Vlans on Mikrotik environment

I will try to explain how to deal with vlans and qos on Mikrotik devices.

In switching technology, we have three modes of ports: Access, Trunk and Hybrid.

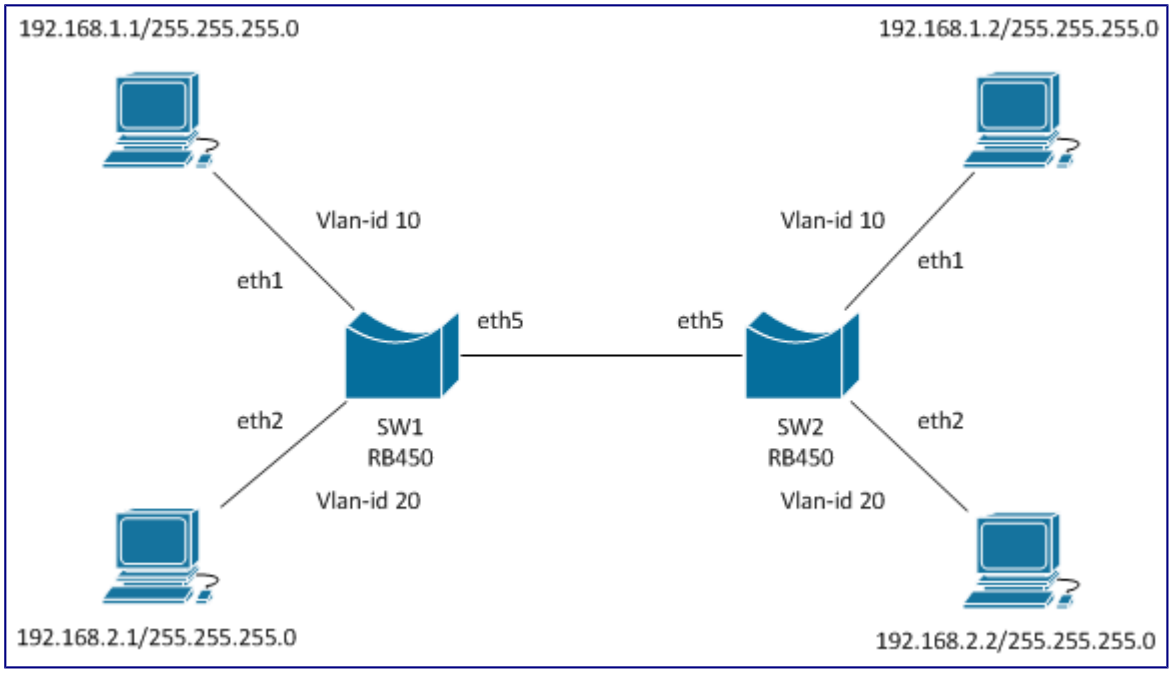
An access port should be used only with untagged packets. This kind of port is where you connect your PC to the switch.

An trunk port is capable of receiving and forwarding packets from multiple vlans. This one is to interconnect switchs.

An Hybrid port is a special mode that allow untagged and tagged packets on the same port. Imagine that you have a Voip desktop phone, you will connect your PC to the phone and the phone to the switch. We will have a vlan for voip and untagged data for the PC.

Vlan interfaces on Mikrotik devices should always be seen as "add tag on egress / remove tag from ingress".

Lets look at this network diagram:



To be able to achieve this setup we need eth1 and eth2 as access-ports and eth5 as trunk port.

To config the vlans on the trunk port:

```
/interface vlan add name=vlan-10 vlan-id=10 interface=ether5 disabled=no
/interface vlan add name=vlan-20 vlan-id=20 interface=ether5 disabled=no
```

To be able to forward the packets from access-ports to vlans we need bridges:

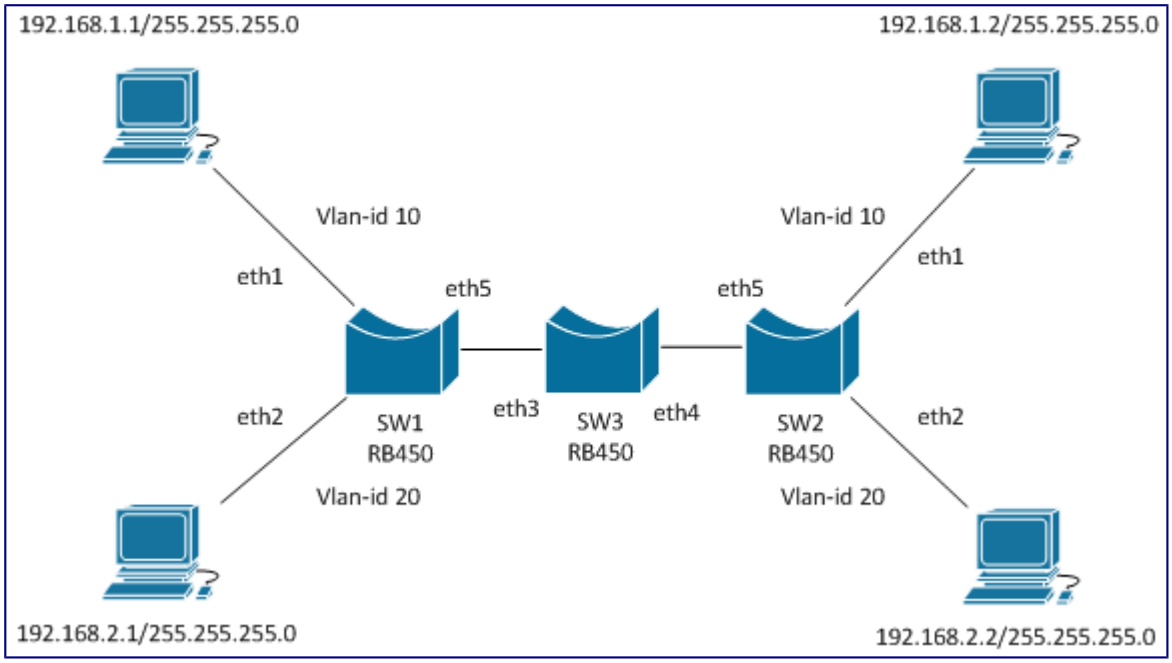
```
/interface bridge add name=br-vlan10 disabled=no
/interface bridge add name=br-vlan20 disabled=no
```

Now just add the ports to the bridges:

```
/interface bridge port add interface="vlan-10" bridge="br-vlan10" disabled=no
/interface bridge port add interface="ether1" bridge="br-vlan10" disabled=no
/interface bridge port add interface="vlan-20" bridge="br-vlan20" disabled=no
/interface bridge port add interface="ether2" bridge="br-vlan20" disabled=no
```

It's done, only hosts on the same network will be able to communicate.

And if we have another switch in the middle of the trunk?

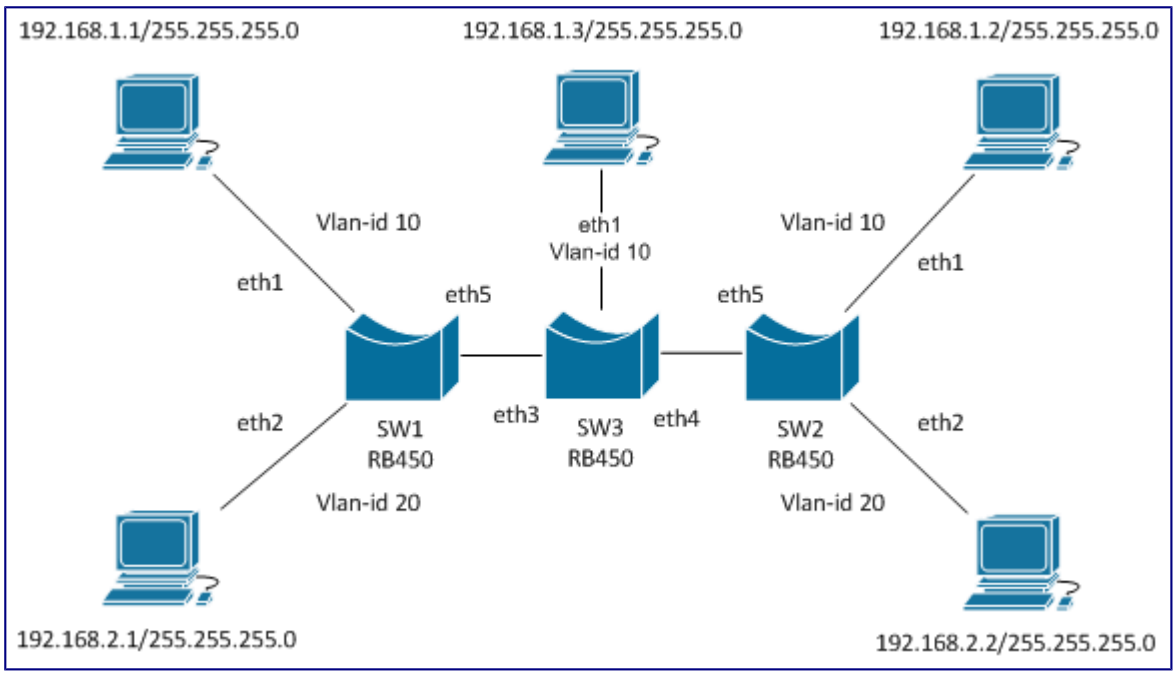


Configuration on SW1 and SW2 remains the same, on SW3 we need to:

```
/interface bridge add name=br-trunk disabled=no
/interface bridge port add interface="ether3" bridge="br-trunk" disabled=no
/interface bridge port add interface="ether4" bridge="br-trunk" disabled=no
```

Interfaces eth3,eth4 are trunk ports and and only need to forward tagged packets. We do not need to do any tag add/remove so there is no need to add vlans.

A more advanced setup is with acess-ports on SW3:



SW1 and SW2 remain the same, on SW3 we need to add:

```
/interface vlan add name=vlan-10 vlan-id=10 interface=br-trunk disabled=no
/interface bridge add name=br-vlan10 disabled=no
/interface bridge port add interface="vlan-10" bridge="br-vlan10" disabled=no
/interface bridge port add interface="ether1" bridge="br-vlan10" disabled=no
```

On SW3 packets arriving at eth1 will be forward inside the br-vlan10 to vlan-10 and here they become tagged.

With their tag set they will go inside br-trunk.

QoS on Vlans

This is called 802.1p. Inside the vlan tag we have 3 bits that are available to set CoS (priority) and go from 0 to 7. 0 is the lowest priority and 7 the highest.

By default all packets have CoS set to 0.

The CoS field can be set in two places: /ip firewall mangle or /interface bridge filter

When working directly on the vlan interface (edge router or device that adds the tag), use /ip firewall mangle.

When dealing with bridges use /interface bridge filter.

To set the CoS field the action that is used on the rules is set-priority. When this is set on the vlan interface, it will set it´s CoS id.

On this set-up we will remain with the previous network diagram.

Lets see if setting our CoS work:

On SW1 set this:

```
/interface bridge filter add chain=output mac-protocol=ip ip-protocol=icmp
action=set-priority new-priority=1
```

On SW3 set this:

```
/interface bridge filter add chain=input ingress-priority=1 action=log
disabled=no
```

Now ping between to pc's on the same network. Then look at the logs on SW3, there should be something like this:

Jan/02/1970 04:08:24	firewall info	forward: in:ether1 out:ether2, src-mac 00:0c:42:43:18:7b, dst-mac 00:24:7e:10:4b:47, vlan-id 20, vlan-prio 0, eth-proto 0800, ICMP (type 0, code 0), 192.168.2.2->192.168.2.1, prio 1->0, len 60
Jan/02/1970 04:08:25	firewall info	forward: in:ether1 out:ether2, src-mac 00:0c:42:43:18:7b, dst-mac 00:24:7e:10:4b:47, vlan-id 20, vlan-prio 0, eth-proto 0800, ICMP (type 0, code 0), 192.168.2.2->192.168.2.1, prio 1->0, len 60
Jan/02/1970 04:08:26	firewall info	forward: in:ether1 out:ether2, src-mac 00:0c:42:43:18:7b, dst-mac 00:24:7e:10:4b:47, vlan-id 20, vlan-prio 0, eth-proto 0800, ICMP (type 0, code 0), 192.168.2.2->192.168.2.1, prio 1->0, len 60
Jan/02/1970 04:08:27	firewall info	forward: in:ether1 out:ether2, src-mac 00:0c:42:43:18:7b, dst-mac 00:24:7e:10:4b:47, vlan-id 20, vlan-prio 0, eth-proto 0800, ICMP (type 0, code 0), 192.168.2.2->192.168.2.1, prio 1->0, len 60

From the logs we see that it was received with prio 1, and was changed to prio 0.

By default bridges always set the CoS to 0. If we want the CoS to remain through all the network, we should set this rule on SW3:

```
/interface bridge filter add chain=forward action=set-priority new-
priority=from-ingress
```

To be continued... (vlans over wifi, wmm)

If you find something wrong or if you need support please send mail to jorge dot amaral at officelan dot pt

http://wiki.mikrotik.com/wiki/Vlans_on_Mikrotik_environment