# Realization of Construction and Simple Operation of Flexible Cloud System by SDN

● Yuko Aki ● Masaki Nakajima ● Yoshitaka Kizuka

**FUJITSU Software ServerView Resource Orchestrator (ROR) is a middleware product which realizes centralized management and effective utilization of information and communications technology (ICT) resources such as servers, storage and networks and ICT cost optimization by improving the operation and management efficiency. Applying this middleware makes it possible to construct a flexible cloud system according to the customer's cloud requirements and needs and to simply operate it. One technology to support this functionality is software-defined networking (SDN), which is a control technology that uses software to allow network configurations and settings to be dynamically changed in a centralized manner. ROR is a core product that realizes SDN in the datacenter domain, in particular. Fujitsu's SDN, which features close coordination between ROR and network virtualization-enabled hardware equipment, is in the practical application phase in the Numazu Software Development Cloud Center. This paper describes product features with the focus on the network functions of ROR from the viewpoint of SDN and future outlook in terms of network operation and management of a cloud system.**

## 1. Introduction

Along with the development of cloud computing, software-defined networking (SDN)[1] has been attracting attention as a technology for centralized control by software for the purpose of flexibly and dynamically changing network configurations and settings according to server virtualization. Fujitsu has rolled out new products based on the concept of SDN architecture (FUJITSU Intelligent Networking and Computing Architecture).[2] We have now realized construction of a flexible cloud system and its simple operation by using FUJITSU Software ServerView Resource Orchestrator (ROR)[3], which is a cloud infrastructure management middleware, as the core and through integration with network virtualization-enabled hardware equipment (the CFX converged fabric switch[4] and the IPCOM VX series virtual appliances[5]). Fujitsu's SDN in the data center domain is in the practical application phase as shown by the utilization at Numazu Software Development Cloud Center[6] used by a few thousand developers as Fujitsu's software development environment.

ROR realizes effective utilization of information and communications technology (ICT) resources including servers, storage and networks together with improvement of operation efficiency and provides an optimum cloud system according to the requirements and needs of the cloud constructed by the customer.

From the perspective of SDN, this paper focuses on the network functions of ROR and provides a description in the following order:

- Fujitsu's approach to SDN as the background
- Characteristic of ROR: automatic deployment of a system and network virtual appliance
- Orientation of open system provision and standardization
- New issues with network operation and management in a cloud system and Fujitsu's proprietary value-added functions that provide the solution

## 2. Fujitsu's approach to SDN

In the process of ICT evolution, servers have undergone a transformation from physical consolidation to virtual consolidation, which has generated frequent additions and changes to a server environment. This transformation to a server environment has a significant impact on network operation and management for reasons including the need for setting and changing the individual network devices. For example, changing a server connection destination involves changing the setting of the virtual LAN (VLAN) and access control list (ACL) of network devices across multiple devices. In a multi-tenant system, it may be required to separate a VLAN for the individual virtual servers and add various network devices for the individual tenants in line with the addition of servers. As shown by these examples, the time and cost required for network operation and management continue to increase.

As server virtualization progresses and evolves, networks are becoming more and more complex and cumbersome. Therefore, the demand for simplifying network operation and management is increasing. As a solution to this issue, SDN and network virtualization have come to raise great expectations.

Accordingly, Fujitsu announced "FUJITSU Intelligent Networking and Computing Architecture," a new architecture that optimizes an entire ICT platform on a network-wide basis, in May 2013[7] as a concept of SDN. Then, provision of data center products was started as the first round of products based on this architecture, which include ROR for centralized management of an entire ICT system using the SDN and virtualization technologies and network devices that support network virtualization and SDN.

Fujitsu's SDN frees administrators from troublesome management operations by allowing them to use software to realize "configuration management" and "settings automation" in multi-hypervisor and multi-vendor network environments. In addition, virtualization-enabled network devices make it possible to reduce the number of installations and save energy and space. Powerful cloud infrastructure is provided by having an integration between software and hardware to reduce the time and cost required for network operation and management and allow for effective utilization and optimization of ICT resources.

## 3. Automatic deployment of system

This section presents the automatic system deployment function, a characteristic of ROR. ROR is capable of conducting centralized management of hardware including networks in addition to servers and storage as virtual resources and providing a system simply and quickly in response to users' requests. For example, it can automatically deploy a system with a patterned configuration (logical platform) as shown in **Figure 1** in a collective manner.

If an infrastructure administrator uses ROR to prepare combinations of standard resources (hardware and OS) as templates, a system can be collectively and automatically deployed according to those templates. Templates can include network devices such as firewalls and server load balancers, which is a major feature. When a system is collectively and automatically deployed, parameters required for starting the OS and networks are set automatically and the infrastructure can be promptly provided without any omission of manual settings or definition errors. Furthermore, tenant user-specific network device rule settings (firewall and server load balancer settings), which are required after automatic deployment, can be automatically conducted simply by inputting parameters on the graphical user interface (GUI) screen.

To realize the automatic system deployment function, it was necessary to be able to simply design sets of servers, firewalls, server load balancers and VLANs that constitute customers' business systems (units of deployment) and automatically configure settings of these networks in a collective manner along with server automatic deployment. It was also necessary to be able to deal with multi-vendor and existing network devices using the same scheme. In order to meet these requirements, we implemented automatic network settings with the following configuration and interfaces (**Figure 2**).

- Orchestrator (entire system control and management)

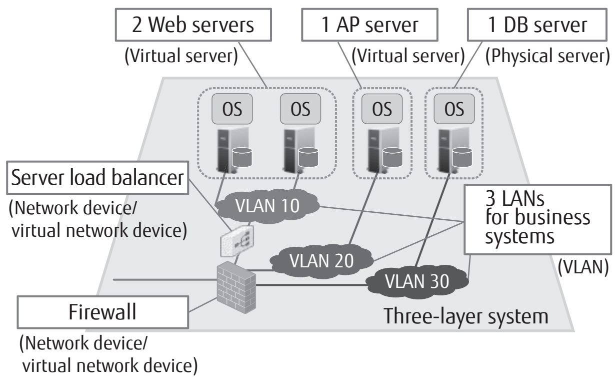


**Figure 1**
**Example of logical platform.**

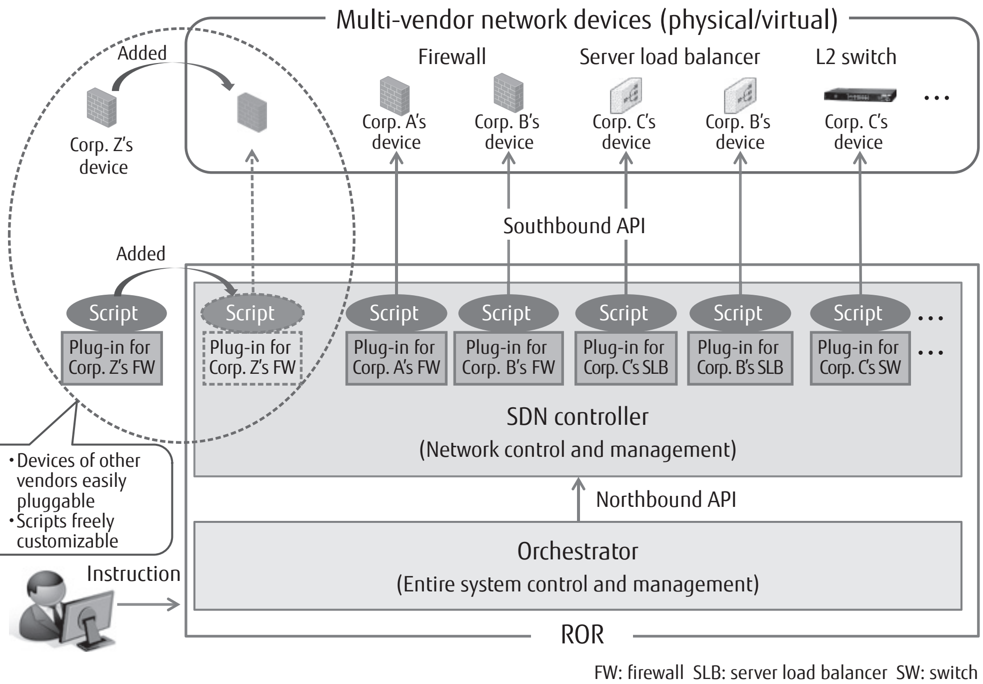


**Figure 2**
**Implementation of automatic network setting.**

- SDN controller (network control and management)
- Physical and virtual multi-vendor network devices (firewalls, server load balancers and Layer 2 switches)
- Northbound API (interface between Orchestrator and SDN controller)
- Southbound API (interface between SDN controller and respective device)

For centralized management of multi-vendor network devices and prompt incorporation of targets of automatic deployment, we carried out the following.

1) We provided on the SDN controller southbound APIs, or scripts that support control commands of the respective network devices, in a pluggable manner so that it is easy to add new devices or devices of other vendors.
2) We provided standard "sample scripts" that support typical setting/operation patterns for network devices to be managed, and this makes it possible to promptly incorporate network devices as targets of automatic deployment of a system.
3) We also offered script customization according to customers' environments and individual customization services to meet the demands for script writing to support devices of other vendors not covered by the standard support.

## 4. Provision of network virtual appliance

The approach as described in the previous section made it possible to incorporate network devices as targets of automatic deployment of a system, which has provided a scheme of automating setting and changing operation of network devices. However, the issue of costs involved in adding and setting network devices, accompanying an addition and change of servers, still remained.

In particular, to start a small cloud infrastructure environment for gradual enhancement, it is necessary to not only simply add servers but also to change network configurations and add devices. This caused problems such as the need to redesign networks and different timings of delivery of additional devices, and as a result timely environment construction was hindered.

Accordingly, we then worked on providing a network virtual appliance that runs on a server, which has been provided as "NS Option," an optional product of ROR. The appliance has a virtual machine (VM) concept with network service functions (firewall/server load balancer) implemented on a dedicated OS, and this allows multiple appliances to be deployed on the physical server managed by ROR. By incorporating them as targets of automatic deployment of a system of ROR, firewalls and server load balancers required for business systems can be dynamically and flexible deployed as required.

Network virtual appliances have several benefits as compared with dedicated network devices (physical equipment):

- Inexpensive
- Can be introduced in a short time
- No purchase of additional physical network devices (firewalls/server load balancers) is required for addition of servers
- Installation space or cabling not required

The network virtual appliance offered as NS Option is an engine in common with FUJITSU Cloud IaaS Trusted Public S5[8], a set of network services currently offered in six sites around the world, and has a sufficient track record. We intend to enhance its network service functions including the VPN services.

## 5. Enhancement of SDN controller and provision of open system

In terms of network setting and change from the SDN controller in ROR, the cloud network environment to be automated is estimated to become increasingly multi-vendor for both virtual and physical networks due to the increasing requirements that cloud systems are expected to meet:

- Connection and integration with public cloud
- Integration with SDN connection technologies of various companies
- Support for industry standard network service functions

In order to promptly meet these requirements, it is necessary to incorporate plug-ins for other companies' network devices that support standard APIs by using OSS (OpenStack[9] Neutron, OpenDaylight[10]) integration and support overlays such as VXLAN, NVGRE and STT, which are the latest network virtualization technologies.

For that purpose, we first plan to support various network resources by incorporating Neutron, which is part of ROR's OpenStack support[11] and a network core function, and provide integration with Midokura's network virtualization solution Midokura Enterprise MidoNet.[12]

In the future, we intend to further enhance the SDN controller to enable ROR to control other companies' devices that are supported by OpenStack Neutron. For example, we will aim to provide an open ecosystem by OpenStack Neutron integration through vendor collaboration including Cicso's SDN controller (Extensible Network Controller (XNC))[13] and VMware's network virtualization product (NSX).[14] This will enable us to offer various choices to our customers.

## 6. Issues with network operation and management

As explained earlier, automatic deployment by ROR and provision of network virtual appliances have made it possible to simplify operations related with the construction and addition (configuration change) of cloud systems. This section describes issues with network operation and management in a cloud system.

### 6.1 Division of roles between tenant administrators and infrastructure administrators

In a cloud system, networks are generally managed by tenant administrators and the infrastructure administrators. The tenant environment relating to services for users including firewalls and server load balancers (such as network virtual appliances) is owned or managed by tenant administrators. Meanwhile, the infrastructure environment including network devices (physical equipment) and virtual switches is owned or managed by infrastructure administrators. There would be no problem if their respective scopes of management were completely independent but, in reality, their troubles mutually affect each other. For that reason, they often work in cooperation to solve them. In many cases, troubles of either side oblige the other to cooperate in investigations or other activities.

### 6.2 Physical and virtual networks

1) Understanding of relationships (association)

In a cloud system, virtual networks can be freely constructed for the respective tenants on the same physical network. This makes it difficult to collate configuration information of physical and virtual networks and understand the relationships between them. In particular, grasping the current states of virtual networks, which can be freely changed, by manual labor is hardly possible.

2) Understanding extent of network troubles' impact

It is difficult to quickly gain information about the extent of impact of network device failures or other problems with physical networks: which virtual networks are affected and how the problems spread to networked servers/VMs and storage. For this reason, it is impossible to immediately contact and check with users affected by the troubles.

## 7. Realization of self-service of network management

We have taken the following approaches to solve the issues mentioned in the previous section.

### 7.1 Self-service of network management

In the operation life cycle of a cloud system, operations of tenant administrators and infrastructure administrators should preferably be as described below.

1) The two can complete their own operations easily within their own scopes of responsibility.
2) When the two work in cooperation, it does not involve unnecessary exchange of ideas and opinions, and the respective operations can be carried out smoothly without mistake.

The concept of "self-service of network management" is to provide functions for satisfying the requirements above.

To that end, we have worked with frontline systems engineers (SEs) to identify solutions by setting up hypotheses of issues during operations and specifying use cases. In addition, we have used an evaluation prototype starting in the planning phase and established a technique of agile development to allow SEs to conduct evaluations and to reflect the results in a short time.

### 7.2 New NetworkViewer

NetworkViewer is an integrated management screen that can visualize a network made up of physical/virtual servers and network devices in a map format or table format. In particular, in order to help users understand the relationships between physical and virtual networks and the extent of impact of network troubles, we have developed the new NetworkViewer based on the concept of "self-service of network management." As shown in **Figure 3**, it features views provided respectively for physical and virtual networks, which allow them to be managed from the viewpoint of the user's desired layer (physical/virtual) and makes it easy to identify mutual relationships.

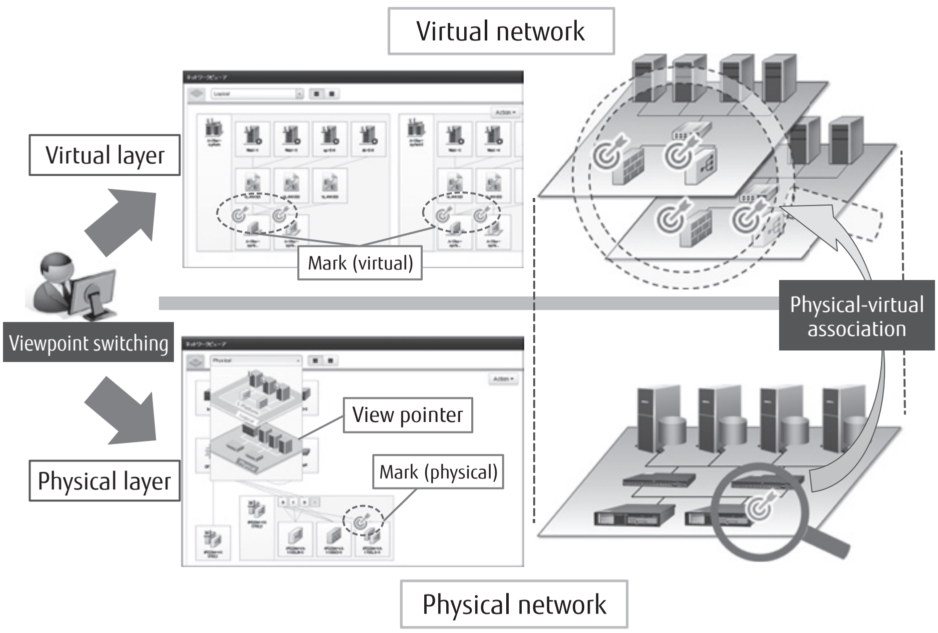


**Figure 3**
**Features of new NetworkViewer.**

1) User's viewpoint switching (view pointer)

The viewpoint can be switched between the physical and virtual layers as desired according to the user's role.

2) Association between physical and virtual networks (marking)

Marking the icon for a resource (server or network device/virtual appliance) on the screen for one layer causes the associated resource on the other layer to be marked, allowing the relationship between them to be understood. For example, in Figure 3, when the icon for one unit of IPCOM VX (virtual appliance with two functions: firewall and server load balancer) is marked on the physical network and the viewpoint is switched to the virtual layer, the two systems (tenants) that use the marked IPCOM VX (physical equipment) are shown. Furthermore, the icons for firewalls and server load balancers used in the systems are also marked. In this way, the respective relationships can be easily identified.

3) Visualization of extent of impact in physical and virtual networks

Connectivity (configuration information) of server and network device can be identified. This feature, when combined with the association between the physical and virtual networks as described above, helps users to understand how a failure generated in one layer affects the other layer and also which of the connected servers or VMs is affected. This makes it possible to immediately contact and check with users affected by any trouble generated.

As with the automatic deployment of a system, the new NetworkViewer supports multi-vendor and multi-hypervisor environments. In the future, we intend to strengthen network self-service and visualization also including OpenStack to enhance the system and simplify and speed up on-site network operations and troubleshooting based on the concept of network-integrated operations and management platform.

## 8. Conclusion

The network functions of ROR have been enhanced as in the close integration with hardware products in line with Fujitsu's SDN architecture, standardization and ecosystem support. This has been done by incorporating the OSS cloud network platform and strengthening features in order to differentiate the product from those of our competitors in the areas of self-service and visualization of networks. We intend to continue incorporating the latest technologies and reflecting frontline opinions for further flexibility and operability of SDN-based cloud systems.

## References


1) SDN: Software-Defined Networking (SDN) Definition. *https://www.opennetworking.org/sdn-resources/sdn-definition*
2) Fujitsu: Network-wide Optimization. *http://www.fujitsu.com/global/vision/2014/chapter3/02/network-wide/*
3) Fujitsu: FUJITSU Software ServerView Resource Orchestrator. *http://www.fujitsu.com/global/products/software/infrastructure-software/*
4) Fujitsu: Extension Equipment [Converged Fabric Switch] (in Japanese). *http://jp.fujitsu.com/platform/server/primergy/peripheral/expand/cf.html*
5) Fujitsu: FUJITSU Network IPCOM VX Series (in Japanese). *http://fenics.fujitsu.com/products/ipcom/products/lineup/ipcom_vx.html*
6) Fujitsu: Practical Case Example: Numazu Software Development Cloud Center (in Japanese). *http://software.fujitsu.com/jp/middleware/cloud/casestudies/numazu-cloud/?mw=cloud*
7) Fujitsu: Fujitsu Develops New Architecture for Network-Wide Optimization of ICT Platforms. *http://www.fujitsu.com/global/about/resources/news/press-releases/2013/0508-01.html*
8) Fujitsu: Fujitsu Cloud IaaS Trusted Public S5. *http://welcome.globalcloud.global.fujitsu.com/*
9) OpenStack. *http://www.openstack.org/*
10) OpenDaylight. *http://www.opendaylight.org/*
11) T. Yanagawa: OpenStack-based Next-generation Cloud Resource Management. *Fujitsu Sci. Tech. J.*, Vol. 51, No. 2, pp. 62–65 (2015). *http://www.fujitsu.com/downloads/MAG/vol51-2/paper09.pdf*
12) Midokura Enterprise MidoNet. *http://www.midokura.com/midonet-enterprise/*
13) Cisco XNC. *http://www.cisco.com/c/en/us/products/cloud-systems-management/open-sdn-controller/index.html*
14) VMware NSX. *http://www.vmware.com/products/nsx/*

**Yuko Aki**
*Fujitsu Ltd.*
Ms. Aki is currently engaged in development of cloud platform software.

**Yoshitaka Kizuka**
*Fujitsu Ltd.*
Mr. Kizuka is currently engaged in development of cloud platform software.

**Masaki Nakajima**
*Fujitsu Ltd.*
Mr. Nakajima is currently engaged in development of cloud platform software.