Práctica VLAN

1 Introducción Teórica

Se trata de hacer uso de las funcionalidades llamadas VLAN que permiten los conmutadores gestionables en general posibilitar la división en diferentes segmentos de red de enlace a los equipos que estén directa o indirectamente conectados a uno o varios conmutadores.

Existen básicamente 3 tipos de VLAN, las VLAN basadas en MAC, las basadas en capa 3, las basadas en reglas y las basadas en puertos. Este último tipo es el mas extendido y el único que se utilizará en esta práctica y el que se describe a continuación.

Por defecto, todos los puertos de un conmutador están en el mismo dominio de broadcast de nivel de enlace. Las VLAN separan de forma lógica los puertos de un mismo conmutador en diferentes dominios de broadcast, de forma que las tramas broadcast gestionadas por un switch no serán reenviadas a todos los puertos del switch sino a los puertos asociados a la misma VLAN que la trama generatriz. Así, puede decirse que una VLAN es un dominio de broadcast de nivel 2 o de enlace.

Cada VLAN en una red tiene asociado un identificador llamado VLAN_ID. Este identificador puede estar asociado al puerto de entrada de la trama (membresia basada en puerto), o a una etiqueta con el VLAN_ID insertada en la trama de salida llamada 802.1Q (membresía explícita).

El formato de la etiqueta 802.1Q está representado en la figura 1 donde se muestra insertado en una trama estándar 802.3.

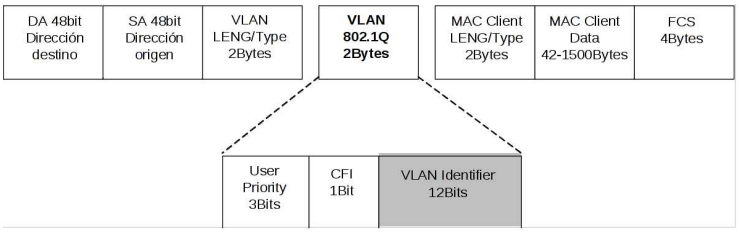

Figure 1: Etiqueta 802.1Q

Dentro de la etiqueta 802.1Q, el campo "User priority" se regula por la norma 802.1p, el bit CFI siempre está a "0" y el campo de 12 bits "VLAN Identifier" es el VLAN_ID (o "VID" o "vid"). Al "User priority" y al bit CFI se le llama TPID.

1.1 Tipos de puerto VLAN

En las VLAN basadas en puerto existen dos tipos de asignación de VLAN por puerto, básicamente dependiendo de si la trama entra en el puerto o sale del puerto; así existe el puerto en **modo Access** y el pueto en **modo Trunk**.

1.1.1 Puerto en modo Access

El modo Acces es el modo de funcionamiento mas sencillo, donde la membresía a una VLAN depende exclusivamente del puerto de entrada al conmutador de la trama y se gestiona exclusivamente por las colas del conmutador de forma interna. Los dispositivos conectados a un puerto del conmutador con una VLAN asignada no reciben ningún tipo de información sobre ello, y envian y reciben tramas estándar

802.3 hacia/desde el conmutador.

Un puerto puede formar parte de una sola VLAN en modo Access (sin etiquetar). No obstante existen marcas de conmutadores que permiten mas de una VLAN por puerto sin etiquetar, como el modo "Multi" de CISCO, lo que hace que en esos conmutadores no se permita simultaneidad entre los modos "Multi" y "Trunk".

En los Mikrotik RB2011 con OpenWRT (y en una mayoría de otros modelos) no existe el modo "Multi". La configuración de un puerto en varias VLAN suele considerarse un error y se gestiona mediante el PVID (priority VID) descrito mas adelante.

1.1.2 Puerto en modo Trunk

Este modo es también llamado modo etiquetado o modo "tagged". Indica que todas las tramas llevan una etiqueta 802.1Q en la cabecera Ethernet con el identificador de VLAN correspondiente. Si la trama es de salida del conmutador, el VLAN_ID insertado es el asociado al puerto del origen de la trama (es decir, al puerto por donde entró la trama), y si la trama es de entrada sólo será reconocida si lleva una cabecera compatible con 802.1Q.

Las tramas etiquetadas que llegan a un puerto trunk serán redirigidas hacia los puertos asociados a la VLAN indicada en el VLAN_ID incluido en la trama. Si una trama llega sin etiqueta 802.1Q, el comportamiento del Switch dependerá del sistema operativo del mismo. Básicamente en el caso de Cisco estas serán descartadas, y en el caso de OpenWRT la trama seá asociada a la VLAN por defecto, llamado PVID. En otros Switches puede darse la opción tanto de descartar como de asignar la PVID, siendo esta última opción la mas común.

1.2 VLAN por defecto y PVID

En general se suele llamar VLAN por defecto (Default VLAN) a la VLAN en la que está asignada la CPU del propio conmutador. Este término suele confundirse con el PVID, aunque no son lo mismo, pues la VLAN por defecto está referida a todo el conmutador, y el PVID está referido a un puerto.

El PVID es el VLAN_ID configurado para ese puerto específico. El valor del PVID dependerá del tipo de puerto al que se le asigne:

- Puerto Access: el PVID es el mismo que el VLAN_ID asignado a ese puerto.
- Puerto Trunk: el PVID se configurará manualmente para asignar un VLAN_ID a todas las tramas entrantes que no lleven etiqueta 802.1Q. En general, es recomendable que no se gestionen tramas sin etiquetar en este tipo de puertos para evitar complicaciones en la transmisión de tramas; y en caso de asignacón de un PVID en esos puertos, se considera una buena práctica que el PVID sea el mismo que la VLAN por defecto.

1.3 VLAN en OpenWRT

OpenWRT mantiene su propia numeración de puertos que no siempre se corresponde con los etiquetados en la carcasa de los dispositivos. En particular, en los equipos Mikrotik RB2011 el mapeo de puertos de "carcasa" con puertos de "OpenWRT" aparece en la figura 2.

Como puede verse en la figura 2, en el Mikrotik RB2011 conviven dos conmutadores independientes (switch0 y switch1). Para ambos conmutadores, la CPU del Mikrotik RB2011 con OpenWRT está conectada al puerto 0.

Existen dos API para la gestión de las VLAN en OpenWRT , una basada en el sistema */etc/config/network*, y la mas actual basada en la herramienta `swconfig` . En el caso del Mikrotik RB2011 con OpenWRT funcionan ambos. Se utilizará el sistema */etc/config/network* para una configuración permanente y el sistema basado en `swconfig` para configuración en tiempo real.

- **Sistema swconfig**

  Los comandos principales son:

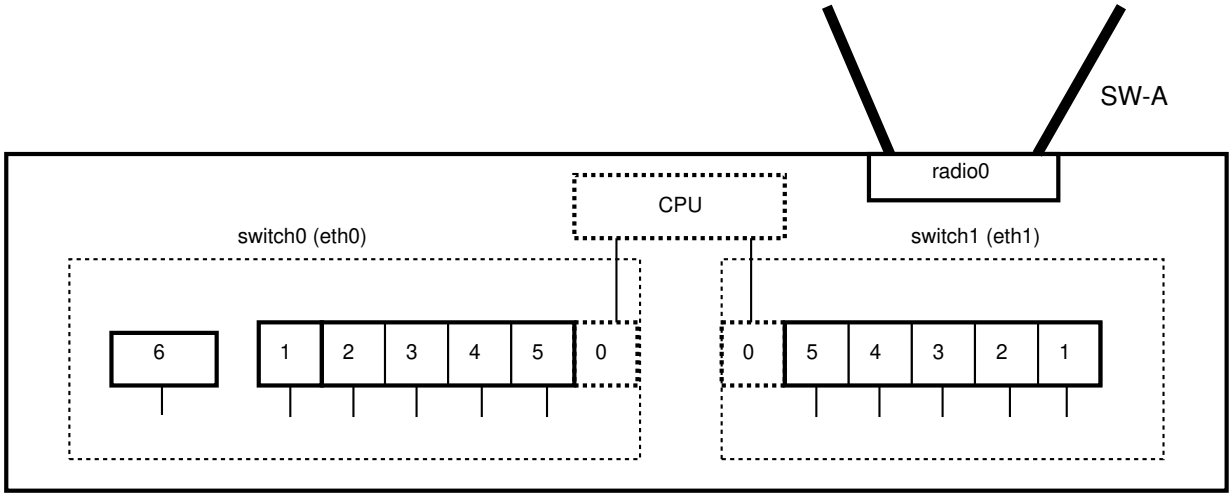

Figure 2: Arquitectura interna - Mikrotik RB2011

– Para conocer la sintaxis de swconfig

```
SWA# swconfig
swconfig dev <dev> [port <port>|vlan <vlan>] (help|set <key> <value>|get <key>|load <↩
    config>|show)
```

– Para conocer el nombre de los Switch internos del dispositivo:

```
SWA# swconfig list
```

– Para visualizar información de VLAN y puertos de cada switch:

```
SWA# swconfig dev <switch> show
```

– Para conocer las opciones de los atributos y argumentos de la sintaxis de cada switch:

```
SWA# swconfig dev <switch> help
```

– Para visualizar la tabla puerto/mac:

```
SWA# swconfig dev switch0 get arl_table
```

– Para activar/desactivar las vlans:

```
SWA# swconfig dev <switch> set enable_vlan 1
SWA# swconfig dev <switch> set enable_vlan 0
SWA# swconfig dev <switch> set apply
```

– Para activar o desactivar un puerto (desactualizado):

```
SWA# swconfig dev <switch> port <portno> set disable <0|1>
```

– Para poner puertos en VLANs:

```
SWA:/# swconfig dev <switch> vlan <VLAN> set vid <VLAN>
SWA:/# swconfig dev <switch> vlan <VLAN> set ports 'PORTS'
SWA:/# swconfig dev <switch> set enable_vlan 1
SWA:/# swconfig dev <switch> set apply
```

Los puertos se ponen separados por espacios; los puertos que estén configurados como trunk llevarán una "t" justo detrás, y los que estén configurados como access (o untagged) llevarán una "u" justo detrás o no llevarán nada.

- Para asignar un pvid a un puerto:

```
SWA:/# swconfig dev <switch> port <PORT> set pvid <VLAN>
SWA:/# swconfig dev <switch> set apply
```

- Asociar una VLAN con VID recién creada con una interfaz IP:

```
SWA:/# ip link add link eth0 eth0.101 type vlan proto 802.1q id 101
SWA:/# ip link set up dev eth0.101
SWA:/# ip addr add 10.A.101.1/24 dev eth0.101
```

El "vid" es lo que asocia la interface IP con la VLAN. Por cuestiones de organización y claridad se recomienda que el nombre de la interface también lleve el "vid" como en el ejemplo (eth0.102), aunque el nombre de la interface podría ser distinto. Para conocer el VID asociado a una interfaz se puede consultar el fichero */proc/eth0.102*

```
SWA:# cat /proc/eth0.102
eth0.102  VID: 102       REORDER_HDR: 1  dev->priv_flags: 1001
         total frames received          6359
          total bytes received        625220
      Broadcast/Multicast Rcvd           138

      total frames transmitted          4247
       total bytes transmitted        1191442
Device: eth0
INGRESS priority mappings: 0:0  1:0  2:0  3:0  4:0  5:0  6:0 7:0
 EGRESS priority mappings:
```

2 Descripción

La práctica pretende adquirir cierta soltura en las tecnologías de redes privadas virtuales (VLAN) tanto en su concepto como en su componente práctica.

Para ello se dispone del Mikrotik RB2011 que se configurará como conmutador con el sistema operativo OpenWRT .

Esta práctica tiene una primera parte diseñada para ser realizada de forma individual y una segunda parte diseñada para ser realizada en pareja o en grupo.

2.1 Objetivos

El objetivo es el aprendizaje y manejo del concepto de VLAN tal y como se describe en el estándar IEEE 802.1Q.

Para ello se utilizan los equipos Mikrotik RB2011 con sistema operativo OpenWRT . No obstante, el alumnado deberá tener en cuenta que la implementación de VLAN en equipos de diferentes fabricantes obligará a conocer de forma detallada sus particularidades. sus comandos y sus métodos, a pesar de existir una visión estandarizada del concepto de VLAN.

El alumnado deberá tener en cuenta además que la selección de las VLAN y sus modos tendrá una repercusión directa en los diagramas topológicos del conjunto de la red y que deberá realizarse con una visión global de la misma, en los tres primeros niveles del modelo TCP/IP, en el físico, en el de enlace y en el de red IP.

2.2 Situación inicial

Dadas las características de compartición del laboratorio y por tanto de sus equipos, la configuración inicial de los equipos puede variar, por lo que habrá que uniformarla en la medida de lo posible.

- Situación de partida de los PC's

  Los PCs deberán arrancar con un direccionamiento de red acorde a la red plana del laboratorio (192.168.29.0/24) y con salida a Internet a través de F0 (192.168.29.1). Por ejemplo: el PC13 arrancará con la dirección IP 192.168.29.113/24 y tendrá como puerta de enlace (Gateway) a F0.

- Situación de partida de las pasarelas (RBM)

  Los RouterBoardsMicrotik (RBM) arrancan con la dirección ip 192.168.29.A siendo A el número de RBM escrito en su carcasa, por ejemplo, el RBM21 arranca con la dirección IP 192.168.29.21. Esta dirección es accesible en la interfaz "br-lan" de la figura 3, es decir, el PC gestor de cada RBM deberá conectarse con el latiguillo con conectores RJ45 a cualquier puerto de la interfaz "lan".

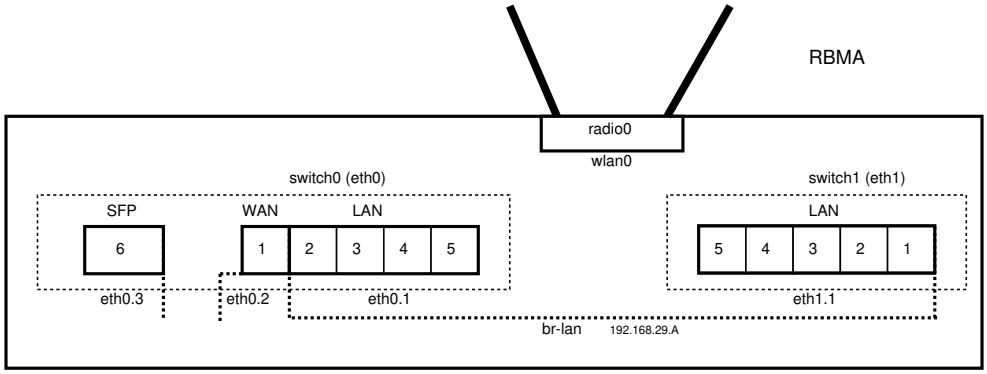

Figure 3: Situación de partida

Para que funcionen como conmutadores, será necesario acceder a ellos y ejecutar el comando:

Listing 1: Conversión en router.

```
root@RBMA:~# ./isa_vlan.sh
```

Desde ese momento, la configuración de las interfaces cambia, así como el direccionamiento IP, según se muestra en la figura 4 y en la tabla 1. Los Mikrotik RB2011 pasarán a convertirse en conmutadores (switch) y tomarán el nombre de SWA, siendo A el mismo número asociado al RBMA anterior.

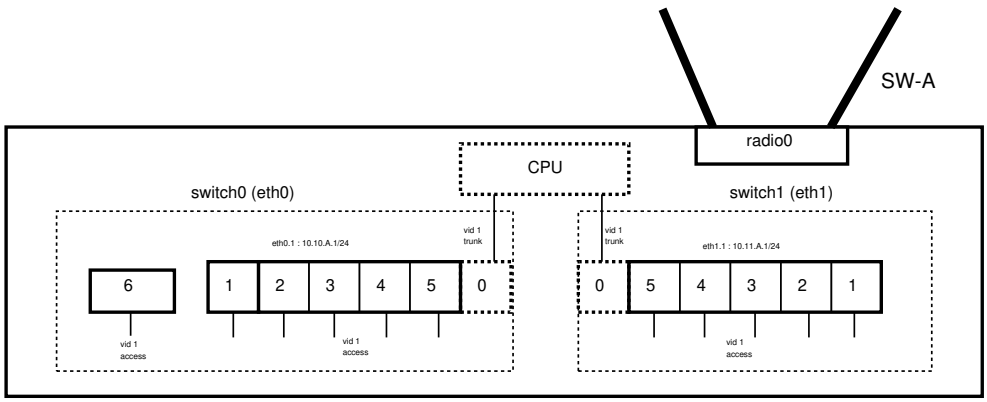

Figure 4: Situación de partida como conmutador.

Table 1: Situación inicial de los conmutadores Mikrotik RB2011

Switch	VLAN	Puertos	Dir. IP
switch0	VLAN 1	1 2 3 4 5 6 0t	10.10.A.1/24
switch1	VLAN 1	1 2 3 4 5 0t	10.11.A.1/24

Los Mikrotik RB2011 tienen incorporados 2 conmutadores (switch0 y switch1) independientes, reconocibles a nivel de interfaz como eth0 y eth1 respectivamente. Por motivos de simplicidad se trabajará a nivel de VLAN exclusivamente con el conmutador switch0, sirviendo el conmutador switch1 como conector de consola para la configuración del SWA.

El switch0 dispone de 7 puertos numerados del 0 al 6. El puerto 6 está deshabilitado. El puerto 0 es un puerto interior que conecta el switch con la CPU del RBM. Los puertos del 1 al 5 son los puertos

con interfaz física rj45 ubicados a la izquierda del frontal de la carcasa del Mikrotik RB2011 (ver figura 4). Se parte de la VLAN 1 (vid 1) a la que están asociados todos los puertos en modo access y el puerto 0 (CPU) en modo trunk.

Se verá la situación inicial para los conmutadores y los equipos de usuario.

- **conmutadores SWA OpenWrt**

  Se dispone de un equipo Mikrotik RB2011 en cada puesto. Cada uno es accesible a través del "switch1" via *ssh* en la dirección IP *10.11.A.1/24* con usuario "root" y passwd "provisional".

  Sólo se trabajará con el "switch0" a nivel de VLAN.

  La configuración inicial se muestra en la figura 4. Esta configuración es una configuración por defecto bastante habitual en el arranque de los equipos conmutadores de cualquier fabricante o sistema operativo. En ella, todos los puertos físicos del conmutador (switch0) están en la VLAN 1 (vid 1) en modo access y el puerto interno que conecta con la CPU del dispositivo conmutador (en este caso el puerto 0) pertenece también a la VLAN 1 pero en modo trunk (indicado con una "t" final en la tabla 1).

  Un resumen de la configuración inicial puede verse en la tabla 2 desde el punto de vista de los puertos del switch0.

Table 2: Situación inicial de switch0 de los Mikrotik RB2011

Puerto	VLAN	modo
0 (CPU)	vid 1	trunk
1	vid 1	access
2	vid 1	access
3	vid 1	access
4	vid 1	access
5	vid 1	access

  La configuración del switch1 no se tocará para no perder conectividad con el dispositivo Mikrotik RB2011 .

- **equipos PC**.

  Los PC's tienen la configuración inicial de la red plana del laboratorio, y deberán configurarse según las normas para poder acceder a los conmutadores.

3 Preparación

Se utilizará el método *swconfig* con los comandos presentados en la sección 1.3. Las acciones básicas son:

Habilitar el switch para disponer de capacidades VLAN Primeramente se activará el switch con las capacidades VLAN. Por ejemplo el switch0. La capacidad VLAN ya está habilitada.

```
SWA:/# swconfig dev switch0  set enable_vlan 1
SWA:/# swconfig dev switch0  set apply
```

Crear VLAN Se crearán las VLAN. Por ejemplo la VLAN 101 y la VLAN 102

```
SWA:/# swconfig dev switch0 vlan 101 set vid 101
SWA:/# swconfig dev switch0 vlan 102 set vid 102
SWA:/# swconfig dev switch0 set apply
```

Nota, el argumento de "vlan" no tiene porqué coincidir con el argumento de "vid". Se pueden utilizar alias para el identificador "vlan", como por ejemplo "MONITORIZACION" o "INFORMATICA". Si se utilizan identificadores numéricos, se recomienda firmemente que sean iguales al "vid".

Asociar VLAN a puertos Se asociarán a cada VLAN los puertos deseados. Por ejemplo los puertos 1,2 y 3 en modo access para la VLAN 101 y los puertos 4 y 5 en modo access para la VLAN 102; el puerto 0 se asociará en modo trunk a ambas VLAN.

```
SWA:/# swconfig dev switch0 vlan 101 set ports '1 2 3 0t'
SWA:/# swconfig dev switch0 vlan 102 set ports '4 5 0t'
SWA:/# swconfig dev switch0 set apply
```

Se recuerda que el añadido "t" en el número del puerto se refiere a "modo trunk" (o "modo tagged").

Eliminar un puerto de una VLAN Es el mismo proceso de asociación, pero sin incluir el puerto que se desea eliminar. Por ejemplo, a la situación anterior se le quiere eliminar el puerto 3 de la VLAN 101 y se quiere añadir el puerto 3 en la VLAN 102.

```
SWA:/# swconfig dev switch0 vlan 101 set ports '1 2 0t'
SWA:/# swconfig dev switch0 vlan 102 set ports '3 4 5 0t'
SWA:/# swconfig dev switch0 set apply
```

Eliminar una VLAN No existe un comando específico para eliminar una VLAN. No obstante una VLAN sin puertos asociados no será operativa y no aparecerá en los registros de estado de VLAN. Por ejemplo se elimina la VLAN 102.

```
SWA:/# swconfig dev switch0 vlan 102 set ports ''
SWA:/# swconfig dev switch0 set apply
```

Asociar una VLAN con una interfaz IP Además de incluir el puerto 0 en la asignación de puertos a una VLAN, para poder acceder a la CPU del switch será necesario crear una interfaz IP y asignar una IP a dicha VLAN. Por ejemplo, crear la interfaz asociada a la VLAN 101 del switch0 y asignarle una IP adecuada. Este paso no será necesario salvo por indicación del docente.

```
SWA:/# ip link add link eth0 eth0.101 type vlan id 101 proto 802.1Q
SWA:/# ip link set up dev eth0.101
SWA:/# ip addr add 10.A.101.1/24 dev eth0.101
```

Eliminar una interfaz asociada a una VLAN Se trataría de ejecutar el comando anterior utilizando el parámetro "del" en lugar del "add".

```
SWA:/# ip link del link eth0 eth0.101 type vlan id 101 proto 802.1Q
```

4 Desarrollo

Este consistirá en la creación de determinadas LAN virtuales (VLAN) y de la realización de algunas pruebas de conectividad de los equipos de usuario pertenecientes a ellas para comprobar su funcionamiento. Asimismo se prestará especial atención a la transmisión de la información de las VLAN entre conmutadores mediante la técnica de trunking con etiquetas 802.1Q.

Se sugiere que el alumno cambie puertos, configuraciones y nombres de VLAN, siempre que sólo afecte al conmutador al que está conectado o que mantenga esos cambios de forma pública, para conocimiento de los otros participantes de la práctica.

La práctica tendrá dos partes: i) pruebas sobre un único conmutador; ii) pruebas sobre dos conmutadores.

4.1 Pruebas sobre un único conmutador

Cada puesto realizará pruebas sobre el conmutador asociado al mismo. Se partirá de la topología de la figura 5.

Una vez configuradas las VLAN en el switch0 usando el PC-A conectado al switch1 (que hará de consola), las pruebas se harán conectando el PC-A a los puertos del switch0 que corresponda.

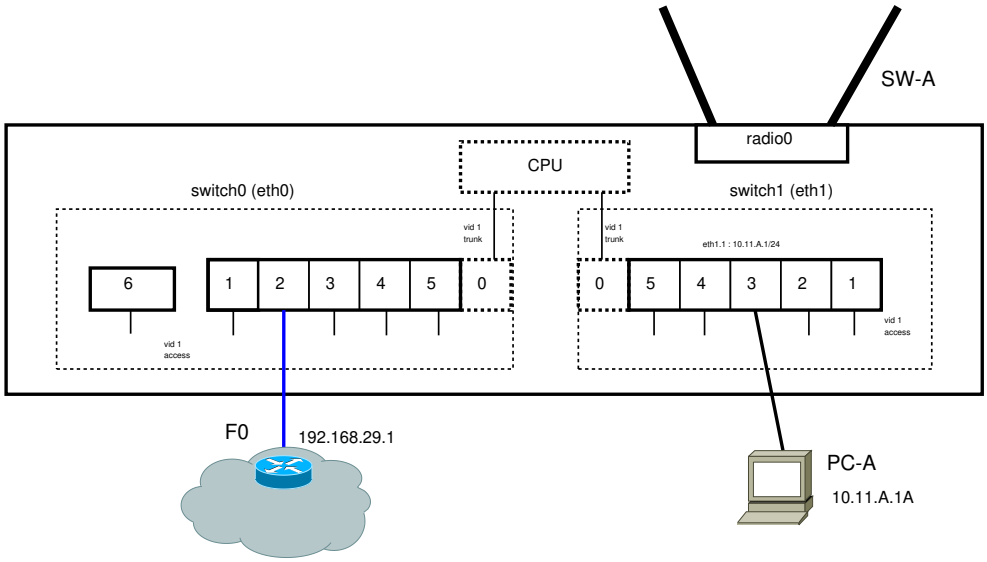

Figure 5: Topología de pruebas inicial.

Se realizarán dos pruebas:

- **Equipos en la misma VLAN**
  - Se creará la VLAN 101 en los puertos 1,2,3 en modo access, y en el puerto 0 en modo trunk.

```
SWA:/# swconfig dev switch0 vlan 101 set ports '1 2 3 0t'
```

  - Se creará la VLAN 102 en los puertos 4,5, y en el puerto 0 en modo trunk.

```
SWA:/# swconfig dev switch0 vlan 102 set ports '4 5 0t'
SWA:/# swconfig dev switch0 set apply
```

  - Se conectará el F0 (cable azul) al puerto 2.
  - Se conectará el PC-A al puerto 3.
  - Se probará la conectividad entre PC-A y FO mediante la utilidad ping. Recordad que ambos tienen que estar en la misma subred IP.

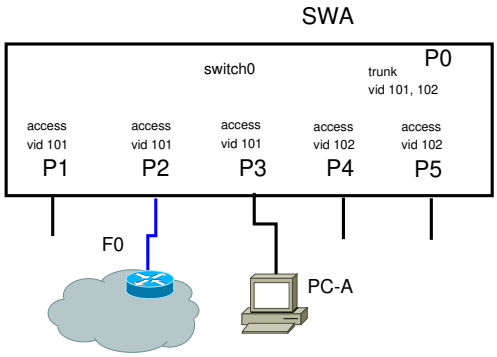

Figure 6: Modo access. Misma VLAN (mismo vid).

- **Equipos en distinta VLAN**
  - Misma configuración anterior de asignación de VLAN a puertos.
  - Se conectará el F0 (cable azul) al puerto 2.

– Se conectará el PC-A al puerto 4.

– Se probará la conectividad entre PC-A y FO mediante la utilidad ping. Recordad que ambos tienen que estar en la misma subred IP.

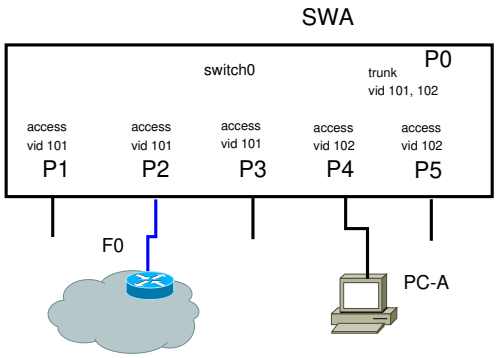

Figure 7: Modo access. Distinta VLAN (distinto vid).

Se invita al alumnado a crear la configuración y probar la tabla 3 de puertos y vlan. Poner "X" en los cuadrados en los que hay conectividad.

Se configurará el conmutador SWA correspondiente para que todos los PC conectados a él pertenezcan a diferentes VLAN; particularmente se configurarán según la tabla 3.

Table 3: Mismo SW, distintas VLAN

	Puerto	1	2	3	4	5
Puerto	VLAN	102	101	102	101	102
1	102					
2	101					
3	102					
4	101					
5	102					

4.2 Pruebas entre dos conmutadores

Se procederá de forma individual a la configuración de los conmutadores SWA y SWB teniendo una visión global de la topología y poniendose de acuerdo el alumnado de los puestos A y B.

La unión entre ambos conmutadores se hará a través del puerto 5, y sólo el SWA tendrá conexión a F0 para evitar bucles indeseados. La figura 8 visualiza de forma genérica la topología, donde tanto PC-A como PC-B irán cambiando de puerto para probar la conectividad con las diferentes configuraciones.

Se cuenta con el modo "access", ya trabajado en la topología de un solo conmutador, y con el modo "trunk" o 802.1Q que permite al puerto que esté configurado en ese modo enviar información de las VLAN a las que pertenece, a través de tramas Ethernet, mediante encapsulación 802.1Q. El otro extremo debe de estar también configurado en ese modo para interpretar esos datos.

Se realizarán dos pruebas:

- **Interconexión en modo Access.**

  En este modo de funcionamiento, la membresía de las VLAN no se transmite a través de los puertos al no llevar las tramas etiqueta 802.1Q.

  – Se crearán las VLAN en los dos conmutadores según la tabla 4. Se permite al alumnado crear otras configuraciones de forma consensuada entre los conmutadores. Se recomienda incluir en "modo trunk" el puerto 0 en todas las VLAN.

    En SWA:

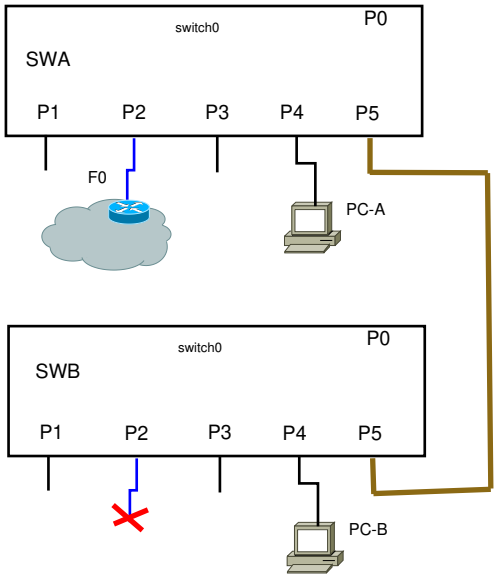

Figure 8: Topología de dos conmutadores.

```
SWA:/# swconfig dev switch0 vlan 101 set ports '1 2 5 0t'
SWA:/# swconfig dev switch0 vlan 102 set ports '3 4 0t'
SWA:/# swconfig dev switch0 set apply
```

En SWB:

```
SWB:/# swconfig dev switch0 vlan 101 set ports '3 4 0t'
SWB:/# swconfig dev switch0 vlan 102 set ports '1 2 5 0t'
SWB:/# swconfig dev switch0 set apply
```

– Se probará la conectividad entre PC-A, PC-B y FO mediante la utilidad ping. Recordad que ambos tienen que estar en la misma subred IP.

Table 4: Diferentes SW, modo "access"

			SWA					SWB				
			P1	P2	P3	P4	P5	P1	P2	P3	P4	P5
		VLAN	101	101	102	102	101	102	102	101	101	102
SWA	P1	101										
	P2	101										
	P3	102										
	P4	102										
	P5	101										
SWB	P1	102										
	P2	102										
	P3	101										
	P4	101										
	P5	102										

- **Interconexión en modo Trunk.**

  En este modo de trabajo, se transmite por el puerto trunk el VLAN_ID asociado al puerto de entrada de la trama, es decir, la trama tiene un formato 802.1Q. El modo trunk se configurará en los enlaces entre los conmutadores Mikrotik RB2011 según la figura 8.

  – Se crearán las VLAN en los dos conmutadores según la tabla 5. Se permite al alumnado crear otras configuraciones de forma consensuada entre los conmutadores. Se recomienda incluir en "modo trunk" el puerto 0 en todas las VLAN.

En SWA:

```
SWA:/# swconfig dev switch0 vlan 101 set ports '1 2 5t 0t'
SWA:/# swconfig dev switch0 vlan 102 set ports '3 4 5t 0t'
SWA:/# swconfig dev switch0 set apply
```

En SWB:

```
SWB:/# swconfig dev switch0 vlan 101 set ports '3 4 5t 0t'
SWB:/# swconfig dev switch0 vlan 102 set ports '1 2 5t 0t'
SWB:/# swconfig dev switch0 set apply
```

– Se probará la conectividad entre PC-A, PC-B y FO mediante la utilidad ping. Recordad que ambos tienen que estar en la misma subred IP.

Table 5: Diferentes SW, modo "trunk"

			SWA					SWB				
			P1	P2	P3	P4	P5	P1	P2	P3	P4	P5
		VLAN	101	101	102	102	101t 102t	102	102	101	101	102t 101t
SWA	P1	101										
	P2	101										
	P3	102										
	P4	102										
	P5	101t, 102t										
SWB	P1	102										
	P2	102										
	P3	101										
	P4	101										
	P5	102t, 101t										

Se invita al alumnado a crear otras configuraciones de puertos y vlan. Poner "X" en los cuadrados en los que hay conectividad.