UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SEGMENTACIÓN DE REDES LAN MEDIANTE VLANS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

VIRGILIO AUGUSTO ESPINOZA DEL PINO

PROMOCIÓN
1984 – I I

LIMA – PERÚ
2006

SEGMENTACIÓN DE REDES LAN MEDIANTE VLANS

SUMARIO

Sabemos que la mayoría de las redes LAN implementadas en nuestro país están basadas en Ethernet, estas redes LAN han crecido en numero de computadores en los últimos años. El tráfico de datos en las LAN se ha incrementado como consecuencia de nuevos servicios y más computadores en la LAN.

En varias empresas estatales se tienen un buen número de computadores todos ellos en un solo dominio de difusión, con problemas de congestión debidos al alto tráfico de difusión.

El presente trabajo, intenta mostrar como podemos mejorar el rendimiento de la LAN mediante el uso de redes LAN virtuales (VLAN). En los primeros capítulos se describe en que consisten las VLANs, los tipos de VLAN, los protocolos utilizados.

Más adelante se muestran como se configuran las VLAN en conmutadores de la marca Cisco, luego se tiene una aplicación de un proyecto de VLAN en una empresa local.

Finalmente se describe las ventajas que se tienen al implementar VLAN, que mejoras se logran en la red.

INDICE

PROLOGO

El presente trabajo pretende mostrar, como se puede mejorar el rendimiento de las redes Ethernet mediante la implementación de VLAN. El trabajo solo muestra en detalle la implementación de VLANs estáticas en conmutadores Cisco por su facilidad de configurar y administrar.

Para mostrar la utilidad que se obtiene de la implementación de VLANs se ha tomado como ejemplo la red de una empresa estatal, que tiene problemas congestión. Ya que opera en un solo dominio de difusión.

En el capitulo I se hace una reseña breve de la evolución de las redes Ethernet, el paso de las redes compartidas a las redes conmutadas. En las primeras redes Ethernet el ancho de banda era compartido y se tenían colisiones, en las redes conmutadas el ancho de banda es dedicado y no hay colisiones, pero los mensajes de difusión no se pueden limitar.

En el capitulo II se indica conceptos fundamentales acerca de las VLANs, los tipos de VLAN, como operan las VLAN, se mencionan también algunas ventajas que se tienen al implementarlas.

Además, se mencionan los protocolos utilizados para identificar los paquetes que pertenecen a un grupo de VLAN, aquí se describe dos importantes protocolos como son ISL y IEEE 802.1q. También se menciona el protocolo VTP utilizado por los conmutadores Cisco, para mantener la consistencia de la configuración de VLAN a través de toda la red.

En el capitulo III trata de la configuración de VLAN estáticas en conmutadores Cisco, es decir la creación, verificación y eliminación de VLAN. Así como la asignación de puertos de los conmutadores a las VLAN creadas.

También se muestra la configuración de enlaces troncales, entre conmutadores y en los enrutadores o dispositivos de capa 3. Así como, las maneras de lograr que las VLAN se comuniquen, mediante un enrutador con una única conexión a los conmutadores, o mediante un conmutador de capa3.

El capitulo IV trata de la implementación de VLAN en una empresa que cuenta con cerca de 350 hosts, todos en un solo dominio de difusión. En ella se tenían problemas de exceso de mensajes de difusión, la red cada vez se hacia mas lenta y era necesario mejorar el rendimiento de la red. Aquí se propone como solucionar este problema.

Finalmente se indican las ventajas que se obtienen de implementar las VLANs.

CAPITULO I

INTRODUCCIÓN

Ethernet se ha consolidado en los últimos años como el estándar predominante en las redes locales de ámbito empresarial y metropolitano, por sus altas prestaciones, compatibilidad con equipos Ethernet de distintas velocidades, economía, capacidad de configuración e independencia del direccionamiento IP. Ethernet, ha evolucionado en capacidad desde 10 Mbps a 10 Gbps en 23 años y de los simples puentes que unían dos redes locales se ha pasado a los conmutadores Gigabit. [Stallings]

Las redes Ethernet han evolucionado desde utilizar en sus orígenes un medio compartido a ser punto a punto y desde rango LAN a distancias de rango WAN. Este ha sido un cambio gradual, pero radical desde el punto de vista de Ethernet, porque supone la práctica desaparición del medio compartido, algo esencial en los orígenes de Ethernet.

Las redes Ethernet han evolucionado considerablemente, desde aquellas que utilizaban cable coaxial en una topología en bus, pasando por las redes basadas en concentradores, a las redes conmutadas actuales.

Hace algunos años en las redes Ethernet basadas en concentradores se tenían problemas de colisiones, a medida que la red crecía en número de computadores las colisiones aumentaban. Las colisiones disminuyen el rendimiento de la red. Con el reemplazo de los concentradores por conmutadores se redujeron la cantidad de colisiones. Los conmutadores nos segmentan la red en múltiples dominios de colisión. [Tanenbaun]

Algo que no puede mejorar ni el conmutador, ni el concentrador, es el envío de mensajes de difusión dentro de una red LAN, los que se asemejan a aquellos anuncios que escuchamos en una tienda por departamentos. Estos mensajes los escuchamos todos los que estamos en la tienda (la red LAN), ya sea que estén buscando a alguien o

anunciando algún producto, y ninguna de las personas (computadoras) que estamos dentro de la tienda nos encontramos exentos de hacerlo.

En una LAN estos mensajes de difusión son enviados a través de todos los puertos de un concentrador o de un conmutador. Si una computadora quiere comunicarse con otra y no sabe en dónde se encuentra, entonces la "vocea" dentro de la LAN, creando tráfico dentro de ésta, además todas las computadoras escucharán el mensaje pero sólo podrá contestarlo la que se está buscando, no importando si se encuentra o no conectada dentro del conmutador o concentrador.

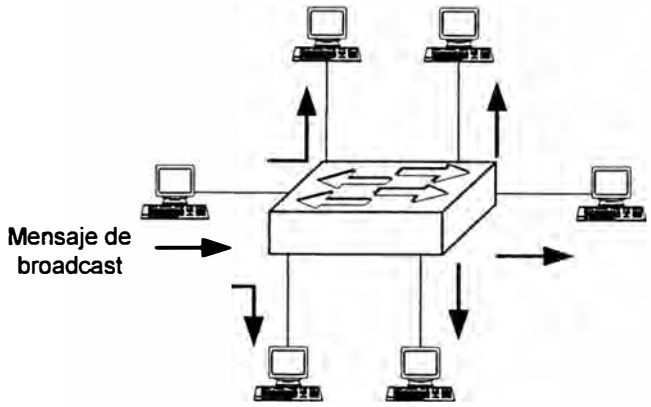


Fig. 1.1 Mensajes de difusión

Estos mensajes de difusión son, en muchas ocasiones, tráfico innecesario como cuando estamos tratando de encontrar una computadora en específico, pero afectamos a todas las que estén dentro del "dominio de difusión" o LAN.

Además en la actualidad en una red, los computadores de escritorio, son cada día más poderosos y corren complejos programas cliente/servidor, o aplicaciones multimedia que generan una gran demanda por ancho de banda.

Una característica importante de la conmutación de Ethernet es la capacidad para crear redes de área local virtuales (VLAN). Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por función laboral o departamento, sin importar la ubicación física de los usuarios.

El tráfico entre las VLAN está restringido. Los conmutadores y puentes envían tráfico de unidifusión, multidifusión y difusión sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. En otras palabras, los dispositivos en la VLAN sólo se

comunican con los dispositivos que están en la misma VLAN. Los enrutadores suministran conectividad entre diferentes VLAN.

Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica. Las empresas con frecuencia usan las VLAN como una manera de garantizar que un conjunto determinado de usuarios se agrupen lógicamente más allá de su ubicación física. Las organizaciones usan las VLAN para agrupar usuarios en el mismo departamento.

Por ejemplo, los usuarios del departamento de Ventas se ubican en la VLAN de Ventas, mientras que los usuarios del Departamento de Ingeniería se ubican en la VLAN de Ingeniería. Las VLAN pueden mejorar la escalabilidad, seguridad y gestión de red. Los enrutadores en las topologías de VLAN proporcionan filtrado de difusión, seguridad y gestión de flujo de tráfico.

Las VLAN que están correctamente diseñadas y configuradas son herramientas potentes para los administradores de red. Las VLAN simplifican las tareas cuando es necesario hacer agregados, mudanzas y modificaciones en una red. Las VLAN mejoran la seguridad de la red y ayudan a controlar los mensajes de difusión de Capa 3. Sin embargo, cuando se las configura de manera incorrecta, las VLAN pueden hacer que una red funcione de manera deficiente o que no funcione en absoluto. La configuración e implementación correctas de las VLAN son fundamentales para el proceso de diseño de red.

CAPITULO II

MARCO TEÓRICO

2.1 Definición de VLAN

Una VLAN se encuentra conformada por un conjunto de dispositivos de red, los cuales funcionan de igual manera como lo hacen los de una LAN, pero con la diferencia de que las estaciones que constituyen la VLAN no necesariamente deben estar ubicadas en el mismo segmento físico. La VLAN básicamente es una subred definida por software y es considerada como un dominio de difusión. [Froom]

La tecnología de los Conmutadores es muy similar a la tecnología de Puentes. En este caso el Puente se encarga de unir dos segmentos de red con diferente subcapa MAC, copiando tramas de un lado a otro, en caso que sea necesario, respetando el formato del encabezado de la misma.

Los Conmutadores conectan 2 segmentos de red de acuerdo a una tabla de direcciones MAC, para saber en que segmento transmitir la trama entrante. Sobre Ethernet, se mejora la utilización del ancho de banda del medio de transmisión, al segmentar la red en dominios de colisión y selectivamente transmitir el tráfico presente al segmento adecuado.

Igualmente importante, los enrutadores son vitales para la tecnología de conmutación, ya que de ellos depende la comunicación entre los grupos de trabajo definidos para cada VLAN.

Las VLAN segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular comparten la misma VLAN, sin importar la conexión física o la ubicación.

Prácticamente cada protocolo de red crea tráfico de difusión. Los computadores con *Windows de Microsoft*, crean mensajes de difusión para anunciar o solicitar los servicios. Aún más, las aplicaciones multimedia crean tramas de difusión y de multidifusión que se distribuyen a través del dominio de difusión.

Los mensajes de difusión son necesarios para sostener las operaciones de protocolo, y es por lo tanto aceptable la sobrecarga de la red. Los mensajes de difusión van a todos los dispositivos en el dominio de difusión y debe ser procesado por los dispositivos que lo reciben. A excepción del tráfico basado en multimedia, las tramas de difusión raramente transportan datos de usuario. Desde que los conmutadores inundan de difusión, ellos consumen ancho de banda en la LAN, teniendo como resultado una reducción del ancho de banda para el tráfico productivo.

Los mensajes de difusión influyen también en el desempeño de las estaciones de trabajo. Cualquier difusión recibida por una estación de trabajo interrumpe la CPU y lo previene de trabajar en aplicaciones de usuario. Cuando el número de mensajes de difusión por segundo aumenta en la interfaz, la utilización efectiva de la CPU disminuye. Si los mensajes de difusión y multidifusión crean problemas en la red, crear dominios de difusión más pequeños pueden mitigar los efectos negativos.

Una VLAN es un dominio de difusión que se crea en uno o más conmutadores. Un mensaje de difusión que ocurre en una subred no será trasmitido por defecto, a otra subred. Los enrutadores, o los dispositivos de capa-3, proporcionan esta función de límite de difusión. Cada uno de estas subredes requiere un número de red único. Y para moverse a partir de un número de red a otro, se necesita un enrutador. En este caso de dominios de difusión y de conmutadores, cada uno de estos dominios de difusión separados es una VLAN separada; y por lo tanto, se necesita una función de enrutamiento.

Los computadores en VLANs diferentes no pueden comunicarse uno con el otro a menos que la red se configure explícitamente para permitirlo. Si la red tiene un mapeo uno a uno entre subredes de IP y VLANs, los computadores en VLANs diferentes deben comunicarse mediante enrutamiento IP. En este caso, las listas de control de acceso (ACL) puede filtrar el tráfico entre VLANs.

En la Figura 2.1, se crea una VLAN con un enrutador y un conmutador. Existen tres dominios de difusión separados. El enrutador encamina el tráfico entre las VLAN mediante enrutamiento de Capa 3. [Froom]

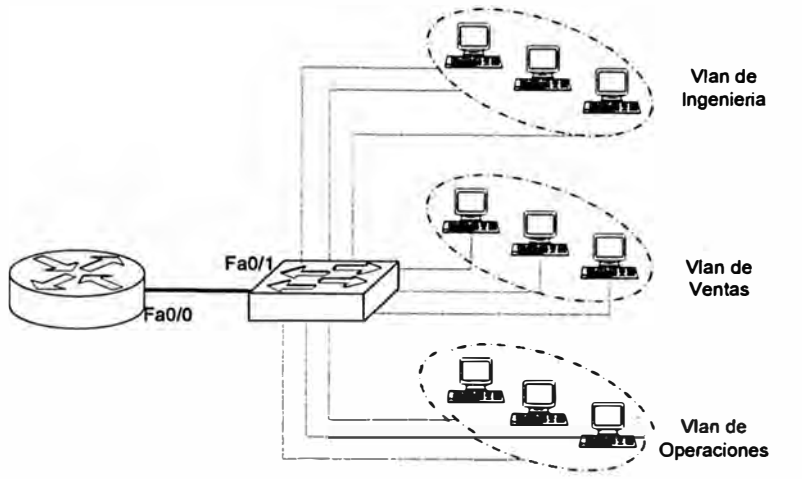


Fig. 2.1 Vlan y dominios de difusión

El conmutador en la Figura 2.1 envía tramas a las interfaces del enrutador cuando se presentan ciertas circunstancias:

- Si es una trama de difusión
- Si está en la ruta a una de las direcciones MAC del enrutador

La implementación de VLAN en un conmutador hace que se produzcan ciertas acciones:

- El conmutador mantiene una tabla de puenteo separada para cada VLAN.
- Si la trama entra en un puerto en la VLAN 1, el conmutador busca la tabla de puenteo para la VLAN 1.
- Cuando se recibe la trama, el conmutador agrega la dirección origen a la tabla de puenteo si es desconocida en el momento.
- Se verifica el destino para que se pueda tomar una decisión de envío.
- Para aprender y enviar se realiza la búsqueda en la tabla de direcciones para esa VLAN solamente.

2.2 Operación de las VLAN

Una VLAN se compone de una red conmutada que se encuentra lógicamente segmentada. Cada puerto del conmutador se puede asignar a una VLAN. Los puertos asignados a la misma VLAN comparten los mensajes de difusión. Los puertos que no

pertenecen a esa VLAN no comparten esos mensajes de difusión. Esto mejora el desempeño de la red porque se reducen los mensajes de difusión innecesarios.

Las VLAN de asociación estática se denominan VLAN de asociación de puerto central y basadas en puerto. Cuando un dispositivo entra a la red, da por sentado automáticamente que la VLAN está asociada con el puerto al que se conecta.

La VLAN por defecto para cada puerto del conmutador es la VLAN de administración. La VLAN de administración siempre es la VLAN 1 y no se puede borrar. Por lo menos un puerto debe asignarse a la VLAN 1 para poder gestionar el conmutador. Todos los demás puertos en el conmutador pueden reasignarse a VLAN alternadas.

Las VLAN de asociación dinámica son creadas mediante software de administración de red. Si utilizamos conmutadores Cisco se usa *CiscoWorks 2000* o *CiscoWorks for Switched Internetworks* para crear las VLAN dinámicas. Las VLAN dinámicas permiten la asociación basada en la dirección MAC del dispositivo conectado al puerto del conmutador. Cuando un dispositivo entra a la red, el conmutador al que está conectado consulta una base de datos en el Servidor de Configuración de VLAN para la asociación de VLAN.

En la asociación de VLAN de puerto central basada en puerto, el puerto se asigna a una asociación de VLAN específica independiente del usuario o sistema conectado al puerto.

2.3 Tipos de VLAN

Las VLAN pueden ser clasificadas en una variedad de maneras. Las VLAN se clasifican como locales (geográfico) o de extremo a extremo (campus). Alternativamente, las VLAN se clasifican como o basadas en puerto (estáticas) o dinámico.

El número de VLANs en un conjunto de conmutadores puede variar mucho, dependiendo de varios factores. Esto incluye los patrones de tráfico, los tipos de aplicaciones, necesidades de administración de la red y grupos comunes. Además, un factor importante a definir el tamaño del conjunto de conmutadores y el número de VLANs en el esquema de direccionamiento IP.

Adicionalmente es recomendable que las VLANs no debieran extenderse fuera del dominio de Capa 2 del conmutador de la capa de distribución. Con muchos usuarios

esparcidos a través de tres departamentos en un edificio, cuatro VLANs se requeriría bajo las limitaciones recomendadas.

Al dimensionar las VLANs en el conjunto de conmutadores, hay dos métodos básicos de definir los límites de VLAN:

- VLANs de extremo a extremo
- VLANs locales

2.3.1 VLANs de extremo a extremo

Las VLANs pueden existir o como redes de extremo a extremo (campus) o pueden existir dentro de un área geográfico limitado (local).

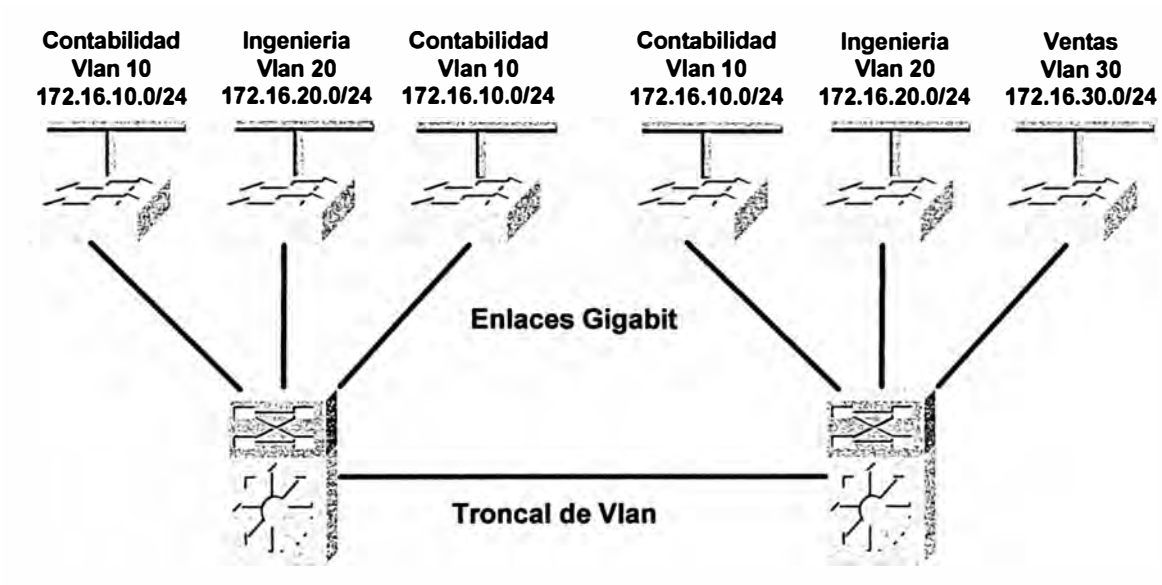


Figura 2.2 Vlan de extremo a extremo

Una VLAN de extremo a extremo comprende las características siguientes:

- Los Usuarios son agrupados en las VLANs independiente de la ubicación física y dependiente de la función del grupo o trabajo.
- Todos usuarios en un VLAN deben tener los mismos patrones de flujo de tráfico 80/20.
- Si un usuario se mueve en la red de campus, la asociación de VLAN para ese usuario no debe cambiar.

- Cada VLAN tiene un conjunto común de requisitos de seguridad para todos miembros.

Los enlaces de *backbone* en una LAN conmutada deben ser más rápidos que los enlaces del nivel de acceso. Cada conmutador llega a ser finalmente un miembro de todas las VLANs. Fast Ethernet *Inter-Switch Link* (ISL) o IEEE 802.1Q se utiliza para llevar información de múltiples VLAN entre los armarios de cableado y los conmutadores de la capa de distribución.

En el núcleo, un enrutador permite la comunicación de entre subredes. La red diseñada, es basada en patrones de flujo de tráfico, para tener el 80 por ciento del tráfico dentro de la VLAN y el 20 por ciento que cruzan el router hacia los Servidores de la empresa, al Internet y la WAN. VLANs de punta a punta permite dispositivos para ser agrupados basado sobre el uso del recurso. Esto incluye parámetros tales como el uso del Servidor, los equipos de proyecto y los departamentos. El objetivo de las VLANs de extremo a extremo es mantener el 80 por ciento del tráfico en el VLAN local.

Cuando las redes corporativas mueven a centralizar sus recursos, las VLANs de extremo a extremo se hacen difíciles de mantener. Los usuarios requieren utilizar muchos recursos diferentes, muchos de los cuales no están en "su" VLAN. A causa de este cambio en la colocación y el uso de recursos, las VLANs son ahora creadas con frecuencia alrededor de los límites geográficos (local).

2.3.2 VLANs Locales

El modelo de VLAN Local tiene VLANs dedicados para cada conmutador de la capa de acceso, con la conmutación de Capa 3 entre armarios de cableado realizado en la capa de distribución.

En el modelo de VLAN Local, los usuarios del mismo departamento están en la misma VLAN sólo si sus conmutadores de capa de acceso son conectados al mismo conmutador de la capa de distribución. Si el conmutador de capa de acceso es conectado a un conmutador diferente de la capa de distribución, los usuarios son asignados una VLAN diferente, en una dirección de subred diferente, a pesar de ser usuarios del mismo departamento.

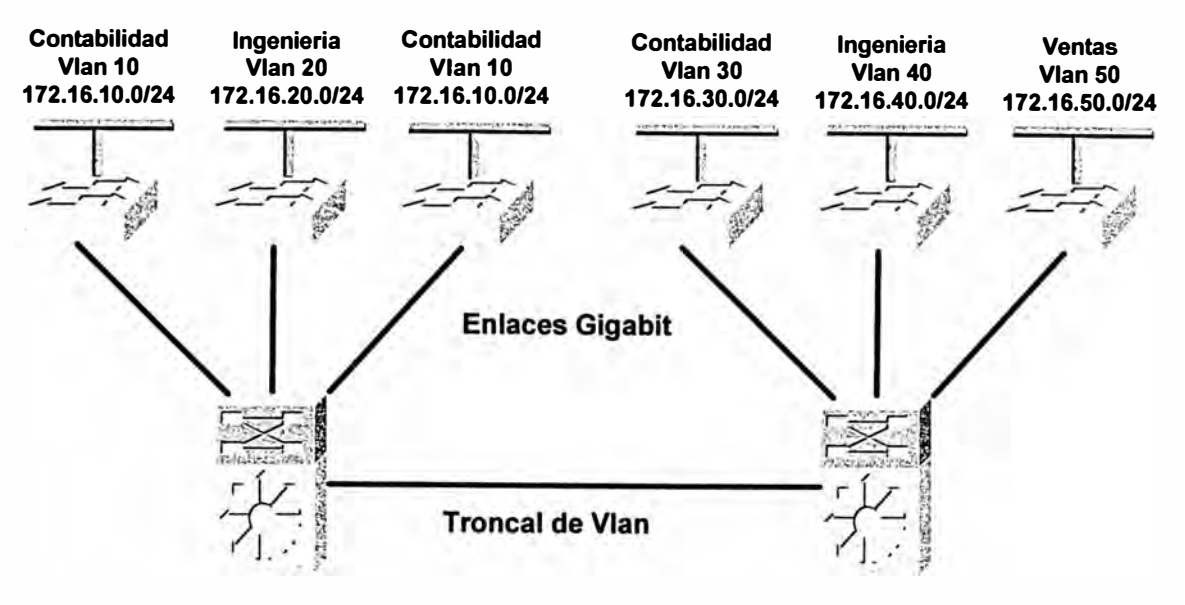


Figura 2.3 Vlan locales

VLANs geográficas son también considerablemente más fáciles de administrar y entender que las VLANs que atraviesan áreas geográficas diferentes.

2.3.3 Asociación de VLAN basadas en puerto

En las VLAN basadas en puerto, el puerto es asignado a una VLAN específica independiente del usuario o el sistema conectado al puerto. El administrador de la red realiza típicamente la tarea de asignar la VLAN. La configuración del puerto está estática y no puede ser cambiada automáticamente a otro VLAN sin una reconfiguración manual.

Después que un puerto ha sido asignado a una VLAN, el puerto no puede enviar ni recibir de dispositivos en otra VLAN sin la intervención de un dispositivo de Capa 3.

El dispositivo que es conectado a un puerto no tiene idea que existe una VLAN. El dispositivo sabe simplemente que es miembro de una subred y que debe ser capaz de comunicarse con todos los otros miembros de la subred simplemente enviando información al segmento de cable.

El conmutador es responsable de identificar la información que vino desde una VLAN específica y asegurar que la información llega a todos los otros miembros de la VLAN. El conmutador es también responsable de asegurar que puertos en una VLAN diferente no reciban la información.

Este enfoque es bastante sencillo, rápido, y fácil de manejar en el que no hay tablas de consulta complejas requeridas para la segmentación de VLAN. Si la VLAN basadas en asociación de puerto se hacen con un circuito integrado de aplicación-específica (ASIC), el desempeño es muy bueno. Un ASIC permite realizar el mapeo de puerto a VLAN en el nivel de *hardware*.

2.3.4 VLANs Dinámicas

Con un Servidor de Políticas de Administración de VLAN (VMPS), los puertos pueden ser asignados a las VLANs dinámicamente, basado en la información ingresada en la base de datos de VMPS. Cuándo un host se mueve de un puerto en un conmutador en la red a un puerto en otro conmutador en la red, el conmutador asigna dinámicamente el nuevo puerto a la VLAN apropiada para ese host.

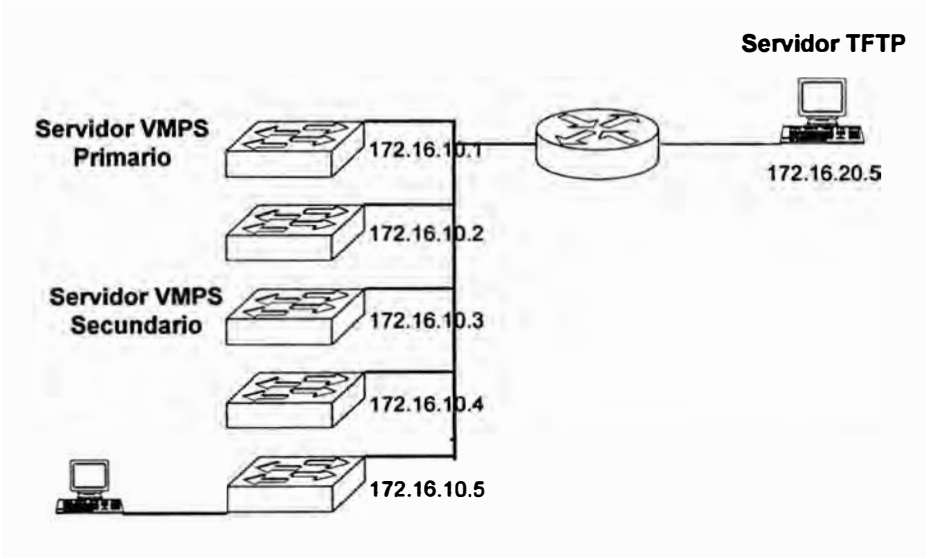


Fig. 2.4 VLAN dinámicas

Cuándo VMPS se habilita, una base de datos de mapeo ***MAC_address-VLAN*** se descarga desde un Servidor TFTP y VMPS comienzan a aceptar los pedidos de los clientes. Si el conmutador es reiniciado, la base de datos de VMPS se descarga del Servidor TFTP automáticamente y VMPS es rehabilitado.

VMPS abre una conexión usando el Protocolo de Datagrama de Usuario (UDP) para comunicarse y escuchar los pedidos del cliente. Cuándo el servidor VMPS recibe un pedido válido de un cliente, busca en su base de datos de mapeo ***MAC_address- VLAN.***

Las siguientes pautas y restricciones se aplican en la asociación dinámica de puertos a VLAN:

- VMPS se debe configurar antes los puertos puedan ser configurados como dinámicos.
- Cuándo un puerto se configura como dinámico, el spanning tree *PortFast* es habilitado automáticamente para ese puerto.
- Si un puerto se convierte de estático a dinámico en la misma VLAN, el puerto se conecta inmediatamente a esa VLAN, pero VMPS verificará finalmente la legalidad del computador en el puerto.
- Los puertos seguros estáticos no pueden convertirse a puertos dinámicos a menos que la seguridad se inhabilite antes de hacerlo puerto dinámico.
- Los puertos estáticos que son troncales no pueden convertirse en puertos dinámicos a menos que el *Trunking* se inhabilite en el puerto antes de cambiarlo de estático a dinámico.

2.4 Ventajas de las VLAN

Las VLAN permiten que los administradores de red organicen las LAN de forma lógica en lugar de física. Ésta es una ventaja clave. Esto permite que los administradores de red realicen varias tareas:

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad

Cuándo las VLANs son implementadas con dispositivos de red conmutados, otro nivel de protección se añade a la red. Los conmutadores puentean el tráfico dentro de un VLAN. Cuándo una estación transmite, la trama va al host destino. Tan pronto como se conoce que es un trama unicast conocida, el conmutador no distribuye la trama a todos los usuarios en la VLAN.

Las listas del acceso a veces son implementadas por cuestiones de seguridad, y ellas también son utilizadas para prevenir el flujo de tráfico a un segmento y así resguardar el ancho de banda.

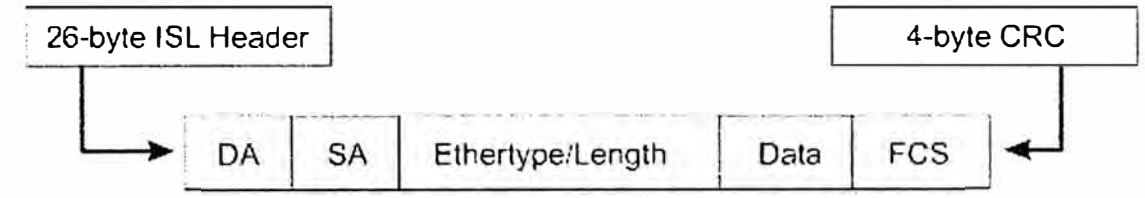
2.5 Protocolos

La identificación de VLAN permite reconocer lógicamente que paquetes pertenecen a que grupo de VLAN. Existen múltiples métodos de *Trunking*:

- Inter-Switch Link (ISL)
- IEEE 802.1Q
- IEEE 802.10
- ATM LAN *Emulation* (LANE)

2.5.1 Inter-Switch Link

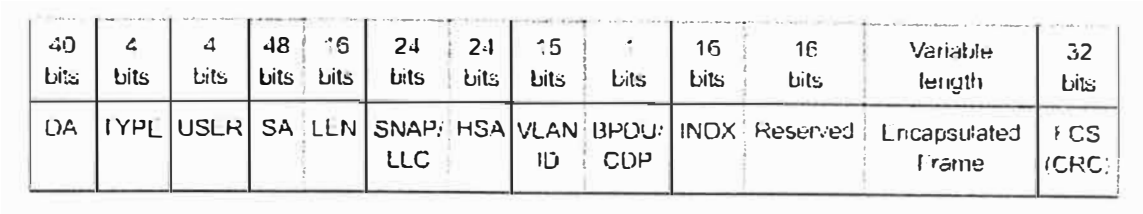
Inter-Switch Link (ISL) es un protocolo propietario de Cisco usado para interconectar múltiples conmutadores y para mantener la información de las VLAN como el tráfico que viaja entre los conmutadores en enlaces troncales. Esta tecnología proporciona un método para multiplexar los grupos del puente (VLANs) sobre un *backbone* de alta velocidad. Se define para Fast Ethernet, Gigabit Ethernet, al igual que IEEE 802.1Q. ISL ha estado disponible en los routers Cisco desde el IOS Cisco revisión 11.1. [Odom]



DA = Destination Address
SA = Source Address
FCS = Frame Check Sequence

Fig. 2.5 Trama ISL

Con el ISL, una trama Ethernet se encapsula con un encabezado que transporta las identificaciones de VLAN entre los conmutadores y los routers. ISL agrega al paquete un encabezado de 26-byte que contiene una identificación de VLAN de 10-bit. Además, un CRC de 4-byte se añade al final de cada trama. Los campos en el encabezado ISL identifican a que VLAN particular pertenece la trama.



40 bits	4 bits	4 bits	48 bits	16 bits	24 bits	24 bits	15 bits	1 bits	16 bits	16 bits	Variable length	32 bits
DA	TYPE	USER	SA	LEN	SNAP/ LLC	HSA	VLAN ID	BPDU/ CDP	INDX	Reserved	Encapsulated Frame	FCS (CRC)

Fig. 2.6 Campos en el encabezado ISL

Una identificación de VLAN se agrega solamente si la trama se envía a un puerto configurado como enlace troncal. Si la trama será enviada a un puerto configurado como enlace de acceso, se quita el encapsulado ISL.

2.5.2 El protocolo de IEEE 802.1Q

El nombre oficial para el protocolo de IEEE 802.1Q es el estándar para Redes Virtuales conmutadas de Area Local y se relaciona con la capacidad de llevar el tráfico de más de una subred bajo un solo cable. El comité de IEEE 802.1Q definió este método de multiplexado de VLANs en un esfuerzo de proporcionar soporte de VLAN a diferentes vendedores.

Tanto el etiquetado ISL como IEEE 802.1Q realizan etiquetado explícito, esto significa que la trama es etiquetada con información de VLAN explícitamente. Sin embargo, mientras ISL utiliza un proceso externo de etiquetado que no modifica la trama existente de Ethernet, IEEE 802.1Q utiliza un proceso interno de etiquetado que modifica la trama de Ethernet. Este proceso interno de etiquetado es lo que permite a IEEE 802.1Q trabajar en ambos enlaces de acceso y como troncales, porque las tramas parecen ser una trama estándar de Ethernet.

El esquema de la trama etiquetada IEEE 802.1Q tiene también apreciablemente menos sobrecarga que el etiquetado ISL. En comparación con los 30 bytes agregados por ISL, 802.1Q agrega sólo 4 bytes en la trama Ethernet.

Recordemos que, una trama Ethernet tiene como máximo 1518 bytes, al agregarse el etiquetado de 4 bytes. Se crea un nuevo CRC para la trama modificada.

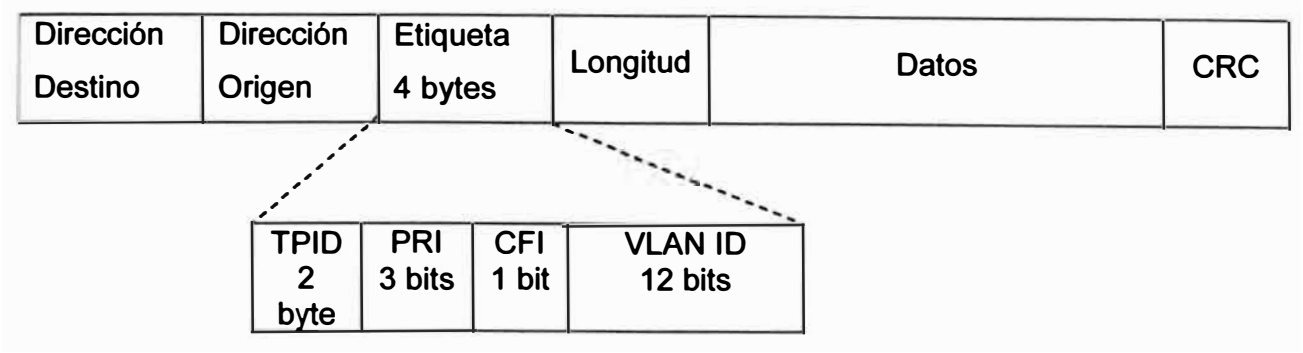


Fig. 2.7 Trama IEEE 802.1q

El encabezado IEEE 802.1Q contiene lo siguiente:

- Una etiqueta de 4 bytes que contiene una etiqueta de identificación de protocolo (TPID) y una etiqueta de información de control (TCI).

La TPID de 2 byte con un valor fijo de 0x8100 que indica que la trama lleva la información de etiqueta 802.1Q/802.1p.

La TCI contiene los elementos siguientes:

- Tres bits de prioridad de usuario.
- Un bit indicador canónico de formato (CFI). Configurado en 0 (cero) para conmutadores Ethernet y en 1 (uno) para redes Token Ring.
- Doce Bits de identificación de VLAN (VID) único que identifica la VLAN a la que la trama pertenece. De las 4096 posibles VLAN IDs, el numero máximo de VLAN configurables es 4094. La VLAN ID 0 es usado para indicar prioridad de tramas y el 4095 esta reservada.

El estándar 802.1Q puede crear un panorama interesante en la red. Recordemos que el tamaño máximo para una trama de Ethernet según lo especificado por IEEE 802,3 son 1518 bytes, esto significa que si una trama máxima de Ethernet es etiquetada, el tamaño de la trama será 1522 bytes, un número que viola el estándar IEEE 802,3. Para resolver este asunto, el comité 802,3 creó un subgrupo llamado 802.3ac para extender el tamaño máximo de Ethernet a 1522 bytes.

2.5.3 El protocolo IEEE 802.10

Este estándar fue originalmente establecido para direccionar las LAN dentro de las VLAN tomando el formato de cabecera de la trama y evitando el transporte de la trama etiquetada.

Las VLANs se puede multiplexar a través de un enlace principal de FDDI que soporte el protocolo IEEE 802,10.

Interfases FDDI que soportan IEEE 802,10 toman decisiones de envió selectivas dentro de un dominio de red basado en una identificación de VLAN. Esta identificación de VLAN son 4 byte IEEE 802,10 de usuario-configurable, *Security Association Identifier* (SAID).

El SAID identifica el tráfico que pertenece a una VLAN en particular.

2.5.4 ATM LAN Emulation (LANE)

La Emulación de Lan ATM (LANE) es un estándar definido por el Foro de ATM que permite que dos estaciones conectadas vía ATM tengan las mismas capacidades que ellos tendrían normalmente en una Lan, tal como Ethernet y Token Ring. Como su nombre sugiere, la función del protocolo LANE deberá emular una Lan en una red de ATM. Específicamente, el protocolo de LANE define mecanismos para emular una Lan IEEE 802,3 Ethernet o una Lan 802,5 Token Ring.

2.6 VLAN Trunking Protocol (VTP)

El rol del Protocolo de VLAN Trunking (VTP) es mantener la consistencia de configuración de VLANs a través de toda la red. VTP es un protocolo de mensajería que utiliza las tramas de las troncales de capa 2 para manejar la adición, la eliminación, y renombrado de VLANs en una red base desde un conmutador centralizado que está en el modo de servidor VTP. VTP es responsable de la sincronización de la información de VLAN dentro de un dominio VTP. Esto reduce la necesidad de configurar la misma información de VLAN en cada conmutador.

VTP minimiza las posibles inconsistencias de configuración que surgen cuándo se hacen cambios. Estas inconsistencias pueden tener como resultado fallas en la seguridad. VTP proporciona un esquema de mapas que permite que la troncal continué dentro de una red que emplea tecnologías mixtas.

VTP proporciona los siguientes beneficios:

- Consistencia de configuración de VLAN a través de la red
- Esquema mapas que permite a una VLAN ser troncal sobre medios mixtos.
- Rastreo y control exactos de las VLANs
- Cobertura Dinámica de la adición de VLANs a través de la red
- Configuración "*plug-and-play*" cuando se agregan VLANs nuevas.

Usando VTP, cada conmutador de la Familia Catalyst de Cisco anuncia en sus puertos troncales lo siguiente:

- El dominio de Administración.
- El número de revisión de configuración.
- VLANs conocidas y sus parámetros específicos.

2.6.1 Operación de VTP

Un dominio VTP se compone de uno o más dispositivos interconectados que comparten el mismo nombre del dominio VTP. Un conmutador se puede configurar para estar sólo en un dominio VTP. La información global de VLAN es propagada a través de la red por los puertos troncales conectados del conmutador.

Al transmitir los mensajes de VTP a otros conmutadores en la red, el mensaje de VTP se encapsula en una trama de protocolo de troncal tal como ISL o IEEE 802.1Q. El encabezamiento de VTP varía, dependiendo del tipo del mensaje de VTP, pero generalmente, cuatro ítems se encuentran en todos mensajes de VTP:

- **La versión de protocolo de VTP** – Versión 1 o 2
- **Tipo de mensaje VTP** – Indica uno de cuatro tipos
- **La longitud del nombre del dominio de Administración** – Indica el tamaño del nombre que sigue
- **El nombre del dominio de Administración** – El nombre configurado para el dominio de administración

Modos VTP

Los conmutadores pueden operar en cualquiera de uno de los siguiente tres modos de VTP: servidor, cliente, o transparente.

Servidor

Por omisión, un conmutador Catalyst está en el modo de servidor de VTP y en el estado del "sin dominio de administración" hasta que el conmutador reciba un anuncio para un dominio sobre un enlace troncal o el dominio de administración de la VLAN sea configurado. Un conmutador que esta en el modo de servidor VTP y tiene un nombre de dominio especificado puede crear, modificar y borrar VLANs.

Los servidores VTP pueden también especificar otros parámetros de configuración tales como la versión de VTP y poda de VTP para el dominio entero de VTP. La información de VTP se almacena en la NVRAM.

Los servidores VTP anuncian su configuración de VLAN a otros conmutadores en el mismo dominio de VTP y sincronizan la configuración de VLAN con otros conmutadores basados en anuncios recibidos sobre los enlaces troncales. Cuándo un cambio es hecho a la configuración de VLAN en un servidor VTP, el cambio es propagado a todos los conmutadores en el dominio VTP.

Los anuncios de VTP se transmiten a todas las conexiones troncales, inclusive ISL, IEEE 802.1Q, IEEE 802,10 y troncales ATM LANE.

Cliente

El cliente VTP mantiene una lista llena de todo VLANs dentro del dominio de VTP, pero no almacena la información en NVRAM. Los clientes de VTP se comportan igual que los servidores VTP, pero no pueden crear, cambiar, ni borrar VLANs. Cualquiera cambio hecho debe ser recibido de un anuncio del servidor VTP.

Transparente

Conmutadores VTP transparente no toman parte en VTP. Un conmutador VTP transparente no anuncia su configuración de VLAN, y no sincroniza su configuración de VLAN basada en anuncios recibidos.

Las VLANs se puede configurar en un conmutador en el modo transparente VTP, pero la información es local al conmutador (la información de VLAN no es propagada a otros conmutadores) y es almacenado en la NVRAM.

Anuncios de VTP

Los anuncios periódicos de VTP se envían a cada puerto troncal con la dirección MAC destino multicast de 01-00-0C-CC-CC-CC. Los anuncios de VTP contienen la información de configuración siguiente:

- Identificaciones de VLAN (ISL y 802.1Q)
- Nombres de LAN Emuladas (ATM LANE)
- Valores SAID 802.10 (FDDI)
- Nombre del dominio VTP
- Numero de revisión de configuración VTP
- Configuración de VLAN, incluyendo el tamaño de la unidad máxima de transmisión (MTU) para cada VLAN.
- Formato de trama

CAPITULO III

CONFIGURACIÓN DE VLANS EN CONMUTADORES CISCO

Configurar VLANs es realmente bastante fácil. Saber que usuarios estarán en cada VLAN no lo es. Esto puede tomar algo de tiempo, pero una vez que se ha decidido el número de VLANs que se quiere crear, y establecido a los usuarios que se quiere pertenezcan a una VLAN. La creación de VLANs en un conmutador es una tarea muy directa y sencilla.

Cada conmutador Cisco viene con una configuración predefinida. Por ejemplo hay ya algunas VLANs preconfiguradas, como la VLAN 1. La VLAN 1 es llamada a veces la VLAN de administración.

3.1 Configurando VLANs estáticas

VLANs estáticas son puertos en un conmutador que son asignados manualmente a una VLAN utilizando una aplicación de administración de VLAN o trabajando directamente dentro del conmutador. Estos puertos mantienen su configuración asignada a la VLAN hasta que un administrador los cambie. Aunque las VLANs estáticas requieren ingresar los cambios manuales, ellas son seguras, fáciles de configurar, y administrar.

Este tipo de VLAN trabaja de bien en las redes donde los movimientos son administrados y controlados. Es también apropiado para las redes que emplean un software robusto de administración de VLAN para configurar los puertos.

Hay realmente dos métodos que pueden utilizarse para crear VLAN. El método antiguo requiere entrar a la base de datos de VLAN y crear la VLAN, de esta manera:

```
2950# vlan database
2950(vlan)# vlan VLAN # [name VLAN_name]
```

Desde la IOS 12.1 (9) EA1 y posteriores, se puede utilizar esta configuración:

```
2950(config)# vlan VLAN_#
2950(config-vlan)# name VLAN_name
```

Cuándo se ejecuta la orden **vlan,** se ingresa al modo de Sub-Configuración de VLAN, donde se pueden ingresar parámetros para la configuración de las VLAN, tales como el nombre de la VLAN.

Una vez que se ha creado la VLAN, se necesita asignar las interfases a la VLAN.
El comando **switchport mode** se puede utilizar para configurar la interfase como acceso, dinámico o troncal.

```
2950(config-if)#switchport mode [access | dynamic | trunk]
```

Para asociar estáticamente una interfase con una VLAN, utilice las siguientes órdenes:

```
2950(config-if)#switchport mode access
2950(config-if)#switchport access vlan number
```

Por ejemplo veamos como configurar VLANs en el conmutador 2950 creando tres VLANs para tres departamentos diferentes.

Ingresamos al modo de Base de datos de Vlan.

```
2950#vlan database
2950(vlan)#
```

Ingresamos los comandos de configuración, uno por línea.

```
2950 (vlan)#vlan 2
2950 (vlan)#name Informatica
```

En este momento, le damos un nombre a la VLAN. Creemos una pareja más VLANs y entonces verifiquemos nuestros cambios.

```
2950(vlan)#vlan 3
```

```
2950(vlan)#name Ventas
2950(vlan)#vlan 4
2950(vlan)#name Finanzas
2950(vlan)#exit
2950#
```

Ahora asignamos la interfase 2 a la VLAN 2, la interfase 3 a la VLAN 3, y la interfase 4 a la VLAN 4:

```
2950(config-if)#int f0/2
2950(config-if)#switchport access vlan 2
2950(config-if)#int f0/3
2950(config-if)#switchport access vlan 3
2950(config-if)#int f0/4
2950(config-if)#switchport access vlan 4
2950(config-if)#
```

Los conmutadores 2950 y 3550 tienen un comando **interface range** que permite identificar un rango de interfases para una operación subsiguiente. Por ejemplo, varios puertos pueden ser asignados a un VLAN con un comando **switchport**.

```
2950(config)#interface range fa0/1 - 6
2950(config-if-range)#switchport access vlan 10
```

Este comando asignará los puertos 1 al 6 a la **vlan 10** en una sola línea de comandos.

3.1.1 Verificación de la configuración de VLAN

Una vez que en el conmutador se ha creado VLANs y se asociado los puertos a las VLANs, se pueden utilizar comando **show** para revisar y verificar la configuración, el comando **show vlan brief,** nos mostrará la información acerca de las VLANs creadas y los puertos asociados a estas.

```
2950#sh vlan brief
```

```
VLAN       Name              Status     Ports
---- -------------------- --------- -------------------------------
1       default             active     Fa0/1, Fa0/5, Fa0/6, Fa0/7,
                                       Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                       Fa0/12
2     Informatica           active     Fa0/2
3     Ventas                active     Fa0/3
4     Finanzas              active     Fa0/4

1002  fddi-default          active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active
```

Al configurar VLANs, hay que tener presente que:

- Una VLAN creada permanece sin uso hasta que no se le asigne los puertos.
- La configuración predefinida tiene todos los puertos del conmutador en la VLAN 1.

3.1.2 Eliminando VLANs

Se inicia en el modo de EXEC privilegiado, se ingresa a la base de datos de VLAN y se usa la forma no del comando.

A continuación se muestra el comando que se utiliza para eliminar una VLAN de un conmutador:

```
2950#
2950#vlan database
2950(vlan)#no vlan 2
```

Cuando se elimina una VLAN, todos los puertos asignados a esa VLAN quedan inactivos. Los puertos, sin embargo, quedan asociados a la VLAN eliminada hasta que se los asigna a una nueva VLAN.

Cuándo una VLAN se borra de un conmutador que está en modo servidor VTP (VLAN Trunking Protocol), la VLAN se borra de todos los conmutadores en el dominio de VTP.

Cuándo una VLAN se borra de un conmutador que está en el modo VTP transparente, la VLAN se borra sólo en ese conmutador específico.

Una VLAN no se puede borrar de un conmutador que está en el modo de cliente VTP.

3.2 Configuración de enlaces troncales

Cuándo se trabaja con VLANs, los conmutadores soportan dos tipos de conexiones: los enlaces de acceso y los troncales. [Lammle]

Enlaces de Acceso y enlaces troncales

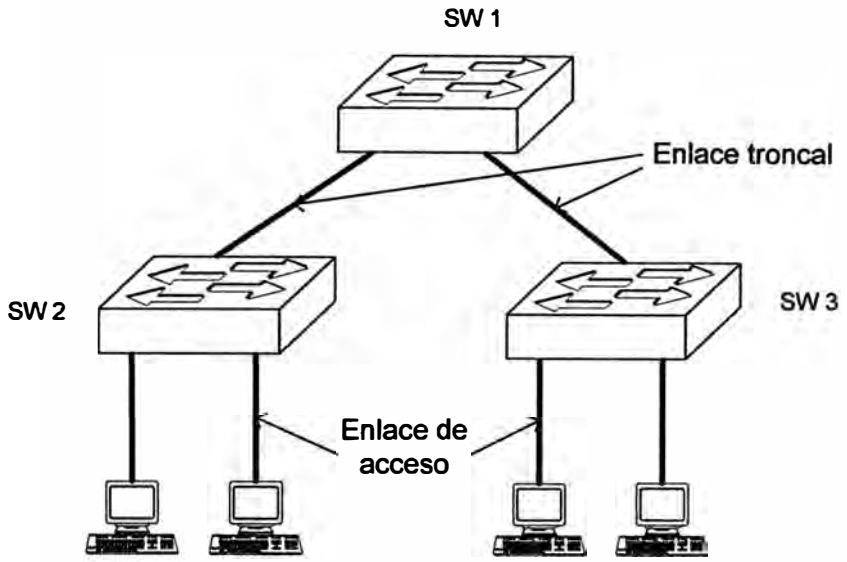


Fig. 3.1 Enlaces troncales

Un puerto de acceso es un puerto del conmutador que conecta a un dispositivo de usuario final o un servidor; las tramas transmitidas en un enlace de acceso se parecen a cualquier otra trama de Ethernet.

Un enlace troncal se diferencia de un enlace de acceso en que es capaz de soportar múltiples VLANs.

Las VLANs son multiplexadas sobre el enlace con un protocolo de *trunking*. El enlace troncal no pertenece a una VLAN específica. Los enlaces troncales se utilizan típicamente para conectar conmutadores a otros conmutadores, a los routers, o a un servidor que tiene una tarjeta de la red de IEEE 802.1q habilitado para tomar parte en múltiples VLANs.

Las troncales pueden extender las VLANs a través de una red entera. Un troncal se puede configurar para transportar todas las VLANs o un conjunto restringido de VLANs.

Las troncales se configuran típicamente en los puertos que soportan el ancho de banda más grande para un conmutador dado. Los conmutadores Catalyst soportan los enlaces troncales en Fast Ethernet, en Gigabit Ethernet, y en puertos 10 Gigabits Ethernet.

Sin enlaces troncales, múltiples enlaces de acceso se tendrían que instalar para sostener múltiples VLANs entre conmutadores (una conexión por VLAN).

Esto es claramente ni una solución rentable ni escalable. ***Trunking*** es absolutamente esencial para interconectar conmutadores en una red de *campus.*

En un conmutador 2950 se usa el comando switchport:

Primero ingresamos al modo de interfase y luego lo configuramos como troncal

```
2950 #config t
2950(config)# interface int f0/12
2950(config-if)#switchport mode trunk
2950(config-if)#^Z
2950 #
```

Para deshabilitar la troncal en la interfase, use el comando ***switchport mode access***.

3.3 Enrutamiento entre VLANs

Configurar LANs virtuales (VLANs) ayuda a controlar el tamaño de los dominios de broadcast y mantener de manera local el tráfico. La desventaja a este beneficio es que dispositivos (hosts) en VLANs diferentes son incapaces de comunicarse sin la presencia de alguna manera de enrutamiento de capa 3.

Para proporcionar enrutamiento entre VLANs, tres componentes claves deben estar presentes. Estos son un conmutador con la capacidad de crear VLAN, un router y alguna forma de conectividad entre los dos.

El router puede ser una unidad autónoma externa o se puede integrar dentro del hardware del conmutador. Los nombres comunes usados para describir routers que se integran dentro del conmutador incluye: Módulo de enrutamiento del conmutador (RSM), Procesador de enrutamiento (RP), Módulo de Servicios de la Capa 3 o son referidos simplemente a como conmutador de Capa 3.

Si se emplea un router externo para realizar el enrutamiento Inter-VLAN, la conexión al conmutador puede ser vía una conexión Fast Ethernet separada para cada VLAN o puede ser utilizado una sola conexión de enlace troncal.

Para redes con apenas un par de VLANs, utilizar una interfaz física para cada VLAN puede ser una estrategia de enrutamiento Inter-VLAN viable. Sin embargo, para redes con más VLANs, una estrategia de enrutamiento que utiliza interfaces virtuales deber ser a lo que se llega.

Ambos router externo y router interno se pueden utilizar con subinterfaces. La diferencia entre las dos soluciones implica una compensación (compromiso) entre el costo y el desempeño.

Un router externo de nivel de entrada es generalmente más barato que un conmutador con funcionalidad de capa 3, pero la falta de integración entre los elementos de la capa 2 y 3 de la red y la naturaleza del tráfico "hacia" y "desde" los routers externos limitará el desempeño.

Una vez que la capacidad de 100 Mbps del enlace externo del router se excede, el uso de un procesador integrado de enrutamiento llega a ser la única opción práctica para proporcionar enrutamiento Inter-VLAN.

Sin importar la técnica de enrutamiento elegida, es esencial que los elementos de conmutación (conmutadores) de la capa de acceso y de distribución estén alineados con la funcionalidad de enrutamiento en la capa de la distribución. En especial, se debe tener cuidado para asegurarse que el conmutador de la capa distribución sea la raíz del Spanning Tree para cada VLAN que es enrutado por el router de la capa de distribución.

3.3.1 Tarjetas Cisco con característica de la capa 3

Aunque el desempeño de procesadores de enrutamiento (*route switch processors*) sea generalmente adecuado para aplicaciones típicas, hay circunstancias donde se requiere desempeño adicional. Las situaciones que pueden requerir el desempeño adicional de enrutamiento incluyen lo siguiente:

- Una alta proporción de tráfico necesita cruzar las fronteras de la VLAN.
- Una gran cantidad de interfaces están presentes y muchos son Gigabit o mayores en velocidad.
- La capacidad de conmutación adicional se ha proporcionado por la adición de un *Switch Fabric Module*.

Dos tarjetas con característica de capa 3 están disponibles para los conmutadores Catalyst 6000 son la *Multilayer Switch Feature Card* (MSFC) y la *Policy Feature Card* (PFC).

3.3.2 Configurando enrutamiento Inter-VLAN en una red conmutada

La primera tarea siempre debe ser activar la funcionalidad de enrutamiento IP en los conmutadores con el comando:

```
Switch (config)# ip routing
```

Lejos el método más común de lograr el enrutamiento Inter-VLAN es configurar la interfaz virtual en el conmutador. Utilizando esta técnica, el router tiene una interfase virtual en cada VLAN creado en el conmutador. En vez de configurar una interfaz física para cada VLAN, el router utiliza un interfaz virtual.

Por ejemplo, los siguientes comandos permitirán al router enrutar el tráfico hacia y desde la VLAN 10.

```
Switch (config)#interface vlan 10
Switch(config-if)#ip address 10.0.1.1 255.255.255.0
```

Estos comandos tienen el mismo efecto como si un interfaz físico del router fuera conectado a un puerto del conmutador en la VLAN apropiada.

3.3.3 Configurando enrutamiento Inter-VLAN vía un puerto enrutado

Aunque sea más común configurar enrutamiento Inter-VLAN utilizando la interfase virtual (VLAN), es también posible configurar un switchport físico como una interfase enrutada. Por este proceso, es posible cambiar un puerto 12 o 24 Ethernet conmutado a un puerto 12 o 24 Ethernet enrutado.

Para cambiar un switchport en una interfase enrutada, es simplemente el apagar la funcionalidad de switchport.

```
Switch (config)#interface fa 0/1
Switch(config-if)#no switchport
```

Una vez que la funcionalidad de Capa 2 se apagado, la interfase puede ser tratada como si fuera una interfase de un router. Por ejemplo una dirección IP puede ser especificado.

```
Switch (config-if)#ip address 172.16.1.1 255.255.255.0
```

El switchport o interfase ahora puede ser utilizado como un puerto físico de un router para la conexión a dispositivos externos.

3.3.4 Configurando enrutamiento Inter-VLAN en un Router con un enlace único

Para que el enrutamiento entre VLAN funcione correctamente, el routers y los conmutadores involucrados deben admitir el mismo encapsulamiento.

En un router, una interfaz se puede dividir lógicamente en varias subinterfaces virtuales. Las subinterfaces ofrecen una solución flexible para el enrutamiento de varias corrientes de datos a través de una interfaz física única. Para definir las subinterfaces en una interfaz física, realice las siguientes tareas:

- Identifique la interfaz.
- Defina el encapsulamiento de la VLAN.
- Asigne una dirección IP a la interfaz.

Para identificar la interfaz utilice el comando **interface** en el modo de configuración global.

Router(config)#**interface fastethernet** *port-number. subinterface-number*

port-number identifica la interfaz física y *subinterface-number* identifica la interfaz virtual.

El router debe poder comunicarse con el conmutador utilizando un protocolo de enlace troncal estandarizado. Esto significa que ambos dispositivos conectados entre sí deben comprenderse. En el ejemplo, se utiliza 802.1Q. Para definir el encapsulamiento de la VLAN, introduzca el comando **encapsulation** en el modo de configuración de interfaz.

Router(config-if)#**encapsulation dot1q** *vlan-number*

vlan-number identifica la VLAN para la cual la subinterfaz transportará el tráfico. Se agrega un ID de VLAN a la trama sólo cuando la trama está destinada a una red no local. Cada paquete de VLAN transporta el ID de VLAN dentro del encabezado del paquete.

Para asignar una dirección IP a la interfaz, introduzca el siguiente comando en el modo de configuración de interfaz.

Router(config-if)#**ip address** *ip-address subnet-mask*

ip-address y *subnet-mask* son las direcciones y la máscara de red de 32 bits de la interfaz específica.

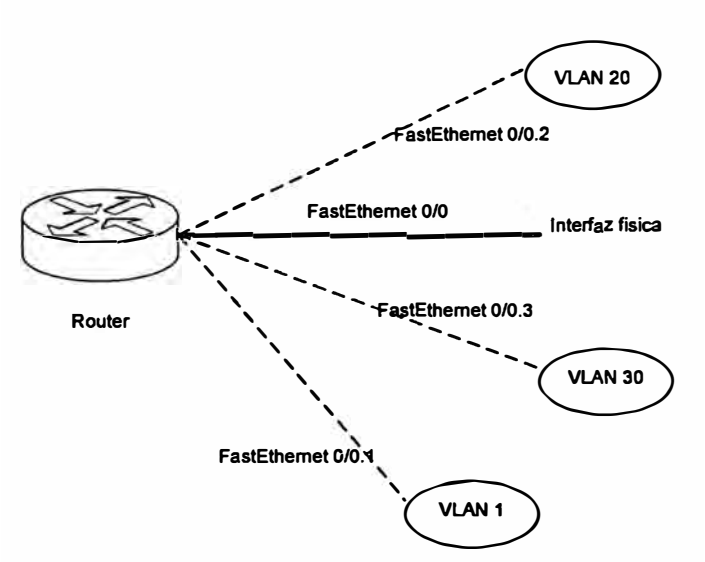


Fig. 3.2 Sub-interfases

En el ejemplo, el router tiene tres subinterfaces configuradas en la interfaz Fast Ethernet 0/0. Estas tres subinterfaces se identifican como 0/0.1, 0/0.2 y 0/0.3. Todas las interfaces se encapsulan para 802.1q. La interfaz 0/0.1 enruta paquetes para la VLAN 1, mientras que la interfaz 0/0.2 enruta paquetes para la VLAN 20 y la interfaz 0/0.3 enruta paquetes para la VLAN 30.

3.3.5 Configurando enrutamiento en un Servidor Linux como enrutador

Algunas organizaciones no pueden afrontar la adquisición de dispositivos de red como los enrutadores necesario para el enrutamiento entre VLANs. Una solución posible, a corto e incluso a largo plazo es convertir las computadoras de escritorio en enrutadores por la instalación totalmente gratis del software correspondiente y las tarjetas de red correspondientes.

Una alternativa para redes no muy grandes, es la de configurar un servidor Linux como enrutador. El servidor debe tener dos tarjetas de red configuradas.

Configuraciones de tarjetas en el router:

/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.2.33
NETMASK=255.255.255.0
NETWORK=192.168.2.0
BROADCAST=192.168.2.255
ONBOOT=yes
MII_NOT_SUPPORTED=no
USERCTL=yes
IPV6INIT=no
IPV6TO4INIT=no
PEERDNS=yes
NETMASK=255.255.255.0
IPADDR=192.168.2.33
```

/etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
IPADDR=192.168.1.33
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
MII_NOT_SUPPORTED=no
USERCTL=yes
IPV6INIT=no
IPV6TO4INIT=no
PEERDNS=yes
NETMASK=255.255.255.0
IPADDR=192.168.1.33
```

Una vez configuradas las tarjetas de red, pasamos a darle las instrucciones al Router para que enrute:

```
#/etc/init.d/network stop
#echo 1 > /proc/sys/net/ipv4/ip_forward
#/etc/init.d/network start
#iptables --append FORWARD --in-interface eth0 -j ACCEPT
#iptables --table nat --append POSTROUTING --out-interface eth1 -j
MASQUERADE
```

Esta configuración es viable, pero se ve algo complicado. Pero la configuración de enrutamiento se puede hacer más simple si instalamos **ZEBRA** sobre el servidor Linux.

ZEBRA es un paquete de software de enrutamiento que provee TCP/IP basado en los servicios de enrutamiento con varios protocolos soportados como pueden ser RIP, OSPF y BGP. Soporta además la posibilidad de implementar estos protocolos de enrutamiento con IPV4 o IPV6.

ZEBRA es un software que permite montar enrutadores sobre sistemas operativos tipo Unix. Este software dispone de una interfaz de configuración basada en el Cisco IOS, por lo que será útil a los administradores familiarizados con enrutadores Cisco.

Instalación de ZEBRA desde el código fuente

La instalación es la típica de cualquier paquete de código fuente. Descomprimimos, compilamos e instalamos el paquete:

```
tar xvfz zebra-0.93a.tar.gz
cd zebra-0.93a.tar.gz
./configure
make
su
make install
```

Daemons

ZEBRA instala cinco *daemons* que escuchan en puertos consecutivos. A continuación una tabla muestra cuales son los *daemons* y en que puertos escuchan:

Tabla 3.1 Demonios y puertos asociados

zebra	**2601 tcp**
ripd	**2602 tcp**
ripngd	**2603 tcp**
ospfd	**2604 tcp**
bgpd	**2605 tcp**

Archivos de configuración

Los archivos de configuración están en /usr/local/etc/. Con la instalación de las fuentes viene un archivo de ejemplo para cada uno de los *daemons*. Estos no son utilizados directamente por ZEBRA, hay que cambiarles el nombre. Son los siguientes:

Tabla 3.2 Ficheros de configuración

Nombre original	Fichero de configuración
zebra.conf.sample	zebra.conf
ripd.conf.sample	ripd.conf
ripngd.conf.sample	ripngd.conf
ospf.conf.sample	ospf.conf
bgpd.conf.sample	bgpd.conf

Configurando el router

Para realizar la configuración del enrutador se puede acceder directamente a cada uno de los protocolos (*daemons*) que utiliza ZEBRA. Simplemente haga un telnet al puerto que desee, por ejemplo, para configurar rip:

```
$ telnet localhost ripd
```

ZEBRA proporciona una herramienta que integra todos los protocolos/*daemons*. Esta herramienta es vtysh:

```
$ vtysh
Hello, this is Zebra (version 0.92a).
Copyright 1996-2001 Kunihiro Ishiguro
zebra>
```

Para quienes hemos configurado alguna vez un router Cisco esto nos resulta familiar.

Configuración básica

Accedemos al modo ***enable*** y empezamos con la configuración:

```
zebra>en
zebra#sh run
Building configuration
Current configuration
!!
zebra#
```

No hay configuración, por lo que reiniciaremos el demonio zebra para que vuelva a leerla, por ejemplo:

```
/etc/rc.d/init.d/zebra restart
```

Entramos de nuevo en zebra:

```
$ vtysh
Hello, this is Zebra (version 0.92a).
Copyright 1996-2001 Kunihiro Ishiguro
mypc>
mypc>en
mypc#sh run
Building configuration
Current configuration
!!i
nterace lo
!i
nterface eth0
!
mypc#
```

A partir de aquí la configuración es similar a la de un router Cisco. Hay cosas que son un poco diferentes, pero sabiendo configurar enrutadores Cisco y con unos conocimientos básicos de redes en Linux no se tendrá ningún problema.

CAPITULO IV

APLICACIÓN

La empresa ABC encargada de la recaudación de impuestos de un gobierno local, utiliza una LAN en la que tiene actualmente alrededor de 350 computadores personales, 15 impresoras Láser en red, 20 servidores, 30 conmutadores. Utilizan aplicaciones cliente/servidor. El sistema operativo de los Servidores es Windows 2000 Server y Windows 2003 Server, en las estaciones de trabajo se tiene Windows 98, Windows 2000 Profesional y Windows XP Profesional.

Además cuenta con cámaras IP, que monitorean algunas áreas de la empresa. Entre los Servidores cuenta con servidor de Correo, de paginas Web, de base de datos, de Intranet, la salida a Internet es a través de un servidor Proxy. Todos dentro de un solo Dominio de Difusión.

Los mensajes de difusión en exceso hacen que la red sea "lenta", se ha utilizado un analizador de protocolos y se ha confirmado que hay un exceso de mensajes de difusión. Además de existir un potencial problema de seguridad, ya que los usuarios de un área pueden acceder a los computadores de otra área.

Además la empresa cuenta con 4 oficinas descentralizadas con las cuales se tienen enlaces dedicados.

Se tienen implementados políticas de seguridad a las estaciones con Windows 98 que impide a los usuarios compartir sus recursos libremente. Los recursos se comparten con autorización de la Gerencia respectiva y por el personal de Soporte Técnico de la Gerencia de Informática.

Para mejorar la seguridad de acceso a los servidores Web, de correo etc., desde fuera de la red y desde la red interna se esta creando una DMZ.

La distribución de computadores en la empresa es como sigue:

Tabla 4.1 Distribución de computadores

Area	Cantidad de computadores
Jefatura	8
Gerencia de Administración	38
Gerencia de Asuntos Legales	23
Gerencia de Planeamiento	36
Gerencia de Operaciones	154
Gerencia de Informática	39
Sala de Servidores y Cámaras IP	30
Total	328

Para reducir el efecto negativo de los mensajes de difusión, se plantea. Crear VLANs de tal manera que los mensajes de difusión no se propaguen por toda la red.

En este trabajo se desarrollara la creación de VLANs.

Se plantea crear las siguientes VLAN:

VLAN 2, Jefatura, Ger. Administración y Asuntos Legales
VLAN 3, Ger. Operaciones
VLAN 4, Ger. Planeamiento, Ger. Informática y Cámaras IP.

VLAN 5, Sala de Servidores.

Elección de la dirección de red

Usaremos la dirección privada de clase B 172.16.0.0, la cual se dividirá en subredes.

Tabla 7.2 distribución de Vlan

VLAN	Nombre de la Vlan	Dirección de red
1	Vlan1	172.16.10.0 /24
2	Ger_Adm	172.16.11.0 /24
3	Operaciones	172.16.12.0 /24
4	Informática	172.16.13.0 /24
5	Servidores	172.16.14.0 /24

A continuación se tiene la configuración del Conmutador principal.

Configuración del Conmutador Principal

Configuración basica

```
Switch>enable
Switch# configure terminal
Switch (config)#hostname Principal
Principal (config)#int vlan 1
Principal (config-if)#ip add 172.16.10.1 255.255.255.0
Principal (config-if)# no shutdown
```

Configuración de Vlan

Utilizamos el protocolo VTP, para que la configuración de VLANs se replique en los demás conmutadores. Nombre de Dominio VTP **sat**, switch en modo vtp server.

```
Principal # vlan database
Principal (vlan) #vtp server
Principal (vlan) #vtp domain sat
```

```
Principal (vlan) #vlan 2 name Ger Adm
Principal (vlan) #vlan 3 name Operaciones
Principal (vlan) #vlan 4 name Informatica
Principal (vlan) #vlan 5 name Servidores
Principal (vlan) # exit
```

```
Exiting....
Principal#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14
2    ger_adm                           active
3    Operaciones                       active
4    Informatica                       active
5    Servidores                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Principal#
```

Fig. 4.1 Vlans creadas

Ahora asignamos puertos a las Vlans.

```
Principal (config) # int range fa0/7 -12
Principal (config-range) #switchport access vlan 4
Principal (config) # int range fa0/13 -24
Principal (config-range) # switchport access vlan 5
```

Los primeros puertos se dejan en la Vlan 1.

No se configuran puertos para la Vlan de operaciones, ni para la Vlan Ger_Adm.

Configuración del Switch de Operaciones

Configuración basica

```
Switch>enable
Switch# configure terminal
Switch (config) #hostname Opera_1
Opera_1 (config) # int vlan 1
Opera_1 (config-if) #ip add 172.16.10.2 255.255.255.0
Opera_1 (config-if) # no shutdown
```

Configuración de Vlan

El nombre del Dominio VTP es **sat**. Se configura en modo vtp client.

```
Opera_1 #vlan database
Opera_1 (vlan) # vtp client
Opera_1 (vlan) # vtp domain sat
Opera_1 (vlan) # exit
Opera_1 #
```

Hay que configurar los enlaces troncales.

```
Opera_1 (config) # int ga0/1
Opera_1 (config-if) # switchport mode trunk
```

Con las troncales configuradas y el switch como cliente VTP, la configuración de vlans se propaga a este switch. Podemos verificar la creación de las Vlans. Para ello utilizamos el comando Show Vlan.

Se configuran todos los enlaces troncales necesarios. Luego asignamos los puertos a las Vlan correspondientes. En este switch del área de Operaciones, la mayoría de los puertos pertenecen a la Vlan operaciones. Se deja por lo menos un puerto en la Vlan 1, se

reservan puertos para la vlan de informática, ya que en el área de Operaciones se tienen cámaras Ip instaladas.

```
Opera_1#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
2    ger_adm                           active
3    operaciones                       active
4    informatica                       active
5    servidores                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

Fig. 4.2 Vlans creadas en el switch de Operaciones

Por la cantidad de hosts en el área de Operaciones, se necesitara por lo menos 3 Switch de 48 puertos y 2 de 24 puertos, los cuales se denominaran; Opera_1, Opera_2, Opera_3, Opera_4, Opera_5.

La configuración de Vlan en cada switch es similar, es decir se configura el enlace troncal, se estable el dominio vtp **sat,** en modo vtp client.

La asignación de puertos en cada switch de 48 puertos, será de la siguiente manera:

Tabla 4.3 Asignación de puertos

Id. de Puerto	Cant. de puertos	Vlan Id.	Nombre de la Vlan
fa0/1 – fa0/2	2	1	Vlan 1
fa0/3 – fa0/6	4	4	Informatica
fa0/7 – fa0/48	42	3	Operaciones

Los dos puertos Gigabit se configuran como enlaces troncales.

Para lograr esto ingresamos los siguientes comandos:

```
Opera_1 (config) # int range fa0/3 -6
Opera_1 (config-range) #switchport access vlan 4
Opera_1 (config) # int range fa0/7 -48
Opera_1 (config-range) # switchport access vlan 3
```

Esta configuración la repetimos para los switches Opera_2, Opera_3, Opera_4 y Opera_5.

Para la Jefatura, Ger. Administración y Asunto Legales, necesitamos 1 switch de 48 puertos y 2 de 24 puertos. A los cuales denominaremos, Adm_1, Adm_2 y Adm_3.

La configuración de los switches será como sigue:

Configuración basica

```
Switch>enable
Switch# configure terminal
Switch (config)#hostname Adm_1
Adm 1 (config)#int vlan 1
Adm 1 (config-if)#ip add 172.16.10.7 255.255.255.0
Adm 1 (config-if)# no shutdown
```

Configuración de Vlan

El nombre del Dominio VTP es **sat**. Se configura en modo vtp client.

```
Adm 1 #vlan database
Adm 1 (vlan) # vtp client
Adm 1 (vlan) # vtp domain sat
Adm 1 (vlan) # exit
Adm 1 #
```

Hay que configurar los enlaces troncales.

```
Adm 1 (config) # int ga0/1
Adm 1 (config-if) # switchport mode trunk
```

Con las troncales configuradas y el switch como cliente VTP, la configuración de vlans se propaga a este switch.

Esta tarea se repite para los switches Adm_2 y Adm_3. Con la diferencia de asignar una dirección Ip distinta en la interface vlan 1, que es la que se utiliza para administrar el switch.

La asignación de puertos en el switch de 48 puertos, será de la siguiente manera:

Tabla 4.4 Asignación de puertos en el switch de Administración de 48 puertos

Id. de Puerto	Cant. de puertos	Vlan Id.	Nombre de la Vlan
fa0/1 – fa0/2	2	1	Vlan 1
fa0/3 – fa0/6	4	4	Informatica
fa0/7 – fa0/48	42	2	Ger_Adm

La asignación de puertos a las vlan en el switch de 24 puertos,

Tabla 4.5 Asignación de puertos en el switch de Administración de 24 puertos

Id. de Puerto	Cant. de puertos	Vlan Id.	Nombre de la Vlan
fa0/1 – fa0/2	2	1	Vlan 1
fa0/3 – fa0/4	2	4	Informatica
fa0/5 – fa0/24	20	2	Ger_Adm

Para Informatica, Planeamiento y cámaras Ip se necesita, 2 switches de 48 puertos. A los que denominaremos, Inform_1, Inform_2.

La configuración de los switches será como sigue:

Configuración basica

```
Switch>enable
```

```
Switch# configure terminal
Switch (config)#hostname Inform_1
Inform_1 (config)#int vlan 1
Inform_1 (config-if)#ip add 172.16.10.9  255.255.255.0
```

Configuración de Vlan

El nombre del Dominio VTP es **sat**. Se configura en modo vtp client.

```
Inform_1 #vlan database
Inform_1 (vlan) # vtp client
Inform_1 (vlan) # vtp domain sat
Inform_1 (vlan) # exit
Inform_1 #
```

Hay que configurar los enlaces troncales.

```
Inform_1 (config) # int ga0/1
Inform_1 (config-if) # switchport mode trunk
```

Con las troncales configuradas y el switch como cliente VTP, la configuración de vlans se propaga a este switch.

La asignación de puertos en el switch de 48 puertos, será de la siguiente manera:

Tabla 4.6 Asignación de puertos del switch de Informatica

Id. de Puerto	Cant. de puertos	Vlan Id.	Nombre de la Vlan
fa0/1 – fa0/2	2	1	Vlan 1
fa0/3 – fa0/4	2	2	Ger_Adm
fa0/5 – fa0/48	44	3	Informatica

Configurando el enrutamiento entre VLAN

Primero habilitamos el enrutamiento en el Switch

```
Switch (config)# ip routing
```

Ahora creamos las interfases virtuales para todas las VLANs

```
Switch (config)#interface vlan 2
Switch(config-if)#ip address 172.16.11.1 255.255.255.0

Switch (config)#interface vlan 3
Switch(config-if)#ip address 172.16.12.1 255.255.255.0

Switch (config)#interface vlan 4
Switch(config-if)#ip address 172.16.13.1 255.255.255.0

Switch (config)#interface vlan 5
Switch(config-if)#ip address 172.16.14.1 255.255.255.0
```

Configurando el protocolo de enrutamiento EIGRP

Configuramos EIGRP en todos los conmutadores de la capa de distribución.

```
Switch (config)#router eigrp 10
Switch (config-router)#network 172.16.0.0
```

Configurando las interfases virtuales para el envió de difusión de DHCP

Configuramos los conmutadores de la capa de distribución, para que puedan enviar los pedidos de los clientes DHCP ubicados en los conmutadores de la capa de acceso.

```
Switch (config)#interface vlan 2
Switch(config-if)#no ip direct-broadcast
Switch(config-if)#ip helper-address 172.16.14.254
Switch (config)#interface vlan 3
Switch(config-if)#no ip direct-broadcast
Switch(config-if)#ip helper-address 172.16.14.254
Switch (config)#interface vlan 4
Switch(config-if)#no ip direct-broadcast
Switch(config-if)#ip helper-address 172.16.14.254
```

De este modo logramos que los computadores obtengan su dirección IP, puerta de enlace predeterminada, DNS y otros parámetros desde un servidor DHCP.

A continuación el esquema simplificado de la red.

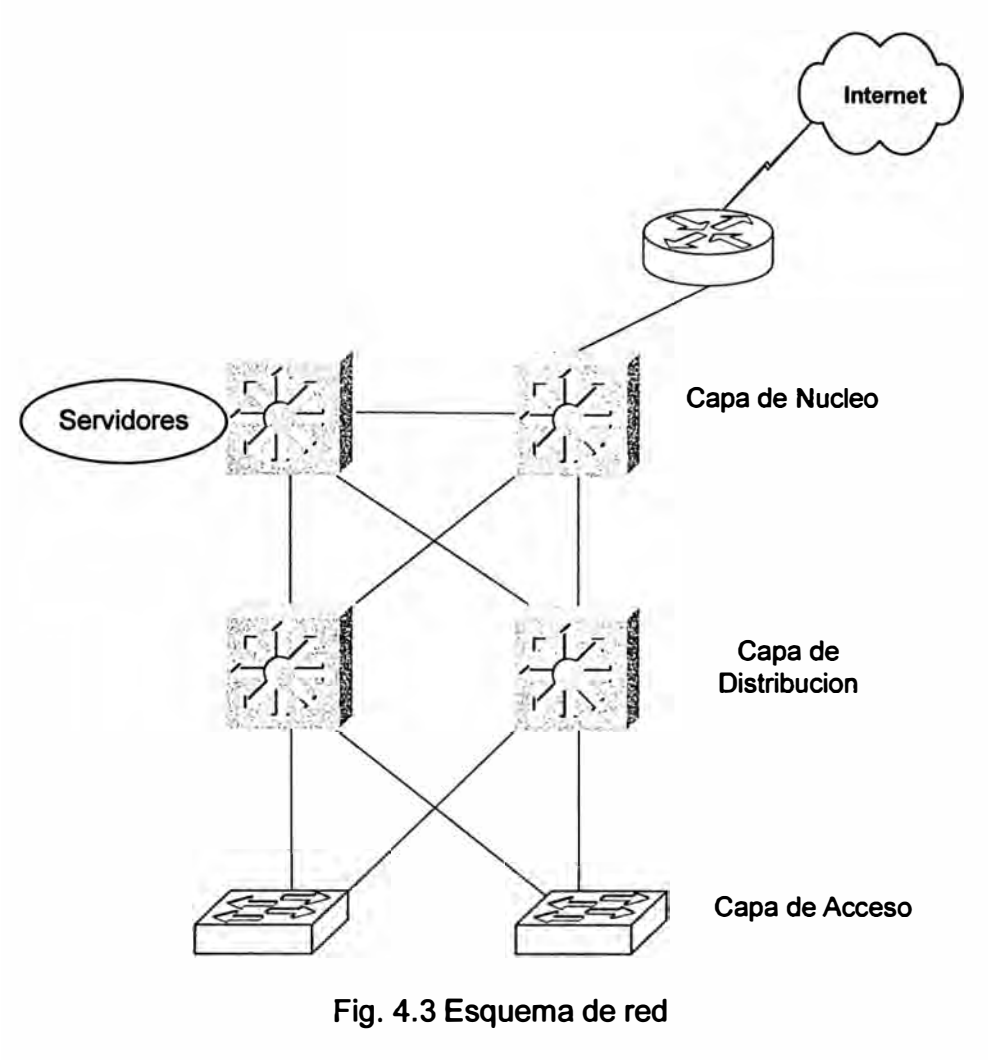


Fig. 4.3 Esquema de red

Los servidores se instalaran en el conmutador de la capa de núcleo.

En los conmutadores de la capa de distribución se crean las Vlan y se configuran como **servidores vtp**. Aquí se configura el enrutamiento entre las Vlans y las listas de acceso.
En los conmutadores de la capa de acceso se configuran como **clientes vtp**, y la asignación de puertos a las vlans dependerá de la ubicación del conmutador en el área de trabajo.

Una lista de acceso que permite que los computadores de la Vlan 3, tengan acceso solo a los servidores y no a otras Vlan, sería como sigue:

```
Switch(config)#access-list 100 permit ip 172.16.12.0
0.0.0.255 172.16.14.0 0.0.0.255

Switch(config)# int vlan3


Switch(config-if)#ip access-group 100 in
```

CONCLUSIONES

1. El segmentar la red mediante VLANs permite, mejorar el rendimiento de la red. Al tener la red segmentada en diferentes dominios de difusión, se pueden crear listas de acceso. Las cuales nos permiten mejorar la seguridad dentro de la LAN.

2. En empresas que no cuentan con recursos económicos para adquirir un conmutador con funciones de capa 3, el enrutamiento entre VLANs se puede implementar utilizando Servidores Linux configurados como router. (Cap. III)

3. El implementar las VLANs permite preparar las redes para el uso de aplicaciones multidifusión.

4. El implementar las VLANs en la empresa ABC se redujo la propagacion de tráfico de difusión en la LAN.

5. La elección del dispositivo de enrutamiento es importante para que este no se convierta en un "cuello de botella". Esto dependerá de las condiciones de tráfico en la red.

6. En redes con alto tráfico entre Vlans lo ideal es utilizar conmutadores (capa 3) con funciones de enrutamiento.

ANEXO A

GLOSARIO DE TÉRMINOS

ACL (lista de control de acceso):
Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router).

ARP
Address Resolution Protocol. Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826.

ATM (modo de transferencia asíncrona):
Estándar internacional para relay de celdas en el que varios tipos de servicios (por ejemplo, transmisión de voz, vídeo o datos) se transmiten en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retardos de tránsito. ATM se encuentra diseñado para aprovechar los medios de transmisión de alta velocidad como E3, SONET y T3.

Broadcast
Paquete de datos que se envía a todos los nodos de una red.

Capa de enlace de datos
La Capa 2 del modelo de referencia OSI. Esta capa suministra un tránsito confiable de datos a través de un enlace físico.

Capa de red
La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. La capa de red es la capa en la que se produce el enrutamiento.

CiscoWorks

Conjunto de aplicaciones de software para administración de internetwork basadas en SNMP. CiscoWorks incluye aplicaciones para monitorear el estado del router y del servidor de acceso, gestionar los archivos de configuración y diagnosticar los problemas de las redes. Las aplicaciones CiscoWorks se integran en varias plataformas de administración de red basadas en SNMP, incluyendo SunNet Manager, HP OpenView e IBM NetView.

Colisión

En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico.

Dirección de broadcast

Dirección especial que se reserva para enviar un mensaje a todas las estaciones. Por lo general, una dirección de broadcast es una dirección MAC destino compuesta por todos unos.

Dominio de broadcast

Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo del conjunto. Los dominios de broadcast generalmente están limitados por routers dado que los routers no envían tramas de broadcast.

Dominio de colisión

En Ethernet, el área de la red dentro del cual las tramas que han sufrido colisiones se propaga. Los repetidores y los hubs propagan las colisiones; los switches LAN, los puentes y los routers no lo hacen.

ELAN

LAN emulada. Red ATM en la que se emula una LAN Ethernet o Token Ring utilizando un modelo cliente-servidor. Las ELAN están compuestas por un LEC, un LES, un BUS y un LECS. Pueden existir múltiples ELAN en una sola red ATM de forma simultánea. Las ELAN se definen a través de la especificación LANE.

Encapsular:

Colocar un encabezado de protocolo en particular a los datos. Por ejemplo, a los datos de

Ethernet se les agrega un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red simplemente se coloca en el encabezado utilizado por el protocolo de enlace de datos de la otra red.

Enrutamiento:
Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ethernet:
El método de conexión más común en las redes de área local, LANs. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

FDDI (Interfaz de datos distribuida por fibra):
Estándar de LAN, definido por ANSI X3T9.5, que especifica una red de transmisión de tokens de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI usa una arquitectura de anillo doble para brindar redundancia.

LAN
Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas.

MAC
Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de *tokens* o contención.

Multicast
Paquetes individuales que la red copia y envía a un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de dirección destino.

Unicast

Mensaje que se envía a un solo destino de red.

VLAN (LAN virtual):

Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

VLAN de puerto central:

VLAN en la que todos los nodos en la misma VLAN se conectan al mismo puerto de switch.

VLAN dinámica (VLAN basada en las direcciones MAC, las direcciones lógicas o el tipo de protocolo de los paquetes de datos.

VLAN estática:

VLAN en la que los puertos de un switch se asignan estáticamente.

BIBILIOGRAFIA

1. William Stallings, Comunicaciones y Redes de Computadores, Séptima edición, Pearson Educación S.A. Madrid, 2004.
2. Andrew S. Tanenbaum, Redes de Computadoras, Cuarta Edición, Pearson Educación, México, 2003.
3. Richard Froom, CCNP Self-Study: Building Cisco Multilayer Switched Networks, third edition, Cisco Press, 2006.
4. Wendell Odom, CCNA ICND Exam Certification Guide, Cisco Systems, Cisco Press, 2004.
5. Todd Lammle, Cisco® Certified Network Associate Study Guide, 5th Edition, SYBEX, 2005.