

VLANS



Antes de Imprimir este documento
considere si es necesario
Ayudemos al Ambiente !!!!

Universidad San Carlos de Guatemala
— DANILO ESCOBAR —

VLANs

► VLANs

Al crecer el número de dispositivos dentro de las primeras redes los siguientes problemas se volvieron evidentes.

1. Más dispositivos implicaban una mayor cantidad de concentradores y una mayor transmisión de *broadcasts* lo que impactaba negativamente el rendimiento y escalabilidad de la red.
2. Grupos con diferentes funciones dentro de una organización se encontraban limitados físicamente debido a su conexión con los dispositivos (Ej.: Todas las secretarías debían estar conectadas al mismo *switch* para acceder a los servicios que necesitaban). Limitando su movilidad y condicionando su ubicación dentro de un inmueble.
3. Para conectar grupos asociados a redes diferentes se necesitaba introducir algún dispositivo capaz de enrutar entre las mismas o añadir interfaces a equipos existentes, lo que incrementaba los costos.
4. Pobre control de acceso y poca capacidad para aplicar calidad de servicio.

Para solucionar o paliar estos problemas se introduce el concepto de las redes locales virtuales mejor conocidas como *Virtual LANs (VLANs)*.

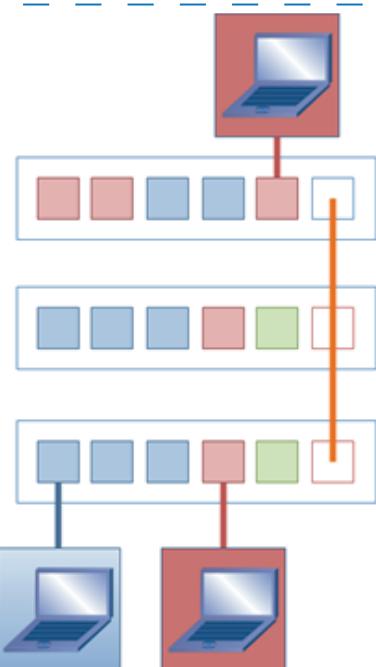
Las VLANs fueron creadas en los años 80 por Walter David "Dave" Sincoskie y permiten separar los puertos de cada *switch* y asignarlos a grupos lógicos distintos donde cada uno de ellos constituye su propio dominio de *broadcast* lo que posibilita la utilización de varias redes independientes dentro de un mismo concentrador.

Dicha tecnología permite agregar usuarios a una agrupación lógica accesible desde cualquier *switch* de acceso en la infraestructura, lo que elimina las limitaciones físicas, reduce el *broadcast*, y mejora el control de acceso.

La asignación a estos grupos se realiza de manera individual dentro de la configuración cada puerto, siendo imposible que dispositivos finales conozcan la VLAN a la que están conectados, estando todos asignados a la VLAN 1 por defecto.

VLANs

Para mostrar el funcionamiento de esta tecnología se presenta el siguiente ejemplo, en donde varias VLANs han sido configuradas y pueden ser consideradas, para propósitos prácticos, redes completamente separadas (Ej.: Los puertos rojos solo podrán alcanzar los puertos del mismo color).



Implementación de VLANs.

Adviértase también la existencia de un puerto con un funcionamiento especial, encargado de transmitir información de todas las VLANs hacia los demás switches, llamado puerto troncal (*Trunk*) por Cisco y como puerto etiquetado (*Tagged Port*) por todos los demás fabricantes, y que facilita en gran medida la escalabilidad de la red (De lo contrario se necesitaría un enlace entre switches por cada uno de los grupos lógicos).

Para crear una VLAN y asignarle un nombre es posible utilizar la siguiente secuencia de instrucciones desde el modo de configuración global.

```
Switch(config)#vlan 10  
Switch(config-vlan)#name TECNICOS
```

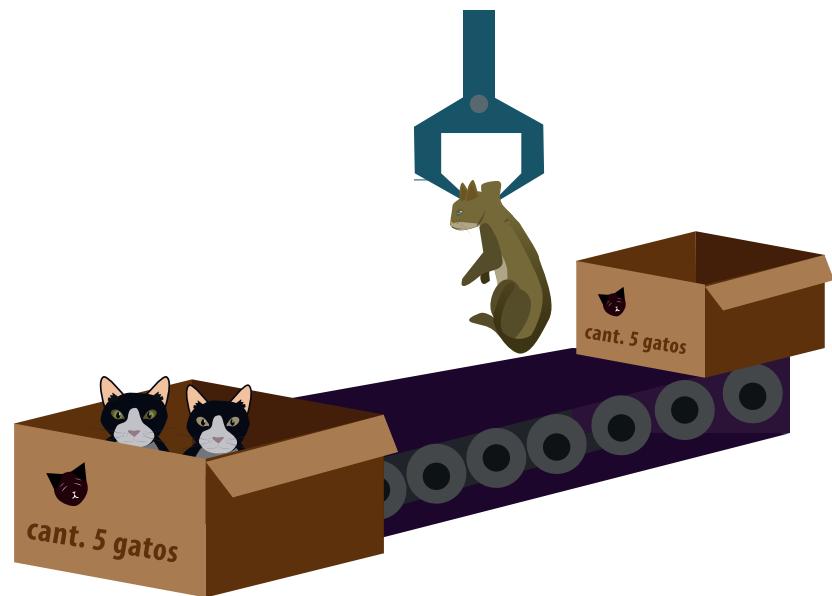


VLANs

Para visualizar las VLANs existentes así como los puertos asignados a ellas se utiliza el comando *show vlan brief*.

```
Switch# show vlan brief
```

| 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 |
| 10 TECNICOS | active | |
| 1002 fddi-default | active | |
| 1003 token-ring-default | active | |
| 1004 fddinet-default | active | |
| 1005 trnet-default | active | |



La VLAN 1 es la VLAN por Defecto a donde están asignados todos los puertos mientras que las VLANs 1002-1005 son mantenidas por cuestiones de compatibilidad, por lo que ninguna de ellas puede ser removida.

VLANs

Modos de un puerto

Los puertos de un switch pueden trabajar en uno de los siguientes modos.

- Modo troncal (*mode trunk*): Configura el puerto para que etiquete, envíe y posibilite la comunicación entre VLANs en switches diferentes.

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode trunk
```

Los enlaces troncales son examinados con más detalle más adelante.

- Modo de acceso (*mode access*): Configura el puerto para no utilizar ninguna marcación y funcionar en una VLAN específica, siendo por defecto la VLAN 1.

```
Switch(config)# interface fastEthernet 0/2
Switch(config-if)# switchport mode access
```

Una vez en el modo de acceso es posible asignar dicho puerto a una VLAN específica, de la manera que se muestra a continuación.

```
Switch(config-if)# switchport access vlan 10
```

Es posible verificar la asignación utilizando nuevamente el comando *show vlan brief* o a través del comando *show vlan name* como se muestra acto seguido.

| Switch# show vlan brief | | | |
|-------------------------|--------|---|--|
| VLAN Name | Status | Ports | |
| 1 default | active | 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 | |
| 10 TECNICOS | active | Fa0/2 | |
| 1002 fddi-default | active | | |
| 1003 token-ring-default | active | | |
| 1004 fddinet-default | active | | |
| 1005 trnet-default | | | |

VLANs



```
Switch# show vlan name TECNICOS
```

| VLAN Name | Status Ports |
|---------------------------------|---|
| 10 TECNICOS | active Fa0/2 |
| VLAN Type SAID | MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 |
| 10 enet 100010 1500 - - - - 0 0 | |

!! Nótese que los puertos en modo troncal no son mostrados en la salida de !! ninguno de estos comandos (El puerto Fa 0/1 no se encuentra en la lista de !! puertos).

Enlaces troncales

Están formados por puertos especiales que posibilitan la transmisión de información de múltiples VLANs a través de un solo enlace y que pueden utilizar uno de los siguientes protocolos para encapsular la información.

- Inter-Switch Link (ISL): Un protocolo propietario de Cisco ahora deprecado y no soportado en todos los dispositivos de este fabricante por lo que su funcionamiento y comportamiento no serán discutidos en este trabajo.
- 802.1Q: El estándar abierto creado por la IEEE, cuyo comportamiento y características moldearán el resto de las discusiones presentadas.

La función de un puerto troncal consiste en marcar o etiquetar (de ahí el nombre de puerto etiquetado) las tramas con la información de la VLAN donde se originó antes de enviarlas hacia otro dispositivo donde serán recibidas por otro puerto, con el mismo rol, el cual removerá dicha marcación para luego reenviar dichas tramas a la VLAN correcta.

VLANs

Al contrario de otros fabricantes en donde deben ser agregadas manualmente, Cisco permite por defecto la transmisión de todas las VLANs a través de los enlaces troncales, siendo posible limitar las mismas con el comando `switchport trunk allowed vlan`.

```
Switch(config-if)# switchport trunk allowed vlan ?
```

WORD VLAN IDs of the allowed VLANs when this port is in trunking mode
add add VLANs to the current list
all all VLANs
except all VLANs except the following
non no VLANs
remove remove VLANs from the current list

A manera de ejemplo, si el objetivo fuera permitir solamente las VLAN 10 y 20 a través del enlace se podría utilizar el comando anterior de la siguiente manera.

```
Switch(config-if)# switchport trunk allowed vlan 10,20
```

Para mostrar una lista de las interfaces troncales, las VLANs que pueden ser transmitidas a través de los mismos, así como otros detalles importantes se utiliza la instrucción `show interfaces trunk`.

```
Switch# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 10,20

Port Vlans allowed and active in management domain
Fa0/1 10,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 10,20
```



VLANs

► *Dynamic Trunking Protocol (DTP)*

Es un protocolo propietario de Cisco que busca simplificar el uso del *switch* al usuario final al negociar automáticamente el modo de un puerto para que este funcione como un puerto de acceso o uno troncal.

Para tratar de establecer un enlace troncal automáticamente con otro dispositivo, es posible configurar el puerto de un *switch* como *Dynamic Desirable*, *Dynamic Auto* o directamente en modo *trunk* (Cuya configuración vuelve a mostrarse para completar el ejemplo).

```
Switch(config)# interface fastethernet 0/3
Switch(config-if)# switchport mode dynamic desirable
```

```
Switch(config-if)# interface fastethernet 0/4
Switch(config-if)# switchport mode dynamic auto
```

```
Switch(config-if)# interface fastethernet 0/5
Switch(config-if)# switchport mode trunk
```

No todas las combinaciones de los modos mencionados resultan en la formación de un enlace troncal debido a diferencias en su funcionamiento

Los modos *Dynamic Desirable* y *Trunk* tratarán activamente de formar un enlace troncal, mientras que en el modo *Dynamic Auto* el puerto será un troncal solamente cuando el otro lado lo solicita. De esta manera si en los dos extremos de un enlace se tienen los modos *Dynamic Auto* y *Dynamic Desirable* respectivamente, se volverá un enlace troncal, mientras que si los dos extremos están configurados como *Dynamic Auto* el enlace troncal no se formará quedando los puertos en el modo de acceso.

La ejecución de DTP constituye un gran riesgo de seguridad dentro de una red, ya que un atacante podría negociar, a través de un dispositivo real o *software* especial, un enlace troncal con el *switch* donde está conectado y tener acceso a todas las VLANs existentes, ataque conocido como *switch spoofing*.

Por esta razón, es una mejor práctica configurar manualmente tanto los puertos troncales como los de acceso para luego deshabilitar DTP en todas las interfaces con el siguiente comando.

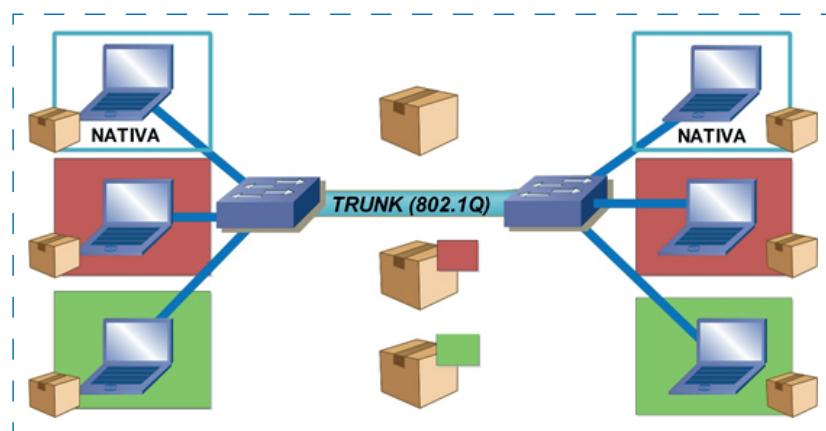
```
Switch(config-if)# switchport nonegotiate
```

VLANs

VLAN nativa

Por cuestiones de retrocompatibilidad e interoperabilidad con otros dispositivos el estándar 802.1Q ofrece la posibilidad de que las tramas sean enviadas con o sin etiqueta a través de un enlace troncal.

Las tramas sin etiquetar, destinadas originalmente a dispositivos incapaces de trabajar con dicha marcación, pertenecen a una VLAN especial llamada VLAN nativa.



Las tramas pertenecientes a la VLAN Nativa se envían sin etiquetar a través de un enlace troncal.

Cualquier VLAN, existente o no dentro del switch, puede tomar el rol de la VLAN nativa en un troncal, responsabilidad que recae por defecto sobre la VLAN 1 misma donde la cual están asignados todos los puertos de manera predeterminada lo que a menudo es fuente de confusión.

La VLAN 1 tiene una importancia especial, al ser utilizada como VLAN predeterminada por todos los fabricantes, siendo en el caso de Cisco empleada también para la transmisión de ciertos protocolos de control tales como el *Cisco Discovery Protocol* (CDP), *Port Aggregation Protocol* (PAgP) y *Vlan Trunking Protocol* (VTP) independientemente de si la VLAN 1 es la VLAN nativa o no.

Por esta razón la VLAN 1 no puede ser eliminada de un switch ni completamente filtrada de un enlace troncal.

Tomando en cuenta que en un puerto troncal de los dispositivos Cisco todas las VLAN son permitidas por defecto es posible utilizar el siguiente comando para intentar remover la VLAN 1 de dicho enlace.

```
Switch(config-if)# switchport trunk allowed vlan remove 1
```

VLANs

Al ejecutar el comando anterior se consigue filtrar todo el tráfico enviado por los usuarios asignados a esa VLAN en particular, más no el tráfico de los protocolos de control mencionados anteriormente que continuarán funcionando con normalidad.

De manera separada a toda la funcionalidad que acaba de explicarse, la VLAN 1 se utiliza también de manera predeterminada para cumplir la función de la VLAN nativa, aunque esto puede cambiarse de manera individual dentro de cada puerto troncal como se muestra a continuación.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport trunk native vlan ?
<1-1005> VLAN ID of the native VLAN when this port is in
trunking mode
Switch(config-if)# switchport trunk native vlan 100
```

Nótese que ahora la VLAN que enviará sus paquetes sin ningún tipo de marcación será la VLAN 100, mientras que la funcionalidad de la VLAN 1 permanecerá inalterada, con la única diferencia de que el tráfico generado por los protocolos que hacen uso de la misma serán etiquetados lo que tampoco impedirá su correcto funcionamiento.

Una consideración importante es que al ser configurada sobre cada puerto de manera individual existe la posibilidad de configurar un enlace cuyos dos extremos utilicen una VLAN

Nativa diferente, condición que se conoce como discrepancia de VLANs Nativas (*Native VLAN Mismatch*) y que en el caso de Cisco puede ser detectada gracias al *Cisco Discovery Protocol* (CDP) el cual bloqueará las VLANs en conflicto para evitar problemas más serios dentro de la red.

```
Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk

Switch2(config)# interface fastethernet 0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk native vlan 10
Switch2(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on FastEthernet0/1 (10), with Switch FastEthernet0/1 (1).
```

Los protocolos que hacen uso de la VLAN Nativa para intercambiar información son DTP y *Spanning-Tree Protocol* (STP) el cual es un protocolo cuya función consiste en evitar bucles de capa 2 y que se presenta más adelante.

La elección de una VLAN nativa no es sencilla, debiendo considerarse varios factores dependiendo de los cuales no será posible llegar a una solución completamente satisfactoria en todos y cada uno de los casos.

VLANs

El primer factor será la interoperabilidad con dispositivos de otros fabricantes, algunos de los cuales solo son capaces de utilizar la VLAN 1 como VLAN nativa, forzando a los demás switches a utilizar la misma configuración.

El segundo factor es el de la seguridad. El estándar 802.1Q no incluye ninguna limitación acerca del número de etiquetas presentes en una misma trama, por lo que es posible que un atacante marque o doble marque su propia información con la intención de alcanzar una VLAN diferente, ataque que se conoce como salto entre VLANs (VLAN Hopping). Para mitigar este ataque se presentan las siguientes opciones:

1. No asignar ningún puerto en modo de acceso del switch a la VLAN Nativa.
2. Filtrar la VLAN Nativa de los puertos troncales. Lo que no es recomendado ya que puede interrumpir el correcto funcionamiento de ciertos protocolos.
3. Forzar la marcación de los paquetes provenientes de la VLAN nativa, lo que puede realizarse desde el modo de configuración global:

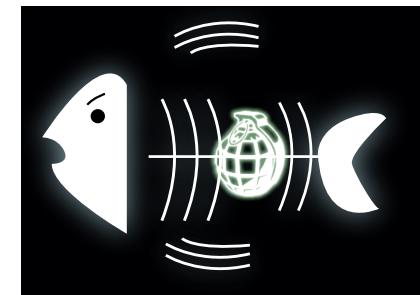
```
Switch(config)# vlan dot1q tag native
```

O en cada puerto troncal:

```
Switch(config)# interface fastethernet 0/1  
Switch(config-if)# switchport trunk native vlan tag
```

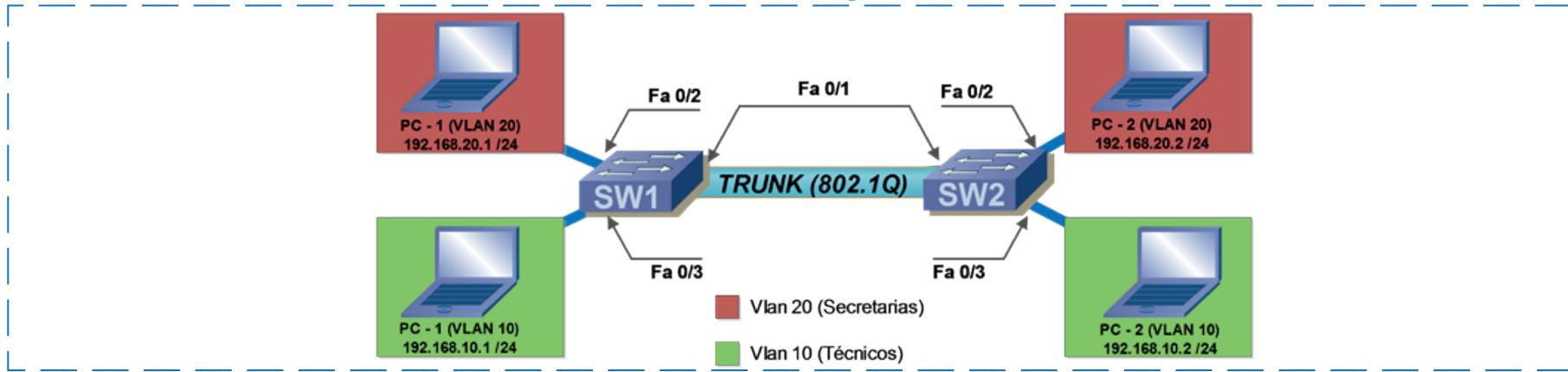
Esta opción no está disponible en toda la gama de switches Cisco y podría no ser interoperable con dispositivos de otros fabricantes.

Dadas las consideraciones anteriores se recomienda, por razones de diseño y seguridad, no utilizar la VLAN 1 ni la VLAN Nativa en ningún puerto de acceso, o en otras palabras, no utilizar estas dos VLANs especiales en redes destinadas a los usuarios.



VLANs

Resumen de la configuración VLANs



Switch SW1

```
SW1(config)# vlan 10
SW1(config-vlan)# name Tecnicos

SW1(config)# vlan 20
SW1(config-vlan)# name Secretarias

SW1(config)# interface fastethernet 0/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport nonegotiate
SW1(config-if)# switchport trunk allowed vlan 10,20

SW1(config)# interface fastethernet 0/2
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20

SW1(config)# interface fastEthernet 0/3
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
```

Switch SW2

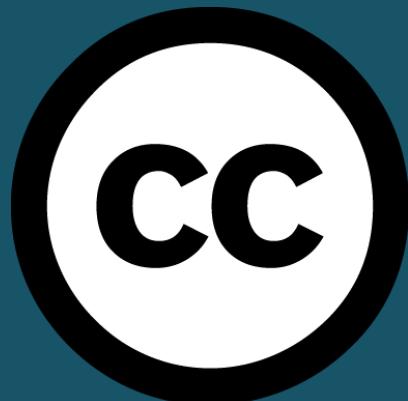
```
RSW2(config)# vlan 10
SW2(config-vlan)# name Tecnicos

SW2(config)# vlan 20
SW2(config-vlan)# name Secretarias

SW2(config)# interface fastethernet 0/1
SW2(config-if)# switchport mode trunk
SW2(config-if)# switchport nonegotiate
SW2(config-if)# switchport trunk allowed vlan 10,20

SW2(config)# interface fastethernet 0/2
SW2(config-if)# switchport mode access
SW2(config-if)# switchport access vlan 20

SW2(config)# interface fastEthernet 0/3
SW2(config-if)# switchport mode access
SW2(config-if)# switchport access vlan 10
```



► **Diseño y edición:**

María Esther Pineda
Carolina Villatoro

► **Descargo de Responsabilidad**

El autor y los colaboradores de este trabajo han hecho su mejor esfuerzo en la preparación del mismo para asegurar que su contenido sea lo más exacto posible, sin embargo, no se hacen responsables por el uso de la información en este documento así como de errores u omisiones que pudieran resultar en pérdida de cualquier tipo.

La información está proporcionada “como está” para ser utilizada bajo “su propia cuenta y riesgo”.