# VLANs and Simple Multi-layer Switching

If you have several computers in the same area that need to be on different networks, you could install a switch for each network. The switches would have their own connections back to a router that places the switches on separate networks. Purchasing separate switches for each network would be needlessly expensive. The concept of Virtual Local Area Networks, or VLANs was invented for this purpose. It allows you to break a switch into pieces that are on different networks.

Diagram

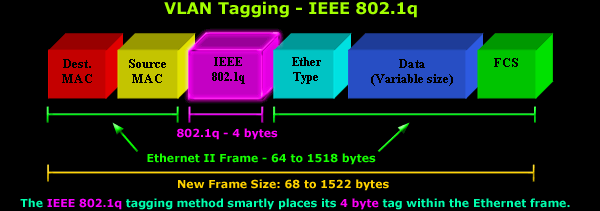
Description automatically generated

The switch keeps traffic for the VLANs separate and requires the traffic to go through a router if it needs to go from one VLAN to another. The diagram below shows a switch where 1/3 of its ports are on VLAN 10, 1/3 on VLAN 20, and 1/3 on VLAN 30. The switch uses a VLAN trunk port, that carries traffic for all three VLANs, to connect to the router or the rest of the network.

A picture containing shape

Description automatically generated

You may ask, “If traffic from all three VLANs is on the same trunk port, how does the network keep them separate? How does it know which traffic is from which VLAN?” The answer is that the switch adds a VLAN tag, four bytes long, in the Ethernet (data link layer) portion of the packet. It only does this on trunk ports, access ports do not add VLAN tags (except when Voice over IP (VoIP) phones are involved, but we will ignore that.) The drawing below shows the added VLAN tag, which is specified in the IEEE standard 802.1q.



# Simulation – Part 1

First, we will mockup the lab in the Packet Tracer simulator. Be sure to use a 3560-24PS switch for the center switch and 2960 switches for the outer switches. Note: if your center switch is powered off, you probably have a 3**65**0 switch instead of a 3**56**0. You can change the switch to a 3560 or add a power supply as shown at the end of this document.

Diagram

Description automatically generated

We will have two VLANs with two different IP networks.

It will be easier to keep things straight if we use VLAN 10 with the 19.168.10.0 network and VLAN 20 with the 192.168.20.0 network. (There is no requirement that the network addresses include the VLAN numbers—it is just easier to remember.)

Note that the switch ports that connect to computers are **access ports**. The switch ports that connect to other switches are **trunk ports**.

## Step 1 – add VLANs

Each switch needs to know what VLANs exist. There are protocols that will allow you to configure the VLANs on one switch and have them automatically distributed to the other switches, but for this lab it is easier to configure them manually. On each switch, use the VLAN Database selection in the Config tab to add VLANs 10 and 20. You can name them whatever you like.

Graphical user interface, text, application

Description automatically generated

## Step 2 – configure the access ports

Once the VLANs are configured, you can configure the ports that connect to your computers as access ports. Make sure that the VLAN number and the network address you have chosen match what you will put on the PC. Pay attention to the drawing where we selected the networks and numbers for the VLANs. For each switch configure the correct VLAN as shown below. You only need to do this for ports that have computers connected to them. (Ports where you do not configure a VLAN are set to VLAN 1 by default.)

Graphical user interface, application

Description automatically generated

## Step 3 – configure the trunk ports

The ports that connect to other switches need to be configured as trunk ports. The switches on the outside have one trunk port that connects to the center switch. The center switch has two trunk ports. Select Trunk for the proper port. Note that the dropdown with the individual VLANs has all VLANs checked. This means all VLANs can transit the trunk link. (In more advanced configurations you can exclude some VLANs from some links, but we will not do that.)

Graphical user interface, text

Description automatically generated

## Step 4 – configure the computers

Configure the PC with an address that matches the network that will be assigned to the VLAN the PC is connected to. Do not worry about the default gateway, we will come back to that later.

Graphical user interface, text, application, email

Description automatically generated

## Step 5 – Test

If everything is properly configured, PCs that are on the same VLAN should be able to ping each other. PCs that are on different VLANs should not be able to ping each other. Make sure that is working before proceeding to the next step.

## Step 6 – Configure routing on the multilayer switch

This step will need to be done from the Command Line Interface (CLI) of the center switch. It is important that you chose a 3560 switch for the center and that it appears as a Multilayer switch.  
A screenshot of a computer

Description automatically generated with low confidence

“Multilayer” means that the switch has hardware and software to perform routing as well as switching functions.

Enter the following commands. Since the VLAN interfaces do not yet exist, the switch will create virtual interfaces when you enter interface vlan 10 or interface vlan 20. The command ip routing tells the switch to enable its routing software.

ip routing

interface vlan 10  
ip address 192.168.10.1 255.255.255.0  
no shutdown

interface vlan 20  
ip address 192.168.20.1 255.255.255.0  
no shutdown

Graphical user interface, text, application, email

Description automatically generated

This is an excerpt from show running-configuration shows how your configuration should look when you are done.

Text

Description automatically generated

## Step 7 – Configure the default gateway on the PCs

Now that you have configured the addresses for the interfaces on the multilayer switch, you can use them to configure the default gateways for the PCs. The default gateway for PCs on VLAN 10 should be 192.168.10.1, and 192.168.20.1 for VLAN 20.

Graphical user interface, text, application, email

Description automatically generated

## Step 8 – Test

At this point, all PCs should be able to ping each other. The center multilayer switch should have both networks in its route table since they are directly connected.

Text, letter

Description automatically generated

# Simulation – Part 2

Now that we have one side of the classroom working, let’s create the other side and connect the two sides together. The switches we have configured with VLAN 10 and 20 will represent one side of the classroom. Now add the second side of the classroom to your simulation. The configuration will be almost identical, except that we will use VLAN 30 with the 192.168.30.0 network and VLAN 40 with the 192.168.40.0 network.

Get the new network working as you did before, using the same steps. When you are finished, all the PCs on the bottom (new) network should be able to ping each other. We have some work to do before the two sides will be able to ping each other, however.

The VLAN interfaces on the new middle switch will be:  
Text, letter

Description automatically generated

Diagram

Description automatically generated

The middle switches should be configured as shown below.

|  |  |
| --- | --- |
| **Multilayer Switch 0** | **Multilayer Switch 1** |
| interface FastEthernet0/1 | interface FastEthernet0/1 |
| switchport access vlan 10 | switchport access vlan 40 |
| ! | ! |
| interface FastEthernet0/2 | interface FastEthernet0/2 |
| ! | ! |
| <snip> | <snip> |
| interface FastEthernet0/23 | interface FastEthernet0/23 |
| ! | ! |
| interface FastEthernet0/24 | interface FastEthernet0/24 |
| no switchport | no switchport |
| ip address 192.168.100.1 255.255.255.0 | ip address 192.168.100.2 255.255.255.0 |
| duplex auto | duplex auto |
| speed auto | speed auto |
| ! | ! |
| interface GigabitEthernet0/1 | interface GigabitEthernet0/1 |
| switchport trunk encapsulation dot1q | switchport trunk encapsulation dot1q |
| switchport mode trunk | switchport mode trunk |
| ! | ! |
| interface GigabitEthernet0/2 | interface GigabitEthernet0/2 |
| switchport trunk encapsulation dot1q | switchport trunk encapsulation dot1q |
| switchport mode trunk | switchport mode trunk |
| ! | ! |
| interface Vlan1 | interface Vlan1 |
| no ip address | no ip address |
| shutdown | shutdown |
| ! | ! |
| interface Vlan10 | interface Vlan30 |
| mac-address 0004.9a4d.8601 | mac-address 0002.175d.e601 |
| ip address 192.168.10.1 255.255.255.0 | ip address 192.168.30.1 255.255.255.0 |
| ! | ! |
| interface Vlan20 | interface Vlan40 |
| mac-address 0004.9a4d.8602 | mac-address 0002.175d.e602 |
| ip address 192.168.20.1 255.255.255.0 | ip address 192.168.40.1 255.255.255.0 |
| ! | ! |

If you look carefully, you will see both switches have entries on interface FastEthernet0/24 that we have not discussed.

There are two methods to declare interfaces on a switch that are to be used for routing. The first is the method we used above, where we created virtual interfaces (int vlan 10, 20, etc.) A second method is to take a physical interface and change it from a switch port to a router port. In Cisco IOS, the command to do that is no switchport (strange, but it works.) We are demonstrating the use of physical interfaces as router interfaces in the connection between the two sides of the classroom network. Enter these commands on the two multilayer switches.

|  |  |
| --- | --- |
| **Multilayer Switch0** | **Multilayer Switch 1** |
| interface FastEthernet0/24 | interface FastEthernet0/24 |
| no switchport | no switchport |
| ip address 192.168.100.1 255.255.255.0 | ip address 192.168.100.2 255.255.255.0 |
|  |  |

Here is a drawing that shows only the network connecting the two sides.  
Diagram

Description automatically generated

Once you have the IP addresses configured for the interfaces that connect the two sides, there is one step remaining: routing. In our case it is easy and can be covered by default routes. If Multilayer Switch 0 receives traffic that it is not on a directly connected network, it simply forwards the traffic on to Multilayer Switch 1.

**Multilayer Switch 0**  
ip route 0.0.0.0 0.0.0.0 192.168.100.2

Likewise, Multilayer Switch 1 forwards traffic on to Multilayer Switch 0.

**Multilayer Switch 1**  
ip route 0.0.0.0 0.0.0.0 192.168.100.1

## Test

If you are lucky and have made no typographic or logical errors, every PC should be able to ping every other PC. If not, troubleshoot the problems in a logical manner with the assistance of the instructor. Anyone can slap things together; it takes expertise to solve problems and make the network work.

# Now with real hardware

Put your design into action using the classroom hardware. Be careful that the two middle switches are Cisco 3560 24 PoE switches, as they are the only multilayer switches we have. For the outer switches, any of the other switches will do. Remember that one side of the class will need to use VLANS 30/40 on networks 192.168.30.0/192.168.40.0 and the other side will need to use VLANS 10/20 on networks 192.168.10.0/192.168.20.0

# Hand In

1. the file from your Packet Tracer simulation
2. Write two questions that I could ask students to see if they understand VLANs and this lab.

## Note on 3650 switches

The 3650 switch will not power on unless you add a power supply as shown below. The 3**65**0 requires that you give it power supplies (or you can just change to a 3**56**0.)Graphical user interface

Description automatically generated