IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.6, No 4, July-August 2016

Proposal of the Management System in LAN by using VNIC and Unique ID

Satoshi Kodama
Dept. of Information Science
Tokyo University of Science
Tokyo, Japan

Rei Nakagawa, Toshimitsu Tanouchi
Dept. of Information Science
Tokyo University of Science
Tokyo, Japan

***Abstract*—In recent years, Local Area Network becomes essential to manage a local communication in university, company, and so on. LAN comes to be consisted of a large number of devices. There is many crowded network segment in a short interval. This situation makes a control of LAN complicated. The control is often implemented by using functions of a network device such as Virtual LAN(VLAN). However, it is not easy to change the network layout, and it has problems such as the restriction of hardware and the problem of flexibility. This paper proposes the management system to relax these problems. It has the function to manage communication between devices in LAN by using Virtual Network Interface Card(VNIC) and the unique ID that is made from device's specific information. We conducted experiments to certify the effectiveness of our method. Experimental results show that the implementation of this system as a software makes it easy to manage the devices flexibly in LAN**

Keywords-Cross-Layer, Network Architecture, VLAN, Software-Defined-Network

I. INTRODUCTION

Background

Local Area Network(LAN) is often used to manage a local communication. With development of internet technology, the number of devices has been increasing sharply in LAN; the configuring of the device has been complicated. Besides, the purpose of using the LAN also ranges from business use to personal use. For instance, in the company, there are often more restrictions in the security than personal use especially. For example, in the case of an Intranet that is built in company by a wired LAN, secrecy is considered important in order not to leak critical information for outside of the company. An Intranet is often composed of not a wireless LAN but a wired LAN because a wireless LAN has more problems in the security such as wiretapping. However, this situation may be an obstacle to the flexibility. For example, the reconstruction of the Intranet can turn to be cause of a security vulnerability. The secondary, the addition of the network segment in the Intranet can turn to be cause of compatibility issues of the device for the technologies such as "Port based VLAN" and "Tagged VLAN". Moreover, the Intranet system that has these functions costs very much. Hence, the need for the solution against these problems and the research for the improvements has been growing [1][2].

Virtual LAN

Virtual LAN is used as a LAN management system widely now. It manages the communication among the same group and the communication only for between the devices in each specific group. Thereby, VLAN assigns the network device to certain VLAN Group. It can manage the quantity of communication and the range of it. There are some methods to control VLAN Group. However, in some cases, it has problems in flexibility. For example, in the case of the method called "Port based VLAN", this method determines a VLAN Group by the port information that the device connects with. This method has the problem that a performance becomes poor when a network layout is changed frequently. Secondary, in the case of the method called "Tagged VLAN", this method determines a VLAN Group by reading the data that is called "VLAN Tag" in the customized packet. This method has the problem that the device cannot recognize communication normally when it is non-correspondence for the method. Moreover, small differences in the setting that is unique to the maker of the device may influence the problem in the compatibility. In brief, VLAN has problems in the flexibility about extensibility of a network.

Software defined network

In recent years, the architecture called Software Defined Network (SDN) attracts interests as the new network management system. It is difficult to change the highly confidential network when it is built once. There are problems about the flexibility such as changing a network layout and configuring Quality of Service (QoS) every application. SDN decouples the network control and forwarding functions that enable the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. In other words, SDN takes measures against problems of a network management by making it programmable as a software [3][4][5]. However, SDN takes much time to implement it because SDN has problems such as the interconnection-related problem, and the introduction cost of the device composing SDN.

The purpose of this study

In the previous research, the network management system that has the following two functions; the first, it is managing communication between the devices by assigning client-number on the system to the device and admitting the communication between specific client-number; the second, it is the prohibition of the communication between the third party that connects to the LAN illegally and the authorized user [6]. In brief, these functions perform a behavior similar to that of VLAN. In addition to the above functions, this study aims at the solution against the problems for VLAN that are both the restriction of hardware and the problem of flexibility. We are finally intended to implement these functions as a software to each device in a wired LAN.

II. System Overview

This section describes an overview of the system that we propose on LAN. This system has two following functions.

(1) Manage the communication between specific PC-numbers on the system by using the ID that is made from a unique information of the device.

(2) Renew an Ethernet Frame in LAN in consideration of the compatibility with a conventional device.

Figure 1 shows the system overview. This system is composed of 7 terminals (6 clients and 1 server). Each of an authorized clients is connected to each NIC of the server(eth0, eth1, eth2, eth3, eth4, eth5) with a wired LAN cable through NIC(eth0) of the client. The router that is prepared as a conventional device is connected to NIC of the server(eth7). The movement of the start preparations for the system is as follows.

(1) Both of the client and the server start VNIC together.

(2) The client executes the program called "./bridge", and the server executes the program called "./serverBridge". The "./bridge" program performs the bridging between VNIC and NIC in the client, and the "./serverBridge" program performs synchronizing of the ID in addition to the same process of the "./bridge" program in the server.

(3) In past a series of processing, the server reads the text file that is written as the correspondence information of PC-number with Communication Groups.

(4) The client and the server each start communication.

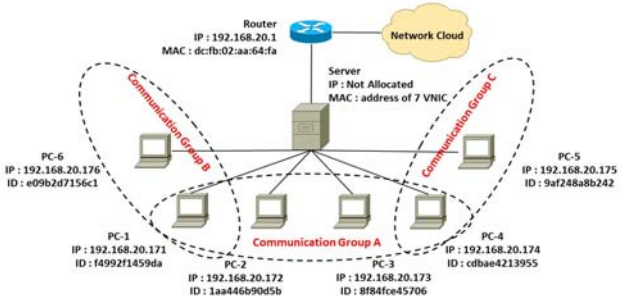

Figure 1. Overview of the LAN Management System

III. System Detail

This section describes a detail of the two functions that are mentioned in preceding section.

Managing the communication between specific PC-numbers

The purpose of this function is the control of communication among the authorized devices. This process is represented mainly by two following processing, making the unique ID of the client and assigning PC-number to the clients in LAN. As for making the unique ID, the unique ID is hash value that is generated from the key that is made from the serial number of the client's HDD and the version information of the client's OS by executing the program; this unique ID is used as the client's MAC address and is used for renewal of the Ethernet frame. As for assigning PC-number to the clients, the authorized client's ID is registered with the list of the management information that is described in "group.txt" as shown in the Figure 2. Besides, with the devices such as a router and the printer, MAC addresses of these are registered because these own ID cannot be made.

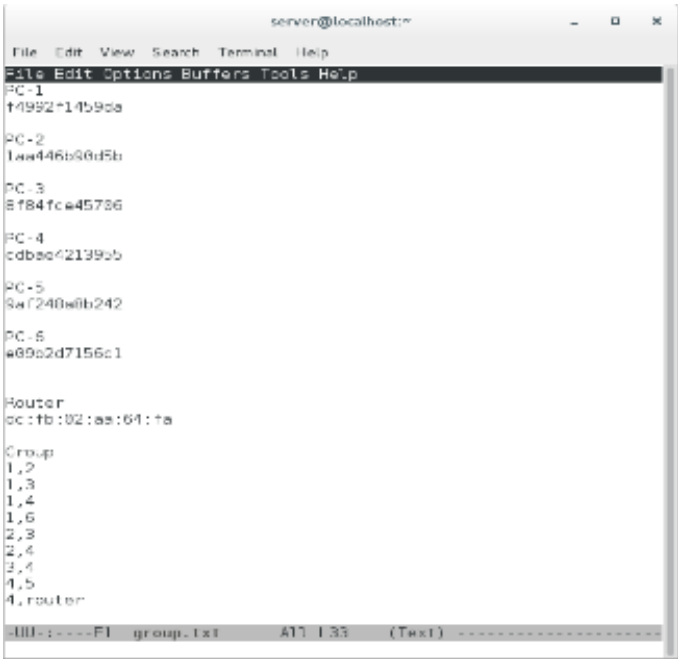

Figure 2. Correspondence information of the client's ID with the Communication Group(group.txt)

The detailed movement of the communication control by grouping the clients is as follows.

(1) When the server receives an Ethernet frame that the client transmitted, the server determines the PC-number of the source client from the source MAC address and the PC-number of the destination client from the destination MAC address in referring to the management information that is described in the "group.txt". If the MAC address is not registered with

either PC-number that is described in "group.txt", the server will cancel the communication.

(2) If the MAC address is registered with each PC-number, the server will determine whether the communication between the PC-numbers that each of the clients is registered with is admitted or not according to the "group" section in "group.txt". If it is not admitted, the server will cancel the communication.

(3) If the communication between the clients is admitted, the server will continue transmitting the Ethernet frame.

Renewal of an Ethernet frame

The purpose of this function is renewal of an Ethernet frame, which is customized for better compatibility with a conventional device. While our system runs, both the server and the authorized clients perform a bridging between VNIC and NIC as shown in the Figure 3; when VNIC receives an Ethernet frame and transmits it, the bridging renews the Ethernet frame. As for renewal of an Ethernet frame, a hash value is used for the data part of the Ethernet frame. This hash value is generated from the unique ID of the device. When the device transmits the Ethernet frame, the bridging adds the hash value to every byte from the top of the data part. When the device receives the Ethernet frame, the bridging subtracts the hash value from every byte from the top of the data part. Therefore, the bridging renews the data part without changing the sizes of it. On the other hand, in the case of the communication between the server and a conventional device, the normal Ethernet frame is used because a conventional device cannot restore the renewed data. The detailed movement of the renewal of an Ethernet frame is as follows.

(1) When an authorized client transmits an Ethernet frame, the client renews the data part of Ethernet frame by adding a hash value that is generated from the client's own unique ID, and transmits it.

(2) When a server receives the Ethernet frame, the server renews the data part of the Ethernet frame by subtracting a hash value that is generated from the unique ID that is registered with PC-number as the client in the "group.txt".

(3) The server determines whether the current communication partner is a conventional device or not. In the case of a conventional device, the server just transmits an Ethernet frame. In the case of the authorized client, the server transmits the Ethernet frame that is renewed by adding a hash value that is generated from the client's own unique ID.

(4) When the client receives an Ethernet frame, the client renews the data part of the Ethernet frame by subtracting a hash value that is generated from the client's own unique ID. When the conventional device receives the Ethernet frame, the device do not make any change to the Ethernet frame.

In the reverse communication, the devices can communicate normally by performing similar movement.

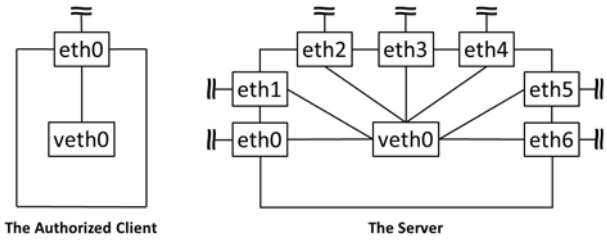

Figure 3. Overview of the bridging between NIC and VNIC

IV. RESULTS

This section describes the experimental results at the system that is composed of devices as shown in the Figure 1. The system depends on the management information as shown in the Figure 2. Details of the device-specific information are as shown in the Table 1, Table 1 and Table1.

TABLE 1. COMMUNICATION GROUP A

	PC-3	**PC-1, PC-2, PC-4**
OS	Cent OS 7	Cent OS 7
CPU	Intel (R) Core(TM) i7-2600 3.40GHz	Intel (R) Core(TM)2 Duo E8135 2.66GHz
MEMORY	4.0GB	4.0GB
LAN System	10/100/1000BASE-T Gigabit Ethernet	10/100/1000BASE-T Gigabit Ethernet

TABLE 2. COMMUNICATION GROUP B

	PC-1, PC-6
OS	Cent OS 7
CPU	Intel (R) Core(TM)2 Duo E8135 2.66GHz
MEMORY	4.0GB
LAN System	10/100/1000BASE-T Gigabit Ethernet

TABLE 3. COMMUNICATION GROUP C AND SERVER

	PC-4, PC-5	**Server**
OS	Cent OS 7	Cent OS 7
CPU	Intel (R) Core(TM)2 Duo E8135 2.66GHz	Intel (R) Core(TM) i7-6700 3.40GHz
MEMORY	4.0GB	16.0GB
LAN System	10/100/1000BASE-T Gigabit Ethernet	10/100/1000BASE-T Gigabit Ethernet

Communication control by the grouping

Figure 4 shows that the admitted communication between "PC-4" and "PC-1" succeeded. Figure 5 shows that the prohibited communication between "PC-4" and "PC-6" is cancelled. Figure 6 shows that the admitted communication between "PC-4" and the Router as a conventional device.

As a result, the communication control is carried out according to the correspondence information of PC-number with the admitted communication as Figure 2 shows.

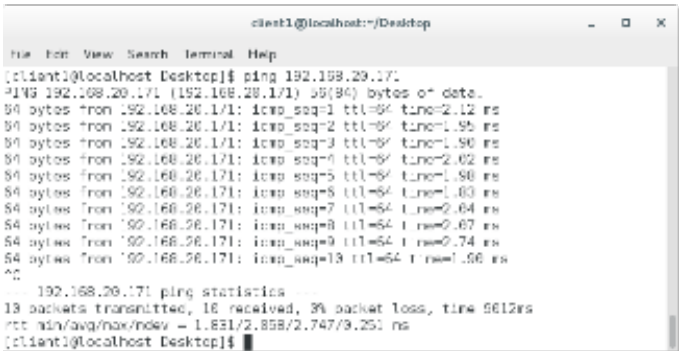

Figure 4. Communication between “PC-4” and “PC-1”

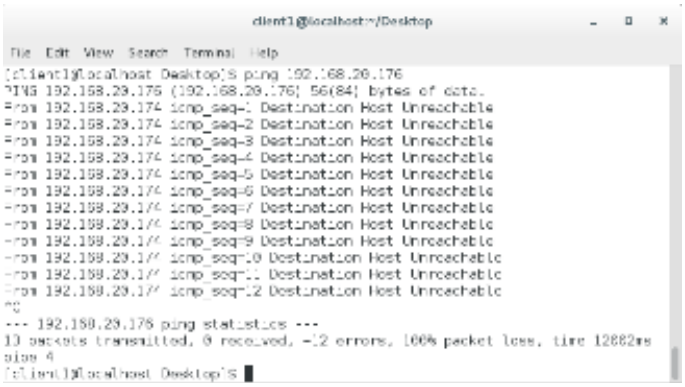

Figure 5. Communication between “PC-4” and “PC-6”

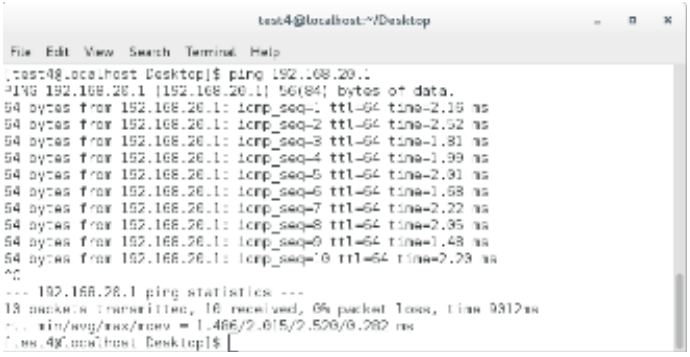

Figure 6. Communication between “PC-4” and the router

Normal Ethernet frame and renewed Ethernet frame

We confirmed whether the renewal of the Ethernet frame succeeded or not through the communication experiment by using the TCPDUMP command. Figure 7 shows the normal Ethernet frame on the communication between “PC-1” and “PC-4”. Figure 8 shows the renewed Ethernet frame on the communication between “PC-1” and “PC-4”.

As a result, the renewal of the Ethernet frame succeeded.

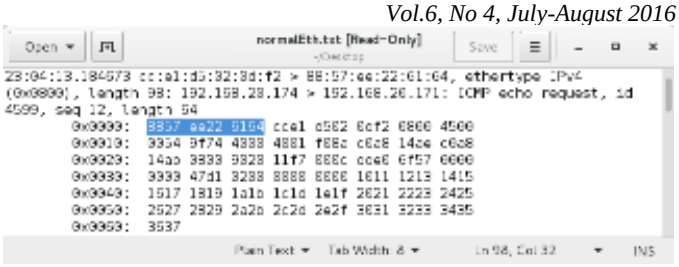

Figure 7. The normal Ethernet frame between “PC-1” and “PC-4”

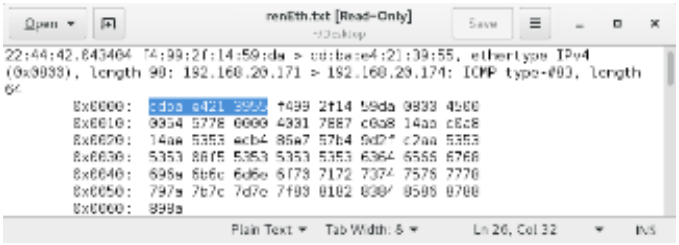

Figure 8. The renewed Ethernet frame between “PC-1” and “PC-4”

Measurement of the throughput on the system

We conducted the measurement experiment of the transmission rate in order to compare the system that we propose with the system using a conventional device by using the client-server system by apache. We build the conventional system that Figure 9 shows as a target for comparison. Table 2 shows that throughput in the conventional system and throughput in the proposed system.

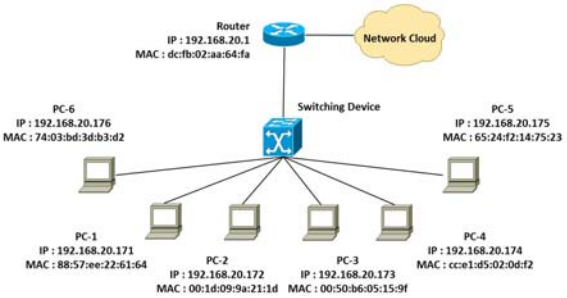

Figure 9. The VLAN system as a target for comparison

TABLE 4. COMPARISON OF THROUGHPUT

Number of trials	Time of conventional system (Mbps)	Time of proposed system (Mbps)
1	11.2	11.2
2	11.2	11.2
3	11.2	11.1
4	11.2	11.2
5	11.2	11.1

As a result, the proposed system can communicate without losing throughput in comparison with a conventional system.

V. CONCLUSION

We proposed We archived the LAN management system which enables two following functions.

(1) The system lets each of the clients belongs to each of the PC-numbers, and controls the communication between PC-numbers by assigning each of the PC-numbers to each of the Communication Groups.

(2) The system performs the renewal of data in consideration of the compatibility with a conventional device.

(3) The implementation of the system as a software relaxes both the restriction of hardware and the problem of flexibility in VLAN.

In (3) statement, we can compose the system as Figure 10 shows.

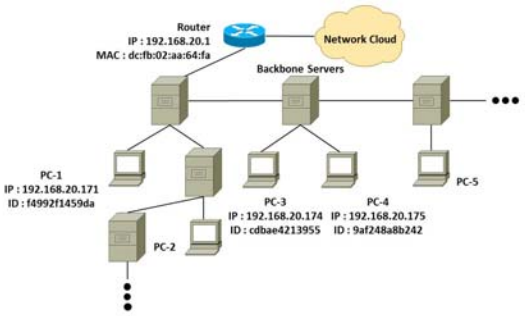

Figure 10. The flexibility of the proposed system

The system obtains three improvements. The firstly, it is the realization of hierarchical structure. The secondary, it is the unitary management of the backbone servers. The thirdly, it is working with both the software and any device without using the specific device. Thus, the system manages LAN flexibly and relaxes the restriction of hardware.

VI. DISCUSSION

The need for VNIC

This study enables both control of the communication and renewal of an Ethernet frame by performing bridging between VNIC and NIC. At the initial stage of the experiment, we tried renewal of the Ethernet frame using the Raw socket on NIC. However, both of a normal Ethernet frame and a renewed Ethernet frame were transmitted at the same time. The reason for this phenomenon is that the renewed Ethernet frames is transmitted without the normal Ethernet frame being canceled. As a result, the renewed Ethernet frame duplicates with the normal Ethernet frame because the renewed Ethernet frame is made from the copy of the awaiting transmission buffer of NIC. Therefore, as a countermeasure, we propose the method that the renewed Ethernet frame is transmitted from the VNIC instead of NIC. VNIC cannot transmit the normal Ethernet frame. Besides, VNIC can copy the normal Ethernet frame to VNIC's own awaiting transmission buffer through the Raw socket on NIC. Thereby, VNIC can transmit only the renewed Ethernet frame.

The need for the periodical update of the unique ID

. We had concerns of information leakage by outflow of the ID from the system for using the same ID. We inspected whether both update of the ID and synchronization of it were possible during communication on the system. The detailed movement of periodical update for the unique ID is as follows.

(1) The server generates random number, and makes ARP packets that stored away the random number. The server transmits each of ARP packets for all authorized clients. Till the update finishes from this point in time, the server stores the Ethernet frame in the awaiting transmission buffer.

(2) When the authorized client receives the ARP packet from the server, the client takes out a random number (r1) from the ARP packet and generates a hash value (h1) from both of the client's own unique ID (id1) and the random number (r1). Since then, this hash value is used as new client's unique ID (id2).

(3) . The client generates the new hash value (h2) from both of the new ID (id2) and the random number (r1). The client stores this new hash value (h2) and the new ID (id2) in the ARP packet and transmits it as a Gratuitous ARP packet.

(4) When the server receives the Gratuitous ARP packet from the client, the server generates the hash value (h3) from both of the unique ID (id3) that is registered with the server as the client and the random number (r1), and the server compares the hash value (h2) that is stored in the Gratuitous ARP packet with the hash value (h3). If “h2” matches “h3”, the unique ID (id3) will be updated to the new ID (id2). After the update is finished, if there is the Gratuitous ARP packet in the awaiting transmission buffer, the server will transmit it.

(5) When the client receives the Gratuitous ARP packet from the server, the client updates the client's own ARP table with the new ID (id2).

Figure 11 shows that the periodical update of the unique ID succeeded according to the above series of movement. However, there is a problem of the update interval. The above series of movement are implemented to work as the event-driven by the server. Therefore, the ID can be updated only at the static time interval that the server appointed. As a future issue, It is necessary to grope for a method to set the update interval dynamically by the server collaborating with the client.

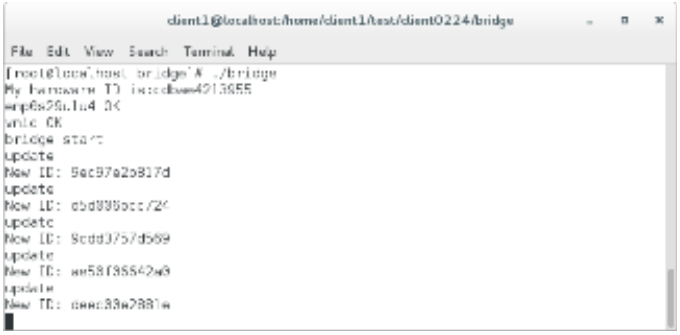

Figure 11. The periodical update of the unique ID

REFERENCES

[1] Dmitry Drutskoy, Eric Keller, and Jennifer Rexford. “scalable network virtualization in software defined network” IEEE Internet Computing, 17(2):20–27, 2013.

[2] Sean Wilkins. “Virtual vs. Physical LANs: Device Functionalities” CCNA Routing and Switching 200-120 Network Simulator, 2015

[3] Albert Greenberg, Gisil Hjalmtysson, David A. Maltz, Andy Myers, Jennifer Rexford, Geoffrey Xie, Hong Yan and Jibin Zhang. “a clean state 4d approach to network control and management”. ACM SIGCOMM Computer Communication Review, 35(5):41-54, 2005.

[4] Hyojoon Kim and Nick Feamster. “improving network management with software defined network”. IEEE Communications Magazine, 51(2):114--119, 2013.

[5] Soheil~Hassas Yeganeh, Amin Tootoonchian, and Yashar Ganjali. “on scalability of software-defined networking”. IEEE Communications Magazine, 51(2):136--141, 2013.

[6] Yuta Watanabe and Satoshi Kodama. “implementation of flexible network system with the grouping method by using vnic and unique id”