Network Administration System for Bring Your Own Device(BYOD)
Over Software Defined Networking

By
GOOI HAO MING

A REPORT
SUBMITTED TO
Universiti Tunku Abdul Rahman
in partial fulfillment of the requirements
for the degree of
BACHELOR OF COMPUTER SCIENCE (HONS)
Faculty of Information and Communication Technology
(Perak Campus)

January 2017

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: _____

_____

_____

Academic Session: _____

I _____

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified By,

_____ _____

(Author's signature) (Supervisor's Signature)

Address:

_____

_____ _____

_____ Supervisor's name

Date: _____ Date: _____

Network Administration System for Bring Your Own Device(BYOD)
Over Software Defined Networking

By
GOOI HAO MING

A REPORT
SUBMITTED TO
Universiti Tunku Abdul Rahman
in partial fulfillment of the requirements
for the degree of
BACHELOR OF COMPUTER SCIENCE (HONS)
Faculty of Information and Communication Technology
(Perak Campus)

January 2017

DECLARATION OF ORIGINALITY

I declare that this report entitled "Network Administration System for BYOD over SDN" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : _____

Name : _____

Date : _____

ACKNOLEDGEMENTS

I would like to thank my supervisor, Dr Liew Soung Yue who always give me advice and guide me during the Final Year Project. Since the Software Define Networking(SDN) is still a new topic, without Dr Liew help and encouragement I may not able to handle this project.

Lastly, I would like to thank all the people who help and give me advice while I taking this project.

ABSTRACT

Nowadays, the technology is growing fast, Internet is one of the example. There are many services that provided through the Internet such as cloud service and server virtualisation. User don't have to purchase the powerful machine to support this kind of services but need to purchase more on the bandwidth. The services that provided no longer a simple service like e-mail service or web service. In order to use the cloud services, user require a good bandwidth to support it. In the other hand, the increasing of people using the Internet also one of the issue that cause the lack of bandwidth. To solve this problem, the current network equipment and network architecture need to be upgrade.

In this report, we will propose a new application implement on a new network architecture that will significantly increase the network performance. In order to achieve the goal, the Software Defined Networking(SDN) will be implement and a SDN application will develop to use in the SDN. There are two important point of SDN that need to be highlighted which is the network traffic can be directly programmable and it is vendor independent. By using this technology, we can ensure that the network resources can be manage in more efficient way.

The final outcome out this project is to develop an application for the software defined networking to increase the performance and the stability of the network.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

SDN	Software Defined Networking
VLAN	Virtual Local Area Network
QoS	Quality of Service
HP	Hewlett-Packard
MAC Address	Media Access Control Address
GUI	Graphical User Interface
ACL	Access Control List
NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocols
SSH	Secure Shell
HTTP	Hypertext Transfer Protocols
TCP	Transmission Control Protocol
REST	Representational State Transfer
SOAP	Simple Object Access Protocols
XML	eXtensible Markup Language
RPC	Remote Procedure Call
JSON	JavaScript Object Notation
SSL	Secure Socket Layer
ONOS	Open Network Operating System
API	Application Program Interface
CSS	Cascading Style Sheet
IP	Internet Protocols
URL	Uniform Resource Locator
PC	Personal Computer
UTAR	Universiti Tunku Abdul Rahman
Kbps	Kilobits per Second
Mbps	Megabits per Second

1.0 Introduction

1.1 Introduction to Traditional Networking

Now a day, Internet has become a part of our life. People use the Internet to finish their job or task like searching some material or performing some important transaction. The network had become more congest due to the services provided over the internet that require more bandwidth like cloud service or server virtualization. This kind of situation may not be able to handle by the current network equipment. In order to provide the more reliable and high quality of service of the network, the current network environment need to be upgraded. This issue has serious impact on the area of education such as the university area or the campus area. There are many student or researcher in the university, they need to search for the material through the internet in order to help them finish their project or research. As a network administrator it is very hard to manage the network resource and allocate it under the traditional network environment. The traditional network need to spend more man power and time to manage.

Open Networking Foundation White Paper (2012, p.3) stated that the existing network are hierarchical. The network was built with tiers of Ethernet switches arranged in a tree structure. This kind of architecture is so call a static architecture and is enough for the client-server computing. However, we need a dynamic architecture to meet our needs. According to Open Networking Foundation White Paper (2012, p.4) there some limitations of the traditional networking, which stated below.

1.1.1 Limitation of Traditional Networking

- Complexity

  Since the traditional network are hierarchical, different layer network device need to connect with each other to make the network can be function. When there is a new subnet add into the existing network, the network administrator need to configure all the configuration of each layer network device so that the new subnet can

communicate with the existing subnet or go to the internet. For example, the network administrator need to configure the IP route for the new subnet in the router in order to let the router able to route to the new subnet. If the new subnet need to divide into different VLANs, the VLAN configuration also need to be done in the switch.

- Inconsistent Policies

  To implement a network-wide policy, network administrator may need to configure thousands of device and mechanisms. The process of configure the policy consume much time and it is also very difficult to apply a consistent set of access, security and QoS.

- Vendor Dependence

  The traditional network built with different vendor network equipment at most of the time. Each of the vendor will have their own command to configure the network device like Cisco, HP, Huawei and more. It is very hard for the network administrator to memorize all the command for the network device come from different vendor.

1.2 Introduction of Software Defined Networking

Software defined networking is a new architecture for networking. It makes the network dynamic, manageable, cost-effective and dealing with the high-bandwidth. This architecture separates the network control and forwarding function to enable the network control becomes programmable and the underlying infrastructure to be abstracted for application and network services. In order to let the control plane communicate with the data plane, the OpenFlow protocol is used. According to the Open Networking Foundation (2013) there are some key points that need to highlight for the architecture.

The architecture makes the network programmable. It separates the network control from the forwarding function, so that we can write the program for the controller to control the network. Moreover, the architecture makes the network can be managed centrally. The network intelligence is centralized in software-based SDN controller that maintains the global view of the network, which appears to applications and policy engines as a single, logical switch. Besides that, the architecture is an open standards-based and vendor-neutral. The SDN switches are controlled by the SDN controller so that different vendor SDN switches also can communicate with each other.

Figure 1-2-F1 and 1-2-F2 show the traditional network architecture and Software Defined Networking architecture.

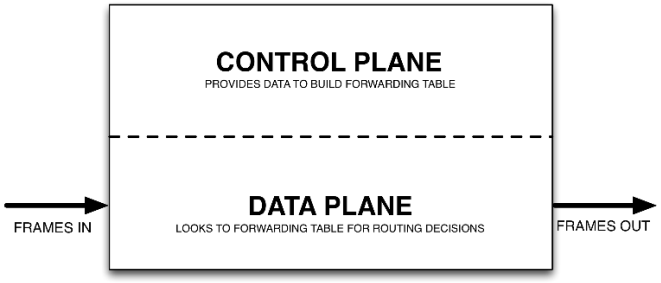


Figure 1-2-F1: Traditional Network architecture
(Software Defined Networking vs Traditional Networking 2013)

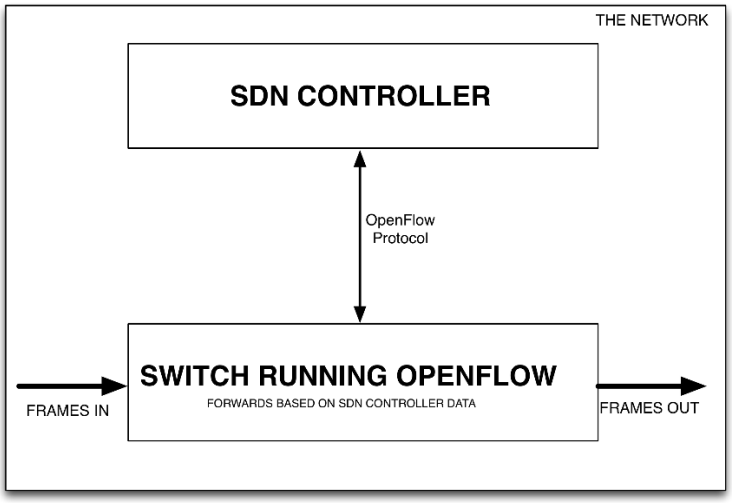


Figure 1-2-F2: Software Defined Networking Architecture
(Software Defined Networking vs Traditional Networking 2013)

1.2.1 Introduction of Openflow Protocols

OpenFlow protocol is a standard communication interface defined between the control layer and forwarding function layer of the SDN architecture. The forwarding plane of network devices such as SDN switches can be direct access and manipulate by using the OpenFlow protocol. The concept of flow is use by OpenFlow to identify the network traffic. It based on some pre-defined rule that has been insert into the flow table to decide if the traffic need to forward or drop. The are some parameter that exist in the flow table which is source MAC address, destination MAC address, source IP address, destination IP address, action and etc. Figure 1-2-F3 show a simple flow table.

Flow Table comparable to an instruction set

MAC src	MAC dst	IP Src	IP Dst	TCP dport	...	Action	Count
*	10:20:.	*	*	*	*	port 1	250
*	*	*	5.6.7.8	*	*	port 2	300
*	*	*	*	25	*	drop	892
*	*	*	192.*	*	*	local	120
*	*	*	*	*	*	controller	11

Figure 1-2-F3: flow table(Open Network Foundation White Paper(2012,p.9))

1.2.2 Benefits of Software Defined Networking

According to Open Network Foundation White Paper(2012, p.11), there are some benefits by implementing the software defined networking which stated below.

- ✓ Centralized control of multi-vendor environments

  Since the OpenFlow protocol is the standard protocol it can be use on any network device that come form different vendor as long as the network device support the OpenFlow protocol. The network administrator can use the SDN management tool to manage the entire network.

- ✓ Reduce complexity through automation

  SDN offer a flexible network automation and management tools, which automate the task that need to done manually today. The management tools can help to reduce operational overhead and decrease network instability.

1.3 Project Scope and Objectives

1.3.1 Project Scope

The scope of this project is to develop a network administration system over the software defined networking for organization. The function of the system will mainly focus on network access control. According to the previous project, the application able to performs the access controls function but is only for the devices that hardcode inside the program. To overcome this kind of problem, this project required to support all the network device that connected to the SDN network no matter it is new connected or pre-register. Beside that, the system will also able to control the bandwidth by different user group. Moreover, this project will also provide a user friendly GUI to let the organization can manage the network easily. The target user is the network administrator of the organization.

1.3.2 Problem Statement

Nowadays, many of the organization are facing bandwidth issue. The bandwidth issue mainly came form the user consume much more bandwidth on non-productive activity such as watching video from internet like Youtube. Moreover, user downloaded too much files from the Internet may also cause the bandwidth issue. This problem may cause the productivity of the organization decrease. In order to solve this issue and increase the productivity of the organization, the access control and bandwidth control have become more important for the network admin to mange the network. By using access control, network admin able to restrict the user to access certain. By using bandwidth control, network admin able to limit the bandwidth for each user. Beside that, network administrator also need a user-friendly GUI for the ease of administering the network.

The existing solution that solves the problem is configuring the access control list(ACL) that in the router. The router not only performing the access control function, it also performing routing, NAT and sometimes also providing DHCP service. If router perform all this all the same time, the router will need to have more processing power and the efficiency of the router will decrease.

1.3.3 Project Objectives

The main objective of this project is to develop a network administration system for the SDN controller to control all the SDN based switched. The function of the system mainly focusses on the access control. The access control function can be divided into several parts which is normal access control, time-based access control and user-group access control.

The first sub-objective is to develop a bandwidth control function and add into the network administrator system. The bandwidth control function can limit user bandwidth based on the user group.

The second sub-objective is to build a database to store all the configuration information which is access control policy information, registered device information, and bandwidth control policy information. Moreover, the system will also provide a domain name database. The domain name database will store all the information like domain name, public IP address and subnet mask. The domain name database will be used when user create a new access control policy.

The third sub-objective is to develop a web-based user friendly GUI for the system. The network administrator can easily create

the access control policy, bandwidth control policy, register device and more by using the GUI.

2.0 Literature Review

2.1 Review on Just For Fun Network Management System

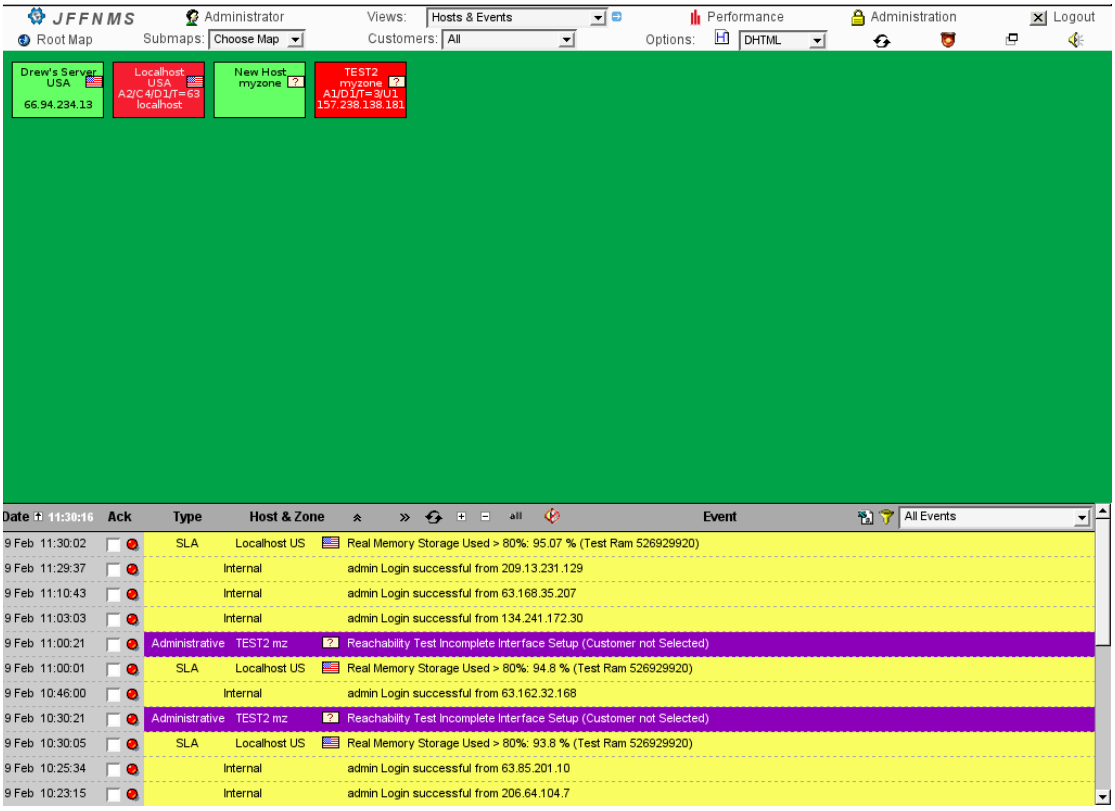


Figure 2-1-F1 Just for Fun Network Management System

Just for Fun Network Management System is a free software coded in php5 and is licensed under the GNU GPL version 2 or later. It can be run on every system that supports the PHP. The database used by this software is MySQL.

There are several strengths for this software. One of the strength is this software provide a Web GUI for the user which can access on everywhere. It works with SSH or HTTPS. The Web GUI also provides a graphical interface that showing the traffic, round trip time and packet loss monitoring.

Moreover, the network will auto discovery the interface or the host. This means that when there is a new device that connects to the network it will auto discover it and then updates to its database. This software is able to plot

out a graph that shows the performance for the particular interface. User also can configure the event type and the security level.

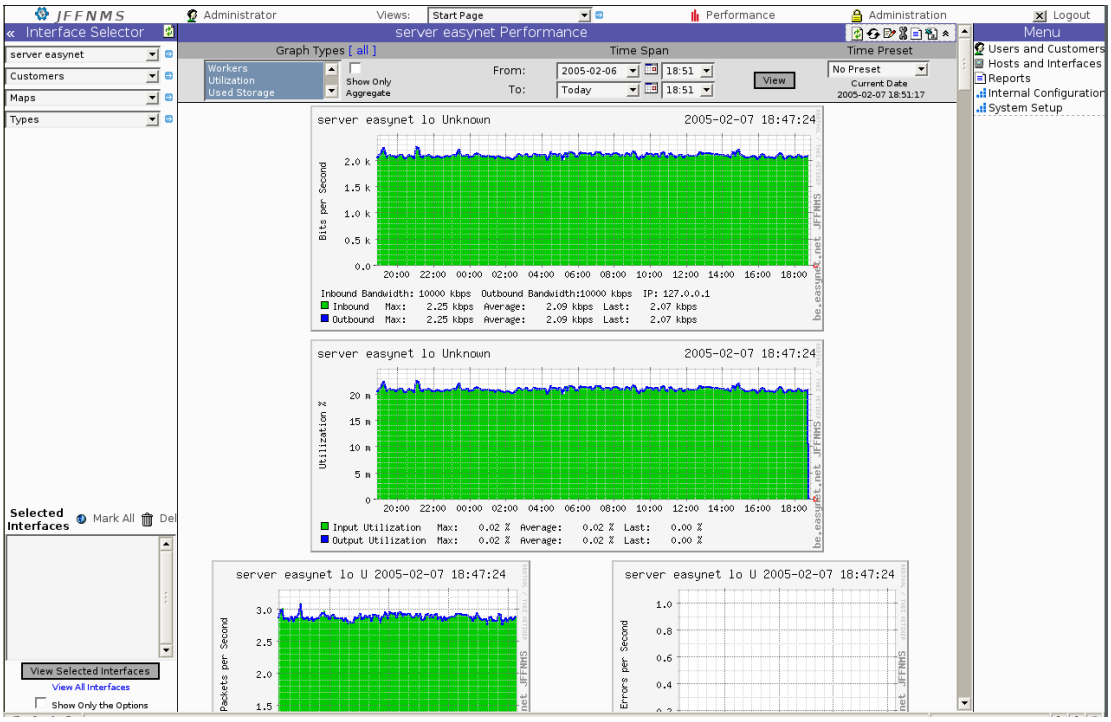


Figure 2-1-F2 Performance Graph for the selected interface

Besides that, this software supports Linux IPTables Firewall via custom net-snmp plugin. This kind of feature is for the firewall packets and traffic monitoring. Linux TC(traffic shapper) via custom net-snmp plugin for TC Class Graphing also support in this software.

Besides, this software enables to perform the nmap and TCP port discovery. This feature allow user to do the pot scan for the certain device.

In overall, this software includes many features that allow user can manage and monitor their network efficiency. The GUI provided allows the user do their configuration easily. However, there are some limitations found in this software.

First, this software does not allow to categories the host that are connected into the network. To over this limitation, a table that differentiate the user

level can be implemented in the database. According to this table, the software can perform the access control for different user level.

Second, this software is coded in PHP and use the MySQL as the database. Some of the system that does not support the PHP and MySQL may not able to use this software.

2.2 Review on Raisecom Network Management System: NView NNM

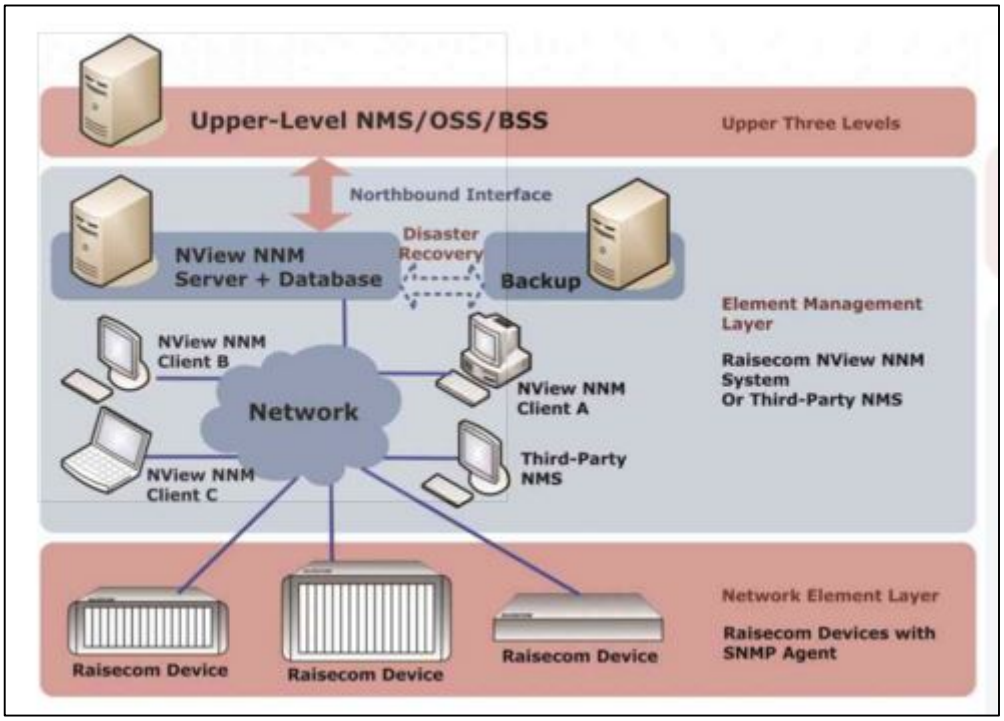


Figure 2-2-F1 TMN(Telecommunication Management Network) Architecture

Raisecom Network Management System NView NNM covers the two lowest layers of the TMN(Telecommunication Management Network) architecture which is element management layer and network element layer. According to Raisecom (2011) this software is based on the FCAPS model so that it includes the fault, configuration, performance and security management function.

Raisecom NView NNM is a client/server structure system. It allows several clients can work with only one server in order to achieve the efficient device monitoring and managing. This software integrates a uniform platform, consisting of topology, inventory, configuration, customer, fault, performance and security management components. The system also provides a disaster recovery solution. This will help to protecting the server from the fatal disaster. There is a backup server keeping synchronize with the main server to prevent any data lost.

There are some functions and features that need to highlight in this software. The first is topology management. The system is able to display all the graphical network element and links. The information that will be displayed is the port, card and device. User can figure out the network structure by this information.

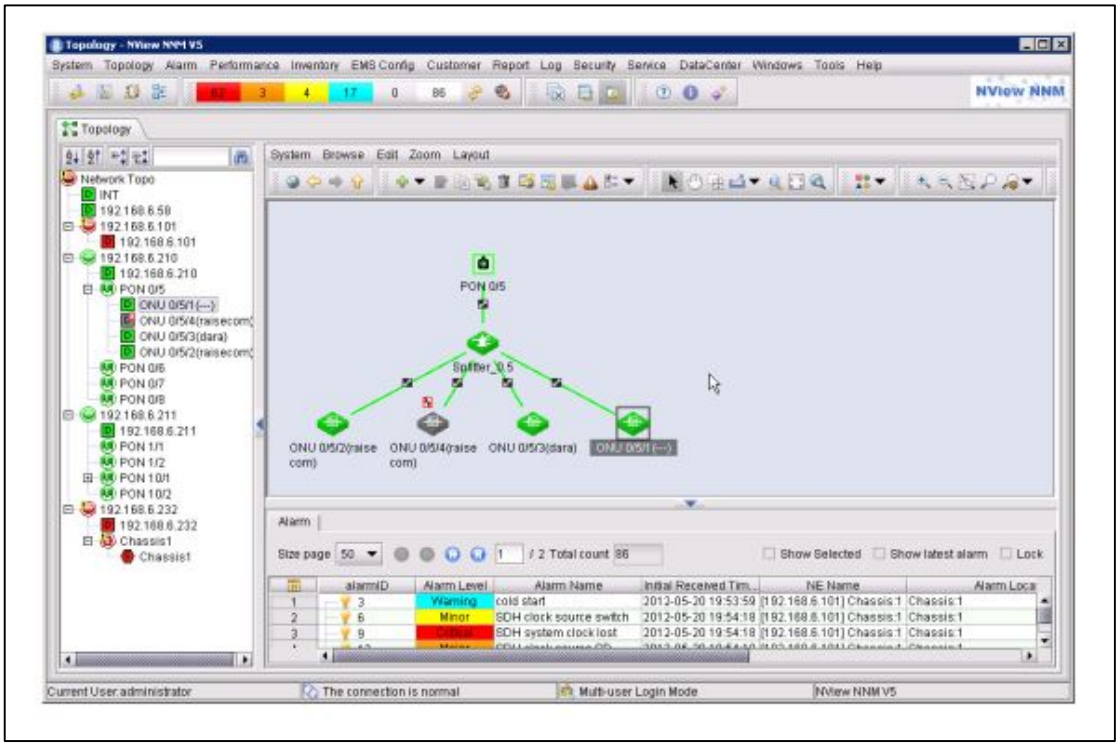


Figure 2-2-F2 Topology Management

The second management that need to highlight is the configuration management. The configuration can be distributed across the network. It is very easy to do the configuration for the particular device by just clicking the graphical icon that represents to the device.

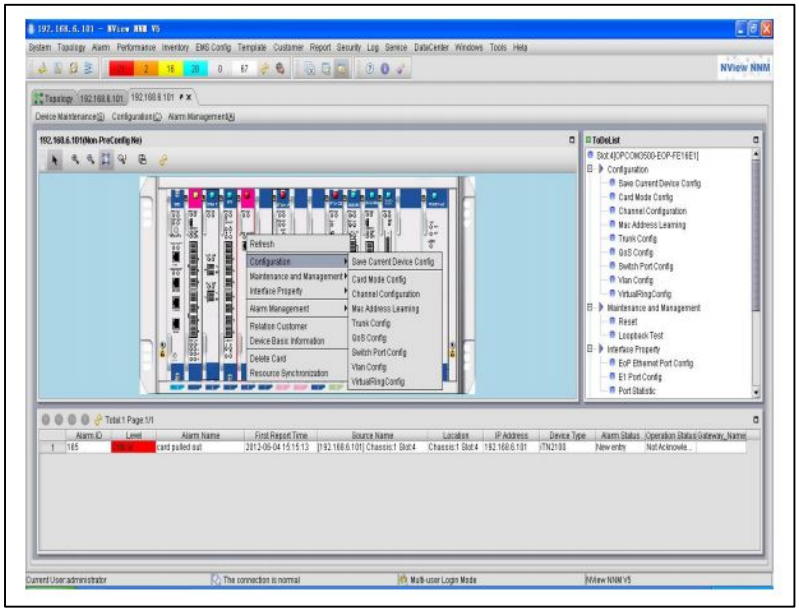


Figure 2-2-F3 Configuration Management

The third management needs to be highlighted is the security management. User can create some group to categorize all devices that connect to the network in the security management module. Only the user that has been authorized is able to login to the system.

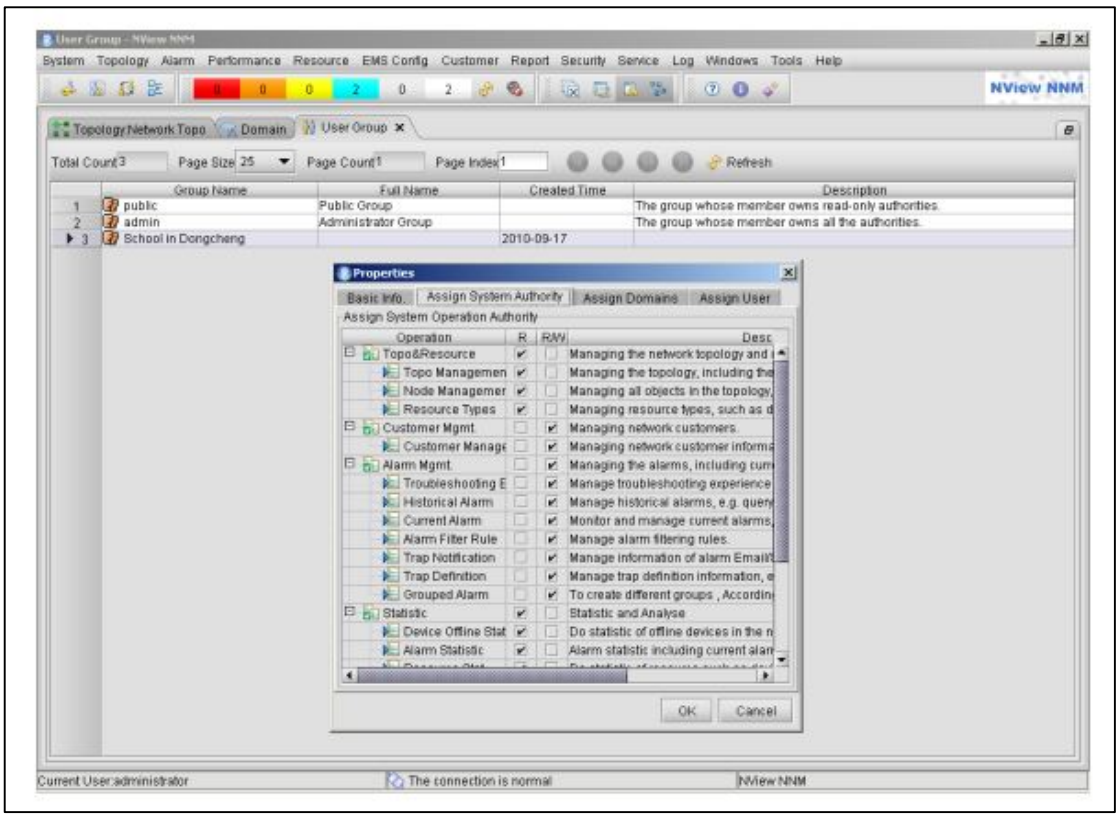


Figure 2-2-F4 Security Management

In overall, this software includes many features allowing user can manage and monitor their network efficiency. However there are some minor limitations in this software. This system is only supported by the Raisecom network device. For those who want to use this system they need to purchase the Raisecom network device.

To overcome the limitation, the SDN can be used in this situation. SDN is a standard for all the SDN enabling switched even there are different kinds of vendor switches.

2.3 Review on Representational State Transfer(REST) and Simple Object Access Protocols(SOAP)

2.3.1 Introduction to REST

REST is a standard based architecture for Web. It use HTTP protocols to perform the data communication. In this architecture, REST server can be simply access by the REST client and get the resource. Each resources is identify by a unique id which is a unique URL. REST resource can be represented in the different format such as text, JSON and XML. There are some common HTTP method that used in REST architecture which is stated below.

- ✓ GET – used to access and read the resource
- ✓ PUT – used to create a new resource
- ✓ DELETE – used to delete the resource
- ✓ POST – used to update existing resource

2.3.2 Introduction to SOAP

SOAP is a messaging protocol. It is use to exchanging information among computer over the HTTP protocol. SOAP message are written in XML format so that it can be run on any operating system as long as the system support XML. Basically, SOAP is used for making the remote procedure call(RPC) across the machine that is located in the network. There are some advantages of SOAP that stated below.

- Since the SOAP is posting the the message over HTTP protocol which the port number is 80, so it is able to past through the machine firewall easily.
- The data in SOAP is formatted in XML, so it is can be extend easily and run in various system.

2.3.3 Comparison Between REST and SOAP

There are some comparisons between REST and SOAP regarding data format, cache ability, data structure, message reliability and security. The comparison table shown below.

	REST	**SOAP**
Data Format	JSON,XML	XML
Cache Ability	Reads can be cache	Reads cannot be cache
Data Structure	Simple	More Complex
Message Reliability	Not Reliable	Provide end-to-end reliable
Security	SSL Support	SSL support, provides a standard implementation of data integrity and data privacy

Table 2-3-T1 REST and SOAP Comparison

Based on the table above, REST is chosen for this project. The data format that REST support are JSON and XML where SOAP only support XML, so that the data can be push into the switch in by using XML or JSON format depend on which format that prefer. Moreover, the data structure for REST is more simple where SOAP is more complex.

2.4 Review on Different SDN Controller

2.4.1 Overview on Open Daylight SDN Controller

Open Daylight SDN controller open source SDN platform for the SDN network of any size and scale. The controller enables the network service work under different vendor network device environment. There are some feature that need to highlighted for the Open Daylight Controller.

- ✓ Micro services architectures

  Open Daylight use model-driven approach to describe the network, the function and the resulting state. For the data structure, Open Daylight uses Yang Model to represent. It allows the services that had created to combine together with the other service to solve the problem. In the Model Driven Service Abstraction Layer(MD-SAL), then function can be combine or bundle into a service then the service will be install or load into the controller.

- ✓ Multiprotocol support

  Open Daylight support boarder set of protocols in any software defined networking platform which is the traditional and emerging. The multiprotocol support improve programmability of modern network and solve the user needs.

2.4.2 Overview on Open Network Operating System(ONOS) SDN Controller

According to Introducing ONOS Whitepaper (p.3), ONOS is the first open source SDN controller. The controller was targeted specifically at the mission critical networks and service provider. It provides the high availability, scale-out, and performance for the network. Moreover, the controller has created useful Northbound abstraction and APIs that allow user to develop the application for the controller easily.

According to Introducing ONOS Whitepaper (p.4), the architecture of the ONOS had provided some feature and stated below.

- ✓ Distributed core provides high availability, scalability and performance. The distributed core bring carrier grade feature to the SDN control plane.

- ✓ Northbound abstraction and APIs include network graph and application that make the network management task more easy such as network configuration and network monitor.

- ✓ Southbound abstraction enable pluggable southbound protocol for controlling the legacy device and OpenFlow enabled device.

- ✓ Software Modularity make the develop, maintain and debug more easy.

2.4.3 Comparison between Open Daylight Controller and ONOS SDN Controller

The table below had show some comparison between the Open Daylight Controller and ONOS controller.

	Open Daylight	**ONOS**
Legacy Network Interoperability	Yes	Partial
Service Insertion and Chaining	Yes	Partial
Network Monitor	Yes	Yes
Policy Enforcement	Yes	Partial
Load Balancing	Yes	No
Traffic Engineering	Yes	Partial
Dynamic Network Tap	Yes	No
Campus Network	Partial	No
Routing	Yes	Yes

Table 2-4-T1 Open Daylight and ONOS Comparison

Based on the table above, Open Daylight is more suitable to use as this project. Open Daylight able to perform the load balancing. The load balancing is very important to a campus network, because there are many user access to the campus network to do their own work. The network traffic will be very congested, so that the load balancing need to be perform. Moreover, Open Daylight is suitable to be use under the campus network where ONOS is not suitable for the campus network.

3.0 Methodology and Technology Involve

3.1 Method Involved

The methodology that we use for this project is rapid application development. Basically, rapid application development will use more time on development but less time on planning.

Dynamic system development method(DSDM) is a kind of agile software development. By using this methodology, we could fix the cost, quality and time, so that this project can be finish within the time constraint and meet the requirement.

3.2 Technology Involved

In this project we will develop a network administration system for the SDN controller named Web-based GUI SDN Application. The hardware we using in this project is HP switch 2920-24G which is a switch support OpenFlow protocol, Cisco Router with DHCP service and NAT enabled to provide the device IP address and enable the device to surf internet, a TP Link Wireless AP which enable mobile device connect to the network.

There is some software use that use to develop the application which is OpenDaylight, Apache, Postman, Mininet, Netbean, Ubuntu 14.04. The OpenDaylight is an open source SDN controller installed into a pc which running the Ubuntu 14.04. The Apache is installed in the pc and enable it to host the Web-based GUI SDN Application. Postman provide an environment that use to test to insert the flow into the switch by using REST. Mininet is a network simulation software that can generate a SDN network environment. Netbean is a IDE that use to develop the Web-based SDN Application.

3.2.1 Web-based GUI SDN Application

Web-based GUI SDN Application is a SDN Controller application and the application use the REST protocol to communicate with the SDN switch. This application will provide

access control function, device management, bandwidth control function and domain name database. This application is coded in various programming language. PHP language is the main language that used to develop this application. PHP enable us to communicate with the SDN switch by using the cURL extension. cURL provide the REST function so that we can use cURL to communicate with the switch. Moreover, XML will also be used in this project. The configuration of the flows will be formatted into XML form and push into the SDN switch in order to insert the flow.

Beside that, the system able to perform time-based access control function. This function is the combine used of PHP and Linux system scheduler which is CRONTAB to perform. CRONTAB will run the process when it reach the time that had set for the process. In order to let the application to perform CRONTAB, the SSH2 extension in PHP will be used.

Moreover, MySQL is chosen to be the DBMS (Database Management System) for the application. PHP will be used to connect to MySQL to retrieve data from the database. Beside that, HTML and CSS will also be use to develop the application in order to make the application more user friendly.

The IDE that used to develop the application are Netbean, XAMPP and Google Chrome. Netbean is used to code the program and compile the program. XAMPP is used to host the local server with MySQL database and show the PHP content. The web browser is used to display the GUI for the user.

3.2.2 Additional Hardware

- HP switch 2920-24G
- Cisco Route
- TP Link Wireless Access Point

The network structure show in figure 3-2-F1.

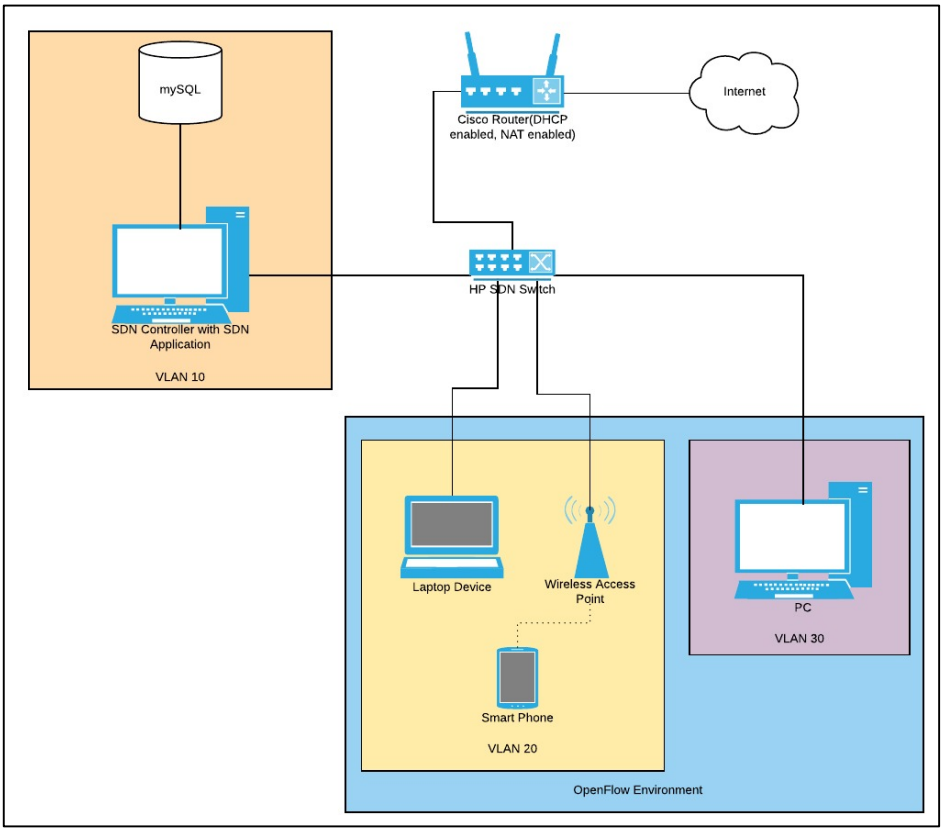
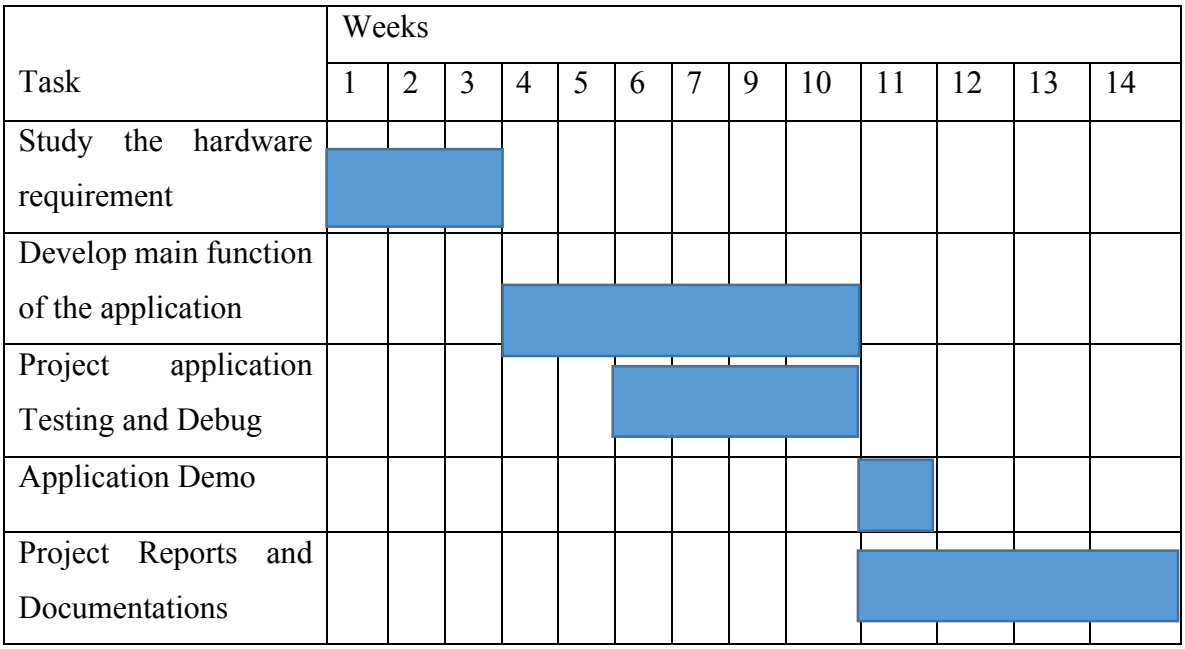


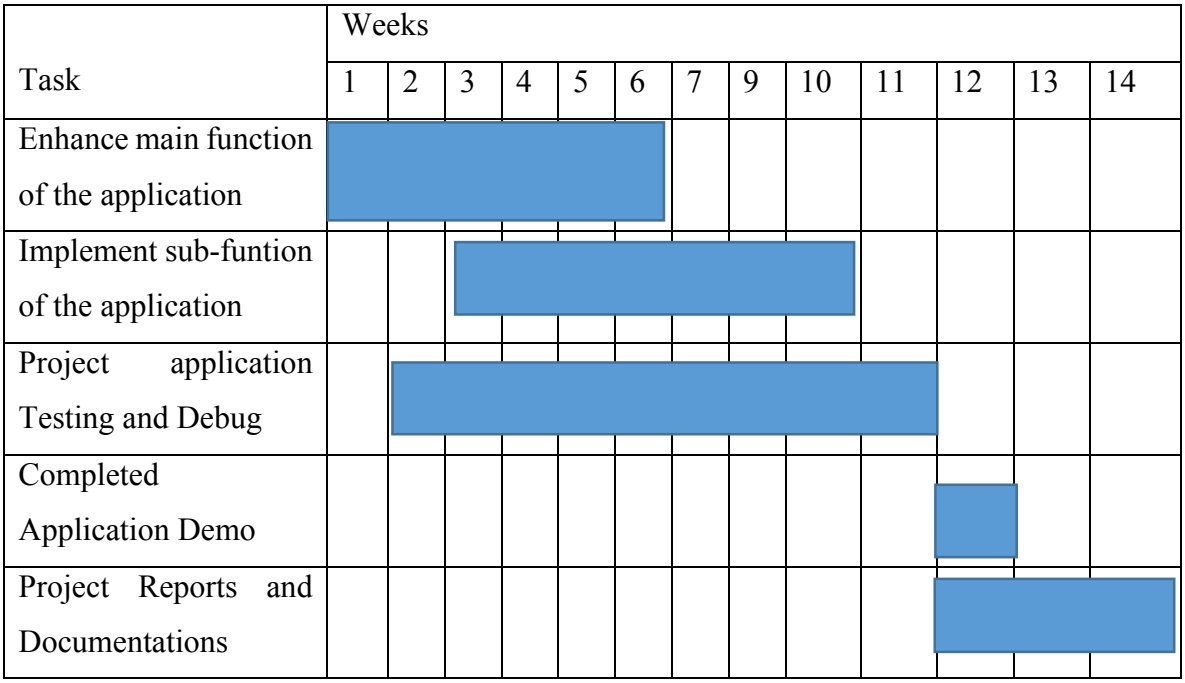
Figure 3-2-F1 Network Structure

3.3 Gantt Chart

3.3.1 FYP 1 Gantt Chart



3.3.2 FYP 2 Gantt Chart



4.0 System Design

4.1 System Architecture

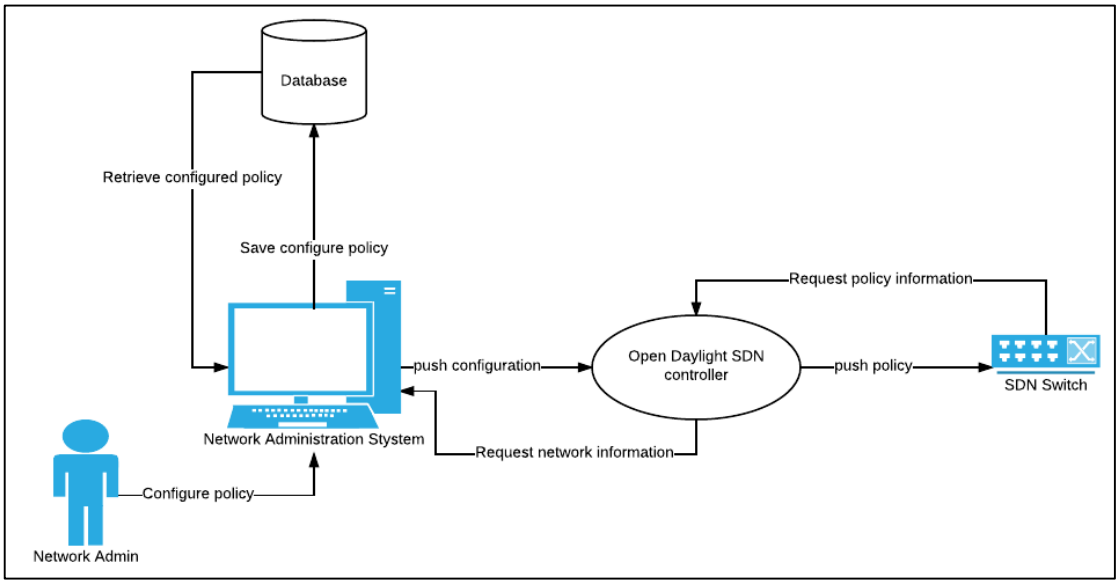


Figure 4-1-F1 Overall Framework of the System

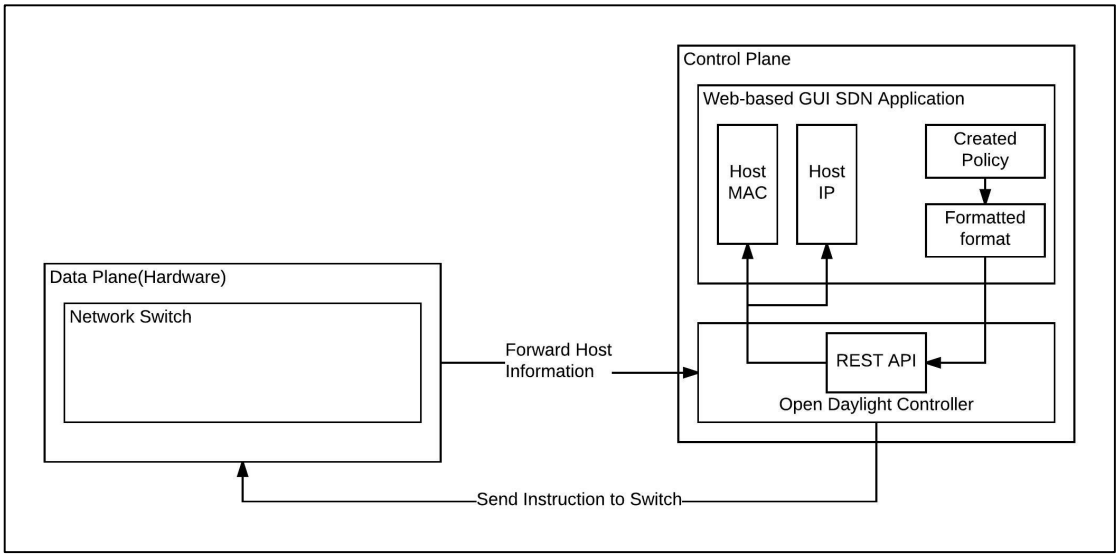


Figure 4-1-F2 System Architecture between web-based GUI SDN Application, controller and switch

Figure 4-1-F1 is the overall framework of the system. It includes the database, Open Daylight SDN Controller, HP SDN switch and Web-based SDN Application. Figure 4-1-F2 is the System Architecture between web-

based GUI SDN Application, controller and switch. It show how the data flow between these devices and application.

When network administrator created a new policy, the information of the policy will be save to database. After that, it will be formatted into XML format and send to the controller. The controller will push the policy to the SDN switch.

When the network administrator request for the host information, the SDN switch will send all the connected hosts to the controller. After that, the controller will send the host information like host mac address, host IP address to the application.

At the SDN switch, it can be divide into two scenarios which is recognized device connect to the network and unrecognized device connect to the network.

a) Recognized Device

   When there is a recognized device connect to the network, the SDN switch will check its flow table inside the switch and perform the task. The switch may forward the packet or may drop the packet based on the flow table.

b) Unrecognized Device

   By default, the SDN switch will drop all the packet sent from the unrecognized device. When there is a device connect to the network, the switch will first check the flow table. If the flow table does not have the device information it will drop all the packet sent by this device.

   The device must register at the network administrator side then the device only can connect to the network.

4.1.1 HP Switch OpenFlow Flow Table Architecture and Design

The OpenFlow protocols version used in this system is version 1.3. Compare to version 1.0, version 1.3 support meter and multiple table.

Meter feature has been used to implement the bandwidth control function in this system. Moreover, the multiple table feature also has been use in this table.

The purpose of using multiple table in this system is to increase the maximum flow entries in the SDN switch. Moreover, the other purpose of using multiple tables is to make the different policy manage by different table in order to make it easier to manage.

Based on the HP switch, the default tables enabled in the switch are start table, policy table and one software flow table. When the HP switch receive a packet it will first go into the start table. Normally, start table will not do any checking, it will directly go to policy table.

Policy table able match the following attribute which is, IPv4 source and destination, source MAC address and destination MAC address, VLAN ID and more. After done matching, it will apply the action such as drop, go to other table for further matching or forward the packet to the port desire. If there is no any matching in the policy table, the switch will go to the next table which is software flow table and look for matching. The software flow table is the last table in the HP switch, if still don't have any matching the switch will drop the packet. Figure 4-1-F3 shows the architecture regarding the flow table in the HP switch.

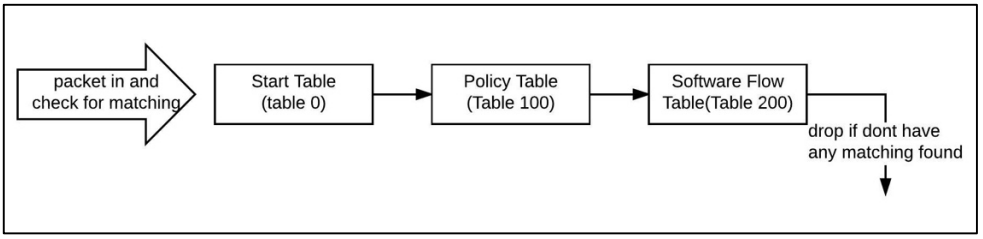


Figure 4-1-F3 HP Switch Flow Table Architecture

The action that mention above not only policy table can perform, software flow table also able to perform. But there is one action only can perform by policy table which is apply meter. Meter is a feature that allow to perform bandwidth control. In order to use meter, a flow is needed to create and attach with the meter. Since the Policy table is the only one table able to apply meter in a flow, so the flow that attach with meter need to create in this table.

In order to achieve the goal of this project, a new software flow table has been created. The total number of software flow table can be created in the HP switch is 4. The total number of table used in this project is which is, start table, policy table and two software flow table. Start table is not allowing to insert any flow, so all the flow insertion will be at the policy table and software flow table. The total flow entries can be insert into the policy table is 1000 where software flow table is 16000.

In this project, a flow table architecture has been designed based on the function provided in the system in order to achieve the goal of the project. The architecture shows in Figure 4-1-F4.

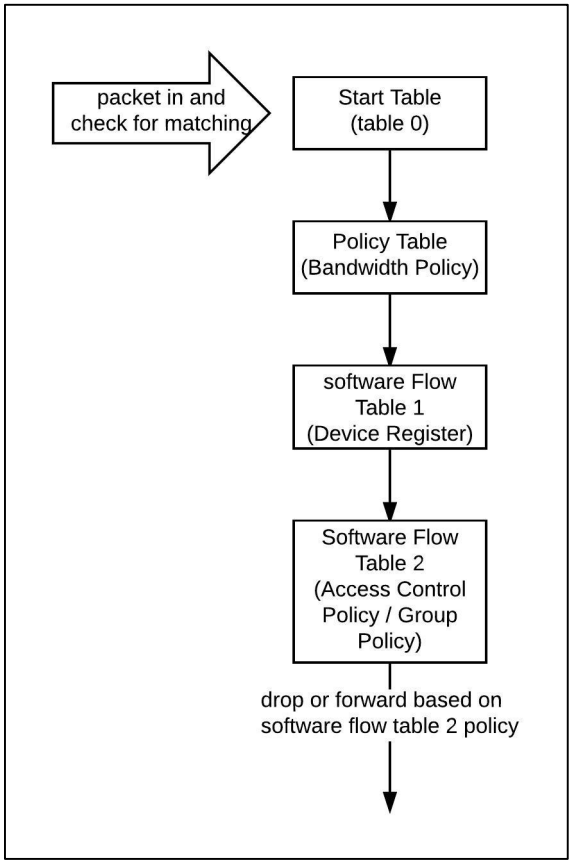


Figure 4-1-F4 Project Flow Table Architecture

The bandwidth policy entry will be inserted into the policy table, device registered entry will be inserted into the software flow table 1 and the access control policy or group policy will be inserted into the software flow table 2. By using this architecture, no only to make the policy can be easier to mange but also increase the number of entry of each policy. The software flow table 1 is responsible for device register entry, it allows up to 16000 devices to register in the system. Moreover, the software flow table 2 is responsible for access control policy and group policy, it allows up to 16000 entries of policy to be insert in the system. Beside that, the policy table is responsible for bandwidth policy, it allows up to 1000 bandwidth policy to be insert in the system.

4.2 Functional Modules of Web-based GUI SDN Application

❖ Admin Login

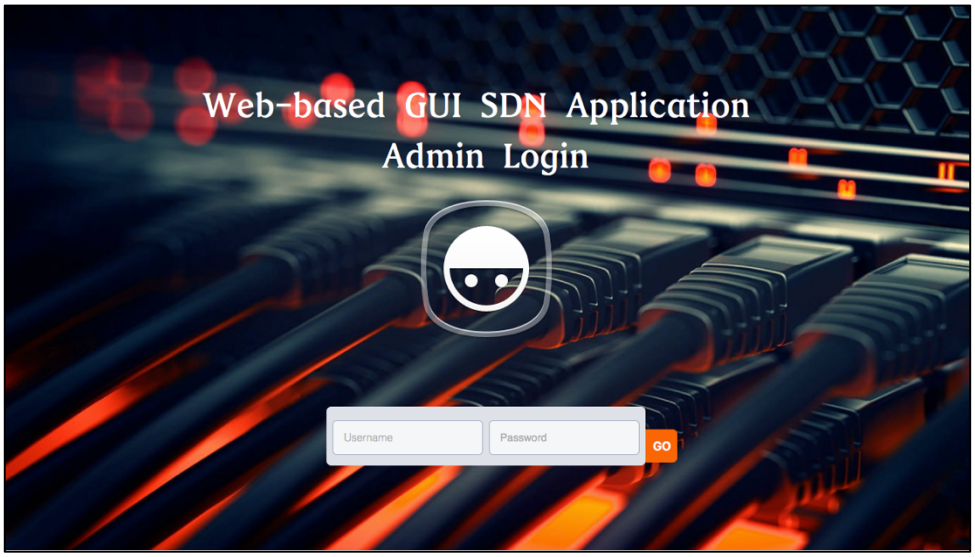


Figure 4-2-F1 Login Page

Figure 4-2-F1 is the login page for the system. Network administrator need to enter the username and password in order to login into the system.

❖ Logout

The logout function is to allow the admin to logout from the system.

❖ Dashboard

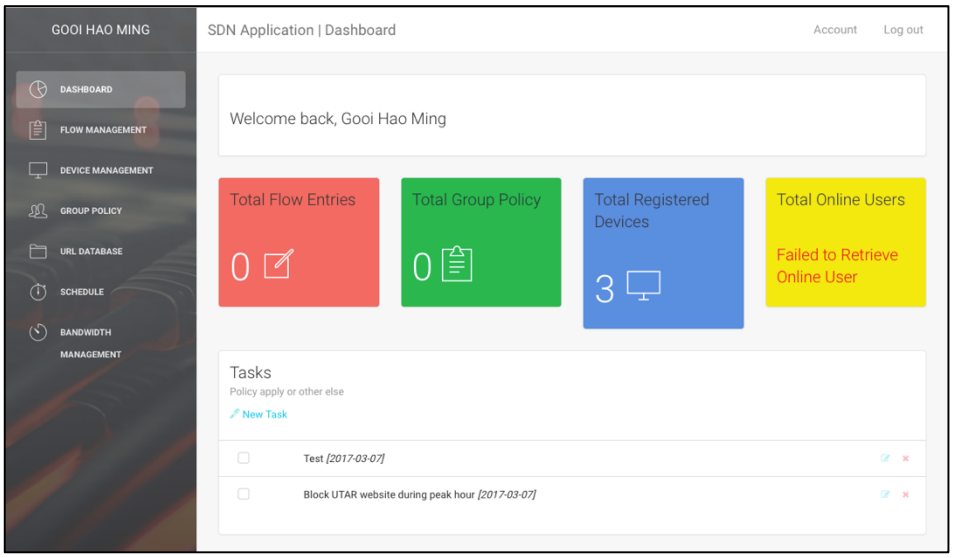


Figure 4-2-F2 Dashboard

Figure 4-2-F2 is the dashboard of the system. At the dashboard, it shows the total number of flow entries, total number of group policy, total number of registered devices and total number of online user. By clicking each details, it will navigate user to the respective page.

The dashboard also provides a side navigation bar to let user navigate to each function. By clicking the account, it will navigate user to account management pages.

The dashboard also provides a task management for the network administrator. The network administrator can add or delete the task at this section. After finish the task, the admin can check it.

❖ **Admin Account Management**

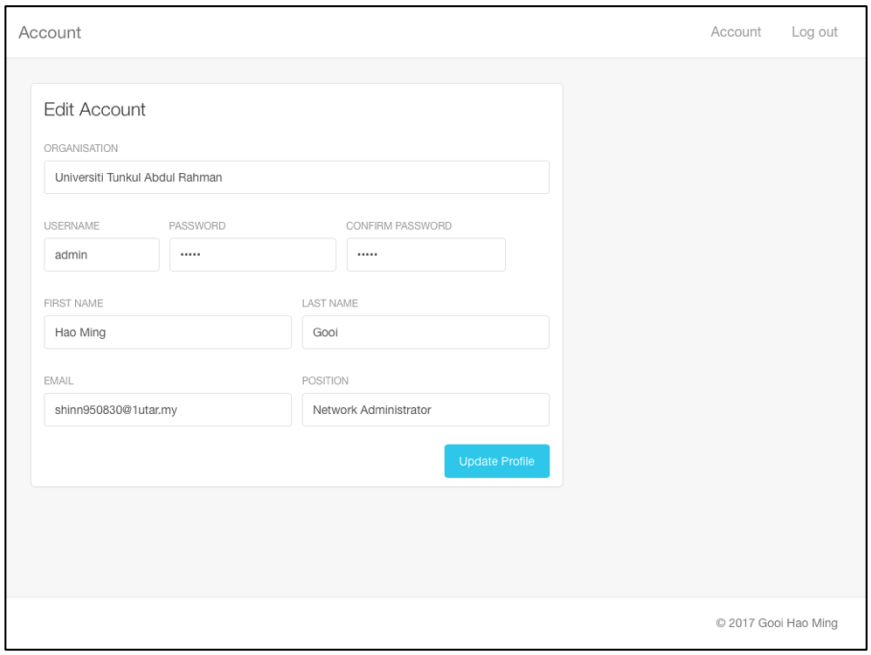


Figure 4-2-F3 Admin Account Management

Figure 4-2-F3 is the admin account management page. Admin can update or edit the account information such as username, password, email and so on.

❖ Flow Management

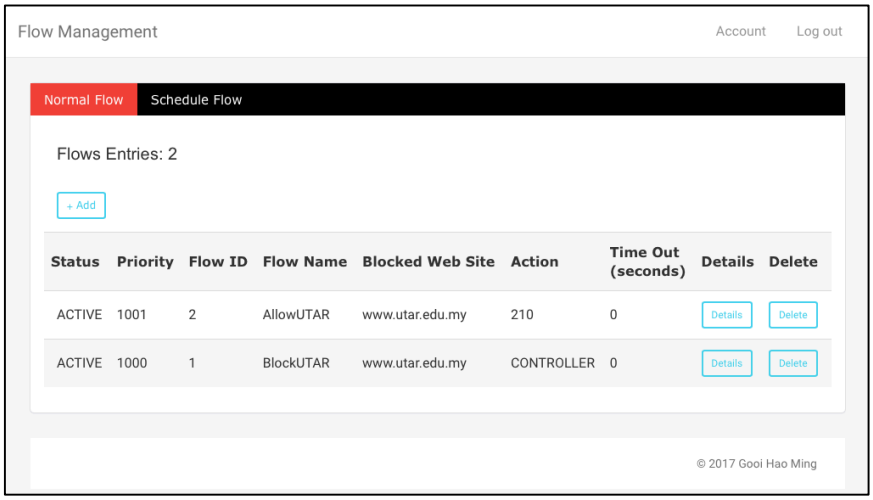


Figure 4-2-F4 Flow Management

Figure 4-2-F4 is the Flow Management page. Admin can navigate to normal flow or schedule flow. Moreover, admin able to view, create a new flow or delete existing flow at this page.

At the flow management page, it allows admin to create two type of flow which is normal flow and schedule flow.

Normal Flow

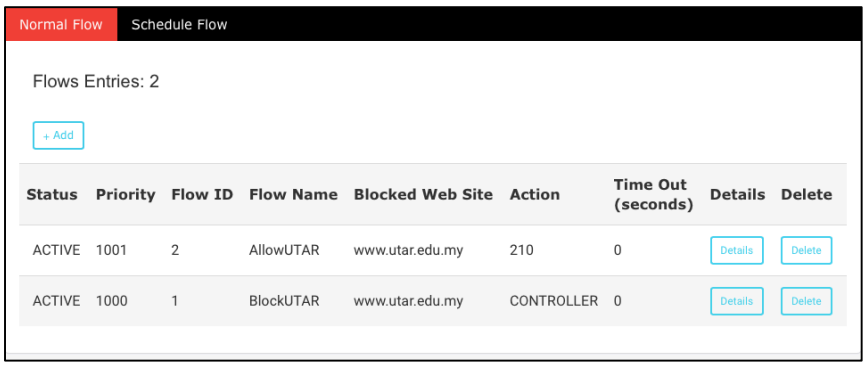


Figure 4-2-F5 Normal Flow Section

Figure 4-2-F6 Normal Flow Details

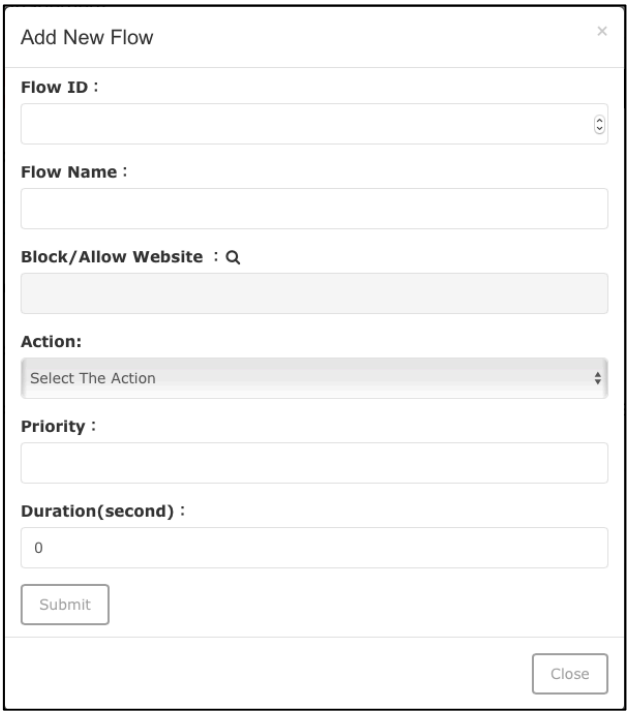


Figure 4-2-F7 Add Normal Flow Form

Figure 4-2-F5 is the Normal Flow Management section. Normal flow will apply to all the user regardless user group. By using this function, admin able to allow or disallow the user to access the certain site.

Admin can create a new flow by click the "+ Add" button. To delete the flow, admin can click the "Delete" button.

In order to create a new normal flow, admin need to provide the following information which is Flow ID, Flow Name, Block/Allow Website (refer to URL database section), Action, Priority, Duration. Figure 4-2-F7 is the form of add new normal flow.

The flow id must be unique, if there is a flow id exist the admin will not able to proceed. For the Block/Allow Website it will access the URL database and let admin choose which site that the admin want. For the priority, the highest priority will be process first. For the duration, it will decide how long the flow exist. If the duration is set to 10 second, the flow will become inactive after 10 second when the flow was created.

After the flow was created, admin can click the details button to view more details about the flow. Figure 4-2-F6 show the details of the normal flow.

Schedule Flow

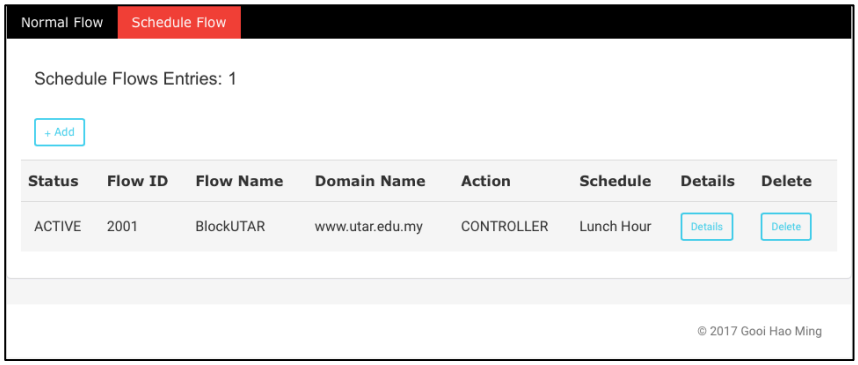


Figure 4-2-F8 Schedule Flow Section

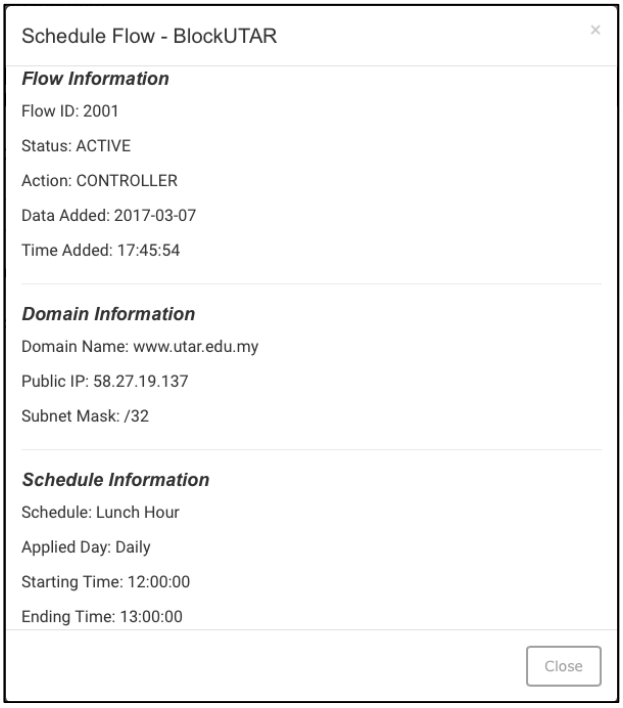


Figure 4-2-F9 Schedule Flow Details

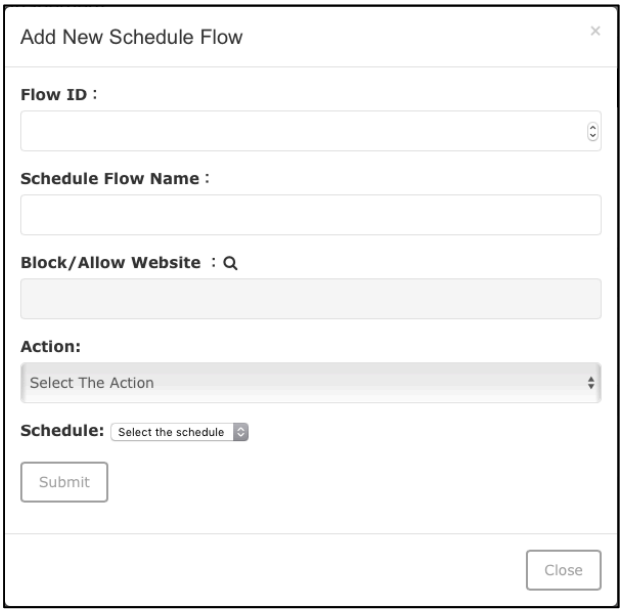


Figure 4-2-F10 Add Schedule Flow Form

Figure 4-2-F8 is the Schedule Flow Section. Schedule flow is applied to all the user regardless user group. By using this function, admin able to allow or disallow the user to access the certain site in a time range. For an example, if the admin select “Lunch Hour(12:00pm- 2:00pm)” the flow will run at 12pm and end in 2:00pm. Admin can create a new

schedule flow by click the "+ Add" button. To delete the flow, admin can click the "Delete" button.

In order to create a new schedule flow, admin need to provide the following information which is Flow ID, schedule flow name, Block/Allow Website(refer to URL database section), action and Schedule(refer to schedule section). Figure 4-2-F10 is the form of add new normal flow.

The flow id must be unique, if there is a flow id exist the admin will not able to proceed. For the Block/Allow Website it will access the URL database and let admin choose which site that the admin want. For the schedule it will let the user choose form the schedule that had create.

After the flow was created, admin can click the details button to view more details about the flow. Figure 4-2-F9 show the details of the normal flow.

❖ **Device Management**

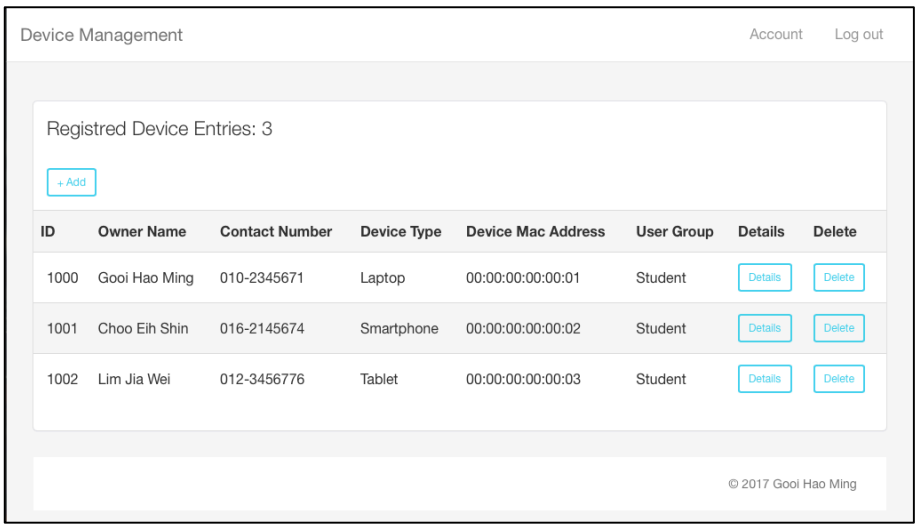


Figure 4-2-F11 Device Management

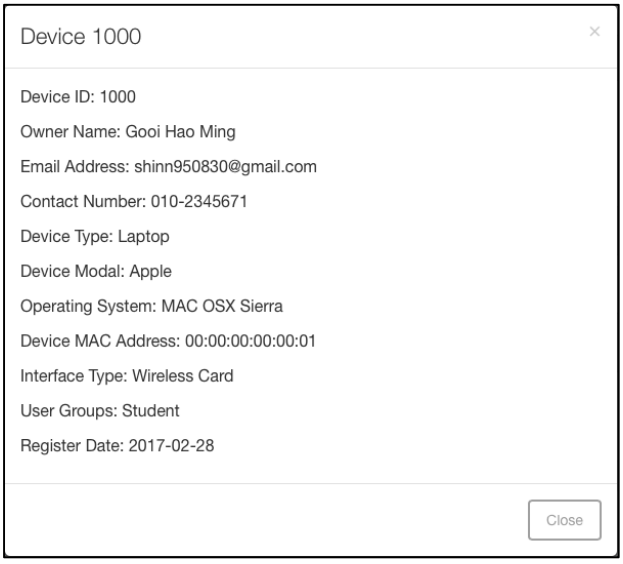


Figure 4-2-F12 Device Details

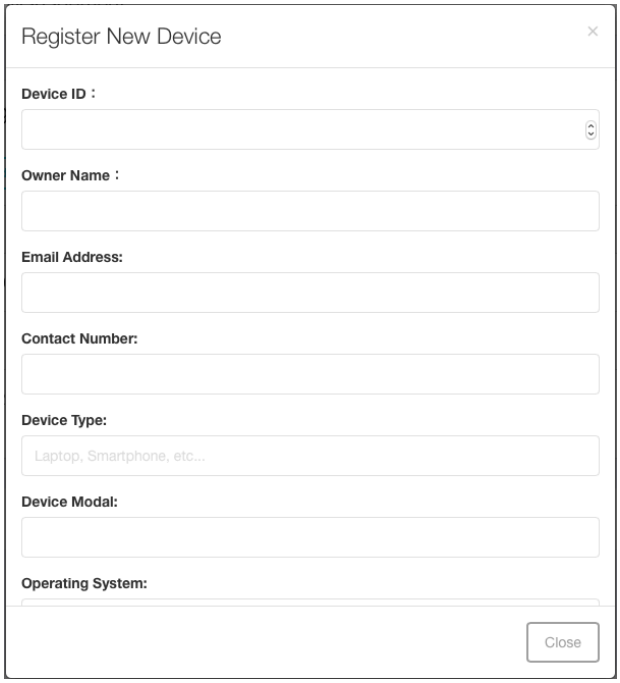


Figure 4-2-F13 Register Device Form

Figure 4-2-F11 is the device management page. In this page, admin able to register a new device, view the registered device and remove the registered device. Admin can click the "Details" button to view more information about the device and click "Delete" to remove the device.

Any device that want to connect to the network it need to register first then only can connect and use the resource.

In order to registered the device, the following information need to provide. Device ID, owner name, email address, contact number, device type, device modal, operating system, device MAC address, interface type and user group. Figure 4-2-F13 is the form of register device.

The system will perform some checking at the device id and device MAC address. If there is any same id and MAC address found in the database, the register process can not proceed.

❖ Group Policy Management

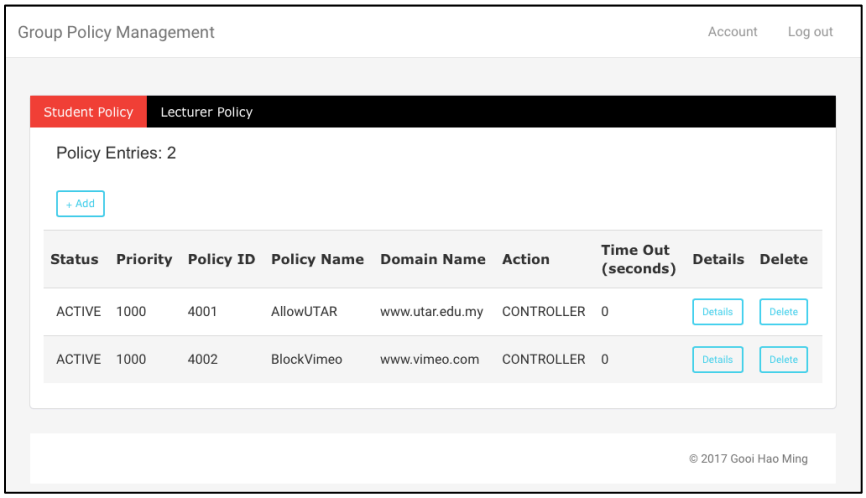


Figure 4-2-F14 Group Policy Management

Figure 4-2-F14 is the Group Policy Management page of the system. Admin can navigate to student policy or lecturer policy. Moreover, admin able to view, create a new policy or delete existing policy at this page. By using this function, admin able to allow or disallow the certain user group to access the certain site.

At the group policy management page, admin allow to create two type of policy which is student policy and lecturer policy.

Student Policy

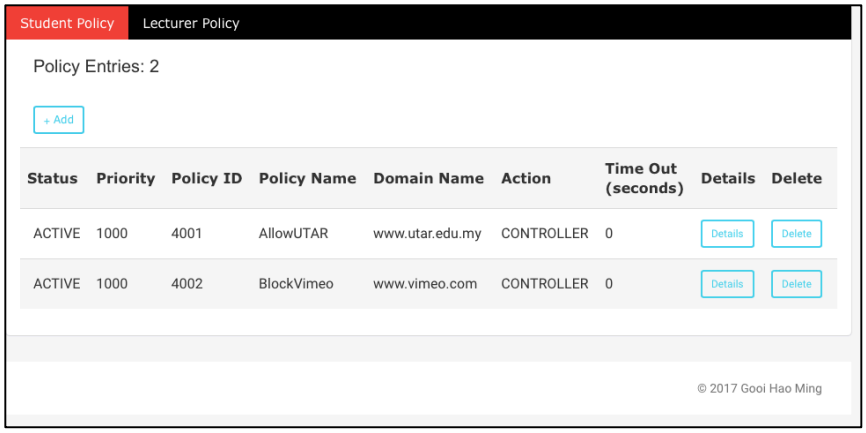


Figure 4-2-F15 Student Policy Section

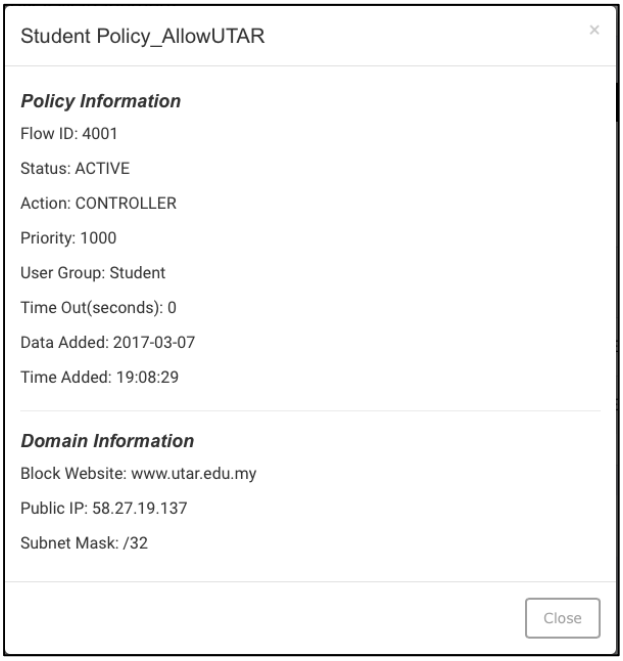


Figure 4-2-F16 Student Policy Details

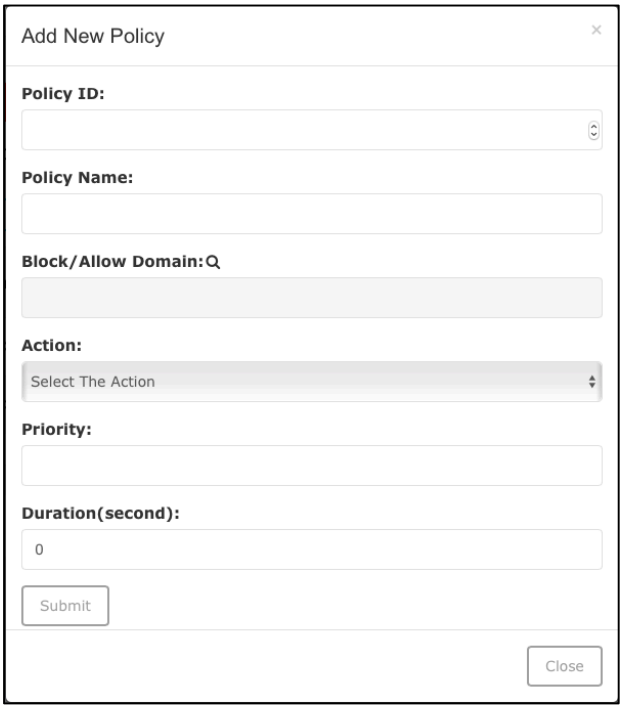


Figure 4-2-F17 Add New Policy Form

Figure 4-2-F15 is the student policy section. Student policy will only apply to the student group where lecturer group will not be affect. Admin can create a new policy by click the "+ Add" button. To delete the policy, admin can click the "Delete" button.

In order to create a new policy, admin need to provide the following information which is Policy ID, Policy Name, Block/Allow Website(refer to URL database section), Action, Priority, Duration. Figure 4-2-F17 is the form of add new policy flow.

The Policy ID must be unique, if there is the policy ID is exist in the database the admin will not able to proceed. For the Block/Allow Website it will access the URL database and let admin choose which site that the admin wants. For the priority, the highest priority will be process first. For the duration, it will decide how long the flow exist. If the duration is set to 10 second, the flow will become inactive after 10 second when the flow was created.

After the policy was created, admin can click the details button to view more details about the policy. Figure 4-2-F16 show the details of the student policy.

Lecturer Policy

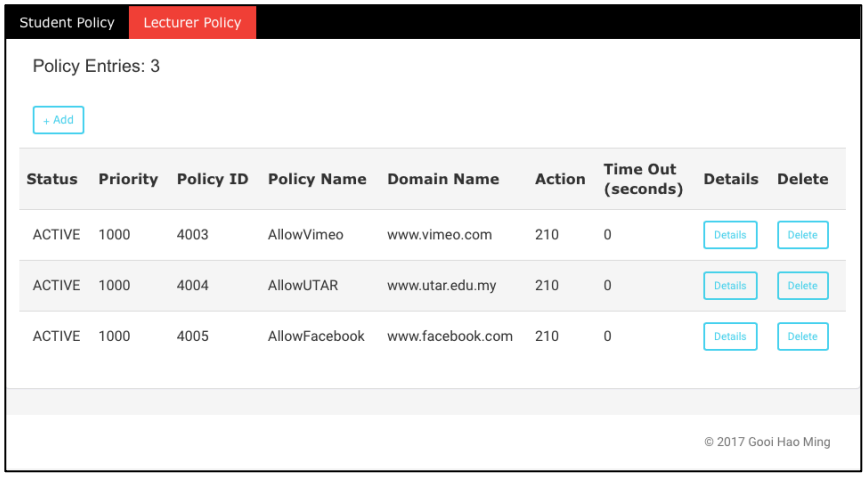


Figure 4-2-F18 Lecturer Policy Section

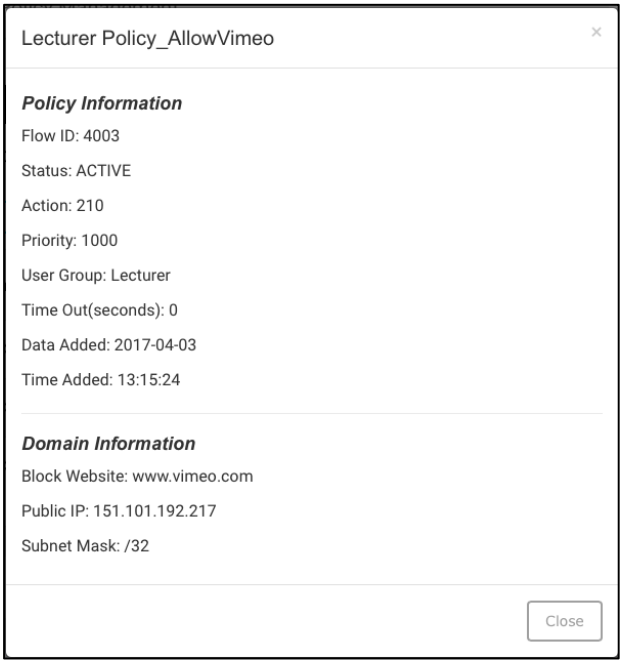


Figure 4-2-F19 Lecturer Policy Details

Figure 4-2-F18 is the lecturer policy section. Lecturer policy will only apply to the lecturer group where student group will not be affect. Admin can create a new policy by click the "+ Add" button. To delete the policy, admin can click the "Delete" button.

In order to create a new policy, admin need to provide the following information which is Policy ID, Policy Name, Block/Allow Website(refer to URL database section), Action, Priority, Duration. Figure 4-2-F17 is the form of add new normal flow.

The Policy ID must be unique, if there is the policy ID is existed in the database the admin will not able to proceed. For the Block/Allow Website it will access the URL database and let admin choose which site that the admin wants. For the priority, the highest priority will be process first. For the duration, it will decide how long the flow exist. If the duration is set to 10 second, the flow will become inactive after 10 second when the flow was created.

After the policy was created, admin can click the details button to view more details about the policy. Figure 4-2-F19 show the details of the lecturer policy.

❖ URL Database

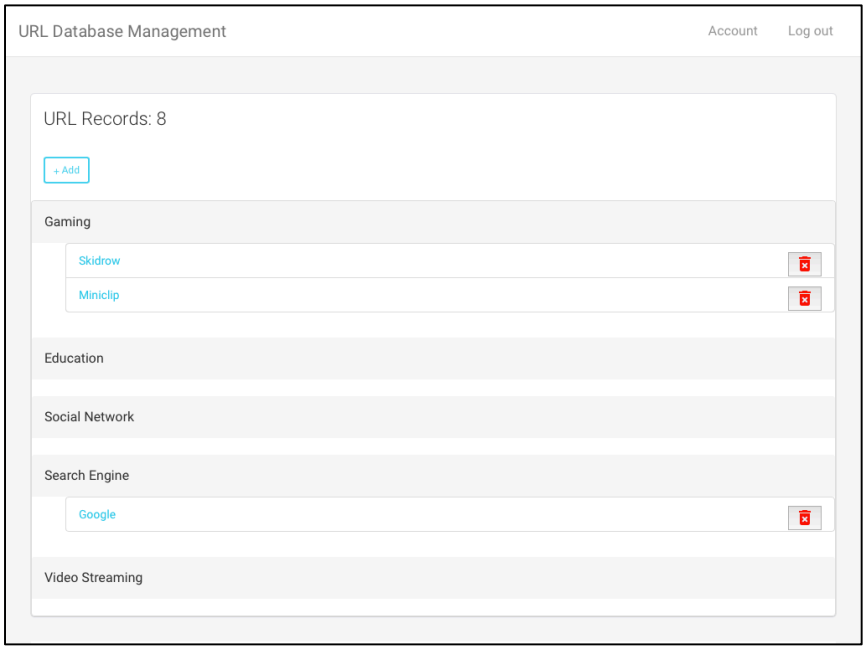


Figure 4-2-F20 URL Database Management

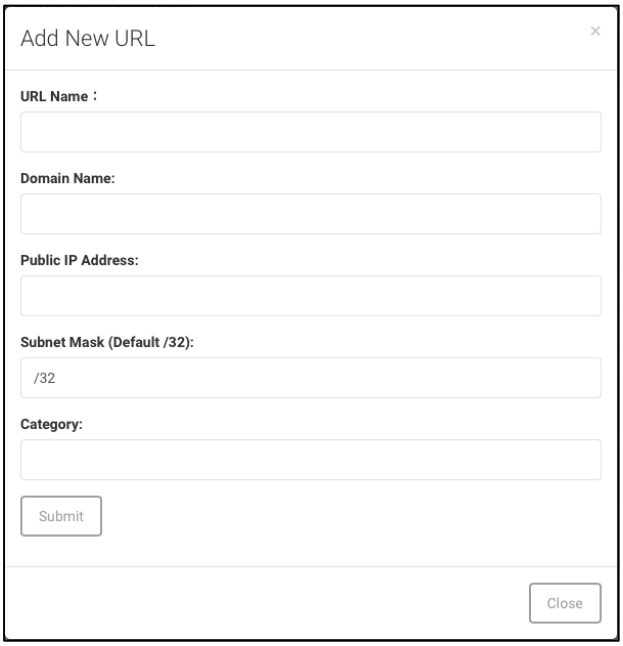


Figure 4-2-F21 Add New URL

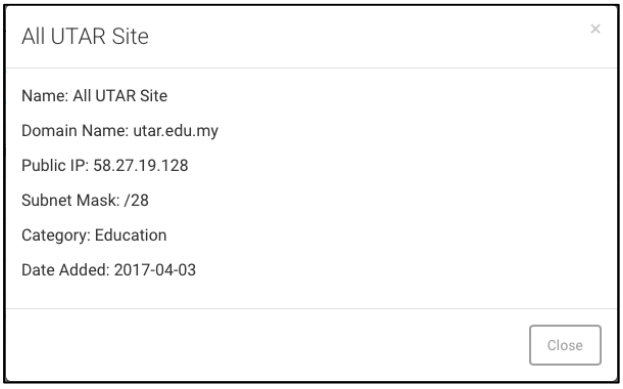


Figure 4-2-F22 URL Details

Figure 4-2-F20 is the URL Database management page. The URL database will store all the URL or domain that the admin added in. The URL database will be used when admin want to create a new flow, new schedule flow, student policy or lecturer policy.

Now a day, some of the networking company product will also provide a URL database. The URL database provide their customer all the URL or domain name around the world. If the customer wants to block the access to some website, they just need to create a policy and select or enter the URL name, then the system will look for the URL database and retrieve all the information about the URL or domain name like public IP address. The company also allow their customer to update the URL database when there are new URLs or domain names. They also allow their customer manually add the new entry into the database.

Back to the system, in order to create a new URL, admin need to provide the following information which is URL name, domain name, public IP address, subnet mask, and category. Figure 4-2-F21 is the form of add new URL.

When the admin enters the domain name, the system will automatic resolve the public IP address of the domain name.

For the subnet mask, by default it is /32(255.255.255.255). If the domain name bind with more than one IP addresses or admin want to add all the site that related and its public IP address is in a range then the subnet mask will change.

After the URL entry was created, admin can click the details button to view more details about the URL entry. Figure 4-2-F22 show the details of the URL entry.

❖ Schedule Management

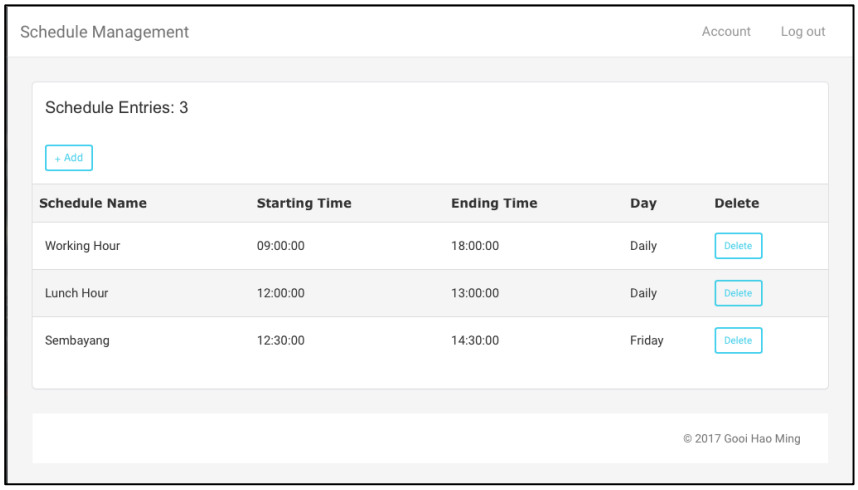


Figure 4-2-F23 Schedule Management

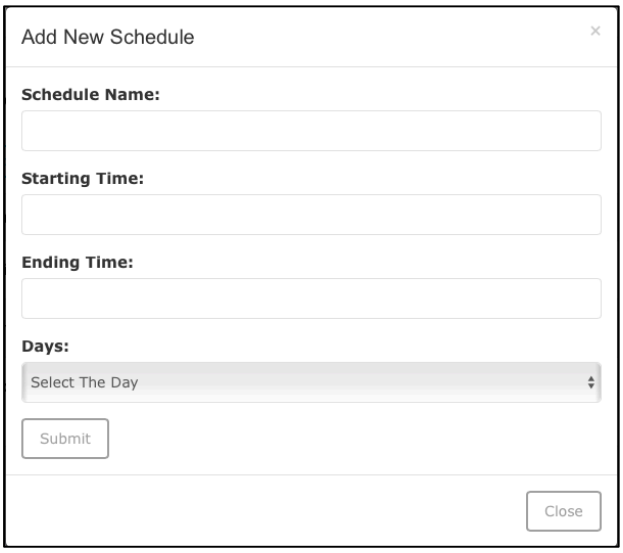


Figure 4-2-F24 Add New Schedule Form

Figure 4-2-F23 is the Schedule Management page of the system. The schedule management allow user to view, create new schedule and delete schedule.

The schedule will be use when create a new schedule flow. Moreover, the created schedule can be use in more than one schedule flow. For an example, if the admin want more than one flow run in "Working Hour", the admin can just create the flow and select the "Working Hour" for the schedule.

In order to create a new schedule, admin need to provide the following information which is schedule name, starting time, ending time, and days. Figure 4-2-F24 is the form of add new schedule.

❖ Bandwidth Management

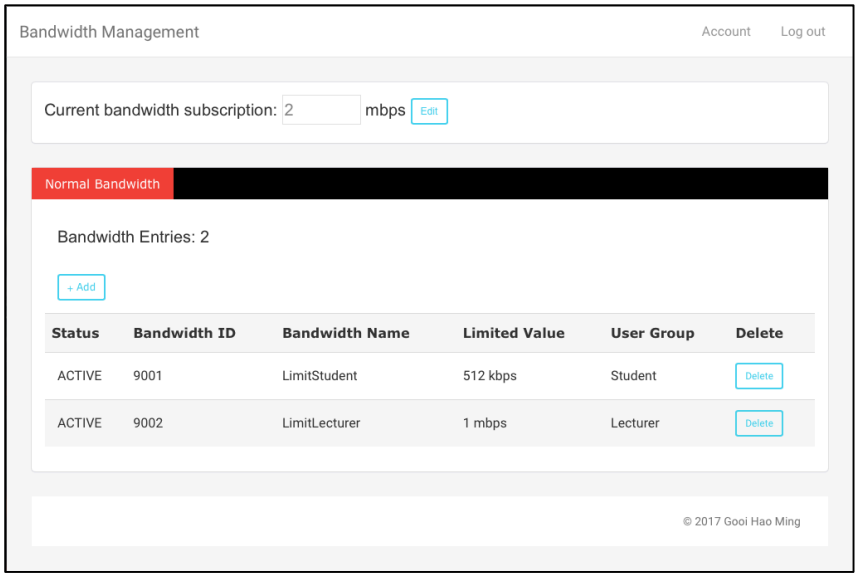


Figure 4-2-F25 Bandwidth Management

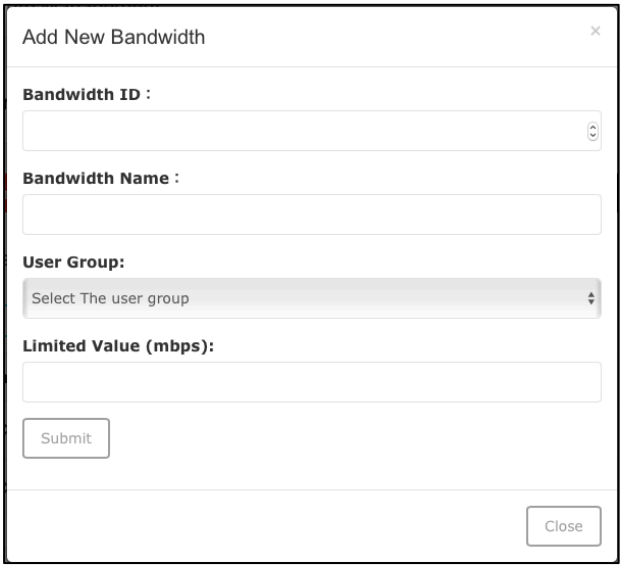


Figure 4-2-F26 Add New Bandwidth Policy Form

Figure 2-3-F25 is the bandwidth management page for the system. Bandwidth management allow admin to create a policy to limit the bandwidth for a certain user group or all of the user group. Moreover, admin also can edit the current subscription of the bandwidth form the ISP. By click the "+ Add" button, admin allow to add a new bandwidth policy, by click the "Delete" button admin allow to remove the policy.

In order to create a new bandwidth policy, admin need to provide the following information which is Bandwidth ID, Bandwidth name, user group, and limit value in mbps. Figure 4-2-F26 is the form of add new bandwidth policy.

For the user group, there have three selections for the admin which is All, student and lecturer.

For the limited value, admin only can enter the value that is less than or equal to the current subscription. If the admin enters the value larger than the current subscription, admin is not able to proceed the proceed.

4.3 Setup SDN Environment

- **Install Open Daylight SDN Controller**

  Open Daylight is an open source SDN controller. We download the platform from its official website and install into a PC running Ubuntu operating system.

- **Configure HP Switch 2920-24G**

  In order to enable the OpenFlow protocols, we need to create an instance and VLAN in the switch. First, we have created three VLAN which is VLAN10 for controller, VLAN20 for student group and VLAN30 for lecturer group. After that, we create an instance named "opendaylight" and assign VLAN20 and VLAN30 as the instance member. Then we create a new controller id and assign it to VLAN 10. Finally, we assign the created controller id to manage the instance "opendaylight".

- **Configure Cisco Route**

  In this project, Cisco router act as a DHCP server. All the host in the SDN network will get the IP address form the router based on their VLAN group. Moreover, the Cisco router also configured with Network Address Translation(NAT) to allow all the host form the SDN network to access the internet.

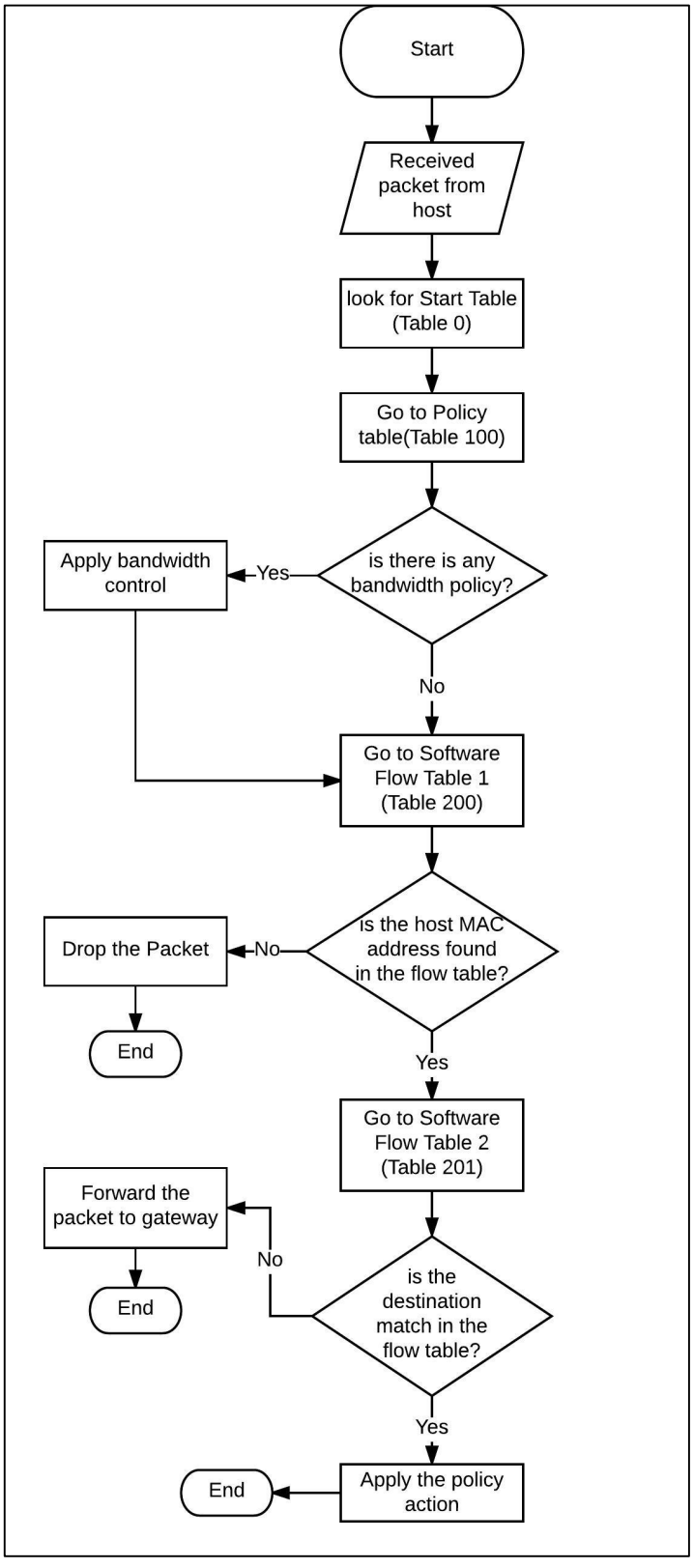
- **Setup Wireless Connection**

  In order to allow the wireless connection in the SDN network, we decided to setup a wireless access point and attach it to the HP switch. The DHCP function was disable in the wireless point, so all the host that connect to the wireless access point will get the IP from the Cisco router.

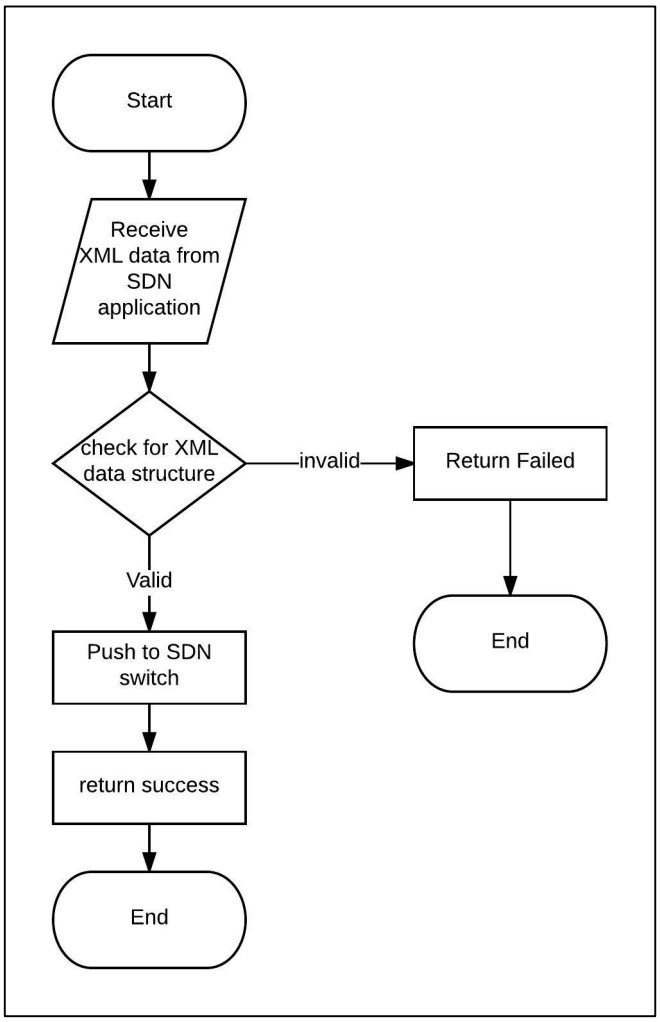
4.4 Project Flow Chart

4.4.1 Controller and SDN Switch Flow Chart

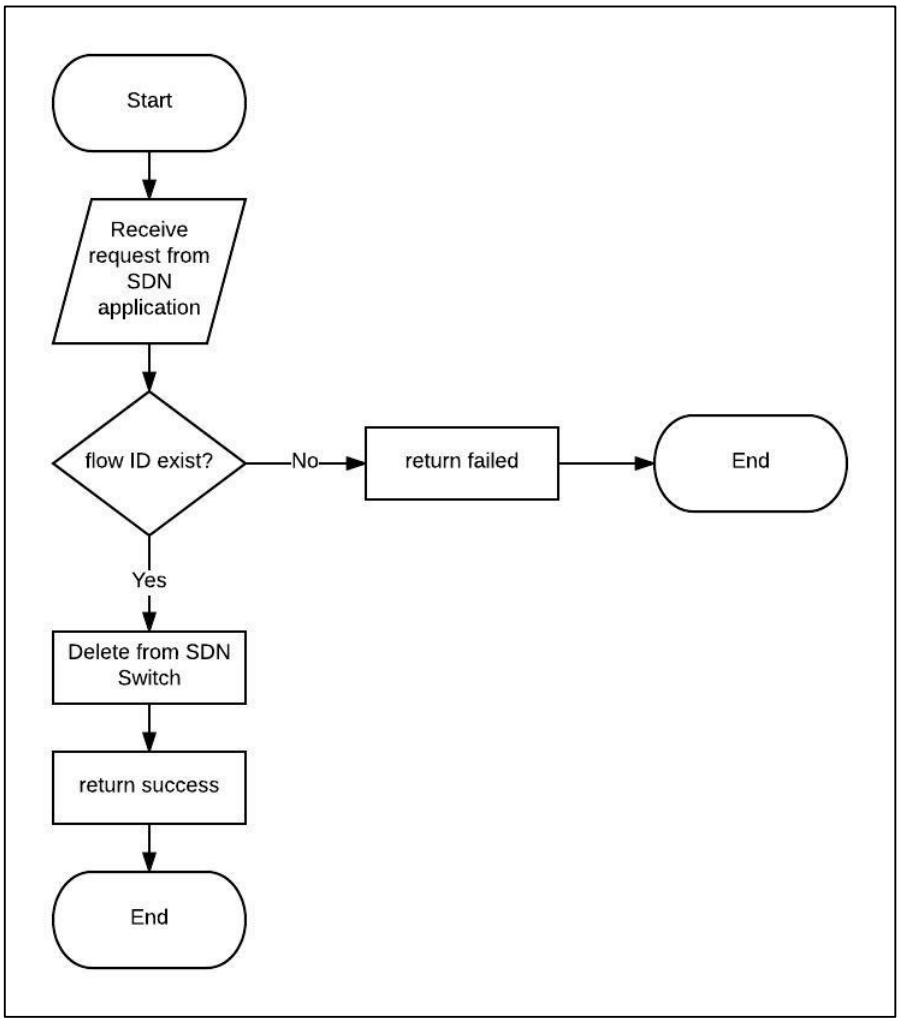
❖ **Receive Packet**



❖ **Push Flow**

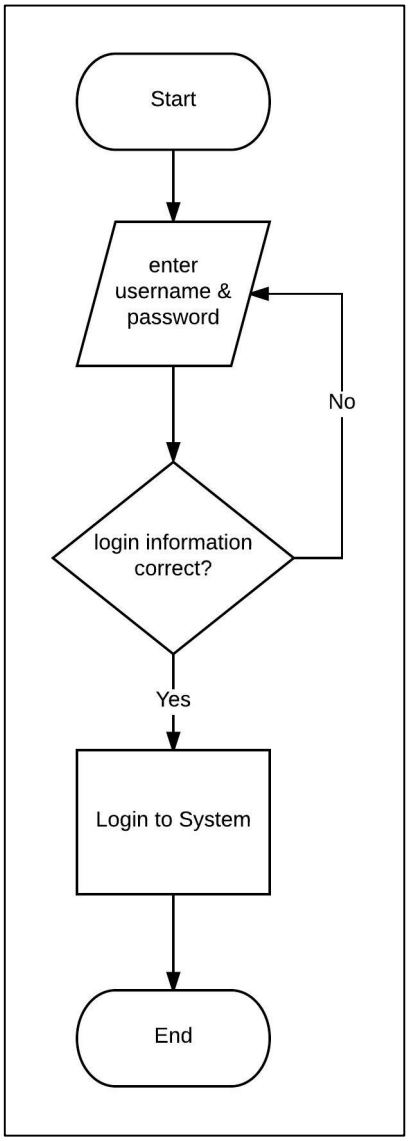

Start
Receive XML data from SDN application
check for XML data structure
invalid
Return Failed
End
Valid
Push to SDN switch
return success
End

❖ **Remove Flow**

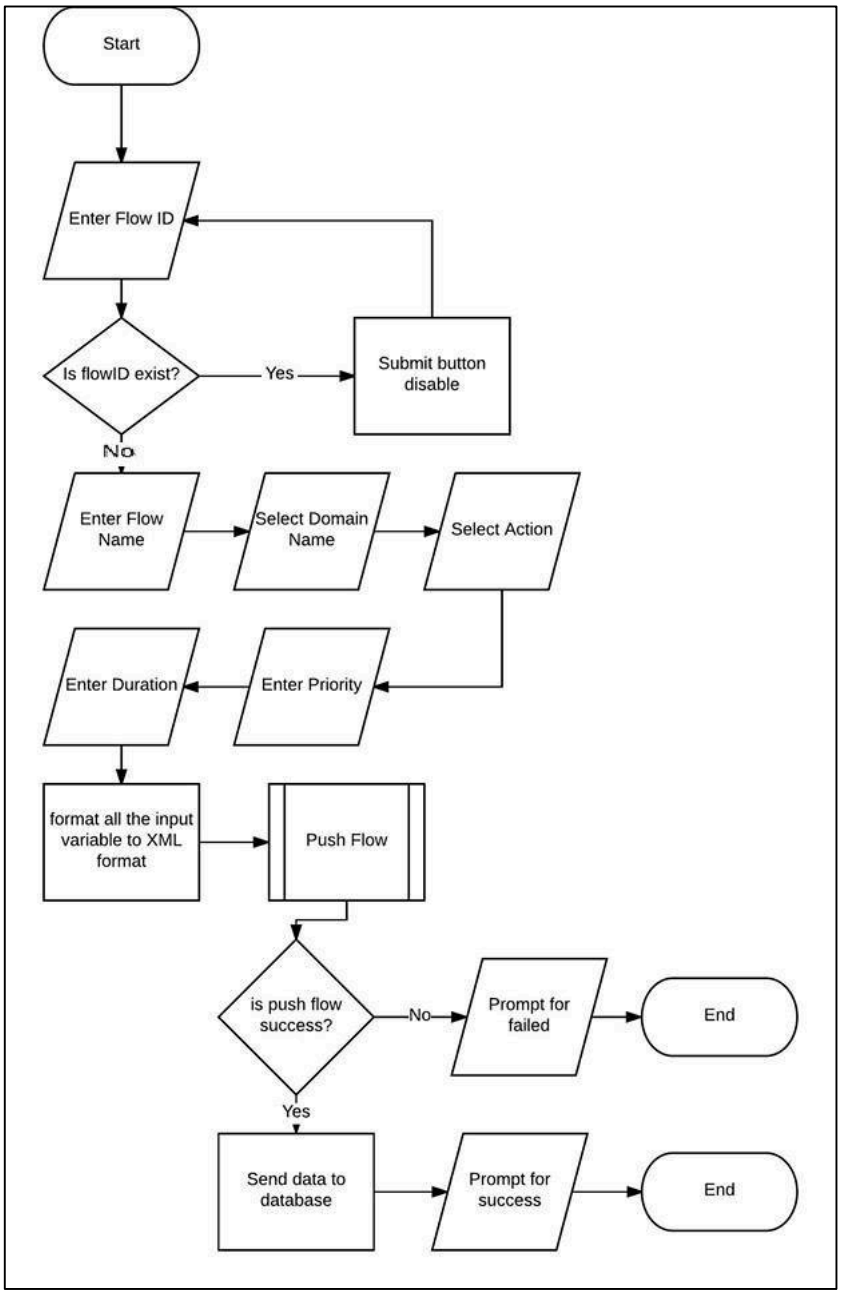

Start
Receive request from SDN application
flow ID exist?
No
return failed
End
Yes
Delete from SDN Switch
return success
End

4.4.2 Web-based GUI SDN Application Flow Chart

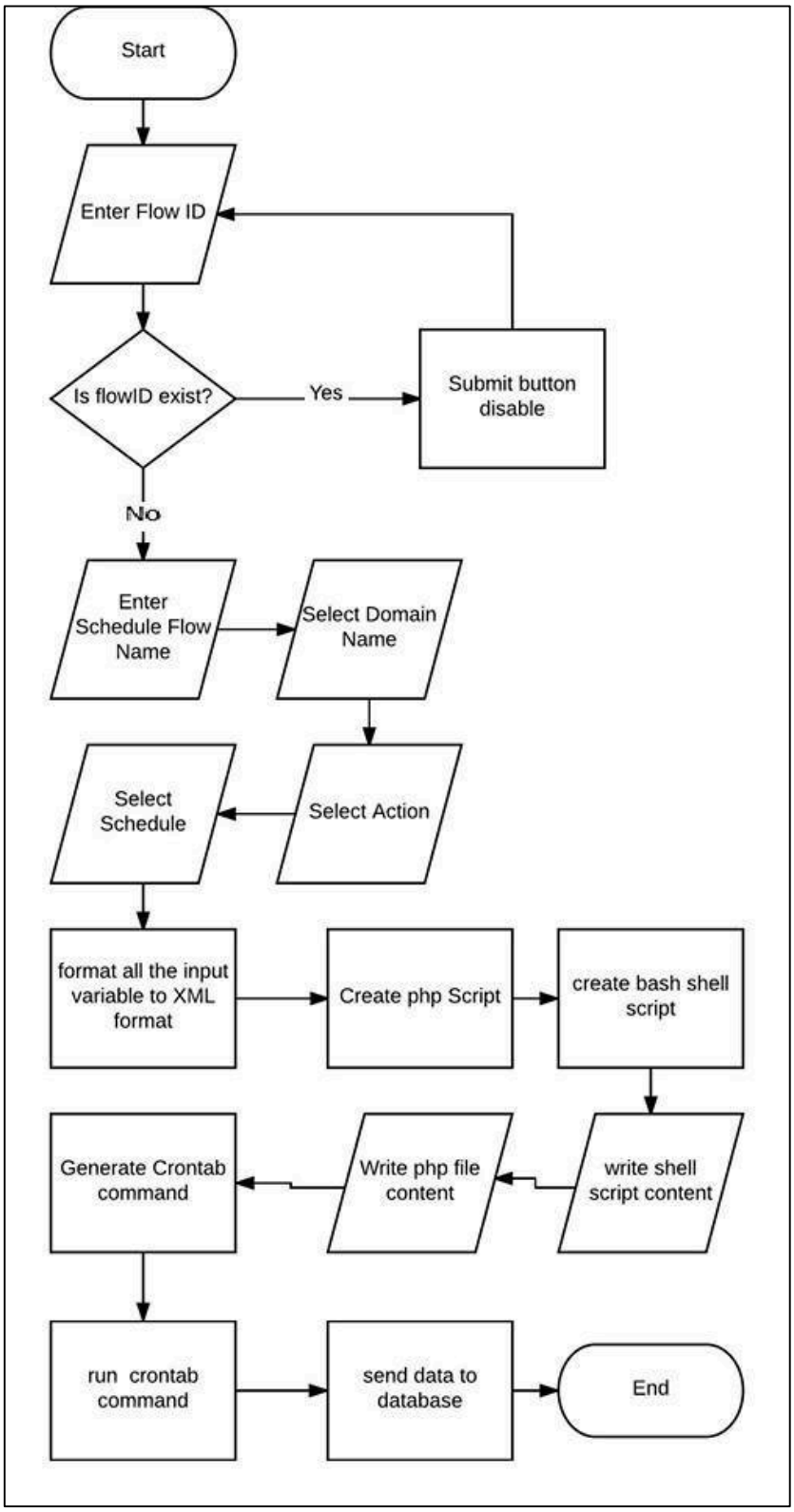
❖ **Login**



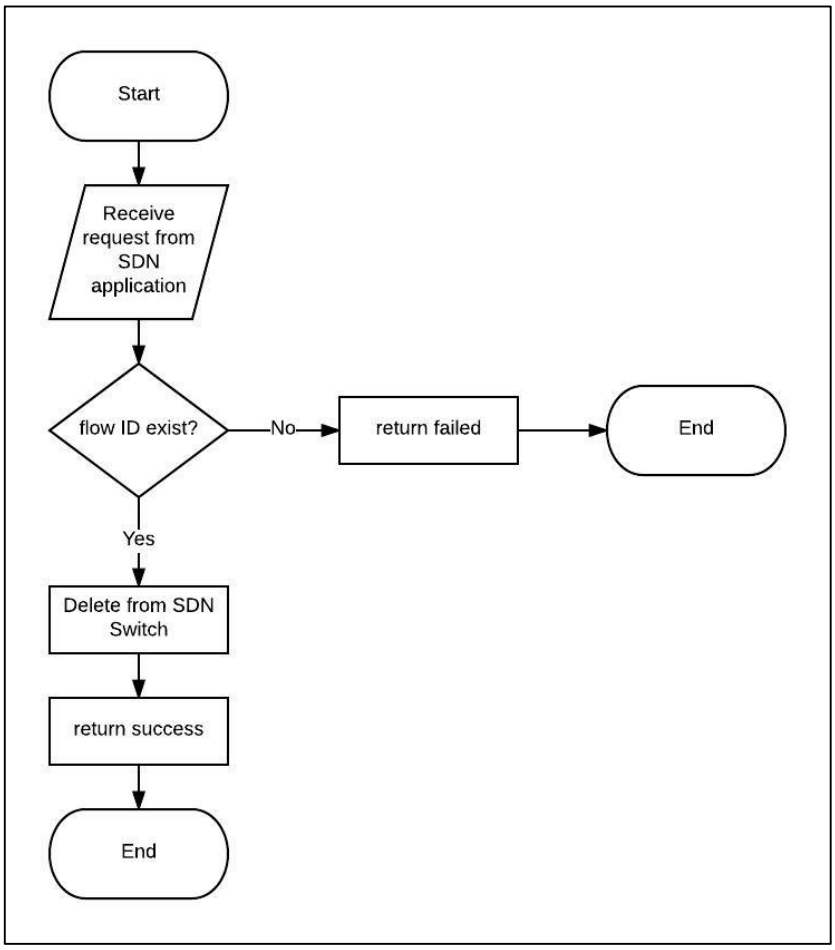
❖ **Create Normal Flow**



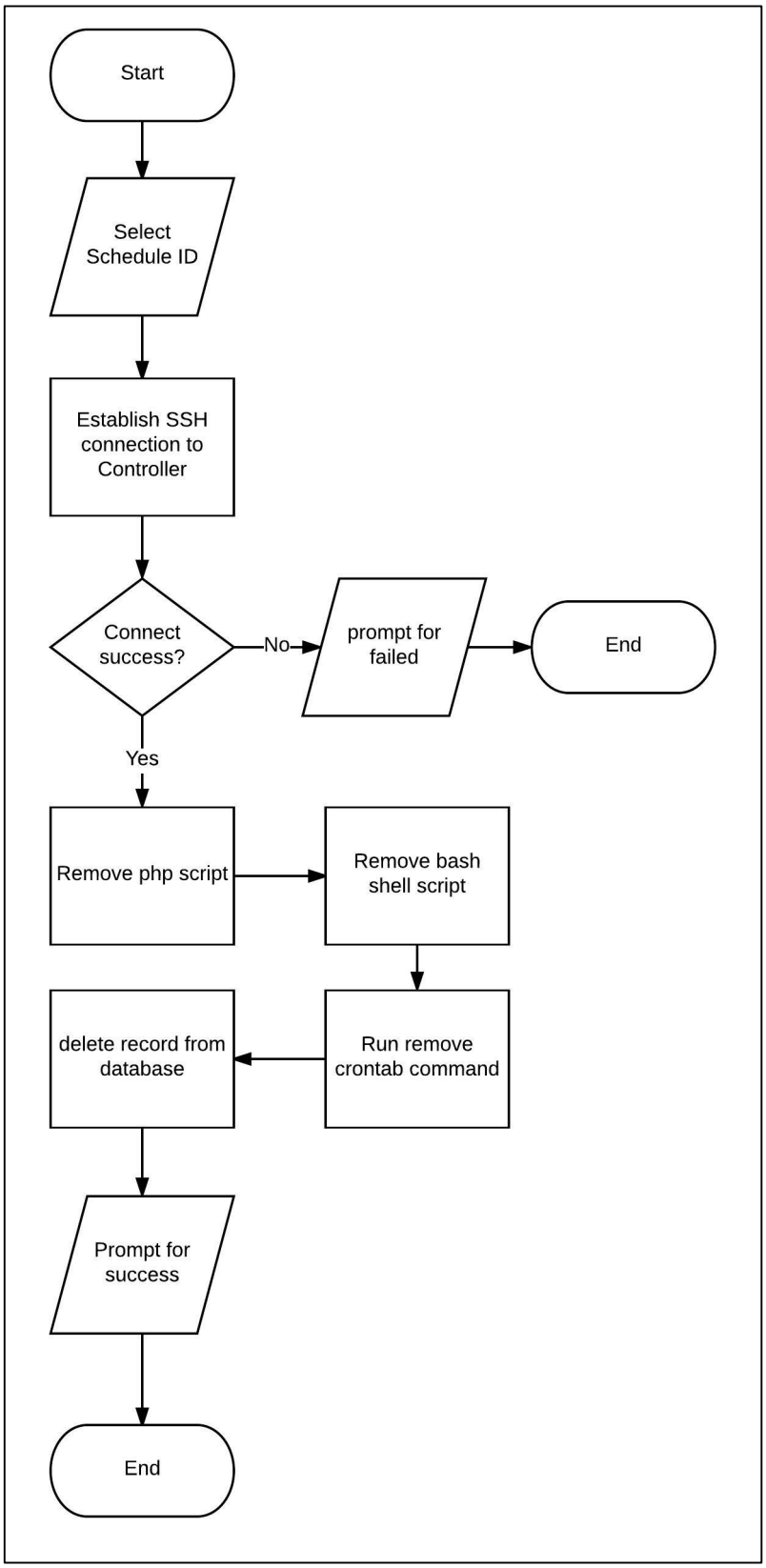
❖ **Create Schedule Flow**



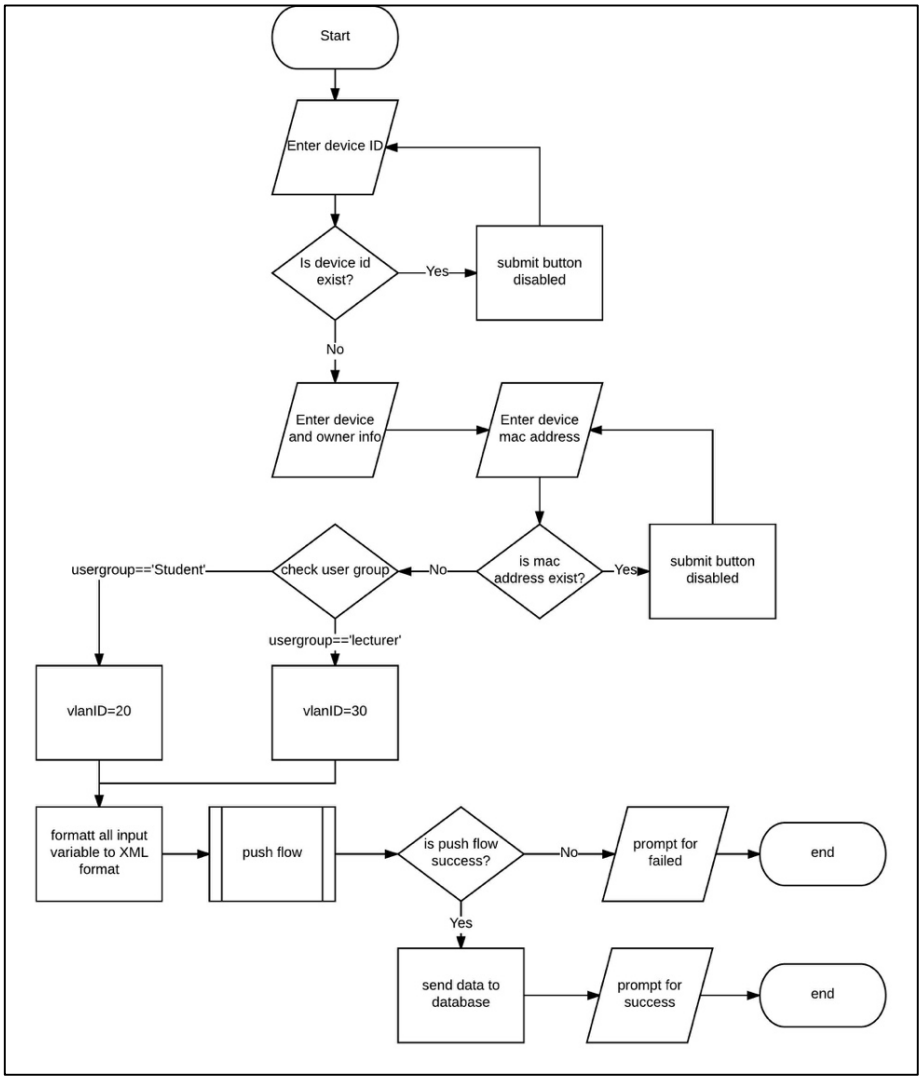
❖ **Remove Normal Flow**



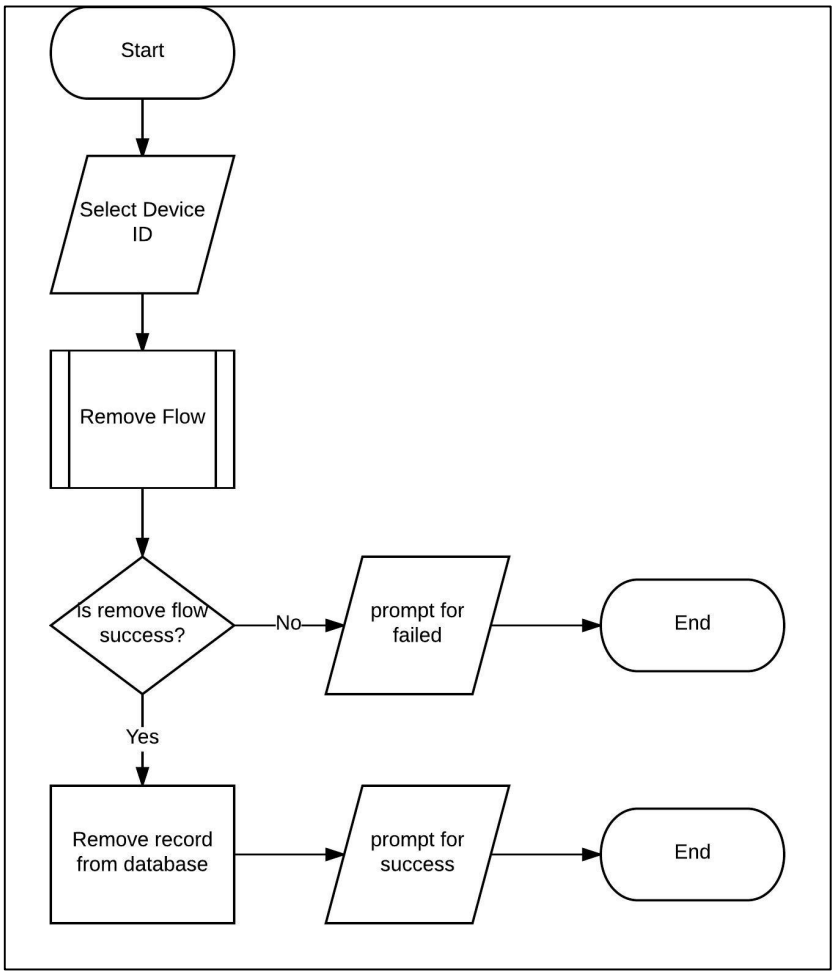
❖ **Remove Schedule Flow**



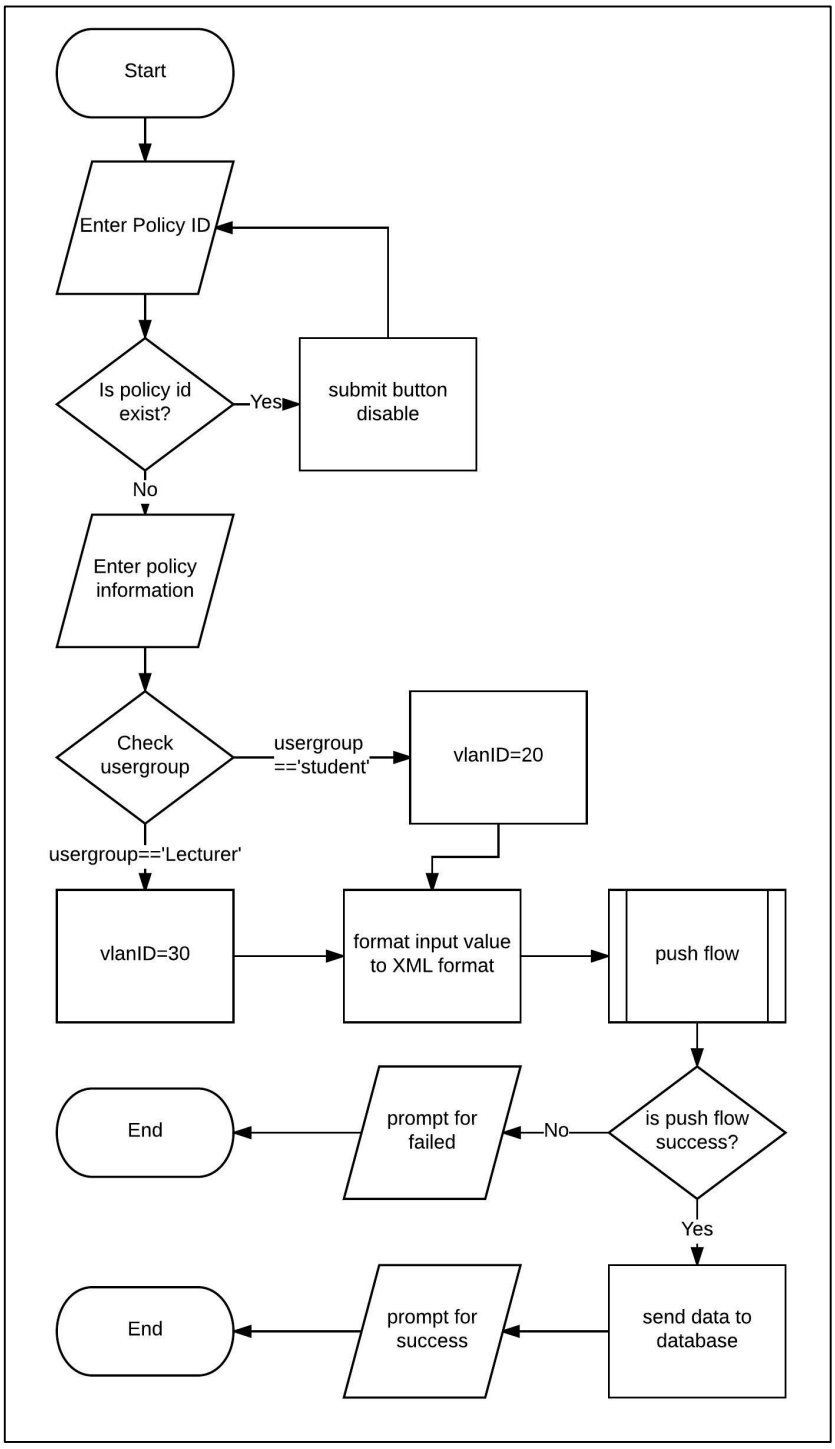
❖ Register Device



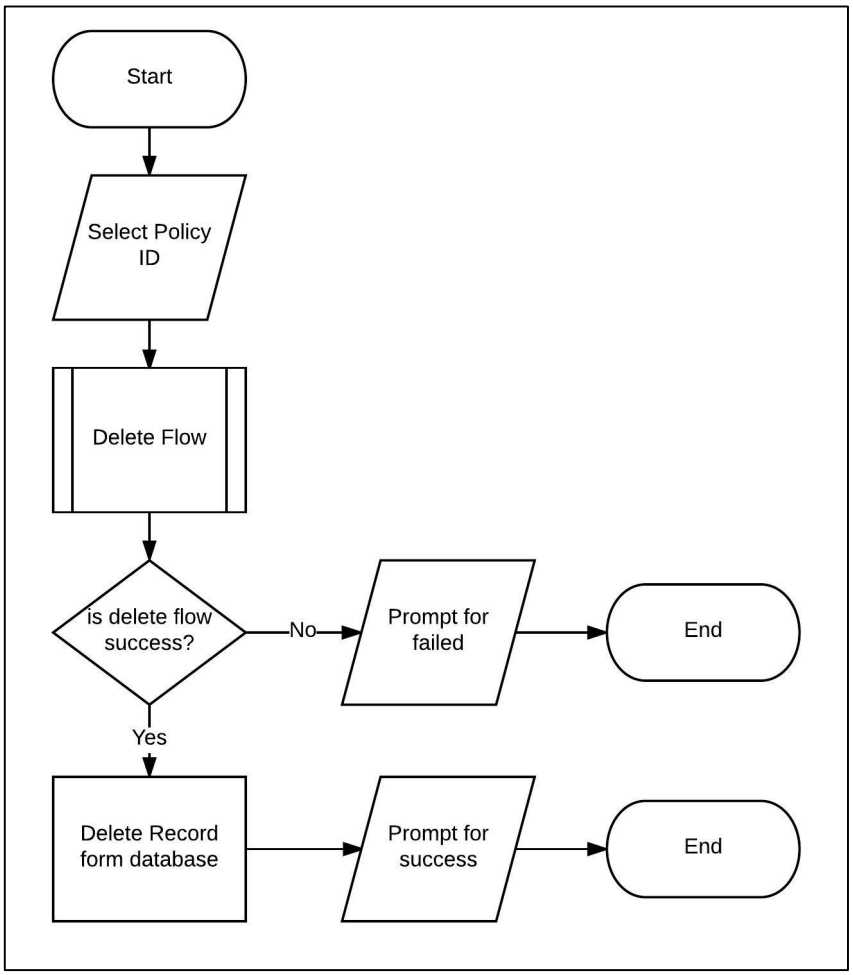
❖ **Remove Device**



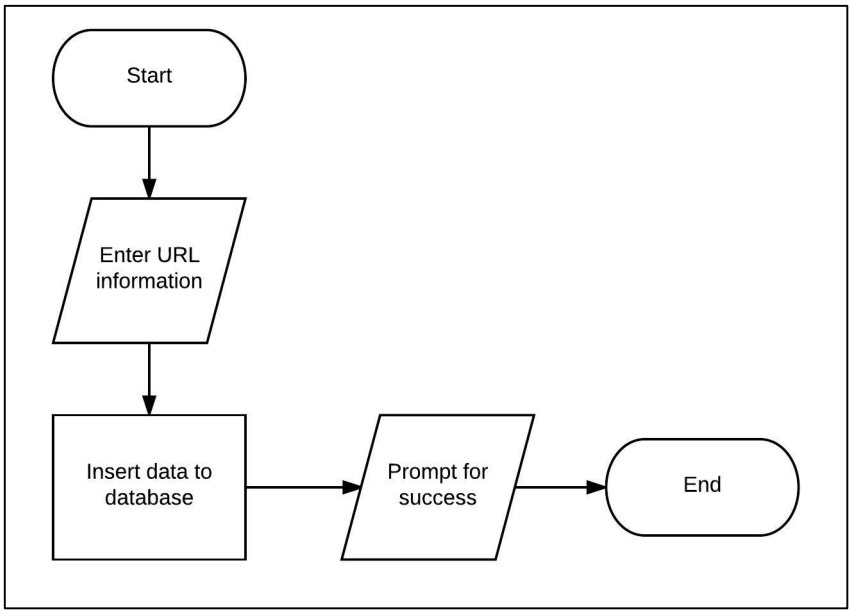
❖ **Create Policy**



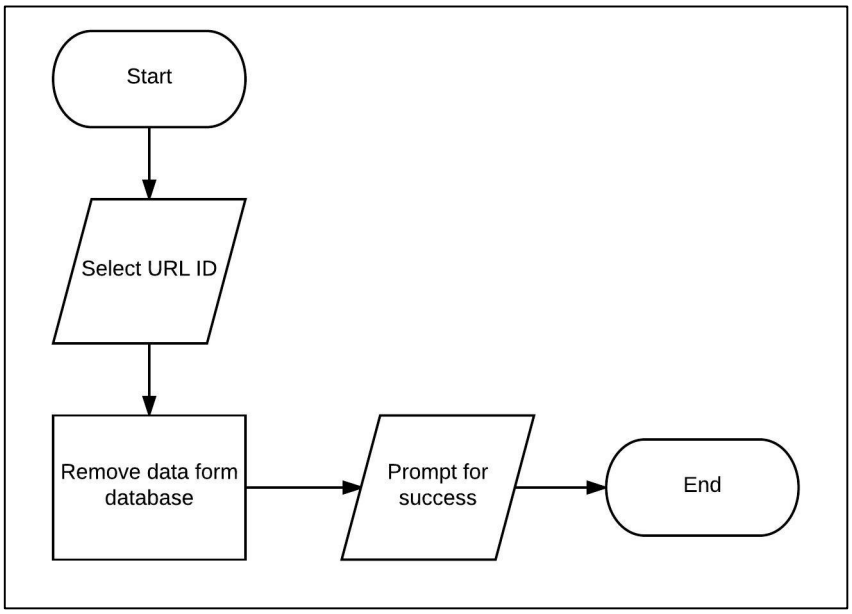
❖ **Remove Policy**



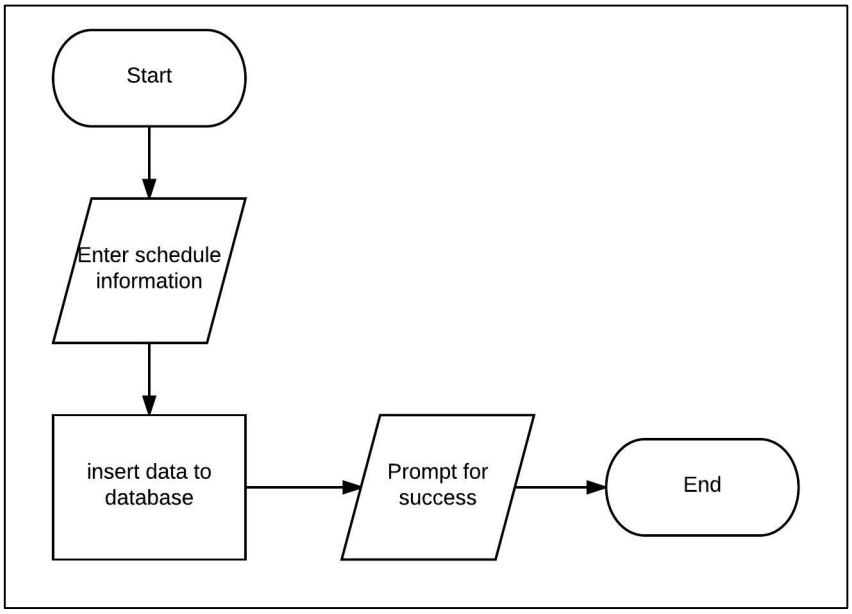
❖ **Create URL Entry**



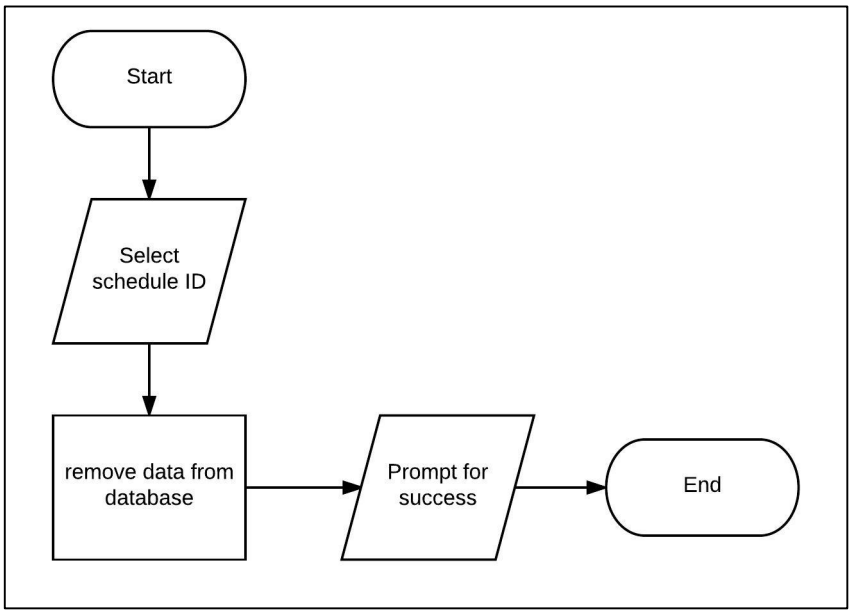
❖ **Remove URL Entry**



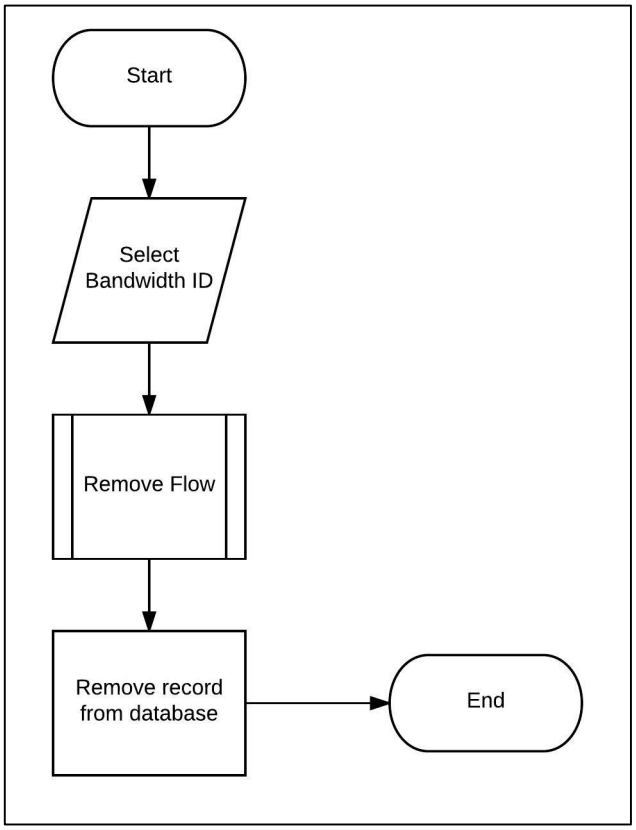
❖ **Create Schedule**



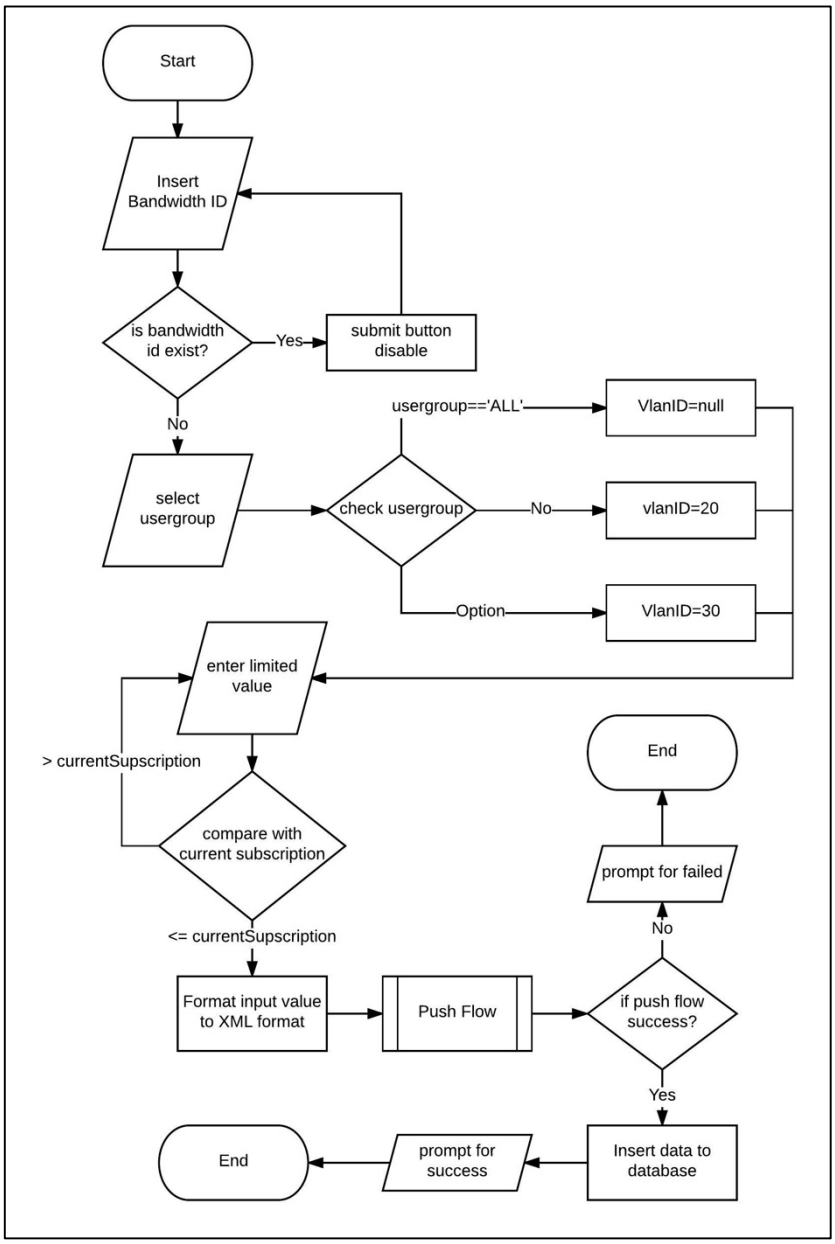
❖ **Remove Schedule**



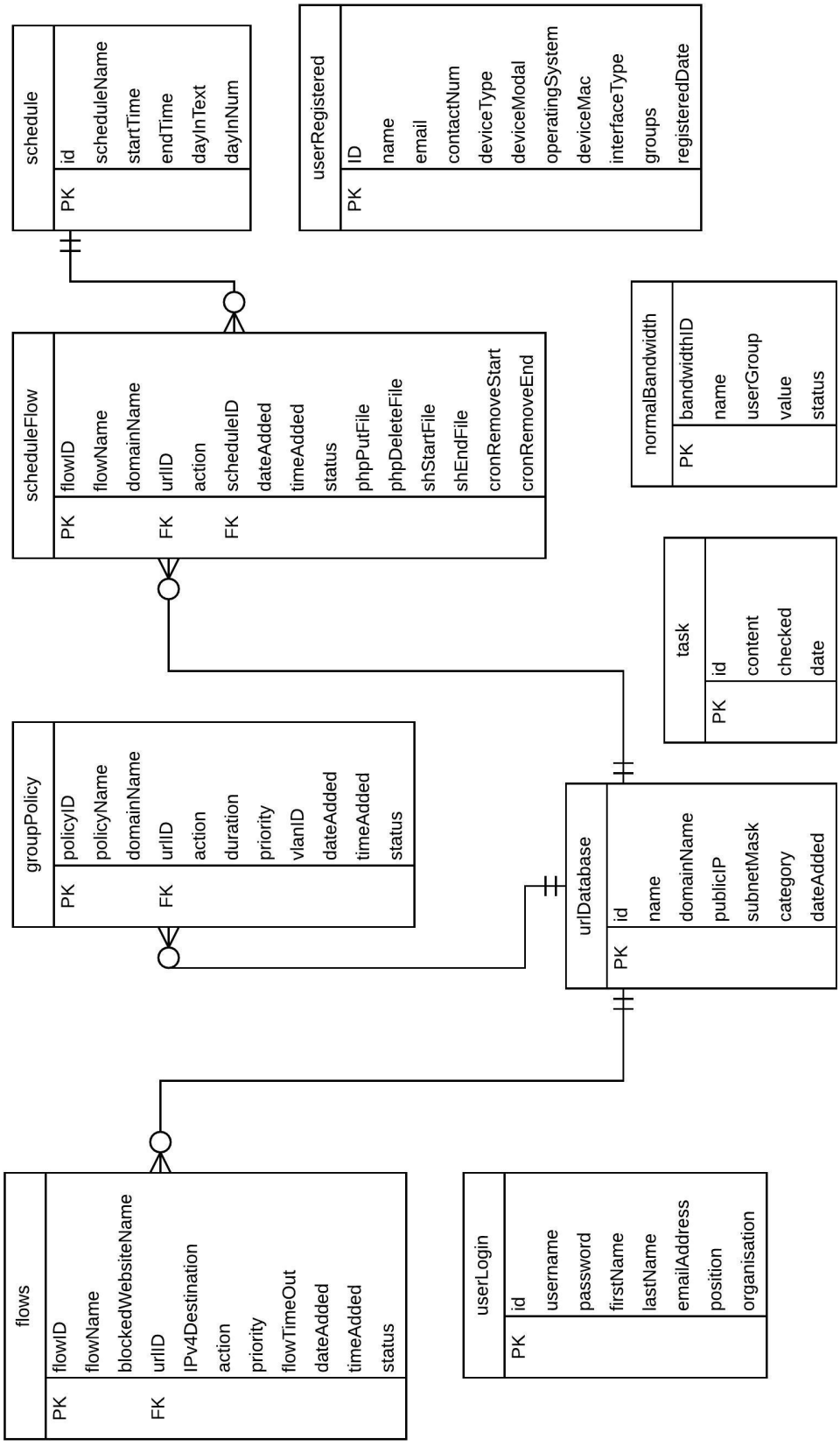
❖ **Remove Bandwidth Policy**



❖ Create Bandwidth Policy



4.5 Database ER Diagram



5.0 System Implementation

Since the project is implemented by using the real network equipment, it is not the simulation so we need to setup both hardware and software.

5.1 Hardware Setup

5.1.1 Design network topology

Before we start to implement the system, we have to design a network topology. The network topology shows in Figure 5-1-F1.

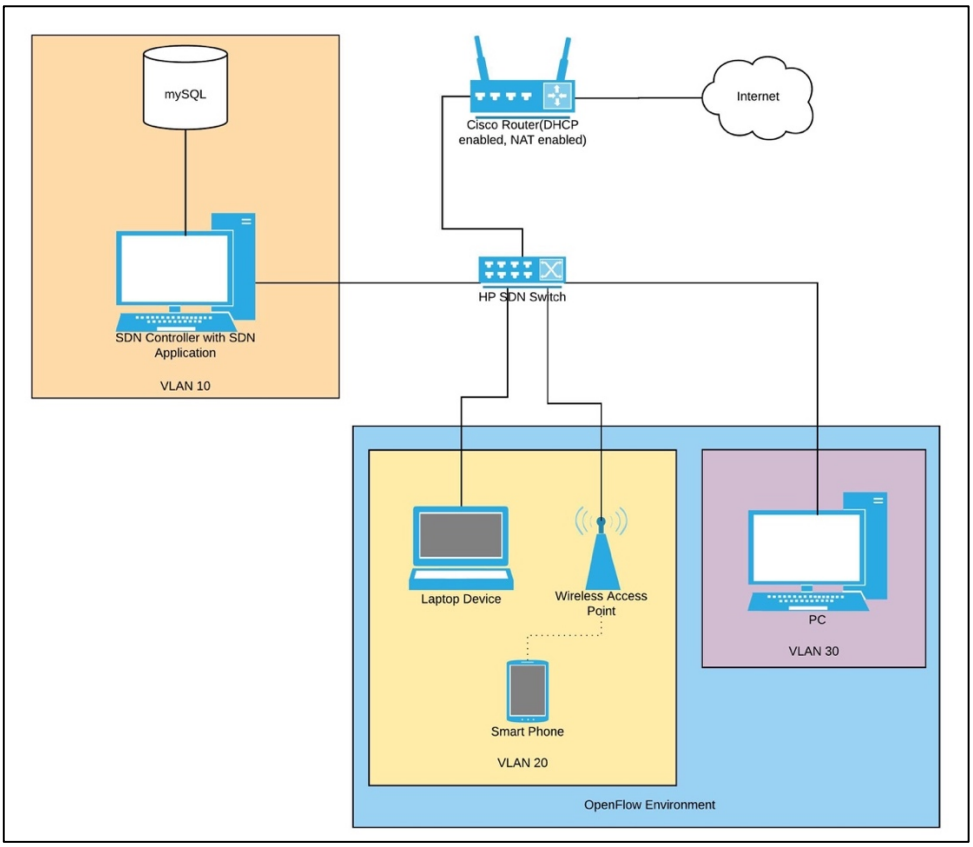


Figure 5-1-F1 Network Topology

The SDN controller is assign to VLAN10, where there is a laptop, smartphone, wireless access point is assign to VLAN20 known as student group and lastly a desktop is assign to VLAN30 known as lecturer group.

There is also a router connect to the SDN switch and ISP site. The router act as a DHCP server to provide IP address for the

SDN network host. Beside that, the router also acts as a gateway to the Internet.

5.1.2 Configure HP Switch

I have created three VLAN in the HP switch which is VLAN10 for the controller, VLAN20 for the student group and VLAN30 for the lecturer group. After that, I assign port 1-9 to VLAN10, port 11-15 to VLAN20 and port 16-20 to VLAN30. In order to let all the VLAN go to the router site, I have configured port 24 as a trunk port.

After that, I have to create an Openflow instance and controller id in the switch in order to enable the OpenFlow function in the switch.

All the switch configuration has shown in Table 5-1-T1 in step by step. A console cable is needed to connect to the switch and use terminal to access the switch. All the command need to enter in the console.

Step 1: Access to switch configure terminal	
Command	**sdnFYP#** configure terminal
Step 2: Create VLAN and Trunk Port	
Command	**sdnFYP(config)#** trunk 24 trk1 **sdnFYP(config)#** vlan10 **sdnFYP(vlan-10)#** untagged 1-9 **sdnFYP(vlan-10)#** tagged trk1 **sdnFYP(config)#** vlan 20 **sdnFYP(vlan-20)#** untagged 11-15 **sdnFYP(vlan-20)#** tagged trk1

	sdnFYP(config)# vlan 30 **sdnFYP(vlan-30)#** untagged 16-20 **sdnFYP(vlan-30)#** tagged trk1
Step 3: Create controller id and OpenFlow instance	
Command	**sdnFYP(config)#** openflow **sdnFYP(openflow)#** controller-id 1 ip 192.168.10.1 controller-interface vlan 10 **sdnFYP(openflow)#** instance opendaylight **sdnFYP(of-inst-opendaylight)#** member vlan 20,30 **sdnFYP(of-inst-opendaylight)#** controller-id 1 **sdnFYP(of-inst-opendaylight)#** version 1.3 **sdnFYP(of-inst-opendaylight)#** default-miss-action output-normal **sdnFYP(of-inst-opendaylight)#** software-flow-table 2
Step 4: Start Openflow Instance	
Command	**sdnFYP(of-inst-opendaylight)#** enable

Table 5-1-T1 Steps and commands to configure HP switch

After all the configuration have done. Connect a Fast Ethernet cable from the port-24 of the switch to the Cisco router.

5.1.3 Configure Cisco Router

In order to let the SDN host get IP address and access to the internet, I have to configure the Cisco router. What I need to configure is the DHCP service, NAT and the Routing.

All the router configuration has shown in table 5-1-T2 in step by step. A console cable is needed to connect to the router and use terminal to access the switch. All the command need to enter in the console.

Step 1: Access to router configuration terminal	
Command	**fypRouter#** configure terminal
Step 2: Create DHCP Pool	
Command	**fypRouter(config)#** ip dhcp excluded-address 192.168.10.1 **fypRouter(config)#** ip dhcp pool VLAN10 **fypRouter(dhcp-config)#** network 192.168.10.0 255.255.255.0 **fypRouter(dhcp-config)#** default-router 192.168.10.254 **fypRouter(dhcp-config)#** dns-server 8.8.8.8 **fypRouter(config)#** ip dhcp excluded-address 192.168.20.1 **fypRouter(config)#** ip dhcp pool VLAN20 **fypRouter(dhcp-config)#** network 192.168.20.0 255.255.255.0 **fypRouter(dhcp-config)#** default-router 192.168.20.254 **fypRouter(dhcp-config)#** dns-server 8.8.8.8 **fypRouter(config)#** ip dhcp excluded-address 192.168.30.1 **fypRouter(config)#** ip dhcp pool VLAN30

	fypRouter(dhcp-config)# network 192.168.30.0 255.255.255.0 **fypRouter(dhcp-config)#** default-router 192.168.30.254 **fypRouter(dhcp-config)#** dns-server 8.8.8.8
Step 3: Configure interface	
Command	**fypRouter(config)#** interface FastEthernet0/0 **fypRouter(config-if)#** ip address 192.168.209.5 255.255.255.0 **fypRouter(config-if)#** ip nat outside **fypRouter(config-if)#** no shutdown **fypRouter(config)#** interface FastEthernet0/1 **fypRouter(config-if)#** no shutdown **fypRouter(config)#** interface FastEthernet0/1.10 **fypRouter(config-subif)#** encapsulation dot1Q 10 **fypRouter(config-subif)#** ip address 192.168.10.254 255.255.255.0 **fypRouter(config-subif)#** ip nat inside **fypRouter(config)#** interface FastEthernet0/1.20 **fypRouter(config-subif)#** encapsulation dot1Q 20 **fypRouter(config-subif)#** ip address 192.168.20.254 255.255.255.0 **fypRouter(config-subif)#** ip nat inside

	fypRouter(config)# interface FastEthernet0/1.30 **fypRouter(config-subif)#** encapsulation dot1Q 30 **fypRouter(config-subif)#** ip address 192.168.30.254 255.255.255.0 **fypRouter(config-subif)#** ip nat inside
Step 4: Configure default route	
Command	**fypRouter(config)#** ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 192.168.209.250
Step 5: Configure NAT	
Command	**fypRouter(config)#** access-list 20 permit 192.168.0.0 0.0.255.255 **fypRouter(config)#** ip nat pool NAT-POOL 192.168.209.10 192.168.209.20 netmask 255.255.255.0 **fypRouter(config)#** ip nat inside source list 20 pool NAT-POOL overload

Table 5-1-T2 Steps and Commands to configure Cisco Router

5.1.4 Configure TP-Link Wireless Access Point

In order to provide wireless connection, I decide to setup a wireless access point. The wireless access point is connect to switch port 12 and assign to VLAN20. I also have assigned an IP address for the access point which is 192.168.20.1.The steps to configure the wireless access point is show below.

Step 1: Access to the wireless access point

The default IP address for the wireless access point is 192.168.0.1. Launch a web browser and enter the IP address. The username and password for the access point is “admin”. Figure 5-1-F2 show the dashboard of the access point.

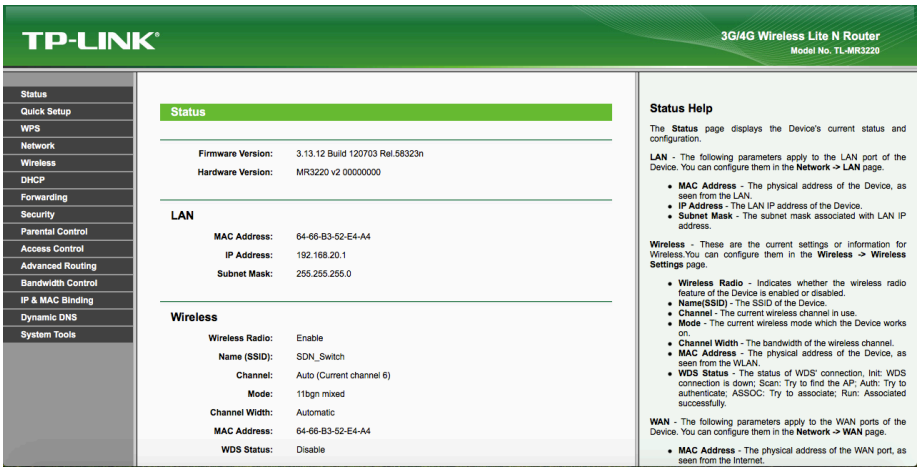


Figure 5-1-F2 Wireless access point Dashboard

Step 2: Change the IP address of the Access Point

The default IP address have to change to under the VLAN20 Subnet. Select Network at the side navigation bar and click LAN.

After that, change the IP address to 192.168.20.1 and select the subnet mask which is 255.255.255.0.

After finish changing the IP address, the access point will prompt and ask for restart. When the access point finish restart, access to the wireless point by using the new IP which is 192.168.20.1.

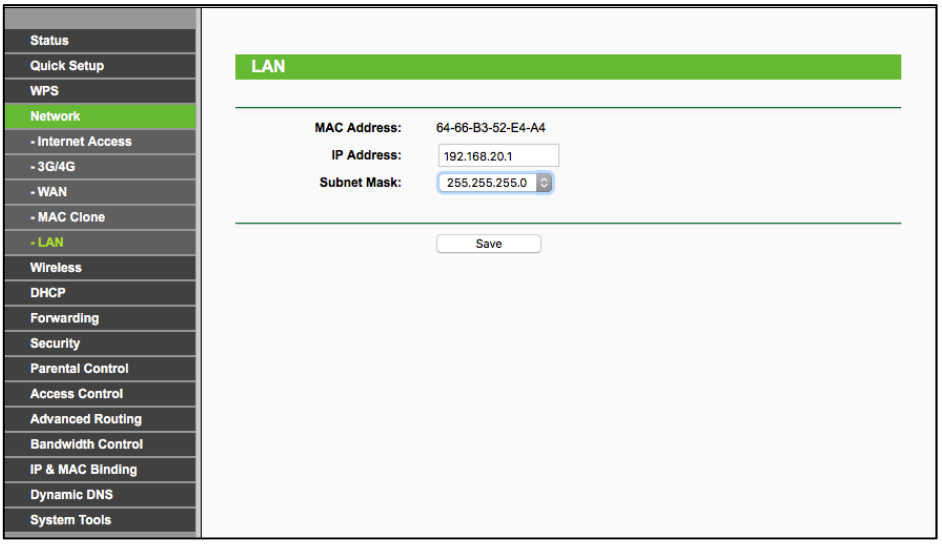


Figure 5-1-F3 Access Point LAN Page

Step 3: Wireless Setting

The wireless function should configure. Select the wireless form the side navigation bar and click Wireless Settings.

After that, change the Wireless Network Name to “SDN_switch” then click save button.

Moreover, configure the wireless security. Select Wireless and click wireless security. Then select “WPA/WPA2” and enter “fyp123456” as the password and click save button.

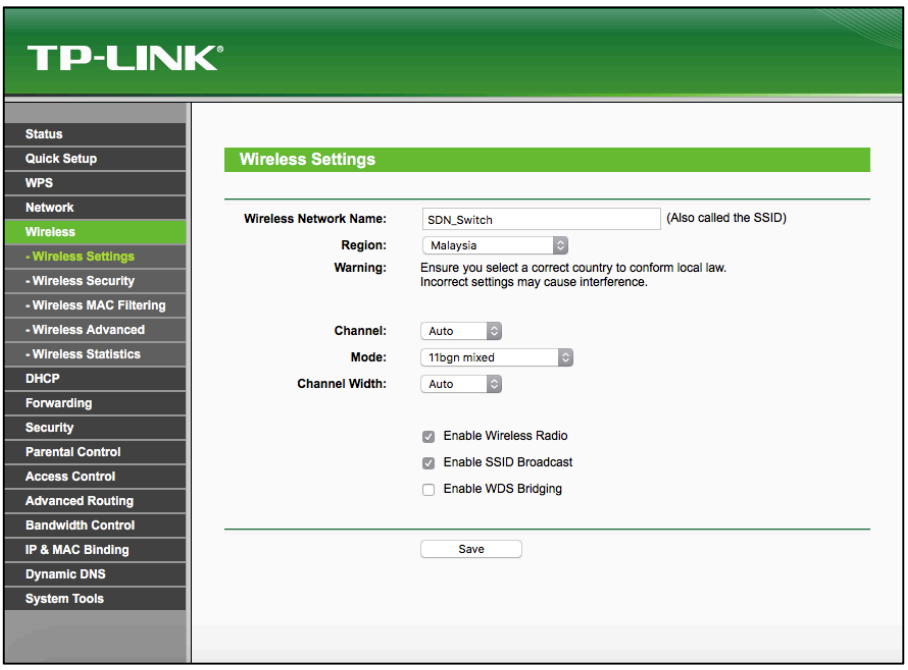


Figure 5-1-F4 Access Point Wireless Settings

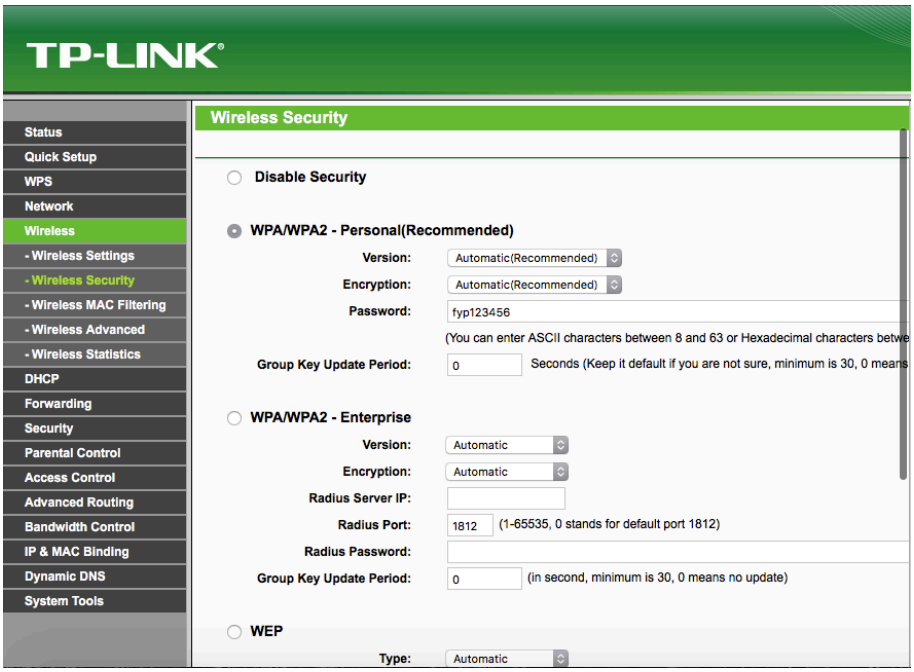


Figure 5-1-F5 Access Point wireless security

Step 4: Disable DHCP Function

The Cisco router has provided the DHCP service, so the DHCP function in the access point need to disable. Select DHCP at the side navigation bar and click DHCP Setting. Select disable function and and click save button.

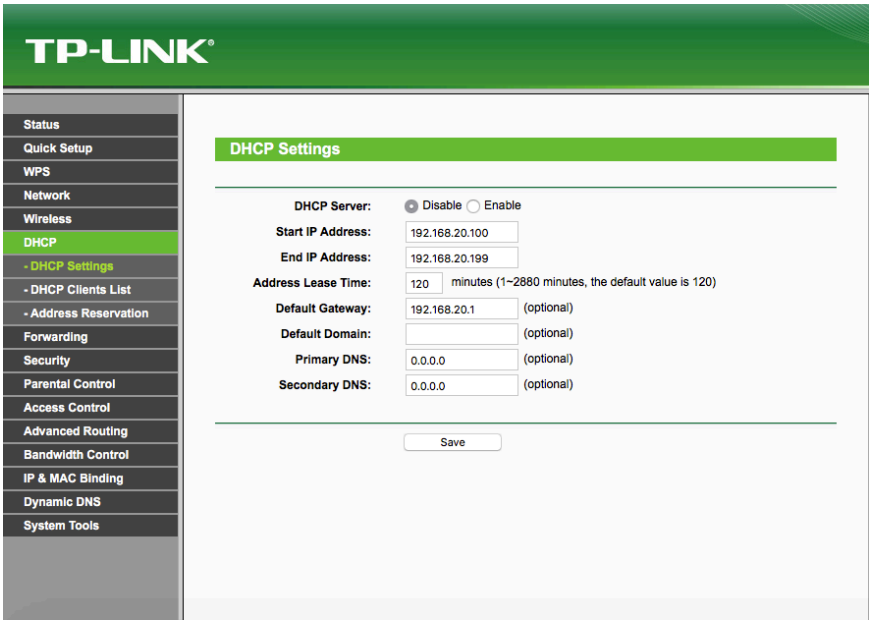


Figure 5-1-F6 Access Point DHCP function

5.1.5 SDN Controller

A desktop will be use as SDN controller. The desktop is running Ubuntu 14.04 LTS operating system. Based on the network topology in figure 5-1-F1, the desktop is connect to the SDN switch and assign with a static IP address which is 192.168.10.1. The desktop is belong to VLAN10.

5.1.6 Smartphone and PC

There are one smartphone, one laptop and one desktop will be act as the SDN network host in this project.

The smartphone that will be use is Sony Xperia Z3 running Android 6.0 operating system. The smartphone connects to the SDN network by using wireless connection and the IP address of the smartphone will be get from the Cisco router.

Moreover, the laptop that will be use is Apple MacBook Pro running MAC OSX Sierra operating system. The laptop is directly connected to the port 13 of the SDN switch and the IP address will be get from the Cisco router.

Lastly, the desktop that will be use is Acer Veriton running Ubuntu 14.04 LTS operating system. The desktop is directly connected to the port 20 of the SDN switch and the IP address will be get from the Cisco router.

The smartphone and the laptop will be assign to VLAN20 and act as student group device where the desktop will be assign to VLAN30 and act as lecturer group device.

5.2 Software Setup

5.2.1 Install and configure Open Daylight

Open Daylight is an open source SDN controller platform. It can be download from the official website. The download link is provided below.

https://nexus.opendaylight.org/content/repositories/opendaylight.release/org/opendaylight/integration/distribution-karaf/0.3.4-Lithium-SR4/distribution-karaf-0.3.4-Lithium-SR4.zip

The step of install and configure Open Daylight shows below.

Step 1: Download the Open Daylight to the controller

Step 2: Unzip the downloaded file.

Step 3: Launch the terminal and navigate to the unzipped folder.

Step 4: Start the Open Daylight Program using the following command "./bin/karaf". If the controller run successfully it will show the starting page in the terminal shown in figure 5-2-F1.

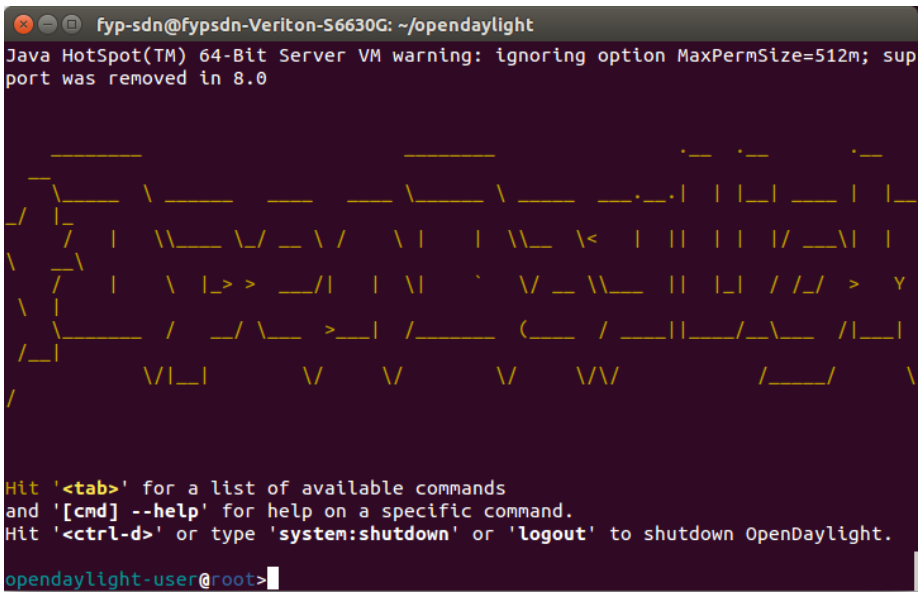


Figure 5-2-F1 Open Daylight Start Page

Step 5: Install the feature for the Open Daylight by using the following command “feature:install odl-restconf odl-l2switch-switch odl-mdsal-apidocs odl-dlux-core”

Step 6: Shutdown the Open Daylight Controller by using the following command “logout”.

Step 7: In order to let the open Daylight compatible with the HP switch, the source file of the open Daylight need to modified. Navigate to the Open Daylight in file explorer. Go to “etc” folder then to “opendaylight” folder then to karaf folder. The directory is “etc/opendaylight/karaf”. After that, look for the several file and modify it which is “52-loopremover.xml”, “54-arphandler.xml”, “58-l2switchmain.xml”.

First open the “52-loopremover.xml” file and change the value in “<lldp-flow-table-id>” tag to 200, then save it and close. Figure5-2-F2 show the 52-loopremover.xml file.

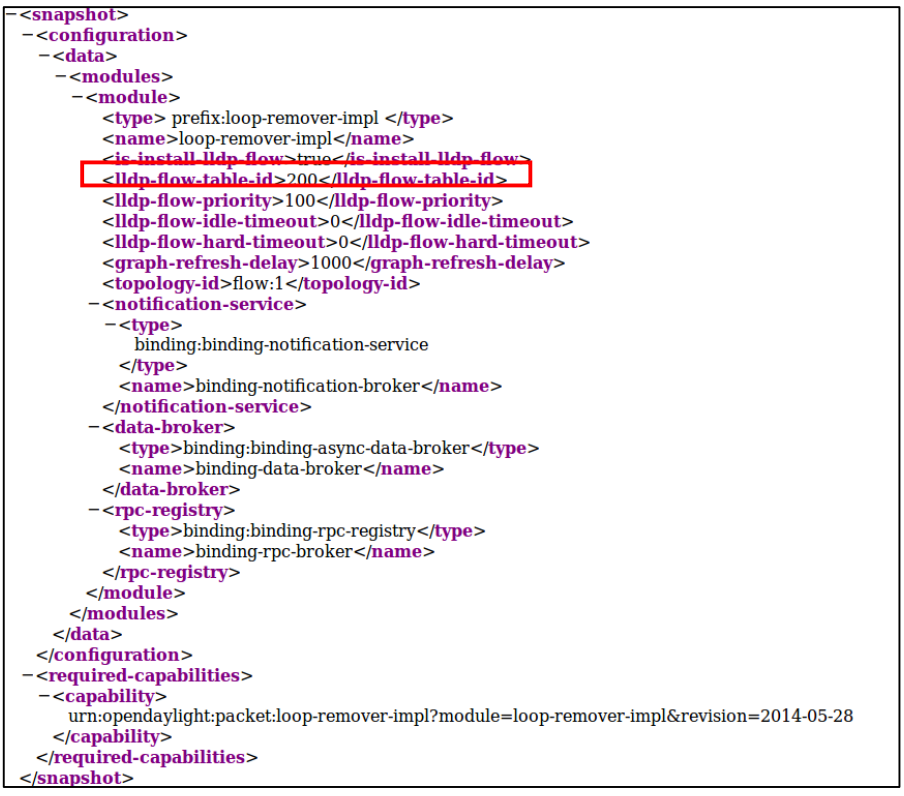


Figure 5-2-F2 52-loopremover.xml File

After that, open "54-arphandler.xml" file. Change the value in "<arp-flow-table-id>" tag and "<flood-flow-table-id>" tag to 200 then save it and close. Figure 5-2-F3 show the 54-arphandler.xml file.

Figure 5-2-F3 54-arphandler.xml File

Moreover, open file "58-l2switchmain.xml" file. Change the value in "<dropall-flow-table-id>" tag and "<reactive-flow-table-id>" tag to 200 then save it and close. Figure 5-2-F4 show the 58-l2-switchmain.xml file.

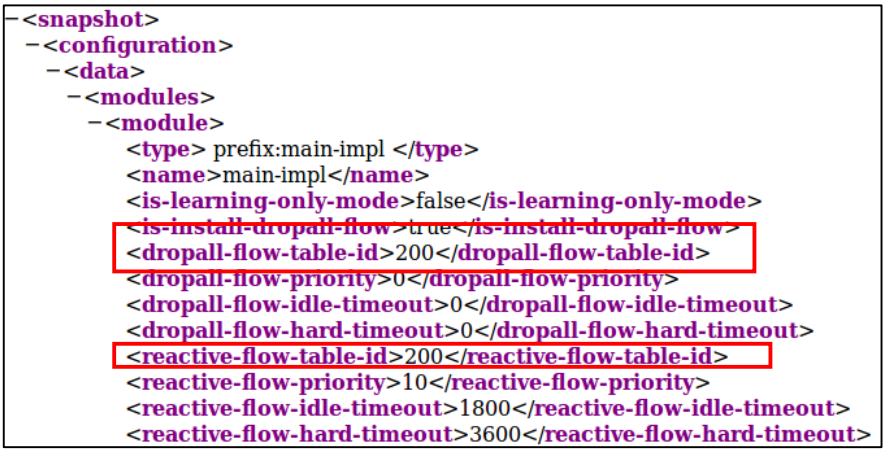


Figure 5-2-F4 58-l2switchmain.xml

Step 8: Launch terminal and run the Opendaylight Program by using the following command "./bin/karaf".

Step 9: The Open Daylight is running in the controller pc and compatible with HP switch.

5.2.2 Setup Apache server and MySQL

Since the Web-based GUI SDN Application is a web-based system. So the controller desktop have to install Apache server and MySQL. XAMPP has been chosen because XAMPP include both Apache server and MySQL.

Step 1: Download XAMPP form the internet. The download link is provided below.
https://www.apachefriends.org/xampp-files/5.6.30/xampp-linux-x64-5.6.30-0-installer.run

Step 2: Launch the terminal and navigate to the download folder. After that, use the following command to make the installer file executable “chmod +x xampp-linux-x64-5.6.30-0-installer.run”.

Step 3: Install the XAMPP require the super user privilege. Use the following command to run the installer “sudo ./xampp-linux-x64-5.6.30-0-installer.run”, then enter the super user password to proceed.

Step 4: The installer will open a graphical setup wizard. Just follow the instruction show in the window to install the XAMPP.

Step 5: The XAMPP was successfully install in the controller desktop.

5.2.3 Install ssh2 Extension for PHP

The SDN application have the time scheduling function, it use the Linux scheduler to run the process. In order to use this function, SSH2 extension need to add in to the PHP in order the application able to establish SSH connection to the controller system.

Step 1: Launch terminal and enter the following command "sudo apt-get install libssh2-1-dev libssh2-php" to install ssh2 extension, then enter the super user password to proceed.

Step 2: After the installation finish, run the following command "php –m | grep ssh2", the SSH2 should appear.

Step 3: run the following command "sudo service apache2 restart" to restart the apache server.

5.2.4 Install NetBean

The web-based GUI SDN Application is developed by using NetBean. In order to run the application, NetBean need to install in the controller pc.

Step 1: Download the NetBean installer from the official website. The download link is provided below.
http://download.netbeans.org/netbeans/8.2/final/bundles/netbeans-8.2-linux.sh

Step 2: After finish download, launch the terminal and navigate to the download folder. Then, use the following code to make the installation file executable "chmod +x netbeans-8.1-php-linux-x64.sh".

Step 3: Install the NetBeans require the super user privilege. Use the following command to run the installer "sudo ./netbeans-8.1-php-linux-x64.sh", then enter the super user password to proceed.

Step 4: The installer will open a graphical setup wizard. Just follow the instruction show in the window to install the NetBeans.

Step 5: The NetBeans was successfully install in the controller desktop.

5.3 System Operation

5.3.1 Start Open Daylight Controller

In order to start the Open Daylight Controller, launch the terminal and navigate to the Open Daylight folder. After that, run the following command "./bin/karaf" and the Open Daylight should start successfully. Figure 5-3-F1 show the window when the controller successfully run.

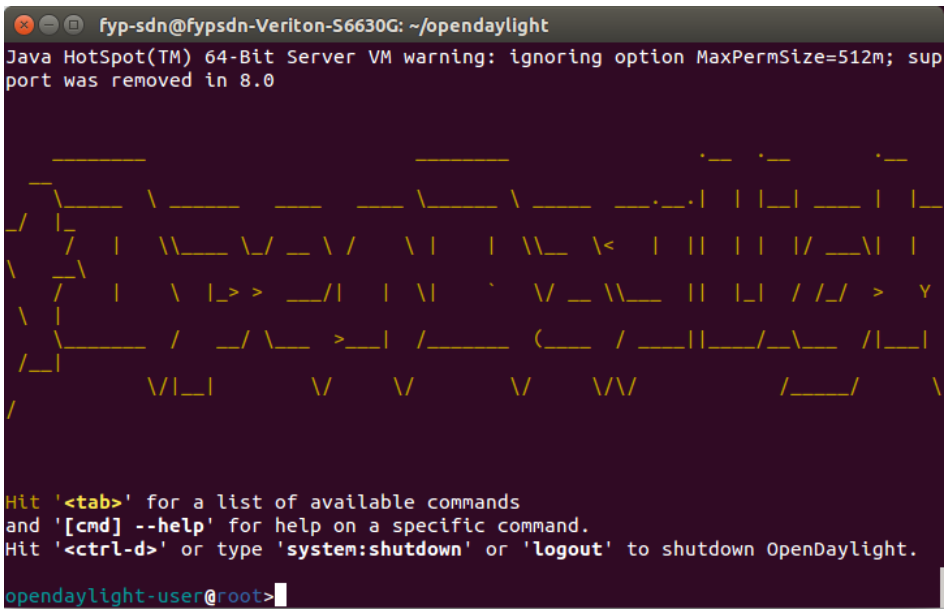


Figure 5-3-F1 Open Daylight Start Window

After that, open a web browser and enter the following address "localhost:8181/index.html" should able to access the Open Daylight login page. The username and password is "admin" to login to Open Daylight GUI. Figure 5-3-F2 show the login page of Open Daylight.

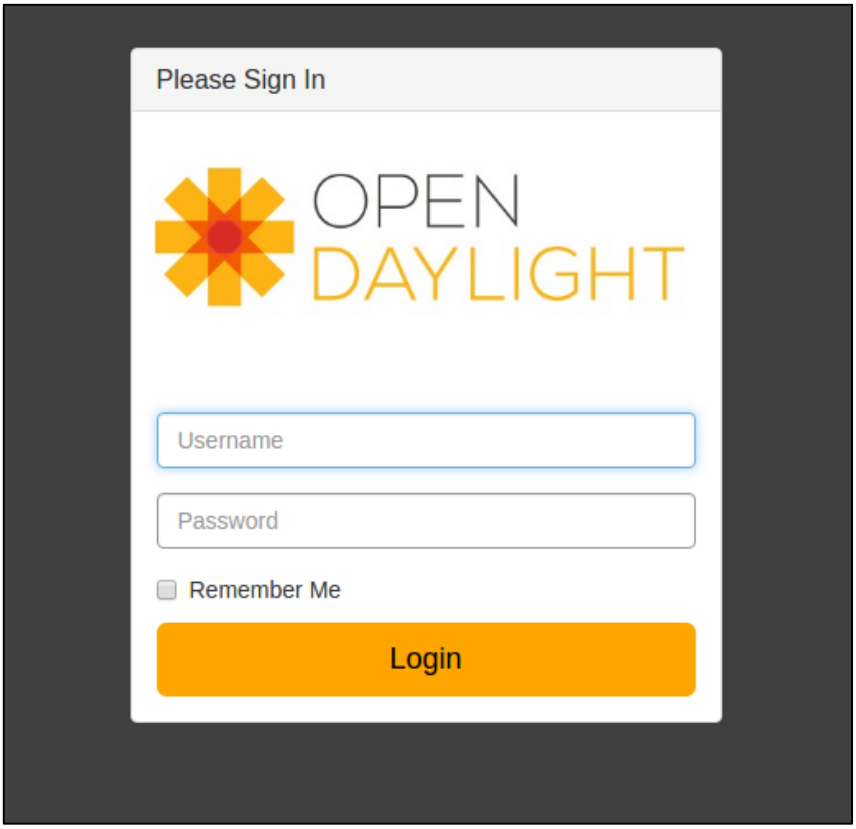


Figure 5-3-F2 Open Daylight Login Page

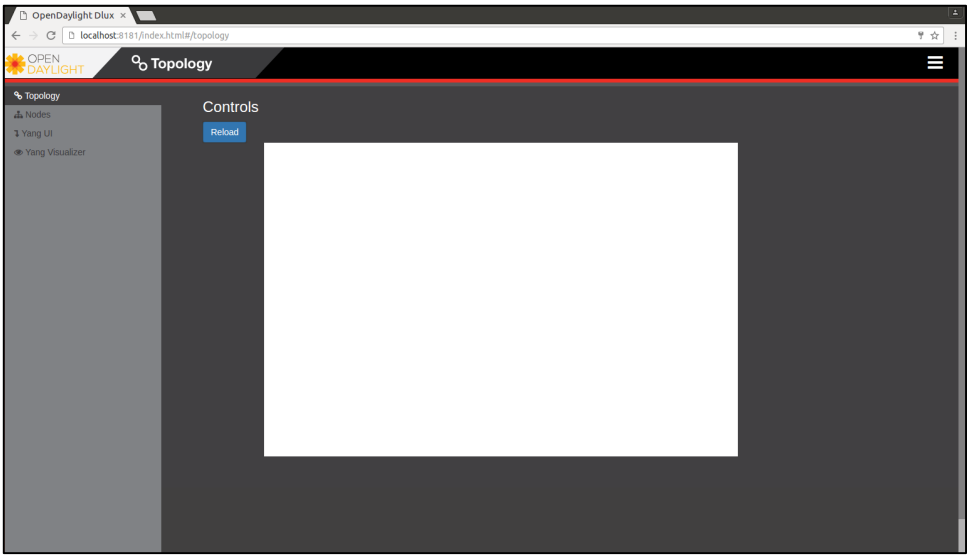


Figure 5-3-F3 Open Daylight GUI Home Page

5.3.2 Enable OpenFlow function in HP Switch

In order to start the SDN network environment, an OpenFlow instance and Controller has created and configure in the HP switch. The steps and commands to enable OpenFlow Protocols and OpenFlow instance in HP switch show below.

Steps 1: enable OpenFlow Protocols	
Command	sdnFYP(config)# openflow sdnFYP(openflow)# enable
Step 2 : enable OpenFlow Instance	
Command	sdnFYP(openflow)# instance opendaylight sdnFYP(pf-inst-opendaylight)# enable

After the OpenFlow Protocols and OpenFlow Instance has been enabled, the following command can help to check for the status which is "*show openflow*" able to view the status of the openflow protocol and the status of the openflow instance, "*show openflow controllers*" able to view all the controller create in the switch and "*show openflow instance opendaylight*" able to view the information about instance opendaylight and the connectivity status between the controller. Figure 5-3-F4 show "show openflow" command output, Figure 5-3-F5 show "show openflow controllers" command output and Figure 5-3-F6 show "show openflow instance opendaylight " command output.

```
OpenFlow                    : Enabled
Egress Only Ports Mode      : Disabled

Instance Information

                                                 No. of     No. of     OpenFlow
 Instance Name                    Oper. Status   H/W Flows  S/W Flows  Version
 -------------------------------- ------------ ---------- ---------- --------
 opendaylight                     Up           2          13         1.3
```

Figure 5-3-F4 "show openflow" Command Output

```
sdnFYP(of-inst-opendaylight)# show openflow controllers

 Controller Information

 Controller Id IP Address               Port   Interface
 ------------- ------------------------ ------ --------------
 1             192.168.10.1             6633   VLAN 10
```

Figure 5-3-F5 “show openflow controllers” Command Output

```
sdnFYP(of-inst-opendaylight)# show openflow instance opendaylight

 Configured OF Version          : 1.3
 Negotiated OF Version          : 1.3
 Instance Name                  : opendaylight
 Data-path Description          :
 Administrator Status           : Enabled
 Member List                    : VLAN 20,30

 Pipeline Model                 : Standard Match
 Listen Port                    : 6633
 Operational Status             : Up
 Operational Status Reason      : NA
 Datapath ID                    : 001440a8f0ced3c0
 Mode                           : Active
 Flow Location                  : Hardware and Software
 No. of Hardware Flows          : 2
 No. of Software Flows          : 13
 Hardware Rate Limit            : 0 kbps
 Software Rate Limit            : 100 pps
 Conn. Interrupt Mode           : Fail-Secure
 Maximum Backoff Interval       : 60 seconds
 Probe Interval                 : 10 seconds
 Hardware Table Miss Count      : NA
 No. of Software Flow Tables    : 1
 Egress Only Ports              : None
 Table Model                    : Policy Engine and Software
 Source MAC Group Table         : Disabled

 Default Miss Action            : Output-Normal
 Packet-In VLAN Tagging         : Default

 Controller Id Connection Status Connection State Secure Role
 ------------- ----------------- ---------------- ------ ------
 1             Connected         Active           No     Master
```

Figure 5-3-F6 “show openflow instance opendaylight” Command Output

After that, back to the Open Daylight GUI should be able to view a network topology with a SDN switch and all host connected to the switch. Figure 5-3-F7 show the Open Daylight main page with network topology.

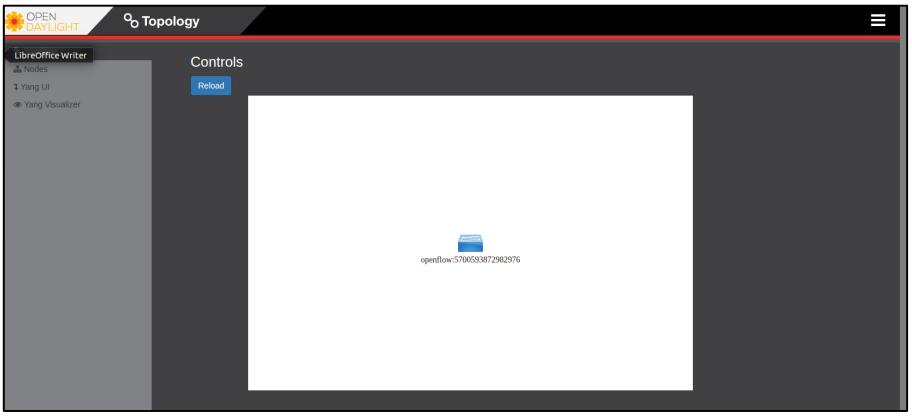


Figure 5-3-F7 Open Daylight Main Page with Network Topology

5.3.3 Start Web-based GUI SDN Application

After the SDN controller and HP switch connect to each other, the Web-based SDN GUI Application can be start.

Launch NetBeans IDE and open the project in the NetBeans, then click run project. The NetBeans will start the webserver automatically and open a web browser to access the application. Figure 5.3.F8 show the login in page of the application.

Figure 5-3-F8 Login Page of the System

After login into the system, then can perform the function like access control or bandwidth control.

5.4 Concluding Remark

This chapter shows the step on how to setup and configure all the hardware and software needed in the project. All the configure are very important and must configure right else the whole system could not be work. Moreover, Web-based GUI SDN Application is only the main system that implement Network Administration System for Bring Your Own Device into the SDN network.

6.0 System Evaluation and Discussion

6.1 System Testing and Performance Metrics

In this chapter, each function module will be test by using different test case and policy.

For the device register module, the test case set for this module is to test the host whether able to get the IP from the DHCP server. Theoretically when a device connects to a network, the first packet sent by the host is DHCP discovery packet in order to look for a DHCP server at the network and get a usable IP address from the server. By default, the SDN switch will drop all the packet sent by unrecognized device including the discovery packet. If the device had registered, then the switch will forward the DHCP packet and the device will able to get the IP address and connected to the network successfully.

For the normal access control module and group policy module, the test case for these modules is to test the host in the SDN network whether able to reach the destination by using ping. Ping is a very useful tools to test the connectivity between two host. If the access control policy is set to block some site, then the host would not be able to reach the site.

For the schedule access control module, the test case for this module is to test the host whether able to reach the destination in certain time. While ping tools be used to test this module and set a range of time to test it.

Lastly, for the bandwidth control module, the test case for this module is to test the host bandwidth by using www.speedtest.net. This website provides a service to let user to test their Internet bandwidth.

Each module will be test in two condition which is OpenFlow protocols disable in the HP switch and OpenFlow enabled in the HP switch.

6.2 Testing Setup and Result

6.2.1 Testing on Device Register Module

In this module, each device will be test whether able to get IP address from the DHCP server. The device that used for testing show in the table below.

Device	MAC Address	User Group	Status
Apple MacBook Pro	a2:2f:65:35:7f:91	Student	Registered
Sony Xperia Z3	ba:6f:64:76:bf:cd	Student	Unregistered
Dell Veriton	15:a1:89:79:8b:ac	Lecturer	Registered

Table 6-2-T1 Device used for Test Device Register Module

Condition 1: OpenFlow Protocols Disable

In condition 1, the OpenFlow Protocols will be disabled in the HP switch. The testing result is shows below.

Device	User Group	Status	IP address
Apple MacBook Pro	Student	Able to get the IP address from DHCP server	192.168.20.21
Sony Xperia Z3	Student	Able to get the IP address from DHCP server	192.168.20.22
Dell Veriton	Lecturer	Able to get the IP address from DHCP server	192.168.10.2

Table 6-2-T2 Device Register Module Test Result(Condition 1)

In the condition 1, all the device able to get the IP address from the DHCP server. When the OpenFlow Protocols in the HP is

disabled, the SDN switch is just like a normal switch that perform packet forward function.

Condition 2: OpenFlow Protocols Enabled

In condition 2, the OpenFlow protocols is enabled in the switch. The testing result is shows below.

Device	**User Group**	**Status**	**IP address**
Apple MacBook Pro	Student	Able to get the IP address from DHCP server	192.168.20.21
Sony Xperia Z3	Student	No able to get the IP address from DHCP server	-
Dell Veriton	Lecturer	Able to get the IP address from DHCP server	192.168.10.2

Table 6-2-T3 Device Register Module Test Result(Condition 2)

In condition 2, Apple MacBook Pro and Dell Veriton able to get the IP address from the DHCP server, where Sony Xperia Z3 cannot get the IP from the DHCP server.

Sony Xperia Z3 is an unregistered device, the SDN don't have any information about the device. When Xperia Z3 send a DHCP request to the through the switch, the switch will directly drop the packet, so the Xperia Z3 will not able to get any reply from the DHCP server.

6.2.2 Testing on Access Control Module

In this module each device will be tested whether can reach the destination. The device that use for testing show in the table below.

Device	User Group	IP Address
Apple MacBook Pro	Student	192.168.20.21
Sony Xperia Z3	Student	192.168.20.22
Dell Veriton	Lecturer	192.168.30.2

Table 6-2-T4 Device Used for Test Access Control Module

Policy that used to test for the module show in the table below.

No.	Domain Name	Public IP	Subnet Mask	Priority	Action
1	www.utar.edu.my	58.27.19.137	/32	1000	Drop
2	www.utar.edu.my	58.27.19.137	/32	1001	Allow
3	www.vimeo.com	151.101.0.0	/16	1000	Drop
4	portal.utar.edu.my	58.27.19.139	/32	1000	Drop
6	All UTAR Site	58.27.19.128	/28	1100	Drop

Table 6-2-T5 Policy used to Test Access Control Module

The destination site that used to test for the module show in the table below.

No	Name	Domain Name	Public IP
1	UTAR website	www.utar.edu.my	58.27.19.137
2	UTAR student portal	portal.utar.edu.my	58.27.19.139
3	UTAR wble	wble.utar.edu.my	58.27.19.142
5	Vimeo	www.vimeo.com	151.101.0.217
6	Google	www.google.com	172.217.20.164

Table 6-2-T6 Destination Site used for Test Access Control

Condition 1: OpenFlow Disabled

In condition 1, the OpenFlow protocols is disabled in the switch. The policy that apply to this condition is policy 1,2 and 3. The ping test result show below.

Host	Destination			
	UTAR Website	**UTAR Wble**	**Vimeo**	**Google**
MacBook Pro	Success	Success	Success	Success
Xperia Z3	Success	Success	Success	Success
Dell Veriton	Success	Success	Success	Success

Table 6-2-T7 Access Control Test Result (Condition 1)

Since the OpenFlow protocols is disabled in the switch and the switch is just act as a normal switch to forward all the packet. So all the devices are successfully ping with all the destination sites.

Condition 2: OpenFlow Enable

In condition 2, the OpenFlow protocols is enabled in the switch.

Test Case 1(basic policy rules): Applied Policy 1 and Policy 4

The policy 1 shows that is to block the access to UTAR website where policy 4 shows that to block the UTAR student portal. The ping test result show below.

Host	Destination				
	UTAR Website	**UTAR Wble**	**Vimeo**	**Google**	**UTAR student Portal**
MacBook Pro	Failed	Success	Success	Success	Failed
Xperia Z3	Failed	Success	Success	Success	Failed
Dell Veriton	Failed	Success	Success	Success	Failed

Table 6-2-T8 Access Control Test Result (Condition 2) - Test Case 1

From the result shows at Table 6-2-T8 all the device failed to reach UTAR website and UTAR student portal where UTAR

wble, Vimeo and Google was able to reach. The policy had successfully block the access to the UTAR website and UTAR student portal.

Test Case 2 (priority issue): Applied policy 1 and policy 2

The policy 1 shows that is to block the access to UTAR website with priority 1000 where policy 2 shows that is to allow to access to UTAR website with priority 1001. The ping test result show below.

Host	**Destination**				
	UTAR Website	**UTAR Wble**	**Vimeo**	**Google**	**UTAR student Portal**
MacBook Pro	Success	Success	Success	Success	Success
Xperia Z3	Success	Success	Success	Success	Success
Dell Veriton	Success	Success	Success	Success	Success

Table 6-2-T9 Access Control Test Result (Condition 2) – Test Case 2

From the result shows at Table 6-2-T9, all the device is able to reach the UTAR website. Although policy 1 is to block the access to UTAR website but the priority of the policy 1 is lower than policy 2. So the SDN switch will choose the highest priority policy if the domain name of the two policy is same. The SDN will choose policy 2 which to allow the access to UTAR website.

Test Case 3 (subnet mask issue): Applied policy 3 and policy 4

Policy 3 shows that is to block the access to Vimeo, where policy 4 shows that is to block all the access to all the UTAR site such as UTAR website, UTAR student portal, UTAR wble and more. The ping test result shows below.

Host	**Destination**				
	UTAR Website	**UTAR Wble**	**Vimeo**	**Google**	**UTAR student Portal**
MacBook Pro	Failed	Failed	Failed	Success	Failed
Xperia Z3	Failed	Failed	Failed	Success	Failed
Dell Veriton	Failed	Failed	Failed	Success	Failed

Table 6-2-T10 Access Control Test Result (Condition 2) – Test Case 3

From the result shows at Table 6-2-T10 all the devices are not able to reach Vimeo and all UTAR related site. The main purpose of this test case is to show that if admin want to block the access to all the website that are related or from a same company like all the UTAR site such as UTAR official site, UTAR student portal, UTAR course register site and more, admin don't have to insert the policy one by one for each site because one policy only can insert one IP address. Admin just need to calculate from the IP and get the range of these IP addresses and the subnet mask then add into the policy will do.

6.2.3 Testing on Schedule Access Control Module

In this module each device will be tested whether can reach the destination in certain time constraint. The device that use for testing show in the table below.

Device	User Group	IP Address
Apple MacBook Pro	Student	192.168.20.21
Sony Xperia Z3	Student	192.168.20.22
Dell Veriton	Lecturer	192.168.30.2

Table 6-2-T11 Device Used to Test Schedule Access Control

Policy that used to test for the module show in the table below.

No.	Domain Name	Days	Start Time	End Time	Action
1	www.utar.edu.my	Daily	12:30pm	2:30pm	Drop
2	www.vimeo.com	Friday	12:30pm	2:30pm	Allow
3	www.vimeo.com	Daily	9:00am	6:00pm	Drop

Table 6-2-T12 Policy Used to Test Schedule Access Control

The destination site that used to test for the module show in the table below.

No	Name	Domain Name
1	UTAR website	www.utar.edu.my
2	Vimeo	www.vimeo.com
3	Google	www.google.com

Table 6-2-T13 Destination Site Used to Test Schedule Access Control

Condition 1: OpenFlow protocols disable

In condition 1, the OpenFlow protocols is disabled in the switch. Apply Policy 1,2 and 3. The ping test result is shows below.

		9am-6pm			12pm-3pm		
Monday	**Host**	**UTAR**	**Vimeo**	**Google**	**UTAR**	**Vimeo**	**Google**
	MacBook Pro	Success	Success	Success	Success	Success	Success
	Xperia Z3	Success	Success	Success	Success	Success	Success
	Dell Veriton	Success	Success	Success	Success	Success	Success
Friday	**Host**	**UTAR**	**Vimeo**	**Google**	**UTAR**	**Vimeo**	**Google**
	MacBook Pro	Success	Success	Success	Success	Success	Success
	Xperia Z3	Success	Success	Success	Success	Success	Success
	Dell Veriton	Success	Success	Success	Success	Success	Success

Table 6-2-T14 Schedule Access Control

Test Result (Condition 1)

Since the OpenFlow protocols is disabled in the switch and the switch is just act as a normal switch to forward all the packet. So all the devices are successfully ping with all the destination sites.

Condition 2: OpenFlow Protocols Enable

In condition 2, the OpenFlow protocols is enabled in the switch.

The policy that applied is policy 1,2 and 3. Policy 1 show that is to block the access to UTAR website daily from 12pm to 2pm. Moreover, policy 2 show that is to allow the access to Vimeo by Friday from 12:30pm to 2:30pm. Lastly, policy 3 show that to block the access to Vimeo daily from 9am to 6pm. The ping test result show below.

		9am-6pm			12pm-2:30pm		
Monday	**Host**	**UTAR**	**Vimeo**	**Google**	**UTAR**	**Vimeo**	**Google**
	MacBook Pro	Success	Failed	Success	Failed	Failed	Success
	Xperia Z3	Success	Failed	Success	Failed	Failed	Success
	Dell Veriton	Success	Failed	Success	Failed	Failed	Success
Friday	**Host**	**UTAR**	**Vimeo**	**Google**	**UTAR**	**Vimeo**	**Google**
	MacBook Pro	Success	Failed	Success	Failed	Success	Success
	Xperia Z3	Success	Failed	Success	Failed	Success	Success
	Dell Veriton	Success	Failed	Success	Failed	Success	Success

Table 6-2-T15 Schedule Access Control

Test Result (Condition 2)

From the result show at Table 6-2-T15, all the device can access to UTAR and Google daily from 9am to 6pm. When the time reached 12:30pm, UTAR website not allow to access. After 2:30pm the UTAR website is allow to access. Moreover, Vimeo only allow to access by Friday during 12:30pm until 2:30pm.

6.2.4 Testing on Group Policy Module

In this module, each device will be assign into different group and test which group of the device whether able to reach the site based on the policy applied. The device information that use for the testing shows below.

Device	User Group	IP Address
Apple MacBook Pro	Student	192.168.20.21
Sony Xperia Z3	Student	192.168.20.22
Dell Veriton	Lecturer	192.168.30.2

Table 6-2-T16 Device Used to Test Group Policy

Policy that use to test the module shows below.

No.	Domain Name	User Group	Action
1	www.utar.edu.my	Student	Drop
2	www.vimeo.com	Lecturer	Allow
3	www.vimeo.com	Student	Drop

Table 6-2-T17 Policy Used to Test Group Policy

The destination site that used to test for the module show in the table below.

No	Name	Domain Name
1	UTAR website	www.utar.edu.my
2	Vimeo	www.vimeo.com
3	Google	www.google.com

Table 6-2-T18 Destination Site Used to Test Group Policy

Condition 1: OpenFlow Protocols Disabled

In condition 1, the OpenFlow protocols is disabled in the HP Switch. The ping test result is shows below.

Host	Destination		
	UTAR website	Vimeo	Google
MacBook Pro	Success	Success	Success
Xperia Z3	Success	Success	Success
Dell Veriton	Success	Success	Success

Table 6-2-T19 Group Policy Test Result (Condition 1)

Since the OpenFlow protocols is disabled in the switch and the switch is just act as a normal switch to forward all the packet. So all the devices are successfully ping with all the destination sites.

Condition 2: OpenFlow Protocols Enabled

In condition two, the OpenFlow protocols is enabled in the switch.

Test Case: Applied policy 1, 2 and 3

Policy 1 shows that the switch need to block the student group to access the UTAR website. Beside that, policy 2 show that the switch allows the lecturer group to access the Vimeo website. Moreover, the policy 3 show that the switch need to block the student group to access the Vimeo site. The ping test is result is shows below.

Host	**Destination**		
	UTAR website	**Vimeo**	**Google**
MacBook Pro	Failed	Failed	Success
Xperia Z3	Failed	Failed	Success
Dell Veriton	Success	Success	Success

Table 6-2-T20 Group Policy Test Result (Condition 2)

From the ping test result shows in Table 6-2-T20, MacBook Pro and Xperia Z3 are not able to reach the UTAR website and Vimeo website because these two device is under student group. Beside, Dell Veriton able to reach the Vimeo website because this device is under lecturer group.

There is also another point need to highlight in this test result which is all the three device able to reach google site. Since there is no any policy that block the access to google website, so by default the SDN will forward all the packet sent form recognized device to any destination if there is no any policy to drop the packet.

6.2.5 Testing on Bandwidth Control Module

In this module, each device will be assign to different group and run a speed test based on the policy applied. All the speed test result comes form www.speedtest.net. The current bandwidth subscription form the ISP is **2mbps.** The device information used for testing shows below.

Device	User Group	IP Address
Apple MacBook Pro	Student	192.168.20.21
Dell Veriton	Lecturer	192.168.30.2

Table 6-2-T21 Device Used to Test Bandwidth Control

Policy that used to test the module show below.

No.	Limited Bandwidth	User Group
1	512kbps	All
2	1mbps	All
3	512kbps	Student
4	1mbps	Student
5	512kbps	Lecturer
6	1mbps	Lecturer

Table 6-2-T22 Policy Used to Test Bandwidth Control

* All the speed test destination server set to Telekom Malaysia Berhad.

Before the testing, each device had to run a speed test that don't have any bandwidth control policy applied. The speed test result shows below.

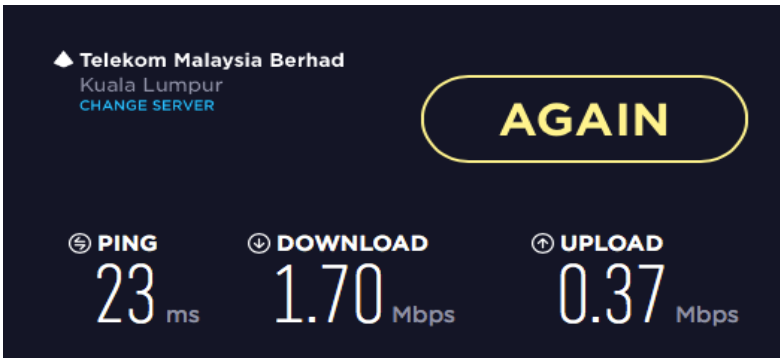
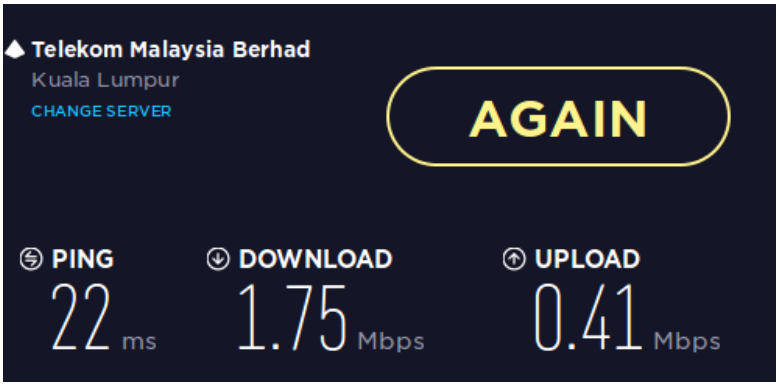
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T23 Original Bandwidth

Based on the speed test result, the download speed of the two device is around 1.70Mbps to 1.75Mbps. That's means this is the speed before the policy applied.

Condition 1: OpenFlow Protocols Disabled

In condition 1, the OpenFlow protocols is disabled in the HP Switch. The policy applied in condition 1 is policy 2 which is limit all the user group bandwidth to 1mbps. The speed test result shows below.

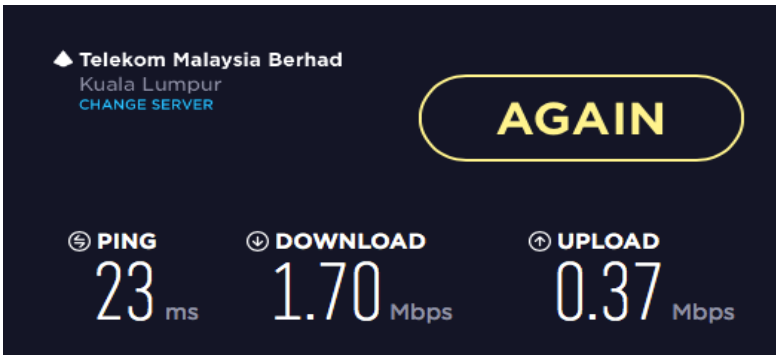
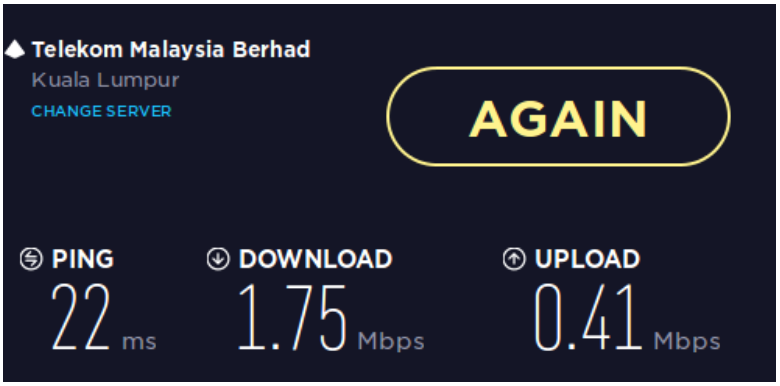
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T24 Bandwidth Control Test Result (Condition 1)

Based on the speed test result, the download speed of these two device is around 1.70Mbps to 1.75Mbps same as the download speed that don't have any policy applied. It is because the OpenFlow protocols is disable in the switch so the switch cannot perform any bandwidth control.

Condition 2: OpenFlow Protocols Enabled

In condition 2, the OpenFlow protocols is enabled in the switch. The HP switch should be able to control the bandwidth based on the policy.

Test Case 1: Applied Policy 1

Policy 1 is to limit all user group bandwidth to 512kbps. The speed test result shows below.

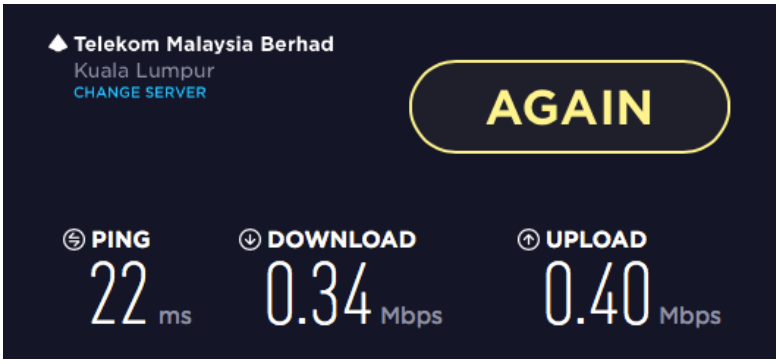
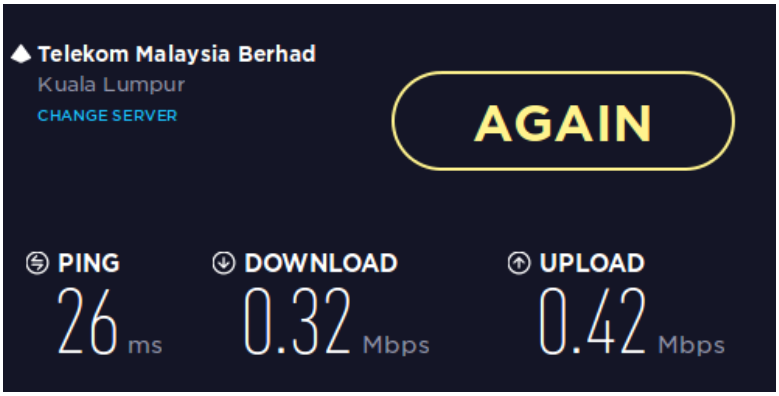
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T25 Bandwidth Control Test Result (Condition 2) – Test Case 1

Based on the speed result, the download speed of the two device around 0.32Mpbs to 0.34Mbps. Compare to the original download speed which is around 1.70Mbps to 1.75Mbps, the download speed has limited around 80% from the original speed.

Test Case 2: Applied Policy 2

Policy 2 is to limit all user group bandwidth to 1Mbps. The speed test result shows below.

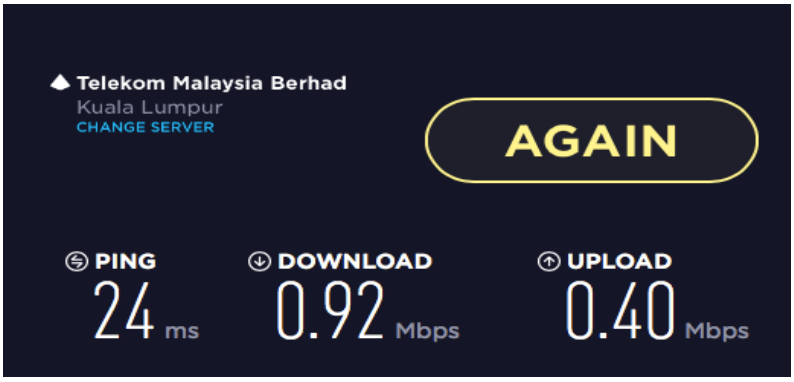
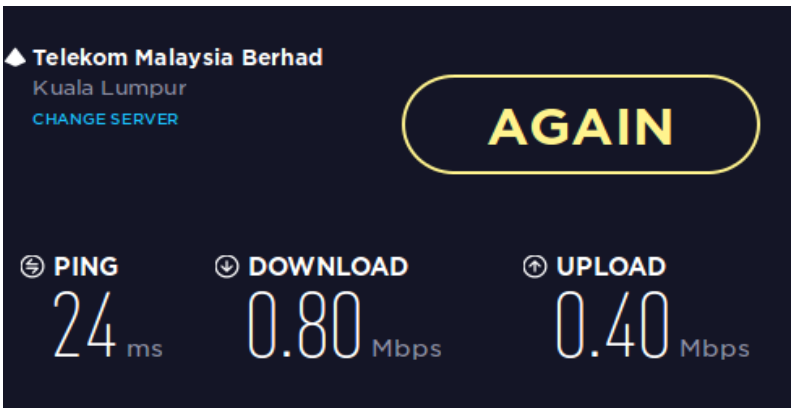
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T26 Bandwidth Control Test Result (Condition 2) – Test Case 2

Based on the speed test result, the download speed of the two device around 0.8Mbps to 0.92Mbps. Compare to the original download speed, the download speed has drop 50%.

Test Case 3: Applied Policy 3

Policy 3 is to limit student group bandwidth to 512kbps. The speed test result shows below.

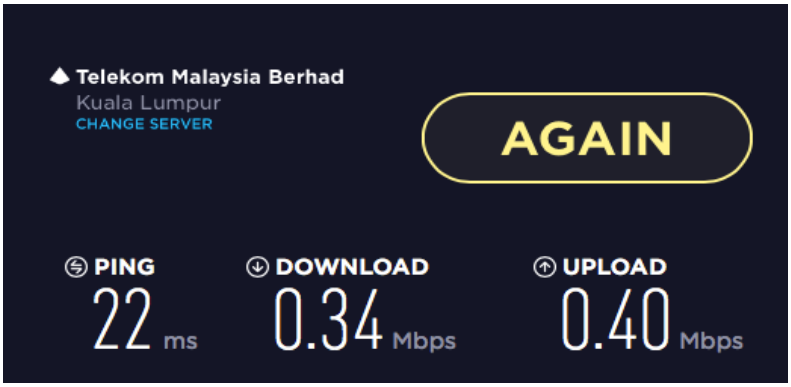
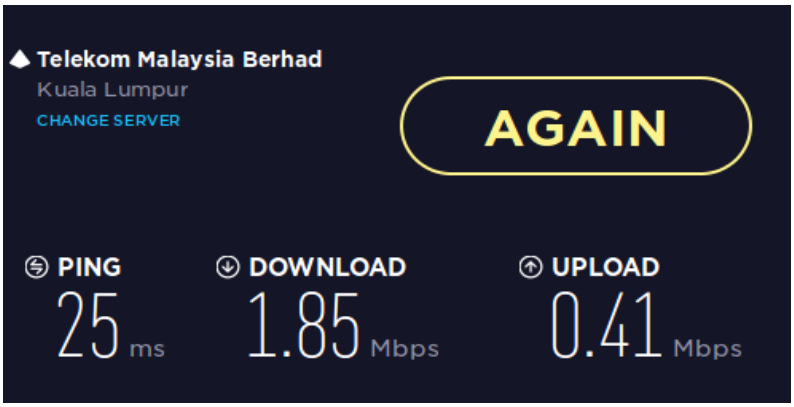
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T27 Bandwidth Control Test Result (Condition 2) – Test Case 3

Based on the speed test result, MacBook Pro is assigned to student group so the bandwidth is affected by the policy and the download speed had dropped to 0.34Mbps where Dell Veriton still remain around 1.85Mbps.

Test Case 4: Applied Policy 4

Policy 4 is to limit student group bandwidth to 1Mbps. The speed result shows below.

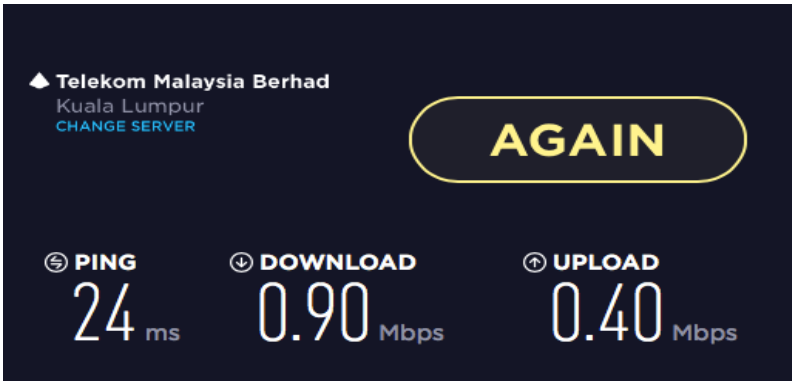
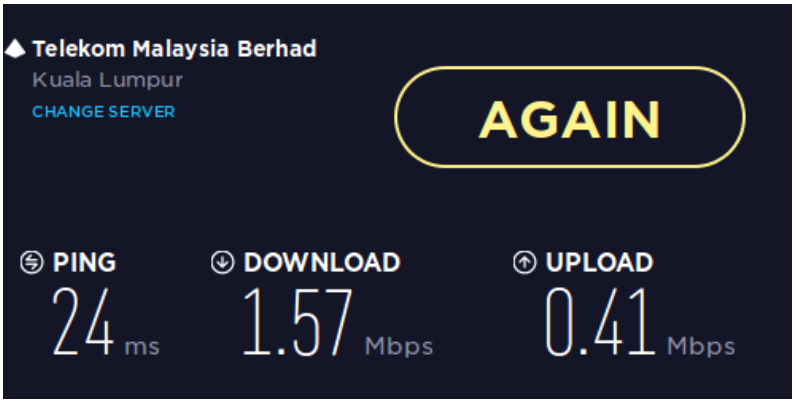
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T28 Bandwidth Control Test Result (Condition 2) – Test Case 4

Based on the speed test result, MacBook Pro is assigned to student group so the bandwidth is affected by the policy and the download speed had dropped to 0.90Mbps where Dell Veriton still remain around 1.57Mbps.

Test Case 5: Applied Policy 5

Policy 5 is to limit lecturer group bandwidth to 512Kbps. The test result is shows below.

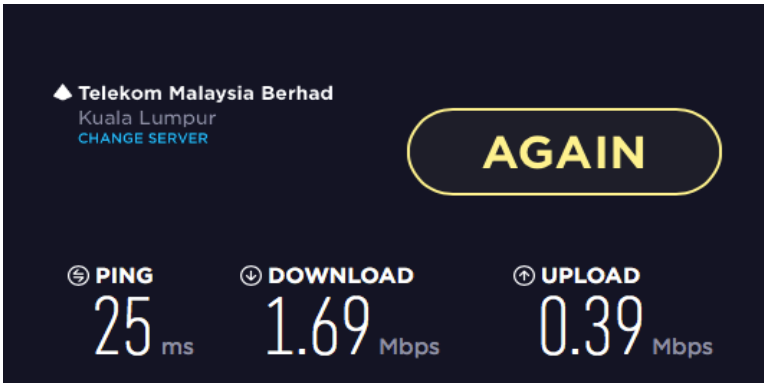
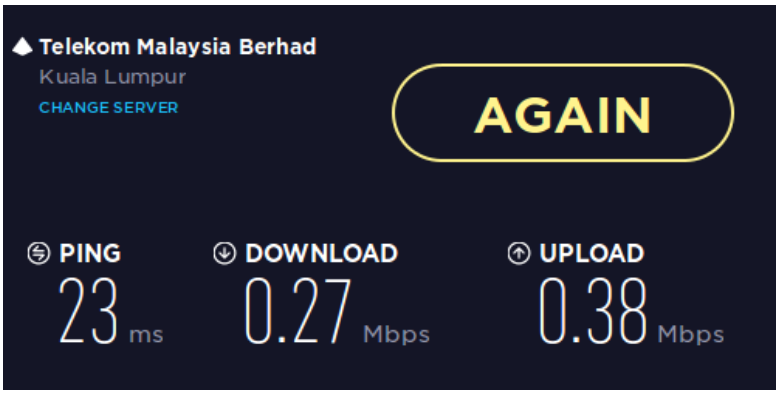
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T29 Bandwidth Control Test Result (Condition 2) – Test Case 5

Based on the speed test result, Dell Veriton is assigned to lecturer group so the bandwidth is affected by the policy and the download speed had dropped to 0.27Mbps where MacBook Pro still remain around 1.69Mbps.

Test Case 6: Applied Policy 6

Policy 6 is to limit lecturer group bandwidth to 1Mbps. The speed test result shows below.

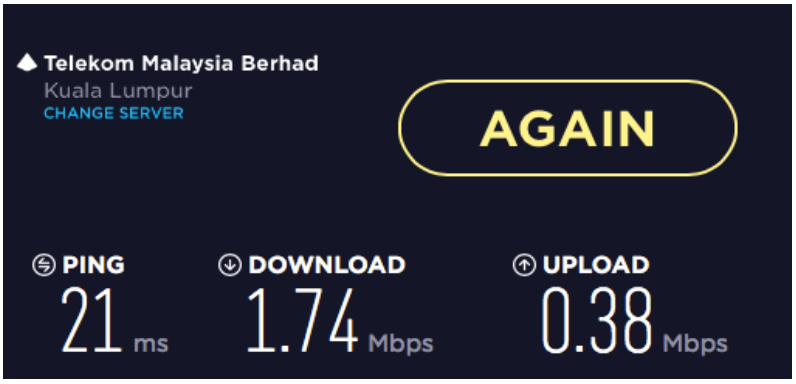
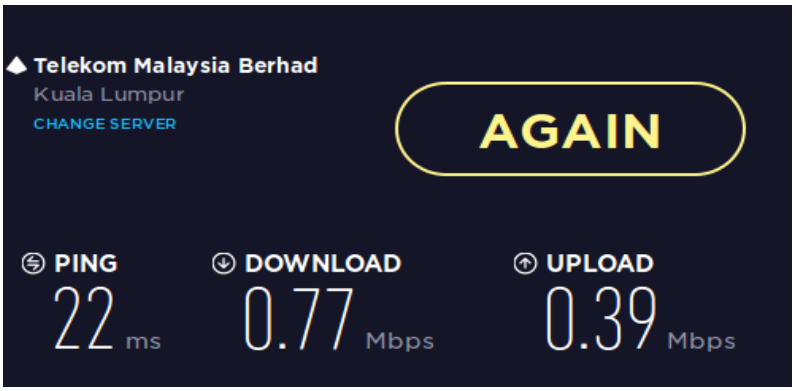
MacBook Pro (Student Group) 
Dell Veriton (Lecturer Group) 

Table 6-2-T30 Bandwidth Control Test Result (Condition 2) – Test Case 6

Based on the speed test result, Dell Veriton is assigned to lecturer group so the bandwidth is affected by the policy and the download speed had dropped to 0.77Mbps where MacBook Pro still remain around 1.74Mbps.

6.3 Project Challenge

In this project there are many problems and challenge encountered. In order to finish the project and achieve the goal of the project, the problems need to be solved. The problem that need to solved shows below.

- **Study and understand about Software Defined Networking(SDN)**

  Software Defined Networking is a new network architecture. Compare to traditional networking, the control plane and the data plane has been separate from the network equipment in SDN. In SDN, the control plane no longer handle by the network equipment itself, it is handle by the SDN controller.

  In the university, the lecture only teaches about the traditional networking. Before start to develop the application, some time needed to spend on study about software defined networking and understand how it works and what protocols is used to communicate. Since the software defined networking still quite a new technologies and it keep changing in time to time so the resources that found is very less or is an old version.

- **Develop SDN Application**

  There are some challenges in application development. Before start to develop the application, the language used to develop need to chose. Since the application that want to developed is a web-based system, so the main programming language to develop the application is PHP and HTML.

  There resource about develop SDN application that found in the Internet mainly in Java or python. There are less people using PHP and HTML to develop the SDN application. The controller that used in this system is Open Daylight. It provides the REST API service that can push the flow into the SDN switch. In order to use the REST API in

Open Daylight, some time needed to find out how to use REST function like GET, POST and DELETE in PHP.

- **HP switch and Cisco Router Configuration**

  The SDN switch used in this project is HP 2920-24G which is a HP branded switch. There some configuration need to be done in order to enable the OpenFlow protocols in the switch.

  In the university, Cisco branded network equipment and Cisco command is learned. Although some of the command is similar but also need to spend some time on learning the HP switch command and how to use the command to do the configuration. Moreover, there is a Cisco branded router used in this project. In order to let the VLAN created in the HP switch able to communicate with the Cisco router, the trunk configuration in the switch and the sub-interface in the router is needed.

- **Compatibility of Open Daylight with HP SDN Switch**

  There are many resources found in the Internet about how to build a SDN network by using the SDN controller like Open Daylight and connect with Mininet. Mininet is just a simulation tools that simulate a virtual SDN environment, it is not suitable to use in this project. There is less resource on how to use Open Daylight connect with the HP SDN switch. A lot of time is spent, in order to figured out how to make this possible. Not only the configuration need to be done in the HP switch, the source file of the Open Daylight also need to be modified.

6.4 SWOT

6.4.1 Strength

There are several strengths in this system. The first strength is the access control function. In the traditional networking, the access control function is handle by the router known as Access Control List. The policy is inserted when it is needed by the network admin into the ACL. For example, when the admin wants to block the access to certain destination in certain period, the admin needs to wait until the time is reached then only insert the policy. But this method is not very efficient. The system proposed in this project was able to solve this problem by using the schedule access control. This function allowed admin to predefined a policy and set a time period to run the policy.

Moreover, the system proposed in this project also able to defined an access control policy based on the user group. For example, student group not allowed to access the UTAR site whereby the lecturer group is allowed to access.

In the other hand, the system also able to perform the bandwidth control function. This function is to limit the bandwidth based on the user group. For example, the system can allocate 1Mbps bandwidth to lecturer group and 512kbps bandwidth to student group.

Last but not least, the system also provided a user friendly GUI for the network administrator. By using this GUI, admin can easily create or delete the policy into the SDN switch and don't have to enter any single command.

6.4.2 Weakness

There are some weaknesses in the system. When the network administrator wants to delete the policy, the admin need to delete the policy one by one. The system not allow the admin to select all the policy and delete it in the same time.

Moreover, this system only support IPv4 address. Now a day, some of the domain name is bind with IPv6 address. If the domain name is using IPv6 address, the system will no able to handle.

Besides that, if the domain name was bind with more than one public IP addresses and the addresses are not in the same range, the admin should create more than one policy with different public IP address else the admin will not able to block the access to the site.

6.4.3 Opportunities

The system proposed in this project able to help the university to control the network resource. Moreover, the system can be modified based on the university policy or user requirement.

6.4.4 Threats

There are some threats in this system. When the user connects to the SDN network, user don't have to do any authentication. Since the device need register its MAC address in the system then the device only can connect to the SDN network. But there is some software can modify the device MAC address. If someone modified their device MAC address to the MAC address that have registered, then the device is able to connect to the network.

Moreover, network administrator should have some knowledge on SDN. If the system is malfunction, the admin should access into the switch and do some troubleshooting.

6.5 Objective Evaluation

All the 4 objective of this project has successfully achieved which shows below.

1. Implement access control function
   - ✓ This project has successfully implemented the access control function in the system. The access control function can be divided into 3 type which is normal access control, schedule access control and group policy access control.

2. Implement bandwidth control function
   - ✓ This project has successfully implemented the bandwidth control function in the system. The bandwidth control function able to allocate different bandwidth to different user group.

3. Build Database
   - ✓ This project has successfully build a database for the system. The database is used to store all the access control policy and the bandwidth control policy that has created. Moreover, the system also included a URL database that store all the URL or domain name around the world. The URL database will be used when created an access control policy.

4. Provide graphical user interface
   - ✓ This project has designed a GUI for the system. By using this GUI, all the policy can be created easily.

6.6 Concluding Remark

Based on the testing result for all the module in chapter 6.2, the system is performing well and come out with expected outcome. Lastly, the project consider success since all the objectives has achieved.

7.0 Conclusion and Recommendation

7.1 Conclusion

Software defined networking is a new architecture for networking. There are some benefits by using SDN which is centralize control of multi-vendor environment, and reduce complexity through automation. Moreover, SDN also allowed to develop a new application based on the user requirement. The system that proposed is this project is just implement the access control function and bandwidth control function. But SDN can perform more function than what the system in this project can perform. SDN able to help people to solve many things in networking and help people to manage their network well.

7.2 Recommendation

There are some enhancements for the system proposed in this project. The enhancements show below.

1. IPv6 support

   Since the IPv6 has become more popular in the future, some of the domain name has chose to used IPv6 as the public IP address. The system should able to support the IPv6 in order to follow up the current trend.

2. Provide user authentication

   Since there is some vulnerability by using MAC address to register a device. The system should able to provide user to use username and password to login when they connect to the network. By doing so, the security of the network will be increase.

3. Provide backup and restore solution

   Backup and restore has become very important for every system. The system proposed in this project can implement the backup and restore solution in the future. The backup function able backup all the policy created in the system and restore it when the admin accidentally delete policy or the system corrupt

8.0 References

Just for Fun Network Management System (2009) Just for Fun Network Management System Feature [Online] Available from: < http://www.jffnms.org/features/> [Accessed 28 July 2016]

Open Networking Foundation (2013) Software-Defined Networking (SDN) Definition [Online] Available from: < https://www.opennetworking.org/sdn-resources/sdn-definition> [Accessed 27 July 2016]

Raisecom (2011) Raisecom Network Management System: NView NNM [Online] Available from: <https://www.raisecom.com/sites/default/files/RC_DS_NView%20NNM_V5.4_20120615.pdf > [Accessed 28 July 2016]

Open Networking Foundation White Paper (2013) Software-Defined Networking: The New Norm for Networks [Online] Available from: < http://www.bigswitch.com/sites/default/files/sdn_resources/onf-whitepaper.pdf> [Accessed 27 July 2016]

Open Daylight Platform overview[online] Available from: < https://www.opendaylight.org/platform-overview > [Accessed 28 July 2016]

ONOS White Paper (2014) Introducing ONOS – a SDN network operating system for service provide [Online] Available from: < http://onosproject.org/wp-content/uploads/2014/11/Whitepaper-ONOS-final.pdf > [Accessed 28 July 2016]

Appendix

Appendix 1

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 1
Student Name & ID: Gooi Hao Ming – 1405073	
Supervisor: Dr. Liew Soung Yue	
Project Title: Network Administration System For Bring Your Own Device(BYOD) over Software Defined Networking(SDN)	

1. WORK DONE - Check and configure the network equipment - Review FYP 1
2. WORK TO BE DONE - Appointment with supervisor and discuss process - Plan for the function that want to implement
3. PROBLEMS ENCOUNTERED - No
4. SELF EVALUATION OF THE PROGRESS - Progress ok

Supervisor's signature

Student's Signature

Appendix 2

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 4
Student Name & ID: Gooi Hao Ming – 1405073	
Supervisor: Dr. Liew Soung Yue	
Project Title: Network Administration System For Bring Your Own Device(BYOD) over Software Defined Networking(SDN)	

1. WORK DONE - Finish implement schedule access control - Redesign user interface
2. WORK TO BE DONE - Implement Group Policy
3. PROBLEMS ENCOUNTERED - Hard to understand and implement crontab that use to implement schedule access control
4. SELF EVALUATION OF THE PROGRESS - Progress a bit slower, spend more time in understanding

Supervisor's signature

Student's Signature

Appendix 3

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 6
Student Name & ID: Gooi Hao Ming – 1405073	
Supervisor: Dr. Liew Soung Yue	
Project Title: Network Administration System For Bring Your Own Device(BYOD) over Software Defined Networking(SDN)	

1. WORK DONE - Finish implement group policy - Finish implement device registered module
2. WORK TO BE DONE - Build URL database - Design Dashboard for the system
3. PROBLEMS ENCOUNTERED - No
4. SELF EVALUATION OF THE PROGRESS - Progress back to normal

Supervisor's signature

Student's Signature

Appendix 4

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 8
Student Name & ID: Gooi Hao Ming – 1405073	
Supervisor: Dr. Liew Soung Yue	
Project Title: Network Administration System For Bring Your Own Device(BYOD) over Software Defined Networking(SDN)	

1. WORK DONE - URL database successfully develop and used in access control module
2. WORK TO BE DONE - Planning to add bandwidth control into the system
3. PROBLEMS ENCOUNTERED - No
4. SELF EVALUATION OF THE PROGRESS - Progress is ok

Supervisor's signature

Student's Signature

Appendix 5

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 10
Student Name & ID: Gooi Hao Ming – 1405073	
Supervisor: Dr. Liew Soung Yue	
Project Title: Network Administration System For Bring Your Own Device(BYOD) over Software Defined Networking(SDN)	

1. WORK DONE - The bandwidth control module successfully implement - Main function of the system has developed
2. WORK TO BE DONE - Testing and debug the whole system
3. PROBLEMS ENCOUNTERED - No
4. SELF EVALUATION OF THE PROGRESS - Progress ok, all the objective has been successfully implement

Supervisor's signature

Student's Signature

Appendix 6

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 12
Student Name & ID: Gooi Hao Ming – 1405073	
Supervisor: Dr. Liew Soung Yue	
Project Title: Network Administration System For Bring Your Own Device(BYOD) over Software Defined Networking(SDN)	

1. WORK DONE - All the testing has been done
2. WORK TO BE DONE - Write the FYP report - Prepare for the presentation and demonstration
3. PROBLEMS ENCOUNTERED - No
4. SELF EVALUATION OF THE PROGRESS - Overall progress ok

Supervisor's signature

Student's Signature

Network Administration System for BYOD over SDN

ORIGINALITY REPORT

%7	%5	%4	%4
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.slideshare.net Internet Source	%1
2	S. Rakheja. "Assessment of open-loop rollover control of articulated vehicles under different manoeuvres", International Journal of Heavy Vehicle Systems, 2002 Publication	<%1
3	www.raisecom.com Internet Source	<%1
4	Submitted to University of Leeds Student Paper	<%1
5	fengnet.com Internet Source	<%1
6	www.downloads.netgear.com Internet Source	<%1
7	en.wikipedia.org Internet Source	<%1
8	Submitted to Informatics Education Limited Student Paper	<%1
9	docplayer.net	

	Internet Source	<%1
10	Submitted to 6908 Student Paper	<%1
11	Submitted to British Institute of Technology and E-commerce Student Paper	<%1
12	Submitted to Universiti Tunku Abdul Rahman Student Paper	<%1
13	Submitted to Colorado Technical University Online Student Paper	<%1
14	basicnetworkingconcepts.blogspot.com Internet Source	<%1
15	jffnms.org Internet Source	<%1
16	www.ohrd.wisc.edu Internet Source	<%1
17	Lecture Notes in Computer Science, 2015. Publication	<%1
18	Bakshi, K.. "Considerations for Software Defined Networking (SDN): Approaches and use cases", 2013 IEEE Aerospace Conference, 2013. Publication	<%1
19	Submitted to Middlesex University Student Paper	<%1

20	publications.theseus.fi Internet Source	<%1
21	internetworkmaterials.blogspot.com Internet Source	<%1
22	ask.opendaylight.org Internet Source	<%1
23	blog.ccna.com.br Internet Source	<%1
24	Wee, Susie. "1.4 The next generation of networked experiences", 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014. Publication	<%1
25	Submitted to Dublin City University Student Paper	<%1
26	"China Unicom and ONOS Sign Letter of Intent at the 2015 China SDN/NFV Conference.(Conference news)", PR Newswire, April 30 2015 Issue Publication	<%1
27	www.derentwickler.de Internet Source	<%1
28	Submitted to Oxford Brookes University Student Paper	<%1
29	Submitted to Universiti Teknologi Malaysia Student Paper	<%1

30	www.panticz.de Internet Source	<%1
31	dedysetyo.net Internet Source	<%1
32	dcnglobal.pl Internet Source	<%1
33	Submitted to Columbia College of Missouri Student Paper	<%1
34	Submitted to University of Auckland Student Paper	<%1
35	www.cnt.com Internet Source	<%1
36	Submitted to The Hong Kong Polytechnic University Student Paper	<%1
37	Submitted to Southern New Hampshire University - Distance Education Student Paper	<%1
38	www.lsicsi.com Internet Source	<%1
39	www.webmonkeys.org.uk Internet Source	<%1
40	www.qmul.ac.uk Internet Source	<%1
41	Wang, Haopei, Lei Xu, and Guofei Gu. "FloodGuard: A DoS Attack Prevention	<%1

Extension in Software-Defined Networks", 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2015.
Publication

42	www.pluke.com Internet Source	<%1
43	media.netcomm.com.au Internet Source	<%1
44	documentation.netgear.com Internet Source	<%1
45	www.dslreports.com Internet Source	<%1
46	www.alliedtelesis.se Internet Source	<%1
47	3g.co.za Internet Source	<%1
48	archive.org Internet Source	<%1
49	Submitted to Indian School of Mines Student Paper	<%1
50	Submitted to Western Governors University Student Paper	<%1

EXCLUDE QUOTES OFF EXCLUDE MATCHES < 8 WORDS

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	
ID Number(s)	
Programme / Course	
Title of Final Year Project	

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index:_____ % **Similarity by source** Internet Sources: _____% Publications: _____% Student Papers: _____%	
Number of individual sources listed of more than 3% similarity: _____	
Parameters of originality required and limits approved by UTAR are as Follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

_____
Signature of Supervisor

Name: _____

Date: _____

_____
Signature of Co-Supervisor

Name: _____

Date: _____