The Dynamic Network Configuration Method that reflects User Requests using OpenFlow

Takeshi OOWARI, Ayumu YOSHINE and Osamu MIZUNO
Graduate School of Electrical and Electronic Engineering,
Kogakuin University
Tokyo, Japan

***Abstract*—Business network is designed to match their organizational structure. Therefore, network reconfiguration is required to meet change of organizational structure and requirements from users. However, quick and detailed reconfiguration is difficult because configuration in conventional network equipment need to be modified manually for each network apparatuses. The purpose of this study is to improve quick response of network reconfiguration to meet users' requests. We realize the access control method based on organizational structure by cooperating OpenFlow and database that saved user information. We propose the network control scheme that users are able to edit structure information. To confirm the proposed methods, we made test bed and performed operation verification. As a result, we confirmed that the change of structure information by users was reflected in network control within 5 seconds.**

Keywords—SDN; OpenFlow; Network Control

I. INTRODUCTION

Business network of such as companies and universities are designed to match their organizational structure consisting of elements such as user's job title and affiliation. Network reconfiguration is required, if organizational structure has changed with such as personnel moving. In addition, demands may occur to an administrator from users in the organization network. For example, there are requirements of such as grant and change of access authority. However, configuration in conventional network equipment changes manually for each equipment units. Therefore, detailed correspond is difficult in conventional network equipment. Following requirements for network system needs to be solved to meet demand from users.

1) Network control that based on user affiliation

2) Quick responsiveness of the network reconfiguration at time of the change of affiliation information

3) Quick reflection of user requests to network

The purpose of this study is to improve quick response of network reconfiguration to requests from users. Here we describe test bed construction and the operation verification.

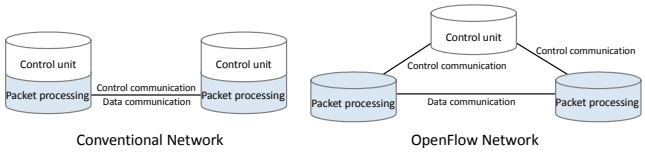

Figure 1. Conventional and OpenFlow network[2]

II. RELATED TECHNOLOGY

A. OpenFlow

OpenFlow[1] is known as one of the technologies of Software Defined Networking (SDN). OpenFlow is network architecture with several characteristics different from conventional network. The first characteristic is that network equipment is divided into control device and transfer device. Second, the transfer devices are centrally controlled by the control device. Finally, operations of the control device are directly programmable. Figure 1 shows comparison of conventional and OpenFlow network[2]. In OpenFlow, the control device is called an OpenFlow Controller, and transfer device is called an OpenFlow Switch. Moreover, exchange of control signals is carried out in accordance with OpenFlow protocol.

OpenFlow Switch transfers packets according to a transfer rule set that is called Flow Entry. Flow Entry is consisted of following three elements.

1) Header Field: Match condition of packets is listed

2) Action: Handling of packet that matched a condition is listed

3) Counters: Statistics such as the number of packets and quantity of communication data that match Flow Entry is stored.

Match conditions of Flow Entry is limited to physical information such as terminal information and the port number of switches. Therefore, OpenFlow can't perform network control based on user affiliation information.

B. Previous Reserch

Whereas the problem in OpenFlow, there are methods [3][4] that reflect organizational structure to network control by cooperate OpenFlow Controller with database of Directory Services. Directory Services is a service that performs access control to each resource, and user authentication. To achieve the above services, Directory Services has a database that

stores management information including information such as user's job title and affiliation. When user performs authentication in Directory Services, OpenFlow Controller relates the user's affiliation information and terminal information. From the above, OpenFlow Controller can derive the affiliation information corresponding to the terminal information from the database, and performs network control based on organization structure.

Requirement 1 that mentioned in Chapter I is satisfied by the above method. However, the method is believed to be changed the affiliation information in database by the service administrator. Therefore, there is possibility that the change of fine affiliation information is delayed. It is difficult to meet Requirement 3.

III. The Dynamic Network Configuration Method that Reflects User Requests

A. *Overview of the method*

The method performs network configuration based on user affiliation information, and reflects the latest affiliation information to the network control by deciding whether perform packet transfer to every communication requests occur. Moreover, delay of reflection of user requests in the network is reduced by providing limited editing authority of affiliation information that based on user's job title and affiliation.

There are two functions to realize the method. One is the access control function that based on organizational structure. The other is the affiliation information editing function that based on user's authority. OpenFlow Controller performs the access control function, and the administration Web server provides to users the affiliation information editing function. Figure 2 shows system block diagram of the method.

B. *Access Control Function based on Organizational Structure*

The function performs access control according to organizational structure by associating terminal information and user's affiliation information. The OpenFlow Controller checks whether source terminal is associated with the user information, when an OpenFlow Switch queried processing of packets to the OpenFlow Controller. The OpenFlow Controller inquires login information to the administration web server, if source terminal was not associated with user's affiliation information. If there is information of the source terminal in the login information, the OpenFlow Controller associates the user's affiliation information and MAC address of the source terminal. Subsequently, the OpenFlow Controller compares information that is associated with the destination and the source terminal. Only when they matched affiliation information that was compared the source and the destination, the OpenFlow Controller performs route calculation and sets Flow Entry to OpenFlow Switches as necessary. If not, the packet would be dropped. Figure 3 shows a flowchart of the function operation.

C. *Affiliation information editing function based on user's authority*

The administration Web server provides Web pages to edit affiliation information based on authority. In this Web page, a

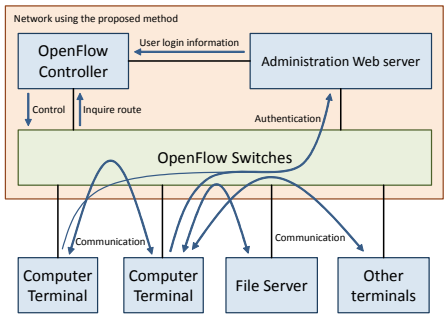

Figure 2. Outline block diagram of the proposed method

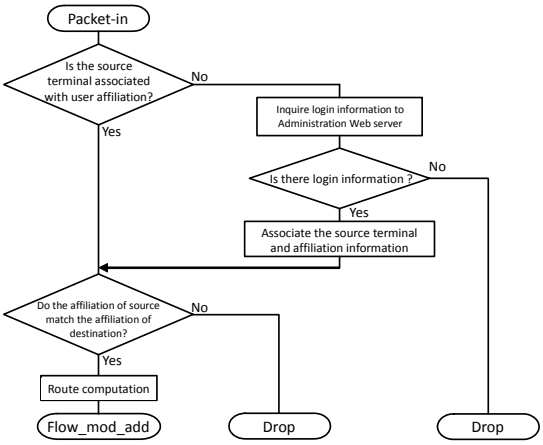

Figure 3. Flowchart that determine whether perform transfer packet

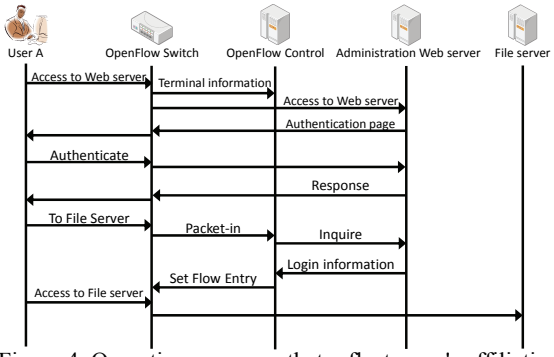

Figure 4. Operation sequence that reflects user's affiliation

user can add affiliation information, remove them. It also gives editing authority to a user. Affiliation information is represented in tree structure, and the administrator of the organization network is located vertex of the tree. User's editing authority is set for each affiliation to give appropriate editing authority, when a user has several affiliation or job title, access rights.

*1) Addition of a new affiliation to a user:*The user is able to add the affiliation that given edit authority or belongs to lower one.

*2) Removing the affiliation information from user information in database:*The user is required upper authority than user's authority to add the affiliation information.

3) Setting of editing authority: The user must belong to upper affiliation than the edit target.

D. *Operation of the method*

In case of using network that provided by the method, a user perform authentication to the administration Web server. The access control function works only for a terminal that authenticated to the server. As an exception, access to the administration Web server is allowed to all terminals. Figure 4 shows operation sequences of the proposed method.

IV. OPERATION CHECK OF THE METHOD

A. *Overview of Operation check*

We build a test bed to verify proposed its operation. The verification includes whether the proposed methods meet the requirements shown in Chapter I.

B. *Constructed of the testbed*

The test bed network consists of an OpenFlow Controller, three OpenFlow Switches, an administration Web server, two note PCs for hosts, and a file server. We used MySQL as database. Table 1 shows the test bed environment, and Figure 5 shows overview of test bed network. In addition, there are two affiliation named 'g1-1' and 'g1-2'. 'g1-1' has affiliation of the file server.

The OpenFlow Controller sends topology exploration packets like LLDP to all switches to every 30 seconds. Moreover, route is defined by the Dijkstra algorithm, and the route with minimum number of hops is used.

C. *Verification of the network control based on user requests*

Host1 accessed to the file server while switching authentication to users of different affiliation as a verification of the access control operation based on organizational structure. We switched user that authenticate from “unauthenticated user” to “a user belongs to g1-1” to “a user belongs to g1-2”. Table 2 shows the result that is expected and actual results. Figure 6 shows the screen output of the OpenFlow Controller, when OpenFlow Controller allowed packets transfer. As a result, it confirmed that only users who have affiliation information of host1 could access to file server.

In addition, we were subjected to the following verification to confirm of whether performing the dynamic correspondence of the network whereas change of affiliation information by a user.

1) Host1 performs to authenticate with user A, host2 performs to authenticate with user B that has edit authority.
2) Host2 changes affiliation of user A from "Not affiliation" to "g1-1" to "g1-2".
3) Host1 performs access to File server whenever affiliation of user A is changed.

Table 3 shows the result that is expected and the actual result. As a result, it confirmed that communication to File Server was allowed only if affiliation information of user A was consistent with the affiliation information of file server. We confirmed that the change of structure information was reflected in network control within 5 seconds in both of two times of verification.

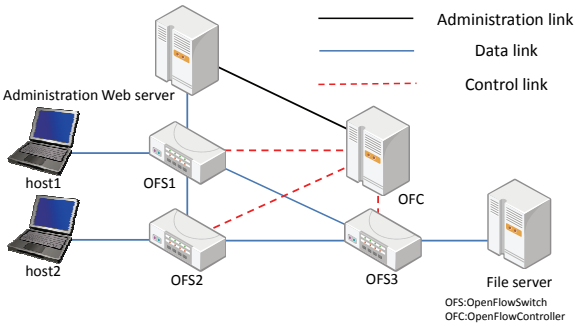

Figure 5. Test bed

Table 1. Environment

Equipments	Model number	Remarks
OpenFlow Controller	IBM System x3250 M4	Trema0.4.7
OpenFlow Switch*3	Pica8 p-3290	OpenFlow1.0
Administration Web server	HP ProLiant MicroServer	Apache2.2.22
File server	HP ProLiant MicroServer	samba 4.0.0alpha18
Notebook PC*2	HP Probook 6570b	

Table 2. Result of verification that change the user to authenticate

Authentication user	Unauthenticated user	User belongs to g1-1	User belongs to g1-2
Expected result	Inaccessible	Accessible	Inaccessible
Actual result	Inaccessible	Accessible	Inaccessible

```
==packet_in=2015-01-06 12:32:29 +0900============================
7461348157367084516()->7461348157367084546(7461348157367084516)
send flow_mod to 7461348157367084546 :: action => Transfer to 7461348157367084516 from port 2
send flow_mod to 7461348157367084516 :: action => Transfer to host from port 1
MAC:d4:c9:ef:4f:19:dc => 38:ea:a7:ab:f3:1e
group match:g1-1
==packet_in=2015-01-06 12:32:29 +0900============================
7461348157367084546()->7461348157367084516(7461348157367084546)
send flow_mod to 7461348157367084546 :: action => Transfer to 7461348157367084546 from port 2
send flow_mod to 7461348157367084546 :: action => Transfer to host from port 3
MAC:38:ea:a7:ab:f3:1e => d4:c9:ef:4f:19:dc
IP:192.168.14.4 => 192.168.14.2
group match:g1-1
```

Figure 6. Screenshot of when affiliation information matched

Table 3. Result of verification that change the user affiliation

UserA affiliation	Not affiliation	g1-1	g1-2
Expected result	Inaccessible	Accessible	Inaccessible
Actual result	Inaccessible	Accessible	Inaccessible

V. CONCLUSION

Whereas the problems that detailed correspond is difficult in conventional network, we proposed the network configuration method that reflects the change of organizational structure by users using OpenFlow. We build test bed and confirmed operations of the proposed methods. As a result, we confirmed the OpenFlow Controller was allowed to communicate, only when affiliation of source terminal matched with destination terminal. In addition, we confirmed that the change of structure information by users was reflected in network control within 5 seconds.

REFERENCES

[1] N. McKeown et al., “OpenFlow: enabling innovation in campus networks,” SIGCOMM Comput. Commum. Rev., Vol.38, No.2.pp 69-74,Mar., 2008.

[2] Akimichi, Naoki MIYANAGA, Atushi IWATA, “Mastering TCP/IP OpenFlow Ver.” Ohmsha, 2013.

[3] Shigeaki MAEDA et al., “The proposal of Dynamic Network Control Method Affected by Organizational Structure Using SDN/OpenFlow” IEICE Technical Report, Vol. 113, No. 473.pp 187-192, Mar., 2014.

[4] Yoshinao KIKUCHI and Yuji AGAWA, “Proposal on office network setting method using SDN and auhentication infrastructure” IEICE Technical Report, Vol. 114, No. 139.pp 61-66, July, 2014.