Unidad II

Redes VLAN

Una **VLAN** (acrónimo de *virtual LAN*, «**red de área local virtual**») es un método para crear redes lógicas independientes dentro de una misma red física.[1] Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

2.1. Tipos VLAN.

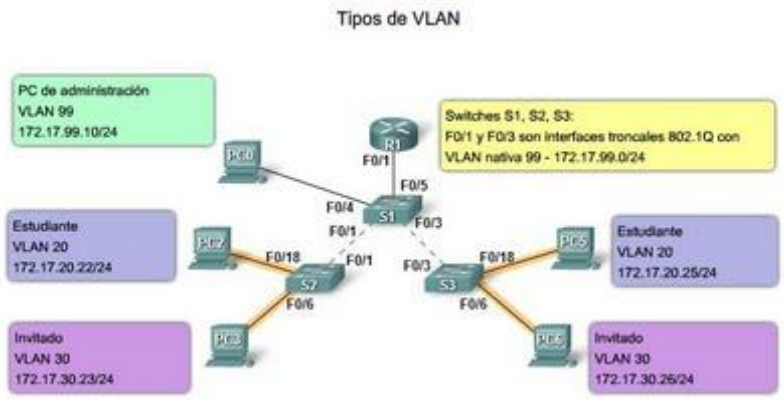
Hoy en día, existe fundamentalmente una manera de implementar las VLAN: VLAN basada en puerto. Una VLAN basada en puerto se asocia con un puerto denominado acceso VLAN.

Sin embargo, en las redes existe una cantidad de términos para las VLAN. Algunos términos definen el tipo de tráfico de red que envían y otros definen una función específica que desempeña una VLAN. A continuación, se describe la terminología común de VLAN:

VLAN de Datos

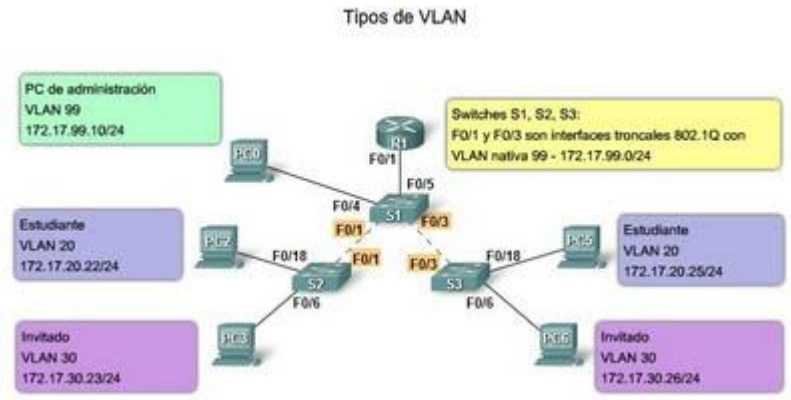
Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de 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.



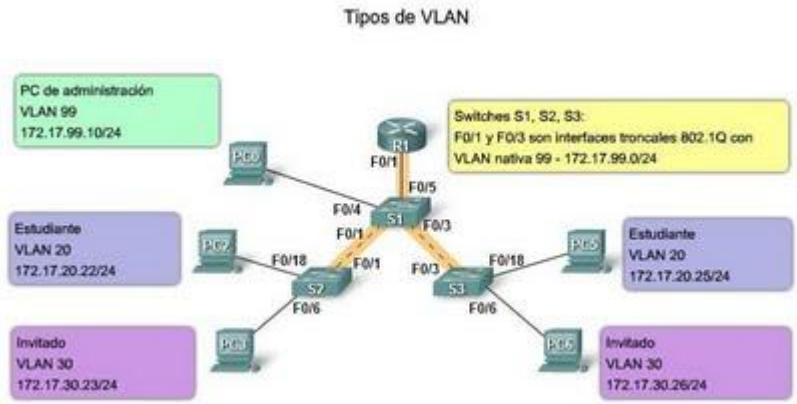
VLAN Predeterminada

Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego 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 de Cisco es 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. En la figura, el tráfico de la VLAN1 se envía sobre los enlaces troncales de la VLAN conectando los switches S1, S2 y S3. Es una optimización de seguridad para cambiar la VLAN predeterminada a una VLAN que no sea la VLAN 1; esto implica configurar todos los puertos en el switch para que se asocien con una VLAN predeterminada que no sea la VLAN 1. Los enlaces troncales de la VLAN admiten la transmisión de tráfico desde más de una VLAN.



VLAN Nativa

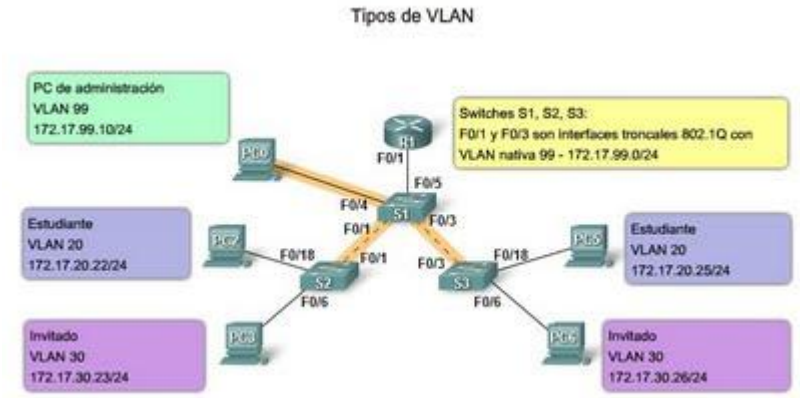
Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. En la figura, la VLAN nativa es la VLAN 99. El tráfico no etiquetado lo genera una computadora conectada a un puerto de switch que se configura con la VLAN nativa. Las VLAN se establecen en la especificación IEEE 802.1Q para mantener la compatibilidad retrospectiva con el tráfico no etiquetado común para los ejemplos de LAN antigua. Para nuestro fin, una VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal. Es una optimización usar una VLAN diferente de la VLAN 1 como 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. Debido a que la configuración lista para usar de un switch de Cisco tiene a VLAN 1 como la VLAN predeterminada, puede notar que la VLAN 1 sería una mala opción como VLAN de administración; no querría que un usuario arbitrario se conectara a un switch para que se configurara de manera predeterminada la VLAN de administración. Recuerde que configuró la VLAN de administración como VLAN 99 en el capítulo Configuración y conceptos básicos de switch.



VLAN de voz

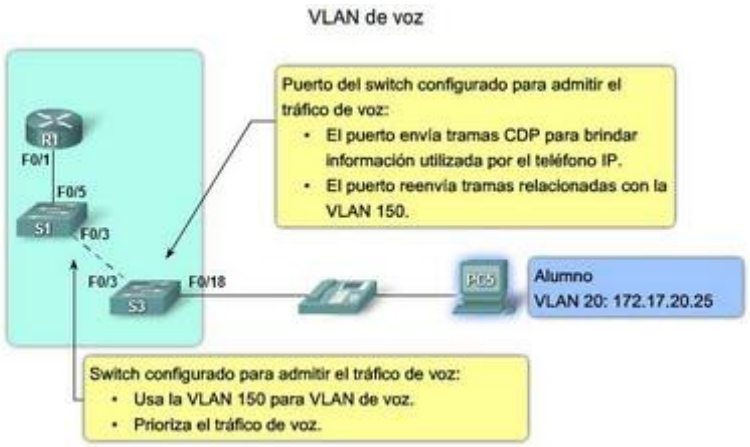
Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. El tráfico de VoIP requiere:

- 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

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP. Los detalles sobre cómo configurar una red para que admita VoIP están más allá del alcance del curso, pero es útil resumir cómo una VLAN de voz funciona entre un switch, un teléfono IP de Cisco y una computadora.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes. El puerto F0/18 en S3 se configura para que esté en modo de voz a fin de que diga al teléfono que etiquete las tramas de voz con VLAN 150.

Las tramas de datos que vienen a través del teléfono IP de Cisco desde la PC5 no se marcan. Los datos que se destinan a la PC5 que llegan del puerto F0/18 se etiquetan con la VLAN 20 en el camino al teléfono, que elimina la etiqueta de la VLAN antes de que los datos se envíen a la PC5. Etiquetar se refiere a la adición de bytes a un campo en la trama de datos que utiliza el switch para identificar a qué VLAN se debe enviar la trama de datos. Más adelante, aprenderá cómo se etiquetan las tramas de datos.

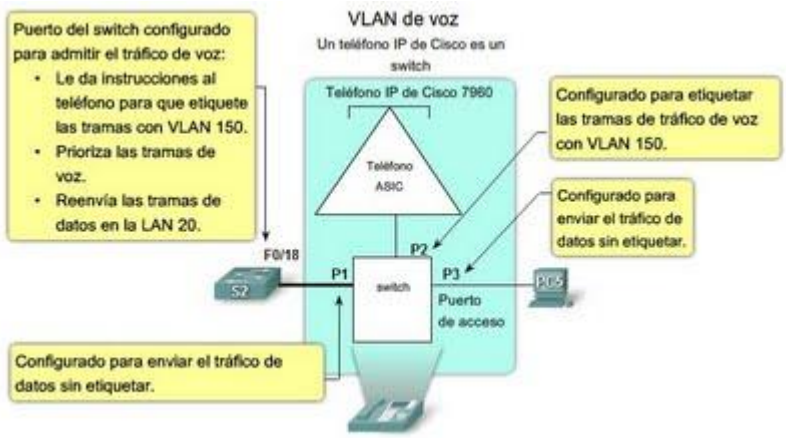


Un teléfono de Cisco es un switch

El teléfono IP de Cisco contiene un switch integrado de tres puertos 10/100, como se muestra en la figura. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

- El puerto 1 se conecta al switch o a otro dispositivo de voz sobre IP (VoIP).
- El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.
- El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

La figura muestra una manera de conectar un teléfono IP.



La función de la VLAN de voz permite que los puertos de switch envíen el tráfico de voz IP desde un teléfono IP. Cuando se conecta el switch a un teléfono IP, el switch envía mensajes que indican al teléfono IP conectado que envíe el tráfico de voz etiquetado con el ID 150 de VLAN de voz. El tráfico de la PC conectada al teléfono IP pasa por el teléfono IP sin etiquetar. Cuando se configuró el puerto del switch con una VLAN de voz, el enlace entre el switch y el teléfono IP funciona como un enlace troncal para enviar tanto el tráfico de voz etiquetado como el tráfico de datos no etiquetado.

2.2. Protocolos de enlace VLAN.

Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el IEEE 802.1Q, STP y VTP (cuyo equivalente IEEE es GVRP). El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN. El cometido principal de Spanning Tree Protocol (STP) es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos. VTP (VLAN Trunking Protocol) es un protocolo propietario de Cisco que permite una gestión centralizada de todas las VLANs.

El **protocolo de etiquetado IEEE 802.1Q** es el más común para el etiquetado de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com. El IEEE 802.1Q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde sólo cambia el valor del campo Ethertype, que en las tramas 802.1Q vale X'8100, y se añaden dos bytes para codificar la prioridad, el CFI y el VLAN ID. Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con bridges y switches sin capacidad de VLAN.

Para evitar el bloqueo de los switches debido a las tormentas broadcast, una red con topología redundante tiene que tener habilitado el **protocolo STP**. Los switches utilizan STP para intercambiar mensajes entre sí (BPDUs, Bridge Protocol Data Units) para lograr de que en cada VLAN sólo haya activo un camino para ir de un nodo a otro.

En los dispositivos Cisco, **VTP (VLAN trunking protocol)** se encarga de mantener la coherencia de la configuración VLAN por toda la red. VTP utiliza tramas de nivel 2 para gestionar la creación, borrado y renombrado de VLANs en una red sincronizando todos los dispositivos entre sí y evitar tener que configurarlos uno a uno. Para eso hay que establecer primero un **dominio de administración VTP**. Un dominio VTP para una red es un conjunto contiguo de switches unidos con enlaces trunk que tienen el mismo nombre de dominio VTP.

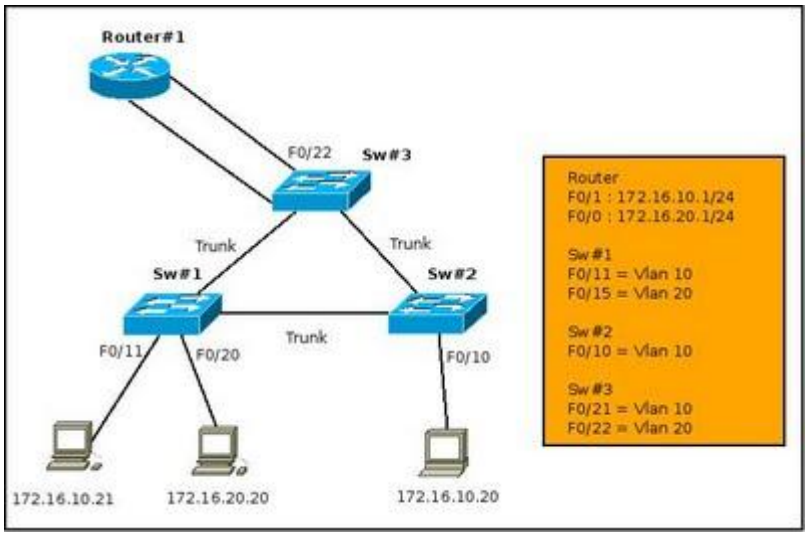
Los switches pueden estar en uno de los siguientes modos: servidor, cliente o transparente. El **servidor** es el modo por defecto, anuncia su configuración al resto de equipos y se sincroniza con otros servidores VTP. Un switch **cliente** no puede modificar la configuración VLAN, simplemente sincroniza la configuración en base a la información que le envían los servidores. Por último, un switch está en modo **transparente** cuando sólo se puede configurar localmente pues ignora el contenido de los mensajes VTP.

VTP también permite «podar» (función VTP prunning), lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino. Con lo que se ahorra ancho de banda en los posiblemente saturados enlaces trunk.

2.3. Enrutamiento inter VLAN.

El **enrutamiento entre vlans** o **inter vlan routing**, resulta necesario una vez que se posee una infraestructura de red con vlan implementadas, debido a que los usuarios necesitaran intercambiar información de una red a otra.

Es importante recordar que cada VLAN es un dominio de broadcast único. Por lo tanto, de manera predeterminada, las computadoras en VLAN separadas no pueden comunicarse.

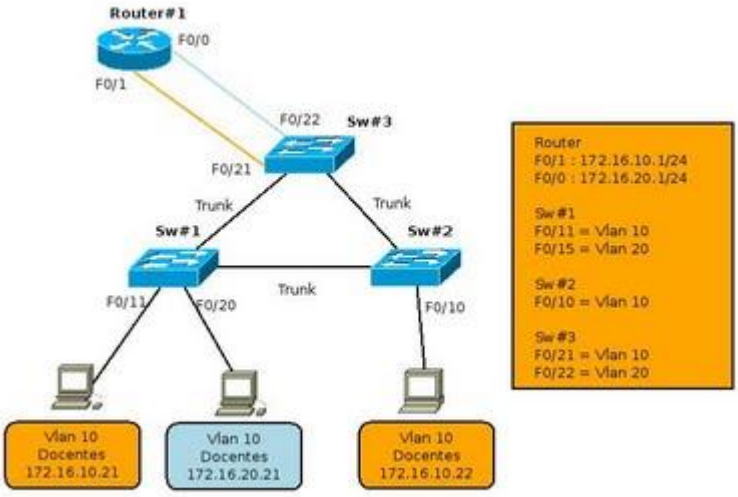


Existe una manera para permitir que estas estaciones finales puedan comunicarse; esta manera se llama **enrutamiento entre vlan (Inter vlan routing)**.

El **enrutamiento entre VLAN** es un proceso que permite reenviar el tráfico de la red desde una VLAN a otra mediante un enrutador. Las VLAN están asociadas a subredes IP únicas en la red. Esta configuración de subred facilita el proceso de enrutamiento en un entorno de múltiples VLAN.

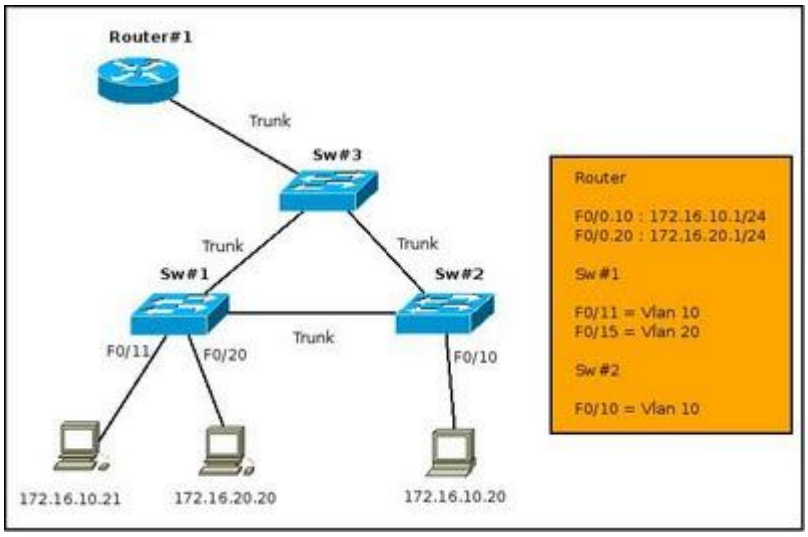
Tradicionalmente, el enrutamiento de la LAN utiliza enrutadores con interfaces físicas múltiples. Es necesario conectar cada interfaz a una red separada y configurarla para una subred diferente.

En una red tradicional que utiliza múltiples VLAN para segmentar el tráfico de la red en dominios de broadcast lógicos, el enrutamiento se realiza mediante la conexión de diferentes interfaces físicas del enrutador a diferentes puertos físicos del switch. Los puertos del switch conectan al enrutador en modo de acceso; en este modo, diferentes VLAN estáticas se asignan a cada interfaz del puerto. Cada interfaz del switch estaría asignada a una VLAN estática diferente. Cada interfaz del enrutador 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 entre VLAN** tradicional requiere de interfaces físicas múltiples en el enrutador y en el switch. Sin embargo, no todas las configuraciones del enrutamiento entre VLAN requieren de interfaces físicas múltiples.

Algunos software del enrutador permiten configurar interfaces del enrutador como enlaces troncales. Esto abre nuevas posibilidades para el enrutamiento entre VLAN. "enrutador-on-a-stick" es un tipo de configuración de enrutador en la cual una interfaz física única enruta el tráfico entre múltiples VLAN en una red.



Enrutamiento entre Vlan, subinterfaces (**Router on a Stick**)

La interfaz del enrutador se configura para funcionar como enlace troncal y está conectada a un puerto del switch configurado en modo de enlace troncal. El enrutador realiza el **enrutamiento entre 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 subinterfaces. El enrutador 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 enrutador 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. Aprenderá más acerca de las interfaces y las subinterfaces en el siguiente tema.

Algunos switches pueden realizar funciones de Capa 3, lo que remplaza la necesidad de utilizar enrutadors dedicados para realizar el enrutamiento básico en una red. Los switches multicapas pueden realizar el enrutamiento entre VLAN.

Para habilitar un switch multicapa para realizar funciones de enrutamiento, es necesario configurar las interfaces VLAN en el switch con las direcciones IP correspondientes que coincidan con la subred a la cual la VLAN está asociada en la red. El switch multicapa también debe tener el IP routing habilitado.

2.4. Resolución de problemas de VLAN.

Cuando configura la VLAN y los enlaces troncales en una infraestructura conmutada, estos tipos de errores de configuración son los más comunes, en el siguiente orden:

Faltas de concordancia de la VLAN nativa: los puertos se configuran con diferentes VLAN nativas, por ejemplo si un puerto ha definido la VLAN 99 como VLAN nativa y el otro puerto de enlace troncal ha definido la VLAN 100 como VLAN nativa. Estos errores de configuración generan notificaciones de consola, hacen que el tráfico de administración y control se dirija erróneamente y, como ya ha aprendido, representan un riesgo para la seguridad.

Faltas de concordancia del modo de enlace troncal: un puerto de enlace troncal se configura con el modo de enlace troncal "inactivo" y el otro con el modo de enlace troncal "activo". Estos errores de configuración hacen que el vínculo de enlace troncal deje de funcionar.

VLAN admitidas en enlaces troncales: la lista de VLAN admitidas en un enlace troncal no se ha actualizado con los requerimientos de enlace troncal actuales de VLAN. En este caso, se envía tráfico inesperado o ningún tráfico al enlace troncal.

Problema	Resultado	Ejemplo
Falta de concordancia en la VLAN nativa	Presenta un riesgo a la seguridad y crea resultados no deseados.	Por ejemplo, un puerto la ha definido como VLAN 99, el otro como VLAN 100.
Falta de concordancia en el modo de enlace troncal	Causa pérdida de la conectividad de la red.	Por ejemplo, en un puerto está configurado como "off" y en otro como modo de enlace troncal "on".
VLAN y Subredes IP	Causa pérdida de la conectividad de la red.	Por ejemplo, las computadoras de los usuarios pueden haber sido configuradas con las direcciones IP incorrectas.
VLAN permitidas en enlaces troncales	Provoca tráfico no deseado o no se envía el tráfico a través del enlace troncal.	La lista de las VLAN permitidas no admite los requisitos de enlace troncal de VLAN actuales.

2.5. Seguridad en VLAN.

Todo buen administrador de redes sabe que seguramente el próximo ataque a sus sistemas provenga de su red. Por malicia o desconocimiento, los usuarios que se encuentran del lado interno tienen mucho más poder destructivo que los externos y eso es así gracias a los administradores confiados.

Hoy en día la gran mayoría de administradores ya tiene esto en cuenta y los usuarios internos están más controlados, aunque sea a nivel de aplicación. Como este blog nace con la idea de ayudar a los que menos experiencia tienen, vamos a explicar un poco por encima lo que podemos hacer para no dejar andar a nuestros usuarios a su antojo por toda nuestra red.