VLAN

La VLAN (LAN Virtual) aparece como solución a la separación lógica de redes, es decir, cuando en una red física, en la que todos los dispositivos están unidos se desea independizar en grupos estos dispositivos, por ejemplo en un edificio donde están conectados los equipos de profesores y alumnos se desea que estos funcionen separadamente, para esto aparecen las VLAN que separan los equipos sin necesidad de cambiar ningún cableado.

Una VLAN permite que un administrador de red cree grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Cuando configura una VLAN, puede ponerle un nombre para describir la función principal de los usuarios de esa VLAN

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada

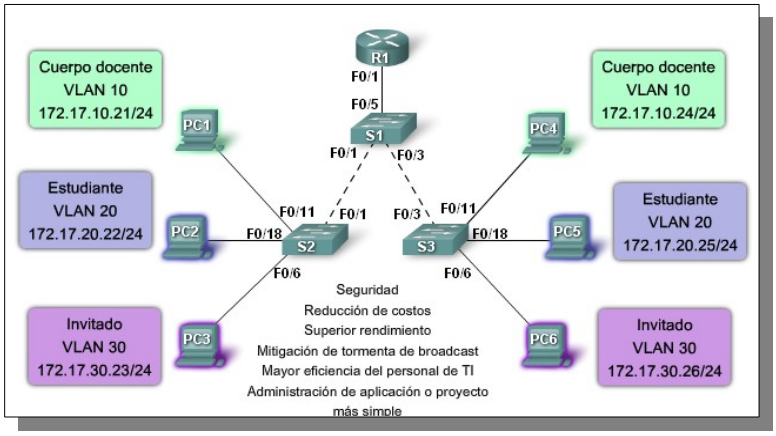
- **Red sin VLAN :** En funcionamiento normal, cuando un switch recibe una trama de broadcast en uno de sus puertos, envía la trama a todos los demás puertos.
- **Red con VLAN :** Cuando las VLAN se implementan en un switch, la transmisión del tráfico de unicast, multicast y broadcast desde un host en una VLAN en particular, se limitan a los dispositivos presentes en la VLAN.

La fragmentación de un gran dominio de broadcast en varias partes más pequeñas reduce el tráfico de broadcast y mejora el rendimiento de la red. La fragmentación de dominios en VLAN permite además una mejor confidencialidad de información dentro de una organización. La fragmentación de dominios de broadcast puede realizarse con las VLAN (en los switches) o con routers. Cada vez que dispositivos en diferentes redes de Capa 3 necesiten comunicarse, es necesario un router sin tener en cuenta si las VLAN están en uso.

Ventajas de las VLAN

Estas son las ventajas mas importantes de las VLAN (por favor observar la siguiente figura):

Seguridad: Los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial. Las computadoras del cuerpo docente se encuentran en la VLAN 10 y están completamente separadas del tráfico de datos del Invitado y de los estudiantes.



Reducción de costo: El ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

Mejor rendimiento: La división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.

Mitigación de la tormenta de broadcast: La división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast. La segmentación de LAN impide que una tormenta de broadcast se propague a toda la red. En la figura puede observar que, a pesar de que hay seis computadoras en esta red, hay sólo tres dominios de broadcast: Cuerpo docente, Estudiante y Invitado.

Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando proporciona un switch nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre. En la figura, para una identificación más fácil se nombró "Estudiante" a la VLAN 20, la VLAN 10 se podría nombrar "Cuerpo docente" y la VLAN 30 "Invitado ".

Administración de aplicación o de proyectos más simples: Las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar un proyecto o trabajar con una aplicación especializada sea más fácil, por ejemplo una plataforma de desarrollo de e-learning para el cuerpo docente. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red.

Tipos de VLAN

VLAN de Datos : Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario.

VLAN Predeterminada : Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada justo despues del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. 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 suele ser la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no la puede volver a denominar y no la puede eliminar. El tráfico de control de Capa 2, como CDP y el tráfico del protocolo spanning tree se asociará siempre con la VLAN 1: esto no se puede cambiar.

VLAN Nativa : Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa.

VLAN de Administración : Una VLAN de administración es cualquier VLAN que usted configura para acceder a las capacidades de administración de un switch. La VLAN 1 serviría como VLAN de administración si no definió proactivamente una VLAN única para que sirva como VLAN de administración. Se asigna una dirección IP y una máscara de subred a la VLAN de administración. Se puede manejar un switch mediante HTTP, Telnet, SSH o SNMP.

VLAN de voz : Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. 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
- Demora de menos de 150 milisegundos (ms) a través de la red

Etiquetado de trama 802.1Q

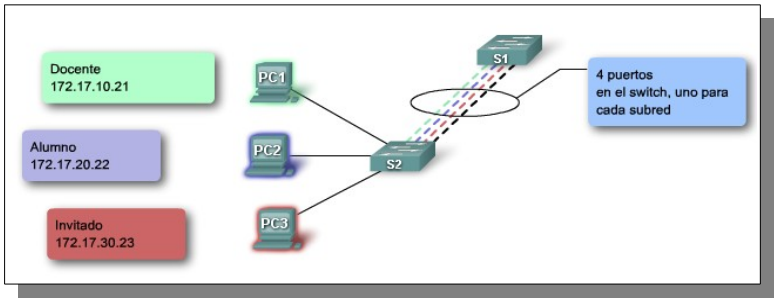
Recuerde que los switches son dispositivos de capa 2. Sólo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado a agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama. Es decir, cuando una trama circula por un puerto configurado en modo acceso es una trama ethernet normal, pero cuando circula por un puerto configurado en modo troncal debe indicar a que VLAN pertenece esta trama y por tanto es necesario añadirle esta información, esto es lo que hace el etiquetado 802.1Q.

802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original.

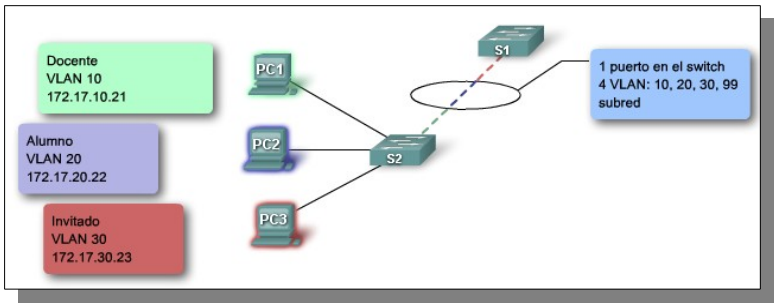
Enlace troncal de la VLAN

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

SIN ENLACE TRONCAL:



CON ENLACE TRONCAL:



VLAN nativa

El punto 9 del estándar define el protocolo de encapsulamiento usado para multiplexar varias VLAN a través de un solo enlace, e introduce el concepto de las VLAN nativas. Las tramas pertenecientes a la VLAN nativa no se etiquetan con el ID de VLAN cuando se envían por el trunk. Y en el otro lado, si a un puerto llega una trama sin etiquetar, la trama se considera perteneciente a la VLAN nativa de ese puerto. Este modo de funcionamiento fue implementado para asegurar la interoperabilidad con antiguos dispositivos que no entendían 802.1Q.

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.

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. En los equipos de Cisco Systems la VLAN nativa por defecto es la VLAN 1.

Comandos de IOS para VLAN

Crear VLAN **:** Pasar al modo de configuración con configure terminal y ejecutar:

vlan numero
name nombre

Asignar un puerto **:** Entrar en la interface con: interface fast…

switchport mode access
switchport access vlan numero

Comprobar

show vlan

Borrar una vlan

no vlan numero

Crear un enlace troncal

Entrar en la interface con: interface fast…

switchport mode trunk

También es aconsejable cambiar la vlan native.

switchport trunk native vlan numero

Indicar las vlan que permite

switchport access trunk allowed vlan add vlan-id

Ver estado del protocolo VTP (VLAN Trunk Protocol)

show vtp status

Configuración de dominio VTP : En el switch servidor:

vtp domain nombredominio

Configuración de la version VTP en todos los switchs
vtp version 1 (hay hasta 3 versiones pero esta es la más extendida)

Configuración modo cliente VTP
vtp mode client

Ejemplo 1 de configuracion VLAN en Packet Tracert

show vlan // en modo no privilegiado
*configure termina*l
vlan 2 // en modo privilegiado
? // ayuda
name sistemas
vlan 3
name gerencia
end
show vlan // en modo no privilegiado

configure terminal

int fa0/1
switchport mode access
switchport access vlan 2
end

int fa0/2
switchport mode access
switchport access vlan 2
end
show running-config // en modo no privilegiado
show vlan // en modo no privilegiado

Si queremos asignar una ip para acceder al switch y administrarlo:
interface vlan 2 // en modo privilegiado
ip address 192.168.0.200 255.255.255.0
no shutdown
show running-config // en modo no privilegiado
show vlan // en modo no privilegiado
configure terminal
line vty 0 15
password cisco
login
end
enable secret cisco // en modo privilegiado

Ejemplo 2 de configuracion VLAN en Packet Tracert

configure terminal
int fa0/24
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit
exit
show interface trunk

Trunk – Configurando el router

configure terminal
int fa0/0
no shutdown
exit
int fa0/0.2

?
encapsulation dot1q 2
ip address 192.168.1.1 255.255.255.0
exit
int fa0/0.3
encapsulation dot1q 3
ip address 192.168.2.1 255.255.255.0
exit
int fa0/0.4
encapsulation dot1q 4
ip address 192.168.3.1 255.255.255.0
exit

Para desligar una VLAN

int fa0/18
no switchport access vlan
end
show vlan brief

Para eliminar VLAN 20

Antes de eliminar una VLAN, Asegurarse de reasignar primero todos los miembos de una VLAN a otra.

no vlan 20
end
show vlan brief

Restablecer el enlace troncal al esteado determinado

interface fa0/2
no switchport trunk allowed vlan
no switchport trunk native vlan
end
show interface fa0/2 switchport
switchport mode access

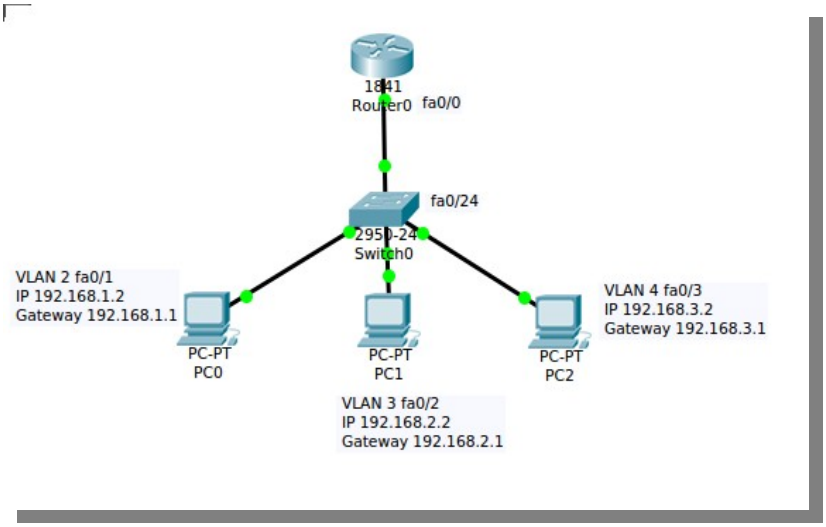
Enrutamiento de un Router con dos VLAN (5 y 8)

Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0.5
Router(config-subif)#encapsulation dot1Q 5
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0.8
Router(config-subif)#encapsulation dot1Q 8
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no sh

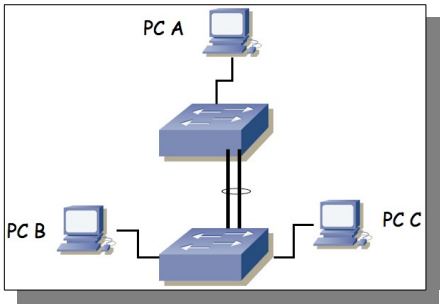
El protocolo IEEE 802.1Q

También conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

Trunk – Configurando el switch



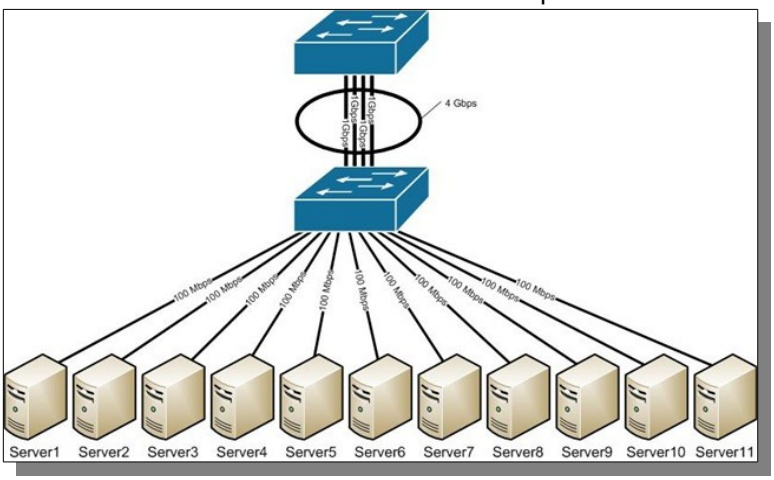
Agregación de enlaces (Etherchanel).



La agregación de enlaces, o IEEE 802.3ad, describe cómo utilizar varios enlaces Ethernet full-dúplex en la comunicación entre dos equipos, repartiendo el tráfico entre ellos. La mayoría de las implementaciones actuales se adecúan al estandard 802.3ad.

Trunking o bonding o la agregación de enlaces es una manera económica de instalar una red de alta velocidad más rápida de lo que permita un solo puerto o dispositivo de la tecnología de que se disponga.

Básicamente consiste en agrupar varios dispositivos que trabajan simultáneamente a su velocidad máxima como si fuera un único enlace de mayor capacidad. Esto también resuelve los problemas de enrutamiento que causa el tener varios caminos al mismo destino ya que a nivel de red el grupo de enlaces se presenta como un único enlace de mayor capacidad. La agregación de enlace permite que la velocidad de los enlaces de la red crezca incrementalmente como respuesta a una demanda creciente en el uso de la red sin tener que sustituir el hardware actual por otra tecnología más rápida y, posiblemente, más costosa.



Para la mayoría de las instalaciones, es común instalar más medios (fibra óptica y par trenzado) de lo estrictamente necesario. Se hace esto porque el coste de la mano de obra de instalación es mucho más alto que el del cable y evita volver a instalar más medios de transmisión ante un aumento de las necesidades de la red. La agregación de enlaces permite usar estos cables adicionales para aumentar la velocidad de los enlaces con un coste mínimo.

Podemos configurar un Etherchannel de tres formas diferentes, Port Aggregation Protocol

(PAgP), Link Aggregation Control Protocol (LACP) o en modo ON, además ambos extremos se han de configurar en el mismo modo. Cuando se configura PAgP o LACP el switch negocia con el otro extremo que puertos deben ponerse activos. Cuando configuramos en modo ON no se realiza ningún tipo de negociación, el switch obliga a todos los puertos compatibles a ponerse activos.

PAgP es un protocolo propietario de Cisco, PAgP se encarga de agrupar puertos de características similares de forma automática. PAgP es capaz de agrupar puertos de la misma velocidad, modo dúplex, troncales o de asignación a una misma VLAN.

PAgP se puede configurar de dos modos:

- Auto, establece el puerto en una negociación pasiva, el puerto solo responderá a paquetes PAgP cuando los reciba, pero nunca iniciará la negociación.
- Desirable, establece el puerto en modo de negociación activa, este puerto negociará el estado cuando reciba paquetes PAgP y también podrá iniciar una negociación contra otros puertos.

Hay que tener en cuenta que un puerto en modo desirable puede formar grupo con otro puerto en el mismo modo, también podrá formar grupo con un puerto en modo auto. Dos puertos en modo auto nunca podrán formar grupo ya que ninguno de ellos puede iniciar una negociación.

LACP es un protocolo definido en el estándar 802.1ad y que puede ser implementado en switches cisco. LACP y PAgP funcionan de forma muy similar ya que LACP también puede agrupar puertos por su velocidad, modo dúplex, troncales, VLAN nativas, etc.

LACP también tiene dos modos de configuración:

- Activo, un puerto en este estado es capaz de iniciar negociaciones con otros puertos para establecer el grupo.
- Pasivo, un puerto en este estado es un puerto que no iniciará ningún tipo de negociación pero si responderá a las negociaciones generadas por otros puertos.

Al igual que LAgP, dos puertos pasivos nunca podrán formar grupo.
El modo ON es un modo de configuración en el cual se establece toda la configuración del puerto de forma manual, no existe ningún tipo de negociación entre los puertos para establecer un grupo. En este tipo de configuración es totalmente necesario que ambos lados estén en modo ON.

VLAN y subredes IP
Cada VLAN debe corresponder a una subred IP única. Si dos dispositivos en la misma VLAN tienen direcciones de subred diferentes, no se pueden comunicar. Este tipo de configuración incorrecta es un problema común y de fácil resolución al identificar el dispositivo en controversia y cambiar la dirección de subred por una dirección correcta.
SVI
SVI (interfaz virtual del switch) es una interfaz lógica configurada para una VLAN específica. Es necesario configurar una SVI para una VLAN si desea enrutar entre las VLAN o para proporcionar conectividad de host IP al switch. De manera predeterminada, una SVI se crea por la VLAN predeterminada (VLAN 1) para permitir la administración de switch remota.
Un switch de Capa 3 tiene la capacidad de enrutar transmisiones entre las VLAN. El procedimiento es el mismo que se describió para la comunicación entre VLAN utilizando un router distinto, excepto que las SVI actúan como las interfaces del router para enrutar los datos entre las VLAN.

VTP
Protocolo de enlace troncal de VLAN. A medida que crece una red se vuelve más complicado la administración de VLAN, en esta situación es conveniente conocer si existe una forma para que los switches sepan cuáles son las VLAN y los enlaces troncales, de modo que no tenga que configurarlos manualmente, este es el problema que soluciona VTP.

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de

cliente del VTP. 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.

Conceptos para trabajar con VTP:

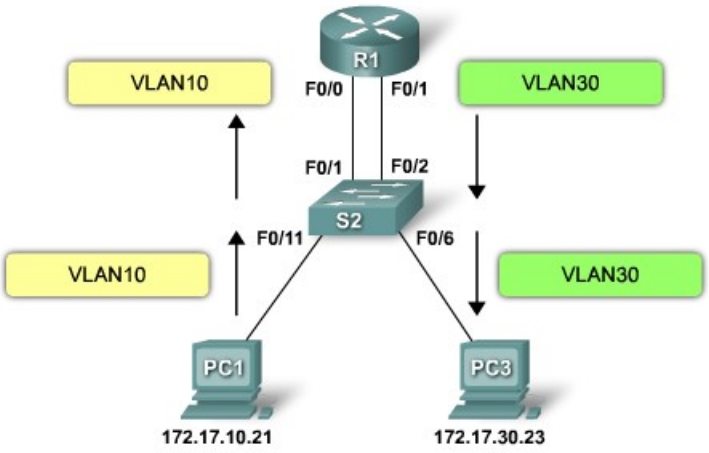
- **Dominio del VTP** **:** Consiste de uno o más switches interconectados. Todos los switches en un dominio comparten los detalles de configuración de la VLAN usando las publicaciones del VTP. Un router o switch de Capa 3 define el límite de cada dominio.
- **Publicaciones del VTP** **:** El VTP usa una jerarquía de publicaciones para distribuir y sincronizar las configuraciones de la VLAN a través de la red.
- **Modos del VTP** **:** Un switch se puede configurar en uno de tres modos: servidor, cliente o transparente.
- **Servidor del VTP** **:** Los servidores del VTP publican la información VLAN del dominio del VTP a otros switches habilitados por el VTP en el mismo dominio del VTP. Los servidores del VTP guardan la información de la VLAN para el dominio completo en la NVRAM. El servidor es donde las VLAN se pueden crear, eliminar o redenominar para el dominio.
- **Cliente del VTP** **:** Los clientes del VTP funcionan de la misma manera que los servidores del VTP pero no pueden crear, cambiar o eliminar las VLAN en un cliente del VTP. Un cliente del 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. Debe configurar el modo de cliente del VTP en un switch.
- **VTP transparente** **:** los switches transparentes envían publicaciones del VTP a los clientes del VTP y servidores del VTP. Los switches transparentes no participan en el VTP. Las VLAN que se crean, redenominan o se eliminan en los switches transparentes son locales para ese switch solamente.
- **Depuración del VTP** **:** La depuración del VTP aumenta el ancho de banda disponible para la red mediante la restricción del tráfico saturado a esos enlaces troncales que el tráfico debe utilizar para alcanzar los dispositivos de destino. Sin la depuración del VTP, un switch satura el broadcast, el multicast y el tráfico desconocido de unicast a través de los enlaces troncales dentro de un dominio del VTP aunque los switches receptores podrían descartarlos.

Encapsulación de la trama del VTP

Una trama del VTP consiste en un campo de encabezado y un campo de mensaje. La información del VTP se inserta en el campo de datos de una trama de Ethernet. La trama de Ethernet luego se encapsula como una trama troncal de 802.1Q (o trama ISL). Cada switch en el dominio envía publicaciones periódicas de cada puerto de enlace troncal a una dirección multicast reservada. Los switches vecinos reciben estas publicaciones que actualizan las configuraciones de sus VTP y VLAN si es necesario.

Enrutamiento inter VLAN

En una red tradicional que utiliza VLAN múltiples para segmentar el tráfico de la red en dominios de broadcast lógicos, el enrutamiento se realiza mediante la conexión de diferentes interfaces físicas del router a diferentes puertos físicos del switch. Los puertos del switch conectan al router en modo de acceso; en el modo de acceso, diferentes VLAN estáticas se asignan a cada interfaz del puerto. Cada interfaz del switch estaría asignada a una VLAN estática diferente. Cada interfaz del router puede entonces aceptar el tráfico desde la VLAN asociada a la interfaz del switch que se encuentra conectada, y el tráfico puede enrutarse a otras VLAN conectadas a otras interfaces.



El enrutamiento inter VLAN tradicional requiere de interfaces físicas múltiples en el router y en el switch. Sin embargo, no todas las configuraciones del enrutamiento inter VLAN requieren de interfaces físicas múltiples. Algunos software del router permiten configurar interfaces del router como enlaces troncales. Esto abre nuevas posibilidades para el enrutamiento inter VLAN.

"Router-on-a-stick" es un tipo de configuración de router en la cual una interfaz física única enruta el tráfico entre múltiples VLAN en una red.

La interfaz del router se configura para funcionar como enlace troncal y está conectada a un puerto del switch configurado en modo de enlace troncal. El router realiza el enrutamiento inter VLAN al aceptar el tráfico etiquetado de la VLAN en la interfaz troncal proveniente del switch adyacente y enrutar en forma interna entre las VLAN, mediante subinterfaz. El router luego reenvía el tráfico enrutado de la VLAN etiquetada para la VLAN de destino, por la misma interfaz física.

Las subinterfaces son interfaces virtuales múltiples, asociadas a una interfaz física. Estas interfaces están configuradas en software en un router configurado en forma independiente con una dirección IP y una asignación de VLAN para funcionar en una VLAN específica. Las subinterfaces están configuradas para diferentes subredes que corresponden a la asignación de la VLAN, para facilitar el enrutamiento lógico antes de que la VLAN etiquete las tramas de datos y las reenvíe por la interfaz física.

Uso del router como gateway
El enrutamiento tradicional requiere de routers que tengan interfaces físicas múltiples para facilitar el enrutamiento inter VLAN. El router realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz está configurada con una dirección IP para la subred asociada con la VLAN conectada a ésta. Al configurar las direcciones IP en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN pueden comunicarse con el router utilizando la interfaz física conectada a la misma VLAN. En esta configuración los dispositivos de red pueden utilizar el router como un gateway para acceder a los dispositivos conectados a las otras VLAN.

El proceso de enrutamiento requiere del dispositivo de origen para determinar si el dispositivo de destino es local o remoto con respecto a la subred local. El dispositivo de origen realiza esta acción comparando las direcciones de origen y destino con la máscara de subred. Una vez que se determinó que la dirección de destino está en una red remota, el dispositivo de origen debe identificar si es necesario reenviar el paquete para alcanzar el dispositivo de destino. El dispositivo de origen examina la tabla de enrutamiento local para determinar si es necesario enviar los datos. Generalmente, los dispositivos utilizan los gateways predeterminados como destino para todo el tráfico que necesita abandonar la subred local. El gateway predeterminado es la ruta que el dispositivo utiliza cuando no tiene otra ruta explícitamente definida hacia la red de destino. La interfaz del router en la subred local actúa como el gateway predeterminado para el dispositivo emisor.

Una vez que el dispositivo de origen determinó que el paquete debe viajar a través de la interfaz del router local en la VLAN conectada, el dispositivo de origen envía una solicitud de ARP para determinar la dirección MAC de la interfaz del router local. Una vez que el router reenvía la respuesta ARP al dispositivo de origen, éste puede utilizar la dirección MAC para finalizar el entramado del paquete, antes de enviarlo a la red como tráfico unicast.

Dado que la trama de Ethernet tiene la dirección MAC de destino de la interfaz del router, el switch sabe exactamente a qué puerto del switch reenviar el tráfico unicast para alcanzar la interfaz del router en dicha VLAN. Cuando la trama llega al router, el router elimina la información de la dirección MAC de origen y destino para examinar la dirección IP de destino del paquete. El router compara la dirección de destino con las entradas en la tabla de enrutamiento para determinar si es necesario reenviar los datos para alcanzar el destino final. Si el router determina que la red de destino es una red conectada en forma local, como sería el caso en el enrutamiento inter VLAN, el router envía una solicitud de ARP fuera de la interfaz conectada físicamente a la VLAN de destino. El dispositivo de destino responde al router con la dirección MAC, la cual luego utiliza el router para entramar el paquete. El router envía el tráfico unicast al switch, que lo reenvía por el puerto donde se encuentra conectado el dispositivo de destino.

Después de la configuración de servidor y clientes se configuran las vlan, los switch deducirán cuales son los enlaces troncales.
Existen dos comandos del IOS de Cisco para confirmar que el dominio de VTP y las configuraciones de VLAN se han transferido al switch S2. Use el comando show VTP status para verificar lo siguiente:
El número de revisión de configuración se ha incrementado.
Existen ahora nuevas VLAN indicadas por el número existente de VLAN. El nombre de dominio se ha cambiado.
Utilice el comando show vtp counters para confirmar que se realizaron las publicaciones.

Configuración de link troncal de Etherchannel L2 modo ON (Switch 1)
Switch1# configure terminal
Switch1(config)# interface range gigabitethernet0/1 - 4
Switch1(config-if-range)# switchport mode trunk
Switch1(config-if-range)# channel-group 1 mode on
Switch1(config-if-range)# exit
Switch1(config)# Para crear varias subinterfaces en un router:exit
Switch1# copy run start
Configuración de link troncal de Etherchannel L2 modo ON (Switch 2)
Switch2# configure terminal
Switch2(config)# interface range gigabitethernet0/1 - 4
Switch2(config-if-range)# switchport mode trunk
Switch2(config-if-range)# channel-group 1 mode on
Switch2(config-if-range)# exit
Switch2(config)# exit
Switch2# copy run start
Configuración de link troncal de Etherchannel L2 con LACP (Switch 1)
Switch# configure terminal
Switch1(config)# interface range gigabitethernet0/1 - 4
Switch1(config-if-range)# switchport mode trunk
Switch1(config-if-range)# channel-group encapsulation LACP
Switch1(config-if-range)# channel-group 1 mode active
Switch1(config-if-range)# exit
Switch1(config)# exit
Switch1# copy run start
Configuración de link troncal de Etherchannel L2 con LACP (Switch 2)
Switch2# configure terminal
Switch2(config)# interface range gigabitethernet0/1 - 4
Switch2(config-if-range)# switchport mode trunk
Switch2(config-if-range)# channel-group encapsulation LACP
Switch2(config-if-range)# channel-group 1 mode active
Switch2(config-if-range)# exit
Switch2(config)# exit
Switch2# copy run start
Una vez hecho esto podemos configurar la interfaz lógica de la siguiente forma:
Switch1# configure terminal
Switch1(config)# interface port-channel 1
Switch1(config-if)#
Desde este modo de configuración podemos configurar parámetros que se aplicaran a todos los puertos del grupo. Para chequear que el Etherchannel esta funcionando usamos el siguiente comando:
Switch1> show port channel 1

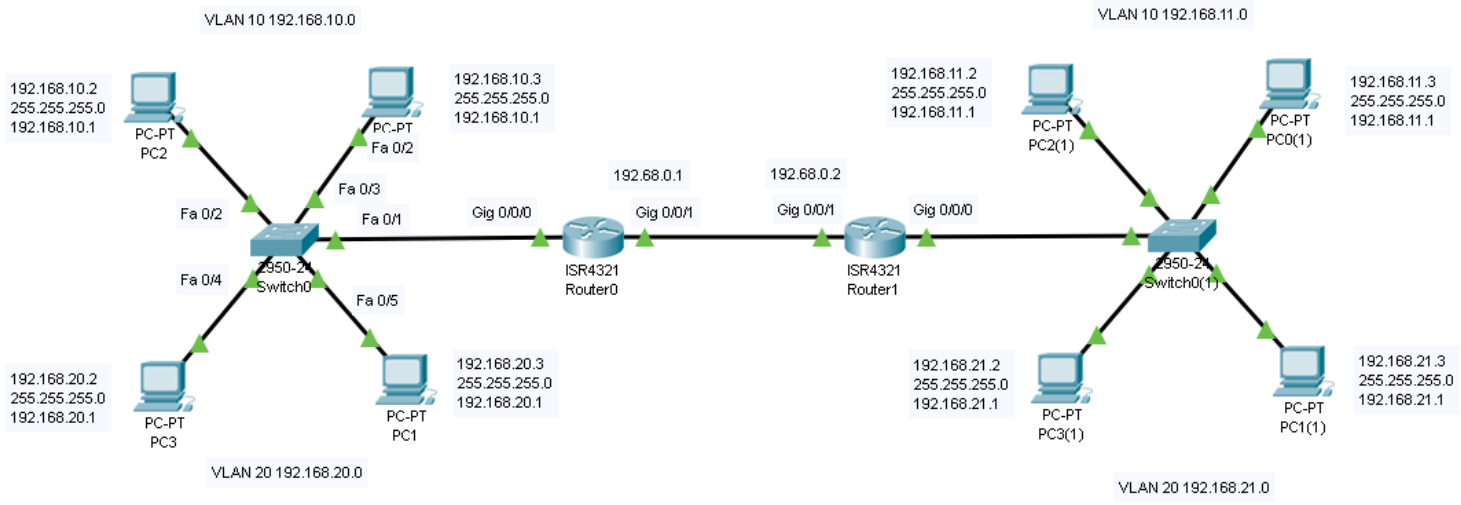
Port	Status	Channel mode	Channel status	Neighbor device	Neighbor	Neighbor port
0/1	connected	on	channel	Switch2		0/1
0/2	connected	on	channel	Switch2		0/2
0/3	connected	on	channel	Switch2		0/3
0/4	connected	on	channel	Switch2		0/4

Para crear varias subinterfaces en un router:

1. interface f0/0.10 en el modo de configuración global para crear la subinterfaz del router. La sintaxis para la subinterfaz es siempre la interfaz física, en este caso f0/0, seguida de un punto y un número de subinterfaz. El número de la subinterfaz es configurable, pero generalmente está asociado para reflejar el número de VLAN
2. Antes de asignar una dirección IP a una subinterfaz, es necesario configurar la subinterfaz para que funcione en una VLAN específica mediante el comando encapsulation dot1q vlan id
3. comando ip address direccion mascara asigna la subinterfaz a la dirección IP apropiada para esa VLAN.

Ejemplos :

Dos vlan (10 y 20) en cada switch, en cada switch cuatro equipos, dos en cada vlan. Unidos con dos routers (uno en cada oficina)



Router 1

```
Router>en
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#no shutdown
Router(config-if)#interface gigabitEthernet 0/0/1
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0/0.10
Router(config-subif)#no shutdown
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0/0.20
Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#exit
Router(config)#ip route 192.168.11.0 255.255.255.0 192.168.0.2
Router(config)#ip route 192.168.21.0 255.255.255.0 192.168.0.2
Router(config)#exit
```

Router 2

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0/0.10
Router(config-subif)#
```

```
Router(config-subif)#no shutdown
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.11.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0/0.20
Router(config-subif)#no shutdown
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.21.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ip address 192.168.0.2 255.255.255.0
Router(config-if)#exit
Router(config)#ip route
Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.0.1
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.0.1
Router(config)#exit
Router#
```