Understanding, Design and Configuration of Virtual Local Area Networks

Khin Aye Thu

Abstract - **Nowadays, Virtual Local Area Networks are widely used in enterprise networks to support network policies. The concept of VLANs, main idea, operation, configurations, applications, advantages and disadvantages expressed. On the same LAN appeared geographical distribution. A VLAN is used to improve network performance. A VLAN is the separation of large broadcast domains into smaller ones. A VLAN is provided data link connectivity for a subnet. VLANs are implemented to achieve security, scalability and ease of network traffic management. A VLAN could be used to separate traffic within the organization. A bridge or a switch can be used to prevent collisions through all the workstations from traveling in the network. Routers require more processing of incoming traffic with compared to switches. For VLANs, the Institute of Electrical and Electronic Engineers (IEEE) is currently working on a draft standard 802.1Q. VLAN membership based on port members, IP addresses, IP multicast addresses, MAC addresses and combination of these. A switch in a VLAN-enabled network needs a lot of ports. The two main types of links VLAN switches are access links and trunk links. Access links are configured to access a specific VLAN and trunk links are always configured to carry data from all available VLANs. In VLANs, layer 3 switch must have fast switching fabric and support for routing protocols. A VLAN network is provided physical security and physical access must be strictly controlled.**

Index Terms -- ***VLAN, LAN, IEEE 802.1Q, Port, IP.***

1. INTRODUCTION

A virtual local area network (VLAN) is a group of devices on one or more LANs that are configured to communicate in the same wire located on a number of different LAN segment. A broadcast domain is the set of all devices received broadcast frames within the set originating from any device.

Computer networks can be divided into local area networks (LANs) and wide area networks (WANs). Generally, in the same network at the specific location, switches, bridges, hubs, servers and workstations such network devices connected to each other known as LANs. A VLAN allows in a simulated environment a network of computers and users to communicate.

Cisco Packet Tracer is a software allowed users to simulate the complete network by adding and connecting difference network devices. The configuration of cisco routers and switches used command line interface.

Manuscript received October, 2018.

Khin Aye Thu, *Faculty of Computer Systems and Technologies, University of Computer Studies, Hinthada, (e-mail: ayethuu@gmail.com), Myanmar, +959428580525.*

2.FIVE TYPES OF VLAN

2.1 Data or user VLAN

Data VLAN is carried files, e-mails, application traffic and user traffic. VLAN for each group of users are separated.

2.2 Voice VLAN

Voice VLAN is used with IP phone to carry voice traffic. Without phone calls, communication over the network is not complete. Phone acts as a switch. Given priority, voice traffic is tagged. Data not tagged, it is no priority.

2.3 Management VLAN

A management VLAN has the switch IP address and subnet mask. A network administrator defines VLAN 1 as the management VLAN. For security,VLAN 1 is better not to use.

2.4 Native VLAN

An 802.1Q trunk port assigned in Native VLAN. The 802.1Q trunk port places untagged traffic. Native VLAN does not have a tag.

2.5 Default VLAN

For Cisco switches , VLAN 1 is default VLAN. VLAN 1 carries CDP and STP (spanning tree protocol) traffic. Initially, all ports are in the VLAN 1. All the features of any VLAN has in VLAN 1. This cannot be changed. Cannot delete or rename.

3. SWITCH PORT MODES

There are two types of switch ports modes: access port and trunk port.

3.1 Access port

Typically, access port is for a switch to host connection. This is assigned one VLAN. Commands are

#interface f [interface no:]
#switchport mode access
#switchport access vlan [vlan no:]

3.2 Trunk port

Typically, trunk port is a link between a router and a switch or two switches. This is assigned to traverse the link in multiple VLANs. Commands are

#interface f [interface no:]
#switchport mode trunk

4. DESIGN AND CONFIGURATION OF VLAN

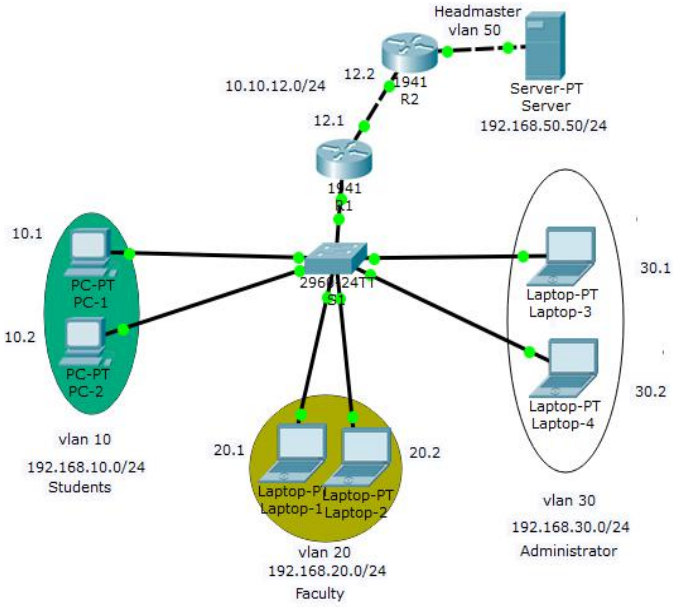

Fig.1: Virtual local area network created using cisco packet tracer

Figure 1 shows that the design of virtual local area network.

Table -1: Addressing Table

Table -2: Switch Port Assignment Specifications

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0.10	192.168.10.254	255.255.255.0	N/A
	G0/0.20	192.168.20.254	255.255.255.0	N/A
	G0/0.30	192.168.30.254	255.255.255.0	N/A
	G0/1	10.10.12.1	255.255.255.0	N/A
R2	G0/0	10.10.12.2	255.255.255.0	N/A
	G0/1	192.168.50.254	255.255.255.0	N/A
S1	VLAN 99	192.168.99.2	255.255.255.0	N/A
Server	NIC	192.168.50.50	255.255.255.0	192.168.50.254
PC-1	NIC	192.168.10.1	255.255.255.0	192.168.10.254
PC-2	NIC	192.168.10.2	255.255.255.0	192.168.10.254
Laptop-1	NIC	192.168.20.1	255.255.255.0	192.168.20.254
Laptop-2	NIC	192.168.20.2	255.255.255.0	192.168.20.254
Laptop-3	NIC	192.168.30.1	255.255.255.0	192.168.30.254
Laptop-4	NIC	192.168.30.2	255.255.255.0	192.168.30.254

Ports	Assignment	Network
S1 F0/1	VLAN 10-Students	192.168.10.0/24
S1 F0/2	VLAN 10-Students	192.168.10.0/24
S1 F0/3	VLAN 20-Faculty	192.168.20.0/24
S1 F0/4	VLAN 20-Faculty	192.168.20.0/24
S1 F0/5	VLAN 30-Administrator	192.168.30.0/24
S1 F0/6	VLAN 30-Administrator	192.168.30.0/24
S1 F0/7	802.1Q Trunk	N/A
S1	VLAN 99-Management	N/A

4.1 Build the Network and Configure Basic Device Settings

Step 1: Cable the network.

Step 2: Initialize and reload the routers and switch.

Step 3: Configure basic settings for **each router and switch**.

i. Disable DNS lookup.

ii. Assign device name as shown in the topology.

iii. Assign **cisco** as the privileged EXEC password.

iv. Assign **class** as the console and **class** as vty passwords.

v. Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.

vi. Configure **logging synchronous** for the console line.

vii. Configure the IP address listed in the Addressing Table for all interfaces.

viii. Copy the running configuration to the startup configuration.

Router R1 Configuration:

```
Router>enable
Router#config t
i.   Router(config)# no ip domain lookup
ii.  Router(config)#hostname R1
iii. R1(config)#enable password cisco
iv.  R1(config)#line console 0
     R1(config-line)#password class
     R1(config-line)#login
     R1(config)#exit
     R1(config)#line vty 0 15
     R1(config-line)#password class
     R1(config-line)#login
     R1(config)#exit
v.   R1(config)#banner motd #" unauthorized access is
     prohibited"#
vi.  R1(config)#line console 0
     R1(config-line)#logging synchronous
     R1(config-line)#exit
vii. R1(config)#interface g0/0
     R1(config-if)#no ip address
     R1(config-if)#exit
     R1(config)#interface g0/0.10
     R1(config-subif)#encapsulation dot1Q 10
```

R1(config-subif)#ip address 192.168.10.254 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.254 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.30.254 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/1
R1(config-if)#ip address 10.10.12.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#exit

viii. R1#copy running-config startup-config

Router R2 Configuration:

Router>enable
Router#config t

i. Router(config)# no ip domain lookup
ii. Router(config)#hostname R2
iii. R2(config)#enable password cisco
iv. R2(config)#line console 0
R2(config-line)#password class
R2(config-line)#login
R2(config)#exit
R2(config)#line vty 0 15
R2(config-line)#password class
R2(config-line)#login
R2(config)#exit
v. R2(config)#banner motd #" unauthorized access is prohibited"#
vi. R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#exit
vii. R2(config)#interface g0/0
R2(config-if)#ip address 10.10.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface g0/1
R2(config-if)#ip address 192.168.50.254 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#exit
viii. R2#copy running-config startup-config

Switch S1 Configuration:

Switch>enable
Switch#config t

i. Switch(config)# no ip domain lookup
ii. Switch(config)#hostname S1
iii. S1(config)#enable password cisco
iv. S1(config)#line console 0
S1(config-line)#password class
S1(config-line)#login
S1(config)#exit
S1(config)#line vty 0 15
S1(config-line)#password class
S1(config-line)#login
S1(config)#exit
v. S1(config)#banner motd #" unauthorized access is prohibited"#
vi. S1(config)#line console 0
S1(config-line)#logging synchronous
S1(config-line)#exit
vii. S1(config)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
S1(config)#exit
viii. S1#copy running-config startup-config

Step 4: Configure VLAN on S1.

S1(config)#vlan 10
S1(config-vlan)#name Students
S1(config-vlan)#exit
S1(config)#valn 20
S1(config-vlan)#name Faculty
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name Administrator
S1(config-vlan)#exit
S1(config)#vlan 50
S1(config-vlan)#name Headmaster
S1(config-vlan)#exit
S1(config)#vlan 99
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#interface f0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#interface f0/3
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#exit
S1(config)#interface f0/4
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#exit

```
S1(config)#interface f0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#exit
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#exit
S1(config)#interface f0/7
S1(config-if)#switchport mode trunk
S1(config-if)#exit
S1(config)#exit
S1#copy running-config startup-config
```

Step 5: Configure PC hosts and server.

Step 6: Test connectivity.

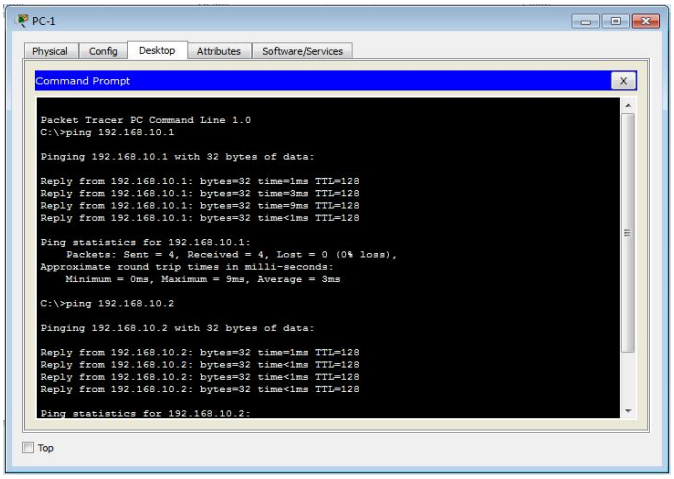

Fig. 2: Ping test from PC-1 to PC-2

Figure 2 shows that test connectivity to ping the IP address of PC-2 from PC-1.

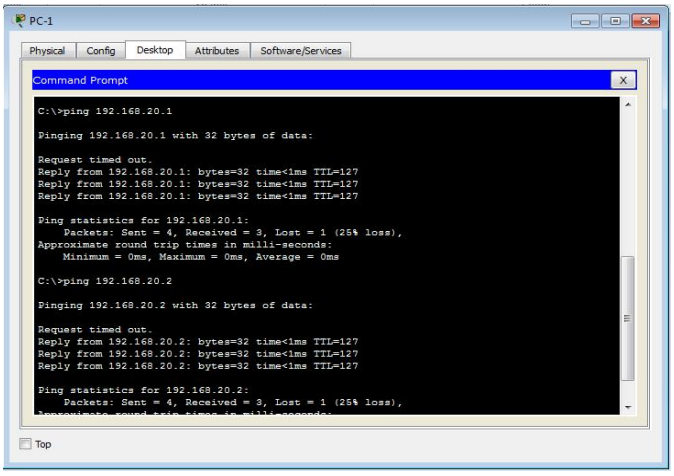

Fig. 3: Ping test from PC-1 to Labtop-1 and Laptop-2

Figure 3 shows that test connectivity to ping the IP addresses of Laptop-1 and Laptop-2 from PC-1.

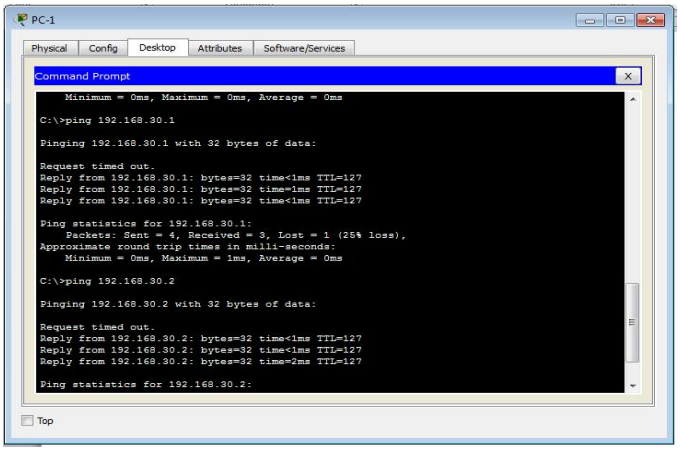

Fig. 4: Ping test from PC-1 to Labtop-3 and Laptop-4

Figure 4 shows that test connectivity to ping the IP addresses of Laptop-3 and Laptop-4 from PC-1.

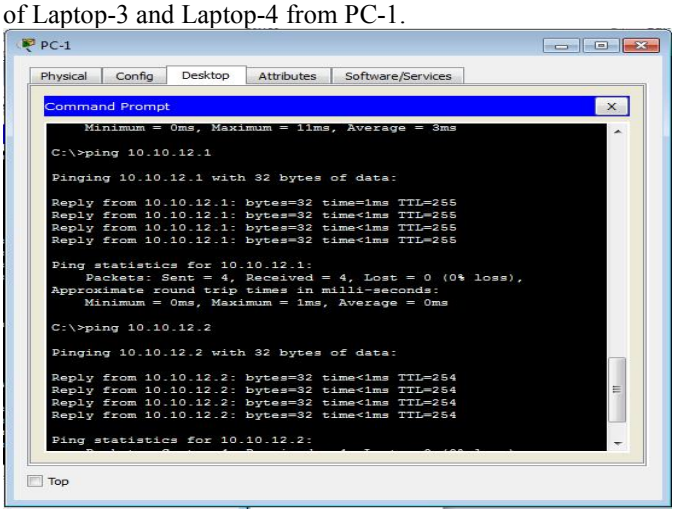

Fig. 5: Ping test from PC-1 to 10.10.12.0 subnet

Figure 5 shows that test connectivity to ping the IP addresses of 10.10.12.0 subnet from PC-1.

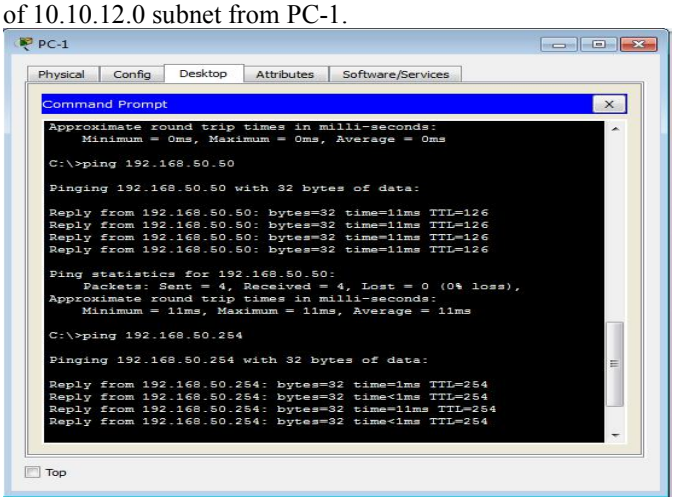

Fig. 6: Ping test from PC-1 to Server

Figure 6 shows that test connectivity to ping the IP addresses of 192.168.50.50 subnet and Server from PC-1.

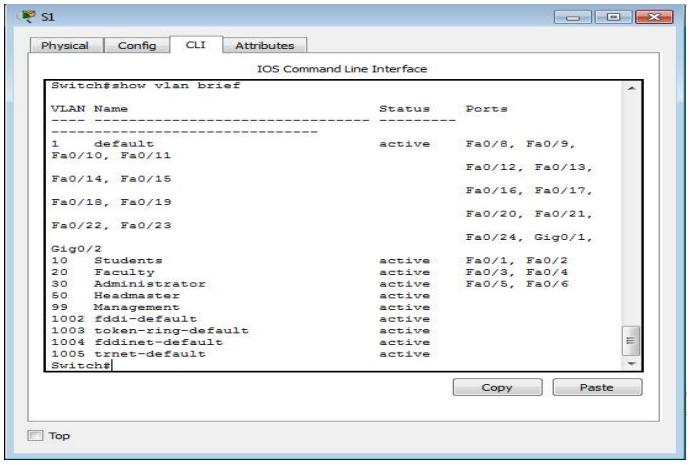

Fig. 7: show vlan brief command from S1

Figure 7 shows that the view of VLAN database from S1, verify that VLANs are assigned to the correct interfaces.

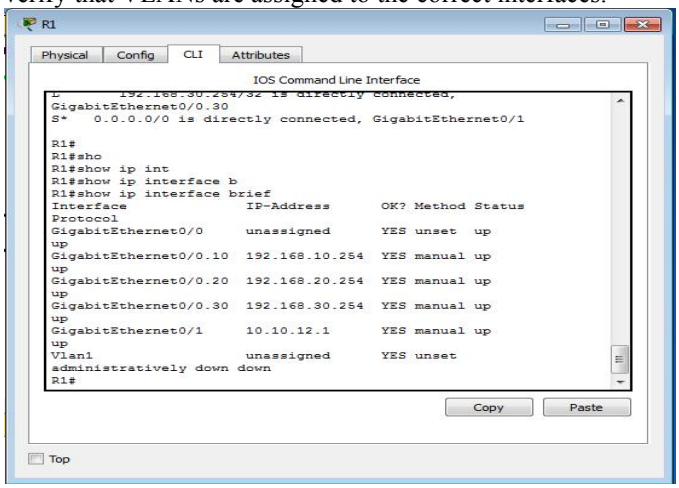

Fig. 8: show ip interface brief command from R1

Figure 8 shows that the view of interfaces from R1, verify that correct interfaces.

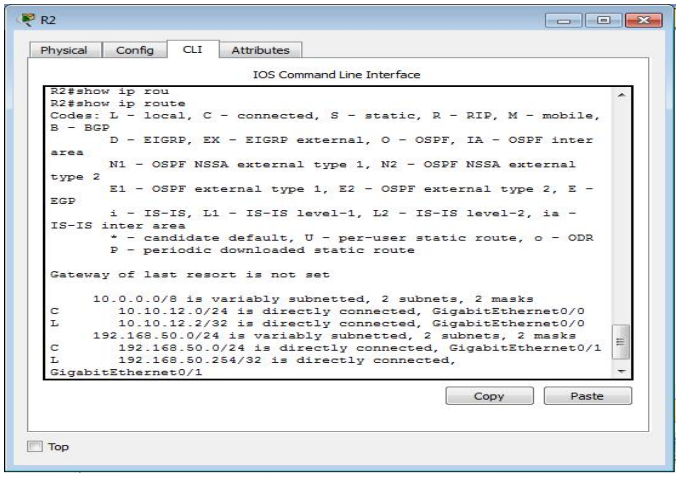

Fig. 9: show ip route command for R2

Figure 9 shows that the view of subnets and directly connected from R2, verify that correct subnets.

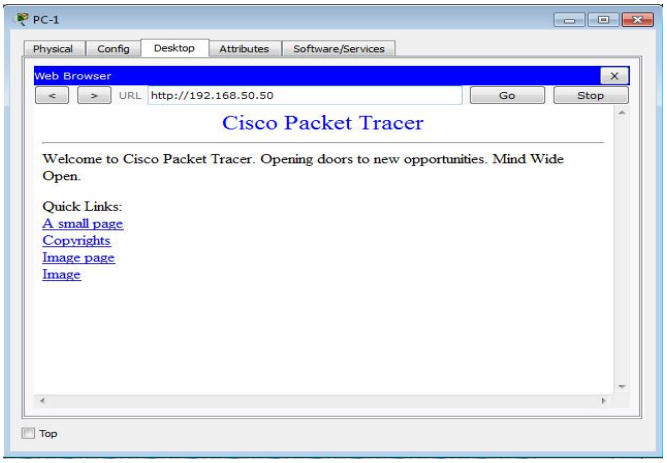

Fig. 10: Use PC1 to access web server (Server) from Web Browser

Figure 10 shows that verify the web servers by accessing the web pages.

5. ADVANTAGES AND DISADVANTAGES OF VLAN

Advantages

VLANs provided confine of broadcast domains, ease of administration, reduced broadcast traffic, higher performance, and security policies. On a VLAN by broadcast domains are confined, not intended end stations are prevented.

Disadvantages

VLANs are more difficult managing rather than only one LAN. The traffics within VLAN must go through a router. A VLAN cannot forward to another VLAN.

6. CONCLUSION

The utilization of Virtual Local Area Networks provided simplify network management and improved network security. VLANs provided independent of physically implementation. VLAN is cost reducing logically management of computers changing environments.

7. ACKNOWLEDGEMENT

I would like to thank my teachers and my friends for the support at the University of Computer Studies, Hinthada. I would like to take this opportunity to thank my family.

8. REFERENCES

[1] CCNA Routing and Switching Courses, University of Computer Studies, Mandalay, 2013.

[2] Gyan Prakash Pal, Sadhana Pal Faculty of Electronics & Communication Engineering Department, SIT, Meerut, VGI, Greater Noida (India) "Virtual Local Area Network (VLAN)" International Journal of Scientific Research Engineering & Technology (IJSRET) Volume 1, Issue 10 pp 006-010, January 2013.

[3] JAMES F.KUROSE, KEITH W.ROSS, "COMPUTER NETWORKING", A Top-Down Approach, 6 th Edition.

[4] Minlan Yu and Jennifer Rexford, Princeton University Xin Sun and Sanjay Rao, Purdue University Nick Feamster, Georgia Institute of Technology "A Survey of Virtual LAN Usage in Campus Networks" IEEE Communications Magazine , July 2011.

[5] Surabhi Surendra Tambe Final year Btech EXTC student, Electrical Engineering Department, VJTI, Matunga, Mumbai, India "Understanding Virtual Local Area Networks" International Journal of Engineering Trends and Technology (IJETT)- Volume 25 Number 4-July 2015.

BIOGRAPHY

Khin Aye Thu received M.Sc. (Physics) from University of Pathein in 2002 and M.A.Sc. from University of Computer Studies, Yangon in 2003. She worked as Lecturer in the Faculty of Computer Systems and Technologies, University of Computer Studies, Hinthada, Myanmar (Burma).