# VLAN

## INTRODUCCIÓN

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.

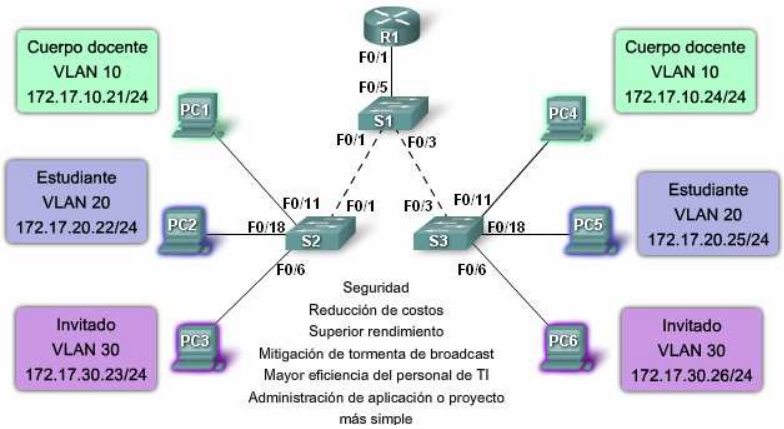
**Red con VLAN**.- Cuando las VLAN se implementan en un switch, la transmisión del tráfico de unicast, multicast y broadcast desde un host en una VLAN en particular, se limitan a los dispositivos presentes en la VLAN.

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

La productividad del usuario y la adaptabilidad de la red son impulsores clave para el crecimiento y el éxito del negocio. La implementación de la tecnología de VLAN permite que una red admita de manera más flexible las metas comerciales. Los principales beneficios de utilizar las VLAN son los siguientes:

**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 después 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 1serviría 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

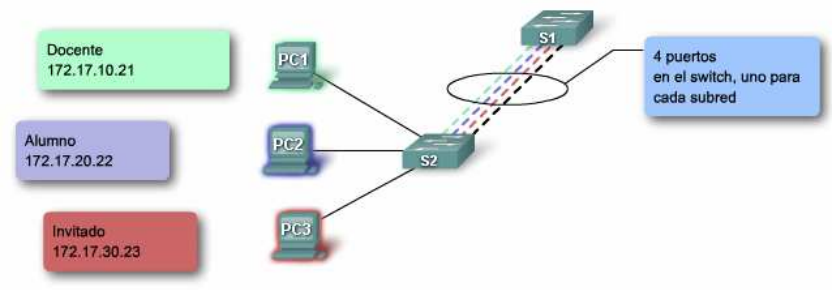
Recuerde que los switches son dispositivos de capa 2. Sólo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace 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. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama. Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza a un recálculo del campo "FCS".

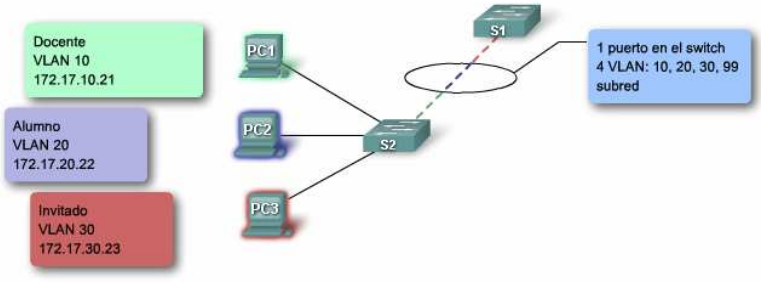
## ENLACE TRONCAL DE LA VLAN

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**

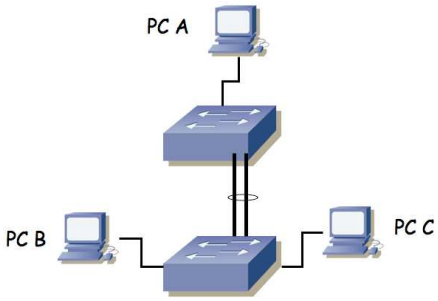
El punto 9 del estándar define el protocolo de encapsulamiento usado para multiplexar varias VLAN a través de un solo enlace, e introduce el concepto de las VLAN nativas. Las tramas pertenecientes a la VLAN nativa no se etiquetan con el ID de VLAN cuando se envían por el trunk. Y en el otro lado, si 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. Por la VLAN 1 además de datos, se manda información sobre PAgP, CDP, VTP.

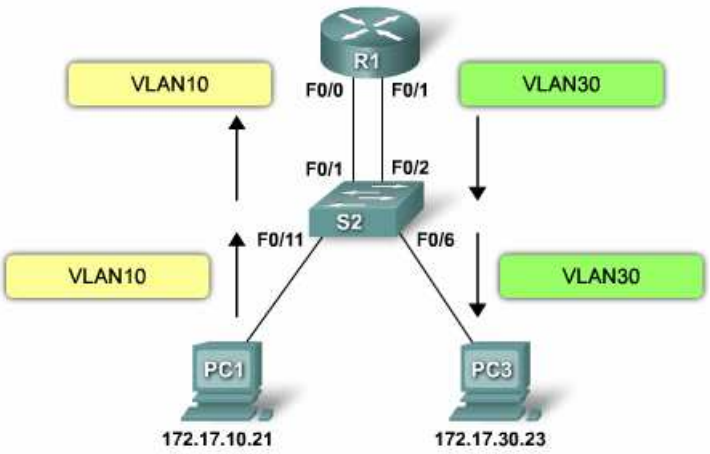
## VLAN Y SUBREDES IP

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.




## 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.

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.

## COMANDOS DE IOS PARA VLAN

Poner IP a la VLAN

```
Sw# configure terminal
Sw(config)# interface Vlan1
Sw(config-if)# ip address 192.168.1.2 255.255.255.0
Sw(config-if)# no shutdown
Sw(config)# ip default-gateway 192.168.1.1
```

Crear VLAN

- Pasar al modo de configuración con configure terminal y ejecutar:
  a. vlan numero
  b. name nombre

Asignar un puerto

- Entrar en la interface con: interface fast…
  a. switchport mode access
  b. switchport access vlan numero

Comprobar

- Show vlan

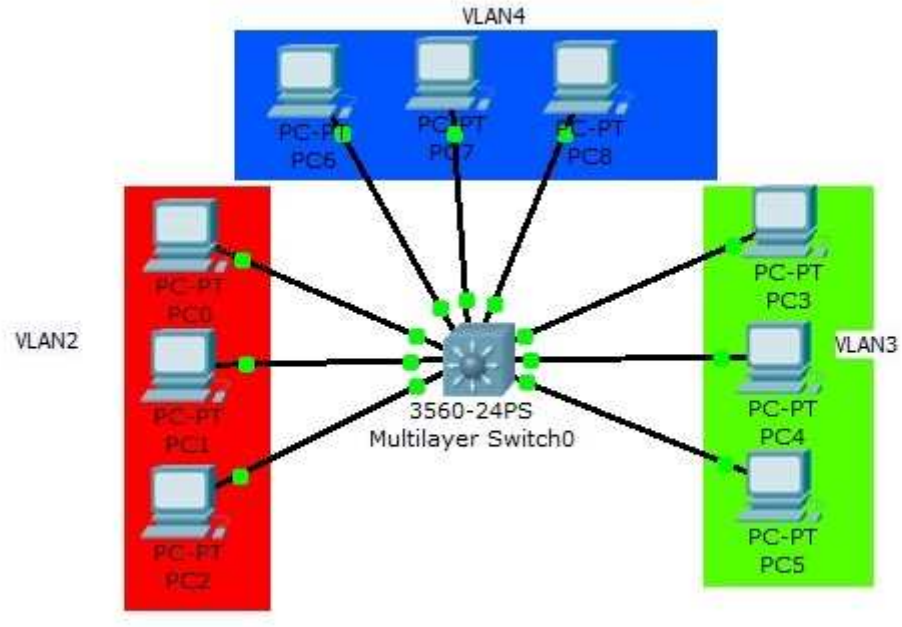
Borrar una vlan

- 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 trunk allowed vlan add vlan-id

**Un ejemplo en Packet tracer de Red con VLANs**




Dentro de las VLANs de cisco que hemos visto podremos encontrar 2 tipos **vlan access** y **vlan trunk**

- **Vlan access** (Vlan basada en el puerto) nos permite asignar un puerto del switch a una vlan previamente creada. Para crear las Vlan utilizaremos los siguientes comandos:

  **Creación de Vlans**
  Switch#
  Switch#vlan database
  Switch(vlan)#vlan 3 name verde
  VLAN 3 added:
  Name: verde
  De este modo hemos creado la vlan 3 con nombre verde.

  **Eliminación de Vlans**
  Switch#
  Switch#vlan database
  Switch(vlan)#no vlan 3
  De este modo hemos eliminado la vlan 3.

  Para añadir un puerto a una vlan deberemos seguir los siguientes pasos:

  **Asignando Vlan a un puerto**

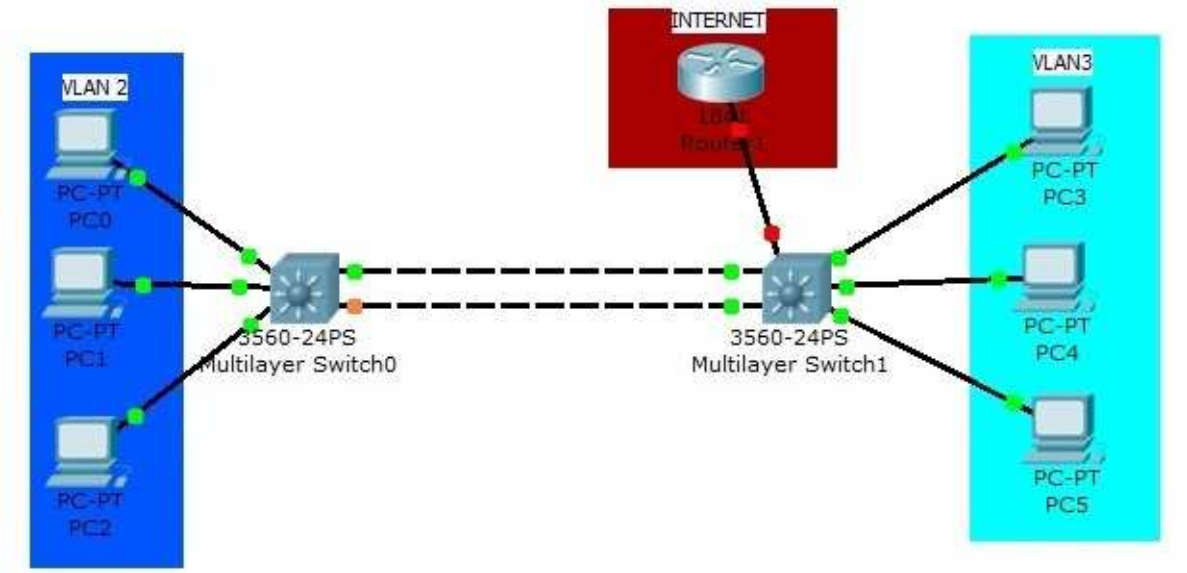
  Switch#configure terminal
  Switch(config)#interface fastEthernet 0/1
  Switch(config-if)#switchport access vlan 3

  **Nota**
  Asegurarse de que el puerto está configurado como vlan access y si no ejecutar:

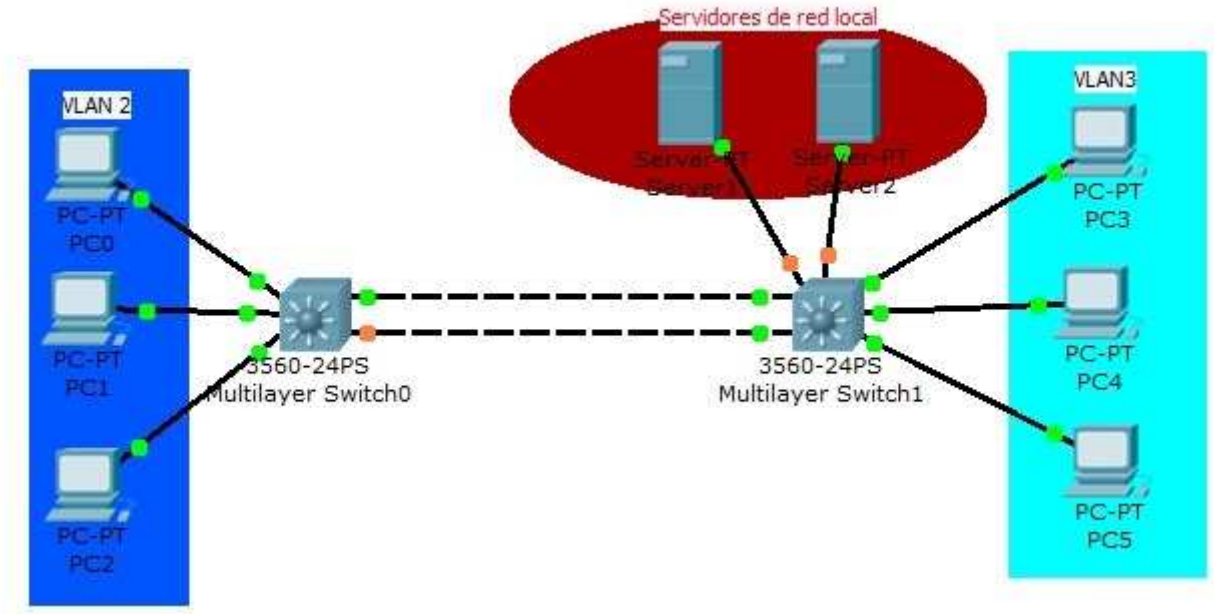
  Switch#configure terminal
  Switch(config)#interface fastEthernet 0/1
  Switch(config-if)#switchport mode access

  De este modo el puerto fastEthernet 0/1 pertenece ahora a la vlan 3.

- **Vlan trunk** es usado para crear enlaces a través de 2 switch de modo que el tráfico entre estos sea divido por varios enlaces en modo **VLAN trunk**.




**Ejemplo de una red Vlan trunk con servidores locales**




**Cambiar un puerto a modo trunk**

Switch>enable
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Podemos modificar un puerto en modo trunk para elegir que vlans pasan a través de éste.

**Quitar vlan de un puerto Vlan trunk**

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport trunk allowed vlan remove 1
```

**Añadir Vlan a un puerto Vlan trunk**

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport trunk allowed vlan add 1
```