**VLANs**

**VLANs (redes virtuales) nos permiten implementar de forma eficiente el tráfico dentro de una red de cobertura local.**

**Las VLANs se pueden instalar tanto en el router como en el switch.**

Se lee el ejercicio 15, lo que se pide hasta las preguntas.

Con el video podemos ver cuál es el significado de las VLANs.

**VLANs permiten segmentar el tráfico cuando tenemos la necesidad de dividir de forma lógica distintos segmentos.** Por ejemplos: Una analogía con el tecnológico de Monterrey donde tenemos el segmento de estudiantes, segmento de servidores, segmento de profesores y un segmento para invitados. Y esto se logra a través del uso de VLANs.

**Cada VLAN corresponde a un dominio de broadcast, es decir, a una misma subred.**

**Presentación CISCO VLANS**

Para las **VLANs necesitamos aplicar el concepto de las VLSMs** para hacer una segmentación dependiendo las restricciones de conectividad y así formar las subredes o bloques.

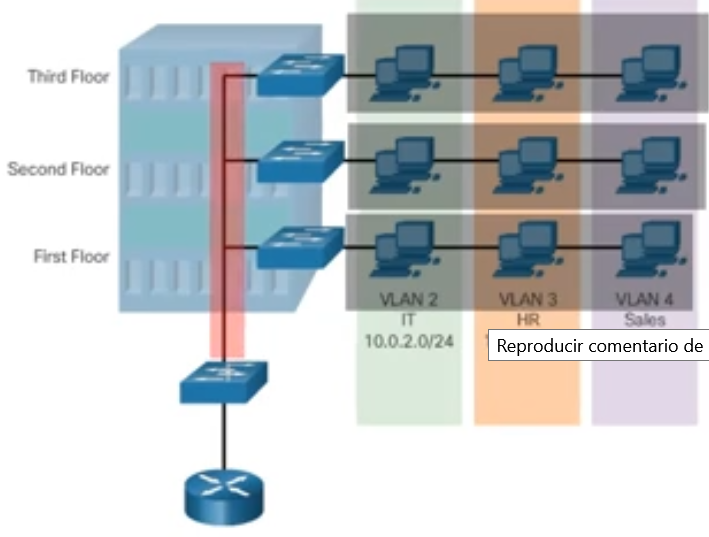
En este ejemplo, tenemos tres dominios de broadcast de distinto color, cada uno de ellos asociado con un grupo de puertos en cada uno de los distintos switches.

**Los puertos de cada switch están asignados a VLANs distintas.**

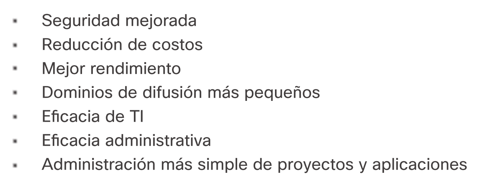
Los tres tipos de tráfico circulan por el mismo switch (enmarcado en rectángulo)



Es importante comentar que en el caso de las **comunicaciones que se están dando entre los switches** **hay una conexión de todas esas redes virtuales que es identificado como de tipo troncal.** Para formar los enlaces de tipo troncal, el puerto en el switch se configura como de tipo troncal.



**Beneficios de las VLANs**

****

**Mejora la seguridad**,

* Los switches se pueden programar y cada uno de los puertos están asociados únicamente con una MAC que se puede conectar. A través de asignar a cada puerto del switch una MAC específica.
* Adicionalmente incrementamos la seguridad ya que no hay tráfico que circule entre todas las subredes logrando con ello una segmentación, teniendo un control de los distintos tipos de usuarios.

**Reduce costos.** No necesitamos varios routers para segmentar el tráfico, puedo tener un router y con uno o dos puertos ethernet son suficientes para generar un conjunto de segmentos de red. ( le conecto switches en los que se segmenta el tráfico).

**Puedo conseguir un Mejor desempeño**. Con las VLANs puedo incrementar la posibilidad de segmentar el tráfico, conseguir por cada segmento un mejor desempeño.

Específicamente podemos separar el tráfico de los usuarios (el tráfico de datos) y el tráfico de telefonía. Cada VLAN tiene su propia aplicación en específico.

VLAN 150 que corresponde con el uso de telefonía IP.

**Podemos tener dominios de broadcast más controlados de distinto tamaño y más reducidos.** podemos tener dominios de broadcast en segmentos reducidos, de distintos tamaños según las necesidades.

Es **más eficiente para los administradores que gestionan los recursos de IT**, ya que los administradores pueden conectarse de manera remota y de manera muy simple pueden cambiar los puertos de una VLAN a otra VLAN. Es más rápido y eficiente realizar este tipo de cambios, ya que son cambios lógicos no físicos.

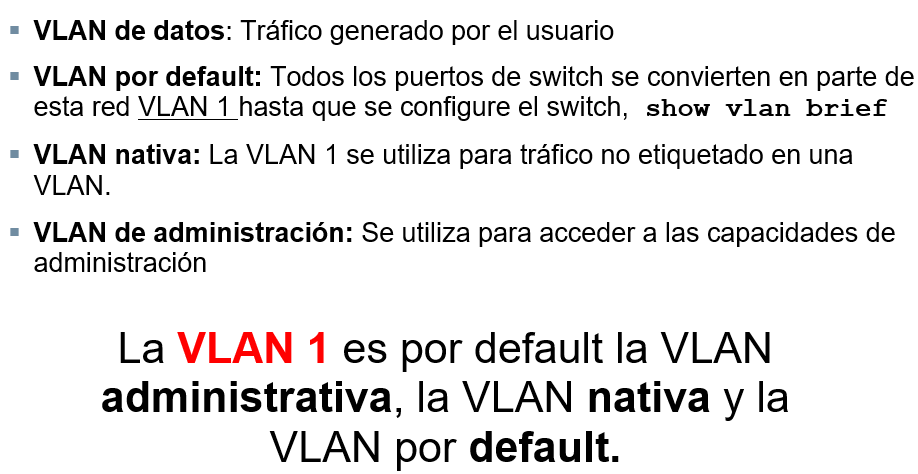
Finalmente, podemos **simplificar la gestión de los proyectos**.

**Tipos de VLANs**

Antes de que un switch sea configurado, todos los puertos de un switch pertenecen a la VLAN 1.

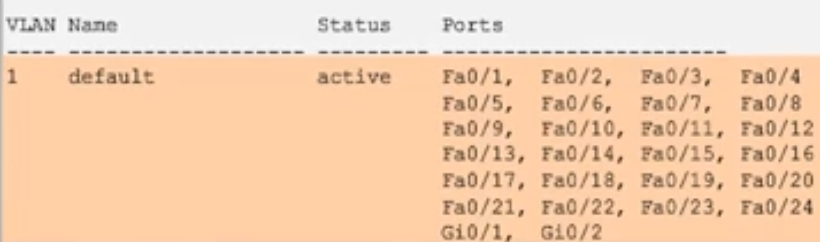
**Características importantes de la VLAN 1:**

* Mientras no existan VLANs configuradas todo el tráfico que fluye a través de un switch circula en la VLAN 1 por default.
* Todos los puertos de un switch pertenecen a la VLAN 1.
* La VLAN nativa que es la administradora de todo es la VLAN 1, por ahí circula todo el tráfico que no ha sido identificado en una VLAN.
* Hay una VLAN administrativa que por default es la VLAN 1. En el laboratorio pasado cambiamos la VLAN administrativa de la VLAN 1 a la VLAN 99.



Cuando hacemos un acceso remoto por telnet o ssh nos conectamos a la IP de la **VLAN 1** que es la vlan administrativa.

Al momento que se inicializa el equipo todos los puertos pertenecen a la VLAN 1.



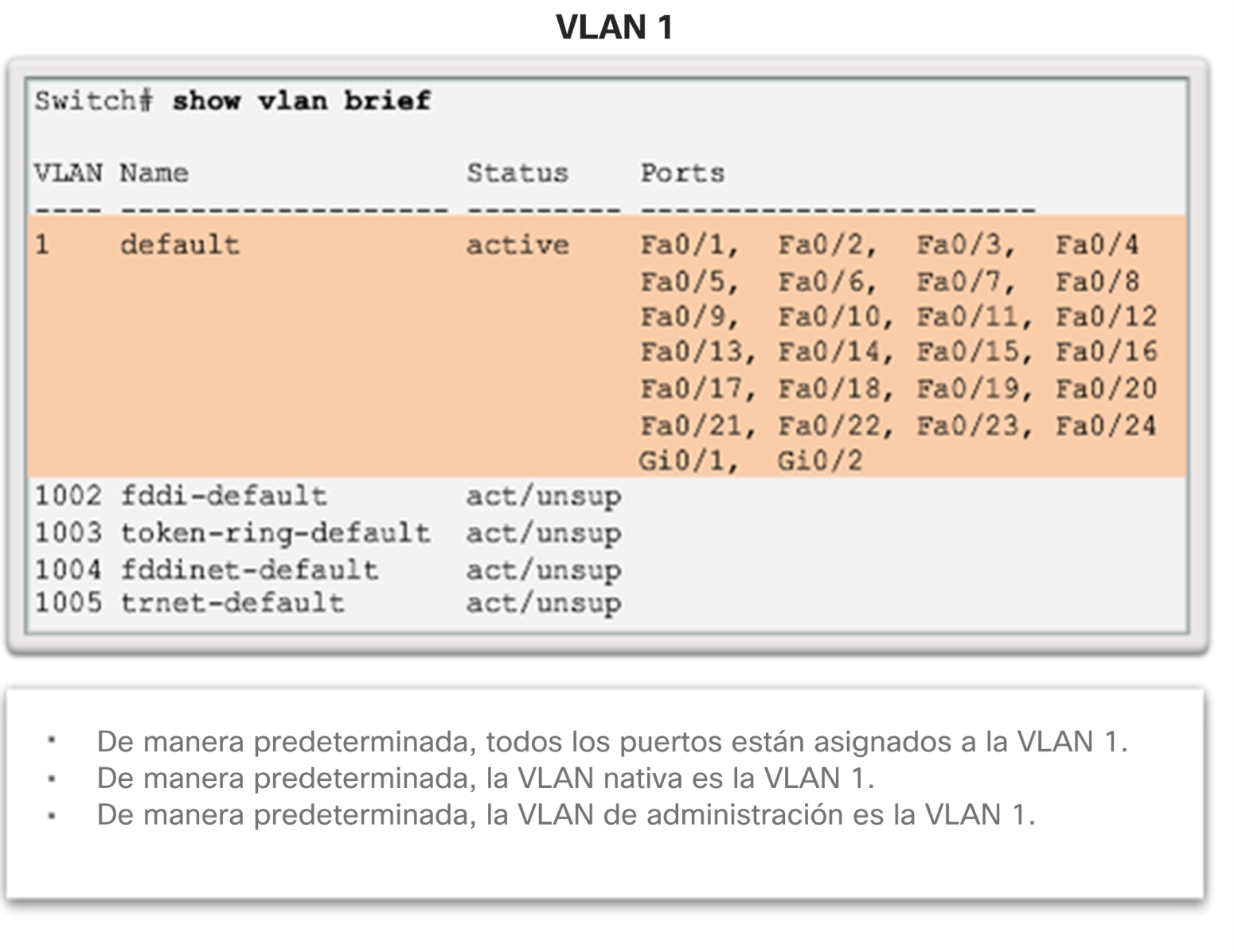
Tenemos arriba de **4000 VLANs** (2 a la 12) = 4096, pero de la 1 a la 1001 son las VLANs que nosotros podemos administrar, las otras son VLANs extendidas.

Las VLAN que no se pueden mover son la:

* VLAN 1 por default, siempre existirá, nosotros podemos mover los puertos a otras VLANs pero la VLAN 1 continuará existiendo.
* 1002 que corresponde a una comunicación por FDDI fibra óptica
* 1003 por token ring

No se pueden mover, están definidas en los equipos y han sido creadas con estos propósitos.

Y otras adicionales como la 1004 y la 1005.

****

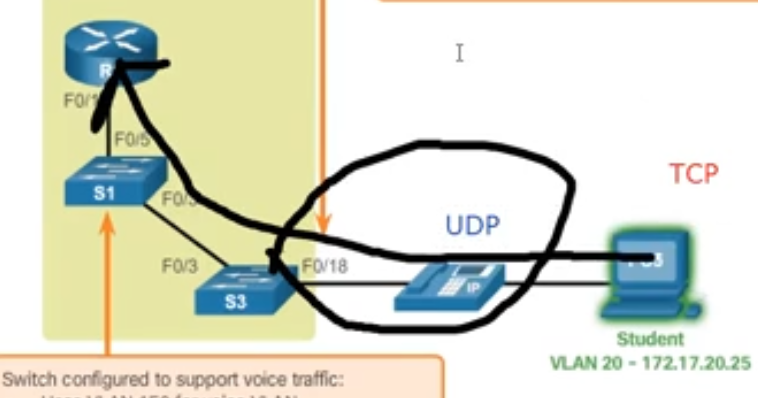
Específicamente podemos separar el tráfico de los usuarios (el tráfico de datos) y el tráfico de telefonía. Cada VLAN tiene su propia aplicación en específico.

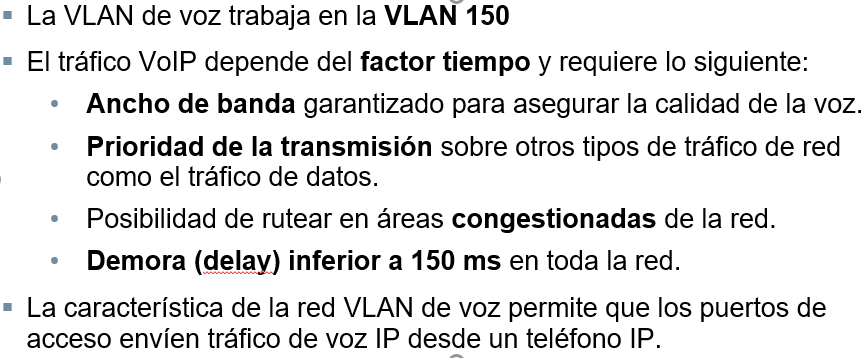
**VLAN 150** que corresponde con el uso de telefonía IP.

Todo el tráfico de la PC5 (tráfico de datos) hacia el Internet utiliza el protocolo **TCP**.

La telefonía IP utiliza el protocolo **UDP** para sacar las llamadas al exterior. El tráfico de telefonía tiene prioridad.

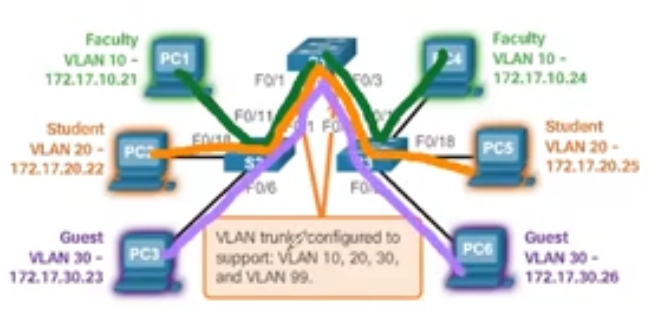
El delay no puede ser mayor de 150 milisegundos, ya que de lo contrario no sería una llamada en tiempo real, parecería una llamada interrumpida, que la otra persona no puede escuchar muy bien y se pierden las comunicaciones.





VLAN de datos son las VLAN de los usuarios, la VLAN de los docentes, estudiantes, invitados son VLANs se datos. La VLAN nativa y por default son vlans de datos. **Por default todo es datos.** Para poder transportar telefonía necesitas activar la VLAN 150.

Si queremos tener segmentación lógica debemos activar las VLANs correspondientes.

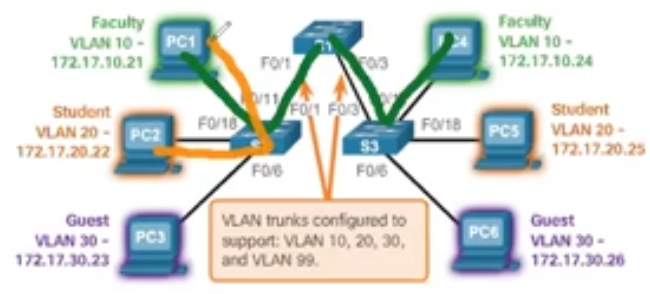


El tráfico de faculty cuando nosotros trabajamos de forma local se quedan dentro de las mismas comunicaciones **pero cuando las comunicaciones salen y tienen que utilizar los servicios de otro switch, esos puertos se tienen que habilitar como troncales**. Las conexiones entre los switches tienen que habilitarse como troncales. **A diferencia de los puertos de faculty, student y guest que tienen que estar habilitados como puertos de acceso.**

Recuerden que en el nivel de acceso nos conectamos físicamente a los switches. Es en el momento en el que el puerto se convierte de acceso, ya que le da acceso a la red.

**Para que se pueda dar la comunicación los puertos deben identificarse como troncales.** Un enlace troncal se identifica con el **protocolo 802.1Q** que identifica el tráfico entre vlans.

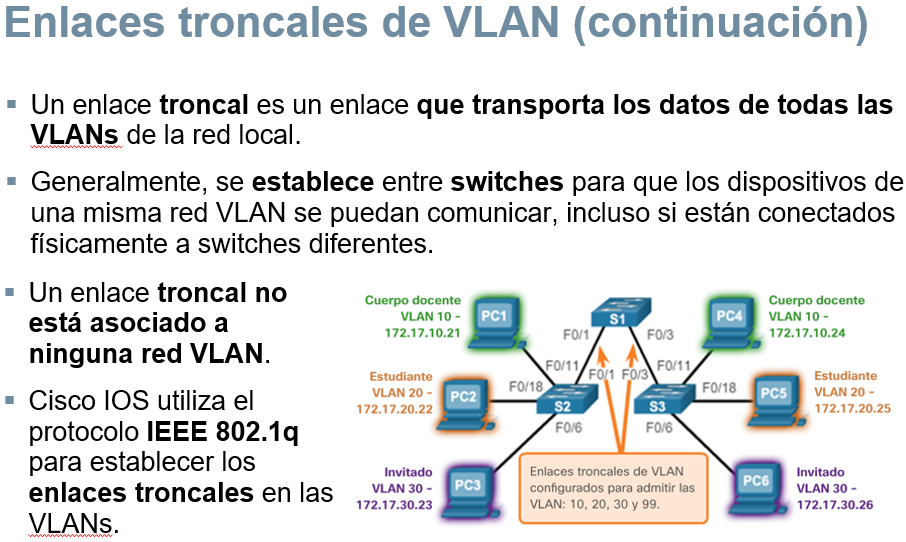
Comunicar VLANs distintas no va a poder ocurrir, ya que el switch no es capa 3 y no puede rutear.



**Notas importantes:**

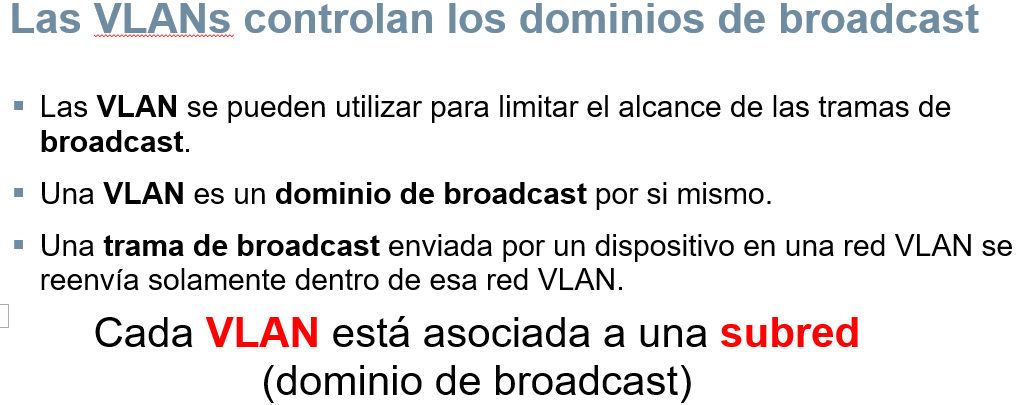
* Todos los puertos por default son de datos.
* Si queremos transmitir telefonía IP hay que activar en el puerto como de telefonía, activando la **VLAN 150**
* Si segmentamos necesitamos el uso de las VLANs (estudiantes, profes, invitados)
* Si queremos que se de el tráfico entre VLANs se deben habilitar los puertos troncales.

¿Qué es lo que un puerto troncal realiza?



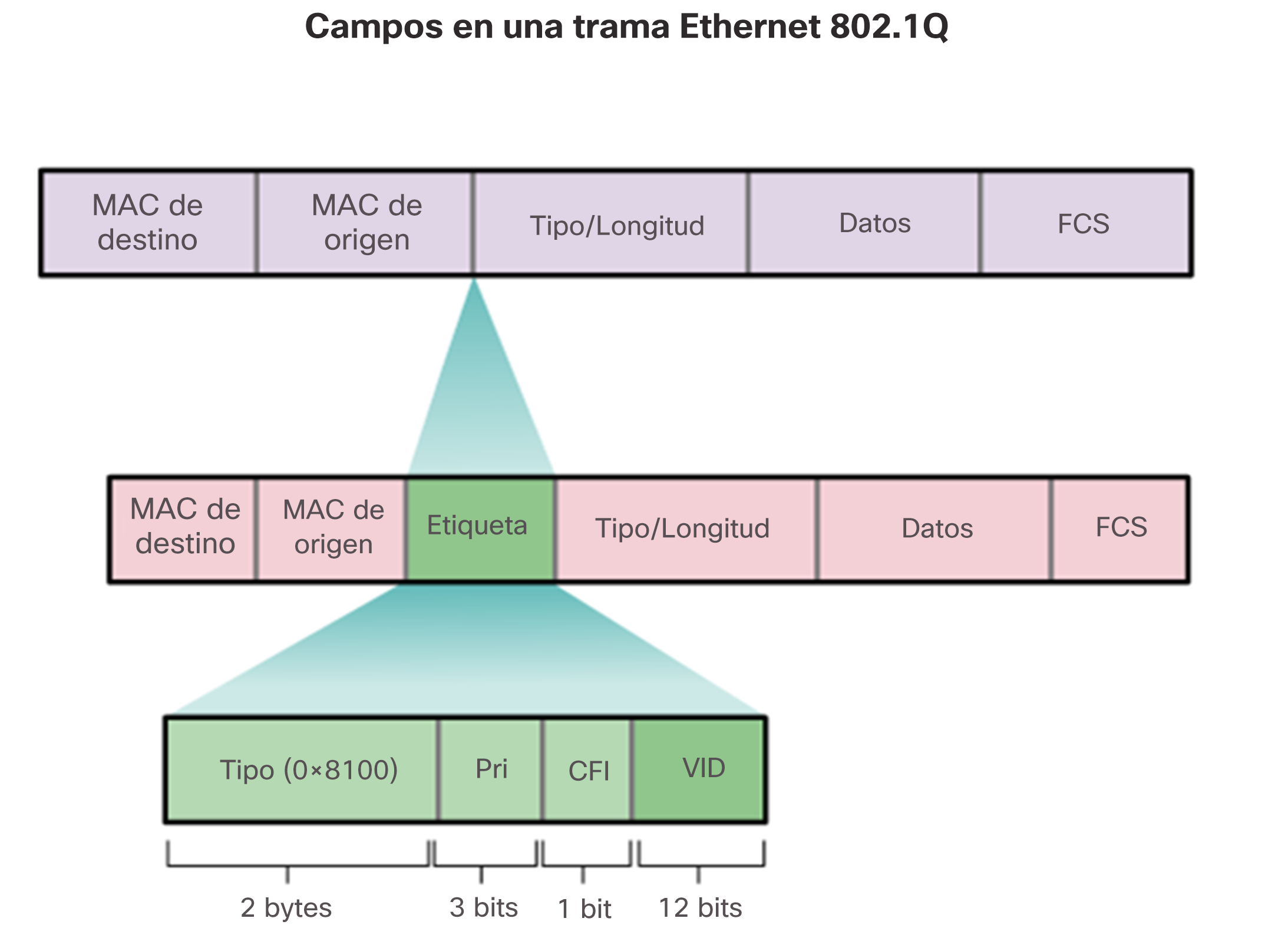
Existen tres tipos de puertos que pueden existir:

1. Puertos de datos o acceso
2. Puertos de telefonía
3. Puertos troncales (Pueden englobar los puertos de datos y de telefonía)Transporta tanto datos como telefonía al siguiente switch o al router.



**Cuando hay necesidad de enviar un mensaje de broadcast solamente en ese segmento es donde se da el intercambio de información.**

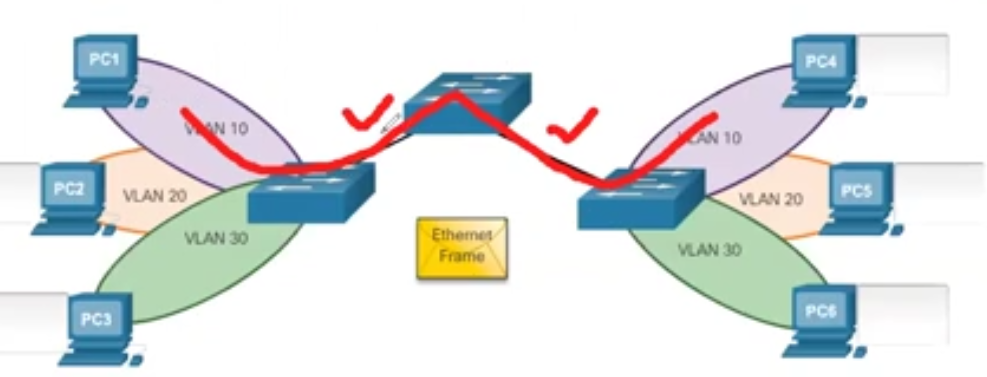
A la trama original Ethernet se le agrega otro elemento que es la etiqueta.

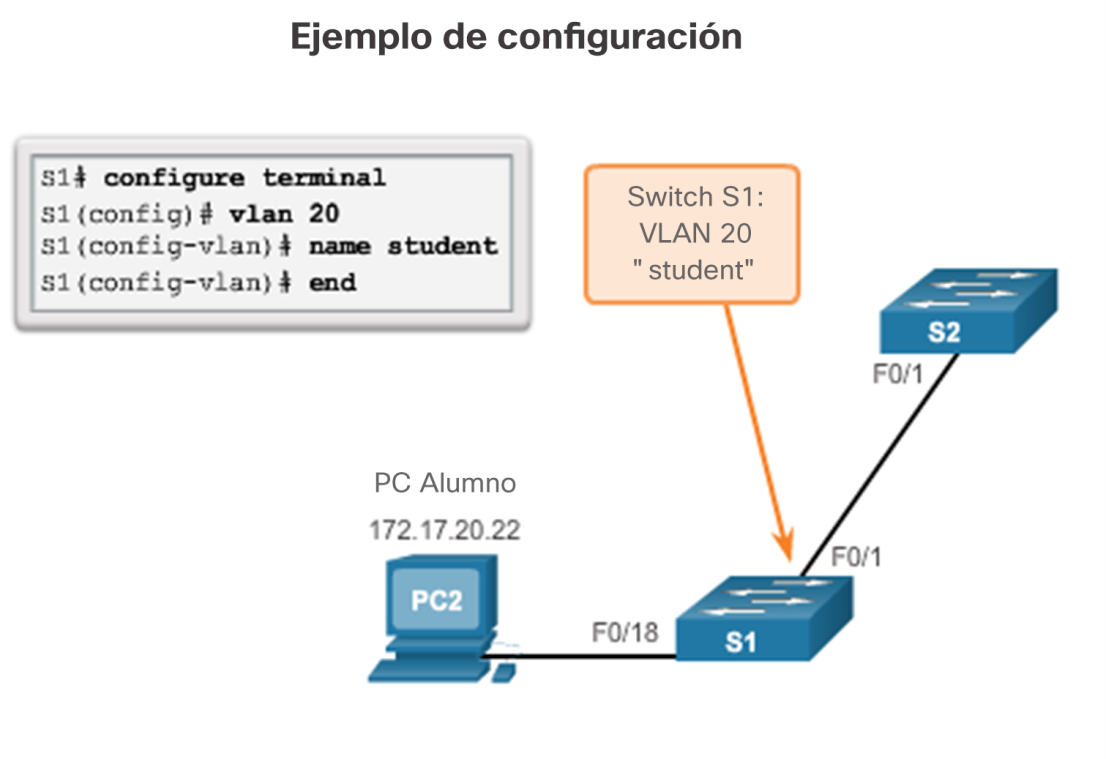


Se utilizan 12 bits para el identificador de la vlan **2 a la 12 = 4096**.

La VLAN #10 solamente se puede comunicar con servicios de la VLAN 10. La comunicación se va a dar por los puertos troncales. Los puertos troncales son los que interconectan switch con switch y si estuviera conectado con un router, también sería troncal.

Todos los switches deben tener la misma base de datos, deben manejar la vlan10, 20 y 30, de lo contrario las VLANs no se van a poder comunicar





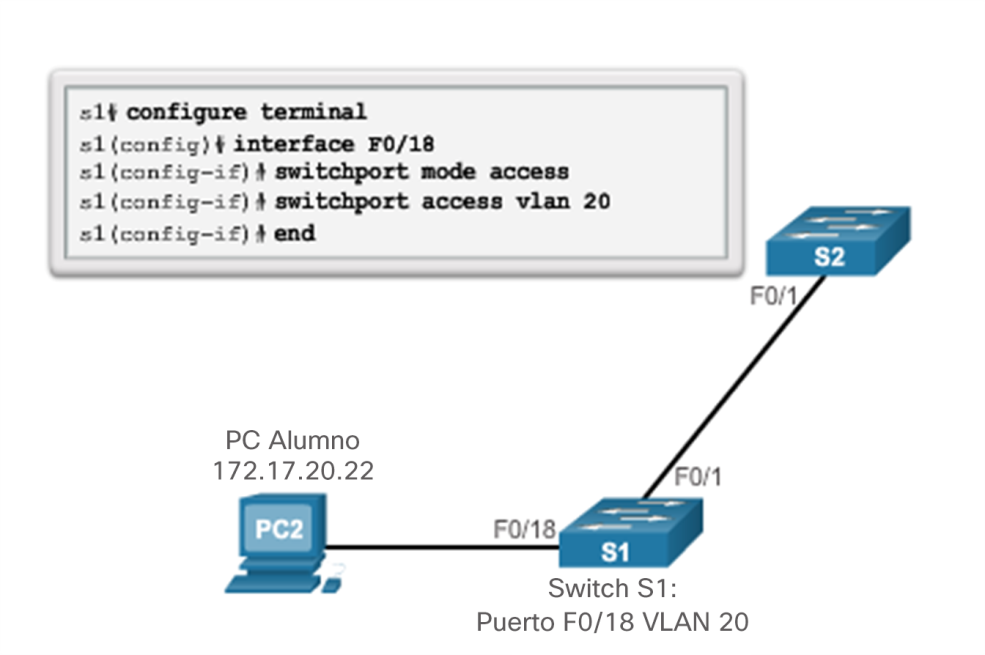
El nombre de la vlan es opcional, internamente las vlans no se conocen por nombre se conocen por etiqueta, las tramas se van a etiquetar con el id de la vlan.

Esto se identifica como la creación de la base de datos.



* **Identificar la interface que vamos a asignar.**
* **Identificar el modo del puerto. EL puerto puede ser de acceso, troncal o de telefonía.**
* **El puerto de acceso es un puerto de datos.**
* **La interface o rangos de interfaces se debe asociar a una vlan. Hay que asociar a la vlan correspondiente los puertos que estamos haciendo referencia.**

El puerto número 18 que pertenece a la vlan 20 está identificado como un puerto de acceso.



El nombre de la vlan no se utiliza en ningún momento solamente en la base de datos del switch. Y nos sirve para identificar que significa la vlan 10, o la vlan 20 etc.

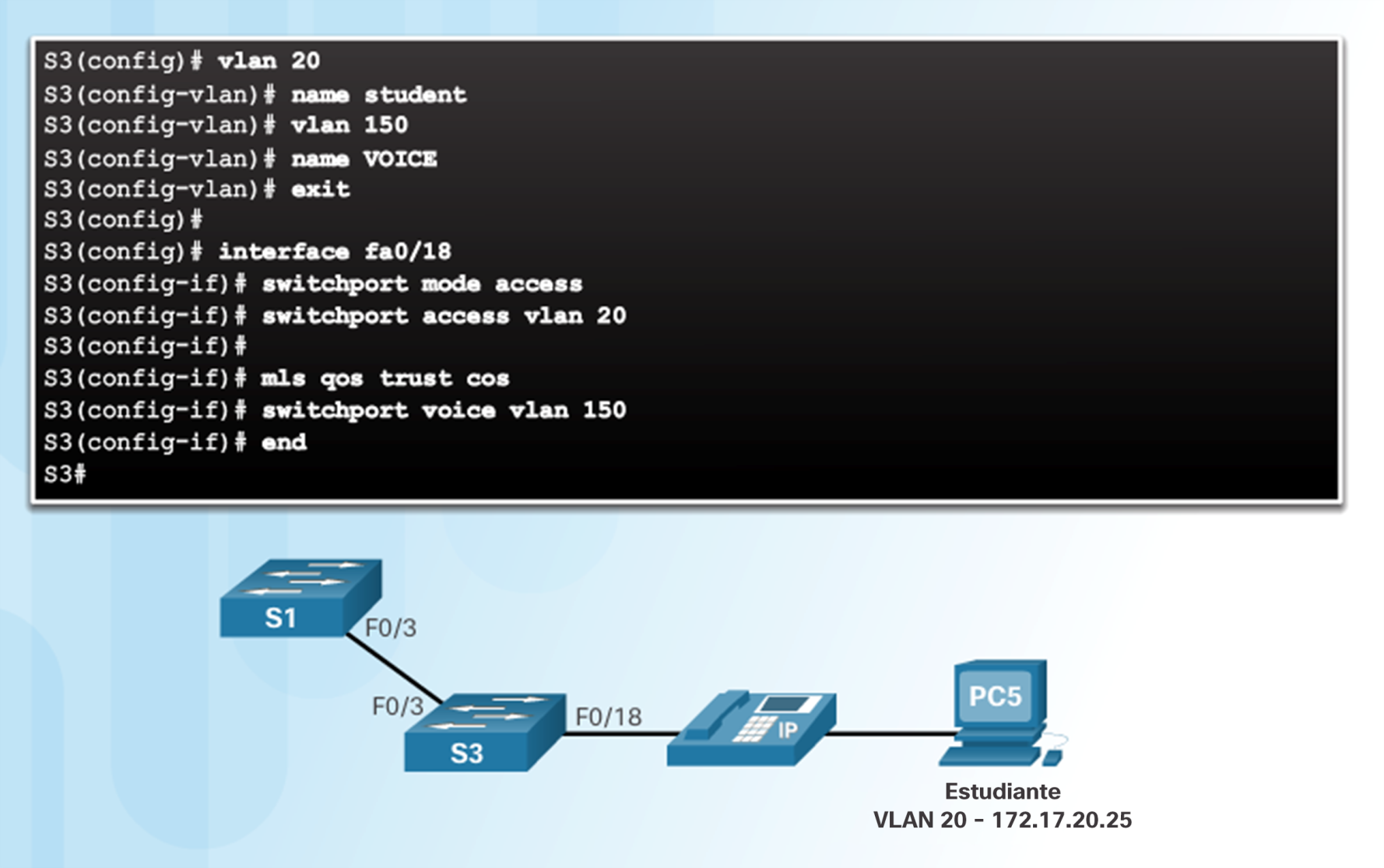
Recuerden existen tres tipos de puertos:

1. Puertos de datos o acceso
2. Puertos de telefonía
3. Puertos troncales (Pueden englobar los puertos de datos y de telefonía)Transporta tanto datos como telefonía al siguiente switch o al router.

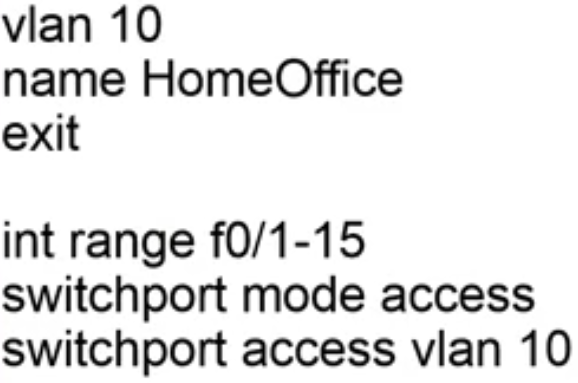
En la siguiente **implementación la PC y el teléfono están conectados al puerto 18**. El puerto 18 debe poder compartir datos y telefonía.

Se crean la **vlan 20** de **estudiantes** y la **vlan 150** es de **telefonía**.

1. En la segunda parte se asigna el **puerto 18 a la vlan 20 de datos**.
2. Después viene la **configuración para telefonía**. De esta forma un mismo puerto mezcla datos y telefonía. En nuestros ejercicios solamente trabajaremos con puertos de acceso y troncales.



La palabra range me permite configurar varios puertos pertenecen a la vlan 10. La primera parte es la creación de la base de datos. La segunda parte es la asignación de los puertos a la base de datos de la vlan 10.



**Comandos para verificar la información de las VLANs**

**Sh vlan brief** me muestra la información de la vlans en forma resumida.

**Sh vlan** me muestra la información de todas la vlans configuradas.

**Como configurar enlaces troncales.**

1. **Identifico interface o interfaces troncales.**
2. **Swith mode trunk**
3. **End**

Con estos tres comandos se configura un enlace troncal en equipos cisco, que tienen las mismas bases de datos.



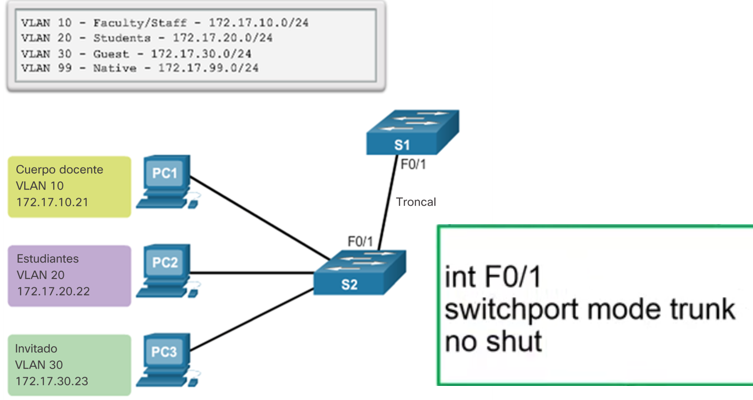
Si nos conectamos con otros equipos que no son CISCO, se requieren configurar el resto de los comandos.

* Cual es vlan nativa.
* Identificar la lista de vlans que se van a poder intercambiar.



**Pasos para configurar VLANs en los switches:**

1. **Creación de la base de datos. Dando vlan y name.**
2. **Definir el tipo de puerto que se va a utilizar : acceso, troncal o de telefonía.**
3. **Asociación de puertos a la vlan.**
4. **Identificar el puerto troncal y programarlo.**

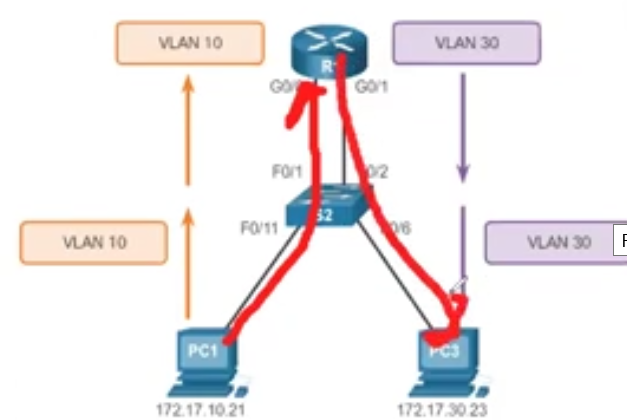


Para completar la configuración y poder conectarnos con un proveedor de servicios vamos a requerir un **router**.

* Para llevar a cabo la configuración del router se requieren de **subinterfaces**.
* Si queremos que se comuniquen dos vlans nativamente no se consigue, para esto se requiere un **router**.

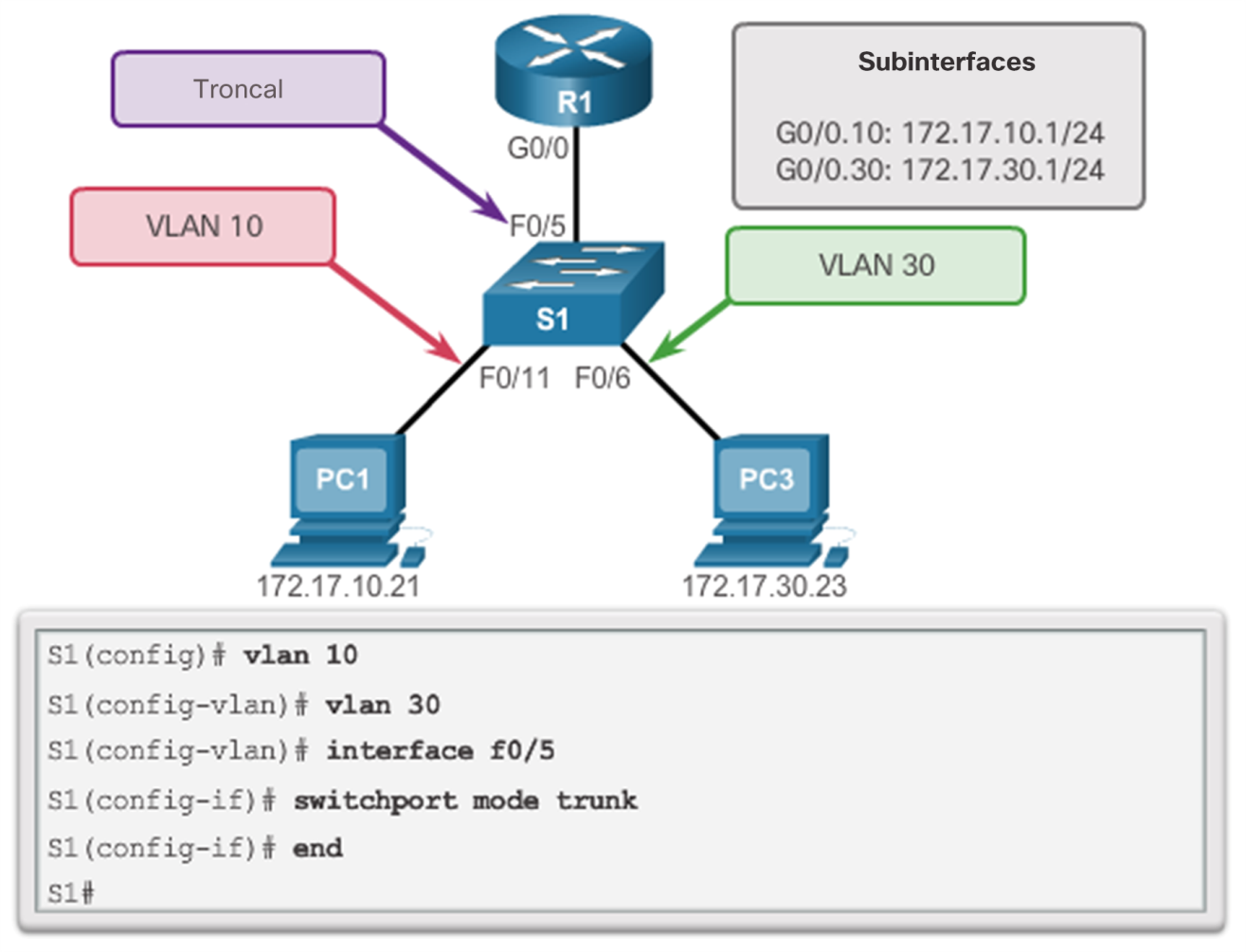
Para que se pueda dar la comunicación entre vlans distintas (vlan 10 y 30), el switch debe tener configuradas las vlan 10 y 30.

El router debe poder trabajar lógicamente con una interface con segmentos independientes y cada uno de ellos se llaman subinterfaces y es una segmentación lógica. Para que el tráfico pueda fluir el router toma decisiones.



Las subinterfaces se configuran como si fueran interfaces independientes.

* El concepto de **router-on-a-stick** utiliza **solo una** de las **interfaces físicas del router**.
* Una de las interfaces físicas del router (ejemplo: g0/0) se **configura como un puerto troncal 802.1Q** para que pueda comprender las etiquetas de las VLANs.
* Se crean **subinterfaces** **lógicas**, **una por cada VLAN**.
* Cada **subinterfaz** se **configura** con una **dirección IP proveniente de la VLAN** que representa.
* Los **miembros de las VLAN** (hosts) se configuran para utilizar la **dirección de subinterfaz** como **default gateway**.



!Subinterface for VLAN 10

int g0/0.**10 Identificar con un punto concatecado la subinterface que estoy definiendo**

decription HomeOffice

encapsulation dot1q **10**

ip address 172.17.10.1 255.255.255.0

!Subinterface for VLAN 30

int g0/0.**30 Subinterface .30**

decription Entretenimiento

encapsulation dot1q **30 establecer el tipo de encapsulamiento dot1q**

ip address 172.17.30.1 255.255.255.0

**Y así para todas las vlans**

int g0/0

no shut

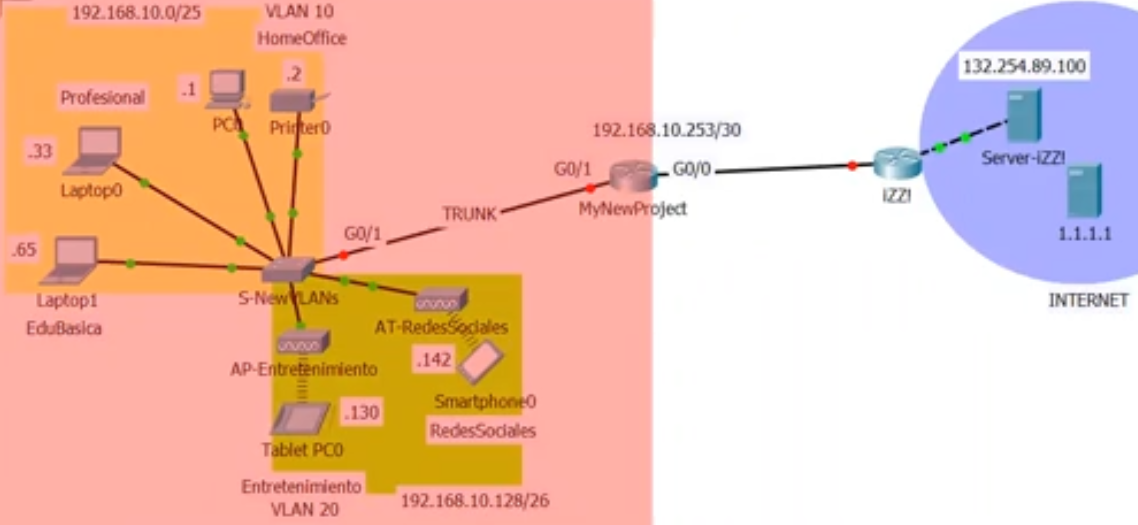
**Finalmente se levanta el puerto y se levantan todas las subinterfaces que son lógicas.**

**Ir ejercicio, después de las preguntas:**

Diagrama

Descripción generada automáticamente

Todo lo que está del lado derecho de MyNewProject ya está configurado. El proveedor de servicio IZZI y los servidores ya están configurados.



* En el **router MyNewProject**, hay que configurar la interface **g0/0** que conecta con el ISP.
* En el **switch** hay que configurar la interface **g0/1** como troncal.
* En el **router MyNewProyect** hay que configurar en la interface física **g0/1** **tantas subinterfaces como vlans tengamos.**

**En la vlan 10 (HomeOffice) podríamos tener máximo 128 - 2 direcciones IP.**

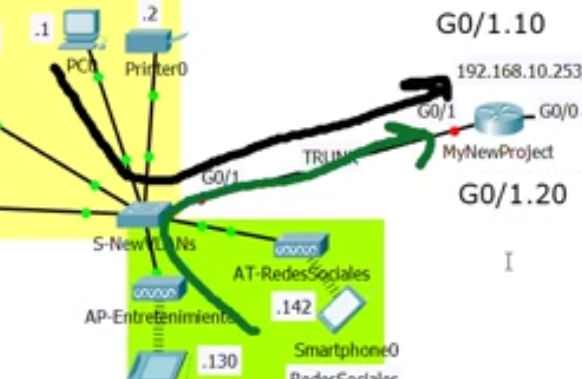
**En la vlan 20** **(Entretenimiento) podríamos tener máximo 64 - 2 direcciones IP.**

Analizamos la ip de la PC0, checamos su IP y su default gateway es la última ip válida de la subred.

El tráfico de color amarillo va a llegar a una de las subinterfaces.

El tráfico de color verde va a llegar a la subinterfaces correspondiente.

Las subinterfaces a programar son **g0/1.10** y **g0/1.20**, se sugiere poner como número de subinterface el número o id de la vlan.



1. En el switch hay que definir dos vlans en la base de datos: vlan 10 y vlan 20.
2. Una vez creada la base de datos, hay que asignar los puertos de acceso a estas vlans.

Los puertos del 1 al 15 son asociados a la vlan 10.

Los puertos del 16 al 24 son asociados a la vlan 20.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Segmento** | **VLAN** | **Puertos asignados** | **Dirección de subred** | **Máscara de subred** |
| **Home Office** | 10 | 1 – 15 | 192.168.10.0 | 255.255.255.128 |
| **Entretenimiento** | 20 | 16 – 24 | 192.168.10.128 | 255.255.255.192 |

1. Definir el puerto troncal como g0/1
2. En el router hay que crear la configuración de las subinterfaces.

Abrir archivos con comandos básicos de configuración de vlans.

* Configuración el router
* Configuración del switch
* Pruebas de conectividad

---------------------------------------------------------------

Configuración parcial del router MyNewRouter

---------------------------------------------------------------

ena

config t

hostname MyNewRouter

enable secret class

no ip domain-lookup

line con 0

password cisco

login

logging sync

line vty 0 4

password cisco

login

int g0/0

ip add 192.168.10.253 255.255.255.252

no shut

--- En esta sección debes incluir la configuración de las Subinterfaces ---

!COPIAR CONFIGURACIÓN DE COMANDOS

int g0/1.10

description VLAN Home Office

encapsulation dot1q 10

! dot1q protocolo aceptado para intercambio de vlans

ip add 192.168.10.126 255.255.255.128

! La última ip de la subred

! VLAN 10, todo su tráfico va a llegar por la subinterfaz g0/1.10

! VLAN 20, todo su tráfico va a llegar por la subinterfaz g0/1.20

! Debe corresponder el identificador de la subinterface con el de la vlan.

int g0/1.20

description VLAN Entretenimiento

encapsulation dot1q 20

ip add 192.168.10.190 255.255.255.192

int g0/1

no shut

!--------------------------------------------------------------------------------------------------

!PARA CONECTARNOS CON EL EXTERIOR ESTAMOS CONFIGURANDO UNA RUTA POR DEFAULT!DIRECTAMENTE CONECTADA.

ip route 0.0.0.0 0.0.0.0 g0/0

**COPIAR Y PEGAR CONFIGURACIÓN DEL ROUTER**

!HACER ACCESO WEB HACIA SERVIDOR izzi al exterior y no es exitoso, ya que el

!switch no está configurado.

**Laptop 1 hago acceso web hace servidor IZZI (132.254.89.100)**

-----------------------------------------------------

Configuración parcial del switch S-NewVLANs

-----------------------------------------------------

ena

config t

hostname S-NewVLANs

enable secret class

no ip domain-lookup

line con 0

password cisco

login

logging sync

line vty 0 15

password cisco

login

-- En esta sección agregar los comandos de configuración de VLANs --

-----------------------------------------------------------------------------------------------

!COPIAR COMANDOS DE CONFIGURACIÓN DEL SWITCH

! 1. Creación de las VLANs con nombre. Creación de la base de datos con la vlan 10 y 20.

! 2. Asignación de los puertos a la VLAN correspondiente.

! 3. Definir el puerto troncal

! Creacción de las VLANs con nombre HomeOffice

vlan 10

name HomeOffice

! nombre opcional

exit

!Asignar los puertos que le corresponden a la vlan 10

!A través de range f0/1-15 los primeros 15 puertos

interface range f0/1-15

switchport mode access

!Datos y no troncal

switchport access vlan 10

! vlan asociada a esos puertos que acabo de definir

! Creacción de las VLANs con nombre Entretenimiento

vlan 20

name Entretenimiento

exit

interface range f0/16-24

switchport mode access

switchport access vlan 20

!DEFINIR PUERTO TRONCAL G0/1

! Definición del o los puertos TRUNK

interface g0/1

switchport mode trunk

no shut

**COPIO CONFIGURACIÓN EN SWITCH.**

**En este momento ya me puedo comunicar con el exterior y de manera interna.**

**Laptop 1 hago acceso web hace servidor IZZI (132.254.89.100)**

**Tablet PC0 hago acceso web hace servidor IZZI (132.254.89.100)**

PC0 hacia el exlterior Server IZZI (Acceso web exitoso)

Estoy probando que por una interface física g0/1 están saliendo el tráfico de dos vlans o subredes distintas que están dividiendo el tráfico de forma lógica.

**Necesito verificar si de la vlan amarilla puedo pasar a la vlan verde.**

**Tablet PC0 hago ping 192.168.10.2 (impresora)**

Un solo puerto en el switch tiene que ser definido como troncal y el troncal lo que hace es transportar el tráfico de la vlan verde y el trafico de la vlan amarilla hacia las subinterfaces correspondientes. El troncal del switch puede llevar todos los tráficos posibles hacia otros switches o hacia el router. Para que el router pueda identificar de donde proviene que cosa en el router se deben configurar las subinterfaces.

