

# Configuración VLANs (Virtual Local Area Networks)

## PREPARACIÓN DE LA PRÁCTICA

Antes de empezar la práctica seguid las indicaciones siguientes:

→ Aseguraos de que habeis arrancado la partición “PRÁCTICA RDC LOCAL”.

→ Cada grupo debe tener asignados o a su disposición:

- 2 switches (conocer su dirección IP y ubicación en el armario).
- 4 PC (identificar su conector en el panel de conexiones ubicado en el armario).
- 4 cables Ethernet directos para conectar cada PC a alguno de los switches.
- 1 cables Ethernet cruzado para interconectar los dos switches.

→ En esta práctica trabajaremos con la interfaz eth1 (cable amarillo) que da acceso a la red interna del laboratorio. Tras conectar los cables, aseguraos de que está activada la conexión “DCLAN eth1-Estática” en el “Network Manager” (icono en el panel superior) y que tenéis asignada una dirección en el rango 192.168.0.0/24 para la interfaz eth1 (se puede comprobar con *ifconfig*).

→ Conectad un PC a la boca nº 1 de uno de los switches y reinicializadlo a los valores de fábrica:

- a) Desde un terminal: telnet <dir\_IP\_switch> (login/password=security/security)
- b) En el menú del switch: Root menu – System – Initialize

Detectaremos que se ha reinicializado porque se pierde la conexión telnet.

Repetid la operación de reinicialización con el otro switch.

## 1. Introducción

Una VLAN (Virtual Local Area Network) o red virtual nos permite segmentar una red Ethernet en varios dominios de broadcast totalmente aislados, de manera que para que los nodos que forman una VLAN se comuniquen con los que forman otra VLAN diferente, los paquetes tienen que atravesar uno o más routers. Las VLANs nos permiten segmentar la red sin ninguna restricción física.

Las ventajas que nos pueden aportar las VLANs son entre otras:

- Proporcionan una segmentación de la red flexible (escalabilidad).
- Es muy fácil cambiar y mover dispositivos en la red (mejor gestión de recursos).
- Facilidad de encontrar y aislar averías.
- Proporcionan seguridad extra (los dispositivos sólo pueden comunicarse directamente con otros dispositivos que están en la misma VLAN).
- Control de tráfico de broadcast.
- Separación de protocolos.

### 802.1Q (VLAN Tagging)

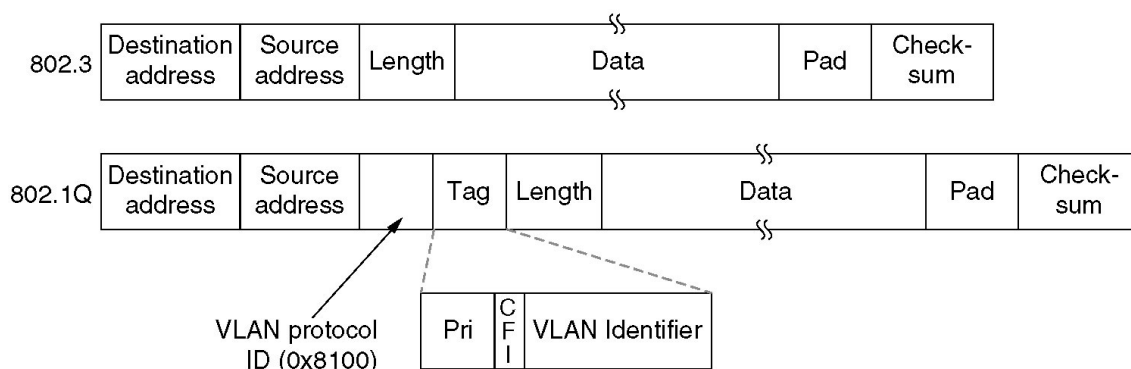
El protocolo más utilizado actualmente para implementar las VLANs es el **IEEE 802.1Q**. IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de IEEE para proveer de un protocolo multi-fabricante que permitiese multiplexar varias VLANs sobre un mismo enlace (*Trunk*). Posteriormente se convirtió en el nombre del estándar definido en ese proyecto que define el protocolo de encapsulamiento usado para implementar VLANs en redes Ethernet.

Permite identificar a una trama como proveniente de un equipo conectado a una red determinada. Una trama perteneciente a una VLAN sólo se va a distribuir a los equipos que pertenezcan a su misma VLAN, por lo que:

- Separamos dominios de difusión
- Separamos usuarios

### Formato de la trama

802.1Q no encapsula la trama original Ethernet sino que añade 4 bytes al encabezado original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.



Formatos de trama 802.3 (tradicional) y 802.1Q

La VLAN tag se inserta en la trama Ethernet entre el campo Source MAC Address y el campo Length. Los primeros 2 bytes del VLAN tag consisten en el "Tag Type" (tipo de tag) de 802.1Q y siempre está puesto a 0x8100. Los últimos 2 bytes contienen la siguiente información:

- Los primeros 3 bits son el campo User Priority Field que pueden ser usados para asignar un nivel de prioridad.
- El próximo bit es el campo Canonical Format Indicator (CFI) usado para indicar la presencia de un campo Routing Information Field (RIF).
- Los restantes 12 bits son el VLAN Identifier (VID), que identifica de forma única a la VLAN a la cual pertenece la trama Ethernet.

Con el agregado del VLAN tag, el estándar 802.3ac permitió que la longitud máxima de la trama Ethernet fuese extendida de 1518 a 1522 bytes.

### **“VLAN por defecto” y VLAN de administración**

Para permitir la compatibilidad con hardware sin soporte 802.1Q, el estándar define que por cada puerto existirá una VLAN por defecto a la que será asignada cualquier trama que llegue sin etiquetar. Así mismo, el tráfico perteneciente a la “VLAN por defecto” de cada puerto será enviado sin etiquetar, en formato Ethernet<sup>1</sup>.

Los fabricantes generalmente distribuyen sus equipos con el ID 1 preconfigurado como “VLAN por defecto” para todos los puertos. Esto quiere decir que, inicialmente, todos los puertos del switch pertenecen a la VLAN 1. Es posible reasignar el ID de la “VLAN por defecto” de un puerto. Este cambio de configuración permitirá vincular los equipos conectados en determinados puertos a diferentes VLAN, de acuerdo con la política de gestión de la red que pretenda establecer el administrador. Además es posible asignar más de una VLAN a un único puerto.

Es una buena práctica definir una VLAN propia para administración de la red, que nos permita aislar la configuración de los dispositivos del resto de tráfico. Idealmente, solo el administrador y los dispositivos de conmutación deben formar parte de la VLAN de administración. En despliegues reales, se recomienda que la VLAN de administración difiera de la “VLAN por defecto”, ya que si coinciden, cualquier dispositivo conectado a un puerto sin configurar tendrá acceso a toda la VLAN de administración. Para ello, el administrador puede, por ejemplo, definir un puerto de cada dispositivo de la red como perteneciente a una única VLAN que se utilizará para administración.

### **Configuración en los switches**

Aunque el estándar no hace diferencia, muchos fabricantes definen dos tipos de puertos:

#### **1. Puertos de acceso:**

- Son aquellos en los que tan solo se ha definido la VLAN por defecto (solo una VLAN).
- Se suelen conectar a dispositivos no 802.1Q.
- Mapean el puerto a una única VLAN programada.
- A las tramas entrantes se les añade el TAG 802.1Q.
- A las tramas salientes se les quita el TAG 802.1Q (en caso de llevarlo).

#### **2. Puertos 802.1Q Trunk (o *tagged*):**

- Tienen más de una VLAN definida.
- Se utilizan para conectar switches entre si y que pueda pasar la información de diferentes VLANs a través de ellos.
- Las tramas entrantes y salientes llevan el Tag 802.1Q.

---

<sup>1</sup> Algunos fabricantes (principalmente CISCO) se refieren a la “VLAN por defecto” como “VLAN nativa”. Sin embargo, el estándar no menciona el término “nativa”.

## 2. Objetivos y organización de la práctica

El aula dispone de una serie de switches para la realización de la práctica. El objetivo consistirá en administrar las VLANs que crearemos en dichos switches, y ver cómo funciona la comunicación entre equipos de una misma VLAN y entre equipos de VLANs diferentes. También efectuaremos algunas capturas de tráfico para comprobar el alcance de las difusiones dependiendo de la VLAN donde se efectúen.

La práctica se estructura en las siguientes secciones:

**Parte 1. Creación de las VLANs.** Crearemos 2 redes virtuales (VLANs) con 2 puertos asignados en cada una. Esto lo haremos en dos switches.

**Parte 2. Comunicación intra-switch.** Averiguaremos si los equipos conectados a un mismo switch pueden comunicar entre ellos, primero en el caso de pertenecer a la misma VLAN y luego en caso de pertenecer VLANs diferentes.

**Parte 3. Comunicación inter-switch.** Comprobaremos la conectividad entre equipos conectados a diferentes switches. Veremos cómo configurar el puerto que une los switches como puerto *tagged* (deben ser puertos 802.1q) y cómo indicar las VLANs que se le asignan.

**Parte 4. Comprobar la separación de dominios de difusión que ofrecen las VLANs.** Para conseguir este objetivo, un PC de una VLAN llevará a cabo la captura de tramas<sup>2</sup> mientras desde otro equipo se lanza la difusión<sup>3</sup>. Ambos equipos podrán estar conectados al mismo o diferente switch y pertenecer a la misma o diferente VLAN.

**Parte 5. Administración de un switch a través de una VLAN de administración.** Comprobaremos que, si no tomamos las precauciones necesarias, es posible administrar uno de nuestros switches remotamente desde un puerto en el que no se ha definido explícitamente ninguna VLAN.

Para optimizar el uso de recursos del laboratorio cada grupo trabajará con 2 switches y 4 ordenadores con los propósitos siguientes:

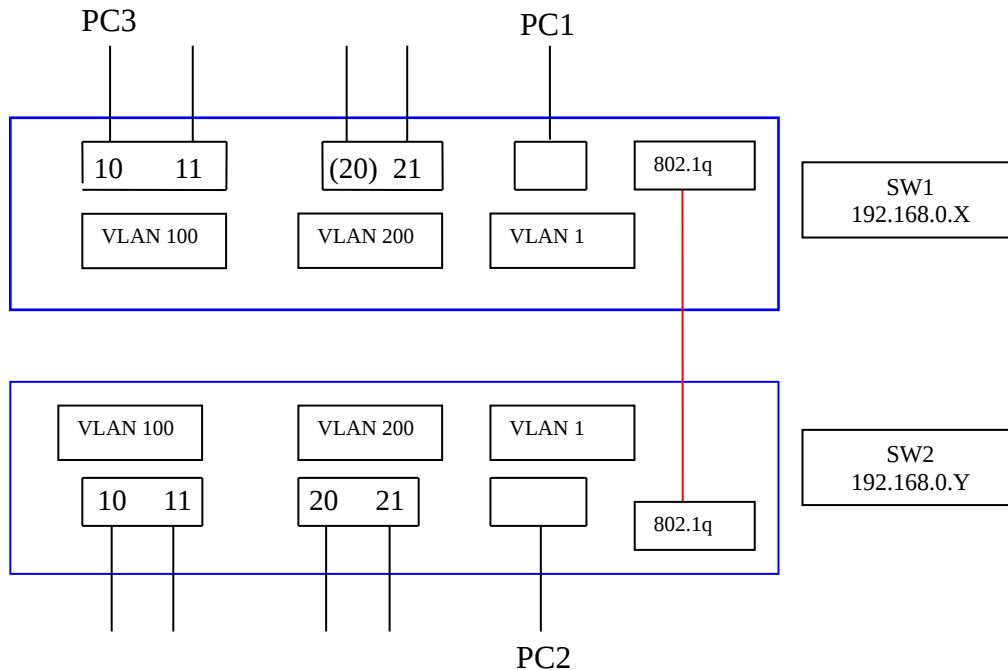
- SW1 y SW2: En ambos crearemos las VLAN-100 y VLAN-200
- PC1: Administración VLAN-100
- PC2: Administración VLAN-200
- PC3: Pruebas de comunicación. Conectado al puerto 10 de la VLAN-100
- PC4: Pruebas de comunicación. Se conectará a diferentes puertos y VLANs dependiendo del ejercicio en curso.

La figura siguiente muestra el esquema de dispositivos y conexiones propuesto:

---

<sup>2</sup> Se puede realizar la captura de tramas mediante la orden `tcpdump` o algún analizador de protocolos, por ejemplo Wireshark.

<sup>3</sup> Se pueden generar mensajes broadcast mediante la orden `ping` o la utilidad NMAP (disponible en [www.insecure.org](http://www.insecure.org) o en el repositorio de una distribución Linux).



Se propondrá comprobar la comunicación en los siguientes casos:

- **Parte 2:** PC3 – PC4(SW1,Port-11)  
PC3 – PC4(SW1,Port-20)
- **Parte 3:** PC3 – PC4(SW2,Port-10)  
PC3 – PC4(SW2,Port-20)

### 3. Implementación de la práctica

Como es habitual en la mayoría de switches, la VLAN 1 viene ya creada por defecto (VLAN ID 1 y Local ID 1) y a ella están asignados todos los puertos del switch.

En el armario de red del laboratorio, conectad un cable directo de PC1 a SW1. Conectad también PC2 a SW2. Durante toda la práctica administraremos las VLANs del SW1 desde PC1 y las del SW2 desde PC2.

#### Preparación

La configuración de los switches se hará a través de telnet (security/security)<sup>4</sup>. Cuando nos conectemos a alguno de los switches se nos presentará el menu principal con sus opciones. Si no lo hemos hecho antes, debemos reinicializar el dispositivo para borrar posibles configuraciones anteriores mediante las opciones “system – initialize”.

<sup>4</sup> Alternativamente, la mayoría de switches ofrecen una interfaz web para ser administrados (acceso típico con [http://dirección\\_IP\\_Switch](http://dirección_IP_Switch)). No obstante, desaconsejamos el uso de dicha interfaz en los modelos del laboratorio por tener deficiencias en el manejo de las VLANs.

En “bridge - vlan” encontraremos las opciones propias de la gestión de VLANs como crear, borrar o modificar una VLAN, añadir y eliminar puertos de la VLAN y mostrar información de su configuración (ver figura).

```

C:\ Telnet 158.42.180.59
multicastfiltering - Administer multicast filtering
port - Administer bridge ports
stpForwardDelay - Set the bridge Spanning Tree forward delay
stpHelloTime - Set the bridge Spanning Tree hello timer
stpMaxAge - Set the bridge Spanning Tree maximum age
stpPriority - Set the Spanning Tree bridge Priority
stpState - Enable/Disable Spanning Tree on a bridge
vlan - Administer VLANs

Type "q" to return to the previous menu or ? for help.
-----smer-01 (1)-----
Select menu option (bridge): vlan

Menu options: -----3Com SuperStack II Switch 1100-----
addPort - Add a port to a VLAN
create - Create a VLAN
delete - Delete a VLAN
detail - Display detail information
modify - Modify a VLAN
removePort - Remove a port from a VLAN
summary - Display summary information

Type "q" to return to the previous menu or ? for help.
-----smer-01 (1)-----
Select menu option (bridge/vlan):

```

## Parte 1. Creación de VLANs

Una VLAN se define mediante:

- VLAN Name: nombre descriptivo para la VLAN (ventas, contabilidad, etc.)
- VLAN ID: identificador de la VLAN creada.
- Local ID: identifica la VLAN localmente en la pila

### 1.1. Crear las VLANs

Creamos 2 VLANs en el switch SW1 con ID 100 y 200, y nombre VLAN 100 y VLAN 200, respectivamente. El Local ID no lo utilizaremos (poned el valor sugerido a continuación). Teclead la opción “create”

```

Enter VLAN ID (2-4094) [2]: 100
Enter Local ID (2-16): 4
Enter VLAN Name [VLAN 200]: VLAN 100

```

```

Enter VLAN ID (2-4094) [2]: 200
Enter Local ID (2-16): 5
Enter VLAN Name [VLAN 300]: VLAN 200

```

### 1.2. Añadir puertos del swicth a cada VLAN

Añadiremos los puertos 10 y 11 a VLAN 100, y los puertos 20 y 21 a VLAN 200. Estos seran los puertos de acceso, donde conectaremos los puestos de trabajo que usaremos en las pruebas de comunicación, por lo que no deben ser configurados como *tagged*. Teclear la opción “addPort”

```

Select VLAN ID (1-4094) [1]: 100
Select Ethernet port (1-14, all): 10
Enter tag type (none, 802.1Q) [802.1Q]: none

```

### 1.3. Mostrar la información de las VLANs

Comprobad los valores introducidos con la opción “detail”. La opción “summary” muestra lo mismo excepto los puertos.

### 1.4. Configurar el switch SW2

Repetid los pasos anteriores sobre SW2 para crear en este las mismas VLANs.

## Parte 2. Comunicación intra-switch

Ahora pasaremos a comprobar la conectividad entre equipos de un mismo switch dependiendo de si pertenecen o no a la misma VLAN.

Conectad un cable directo desde los puestos de trabajo PC3 y PC4 a los puertos de acceso de VLAN 100 de SW1.

Hacer ping desde PC3 a PC4 ¿Hay comunicación? ¿Porqué?

Cambiad el cable de PC4 al puerto 20.

Hacer ping desde PC3 a PC4 ¿Hay comunicación? ¿Por qué?

Hacer ping desde PC3 a PC1 ¿Hay comunicación? ¿Por qué?

Haced los cambios necesarios en la configuración de las VLANs para pasar el puerto 20 de VLAN 200 a VLAN 100 y mostrad por pantalla información actualizada de ambas VLANs para comprobar que se ha reasignado correctamente el puerto.

Hacer ping desde PC3 a PC4 ¿Hay comunicación? ¿Porqué?

## Parte 3. Comunicación inter-switch

En esta sección el objetivo será ver si se comunican equipos que están conectados en diferentes switches.

Conectad los dos switches SW1 y SW2 con un cable cruzado. Este será el *trunk* entre ambos dispositivos.

3.1 Configurar los puertos que unen ambos switches como de tipo 802.1Q (puertos *tagged*) para que acepten tramas de las VLAN 100 y VLAN 200. Para añadir una VLAN podemos hacerlo a semejanza de como se indicó en el punto 1.2, o bien directamente con una única orden

Sintaxis: `bridge vlan addport <VLAN ID> <Num_Puerto> 802.1Q`

Ejemplo: `bridge vlan addport 100 24 802.1Q`

3.2 Comprobad que los cambios han sido realizados mostrando la información de las VLANs en pantalla.

Conectad el cable de PC4 de manera adecuada para poder llevar a cabo las comprobaciones siguientes.

3.3 Hacer un ping de un equipo conectado a una VLAN de un switch a otro equipo conectado a la misma VLAN de otro Switch. ¿Hay comunicación?

3.4 Hacer un ping de un equipo conectado a una VLAN de un switch a otro equipo conectado a una VLAN diferente de otro Switch. ¿Hay comunicación?

#### **Parte 4. Comprobar la separación de dominios de difusión que ofrecen las VLANs**

Ahora comprobaremos el aislamiento de *tormentas broadcast* que ofrecen las VLANs. Para generar la difusiones podemos utilizar, por ejemplo, la orden ping con la opción -b que permite enviar *echo request* a todas las máquinas de una red

```
ping -b 192.168.0.255
```

Para ello, haremos que PC3 ejecute la orden anterior mientras en PC4 hacemos una captura de tramas

```
tcpdump -i eth1
```

en los casos en que: a) ambos equipos pertenecen a la misma VLAN en switches diferentes; y b) los equipos pertenecen a VLANs diferentes estando conectados al mismo switch.

#### **Parte 5. Administración de un switch a través de una VLAN de administración.**

Finalmente, comprobaremos si es posible administrar un switch desde un equipo no conectado a este switch.

*Nota: Los switches del laboratorio solo aceptan ser configurados desde la VLAN 1.*

Desconectad el cable de PC1 de SW1. A partir de este momento ya no podremos administrar este switch desde PC1.

Intentad conectar mediante telnet desde PC2 a SW1. ¿Es posible? ¿Atraviesan las tramas de PC2 el enlace trunk? Comprobadlo mediante la opción “detail” del menú. Cambiad la configuración del enlace trunk para que el SW1 no sea configurable desde PC2.

Proponed una configuración que permita que solo el administrador de la red tenga acceso para configurar los switches.

**Y para terminar una última pregunta... En la presente sesión hemos comprobado que no hay conectividad entre dos PCs pertenecientes a diferentes VLANs. Sin embargo, en la práctica hay muchos casos en que dicha conectividad si que es posible y necesaria, por ejemplo, al conectarse al servidor web de la ETSINF desde el navegador de una aula informática de la propia ETSINF ¿Cómo crees que se implementa esta solución?**



## 4. Anexo

Se adjunta la estructura de menús de la interface de línea de comandos del Switch:

