Universidad Tecnológica de El Salvador

FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS
CARRERA TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

T E M A:

"IMPLEMENTACION DE UNA PLATAFORMA DE SEGURIDAD EN UNA RED PARA EL MEJOR FUNCIONAMIENTO DE LOS RECURSOS INFORMATICOS DE BUFETE MADRIGAL GOMEZ E HIJOS"

TRABAJO DE GRADUACIÓN PRESENTADO POR:
JORGE ALBERTO CARRANZA GÓMEZ
WILLIAM ALEXANDER MARTÍNEZ LÓPEZ
LUIS RODRIGO PALOMO QUIÑONEZ

PARA OPTAR AL GRADO DE:
TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

SEPTIEMBRE, 2009

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

PAGINA DE AUTORIDADES

Lic. JOSE MAURICIO LOUCEL
RECTOR

Ing. NELSON ZÁRATE SÁNCHEZ
VICERRECTOR ACADÉMICO

Ing. LORENA DUQUE DE RODRÍGUEZ
DECANO

JURADO EXAMINADOR

Ing. SIGIFREDO EDUARDO PORTILLO
SEGUNDO VOCAL

Ing. VICENTE ZARCEÑO
PRIMER VOCAL

Ing. EDUARDO ELISEO PEÑATE
PRESIDENTE

SEPTIEMBRE, 2009

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

Agradecimientos

Doy gracias a DIOS todopoderoso de todo corazón por haberme brindado escalar un peldaño más, y darme el conocimiento y fuerza necesaria para concluir con mis estudios a corto plazo.

Agradezco de una manera muy especial a todas y cada una de las personas que nos brindaron su apoyo y colaboración desinteresada, durante la realización de nuestro trabajo de graduación.

Especialmente a nuestros familiares y amigos:

Elena Isabel López De Martínez, Jesús Martínez Cañas. Gustavo Adolfo Portillo

A nuestro asesor: Ing. Vicente Zarceño

A nuestros compañeros de trabajo:

Jorge Alberto Carranza, Luis Rodrigo Palomo. Por su incondicional apoyo durante el ultimo trayecto de nuestro trabajo de graduación, por ser unos compañeros con un enorme potencial de conocimiento para llegar al éxito, muchas bendiciones.

William Alexander Martínez López

Agradecimientos

A DIOS TODOPODEROSO:

Por haberme dado la oportunidad de poder culminar mi carrera con éxito, por su fortaleza espiritual, por la perseverancia que puso en mí para poder alcanzar esta meta y por estar conmigo todos los días de mi vida.

A MI FAMILIA:

Gracias por el apoyo brindado, por sus consejos y por creer en mí, a mí hermano, mis primos, mis tías, mi tío y mi abuelita.

A MIS AMIGOS:

Por su apoyo en el desarrollo de este trabajo y por su amistad.

A MI ASESOR:

Vicente Zarceño, por su paciencia y tiempo dedicado, por ayudarme a salir Adelante, por la asesoría que siempre nos brindó a lo largo del proceso.

A ALGUIEN MUY ESPECIAL:

Por haberme apoyado durante todo este tiempo, por su paciencia y por el fruto otorgado al final de esta carrera.

Jorge Alberto Carranza Gómez

Agradecimientos

En primer lugar le dedico estos agradecimientos a Dios todopoderoso que supo darme la fuerza necesaria para desarrollar con éxito la tesis de graduación.

En segundo lugar agradezco a mis compañeros de tesis por tener la paciencia suficiente para poder realizar esta tesis junta y poder superar tantos obstáculos que se nos presentaron.

En tercer lugar agradezco a nuestro asesor Vicente Zarceño toda la ayuda y el apoyo que nos brindo en este tiempo para desarrollar con éxito nuestra tesis de graduación

Por último lugar agradezco a mi familia porque sin ella no habría podido terminar mis estudios ya que ellos fueron el soporte para el desarrollo de mis estudios, siempre han sido mi inspiración para todos mis estudios y por eso les dedico este éxito y todos los vendrán en mi vida.

Luis Rodrigo Palomo Quiñonez

INDICE

CAPITULO I

GENERALIDADES DEL PROYECTO

1.1 Situación Problemática

La red informática del Bufete Madrigal se encuentra trabajando con anormalidades puesto que se nota en ciertas horas una lentitud desde las estaciones de trabajo, cuando los usuarios realizan sus operaciones cotidianas como buscar archivos con formato Microsoft Word en el servidor, ver correo electrónico, imprimir documentos, etc., este tipo de tráfico ocasiona saturación en la red, puesto que las computadoras se congelan por momentos, aunque no debería de suceder ese tipo de fallas en la red por ser tareas que en teoría son de poco utilización de ancho de banda pero la utilización de diferentes programas que utilizan la red y que no son parte del trabajo diario (navegar por diversión, chateo, mandarse archivos de gran tamaño por la red, bajar archivos de música, películas etc.) demuestran que el rendimiento de la misma reduce su funcionalidad, y crea congestionamiento en los diferentes paquetes de información, los programas que trabajan en línea (conectados a Internet) no son auditados en sus procedimientos por algún tipo de documento o normativa técnica. Sin hablar la posible existencia de alguna PC infectada con un Spyware o Malware (Parásitos) que provocan tormentas de broadcast sin razón y de esa forma no importando que tarea realice el usuario siempre encontrara saturada la red y sin control alguno para ubicar el nodo que presenta la falla aparente. Cuando se encuentra trabajando la transmisión de información en las diferentes unidades o departamentos que se encuentran interconectadas bajo el

ambiente de red, utilizan recursos del servidor de archivos que está trabajando en línea con programas de aplicación y procesos administrativos en cada punto de conexión, ver fig. 1.

Otra situación importante dentro del esquema es el usuario que por desconocimiento del entorno de la red, realiza procedimientos erróneos en los programas de aplicación que se encuentran trabajando en línea con las demás terminales de la red y a su vez afecta el rendimiento de la misma.

El bajo rendimiento de la Red Informática posee parámetros claros que no benefician al desarrollo del funcionamiento de la Red Técnica, es de tener en cuenta el gran congestionamiento en la red por el volumen de información manejada, el equipo con características técnicas de Hardware mínimos (switch no administrable), la confiabilidad con la seguridad tanto de información como de usuarios sin la autorización registrada al Servidor de Archivos en uso.

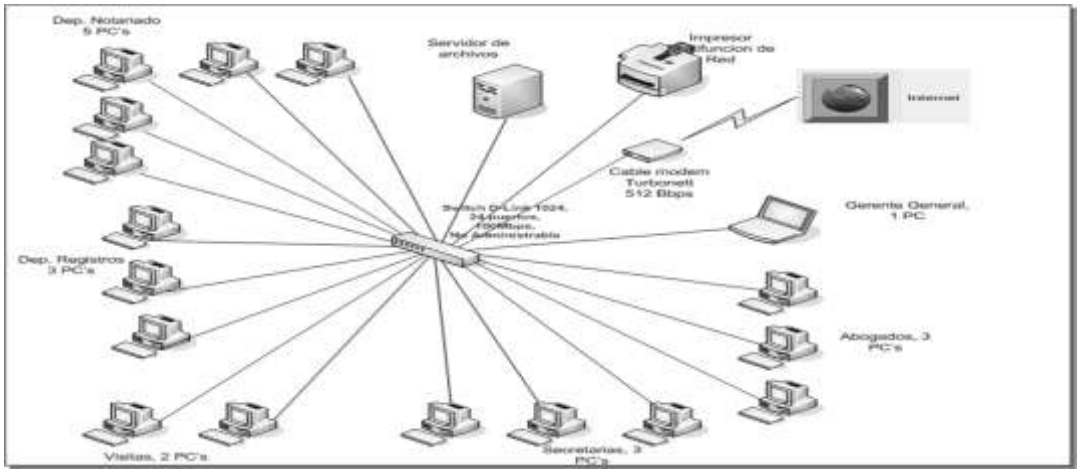


Fig. 1 red Actual, 19 equipos conectados en un edificio de 3 plantas.

1.2 Justificación de la investigación

Dada la problemática que presenta la red Informática del Bufete Madrigal Gómez e Hijos, se realizó una propuesta de una plataforma de seguridad básica orientada desde los equipos de comunicación para optimizar el rendimiento de la red Técnica – Jurídica. Es importante la investigación ya que con ello se pretende mejorar la seguridad, control, acceso y rendimiento. Se lograra lo siguiente:

- ✓ Habrá una red más segura en un 35% por el hecho de que ninguna red es 100% seguro y sobre todo porque nuestra plataforma de seguridad está orientada desde los equipos de comunicación contra ataques de cualquier tipo de anomalía tipo spyware que son los mayores causantes de lentitud en la red y los equipos, ya que muchos de ellos saturan la red con tormentas de broadcast.
- ✓ Habrá un control de acceso seguro para la red.
- ✓ Se logrará una plataforma de seguridad básica basada en hardware que es una administración de control de flujo.
- ✓ Se regulará el acceso a internet por cada puesto y departamento de la compañía, esto se realizara con la aplicación de ACL en cada departamento.
- ✓ Se evaluará segmentación de la red para reducir los dominios de broadcast, ya que se consta de 19 equipos conectados, de esa manera será más eficiente la red por tener dominios de broadcast reducidos y por departamentos (Notariado, Registros, Secretarias, Abogados, Servidor, Visitas) y de esa manera mantener la congestión en

VLAN separadas y con acceso cada uno de ellos solamente a los recursos necesarios y no en un solo dominio como se maneja actualmente.

- ✓ Se evaluará la instalación de antivirus, para reducir y tener un filtro donde que permitirá reducir las amenazas de trasferencias de virus y parásitos por el uso de memorias USB.
- ✓ La adquisición de tecnología para la compañía tiene que ser según la plática con el Gerente General de forma paulatina y gradual, ya que hay que aprovechar los recursos que se tienen actualmente (Cableado estructurado cat 5e, patchpanel Cat5e, servidor de archivos con Windows 2003 Server Standard) para posteriormente poder adquirir la tecnología necesaria para lograr un nivel mayor de seguridad y de acceso requerido.

1.3 Delimitación

1.3.1 Delimitación geográfica

El bufete está ubicado en la 87 Avenida Norte No. 147, Col. Escalón, San Salvador, El Salvador, C.A.

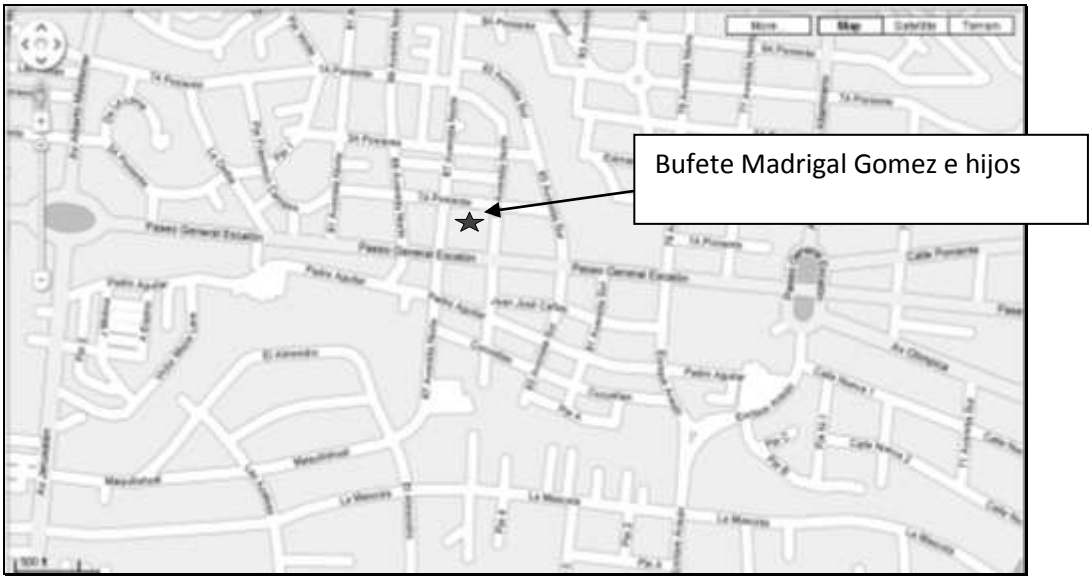


Fig. 2. Ubicación actual del bufete

1.3.2 Delimitación temporal

La implementación de la plataforma de seguridad en el acceso, control de acceso a internet y el rendimiento de la red Informática del Bufete Madrigal Gómez e Hijos tomara un tiempo empezando desde el 12 de Febrero de 2009 y finalizando el 6 de Junio de 2009.

1.3.3 Delimitación organizacional

El desarrollo del proyecto es solamente en la oficina central del bufete, ubicada en San Salvador solamente.

1.3.4 Delimitación específica

La investigación de la propuesta de seguridad en el acceso, control de acceso a internet y rendimiento de la red Informática del Bufete Madrigal Gómez e Hijos se realizó en las instalaciones del bufete, analizando los procesos técnicos, manejo de paquetes, evaluación del entorno de trabajo y la red de transmisión de datos, los diferentes equipos de computación desde las terminales al Servidor de Archivos, localización de la recepción de información y el despacho de los diferentes paquetes de aplicación por los usuarios que interactúan a diario con cada flujo técnico de Información.

1.4 Objetivos

1.4.1 Objetivo General

Realizar la implementación de una plataforma de seguridad de red, para mejorar el funcionamiento de los recursos informáticos del bufete Madrigal Gómez e hijos.

1.4.2 Objetivo Específico

- ✓ Realizar un estudio técnico para la evaluación del reemplazo de equipos de comunicación que proporcionen flexibilidad para la administración de la red del bufete Madrigal Gómez e hijos.
- ✓ Montaje de equipos de comunicación que serán proporcionados por el grupo de tesis.
- ✓ Implementación y análisis de configuraciones de los equipos de comunicación para implantar la seguridad de acceso a la red partiendo de la distribución física de los departamentos del bufete Madrigal Gómez e hijos e implementación de políticas de seguridad para tener restricciones de acceso a la red así como la actualización de antivirus para mejorar el rendimiento de los equipos finales.

1.5 Alcances

1- Por medio del estudio técnico de los equipos actuales de comunicación se obtiene la información idónea para la selección de los equipos que deben de ser reemplazados de la red actual del bufete Madrigal Gómez e hijos.

2- Sustituir los equipos que posee el bufete, por equipo más sofisticado y administrable como son Router Cisco Serie 800 y Switch Cisco 2950 con más opciones de administración que faciliten desarrollar niveles de seguridad básica basada en hardware.

3- Brindar acceso seguro a los recursos de la red obteniendo altos niveles de seguridad básica basada en hardware para mejorar su funcionabilidad a fin de resguardar y garantizar la información del bufete Madrigal Gómez e hijos.

1.6 Documentación Técnica

1.6.1 ¿Qué se entiende por seguridad en una red LAN?

Seguridad en una red LAN es un tema grandísimo pero de forma general se puede decir que es permitir o denegar cualquier tipo de servicio a los usuarios de una red, acceso a internet, acceso a correo electrónico, acceso a recursos compartidos, acceso a la red misma, acceso a servidores, etc.

1.6.2 ¿Que es una red LAN?

Una LAN es una red de área local de una empresa, es decir equipos interconectados por un medio y equipos de concentración y que entre ellas utilizan los recursos compartidos llámense impresoras, internet, servidores, correo electrónico, entre otros.

1.6.3 ¿Que es una WAN?

Una WAN es una red de área extensa, es decir una red que interconecta equipos a nivel continental, entre países y equipos que se encuentran en diferentes ubicaciones y entre ellos hay una enorme distancia y es necesario contar con proveedores de enlaces que nos permitan dicha conexión caso contrario no podremos alcanzar la conexión entre equipos de redes locales externas.

Esta seguridad puede ser administrada dependiendo de la complejidad que se requiera por servidores y políticas de seguridad, por equipos de comunicación llámense Switches

y Routers, por VLAN y ACL y por el mismo control de los niveles o privilegios que les den a los usuarios de la red

1.6.4 ¿Qué es un switch?

Un switch es el encargado de brindar conexión entre los diferentes equipos de una red local, permite una conexión de uno a uno de sus puertos, gracias a la tecnología de conmutación y a la creación de su tabla de direcciones que está asociada los puertos del equipo con cada dirección Mac Address que se conecte a él, es por ello que se conoce al switch como el equipo más utilizado así como la razón por la cual están sustituyendo a los tan conocidos HUB que no tenían estas tecnologías y congestionaban la red. Los switches administrables son capaces de brindar una seguridad por puerto, y a su vez también permiten la creación de redes privadas virtuales, VLAN para optimizar el uso de la red en segmentos más seguros y fiables.

1.6.5 ¿Que es un Router?

Es un dispositivo de red inteligente que opera a nivel de capa 3 del modelo OSI que permite interconectar redes de datos que no pertenecen al mismo rango de direcciones, y que tengan diferentes protocolos de comunicación, así como también permite dar salida de una LAN hacia una WAN de forma que funciona el dispositivo que brinda acceso a la red de redes Internet para una red local de una empresa. Hay varios modelos de Router dependiendo de la marca y modelo, unos permiten una administración sencilla y de fácil utilización como los usados de forma casera y otros pueden ser muy robustos

que tienen una administración más compleja pero que permiten una administración más minuciosa y estricta que ofrece mucha seguridad para el acceso y ruteo de la información de los equipos de la red LAN se encuentren.

1.6.6 ¿Qué es una VLAN?

Una red Virtual de Área Local, VLAN es una segmentación de una red en varias redes virtuales es decir de una red se puede crear varias redes virtuales que aunque estén conectadas al mismo switch no se pueden ver entre ellas porque son virtualmente redes separadas lógicamente y no será posible su interconexión a no ser que se tenga un router en esa red que permite la conexión entre esas redes. El objetivo de crear VLAN en una red local es independizar los dominios de broadcast y que sean más pequeños aunque serian varios dominios con poco congestionamiento, pero se optimiza la red porque el caso contrario sería crear un solo dominio de broadcast que produciría lentitud y retraso en la entrega de paquetes y por ende todas sus aplicaciones que se utilicen.

1.6.7 ¿Qué son las listas de control de acceso, ACL?

Son mecanismos lógicos que permiten realizar una especie de control o filtrado de la información que uno desea que salga o ingrese en nuestra red, estos controles se configuran en las interfaces de los router, sean éstas interfaces seriales o interfaces de red (Ethernet, Fast Ethernet, etc.)

Se dividen en 2 tipos, ACL estándar, donde se utiliza un rango numérico entre 1 y 99 para identificarlas, su sintaxis es sencilla y solo tenemos que especificar una dirección de origen.

Access-list 1 permit host 172.17.3.10

access-list 1 deny 172.17.3.0 0.0.0.255

Access-list 1 permit any

La ACL extendida en la cual se puede definir el protocolo así como también direcciones o rangos de direcciones de origen o destino, prácticamente de lo más especifico a lo más general y funciona como un filtro. Su sintaxis es la siguiente:

```
access-list 101 permit ip host 172.17.3.10 host 172.16.0.1
access-list 101 deny ip 172.17.3.0 0.0.0.255 host 172.16.0.1
access-list 101 permit ip any any

access-list 102 permit icmp any host 172.16.0.1
access-list 102 permit tcp any host 172.16.0.1 eq www
```

Listas de Control de Acceso, el uso de ellas en un router necesita la creación de un listado si bien pueden ser restricciones también pueden ser líneas que permitan un acceso especifico por puerto o dirección IP, de forma más general se puede restringir o permitir el acceso o salida de la red desde el router, de manera que solamente el administrador de la red puede ingresar al equipo para poder modificar dicha lista de restricciones.

1.6.8 Router CISCO series 800

Fig 3. Router cisco series 800

El router Cisco series 800 aunque en su fabricación soporta la administración de ACL, soporta VLAN, ofrece una mayor fiabilidad y seguridad de la red a través del poder de Cisco IOS ® Software tecnología adaptada para las pequeñas oficinas.

El router tiene características de seguridad mejoradas, como un cortafuegos de estado y de seguridad IP (IPSec) para permitir el cifrado VPN. Estas características permiten a pequeñas oficinas realizar sus negocios a través de Internet al tiempo que se protegen los valiosos recursos.

El router Cisco 800 extiende el poder de la tecnología del software Cisco IOS a las pequeñas oficinas. Cisco IOS Software ofrece mayor seguridad, fiabilidad y seguridad de inversión, combinado con un bajo coste de propiedad, para permitir que los clientes se beneficien del aumento de la productividad, la simplificación de la comunicación, y la reducción de los costos. El router Cisco 800 permite a los clientes beneficiarse de servicios de valor añadido tales como servicios de red gestionados, redes privadas virtuales (VPN), de punto de venta (POS), aplicaciones y acceso seguro a Internet.

Características Técnicas

Característica	**Beneficio**
Norma de Seguridad	
PAP, CHAP, MS-CHAP, y ACL	• Protege la red de accesos no autorizados
Ruta del router y la autenticación	• Acepta las actualizaciones de tabla de enrutamiento sólo se conocen los routers, velar por que no exista información corruptos de fuentes desconocidas se recibe
Seguridad reforzada	
Cisco IOS Firewall de conjunto de características	• Ofertas de los usuarios internos seguro, por aplicación dinámica ACL para todo el tráfico a través de los perímetros • Defiende y protege los recursos contra el router de denegación de servicio ataques • Los controles y las cabeceras de paquetes de gotas paquetes sospechosos • Protege contra desconocidos, los applets de Java maliciosos • Detalles de las operaciones para la presentación de informes para cada aplicación, por característica base
Cifrado IPSec (DES y 3DES)	• Garantiza la integridad de los datos y la autenticidad de origen mediante el uso de la encriptación basada en estándares • Proporciona seguridad para todos los usuarios de la LAN sin configuración de cada PC
Confiabilidad superior	

Cisco IOS Software de la tecnología	• Una tecnología que se utiliza en toda la columna vertebral de Internet
Router standalone	• Proporciona acceso a Internet a múltiples usuarios sin depender de un servidor dedicado o PC, si un usuario de la LAN falla, otros usuarios pueden acceder a Internet
Gestión	
Cisco Configmaker, SNMP, Servicio de fiabilidad (SA) de agente, TACAS +	• Interfaz gráfica de usuario (GUI) basada en las ventanas de configuración de herramientas para los usuarios novatos • Gestión y supervisión remota a través de SNMP o Telnet y la gestión local a través de puerto de consola
Inversiones seguras	
Sobre el terreno de memoria ampliable	• Permite a los clientes añadir características como las necesidades de ampliar la creación de redes
Avanzada arquitectura de procesador y la memoria	• Garantiza la plataforma puede soportar el procesador aplicaciones
Asistencia en todo el mundo	• Ayuda a los clientes a mantener sus routers Cisco serie 805 corriendo todo el tiempo
Bajo costo de propiedad	
Reducir los costes en 15periféricos.	• Permite a los clientes utilizar los conocimientos existentes de Cisco IOS Software para la instalación y la capacidad de administración
Optimización del ancho de banda	
Calidad de servicio (QoS) y ponderado Feria cola	• Garantiza tiempos de respuesta consistente para múltiples aplicaciones de la asignación de ancho de banda inteligente • Da la prioridad más importante de aplicaciones de uso de la línea de la WAN

Elección de encapsulado (Point-to-Point Protocol [PPP], de alto nivel de enlace de datos de control [HDLC], Frame Relay)	• Garantiza la compatibilidad con la red existente
"Instantánea" de enrutamiento de IP y de Internetwork Packet Exchange (IPX)	• Permite el uso eficiente de ancho de banda disponible
De paquetes de datos X.25	• Permite la transferencia de datos mediante redes X.25
Instalación y Configuración simplificada	
NAT	• Permite a las empresas la conservación de valiosas direcciones IP • Reduce el tiempo y los costos mediante la reducción de la dirección IP de gestión de
Cisco IOS Software de fácil de propiedad intelectual	• Permite verdadera movilidad cliente direcciones IP se configura a través de la transparencia de Cisco IOS Protocolo de control de dinámica de host (DHCP) cada vez que un cliente enciende
Con códigos de color y los cables y los puertos de inicio rápido Manual de referencia	• Ayuda a los usuarios a hacer las conexiones • Proporciona fácil de seguir las instrucciones de instalación

1.6.9 CISCO Switch Catalyst 2950 Series

Switches Ethernet Inteligentes Catalyst 2950: Las series Cisco Catalyst 2950 es una línea de dispositivos de configuración fija, apilables e independientes, que entregan conectividad Fast Ethernet y Giga bit Ethernet a velocidades de cable para redes de tamaño mediano. Esta es la familia de switches de Cisco con precios más asequibles. Cuando se agrega con un switch de los series Catalyst 3550, la solución queda activada para routing IP desde el extremo al core de la red.

Fig. 4.cisco switch catalyst 2950

El Cisco Catalyst ® 2950 Series es una línea de configuración fija, apilables, y los conmutadores independientes que proporcionan alambre velocidad Fast Ethernet y Giga bit Ethernet. Esta línea de productos ofrece dos conjuntos de funciones de software y

una amplia gama de configuraciones para que las pequeñas, medianas y sucursales de empresas, y ambientes industriales para seleccionar la combinación correcta para la red. La imagen estándar (SI) Las ofertas de software Cisco IOS ® para funcionalidad básica de datos, vídeo y servicios de voz. Para las redes de los requisitos de seguridad adicionales, avanzada calidad de servicio (QoS) y alta disponibilidad, la Mejora de la imagen (IE) ofrece servicios inteligentes de software tales como la limitación de velocidad y filtrado de seguridad para el despliegue en la red.
Duras para los entornos de red, el nuevo Cisco Catalyst 2955 Series son los interruptores de grado industrial que son ideales para la industria de soluciones de redes (Ethernet despliegues industriales), sistemas de transporte inteligentes (ITS), y soluciones de red de transporte. También es adecuado para muchas de utilidad militar y aplicaciones de mercado donde las condiciones ambientales exceder las especificaciones de los productos comerciales de conmutación.

Catalizador en cuenta en todos los conmutadores de 2950 y 2955 es el Cisco Clúster Management Suite (CMS) de software, que permite a los usuarios configurar y solucionar problemas de forma simultánea múltiples conmutadores Catalizador de escritorio utilizando un navegador web estándar

CAPITULO II

PROYECTO TEMÁTICO

2.1 Planteamiento del proyecto temático

El desarrollo de este proyecto ha conllevado a la realización de diferentes etapas para poder desarrollar una propuesta de una herramienta que sea capaz de brindar seguridad en la red del bufete Madrigal Gómez e hijos.

Dentro de las fases que se realizaran, para dicho proyecto podemos mencionar las siguientes:

Fase 1: Estudio técnico e investigación tecnológica para implementar la plataforma de seguridad en el bufete Madrigal Gómez e hijos.

En esta etapa se centrara en la investigación de todos los contenidos técnicos y los estudios que se deben de realizar para poder tener un buen análisis.

Esta fase comprende tres etapas las cuales son:

1. Identificar y analizar las necesidades a cubrir:

-Se contactará al jefe del bufete madrigal Gómez e hijos con quien se analizarán las necesidades actuales que tienen el bufete Madrigal Gómez e hijos, relacionado con la seguridad y la conectividad que se tiene en los diferentes departamentos.

-Se definirá la estructura, objetivos, alcances, contenido y reportes que se presentarán en el documento que contendrá el estudio técnico.

2- Describir de forma general las diferentes opciones de tecnologías disponibles:

Se hará una búsqueda de información en diferentes recursos tales como internet, libros, revistas técnicas, etc., que permita conocer parte de las tecnologías disponibles para la implementación de la plataforma de seguridad de la red, para tener una descripción general de las diferentes características, ventajas y desventajas para presentarlas al jefe del bufete Madrigal Gómez e hijos, que le servirá para conocer de forma general las tecnologías.

3- Elaboración del estudio técnico:

En esta etapa se elaborará el documento técnico el cual será presentado al jefe del bufete Madrigal Gómez e hijos para que pueda tener una idea de la plataforma de seguridad que se le va a implementar.

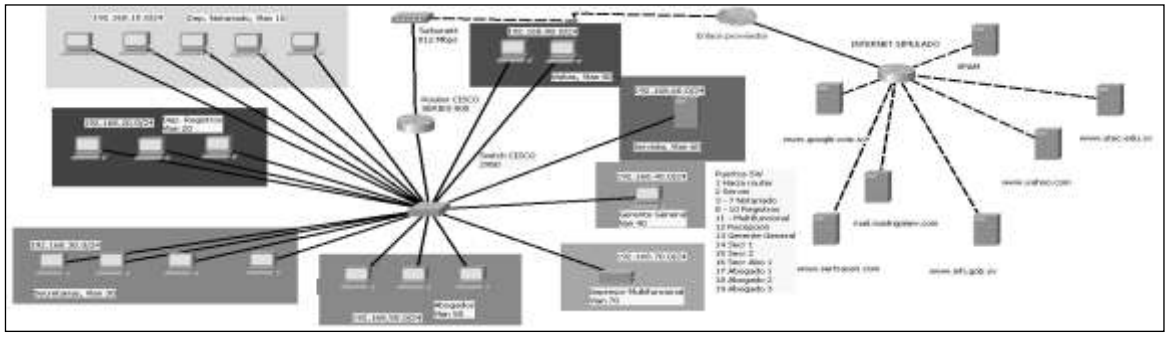


Fig. 5. Diagrama propuesto, creación de VLAN por departamento y restricciones por ACL, Archivos de configuración en Anexos.

Fase 2: Montaje de equipos de comunicación y mantenimiento preventivo del cableado estructurado.

En esta etapa se realizara el montaje de los equipos de comunicación, además daremos mantenimiento preventivo al cableado estructurado, todo esto para dejar en un buen funcionamiento toda la parte física del bufete Madrigal Gómez e hijos.

Los equipos que vamos a instalar son tecnología de CISCO, las cuales son un ROUTER CISCO SERIES 800 que nos va a servir para poder realizar las ACL, que son un tipo de seguridad que se pueden aplicar a diferentes departamentos.

Además utilizaremos un Switch Ethernet Inteligentes Catalyst 2950 que nos brindara las ventajas para poder realizar las VLAN para optimizar la seguridad en los diferentes departamentos del bufete Madrigal Gómez e hijos.

Fase 3: configuraciones de los equipos de comunicación y desarrollo de las políticas de seguridad.

En esta etapa lo que se busca en primer lugar es configurar los diferentes equipos de comunicación de la plataforma de seguridad.

Además se espera que en esta etapa se puedan programar las diferentes políticas de seguridad que el jefe del bufete nos brindara para los diferentes departamentos, además se buscara la optimización de los recursos.

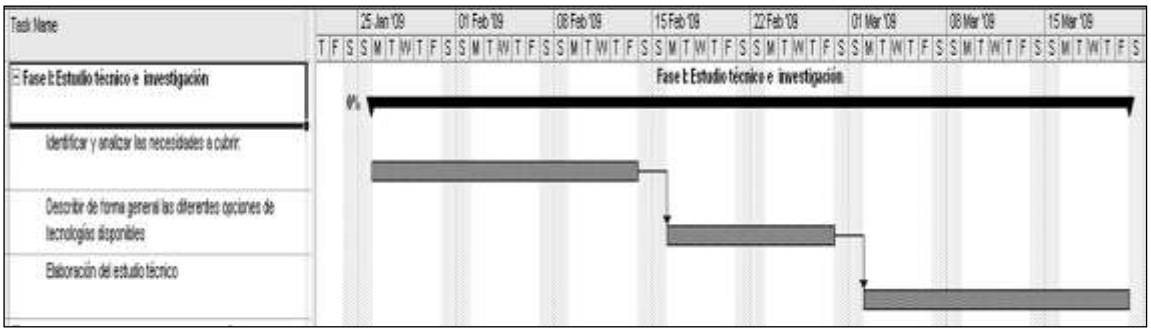
Luego realizaremos pruebas de funcionamiento de las ALC y de las Vlan para poder evaluar el buen funcionamiento de la plataforma de seguridad del bufete Madrigal

Gómez e hijos, en las cuales se verificará que la plataforma no esté provocando conflictos en las ACL y en las Vlan, ni que las políticas de seguridad afecten la comunicación de los diferentes departamentos.

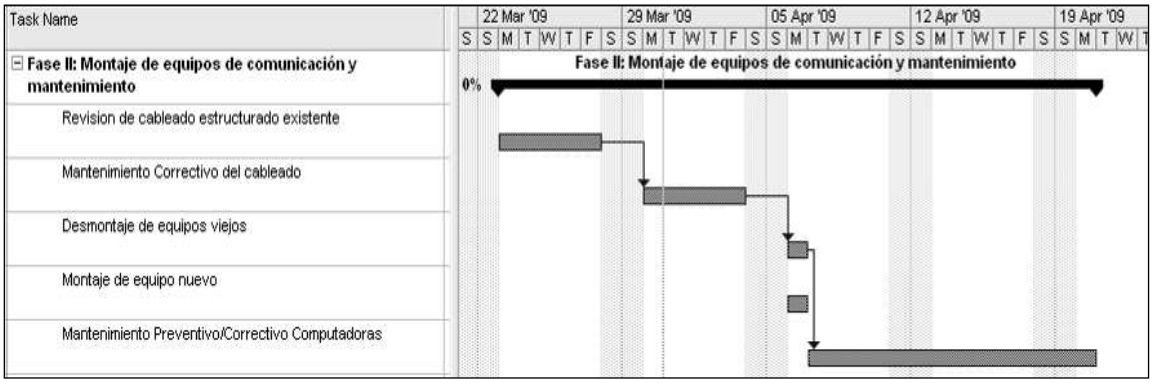
Además se evaluará el fácil uso que se tenga de la plataforma de seguridad con el usuario del bufete Madrigal Gómez e hijos, para que no tengan problemas en el desarrollo de su trabajo.

2.2 Cronograma de actividades

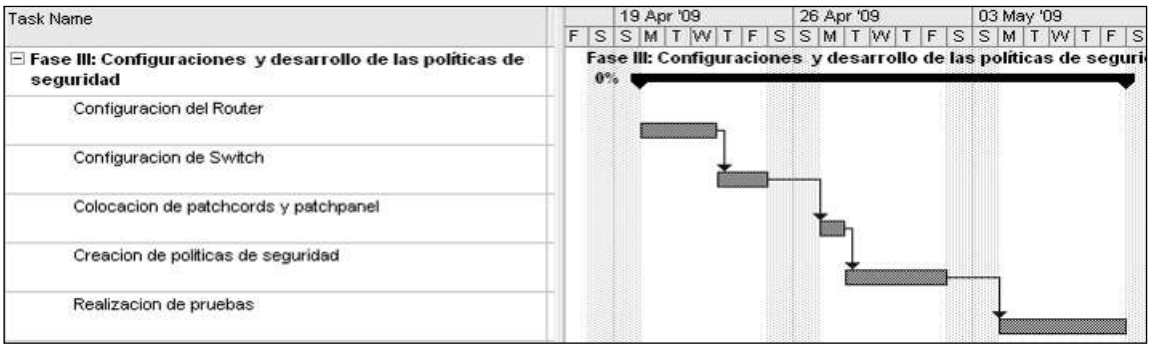
Fase I



Fase II



Fase III



2.3 Evaluación técnica y económica

2.3.1 Evaluación Técnica

EVALUACIÓN TÉCNICA DE ROUTERS SERÁ CONSIDERADO COMO APROBADO SI ALCANZA UNA PONDERACIÓN MÍNIMA DEL 80%								
Característica, atributo o elemento	Parámetro o valoración requerida	Peso	Opciones a evaluar					
			Producto 1 ROUTER CISCO SERIES 800		Producto 2 Router Dlink 520		Producto 3 Router Xtech	
			Calificación	Puntaje	Calificación	Puntaje	Calificación	Puntaje
1) Administrable	Permite administracion	30%	2	60	0	0	0	0
2) ACL	Soporta ACL	20%	2	40	0	0	0	0
3) VLAN	Soporta VLAN	10%	2	20	0	0	0	0
4) Ancho de banda puertos LAN Ethernet	100 Mbps	20%	1	20	0	0	0	0
5) Puerto LAN Ethernet	RJ45	5%	2	10	2	10	2	10
6) Puerto WAN Serial	Serial	5%	2	10	0	0	0	0
7) Puerto Consola	RJ45	10%	2	20	0	0	0	0
TOTALES		100%		180		10		10
PONDERACIÓN FINAL			90		10		10	
RESULTADO OBTENIDO			APROBADO		REPROBADO		REPROBADO	

EVALUACIÓN TÉCNICA DE SWITCHES SERÁ CONSIDERADO COMO APROBADO SI ALCANZA UNA PONDERACIÓN MÍNIMA DEL 80%								
Característica, elemento	Parámetro o valoración requerida	Peso	Opciones a evaluar					
			Producto 1 Switch CISCO Series 2690		Producto 2 Switch Dlink		Producto 3 Switch Xtech	
			Calificación	Puntaje	Calificación	Puntaje	Calificación	Puntaje
1) Administrable	Permite administracion	30%	2	60	0	0	0	0
2) VLAN	Soporta VLAN	20%	2	40	0	0	0	0
3) Puerto LAN Ethernet	48 puertos	10%	2	20	1	10	1	10
4) Puerto Consola	RJ45	20%	2	40	0	0	0	0
5) Ancho de Banda	100 Mbps	10%	2	20	1	10	1	10
TOTALES		90%		180		20		20
PONDERACIÓN FINAL			90		10		10	
RESULTADO OBTENIDO			APROBADO		REPROBADO		REPROBADO	

2.3.2 Evaluación Económica

Proveedor / Descripción	GBM	SISTEMAS CC	SERVICIOS GLOBALES	STC SOPORTE TECNICO CERTIFICADO	CET
Router Cisco Series 800	$ 2,500.00	$ 2,625.00	$ 2,005.00	$ 1000.00	$ 1,900.00
Switch Cisco 2950	$ 1,950.00	$ 2,005.00	$ 1,900.00	$ 800.00	$ 1,750.00
Totales	**$4,500.00**	**$4,630.00**	**$3,905.00**	**$1800.00**	**$3,650.00**

2.4 Presupuesto proyectado

Cliente: Bufete Madrigal Gómez e hijos.

Dirección: ubicada en la 87 Avenida Norte No. 147, Col. Escalón, San Salvador, El Salvador, C.A.

-El bufete Madrigal Gómez e hijos ya posee una estructura de red, para la cual no se va a necesitar invertir para la construcción de la red.

-El equipo físico (switch y router) serán comprados de segunda mano, con un costo entre los $800.00 cada uno de ellos.

- También se realizaran mantenimientos preventivos y correctivos en el cableado estructurado y equipos de computo finales si fuera necesario, esto se realizara para que no exista la posibilidad de que hubiesen fallas por mal funcionamiento de ellos y de esa forma estar seguros que todo queda funcionando bien tanto los equipos de comunicación como el cableado estructurado y los equipos finales.

Se ha considerado la creación de la configuración básica de los equipos, usuarios y contraseñas.

2.5 Oferta técnica

San salvador 19 de marzo del 2009

Señores
Bufete Madrigal Gómez e hijos
Presente.
Respetable señores:

Por este medio le presentamos la oferta técnica para la implementación de una plataforma de seguridad para la red.

Nuestra propuesta de Seguridad está basada en equipo marca Cisco, los cuales son administrables completamente, además de su reconocida capacidad a nivel mundial en el área de interworking; con nuestra solución el nivel de seguridad de su red se incrementará ya que la configuración de los equipos permitirá ejecutar controles bien específicos sobre los diferentes tipos de tráfico que circulan sobre la red LAN, aislando todo el tráfico innecesario proveniente de Internet, controlando los accesos de los usuarios, segmentando la red, denegando servicios y bloqueando puertos que pueden convertir a su red en vulnerable.

Como parte de nuestra solución se realizará lo siguiente: Se sustituirá el switch D-link que está actualmente y se instalará un switch CISCO, también proporciona seguridad en el acceso puesto que se aplicará la configuración de puerto seguro, y se segmentara la red en VLAN para protección de cada área de trabajo.

Se instalará un Router Series 800 el cual proporcionara interconexión entre la red local y la salida a internet que será proporcionado por un enlace ADSL (enlace

ADSL_Turbonett), pero no obstante se aplicara más seguridad con este equipo de forma que se emplearan Listas de Control de Acceso ACL para que los usuarios tengan un filtro por el cual salir o no salir al mundo público, así como mejor protección del servidor de archivos que contará con su zona desmilitarizada la cual, su servidor no será visto desde el exterior sino solo por los usuarios de la red local.

Se sustituirán los puntos de red que se encuentren defectuosos, se realizará mantenimiento del cableado y las cajas ortogonales, así como los conectores respectivos, re ponchado de patchpanel y cambios de patchcord, así como su respectiva identificación de los puntos de red.

Sin nada más que comentar y esperando que les guste nuestra propuesta nos despedimos cordialmente y que pasen un feliz día.

Atentamente.

Jorge Carranza	William Martínez	Luis Palomo

2.5.1 Oferta económica

San salvador junio del 2009

Señores

Bufete Madrigal Gómez e hijos

Presente.

Respetable señores:

Por este medio le presentamos la oferta económica para la implementación de una plataforma de seguridad.

El costo de esta plataforma en otros lugares es sumamente caro, pero estando consientes de la situación económica que existe a nivel mundial, ofrecemos una oferta sumamente económica para el beneficio de la empresa.

CANTIDAD	DESCRIPCION	PRECIO
1	Router Cisco Series 800	$1000.00
1	Switch Cisco 2950	$800.00
1	Análisis de red Actual	$250.00
1	configuración de Router	$550.00
1	Configuración de switch	$450.00
1	Mantenimiento Preventivo, Correctivo del cableado estructurado.	$350.00
1	Montaje de los Equipos de comunicación.	$200.00
1	Actualización del Sistema Operativo	$210.00
1	Documentación técnica de la red	$190.00
1	Creación de políticas de seguridad	$195.00
	Total	**$4195.00**

Al final garantizamos el buen funcionamiento de la plataforma de seguridad.

Esperamos que nuestros servicios satisfagan las necesidades de su empresa y esperando su respuesta nos despedimos con bendiciones y éxitos.

Atentamente

Jorge Carranza	William Martínez	Luis Palomo

CONCLUSIONES

- El bufete Madrigal Gómez e Hijos cuentan con una red que no tiene protección de acceso ni ninguna aplicación de administración que controle el acceso de la red.

- El acceso a Internet a la red del Bufete Madrigal no está administrado, y no todos los usuarios necesitan salida a internet para el desarrollo del trabajo diario.

- El Bufete Madrigal tiene metas de crecer en un 50% en los próximos de 2 a 3 años y contemplan la posibilidad de tener sucursales en algún momento, y no tiene la capacidad de poder conectarse a otra red si no tiene el equipo necesario.

Recomendaciones

- Realizar un estudio técnico para diagnosticar problemas, esquemas, que proporcionen un preámbulo que permita conocer la situación actual y poder crear posibles soluciones.

- A partir del estudio técnico realizar un planteamiento de seguridad básica basada en hardware de red para lograr tener sectorizado cada departamento de red, y sus accesos de forma de reducir cada red en unas más pequeñas y de esa forma evitar congestiones de flujo de información en toda la red.

- Mantener una administración adecuada de los equipos, puesto que todo dependerá de dicha administración de los equipos de comunicación, puesto que de otra forma no podrán tener acceso a la red, aunque es una plataforma de seguridad básica es muy estable y de poca asistencia si no hay cambios en la red.

Bibliografía

-Academia cisco. *Libro CCNA exploration 1 y 2.* Primera edición. México. Cisco Systems. 2009.750 p.

-Fonseca Antonio, H. *Trabajo de graduación: apoyar la formación académica de los estudiantes católico palestino de San Luis Talpa a través de la implementación seguro a internet y del desarrollo de un sistema de acceso Web a servicios educativos virtuales.* San Salvador. Tesis. 2008. 200 p.

-Steve, M. *Interconexión de dispositivos de red cisco libro de autoestudio CCNA.* Segunda edición. Ciudad de México. Pearson Alhambra.2004. 488 p.

Monografias.com.*cableado estructurado, normas y estándares.* [en línea]. Lugar:monografias.com.2009.[consulta:15 de marzo del 2009]. http://www.monografias.com/trabajos11/cabes/cabes.shtml

Textoscientificos.com.*Creación de Vlans, conceptos y aplicaciones.* [en línea]. Lugar:textoscientificos.com.2008.[consulta:28 de marzo del 2009]. http://www.textoscientificos.com/redes/redes-virtuales

Monografias.com. *Información sobre subneteo VLSM.* [en línea]. Lugar:monografias.com. 2007.[consulta: 3 de abril del 2009]. http://www.monografias.com/trabajos67/ejercicio-subneteo/ejercicio-subneteo.shtml

Wordpress.com. *Blogs sobre router.* [en línea]. Lugar:wordpress.com.2006. [Consulta: 3 de abril del 2009]. http://es.wordpress.com/tag/router/\

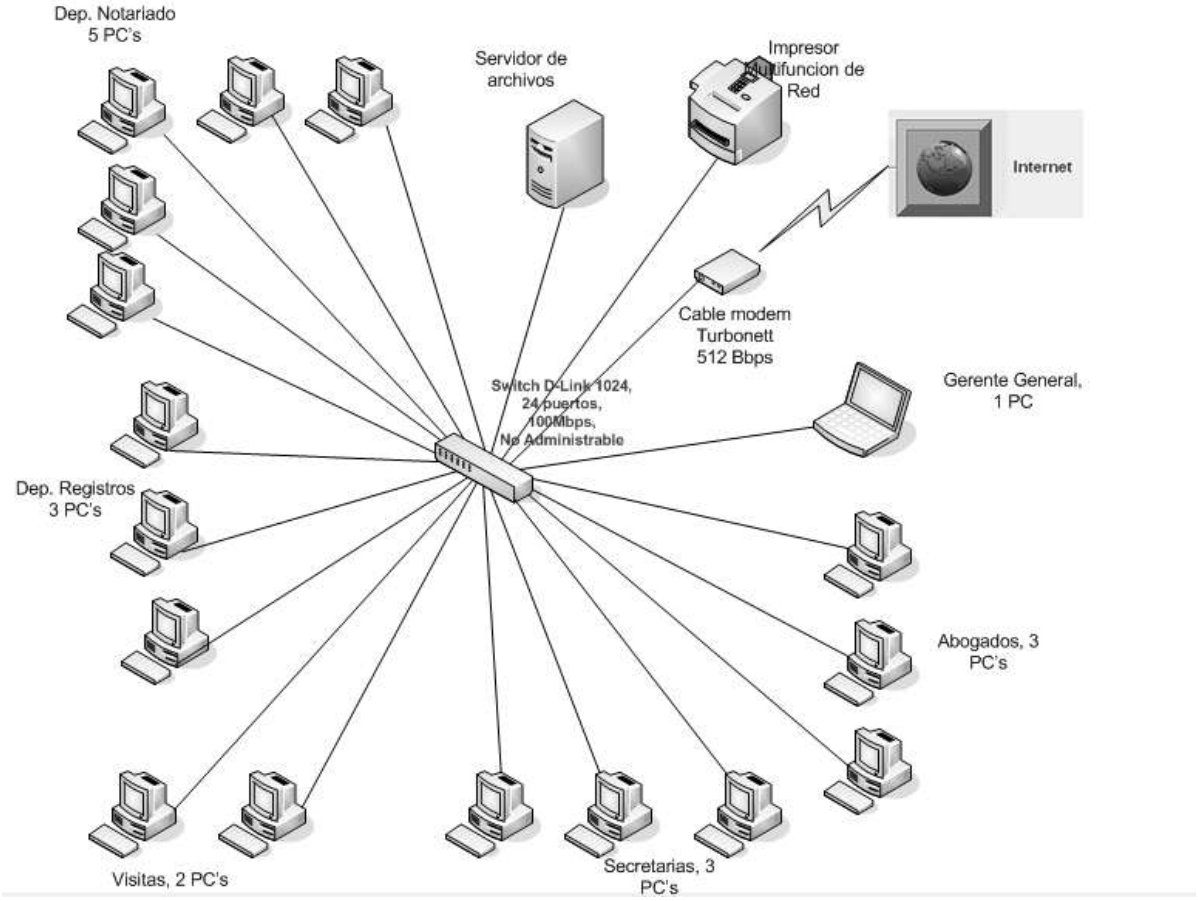
Aprenderedes.com.*Proceso de configuración de ACL*. [en línea]. Lugar:aprenderedes.com.2006.[consultado:25 de mayo del 2009]. http://aprenderedes.com/2006/11/03/proceso-de-configuracion-de-acl/

ANEXOS

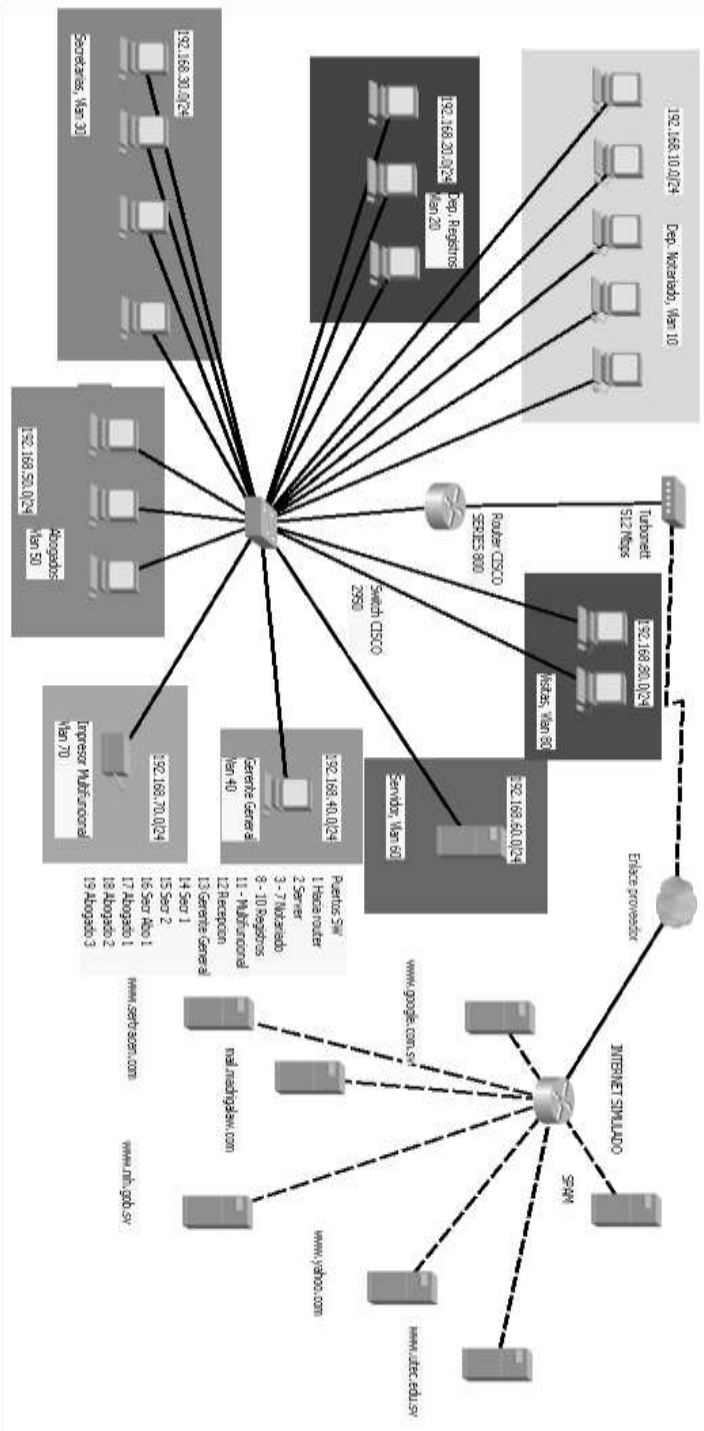
3.1 Subneteo para las diferentes Vlans

No	Host	Bits	Mask	Intervalo	Rango
10 Notariado	6	3	/29 (255.255.255.248)	0.0.0.7	192.168.10.0 - 192.168.10.7
20 Registros	6	3	/29 (255.255.255.248)	0.0.0.7	192.168.20.0 - 192.168.20.7
30 Secretarias	6	3	/29 (255.255.255.248)	0.0.0.7	192.168.30.0 - 192.168.30.7
40 Gerencia	2	2	/30 (255.255.255.252)	0.0.0.3	192.168.40.0 - 192.168.40.3
50 Abogados	6	3	/29 (255.255.255.248)	0.0.0.7	192.168.50.0 - 192.168.50.7
60 Servidor	2	2	/30 (255.255.255.252)	0.0.0.3	192.168.60.0 - 192.168.60.3
70 Impresores	2	2	/30 (255.255.255.252)	0.0.0.3	192.168.70.0 - 192.168.70.3
80 Visitas	6	3	/29 (255.255.255.248)	0.0.0.7	192.168.80.0 - 192.168.80.7

3.2 Diagrama de Red Actual Bufete Madrigal Gómez e Hijos



3.3 Diagrama de red propuesto Madrigal Gómez e Hijos



3.4 Configuración de Router

```
Router#sh runn
Building configuration...

Current configuration : 5907 bytes
version 12.4
no service password-encryption
hostname Router
!
!
enable secret 5 $1$mERr$NGWzcYUiBH/i5DS7.B7pT0
enable password utec
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.248
 ip access-group 110 in
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.248
 ip access-group 120 in
```

```
!
interface FastEthernet0/0.3
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.248
 ip access-group 130 in
!
interface FastEthernet0/0.4
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.252
 ip access-group 140 in
!
interface FastEthernet0/0.5
 encapsulation dot1Q 50
 ip address 192.168.50.1 255.255.255.248
 ip access-group 150 in
!
interface FastEthernet0/0.6
 encapsulation dot1Q 60
 ip address 192.168.60.1 255.255.255.252
 ip access-group 160 in
!
interface FastEthernet0/0.70
 encapsulation dot1Q 70
 ip address 192.168.70.1 255.255.255.252
 ip access-group 170 in
!
interface FastEthernet0/0.80
 encapsulation dot1Q 80
 ip address 192.168.80.1 255.255.255.248
 ip access-group 180 in
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.0.0.0
 ip access-group 105 in
```

```
 duplex auto
 speed auto
!
interface Serial0/2/0
 no ip address
 shutdown
!
interface Serial0/2/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
!
access-list 120 permit udp any any eq bootpc
access-list 120 permit udp any any eq bootps
access-list 120 permit ip any host 192.168.60.2
access-list 120 permit ip any host 192.168.70.2
access-list 120 permit ip any host 75.53.180.66
access-list 120 permit ip any host 201.247.241.5
access-list 120 permit ip any host 168.243.205.73
access-list 120 deny ip any any
access-list 130 permit udp any any eq bootpc
access-list 130 permit udp any any eq bootps
access-list 130 permit ip any host 192.168.60.2
access-list 130 permit ip any host 192.168.70.2
access-list 130 permit ip any host 75.53.180.66
access-list 130 deny ip any any
access-list 110 permit udp any any eq bootpc
```

access-list 110 permit udp any any eq bootps

access-list 110 permit ip any host 192.168.60.2

access-list 110 permit ip any host 192.168.70.2

access-list 110 permit ip any host 75.53.180.66

access-list 110 deny ip any any

access-list 140 permit udp any any eq bootpc

access-list 140 permit udp any any eq bootps

access-list 140 permit ip any host 192.168.60.2

access-list 140 permit ip any host 192.168.70.2

access-list 140 permit ip any host 75.53.180.66

access-list 140 deny ip any 192.168.10.0 0.0.0.255

access-list 140 deny ip any 192.168.20.0 0.0.0.255

access-list 140 deny ip any 192.168.30.0 0.0.0.255

access-list 140 deny ip any 192.168.50.0 0.0.0.255

access-list 140 deny ip any 192.168.80.0 0.0.0.255

access-list 140 permit ip any any

access-list 140 deny ip any any

access-list 150 permit udp any any eq bootpc

access-list 150 permit udp any any eq bootps

access-list 150 permit ip any host 192.168.60.2

access-list 150 permit ip any host 192.168.70.2

access-list 150 permit ip any host 75.53.180.66

access-list 150 deny ip any 192.168.10.0 0.0.0.255

access-list 150 deny ip any 192.168.20.0 0.0.0.255

access-list 150 deny ip any 192.168.30.0 0.0.0.255

access-list 150 deny ip any 192.168.50.0 0.0.0.255

access-list 150 deny ip any 192.168.80.0 0.0.0.255

access-list 150 permit ip any any

access-list 150 deny ip any any

access-list 160 permit ip any 192.168.10.0 0.0.0.7

access-list 160 permit ip any 192.168.20.0 0.0.0.7

access-list 160 permit ip any 192.168.30.0 0.0.0.7

access-list 160 permit ip any 192.168.40.0 0.0.0.3

access-list 160 permit ip any 192.168.50.0 0.0.0.7

```
access-list 160 deny tcp any any
access-list 170 permit ip any 192.168.10.0 0.0.0.7
access-list 170 permit ip any 192.168.20.0 0.0.0.7
access-list 170 permit ip any 192.168.30.0 0.0.0.7
access-list 170 permit ip any 192.168.40.0 0.0.0.3
access-list 170 permit ip any 192.168.50.0 0.0.0.7
access-list 170 deny tcp any any
access-list 180 permit udp any any eq bootpc
access-list 180 permit udp any any eq bootps
access-list 180 deny ip any 192.168.10.0 0.0.0.255
access-list 180 deny ip any 192.168.20.0 0.0.0.255
access-list 180 deny ip any 192.168.30.0 0.0.0.255
access-list 180 deny ip any 192.168.50.0 0.0.0.255
access-list 180 deny ip any 192.168.80.0 0.0.0.255
access-list 180 deny ip any 192.168.40.0 0.0.0.255
access-list 180 deny ip any 192.168.60.0 0.0.0.255
access-list 180 deny ip any 192.168.70.0 0.0.0.255
access-list 180 permit ip any any
access-list 180 deny ip any any
access-list 105 deny ip host 89.0.0.10 any
access-list 105 permit ip any any
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.40.1
ip dhcp excluded-address 192.168.50.1
ip dhcp excluded-address 192.168.60.1
ip dhcp excluded-address 192.168.70.1
ip dhcp excluded-address 192.168.80.1
!
ip dhcp pool NOTARIADO
 network 192.168.10.0 255.255.255.248
 default-router 192.168.10.1
```

```
 dns-server 192.168.60.2
ip dhcp pool REGISTROS
 network 192.168.20.0 255.255.255.248
 default-router 192.168.20.1
 dns-server 192.168.60.2
ip dhcp pool SECRETARIAS
 network 192.168.30.0 255.255.255.248
 default-router 192.168.30.1
 dns-server 192.168.60.2
ip dhcp pool ABOGADOS
 network 192.168.50.0 255.255.255.248
 default-router 192.168.50.1
 dns-server 192.168.60.2
ip dhcp pool VISITAS
 network 192.168.80.0 255.255.255.248
 default-router 192.168.80.1
 dns-server 192.168.60.2
ip dhcp pool GERENCIA
 network 192.168.40.0 255.255.255.252
 default-router 192.168.40.1
 dns-server 192.168.60.2
!
banner motd ^CADVERTENCIA... ESTA ENTRANDO A UN SISTEMA RESTRINGIDO, SI NO ES ADMINISTRADOR FAVOR CERRAR SESION^C
line con 0
 password utec
 login
line vty 0 4
 password redes
 login
!
!
End
```

3.5 Configuración de Switch

```
Switch#sh runn

Building configuration...


Current configuration : 4114 bytes

!

version 12.2

no service password-encryption

!

hostname Switch

!

enable secret 5 $1$mERr$NGWzcYUiBH/i5DS7.B7pT0

enable password utec

!

!

!

interface FastEthernet0/1

 switchport mode trunk

!

interface FastEthernet0/2

 description "PUERTO PERTENECIENTE A VLAN60 DE SERVIDOR"

 switchport access vlan 60

 switchport mode access

 switchport port-security mac-address sticky

!

interface FastEthernet0/3

 description "PUERTO PERTENECIENTE A VLAN10 DE NOTARIADO"

 switchport access vlan 10

 switchport mode access

 switchport port-security mac-address sticky

!

interface FastEthernet0/4

 description "PUERTO PERTENECIENTE A VLAN10 DE NOTARIADO"

 switchport access vlan 10
```

```
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 description "PUERTO PERTENECIENTE A VLAN10 DE NOTARIADO"
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 description "PUERTO PERTENECIENTE A VLAN10 DE NOTARIADO"
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 description "PUERTO PERTENECIENTE A VLAN10 DE NOTARIADO"
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 description "PUERTO PERTENECIENTE A VLAN20 DE REGISTROS"
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/9
 description "PUERTO PERTENECIENTE A VLAN20 DE REGISTROS"
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
```

```
 description "PUERTO PERTENECIENTE A VLAN20 DE REGISTROS"
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
!
interface FastEthernet0/12
 description "PUERTO PERTENECIENTE A VLAN30 DE SECRETARIAS"
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/13
 description "PUERTO PERTENECIENTE A VLAN70 DE IMPRESORAS"
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 description "PUERTO PERTENECIENTE A VLAN30 DE SECRETARIAS"
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/15
 description "PUERTO PERTENECIENTE A VLAN30 DE SECRETARIAS"
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 description "PUERTO PERTENECIENTE A VLAN30 DE SECRETARIAS"
 switchport access vlan 30
```

```
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/17
 description "PUERTO PERTENECIENTE A VLAN50 DE ABOGADOS"
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 description "PUERTO PERTENECIENTE A VLAN50 DE ABOGADOS"
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 description "PUERTO PERTENECIENTE A VLAN50 DE ABOGADOS"
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
!
interface FastEthernet0/21
 description "PUERTO PERTENECIENTE A VLAN80 DE VISITAS"
 switchport access vlan 80
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/22
 description "PUERTO PERTENECIENTE A VLAN80 DE VISITAS"
 switchport access vlan 80
 switchport mode access
 switchport port-security mac-address sticky
```

```
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd ^CADVERTENCIA... ESTA ENTRANDO A UN SISTEMA RESTRINGIDO, SI NO ES ADMINISTRADOR FAVOR CERRAR SESION^C
line con 0
 password utec
 login
!
line vty 0 4
 password redes
 login
line vty 5 15
 login
!
!
End
```