



## EFFECTIVE IMPLEMENTATION OF VLAN AND ACL IN LOCAL AREA NETWORK

**Abubucker Samsudeen Shaffi**

Faculty of Computing Studies, Gulf College  
Muscat, Sultanate of Oman.

Email: [abobacker.shaffi@gulfcollegeoman.com](mailto:abobacker.shaffi@gulfcollegeoman.com)

**Mohaned Al-Obaidy**

Faculty Head for Computing Awards, Gulf College  
Muscat, Sultanate of Oman.

Email: [mohaned@gulfcollegeoman.com](mailto:mohaned@gulfcollegeoman.com)

### Abstract:

Most of the Organizations such as public and private sectors have started deploying computers to their employees to perform their daily work and access resources from their network. This technology has enabled to operate their businesses much faster and more conveniently and also make easy for the organization; there are some problems still faced by the organization such as poor network design by having large broadcast within the network, low security and overhead management. Therefore, many organisations have decided to implement VLAN (Virtual Local area Networks) and ACL (Access Control List) to solve these problems. This paper indicates to redesign Local Area Network by using VLAN and ACL solution.

Keywords: VLAN, ACL

### 1. INTRODUCTION OF VLAN AND ACL

#### 1.1 Vlan

Virtual LAN or VLAN allows network engineers and network administrators to make logical network from physical network. This technology is used to segment a complex network into smaller networks for better manageability, improved performance and security. VLAN logically create segments within the switch based on an organization's function such as department or geographical locations. Therefore, implementing VLAN for any network will achieve the following benefits:

- Easily relocate PCs on the Local Area Network.
- Easily add or remove hosts to or from the LAN.
- Easily modify the LAN configuration.
- Easily control network traffic between the LAN.

- Improve network security.
- Easily manage the network administrations
- Reduce the cost

#### 1.2 Acl

Network security has become the vital role for any organization. The ACL can be implemented in router can be used to apply for network security. Cisco IOS software has features that can implement security for network by using Access Control List. ACL can be used to prevent some packets from flowing through the network. Implementing ACL will achieve the following:

- Prevent unwanted traffic in the network
- Prevent employees from using systems they should not use.
- Protect critical devices existing in the network.

- ACL provides access or denied services.

## 2. SCENARIO

The organization has many departments such as Human Resource, IT department and Finance. Many organizations have some problems in the existing design. For example if any computer request for particular service, the request will be sent to the entire LAN until it gets an acknowledgment from the receiver. Therefore, this network will have a heavy broadcast. Besides, the organisation does not have a switch for each department to reduce broadcasting and to increase the number of broadcasts, because a switch has one broadcast and many collisions. If the two employee attempts send data at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred it will continue to be propagated throughout the network by hubs and repeaters. Retransmitting the losing data, it leads a significant wastage of time and resources. Also, the current setup does not filter unwanted traffic travelling across the network to main hosts. So this will let the most important host vulnerable to any attacks internally. Poor design and large broadcast domain in the existing network will affect network performance and security of the network. Some time it is very difficult to isolate the problems in the networks. It is very difficult to manage the whole networks by the Network administrator. The Figure 1 indicates the existing organization infrastructure.

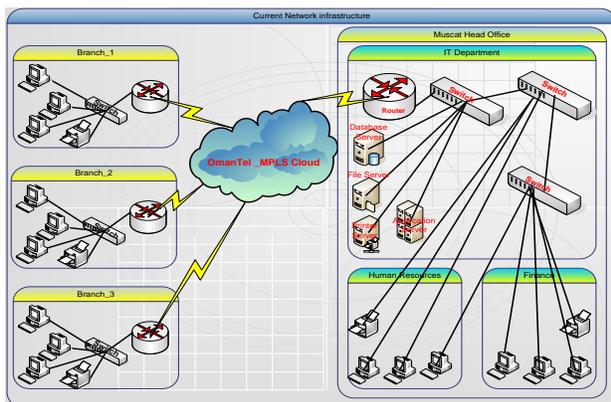


Figure 1: Design for existing organization infrastructure

This organization has started connected all branches through MPLS technology provided by ISP (Internet Service Provider). There is a problem with existing design. All these problems can be solved by the implementation of VLAN and ACL in the organization networks.

## 3. FUNCTIONAL REQUIREMENTS

The type of functionality required for the organization is:

- Network engineer should erase any configuration stored in the router before setting up the new network design.
- Network engineer should choose class B IP address to this network for further growth.
- Network engineer should enter strong password for the network devices. Also, it should be encrypted.
- Each device configured such as router and switch should be backed up and stored in a secure place.
- VLAN encapsulation should be 802.1q
- Network admin should apply Extended Access Control List.
- Network engineer or administrator should create sub interfaces for each VLAN in the router.
- Assign each port in the switch to its related VLAN.

## 4. IMPLEMENTATION OF VLAN:

The VLAN will help to solve this problem. The requirement for new design is Cisco layer 2 switches and layer three devices to carry out the new setup. The organization need to purchase the managed switch which supports the VLAN interface. VLAN should be membership by using port number. All ports or interfaces in the switch are considered in one VLAN and one broadcast domain. The solution for this problem is by configuring VLAN in the switches and to put some ports into one broadcast domain and some into another broadcast within the same switch. So, this will segment hosts into smaller LAN to reduce overhead caused to each device. Therefore, Network

Administrator has created VLAN for each department then enabled the communication between them by using layer three devices. Access Control List has been used to enforce better security and to filter unwanted packets.

#### 4.1 Operation of VLAN

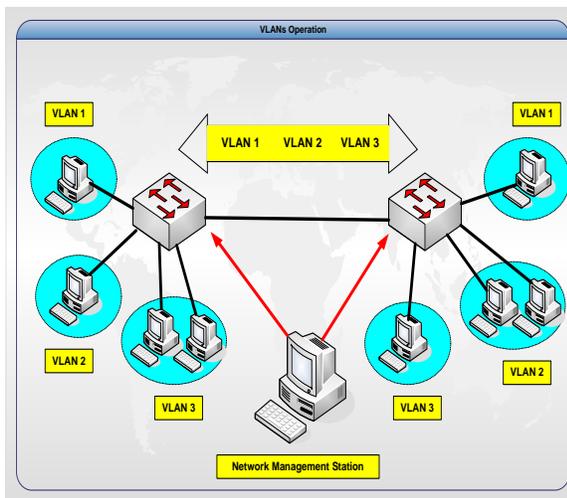


Figure 2: VLANs Operation

VLAN can be implemented in each switch. It acts as one broadcast domain. Switch ports could be assigned to different VLAN. Therefore, any ports assigned to the same VLAN share the same broadcast domain. Each switch can carry more than one VLAN as shown in Figure 2, there are two switches, and each one handles several VLAN. Each VLAN can assign to each department according to the organization requirements shown below.

Table 1: Assigning switch port to VLANs

Switch Port	VLAN	Departments
1	VLAN-1	Human resource
2	VLAN-2	IT
3	VALN-3	Finance

To enable communication between VLAN, trucking Protocol is configured in the link between switches. It will use 802.1q trunking protocol, because the majority of respondents used it for their network configuration. Also, 802.1q is IEEE standard, so we

can enable communication between VLANs with different vendor of switches.

#### 5. IMPLEMENTATION OF ACL

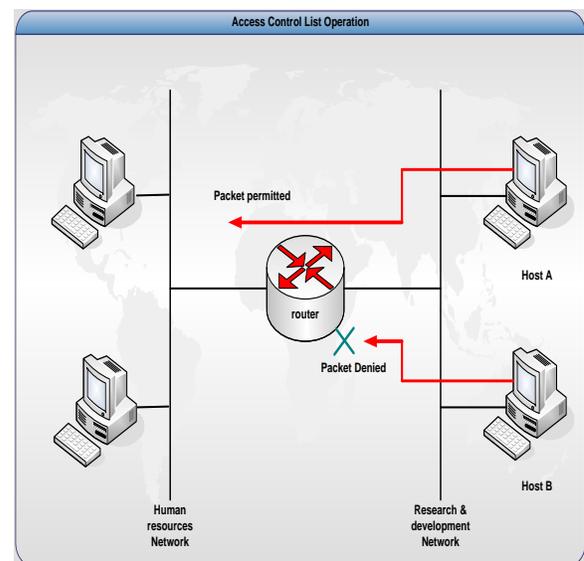


Figure 3: Access Control List Operations

The Network Administrator implements the ACL in the router to give the permission to access or denied permission for the employee in the organization. The Access control list is a technique used to prevent the unwanted the network traffic through the control of packets that are sent or blocked at router interface. The router test every packet accordance with the criteria set within ACLs. Then it makes the decision whether to forward or drop the packet based on IP address and port. The network administrator can use ACL to restrict contents of routing update and to provide security for the network by filtering unwanted traffic. For example, you can permit e-mail traffic to be routed, but at the same time block all Telnet traffic. Network administrator should use access lists to provide a basic level of security for accessing their network.

#### 6. CONFIGURATION OF ROUTER, SWITCH AND HOST

**6.1 Router configuration** For this setup, we will create sub-interfaces for each VLAN needed for each

section. These sub- interfaces that will be created in layer three devices will enable communication between different VLANs. Besides, it will restrict each section to specific IP address scheme. Also, Access Control List will be implemented in the layer three devices to restrict specific hosts from particular action such as telnet.

**6.2 Switch configuration** The setup needed for this device is creating VLANs and assigning each port to its related VLAN. Also, security will be implemented for layer two devices by enabling secret password for switch, console and telnet session.

**6.3 Host configuration** For these devices, assigning IP address will be assigned for each host according to its related VLAN. Also, the default gateway will be the IP address assigned for the sub-interface in the layer three devices.

## 7. TESTING

### 7.1 Scope

The type of testing that will be addressed by plan to ensure the communication between different VLAN through layer three devices. Also, to ensure that each access control list in the routers functioning correctly.

### 7.2. Network administrator Procedures

Network administrator should make sure that every testing phase success. Otherwise, if there is any change, he/she must update the configuration of the item as well as user manual.

### 7.3. Test Strategy

The test document should include the following details of the test strategies, to make the test more efficiently.

Test Strategy	Descriptions
Purpose for this level of test	This will show the test target to meet organizations objective. For example: Ensure ACL function properly and without mistakes.
Items to be tested	This will determine the source host and the

	destination host which to be tested.
Expected Result	This will show the expected result before the test (Pass or fail).
Actual result	This will display the actual result after the test has been completed. For example, Access Control List functions as design without error.
Technique	This will show the test how will be done. For example, this test done by sending denied packet to specific network.
Responsibilities	Here will show the test done by whom.
Schedules	It will display the date of the test.
Comment	It will show if there is a special consideration.

### 7.4 Testing Network Devices

#### 7.4.1 Host to host connection

We going to test connectivity from host connected to switch and host connected in different switch in the same VLAN ID by using ping command. As well as testing the communication between host and the router interface. Also, this project will test the communication between hosts in the same VLAN switch.

#### 7.4.2 Access Control List testing

We going to test ACLs by using Run program in workstation when we want to test access-list from workstation to other destination. On the other hand, when we want to test it from each router to other destination we use Hyper Terminal software.



### 7.4.3 Remote Login Testing

The Telnet service provides a remote login capability. This lets a network engineer on one host or computer log into another host and acts as if he/she is directly in front of the remote router or switch. The connection can be anywhere on the local network. Telnet uses TCP protocol to maintain a connection between two devices. Telnet uses port number 23.

### 7.5 Testing Results

#### 7.5.1 Host to Host Testing

<u>Network Design Using VLAN and ACL</u>	
<b>Test Name</b>	Host to Host
<b>Date</b>	25/06/2012
<b>Test Target</b>	To ensure that there is communication between hosts in the VLAN 2
<b>Source IP</b>	180.182.2.11
<b>Destination IP</b>	180.182.2.12
<b>Technique</b>	By sending Packet from Packet Tracer or by using Ping functionality
<b>Expected result</b>	Pass
<b>Actual Result</b>	Successful. There is a communication between host in the VLAN 2
<b>Comment</b>	
<b>Done By</b>	Administrator

#### 7.5.2 VLAN to Router

<u>Network Design Using VLAN and ACL</u>
--

<b>1</b>	<b>Test Name</b>	VLAN to Router sub-
<b>2</b>	<b>Date</b>	26/06/2012
<b>3</b>	<b>Test Target</b>	To ensure that there is communication between VLAN 2 and its related sub-interface in the router.
<b>4</b>	<b>Source IP</b>	180.182.2.11
<b>5</b>	<b>Destination IP</b>	180.182.2.1
<b>6</b>	<b>Technique</b>	By sending Packet from Packet Tracer or by using Ping functionality
<b>7</b>	<b>Expected result</b>	Pass
<b>8</b>	<b>Actual Result</b>	Successful after fixing the problem and now there is communication between VLAN 2 and it is related sub-interface.
<b>9</b>	<b>Comment</b>	This project has trace what was the problem and find out that on the router sub-interface after encapsulation type we must put the same VLAN ID (encapsulation dot1q 2). So the problem fixed and the result successful as it was planned.
<b>10</b>	<b>Done By</b>	Administrator

#### 7.5.3 Testing Access Control List

<u>Network Design Using VLAN and ACL</u>		
1	<b>Test Name</b>	Checking Access Control List
2	<b>Date</b>	26/06/2012
3	<b>Test Target</b>	To ensure that all hosts in VLAN 3 can not establish Telnet session to router sub-interfaces.
4	<b>Source IP</b>	180.183.3.11 180.183.3.12
5	<b>Destination IP</b>	180.182.2.1 180.183.3.1 180.184.4.1
6	<b>Technique</b>	By sending Packet from Packet Tracer or by using Telnet session.
7	<b>Expected result</b>	Failed, Telnet session can not establish
8	<b>Actual Result</b>	Successful , Telnet session can be established
9	<b>Comment</b>	This project has trace what was the problem and it find out that Access list after it created should be applied on the router to its related logical interface. So the problem fixed and now telnet session can not establish.
10	<b>Done By</b>	Administrator

#### 7.5.4 Testing Routing Functionality

<u>Network Design Using VLAN and ACL</u>		
1	<b>Test Name</b>	Routing Functionality

2	<b>Date</b>	26/06/2012
3	<b>Test Target</b>	To ensure that there is communication between router02 LAN and IT department VLAN 2, because all servers existing in this VLAN
4	<b>Source IP</b>	185.185.5.11
5	<b>Destination IP</b>	180.182.2.1 180.182.2.11 180.182.2.12 180.182.2.13
6	<b>Technique</b>	By sending Packet from Packet Tracer or by using Ping Functionality.
7	<b>Expected</b>	Successful
8	<b>Actual Result</b>	Successful, there is communication between router02 and VLAN 2
9	<b>Comment</b>	To enable routing, we should maintain ip route command in both router01 and router02.
10	<b>Done By</b>	Administrator

#### 8. NETWORK DESIGN FOR VLAN & ACL

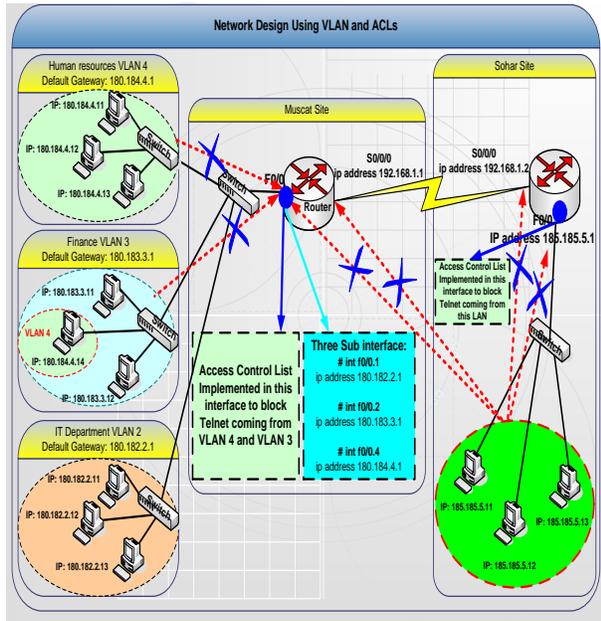


Figure 4: Network design Using VLAN and ACL

The above diagram clearly indicates the how the organizations are effectively implemented the VLAN in switch and ACL in router and how does it operates.

## CONCLUSION

This paper 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:

- To improve manageability that groups users by section instead of by physical section.

- To filter unwanted packets by using ACL such as Telnet and Ping.
- To have more than one broadcast within the same switch by creating more than one VLAN.
- To have an overview of how to troubleshoot VLAN configuration.
- To reduce the cost which eliminate the need for expensive router.

## REFERENCES

- [1]. Computer Networks and Internets, 3rd Edition Comer, D. E. and Droms, R. E. Prentice Hall 2003
- [2]. Computer Networks, 4th Edition Tanenbaum, A. S. Prentice Hall 2004
- [3]. CCNA Voice : Study Guide Exam 640-460 : Froehlich, Andrew, Sybex
- [4]. Computer and Network Technology : Proceedings of the International Conference On ICCNT 2009: Zhou, Jianhong Mahadevan, Venkatesh, World Scientific Publishing Co.
- [5]. Computer Network, Shinde, S.S. New Age International
- [6]. CCNA : Cisco Certified Network Associate Review Guide (640-802): Lammle, Todd, Sybex
- [7]. Odom, W 2008, CCNA Official Exam Certification Library, Third Edition, Cisco Press, USA
- [8]. CCNA Security Study Guide : Exam 640-553 , Boyles, Tim, Sybex