Configuración de VLANs (Virtual Local Area Networks)

GII - ETSINF - UPV

14 de marzo de 2023

Índice

Preparación de la práctica

Antes de empezar la práctica seguid las indicaciones siguientes:

1. Cada grupo debe tener asignados o a su disposición:
   - 2 Switches (conocer su dirección IP y ubicación en el armario).
   - 4 PCs (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 cable Ethernet cruzado para interconectar los dos switches.
2. En esta práctica trabajaremos con la interfaz eno1 (cable amarillo) que da acceso a la red interna del laboratorio. Tras conectar los cables, aseguraos de que está activada la conexión "eno1" 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 eno1 (se puede comprobar con *ip addr*).

   ¡Advertencia! La conexión sólo estará disponible cuando el adaptador PC detecta la red, es decir, cuando se conecta el cable. Además, cada vez que desconecte o vuelva a conectar el cable, es posible que deba volver a seleccionar la conexión.
3. Conecte uno de los PC a cualquiera de los switches y reinícielo a los valores predeterminados:
   a) En una terminal: telnet <dir_IP_switch>(login/password=security/security)
   b) En el menú del switch: *Root menu – System – Initialize*
4. Notará que el switch se ha reiniciado porque la conexión telnet se ha roto.
5. Repita los pasos anteriores para restablecer 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 VLAN nos permiten segmentar la red sin ninguna restricción física.

Las ventajas que nos pueden aportar las VLAN 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.

1.1. 802.1Q (VLAN Tagging)

El protocolo más utilizado actualmente para implementar las VLAN 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 VLAN 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 VLAN en redes Ethernet.

El uso de etiquetas VLAN permite vincular una trama 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 tanto los usuarios como los dominios de difusión.

1.2. 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 (ver figura 1).

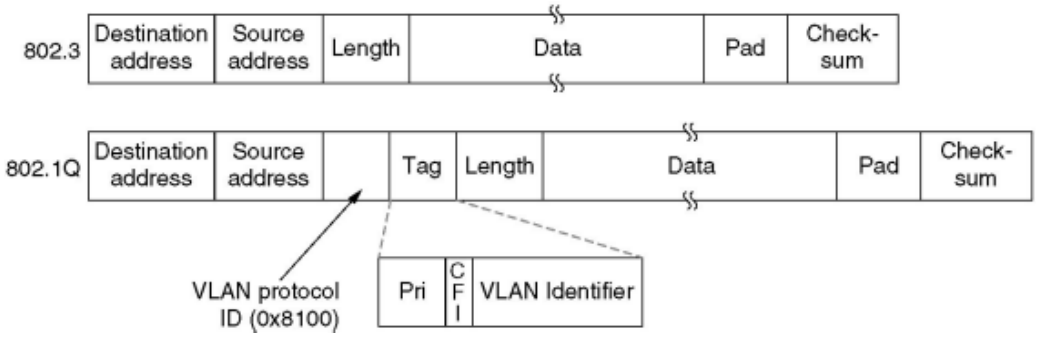

Figura 1: Formato de trama Ethernet y 802.1Q.

La VLAN tag se inserta en la trama Ethernet entre los campos *Source MAC Address* y *Length*. Los primeros 2 bytes del VLAN tag consisten en el *Tag Type* 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.

1.3. "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. Algunos fabricantes (principalmente CISCO) se refieren a la "VLAN por defecto" como "VLAN nativa". Sin embargo, el estándar no menciona el término nativa en ningún momento. El *VLAN ID* por defecto es definido por el administrador de la red.

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 la VLAN que se utilizará para administración.

1.4. Configuración de los switches

Aunque el estándar no los distingue, muchos fabricantes definen dos tipos de puertos:

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).

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 VLAN a través de ellos.
- Las tramas entrantes y salientes llevan el Tag 802.1Q.

2. Organización de la práctica

El aula dispone de una serie de switches para la realización de la práctica. El objetivo consistirá en administrar las VLAN que crearemos en dichos switches, y ver cómo funciona la comunicación entre equipos de una misma VLAN, y entre equipos de VLAN 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:

1. **Creación de las VLAN.** Crearemos 2 redes virtuales (VLAN) con 2 puertos asignados en cada una. Esto lo haremos en ambos switches.
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 VLAN diferentes.

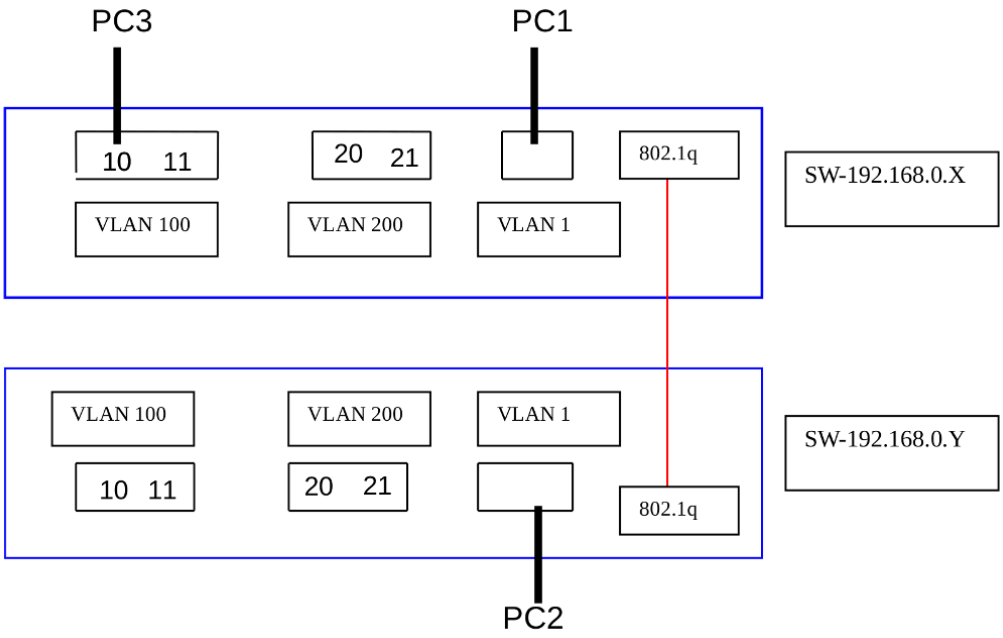

Figura 2: Esquema propuesto para las conexiones entre dispositivos.

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 VLAN que se le asignan.
4. **Comprobar la separación de dominios de difusión que ofrecen las VLAN.** Para conseguir este objetivo, un PC de una VLAN llevará a cabo la captura de tramas[1] mientras desde otro equipo se lanza la difusión[2]. Ambos equipos podrán estar conectados al mismo o diferente switch y pertenecer a la misma o diferente VLAN. Verifica todos los escenarios: (i) ambos PCs conectados al mismo switch, (ii) a diferentes switches, (iii) a la misma VLAN, y (iv) a diferentes VLAN.
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 mayor claridad 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 VLAN dependiendo del ejercicio en curso.

La figura 2 muestra el esquema de dispositivos y conexiones propuesto:
Se propondrá comprobar la comunicación en los siguientes casos:

- PC3-PC4(SW1, Port-11)
- PC3-PC4(SW1, Port-20)
- PC3-PC4(SW2, Port-10)
- PC3-PC4(SW2, Port-20)

[1] Se puede realizar la captura de tramas mediante la orden tcpdump o algún analizador de protocolos, por ejemplo Wireshark.
[2] Se pueden generar mensajes broadcast mediante la orden ping o la utilidad NMAP (disponible en www.insecure.org o en el repositorio de una distribución Linux).

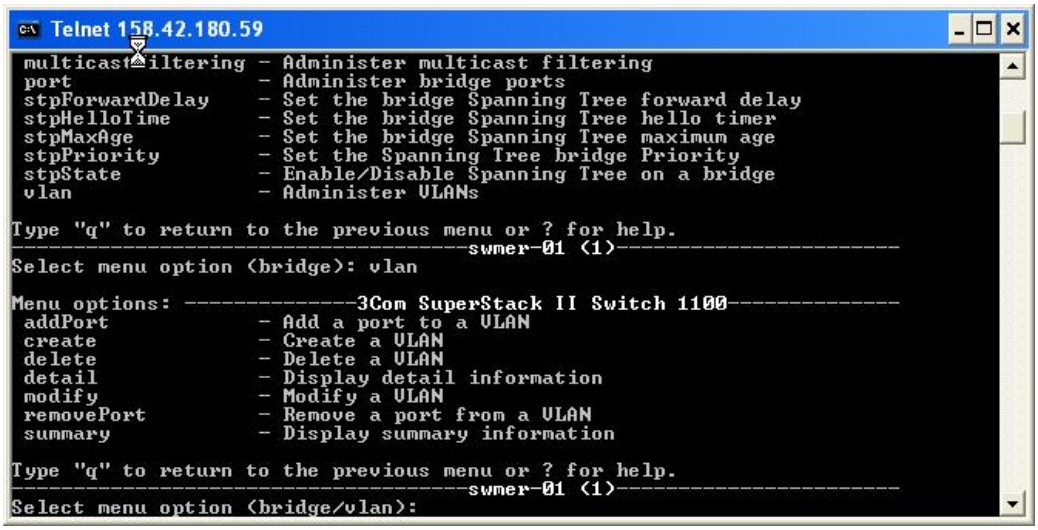

Figura 3: Menú VLAN del switch.

3. Implementación

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

En el armario de red del laboratorio, conectad un cable directo desde un PC (lo llamaremos PC1) a la boca nº 1 de uno de vuestros switches (SW1). Conectad también otro PC (PC2) al otro switch (SW2). Durante toda la práctica administraremos las VLAN del SW1 desde PC1 y las del SW2 desde PC2.

Preparación

La configuración de los switches se hará con telnet (login/password=security/security)[3]. Cuando nos conectemos a alguno de ellos se nos presentará el menu principal con sus opciones. Si no lo has hecho antes, reinicializa SW1 y SW2 para cargar los valores de fábrica y borrar así posibles configuraciones anteriores mediante la opción "system→initialize".

En "bridge→vlan" encontraremos las opciones propias de la gestión de VLAN, como crear, borrar o modificar una VLAN, añadir y eliminar puertos de la VLAN, y mostrar información de su configuración (ver figura 3).

Part 1. Creación y configuración 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.

Crea las VLANs

Creamos 2 VLAN 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). Teclea la opción "create" y sigue los siguientes pasos:

[3]También se puede usar la interfaz web, pero es inestable y no la recomendamos.

```
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
```

Añadir puertos del switch a cada VLAN

Añade los puertos 10 y 11 a VLAN 100, y los puertos 20 y 21 a VLAN 200. Estos serán 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*. Teclea la opción "addPort" y sigue los siguientes pasos:

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

Comprobar la configuración

Comprobad los valores introducidos con la opción "detail". La opción "summary" muestra lo mismo excepto los datos relativos a los puertos.

Configurar el switch SW2

Repite los pasos anteriores sobre SW2 para crear en éste las mismas VLAN.

Parte 2. Comunicación intra-switch

Ahora pasaremos a comprobar la conectividad entre equipos de un mismo switch dependiendo de si pertenecen a la misma VLAN (caso 1) o no (caso 2).

1. Conecta un cable directo desde los puestos de trabajo PC3 y PC4 a los puertos de acceso de VLAN 100 de SW1.
2. Hacer ping desde PC3 a PC4 ¿Hay comunicación? ¿Por qué?
3. Cambiad el cable de PC4 al puerto 20 del switch SW1.
4. Hacer ping desde PC3 a PC4 ¿Hay comunicación? ¿Por qué?
5. Hacer ping desde PC3 a PC1 ¿Hay comunicación? ¿Por qué?
6. Averiguad y haced los cambios necesarios en la configuración de las VLAN para pasar el puerto 20 de VLAN 200 a VLAN 100. Mostrad por pantalla información actualizada de ambas VLAN para comprobar que se ha reasignado correctamente el puerto.
7. 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. Sigue los siguientes pasos:

1. Conecta los dos switches SW1 y SW2 con un cable cruzado. Este será el trunk entre ambos dispositivos.
2. Configura 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 directamente con una única orden:

```
Syntax:   bridge vlan addport <VLAN ID> <Num_Puerto> 802.1Q
Example:  bridge vlan addport 100 24 802.1Q
```

3. Agrega ambas VLAN al puerto 24 en ambos switches.
4. Comprueba la configuración.
5. Conecta el cable de PC4 de manera adecuada para poder llevar a cabo las comprobaciones siguientes.
   a) 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?
   b) 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 VLAN

Ahora comprobaremos el aislamiento de tormentas broadcast que ofrecen las VLAN. 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.

1. Haga ping a una dirección de broadcast desde PC3 usando el comando:

   ```
   ping -b 192.168.0.255
   ```

2. Ejecuta un sniffer en PC4 (Wireshark, o simplemente, "sudo tcpdump -i eno1")
3. ¿Se reciben los mensajes de difusión en PC4? ¿Por qué?
4. Repite el experimento anterior en estos escenarios:
   a) Ambos equipos pertenecen a la misma VLAN en switches diferentes.
   b) Los equipos pertenecen a VLAN diferentes estando conectados al mismo switch.
5. ¿Se reciben los mensajes de difusión en ambos casos? ¿Por qué? ¿Por qué no?

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.

1. Desconectad el cable de PC1 de SW1.
2. Intenta hacer telnet desde PC2 a SW1. ¿Es posible?
3. ¿Atraviesan las tramas de PC2 el enlace trunk? Comprobadlo mediante la opcion "detail" del menú. ¿Qué puedes concluir?
4. Propone 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 PC pertenecientes a diferentes VLAN. Sin embargo, en la práctica, hay muchos casos en que dicha conectividad sí 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?

A. Estructura de menús de la interfaz de línea de comandos del Switch