

Faculty of Engineering and Technology

Electrical and Computer Engineering Department

ENCS 413 Report

Ameer Alqam 1120217

Sondos Samara 1121775

Omar Muhtaseb 1122010

Dr.Iyad Tumar

TA. Odai Salman

*Created by Omar Muhtaseb*

**Abstract**

This report will present the main concepts about creating and configuration the Access-List and virtual LANs, it will introduce the way to control transferring information between networks (Permitting and denying), and this will show how to save the privacy of the networks using the access-lists. Both types of the access lists (Extended and standard) will be explained. Beside the Access list, the virtual LANs will be also introduced. The creation, configuration and controlling will be explained with the both sides router and the switch when creating and dealing with the VLANs?

Table of Contents

[1. Theory 1](#_Toc449570557)

[1.1 VLAN 1](#_Toc449570558)

[1.1.1 VLAN Introduction 1](#_Toc449570559)

[1.1.1 Trucks 1](#_Toc449570560)

[1.1.2 RoS 2](#_Toc449570561)

[1.1.3 VLAN Configuration 2](#_Toc449570562)

[1.2 Switch Virtual Interface (SVI) 2](#_Toc449570563)

[1.3 Access Control List 3](#_Toc449570564)

[1.3.1 Access Control List Introduction 3](#_Toc449570565)

[1.3.2 Standard and Extended ACL 3](#_Toc449570566)

[1.3.3 ACL Configuration 3](#_Toc449570567)

[2. Procedure and Discussion 4](#_Toc449570568)

[2.1 VLAN 4](#_Toc449570569)

[2.2 SVI 6](#_Toc449570570)

[2.3 Access Control List 7](#_Toc449570571)

[3. Conclusion 9](#_Toc449570572)

[4. References 10](#_Toc449570573)

# Theory

## VLAN

**VLAN** is an acronym for **V**irtual **L**ocal **A**rea **N**etwork. V in VLANs refers to the logical separation among LANs, despite the verity that they might be in the same physical network. .A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire. It was explicitly evolved to establish a fictional isolation amongst users. So as to afford more control, security and privacy among distinct VLANs.[1]

### VLAN Introduction

In a veritable network, multiple VLANs are created to distinguish users. Each VLAN is assigned to a unique id. While each end-user device has to be designated to a sole VLAN, the default VLAN for non-appointed devices has an id of 1. With no further configurations, the users in the same VLAN can communicate with each other. On the other hand, diverse VLANs’ users have no ability to establish connections between each other. In other sense, packets cannot cross the illusional boundaries of VLANs. One proposed solution in a physical manner is to attach a link from each VLAN to a router that handle routing details. However, this seems to be infeasible solution with larger networks. A more sophisticated solution is to use **trunks** or **router-on-a-stick**. [2] [3]

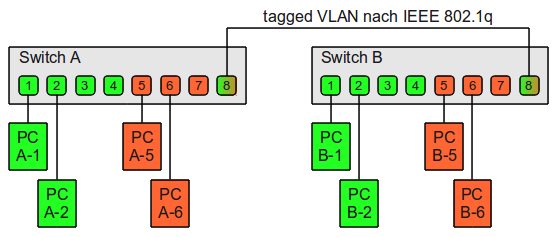


Figure 1 Virtual LAN

### Trucks

**Trunks** are special kind of cables that permit the management of the VLANs traffic. They are used for the allowance of packets’ exchange between two uneven VLANs. Tagging mechanism is applied in trunks in order to mark the packets with the destination VLAN id. Trunks and mainly used to link two switches. Only it can connect a switch and a router in case of router-on-a-stick.

### RoS

**R**outer **o**n a **S**tick, or **RoS** as it is called, is a router with single connection to the network. It is used to forward packets between two or more distinguishable VLANs. RoS has considered to be an admirable solution to the VLANs issue. However, with such considerable number of VLANs, the bandwidth cannot be utterly utilized by sole VLAN. RoS’s connected interface is subdivided into sub partitions in order to accommodate all VLANs in the network. Each VLAN has its own sub interface that will pass through in the communication process. [6]

Figure 2 Router on a Stick

### VLAN Configuration

To create a VLAN, the following command used:

#Switch(config)#vlan [Number]

To assign this VLAN to an interface the following command used:

#Switch(config-if)#switchport access vlan 10

To configure one of the interfaces as a trunk the following command used:

#Switch(config-if)#switchport mode trunk

## Switch Virtual Interface (SVI)

SVIs are interfaces that are normally used for switching. However they can be used as virtual layer 3 switches to route traffic between layer 3 interfaces. Thus, there is no need for a physical router. These interfaces are used in special switches called layer 3 switches. Layer 3 switch is a device that operates in layer 2 and provides functionality in layer 3. The major difference with the ordinary router is that it uses application-specific integrated circuit (ASIC) hardware to accomplish the routing. While the router uses software runs on a microprocessor. [8][9]

## Access Control List

### Access Control List Introduction

Access Control List, or **ACL**, is a management criterion that is used to dominate the packets transmission that passes through a specific router. The control can be imposed on the packets by denying some of being forwarded to a nominated destination. The blocking mechanism is managed at the router’s interfaces. Each packet has to be inspected to determine whether to be dropped or forwarded. Access list can be obliged on source address or destination address. ACL has some peculiar network identifying technique as it uses the wildcard masks to define the network. Wildcard masks which are basically the first complement of the normal subnet mask in binary, making them seem confusing at first. [1]

### Standard and Extended ACL

Mainly, there are two basic types of the Access Lists, a **Standard** and **Extended** ACL. In the Standard ACL, packets filtration is achieved by monitoring the source IP address of the packets and drop the ones with no permission to be sent. This type of filtration is given numbers 1 – 99. On the other hand, The Extended ACL extends to include the source and the destination IP addresses. It controls the traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL. This criterion has a range of 100-199 of numbers.

### ACL Configuration

In order to create ACL, use the following command:

#access-list access-list-number {permit|deny} {host|source source-wildcardmask|any}

In order to assign the access list to an interface,use the following command:

#interface <interface>

#ip access-group [number] {in|out}

# Procedure and Discussion

## VLAN

In the first experiment we have created our own topology to minimize the number of possible routers that can be used to accomplish the communication between all the provided VLANS. To do so, we used a lone router only to do all the routing operations. To make up this network, it was adequate to connect the router to only one switch. Then we had to define all the connections between switches and the single switch-to-router connection as trunks. In order to enable the communication amongst various VLANs.

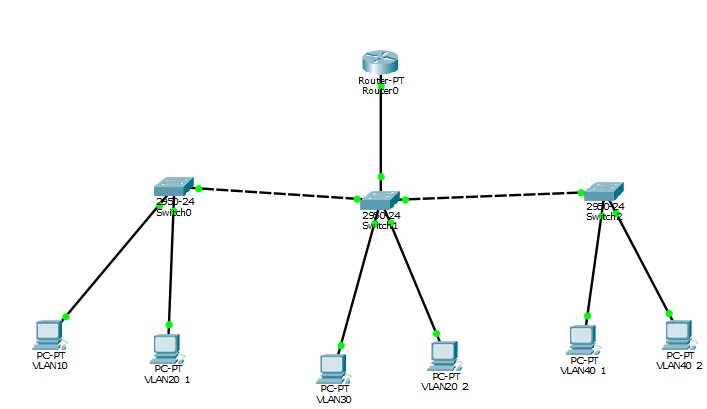


Figure 3 VLAN Topology

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **IP Address** | **Gateway** | **VLAN** |
| **PC0** | 193.168.1.2/24 | 192.168.1.1 | VLAN 10 |
| **PC1** | 193.168.2.2/24 | 192.168.2.1 | VLAN 12 |
| **PC2** | 193.168.3.2/24 | 192.168.3.1 | VLAN 30 |
| **PC3** | 193.168.2.3/24 | 192.168.2.1 | VLAN 20 |
| **PC4** | 193.168.4.2/24 | 192.168.4.1 | VLAN 40 |
| **PC5** | 193.168.4.3/24 | 192.168.4.1 | VLAN 40 |

Table 1 VLAN Topology Configuration

As for the router, the configuration was as follows:

|  |  |
| --- | --- |
| **Interface** | **IP** |
| FastEthernet0/0.10 | 193.168.1.1/24 |
| FastEthernet0/0.20 | 193.168.2.1/24 |
| FastEthernet0/0.30 | 193.168.3.1/24 |
| FastEthernet0/0.40 | 192.168.40.1/24 |

Table 2 VLAN Router Configuration

In order to assign VLANs

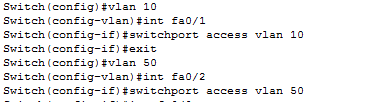


Figure 4 VLAN Command

Each “switch to router” cabling or “switch to switch” cabling should be configured as TRUNK. For example for switch0 the following commands used:

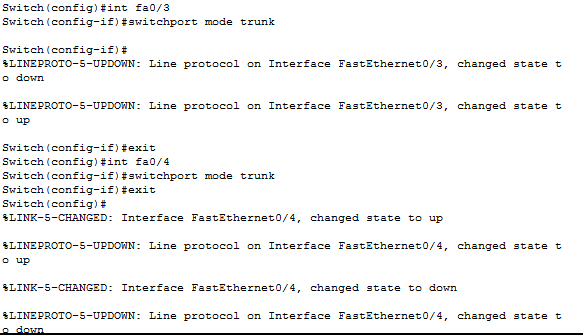


Figure 5 Trunk Enabling

Because of router on stick concept, in router interface we have to do sub interface for each VLAN configured on the switch. For example for router0 that connected to switch 0, where the last have vlan10 and vlan20, the following commands used:

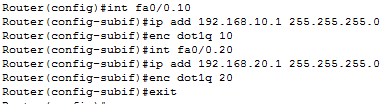


Figure 6 Router Sub-Interfaces

After finishing with network configuration, the network became ready to be tested.

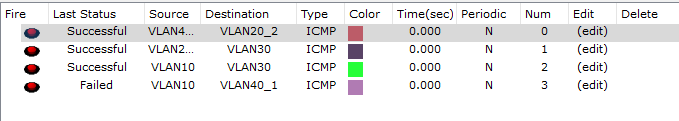


Figure 7 VLAN Testing

A crucial note had to be induced in this experiment that we have to define all the VLANs that are connected to the router in order to enable proper routing. In the lab, we were not able to establish the connection between any two different VLANs except for VLAN 20 and 30. We tried many and many times with the TA. Oday and Dr. Iyad with no luck. Thus, we finished the lab with no working network. However, thanks to TA. Oday that he was able to figure it out and solve the dilemma.

## SVI

In the second experiment we used the modified the topology we had created in the previous experiment. With the same end-users devices, and with the same given IPs, we connected the RoS to the network. By replacing the original and normal router by multilevel switch.

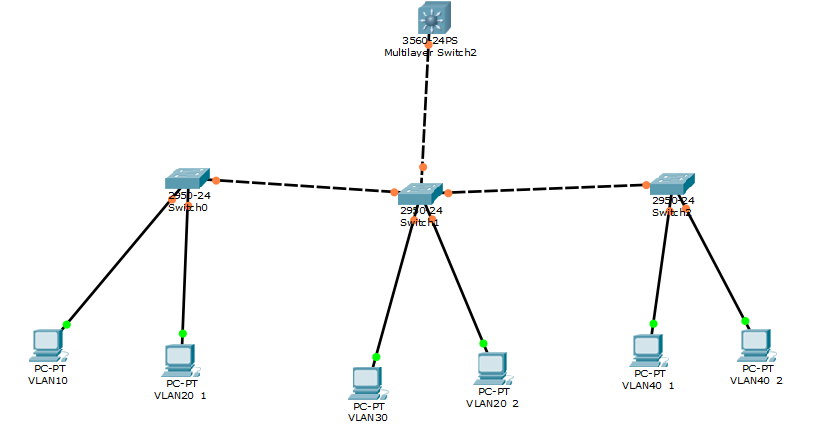


Figure 8 VLAN Topology

All we have to do is to configure the multilevel switch with the given VLANs. And to enable routing on the multilevel switch.

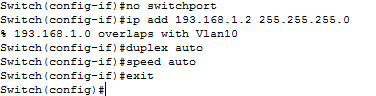


Figure 9 RoS Configuration

We used the rip routing protocol as the routing protocol on the multilevel switch.

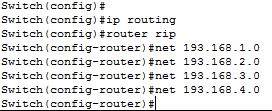


Figure 10 RoS Configuration

The network had to be tested at last.

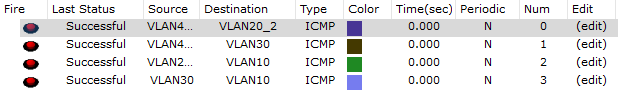


Figure 11 SVI Testing

## Access Control List

In this experiment, we created a topology with three networks to implement the ACL. First of all, we define IPs to the end-user devices. Then we configure the routers with routing algorithm. Finally, we add some IPs to the access control list on different routers to implement ACL.

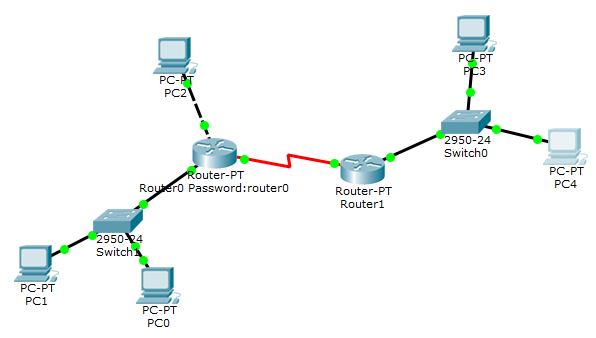


Figure 12 ACL Topology

End-user devices were given the following IPs.

|  |  |  |
| --- | --- | --- |
| **Device** | **IP Address** | **Gateway** |
| **PC0** | 193.168.1.3/24 | 193.168.1.1 |
| **PC1** | 193.168.1.2/24 | 193.168.1.1 |
| **PC2** | 193.168.0.2/24 | 193.168.0.1 |
| **PC3** | 193.168.2.2/24 | 193.168.2.1 |
| **PC4** | 193.168.2.3/24 | 193.168.2.1 |

Table 3 ACL IPs

Then we configured the router with these settings.

|  |  |  |
| --- | --- | --- |
| **Router** | **Interface** | **IP** |
| **Router** | FastEthernet0/0 | 193.168.1.0/24 |
| **Router0** | FastEthernet1/0 | 193.168.0.1/24 |
| **Router0** | Serial2/0 | 10.0.0.1/24 |
| **Router2** | FastEthernet0/0 | 193.168.2.1/24 |
| **Router2** | Serial2/0 | 10.0.0.2/24 |

Table 4 Routers' Interfaces Configurations

Then we enabled rip routing algorithm on the routers. After that, we started to implement the ACL. The first to do was to use a standard ACL to deny PC2 from accessing the 193.168.2.0/24 network.



Figure 13 Task 1

After creating the access list, we had to apply to the interface.



Table 5 Apply Access List

The result of applying the access list was:

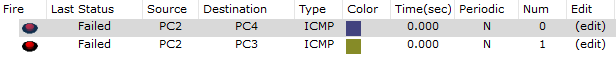


Table 6 Task 1 Result

As for task 2, we had the following. The user on PC1 should be denied access to the serial link between R1 and R2; all other traffic should be allowed. Create and apply an access-list with no more than TWO statements to achieve this objective.

# Conclusion

To conclude what was done and learned from this experiment it will be summarized that two main concepts in computer networks were discussed and tried to be implemented, the two concepts are VLANs and ACLs.

Access Lists allow the networks to have an ability for creating a specific access-list to permit or deny a source (host or other network) from accessing the network. This experiment helped by trying to implement both. The second part of the experiment was to create a physical attach between hosts by creation the VLAN. In another words, it’s a creation for a logically separated networks. We had some hardships at this part of the experience but it was done successfully at last.

Other important thing that the experiment shows and explains is the multiple switch, in which it could be used both ways as a router or as a switch depending on the configuration for it. The basic thing to be learned from this experiment that admin have an ability to control and manage the network and to deal with the security and privacy stuff using some commands.

# References

* <http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html#wp1000893>

Access date 27/4/2016 7:53 PM

* http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#extacls Accessed date 13/4/2016 1:34 am
* <http://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual_lans/>

Accessed date 27/4/2016 8:19 PM

* <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/122SX/configuration/guide/book/vlans.html>

Accessed date 27/4/2016 8:27 PM

* <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/122SX/configuration/guide/book/vlans.html>

Accessed date 27/4/2016 9:14 PM

* <http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/14976-50.html>

Accessed date 27/4/2016 9:33:59 PM