

A Nationwide 400-Gbps Backbone Network for Research and Education in Japan

Takashi KURIMOTO^{†a)}, Koji SASAYAMA[†], *Senior Members*, Osamu AKASHI[†], Kenjiro YAMANAKA[†], Naoya KITAGAWA[†], *Members*, and Shigeo URUSHIDANI[†], *Fellow*

SUMMARY This paper describes the architectural design, services, and operation and monitoring functions of Science Information NETwork 6 (SINET6), a 400-Gigabit Ethernet-based academic backbone network launched on a nationwide scale in April 2022. In response to the requirements from universities and research institutions, SINET upgraded its world-class network speed, improved its accessibility, enhanced services and security, incorporated 5G mobile functions, and strengthened international connectivity. With fully-meshed connectivity and fast rerouting, it attains nationwide high performance and high reliability. The evaluation results of network performance are also reported.

key words: *research and education, backbone network, L2VPN, L3VPN*

1. Introduction

Research and education networks (RENs) are dedicated to meeting the requirements of research and education (R&E) communities that cannot be handled by commercial network services. They are built by their nodes and links and many have dedicated international links. The unique requirements mainly come from data-driven research projects and their global collaboration.

Data-driven research, such as high-energy physics (e.g., LHC [1] in Switzerland, Belle II [2] in Japan), nuclear fusion science (e.g., ITER [3] in France, LHD [4] in Japan), and astronomy (e.g., eVLBI [5] in many sites), deal with a large volume of data in their experimentations to find new world-changing phenomena. Because the experimental instruments have become more sophisticated and the measuring devices for them have also been improved in terms of sensitivity and resolution, the volumes of data have been heavily increasing. The data measured by them are transferred to their computing/storage sites, screened and analyzed, and selected data are also stored. These data are shared among researchers and transferred between the related research sites. Therefore, they need very-high-speed networks to transfer such large volumes of data. There are also many other data-intensive applications in RENs such as supercomputers and artificial intelligence (AI)-based research.

The data mentioned above include competitive and confidential content in many cases that should be treated se-

curely. Closed communication environments are therefore required for these projects, and multiprotocol label switching (MPLS)-based VPNs are usually established for this purpose.

Many large experimental facilities cannot be built and managed without international collaboration. Therefore, they need to build global networks that share and transfer data among multiple countries. For example, the LHCONe [6] network for high-energy physics, including LHC and Belle II, has been built as a worldwide layer-3/2 VPN (L3/2VPN) over many RENs, providing a worldwide, high-speed, and secure communication environment.

For effective global collaborations, communities of RENs are also collaborating to develop their own tools to bridge the differences of distance and location. For example, researchers often suffer from slow data transfer speeds when using normal TCP over large-latency international lines. Data Mover Challenges [7] have been done using these international lines of many RENs, promoting the deployment of data transfer acceleration tools for over 100-Gbps speed. RENs also provide eduroam [8] for mutual use of campus Wi-Fi by global-scale authentication cooperation so that researchers can flexibly use these Wi-Fis in all over the world.

There are many RENs operating hierarchically in the world. Each country generally has at least one national REN (NREN) and sometimes accommodates regional RENs (e.g., on a state level in the US). There are also continental-level RENs funded by multiple RENs or countries that have strong cultural ties. For effective interconnectivity, there are academic Internet exchange points in major cities around the world where many RENs can be connected on a layer-2 or layer-3 level. The following are examples of RENs.

In the US, the Internet2 Network [9] and ESnet [10] are two major networks on a national level. The former serves over 300 universities and 46 regional and state networks (e.g., CalREN in California [11]), and the latter mainly serves 50 Department of Energy (DOE) research organizations. In Canada, CANARIE [12] is the NREN for 12 provincial and territorial networks (e.g., ORION in Ontario [13]). In Europe, the GÉANT Network [14] is the backbone network connecting 37 European NRENs, such as DFN [15] in Germany, JISC [16] in the UK, RENATER [17] in France, and SURF [18] in the Netherlands. In Northern Europe, NORDUnet [19] is the backbone network for five Nordic NRENs (e.g., Sunet [20] in Sweden). In Latin America, RedCLARA [21] provides the interconnection for twelve

Manuscript received February 27, 2023.

Manuscript revised May 12, 2023.

Manuscript publicized June 1, 2023.

[†]The authors are with the National Institute of Informatics, Tokyo, 101-8430 Japan.

a) E-mail: tkurimoto@nii.ac.jp

DOI: 10.1587/transcom.2022TMI0002

countries' NRENs such as RNP [22] in Brazil. In Africa, there are three main backbone networks: ASREN [23] for the Arab region, WACREN [24] for West and Central Africa, and UbuntuNet [25] for Eastern and Southern Africa. In the Asia-Pacific region, there are many NRENs, such as CER-NET [26] in China, KREONET [27] in Korea, SingAREN [28] in Singapore, AARNet [29] in Australia, REANNZ [30] in New Zealand, and SINET [31] in Japan, and the Asia Pacific Advanced Network (APAN) [32] aims to form a backbone network in the region. APAN itself does not have a real network but efforts have been made to form a backbone network in cooperation with the Asi@Connect project [33] supported by the European Union.

Among the aforementioned RENs, SINET is one of the most advanced networks in terms of network speed and service. A new SINET, SINET6, started its operation in April 2022 by introducing 400-Gigabit Ethernet (400GE)-based lines nationwide. The Internet2 network and ESnet also introduces 400-Gbps lines nationwide in Jan. 2022 and Dec. 2022, respectively, but SINET covers the national land more densely, which effectively enables about 1,000 universities and research institutions to have high-speed access environments to SINET. SINET provides a variety of network services including its original on-demand and 5G mobile services as well as VPN services to support a wide range of research activities.

This paper reports the architectural design, services, operation and monitoring functions, and performance evaluations of SINET6. The remainder of this paper is organized as follows. Section 2 clarifies the requirements for SINET6 from various aspects. Section 3 describes the network architecture and services to meet the requirements. Section 4 describes the operation and monitoring functions. Section 5 shows a number of performance evaluations of SINET6. Section 6 concludes the paper.

2. Requirements for SINET6

The National Institute of Informatics (NII) has held several SINET meetings regularly to hear from its users and to clarify the requirements for next-generation networks. Considering these requirements, we have determined the direction of SINET6 (Fig. 1). This section describes the main requirements and the corresponding directions.

2.1 Sufficient Bandwidth for Internet and VPNs

SINET needs to support a wide range of R&E activities and directly accommodate many large experimental facilities, supercomputers, cloud data centers, and so on (Fig. 2). To access these facilities, universities and research institutions can utilize SINET as both a high-speed Internet-access network and high-speed VPN by logically separating their access lines with VLANs. They usually plan to upgrade the campus LANs along with SINET. Therefore, a nationwide network speed upgrade has been the strongest request from users.

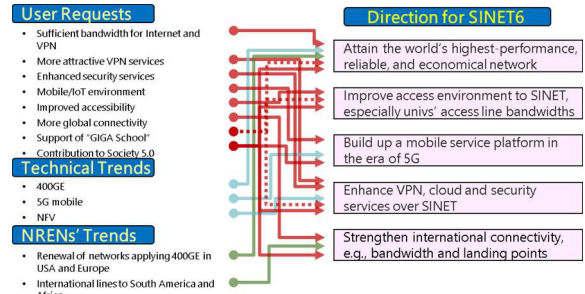


Fig. 1 User requirements and direction of SINET6.

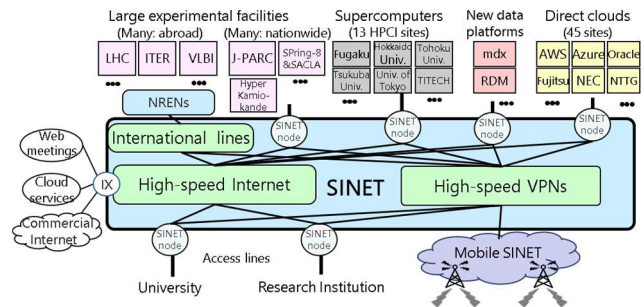


Fig. 2 Connectivity via SINET.

2.2 More Attractive VPN Services

SINET provides layer-3 VPN (L3VPN), point-to-point layer-2 VPN (L2VPN), multipoint-to-multipoint layer-2 VPN (virtual private LAN service; VPLS) services, and has been required to provide enhanced VPN capabilities to enrich communication environments. For example, many universities and research institutes have campuses in multiple locations, and the configuration of inter-campus networks through SINET is an issue. To develop an easy configuration change among multiple campuses, a service that enables multiple VLAN configurations without SINET operators is required. As another example, because various state-of-the-art equipment and devices are connected to SINET for demonstration experiments, there is a need for an on-demand service that enables users to freely change the VPN configuration such as bandwidth and delay. We have developed and improved our original services, such as virtual campus LAN and L2 on-demand with the RESTful API, in response to user requests.

Using resources provided by multiple cloud data centers for guaranteed performance, high availability, and fault tolerance, is considered as a new computing paradigm for high-performance scientific applications. Therefore, an environment that achieves inter-cloud computing by connecting distributed clouds via SINET is desired [34].

2.3 Enhanced Security

Universities and research institutes are required to further strengthen their voluntary cyber security systems in response

to security incidents such as information leaks. It is desired to improve their cyber security in cooperation with SINET, and to provide a safe and secure environment for all academic research fields as well as an environment to promote cyber security research. Therefore, SINET is required to provide services to support security improvements. One example is an environment to support security analysis provided by NII-SOCS [35], and another is a mitigation function to block malicious communications in the event of attacks such as a distributed denial of service (DDoS) attack.

2.4 Mobile/IoT Environment

SINET was originally a high-speed fixed network that directly accommodated numerous campus LANs nationwide. In the Internet-of-Things (IoT) era, many terminals including sensor devices in remote sites, should be connected to the campus LANs; moreover, closed network environments to transfer valuable research data securely would be needed. Therefore, a mobile network capability that can collect data in various fields throughout Japan would be required to be incorporated into SINET by a network configuration in which a secured dedicated mobile network is directly connected to a SINET VPN plane.

2.5 Improved Accessibility and More Global Connectivity

Large experimental facilities in Japan are usually located away from cities for a number of reasons, including avoiding urban influences and the need for large spaces. If the access line environment from the experimental facility to SINET is not sufficiently developed, high-speed communication becomes difficult. To solve this problem, it is desirable to increase the number of SINET points of presence (POPs) near the experimental facilities. In addition, several research fields have jointly developed large experimental facilities abroad. When access to these facilities is dependent on multiple overseas REN lines, the lines tend to be congested due to shared use. To improve communication with overseas experimental facilities, it is desirable to establish as many dedicated international circuits as possible.

3. Outline of SINET6

The physical network topology of SINET6 is shown in Fig. 3. Each circle on the map is a SINET POP. SINET has at least one POP in each prefecture and a total of 70 POPs. Each red line is a 400GE-based transmission line between SINET POPs, and the total line length is about 14,000 km. Unfortunately, Okinawa Prefecture, which uses approximately 1,000 km of fiber length from Kyushu, is connected by 100-Gbps lines due to the difficulty of deploying 400GE-based transmission technology. The bandwidths of the international lines are 200 Gbps to Los Angeles and New York, 100 Gbps to Amsterdam, 100 Gbps between Amsterdam and New York, 100 Gbps to Singapore, and 100 Gbps to Guam. These line bandwidths were determined on the basis of their

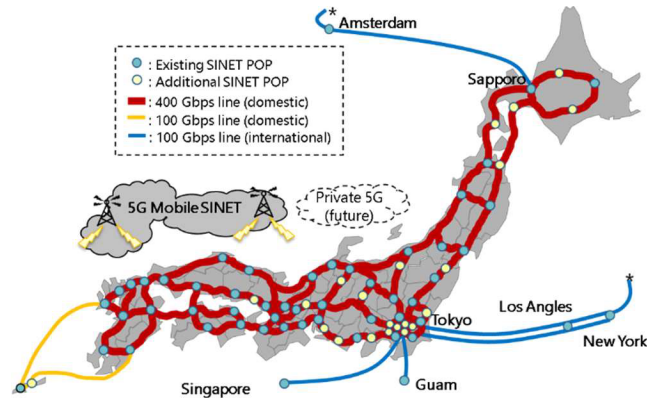


Fig. 3 Physical topology of SINET6.

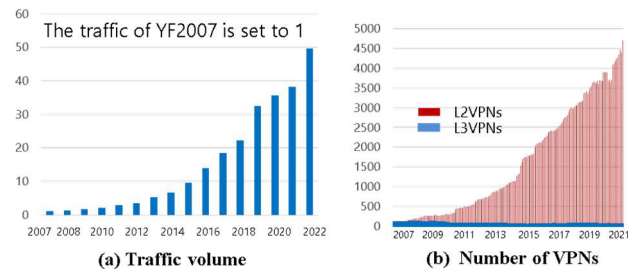


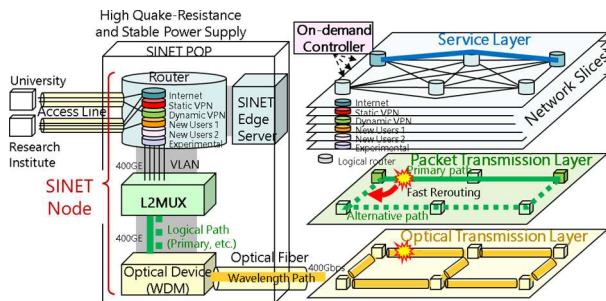
Fig. 4 Demand growth of SINET.

used bandwidths and traffic growth rates. The domestic traffic volume has grown by about 135% per year on average except in 2020 and 2021, which suffered as a result of COVID-19 (Fig. 4(a)), and SINET keeps each average line utilization rate at less than 50%. We then estimated that more than 70% of line sections would need at least 400 Gbps in March 2028 (the end time of SINET6). 400GE-based lines were therefore introduced nationwide by taking into account the balance between network construction and maintenance costs. As for international lines, each necessary bandwidth was determined toward March 2025 because we usually procure international lines every three years by taking into account the cost reduction trends.

SINET6 accommodates 1008 user organizations (including 100% of national, 95% of municipal, and 70% of private universities) and over 3 million users as of March 2023. SINET6 provides a variety of network services for these user organizations, research projects, and individual researchers. For example, VPN services have been popular with research projects for security reasons (Fig. 4(b)). For IoT researchers, SINET provides a mobile service called Mobile SINET that includes 5G capabilities as shown in Fig. 3. Table 1 shows a comparison between SINET5 (as of April 2016) and SINET6 (as of April 2022) from various aspects. The detailed comparisons are explained in the following sub-sections.

Table 1 Enhancement from SINET5 to SINET6.

Feature	SINET5 (as of April 2016)	SINET6
Network architecture	3-layer architecture, /MPLS-TP for packet transmission layer	3-layer architecture, / Segment routing for packet transmission layer
Backbone speed	100 Gbps	400 Gbps (upgrade plan; 800 Gbps on large traffic demand section)
Total IX capacity	200 Gbps	1.2 Tbps
International line	US 100 Gbps Europa 20G bps Singapore 10G bps	US 200 Gbps Europe 100 Gbps (upgrade plan; Europe 400 Gbps) Singapore 100 Gbps Guam 100 Gbps
Access line speed	10ME, 100ME, 1GE, 10GE, 40GE, 100GE	100ME, 1GE, 10GE, 40GE, 100GE, 400GE
Number of POPs	50 POPs	70 POPs
Access line redundant	None	CMUX for access line redundant
Mobile SINET	3G, 4G	4G, 5G , (local 5G)
On demand service	L2oD	L2oD, MroD, FoD
Performance monitor service	perfSONAR	perfSONAR BGP looking glass

**Fig. 5** Three-layer architecture of SINET6.

3.1 High-Performance Network Based on a Three-Layer Network Architecture

The three-layer network architecture of SINET6 is shown in Fig. 5. SINET6 is composed of an optical transmission layer, packet transmission layer, and service layer. This architecture is the same as that of SINET5 but we improved the rerouting functions of the transmission layer for more stable network operations in SINET6. In this section, each layer is described in detail.

Optical transmission layer: This layer is composed of optical fibers and wavelength-division multiplexing (WDM) devices that establish 400-Gbps wavelength paths between 400GE interfaces. For several routes using old optical fibers, we used two 200-Gbps wavelength paths for a 400GE interface. We placed SINET nodes on a building, called a SINET POP, which has superior earthquake resistance and high-power feeding capability. Two big earthquakes with a seismic intensity of 7 hit Kumamoto Prefecture in April 2016 but did not affect the Kumamoto SINET POP. We built an optical fiber network connecting these SINET POPs with sufficient route redundancy for reliability.

SINET traffic demand is expected to continue to increase. For example, there are plans to increase storage for High-Performance Computing Infrastructure (HPCI) data, which will result in increased storage backup traffic between

the Tokyo and Osaka areas. Therefore, the introduction of 800-Gbps lines is being considered as a medium-term future vision for SINET6.

Packet transmission layer: To provide stable network services, a packet transmission network is introduced. The majority of optical fibers are buried underground, and many construction works are carried out above and around them, such as restoring road surfaces, constructing new buildings, and embedding gas pipes and electricity cables. There are more than 1,000 fiber constructions per year in Japan. As these constructions involve the fibers being cut and then re-connected, the wavelength paths on the related routes are out of service during the constructions. The packet transmission network can prevent IP routers from becoming aware of the fiber cuts to stabilize IP routing. This layer is composed of layer-2 multiplexers (L2MUXs), each of which is connected to an IP router with 400GE and has logical paths set up between each pair of IP routers. Each logical path is established on the smallest-latency route. This layer also has rerouting functions for high availability, and direct logical paths can be immediately switched to alternative routes in case of fiber cuts and device failures. We introduced segment routing functions in this layer for more flexible switching, while SINET5 used MPLS-TP protection function in this layer and MPLS fast rerouting function in the service layer. The packet losses by protection switching were evaluated in field tests, and the results are shown in Sect. 5.

Service layer: This layer is composed of IP routers, each of which accommodates access lines of user organizations up to 400GE interfaces. Each IP router has six logical routers corresponding to the Internet (IPv4/IPv6), static VPN, dynamic VPN, two reserved services, and an experimental network. Each pair of IP routers is directly connected with an L2MUX logical path over the shortest route provided by the packet transmission layer, and as a result, IP routers are connected with a fully-meshed topology. This leads to the highest TCP performance with the lowest latency between any sites. A logical router connects to the other 69 logical routers by different VLANs corresponding to the L2MUX logical paths. As there are six logical routers in one IP router, there are a total of $69 \times 6 = 414$ VLANs per IP router connected by corresponding logical paths. In the entire network, 14,490 VLANs are connected with corresponding L2MUX logical paths. IP routers exchange bidirectional forwarding detection (BFD) packets to check the availabilities of the L2MUX logical paths. If IP routers detect no connectivity, they change the forwarding routes from direct routes to routes via relay IP routers. Through such multi-layer coordination, SINET6 has enhanced network availability.

SINET's Internet service is provided in an IPv4/IPv6 dual-stack manner. It provides IPv4/IPv6 full-route data to network researchers as needed. IP multicast capability, usually used for 8K video streaming, is also available. SINET is connected to four kinds of Internet Exchanges (IXs) and has peering with various Internet service providers (ISPs) via SINET gateway routers (GWs) in Tokyo and Osaka for commercial Internet access. The total bandwidth to the IXs

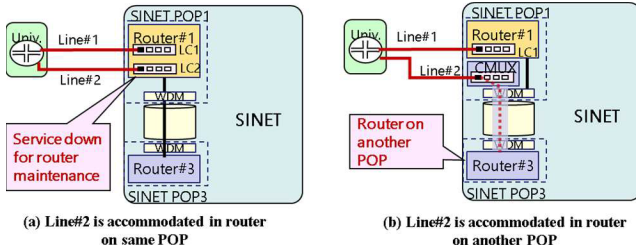


Fig. 6 Access line redundancy service.

is increased to 1.2 Tbps by taking account into the traffic increase of web-based videoconference applications such as Zoom, Teams, and Webex. The total bandwidth to the IXs in April 2016 was 200 Gbps.

3.2 Improvement of Access Environment

SINET6 has an additional 20 POPs (70 POPs in total) compared with SINET5 [37] to improve accessibility to SINET. In addition, SINET6 provides 400GE interfaces throughout Japan to accommodate user organizations' high-speed access lines. Researchers in every prefecture can enjoy ultra-high bandwidth (400 Gbps) communication with any other prefectures with minimum latency. The emphasis here is on the ability to provide up to 400 Gbps at end-to-end, regardless of which service the researchers use (e.g., Internet, VPN). There are 15 400GE, 83 100GE, 18 40GE, 850 10GE, and 640 GE access lines as of March 2023 compared with the 18 100GE, 7 40GE, 218 10GE, and 700 GE access lines in April 2016. The average speed of access lines in SINET6 is more than three times faster compared with that in SINET5.

Network availability has become critical for research. Failure of access lines connecting universities to SINET has a significant impact. For this reason, many universities are redundantly connecting to SINET via multiple lines, as shown in Fig. 6(a). However, in this case, communication is lost in the event of maintenance or failure of SINET router #1. To improve availability, we developed the access line redundant service, where a circuit multiplexer (CMUX) was introduced as shown in Fig. 6(b). Access lines are accommodated in this CMUX and in IP routers at different locations. This enables communication to continue even in the event of a SINET router failure or maintenance.

3.3 Mobile SINET

Mobile networks incorporated into SINET are classified into virtual and private networks. SINET introduced mobile functions up to 4G in Dec. 2018 and provided a mobile service suitable for IoT research. In April 2022, the service was expanded to include 5G capabilities, which has ultra-high-speed performance, and is currently being provided under the name Mobile SINET. It was constructed by logically building a SINET-dedicated mobile virtual network within public mobile networks and directly connecting it to the SINET6 backbone network. This architecture utilizes existing public

mobile networks to efficiently introduce mobile functions to SINET.

It has the following three features. First, Mobile SINET can collect data from university campuses where SINET access lines are connected as well as various areas such as sea and mountain areas where public mobile services are provided. Second, Mobile SINET can utilize the radio waves of the three major mobile carriers in Japan, so users can make complementary use of communication areas and functions that cannot be covered by a single carrier, which improves user convenience. Third, Mobile SINET directly connects SINET-dedicated mobile networks with the SINET6 backbone network to securely transfer valuable research data collected from various areas without being exposed to threats from the Internet. The SINET L2VPN service can securely transfer the collected data to university computers or commercial clouds directly connected to SINET6. In the near future, a private mobile network that can be equipped with unique network functions would be suitable for advanced academic research. We are now working to develop a private 5G network on SINET6 as a future research platform.

3.4 Enhance VPN, Cloud, and Security Services

SINET's VPN services are provided through network slices that are separate from the slice of the Internet-access service (as shown in Fig. 5). VPN services are utilized for research collaboration between user organizations, secure connections between user organizations and direct clouds, in-house connections for distributed campuses, and so on. There are about 4,600 L3VPNs and L2VPN/VPLSs as of March 2023. The number of these VPNs is about 2.3 times higher compared with that in April 2016. For an in-house connection, we introduced a "virtual campus LAN" service that connects geographically different sites as if they were on the same LAN. This service automatically detects VLAN IDs from each site and connects the same VLANs between multiple sites, enabling campus operators to freely set up many VLANs. There are more than 5,640 VLANs among about 200 sites (as of March, 2023). The virtual campus LANs as well as L3VPN and L2VPN/VPLS are provided on the same network slice for static VPNs. In addition, SINET enables users to set up L2VPN/VPLS in an on-demand manner. In addition, traffic mirroring services for security analysis and packet filtering services are provided to meet the demand for security enhancement. The following describes three types of network services that enable users to control their traffic: Layer-2 on Demand (L2oD), Mirror on Demand (MroD), and Filter on Demand (FoD).

L2oD service: On-demand VPNs are configured via SINET's on-demand controller. This service is utilized for various communications. For example, an assured bandwidth, low-delay VPN for remote control, an explicit route VPN for high-bandwidth experiments that need to avoid affecting other users, and a large-delay VPN for new protocols that are tuned for long-delay communication. This on-demand service is provided on a different network slice than

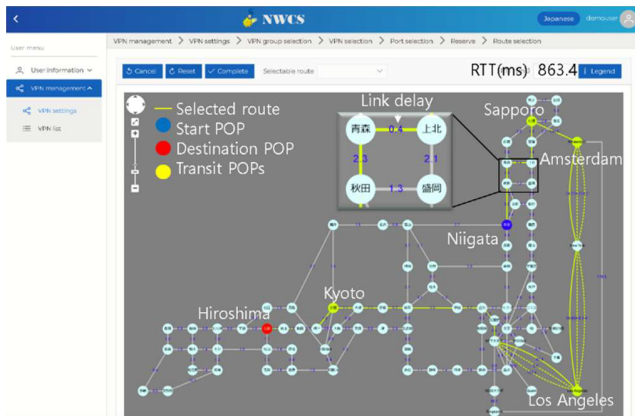


Fig. 7 Route indication function of L2oD. L2VPN is setup between Niigata and Hiroshima via Sapporo, Amsterdam, Los Angeles, and Kyoto. The selected route is shown as a yellow line. The link delay between POPs can be summed to obtain a rough estimate of the round-trip time (RTT). In this example, the RTT is estimated to be 863.4 ms.

the static VPNs because the configurations are frequently changed by users.

Users can flexibly establish a point-to-point layer-2 VPN (L2VPN) and a multipoint-to-multipoint layer-2 VPN (VPLS) among available sites. The path of L2VPN is usually established on the smallest latency route but can be optionally established on an arbitrary route. The route of an L2VPN path can be set up by looking at the network topology map and clicking the transit POPs. For example, as shown in Fig. 7, Niigata (blue circle) and Hiroshima (red circle) can be connected via Los Angeles and Amsterdam (yellow circle). When a path bandwidth is specified, a rate policing function is performed on the ingress router with the specified bandwidth, and packets are forwarded with assured forwarding (AF) class priority; AF class packets are forwarded with priority over best effort (BE) class packets. This makes approximate bandwidth guarantees possible.

The on-demand controller also provides a REST interface for users to build L2VPNs and VPLSs. This API enables users to flexibly set up and remove VPNs using their programs. The controller can also extend VPNs to SINET6 overseas routers located in Los Angeles, New York, Amsterdam, Singapore, and Guam, and connect dynamically to other NREN VPNs using the network service interface (NSI) [38] developed by the international project [39]. Currently, the Network Configuration (NETCONF) protocol [40] is used to control the logical router from the on-demand controller.

MroD and FoD service: SINET6 provides MroD and FoD for NII-SOCS [4] that analyzes the traffic of over 100 national organizations in cooperation with them (Fig. 8). The traffic of their access lines is mirrored and forwarded over L2VPNs to specified central locations as needed. Advanced security devices are placed at the central locations and analyze the mirrored traffic. Because the amount of aggregated mirrored traffic is enormous, mirroring can be turned on and off dynamically by the on-demand controller. FoD is also a service for NII-SOCS that prevents malicious traffic from

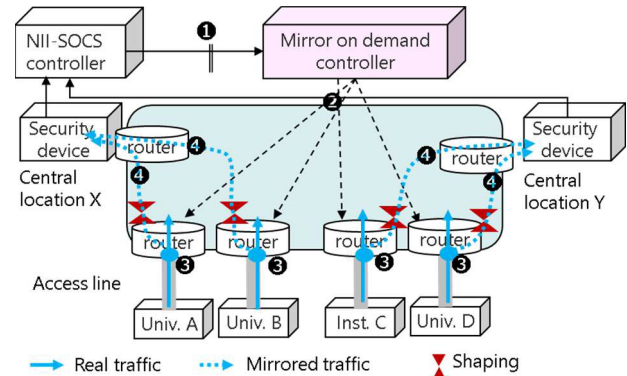


Fig. 8 Function overview of MroD service. (1) receive mirror-requests (target IP address CIDER) from NII-SOCS controller (2) configure mirror on router dynamically (3) packets are replicated (=mirroring) (4) forward mirrored packets to a central location.

being forwarded by SINET6 routers. The IP addresses of the access lines are registered in the system in advance; by specifying the SA/DA of the flows to be blocked via the API, it is possible to drop the packets of the flow at the IP router.

3.5 Strengthened International Connectivity

SINET6 increased the bandwidth between Japan and the USA from 100 to 200 Gbps to meet increasing traffic demands for international research collaboration. In addition, a new international 100-Gbps line was established between Japan and Guam. Guam is an important exchange point for the Oceania region and is used for another rerouting path to Singapore. SINET6 also has a Japan-Amsterdam 100-Gbps line that is connected with the Japan-US and US-Amsterdam lines to provide resilient network connectivity. On the path of international lines, we have set SINET6 POPs in Los Angeles, New York, Amsterdam, Singapore, and Guam and have multiple connections with other RENS' international lines for redundancy purposes.

During SINET6's term, the amount of research data such as LHC and ITER is expected to increase. Therefore, we are planning to increase the speed of the European line to 400 Gbps in the middle of SINET6's term.

4. Network Operation and Management

4.1 Domestic Network Operation

R&E activities are conducted 24 hours a day, 365 days a year. Therefore, SINET6 operations are also available 24 hours a day, 365 days a year. There are two operation categories: maintaining physical connectivity and providing a variety of network services.

The first category refers to the optical layer and packet transmission layer operations. Because each SINET6 L2MUX has multiple physical paths, a single point of failure will not affect communications. However, in the event of multiple concurrent optical fiber failures, communication may be disrupted due to the loss of rerouting routes. In the

case of a failure, the operation center coordinates a prompt restoration to prevent the isolation of a site due to such multiple failures.

The second category refers to an operation to provide network services such as Internet service and VPN services. The operation center monitors Internet reachability and VPN connectivity. When problems arise, the operation center contacts the institutions to quickly restore the system.

Taking severe and large disasters into consideration, network operation centers are set up in two locations, an East and West site, in Japan. Normally, network operations are conducted at the East site, but when the East site goes offline in the event of a disaster, operations can be continued at the West site.

4.2 International Network Operation

We have established international cooperative frameworks such as APOnet [41], Asia-pacific Europe Ring (AER) [42], and Advanced North Atlantic collaboration (ANA) [43]. Through these frameworks, SINET can use other RENs' international lines for mutual traffic backup. This international rerouting capability is essential for the continued support of international R&E projects. In these frameworks, participating RENs prepare backup path VLANs in advance and make them available to each other. By using these VLANs when an international line goes down, SINET and other participating RENs can reroute traffic through these VLANs. This rerouting is controlled by using priority at the interior gateway protocol (IGP) level. In cases of several international line failures in 2023, which include SINET's or other RENs' lines, the traffic was successfully rerouted automatically, enabling SINET to continue to provide connectivity to organizations in SINET. For example, SINET's Singapore–Japan line went down in December 2022, but VLANs on other RENs' lines could deliver traffic from Singapore to Japan via Hong Kong and Guam. In another case, SINET's Singapore–Japan and Japan–Amsterdam lines delivered traffic when other RENs' Singapore–Amsterdam line went down in October 2022.

4.3 Border Gateway Protocol Route Monitoring

We have developed a network behavior visualization system called the Flow Route Information Visualizing System (FRIVS). It collects flow information from all IP routers in SINET and border gateway protocol (BGP) route information from the route reflectors. It integrates this network status information with other related information and stores it in databases. By specifying a time period and filtering conditions, FRIVS can interactively visualize required network behaviors. Visualizing conditions, which are expressed by a sequence of filters, include source or destination IP addresses, port numbers, autonomous system (AS) numbers, organization numbers, and so on.

For example, FRIVS has been applied to monitor videoconference traffic, which has been important due to the

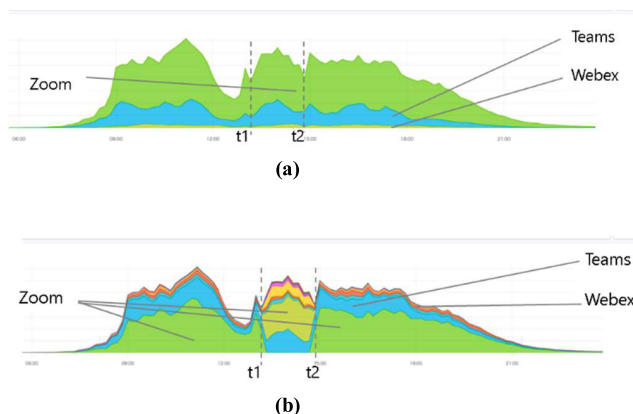


Fig. 9 (a) Observation using grouping by server IP address. It is difficult to infer the reason that caused drops in traffic at t1 and t2. (b) Observation using grouping by AS number. The traffic drops were potentially caused by the AS switchover, since the original AS number was changed at times t1 and t2.

COVID-19 pandemic. One notable discovery is the change of server locations of a conferencing system. Figure 9 shows the time transitions of traffic concerning three videoconference services. Figure 9(a) shows the traffic grouped by videoconference services to which IP addresses of the traffic belong. Figure 9(b) shows the traffic classified by AS numbers to which IP addresses of the traffic belongs. In Fig. 9(a), there are traffic drops at times t1 and t2, but the cause is unknown. However, Fig. 9(b) shows that the AS number of the Zoom traffic sources kept changing. This indicates that the drops in traffic at times t1 and t2 are due to server changes belonging to different ASes. In this case, changing the corresponding filters applied to the same network status data during the same time period helped identify these changes. It was important to grasp such changes to analyze videoconference quality.

4.4 Network Performance Monitoring

To manage the network quality, we have two traffic monitoring systems that monitor packet transmission layers and service layers, respectively. In the packet transmission layer, the amount of forwarded traffic per logical path is collected. In addition, the amount of forwarded traffic per quality of service (QoS) class and the number of packet losses per QoS class are collected at the L2MUX transit interface. At the service layer, the amount of forwarded traffic and packet loss per logical path is collected. This mechanism enables quick detection of network quality degradation.

For service layer network performance anomalies, it is important to be able to grasp the normal state through continuous performance measurement and reference to the results. perfSONAR [44], which has become the de facto standard in the academic network community, is a software tool for this purpose. For network performance measurement of SINET users and the R&E community, and for network monitoring by SINET itself, SINET6 has provided perfSONAR test points. Continuous measurement between multiple points

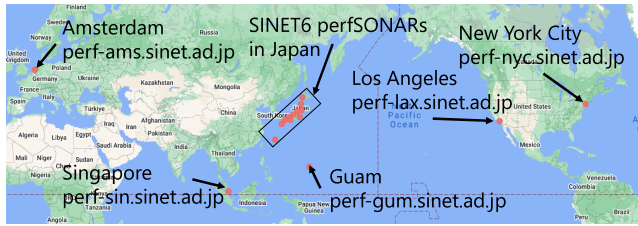


Fig. 10 SINET6 perfSONAR.

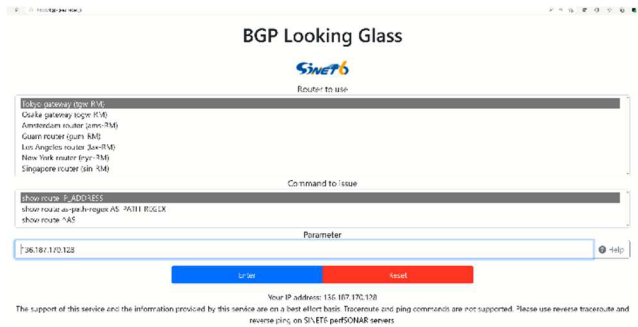


Fig. 11 SINET6 looking glass.

is necessary to detect network performance anomalies and where they occur. For this reason, SINET6 perfSONAR has 11 test points in Japan and 5 connection points with overseas networks (Fig. 10). TCP transfer speeds are measured and visualized by the tool.

The three features of SINET6 perfSONAR are as follows:

First, all 16 servers provide 100GE interfaces, and there are approximately 150 test points[†] for 100GE interfaces worldwide, so SINET provides about 10% of them. Second, the maximum window size is expanded from the standard (64M) to the advanced (512 MB), so that the long-distance TCP throughput test can be conducted at a higher speed. Third, the QoS class less than BE (LTBE) is available. A class with a lower priority than the normal BE is forcibly applied to the TCP throughput traffic originating from the SINET6 server. This feature protects general user traffic from being adversely affected by measurement traffic.

SINET6 also provides the Looking Glass tool as a new service (Fig. 11) [45]. Looking Glass provides users with information related to backbone routing. SINET6 Looking Glass enables users to search for the BGP information from 7 border routers (5 overseas routers and the Tokyo and Osaka gateways).

5. Evaluation

5.1 End-to-End Throughput and Round-Trip Time (RTT)

The end-to-end throughputs were evaluated. We set up loop-back L2VPNs between Tokyo and nine locations (Fig. 12)

[†]Number of servers belonging to “100 Gbps” community in PerfSONAR’s global node directory. (As of Jan. 2023)

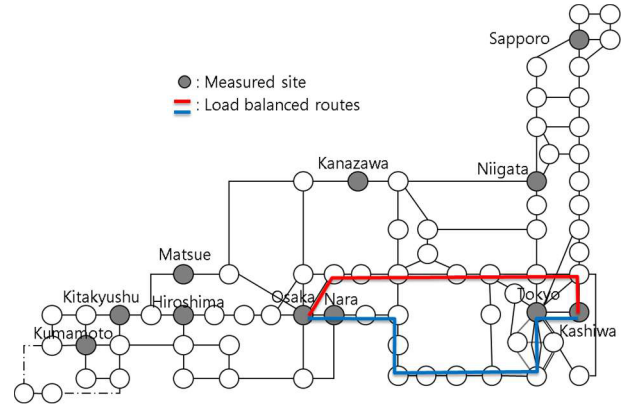


Fig. 12 End-to-end throughput evaluation.

Table 2 Measured throughputs and delays.

Measured Section	Throughput (Gbps)		Round-trip-time (msec)			
	1500B	9140B	Min	Avg	Max	Stdev
Tokyo-Niigata	376.9	395.9	5.414	5.635	6.049	0.118
Tokyo-Kanazawa	376.3	395.2	7.393	7.773	8.855	0.223
Tokyo-Osaka	377.4	396.1	8.471	8.788	9.059	0.137
Tokyo-Nara	376.3	395.2	8.642	8.913	9.174	0.130
Tokyo-Hiroshima	376.5	395.4	13.249	13.539	13.924	0.132
Tokyo-Matsue	377.1	395.9	13.337	13.729	14.005	0.140
Tokyo-Sapporo	377.4	396.1	13.478	13.822	14.216	0.155
Tokyo-Kumamoto	377.0	395.7	17.261	17.566	18.600	0.170
Tokyo-Kitakyushu	377.0	395.9	18.955	19.220	19.544	0.127

and used normal and jumbo packets (lengths of 1500B and 9140B, respectively). Because we need a header overhead (60B) for the L2VPN networking between logical routers, IP routers, and L2MUXs, 379 Gbps and 396 Gbps were the logical maximum throughputs for 1500B and 9140B IP packets, respectively. Table 2 shows that the maximum throughputs over SINET6 were achieved as expected. Note that SINET has the potential to forward over 400-Gbps traffic between two sites by using two different routes. We confirmed a throughput of 791.6 Gbps for 9140B packets between Kashiwa and Osaka by performing load balancing over the two different routes (blue and red lines). Table 2 also shows the evaluation results for round-trip delay and delay standard deviations, which were from 118 to 223 μ s.

Figure 13 shows the RTT measured between routers located at two POPs and its dependencies to the optical fiber length between POPs. As shown in this figure, it is proportional to the fiber length.

5.2 Recovery Times in Several Cases

Protection time depends on the failure event. The fastest protection (local repair) is designed to be less than 50 msec. This short-time switching does not affect IP routing. In a few cases, the longest protection (global repair) time is up to 500 msec. The IP layer fault detection time is adjusted to avoid conflicts with IP-router switching.

We also evaluated recovery times using L2MUX’s

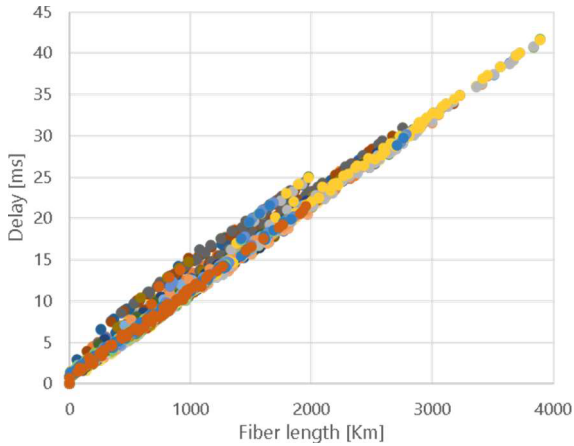


Fig. 13 RTT depending on fiber length.

rerouting functions in the event of a fiber failure between the aforementioned sites. The switching times using the rerouting functions were from 1.4 to 4.7 msec. If the direct logical paths become unavailable, the IP routers detect the status after 3 seconds by using the BFD protocol and change the routes immediately. If one IP router goes down, all other IP routers recalculate the routes using Open Shortest Path First (OSPF) v2/v3. As an IP router has 69 neighbor links, there are 2,415 neighbor links in one network slice, so the total number of neighbor links in SINET6 is 14,490. Nevertheless, we confirmed that OSPF convergence times were within 20 seconds.

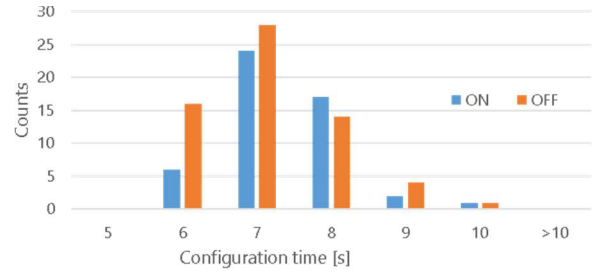
5.3 On-Demand Service Setup Time

We measured the configuration time to set up and delete each node for on-demand L2VPN/VPLSs. Figure 14(a) shows a histogram of configuration time. Among 864 samples, the median values were 8.3 and 8.4 secs for the setting and deleting, respectively. Note that we observed that in rare cases, the times became longer up to 4 minutes. This was caused by a number of important IP-router daemon processes running at the same time.

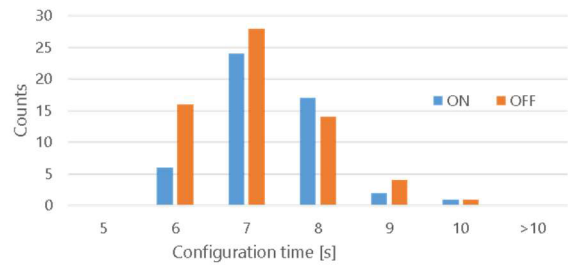
Figure 14(b) shows the configuration time of MroD. For the MroD service, it took about 6.5 secs each to turn the mirror on and off; for NETCONF session establishment, configuration submission, and session closing, it took about 1, 4.5, and 1 sec, respectively.

5.4 Access Line Redundant Switching Time

An evaluation of the switching time in the access line redundancy service was conducted. When the active access line was disconnected, the time required for both the Internet-access service and VPN service to simultaneously switch to the stand-by access line and recover communication was measured. As a result, it was confirmed that communication resumed within one sec.



(a) L2oD setup/delete time



(b) MroD configuration time

Fig. 14 On-demand service setup time.

6. Conclusion

This paper described a 400GE-based R&E network that provides a variety of network services, including its original on-demand services and advanced monitoring tools. A fully-meshed connection, sliced planes, and rerouting functions enhance its performance, stability, and reliability. Performance evaluation results in the real field showed that SINET6 has sufficient performance and reliability.

As the traffic demand is expected to continue increasing, we plan to introduce higher speed link technology, such as 800-Gbps transmission technology, into SINET6 for high-demand domestic sections around 2025. The international lines, such as Europe line, will be expanded to 400 Gbps in 2024. We will also study the feasibility of an Arctic-route under-sea cable to shorten the delay of European lines for higher data-transfer performance. As for wireless technologies, we started experimenting with private 5G technologies for field introduction. We are also interested in non-terrestrial networks (NTNs) for areas where cellular phone signals do not reach to further promote IoT research.

Toward the next SINET, we will continue to develop and deploy innovative networking technologies, such as ultra-high-speed transmission technology of over 1.6 Tbps, flexible wavelength networking technology, etc., to enable more high-capacity and stable network services for the academic community, while also responding economically to ever-increasing demand.

Acknowledgments

We wish to thank all members of the Organization of Science Network Operations and Coordination for their support of SINET. We are also grateful to Prof. Shunji Abe, Yusheng Ji, Kensuke Fukuda, Michihiro Koibuchi, Hiroki Takakura, Kento Aida, and the NII SINET operation team for their continuous cooperation.

References

- [1] "The Large Hadron Collider," CERN, <https://www.home.cern/science/accelerators/large-hadron-collider>
- [2] "Belle II, the first super B-Factory experiment," Belle II Organization, <https://www.belle2.org/>
- [3] "Fusion energy," ITER organization, <https://www.iter.org/>
- [4] "The large helical device (LHD)," National Institute for Fusion Science, https://www-lhd.nifs.ac.jp/pub/index_e.html
- [5] M. Sekido, et al., "Development of an e-VLBI data transport software suite with VDIF," IVS 2010, General Meeting Proceedings, pp.410–414, 2010.
- [6] "Large Hadron Collider Open Network Environment (LHCONE)," <https://lhcone.web.cern.ch/>
- [7] "Data Mover Challenge 2023," SupercomputingAsia (SCA) Conference, <https://www.nssc.sg/data-mover-challenge-2023/>
- [8] "eduroam," The eduroam initiative, <https://eduroam.org/>
- [9] "Internet2," Internet2, <https://internet2.edu/network/>
- [10] "Energy science network," ESnet, <https://www.es.net/>
- [11] "California Research and Education Network (CalREN)," CENIC, <https://cenic.org/>
- [12] "Canada's National Research and Education Network," CANARIE, <https://www.canarie.ca/network/>
- [13] "Ontario's only provincial research and education network," ORION, <https://www.orion.on.ca/>
- [14] "GÉANT is the collaboration of European National Research and Education Networks (NRENs)," GÉANT, <https://geant.org/>
- [15] "Deutsches forschungsnetz," DFN, <https://www.dfn.de/en/>
- [16] "Improving lives through digital transformation," Jisc, <https://www.jisc.ac.uk/>
- [17] "RENATER, the French National Telecommunications Network for Technology, Education and Research," <https://www.renater.fr/en/accueil-english/>
- [18] "SURF is the collaborative organization for IT in Dutch education and research," SURF, <https://www.surf.nl/en/>
- [19] "A voice for nordic values in international negotiations," NORDUnet, <https://nordunet.net/>
- [20] "Sunet (Swedish University Computer Network)," Swedish Research Council, <https://www.sunet.se/en/>
- [21] "RedCLARA: The Latin American space for collaboration and development in education, science and innovation," RedCLARA, <https://www.redclara.net/index.php/en/>
- [22] "The Brazilian network for education and research," RNP, <https://www.rnp.br/>
- [23] "The Arab States Research and Education Network," ASREN, <http://asrenorg.net/>
- [24] "The West and Central African Research and Education Network," WACREN, <https://wacren.net/en/>
- [25] "The alliance of Eastern and South African National Research and Education Networks (NRENs)," UbuntuNet Alliance for Research and Education Networking, <https://ubuntunet.net/>
- [26] "CERNET," <https://www.cernet.com/>
- [27] "Science super highway connecting to data," KREONET, <https://www.kreonet.net/eng/>
- [28] "SingAREN (Singapore Advanced Research and Education Network)," SingAREN, <https://www.singaren.net.sg/>
- [29] "Solutions made for research and education," AARNet, <https://www.aarnet.edu.au/>
- [30] "Moving data, mobilising knowledge," REANNZ, <https://www.reannz.co.nz/>
- [31] "Science Information NETWORK SINET6," National Institute of Informatics, <https://www.sinet.ad.jp/>
- [32] "APAN (the Asia Pacific Advanced Network)," APAN, <https://apan.net/>
- [33] "Asi@connect," TEIN*CC, <http://www.tein.asia/main/?mc=0>
- [34] A. Takefusa, S. Yokoyama, Y. Masatani, T. Tanjo, K. Saga, M. Nagaku, and K. Aida, "Virtual cloud service system for building effective inter-cloud applications," Proc. IEEE CloudCom 2017, pp.296–303, Dec. 2017.
- [35] NII Security Operation Collaboration Services (NII-SOCS): <https://www.nii.ac.jp/service/nii-socs/> (in Japanese).
- [36] D. Katz and D. Ward, "Bidirectional forwarding detection (BFD)," RFC5880, IETF, June 2010.
- [37] T. Kurimoto, S. Urushidani, H. Yamada, K. Yamanaka, M. Nakamura, S. Abe, K. Fukuda, M. Koibuchi, H. Takakura, S. Yamada, and Y. Ji, "SINET5: A low-latency and high-bandwidth backbone network for SDN/NFV era," IEEE ICC2017, 2017.
- [38] "Open Grid Forum (OGF) Network Service Interface," <http://www.ogf.org/>
- [39] A. Takefusa, J. Haga, U. Toseef, T. Ikeda, T. Kudoh, J. Tanaka, and K. Pentikousis, "Realizing business continuity planning over FELIX infrastructure," Proc. 8th IEEE/ACM International Conference on Utility and Cloud Computing (UCC 2015), pp.416–417, Dec. 2015
- [40] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network configuration protocol (NETCONF)," RFC6241, IETF, June 2011.
- [41] Asia Pacific Oceania Network, <https://www.aponet.global>
- [42] <https://www.sinet.ad.jp/news/2022-03-07post-9188> (in Japanese).
- [43] <https://itnews.iu.edu/articles/2022/New-network-partnership-strengthens-ties-between-North-America-Europe-.php>
- [44] <https://www.perfsonar.net/>
- [45] <https://bgp-lg-w.sinet.ad.jp>



Takashi Kurimoto is currently a Professor at NII, Japan, and is involved in the design and implementation of the national research and educational network, Science Information Network (SINET). He has been engaged in research of the switching technology for high-speed computer networks and deployment of next-generation networks. He is a member of Institute of Electronics, Information and Communication Engineers (IEICE), Institute of Electrical and Electronics Engineers (IEEE).



Koji Sasayama received his B.S. and M.S. degrees in Physics and his Ph.D. in Electrical Engineering from Kyoto University, Kyoto, Japan in 1985, 1987, and 1996, respectively. He is a Project Professor at NII, Japan, where he has been engaged in research and development on mobile network systems. He is a member of IEEE and IEICE of Japan, and he received their Young Engineer Award in 1993.



Osamu Akashi received his B.S. and M.S. degrees in Information Science and his Ph.D. in Mathematical and Computing Sciences from the Tokyo Institute of Technology in 1987, 1989, and 2001, respectively. He is a Project Professor at NII, Japan. His research interests are distributed systems, network management, and network architecture. He is a member of the Association of Computing Machinery (ACM), IEICE, Information Processing Society of Japan (IPSJ), and Japan Society for Software Science and Technol-

ogy (JSSST).



Kenjiro Yamanaka is currently an Associate Professor at NII, Japan, and he is involved in the design and implementation of SINET. He has been engaged in research of the switching technology for high-speed computer networks and deployment of next-generation networks.



Naoya Kitagawa received his Ph.D. in Information Science from Nagoya University, Japan in 2014. In 2014, he joined the Institute of Engineering, Tokyo University of Agriculture and Technology, as an Assistant Professor. Since 2020, he has been a Project Associate Professor with the Research and Development Center for Academic Networks, NII, Japan. His research interests include the Internet, network security, and distributed systems. He is a member of IEEE and IPSJ.



Shigeo Urushidani is a Professor and Deputy Director General of NII, Japan. He was involved in SINET as a visiting researcher in 1998 and has been responsible for its design and implementation since 2006. He received his B.E. and M.E. degrees from Kobe University in 1983 and 1985, respectively, and received his Ph.D. from the University of Tokyo in 2002. He was President of the Communications Society of IEICE from June 2018 to May 2019.