Departament d'Enginyeria Telemàtica

UNIVERSITAT POLITÈCNICA DE CATALUNYA

PRÁCTICA 3

Configuración de VLAN

Objetivos

- Configurar VLAN por puertos
- Configurar enlaces de acceso (VLAN no etiquetadas)
- Configurar enlaces troncales (VLAN etiquetadas)
- Monitorizar el tráfico de un puerto de un conmutador desde otro puerto

Material Utilizado

- Conmutadores D-LINK DGS-3630-28TC
- Equipos de laboratorio utilizados en las prácticas anteriores
- Imagen de software del laboratorio 331: Linux Ubuntu

Duración

- Esta práctica consta de una sesión de 2 horas.

1 ¿Qué son las VLAN?

Los conmutadores utilizan la información de las direcciones de cada trama para controlar el intercambio de tramas en la red. Por medio de la monitorización de las tramas que recibe, un conmutador distingue qué dispositivos están conectados a través de sus puertos y envía las tramas solamente a los puertos adecuados.

Un conmutador reduce la cantidad de tráfico innecesario puesto que la información recibida en un puerto se envía solo al dispositivo que tiene la dirección de destino correcta, a diferencia de un concentrador o HUB, que la envía a todos los puertos.

Una VLAN es un grupo flexible de dispositivos que se pueden colocar en cualquier lugar de la red, pero se comunican como si estuvieran en el mismo segmento LAN. Con VLAN, se puede segmentar la red sin tener restricciones físicas, un inconveniente del diseño de redes tradicionales. A modo de ejemplo, con VLANs se puede segmentar una red según:

- **Grupos departamentales**: por ejemplo, en una empresa, se puede tener una VLAN para el departamento de comercialización, otro para el departamento de finanzas, y otro para el departamento del desarrollo.
- **Grupos jerárquicos**: por ejemplo, se puede tener una VLAN para los directores, otro para los encargados, y otro para el personal general.
- **Grupos de uso**: por ejemplo, se puede tener una VLAN para los usuarios del correo electrónico, y otro para los usuarios de multimedia.
- **Grupos por subred IP**: por ejemplo, se puede tener una VLAN para cada subred IP definida en la red.

1.1 Ventajas de las VLAN

La principal ventaja de las VLAN es que proporciona un sistema de segmentación de la red mucho más flexible que el de las redes tradicionales. Con las VLAN, también se obtienen los beneficios siguientes:

- Facilidad para cambiar y mover los dispositivos en redes IP

  En las redes tradicionales, los administradores de red gastan mucho de su tiempo con movimientos y cambios. Si los usuarios se cambian a otra subred, las direcciones IP se deben actualizar manualmente. Con las VLAN, si una estación en una VLAN2 se mueve a otra parte de la red, solo se debe especificar que el nuevo puerto donde se conecte esta estación transmitirá tráfico de la VLAN2.

- Seguridad extra

  Los dispositivos en cada VLAN sólo pueden comunicarse directamente con dispositivos de la misma VLAN. Si un dispositivo en la VLAN2 necesita comunicarse con un dispositivo de una VLAN3, el tráfico necesita pasar a través de routers o conmutadores de Capa 3, evitando la comunicación directa a nivel MAC (nivel 2).

- Ayuda para controlar el tráfico de broadcast

  En las redes tradicionales, la congestión puede producirse debido al tráfico broadcast, tráfico que está dirigido a todos los dispositivos de red, lo requieran o no. La VLAN puede configurarse para contener sólo aquellos dispositivos que necesiten comunicarse entre ellos.

1.2 VLAN en los conmutadores utilizados

Los conmutadores D-LINK DGS3630 proporcionan las siguientes prestaciones referidas a VLAN:

- Soportan hasta 4094 VLAN usando el estándar IEEE 802.1Q. El estándar IEEE 802.1Q permite a cada puerto:
    - Situarlo en cualquier VLAN definida en el conmutador.
    - Transmitir tramas de varias VLAN simultáneamente usando el etiquetado 802.1Q.
    - Usar el aprendizaje 802.1Q. Un sistema que usa el General VLAN Registration Protocol (GVRP), equivalente al actual Multiple VLAN Registration Protocol (MVRP), que permite al conmutador aprender de los requerimientos VLAN de las estaciones de trabajo conectadas a cada puerto, y coloca los puertos en las VLAN automáticamente.
    - Reenviar tráfico para VLAN desconocidas para el conmutador mediante etiquetado.
- Soportan la definición de VLAN por MAC, por subred IP, Private VLAN, VLAN Tunnel, etc., aunque estos casos no los trataremos en esta práctica.

1.2.1 La VLAN por omisión (o por defecto)

Un conmutador nuevo o inicializado contiene una única VLAN, la VLAN por omisión (o por defecto), con las siguientes definiciones:

- VLAN Name: Default (o VLAN1)
- VLAN ID (VID): 1

Todos los puertos están en esta VLAN, y es la única VLAN que permite el acceso a las funciones de gestión del conmutador, cuando estas funciones se quieren realizar desde un host remoto a través de una conexión telnet o http (interfaz web de configuración).

1.2.2 Definición de nuevas VLAN

Si se quiere mover un puerto de la VLAN por omisión a otra VLAN, primero se debe definir información acerca de la nueva VLAN en el conmutador.

1.2.3 VLAN. Etiquetado y no etiquetado

Cuando se están configurando las VLAN, se debe entender cuándo usar etiquetado de VLAN y cuándo no. Es sencillo: si un puerto debe transmitir tramas de una única VLAN, no es necesario aplicar etiquetado, pero si el puerto necesita tratar tramas vinculadas a más de una VLAN se necesita etiquetado de VLAN.

El estándar IEEE 802.1Q define cómo operan las VLAN en una red de conmutación de tramas de nivel 2. Una trama que cumple IEEE 802.1Q lleva información adicional que permite al conmutador determinar a qué VLAN está vinculada la trama recibida. Si la trama lleva esta información adicional, se dice que está etiquetada.

Para llevar tramas vinculadas individualmente a VLAN diferentes a través de un único enlace físico (backbone o trunk), cada trama debe ser etiquetada con un identificador de VLAN, para que el conmutador pueda clasificar las tramas recibidas según su vinculación a una VLAN. Los routers interconectan VLAN, así que también deben entender el etiquetado 802.1Q.

2 Sesión de laboratorio

En esta sesión de laboratorio vamos a configurar las distintas situaciones que nos vamos a encontrar en las redes LAN en relación a las VLAN. Básicamente consiste en conexiones "etiquetadas" y "no etiquetadas".

En primer lugar, vamos a establecer los requerimientos del escenario que deben seguir todos los grupos de laboratorio, teniendo en cuenta que se formaran 3 grupos con 4 puestos de trabajo. Cada grupo dispone de:

- 2 conmutadores, SW01 y SW02, modelo D-LINK DGS-3630-28TC, con la IP 10.90.90.**x** (**x** = {91, 92, 93, 94, 95, 96}). El profesor os indicará cuáles os corresponden.
- 4 PC de sobremesa. La interfaz eth0 deberán configurarse[1], inicialmente, con una dirección IP de la forma: 10.90.90.z /25 (con z = Número de roseta[2], como muestra el escenario de la Figura 1). Para realizar esta configuración, redordad que usaremos la orden siguiente:

```
sudo ip address add dirección_IP/máscara dev eth0
```

Se van a reservar diversos puertos de los conmutadores para usos específicos:

- Puerto 16 del SW01 y del SW02. Este puerto deberá estar vinculado a la VLAN por omisión (VLAN1) y nos servirá para gestionar los conmutadores vía web, estando conectados al conmutador a través de este puerto.
- Inicialmente, el puerto 19 del SW01 y del SW02 servirá para interconectar los conmutadores entre sí. Además, una vez se haya configurado las VLANs (Sección 2.1.2), servirá para interconectar los conmutadores entre sí en la VLAN2.
- Una vez se haya configurado las VLANs (Sección 2.1.2), el puerto 18 del SW01 y del SW02 servirá para interconectar los conmutadores entre sí en la VLAN 3. Inicialmente, este puerto ha de quedar desconectado para evitar bucles en la red.
- El puerto 16 del SW01 servirá, además, para monitorizar el tráfico entre el puerto 19 del SW01 y SW02 (a partir del apartado 2.3).
- El puerto 22 y 14 del SW1 deberán estar asignados a la VLAN2 y VLAN3, respectivamente. Estos puertos los usaremos para conectar un router en el apartado 2.1.3.

Cada grupo trabajará sobre dos VLAN que creará y configurará, siguiendo los pasos que se indican en los apartados siguientes. El número o identificador de VLAN será 2 y 3 (VLAN2 y VLAN3).

Para comprobar la existencia o no de comunicación entre equipos, se procederá a ejecutar la orden `ping` (que envía paquetes ininterrumpidamente, en un PC con S.O. Linux) hacia los equipos del mismo escenario.

[1] Importante: antes de empezar a configurar manualmente las direcciones IP de la interfaz `eth0` debemos ejecutar:

```
sudo systemctl stop NetworkManager
```

para desactivar el gestor de red genérico de Ubuntu.

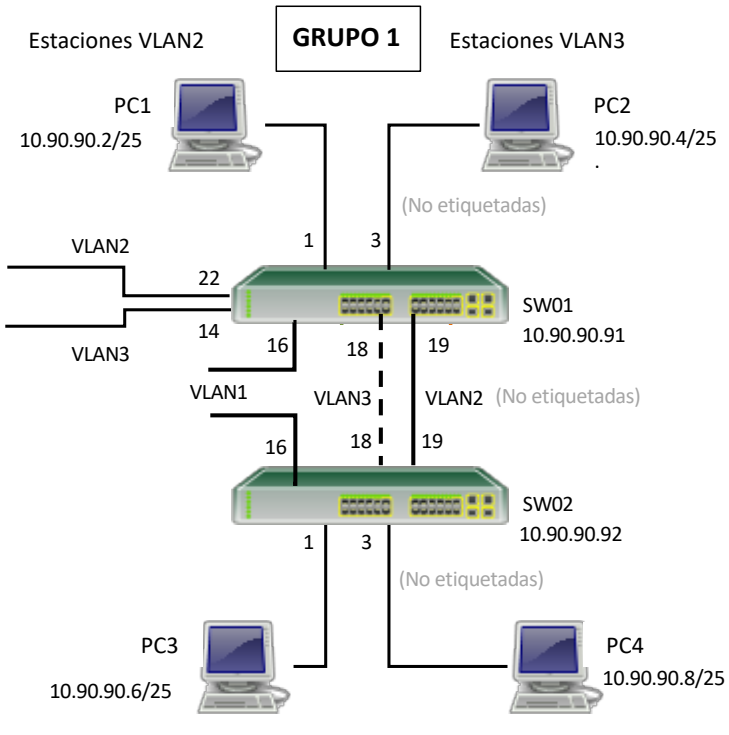
[2] Recordad que el número de roseta (que a su vez se corresponde con número de puerto en el *patch panel* del laboratorio) a la que está conectada la interfaz `eth0` de cada PC está indicada con una etiqueta amarilla en cada PC.

2.1 VLAN definidas por puerto

Tal como hemos visto en clase de teoría, el escenario más simple de VLAN que podríamos formar opera en una pequeña red utilizando un único conmutador. En esta red no sería necesario pasar tráfico de VLAN a través de un enlace entre conmutadores. Todo el tráfico lo manipularía ese único conmutador.

En esta sesión, vamos a utilizar un escenario con dos conmutadores para poder aprender cómo configurar el/los enlaces/s entre ellos. Primero configuramos los puertos de los dos conmutadores de forma que los puertos conectados a cada uno de los PCs del grupo estén en la VLAN que corresponde. Además, configuramos los dos puertos entre los conmutadores para que cada uno esté en una VLAN. De esta forma no es necesario usar etiquetas porque cada puerto está configurado como un puerto de acceso y transportará tráfico de una única VLAN. En el escenario que se muestra en la Figura 1, todas las estaciones de la misma VLAN pueden comunicarse entre ellas, independientemente del conmutador al que están físicamente conectadas, SW01 o SW02, usando el enlace entre conmutadores configurado para su VLAN. Las distintas VLAN estarán completamente separadas y no se podrán comunicar entre ellas; es decir, cada VLAN es un dominio de broadcast independiente.

En primer lugar, el profesor realizará las conexiones mostradas en la Figura 1, en la que están indicados qué equipos/puertos de los conmutadores tendrán que pertenecer a la VLAN 1, 2 o 3. Antes de configurar las VLANs, configuraremos correctamente las IPs de cada PC y comprobaremos que hay conectividad entre los equipos mediante un `ping`.



GRUPO	PC 1	PC 2	PC 3	PC 4	SW01	SW02
1	2	4	6	8	.91	.92
2	12	10	16	14	.93	.94
3	22	24	18	20	.95	.96

Figura 1. Esquema del primer escenario, con dos VLAN. La conexión entre los dos switches por sus puertos 18 se realizará una vez se hayan configurado adecuadamente las VLANs en los dos switches.

PASO 1 – Utilizando los comandos vistos en la práctica 1, configura la interfaz eth0 de cada PC según la asignación indicada para cada grupo en la Figura 1.

Antes de empezar la sesión de laboratorio, hay confeccionar una hoja con los **comandos necesarios para configurar la eth0** del PC que habitualmente usáis, según la configuración de la Figura 1. Para ello, os invitamos a revisar los manuales de las dos prácticas anteriores. También se debe incluir la lista de pasos para la **configuración de las VLAN** en el switch.

PASO 2 – Haz un ping para comprobar con qué equipos del laboratorio tienes conectividad y con cuáles no.

P1. *¿Entre qué equipos tenemos conectividad? ¿A qué nivel (nivel 2 o 3)?*

A continuación, para poder gestionar el conmutador (es decir, crear las VLAN y configurar los puertos correspondientes), debemos conectarnos a este a través de uno de sus puertos que permanecen en la VLAN de gestión (es decir, la VLAN 1, o VLAN por defecto). En nuestro escenario, vamos a utilizar el **puerto 16** del conmutador, puerto que **permanecerá en** toda la práctica asociado a **la VLAN 1**. Desde un PC conectado a ese puerto, podremos acceder a las funciones de gestión del conmutador y configurar los demás puertos del switch en las VLAN de nuestro escenario (Figura 1). A continuación, se detallan los pasos a seguir para

1) Configurar las VLAN que usaremos en la práctica (apartado 2.1.1)
2) Asignar los puertos del switch a las VLAN que se han definido en el paso 1 (apartado 2.1.2)

2.1.1 Configurar las VLAN en los conmutadores SW01 y SW02

Para poder configurar las VLAN que usamos en la práctica, accedemos a las funciones de gestión del conmutador a través de la interfaz web del mismo, utilizando el navegador Firefox, e indicando la dirección IP que corresponda al conmutador (el nombre de usuario y contraseña requeridos son: `admin`, `admin`, respectivamente).

Seleccionamos la opción “L2 Features” y, dentro de este apartado, la opción “VLAN”. Aquí disponemos de diferentes opciones adicionales de las cuales **escogeremos “802.1Q VLAN” para crear la VLAN2 y la VLAN3**. Tal como se muestra en la Figura 2, la VLAN 1 es la “Default VLAN” y ya está creada desde un inicio. Todos los puertos están asignados a esta VLAN por defecto.

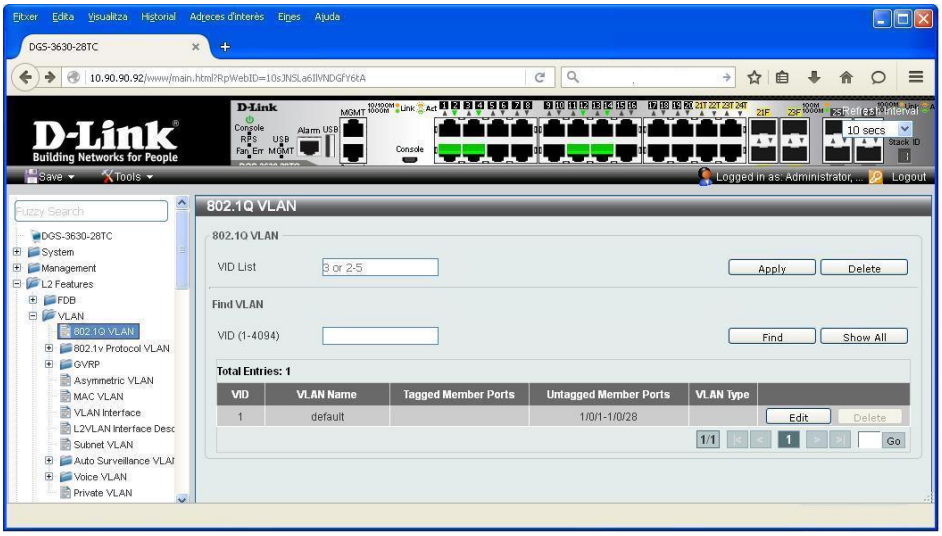


Figura 2. Añadir las VLANs en cada conmutador.

PASO 3 – Cambia la conexión del PC1 desde el puerto 1 del SW01 al puerto 16 del SW01, y cambia la conexión del PC4 desde el puerto 3 del SW02 al puerto 16 del SW02.

PASO 4 – Desde PC1 y PC4, accede al conmutador vía web y crea las VLAN 2 y la VLAN 3 a través de la opción "L2 Features"→ "VLAN"→" 802.1Q VLAN".

Para crear las nuevas VLAN, en el campo "VID list" especificaremos el identificador de la VLAN (o lista de identificadores), un valor entre 1 y 4094, y clicaremos "Apply". Seguidamente, la (o las) nueva VLAN aparecerá en la lista que se muestra en la parte inferior. A través de la opción "Edit" de la VLAN correspondiente podemos cambiar el nombre asignado por defecto a la VLAN, si quisiéramos.

2.1.2 Añadir puertos a las VLAN en los conmutadores SW01 y SW02

Para asignar los puertos a las VLAN según el escenario que se muestra en la Figura 1, utilizaremos la opción "VLAN interfaces" (también dentro del apartado "VLAN"). Aparecerá una lista similar a la que se muestra en la Figura 3. Para cada puerto, podemos ver la asignación de VLAN actualmente activa.

Para configurar un puerto determinado, clicaremos en el botón "Edit" de ese puerto y especificaremos los parámetros que nos piden (Figura 4):

VLAN mode: Utilizaremos "Access" o "Trunk", según sea el caso. Para esta primera parte de la práctica configuraremos el puerto como "Access".

VID (1-4094): Identificador de VLAN. En nuestro caso "2" o "3", para asignar la VLAN2 o VLAN3, respectivamente, a los puertos utilizados que corresponda.

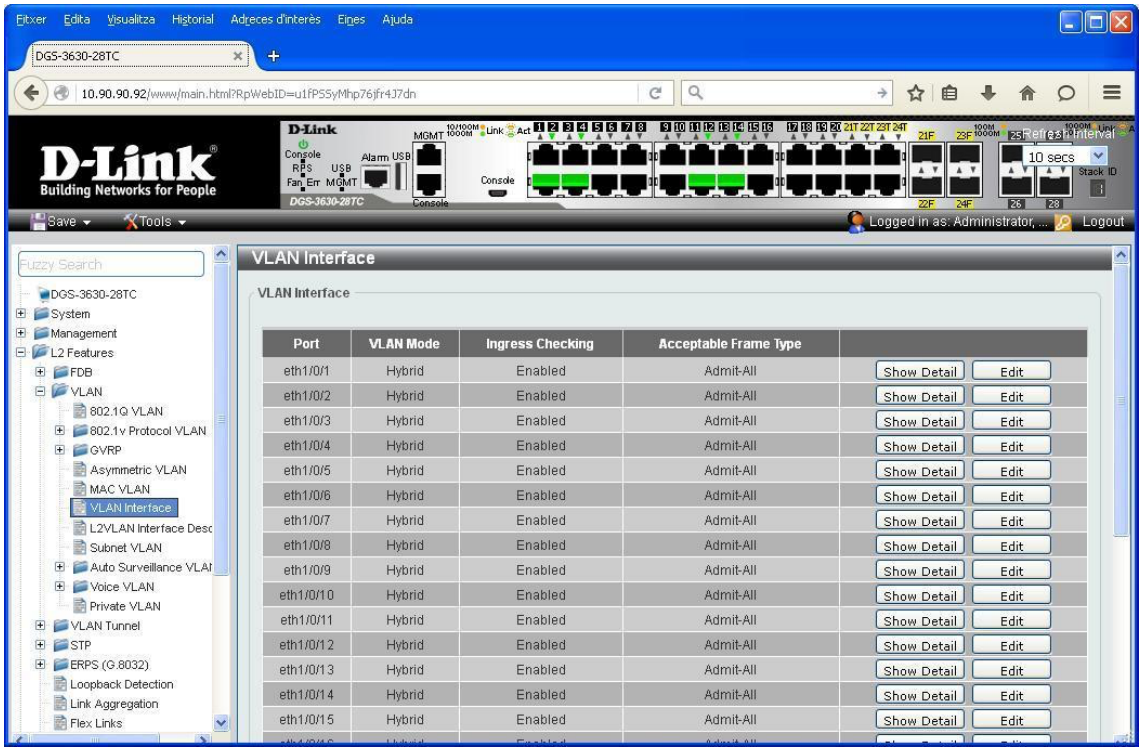


Figura 3. Asignar los puertos a las VLANs en cada conmutador.

Debemos recordar que la gestión del conmutador la realizaremos a través de la VLAN1 y, en nuestro caso, desde un PC conectado al puerto 16 de cada conmutador, el cual ha de mantener esa configuración durante toda la práctica[3].

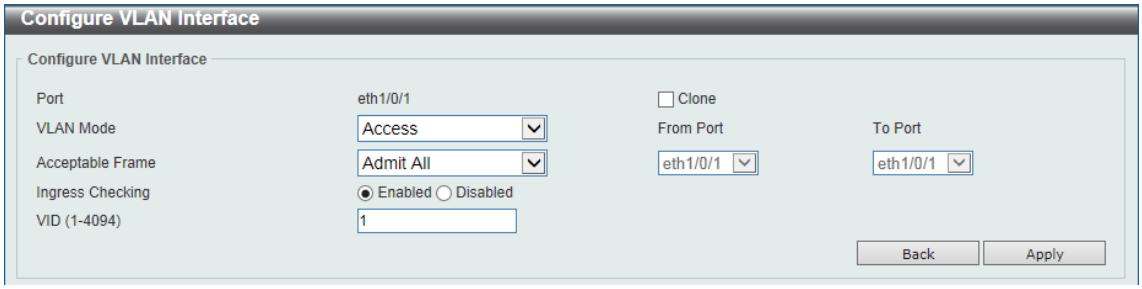


Figura 4. Ejemplo de configuración del puerto 1 como enlace de acceso en la VLAN 1.

PASO 5 – Desde PC1 y PC4, configura los puertos del SW01 y del SW02, respectivamente, involucrados en las dos VLAN, según el escenario indicado en la Figura 1.

Antes de empezar la sesión de laboratorio, hay que entregar al profesor, en la misma hoja escrita a mano y con nombre y apellidos, una tabla con los parámetros "Port", "VLAN Mode", "VID" (ver las Figura 3 y Figura 4) **necesarios para configurar el SW01**, según el escenario indicado en la Figura 1.

P2. *Listar las VLAN existentes hasta ese momento junto con los puertos asignados a cada VLAN (opción 802.1Q VLAN o VLAN interface). ¿Cuántos puertos etiquetados y no etiquetado hay?*

PUNTO DE CONTROL 1 (20%) **Enseña al profesor la configuración VLAN resultante en cada switch y responded a la pregunta P2.**

Una vez configurados los puertos del conmutador, volvemos a poner el PC1 y el PC4 en los puertos del SW correspondientes a la distribución mostrada en la Figura 1 y conectamos los puertos 18 de los dos conmutadores. A continuación, comprobaremos que tenemos conectividad, solamente, entre equipos de la misma VLAN, pero no entre equipos de diferente VLAN.

PASO 6 – Abre el Wireshark en cada ordenador. Comprueba la conectividad entre estaciones de cada VLAN con la orden "ping".

P3. *¿Entre qué equipos tenemos conectividad? ¿A qué nivel (nivel 2 o 3)?*

Comprueba a través del Wireshark, que realmente no recibís más tráfico que el transmitido por los puertos pertenecientes a la VLAN correspondiente.

P4. *Intentad enviar tramas broadcast dentro de una misma VLAN. ¿Es posible recibir tramas broadcast de otras VLAN? ¿Por qué?*

Fijaros que todos los PCs del grupo pertenecen a la misma red IP (10.90.90.0/25) y pensad en qué puede afectar esto sobre los resultados observados.

[3] Si lo configuráramos en otra VLAN estando conectados al puerto 16, ¡perderíamos la posibilidad de seguir cambiando la configuración!

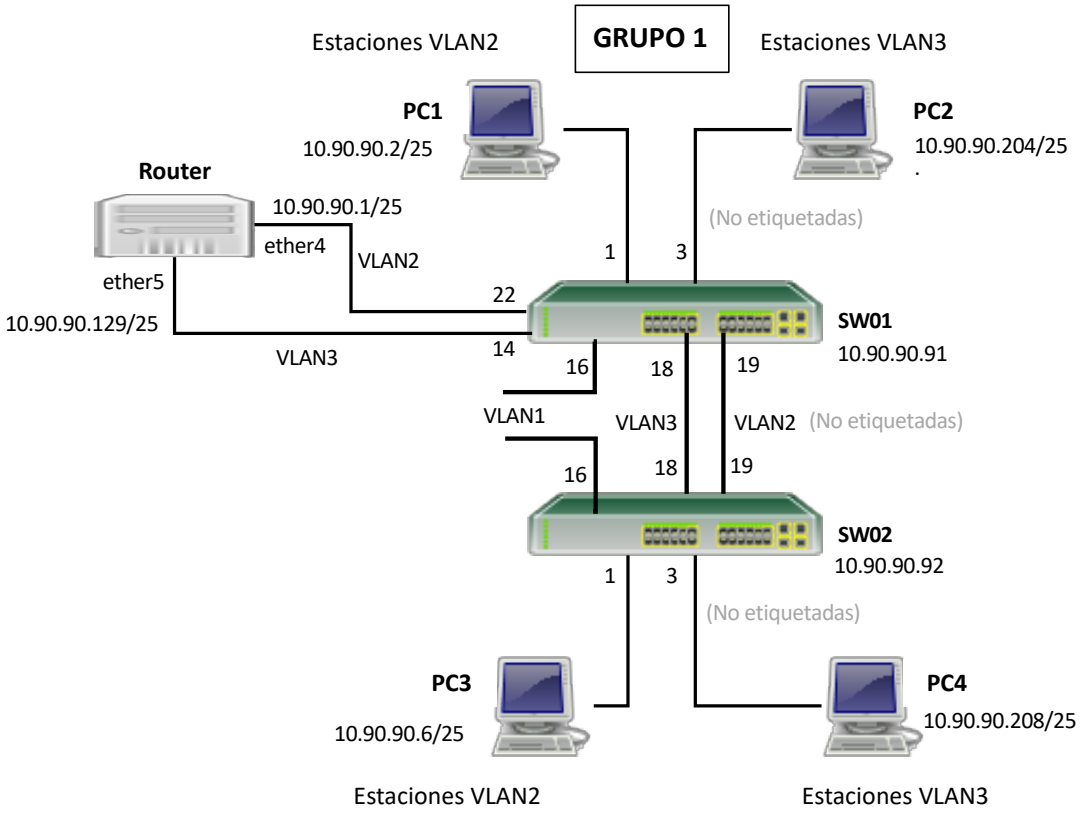
2.1.3 Conectividad entre VLANs

Ahora cambiamos las direcciones IP que tenemos asignadas para que los PCs de diferentes VLAN pertenezcan a diferentes redes IP (o sea, a diferentes dominios de broadcast). En la Figura 5 se muestra el nuevo escenario con router, con una configuración posible para realizar la interconexión entre las dos subredes; cada grupo tiene que adaptar las direcciones según su escenario, mientras el profesor conectará los routers en cada grupo.

Los PCs de la VLAN2 quedaran con la misma IP original, pero en los PCs de la VLAN3 actualizaremos su dirección IP a un valor que sea válido para la subred 10.90.90.128/25 (ver Figura 5). Recuerda que para actualizar la IP en los PCs de la VLAN3 primero debemos borrar la dirección IP asignada anteriormente, con la orden del tipo:

```
sudo ip address del dirección_IP/mascara dev eth0
```

PASO 7 – Cambia la dirección IP de PC2 y PC4, tal como indicado en la Figura 5.



GRUPO	PC 1	PC 2	PC 3	PC 4	SW01	SW02
1	2	204	6	208	.91	.92
2	12	210	16	214	.93	.94
3	22	224	18	220	.95	.96

Figura 5. Escenario de VLAN interconectadas con router.

Además, para poder comunicar equipos de VLANs diferentes necesitamos utilizar un router y configurarlo adecuadamente en el escenario. El router ya estará configurado adecuadamente para que tenga un puerto (#4) en la red 10.90.90.0/25 y otro puerto (el #5) en la red 10.90.90.128/25, tal como indicado en la Figura 5, por este motivo, no es necesario interactuar con el router a nivel de gestión.

También deberemos configurar una ruta IP para que desde cada PC se pueda mandar paquetes a la otra subred, tal como hemos visto en la práctica 1.

PASO 8 – En los PCs de la VLAN2 ejecutad la orden:

```
sudo ip route add 10.90.90.128/25 via 10.90.90.1
```

Y en los PCs de la VLAN3 ejecutad la orden:

```
sudo ip route add 10.90.90.0/25 via 10.90.90.129
```

PASO 9 – Una vez tengamos el nuevo escenario completo, comprobaremos la conectividad entre equipos mediante la orden `ping`.

P5. *¿Es posible recibir tramas Ethernet de otras VLAN? ¿Por qué?*

P6. *¿Es posible recibir paquetes IP de otras VLAN? ¿Por qué?*

P7. *A pesar de estar conectados a los switches, ¿podemos tener diferentes subredes configuradas en un mismo conmutador ya que tenemos configuradas diferentes VLANs?*

Realiza diversas capturas de tramas en los PCs con Wireshark mientras realizamos un `ping` a distintos PCs del escenario. Compara las capturas respecto a un mismo mensaje ICMP_request o ICMP_reply obtenidas en un distinto PC.

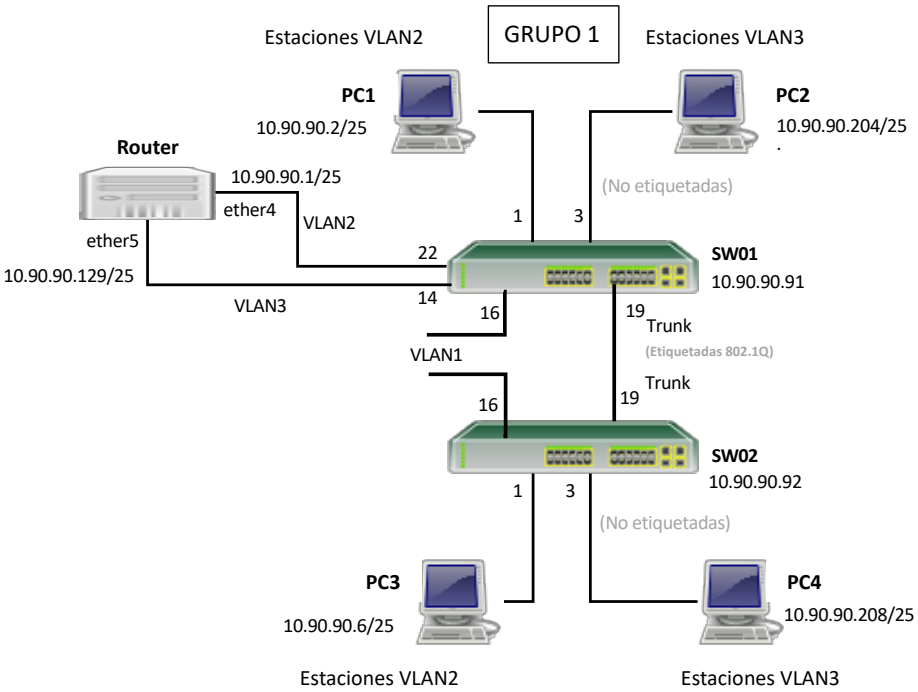
P8. *¿Han aparecido tramas Ethernet con etiqueta de VLAN? ¿Por qué?*

2.2 Conexiones etiquetadas

Tal como se ha visto en teoría, sobre los enlaces donde pasa tráfico de más de una VLAN, las tramas han de ir etiquetadas. Por ejemplo, en una red con más de un conmutador, donde las VLAN pueden estar distribuidas entre diferentes conmutadores, se debe utilizar conexiones etiquetadas 802.1Q (enlaces en modo Trunk) para que todo el tráfico VLAN pueda pasar a través del enlace entre los dos conmutadores y cada trama MAC pueda ser clasificada según la VLAN a la que está asociada. De esta forma se hace un uso más eficiente de los puertos disponibles del conmutador, a diferencia de la opción aplicada en el apartado anterior.

El escenario que se muestra en la Figura 6, todas las estaciones en la VLAN2, o en la VLAN3, pueden comunicarse con las otras estaciones de su VLAN (en la VLAN2, o en la VLAN3, respectivamente) independientemente del conmutador al que están físicamente conectadas, SW01 o SW02, usando un único enlace entre conmutadores. Usaremos el puerto 19 para interconectar los dos conmutadores (y desconectaremos el puerto 18, usado hasta ahora). Por el puerto 19 debe pasar el tráfico de todas las VLAN sin perder su pertenencia a una VLAN concreta. Este comportamiento lo conseguimos configurando el puerto 19 del SW1 y del SW2 como un puerto VLAN de tipo TRUNK.

Para establecer esta configuración, partiremos de las VLANs y puertos configurados en el apartado anterior en el conmutador SW01 y SW02, y completándolo con los pasos que se explican en el punto 2.2.1.



GRUPO	PC 1	PC 2	PC 3	PC 4	SW01	SW02
1	2	204	6	208	.91	.92
2	12	210	16	214	.93	.94
3	22	224	18	220	.95	.96

Figura 6. Configuración del escenario con etiquetas.

2.2.1 Añadir el puerto 19 de cada switch como puerto trunk de VLAN

Podemos configurar el puerto 19 en modo “TRUNK” desde la opción de configuración “VLAN interface” de la interfaz web de gestión del conmutador. Esto debe hacerse para cada conmutador, dado que debemos emplear las etiquetas 802.1Q en cada uno de los dos puertos 19.

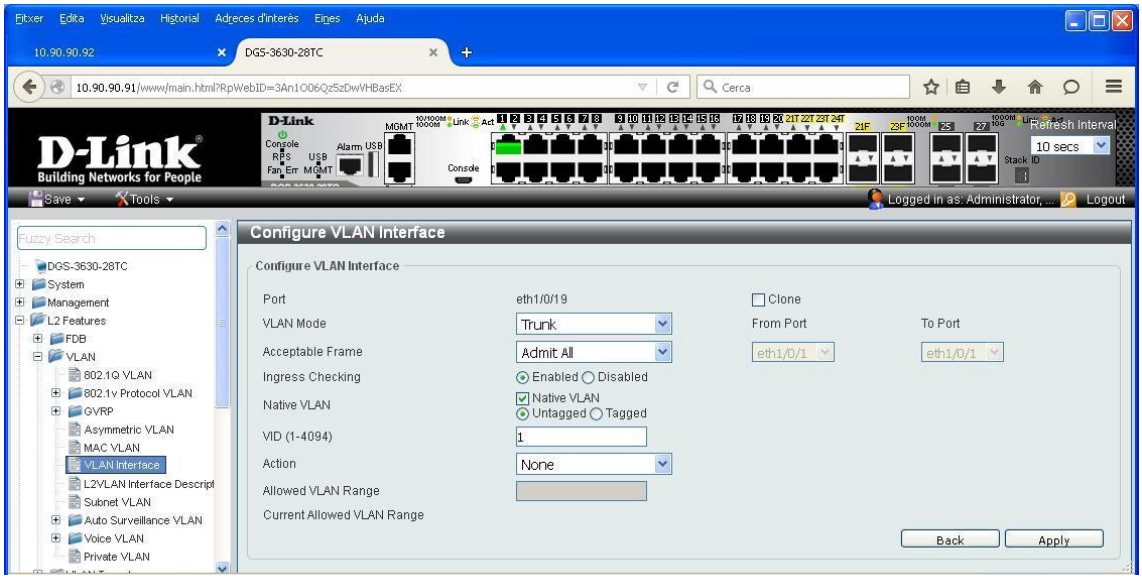


Figura 7. Configuración del puerto 19 de cada switch en modo *trunk*.

PASO 10 – Conecta el PC3 en el puerto 16 del SW02 y configura el puerto 19 en modo trunk. Vuelve a conectar el PC3 en el puerto 3 del SW02.

PASO 11 – Conecta el PC1 en el puerto 16 del SW01 y configura el puerto 19 en modo trunk. Vuelve a conectar el PC1 en el puerto 1 del SW01.

Una vez realizada la configuración comprueba los detalles seleccionando otra vez la opción "VLAN Interface".

2.2.2 Comprobar la pertenencia a la VLAN

Desde la opción "VLAN Interface" y "802.1Q VLAN" chequear la información mostrada para los puertos que estáis utilizando (equipos y para interconexión entre conmutadores).

P9. *Tomad nota de la información relativa a VLAN Mode, puertos asociados a cada VLAN, etc.*

2.2.3 Conectar los dos conmutadores

Comprobad que están conectados el puerto 19 del SW01 y el puerto 19 del SW02.

PASO 12 – Ejecuta una captura de Wireshark en la *eth0* de cada PC. Comprueba que podéis comunicar entre los equipos de la misma VLAN, utilizando el comando *ping*.

PASO 13 – También comprueba que podéis comunicar con los equipos de la otra VLAN de vuestro grupo. Observa en el Wireshark el tráfico generado en vuestra red.

P10. *¿Qué configuración (la del apartado 2.1 o del apartado 2.2) os parece mejor para interconectar equipos de la misma VLAN que están en diferentes conmutadores? ¿Por qué?*

P11*. ¿Habéis observado tramas etiquetadas en este escenario? ¿Por qué?*

PUNTO DE CONTROL 2 (20%)

Enseña al profesor los resultados del paso 13 y comentad la pregunta P11.

2.3 Funciones de monitorización. Copia de tráfico

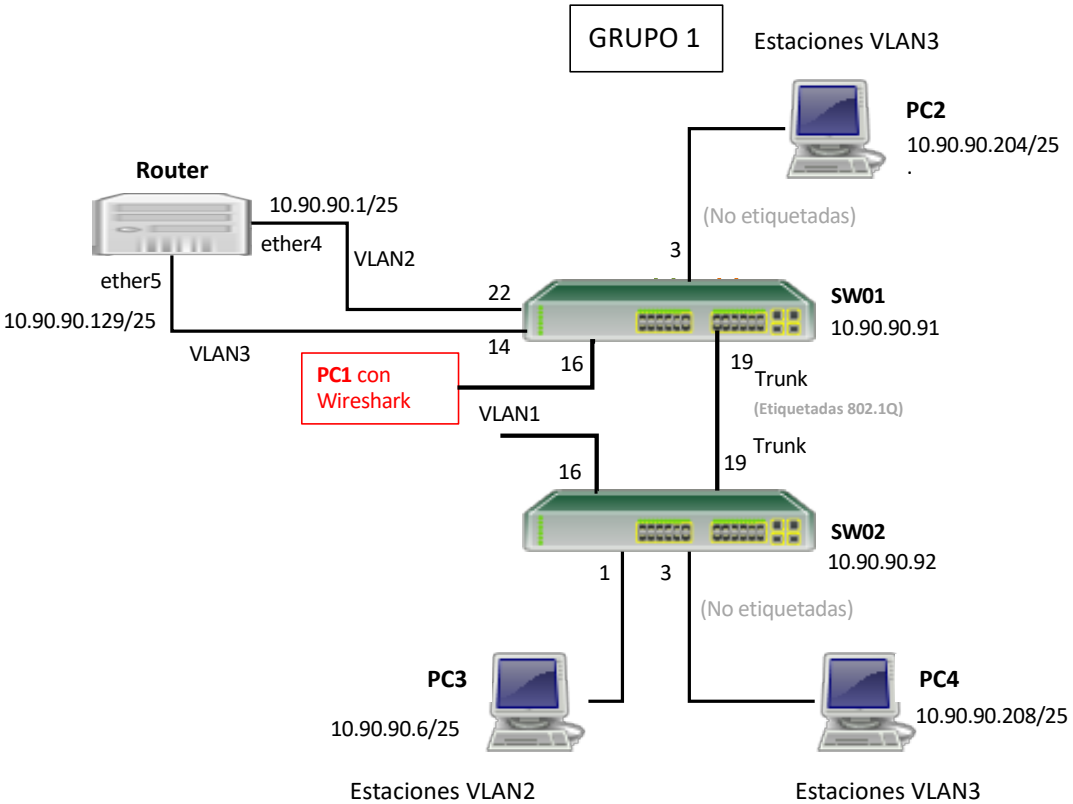
Para poder analizar el tráfico que fluye por un puerto determinado podemos utilizar la opción "Mirror Settings" del conmutador. Esta opción permite "copiar" el tráfico que entra y/o sale por un puerto y ofrecerlo en otro puerto, desde donde podremos usar un analizador de protocolos (por ejemplo, Wireshark en un PC conectado a dicho puerto) para poder realizar un seguimiento de los intercambios de tramas que pasan por un puerto determinado.

***P12.** ¿Es posible que el puerto origen tenga un ancho de banda mayor o igual al del puerto destino? Comentar la respuesta.*

Para realizar la configuración del *mirroring*, tenemos que conectar uno de los PCs al puerto 16 del conmutador y así podremos acceder a la gestión del mismo (recuerda que debe ser un puerto que esté en la VLAN1), tal como se muestra en la Figura 8.

Desde ahí, configuramos la "copia" de tráfico del puerto 19 ("Source") al puerto 16 ("Destination") del SW1

PASO 14 – Conecta el PC1 al puerto 16 del SW01. Desde el PC1 accede a la opción de configuración "Monitoring"/"Mirror settings" del switch. Asigna el puerto 16 como *destination*, y el puerto 19 como *source*.



GRUPO	PC 1	PC 2	PC 3	PC 4	SW01	SW02
1	2	204	6	208	.91	.92
2	12	210	16	214	.93	.94
3	22	224	18	220	.95	.96

Figura 8. Configuración del *mirroring* del tráfico del puerto 19 hacia el puerto 16 del SW01.

PASO 15 – Arranca el Wireshark en cada PC con una captura de tráfico por la interfaz *eth0*.

A continuación, generamos tráfico (por ejemplo, con un ping) entre PCs y capturamos el tráfico que pasa por el enlace TRUNK mediante el PC1 conectado al puerto 16 del SW01 (que está observando –*mirroring*-el tráfico que pasa por el puerto 19, configurado en modo trunk). Simultáneamente, estamos capturando también el tráfico en los demás PC, en especial los involucrados en el ping (origen y destino), para comparar las distintas capturas para los casos especificados a continuación.

PASO 16 – Ping desde PC2 a PC3

PASO 17 – Ping desde PC2 a PC4

PASO 18 – Ping desde PC3 a PC4

P13. *¿Podéis visualizar el tráfico que se transmiten los PCs indicados en los casos anteriores?*

P14. *¿Las tramas capturadas en PC1 muestran una etiqueta de VLAN? ¿De qué VLAN? ¿y las tramas capturadas por los demás PCs? Razonad el porqué del comportamiento que estáis observando. Comparad los resultados de los diferentes casos.*

P15. *¿El PC conectado al puerto destino del "mirror" (puerto 16 del conmutador) está asociado a la misma VLAN que los demás PCs? Razonad la respuesta.*

PUNTO DE CONTROL 3 (20%)

Enseña al profesor los resultados del paso 18 y responded a la pregunta P14.