REDISEÑO DE LA RED DE OPTIMIZA

LUIS EDUARDO NAVARRO CARDENAS
ANGELA MARIA RUIZ BECARIA
RAFAEL ZAMORA MADRID

CORPORACION UNIVERSITARIA UNITEC
ESCUELA DE INGENIERIA
FACULTAD DE SISTEMAS Y COMPUTADORES
BOGOTA
2006

REDISEÑO DE LA RED DE OPTIMIZA

LUIS EDUARDO NAVARRO CARDENAS
ANGELA MARIA RUIZ BECARIA
RAFAEL ZAMORA MADRID

TRABAJO DE INVESTIGACION
CICLO PREPARATORIO PARA GRADO
C.P.G.

CORPORACION UNIVERSITARIA UNITEC
ESCUELA DE INGENIERIA
FACULTAD DE SISTEMAS Y COMPUTADORES
BOGOTA
2006

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el entorno empresarial actual las comunicaciones son la base de toda organización y de esta se derivan procesos supremamente complejos los cuales no pueden parar de un momento a otro, es por esto que la conectividad inmediata y siempre activa entre las diferentes estaciones de trabajo y entre las diferentes ramas de las organizaciones es cada vez mas rápida y eficaz y sus procesos empiezan cada día a transformarse en procesos continuos sin ninguna perdida deliberada ni involuntaria de tiempo herramientas como el *Messenger* o como *NetMeeting* por nombrar algunas han llevado la comunicación intra organizacional y con los clientes y proveedores a niveles que diez años atrás no alcanzaríamos a imaginarnos, el poder estar en línea con todos los clientes y a su vez con los proveedores transformo el proceso de ventas y de entregas de mercancías además de saber de ultima mano e inmediato la capacidad de venta disponible con los proveedores hace que la satisfacción del cliente sea cada vez mejor y que su recordación de la organización sea mas duradera.

A medida que avanzamos, se han desarrollado mejoras para la captura, transporte, almacenamiento y procesamiento de información. El entorno de las redes ha mostrado un progreso en muy corto tiempo manejando el intercambio de información en tiempo muy corto, al mismo tiempo proporciona seguridad en el transporte de los datos.

Las redes en general consisten en compartir recursos, uno de sus objetivos es permitir que toda la información este disponible para cada uno de los usuarios de la red sin importar la localización del recurso o del usuario. También proporciona varias fuentes alternativas de suministro y una fiabilidad, es por ello que hoy en día no solo las empresas ven la necesidad de contar con herramientas tecnológicas para suplir necesidades frente a la comunicación sino que también acceden a un sin numero de posibilidades y facilidades que ofrece la tecnología y más aun cuando estos avances permiten desarrollar un mejor desempeño de la empresa, la cual, al interactuar con los usuarios realiza un análisis para dar respuesta a la necesidades en común, logrando una mayor satisfacción

2. RESEÑA DE OPTIMIZA

OPTIMIZA, se conformó en el año 2002, como respuesta a las necesidades de las empresas colombianas referentes a la viabilidad de adquirir soluciones tecnológicas de software, abiertas, robustas, flexibles, escalables, integradas, enfocadas al usuario final y de costo moderado, que les permitieran concentrarse en el objeto de su negocio y que a la vez les proporcionaran las herramientas necesarias para seguir siendo competitivas o bien tornarse en competitivas dentro del sector donde se desenvuelven.

Partiendo de las anteriores premisas y aprovechando la extraordinaria dinámica que desde hace más de diez años ha tenido la Industria Uruguaya de Tecnologías de la Información (TI), su experiencia internacional y el alto valor agregado que involucran sus soluciones, incluyendo la aplicación de las mejores prácticas empresariales, OPTIMIZA ha seleccionado y obtenido la representación exclusiva para Colombia de compañías de desarrollo de tecnología de ese país, especializadas en ofrecer soluciones para:

Business Intelligence (BI)
Enterprise Resource Planning (ERP)
Core Banking (CB)
Point of Sale (POS)

OPTIMIZA las implementa, soporta, mantiene y ofrece la consultoría relacionada tanto estratégica como en áreas de procesos y gestión.

3. OBJETIVOS

3.1. Objetivo General

Presentar una propuesta a la empresa, con el fin de generar una mejora que permita tener una red fiable, manejable, adaptable y escalable, cubriendo las necesidades básicas, tales como la comunicación de los dispositivos, la seguridad lógica y física de la red.

3.2. Objetivos Específicos

- Se diagnostica el estado físico de la red a nivel de cableado, canaletas, tomas, conectores y centro de cableado.
- Se revisa la conexión entre los *host*, evaluando tiempos de respuesta y fallas de conectividad.
- Se analiza entre las distintas áreas de la empresa sus diferentes tipos y clases de conexión.
- Con la ayuda de la información recolectada, se verifican los niveles de seguridad y se identifican las características de la red en las capas de red y aplicación.

4. FACTIBILIDAD

4.1 Factibilidad Técnica

La propuesta desde el punto de vista técnico es realizable, debido a que en el mercado se encuentra los diferentes equipos y dispositivos de comunicación que darán soporte a la implementación de la propuesta de solución de la red.

4.2 Factibilidad Económica

Optimiza evaluará los costos de la propuesta, y decidirá si es viable o no, basándose en el presupuesto del 2007.

4.3 Factibilidad Operacional

El levantamiento de información que se realizó en la empresa Optimiza, determinó que la red de comunicaciones locales, solucionó múltiples inconvenientes que se presentaba con el manejo de la información en las dependencias que allí funcionan, lo cual garantizan un acuerdo entre los usuarios de la red.

Por lo tanto, todas las recomendaciones sobre la optimización de la misma deberán ser aprovechadas para el beneficio de la empresa.

5. PLANTEAMIENTO DEL PROBLEMA

Mediante el estudio que se le realizo a la empresa OPTIMIZA se verifico que en la infraestructura física de sus redes, tiene algunos deterioros en el recorrido del cableado, además la falta de canaleta en algunos sectores, y algunos conectores desgastados hacen que la red este propensa a sufrir mayores daños. Por este concepto para la infraestructura física se realizaran mejoras en algunos tramos del cableado, con mayor profundidad en los centros de computo, que es donde se presenta mayor avería ya que hay canaletas abiertas y cableado desgastado.

No hay seguridad, ni administración de usuarios y la cantidad de colisiones es alta, por no estar segmentada la red.

6. ALCANCE

Nos enfocaremos principalmente en el mejoramiento de la parte física de la red y de las políticas de seguridad que tienen que seguir para tener una red más confiable, mediante la aplicación de 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

7. MARCO TEORICO

El siglo XX se ha visto conmocionado por una revolución más grande que las de otros siglos. La revolución de la información y más aún el del intercambio de ésta, nunca antes se había contemplado tanta cooperación y convergencia de tecnologías y personas. Con las redes telefónicas y de datos se comenzó la revolución de la información, inicialmente se utilizó la red telefónica para transmitir datos. Hoy en día ocurre lo contrario, debido a que las redes de datos son más aptas desde su construcción para integrar varios servicios.

Las redes de datos están permitiendo que todas las tecnologías que surgieron estén siendo integradas hacia un mismo ente de comunicación, ahora la interconexión de estas redes está permitiendo la centralización, concentración y almacenamiento de la información dispersa por los continentes, agilizando el trabajo, el comercio, los negocios y demás situaciones cotidianas.

A comienzos de la era de la informática, los principales actores de esta evolución eran equipos costosos, grandes, complejos y lentos en comparación a los actuales equipos donde toda la información era clasificada y procesada para entregar un resultado organizado, hoy en día estos equipos con los adelantos en otras áreas de investigación como la microelectrónica y la ingeniería de materiales llevaron los antiguos modelos, lentos y costosos, a equipos del uso diario, hasta casi convertirlos en equipos de primera necesidad, tan baratos que una persona con un ingreso promedio puede adquirir. Con todas estas ventajas, no es extraña la integración a gran escala de ellos. El advenimiento de tecnologías más accesibles al común de personas, hacen que tratemos de plasmar todas las necesidades de comunicación para poder utilizarlas en una red de datos única.

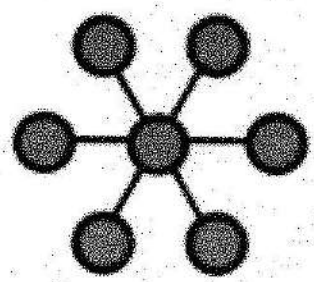
7.1 Topología Física de la Red

La topología es el mapa o plan de la red. La topología física describe como se distribuyen los cables y la topología lógica y eléctrica como se vehiculan los datos, es decir, la topología física es la descripción del camino que unen los cables para unir los nodos: la topología lógica explica como fluyen los mensajes hasta las estaciones existen varias formas de topología física que son:

7.1.1 Topología de estrella

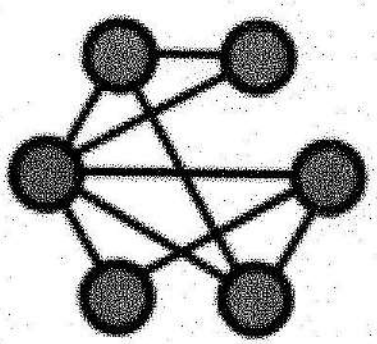
En esta topología todos los nodos se encuentran conectado a una ubicación central común, es decir que todo el cableado se encuentra conectado a un

dispositivo central si uno de los enlaces falla, solo fallara Inc. parte de la red y el resto de esta no se verá afectada.



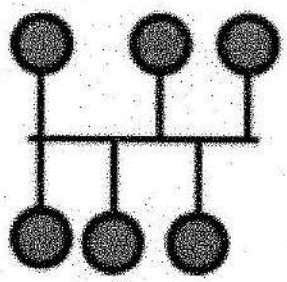
7.1.2 Topología en malla

Conecta a todos los dispositivos de la red y proporciona una ruta para cada dispositivo, pues todos se encuentran interconectados entre si.



7.1.3 Topología de bus

Conecta múltiples dispositivos a un cable principal y, a veces se denomina backbone, una de sus ventajas son el costo y la factibilidad de su instalación; pero si el backbone normalmente utilizada las wan, si esta falla el resto de la red se ve seriamente afectada.

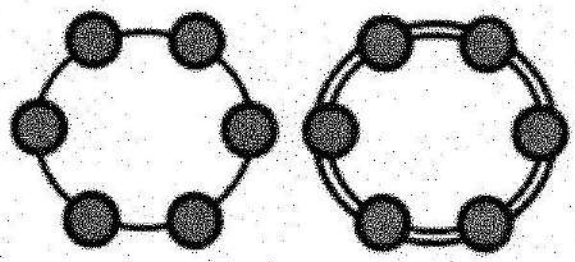


7.1.4 Topología de anillo

Cada dispositivo de la red se encuentra conectado con otros dispositivos, el cable no tiene principio ni fin.

7.1.5 Topología de anillo doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos. La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.



7.2 Componentes de la Topología Física

7.2.1 Normas y estándares requeridos para el sistema de cableado

- **ANSI/tia/EIA 568-a** *Comercial building telecomunications cabling* estándar (octubre 1995). Documento principal que regula todo lo concerniente a sistemas de cableado estructurado para edificios comerciales en cuanto a servicios de voz, datos, imagen y video.

- **ANSI/EIA/TIA-569** *Comercial building estándar for telecomunication pathways and space* (octubre 1990) documento que especifica los estándares para los conductos, pasos y espacios necesarios para la instalación de sistemas estandarizados de telecomunicación.

- **ANSI/EIA/TIA-570** *residencial and Light comercial telecommunicaction wiring standard* (junio 1991)especifica normas para la instalación de sistemas de telecomunicaciones en áreas residenciales y comerciales de baja densidad

- **ANSI/TIA/EIA-606** *The administration standard for the telecommunications infrastructure of commercial building* (febrero 1993).Regula y sugiere los métodos para la administración de los sistemas de telecomunicaciones. La administración se refiere a documentación, etiquetado, planos, reportes y hojas de trabajo.

- **ANSI/TIA/EIA-607** *Commercial building grounding and bonding requierements for telecommunications* (agosto 1994). Regula las especificaciones sobre los sistemas de tierra para equipo de telecomunicaciones.

- **TIA/EIA TSB-36** Especificaciones adicionales para cables UTP

- **TIA/EIA TSB-40** Especificaciones adicionales en transmisión para cables UTP.

- **TIA/EIA TSB-67** *Transmission performance specifications for fiel testing of unshielder twisted-pair cabling system – draft* (septiembre 1995), regula las especificaciones de equipos para prueba, medición y certificación de sistemas de cableado estructurado.

- **TIA/EIA TSB-72** *Centralized optical fiber cabling guidelines – draft* (septiembre 1995), regula la instalación de sistemas centralizados de fibra óptica.

- **TIA/EIA TSB-75** Adicional horizontal cabling *practices for open offices –draf* (junio 1996).regula lo concerniente a espacios de oficinas abiertos u oficinas con mucho personal.

- **IEEE 902.3i ethernet 10/100base – t-LAN** Estandariza los requerimientos de medios y distancias para redes 10mbps.

- **IEEE 802.3u Ethernet 10/100base t-LAN.** Estandariza los requerimientos de medios y distancias para redes 100mbps.

- **ANSI x3t9.5 FDDI.** Define los estándares para las redes locales de 100mbps basadas en fibra óptica o UTP.

7.3 Características del cableado

7.3.1 Conectores RJ

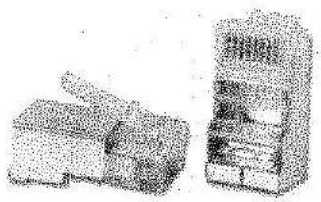
El conector RJ se ha diseñado en varios estándares distintos, cada uno con una nomenclatura. Los más usuales son el RJ-11 y el RJ -45.

7.3.2 RJ-11

Puede albergar como máximo un total de 6 pines, aunque podemos encontrarlo en el mercado con los formatos de 2, 4 y 6 pines según la aplicación a la cual estén destinados.

7.3.3 RJ-45

Pueden albergar como máximo un total de 8 pines aunque igual que el anterior lo podemos encontrar en diferentes formatos según nuestras necesidades. El más usual es el de 8 pines, el cual se usa en el estándar RDSI.



7.3.4 Cable

A la hora de elegir el cable se debe tener en cuenta:

- cuantos equipos se van a conectar
- distribución física
- el ancho de banda que se necesite

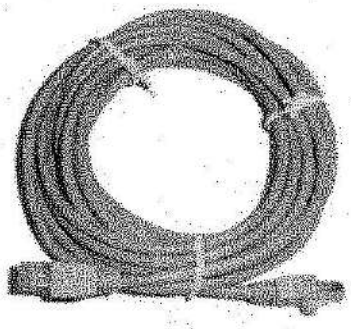
- la existencia de redes ya montadas o de equipos con tarjetas de red aprovechables.
- las condiciones ambientales del edificio: temperatura, humedad, etc.

Si se necesita conectar pocos equipos en una misma habitación se podrá realizar con un cable coaxial, pero si se tienen varios equipos en espacios diferentes habrá que ver un cableado estructurado como UTP o fibra óptica en los casos en que las inferencias externas o las necesidades de ancho de banda así lo requieran.

El cable UTP esta compuesto por cuatro pares de hilos trenzados de menos de 38mm. El hilo usado es de 0.5mm y esta indicado para se utilizado a temperaturas entre -10°c a 60°c

El cable UTP se clasifica en categorías, dependiendo de la velocidad máxima que pueda soportar.

Categoría	Velocidad máxima	Distancia máxima
3	10 mhz	100 m
4	20 mhz	100 m
5	100 mhz	100 m
6	100 mhz	100 m



7.4 Topología Lógica

La topología lógica de una red es la forma en que los *hosts* se comunican a través del medio. Los dos tipos más comunes de topología lógica son de *broadcast (Ethernet)* y transmisión de *tokens (Token Ring)*

La topología de *broadcast* significa que cada *host* envía sus datos hacia todos los demás *host* del nodo de red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que sirve, esta es la forma en que funciona *Ethernet*.

La transmisión de *tokens*, controla el acceso a la red al transmitir un *token* eléctrico de forma secuencial a cada *host*. Cuando un *host* recibe un *token*, significa que el *host* puede enviar datos a través de la red. Si el *host* no tiene ningún dato para enviar, transmite el *token* hacia el siguiente *host* y el proceso se vuelve a repetir.

7.5 Segmentación de Colisiones

7.5.1 Colisión

En *Ethernet*, el resultado de nodos transmitiendo a la vez. Las tramas de cada dispositivo colisionan y quedan dañadas cuando fluyen en el mismo medio físico.

7.5.2 Segmentación

El proceso de dividir un solo dominio de colisión en dos o más dominios de colisión de ancho de banda, con el fin de reducir las colisiones y la congestión de la red.

7.6 Protocolos de Comunicaciones

El protocolo de comunicación a utilizar en la red para permitir la conexión a Internet, conexión de redes y además el manejo de los errores en la transmisión de los datos es el TCP/IP, el cual administra el enrutamiento y el envío de datos, y controla la transmisión por medio del uso de señales de estado predeterminados.

Dicho protocolo es comúnmente utilizado por todos los computadores conectados a Internet, de manera que estos pueden comunicarse entre sí.

7.7 Direcciones IP

7.7.1 Clase A

Cuando esta escrito en formato binario, el primer *bit* (el *bit* que esta ubicado más a la izquierda) de las direcciones clase A es siempre es 0. Los administradores internos de la red asignan los 24 bits restantes. Una manera fácil de reconocer su dispositivo forma parte de una red clase A es verificar el primer octeto de su dirección IP, cuyo valor debe estar entre 0 y 126. (127 comienza con un *bit* 0, pero esta reservado para fines especiales)

Todas las direcciones IP clase A utilizan solamente los primeros 8 bits para identificar la parte de red de la dirección.

Los tres octetos restantes se pueden utilizar para la parte de *host* de la dirección. A cada una de las redes que utilizan una dirección IP clase A se le puede asignar hasta 16'777.214diiiirecciones IP posibles para los dispositivos que están conectados a la red.

7.7.2 Clase B

Los primeros 2 bits de una dirección clase B siempre son 10 (1 y 0). Los administradores internos de la red asignan los 16 bits restantes.

Las direcciones IP clase B siempre tienen valores que van los 128 al 191 en su primer octeto. Todas las direcciones IP clase B utilizan los primeros 16 bits para identificar la parte de la red de la dirección. Los 2 octetos restantes de la dirección IP se encuentran reservados pata la porción de *host* de la dirección.

Cada red que usa un esquema de direcciones IP clase B puede tener asignadas hasta 65.534 direcciones IP posibles a dispositivos conectados a su red.

7.7.3 Clase C

Los 3 primeros bits de una dirección clase C siempre son 110 (1, 1 y 0). Los administradores internos de la red asignan los 8 bits restantes.

Las direcciones IP clase C siempre tienen valores que van 192 al 223 en su primer octeto. Todas las direcciones IP clase C utilizan los primeros 24 bits para identificar la porción de red de la dirección. Solo se puede utilizar el último octeto de una dirección IP clase C para la parte que corresponde al *host*.

A cada una de las redes que utilizan una dirección IP clase C se les pueden asignar hasta 254 direcciones IP posibles para los dispositivos que están conectados a la red.

7.7.4 Mascara de Subred

Mascara de dirección de 32 bits que se usan en para indicar los bits de una dirección IP que se utilizan para la dirección de subred. A veces se denomina simplemente mascara.

7.8 VLAN

Una VLAN es un agrupamiento lógico de dispositivos o usuarios, estos se pueden agrupar por función, departamento, aplicación, etc., independientemente de su ubicación física en un segmento. La configuración VLAN se hace en el *switch* través del software.

La LAN se divide cada vez más en grupos de trabajo conectados a través de *backbones* comunes que forman topologías VLAN, las VLAN segmentan lógicamente la infraestructura física de una LAN en distintas subredes (o dominios de difusión) de forma que las tramas de difusión solo están conmutadas entre puertos de la misma VLAN.

7.8.1 Los Routers de las VLAN

El papel tradicional del *router* consiste en proporcionar *firewalls*, administración de la difusión y procesamiento y distribución de ruta. Los *switches* asumen algunas de estas tareas, los *routers* siguen sendo vitales en las arquitecturas VLAN ya que proporcionan rutas conectadas entre las distintas VLAN. Tan solo se utilizará un *router* para la conexión a Internet apoyado por el *firewall* que manejará la seguridad para Internet.

7.8.2 Implementación de las VLAN

Una VLAN conforma una red conmutada que está segmentada lógicamente por funciones, equipos de proyectos o aplicaciones, sin tener en cuenta la ubicación física de los usuarios. Cada puerto del *switch* puede ser signado a una VLAN. Los puertos asignados a la misma VLAN comparten estas difusiones. Los puertos que o pertenezcan a esa VLAN no comparten estas difusiones. Con esto se maneja el rendimiento general de la red. Existen tres métodos de implementación VLAN:

- **VLAN de Puerto Central:** a todos los nodos conectados a los puertos de la misma VLAN se le asigna el mismo ID de VLAN. Logrando que la red sea más eficaz.
- **VLAN Estáticas:** puertos de un *switch* que se asignan estáticamente a una VLAN, se mantiene la configuración asignada hasta que se cambian.
- **VLAN Dinámicas:** Puertos de un *switch* que se pueden determinar automáticamente de sus tareas VLAN, que se basa en el direccionamiento MAC, direccionamiento lógico ó el tipo de protocolo de los paquetes de datos.

A medida que las subredes IP han crecido, los administradores han buscado formas de utilizar su espacio de direccionamiento con más eficiencia. Aqui se presenta una técnica que se denomina VLSM (MASCARA DE SUBRED DE LONGITUD VARIABLE). Con VLSM, un administrador de red puede usar una máscara larga en las redes con pocos *hosts*, y una máscara corta en las subredes con muchos *hosts*.

VLSM se desarrollo por los siguientes motivos:

- La crisis del direccionamiento.
- La fuerza de tareas de ingeniería de Internet identifico dos problemas en 1992.
- La escasez de direcciones de red clase B IPv4 no asignadas.
- El rápido aumento del tamaño de las tablas de enrutamiento de Internet.

Las siguientes son algunas soluciones a corto plazo para la escasez de direcciones IPv4:

- La división en subredes 1985.
- La división en subredes de longitud variables en 1987.
- El enrutamiento inter dominio sin clase en 1993.
- Las direcciones IP privadas.
- La traducción de direcciones de red (NAT).

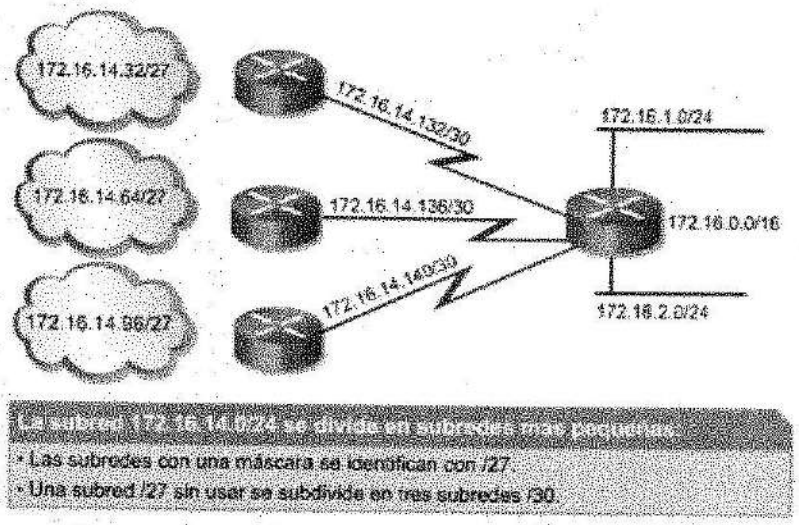
VLSM se utiliza por los siguientes motivos:

- La solución definitiva es IPv6 con espacio de direccionamiento de 128 bits.
- Permite obtener 340.283.366.920.938.463.374.607.431.768.211.456 direcciones.

Para poder implementar VLSM, un administrador de red debe usar un protocolo de enrutamiento que brinde soporte para él. Los *routers* Cisco admiten VLSM con los protocolos de enrutamiento OSPF, IS-IS integrado, EIGRP, RIP v2 y enrutamiento estático.

Los siguientes tipos de protocolo admiten VLSM: OSPF, IS-IS integrado, EIGRP, RIP v2, enrutamiento estático.

VLSM permite que una organización utilice más de una máscara de subred dentro del mismo espacio de direccionamiento de red. La implementación de VLSM maximiza la eficiencia del direccionamiento y con frecuencia se la conoce como división de subredes en subredes.



Los protocolos de enrutamiento con clase necesitan que una sola red utilice la misma máscara de subred. Por ejemplo, una red con la dirección de 192.168.187.0 puede usar sólo una máscara de subred, por ejemplo 255.255.255.0.

Un protocolo de enrutamiento que admite VLSM le confiere al administrador de red la libertad para usar distintas máscaras de subred para redes que se encuentran dentro de un sistema autónomo.

La dirección dividida en subredes es 172.16.32.0/20

La forma binaria es 10101100.00010000.00100000.00000000

La dirección VLSM es 172.16.32.0/26

La forma binaria es 10101100.00010000.0010.0000.00.000000

1a subred:	172	.	16	.0010	.0000.00	.000000	= 172.16.32.0/26
2a subred:	172	.	16	.0010	.0000.01	.000000	= 172.16.32.64/26
3a subred:	172	.	16	.0010	.0000.10	.000000	= 172.16.32.128/26
4a subred:	172	.	16	.0010	.0000.11	.000000	= 172.16.32.192/26
5a subred:	172	.	16	.0010	.0001.00	.000000	= 172.16.33.0/26
	Network			**Subred**	**Subred VLSM**	**Host**	

La siguiente figura muestra un ejemplo de cómo un administrador de red puede usar una máscara de 30 bits para las conexiones de red, una máscara de 24 bits para las redes de usuario e incluso una máscara de 22 bits para las redes con hasta 1000 usuarios.

Máscaras de subred		
255.255.255.252	11111111.11111111.11111111.11111100	30 bits
255.255.255.0	11111111.11111111.11111111.00000000	24 bits
255.255.252.0	11111111.11111111.11111100.00000000	22 bits

7.8.3 Desperdicio de Espacio

Ahora se explicará cómo determinados esquemas de direccionamiento pueden desperdiciar espacio de direccionamiento.

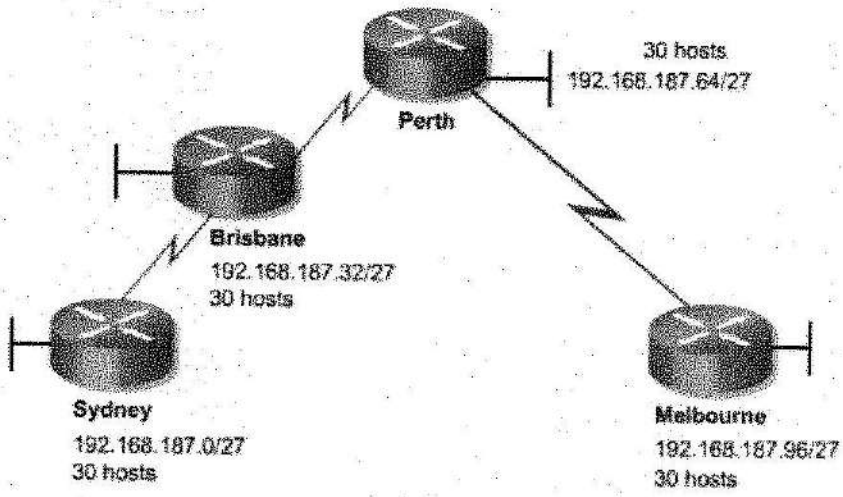
En el pasado, se suponía que la primera y la última subred no debían utilizarse. El uso de la primera subred, conocida como la subred cero, no se recomendaba debido a la confusión que podría producirse si una red y una subred tuvieran la misma dirección. Este concepto también se aplicaba al uso de la última subred, conocida como la subred de unos. Con la evolución de las tecnologías de red y el agotamiento de las direcciones IP, el uso de la primera y la última subred se ha convertido en una práctica aceptable si se utilizan junto con VLSM.

En la Figura, el equipo de administración de red ha pedido prestados tres bits de la porción de *host* de la dirección Clase C que se ha seleccionado para este esquema de direccionamiento. Si el equipo decide usar la subred cero, habrá ocho subredes utilizables. Cada subred puede admitir 30 *hosts*. Si el equipo decide utilizar el comando no ip *subnet-zero*, habrá siete subredes utilizables

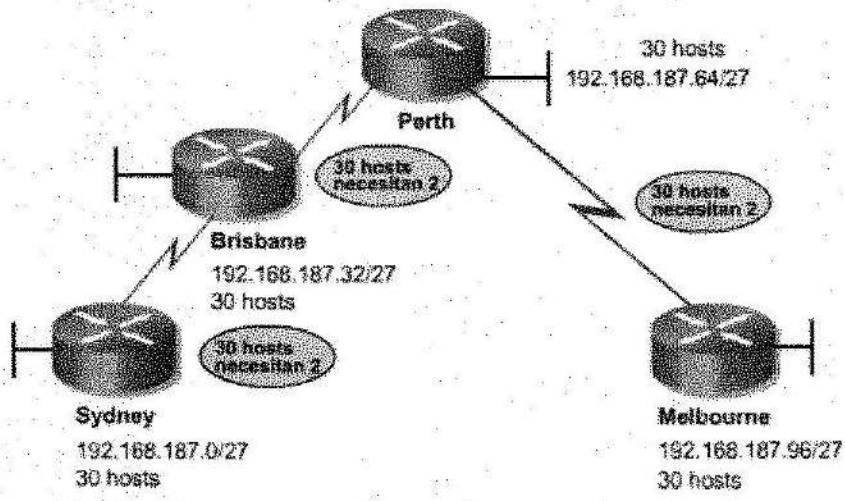
con 30 *hosts* en cada subred. Los *routers* Cisco con la versión 12.0 o posterior del IOS Cisco, utilizan la subred cero por defecto.

Número de subred	Dirección de subred	
Subred 0	192.168.187.0	/27
Subred 1	192.168.187.32	/27
Subred 2	192.168.187.64	/27
Subred 3	192.168.187.96	/27
Subred 4	192.168.187.128	/27
Subred 5	192.168.187.160	/27
Subred 6	192.168.187.192	/27
Subred 7	192.168.187.224	/27

A continuación, cada una de las oficinas remotas de Sydney, Brisbane, Perth y Melbourne puede tener 30 *hosts*. El equipo se da cuenta que tiene que direccionar los tres enlaces WAN punto a punto entre Sydney, Brisbane, Perth y Melbourne. Si el equipo utiliza las tres últimas subredes para los enlaces WAN, se usarán todas las direcciones disponibles y no habrá más espacio para el crecimiento. El equipo también habrá desperdiciado las 28 direcciones de *host* de cada subred simplemente para direccionar tres redes punto a punto. Este esquema de direccionamiento implicaría un desperdicio de un tercio del espacio de direccionamiento potencial.



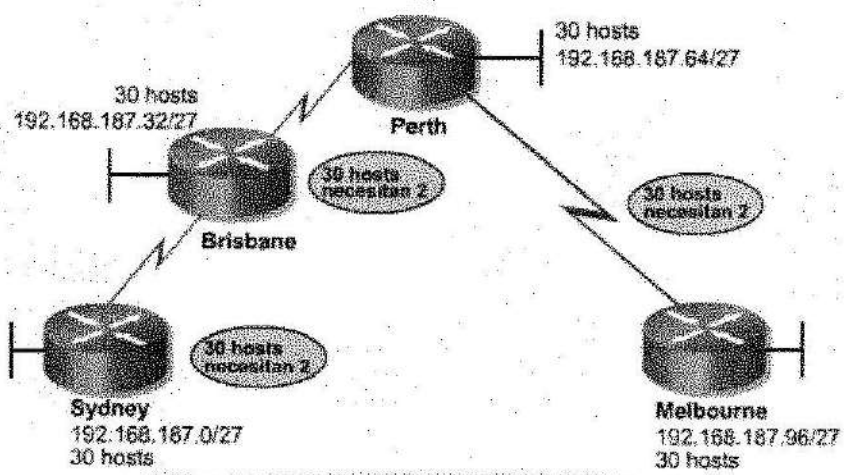
Este tipo de esquema de direccionamiento es adecuado para las LAN pequeñas. Sin embargo, representa un enorme desperdicio si se utilizan conexiones punto a punto.



7.8.4 Cuándo usar VLSM

Es importante diseñar un esquema de direccionamiento que permita el crecimiento y no implique el desperdicio de direcciones. Esta página permitirá analizar la manera de usar VLSM para evitar el desperdicio de direcciones en los enlaces punto a punto.

Como se muestra en la Figura, el equipo de administración de red ha decidido evitar el desperdicio debido al uso de la máscara /27 en los enlaces punto a punto. El equipo aplica VLSM al problema de direccionamiento.



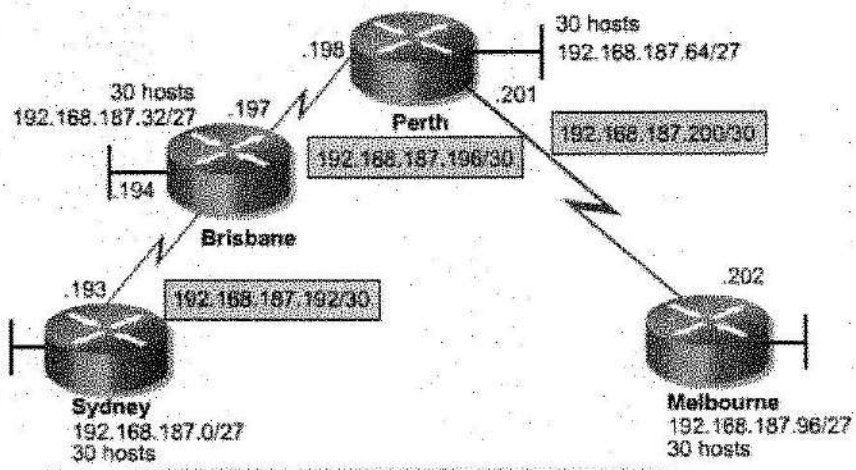
Use VLSM en los enlaces punto a punto que sólo necesitan dos direcciones de host válidas en lugar de 30.

Para aplicar VLSM al problema de direccionamiento, el equipo divide la dirección Clase C en subredes de distintos tamaños. Subredes más grandes se crean para las LAN. Se crean subredes muy pequeñas para los enlaces WAN y otros casos especiales. Una máscara de 30 bits se utiliza para crear subredes con sólo dos direcciones de *host* válidas. Ésta es la mejor solución para las conexiones punto a punto. El equipo tomará una de las tres subredes que anteriormente quedaba asignada a los enlaces WAN y la volverá a dividir en subredes con una máscara de 30 bits.

En el ejemplo, el equipo ha tomado una de las últimas tres subredes, la subred 6, y la ha dividido nuevamente en varias subredes. Esta vez, el equipo utiliza una máscara de 30 bits. Las siguientes tablas demuestran que después de aplicar VLSM, el equipo posee ocho intervalos de direcciones que se pueden usar para los enlaces punto a punto.

Número de subred	Dirección de subred	
subred 0	192.168.187.0	/27
subred 1	192.168.187.32	/27
subred 2	192.168.187.64	/27
subred 3	192.168.187.96	/27
subred 4	192.168.187.128	/27
subred 5	192.168.187.160	/27
subred 6	192.168.187.192	/27
subred 7	192.168.187.224	/27

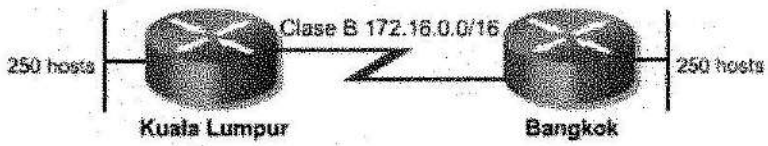
Número de subred	Dirección de subred	
sub-subred 0	192.168.187.192	/30
sub-subred 1	192.168.187.196	/30
sub-subred 2	192.168.187.200	/30
sub-subred 3	192.168.187.204	/30
sub-subred 4	192.168.187.208	/30
sub-subred 5	192.168.187.212	/30
sub-subred 6	192.168.187.216	/30
sub-subred 7	192.168.187.220	/30



Observe la máscara /27 para las LAN y la máscara /30 para los enlaces seriales.

7.8.5 Cálculo de subredes con VLSM

VLSM ayuda a manejar las direcciones IP. En esta página se explicará cómo usar VLSM para establecer máscaras de subred que cumplan con los requisitos del enlace o del segmento. Una máscara de subred debe satisfacer los requisitos de una LAN con una máscara de subred y los requisitos de una WAN punto a punto con otra máscara de subred.



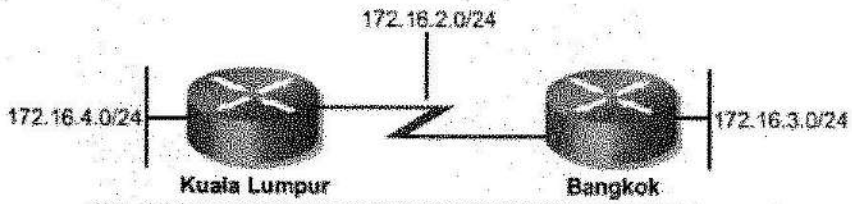
Cada LAN debe admitir más de 250 hosts. La red Clase B 172.16.0.0/16 se puede dividir en subredes con una máscara de 24 bits de 255.255.255.0 para crear subredes lo suficientemente grandes para cada LAN.

El ejemplo muestra una red que necesita un esquema de direccionamiento.

El ejemplo incluye una dirección Clase B de 172.16.0.0 y dos LAN que requieren al menos 250 *hosts* cada una. Si los *routers* usan un protocolo de enrutamiento con clase, el enlace WAN debe formar una subred de la misma red de Clase B. Los protocolos de enrutamiento con clase, como por ejemplo RIP v1, IGRP y EGP, no admiten VLSM. Sin VLSM, el enlace WAN necesitaría la misma máscara de subred que los segmentos LAN. La máscara de 24 bits de 255.255.255.0 puede admitir 250 *hosts*.

Clase B dividida en subredes como 255.255.255.0

Número	ID	Intervalo	Broadcast
0	172.16.0.0	172.16.0.1 - 172.16.0.254	172.16.0.255
1	172.16.1.0	172.16.1.1 - 172.16.1.254	172.16.1.255
2	172.16.2.0	172.16.2.1 - 172.16.2.254	172.16.2.255
3	172.16.3.0	172.16.3.1 - 172.16.3.254	172.16.3.255
4	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
5	172.16.5.0	172.16.5.1 - 172.16.5.254	172.16.5.255
6	172.16.6.0	172.16.6.1 - 172.16.6.254	172.16.6.255
7	172.16.7.0	172.16.7.1 - 172.16.7.254	172.16.7.255
8	172.16.8.0	172.16.8.1 - 172.16.8.254	172.16.8.255
9	172.16.9.0	172.16.9.1 - 172.16.9.254	172.16.9.255
10	172.16.10.0	172.16.10.1 - 172.16.10.254	172.16.10.255
11	172.16.11.0	172.16.11.1 - 172.16.11.254	172.16.11.255
12	172.16.12.0	172.16.12.1 - 172.16.12.254	172.16.12.255
13	172.16.13.0	172.16.13.1 - 172.16.13.254	172.16.13.255
14	172.16.14.0	172.16.14.1 - 172.16.14.254	172.16.14.255
15	172.16.15.0	172.16.15.1 - 172.16.15.254	172.16.15.255

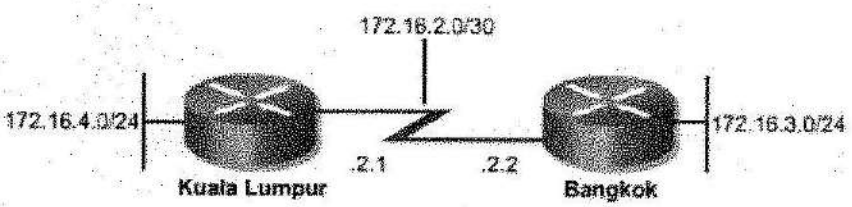


Cada enlace puede admitir más de 254 hosts. El enlace WAN sólo necesita dos hosts, uno para cada interfaz de router. Por lo tanto, se desperdiciarían 252 direcciones.

El enlace WAN sólo necesita dos direcciones, una para cada *router*. Esto significa que se han desperdiciado 252 direcciones.

Si se hubiera utilizado VLSM, todavía se podría aplicar una máscara de 24 bits en los segmentos LAN para los 250 *hosts*. Se podría usar una máscara de 30 bits para el enlace WAN dado que sólo se necesitan dos direcciones de *host*.

Aquí se muestra dónde se pueden aplicar las direcciones de subred de acuerdo a los requisitos de cantidad de *host*. Los enlaces WAN usan direcciones de subred con un prefijo de /30. Este prefijo sólo permite dos direcciones de *host* lo que es justo lo suficiente para una conexión punto a punto entre un par de *routers*.



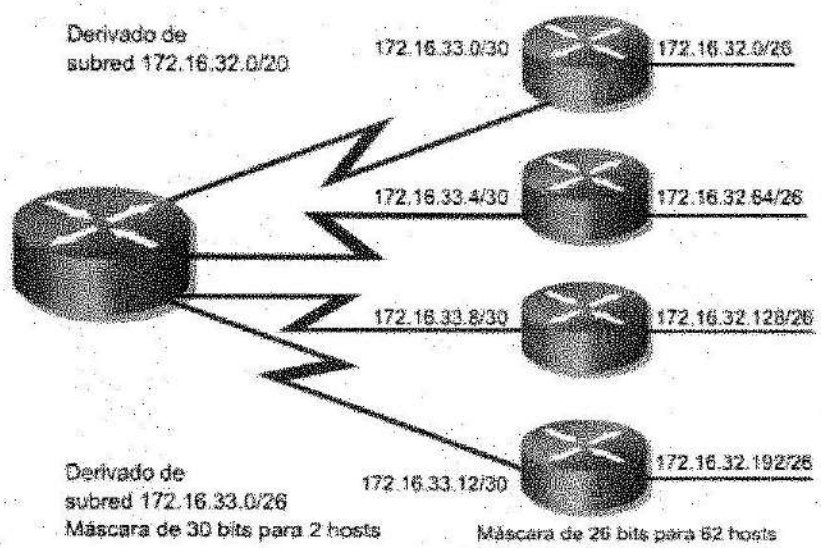
El /30 significa que se pierden menos direcciones.
Las direcciones de subred utilizadas se generan cuando la subred 172.16.32.0/20 se divide en subredes /26.

La dirección dividida en subredes es 172.16.32.0/20
La forma binaria es 10101100.00010000.00100000.00000000

La dirección VLSM es 172.16.32.0/26
La forma binaria es 10101100.00010000.0010|0000.00|000000

subred 1:	172	.	16	.0010	0000.00	000000	= 172.16.32.0/26
subred 2:	172	.	16	.0010	0000.01	000000	= 172.16.32.64/26
subred 3:	172	.	16	.0010	0000.10	000000	= 172.16.32.128/26
subred 4:	172	.	16	.0010	0000.11	000000	= 172.16.32.192/26
subred 5:	172	.	16	.0010	0001.00	000000	= 172.16.33.0/26
	Red			**Subred**	**Subred VLSM**	**Host**	

Para calcular las direcciones de subred que se utilizan en los enlaces WAN, siga subdividiendo una de las subredes /26 que no se utilizan. En este ejemplo, 172.16.33.0/26 se sigue subdividiendo con un prefijo de /30. Esto permite obtener cuatro bits de subred adicionales y por lo tanto 16 (24) subredes para las WAN. Cómo calcular un sistema VLSM.



VLSM se puede usar para dividir en subredes una dirección que ya está dividida en subredes. Se puede tomar a modo de ejemplo, dirección de subred 172.16.32.0/20 y una red que necesita diez direcciones de *host*. Con esta dirección de subred, existen 212 – 2 ó 4094 direcciones de *host*, la mayoría de las cuales quedarán desperdiciadas. Con VLSM es posible dividir 172.16.32.0/20 en subredes para crear más direcciones de red con menos *hosts* por red. Cuando 172.16.32.0/20 se divide en subredes dando como resultado 172.16.32.0/26, existe una ganancia de 26 ó 64 subredes. Cada subred puede admitir 26 – 2 ó 62 *hosts*.

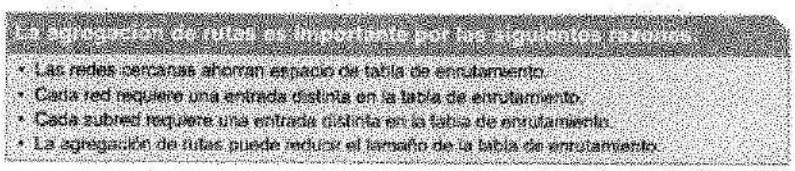
Para aplicar VLSM en 172.16.32.0/20, siga los pasos que aparecen a continuación:

- Paso 1. Escribir172.16.32.0 en su forma binaria.
- Paso 2. Trazar una línea vertical entre el *bit* número 20 y 21, tal como aparece en la Figura A. El límite de subred original fue /20.
- Paso 3. Trazar una línea vertical entre el *bit* número26 y 27, tal como aparece en la Figura A. El límite de subred original /20 se extiende a seis bits hacia la derecha, convirtiéndose en /26.
- Paso 4. Calcular las 64 direcciones de subred por medio de los bits que se encuentran entre las dos líneas verticales, desde el menor hasta el mayor valor. La figura muestra las primeras cinco subredes disponibles.

Es importante recordar que se pueden seguir subdividiendo sólo las subredes no utilizadas. Si se utiliza alguna dirección de una subred, esa subred ya no se puede subdividir más. En la Figura B, se utilizan cuatro números de subred en las LAN. La subred 172.16.33.0/26 no utilizada se sigue subdividiendo para utilizarse en los enlaces WAN.

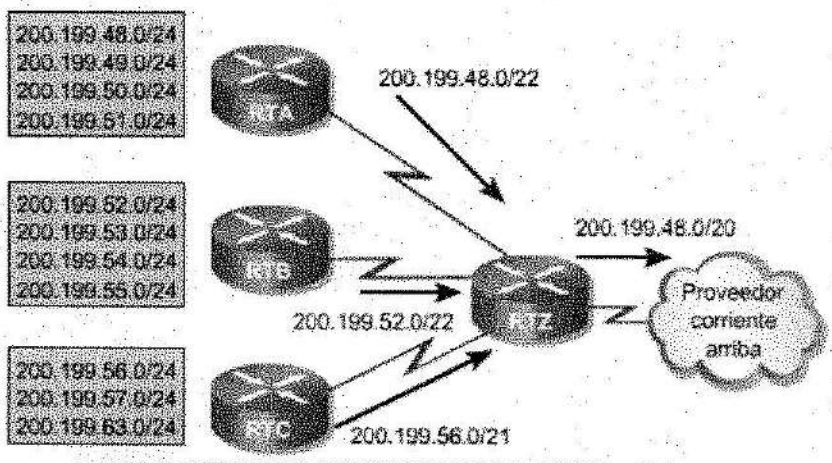
7.8.6 Unificación de rutas con VLSM

Cuando se utiliza VLSM, es importante mantener la cantidad de subredes agrupadas en la red para permitir la unificación. Por ejemplo, redes como 172.16.14.0 y 172.16.15.0 deberían estar cerca de manera que los *routers* sólo tengan que poseer una ruta para 172.16.14.0/23.



El uso de enrutamiento entre dominios sin clase (CIDR) y VLSM evita el

desperdicio de direcciones y promueve la unificación o el resumen de rutas. Sin el resumen de rutas, es probable que el enrutamiento por el *backbone* de Internet se habría desplomado antes de 1997.



El resumen de rutas reduce el tamaño de la tabla de enrutamiento al agregar rutas a varias redes en una sola superred.

La Figura muestra cómo el resumen de rutas reduce la carga de los *routers* corriente arriba. Esta compleja jerarquía de redes y subredes de varios tamaños se resume en diferentes puntos con una dirección prefijo, hasta que la red completa se publica como sola ruta unificada de 200.199.48.0/22. El resumen de ruta o la superred, sólo es posible si los *routers* de una red utilizan un protocolo de enrutamiento sin clase, como por ejemplo OSPF o EIGRP. Los protocolos de enrutamiento sin clase llevan un prefijo que consiste en una dirección IP de 32 bits y una máscara de bits en las actualizaciones de enrutamiento. En la Figura, el resumen de ruta que finalmente llega al proveedor contiene un prefijo de 20 bits común a todas las direcciones de la organización. Esa dirección es 200.199.48.0/22 ó 11001000.11000111.0011. Para que el resumen funcione, las direcciones se deben asignar cuidadosamente de manera jerárquica para que las direcciones resumidas compartan la misma cantidad de bits de mayor peso.

Es importante recordar las siguientes reglas:

- Un *router* debe conocer con detalle los números de las subredes conectadas a él.
- No es necesario que un *router* informe a los demás *routers* de cada subred si el *router* puede enviar una ruta agregada para un conjunto de rutas.
- Un *router* que usa rutas unificadas tiene menos entradas en su tabla de enrutamiento.

VLSM aumenta la flexibilidad del resumen de ruta porque utiliza los bits de mayor peso compartidos a la izquierda, aun cuando las redes no sean contiguas.

Direcciones	Primer octeto	Segundo octeto	Tercer octeto	Cuarto octeto
192.168.96.0	11000000	10101000	01100000	00000000
192.168.99.0	11000000	10101000	01100011	00000000
192.168.100.0	11000000	10101000	01100100	00000000
192.168.101.0	11000000	10101000	01100101	00000000
192.168.102.0	11000000	10101000	01100110	00000000
192.168.105.0	11000000	10101000	01101001	00000000

La ruta resumida es 192.168.96.0/20

192.168.96.0	11000000	10101000	01100000	00000000

La Figura anterior muestra que las direcciones comparten los primeros 20 bits. Estos bits aparecen en rojo. El *bit* número 21 no es igual para todos los *routers*. Por lo tanto, el prefijo para el resumen de ruta será de 20 bits de largo. Esto se utiliza para calcular el número de red del resumen de ruta.

La siguiente figura muestra que las direcciones comparten los primeros 21 bits. Estos bits aparecen en rojo. El *bit* número 22 no es igual para todos los *routers*.

Por lo tanto, el prefijo para el resumen de ruta será de 21 bits de largo. Esto se utiliza para calcular el número de red del resumen de ruta.

Direcciones	Primer octeto	Segundo octeto	Tercer octeto	Cuarto octeto
172.16.0.0	10101100	00010000	00000000	00000000
172.16.2.0	10101100	00010000	00000010	00000000
172.16.3.128	10101100	00010000	00000011	10000000
172.16.4.0	10101100	00010000	00000100	00000000
172.16.4.128	10101100	00010000	00000100	10000000

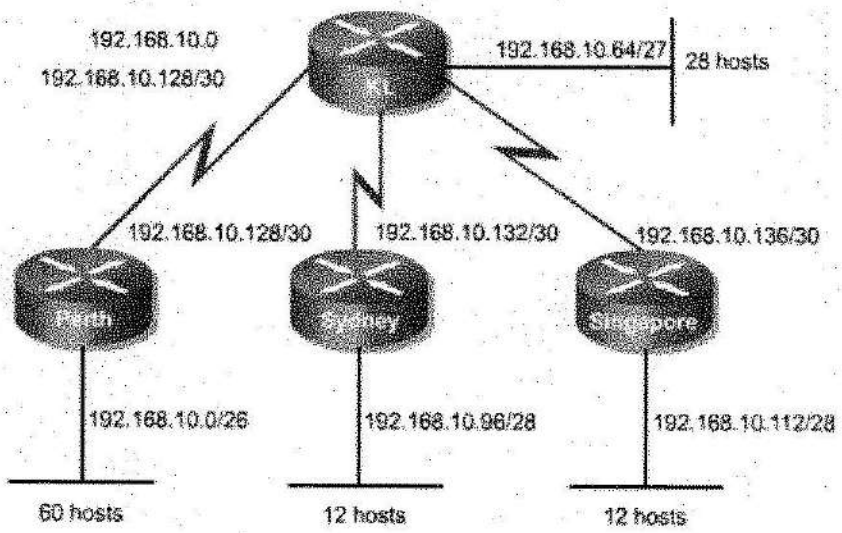
Respuesta:

172.16.0.0/21	10101100	00010000	00000000	00000000

7.8.7 Configuración de VLSM

A continuación, se presentan los cálculos de VLSM para las conexiones LAN

de la Figura:



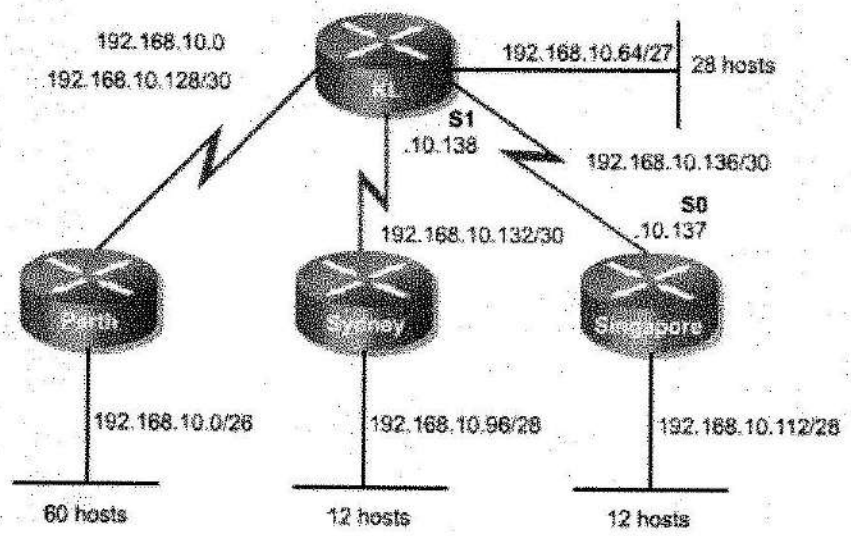
- Dirección de red: 192.168.10.0
- El *router* Perth tiene que admitir 60 *hosts*. Esto significa que se necesita un mínimo de seis bits en la porción de *host* de la dirección. Seis bits proporcionan 26 – 2 ó 62 direcciones de *host* posibles. Se asigna la subred 192.168.10.0/26 a la conexión LAN para el *router* Perth.
- Los *routers* Sydney y Singapur deben admitir 12 *hosts* cada uno. Esto significa que se necesitan un mínimo de cuatro bits en la porción de *host* de la dirección. Cuatro bits proporcionan 24 – 2 ó 14 direcciones de *host* posibles. Se asigna la subred 192.168.10.96/28 a la conexión LAN para el *router* Sydney y la subred 192.168.10.112/28 a la conexión LAN para el *router* Singapur.
- El *router* KL tiene que admitir 28 *hosts*. Esto significa que se necesitan un mínimo de cinco bits en la porción de *host* de la dirección. Cinco bits proporcionan 25 – 2 ó 30 direcciones de *host* posibles. Se asigna la subred 192.168.10.64/27 a la conexión LAN para el *router* KL.

A continuación, se presentan los cálculos de VLSM para las conexiones punto a punto de la Figura:

- La conexión de Perth a Kuala Lumpur requiere sólo dos direcciones de *host*. Esto significa que se necesita un mínimo de dos bits en la porción de *host* de la dirección. Dos bits proporcionan 22 – 2 ó 2 direcciones de *host* posibles. Se asigna la subred 192.168.10.128/30 a la conexión de Perth a Kuala Lumpur.
- La conexión de Sydney a Kuala Lumpur requiere sólo dos direcciones de *host*. Esto significa que se necesita un mínimo de dos bits en la porción de host de la dirección. Dos bits proporcionan 22 – 2 ó 2 direcciones de host posibles. Se asigna la subred 192.168.10.132/30 a la conexión de

Sydney a Kuala Lumpur.

- La conexión de Singapur a Kuala Lumpur requiere sólo dos direcciones de *host*. Esto significa que se necesita un mínimo de dos bits en la porción de *host* de la dirección. Dos bits proporcionan 22 – 2 ó 2 direcciones de *host* posibles. Se asigna la subred 192.168.10.136/30 a la conexión de Singapur a Kuala Lumpur.



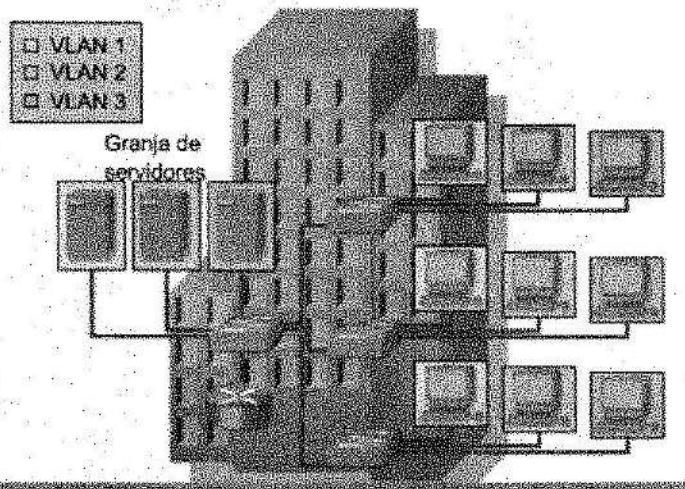
La siguiente configuración es para la conexión punto a punto de Singapur a KL:

```
Singapore(config)#interface serial 0
Singapore(config-if)#ip address 192.168.10.137 255.255.255.252

KualaLumpur(config)#interface serial 1
KualaLumpur(config-if)#ip address 192.168.10.138 255.255.255.252
```

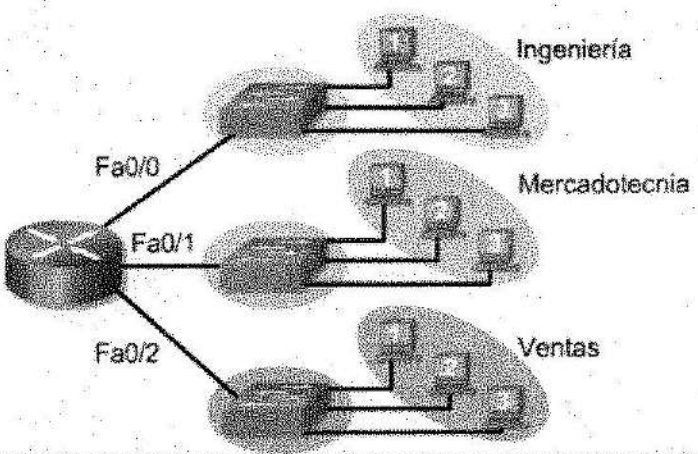
7.8.8 Dominios de *broadcast* con VLAN y *routers*

Una VLAN es un dominio de *broadcast* que se crea en uno o más *switches*. El diseño de red en las Figuras A y B requiere de tres dominios de *broadcast* separados.



- Un switch crea un dominio de broadcast
- Las VLAN ayudan a gestionar los dominios de broadcast
- Las VLAN se pueden definir como grupos de puertos, usuarios o protocolos
- Los switch LAN y el software de administración de red suministran un mecanismo para crear las VLAN

Figura A



Se pueden usar tres switch y un router sin formar una VLAN:

- Switch para Ingeniería
- Switch para Ventas
- Switch para Mercadotecnia
- Cada switch trata a todos los puertos como miembros de un solo dominio de broadcast
- El router se usa para enrutar los paquetes entre los tres dominios de broadcast

Figura B

La Figura B muestra como los tres dominios de *broadcast* se crean usando tres *switches*. El enrutamiento de capa 3 permite que el *router* mande los paquetes a tres dominios de *broadcast* diferentes.

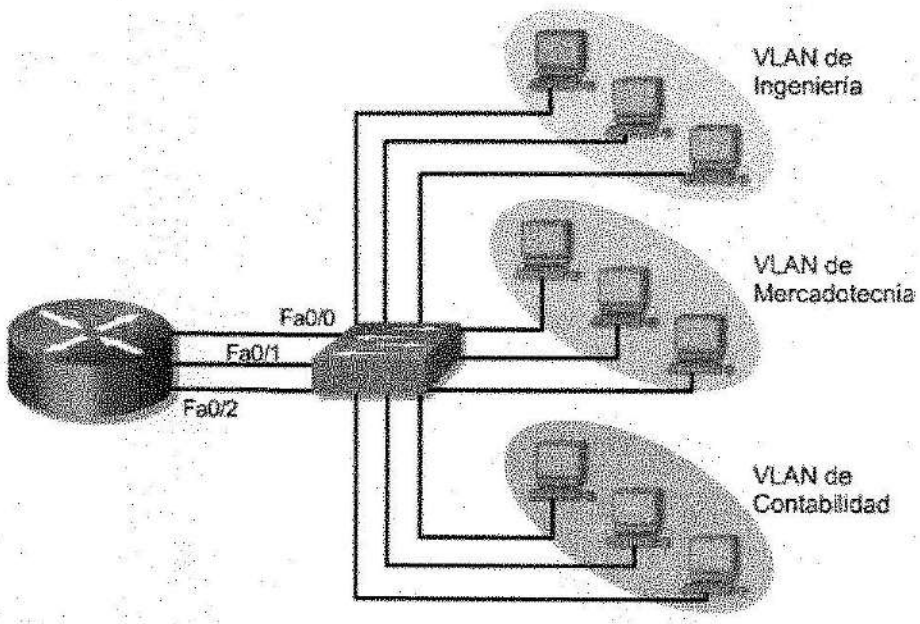


Figura C

En la Figura C, se crea una VLAN con un *router* y un *switch*. Existen tres dominios de *broadcast* separados. El *router* enruta el tráfico entre las VLAN mediante enrutamiento de Capa 3. El *switch* en la Figura C envía tramas a las interfaces del *router* cuando se presentan ciertas circunstancias:

- Si es una trama de *broadcast*
- Si está en la ruta a una de las direcciones MAC del *router*

Si la Estación de Trabajo 1 de la VLAN de Ingeniería desea enviar tramas a la Estación de Trabajo 2 en la VLAN de Ventas, las tramas se envían a la dirección MAC Fa0/0 del *router*. El enrutamiento se produce a través de la dirección IP de la interfaz del *router* Fa0/0 para la VLAN de Ingeniería.

Si la Estación de Trabajo 1 de la VLAN de Ingeniería desea enviar una trama a la Estación de Trabajo 2 de la misma VLAN, la dirección MAC de destino de la trama es la de la Estación de Trabajo 2.

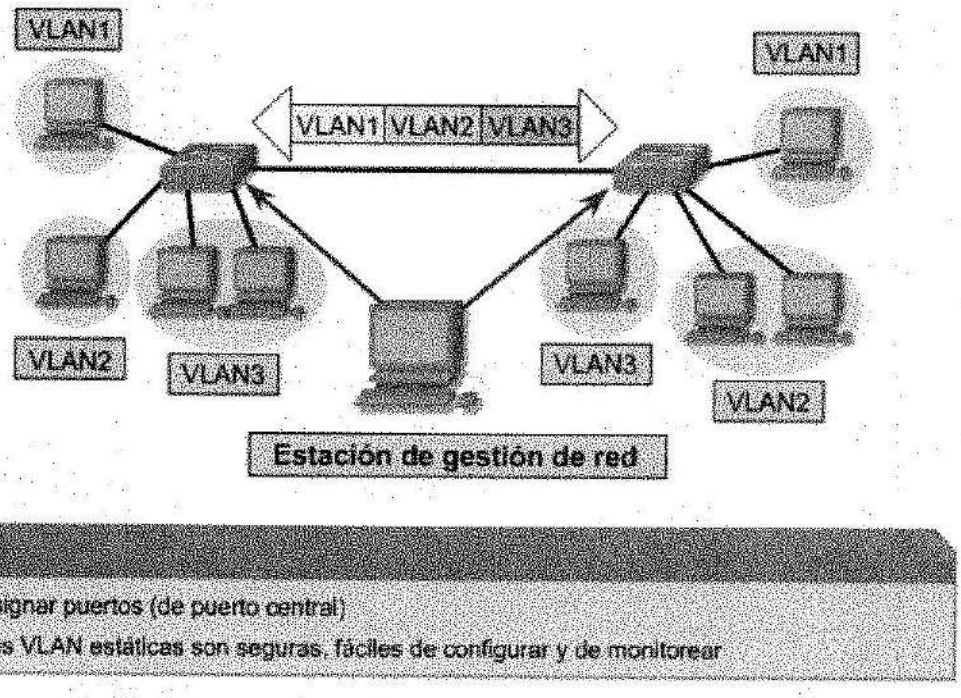
La implementación de VLAN en un *switch* hace que se produzcan ciertas acciones:

- El switch mantiene una tabla de puenteo separada para cada VLAN.
- Si la trama entra en un puerto en la VLAN 1, el *switch* busca la tabla de puenteo para la VLAN 1.

- Cuando se recibe la trama, el *switch* 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.

7.8.9 Operación de las VLAN

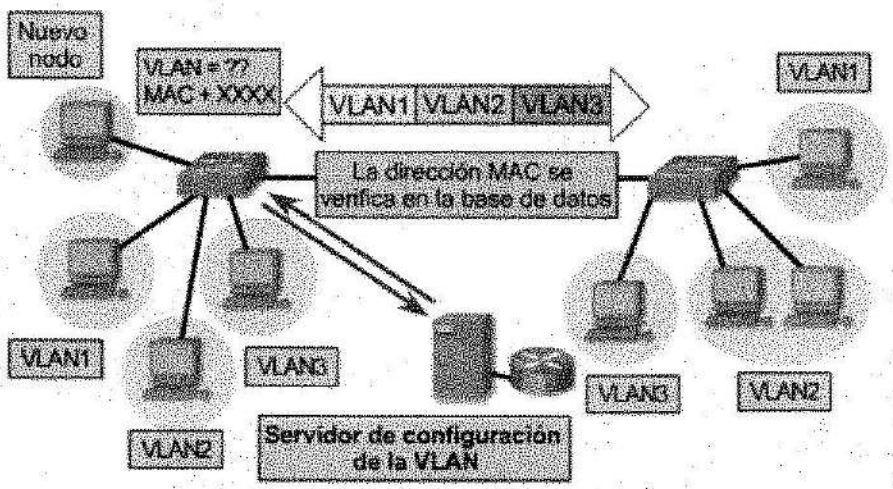
Una VLAN se compone de una red conmutada que se encuentra lógicamente segmentada. Cada puerto de *switch* se puede asignar a una VLAN. Los puertos asignados a la misma VLAN comparten *broadcasts*. Los puertos que no pertenecen a esa VLAN no comparten esos *broadcasts*. Esto mejora el desempeño de la red porque se reducen los *broadcasts* 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.



Los usuarios conectados al mismo segmento compartido comparten el ancho de banda de ese segmento. Cada usuario adicional conectado al medio compartido significa que el ancho de banda es menor y que se deteriora el desempeño de la red. Las VLAN ofrecen mayor ancho de banda a los usuarios que una red *Ethernet* compartida basada en *hubs*. La VLAN por defecto para cada puerto del *switch* es la VLAN de administración. La VLAN de

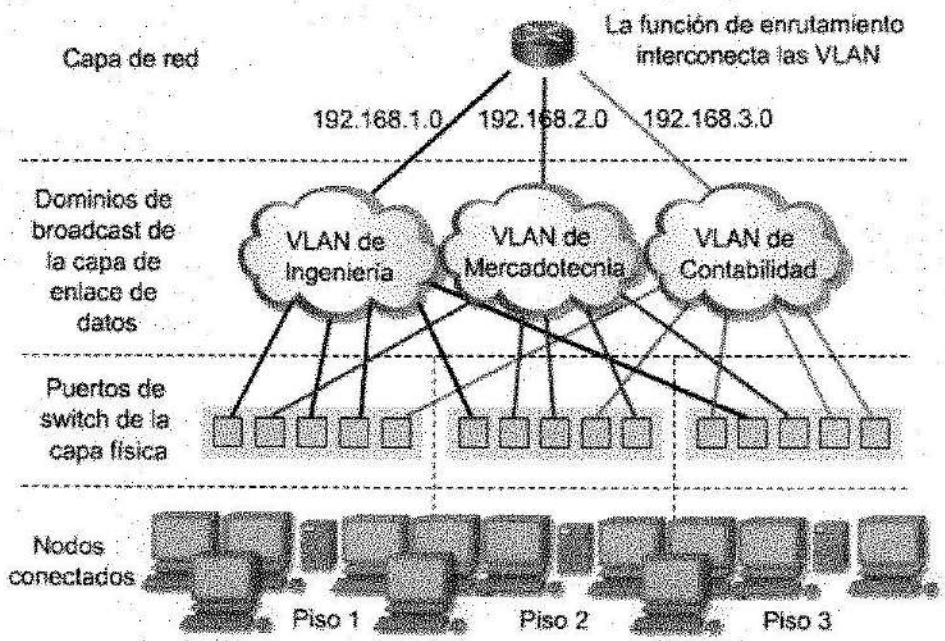
administración siempre es la VLAN 1 y no se puede borrar. Por lo menos un puerto debe asignarse a la VLAN 1 para poder gestionar el *switch*. Todos los demás puertos en el *switch* pueden reasignarse a VLAN alternadas.

Las VLAN de asociación dinámica son creadas mediante software de administración de red. 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 de *switch*. Cuando un dispositivo entra a la red, el *switch* al que está conectado consulta una base de datos en el Servidor de Configuración de VLAN para la asociación de VLAN.



- Las VLAN se asignan mediante una aplicación de administración de VLAN centralizada
- Las VLAN basadas en la dirección MAC, dirección lógica o tipo de protocolo
- Menor administración en el armario de cableado
- Notificación cuando un usuario no reconocido se agrega a la red

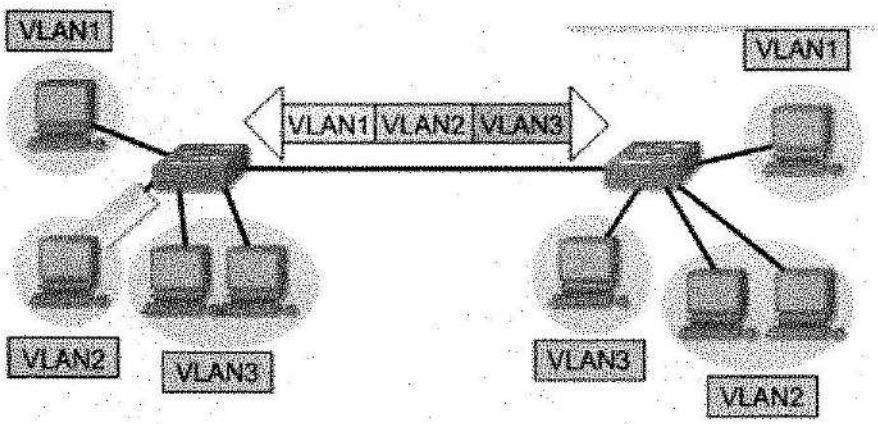
En la asociación de VLAN de puerto central basada en puerto, el puerto se asigna a una asociación de VLAN específica independiente del usuario o sistema conectado al puerto. Al utilizar este método de asociación, todos los usuarios del mismo puerto deben estar en la misma VLAN. Un solo usuario, o varios usuarios pueden estar conectados a un puerto y no darse nunca cuenta de que existe una VLAN. Este método es fácil de manejar porque no se requieren tablas de búsqueda complejas para la segmentación de VLAN.



Los administradores de red son responsables por configurar las VLAN de forma estática y dinámica.

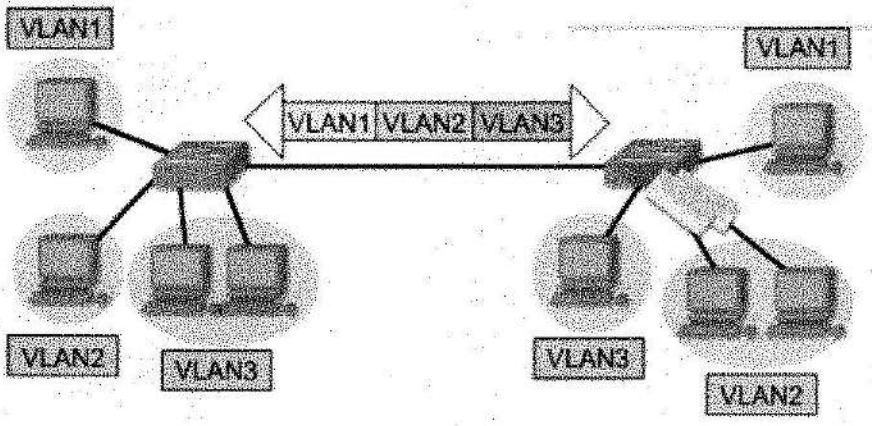
Configuración de las VLAN	Descripción
Estáticamente	Los administradores de red configuran puerto por puerto. Cada puerto está asociado a una VLAN específica. El administrador de red es responsable de escribir las asignaciones entre los puertos y las VLAN.
Dinámicamente	Los puertos pueden calcular dinámicamente su configuración de VLAN. Se usa una base de datos de software que contiene un mapeo de direcciones MAC a VLAN, que el administrador de red debe configurar primero.

Los puentes filtran el tráfico que no necesita ir a los segmentos, salvo el segmento destino. Si una trama necesita atravesar un puente y la dirección MAC destino es conocida, el puente sólo envía la trama al puerto de puente correcto. Si la dirección MAC es desconocida, inunda la trama a todos los puertos en el dominio de *broadcast*, o la VLAN, salvo el puerto origen donde se recibió la trama. Los *switches* se consideran como puentes multipuerto.



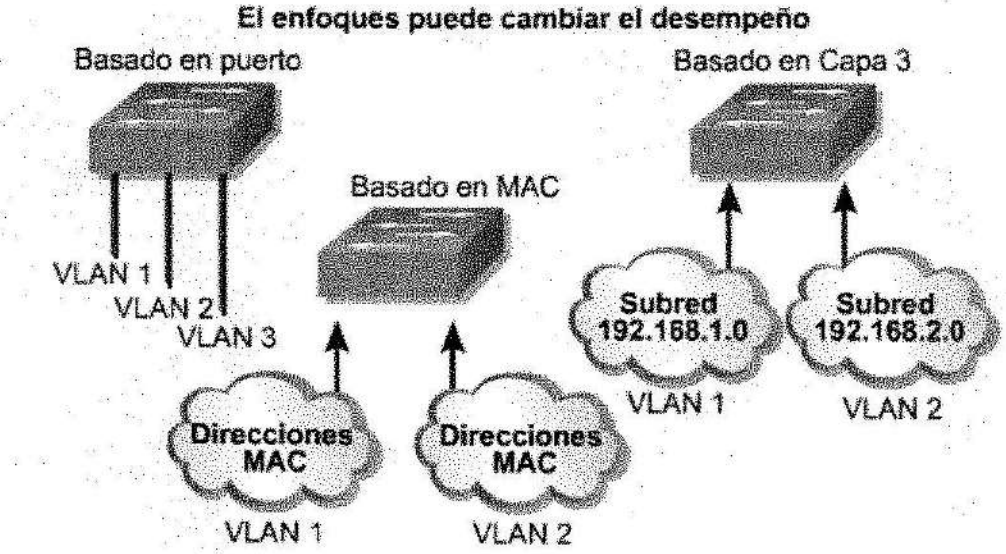
Ventana emergente

Una transmisión broadcast consiste en un solo paquete de datos que se envía al switch, donde se copia y se envía a todos los nodos de la red. El nodo origen agrega a los paquetes una dirección broadcast que especifica que el paquete se debe enviar a todos los nodos destino posibles. Entonces, los paquetes se envían a la red. El switch copia los paquetes y los envía a todos los nodos de la red.



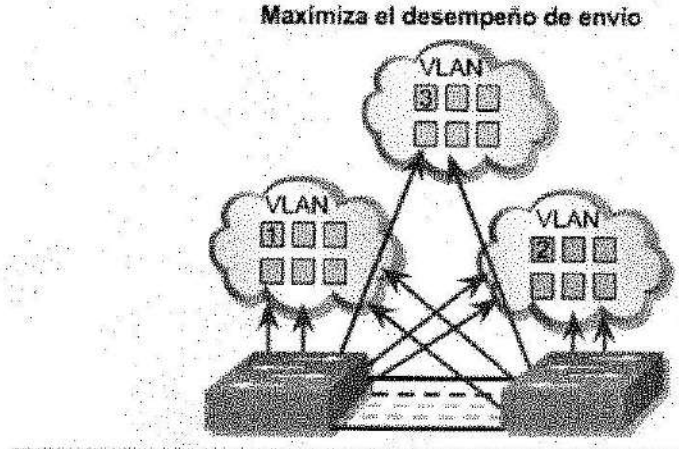
7.8.11 Tipos de VLAN

En esta página se describen tres asociaciones básicas de VLAN que se utilizan para determinar y controlar de qué manera se asigna un paquete, en esta página se describen tres asociaciones básicas de VLAN que se utilizan para determinar y controlar de qué manera se asigna un paquete



- Impulsado por puerto
- Impulsado por dirección MAC
- Impulsado por dirección de red

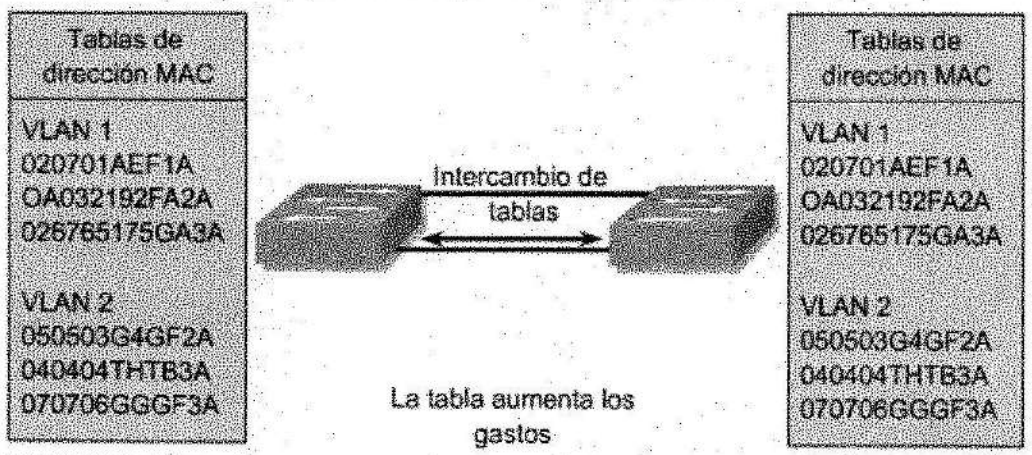
Establecer una membresía a una VLAN



- Asignado por el usuario por asociación de puerto
- No requiere verificación si se hace en ASIC
- Se administra fácilmente mediante las GUI
- Maximiza la seguridad entre las VLAN
- Los paquetes no se "filtran" a otros dominios
- Se controla fácilmente en toda la red

Membresía por puerto

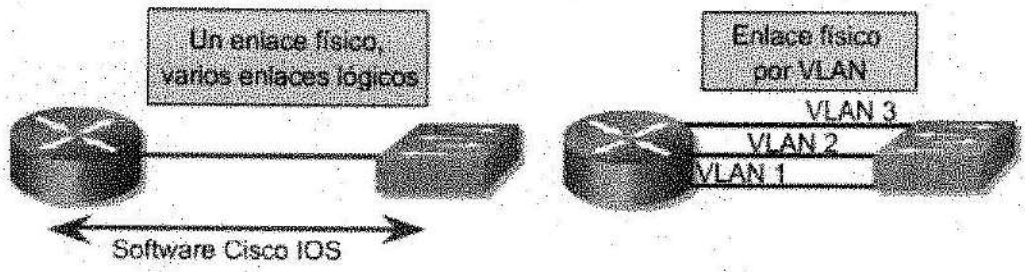
Requiere filtros, afecta el desempeño



- Asignado por el usuario de acuerdo a las direcciones MAC
- Ofrece flexibilidad, pero aumenta el gasto
- Tiene impacto sobre el desempeño, la escalabilidad y la administración
- Ofrece un proceso similar para las capas superiores

Membresía por dirección MAC

Dos enfoques de topología física



El uso de los routers de Capa 3 para conectar las VLAN ofrece los siguientes beneficios:

- Seguridad y gestión adicional
- Enlaces lógicos conservan los puertos físicos
- Los routers controlan el acceso a las VLAN
- Se pueden admitir hasta 255 VLAN o más por router

Comunicación entre las VLAN

Tipos de VLAN	Descripción
Basado en puerto	• Método de configuración más común • Los puertos se asignan individualmente, en grupos, en filas o en 2 o más switches • Uso sencillo • Se implementa a menudo donde el Protocolo de Control de Host Dinámico (DHCP) se usa para asignar las direcciones IP a los hosts de red
Dirección MAC	• Se implementa con escasa frecuencia hoy en día • Es necesario introducir y configurar cada dirección de forma individual • Los usuarios lo consideran útil • Administración, diagnóstico de fallas y gestión difíciles
Basado en protocolo	• Se configuran como las direcciones MAC, pero usan una dirección lógica o IP • Ya no son comunes debido a DHCP

VLAN basadas en puerto
VLAN basadas en direcciones MAC
VLAN basadas en protocolo
La cantidad de VLAN en un *switch* varía según diversos factores:

Patrones de tráfico
Tipos de aplicaciones
Necesidades de administración de red
Aspectos comunes del grupo
El esquema de direccionamiento IP es otra consideración importante al definir la cantidad de VLAN en un *switch*.

Por ejemplo, una red que usa una máscara de 24 bits para definir una subred tiene en total 254 direcciones de *host* permitidas en una subred. Dado que es altamente recomendada una correspondencia de uno a uno entre las VLAN y las subredes IP, no puede haber más de 254 dispositivos en una VLAN. También se recomienda que las VLAN no se extiendan fuera del dominio de Capa 2 del *switch* de distribución.

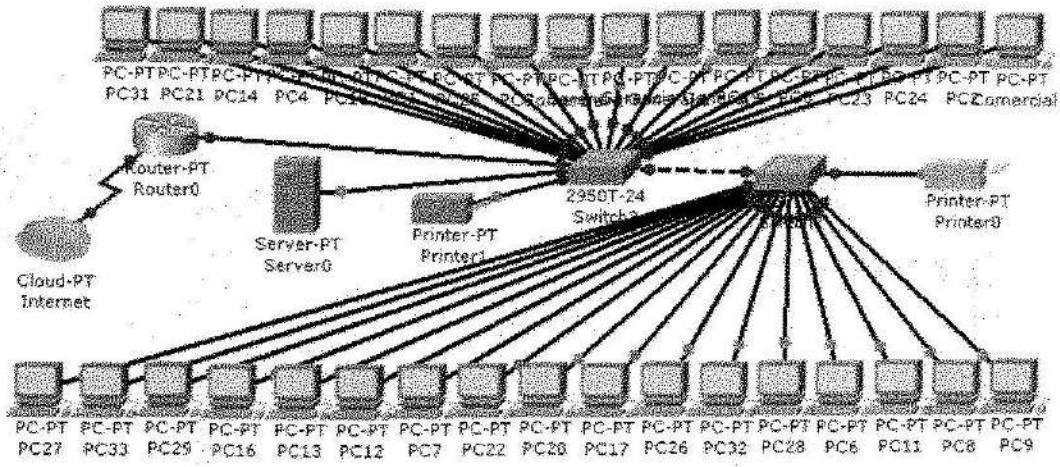
Existen dos métodos principales para el etiquetado de tramas: el enlace *Inter-Switch* (ISL) y 802.1Q. ISL es un protocolo propietario de Cisco y antiguamente era el más común, pero está siendo reemplazado por el etiquetado de trama estándar IEEE 802.1Q.

Etiquetado	Método	Medios	Descripción
Enlace Inter-Switch (ISL)	Fast Ethernet	El encabezado ISL encapsula la trama de la LAN y hay un campo de ID de VLAN en el encabezado ISL	La longitud de la trama se aumenta
802.1Q	Fast Ethernet	Protocolo VLAN Ethernet definido por IEEE	El encabezado se modifica
Emulación de LAN (LANE)	ATM	No hay etiquetas	La conexión virtual supone la existencia de un ID de VLAN

A medida que los paquetes son recibidos por el *switch* desde cualquier dispositivo de estación final conectado, se agrega un identificador único de paquetes dentro de cada encabezado. Esta información de encabezado designa la asociación de VLAN de cada paquete. El paquete se envía entonces a los *switches* o *routers* correspondientes sobre la base del identificador de VLAN y la dirección MAC. Al alcanzar el nodo destino, el ID de VLAN es eliminado del paquete por el *switch* adyacente y es enviado al dispositivo conectado. El etiquetado de paquetes brinda un mecanismo para controlar el flujo de *broadcasts* y aplicaciones, mientras que no interfiere con la red y las aplicaciones. La emulación de LAN (LANE) es una forma en que una red de Modo de Transferencia Asíncrona (ATM) simula una red *Ethernet*. No hay etiquetado en LANE, pero la conexión virtual utilizada implica un ID de VLAN.

8. ESTADO ACTUAL DE LA COMPAÑÍA OPTIMIZA

Optimiza cuenta con 36 estaciones de trabajo, todas en buen estado, cada uno de los cuales se conecta a la red. Las instalaciones están en perfecto estado, toda la red se conecta por medio de canaletas. En el cuarto de Telecomunicaciones, cuenta con un *Router* CISCO REF. 1700 (ETB conexión Internet), un *Switch* marca TRENDNET, un *Switch* marca D_link, una UPS y un servidor. Las instalaciones en este cuarto no están muy bien organizadas, en los *Raks* no se diferencia bien un equipo de otro y asimismo se cuentan con equipos sueltos, el cuarto de telecomunicaciones no presenta problemas de humedad, pero si de ventilación, debido a que se encuentra completamente encerrado y no cuenta con sistemas de ventilación alguno.



8.1 Cuarto de Cableado

El cuarto de cableado se encuentra en malas condiciones por:

- No tiene buena iluminación.
- No tiene ningún tipo de climatización.
- Se encuentra desordenado y sucio.
- En el *rack* los equipos no se distinguen y los cables están regados por todos los lados, esto hace que no se pueda identificar cada dispositivo
- El servidor se encuentra ubicado a la entrada del cuarto de cableado, por ser tan pequeño este cuarto se corre el riesgo que por accidente cualquier persona lo puede voltear.
- El acceso al personal no esta restringido, no existe ningún tipo de seguridad para acceder a el.

8.2 Componentes del Centro de Cableado

Equipo	Características	Conexión (cable)
Servidor	2 tarjetas de red, Pentium III de 900 Mhz, 512 *Ram*, 3 Discos Duros de 18 GB c/u.	
Router cisco REF. 1700	(ETB conexión Internet)	La conexión del *Router* al *Switch* TRENDNET esta hecha con cable UTP categoría 6.
Switch	24 puertos 10/100 mbps, marca TRENDNET	La conexión del *Switch* TRENDNET al *Switch* D_link esta hecha con cable UTP categoría 6.
Switch	24 puertos marca D_link	
UPS		

Las conexiones de los *Switch* a los *host* están hechas con cable UTP categoría 5e. La topología utilizada para esta red es de Árbol.

Nota: los *switch* y *router* no están colocados correctamente en el *rack* están sueltos.

8.3 Host

Nombre de equipos	Total por área
Comercial 1-2	2
Gerencia General 1-2	2
Financiero 1-2	2
Contabilidad 1-2	2
Tesorería 1	1
Archivo 1	1
Facturación 1	1
Producción 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15	15
Cartera 1	1
Nomina 1-2	2
Administrativa 1-2	2
Sistemas 1-2-3	3
Impresoras de red	2

8.4 *Topología*

En la empresa OPTIMIZA manejan una estructura de red en árbol, la cual es similar a la topología en estrella extendida; la diferencia principal es que no tiene un nodo central.

8.5 Descripción de los *switch*

- TRENDnet TEG-S2400I

24 PUERTOS 10/100 MBPS SNMP *Switch* con opción de modulo *gigabit*

El TEG-S2400i de TRENDnet es un *Switch* capa 2 de alto rendimiento con administración SNMP basada en web y provee 24 puertos 10/100 mbps y una entrada para un modulo *gigabit*. La entra del modulo *gigabit* permite tanto fibra como cobre, dando flexibilidad de conexión a servidores de *gigabit* o *backbones gigabit*. Soporta VLAN. El TEG-S2400i de TRENDnet es poderoso y fácil de usar, reduciendo tráfico innecesario y mejorando la seguridad de la red, a demás tiene las siguientes características:

- 24 puertos Ethernet/Fast Ethernet 10/100Mbps.
- Entrada para modulo gigabit que soporta los siguientes módulos opcionales: 1puerto 100Base-FX, 2 puertos 100Base-FX, 2 puertos gigabit cobre, 1 puerto gigabit fibra o 2 puertos gigabit fibra.
- Modo de transferencia Full/Half-duplex en cada puerto 10/100Mbps.
- Control de flujo IEEE 802.3x para operación full-duplex.
- 14K direcciones MAC y 4K entradas VLAN por dispositivo.
- 3MB buffer de paquetes y 1MB buffer de control por dispositivo.
- Soporta port-based VLAN (26 grupos), IEEE 802.1Q Tag-based VLAN y IEEE 802.1P port-based Quality of Service (QoS).
- Tasa de transferencia de datos:
- Ethernet: 14,880 pps
- Fast Ethernet: 148,800 pps
- Gigabit Ethernet: 1,488,000 pps

- D-Link DES 1024D - Switch- 24 puertos

- Tipo de dispositivo: Conmutador
- Factor de forma: Externo
- Dimensiones (Ancho x Profundidad x Altura) 28 cm x 18 cm x 4.4 cm
- Peso 1.9 kg
- Cantidad de puertos 24 x *Ethernet* 10Base-T, *Ethernet* 100Base-TX
- Velocidad de transferencia de datos: 100 Mbps
- Protocolo de interconexión de datos *Ethernet*, *Fast Ethernet*

- Características Control de flujo, capacidad *duplex*, conmutador MDI/MDIX.
- Cantidad de puertos 24 x *Ethernet* 10Base-T, *Ethernet* 100Base-TX.
- Velocidad de transferencia de datos: 100 Mbps.
- Protocolo de interconexión de datos *Ethernet, Fast Ethernet.*
- Tecnología de conectividad Cableado.
- Protocolo de conmutación *Ethernet.*
- Tamaño de tabla de dirección MAC 8K de entradas.
- Interfaces 24 x red - Ethernet 10Base-T/100Base-TX - RJ-45.
- Dispositivo de alimentación: Fuente de alimentación.
- Voltaje necesario : CA 100/240 V (50/60 Hz).
- Consumo eléctrico en funcionamiento: 10 vatios.

La empresa OPTIMIZA maneja un servidor DHCP para todos los equipos conectados a la red en, el servidor manejan direcciones estáticas, no se manejan VLAN debido a que la mayoría de *switch* con que cuentan, no tienen puerto de configuración por consola, solo cuentan con un *switch* que soporta VLAN pero no tiene configuración alguna.

8.6 Router CISCO 1700

10/100 BASET MODULAR ADSL IN
Descripción del producto Cisco 1701 ADSL *Security Access Router* – encaminador.

Proporciona un rápido, fiable y seguro acceso a Internet y a redes remotas a través de diferentes tecnologías de acceso WAN de alta velocidad. Ofrece una extensa familia de características de seguridad integradas. También proporciona una vía de acceso a servicios como la Voz por IP o "*Voice-over-IP*" y telefónica IP a través de la convergencia de las redes de voz y datos que ofrecen servicios de procesamiento de llamada y calidad de servicio, a demás tiene las siguientes características:

- Factor de forma Externo – modular
- Características Capacidad: *duplex*, negociación automática, soporte VLAN
- Dimensiones: (Ancho x Profundidad x Altura) 28.4 cm x 22.1 cm x 7.9 cm
- Peso: 1.3 kg
- Alimentación: CA 110/230 V (50/60 Hz)
- Memoria RAM 64 MB (instalados) / 96 MB (máx.)
- Tipo de dispositivo: Encaminador
- Protocolo de interconexión de datos *Ethernet*, ISDN, *Fast Ethernet*
- Memoria Flash 32 MB (instalados) / 32 MB (máx.)

- Interfaces 1 x módem - ADSL (WAN) ¦ 1 x módem - ISDN BRI ¦ 1 x red – *Ethernet* 10Base-T/100Base-TX - RJ-45 ¦ 1 x gestión - auxiliar - RJ-45 ¦ 1 x gestión - consola - RJ-45.
- Total ranuras de expansión (libres) Memoria ¦ 1 (1) x Ranura de expansión.
- Cables incluidos 1 x adaptador serie ¦ 1 x cable de módem ¦ 1 x cable de red ¦ 1 x cable serie.
- Características Capacidad *duplex*, negociación automática, soporte VLAN.
- Protocolo de interconexión de datos *Ethernet*, ISDN, *Fast Ethernet* .
- Indicadores de estado Actividad de enlace, estado de colisión, modo puerto *duplex*, alimentación, tinta OK.
- Dispositivo de alimentación Adaptador de corriente – externa.

8.7 Aplicaciones Usadas por Optimiza

8.7.1 Servidor ISA

Microsoft Internet Security and Acceleration (ISA) es la solución de caché Web, servidor de seguridad avanzado en el nivel de aplicación y red privada virtual (VPN) que permite obtener el máximo provecho de las inversiones en tecnologías de la información existentes al mejorar la seguridad de la red y el rendimiento.

ISA Server ofrece una protección avanzada, facilidad de uso y acceso rápido y seguro para todo tipo de redes. Resulta especialmente conveniente para proteger redes donde se utilizan aplicaciones de Microsoft, como Microsoft *Outlook Web Access* (OWA), Servicios de Microsoft *Internet Information Server*, entre otras.

ISA Server 2004 contiene un servidor de seguridad del nivel de aplicación con multitud de características que ayuda a proteger a las organizaciones de todos los tamaños frente a amenazas, tanto internas como externas, realiza una inspección minuciosa de protocolos de Internet, como el Protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*), que le permite detectar numerosas amenazas que se escapaban a los servidores de seguridad tradicionales. El servidor de seguridad integrado y la arquitectura de VPN de ISA Server permiten el filtrado y la inspección con estado de todo el tráfico VPN. También posibilita la inspección de los clientes VPN para soluciones de cuarentena basadas, con lo que contribuye a proteger las redes frente a ataques que se producen a través de una conexión VPN.

Manejan el programa ISA Server 2000 así mismo un servidor wins para validación de usuarios, contraseñas y permisos en la red, cada área tiene acceso solo a la información requerida de esta forma el área de contabilidad solo tiene acceso a la información útil para ellos

8.7.2 Suite de oficina Microsoft Office

Microsoft Office System proporciona los componentes básicos para crear soluciones que ayudarán a alcanzar los siguientes objetivos:

- Proporcionar a los usuarios empresariales mejor acceso a la información, de forma que puedan obtener conocimientos más profundos y tomar medidas más eficaces.
- Mejorar la capacidad de la organización para anticipar, administrar y responder a los cambios del mercado.
- Permitir que los equipos y las organizaciones colaboren con rapidez y agilidad.
- Aumentar la productividad individual y el número de usuarios que participan en entornos cada vez más exigentes.

8.7.3 Sistema Administrativo Uno

El sistema UNO es un conjunto de soluciones informáticas integradas linealmente que permiten llevar un registro y control permanente de la información para la automatización en las diferentes áreas. En ella se toma todo el módulo financiero que abarca: tesorería, cartera por pagar, cartera por cobrar, contabilidad activos fijos, y lo compenetra con el sistema comercial y manufactura. Cumple así con la condición fundamental de integración, que lo cataloga sin lugar a duda como un sistema a la altura de las más reconocidas ERP del mundo.

8.7.4 Servidor WINS

Los servidores de Servicio de nombres Internet de Windows (WINS) asignan dinámicamente direcciones IP a nombres de equipo (nombres *NetBIOS*). Esto permite a los usuarios tener acceso a los recursos a través del nombre del equipo en lugar de a través de la dirección IP.

9. PROPUESTA DE MEJORAMIENTO

De acuerdo a la investigación realizada en OPTIMIZA vamos a presentar una propuesta la cual dividiremos en fases para su óptimo desarrollo y desempeño. Estas fases serán secuénciales a corto mediano y largo plazo en un término de 7 u 8 meses, de acuerdo a las necesidades requeridas por los procesos y actividades de la organización.

En la verificación de la rede lógica se encontró que no hay grupos de usuario ni políticas informáticas de seguridad, establecidas en la compañía. Es por esto que se evaluara que tipo de usuarios se conectan y cual es la transferencia de datos que estos utilizan en la red.

9.1 Capa física

Reestructuración de la red

9.2 Cableado

La configuración de los cables debe cumplir con la norma **ANSI/EIA/TIA-569**.

- Normalización del cableado: etiquetas, identificación, señalización.
- Colocación de cables
- Introducción de los cables en los *patch panels*
- Prueba de cables
- Documentación de cables
- Instalación de *switches*
- Configuración de los *switches*
- Instalación y configuración de los PCs

9.3 Normatividad

Para el caso especifico de OPTIMIZA nos basaremos en la norma EIA/TIA-606 la cual se basa en el etiquetado del cableado.

9.3.1 Especificaciones EIA/TIA-606

• La norma EIA/TIA-606 especifica que cada unidad determinación hardware debe tener algún tipo de identificador único.

• Se recomienda la utilización de nomenclatura neutra "PC de María" no es válida porque María tal vez dentro de tres meses no trabajará en la empresa y no se sabrá a qué equipo corresponde.
• Se recomienda utilizar un identificador de sala y un identificador de conector, de esta forma podemos saber a qué conector de qué sala se refiere el cableado en si.
• Tendremos que etiquetar con el mismo nombre los dos extremos del cable y los conectores de pared o suelo.
• Es recomendable utilizar una nomenclatura que nos indique los dos extremos del cable.
–P.E. 21PC2-01PP1P1 (Sala 21 PC2 a Sala 101 Patch Panel 1(puerto 1).

9.4 Implementación VLSM

Se propone implementar VLSM (MASCARA DE SUBRED DE LONGITUD VARIABLE) para dividir la red existente en varias subredes. Esta división pretende solucionar el problema actual de la compañía con respecto a la falta de direcciones, además brinda seguridad, maximiza la eficiencia de la red facilitando el direccionamiento y hace más fácil la administración, configuración y monitoreo de la red.

Los equipos disponibles actualmente en la empresa soportan los servicios de VLSM por lo cual no se generaría ningún costo en cuanto a dispositivos de hardware.

Ahora mostraremos la forma de realizar la segmentación de la red utilizando VLSM.

Tomamos una dirección privada de clase C (ahora se hará de esta forma ya que no podemos trabajar con la dirección de red de la compañía).
RED 192.168.0.0 /24 MASCARA 255.255.255.0

Teniendo en cuenta el tamaño de la empresa se realizo la agrupación en subredes lógicas de la siguiente manera:

Nombre del área	Equipos por área	Subred lógica
Comercial	2	Subred área administrativa
Gerencia General	2	Subred área administrativa
Financiero	2	Subred área administrativa
Contabilidad	2	Subred área administrativa
Tesorería	1	Subred área administrativa
Archivo	1	Subred área de producción
Facturación	1	Subred área administrativa

Producción	15	Subred área de producción
Cartera	1	Subred área administrativa
Nomina	2	Subred área administrativa
Administrativa	2	Subred área administrativa
Sistemas	3	Subred área administrativa
Impresoras	2	Subred área de producción

Se utiliza una mascara de red de 26 bits 255.255.255.192 como se muestra en la siguiente tabla:

Subred	Equipos activos	Id Subred	Intervalo	*Broadcast*	Dirección para *host*	Mascara subred
área administrativa	18	192.168.0.32/26	192.168.0.33 - 192.168.0.62	192.168.0.63	62	255.255.255.192
área de producción	18	192.168.0.64/26	192.168.0.65 - 192.168.0.94	192.168.0.95	62	255.255.255.192

Como se muestra en la tabla anterior, esta división se tendrá una capacidad de aumento de los *host* en la red.

Ahora se tendrán que configurar el servidor DHCP para que asigne las direcciones IP de acuerdo al área a la que corresponda cada *host*.

También se tendrá que configurar el *router* con la nueva configuración de la red para que brinde enrutamiento de paquetes entre las *VLAN's*.

9.5 Implementación VLAN

Se propone implementar VLAN subdividir la red en grupos lógicos agrupados por áreas funcionales. Esta división contribuirá aun mas a brindar seguridad, aumentar la eficiencia de la red y facilitar la administración, configuración y monitoreo de la red.

La agrupación de las VLAN se hará teniendo en cuenta las subredes presentadas en la división hecha con VLSM así:

Subred	VLAN	Id. subred	Intervalo	Broadcast	Mascara de subred
Área administrativa	Área administrativa	192.168.0.32 /26	192.168.0.33 - 192.168.0.62	192.168.0.63	255.255.255.192
Área producción	Área Producción	192.168.0.64 /26	192.168.0.65 - 192.168.0.94	192.168.0.95	255.255.255.192

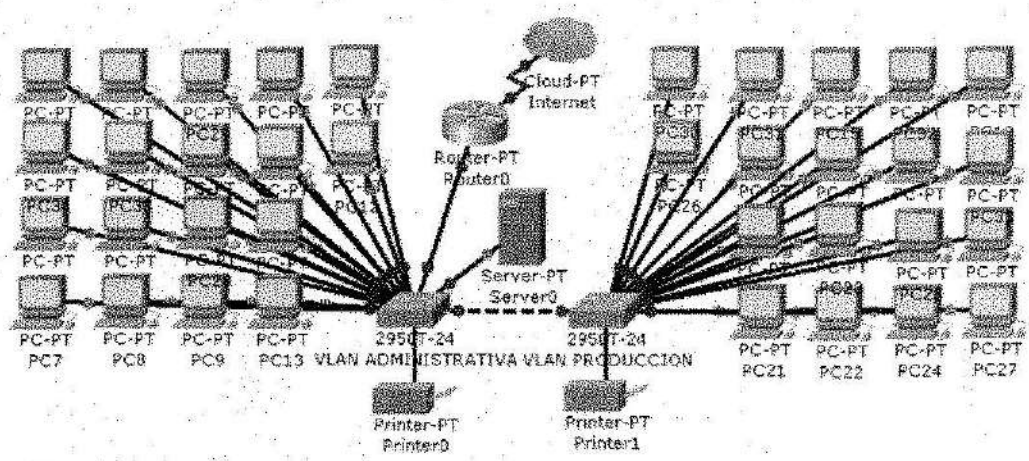
Ahora se tendrán que configurar los *switches* para que administrar las VLAN y también los *router* para brindar enrutamiento entre las VLAN.

9.6 Costos

Dependiendo las necesidades de la empresa OPTIMIZA anexamos cuadro de costos describiendo cada ITEM con su respectivo tiempo de instalación y compra y por supuesto su valor estimado.

Adecuación centro de cableado y nuevos tramos de cable		
Descripción	**Tiempo Aprox.**	**Valor**
Aire acondicionado para centro de cableado	8 DIAS	$ 1.500.000
Ventilación *Racks*	8 DIAS	$ 300.000
Etiquetación	2 DIAS	$ 150.000
Cableado nuevo (tramos que se necesitan)	15 DIAS	$ 305.000
Mano de obra calificada	6 DIAS	$ 1.500.000
TOTAL	**39 DIAS**	**$ 3.755.000**

10. DIAGRAMA FINAL DE LA RED



10. CRONOGRAMA

12. CONCLUSIONES

Al aplicar la propuesta de la modificación de la red, se garantizará un trabajo más óptimo, no solo en el funcionamiento de la red si no en su administración.

Se certifica que la red será más segura debido a la segmentación por departamento.

Se minimizarán las caídas de la red por el mejoramiento de cableado y la organización del mismo.

Al implementar políticas de seguridad y restricciones en el cuarto de cableado, se asegura la estabilidad física de los equipos, sin que exista la intervención de terceros.

Al aplicar un correcto diseño de VLAN, se tendrá un mejor nivel de seguridad y aprovechamiento de la red.

13. BIBLIOGRAFÍA

ROMERO, Juan Carlos. Estudio de *Subnetting*, *Vlsm*, CIDR y Comandos de Administración y Configuración de *Routers*. http://www.monografias.com/trabajos35/subnetting-vlsm/subnetting-vlsm.shtml

Wikimedia Foundation, Inc., Topología de red http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

Martínez, Evelio. ESTÁNDARES DE CABLEADO (Par trenzado UTP), 1997 http://www.eveliux.com/fundatel/cableado.html

Puigdemunt , Eduard i Gelabert. Puertos. 1999 http://www.pchardware.org/puertos.php

Ing García, Jorge Álvarez. FUNDAMENTOS DE NETWORKING. http://members.fortunecity.es/unitec/resumen2.htm

Sankar, Krishna. Cisco Wireless LAN Security: : Expert Guidance for Securing Your 802.11 Networks. Cisco Press, 2004. 419 páginas

Barnes, David. Sakandar, Basir. Cisco LAN Switching Fundamentals. Cisco Press, 2004. 408 páginas

ACADEMIA DE NETWORKING DE CISCO SYSTEMS CCNA 3 Y 4. 3E, Cisco Systems (Pearson Educación). 944