# UNIVERSIDAD POLITÉCNICA SALESIANA
# SEDE QUITO

**CARRERA: INGENIERÍA ELECTRÓNICA**

**Tesis previa a la obtención del título de: INGENIERO ELECTRÓNICO**

**TEMA:**

**ANÁLISIS Y DISEÑO DE LA RED DE FRONTERA (BORDE) DE LA CASA INSPECTORIAL SALESIANA UBICADA EN LA CIUDAD DE QUITO EN EL SECTOR EL GIRÓN.**

**AUTOR:**

**ANTONIO LEONARDO SUÁREZ FARINANGO**

**DIRECTOR:**

**VERÓNICA EMMA SORIA MALDONADO**

**Quito, febrero del 2015**

**DECLARACIÓN DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL PROYECTO DE GRADO**

Yo autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Quito, enero del 2015

---

ANTONIO LEONARDO SUÁREZ FARINANGO

CI: 171809885-6

## DEDICATORIA

Dedico este proyecto de titulación a mi familia, a mi mamita que fue el pilar fundamental en este proyecto, a mi papi que supo aconsejarme hasta conseguir este tan anhelado título, a mis hermanos por el apoyo y a quien fue un pilar fundamental en el desempeño y culminación de mi carrera profesional, mi hijita Valerie Camila y a mi esposita Jessica que a pesar de todas las adversidades logramos culminar una de nuestras metas. Y a todos quienes con su paciencia supieron darme un apoyo incondicional y además emocional para llegar a obtener este tan anhelado título de profesional.

Antonio Leonardo Suárez Farinango

## AGRADECIMIENTO

Agradezco a mi tutor Ing. Verónica Soria, quien con su valiosa paciencia y asesoramiento ayudó al desempeño del proyecto de titulación. A mi lector Ing. Jorge Lopéz, por sus sugerencias empleadas para culminar el proyecto de titulación. Tambien agradezco a mis amigos que supieron estar incondicionalmente y sobre todo a mis amigas con quienes hoy culminare una meta más en mi proyecto de vida María Cristina López y a mi linda esposa Jessica Espinoza.

Antonio Leonardo Suárez Farinango

# ÍNDICE

## ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

## RESUMEN

El diseño y análisis del presente proyecto se basa en la intercomunicación de la Casa Inspectorial Salesiana con sus obras a nivel nacional, en la infraestructura actual no cuentan con los equipos necesarios para establecer una comunicación en la que se va a basar en los rediseños: de campus y los módulos remotos. El presente diseño hace referencia al diseño y selección de equipos necesarios para obtener una comunicación efectiva y garantizar la calidad de servicio, para pasar algunas aplicaciones, las cuales son telefonía VoIP y videoconferencia. Los equipos con los que se van a diseñar, tanto en el campus como en los módulos remotos son los adecuados para el diseño, ya que soportan protocolos de enrutamiento y calidad de servicio.

El diseño es un modelo de cisco CEAM (Cisco Enterprise Architecture Model) en el que el modelo Cisco Enterprise Architecture mantiene el concepto de componentes de capa de distribución y de acceso que conectan a los usuarios, los servicios WAN, y granjas de servidores a través de un backbone de campus de alta velocidad. Los equipos para el diseño son: ASA, WSA, Bluecoat. Las funciones de estos dispositivos marca Cisco cumplen funciones de firewall, VPN y servidor proxy.

En conclusión este proyecto tiene como finalidad la intercomunicación entre la matriz la cual es la Casa Inspectorial Salesiana y las obras, mediante esta comunicación lo que se pretende es pasar aplicaciones como telefonía y videoconferencia, por líneas arrendadas de los ISP, esto dependerá de los enlaces y el ancho de banda requerido para no tener pérdidas y garantizar calidad de servicio.

## ABSTRACT

The design and analysis of this project is based on the intercom Salesian provincial house with his works at the national level, the current infrastructure does not have the equipment necessary to establish a communication to be based on the redesign: Campus and the remote modules. This project refers to the different teams that will be designed for effective communication and ensure quality of service, to spend some applications, which are VoIP and video telephony. The teams we are going to design both the campus and the remote modules are suitable for the design, and supporting routing protocols and quality of service.

The design is a model of cisco CEAM (Cisco Enterprise Architecture Model) in which the Cisco Enterprise Architecture model retains the concept of distribution layer components and access to connect users, WAN services, and server farms through a backbone of high-speed campus. The teams for the design are: ASA, WSA, Bluecoat. The functions of these devices comply brand Cisco firewall, VPN and proxy server.

In conclusion, this project aims intercommunication between the matrix which is the Salesian Provincial House and the works by this paper the aim is to spend as telephony and videoconferencing applications for ISPs leased lines, this will depend on the links and the bandwidth required to avoid losses and guarantee quality of service.

# INTRODUCCIÓN

Hoy en día la tecnología se va ampliando para brindar un soporte eficiente, correspondiente a las necesidades de las empresas y/o de las organizaciones que se han hecho que se transfieran los esfuerzos para impulsar proyectos de renovación de infraestructura tecnológica en sistemas y redes de telecomunicaciones que logren cubrir las necesidades fundamentales de las empresas y se logre abastecer los servicios que demandan los equipos para las redes de comunicaciones en beneficio de la Casa Inspectorial Salesiana, además facilitar la administración a los usuarios finales, cuyas obras han hecho que cambie la metodología en cómo se administra las redes de las telecomunicaciones mediante herramientas y/o aplicaciones remotas, dando un cambio total a las funcionalidades y cierta parte a las redes de la información para que logren administrar eficientemente la nueva era de las tecnologías de comunicación, algunas aplicaciones a ser diseñadas son: video conferencia, telefonía VoIP, además el aumento de las industrias de las computadoras, se ha partido de acuerdo a la demanda de empresas y usuarios, en las que van implementando nuevos satélites para la intercomunicación de ciudad a ciudad o país a país, lo que ha permitido que muchas empresas opten por renovar su tecnología para mejorar y aumentar su productividad.
El diseño de este proyecto será para aplicar a una futura implementación de la Casa Inspectorial Salesiana. Y la intercomunicación con sus obras, para este proyecto se partió desde el análisis de la matriz y de sus obras en la que se obtuvo asesoramiento de la dirección de sistemas de la UPS.

En los capítulos se tratará:
Capítulo 1: se analizará el problema a resolver, los antecedentes, objetivos, justificación, el alcance y la metodología de investigación desarrollada.

Capítulo 2: se presenta conceptos teóricos, E-Commerce/DMZ/Internet, Enterprise WAN, Remote Access VPN, WAN, LAN, ISP, IPS y DNS, protocolos a utilizar y metodología a basarse PPDIOO.

Capítulo 3: se realiza la situación actual de cada obra, la metodología de cada obra, análisis de la infraestructura tanto lógica como física, servidores e ISP y modelos

jerárquicos, diagramas de MDF e IDF’s, protocolos utilizados en las obras, además el control de ancho de banda.

Capítulo 4: se considera el modelo a basarse en el diseño CEAM, el análisis de costos de las diferentes marcas y equipos para el diseño. Fases de preparación, planificación y diseño, análisis de protocolos soportados en cada dispositivo, diseño físico y lógico, configuración de equipos.
Además de las conclusiones y recomendaciones.
Anexos.

# CAPÍTULO 1
# PLANTEAMIENTO DEL PROBLEMA

En este capítulo se analizará el problema planteado, antecedentes, objetivos, generales y específicos, justificación, delimitación y la metodología basada en Cisco.

## 1.1. Antecedentes

Este proyecto está orientado a la intercomunicación de Casa Inspectorial Salesiana con algunas de sus obras a nivel nacional, las tecnologías de comunicación se van desarrollando a manera que pasa el tiempo en la cual son claves los equipos de última generación, ya que estos brindan un soporte eficaz correspondientes a la demanda de usuarios y necesidades de empresas u organizaciones, en que los equipos abastecen la necesidad de cada servicio expuesto. Los equipos con los que se va a realizar el siguiente diseño son de gran escalabilidad, se pueden partir desde los dispositivos diseñados para una futura implementación, los cuales cumplen con los requerimientos concernientes a necesidades. En consecuencia las tecnologías de la información (TI) son las que interactúan con el procesamiento y distribución de la información.

Hoy en día hay muchas alternativas en las que permiten la administración y el acceso a los recursos compartidos de información, en la actualidad existen varias herramientas en las que interactúan las redes de computadoras.

El concepto de las redes de computadoras se la define como: “es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.” (Tanenbaum,2003, pág. 1)

El manejo de los flujos de información a través de una red de computadoras eficiente, permite un desarrollo importante ya que la información estará lista en el momento solicitado, y la administración de datos es un factor importante ya será un indicador que muestre la efectividad con la que trabaja la red de datos.

## 1.2. Problema a resolver

La infraestructura actual de la Casa Inspectorial Salesiana del Ecuador, no tiene un diseño de red de frontera (borde) que permita tener una intercomunicación entre la Casa Inspectorial y sus obras en función de las necesidades y/o requerimientos. La falta de comunicación de la matriz con sus obras en VoIP y videoconferencia, los costos que infieren en no tener establecida la intercomunicación entre la matriz y sus obras, la falta de administración sobre las obras desde la matriz.

Lo que se propone es la conectividad a través de equipos activos de red para la comunicación con los mismos.

La red de campus está establecida con algunos equipos, los cuales no son adecuados y suficientes para la intercomunicación entre la matriz y sus obras. Por esta razón se diseñará la red de frontera basada en el rediseño de la red de campus y los módulos remotos que proporcionará la comunicación entre la matriz y sus obras.

Con respecto a la administración y mantenimiento sobre los equipos de infraestructura y red, se debe tomar muy en cuenta el tiempo de respuesta, para solventar las necesidades de las obras y de los usuarios finales.

En la actualidad la Casa Inspectorial Salesiana cuenta con una estructura en sistemas informáticos distribuida geográficamente a nivel nacional. Los diferentes dominios que actualmente existen en cada obra, se obtienen de acuerdo a los servicios que los provee el ISP, cada red local presenta una configuración personalizada, las obras tienen segmentos muy diferentes en los cuales no se pueden realizar una comunicación, es uno de los percances, en la que se requiere realizar una segmentación por matriz y por cada obra, para obtener una diferenciación tanto de la una como de la otra.

Algunos de los servicios con la que cuentan la matriz y sus obras son: correo electrónico, el cual se lo puede realizar localmente, pero la necesidad de comunicación entre las sedes que se encuentran en diferentes ciudades del Ecuador hace que el servicio se lo realice de manera externa; es decir, crea una carga de datos desde el lugar de origen hasta su destino, este tráfico generado consume recursos de red (servicio de

Internet) que afectan a la calidad del servicio (QoS) de otras aplicaciones. (Dominguez Ayala & Chicaiza Iza, 2008, pág. 17)

Con lo descrito a lo anterior se puede hacer una observación. Pregunta ¿Qué diseño de interconexión puede mejorar los servicios que presta la red de la Casa Inspectorial, a los diferentes usuarios, guardando una estandarización única que permita realizar una auditoría no solo a los equipos sino a la información que se envía desde la red, ejecutando un mejor control de calidad y monitoreo de los diferentes enlaces y redes internas?

## 1.3. Objetivos

### 1.3.1. Objetivo general.

Analizar y diseñar la red de frontera (borde) de la Casa Inspectorial Salesiana del Ecuador, con la finalidad de obtener una óptima intercomunicación de la matriz con las obras salesianas.

### 1.3.2. Objetivos específicos.

- Analizar la situación actual de la Casa Inspectorial Salesiana concerniente a las necesidades de interconexión para el levantamiento de información del funcionamiento de la comunicación de la red.
- Diseñar la red de frontera de la Casa Inspectorial Salesiana considerando las necesidades para la interconexión entre la matriz y las sucursales salesianas.
- Realizar pruebas de intercomunicación con algún servicio expuesto.
- Analizar los requerimientos, parámetros actuales y proyectados que deberá otorgar el diseño de la red para la interconexión local y nacional.
- Determinar los equipos deben usarse dentro de la estructura de la red que permitan mantener un buen desempeño de está, con base en el análisis, de los requerimientos de la interconexión.
- Diseñar la mejor solución para presentarla como una opción aplicable a la Casa Inspectorial Salesiana acorde a sus requerimientos.
- Explicar los beneficios que proveerá el diseño de red propuesto.
- Indicar las proyecciones de crecimiento (escalabilidad) del diseño entregado a la Casa Inspectorial Salesiana.

## 1.4. Justificación del trabajo

La Casa Inspectorial no cuenta con una red de frontera establecida. Por lo cual no existe conectividad entre la Casa Inspectorial Salesiana (Matriz) con las obras Salesianas. Por lo antes mencionado se partiría desde el rediseño de campus para acoplar esta red de frontera.

Para este proyecto se necesita una red de fácil escalabilidad, ya que a partir de este tema, se desprenden varios subtemas. Los cuales necesitarán del crecimiento de la red, algunos de los proyectos posteriores es obtener una clasificación de las sucursales o redes remotas que se podrán comunicar por medio de la red de frontera de la Casa Inspectorial con la red WAN. En esto se aplicará un diseño de red basada en modelos jerárquicos ECNM y metodologías basadas en el ciclo de vida de una red PPDIOO.

## 1.5. Delimitación

Este proyecto tiene por alcance el diseño de la red de frontera (borde) de la Casa Inspectorial Salesiana del Ecuador ubicada en Quito, que será desarrollado en un período de 12 meses a partir de la aprobación del plan.
Se pretende analizar e identificar algunos de los problemas existentes al momento en la red actual y plantear alternativas para mejorar la conectividad entre la matriz y las sucursales, se brindará nuevos servicios y aplicaciones los que son videoconferencias y telefonía IP. El diseño será la conectividad entre la matriz con las obras Salesianas, con estos dos servicios expuestos.

"Se utilizará el diseño de cuatro capas que son:

- Redes y servidores de comercio electrónico
- Conectividad a Internet y la zona desmilitarizada (DMZ)
- VPN y acceso remoto
- Empresa WAN". (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 50)

Para la realización de este proyecto se utilizará la metodología PPDIOO, del cual las fases a utilizar son preparación, planeación y diseño.

En la fase de preparación se tomará en cuenta la justificación financiera para lo cual se utilizará tablas de decisión en cuanto equipamiento que podrá soportar la arquitectura.

En la fase de la planeación se identificará los requerimientos y necesidades en cuanto a aplicaciones de la red de frontera de la Casa Inspectorial Salesiana.

En la fase del diseño se realizará el diseño de la red de frontera basada en los requerimientos técnicos obtenidos dentro de la fase de planeación.

Este proyecto consta del análisis, diseño, justificación financiera orientada a la implementación a futuro y pruebas de funcionamiento de la red de frontera para la Casa Inspectorial para lo cual se utilizará los programas de simulación Packet Tracer y GNS3 los cuales son de fácil manejo y adquisición, dentro de este proyecto no consta la implementación.

La Casa Inspectorial Salesiana se encuentra ubicada en la Calle Madrid E12-68 y Andalucía a lado de la Universidad Politécnica Salesiana del Campus El Girón.

# CAPÍTULO 2

Este capítulo consta de algunos conceptos básicos como: E-Commerce/DMZ/Internet, Enterprise WAN, Remote Access VPN, WAN, LAN, ISP, IPS y DNS, protocolos a utilizar y metodología a basarse PPDIOO.

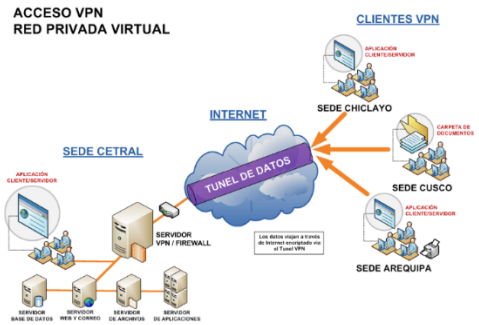
## 2.1. Marco Teórico

En el siguiente diseño se van a describir algunos de los protocolos utilizados en el diseño de frontera (borde), para esto se hace referencia al diseño de arquitectura de Cisco algunos de los más conocidos son:

### 2.1.1. Red privada virtual VPN

Una VPN (Virtual Private Network o Red Privada Virtual), es la tecnología que permite extender una red privada LAN hacía la red mundial WAN, mediante un proceso de encapsulación (tunneling) y en su caso de encriptación, de tal manera que desde cualquier lugar del mundo se podrá conectar con una red local, y trabajar de manera similar tal como si se estuviera físicamente dentro de ella, para ello es necesario una conexión a Internet. Además es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Figura 1. Acceso VPN red privada virtual.




Fuente: (Seguridad y Redes, 2010, págs. 3 - 4)

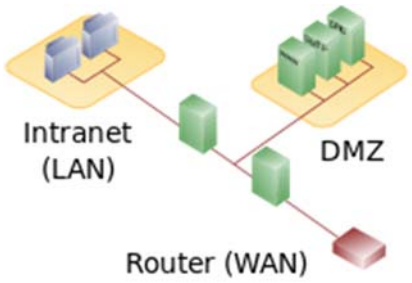
Los dos tipos de VPN cifradas son:

- **"VPN IPSec de sitio a sitio:** Esta alternativa a Frame Relay o a las redes WAN de línea alquilada permite a las empresas llevar los recursos de la red a las sucursales, las oficinas instaladas en casa y los sitios de partners comerciales.
- **VPN de acceso remoto:** Esta modalidad lleva prácticamente cualquier aplicación de datos, voz y vídeo al escritorio remoto, emulando el escritorio de la oficina principal. Una VPN de acceso remoto puede instalarse utilizando VPN SSL, IPsec o ambas, dependiendo de los requisitos de implementación. (Seguridad VPN, 2014, pág. 1)

### 2.1.2. Zona desmilitarizada o red perimetral DMZ

Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa, los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. (Jean, 2011, pág. 1)

Figura 2. Acceso VPN red privada virtual.



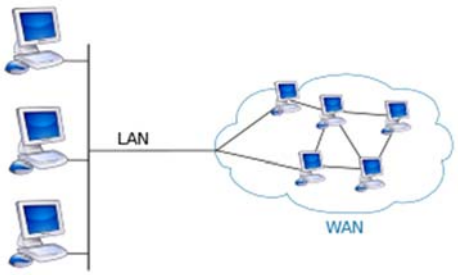

Fuente: (Jean, 2011, pág. 1)

### 2.1.3. Red de área amplia WAN

Es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales, llamadas LAN, por lo que sus miembros no están todos en una misma ubicación física.

Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de internet (ISP) para proveer conexión a sus clientes. (Red de área amplia WAN, 2014, pág. 1)

Figura 3.Red de área amplia WAN

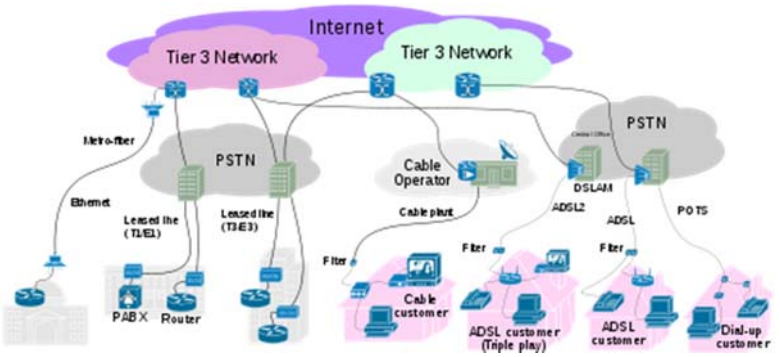



Fuente: (Mühlböck, 2011, pág. 1)

### 2.1.4. Proveedor de servicios de Internet ISP

Es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cablemódem, GSM, Dial-up. (ferre, 2010, pág. 1)

Figura 4. Proveedor de servicios de Internet

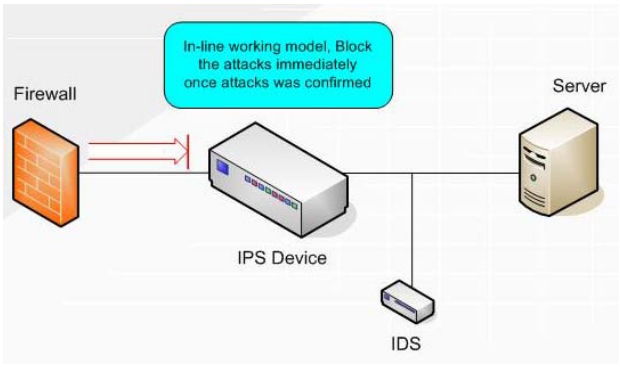



Fuente: (ferre, 2010, pág. 1)

### 2.1.5. Sistema de prevención de intrusos IPS

Es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos. (Ji, 2007, pág. 5)

Figura 5. Sistema de prevención de intrusos




Fuente: (Ji, 2007, pág. 5)

### 2.1.6. Sistema de nombres de dominio DNS

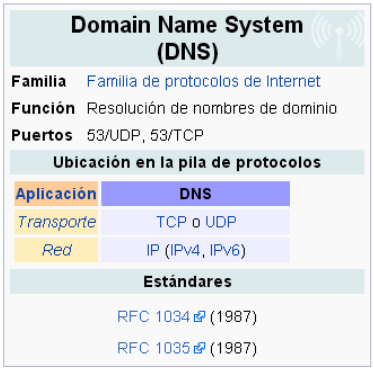
Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en

identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

El servicio DNS es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 53 (Domain Name System. August 3, 2014, pág.1), (Galvez, 2013, pág. 2)

Figura 6. Sistema de prevención de intrusos




Fuente: Domain Name System. 1987, pág.1, (Galvez, 2013, pág. 2)

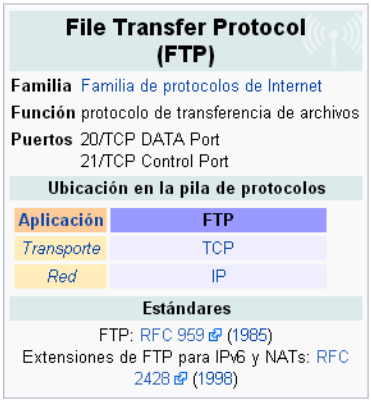
### 2.1.7. Protocolo de transferencia de archivos FTP

Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el

login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos (File Transfer Protocol. March 31, 2014, pág. 1)

Figura 7. File Transfer Protocol




File Transfer Protocol. 1998, pág. 1

### 2.1.8. Protocolo de transferencia de hipertexto HTTP

Es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP. La especificación completa del protocolo HTTP está recogida en el RFC 1945 (estándar). Fue propuesto por Tim Berners-Lee, atendiendo a las necesidades de un sistema global de distribución de información como el World Wide Web.

En el protocolo HTTP las URLs comienzan con "http://" y utilizan por defecto el puerto 80, las URLs de HTTPS comienzan con "https://" y utilizan el puerto 443 por defecto.

Figura 8. Seguridad de protocolo de Internet IPsec

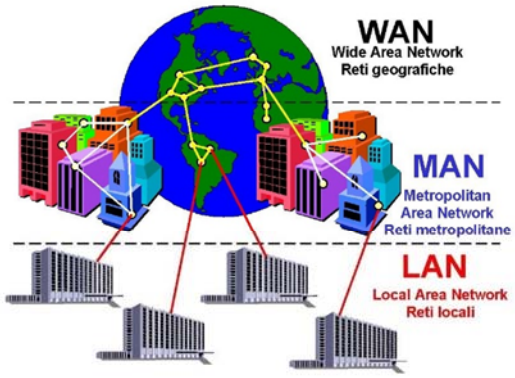

Fuente: Arturo de la Escalera Hueso, 2001, pág. 11

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

### 2.1.9. Red de área metropolitana MAN

Es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50 ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10 Mbit/s ó 20 Mbit/s, sobre pares de cobre y 100 Mbit/s, 1 Gbit/s y 10 Gbit/s mediante fibra óptica.

Figura 9. Diagrama de MAN




Fuente: Arturo de la Escalera Hueso, 2001, pág. 11

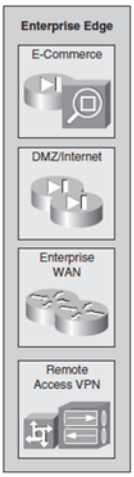
### 2.1.10. Diseño zona de borde de la empresa

El borde de la infraestructura de red actúa como puerta de enlace para la empresa. La infraestructura de borde sirve para la mayoría de las áreas de la red de la empresa, incluyendo el centro de datos, el campus y sucursales remotas. Este diseño es esencial para asegurar la disponibilidad de servicios de Internet y datos a todos los usuarios de la empresa.

Como se muestra en la Figura 10, el borde de la empresa se compone de los siguientes submódulos:

- “E-commerce network and servers
- Internet connectivity and demilitarized zone (DMZ)
- VPN and remote access
- Enterprise WAN” (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 50)

Figura 10. Enterprise Edge Module




Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 50)

### 2.1.11. E-Commerce Module

El diseño se utiliza para identificar la alta disponibilidad, componentes, métodos de diseño y topologías para los módulos de comercio electrónico. El módulo de comercio electrónico permite a las organizaciones apoyar las aplicaciones de comercio electrónico a través del Internet. El diseño para este módulo es similar que el diseño realizado por otros autores. Los dispositivos ubicados en el submódulo de comercio electrónico incluyen:

- Web and aplication servers: interfaz de usuario principal para la navegación e-commerce.
- Database servers: Contienen la aplicación y la información de transacciones.
- Firewall and firewall routers: rigen la comunicación entre los usuarios del sistema.
- Network intrusión prevention systems (IPS): Proveen supervisión de claves de red de segmentos en el módulo para detectar y responder a los ataques contra la red.
- Multilayer switch with IPS modules: Proporcionan transporte de tráfico y control de la seguridad integrada.

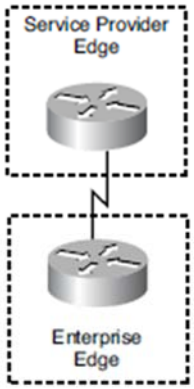
### 2.1.12. Internet Connectivity Module

Los submódulos de Internet del borde de la empresa ofrecen servicios como servidores públicos, correo electrónico y DNS. También se proporciona conectividad a uno o varios proveedores de servicios de Internet (ISP).
Los componentes de este submódulos incluyen:

- Firewall and firewall routers: Proporciona protección de los recursos, el filtrado activo de tránsito y terminación de VPN para sitios remotos y usuarios
- Internet edge routers: Proporciona filtrado básico y conectividad de múltiples capas
- FTP and HTTP servers: Permite tener aplicaciones web para que la empresa interactúe con el mundo a través de la Internet público.
- SMTP relay servers: sirve de enlace entre Internet y el servidor de correo.
- DNS servers: Sirven como autoridad del servidor DNS externo para la empresa y el relé de solicitudes internas a través de Internet

Algunos modelos se conectan a la empresa a través de Internet. La forma más simple es tener un solo circuito entre la empresa y el SP, como se muestra en la Figura 11. El inconveniente es que no tiene redundancia entre los circuitos, tanto para la empresa como para el proveedor de servicio.

Figura 11. Enterprise Edge Module



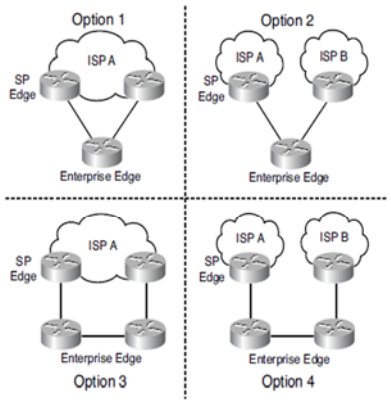

Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 51)

Se puede utilizar las soluciones de varios hosts para proporcionar redundancia o conmutación por error para el servicio de Internet.

La Figura 12 muestra cuatro opciones multihoming Internet:

- Routers individuales, dobles enlaces a un ISP
- Routers individuales, dobles enlaces a dos ISPs
- Routers duales, enlaces dobles a un ISP
- Routers duales, enlaces dobles a dos ISPs

Figura 12. Conexión simple al internet




Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 52)

1: Proporciona redundancia de enlaces, pero no proporciona redundancia de ISP y router locales.
2: Proporciona enlace redundancia del ISP, pero no proporciona redundancia para un error de enrutador local.
3: Ofrece enlace y router de redundancia locales, pero no prevé un fracaso de ISP.
4: Proporciona redundancia completa del router local, enlaces, y los ISP.

### 2.1.13. VPN / Acceso Remoto

El módulo de acceso VPN permite a los usuarios individuales establecer conexiones seguras con una red de ordenadores a distancia del borde de la empresa, aquellos

usuarios pueden acceder a los recursos seguros en esa red como si estuvieran directamente conectados a los servidores de red, incluyendo la autenticación para usuarios remotos y sitios. Los componentes de este submódulo son:

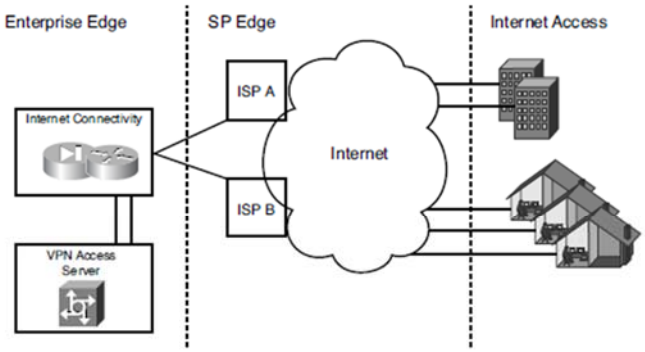
- Firewalls: Proporcionan el filtrado de tráfico, autentican sitios remotos de confianza y proporcionan conectividad mediante túneles IPsec
- Dial-in access concentrators: son usuarios individuales, esto se trabaja individualmente, interactua con Active Directory.
- Cisco Adaptive Security Appliances (ASA) : se encarga de terminar túneles IPsec, autenticar usuarios remotos individuales, y proporcionar servicios de prevención de intrusiones y firewall
- Network intrusión prevention system (IPS) appliances: es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos

La VPN utiliza un servidor de terminales de acceso remoto, este módulo se conecta a la PSTN. Las redes actuales a menudo prefieren VPNs más que servidores de terminales de acceso remoto y dedicado a enlaces WAN.

Ahora los usuarios optan por un mejor aprovechamiento de los ISPs a través de las VPNs para reducir los gastos de comunicación. Para aplicaciones críticas, los ahorros de costos podrían ser compensados por una reducción en el costo de la empresa y la pérdida de servicio.

Los usuarios pueden acceder a través de su hogar o de cualquier parte, hasta de sus celulares móviles, al Internet utilizando el SP local con túneles asegurados IPsec para la VPN.

Figura 13. Opciones Multihoming de Internet




Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 53)

La figura 13 muestra un diseño de VPN. Las sucursales pueden obtener acceso local a Internet de un ISP.

Los teletrabajadores también obtienen acceso local a Internet. Software de VPN crea túneles VPN garantizados al servidor VPN que se encuentra en el submódulo de VPN del borde de la empresa.

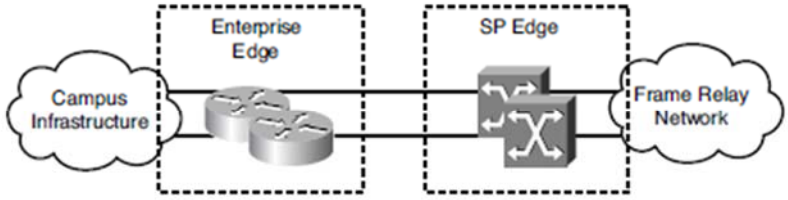
### 2.1.14. Enterprise WAN

El borde de la empresa WAN incluye el acceso a las redes WAN's, además proporciona a los usuarios de sitios remotos geográficamente dispersos, acceso a los mismos servicios de red.
Las tecnologías WAN son las siguientes:

- Multiprotocol Label Switching (MPLS)
- Metro Ethernet
- Leased lines.
- Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH).
- PPP
- Frame Relay
- ATM
- Cable

- Digital subscriber line (DSL)
- Wireless

Figura 14. WAN Module.




Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 54)

Para el diseño del borde de la empresa se recomienda las siguientes directrices:

- Determinar la conexión necesaria para conectarse a la red corporativa a través de Internet. Estas conexiones se asignan al módulo de conexión a Internet.
- Crear el módulo de comercio electrónico para los clientes y socios que requieren acceso a Internet para las aplicaciones de negocio y base de datos.
- Diseñar el acceso remoto / módulo de VPN para el acceso VPN a la red interna a través de Internet. Poner en práctica la política de seguridad y configurar los parámetros de autenticación y autorización.
- Asignar las secciones de borde que tienen conexiones permanentes a las oficinas remotas. Asignar estos a la WAN, red de metro-area de la zona (MAN), y el módulo de VPN.

### 2.1.15. Módulo de borde de proveedor de servicio

El módulo de borde SP, que se muestra en la figura 15, se compone de los servicios de borde SP tales como la siguiente:

- Servicios de Internet
- Servicios de PSTN
- Servicios WAN

Figura 15. Módulo de frontera (borde) SP WAN / Internet.


Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 55)

Las empresas utilizan productos especiales para la adquisición de servicios de red. ISPs ofrecen a las empresas el acceso a la Internet.

Los ISP's puede enrutar las redes de la empresa a su red y el uso del upstream se refiere a la velocidad con que los datos pueden ser transferidos de un cliente a un servidor. Algunos ISP's pueden proporcionar servicios de Internet con acceso DSL. Conectividad con múltiples ISP's se describe en "Edge internet. (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 55)

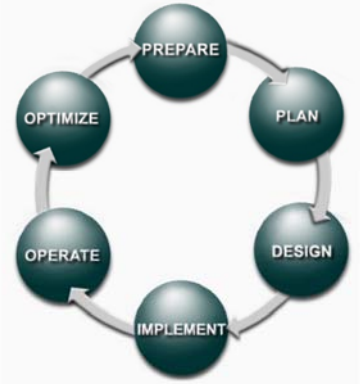
Para los servicios de voz, los proveedores de PSTN ofrecen acceso a la red mundial de voz pública. Para la red de la empresa, la PSTN permite a los usuarios de acceso telefónico acceder a la empresa a través de tecnologías" inalámbricas analógicas o celular. También se utiliza para la copia de seguridad de WAN a través de los servicios RDSI.

## 2.2. Metodología PPDIOO

Cisco ha formalizado el ciclo de vida de una red en seis fases: Preparar, planificar, diseñar, implementar, operar y optimizar. Mejor conocido como PPDIOO. El ciclo de vida PPDIOO tiene cuatro ventajas principales:

“Baja el costo total de propiedad por validación de requerimientos de tecnología y planeamiento para cambios de infraestructura y requerimientos de recursos.
Incrementa la disponibilidad de la red por la producción de un sólido diseño de red y validaciones en las operaciones.
Mejora la agilidad de negocios estableciendo requerimientos y estrategias tecnológicas.
Velocidad de acceso para aplicaciones y servicios, mejorando disponibilidad, fiabilidad, seguridad, escalabilidad y performance.”

Figura 16. Metodología PPDIOO.




Fuente: (Occhiogrosso, 2009, pág. 1)

Preparación: Establece la organización y los requerimientos del negocio, desarrolla una estrategia de red, y se propone una arquitectura conceptual de alto nivel para apoyar la estrategia. Crea un caso de negocios para establecer una justificación financiera para la estrategia de red

Planeación: Identifica los requerimientos de red realizando una caracterización y evaluación de la red, realizando un análisis de las deficiencias contra las buenas prácticas de arquitectura. Se elabora un plan de proyecto desarrollado para administrar las tareas, asignar responsables, verificación de actividades y recursos para hacer el diseño y la implementación. El plan del proyecto se alinea con los parámetros de alcance, costo y recursos establecidos con los requisitos de negocio originales. Este plan de proyecto es seguido durante todas las fase del ciclo.

Diseño: El diseño de la red se desarrolla sobre la base de los requisitos técnicos y comerciales obtenidos en las fases anteriores. La especificación de diseño de la red es un diseño detallado integral que cumple con los requisitos técnicos y de negocio actuales. Proporciona alta disponibilidad, fiabilidad, seguridad, escalabilidad y rendimiento. El diseño incluye diagramas de red y una lista de equipo. El plan del proyecto se actualiza con más información granular para su implementación. Una vez aprobada la fase de diseño, se inicia la fase de Implementación.

Implementación: Nuevo equipamiento es instalado y configurado en esta fase. El plan de proyecto es seguido durante esta fase. Los cambios deben ser comunicados en una reunión de control de cambios, con la necesaria aprobación para proceder. Cada paso en la implementación debe incluir una descripción, guía de implementación, detallando tiempo estimado para implementar, pasos para rollback en caso de falla e información de referencia adicional.

Operación: Mantiene el estado de la red día a día. Esto incluye administración y monitoreo de los componentes de la red, mantenimiento de ruteo, administración de actualizaciones, administración de performance, e identificación y corrección de errores de red. Esta fase es la prueba final de diseño.

Optimización: Envuelve una administración pro-activa, identificando y resolviendo cuestiones antes que afecten a la red. Esta fase puede crear una modificación al diseño si demasiados problemas aparecen, para mejorar cuestiones de desempeño o resolver cuestiones de aplicaciones. (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, págs. 13 - 14).

Tabla 1. Descripción breve de las fases del PPDIOO.

| Fase | Descripción. |
|---|---|
| Preparación | Establece los requisitos de organización y de negocio, desarrolla una estrategia de red, y propone una arquitectura de alto nivel |

| | |
|---|---|
| Planeación | Identifica los requisitos de la red mediante la caracterización y la evaluación de la red, la realización de un análisis de las deficiencias |
| Diseño | Proporciona alta disponibilidad, fiabilidad, seguridad, escalabilidad y rendimiento |
| Implementación | Instalación y configuración de nuevos equipos |
| Operación | Operaciones de red del día a día |
| Optimización | Gestión de la red proactiva; modificaciones en el diseño |

Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 15)

En el capítulo 2 se hizo un breve recuento sobre algunos conceptos básicos, entre los cuales están las diferentes etapas que conforman el módulo de red de frontera. Además la metodología en la que se va a basar, para realizar el diseño jerárquico de Cisco.

# CAPÍTULO 3

# SITUACIÓN DE LAS OBRAS SALESIANAS DEL ECUADOR.

En este capítulo se hace un breve resumen de la situación actual de la red de las obras de la Casa Inspectorial Salesiana, la misma que no tiene diseñada ni implementada una red de frontera en ninguna obra ni en la matriz, lo que se pretende diseñar. A continuación se detallará la información más relevante de algunas obras para posteriormente realizar el diseño, ya que mantienen un mismo diseño de red y mismos dominios de broadcast.

## 3.1. Obras que conforman la Casa Inspectorial Salesiana Del Ecuador

### 3.1.1. Obra Colegio Técnico Don Bosco La Kennedy

#### 3.1.1.1. Ubicación

Se encuentra ubicado al norte de la ciudad de Quito, Rafael Bustamante E6-87 y Gonzalo Zaldumbide (Colegio Técnico Don Bosco).

#### 3.1.1.2. Situación actual

En el diseño de la infraestructura de Networking de la obra Don Bosco Kennedy existe una estructura de distribución física de los equipos de acuerdo a su funcionalidad, por lo tanto para efectos de este análisis se los ha clasificado de acuerdo al rol que cumple cada uno de los equipos dentro de las capas del diseño de Networking (Core, Distribución y Acceso).

#### 3.1.1.3. Capa de Núcleo

Esta capa está conformada por: Switch Cisco Catalyst 4500E que contiene 48 interfaces GigaEthernet a través de enlaces de fibra óptica y 96 enlaces UTP. Este Switch está ubicado en el MDF1 en el Data Center de la Universidad Politécnica Salesiana, a través de este switch se brinda el servicio de Backbone (Núcleo de la red), conectándose a los switch’s de la capa de acceso ubicados en los SDF’s (cuartos de distribución secundarios de cableado) mediante la utilización de enlaces de fibra óptica. La velocidad de comunicación del Backbone es de hasta 1Gbps.

#### 3.1.1.4. Capa de Distribución

Esta capa está conformada por 1 Switch Cisco 4507 Gigabit, 1 Switch Catalyst 2960 2 Switch's D-Link 1024R, Switch's D-Link DSS24, 3Com Super Stack 3250, 3Com Super Stack 3250, 3Com 3226, switch catalyst 2960, 3Com 4200G, HP A5120 Series JE068A, HP V1910, HP A5120 Series JE068A, D-Link DS-1228, Trendnet TE100-S163G y 3Com 2016 se encuentran distribuidos de la siguiente manera:

Switch Cisco Gigabit SG300-52 ubicado en el MDF1 de la oficina de informática, este dispositivo brinda servicio de acceso Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de un enlace de fibra óptica a 1 Gbps.

Switch's 3Com ubicado en el SDF0 ubicado en los laboratorios de Informática, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de fibra óptica a 1 Gbps.

Switch's TP-Link Gigabit TL-SG1024 ubicado en el SDF1 ubicado 1er Piso, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de fibra óptica a 1 Gbps.

Switch's TP-Link Gigabit TL-SG1024 ubicado en el SDF2 ubicado 2do Piso, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de fibra óptica a 1 Gbps.

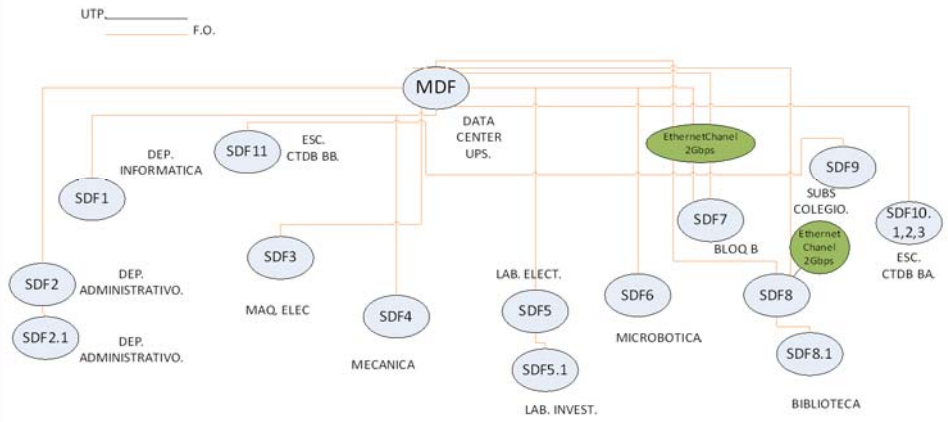
Switch's TP-Link Gigabit TL-SG1024 ubicado en el SDF2.1 ubicado 3er Piso, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con

Switch’s de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps.

#### 3.1.1.5. Capa de Acceso

Esta capa está conformada por 1 Switch 3Com y 3 Switch’s TP-Link Gigabit TL-SG1024, en la cual se encuentran incluidos los switches de acceso. La distribución de los switches de esta capa es la siguiente:

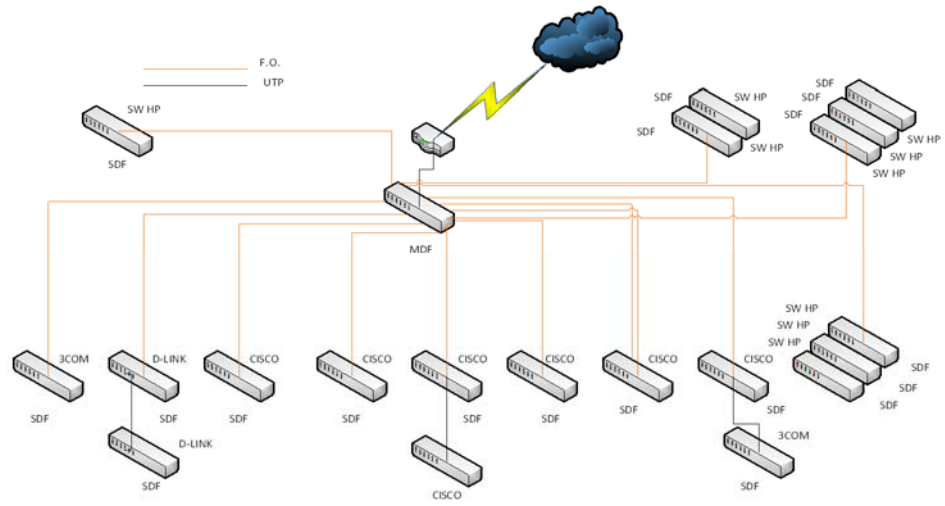
Figura 17. Diagrama de distribución MDF y SDF interna de la red LAN Don Bosco La Kennedy.




Elaborado por: Leonardo Suárez.

La topología que se emplea en esta red es del tipo cascada, la misma que está conformada en su mayoría por switchs cuya funcionalidad está limitada a la transmisión de paquetes para aproximadamente 284 dispositivos de red. A continuación se presenta un diagrama del esquema de conectividad de la infraestructura de red.

Figura 18. Diagrama de distribución MDF y SDF de la red LAN de la obra.




Elaborado por: Leonardo Suárez.

A continuación un breve resumen de los MDF y SDF's de la obra Don Bosco La Kennedy.

Tabla 2. Distribución de MDF y SDF's.

| FUNCIÓN | DISPOSITIVO | INT. | UBICACIÓN | VELOCIDAD | SERVICIOS |
|---|---|---|---|---|---|
| CORE | MDF | UTP/F.O | .DATA CENTER UPS | 100Mbps/1Gbps | Núcleo de la red |
| ACCESO | SDF1 | F.O. | DEP. INFORMATICA. | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF2 | F.O. | DEP. ADM. COLEGIO | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF2.1 | F.O. | DEP. ADM. COLEGIO | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF3 | F.O. | MAQ. ELECTRICAS. | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF4 | F.O. | MECANICA. | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF5 | F.O. | LAB. ELECTRICA | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF5.1 | UTP. | LAB. INVESTIGAC. | 100Mbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF6 | F.O. | MICROBOTICA. | 1Gbps | Pág. Web, Mail, Internet. |

| | | | | | |
|---|---|---|---|---|---|
| ACCESO | SDF7 | F.O. | BLOQUE B PISO 3 | 2Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF8 | F.O. | BIBLIOTECA | 2Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF8.1 | F.O. | BIBLIOTECA | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF9 | F.O. | SUBSUELO COLEGIO. | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF10.1, 2, 3. | F.O. | ESC. CTDB BLOUE A. | 1Gbps | Pág. Web, Mail, Internet. |
| ACCESO | SDF11.1, 2, 3. | F.O. | ESC. CTDB BLOQUE B. | 1Gbps | Pág. Web, Mail, Internet. |

Elaborado por: Leonardo Suárez.

En lo referente a los servicios de autenticación, acceso a Internet, correo electrónico y aplicaciones de usuarios de la obra se utilizan los siguientes servidores:

Tabla 3. Servidor de la obra Don Bosco.

| **Código** | **Modelo** | **Funcionalidad** |
|---|---|---|
| SER1 | HP PROLIANT DL120 G7 | Servidor de backup de calificaciones 2 GB RAM Windows 2008. |
| SER2 | HP PROLIANT ML150 | Servidor de contabilidad 2 GB RAM Windows 2003. |

Elaborado por: Leonardo Suárez.

#### 3.1.1.6. Análisis de la infraestructura lógica

La red LAN establecida en la obra Don Bosco La Tola de la ciudad de Quito utiliza Ethernet como el protocolo de comunicaciones y utiliza los estándares 10BaseT y 100BaseT. Por otra parte como protocolo de red se utiliza TCP/IP.

Se debe tomar en cuenta que hasta un tiempo no tenían segmentación ni un plan IP establecido, se optó por integrar a la obra en la red de la Universidad Politécnica Salesiana la cual brindó un servicio de Internet y una segmentación establecida por la Universidad a la obra mencionada. En la cual se ha implementado un esquema de VLAN’s de acuerdo a la red estudiada y establecida.

De acuerdo al estudio en la red LAN de la obra se ha establecido que se va a implementar 6 VLAN's, cada una de estas para un dominio de Brodcast. A continuación se describe las diferentes VLAN's establecidas en la red LAN de la obra.

Tabla 4. Distribución de VLAN's Don Bosco La Kennedy.

| VLAN ID | SERVICIO DE VLAN. |
|---|---|
| 21 | VLAN-COLEGIO |
| 224 | CES-DOCENTES |
| 228 | CES-COLEGIO |
| 229 | CES-ESCUELA |
| 231 | CES-ADM |
| 234 | CES-ESEMTIA-DOC |

Elaborado por: Leonardo Suárez.

El direccionamiento asignado por la UPS y brindado a partir del plan IP es de clase B privadas, a continuación se detalla la segmentación de VLAN's:

Direccionamiento IP:

Nombre: Subred VLAN 21 Colegio.
Descripción: Red LAN de la UPS hacia la obra.
Network: 172.17.145.254
Mascara: 255.255.255.0
Rango IP: 172.17.145.1- 172.17.145.254
Núm. Hosts: 254 válidos (1 Subred y 1 Broadcast)

Nombre: Subred VLAN 224 Docentes.
Descripción: Red LAN de la obra asignada a los docentes.
Network: 172.17.224.254
Mascara: 255.255.254.0
Rango IP: 172.17.224.1- 172.17.225.254
Núm. Hosts: 510 válidos (1 Subred y 1 Broadcast)

Nombre: Subred VLAN 228 Colegio.
Descripción: Red LAN de la obra asignada al colegio (alumnos).
Network: 172.17.228.254
Mascara: 255.255.255.0
Rango IP: 172.17.228.1- 172.17.228.254
Núm. Hosts: 254 válidos (1 Subred y 1 Broadcast)

Nombre: Subred VLAN 229 Escuela.
Descripción: Red LAN de la obra asignada a la escuela (alumnos).

| | |
|---|---|
| Network: | 172.17.229.254 |
| Mascara: | 255.255.255.0 |
| Rango IP: | 172.17.229.1- 172.17.229.254 |
| Núm. Hosts: | 254 válidos (1 Subred y 1 Broadcast) |

| | |
|---|---|
| Nombre: | Subred VLAN 231 Administrativos. |
| Descripción: | Red LAN de la obra asignada a los administrativos. |
| Network: | 172.17.231.254 |
| Mascara: | 255.255.255.0 |
| Rango IP: | 172.17.231.1- 172.17.231.254 |
| Núm. Hosts: | 254 válidos (1 Subred y 1 Broadcast) |

| | |
|---|---|
| Nombre: | Subred VLAN 234 Esemtia-Docentes. |
| Descripción: | Red LAN de la obra asignada a los docentes esemtia. |
| Network: | 172.17.235.254 |
| Mascara: | 255.255.254.0 |
| Rango IP: | 172.17.235.1- 172.17.236.254 |
| Núm. Hosts: | 510 válidos (1 Subred y 1 Broadcast) |

Cabe recalcar que el direccionamiento IP de esta obra es asignada por la UPS ya que se acopló la obra a la UPS, por lo cual es necesario saber si se optaría por mantener el plan IP establecido a esta obra o cambiarlo y si este sería el caso tomar este direccionamiento para acoplarlas en las demás obras para integrar los mismos dominios de broadcast en las obras para que abarque todos los diseños de red y se puedan conectar todas las obras de la Casa Inspectorial Salesiana sede Quito.

En los diferentes dominios de colisiones y dominios de broadcast se debe mencionar que actualmente existen seis dominios que están en la obra, por las seis subredes que se describen anteriormente. También es importante mencionar que en esta obra si existe un plan IP y una segmentación de VLAN’s o ruteadores que segmente la mencionada red.

La red LAN de la obra La Tola de la Casa Inspectorial Salesiana brinda servicio a aproximadamente 215 estaciones de trabajo de las cuales 56 son utilizadas por personal de la obra y las restantes 159 son equipos de computación ubicados en laboratorios. En la siguiente tabla se muestra la distribución de Switches y salidas de datos por cada uno de los SDF existente en la obra salesiana.

Tabla 5. Distribución de Switch’s de la obra.

| CÓDIGO | NOMBRE DEL SDF | CANT. SWITCH | CANT. PORTS UTP/F.O. | PUERTOS USADOS UTP/F.O. |
|---|---|---|---|---|
| MDF | .DATA CENTER UPS | 1 | 96/48 | 48/35 |
| SDF1 | DEP. INFORMATICA ESC. Y COL | 1 | 48/4 | 30/1 |
| SDF2 | DEP. ADM. COLEGIO | 1 | 16/- | 14/- |
| SDF2.1 | DEP. ADM. COLEGIO | 1 | 16/- | 14/- |
| SDF3 | MAQ. ELÉCTRICAS. | 1 | 24/4 | 18/1 |
| SDF4 | MECÁNICA. | 1 | 24/4 | 15/1 |
| SDF5 | LAB. ELÉCTRICA | 1 | 48/4 | 41/1 |
| SDF5.1 | LAB. INVESTIGAC. | 1 | 48/4 | 40/2 |
| SDF6 | MICROBÓTICA. | 1 | 48/4 | 25/1 |
| SDF7 | BLOQUE B PISO 3 | 1 | 48/4 | 30/2 |
| SDF8 | BIBLIOTECA | 1 | 48/4 | 35/2 |
| SDF8.1 | BIBLIOTECA | 1 | 48/4 | 20/- |
| SDF9 | SUBSUELO COLEGIO. | 1 | 24/2 | 20/1 |
| SDF10.1, 2, 3. | ESC. CTDB BLOUE A. | 3 | 72/6 | 62/1 |
| SDF11.1, 2, 3. | ESC. CTDB BLOQUE B. | 3 | 72/6 | 30/1 |

Elaborado por: Leonardo Suárez.

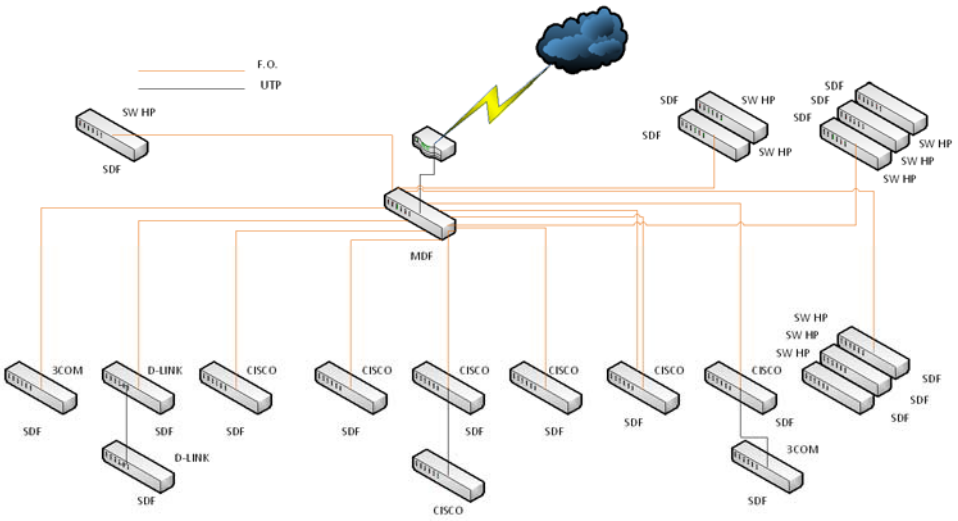
#### 3.1.1.7. Proveedores de servicios externos (Servicio de Internet)

En la infraestructura establecida de Networking de la Obra Salesiana, se dispone de un enlace para el acceso a Internet contratado con la empresa Telconet, La velocidad del enlace de acceso a Internet es de 23 Mbps que le brinda la UPS y cumple con las siguientes funciones:

Brinda acceso a los servicios de navegación y acceso al correo electrónico.
En lo relacionado a la infraestructura de comunicaciones utilizada para brindar este servicio se debe señalar que se lo realiza mediante la utilización de una línea dedicada que se interconecta directamente con los equipos del proveedor a través Router Cisco 881.

En las siguientes tablas se detallan el tipo de líneas utilizadas para realizar las conexiones hacia el proveedor de Internet y el equipamiento utilizado.

Figura 19. Línea usada para conexión a ISP.




Elaborado por: Leonardo Suárez.

Tabla 6. Equipos usados para conexión a Internet.

| CANTIDAD | DISPOSITIVO | FUNCIÓN/SERVICIO |
|---|---|---|
| 1 | CISCO 881 | Bridge/Switch Cisco Internet 23 Mbps |

Elaborado por: Leonardo Suárez.

Para el acceso a Internet el proveedor del servicio ha asignado una subred con 30 direcciones IP públicas (Direcciones IP Reales). Lo relacionado al direccionamiento IP (IP no reales) que se utiliza en las subredes se resume a continuación:

Direccionamiento IP:

| | |
|---|---|
| Nombre: | Subred Internet |
| Descripción: | Acceso a Internet 23 Mbps |
| Network: | 190.95.206.164 |
| Mascara: | 255.255.255.224 |
| Rango IP: | 190.95.206.161- 190.95.206.190 |
| Núm. Hosts: | 30 válidos (1 Subred y 1 Broadcast) |

Se debe mencionar que la implementación subredes administrativas y de laboratorio se conectan a través de un servidor Linux que cumple con la funcionalidad de Proxy Firewall.

La necesidad de implementar una nueva infraestructura tecnológica que prepare lo que sea necesario para la implementación de aplicaciones y servicios estandarizados en toda la Casa Inspectorial Salesiana, inició un proceso de planificación y de ajuste en toda la infraestructura física y de direccionamiento lógico de la red como una medida necesaria para iniciar el proyecto a nivel nacional en las diferentes obras.

#### 3.1.1.8. Servicios

Para brindar los servicios de WEB Server y correo electrónico dentro del actual esquema de comunicaciones se lo hace a través de acceso al Internet ya que cuentan con los servicios en la nube. Este problema debe ser corregido incluyendo los servidores en una DMZ (Red Desmilitarizada) y expuesta hacia el Internet mediante la utilización de esquemas NAT (traducción de direcciones).

La obra Salesiana cuenta con algunas oficinas administrativas y laboratorios, los cuales están distribuidos en diferentes dependencias, cada una de estas, tienen equipos informáticos conectados en red, estos laboratorios llevan un orden en la infraestructura de la red pero no en instalaciones, ya que se acoplaron a la segmentación de red de la UPS, la misma que les da soporte en infraestructura y redes.

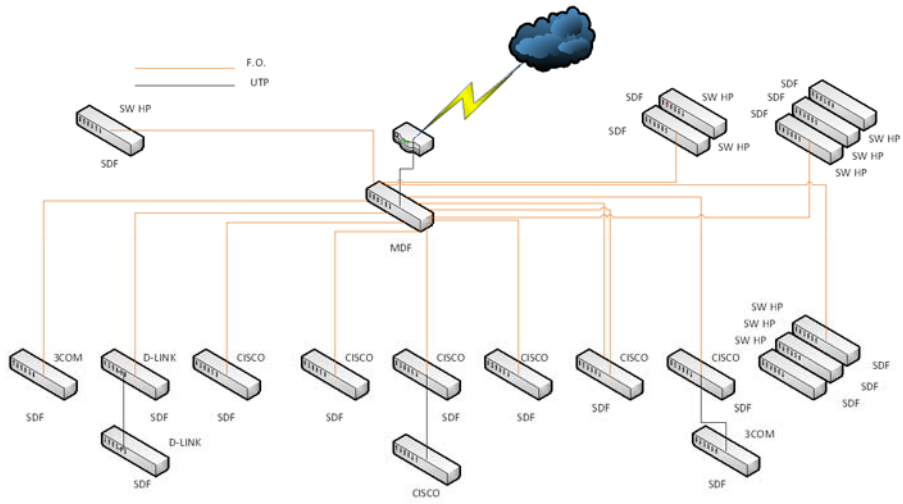
Los edificios que conforman la obra no prestan las debidas facilidades para la instalación de elementos activos y pasivos de Networking, por lo que es necesario realizar algunas modificaciones a las edificaciones y de esta manera adecuar el espacio físico en donde se situará los mencionados elementos.
En la actualidad se lleva a cabo la construcción de un proyecto y la instalación del cableado estructurado que garantizará a los usuarios la funcionalidad y disponibilidad a través de AP’s de la red.

El acceso a la red y la comunicación de los dos edificios principales se lo realiza a través de un enlace de fibra óptica vía interna que atraviesa de un bloque a otro.

Dentro de un proceso de mejora continua de los proveedores de servicio ISP y de algunas adaptaciones realizadas a requerimientos nacionales de la obra, la salida de

Internet de la obra del colegio no ha tenido modificaciones en la infraestructura tecnológica con los proveedores de servicios (ISP).

Figura 20. Diagrama de acceso a Internet a la obra Salesiana.




Elaborado por: Leonardo Suárez.

La propuesta se basará en algunos diseños de red establecidos basados en Cisco (CEAM) para aplicaciones y servicios estandarizados en toda la Casa Inspectorial Salesiana.

Además se va a empezar un proceso de planificación y de ajustes en toda la infraestructura física y de direccionamiento lógico de la red como una medida necesaria para iniciar el proyecto de diseño con las obras a nivel nacional, como son Riobamba, Ibarra y Esmeraldas.

En la Casa Inspectorial sede Quito con sus obras alrededor se tiene que cambiar el direccionamiento para que se restablezca la comunicación entre la matriz y sus obras para poder adaptarse con la infraestructura actual y preparar a la Casa Inspectorial sede Quito para el proyecto nacional de interconexión.

En la Casa Inspectorial Salesiana se va a diseñar el direccionamiento lógico para poder acoplarse con algunas de las obras a nivel nacional.

La infraestructura D-Link, 3Com y Cisco (equipos de la UPS), es la red actual de la Casa Inspectorial Salesiana la cual brinda el soporte necesario para la creación de VLAN’s, por lo que existe 6 subredes y es provista por la UPS.

### 3.1.2. Obra Unidad Educativa Salesiana Fiscomisional "Don Bosco" La Tola

#### 3.1.2.1. Ubicación

Esta obra se encuentra ubicado en Quito sector La Tola en las calles Vicente León y Los Ríos.

#### 3.1.2.2.Situación actual

En el diseño de la infraestructura de Networking de la obra Don Bosco La Tola no se puede apreciar claramente una estructura de distribución física de los equipos de acuerdo a su funcionalidad, pero para efectos de este análisis se ha decido clasificarlos de acuerdo al rol que cumple cada uno de los equipos y su similitud con las funciones de cada una de las capas de un diseño de Networking (Core o Núcleo, Acceso y Distribución), para detallar la función de cada uno en la infraestructura actual en el que se va a basar en el modelo Cisco Enterprise Architecture Model.

#### 3.1.2.3. Capa de Core o Núcleo

Esta capa está conformada por: switch Cisco Gigabit SG300-52 que contiene 52 interfaces GigaEthernet a través de 2 enlaces de fibra óptica. Este switch está ubicado en el MDF1 en los laboratorios de Informática, a través de este Switch se brinda el servicio de backbone (Núcleo de la red), conectándose a los switch’s de la capa de acceso ubicados en los SDF’s (cuartos de distribución secundarios de cableado) mediante la utilización de enlaces de fibra óptica. La velocidad de comunicación del Backbone es de hasta 1Gbps.

#### 3.1.2.4. Capa de Distribución

Esta capa está conformada por 1 Switch Cisco Gigabit SG300-52 y 3 Switch's TP-Link Gigabit TL-SG1024 distribuidos de la siguiente manera:

Switch Cisco Gigabit SG300-52 ubicado en el MDF1 de la oficina de informática, este dispositivo brinda servicio de acceso Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de un enlace de fibra óptica a 1 Gbps.

Switch's 3Com ubicado en el SDF0 ubicado en los laboratorios de Informática, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de fibra óptica a 1 Gbps.

Switch's TP-Link Gigabit TL-SG1024 ubicado en el SDF1 ubicado 1er Piso, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de fibra óptica a 1 Gbps.

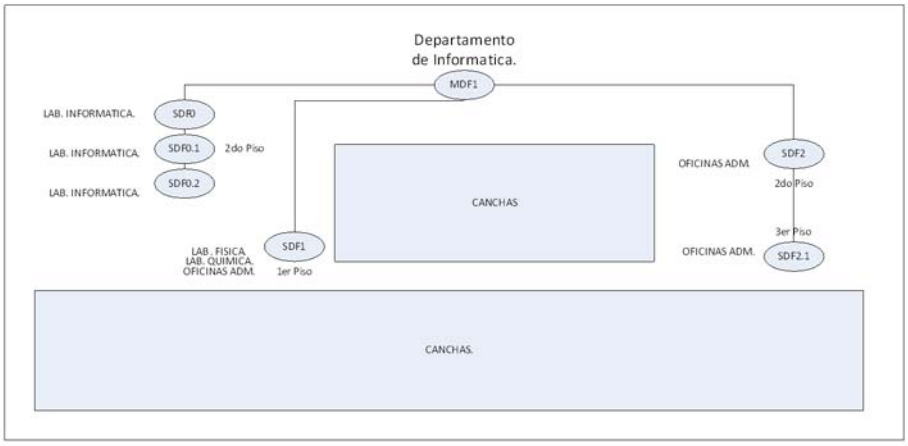
Switch's TP-Link Gigabit TL-SG1024 ubicado en el SDF2 ubicado 2do Piso, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de fibra óptica a 1 Gbps.

Switch's TP-Link Gigabit TL-SG1024 ubicado en el SDF2.1 ubicado 3er Piso, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps.

### 3.1.2.5. Capa de Acceso

Esta capa está conformada por 1 Switch 3Com y 3 Switch's TP-Link Gigabit TL-SG1024, en la cual se encuentran incluidos los switches de acceso. La distribución de los switches de esta capa es la siguiente:

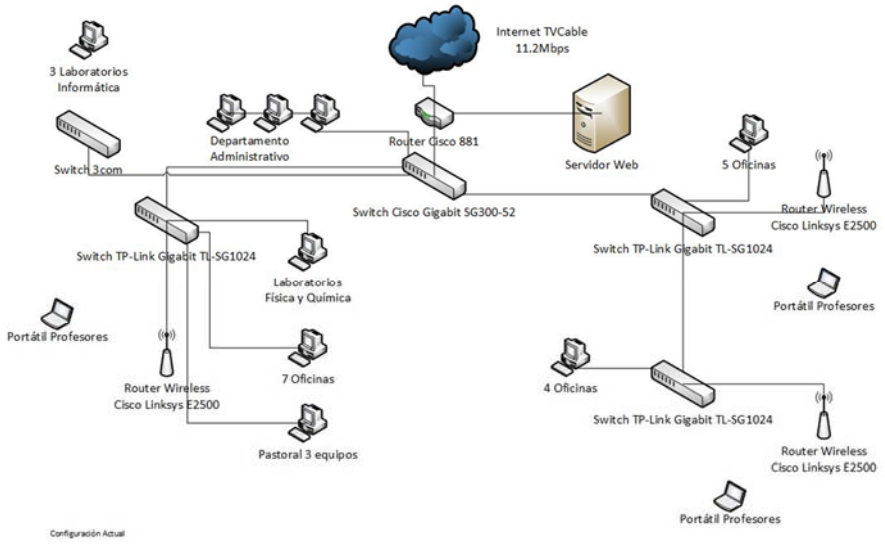
Figura 21. Diagrama de distribución MDF y SDF interna de la obra.




Elaborado por: Leonardo Suárez.

La topología que se emplea en esta red es del tipo cascada, la misma que está conformada en su mayoría por Switch's cuya funcionalidad está limitada a la transmisión de paquetes para aproximadamente 284 dispositivos de red. A continuación se presenta un diagrama del esquema de conectividad de la infraestructura de red.

Figura 22. Diagrama de distribución MDF y SDF de la red LAN de la obra.




Elaborado por: Leonardo Suárez.

A continuación un breve resumen de los MDF y SDF's de la obra Don Bosco La Tola.

Tabla 7. Tabla de distribución MDF y SDF's.

| FUNCIÓN | DISPOSITIVO | INTERFACE | UBICACIÓN | VELOCIDAD | SERVICIOS |
|---|---|---|---|---|---|
| CORE | MDF1 | UTP/F.O. | OFIC INFORMAT. | 100Mbps/1Gbps | Pág. Web mail e Internet |
| ACCESO | SDF0 | UTP | LAB. INFOR. | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF1 | F.O. | LAB. FIS. QUIMIC. | 1Gbps | Pág. Web mail e Internet |
| ACCESO | SDF2 | F.O. | DEP ADMINIST. | 1Gbps | Pág. Web mail e Internet |
| ACCESO | SDF2.1 | UTP | SALA DE PROFESORES | 100Mbps | Pág. Web mail e Internet |

Elaborado por: Leonardo Suárez.

En lo referente a los servicios de autenticación, acceso a Internet, correo electrónico y aplicaciones de usuarios de la obra se utilizan los siguientes servidores:

Tabla 8: Servidor de la obra Don Bosco.

| Código | Modelo | Funcionalidad |
|---|---|---|
| SER1 | HP PROLIANT ML370 G6 | Servidor de página web. Memoria 6 GB RAM Windows 2003. |

Elaborado por Leonardo Suárez.

### 3.1.2.6. Análisis de la infraestructura lógica

La red LAN establecida en la obra Salesiana utiliza Ethernet como el protocolo de comunicaciones y utiliza los estándares 10BaseT y 100BaseT. Por otra parte como protocolo de red se utiliza TCP/IP.

La clase de dirección la red TCP/IP que se utiliza es del tipo C privada. Esta subred es proporcionada por los ISP la misma que utiliza direcciones IP privadas y que tiene las siguientes características:

Direccionamiento IP:

| | |
|---|---|
| Nombre: | Subred LAN Don Bosco La Tola. |
| Descripción: | Red LAN Don Bosco La Tola |
| Network: | 192.168.0.0 |
| Mascara: | 255.255.255.0 |
| Rango IP: | 192.168.0.1 - 192.168.0.255 |
| Núm. Hosts: | 254 válidos (1 Subred y 1 Broadcast) |

Cabe recalcar que este direccionamiento IP es similar al utilizado en las demás Obras, lo cual es necesario cambiarlo si se desea integrar los mismos en una sola red que abarque todas las Obras de la Casa Inspectorial Salesiana sede Quito.

En los diferentes dominios de colisiones y dominios de broadcast se debe mencionar que actualmente existe un solo dominio en la obra, por lo cual no existe una segmentación de red, por este motivo son más propensos a recibir ataques externos, como virus que se propaguen por broadcast a los dispositivos finales y podrían verse afectados.

La red LAN de la obra La Tola de la Casa Inspectorial Salesiana brinda servicio a aproximadamente 284 estaciones de trabajo de las cuales 80 son utilizadas por personal de la obra y las restantes 204 son equipos de computación ubicados en laboratorios. En la siguiente tabla se muestra la distribución de switches y salidas de datos por cada uno de los SDF existente en la obra Don Bosco La Tola.

Tabla 9: Distribución de Switch’s Obra Don Bosco La Tola.

| CÓDIGO | NOMBRE DEL SDF | CANT. SWITCH | CANT. PORTS UTP/F.O. | CANT. PORTS LIBRES UTP/F.O. |
|---|---|---|---|---|
| MDF1 | MDF en el departamento de Informática | 1 | 48/4 | 38/3 |
| SDF0, 0.1 y 0.2 | SDF en los laboratorios de Informática. | 3 | 144/4 | 90/2 |
| SDF1 | SDF Laboratorio de física y química | 1 | 48/4 | 42/3 |
| SDF2 | SDF en el Departamento Administrativo u oficinas. | 1 | 48/4 | 29/3 |
| SDF2.1 | SDF en el departamento Sala de profesores | 2 | 48/- | 40/- |

Elaborado por Leonardo Suárez.

### 3.1.2.7. Proveedores de servicios externos (Servicio de Internet)

En la infraestructura establecida de Networking de la Obra Salesiana, se dispone de un enlace para el acceso a Internet contratado con la empresa TV Cable, La velocidad del enlace de acceso a Internet es de 11.2 Mbps y cumple con las siguientes funciones: Brinda acceso a los servicios de navegación y acceso al correo electrónico.

En lo relacionado a la infraestructura de comunicaciones utilizada para brindar este servicio se debe señalar que se lo realiza mediante la utilización de una línea dedicada que se interconecta directamente con los equipos del proveedor a través router Cisco 881 que al mismo tiempo cumple con las funciones de ruteador.

En la siguiente tabla se detalla el tipo de línea utilizada para realizar las conexiones hacia el proveedor de Internet y el equipamiento utilizado.

Tabla 10. Líneas Dial up para usuarios remotos.

| RACK | CÓDIGO | DESCRIPCIÓN | LP Ó LINEA |
|---|---|---|---|
| Est. Módems | COM1 | Línea de acceso Dial Up | Dial Up |

Elaborado por Leonardo Suárez.

Tabla 11. Equipos para prestar servicio de Internet a usuarios remotos.

| CANTIDAD | DISPOSITIVO | FUNCIÓN/SERVICIO |
|---|---|---|
| 1 | Router Cisco 2801 | Router de Internet 2 Ports GigaEthernet |

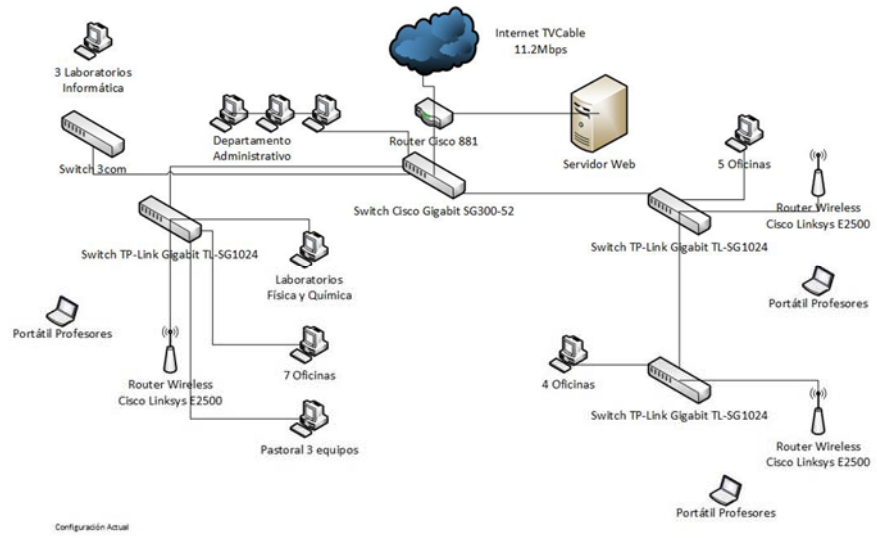
Elaborado por Leonardo Suárez.

Debido a que existe un enlace para el acceso a Internet, el proveedor del servicio ha asignado dos subredes con direccionamiento IP público (direcciones IP simuladas). Lo relacionado al direccionamiento IP que se utiliza para cada una de las subredes se resumen a continuación:

Direccionamiento IP:

| | |
|---|---|
| Nombre: | Subred Internet |
| Descripción: | Acceso a Internet 11.2 Mbps |
| Network: | 64.46.84.192 |
| Mascara: | 255.255.255.248 |
| Rango IP: | 64.46.84.192 - 64.46.84.199 |
| Núm. Hosts: | 6 válidos (1 Subred y 1 Broadcast) |

Figura 23. Línea usada para conexión a ISP.




Elaborado por: Leonardo Suárez.

Tabla 12. Equipos usados para conexión a Internet.

| **Cantidad** | **Dispositivo** | **Función/Servicio** |
|---|---|---|
| 1 | CISCO 881 | Bridge/Switch Cisco Internet 11.2 Mbps |

Elaborado por Leonardo Suárez.

Para el acceso a Internet el proveedor del servicio ha asignado una subred con 8 direcciones IP públicas (Direcciones IP Reales). Lo relacionado al direccionamiento IP que se utiliza en las subredes se resume a continuación:

Direccionamiento IP:

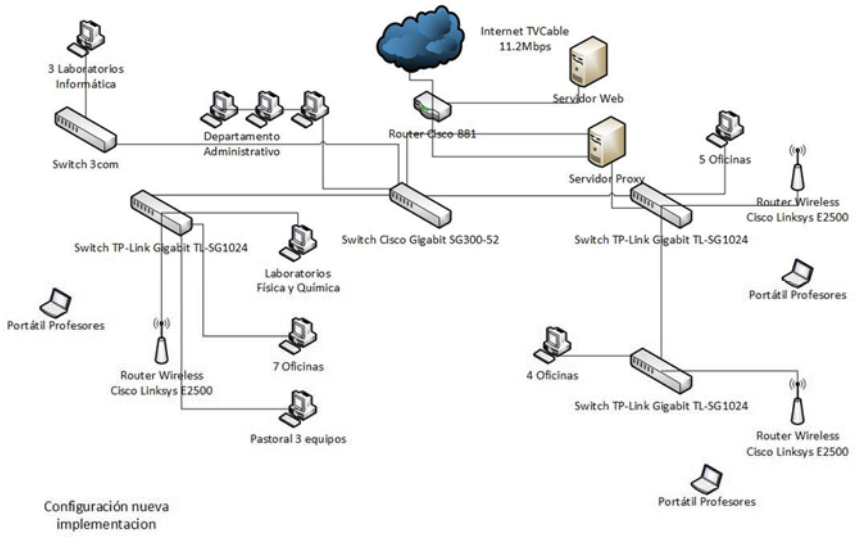
| | |
|---|---|
| Nombre: | Subred Internet |
| Descripción: | Acceso a Internet 11.2 Mbps |
| Network: | 64.46.84.192 |
| Mascara: | 255.255.255.248 |
| Rango IP: | 64.46.84.192 - 64.46.84.199 |
| Núm. Hosts: | 6 válidos (1 Subred y 1 Broadcast) |

Se debe mencionar que la implementación subredes administrativas y de laboratorio se conectan a través de un servidor Linux que cumple con la funcionalidad de proxy Firewall.

En la actualidad se lleva a cabo la realización de un servidor proxy implementado en Linux.

En el siguiente diagrama se muestra los componentes utilizados y las interconexiones existen que son utilizadas para brindar el servicio de Internet.

Figura 23. Diagrama de acceso a Internet con servidor proxy




Elaborado por: Leonardo Suárez.

La necesidad de implementar una nueva infraestructura tecnológica que prepare lo que sea necesario para la implementación de aplicaciones y servicios estandarizados en toda la obra Salesiana, inicio un proceso de planificación y de ajuste en toda la infraestructura física y de direccionamiento lógico de la red como una medida necesaria para iniciar el proyecto a nivel nacional en las diferentes obras.

#### 3.1.2.8. Servicios

A continuación se hace un breve resumen del diseño establecido de red. Además los diferentes servicios y aplicaciones más relevantes de la obra se presentan a continuación.

Para brindar los servicios de WEB Server y correo electrónico dentro del actual esquema de comunicaciones se utilizan dos servidores, los mismos que poseen dos tarjetas de red; la primera para conectarse con la red interna y la segunda para conectarse a Internet, por lo cual existe un bucle en cada uno de los servidores y al verse expuestos directamente hacia Internet no se benefician del firewall que actualmente existe instalado utilizando Linux. Este problema debe ser corregido incluyendo los servidores en una DMZ (Red Desmilitarizada) y expuesta hacia el Internet mediante la utilización de esquemas NAT (Traducción de Direcciones).

La obra Salesiana cuenta con algunas oficinas administrativas y laboratorios, los cuales están distribuidos en diferentes dependencias, cada una de estas, tienen equipos informáticos conectados en red, pero estos laboratorios no llevan un orden tanto en infraestructura e instalaciones.

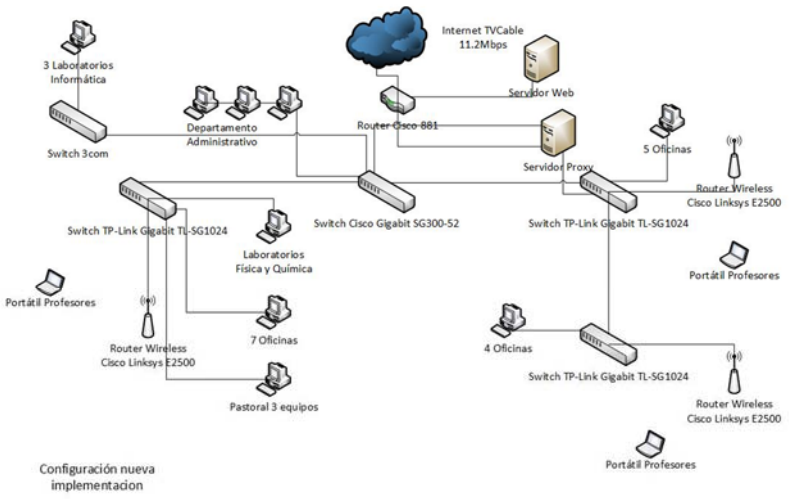
Los edificios que conforman el campus de la institución no prestan las debidas facilidades para la instalación de elementos activos y pasivos de Networking, por lo que es necesario realizar algunas modificaciones a las edificaciones y de esta manera adecuar el espacio físico en donde se situará los mencionados elementos.

En la actualidad se lleva a cabo la construcción de un proyecto y la instalación del cableado estructurado que garantizará a los usuarios la funcionalidad y disponibilidad a través de AP's de la red.

El acceso a la red y la comunicación de los dos edificios principales se lo realiza a través de un enlace de cable UTP vía interna que atraviesa de un bloque a otro.

Dentro de un proceso de mejora continua de los proveedores de servicio ISP y de algunas adaptaciones realizadas a requerimientos nacionales de la obra, la salida de Internet de la obra del colegio no ha tenido modificaciones en la infraestructura tecnológica con los proveedores de servicios (ISP).

Figura 24. Diagrama de acceso a Internet a la obra Salesiana.




Elaborado por Leonardo Suárez.

La propuesta se basará en algunos diseños de red establecidos basados en Cisco (CEAM) para aplicaciones y servicios estandarizados en toda la Casa Inspectorial Salesiana.

Además se va a empezar un proceso de planificación y de ajustes en toda la infraestructura física y de direccionamiento lógico de la red como una medida necesaria para iniciar el proyecto de diseño con las obras a nivel nacional, como son Riobamba, Ibarra y Esmeraldas.

En la Casa Inspectorial sede Quito con sus obras alrededor se tiene que cambiar el direccionamiento para que se restablezca la comunicación entre la matriz y sus obras para poder adaptarse con la infraestructura actual y preparar a la Casa Inspectorial sede Quito para el proyecto nacional de interconexión.

En la Casa Inspectorial Salesiana se va a diseñar el direccionamiento lógico para poder acoplarse con algunas de las obras a nivel nacional.

La infraestructura D-Link, Cisco (equipos de la UPS), es la red actual de la Casa Inspectorial Salesiana que no brinda aún el soporte necesario para la creación de VLAN's, por lo que solo existe una subred y es brindada por los ISP.

### 3.1.3. Obra Sánchez Cifuentes Ibarra.

#### 3.1.3.1. Ubicación

Esta obra se encuentra ubicada al norte de la ciudad de Quito cuenta con dos bloques de edificios, ubicados a la altura de la Avenida Sucre 12-52 y Obispo Mosquera (Toda la manzana).

**Situación actual.**

En el diseño de la infraestructura de red (Networking) de la Obra Sánchez Cifuentes no muestra una estructura clara de la distribución física de los equipos de acuerdo a su funcionalidad, pero para efectos de este análisis se ha decido clasificarlos de acuerdo al rol que cumple cada uno de los equipos y su similitud con las funciones de cada una de las capas de un diseño jerárquico de Networking (Core, Distribución y Acceso):

para detallar la función de cada uno en la infraestructura actual en el que se va a basar en el modelo Cisco Enterprise Architecture Model.

#### 3.1.3.2. Capa Core o Núcleo.

Está capa está conformada por: Switch D-Link DG1024D Gigabit Switch que contiene 24 interfaces Ethernet a través de 1 enlace de Ethernet del ISP.
Está ubicado en el MDF1 en el Departamento de Informática segundo piso, brinda servicio de Backbone (Núcleo de la red), allí se conectan 4 Switch's de la capa de acceso ubicados en los SDF's (Departamentos de Secretaria, Financiero, Biblioteca y laboratorios de informática tanto el colegio como la escuela) mediante cable UTP. La velocidad del Backbone es de hasta 100 Mbps.

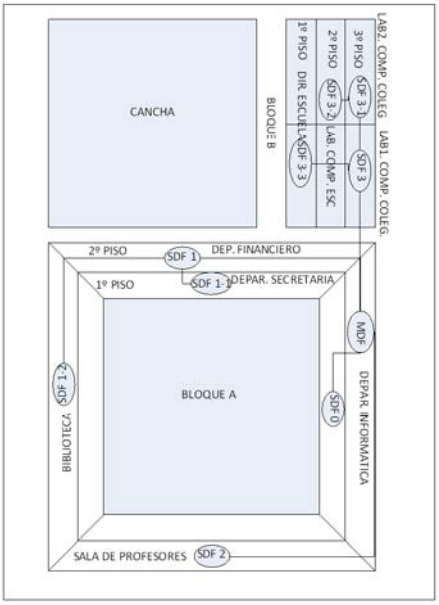
**Capa de Distribución**

Está capa está conformada por 4 Switch's distribuidos de la siguiente manera.
Switch D-Link DES-1008D Ubicado en el SDF1 en el departamento Financiero (Planta Baja del Bloque A), Brinda servicio de acceso a la red y la conectividad con Switch's de la capa de acceso a través de enlaces UTP Velocidades de hasta 100 Mbps.
Switch D-Link DES-1008D ubicado en el SDF2 en el departamento de secretaria (Primer piso Bloque A), este dispositivo brinda servicio de acceso a la red y la conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps.
Switch D-Link DES-1024Di ubicado en el SDF3 en la biblioteca (Primer Piso del Bloque A), este dispositivo brinda servicio de acceso a la red y la conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps.
Switch D-Link DES-1008D ubicado en el SDF4 de la Sala de profesores (Primer Piso del Bloque A), este dispositivo brinda servicio de acceso a la red y la conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps.
Switch D-Link DES- DG1024D ubicado en el SDF5 en los laboratorios de informática (Tercer Piso del Bloque A), este dispositivo brinda servicio de acceso a la red y la conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps.

### 3.1.3.3. Capa de Acceso

Esta capa está conformada por 8 Switch's, en la cual se encuentran incluidos los Switch's de la Capa de acceso debido a que cumplen con esta funcionalidad.

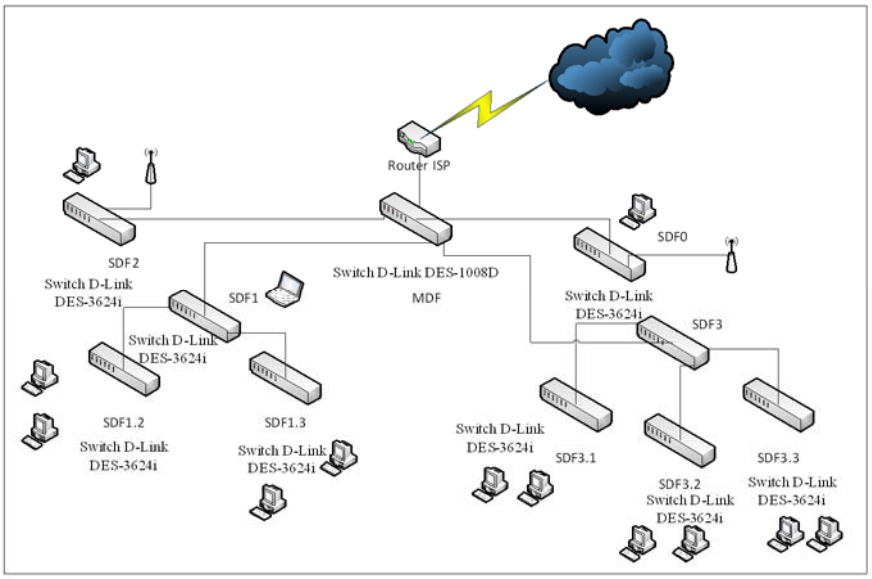
Figura 25. Diagrama de distribución MDF y SDF interna de la red LAN Sánchez Cifuentes Ibarra. (Conexiones UTP).




Elaborado por Leonardo Suárez.

La topología de conectividad que se emplea en esta red es del tipo estrella extendida, la misma que está conformada en su mayoría por Switch's cuya funcionalidad está limitada a la transmisión de paquetes para aproximadamente 120 dispositivos de red. A continuación se presenta un diagrama del esquema de conectividad de la infraestructura de red.

Figura 26. Diagrama de distribución MDF y SDF de la red LAN de la obra.




Elaborado por Leonardo Suárez.

A continuación un breve resumen de los MDF y SDF's de la obra Sánchez Cifuentes Ibarra.

Tabla 13. Resumen de Switch's MDF y SDF's.

| FUNCIÓN | DISPOSITIVO | INTERFACE | UBICACIÓN | VELOCIDAD | SERVICIOS |
|---|---|---|---|---|---|
| CORE | MDF1 | UTP | OFIC INFORMAT. | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF0 | UTP | OFIC INFORMAT. | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF1 | UTP | DEP. FINAN. | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF1,1 | UTP | DEP SECRET. | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF1,2 | UTP | BIBLIOTECA | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF2 | UTP | SALA DE PROFESORES | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF3 | UTP | LAB. COM. COL | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF3,1 | UTP | LAB. COM. COL | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF3,2 | UTP | LAB. COMP. ESC. | 100Mbps | Pág. Web mail e Internet |
| ACCESO | SDF3,3 | UTP | DIRECCIÓN ESC/COL | 100Mbps | Pág. Web mail e Internet |

Elaborado por Leonardo Suárez.

En lo referente a todos los servicios que contiene la obra, algunos de estos son: correo electrónico, página Web y aplicaciones. Los usuarios de la obra, tienen todos estos servicios en la nube, por lo cual acceden a sus aplicaciones a través de Internet.

.

### 3.1.3.4. Análisis de la infraestructura lógica

La red LAN establecida en la obra Sánchez Cifuentes de la ciudad de Ibarra utiliza Ethernet como el protocolo de comunicaciones y utiliza los estándares 10BaseT y 100BaseT. Por otra parte como protocolo de red se utiliza TCP/IP.

La clase de dirección la red TCP/IP que se utiliza es del tipo C privada. Esta subred es proporcionada por los ISP la misma que utiliza direcciones IP privadas y que tiene las siguientes características:

Direccionamiento IP:

| | |
|---|---|
| Nombre: | Subred LAN Sánchez Cifuentes |
| Descripción: | Red LAN Sánchez Cifuentes |
| Network: | 192.168.0.0 |
| Mascara: | 255.255.0.0 |
| Rango IP: | 192.168.0.0 - 192.168.255.255 |
| Núm. Hosts: | 65534 válidos (1 Subred y 1 Broadcast) |

Cabe recalcar que este direccionamiento IP es similar al utilizado en las demás obras, lo cual es necesario cambiarlo si se desea integrar los mismos en una sola red que abarque todas las obras de la Casa Inspectorial Salesiana sede Quito.

En los diferentes dominios de colisiones y dominios de broadcast se debe mencionar que actualmente existe un solo dominio en la obra, lo cual no existe una segmentación de red por lo cual son propensos a recibir ataques externos, como virus que se propaguen por broadcast a los dispositivos finales y podrían verse afectados.

La red LAN de la obra Sánchez Cifuentes de la Casa Inspectorial Salesiana brinda servicio a aproximadamente 120 estaciones de trabajo de las cuales son 40 utilizadas por personal de la obra y las restantes 80 son equipos de computación ubicados en aulas de laboratorios para estudiantes. En la siguiente tabla se muestra la distribución

de Switches y salidas de datos por cada uno de los SDF existente en la Obra Sánchez Cifuentes.

Tabla 14. Distribución de los Switch's Obra Sánchez Cifuentes

| CÓDIGO | NOMBRE DEL SDF | CANT. SWITCH | CANT. PORTS UTP/F.O. | CANT. PORTS LIBRES UTP/F.O. |
|---|---|---|---|---|
| MDF1 | MDF en el departamento de Informática | 1 | 24/- | 2/- |
| SDF0 | SDF en el departamento de Informática | 1 | 24/- | 14/- |
| SDF1 | SDF en el departamento Financiero | 1 | 8/- | 4/- |
| SDF1-1 | SDF en el departamento de Secretaria | 1 | 8/- | 5/- |
| SDF1-2 | SDF en la Biblioteca | 1 | 8/- | 6/- |
| SDF2 | SDF en el departamento de secretaria | 1 | 8/- | 2/- |
| SDF3 | SDF en laboratorio 1 de computación | 1 | 24/- | 3/- |
| SDF3-1 | SDF en laboratorio 2 de computación | 1 | 24/- | 3/- |
| SDF3-2 | SDF en laboratorio 3 de computación. | 1 | 24/- | 3/- |
| SDF3-3 | SDF en laboratorio de computación ESC. | 1 | 24/- | 4/- |

Elaborado por Leonardo Suárez.

### 3.1.3.5.Proveedores de servicios externos (Servicio de Internet)

En la infraestructura establecida de Networking de la Obra Salesiana, se dispone de un enlace para el acceso a Internet contratado con la empresa CNT, La velocidad del enlace de acceso a Internet es de 15 Mbps y cumple con las siguientes funciones:
Brinda acceso a los servicios de navegación y acceso al correo electrónico.

En lo relacionado a la infraestructura de comunicaciones utilizada para brindar este servicio se debe señalar que se lo realiza mediante la utilización de 1 línea dedicada

que se interconecta directamente con los equipos del proveedor a través Router Cisco 881 que al mismo tiempo cumple con las funciones de ruteador.

En la siguiente tabla se detalla el tipo de línea utilizada para realizar las conexiones hacia el proveedor de Internet y el equipamiento utilizado.

Tabla 15. Líneas Dial up para usuarios remotos.

| RACK | CÓDIGO | DESCRIPCIÓN | LP Ó LINEA |
|---|---|---|---|
| Est. Módems | COM1 | Línea de acceso Dial Up | Dial Up |

Elaborado por Leonardo Suárez.

Tabla 16. Líneas Dial up para usuarios remotos.

| CANTIDAD | DISPOSITIVO | FUNCIÓN/SERVICIO |
|---|---|---|
| 1 | D-Link DES-1024R+ | Switch Servicios de Internet 24 UTP Ports |

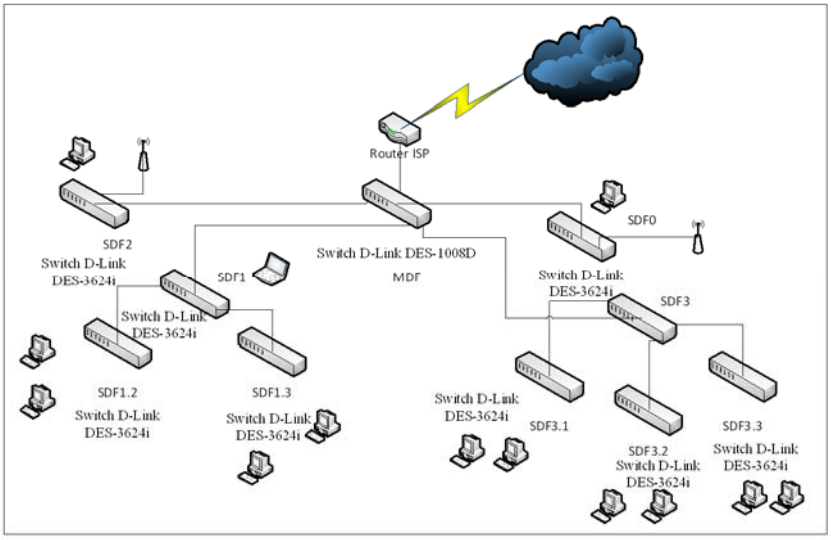
Elaborado por Leonardo Suárez.

Debido a que existe un enlace para el acceso a Internet, el proveedor del servicio ha asignado dos subredes con direccionamiento IP público (direcciones IP simuladas).
Lo relacionado al direccionamiento IP que se utiliza para cada una de las subredes se resumen a continuación:

Direccionamiento IP:

| | |
|---|---|
| Nombre: | Subred Internet |
| Descripción: | Acceso a Internet 15 Mbps |
| Network: | 64.46.84.192 |
| Mascara: | 255.255.255.248 |
| Rango IP: | 64.46.84.192 - 64.46.84.199 |
| Núm. Hosts: | 6 válidos (1 Subred y 1 Broadcast) |

Figura 27. Línea usada para conexión a ISP




Elaborado por Leonardo Suárez.

La necesidad de implementar una nueva infraestructura tecnológica que prepare lo que sea necesario para la implementación de aplicaciones y servicios estandarizados en toda la obra Salesiana, inicio un proceso de planificación y de ajuste en toda la infraestructura física y de direccionamiento lógico de la red como una medida necesaria para iniciar el proyecto a nivel nacional en las diferentes obras.

#### 3.1.3.6. Servicios

A continuación se hace un breve resumen del diseño establecido de red. Además los diferentes servicios y aplicaciones más relevantes de la obra en lo cual se realiza a continuación.

Acceso a Internet Dial up. (A los usuarios remotos que se conectan a la red vía RAS se les asigna unas 30 direcciones IP de este segmento para que puedan hacer uso de este servicio.)

Para brindar los servicios de WEB Server y correo electrónico dentro del actual esquema de comunicaciones se utilizan dos servidores, los mismos que poseen dos tarjetas de red; la primera para conectarse con la red interna y la segunda para conectarse a Internet, por lo cual existe un bucle en cada uno de los servidores y al

verse expuestos directamente hacia Internet no se benefician del firewall que actualmente existe instalado utilizando Linux. Este problema debe ser corregido incluyendo los servidores en una DMZ (Red Desmilitarizada) y expuesta hacia el Internet mediante la utilización de esquemas NAT (Traducción de Direcciones).

La obra Salesiana cuenta con algunas oficinas administrativas y laboratorios, los cuales están distribuidos en diferentes dependencias, cada una de estas, tienen equipos informáticos conectados en red, pero estos laboratorios no llevan un orden tanto en infraestructura e instalaciones.

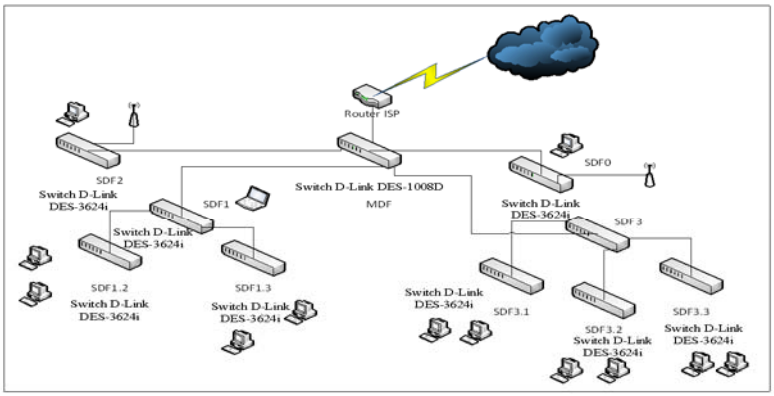
Los edificios que conforman el campus de la institución no prestan las debidas facilidades para la instalación de elementos activos y pasivos de Networking, por lo que es necesario realizar algunas modificaciones a las edificaciones y de esta manera adecuar el espacio físico en donde se situara los mencionados elementos.

En la actualidad se lleva a cabo la construcción de un proyecto y la instalación del cableado estructurado que garantizara a los usuarios la funcionalidad y disponibilidad a través de AP’s de la red.

El acceso a la red y la comunicación de los dos edificios principales se lo realiza a través de un enlace de cable UTP vía interna que atraviesa de un bloque a otro.

Dentro de un proceso de mejora continúa de los proveedores de servicio ISP y de algunas adaptaciones realizadas a requerimientos nacionales de la obra, la salida de Internet de la obra del colegio no ha tenido modificaciones en la infraestructura tecnológica con los proveedores de servicios (ISP).

Figura 28. Diagrama de acceso a Internet a la obra Salesiana.




Elaborado por Leonardo Suárez.

La propuesta se basará en algunos diseños de red establecidos basados en Cisco (CEAM) para aplicaciones y servicios estandarizados en toda la Casa Inspectorial Salesiana. Además se va a empezar un proceso de planificación y de ajustes en toda la infraestructura física y de direccionamiento lógico de la red como una medida necesaria para iniciar el proyecto de diseño con las obras a nivel nacional, como son Riobamba, Ibarra y Esmeraldas.

En la Casa Inspectorial sede Quito con sus obras alrededor se debe cambiar el direccionamiento para que se restablezca la comunicación entre la matriz y sus obras para poder adaptarse con la infraestructura actual y preparar a la Casa Inspectorial sede Quito para el proyecto nacional de interconexión.

En la Casa Inspectorial Salesiana se va a diseñar el direccionamiento lógico para poder acoplarse con algunas de las obras a nivel nacional.

La infraestructura D-Link actual de la Casa Inspectorial Salesiana no brinda aún el soporte necesario para la creación de VLAN’s, por lo que solo existe una subred y es brindada por los ISP.

### 3.1.4. Obra Colegio Fiscomisional Salesiano De Bachillerato San Rafael

#### 3.1.4.1. Ubicación

Se encuentra ubicado al noreste de la ciudad de Quito, es un conjunto de edificios ubicados C/ Porta de la Morera, 24-03203 ELCHE (Frente al Huerto del Cura).

#### 3.1.4.2. Situación actual

En el diseño de la infraestructura de Networking de la obra de Esmeraldas existe una estructura de distribución física de los equipos de acuerdo a su funcionalidad, por lo tanto para efectos de este análisis se los ha clasificado de acuerdo al rol que cumple cada uno de los equipos dentro de las capas del diseño de Networking (Core, Distribución y Acceso).

#### 3.1.4.3. Capa de Núcleo

Esta capa está conformada por: switch cisco catalyst 3560 Gigaswitch que contiene 4 interfaces GigaEthernet a través de enlaces de fibra óptica y 48 enlaces UTP. Este Switch está ubicado en el MDF del Departamento de Informática, a través de este Switch se brinda el servicio de Backbone (Núcleo de la red), conectándose a los Switch’s de la comunidad y el colegio cumplen con la función de la capa de borde ubicados en los SDF’s (Cuartos de Distribución Secundarios de cableado) mediante la utilización de enlaces de fibra óptica. La velocidad de comunicación del Backbone es de hasta 1Gbps.

#### 3.1.4.4. Capa de Distribución

Esta capa está conformada por 3 Switch’s distribuidos de la siguiente manera:
Switch cisco 2960 ubicado en el SDF1 ubicado en el colegio María Auxiliadora, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch’s de la capa de acceso a través de enlaces UTP a velocidades de hasta 100

Mbps. La conexión con el Backbone de la red se lo realiza a través de un enlace de UTP a 100 Mbps.

Switch cisco 2960 ubicado en el SDF2 ubicado en los laboratorios del colegio San Rafael, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de UTP a 100 Gbps.

Switch cisco 2960 ubicado en el SDF3 ubicado en la comunidad, este dispositivo brinda servicio de acceso al Backbone de la red y conectividad con Switch's de la capa de acceso a través de enlaces UTP a velocidades de hasta 100 Mbps. La conexión con el Backbone de la red se lo realiza a través de enlaces de UTP a 100 Gbps.

La distribución de los Switches de esta capa es la siguiente:

Tabla 17. Distribución de los Switch's de la obra.

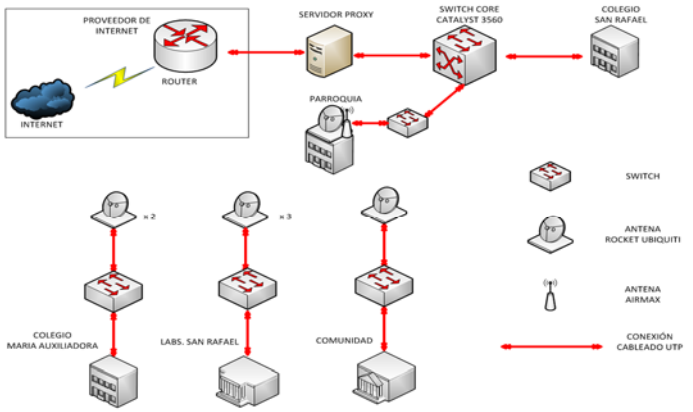
| **Código** | **Nombre del SDF** | **Cant. Switch** | **Cant. Ports UTP/F.O.** | **Puertos Usados UTP/F.O.** |
|---|---|---|---|---|
| MDF | MDF en el departamento de Informática | 1 | 24/4 | 4/2 |
| SDF0 | SDF en el departamento de Informática | 1 | 24/4 | 12/2 |
| SDF1 | SDF en el departamento Financiero | 1 | 24/- | 12/- |
| SDF2 | SDF en el departamento de Secretaria | 1 | 24/- | 14/- |
| SDF3 | SDF en la Biblioteca | 1 | 24/- | 20/- |
| SDF3.1 | SDF en el departamento de secretaria | 1 | 24/- | 10/- |

Elaborado por Leonardo Suárez.

La topología de conectividad que se emplea en esta red es del tipo estrella extendida, la misma que está conformada en su mayoría por Switch's de Capa 2, por lo cual se han implementado VLAN's para organizar las estaciones de usuarios.

Estos dispositivos brindan servicio de transmisión de datos para aproximadamente 6 dispositivos de red. A continuación se presenta un diagrama del esquema de conectividad de la infraestructura de red.

Figura 29. Diagrama de acceso a Internet a la obra Salesiana




Elaborado por Leonardo Suárez.

En lo referente a los servicios de autenticación, acceso a Internet, correo electrónico y aplicaciones de usuarios de la obra se utilizan los siguientes servidores:

Tabla 18. Servidor de la obra.

| **Código** | **Modelo** | **Funcionalidad** |
|---|---|---|
| SER1 | IBM SYSTEM X3650-M3 RACK 2U | Servidor de página web. Memoria 4 GB RAM Linux. |

Elaborado por Leonardo Suárez.

A continuación un breve resumen de los MDF y SDF's de la obra San Rafael de Esmeraldas.

Tabla 19. Distribución de los MDF y SDF's de la obra.

| Función | Dispositivo | Interface | Ubicación | Velocidad | Servicios |
|---|---|---|---|---|---|
| CORE | MDF | UTP | DEP. INFO | 100Mbps | Núcleo de la red. |
| ACCESO | SDF1 | UTP | PARROQUIA | 100Mbps | Internet, pág. WEB. |
| ACCESO | SDF2 | UTP | MARIA AUX. | 100Mbps | Internet, pág. WEB. |
| ACCESO | SDF3 | UTP | LAB. SAN RAFAEL | 100Mbps | Internet, pág. WEB. |
| ACCESO | SDF4 | UTP | COMUNIDAD | 100Mbps | Internet, pág. WEB. |

Elaborado por Leonardo Suárez.

#### 3.1.4.5. Análisis de la infraestructura lógica

La red LAN establecida en la obra Salesiana utiliza Ethernet como el protocolo de comunicaciones y utiliza los estándares 10BaseT y 100BaseT. Por otra parte como protocolo de red se utiliza TCP/IP.

La Clase de dirección de red TCP/IP que se utiliza es del tipo C. Está subred está dividida en dos segmentos de red independientes; el primer segmento se lo utiliza para brindar el servicio de red y acceso a Internet a los usuarios administrativos; y, el segundo segmento para brindar acceso a los laboratorios. Las direcciones IP privadas que son utilizadas por cada uno de estos segmentos tienen las siguientes características:

Direccionamiento IP:

| | |
|---|---|
| Nombre: | Subred LAN Administrativa |
| Descripción: | Red LAN de la obra Administrativa |
| Network: | 192.168.0.0 |
| Mascara: | 255.255.255.0 |
| Rango IP: | 192.168.0.1 - 192.168.0.255 |
| Núm. Hosts: | 254 válidos (1 Subred y 1 Broadcast) |
| Nombre: | Subred LAN Laboratorios |

| | |
|---|---|
| Descripción: | Red LAN de la obra de los laboratorios |
| Network: | 192.168.10.0 |
| Mascara: | 255.255.255.0 |
| Rango IP: | 192.168.10.1 - 192.168.10.255 |
| Núm. Hosts: | 254 válidos (1 Subred y 1 Broadcast) |

Cabe recalcar que este direccionamiento IP es similar al utilizado en las demás obras, lo cual es necesario cambiarlo si se desea integrar los mismos en una sola red que abarque todas las obras de la Casa Inspectorial Salesiana sede Quito.

En los diferentes dominios de colisiones y dominios de broadcast se debe mencionar que actualmente existen dos dominios que están en la obra, por las dos subredes que se describen anteriormente. También es importante mencionar que no existen un plan IP o una segmentación de VLAN's o ruteadores que segmente la mencionada red.

La red LAN de la obra San Rafael de la Casa Inspectorial Salesiana brinda servicio a aproximadamente 220 estaciones de trabajo de las cuales 60 son utilizadas por personal de la obra y las restantes 160 son equipos de computación ubicados en laboratorios. En la siguiente tabla se muestra la distribución de Switches y salidas de datos por cada uno de los SDF existente en la obra salesiana.

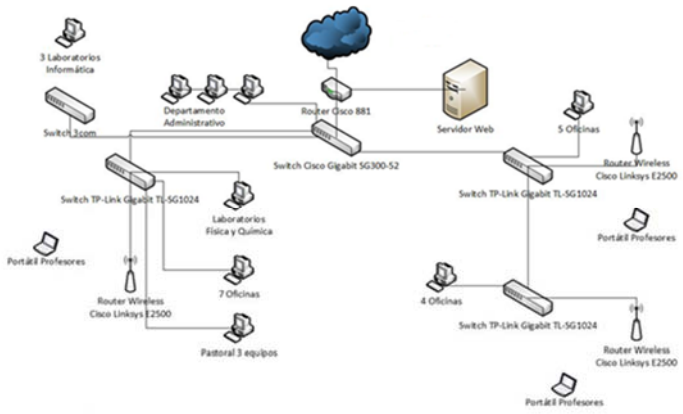
#### 3.1.4.6. Proveedores de servicios externos (Servicio de Internet)

En la infraestructura establecida de Networking de la obra Salesiana, se dispone de un enlace para el acceso a Internet contratado con la empresa CNT, La velocidad del enlace de acceso a Internet es de 15 Mbps y cumple con las siguientes funciones:
Brinda acceso a los servicios de navegación y acceso al correo electrónico.

En lo relacionado a la infraestructura de comunicaciones utilizada para brindar este servicio se debe señalar que se lo realiza mediante la utilización de 1 línea dedicada que se interconecta directamente con los equipos del proveedor a través Router Cisco 881 que al mismo tiempo cumple con las funciones de ruteador.

En las siguientes tablas se detallan el tipo de líneas utilizadas para realizar las conexiones hacia el proveedor de Internet y el equipamiento utilizado.

Figura 30. Diagrama de acceso a Internet a la obra Salesiana




Elaborado por Leonardo Suárez.

Tabla 20. Equipos usados para conexión a Internet.

| **Cantidad** | **Dispositivo** | **Función/Servicio** |
|---|---|---|
| 1 | CISCO 881 | Bridge/Switch Cisco Internet 15 Mbps |

Elaborado por Leonardo Suárez.

Para el acceso a Internet el proveedor del servicio ha asignado una subred con 8 direcciones IP públicas (Direcciones IP's simuladas). Lo relacionado al direccionamiento IP que se utiliza en las subredes se resume a continuación:

Direccionamiento IP:

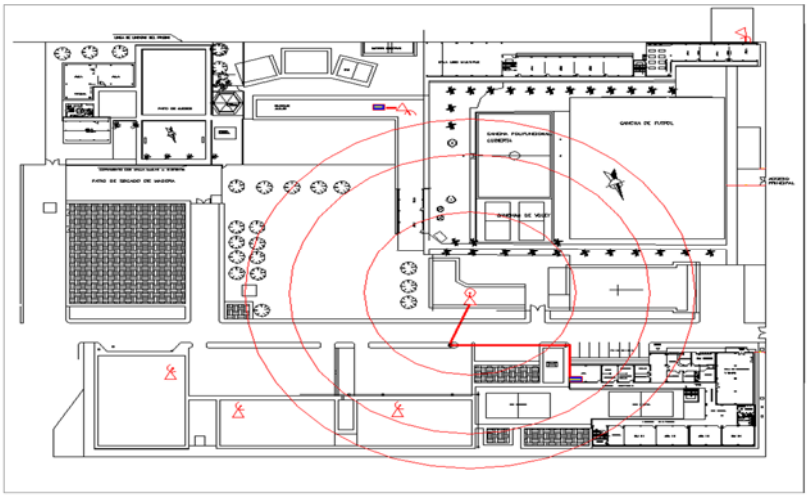
| | |
|---|---|
| Nombre: | Subred Internet |
| Descripción: | Acceso a Internet 15 Mbps |
| Network: | 64.46.84.192 |
| Mascara: | 255.255.255.248 |
| Rango IP: | 64.46.84.192 - 64.46.84.199 |
| Núm. Hosts: | 6 válidos (1 Subred y 1 Broadcast) |

Se debe mencionar que la implementación subredes administrativas y de laboratorio se conectan a través de un servidor Linux que cumple con la funcionalidad de Proxy Firewall.

En la actualidad se lleva a cabo la realización de la implementación de AP's (conexión inalámbrica) para brindar acceso Wireless en la obra.

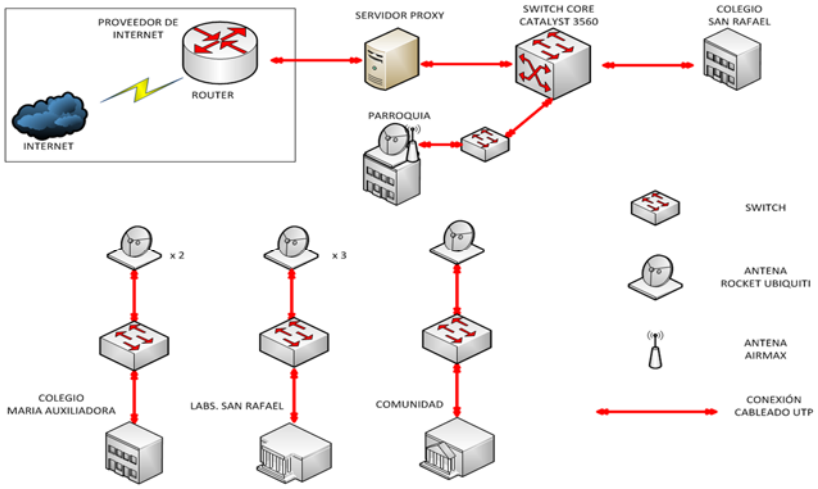
En el siguiente diagrama se muestra los componentes utilizados y las interconexiones existentes que son utilizadas para brindar el servicio inalámbrico.

Figura 31. Diagrama de survey en la obra salesiana



Elaborado por Leonardo Suárez.

Figura 32. Diagrama de implementación de cobertura inalámbrica




Elaborado por Leonardo Suárez.

La propuesta se basará en algunos diseños de red establecidos basados en Cisco (CEAM) para aplicaciones y servicios estandarizados en toda la Casa Inspectorial Salesiana. Además se va a empezar un proceso de planificación y de ajustes en toda la infraestructura física y de direccionamiento lógico de la red como una medida

necesaria para iniciar el proyecto de diseño con las obras a nivel nacional, como son Riobamba, Ibarra y Esmeraldas.

En la Casa Inspectorial sede Quito con sus obras alrededor se debe cambiar el direccionamiento para que se restablezca la comunicación entre la matriz y sus obras para poder adaptarse con la infraestructura actual y preparar a la Casa Inspectorial sede Quito para el proyecto nacional de interconexión.

En la Casa Inspectorial Salesiana se va a diseñar el direccionamiento lógico para poder acoplarse con algunas de las obras a nivel nacional.

La infraestructura D-Link, Cisco (equipos de la UPS), es la red actual de la Casa Inspectorial Salesiana que no brinda aún el soporte necesario para la creación de VLAN's, por lo que solo existe una subred y es brindada por los ISP.

La necesidad de implementar una nueva infraestructura tecnológica para cubrir las necesidades de las obras como es la implementación de cobertura inalámbrica que prepare lo necesario para la implementación de aplicaciones y servicios estandarizados en toda la Casa Inspectorial Salesiana, inició un proceso de planificación y de ajuste en toda la infraestructura física y de direccionamiento lógico de la red como una medida necesaria para iniciar el proyecto a nivel nacional en las diferentes obras.

Se hizo un breve recuento sobre la información de infraestructura de red de las obras antes mencionadas, en lo cual se puede constatar el diseño de red real que tienen las diferentes obras, se debe tomar en cuenta que son similares topologías y direccionamiento cubiertos por el proveedor y sus equipos físicos.

A continuación se presenta algunos de los protocolos utilizados en una obra la cual es Don Bosco La Kennedy, lo que permitirá verificar cuales son las aplicaciones más utilizadas en esta obra.

Para la realización de captación de protocolos utilizados en esta obra, se utilizará un software libre el cual es WIRESHARK.
Un resumen de los diferentes protocolos utilizados en el modelo OSI.

- Capa 1: Nivel físico

  Cable coaxial o UTP categoría 5, categoría 5e, categoría 6, categoría 6a Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232.
- Capa 2: Nivel de enlace de datos

  ARP, RARP, Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC., CDP
- Capa 3: Nivel de red

  IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX, AppleTalk.
- Capa 4: Nivel de transporte

  TCP, UDP, SPX.
- Capa 5: Nivel de sesión

  NetBIOS, RPC, SSL.
- Capa 6: Nivel de presentación.

  ASN. 1.
- Capa 7: Nivel de aplicación

  SNMP, SMTP, NNTP, FTP, SSH, HTTP, CIFS (también llamado SMB), NFS, Telnet, IRC, POP3, IMAP, LDAP, Internet Mail 2000, y en cierto sentido, WAIS y el desaparecido GOPHER.

A continuación el número de puerto con los protocolos más utilizados.

Tabla 21. Puertos con los protocolos más utilizados.

| Puerto | Servicio |
|---|---|
| 21 | FTP |
| 22 | ssh |
| 25 | SMTP |
| 53 | DNS |
| 80 | http |
| 110 | POP3 |
| 143 | IMAP |
| 443 | https |
| 993 | IMAP ssl |
| 995 | POP ssl |

Fuente: (Debish, 2012, pág. 1)

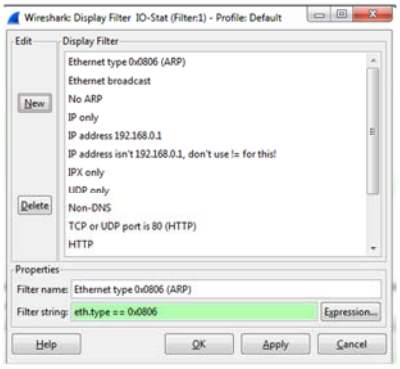
Se hará una breve descripción de algunos de los protocolos menos significativos como son:

- CDP: (Protocolo de descubrimiento de Cisco), es un protocolo de red este protocolo es de propiedad de la capa de enlace de datos, este protocolo es desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Este protocolo es usado para compartir información con otros equipos Cisco conectados directamente, en la cual conste la misma versión y estar en el mismo segmento de red. (Ariganello, 2006, pág. 1)

- IGMP: (Internet Group Management Protocol) El protocolo de red IGMP se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia. (Aboutabi, 2003, págs. 3 - 7)

- SPX: es un protocolo de Intercambio de Paquetes en Secuencia (SPX) es la implementación del protocolo SPP (Sequenced Packet Protocol) de Xerox. Es un protocolo fiable basado en comunicaciones con conexión y se encarga de controlar la integridad de los paquetes y confirmar los paquetes recibidos a través de una red. Pertenece a la capa de transporte (nivel 4 del modelo OSI) y actúa sobre IPX para asegurar la entrega de los paquetes (datos), ya que IPX por sí solo no es capaz. Es similar a TCP ya que realiza las mismas funciones. Se utiliza principalmente para aplicaciones cliente/servidor. (Atelin & Dordoigne, 2007, págs. 8 - 9)

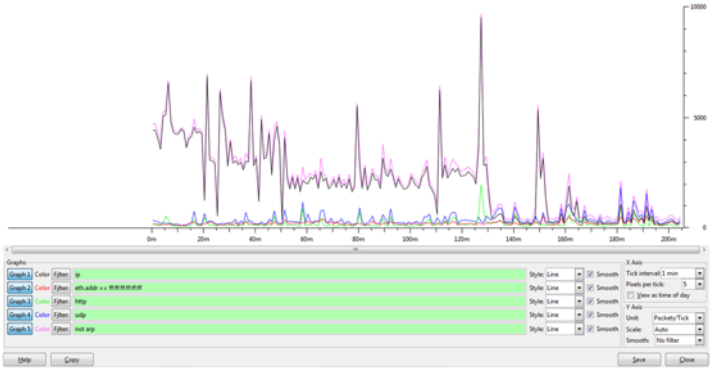
Figura 33. Tabla de protocolos




Elaborado por Leonardo Suárez.

En la figura 33 se presenta, los protocolos más relevantes utilizados en esta obra.

Figura 34. Protocolos utilizados



Elaborado por Leonardo Suárez

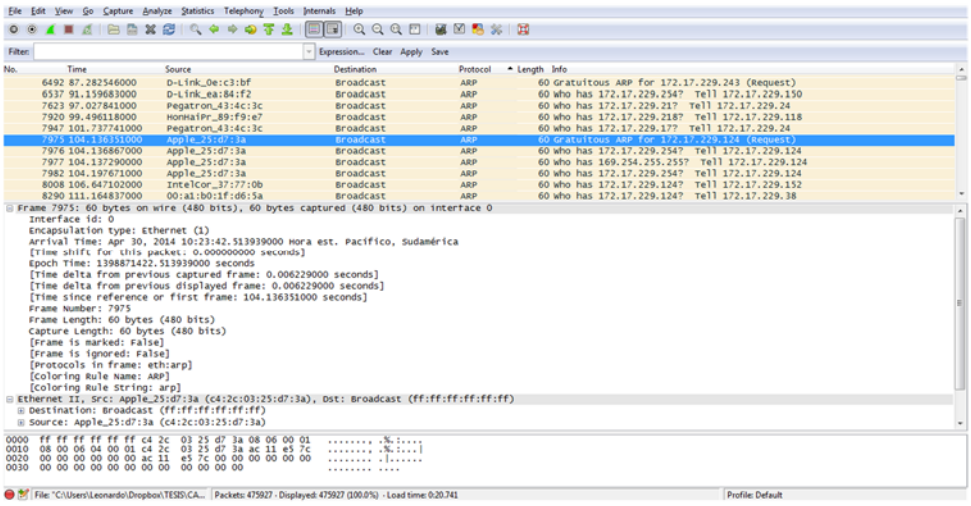
En la figura 34 se presenta algunos de los protocolos utilizados los cuales son: IP, Ethernet, HTTP y UDP.

Figura 35. Protocolos utilizados 2

Elaborado por Leonardo Suárez

En la figura 35 se presenta los protocolos utilizados los cuales son: Ethernet, Tcp port 80, Tcp port 25, Udp port 53 e IPX.

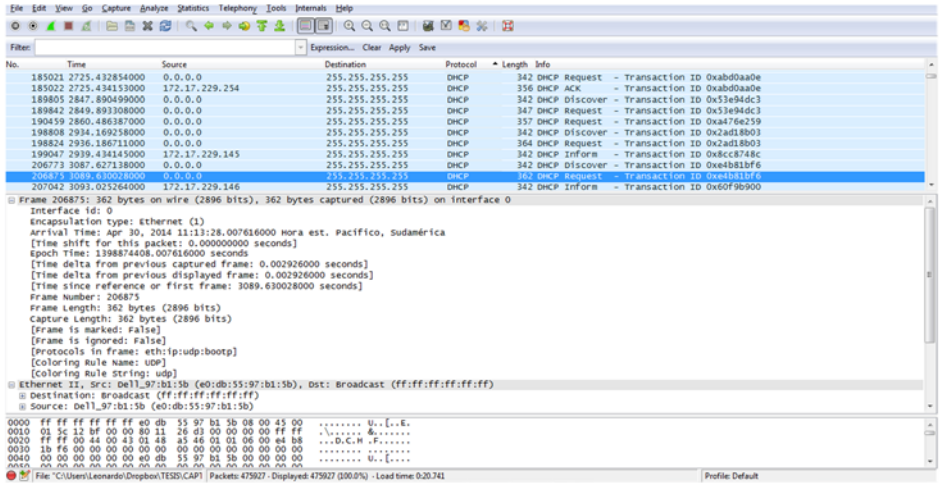
Figura 36. Protocolos utilizados ARP



Elaborado por Leonardo Suárez

En la figura 36 se hace una recopilación del protocolo ARP el cual se ha hecho una captura de paquetes para diagnosticar el tráfico en la obra.

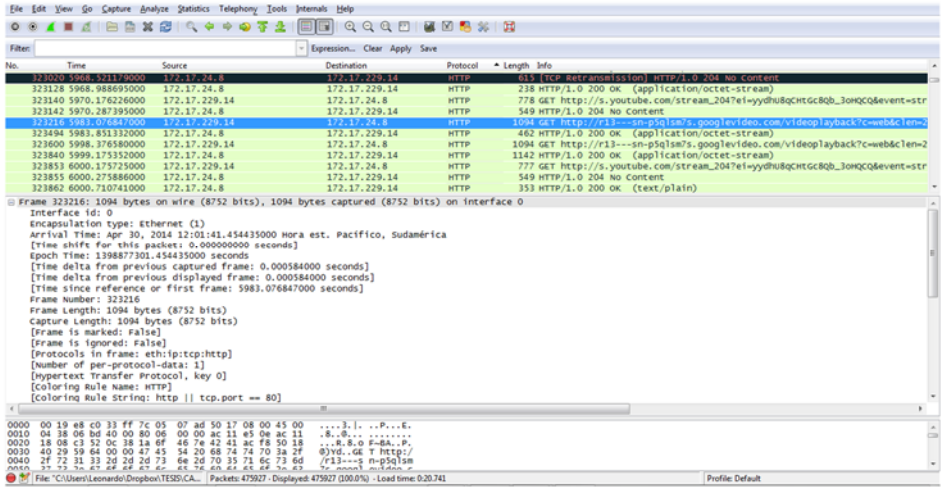
Figura 37. Protocolos utilizados DHCP



Elaborado por Leonardo Suárez

En la figura 37 se hace una recopilación del protocolo DHCP el cual se ha hecho una captura de paquetes para diagnosticar el tráfico en la obra.

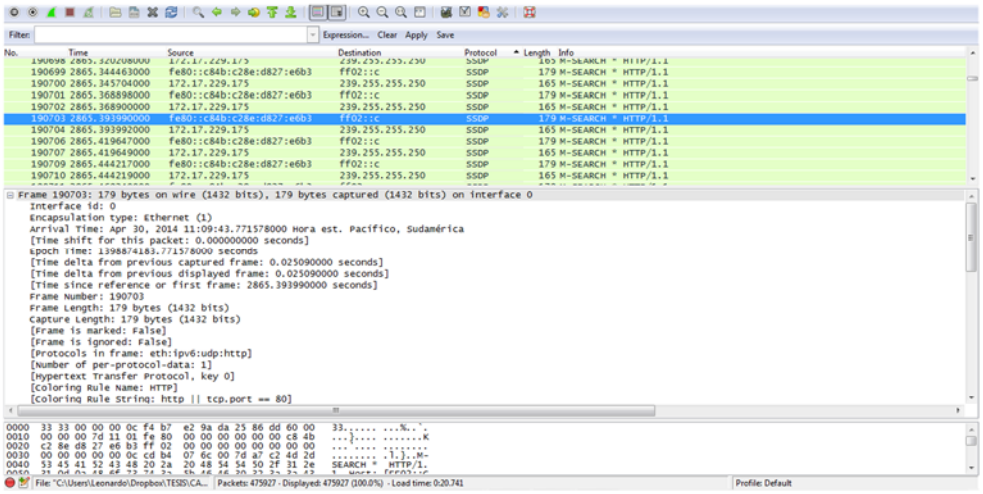
Figura 38. Protocolos utilizados DHCP



Elaborado por Leonardo Suárez

En la figura 38 se hace una recopilación del protocolo HTTP el cual se ha hecho una captura de paquetes para diagnosticar el tráfico de navegación en la obra.

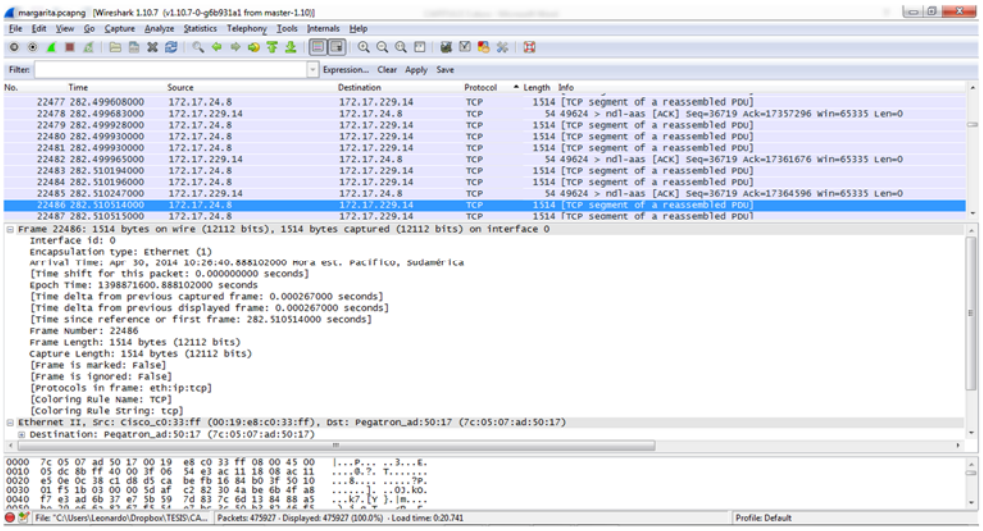
Figura 39. Protocolos utilizados SSDP




Elaborado por Leonardo Suárez

En la figura 39 se hace una recopilación del protocolo SSDP el cual se ha hecho una captura de paquetes para diagnosticar el tráfico en la obra.

Figura 40. Protocolos utilizados TCP




Elaborado por Leonardo Suárez

En la figura 40 se hace una recopilación del protocolo TCP el cual se ha hecho una captura de paquetes para diagnosticar el tráfico en la obra.

A continuación se hace un breve resumen sobre el control de ancho de banda, en la cual se hace este control sobre un servidor proxy (htb-gen-rates), este servicio es proporcionado por la UPS, se hace una referencia:

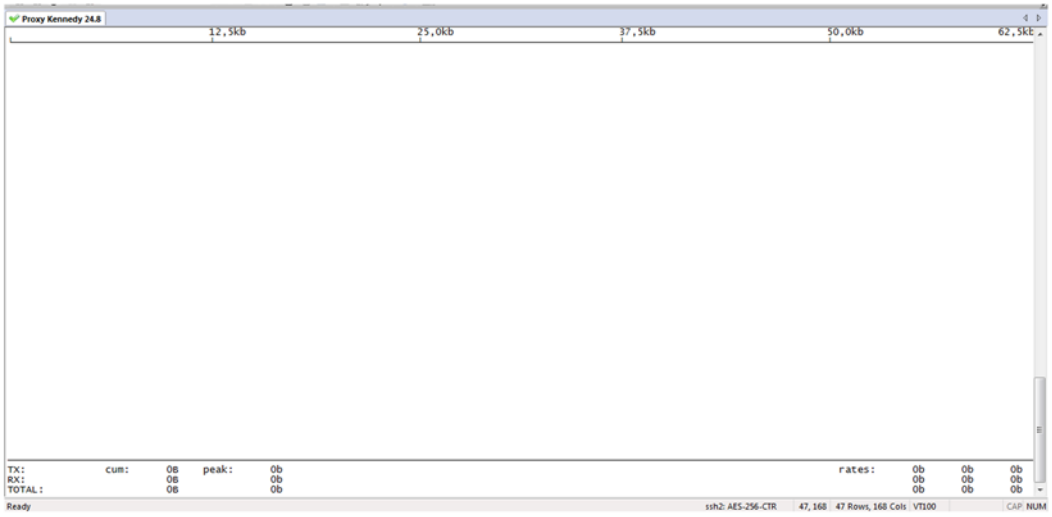
Tabla 22. Control de ancho de banda del servidor proxy.

| CONTROL DE ANCHO DE BANDA SERVIDOR PROXY | | | | | |
|---|---|---|---|---|---|
| **VLAN** | **RED** | **DOWN** | **UP** | **DOWN** | **UP** |
| 21 | COLEGIO | 3072Kbps | 5120Kbps | 3072Kbps | 5120Kbps |
| 224 | CES DOCENTES | 3072Kbps | 5120Kbps | 3072Kbps | 5120Kbps |
| 228 | CES COLEGIO | 2048Kbps | 6096Kbps | 2048Kbps | 6096Kbps |
| 229 | CES ESCUELA | 4072Kbps | 6120Kbps | 4072Kbps | 6120Kbps |
| 231 | CES ADM | 512Kbps | 1024Kbps | 512Kbps | 1024Kbps |
| 234 | CES ESEMTIA DOC | 3072Kbps | 6120Kbps | 3072Kbps | 6120Kbps |

Elaborado por Leonardo Suárez.

Figura 41. Ancho de banda utilizado en la red ces docentes.

Utilizando comandos iftop –f 172.17.226.0/23

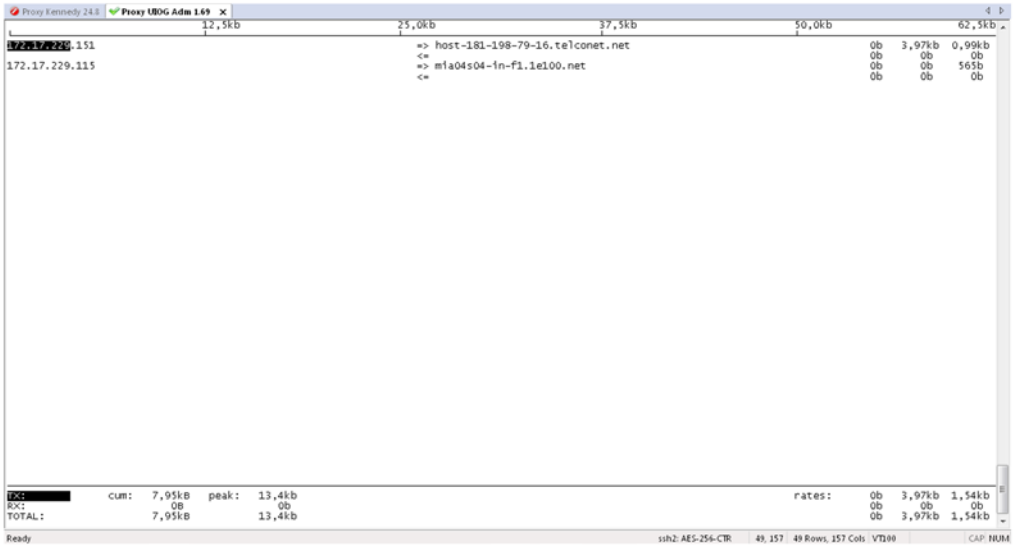



Elaborado por Leonardo Suárez

.

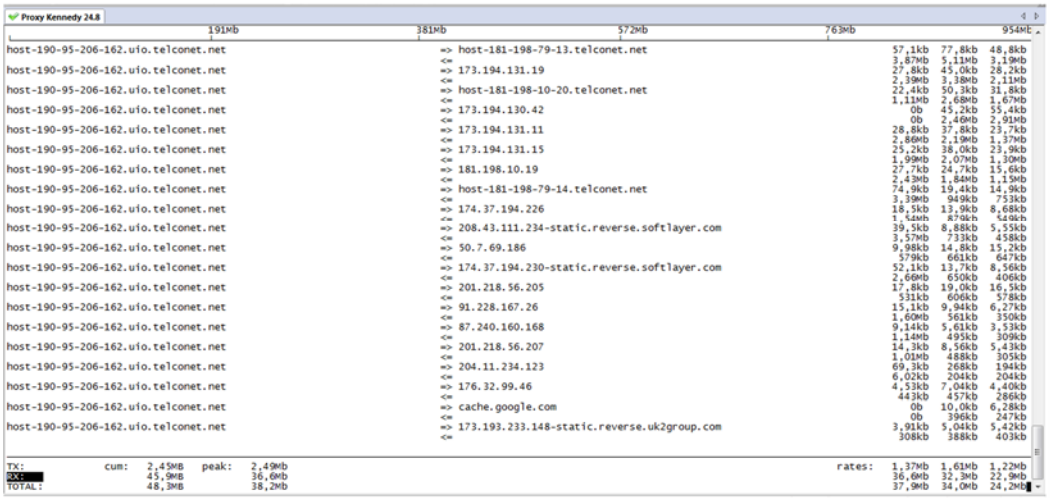
Figura 42. Ancho de banda utilizado en la red ces escuela.

Utilizando comandos iftop –f 172.17.229.0/23




Elaborado por Leonardo Suárez

Figura 43. Resumen del consumo de ancho de banda controlado por htb-gen-rates este servicio proporciona el server del proxy




Elaborado por Leonardo Suárez

De acuerdo a las figuras 41, 42 y 43 se realizó un monitoreo de las diferentes redes expuestas, para saber el consumo del ancho de banda en la obra. En la que se puede constatar que el ancho de banda que le brinda la UPS no es suficiente, lo cual se debe hacer un incremento para solventar la demanda de los usuarios.

A partir de este levantamiento de información se partirá con el diseño, para optar por los equipos físicos de red más relevantes e importantes, que cumplan con las funciones requeridas por el diseño establecido.

Para lo cual se tomó como base para realizar el diseño de Cisco, se basa en la guía de los diferentes diseños generados por la UPS y los estudiantes como contraparte para algunos diseños elaborados y establecidos. Por lo que se abordará de forma muy concisa el tema del modelo de Cisco Enterprise Architecture Model (CEAM) que será la base para el diseño de interconexión de las redes LAN de la Casa Inspectorial Salesiana.

# CAPÍTULO 4

## 4.1. Diseño para el área de frontera (borde) de la empresa.

El diseño que se va a realizar a continuación, está basado en la metodología y arquitectura de Cisco. En la que se puede obtener escalabilidad, disponibilidad, seguridad y facilidad de gestión entre la matriz y las sucursales.

### 4.1.1. Cisco Enterprise Architecture Model (CEAM).

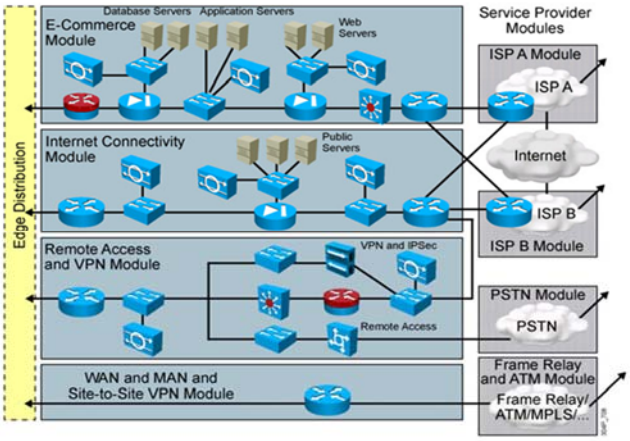
El diseño que se va a establecer a continuación se lo tomará en cuenta para una futura implementación, por su modularidad y flexibilidad con la que este modelo forma el diseño de red, por lo cual facilita la implementación y solución a los problemas existentes.

Para obtener un balance en el modelo jerárquico de redes (core, acceso y distribución), Cisco desarrolló un modelo el Cisco Enterprise Architecture Model (CEAM), este diseño tiene muchas ventajas tanto en lo físico como en lo lógico.

Los objetivos principales del CEAM son:

Una red mucho más determinística con claras funciones y bondades entre módulos.
El modelo tiene una clara demarcación entre módulos que facilita al diseñador de la red saber y tener un panorama mucho más claro de que tráfico es permitido dentro y fuera de cada punto de demarcación.
Facilidad de diseño, incremento de escalabilidad y conseguir resolver problemas más fácilmente por el método de divide y conquista.
Simplifica la escalabilidad de las redes. Añadir un edificio nuevo en el campus, una oficina remota en la WAN, o servidores en la granja de servidores será una tarea más fácil.

Figura 44. Diagrama de red de frontera




Fuente: www.cisco.com

## 4.2. Metodología PPDIOO

La metodología consiste en la siguiente sección que se enfoca sobre la metodología de diseño de las tres primeras fases las cuales serán aplicadas para este diseño, son:

1: Identificar los requerimientos de red
2: Caracterizar la red existente
3: Diseño de la topología de red y solución.

Este diseño utiliza la metodología llamada top-down la cual inicia desde la capa Aplicación del modelo OSI y continua con las demás capas en forma descendente validando los requerimientos de la Casa Inspectorial Salesiana.

Este modelo de red, es de gran ayuda para que los analizadores de red, puedan realizar un análisis total de todos los requerimientos iníciales y los objetivos que se desea alcanzar, al utilizar Cisco Systems se recomienda un modelo jerárquico de tres capas (core, distribución y acceso), al tomar esto en cuenta se incluyen criterios de SONA Framework (Service Oriented Network Architecture - Arquitectura de redes orientadas a servicios), AON (Aplication Oriented Networking – Redes Orientadas a Aplicaciones) IIN (Intelligent Informations Netwok – Red inteligente de información) y para los componentes de la red utilizan los modelos sugeridos de Cisco para que estos se adapten al alcance de la red y al área funcional que se desee diseñar, para el

caso de la Casa Inspectorial Salesiana Sede Quito se utilizará el modelo CEAM (Cisco Enterprise Architecture Model).

Este modelo de diseño de red provee integridad, la integridad le permite al diseñador evaluar cualquier solución de red (por ejemplo, VoIP, como también almacenamiento de información en la red backups) y algunos servicios inteligentes de red como: seguridad, calidad de servicio (QoS), y sobre todo tener administración sobre la infraestructura de la red con respecto a cada módulo.

Este modelo de diseño de red de Cisco permitirá realizar la interconexión de la matriz además que permitirá integrar los conceptos de SONA para lograr migrar a una infraestructura IIN con respecto a la globalidad de la red de la matriz.
SONA (Service-Oriented Network Architecture – Arquitectura de Red orientada a servicios)

EL Concepto de SONA Framework es un marco arquitectónico que guiará a la red de la empresa a una red inteligente de información que soporte nuevas estrategias de IT.

Con SONA se logrará la administración centralizada de una plataforma común y unificada sobre un sistema integrado de aplicaciones y servicios a grandes velocidades con calidad de servicio. SONA está compuesto por tres capas de diseño:
Capa infraestructura de red: Contiene la arquitectura empresarial de Cisco (Campus, LAN, WAN) (Dominguez Ayala & Chicaiza Iza, 2008, págs. 93 - 94)

## 4.3. Primera fase.

### 4.3.1. Fase de preparación

En esta fase de preparación se establece la organización y los requerimientos de la Casa Inspectorial Salesiana, se desarrolla una estrategia de red, y se propone una arquitectura conceptual de alto nivel para apoyar la estrategia. Establecer técnicas es una justificación económica para una estrategia de red.

Un breve análisis a los diferentes costos de los posibles equipos a utilizar en el modelo planteado.

## CISCO

Tabla 23. Cotización de equipos Cisco

| ***NOMBRE DEL EQUIPO*** | ***VALOR UNITARIO*** | ***CANTIDAD*** | ***TOTAL*** |
|---|---|---|---|
| NGFW ASA 5545-Xw/ SW 8GE Data 1GE Mgmt AC 3DES/AES 2SSD120 | $ 9754,76 | 1 | $ 9754,76 |
| WSA WEB SECURITY APPLIANCE WITH SOFTWARE | $ 5818,81 | 1 | $ 5818,81 |
| SMARNET 8X5XNBD WSA S380 WEB SECURITY 1YEAR | $ 760,03 | 1 | $ 760,03 |
| BLUE COAT PACKETSHAPER 12000, 1000BASE-T, UP TO 200MBPS OF SHAPING, 2048/5000 CLASSES | $ 65899,69 | 1 | $ 65899,69 |
| BLUE TOUCH PARTNER SUPPORT, 24X7 L3 SOFTWARE ONLY, PS12000-L200M, 1 YEAR | $ 8609,48 | 1 | $ 8609,48 |
| SAME DAY SHIPMENT HARDWARE SUPPORT, PS12000-L200M, 1 YEAR | $ 2152,37 | 1 | $ 2152,37 |
| **TOTAL** | $ 92,995,14 | | $ 92,995,14 |

Elaborado por Leonardo Suárez.

## HP

Tabla 24. Cotización de equipos HP

| ***NOMBRE DEL EQUIPO*** | ***VALOR UNITARIO*** | ***CANTIDAD*** | ***TOTAL*** |
|---|---|---|---|
| TIPPINGPOINT NEXT-GENERATION INTRUSION PREVENTION SYSTEM (IPS) | $ 10.200,00 | 1 | $ 10.200,00 |
| TIPPINGPOINT NEXT-GENERATION FIREWALL (NGFW) | $ 9.000,00 | 1 | $ 9.000,00 |
| Cortafuegos HP F5000-S y HP F5000C: Son cortafuegos VPN | $ 10.424,03 | 1 | $ 10.424,03 |
| **TOTAL** | $ 29.624,03 | | $ 29.624,03 |

Elaborado por Leonardo Suárez.

## HUAWEI

Tabla 25. Cotización de equipos HUAWEI

| ***NOMBRE DEL EQUIPO*** | ***VALOR UNITARIO*** | ***CANTIDAD*** | ***TOTAL*** |
|---|---|---|---|
| High-end Firewall Tbit Firewall Eudemon8000E-X Series | $ 12.000,00 | 1 | $ 12.000,00 |
| Mid-end/Low-end Firewall USG5100 Unified Security Gateway | $ 9.000,00 | 1 | $ 9.000,00 |
| Mid-end/Low-end Firewall USG5500 Unified Security Gateway | $ 8.000,00 | 1 | $ 8.000,00 |
| NIP2000-5000 Intrusion Prevention System Series product | $ 10.424,03 | 1 | $ 10.424,03 |
| USG6600 Next Generation Firewall | $ 15.000,00 | 1 | $ 15.000,00 |
| AntiDDoS8000 Series DDoS Defend System | $ 7.500,00 | 1 | $ 7.500,00 |
| **TOTAL** | $ 27.424,03 | | $ 27.424,03 |

Elaborado por Leonardo Suárez.

En esta fase se realizará una justificación financiera para el diseño de red que unifique a todas las obras Salesianas.

En base a los presupuestos y características de los diferentes equipos adquiridos, se parte desde una línea base tomando en cuenta las diferentes características de la marca de los equipos antes mencionados:

Los protocolos que soportan cada marca son:

Tabla 26. CISCO ASA 5545-X WSA WEB SECURITY APPLIANCE

Figura 45. CISCO ASA 5545-X

Figura 46. WSA WEB SECURITY APPLIANCE

| **CARACTERISTICAS** | ***WSA Web Security Appliance S380*** | **CARACTERISTICAS** | ***ASA 5545-X*** |
|---|---|---|---|
| **Tipo de dispositivo** | Aparato de seguridad | **Marca** | Cisco |
| **Altura (unidades de bastidor)** | 2U | **Series** | ASA 5545-X |
| **Procesadores instalados** | 1 x Intel Xeon E5-2600 series 2 GHz | **Peso del producto** | 8 Kg |
| **Memoria RAM** | 16 GB DDR3 SDRAM | **Dimensiones del producto** | 48,4 x 42,9 x 4,2 cm |
| **Disco duro** | HDD intercambio en caliente - 600 GB x 4 - SATA 3Gb/s - 2.5" SFF | **Número de modelo del producto** | ASA5545-2SSD120-K9 |
| **Nivel RAID** | RAID 10 | **Factor de forma** | 1U |
| **Protocolo de interconexión de datos** | Ethernet, Fast Ethernet, Gigabit Ethernet | **Capacidad de la memoria RAM** | 12288 MB |
| **Protocolo de gestión remota** | Telnet, HTTP, HTTPS, SSH, CLI | **Capacidad del disco duro** | 240 GB |
| **Capacidad** | Conexión / cantidad de usuarios : 1500 - 6000 | **Descripción del disco duro** | SSD |
| **Características** | Negociación automática, soporte LDAP, análisis de antivirus, protección anti-spam, Prevención de pérdida de datos (DLP) | **Número de puertos USB 2.0** | 2 |
| **Compartimentos de expansión** | 22 (total) / 18 (libre) x intercambio en caliente - 2.5" | **Potencia** | 86 vatios |
| **Interfaces** | 4 x 1000Base-T - RJ-45 ¦ 1 x management - RJ-45 ¦ 2 x USB 2.0 - Type A ¦ 1 x 1000Base-T (administración) - RJ-45 | | |
| **Redundancia de alimentación** | Sí | | |
| **Potencia suministrada** | 650 vatios | | |
| **Software incluido** | Controladores y utilidades | | |
| **Costo aproximado 2014 + 1 año de licenciamiento** | ~$5.900+760 | | |

Elaborado por: Leonardo Suárez.

Tabla 27. Cisco bluecoat 12000


Figura 47. Cisco bluecoat 12000

| | |
|---|---|
| **SERIE DE PACKETSHAPER** | 12000 \| 12000 ISP**** |
| **Flujos de IP (TCP)*** | 450 000 \| 900 000 |
| **Flujos de IP (UDP)*** | 225 000 \| 400 000 |
| **Clases** | 2 048 \| 5 000 / 10 000 |
| **Particiones dinámicas** | 20 000 \| 20 000 |
| **Particiones estáticas** | 2 048 \| 5 000 / 7 500 |
| **Políticas de gestión** | 2 048 \| 5 000 |
| **Cantidad máxima de reglas de coincidencia** | 12 288 \| 20 000 / 25 000 |
| **Hosts IP*** | 300 000 \| 540 000 |
| **Túneles activos** | 1 000 \| N/D |
| **Velocidades de vínculos con opciones de gestión** | 500 Mbps/1 Gbps/Sin límite |
| **Compresión***** | 155 Mbps \| N/D |
| **Puertos integrados (pares)** | Cobre: 1x10/100/1 000 Mbps |
| **Módulos de expansión de LAN** | Cobre, dos puertos (1): 10/100/1000 BASE-T |
| | o 10 GBASE-CX4 |
| | Cobre, cuatro puertos (1): |
| | 10/100/1000 BASE-T |
| | Fibra, dos puertos (1): 1000 BASE-SX, |
| | 1000 BASE-LX, 10 GBASE-SR, 10 GBASE-LR |
| | Fibra, cuatro puertos (1): 1000 BASE-SX o |
| | 1000 BASE-LX |
| **Uso compartido de carga doble redundante** | Sí; intercambiable en caliente |

Elaborado por: Leonardo Suárez.

## HEWLETT PACKARD (HP)

Tabla 28: IPS S110.

Figura 48. IPS S110

| Características | IPS S110 | IPS (NIP5500) |
|---|---|---|
| Rendimiento de red | 100Mbps | 10 Gigabit |
| Contextos de seguridad | 250000 | |
| Puertos | 8 RJ-45 puertos 10/100/1000 de detección automática (IEEE 802.3 tipo 10Base-T, IEEE 802.3u Tipo 100BASE-TX, IEEE 802.3ab Tipo 1000BASE-T) | BYPASS: 4 × GE (RJ45) 2Line (LC / UPC) Interfaz: 8 × GE (RJ45) 8 × GE (SFP) |

| | | |
|---|---|---|
| | Duplex: 10BASE-T / 100BASE-TX: la mitad o completa; 1000BASE-T: sólo completo | 2 × 10GE 2 × 10 GE + 8GE |
| DDoS | Sí | Sí |
| P2P | Sí | Sí |

Elaborado por: Leonardo Suárez.

## HP TippingPoint Next-Generation Firewall (NGFW)

Figura 48. HP TippingPoint Next-Generation Firewall (NGFW)

| **Características** | **HP TippingPoint Next-Generation Firewall (NGFW)** | **HP Firewall Cortafuegos VPN** | **USG6600 NEXT GENERATION FIREWALL** |
|---|---|---|---|
| Enlaces | OSPF, RIP, BGP | RIP, BGP-4, OSPF | RIP, OSPF, BGO-4, |
| Soporta VLAN | Sí | Sí | Sí |
| Soporta NAT | | Sí | |
| Soporta SNMP | | Sí | |
| IPSec | Sitio a sitio | Sí | Sí |
| VPN | Cliente a sitio | Sí | Sí |
| Política Integrada | Active Directory, LDAP o servicios de autenticación RADIUS. | | |
| Control de acceso | Basado en roles RBAC | Basado en zona | |

Elaborado por: Leonardo Suárez.

**HUAWEI**

Tabla 29. USG5100 Unified Security Gateway

Figura 49. USG5100 Unified Security Gateway

| Modelo | USG5120 | USG5150 |
|---|---|---|
| Rendimiento | | |
| Firewall | 2.5 Gbit / s | 4 Gbit / s |
| VPN | 1 Gbit / s | 2 Gbit / s |
| Número recomendado de usuarios | 800-1000 | 1000-1200 |
| Expansión y E / S | | |
| Puerto fijo | 2 x GE 2 x GE (combo) | 4 x GE (combo) |
| Ranura de expansión | 4 x MIC 2 x 2 x FIC DFIC | 4 x MIC 2 x 4 x FIC DFIC |
| Características de enrutamiento | | |
| IPv4 | 802.1Q, enrutamiento estático, WCMP, enrutamiento basado en políticas, RIP, OSFPv1/v2, BGP4, IS-IS, DHCP y agregación de enlaces | |
| IPv6 | El enrutamiento estático, enrutamiento basado en políticas, RIPng, OSPFv3, BGP4 +, e IS-ISv6 | |
| Multicast | IGMP v1/2/3, PIM-DM, PIM-SM, y MSDP | |
| Funciones de seguridad | | |
| Tipos de VPN | IPSec VPN, SSL VPN, MPLS VPN, VPN L2TP, GRE y VPN | |
| La autenticación de usuarios | Web Local, LDAP, AD, y RADIUS | |
| Defensa de seguridad básico | Control de acceso de aplicación / basado en el usuario-, NAT, control de ancho de banda application / basado en el usuario-, anti-DDoS, cortafuegos / VPN de alta disponibilidad y balanceo de carga | |
| UTM | IPS basado en firmas, AV, AS, filtrado de URL, control de aplicaciones, palabras clave / filtrado de motor de búsqueda, la firma definida por el usuario, manual de / / de actualización automática de la firma local de | |
| Potencia | 210 W | 300 W |

Elaborado por: Leonardo Suárez.

En las tablas anteriores se hace una comparación entre diferentes equipos propuestos, en la que se compara eficiencia, y escalabilidad, para obtener resultados en cuanto a voz y video. En la que se partió desde una línea base, los equipos que cumplen con los requerimientos fueron Cisco. Los dispositivos que se han escogido soportan los diferentes protocolos analizados y monitoreados.

### 4.3.2. Fase de planeación

En esta fase de planeación se identifica los requerimientos de la red basados en necesidades de las instalaciones y en las necesidades del usuario. Esta fase se caracteriza por evaluar los sitios de la infraestructura de red, realiza un análisis de brechas contra arquitecturas de mejores prácticas, y se ve en el entorno operativo. Un plan de proyecto se desarrolla para gestionar las tareas, los responsables, y los recursos para hacer el diseño y la implementación. El plan del proyecto se alinea con los parámetros de alcance, costo y recursos establecidos con los requisitos de negocio

originales. Este plan de proyecto es seguido (y actualizado) durante todas las fases del ciclo.

A continuación se establece una recopilación de información en la que constan datos de algunas obras establecidas con los requerimientos necesarios para la interconexión de la matriz con las obras.

#### 4.3.2.1. Obra Colegio Técnico Don Bosco La Kennedy

Las falencias de esta obra se encuentra en el capítulo 3 en las figuras 17, 18 y tabla 2 en esos recuadros se constata la topología de red implementada en la obra, que no es la adecuada para la interconexión con la matriz, porque en esta obra se tiene que considerar que se acopló a la UPS por ende se unió al diseño de red de la UPS, en este diseño se segmento la red y el plan IP por lo que se tiene constancia para un futuro diseño, por lo que se constató que tienen algunos dominios de broadcast. En la obra Don Bosco de la Kennedy.

Los requerimientos de la obra es que no tienen segmentación de red, un plan IP establecido y un control de ancho de banda para la red, por lo que estos servicios se están brindando por parte de la UPS en lo que sería necesario tener sus propios servicios, una segmentación de red y un buen ancho de banda dependiendo de los usuarios de la obra.

#### 4.3.2.2. Obra Unidad Educativa Salesiana Fisco misional "Don Bosco" La Tola

Las falencias de esta obra se encuentra en el capítulo 3 en las figuras 21, 22, y tabla 7, 9 en esos recuadros se constata la topología de red implementada en la obra, que no es la adecuada para la interconexión con la matriz, se debe tener en cuenta que existe en la actualidad una implementación de un servidor proxy para que interactúe como firewall y protección tanto el correo como para la página web, además se constató que no existe una segmentación de red o algún dominio de broadcast, aparte que el que les provee (ISP). En la obra Don Bosco La Tola.

Las falencias de la obra es que no tienen segmentación de red, un plan IP establecido y un control de ancho de banda para la red, lo que sería adecuado es hacer una segmentación de red y tener un control de ancho de banda dependiendo de los usuarios de la obra.

#### 4.3.2.3. Obra Sánchez Cifuentes Ibarra

La falencia de esta obra se encuentra en el capítulo 3 en las figuras 25, 26 y tabla 13 en esos recuadros se constata la topología de red implementada en la obra, que no es la adecuada para la interconexión con la matriz, en la actualidad se lleva un proyecto de Wireless, en esta obra se debe tomar en cuenta que en las demás obras contienen el mismo dominio y el mismo direccionamiento. En la obra Sanchez Cifuentes de Ibarra. Las falencias de la obra es que no tienen segmentación de red, un plan IP establecido, control de ancho de banda para la red y solventar la red inalámbrica, lo que sería adecuado es hacer una segmentación de red, tener control de ancho de banda dependiendo de los usuarios de la obra y Wireless.

#### 4.3.2.4. Obra Colegio Fisco misional Salesiano de bachillerato San Rafael

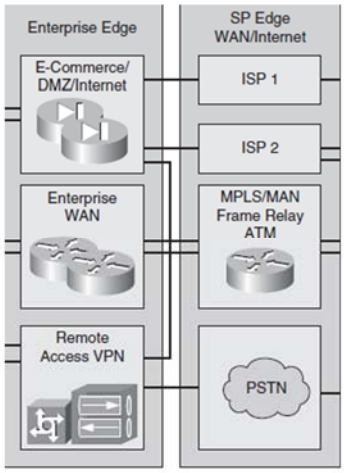
La falencia de esta obra se encuentra en el capítulo 3 en las figuras 29, 30, y tablas 17, 18, 19 en esos recuadros se constata la topología de red implementada en la obra, que no es la adecuada para la interconexión con la matriz, se debe tomar en cuenta que en esta obra se realiza un proyecto de Wireless para brindar conexión inalámbrica a todo el personal de la obra, además se debe considerar el mismo direccionamiento y el mismo dominio, aparte que el que les provee el ISP. En esta obra se tiene que mencionar que brinda servicios a la comunidad y al colegio por lo cual se tiene que considerar el diseño establecido para la interconexión. En la obra Salesiana San Rafael. Las falencias de la obra es que no tienen segmentación de red, un plan IP establecido, control de ancho de banda para la red y solventar la red inalámbrica, lo que sería adecuado es hacer una segmentación de red, tener control de ancho de banda dependiendo de los usuarios de la obra y Wireless.

### 4.3.3. Fase de diseño

El diseño de la red se desarrollará en base de los requisitos técnicos y comerciales obtenidos en las fases anteriores. El mismo es un diseño detallado integral que va a cumplir con los requisitos técnicos y de necesidades actuales. En lo que proporcionará alta disponibilidad, fiabilidad, seguridad, escalabilidad y rendimiento. En este diseño se incluirá diagramas de red y algunas listas de equipos de red. El plan del proyecto se basa con la información más importante para su consideración en una futura implementación. Una vez aprobada la fase de diseño, se iniciará con la fase de Implementación, la cual será otro proyecto.

Este proyecto se basará en un diseño de Cisco Enterprise Architecture Model.

Figura 50. Diagrama de red de frontera




Fuente: (Bruno & Jordan, CCDA 640-864 Official Cert Guide, 2013, pág. 48)

El diagrama de la figura 50, corresponde a una parte del diseño jerárquico de Cisco, ya que constituye parte de un diagrama global. El enfoque principal para el presente proyecto es el diseño de frontera (borde) figura 44, ya que constituye cuatro etapas las cuales son: E-Commerece/DMZ/Internet, Enterprise WAN y Remote Access VPN.

### 4.3.4. Diseño lógico de la red de frontera

Para obtener la intercomunicación entre la matriz y sus obras se configuro en los dispositivos de frontera. El tipo de enrutamiento es OSPF.

- OSPF: Open Shortest Path First es un protocolo de enrutamiento jerárquico de pasarela interior, usa el algoritmo SWD enlace-estado este tipo de enrutamiento sirve para calcular la ruta más corta posible, utilizando la métrica de menor costo.
- Se optó por enrutamiento OSPF porque utiliza la trayectoria más corta, además se usa muy frecuentemente como protocolo de encaminamiento interior en redes TCP/IP. Las ventajas de este tipo de enrutamiento, son: mayor eficiencia, agilidad y eficacia en la entrega de paquetes, por utilizar el camino más corto.

Los tipos de enlaces se describen a continuación:

- El módulo WAN utiliza diferentes tecnologías de direccionamiento de tráfico entre los módulos remotos y la matriz.
- En este módulo estarán todos los enlaces que están dedicados exclusivamente para conexiones con las ubicaciones remotas.

Enlaces de datos y voz:
Líneas arrendadas con empresas como:

- Telconet
- CNT

Los tipos de enlaces que se utilizaran para telefonía son los **E1** es una trama síncrona de 2,048 mbps. Transmiten canales de voz. Como cada canal de voz utiliza 64 kbps, la cual se configura en las tarjetas de los router de frontera, para el servicio de voz.

Se presenta el direccionamiento que se diseñó para la Casa Inspectorial Salesiana como para sus obras. La opción más adecuada son las de clase B ya que se utiliza para las redes de tamaño mediano.

Se ha escogido el direccionamiento de clase B para una empresa mediana, ya que mediante este plan IP nos sirve para seguir aumentando, dependiendo de la demanda de usuarios, ya sea este para la matriz como para sus obras.

Tabla 30. Plan IP.

| | CASA INSPECTORIAL | | | SUBREDES 172.17.0.0-172.17.5.0 | | |
|---|---|---|---|---|---|---|
| NOMBRE SUBRED | DESCRIPCION | DIRECCION DE RED | MASCARA | GATEWAY | RANGO IP | # DE HOST |
| VLAN 1 | VLAN DE DEFAULT | 172.17.0.0 | 255.255.255.0 | 172.17.0.254 | 172.17.0.1-172.17.0.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN | VIRTUAL LAN DMZ | 172.17.1.0 | 255.255.255.0 | 172.17.1.254 | 172.17.1.1-172.17.1.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 3 | VLAN ADMINISTRATIVOS | 172.17.2.0 | 255.255.255.192 | 172.17.2.62 | 172.17.2.1-172.17.2.62 | 62 (1 SUBRED 1 BROADCAST) |
| VLAN 5 | VLAN PRINCIPALES | 172.17.2.64 | 255.255.255.192 | 172.17.2.126 | 172.17.2.65-172.17.2.126 | 62 (1 SUBRED 1 BROADCAST) |
| VLAN 6 | VLAN SECUNDARIOS | 172.17.2.128 | 255.255.255.192 | 172.17.2.190 | 172.17.2.129-172.17.2.190 | 62 (1 SUBRED 1 BROADCAST) |
| VLAN 2 | TELEFONIA VoIP | 172.17.3.0 | 255.255.255.0 | 172.17.3.254 | 172.17.3.1-172.17.3.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 4 | VLAN WIRELESS | 172.17.4.0 | 255.255.255.0 | 172.17.4.254 | 172.17.4.1-172.17.4.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 7 | INTERNET | 172.17.5.0 | 255.255.255.0 | 172.17.5.254 | 172.17.5.1-172.17.5.254 | 254 (1 SUBRED 1 BROADCAST) |

| | OBRA DON BOSCO LA KENNEDY | | | SUBREDES 172.17.6.0-172.17.19.0 | | |
|---|---|---|---|---|---|---|
| NOMBRE SUBRED | DESCRIPCION | DIRECCION DE RED | MASCARA | GATEWAY | RANGO IP | # DE HOST |
| VLAN 1 | VLAN DE DEFAULT | 172.17.6.0 | 255.255.255.0 | 172.17.6.254 | 172.17.6.1-172.17.6.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN | VIRTUAL LAN DMZ | 172.17.7.0 | 255.255.255.0 | 172.17.7.254 | 172.17.7.1-172.17.7.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 3 | VLAN ADMINISTRATIVOS | 172.17.8.0 | 255.255.255.0 | 172.17.8.254 | 172.17.8.1-172.17.8.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 5 | VLAN ESENTIA-DOCENTES | 172.17.10.0 | 255.255.254.0 | 172.17.11.254 | 172.17.10.1-172.17.11.254 | 510 (1 SUBRED 1 BROADCAST) |
| VLAN 6 | VLAN DOCENTES | 172.17.12.0 | 255.255.254.0 | 172.17.13.254 | 172.17.12.1-172.17.13.254 | 510 (1 SUBRED 1 BROADCAST) |
| VLAN 7 | VLAN COLEGIO | 172.17.14.0 | 255.255.255.0 | 172.17.14.254 | 172.17.14.1-172.17.14.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 8 | VLAN ESCUELA | 172.17.15.0 | 255.255.255.0 | 172.17.15.254 | 172.17.15.1-172.17.15.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 2 | TELEFONIA VoIP | 172.17.16.0 | 255.255.255.0 | 172.17.16.254 | 172.17.16.1-172.17.16.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 4 | VLAN WIRELESS | 172.17.17.0 | 255.255.255.0 | 172.17.17.254 | 172.17.17.1-172.17.17.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 9 | VLAN UPS-COLEGIO | 172.17.18.0 | 255.255.255.0 | 172.17.18.254 | 172.17.18.1-172.17.18.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 10 | INTERNET | 172.17.19.0 | 255.255.255.0 | 172.17.19.254 | 172.17.19.1-172.17.19.254 | 254 (1 SUBRED 1 BROADCAST) |

| | OBRA DON DOSCO LA TOLA | | | SUBREDES 172.17.21.0-172.17.32.0 | | |
|---|---|---|---|---|---|---|
| NOMBRE SUBRED | DESCRIPCION | DIRECCION DE RED | MASCARA | GATEWAY | RANGO IP | # DE HOST |
| VLAN 1 | VLAN DE DEFAULT | 172.17.20.0 | 255.255.255.0 | 172.17.20.254 | 172.17.20.1-172.17.20.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN | VIRTUAL LAN DMZ | 172.17.21.0 | 255.255.255.0 | 172.17.21.254 | 172.17.21.1-172.17.21.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 3 | VLAN ADMINISTRATIVOS | 172.17.22.0 | 255.255.255.0 | 172.17.22.254 | 172.17.22.1-172.17.2.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 5 | VLAN APLICACION-DOCENTES | 172.17.24.0 | 255.255.254.0 | 172.17.25.254 | 172.17.24.1-172.17.25.254 | 510 (1 SUBRED 1 BROADCAST) |
| VLAN 6 | VLAN DOCENTES | 172.17.26.0 | 255.255.254.0 | 172.17.27.254 | 172.17.26.1-172.17.27.254 | 510 (1 SUBRED 1 BROADCAST) |
| VLAN 7 | VLAN COLEGIO | 172.17.28.0 | 255.255.255.0 | 172.17.28.254 | 172.17.28.1-172.17.28.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 8 | VLAN ESCUELA | 172.17.29.0 | 255.255.255.0 | 172.17.29.254 | 172.17.29.1-172.17.39.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 2 | TELEFONIA VoIP | 172.17.30.0 | 255.255.255.0 | 172.17.30.254 | 172.17.30.1-172.17.30.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 4 | VLAN WIRELESS | 172.17.31.0 | 255.255.255.0 | 172.17.31.254 | 172.17.31.1-172.17.31.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 9 | INTERNET | 172.17.32.0 | 255.255.255.0 | 172.17.32.254 | 172.17.32.1-172.17.32.254 | 254 (1 SUBRED 1 BROADCAST) |

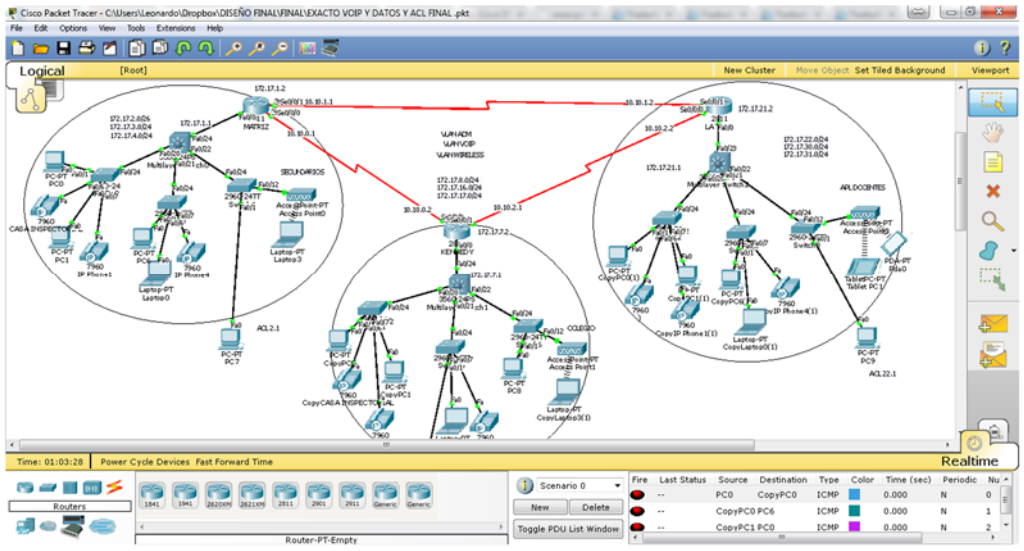
| | OBRA COLEGIO SÁNCHEZ CIFUENTES | | | SUBREDES 172.17.33.0-172.17.40.0 | | |
|---|---|---|---|---|---|---|
| NOMBRE SUBRED | DESCRIPCION | DIRECCION DE RED | MASCARA | GATEWAY | RANGO IP | # DE HOST |
| VLAN 1 | VLAN DE DEFAULT | 172.17.33.0 | 255.255.255.0 | 172.17.33.254 | 172.17.33.1-172.17.33.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN | VIRTUAL LAN DMZ | 172.17.34.0 | 255.255.255.0 | 172.17.34.254 | 172.17.34.1-172.17.34.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 3 | VLAN ADMINISTRATIVOS | 172.17.41.0 | 255.255.255.128 | 172.17.41.126 | 172.17.41.1-172.17.41.126 | 126 (1 SUBRED 1 BROADCAST) |
| VLAN 5 | VLAN APLICACION-DOCENTES | 172.17.35.0 | 255.255.255.0 | 172.17.35.254 | 172.17.35.1-172.17.35.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 6 | VLAN DOCENTES | 172.17.36.0 | 255.255.255.0 | 172.17.36.254 | 172.17.36.1-172.17.36.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 7 | VLAN COLEGIO | 172.17.37.0 | 255.255.255.0 | 172.17.37.254 | 172.17.37.1-172.17.37.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 8 | VLAN ESCUELA | 172.17.38.0 | 255.255.255.0 | 172.17.38.254 | 172.17.38.1-172.17.38.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 2 | TELEFONIA VoIP | 172.17.41.128 | 255.255.255.128 | 172.17.41.254 | 172.17.41.129-172.17.46.254 | 126 (1 SUBRED 1 BROADCAST) |
| VLAN 4 | VLAN WIRELESS | 172.17.39.0 | 255.255.255.0 | 172.17.39.254 | 172.17.39.1-172.17.39.254 | 254 (1 SUBRED 1 BROADCAST) |
| VLAN 9 | INTERNET | 172.17.40.0 | 255.255.255.0 | 172.17.40.254 | 172.17.40.1-172.17.40.254 | 254 (1 SUBRED 1 BROADCAST) |

Elaborado por: Leonardo Suárez.

#### 4.3.4.1.Configuración de los dispositivos finales routers en con las herramientas GNS3 y Packet tracer

A continuación se presenta las debidas configuraciones de los dispositivos basados en la red de frontera, en los que consta QoS, videoconferencia, VPN, VoIP y ACL, que vendrían a simular los equipos diseñados los cuales son WSA y ASA.

Figura 51. Diagrama de red de frontera en packet tracer.




Elaborado por: Leonardo Suárez.

- **Configuración del router de la Casa Inspectorial Salesiana**

Se presenta a continuación las configuraciones a nivel de router de frontera en la que se encuentra configurado VPN, ACL, videoconferencia, VoIP y QoS.

QoS se implementó en los dispositivos de frontera para garantizar calidad de servicio correspondiente a voz y videoconferencia, en la que se diseñó y se simuló, además de las respectivas configuraciones en los enlaces para no tener pérdidas en cuanto a voz y video. Se tomó como referencia las configuraciones de dos routers para basarse en los demás, lo único que cambian en los otros dispositivos son los direccionamientos que se basa en la tabla del plan IP.

- **Configuración de router**

A continuación se presenta el contenido del archivo running-config del Router perteneciente a la Casa Inspectorial Salesiana, configurado en el simulador Packet Tracer:

```
### Configuración del nombre del router que viene por defecto ###
hostname GW-CASA_INSP
### Configuración del pass enable del dispositivo para ingresar al modo global ###
enable password 7 0835495D000A
###Configuración para habilitar el pool de los teléfonos IP dado el segmento de red con la opción de 150 al gateway de voz###
ip dhcp pool VOZ_IP (E1)
 network 172.17.3.0 255.255.255.0
 default-router 172.17.3.254
 option 150 ip 172.17.3.254
###Configuración para habilitar el pool de la red administrativa dado el segmento de red con su respectivo gateway ###
ip dhcp pool ADM
 network 172.17.2.0 255.255.255.192
 default-router 172.17.2.62
###Configuración para habilitar el pool de la red de WIRELESS dado el segmento de red con su respectivo gateway ###
ip dhcp pool WIRELESS
 network 172.17.4.0 255.255.255.0
 default-router 172.17.4.254
###Configuración para habilitar el pool de la red principales dado el segmento de red con su respectivo gateway ###
ip dhcp pool PRINCIPALES
 network 172.17.2.64 255.255.255.192
 default-router 172.17.2.126
###Configuración para habilitar el pool de la red secundarios dado el segmento de red con su respectivo gateway ###
ip dhcp pool SECUNDARIOS
```

```
 network 172.17.2.128 255.255.255.192
 default-router 172.17.2.190
###Configuración para habilitar aaa para los multiples usuarios###
aaa new-model
aaa authentication login default local
### Configuración del usuario creado por la aaa###
username jespinoza privilege 15 secret 5 $1$mERr$gc0bTUXHJaVERV37j2m5D0
username lsuarez privilege 15 secret 5 $1$mERr$gc0bTUXHJaVERV37j2m5D0
username mlopez privilege 15 secret 5 $1$mERr$gc0bTUXHJaVERV37j2m5D0
### Configuración de política de encriptación para VPN con un número ###
crypto isakmp policy 10
 ### Configuración de algoritmo de encriptación de 256 bits
encr aes 256
### Configuración de claves pre-compartidas  ###
authentication pre-share
 ### Configuración de grupo deffie-hellman 2 ###
group 2
### Configuración de tiempo de vida para la conexión entre 60-84600###
lifetime  84600
### Configuración de clave para la conexión y dirección donde se establece la
conexión, este será la interfaz de la salida del router de la Kennedy ###
crypto isakmp key tesis address 10.10.0.2
### Configuracion de la transformada de ipsec el nombre puede ser cualquiera,
además de los tipos de cifrado que se usara en la transformada ###
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
### Configuración de la encriptación para asociar a la transform CMAP nombre
cualquiera, se debe tomar en cuenta que el número es de la política creada
anteriormente ###
crypto map CMAP 10 ipsec-isakmp
 ### Configuración de la interfaz remota ###
set peer 10.10.0.2
  ### Asociacion de la ACL creada a continuación ###
set transform-set TSET
 match address 101
```

```
### Habilitación del protocolo ssh con el nombre de dominio cualquiera ###
ip ssh version 2
ip domain-name ssh
spanning-tree mode pvst
### Creación de clases para la QoS de voz ###
class-map match-all Voz
 match ip dscp default
class-map match-all Mision-Critica
class-map match-any VOICE
 match access-group 101
class-map match-all Mejor-esfuerzo
 match ip dscp default
class-map match-all ssh
 match ip dscp default
### Creación de políticas para QoS en el enlace ###
policy-map SetQoS
 class Voz
  priority percent 30
 class ssh
  priority percent 10
 class class-default
  fair-queue
  random-detect dscp-based
### Creación de políticas para QoS para ser configuradas a nivel de interfaz ###
policy-map SetQoS_IN
 class Voz
  set ip dscp default
 class VOICE
  set ip dscp ef
 class ssh
  set ip dscp default
### Configuración de la interface con su IP respectiva y con listas de accesos para
las ACL, además control de QoS en enlace interno ###
interface FastEthernet0/0
```

```
 no ip address
 service-policy input SetQoS_IN
 duplex auto
 speed auto
###Configuración para habilitar subinterfaces para obtener enrutamiento inter VLAN y tener comunicación entre las diferentes redes internas, esta subinterfaz es creada una IP para administración de equipo, ingresar remotamente para administrarlo###
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
ip address 172.17.1.2 255.255.255.0
###Configuración para habilitar subinterfaces para obtener enrutamiento inter VLAN y tener comunicación entre las diferentes redes internas asignado su IP la cual es el gateway ###
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 172.17.3.254 255.255.255.0
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 172.17.2.62 255.255.255.192
 ip access-group ADM in
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 172.17.4.254 255.255.255.0
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 172.17.2.126 255.255.255.192
interface FastEthernet0/0.6
 encapsulation dot1Q 6
 ip address 172.17.2.190 255.255.255.192
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
```

### Configuración de la interface externa del router, asociación de encriptación crypto map para la VPN y políticas de calidad de servicio en el enlace ###
interface Serial0/0/0
 bandwidth 1000000
 ip address 10.10.0.1 255.255.255.0
 ip access-group 1 out
 service-policy output SetQoS
 crypto map CMAP
### Configuración de la interface con su IP respectiva y con listas de accesos para las ACL, además control de QoS en enlace externo que actuara como DCE ###
interface Serial0/0/1
 ip address 10.10.1.1 255.255.255.252
 service-policy output SetQoS
interface Vlan1
 no ip address
### Configuración de enrutamiento dinámico, para la intercomunicación con las demás áreas ###
router ospf 1
 log-adjacency-changes
 network 10.10.0.0 0.0.0.255 area 0
 network 10.10.1.0 0.0.0.3 area 0
 network 172.17.1.0 0.0.0.255 area 0
 network 172.17.2.0 0.0.0.63 area 0
 network 172.17.3.0 0.0.0.255 area 0
 network 172.17.4.0 0.0.0.255 area 0
 network 172.17.0.0 0.0.0.255 area 0
ip classless
### Creación de la lista de acceso que permita la conectividad entre la red local y la remota para las VPN ##
access-list 101 permit ip 172.17.2.0 0.0.0.63 172.17.8.0 0.0.0.255
### Creación de la lista de acceso que permita la conectividad entre la red local y la remota o viceversa ##
ip access-list extended ADM
 deny ip host 172.17.2.1 any

```
 permit ip any any
### Configuración de dial peer para VoIP con su destination pattern que se puedan comunicar con las demás sucursales dependiendo el primer digito ###
dial-peer voice 1 voip
 destination-pattern 2...
 session target ipv4:10.10.0.2
dial-peer voice 3 voip
 destination-pattern 3...
 session target ipv4:10.10.1.2
telephony-service
 max-ephones 5
 max-dn 5
 ip source-address 172.17.3.254 port 2000
 auto assign 1 to 5
### Registración de telefonos con su ID y su numero de extensión ###
ephone-dn 1
 number 1101
ephone-dn 2
 number 1102
ephone-dn 3
 number 1103
ephone-dn 4
 number 1104
ephone-dn 5
 number 1105
### Configuración automática a través de los aut-assig con su mac de telefono y tipo ##
ephone 1
 device-security-mode none
 mac-address 0060.2F74.DAD1
 type 7960
 button 1:1
ephone 2
 device-security-mode none
```

```
 mac-address 0040.0B30.201D
 type 7960
 button 1:2
ephone 3
 device-security-mode none
 mac-address 0090.2BBA.48B0
 type 7960
 button 1:3
ephone 4
 device-security-mode none
 mac-address 0060.2FB8.9E34
 type 7960
 button 1:4
ephone 5
 device-security-mode none
 mac-address 0005.5E38.88C4
 type 7960
 button 1:5
###Configuración de banner, que se visualizara en el ingreso al dispositivo por ssh###
banner motd ^C Acceso restringido ^C
### Configuración de encriptación de contraseñas para acceso al dispositivo mediante ssh ###
line con 0
line aux 0
line vty 0 4
 session-limit 3
 password 7 0835495D000A
 logging synchronous
 transport input ssh
end
```

- **Configuración de router**.

Se presenta a continuación el contenido del archivo running-config del Router perteneciente a la Casa Salesiana, configurado en el simulador GNS3:

```
### Configuración del nombre del router que viene por defecto ###
hostname CASA_INSP
boot-start-marker
boot-end-marker
### Configuración del pass enable del dispositivo para ingresar al modo global ###
enable secret 5 $1$SL.2$DeHxOKTxjWgmwD1RqP4sI0
enable password 7 0835495D000A
###Configuración para habilitar aaa para los multiples usuarios###
aaa new-model
aaa authentication login default local
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
### Habilitación del protocolo ssh con el nombre de dominio cualquiera ###
ip domain name ssh
multilink bundle-name authenticated
### Configuración del usuario creado por la aaa###
username lsuarez privilege 15 secret 5 $1$mERr$gc0bTUXHJaVERV37j2m5D0
username jespinoza privilege 15 secret 5 $1$mERr$gc0bTUXHJaVERV37j2m5D0
username mlopez privilege 15 secret 5 $1$mERr$gc0bTUXHJaVERV37j2m5D0
archive
 log config
  hidekeys
ip tcp synwait-time 5
### Creación de clases para la QoS de voz ###
class-map match-all Voz
 match ip dscp cs5  ef
class-map match-all INTERNETK
```

```
 match protocol http
 match protocol pop3
 match protocol snmp
 match protocol imap
 match protocol dns
class-map match-all VIDEO
 match protocol sip
 match protocol h323
class-map match-all Video
 match ip dscp default
class-map match-all Mision-Critica
 match ip dscp cs3  af31  af32  af33
class-map match-any VOICE
 match access-group 101
class-map match-all ssh
class-map match-all Mejor-esfuerzo
 match ip dscp default
### Creación de políticas para QoS en el enlace ###
policy-map TELCONET
 class VIDEO
    police 384000 6000
 class INTERNETK
    police 256000 6000
  bandwidth 256
  shape average 256000 6000
 class class-default
  bandwidth 640
  shape average 640000 6000
### Creación de políticas para QoS en el enlace ###
policy-map SetQoS
 class Video
  priority percent 20
 class Mejor-esfuerzo
  bandwidth percent 15
```

```
 class Voz
  priority percent 10
 class ssh
  priority percent 10
### Creación de políticas para QoS para ser configuradas a nivel de interfaz ###
policy-map SetQoS_IN
 class Video
  set ip dscp default
 class VOICE
  set ip dscp ef
 class ssh
  set ip dscp default
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
### Configuración de la interface con su IP respectiva y con listas de accesos para las ACL, además control de QoS en enlace interno ###
interface FastEthernet1/0
 ip address 172.17.2.62 255.255.255.192
 ip access-group 100 in
 duplex auto
 speed auto
 service-policy input SetQoS_IN
### Configuración de la interface externa del router, asociación y políticas de calidad de servicio en el enlace ###
interface FastEthernet1/1
 ip address 10.10.1.1 255.255.255.0
 duplex auto
 speed auto
 service-policy output SetQoS
### Configuración de la interface externa del router, asociación y políticas de calidad de servicio en el enlace ###
interface FastEthernet2/0
```

```
 ip address 10.10.0.1 255.255.255.0
 duplex auto
 speed auto
 service-policy output SetQoS
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/1
 no ip address
 shutdown
 duplex auto
 speed auto
### Configuración de enrutamiento dinámico, para la intercomunicación con las
demás áreas ###
router ospf 1
 log-adjacency-changes
 network 10.10.0.0 0.0.0.255 area 0
```

```
 network 10.10.1.0 0.0.0.3 area 0
 network 10.10.1.0 0.0.0.255 area 0
 network 172.17.2.0 0.0.0.63 area 0
 network 172.17.2.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
logging alarm informational
### Creación de la lista de acceso que permita la conectividad entre la red local y la
remota para permitir o denegar videoconferencia, ssh y hacer ping ##
access-list 100 deny   icmp 172.17.2.0 0.0.0.63 host 172.17.22.2 log
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 3032
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 3033
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 3034
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 3035
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 3036
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 3037
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 1720
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 eq 5060
access-list 100 permit tcp 172.17.22.0 0.0.0.24 host 172.17.2.1 eq 5060
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.22.2 log
access-list 100 permit udp 172.17.2.0 0.0.0.63 host 172.17.22.2 log
access-list 100 permit tcp 172.17.2.0 0.0.0.63 host 172.17.2.62 log
access-list 100 permit udp 172.17.2.0 0.0.0.63 host 172.17.2.62 log
control-plane
gatekeeper
 shutdown
###Configuración de banner, que se visualizara en el ingreso al dispositivo por
ssh###
banner motd ^C Acceso restingido ^C
### Configuración de encriptación de contraseñas para acceso al dispositivo
mediante ssh ###
line con 0
 exec-timeout 0 0
```

```
 privilege level 15
 password 7 044F0E150632
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password 7 0835495D000A
 session-limit 3
 logging synchronous
 transport input ssh
end
```

### 4.3.5. Diseño físico de la red de frontera

Este diseño fue realizado en base a las figuras 52 – 56, antes mencionadas en la marca Cisco, ya que fue tomado como referencia para establecer el diseño de la red de frontera, en la cual esta metodología cumple los requerimientos de escalabilidad, disponibilidad, seguridad y facilidad de gestión para administración de equipos tanto en la red interna como en la red externa.

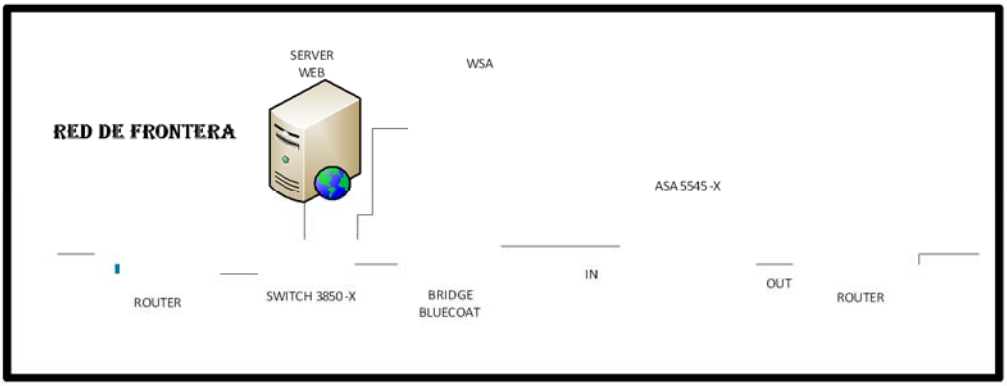
Tabla 31. Presupuesto referencial costo implementación.

| ***NOMBRE DEL EQUIPO*** | ***VALOR UNITARIO*** | ***CANTIDAD*** | ***TOTAL*** |
|---|---|---|---|
| NGFW ASA 5545-Xw/ SW 8GE Data 1GE Mgmt AC 3DES/AES 2SSD120 | 9.754,76 € | 1 | 9.754,76 € |
| WSA WEB SECURITY APPLIANCE WITH SOFTWARE | 5.818,81 € | 1 | 5.818,81 € |
| SMARNET 8X5XNBD WSA S380 WEB SECURITY 1YEAR | 760,03 € | 1 | 760,03 € |
| BLUE COAT PACKETSHAPER 12000, 1000BASE-T, UP TO 200MBPS OF SHAPING, 2048/5000 CLASSES | 65.899,69 € | 1 | 65.899,69 € |
| BLUE TOUCH PARTNER SUPPORT, 24X7 L3 SOFTWARE ONLY, PS12000-L200M, 1 YEAR | 8.609,48 € | 1 | 8.609,48 € |
| SAME DAY SHIPMENT HARDWARE SUPPORT, PS12000-L200M, 1 YEAR | 2.152,37 € | 1 | 2.152,37 € |
| **TOTAL** | 92.995,14 € | | 92.995,14 € |

Elaborado por Leonardo Suárez.

Este proyecto se tomará en cuenta para proyectos posteriores en cuanto a implementación y funcionamiento.

Figura 52. Diagrama físico de red de frontera

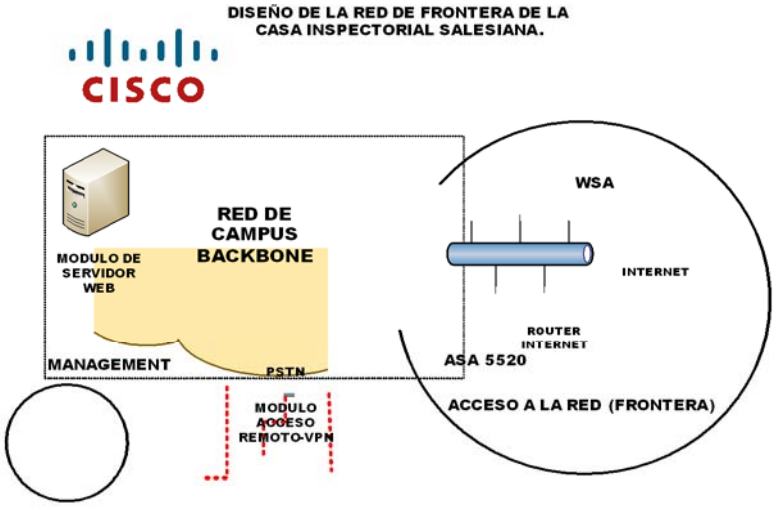



Fuente: www.cisco.com, Leonardo Suárez.

En la figura 52 se muestra las diferentes funcionalidades de cada área, como van a interactuar y cual va hacer su función en la red de frontera.

Estos equipos a utilizar tienen como función, garantizar la calidad de servicio y la disponibilidad para los usuarios finales.

Figura 53. Diseño físico de la red de frontera (borde), por medio de los dispositivos correspondientes




Elaborado por: Leonardo Suárez.

Tabla 32. Descripción del módulo PVDM3.

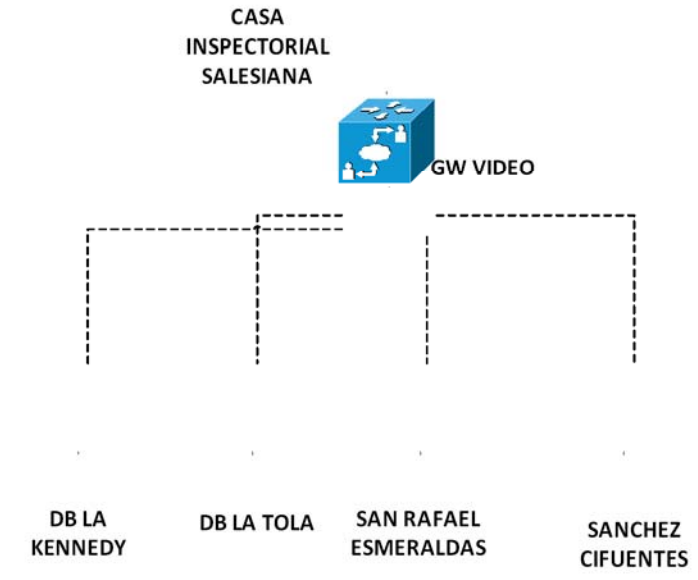
| Nombre | Códecs de baja complejidad | Códecs de mediana complejidad | Códecs de alta complejidad |
|---|---|---|---|
| Módulo PVDM3 | G.711, ClearChannel y paso | G.729a, G.729ab, G.726, | G.723.1, G.728, G.729, G.729b, |
| | a través de fax o módem | G.722 y retransmisión de fax | Internet Low Bitrate Codec (iLBC) y retransmisión de módem |

Elaborado por Leonardo Suárez.

En la tabla 32, se hace a la referencia a los módulos del router de frontera, ya que estos módulos soportan video y VoIP, en la que se debe tomar en cuenta para ser instalada, los canales y la demanda de llamadas por usuario desde la matriz hacia las sucursales y viceversa o llamadas hacia el exterior, ya sea convencional o celular.

### 4.3.6. Video conferencia

Figura 54. Conexión de equipos de videoconferencia.




Elaborado por: Leonardo Suárez.

### 4.3.7. Calidad de servicio QoS VoIP y videoconferencia

QoS trabaja como el engranaje de las redes modernas porque realiza el marcado del tráfico (clasificación), reserva y da prioridad a cierta clase de tráfico sobre otros (que hacen cola) y en caso de congestión, puede comenzar a tirar el tráfico menos importante basado en la clasificación del mismo (WRED, Weighted Random Early Detection). La calidad de servicio punto-a-punto (end-to-end QoS). Con este

acercamiento, se puede garantizar en gran parte que el tráfico más sensible, tal como voz y vídeo, tenga prioridad sobre el tráfico menos importante (no en tiempo real) como por ejemplo el tráfico normal de Internet o FTP.

QoS puede ser utilizada para seguridad y para limitar el ancho de banda garantizando que el tráfico que pasa por el enlace WAN no está sobre utilizado. Esto lo realiza limitando o conformando el tráfico de salida de la interfaz WAN.

El sistema operativo IOS tiene varias maneras y mecanismos que se pueden utilizar para implementar y configurar QoS, uno de los mejores métodos y de uso cada vez más general es por línea de comandos ó MQC (Modular QoS Command-Line)." (Prado, 2011, pág. 1)

#### 4.3.7.1. Requerimientos para la política de Calidad de Servicio

- ✓ VOIP-RTP con marcado DSCP=EF. El tráfico debe ser manejado primero en el caso de haber congestión en la interfaz. Además debe ser garantizado y limitado en todo momento hasta un máximo de 30% del ancho de banda de la interfaz de WAN.
- ✓ Señalización de VoIP con marcado CS3. El tráfico debe tener un ancho de banda garantizado de mínimo 8% en caso de congestión.
- ✓ El tráfico de Telnet necesita un 3% del ancho de banda garantizado en caso congestión.
- ✓ El tráfico de Telnet que va al equipo con dirección IP x.x.x.x necesita el 5% del ancho de banda de la interfaz garantizada en caso de congestión.
- ✓ Si hay 30 paquetes en la cola con CS 6 (paquetes de sistema) el enrutador tiene que comenzar a tirar estos paquetes, si los paquetes alcanzan 40, un 25% de los paquetes debe ser tirado, si el número es mayor a 40 todos los paquetes con CS 6 debe ser descartados." En este artículo se basó para las configuraciones de QoS ya que es lo recomendado, referente a la demanda de tráfico que se va a obtener entre matriz y sucursal (Prado, 2011, pág. 1)

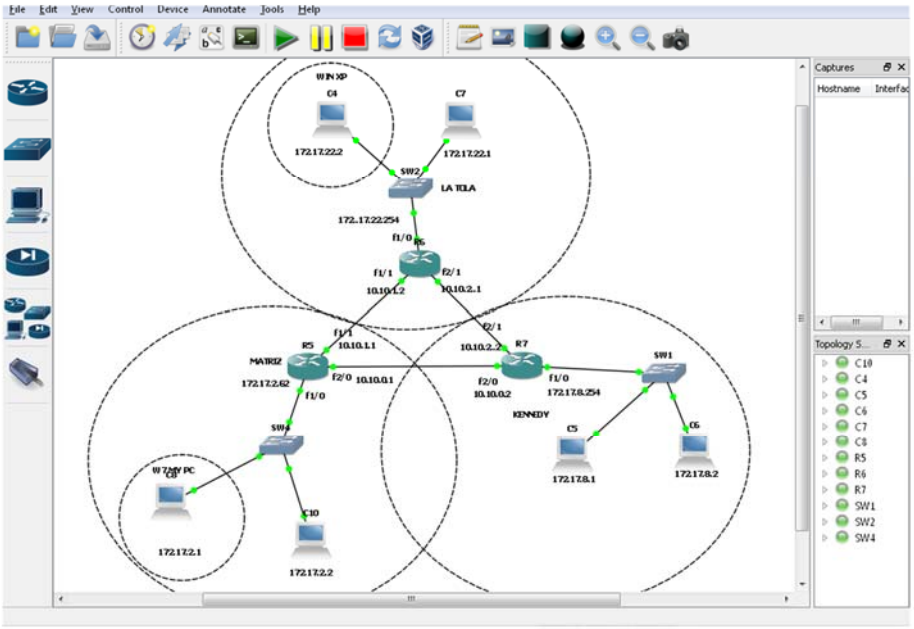
## 4.4. Pruebas de simulación y conexiones

En las pruebas siguientes se presenta la topología en el software GNS3. En el cual se encuentra configurada QoS en los enlaces para videoconferencia y VoIP, a nivel de router se encuentran configurados ACL que vendrían a simular los dispositivos de WSA y ASA respectivamente.

### 4.4.1. Videoconferencia

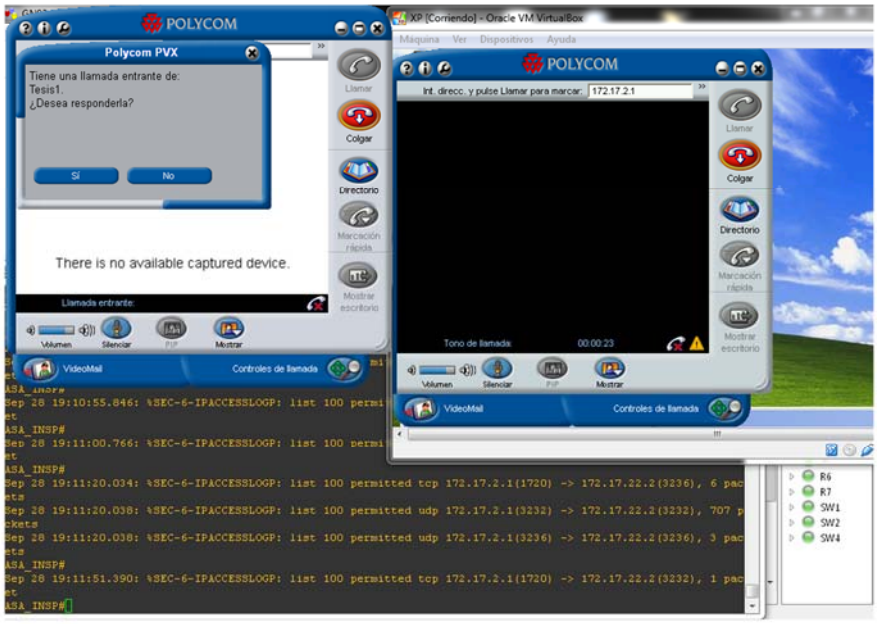
En la figura 55, se encuentra simulado videoconferencia con el software GNS3, las que se encuentran montadas en una máquina virtual y física.

Figura 55. Diseño para simulación de equipos de videoconferencia GNS3




Elaborado por: Leonardo Suárez.

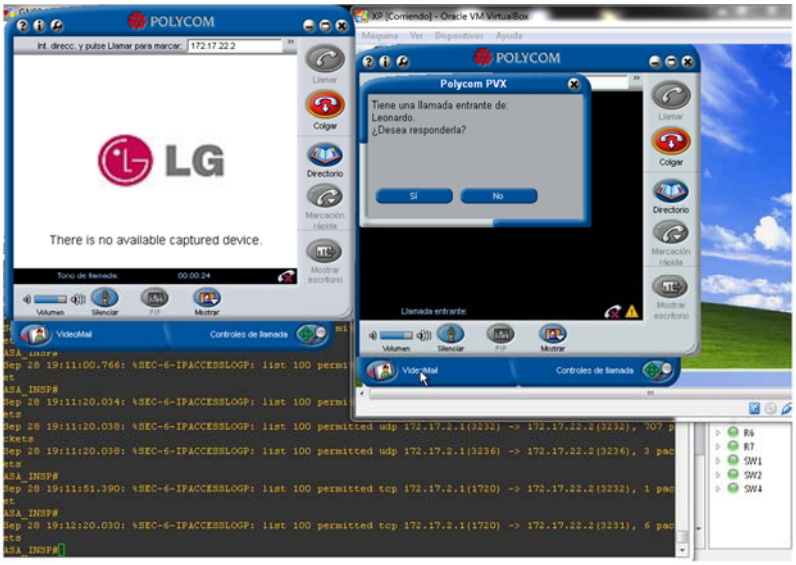
Figura 56. Simulación de videoconferencia desde la sucursal a la matriz GNS3




Elaborado por: Leonardo Suárez.

Pruebas de conectividad en lo que interactúan videoconferencia, QoS y ACL, en lo que se constata que se encuentran permitidos los puertos para videoconferencia, como se puede observar en la figura 56.

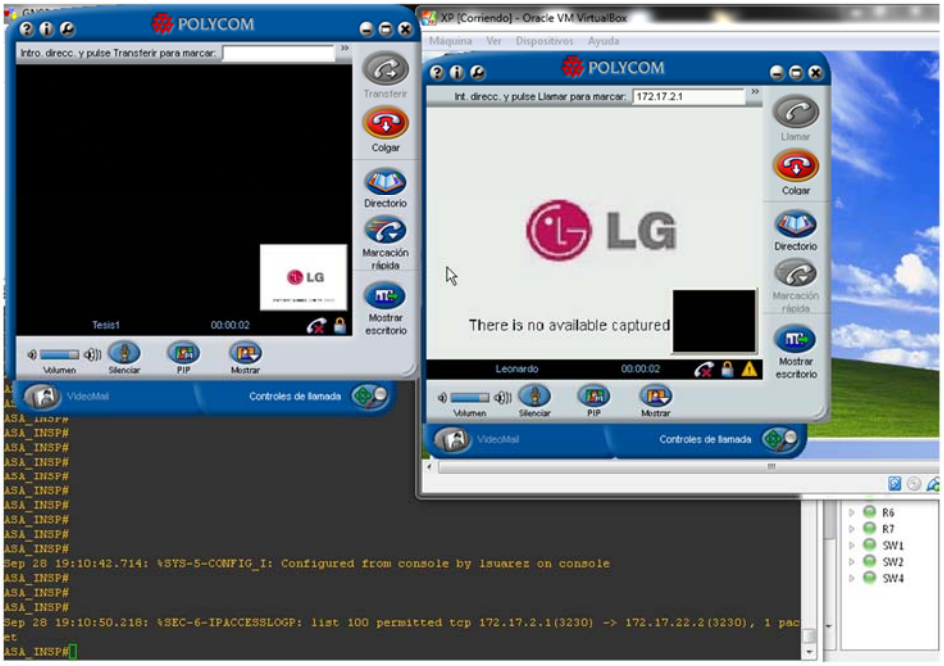
Figura 57. Simulación de videoconferencia desde la matriz a la sucursal GNS3




Elaborado por: Leonardo Suárez.

Pruebas de conexión desde la matriz hacia la obra en lo que se puede visualizar en la figura 57, esto se encuentra simulado en una máquina física que es la matriz y la otra que es virtualizada que se asemeja a una sucursal.

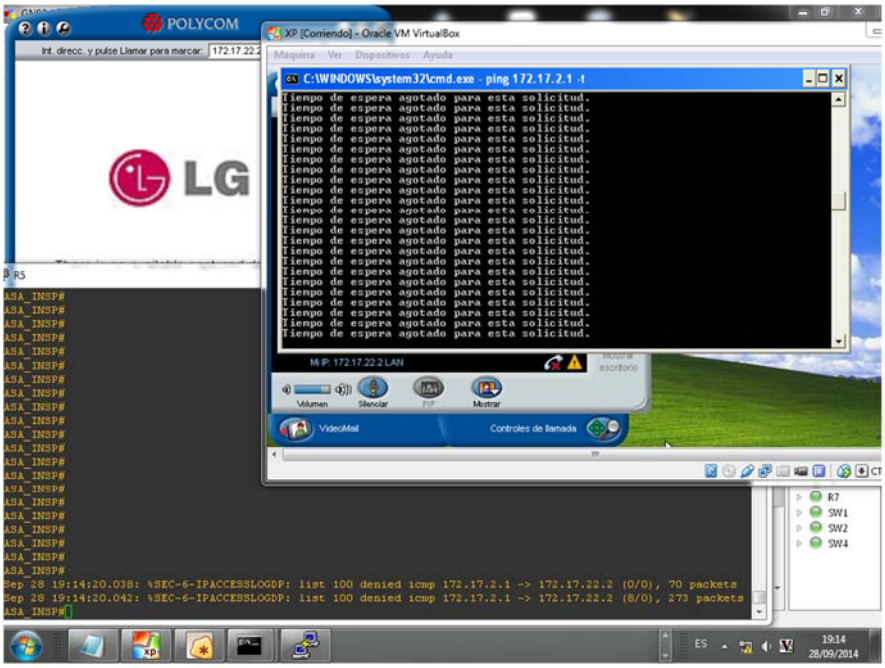
Figura 58. Simulación de videoconferencia desde la matriz a la sucursal GNS3




Elaborado por: Leonardo Suárez.

Pruebas de comunicación en la figura 58, en la que se encuentra establecida ya la videoconferencia entre la matriz con la sucursal, y lo q se hace la referencia en la parte de abajo que están interactuando ACL que permiten videoconferencia.

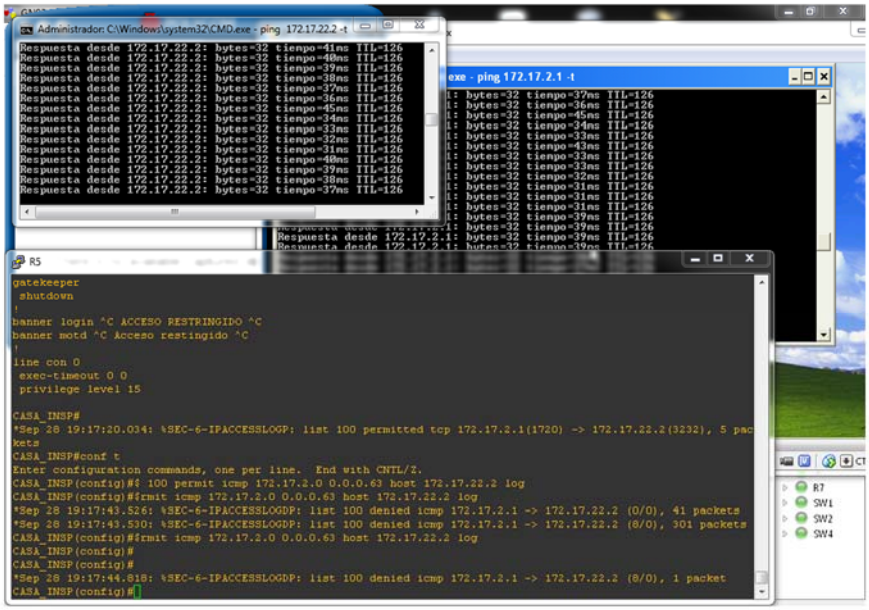
Figura 59. ACL denegado icmp desde la sucursal hacia la matriz GNS3




Elaborado por: Leonardo Suárez.

En la figura 59, se encuentran configuradas ACL por lo que se visualiza que tienen efecto en lo que se encuentra denegado en protocolo ICMP desde la sucursal hacia la matriz.

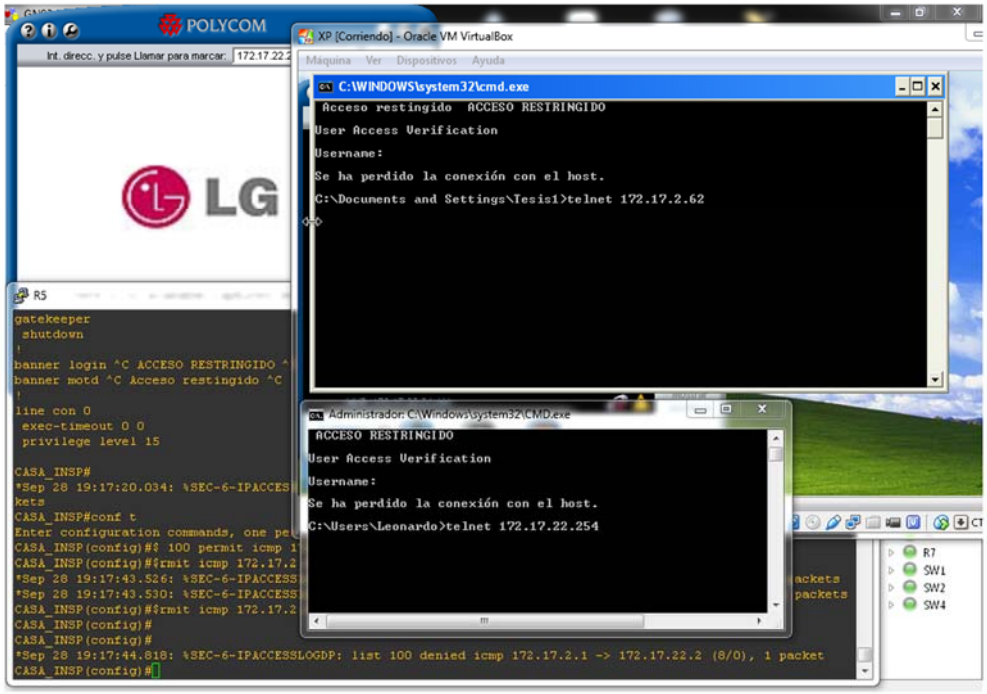
Figura 60. ACL permitido ICMP desde la sucursal hacia la matriz GNS3




Elaborado por: Leonardo Suárez.

A continuación se muestra en la figura 60, que estan configuradas ACL por lo que se visualiza que tienen efecto, en lo que se encuentra permitido el protocolo ICMP desde la sucursal hacia la matriz y viceversa.

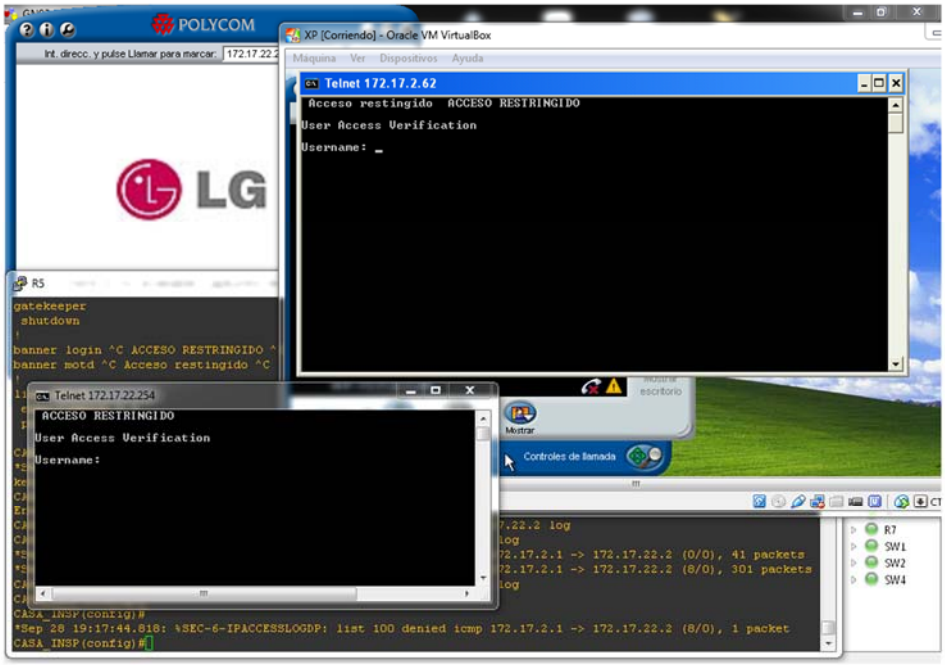
Figura 61. ACL denegado ssh desde la sucursal hacia la matriz GNS3




Elaborado por: Leonardo Suárez.

En la figura 61, se encuentran configuradas ACL por lo que se visualiza se encuentra denegado en protocolo ssh, ya que se encuentra habilitado el protocolo ssh para obtener una intercomunicación efectiva y claves encriptadas para el acceso de administración de dispositivos.

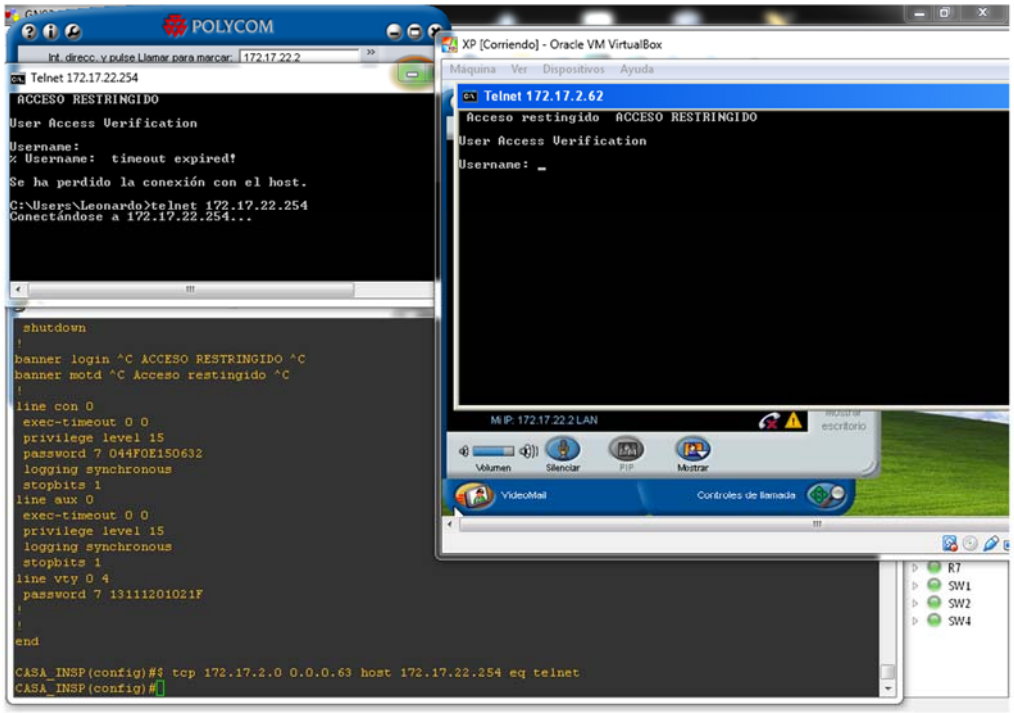
Figura 62. ACL permitido ssh desde la sucursal hacia la matriz GNS3




Elaborado por: Leonardo Suárez.

En la figura 62, se encuentran configuradas ACL por lo que se encuentra permitido el protocolo telnet y ssh, para administracion de dispositivos tanto en la matriz como en las sucursales.

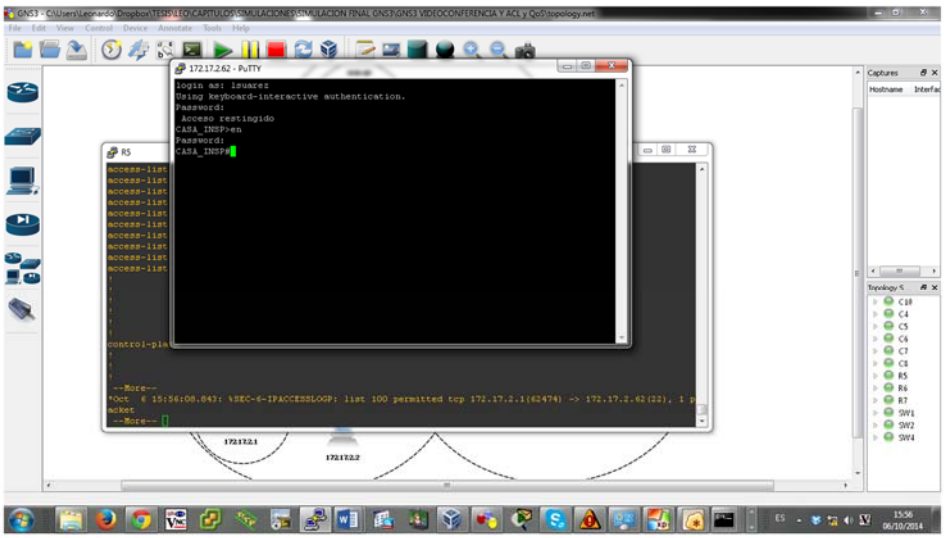
Figura 63. ACL denegado ssh para la matriz y permitida para la sucursal GNS3




Elaborado por: Leonardo Suárez.

En la figura 63, se encuentran configuradas ACL por lo que se visualiza, se encuentra denegado para una red de la matriz y permitida para la red de la sucursal el protocolo ssh.

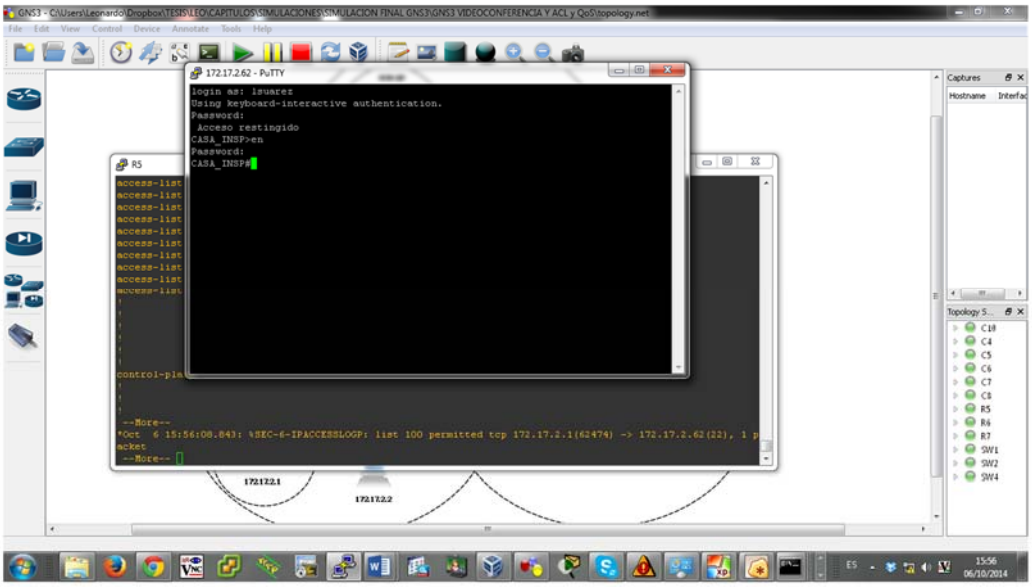
Figura 64. ACL permitido ssh para administración de equipos GNS3




Elaborado por: Leonardo Suárez.

En la figura 64, está habilitado el protocolo ssh para administrar los equipos de la matriz como en las sucursales, como se muestra a continuación.

Figura 65. ACL permitido ssh para administración de equipos GNS3

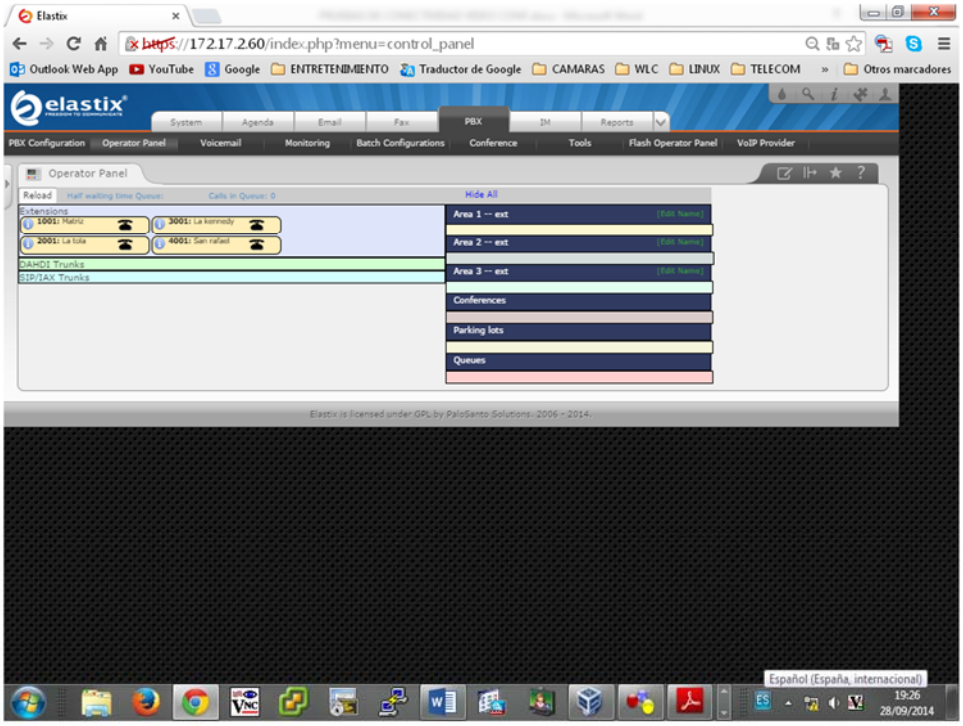



Elaborado por: Leonardo Suárez.

A continuación en la figura 65, se muestra la administración de equipos por medio de ssh habilitada en los equipos de frontera, tanto en router como a nivel de switch.

Se realiza una comparación entre el call manager de cisco y una herramienta montada en software libre la cual es Elastix, por lo que se simuló que el software no tiene algunas de las características y ventajas de call manager de Cisco.

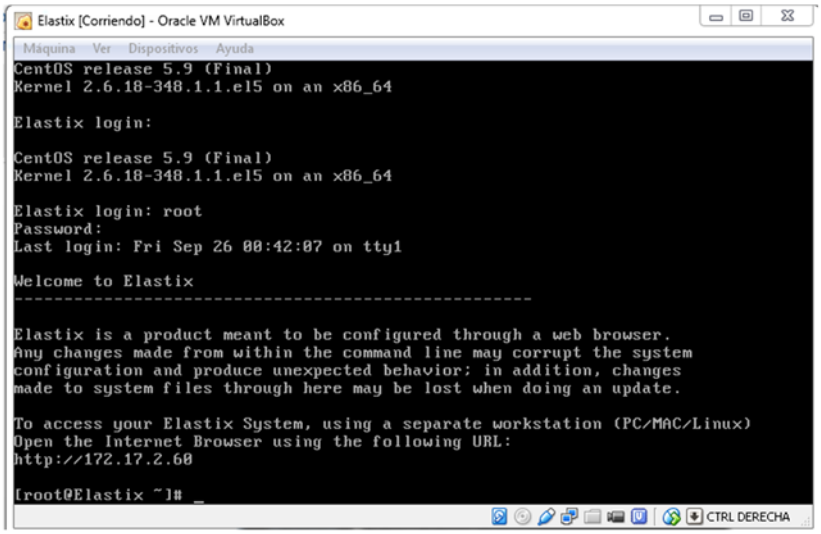
Figura 66. Call manager Elastix




Elaborado por: Leonardo Suárez.

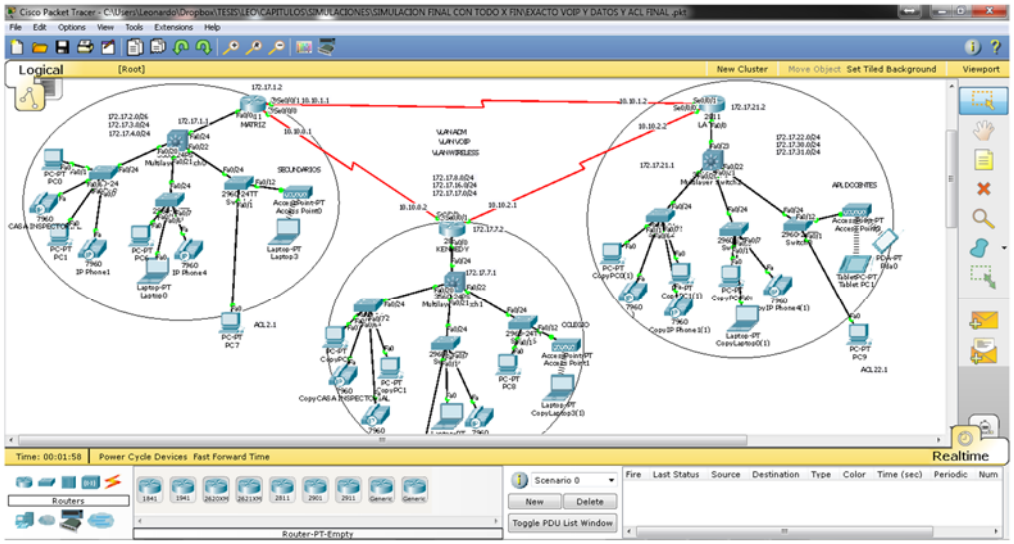
A continuación se presenta el servidor de software Elastix montada en una máquina virtual, la cual simula una CME en software libre.

Figura 67. Servidor de call manager Elastix




Elaborado por: Leonardo Suárez.

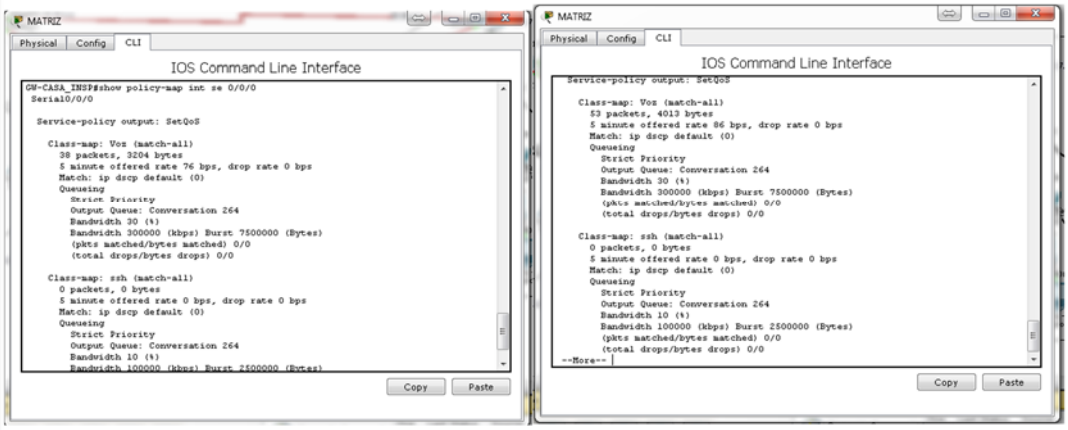
Figura 68. Simulación de telefonía y datos Packet Tracer




Elaborado por: Leonardo Suárez.

En la figura 68, se utilizó la herramienta packet tracer para simular VoIP y datos, en lo que se muestra a continuación.

Figura 69. Resultados de la simulación de QoS de VoIP y datos Packet Tracer.




Elaborado por: Leonardo Suárez.

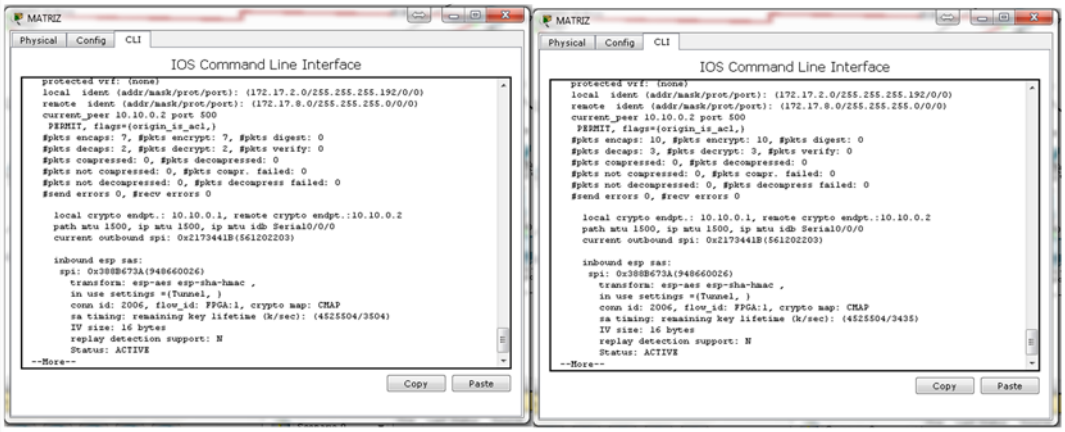
En la figura 69, se muestra las respectivas pruebas que se realizó para garantizar QoS concerniente a VoIP, en lo que se constató que se encuentra garantizado QoS con una prioridad del 30% para telefonía.

Figura 70. Resultados de la simulación de telefonía Packet Tracer.


Elaborado por: Leonardo Suárez.

En la figura 70, se muestra las respectivas pruebas en cuanto a telefonía, por lo que se obtuvo la comunicación entre la matriz y la sucursal.

Figura 71. Resultados de la simulación de encriptación de paquetes VPN.




Elaborado por: Leonardo Suárez.

En la figura 71, se muestra las respectivas pruebas que se realizó para las VPN, en lo que se constató que se encuentra en funcionamiento, como se muestra a continuación la encriptación de paquetes va aumentando, para acceder de la sucursal hacia la matriz y viceversa.

En este capítulo se realizó la etapa de diseño tanto lógico como físico, además de las configuraciones de cada dispositivo, en la que demuestra las pruebas y resultados, en lo que se constató la eficiencia en los enlaces, cada una de esas configuradas QoS, telefonía, datos y VPN como se muestran en las figuras anteriores.

# CONCLUSIONES

- El modelo jerárquico que se optó para el diseño expuesto, fue por eficiencia y escalabilidad en cuanto a la marca Cisco, ya que estos equipos cumplen con requerimientos necesarios según los estudios realizados, para la intercomunicación entre la matriz y las diferentes sucursales.

- A partir de los análisis y requerimientos de la matriz como sus obras, se logró identificar la demanda de usuarios para las diferentes aplicaciones, como el ancho de banda para la matriz y las obras. En la que se constata que el ancho de banda adquirido no es suficiente, tanto la matriz como en las sucursales.

- El número de usuarios en las sucursales es alrededor de 200 – 250, mientras que en la matriz son 80 – 100 usuarios. Por lo que afecta el ancho de banda establecido en cada una de las obras, y el no tener segmentada las diferentes redes, ya que los laboratorios se consumen todo el ancho de banda de la obra. Por lo que se optó generar un nuevo plan IP y establecer de acuerdo a sus necesidades.

- Se debe tomar en cuenta el ancho de banda para los enlaces, para garantizar las diferentes aplicaciones simuladas, en las cuales son VoIP y videoconferencia. Ya que al no tener un buen ancho de banda tendrían algunas consecuencias, tales como saturación y pérdidas en el enlace.

- Al realizar el diseño se pudo abarcar con las necesidades tanto de la matriz como de cada obra, para tener una comunicación eficaz, transparente y confiable. Se verifico estos requerimientos con la configuración de QoS, en la cual se garantiza un cierto porcentaje para VoIP y video.

- Este diseño que se planteó es una de las soluciones para la intercomunicación entre la matriz y sus obras, en lo que se refiere a VoIP y videoconferencia, además de costo beneficio para la Casa Inspectorial Salesiana.

- Este diseño está enfocado a la disponibilidad, eficiencia y escalabilidad; ya que los equipos diseñados, son equipos de tercera generación, en la cual son dispositivos escalables, además que se pueden partir de estos para otro proyecto.

- Los equipos que se escogieron para este diseño son de gran escalabilidad y confiables, ya que con estos dispositivos se obtendrá calidad de servicio en cuanto a VoIP y videoconferencia. Ya que soportan módulos PDVM3.

## RECOMENDACIONES

- Se debe tomar en cuenta el ancho de banda tanto para la matriz como sus obras, para que tengan una intercomunicación eficaz, y que no se saturen los enlaces en las aplicaciones diseñadas.

- Se debe aumentar el ancho de banda según el estudio analizado y dependiendo de los diferentes dominios de broadcast que se generaron tanto para la matriz como para las sucursales.

- El diseño que se va a implementar a futuro se tiene que basar en el direccionamiento explicito, y originado en este proyecto.

- Los enlaces ya sean por líneas arrendadas o enlaces P2P se recomienda tener un ancho de banda por cada enlace para garantizar una óptima intercomunicación para las diferentes y futuras aplicaciones diseñadas.

- Los equipos que fueron tomados para el diseño son equipos escalables, no pueden ser sustituidos ni reemplazados, se parten de estos dispositivos implementados, ya que fue una de las ventajas para el diseño explícito.

- Este diseño se debe tomar como base para futuras aplicaciones, en las cuales se debe hacer un análisis y estudio para el incremento del ancho de banda, tanto en la matriz como en las sucursales, dependiendo la demanda de usuarios.

## LISTA DE REFERENCIAS


Aboutabi, M. (2003). *Internet Group Management Protocol (IGMP).* The McGraw-Hill.

Ariganello, E. (06 de 09 de 2006). *Seguridad Informática* . Obtenido de Seguridad Informática : http://aprenderedes.com/2006/09/protocolo-cdp/

Atelin, P., & Dordoigne, J. (2007). *TCP/IP y protocolos de Internet.* ENI.

Bruno, A., & Jordan, S. (17 de Diciembre de 2013). *CCDA 640-864 Official Cert Guide.* Obtenido de http://cisco.donntu.edu.ua/materials/640-864-ccda.pdf

Debish. (19 de 03 de 2012). *Puertos y firewalls (básico).* Obtenido de Puertos y firewalls (básico): http://www.debianhackers.net/de-puertos-y-firewalls-basico

Dominguez Ayala, J. C., & Chicaiza Iza, O. P. (2008). *Análisis Y Diseño Técnico Económico De La Red De Interconexion De Las Redes En Los Campus Girón, Sur, Kennedy Y Cayambe De La Universidad Politécnica Salesiana Sede Quito.* Quito: Universidad Politecnica Salesiana.

ferre, L. (16 de 04 de 2010). *Proveedor_de_servicios_de_Internet*. Obtenido de Proveedor_de_servicios_de_Internet: http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet#mediaviewer/Archivo:Internet_Connectivity_Access_layer.svg

Galvez, A. E. (28 de 08 de 2013). *Wikilibros*. Obtenido de Wikilibros: http://es.wikibooks.org/wiki/DNS_en_BIND

Jean, S. (11 de 03 de 2011). *Zona Desmilitarizada*. Obtenido de Zona Desmilitarizada: http://es.scribd.com/doc/51730104/DMZ-Zona-desmilitarizada

Ji, X. (09 de 2007). *INTRUSION PREVENTION SYSTEMS: Network Based IPS (NIPS).* Obtenido de INTRUSION PREVENTION SYSTEMS: Network Based IPS (NIPS): http://www.foursquaretraining.co.uk/software_development_and_ebusiness_articles/intrusion_prevention_systems_5.html

Magliano, W. (09 de 04 de 2014). *Walter's Blog*. Obtenido de Walter's Blog: http://wmagliano.wordpress.com/2008/09/27/diseno-de-redes-capitulo-1-ppdioo/

Mühlböck, H. (11 de 05 de 2011). *Red de área amplia*. Obtenido de Red de área amplia: http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia#mediaviewer/Archivo:LAN_WAN_scheme.svg

Nadimi, A. (28 de 07 de 2009). *Enterprise Internet Edge Design Guide*. Obtenido de Enterprise Internet Edge Design Guide: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/IE_DG.html#wp102105

Occhiogrosso, S. (09 de Mayo de 2009). *Took the CCDA Exam 640-863.* Obtenido de http://ccie-or-null.net/2011/05/09/the-cisco-ppdioo-life-cycle/

Prado, R. (11 de 07 de 2011). *CALIDAD DE SERVICIO para enlaces WAN usando MQC*. Obtenido de CALIDAD DE SERVICIO para enlaces WAN usando MQC: https://supportforums.cisco.com/es/document/68116

*Red de área amplia WAN*. (03 de 06 de 2014). Obtenido de Red de área amplia WAN: http://www.librosvivos.net/smtc/PagPorFormulario.asp?TemaClave=1039&est=0

*Seguridad VPN*. (11 de 08 de 2014). Obtenido de Seguridad VPN: http://www.cisco.com/web/ES/solutions/es/vpn/index.html

*Seguridad y Redes*. (2010). Obtenido de Seguridad y Redes: http://www.silcom.com.pe/soluciones_seguridad_redes.html

*Sifra consultores, S.A de C.V*. (09 de 04 de 2014). Obtenido de Sifra consultores, S.A de C.V: http://www.sifra.net.mx/metodolog%C3%ADa/ppdioo.aspx