

UD3. VLANs

Índice

Introducción.....	2
El problema del tráfico broadcast.....	2
Tipos de VLAN.....	4
Enlaces troncales.....	6
ISL (Inter-Switch Link Protocol).....	7
IEEE 802.1Q.....	7
Tipos de VLAN por su asignación de puertos.....	8
VLAN nativa.....	9
Tramas etiquetadas en la VLAN nativa.....	9
Tramas sin etiquetar en la VLAN nativa.....	9
Enlace troncal en VLAN de Voz.....	10
Protocolos.....	11
DTP.....	11
VTP.....	12
Ejemplo configuración VTP.....	13
Procedimiento para configurar VTP.....	14
configuración de puertos troncales y de acceso.....	14
Configuración de VTP.....	14
Creación de las VLAN.....	15
Asignación de puertos a las VLANs.....	15

Introducción

El problema del tráfico broadcast

El consumo de CPU por tráfico unicast en una red es mínimo pues la tarjeta de red descarta el que no es para nosotros, sin pasarlo a la CPU.

Los paquetes broadcast en cambio han de ser tratados siempre por la CPU, pues en principio su contenido puede ser relevante.

Los conmutadores no filtran el tráfico broadcast, de modo que éste se transmite hasta los últimos rincones de la LAN, además los paquetes broadcast suelen ser pequeños (64 bytes), lo cual agrava el problema cuando el caudal es elevado. 5000 pps (paquetes por segundo) de tráfico broadcast consumen en torno a un 10% de CPU en un Intel T2400 a 1,83 GHz

En cualquier LAN hay normalmente diversos protocolos que necesitan enviar regularmente mensajes broadcast y dados unos protocolos y servicios en una LAN la cantidad de tráfico broadcast suele ser proporcional al número de equipos.

Cuando la LAN crece el tráfico broadcast aumenta y puede degradar de forma apreciable el rendimiento de los ordenadores conectados. Cuando el tráfico broadcast en una LAN supera de media los 50-100 pps debería investigarse su origen, ya que o bien:

- Hay un número excesivo de ordenadores en esa LAN, o

- Se está utilizando algún protocolo muy 'charlatán' (que hace muchos envíos broadcast), o

- Hay algún problema en la red (por ejemplo un ordenador infectado por virus)

Supongamos que en una LAN con 100 ordenadores hay una media de 100 pps broadcast (1pps por ordenador), y que esto consume el 0,2% de la CPU de cada ordenador

Si la LAN crece a 1000 ordenadores y se mantienen los mismos protocolos y servicios tendremos 1000 pps de broadcast, con un consumo de CPU del 2% en cada uno de los ordenadores

Si en vez de eso creamos 10 LANs, cada una con 100 ordenadores, mantendremos el consumo de CPU en el 0,2%

La solución es hacer LANs pequeñas y conectarlas a nivel de red con routers

Las recomendaciones oscilan entre 256 y 1024 equipos por LAN como máximo, aunque esto depende mucho de los protocolos y servicios utilizados

La separación en varias LANs obliga a tener múltiples conmutadores por edificio, incluso por armario. También es preciso tender cables independientes entre los conmutadores de cada LAN, entre armarios y entre edificios. La red es poco flexible, pues para cambiar un ordenador de LAN hay que ir físicamente al armario y cambiar la conexión a otro conmutador.

Se puede dar la circunstancia de que un conmutador tenga puertos sobrantes, mientras que otro está lleno y no tiene sitio para ampliaciones

Para resolver todos estos problemas se inventaron las VLANs (Virtual LANs)

Una VLAN (acrónimo de virtual LAN, «red de área local virtual») es un método para crear redes

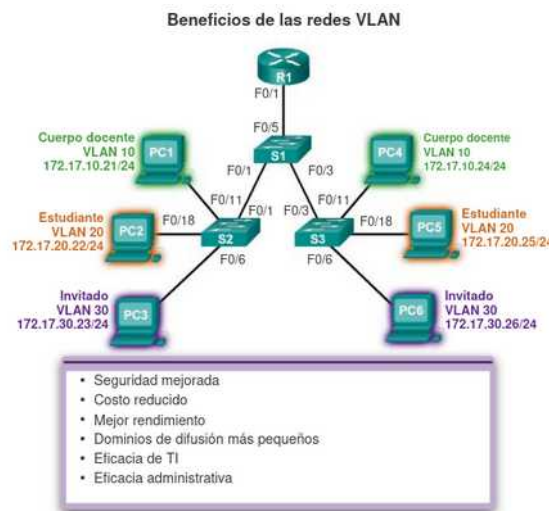
lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3).



En un switch, atendiendo a su función dentro de la VLAN, existirán dos tipos de puertos:

Puertos de acceso (access)

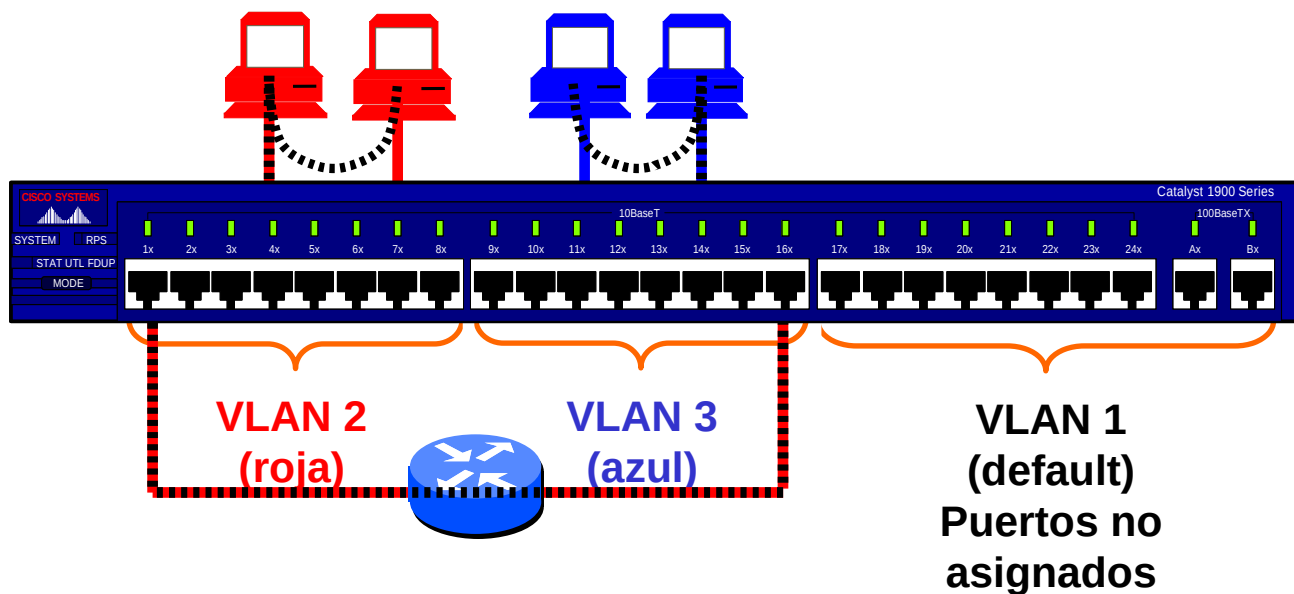
Puertos troncales (trunk)



Los puertos de **acceso** son aquellos a los que se conectan directamente los equipos terminales (ordenadores o periféricos). Por ellos solo viajan tramas pertenecientes a una única VLAN.

Los puertos **troncales** son aquellos por los que circulan tramas de una o más VLANs. Para distinguir el tráfico de las distinta VLANs es necesario etiquetar las tramas indicando que VLAN pertenecen.

La VLAN por defecto es aquella a la que están asignados los puertos no asignados a ninguna VLAN



Tipos de VLAN

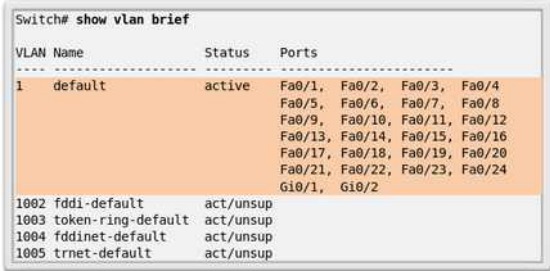
Existen diferentes tipos de redes VLAN, los cuales se utilizan en las redes modernas. Algunos tipos de VLAN se definen según las clases de tráfico. Otros tipos de VLAN se definen según la función específica que cumplen.

VLAN de datos

Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios. Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. A veces a una VLAN de datos se la denomina VLAN de usuario. Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.

VLAN predeterminada

Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches Cisco es la VLAN 1. En la ilustración, se emitió el comando **show vlan brief** en un switch que ejecuta la configuración predeterminada. Observe que todos los puertos se asignan a la VLAN 1 de manera predeterminada.



VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- De manera predeterminada, todos los puertos están asignados a la VLAN 1 para reenviar datos.
- De manera predeterminada, la VLAN nativa es la VLAN 1.
- De manera predeterminada, la VLAN de administración es la VLAN 1.

La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

VLAN nativa

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El tráfico con etiquetas hace referencia al tráfico que tiene 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. El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

Las VLAN nativas se definen en la especificación IEEE 802.1Q a fin de mantener la compatibilidad con el tráfico sin etiquetar de modelos anteriores común a las situaciones de LAN antiguas. Una VLAN nativa funciona como identificador común en extremos opuestos de un enlace troncal.

Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN. De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio conmutado.

VLAN de administración

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada. Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP. Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.

En el pasado, la VLAN de administración para los switches 2960 era la única SVI activa. En las versiones 15.x de IOS de Cisco para los switches de la serie Catalyst 2960, es posible tener más de una SVI activa. Con IOS de Cisco 15.x, se debe registrar la SVI activa específica asignada para la administración remota. Si bien, en teoría, un switch puede tener más de una VLAN de administración, esto aumenta la exposición a los ataques de red.

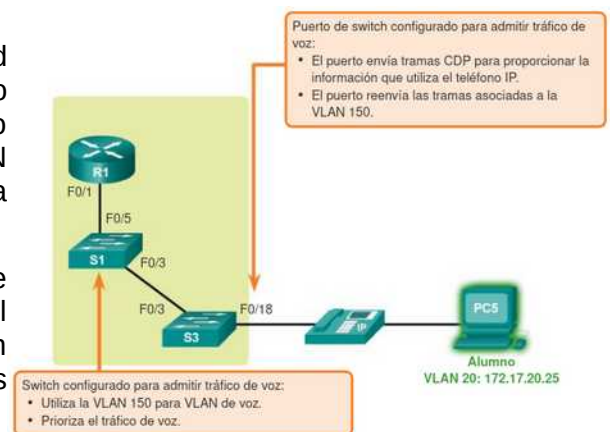
VLAN de Voz

Se necesita una VLAN separada para admitir la tecnología de voz sobre IP (VoIP). El tráfico de VoIP requiere:

- Ancho de banda garantizado para asegurar la calidad de la voz
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Una demora inferior a 150 ms a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP. Los detalles sobre cómo configurar una red para que admita VoIP exceden el ámbito de este curso, pero es útil resumir cómo funciona una VLAN de voz entre un switch, un teléfono IP Cisco y una computadora.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes.



Enlaces troncales

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

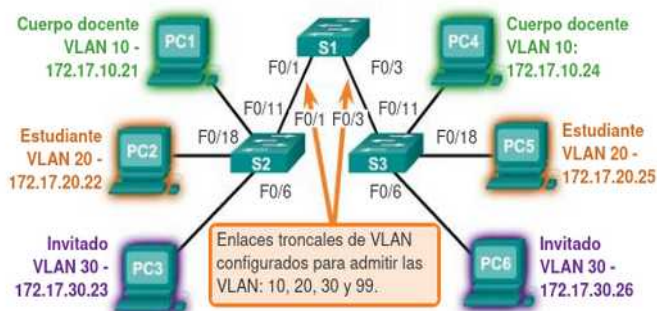
Las VLAN no serían muy útiles sin los enlaces troncales de VLAN. Los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para varias VLAN entre switches y routers. También se puede utilizar un enlace troncal entre un dispositivo de red y un servidor u otro dispositivo que cuente con una NIC con capacidad 802.1Q. En los switches Cisco Catalyst, se admiten todas las VLAN en un puerto de enlace troncal de manera predeterminada.

En la ilustración, los enlaces entre los switches S1 y S2, y S1 y S3 se configuraron para transmitir el tráfico proveniente de las VLAN 10, 20, 30 y 99 a través de la red. Esta red no podría funcionar sin los enlaces troncales de VLAN.

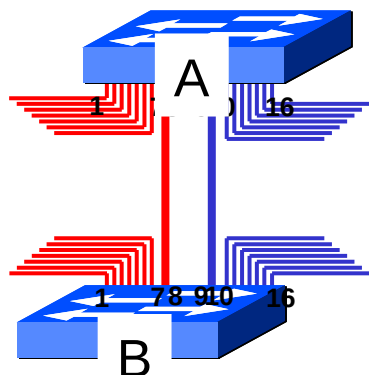
VLAN 10 de cuerpo docente/personal:
172.17.10.0/24
VLAN 20 de estudiantes: 172.17.20.0/24
VLAN 30 de invitados: 172.17.30.0/24
VLAN 99 de administración y nativa:
172.17.99.0/24

Las interfaces F0/1 a 5 son interfaces de enlace troncal 802.1Q con una VLAN nativa 99.
Las interfaces F0/11 a 17 están en la VLAN 10.
Las interfaces F0/18 a 24 están en la VLAN 20.
Las interfaces F0/6 a 10 están en la VLAN 30.

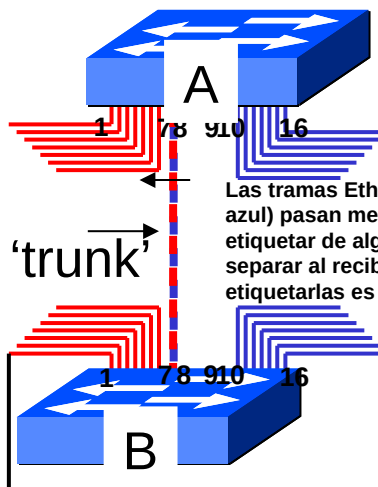


Cuando se configuran VLANs en un conmutador los puertos asignados a cada VLAN se comportan como un conmutador independiente. Si se interconectan dos conmutadores por un puerto solo se comunica la VLAN a las que estos puertos pertenecen

Si tenemos varias VLANs y las queremos conectar todas hemos de establecer un enlace diferente para cada una. Esto puede consumir muchos puertos en los conmutadores y muchos cables en la red. Para evitarlo se pueden configurar puertos que conectan todas las VLANs automáticamente; se les llama puertos 'trunk'



Enlace 'trunk'

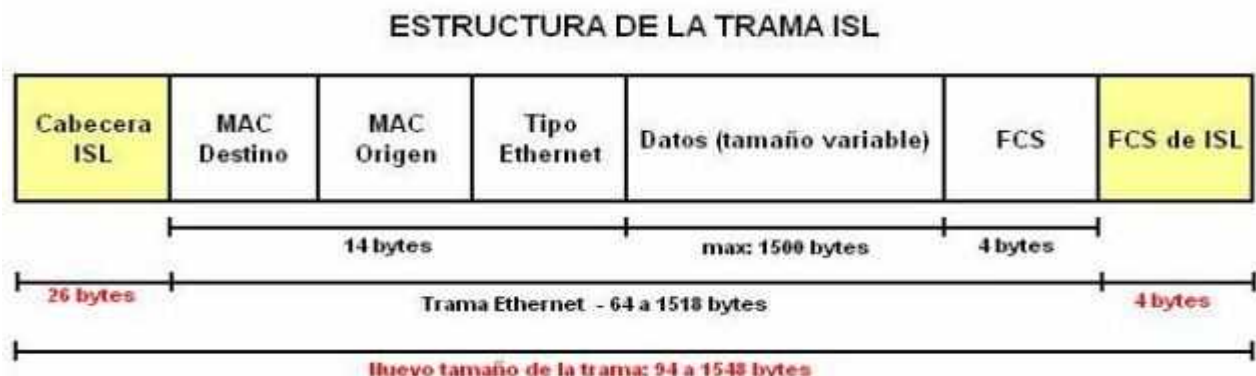


Las tramas Ethernet de ambas VLANs (roja y azul) pasan mezcladas por el cable. Se han de etiquetar de alguna forma para que se puedan separar al recibirlas. La forma habitual de etiquetarlas es según el estándar 802.1Q

En un enlace 'trunk' viajan mezcladas tramas de diferentes VLANs. Para separarlas correctamente en destino hay que marcarlas antes de enviarlas por el enlace 'trunk'. Al principio cada fabricante estableció su sistema de marcado propietario.

ISL (Inter-Switch Link Protocol)

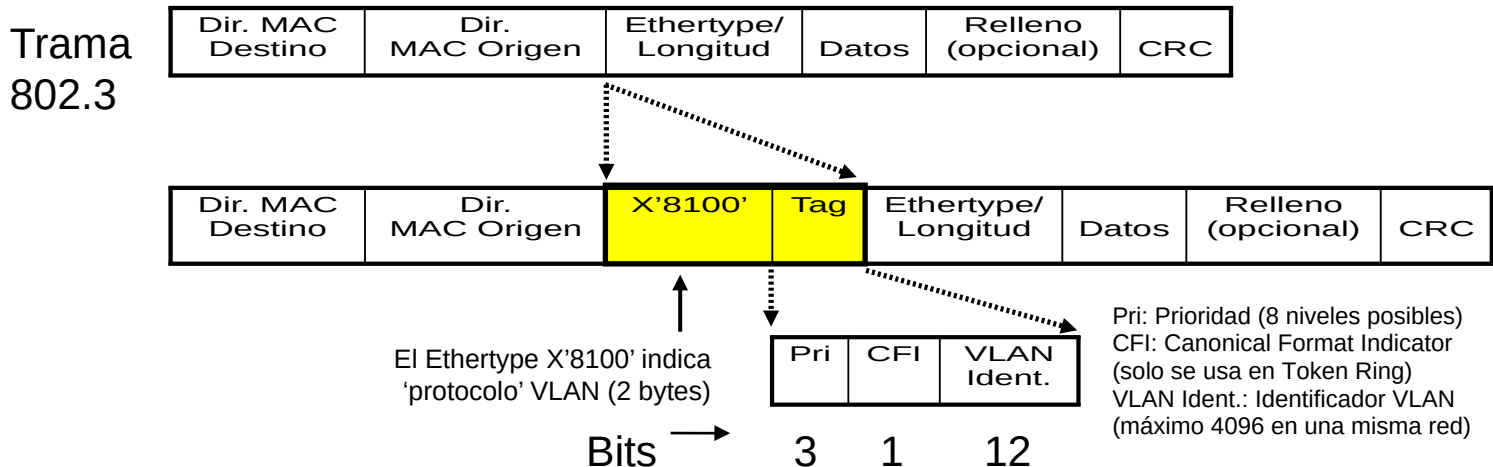
ISL es un protocolo propietario de Cisco que está en desuso. Este protocolo no altera la trama original, porque éste encapsula la trama Ethernet con una nueva cabecera de 26 bytes, que contiene al identificador VLAN (VLAN ID), y además añade un campo de secuencia de chequeo de trama (FCS ó CRC) de 4 bytes al final de la trama, como se muestra en la figura. Por lo tanto, como la trama ha sido encapsulada por ISL con nueva información, solamente los dispositivos que conozcan ISL podrán leer estas nuevas tramas



Los protocolos propietarios impedían establecer enlaces trunk entre conmutadores de diferentes fabricantes. En 1997 el IEEE aprobó 802.1Q, un estándar que establecía una forma de marcado de VLANs independiente de fabricante.

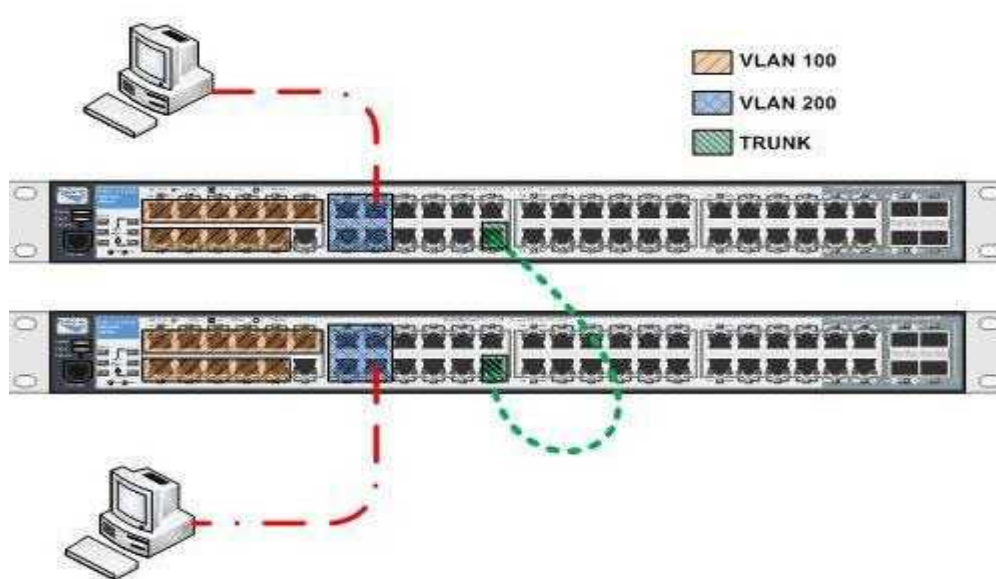
IEEE 802.1Q

El estándar IEEE 802.1Q (también llamado dot1q) especifica el etiquetado de tramas como un método para implementar VLANs. Insertando un campo de 4 bytes dentro de la trama Ethernet para identificar a que VLAN pertenece la información que se está transportando entre dispositivos de capa 2. Para ello hubo que insertar un campo nuevo en la estructura de la trama Ethernet



El proceso de insertar el campo IEEE 802.1Q dentro de la trama Ethernet provoca que el campo FCS (CRC) sea inválido, debido a que se ha alterado la trama, por lo tanto es esencial que un nuevo FCS sea recalculado, basado en la nueva trama que contiene al campo IEEE 802.1Q. Este proceso es automáticamente desarrollado por el switch antes de que la trama sea enviada por el enlace troncal.

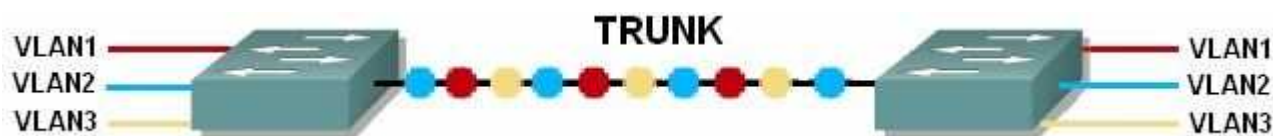
Este método es el más popular por ser empleado por switches de diferentes fabricantes, ofreciendo compatibilidad entre equipos. Incluso los switches Cisco pueden manejar este estándar.



Los enlaces troncales o trunks, son enlaces capaces de transportar el tráfico de más de una VLAN y se suele utilizar para **interconectar dos switches, un switch y un router**, incluso interconectar un switch y un servidor al cual se le ha instalado una NIC especial capaz de soportar trunking. Los enlaces troncales nos permiten transportar de forma lógica las VLANs utilizando un enlace físico.

Un enlace troncal (trunk) puede ser un único enlace físico o estar conformado por varios de ellos usando la técnica de agregación (link aggregation) que permite combinar varios enlaces físicos en un enlace lógico que funciona como un único puerto de mayor ancho de banda.

Otras denominaciones para la agregación de enlaces son Trunking o Bonding. Cisco lo denomina EtherChannel (Modos: ON, PAgP o LACP).



Los puertos de un switch pueden estar etiquetados (**tagged**) o no etiquetados (**untagged**).

Tipos de VLAN por su asignación de puertos

Hay básicamente tres mecanismos de asignación de puertos de switch a VLANs:

Estático, por configuración: se especifica en la configuración a que VLAN pertenece cada puerto

Dinámico, por dirección MAC: el switch asigna el puerto a la VLAN correspondiente de acuerdo con una asignación MAC-VLAN previamente almacenada en una base de datos

Dinámico, por autenticación usuario/password (protocolo 802.1x): el switch, después de validar al usuario, asigna el puerto a la VLAN que le corresponde, de acuerdo con la información contenida en una base de datos que relaciona usuarios y VLANs

La asignación dinámica es más versátil, pero no está disponible en todos los equipos

VLAN nativa

Normalmente un puerto de switch configurado como un puerto troncal envía y recibe tramas Ethernet etiquetadas con IEEE 802.1q. Si un switch recibe **tramas Ethernet sin etiquetar** en su puerto troncal, se remiten a la VLAN que se configura en el switch como VLAN nativa. Ambos lados del enlace troncal deben configurarse para estar en la misma VLAN nativa. Es muy importante que este número de vlan nativa sea igual en ambos extremos de la conexión entre dos switches o entre un switch y un Router configurado con subinterfaces (con la palabra clave "native" en el comando "encapsulation").

La VLAN nativa **es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como trunk**. Sólo se puede tener una VLAN nativa por puerto. En los equipos de Cisco Systems la VLAN nativa por defecto es la **VLAN 1**. Por la VLAN 1 además de datos, se manda información sobre PAgP, CDP, VTP.

Para establecer un trunking 802.1Q a ambos lados debemos tener la misma VLAN nativa porque la encapsulación todavía no se ha establecido y los dos switches deben hablar sobre un link sin encapsulación (usan la native VLAN) para ponerse de acuerdo en estos parámetros.

La VLAN nativa se usa para transportar tráfico sin etiquetar (o tráfico que no usa el 802.1Q tag).

La VLAN nativa proporciona un detalle adicional interesante: Permitir conexiones a dispositivos que no entienden el enlace troncal (802.1Q), por ejemplo, un Switch Cisco podría conectarse, por ejemplo, a un Switch no administrable que no entienda el enlace troncal 802.1Q. El switch Cisco enviará tramas en la VLAN nativa el cual no estará etiquetado, de modo que el otro Switch no-Cisco entendería la trama y la aceptaría.

Cisco recomienda por seguridad cambiar el numero de vlan nativa por una que no es utilizable (no usar la vlan 1). Los ataques de vlan siempre se dirigen en primera instancia a la vlan 1 para acceder al switch o a los paquetes de otras vlans.

La vlan de administración no es igual que la vlan nativa. Sirve para acceder al switch por medio de su interfaz vlan (por defecto interfaz vlan 1)

Generalmente, la vlan nativa no debe tener ningún puerto de acceso asignado a esa vlan (se recomienda que la vlan sea no usada, o conocida como "unused vlan")

Tramas etiquetadas en la VLAN nativa

Algunos dispositivos que admiten enlaces troncales agregan una etiqueta VLAN al tráfico de las VLAN nativas. El tráfico de control que se envía por la VLAN nativa no se debe etiquetar. Si un puerto de enlace troncal 802.1Q recibe una trama etiquetada con la misma ID de VLAN que la VLAN nativa, descarta la trama. Por consiguiente, al configurar un puerto de un switch Cisco, configure los dispositivos de modo que no envíen tramas etiquetadas por la VLAN nativa. Los dispositivos de otros proveedores que admiten tramas etiquetadas en la VLAN nativa incluyen: teléfonos IP, servidores, routers y switches que no pertenecen a Cisco.

Tramas sin etiquetar en la VLAN nativa

Cuando un puerto de enlace troncal de un switch Cisco recibe tramas sin etiquetar (poco usuales en las redes bien diseñadas), envía esas tramas a la VLAN nativa. Si no hay dispositivos asociados a la VLAN nativa (lo que no es poco usual) y no existen otros puertos de enlace troncal (lo que no es poco usual), se descarta la trama. La VLAN nativa predeterminada es la VLAN 1. Al configurar un puerto de

enlace troncal 802.1Q, se asigna el valor de la ID de VLAN nativa a la ID de VLAN de puerto (PVID) predeterminada. Todo el tráfico sin etiquetar entrante o saliente del puerto 802.1Q se reenvía según el valor de la PVID. Por ejemplo, si se configura la VLAN 99 como VLAN nativa, la PVID es 99, y todo el tráfico sin etiquetar se reenvía a la VLAN 99. Si no se volvió a configurar la VLAN nativa, el valor de la PVID se establece en VLAN 1.

Enlace troncal en VLAN de Voz

Recuerde que, para admitir VoIP, se requiere una VLAN de voz separada.

Un puerto de acceso que se usa para conectar un teléfono IP de Cisco se puede configurar para usar dos VLAN separadas: una VLAN para el tráfico de voz y otra VLAN para el tráfico de datos desde un dispositivo conectado al teléfono. El enlace entre el switch y el teléfono IP funciona como un enlace troncal para transportar tanto el tráfico de la VLAN de voz como el tráfico de la VLAN de datos.

El teléfono IP Cisco contiene un switch integrado 10/100 de tres puertos. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

- El puerto 1 se conecta al switch o a otro dispositivo VoIP.
- El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.
- El puerto 3 (puerto de acceso) se conecta a un PC u otro dispositivo.

En el switch, el acceso está configurado para enviar paquetes del protocolo de descubrimiento de Cisco (CDP) que instruyen a un teléfono IP conectado para que envíe el tráfico de voz al switch en una de tres formas posibles, según el tipo de tráfico:

En una VLAN de voz con una etiqueta de valor de prioridad de clase de servicio (CoS) de capa 2.

En una VLAN de acceso con una etiqueta de valor de prioridad de CoS de capa 2.

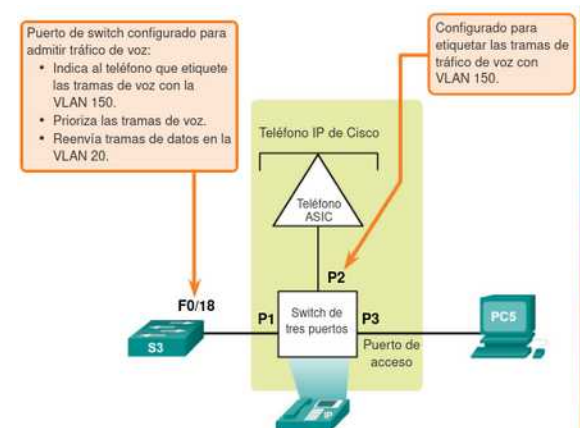
En una VLAN de acceso sin etiqueta (sin valor de prioridad de CoS de capa 2).

En la figura, la computadora del estudiante PC5 está conectada a un teléfono IP de Cisco, y el teléfono está conectado al switch S3. La VLAN 150 está diseñada para transportar tráfico de voz, mientras que la PC5 está en la VLAN 20, que se usa para los datos de los estudiantes.

switchport mode access

switchport access vlan 20

switchport voice vlan 150



Ejemplo de configuración

En la figura, se muestra un resultado de ejemplo. El análisis de los comandos de voz de IOS de Cisco exceden el ámbito de este curso, pero las áreas resaltadas en el resultado de ejemplo muestran que la interfaz F0/18 se configuró con una VLAN configurada para datos (VLAN 20) y una VLAN configurada para voz (VLAN 150)

```
S1# sh interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

Protocolos

DTP

DTP (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

DTP se habilita automáticamente en un puerto del switch cuando se configura un modo de trunking adecuado en dicho puerto. Para ello el administrador debe ejecutar el comando `switchport mode` adecuado al configurar el puerto:

`switchport mode {access | trunk | dynamic auto | dynamic desirable}.`

Con el comando `switchport nonegotiate` se desactiva DTP.

En switches Catalyst 2960 de Cisco el **modo dynamic auto** es el modo por defecto. El puerto aguardará pasivamente la indicación del otro extremo del enlace para pasar a modo troncal. Para ello envía periódicamente tramas DTP al puerto en el otro lado del enlace indicando que es capaz de establecer un enlace troncal. Esto no quiere decir que lo solicita, sino que sólo lo informa. Si el puerto remoto está configurado en modo on o dynamic desirable se establece el enlace troncal correctamente. Sin embargo, si los dos extremos están en modo dynamic auto no se establecerá el enlace como troncal, sino como acceso.

switchport mode access: Pone la interfaz (puerto de acceso) a modo nontrunking permanente a toda costa independientemente de si la interfaz del vecino es un trunk o no.

switchport mode dynamic auto: La interfaz será una interfaz de trunk si la interfaz del vecino está puesta a trunk o desirable.

switchport mode dynamic desirable: La interfaz activamente intenta convertir el enlace a un enlace trunk. La interfaz deviene una interfaz trunk si el la del vecino está puesta a trunk, desirable, o auto. Esto es el modo por defecto de los switches más viejos como el Catalyst 2950 y 3550

switchport mode trunk: Pone la interfaz a modo trunk permanente y negocia para convertir el enlace del vecino a modo trunk también. La interfaz deviene una interfaz de trunk incluso si la interfaz del vecino no lo es, pero tendrá conectividad limitada.

En resumen:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

VTP

VTP son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

VTP opera en 3 modos distintos:

- Servidor
- Cliente
- Transparente

Servidor

Es el modo por defecto. Desde él se pueden crear, eliminar o modificar VLANs. Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces trunk. Debe haber al menos un servidor. Se recomienda autenticación MD5.

Cliente

En este modo no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN.

Transparente

Desde este modo tampoco se pueden crear, eliminar o modificar VLANs que afecten a los demás switches. La información VLAN en los switches que trabajen en este modo sólo se puede modificar localmente. Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio.

Los administradores cambian la configuración de las VLANs en el switch en modo servidor. Después de realizar cambios, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces permitidos en el trunk (VLAN 1, por defecto), lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP. En este modo no se podrán crear VLANs, sino que sólo se podrá aplicar la información que reciba de las publicaciones VTP.

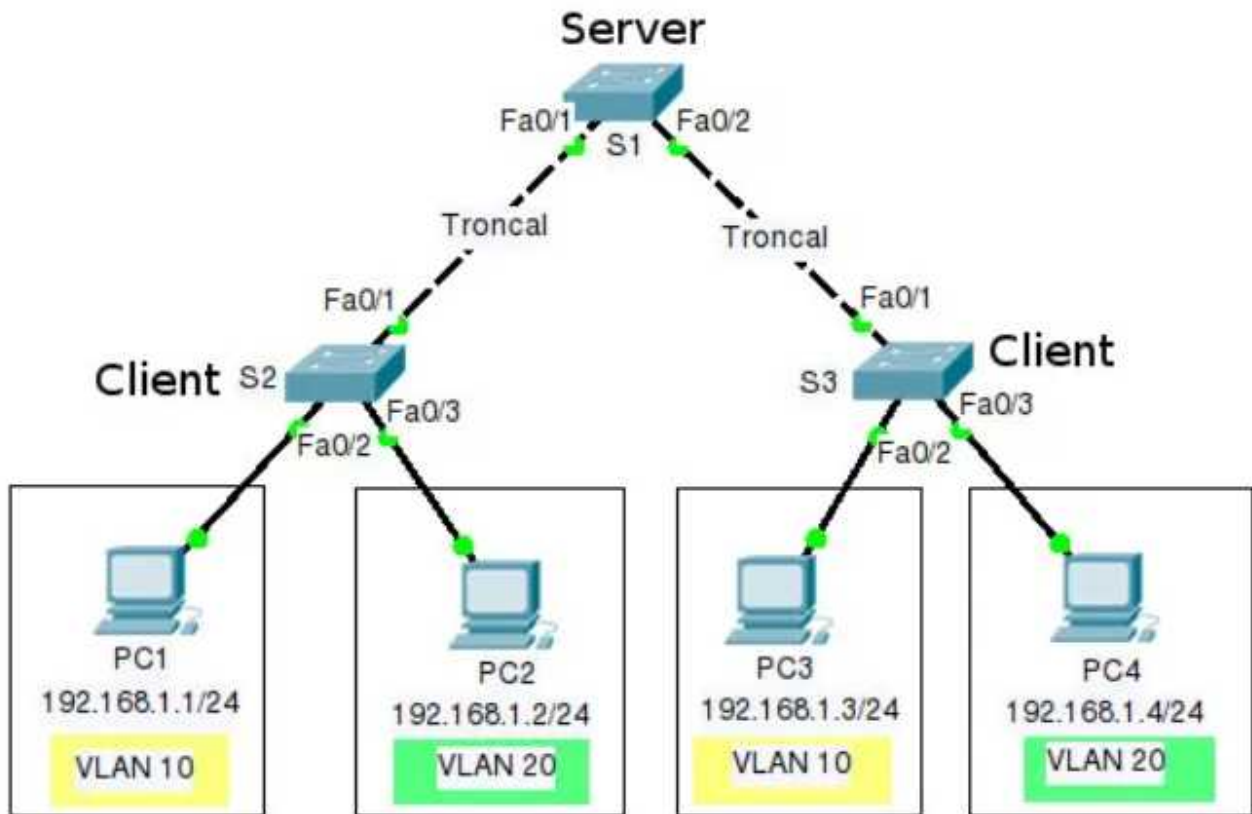
El modo por defecto de los switches es el de servidor VTP. Se recomienda el uso de este modo para redes de pequeña escala en las que la información de las VLANs es pequeña y por tanto de fácil almacenamiento en las NVRAMs de los switches.

En redes de mayor tamaño, el administrador debe elegir qué switches actúan como servidores, basándose en las capacidades de éstos (los mejor equipados serán servidores y los demás, clientes).

El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP.

Las configuraciones se almacenan en un archivo de base de datos de VLAN, denominado **vlan.dat**. El archivo vlan.dat se encuentra en la memoria flash del switch.

Ejemplo configuración VTP:



El protocolo VTP facilita la configuración de VLANs en múltiples switches de manera simultánea solo con la configuración del switch denominado como servidor (server).

Inicialmente configuraremos los puertos troncales en los 3 switches, luego procederemos a configurar el resto de los puertos como acceso por motivos de seguridad, luego configuraremos el protocolo VTP en los 3 switches, las VLANs a utilizar las configuraremos en el switch denominado como servidor y por último configuraremos los puertos en sus respectivas VLAN.

Las VLAN que utilizaremos serán las siguientes:

- VLAN 10 (Administración)
- VLAN 20 (Ventas)

A medida que se haga la configuración, se explicarán los pasos uno por uno:

Procedimiento para configurar VTP

Configuración de puertos troncales y acceso

Configuración de VTP

Configuración de las VLAN en el switch server y verificación en todos los switches de las VLAN

Asignación de los puertos a las VLANs

Estado en de la red

Procedimiento para configurar VTP

configuración de puertos troncales y de acceso

Para realizar la configuración de VTP, se debe configurar como troncales (trunk), las interfaces que conectan los switches entre sí, para esto debemos ingresar al método de configuración global S1(config)#, utilizando el comando interface seguido la interfaz correspondiente ingresamos al modo de configuración de la interfaz S1(config-if)# (interface range si queremos configurar varias interfaces a la vez) y utilizando el comando **switchport mode trunk** configuramos el puerto como troncal. Seguidamente por motivos de seguridad configuramos los demás puertos como acceso ingresando al modo de configuración de interfaces S1(config-if-range)# y utilizando el comando **switchport mode access**.

- Configuración de las interfaces de Switch1 (S1)
 - S1(config)# interface range fastEthernet 0/1–2
 - S1(config-if-range)# switchport mode trunk
 - S1(config-if-range)# exit
 - S1(config)# interface range fastEthernet 0/3–24
 - S1(config-if-range)# switchport mode access
- Configuración de las interfaces de Switch2 (S2)
 - S2(config)# interface fastEthernet 0/1
 - S2(config-if)# switchport mode trunk
 - S2(config-if)# exit
 - S2(config)# interface range fastEthernet 0/2–24
 - S2(config-if-range)# switchport mode access
- Configuración de las interfaces de Switch3 (S3)
 - S3(config)# interface fastEthernet 0/1
 - S3(config-if)# switchport mode trunk
 - S3(config-if)# exit
 - S3(config)# interface range fastEthernet 0/2–24
 - S3(config-if-range)# switchport mode access

Configuración de VTP

Después debemos configurar el **nombre del dominio VTP** desde el modo de configuración global S1(config)# utilizando el comando **vtp domain** seguido del **nombre del dominio** (el nombre del dominio es sensible a mayúsculas). Y habilitar la versión 2 con **vtp version 2**

Asignamos una contraseña al dominio con el comando **vtp password** seguido de la **contraseña** que deseamos utilizar y por último debemos especificar el modo en el que el switch funcionará, esto con el comando **vtp mode** seguido del **modo** (**server**, **client**, **transparent**).

Configuración del nombre, contraseña y modo del S1

- S1(config)#vtp domain Practica
- S1(config)#vtp password seguro
- S1(config)#vtp mode server
- Configuración del nombre, contraseña y modo del S2
 - S2(config)#vtp domain Practica // no hace falta, ya lo coge por los mensajes que manda S1
 - S2(config)#vtp password seguro
 - S2(config)#vtp mode client
- Configuración del nombre, contraseña y modo del S3
 - S3(config)#vtp domain Practica // no hace falta, ya lo coge por los mensajes que manda S1
 - S3(config)#vtp password seguro
 - S3(config)#vtp mode client

Creación de las VLAN

Una vez configurado VTP debemos ingresar las VLANs en el switch que está en modo servidor para que los que están en modo cliente puedan aprender las VLANs automáticamente, esto lo conseguimos desde el modo de configuración global S1(config)# utilizando el comando **vlan** seguido del **número de la VLAN** (1-1005). En el modo de configuración de VLAN S1(config-vlan)# asignamos un nombre a la VLAN utilizando el comando name seguido del nombre que deseamos asignar a la VLAN.

```
S1(config)# vlan 10
S1(config-vlan)# name Administracion
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name Ventas
S1(config-vlan)# exit
```

Si ahora vamos a los switches S2 y S3 y tecleamos show vlan brief veremos las VLAN creadas también allí.

Asignación de puertos a las VLANs

Por último debemos asignar las VLAN a los puertos, esto lo conseguimos desde el modo de configuración global S1(config)# utilizando el comando interface o interface range seguido de la interfaz que deseamos asignar a una VLAN específica, y dentro del modo de configuración de interfaz utilizamos el comando **switchport access vlan** seguido del número de la VLAN correspondiente.

Asignación de los puertos a la VLAN10 y a la VLAN20

```
S2(config)# interface fastEthernet 0/2
S2(config-if)# switchport access vlan 10
S2(config-if)# exit
S2(config)# interface fastEthernet 0/3
S2(config-if)# switchport access vlan 20
S3(config)# interface fastEthernet 0/2
S3(config-if)# switchport access vlan 10
S3(config-if)# exit
S3(config)# interface fastEthernet 0/3
S3(config-if)# switchport access vlan 20
```

Información sobre VTP

```
S2# show vtp status
```