IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

# A Simulation based study on Network Architecture Using Inter-VLAN Routing and Secure Campus Area Network (CAN)

**S.Somasundaram[1*], M.Chandran[2]**

[1*] Department of Computer Applications, SRMV College of Arts & Science, Coimbatore, Tamilnadu ,India
[2] Department of Computer Applications, SRMV College of Arts & Science, Coimbatore, Tamilnadu ,India

*Corresponding Author: onsomasundaram@gmail.com*

**Available online at: www.ijcseonline.org**

Received: 20/Feb//2018, Revised: 26/Feb2018, Accepted: 19/Mar/2018, Published: 30/Mar/2018

***Abstract*—**Today development of computer and information technology, computer and network have been very popular. At the same time, security is important to secure the data, especially in campus environment. A campus network faces, many challenges such as IP address allocation, network failure, detecting rogue system user and determining slowing network etc., This research is mainly targeted towards campus networks which deliver the required security and best performance. To reduce the maximum wastage of IP address space using VLSM technique. A network is divided into different subnets. This technique will improve the security and traffic isolation. To improve the network speed on campus area network using etherchannel technique. This technique increases the network speed and redundant path between two devices. To multiple smaller broadcast domain using VLAN. To Communicate different VLAN using Inter-VLAN technique. This technique is implemented using multilayer switch. To secure and control a network traffic using VLAN Access Control List (VACL). Secured network protects an institution from security attacks associated with network. A campus network has a number of uses, such as education, research, learning, supervision, e-library, result publishing and association with the external users. Network security prevents the campus network from different types of threats and attack. The system can efficiently control and handle the reliable operation of the campus network.

***Keywords*—** Etherchannel, VLSM, VLAN , Inter-VLAN, VACL

## I. INTRODUCTION

This research work is completely based upon secure the data and reliable communication in campus area network. Today development of computer and information technology, computer and network have been very popular. At the same time, security is important to secure the data, especially in campus environment. A campus network faces, many challenges such as IP address allocation, network failure, detecting rogue system user and determining slowing network etc., This thesis is mainly targeted towards campus networks which deliver the required security and best performance.

Secured network protects an organization from security attacks associated with network. A campus network has a number of uses, such as education, research, learning, supervision, e-library, result publishing and association with the external users. Network security prevents the campus network from different types of threats and attack. The system can efficiently control and handle the reliable operation of the campus network.

The prior systems in the network primarily focus on corporate industry network. This Research focuses not only the corporate industry network, it also Campus area network. This system accomplished through the subnetting and Variable Length Subnet Masking (VLSM) technique for IP address allocation, Virtual Local Area Network (VLAN) for secure and cost reduction of campus area network, Inter-VLAN communication for connecting two different VLAN, Etherchannel technique for increase the campus area network speed and VLAN Access Control List (ACL) technique for secure the Campus Area Network

## II. REVIEW OF LITERATURE

### IP Address Space Management

A new technique of subnetting for class C IP addresses to minimize the wastage of address space. Different techniques such as Fixed Length Subnet Masking (FLSM) and Variable length Subnet Masking (VLSM) these techniques yields minimum address space wastage. [25].

### Fixed length subnet masking

FLSM is the technique to design different sub networks of different or same sizes in a physical network by adding some bits in a network address for security [2,3,4,5] and traffic isolation [3,4,7] purposes. This technique also solves the routing table expansion problem [7] by ensuring the invisibility of subnet structure of a private network. This generates same route to any host of the network because for a given network number all the

hosts use same network prefix but different subnet number. Table 4 depicts different subnet mask of class C network as per requirements of an organization.

Routers outside and within the subnetted environment behave differently. Router outside the subnetted environment use only the network prefix while the router within the subnetted environment use the extended network prefix to rout the traffic to individual subnet. The extended network prefix comprises of network prefix and the subnet number. Prefix length is determined by counting the contiguous 1-bit in a subnet mask. A subnetted network address is usually specified as <network address>/<prefix length>.

FLSM suffers from huge wastage of address space for variable size subnets e.g. 60, 50, 40 and 30. If we choose the largest subnet of 60 then class C network will have four equal subnets of 64 to accommodate all the variable size subnets in Fig 2.1.[25]

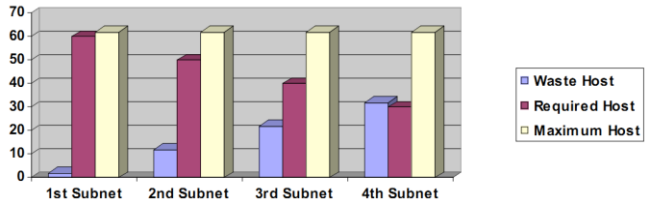



Fig 2.1: FLSM Technique

**Variable length subnet masking**

This technique incorporates multiple size subnets or multiple level subnets to maximize the utilization of IPs. It is obvious that more than one subnet masks can be used for a subnetted network. VLSM [8] divides an address space recursively and aggregates to reduce routing information [9,25].This technique uses a hierarchical structure where subnets may be further subnetted.

Using the same data set as in FLSM, the subnets of 60, 50 and 40 remain same, however, the subnet of 30 is further divided into two parts. The address space wastage is reduced to 16% as compared to that of FLSM with 27% (Fig. 2.2).

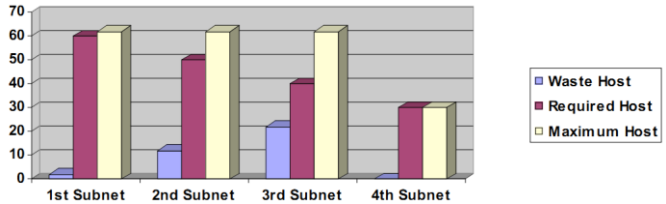



Fig 2.2: VLSM Technique

**2.2 Effective Remote Management for Inter-VLAN Routing Networks**

VLANs are extensively used in enterprise network to ease management of hosts to improve scalability and flexibility. Despite their wide usage in enterprise network, VLAN security is a greater concern for the network administrator due to very little attention has been paid on error prone, unsystematic, high risk of misconfiguration in the design and management of enterprise VLAN network[10,19].

**2.2.1 Remote Management of VLAN**

The remote connectivity can be done by using any routing protocols from static or dynamic. In our paper we use static routing protocol. We have configured telnet port vty along with other required authentication. Your management VLAN does not have to be the same as your Native VLAN. Matter of fact, it is good practice to make sure that they are different. Your management VLAN should only carry in-band management traffic and should not be the default VLAN. We have specified an ip address to vlan 10 & make sure that they are not shutdown. Also specify ip default gateway to router0 in the server switch. The configuration of server switch A for telnet support is given below:[10,12,19]

**2.2.2 Access-List Based Inter-VLAN Communication**

ACL's are used to secure and control traffic into or out of networks. In modern implementations, central file servers and services are usually placed in their own isolated VLAN, securing them from possible network attacks while controlling access to them. An administrator can smartly disable ICMP echoes and other protocols used to detect a live host, avoiding possible detection by an attacker host located over a different VLAN [10,11,19,23]. After configuring ACL, router works as a firewall and checks each statement sequentially before forwarding the traffic to its destination. By using standard or extended access-lists, a router processes each ACL from top to bottom, one statement at a time. We propose extended ACL's to filter the traffic between VLAN's or between hosts of a VLAN. Also we can use standard ACL to restrict telnet access from the remote network. The configuration of ACL as per figure 1on router0 is shown below:

access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 101 permit ip any any
To configure a more restrictive ACL, create permit entries and omit the permit any entry at the end of the standard ACL.
access-list 15 permit host 192.168.4.1 209.157.22.32

access-list 15 permit 192.168.4.0 0 0.0.0.255
telnet access-group 15

### 2.3 Effective VTP Model for Enterprise VLAN Security

VLAN's are widely used in today's enterprise networks to improve scalability & flexibility at core, distribution and access layers. VLAN's are no longer confined to LAN environments and are becoming more widespread in their use. Unfortunately VLAN security issues has raised concerns and caused some network architects to re-focus on the associated issues. Two key issues required to implement inter-VLAN communication i.e. Effective VLAN design according to organizational need to reduce the much complex administrative work, and to overcome security issues related with VTP design model.[19,20,23]

#### 2.3.1 VTP Reduces Administrative Work

In Fig 2.3, VLAN design is used using VLAN Trunking protocol (VTP) to fulfill our objective to reduce the much administrative work with less costing. In the first part we have configure the VTP model by interconnecting four switches such that one acts as VTP Server and the other three are clients. VTP server will automatically update the summary/subset advertisement to all the connected clients. In the second part we have connected a router with single interface with the VTP Server switch to simulate inter-VLAN Routing.[19,22,26]

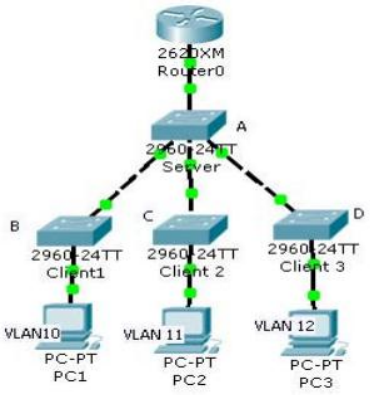



*Fig 2.3: Enabling VTP Protocol*

### 2.4 Design and Implementation of the CAN Monitoring System

With the development of computer and information technology, computer and network have been popular. At the same time, security problem has greatly aroused people's attention, especially in campus environment. Campus network as an important part of the campus life, people also arouse enough attention to the problems of personal computer safety management. Running a set of effective campus network monitoring software is real needed for the campus network management and maintenance personal safety. In order to ensure the safety, reliability and steady running of the campus network, according to the present situation and development of the campus network, people plan and design to use network monitoring system on the campus network security management. The system can effectively control and manage the reliable operation of the campus network.[22,24]

#### 2.4.1 Characteristics of campus network

The main characteristics of the campus network: network resources have the characteristics of centralization, but geographically have certain distribution pattern; campus network covers quite large geographical scope, network deployment scale has diversity; campus network with multiple administrative domain is used for the calculation of large-scale scientific computing needs; general campus network are based on CERNET platform, whose network speed is fast, but most of the campus network has certain constraints; in terms of logic structure design, its structure is not very complex and should pay attention to the characteristics of its heterogeneity and dynamics in the process of design.[24]

#### 2.4.2 Campus network monitoring system.

At present, the network Monitoring System based on campus network structure GMA has been widely used as a standard in the industry in many Grid Monitoring systems.GMA network monitoring system structure is mainly made based on "producer consumer" model, which provides network a network monitoring system through this model to achieve interoperability of the system architecture. At the same time, it also gives the system an integral solution. In the system framework based on GMA, monitoring system is mainly divided into two development directions: one is RGMA based on Relation Grid Monitoring structure, another is GLOBUS MDS based on hierarchy. At present a lot of domestic relative research, scientific research achievements are mainly GMA - C monitoring system, GRIDMON monitoring system etc. All these monitoring systems have achieved the goal that unify the system's dynamic information and static information to an LDAP directory based on the LDAP directory service structure, and solve the problem of campus network interface through the middleware technology. Adopting the centralized management is the characteristic of monitoring system itself. [24]

## III. METHODOLOGY

### 3.1 IP Address Allocation to Campus Area Network (CAN)

In this technique we propose a new mechanism for the address space management of class C with subnet.

### 3.1.1 Subnetting

A subnet is a process of dividing one large network into multiple smaller network. subnetting of IP addresses to handle wastage of address space.

### Subnetting of Class C Address

Class C address are used by the networks having less than or equal to 254 hosts. (Total IP address 256. Two IP address such First Address (Network Address) and Last Address (Broadcast Address) not possible to assign the client. Address (Broadcast Address) not possible to assign the client.[15]

| Starting Address | Subnet Mask | Host Range | No Of Hosts Per Sub-network |
|---|---|---|---|
| Network Address 200.1.1.0/**24** | 255.255.255.0 | 200.1.1.0 to 200.1.1.255 | 256 |

*Table 3.1: Before Subnetting /24*

### Subnetting of /25 Prefix

The Single Network is divided into two subnetwork. Each network contain 128 IP address (only 126 is usable Host Address.

IP Address = 200 . 1 . 1 . 0 /25
Subnet mask = 255 . 255.255.128
Wild Card Mask = 0 . 0 . 0 .127
Network Address = 200 . 1 . 1 . 0
Broadcast Address = 200 . 1 . 1 .127

(If you find the broadcast address simply add Wildcard mask + Network Address)

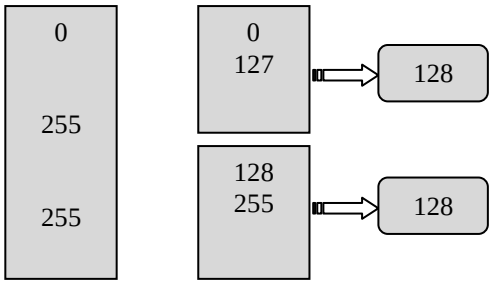



Fig 3.1: Subnetting of /25 prefix

| Starting Address | Sub Networks | Subnet Mask | Host Range | No Of Hosts Per Sub-network |
|---|---|---|---|---|
| Network Address 200.1.1.0/24 | Network Address 200.1.1.0/25 | 255.255. 255.128 | 200.1.1.0 to 200.1.1.127 | 128 |
| | Network Address 200.1.1.128/25 | 255.255. 255.128 | 200.1.1.128 to 200.1.1.255 | 128 |

Table 3.2: After Subnetting using network prefix /25

Subnetting of Class B Address

| Starting Address | Subnet Mask | Host Range | No of Hosts in Network |
|---|---|---|---|
| Network Address 150.1.1.1/16 | 255.255 .0.0 | 150.1.0.0 to 150.1.255.255 | 65536 |

Table 3.3: Before Subnetting /16

| Starting Address | Sub Networks | Subnet Mask | Host Range | No Of Hosts Per Sub-network |
|---|---|---|---|---|
| Network Address 150.1.1.1/ 16 | Network Address 150.1.0.0/18 | 255.255.19 2.0 | 150.1.0.0 to 150.1.63.255 | 16384 |
| | Network Address 150.1.64.0/18 | 255.255.19 2.0 | 150.1.64.0 to 150.1.127.255 | 16384 |
| | Network Address 150.1.128.0/1 8 | 255.255.19 2.0 | 150.1.128.0 to 150.1.191.255 | 16384 |
| | Network Address 150.1.192.0/1 8 | 255.255.19 2.0 | 150.1.192.0 to 150.1.255.255 | 16384 |

Table 3.4:After Subnetting using network prefix /18

### 3.1.2 Variable Length Subnet Masking

Variable Length Subnet Masking (VLSM) allows the use of different masks for each subnet. After a network address is subnetted, those subnets can be further subnetted. As you most likely recall, VLSM is simply subnetting a subnet. VLSM can be thought of as sub-subnetting.

### VLSM and IP Address

Another way to view the VLSM subnets is to list each subnet and its sub-subnets. In the Table 3.5 , the 200.1.1.0/24 network is the starting address space. It is subnetted with a /25 mask on the first round of subnetting. It is subnetted with a /26 mask on the second round of subnetting. . It is subnetted with a /27 mask on the third round of subnetting. . It is subnetted with a /28 mask on the fourth round of subnetting. . It is subnetted with a /29 mask on the fifth round of subnetting. . It is subnetted with a /30 mask on the sixth round of subnetting. [15]

| Starting Address | Sub Networks | Subnetting of Subnet | Subnetting of Subnet | Subnetting of Subnet | Subnetting of Subnet | Subnetting of Subnet | Subnetting of Subnet |
|---|---|---|---|---|---|---|---|
| Network Address 200.1.1.0/24 | Network Address 200.1.1.0/25 | Network Address 200.1.1.0/26 | Network Address 200.1.1.0/27 | Network Address 200.1.1.0/28 | Network Address 200.1.1.0/29 | Network Address 200.1.1.0/30 | Minimum 2 bit are required in Sub Netting |
| | | | | | | Network Address 200.1.1.4/30 | No.of Host 4 Usable Host 2 |
| | | | | | Network Address 200.1.1.8/29 | No.of Host 8 Usable Host 6 | |
| | | | | Network Address 200.1.1.16/28 | No.of Host 16 Usable Host 14 | | |
| | | | Network Address 200.1.1.32/27 | No.of Host 32 Usable Host 30 | | | |
| | | Network Address 200.1.1.63/26 | No.of Host 64 Usable Host 62 | | | | |
| | Network Address 200.1.1.128/25 | No.of Host 128 Usable Host 126 | | | | | |

**Table 3.5:Subnet of Subnet**

### 3.2 VLAN Implementation to Campus Area Network (CAN)

VLANs segment a network, creating multiple broadcast domains, they effectively allow traffic from the broadcast domains to remain isolated while increasing the network's bandwidth, availability and security. We have suggested some VLANs for better security of campus network and reducing Broadcast.[16]

### 3.3 VTP Implementation

VLAN design is used using VLAN Trunking protocol (VTP) to fulfill our objective to reduce the much administrative work with less costing. We have configure the VTP model by interconnecting five switches such that one (Central_Office Switch) acts as VTP Server and the other three are clients. VTP server will automatically update the summary/subset advertisement to all the connected clients. In the second part we have connected a router with single interface with the VTP Server switch to simulate inter-VLAN Routing.[19]

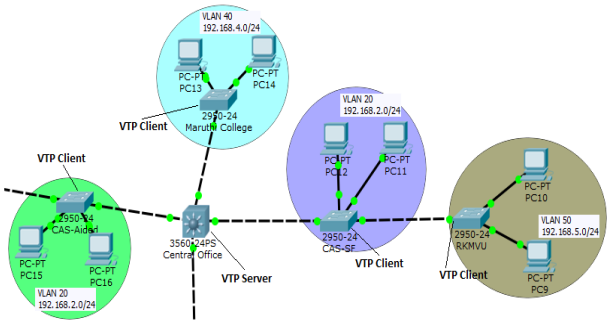



Fig 3.8:VTP Implementation on CAN.

### 3.4 Inter-VLAN Routing Implementation to Campus Area Network (CAN)

Inter-VLAN routing technique is a technique which is used to allow different VLANs to communicate. In order to communicate we make use of router interface or multilayer switches. Different methods for accomplishing inter-VLAN routing.

#### 3.4.1 Traditional inter-VLAN

Traditionally, LAN routing has used routers with multiple physical interfaces. Each interface needed to be connected to a separate network and configured for a different subnet.

In a traditional network that uses multiple VLANs to segment the network traffic into logical broadcast domains, routing is performed by connecting different physical router interfaces to different physical switch ports. The switch ports connect to the router in access mode; in access mode, different static VLANs are assigned to each port interface. Each switch interface would be assigned to a different static VLAN. Each router interface can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces. In Fig 3.10 Traditional inter-VLAN routing requires multiple physical interfaces on both the router and the switch. However, not all inter-VLAN routing configurations require multiple physical interfaces. Some router software permits configuring router interfaces as trunk links. This opens up new possibilities for inter-VLAN routing.[16,26]

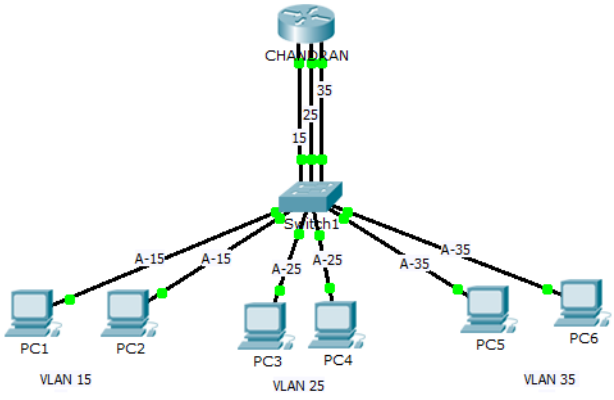



Fig 3.10: Traditional inter-VLAN

#### 3.4.2 Router-on-a-stick

Fig 3.11 "Router-on-a-stick" is a type of router configuration in which a single physical interface routes traffic between multiple VLANs on a network. As you can see in the figure, the router (CHANDRAN) is connected to switch1 using a single, physical network connection. The router interface is configured to operate as a trunk link (T)

and is connected to a switch port configured in trunk mode. The router performs the inter-VLAN routing by accepting VLAN tagged traffic on the trunk interface coming from the adjacent switch and internally routing between the VLANs using subinterfaces. The router then forwards the routed traffic-VLAN tagged for the destination VLAN-out the same physical interface.

Subinterfaces are multiple virtual interfaces, associated with one physical interface. These subinterfaces are configured in software on a router that is independently configured with an IP address and VLAN assignment to operate on a specific VLAN. Subinterfaces are configured for different subnets corresponding to their VLAN assignment to facilitate logical routing before the data frames are VLAN tagged and sent back out the physical interface. [16,26]

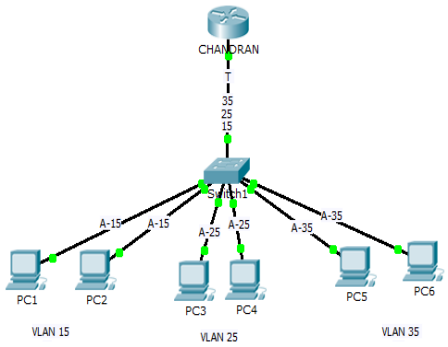



Fig 3.11: Router-on-a-stick

### 3.4.3 Inter-VLAN routing using Multilayer switch

Switches can perform Layer 3 functions, replacing the need for dedicated routers to perform basic routing on a network. Multilayer switches are capable of performing inter-VLAN routing.

In Fig 3.12 multilayer switch to perform routing functions, VLAN interfaces on the switch need to be configured with the appropriate IP addresses that match the subnet that the VLAN is associated with on the network. The multilayer switch also must have IP routing enabled. [16,26]

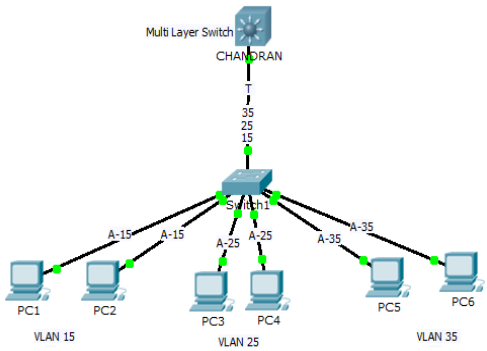



Fig 3.12 : Inter-VLAN routing using Multilayer switch

### 3.5 Redundant Link configuration

The Local Area Network data travel from source to destination it was enabled more than one links on the switch1 to switch2 then the network was increased reliability.

#### 3.5.1 STP with redundant Link

The already implemented technique Spanning Tree Protocol (STP) will block redundant links to prevent routing loops.

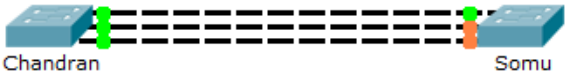



Fig 3.13 :STP with redundant Link

#### 3.5.3 Link Aggregation using Etherchannel

Link aggregation is the ability to create one logical link using multiple physical links between two devices. This allows load sharing among the physical links, rather than having STP block one or more of the links. EtherChannel is a form of link aggregation used in switched networks

#### 3.5.3.1 Etherchannel

Etherchannel is a new technique to increase the Local Area Network speed. This technique make a single logical link to multiple physical link. The etherchannel implemented in two LAN devices and allow load sharing among the physical link. Etherchannel can be done by using Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) configuration.


Fig 3.17 :Link Aggregation

#### 3.5.3.2 EtherChannels Protocol

EtherChannels can be formed through negotiation using one of two protocols, PAgP or LACP. These protocols allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches.

## IV. RESULTS AND DISCUSSION

### 4.1 IP Address Allocation Result

Multiple size subnets or multiple level subnets to maximize the utilization of IPs. It is obvious that more than one subnet masks can be used for a subnetted network. VLSM divides an address space recursively and aggregates to reduce routing information .This technique uses a

hierarchical structure where subnets may be further subnetted.

In Table 4.2 IP Address was allocated in 7 institute in Vidyalaya Campus. And compare the three method of IP allocation and find the suitable technique is VLSM.

| Place | No Of User | Wastage IP (Using class C | | |
|---|---|---|---|---|
| | | Normal IP | Subnetting | VLSM |
| B.Ed & GTTI | 10 | 244 | 20 | 4 |
| CAS-Aided & SF | 100 | 154 | 26 | 26 |
| RKMVU | 25 | 229 | 5 | 5 |
| School | 10 | 244 | 20 | 4 |
| Maruthi College | 10 | 244 | 20 | 4 |
| ITI | 12 | 242 | 18 | 2 |
| Polytechnic | 30 | 224 | 96 | 0 |
| Total Wastage IP | | 1581 | 205 | 45 |
| **Total IP Network Used** | | **7** | **2** | **1** |

Table 4.2: IP Address Allocation in Campus Area Network

In Fig 4.1: Comparing the three method of IP address allocation in Chart View.

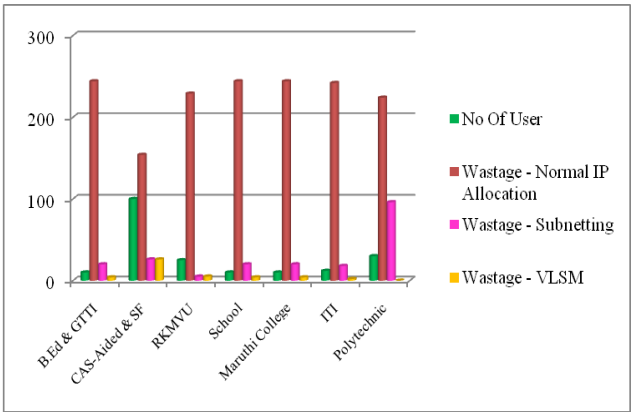



Fig 4.1: Comparing the three method of IP allocation

**4.2 VLAN Implementation Result**

In Table 4.3 mention about the Vlan allocation in different institute of Vidyalaya campus.

| S.No | VLAN ID | VLAN NAME |
|---|---|---|
| 1 | VLAN 20 | CAS_Aided&SF |
| 2 | VLAN 30 | B.Ed&GTTI |
| 3 | VLAN 40 | MaruthiCollege |
| 4 | VLAN 50 | RKMVU |
| 5 | VLAN 60 | Polytechnic |
| 6 | VLAN 70 | ITI |
| 7 | VLAN 80 | School |

Table 4.3: VLAN Allocation

```
CentralOffice(config)#vlan 20
CentralOffice(config-vlan)#name CAS_Aided&SF
CentralOffice(config-vlan)#exit
CentralOffice(config)#vlan 30
CentralOffice(config-vlan)#name B.Ed&GTTI
CentralOffice(config-vlan)#exit
CentralOffice(config)#vlan 40
CentralOffice(config-vlan)#name MaruthiCollege
CentralOffice(config-vlan)#exit
CentralOffice(config)#vlan 50
CentralOffice(config-vlan)#name RKMVU
CentralOffice(config-vlan)#exit
 CentralOffice(config)#vlan 60
CentralOffice(config-vlan)#name Polytechnic
CentralOffice(config-vlan)#exit
CentralOffice(config)#vlan 70
CentralOffice(config-vlan)#name ITI
CentralOffice(config-vlan)#exit
CentralOffice(config)#vlan 80
CentralOffice(config-vlan)#name School
CentralOffice(config-vlan)#exit
CentralOffice(config)#exit
```

```
CentralOffice#show vlan
VLAN  Name                             Status    Ports
---- -------------------------------- --------- -------------------
  1   default                          active    Fa0/1, Fa0/2,
                                                 Gig0/1, Gig0/2
20    CAS_Aided&SF                     active
30    B.Ed&GTTI                        active
40    MaruthiCollege                   active
50    RKMVU                            active
60    Polytechnic                      active
70    ITI                              active
80    School                           active
1002  fddi-default                     act/unsup
1003  token-ring-default               act/unsup
1004  fddinet-default                  act/unsup
1005  trnet-default                    act/unsup
```

### 4.3 VLAN Trunking Protocol (VTP) Implementation Result

**VTP Server:**

```
Centraloffice(config)# vtp mode Server
Centraloffice(config)#vtp domain Vidyalaya
Centraloffice(config)#vtp password vidyalaya
Centraloffice(config)#^Z
```

**VTP Client:**

```
RKMVU#config t
RKMVU(config)#vtp mode Client
RKMVU(config)# vtp domain Vidyalaya
RKMVU(config)# vtp password vidyalaya
RKMVU(config)#^Z
```

### 4.4 Inter-VLAN routing Implementation Result

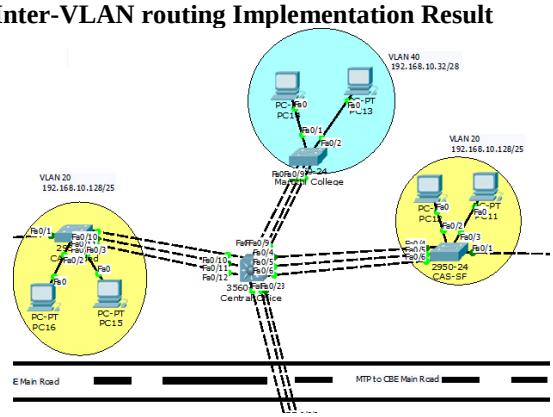



Fig 4.2 : Inter-VLAN routing using Multilayer switch

```
Centraloffice(config)#ip routing
Centraloffice(config)#interface vlan 20
Centraloffice(config-if)#ip address 192.168.2.254
255.255.255.0
Centraloffice(config-if)#exit
Centraloffice(config)#INterface VLan 30
Centraloffice(config-if)#IP ADDress 192.168.3.254
255.255.255.0
Centraloffice(config-if)#exit
Centraloffice(config)#INterface VLan 40
Centraloffice(config-if)#IP ADDress 192.168.4.254
255.255.255.0
Centraloffice(config-if)#exit
Centraloffice(config)#interface vlan 50
Centraloffice(config-if)#no shu
Centraloffice(config-if)#ip address 192.168.5.254
255.255.255.0
Centraloffice(config-if)# exit
Centraloffice(config)#INterface VLan 60
Centraloffice(config-if)#IP ADDress 192.168.6.254
255.255.255.0
Centraloffice(config-if)#exit
Centraloffice(config)#INterface VLan 70
Centraloffice(config-if)#ip address 192.168.7.254
255.255.255.0
Centraloffice(config-if)#exit
Centraloffice(config)#INterface VLan 80
Centraloffice(config-if)#IP ADDress 192.168.8.254
255.255.255.0
Centraloffice(config-if)#
```

### 4.5 Redundant Link Configuration Result

```
Central-Office(config)#interface range fastEthernet 0/1-3
Central-Office(config-if-range)#channel-group 1 mode
active
Central-Office(config-if-range)#exit

Central-Office(config)#interface port-channel 1
Central-Office(config-if)#switchport mode trunk
Central-Office(config-if)#^Z

Central-Office#show spanning-tree active
        VLAN0001
         Spanning tree enabled protocol ieee
         Root ID    Priority    32769
                    Address     0001.4310.A1CB
                    Cost        19
                    Port        4(FastEthernet0/4)
                    Hello Time  2 sec  Max Age 20 sec
        Forward Delay 15 sec

         Bridge ID  Priority    32769  (priority 32768 sys-
        id-ext 1)
                    Address     0090.0CA6.941A
                    Hello Time  2 sec  Max Age 20 sec
        Forward Delay 15 sec
                    Aging Time  20
```

| Interface | Role | Sts | Cost | Prio.Nbr | Type |
|---|---|---|---|---|---|
| Fa0/4 | Root | FWD | 19 | 128.4 | P2p |
| Fa0/5 | Altn | BLK | 19 | 128.5 | P2p |
| Fa0/6 | Altn | BLK | 19 | 128.6 | P2p |
| Fa0/7 | Desg | FWD | 19 | 128.7 | P2p |
| Fa0/8 | Desg | FWD | 19 | 128.8 | P2p |
| Fa0/9 | Desg | FWD | 19 | 128.9 | P2p |
| Fa0/10 | Desg | FWD | 19 | 128.10 | P2p |
| Fa0/11 | Desg | FWD | 19 | 128.11 | P2p |
| Fa0/12 | Desg | FWD | 19 | 128.12 | P2p |
| Po1 | Desg | FWD | 8 | 128.27 | Shr |

```
Central-Office#config t
Central-Office(config)#interface range fastEthernet 0/4-6
Central-Office(config-if-range)#channel-group 2 mode active
Central-Office(config-if-range)#exit
Central-Office(config)#interface port-channel 2
Central-Office(config-if)#switchport mode trunk
Central-Office(config-if)#exi
Central-Office(config)#interface range fastEthernet 0/7-9
Central-Office(config-if-range)#channel-group 3 mode active
Central-Office(config-if-range)#exit
```

```
Central-Office(config)#interface port-channel 3
Central-Office(config-if)#switchport mode trunk
Central-Office(config-if)#exit

Central-Office(config)#interface range fastEthernet 0/10-12
Central-Office(config-if-range)#channel-group 4 mode
active
Central-Office(config-if-range)#exit

Central-Office(config)#interface port-channel 4
Central-Office(config-if)#switchport mode trunk
Central-Office(config-if)#
Central-Office#show spanning-tree active
        VLAN0001
          Spanning tree enabled protocol ieee
          Root ID    Priority    32769
                Address     0001.4310.A1CB
                Cost        8
                Port        28(Port-channel 2)
                Hello Time  2 sec  Max Age 20 sec
        Forward Delay 15 sec
        Bridge ID  Priority    32769  (priority 32768 sys-id-
        ext 1)
                Address     0090.0CA6.941A
                Hello Time  2 sec  Max Age 20 sec
        Forward Delay 15 sec
                Aging Time  20

        Interface       Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------
        Po4             Desg FWD 8         128.30   Shr
        Po3             Desg FWD 8         128.29   Shr
        Fa0/7           Desg FWD 19        128.7    P2p
        Fa0/8           Desg FWD 19        128.8    P2p
        Fa0/10          Desg FWD 19        128.10   P2p
        Fa0/11          Desg FWD 19        128.11   P2p
        Po1             Desg FWD 8         128.27   Shr
        Po2             Root FWD 8         128.28   Shr
Central-Office#
```

### 4.5.1 Port Channel

The Fig 4.3 mention about the etherchannel configuration in four institute of vidyalaya campus. In this figure Three physical line was converted in single virtual line in each institute

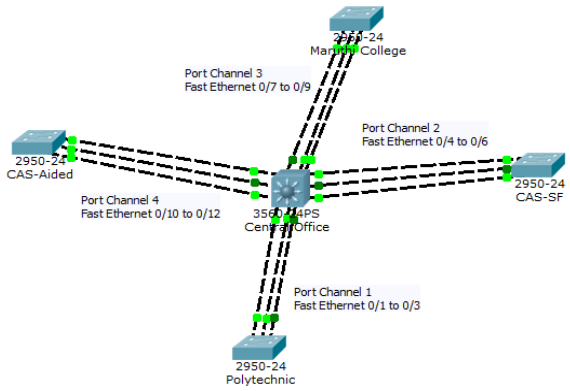
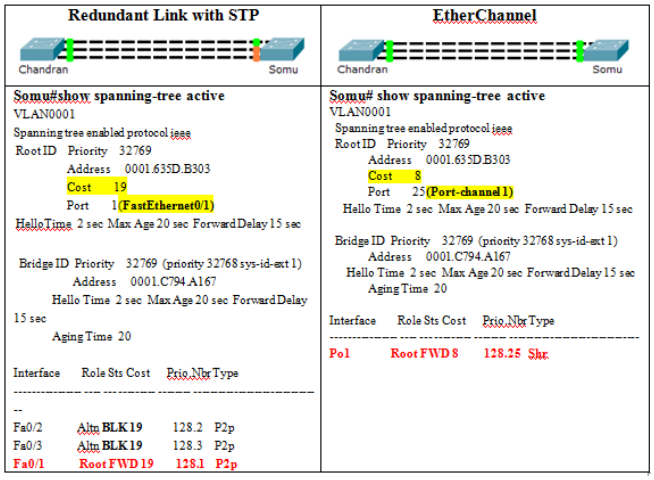



Fig 4.3 : Port Channel Configuration

### 4.5.2 Difference between STP Network and Etherchannel Network

In fig 4.4 is mention about the major difference between redundant link with STP Network and Etherchannel based Network.




| Network Performance | No of Port Usage | Speed (Per Sec) | Redundant | Network | Data Travelling Time |
|---|---|---|---|---|---|
| Using STP | 3 | 100Mbps | Yes | Sw1 Sw2 | 0.988 Sec |
| Etherchannel | 3 | 300Mbps | Yes | S1 S2 | 0.023Sec |

Fig 4.4 : Comparison of STP Network and Etherchannel Network

### 4.6 VLAN ACL (VACL) Configuration Result

VLAN ACL also called VLAN map provides packet filtering for all types of traffic that are bridged within a VLAN or routed into or out of the VLAN. Unlike Router ACL, VACL is not defined by a direction. All packets

entering the VLAN are checked against the VACL. It is possible to filter traffic based on the direction.

```
Central-Office#config t
Central-Office(config)#access-list 100 deny tcp host
192.168.10.18 host 192.168.10.132 eq 7
Central-Office(config)#access-list 100 permit ip any any
Central-Office(config)#exit
Central-Office(config)#interface vlan 20
Central-Office(config-if)#ip access-group 100 in
Central-Office(config-if)#exi
Central-Office(config)#access-list 10 deny host
192.168.10.18
Central-Office(config)#access-list 10 permit any
Central-Office(config)#exit

Central-Office#config t
Central-Office(config)#interface vlan 20
Central-Office(config-if)#ip access-group 10 out
Central-Office(config-if)#exit

Central-Office#show access-lists
        Extended IP access list 100
           deny tcp host 192.168.10.18 host 192.168.10.132
        eq 7
           permit ip any any (19 match(es))
        Standard IP access list 10
           deny host 192.168.10.18 (3 match(es))
           permit any (2 match(es))
Central-Office#
```

## V. CONCLUSION AND FUTURE SCOPE

This research work is completely based upon new network architecture and its security of Campus Area Network (CAN). Class C addresses are most widely used but are limited to 254 hosts at the most. To cater the performance issue, a network is divided into different subnets instead of using maximum hosts on a single network. This way we achieve improved security, controlled administration and traffic isolation, but at the cost of address space wastage. This wastage is maximum for FLSM and is reduced using VLSM.

EtherChannel aggregates multiple switched links together to load balance over redundant paths between two devices. All ports in one EtherChannel must have the same speed, duplex setting, and VLAN information on all interfaces on the devices at both ends. setting configured in the port channel interface configuration mode will be useful to the individual interfaces in that EtherChannel. This Technique improve the network speed in Campus Area Network.

ACL's is used to secure and control traffic into or out of networks. In their individual VLAN, securing network attacks and controlling access to them. An administrator can disable ICMP echoes and other protocols used to detect a live host, avoid probable detection by an attacker host located over a different VLAN. After configuring ACL, router works as a firewall and checks each statement sequentially before forwarding the traffic to its destination. By using standard or extended access-lists, a router processes each ACL from top to bottom, one statement at a time. We propose extended ACL's to filter the traffic between VLAN's or between hosts of a VLAN.

To realize the following network design, network will be scalable, security and the network will be easy to maintain. In this research work, we propose a condensed cost effective, scalability, protection and secure campus network design based on the work atmosphere.

## REFERENCES


[1] Cisco Networking Academy "CCNA 3 and 4 Companion Guide", Pearson Education,2003

[2] W. A. Arbaugh, J. R. Davin, "Security for virtual private intranets," Computer, vol. 31 (9), pp. 48-55, 1998.

[3] P. Vicrt-Blanc-Primet, J. Zeng, "Traffic isolation and network resource sharing for performance control in grids," utonomic and Autonomous Systems and International Conference on Networking and Services, 2005.

[4] L. S. Putledge, L. J. Hoffman, "A survey of issues in computer network security," Computers and Security, vol. 5 (4), pp. 296-308, 1986.

[5] G. Rapp, "Survey of the computer and network security issues from evalutation criteria to open systems," Proceedings of the Conference on the Challenge of Networking: Connecting Equipment, Humans, Instituitions, 1993.

[6] R. Venkatesmaran, "Virtual private networks," IEEE Potetials, vol. 20, pp. 11-15, 2001.

[7] M. A. Ruiz-Sanchez, E. W. Biersack, W. Dabbous, "Survey and taxonomy of IP address lookup algorithms," IEEE Network, vol 15 (2), pp. 8-23, 2001

[8] V. Grout, "Towards an optimal routing strategy," Proceedings of IADIS WWW/Internet, 2003.

[9] C. L. Hedrick, "RFC1058: Routing information protocol," Internet RFCs,1988.

[10] "InterVLAN Routing – Routing between VLAN Networks" Available:http://www.firewall.cx/networking- topics/vlan-networks/222-intervlan-routing.html.

[11] Milan 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 Paper in IEEE Communications Magazine July, Volume: 49, Issue: 7 pp. 98-103

[12] K. Okayama , "A Method of Dynamic Interconnection of VLANs for Large Scale VLAN Environment", IEEE, ISBN: 4-88552-216-1, page.427 - 432

[13] Cisco Press,"CCNA Exploration Course Booklet: LAN Switching and Wireless, Version 4.0" Cisco networking Academy.

[14] Allan Johnson, "LAN Switching and Wireless: CCNA Exploration Labs and Study Guide" Cisco Press,ISBN: 1587132028,2008.

[15] Somasundaram.S , Chandran.M. "Discovery of Geo-Locations by Tracing IP Address Using VLSM Technique". International Journal of P2P Network Trends and Technology (IJPTT)".V11:1-4 Sep 2014. ISSN: 2249-2615. www.ijpttjournal.org. Published by Seventh Sense Research Group.

[16] Somasundaram.S, Chandran.M. "A Simulation Based Study on Inter-VLAN Routing" International Journal of Computer Sciences and Engineering (JCSE)". Volume 4 Issue 7, Page 24 -29, July 2016. ISSN: 2347-2693
[17] Cisco, "Configure InterVLAN Routing on Layer 3 Switches", 2016, [Online]. Available:http://www.cisco.com /c/en/us/support/docs/lan-switching/inter-vlan-routing/ 41860 - howto-L3-intervlanrouting.pdf
[18] Cisco," Configuring InterVLAN Routing with Catalyst 3750/3560/3550 Series Switches", 2014 [Online]. Available: http://www.cisco.com/c/en/us/ support/docs/lan-switching/inter-vlan-routing/41260-189.pdf
[19] Rajiv O. Verma, S.S. Shriramwar "Effective VTP Model for Enterprise VLAN Security" 2013 International Conference on Communication Systems and Network Technologies
[20] Cisco, "Understanding vlan trunk protocol (vtp)," 2007. [Online].Available:http://www.cisco.com/application/pdf /paws /10558/21.pdf
[21] Cisco, "Troubleshooting vlan trunk protocol (vtp)," 2007.[Online].Available:http://www.cisco.com/application/pdf/paws/98155/tshoot-vlan.pdf
[22] Sharada Ramani and R. M. Goudar,"Improved Bandwidth Aggregation using Available Lower Bandwidth Links", International Journal of Computer Sciences and Engineering, Volume-4, Issue-6, ISSN: 2347-2693, 2016
[23] Rajiv O. Verma, "Effective Remote Management for Inter-VLAN Routing Networks" International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 - 4847,2013.
[24] LI Xingyu, Jiang Tingting, "Design and implementation of the Campus Network Monitoring System" IEEE Workshop on Electronics, Computer and Applications, 2014.
[25] M.R. Sabir , M.S. Mian , K. Sattar and M.A. Fahiem, "IP Address Space Management using Aggregated Fixed Length Subnet Masking", IEEE Network.
[26] "Cisco Packet Tracer 6.0.1 Tool" Cisco Networking Academy

## Authors Profile

***S.Somasundaram*** currently pursuing Ph.D and currently working as Assistant –Professor in Department of Computer Applications, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore, India since 2014. He is CCNA Certified Engineer and Certified Instructor. His main research work focuses on Network Security. He has published 3 research papers in reputed international journals.

***M.Chandran*** currently pursuing Ph.D. and currently working as Assistant –Professor in Department of Computer Applications, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore, India since 2006. His main research work focuses on Quality analysis in software Engineering and Web based analysis. He has published 12 research papers in reputed international journals and Presented 2 International paper .He has Co-investigator for UGC 1 Miner Research Project and so on. He has 10 years of teaching experience and 5 years of Research Experience.