VLANS REPORT

The cisco definition of a VLAN is as follows "*A group of devices on one or more LAN's that are configured in a way that they can communicate as if they were attached to the same wire*".

So why would we use VLAN's?

VLAN's are useful for allowing certain devices on a network to communicate to one another while not causing high congestion. A network consisting of a couple of hundred devices and no VLAN's can get congested very fast and cause notable delays. By configuring VLAN's within a network we can help relieve congestion by only communicating messages to relevant devices rather than every device on the network. If we had an office scenario with fifty devices in a sales department and fifty devices in an accounting department, we could create two separate VLAN's so broadcast messages are not send to everyone, in turn, slowing down the network. If there is a broadcast within in a VLAN, it stays within that VLAN. Also, if there is a fault within a network, only the devices on that VLAN will be affected.

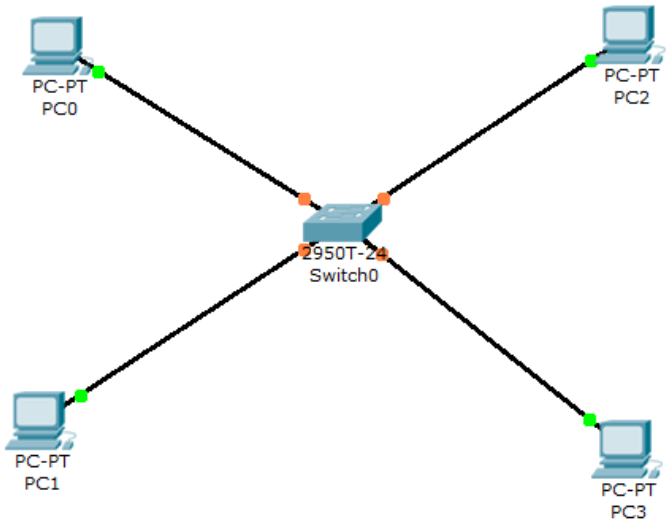
Rules about VLANS

Although VLAN's are relatively simple to configure, care must be taken regarding the assigning of IP addresses and the addressing scheme used. All devices in the same VLAN must have the same subnet. Trunk links are used to communicate messages across switches but in order to communicate between VLAN's, a layer 3 device must be used. The default VLAN is 1. When creating VLAN's, the default is automatically set to vlan1. As this is the default, it is recommended that when configuring a management VLAN, VLAN 1 is never chosen for security purposes.

Access & Trunk links

An access link is generally a connection between a switch and a host/end device. Access links can only carry traffic for one VLAN. When traffic has to go between two switches, a trunk link is used. When traffic travels between switches, a tag is applied to the packet to inform the receiving switch of where to send the packet. Unlike access links, a trunk link can carry traffic from different VLAN's at any given time. Trunk link connections can connect Switch – Switch, Switch – Router, or Switch – Server.

Configuring a VLAN.



So let's assume that the four PC's shown in the screenshot above are all on an office network. We want to create two separate VLANS, one for PC's 0 and 2 which are in the accounting department, and one for PC's 1 and 3 which are in the Sales department.

The first step is to initialize the VLAN on the switch.

```
Switch(config)#vlan 2
Switch(config-vlan)#name accounting
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name sales
Switch(config-vlan)#exit
```

We have now created the two separate VLAN's, but if we use the *show vlan brief* command, we see that no ports have been assigned. Note that the default VLAN is VLAN 1 and so when creating a new VLAN, it is customary to start from 2.

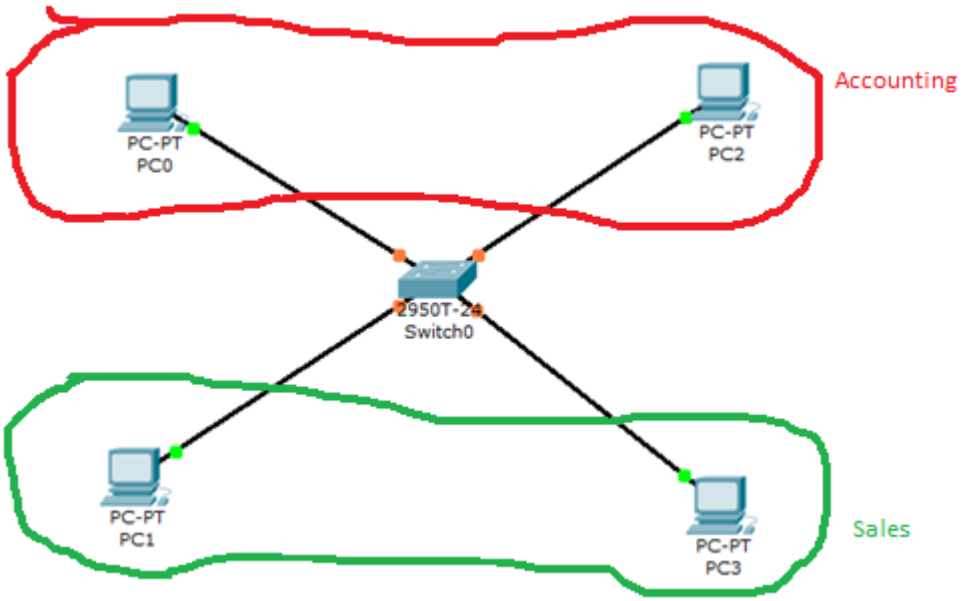
```
2    accounting                       active
3    sales                            active
```

The next step is to assign each of the ports to a VLAN. Using the commands below it is possible to assign a port to a VLAN.

```
Switch(config)#int fa0/2
Switch(config-if)#switch mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa
```

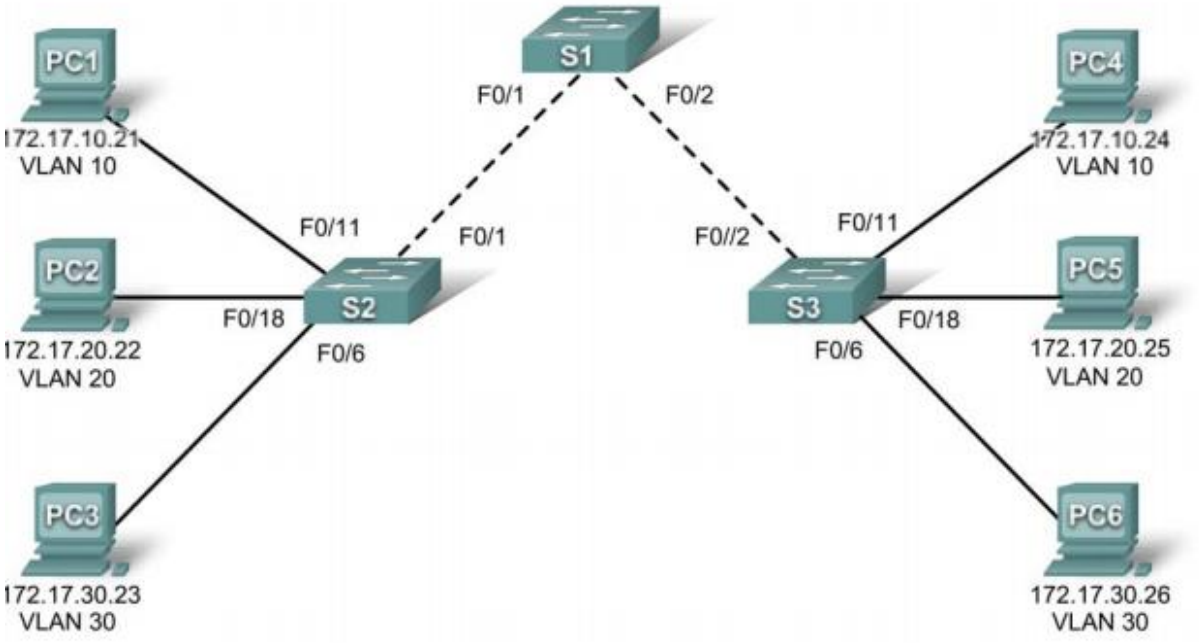
After adding each port to a VLAN, the *show vlan brief* command can be used to confirm they have been successfully configured.

```
2    accounting                       active    Fa0/1, Fa0/2
3    sales                            active    Fa0/3, Fa0/4
```



A network containing 2 VLAN’s has successfully been created. Any broadcasts meant for the accounting department or the sales department will only be send to end devices within their respective VLAN’s, reducing traffic and thus making the network more manageable. Obviously a network with so few PC’s would not need to be divided into separate VLANS. This is for example purposes only.

Lab – Basic VLAN configuration



The aim of this lab is to successfully recreate the network shown. In order to do so, a number of VLAN's need to be configured. To create the different VLANS, we follow the same procedure as before.

```
S1(config)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name Guest(Default)
S1(config-vlan)#exit
```

Here 4 separate VLAN's have been created using Switch 1. We verify this using *show vlan brief*

```
10   Faculty/Staff                  active
20   Students                       active
30   Guest(Default)                 active
99   Management&Native              active
```

After configuring the VLANS on switches 2 and 3 and assigning the relevant ports to each VLAN, their respective tables are as follows

Switch 2:

```
10   Faculty/Staff                  active    Fa0/11
20   Students                       active    Fa0/18
30   Guest(Default)                 active    Fa0/6
99   Management&Native              active
```

Switch 3:

```
10   Faculty/Staff                  active    Fa0/11
20   Students                       active    Fa0/18
30   Guest(Default)                 active    Fa0/6
99   Management&Native              active
```

We can see from the tables above that the correct ports have been assigned. We now need to assign a management VLAN to the network.

Why do we need a management VLAN?

A management VLAN is configured to allow for the managing of switches on the network. By adding an IP to the management switch, the network administrator can manage the switch remotely.

```
S1(config)#int vlan 99

%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

```
S2(config)#int vlan 99

%LINK-5-CHANGED: Interface Vlan99, changed state to up
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
```

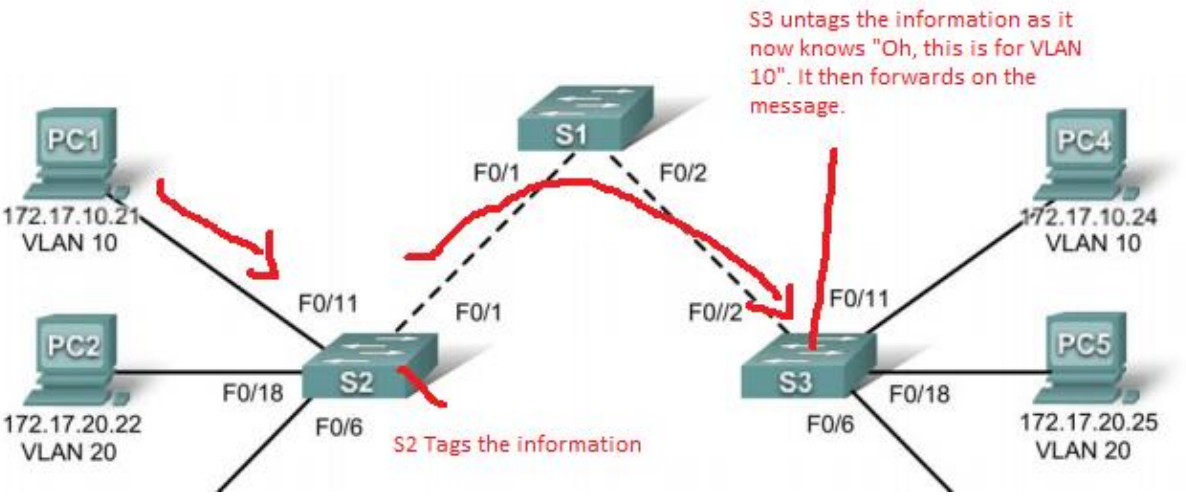
```
S3(config)#int vlan 99

%LINK-5-CHANGED: Interface Vlan99, changed state to up
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
```

We now need to address the issue of tagging. When information is passed across a trunk link, it needs to be tagged.

Why does the information need to be tagged?

Take the topology we are configuring. If PC1 wants to send a message to PC4, it has to pass a trunk link. PC1 sends its message, say a broadcast, to S2. S2 knows that the information is for VLAN 10 so it alters the frame to include a tag that essentially says “I am for VLAN 10.” When the frame reaches the other end of the trunk link, Switch 3 sees the tag and knows where to send the frame. It removes the tag and forwards to the intended destination(s). Tagging frames before they go onto trunk links

assures that the information reaches its intended destination without being sent to incorrect destinations.



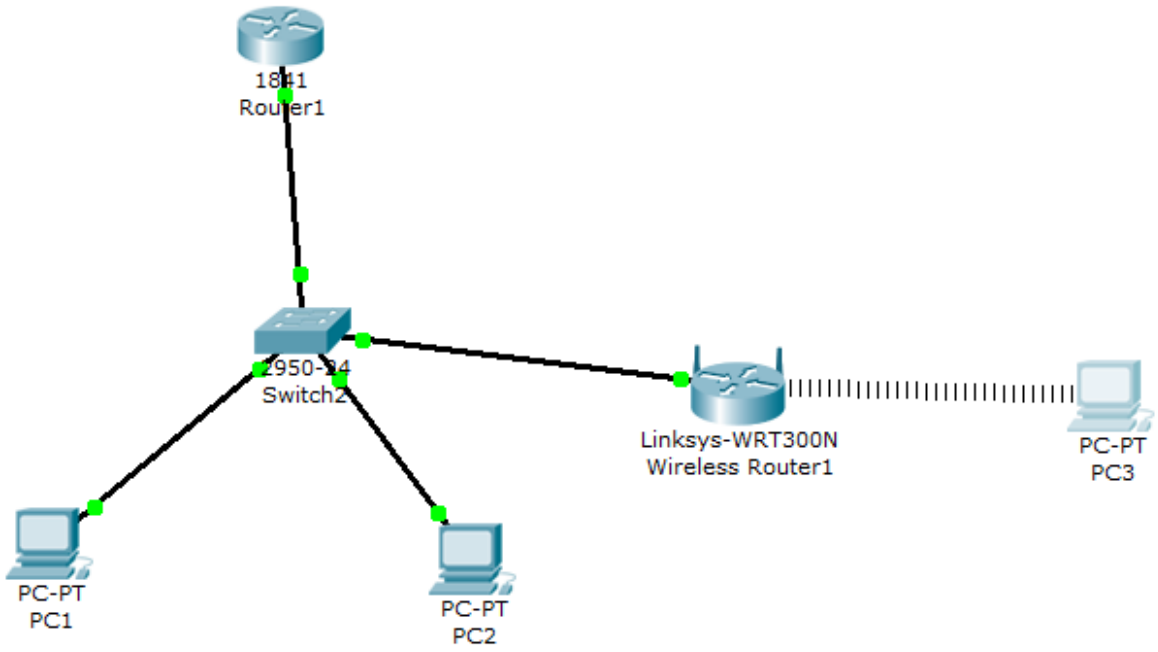
After configuring the trunks using the *switchport mode trunk* command on all switches, we can check to see that they have been initialized correctly using the *show int trunk* command

```
S1#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,99
Fa0/2       1,10,20,30,99
```

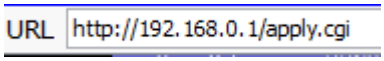
We can check to see that the trunk link is correctly configured by pinging switches 2 and 3 from switch 1.

```
S1#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms


S1#ping 172.17.99.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/6 ms
```

Basic Wireless Configuration

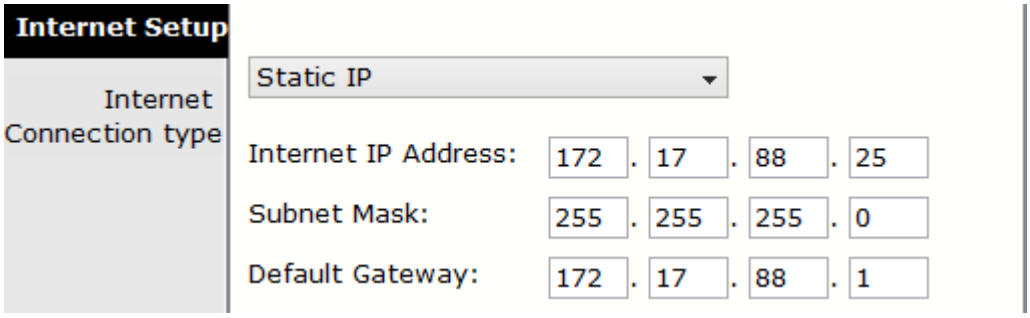


When I was configuring the topology shown, I found that the default IP address of the wireless router was 192.168.0.1 as opposed to 192.168.1.1.

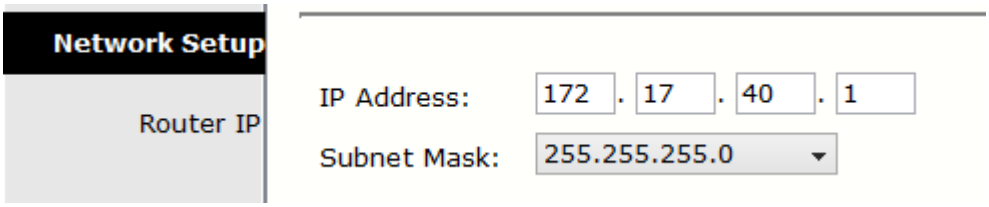


I also found that in contrast with the spec, to be able to access the wireless router via PC3, the username and password were both “admin”. Apparently it is common amongst newer routers to have this set as their default.

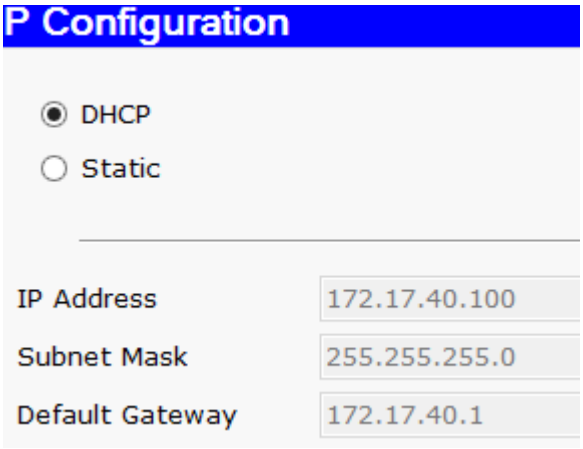
Under the *Internet Setup* tab, I changed the connection type and then set the IP address, subnet mask and default gateway of the router.



I then altered the router IP settings under the Network Setup tab.

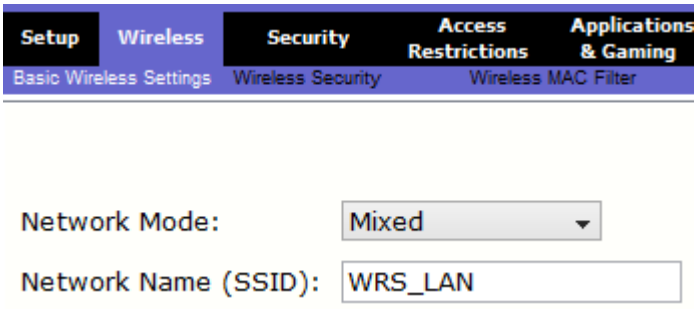


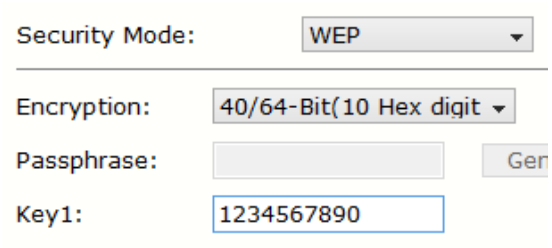
After the new changes are saved, a new connection must be established. As PC 3 was originally allocated an IP on the 192.168.0.1 network, I had to reselect the DHCP setting under PC 3's IP address tab, in order to get an IP on the 172.17.40.1 network

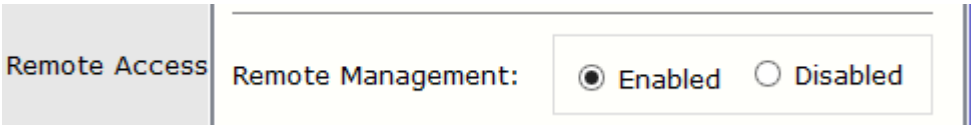


After doing so, it is once again possible to access the router via the web browser. The username and password are the same as before, "admin".

Under the Wireless tab, it is possible to alter the name of a LAN. Whatever is entered here will be visible when we search for a connection later after inserting the Linksys card into PC 3. In this case, the visible connection will be WRS_LAN.







In order to log in, the new password “cisco123” must now be used.

To enable PC3 to wirelessly connect to the router, the computer must be turned off and the linkseys-WMP300N must be inserted. After turning it on, a wireless connection can be established by selecting the WRA_LAN SSID and entering the key “1234567890”.

Now that the wireless has been enabled, it is possible to ping PC’s 1 and 2 from PC3.

```
PC>ping 172.17.20.22

Pinging 172.17.20.22 with 32 bytes of data:

Request timed out.
Reply from 172.17.20.22: bytes=32 time=37ms TTL=126
Reply from 172.17.20.22: bytes=32 time=14ms TTL=126
Reply from 172.17.20.22: bytes=32 time=14ms TTL=126
```

```
PC>ping 172.17.10.21

Pinging 172.17.10.21 with 32 bytes of data:

Request timed out.
Reply from 172.17.10.21: bytes=32 time=22ms TTL=126
Reply from 172.17.10.21: bytes=32 time=20ms TTL=126
Reply from 172.17.10.21: bytes=32 time=15ms TTL=126

Ping statistics for 172.17.10.21:
```

Mistakes I made in this lab

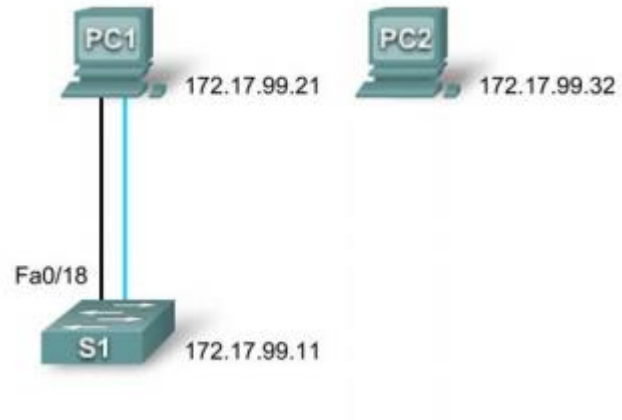
After configuring the majority of settings for this lab, I reset the router, instead of turning off PC 3.

After I had the topology configured I tried to ping both PC1 and PC2. The ping to PC2 was successful however the one to PC 1 failed. I had set the incorrect IP address on the fa0/1.10 interface.

Problems

I had a major problem trying to log in to the wireless router via PC 3 after I changed the password to "cisco123". To log in initially the username and password were both "admin", even though the spec specified that the username should be left blank. When the password was changed I was unable to log back in. I had to access the GUI of the router directly as opposed to through the web browser from PC 3. After I set the password that way, it worked perfectly.

Lab 2.5.1 Basic Switch Configuration



Here the VLAN 99 is created and assigned an IP address.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#int vlan 99

%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

After configuring all ports from 1 – 24 to be in VLAN 99, we get a confirmation message informing us that VLAN 99 is up.

```
S1(config)#interface range fa0/1 - 24
S1(config-if-range)#whitchport access vlan 99
                   ^
% Invalid input detected at '^' marker.

S1(config-if-range)#switchport access vlan 99

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if-range)#exit
```

After setting the IP address on PC 1, a ping can be successfully sent to the switch.

```
PC>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.11: bytes=32 time=4ms TTL=255
Reply from 172.17.99.11: bytes=32 time=5ms TTL=255
Reply from 172.17.99.11: bytes=32 time=5ms TTL=255
```

After setting the speed on the fa0/18 port and configuring full duplex, the link between the switch and the PC goes down.

We can then record the mac addresses of both PC 1 and PC2

PC 1:

```
Physical Address.....: 00E0.F9A8.2B3C
IP Address.....: 172.17.99.21
```

PC 2:

```
Physical Address.....: 0060.5CA6.AE7E
IP Address.....: 172.17.99.32
```

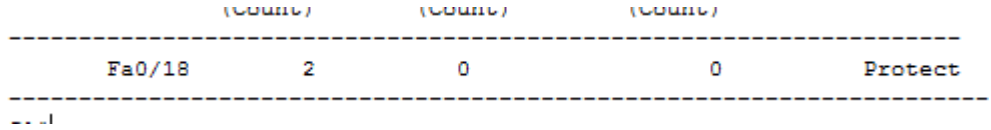
We can configure a static MAC address on the fa0/18 port using PC 1's MAC address.

```
S1(config)#mac-address-table static 00E0.F9A8.2B3C vlan 99 interface fa0/18
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    00e0.f9a8.2b3c    STATIC      Fa0/18
--
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation protect
S1(config-if)#end
```

Why use port security?

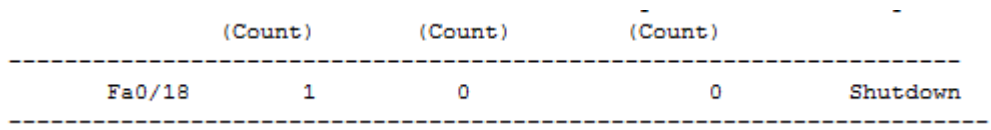
Adding port security to a switch gives the administrator more control over the network. The administrator can determine which MAC addresses have access to the network, thus preventing any unwanted connections, reducing risk of attack from a rogue source.

There are a number of different ways security can be implemented among the ports. In the first example, a maximum count of 2 mac addresses can be assigned to the fa0/18 port.



	(Count)	(Count)	(Count)	
Fa0/18	2	0	0	Protect

In the second example, the configuration shows that only 1 mac address is allowed and that any violation of that protocol results in shutdown.



	(Count)	(Count)	(Count)	
Fa0/18	1	0	0	Shutdown

If we now disconnect PC 1 and connect PC 2, the ping is not successful and a shutdown takes place as the mac address of PC 2 is not that which is expected by the switch. The port status changes to Secure-Shutdown.

Conclusion: Advantages of VLAN's

Dividing a network into multiple VLAN's reduces congestion on the network.

VLAN's allow for greater security. The administrator can configure port security to monitor access to the network.

Packets are kept securely within their intended VLAN's.

Broadcasts are not spread across VLAN's.

Convenience – If users on a VLAN need to change location, say to a different floor in a building, no extra configuration needs to be done as their MAC addresses will still be registered to their respective VLANs.

Disadvantages of VLAN's

The network is more complicated to manage than if only one giant LAN was configured.

In order to communicate across multiple VLAN's a router is needed.

Why use inter-VLAN routing if VLAN's are set up to segregate parts of a network?

VLAN's are not necessarily configured to segregate areas within a network, but more so to facilitate easier network management (through implementation of an organized system), faster bandwidth, and by stopping unnecessary broadcasts.