# Secure Network Implementation using VLAN and ACL

Mr J. Ramprasath, Dr S. Ramakrishnan, P. Saravana Perumal, M. Sivaprakasam, Vishnuraj, U. Manokaran

Department of Information Technology, Dr. Mahalingam College of Engineering and Technology, Pollachi, Tamil Nadu, India

***Abstract*****—***The contributions of this article are two folds; first, we introduce the virtual LAN and second one is the introduction of time varying nodes. In virtual LAN implementation we segregate the network into two groups such as staff and students systems. By separating the network into two groups the staff system will receive only their information and students system will receive only the student's data and no other staff information will be received. By introducing this concept, security is maintained so that unwanted access of data is restricted. The router and the switches in the LAN will be configured to implement the virtual LAN. Each VLAN is given a separate name and identification number. By using this we can easily identify the VLAN's present inside the campus network. Data can be transferred only within the nodes present inside the VLAN. No other nodes present outside VLAN can receive the data which means that security is assured for sure. The main aim of moving to VLAN is that it can provide segregation of groups, by means of which security is provided. Here these concepts are used for the campus network which consists of two groups such as students and staff.*

***Keywords— VLAN, time varying nodes, Firewall***

## I. INTRODUCTION

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and multicast, unicast and broadcast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN [1] is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge. Because a VLAN [1] is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

## II. NEEDS OF VLAN

Initially LANs were very flat—all the workstations were connected to a single piece of coaxial cable, or to sets of chained hubs. Every packet that any device puts onto the wire gets sent to every other device on the LAN. The number of workstations on the typical LAN grew, they started to become hopelessly congested; there were just too many collisions, because most of the time when a workstation tried to send a packet, it would find that the wire was already occupied by a packet sent by some other device.

The three solutions for this congestion that were developed:

- Using routers to segment LANs
- Using switches to segment LANs
- Using VLANs to segment LAN

Routers that forward data in software become a bottleneck as LAN data rates increase. Doing away with the routers removes this bottleneck. Because workstations can be moved from one VLAN to another just by changing the configuration on switches, it is relatively easy to put all the people working together on a particular project all into a single VLAN. They can then more easily share files and resources with each other. To be honest, though, virtual workgroups sound like a good idea in theory, but often do not work well in practice. It turns out that users are usually more interested in accessing.

## III. OVERVIEW

Normally in our campus, FTP is provided to transfer the data from one system to the other system. In the existing LAN the FTP has two logins. One of the login is used by the staff and the other is used by the student. Since security is not provided, even the student can login into the staff FTP by entering their password. For example the staff may have the exam question paper in their FTP, students by logging in can easily get the question papers. In the present system one can easily access to the others account because it is the only password protected system. In order to avoid these kinds of issues we are going for VLAN implementation for the campus network. The main objective of this project is to provide the security to the existing LAN connection by implementing VLAN.

In the normal system, there will be wastage of resources. This means that, when VLAN is implemented the appropriate details will go only to that system. For example the data corresponding to the staff system will reach only staff systems and the data corresponding to the student system will reach only the student systems. A main disadvantage present in this system is that, staff system will not be used continuously after the working hours. Whereas, only the students will use the system in the extra hours and during non-working days. This leads to wastage of resources. In order to avoid this kind of situation we are going in for time varying nodes. By using this time varying nodes we can allot time for the particular resources [2]. Only for that particular time that resource will be active and after that time the resource will be allotted for different use.

### 3.1 Creating the VLAN

Initially enter into the global configuration mode by giving the command configure terminal. Then the second step is to create a VLAN with a valid id number. This is done by giving the command vlan vlan_id. The number of vlans will be decided based on the user requirements. For example in the college network staffs and the students require separate VLANs so two VLANs will be created. In this way the number of VLAN creation varies. The third step is to specify the names for the VLAN that we have created in the previous step. This is done by giving the command name vlan_name. Finally, return to the privileged EXEC mode by giving end.

The following table describes about the steps involved.

*TABLE 1 Creating the VLAN*

| | |
|---|---|
| Enter global configuration mode | S1# configure terminal |
| Create the vlan | S1 (config)# VLAN VLAN_id |
| Specify unique name | S1 (config)# name vlan_name |
| Return | S1 (config)# End |

### 3.2 Assigning the Ports to VLAN

Initially enter into the global configuration mode by giving configure terminal command. Then enter into the interface configuration mode by using the command interface interface_id and configure the management interface IP address by giving the command ip address particular_ip_address. Set the port to access mode using switchport mode access and assign the port to a VLAN by switch port access vlan vlan_id command. At last return to the privileged EXEC mode by giving end command. The following table describes about the steps involved in the port assignment to the VLAN in detail:

*TABLE 2 Assigning the ports to VLAN*

| | |
|---|---|
| Enter global configuration mode. | S1 # **configure terminal** |
| Enter interface configuration mode for the SVI | S1(config) # **interface** interface_id |
| Configure the management interface IP address | S1(config) # **ip address 172.17.99.11** |
| Set the port to access mode | S1(config) # **switchport mode access** |
| Assign the port to a VLAN | S1(config) # **switchport access vlan** vlan_id |
| Return to the privileged EXEC mode | S1(config) # **end** |

### 3.3 Configuring the Trunk Links

The first and foremost step is to enter into the global configuration mode by giving configure terminal. The second step is to enter into the interface configuration mode by using the command interface interface_id. In addition to it specify the list of VLANs to be allowed to trunk link by giving switchport trunk allowed vlan vlan_list. Then return to the privileged EXEC mode by giving the end command.The following table describes about the steps involved in configuring the trunk links in detail:

*TABLE 3 Configuring the Trunk Links*

| | |
|---|---|
| Enter global configuration mode. | S1 # **configure terminal** |
| Enter interface configuration mode. | S1(config) # **interface** interface_id |
| Force the link to be a trunk link. | S1(config) # **switchport mode trunk** |
| Specify a native VLAN for untagged 802.1Q trunks | S1(config) # **switchport trunk native vlan vlan_id** |
| Specify the list of VLANs to be allowed on the trunk link. | S1(config) # **switchport trunk allowed vlan vlan_list** |
| Return to the privileged EXEC mode | S1(config) # **end** |

### 3.4 Inter VLAN Routing

Networks are constantl constantly evolving, and in the past few years a number of trends have become apparent. First of all, the Internet Protocol (IP) has become the Layer 3 protocol of choice for modern networks, with other Layer 3 protocols such as Internetwork Packet Exchange (IPX) and AppleTalk rapidly being phased out. IP interconnects the Internet. The increasing reliance of organizations on the Internet has promoted IP as the Layer 3 protocol of choice. Secondly, local-area networks (LANs) have seen tremendous advances in terms of performance, bandwidth, and lowering cost. The LAN provides the medium over which users and devices connect to the internal IP network and the Internet hence is an important component of networking. LAN topologies have evolved from traditionally being single, flat broadcast domains into multi-virtual LAN (VLAN) topologies, with inter-VLAN routing required to enable communications between each VLAN [2]. Multiple VLANs increase network efficiency by reducing broadcast domain size, as well as providing a mechanism to allow network layer access control to be applied between VLANs.

### 3.5 Configure Inter VLAN Routing

This logical diagram explains a simple inter VLAN routing [3] scenario. The scenario can be expanded to include a multi-switch environment by first configuring and testing inter-switch connectivity across the network before configuring the routing capability. For such a scenario that uses a Catalyst 3550, refer to Configuring Inter VLAN Routing with Catalyst 3550 Series Switches.

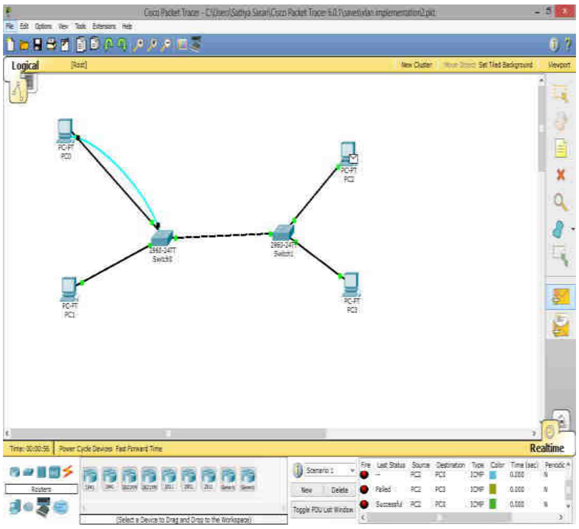
## IV. RESULTS AND DISCUSSIONS

In the existing system that is in the normal LAN we face numerous problems. In order to avoid these tough scenarios, we have implemented virtualization concept in LAN which is also known as VLAN. By the usage of this virtualization concept we can reduce the number of problems that occurs in our existing system. Though it may require some additional hardware components, it is one of the best methods to prevent the problems that occur frequently in our existing system. Grouping facility is not available in our current LAN. But this can be very easily done with the help of virtualization techniques i.e. by implementing the VLAN. The nodes that we want to group can be done just by configuring the switches. Once they are configured correctly each VLAN is given a name and id. These names and ids are used only for the purpose during verification and if there comes any situation which involves the addition or removal of nodes from the VLAN then these ids and the names can be used. So virtualization concept helps the users by allocating the nodes into separate groups and thus security is also provided, which is the major need.

Since, in our project we have implemented the VLAN concept for campus networks we have named the VLANs as staff VLAN and student VLAN. The confidential data transferred from the staff VLAN will not reach the student VLAN, which means that security is assured.

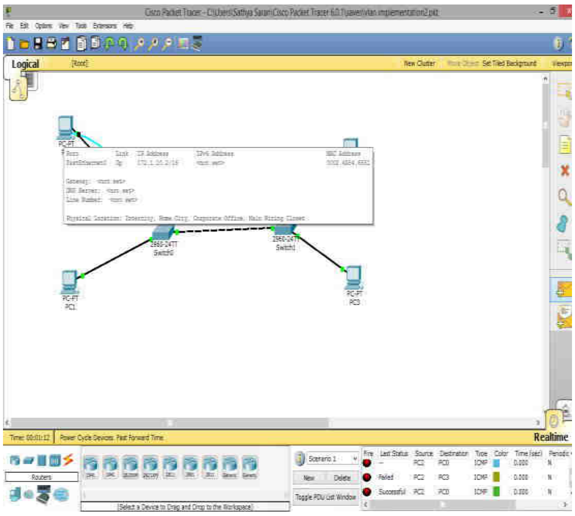
The figure given below shows the maximum number of nodes that can be accommodated to the switch. Based upon the requirements of VLAN the appropriate switch can be used.

And here the below figure shows us about the packet transfer. Packets can be transferred only between the nodes present inside the VLAN. This shows that the grouping is done and security is maintained. The two groups such as the student group and the staff group commonly mentioned here as student VLAN and staff VLAN are used in the campus networks. Here the packets from the staff VLAN cannot propagate to the student VLAN and the vice versa is also not possible. By means of using this VLAN we can share the data among the users of similar kinds. Grouping and security is also provided which is not available in the existing system. The output is shown as successful if and only if the packet is delivered correctly. If there is any loss of packets or any hardware problems or if the user tries to transfer the content to different VLANs we cannot get proper output.



| Fire | Last Status | Source | Destination | Type | Color | Time (sec) | Periodic |
|---|---|---|---|---|---|---|---|
| ● | -- | PC2 | PC3 | ICMP | 🟦 | 0.000 | N |
| ● | Failed | PC2 | PC3 | ICMP | 🟨 | 0.000 | N |
| ● | Successful | PC2 | PC3 | ICMP | 🟩 | 0.000 | N |

*Fig.1: VLAN connection*



| Port | Link | IP Address | IPv6 Address | MAC Address |
|---|---|---|---|---|
| FastEthernet0 | Up | 172.1.20.2/16 | <not set> | [illegible] |

Gateway: <not set>
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

| Fire | Last Status | Source | Destination | Type | Color | Time (sec) | Periodic |
|---|---|---|---|---|---|---|---|
| ● | -- | PC2 | PC0 | ICMP | 🟦 | 0.000 | N |
| ● | Failed | PC2 | PC3 | ICMP | 🟨 | 0.000 | N |
| ● | Successful | PC2 | PC0 | ICMP | 🟩 | 0.000 | N |

*Fig.2: Packet Transfer*

## V. CONCLUSIONS

In our project we have implemented the secured LAN for the campus by implementing the VLAN. VLANs are mutually isolated and packets can only pass between them via a router. The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch. Thus by implementing the concept of VLAN, segregation of groups is done, so that the security will be provided. The major advantage is that it reduces the unwanted access of the packets. Thus by using the virtualization concept network traffic will be reduced and security will be provided. A secured campus network can be implemented. Inter VLAN routing is implemented in the routers. Inter VLAN routing helps in the communication between routers.

## VI. FUTURE WORK

The future work is the introduction of time varying nodes. Experimental results demonstrate the performance achieved by the proposed work in terms of the increased profit, resource utilization and number of accepted requests. A novel model for time varying VN requests based on demand-utility functions will be presented. By using the time varying nodes we can allocate the time for specific nodes. Once the time is allocated for the nodes present in VLAN, the functionality of the nodes varies. So that the VN users can determine the required resources for the VN requests embedded using a novel hierarchical VN embedding scheme via exact sub graph matching.

## REFERENCES

[1] Pricing Utility-Based Virtual Networks, On Network and Service Management, Vol. 10, No. 2, June 2013

[2] Reconfigurable Data Planes for Scalable Network Virtualization on Computers, Vol. 62, No. 12, December 2013

[3] Yaozu Dong, Xiantao Zhang, Jinquan Dai, and Haibing Guan, A Hybrid Virtualization Solution Balancing Performance and Manageability

[4] Ashiq Khan, Alf Zugenmaier, Dan Jurca, Wolfgang Kellerer, DOCOMO Communications Laboratories Europe GmbH, Network Virtualization:A Hypervisor for the Internet

[5] http://www.cis.ohio-state.edu/~jain/cis788-97