

## Práctica 2. VLANs y enrutamiento entre VLANs

### Objetivos de aprendizaje

- Comprender el concepto de VLAN (Virtual LANs).
- Diferenciar entre puertos de acceso y puertos troncales. Diferenciar tramas etiquetadas y tramas sin etiquetar.
- Ser capaz de configurar distintos tipos de puerto en un switch.
- Ser capaz de configurar una interfaz administrativa y VLAN de gestión.
- Ser capaz de configurar el enrutamiento entre VLANs en un router.

### Introducción

Un switch es un dispositivo de la capa 2 del modelo OSI que opera como un *bridge* transparente. Su cometido es la conmutación de tramas (en este caso del protocolo Ethernet) entre los dispositivos conectados utilizando las direcciones MAC. Cada switch mantiene una tabla de conmutación como la de la figura 1.

La tabla de conmutación de un switch no es conocida sino que se rellena mediante un proceso de aprendizaje. En la figura 2 se muestra el proceso que se sigue cuando llega una trama al switch.

- Aprendizaje: Cada vez que un host A envía una trama a otro host B, el switch examina la dirección de origen de la trama recibida y le asocia el puerto entrada en la tabla de conmutación del switch.
- Inundación: El switch examina la dirección MAC de destino de la trama, revisa la tabla de conmutación y si no encuentra una entrada con esa dirección reenvía la trama a todos los puertos excepto aquel por el que recibió la trama. Con las direcciones de broadcast y multicast siempre se produce la inundación.
- Reenvío: Cuando el host B responde al host A, el switch revisa si la dirección de destino de la trama está ya en la tabla de reenvío (en este caso lo está debido a que es una trama de respuesta) y cuando encuentra la dirección reenvía la trama directamente al puerto anotado en la tabla de reenvío.
- Filtrado: Cuando la dirección MAC de origen y de destino se asocian al mismo puerto, el switch filtra la trama porque esta ya ha llegado a su destino.

MAC Address	Puerto de salida	Edad (minutos)

Figura 1: Tabla de conmutación de un switch.

- *Aging*: Cuando se añade una nueva entrada la tabla de reenvío esta va acompañada de un contador. Este contador se resetea a cero cada vez que llega un paquete desde la dirección MAC correspondiente al a entrada. Si en algún momento este contador supera un cierto umbral de tiempo la entrada se elimina.

Como Ethernet es un medio compartido, se produce un problema de rendimiento cuando hay muchos dispositivos conectados a la LAN mediante un hub. Con la aparición de los switches es posible acotar los dominios de colisión y dominios de broadcast. Los dominios de colisión son áreas de una LAN en la que las estaciones compiten por el acceso al medio físico compartido. Al utilizar un switch cada host emisor y receptor forman un dominio de colisión separado solucionándose así el problema de rendimiento y escalabilidad. Por otra parte, un dominio de broadcast es el área de una LAN por la que se propagan las tramas broadcast. Los dominios de broadcast no se reducen a un medio físico compartido, si no que quedan limitados por los routers (dispositivos de capa 3) que normalmente no reenvían las tramas de tipo broadcast. Si un dominio de broadcast se hace demasiado grande, debido la cantidad de dispositivos conectados, la red puede sufrir problemas de rendimiento debido a una cantidad elevada de tráfico broadcast.

Para solucionar los problemas de rendimiento se segmenta la LAN separando un dominio de colisión grande en varios de menor tamaño. Esto permite optimizar el ancho de banda ya que en cada dominio de colisión habrá un menor número de hosts que compiten por el acceso al medio compartido. Esta separación es la que se consigue mediante un *bridge*. En una red conmutada con switches, cada puerto representa un dominio de colisión separado si se utiliza una comunicación half-duplex mientras que si se emplea full-duplex no se producen colisiones. Por otro lado, la segmentación también permite acotar los dominios de broadcast separándolos en varios dominios de broadcast de menor tamaño, lo que mejora el rendimiento. Para segmentar los dominios de broadcast se necesitan switches de capa 3 o routers, ya que la segmentación consiste en separar una LAN en múltiples redes de menor tamaño.

Los switches permiten separar una LAN en múltiples dominios de broadcast utilizando VLANs (Virtual LANs). Las VLANs consisten en asignar los puertos del switch a distintos dominios de broadcast generando distintas redes que comparten hardware (véase la figura 3). Un dispositivo conectado a un switch con VLANs sólo podrá conectarse con otros dispositivos asignados a la misma VLAN, es decir, de su mismo dominio de broadcast. Como las VLANs se comportan como redes físicamente separadas, la interconexión de las mismas se hace mediante un router (igual que en el caso se las redes reales).

## Tramas etiquetadas y no etiquetadas

Para interconectar dos switches con varias VLANs configuradas se pueden optar por dos alternativas:

- Establecer un enlace distinto por cada VLAN entre ambos dispositivos: Esta alternativa es poco eficiente, sobre todo cuando el número de VLANs es elevado.
- Establecer un enlace troncal entre ambos dispositivos: Los enlaces troncales pueden transmitir tramas procedentes de varias VLANs gracias al uso de tramas etiquetadas con el identificador de VLAN. De este modo, las distintas VLANs comparten el mismo enlace entre dispositivos.

Para poder establecer enlaces troncales entre dos dispositivos, es necesario que las tramas pertenecientes a una VLAN en el dispositivo de salida sean reconocidas como tramas de dicha VLAN en el dispositivo de destino, ya que la premisa de que las tramas pertenecientes a una VLAN sólo deben reenviarse a dispositivos de la misma VLAN debe seguir cumpliéndose. Para conseguir esto, se utilizan las **tramas etiquetadas** que son la trama original añadiendo datos relativos a la VLAN. Esto permite al switch o router de destino determinar los puertos a los que puede reenviar la trama en función de la VLAN. Existen distintos métodos para etiquetar tramas. Los más utilizados son el IEEE 802.1Q y el ISL (propietario de Cisco). Para interconectar dispositivos de distintos fabricantes se utiliza el IEEE 802.1Q que consiste en una modificación de la trama IEEE 802.3 convencional como se muestra en la figura 4.

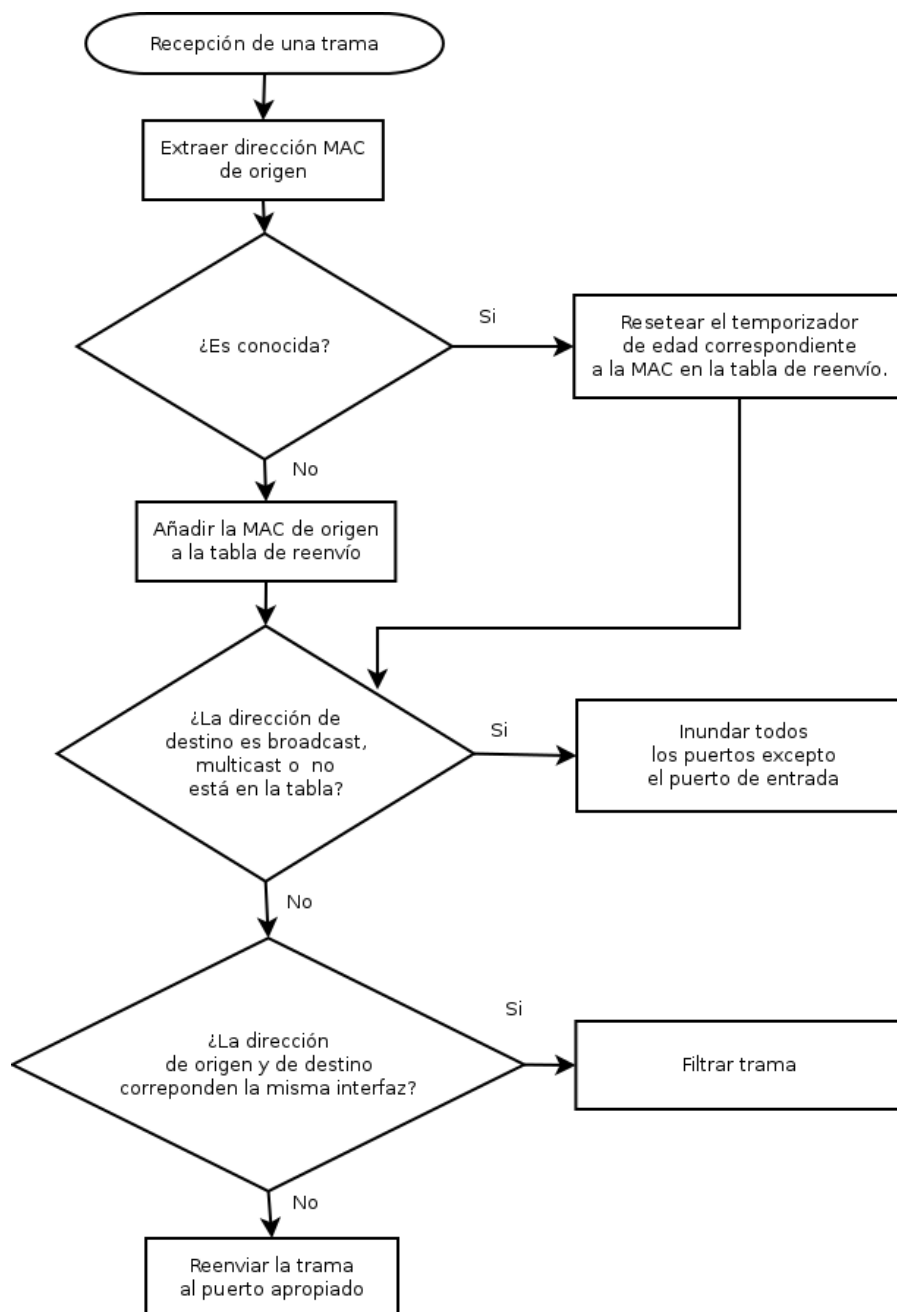


Figura 2: Diagrama de flujo del funcionamiento de un switch.

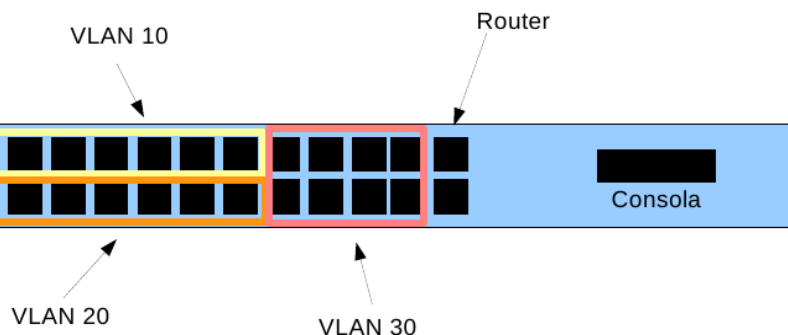


Figura 3: Ejemplo de asignación de puertos a VLANs

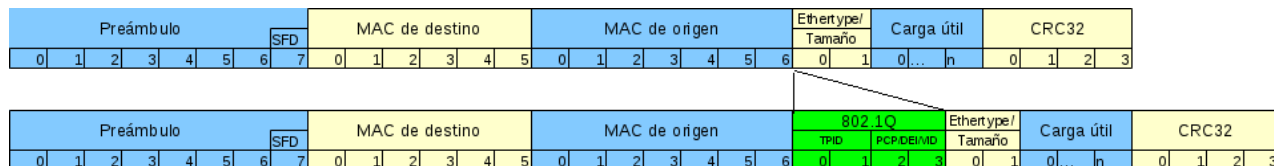


Figura 4: Trama IEEE 802.3 convencional (arriba) y Trama IEEE 802.1Q (abajo)

En la terminología Cisco aquellos enlaces que interconectan dos dispositivos y que, normalmente, transportan tramas etiquetadas se denominan *trunk*. Es importante tener en cuenta que el término *trunk* puede ser ambiguo. Algunos fabricantes lo emplean para denominar los enlaces agregados (conjuntos de enlaces que se hacen aparecer como uno sólo para tener más ancho de banda). Lo importante es recordar por los enlaces troncales deben viajar tramas etiquetadas, ya sea con el estándar IEEE 802.1Q o ISL [1, 2].

Sin embargo existe una excepción a lo expuesto anteriormente, que se produce cuando se define una **VLAN nativa**. Al configurar un *trunk* se puede indicar una VLAN nativa, cuyas tramas viajan a través del enlace sin etiquetar. Al definir una VLAN como nativa en un trunk se ordena al switch que cualquier trama sin etiquetar que entre por el trunk se trate como si fuese de la VLAN a la que se ha designado como nativa. Obviamente, sólo puede existir una VLAN nativa en cada *trunk*.

Hasta el momento, nada se ha dicho sobre los puertos a los que se conectan los dispositivos. Estos puertos se denominan **puertos de acceso** y se caracterizan por que las tramas que entran y salen de los mismos no están etiquetadas. A cada puerto de acceso se le asigna un identificador de VLAN, de modo que cuando una trama sin etiquetar entra en el dispositivo éste puede determinar a qué VLAN pertenece y, por tanto, con qué puertos se puede conmutar. Por supuesto, un puerto de acceso no puede estar en más de una VLAN.

Algunos fabricantes, no aplican la terminología de puertos troncales/acceso, sino que la configuración se realiza indicando si las tramas que van a viajar por ellos son etiquetadas o no etiquetadas (*tagged* o *untagged*).

## Referencias

- [1] Jim Kurose y Keith Ross, Redes de Computadoras. Un enfoque descendente, Addison-Wesley, 5ª Edición.
- [2] Todd Lammle, CCNA Study Guide. Sybex <http://site.ebrary.com/lib/bull/docDetail.action?docID=10131903> (Accedido el 17/12/2014 desde la red interna de la Universidad de La Laguna)

## 1. Introducción al switch TP-Link T2500G-10TS y TP-Link TL-SG3210

Este switch dispone de 10 puertos en total. Ocho de ellos son puertos Gigabit Ethernet por par trenzado y dos son interfaces de fibra óptica.

La primera conexión al switch se hace mediante el cable de consola, utilizando el programa `screen`. La velocidad de la línea será de 38400 baudios.

```
screen /dev/ttyUSB0 38400
```

Una vez se accede a la consola del dispositivo deberemos además entrar en modo privilegiado con el fin de poder configurar el dispositivo. Esto se hace mediante el comando `enable`.

```
T2500G-10TS>enable
```

```
T2500G-10TS#
```

A partir de aquí tenemos acceso a la configuración del dispositivo, pero para realizar cambios en la configuración deberíamos cambiar al modo de configuración.

```
T2500G-10TS#configure
```

```
T2500G-10TS(config)#
```

Para salir de un modo y pasar al modo anterior utilice el comando `exit`.

**En la interfaz de línea de órdenes de este switch la tecla backspace equivale a la tecla de suprimir.**

A continuación se indican brevemente los elementos más importantes y su configuración a través de la interfaz de línea de órdenes.

### 1.1. Resetar la configuración del dispositivo

Para volver a la configuración de fábrica del dispositivo se utiliza el comando `reset`.

```
2500G-10TS#reset
```

### 1.2. Revisar la configuración del dispositivo

Para mostrar la configuración completa del dispositivo se utiliza la orden `show running-config` estando en modo privilegiado.

```
2500G-10TS#show running-config
!T2500G-10TS
#
#
#
#
#
#
mac address-table aging-time 300
#
logging buffer 6
```

```
no logging file flash
#
#
no service password-encryption
#
system-time ntp UTC+08:00 133.100.9.2 139.78.100.163 12
#
#
user name admin privilege admin secret 5 $1$B0B2B>B8G9E6J4J6D2H8D9@=D9H/A>L2$'}./
#
#
port-channel load-balance src-dst-mac
#
#
#
#
#
interface gigabitEthernet 1/0/1
#
interface gigabitEthernet 1/0/2
#
interface gigabitEthernet 1/0/3
#
interface gigabitEthernet 1/0/4
#
interface gigabitEthernet 1/0/5
#
interface gigabitEthernet 1/0/6
#
interface gigabitEthernet 1/0/7
#
interface gigabitEthernet 1/0/8
#
interface gigabitEthernet 1/0/9
    speed 1000
    duplex full
#
interface gigabitEthernet 1/0/10
    speed 1000
    duplex full
#
interface vlan 1
ip address 192.168.0.1 255.255.255.0
#
#
end
```

### 1.3. Guardar la configuración en ejecución

El switch no guarda la configuración en ejecución automáticamente. Esto deberá hacerse mediante el siguiente comando:

```
T2500G-10TS#copy running-config startup-config
Start to save user config.....
```

```
Saving user config OK!
```

```
T2500G-10TS#
```

### 1.4. Fijar el nombre del dispositivo

Como se ha dicho anteriormente, es conveniente fijar un nombre de dispositivo para poder identificarlo cuando se accede de forma remota a través de la red de gestión. Esto se hace desde el modo de configuración mediante el comando `hostname`.

```
T2500G-10TS#configure
```

```
T2500G-10TS(config)#
```

```
T2500G-10TS(config)#hostname S1
```

```
S1(config)#
```

### 1.5. Manejo de interfaces

Para el estado de las distintas interfaces del switch se utiliza el comando `show interface status`.

```
S1#show interface status
```

Port	Status	Speed	Duplex	FlowCtrl	Active-Medium
----	-----	-----	-----	-----	-----
Gi1/0/1	LinkUp	1000M	Full	Disable	Copper
Gi1/0/2	LinkDown	N/A	N/A	N/A	Copper
Gi1/0/3	LinkDown	N/A	N/A	N/A	Copper
Gi1/0/4	LinkDown	N/A	N/A	N/A	Copper
Gi1/0/5	LinkDown	N/A	N/A	N/A	Copper
Gi1/0/6	LinkDown	N/A	N/A	N/A	Copper
Gi1/0/7	LinkDown	N/A	N/A	N/A	Copper
Gi1/0/8	LinkDown	N/A	N/A	N/A	Copper
Gi1/0/9	LinkDown	N/A	N/A	N/A	Fiber
Gi1/0/10	LinkDown	N/A	N/A	N/A	Fiber

Para configurar cualquier aspecto relacionado con una interfaz debemos pasar a modo de configuración y seleccionarla:

```
S1(config)# interface gigabitEthernet 1/0/1
S1(config-if)#
```

Una vez en este modo se pueden modificar los parámetros de la interfaz. Para salir del modo de configuración de interfaz utilice la orden **exit**.

Es posible seleccionar un rango de interfaces para aplicarles la misma configuración mediante **interface range**: Por ejemplo, la siguiente secuencia de comandos selecciona las interfaces de 1 a 5.

```
S1(config)# interface range gigabitEthernet 1/0/1-5
S1(config-if)#
```

## 1.6. Manejo de VLANs

Para mostrar las VLAN, su nombre y los puertos que tienen asociadas se utiliza el comando **show vlan**

```
S1#show vlan
VLAN  Name                Status  Ports
-----
1      Default VLAN          active  Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8
                                           Gi1/0/9, Gi1/0/10
```

```
S1#
```

Para crear una nueva VLAN se debe pasar a modo de configuración y aplicar el comando:

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#exit
```

```
S1#show vlan
VLAN  Name                Status  Ports
-----
1      Default VLAN          active  Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8
                                           Gi1/0/9, Gi1/0/10
99     management          active
```

Con los pasos anteriores se ha creado la VLAN con identificador 99 y se le ha asignado un nombre, en este caso **management**.

Si deseamos eliminar una VLAN sólo tenemos que teclear en modo de configuración:

```
S1(config)#no vlan 10
```

El comando anterior eliminaría la VLAN con identificador 10.



## 1.7. Manejo de la misma configuración para varias interfaces

Al contrario que sucede en los routers, en un switch es posible que se quiera aplicar la misma configuración a varias interfaces. Para ello, la interfaz de comandos nos permite seleccionar un rango de interfaces al que se aplica una configuración. Por ejemplo, en el siguiente comando se seleccionan los puertos del 3 al 7.

```
S1(config)# interface range gi 1/0/3-7
S1(config-if-range)#
```

## 1.8. Añadir puertos a una VLAN

En los switches disponibles en el laboratorio hay que distinguir tres casos:

- T2500G-10TS V1: Sólo permiten puestos de acceso y troncales. Aunque se puede configurar en modo general la funcionalidad está limitada.
- T2500G-10TS V2: Sólo permiten puertos de tipo general.
- TP-Link TL-SG3210: Sólo permiten puertos de tipo general.

Para averiguar el tipo de switch al que estamos conectados podemos hacer uso de la orden `show system-info`.

```
SW1#show system-info
```

```
System Description - JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots
System Name       - SW1
System Location   - SHENZHEN
Contact Information - www.tp-link.com
Hardware Version  - T2500G-10TS 1.0
Software Version  - 1.0.1 Build 20171225 Rel.67244(s)
Bootloader Version - TP-LINK BOOTUTIL(v1.0.0)
Mac Address       - D8-0D-17-8C-02-41
Serial Number     - 218C412000094
System Time       - 2006-01-01 08:01:20
Running Time      - 0 day - 0 hour - 1 min - 26 sec
```

```
SW1#
```

Debemos fijarnos en la versión de hardware y software que indicará el tipo de dispositivo del que se trata.

Antes de comenzar a definir los distintos tipos de puerto debemos definir el concepto de PVID, que no es más que el VID por defecto corresponde a un puerto, siendo el VID el identificador numérico de una VLAN previamente definida.

### 1.8.1. Puertos de acceso

Recordemos que los puertos de acceso son aquellos destinados a conectar dispositivos y, por tanto, transportan tramas sin etiquetar. El comportamiento es el siguiente:

- Cuando se recibe una trama no etiquetada, se etiqueta con la el PVID y se retransmite.
- Cuando se recibe una trama etiquetada cuyo VID coincide con el PVID se retransmite.
- Cuando se recibe una trama no etiquetada cuyo VID no coincide con el PVID se descarta.

- Cuando emite una trama la emite sin etiquetar.

Por ejemplo, para hacer que el puerto Gi1/0/7 sea de acceso perteneciente a la VLAN 10 se utiliza la siguiente secuencia de comandos.

```
S1(config)# interface Gi1/0/7
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# no shutdown
S1(config-if)# end
```

### 1.8.2. Puertos troncales

Los puertos troncales sirven para interconectar switches con switches o switches con routers. Las tramas transmitidas por este tipo de puertos son tramas etiquetadas. El comportamiento es el siguiente:

- Cuando se recibe una trama no etiquetada a través de este puerto se etiqueta con el PVID y se filtra o no en función de la lista de VLAN permitidas para este puerto.
- Cuando se recibe una trama etiquetada a través de este puerto se filtra o no en función de si el VID está en la lista de VLAN permitidas del puerto.
- Cuando se va a emitir una trama etiquetada a través de este puerto sólo se emite si la lista de VLAN permitidas para este puerto. Las tramas emitidas son tramas etiquetadas salvo que el VID coincida con el PVID.

Por ejemplo, para hacer que el puerto Gi1/0/1 sea troncal y permita tramas de las VLAN 10,20 y 99 utilice la siguiente secuencia de comandos:

```
S1(config)# interface Gi1/0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# no shutdown
S1(config-if)# end
```

El PVID fijado para el puerto troncal permite indicar una VLAN para la que se reenvían tramas sin etiquetar. Si por ejemplo configuramos como PVID del puerto la VLAN 10, las tramas correspondientes a esta VLAN se reenvían sin etiquetar y si se recibe una trama sin etiquetar se considera que es de la VLAN 10. Para fijar el PVID de un puerto se utiliza la siguiente secuencia de comandos:

```
S1(config)# interface Gi1/0/1
S1(config-if)# switchport pvid 10
```

Esto se podría haber hecho como parte de la secuencia de comandos anterior. Es importante examinar la configuración de los puertos por si hubieran heredado un PVID por defecto. Si definimos el PVID para un puerto, se dice que la VLAN con este VID es la **VLAN nativa**.

### 1.8.3. Puertos generales

Los puertos de tipo general son una mezcla entre puerto troncal y de acceso. El comportamiento es el siguiente:

- Cuando se recibe una trama no etiquetada a través de este puerto se etiqueta con el PVID y se filtra o no en función de la lista de VLAN permitidas para este puerto.

- Para pasar un puerto a modo general deberá ejecutar el comando:

»”La siguiente secuencia de comandos configura el PVID del puerto a la VLAN 10:

El comportamiento que tenemos es el siguiente: Al haber fijado como PVID del puerto la VLAN 10, tenemos que las tramas no etiquetadas que llegan a este puerto se consideran de la VLAN 10. Además al estar la VLAN 10 en la lista de VLAN permitidas esta trama no se va a filtrar y se va reenviar etiquetándola con el PVID (nótese que al salir del switch esta etiqueta puede ser retirada dependiendo del tipo puerto de salida). Si el

puerto va a emitir una trama de la VLAN 10 esta será no etiquetada tal y como se indicó en la regla de egreso (untagged). Si se recibe una trama etiquetada con el VID 20 ó 99 esta se deja entrar en el switch, ya que está en la lista de VLAN permitidas. Si recibimos una trama etiquetada con un VID de otra VLAN esta se filtra a la entrada del puerto. Por otra parte, si se va a reenviar una trama perteneciente a estas VLANs por este puerto esta se va emitir como trama etiquetada con el VID de la VLAN correspondiente. Es decir que tenemos el comportamiento de un puerto troncal para las VLAN 20, 99 con la VLAN 10. El último paso quita la VLAN 1 (VLAN por defecto) de la lista de puertos permitidos de este puerto.

Para asegurar que el funcionamiento del puerto es el que esperamos es conveniente que revisemos su configuración y revisemos que la lista de VLAN permitidas sea la que deseamos:

```
#show interface switchport gi 1/0/1
Port Gi1/0/1:
PVID: 10
Acceptable frame type: All
Ingress Checking: Enable
Member in LAG: N/A
Link Type: General
Member in VLAN:
Vlan      Name      Egress-rule
----      -
10        N/A      Untagged
20        N/A      Tagged
99        N/A      Tagged
```

Se queremos que se comporte como puerto de acceso puro debemos hacer lo siguiente:

```
S1(config)# interface Gi1/0/1
S1(config-if)# switchport pvid 10
S1(config-if)# switchport general allowed vlan 10 untagged
S1(config-if)# no switchport general allowed vlan 1
S1(config-if)# end
```

Nótese que además hemos retirado el puerto de la VLAN 1 que es la VLAN por defecto. Si revisamos la configuración del puerto debemos ver algo como lo siguiente:

```
#show interface switchport gi 1/0/1
Port Gi1/0/1:
PVID: 10
Acceptable frame type: All
Ingress Checking: Enable
Member in LAG: N/A
Link Type: General
Member in VLAN:
Vlan      Name      Egress-rule
----      -
10        N/A      Untagged
```

En cambio si queremos que se comporte como un puerto troncal puro, hacemos:

```
S1(config)# interface Gi1/0/1
S1(config-if)# switchport pvid 1
```

```
S1(config-if)# switchport general allowed vlan 20, 99 tagged
S1(config-if)# no switchport general allowed vlan 1
S1(config-if)# end
```

```
#show interface switchport gi 1/0/1
Port Gi1/0/1:
PVID: 1
Acceptable frame type: All
Ingress Checking: Enable
Member in LAG: N/A
Link Type: General
Member in VLAN:
Vlan      Name      Egress-rule
----      -
20        N/A      Tagged
99        N/A      Tagged
```

Al igual que en el caso anterior hemos quitado el puerto de la VLAN por defecto.

## 1.9. VLAN de gestión

Como se vio en la práctica 1, es conveniente que los dispositivos puedan accederse de manera remota. Para ello es necesario que tengan activa una interfaz de gestión que pertenezca a una VLAN de gestión. Para configurar la VLAN de gestión se usa el comando `ip management-vlan`<sup>1</sup> y se indica el identificador de la VLAN de gestión. Además debemos asignar la dirección IP a la interfaz de gestión dentro de esta VLAN, como se muestra en el ejemplo:

```
S2(config)#ip management-vlan 99

S1(config)#interface vlan 99

S1(config-if)#ip address 10.10.10.3 255.255.255.0
```

En el modelo T2500G-10TS V1 además se obliga a que exista un puerto con el PVID de la vlan que se configure como VLAN de gestión. Por ello, conviene hacer la VLAN de gestión la VLAN nativa de los puertos troncales.

## 2. Enrutamiento entre VLANs con routers MikroTik

Para que exista conectividad entre la VLAN los paquetes deberían pasar por un router, ya que están cambiando de red. Para que el router pueda recibir paquetes de ambas VLANs deberá tener asignada una dirección en cada una de ellas. Utilizaremos la interfaz `ether1` para conectar con el switch y crearemos dos interfaces virtuales dependientes de `ether1`, una en cada VLAN:

```
[admin@MikroTik] > interface vlan add interface=ether1 name=ether1.10 vlan-id=10
[admin@MikroTik] > interface vlan add interface=ether1 name=ether1.20 vlan-id=20
[admin@MikroTik] > interface vlan add interface=ether1 name=ether1.99 vlan-id=99
```

<sup>1</sup>Este comando se utiliza cuando el switch sólo permite acceder a la configuración por una única VLAN como es el caso de los T2500G-10TS. En los switches que permiten una interfaz de gestión por VLAN como el TP-Link TL-SG3210 no es necesario ejecutarlo. Se configura directamente la interfaz en la VLAN correspondiente.

El argumento `vlan-id` indica el identificador de VLAN a esperar y el argumento `name` es un nombre que utilizaremos para identificar la interfaz virtual en procesos de configuración posteriores. Una buena práctica es asignar a la interfaz virtual el nombre de la interfaz física de la que depende y añadir el identificador de VLAN. De este modo, se sabe inmediatamente a qué interfaz física y VLAN corresponde.

Asigne la dirección al router dentro de cada una de las interfaces virtuales dentro de su VLAN:

```
[admin@MikroTik] > ip address add address=192.168.0.1/24 interface=ether1.10  
[admin@MikroTik] > ip address add address=192.168.1.1/24 interface=ether1.20  
[admin@MikroTik] > ip address add address=10.10.10.1/24 interface=ether1.99
```

Tenga en cuenta que estas son las direcciones deben asignarse como puerta de enlace en los PCs pertenecientes a las respectivas redes.

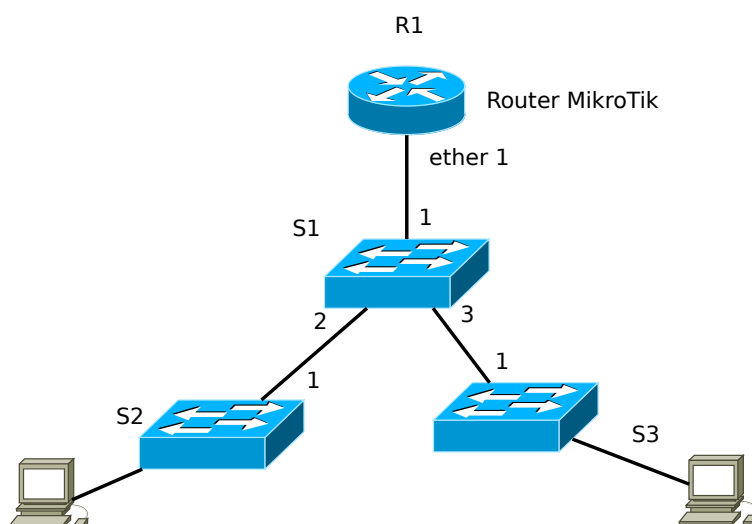


Figura 5: Topología física.

## Tareas a realizar en el laboratorio

1. Verifique revisando la parte frontal de los switches el modelo que está usando en cada caso. Para saber si está usando la versión 1 o la versión 2 de los switches TP-Link T2500G-10TS deberá revisar la etiqueta de la parte inferior del dispositivo. Esto es importante porque, tal y como se ha indicado anteriormente, las configuraciones que se pueden realizar difieren de un modelo a otro.
2. Limpie la configuración de todos los dispositivos que vaya a utilizar.
3. Realice la conexión de cableado que se indica en la figura 5. Anote los identificadores de los puertos y sus conexiones.
4. Deberán crearse 3 VLANs en cada uno de ellos, utilizando los identificadores indicados en la tabla 1.

VLAN	Nombre	Red
10	alumnos	192.168.0.0/24
20	profesores	192.168.1.0/24
99	gestion	10.10.10.0/24

Tabla 1: Nombres, identificadores y números de red de las VLANs.

5. En los switches de acceso (S2 y S3) para que acepten tramas no etiquetadas de las VLAN que se indican a continuación.
- S2: 4-5 VLAN 10, 6-7 VLAN 20
  - S3: 4-5 VLAN 10, 6-7 VLAN 20

6. Configure los puertos 1-3 para que retransmitan tramas etiquetadas de las VLAN 10,20 y tramas no etiquetadas de la VLAN 99.

7. Configure la VLAN 99 como VLAN de gestión en los 3 switches. A continuación añada el puerto 8 a la VLAN 99 para que se pueda conectar un PC. Compruebe que es posible acceder a la configuración de los tres switches mediante telnet. Recuerde que el PC deberá estar en la red 10.10.10.0/24.

Es importante asegurarse de que la configuración por defecto de la VLAN administrativa no tiene asignada una dirección del rango que vayamos a utilizar para otro propósito.

8. Retire los puertos de la VLAN por defecto. En estos dispositivos, la VLAN por defecto es la VLAN 1. Esto lo podemos comprobar visualizando las VLAN a las que pertenecen cada uno de los puertos:

```
S2#show vlan
```

VLAN	Name	Status	Ports
1	System-VLAN	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9, Gi1/0/10
10	N/A	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5
20	N/A	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/6, Gi1/0/7
99	N/A	active	Gi1/0/1, Gi1/0/2, Gi1/0/3

Observe como aunque se hayan reasignado puertos a otra VLAN estos puede que sigan perteneciendo a la VLAN 1. Para evitarlo vamos a retirar los puertos de esta VLAN:

```
S1(config)# interface range gi 1/0/1-7
```

```
S1(config-if-range)# no switchport general allowed vlan 1
```

A continuación, compruebe que los puertos indicados ya no pertenecen a la VLAN 1.

```
S2#show vlan
```

VLAN	Name	Status	Ports
1	System-VLAN	active	Gi1/0/8, Gi1/0/9, Gi1/0/10
10	N/A	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5
20	N/A	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/6, Gi1/0/7
99	N/A	active	Gi1/0/1, Gi1/0/2, Gi1/0/3

Asegúrese de retirar de la VLAN por defecto los puertos que vaya a usar en cada dispositivo.

9. Conecte un PC al puerto 4 de S2 y otro al puerto 5 de S3 (ambos perteneces a la VLAN 10). Añada ambos PCs a la red 192.168.0.0/24 ¿Se puede conectar?



10. Conecte un PC al puerto 6 de S2 y otro al puerto 7 de S3 (ambos pertenecen a la VLAN 20). No modifique la configuración de red de los PC ¿Se puede conectar?
11. Conecte un PC al puerto 4 de S2 y otro al puerto 6 de S3. No modifique la configuración de red de los PC ¿Se puede conectar? ¿por qué?
12. Con lo realizado hasta el momento, no se pueden interconectar dispositivos de distintas VLANs. Para ello, como se ha dicho anteriormente, se necesita un router. Configure ahora el router para que haga el enrutamiento entre las 3 VLANs. Sitúe un PC en cada VLAN y compruebe si puede conectar con el PC de la otra VLAN (Recuerde configurar correctamente direcciones y las puertas de enlace de los PCs).