Research toward Realizing a Future Network Architecture

Seisho Yasukawa, Hiroaki Sato, Takeshi Hirota, Takuya Tojo, Ken-ichi Endo, Yasunobu Kasahara, and Hiroshi Suzuki

Abstract

In the 5G (fifth-generation mobile communications) and Internet of Things era, trends such as work on social infrastructure services, the explosive increase in the number of terminals and the amount of network traffic, and the use of artificial intelligence for smart devices and services will have a huge impact on networks, thereby increasing the need for new network architectures. This article analyzes the impact of these trends, examines network requirements, and introduces initiatives to develop the necessary architectures and key technological elements verified by proof of concept.

Keywords: network architecture, 5G, PoC

1. Five elemental technologies

The NTT laboratories are studying network infrastructure architectures and practical elemental technologies that will provide B2B2X (business-to-business-to-X) model business and other societal infrastructures in the future as we fully enter the fifth-generation mobile communications and Internet of Things (5G/IoT) era.

This article reports on the following five elemental technologies.

(1) Network slice technology, which provides 5G transport able to accommodate multiple societal infrastructures such as self-driving and remote factory control and new digital services such as IoT. It can isolate multiple logical service networks for operators with different characteristics.

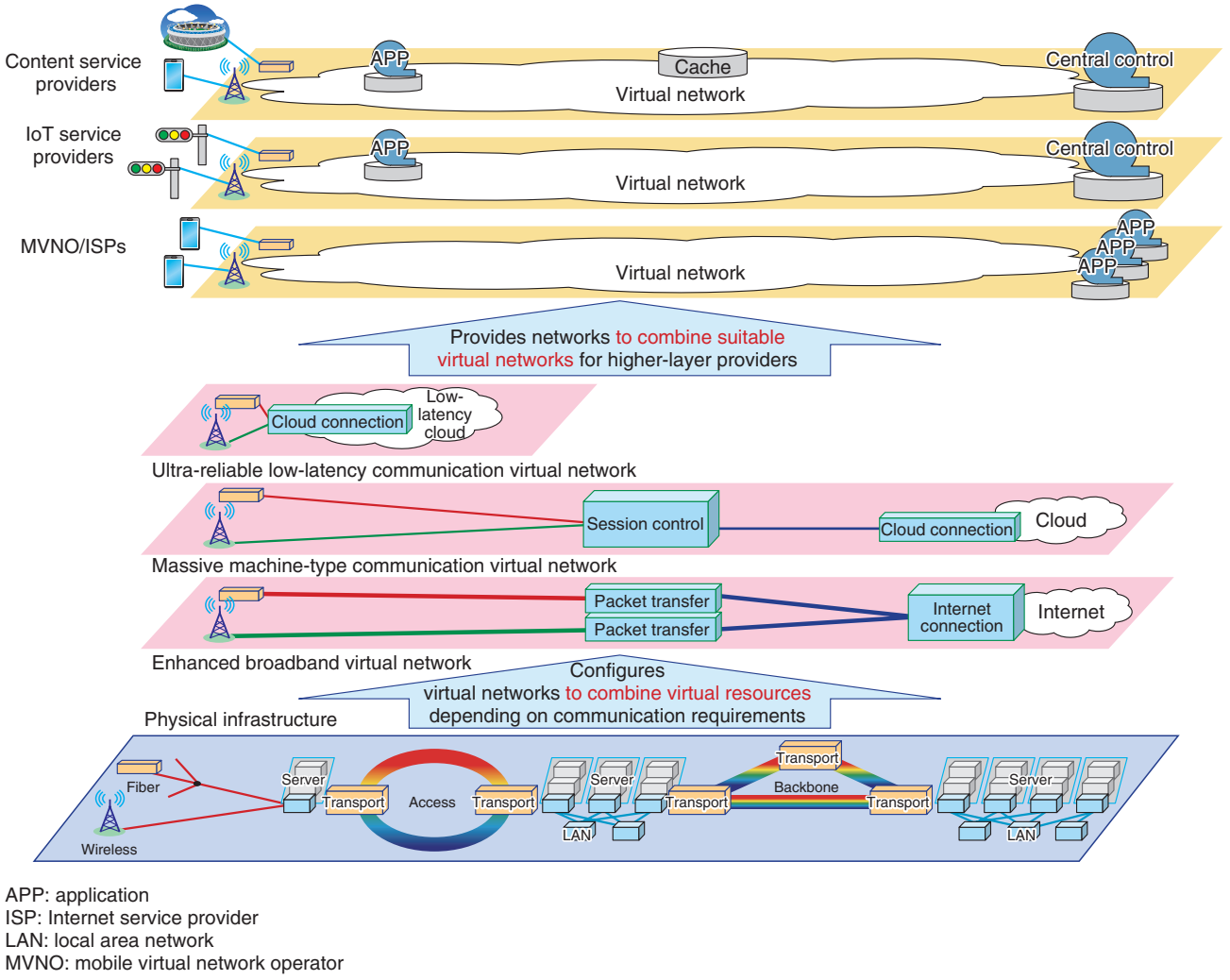
(2) Cloud native software-defined anything (SDx)* control technology, which enables cloud operators to create their own services by tuning and linking cloud applications and network applications from a simple catalog of applications on a self-service basis.

(3) Multi-layer software-defined networking (SDN) control technology, which provides integrated control of Internet protocol (IP) and transport layers using an SDN controller, for rapid service provision and resource optimization over the entire network.

(4) Content delivery network (CDN) technology, which is important for realizing 5G transport and will provide economical, high-quality distribution of high-definition, realistic video content including 4K/8K, augmented reality (AR), and virtual reality (VR) content.

(5) Inter-network cooperative mechanisms for protecting systems against massive cyberattacks. The mechanisms deal with increasingly large-scale and diverse distributed denial of service (DDoS) attacks by obtaining and spreading security threat information among network operators beforehand as a preventive defense against attacks. These mechanisms also link multiple network security functions to implement stronger detection and prevention functions.

* SDx: A general term for technology to control information technology infrastructure resources (servers, storage, networks, etc.) via software.



APP: application
ISP: Internet service provider
LAN: local area network
MVNO: mobile virtual network operator

Fig. 1. Network slice concept.

2. Network slice technology

Network slicing is a major new and innovative 5G era network technology, along with high-capacity packet transport and low-latency datacenter connection technologies. Network slicing involves managing physical equipment (physical resources) such as servers and routers as resources that can be partitioned virtually (virtual servers, virtual links, virtual network functions, etc.). This technology makes it possible to configure virtual networks (slices) by combining these virtual resources on the shared physical equipment (**Fig. 1**). A strength of network slicing, unlike conventional virtual private networks (VPN) and virtual routers, is that programmably controlled end-to-end networks can be configured immediately, like a cloud service, by flexibly combining virtual lines, virtual servers, virtual network functions, virtual high-order application functions, and virtual operations support systems and business support systems (OSS/BSS). The slice user is able to freely select network functions and control protocols and to control routes without being restricted by physical network functions, hierarchical structures, or operational rules.

As extreme examples, an IoT service provider could operate a network without using Ethernet or IP, or a content service provider could use its own routing control protocols and its own quality of service (QoS) policies that do not conform to international standards.

Network slicing is useful, for example, for achieving

a variety of communication conditions on the same physical equipment, as with 5G networks, or for providing program-controllable virtual resources to higher-layer service providers.

The international standards for 5G cover three communication modes for implementing various communication conditions: high-capacity broadband communication (e.g., 4K/8K video distribution), massive machine-type (many session/connection) communication (e.g., IoT), and ultra-reliable low-latency communication (e.g., for AR, self-driving cars); and we are studying ways to configure virtual networks that realize each of these (Fig. 1).

For example, most of the traffic in a high-capacity broadband communications network would be transferred via the Internet, so deploying a packet transport function with a tree structure and the Internet connection as the root would be efficient. For a many session/connection communication network, it would be effective to deploy many session/connection functions at the location where the sessions are needed. For an ultra-reliable low-latency communication network, deploying an ultralow-latency cloud near the access location would be effective for connecting to a datacenter within a range that meets latency requirements.

Three types of services for providing virtual resources to higher-layer service providers are being considered. They are: network slicing as a service (NSaaS), which provides an end-to-end virtual network with a full set of functions that can be oriented, for example, to Internet service providers (ISPs) and mobile virtual network operators (MVNO); network slicing platform as a service (NPaaS), which provides virtual network platforms that can be combined and customized by higher-layer service providers; and network slicing infrastructure as a service (NIaaS), which provides individual components such as virtual servers and virtual links.

For example, an MVNO or ISP could use NSaaS to procure a full set of virtual communications-operator facilities, including virtual OSS and BSS, and then conduct business using only its own subscriber web user interface. Or, as live events are held in cities like Tokyo, Nagoya, and Sapporo on a daily or weekly basis, a content provider could use NPaaS to move its own live video processing and distribution functions to buildings near the venues and configure virtual CDNs on a daily or weekly basis to satisfy latency requirements. The NTT laboratories are working on international standardization and research and development (R&D) on network slicing technologies including slice management, slice gateways, slice isolation, and telemetry, aiming for commercial implementations in 202x.

2.1 Slice management technology

Slice management technology is being modeled in three layers, for the infrastructure provider, slice provider, and slice operator (higher-layer service provider), and application programming interfaces (APIs) between these layers are being studied (**Fig. 2**).

The infrastructure provider owns the network and datacenter facilities and manages them as pools of resources such as virtual links (bandwidth) and virtual servers (central processing unit (CPU) capacity). A slice provider procures virtual resources from the infrastructure provider through an API and configures slices. In practical operation, this three-layer model is not limited to simple, horizontal specialization, and APIs are created taking all kinds of real configurations into consideration. For example, a slice operator might combine virtual resources from its own facilities with virtual resources from other facilities and control programs centrally without regard for whose facility is being used.

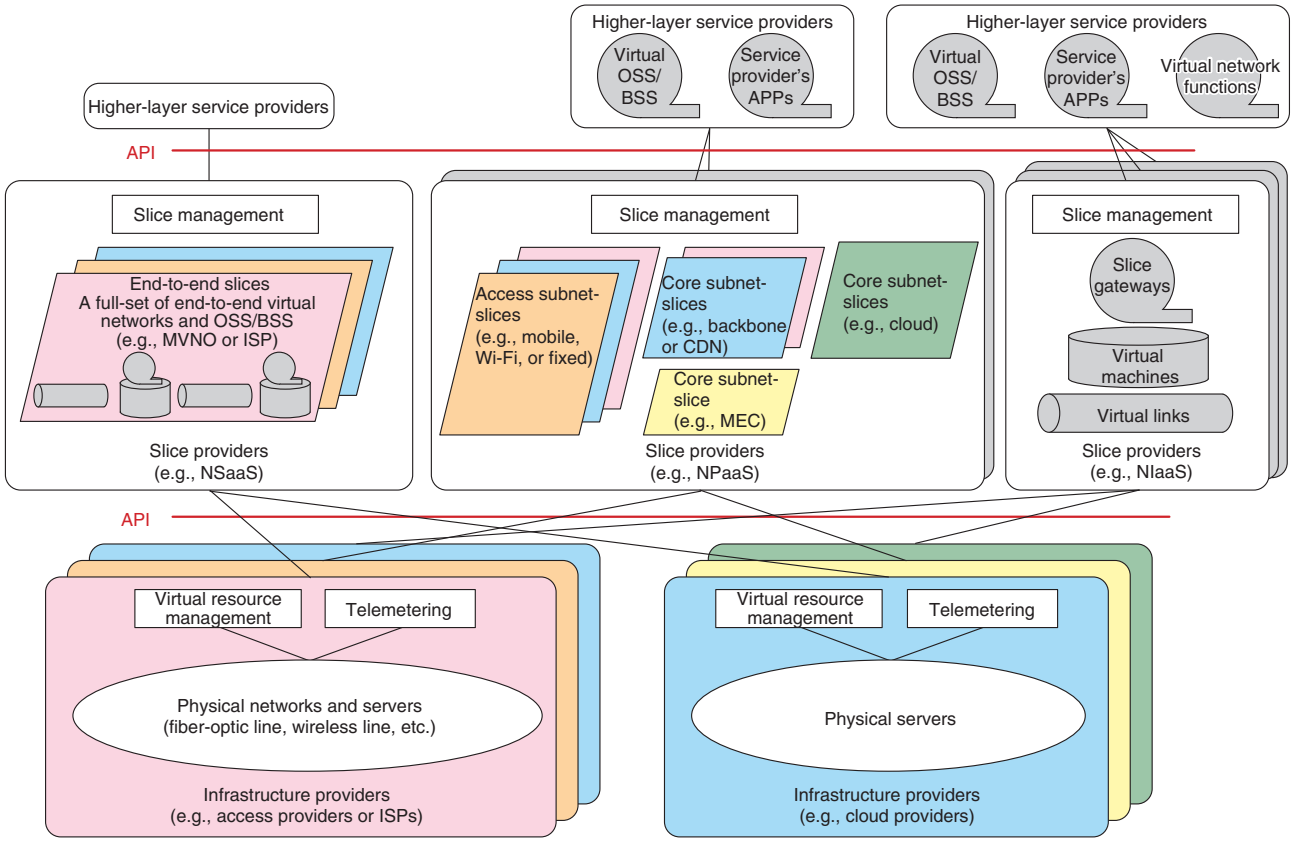
We are also studying ways to apply telemetry technology to programmable slice monitoring, control, and collection of analysis data, in units of slices, from APIs for slice operators.

2.2 Slice gateway technology

Slice gateway technology is used for connecting slices among slice providers and for connecting subslices within a slice provider. We are studying technologies to link slice management functionality with slice access authentication functionality and packet transport functions, to allow packets to be transported to appropriate slices (or subslices) based on slice connection policies. It also provides the edge functionality for slice isolation, as described next.

2.3 Slice isolation technology

Slice isolation involves isolating end-to-end traffic flow among slices, over link segments, including traffic within physical servers. The future goal is to achieve complete noninterference among slices so they will not affect each other, regardless of traffic congestion, functional faults, or software bugs. However, this is difficult to achieve with the current virtualization technology, so we are studying implementations ranging from loose isolation, on the level of controlling QoS priorities, to strict isolation, which



MEC: multi-access edge computing

Fig. 2. Network slice model.

maintains a higher degree of noninterference by securing resources such as virtual link bandwidth and virtual server CPU. For virtual link protocols in particular, there are international standard protocols that can separate multiple flows, for example, VXLAN (Virtual eXtensible Local Area Network), MPLS (Multi-Protocol Label Switching), and segment routing (SR). The NTT laboratories are working to augment these protocols to incorporate requirements for isolation and create new international standards.

3. Cloud native SDx control technology

Cloud native SDx control provides services easily and rapidly using automatic end-to-end control for network and cloud environments. It also offers the applications needed to provide services, rather than just providing individual network services (**Fig. 3**).

Conventional network services were simply functions that connect service users and service providers. Service providers are now providing diverse services on cloud environments, but the inability of cloud platforms to coordinate with networks is an obstacle to providing services quickly. As such, we aim to achieve rapid provision of services by collectively controlling networks, cloud environments used by service providers, and even applications. Implementing this concept requires mechanisms to automatically configure resources for providing services (networks, cloud resources, etc.), and to manage the information needed to support the resources.

We are studying ways to provide these automated mechanisms as user-friendly service configuration patterns that service providers can customize according to their own services, based on various technologies such as cloud environment workflows, cloud environment control, and network control. Automatic control of these various resources also requires appropriate management of information, such as what resources are being controlled, the state of each

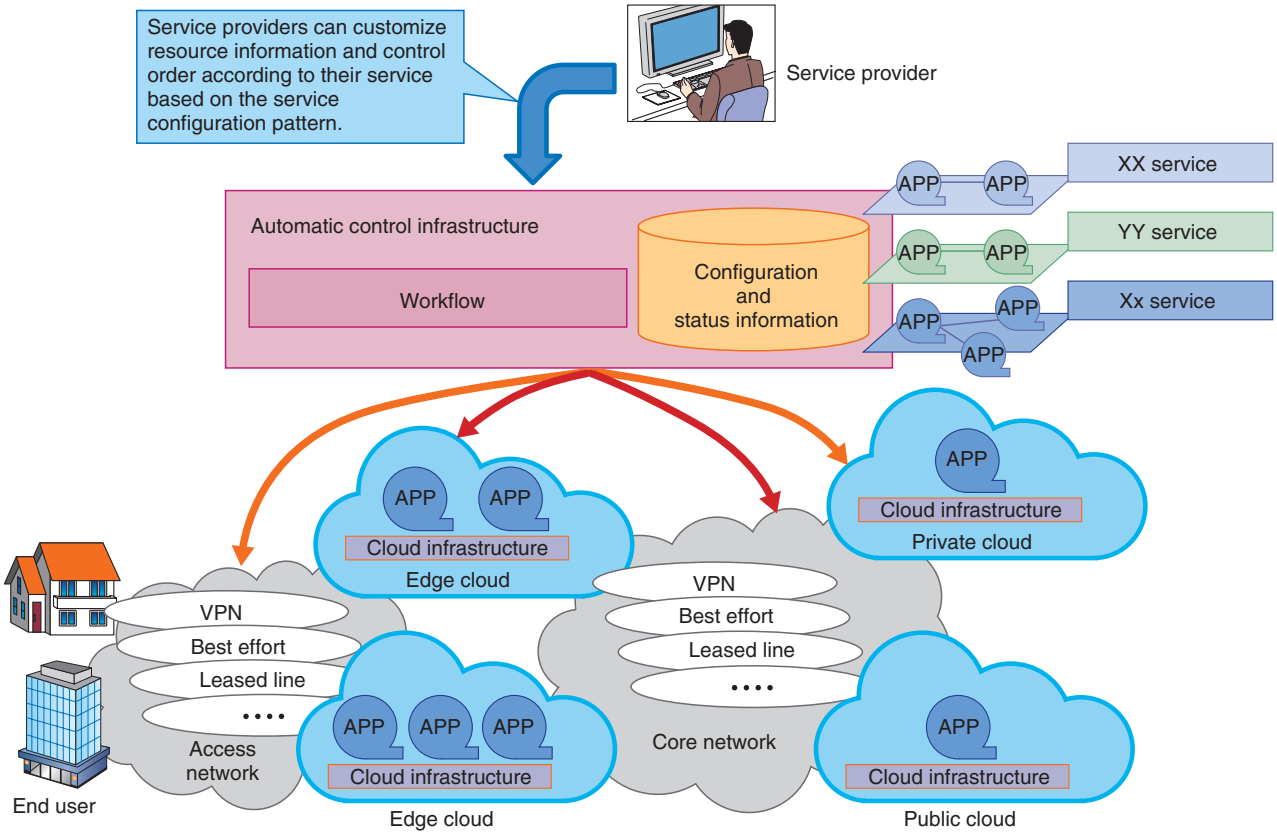


Fig. 3. Cloud native SDx control technology.

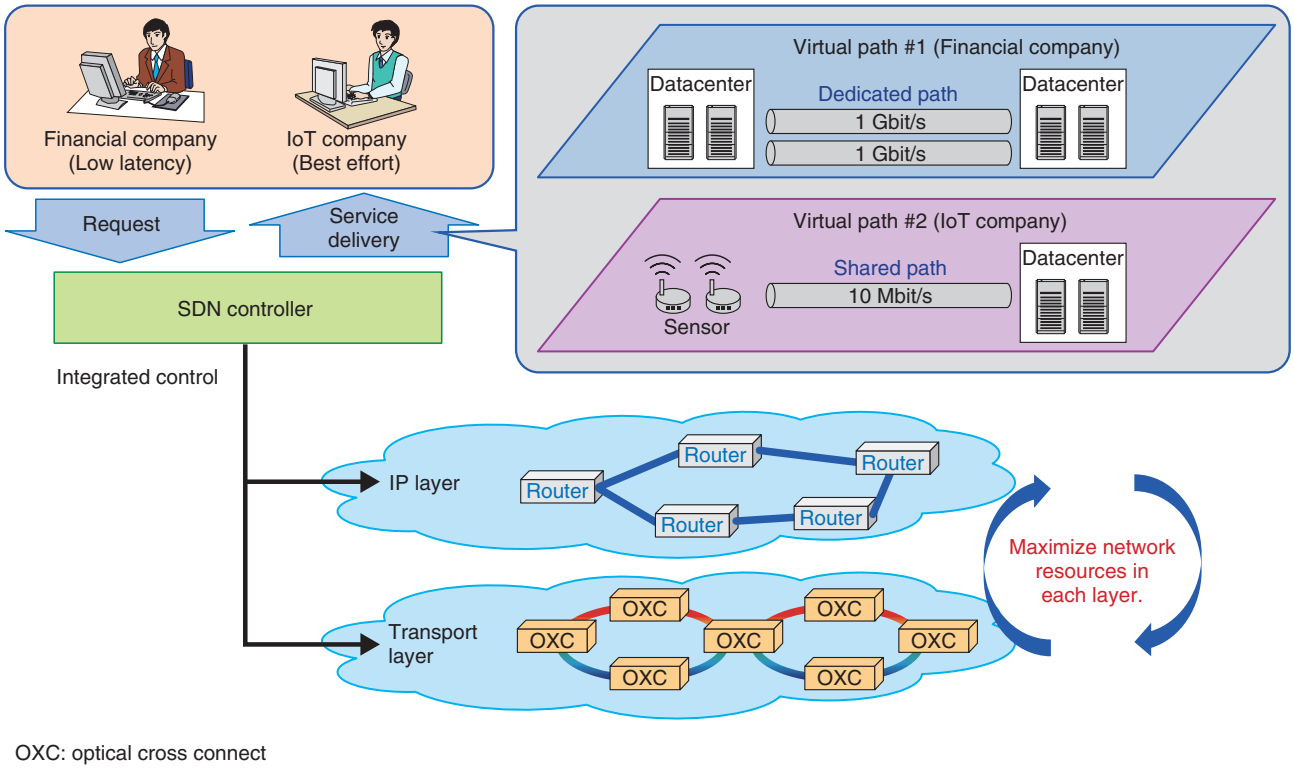
resource, and in what order settings need to be applied. Consequently, we have been studying models for entities being controlled and ways to manage overall configuration and state information, so that the various entities being controlled can be handled uniformly, rather than being dependent on particular services or physical equipment.

By establishing methods for the modeling and configuration management that we are currently studying, and building them into an automated control mechanism, we will realize a control platform able to centrally manage the resources needed for services and to control them automatically.

4. Multi-layer SDN control technology

We are studying multi-layer SDN control technology in order to achieve rapid service provision and overall optimization of network resources. Multi-layer SDN control integrates the control of IP and transport layers from the SDN controller, enabling the settings needed in routers and transport equipment to be done simultaneously, so that paths for different types of services such as IP-VPN or dedicated Ethernet lines can be provided on-demand from the SDN controller (**Fig. 4**). In addition to working to achieve rapid provision of services in this way, we are also studying ways to provide various grades of quality and reliability, in anticipation of the various levels of service that will be required in the 5G era [1].

Specifically, we are studying (1) implementation of routing control and protection in the IP layer with SR suitable for SDN control, (2) implementation of routing control and restoration in the transport layer with optical wavelength switching, (3) real-time monitoring of the network state using streaming telemetry technology, and (4) optical wavelength defragmentation to reorganize fragmented optical wavelengths (**Fig. 5**). By combining these elemental technologies, we aim to achieve graded quality and reliability, an SDN controller that can control IP and transport layers autonomously according to network conditions, and new network operations that will maximize the utilization of all network resources. We are currently



OXC: optical cross connect

Fig. 4. Multi-layer SDN control technology.

implementing prototypes of the controller functions shown in Fig. 5, based on an open-source SDN controller called ONOS (Open Network Operating System) and verifying the technology as we work to establish multi-layer control technology.

5. CDN technology

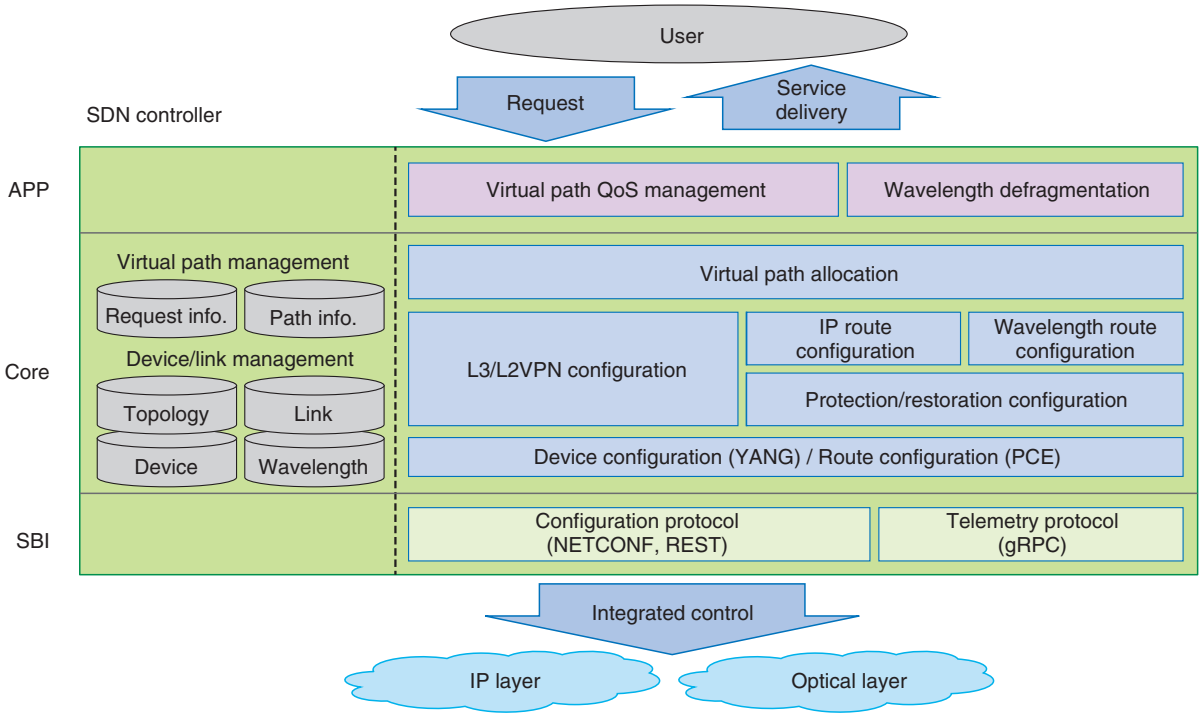
We are studying CDN technologies for high quality, economical distribution of high-definition, highly realistic next-generation video content, including 4K/8K and AR/VR (**Fig. 6**). CDN is based on three key technologies: video quality of experience (QoE) control and distribution design technology, real-time high-capacity distribution technology, and state visualization technology.

5.1 Video QoE control and distribution design technology

Video QoE control and distribution design technology is designed to implement video content distribution economically, based on QoE. It will be able to preserve QoE while achieving efficient utilization of facilities by optimizing the balance between QoE and facility resources. It will use information measured from the various equipment, applications, and terminals on the network to estimate QoE, viewing conditions, and the states of servers, networks, and other resources. It will select distribution servers and routes (server/content navigation) to control traffic according to factors such as the viewer's subscribed services, and perform content cache placement linked with this control.

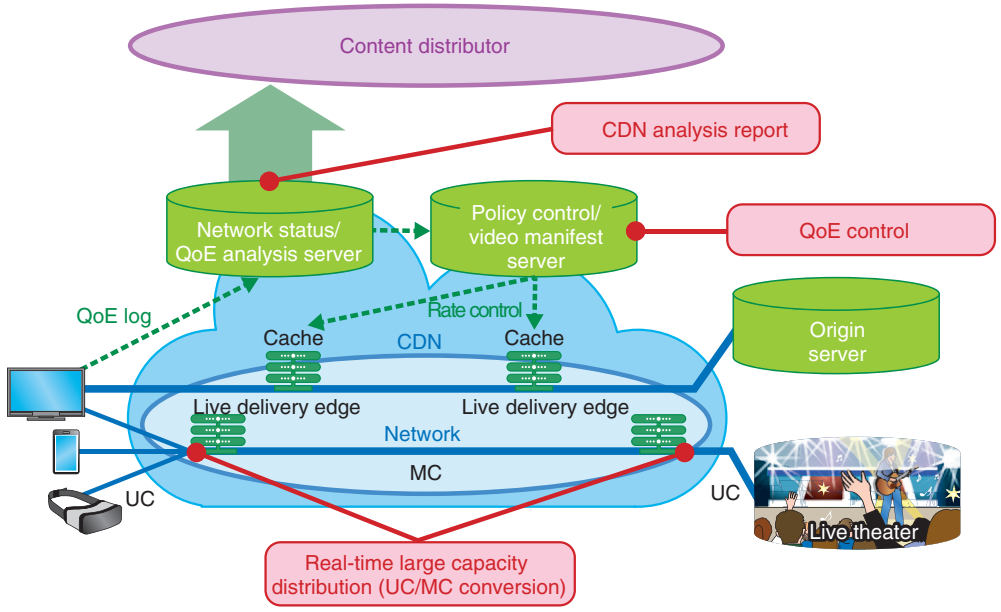
5.2 Real-time high-capacity distribution technology

Real-time high-capacity distribution technology realizes efficient and stable, high-capacity live video distribution. Normally, HTTP (Hypertext Transfer Protocol) based unicast communication is used between distribution servers and terminals, so when viewer demand increases due to events such as live coverage, the load on distribution servers and the network increases greatly. Converting distribution over the network segments to multicast and leaving distribution server and terminal communication as unicast (unicast/multicast conversion) makes it possible to avoid multiple distributions of the same live



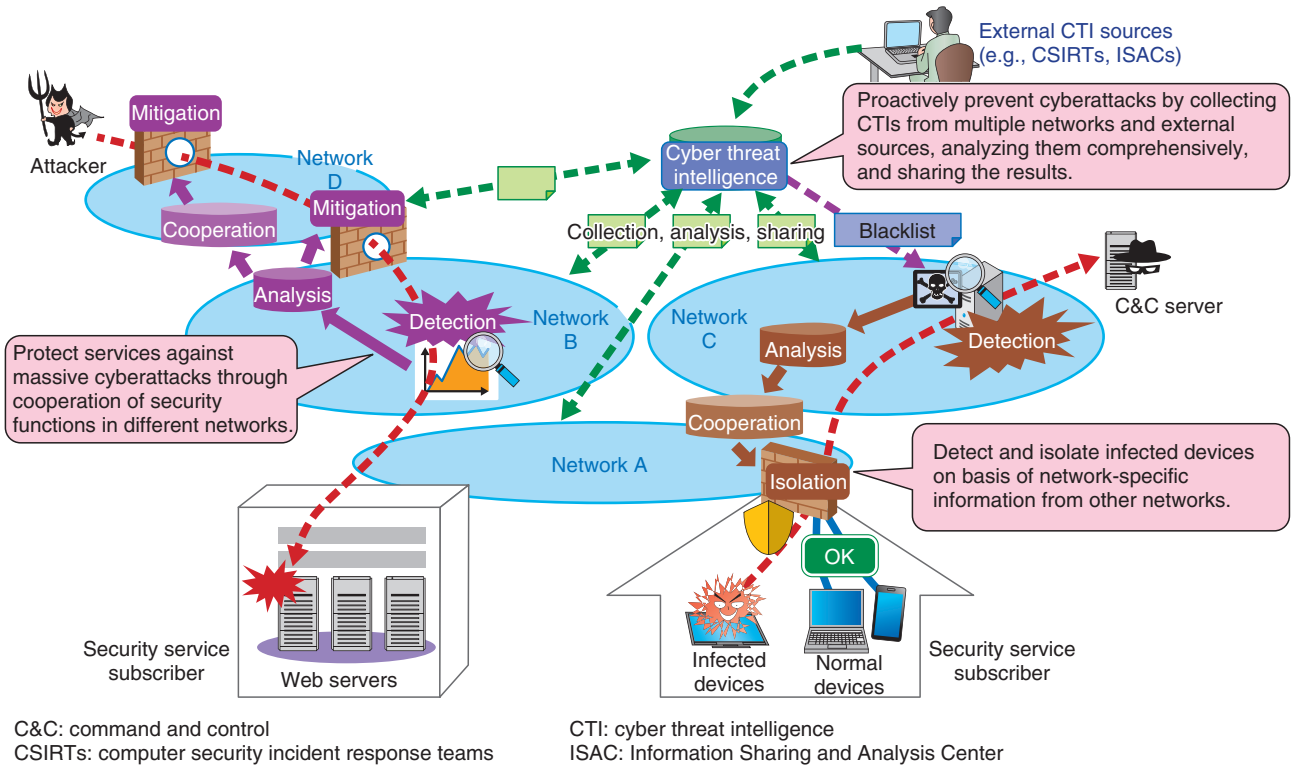
gRPC: An open source remote procedure call (RPC) system.
NETCONF: Network Configuration Protocol
PCE: Path Computation Element
REST: Representational State Transfer
SBI: southbound interface
YANG: Yet Another Next Generation

Fig. 5. Elements of multi-layer SDN control technology.



QoE: quality of experience
UC/MC: unicast/multicast

Fig. 6. CDN technology.



C&C: command and control
CSIRTs: computer security incident response teams
CTI: cyber threat intelligence
ISAC: Information Sharing and Analysis Center

Fig. 7. Cooperative mechanisms for protecting systems against massive cyberattacks.

video and also increases the utilization efficiency of distributor servers and other facilities, while still achieving stable distribution.

5.3 State visualization technology

State visualization technology is designed to estimate and visualize metrics such as distribution conditions, QoE, and viewing behavior (playback, pause, seek, termination of video) from information measured and accumulated from devices, applications, and terminals on the network, and to provide this information to content distributors. This enables content distributors to understand the characteristics of content viewing by viewers, helping them to improve efficiency.

We hope to implement a high-performance, economical CDN platform using these technologies, carrier network platforms, and the accompanying management information.

6. Cooperative mechanisms for protecting against massive cyberattacks

With recent increases in the scale of DDoS attacks and diversification in the types of malware, it is becoming difficult for individual networks to deal with such attacks efficiently in terms of performance and functionality. To overcome this, it is important to strengthen detection and protection functions by obtaining and sharing security threat information among network operators as preventative attack countermeasures and to link the security functions among multiple networks. Therefore, efforts are underway to realize advanced preventative defense capabilities, increased capacity of DDoS attack defenses, and advanced detection and prevention mechanisms for malware infection (**Fig. 7**).

6.1 Advanced proactive defense

For advanced proactive defense, we are studying mechanisms that generate and share network-aided cyber threat intelligence (CTI) faster and more accurately through comprehensive analysis of network flows and other network-specific information between multiple networks as well as collecting CTI from external sources. These mechanisms will contribute to advancing proactive defense techniques such as expanding domain name system (DNS)

blacklist information.

6.2 Increased capacity of DDoS attack defenses

To increase the capacity of DDoS attack defenses, we are studying a mechanism to distribute DDoS attack traffic to the defense functions of networks on the attack route while considering the defense capacity of each network. This is expected to achieve appropriate cooperation of defense functions.

This mechanism has enabled us to defend against attacks of dramatically higher bandwidth than single-network countermeasures.

6.3 Advanced detection and prevention mechanisms for malware infection

To achieve more advanced malware infection detection and prevention mechanisms, infected devices must be rapidly and accurately detected and isolated to prevent information leaks and other consequences. However, it is difficult to isolate only the infected devices on each network when the DNS server that can detect the typical behavior of malware (i.e., a C&C (command and control) server) and the devices are on different networks. Therefore, we are studying a mechanism to link the detection information in the DNS server and the device information, in order to quickly and accurately isolate the infected devices.

This initiative aims to achieve a mechanism to detect and protect against cyberattacks by linking functions and information of multiple networks. In the future, we plan to evaluate the technology on commercial networks, identify issues toward practical implementation, and promote system implementation.

7. Future prospects

We have described the results of studying future network technologies, including network slicing, cloud-native SDx, multi-layer SDN control, CDN, and inter-network cooperative mechanisms for protecting systems against the expanding and diversifying cyberattacks. We will continue to demonstrate technologies with proof of concept systems, move elemental technologies toward completeness, and refine the overall architectures.

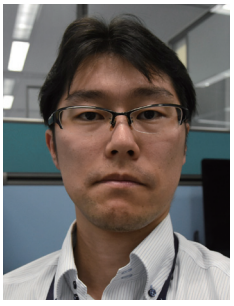
Reference

[1] T. Tojo, T. Matsukawa. S. Okada, S. Arai, and S. Yasukawa, “Multi-level Reliability Architecture for Network Slicing in Metro Networks,” Proc. of the 23rd IEEE International Symoposium on Local and Metropolitan Area Networks (IEEE LANMAN 2017), Osaka, Japan, June 2017.

Seisho Yasukawa
Group Leader, Senior Research Engineer, NTT Network Technology Laboratories.
He received a B.E. and M.E. in applied physics from the University of Tokyo in 1993 and 1995. Since joining NTT in 1995, he has conducted R&D of asynchronous transfer mode (ATM) based multimedia switching and NGN (Next Generation Network) architecture. He has also been engaged in standardization activities related to P2MP (Point-to-Multipoint)-MPLS. His current research involves 5G transport technology.

Hiroaki Sato
Senior Research Engineer, NTT Network Service Systems Laboratories.
He joined NTT in 1992 after receiving a master's degree from Tokyo Institute of Technology. He developed asynchronous transfer mode passive optical network (ATM-PON) systems, IP multicast CDN systems, and IPv6 backbone systems for Internet access. He specified the video streaming guideline on LTE (Long Term Evolution) for content providers and developed SDN-LAN to connect network functions virtualization systems including vEPC (virtual evolved packet core) in NTT DOCOMO. Since returning to NTT, he has been investigating vCPE (virtual customer premises equipment) using open source software and 5G transport with network slicing.

Takeshi Hirota
Senior Research Engineer, Network Architecture Innovation Project, NTT Network Technology Laboratories.
He has worked on the development of a network management system for synchronous digital hierarchy, ATM, and packet transport technology. He is currently researching automatic unified control from networks to cloud environments. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).



Takuya Tojo
Senior Research Engineer, Network Architecture Innovation Project, NTT Network Technology Laboratories.
He received a B.E. and M.S. in computers and systems engineering in 2002 and 2004, and a Ph.D. in advanced science and technology in 2007 from Tokyo Denki University. He joined NTT Service Integration Laboratories in 2004. From 2012 to 2014, he was with NTT DOCOMO. He is a member of IEICE.

Ken-ichi Endo
Senior Research Engineer, Network Architecture Innovation Project, NTT Network Technology Laboratories.
He received a B.E. and M.S. in electronic engineering in 1984 and 1986. He joined NTT LSI Laboratories in 1986. He has been with NTT Network Technology Laboratories since 2012, where he is studying distribution of next-generation video content.

Yasunobu Kasahara
Senior Research Engineer, Access Network Service Innovation Group, Access Network Service Systems Project, NTT Access Network Service Systems Laboratories.
He received a B.E. and M.E. in electronic engineering from Nihon University, Chiba, in 1996 and 1998. He joined NTT in 1998 and worked on the development of optical access systems such as ATM systems, passive optical networks, and layer 2 switches. He is currently engaged in R&D of content distribution technologies for emerging services. He is a member of IEICE.

Hiroshi Suzuki
Researcher, Transport Service Systems Development Project, NTT Network Service Systems Laboratories.
He received a B.E. and M.E. from Shizuoka University in 2008 and 2011. He joined the NTT Group in 2011. His recent research involves cooperative mechanisms for protecting against massive cyberattacks.