# Overview

The purpose of the VLAN lab is to set up a LAN environment with 2 Virtual LANs on a managed switch. The lab uses a Dell PowerConnect 2716. This switch is configured through an Ethernet port using a Web GUI interface

The basis of the lab is to set up 3 PCs with connections to a managed switch. The PCs (VMs) will be set to ping each other. Then, one at a time, two of the PCs ports on the switch will be “moved” to a VLAN. The effect of the reconfiguration will be noted through monitoring the pings of the PCs. The lab is may be done by 1 to 3 students per lab station (switch). Each student will submit their own lab report.

The lab’s network is 172.16.0.0/16. De facto Class C private networks are 192.168.1.0/24. The default access port for the Dell switch (192.168.2.1) is on a different network than the de facto Class C network. During this lab you will not be able to access your home directories when you disconnect the workstation from the lab network.

## Concepts

* Major
	+ Managed switch maintenance
	+ Creation and impact of a Virtual LAN
* Minor
	+ Subnets
	+ NIC configuration
	+ VM “convenience”
	+ *root* authority is required for certain operations

# Part1

## New Linux tricks

The first part is to familiarize you with a new aspect of Linux. This segment will be creating new users for your Debian VM.

Directories/Files of interest:

* /home
	+ default directory for users (optional) home directory
* /etc/passwd
	+ file with user ids and attributes definitions
* /etc/shadow
	+ file with “secure” password and attributes definitions

Before creating the new user ids check the contents of the above directory and files. Find your ID and the root ID in each of them. Get a copy of the above files and directory contents to include in your report. *(****Hint:*** *for getting a listing of the contents of the /home directory try:* ls /home > home1.txt *).* Include that listing of the file contents and directory contents in your report. \*\* You may strip out many of the “weird” userids in the passwd and shadow file to shorten the lists for your report, but be sure to leave root and the userids you created.

### Create a new user using the GUI:

There is a new Gnome GUI. You can create a user by either Gnome 3 or Gnome Classic

#### Gnome 3

1. Click on your userid in the top right corner
2. Select system settings
3. Under system select user accounts
4. Unlock the screen. Your root pw is required
5. Click on the +
6. Enter the data for the new user
7. Highlight the new userid and click on the password box to enter a new password, then click *Change*
8. Relock the *User Accounts* screen

#### Gnome Classic

1. Install Users and Group from a terminal
	1. apt-get install gnome-system-tools
2. Under *System* 🡪 *Administration* select *Users and Groups*
3. Enter the root password when prompted
4. Click on *Add User*
5. Enter a username (your choice for the username, but remember it!!!)
6. Ensure *Set password by hand* is set and enter
	1. User password
	2. Confirmation
7. The other fields are optional
8. Click *OK*

#### Both

1. Get a copy of the files and directory contents again. Include these in your report. \*\*
2. Test the new ID by logging in from tty2

***Important Note:*** When in the virtual machine, hitting <ctrl>+<alt> will revert control back to the base workstation. In your virtual machine (and the base machine) <ctrl>+<alt>+<Fn> is used for switching to a terminal. There is a special sequence, <ctrl>+<alt>+<space> that flags the VM controller the next <ctrl>+<alt>+ whatever is meant for the VM itself. To switch to tty2 in the VM one would then do a <ctrl>+<alt>+<space> followed by <ctrl>+<alt>+<F2>. This <ctrl>+<alt>+<space> sequence can be used wherever a <ctrl>+<alt>+ something is needed for the VM.

### Create a new user using the CLI:

1. Start a terminal
2. Switch to root access
3. Create a new user (Again your choice for the ID, but remember it!!!)
	1. useradd *newID*
4. Set a password for the new user
	1. passwd *newID*
5. Create a home directory for the new user
	1. mkdir /home/*newID*
	2. chown *newID*:users /home/*newID*
		1. the :users above sets the group to *users*
6. Get a copy of the files and directory contents again. Include these in your report. \*\*
7. Test the new ID by logging in
	1. Open a GUI terminal and use *su* this time to log on as the new ID

Note: *adduser* is an improved version of *useradd* that makes some of the tasks of creating a user id easier.

**Q1:** When is it best to use the GUI?

**Q2:** When is it best to use the CLI?

**Q3:** Discuss what files and directories were changed as the new users were added in the above steps. Note the size of the encrypted password in the */etc/shadow* file for all “normal” ids. This is where you discuss the file and directory contents gathered above.

# Part 2:

## Dell PowerConnect 2716

The lab setup will consist of 3 PCs, 3 CentOS VMs, one 2716 switch and Ethernet cables. You will need to use 3 PCs that are within reasonable reach of each other (cable length). This part of the lab will be done by groups of 3 students at 3 workstations.

### Lab Overview – read and understand this section before doing the Lab Procedures

* Start a CentOS Linux VM on all your workstations:
	+ Configure the VMs to communicate to the switch’s default network (192.168.2.0)
* Connect all devices (workstations) to the switch (in unmanaged mode)
* Set all VMs to ping each other via the 192.168.2.0 network
	+ The lab write-up documents using IP addresses 192.168.2.21, 192.168.2.22, and 192.168.2.23. You may use any address 192.168.2.n with the exception of n being 0, 1 or 255. Think about why those addresses can’t be used.
		- This assumes all the groups are working on separate physical networks.
	+ Two approaches can be used ensure unique host ids if all workstations in the lab are on a single merged network:
		- All machines use the PC id as the host id (except for PC01 uses 29)
		- All groups use a different network: eg. 192.168.n.0. By using one of the group’s PC number as the subnet unique host names are guaranteed. Eg. PC03, PC04, and PC05 are working together: use subnet 192.168.3.x as the subnet.
* Enable management mode on the switch
* Connect to the management port on the switch from one of the VMs and set up a VLAN
	+ Move one of the ports to the new VLAN and note the impact on pings
	+ Move another port to the new VLAN and note the impact on pings

###

Figure 1 – Dell PowerConnect 2716. Note that the System LED and the Default switch may be labeled Managed Mode depending on vintage of the switch.

### Lab Procedure

#### Part 1- Prep VMs

##### Start VMs, Reconfigure Ethernet/IP

The VMs’ Ethernet NICs needs to be reconfigured for each of the VMs to access the 192.168.2.0 subnet. This will allow the VMs to communicate with the default configuration port on the Dell switch.

**Note:** the instructions for the VMs for this lab are for the CentOS operating system. The lab may be done with either the CentOS or Debian VMs. The location and content of the network configuration files is different for the two Linux distros. The appendix at the end of the Lab notes the Debian differences.

1. Ensure the switch in unmanaged mode
	1. If the System (Managed Mode) LED is on, use a thin rod to push the Default (Managed Mode) switch (See )
	2. If it is necessary to change modes, it will take up to two minutes ***or longer*** for the switch to change states
2. Download a copy the CentOS VM (made in the previous lab) to the /scratch directory on each physical machine (do not alter the original copy, you will need it for later labs.)
3. Start each VM on all 3 workstations with VMware player.
	1. If asked, say you **moved** the VMs.
4. Login to each VM, then open a root terminal in each one (from *applications > accessories*). Edit the config file for the VM’s IP Ethernet address using vi (or the variant of your choice). (Reference the PowerPoint presentations or the cheat sheet if you forgot the vi commands. The TA will not help you until you have reviewed the instructions).
	1. Use *ifconfig* to check which Ethernet interface is defined (Hint: for VMs it is usually not eth0)
		1. Note: *ifconfig* can temporarily change the ip address, for this lab we want a permanent change so we need to edit the NIC’s config file.
	2. The editing must be done with an id with root authority.
	3. Edit */etc/sysconfig/network-scripts/ifcfg-eth0:* where eth0 is what ifconfig reported
	Notes:
		1. eth0 may be eth1 or eth8 (or another name/number)
		2. Do not change the MAC address (aka HWADDR in CentOS)
		3. Always make a backup before changing a critical system file
		4. Change BOOTPROTO value from *dhcp* to *none*
			1. Note: commenting out a line is usually desired in case the file will need to be reverted to its original state. You can duplicate the BOOTPROTO line and change the value to *none* on one of them. Then you can comment out the one you don't want for that lab session.
		5. Add the two lines as seen above if needed, if not, change the IPADDR to your address e.g. 192.168.2.xx with xx the number you want on your machine.
			1. The example shows PC21 as (192.168.2.21) for the machine address, make sure all your VMs have a unique number
		6. NOTE: on your machine the HWADDR (i.e. MAC address) will vary from workstation to workstation.  ***Do not change this address!***
	4. Save the file

***EXAMPLES:***

BEFORE:

AFTER:



1. Restart the VM so the new IP addresses are implemented
	1. An alternate to restarting the VM is to stop and start the NIC (CentOS):
		1. ifdown eth0
		2. ifup eth0

**Hint:** you may get an error stating the command you entered is not found. If so, you are not doing the step correctly. Review old labs before asking the TA what the problem is.

1. Verify configuration
	1. Use *ifconfig* to verify the changes worked
2. Repeat the above steps 3-5 for the other 2 physical machines.
	1. This exercise example uses addresses 192.168.2.22 and 192.168.2.23 for the other two VMs
	2. You may use these addresses or any other you wish (within reason)
	3. Make sure you use addresses appropriate for your machines (that match your physical machines number).

#### Part 2 - Set up Hardware

Make sure the switch is still in unmanaged mode (as done in step 1 in the preceding section).

Reconnect the hardware through the switch. Connect the 3 PCs to the switch. You may use any port, but for this lab we will have the PC’s connected to ports 1, 2 and 3 on the PowerConnect 2716. If you use a different port configuration carefully note which switch ports are used for each connection.

***Warning:***

* Disconnecting the base machines from the lab network will “break” the NFS file connection for the physical machines, you will not be able to access network files on the physical host computer (i.e. network\_storage). The VMs should not be affected.

#### Part 3 - Start Pings

On each VM, set up pings to each of the other VMs you have connected on the switch. Use a separate terminal for each of the pings. All pings should be working. So VM 1 (e.g. 192.168.2.21) will have two command terminals open, one pinging 192.168.2.22 and one pinging 192.168.2.23. The other two VMs will also be pinging the other VMs.

**Optional:** switch to the base workstations, discover their IP addresses and get them to ping each other also. (This will only work if the base machine is not frozen.) Since the students are not allowed root access the explicit path to *ifconfig* will need to be in the command: /sbin/ifconfig

Do a data capture to show the pinging on all VMs for your report. A screenshot is not allowed. You may share the data captures with your workmates.

#### Part 4 - Create and Change VLAN Ports

Change the switch to managed mode. Use a thin rod to push the System switch.

**Important:**  it is very important to be patient. You may need to wait as long as 5 minutes for the switch to completely switch modes*. Bad things will happen if you don’t.*

1. Open a browser from inside one of the VMs (e.g. the one using IP address 192.168.2.21)
	1. Enter the IP address for the switch (<http://192.168.2.1>)
	2. The default userid for the switch is *admin* and there is no password.
	3. Familiarize yourself with the interface.
2. Open VLAN Membership
	1. Note the setting in the report area
	2. Create VLAN
		1. Click on the radio button and enter an ID (use 100 as for the PVID above)
	3. Apply changes
	4. Ensure the VLAN ID 100 is selected
	5. on the graphic below set Ports 2 and 3 to U and apply changes
	6. Click on VLAN Port Settings
	7. Change ports 2 and 3 to use PVID 100, and apply changes
		1. Screen-captures of the pings after each move for each port
		2. Screen-capture of the switch management web interface after all changes done
	8. Notice now the VMs on ports 2 and 3 are now pinging, the VM on port 1 now cannot reach the VMS on ports 2 and 3 and vice versa
	9. **Q4:** What will happen if port 1 is shifted to VLAN 100?
	10. (Optional) move port 1 to VLAN 100 and note what happens
3. Reset the switch to unmanaged (hold the managed mode button for a full second before letting go, takes about 2 minutes to come back)
	1. **Q5:** What happens to the pings?
	2. Try refreshing the managed switch’s configuration page and note what happens.
4. Reset the switch to managed (again, takes about 2-5 minutes)
	1. Open the managed port interface from a different VM
	2. **Q6:** What has happened to the status of the VLAN Settings you had changed before?
	3. Note the affected ports should be pinging

### Closing comments

Take appropriate screen shots and text captures (as appropriate), close your VMs, make copies of the VMs (only if you want to save them for a while), and delete the copies you made on the physical machine scratch directories (do NOT delete the original in your network\_storage directory or USB drive unless you want the headache of recreating it later).

**Q7:** Discuss (and support with file or screen-captures) the pings in the un-managed switch, and then with the managed switch as each of the ports is moved to the VLAN. Include a diagram of the lab setup

Note that screen shots taken while the PCs and VMs are disconnected from the network cannot be saved to ***network\_storage***. Plan accordingly.

Items noted with a \*\* are the key concepts for this lab. Pay special attention to what is done at these steps and why.

# Addenda

## Debian changes

The network configuration files for Debian are in the */etc/network* directory. The file is *interfaces*. Following is an example of how the file should be changed. Note that the # are comment lines and it is very important to comment out those lines! Do not delete them, they may needed in a future lab.

# This file describes…

# The loopback network interface

auto lo

iface lo inet loopback

# The primary network interface

allow-hotplug eth0

# iface eth0 inet dhcp

#

auto eth0

iface eth0 inet static

address 192.168.2.21

netmask 255.255.255.0

**Hint:** For Debian the commands to start and stop the NIC are:

* + 1. ifconfig eth0 down
		2. ifconfig eth0 up