International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

Virtualization of Campus LAN and analyzing traffic issues of these VLANs

Mohammad Serazul Islam, Md. Javed Hossain, Mohammed Humayun Kabir

Abstract— Recently, network virtualization has been pushed forward by its proponents as a long-term solution to the gradual ossification problem faced by the existing network and proposed to be an integral part of the next-generation networking paradigm. By allowing multiple LAN architectures to cohabit on a shared physical substrate, network virtualization provides flexibility, promotes diversity, promises security and increased manageability. This research work is basically on VLAN in networks and also the deployment of VLAN in various environments. It also includes some advantages and disadvantages of this technique. This research work also includes how traffic is passing between VLAN at different layer switch and also shows trunking of the VLAN. It includes basic security and enhanced security too. Network performance can be a factor in an organization's productivity and its reputation for delivering as promised. One of the contributing technologies to excellent network performance is the separation of large broadcast domains into smaller ones with VLANs. Smaller broadcast domains limit the number of devices participating in broadcasts and allow devices to be separated into functional groupings, such as database services for an accounting department and high-speed data transfer for an engineering department.

Index Terms—VLAN, Trunk, PDU, MTU, ACL, MVRP, VTP, VoIP

1 INTRODUCTION

The OSI Reference Model defines the process of connecting two layers of networking functions. The application layer provides the user's interface. The presentation layer determines how data is represented to the user. The session layer is responsible for setting up and tearing down connections. The transport layer is responsible for the mechanics of connections, including guaranteed services. The network layer provides a logical topology and layer-3 addresses: routers operate here. The data link layer defines MAC addresses and how communication is performed on a specific media type: switches, bridges, and NICs (Network Interface Controllers) operate here. The physical layer defines physical properties for connections and communication: repeaters and hubs operate here. The data link layer defines hardware addressing. MAC addresses are 48-bits in length in hexadecimal. The first 24 bits (6 digits) are the OUI (Organizationally Unique Identifier). MAC addresses only need to be unique on a logical segment [1].

A PDU (Protocol Data Unit) describes data and its overhead. A PDU at the application layer is referred to as data; the transport layer PDU is called a segment, the network layer PDU is called a packet or datagram, the data link layer PDU is called a frame and the physical layer PDU is called bits. As traffic goes down the protocol stack, each layer encapsulates the PDU from the layer above it [1].

At the destination, a de-encapsulation process occurs network segmentation with virtual local area networks (VLANs) creates a collection of isolated networks within the data center. Each network is a separate broadcast domain. When properly configured, VLAN segmentation severely hinders access to system attack surfaces. It reduces packet-sniffing capabilities and increases threat agent effort. Finally, authorized users only "see" the servers and other devices necessary to perform their daily tasks [2].

Another advantage of segmentation is protocol separation. Network architects can limit certain protocols to certain segments of the enterprise. For example, if IPX or AppleTalk systems exist on your wire, they can each have their own VLAN in which to operate. This limits traffic in each VLAN to relevant packets [2].

Finally, use of VLANs enables secure, flexible user mobility. For example, a user assigned to a specific VLAN will always connect to that VLAN regardless of location. This is particularly helpful when designing wireless constraints. A VLAN is a logically separate IP sub network. VLANs allow multiple IP networks and subnets to exist on the same switched network. The fig. 1 shows a network with three computers. For computers to communicate on the same VLAN, each must have an IP address and a subnet mask that is consistent for that VLAN. The switch has to be configured with the VLAN and each port in the VLAN must be assigned to the VLAN. A switch port with a singular VLAN configured on it is called an access port. Remember, just because two computers are physically connected to the same switch does not mean that they can communicate. Devices on two separate networks and subnets must communicate via a router (Layer 3), whether or not VLANs are used. You do not need VLANs to have multiple networks and subnets on a switched

- *Mohammad Serazul Islam is currently pursuing masters degree program in Computer Science and Telecommunication Engineering department of Noakhali Science and Technology University, Sonapur, Noakhali-3814, Bangladesh, E-mail: mseraz.i@gmail.com*
- *Md. Javed Hossain is currently serving as an Associate Professor in Computer Science and Telecommunication Engineering department of Noakhali Science and Technology University, Sonapur, Noakhali-3814, Bangladesh, E-mail: javed.nstu@gmail.com*
- *Dr. Mohammed Humayun Kabir is currently serving as an Associate Professor in Computer Science and Telecommunication Engineering department of Noakhali Science and Technology University, Sonapur, Noakhali-3814, Bangladesh, E-mail: hkabir269@gmail.com*

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

network, but there are definite advantages to using VLANs [2].

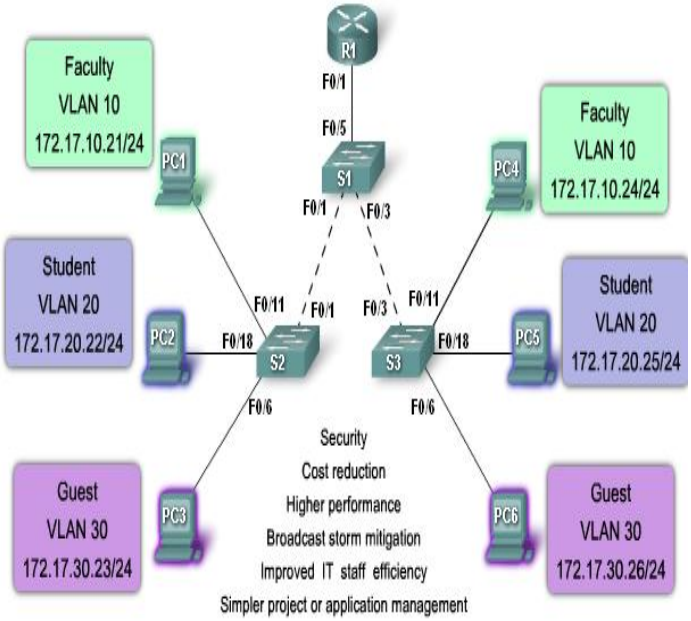

Fig. 1. Three VLAN design

2 RELATED WORKS

There is growing interest on virtualization of network in recent years. Virtualization of network is mainly four types: Virtual Local Area Network, Virtual Private Network, Programmable Network and Overlay Network. Among these networks VLAN is the most popular system based on the motivation:

a) To reduce overhead by limiting the size of each broadcast domain.
b) Also making better security by including sensitive devices into VLAN.
c) Also making special traffic separate than main.

Network Virtualization: State of the Art and Research Challenges [4]. There are some other related works that are already been completed by the researchers to utilize the network fruitfully and efficiently. Study on VLAN in Wireless Networks [2]. The Virtual LAN Technology Report [1]. Besides these, our target is to analysis the security of the proposed VLAN. We can get help from the research work: Designing Protection System of LAN Security [3]. Through effective implementation of VLAN, we will get secured and less expensive network by using effective implementation of VLAN and ACL (Access Control List) in LAN [5].

3 VLAN

3.1 Introducing VLAN

To appreciate why VLANs are being widely used today, consider a small community college with student dorms and the faculty offices all in one building. The fig. 2, shows that the student computers in one LAN and the faculty computers in another LAN. This works fine because each department is physically together, so it is easy to provide them with their network resources.

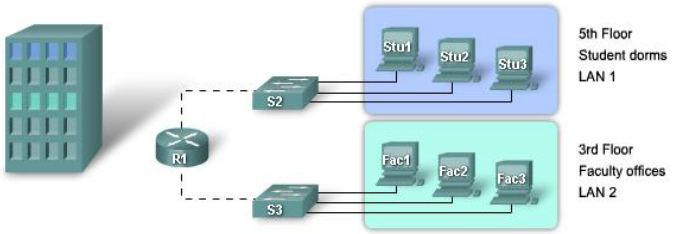

Fig. 2. One building VLAN

A year later, the college has grown and now has three buildings. In the fig. 3, the original network is the same, but student and faculty computers are spread out across three buildings. The student dorms remain on the fifth floor and the faculty offices remain on the third floor. However, now the IT department wants to ensure that student computers all share the same security features and bandwidth controls. How can the network accommodate the shared needs of the geographically separated departments? Do you create a large LAN and wire each department together? How easy would it be to make changes to that network? It would be great to group the people with the resources they use regardless of their geographic location, and it would make it easier to manage their specific security and bandwidth needs [5].

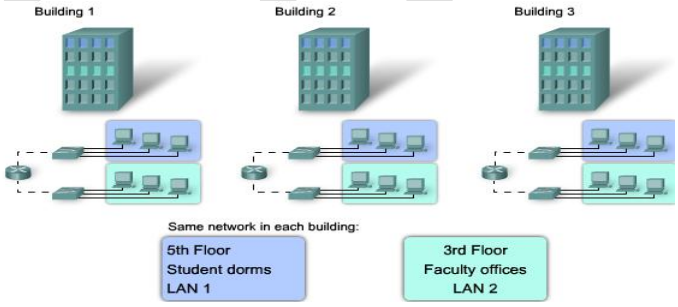

Fig. 3. Many buildings VLAN

3.2 VLAN Types

Today there is essentially one way of implementing VLANs - port-based VLANs. A port-based VLAN is associated with a port called an access VLAN.

However in the network there are a number of terms for VLANs. Some terms define the type of network traffic they carry and others define a specific function a VLAN performs. The following describes common VLAN terminology [7]:

3.2.1 Data VLAN

A data VLAN is a VLAN that is configured to carry only user-generated traffic. A VLAN could carry voice-based traffic or traffic used to manage the switch, but this traffic would not be part of a data VLAN. It is common practice to separate voice

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

and management traffic from data traffic. The importance of separating user data from switch management control data and voice traffic is highlighted by the use of a special term used to identify VLANs that only carry user data - a "data VLAN". A data VLAN is sometimes referred to as a user VLAN [8].

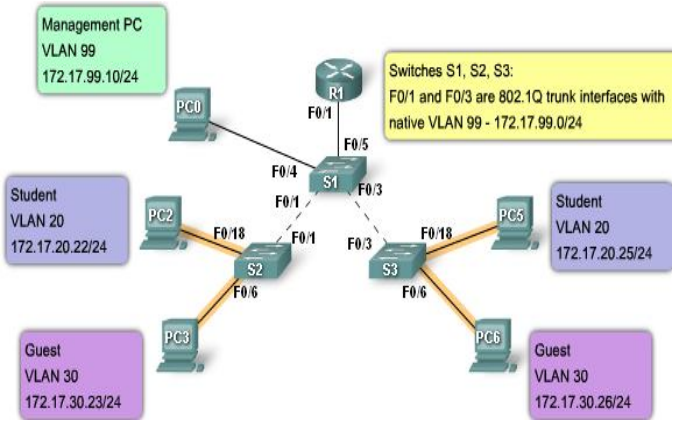

Fig. 4. Data VLAN

3.2.2 Default VLAN

All switch ports become a member of the default VLAN after the initial boot up of the switch. Having all the switch ports participate in the default VLAN makes the all part of the same broadcast domain. This allows any device connected to any switch port to communicate with other devices on other switch ports. The default VLAN for Cisco switches is VLAN 1. VLAN 1 has all the features of any VLAN, except that you cannot rename it and you cannot delete it. Layer 2 control traffic, such as CDP and spanning tree protocol traffic, will always be associated with VLAN 1 - this cannot be changed. In the figure, VLAN 1 traffic is forwarded over the VLAN trunks connecting the S1, S2, and S3 switches. It is a security best practice to change the default VLAN to a VLAN other than VLAN 1; this entails configuring all the ports on the switch to be associated with a default VLAN other than VLAN 1. VLAN trunks support the transmission of traffic from more than one VLAN. Although VLAN trunks are mentioned throughout this section, they are explained in the next section on VLAN trunking [8].

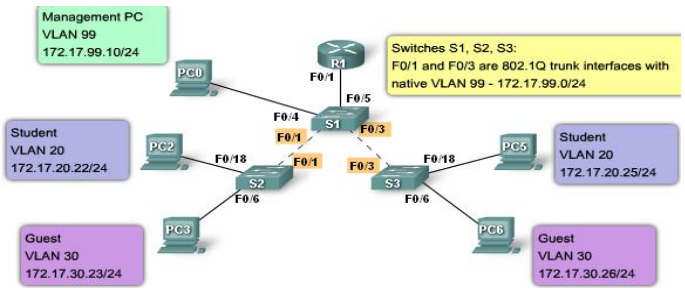

Fig. 5. Default VLAN

3.2.3 Native VLAN

A native VLAN is assigned to an 802.1Q trunk port. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as Ill as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. In the figure, the native VLAN is VLAN 99. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. Native VLANs are set out in the IEEE 802.1Q specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For my purposes, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN [8].

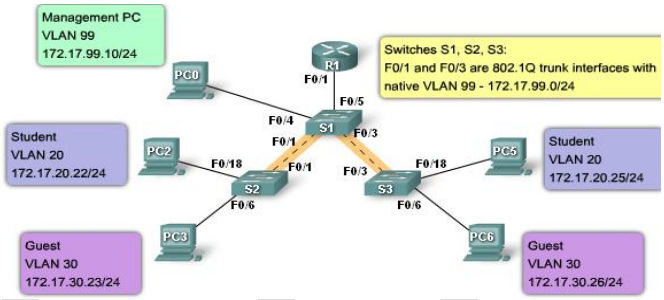

Fig. 6. Native VLAN

3.2.4 Management VLAN

A management VLAN is any VLAN you configure to access the management capabilities of a switch. VLAN 1 would serve as the management VLAN if you did not proactively define a unique VLAN to serve as the management VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Since the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, you see that VLAN 1 would be a bad choice as the management VLAN; you should not want an arbitrary user connecting to a switch to default to the management VLAN [8].

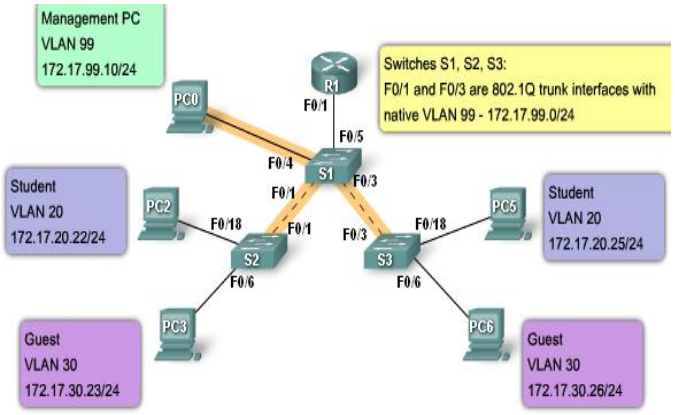

Fig. 7. Management VLAN

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

3.2.5 Voice VLAN

It is easy to appreciate why a separate VLAN is needed to support Voice over IP (VoIP). Imagine you are receiving an emergency call and suddenly the quality of the transmission degrades so much you cannot understand what the caller is saying. VoIP traffic requires:

i) Assured bandwidth to ensure voice quality.
ii) Transmission priority over other types of network traffic
iii) Ability to be routed around congested areas on the network.
iv) Delay of less than 150 milliseconds (ms) across the network [8].

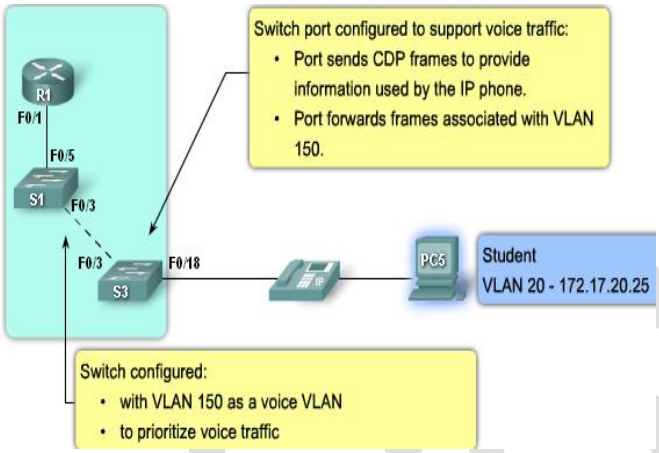

Fig. 8. Voice VLAN

3.3 Properties of VLAN

VLAN ID Ranges

Normal Range VLANs

a) They are used in small and medium-sized business and enterprise networks.
b) Identified by a VLAN ID between 1 and 1005.
c) IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
d) IDs 1 and 1002 to 1005 are automatically created and cannot be removed.
e) Configurations are stored within a VLAN database file, called vlan.dat. The vlan.dat file is located in the flash memory of the switch.
f) The VLAN trunking protocol (VTP), which helps to manage VLAN configurations between switches, can only learn normal ranges of VLANs and stores them in the VLAN database file [6].

Extended Range VLAN

a) Enable service providers to extend their infrastructure to a greater number of customers. Some global enterprises could be large enough to need extended range VLAN IDs.
b) They are identified by a VLAN ID between 1006 and 4094.
c) Support fewer VLAN features than normal range VLANs.
d) Are saved in the running configuration file.
e) VTP does not learn extended range VLANs [6].

3.4 VLAN trunking

Trunking

Many organizations have more than one switch. Further, VLANs are not dependent on the actual location of an end-point device or switches. When using two Q-switches to manage VLANs, a trunk is configured between them using a port on each switch: a trunk port. During a broadcast, all VLAN packets entering either switch are sent via the trunk to the other switch. This allows VLAN members to exist in different locations and still use all VLAN-assigned resources [7].

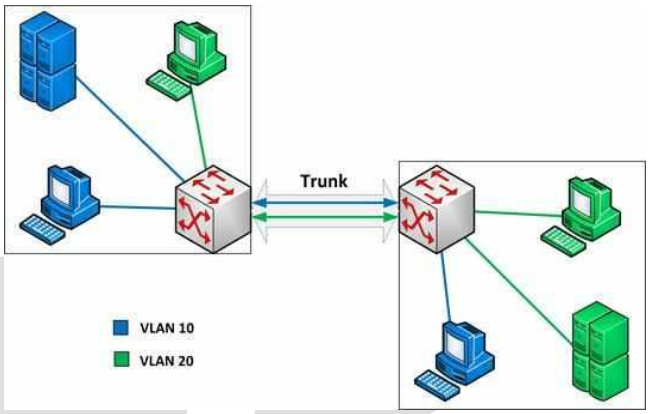

Fig. 9. VLAN Trunking

Configure an 802.1Q Trunk [9]:

To configure a trunk on a switch port, use the switch port mode trunk command. When we enter trunk mode, the interface changes to permanent trunking mode and the port enters into a DTP negotiation to convert the link into a trunk link even if the interface connecting to it does not agree to the change. In this course, we will configure trunk using only the switch port mode trunk command. In the example, we will configure VLAN 99 as the native VLAN. The command syntax used to allow a list of VLANs on the trunk is shown. On this trunk port, allow VLANs 10, 20, and 30.

Cisco IOS CLI Command Syntax	
Enter global configuration mode.	#configure terminal
Enters the interface configuration mode for the defined interface.	(config)#interface *interface id*
Force the link connecting the switches to be a trunk link.	(config-if)#switchport mode trunk
Specify another VLAN as the native VLAN for untagged for IEEE 802.1Q trunks.	(config)#switchport trunk native vlan *vlan-id*
Add the VLANs allowed on this trunk.	(config-if)#switchport trunk allowed vlan add *vlan-list*
Return to privileged EXEC mode.	(config-if)#end

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

We are familiar with this topology. The VLANs 10, 20, and 30 will support the Faculty, Student, and Guest computers, PC1, PC2, and PC3. The F0/1 port on switch S1 will be configured as a trunk port to allow VLANs 10, 20, and 30. VLAN 99 will be configured as the native VLAN [5].

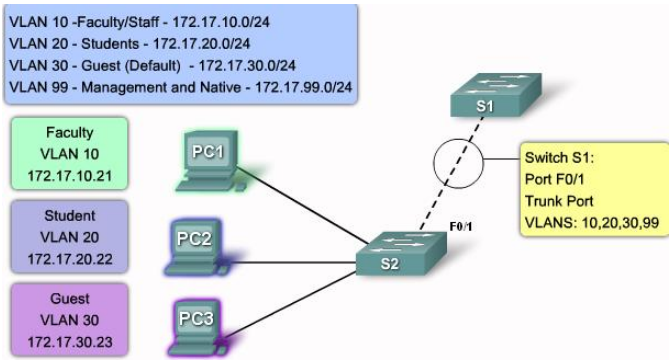

Fig. 10. Configure a Trunk VLAN

The example configures port F0/1 on switch S1 as the trunk port. It reconfigures the native VLAN as VLAN 99 and adds VLANs 10, 20, and 30 as allowed VLANs on port F0/1 [8].

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#switchport trunk allowed vlan add 10,20,30
S1(config-if)#end
```

The first highlighted area shows that port F0/1 has its administrative mode set to Trunk-the port is in trunking mode. The next highlighted area verifies that the native VLAN is VLAN 99, the management VLAN. At the bottom of the output, the last highlighted area shows that the enabled trunking VLANs are VLANs 10, 20, and 30 [5].

```
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
```

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
20   student                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int fa 0/1
S1(config-if)#switch access vlan 20
S1(config-if)#switch mode access
S1(config-if)#^Z
```

```
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

3.5 Configuring VLAN

Packets belong to VLANs, not devices. Each packet arriving at a VLAN-configured Q-switch is checked to see if it meets the criteria for belonging to any of the connected LANs. An administrator can use any of several approaches for VLAN configuration [6]:

- Port assignment
- MAC address
- IP Subnet
- Dynamic assignment
- Device assignment
- Protocols
- Applications

In this topic, I will learn how to create a static VLAN on a Cisco Catalyst switch using VLAN global configuration mode. There are two different modes for configuring VLANs on a Cisco Catalyst switch, database configuration mode and global configuration mode. Although the Cisco documentation mentions VLAN database configuration mode, it is being phased out in favor of VLAN global configuration mode [2].

I will configure VLAN with IDs in the normal range. Recall there are two ranges of VLAN IDs. The normal range includes IDs 1 to 1001, and extended range consists of IDs 1006 to 4094. VLAN 1 and 1002 to 1005 are reserved ID numbers. When you configure normal range VLANs, the configuration details are stored automatically in flash memory on the switch in a file called vlan.dat [8].

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	#**configure terminal**
Create a VLAN. Vlan id is the VLAN number that is to be created. Switches to VLAN configuration mode for VLAN vlan id.	(config)#**vlan** *vlan id*
(Optional) Specify a unique VLAN name to identify the VLAN. If no name is entered the VLAN number, padded zeros, is appended the word 'VLAN', for example, VLAN0020.	(config-vlan)#**name** *vlan name*
Return to privileged EXEC mode.You must end your configuration session for the configuration to be saved in the vlan.dat file and for configuration to take effect.	(config-vlan)#**end**

The student VLAN, VLAN 20, is configured on switch S1. In the topology example, the student computer, PC2, is not in a VLAN yet it, but has an IP address of 172.17.20.22. [5].
The figure shows an example of using the show VLANs brief command to display the contents of the vlan.dat file. The student VLAN, VLAN 20, is highlighted in the screen capture. The default VLAN IDs 1 and 1002 to 1005 are shown in the screen output.
Note: In addition to entering a single VLAN ID, you can enter a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens using the VLANs VLANs-id command, for example: switch (config) #vlan 100,102,105-107 [5].
Assign a Switch Port
After I have created VLAN, assign one or more ports to the VLAN. When I manually assign a switch port to a VLAN, it is known as a static access port. A static access port can belong to only one VLAN at a time [5].

Cisco IOS CLI Command Syntax	
Enter global configuration mode.	#**configure terminal**
Enter the interface to assign the VLAN.	(config)#**interface interface id**
Define the VLAN membership mode for the port.	(config-if)#**switchport mode access**
Assign the port to a VLAN.	(config-if)#**switchport access vlan vlan id**
Return to privileged EXEC mode.	(config-if)#**end**

3.6 VLAN Security
I already looked at segmentation and use of access control lists to protect system attack surfaces. However, switches and the VLANs they manage each possess its own attack surface. Out-of-the-box, most Q-switches are not ready to help protect anything [9].

3.6.1 Physical security
The first step in securing a switch is restricting physical access. Make sure it is behind a locked door. Under no circumstances should unauthorized people gain physical access to it or any other infrastructure equipment [3].

3.6.2 Password Access
Under no circumstances should remote or local access be password-free. For example, configure secure shell (SSH) or Telnet ports for password-only access. Further, access should conform to the roles performed by each person with management responsibilities [3].

3.6.3 Role-based Access Control
In many organizations, privileged access to a switch means full access. Regardless of role, each administrator can perform any management task on the device. This is never a good idea. Instead, configure the switch so that each user has a unique login and password. In addition, assign privilege levels based on the user's role in switch administration. No more than one or two administrators should have full access. Finally, configure password encryption [7].

4 PROPOSED VLAN CONFIGURATION AND IMPLEMENTATION

4.1 Sequential process of implementation
Implementation Process
We have covered a lot of concepts in this chapter. It is time to put it all together into an implementation plan: a plan that provides architecture-specific segmentation and safe switch operation. The process consists of

1. Configure all ports as access ports.
2. Configure switch security: control physical access, create role-based user accounts, restrict telnet ports to account and password only access and enable port security.
3. Configure trunks.
4. Configure VTP / MVRP (Multi-Vendor Recertification Program) recommended to shut it off.
5. Create VLANs.
6. Assign an IP address range to each VLAN.
7. Assign ports to VLANs: by IP address (recommended for most static wired networks), by MAC address, by port assignment, by dynamic assignment (recommended for most wireless networks and shared switch port networks), by protocols and by applications.
8. Remove all data VLANs from the native VLAN.
9. Assign unused, connected ports to an unused VLAN.
10. Create and apply L2 ACLs and VACLs.
11. Create and apply L3 ACLs.

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

4.2 Cisco Packet Tracer

Interface Overview

When we will open Packet Tracer, by default we will be presented with the following interface:

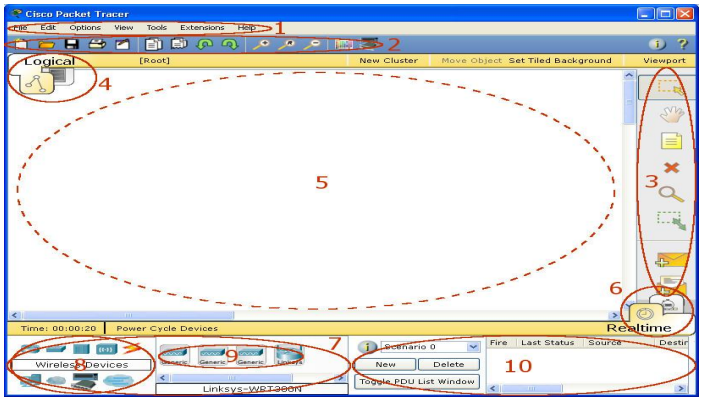

Fig. 11. Interface Overview

Simulation Mode

In Simulation Mode, we can "freeze" time --we have direct control over time related to the flow of PDUs. We can see the network run step by step, or event by event, however quickly or slowly we like. We can set up scenarios, such as sending a ping packet from one device to another. However, nothing "runs" until we capture it or play it (re-playing the captured events as an animation). When we capture or play the simulation, we will see graphical representations of packets traveling from one device to another. We can make a pause of the simulation or step forward or backward in time, investigating many types of information on specific PDUs and devices at specific times. However, other aspects of the network will still run in real time. For example, if we turn off a port, its link light will respond immediately by turning red [8].

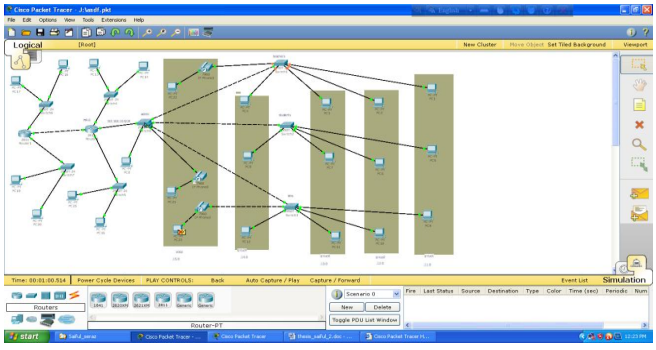

Fig .12. Simulation Mode

4.3 OPNET@ It Guru

OPNET @It Guru is a one kind of simulator which is broadly used to simulate the IT based thesis work or research. Our proposed research work is also simulated by OPNET @ IT Guru to explain traffic received-sent-dropped average with respect to time [8].

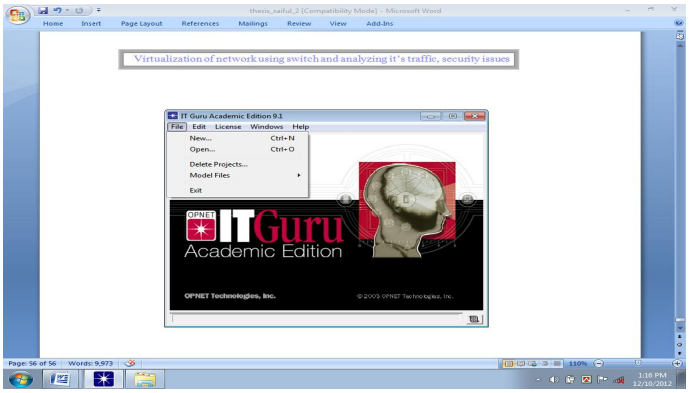

Fig .13. OPNET User interface

4.4 Design and simulation

4.4.1 Design and simulation of proposed VLAN with packet tracer

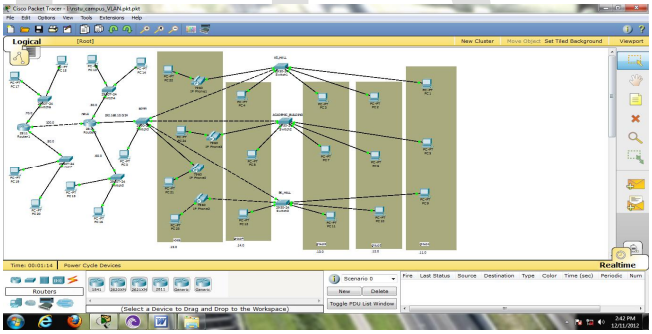

Fig. 14. Design view of VLANs

In the fig. 14, we have designed campus VLAN. There are six VLANs in our implementation. Here we have created four data VLANs. They are VLAN 10, VLAN 20, VLAN 30 and VLAN 40 named respectively as group1, group2, group3 and gruop4. Here is also a voice VLAN. Its VLAN id is 50. There is also a Default VLAN named by VLAN1. We declare this VLAN as Native or Management VLAN.

```
AS_HALL#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/7, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
10   group1                            active    Fa0/2
```

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

```
20   group2                  active    Fa0/4
30   group3                  active    Fa0/6
40   group4                  active    Fa0/8
50   Voice                   active    Fa0/3
1002 fddi-default            act/unsup
1003 token-ring-default      act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default           act/unsup
VLAN Type  SAID       MTU (Maximum Transmission Unit)
Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet 100001     1500 -      -      -    -        0     0
10   enet 100010     1500 -      -      -    -        0     0
Verification of this VLAN
Packet Tracer PC Command Line 1.0
PC>ping 192.168.11.255

Pinging 192.168.11.255 with 32 bytes of data:
Reply from 192.168.11.3: bytes=32 time=111ms TTL=128
Reply from 192.168.11.2: bytes=32 time=140ms TTL=128
Reply from 192.168.11.1: bytes=32 time=42ms TTL=255
Reply from 192.168.11.3: bytes=32 time=42ms TTL=128
Reply from 192.168.11.2: bytes=32 time=42ms TTL=128
Reply from 192.168.11.1: bytes=32 time=78ms TTL=255
Reply from 192.168.11.3: bytes=32 time=78ms TTL=128
Reply from 192.168.11.2: bytes=32 time=78ms TTL=128
Reply from 192.168.11.1: bytes=32 time=91ms TTL=255
Reply from 192.168.11.3: bytes=32 time=91ms TTL=128
Reply from 192.168.11.2: bytes=32 time=91ms TTL=128
PC>ping 192.168.10.255
Pinging 192.168.10.255 with 32 bytes of data:
Reply from 192.168.11.1: bytes=32 time=50ms TTL=255
Reply from 192.168.11.1: bytes=32 time=78ms TTL=255
Reply from 192.168.11.1: bytes=32 time=65ms TTL=255
Reply from 192.168.11.1: bytes=32 time=58ms TTL=255
Ping statistics for 192.168.10.255:Packets: Sent = 4, Received =
4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 50ms, Maximum = 78ms, Average = 62ms
```

Why implemented?

The interface f0/0 of router nstu1 (IP address is 192.168.10.0/24) covers the AS_Hall, BK_Hall, Academic building. As a result a lot of users try to use the same network at a time. So the broadcast load increases highly. It may hamper the security system. Now if we divide the network 192.168.10.0/24 into five sub networks 192.168.11.0/24, 192.168.12.0/24, 192.168.13.0/24, 192.168.14.0/24, 192.168.15.0/24. The broadcast domain of 192.168.10.0/24 divided into five virtual domains. As a result load balancing and security of network be ensured.

Besides if we want to implement the network physically, it may need extra wire and instrument. But for virtual implementation it is low cost comparatively.

4.4.2 Performance analysis of proposed VLAN with Packet tracer

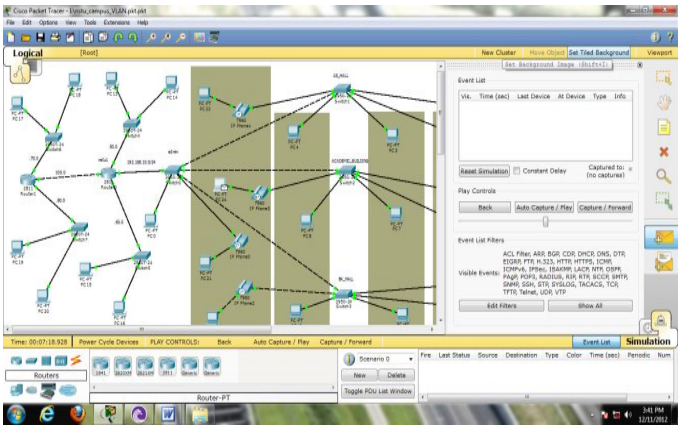

Fig. 15. Performance analysis of proposed VLAN

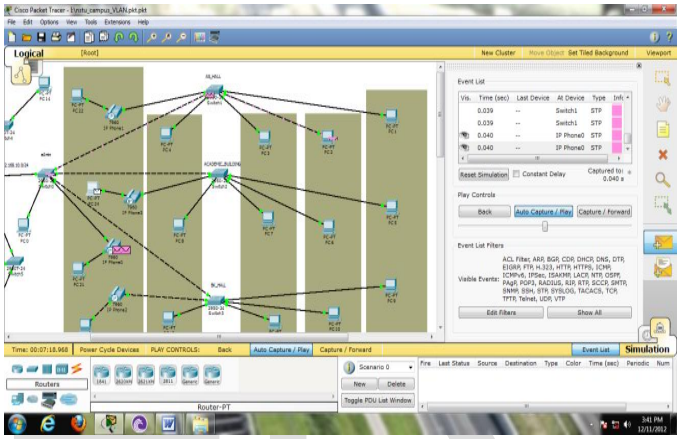

Fig. 16. Performance analysis of proposed VLAN

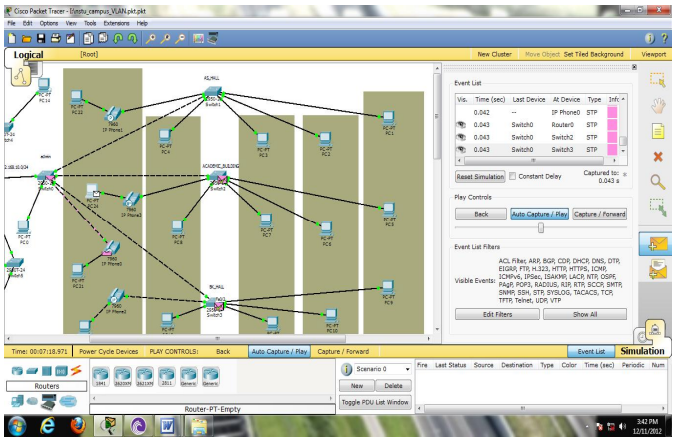

Fig. 17. Performance analysis of proposed VLAN

Performance analysis of proposed VLAN have been shown in fig. 15 to fig. 17.

4.4.3 Traffic analysis of proposed VLAN with OPNET

Three VLANs configuration and simulation results

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

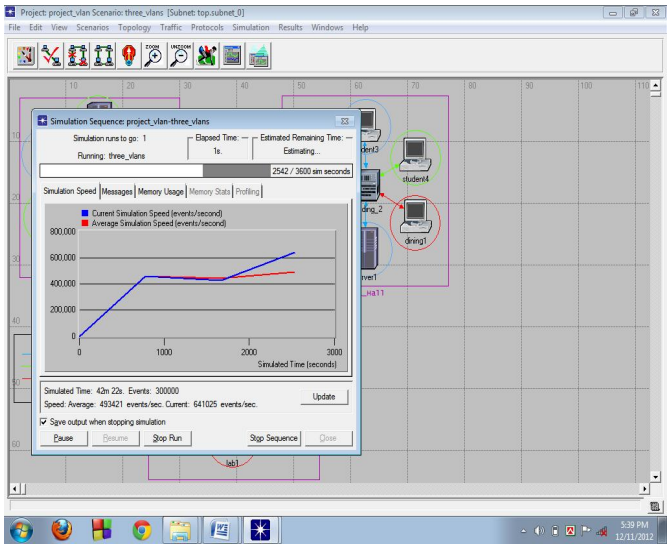

Fig. 18. Simulation process window

Fig. 18, shows the simulation process window. Red line of the graph indicates the average simulation speed (events/seconds) and blue line of the graph indicates the current simulation speed (events/seconds). After completing the simulation process, we can calculate average traffic sent_recieved_dropped (bits/seconds) in each VLAN.

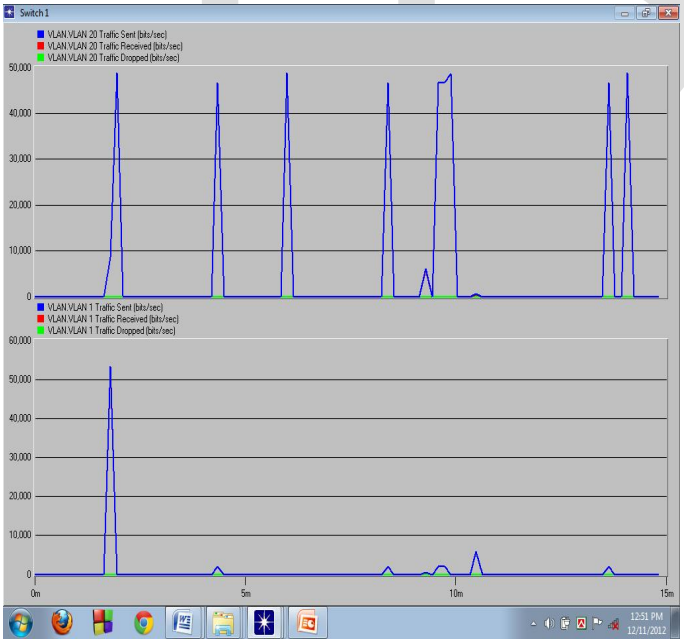

Fig. 19. VLAN traffic of switch 1

Now we shall analyze the traffic of VLANs in switch1. Here, fig. 19, shows traffic analysis of VLAN 20 and VLAN 1. In switch1 VLAN 20 is not receiving any traffic. It is only sending the traffic. Her traffic dropped rate is zero. VLAN 1 is also sending the traffic but not receiving.

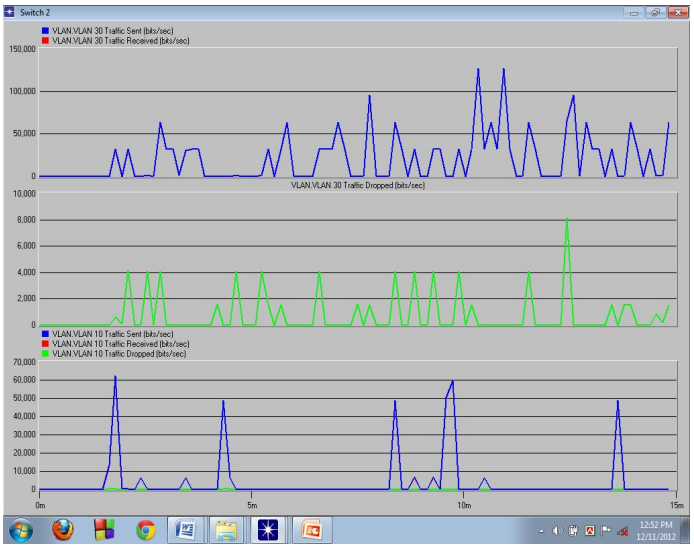

Fig. 20. VLAN traffic of switch 2

Fig. 20, shows the traffic analysis of the VLANs of switch2. Here VLAN 30 is sending the traffic but not receiving any traffic. Data dropped rate is very high. VLAN 10 is also sending the data but not receiving any data. Here data dropped rate is zero.

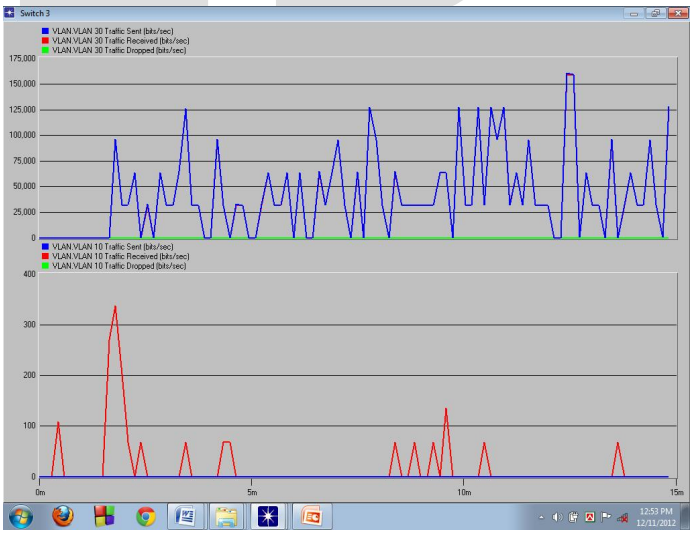

Fig. 21. VLAN traffic of switch 3

Fig. 18-21: Traffic analysis results overview. Fig. 21, shows here also VLAN 30 in switch3 is sending data but not receiving any data. Data dropped rate is zero. But VLAN 10 at switch3 is only receiving the traffic. That means VALN 10 of switch2 sends traffic and VLAN 10 of switch3 receives the traffic.

4.5 Advantages of this proposed VLAN

a) Our implemented research work will decrease the

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

broadcast load and also will increase security to entire network.
b) Whole network will be saved from network jamming.
c) Implementation cost is very low.
d) Easy to operate.
e) Clients of voice VLAN can communicate with each other by IP telephony.
f) Proper utilization BW can be ensured by this research work.

5 CONCLUSION AND FUTURE WORK

5.1 Conclusion

This research work is more helpful to the organization for the effective implements of VLAN and to enhance network security by keeping devices that operates with sensitive information on a separate VLAN. The organizations will get the following benefits:

a) To improve manageability that group users by section instead of physical section.
b) To filter unwanted packets by using ACL such as Telnet and Ping.
c) To have more than one broadcast within the same switch by creating more than one VLAN.
d) To have an overview of how to troubleshoot VLAN configuration.
e) To reduce the cost which eliminate the need for expensive router.

5.2 Future work

a) Our target is to convert the wired VLAN into wireless VLAN.
b) Then we shall make the VLAN as a Green VLAN by reducing the power consumption.
c) To save our proposed VLANs from unauthorized users, our target will be to improve the security techniques.

REFERENCES

[1] David Passmore and John Freeman, "The Virtual LAN Technology Report", 3COM White Paper, May 1996.
[2] Rajul Chokshi and Dr. Chansu Yu, "Study on VLAN in Wireless Networks", 2007.
[3] Kaiyuan Yang, "Designing Protection System of LAN Security", 2011.
[4] N. M. Mosharaf Kabir Chowdhury and Raouf Boutaba, "Network Virtualization: State of the Art and Research Challenges", IEEE Communications Magazine, July 2009.
[5] Abubucker Samsudeen Shaffi & Mohaned Al-Obaidy, "Effective Implementation of VLAN and ACL in Local Area Network", vol.4, no. 1, JITBM & ARF, 29 August 2012.
[6] Paul C. Rollins, "Virtual Local Area Networks and Wireless Virtual Local Area Networks", 3 May 2001.
[7] M Zhu, M Molle and Brahman, "Design and Implementation of Application-based Secure VLAN", *Proc. 29th Annual IEEE international conference on Local Computer Network*, ISSN 0742-1303, pp. 407-408, 16-18 November 2004.
[8] Indell Odom, *CCNA Self-Study CCNA INTRO Exam Certification Guide,* CCIE No. 1624.
[9] IEEE 802.1: 802.1Q – Virtual LANs. *IEEE Computer Society,* available at http://www.ieee802.org/1/pages/linksec/.

IJSER