VLANs

Lesson 0 – an introduction

Università Ca'Foscari Venezia

CLIL Content and Language Integrated Learning

What is a ***subnet*** and
Why is it a good idea to divide a network in sub-networks?

What is a ***broadcast domain***?

a ***broadcast domain***

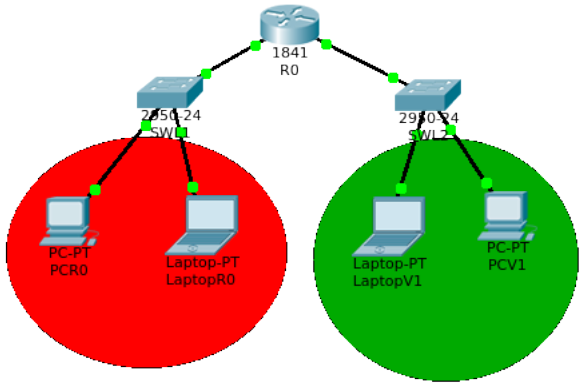
contains all devices that can reach each other at the data link layer (OSI layer 2) by using broadcast

All ports on a hub or a switch are by default in the same broadcast domain

All ports on a router are in the different broadcast domains and routers don't forward broadcasts from one broadcast domain to another.

[https://study-ccna.com/collision-broadcast-domain/]

We know that in order to subnet a LAN we need a L3 device: a router



VLANs – Lesson 0 – an introduction

We know that subnetting a LAN has some valuable advantages:

- It divides a single broadcast domain in smaller ones, improving performances
- It enforces security
- It Makes easier the management and troubleshooting of the network

VLAN definition

VLAN is a way of diving a broadcast domain.

Or, to be precise:

*"VLAN technology logically segments the network into separate **Layer 2** broadcast domains whereby packets are switched between ports designated (set) to be within the same VLAN"*

[Cisco Net Academy]

VLAN benefit

Beside the benefits of traditional subnetting, VLAN gives two more advantages:

1. It reduces the number of intermediate devices;

2. It separates the logical topology of network segments from the physical topology. That allow logical network topologies to overlay the physical switched infrastructure…

Therefore, reconfiguration of the network can be done through software rather than by physically unplugging and moving devices or wires.

Our Lessons

1. Configuring port based VLAN (untagged) on the same switch
2. Extending VLANs to a second switch: Trunk link (tagged ports) and IEEE 802.1Q frame
3. Inter VLAN routing (using a router and sub-interfaces)
4. Inter VLAN routing using a L3 switch
5. Access Control List

VLANs – Lesson 1

Foreword: these notes are meant for the students of the fifth year in computer science at ITI Marzotto-Luzzatti – Valdagno.

They are completed by other teaching material like video lessons, online quizzes, laboratories. All the material, excepted the videos, is available at https://www.v-learning.it/iis/

A special thanks to Mattia Bedani and Francesca Rodighiero

VLANs – Lesson 1

We are *going to learn*

How to define and configure two different **port based VLANs** on a Cisco switch

Tools needed…

only Packet Tracer (7.0)

You should *already know*

what is in the CCNA routing and Switching syllabus, in particular:

- Behaviour of a switch
- Ethernet (IEEE 802.3)
- IPv4 subnetting
- ARP protocol
- IOS basic CLI commands

VLANs – Lesson 1 - A definition

VLAN (Virtual Local Area Network) is a technology that allows to logically divide a broadcast domain at Layer 2 (Data Link layer)

or, in other words,

A technology that can divide a LAN in sub-networks without the need of a router.

VLANs – Lesson 1 – IOS Commands

Command	Comment
S0(config)#**vlan** *vid*	*defines a VLAN and puts the switch into VLAN configuration mode*
S0(config-vlan)#**name** *VLAN_NAME*	*gives a name to the VLAN*
S0#**show vlan**	*displays VLAN information*
S0(config)#**interface** fa *n/m*	You can also use the **range** option: int range fa n/m - q
S0(config-if)#**switchport mode access**	Enter access mode
S0(config-if)#**switchport access vlan** *vid*	*assigns an access port to the VLAN identified by vid*
S0(config-if)#**spanning-tree portfast**	it is used to disable the spanning tree protocol, improving the performances of the network. But, as the IOS warning message says, be carefull...

VLANs – Lesson 1 – step by step

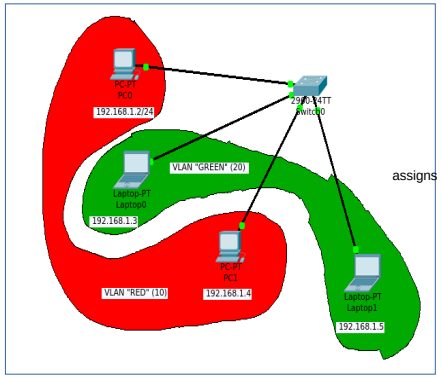
1. **Create a small LAN** : take a bunch of end devices and put them together through a switch (just pay attention to the ports you are connecting the PCs to)
2. **Assign an appropriate IP address** : you may use a typical private IP address scheme: 192.168.1.0/24
3. **Visualize the broadcast domain** : watch the broadcast communication caused by an ARP request (remember to clear the arp cache; *arp -d*)
4. **Create two vlans**: the RED one (id 10) and the GREEN one (id 20). Use the commands: S0(config)#**vlan** *10*;S0(config-vlan)#**name** *RED* ...
5. **Check vlan configuration :** S0#show vlan. Note that all ports are assigned to VLAN 1 by default.
6. **Assign ports :** from 2 to 5 to the RED vlan, from 10 to 15 to the GREEN one:
   - S0(config)#interface range fastEthernet 0/2 – 5
   - S0(config-if)#switchport mode access
   - S0(config-if)#switchport access vlan *10*
   - S0(config-if)#spanning-tree portfast

   Do the same for the GREEN vlan

VLANs – Lesson 1 – step by step

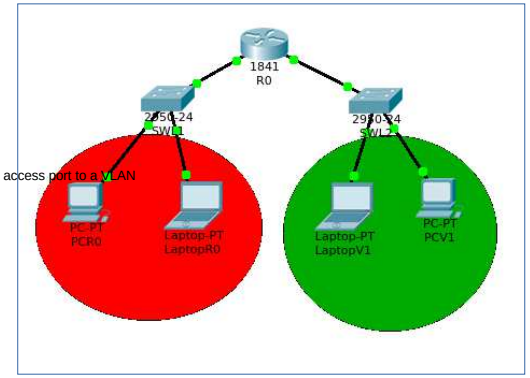
7. **Check vlan configuration again** : and notice that the interfaces you assigned to the RED and GREEN vlans are not members of the VLAN 1 anymore.
8. **Check interoperability** between PCs members of the same vlan and see that they cannot communicate with end-devices belonging to a different vlan (use the ping command)
9. **Visualize broadcast domains again** and see they are reduced.
10. **Visualize the mac table** : S0#show mac-address-table

Advantage n.1:
VLANs reduce the number of intermediate devices therefore reducing costs and complexity



a) Using VLAN technology

assigns an access port to a VLAN



b) without VLAN technology

VLANs – Lesson 1 - Practice

Exercise 1.1:

Now it is your turn:
Create three different VLANs on the same switch:
vlan 10 : “guest” - fa 0/2 – 0/4
vlan 20 : “student” - fa 0/5 – 0/15
vlan 30 : “teacher” - fa 0/16 – 0/20
And check, using the ping command, that each vlan is separated from the others.

VLANs – Lesson 2

WE are *going to learn*

- How to configure a trunk link (tagged port), between two switches
- The IEEE 802.1Q frame

Required tools:

Packet Tracer

You should *already know*

what is in the CCNA routing and Switching syllabus

And what is in Lesson 1:

how to configure an access vlan port (untagged)

VLANs – trunk link

A **Trunk link** can carry multiple VLAN traffic and is normally used to connect switches to other switches or to routers.

To identify the VLAN a frame belongs to, the switch must support the IEEE 802.1Q standard.

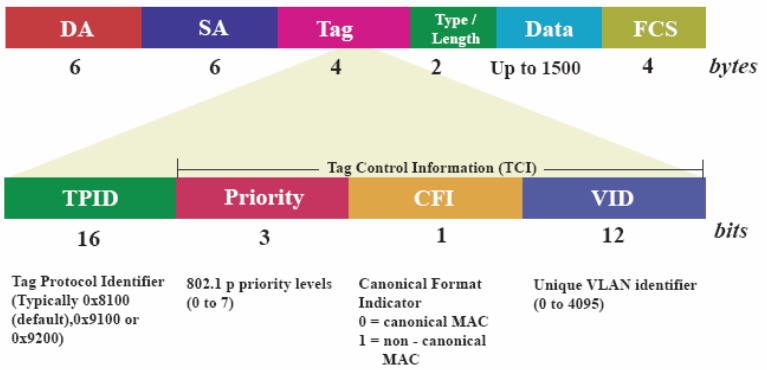
VLANs – Lesson 2 – IOS Commands

```
S0(config)#interface fastEthernet n/m
S0(config-if)#switchport mode trunk
S0(config-if)#switchport trunk allowed vlan x,y
```

// by default, a trunk port sends traffic to and receives traffic from all VLANs. This command specifies that only the x and y vlan are allowed on the link.

```
S0#show interfaces trunk
```

VLANs – IEEE 802.1Q Frame



- TPID always have a value of 0x8100 to signify an 802.1Q tag.
- The Priority field is used by 802.1Q to implement Layer 2 quality of service (QoS).
- The CFI (Canonical Format Identifier) bit is used for compatibility purposes between Ethernet and Token Ring.
- The VID field is used to distinguish between VLANs on the link.

Dot1Q and Native Vlan

In simulation mode you can notice that vlan 1 is the only one that is not tagged in the trunk.

That's because VLAN 1 is the native vlan (and the default one)

native *VLAN frames are transmitted unchanged through a trunk link*

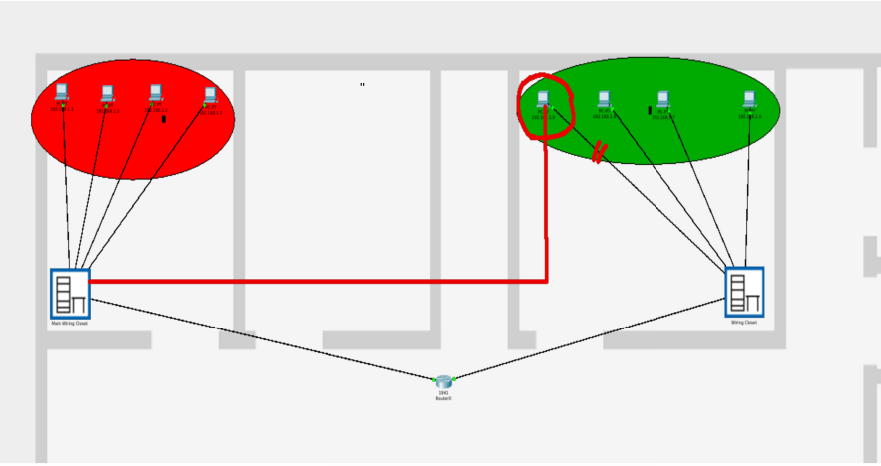
VLANs – Lesson 2 – 2nd Advantage

VLAN technology makes ***logical topology independent from the physical one*** and that provides an easy, flexible, less costly way to modify logical groups in changing environments.

For example: if I need to change the vlan (or subnet) a PC belongs to, I only need to change one switch interface set-up, using a couple of CLI commands - given from a remote terminal, if you like…

While, without VLANs, you have either to move the PC to a different room or to lay down a new cable through the building… In any case

you need to change the physical topology.



VLANs – Lesson 2 – Practice

Now it is your turn

Exercise 2.1:

Extend Exercise 1.1 so that the tree VLANs are replicated on a second switch (work in physical topology mode and place the new switch in a different room), connected to the first by a trunk link.

Exercise 2.2:

Analyse in simulation mode what happen if you use an access port (i.e a RED vlan interface) instead of a trunk link. Which frames are allowed to go through the link? Why ?

VLANs – Lesson 3

We are *going to learn*

- How to allow different VLANs to communicate with each other (inter VLAN routing)
- The configuration of sub-interfaces in a router

Required tools:

Packet Tracer

You should *already know*

what is in the CCNA routing and Switching syllabus

And what is in Lesson 1 and Lesson 2:

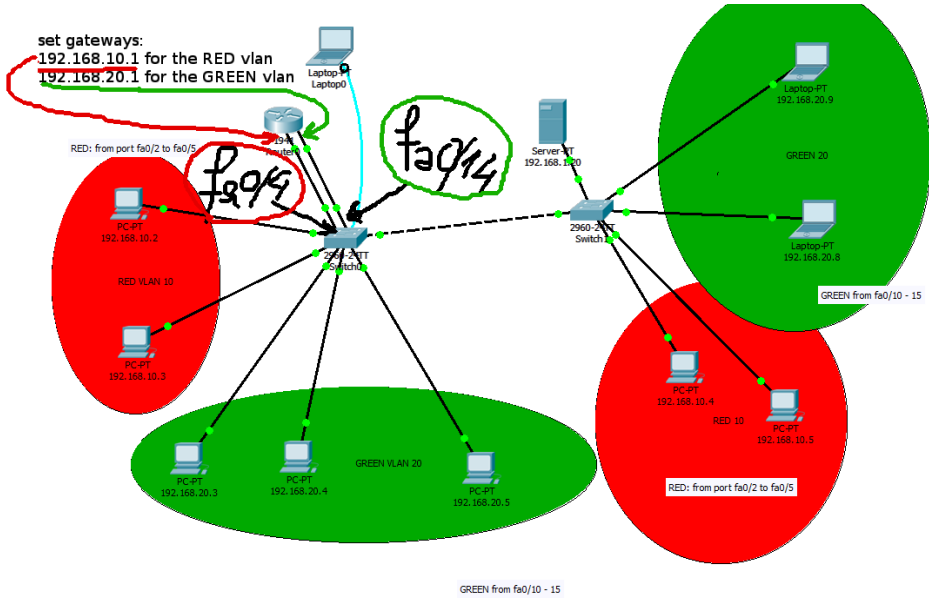
how to configure an access vlan port (untagged) and a trunk link (tagged)

Lesson 3 - Inter VLAN Routing

So far we have learnt how to divide a broadcast domain in VLANs that are logically separated at Data Link Layer.

But if we want them to be able to communicate, we need a Layer 3 device: a **router**

Therefore we need to distinguish the VLANs at Network Layer (layer 3) choosing a different IP network address for each VLAN: 192.168.10.0/24 for the RED vlan and 192.168.20.0/24 for the GREEN one.



If we want also the vlan 1 to be able to communicate with the others, we must add an interface to The router and connect it to a vlan1 interface on the Switch0...

Lesson 3 - Inter VLAN Routing

But if we had 10 different vlans to connect, we would need 10 different interfaces on the router and 10 different cables going from the switch to the router…

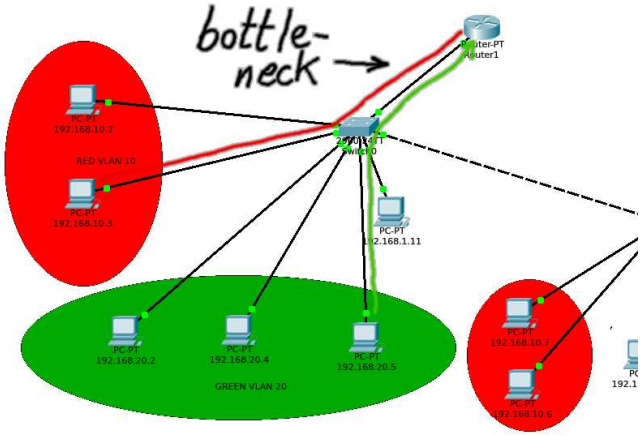
That is not much sensible (and quite costly).

Actually there is a better solution: **logical sub interfaces**

VLANs – Lesson 3 – IOS Commands
(for sub-interfaces)

```
R0(config)#interface fastEthernet n/m
R0(config-if)#no ip address
R0(config-if)#no shutdown
R0(config)#interface fastEthernet n/m.10
R0(config-subif)#encapsulation dot1q 10
// Or, for the native vlan:
R0(config-subif)#encapsulation dot1q 1 native
R0(config-subif)#ip address 192.168.10.1
255.255.255.0
```

Inter VLAN routing – bottleneck



We'll learn in the next lesson how to avoid this bottleneck using a Layer 3 switch.

VLANs – Lesson 3 – Practice

Now it is your turn

Exercise 3.1:

Enhance Exercise 2.2 allowing all the VLANs to communicate with each other. Use three different interfaces in the router.

Exercise 3.2:

Improve Exercise 3.1 using sub-interfaces in the router and a trunk link to connect it to the switch.

VLANs – Lesson 4 : Multilayerswitch

We are *going to learn*

- How to implement inter VLAN routing through a multilayer switch
- The configuration of L3 interfaces on a L3switch

Required tools:

Packet Tracer

You should *already know*

what is in the CCNA routing and Switching syllabus

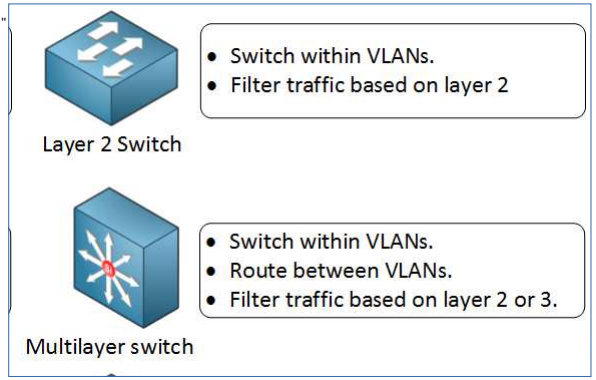
And what is in previous lessons (1,2 and 3):

Access and trunk vlan port configuration and inter VLAN routing through a common router

Lesson 4 - Inter VLAN Routing through a multilayer switch

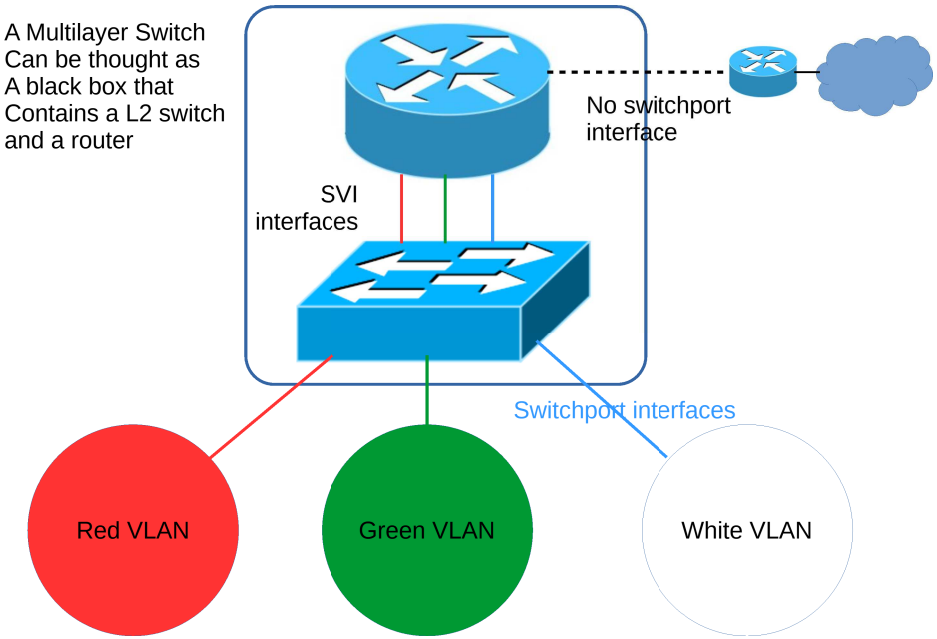
In the former lesson we observed the bottleneck represented by the trunk link between the switch and the router.

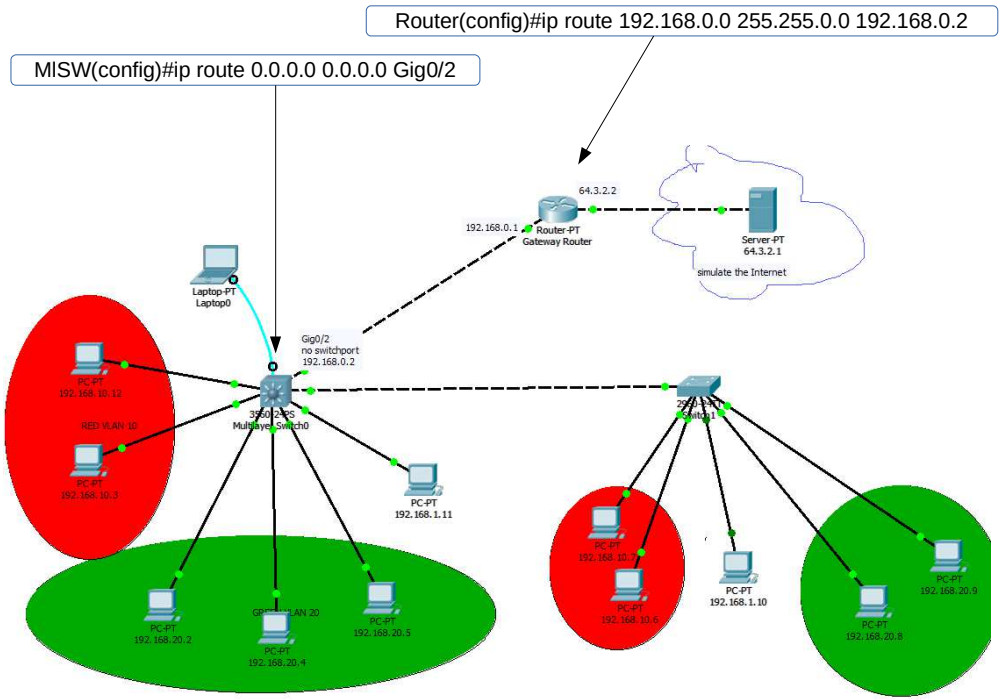
We can improve the situation by using a Multilayer switch that implements both the functionalities of a switch and a router



InterVLAN routing – L3 switch

A Multilayer Switch
Can be thought as
A black box that
Contains a L2 switch
and a router





VLANs – Lesson 4 – L3switch configuration

We need to configure the new L3 switch with the same list of commands of the switch it is substituting. We could copy the config file, but it is a useful exercise to insert all the commands again.

Beside, to implement interVLAN routing we need to configure the SVIs the way we've learnt last year...

MlSw01(config)#**int vlan 10**

MlSw01(config-if)#**ip address 192.168.10.1 255.255.255.0**

MlSw01(config-if)#**no shut**

Remember! explicitly enable routing:

MlSw01(config)#**ip routing**

VLANs – Lesson 4

The trunk link between the Multilayer Switch and the L2 switch

Note: the default mode configuration for a Cisco switch interface is "dynamic auto", therefore, when we connect it to another trunk port it set itself automatically to trunk mode

VLANs – Lesson 4

The connection between the Multilayer Switch and the router Gatway

We set the port that connect the multilayer switch to the router Gateway to **"no switchport"** mode so that it becomes a layer 3 interface and we can assigned it an IP address.

MlSw01(config)#**int** Gig0/2

MlSw01(config-if)#**no switchport**

MlSw01(config-if)#**ip address** 192.168.0.2 255...

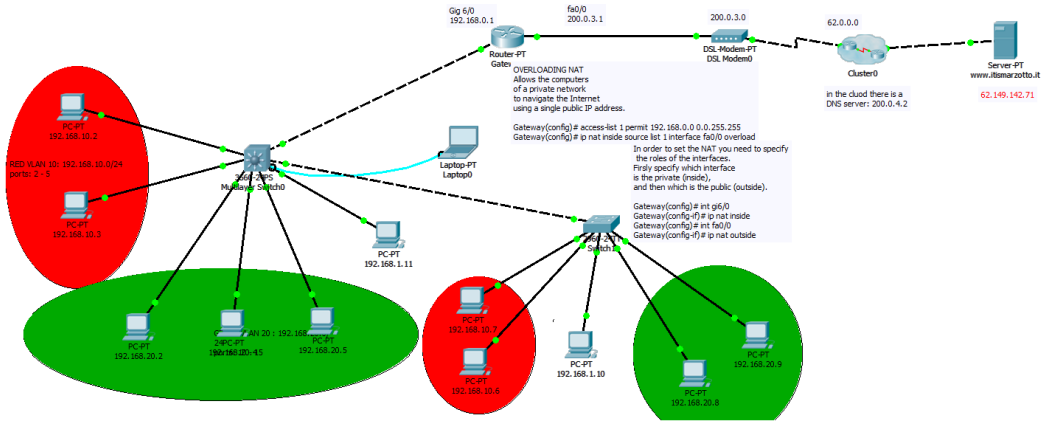
MlSw01(config-if)#**no shutdown**

Now we only need to configure the default route on the L3 switch so that all the vlans can access the Internet

MlSw01(config)#**ip route** 0.0.0.0 0.0.0.0 Gig0/2

To better simulate the Internet we can use a Cluster and implement NAT on our Router Gateway.

But this is another lesson ...



VLANs – Lesson 4 – Practice

Now it is your turn

Exercise 4.1:

Enhance Exercise 3.2 using a L3 switch instead of SW1 and the router. Add a gateway router and a public web site to simulate the internet connection.

We’ll learn in the next lesson how to apply Access Control Lists to filter the traffic.

VLANs – Lesson 5 : ACL

We are *going to learn*

- How to filter the traffic between different VLANs applying standard Access Control Lists

Required tools:

Packet Tracer

You should *already know*

what is in the CCNA routing and Switching syllabus

And what is in previous vlan lessons (1,2,3 and 4):

Access and trunk vlan ports; inter VLAN routing through a router or a multilayer switch

Lesson 5 – Standard ACL

A (Standard) **Access Control List** is a list of access entries with the following structure:

```
access-list id {deny | permit} source_ip_add wildcard_mask
```

use a **deny** or **permit** keyword and specify the type of packets that you want the device to *drop* or to *accept* for further processing. By default, an access list denies everything because the list is terminated by an implicit deny any entry. ***Therefore, you must include at least one permit entry to create a valid access list.***

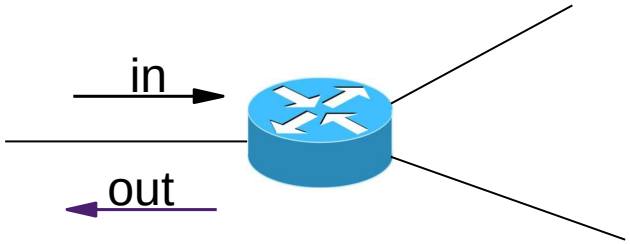
Note: the ***order*** of the entries is very important since the device applies each entry in the order in which it occurs in the access list.

VLAN Lesson 5 : ACL (2)

When the list is complete, it has to be applied to an interface:

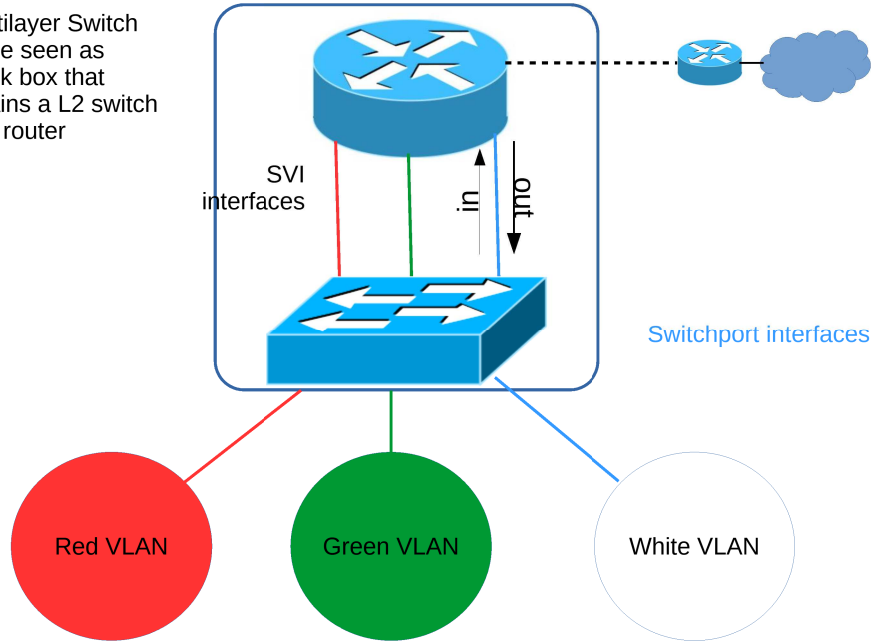
```
R0(config)# interface {id | vlan ..}
R0(config-if)# ip access-group id {in | out}
```

use a **in** or **out** keyword to apply the access list to the incoming or outgoing packets on the specified interface.



ACL on a L3 switch

A Multilayer Switch
Can be seen as
a black box that
Contains a L2 switch
and a router



VLANs – Lesson 5 – ACL on L3 switch

If, for instance, we want the RED VLAN to be isolated from the GREEN and the WHITE VLANs, but to be able to navigate the Internet, we can set the following ACLs

MlSw01(config)# **access-list** 19 **deny** 192.168.1.0 0.0.0.255
MlSw01(config)# **access-list** 19 **deny** 192.168.20.0 0.0.0.255
MlSw01(config)# **access-list** 19 **permit any**
MlSw01(config)# **int vlan** 10
MlSw01(config-if)# **ip access-group** 19 **out**

Try and check in simulation mode the result of a ping from the RED to the GREEN vlan… You'll get a "*request time out*" response.

VLANs – Lesson 5 – ACL on L3 switch

The previous ACL, applied to the RED vlan, deny all packets coming from the GREEN and the WHITE vlans; but does not block a packet coming from the RED and aiming to the GREEN or the RED. To achieve this we can set the following ACL

MlSw01(config)# **access-list** 18 **deny** 192.168.10.0 0.0.0.255
MlSw01(config)# **access-list** 18 **permit any**
MlSw01(config)# **int vlan** 20
MlSw01(config-if)# **ip access-group** 18 **out**
MlSw01(config)# **int vlan** 1
MlSw01(config-if)# **ip access-group** 18 **out**

VLANs – Lesson 5 – ACL on L3 switch

Can you work out the ACL that deny a specific host (192.168.10.2) of the RED vlan the navigation of the internet?

Can you work out the ACL that deny the access to the internet to a range of ip addresses (192.168.10.1 – 192.168.0.7)

1st answer:
MlSw01(config)# **access-list** 17 **deny** 192.168.10.2
MlSw01(config)# **access-list** 17 **permit any**
MlSw01(config)# **int vlan** 10
MlSw01(config-if)# **ip access-group** 17 **in**

2nd answer: the same as before, just add the wildcard mask:
MlSw01(config)# **access-list** 17 **deny** 192.168.10.0 0.0.0.7

VLANs – Lesson 5 – A further look

delete an ACL from an interface

just put **no** ahead:

For instance, to delete ACL 18 from SVI 10:

(config)**# int vlan 10**

(config-if)**# no ip access-group *18* out**

VLANs – Lesson 5 – A further look

delete a single entry in a ACL

 # show access-lists ***// shows something like:***

Standard IP access list *19*
10 deny 192.168.20.0 0.0.0.255
20 deny 192.168.1.0 0.0.0.255
30 permit any
...

(config)# ip access-list standard *19*

(config-std-nacl)# no ***10*** //delete the first entry

VLANs – Lesson 5 – A further look

add a single entry to an ACL

// add an entry to ACL 19 in third position

Switch(config)#**ip access-list standard** *19*

Switch(config-std-nacl)#*25* deny 192.168.30.0 0.0.0.255

Switch(config-std-nacl)#end

Switch#show access-lists

VLANs – Lesson 5 – A further look

ACL can be of two types:

1) **Standard** (range 1-99 e 1300-1999)
   - Easy identification of the addresses (only source).
   - permit or deny of a whole family of protocols.
2) **Extended** (range 100-199 e 2000-2699)
   - complex identification of the addresses (source and destination) .
   - permit or deny a specific protocol or service.

You can find out more about this topic at:

http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#standacl

VLANs – Lesson 5 – Practice

It is now your turn

Exercise 5.1:

Add to Exercise 4.1 another VLAN: “Server” (id 40) and put a web and a DNS server in it; set the proper ACLs so that

- Vlan “Guest” can access only the Internet but none of the other vlans
- “Student” and “Teacher” vlans can’t talk to each other but can access the “Server” vlan