CORPORACIÓN UNIVERSITARIA LATINOAMERICANA
CUL

PROGRAMA DE INGENIERIA DE SISTEMAS
X SEMESTRE

DIPLOMADO SEGURIDAD EN REDES INFORMATICAS

TEMA:

DISEÑO DE UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP) EN AREAS RURALES

PRESENTADO POR:

CHRISTIAN HERAZO
LEONARDO TORRES
JORGE HERRERA
GENESIS TAFUR

DIRIGIDO A

ING. LUIS FRAN CARDOZO

BARRANQUILLA, ATLANTICO.

11 DE OCTUBRE DEL 2018

Tabla de contenido

RESUMEN:

Las personas que viven en áreas rurales en Colombia, tienen una problemática social que no les permite progresar en el ámbito informático y esa problemática está dada por la nula o poca facilidad para conectarse en internet.

En este documento trataremos de diseñar el concepto lógico de un proveedor de internet para áreas rurales y así mitigar una problemática social.

Gracias a las conexiones satelitales lograremos solucionar esa problemática, llevando hasta los hogares directamente por medio de cables y así facilitarles el acceso a internet.

Aplicando las reglas de cableado estructurado en esas redes, podremos brindar un servicio eficiente a esas personas que necesitan la conexión.

Usando los postes de alumbrado público para seguir una guía que facilite la instalación de esos cables.

INTRODUCCION:

Hoy en día en uso del internet es algo que se ha convertido en algo común, como comer, ducharse, entre otras actividades que podríamos nombrar. El internet es una necesidad para muchos ya que gracias a este, muchos pueden desempeñar diversas actividades laborales o personales, es decir el internet es una necesidad hoy en día. Por esta razón diversas compañías han creado medios para distribuir este.

A pesar de que el internet es algo común, algo que se utiliza diariamente, en algunas locaciones, como los municipios del atlántico, este no funciona de manera ideal. En algunos municipios el internet no llega hasta los hogares como se puede observar en las ciudades, ellos recurren a tener planes de datos móviles, los cuales no son tan económicos y además de eso siguen sin ser un excelente servicio, por esta razón hemos decidido implementar la creación de una red ISP y colocar cada uno de los procedimientos a realizar, desde la conexión con el proveedor satelital, hasta la forma de suministrarle el internet a los clientes, ya sea cableada o por medio de señales abiertas basadas en el protocolo de wifi de largo alcance, pasando por la infraestructura interna que se encarga de administrar la información y los datos (internet) para cada cliente.

1. PLANTEAMIENTO DEL PROBLEMA:

1.1. DESCRIPCIÓN DE PROBLEMA:

En muchos municipios del atlántico se vive una problemática social, y esa es el hecho de que no en todos esos municipios hay acceso a internet de calidad y en muchos casos, ni siquiera hay ningún tipo de servicio de internet; las operadoras que se encuentran a nivel nacional, no ven rentables estos municipios por la cantidad de clientes que hay en esos territorios, entonces para sus ingresos, no justificaría invertir grandes cantidades de dinero en infraestructura, para pocos clientes, pero con un proyecto pequeño y llevando internet satelital a esos sitios para distribuirlos por medio de ondas electromagnéticas a las casas cercanas y vendiéndoles el servicio a un costo que puedan pagar esas personas, se puede solventar esa problemática.

La mayoría de personas en áreas rurales que necesitan internet en momentos puntuales, tienen que comprar paquetes de internet limitados a las operadoras móviles, lo cual impide que puedan enviar cantidades de información y datos a precios asequibles, lo cual limita el progreso de ese sitio.

1.2. FORMULACION DEL PROBLEMA:

En muchos municipios en el área rural del atlántico no hay proveedores de internet que ofrezcan un servicio para el hogar, lo cual lleva a que muchas personas usen el servicio de internet móvil, el cual es demasiado costoso por ser limitado a la cantidad de megabits que compres al día, semana, o mes.

¿De qué manera poder llevar un servicio de internet a las personas que viven en áreas rurales de forma segura?

¿Cómo sería la forma de hacerles llegar el internet hasta sus hogares?

¿En que beneficiaría a las personas locales un proyecto así?

2. OBJETIVOS:

2.1. OBJETIVO GENERAL:

Diseñar, desarrollar e implementar un proveedor de servicios de internet (ISP) para zonas rurales que no tienen acceso a internet o los precios son muy costosos y limitados para la mayoría de sus habitantes.

2.2. OBJETIVOS ESPECIFICOS:

- Identificar la problemática de las personas que viven en áreas rurales con respecto al servicio de internet brindado por otros proveedores.

- Diseñar la estructura física del ISP y colocar cada uno de los procedimientos a realizar, desde la conexión con el proveedor satelital, hasta la forma de suministrarle el internet a los clientes, ya sea cableada o por medio de señales abiertas basadas en el protocolo de wifi de largo alcance, pasando por la infraestructura interna que se encarga de administrar la información y los datos (internet) para cada cliente.

- Desarrollar la red lógica de todas las conexiones que saldrán desde el ISP hasta cada cliente, aplicando las reglas de cableado estructurado en toda la red, documentando cada una de dichas conexiones.

3. JUSTIFICACION

En nuestro país se vive una problemática en general, la cual perjudica de una manera significativa a personas de áreas rurales, y esa es el hecho de no tener internet en sus casas las 24 horas del día a precios económicos y un servicio ilimitado de acceso a la web.

Durante muchos años, en el país, las empresas grandes proveedoras de servicios de internet han tenido estas áreas rurales como no viables, ya que no deseen invertir en infraestructura para la poca cantidad de clientes.

Con la llegada de la tecnología de internet dedicado por medio de satélites, muchas empresas internacionales han visto un hueco en el mercado para llegar a esa población,

pero todavía poseen precios altos, para la mayoría de personas que habitan estas zonas rurales, pero a medida que se solicita mayor ancho de banda de internet, menor será el precio a pagar por cada megabits por segundos que provee esas empresas, el punto está en solicitar un servicio satelital con gran cantidad de megabits, en torno de los 200 a 300 para que el costo para revenderlo sea accesible para esa población que vive en áreas rurales.

Se sabe de antemano que el internet está catalogado en todos los países como una necesidad, no solo un lujo, porque facilita la vida de las personas, por ejemplo un estudiante para investigar, un trabajador, para enviar información a la empresa, entre otros ejemplos más; nuestra idea de una ISP quiere llegar a todas esas áreas rurales para garantizarles internet a esas personas que no pueden porque no hay proveedores o los que hay, son muy costosos.

También es sabido que para que una empresa grande proveedora de internet, invierta en infraestructura, tiene que ser a poblaciones grandes que justifique esa inversión a corto/largo plazo, lo cual no cumple el área rural, pero una pequeña empresa si podría asumir esos costos de infraestructura al estar limitada al principio a una pequeña área.

4. ESTADO DEL ARTE:

Empresas constituidas en la ciudad de barranquilla como una ISP y de allí fueron ofreciendo más servicios hasta ser lo que son ahora, entre esas tenemos a ITELKOM

4.1. ITELKOM

4.1.1. Historia:

En enero de 2011 Con una pequeña red inalámbrica metropolitana en la ciudad de Barranquilla nace iTelkom como una empresa Telco local que prestaba únicamente servicios de internet y datos al segmento pyme y hogar.

Conexión a cable submarino

En febrero de 2013 nos conectamos por primera vez y directamente a un cable submarino. Se firma nuestro primer contrato de acceso internacional y se cierra en Estados Unidos paralelamente un acuerdo con la empresa Tier 1 Cogent.

Proyecto Nube

En octubre de 2014 iTelkom gana la CONVOCATORIA NACIONAL PARA EL APOYO A LA INNOVACIÓN EMPRESARIAL (INNpulsa-Mi Pyme) con el proyecto presentado de nuestra plataforma de nube (LOW COST/Alta Disponibilidad), lo que nos permitió hacer realidad los servicios de nube eficiente, de alta disponibilidad y a menor precio que actualmente iTelkom ofrece.

Compra Redes Integrales

En febrero de 2016 iTelkom compra la operación, facturación e infraestructura de la empresa Redes Integrales S.A. de la ciudad de Cartagena, consolidamos la operación en la Heroica, establecemos oficina comercial y seguimos avanzando en nuestros sueños.

Area I+D

En agosto de 2016 nace el área I+D iTelkom, se asigna presupuesto y se nombra un Director de I+D; se crea internamente una fábrica de software que busca desarrollar soluciones que impacten la productividad de nuestros clientes en el uso de nuestros productos.

4.1.2. Como Trabajamos

En iTelkom soñamos con redefinir la gestión y la integración de tecnologías digitales que aporten a nuestros socios de negocios agilidad operacional y una experiencia de uso simple en su gestión TI, creemos en la incorporación de valor a través de la innovación, el uso del software abierto, el análisis de datos, la movilidad WiFi y el matrimonio de software y dispositivos, sirviéndolo todo como servicio a nuestros clientes. Nuestro reto es ayudar a las empresas a alcanzar una significativa y sustancial mejora en su eficiencia a través del uso de nuestra infraestructura digital de telecomunicaciones, plataforma de nube, desarrollo de aplicaciones, sistema de información y la ciberseguridad sincronizada.

4.1.3. SERVICIOS OFRECIDOS

INTERNET

Internet dedicado en fibra Optica

Internet Inalambrico(Flex - Lite)

Internet para Eventos

CIBERSEGURIDAD

En Dispositivos (Antivirus)

En la Red (NGFW Firewall)

Arquitectura de Seguridad Sincroniza

CLOUD & PRODUCTIVIDAD
VPS Cloud

Microsoft

REDES EMPRESARIALES
Redes Wifi

4.2. Dialnet de Colombia S.A. E.S.P.

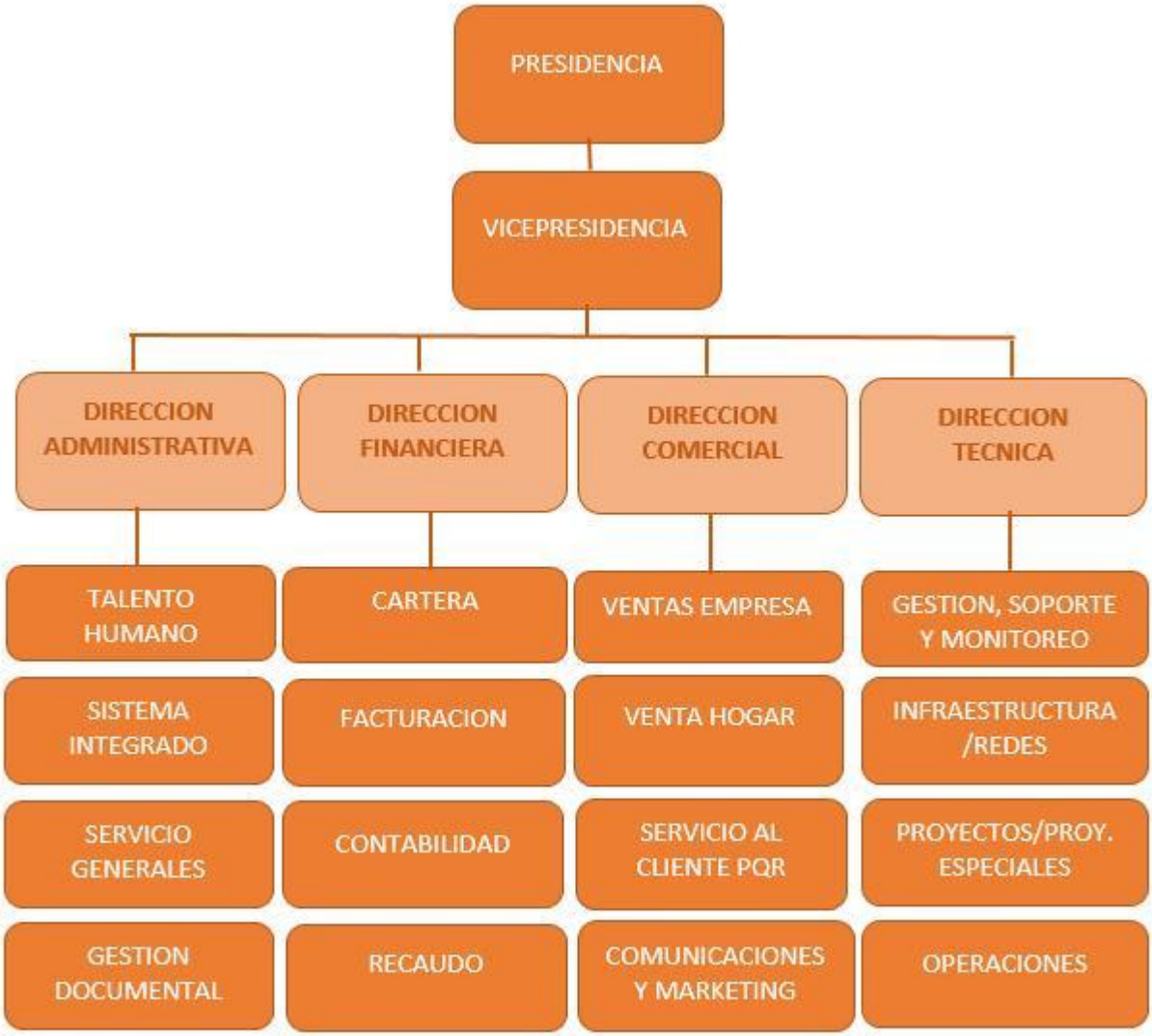
4.2.1. QUIENES SOMOS

Somos una empresa líder en la prestación de servicios relacionados con el sector de las telecomunicaciones, con una amplia experiencia y caracterizados siempre por nuestra calidad y excelente servicio.

Manteniendo nuestra alta inversión en infraestructura y personal, **Dialnet de Colombia S.A. E.S.P.** ayuda a obtener una conexión confiable y escalable para nuestros clientes y le brinda a las empresas una ventana al borde de la competitividad.

Dialnet de Colombia S.A. E.S.P. es el Proveedor de Servicios de Internet con proyección hacia el mercado corporativo que le proporciona la oportunidad de reducir sus costos de hacer negocios con el uso de la Internet sin sacrificar la calidad del servicio. A través de nuestro personal proporciona el conocimiento y la experiencia profesional para ayudarle a optimizar sus estrategias de negocios de Internet y encontrar nuevas posibilidades.

4.2.2. Organigrama



4.2.3. Misión, Visión y Política de Calidad

Misión

Somos un equipo líder, motivados en ofrecer soluciones integrales emergentes e innovadoras, comprometidos con la necesidad de conectar equipos, personas y empresas con el mundo tecnológico a través de las telecomunicaciones.

Visión

Ser la mejor alternativa tecnológica en ofrecer soluciones integrales e innovadoras en el sector de las telecomunicaciones, caracterizados por nuestras actuaciones responsables con

nuestro entorno social-ambiental, bajo altos estándares de calidad, cobertura y confiabilidad.

4.2.4. Política de Calidad

Dialnet de Colombia S.A. E.S.P. en concordancia con nuestra misión y con fundamento en el direccionamiento estratégico, ofrece servicios con calidad, mediante criterios de eficiencia y mejoramiento continuo en todos sus procesos, empleando los recursos de manera eficaz a través de funcionarios competentes y comprometidos con el fortalecimiento de la gestión institucional, lo cual resultara, en la proyección de **Dialnet de Colombia S.A. E.S.P.** como una empresa líder en el sector de las telecomunicaciones. Nuestro sistema se soporta en un recurso humano competente, calificado y responsable al igual que una infraestructura adecuada y canales de comunicación efectivos que permiten detectar oportunidades de mejora.

Nuestras Fortalezas

4.2.5. Velocidad

Dialnet de Colombia S.A. E.S.P. ofrece rangos de velocidad que se ajustan a los requerimientos de las compañías. Es por esto que cuenta con servicios de gran capacidad diseñados para brindar soluciones empresariales a sus clientes.

Confiabilidad

Las soluciones de infraestructura de **Dialnet de Colombia S.A. E.S.P.** permiten disponer de la máxima**escalabilidad**, **seguridad**, **confiabilidad** y **disponibilidad** de infraestructura tecnológica. **Dialnet de Colombia S.A. E.S.P.** hace uso de su Backbone de fibra óptica para conexión a internet o transmisión de datos, con solución de último kilómetro con fibra o radio enlace.

4.2.6. Servicio

Servicio altamente confiable, garantizando un 99.6% de disponibilidad. El Equipo de Soporte Técnico de**Dialnet de Colombia S.A. E.S.P.** brinda apoyo a través de su Call Center en los niveles de Asistencia Remota y Asistencia Personalizada, vía e-mail ó en nuestro Sitio Web.

Monitoreo

Dialnet de Colombia S.A. E.S.P. Brinda la posibilidad de obtener reportes que permiten obtener información acerca del consumo del ancho de banda diario, mensual y anual; de esta forma se hace posible la verificación del estado de los servicios adquiridos.

Fibra Óptica

Las soluciones de infraestructura de **Dialnet de Colombia S.A. E.S.P.** le permiten disponer de la máxima **escalabilidad**, **seguridad**, **confiabilidad** y **disponibilidad** de infraestructura tecnológica.

Dialnet de Colombia S.A. E.S.P. hace uso de su BackBone de Fibra Óptica que le conecta a internet y transporta tus datos, con solución de último kilómetro de Fibra o radio de Enlace.

Todos nuestros nodos están interconectados con fibra óptica y cuenta con un enlace de respaldo por si esta llega a fallar, y la salida internacional desde dialnet corre sobre fibra óptica hasta nuestro carrier internacional. Nuestro servicio es altamente confiable, **garantizando un 99.6% de disponibilidad.**

4.2.7. Indicadores de línea gratuita

Dando cumplimiento a las regulaciones y obligaciones legales emitidas por el ministerio de tecnologías de la información y las comunicaciones, exponemos los indicadores que miden las condiciones de calidad de prestación del servicio en relación a la atención al usuario para la línea gratuita.

Indicadores Línea Gratuita

4.2.8. Soporte

Ofrecemos una solución confiable y las posibilidades de fallas en el sistema son altamente bajas. Aun así el Equipo de Soporte Técnico de Dialnet de Colombia le brindara asistencia técnica tanto remota como personalizada, respondiendo a sus inquietudes a través de notificaciones vía e-mail o telefónica por medio de nuestro Centro de gestión.

Le brindaremos la posibilidad de obtener reportes(*) acerca del consumo del ancho de banda tanto diario como mensual y anual, permitiéndole así al usuario corroborar que Dialnet de Colombia le está garantizando la prestación del servicio y establecer si necesita ampliar su ancho de banda.

4.2.9. Herramientas Utilizadas.

Monitoreo
Se puede observar las gráficas del consumo y disponibilidad de su conexión (Canales Dedicados) representados en Kbps, mediante un usuario y contraseña proporcionado por nosotros.

Tickets

Mediante este sistema se hará un seguimiento de los inconvenientes que presente usted con el servicio.

4.2.10. VALORES CORPORATIVOS

INNOVACIÓN: Somos una empresa con personal altamente creativo, que imparte un sello particular a todo lo que ofrece.
COMPROMISO: Con un equipo dinámico y responsable entregamos nuestro mayor esfuerzo para la consecución de las metas.
CONFIABILIDAD: Somos un equipo confiable, en el ejercicio de nuestras labores actuamos siempre con rectitud.
CALIDEZ: Nuestra vocación es brindar a nuestros socios de negocio, una atención oportuna y digna de respeto.
OPTIMISMO: Le inyectamos entusiasmo a todo lo que emprendemos.

PRINCIPIOS CORPORATIVOS

ESTAMOS ORIENTADOS AL CLIENTE: preocupados por atender de la mejor manera a nuestros clientes logrando solucionar sus requerimientos en el menor tiempo.
OFRECEMOS CALIDAD EN EL SERVICIO: Ofrecemos servicios Optimo considerando el mejoramiento continuo de cada proceso.
NOS MANTENEMOS A LA VANGUARDIA DE LA TECNOLOGÍA: Nos esforzamos por actualizar nuestras plataformas, equipos y servicios.

4.3. VISIÓN GENERAL DE VLAN

La solución para la comunidad de la universidad es utilizar una tecnología de red denominada LAN (VLAN) virtual. 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. Como otro ejemplo, todas las computadoras de los estudiantes se pueden configurar en la VLAN "Estudiante". Mediante las VLAN, puede segmentar de manera lógica las redes conmutadas basadas en equipos de proyectos, funciones o departamentos. También puede utilizar una VLAN para estructurar geográficamente su red para respaldar la confianza en aumento de las empresas sobre trabajadores domésticos. En la figura, se crea una VLAN para los estudiantes y otra para el cuerpo docente. Estas VLAN permiten que el administrador de la red implemente las políticas de acceso y seguridad para grupos particulares de usuarios. Por ejemplo: se puede permitir que el cuerpo docente, pero no los estudiantes, obtenga acceso a los servidores de administración de e-learning para desarrollar materiales de cursos en línea.

4.3.1. Detalles de la 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. La figura muestra una red con tres computadoras. Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. En el switch deben darse de alta las VLANs y cada puerto asignarse a la VLAN correspondiente. Un puerto de switch con una VLAN singular configurada en el mismo se denomina puerto de acceso. Recuerde que si dos computadoras están conectadas físicamente en el mismo switch no significa que se puedan comunicar. Los dispositivos en dos redes y subredes separadas se deben comunicar a través de un router (Capa 3), se utilicen o no las VLAN. No necesita las VLAN para tener redes y subredes múltiples en una red conmutada, pero existen ventajas reales para utilizar las VLAN.

4.3.2. 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.

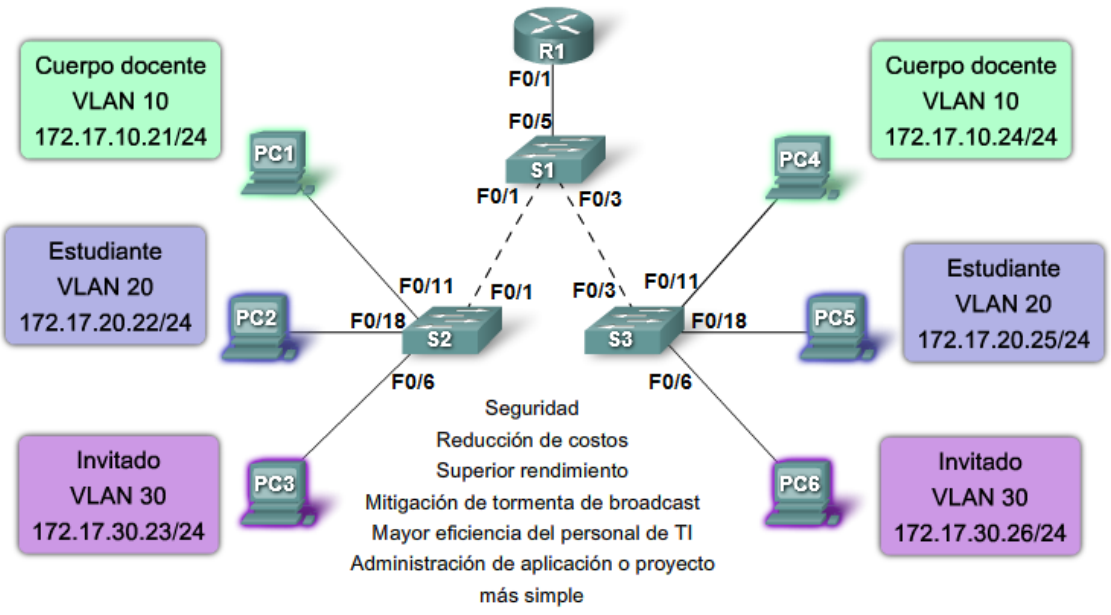
Reducción de costo: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

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. Como se analizó en el capítulo "Configure un switch", 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 e 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.



4.3.3. Rangos de las VLAN

Rangos del ID de la VLAN
El acceso a las VLAN está dividido en un rango normal o un rango extendido.

VLAN de rango normal

Se utiliza en redes de pequeños y medianos negocios y empresas.

Se identifica mediante un ID de VLAN entre 1 y 1005.

Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.

Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar. Aprenderá más acerca de VLAN 1 más adelante en este capítulo.

Las configuraciones se almacenan dentro de un archivo de datos de la VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.

El protocolo de enlace troncal de la VLAN (VTP), que ayuda a gestionar las configuraciones de la VLAN entre los switches, sólo puede asimilar las VLAN de rango normal y las almacena en el archivo de base de datos de la VLAN.

VLAN de rango extendido

Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.

Se identifican mediante un ID de VLAN entre 1006 y 4094.

Admiten menos características de VLAN que las VLAN de rango normal.

Se guardan en el archivo de configuración en ejecución.

VTP no aprende las VLAN de rango extendido.

255 VLAN configurables

Un switch de Cisco Catalyst 2960 puede admitir hasta 255 VLAN de rango normal y extendido, a pesar de que el número configurado afecta el rendimiento del hardware del switch. Debido a que la red de una empresa puede necesitar un switch con muchos puertos, Cisco ha desarrollado switches a nivel de empresa que se pueden unir o apilar juntos para crear una sola unidad de conmutación que consiste en nueve switches separados. Cada switch por separado puede tener 48 puertos, lo que suma 432 puertos en una sola unidad de conmutación. En este caso, el límite de 255 VLAN por un solo switch podría ser una restricción para algunos clientes de empresas.

Características de VLAN

- ID de VLAN
  - ID de campo normal
    - 1 – 1005
    - 1002 -1005 se reservan para Token Ring y las VLAN FDDI
    - 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar
    - Se guarda en el archivo vlan.dat en la memoria flash
  - ID de campo ampliado
    - 1006 – 4094
    - Se diseñan para los proveedores de servicios
    - Poseen menos opciones que las VLAN de campo normal
    - Se guardan en el archivo de configuración en ejecución
- Un switch Cisco Catalyst 2960 admite 255 VLAN de campo normal y ampliado

4.3.4. Tipos de VLAN

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.

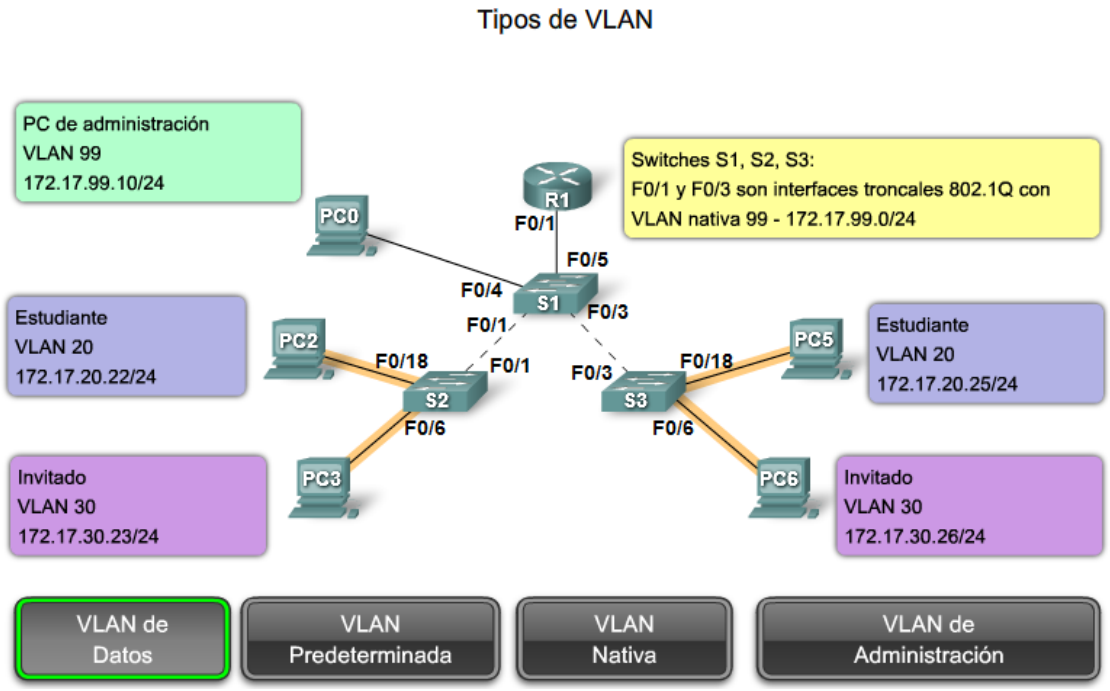
El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

La 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.

Nota: La comunicación entre el switch y el teléfono IP la facilita el protocolo CDP. Este protocolo se analizará en detalle en CCNA Exploration: Curso sobre Conceptos y protocolos de enrutamiento.

Ejemplo de configuración

La figura muestra el resultado del ejemplo. Un análisis de los comandos IOS de Cisco está más allá del alcance de este curso pero puede observar que las áreas destacadas en el resultado del ejemplo muestran la interfaz F0/18 configurada con una VLAN configurada para datos (VLAN 20) y una VLAN configurada para voz (VLAN 150).



4.3.5. Tipos de tráfico de red

En CCNA Exploration: En Aspectos básicos de redes, aprendió sobre los diferentes tipos de tráfico que puede manejar una LAN. Debido a que una VLAN tiene todas las características de una LAN, una VLAN debe incorporar el mismo tráfico de red que una LAN.

Administración de red y tráfico de control

Muchos tipos diferentes de tráfico de administración de red y de control pueden estar presentes en la red, como las actualizaciones de Cisco Discovery Protocol (CDP), Simple Network Management Protocol (SNMP) y tráfico de Remote Monitoring (RMON).

Telefonía IP

Los tipos de tráfico de telefonía IP son el tráfico de señalización y el tráfico de voz. El tráfico de señalización es responsable de la configuración de la llamada, el progreso y la desconexión y atraviesa la red de extremo a extremo. El otro tipo de tráfico de telefonía consiste en paquetes de datos de la conversación de voz existente. Como acaba de ver, en una red configurada con VLAN, se recomienda con énfasis asignar una VLAN diferente a la VLAN 1 como VLAN de administración. El tráfico de datos debe asociarse con una VLAN de datos (diferente a la VLAN 1) y el tráfico de voz se asocia con una VLAN de voz.

IP Multicast

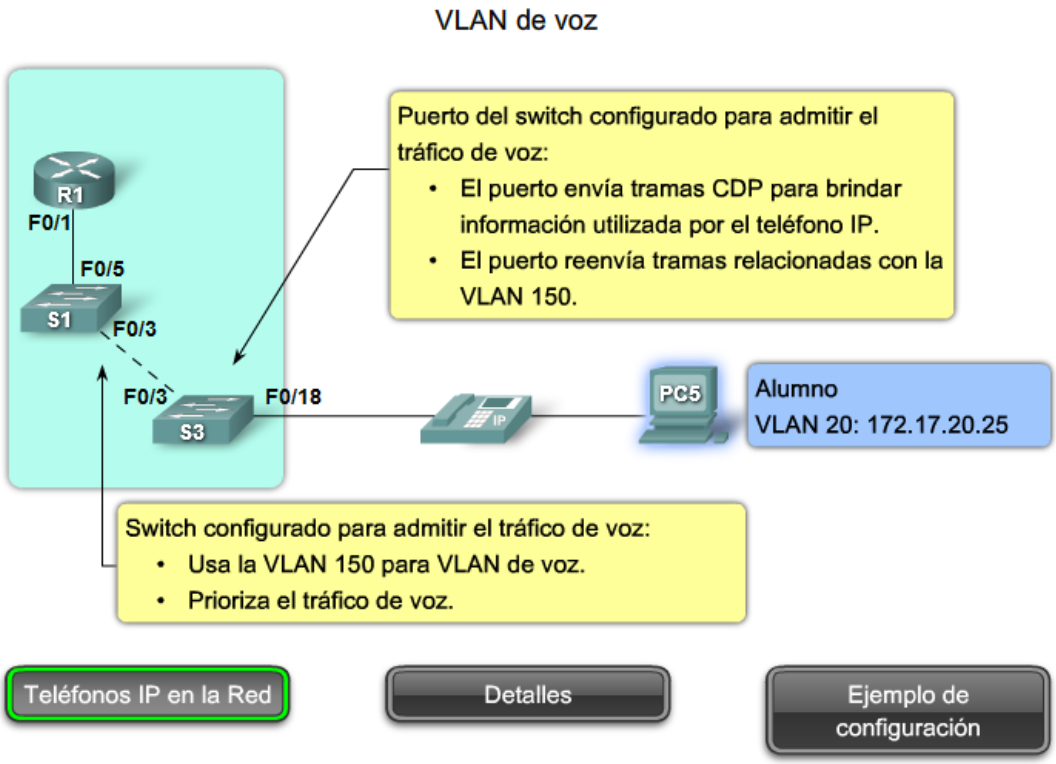
El tráfico IP multicast se envía desde una dirección de origen particular a un grupo multicast que se identifica mediante un único IP y un par de direcciones MAC de grupo de destino. Broadcasts Cisco IP/TV son ejemplos de aplicaciones que genera este tipo de tráfico. El tráfico multicast puede producir una gran cantidad de datos que se transmiten a través de la red. Cuando la red debe admitir tráfico multicast, las VLAN deben configurarse para asegurarse de que el tráfico multicast se dirija sólo a aquellos dispositivos de usuario que utilizan el servicio proporcionado, como aplicaciones de audio o video remoto. Los routers se deben configurar para asegurar que el tráfico multicast se envíe a las áreas de red cuando se le solicita.

Datos normales

El tráfico de datos normales se relaciona con el almacenamiento y creación de archivos, servicios de impresión, acceso a la base de datos del correo electrónico y otras aplicaciones de red compartidas que son comunes para usos comerciales. Las VLAN son una solución natural para este tipo de tráfico, ya que pueden segmentar a los usuarios por sus funciones o área geográfica para administrar de manera más fácil las necesidades específicas.

Clase Scavenger

Se pretende que la clase Scavenger proporcione servicios less-than-best-effort a ciertas aplicaciones. Las aplicaciones que se asignan a esta clase contribuyen poco o nada a los objetivos organizativos de la empresa y están generalmente orientadas, por su naturaleza, al entretenimiento. Esto incluye aplicaciones compartidas de medios entre pares (KaZaa, Morpheus, Groekster, Napster, iMesh, y demás), aplicaciones de juegos (Doom, Quake, Unreal Tournament, y demás) y cualquier aplicación de video de entretenimiento.



4.3.6. Enlaces Troncales de las VLAN

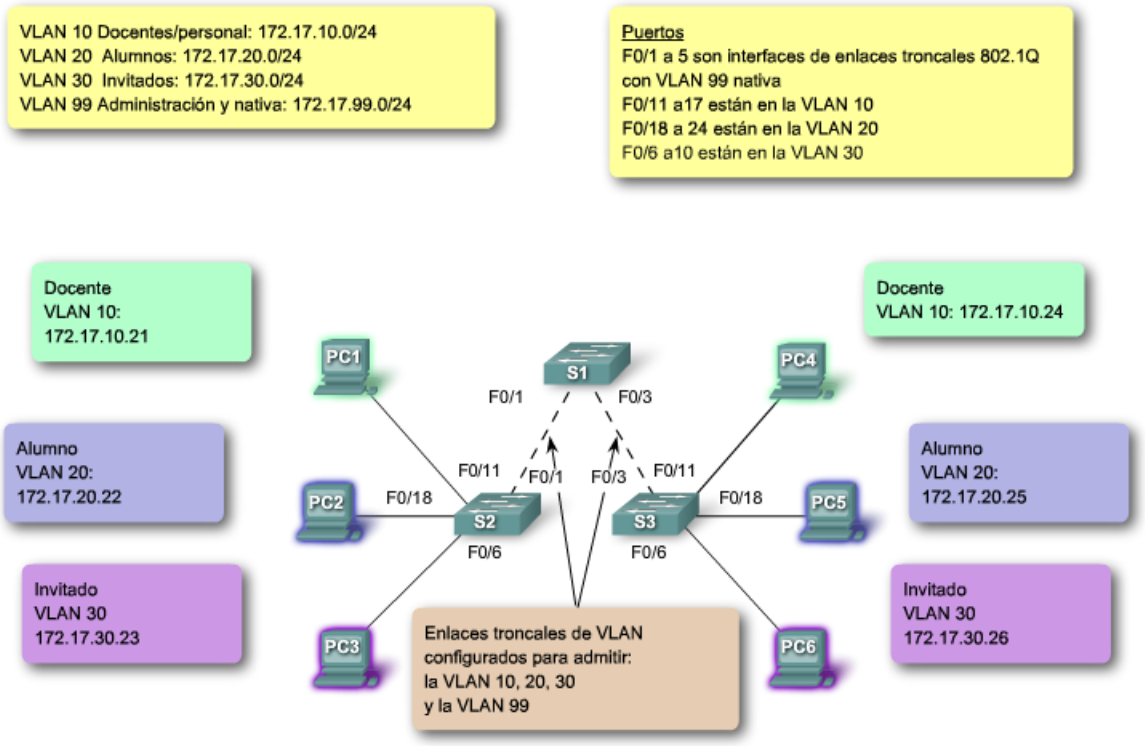
¿Qué es un enlace troncal?

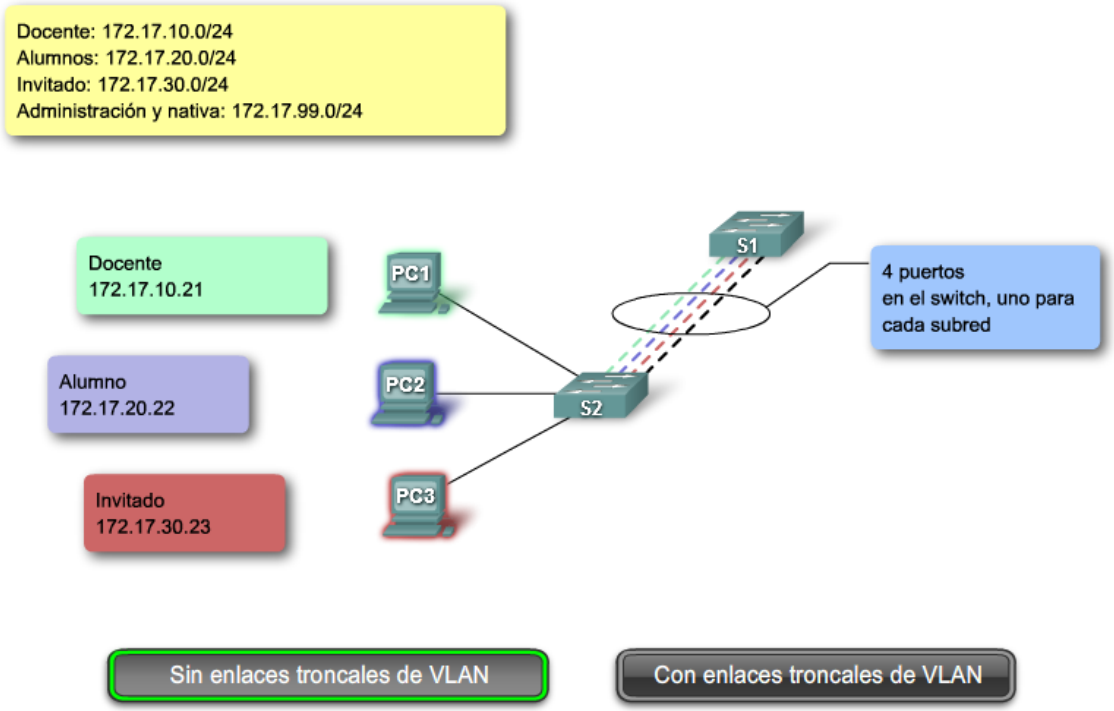
Es difícil describir las VLAN sin mencionar los enlaces troncales de la VLAN. Aprendió acerca de controlar broadcasts de la red con segmentación de la VLAN y observó la manera en que los enlaces troncales de la VLAN transmitieron tráfico a diferentes partes de la red configurada en una VLAN. En la figura, los enlaces entre los switches S1 y S2 y entre S1 y S3 están configurados para transmitir el tráfico que proviene de las VLAN 10, 20, 30 y 99. Es posible que esta red no funcione sin los enlaces troncales de la VLAN. El usuario descubrirá que la mayoría de las redes que encuentra están configuradas con enlaces troncales de la VLAN. Esta sección une su conocimiento previo sobre el enlace troncal de la VLAN y proporciona los detalles necesarios para poder configurar el enlace troncal de la VLAN en una red.

Definición de 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. Más adelante en esta sección, aprenderá acerca de 802.1Q.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.





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 agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

El etiquetado de la trama se mencionó en diferentes oportunidades. La primera vez se hizo en referencia a la configuración del modo de voz en un puerto de switch. En esa sección aprendió que una vez que se configura, un teléfono de Cisco (que incluye un switch pequeño) etiqueta las tramas de voz con un ID de VLAN. También aprendió que los ID de VLAN pueden estar en un rango normal, 1-1005 y en un rango ampliado, 1006-4094. ¿De qué manera se insertan los ID de la VLAN en la trama?

Descripción general del etiquetado de la trama de la VLAN

Antes de explorar los detalles de una trama 802.1Q, es útil comprender lo que hace un switch al enviar una trama a un enlace troncal. Cuando el switch recibe una trama en un puerto configurado en modo de acceso con una VLAN estática, el switch quita la trama e inserta una etiqueta de VLAN, vuelve a calcular la FCS y envía la trama etiquetada a un puerto de enlace troncal.

Nota: Más adelante, en esta sección, se presenta una animación de la operación de enlace troncal..

Detalles del campo de etiqueta de VLAN

El campo de etiqueta de la VLAN consiste de un campo EtherType, un campo de información de control de etiqueta y del campo de FCS.

Campo EtherType

Establecido al valor hexadecimal de 0x8100. Este valor se denomina valor de ID de protocolo de etiqueta (TPID, por su sigla en inglés). Con el campo EtherType configurado al valor TPID, el switch que recibe la trama sabe buscar la información en el campo de información de control de etiqueta.

Campo Información de control de etiqueta

El campo de información de control de etiqueta contiene:

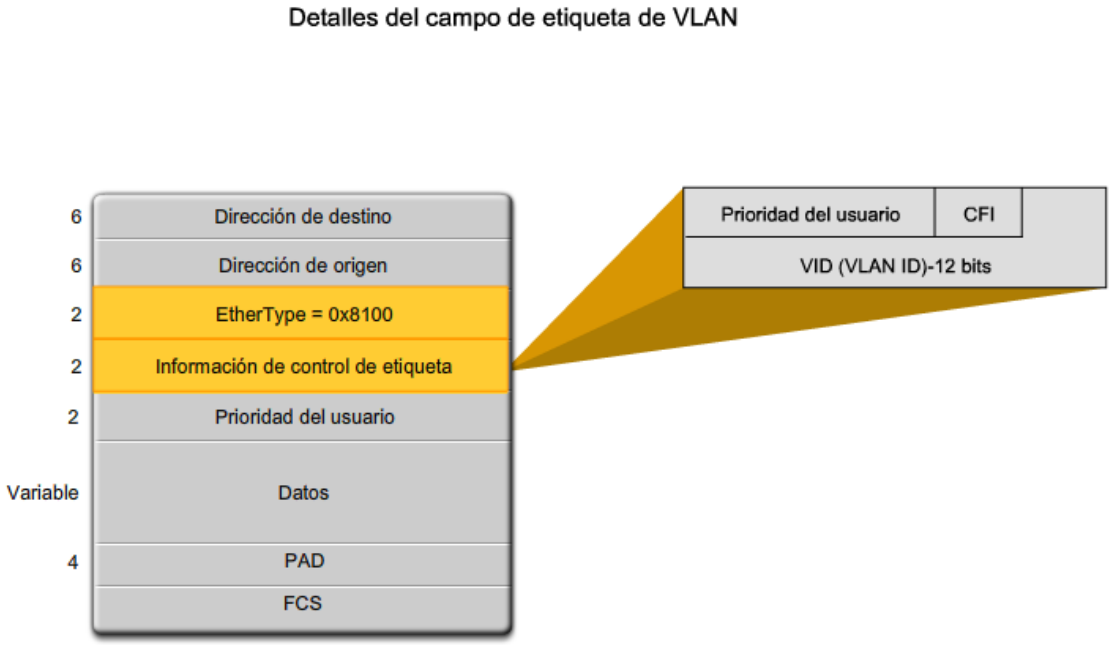
3 bits de prioridad del usuario: utilizado por el estándar 802.1p, que especifica cómo proporcionar transmisión acelerada de las tramas de la Capa 2. Una descripción de IEEE 802.1p está más allá del alcance de este curso; sin embargo el usuario aprendió algo sobre esto anteriormente en el análisis sobre las VLAN de voz.

1 bit de Identificador de formato ideal (CFI, por su sigla en inglés): permite que las tramas Token Ring se transporten con facilidad a través de los enlaces Ethernet.

12 bits del ID de la VLAN (VID): números de identificación de la VLAN; admite hasta 4096 ID de VLAN.

Campo FCS

Luego de que el switch inserta los campos de información de control de etiqueta y EtherType, vuelve a calcular los valores FCS y los inserta en la trama.



4.3.7. VLAN nativas y enlace troncal 802.1Q

Ahora que el usuario sabe más acerca de cómo un switch etiqueta una trama con la VLAN adecuada, es momento de explorar la manera en que la VLAN nativa admite el switch en el manejo de tramas etiquetadas y sin etiquetar que llegan en un puerto de enlace troncal 802.1Q.

Tramas etiquetadas en la VLAN nativa

Algunos dispositivos que admiten enlaces troncales etiquetan la VLAN nativa como comportamiento predeterminado. El tráfico de control enviado en la VLAN nativa debe estar sin etiquetar. Si un puerto de enlace troncal 802.1Q recibe una trama etiquetada en la VLAN nativa, éste descarta la trama. Como consecuencia, al configurar un puerto de switch en un switch Cisco, es necesario identificar estos dispositivos y configurarlos de manera

que no envíen tramas etiquetadas en la VLAN nativa. Los dispositivos de otros proveedores que admiten tramas etiquetadas en la VLAN nativa incluyen: teléfonos IP, servidores, routers y switches que no pertenecen a Cisco.

Tramas sin etiquetar en la VLAN nativa

Cuando un puerto de enlace troncal de switch Cisco recibe tramas sin etiquetar, éste envía esas tramas a la VLAN nativa. Como debe recordar, la VLAN nativa predeterminada es la VLAN 1. Al configurar un puerto de enlace troncal 802.1Q, se asigna el valor del ID de la VLAN nativa al ID de la VLAN de puerto predeterminado (PVID). Todo el tráfico sin etiquetar que ingresa o sale del puerto 802.1Q se envía en base al valor del PVID. Por ejemplo: si la VLAN 99 se configura como la VLAN nativa, el PVID es 99 y todo el tráfico sin etiquetar se envía a la VLAN 99. Si la VLAN nativa no ha sido configurada nuevamente, el valor de PVID se configura para la VLAN 1.

En este ejemplo, la VLAN 99 se configura como VLAN nativa en el puerto F0/1 en el switch S1. Este ejemplo muestra cómo volver a configurar la VLAN nativa desde su configuración predeterminada de la VLAN 1.

Comenzando en el modo EXEC privilegiado, la figura describe la manera de configurar la VLAN nativa en el puerto F0/1 en el switch S1 como un enlace troncal IEEE 802.1Q con la VLAN 99 nativa.

Al utilizar el comando show interfaces interface-id switchport puede verificar rápidamente si ha vuelto a configurar la VLAN nativa desde la VLAN 1 a la VLAN 99 de manera correcta. El resultado resaltado en la captura de pantalla indica que la configuración fue un éxito.

VLAN Nativas y Enlace troncal 802.1Q

Tramas con etiquetas en la VLAN nativa

- Descartadas por el switch
- Los dispositivos no deben etiquetar el tráfico de control destinado a la VLAN nativa

Tramas sin etiquetas en la VLAN nativa

- Tienen su PVID modificado al valor de la VLAN nativa configurada
- Permanece sin etiquetar
- Son reenviadas en la VLAN nativa configurada

VLAN Nativas y Enlace troncal 802.1Q

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global en el switch S1.	`S1#configure terminal`
Ingresar el modo de configuración de interfaz.	`S1(config)#interface F0/1`
Definir la interfaz F0/1 como un enlace troncal IEEE 802.1Q.	`S1(config-if)#switchport mode trunk`
Configurar la VLAN 99 para que sea la VLAN nativa.	`S1(config-if)#switchport trunk native vlan 99`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

VLAN Nativas y Enlace troncal 802.1Q

```
S1#show interfaces F0/1 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
…
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
….
Trunking VLANs Enabled: ALL
```

Operación de Enlace Troncal

Enlace troncal en acción

El usuario ha aprendido la manera en que un switch maneja el tráfico sin etiquetar en un enlace troncal. El usuario sabe que las tramas que atraviesan un enlace troncal están etiquetadas con el ID de la VLAN del puerto de acceso donde llegó la trama. En la figura, la PC1 en la VLAN 10 y la PC3 en la VLAN 30 envían tramas de broadcast al switch S2. El switch S2 etiqueta esas tramas con el ID adecuado de la VLAN y luego envía las tramas a través del enlace troncal al switch S1. El switch S1 lee el ID de la VLAN en las tramas y los envía en broadcast a cada puerto configurado para admitir la VLAN 10 y la VLAN 30. El switch S3 recibe esas tramas, quita los ID de la VLAN y los envía como tramas sin etiquetar a la PC4 en la VLAN 10 y a la PC 6 en la VLAN 30.

Modo de enlaces troncales

El usuario ha aprendido la manera en que el enlace troncal 802.1Q funciona en los puertos de switch de Cisco. Ahora es momento de examinar las opciones de configuración del modo de puerto de enlace troncal 802.1Q. Primero, es necesario analizar un protocolo de enlace troncal anterior de Cisco denominado enlace entre switch (ISL, Inter-Switch Link), debido a que verá esta opción en las guías de configuración de software del switch.

IEEE, no ISL

Aunque se puede configurar un switch de Cisco para admitir dos tipos de puertos de enlace troncal, IEEE 802.1Q e ISL; en la actualidad, sólo se usa el 802.1Q. Sin embargo, las redes antiguas siguen usando ISL, y es útil aprender sobre cada tipo de puerto de enlace troncal.

Un puerto de enlace troncal IEEE 802.1Q admite tráfico simultáneo etiquetado y sin etiquetar. A un puerto de enlace troncal 802.1Q se le asigna un PVID predeterminado y todo el tráfico sin etiquetar se transporta en el PVID predeterminado del puerto. Se supone que todo el tráfico etiquetado y sin etiquetar con un ID nulo de la VLAN pertenece al PVID predeterminado del puerto. El paquete con un ID de VLAN igual al PVID predeterminado del puerto de salida se envía sin etiquetar. El resto del tráfico se envía con una etiqueta de VLAN.

En un puerto de enlace troncal ISL se espera que todos los paquetes recibidos sean encapsulados con un encabezado ISL y que todos los paquetes transmitidos se envíen con un encabezado ISL. Las tramas nativas (sin etiquetar) recibidas de un puerto de enlace troncal ISL se descartan. ISL ya no es un modo de puerto de enlace troncal recomendado y no se admite en varios de los switches de Cisco.

DTP

El protocolo de enlace troncal dinámico (DTP) es un protocolo propiedad de Cisco. Los switches de otros proveedores no admiten el DTP. El DTP es habilitado automáticamente en un puerto de switch cuando algunos modos de enlace troncal se configuran en el puerto de switch.

El DTP administra la negociación de enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP. El DTP admite los enlaces troncales ISL y 802.1Q. Este curso se concentra en la implementación de 802.1Q del DTP. Un análisis detallado sobre el DTP está más allá de este curso, sin embargo aprenderá sobre esto en las prácticas de laboratorio y actividades asociadas con este capítulo. Los switches no necesitan que el DTP realice enlaces troncales, y algunos switches y routers de Cisco no admiten al DTP. Para aprender más sobre la admisión de DTP en switches de Cisco, visite: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml.

4.3.8. Modos de enlaces troncales

Un puerto de switch en un switch de Cisco admite varios modos de enlaces troncales. El modo de enlace troncal define la manera en la que el puerto negocia mediante la utilización del DTP para configurar un enlace troncal con su puerto par. A continuación, se observa una breve descripción de los modos de enlaces troncales disponibles y la manera en que el DTP se implementa en cada uno.

Activado (de manera predeterminada)

El puerto del switch envía periódicamente tramas de DTP, denominadas notificaciones, al puerto remoto. El comando utilizado es switchport mode trunk. El puerto de switch local notifica al puerto remoto que está cambiando dinámicamente a un estado de enlace troncal. Luego, el puerto local, sin importar la información de DTP que el puerto remoto envía como respuesta a la notificación, cambia al estado de enlace troncal. El puerto local se considera que está en un estado de enlace troncal (siempre activado) incondicional.

Dinámico automático

El puerto del switch envía periódicamente tramas de DTP al puerto remoto. El comando utilizado es switchport mode dynamic auto. El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales pero no solicita pasar al estado de enlace troncal. Luego de una negociación de DTP, el puerto local termina en estado de enlace troncal sólo si el modo de enlace troncal del puerto remoto ha sido configurado para estar activo o si es conveniente. Si ambos puertos en los switches se configuran en automático, no negocian para estar en un estado de enlace troncal. Negocian para estar en estado de modo de acceso (sin enlace troncal).

Las tramas de DTP convenientes y dinámicas

Las tramas de DTP se envían periódicamente al puerto remoto. El comando utilizado es switchport mode dynamic desirable. El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales y solicita al puerto de switch remoto pasar al estado de enlace troncal. Si el puerto local detecta que el remoto ha sido configurado en

modo activado, conveniente o automático, el puerto local termina en estado de enlace troncal. Si el puerto de switch remoto está en modo sin negociación, el puerto de switch local permanece como puerto sin enlace troncal.

Desactivación del DTP

Puede desactivar el DTP para el enlace troncal para que el puerto local no envíe tramas de DTP al puerto remoto. Utilice el comando switchport nonegotiate. Entonces el puerto local se considera que está en un estado de enlace troncal incondicional. Utilice esta característica cuando necesite configurar un enlace troncal con un switch de otro proveedor.

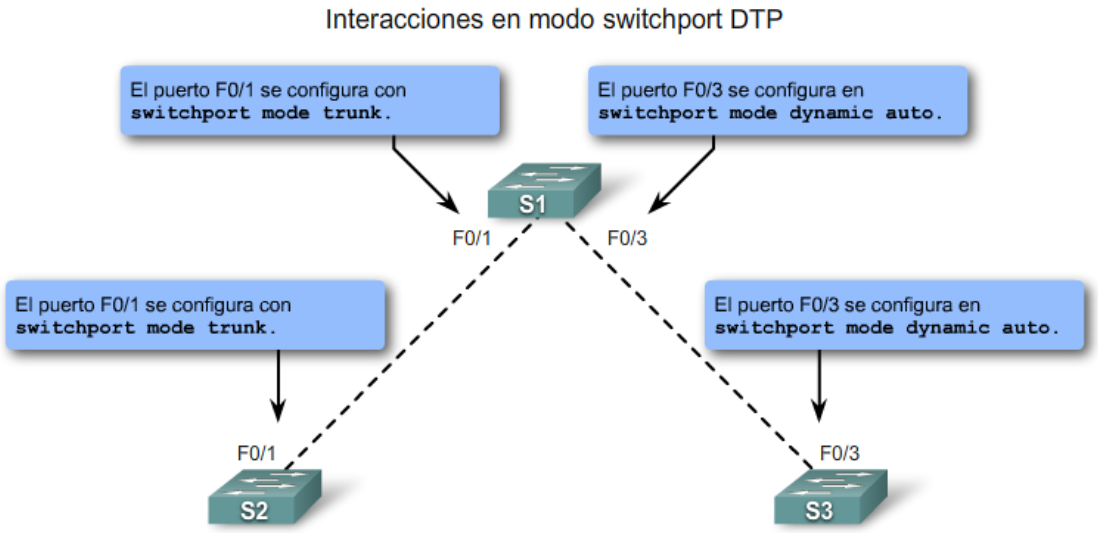
Ejemplo de modo de enlace troncal

En la figura, los puertos F0/1 en los switches S1 y S2 se configuran con modo de enlace troncal activado. Los puertos F0/3 en los switches S1 y S3 se configuran para que estén en modo de enlace troncal automático. Cuando se completen las configuraciones de switch y los switches están configurados por completo, ¿Qué enlace se configurará como enlace troncal?

El enlace entre los switches S1 y S2 se convierte en enlace troncal porque los puertos F0/1 en los switches S1 y S2 se configuran para ignorar todas las notificaciones del DTP y aparecen y permanecen en modo de puerto de enlace troncal. Los puertos F0/3 en los switches S1 y S3 se establecen en automático, entonces negocian para estar en estado predeterminado, el estado de modo de acceso (sin enlace troncal). Esto da por resultado un enlace troncal inactivo. Cuando configura un puerto de enlace troncal para que esté en modo de puerto de enlace troncal, no existe ambigüedad sobre en qué estado se encuentra el enlace troncal: está siempre activo. Además, es fácil recordar en qué estado están los puertos de enlaces troncales: si se supone que el puerto es un enlace troncal, el modo de enlace troncal es activo..

Nota: El modo switchport predeterminado para una interfaz en un switch Catalyst 2950 es conveniente y dinámico, pero el modo switchport predeterminado para una interfaz en un switch Catalyst 2960 es automático y dinámico. Si S1 y S3 fueran switches Catalyst 2950

con interfaz F0/3 en modo switchport predeterminado, el enlace entre S1 y S3 se convertiría en un enlace troncal activo.



4.3.9. Configuración de las VLAN y enlaces troncales

En este capítulo, ha visto ejemplos de los comandos utilizados para configurar las VLAN y los enlaces troncales de las VLAN. En esta sección aprenderá sobre los comandos clave IOS de Cisco necesarios para crear, eliminar y verificar las VLAN y los enlaces troncales de las VLAN. Por lo general, estos comandos poseen muchos parámetros opcionales que extienden las capacidades de la tecnología de las VLAN y enlaces troncales de las VLAN. Estos comandos opcionales no se presentan; sin embargo, se suministran referencias en caso de que desee investigar estas opciones. Esta sección se enfoca en suministrarle las habilidades y conocimientos necesarios para configurar las VLAN y los enlaces troncales de la VLAN con sus características clave.

En esta sección, se muestra la sintaxis de configuración y verificación para un lado de la VLAN o del enlace troncal. En las prácticas de laboratorio y actividades configurará ambos lados y verificará que el enlace (VLAN o enlace troncal de VLAN) esté configurado correctamente.

Nota: Si desea mantener la configuración activa recién configurada, debe guardarla en la configuración de inicio.

Agregue una VLAN

En este tema, aprenderá a crear una VLAN estática en un switch Cisco Catalyst mediante el modo de configuración global de la VLAN. Existen dos modos diferentes para configurar las VLAN en un switch Cisco Catalyst: modo de configuración de base de datos y modo de configuración global. A pesar de que la documentación de Cisco menciona el modo de configuración de base de datos de la VLAN, se elimina a favor del modo de configuración global de la VLAN.

El usuario configurará las VLAN con los ID en el rango normal. Recuerde que existen dos rangos de ID de la VLAN. El rango normal incluye los ID 1 a 1001 y el rango ampliado consiste de los ID 1006 a 4094. VLAN 1 y 1002 a 1005 son números de ID reservados. Cuando configura las VLAN de rango normal, los detalles de configuración se almacenan automáticamente en la memoria flash del switch en un archivo llamado vlan.dat. Debido a que el usuario configura frecuentemente otros aspectos de un switch Cisco al mismo tiempo, es una buena práctica guardar los cambios de la configuración activa en la configuración de inicio.

Agregar una VLAN

3.3.2.1 -A: Agregar una VLAN

Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Crear una VLAN. El id de la VLAN es el número de VLAN que se creará. Switches para el modo de configuración de VLAN para el vlan id de la VLAN.	`S1(config)#vlan vlan id`
(Opcional) Especificar un único nombre de VLAN para identificar la misma. Si no se ingresa ningún nombre, el número de la VLAN, relleno con ceros, se anexa a la palabra 'VLAN', por ejemplo, VLAN0020.	`S1(config-vlan)#name Nombre de VLAN`
Volver a modo EXEC privilegiado. Debe finalizar su sesión de configuración para que la configuración se guarde en el archivo vlan.dat y para que la configuración entre en vigencia.	`S1(config-vlan)#end`

4.3.10. Configuración de las VLAN

Asignación de un puerto de switch

Después de crear una VLAN, asígnele un puerto o más. Cuando asigna un puerto de switch a una VLAN en forma manual, se lo conoce como puerto de acceso estático. Un puerto de acceso estático puede pertenecer a sólo una VLAN por vez.

Haga clic en el botón Sintaxis del comando en la figura para revisar los comandos IOS de Cisco para asignar un puerto de acceso estático a la VLAN.

Haga clic en el botón Ejemplo en la figura para ver cómo la VLAN del estudiante, VLAN 20, se asigna estáticamente al puerto F0/18 en el switch S1. El puerto F0/18 se ha asignado a la VLAN 20, de manera que la computadora del estudiante, PC2, está en la VLAN 20. Cuando la VLAN 20 se configura en otros switches, el administrador de red sabe configurar las otras computadoras de estudiantes para encontrarse en la misma subred que PC2: 172.17.20.0 /24.

Haga clic en el botón Verificación en la figura para confirmar que el comando show vlan brief muestra los contenidos del archivo vlan.dat. En la captura de pantalla se resalta la VLAN del estudiante, VLAN 20.

Asignar un puerto de switch

Sintaxis del comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	S1#**configure terminal**
Ingresar la interfaz para asignar la VLAN.	S1(config)#**interface** *interface id*
Definir el modo de asociación de VLAN para el puerto.	S1(config-if)#**switchport mode access**
Asignar el puerto a una VLAN.	S1(config-if)#**switchport access vlan** *vlan id*
Volver al modo EXEC privilegiado.	S1(config-if)#**end**

4.3.11. Administración de las VLAN

Verificación de las vinculaciones de puerto y de las VLAN

Después de configurar la VLAN, puede validar las configuraciones de la VLAN mediante la utilización de los comandos show del IOS de Cisco.

La sintaxis de comando para los diversos comandos show del IOS de Cisco debe conocerse bien. Ya ha utilizado el comando show vlan brief. Se pueden ver ejemplos de estos comandos haciendo clic en los botones de la figura.

En este ejemplo, el usuario puede ver que el comando show vlan name student no produce resultados muy legibles. Aquí se prefiere utilizar el comando show vlan brief. El comando

show vlan summary muestra la cuenta de todas las VLAN configuradas. El resultado muestra seis VLAN: 1, 1002-1005 y la VLAN del estudiante, VLAN 20.

Este comando muestra muchos detalles que exceden el alcance de este capítulo. La información clave aparece en la segunda línea de la captura de pantalla e indica que la VLAN 20 está activa.

Este comando muestra información útil para el usuario. Puede determinar que el puerto F0/18 se asigna a la VLAN 20 y que la VLAN nativa es la VLAN 1. El usuario ha utilizado este comando para revisar la configuración de una VLAN de voz.

Verificación de las vinculaciones de puerto y de las VLAN

Mostrar el comando VLAN

Sintaxis del comando de CLI IOS de Cisco	
show vlan [brief | id *vlan-id* **| name** *Nombre de VLAN* **| summary].**	
Mostrar una línea para cada VLAN con el nombre, estado y los puertos de la VLAN.	**brief**
Mostrar información sobre una sola VLAN identificada por el número de ID de la VLAN. Para la vlan-id, el intervalo es de 1 a 4094.	**id** *vlan-id*
Mostrar información sobre una sola VLAN identificada por el nombre de VLAN. El nombre de la VLAN es una cadena ASCII de 1 a 32 caracteres.	**name** *Nombre de VLAN*
Mostrar el resumen de información de la VLAN.	**resumen**

Mostrar el comando de interfaces

Sintaxis del comando de CLI IOS de Cisco	
show interfaces *[interface-id* **| vlan** *vlan-id]* **| switchport**	
Las interfaces válidas incluyen puertos físicos (incluidos tipo, módulo y número de puerto) y canales de puerto. El intervalo de canales de puerto es de 1 a 6.	*interface-id*
Identificación de VLAN. El intervalo es de 1 a 4094.	**vlan** *vlan-id*
Mostrar el estado de administración y operación de un puerto de conmutación, incluidas las configuraciones de bloqueo y protección del puerto.	**switchport**

Vínculos al puerto de administración

Existen varias formas de administrar las VLAN y los vínculos del puerto de VLAN. La figura muestra la sintaxis para el comando no switchport access vlan.

Reasigne un puerto a la VLAN 1

Para reasignar un puerto a la VLAN 1, el usuario puede usar el comando no switchport access vlan en modo de configuración de interfaz. Examine la salida del comando show vlan brief que aparece inmediatamente a continuación. Note cómo VLAN 20 sigue activa. Sólo se la ha eliminado de la interfaz F0/18. En el comando show interfaces f0/18

switchport, se puede ver que la VLAN de acceso para interfaz F0/18 se ha reestablecido a la VLAN 1.

Reasigne la VLAN a otro puerto

Un puerto de acceso estático sólo puede tener una VLAN. Con el software IOS de Cisco, no necesita quitar primero un puerto de una VLAN para cambiar su membresía de la VLAN. Cuando reasigna un puerto de acceso estático a una VLAN existente, la VLAN se elimina automáticamente del puerto anterior. En el ejemplo, el puerto F0/11 se reasigna a la VLAN 20.

Administrar la pertenencia al puerto

Sintaxis de comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	`S1#configure terminal`
Ingresar el modo de configuración de interfaz para que se configure la interfaz.	`S1(config)#interface` *interface id*
Eliminar la asignación de VLAN en esa interfaz de puerto de switch y cambiarla a la pertenencia de la VLAN predeterminada de VLAN 1.	`S1(config-if)#no switchport access vlan`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Eliminación de las VLAN

La figura proporciona un ejemplo de uso del comando de configuración global no vlan vlan-id para eliminar la VLAN 20 del sistema. El comando show vlan brief verifica que la VLAN 20 ya no está en el archivo vlan.dat.

Alternativamente, el archivo completo vlan.dat puede eliminarse con el comando delete flash:vlan.dat del modo EXEC privilegiado. Después de que el switch se haya vuelto a cargar, las VLAN configuradas previamente ya no estarán presentes. Esto ubica al switch, en forma efectiva, en "de fábrica de manera predeterminada" con respecto a las configuraciones de la VLAN.

Nota: Antes de eliminar una VLAN, asegúrese de reasignar primero todos los puertos miembro a una VLAN diferente. Todo puerto que no se ha movido a una VLAN activa no puede comunicarse con otras estaciones luego de eliminar la VLAN.

4.3.12. Configuración de los enlaces troncales

Configuración de un enlace troncal 802.1Q

Para configurar un enlace troncal en un puerto de switch, utilice el comando switchport mode trunk. Cuando ingresa al modo enlace troncal, la interfaz cambia al modo permanente de enlace troncal y el puerto ingresa a una negociación de DTP para convertir el vínculo a un vínculo de enlace troncal, por más que la interfaz que la conecta no acepte cambiar. En este curso configurará un enlace troncal utilizando únicamente el comando switchport mode trunk. En la figura se muestra la sintaxis de comando IOS de Cisco para especificar una VLAN nativa diferente a la VLAN 1. En el ejemplo, el usuario configura la VLAN 99 como la VLAN nativa. Se muestra la sintaxis de comando utilizada para admitir una lista de las VLAN en el enlace troncal. En este puerto de enlace troncal, admita las VLAN 10, 20 y 30.

El usuario ya conoce esta topología. Las VLAN 10, 20 y 30 admitirán las computadoras del Cuerpo Docente, del Estudiante y del Invitado: PC1, PC2 y PC3. El puerto F0/1 en el switch S1 se configura como un puerto de enlace troncal para admitir las VLAN 10, 20 y 30. La VLAN 99 se configura como la VLAN nativa.

El ejemplo configura al puerto F0/1 en el switch S1 como puerto de enlace troncal. Éste vuelve a configurar la VLAN nativa como VLAN 99 y agrega las VLAN 10, 20 y 30 como las VLAN admitidas en el puerto F0/1.

Un análisis sobre el DTP y los detalles de cómo trabaja cada opción de modo de acceso al puerto de switch supera el alcance del curso. Para más detalles sobre los parámetros asociados con el comando de interfaz switchport mode visite:

Configurar un enlace troncal 802.1Q

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global.	S1#**configure terminal**
Ingresar el modo de configuración de interfaz para la interfaz definida.	S1(config)#**interface** *interface id*
Hacer que el enlace que conecta los switches sea un enlace troncal.	S1(config-if)#**switchport mode trunk**
Especificar otra VLAN como la VLAN nativa para los enlaces troncales IEEE 802.1Q sin etiquetar.	S1(config-if)#**switchport trunk native vlan** *vlan id*
Volver al modo EXEC privilegiado.	S1(config-if)#**end**

Verificación de la configuración del enlace troncal

La figura muestra la configuración del puerto de switch F0/1 en el switch S1. El comando utilizado es el comando show interfaces interface-ID switchport.

La primera área resaltada muestra que el puerto F0/1 tiene el modo administrativo establecido en Enlace Troncal. El puerto se encuentra en modo de enlace troncal. La siguiente área resaltada verifica que la VLAN nativa sea la VLAN 99, la VLAN de administración. En la parte inferior del resultado, la última área resaltada muestra que las VLAN del enlace troncal habilitadas son las VLAN 10, 20 y 30.

Administración de una configuración de enlace troncal

En la figura, se muestran los comandos para reestablecer las VLAN admitidas y la VLAN nativa del enlace troncal al estado predeterminado. También se muestra el comando para reestablecer el puerto de switch a un puerto de acceso y, en efecto, eliminar el puerto de enlace troncal.

En la figura, los comandos utilizados para reestablecer todas las características de enlace troncal de una interfaz de enlace troncal a las configuraciones predeterminadas, están resaltados en el resultado de muestra. El comando show interfaces f0/1 switchport revela que el enlace troncal se ha reconfigurado a un estado predeterminado.

El resultado de la figura muestra los comandos utilizados para eliminar la característica de enlace troncal del puerto de switch F0/1 en el switch S1. El comando show interfaces f0/1 switchport revela que la interfaz F0/1 está ahora en modo de acceso estático.

Administración de una configuración de enlace troncal

Sintaxis de comando de la CLI del IOS de Cisco	
Utilice este comando en el modo de configuración de interfaz para restablecer todas las VLAN configuradas en la interfaz del enlace troncal.	`S1(config-if)#no switchport trunk allowed vlan`
Utilice este comando en el modo de configuración de interfaz para restablecer la VLAN nativa nuevamente a VLAN1.	`S1(config-if)#no switchport trunk native vlan`
Utilice este comando en el modo de configuración de interfaz para restablecer la interfaz de puerto de enlace troncal nuevamente a un puerto de modo de acceso estático.	`S1(config-if)#switchport mode access`

4.3.13. Problemas comunes con los enlaces comunes

Problemas comunes con enlaces troncales

En este tema, el usuario aprende sobre los problemas comunes de la VLAN y el enlace troncal, que suelen asociarse a configuraciones incorrectas. 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.

Si ha descubierto un problema con una VLAN o con un enlace troncal y no sabe cuál es, comience la resolución de problemas examinando los enlaces troncales para ver si existe una falta de concordancia de la VLAN nativa y luego vaya siguiendo los pasos de la lista. El resto de este tema examina cómo reparar los problemas comunes con enlaces troncales. El próximo tema presenta cómo identificar y resolver la configuración incorrecta de la VLAN y las subredes IP.

Problemas comunes con las VLAN y los enlaces troncales

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.

Faltas de concordancia de la VLAN nativa

El usuario es un administrador de red y recibe un llamado que dice que la persona que utiliza la computadora PC4 no se puede conectar al servidor Web interno, servidor WEB/TFTP de la figura. Sabe que un técnico nuevo ha configurado recientemente el switch S3. El diagrama de topología parece correcto, entonces ¿por qué hay un problema? El usuario decide verificar la configuración en S3.

Tan pronto como se conecta al switch S3, el mensaje de error que aparece en el área superior resaltada en la figura aparece en la ventana de la consola. Observa la interfaz con el comando show interfaces f0/3 switchport. Nota que la VLAN nativa, la segunda área resaltada en la figura, se ha establecido como VLAN 100 y se encuentra inactiva. Sigue leyendo los resultados y observa que las VLAN permitidas son 10 y 99, como aparece en el área inferior resaltada.

Debe reconfigurar la VLAN nativa en el puerto de enlace troncal Fast Ethernet F0/3 para que sea VLAN 99. En la figura, el área superior resaltada muestra el comando para configurar la VLAN nativa en VLAN 99. Las dos áreas resaltadas siguientes confirman que el puerto de enlace troncal Fast Ethernet F0/3 ha reestablecido la VLAN nativa a VLAN 99.

Los resultados que aparecen en la pantalla para la computadora PC4 muestran que la conectividad se ha reestablecido para el servidor WEB/TFTP que se encuentra en la dirección IP 172.17.10.30.

Faltas de concordancia del modo de enlace troncal

En este curso ha aprendido que los vínculos de enlace troncal se configuran estáticamente con el comando switchport mode trunk. Ha aprendido que los puertos de enlace troncal utilizan publicaciones de DTP para negociar el estado del vínculo con el puerto remoto. Cuando un puerto en un vínculo de enlace troncal se configura con un modo de enlace troncal que no es compatible con el otro puerto de enlace troncal, no se puede formar un vínculo de enlace troncal entre los dos switches.

En este caso, surge el mismo problema: la persona que utiliza la computadora PC4 no puede conectarse al servidor Web interno. Una vez más, el diagrama de topología se ha mantenido y muestra una configuración correcta. ¿Por qué hay un problema?

Lo primero que hace es verificar el estado de los puertos de enlace troncal en el switch S1 con el comando show interfaces trunk. El comando revela en la figura que no hay enlace troncal en la interfaz F0/3 del switch S1. Examina la interfaz F0/3 para darse cuenta de que el puerto de switch está en modo dinámico automático, la primera área resaltada en la parte superior de la figura. Un examen de los enlaces troncales en el switch S3 revela que no hay puertos de enlace troncal activos. Más controles revelan que la interfaz F0/3 también se

encuentra en modo dinámico automático, la primera área resaltada en la parte inferior de la figura. Ahora ya sabe por qué el enlace troncal está deshabilitado.

Debe reconfigurar el modo de enlace troncal de los puertos Fast Ethernet F0/3 en los switches S1 y S3. En la parte superior izquierda de la figura, el área resaltada muestra que el puerto se encuentra ahora en modo de enlazamiento troncal. La salida superior derecha del switch S3 muestra el comando utilizado para reconfigurar el puerto y los resultados del comando show interfaces trunk y revela que la interfaz F0/3 ha sido reconfigurada como modo de enlace troncal. El resultado de la computadora PC4 indica que la PC4 ha recuperado la conectividad al servidor WEB/TFTP que se encuentra en la dirección IP 172.17.10.30.

Lista de VLAN incorrecta

Ha aprendido que para que el tráfico de una VLAN se transmita por un enlace troncal, debe haber acceso admitido en el enlace troncal. El comando utilizado para lograr esto es el comando switchport access trunk allowed vlan add vlan-id. En la figura, se han agregado la VLAN 20 (Estudiante) y la computadora PC5 a la red. La documentación se ha actualizado para mostrar que las VLAN admitidas en el enlace troncal son las 10, 20 y 99.

En este caso, la persona que utiliza la computadora PC5 no puede conectarse al servidor de correo electrónico del estudiante, que se muestra en la figura.

Controle los puertos de enlace troncal en el switch S1 con el comando show interfaces trunk. El comando revela que la interfaz F0/3 en el switch S3 está correctamente configurada para admitir las VLAN 10, 20 y 99. Un examen de la interfaz F0/3 en el switch S1 revela que las interfaces F0/1 y F0/3 sólo admiten VLAN 10 y 99. Parece que alguien actualizó la documentación pero olvidó reconfigurar los puertos en el switch S1.

Debe reconfigurar los puertos F0/1 y F0/3 en el switch S1 con el comando switchport trunk allowed vlan 10,20,99. Los resultados que aparecen en la parte superior de la pantalla en la figura, muestran que las VLAN 10, 20 y 99 se agregan ahora a los puertos F0/1 y F0/3 en el switch S1. El comando show interfaces trunk es una excelente herramienta para revelar problemas comunes de enlace troncal. La parte inferior de la figura indica que la PC5 ha recuperado la conectividad con el servidor de correo electrónico del estudiante que se encuentra en la dirección IP 172.17.20.10.

Ha aprendido que para que el tráfico de una VLAN se transmita por un enlace troncal, debe haber acceso admitido en el enlace troncal. El comando utilizado para lograr esto es el comando switchport access trunk allowed vlan add vlan-id. En la figura, se han agregado la VLAN 20 (Estudiante) y la computadora PC5 a la red. La documentación se ha actualizado para mostrar que las VLAN admitidas en el enlace troncal son las 10, 20 y 99.

En este caso, la persona que utiliza la computadora PC5 no puede conectarse al servidor de correo electrónico del estudiante, que se muestra en la figura.

Controle los puertos de enlace troncal en el switch S1 con el comando show interfaces trunk. El comando revela que la interfaz F0/3 en el switch S3 está correctamente configurada para admitir las VLAN 10, 20 y 99. Un examen de la interfaz F0/3 en el switch S1 revela que las interfaces F0/1 y F0/3 sólo admiten VLAN 10 y 99. Parece que alguien actualizó la documentación pero olvidó reconfigurar los puertos en el switch S1.

Debe reconfigurar los puertos F0/1 y F0/3 en el switch S1 con el comando switchport trunk allowed vlan 10,20,99. Los resultados que aparecen en la parte superior de la pantalla en la figura, muestran que las VLAN 10, 20 y 99 se agregan ahora a los puertos F0/1 y F0/3 en el switch S1. El comando show interfaces trunk es una excelente herramienta para revelar problemas comunes de enlace troncal. La parte inferior de la figura indica que la PC5 ha recuperado la conectividad con el servidor de correo electrónico del estudiante que se encuentra en la dirección IP 172.17.20.10.

Un problema común en la configuración de la VLAN

VLAN y subredes IP

Como ha aprendido, 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.

Bibliografía

https://sites.google.com/site/paginamodulo3vlan/home

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml#topic1

http://www.cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_troubleshooting_technotes_list.html

http://www.cisco.com/en/US/products/ps6406/products_command_reference_chapter09186a008081874b.html#wp7730585

http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_se/command/reference/cli3.html#wp1948171