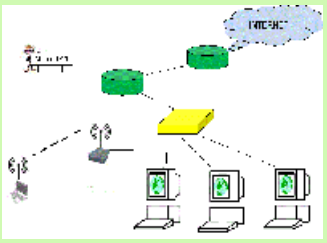
Configuración de redes virtuales.

Caso práctico



El aspecto de la red local de Tomás es hoy muy diferente de cuando renovó uno de los ordenadores y no sabía lo que era un bit. En la red actual tiene tres PC, un ordenador portátil, un punto de acceso, un switch configurable y dos routers.

— ¿Te funciona bien la red? — Le ha preguntado su amiga Antonia— .

— Correctamente. —Ha respondido orgulloso Tomás— .

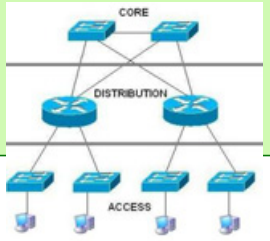
Antonia, que sabe bastante de redes, le ha aconsejado que aunque la red funcione correctamente, es conveniente para prevenir posibles fallos y gestionar bien el tráfico que circula por ella, hacer un seguimiento de su funcionamiento siguiendo algún patrón ya predeterminado.

— Mira el diseño desde el punto de vista **jerárquico**, lo emplean empresas importantes.

Investigando, ha encontrado que aparte de poder dividir la red en niveles como lo hacen OSI y TCP/IP existen otros criterios para el diseño de redes más sencillos de ver, como por ejemplo el "Sistema jerárquico de tres niveles".

El diseño de redes locales a tres capas (núcleo, distribución y acceso) (I).

Caso práctico



— Manos a la obra, veamos de qué va esto del **sistema de tres niveles**.

Tomás ha empezado a buscar información y casi toda la que encuentra viene en inglés, no es que sea un políglota pero parece que no es muy complicado de entender.

El modelo jerárquico de diseño de redes establece que existen las siguientes capas o niveles:

- **Acceso.**
- **Distribución.**
- **Núcleo.**

El modelo jerárquico de tres niveles tiene, entre otras, las ventajas que con él es más fácil diseñar, implementar, mantener y escalar la red; además de hacerla más confiable. Cada una de las capas tiene funciones bien determinadas desde un punto de vista lógico más que físico. Esta división en distintas capas no implica que necesariamente los dispositivos que intervienen sean diferentes en cada una de las capas. Se pueden tener distintos dispositivos en una sola capa o un mismo dispositivo realizando funciones relativas a más de una capa.

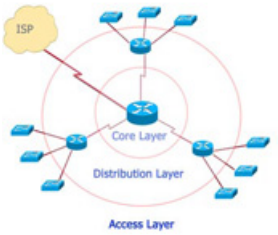
La capa **Acceso** es la capa en la que se sitúa el usuario final y tiene como objetivo **facilitar el acceso al resto de la red**. En esta capa aparecen dispositivos como PC, routers, switches, concentradores, puntos de acceso, teléfonos IP o impresoras, todos los dispositivos que están al alcance de los usuarios. En esta capa se utilizan conmutadores de nivel 2 para conectar los dispositivos a la capa de distribución.

La capa **Distribución** es la encargada de **controlar el flujo de tráfico de la red** mediante el enrutamiento entre las **LAN virtuales** (VLAN) definidas en la capa de acceso.
Cuando una red tiene dos o más protocolos de enrutamiento, RIP e IGRP, la información entre los diferentes dominios de enrutamiento es compartida, o redistribuida, en la capa de distribución. En esta capa se utilizan a veces conmutadores de nivel 3.

En la capa Distribución es donde se agrega el cableado en racks específicos y se usan los switches para crear separaciones de grupos y redes, es donde se aplican las políticas de red como pueden ser firewalls, listas de acceso, selección de rutas y/o QoS (calidad de servicio).

La capa **Núcleo** es la red troncal, es la capa donde se da la mayor velocidad de interconexión. En esta capa se incluye la gama alta de cables de alta velocidad, tales como cables de fibra.
El objetivo de esta capa es **proporcionar una estructura de transporte optimizado y fiable** para enviar tráfico a velocidades muy altas.

El diseño de redes locales a tres capas (núcleo, distribución y acceso) (II).



Cada capa (núcleo, distribución y acceso) tiene una función bien definida, cada nivel exige un conjunto diferente de características para los enrutadores, conmutadores y tipos de enlaces.

Como se puede ver en la figura, en el diseño jerárquico de la red en tres niveles, los dispositivos utilizados pueden ser iguales, lo que si difiere bastante son los protocolos utilizados o las tecnologías necesarias en cada uno de los ellos.

Otra conclusión que se puede sacar es que cuanto más lejos del usuario (capa de acceso), más cerca del ISP (capa núcleo). Además se puede ver en las figuras anteriores como la capa encargada de encontrar el mejor camino hacia la red WAN es la capa de distribución.

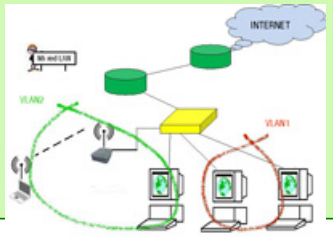
Autoevaluación

¿Qué capa del modelo de diseño jerárquico controla el flujo del tráfico de la red con políticas y delimita los dominios de broadcast al ejecutar funciones de enrutamiento entre las LAN virtuales (VLAN)?

- Aplicación.
- Acceso.
- Distribución.
- Red.

Implantación y configuración de redes virtuales.

Caso práctico



— ¿Utilizas redes virtuales Tomás? Con esos equipos que tienes en tu casa podrías configurarlas. — Esto es lo que Antonia ha comentado a su amigo Tomás. Nuestro personaje no sale de su asombro, cada día tiene que aprender algo nuevo. Afortunadamente hay mucha bibliografía sobre las redes virtuales por lo que Tomás se ha puesto otra vez a estudiar, ahora es el turno para las VLAN (Virtual Local Area Network).

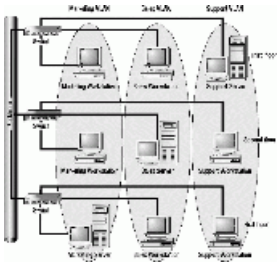
Una red LAN se caracteriza porque los dispositivos que forman parte de ella comparten todos los recursos disponibles y uno de estos recursos es el **ancho de banda de la red**. A medida que la red va incorporando dispositivos, el ancho de banda disponible para cada uno va disminuyendo. Para solucionar este problema se utilizan los concentradores, conmutadores y routers. Y para mejorar el rendimiento se pueden utilizar las VLAN tanto en conmutadores de nivel 3, como en routers.

Se puede definir una Red de Área Local Virtual (VLAN) como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, pertenecen a una misma LAN. Esto se puede conseguir mediante la configuración de los dispositivos de interconexión, ya sean conmutadores o routers.

Las VLAN se pueden crear por:

- **Puerto.**
- **MAC.**
- **Protocolo.**
- **Subredes IP.**
- **Binding.**
- **DHCP.**

Ejemplo: En la imagen se ve como hay tres redes virtuales (Sales, Marketing, Support) y cada una de ellas tiene dispositivos situados en lugares físicos diferentes unidos a través de una red troncal. Es un ejemplo claro de cómo funciona una red VLAN, físicamente pertenecen a redes diferentes y lógicamente se pueden agrupar en una misma red local virtual.



Tipos de VLAN.

Las VLAN se pueden clasificar atendiendo a varios criterios.

Entre los tipos de VLAN más importantes están:

VLAN de puerto central: Todos los nodos de la VLAN se conectan a un mismo puerto del router o del conmutador.

VLAN estáticas: Los puertos se asignan a los equipos de antemano, se configura puerto por puerto.

VLAN por puerto: También se denominan VLAN de Nivel 1. Se asignan los puertos a una determinada VLAN. Por ejemplo, los puertos 1, 3, 5 y 7 a la VLAN1, los puertos 2, 4, 6 y 8 a la VLAN2.

VLAN por direcciones MAC: Denominadas VLAN de Nivel 2. En este caso se emplean las direcciones MAC de los elementos que formarán las VLAN. Cada VLAN estará compuesta por una serie de direcciones MAC.

VLAN por protocolo: Este tipo de VLAN se forma discriminando los elementos según el protocolo que se esté utilizando. Por ejemplo, una VLAN estaría formada por los equipos que utilizasen el protocolo IP y otra por los equipos que utilizasen IPX.

VLAN por dirección IP: Llamadas VLAN de nivel 3. El discriminante en este caso es la dirección IP de los elementos que forman la red. Se utiliza la dirección de red para crear las distintas VLAN. Por ejemplo, todos los equipos con dirección de red 10.0.0.0 constituirán la VLAN1.

VLAN por nombre de usuario: Los equipos se agrupan en VLAN dependiendo de una autenticación con un nombre de usuario.

VLAN dinámicas: También se llaman DVLAN (Dynamic Virtual Local Area Network). Este tipo de redes virtuales utilizan para su configuración las direcciones MAC, los protocolos y las direcciones lógicas. Los puertos de los dispositivos que son capaces de gestionar estas redes autoconfiguran los puertos para que un equipo pueda unirse a una determinada VLAN.

Autoevaluación

Una VLAN es un espacio dentro de una red LAN. Las VLAN pueden proporcionar dominios de difusión diferentes dentro de una misma red LAN. Teniendo en cuenta el párrafo anterior, si en una red LAN se tiene instalado un dispositivo como el router que es capaz de generar diferentes dominios de difusión ¿Significa esto que existe alguna red VLAN?

- ○ Sí. Porque el router trabaja a nivel 2.
- ○ Sí. Ya que el router posee una parte WAN y una parte LAN.
- ○ Sí. Existe la VLAN predeterminada.
- ○ Sí. Aunque solo podría darse en la parte WAN.

¿Cómo se crea una VLAN?

Las VLAN se pueden crear en conmutadores y en routers, sin definir ninguna VLAN, un conmutador considera que todas sus interfaces están en el mismo dominio de difusión, en la VLAN 1. Por defecto, en el nivel jerárquico de acceso, las interfaces envían y reciben datos en esta única VLAN. Los pasos para configurar una VLAN distinta a la predeterminada son:

- **Entrar al modo de configuración global.**
- **Utilizar el comando vlan para crear la vlan Nº.**

Si se desea configurar una VLAN para cada una de las interfaces de acceso:

- **Entrar en el modo de configuración específico de cada interfaz.**
- **Utilizar el comando switchport access vlan Nº.**

La mayoría de los dispositivos que son capaces de soportar redes virtuales VLAN, tienen la capacidad de configuración vía web. En este caso, bastaría con seleccionar los puertos que fueran a formar parte de la VLAN correspondiente.

Diagnóstico de incidencias en redes virtuales.

Caso práctico

— Todo lo que no mejora, empeora.
Siguiendo el consejo de Antonia, Tomás ha decidido crear dos VLAN en su red, una para el punto de acceso y otra para los ordenadores conectados por cable. Después de aprender los comandos de configuración y crear las VLAN ha descubierto que su red ha dejado funcionar.
— ¡Antonia, vaya consejos que me das, has conseguido que mi red deje de funcionar con esto de las VLAN!
— No te preocupes que seguro que tienes algún pequeño fallo de configuración, ahora voy y te echo una ojeada.

Antonia ha revisado la configuración hecha por Tomás y ha descubierto que Tomás había dejado las interfaces en **modo down**, la solución ha sido sencilla, ejecutar el comando **no shutdown**. — Para que esto no te vuelva a ocurrir te voy a enseñar cómo prevenir alguno de estos errores.

En las redes virtuales se pueden dar múltiples incidencias, y la mayoría están relacionadas con la mala configuración hecha por parte del usuario. La comprobación elemental es probar la conectividad entre los elementos que forman la VLAN, por ejemplo, con el comando ping. Si la conectividad existe hay que pasar a indagar en la configuración con otros comandos, el comando más básico que se tiene para poder verificar la configuración es el comando **show**.

PAR05#show vlan

La salida de este comando nos da una estadística de las VLAN creadas y los parámetros que tienen configurados.
Las VLAN más comunes son las creadas **"por puerto"**, por tanto una de las primeras comprobaciones que se tienen que realizar es la configuración de los puertos.

PAR05#show interface FastEthernet0/1 switchport

Con la línea de comandos anterior verificamos la configuración de la interfaz 0/1. El aspecto que tiene la salida de este comando es el siguiente.

Como se puede ver en la imagen, la salida del comando nos muestra los parámetros de interfaz fastethernet0/1, como la identificación (Fa0/1), el estado (down), la VLAN a la que pertenece (VLAN0002) y otros.

Problemas en la negociación VLAN.

En ocasiones, las velocidades configuradas en los puertos del conmutador son diferentes a las velocidades de las tarjetas de red de los equipos conectados a esos puertos y que forman parte de las VLAN.

Un símil con el atletismo sería la carrera de relevos, en la que la clave está en la sincronización de las velocidades de los atletas para que haya un traspaso del testigo con éxito. Ambos corredores deben establecer una velocidad con la que el paso del testigo de uno a otro no produzca la caída de este y aún no produciéndose, debe permitir que el traspaso sea lo más rápido posible para poder ganar la carrera.

El mensaje que indica que existe una mala negociación suele contener las palabras **%LINK-4-ERROR**.

Para solucionar este problema se debe comprobar la configuración de las tarjetas de red.

En el sistema operativo que se utilice se accederá a las propiedades de la tarjeta de red y en ellas a la opción "Tipo de conexión". En esta opción se podrá configurar la velocidad y el tipo de comunicación dúplex.

Una vez comprobada la configuración de la tarjeta, se debe comprobar la configuración del conmutador. Para ello emplearemos el comando show.

```
PAR05#show running-config interface fastethernet0/1
```

Se comprueba que el tipo de comunicación dúplex es diferente y la velocidad también, se puede utilizar el modo auto en las dos partes o establecer de manera manual las configuraciones para que sean compatibles.

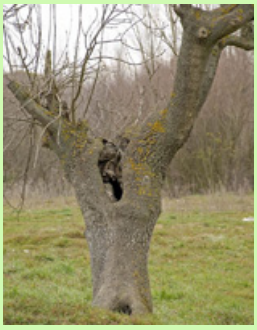
Autoevaluación

Dada una red en la que existen varias VLAN definidas, los equipos de esa red:

- ○ Están todos en una misma VLAN por defecto.
- ○ Aquellos equipos que pertenecen a alguna VLAN están en la predeterminada también.
- ○ Se puede obtener respuesta de todos los equipos si ejecuto el comando ping desde cualquiera de ellos.
- ○ No existe ningún equipo que no pertenezca a alguna VLAN.

Definición de enlaces troncales en los conmutadores y «router». El protocolo IEEE802.1Q.

Caso práctico



— ¿Otra vez tú? ¿Qué ocurre ahora?
— Pues que lo que me arreglaste funcionaba, pero que me he puesto a configurar más VLAN y ya sabes que tengo un router de por medio y no me funciona la conexión a Internet.
El arreglo de Antonia hizo que sus equipos formaran parte de las VLAN creadas, pero Antonia se olvidó del detalle de hacer que las dos redes virtuales salieran a Internet utilizando el mismo camino entre el conmutador y el router.
— ¡Se me olvidó definirte el enlace troncal del conmutador! — ¿Enlace troncal?
— Claro, como las ramas de un árbol siempre confluyen en el tronco, las VLAN deben confluir en un mismo camino para poder llegar hasta tu router y alcanzar Internet.
Tomás aprenderá hoy que es eso de **enlace troncal**. A este paso, su cerebro se va a deforestar con tanto esfuerzo diario.

Un enlace troncal es la conexión física y lógica entre conmutadores o entre conmutadores y enrutadores, a través de la cual viaja el tráfico de red. Este enlace puede admitir el tráfico de varias VLAN, para ello tiene la característica de agrupar varios enlaces lógicos en un solo enlace físico.
El enlace troncal es un puerto del conmutador definido con esta capacidad y debe ser diferente a los puertos que funcionan como conexión de los dispositivos que forman las VLAN. Para definir un puerto como enlace troncal se utiliza el comando **switchport** desde el modo de configuración específico de la interfaz.

```
PAR05(config-if)#switchport mode trunk
```

La función de este puerto es gestionar todo el tráfico que le llegue para poder enviarlo a otro conmutador o a otro router por lo que a medida que aumenta el número de redes VLAN, el tráfico se puede hacer más lento. Para solucionar este problema el conmutador puede utilizar dos mecanismos:

- **Filtrado de tramas.**
- **Etiquetado de tramas.**

Estos dos mecanismos utilizan protocolos cuya función es:

- **Gestionar todas las tramas que llegan procedentes de diferentes VLAN y enviarlas por un mismo canal físico.**
- **Enviar cada trama que recibe al puerto correspondiente.**

Etiquetado de tramas. Protocolo IEEE802.1Q.

El etiquetado de tramas, como se puede adivinar, consiste en añadir una etiqueta identificativa a la trama para identificar la VLAN a la que pertenece. Existen varios métodos para ello, pero los más destacados son:

- **ISL (Inter Switch Link).**
- **Protocolo IEEE802.1Q.**

El **ISL** es un protocolo **creado por Cisco Systems** y el **802.1Q** es el protocolo **creado por** el organismo de estandarización **IEEE** para las tramas Ethernet. El protocolo 802.1Q también recibe el nombre de trunking o **Dot1q**.

El etiquetado de la trama se hace antes de salir del enlace troncal y se elimina en el conmutador destino antes de reenviar la trama al puerto correspondiente. Este etiquetado se hace a nivel enlace del modelo OSI, consume pocos recursos y agiliza mucho el tráfico en el enlace entre conmutadores para varias VLAN definidas.

El mecanismo que utiliza IEEE802.1Q es introducir un encabezado en la trama Ethernet después de la dirección MAC origen, donde se especifica la VLAN-ID con 12 bits.

En la imagen se puede observar como el protocolo 802.1Q no encapsula la trama Ethernet, sino que intercala sus bits en la trama.

Los componentes de la trama 802.1Q son:

- **El campo TPID (Tag Protocol ID): Compuesto por 2 bytes, en las tramas Ethernet se identifica por el valor en hexadecimal 0x8100.**
- **El campo TCI (Tag Control Information): Compuesto por 2 bytes.**
- **Priority User: Son 3 bits que establecen la prioridad del servicio (QoS).**
- **CFI (Canonical Format Indicador): Es 1 bit que indica el sentido de lectura de la trama.**
- **VLAN-ID: Son 12 bits que identifican a cada una de las VLAN. Con este campo se pueden llegar a identificar 2^{12} VLAN (4096) distintas.**

Autoevaluación

La diferencia entre ISL y 802.1q es que:

- No hay diferencia, conceptos idénticos.
- ISL es compatible con todo tipo de redes.
- 802.1q solamente es compatible con redes Cisco.
- 802.1q es compatible con la mayoría de las redes e ISL solo con redes Cisco.

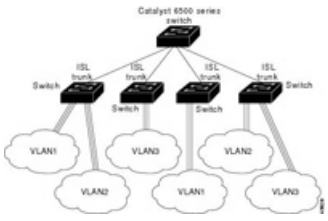
ISL (Inter Switch Link).

ISL (enlace entre switches) es un protocolo trunking propiedad de Cisco Systems que se puede instalar en todas las redes Cisco.

A diferencia del 802.1Q, este protocolo encapsula cada trama añadiendo otra cabecera de 26 bytes y un nuevo CRC de 4 bytes al final. Otra diferencia con el 802.1Q, es que encapsula el tráfico no marcado, lo que se conoce como VLAN nativa.

La VLAN nativa puede ser modificada, para otra VLAN que no sea la VLAN 1, con el siguiente comando:

PAR05(config-if)#switchport trunk native vlan vlan-id



La VLAN nativa es la red VLAN a la que pertenecería un puerto antes de ser configurado como troncal. Solamente se puede tener una VLAN nativa por puerto.

Así como el protocolo 802.1Q puede ser utilizado en todas las redes, el ISL solamente se puede utilizar en redes Cisco y actualmente hay dispositivos de esta marca que ya no lo soportan. Como se puede ver en la figura, ISL tiene el mismo cometido que 802.1q, definir el camino que han de seguir las tramas de las diferentes VLAN a través de los dispositivos de interconexión de la red.

Por defecto, los puertos de un conmutador están configurados en modo acceso, para configurar un puerto en modo trunk, junto con el comando se utilizan los siguientes modificadores para poder escoger el tipo de encapsulado:

- **ISL: Se encapsulan y etiquetan todas las tramas.**
- **Dot1q: Etiqueta todo excepto la VLAN nativa (protocolo 802.1Q).**
- **Negotiate: Se negocia el tipo favoreciendo a ISL.**

El comando **switchport** se utilizaría en modo de configuración específico con cada uno de estos modificadores:

PAR05(config-if)#switchport trunk encapsulation {isl|dot1q|negotiate}

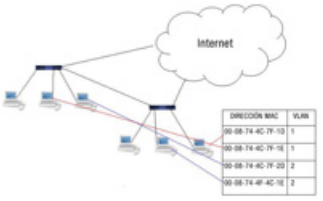
Autoevaluación

El siguiente comando:

PAR05(config-if)#switchport trunk native vlan 13

- Convierte el puerto 13 en puerto troncal.
- Convierte en VLAN nativa la VLAN 13.
- Esta orden está mal construida porque no se puede emplear trunk y native al tiempo.
- Con esta orden se vuelve el puerto 13 a su estado original, deja de ser troncal.

Filtrado de tramas.



El método de filtrado de tramas se basa en **examinar la información** acerca de la trama (direcciones MAC, protocolos).

Cada uno de los switches contienen una tabla, que se conoce como **tabla de filtrado**, con información de los equipos (direcciones MAC). Estas tablas se comparten con los demás conmutadores a través de la red principal.

Cada uno de los registros de las tablas se comparan con las tramas que entran al conmutador, después de comparar, el conmutador opera de una u otra manera, permitiendo o denegando el paso de las tramas.

La situación en la que se dan las VLAN suele ser muy parecida a la situación de la figura anterior. Varios equipos conectados a conmutadores diferentes y los conmutadores conectados a una red WAN (utilizando un router, aunque no aparezca en la figura). Con este planteamiento, el filtrado de tramas utiliza en cada conmutador una tabla similar a la que aparece en la figura. Las tablas relacionan las direcciones MAC de los equipos y la VLAN a la que pertenecen y además tienen la particularidad de que todos los conmutadores las conocen.

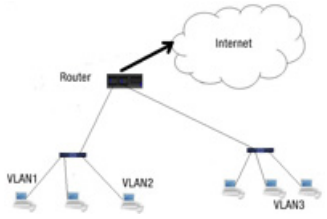
Cuando un paquete entra en uno de los switch, este compara la información de esta trama con el contenido de las tablas y discrimina el tráfico según la VLAN a la que pertenezca.

Autoevaluación

El filtrado de tramas utiliza:

- El encapsulado Dotq1.
- ISL.
- El protocolo Negotiate.
- Tablas que contienen direcciones físicas de equipos de la red.

Subinterfaces.



Las redes en las que se utilizan VLAN tienen una disposición física como la de la figura siguiente:

En esta situación, lo lógico sería disponer de tantos canales físicos entre los conmutadores y el router como VLAN hubiera definidas. Pero la realidad es que las redes que tienen varias VLAN deben utilizar un mismo enlace troncal para comunicarse con el router, es decir, utilizar una interfaz del router única.

Para conseguir que todas las VLAN utilicen la misma interfaz física del router, el router admite

varias interfaces lógicas en los enlaces físicos individuales. Una interfaz identificada por FastEthernet0/0 puede admitir tres interfaces virtuales identificadas como:

FastEthernet0/0.1
FastEthernet0/0.2
FastEthernet0/0.3.

Estas **interfaces virtuales** reciben el nombre de **subinterfaces, interfaces lógicas** dentro de una interfaz física. Cada una de estas subinterfaces admite**una VLAN diferente** y se le asigna una dirección IP. Para que haya comunicación entre los dispositivos de cada VLAN todos deben tener una dirección IP del tipo de la dirección de la subinterfaz. Si la subinterfaz FastEthernet 0/0.1 tiene asignada la dirección IP 192.168.1.1, los dispositivos que se comunican con ella son los que utilizan las direcciones 192.168.1.2, 192.168.1.3 y 192.168.1.4. Para definir una subinterfaz en una interfaz física se deben seguir los siguientes pasos:

- **Identificar la subinterfaz.**
- **Definir el encapsulamiento de la VLAN.**
- **Asignar una IP a la interfaz.**

Las órdenes siguientes configuran una subinterfaz, le asignan la VLAN1 llamándola ASIR2011, definen el encapsulamiento 802.1q y asignan la dirección 192.168.1.1 a dicha subinterfaz.

```
PAR05(config)#interface FastEthernet 0/0.1
PAR05(config-subif)#description ASIR2011 VLAN1
PAR05(config-subif)#encapsulation dot1q 1
PAR05(config-subif)#ip address 191.168.1.1 255.255.255.0
```

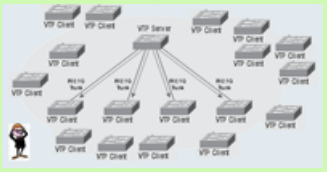
Autoevaluación

¿Qué elemento necesitamos cuando se utiliza una interfaz del router como enlace entre redes VLAN?

- Una interfaz física por VLAN.
- Una interfaz física por cada subinterfaz.
- Un enlace troncal por cada VLAN.
- Una red o subred por cada VLAN.

Protocolos para la administración centralizada de redes virtuales; el protocolo VTP.

Caso práctico



— ¡Pues funciona!
— Pues claro que funciona Tomás, eres un incrédulo.
— Claro que, es un poco lío lo de configurar uno por uno cada conmutador.
— ¡Más problemas! Vas a acabar conmigo.
— Lo que digo, es que si tengo que repetir todos estos pasos cada vez que cambie de conmutador me voy a eternizar ¿En las empresas grandes lo hacen igual?
Antonia ha conseguido que las VLAN de Tomás funcionen pero está ya un poco cansada de tanto trabajo extra.
— No, en las empresas grandes, donde hay muchos conmutadores, utilizan mecanismos que centralizan la administración.
— Es lo último que te pido ¿Me enseñas?
— Bueno, te hablaré del protocolo **VTP**.
Tomás va conocer el protocolo VTP utilizado para gestionar una red con varias VLAN de manera centralizada.

Si la red está formada por varios conmutadores con varias VLAN definidas, se hace necesaria alguna herramienta que permita **administrar** con garantías dicha red, asegurando el buen funcionamiento aunque se eliminen o agreguen dispositivos o configuraciones VLAN.

La solución de la gestión pasa por **centralizar tareas**, de lo contrario, es necesaria la intervención manual en cada conmutador y en cada VLAN.

El protocolo VTP permite la **gestión centralizada** de la red creando los **dominios VTP**. Un dominio VTP es un switch o varios, interconectados, que comparten un mismo entorno VTP. Cada switch solamente puede estar en 1 dominio VTP.

El uso del protocolo VTP soluciona los problemas derivados de la escalabilidad de la red y de las modificaciones de las VLAN que forman parte de ella. Cualquier cambio que se produce en la red se comunica a todos los integrantes del dominio VTP gracias al protocolo VTP. Los mensajes del protocolo VTP viajan encapsulados con los mensajes del protocolo de enlace troncal (ISL, IEEE802.1q).

Para saber más

Como curiosidad puedes ver este vídeo de cisco donde se explica el funcionamiento de VTP.

VTP

Operación VTP.

El protocolo VTP opera con mensajes entre los componentes de la red a través de los enlaces troncales. Los elementos que forman parte de un mensaje VTP son:

a. Versión de protocolo VTP.
b. Tipo de mensaje.
c. Longitud del nombre de dominio de administración.
d. Nombre del dominio de administración.

Los conmutadores de la red son los que emiten y reciben los mensajes y pueden actuar dentro del dominio de los siguientes modos:

- **Servidor.**
- **Cliente.**
- **Transparente.**

Cuando un conmutador se configura en **modo servidor** (es el estado por defecto), puede crear, modificar y suprimir redes VLAN y otros parámetros que afecten al dominio VTP. Las configuraciones que se hagan en un conmutador que funcione en este estado se guardan en memoria NVRAM.

El **modo cliente** por contra no permite cambiar la configuración de las VLAN, ni los parámetros que afecten al dominio. En este estado los conmutadores reciben los mensajes pero no pueden hacer cambios. Los puertos de un switch cliente no se pueden utilizar en una nueva VLAN antes de que el servidor VTP notifique al switch cliente la creación de la VLAN.

El otro modo en el que pueden funcionar los conmutadores es el **modo transparente**. En este modo el conmutador puede crear, suprimir o modificar VLAN, pero los cambios no se transmiten a otros conmutadores del dominio, afectan solo al switch local.

Funciones posibles de los conmutadores en un dominio VTP

	SERVIDOR	CLIENTE	TRANSPARENTE
Enviar mensaje VTP	Si	Si	No
Recibir mensaje VTP	Si	Si	No
Crear VLAN	Si	No	Si (local)

En la tabla anterior se puede ver un resumen de cómo actúan los conmutadores dependiendo de su configuración como servidor, cliente o transparente en un dominio VTP.

Autoevaluación

Tener un solo switch en nuestra red o tener varios switches que pertenezcan todos a la misma VLAN, es una situación que:

- Exige utilizar el protocolo VTP.
- No necesita del protocolo VTP.
- VTP nunca funcionaría en una situación así.
- No existe ninguna red en la que todos los conmutadores pertenezcan a la misma VLAN.

Configuración de VTP.

La configuración del protocolo VTP se puede estructurar en varios pasos:

- **Determinar el número de versión del VTP que se utilizará.**
- **Decidir si el conmutador será parte de un dominio existente o se creará uno nuevo.**
- **Elegir el modo de actuación del switch.**

Para empezar se especifica el modo de la base de datos VLAN y el número de versión VTP.

```
PAR05#vlan database
PAR05(vlan)#vtp v2-modo
```

Las versiones 1 y 2 de VTP son incompatibles dentro de un mismo dominio. Es recomendable no habilitar la versión 2 a menos que se esté seguro de que todos los conmutadores en el dominio soporten dicha versión. Si decidimos crear un nuevo dominio:

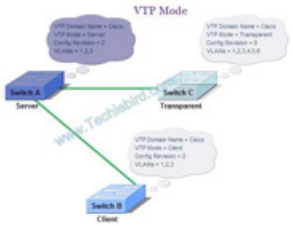
```
PAR05(vlan)#vtp domain PAR05
```

Para establecer el modo del switch se utiliza:

```
PAR05(vlan)#vtp {client|server|transparent}
```

En modo privilegiado se utiliza el comando show para ver las estadísticas de la configuración VTP.

```
PAR05#show vtp counters
PAR05#show vtp status
```



Debes conocer

En el siguiente enlace podrás ver un ejemplo de configuración VTP para una red como la de esta figura.

VTP.

Autoevaluación

¿Qué afirmación es verdadera cuando VTP está configurado en una red que incorpora VLAN?

- VTP sólo es compatible con el estándar 802.1Q.
- Un switch configurado para VTP puede pertenecer a más de un dominio VTP.
- El VTP comunica dinámicamente las adiciones, eliminaciones y modificaciones de la VLAN a todos los switch del mismo dominio VTP.
- Las publicaciones VTP se transmiten por enlaces de acceso a otros switches.

Tipos de mensajes VTP.

Cuando se instala el protocolo VTP en una red, cada puerto de cada conmutador publica en todo el dominio de administración las VLAN

que conocen y los parámetros conocidos de estas. Gracias a esto, los elementos del dominio conocen todas las modificaciones que se producen.

Los mensajes que emiten los puertos son:

- **Creación y eliminación de VLAN.**
- **Suspensión o activación de VLAN.**
- **Cambio de nombre de VLAN.**
- **Cambio de unidad máxima de transmisión de VLAN.**

A su vez estos mensajes pueden ser de tres tipos:

- **Petición de aviso.**
- **Aviso de configuración.**
- **Resumen de configuración.**

Una **petición de aviso** es un mensaje que utilizan los conmutadores cliente para poder actualizar la configuración existente en su dominio. La respuesta que espera el conmutador debe venir del conmutador configurado como servidor.

El servidor envía un **mensaje de configuración** con todos los parámetros necesarios para la configuración VTP, entre los que se encuentra el asegurarse de que todos los conmutadores que forman parte del dominio estén configurados con la misma versión de configuración de VLAN. Para cumplir esto, el servidor envía mensajes en intervalos de tiempos relativamente pequeños aunque no haya habido cambios.

Los mensajes de **resumen de configuración** los envían los servidores de los dominios VTP generalmente cada cinco minutos.

Estos mensajes están compuestos principalmente de:

- **Número de revisión de configuración. Es un contador que se incrementa cada vez que se actualiza la configuración VTP. Si se resetea el conmutador este valor se pone en cero.**
- **Identificación actualizada. Dirección IP del conmutador que incrementó por última vez el número de revisión de configuración.**
- **Tiempo de la última actualización.**

Cuando un switch recibe un mensaje de resumen de configuración, compara el nombre del dominio VTP con el suyo, si es diferente, descarta el mensaje. Si pertenece al mismo dominio, compara el número de revisión, si es menor o igual que el suyo, descarta el mensaje, en caso contrario (mayor) envía un mensaje de petición de aviso para obtener una nueva configuración.

Autoevaluación

¿Qué pasaría si se incluyera un nuevo switch en una red con dominio VTP con un número de revisión de configuración superior al del servidor del dominio?

- Este switch podría mandar ese número a los demás conmutadores y destruir la configuración VTP que tienen.
- Esta situación no se puede dar.
- El switch configurado como transparente mandaría un mensaje de error al servidor VTP.
- El servidor VTP inicializaría el número de revisión de configuración a 0.

Anexo.- Licencias de recursos.