SINET6: Nationwide 400GE-Based Academic Backbone Network in Japan

Takashi Kurimoto, Koji Sasayama, Osamu Akashi, and Shigeo Urushidani
National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430 Japan
{tkurimoto, k_sasayama, akashi, and urushi}@nii.ac.jp

Abstract: This paper describes the practical network design of a newly-launched nationwide 400GE-based academic backbone network called SINET6. Its fully-meshed architecture with multi-layer network coordination, network services with on-demand capabilities, and performance evaluations are reported. © 2022 The Authors

1. Introduction

The Science Information Network (SINET) is a Japanese national research and education network that connects about 1,000 universities and research institutions. Data-driven research, such as on high-energy physics, nuclear fusion science, and astronomy, and AI-based research has been requiring more and more network bandwidth nationwide [1]. High-realistic communications using uncompressed 8K video also need high bandwidths, at least 25 Gbps and up to 150 Gbps. Research projects dealing with sensitive data, such as medical data, require closed network environments separated from the Internet for security reasons. Remote operations, such as remote surgery [2], require assured bandwidths between specified sites for stable operation. Such wide-ranging requirements have been urging SINET to evolve as a unique network in Japan. A new SINET, SINET6, was launched in April 2022 to meet the latest requirements. It places 70 SINET nodes nationwide and connects them over 400-Gigabit Ethernet (400GE)-based lines, excluding one prefecture. Its variety of network services including VPN and on-demand services effectively supports a wide range of research activities. It also incorporates 5G mobile technology for fostering IoT research. This paper reports its network architecture, network services, and performance evaluation results.

2. Network Architecture and Services

2.1. Requirements for SINET6

SINET needs to support a wide range of research and educational activities and directly accommodate many large experimental facilities, supercomputers, cloud data centers, and so on (Fig. 1). To access these facilities, researchers can utilize SINET as an Internet-access network and virtual private networks (VPNs). High-speed and high-transfer performance are the strongest requests from researchers for both network services. SINET has enhanced VPN capabilities at the request of users. In addition to L3VPN, L2VPN, and VPLS services, we have developed and improved our original services, such as virtual campus LAN, L2 on-demand with the RESTful API, and mobile VPN services, in response to user requests. Toward SINET6, we set design targets with a wide range of user requests in mind: attaining the world's highest performance using 400GE interfaces, improving the access environment to SINET, incorporating 5G mobile capability, enhancing security services, and strengthening international connectivity.

2.2. Network Architecture

The optical network topology of SINET6 is shown in Fig. 2. SINET6 has an additional 20 nodes (70 nodes in total) compared with SINET5 [3] in order to improve the accessibility to SINET and reduce the 400GE-based transmission distance. Each red line is a 400GE-based transmission line, and the total of the line lengths is about 14,000 km. SINET6 needed 400GE interfaces throughout Japan to accommodate user organizations' high-speed access lines. There are 12 400GE, 67 100GE, 19 40GE, 793 10GE, and 640 GE access lines (1,531 in total) as of Sep. 2022. Note that many user organizations have multiple campuses at distributed sites. It was difficult for Okinawa prefecture, about 1,000 km far from Kyushu Island, to deploy 400GE-based transmission technology over the existing undersea cables. The three-layer network architecture of SINET6 is shown in Fig. 3. The lowest layer is an optical transmission layer composed of optical fibers and WDM devices that establish 400-Gbps wavelength paths for 400GE interfaces. Here, for some routes using old optical fibers, we used two 200-Gbps wavelength paths for a 400GE interface. The middle layer is a packet transmission layer composed of layer-2 multiplexers (L2MUXs), which set up logical paths between each pair of IP routers. The top layer is a service layer composed of IP routers, each of which accommodates access lines of user organizations and uses multiple 400GE interfaces for the backbone. Each IP router has six logical routers for different services. The middle layer connects each pair of logical routers directly over the shortest route, leading to the highest performance between any sites. SINET6 ultimately has a fully-meshed topology in the service layer. The middle 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. IP routers exchange bidirectional forwarding detection (BFD) packets to check the availabilities of the direct logical paths. If they find there are no such paths, they change the forwarding routes from direct routes to routes via relay IP routers. Through such multi-layer coordination, SINET6 has enhanced network availability.

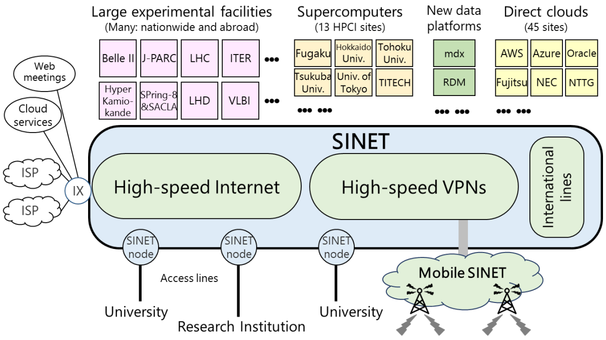

Fig. 1 In and around SINET

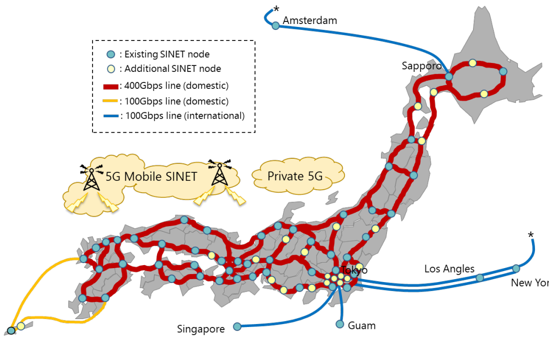

Fig. 2 Optical network topology of SINET6

2.3. *Network Services*

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's VPN services are provided by separate network slices from that of the Internet-access service (Fig. 3). VPN services are utilized for research collaboration among user organizations, secure connections between user organizations and direct clouds, in-house connections for distributed campuses, and so on. For an in-house connection, we introduced a "virtual campus LAN" service that connects geographically different sites as if they were in the same LAN. This service automatically detects VLAN IDs from each site and connects the same VLANs among multiple sites, enabling campus operators to freely set up many VLANs. There are more than 5,500 VLANs among about 200 sites, as of Sep. 2022. The virtual campus LANs as well as L3VPN and L2VPN/VPLS are provided on the same network slice for static VPNs. SINET can also set up L2VPN/VPLS in an on-demand manner. This service is utilized for remote operations that need assured bandwidth and small delay jitter, high-bandwidth experiments that need routes to be specified to avoid affecting other users, and experiments on new protocols that need a large delay. This on-demand service is provided on a different network slice from the other VPNs because the configurations are frequently changed by users.

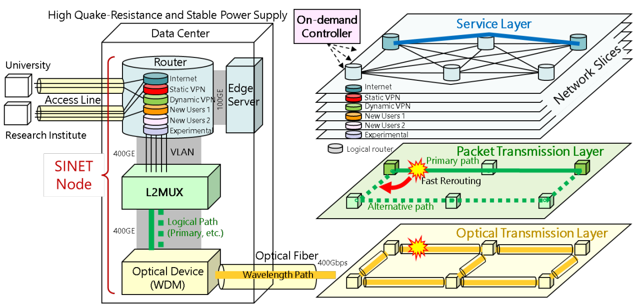

Fig. 3 Network architecture of SINET6

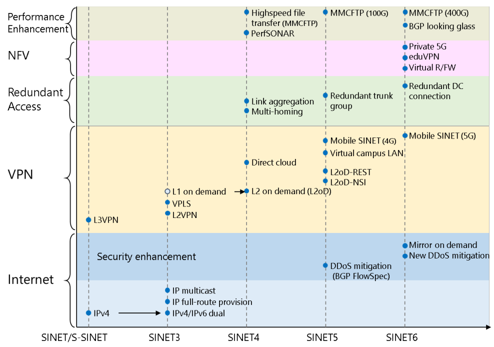

Fig. 4 Network service growth of SINET

2.4. *Network Resource Control Functions*

The static VPNs are configured manually by SINET operators. As for a virtual campus LAN, SINET operators specify the range of VLAN IDs, and virtual switches of IP routers automatically detect and set up the VLANs. On the other hand, on-demand VPNs are configured via SINET's on-demand controller, to which registered researchers input configuration parameters. An on-demand L2VPN is established by specifying a pair of access lines and their VLAN IDs. At the same time, its QoS class and necessary bandwidth can be specified. In addition, the path route of the L2VPN can be specified through a graphical user interface in order to get the necessary latency or avoid high-usage-rate routes. For a larger latency, researchers can specify even SINET's round-the-world route (Tokyo - Los Angeles - New York - Amsterdam - Sapporo). This on-demand controller also has a RESTful API for automatic control from other devices. In SINET6, this API was expanded to provide a new function, called mirror on demand, for NII-SOCS [4] that analyzes the traffic of over 100 national organizations in collaboration with them. The traffic of their access lines is mirrored and forwarded over L2VPNs to specified hub locations. Advanced security devices are placed at the hub locations and analyze the mirrored traffic. Since the amount of mirrored traffic is enormous, the mirrored targets can be turned on and off dynamically by the on-demand controller.

3. Performance Evaluations

3.1. End-to-End Throughput

End-to-end throughputs were evaluated during the construction phase of SINET6. In this evaluation, we set up loopback L2VPNs between Tokyo and nine locations (Fig. 5) and used normal and jumbo packets (lengths of 1500B and 9140B, respectively). Since 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 1 shows that the maximum throughputs over SINET6 were almost 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 routes (blue and red lines). Table 1 also shows the evaluation results for round-trip delay and delay deviation. The delay standard deviations were from 118 μs to 223 μs.

3.2. Recovery Times in Several Cases

We also evaluated recovery times using L2MUX's rerouting functions for the case where a fiber failure occurs between the above-mentioned sites. The switching times using rerouting functions were from 1.4 msec to 4.7 msec. If the direct logical paths become unavailable, IP routers detect the status after 3 seconds by using the BFD protocol and change the routes immediately. If an IP router goes down, all other IP routers recalculate the routes by OSPFv2/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. Yet, we confirmed that OSPF convergence times were within 20 seconds.

3.3. Setting Time of L2 on Demand

We measured the setting and deleting times of on-demand L2VPNs using the RESTful API. Among 100 samples, the average times were 8.6 seconds and 11.2 seconds, respectively, for the setting and deleting. Note that we observed that the times became longer at most 10 minutes in rare cases when supposedly some kinds of IP-router daemon processes ran.

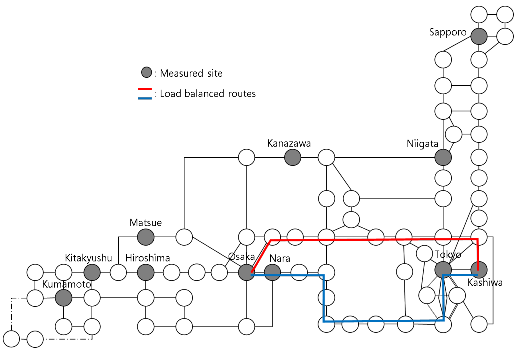

Fig. 5 Performance measurement sites

Table 1 Measured throughputs and delays

Measured Section	Throughput (Gbps)		Round-Trip Delay (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

4. Conclusion

This paper described a 400GE-based academic backbone network that provides a variety of network services through multi-layer coordination and sliced network planes. Performance evaluation results showed that SINET6 has full performance between any sites and can find new routes immediately when an optical fiber cut occurs.

References
[1] SINET usage examples: https://www.sinet.ad.jp/category/en/case_en
[2] Y. Ebihara et al, "Tele-assessment of bandwidth limitation for remote robotics surgery," Surgery Today, 2022.
[3] T. Kurimoto et al, "SINET5: A low-latency and high-bandwidth backbone network for SDN/NFV era," IEEE ICC2017, 2017.
[4] NII Security Operation Collaboration Services (NII-SOCS): https://www.nii.ac.jp/service/nii-socs/ (in Japanese)