abstraction technologies, the network copes with business model changes using two network technologies. One offers combinations of various network elements, and the other automatically controls networks based on middle B operator requirements (Fig. 2).

3.1 Technology offering combinations of various network elements

With these technologies, we can define virtual networks that combine network elements for middle B operators as *service slices* and enable abstraction and customization of service slices according to middle B operators' use cases.

Service slices support patterns in which network



App: application
 BBU: base band unit
 BRAS: broadband remote access server
 CP: computing
 EPC: evolved packet core
 NFV: network functions virtualization [3]
 OLT: optical line terminal
 SDN: software-defined network
 VM: virtual machine

Fig. 2. Network abstraction technologies.

functions and the physical configuration are concealed and middle B operators entrust the specific configuration to us, as well as patterns in which middle B operators specify the physical configuration themselves. An example of the former would be holding a videoconference for a maximum of 10 bases within an end-to-end delay of not more than 500 ms, where the specific physical configuration is entrusted to us. An example of the latter could be placing a videoconferencing control server in a Tokyo datacenter, with the physical configuration specified.

With the entrusting pattern based on middle B operator requirements, the deployment and inter-

functional path of the required network and application functions are automatically determined according to the resource usage situation and service requirements. As a result, even operators (such as those from other industries participating in the Hikari Collaboration Model) who could not previously develop network-using services due to a lack of detailed knowledge about the network can now easily initiate services. With the specified physical configuration pattern, we can support some middle B operators such as existing carriers and Internet service providers (ISPs) who require the maintenance and operation model where they understand the network's

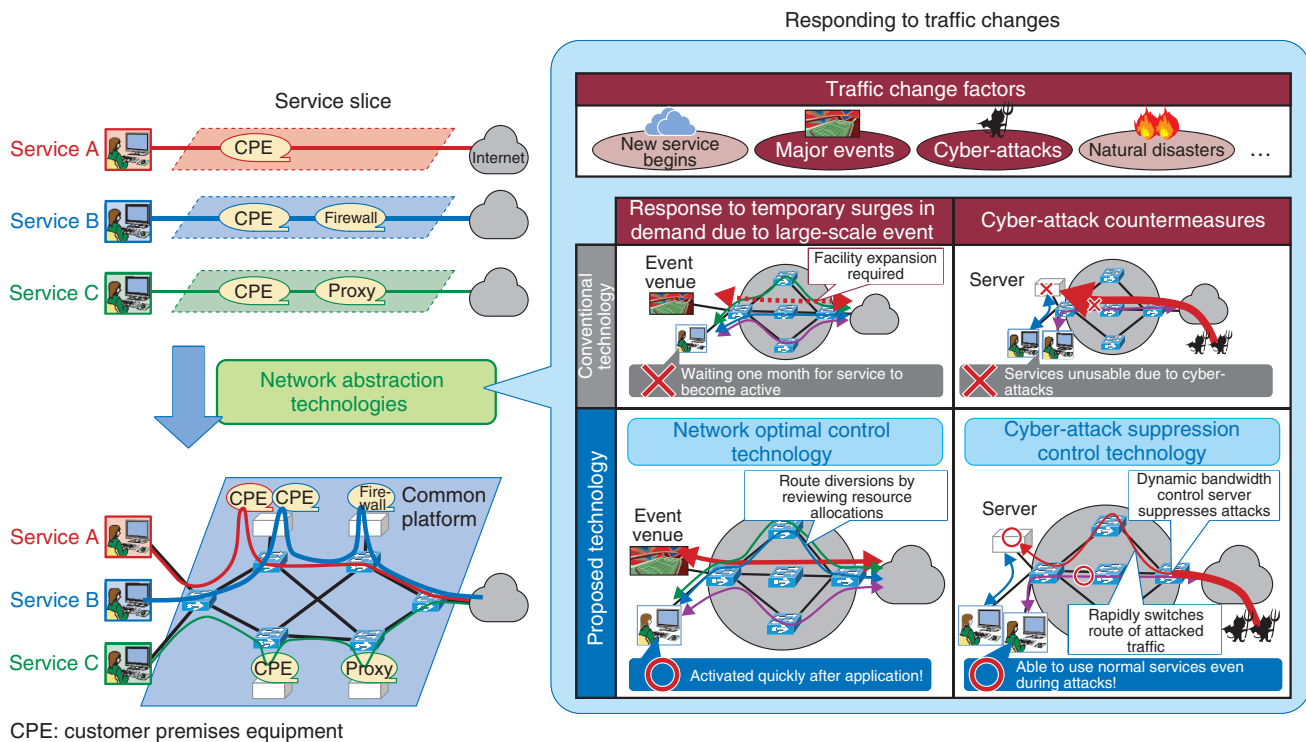


Fig. 3. Network resource optimal control and cyber-attack suppression control technologies.

specific physical configuration and can request to change the configuration as needed according to service usage conditions. We have succeeded in providing services responding to the needs of diverse middle B operators by supporting both of these patterns.

3.2 Technology to automatically control networks based on middle B operator requirements

This technology can automate at a stroke the processes from the determination of the network configuration through to the configuration of physical equipment based on middle B operators' requirements. With this technology, automated processing takes place with a series of virtual network function installations and equipment settings based on catalogues (service slice templates whose contents were previously determined) selected by middle B operators to match the service requirements. Prompt, easy service provision is achieved by providing functions for automating a series of network configuration processes to middle B operators as service slices.

In this way, by combining the two network abstraction technologies described above, network-using middle B operators can simply and promptly provide more diverse services than were previously available.

4. Network resource optimal control technology

With virtualized networks such as NetroSphere, we provide services by assigning physical network resources to service slices created based on middle B operator requirements [2]. These resource allocations enable free and flexible operation, but the allocation has an impact on facility use efficiency, service quality, and reliability. We aim to control resources appropriately in response to various traffic changes, so here, we introduce network optimal control technologies applied to respond to temporary increases in demand (Fig. 3).

When hosting new services with physical networks that already accommodate numerous services, capacity may be lacking due to insufficient usable resources, and new services may not be accommodated. In such cases, we can accommodate the relevant service capacity by reviewing the overall network resource allocation. For example, we can assume there will be large-scale demand for fixed periods such as during the Olympics and the World Cup. With conventional technology, problems with insufficient resources can be solved by expanding the facilities in advance. For the carrier, however, the equipment remains idle after

the event is over and becomes a case of over-investment. Moreover, customers have to wait for the service to launch during the period of facility expansion, so the application must be completed long before the actual usage period.

Accordingly, network resource optimal control technology does not involve expanding the facilities but instead accommodates new demand by redeploying existing services to alternative routes. This technology uses features of virtual networks capable of flexibly changing service slices and physical resource mapping. In this case, however, numerous restrictions must be considered. From the standpoint of operational costs, it is preferable to limit the number of resource-redeployed services as much as possible. From a service quality standpoint, it is necessary to preserve quality conditions required at different levels for each service, including bandwidth, delay, and packet loss ratios. Moreover, from a facility cost standpoint, it is desirable to expand surplus resources as much as possible after resource redeployment. The number of combinations of services for which resource redeployment is possible and that enable alternative routes is huge. Thus, it is very difficult to calculate the optimal solution to meet the above-mentioned restrictions from among all combinations. However, solutions can be discovered quickly using heuristic solutions^{*1}.

With this network resource optimal control technology, it is possible for carriers to effectively exploit existing facilities and for customers to use services promptly.

5. Cyber-attack suppression control technology

We have been conducting research on cyber-attack suppression control technology in order to prevent cyber-attacks such as harmful distributed denial of service (DDoS) attacks^{*2} (Fig. 3). DDoS attacks not only impede services supplied from targeted servers but also have an impact (e.g., congestion) on the network path links that cyber-attack traffic flows through. This becomes a problem for both middle B operators and carriers. Furthermore, with conventional means to prevent cyber-attacks that install security products on networks, it is necessary to forward all cyber-attack traffic to the security products. At such times, the security products may not function very well due to issues such as the previously mentioned route congestion.

Accordingly, in addition to security products, cyber-attack suppression control technology limits

the impact of cyber-attacks by controlling whole network paths and bandwidths. Examples of specific techniques include diversion route high-speed recalculation to accelerate route switching by searching for local diversion routes in the event of network congestion caused by DDoS attacks. This is deemed applicable for large networks such as ISP networks. Another technique is dynamic bandwidth control to limit the impact of cyber-attacks by dynamically controlling bandwidth so that the volume of traffic flowing to the target is distributed evenly at multiple gateways at the network endpoint nodes, and service is maintained. By using these technologies, we can provide customers with stable service quality even during cyber-attacks.

6. Future development

Any of the three technologies introduced in this article can be considered important factors in the need to realize robust networks that can respond to changes in the NetroSphere concept. In the future, in order to accelerate the implementation of these technologies, we will undertake wide-ranging collaborations both in Japan and abroad with vendors and research institutes, open source groups, and others specializing in various fields and will push forward with establishing technologies through joint research development and verification tests.

References

- [1] Press release issued by NTT on February 19, 2015.
<http://www.ntt.co.jp/news/2015/1502e/150219a.html>
- [2] K. Ono, H. Yoshioka, M. Kaneko, S. Kondoh, M. Miyasaka, Y. Soejima, T. Moriya, K. Kanishima, A. Masuda, J. Koga, T. Tsuchiya, N. Yamashita, K. Tsuchikawa, and T. Yamada, "Implementing the NetroSphere Concept at NTT," NTT Technical Review, Vol. 13, No. 10, 2015.
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201510fa2.html>
- [3] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration," V1.1.1, 2014.

^{*1} Heuristics solution: The heuristics solution uses experiential principles that may be effective to solve problems to derive executable solutions. It enables solutions to be calculated more quickly than an optimal solution, with some loss of accuracy.

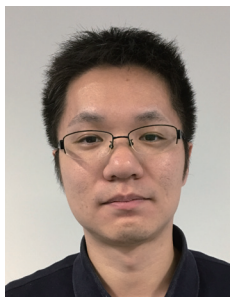
^{*2} DDoS attack: DDoS attacks render services inoperable at targeted servers either by consuming a large amount of bandwidth by sending out packets in large volumes or exploiting loads generated by, for example, session formations and the consumption of server resources such as CPU (central processing unit) and memory. DDoS attacks can be scaled up and become more difficult to defend in the case of multiple attackers or where attackers use multiple terminals simultaneously to attack the target.



Kenta Kawakami

Research Engineer, Network Technology Planning Group, Network Strategy Project, NTT Network Technology Laboratories.

He received a B.S. in information science from Kyushu University in 2004 and an M.E. in engineering from Tokyo Institute of Technology in 2006. In 2006, he joined NTT Service Integration Laboratories, where he was involved in researching and standardizing NGN architecture, especially IPTV (Internet protocol television) and QoS (quality of service) architecture. He has contributed to many standards developing organizations, including the European Telecommunications Standards Institute, Telecoms & Internet converged Services & Protocols for Advanced Network (ETSI TISPAN), 3GPP (3rd Generation Partnership Project), ITU-T (International Telecommunication Union, Telecommunication Standardization Sector), and BBF (Broadband Forum). He was a rapporteur of the standard specification for the DIAMETER protocol (ETSI TS 183 017 "Gq' interface based on DIAMETER protocol"). In 2010, he transferred to NTT EAST R&D Center and developed the domain name system for NGN. He also contributed to starting new IPv6 services and launched an NFV/SDN research project for application to the future carrier network. He has been with NTT Network Technology Laboratories since 2015.



Masahiro Kobayashi

Engineer, Communication Traffic & Service Quality Project, NTT Network Technology Laboratories.

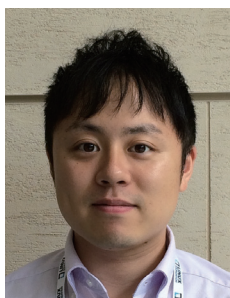
He received his B.S. and M.S. in information science from Tohoku University, Miyagi, in 2007 and 2009. He joined NTT in 2009. He is currently studying optimal resource control in the virtualized communication network at NTT Network Technology Laboratories. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).



Kazufumi Yogo

Engineer, Green IT Infrastructure Consideration Group, Technology Innovation Department, NTT WEST.

He received a B.E. in electrical and electronic engineering and an M.E. in informatics from Kyoto University in 2009 and 2011. He joined NTT Network Technology Laboratories in 2013 and has been researching network virtualization including SDN/NFV and network security. He is a member of IEICE.



Kenzo Okuda

Network Architecture Innovation Project, NTT Network Technology Laboratories.

He received his B.E. and M.E. in information and communication engineering from Osaka City University in 2012 and 2014. He joined NTT Network Technology Laboratories in 2014 and studied network architecture, including software-defined networks, service function chaining, hypervisor based virtualization, container-based virtualization, and deployment scenarios in the Network Architecture Innovation Project. He is a member of IEICE.



Masayuki Sekiguchi

Senior Research Engineer, Network Strategy Project, NTT Network Technology Laboratories.

He received a B.E. in engineering from Hosei University, Tokyo, in 1998. He joined NTT Communications in 2000 and worked as a network engineer in hosting service development. During 2008–2010, he worked as a system engineer at NTT Network Service Systems Laboratories developing an NGN session control server. During 2010–2014, he was with NTT Communications, where he was involved in the development of a VPN (virtual private network) service.



Toshiyuki Kurahashi

Senior Research Engineer, Network Architecture Innovation Project, NTT Network Technology Laboratories.

He received his B.E. and M.E. in information science from Kyoto University in 1995 and 1997. He joined NTT in 1997 and has been engaged in research and development of remote learning systems, integration of image and video systems, and development of NGN session control servers. He is currently researching the control architecture of a future carrier network, over which many kinds of services can be flexibly and easily deployed.



Seisuke Arai

Research Engineer, Network Architecture Innovation Project, NTT Network Technology Laboratories.

He received a B.E. in mechanical engineering from Doshisha University, Kyoto, in 1997 and an M.E. in information science from Japan Advanced Institute of Science and Technology, Ishikawa, in 1999. He joined NTT EAST in 1999 and was involved in network service and system development of Hikari Denwa and a carrier operating system. In 2015, he transferred to the Network Architecture Project of NTT Network Technology Laboratories, where he researched network orchestration and a service model driven networking engine. He is now researching next generation carrier transport and core network topology.



Toshiaki Tsuchiya

Senior Research Engineer, Communication Traffic & Service Quality Project, NTT Network Technology Laboratories.

He received his B.S. and M.S. in information science from Tokyo Institute of Technology in 1990 and 1992. He joined NTT laboratories in 1992 and has been working in the area of provisioning and management of telecommunication networks. His current research interests are queueing theory, performance evaluation, and resource optimization of communication systems. He is a member of IEICE and the Operations Research Society of Japan.



Nobuya Shirai

Senior Research Engineer, Network Architecture Innovation Project, NTT Network Technology Laboratories.

He received his B.S and M.S in materials science from Himeji Institute of Technology, Hyogo, in 1995 and 1997. He joined NTT in 1997 and was engaged in research and development of the broadband access server for FLET'S ADSL, B-FLET'S, and FLET'S HIKARI NEXT services at NTT WEST. He is currently researching network security of carrier networks.
