***Abstract— The general logical notion of Virtual Local Area Networks (VLAN’s) are to sectionalize a single network into many sub-networks by distinguishing user and devices. Due to this, VLAN’s forms an important concept in the field of network engineering. The application of VLAN’s are in network security, scalability and network management. VLAN’s main objective is to segregate a network by creating multiple broadcast domains. The other rapidly growing application of VLAN is in the field of campus networks. Traditionally IEEE802.1Q are used in campus wi-fi systems, but due to elaborate and complex system configuration in the former, OpenFlow is used as an alternate technology for simpler network design and configuration.***

I. **INTRODUCTION**

The emergence of VLAN technology has revolutionized the data management and data security of library network. Due to the digital conversion of library database, the development has also led to various problems. The one of the main problem of digitalization is the network management and other is to reduce the ever-growing complex nature of the database. In this case VLAN is the answer to all this problem. After the introduction of VLAN, the network have become more convenient and flexible in compare to traditional technology. One of the major advantage of switching to VLAN technology is the proper handling of broadcast storms by dividing network into small similar application networks. The database security and security of ethernet is also taken care by the VLAN. The other specific application is in campus network, IEEE802.1Q technology is used in various countries. In the existing technology, various logical VLAN’s are constructed over minimal optical or copper cables. But this increases the overall complexity of the network as there are many smaller groups as user-guest, user-students. This problems can be overcome with the introduction of the new technology known as OpenFlow technology. Openflow technology have already gathered attention from worldwide. With the help of Openflow, the overall logical VLAN’s can be limited and the security of the network can be improved to the larger extent. The OpenFlow does not need VLAN tag in the packet header, which is mandatory in IEEE802.1Q.

VLAN is a blooming technology which can form virtual areas by dividing a Local Area Network into different sections in a logical way rather than in a physical way .The increase in use of VLAN breaks many views of older networks by making the network more flexible and convenient .

**II. Application of VLAN**

1. *Reducing the broadcast storm in the network.*

The major limitation of bridge Is that it cannot remove broadcast storm. The data is transmitted to all devices if the device destination is unknown and due to this reason, the data get broadcasted and broadcast storms takes place. VLAN can minimize the broadcasts, the ports which are in broadcasting mode will not be affected by the storm of the other VLAN.VLAN decreases the occurrence of broadcast storm.

1. *To increase the network security*

In older Local Area Network any computer or host on network can easily track or download the data from the computers which are in the local area network and thus increasing the security risks. But if we divide the LAN into different small VLAN, the data stays within the VLAN and data exchange cannot take place directly within different VLAN.A single VLAN traffic doesn’t interfere with the traffic of other VLAN by introducing this mechanism in the network the security vulnerabilities are reduced to a certain extent and the intrusion of different traffic and unwanted users can be easily avoided by using this Mechanism.

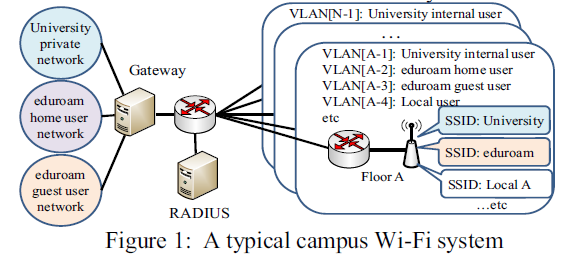
1. *Easy Management and defense of network*

In older IP networks, people who use to deal with network management used to spend a lot of time on network management and dealing the changes in the network. If in case a user needed a new IP address they had to revise the whole IP configuration and needed to revise the address of each station on the network. But after the introduction of VLAN if a workstation needed a new IP address we just have to assign a new port of a VLAN to a workstation and can be done with the few mouse operations. With the help of centralized management process of VLAN ,network managers can divide the network in to different small subnets, segregate different users and changing ports to VLAN , set up security grades providing restrictions to access and reducing the broadcast area region. All this functions effectively increase network performance by improving the controllability, flexibility and monitoring network management and thus reducing management costs.

**II. CAMPUS NETWORKS**

Use of VLANs is become popular in campus networks , Particularly campus Wi-fi networks such as eduroam require a large number of VLAN IDS when we want to separate and secure users communications. It is based on IEEE 802.1X and RADIUS proxies. The eduroam has been used worldwide this days.

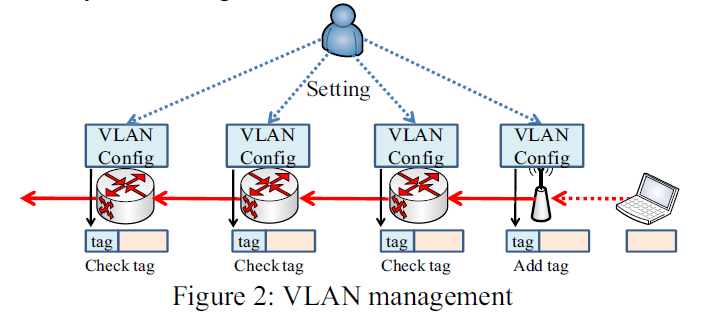
A roaming system including eduroam in campus networks has multiple access points . An Access point may contain multiple SSIDs such as for university Private network eduroam and Local Area Network. An individual VLAN id is allocated to each and every access point present in the campus networks. There might be few cases where multiple SSIDs may be given to a single access point.



**III. PROBLEMS IN CAMPUS NETWORKS**

Using a lot of VLANs has two major problems. The first problem is the limited number of VLAN IDs. The second problem is that system configuration work is laborious and more time consuming.

There is a VLAN check tag in the packet which indicates the information about the VLAN identification based on that the receiving port decides which VLAN it belongs to. There are types of VLAN identification Mechanism that are been used they are 802.1q and ISL Where ISL is a cisco proprietary .802.1q is a widely used protocol for VLAN identification because of less overhead .



1. *The number of VLAN*

The special field such as VLAN tag is necessary in the header of the packet because the ID field of VLAN tags is 12 bit long so it can only assign up to 4096 VLAN id where few of them are already being used for management and native VLAN purpose. Although there are few other ways to increase the number of VLAN by using different versions of 802.1q

1. *Network Management Cost*

In the VLAN based network VLAN , the nodes which are present at the end points they add a VLAN tag to the packet and the nodes which are there at the core end checks the VLAN tag information and based on that information it judges the forwarding port of the network. Each and every node needs to configured manually so they keep the VLAN information with them and can make forwarding decisions.

IV. **CAMPUS VLAN BASED ON OPENFLOW**

A flexible way of access management system for campus VLAN is mainly based on OpenFlow. The system here also depends on OpenFlow and enables easy configuration and the management of virtual networks without even using the special field called tag field in the packet.

1. ***OpenFlow***
2. *Architecture*

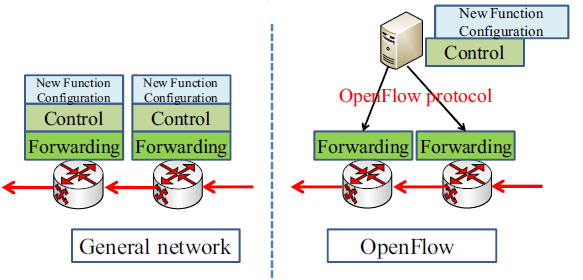
The architecture of Openflow mainly consists of many OpenFlow switches and one central controller server.

OpenFlow has a plane which deals with the data known as Data Forwarding Plane and the mechanism of forward in that is pretty much simpler in that. A forwarding entry in the switch is taken into account whenever the OpenFlow switch receives a packet. If the flow information is present in the forwarding data plane the packet is forwarded according to the forward entry. If in case, there is no forwarding entry in the packet then the packet is forwarded to the Openflow Controller.

An Integrated control plane Is present in the Openflow Controller. During the forwarding the packet from a switch OpenFlow controller switch decides the forwarding port of packet and writes the forwarding entry table with the help of OpenFlow Protocol. The OpenFlow protocol also performs tasks like path calculation, QOS control etc.

There is also one another feature present in the OpenFlow Controller switch for receiving the first packet of communication which is flow of OpenFlow.

1. *The Comparison with general network*

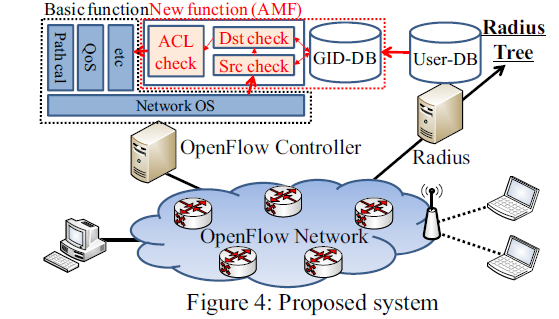
**

As shown in figure network systems like IP, optical transport and mobile network consists of two types of plane known as data plane and control plane. These nodes do not depend on each other and are loosely attached i.e. their control plane are isolated from each other and cannot communicate with each other. Therefore, classification information on the virtual network is notified to next network node by using VLAN tag. Each node needs to be configured independently.

On the other side of the image Openflow has data forwarding planes which are independent of each other and control plane which is integrated.By introducing open interfaces between data forwarding planes and the control plane .All nodes of Openflow network are affected by the mechanism of integrated control plane and it is different from the general network system.

*B.* ***The proposed access management system.***

*1) Basic Concept*

**

The above proposed system does management of virtual network groups which are similar to the older VLAN by utilizing the concept of OpenFlow. This can be achieved by introducing Access Management Function to Openflow with basic functions. AMF consists a database which stores Virtual Group Ids(GIDs), checking the source and destination addresses and also ACL check Function. GID and address such as MAC, IP and port are pairs of the record in GID DBs.

2). *Eduroam access network using OpenFlow*

As source of Address information in GID DBs,

various forms are possible in general. For example, static MAC/IP/port addresses list or dynamic IP address from DHCP and so on. In the case of eduroam, the source of Address information is User-DB of RADIUS server. UserDB of the RADIUS server is enhanced, so it can store GID(static information) and MAC (dynamic information) address besides user name (static information). For pre-configuration of GID DBs, three communications for RADIUS packet, reporting packet between RADIUS server and OpenFlow controller and DHCP packet are set to accept.

Step1. Authentication

Whenever an user tries to connects the network, the user node sends an EAP packets which is forwarded to an access Point. The Access Point sends RADIUS Access-Request packets including Calling Station ID (= user MACaddress) to RADIUS server. If the authentication succeeds, Calling Station ID is saved in User DB as MAC address

Step2. Reporting

After saving the MAC address the RADIUS server sends a report of things like MAC address and GID of the user ahead to OpenFlow Controller .Openflow Controller further saves this information in GID DBs . After this RADIUS server sends RADIUS packet to the Access Point.

Step3. DHCP

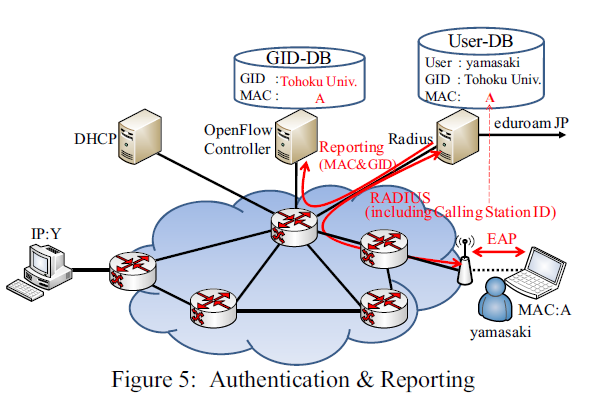
Initially the user doesn’t have any IP address immediately. Afterwards the user node sends DHCP request. This packet is forwarded to OpenFlow controller because it is the first packet of the communication. The AMF in the OpenFlow Controller accepts the communication because it has been set to be accepted .

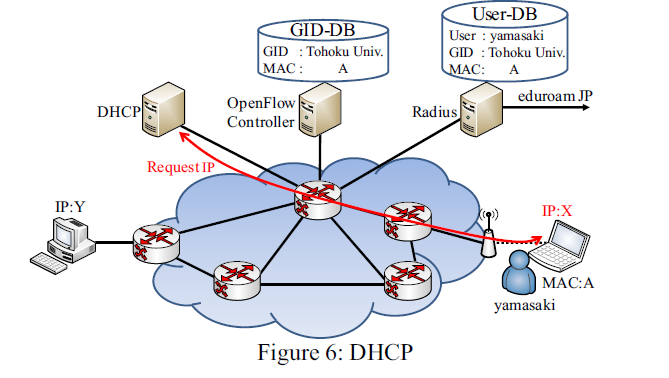
Step4. Access management

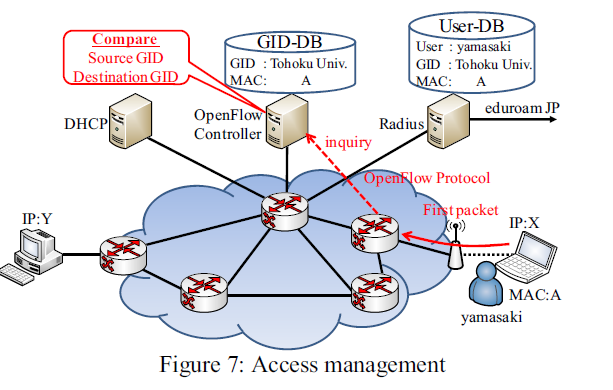
When traffic like HTTP, FTP is generated in the network an Openflow switch sends the first packet to OpenFlow Controller. Then AMF performs operations such as checking the Group IDs of Source and Destination address and based on the information acceptance or rejection is performed.

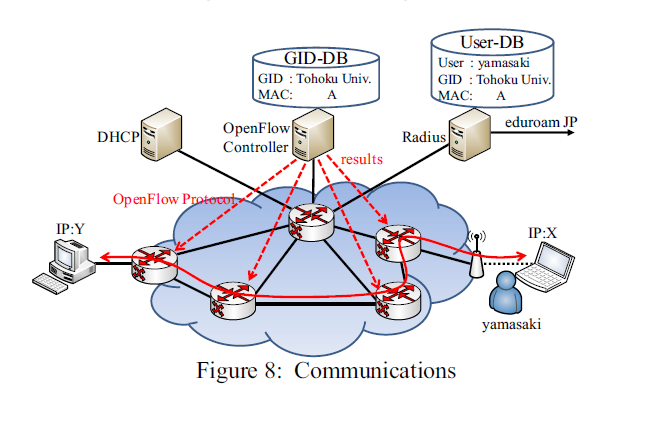
Step5. Communications

If the communication is accepted then basic functions like path calculation are executed. Then, next forwarding port is noted in the forwarding entry of each OpenFlow Switch in the communication.









**VII. CONCLUSION**

In this report, we are introducing a flexible way of access management which is based on a mechanism called OpenFlow. The overall communication is managed using Virtual Group IDs (GID) which is managed in a OpenFlow Controller. The restriction of ID is minimized and even on changing the GID the overall configuration of the switches are not needed to updated because the use of GID is only done in OpenFlow Controller.

In evaluation results of the system, we have shown the time for authentication and pings, data retrieval. Th e times for authentication and pings are about 10ms longer than basic OpenFlow controller. However, they are practicable times.

**REFERENCES**

[1]IEEE802.1Q,http://www.ieee802.org/1/pages/802.1Q.html.

[2] L.Florio, K. Wierenga, “Eduroam, providing mobility for roaming users,” EUNIS, June 2005.

[3] “AKARI”, <http://akari-project.nict.go.jp/>

[4] **“**Flexible Access Management System for Campus VLAN Based on OpenFlow” . Yasuhiro YAMASAKI\* Yoshinori MIYAMOTO\* Junichi YAMATO† Hideaki GOTO Hideaki SONE

Cyberscience Center, Tohoku University, Japan

[5] The Application of VLAN in College Library Network

Sun Litan Library Shandong University of Technology