Electronic Preprint for Journal of Information Processing Vol.21 No.3

Regular Paper

A Configuration of Location Free Network Applicable to Location Dependent Services

Yoshihiro Ohsumi[1,a)] Kiyohiko Okayama[1,b)] Nariyoshi Yamai[1,c)]

Received: October 22, 2012, Accepted: March 1, 2013

Abstract: By using a dynamic VLAN feature of recent network equipment, we can configure a location-free network environment which can authenticate a user of a terminal and assign a VLAN for his/her terminal dynamically so that the user can connect his/her terminal to the same VLAN anywhere in the organization. However, on such a location-free network environment, it is difficult to use some location dependent services. One typical location dependent service is site license of an electronic journal (e-journal) that users can access the contents only if they are in specific locations. In this paper, we propose configuration of a location free network which can adapt location dependent services by devising the allocation of the VLAN-IDs and the subnet IP addresses. By this method, since no special equipment is required, it is possible to build a network system without extra cost. We configured the network system based on the proposed method on the campus network of Okayama University and confirmed the effectiveness and the practicability on accessing some site-licensed e-journals.

Keywords: VLAN, location free network, location dependent services, electronic journal, site license

1. Introduction

Recently, network equipment has become highly advanced, that is, they have been able to provide various additional functions as well as high capacity and high reliability. As a security function, when a terminal is connected to the network, the network equipment can authenticate the terminal or its user, and connect the authorized terminal to a specific VLAN according to the authentication result. By such an authentication function, when a user connects his/her terminal to the network from anywhere, it is always able to be connected to a subnet of the same VLAN-ID. We call such a network a "location free network." However, when a location free network is configured by means of conventional methods, since the IP address of the user's terminal is within the same range regardless of its location, it is difficult to use some location dependent services, such as a site licensed electronic journal (e-journal) with access control based on user's IP address.

In this paper, we propose a network system applicable to location dependent services even on the location free network. This system determines the location of the user, and allows servers to perform access control based on the client's IP address by assigning a different subnet with the same VLAN-ID based on the user's location. In addition, even when authorized users connecting from the outside of the organization by VPN (Virtual Private Network) service [1] (VPN users hereafter) and users in the organization but not belonging to the organization (guest users hereafter) access the servers, the proposed system allows servers to perform access control similarly by assigning different VLANs to them.

In the rest of the paper, we focus on site license of e-journal as an example of typical location dependent service since we have configured our campus network system for it. In Section 2, we explain a site license of an e-journal, a location free network and problems on configuring a location free network. Then, in Section 3, we describe the configuration method of the proposed location free network system in detail. In Section 4, we explain how to configure our network system according to the proposed method. Finally we show the summary and future works in Section 5.

2. Problems on Access to Location Dependent Services from the Location Free Network

2.1 Target Network Environment

In this paper, we assume the environment where a user belonging to the organization accesses e-journal content from various places in the organization or outside the organization with VPN service, and guest users in the organization also access e-journal content. The contract type of each e-journal is site license, and the terms and conditions vary with an e-journal. In other words, some of e-journals may be used only from the specific site and/or location.

An authentication server is operated in the organization, and a fixed VLAN-ID is assigned to each user or each MAC address of the terminal. By configuring a location free network using this authentication server, a terminal will be connected to the subnet of the same VLAN-ID even if a user connects his/her terminal at any location in the organization. When a terminal is connected to the network, a user and his/her terminal must be authenticated.

[1] Center for Information Technology and Management, Okayama University, Okayama 700–8530, Japan
[a)] y-oosumi@okayama-u.ac.jp
[b)] okayama@okayama-u.ac.jp
[c)] yamai@okayama-u.ac.jp

Then, if this authentication succeeds, an IP address is assigned to the terminal by a DHCP (Dynamic Host Configuration Protocol) [2] server, and the terminal will be connected to the subnet having the VLAN-ID specific to the user or the terminal. In this paper, we assume the authentication method is WEB authentication and/or MAC authentication, and method of dynamic VLAN is MAC address based VLAN, as used by popular L2 switches such as AX2400S manufactured by ALAXALA Networks, which is used in our university. In addition, the organization has two or more sites which are geographically separated regions such as campuses of a university, branches of a company, and so on. **Figure 1** shows the access to e-journals.

2.2 Site License of E-journal

An e-journal is an academic journal or an intellectual magazine that can be accessed via the Internet. When an organization makes a contract for an e-journal, it often prefers a site license. In such case, any users belonging to the specific department and/or in the specific site may access the e-journal contents freely, provided that the organization satisfies the terms and conditions. In order to satisfy the terms and conditions, the contracting organization has to provide a way to verify whether each user's access is authorized or not. As a verifying method of the authorized access, the client's IP address and/or user authentication are usually used. In the former method, the organization notifies the e-journal provider of the range of the IP addresses used in the site, and the e-journal server performs access control based on the client's IP address. On the other hand, in the latter method, the organization operates a proxy server with authentication, to perform access control and the e-journal server accepts only the requests from the proxy server. In recent years, Shibboleth [3] authentication is widely used as an alternative user authentication method. For example, some e-journals support GakuNin [4], the Academic Access Management Federation in Japan, to perform access control by means of Shibboleth [5]. With Shibboleth authentication, an authorized user can usually access the e-journal contents regardless of his/her location.

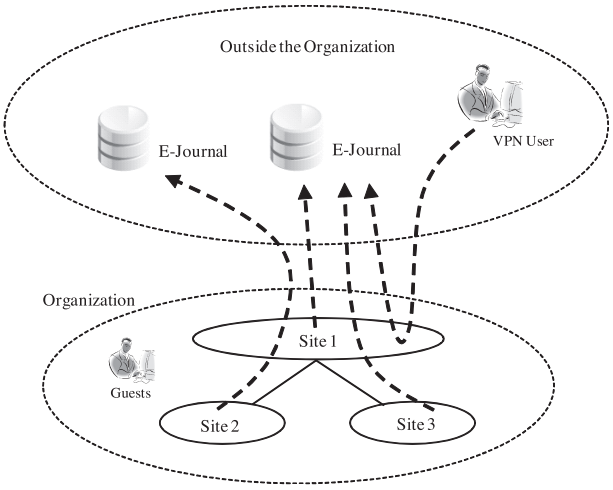

Fig. 1 Access to e-journals.

2.3 Location Free Network

In recent years, with the improvement of function and performance of network equipment, it has been able to authenticate terminals and users when a terminal is connected to the network. For the authentication method, several authentication methods are generally used, namely WEB authentication by a user name and password, MAC address authentication by the MAC address of the terminal, and IEEE802.1X authentication by EAP (Extended authentication protocol) [6]. With these authentication methods, not only the network can exclude the unauthorized user, but also it can connect the user's terminal to the specific VLAN based on the attribute of the user or the terminal by dynamic allocation of the VLAN (Dynamic VLAN). Such a network is called "location free network." Since a location free network allows a user to connect his/her terminal to the same network automatically wherever in the organization the user is, it has been used in many organizations recently.

2.4 Problems of Location Free Network

As described above, a location free network allows the user to connect to the same subnet from anywhere, but some problems occur due to the configuration of the network and the use of an e-journal.

2.4.1 Problems on the Configuration

The simplest method to construct a location free network is to configure each subnet by a single VLAN spanning over all sites of the organization. However, many organizations do not adopt this method for several reasons. One typical reason is the impact of possible broadcast storms spreading over all sites.

Another method is to configure a separate VLAN with the same VLAN-ID in each site, which has the same IP address range. Since each terminal must has a unique IP address, different VLANs with the same VLAN-ID have to be connected by a proxy server or a NAT (Network Address Translation) [7] system. In this method, the possible impact of broadcast storms would be reduced within a site. However, there are still other problems such as the cost for operating a proxy server or NAT system at each site.

Yet another method is to configure separate VLANs with a unique VLAN-ID in each site. This method also separates broadcast domains into sites. However, since this method requires additional data such as VLAN-IDs for each site and/or additional servers for authentication with such data, other problems would still exists in terms of administrative costs.

2.4.2 Problems of the Site License in Location Free Network

When an organization operating location free networks makes a contract for site license of an e-journal, some problems may arise. If a site license is contracted with geographical conditions, namely for only a part of the organization such as a specific site or a specific area, the organization has to provide a way to determine whether each user accesses the e-journal from the specific site or area, in order to guarantee the use condition of the site license. In addition, a method to distinguish VPN users from users in the site, and guest users from regular users is often required to guarantee the use condition. Since many e-journal servers perform access control based on clients' IP address, this method should

determine the location or the affiliation of a user base on the IP address.

Note that Shibboleth authentication cannot solve the above problems since an authorized user can usually access the e-journal contents regardless of his/her location, as mentioned in Section 2.2.

3. A Location Free Network System Applicable to Location Dependent Services

As mentioned in the previous section, if a location free network is configured using a conventional method, some problems occur when using location dependent services such as the kind of site license of the e-journal. Therefore, a new configuration method of a location free network applicable to location dependent services is required. In addition, it should be applicable flexibly to various network topologies and various requirements.

In this section, we propose a configuration method of a location free network system to solve these problems by introducing a new allocation method of the subnet for a VLAN-ID. We explain the details of the proposed method below.

3.1 Allocation Policy of the Subnet for a VLAN-ID after Authentication

The main factor of the problem described in Section 2.4 is that the mapping from a VLAN-ID to the corresponding subnet IP address range is fixed. In other words, when a VLAN-ID is determined according to the result of authentication, an IP address of the same subnet IP address range is assigned to the user's terminal regardless of the user's location and hence it is impossible for servers to verify the client's location by the client's IP address.

To solve this problem, we propose a method that assigns to the user's terminal an appropriate subnet corresponding to the user's location even if the user's information such as his/her VLAN-ID is the same in every site. Since this method uses different IP addresses for the subnets with the same VLAN-ID according to user's location, it can adapt to location dependent services such as some site license of an e-journal with geographical conditions. Furthermore, since this method does not require additional data or servers, it can be implemented with low cost.

3.2 Connection between Sites via L3 Switches with VRF Function

Recently, many organizations have introduced routers or layer 3 (L3) switches with Virtual Routing and Forwarding (VRF) function [8] to separate groups of subnets called VRF domains logically by security and policy reasons. By using VRF function, several virtual routers called VRF instances co-exist within a single router or L3 switch simultaneously. Hereafter, we use "L3 switch" as a general term for router and L3 switch for simplicity.

When two sites in the organization are connected by L3 switches with VRF function, we can configure the network to assign a different subnet with the same VLAN-ID in each site, as shown in **Fig. 2**. In this figure, there are two VRF instances, "General Network" and "Location Free Network," in each L3 switch, and each VRF instance in Site 1 is connected to its peer VRF instance in Site 2 via a separate VLAN. In this configuration, each L3 switch can use a different subnet for the same VLAN-ID since VLANs of these sites with the same VLAN-ID are separated. Consequently, a server of a location dependent service can verify the client's location by the client's IP address. For example in Fig. 2, if the client's IP address is in a.b.X.0/24 and a.b.W.0/24, the client's location is Site 1 and Site 2, respectively.

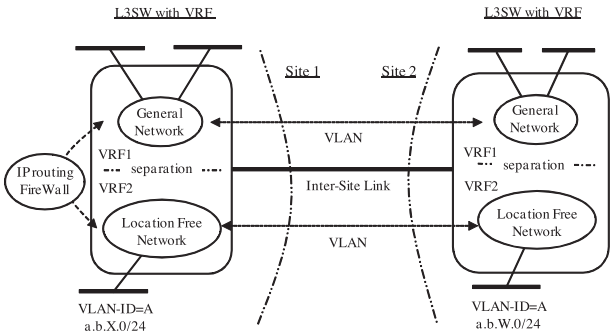

Fig. 2 Connection between sites via L3 switch with VRF function.

3.3 Connection between Sites via L2/L3 Switches with VLAN-ID Conversion

3.3.1 VLAN-ID Conversion between the Sites

We now consider the case where an L3 switch of a site, namely Site 2 in Fig. 2, does not have VRF function for some reason such as budget limit. In this case, it is difficult or troublesome to connect all VRF instances in Site 1 to the L3 switch in Site 2 since all VRF instances in Site 1 would be connected via the L3 switch in Site 2.

Instead of the above connections, we can configure the network to connect only one VRF instance in Site 1, for example "General Network" in Fig. 2, to the L3 switch in Site 2. In this case, all segments for other than General Network, for example the segment in Site 2 for "Location Free Network" in Fig. 2, would be connected directly to the corresponding VRF instances in Site 1 via separate VLANs. However, if a location free network is operated with this configuration, the VRF instance for the location free network cannot distinguish two segments in Sites 1 and 2 since they have the same VLAN-ID on the L3 switch in Site 1. Actually, the VRF instance deals with these two segments as a single subnet spanning over both sites. Consequently, servers for location dependent services cannot verify the client's location on this configuration.

In order to solve this problem, we propose a method that connects the segments in the sites without VRF function to the corresponding VRF instances with VLAN-ID conversion, as shown in **Fig. 3**. In this figure, the segment of VLAN-ID=A in Site 2 is connected to the VRF instance "Location Free Network" as the segment of VLAN-ID=B, which is different from the segment for location free network in Site 1. VLAN-ID conversion can be performed anywhere between the segment in Site 2 and the VRF instance in Site 1, provided that both VLAN-IDs are not used for other segments in the L2/L3 switches on this inter-site VLAN. If either L3 switches do not have such function, we can use a L2 switch as a VLAN-ID converter. Many kinds of L2 switches, for example those of Cisco Systems or ALAXALA Networks, have such a function.

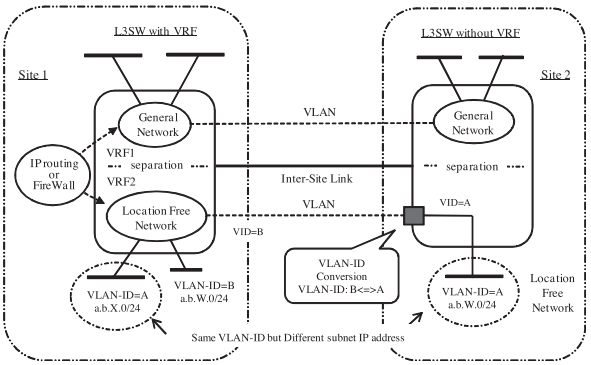

Fig. 3 Connection via L3 switch with VLAN-ID conversion.

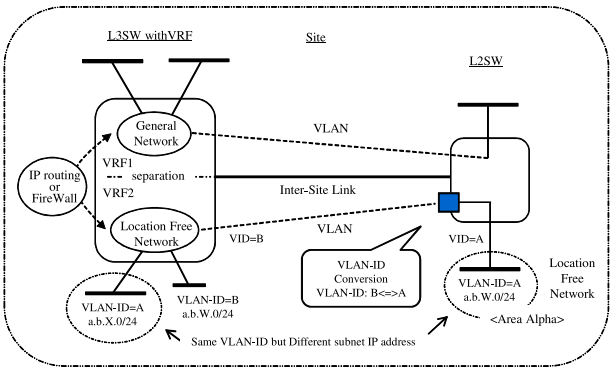

Fig. 4 Connection via L2 switch with VLAN-ID conversion.

3.3.2 VLAN-ID Conversion within the Site

When a location dependent service should verify a specific area within a site, it is necessary to distinguish the segments in the specific area from those in the other areas. For example, if a faculty or a department in a university makes a contract for a site license of an e-journal, the server might accept the request from only the users within the specific faculty or department.

In this situation, the VLAN-ID conversion technique is also applicable, as shown in **Fig. 4**. In this figure, the user's terminal is connected to the segment VLAN-ID=A anywhere in the site. If the user is in Area Alpha, his/her segment is eventually treated as VLAN-ID=B at the L3 switch and an address of a.b.W.0/24 is assigned to the user's terminal. Otherwise, the user's segment is VLAN-ID=A and an address of a.b.X.0/24 is assigned to the user's terminal.

3.4 Application to Location Dependent Services

Since the proposed method provides a way to identify the location of the terminal by its IP address, servers or network equipment such as firewalls used for location dependent services can perform access control over the user's access based on IP address. For example, we can introduce a site license of an e-journal with geographical conditions into a specific site, while users of the organization can connect their terminal to a location free network under the same policy from anywhere in the organization.

Since the proposed method is based on the dynamically assigned VLAN according to the user's attribute, it can be used along with any authentication method, such as WEB authentication, MAC address authentication and IEEE802.1X authentication. In addition, it can also deal with VPN users and guest users.

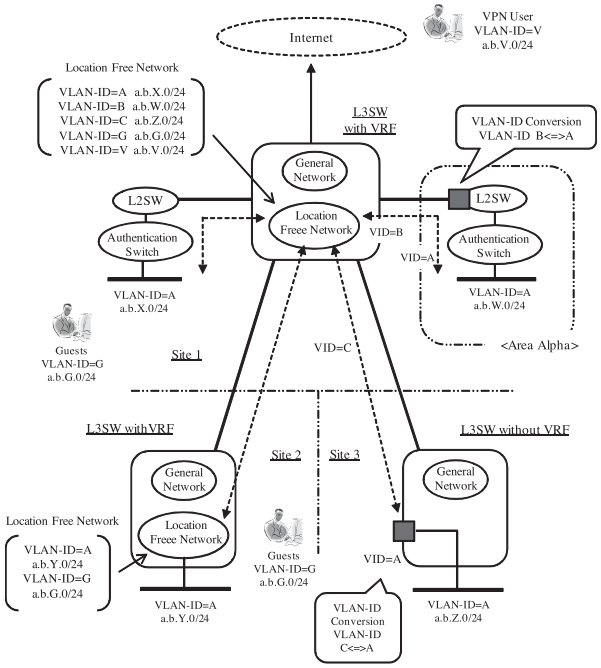

Fig. 5 Configuration of the proposed location free network system (global IP address environment).

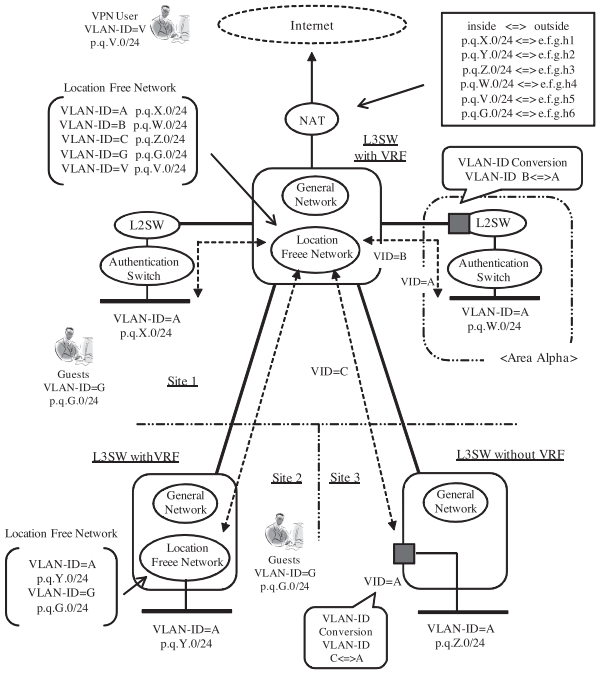

Fig. 6 Configuration of the proposed location free network system (private IP address environment).

If various attributes of authenticated user, such as his/her affiliation, position and so on are available, access control based on these attribute of the user can be performed flexibly.

3.5 System Configuration

In this section, we explain a sample configuration of a location free network system introducing the proposed method. The network system consists of a RADIUS [9] server, a DHCP server, L3 switches, (normal) L2 switches, L2 switches with authentication function (authentication switches), and an optional NAT router, as shown in **Figs. 5** and **6**.

The RADIUS server is used for user authentication. It has a VLAN-ID as a property value for each user as well as user's password. Authentication switches authenticate a user's terminal, cooperating with the RADIUS server. When a terminal is connected to an authentication switch, the switch performs user authentication by sending a request containing the user name and password to the RADIUS server. Then, the RADIUS server checks the user name and password, and responds to the authentication switch the result and the VLAN-ID. If this authentication succeeds, the authentication switch then connects the user's terminal to that VLAN according to the VLAN-ID in the response. Finally, the terminal obtains its IP address from the DHCP server.

There are three L3 switches in each figure. Those in Sites 1 and 2 have VRF function. However, the one in Site 3 does not have VRF function but have VLAN-ID conversion function. The table of subnet address ranges for VLANs in each L3 switch is shown in the figures. The segment VLAN-ID=A in Site 3 is connected to the VRF instance "Location Free Network" in Site 1 as VLAN-ID=C by VLAN-ID conversion at the L3 switch in Site 3. As for L2 switches, the one in Area Alpha has VLAN-ID conversion function, by which it connects its segment VLAN-ID=A to the VRF instances to the L3 switch in Site 1 as VLAN-ID=B.

If private IP addresses are used in the network of the organization, a NAT system is required to access the Internet. The NAT system translates a private IP address into the corresponding global IP address according to sender's IP address.

There are three kinds of users, regular users, guest users and VPN users, which correspond to VLAN-ID of A, G and V, respectively. Note that we omit the VPN server in Figs. 5 and 6 for simplicity and assume all VPN users are connected to the designated subnet of VLAN-ID=V regardless of their attribute. We also assume users other than regular users do not use location dependent services in this sample configuration for simplicity. However, it is easy to relax this restriction by applying the same method as for regular users.

3.6 Procedure of Connecting User's Terminal to the System

3.6.1 Access Restriction Assumption

We assume that the organization makes contracts for four e-journals K, L, M and N with the following conditions. As a common condition for all e-journals, they are available to only the users belonging to the organization but not guest users. In addition, the e-journal K can be used from all sites in the organization and from outside via VPN service. The rest of e-journals L, M and N can be used only from Site 1, Site 2, and Area Alpha in Site 1, respectively. These restrictions are summarized in **Tables 1** and **2**.

The administrator of the network then asks the providers of these e-journals to perform access control according to Table 1 or 2.

3.6.2 System Behavior on Global IP Address Environment

Figure 5 shows the configuration for global IP address environment. In this figure, we consider that a user connects his/her terminal to the network via one of authentication switches or the VPN server. The user's terminal is connected to an appropriate subnet by the following steps:

Table 1 Example of access control to e-journals (global IP address environment).

User type and location (IP address range)	Access to e-journals			
	K	L	M	N
Regular users in Site 1 other than Area Alpha (a.b.X.0/24)	OK	OK		
Regular users at Area Alpha in Site 1 (a.b.W.0/24)	OK	OK		OK
Regular users in Site 2 (a.b.Y.0/24)	OK		OK	
Regular users in Site 3 (a.b.Z.0/24)	OK			
VPN Users (a.b.V.0/24)	OK			
Guests (a.b.G.0/24)				

Table 2 Example of access control to e-journals (private IP address environment).

User type and location (IP address range)	Global IP address	Access to e-journals			
		K	L	M	N
Regular users in Site 1 other than Area Alpha (a.b.X.0/24)	e.f.g.h1	OK	OK		
Regular users at Area Alpha in Site 1 (a.b.W.0/24)	e.f.g.h4	OK	OK		OK
Regular users in Site 2 (a.b.Y.0/24)	e.f.g.h2	OK		OK	
Regular users in Site 3 (a.b.Z.0/24)	e.f.g.h3	OK			
VPN Users (a.b.V.0/24)	e.f.g.h5	OK			
Guests (a.b.G.0/24)	e.f.g.h6				

(1) The authentication switch or the VPN server authenticates the user in cooperation with the RADIUS server. If the authentication succeeds, the RADIUS server responds with the corresponding VLAN-ID as well as the authentication result. In this example, VLAN-ID is either A or G. Note that when the VPN server authenticates the user, it receives a VLAN-ID other than V, but the VPN server always uses V as VLAN-ID, as mentioned in Section 3.5.

(2) The authentication switch connects the terminal to the corresponding VLAN, A or G. The VPN server always connects the terminal to the designated VLAN V. The terminal now belongs to an appropriate subnet as follows:

- (a) If the user is a VPN user, the terminal belongs to the subnet a.b.V.0/24 since the VPN router has only this subnet for VLAN-ID=V, regardless of the user's attribute.
- (b) If the user is a guest user, the terminal belongs to the subnet a.b.G.0/24 since there exists only one subnet for VLAN-ID=G, which spans over all the sites.
- (c) If the user is a regular user in Site 1 but not at Area Alpha, the terminal belongs to the subnet a.b.X.0/24 since the VLAN-ID=A is directly connected to the VRF instance "Location Free Network" in Site 1.
- (d) If the user is a regular user in Site 2, the terminal belongs to the subnet a.b.Y.0/24 since the VLAN-ID=A is directly connected to the VRF instance "Location Free Network" in Site 2.
- (e) If the user is a regular user in Site 3, the terminal belongs to the subnet a.b.Z.0/24 since the segment of

VLAN-ID=A in Site 3 is connected with VLAN-ID conversion to the VRF instance "Location Free Network" in Site 1 as VLAN-ID=C.

(f) If the user is a regular user at Area Alpha in Site 1, the terminal belongs to the subnet a.b.W.0/24 since the segment of VLAN-ID=A in Area Alpha is connected with VLAN-ID conversion to the VRF instance "Location Free Network" in Site 1 as VLAN-ID=B.

The resulting subnets are summarized in the left column of Table 1.

After connected to the corresponding subnet, the terminal obtains an IP address available for the subnet from the DHCP server. Consequently, all e-journals can perform access control over the organization properly based on the IP address.

3.6.3 System Behavior on Private IP Address Environment

Figure 6 shows the configuration for private IP address environment. This figure is very similar to Fig. 5, but the address range for all subnets is changed from a.b.0.0/16 in the global address space to p.q.0.0/16 in the private address space. The system behavior in this environment is as same as that in global IP address environment. The user's terminal is connected to an appropriate subnet as shown in the left column of Table 2.

When the terminal accesses e-journal contents, its address in p.q.0.0/16 is translated to the corresponding global address in e.f.g.0/24, as shown in "Global IP address" column of Table 2. Consequently, all e-journals can perform access control over the organization properly based on the IP address even on this environment.

4. Implementation of the System

4.1 Outline of the System

We implemented a location free network system at Okayama University Campus Network System based on the proposed method described in the previous section. **Figure 7** shows the components of our implemented system. Some components have been redundantly implemented for high availability. The implemented system spans over six campuses. All inter-campus links except for the one between Tsushima and Misasa campuses are laid on Okayama Information Highway (OKIX) [10]. The inter-campus link between Tsushima and Misasa campuses goes through OKIX and Tottori Information Highway (TIH) [11].

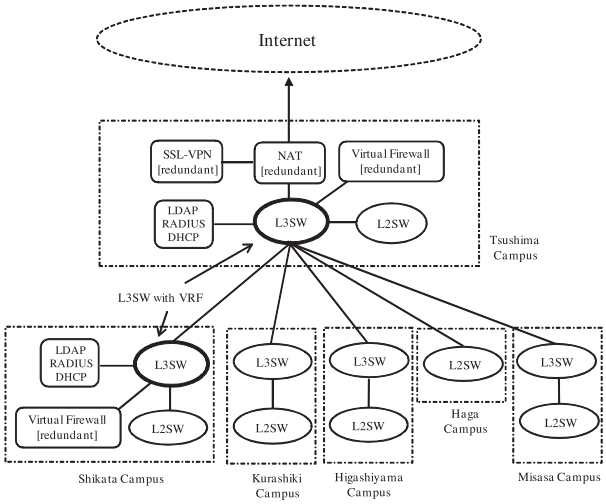

Fig. 7 The components of the implemented system.

Only the L3 switches in Tsushima and Shikata campuses are equipped with VRF function and each of them have a VRF instance for location free network. These two VRF instances are connected directly to each other via a VLAN on OKIX, and the VRF instance in Tsushima campus is connected to other VRF instances in the same switch via the virtual firewall system for security reason. The segments in Tsushima and Shikata campuses are connected directly to the VRF instance in the same campus. The segments for location free network on other campuses, namely Kurashiki, Higashiyama, Haga and Misasa campuses are connected to the VRF instance in Tsushima campus with VLAN-ID conversion. Since Haga campus does not have any L3 switch, the segment for location free network on this campus is connected by the method described in Section 3.3.2. On the L2/L3 switches in the campuses other than Tsushima campus, VLAN-ID conversion functions are configured by several "switchport vlan mapping" commands of ALAXALA Networks switches.

Note that the method of VLAN-ID conversion between a L3 switch and a L2 switch at the same campus is not being used at present since Okayama University does not have any site licenses valid only for a specific area.

4.2 Components of the System

4.2.1 Authentication Switches

AX2400S [12] switches manufactured by ALAXALA Networks are used for the floor switches and these are also used as the authentication switches.

4.2.2 RADIUS Servers

FreeRADIUS [13] is used on RADIUS servers. These servers cooperate with LDAP [14] servers to process authentication request sent from authentication switches.

4.2.3 Authentication Servers

As authentication servers, LDAP servers of Okayama University Integrated Authentication System are used as are since all members of Okayama University including all students are registered. A VLAN-ID is registered as an attribute of each user in these servers and is used for authentication.

4.2.4 NAT System

Since all subnets for location free networks except for those for VPN users are operated in private IP address space, NAT systems are required. Some appliances with NAT function are introduced for the NAT system.

According to the configuration described in Section 4.3, these equipments perform network address translation between the private addresses of the following kinds of location free networks to the corresponding global IP addresses.

- The one for teachers and staff in each campus
- The one for students in each campus
- The one for guest users commonly used for all campuses except for Shikata campus
- The one for guest users in Shikata campus

4.2.5 SSL-VPN System

Some dedicated SSL-VPN appliances are introduced for the SSL-VPN system. Two designated subnets in global IP address

space, one for teachers and staff, and the other for students are allocated for VPN users. The SSL-VPN system connects the user's terminal to one of these subnets according to the user's type but the user's VLAN-ID, returned by the RADIUS server.

4.2.6 Virtual Firewall System

Some dedicated firewall appliances with virtual firewall function are introduced. These appliances are used for monitoring traffic from the each kind of location free networks to campus network in global IP address space, as part of Unified Threat Management (UTM).

4.3 Operation of the Location Free Network System

In our location free network environment, each user has a VLAN-ID based on user type (teachers, staff, and students) and user's affiliation (faculty, department or institution), which is registered in Okayama University Integrated Authentication System. The subnet for each segment has an IP address range of netmask /22-/24, depending on the number of the users, in 10.0.0.0/8 private address space. For guest users, a subnet of /24 range in 10.0.0.0/8 private address space is allocated. For VPN users, two subnets of /24 range in 150.46.0.0/16 global address space are allocated. The numbers of VLAN-IDs for location free networks are 212 for teachers and staff, 164 for students, 73 for guest users, and 2 for VPN users.

We have configured this location free network system in Tsushima and Shikata campuses for users belonging to faculties in these two campuses and Kurashiki, Misasa, Higashiyama and Haga campuses. When a user of Kurashiki, Misasa, Higashiyama and Haga campuses connects his/her terminal to the location free network in his/her resident campus, the terminal is allocated to the subnet dedicated for the campus, which is connected to the VRF instance in Tsushima campus with VLAN-ID conversion. If the same user moves to Tsushima or Shikata campus, his/her terminal is connected to the different subnet with the VLAN-ID for this user. When the user accesses to outside Okayama University, the private IP address assigned to the user's terminal is translated into the corresponding global IP address by NAT system, according to its location. Thus it is possible for location dependent services to identify the user's location where the terminal is connected to the network even in the location free network system.

However, in Kurashiki, Misasa, Higashiyama and Haga campuses, we did not prepare subnets of the location free network for users residing in Tsushima and Shikata campuses. Instead, we prepare two common subnets, one for all teachers and staff and the other for all students regardless of their affiliation. In Kurashiki, Misasa, Higashiyama and Haga campuses, Users residing in Tsushima and Shikata campuses connect his/her terminal by specifying the corresponding common subnet.

We have adopted this configuration by the following reasons. If we would prepare all subnets, the proposed method would consume 449 (=212+164+73) VLAN-IDs for each campus. Thus the total number of required VLAN-IDs in Tsushima campuses would be as many as 2245 (=449*5) VLAN-IDs for the location free network. In addition, if we would have more sites or areas for a location dependent service in future, we would consume additional 449 VLAN-IDs for each site or area. Consequently we preferred the current configuration to that of a full location free network.

Note that the number of required VLAN-IDs can be reduced by assigning a VLAN-ID to each user based on only user type, for example. However, since we had already assigned it based on user type and user's affiliation before we introduced the location free network, we did not re-assign VLAN-IDs.

4.4 Application to Access Control for E-journals

Before we introduced the location free network, some e-journals contracted by Okayama University library had been performed access restriction limited to a specific range of global IP addresses, which was used fixedly in the specific campus. When we started the location free network service, we notified the e-journal providers of global IP addresses translated to by the NAT system, as described in Section 4.2.4. These global IP addresses were set to e-journal servers to perform access control according to the terms and conditions of site licenses.

The providers and we checked if the servers performed access control correctly by accessing the servers from each campus and the outside of our university via VPN, including accessing by a guest user. Consequently, we confirmed the access control on the servers worked correctly. The location free network has been working since May 2011. Currently, Okayama University Library has made contracts for about 6,500 e-journal services, about 500 of which are site licensed with geographical conditions.

Thus we can say that the proposed method can configure a location free network system applicable to location dependent services.

5. Conclusion

In this paper, we proposed a location free network system applicable to location dependent services. It can be applied to various network topologies flexibly, by introducing inter-site VLANs with VLAN-ID conversion as well as inter-site VLANs between VRFs of different sites. We confirmed the effectiveness and the practicability by configuring the system on Okayama University Campus Network System and applying the system to some e-journals.

Since we provide many VLANs based user's attribute such as user's type and affiliation, this system can be applied to services limited to specific faculty members in the specific site, for example. Thus we would like to verify the system by applying to such services as a further work. In addition, as another future work, we would like to develop a method that reduces the number of VLANs since the proposed system uses too many VLANs to apply to the organization with many sites or areas.

References

[1] Anderson, L. and Madsen, T.: Provider Provisioned Virtual Private Network (VPN) Terminology, RFC 4026, IETF (2005).
[2] Droms, R.: Dynamic Host Configuration Protocol, RFC 2131, IETF (1997).
[3] Shibboleth consortium: Shibboleth — Home (online), available from ⟨http://shibboleth.net/⟩ (accessed 2013-01-21).
[4] National Institute of Informatics: Academic Access Management Federation GakuNin — Outline of GakuNin (online), available from

⟨http://www.gakunin.jp/docs/en/fed/about⟩ (accessed 2013-01-21).
[5] National Institute of Informatics: Academic Access Management Federation GakuNin — Participants (online), available from ⟨http://www.gakunin.jp/docs/en/fed/participants⟩ (accessed 2013-01-21).
[6] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H. (Eds.): Extensible Authentication Protocol (EAP), RFC 3748, IETF (2004).
[7] Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC 1631, IETF (1994).
[8] ALAXALA Networks Corporation: Virtualization: Network Partition (online), available from ⟨http://www.alaxala.com/en/solution/virtualization/index.html⟩ (accessed 2013-01-21).
[9] Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC 2865, IETF (2000).
[10] Okayama Prefectural Government: OKIX (in Japanese) (online), available from ⟨http://www.pref.okayama.jp/page/detail-8208.html⟩ (accessed 2013-01-21).
[11] Tottori Prefecture Agency: Tottori information highway (in Japanese) (online), available from ⟨http://www.pref.tottori.lg.jp/10012.htm⟩ (accessed 2013-01-21).
[12] ALAXALA Networks Corporation: AX2400S (in Japanese) (online), available from ⟨http://www.alaxala.com/jp/products/AX2400S/index.html⟩ (accessed 2013-01-21).
[13] The FreeRADIUS Server Project: FreeRADIUS: The world's most popular RADIUS Server (online), available from ⟨http://freeradius.org/⟩ (accessed 2013-01-21).
[14] Zeilenga, K. (Ed.): Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, RFC 4510, IETF (2006).

Yoshihiro Ohsumi received his B.E. in science and engineering from Kinki University, Japan, in 1983. From April 1992, he joined the Computer Center (at present, Center for Information Technology and Management), Okayama University, as a technical official. His research interests include distributed systems, network architecture and the Internet. He is currently in Okayama University graduate school of natural science and technology (Doctor's Course).

Kiyohiko Okayama received his B.S., M.S. and Ph.D. degrees in information and computer sciences from Osaka University, Japan, in 1990, 1992 and 2001, respectively. After he has worked in the Department of Information System at Osaka University and in the Graduate School of Information Science at Nara Institute of Science and Technology as a research associate, he joined the Department of Communication Network Engineering at Okayama University in 2000. From 2005 to 2011, he joined the Information Technology Center at Okayama University. Since 2011, he has been an associate professor in Center for Information Technology and Management at Okayama University. His research interests include network design and network security. He is a member of IEICE.

Nariyoshi Yamai received his B.E. and M.E. degrees in electronic engineering and his Ph.D. degree in information and computer science from Osaka University, Osaka, Japan, in 1984, 1986 and 1993, respectively. In April 1988, he joined the Department of Information Engineering, Nara National College of Technology, as a Research Associate. From April 1990 to March 1994, he was an Assistant Professor in the same department. In April 1994, he joined the Education Center for Information Processing, Osaka University, as a Research Associate. In April 1995, he joined the Computation Center, Osaka University, as an Assistant Professor. From November 1997 to March 2006, he joined the Computer Center, Okayama University, as an Associate Professor. Since April 2006, he has been a Professor in Information Technology Center (at present, Center for Information Technology and Management), Okayama University. His research interests include distributed system, network architecture and the Internet. He is a member of IEICE and IEEE.