**COMPUTER COMMUNICATION AND NETWORKING**

**( CCN )**

**PROJECT**

**TOPIC: GNS3 BASED VLAN ACL**

**Instructor: Sir Dileep Kumar**

Pre-requisites of this project:

1. Installation of GNS3
2. VMware workstation
3. C7200 router IOS Image
4. Number of switches including c3640, c3725, layer2 switch.

At the start of this project, we downloaded the gns3 from [www.gns3.com](http://www.gns3.com) .

It is downloaded on a low spec laptop due to which I faced the overheating issues number of times.

The VMware workstation was also download from the above website.

Understanding that which switch would be the best to use in this project was too confusing as many switches are available on google.

We were sitting idle for almost 15 to 20 days as we were trying to understand the basic concept of VLAN and ACL and how they both combine to form a network. We watched many tutorial videos in which they were creating a VLAN but almost every video had a different approach so we picked the approach that was easy to understand.

**Understanding VLAN:**  
Virtual Local Area Networks is a custom network which is created from one or more than one LAN. It enables a group of devices available in multiple networks to be combined into one logical network. Without VLANs, a broadcast sent from a host can easily reach all network devices. But by using VLANS, a broadcast can only reach the devices that are available in the same VLAN.

**Understanding ACL:**ACL also known as Access Control List is basically a set of rules that determines that which packet should be accepted or rejected by which network. It performs packet filtering to control the movement of packets through a network. It provides security by limiting the access of traffic into a network.

**HOW TO DOWNLOAD A ROUTER/SWITCH**

1. First, we have to download an IOS image of the router from any website.

I used <https://protechgurus.com/download-gns3-ios-images/> this website for downloading Purpose.

![Graphical user interface, text, application, email

Description automatically generated]()

1. Then we will go to the Edit option from the top bar and click on ‘preference’. The above window will appear after clicking on it. Next click on the IOS routers option

![Graphical user interface, application

Description automatically generated]()

1. Now, select the New option and select the directory where IOS Image of the router is placed.
2. After selecting the image, just follow the simple instructions that will download the router for you.

**TOPOLOGY**

Now, coming on to the main topic, there were number of ways that the topology of this project could be created. I tried many different topologies but due to lack of skills in networking area, I was facing problems in almost every topology. And in the last few days, this topology was decided by us:

![Diagram

Description automatically generated]()

I had the option to connect router with both the switches and to remove the direct link between them but that would be an ordinary approach. Therefore, I decided to implement the VLAN by connecting the two switches. I used the **TRUNK** link to connect the two switches. Trunk links are used to pass the VLAN information in between the switches. Moreover, I created two VLANs here VLAN 10 and VLAN 20, both have two Virtual PCs connected to them on different switches.

**CONFIGURATION**

I will try to cover the main parts of configuration of this project here and the screenshots of the configuration part for verification purpose are attached in the next section:

1. At the start of this project, I started all nodes and changed the hostnames of switches by going in config mode

*Switch1 > en*

*Switch1 # config*

*Switch1 (config) # hostname SW1*

1. After this, I created the switch 2 as VTP server and switch 1 as VTP client by using the command:

*SW2 (config)# vtp mode server*

*SW1 (Config) # vtp mode client*

1. After this, Vlans were created by using the following commands

*SW2 (Config)# Vlan 10*

*SW2(config-vlan)#vlan 20*

1. After this, trunk links have to be enabled and for this purpose, I used this command on both the ethernets connecting the two switches together:

*SW2/SW1 (config-if)# switchport trunk encapsulation dotiq*

*SW2/SW1 (config-if)# Switchport mode trunk*

1. We check the Vlans and their names by using the command

*SW2(Config)# do show vlan*

1. Next step is to assign IP addresses to the VLAN Interface

*SW2 (config-if)# interface vlan 10*

*SW2 (config-if)# ip add 192.168.10.254 255.255.255.0*

*SW2 (config-if)# no shutdown*

*SW2 (config-if)#interface vlan 20*

*SW2 (config-if)#ip add 192.168.20.254 255.255.255.0*

*SW2 (config-if)#no shutdown*

We can check the interface and ip assigned to them by using the command

*SW2 (config-if)#do show ip interface brief*

1. Now, we have to assign the Vlans to the ethernet connection that connects it to the Virtual PC.

*SW1 (config-if)# interface gig 0/1*

*SW1 (config-if)#switchport mode access*

*SW1 (config-if)#switchport access vlan 20*

*SW1 (config-if)#no shutdown*

*SW1 (config-if)# interface gig 0/2*

*SW1 (config-if)#switchport mode access*

*SW1 (config-if)#switchport access vlan 10*

*SW1 (config-if)#no shutdown*

*SW2 (config-if)# interface gig 0/1*

*SW2 (config-if)#switchport mode access*

*SW2 (config-if)#switchport access vlan 20*

*SW2 (config-if)#no shutdown*

*SW2 (config-if)# interface gig 0/2*

*SW2 (config-if)#switchport mode access*

*SW2 (config-if)#switchport access vlan 10*

*SW2 (config-if)#no shutdown*

1. After this, we will assign IP address to the Virtual PC.

*PC1> ip 192.168.20.5 255.255.255.0 gateway 192.168.20.254*

*PC2> ip 192.168.10.5 255.255.255.0 gateway 192.168.10.254*

*PC3> ip 192.168.20.7 255.255.255.0 gateway 192.168.20.254*

*PC4> ip 192.168.10.7 255.255.255.0 gateway 192.168.10.254*

1. After assigning the Ips to the Virtual PC, now we have to create ACL.

I used the extended access control list here and the configuration is:

*SW2 (config)# IP access-list extended CCN*

*SW2 (Config-ext-nacl)# deny imcp 192.168.20.0 0.0.0.255 host 192.168.10.5*

*SW2 (Config-ext-nacl)# permit ip any any*

*SW2 (Config-ext-nacl)#interface vlan 20*

*SW2 (Config-if)# ip access-group CCN in*

Some other ACLs were also created to solve some problems but the pattern to create the ACL is the same as in the above example I took the whole network and used the deny command over it. Screenshots of ACLS working are given below in the verification section.

**SOME SCREENSHOTS OF SOLAR PUTTY FOR VERIFICATION PURPOSE:**

1. I have attached two pics below that shows that switch 1 was used as a client in VTP mode and switch 2 was used as a server.

![Text

Description automatically generated]()

![Text

Description automatically generated]()

1. **I used the command “do sh vlan” in the config mode to get this image:**

![Text

Description automatically generated]()

In the above pic, you can see that I have created VLAN 10 and 20 with the name of DEV AND PRO.

1. I used the command “do sh ip interface brie” here to get this image:

![Text

Description automatically generated]()

Here in the above pic, it is clearly shown that I have created VLAN interface and assigned IP to them which acts as a gateway for the devices.

1. **I took the screenshots before applying ACL to the project to check whether they can access each other or not. Both the Vlans were able to ping each other and all the 4 devices were able to communicate with each other**

**PC1**

![Graphical user interface, text

Description automatically generated]()

**PC2**

![Text

Description automatically generated]()

**PC3**

![Text

Description automatically generated]()

**PC4**

![A computer screen capture

Description automatically generated with low confidence]()

1. **AFTER APPLYING ACL TO THE PROJECT,**

**PC1**

**![Text

Description automatically generated]()**

**PC2**

**![Graphical user interface, text

Description automatically generated]()**

**PC3**

**![Text

Description automatically generated]()**

**PC4**

**![Text

Description automatically generated]()**

In the above pics, it is clearly shown that the VLANs were not able to communicate with each other because of the ACL. As we ping the PC of the other VLAN, the output is **“communication administratively prohibited”**

Below is the screenshot that shows the overall ACLs that were created. Some of them worked and some of them didn’t due to some error. However, overall it worked as you can see the screenshots above that shows the changes after applying the ACL  
![Text

Description automatically generated]()

RESOURCES:

1. <https://gns3.com/community/featured/how-to-configure-acls-for-3-vlan>
2. <https://learningnetwork.cisco.com/s/question/0D53i00000Kt6za/vlan-access>
3. <https://www.computernetworkingnotes.com/ccna-study-guide/configure-extended-access-control-list-step-by-step-guide.html>
4. <https://www.youtube.com/watch?v=A4Mt1Vgx-fw>
5. <https://www.youtube.com/watch?v=BwEcN_bXLkw&t=174s>
6. <https://www.youtube.com/watch?v=IoM4GeLnm5w>
7. <https://www.youtube.com/watch?v=xmCsnoxaWi4&t=304s>
8. <https://www.youtube.com/watch?v=iY1mtCZN11Q&t=2595s>
9. <https://www.youtube.com/watch?v=ittKxuI4FwY&t=236s>
10. <https://networklessons.com/cisco/ccie-routing-switching/vlan-access-list-vacl>