# [VLAN](http://www.ciscoredes.com/ccna3/90-vlan.html" \o "VLAN)

Una VLAN (acrónimo de Virtual LAN) es una subred IP separada de manera lógica, las VLAN permiten que redes IP y subredes  múltiples existan en la misma red conmutada, son útiles para reducir el tamaño del broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos para una empresa, oficina, universidades, etc.) que no deberían intercambiar datos usando la red local.

Cada computadora de  una VLAN debe tener una dirección IP y una máscara de subred correspondiente a dicha subred.

Por mediante la CLI del IOS de un switch, deben darse de alta las VLAN y a cada puerto se le debe asignar  el modo y la VLAN por la cual va a trabajar.

No es obligatorio el uso de VLAN en las redes conmutadas, pero existen ventajas reales para utilizarlas como seguridad, reducción de costo, mejor rendimiento, reducción de los tamaño de broadcast y mejora la administración de la red.

El acceso a las VLAN está dividido en un rango normal o un rango extendido, las VLAN de rango normal se utilizan en redes de pequeñas y medianas empresas, se identifican por un ID de VLAN entre el 1 y 1005 y las de rango extendido posibilita a los proveedores de servicios que amplien sus infraestructuras a una cantidad de clientes mayor y se identifican mediante un ID de VLAN entre 1006 y 4094.

El protocolo de enlace troncal de la VLAN VTP (que lo veremos más adelante) sólo aprende las VLAN de rango normal y no las de rango extendido.

**Tipos de VLAN**

De acuerdo con la terminología común de las VLAN se clasifican en:

**VLAN de Datos.-** es la que está configurada sólo para enviar tráfico de datos generado por el usuario, a una VLAN de datos también se le denomina VLAN de usuario.

**VLAN Predeterminada.-** Es la VLAN a la cual todos los puertos del Switch se asignan cuando el dispositivo inicia, en el caso de los switches cisco por defecto es la VLAN1, otra manera de referirse a la VLAN de predeterminada es aquella que el administrador haya definido como la VLAN a la que se asignan todos los puertos cuando no estan en uso.

**VLAN Nativa.-** una VLAN nativa está asiganada a un puerto troncal 802.1Q, un puerto de enlace troncal 802.1Q admite el tráfico que llega de una VLAN y también el que no llega de las VLAN’s, la VLAN nativa sirve como un identificador común en extremos opuestos de un elace troncal, es aconsejable no utilizar la VLAN1 como la VLAN Nativa.

**VLAN de administración.-** Es cualquier vlan que el administrador configura para acceder a la administración de un switch, la VLAN1 sirve por defecto como la VLAN de administración si es que no se define otra VLAN para que funcione como la VLAN de Administración.

**Modos de puertos del Switch**

**VLAN estática.**- Los puertos de un switch se asignan manualmente a una VLAN (éste es el tipo de VLAN con el que trabajaremos).

**VLAN dinámica.-** La membresía de una VLAN de puerto dinámico se configura utilizando un servidor especial denominado Servidor de Política de Membresía de VLAN (VMPS).

**VLAN de voz.-** El puerto se configura para que esté en modo de voz a fin de que pueda admitir un teléfono IP conectado al mismo tiempo de enviar datos.

**Agregar una VLAN**

Ciscoredes# configure terminal  
Ciscoredes(config)# vlan vlan-id  
Ciscoredes(config-vlan)# name nombre-de-vlan  
Ciscoredes(config-vlan)# exit

* Vlan .- comando para asignar las VLAN
* Valn-id.- Numero de vlan que se creará que va de un rango normal de 1-1005 (los ID 1002-1005 se reservan para Token Ring y FDDI).
* Name.- comando para especificar el nombre de la VLAN
* Nombre-de-vlan.- Nombre asignado a la VLAN, sino se asigna ningún nombre, dicho nombre será rellenado con ceros, por ejemplo para la VLAN 20 sería VLAN0020.

**Asignar puertos a la VLAN**

Ciscoredes# configure terminal  
Ciscoredes(config)# interface interface-id  
Ciscoredes(config-vlan)# switchport mode access  
Ciscoredes(config-vlan)# switchport access vlan vlan-id  
Ciscoredes(config-vlan)# end

Donde:

* interface .- Comando para entrar al modo de configuración de interfaz.
* Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0
* Switchport mode access .- Define el modo de asociación de la VLAN para el puerto
* Switchport access vlan .- Comandos para asignar un puerto a la vlan.
* Vlan-id.- Numero de vlan a la cual se asignará el puerto.

**Vlan de Administración**

Una VLAN de administración le otorga los privilegios de administración al administrador de la red, para manejar un switch en forma remota se necesita asignarle al switch una dirección IP y gateway dentro del rango de dicha subred para esta VLAN, como hemos mencionado anteriormente por defecto la VLAN de administración es la 1, en nuestro ejemplos modificaremos dicha VLAN, los pasos para configurar la VLAN de administración son los siguiente:

Ciscoredes# configure terminal  
Ciscoredes(config)# interface vlan id  
Ciscoredes(config-if)# ip address  a.a.a.a  b.b.b.b  
Ciscoredes(config-if)# no shutdown  
Ciscoredes(config-if)# exit  
Ciscoredes(config)# interface interface-id  
Ciscoredes(config-if)# switchport mode access  
Ciscoredes(config-if)# switchport acces vlan vlan-id  
Ciscoredes(config-if)# exit

Donde:

* interface vlan id .- Entrar al modo de configuración de interfaz para configurar la interfaz VLAN 99
* ip address a.a.a.a b.b.b.b.- Asignar la direción IP y Gateway para la interfaz.
* no shutdown.- Levantar la interfaz (habilitarla)
* exit.- Salir de la interfaz y regresar al modo de configuración global
* interface interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0
* Switchport mode access .- Define el modo de asociación de la VLAN para el puerto
* Switchport access vlan vlan-id  .- Comando para asignar el puerto a una la vlan de administración.

**Configurar un Enlace Troncal**

Enlace Troncal.- Un enlace troncal es un enlace punto a punto entre dos sispositivos de red, el cual transporta más de una vlan. Un enlace troncal de VLAN no pertence a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

Existen deiferentes modos de enlaces troncales como el 802.1Q y el ISL, en la actualidad sólo se usa el 802.1Q, dado que el ISL es utilizado por las redes antiguas, un puerto de enlace troncal IEEE 802.1Q admite tráfico etiquetado y sin etiquetar, el enlace troncal dinámico DTP es un protocolo propiedad de cisco, DTP administra la negociación del enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP.

**Configuración de un enlace troncal 802.1Q en un Switch:**

**Ciscoredes# configure terminal  
Ciscoredes(config)# interface interface-id  
Ciscoredes(config-if)# switchport mode trunk  
Ciscoredes(config-if)# switchport trunk native vlan vlan-id  
Ciscoredes(config-if)# exit**

Donde:

* interface .- Comando para entrar al modo de configuración de interfaz.
* Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0
* Switchport mode trunk .- Definir que el enlace que conecta a los switches sea un enlace troncal
* Switchport trunk native vlan vlan-id .- Especificar otra VLAN como la VLAN nativa para los enlaces troncales.

**Intercomunicación entre VLAN's**

Por si sólo, un switch de capa 2 no tiene la capacidad de enrutar paquetes entre vlan diferentes, si ya tenemos creadas las vlan y hemos asignado más de una computadora a cada vlan, entonces las computadoras que se encuentran en la misma vlan pueden comunicarse entre si, pero que pasaría por ejemplo si la vlan 10 se quiere comunicar con la vlan 20, la comunicación no se llevaría acabo porque las vlan se encuentran en subredes diferentes y el proceso de enrutamiento lo lleva acabo un dispositivo de capa 3 (o un switch de capa 3), por tal motivo configuraremos un router con subinterfeces, ya que cada subinterfaz será designada para cada vlan con su propia subred.

Una interfaz de un router se puede dividir en subinterfaces lógicas, por ejemplo de la interfaz FastEthernet 0/0 podemos derivar varias subinterfaces como: FastEthernet 0/0.10 ,  FastEthernet 0/0.50 , FastEthernet 0/0.30

La configuración de las subinterfaces del router es similar a la configuración de las interfaces físicas sólo que al final agregamos un punto y un numero (.20), por lo regular este número es el mismo con el número de vlan a utilizar, todo esto para una mejor administración.

Configuración de subinterfaces en un router:

Ciscoredes# configure terminal  
Ciscoredes(config)# interface interface-id.numero  
Ciscoredes(config-subif)# encapsulation dot1q numero  
Ciscoredes(config-subif)# ip address a.a.a.a b.b.b.b  
Ciscoredes(config-subif)# exit

Donde:

* configure terminal.- Comando para entrar al modo de configuración global
* interaface interface-id.numero .- serie de comandos para crear una subinterfaz para una vlan
* encapsulation dot1q numero.- configurar la subinterfaz para que funcione en una VLAN específica.
* ip address a.a.a.a b.b.b.b  .- Asignar la dirección IP del puerta de enlace predeterminada para la subred de la VLAN.

# IEEE 802.1Q

El protocolo **IEEE 802.1Q**, también conocido como **dot1Q**, fue un proyecto del grupo de trabajo 802 de la [IEEE](http://es.wikipedia.org/wiki/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](http://es.wikipedia.org/wiki/Ethernet). Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales.

## ]Formato de la trama

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"](http://es.wikipedia.org/wiki/Fcs).

== VLAN nativas ==//// 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.

Durante el diseño se recomienda

* + La VLAN nativa no debe ser la de gestión.
  + Cambiar la VLAN nativa de la 1 a cualquier otra como medida de seguridad.
  + Todos los switches en la misma VLAN nativa.
  + Usuarios y servidores en sus respectivas VLANs.
  + El tráfico entre switches debe ser el único que no se encapsule en enlaces trunk. El resto del tráfico, incluyendo la VLAN de gestión debe ir encapsulado por los trunks. Si no estamos encapsulando cualquiera puede conectar un equipo que no hable 802.1q (switches y hubs) y funcionará sin nuestro control.

**VLAN NATIVA Y ADMINISTRADORA**

La Vlan nativa es una condición usada con interfaces que son configuradas como vlan troncales (enlace troncales).  
  
Cuando un puerto del switch ha sido configurado como un enlace troncal, este es etiquetado con su respectivo identificador de número de vlan. Las tramas de todas las vlan son trasportadas por un enlace en modo troncal, por medio de la un tag que puede ser 802.1Q o ISL, exceptuando a esto, las tramas que pertenecen a la vlan 1.  
  
Por defecto todas las tramas pertenecen a la vlan 1, a su vez pertenecen tambien a la vlan nativa, ademas estas tramas son transportadas sin etiqueta por el enlace troncal.

La vlan nativa de 802.1Q te da la posibilidad de conectar una interfaz en trunk a un switch que no tenga esta posibilidad.  
  
El switch con el trunk siempre podrá comunicarse con el switch que no tiene trunk por medio de la vlan nativa, si ésta no existiese, el switch sin trunk no entendería nada del tráfico proveniente del switch con trunk.  
  
El concepto de vlan nativa permite a los switches la capacidad de reenviar al menos tráfico de una vlan.  
La cuestión es que la VLAN nativa se utiliza para dispositivos antiguos que no entienden el tráfico etiquetado de un trunk. De forma que en un escenario sencillo tenemos dos switches en trunk con la misma VLAN nativa en cada switch, por ejemplo 99. El tráfico que envíe uno de los switches al otro no se va a etiquetar al salir de ese switch, y cuando llegue al otro, al ver que no tiene etiqueta se asume que son datos de la VLAN nativa. Vamos, que en este caso se utiliza el concepto de VLAN pero no para etiquetar, sino para permitir tráfico entre switches/routers antiguos que no comprenden el etiquetado.

La vlan nativa es la vlan que no va etiquetada en los trunks. Las recomendaciones de seguridad dicen que no se use la 1 como nativa entre otras razones debido a que es la vlan es la que por defecto están asignados los puertos del switch.

**La Vlan nativa**  es una  condición usada  con interfaces que son configuradas como vlan troncales (enlace troncales). Cuando un puerto del switch ha sido configurado como un enlace troncal, este es etiquetado con su respectivo identificador de número de vlan. Las tramas de todas las vlan son trasportadas por un enlace en modo troncal, por medio de la un tag que puede ser **802.1Q** o **ISL**, exceptuando a esto, las tramas que pertenecen a la vlan 1.

Por defecto todas las tramas pertenecen a la vlan 1,  a su vez pertenecen tambien a la vlan nativa, ademas estas tramas son transportadas sin etiqueta por el  enlace troncal.

La IEEE que definió el estándar 802.1Q. Propicio que este estándar tuviera compatibilidad con la vlan nativa. es decir, la vlan nativa no esta asociada a ninguna etiqueta en 802.1Q.

La vlan nativa es implícitamente usada para todo el tráfico sin etiqueta en un enlace troncal y puede ser recibida en un puerto configurado con el 802.1Q.

Esta capacidad permite a un puerto 802.1Q convivir por ejemplo, con puerto  802.3 ethernet, enviando y recibiendo trafico sin etiqueta.  sin embargo, en la mayoría de los casos esto puede ser muy perjudicial, porque los paquetes asociados con la**vlan nativa** puede retrasarse o perderse , por ejemplo, esto se ha identificado en QoS, cuando es transmitida en un enlace 802.1Q.

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

**Switch(config-if)#switchport trunk native vlan vlan-id**

* Es recomendado que la vlan nativa nunca sea ocupada para usos administrativos.

Esta vlan originalmente fue usada para controlar trafico como: CDP, VTP, PAgP, DTP, que son transmitidos por la vlan 1. Si tu cambias la etiqueta de la **vlan nativa** a cualquiera que no sea la vlan 1, todo el control de trafico debería ser transmitido por la vlan 1.  Es decir,  el cambio de vlan no modifica el control de tráfico, Esto ayuda a que el control de trafico por defecto  efectuado  solo por la vlan 1 y no por la vlan nativa.

Es importante asegurar que ambos extremos de una conexión switch a switch,  tengan una consistente configuracion de **vlan nativa**. Si la vlan nativa en ambos extremos no es la misma, esto podría atentar el  flujo entre Vlan, aunque IOS recientes avisan de este error.

**Switch(config-if)#switchport trunk native vlan vlan-id**  
  
Es recomendado que la vlan nativa nunca sea ocupada para usos administrativos.  
Esta vlan originalmente fue usada para controlar trafico como: CDP, VTP, PAgP, DTP, que son transmitidos por la vlan 1. Si tu cambias la etiqueta de la vlan nativa a cualquiera que no sea la vlan 1, todo el control de trafico debería ser transmitido por la vlan 1. Es decir, el cambio de vlan no modifica el control de tráfico, Esto ayuda a que el control de trafico por defecto efectuado solo por la vlan 1 y no por la vlan nativa.  
  
Es importante asegurar que ambos extremos de una conexión switch a switch, tengan una consistente configuracion de vlan nativa. Si la vlan nativa en ambos extremos no es la misma, esto podría atentar el flujo entre Vlan, aunque IOS recientes avisan de este error.  
  
**Comandos Basicos**  
  
***Para crear una vlan de administracion***  
  
switch#conf t  
switch(config)#vlannumero de vlan .  
switch(config)#namenombre deseado para la vlan .  
switch(config)#exit  
switch#sh vlan  
  
***Configurar IP al switch (es decir, se crea la vlan administrtiva)***  
  
switch#conf t  
switch(config)#interface vlan nuero de la VLAN de administracion  
switch(config-if)#ip address *// Se asigna la ip recuerda debe estar en el mismo rango que la de la SubInterfaz del router.*  
EJEMPLO:  
  
***SWITCH:***  
interface FastEthernet0/2 **// Es la que va conectada al Router**  
switchport trunk native vlan 11 **// Asigno mi Vlan Adminstradora como Nativa**switchport access vlan 11  
switchport mode trunk  
  
interface Vlan11 **// Asigno la ip a la Vlan de Adminstracion**  
ip address 172.16.6.2 255.255.255.248  
  
  
SERVER\_DF(config)#ip default-gateway **172.16.6.1 // Es la ip de la SubInterfaz**  
  
  
***ROUTER:***  
  
interface GigabitEthernet1/0.11 **// Es mi SubInterfaz**description Vlan de Administracion DF  
encapsulation dot1Q 11 native  
ip address **172.16.6.1** 255.255.255.248  
  
  
***Configurar default-gateway al switch***  
  
switch#conf t  
switch(config)#ip default-gatewayIP del router ***// La de la Subinterfaz***switch(config)#end  
switch#wr  
  
***Ejemplo:***  
  
SERVER\_DF(config)#ip default-gateway **172.16.6.1** **// Es la ip la SubInterfaz**  
***Para habilitar TELNET***  
  
switch#conf t  
switch(config)#line vty 0 4  
switch(config)#passwordcontraseña deseada  
switch(config)#login  
switch(config)#exit  
switch#wr  
  
***Recuerde que para que la computadora pueda hacerle telnet al switch, el puerto al que se conecta dicha computadora debe pertenecer ala misma VLAN que el switch***  
  
***Para agregar vlans a un grupo permitido se hace***  
  
switch#conf t  
switch(config)#interface numero de la interface  
switch(config-if)# switchport trunk allowed vlan add numero de la vlan  
switch(config-if)#end  
switch(config)#exit  
switch#wr  
  
  
***Para modificar la vlan nativa del enlace troncal***  
  
switch#conf t  
switch(config)#interface numero de la interface  
switch(config-if)# switchport trunk native vlan numero de la vlan  
switch(config-if)#end  
switch(config)#exit  
switch#wr

**ENRUTAMIENTO**

Algunos de los trabajos en redes en mi Universisdad han llegado a ser muy latosos les presento algunos para que los chequen.  
  
Algunos de los tipos de enrutamiento:  
  
OSPF  
RIP  
EIGRP  
ESTATICO  
**Configurar OSPF  
(Configuración Básica)**  
  
Router> enable  
  
Router# config terminal  
  
Router(config)# router ospf 1  
(número del 1 al 65535 como ID de Proceso, este número lo adjudica el admin y no tiene que coinidir entre routers de la misma área para ser vecinos)  
  
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0  
(publicamos la red directamente conectada, siempre hay que utilizar la wilcard y el ID del área debe ser la misma para todos los routers del área)  
  
Router(config-router)# network 192.168.10.8 0.0.0.3 area 0  
(publicamos la subred directamente conectada, siempre hay que utilizar la wilcard y el ID del área debe ser la misma para todos los routers del área)  
**Configurar EIGRP  
(Configuración Básica)**  
Router> enable  
  
Router# config terminal  
  
Router(config)# router eigrp 100  
(número del 1 al 65535 como ID de Proceso / Sistema Autónomo, los routers para ser vecinos (adyacentes) tiene que poseer el mismo ID de Proceso / Sistema Autónomo)  
  
Router(config-router)# network 10.0.0.0  
(publicamos la red directamente conectada)  
  
Router(config-router)# network 192.168.10.8 0.0.0.3  
(con la máscara wilcard publicamos una subred específica directamente conectada)  
  
**Configuración de Rutas Estáticas**  
  
Las rutas estáticas se configuran mediante el comando ip route, en el modo configuración global, utilizando la siguiente sintaxis:  
  
  
Router(config)# ip route « IP destino + máscara de red destino ó subred destino » « IP del siguiente salto ó interfaz de salida » « distancia administrativa »  
  
IP destino + máscara de red o subred destino: La IP específica la red o host que se quiere alcanzar junto con la máscara de red o subred correspondiente.  
  
IP del siguiente salto: Es la IP de la interfaz del router conectado directamente al router donde se está configurando la ruta estática.  
  
Interfaz de salida: Es la interfaz serial del router donde se está configurando la ruta estática. Se utiliza en el caso de desconocer la IP del siguiente salto.  
  
Distancia administrativa: Si no se especifica distancia administrativa, esta tomará el valor por defecto de 1 en la tabla de enrutamiento. El valor puede ser de 1-255, siendo 1 el valor que da más importancia a la ruta.  
  
  
**Configurar RIP**  
**(Configuración Básica)**  
  
RIP es muy fácil de configurar así que no creo que tengan problemas.   
  
Cualquier cosa o duda me consultan.  
  
Router> enable  
  
Router# config terminal  
  
Router(config)# router rip  
  
Router(config-router)# network 10.0.0.0  
(publicamos la red directamente conectada)  
  
Router(config-router)# network 172.16.0.0  
(publicamos la red directamente conectada)  
  
Router(config-router)# version 2   
  
**(habilitamos la versión 2 de RIP)**