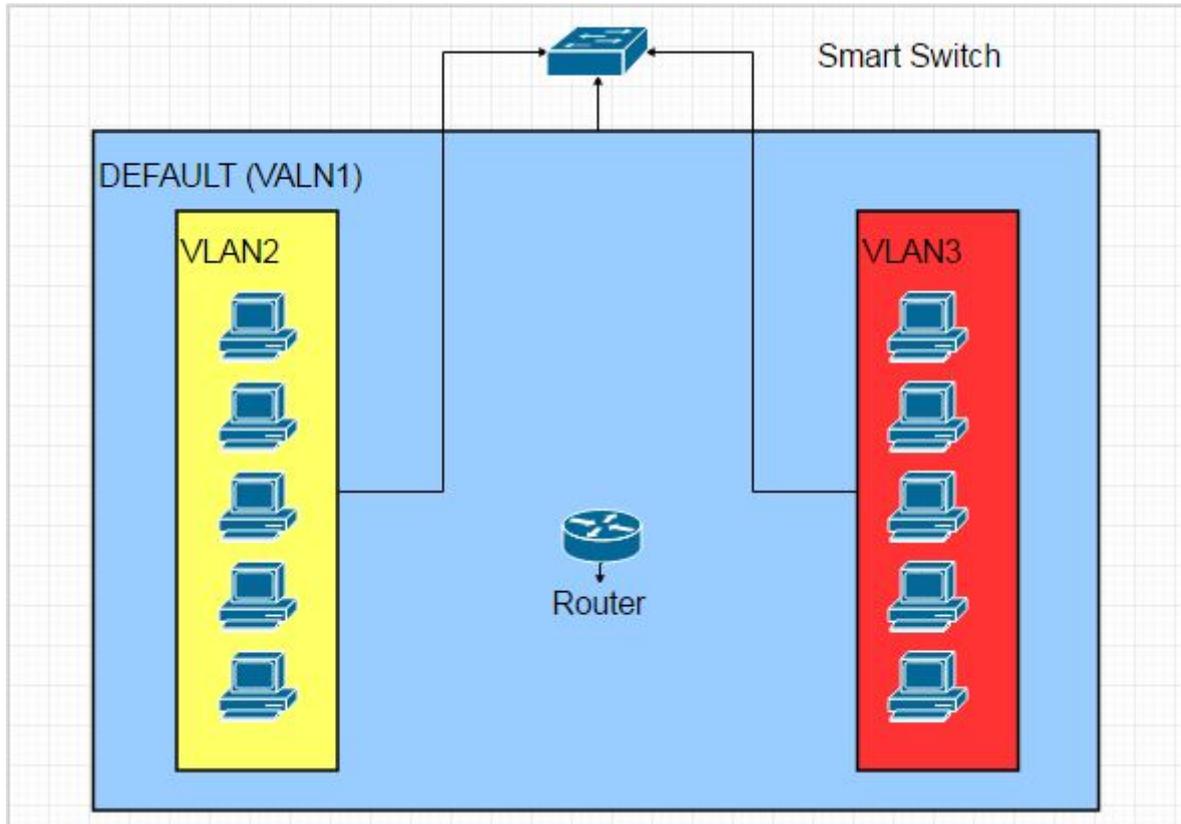


VLANs



Marta Canchado Rodríguez

Fecha: 22/05/2017

Año escolar: 2016/2017

Módulo: Redes Locales

Profesor: José Luis Rodríguez Rodríguez

IES Ramón del Valle Inclán

Índice

Índice	1
Introducción	2
Actividad 1. VLAN: entendiendo la tecnología	2
Actividad propuesta:	2
Solución	2
Actividad 2. Tramas Ethernet Etiquetas. 802.1	3
Actividad 3. Configurando VLANs	3
Actividad propuesta:	3
Ejercicio 1. Segmentando la red en VLANs	4
Solución	4
Ejercicio 2. Acceso a recursos compartidos	10
Solución	11
Ejercicio 3.- VLAN de administración.	15
Solución	15
Ejercicio 4.- Segmentando redes WiFi. Multi SSID.	18
Solución	18
Conclusiones	21
Bibliografía	21

Introducción

En esta tarea se resolverán las diferentes actividades presentadas en la tarea VLANs, analizaremos las ventajas de utilizarlas y llevaremos a cabo distintas configuraciones.

Actividad 1. VLAN: entendiendo la tecnología

Actividad propuesta:

“Para entender el concepto de VLAN vas a ver los siguientes documentos:

- Presentación VLANs-cap3.ppt
- Vídeo VLANs.mov

De la lectura anterior debes aprender:

- Qué es una VLAN
- Beneficios de las redes VLANs: seguridad, reducción de costos, mejor rendimiento, dominios de colisión reducidos, mayor eficiencia del personal TI, administración más simple de aplicaciones y proyectos.
- Tipos de VLANs: datos, voz, predeterminada, nativa, administración”

Solución

Las VLANs nos permiten crear diferentes redes lógicas sin necesidad de tener varios dispositivos físicos, para ello es necesario que nuestro switch gestionable cuente con tecnología VLAN incorporada.

Las ventajas de las VLANs:

- ❖ Reducción de costos, podemos prescindir de tener varios elementos físicos.
- ❖ Seguridad, funciona como un Firewall que impide la conexión entre equipos de VIDs diferentes.
- ❖ Facilidad en la administración, se puede reducir el campo de búsqueda de errores.
- ❖ Mayor rendimiento, reduce el tráfico innecesario de tramas a través de la red.
- ❖ Control de las tramas Broadcast, reduce el número de dispositivos físicos de la red.

Actividad 2. Tramas Ethernet Etiquetas. 802.1

“El encabezado de las tramas de Ethernet estándar no contiene información sobre la VLAN a la que pertenece la trama; por lo tanto, cuando las tramas de Ethernet se colocan en un enlace troncal, se debe agregar la información sobre las VLAN a las que pertenecen. Este proceso, denominado “etiquetado”, se logra mediante el uso del encabezado IEEE 802.1Q, especificado en el estándar IEEE 802.1Q. El encabezado 802.1Q incluye una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original que especifica la VLAN a la que pertenece la trama.

Cuando el switch recibe una trama en un puerto configurado en modo de acceso y asignado a una VLAN, el switch coloca una etiqueta VLAN en el encabezado de la trama, vuelve a calcular la FCS y envía la trama etiquetada por un puerto de enlace troncal.

Las posibles situaciones que nos encontramos son:

Un equipo envía tramas Ethernet sin etiquetar (Untagged). Si el destino estuviera en otra boca del switch se enviará la trama a dicho destino.

Si la trama hubiera que reenviarla a otro switch por un enlace troncal, debe ser etiquetada con el formato indicado anteriormente (Tagged).”

Actividad 3. Configurando VLANs

Actividad propuesta:

“Para realizar esta actividad vamos a usar la documentación de los switches del taller:

DGS_1210 Smart Series Manual.pdf → manual de usuario

DGS_1210 Smart Series Getting Started Guide.pdf → Guía de inicio

DGS_1210_Smart_Series_Datasheet_EN_EU.pdf → Hoja de datos

El siguiente videotutorial te ayudará a entender los conceptos y configuración: https://www.youtube.com/watch?v=i3cOWW4R_aI (D Link Taller Tecnico Gestion redes wifi segmentación VLAN ACL).

Echa un vistazo a la hoja de datos y la guía de inicio. Lo comentaremos en clase.

Para realizar la configuración de VLANs vamos a usar el manual de usuario. En el apartado VLAN>802.1Q VLAN (pág 30) puedes aprender a configurar las VLANs. Existe una VLAN por defecto, la número 1 de nombre “default”, a la que pertenecen todos los puertos

del switch y en modo Untagged. Por esta razón, inicialmente cualquier equipo conectado al switch puede conectar entre sí; existe una única VLAN a la que pertenecen todas los puertos del switch.”

Ejercicio 1. Segmentando la red en VLANs

“Créate una topología de red, usando los switches gestionables del taller, que permita tener 2 VLANs con las siguientes características:

Núm 2 de nombre “Comerciales”. Puertos miembros: 4 al 10

Núm 3 de nombre “Recursos Humanos”. Puerto miembros: 11 al 16

Realiza pruebas de conectividad antes de crear las VLANs y una vez creadas para comprobar cómo se corta el tráfico de red entre los equipos de ambas VLANs. Comprueba que sí hay conectividad entre los equipos de la misma VLAN.

Puedes seguir el siguiente artículo “¿Cómo configurar VLAN estáticas en DGS-1210?”: http://www.dlink.com/es/es/support/faq/switches/layer-2-gigabit/dgs-series/es_dgs-1210_como-configurar-vlan-estaticas.”

Solución

En primer lugar, antes de configurar el switch, se conectan dos equipos (a partir de ahora PC1 y PC2), se cambia la IP de los equipos para que se encuentren en la misma red, 193.168.50.0/24, en concreto al PC1 se le asigna la IP 192.168.50.1 y al PC2 la IP 192.168.50.2. A continuación se hace ping entre las IPs para comprobar la conectividad, como podemos observar en las siguientes capturas se obtiene respuesta, esto se debe a que un switch gestionable por defecto tiene creada la VLAN de nombre Default y VID 1 que contiene todos los puertos del mismo, y por lo tanto permite la comunicación entre ellos.

- ❖ Ping de PC1 a PC2:

```
C:\Users\Marta>ping 192.168.50.2
Haciendo ping a 192.168.50.2 con 32 bytes de datos:
Respuesta desde 192.168.50.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.50.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.50.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\Marta>
```

- ❖ Ping de PC2 a PC1:

```
C:\Users\Administrador>
C:\Users\Administrador>ping 192.168.50.1

Haciendo ping a 192.168.50.1 con 32 bytes de datos:
Respuesta desde 192.168.50.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.50.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.50.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.50.1:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\Administrador>
```

Tras esta primera prueba de conectividad se procede a la creación de las VLANs. Es necesario acceder a la página de configuración del Switch, para ello se cambiará la IP del PC1 a una que se encuentre en la red 10.0.0.0/8, por ejemplo 10.90.90.91 y en la ventana del navegador se escribe la dirección por defecto del Switch (10.90.90.90), aparecerá la siguiente ventana que solicita la contraseña de administración (por defecto admin):



Al escribir la contraseña y pulsar ok aparecerá el gestor de configuración rápida (Smart Wizard) para no seguir esta configuración se pulsa exit:



Y se abrirá la ventana de configuración del Switch:

The screenshot shows the D-Link web management interface for a DGS-1210-24 switch. The left sidebar contains a tree view with 'VLAN' highlighted by a purple box. The main content area displays 'Device Information' with the following details:

Device Information		System Information	
Device Type	DGS-1210-24	System Name	
Boot Version	0.00.005	System Location	
Firmware Version	4.10.023	System Time	01/01/2013 01:29:19
Hardware Version	D1	System Up Time	0 days, 1 hours, 0 mins, 40 seconds
Serial Number	R3WB1G5000654	Login Timeout (minutes)	5
MAC Address	1C-5F-2B-29-E1-60		

IP Address Information			
IPv4 Address	10.90.90.90		
Subnet Mask	255.0.0.0		
Default Gateway	0.0.0.0		
IPv6 Global Unicast Address			
IPv6 Link-Local Address	FE80::1E5F:2BFF:FE29:E160/10		

Device Status and Quick Configurations					
RSTP	Disabled	Settings	SNMP Status	Disabled	Settings
Port Mirroring	Disabled	Settings	802.1X Status	Disabled	Settings
Storm Control	Disabled	Settings	Safeguard Engine	Enabled	Settings
DHCP Client	Disabled	Settings	IGMP Snooping	Disabled	Settings
Jumbo Frame	Disabled	Settings	Power Saving	Enabled	Settings

Desde esta ventana se pulsa sobre VLAN (señalado con un recuadro morado en la imagen anterior), se mostrará lo siguiente:

The screenshot shows the '802.1Q VLAN Settings' page. At the top, there are options for 'Asymmetric VLAN' (with an 'Example' link) and radio buttons for 'Enabled' and 'Disabled'. Below this, it shows 'Total static VLAN entries: 1' and a note 'Maximum 256 entries'. A table lists the existing VLAN entry, which is highlighted with a purple box:

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-28		Delete

At the bottom of the page, there is a 'Page' dropdown set to '01', and 'Back' and 'Next' buttons.

En la imagen anterior se puede observar la VLAN por defecto que se mencionó con anterioridad. Para crear las VLANs tenemos que editar la VLAN 1 porque 1 puerto no puede estar marcados como Untagged en más de una VLAN, una vez modificado la VLAN 1 quedaría así:

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Ya podemos proceder a crear las VLANs pulsando en Add:

- ❖ Se crea la VLAN “Comerciales” de la siguiente forma:

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

- ❖ Y la VLAN “Recursos-Humanos”:

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Como se puede observar en las últimas dos capturas, al crear una VLAN se le asigna un VID (Identificador de VLAN), un nombre descriptivo, y se seleccionan como Untagged (no etiquetados) los puertos que se deseen añadir a cada VLAN, un puerto no puede encontrarse como Untagged en más de un VID distinto a menos que tengamos activa la función de VLAN asimétrica.

La ventana de VLAN quedaría así:

802.1Q VLAN Settings Safeguard

Asymmetric VLAN [Example] Enabled Disabled

Total static VLAN entries: 3
 Maximum 256 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-03, 17-28		<input type="button" value="Delete"/>
2	Comerciales	04-10		<input type="button" value="Delete"/>
3	Recursos-Humanos	11-16		<input type="button" value="Delete"/>

Page 01

Una vez creadas las VLANs hay que asignar desde el apartado VLAN PVID a qué VLAN pertenece cada puerto, en los puertos 4-10 se cambia el valor de 1 a 2, y en los puertos 11-16 se cambia el valor de 1 a 3, quedaría de la siguiente manera:

802.1Q VLAN PVID Settings Safeguard

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14
PVID	1	1	1	2	2	2	2	2	2	2	3	3	3	3
Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
PVID	3	3	1	1	1	1	1	1	1	1	1	1	1	1

Hacemos clic sobre Save para guardar la configuración.

Procedemos a poner a prueba nuestra configuración, para ello se cambia la IP de PC1 para que pertenezca a la red de PC2, se le asigna la IP 10.90.30.1 y se procede a hacer ping teniendo ocupados los puertos 5 (VLAN 2) y 6 (VLAN 2). A continuación se ocupan los puertos 5 (VLAN 2) y 13 (VLAN 3) y se hace ping. Y finalmente se ocupan los puertos 12 (VLAN 3) y 13 (VLAN 3) y se vuelve a hacer un ping.

Si hubiésemos utilizado el comando con el modificador -t, no sería necesario estar repitiendo el ping cada vez que cambiamos el PC de VLAN ya que este modificador manda ping de forma consecutiva hasta que se le dé la orden para que se detenga.

Estos son los resultados:

- ❖ Ping entre VLAN 2 (se producen los mismos resultados entre dos equipos de la VLAN 3):

```
C:\Users\Marta>ping 10.90.90.91
Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128
Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
C:\Users\Administrador>ping 10.90.30.1
Haciendo ping a 10.90.30.1 con 32 bytes de datos:
Respuesta desde 10.90.30.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.30.1: bytes=32 tiempo<1m TTL=128
Estadísticas de ping para 10.90.30.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

- ❖ Ping entre VLAN 2 y VLAN 3:

```
C:\Users\Marta>ping 10.90.90.91
Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Respuesta desde 10.90.30.1: Host de destino inaccesible.
Respuesta desde 10.90.30.1: Host de destino inaccesible.
Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
              (0% perdidos),
```

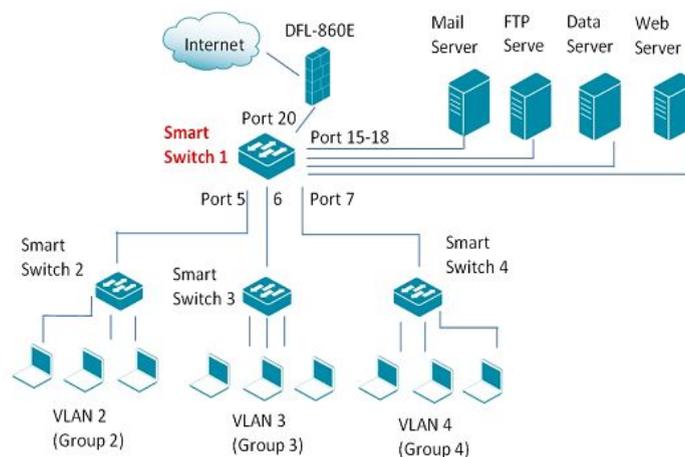
```
C:\Users\Administrador>ping 10.90.30.1
Haciendo ping a 10.90.30.1 con 32 bytes de datos:
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Estadísticas de ping para 10.90.30.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
              (0% perdidos),
```

En resumen:

	VLAN Núm 2	VLAN Núm 3
VLAN Núm 2	hay conectividad	no hay conectividad
VLAN Núm 3	no hay conectividad	hay conectividad

Ejercicio 2. Acceso a recursos compartidos

“En el ejercicio 1 habrás podido observar que un puerto Untagged solo puede pertenecer a una VLAN. ¿Qué solución podemos darle a una red que se encuentre segmentada en varias VLANs pero cuyos equipos necesiten acceder a una zona de servidores y a Internet? Observa la siguiente figura:



Observa que los equipos de la VLAN 2 podrán acceder a los servidores si los puertos 15 al 18 están en la VLAN2 al igual que lo está el puerto 5. El problema es que al ser puerto Untagged no podremos incluirlo en las otras 2 VLANs.

Resumiendo un equipo en una VLAN NO VERÁ EQUIPOS DE OTRA VLAN Para poder acceder a recursos compartidos podemos optar por varias soluciones:

1. un switch de capa 3
2. un router externo nos sirvan de enlace entre las distintas redes.
3. otro mecanismo es que los switches soporten la función VLAN Asimétrica, esto es: permite que varias VLAN circulen por un puerto.

Para dar solución a nuestro problema usaremos la opción tercera, es decir, usaremos VLAN asimétrica. Para ello marca la opción correspondiente en el switch y realiza la siguiente configuración:

VID	VLAN Name	Advertisement	Untagged	Tagged	Forbidden	Delete
1	default	Disabled	05-07,15-18,20			Delete
2	Group2	Disabled	05,15-18,20			Delete
3	Group3	Disabled	06,15-18,20			Delete
4	Group4	Disabled	07,15-18,20			Delete

Realiza pruebas de funcionamiento (dado que tenemos un número limitado de equipos sólo usaremos la VLAN 1, 2 y 3, simula el gateway con un equipo al que tendrán conectividad lógica los equipos de las demás VLANs)”

Solución

Para llevar a cabo esta tarea en primer lugar tenemos que activar la opción de VLAN asimétrica en el apartado 802.1Q VLAN, pulsando en Enabled¹ y guardándolo en Apply:

VID	VLAN Name	Advertisement	Untagged	Tagged	Delete
1	default	Disabled	01-28		Delete

En la VLAN 1 añadiremos como Untagged todos los puertos, los que pertenecen a la VLAN 2 y los que pertenecen a la VLAN 3, además añadiremos el puerto 1 que simulará un servidor; quedaría así:

¹ Al activar la opción de VLAN Asimétrica se resetean los valores de VLANs por lo que si tenías creadas algunas las perderás.

VID Settings Safeguard

VID: 1
 VLAN Name: default

Back Apply

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Ahora pasamos a configurar las otras VLANs, a las que añadiremos el puerto 1:

❖ La VLAN 2 quedaría así:

VID Settings Safeguard

VID: 2
 VLAN Name: Comerciales

Back Apply

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

❖ La VLAN 3 quedaría así:

VID Settings Safeguard

VID: 3
 VLAN Name: Recursos-humanos

Back Apply

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

Resumiendo, en la VLAN 1 se encuentran todos los puertos, en la VLAN 2 se encuentran los puertos del 4-10 y el 1 (servidor) y en la VLAN 3 se encuentran los puertos del 11-16 y el 1 (servidor):

802.1Q Asymmetric VLAN Settings Safeguard

Asymmetric VLAN [Example] Enabled Disabled Apply

Total static VLAN entries: 3 Add

Maximum 256 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01, 04-16		Delete
2	Comerciales	01, 04-10		Delete
3	Recursos-humanos	01, 11-16		Delete

Page 01 Back Next

En el apartado 80.1Q VLAN PVID configuramos a qué VID pertenece cada puerto:

802.1Q VLAN PVID Settings Safeguard

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14
PVID	1	1	1	2	2	2	2	2	2	2	3	3	3	3

Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
PVID	3	3	1	1	1	1	1	1	1	1	1	1	1	1

Apply

Tras la configuración realizamos pruebas de conectividad entre VLAN 1 y VLAN2, entre VLAN 1 y VLAN 3 y entre VLAN 2 y VLAN 3, como ya hemos comprobado en la actividad anterior que entre equipos de la misma VLAN hay conexión, obviaremos hacer ping entre dos PC en la VLAN 2 o dos en la VLAN 3. Estos son los resultados:

❖ Ping entre VLAN 1 y VLAN 2:

```
C:\Users\Marta>ping 10.90.90.91
Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
C:\Users\Administrador>ping 10.90.30.1
Haciendo ping a 10.90.30.1 con 32 bytes de datos:
Respuesta desde 10.90.30.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.30.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.90.30.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

❖ Ping entre VLAN 1 y VLAN 3:

```
C:\Users\Marta>ping 10.90.90.91
Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
C:\Users\Administrador>ping 10.90.30.1
Haciendo ping a 10.90.30.1 con 32 bytes de datos:
Respuesta desde 10.90.30.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.30.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.90.30.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

❖ Ping entre VLAN 2 y VLAN 3:

```
C:\Users\Marta>ping 10.90.90.91
Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Respuesta desde 10.90.30.1: Host de destino inaccesible.
Respuesta desde 10.90.30.1: Host de destino inaccesible.
Respuesta desde 10.90.30.1: Host de destino inaccesible.

Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
```

```
C:\Users\Administrador>ping 10.90.30.1
Haciendo ping a 10.90.30.1 con 32 bytes de datos:
Respuesta desde 10.90.90.91: Host de destino inaccesible.

Estadísticas de ping para 10.90.30.1:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
```

En resumen:

	VLAN 1	VLAN 2	VLAN 3	VLAN 4
VLAN 1	hay conectividad	hay conectividad	hay conectividad	
VLAN 2	hay conectividad	no hay conectividad	no hay conectividad	
VLAN 3	hay conectividad	no hay conectividad	no hay conectividad	
VLAN 4				

Ejercicio 3.- VLAN de administración.

“Para administrar el switch necesitamos tener conectividad IP y también que conectemos el equipo a un puerto del switch habilitado para la administración del mismo. Dicho de otra: podemos securizar el acceso a la gestión del switch habilitando uno o varios puertos en una VLAN específica para su administración. En este ejercicio vas a crear una nueva VLAN de nombre “Administración” y número 10 asignando los puertos 1 y 2. Configura el switch para que esta VLAN sea la de administración (VLAN > 802.1 Management VLAN). Realiza prueba de acceso a la gestión del switch (vía web y ping) desde puertos pertenecientes a la VLAN de administración y desde otros que no sean de gestión.”

Solución

Para cambiar los puertos que tienen acceso a la administración del switch empezaremos por crear una VLAN de VID 10 y nombre Administración a la que añadiremos los puertos 1 y 2:

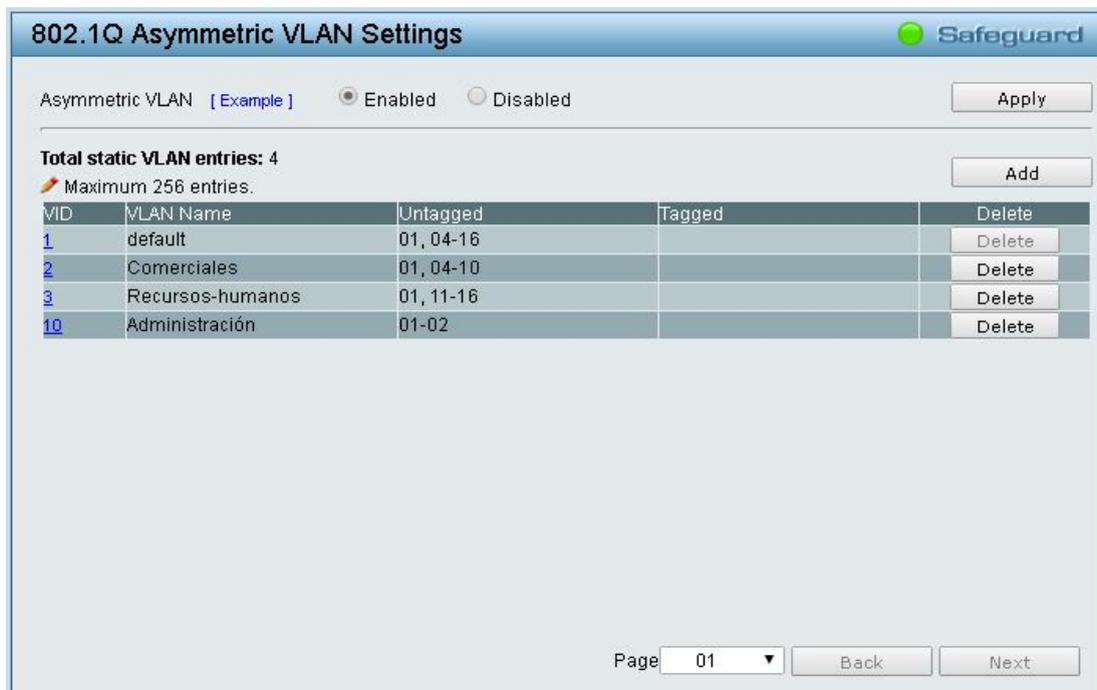
VID Settings Safeguard

VID: 10
 VLAN Name: Administracion [Back] [Apply]

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not member	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>											

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	<input type="radio"/>													
Tagged	All	<input type="radio"/>													
Not member	All	<input type="radio"/>													

De esta manera nuestra configuración de VLANs quedaría así:



A continuación cambiamos los VID asignados a los puerto quedando de la siguiente manera:



Ahora nos dirigimos al apartado 802.1Q Management VLAN, en el que por defecto aparecerá el VID 1 (que en un primer momento incluía todos los puertos del switch) y lo cambiamos activando el Management VLAN seleccionando Enabled y cambiamos en el desplegable el VID 10 (en el que solo se encuentran los puertos 1 y 2):

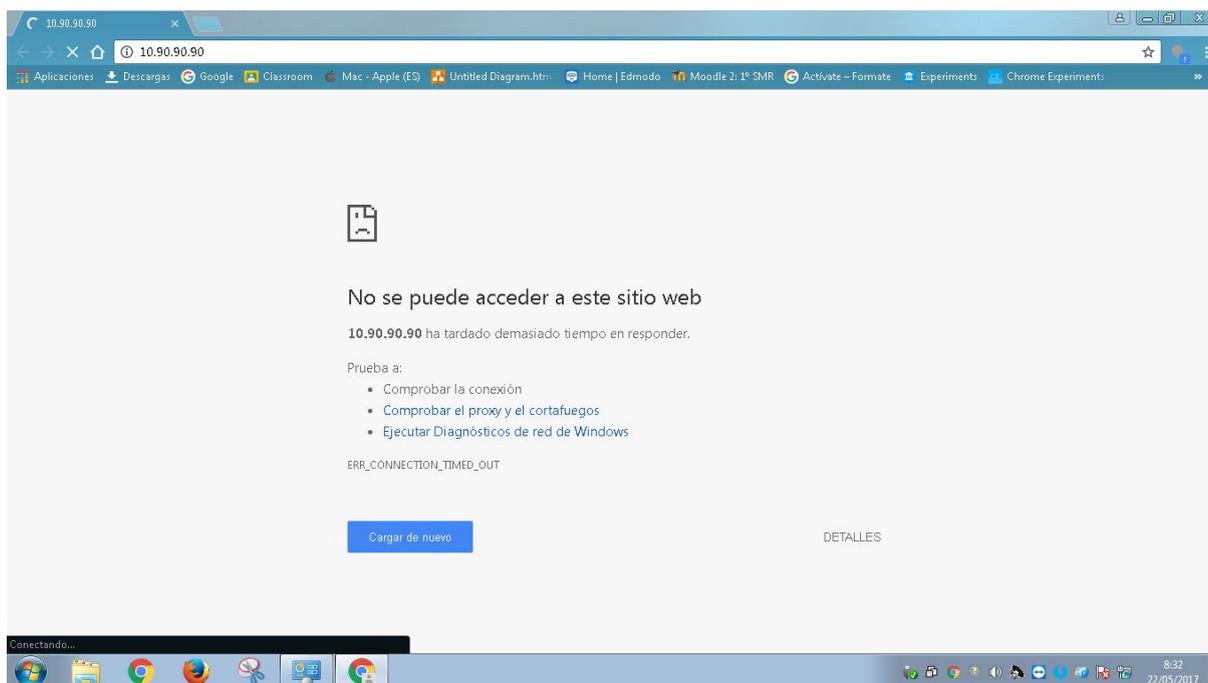


Pulsamos en Apply, ¡CUIDADO!².

Salvamos la configuración y hacemos pruebas para gestionar el Switch, para ello nos conectamos a los puertos 1 y 2 y vemos la siguiente ventana cuando intentamos acceder a la configuración:



Mientras que si nos conectamos desde cualquier otro puerto³ no tendríamos acceso, saldría algo así:

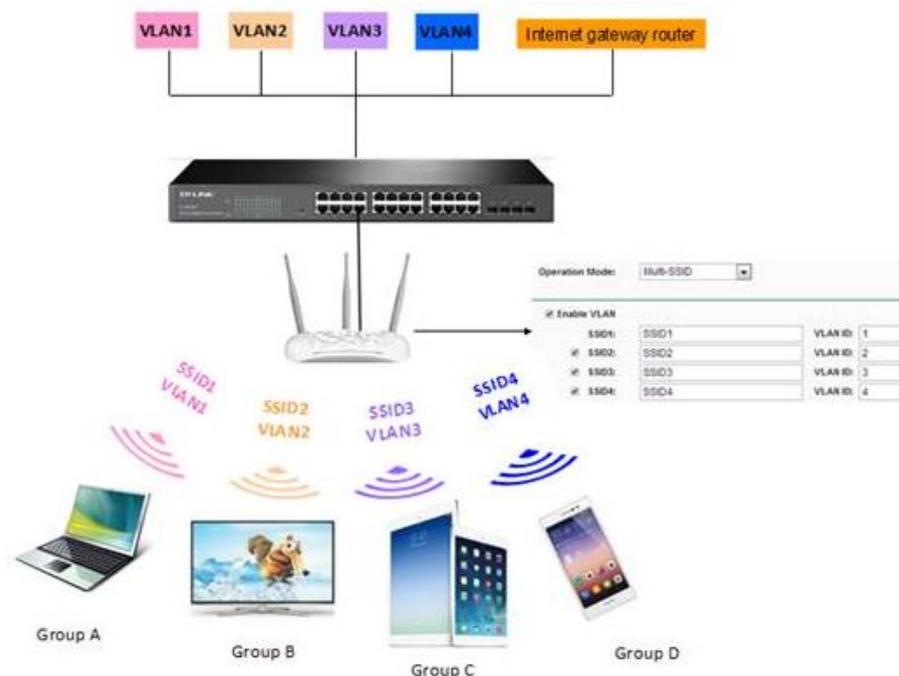


² Si te encuentras administrando el switch desde un puerto que no se encuentre en la VLAN que configuramos como administrativa nos echará de la configuración pero no se guardará; por lo tanto es importante que te encuentres conectado al puerto 1 o 2 en este caso.

³ Si tras configurarlo no cerramos la ventana de configuración y nos cambiamos de puerto, la página cuando intenta recargar nos mostrará un mensaje como si no tuviese conexión, por lo que no nos permitirá configurarlo tampoco.

Ejercicio 4.- Segmentando redes WiFi. Multi SSID.

“Ahora vamos a crear VLANs conectando equipos cableados y equipos WIFI. Para ello vamos a combinar las 2 técnicas vistas de VLANs asimétricas y el uso de un modo WIFI llamado Multi-SSID. La figura siguiente muestra el objetivo de este ejercicio:



Sigue los pasos indicados en el artículo <http://www.tp-link.es/faq-418.html>.

La configuración en el switch debe ser:

Select	VLAN ID	Name	Untagged Ports	Tagged Ports	Operation
<input type="checkbox"/>	1	Default VLAN	1-28		Delete
<input checked="" type="checkbox"/>	2		2,5-8	1	Delete
<input type="checkbox"/>	3		2,7-8	1	Delete
<input type="checkbox"/>	4		2,9-10	1	Delete

Realiza pruebas de funcionamiento (dado que tenemos un número limitado de equipos sólo usaremos la VLAN 1, 2 y 3; simula el gateway con un equipo al que tendrán conectividad lógica los equipos de las demás VLANs):

Solución

Para poner en marcha la actividad propuesta primero tendremos que configurar el WAP en modo Multi-SSID, después lo conectaremos al Switch y finalmente se realizarán pruebas de conectividad entre equipos WIFI y equipos cableados en la misma y en distintas VLANs.

La configuración del Switch de la que partiremos será la siguiente:

802.1Q Asymmetric VLAN Settings Safeguard

Asymmetric VLAN [Example] Enabled Disabled

Total static VLAN entries: 4
Maximum 256 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	03-16		<input type="button" value="Delete"/>
2	Comerciales	03-10		<input type="button" value="Delete"/>
3	Recursos-humanos	03, 11-16		<input type="button" value="Delete"/>
10	Administracion	01-02		<input type="button" value="Delete"/>

Page 01

Como podemos observar tenemos el puerto 3 (en el que conectaremos el WAP) al que acceden las VLANs 2 y 3; además de las VLANs Comerciales y Recursos-humanos (a las que queremos acceder también de forma WIFI) tenemos la VLAN 10 que está configurada como VLAN Administrativa a la que obviamente no queremos tener acceso desde WIFI para evitar problemas de seguridad.

Ahora ya podemos comenzar a configurar el WAP, para ello como aprendimos en tareas anteriores cambiamos la IP del equipo a una que se encuentre en la red del WAP (192.168.0.0/24) y en el buscador ponemos la IP del WAP (192.168.0.254) y nos vamos al apartado Wireless Settings seleccionamos el modo Multi-SSID, activamos el apartado de VLAN y añadimos un SSID por cada VLAN que queramos conectar (la 2 y la 3). La configuración quedaría así:

Wireless Settings

Operation Mode: Multi-SSID ▼

Enable VLAN

SSID1:	<input type="text" value="Equipos VLAN 2"/>	VLAN ID:	<input type="text" value="2"/>
<input checked="" type="checkbox"/> SSID2:	<input type="text" value="Equipos VLAN 3"/>	VLAN ID:	<input type="text" value="3"/>
<input type="checkbox"/> SSID3:	<input type="text" value=""/>	VLAN ID:	<input type="text" value="1"/>
<input type="checkbox"/> SSID4:	<input type="text" value="TP-LINK_AP_7396_4"/>	VLAN ID:	<input type="text" value="1"/>

Channel: Auto ▼

Mode: 11bgn mixed ▼

Channel Width: Auto ▼

Enable Wireless Radio

Enable SSID Broadcast

Save

Ya estaría configurado nuestro WAP, por consiguiente lo conectamos al puerto 3 de nuestro Switch y comenzamos a hacer las pruebas de conectividad:

- ❖ Conectamos el PC2 a la red WIFI “Equipos VLAN 2” y el PC1 por cable a la VLAN 2 (se produce el mismo efecto si conectamos el PC2 a la red WIFI “Equipos VLAN 3” y el PC1 por cable a la VLAN 3):

```

C:\Users\Marta>ping 10.90.90.91

Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Respuesta desde 10.90.90.91: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo=11ms TTL=128

Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 11ms, Media = 6ms
Control-C

```

```

C:\Users\Administrador>ping 10.90.30.1

Haciendo ping a 10.90.30.1 con 32 bytes de datos:
Respuesta desde 10.90.30.1: bytes=32 tiempo=4ms TTL=128
Respuesta desde 10.90.30.1: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 10.90.30.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 4ms, Media = 2ms
Control-C

```

- ❖ Ahora cambiamos el PC1 de puerto y lo conectamos por cable a la VLAN 3:

```

C:\Users\Administrador>ping 10.90.30.1
Haciendo ping a 10.90.30.1 con 32 bytes de datos:
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.

Estadísticas de ping para 10.90.30.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
              (0% perdidos),
C:\Users\Marta>ping 10.90.90.91
Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
              (100% perdidos),

```

En resumen:

	VLAN 1	VLAN 2	VLAN 3	VLAN 4
VLAN 1	hay conexión	hay conexión	hay conexión	
VLAN 2	hay conexión	hay conexión	no hay conexión	
VLAN 3	hay conexión	no hay conexión	hay conexión	
VLAN 4				

Conclusiones

Un switch gestionable tiene muchas funcionalidades, en esta tarea ponemos en marcha el uso de VLANs lo que nos permite de una forma más económica la segmentación de redes en una empresa ya que con un único dispositivo podremos evitar la conexión entre equipos de manera sencilla.

Bibliografía

1. <https://drive.google.com/file/d/0B9zhWCuUq-ZzdnkwLTVNZkxJdUU/view>
2. <https://drive.google.com/file/d/0B9zhWCuUq-ZzUHFkUVFCdC1pNk0/view>
3. <https://drive.google.com/file/d/0B9zhWCuUq-ZzV1FBZE1PLUhJQjQ/view>
4. <https://drive.google.com/file/d/0B9zhWCuUq-ZzZW96MjdTUmRySmM/view>
5. <https://drive.google.com/file/d/0B9zhWCuUq-ZzM3pKUWNiY2IYck0/view>
6. <http://www.tp-link.es/faq-418.html>
7. <http://www.blogcisco.com/blog/2015/12/16/cisco-vlan-ventajas-y-tipos/>
8. <https://sites.google.com/site/isaacivantorresgonzalezvlan/home/ventajas-de-las-vlan>
9. <http://ecovi.uagro.mx/ccna2/course/module3/3.1.1.2/3.1.1.2.html>