Virtualization and Softwarization Technologies for End-to-end Networking

● Naoki Oguchi ● Toru Katagiri ● Kazuki Matsui ● Xi Wang
● Motoyoshi Sekiya

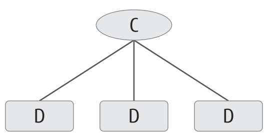
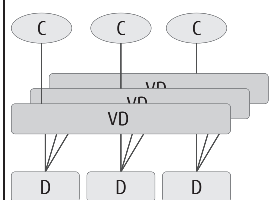
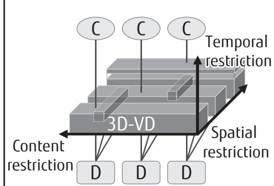
The emergence of 5th generation mobile networks (5G) and Internet of Things (IoT) technologies, as well as the continuous evolution of cloud services, is creating an increasing need for easy and on-demand creation of network slices, which are logically isolated (closed) network spaces spanning user devices and the cloud, tailored for individual businesses and services. While creating network slices within a single network infrastructure using software-defined networking (SDN) is possible, creating an *end-to-end* network slice across multiple network infrastructures remains a challenging task. Skilled network engineers must configure each infrastructure using different protocols and procedures and configure an array of virtual private networks (VPNs) for interconnecting them. In this paper, we explain the issues associated with the creation, operation, and management of end-to-end network slices and our approach to addressing them by using virtualization and softwarization. Specifically, we present the *One Network* Architecture, which virtualizes multiple network infrastructures as one infrastructure and facilitates the creation of network slices on top of it. We also discuss several of the latest research topics such as information centric networking technology deployed over such network slices.

1. Introduction

A network is typically configured by interconnecting physical devices such as routers and switches. These devices have their own data plane and control plane, and are operated autonomously and managed under distributed control [**Table 1 (a)**]. Such a configuration can be advantageous because of its tolerance against partial failures owing to the autonomous control of data transfer by network elements. However, intelligent routing decision and comprehensive management based on knowledge of the entire network are difficult. Moreover, when a network configuration needs to be changed, cable connection/disconnection and reconfiguration of individual devices are necessary.

As cloud technology advances, data center servers and storage have become more virtualized, which

Table 1
History of control technologies.

	(a) Previously	(b) SDN era	(c) Cloud era	(d) Future
Architecture				
Control method	Autonomous distributed	Single point centralized	Centralized individually	Centralized individually
Bandwidth and performance assurance	Link bandwidth assurance	N/A	Link bandwidth and performance assurance	Link bandwidth and performance assurance

C: Control plane D: Data plane VD: Virtual data plane in turn leads to stronger demand for network virtualization and softwarization. Today, the emergence of software defined networking (SDN) has made it possible to separate functions between the data plane and the control plane so that data plane operations can be performed through a single controller instead of configuring multiple devices individually. This enables users to define, control, and establish a virtual network by using software [**Table 1(b)**]. In addition, the use of network functions virtualization (NFV) technology enables more advanced softwarization of network functions.

In recent years, the advent of new technologies such as the Internet of Things (IoT) and 5th generation mobile networks (5G) has created the need for storing large amounts of data generated by IoT devices for use in various fields such as big data analysis. In the cloud computing era, it is assumed that networks can be used securely and efficiently by creating virtually separate *end-to-end* closed spaces (hereafter, network slices) from the device at a user location to the cloud, depending on the type of business or service (**Figure 1**).

To cope with these rapidly changing service demands, these network slices need to be flexible so that they can be readily built and modified on-demand without much human intervention. Also, for stable service provision, these network slices must be able to guarantee their link bandwidth and network processing performance. We propose a virtual data plane architecture that virtualizes different data planes in order to meet these requirements[6] [**Table 1(c)**].

There are spatial restrictions, which specify end points such as terminal devices and IoT devices, in the virtual data plane. We believe that there are also temporal and content restrictions. For temporal restrictions, virtual data planes may be created for the time specified. Content restrictions include the requirement that virtual data planes may be created on the basis of the content of the data. In the future, a 3D virtual data plane that satisfies all these demands will be required [**Table 1(d)**].

In this paper, we introduce a virtual data plane technology that enables quick, easy, and secure connections on-demand from a cloud to a user location. We also describe our latest studies on future control technologies, including information centric networking technology based on information propagated in the virtual data plane.

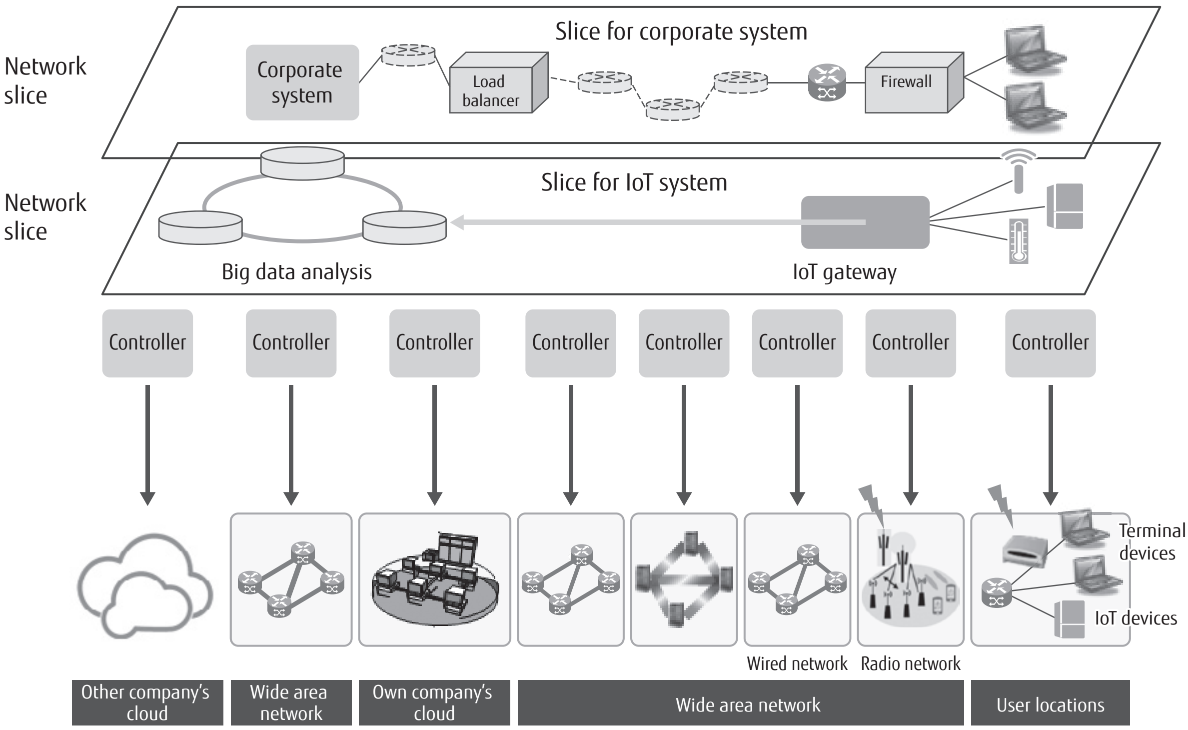


Figure 1
End-to-end network slices.

2. Challenges of building end-to-end network slices

2.1 Integrated management and creation of network slices across heterogeneous network infrastructures

A virtual network is considered an option for on-demand establishment of a network slice.[2)] A virtual network is a network composed of softwarized switches and routers within virtualization software used in server virtualization technologies or physical devices that can work under the SDN. A virtual network that realizes the required network can be built using SDN technology, as shown in **Figure 2**.

However, when establishing an end-to-end network across network infrastructures operated by different corporations with different management policies, it is necessary to know the settings that are unique to each network infrastructure (**Figure 3**). Moreover, users must be made aware of the existence of virtual networks, such as a virtual private network (VPN) and/or virtual extensible local area network (VXLAN)[3)] used to connect network infrastructure, which can make it

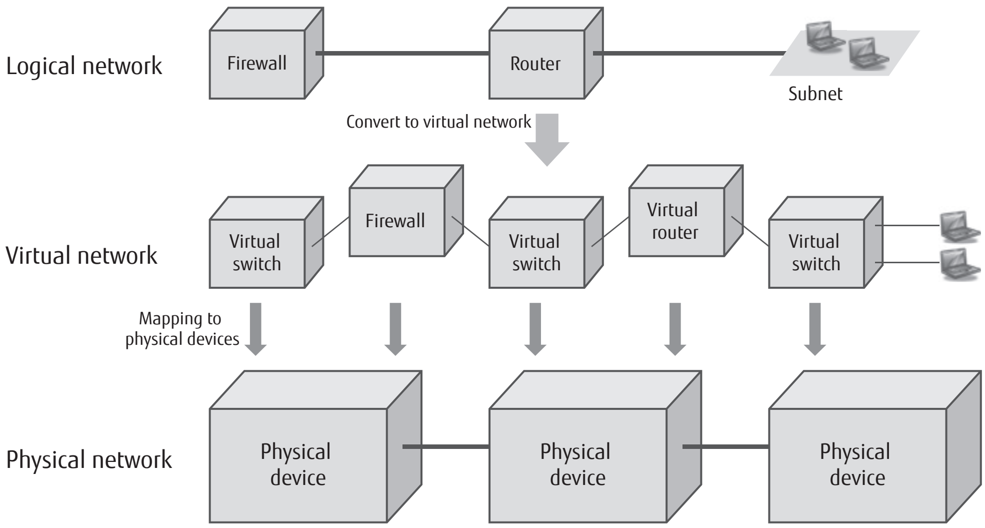


Figure 2
Mapping of logical network to physical network using SDN.

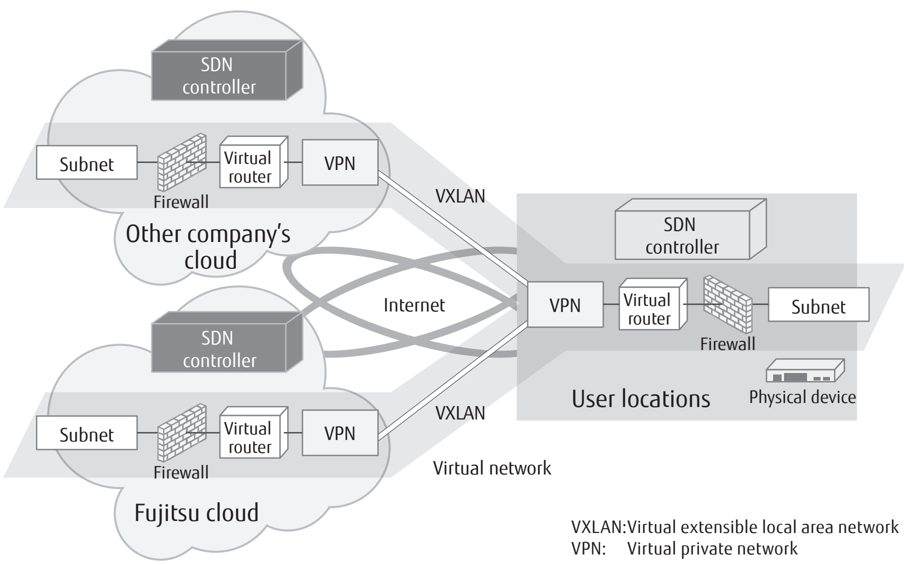


Figure 3
Challenges when building a network across different network infrastructures.

difficult for a person without network expertise to design a network.

2.2 Show universal resource as invariable resource

The network slices required in IoT or 5G sometimes need stable resource such as link bandwidth and network processing performance. Equipped with virtual network functions realized with software on universal resource, end-to-end virtual networks tend to be vulnerable to the effects of other traffic or physical device failures. It is therefore necessary to have a mechanism making such performance vulnerability barely visible to users and to have the services work stably.

2.3 Automatic creation and modification of network slices

The network slices required in IoT or 5G need to be created or deleted in accordance with explicit requests by users or service applications. In the future, network slices are expected to be automatically created over multiple network infrastructures by inferring user intentions without their explicit requests. This means that cloud services will be more efficiently used through organic connections with the services they provide. A mechanism that can manage dynamic changes in the number of terminal devices and IoT devices joining the network slice is also needed.

3. One Network Architecture

We propose the One Network Architecture, which enables network slices spanning heterogeneous network infrastructures to be handled by a single application programming interface (API) and address the aforementioned challenges.

As shown in **Figure 4**, the One Network Architecture makes several network infrastructures look like a single virtual network infrastructure and controls

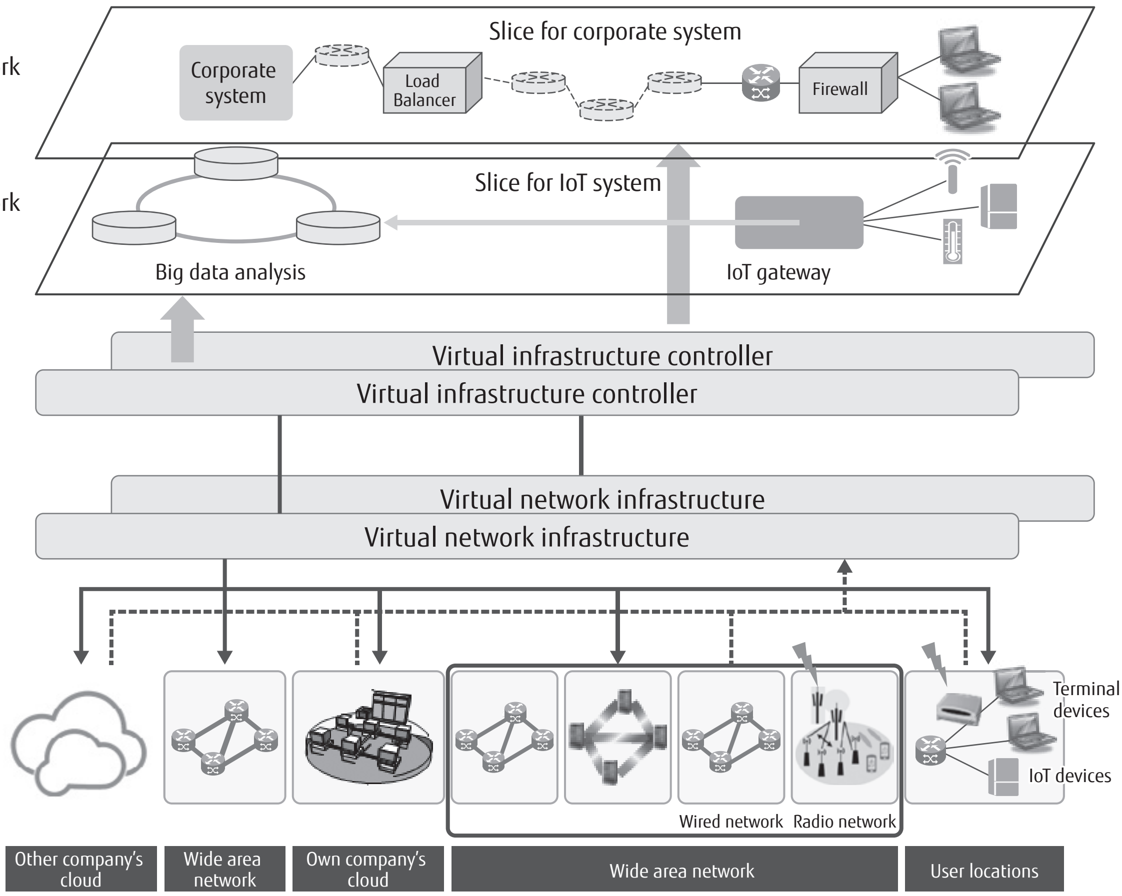


Figure 4
One Network Architecture.

it with a single virtual infrastructure controller. The single API enables the user or an application to create a network slice across several network infrastructures by accessing only the virtual infrastructure controller. This enables the dynamic and automatic configuration of a network slice tailored for the business or service, making the use of services secure and stable.

The following are some applications of the One Network Architecture.

3.1 Usage

1) New offices and shops

When opening a new office or shop, the user can immediately access the business application needed at the site by connecting to the cloud. Security is ensured by assigning a network slice appropriate for the terminal used and user type (**Figure 5**).

2) Factory line sharing

This architecture enables a fabless factory without its own manufacturing facility to use an available shared factory line while configuring the necessary network slices, providing a secure network slice that prevents data from leaking to other factory lines.

3.2 Technologies to realize One Network Architecture

We are developing technologies to configure the virtual network infrastructure needed to implement the One Network Architecture. They include technologies for abstracting the network infrastructure and associated technologies for automatic supplementation, optimum mapping, auto-scaling, and automatic recovery. We are also developing technology for the automatic creation of network slices as a function of a virtual infrastructure controller, wherein a network slice is automatically created depending on the user or service provided by the application. These technologies are described below.

1) Infrastructure abstraction technology

We have developed a technology to create a virtual network infrastructure by using a software object (hereafter, virtual network object) and mapping multiple network infrastructures to it. The virtual network object shows the entire virtual network infrastructure that a user can use, and each network infrastructure is expressed as a sub-object contained in the virtual network object. The virtual network object is equipped with methods that respond to directions from the controller and events occurring in each infrastructure, in order to realize autonomous operation from these events.

As shown in **Figure 6**, this enables the user to design a logical network over the virtual network object and easily build an end-to-end virtual network and manage it without being concerned about other connections, such as VPNs across the network

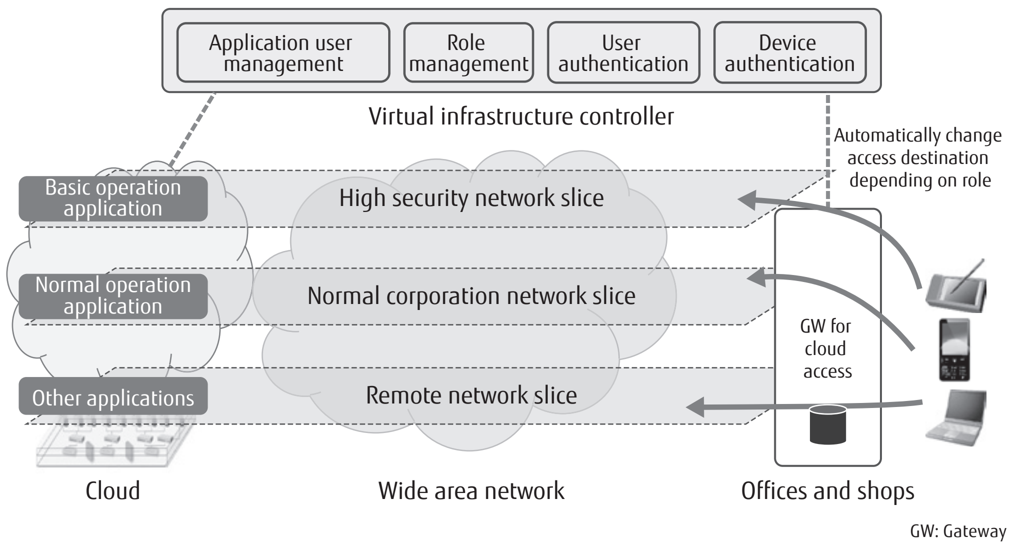


Figure 5
Usage case: new office or shop.

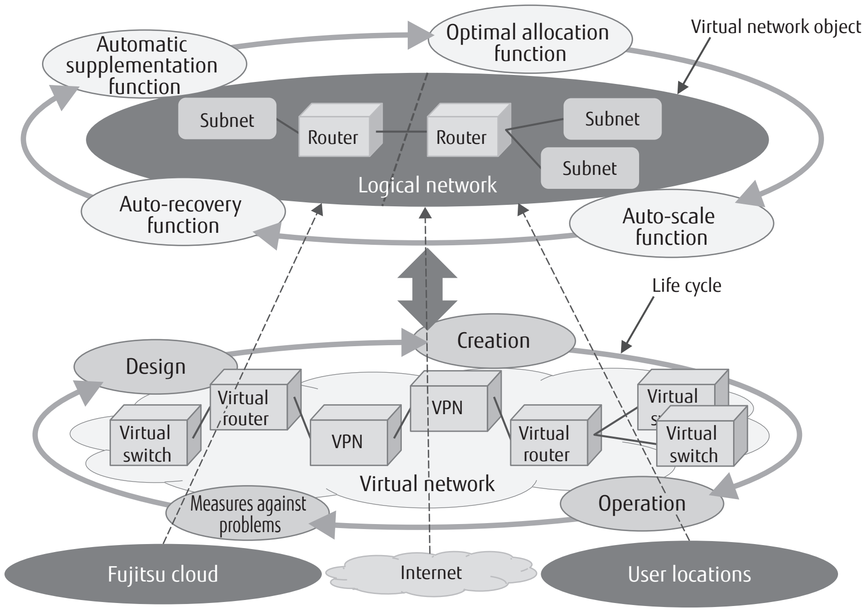


Figure 6
Infrastructure abstraction technology.

infrastructure. Moreover, the life cycle management of the end-to-end virtual network (design, configuration, operation, monitoring, maintenance, and disposal) can be treated as one for the logical network.

We proposed the concept of the virtual network object as a technology to manage optical networks.[4),5)] The application of this technology to the end-to-end virtual network management architecture resulted in a practical management system.[6),7)]

2) Automatic supplementation technology

To make user logical network design easier, we developed a technology to automatically supplement the functions required to build a virtual network by extracting the designer's intentions on the basis of the connection conditions between elements in the network.

Checking the connections between elements at different levels, e.g., network infrastructures, subnets, and nodes located at both ends of the links, by looking at the links between the elements of the logical network designed by a user, as shown in **Figure 7**, the technology can predict the designer's intentions so that the desired functions of the virtual network are automatically supplemented.

3) Optimum mapping technology

This technology can map virtual network functions to an end-to-end physical network consisting of multiple network infrastructures, such as multi-clouds, so that billing and performance are optimized.

4) Auto-scale and auto-recovery technology

With some of the functions realized with software, a virtual network can become vulnerable to the effects of other traffic or physical device failures, which makes the assurance of bandwidth and/or performance difficult. If a virtual network object collects information on resources, communication quality, or failures and then decides which ones may be affected, the technology helps the service work in a stable manner by automatically increasing the number of virtual network functions and/or avoiding disturbances to minimize their impact on users without requiring the user's explicit countermeasures.

5) Technology for network slice automatic configuration

We developed a technology that can automatically create a network slice by inferring the user's intentions so that the services provided by the cloud can be automatically utilized. The technology has the following functions.

- Allocates gateways for cloud access to enable collecting information on the properties and behaviors of devices, users, and applications at

user locations, etc. in order to gather information required for automatic creation of network slices depending on usage (**Figure 8**).
- Automatically analyzes and decides on requirements for the security and responsiveness of network slices depending on environmental changes involving devices, users, or applications.

We aim to improve the adaptability to environmental changes and user experience quality by achieving a more sophisticated way of network slice creation using artificial intelligence.

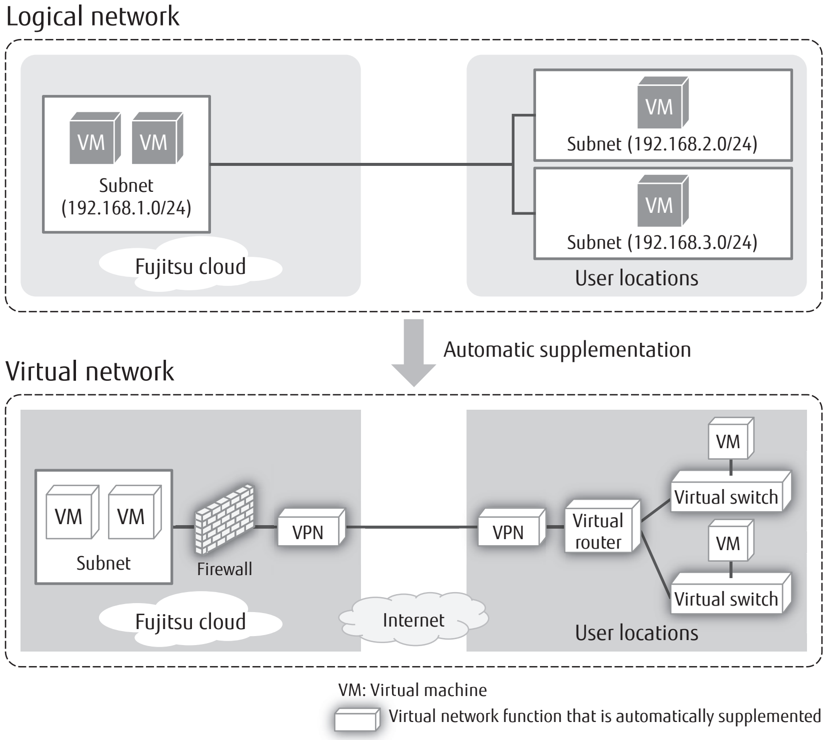


Figure 7
Automatic supplementation technology.

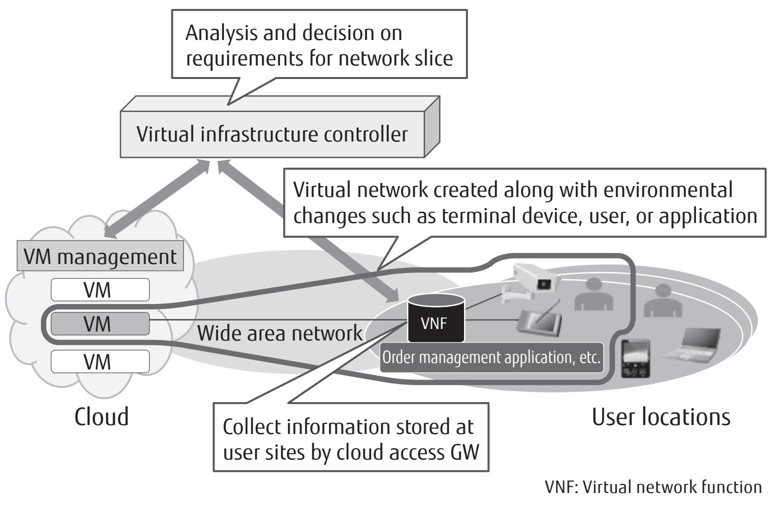


Figure 8
Technology for automatic establishment of network slice.

4. Future challenges and prospects

We have defined the One Network Architecture as a means to configure a spatial network slice depending on the location of the device or service. In the future, a mechanism wherein secure data can be easily shared between network slices owned by different companies, depending on details of the data or content, will be required. This section discusses how the future network will be formed and our efforts to address the challenges.

Recently, there is an increasing number of new services created by orchestrating various cloud services developed by different companies and connecting them through representational state transfer (REST) API. There are also demands to keep systems on each company's premises instead of deploying data in the cloud owing to concerns over security and poor performance. Such cases require a system promoting the development and provision of new services through collaborations between services in the cloud, as well as systems owned by different companies.

In line with our efforts to realize this, we have been promoting R&D for a network technology called Virtual Private Digital Exchange (VPX),[8] a safe, secure, and easy way to share information located at different points in a wide area network, such as a cloud or a company system, as **Figure 9** shows. This technology creates a secure network slice that allows access to only certain types of data among multiple network slices that belong in a cloud, wide area network, and several corporate offices. This enables secure and easy information sharing between participating users and services.

VPX uses both blockchain and distributed web technologies to create a secure network corresponding to the data to be shared, as shown in **Figure 10**. The blockchain has the features of robust verification of transactions and ledger sharing. VPX takes advantages of them as functions of the network gateway responsible for data access. More specifically, these functions are for security management that allows sharing of approved data only with reliable users; identifying data and resolving addresses so that data requested by a user can be easily found and connected; and authentication and authorization when accessing data as well as trace management for traceability. Peer-to-peer connections are achieved by automatically configuring web interfaces for each set of data in a specific network slice in accordance with the data access request and opening address. Data are then encrypted prior to transmission for secure data sharing.

5. Conclusion

The emergence of new technologies such as IoT, 5G, and advanced cloud services has increased the need for easy and on-demand creation of network slices located across heterogeneous network infrastructures by users and/or applications providing services.

In this paper, we discussed the One Network Architecture in which such end-to-end network slices

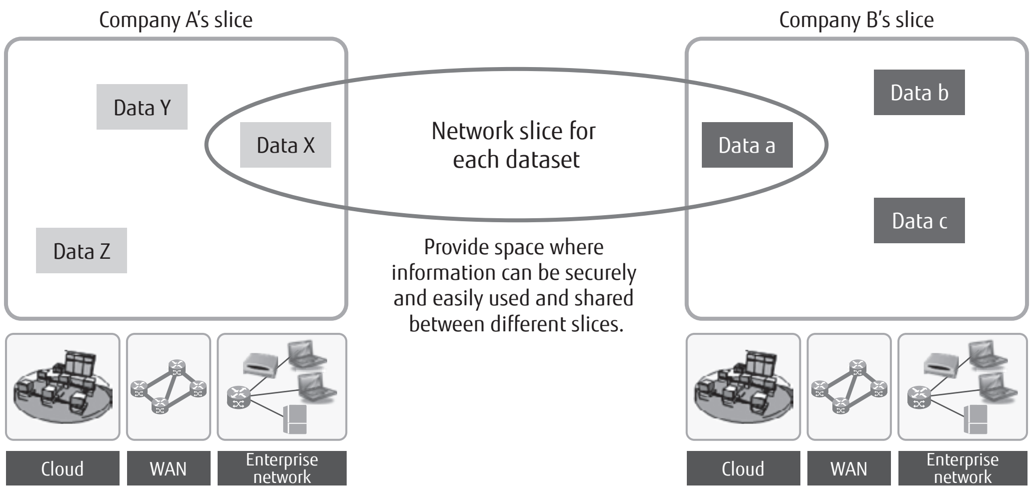


Figure 9
Conceptual drawing for VPX.

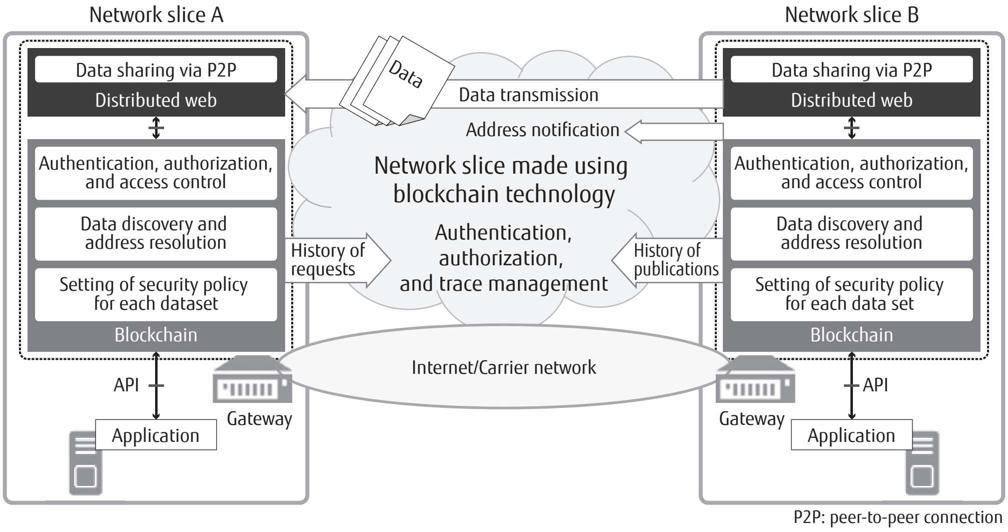


Figure 10
Configuration of VPX technology.

can be configured from one portal and the technologies to implement it. We believe that there will be a demand for an easy and secure information sharing system depending on the details of the data or content, anticipating situations in which there are more frequent exchanges and usages of the data generated through IoT or between different companies. We introduced the technologies we have been developing for such a system. Although these technologies are still under development and there are still a number of challenges to overcome, we will continue to promote research to create new services via networks.

References

1) 5G PPP Architecture Working Group: View on 5G Architecture.
https://5g-ppp.eu/white-papers/
2) B. Sayadi et al.: SDN for 5G Mobile Networks: NORMA perspective. The 10th Competition Law and Economics European Network (CLEEN) Workshop, May 2016.
3) Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks. IETF RFC7348, Aug. 2014.
4) X. Wang et al.: Object-oriented Network Virtualization – An Evolution from SDN to SPN (Invited Paper). Photonic Networks and Devices (Networks) 2014 Paper NT1C.2, as part of Advanced Photonics for Communications Congress, San Diego, California, July 2014.
5) X. Wang et al.: SPN OS: Managing network services with virtual network objects. 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), pp. 149–155, San Francisco, CA, 2015.
6) N. Oguchi et al.: Proposal of building and operating method for end-to-end virtual networks. IEICE technical report NS2016-191, Vol. 116, No. 484, pp. 193–197, Mar. 2017.
7) Fujitsu Laboratories Ltd.: Fujitsu Develops Technology to Simplify Design and Operation of Hybrid- and Multi-Cloud Network Infrastructure.
http://www.fujitsu.com/global/about/resources/news/press-releases/2017/0307-01.html
8) Fujitsu Ltd.: Fujitsu Develops Blockchain-based Software for a Secure Data Exchange Network.
http://www.fujitsu.com/global/about/resources/news/press-releases/2017/0605-01.html

Naoki Oguchi
Fujitsu Laboratories Ltd.
Mr. Oguchi is engaged in research and development for end-to-end virtual network management.

Toru Katagiri
Fujitsu Laboratories Ltd.
Mr. Katagiri is engaged in research of network management.

Kazuki Matsui
Fujitsu Laboratories Ltd.
Mr. Matsui is engaged in research and development of technology for network service infrastructure sophisticatedly connecting humans and things.

Xi Wang
Fujitsu Laboratories America, Inc.
Mr. Wang is engaged in research of network softwarization.

Motoyoshi Sekiya
Fujitsu Laboratories Ltd.
Mr. Sekiya is engaged in research and development of network systems.