Development of an Automatic Managing System of Wide-area Distributed Networks with Defined Network Specification

Yoshiharu Tsuzaki and Yasuo Okabe
Kyoto University
Kyoto, Japan
tsuzakiyo@net.ist.i.kyoto-u.ac.jp
okabe@i.kyoto-u.ac.jp

Ray Atarashi
IIJ INNOVATION INSTITUTE INC.
Tokyo, Japan
ray@iij-ii.co.jp

Tatsuya Hayashi
Lepidum Co. Ltd.
Tokyo, Japan
hayashi@lepidum.co.jp

***Abstract*— Software-Defined Networking (SDN) attracts attention as a technology to control and manage IP networks, which are inherently designed to be operated autonomously and decentralized, in a centralized manner. There have been proposed some SDN protocols like OpenFlow, but they have a restriction that existing legacy network devices which do not support SDN protocols are not controllable. In this paper, we allow an administrator to manage a wide-area distributed network composed of campus networks and data-center networks in which network devices do not have SDN features, in a single unitary policy, under an assumption that the backbone network supports SDN protocols like OpenFlow. We propose a network management system which generates necessary configuration based on defined network specification and sets the configuration to devices automatically and reactively, based on our Service-Defined Networking (SvDN) concept.**

Keywords— Service-Defined Networking; OpenFlow; Widely Distributed Networks

I. Introduction

Recently, the number of devices that construct the network has increased explosively, and services that are provided on a network have diversified. A network system has also become complicated in such a situation. In most of the organizations in industry, network management is consolidated. The scale of a network of which a network administrator takes care of is ever increasing in either of the number and the kind of devices, geographical coverage, and varieties of compositions, and functions. The network administrator always needs to grasp the construction of the whole network and to modify configurations with an utmost care. When a network configuration is required to be changed across multiple network devices, the administrator must set the configuration to each device one-by-one while checking the integrity of the configuration of the devices during all intermediate status. In order to response to an extraordinary demand of temporary events, a network failure, or a security incident, there is a need to set the configuration of the network quickly. The frequency of changing configuration of a large-scale network by a network administrator is increasing every year and the difficulty of them is as well. As an attempt to solve such situations and to manage network configurations from software in a centralized manner, Software-Defined Networking (SDN) [1] represented by OpenFlow [2] has attracted attention in recent years. In SDN, a network policy intended by an administrator is described as software, and the configuration is reflected to each device automatically by the system. However, OpenFlow assumes that each device has an additional hardware support by which the device can be controlled from outside. There remains a problem how replacement of network devices is applied to an existing network in an organization. When a network controlled by SDN is connected to a conventional network, it is possible to control bandwidth or dynamic paths reflecting the defined policy only on limited part of the network controlled by the SDN; the conventional network connected there to has no controllability in coordination.

In this paper, we assume that the backbone network has a function of SDN such as OpenFlow. The goal of our research is to manage a network in a centralized manner with a single policy by an administrator, where the required configurations are to be set on network devices that does not support SDN functions in real time and automatically over geographically separated multiple wide-area distributed networks. We have developed a network management system to implement this concept.

In our proposed network management system, we detect managed devices composing the network, collect the information of them about physical and logical connection configuration, and store it into a database, based on the concept of Service-Defined Networking (SvDN) [3] that we have proposed. The intent of an administrator when he designs a network and writes down as setting information of the devices are described abstractly as a policy that defines a service provided by the network. This policy is interpreted by the software that operates on SDN controller in the backbone network which supports SDN, while it is converted into setting configuration for each device and is reflected on it in the part of the network which does not support SDN.

In the next section, we show related works. Section III describes issues that conventional networks are facing and

978-3-901882-48-7 (c) 2012 IFIP

the concept of SvDN. In Section IV and Section V, we explain target networks and summarize the architecture of our proposal. In Section VI, we explain two use cases. In Section VII, we describe the conclusion and future work.

II. Related Work

NETCONF [4] is one of attempts to standardize the interface in Internet Engineering Task Force (IETF). This technique is not unified about specific setting procedure, formatting, and functions. In addition, vnfpool is one of working groups within IETF have been discussed for virtualization of network function problems.

Heat [5] is the main project of OpenStack orchestration. This technique can automatically create an environment consisting of a virtual machine instances, and also possible to realize the auto scale. However, this technique is difficult to manage the conventional networks which do not support the SDN concepts.

III. Service-Defined Networking

A. *Issues of Network Management*

For a long time, a network administrator has operated manually network configuration changes with command line interface (CLI) such as telnet or secure shell (SSH), or with graphical user interface (GUI) via a web browser for each devices. Since these interfaces have differences of setting method, formatting, and function that supported for each device, he need to be familiar with how to set for all managed devices.

To manage multiple network devices in a centralized manner, by preparing a software function that generates and sets a configuration information of each device, it is possible to manage automatically or semi-automatically. There are products which has such a function. However, how to get and change configurations of network devices is not standardized, and such the products inevitably become poor versatility system by limiting to the devices of specific vendors and including only specific functions.

It is not rare that a network is operated at approximately the same configuration for more than several years. When an engineer who handled design at the time of introduction of the network leaves one's post, another engineer takes over the operation and management. Then because the network design policy has not been documented, he often needs to imagine the policy of the original design from simple wiring diagram and configuration information which stored in each network device. For example, in a dynamic routing protocol such as OSPF (Open Shortest Path First), each link is given a cost, and a path which has minimum total cost is selected. In networks that are already operational, even if the current path is judged that it is not optimal on the operation and the management, it is difficult to grasp beforehand the link and the cost which should be changed. Then the engineer often modifies the costs of the several links in an ad hoc basis. As a result, it is more difficult to grasp the design policy of the whole network from the configuration of each devices.

In large-scale networks that are operated and managed by a few administrators based on a single policy such as corporate network, campus network, and data center network, the problem mentioned above is alleviated by techniques of virtualization which separate the physical configuration and logical configuration. The techniques of virtualization provide a flexibility for a network design, facilitate configuration changes in the network, and enable construction of a flexible network. On the other hand, such techniques provide flexibility that can set multiple practically equivalent network configurations which meet a request and a requirement, and they complicate network structure by exceeding restrictions of physical topology. Generally, in networks that are operational, unless network design is documented and a documentation is updated whenever the network configuration is changed, it is almost impossible to grasp the intention of design policies and original settings.

In the early Internet, the number, type, and function of network devices managed by one administrator were limited, complexity was low, and the need for documentation of the design policy was hard to recognize. When there was no problem of the Internet security, the entire Internet was open, and operated in a simple policy. Each network device operated independently by their own OS, and it was not necessary to be controlled by a single policy for the whole network. Therefore, the networks such as an Intranet of a corporation, a campus network, a backbone network of a carrier, and a data center network of a cloud service provider is operated in a single policy by one or a few administrator, but they have structure which is not suitable to be managed in a centralized manner.

B. *Concept of Service-Defined Networking (SvDN)*

In order to resolve the situation above fundamentally, Software-Defined Networking (SDN) represented by OpenFlow is proposed in an attempt to control a whole network from software in a centralized manner. In the conventional IP network, the whole network is managed by operating OS for each network devices and by working with distributed coordination. In the concept of SDN, the whole network is managed in one virtual OS in a centralized manner. On the other hand, in SDN, while solving the problems of the conventional network, it is assumed that each devices have a special function embedded for receiving control from external.

In contrast, we have proposed Service-Defined Networking (SvDN) as a higher-order concept to encompass conventional virtualization technologies, and new virtualization technologies such as SDN. The SvDN defines that the whole network provides various functions as "services". A network administrator explicitly describes service "specifications", namely constraints and requirements for functions provided by the network, as service descriptions and policy descriptions. Furthermore, SvDN collects information about the connection topology of the network such as physical connections, and stores its information in a topology database. The implementation design is derived from the topology database, the policy description, and the service description, and the configuration information of each device is automatically generated. An API which set the network configuration is prepared on each device, and the adding and the changing of the configuration information is set automatically through its function. In this way, this system enables to operate centrally management of the whole network without being aware of a network construction. Furthermore, by monitoring the status of the operational network that is obtained from statistic information collected by each device in real time, this system provides the ability to execute automatically predetermined settings, and reduces the burden of operation.

IV. Objective Network

In this paper, we assume the following campus network and data center network and also assume that the backbone network which is connected each widely distributed network is possible to control by the SDN controller.

A. Campus Network

The campus networks have devices to guarantee the security such as firewall at the entrance to the Internet, and include many switches such as routers and switches connected to end hosts. These devices may not support SDN functions. We assume that an administrator can change the configuration of the campus networks freely and flexibly. In order to connect to the backbone network, campus networks have external connection lines, and it is necessary to prepare environment in which add tag to the Ethernet frame based on IEEE802.1q and can communicate with the tagged VLAN on L2 to remote locations.

B. Data Center Network

The data center networks are composed of the network including devices that does not support SDN as with the campus networks. In most cases, the companies hold these networks and manage in conjunction with the services within the companies. In order to managing geographically separated multiple widely distributed networks by a single policy in a centralized manner, it is necessary that the administrator can control the network configuration of the data center to some extent. In order to connect to the backbone network, data center networks are also connected to the external connection lines as with the campus network, and the service that can be flexibly set the VLAN configuration is desirable.

C. Backbone Network

The backbone networks are desirable to compose the network which provide environment that can be used the concept of SDN represented by OpenFlow. By connecting the campus networks and the data center networks by these networks, the administrator can manage the whole network flexibly based on proposal architecture in next section.

V. Proposal Architecture

A. Network Management System

Our proposed network management system defines that the whole network provides various functions as services. A network administrator explicitly describes service specifications, namely constraints and requirements for functions provided by the network, as service descriptions and policy descriptions. At the same time, in the campus networks and the data center networks, this system collects information about the connection topology of the network such as physical connection automatically, and stores it in a topology database.

It can automatically build appropriate network setting with maintaining a design policy and an intention of the network by deriving the specifications description of the network from the service description, the policy description,

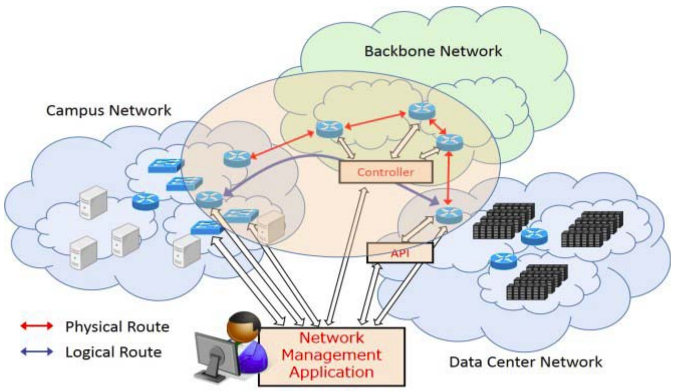

Fig. 1. Managed network with proposed application

and topology database. In figure 1, in the campus network and the data center network side, this system automatically generates the configuration of each device by deriving network specifications and applies it. On the other hand, in the backbone network side, this system automatically operates necessary network configuration without going through hands by transmitting necessary setting information to controllers such as OpenFlow.

B. Architecture

Figure 2 shows the architecture of our proposal automatic management system, and colored parts are modules that are developed in this research. Arrows show flows of data or commands.

Based on the concept of SvDN, our system stores the physical and logical connections and configuration information that are derived from network devices. (These functions correspond to the network topology collection engine and the network topology database in the figure.) An administrator designs network environment and writes down configuration information of each network devices. Then we recognize the intention of the administrator as a service provided. The administrator describes the policy by abstraction and our system recognizes the described policy. (These functions correspond to the defined service specification, the service specification controller, and the service specification database.) Our system designs the network that satisfies the service specification from service specification database and network topology database. (These functions correspond to the network design engine and the network design template database.) Based on the network design database, our system derives configuration of each network devices and SDN devices. (These functions correspond to the network device configuration engine and the network device configuration database.) In the SDN network, the derived configuration is interpreted as software which operates on the SDN Controller. On the other hand, in the conventional network, it is converted into configuration information for each device, and set. (These functions correspond to the configuration provisioning engine.)

VI. Use Case

We assumed that a backbone network connects a campus network and a datacenter network, and we considered the following two scenarios using our architecture.

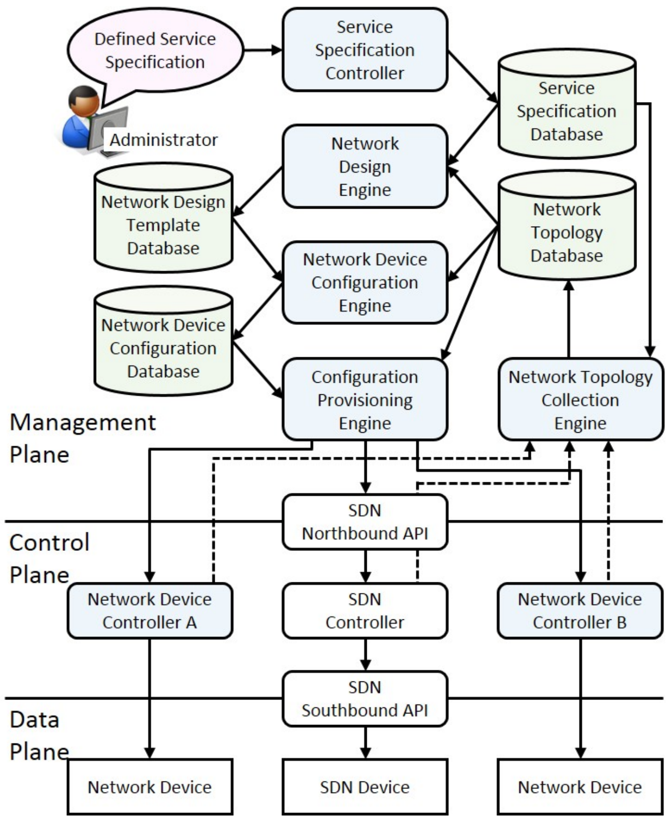

Fig. 2. Architecture of our antomatic management system

A. VLAN Setting

In Figure 3, we considered the scenario that we connect the virtual network interface of a virtual machine (VM) which is generated dynamically in the data center network to the assigned VLAN of the campus network. Our proposed network management system enables to execute the setting configuration about each network automatically, because our system stored information of the campus network and the data center network in a topology database. First, a new VM is generated in the data center network. Next, the network management application sets configuration for each network devices so that VMs in the campus network and a new VM can communicate by assigned VLAN. As a result, the generated VM seems like direct connection to the campus network subnet.

B. Priority Control

In Figure 4, when a distributed denial of service attack (DDoS attack) is occurred for the virtual machine on the data center network, DDoS attack is detected in the virtual machine located in the data center side as a trigger, and this system set the filter for the firewall router in the campus network as an action.

VII. Conclusion

In this paper, we explained an architecture of the operation and management of the wide-area distributed network by the defined network specification. On the assumption that the backbone network has the function of SDN such as OpenFlow, our purpose is that multiple

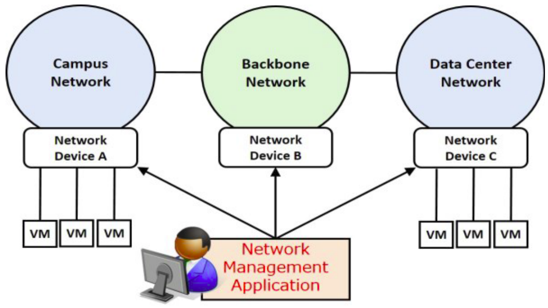

Fig. 3. Use case I (VLAN Setting)

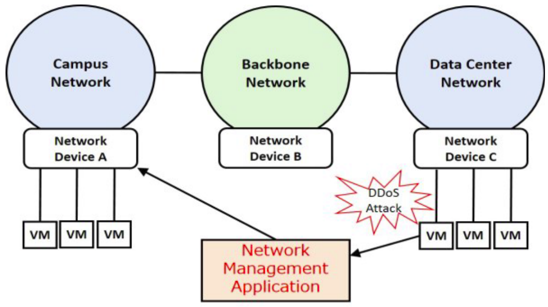

Fig. 4. Use case II (Priority Control)

wide-area distributed networks are managed centrally with single policy by the administrator, and the required settings are to be set in real time and automatically. We also show two use cases. Next, we are going to implement the extension of network management application that operates in conjunction with the content distribution application.

Acknowledgment

This paper receives assistance to Project for Promotion of Advanced Communication Applications Development in Ministry of Internet Affairs and Communications 2013 (Type II) and 2014 (Type I). The authors would like to present our sincere appreciation to Professor Osamu Nakamura and Product Assistant Professor Shigeya Suzuki of Keio University.

Reference

[1] McKeown, Nick, et al, "OpenFlow: enabling innovation in campus networks," ACM SIGCOMM Computer Communication Review, 38.2, pp.69-74, Apr.2008.

[2] Open Networking Foundation, “Software-Defined Networking: The New Norm for Networks,” ONF White Paper, Apr.2012.

[3] Yasuhiro Teramoto, Rei Atarashi, Yoshifumi Atarashi, Yasuo Okabe, “Managing Networks Independently of the Physical Topology by Service Defined Network,” The 1st IEEE International Workshop on Architecture, Design, Deployment and Management of Networks and Applications (ADMNET2013), (Proc. IEEE COMPSAC2013 Workshops), Kyoto, Japan, July.2013.

[4] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, “NETCONF Configuration Protocol (NETCONF),” RFC 6241, IETF, Jun.2011.

[5] OpenStack, “Welcome to the Heat developer documentation! ,” http://docs.openstack.org/developer/heat/ (accessed Sep 24th).