FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

REDISEÑO DE UNA RED LOCAL MULTISERVICIOS PARA EL EDIFICIO MATRIZ DE LA CONAFIPS

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía

Ing. José Julio Freire Cabrera

Autor

Armando Andrés Quilumba Chushig

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación"

_____

Ing. José Julio Freire Cabrera

CC: 170973145-7

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Armando Andrés Quilumba Chushig

CC: 172237377-4

AGRADECIMIENTOS

Un especial agradecimiento para mi padre y mi madre de quienes he recibido un apoyo incondicional para alcanzar todas mis metas, propósitos y objetivos en toda mi trayectoria personal, académica y profesional, con la esperanza de poder retribuir de la misma manera todo su apoyo a tiempo.

AL Dr. Homero Viteri y a los funcionarios del departamento de las TIC's de la CONAFIPS por las facilidades brindadas para la realización del presente trabajo.

En general a todos las compañeros, amigos y ciertos jefes/as de mi trayectoria laboral y académica con gran calidad humana quienes contribuyeron de manera directa e indirecta en hacer realidad este propósito.

Andrés Quilumba

RESUMEN

El presente trabajo está orientado a resolver la individualidad de los sistemas de telecomunicaciones para cada servicio suministrado dentro de un edificio comercial a través redes de telecomunicaciones independientes generando costos innecesarios. La red multiservicios desarrollada en este trabajo solventa estas desventajas mediante integración de distintos servicios de telecomunicaciones vitales para alcanzar la misión, visión y objetivos de la CONAFIPS. Los principales servicios que maneja esta red multiservicios son voz, video, datos, vigilancia, videoconferencia y seguridad contra incendios sobre una misma infraestructura. Finalmente, el diseño desarrollado está en capacidad de soportar exigencias actuales y futuras garantizando escalabilidad, disponibilidad, rendimiento, seguridad, facilidad de administración y mantenimiento.

ABSTRACT

This work is aimed at resolving the individuality of telecommunications systems for each service provided within a commercial building through independent telecommunications networks generating unnecessary costs. The multiservice network developed in this paper overcomes these disadvantages by integrating different services vital telecommunications industry to achieve the mission, vision and goals of the CONAFIPS. The main services are multi-service network handles this voice, video, data, security, and fire safety video on the same infrastructure. Finally, the design developed is able to withstand current and future requirements ensuring scalability, availability, performance, security, ease of management and maintenance.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las comunicaciones desde tiempos inmemoriales han sido de vital importancia para el desarrollo de los pueblos y desde entonces han evolucionado de manera sorprendente hasta el día de hoy. En la actualidad las comunicaciones continúan siendo de gran importancia para las personas y las organizaciones, generando nuevas necesidades de comunicación para desarrollo de las actividades cotidianas comerciales.

En tal virtud, se han desarrollado múltiples sistemas de telecomunicaciones que buscan satisfacer las necesidades actuales de comunicaciones individuales y organizacionales. Dichos sistemas han evolucionado de manera difusa cada una con su propia tecnología, generando una necesidad de adquirir un nuevo sistema por cada servicio que sea requerido para el progreso de una organización.

La propuesta del presente trabajo pretende resolver estas limitaciones a través de la inclusión de todos los servicios de telecomunicaciones vitales para las actividades diarias de una organización comercial, a través de una red multiservicio que unifica varios servicios principalmente la voz, video, datos, vigilancia, videoconferencia, seguridad contra incendios sobre una misma infraestructura.

Finalmente, la red multiservicios deberá tener la capacidad de soportar requerimientos actuales y futuros mediante una arquitectura que garantice escalabilidad, seguridad, disponibilidad, rendimiento, administrabilidad y facilidad de mantenimiento.

1. Capítulo I. Redes Multiservicio

1.1. Conceptos fundamentales

La forma tradicional de disponer redes individuales para brindar soporte a cada servicio de comunicación está siendo cada vez más desplazada debido a la evolución tecnológica de las comunicaciones. Un claro ejemplo son las arquitecturas de redes desarrolladas sobre una plataforma multiservicios basado en características como el alto rendimiento y calidad de servicios (QoS) con la finalidad de obtener la convergencia de las redes (Unipanamericana, 2012).

Los servicios multimedia cada vez se hacen más necesarios en la vida cotidiana de los usuarios. Es decir que la demanda de los usuarios en cuanto a los servicios va en aumento obligando el desarrollo de la tecnología para satisfacer sus necesidades. A través de las redes multiservicios es posible la integración de varios servicios de telecomunicaciones sobre una misma infraestructura, lo cual permite aprovechar los distintos recursos de red para satisfacer las necesidades de comunicación de los usuarios y la implementación de diversos sistemas de comunicación como se muestra en la **Figura 1** (Sanmartín, 2009, p. 7).

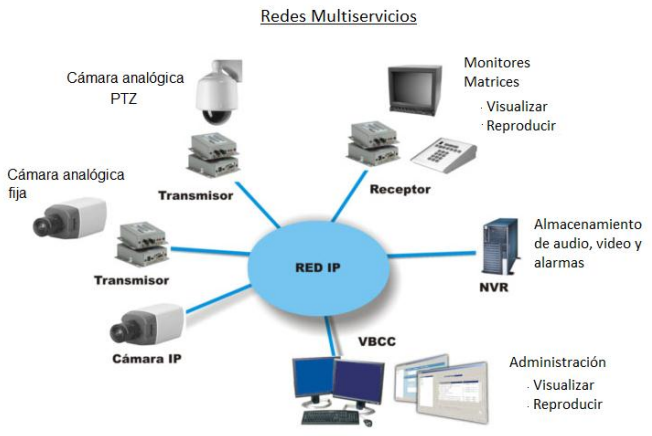


Figura 1.- Esquema general de una red multiservicios.

Las redes multiservicios son ideales para cualquier empresa debido a la excelente relación costo beneficio, ya que brinda la capacidad suministrar servicios de calidad a los usuarios sobre una misma infraestructura, además de facilidades de administración y mantenimiento de la red.

1.2. Características generales

1.2.1. Seguridad de datos

Las redes multiservicios manejan grandes volúmenes de datos y servicios críticos con múltiples accesos desde distintas estaciones de trabajo. Debido a estas razones todo el tráfico debe ser autenticado, autorizado y protegido de un extremo a otro mediante mecanismos de seguridad. Estos mecanismos están encargados de proteger los paquetes que se generan desde un equipo fuente y prevenir de accesos no autorizados o ataques como la falsificación de la dirección fuente, lectura o modificación de mensajes dirigidos a los destinatarios, acceso a servicios no autorizados, captura y reproducción de mensajes legítimos, entre otros (Unipanamericana, 2012).

Los problemas de seguridad en las redes se pueden clasificar de forma general dentro de las siguientes dimensiones: control de acceso, autenticación, confidencialidad, disponibilidad, no repudio y control de integridad que se explican brevemente a continuación (Tanenbaum & Wetherall, 2012, p. 658):

Control de Acceso.- Mecanismo que determina los usuarios que tienen acceso a sistemas específicos y recursos en un momento determinado (Turmero, 2010).

Autenticación.- Es el mecanismo encargado de verificar y determinar la identidad de los usuarios mediante claves o credenciales que presente el usuario antes de establecer la comunicación para facilitar información confidencial (Tanenbaum & Wetherall, 2012, p. 658).

Confidencialidad.- Denominada también como secrecía que significa mantener la información fuera del alcance de los usuarios no autorizados. En

otras palabras, garantizar que la información que circula por la red sea visible sólo para usuarios autorizados (Tanenbaum & Wetherall, 2012, p. 658).

Disponibilidad.- Mecanismo que asegura que los usuarios autorizados tengan acceso a los datos y recursos en el momento que lo requieran (López, 2014).

No repudio.- Su función es la de gestionar firmas proporcionando pruebas de integridad y origen de los datos (Tanenbaum & Wetherall, 2012, p. 658).

Control de la integridad.- Se refiere a la forma de asegurar que un mensaje recibido es realmente el que se envió y no ha sido alterado por algún adversario malicioso en el trayecto (Tanenbaum & Wetherall, 2012, p. 658).

La seguridad no está en un sólo lugar o integrada en una sola capa, debe considerarse que la seguridad se encuentra inmersa dentro de cada una de las capas del modelo OSI (Tanenbaum & Wetherall, 2012, p. 659).

Así, en la *capa física* se puede proteger contra la intervención de los medios de transmisión. Por ejemplo, Algunos sistemas militares poseen tubos sellados que contienen un gas inerte a alta presión, cualquier intento de abrir la tubería habrá fuga del gas que activará la alarma debido a disminución de la presión. Por otra parte está el medio inalámbrico que requiere mecanismos robustos de seguridad y más complejos como el estándar IEEE 802.11i (Tanenbaum & Wetherall, 2012, p. 658) (CCM Benmarch Group, 2015).

En la *capa de enlace de datos.*- Los paquetes de un enlace punto a punto pueden ser encriptados cuando se envía desde una máquina y desencriptar al llegar al destino, sin la necesidad de que el resto de capas intervengan. Sin embargo, el problema se presenta al atravesar varios routers, los cuales deben desencriptar los paquetes, haciéndolos vulnerables a posibles ataques. La encriptación de enlace (link encryption) puede ser implementada en enlaces punto a punto. Los algoritmos más comunes de encriptación utilizados son Triple DES (Data Encription Standart), AES (Advanced encription Standard) en sus variantes de 128, 192, 256 bits para protocolos como PPP (Point to Point Protocol) y VPN de esta capa (Thales Security, 2015) (Cura, 2007).

En la *capa de red,* se pueden implementar firewalls para mantener los paquetes seguros e impedir el ingreso de paquetes maliciosos. En esta capa también trabaja la seguridad IP denominado IPSec que se describe en RFC 2401 como un conjunto de protocolos que aseguran comunicaciones sobre IP mediante la encriptación de cada paquete de un flujo de datos (Tanenbaum & Wetherall, 2012, p. 659).

En la *capa de transporte,* se puede encriptar conexiones enteras de un extremo a otro o de proceso a proceso. Los protocolos de negociación comunes en esta capa son SSL (Secure Socket Layer) y TLS (Transport Layer Secure) que realizan la autenticación del servidor por el cliente, mantienen una comunicación secreta y garantizan la integridad de los datos (Vilajosana, Font, Llorente, & Marqués, 2010, pp. 50-53).

Por último, los mecanismos como la autenticación y el no repudio de usuarios sólo pueden ser garantizados en la *capa de aplicación*. La seguridad en la capa de aplicación de todas las comunicaciones entre el cliente y el servidor están garantizadas mediante protocolos como HTTP y HTTPS (Hypertext Transfer Protocol Secure) (Tanenbaum & Wetherall, 2012, p. 659).

1.2.2. Calidad de servicios QoS

La red multiservicios tiene la particularidad de asignar prioridades a los diferentes servicios y garantizar la entrega eficiente de las aplicaciones en tiempo real como el tráfico de voz y video. También puede ofrecer una amplia gama de funciones de QoS como la limitación de retardos y reserva de ancho de banda, a través de la diferenciación de los distintos servicios y la selección de la ruta óptima mediante modelos de implementación de QoS que se analizan detalladamente a continuación en la sección de modelos de implementación de QoS.

1.3. Modelos de Implementación de QoS

Una red puede ofrecer servicios de calidad cuando garantiza el valor de uno o varios parámetros que lo definen. Para ello existen tres modelos de

implementación de QoS sobre las redes, Best-Effort, IntServ y DiffServ que ofrecen un determinado nivel de calidad definidos a continuación (García, 2007, p. 6).

1.3.1. Mejor esfuerzo (Best-Effort)

Este es el modelo más simple de implementación de QoS, en el cual una aplicación envía información en cualquier instante, en cualquier cantidad, sin ningún permiso y sin notificar previamente a la red. Es decir que en este modelo sencillamente no se garantiza calidad de servicio debido a que no asegura una tasa de transferencia, retraso o fiabilidad. Funciona de manera similar al modelo de cola FIFO para sus transmisiones. TCP/IP fue desarrollado para ofrecer este tipo de servicio. Este modelo es empleado para aplicaciones que no sean sensibles al tiempo como la navegación en páginas web (Vilajosana, Font, Llorente, & Marqués, 2010, p. 51).

1.3.2. Servicios integrados (InterServ)

Es un modelo de implementación de QoS definido por la IETF en 1994. En este modelo es de gran importancia el concepto de flujo, el cual está definido como el tráfico mínimo unidireccional constante de paquetes secuenciales generados por una petición realizada por el usuario y que además requiere de un mismo nivel de calidad de servicios, que puede ser asignada de manera determinada (García, 2007, p. 29).

En IPv4 el flujo se puede identificar según las direcciones y puertos de origen-destino, además del protocolo empleado como TCP o UDP. El direccionamiento IPv6 también permite identificar a través de los mismos parámetros y mediante el contenido de campo *Etiqueta de Flujo* del encabezado como se muestra en la **Figura 2** (García, 2007, p. 30).

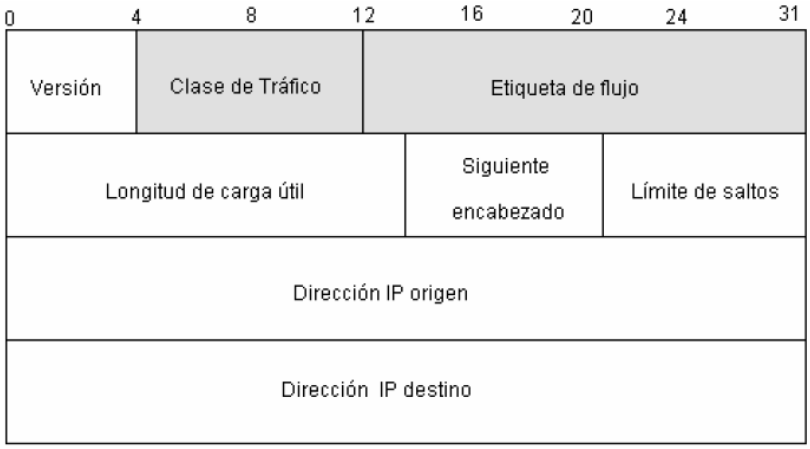


Figura 2.- Encabezado de IPv6.

En este modelo IntServ están definidos tres tipos de servicios (García, 2007).

- *Mejor Esfuerzo.*- No brinda prioridades, es decir no garantiza calidad de servicios.
- *Carga Controlada*.- Puede brindar una calidad de servicios similar a una red de datos con poca carga, proporcionando tiempos de respuesta aceptables, pero de manera eventual puede presentar grandes demoras.
- *Garantizado.*- A través de este servicio es posible garantizar un flujo mínimo y un retardo máximo. En ciertas ocasiones esto no es posible debido a las características del medio físico.

El modelo IntServ cuenta con el protocolo RSVP (Resourse Reservation Protocol) encargado de la señalización y reservación de los recursos necesarios para facilitar los flujos de datagramas por la red y así brindar un nivel garantizado de QoS a las distintas aplicaciones, negociando de punto a punto parámetros de red (García, 2007, p. 30).

La aplicación solicita un determinado nivel de servicio requerido para poder operar adecuadamente, de esta manera se reservan recursos necesarios de red para que pueda comenzar a operar una aplicación. Dichos recursos se mantendrán reservados hasta que finalice la aplicación o hasta que el ancho de

banda empleado por dicha aplicación exceda los recursos reservados como se muestra en la **Figura 3** (García, 2007, p. 31).

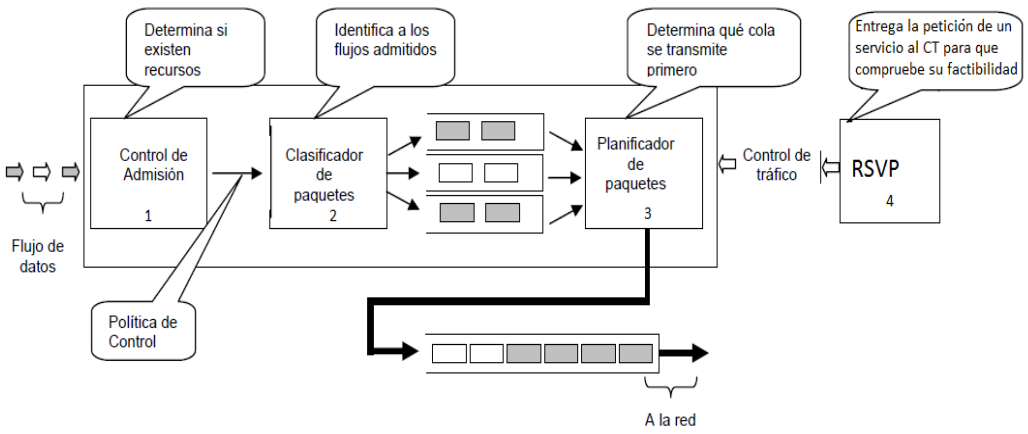


Figura 3.- Componentes de la arquitectura Inter Serv.

En la **Figura 3** RSVP entrega la petición de una aplicación o servicio al control del tráfico (CT) de cada router. El control de admisión determina si dispone de recursos suficientes para brindar la calidad solicitada por el servicio. El clasificador de paquetes identifica los flujos que se admiten. Por último, el planificador determina el orden de transmisión de los flujos (García, 2007, p. 33).

1.3.2.1. Protocolo RSVP (Protocolo de Reservación de Recursos)

RSVP es un protocolo orientado a conexión desarrollado por la IETF en 1990 y está situado en la capa de transporte. Define un método de asignaciones de calidad de servicios donde los receptores tienen la responsabilidad de seleccionar un adecuado nivel de reserva de recursos, iniciando y manteniéndolo activo durante el tiempo requerido. Está orientado a operar en conjunto con protocolos de enrutamiento, sin ser uno de ellos. Dentro de las tecnologías desarrolladas para brindar QoS, esta es una de mayor complejidad (García, 2007, p. 31).

1.3.2.2. Características del protocolo RSVP

RSVP posee las características señaladas a continuación (García, 2007, p. 34):

- Efectúa reservaciones de recursos de red para servicios unicast y multicast, acoplando de forma dinámica a los cambios de rutas y miembros.
- Realiza reservaciones para flujos unidireccionales de datos.
- Transporta y mantiene de forma transparente parámetros de control de tráfico.
- Brinda diversos modelos de reservación de recursos para acoplarse a una gama de servicios o aplicaciones.
- Opera de manera transparente sobre los routers que no brinden soporte a este protocolo.
- Es soportada por las dos versiones de IP.

1.3.2.3. Ventajas y desventajas de IntServ

A continuación se denotan algunas ventajas y desventajas del presente modelo de QoS (García, 2007, p. 42).

Ventajas:

- Facilita la unificación con la gestión de políticas de rendimiento de red gracias a la simplicidad conceptual.
- Calidad de servicio discreta por flujo. Permite notificar a los extremos la disponibilidad de ancho de banda requerido.

Desventajas:

- Escalabilidad baja.- Debido al crecimiento lineal del costo de la implementación del modelo y el tamaño de la red.
- Es orientado a conexión.- Provocando que los ruteadores almacenen información sobre los flujos activos manejados.
- Los informes sobre los estados pueden ser fácilmente admitidos en los ruteadores extremos de la red, pero es costoso y complicado en los

ruteadores intermedios, los cuales deben manejar cientos de enlaces activos.

- En recientes versiones no cuentan con componentes de seguridad para evitar que los servicios san robados, además no cuentan con políticas de control de autenticación y autorización para los usuarios y aplicaciones.
- Todos los componentes de red intercambian y mantienen mensajes sobre el estado y señalización de cada flujo de datos, generando como resultado un considerable ancho de banda en redes de gran tamaño.
- Emplean mensajes periódicos de notificación para mantener las sesiones activas y proteger frente a la pérdida de los paquetes.

Debido a las múltiples desventajas frente a los escasos beneficios que ofrece el modelo de calidad IntServ la IETF ha creado un nuevo modelo optimizado para evitar estos problemas, el cual se denomina DiffServ.

1.3.3. Servicios diferenciados (DiffServ)

DiffServ es un modelo desarrollado por la IETF en 1998 (IETF, 1998) y se ha considerado como uno de los mejores modelos para proporcionar QoS en grandes redes. Su misión es garantizar una mejor calidad de servicio en redes de convergentes, junto a la facilidad de implementación a un bajo costo debido a que no será necesario realizar cambios significativos en la infraestructura de redes actuales. DiffServ está compuesto por un grupo de tecnologías a través de las cuales es posible ofrecer múltiples niveles de calidad de servicios para los distintos servicios y tráfico de datos. En este modelo el tráfico es dividido en diferentes clases a los cuales se les asigna un nivel de prioridad, haciendo de este un proceso que distingue diversos tipos de paquetes IP en los routers (García, 2007, pp. 7-8).

DiffServ es un modelo que contribuye a la estabilidad de la red y al despliegue, por lo tanto no es necesario que este modelo esté implementado en todos los nodos de la red. Gracias al marcado de paquetes que se realiza es posible que aquellos paquetes pertenecientes a una misma clase reciban un tratamiento

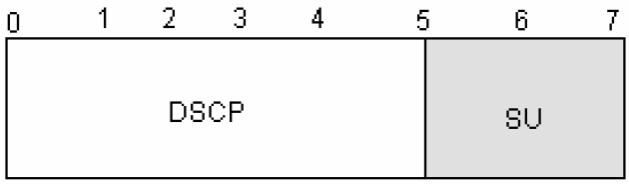
similar en la red. Es decir, si a una clase se le asigna una mayor prioridad o ancho de banda los paquetes de esta clase recibirán un mejor tratamiento en la red.

1.3.3.1. Campos para gestión de QoS en IPv4 e IPv6

En esta arquitectura DiffServ la clasificación de los paquetes se lleva a cabo en los dispositivos o nodos de acceso a la red especificando el contenido en el campo DS (Servicio Diferenciado). Una vez que han ingresado los paquetes el procesamiento dependerá del valor del encabezado IP en su campo DS. En IPv4 el marcado de los paquetes es a través del byte ToS (Tipo de Servicio), y en IPv6 se realiza el marcado mediante el campo TC (Clase de Tráfico). En las dos versiones se utiliza este campo como byte DS (García, 2007, p. 9).

1.3.3.2. Campo (DS) Servicio Diferencial

Para realizar la distinción de los servicios se ha especificado un campo que reemplaza los conceptos de campo ToS en IPv4 y el TC en IPv6, al cual se denomina DS que está compuesto por 8 bits como se muestra en la **Figura 4**, de los cuales los 6 primeros se utilizan como parte del código y los 2 bits restantes no deben ser tomados en cuenta por los nodos que trabajen con DiffServ (García, 2007, pp. 13-14).



D.S.C.P. = Punto de Código de Servicios Diferenciados

S.U. = Sin Uso

Figura 4.- Campo de Servicio Diferenciado.

En el campo DS se realizan asignaciones de prioridades a los paquetes o datagramas en las dos versiones de IP. Gracias a este campo es posible especificar hasta 64 diferentes prioridades de tráfico, sin embargo a nivel de práctica se emplean menos. Cada código definirá un determinado nivel de prioridad, denominado comportamiento PHB (Per Hop Behavior). Existen cuatro PHB definidos para emplear en una red de servicios diferenciados (García, 2007, pp. 15-19).

1. *Default Behavior (BE PHB*).- Equivalente a mejor esfuerzo.
2. *Class Selector (CS PHB).-* Especifica hasta 8 clases diferentes.
3. *Expedited Forwarding (EF PHB).-* Servicio extremo a extremo asegurando bajas pérdidas, retardos, jitter y determinado ancho de banda.
4. *Assured Forwarding (AF PHB).-* Especifica 4 clases, cada una con hasta tres niveles de descartado dependiendo del nivel de congestión.

1.3.3.3. Elementos de la arquitectura DiffServ

La arquitectura DiffServ está compuesta por varios componentes que se describen a continuación y se ilustran en la **Figura 5** (García, 2007, pp. 21-22).

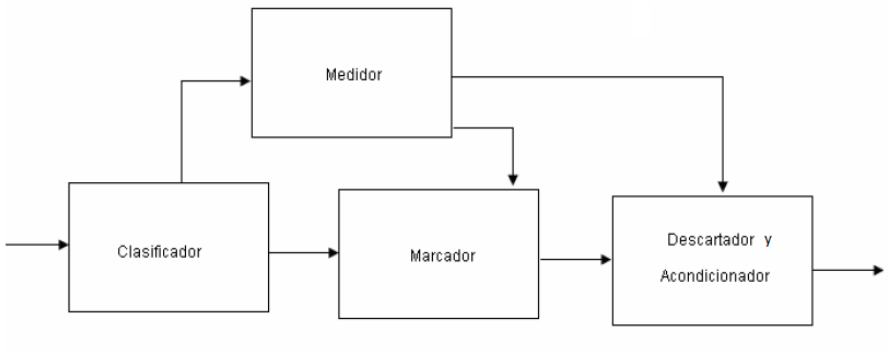


Figura 5.- Arquitectura de DiffServ.

- **Clasificador.-** Guía los paquetes con características similares hacia las siguientes etapas de acondicionamiento de tráfico.
- **Medidor.-** Transfiere información hacia las siguientes funciones de acondicionamiento para definir la acción adecuada para cada paquete.
- **Marcador.-** Marca los paquetes con un determinado código DS para elegir un PHB, conforme a las mediciones del módulo anterior.
- **Acondicionador.-** Descarta los paquetes cuando no dispone espacio suficiente dentro de la cola para mantener el mínimo retardo.
- **Descartador.-** Descarta paquetes con el objetivo de evitar congestionamiento y cumplir con los requerimientos configurados dentro del perfil de tráfico.

1.3.3.4. Ventajas y desventajas de los DiffServ

A continuación se resumen las ventajas y desventajas que caracterizan a este modelo de calidad de servicios (García, 2007, p. 27).

Ventajas

- **Escalabilidad.-** Facilita el soporte escalable para flujos de datos y voz sobre una misma infraestructura.
- **Funcionamiento.-** Para realizar la clasificación los paquetes son examinados una sola vez e inmediatamente marcados y todas las posteriores decisiones de QoS son realizadas conforme al valor de un campo fijo de la cabecera del paquete IP, disminuyendo requerimientos de procesamiento.
- **Flexibilidad.-** Tiene la capacidad para establecer muchos tipos de tráfico.
- **Señalización sencilla-** La señalización es más simple que el protocolo RSVP.
- **Costos reducidos.-** DiffServ representa reducción de costos de gestión.

Desventajas

- No existen reservaciones de ancho de banda de extremo a extremo, es decir que las garantías de servicios pueden ser indiferentes en aquellos nodos de red que no estén implementados adecuadamente los PHB en enlaces de congestión o diseñados de forma inadecuada para el volumen de tráfico que soportará de una determinada clase.

1.4. Aplicaciones soportadas y sus requerimientos en redes multiservicio

Existen varias aplicaciones en general que puede soportar una red multiservicios; por citar algunas, de las más importantes tenemos: Telefonía IP basada en tecnología VoIP, streaming de medios almacenados, streaming de medios en vivo, videoconferencias, video vigilancia, seguridad contra incendios, entre otros (Tanenbaum & Wetherall, 2012, p. 601).

Los requerimientos para este tipo de servicios son similares, debido a que son servicios en tiempo real; es decir, que son sensibles al tiempo, por lo tanto es necesario solventar los siguientes parámetros de red tales como: El tipo de compresión utilizado, la pérdida de paquetes, las demoras, el eco, el jitter, los cuales se explican más adelante en la sección de los parámetros de calidad de voz y video (Edwin, 2009, p. 29).

A continuación se describen brevemente las aplicaciones principales en una red LAN dentro de una organización y se identifican los requerimientos de calidad.

1.4.1. Voz y telefonía sobre IP

La voz sobre protocolo de Internet es la tecnología que permite la transmisión de la voz en paquetes de datos mediante protocolos de comunicación IP. La tecnología VoIP nace con el fin de superar varias limitaciones como los costos que implican las comunicaciones de larga distancia a través de redes independientes como las de telefonía convencional (Edwin, 2009, p. 4).

La telefonía convencional operaba mediante la conmutación de circuitos, la cual requería de un canal permanente para su conexión; esto implicaba un alto consumo de recursos de la red de telefonía tradicional y su vulnerabilidad a las interferencias y crosstalk. La tecnología ToIP (Telefonia sobre IP) ha sido desarrollada de tal forma que hace posible las comunicaciones de voz a través de las redes de datos, mediante la tecnología VoIP. Es decir que el tráfico de voz puede circular por cualquier red IP como una red LAN como se muetra en la **Figura 6**. Esta integración de tecnologías permite varios métodos de comunicaciones cada vez más efectivas y eficientes a través de la red (Edwin, 2009, p. 5).

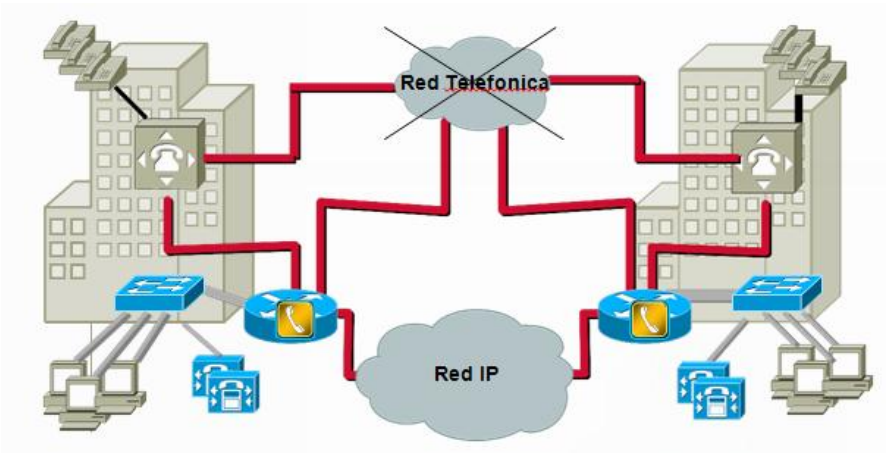


Figura 6.- VoIP en una red empresarial.

Para el establecimiento de las comunicaciones de voz en un sistema de VoIP son necesarios ciertos protocolos de señalización y protocolos de transporte de medios en tiempo real que serán detallados más adelante.

1.4.2. Medios almacenados de flujo continuo (Streaming)

Este caso está presente cuando los medios de flujo continuo como audio y video ya se encuentran almacenados. La manera más sencilla de gestionar medios ya almacenados es no transmitirlos por flujo continuo, pero habría que esperar que se complete la descarga para poder reproducir cualquier medio.

Para resolver esta limitación en esta variante de streaming, el navegador debe envíar una solitud al servidor a través de un protocolo como HTTP (Protocolo de Transferencia de Hipertexto) y este responde enviando un archivo muy corto denominado metadatos[1] usando el mismo protocolo, el cual es entregado al reproductor local de medios y este a su vez envía la solicitud al servidor de medios mediante el protocolo RTSP (Protocolo de Flujo en Tiempo Real) para empezar la descarga. Una vez iniciada la descarga del archivo a través del protocolo TCP (Protocolo de Control de Transmision) o UDP (Protocolo de Datagramas de Usuario) inmediatamente empezará a reproducirse antes de que el medio se haya descargado por completo como se muestra en la **Figura 7** (Tanenbaum & Wetherall, 2012, pp. 612-613).

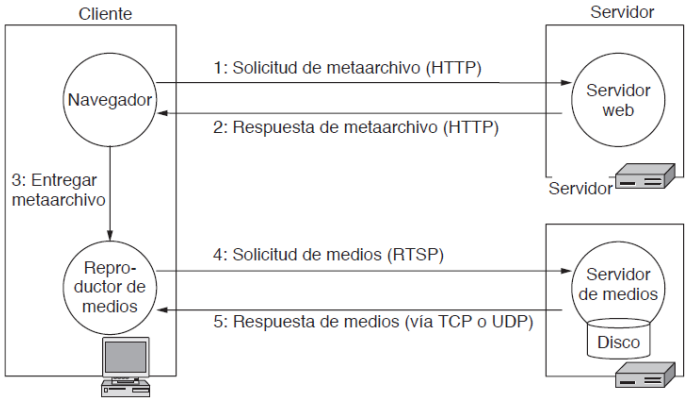


Figura 7.- Transmisión de medios de flujo continuo.

Los protocolos de transporte en tiempo real como el RTSP (Protocolo de Flujo en Tiempo Real) serán detallados más adelante.

[1] Metarchivo.- Es una página vinculada a un determinado medio almacenado. Es un archivo muy corto que sólo proporciona el nombre a un medio.

1.4.3. Transmisión en flujo continuo de medios en vivo

En este esquema el servidor envía cada paquete una sóla vez usando una IP multidifusión a una dirección de grupo. La red entrega una copia del paquete a cada miembro del grupo. Los usuarios que quieren recibir el flujo deben enviar una solicitud al servidor de medios y se unirán al grupo al cual servidor ya se encuentra enviando el flujo continuo en vivo como se muestra en la **Figura 8.** Debido a que la multidifusión es de uno a muchos, los medios se transmiten en paquetes RTP a través de un protocolo de transporte como UDP, el cual no garantiza confiabilidad; es decir, que tal vez algunos paquetes se perderán (Tanenbaum & Wetherall, 2012, pág. 621).

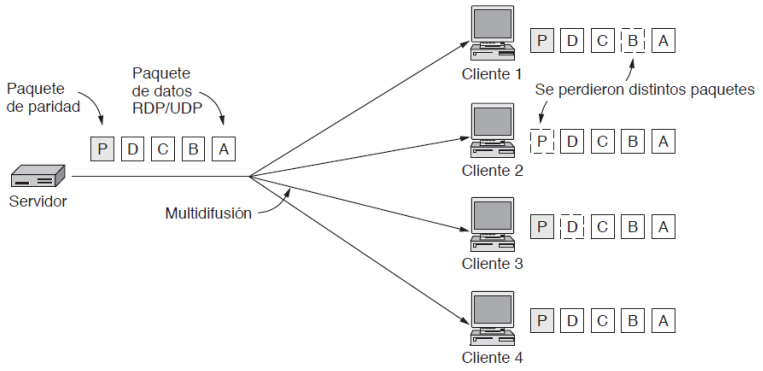


Figura 8.- Multidifusión de medios de flujo continuo en vivo.

1.4.4. Videoconferencia en tiempo real.

Este tipo de flujo posee requerimientos más estrictos en comparación a otros, puesto que requiere de una reducción de latencia adicional. La baja latencia que demanda este servicio es debido a los dos sentidos de comunicación que se maneja en una videoconferencia. La red telefónica posee una latencia en un sentido de comunicación de hasta 150 ms para lograr una calidad aceptable, en llamadas internacionales la latencia es hasta 400 ms, lo cual no es agradable para los usuarios. Por lo tanto, en este tipo de flujo el nivel de latencia tolerable está entre 150 y 200ms para la voz y el video, guardando

sincronía entre ambos para una adecuada apreciación (Haivision, 2012) (Phifer, 2012). Es difícil alcanzar niveles bajos de latencia, pero existen algunas variantes recomendadas como el envío de paquetes cortos y el uso de UDP como protocolo de transporte en lugar de TCP (Tanenbaum & Wetherall, 2012, pp. 623-624).

El codificador y decodificador son componentes que desempeñan un rol fundamental en la implementación de mecanismos para solventar los requerimientos de latencia y jitter de estos flujos.

Los servicios mencionados anteriormente requieren sin duda de modelos que ayuden soportar dichas aplicaciones con QoS, que se explican con detalle en la anterior sección de los modelos de implementación de QoS.

1.5. Protocolos de señalización

Los protocolos de señalización describen mecanismos de control de las comunicaciones de voz y video, que incluyen establecimiento, mantenimiento y finalización. Existen varios protocolos de señalización que poseen funciones similares que se describen a continuación (Millan, 2008).

Los protocolos de señalización más comunes son el IAX (Inter Asterisk Exchange) definido en el RFC-5456, el H.323 desarrollado por la ITU y el SIP del IETF. Todos estos protocolos poseen las mismas tareas básicas como el establecimiento, mantenimiento y finalización de las comunicaciones multimedia a través de señalizaciones propias de cada protocolo (Tanenbaum & Wetherall, 2012, p. 631).

Las tres variantes de señalización pueden trabajar con el protocolo de transporte RTP; es decir, que cualquier protocolo de señalización empleado no influye de manera directa en la calidad de servicios de la comunicación multimedia (VoipForo, 2015).

IAX hace uso de menor ancho de banda en comparación a los dos restantes, debido a que sus mensajes son codificados en forma binaria; en SIP son

mensajes de texto sencillos en su sintaxis y semántica; por último H.323 cuenta con cientos de mensajes codificados en binario (VoipForo, 2015).

La señalización y los datos en IAX se transportan en conjunto, de esta forma se evitan problemas de NAT. En SIP viajan separados, lo cual genera problemas de NAT que pueden ser solucionados con un servidor STUN (Session Traversal Utilities for NAT). En H.323 también se presentan problemas con NAT que pueden ser resueltas mediante el gatekeeper (VoipForo, 2015) (Tanenbaum & Wetherall, 2012, p. 631).

IAX emplea un solo puerto (4569) para el envío de señalización y los datos de todas sus comunicaciones. SIP emplea un puerto para el envío de señalización (5060) y dos puertos por cada comunicación. El H.323 negocia los puertos que se emplearán para: parámetros de llamada, audio, video y RTCP entre cualquiera de los puertos libres de 1024 a 65535 (VoipForo, 2015) (Sáez, 2007, p. 11).

En IAX debido a que la señalización y los datos viajan en conjunto todo el tráfico obligatoriamente pasará por el servidor IAX incrementando el uso de ancho de banda que podría soportar el servidor. En SIP únicamente la señalización pasará por el servidor SIP mientras que los datos de la comunicación pueden viajar de extremo a extremo sin pasar por el servidor SIP. En H.323 el funcionamiento es semejante al SIP (VoipForo, 2015).

Por último, IAX fue diseñado para VoIP y transmisión de video. SIP es de propósito general; es decir, para transmitir cualquier tipo de información además del audio y video. H.323 fue ideado para la transmisión de videoconferencias, pero es más complejo debido a que envía muchos mensajes a la red que pueden ocasionar congestión y tiene limitaciones en comparación a SIP en cuanto a extensibilidad (VoipForo, 2015).

1.6. Transporte de medios

El transporte de medios es el transporte de contenidos multimedia a través de la red de datos, para lo cual es necesario tecnologías que permitan un óptimo

transporte de datos a través de la red, contribuyendo a una mejor calidad de servicios.

Entre las tecnologías que facilitan el transporte de medios están los protocolos de transporte y los códec que se emplean para la transmisión de los datos. Los protocolos de transporte como RTP, RTCP, RTSP son tecnologías que permiten el transporte de medios en tiempo real, procurando al mismo tiempo reducir las demoras y jitter en la red. Los códec por su parte contribuyen a la optimización del tráfico, puesto que muchos de ellos realizan compresión de datos, lo que ayuda a reducir el ancho de banda requerido para su transmisión e influye directamente en la reducción de la congestión y demoras en la red, como se explica a continuación (Tanenbaum & Wetherall, 2012, p. 469).

1.6.1. Protocolo de transporte en tiempo real (RTP)

Este es un protocolo definido por la IETF cuyo funcionamiento básico es multiplexar varios flujos de datos en tiempo real en un solo flujo de paquetes UDP, el cual puede ser enviado a uno o varios destinos. RTP trabaja sobre el protocolo de transporte UDP. El emisor encapsula una determinada cantidad de datos (chunk) dentro de un paquete RTP, que posteriormente se encapsula dentro de un datagrama UDP y por último en un paquete IP para poder viajar. En el receptor se extraen los datos RTP del datagrama UDP y entrega los datos al reproductor local de medios para decodificar y reproducir el contenido. RTP no proporciona ningún trato especial ni garantías especiales sobre la entrega de paquetes a su destinatario; es decir, que los paquetes se pueden perder, retrasar o corromper (Vilajosana, Font, Llorente, & Marqués, 2010, pp. 86-87).

El formato RTP posee varias características que permiten trabajar con multimedia a los receptores, por ejemplo a cada paquete enviado en un flujo RTP se le asigna un número mayor que al predecesor, para poder determinar si falta algún paquete. La retransmisión en RTP no es una opción puesto que podría llegar muy tarde, tampoco tiene mecanismos de confirmación de recepción, ni para solicitar retransmisiones. A continuación en la **Figura 9** se

muestra el encabezado RTP compuesto de tres palabras de 32 bits y eventualmente de algunas extensiones.

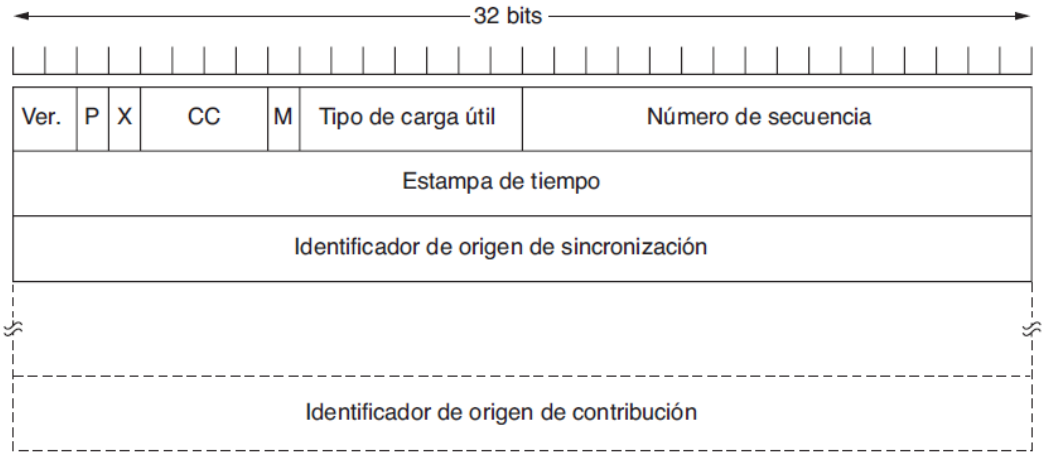


Figura 9.- Formato del encabezado RTP

El campo *Tipo de carga útil* indica el algoritmo de codificación utilizado. La codificación puede cambiar para cada paquete durante la transmisión. El campo *Número de secuencia* es un contador que se incrementa por cada paquete RTP enviado y se utiliza para detectar paquetes perdidos.

La fuente del flujo de transmisión genera la *Estampa de tiempo* para indicar cuándo se creó la primera muestra en el paquete. Este valor ayuda a reducir el jitter en el receptor y permiten que varios flujos estén sincronizados entre sí. El *Identificador de origen de sincronización*, indica a que flujo pertenece cada paquete. Es el método empleado para multiplexar y demultiplexar varios flujos de datos en un sólo flujo de paquetes UDP.

1.6.2. Protocolo de control de transporte en tiempo real (RTCP)

Está definido junto con RTP en el RFC 3550 y se encarga de la retroalimentación, la sincronización y la interfaz del usuario pero no realiza el transporte de medios.

La retroalimentación se puede utilizar para brindar a las fuentes información sobre el retardo, variación en el jitter, ancho de banda, congestión, y otras propiedades de red. Al proporcionar una retroalimentación continua, los algoritmos de codificación y la tasa transmisión de datos se pueden adaptar continuamente con el fin de suministrar la mejor calidad posible bajo las condiciones que se presenten (Tanenbaum & Wetherall, 2012, pp. 471-472).

La sincronización entre los flujos también es manejado por este protocolo para indicar al destino que algoritmo de codificación está siendo utilizado en el paquete actual, para poder modificarlo previo a una solicitud. Distintos flujos pueden manejar distintos relojes, con diferente granularidad. Por último, la interfaz de usuario es una función opcional cuya finalidad es comunicar información de control de sesión; por ejemplo, mostrar la identificación de un participante en la interfaz de usuario (Tanenbaum & Wetherall, 2012, p. 473).

1.6.3. Protocolo de flujo en tiempo real (RTSP)

Este protocolo está definido por la RFC 2326, su finalidad es establecer y controlar uno o varios flujos sincronizados de paquetes multimedia como la voz y el video. Este protocolo no realiza el envío de datos, sino que permite enviar información de control cuando la transmisión de datos está en curso. Es decir que RTSP es un protocolo de control remoto a través de la red para los servidores multimedia (Vilajosana, Font, Llorente, & Marqués, 2010, p. 76).

En este protocolo, en lugar de conexiones, establece y mantienen sesiones con el servidor. Cada una de las sesiones posee su identificador. Una sesión RTSP no se vincula a una sola conexión a nivel de transporte. Es decir, si se mantiene una sesión RTSP, las conexiones o sockets a nivel de transporte pueden ser abiertas o cerradas de acuerdo a la necesidad. El protocolo de transporte puede ser sin conexión como UDP.

1.6.4. Códec

Códec es el acrónimo de codificador y decodificador de flujos de datos multimedia para la transmisión a través de la red. Algunas variantes de códec además de la codificación realizan la compresión de datos, lo cual optimiza el

flujo a través de la red, reduciendo el ancho de banda requerido, el retardo y la congestión en la red como se explica a continuación.

1.6.5. Codecs de voz

La tecnología VoIP requiere que la voz sea digitalizada para el tránsito por la red, para ello es necesario procedimientos que permitan realizar esta función. Los códec son los encargados de codificar y decodificar el flujo o la señal previo a su transmisión describiendo una especificación desarrollada tanto en software como en hardware para dichas funciones. Existen varios tipos de códec como se muestra en la **Tabla 1.** Los dispositivos que conforman un sistema VoIP pueden soportar diferentes tipos de códec, por ello es necesario que se realice una negociación previa entre ellos para seleccionar un determinado códec en común para establecer una llamada (Edwin, 2009, p. 32).

Los códec generalmente proporcionan la funcionalidad de compresión de datos, que puede ser mediante la técnica de supresión de silencios entre otras consideraciones, es decir los silencios de voz no se codifican ni se transmiten lo que implica una optimización en el uso del ancho de banda. A continuación en la **Tabla 1** se muestran los anchos de banda que emplean algunos códec.

Tabla 1.- Ancho de banda de LAN unidireccionales.

Tipo de Códec	Duración de Trama (ms)	Ej. Del tamaño del códec (bytes)	Tamaño de carga útil de voz (bytes)	Paquetes por segundo	Ancho de banda en LAN (Kbps)
G.711 (64kbps)	10	80	160	50	87,2
G.729 (8kbps)	10	10	20	50	31,2
G.723.1 (6,3kbps)	30	24	24	34	21,9
G.723.1 (5,3kbps)	30	20	20	34	20,8
G.726 (32kbps)	5	20	80	50	55,2
G.726 (24kbps)	5	15	60	50	47,2
G.728 (16kbps)	5	10	60	34	31,5
G722_64k (64 Kbps)	10	80	160	50	87,2
ilbc_mode_20(15.2Kbps)	20	38	38	50	38,4
ilbc_mode_30(13.33Kbps)	30	50	50	33,3	28,8

Tomado de: (CISCO, 2013).

Para obtener los valores de ancho de banda LAN de los distintos códec de la anterior tabla, se realiza los cálculos mediante la siguiente fórmula (CISCO, 2013):

Tamaño total del paquete (bytes) = (40 bytes de encabezado IP/UDP/RTP) + (18 bytes de encabezado Ethernet L2) + (Tamaño de carga útil de voz).

*Tamaño total del paquete de voz(bits) = Tamaño total del paquete (bytes) * 8 (bits)*

Paquetes por segundo (PPS)= (8 kbps de velocidad de bits de códec) / 160 bits

(PPS)= (8000 muestras obtenidas por seg.)/160 muestras de voz en un mismo paquete

*Ancho de banda por llamada (kbps)= Tamaño total del paquete de voz(bits) * #PPS.*

1.6.6. Ancho de banda de voz

El ancho de banda de la voz en paquetes depende directamente del tamaño de la ventana en milisegundos, ej: 10ms, 20ms, 30ms y el códec utilizado como se ilustra en la anterior **Tabla 1.**

1.6.7. Codecs de video

De igual forma que la voz, el flujo de video también experimenta procesos de codificación y decodificación previo a su transmisión. La codificación digital de video utiliza algoritmos de compresión que generan codificación de longitud variable y flujos de ancho de banda también variables como se muestra continuación en la **Tabla 2** algunos de los códecs de video más conocidos.

Tabla 2.- Codecs de video más comunes.

Características	MPEG-1	MPEG-2	MPEG-4	H.264/MPEG-4 Part 10/AVC
Codificación	VLC	VLC	VLC	VLC, CAVLC, CABAC
Estimación y compensación de movimiento	Si	Si	Si	Si
Ancho de banda	Hasta 1,5 Mbps	2 a 15 Mbps	64 kbps a 2 Mbps	64 kbps a 150 Mbps
Complejidad del codificador	Baja	Media	Media	Alta
Compatibilidad con estándares previos	Si	Si	Si	No

Tomado de: (Joskowicz, 2013, p. 20).

1.6.8. Ancho de banda de video

El ancho de banda que requiere una determinada aplicación de video en una red IP depende del tipo de codificación utilizado, del tamaño de la pantalla, del tipo de cuantización seleccionado, de la textura y movimiento de la imagen. Al ancho de banda original del video se añade la sobrecarga de paquetes IP, UDP, RTP y tramas Ethernet para la red LAN. A diferencia de codificación de voz, la codificación de video es estadística y los cálculos son aproximados como se muestra en la anterior **Tabla 2** (Joskowicz, 2013, p. 20).

1.7. Parámetros de calidad de voz y video

La calidad de los servicios que se implementan sobre las redes de paquetes IP son afectados por varios factores como:

1.7.1. Pérdida de paquetes

A diferencia de las redes de telefonía convencional, donde por cada conversación se establece un circuito individual estable, las redes de datos admiten determinada tasa de pérdida de paquetes. En aplicaciones

multimedia, el audio y video es encapsulado en paquetes de datos y enviados a su destino sin confirmación de recepción de cada paquete. La pérdida de paquetes en el destino es perceptible para los usuarios debido a que escucharán interrupciones en la voz y cortes en el video. Máximo el 3% de paquetes perdidos es aceptable para tráfico multimedia (Marín, 2008, p. 36).

Debido a que la red IP no garantiza el servicio, frecuentemente presenta pérdidas de paquetes. Es decir, bajo la congestión los paquetes de voz serán descartados de igual manera que los datos, pero estos últimos no son sensibles al tiempo. Dicho de otra forma, los paquetes perdidos de datos se pueden recuperar mediante una retransmisión a diferencia de los paquetes de voz que no pueden recibir este tratamiento por ser sensibles al tiempo. Para reducir las pérdidas de los paquetes de voz se puede enviar información redundante a pesar del costo del ancho de banda; es decir, introduciendo mayor tráfico en la red e incrementando el retardo (Edwin, 2009, p. 31).

1.7.2. Latencia o retardo

El retardo o latencia es debido a varios factores como el algoritmo de compresión que toma determinado tiempo en procesar una trama, el procesamiento que implica la recolección de muestras de voz y encapsulación en paquetes para su transmisión en la red, los protocolos empleados para la transmisión, la congestión del tráfico en la red, la velocidad de los enlaces, los buffers para jitter en el extremo del receptor que agregan retardos para reducir la variación de demoras (jitter) a la que están sometidos los paquetes al transitar por la red, entre los más importantes que influyen directamente en la calidad de servicios.

La latencia de extremo a extremo que incluye todas las demoras citadas anteriormente y el tiempo que emplean los equipos intermedios (routers) en gestionar las colas de paquetes se los puede representar mediante la siguiente ecuación (Edwin, 2009, p. 29).

$$\text{Tiempo Total} = \text{T algoritmo} + \text{T transmisión} + \text{T propagación} + \text{T conmutación} + \text{T cola}$$

$$T\ algoritmo = En\ función\ del\ Códec$$

$$T\ transmisión = Función\ de\ velocidad\ y\ tamaño\ de\ trama, paquete\ o\ celda$$

$$T\ propagación = En\ función\ del\ medio\ de\ transmisión$$

$$T\ conmutación = Depende\ de\ la\ Tecnología\ (Store\ \&\ Forward\ o\ Cutthrough)$$

$$Tiempo\ de\ colas = \ En\ función\ de\ la\ ocupación, prioridad, tamaño\ y\ velocidad$$

1.7.3. Eco

El eco es la percepción de la propia voz luego de haber transcurrido un determinado tiempo desde que se habló. El eco es ocasionado por reflexiones de señales generadas por el equipo en el extremo lejano que regresan al oído del emisor. El eco puede llegar a ser un problema mayor si el retardo del viaje completo llega a ser mayor de 50 milisegundos, en este caso cuando existe el incremento del eco, la red de paquetes de voz tendrá la necesidad de utilizar técnicas para la cancelación del eco que consiste en comparar los datos de voz recibidos con los paquetes de voz que son transmitidos sobre la red de paquetes (Edwin, 2009, p. 31).

1.7.4. Jitter

Es la variación de tiempo entre los paquetes causada por la red, es decir es la variación en las demoras. El jitter afecta la percepción de la voz y puede ser corregido a través de buffers que añaden un retardo adicional al sistema puesto que deben retenerlos por instantes hasta recolectar el último paquete que arribe para poder entregarlos a intervalos constantes. Mientras más grande sea el jitter (variación de demoras) más grande deberá ser el buffer y como consecuencia mayor retardo total tendrá el sistema (Edwin, 2009, p. 30).

Un ejemplo de jitter es cuando dos puntos intercomunicados reciben un paquete cada 20 milisegundos en promedio, pero en cierto instante, uno de los paquetes arriba a los 30 milisegundos y después otro a los 10 milisegundos, entonces el sistema tendrá un jitter de 10 milisegundos.

Por último, se muestra un resumen de los valores tolerables de los principales factores de calidad para servicios multimedia en la **Tabla 3.**

Tabla 3.- Valores tolerables de acuerdo al nivel de QoS.

Factores de Red	Nivel Apropiado	Nivel Aceptable	Nivel Deficiente
Retardo	0 – 150 ms	150 – 300 ms	>300 ms
Pérdidas	0 – 1,5 %	1,5 – 3%	>3%
Jitter	0 – 20 ms	20 – 50 ms	>50 ms

Tomado de: (Haivision, 2012).

1.8. Herramientas y mecanismos para implementar QoS

Los recursos de las redes son finitos por ende la congestión se genera cuando la demanda de recursos sobrepasa los disponibles en una red, por ellos se han desarrollado herramientas como (Erazo, 2009, p. 114):

a) *Clasificación de tráfico.-* Permite dividir el tráfico en varias categorías para el tratamiento individualizado. Puede realizarse mediante VLAN (Virtual LAN), ACL (Access Control List) y NBAR (Network Based Application Recognition) herramienta de clasificación avanzada de aplicaciones desarrollada por CISCO y disponibles en equipos actuales.

b) *Marcado del tráfico.-* Identifica a las tramas según su clase o categoría para su correspondiente tratamiento en la red. Realizado mediante DSCP (Differentiated Services Code Point), CoS (Clase de Servicio), IP Precedence que permite estalecer prioridades de servicios mediante los tres primeros bits del campo ToS.

c) *Administración de colas (Queue Management).-* Permite la gestión de la red mediante la ingeniería de tráfico para priorizar servicios sensibles al tiempo. Entre sus funciones están la planificación, diseño, proyección, dimensionamiento, desarrollo y supervisión de

las redes. Se puede realizar mediante FIFO (First In First Out), PQ (Priority Queuing), LLQ (Low Latency Queuing).

d) *Control de congestión.-* Impide que se llene una cola con tráfico de menor precedencia, para permitir que el tráfico de alta prioridad ingrese en la cola evadiendo la congestión. Realizable mediante RED (Random Early Detection), WRED (Weighted RED) soportadas por equipos actuales.

e) *Política/Control de tráfico.-* Estas herramientas limitan el ancho de banda que un determinado flujo o tráfico emplea en la red, para evitar el desbordamiento. Puede implementarse mediante CAR (Comitted Access Rate) soportada por equipos actuales.

f) *Eficacia del Enlace.-* Proporcionan un método de reducción de retraso experimentado sobre enlaces de baja velocidad. Realizable mediante fragmentación, compresión de payload y encabezado mediante Stacker y cRTP (Compressed Real Time Protocol) respectivamente.

2. Capítulo II. Modelos y metodologías de diseño de redes multiservicio

Las redes LAN en la actualidad constituyen un pilar fundamental en el desarrollo de una empresa o institución, por consiguiente es necesario llevar a cabo un diseño apropiado de la red de acuerdo a una estructura organizada que satisfaga los distintos requerimientos esenciales como escalabilidad, disponibilidad, QoS entre otros. Con esta finalidad se han desarrollado varios métodos que contribuyen al diseño apropiado de las redes mediante el cumplimiento de fases cronológicas que poseen cada una de ellas y se describen en este capítulo.

2.1. Diseño modular

Es la arquitectura de diseño que permite la separación de la red en varios módulos, cada uno con funciones específicas, facilitando el diseño y la administración. Los módulos tienen designados sus respectivas funciones y pueden poseer conectividad física y lógica diferentes. Los principales módulos de una red están identificados como: el módulo del campus empresarial, el bloque de servicios, el centro de datos y el módulo de internet perimetral como se muestra en la **Figura 10.** La modularidad en el diseño de la red contribuye a la flexibilidad y la resolución de fallas mediante el aislamiento del módulo (CISCO, 2015, p. 13).

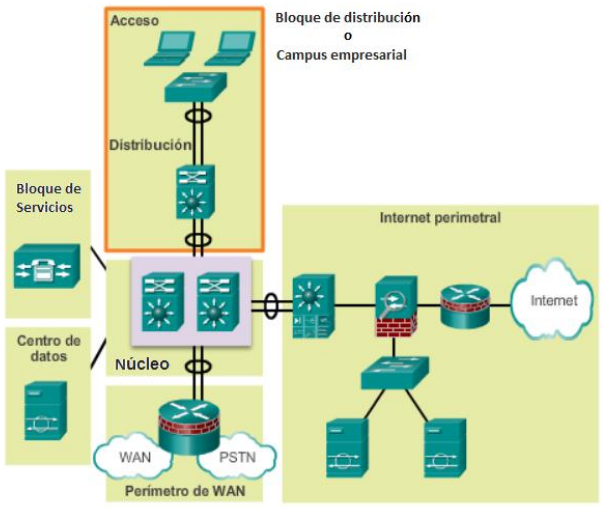


Figura 10.- Arquitectura de diseño modular de red (CISCO, 2015, p. 14).

2.2. Diseño jerárquico de redes

El mantenimiento de una red puede llegar a ser un problema muy complejo en topologías de red cuyo diseño no sea basado en un modelo jerárquico, por ejemplo en una red de topología de estrella extendida puede implicar un crecimiento desordenado, dificultando su administración. Debido a problemas como estos se ha desarrollado el modelo de jerarquización de la red, el cual ofrece varios beneficios de diseño, permitiendo que esta sea más manejable mediante capas que contribuyen a una mejor comprensión, a la identificación y solución agilizada de fallos. Ayuda también a tomar decisiones apropiadas en cuanto a la forma de aplicar cualquier configuración (CISCO, 2010).

La jerarquización no es más que la segmentación lógica de una red en capas o niveles independientes que facilitan en gran medida en el diseño, implementación y mantenimiento, garantizando escalabilidad y confiabilidad, además de una mejor relación costo-beneficio. El modelo jerárquico ayuda a separar de manera lógica y no necesariamente física, es decir que un dispositivo de red puede trabajar en varias capas jerárquicas o varios equipos pueden trabajar sobre una misma capa. Cada una de las capas del modelo jerárquico de redes posee una función específica como se explica brevemente a continuación y se ilustra en la **Figura 11** (CISCO, 2010).

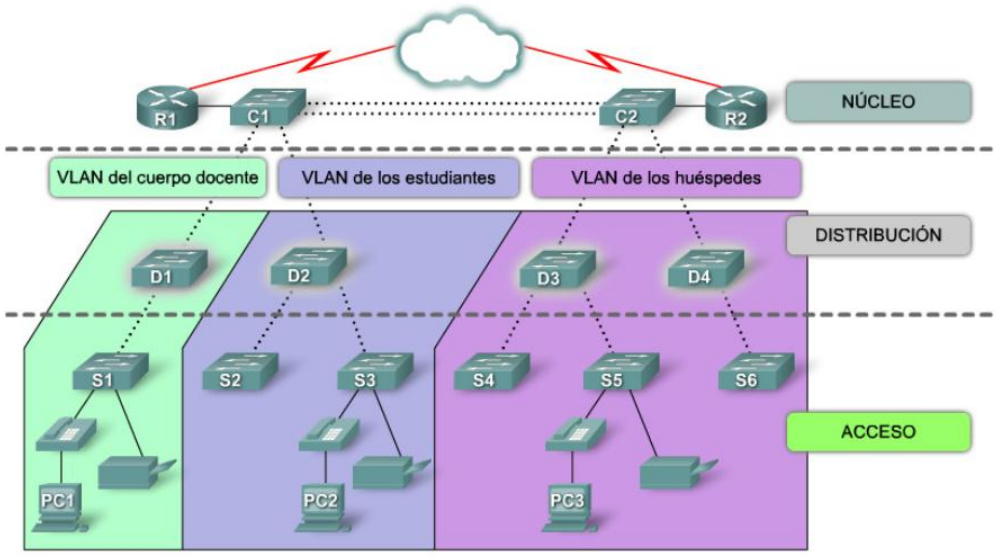


Figura 11.- Modelo de red jerárquica (CISCO, 2010).

2.2.1. Capa de acceso

Esta capa tiene como finalidad proveer una primera conexión de los dispositivos finales tales como PC's, impresoras, teléfonos IP, etc de los distintos grupos de trabajos y usuarios hacia la red, ofreciendo la capacidad de control de acceso de los dispositivos finales (Lopez, 2009). Sus funciones principales son el control de acceso, establecimiento de políticas de acceso, la creación de dominios de colisión, entre las más importantes. Por último, aquí se realiza la conmutación Ethernet y ruteo estático (Ipreference, 2008).

En esta capa se pueden encontrar routers, switches, puentes, hubs y puntos de acceso inalámbricos.

2.2.2. Capa de distribución

Esta capa es la intermediaria en la comunicación entre las capas de acceso y el núcleo cuyas finalidades son el control del tráfico de la red a través del uso de políticas y la segmentación de la red en dominios de broadcast a través de VLAN's (ITESA, 2010). En esta capa se establecen métodos para brindar una respuesta adecuada a la solicitud de los usuarios de la red mediante la implementación de las distintas políticas tales como: listas de control de acceso

(ACL's), el filtrado de paquetes que pasarán al núcleo (Firewall), colas de espera para garantizar QoS, ruteo entre LAN virtuales (VLAN's) definidas en la capa de acceso, dominios de multicast, entre otros. Los switches de esta capa trabajan en las capas 2 y 3 del modelo OSI brindando disponibilidad y redundancia para garantizar la fiabilidad (Ipreference, 2008).

2.2.3. Capa de núcleo

Esta capa es la espina dorsal de la red (backbone de alta velocidad), cuya función principal es gestionar con gran rapidez el tráfico procedente de la capa de distribución, para lo cual esta capa debe poseer una alta capacidad y redundancia para el reenvío de grandes cantidades de datos. La tolerancia a fallos y disponibilidad en esta capa es muy importante puesto que en caso de presentar falla todos los usuarios se verán afectados (Lopez, 2009).

Debido a la gran importancia de la velocidad en esta capa no se llevan a cabo funciones que puedan incrementar la latencia como la implementación de listas de control de accesos, enrutamiento entre VLAN,s, filtrado de paquetes, accesos de grupos de trabajo, entre otros, los cuales deben implementarse en capas inferiores. Tampoco se debe incrementar nuevos equipos (routers) si se determina que la capacidad del núcleo es insuficiente, es recomendable optimizar sobre la plataforma actual antes de añadir un nuevo dispositivo (Ipreference, 2008).

El núcleo debe estar diseñado para garantizar una alta confiabilidad en lo referente a la redundancia, velocidad de sus enlaces y capacidad de sus dispositivos, garantizando baja latencia y tiempos de convergencia mínimos. En esta capa operan switches de capa 3 y routers (CISCO, 2010).

2.3. Beneficios del diseño jerárquico

2.3.1. Escalabilidad

La red jerárquica, al ser de una estructura modular, permite añadir nuevos equipos, nuevos nodos, o nuevos segmentos de red mediante switches a medida que la red va creciendo. Además, en caso de crecimiento del tráfico de

la red es posible aligerar la carga tráfico mediante un switch de mayor capacidad. La consistencia de cada capa del módulo permite una óptima planificación e implementación de nuevas expansiones (Sistemasumma, 2012).

2.3.2. Disponibilidad

Para garantizar la disponibilidad de la red este modelo define el uso de enlaces redundantes mediante switches alternos o de respaldo que ayudan a mantener la comunicación ante cualquier fallo (Sistemasumma, 2012). La redundancia puede ser implementada tanto en la capa del núcleo como en la capa de distribución para asegurar la disponibilidad de una ruta. En la capa de acceso la redundancia se ve limitada debido a que los dispositivos finales como las PC's, impresoras etc. no cuentan la capacidad de ofrecer enlaces redundantes (Lopez, 2009).

Las tecnologías que permiten garantizar la disponibilidad de la red son el STP (Spanning Tree Protocol) definido en el estándar IEEE 802.1D y Etherchannel desarrollado por Cisco de acuerdo a los estándares 802.3 (CISCO, 2015).

2.3.3. Seguridad

La naturaleza de la red jerárquica y su posibilidad de segmentación a través de VPN's permiten definir políticas de seguridad de acceso entre los segmentos de la red de tal manera que puedan acceder determinados equipos a determinados recursos (Sistemasumma, 2012). Además se pueden aplicar políticas de control de acceso mediante restricciones a determinados protocolos de comunicación, por ejemplo HTTP, a los cuales podrán acceder ciertos usuarios. La definición de estas políticas de acceso avanzadas pueden ser implementadas a nivel de la capa de distribución. A nivel de acceso la seguridad de los puertos de los switches permiten el control de los equipos que podrán conectarse a la red. De esta forma es posible brindar seguridad y simultáneamente la facilidad de la administración de la red (CISCO, 2010).

2.3.4. Calidad de servicios QoS

La calidad de servicios está reflejada en el rendimiento de la red, es decir en secciones donde el flujo de datos es de alta densidad se requiere un switch de

alto rendimiento y/o el establecimiento de restricciones mediante políticas de seguridad y políticas de QoS para garantizar el tratamiento adecuado de los datos. La calidad de servicios se puede garantizar empleando los modelos InterServ o el Diffserv, los cuales están descritos en el capítulo anterior (Sistemasumma, 2012).

2.3.5. Facilidad de mantenimiento y administración

Debido a la naturaleza modular de la red jerárquica es posible identificar fallos y resolverlos con mayor rapidez, además facilita la planificación e implementación de nuevos segmentos de acuerdo al crecimiento sin realizar grandes cambios ni inversiones (CISCO, 2010).

2.4. Metodologías de diseño

2.4.1. Diseño de red Top-Down

Esta metodología está compuesta por cuatro fases para el desarrollo del diseño de redes, los cuales se citan a continuación (Milagros, 2013):

1.- *Primera fase.- Análisis de requerimientos.*

En esta primera fase se lleva cabo la identificación de las necesidades, objetivos, metas y restricciones del negocio.

2.- *Segunda fase.- Diseño lógico.*

En esta fase se realiza el diseño de la topología de la red, se establece el modelo de direccionamiento, la selección de protocolos de Switching y Routing para el manejo del tráfico de la red, por último aquí se lleva a cabo el desarrollo de estrategias de seguridad y administración de la red.

3.- *Tercera fase.- Diseño físico.*

Esta fase involucra la elección de tecnologías y equipos los cuales cubrirán satisfactoriamente los requerimientos técnicos del diseño lógico desarrollado en

la fase anterior. Por ejemplo, la selección de tecnologías y equipos para el cableado estructurado.

4.- *Cuarta fase.- Pruebas, optimización y documentación del diseño.*

En esta fase se debe tomar en cuenta que cada diseño es diferente, para lo cual es muy importante seleccionar métodos y herramientas adecuados para una correcta evaluación del diseño de la red. Además, es muy importante comprender completamente el diseño a ser evaluado para establecer un plan de evaluación, por ejemplo realizar pruebas recomendadas por los fabricantes y diseñar escenarios de prueba adecuados, los cuales deben enfocarse en la medición del rendimiento y fallas.

2.4.2. Ciclo de vida de la red según Cisco

Esta metodología denominada por Cisco PDIOO subdivide el ciclo de desarrollo de una red en cinco fases que se describen a continuación (Cajaleón, 2013):

1.- *Fase de planificación.-* Se identifican y detallan los requerimientos de la red.

2.- *Fase de diseño.-* En esta fase se lleva a cabo el diseño de acuerdo a los requerimientos de la fase anterior y se realiza el subdireccionamiento y la asignación de direcciones IP.

3.- *Fase de implementación.-* Es esta fase se realiza el diseño físico de la red como la distribución del cableado, la configuración de VLAN's, etc.

4.- *Fase de operación.-* En esta fase se ejecutan pruebas al diseño, para ello la red es monitoreada al entrar en operación.

5.- *Fase de Optimización.-* En esta fase es donde las fallas que son detectadas son corregidas para el óptimo rendimiento de la red. Si se presentan muchos problemas en esta fase, es posible que requiera un rediseño de la red.

2.4.3. Metodología del INEI

El Instituto Nacional de Estadística e Informática INEI de Perú ha desarrollado su propia metodología a través de un marco metodológico compuesto de cuatro etapas definidas a continuación (Milagros, 2013):

a.- Organización

Es la primera etapa del marco metodológico donde se lleva a cabo el modelamiento de los requerimientos de la red que incluye la identificación de necesidades y limitantes para el desarrollo del diseño.

b.- Análisis

En esta etapa se realiza el análisis de la topología adecuada, la estructura de la red y los recursos necesarios, tomando en cuenta la forma de integración de los distintos segmentos de la red, el crecimiento del número de usuarios y el tráfico.

c.- Desarrollo

En esta fase se lleva a cabo el desarrollo de los diseños lógicos y físicos de acuerdo a los resultados de las etapas anteriores.

d.- Implementación

En esta etapa final se lleva cabo la instalación física y lógica de los diseños desarrollados en la etapa anterior de acuerdo al análisis de los requerimientos iniciales.

2.4.4. Metodología de James McCabe

Esta metodología de diseño de red está compuesta por cuatro fases que se describen brevemente a continuación (Milagros, 2013):

1.- *Fase I.- Análisis de la situación actual.*

En esta fase se observa e identifica las deficiencias y problemas que puede presentar en la actualidad una determinada plataforma de comunicación como una red multiservicios.

2.- *Fase II.- Determinación de los requerimientos*

En esta fase se determinan las necesidades y exigencias que debe satisfacer la red, por ejemplo los requerimientos principales pueden ser la selección de tecnologías de bajo costo, de implementación rápida, que permita escalabilidad y facilidad de mantenimiento.

3.- *Fase III.- Análisis de las necesidades del sistema*

En esta fase se analiza los espacios físicos adecuados para la ubicación de los equipos y dispositivos de red garantizando su correcto desempeño en el manejo del tráfico de la red.

4.- *Fase IV.- Construcción*

Esta fase es el resultado de las tres fases anteriores, el cual consiste en la ejecución del diseño desarrollado de acuerdo al análisis y determinación de los requerimientos y necesidades de la red.

2.5. Análisis comparativo de las metodologías de diseño

Las metodologías de diseño descritas anteriormente en este capítulo, poseen etapas similares para el desarrollo de un diseño de red. El ciclo inicia con la identificación del estado actual de la infraestructura, las necesidades y limitantes para el desarrollo del diseño, denominado requerimientos. A continuación, se lleva a cabo un análisis entre los requerimientos identificados y la elección de las tecnologías y equipos que solventarán dichos requerimientos. Después, procede el diseño físico y lógico mediante la distribución adecuada de los recursos de red. Ciertas metodologías concluyen con la implementación y puesta en marcha de la red con determinadas pruebas

críticas, otras sin embargo además de desarrollar las etapas mencionadas, incluyen una nueva que consiste en la optimización del desempeño de la red.

A pesar de que estas metodologías poseen ciclos similares para el desarrollo de un diseño, cabe mencionar que la metodología más apropiada para el presente trabajo, debido a su popularidad y la adecuada documentación de cada una de sus fases específicas es la metodología Top-Down, la cual es una de las más completas debido a que en su fase final incluye un ciclo muy importante como la optimización de la red y su correspondiente documentación.

La metodología Top-Down y el modelo de diseño jerárquico satisfacen adecuadamente los objetivos planteados para el presente trabajo, cuya finalidad es el diseño de red sin llegar a la etapa de implementación, pero garantizando la escalabilidad, rendimiento, seguridad, disponibilidad, facilidad de mantenimiento y administración a través del modelo jerárquico. Las fases necesarias a desarrollar son las tres primeras y parte de la última como es la documentación del diseño.

El proceso de diseño mediante las fases de la metodología y modelo seleccionados se desarrollan a continuación en los capítulos subsiguientes.

3. Capítulo III. Análisis de requerimientos de la red multiservicio

La CONAFIPS es una entidad financiera pública creada en el año 2011 mediante la Ley Orgánica de la Economía Popular y Solidaria la cual fue iniciada en el año 2007 por el presidente de la república Econ. Rafael Correa. Su creación tiene como finalidad prestar sus servicios a las Organizaciones del Sector Financiero y Popular (OSPF).

Actualmente la matriz de la CONAFIPS cuenta con 94 colaboradores distribuidos en 21 departamentos con un crecimiento planificado del 8% para el próximo año. Dentro del crecimiento planificado se encuentra la creación de dos nuevos departamentos y la ampliación de tres de ellos.

3.1. Análisis de los objetivos comerciales, requisitos de servicios y técnicos

3.1.1. Objetivos comerciales

Dentro de los principales objetivos comerciales referentes al diseño están:

- Diseñar una red multiservicios a un costo relativamente bajo.
- El diseño debe garantizar facilidades para el crecimiento.
- La vida útil del diseño no debe ser menor a diez años

3.1.2. Requerimientos de servicios

La red multiservicios a diseñarse deberá soportar principalmente los siguientes servicios específicos que manejará la institución.

- Telefonía IP para todas las estaciones de trabajo.
- Sistema VIMASEF (Sistema Financiero Contable)
- Correo corporativo
- Conexión hacia internet desde todas las estaciones de trabajo.
- Video vigilancia
- Seguridad contra incendios
- Videoconferencia

- Servidor de dominio
- Servidor de archivos
- Active Directory
- Servidor DHCP
- Servidor DNS
- Servidor WEB
- Servidor de Base de Datos

3.1.3. Requisitos técnicos

Dentro de los requisitos técnicos se deben garantizar los siguientes:

- Escalabilidad
- Disponibilidad
- Rendimiento (QoS)
- Seguridad
- Facilidad de administración

3.2. Requisitos para la escalabilidad

Para garantizar la escalabilidad de la red, el diseño deberá cumplir las siguientes características.

- La capa de acceso brindará la capacidad de agregar nuevos usuarios a la red de acuerdo a las necesidades, mediante la disponibilidad de puertos sin afectar a las capas superiores como la de distribución y el núcleo.
- En la planificación del direccionamiento IP estarán considerados direcciones IP disponibles para nuevos usuarios.
- Para limitar el broadcast y el tráfico innecesario a nivel de distribución y núcleo en el diseño se empleará routers y switches de capas múltiples, junto con la implementación de VLAN’s por cada departamento.

- Aquellos enlaces donde sea necesario un incremento de ancho de banda se utilizarán tecnologías como EtherChannel o balanceo de carga según el caso.
- El direccionamiento IP estará diseñado de manera jerárquica de tal forma que permita efectuar resúmenes y disminuir el tamaño de tablas de enrutamiento.

3.3. Requisitos para la disponibilidad.

Para garantizar la disponibilidad de la red las 24 horas los 7 días de la semana se proporcionará, protecciones técnica y económicamente adecuadas contra fallas de la red tales como:

Enlaces:

- Crear enlaces redundantes desde la capa de acceso hasta el núcleo.
- Emplear protocolos que garanticen una convergencia rápida y funcionamiento confiable, a través de rutas y enlaces redundantes.
- Realizar doble conexión de los servidores en dos switches distintos de la capa de acceso. Establecer conexiones redundantes en la capa de distribución.
- Disponer de conectividad hacia internet mediante dos ISP’s diferentes de ser posible, caso contrario solicitar enlace redundante al único ISP.

Equipamiento:

- Incluir equipamiento redundante y fuentes de energía en los equipos críticos en la medida de lo posible.
- En áreas críticas se agregarán dispositivos finales redundantes como la cámara IP, cada una conectada a switches independientes.
- Reducir tanto como sea posible el tamaño de los dominios de fallas.
- Considerar la virtualización de ciertos recursos en caso de ser necesario.

3.4. Requisitos para el rendimiento de la red

El rendimiento de la red es el resultado de distintos factores como los diferentes tamaños de los paquetes, los grupos de protocolos empleados, las diversas tolerancias al retardo, entre otros. Para lograr un adecuado rendimiento de la red es importante reducir los tiempos de procesamiento de transacciones en los nodos intermedios en base a los parámetros definidos en el capítulo 1 en la **Tabla 3,** para lo cual se realizará:

- Garantizar un reducido diámetro de red.
- Limitar los broadcast y tráfico innecesario.
- Establecer y conservar rutas cortas que aseguren grandes anchos de banda hacia servidores críticos.
- Establecer políticas de tráfico basadas en VLAN.
- Establecer prioridades de tráfico mediante políticas de QoS e identificar sectores posibles de formación de cuellos de botellas y aplicar dichas políticas.

3.5. Requisitos para la seguridad

La seguridad no debe ser minimizada o ignorada, por lo tanto para satisfacer los requisitos mínimos de seguridad debe considerarse:

- Separar todos los segmentos de red de otras redes no seguras como el internet.
- Crear comunicaciones seguras mediante VLAN’s para prevenir cualquier amenaza.
- Establecer seguridad en los puertos de salida de los switches mediante la verificación de la identidad para conceder el acceso a la red que estará basado en las direcciones MAC asociadas a un puerto del switch mediante Port Security.
- Control amenazas externas provenientes del internet a través de una zona desmilitarizada DMZ.

- Implementar soluciones de seguridad a los puntos de acceso inalámbrico para su protección.
- Tomar medidas de seguridad física contra el acceso a los dispositivos de red por personal no autorizado.
- Creación de VLAN’s de administración.

3.6. Requisitos para facilidad de administración

La administración es un aspecto muy importante en una red que está expuesta al crecimiento, lo cual implica que mientras más crezca la red, la administración se convertirá más compleja sin una adecuada planificación. En el presente diseño se contempla al crecimiento como uno de los requisitos técnicos a satisfacer, por lo tanto para facilitar la administración de la red se lo realizará mediante los siguientes procesos.

- Segmentación de la red tanto para facilidad de administración y gestión de la red.
- Direccionamiento planificado para cada segmento de red
- Diseño por capas para limitar eventuales fallas e identificarlas con mayor rapidez.
- Gestión de la red mediante protocolos SNMP (Protocolo Simple de Administración de Red) y Syslog.
- Creación de VLAN’s de administración y de gestión de la red.
- Emplear equipos que sean administrables tanto directa como remotamente.

La administración de la red es un conjunto de funciones que incluye la planificación, asignación, implementación, coordinación, control y supervisión de los recursos de una red. Mientras que la gestión se refiere a la monitorización y control de los recursos de red en tiempo real sin que estos sean solicitados pero que son vitales para que la red se mantenga operativa. (Lino, 2011)

3.7. Requisitos del número de usuarios

La corporación dentro de su planificación para el siguiente año 2016 consta el crecimiento del 8% de su nómina actual, dando como resultado un total de 101 colaboradores y la creación de dos nuevos departamentos que deberán tener acceso a la red multiservicios. La red diseñada debe garantizar flexibilidad ante cambios o modificaciones para usuarios adicionales de acuerdo a nuevos objetivos o necesidades de la empresa. La nómina prevista para el año 2016 se muestra a continuación en la **Tabla 4** que incluye las nuevas vacantes a ocupar y se muestra en los cuadros resaltados.

Tabla 4.- Tabla de proyección de servidores de la CONAFIPS 2016

Dirección/Unidad	No. servidores (as)	Total Servidores (as) nómina	Prestación de Servicios	Total Usuarios
Dirección General	6	6		6
Auditoría Interna (Nuevo departamento)	3	3		3
Dirección de Planificación	2	2	1	3
Dirección de Comunicación Social	4	4		4
Dirección de Asesoría Jurídica	3	3		3
Dirección de Desarrollo de las OSFPS	1	17		17
• Unidad de Análisis de las OSFPS	8			
• Unidad de Fortalecimiento de las OSFPS	8			
Dirección de Productos Financieros	1	11	4	15
Unidad de Crédito	8			
Unidad de Nuevos Productos Financieros	2			

Dirección de Servicios Financieros	0	5	1	6
Unidad de Gestión del Fondo de Garantía	3			
Unidad de Negocios Fiduciarios	2			
Dirección de Inteligencia de Mercados	2	2	1	3
Dirección de Gestión de Riesgos (Nuevo dpto.)	2	2		2
Dirección de Gestión de Coactiva	3	3		3
Dirección Financiera	1	9		9
Unidad de Contabilidad	3			
Unidad de Tesorería e Inversiones	5			
Dirección Administrativa y de Talento Humano	0	11	1	12
Unidad de Administración	8			
Unidad de Administración del Talento Humano	3			
Dirección de Tecnología y Sistemas de la Información	15	15		15
Total		93		101

Todos los servidores usuarios de la red multiservicios de la corporación deberán contar con los siguientes servicios básicos de red tales como: datos VIMASEF (Sistema Financiero Contable), telefonía IP, internet, correo corporativo.

3.8. Requisitos para el cableado estructurado

La estimación de los implementos necesarios en el diseño de la infraestructura física de la red se desarrolla a bajo los lineamientos de las normas EIA/TIA

568B que especifican criterios y métodos estandarizados para el diseño, la construcción y administración de un sistema de cableado estructurado distribuidos en bloques de manera jerárquica cada uno con características específicas.

A continuación se citan los lineamientos generales de la norma EIA/TIA 568B para el desarrollo del diseño del cableado estructurado.

De acuerdo al estándar los componentes considerados para el cableado estructurado son los siguientes (Btcino, 2011, p. 3) (Toro, 2011, p. 2):

3.8.1. Instalación de entrada

Se refiere a las acometidas de los principales servicios contratados como la línea telefónica, internet, enlaces dedicados, entre otros hacia el edifico comercial.

3.8.2. Cuarto de equipos

La norma considera un espacio físico dedicado al alojamiento en un ambiente adecuado para los equipos activos de red como routers switches, entre otros. El espacio está definido de acuerdo al número de estaciones de trabajo como se ilustra en la siguiente **Tabla 5**.

Tabla 5.- Espacios físicos mínimos para cuartos de equipos.

Número de estaciones de trabajo	**Espacio físico (m2)**	**Altura mínima (m)**
De 1 a 100	14	2,44
De 101 a 400	38	2,44
De 401 a 800	74	2,44
De 801 a 1200	111	2,44

Tomado de: (Briceño & Amalia, 2011).

El ambiente del cuarto de equipos debe estar aislado de la contaminación exterior, la temperatura debe mantenerse entre 18^0C y 24^0C, la humedad entre el 30% y 55%, para procurar el funcionamiento correcto o la disponibilidad de los equipos las 24 horas los 365 días del año. Si el ambiente normal no lo permite es necesario emplear equipos de calefacción, ventilación, aire acondicionado, humificadores, deshumificadores dependiendo de las condiciones ambientales del sitio.

La ubicación del cuarto de equipos es muy importante que se encuentre situado en un espacio céntrico para garantizar el equilibrio en las distancias del cableado horizontal como especifica la norma EIA/TIA 568B una distancia máxima de 90m para el susbsistema horizontal.

3.8.3. Cableado vertical o dorsal (backbone)

El cableado vertical constituye el subsistema vertical denominado también dorsal o backbone cuya misión es proveer conectividad entre el cuarto de equipos y los distintos cuartos de telecomunicaciones distribuidos en el edificio comercial, también puede interconectar cuartos de equipos entre edificios (interbuiding). Está formado por medios de transmisión de cobre o fibra óptica dependiendo de la distancia entre los cuartos a comunicar y el ancho de banda requerido. A continuación en la **Tabla 6** se muestra las distancias soportadas por los medios de transmisión reconocidos por la norma.

Tabla 6.- Distancias máximas para el cableado vertical.

Tipo de medio	**Distancia vertical (m)**
Cobre (UTP/ScTP)	90
Cobre (Voz)	500
FO Multimodo	1700
FO Monomodo	2700

Tomado de: (Quang Dung Technology, 2010, p. 4).

3.8.4. Cuarto de telecomunicaciones (Armario de telecomunicaciones)

El cuarto de telecomunicaciones es un espacio físico donde se ubican los equipos que reciben conexiones del cableado vertical y provee conexiones salientes hacia las estaciones de trabajo a través del cableado horizontal. La norma recomienda un mínimo de un cuarto de telecomunicaciones por piso mientras la distancia no supere los 90 m del cableado horizontal.

3.8.5. Cableado horizontal

El cableado horizontal constituye el subsistema horizontal cuya función de acuerdo a la norma es proveer la conexión entre el cuarto o armario de telecomunicaciones y el área de trabajo. La norma establece distancias que no deben exceder los 90 metros.

En este subsistema debe estar planificado el crecimiento, la reducción de los mantenimientos y reubicaciones mediante una topología en estrella.

3.8.6. Área de trabajo

Es el área conformada desde el conector de salida de telecomunicaciones del cableado horizontal hasta el equipo de trabajo que debe emplear un cordón de longitud no mayor de 5 metros como especifica la norma para conectarse en su área. A continuación en la **Tabla 7** se muestra un resumen de las distancias máximas recomendadas por la norma entre el cableado horizontal y la estación de trabajo.

Tabla 7.- Longitud máxima entre cableado horizontal y el área de trabajo

Longitud del cableado horizontal (m)	**Longitud máxima del cable del área de trabajo (m)**	**Longitud máxima entre cables de área de trabajo, patch cord y cordones de equipos (m)**
90	5	10
85	9	14
80	13	18
75	17	22
70	22	22

Tomado de: (Quang Dung Technology, 2010, p. 6).

4. Capítulo IV. Diseño físico y lógico de la red multiservicio

4.1. Diseño físico

Después del análisis de los requerimientos que debe cumplir el presente diseño de red para la corporación, la siguiente etapa consiste en llevar a cabo el desarrollo del diseño físico de la red que se iniciará con la distribución equilibrada del cableado, cuartos de equipos, cuartos de telecomunicaciones, entre otros, conforme a la norma EIA/TIA 568. La distribución de las salidas de datos se realiza sobre los planos arquitectónicos de la planta baja y la planta alta mostrados detalladamente en los **Anexo 1** y **Anexo 2** respectivamente que incluyen sus correspondientes dimensiones para lograr un óptimo diseño de acuerdo a la norma citada.

4.1.1. Diseño físico de la red de la planta baja

El diseño físico de la red de la planta baja del edificio se lleva a cabo de acuerdo al **Anexo 1** donde se esquematiza la ubicación adecuada del cuarto de equipos para la distribución equilibrada del cableado de acuerdo a la norma EIA/TIA 568 y los requerimientos previstos en cuanto al crecimiento del número de usuarios. En esta planta están previstos 106 salidas de telecomunicaciones para los cuales es necesario el siguiente equipamiento como se muestra a continuación en la **Tabla 8.**

Tabla 8.- Equipos finales principales para la planta baja.

No.	Salidas	Cantidad
1	Cámaras IP	6 u
2	Teléfono IP	9 u
3	Impresoras	4 u
4	Control de acceso	3 u
5	Access point	1 u
6	Panel de alarma	1 u
7	Sensores de incendio	3 u
8	Face Plate simple	24 u
9	Face Plate Doble	41 u

En el presente diseño para la planta baja, con el fin de ahorrar costos en equipos están previstos nueve teléfonos IP físicos, destinados únicamente para los usuarios directores de cada departamento de la corporación. El resto de usuarios se comunicarán a través de Softphone. El access point de la planta baja está destinado a proveer datos a los visitantes que se encuentren en la sala de espera del edificio.

4.1.2. Diseño físico de la red de la planta alta

De manera similar al diseño de la planta baja, la planta alta está diseñada de acuerdo al **Anexo 2** donde se ilustra la ubicación adecuada del cuarto de telecomuniciones, para lograr la distribución equilibrada del cableado de acuerdo a la norma EIA/TIA 568 y los requerimientos de crecimiento del número de usuarios. En esta planta están previstas 53 salidas de telecomunicaciones para los cuales se requieren principalmente los siguientes equipos finales como se muestra en la siguiente **Tabla 9.**

Tabla 9.- Equipos finales principales para la planta alta.

No.	Salidas	Cantidad
1	Cámaras IP	1 u
2	Teléfono IP	12 u
3	Impresoras	3 u
4	Control de acceso	0 u
5	Access point	1 u
6	Panel de alarma	1 u
7	Sensores de incendio	3 u
8	Face Plate simple	8 u
9	Face Plate Doble	22 u

Los teléfonos IP de igual manera que en la planta baja para ahorrar costos en el equipamiento se destinarán 12 teléfonos físicos IP únicamente para los funcionarios directivos y ejecutivos de la corporación. El resto de usuarios se comunicarán mediante Softphone. El access point de la planta alta está

destinado a proveer datos a los usuarios que se encuentren en la sala de reuniones del edificio.

4.1.3. Subsistema horizontal

El subsistema horizontal determina la distribución adecuada del cableado respecto a las distancias y condiciones como recomienda la norma TIA/EIA 568 tales como; el enrutamiento mediante bandejas, escalerillas o rejillas sobre el cielo falso, lejos o protegido de las posibles interferencias externas, es decir según las condiciones de la edificación. En los tramos finales del cableado horizontal y cercano al usuario se emplean canaletas que conservan la estética de su área de trabajo.

Para realizar la estimación de la longitud de cable UTP necesaria para el cableado horizontal de la red de la planta baja se efectuará la siguiente ecuación (Cablered, 2010):

$$\boldsymbol{distancia\ cable} = \frac{\sum \boldsymbol{d_{min}} + \sum \boldsymbol{d_{max}}}{\mathbf{2}} * \ \#\boldsymbol{S_{tel}} * \boldsymbol{f_{seg}}$$

Donde:

$\sum d_{min} = holgura + altura + longitud + altura$

$=$ Distancia entre el cuarto de equipos y la salida de datos más cercana

$\sum d_{max} = holgura + altura + longitud + altura$

$=$ Distancia entre el cuarto de equipos y la salida de datos más lejana

$\#S_{tel} = \#\ de\ salidas\ de\ telecomunicaciones$

$f_{seg} = factor\ de\ seguridad\ (entre\ 1{,}1\ y\ 1{,}3)\ de\ \ la\ d_{total}$

Entonces:

$$dc(planta\ baja) = \frac{(2m + 3m + 12m + 3m) + (2m + 3m + 30m + 3m)}{2} * 106 * 1{,}15$$

$$dc(planta\ baja) = \frac{(20m) + (38m)}{2} * 106 * 1{,}15$$

$$dc(planta\ baja) = \frac{58m}{2} * 106 * 1{,}15$$

$$dc(planta\ baja) = 3535{,}1m$$

$$dc(planta\ baja) = 11{,}6\ rollos\ de\ cable\ UTP\ de\ 305\ m\ c.u.$$

Distancia del cable en la planta alta:

$$dc(planta\ alta) = \frac{(2m + 3m + 6m + 3m) + (2m + 3m + 25m + 3m)}{2} * 52 * 1{,}15$$

$$dc(planta\ alta) = \frac{(14m) + (33m)}{2} * 52 * 1{,}15$$

$$dc(planta\ alta) = 1405{,}3m$$

$$dc(planta\ alta) = 4{,}6\ rollos\ de\ cable\ UTP\ de\ 305m\ c.u.$$

En total para el cableado de la red física de las dos plantas del edificio es necesaria la cantidad de 16 rollos de cable UTP de 305 metros de longitud cada uno de ellos.

4.1.4. Subsistema vertical

Es el cableado que comunica el cuarto de equipos de la planta baja con el cuarto de telecomunicaciones de la segunda planta, que debido a su corta distancia de 15 metros, tomando en cuenta la distancia que existe entre ellos y su correspondiente holgura, será suficiente la conexión mediante el mismo cable UTP empleado en el subsistema vertical. El enrutamiento del cable será diferente del utilizado en el subsistema horizontal, es decir que en lugar de bandejas, será necesario una tubería para proteger de las condiciones externas del edificio.

4.1.5. Categoría del cable UTP

La selección de la categoría adecuada de cable UTP para el presente diseño depende básicamente del ancho de banda aproximado de acuerdo a los servicios que manejará la red y de las recomendaciones de la norma TIA/EIA 568, por lo tanto:

La estimación de ancho de banda en este trabajo se realiza mediante la primera aproximación del modelo matemático para la predicción del ancho de banda. Es importante resaltar que esta aproximación ha sido desarrollada considerando enlaces con proyección de crecimiento futuro, además está sujeto a nuevas modificaciones de estructura y datos de entrada que pueden generar nuevos antecedentes. El modelo es el siguiente (Contreras & Contreras, 2012, p. 2):

$$\boldsymbol{WB(bps) = n * P_{AP} * \varphi(n)}$$

Donde:

$WB(bps) = Ancho\ de\ Banda$

$n = número\ de\ usuarios\ de\ la\ red$

$P_{AP} = Peso\ de\ la\ aplicación = 79570\ bps$

$\varphi(n) = Tasa\ de\ ocupación$

Entonces:

$WB(bps) = 160 * 79570 bps * 90\%$

$WB(bps) = 11458080\ bps$

$WB(bps) = 11{,}5\ Mbps$

Del anterior resultado se puede concluir que utilizando el valor aproximado del peso de las aplicaciones (P_{AP}) con una tasa de ocupación al 90 % para una red de 160 usuarios es necesario un ancho de banda mínimo de 11, 5Mbps.

De acuerdo al resultado obtenido, la categoría 6A. cumple y excede los requerimientos de ancho de banda estimado para este trabajo, el desempeño con aplicaciones actuales y futuras como el Ethernet (10Base-T), FastEthernet (100Base-TX), GigabitEthernet (1000Base-T), 10 GigabitEthernet (10GBase-T), aplicaciones de voz y video analógico o digital, entre otros como se muestra en la siguiente **Tabla 10.**

Tabla 10.- Cuadro comparativo de categorías de cable UTP.

Identificación estándar	**Tipo**	**Longitud máxima (m)**	**Ancho de banda máximo teórico (MHz)**	**Velocidad Máxima Teórica (Mbps)**	**Comp. RJ45**	**Aplicación**
UTP CAT1	UTP	100	0,4	0,02	No	No utilizado en la actualidad
UTP CAT2	UTP	100	2	4	No	No utilizado en la actualidad
UTP CAT3	UTP	100	16	10	No	Cables telefónicos
UTP CAT4	UTP	100	20	16	Si	Raramente usado
UTP CAT5	UTP	100	100	100	Si	LAN Convencional
STP/FTP CAT5e	UTP	100	100	100	Si	LAN Convencional
FTP CAT6	UTP	100	250	1000	Si	LAN Gigabit Ethernet
FTP CAT6A	UTP	100	500	10000	Si	LAN Gigabit Ethernet
FTP CAT7	UTP/ STP/ FTP	100	600	10000	Si	LAN Gigabit Ethernet

En consecuencia, se estima conveniente para el presente trabajo de diseño el uso del cable UTP de categoría 6A, debido a sus ventajas técnicas y económicas respecto al resto. El cable UTP CAT7 posee muy altas prestaciones pero su costo es muy elevado y difícil de conseguir por su falta de popularidad.

4.1.6. Cuarto de equipos

En el cuarto de equipos ubicado en la parte central de la planta baja del edificio con 17m^2 de área y 2,88 m de altura, posee condiciones que cumplen con los requisitos de la norma TIA/EIA 568 para el alojamiento de los equipos de las capas de núcleo colapsado y acceso de la planta baja. El alojamiento de estos equipos se distribuyen por capas sobre dos racks de piso estándar de 32 UR cada uno como se muestran en los dos siguientes diagramas de elevación, ilustrados en la **Figura 12** y **Figura 13.**

2UR	ORGANIZADOR
1UR	PATCH PANEL 24 P
1UR	FIREWALL
2UR	ORGANIZADOR
2UR	SERVIDOR WEB
2UR	SERVIDOR INTERNO
1UR	NVR
1UR	PATCH PANEL 24 P
2UR	ORGANIZADOR
1UR	SWITCH 24P CAPA3
2UR	ORGANIZADOR
1UR	PATCH PANEL 24 P
2UR	ORGANIZADOR
1UR	SWITCH 24P CAPA3
2UR	ORGANIZADOR
1UR	MULTITOMA ELECTRICA
3UR	UPS TRIPPLITE 3KVA

Figura 12.- Diagrama de elevación de la capa de núcleo/distribución.

2UR	ORGANIZADOR
1UR	PATCH PANEL 24 P
2UR	ORGANIZADOR
1UR	SWITCH ACCESO 48 P
2UR	ORGANIZADOR
1UR	PATCH PANEL 24 P
2UR	ORGANIZADOR
1UR	PATCH PANEL 24 P
2UR	ORGANIZADOR
1UR	SWITCH ACCESO 48 P
2UR	ORGANIZADOR
1UR	PATCH PANEL 24 P
2UR	ORGANIZADOR
1UR	PATCH PANEL 24 P
2UR	ORGANIZADOR
1UR	SWITCH ACCESO 24 P
2UR	ORGANIZADOR
1UR	MULTITOMA ELECTRICA
3UR	UPS TRIPPLITE 3KVA

Figura 13.- Diagrama de elevación de la capa de acceso PB.

El equipamiento de las capas de núcleo, distribución y acceso están previstas de acuerdo al número de salidas de telecomunicaciones y la estructura jerárquica que garantiza redundancia, seguridad, rendimiento, escalabilidad y facilidad de mantenimiento.

4.1.7. Cuarto de telecomunicaciones

El cuarto de telecomunicaciones que comunica a los usuarios de la planta alta con el cuarto de equipos de la planta baja está ubicado de acuerdo a las recomendaciones de la norma TIA/EI 568 de la manera más centralizada para lograr un equilibrio respecto a las distancias hacia las estaciones de trabajo de la planta alta. En este cuarto, de acuerdo al presente diseño se encuentran

alojados únicamente los equipos de conmutación (switches) de la capa de acceso. El diagrama de elevación con el equipamiento necesario de acuerdo al diseño está representado a continuación en la **Figura 14** sobre un rack de pared estándar de 12 UR.

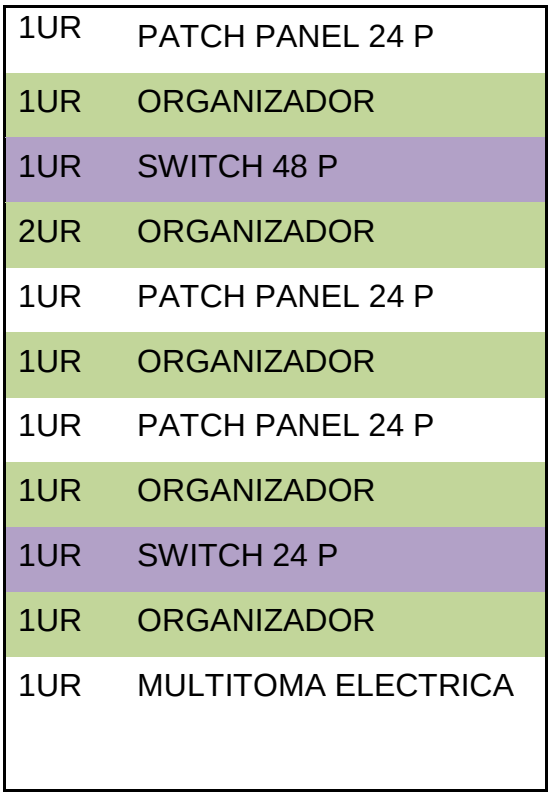


Figura 14.- Diagrama de elevación del cuarto de telecomunicaciones PA.

4.1.8. Elementos activos y pasivos de la infraestructura física

El presente diseño de la infraestructura física de la red está constituido por elementos activos y pasivos que se listan a continuación en la **Tabla 11.** En esta tabla se resume en su totalidad todos los materiales y equipos implicados en el diseño físico. Las marcas de los distintos elementos activos de red se seleccionarán más delante de acuerdo a las características que satisfagan los requerimientos del presente trabajo.

Tabla 11.- Listado general de elementos activos y pasivos de la red.

ELEMENTO	CANTIDAD
Pasivos del cuarto de equipos (PB)	
Rack de piso_32 UR	2
Pacth cord 3fts cat 6A	120
Patch panel modular 24 puertos cat 6A	8
Jack de patch panel cat 6A	20
Organizador horizontal 2UR	15
Blank negro	50
Multitoma Eléctrica	1
Pasivos del cuarto de telecomunicaciones (PA)	
Rack de pared_12 UR	1
Pacth cord 3fts cat 6A	72
Patch panel modular 24 puertos cat 6A	3
Jack de patch panel cat 6A	168
Organizador horizontal 1UR	5
Multitoma Eléctrica	1
Elemtos activos de red (Equipos)	
Servidor	2
Firewall	1
Switch 24 puertos (capa 3)	2
Switch 48 puertos (acceso)	3
Switch 24 puertos (acceso)	2
Central Telefónica IP	1
UPS Tripplite 3KVA	2
Enrutamientos (Pasivos)	
Bandejas/Rejillas metálicas	410 m
Tuberia de Ø 50mm	3 m
Codos de Ø 50mm	2 u
Canaleta mediana 2 canales	410 m
Pasivos del área de usuario	

Face Plate simple	32 u
Face Plate doble	63 u
Patch cord cat 6A 7 fts	158 u
Jack cat 6A	158
Caja sobrepuesta	158
Elementos activos finales (Equipos finales)	
Cámaras IP	7
Teléfono IP	21
Impresoras	7
Equipo de videoconferencia	2
Control de acceso	3
Access Point	2
Panel de Alarma	2
Sensores de incedio	6

4.2. Direccionamiento IP

El direccionamiento IP está desarrollado en base a ocho VLAN que se han considerado como principales en el presente trabajo de acuerdo al nivel de información crítica que manejan cada una de ellas. El direccionamiento en base a las VLAN satisface los requerimientos de rendimiento, seguridad, escalabilidad, facilidad de mantenimiento y administración. Las principales VLAN que maneja la red son:

La primera que manejará la voz y la segunda para los datos; las dos disponibles para todos los usuarios de la corporación. La tercera es exclusiva para el departamento financiero, la cuarta VLAN para dispositivos de red como impresoras, access point, paneles de alarma y dispositivos de control de acceso. La quinta para usuarios visitantes, la sexta exclusiva para videocámaras IP, la séptima para servidores y la última destinada para la administración de la red.

La distribución de las direcciones IP está diseñada en base a tres direcciones privadas clase C debido a que el número de usuarios de voz y de datos no superan los 255 en cada VLAN. La primera dirección destinada para la VLAN de voz es la 192.168.1.0/24 que garantiza la escalabilidad a futuro debido a su amplia gama de direcciones libres. La segunda dirección es la 192.168.2.0/24 prevista para los usuarios de la VLAN de datos, que también garantiza la facilidad para el crecimiento. La tercera y última dirección IP es la 192.168.3.0/24 para el resto de VLAN con densidad de usuarios relativamente pequeña, pero que de igual forma que el resto de direccionamientos está planificado para garantizar la escalabilidad. A continuación, en la **Tabla 12** se muestra la segmentación de la red y la asignación a cada una de las VLAN de acuerdo al número de usuarios e información que manejarán cada una de ellas.

Tabla 12.- Direccionamiento IP en base a las VLAN's y densidad de usuarios.

Departamento	**Usuarios**	**VLAN A Diercción IP**	**VLAN B**	**Diercción IP**
Todos excepto Dirección Financiera	118	VLAN_VOZ 192.168.1.0/24	VLAN_DATOS	192.168.2.0/24
Dirección Financiera	9		VLAN_FINANCIERO	192.168.3.32/27
Impresoras	15	-	VLAN_IMPRESORAS	192.168.3.0/27
Sensores biométricos				
Panel de alarma				
Access Point				
Visitantes	11	-	VLAN_VISITANTES	192.168.3.64/27
Cámaras IP	7	-	VLAN_VIDEOVIGILANCIA	192.168.3.96/27
Servidores	6	-	VLAN_SERVIDORES	192.168.3.128/27
Administrativa	6	-	VLAN_ADMINISTRATIVA	192.168.3.160/27

4.2.1. Distribución de los puertos de los switches de la capa de acceso

A partir de la segmentación realizada y mostrada en la tabla anterior se distribuyen las direcciones IP de acuerdo a la VLAN a la que pertenecen; es decir, que cada switch de la capa de acceso manejará determinadas VLAN en sus puertos de acceso destinados para cada usuario y/o equipo de la red de la corporación. A continuación en la **Tabla 13** se muestra un resumen de las VLAN que maneja cada uno de los switches de acceso.

Tabla 13.- Resumen de las VLAN manejadas por los switches de acceso.

VLAN	No.	SWITCHES CAPA DE ACCESO				
		SW1_PB	SW2_PB	SW3_PB	SW4_PA	SW5_PA
VOZ	10	Si	Si	No	Si	No
DATOS	20	Si	Si	No	Si	No
FINANCIERO	30	No	Si	No	No	No
IMPRESORAS	40	No	Si	Si	Si	Si
VIDEOVIGILANCIA	50	No	No	Si	No	Si
ADMINISTRATIVA	60	No	No	No	No	No
SERVIDORES	70	No	No	No	No	No
VISITANTES	80	No	No	No	Si	No

La asignación específica de las VLAN a cada uno de los puertos de los switches de la capa de acceso conjuntamente con la localización específica en los planos de la edificación se pueden apreciar en los anexos desde **Anexo 8.1.2** hasta **Anexo 8.1.6** donde se muestran el orden sugerido de las direcciones IP para los dispositivos finales conectados a una interfaz del switch de acceso y a sus correspondientes VLAN.

Cabe mencionar que en el presente trabajo se consideró necesario la creación de ocho VLANs principales, cada una con su correspondiente subdireccionamiento de acuerdo a la densidad de usuarios que maneja, de las cuales seis de ellos son asignables a los puertos de los switches de la capa de

acceso como se muestra en el resumen de la anterior **Tabla 13** y de manera detallada en los anexos citados en el párrafo anterior**.** Las dos restantes, la VLAN_SERVIDORES y la VLAN_ADMINISTRATIVA trabajan en la capa de núcleo/distribución con fines de mantenimiento y administración de la red.

4.2.2. Distribución de los puertos de los switches del núcleo/distribución

En esta capa de núcleo/distribución colapsados se manejan todas las VLAN creadas de acuerdo al presente diseño; es decir, que en lugar de recibir conexiones de dispositivos finales, maneja enlaces troncales con tráfico de distintas VLAN y gestiona el enrutamiento para la comunicación interVLAN como se muestra más adelante en la **Figura 15** los dos switches de 24 puertos que operan en esta capa**.** A continuación en la **Tabla 14** y **Tabla 15** se muestra la distribución de los puertos de los switches de la capa de núcleo colapsado con sus correspondientes identificaciones de los enlaces, garantizando la disponibilidad de puertos libres para satisfacer el requerimiento de escalabilidad a futuro y la disponibilidad de la red a través de enlaces redundantes.

Tabla 14.- Distribución de puertos del Switch de Núcleo/distribución 1.

Puerto	Enlace
1	TRONCAL0_DMZ
2	TRONCAL1_SW1PB_ ACCESO_48 P
3	TRONCAL1_SW2PB_ACCESO_48 P
4	TRONCAL1_SW3PB_ACCESO_24 P
5	TRONCAL2_SW4PA_ACCESO_48 P
6	TRONCAL2_SW5PA_ACCESO_24 P
7	ENLACE_SERVIDORES
8	REDUNDANCIA1_CORE
9	REDUNDANCIA2_CORE
10 - 24	SHUTDOWN

Tabla 15.- Distribución de puertos del Switch de Núcleo/distribución 2.

Puerto	Enlace
1	TRONCAL0_DMZ
2	TRONCAL1_SW4PA_ACCESO_48 P
3	TRONCAL1_SW5PA_ACCESO_24 P
4	TRONCAL2_SW1PB_ ACCESO_48 P
5	TRONCAL2_SW2PB_ACCESO_48 P
6	TRONCAL2_SW3PB_ACCESO_24 P
7	REDUNDANCIA1_CORE
8	REDUNDANCIA2_CORE
9-24	SHUTDOWN

4.2.3. Distribución de los puertos del Firewall de la DMZ

El firewall de la Zona Desmilitarizada (DMZ) del presente diseño maneja tres enlaces; el primero un enlace WAN que se identifica como OUTSIDE, el segundo enlace LAN, y el tercero un enlace hacia la DMZ como se muestra en la **Figura 15.** En consecuencia, son necesarios los tres primeros puertos del equipo firewall para los enlaces mencionados. A continuación en la **Tabla 16** se muestra la distribución de los puertos del firewall con su correspondiente VLAN asignada y la identificación de cada uno de los enlaces. La DMZ del presente diseño satisface los requerimientos de seguridad mediante VLANs, ACLs y escalabilidad por sus puertos disponibles.

Tabla 16.- Distribución de puertos del Firewall de la DMZ.

Puerto	VLAN	Enlace
1	OUTSIDE	TRONCAL0_OUTSIDE
2	INSIDE	TRONCAL1_SW6PB_CORE_24P
3	DMZ	SERVIDOR WEB
4	-	SHUTDOWN
5	-	SHUTDOWN
6	-	SHUTDOWN
7	-	SHUTDOWN
8	-	SHUTDOWN

4.3. Diseño lógico

Una vez determinados la cantidad y la ubicación de los distintos elementos activos y pasivos necesarios para el diseño físico de la red, se procede a desarrollar con mayor facilidad el diseño lógico de la misma. En el desarrollo del diseño lógico se podrá apreciar los distintos requerimientos técnicos cubiertos tales como la redundancia, seguridad, disponibilidad y rendimiento de manera satisfactoria. Los requerimientos de escalabilidad y facilidad de administración están cubiertos en la fase de diseño físico y direccionamiento.

4.3.1. Capa de acceso

La capa de acceso a la red del presente diseño está compuesta por un total de 158 salidas de telecomunicaciones planificadas para las dos plantas, de las cuales 106 están previstas para la planta baja y 52 salidas para la planta alta. En consecuencia, los equipos empleados en el diseño lógico de esta capa están constituidos de la siguiente manera. La planta baja está conformada por 3 switches: 2 switches de 48 puertos y 1 switch de 24 puertos que satisfacen perfectamente los requerimientos previstos como el crecimiento futuro, es decir que ciertos puertos de los switches estarán libres y disponibles frente a nuevas necesidades. La seguridad está cubierta a nivel de esta capa mediante la restricción de puertos.

En la planta alta la capa de acceso está conformada por 2 switches, uno de ellos de 48 puertos y el segundo de 24 puertos. De igual manera que en la planta baja, para solventar el crecimiento a futuro, permanecen algunos puertos libres y disponibles ante cualquier nueva necesidad. Los requerimientos de seguridad a nivel de esta capa están garantizados a través de la restricción de acceso a los puertos del switch, mediante direcciones MAC de los equipos finales. A continuación en la **Figura 15** se muestra el diseño de la red por capas jerárquicas.

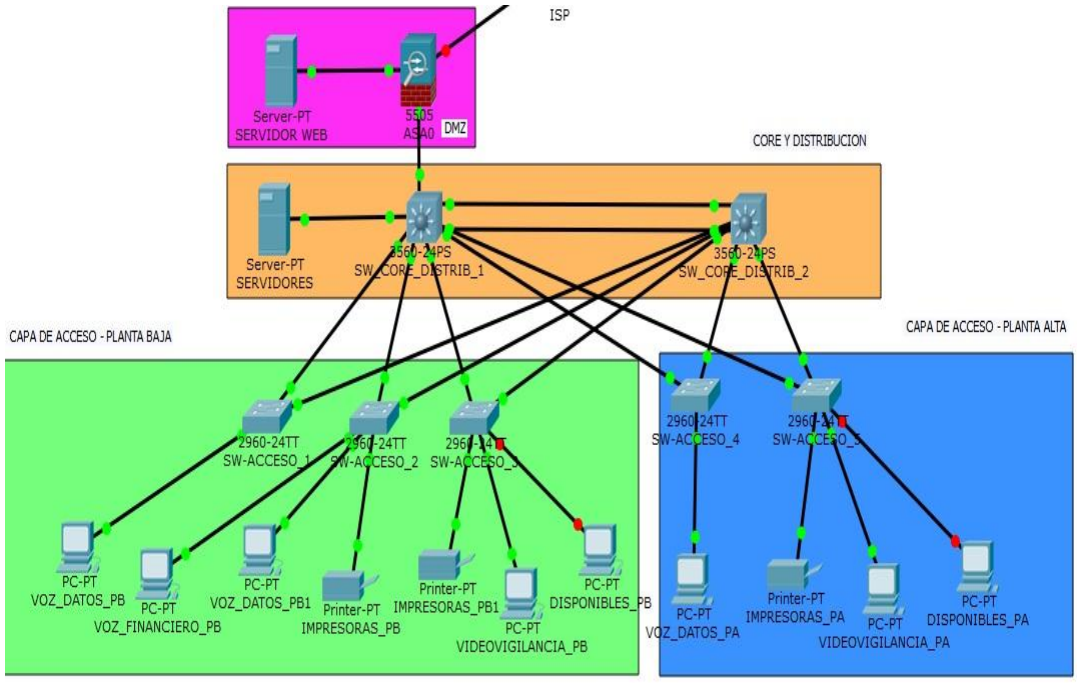


Figura 15.- Topología de la red diseñada por capas jerárquicas.

4.3.2. Capa de distribución y núcleo

La capa de distribución y el núcleo se encuentran fusionadas debido a varios factores que contribuyen a su reducción como el tamaño de la red relativamente pequeña, la disminución de costos y las prestaciones que ofrecen determinados switches de capa tres. Cada switch proporciona conectividad a los switches de acceso mediante enlaces troncales principales y de respaldo como se muestra en la **Figura 15** anterior, el SW_CORE_DITRIB_1 brinda conectividad a los tres switches de acceso mediante los enlaces troncales principales y simultáneamente brinda enlaces de redundancia mediante enlaces troncales secundarios a los switches de acceso de la planta alta del edificio.

El segundo switch SW_CORE_DITRIB_2 de la capa de núcleo/distribución también brinda conectividad mediante enlaces troncales principales a los dos switches de acceso de la planta alta del edificio y simultáneamente brinda

conectividad redundante a los tres switches de acceso de la planta baja mediante enlaces troncales secundarios.

En esta capa es donde se instalan los distintos servidores que brindarán servicios a los usuarios de la red. En este trabajo está previsto un servidor físico y cinco servidores virtuales destinados a proveer servicios a la red de la siguiente manera:

Servidor físico.- Destinado al alojamiento y soporte del sistema VIMASEF (Sistema financiero contable) y la base de datos de la corporación.

Servidor virtual 1.- Destinado a proporcionar servicios de Active Directory, servicio DHCP, servicio DNS, servicio de correo corporativo y servicio de dominio de red mediante Windows Server 2012.

Servidor virtual 2.- Previsto exclusivamente para un servidor de archivos para los usuarios de la red.

Servidor virtual 3.- Destinado para brindar soporte al servicio de telefonía para los usuarios de la red mediante el sistema Asterisk.

Servidor virtual 4.- Previsto para brindar soporte a los servicios de video vigilancia.

Todos los elementos del presente diseño de red antes descritas por capas, manejan información confidencial para la corporación, de tal manera que debe estar protegida ante cualquier amenaza externa a través de redes públicas como el Internet; por lo tanto para garantizar la seguridad a la red interna se establece una zona desmilitarizada (DMZ) que se describe a continuación.

4.3.3. Zona desmilitarizada (DMZ)

La zona desmilitarizada es un módulo de protección ubicado entre la red local y la red pública que aísla a la red local de un sinnúmero de amenazas externas para la red LAN multiservicios de la corporación. En esta zona se implementan todos aquellos recursos de la red local que estarán disponibles al público en

general mediante una red externa como el Internet; es decir, que podrán acceder a ciertos recursos de red de la corporación, sin llegar a comprometer todos los recursos como sucedería sin la intervención de la DMZ.

En el presente diseño ciertos recursos de la red de la corporación estarán disponibles para el acceso público, para ello deben estar alojados en un servidor independiente de la red local, que interactuará con la red externa sin permitir el acceso a los recursos de la red interna; es decir, permitiendo acceder únicamente a esta zona desmilitarizada. En esta zona está previsto únicamente un servidor físico web independiente del resto de servidores como se muestra en la anterior **Figura 15** para conservar la integridad de los recursos internos de la red local.

El elemento principal de esta zona desmilitarizada es el Firewall que filtra los distintos tráficos y conexiones tanto entrantes como salientes desde y hacia la red local. Dependiendo del tamaño de la red local y el grado de confidencialidad de la información que maneja la empresa, la zona desmilitarizada será más robusta, de tal forma que permita manejar los distintos tráficos de manera segura, especialmente el tráfico entrante hacia la red local. En definitiva, la DMZ contribuye a solventar los requerimientos de seguridad de la red local por sus funciones descritas; también facilita la administración y paralelamente optimiza el rendimiento de la red debido a la capacidad de filtrado de los distintos tráficos y conexiones. Además, permite garantizar el crecimiento y/o disponibilidad a futuro mediante puertos disponibles que permitirán incluir nuevos recursos de manera segura.

Por último, el enrutamiento hacia redes externas como el Internet está determinado mediante la traducción de las direcciones privadas que maneja la red interna hacia las direcciones públicas suminsitradas por uno o más ISPs. La tracucción de estas direcciones es realizada mediante el mecanismo denominado NAT (Network Address Translation) que se lleva a cabo en el Firewall de la DMZ. Además, se puede establecer una ruta estática por defecto para cualquier petición hacia el exterior a través de una determinada dirección pública provista por el ISP.

4.4. Configuraciones de los equipos

Sobre la topología de la red jerárquica diseñada y descrita en desarrollo de este capítulo es necesario aplicar configuraciones específicas para garantizar los distintos requerimientos técnicos. Dichas configuraciones deben ser realizadas conforme a las capas jerárquicas del presente diseño que son:

Capa de acceso.- A nivel de esta capa las configuraciones están enfocadas en los puertos mediante asignaciones a una determinada VLAN y la restricción de accesos a través de las direcciones MAC de los equipos finales de la red.

Capa de Distribución/ Core.- En esta capa se llevan a cabo las configuraciones en modo servidor, es decir que la mayor parte de las configuraciones debe estar concentrada en estas dos capas. Entre las principales configuraciones están: VTP (VLAN Trunking Protocol), QoS (Quality of Service), manejo de redundancia de enlaces mediante el protocolo STP (Spanning Tree Protocol), VLAN (Virtual LAN) que se implementan en los switches de esta capa; en este caso el SW_CORE_DITRIB_1 y SW_CORE_DITRIB_2.

4.4.1. Creación del dominio VTP en SW_núcleo/distribución

En la topología implementada, es necesario crear un dominio VTP (VLAN Trunking Protocol) para facilitar la administración de las VLAN en la red. La creación se inicia asignando un nombre al dominio y su correspondiente password en cada uno de los switches que conformarán dicho dominio. En el presente trabajo los dos switches de la capa de núcleo/distribución y los 5 switches de la capa de acceso conforman el dominio VTP denominado CONAFIPS. Después, es imperativo establecer el switch que tomará el rol de servidor y los restantes tomarán el rol de clientes del dominio VTP. Los comandos de configuración se pueden observar en el **Anexo 8.1.7**, **Anexo 8.1.8.**

Una vez configurado el dominio VTP, cualquier VLAN que se cree en el switch servidor se replicará automáticamente a los swiches clientes del dominio VTP. En este trabajo están contemplados la creación de 8 VLAN, cada uno con su correspondiente nombre como se muestra en la **Tabla 12** y su configuración en el **Anexo 8.1.9.** Las interfaces VLAN creadas en el switch servidor se deben asignar su correspondiente dirección IP con su máscara, de acuerdo al plan de direccionamiento (**Tabla 12**) para que puedan actuar como Gateway para los equipos finales de los usuarios. Los comandos de configuración se pueden observar en el **Anexo 8.1.10.**

4.4.2. Configuración de enlaces troncales

Después de la creación de las VLAN necesarias en el dominio VTP, es importante establecer los enlaces troncales que interconectan las capas de acceso, distribución y núcleo. Los enlaces troncales son los encargados de manejar el tráfico entre capas, permitiendo el paso de todas o determinadas VLAN existentes en el dominio. En la configuración de cada switch se debe especificar los puertos que trabajarán en modo troncalizado y las VLAN que permitirán el tránsito como se muestra en el **Anexo 8.1.11** y **Anexo 8.1.12** donde se permite el tráfico de todas las VLAN entre la capa de acceso y distribución/núcleo.

4.4.3. Asignación de las VLAN a los puertos de los switches de acceso

En los switches de la capa de acceso, a pesar de que reciben las actualizaciones de las VLAN creadas en el switch servidor de la capa de núcleo/distribución, requieren de configuraciones de sus interfaces que trabajarán con una determinada VLAN; es decir, que cada puerto del switch de acceso tiene asignado máximo dos VLAN en modo de acceso, una para voz y otra para datos como se muestra en el **Anexo 8.1.13.**

La seguridad a nivel de la capa de acceso se puede establecer mediante la restricción por direcciones MAC, estableciendo el número máximo de direcciones MAC permitidas, en este caso se permite máximo una MAC por puerto. En caso de intento de conexión de una segunda MAC, el puerto bloqueará la conexión y generará alertas como se muestra en el **Anexo 8.1.14.**

4.4.4. Configuración de políticas de calidad de servicios (QoS)

La calidad de servicios QoS está definida por las políticas que se puedan establecer en base a la clasificación de los distintos tipos de tráfico, para su posterior marcado y asignación de sus correspondientes prioridades. Una vez definidas las políticas de calidad de servicios se podrán aplicar una política por interfaz, sea esta de entrada o de salida.

La configuración de QoS se inicia con la creación de clases mediante la agrupación de determinados tipos de tráfico de acuerdo a la prioridad que tendrá en el tránsito por la red. En el presente trabajo están contemplados cuatro grupos clasificados de acuerdo a los servicios prioritarios que maneja la corporación, como se muestra a continuación en la **Tabla 17**; siendo el grupo de la clase denominada VOIP la de mayor prioridad, puesto que maneja tráficos sensibles al tiempo como la voz. La configuración de las clases se muestra en el **Anexo 8.2.1.**

Tabla 17.- Clasificación de grupos de servicios prioritarios de la red.

Grupos prioritarios	Servicio	Tráfico	Prioridad DSCP
Muy Alta (VOIP)	Voz, video	udp, rtp, h323	envío expedito (ef)
Alta	Datos críticos	ftp, telnet, ssh	envío asegurado (af41)
Media	Datos medios	http, snmp, syslog	envío asegurado (af31)
Baja	Datos no críticos	pop3, smtp	envío asegurado (af21)

Una vez configuradas los grupos de las clases de tráfico, es necesario asignar un nivel de prioridad a cada uno de los grupos creados anteriormente dentro de una política denominada MARCADO. Los grupos de tráfico pueden ser

asignados hasta con veinte niveles de prioridad a través del campo DSCP que permite brindar calidad de servicios. En el presente trabajo el grupo VOIP que maneja tráfico sensible al tiempo posee un nivel de prioridad DSCP = envío expedito (ef) lo cual es equivalente a la más alta prioridad como se muestra en la anterior **Tabla 17** y su configuración en el **Anexo 8.2.2.**

La política creada con el nombre MARCADO que contiene a los grupos de tráfico creados anteriormente cada uno con su correspondiente prioridad, deben ser aplicados a las interfaces de entrada por donde ingresa el tráfico, en este caso se aplican a las interfaces troncales del switch de la capa de núcleo/distribución. Cabe mencionar que solamente se puede aplicar una política por interface como se muestra en el **Anexo 8.2.3.**

Después, es necesario crear los mismos grupos de tráfico con los mismos niveles de prioridad de entrada pero con la identificación de salida como se muestra en el **Anexo 8.2.4.** Luego crear una política de salida que contenga a dichos grupos creados. En la política de salida QoS-OUT se establecerá el tratamiento que se brindará a los grupos creados e incluidos en esta política de acuerdo al nivel de prioridad con el que se haya marcado al paquete en la entrada con la política de MARCADO. En este caso la política de salida para la clase VOIP-OUT garantizará un determinado ancho de banda y tamaño de cola como se muestra en el **Anexo 8.2.5.**

Por último, la política creada de salida QoS-OUT debe ser aplicada a las interfaces de salida, tomando en cuenta que únicamente se puede aplicar una política por interface como se muestra en el Anexo **Anexo 8.2.6.**

4.4.5. Configuración de STP (Spanning Tree Protocol)

El protocolo spanning tree se autoconfigura entre los switches que componen la topología, eligen el switch raíz (root) a aquel que posea el menor valor de prioridad, en caso de tener un mismo valor todos los switches, se define al root a aquel que posea la dirección MAC con menor valor. Después de definir el switch raíz sus interfaces pasarán a estado forwarding y no de bloqueo. El resto de switches calculan las rutas de menor costo para llegar al switch raíz. El

costo de las rutas están definidas de acuerdo al ancho de banda del enlace, es decir a mayor ancho de banda el costo disminuye y el puerto pasa a ser Root Port por su menor costo. Además, el switch con menor costo será el puente designado y sus puertos hacia el switch root serán puertos designados.

El puente raíz se debe autoconfigurar en el switch de capa de núcleo/distribución, caso contrario si se autoconfigura en alguno de los switches de la capa de acceso, se debe configurar manualmente a los dos switches de la capa nucleo/distribución, uno de ellos como root primario y el otro como root secundario para todas las VLAN's creadas como se muestra en el **Anexo 8.2.7.**

4.4.6. Configuración de la tecnología Etherchannel

La tecnología Etherchannel consiste en asignar dos interfaces a un mismo enlace, es decir el switch reconocerá a las dos interfaces como un solo enlace, es de gran ayuda para mitigar la congestión generada por los cuellos de botella que puedan formase en un determinado enlace.

La configuración se debe realizar en los dos extremos del enlace donde sea necesario la ampliación, agrupando las interfaces que realizarán esta función como se muestra en el **Anexo 8.2.8.**

4.4.7. Configuración de seguridad en el Firewall

La zona desmilitarizada es el módulo del presente trabajo cuya misión es garantizar la seguridad de la red local multiservcios ante amenazas provenientes de redes externas como el internet. Los equipos de la serie ASA 5500 de la marca cisco manejan distintos enfoques de configuración; es decir, la serie 5505 la configuración está basada en interfaces virtuales, mientras que las series más actuales como la serie 5510 la configuración es en base a interfaces físicas, sin embargo las dos series tiene reservadas la primera interfaz física para la salida y el resto para la red interna y la DMZ.

La configuración se inicia con la creación de tres VLAN que se manejaran en el firewall de la DMZ. Una interfaz VLAN está destinada para la salida hacia la red pública configurada con una dirección IP suministrada por un ISP y con un nivel de seguridad mínimo (0). La siguiente VLAN está destinada para la entrada hacia la red local multiservicios que está configurada con una dirección IP privada que actuará como Gateway con un nivel de seguridad máximo (100). La tercera interfaz VLAN está destinada para la DMZ con una dirección IP privada y con un nivel de seguridad medio (50) como se muestra en el **Anexo 8.3.1, Anexo 8.3.2.** y **Anexo 8.3.3.**

Una vez creadas las tres interfaces VLAN de entrada, salida y de la DMZ, es necesario asignar una interfaz física del firewall. La primera interfaz (fastEthernet 0/0) es recomendada para la salida, y el resto para las entradas y la DMZ como se muestra en el **Anexo 8.3.4.** y **Anexo 8.3.5** Después, se deben crear objetos de red para realizar la traducción tanto para la salida como para la entrada de tráfico desde y hacia la red local o la DMZ. Los objetos de red son entidades de configuración que facilitan las traducciones estáticas o dinámicas. En este caso los objetos creados son para la traducción externa, el servidor web, la DMZ y para la traducción interna, como se muestra desde el **Anexo 8.3.6** hasta el **Anexo 8.3.10.**

Por último, es muy importante crear tantas listas de control de acceso ACLs como sean necesarias especificando el tipo de tráfico que se permite o se deniega de acuerdo a las necesidades. Estas listas de acceso se deben aplicar a sus correspondientes interfaces VLAN creadas con anterioridad y sumando la ruta estática de salida de la red local. Las ACL son peticiones permitidas o restringidas para una entidad de red solicitante. Con el afán de mantener segura la red local se han creado ACLs para permitir cualquier petición TCP hacia el exterior, denegar peticiones IP de la red interna hacia la DMZ y permitir peticiones IP desde el exterior hacia la DMZ, como se muestra en el **Anexo 8.3.11, Anexo 8.3.12** y **Anexo 8.3.13.**

5. Capitulo V. Evaluación del presupuesto

5.1. Descripción técnica y económica de los equipos del diseño

5.1.1. Capa de núcleo/distribución

Esta capa de acuerdo al diseño lógico está compuesto por dos switches de capa tres de 24 puertos cada uno que soportarán VLAN's, políticas de QoS, protocolo STP, ACL´s, rutas estáticas, entre otras funcionalidades. En esta capa no es necesario que los puertos de los equipos soporten PoE porque están enlazados a los equipos de la capa de acceso que están alimentados por el sistema eléctrico del cuarto de equipos. A continuación se describe el modelo de switch cisco que se emplea en este diseño.

5.1.2. Switch Cisco de la serie Catalyst 3750X

La nueva serie de la familia de switches catalyst 3750 cubre satisfactoriamente los requerimientos del presente trabajo a nivel de capa tres, puesto que posee mayor capacidad de transferencia de datos en comparación a las anteriores generaciones. Tiene la capacidad de 10/100/1000 Mbps en cada uno de sus puertos y con interfaces troncales opcionales de 1Gbps y 10 Gbps que garantizan el soporte para servicios actuales y futuros que la red pueda brindar a los usuarios (Cisco Systems, 2013).

Figura 16.- Switch 24 puertos Cisco Catalyst 3750X-24TL.

El switch permite brindar calidad de servicios a la red mediante la aplicación de políticas de QoS de acuerdo a los servicios. Soporta con versatilidad las topologías redundantes mediante el protocolo Spanning Tree evaluando de forma automática las mejores rutas entre sus destinos ante cualquier cambio en su topología. Además, soporta el protocolo VTP que se requiere en el presente diseño para la creación de un dominio donde se puedan replicar las VLAN creadas en el switch de esta serie 3750x en la capa de núcleo/distribución. Permite la agregación opcional de enlaces troncales si así lo requiere la topología. Finalmente, permite la administración mediante web, CLI y SNMP (Cisco Systems, 2013).

Por sus principales características detalladas de esta familia Catalyst 3750X se opta como el modelo adecuado para el presente trabajo dos switches de 24 puertos Catalyst 3750X-24T-L. Este equipo no cuenta con tecnología POE en sus salidas, puesto que no hay necesidad de ellos porque tendrán conexión directa hacia los switches de acceso que se alimentan de la toma eléctrica del rack. . El precio promedio en el mercado de este equipo se encuentra en 2400 USD.

5.1.3. Capa de acceso

En la capa de acceso donde los usuarios se conectan directamente a sus interfaces, está integrado por cinco switches de capa dos, de los cuales tres son de 48 puertos y dos switches de 24 puertos. Los equipos de esta capa a diferencia de los switches de la capa de acceso deberán soportar PoE para los dispositivos finales que funcionan con esta tecnología.

5.1.4. Switch Cisco de la serie Catalyst 2960X

La nueva generación de switches Cisco de la serie catalyst 2960 es adecuado para la capa de acceso, puesto que ofrece varias ventajas que contribuyen a optimizar las comunicaciones unificadas a nivel de capa de acceso, como el soporte y priorización del tráfico de voz sobre el tráfico de datos. Posee capacidades de transferencia de datos de 10/100/1000 Mbps en cada uno de sus puertos. Ofrece accesos seguros mediante direcciones MAC asociadas a los puertos del switch, y la creación de VLAN's. Permite la agregación de enlaces troncales en caso de ser necesario una mayor capacidad de los enlaces (Cisco System, 2016).

Figura 17.- Switch 48 puertos Cisco Catalyst 2960X-24PS-L.

Además, contribuye al soporte de las topologías redundantes mediante el manejo por defecto de Spanning Tree. Sus puertos soportan PoE para la

alimentación directa a través del mismo cable de datos a los equipos finales como teléfonos IP, cámaras IP, puntos de acceso, entre otros, sin la necesidad de tener cerca una toma eléctrica. Finalmente, permite la administración mediante web, CLI y SNMP.

En el presente trabajo de acuerdo a los lineamientos del diseño está determinado como los equipos que se ajustan a las necesidades del diseño son tres switches de 48 puertos Cisco Catalyst 2960X-48LPS-L y dos switches de 24 puertos Cisco Catalyst 2960X-24PS-L para la capa de acceso de la red (Cisco System, 2016). El precio promedio en el mercado es de 2290 USD el switch de 48 puertos y 1290 el switch de 24 puertos.

5.1.5. Zona desmilitarizada DMZ

La zona desmilitarizada del presente diseño está conformada por un cortafuego como elemento principal de protección tanto para la red local como para los mismos equipos que conforman la DMZ. A continuación se describe el equipo seleccionado como el ideal para este trabajo.

5.1.6. Cisco serie ASA 5500

Para la protección de nuestra red ante amenazas externas y para mantener un control de tráfico entrante y saliente desde y hacia la red local se requiere de un firewall que realice todo este trabajo y a la vez establecer una zona desmilitarizada para direccionar conexiones entrantes del exterior hacia esta zona donde se alojan ciertos recursos para el público en general, sin permitir el acceso a la red local (Servinet, 2013, pág. 1).

Figura 18.- Dispositivo de seguridad adaptativa Cisco ASA 5510.

El equipo que se adecua a las necesidades del presente trabajo es el firewall cisco ASA 5510 que tiene 300 Mbps de capacidad de cortafuegos, maneja tasas de conexiones de hasta 6000 sesiones por segundo, soporta hasta 50 túneles VPN, maneja hasta 50 interfaces virtuales VLAN y sus algoritmos de cifrado son DES, AES y Triple DES, por último, el dispositivo permite la administración mediante web, CLI y SNMP (Servinet, 2013, pág. 2). El precio promedio de este equipo en el mercado se encuentra alrededor de 1190 USD.

5.1.7. Servidores HP Prolyant

Los servidores de la marca HP de la familia Prolyant son servidores que garantizan rendimiento, capacidad, disponibilidad, crecimiento y la facilidad acceso al soporte técnico. En el presente trabajo se opta por el servidor de rack HP Proliyant DL380P G8 que solventa de manera satisfactoria los requerimientos de servicios actuales y futuros a ofrecer en la red de la corporación (Hewlett Packard, 2015).

Figura 19.- Servidor HP Prolyant DL380P G8.

Las principales características que posee este servidor son: procesador Xeon E5-2670 de 2,6 GHz, memoria cache de 20 MB, memoria RAM con capacidad de hasta 128 GB, capacidad de almacenamiento hasta 4 x 600GB y cuatro puertos 1GE. Este servidor está destinado para la red interna de la corporación, de tal manera para ciertos servicios para la red externa se requiere un servidor de menores características como el micro servidor HP Prolyant G8 que cuenta con procesador Intel Xeon Dual Core con 8GB de memoria y 1Tb de capacidad que estará ubicado en la DMZ como servidor web (Hewlett Packard, 2015). El precio promedio en el mercado del primer servidor descrito es 4800 USD, mientras que el segundo de menores prestaciones tiene un precio promedio de 1250 USD.

5.1.8. Network Video Recorder NVR Hikvision

Para brindar el servicio de video vigilancia sobre la red multiservicios es necesario un NVR donde se guardarán de manera centralizada todos los eventos capturados por las videocámaras IP de la red local. La marca Hikvision posee varias ventajas en sus equipos de video de acuerdo a los requerimientos en lo relativo al número de cámara y/o el tiempo de grabación (Neotech, 2011, pág. 1).

Figura 20.- Network Video Recorder NVR Hikvision DS-7608NI-SE.

El tiempo de grabación de video depende del número de cámaras IP, la resolución del video, la capacidad de los discos duros que se agreguen al NVR, en este caso se recomienda utilizar dos discos duros de 4TB cada uno para obtener un tiempo máximo de grabación. Para el presente trabajo se ajusta de manera satisfactoria el NVR Hikvision DS-7608NI-SE que cuenta con ocho canales con una resolución de hasta 5 Mega píxeles cada una, trabaja con el formato de compresión de video H.264. Soporta tasas de transferencia de 10/100/1000 Mbps en sus interfaces de red. Posee interfaces de salida de video VGA, HDMI y un puerto USB para la administración directa del NVR (Neotech, 2011, pág. 1). El precio promedio de este equipo en el mercado es 460 USD y el disco duro de 4TB 190 USD cada una.

5.1.9. Cámara IP Hikvision

Las cámaras Ip de la marca Hikvision ofrecen una gran calidad de imagen tanto en el día como en la total oscuridad de la noche, dependiendo del modelo y las necesidades. En este trabajo se consideran además los ambientes donde estarán ubicados las cámaras IP, es decir que estarán ubicados en los exteriores del edificio o a la intemperie para capturar los eventos durante las 24 horas del día en siete puntos estratégicos del edificio (Neotech, 2013, pág. 1).

Figura 21.- Cámara IP Hikvision DS-2CD2010-I.

El modelo de cámara IP que se ajusta a estas condiciones es el Hikvision DS-2CD2010-I, que posee una resolución de 1,3 Mega píxeles, puede trabajar con formatos de video compresión H.264 o MJPEG. La tasa de transferencia de bits oscila entre 32 Kbps y 16Mbps. Trabaja con alimentación PoE que suministran los switches de acceso de este diseño (Neotech, 2013, pág. 1). El precio referencial de este equipo en el mercado está alrededor de 120 USD cada una.

5.1.10. Teléfono IP Cisco

Figura 22.- Teléfono IP Cisco SPA-303G1.

Los teléfonos IP de Cisco además de su calidad como en todos sus equipos, ofrecen múltiples ventajas para los usuarios y administradores de la red. Existen varios modelos de teléfonos IP, en este caso se opta por un teléfono con funciones intermedias, pero que satisfagan las necesidades de comunicación entre los usuarios de la red de la corporación. En tal virtud, el modelo que se ajusta a dichos requerimientos es el Teléfono IP Cisco SPA-303G1 que permite configurar hasta tres extensiones telefónicas, maneja el protocolo SIP, soporta calidad de servicios QoS, maneja codecs G.711, G.726, G.729, G.722, permite ajustar el buffer para mejorar el jitter. Por último, internamente contiene un microswitch que extingue la necesidad de dos salidas de telecomunicaciones en una estación de trabajo, es decir un patch cord conecta de la salida de telecomunicaciones (PoE) al teléfono y del teléfono a la tarjeta de red de la PC (Cisco System, 2010).

Cabe mencionar que a pesar de sus múltiples ventajas de estos teléfonos, debido a sus costos en este trabajo están previstos únicamente 21 teléfonos destinados para los directores y ejecutivos de la corporación, para el resto de usuarios de la red está contemplado el uso de Sofphone soportado por el servidor Asterisk para ahorrar costos en equipamiento y aprovechando la versatilidad de este modelo de teléfono IP. El precio promedio de este modelo de teléfono es 184 USD.

5.1.11. Access point Ubiquiti

Existen una gama de marcas, modelos y prestaciones de este tipo de equipos, pero para el presente trabajo la marca Ubiquiti es ideal debido a que cuenta con varias ventajas en lo relativo a las prestaciones técnicas frente a su precio razonable (UBNT, 2016).

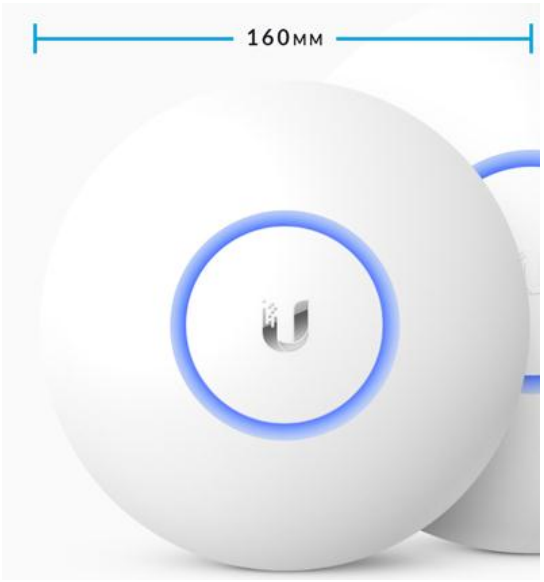


Figura 23.- Access point Ubiquiti UAP-AC-LITE.

En este trabajo debido a que no se considera como servicio prioritario el acceso de datos inalámbrico para los usuario de la corporación y para ahorrar costos se opta por una marca no muy conocida pero de excelente rendimiento y un precio razonable como es el Ubiquiti modelo UAP-AC-LITE, que es ideal para interiores, alcanza hasta 300Mbps trabajando en la banda de 2,4GHz y hasta 867Mbps en la banda de 5GHz, cuenta con un puerto PoE de 10/100/1000 Ethernet (UBNT, 2016). Su precio promedio en el mercado es de 160 USD.

5.1.12. Panel de alarma contra incendios

Figura 24.- Panel de alarma inteligente contra incendios.

La seguridad contra incendios en un edifico comercial se puede reforzar a través de políticas de prevención y sistemas de alerta que ayudan a reducir riesgos de desastres por incendios. El sistema de alarma previsto en este trabajo es el panel de alarma contra incendios de la prestigiosa marca Bosch modelo FPD-7024. Este sistema cuenta con un set completo de sensores térmicos y/o de humo, así como los dispositivos para la activación manual de la alarma mediante palancas manuales para la activación de sirenas auditivas (Rigotech, 2009). Además, este panel permite el monitoreo de alarmas a través de la red local multiservicios desde una estación de monitoreo, permitiendo registrar los eventos y anticiparse de una manera ágil. El precio referencial en el mercado de este equipo es de 590 USD.

5.1.13. Control de acceso

Figura 25.- Control de acceso biométrico ZKTECO U100.

Una de las aplicaciones del sensor biométrico es la identificación para llevar un control adecuado de la asistencia y puntualidad de los colaboradores de una empresa, sobre todo cuando existe un número significativo en su nómina. El equipo elegido por sus prestaciones que se ajustan a los requerimientos del presente trabajo es el ZKTECO U100 que permite la conexión a la red multiservicios, soporta hasta 3200 usuarios registrando huellas dactilares y password, posee una velocidad de verificación de 1 segundo con margen de error de 0,0001% (Zkateco, 2015). Además, posee sistema operativo Kernel Linux y puede trabajar en modo offline si no se encuentra en red por algún motivo. El precio promedio de este dispositivo en el mercado es de 190 USD.

5.2. Presupuesto general para la implementación

El presupuesto estimado del presente proyecto se desarrolla en base a los equipos determinados como idóneos por sus características técnicas y económicas señaladas en el presente capítulo. Estos equipos satisfacen los requerimientos del presente trabajo y por su fácil accesibilidad en el mercado a

través de distintos proveedores. A continuación en la **Tabla 18** se presenta un resumen de los precios unitarios, parciales y el costo total de los equipos activos inherentes al proyecto.

Tabla 18.- Proforma de los elementos activos del proyecto.

Cantidad	Descripción	Precio Unitario	Total
2	Catalyst 3750X-24TL (Capa 3)	$ 2.400,00	$ 4.800,00
3	Catalyst 2960X-48PS-L (acceso)	$ 2.290,00	$ 6.870,00
2	Catalyst 2960X-24PS-L (acceso)	$ 1.290,00	$ 2.580,00
1	ASA 5510	$ 1.190,00	$ 1.190,00
1	Servidor HP Prolyant DL380P G8	$ 4.800,00	$ 4.800,00
1	Micro servidor HP Prolyant G8	$ 1.250,00	$ 1.250,00
1	NVR Hikvision DS-7608NI-SE	$ 460,00	$ 460,00
4	Disco duro 4TB	$ 190,00	$ 760,00
7	Cámara IP Hikvision DS-2CD2010-I	$ 120,00	$ 840,00
21	Teléfono IP Cisco SPA-303G1	$ 184,00	$ 3.864,00
2	Access point Ubiquiti UAP-AC-LITE	$ 160,00	$ 320,00
1	Panel de alarma FPD-7024	$ 590,00	$ 590,00
3	Control biométrico ZKTECO U100	$ 190,00	$ 570,00
2	UPS APC 3KVA	$ 1.145,00	$ 2.290,00
		Total (USD)	$ 31.184,00

Dentro del presupuesto se encuentran clasificados como elementos pasivos el resto de implementos complementarios de la infraestructura de red. A continuación en la **Tabla 19** se muestra el listado de los implementos estimados para el proyecto con su correspondiente precio unitario y total cotizado en el mercado.

Tabla 19.- Proforma de los elementos pasivos de proyecto.

Cantidad	Descripción	Precio Unitario	Total
2	Rack de piso 32 UR 60x80x160	$ 759,00	$ 1.518,00
120	Pacth cord 3fts cat 6A	$ 4,51	$ 541,20
11	Patch panel modular 24 puertos cat 6A	$ 23,00	$ 253,00
188	Jack de patch panel cat 6A	$ 4,81	$ 904,28
15	Organizador horizontal 2UR	$ 12,89	$ 193,35
50	Blank blank negro	$ 0,32	$ 16,00
5	Multitoma Eléctrica	$ 26,84	$ 134,20
1	Rack de pared_12 UR 600x450x635mm	$ 189,75	$ 189,75
72	Pacth cord 3fts cat 6A	$ 4,51	$ 324,72
5	Organizador horizontal 1UR	$ 10,16	$ 50,80
410	Bandejas/Rejillas metálicas Mts 30x5x3 mts	$ 24,16	$ 9.905,60
3	Tuberia de Ø 50mm mts	$ 2,56	$ 7,68
2	Codos de Ø 50mm	$ 0,63	$ 1,26
410	Canaleta mediana 2 canales mts 60x40	$ 4,93	$ 2.021,30
32	Face Plate simple	$ 1,39	$ 44,48
63	Face Plate doble	$ 1,57	$ 98,91
158	Patch cord cat 6A 7 fts	$ 6,33	$ 1.000,14
158	Jack cat 6A	$ 4,81	$ 759,98
158	Caja sobrepuesta	$ 1,54	$ 243,32
16	Bobina cable UTP CAT 6A	$ 327,53	$ 5.240,48
		Total (USD)	$ 23.448,45

Cabe mencionar que las dos listas de precios son referenciales cotizados entre distintos proveedores de las cuales se ha seleccionado la mejor opción en el ámbito económico.

5.3. Análisis del presupuesto general del proyecto

El presupuesto general del presente proyecto está conformado por dos grupos clasificados en elementos activos y pasivos, mostrados en las dos tablas anteriores, danto un total de $ 54.632,45 dólares americanos a la fecha entre los dos grupos. Este valor total es conveniente económicamente, puesto que se han seleccionado las mejores ofertas entre distintos proveedores de cada equipo.

Finalmente, para contrastar los valores totales de los implementos del proyecto se muestra como ejemplo un presupuesto general de un proveedor en particular en la proforma mostrada en el **Anexo 8.3.14** con un total $ 71.764,79 dólares americanos.

Los valores señalados en este capítulo no están incluidos los impuestos, y varían dependiendo del proveedor. Los valores totales presupuestados en este análisis quedan a consideración entorno al ámbito económico de la empresa y de sus recursos disponibles para la ejecución del proyecto.

6. Capítulo VI. Conclusiones y recomendaciones

6.1. Conclusiones

En relación al desarrollo del presente trabajo de diseño de la red multiservicios y el cumplimiento de los objetivos, se puede concluir lo siguiente:

La fundamentación teórica se ha desarrollado a través de la metodología exploratoria con la finalidad de extraer la información apropiada para la realización del presente proyecto.

El análisis de los requerimientos ha sido desarrollado mediante la inspección y determinación de los servicios indispensables para la corporación; de esta manera, contribuyendo a realizar una planificación adecuada de los recursos e implementos necesarios para el desarrollo de la red multiservicios propuesto del presente trabajo.

El dimensionamiento de los recursos de red ha sido determinado en base a la triangulación de la información referente al número de usuarios, dimensiones de los espacios físicos disponibles en base a los planos del edificio comercial y los requerimientos de crecimiento, disponibilidad, seguridad, calidad de servicios, facilidad de mantenimiento y administración.

La metodología de diseño Top-Down seleccionada para el desarrollo del presente diseño posee cuatro fases que se ajustan satisfactoriamente a los objetivos del presente trabajo. De las cuatro fases se desarrollan sólo las tres primeras debido a que este trabajo se enfoca en el diseño.

La primera fase de análisis de requerimientos de diseño de la metodología Top-Down se ha desarrollado mediante la inspección de necesidades referentes a los servicios, escalabilidad, seguridad, rendimiento, administración, mantenimiento y los espacios físicos que disponen en la actualidad esquematizados en planos.

La fase de diseño lógico de la red de la metodología Top-Down se ha desarrollado como consecuencia de la primera fase; es decir, tomando en cuenta los requerimientos iniciales para establecer y aplicar un plan de

direccionamiento, tecnologías, protocolos y topologías que satisfagan dichos requerimientos.

La fase de diseño físico de la red de la metodología Top-Down se ha desarrollado mediante el análisis de los requerimientos, los espacios físicos inspeccionados en la primera fase y conforme a los lineamientos establecidos por la norma TIA/EIA 568 referentes al cableado estructurado.

La fase cuarta y última de la metodología Top-down no se emplea en su totalidad puesto que el presente trabajo está enfocado en el diseño, pero permite la viabilidad de la aplicación total de esta fase en caso de ser implementado. El lineamiento de documentación de esta fase se ha considerado aplicable en este trabajo para fines de optimización del diseño.

La disponibilidad de la red se ha conseguido mediante la implementación de una topología redundante y soportada por el protocolo STP para evitar bucles lógicos por enlaces redundantes hacia un mismo destino.

La escalabilidad de la red se ha garantizado de manera física y lógica a través de la disponibilidad y reservación de recursos de red para el crecimiento a futuro. Dentro de los recursos principales previstos están la disponibilidad de puertos en las tres capas jerárquicas, disponibilidad de direcciones IP de acuerdo al plan de direccionamiento y las prestaciones del equipamiento para soportar esta exigencia.

La seguridad de la red diseñada se ha conseguido mediante la implementación de mecanismos de restricción a nivel de cada capa de la topología jerárquica. Dentro de los principales mecanismos de seguridad del diseño se encuentran: la restricción de los puertos de los switches, la segmentación por VLANs, las listas de acceso (ACLs), la inclusión de una zona desmilitarizada (DMZ) como intermediario entre la red local y la red pública.

La calidad de servicios soportada por la red se ha establecido mediante la priorización de determinados tipos de tráfico de acuerdo al análisis de los requerimientos de los servicios imprescindibles que debe manejar la corporación como la voz y el sistema financiero contable.

El equipamiento del diseño se ha seleccionado en función de los requerimientos del diseño y las prestaciones que poseen cada uno de ellos para satisfacer las exigencias de los servicios actuales y futuros mínimo de hasta diez años.

6.2. Recomendaciones

En relación al desarrollo del diseño propuesto de la red multiservicios se pueden realizar las siguientes recomendaciones:

La implementación del presente diseño es recomendable que sea ejecutada continuando con los lineamientos que establece la metodología Top-Down empleada hasta la tercera fase.

Los teléfonos IP previstos para ciertos usuarios ejecutivos de la red diseñada en el presente trabajo pueden ser reemplazados en su totalidad por las aplicaciones softphones en la etapa de implementación para reducir costos en cuanto al equipamiento telefónico IP.

Los servidores virtuales internos alojados en el servidor físico pueden ser redistribuidos sobre uno o varios servidores físicos, dependiendo de la viabilidad económica de la empresa y del costo-beneficio. Esta redistribución de los servidores es posible gracias al diseño escalable de la red que se traduce en el incremento del rendimiento, la disponibilidad, facilidad de mantenimiento y administración de la red.

En el caso de la implementación del cableado estructurado de la red diseñada en el presente trabajo es recomendable ejecutar el proceso de certificación para determinar su estado inicial en términos de rendimiento. Las pruebas de certificación que se realicen al cableado estructurado, deberán ser documentadas para fines de mantenimiento y administración de la red.

Establecer una política de nomenclatura que identifique cada uno de los componentes del cableado estructurado de la red de tal manera que facilite las tareas de mantenimiento y administración de la infraestructura de la red.

Es recomendable monitorear la red operativa mediante software especializado para verificar el comportamiento de la red con tráfico en tiempo real y determinar posibles deficiencias que pueden ser corregidas u optimizadas por el administrador.

Para la conectividad de la red local hacia el Internet es recomendable contratar dos enlaces, uno principal y el otro como enlace de respaldo, de preferencia de distintos proveedores para garantizar la disponibilidad de este servicio. Si los dos enlaces son suministrados por el mismo proveedor de Internet deben ser independientes el uno del otro.

Finalmente, es recomendable desarrollar un manual de procedimientos estandarizados con instrucciones puntuales para la resolución de un determinado fallo que se pueda presentar en la red operativa y todos aquellos posibles problemas que puedan presentarse de manera eventual. Las nuevas fallas que se presenten también deben ser incluidas en el manual con los pasos realizados para la resolución.

REFERENCIAS

Briceño, J., & Amalia, M. (2011). *Cableado y estructurado de redes*. Recuperado el 20 de diciembre de 2015 de http://www.electronica.7p.com/cableado/equipos.htm

Btcino. (2011). *TIA/EIA-568-B Norma de Cableado de Telecomunicaciones para Edificios Comerciales*. Recuperado el 20 de diciembre de 2015 de http://bibdigital.epn.edu.ec/bitstream/15000/9268/5/Cap%204.pdf

Cablered. (2010). *Cableado estrucurado*. Recuperado el 13 de diciembre de 2015 de http://wwwcableredcom.blogspot.com/

Cajaleón, D. (2013). *Metodologías de Redes*. Recuperado el 10 de octubre de 2015 de http://metodologiasredes.blogspot.com/

CCM Benmarch Group. (2015). *Introducción a Wi-Fi (802.11 o WiFi).* Recuperado el 6 de septiembre de 2015 de http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi

CISCO. (2010). *CCNA3. Conmutación y conexión inalámbrica de LAN.* México: http://www.systemconsultores.com/data/carpetas/2/CCNA3_Capitulo%201%20Diseno%20de%20la%20LAN.pdf.

CISCO. (2015). *CCNA4 Routing and Switching.* Recuperado el 30 de septiembre de 2015 de https://juliorestrepo.files.wordpress.com/2015/03/pdf_ccna4_v5.pdf

CISCO. (2015). *Cisco EtherChannel Technology*. Recuperado el 9 de octubre de 2015 de http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml

Cisco System. (2016). *Cisco Catalyst 2960-X Series Switches Data Sheet.* Recuperado el 8 de enero de 2016 de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html

Cisco System. (2010). *Cisco SPA 303 3-Line IP Phone Data Sheet.* Recuperado el 8 de enero de 2016 de http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/small-business-spa300-series-ip-phones/data_sheet_c78-601648.html

Cisco Systems. (2013). *Cisco Catalyst 3750-X and 3560-X Series Switches Data Sheet.* Recuperado el 8 de enero de 2016 de

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-x-series-switches/data_sheet_c78-584733.html

CISCO. (2013). *Voz sobre IP - Consumo de ancho de banda por llamada*. Recuperado el 24 de agosto de 2015 de http://www.cisco.com/cisco/web/support/LA/102/1024/1024085_bwidth_consume.html

Contreras, O., & Contreras, N. (2012). *Modelo matemático para la predicción de ancho de banda*. Recuperado el 16 de noviembre de 2015 de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0ahUKEwi1hK2TpujKAhUD2B4KHTyNCGYQFghHMAc&url=http%3A%2F%2Fsistemamid.com%2Fdownload.php%3Fa%3D3918&usg=AFQjCNHeEHVH3ciUQD3IN8_DySRUw1XnZQ

Cura, N. J. (2007). *Redes Privadas Virtuales VPN.* Recuperado el 6 de septiembre de 2015 de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCMQFjABahUKEwiYkqCVp-rHAhWBGx4KHRwiAwQ&url=http%3A%2F%2Futn-frc-com.googlecode.com%2Fsvn%2Ftrunk%2FApuntes%2FUnidad%25206%2FSeguridad-vpn.pdf&usg=AFQjCNG-YDWQyvrAIsMuRuCtT5FR3JC7ag&c

Edwin, R. (2009). *Tecnología VoIP y Telefonía IP La Telefonía por Internet.* Bolivia: Priale.

Erazo, C. (2009). *Implantación de Calidad de Servicios en Redes Inalámbricas Wi-Fi.* México DF: Instituto Politécnico.

García, T. (2007). *Análisis de los modelos de servicios diferenciales y servicios integrales para brindar QoS en internet.* Oaxaca: Edixaca.

Haivision. (2012). *Latencia de video*. Recuperado el 23 de agosto de 2015 de http://www.imaginart.es/pdf/haivision_explicacion_latencia.pdf

Hewlett Packard. (2015). *HP ProLiant DL380p Generation8 (Gen8).* Recuperado el 9 de enero de 2016 de http://www8.hp.com/h20195/v2/GetHTML.aspx?docname=c04123238

IETF. (1998). *Definition of the Differentiated Services Field (DS Field).* Recuperado el 6 de septiembre de 2015 de https://tools.ietf.org/html/rfc2474

IETF. (2010). *IAX: Inter-Asterisk eXchange Version 2*. Recuperado el 23 de agosto de 2015 de https://tools.ietf.org/html/rfc5456#page-4

Ipreference. (2008). *El modelo jerárquico de 3 capas de Cisco*. Recuperado el 19 de julio de 2015 de https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

ITESA. (2010). *Descripción general del diseño de redes jerárquicas*. Recuperado el 19 de julio de 2015 de http://www.itesa.edu.mx/netacad/networks/course/module1/1.1.2.1/1.1.2.1.html

Joskowicz, J. (2013). *Voz, video y telefonía sobre IP.* Montevideo-Uruguay: Universidad de la República.

Lino, J. (2011). *Gestión y administración de redes*. Recuperado el 16 de enero de 2016 de http://www.buenastareas.com/ensayos/Gestion-y-Administracion-De-Redes/2539674.html

Lopez, D. (2009). *Modelo de redes jerárquicas*. Recuperado el 19 de julio de 2015 de http://blogxdextecnologia.blogspot.com/2009/07/modelo-de-redes-jerarquicas.html

López, I. (2014). *Confidencialidad, integridad y disponibilidad de la información.* Recuperado el 15 de mayo de 2015 de http://www.belt.es/expertos/experto.asp?id=2245

Marín, A. (2008). *Análisis de la calidad experimentada en aplicaciones de voz sobre IP*. Recuperado el 25 de agosto de 2015 de http://repositorio.bib.upct.es/dspace/bitstream/10317/719/1/pfc2756.pdf

Milagros, S. (2013). *Metodologías para implementar proyectos de redes*. Recuperado el 19 de julio de 2015 de http://metodologiaspararedes.blogspot.com/

Millan, .. R. (2008). *Redes y servicios de telecomunicaciones.* Recuperado el 7 de septiembre de 2015 de http://blogtelecomunicaciones.ramonmillan.com/2008/06/principales-diferencias-entre-h323-y.html

Neotech. (2013). *Hikvision IR Mini Bullet Camera.* Recuperado el 9 de enero de 2016 de http://neotech.ge/wp-content/uploads/2014/05/datasheet_DS-2CD2010-I.pdf

Neotech. (2011). *Hikvision NVR 7600 Series Datashet.* Recuperado el 9 de enero de 2016 de http://neotech.ge/wp-content/uploads/2014/05/nvr_7600sp.pdf

Phifer, L. (2012). *Herramientas para mejorar el rendimiento de vídeo inalámbrico II*. Recuperado el 23 de agosto de 2015 de http://searchdatacenter.techtarget.com/es/consejo/Herramientas-para-mejorar-el-rendimiento-de-video-inalambrico-II

Quang Dung Technology. (2010). *Standart ANSI/TIA/EIA 568-B*. Recuperado el 20 de diciembre de 2015 de http://www.csd.uoc.gr/~hy435/material/Cabling%20Standard%20-%20ANSI-TIA-EIA%20568%20B%20-%20Commercial%20Building%20Telecommunications%20Cabling%20Standard.pdf

Rigotech. (2009). *FPD-7024 Paneles de Control de Alarma de Incendio.* Recuperado el 9 de enero de 2016 de http://www.rigotech.com.ec/docs/catalog/prod_141/FPD-7024.pdf

Sáez, A. (2007). *Estudio de H.323 y SIP.* Recuperado el 8 de septimbre de 2015 de http://www.grc.upv.es/docencia/tdm/trabajos2007/Abel_H.323%20vs%20SIP%20%281%29.pdf

Sanmartín, D. Z. (2009). *Análisis y evaluación del efecto que tendría una regulación de redes multiservicios*. Recuperado el 4 de mayo de 2015 de http://www.dspace.espol.edu.ec/bitstream/123456789/13472/3/PRESENTACION.pdf

Servinet. (2013). *Firewall Cisco ASA 5510 Datashet.* Recuperado el 9 de enero de 2016 de http://www.servinet.net/Portals/122/Especificaciones%20T%C3%A9cnicas%20Firewall%20Cisco%20ASA%205510.pdf

Sistemasumma. (2012). *Redes Jerárquicas*. Recuperado el 19 de julio de 2015 de http://sistemasumma.com/2012/02/19/redes-jerarquicas/

Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras.* Estado de México: Perason educación.

Thales Security. (2015). *Datacryptor Link and Layer 2 Encryption.* Recuperado el 20 de agosto de 2015 de https://www.thales-esecurity.com/products-and-services/products-and-services/network-encryption-appliances/datacryptor-link-and-layer-2-encryption

Toro, J. (2011). *Estudio y diseño de una red de cableado estructurado.* Recuperado el 20 de diciembre de 2015 de http://bibdigital.epn.edu.ec/bitstream/15000/4402/1/CD-4005.pdf

Turmero, P. (2010). *Administración del control de accesos, adecuado a los sistemas de información.* Recuperado el 6 de mayo de 2015 de http://www.monografias.com/trabajos102/administracion-del-control-accesos-adecuado-sistemas-informacion/administracion-del-control-accesos-adecuado-sistemas-informacion.shtml

UBNT. (2016). *UniFi® AC APs Datasheet.* Recuperado el 9 de enero de 2016 de https://www.ubnt.com/download/unifi/default/default/unifi-ac-aps-datasheet

Unipanamericana. (2012). *Redes Multiservicios*. Recuperado el 4 de mayo de 2015 de http://redesmultiservicios.weebly.com/

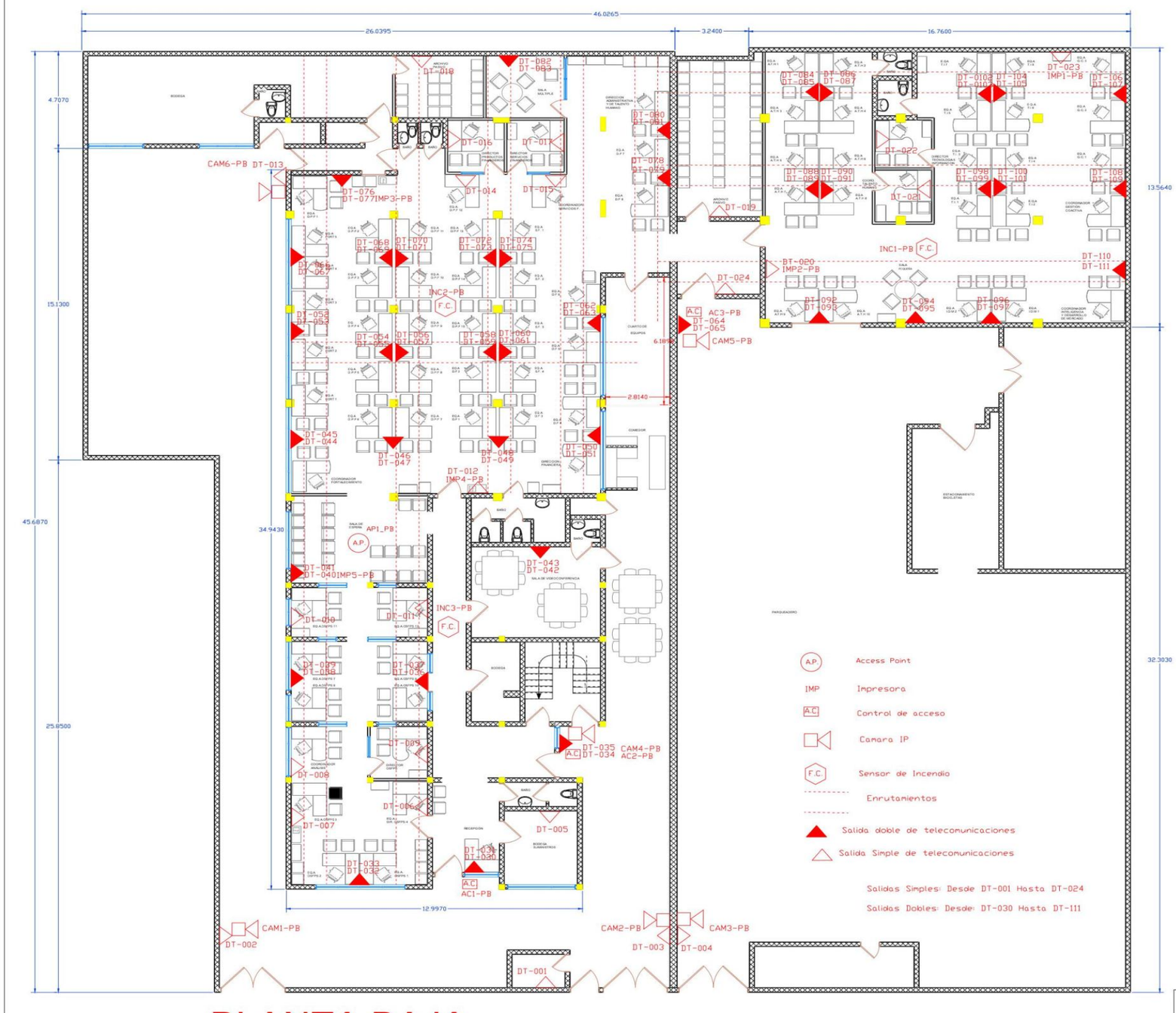
Vilajosana, X., Font, M., Llorente, S., & Marqués, J. (2010). *Redes Multimedia.* Barcelona-España: Eureca Media, S. L.

VoipForo. (2015). *Comparación entre IAX y SIP.* Recuperado el 8 de septiembre de 2015 de http://www.voipforo.com/IAX/IAXvsSIP.php

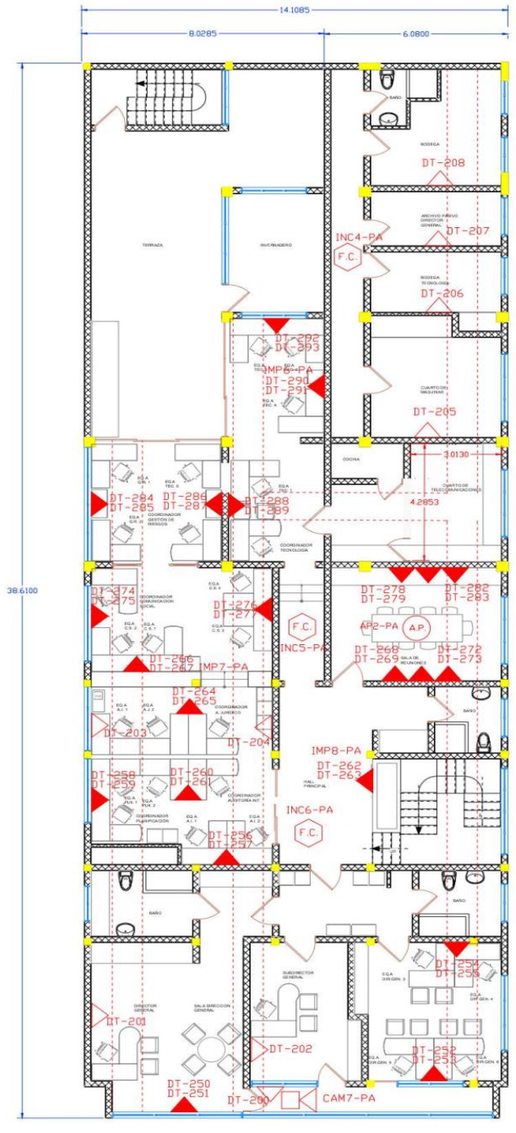
Zkateco. (2015). *Control de acceso biométrico.* Recuperado el 9 de enero de 2016 de http://www.zktecolatinoamerica.com/

ANEXOS

8.1.1. Diagrama esquematizado de red física del edificio



PLANTA BAJA



PLANTA ALTA

ANEXO 1-2 CONAFIPS 2016

8.1.2. Distribución y asignación de puertos del Switch de Acceso 1

PUERTO	DEPARTAMENTO	UBIC.	VLAN A	DIRECCIÓN IP	MSK.	VLAN B	DIRECCIÓN IP	MSK.
1	Recepción	DT-031	VLAN_VOZ	192.168.1.2	/24	VLAN_DATOS	192.168.2.2	/24
2	Dir. de Desarrollo OSFPS	DT-032	VLAN_VOZ	192.168.1.3	/24	VLAN_DATOS	192.168.2.3	/24
3	Dir. de Desarrollo OSFPS	DT-033	VLAN_VOZ	192.168.1.4	/24	VLAN_DATOS	192.168.2.4	/24
4	Dir. de Desarrollo OSFPS	DT-006	VLAN_VOZ	192.168.1.5	/24	VLAN_DATOS	192.168.2.5	/24
5	Dir. de Desarrollo OSFPS	DT-007	VLAN_VOZ	192.168.1.6	/24	VLAN_DATOS	192.168.2.6	/24
6	Dir. de Desarrollo OSFPS	DT-008	VLAN_VOZ	192.168.1.7	/24	VLAN_DATOS	192.168.2.7	/24
7	Dir. de Desarrollo OSFPS	DT-009	VLAN_VOZ	192.168.1.8	/24	VLAN_DATOS	192.168.2.8	/24
8	Dir. de Desarrollo OSFPS	DT-036	VLAN_VOZ	192.168.1.9	/24	VLAN_DATOS	192.168.2.9	/24
9	Dir. de Desarrollo OSFPS	DT-037	VLAN_VOZ	192.168.1.10	/24	VLAN_DATOS	192.168.2.10	/24
10	Dir. de Desarrollo OSFPS	DT-038	VLAN_VOZ	192.168.1.11	/24	VLAN_DATOS	192.168.2.11	/24
11	Dir. de Desarrollo OSFPS	DT-039	VLAN_VOZ	192.168.1.12	/24	VLAN_DATOS	192.168.2.12	/24
12	Dir. de Desarrollo OSFPS	DT-010	VLAN_VOZ	192.168.1.13	/24	VLAN_DATOS	192.168.2.13	/24
13	Dir. de Desarrollo OSFPS	DT-011	VLAN_VOZ	192.168.1.14	/24	VLAN_DATOS	192.168.2.14	/24
14	Dir. de Desarrollo OSFPS	DT-044	VLAN_VOZ	192.168.1.15	/24	VLAN_DATOS	192.168.2.15	/24
15	Dir. de Desarrollo OSFPS	DT-045	VLAN_VOZ	192.168.1.16	/24	VLAN_DATOS	192.168.2.16	/24
16	Dir. de Desarrollo OSFPS	DT-052	VLAN_VOZ	192.168.1.17	/24	VLAN_DATOS	192.168.2.17	/24
17	Dir. de Desarrollo OSFPS	DT-053	VLAN_VOZ	192.168.1.18	/24	VLAN_DATOS	192.168.2.18	/24
18	Dir. de Desarrollo OSFPS	DT-066	VLAN_VOZ	192.168.1.19	/24	VLAN_DATOS	192.168.2.19	/24
19	Dir. de Desarrollo OSFPS	DT-067	VLAN_VOZ	192.168.1.20	/24	VLAN_DATOS	192.168.2.20	/24
20	Dir. de Productos Financeros	DT-016	VLAN_VOZ	192.168.1.21	/24	VLAN_DATOS	192.168.2.21	/24
21	Dir. de Productos Financeros	DT-076	VLAN_VOZ	192.168.1.22	/24	VLAN_DATOS	192.168.2.22	/24
22	Dir. de Productos Financeros	DT-068	VLAN_VOZ	192.168.1.23	/24	VLAN_DATOS	192.168.2.23	/24
23	Dir. de Productos Financeros	DT-069	VLAN_VOZ	192.168.1.24	/24	VLAN_DATOS	192.168.2.24	/24
24	Dir. de Productos Financeros	DT-070	VLAN_VOZ	192.168.1.25	/24	VLAN_DATOS	192.168.2.25	/24
25	Dir. de Productos Financeros	DT-071	VLAN_VOZ	192.168.1.26	/24	VLAN_DATOS	192.168.2.26	/24
26	Dir. de Productos Financeros	DT-054	VLAN_VOZ	192.168.1.27	/24	VLAN_DATOS	192.168.2.27	/24
27	Dir. de Productos Financeros	DT-055	VLAN_VOZ	192.168.1.28	/24	VLAN_DATOS	192.168.2.28	/24
28	Dir. de Productos Financeros	DT-056	VLAN_VOZ	192.168.1.29	/24	VLAN_DATOS	192.168.2.29	/24
29	Dir. de Productos Financeros	DT-057	VLAN_VOZ	192.168.1.30	/24	VLAN_DATOS	192.168.2.30	/24
30	Dir. de Productos Financeros	DT-046	VLAN_VOZ	192.168.1.31	/24	VLAN_DATOS	192.168.2.31	/24
31	Dir. de Productos Financeros	DT-047	VLAN_VOZ	192.168.1.32	/24	VLAN_DATOS	192.168.2.32	/24
32	Dir. de Productos Financeros	DT-014	VLAN_VOZ	192.168.1.33	/24	VLAN_DATOS	192.168.2.33	/24
33	Dir. de Productos Financeros	DT-072	VLAN_VOZ	192.168.1.34	/24	VLAN_DATOS	192.168.2.34	/24
34	Dir. de Productos Financeros	DT-073	VLAN_VOZ	192.168.1.35	/24	VLAN_DATOS	192.168.2.35	/24
35	Dir. de Productos Financeros	DT-058	VLAN_VOZ	192.168.1.36	/24	VLAN_DATOS	192.168.2.36	/24
36	Dir. Administrativa y de TTHH	DT-080	VLAN_VOZ	192.168.1.37	/24	VLAN_DATOS	192.168.2.37	/24
37	Dir. Administrativa y de TTHH	DT-081	VLAN_VOZ	192.168.1.38	/24	VLAN_DATOS	192.168.2.38	/24
38	Dir. Administrativa y de TTHH	DT-021	VLAN_VOZ	192.168.1.39	/24	VLAN_DATOS	192.168.2.39	/24
39	Dir. Administrativa y de TTHH	DT-084	VLAN_VOZ	192.168.1.40	/24	VLAN_DATOS	192.168.2.40	/24
40	Dir. Administrativa y de TTHH	DT-085	VLAN_VOZ	192.168.1.41	/24	VLAN_DATOS	192.168.2.41	/24

41	Dir. Administrativa y de TTHH	DT-086	VLAN_VOZ	192.168.1.42	/24	VLAN_DATOS	192.168.2.42	/24
42	Dir. Administrativa y de TTHH	DT-087	VLAN_VOZ	192.168.1.43	/24	VLAN_DATOS	192.168.2.43	/24
43	Dir. Administrativa y de TTHH	DT-088	VLAN_VOZ	192.168.1.44	/24	VLAN_DATOS	192.168.2.44	/24
44	Dir. Administrativa y de TTHH	DT-089	VLAN_VOZ	192.168.1.45	/24	VLAN_DATOS	192.168.2.45	/24
45	Dir. Administrativa y de TTHH	DT-090	VLAN_VOZ	192.168.1.46	/24	VLAN_DATOS	192.168.2.46	/24
46	Dir. Administrativa y de TTHH	DT-091	VLAN_VOZ	192.168.1.47	/24	VLAN_DATOS	192.168.2.47	/24
47	Dir. Administrativa y de TTHH	DT-092	VLAN_VOZ	192.168.1.48	/24	VLAN_DATOS	192.168.2.48	/24
48	Dir. Administrativa y de TTHH	DT-093	VLAN_VOZ	192.168.1.49	/24	VLAN_DATOS	192.168.2.49	/24

8.1.3. Distribución y asignaciones de puertos Switch de Acceso 2

PUERTO	DEPARTAMENTO	UBIC.	VLAN A	DIR. IP	MK.	VLAN B	DIR. IP	MK.
1	Dirección Financiera	DT-059	VLAN_VOZ	192.168.1.50	/24	VLAN_FINCIERO	192.168.3.34	/28
2	Dirección Financiera	DT-048	VLAN_VOZ	192.168.1.51	/24	VLAN_FINCIERO	192.168.3.35	/28
3	Dirección Financiera	DT-049	VLAN_VOZ	192.168.1.52	/24	VLAN_FINCIERO	192.168.3.36	/28
4	Dirección Financiera	DT-050	VLAN_VOZ	192.168.1.53	/24	VLAN_FINCIERO	192.168.3.37	/28
5	Dirección Financiera	DT-051	VLAN_VOZ	192.168.1.54	/24	VLAN_FINCIERO	192.168.3.38	/28
6	Dirección Financiera	DT-062	VLAN_VOZ	192.168.1.55	/24	VLAN_FINCIERO	192.168.3.39	/28
7	Dirección Financiera	DT-063	VLAN_VOZ	192.168.1.56	/24	VLAN_FINCIERO	192.168.3.40	/28
8	Dirección Financiera	DT-078	VLAN_VOZ	192.168.1.57	/24	VLAN_FINCIERO	192.168.3.41	/28
9	Dirección Financiera	DT-079	VLAN_VOZ	192.168.1.58	/24	VLAN_FINCIERO	192.168.3.42	/28
10	Dir. de Servicios Financieros	DT-017	VLAN_VOZ	192.168.1.59	/24	VLAN_DATOS	192.168.2.50	/24
11	Dir. de Servicios Financieros	DT-015	VLAN_VOZ	192.168.1.60	/24	VLAN_DATOS	192.168.2.51	/24
12	Dir. de Servicios Financieros	DT-074	VLAN_VOZ	192.168.1.61	/24	VLAN_DATOS	192.168.2.52	/24
13	Dir. de Servicios Financieros	DT-075	VLAN_VOZ	192.168.1.62	/24	VLAN_DATOS	192.168.2.53	/24
14	Dir. de Servicios Financieros	DT-060	VLAN_VOZ	192.168.1.63	/24	VLAN_DATOS	192.168.2.54	/24
15	Dir. de Servicios Financieros	DT-061	VLAN_VOZ	192.168.1.64	/24	VLAN_DATOS	192.168.2.55	/24
16	Dir. de Intelig. de Mercados	DT-096	VLAN_VOZ	192.168.1.65	/24	VLAN_DATOS	192.168.2.56	/24
17	Dir. de Intelig. de Mercados	DT-097	VLAN_VOZ	192.168.1.66	/24	VLAN_DATOS	192.168.2.57	/24
18	Dir. de Intelig. de Mercados	DT-110	VLAN_VOZ	192.168.1.67	/24	VLAN_DATOS	192.168.2.58	/24
19	Dir. de Intelig. de Mercados	DT-111	VLAN_VOZ	192.168.1.68	/24	VLAN_DATOS	192.168.2.59	/24
20	Dir. de Gestión de Coactiva	DT-106	VLAN_VOZ	192.168.1.69	/24	VLAN_DATOS	192.168.2.60	/24
21	Dir. de Gestión de Coactiva	DT-107	VLAN_VOZ	192.168.1.70	/24	VLAN_DATOS	192.168.2.61	/24
22	Dir. de Gestión de Coactiva	DT-108	VLAN_VOZ	192.168.1.71	/24	VLAN_DATOS	192.168.2.62	/24
23	Dir. de Gestión de Coactiva	DT-109	VLAN_VOZ	192.168.1.72	/24	VLAN_DATOS	192.168.2.63	/24
24	D.Tecnlgías y Sist. de Inf.	DT-022	VLAN_VOZ	192.168.1.73	/24	VLAN_DATOS	192.168.2.64	/24
25	D.Tecnlgías y Sist. de Inf.	DT-098	VLAN_VOZ	192.168.1.74	/24	VLAN_DATOS	192.168.2.65	/24
26	D.Tecnlgías y Sist. de Inf.	DT-099	VLAN_VOZ	192.168.1.75	/24	VLAN_DATOS	192.168.2.66	/24
27	D.Tecnlgías y Sist. de Inf.	DT-100	VLAN_VOZ	192.168.1.76	/24	VLAN_DATOS	192.168.2.67	/24
28	D.Tecnlgías y Sist. de Inf.	DT-101	VLAN_VOZ	192.168.1.77	/24	VLAN_DATOS	192.168.2.68	/24
29	D.Tecnlgías y Sist. de Inf.	DT-102	VLAN_VOZ	192.168.1.78	/24	VLAN_DATOS	192.168.2.69	/24
30	D.Tecnlgías y Sist. de Inf.	DT-103	VLAN_VOZ	192.168.1.79	/24	VLAN_DATOS	192.168.2.70	/24

31	D.Tecnlgías y Sist. de Inf.	DT-104	VLAN_VOZ	192.168.1.80	/24	VLAN_DATOS	192.168.2.71	/24
32	D.Tecnlgías y Sist. de Inf.	DT-105	VLAN_VOZ	192.168.1.81	/24	VLAN_DATOS	192.168.2.72	/24
33	Archivo Pasivo	DT-019	VLAN_VOZ	192.168.1.82	/24	VLAN_DATOS	192.168.2.73	/24
34	Archivo Pasivo	DT-018	VLAN_VOZ	192.168.1.83	/24	VLAN_DATOS	192.168.2.74	/24
35	Sala pequeña	DT-094	VLAN_VOZ	192.168.1.84	/24	VLAN_DATOS	192.168.2.75	/24
36	Sala pequeña	DT-095	VLAN_VOZ	192.168.1.85	/24	VLAN_DATOS	192.168.2.76	/24
37	Sala múltiple	DT-082	VLAN_VOZ	192.168.1.86	/24	VLAN_DATOS	192.168.2.77	/24
38	Sala múltiple	DT-083	VLAN_VOZ	192.168.1.87	/24	VLAN_DATOS	192.168.2.78	/24
39	Sala de videoconferencia	DT-042	VLAN_VOZ	192.168.1.88	/24	VLAN_DATOS	192.168.2.79	/24
40	Sala de videoconferencia	DT-043	VLAN_VOZ	192.168.1.89	/24	VLAN_DATOS	192.168.2.80	/24
41	Bodega de suministros	DT-005	VLAN_VOZ	192.168.1.90	/24	VLAN_DATOS	192.168.2.81	/24
42	Guardianía	DT-001	VLAN_VOZ	192.168.1.91	/24	VLAN_DATOS	192.168.2.82	/24
43	Impresora 1	DT-023	-	-	-	VLAN_IMPSRS	192.168.3.2	/27
44	Impresora 2	DT-020	-	-	-	VLAN_IMPSRS	192.168.3.3	/27
45	Impresora 3	DT-077	-	-	-	VLAN_IMPSRS	192.168.3.4	/27
46	Impresora 4	DT-012	-	-	-	VLAN_IMPSRS	192.168.3.5	/27
47	Impresora 5	DT-040	-	-	-	VLAN_IMPSRS	192.168.3.6	/27
48	Sensor biométrico 1	DT-030	-	-	-	VLAN_IMPSRS	192.168.3.7	/27

8.1.4. Distribución y asignación de puertos del Switch de Acceso 3

PUERTO	DISPOSITIVO	UBIC.	VLAN A	VLAN B	DIR. IP	MSK.
1	Sensor biométrico 2	DT-034	-	VLAN_IMPRESORAS	192.168.1.3.8	/27
2	Sensor biométrico 3	DT-064	-	VLAN_IMPRESORAS	192.168.1.3.9	/27
3	Panel de alarma	DT-024	-	VLAN_IMPRESORAS	192.168.1.3.10	/27
4	Access Point_PB	DT-041	-	VLAN_IMPRESORAS	192.168.1.3.11	/27
5	Cámaras IP 1	DT-002	-	VLAN_VIDEOVIGILANCIA	192.168.3.66	/28
6	Cámaras IP 2	DT-003	-	VLAN_VIDEOVIGILANCIA	192.168.3.67	/28
7	Cámaras IP 3	DT-004	-	VLAN_VIDEOVIGILANCIA	192.168.3.68	/28
8	Cámaras IP 4	DT-035	-	VLAN_VIDEOVIGILANCIA	192.168.3.69	/28
9	Cámaras IP 5	DT-065	-	VLAN_VIDEOVIGILANCIA	192.168.3.70	/28
10	Cámaras IP 6	DT-013	-	VLAN_VIDEOVIGILANCIA	192.168.3.71	/28
11	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
12	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
13	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
14	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
15	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
16	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
17	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
18	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-

19	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
20	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
21	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
22	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
23	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
24	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-

8.1.5. Distribución y asignaciones de puertos del Switch de Acceso 4

PUERTO	DEPARTAMENTO	UBIC.	VLAN A	DIR. IP	MK.	VLAN B	DIR. IP	MK.
1	Dirección General	DT-201	VLAN_VOZ	192.168.1.92	/24	VLAN_DATOS	192.168.2.83	/24
2	Dirección General (M)	DT-250	VLAN_VOZ	192.168.1.93	/24	VLAN_DATOS	192.168.2.84	/24
3	Dirección General (M)	DT-251	VLAN_VOZ	192.168.1.94	/24	VLAN_DATOS	192.168.2.85	/24
4	Dirección General	DT-202	VLAN_VOZ	192.168.1.95	/24	VLAN_DATOS	192.168.2.86	/24
5	Dirección General	DT-252	VLAN_VOZ	192.168.1.96	/24	VLAN_DATOS	192.168.2.87	/24
6	Dirección General	DT-253	VLAN_VOZ	192.168.1.97	/24	VLAN_DATOS	192.168.2.88	/24
7	Dirección General	DT-254	VLAN_VOZ	192.168.1.98	/24	VLAN_DATOS	192.168.2.89	/24
8	Dirección General	DT-255	VLAN_VOZ	192.168.1.99	/24	VLAN_DATOS	192.168.2.90	/24
9	Dirección de Comunicación Social	DT-274	VLAN_VOZ	192.168.1.100	/24	VLAN_DATOS	192.168.2.91	/24
10	Dirección de Comunicación Social	DT-275	VLAN_VOZ	192.168.1.101	/24	VLAN_DATOS	192.168.2.92	/24
11	Dirección de Comunicación Social	DT-276	VLAN_VOZ	192.168.1.102	/24	VLAN_DATOS	192.168.2.93	/24
12	Dirección de Comunicación Social	DT-277	VLAN_VOZ	192.168.1.103	/24	VLAN_DATOS	192.168.2.94	/24
13	Dirección de Comunicación Social	DT-266	VLAN_VOZ	192.168.1.104	/24	VLAN_DATOS	192.168.2.95	/24
14	Auditoría Interna	DT-256	VLAN_VOZ	192.168.1.105	/24	VLAN_DATOS	192.168.2.96	/24
15	Auditoría Interna	DT-257	VLAN_VOZ	192.168.1.106	/24	VLAN_DATOS	192.168.2.97	/24
16	Auditoría Interna	DT-261	VLAN_VOZ	192.168.1.107	/24	VLAN_DATOS	192.168.2.98	/24
17	Dirección de Planificación	DT-258	VLAN_VOZ	192.168.1.108	/24	VLAN_DATOS	192.168.2.99	/24
18	Dirección de Planificación	DT-259	VLAN_VOZ	192.168.1.109	/24	VLAN_DATOS	192.168.2.100	/24
19	Dirección de Planificación	DT-260	VLAN_VOZ	192.168.1.110	/24	VLAN_DATOS	192.168.2.101	/24
20	Dirección de Asesoría Jurídica	DT-203	VLAN_VOZ	192.168.1.111	/24	VLAN_DATOS	192.168.2.102	/24
21	Dirección de Asesoría Jurídica	DT-204	VLAN_VOZ	192.168.1.112	/24	VLAN_DATOS	192.168.2.103	/24
22	Dirección de Asesoría Jurídica	DT-264	VLAN_VOZ	192.168.1.113	/24	VLAN_DATOS	192.168.2.104	/24
23	Dirección de Asesoría Jurídica	DT-265	VLAN_VOZ	192.168.1.114	/24	VLAN_DATOS	192.168.2.105	/24
24	Dirección de Gestión de Riesgos	DT-284	VLAN_VOZ	192.168.1.115	/24	VLAN_DATOS	192.168.2.106	/24
25	Dirección de Gestión de Riesgos	DT-285	VLAN_VOZ	192.168.1.116	/24	VLAN_DATOS	192.168.2.107	/24
26	Dirección de Gestión de Riesgos	DT-287	VLAN_VOZ	192.168.1.117	/24	VLAN_DATOS	192.168.2.108	/24
27	D.Tecnlgías y Sist. de Información	DT-286	VLAN_VOZ	192.168.1.118	/24	VLAN_DATOS	192.168.2.109	/24
28	D.Tecnlgías y Sist. de Información	DT-288	VLAN_VOZ	192.168.1.119	/24	VLAN_DATOS	192.168.2.110	/24
29	D.Tecnlgías y Sist. de Información	DT-289	VLAN_VOZ	192.168.1.120	/24	VLAN_DATOS	192.168.2.111	/24
30	D.Tecnlgías y Sist. de Información	DT-291	VLAN_VOZ	192.168.1.121	/24	VLAN_DATOS	192.168.2.112	/24

31	D.Tecnlgías y Sist. de Información	DT-292	VLAN_VOZ	192.168.1.122	/24	VLAN_DATOS	192.168.2.113	/24
32	D.Tecnlgías y Sist. de Información	DT-293	VLAN_VOZ	192.168.1.123	/24	VLAN_DATOS	192.168.2.114	/24
33	Bodega	DT-208	VLAN_VOZ	192.168.1.124	/24	VLAN_DATOS	192.168.2.115	/24
34	Archivo Pasivo Dirección General	DT-207	VLAN_VOZ	192.168.1.125	/24	VLAN_DATOS	192.168.2.116	/24
35	Bodega Tecnologías	DT-206	VLAN_VOZ	192.168.1.126	/24	VLAN_DATOS	192.168.2.117	/24
36	Cuarto de Máquinas	DT-205	VLAN_VOZ	192.168.1.127	/24	VLAN_DATOS	192.168.2.118	/24
37	Sala de Reuniones	DT-268	VLAN_VOZ	192.168.1.128	/24	VLAN_VISIT.	192.168.3.50	/28
38	Sala de Reuniones	DT-269	VLAN_VOZ	192.168.1.129	/24	VLAN_VISIT.	192.168.3.51	/28
39	Sala de Reuniones	DT-270	VLAN_VOZ	192.168.1.130	/24	VLAN_VISIT.	192.168.3.52	/28
40	Sala de Reuniones	DT-271	VLAN_VOZ	192.168.1.131	/24	VLAN_VISIT.	192.168.3.53	/28
41	Sala de Reuniones	DT-272	VLAN_VOZ	192.168.1.132	/24	VLAN_VISIT.	192.168.3.54	/28
42	Sala de Reuniones	DT-273	VLAN_VOZ	192.168.1.133	/24	VLAN_VISIT.	192.168.3.55	/28
43	Sala de Reuniones	DT-278	VLAN_VOZ	192.168.1.134	/24	VLAN_VISIT.	192.168.3.56	/28
44	Sala de Reuniones	DT-279	VLAN_VOZ	192.168.1.135	/24	VLAN_VISIT.	192.168.3.57	/28
45	Sala de Reuniones	DT-280	VLAN_VOZ	192.168.1.136	/24	VLAN_VISIT.	192.168.3.58	/28
46	Sala de Reuniones	DT-281	VLAN_VOZ	192.168.1.137	/24	VLAN_VISIT.	192.168.3.59	/28
47	Sala de Reuniones	DT-282	VLAN_VOZ	192.168.1.138	/24	VLAN_VISIT.	192.168.3.60	/28
48	Access Point_PA	DT-283	-	-	-	VLAN_IMPR.	192.168.3.12	/27

8.1.6. Distribución y asignaciones de puertos del Switch de Acceso 5

PUERTO	DISPOSITIVO	UBIC.	VLAN A	VLAN B	DIR. IP	MSK.
1	Impresora 6	DT-290	-	VLAN_IMPRESORAS	192.168.3.13	/27
2	Impresora 7	DT-267	-	VLAN_IMPRESORAS	192.168.3.14	/27
3	Impresora 8	DT-262	-	VLAN_IMPRESORAS	192.168.3.15	/27
4	Panel de alarma	DT-263	-	VLAN_IMPRESORAS	192.168.3.16	/27
5	Cámaras IP 7	DT-200	-	VLAN_VIDEOVIGILANCIA	192.168.3.72	/28
6	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
7	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
8	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
9	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
10	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
11	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
12	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
13	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
14	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
15	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
16	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
17	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
18	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-

19	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
20	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
21	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
22	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
23	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-
24	LIBRE	-	SHUTDOWN	SHUTDOWN	-	-

8.1.7. Creación del dominio VTP SW_Núcleo/Distribución1

SW-PRIMARIO #configure terminal
SW-PRIMARIO (config)#vtp domain CONAFIPS
SW-PRIMARIO VTP domain name from NULL to CONAFIPS
SW-PRIMARIO (config)#vtp password CONAFIPS
Setting device VLAN database password to CONAFIPS
SW-PRIMARIO (config)#vtp mode server //Establece en modo servidor VTP
Setting device to VTP SERVER mode.

8.1.8. Configuración VTP en modo cliente los switches del dominio

SW-SECUNDARIO#configure terminal
SW-SECUNDARIO(config)#vtp domain CONAFIPS
Changing VTP domain name from NULL to CONAFIPS
SW-SECUNDARIO(config)#vtp password CONAFIPS
Setting device VLAN database password to CONAFIPS
SW-SECUNDARIO(config)#vtp mode client //Configuración en modo cliente
Setting device to VTP CLIENT mode.
SW-SECUNDARIO(config)#exit
SW-SECUNDARIO#show vtp status // Verificar el estado de VTP
SW-SECUNDARIO#show vlan brief // Verificar la creación de las VLAN

Las configuraciones VTP dentro de un mismo dominio permiten que el switch configurado en modo servidor (SW_CORE_DISTRIBUCIÓN_1) replique posteriormente las VLAN creadas a todos los switches del dominio configurados en modo cliente, evitando la actualización manual en cada uno de los switches de la red.

8.1.9. Creación de las VLAN en el servidor VTP

```
SW-PRIMARIO#configure terminal
SW-PRIMARIO(config)#vlan 10
SW-PRIMARIO(config-vlan)#name VLAN_VOZ
SW-PRIMARIO(config-vlan)#exit
SW-PRIMARIO(config)#vlan 20
SW-PRIMARIO(config-vlan)#name VLAN_DATOS
SW-PRIMARIO(config-vlan)#exit
SW-PRIMARIO(config)#vlan 30
SW-PRIMARIO(config-vlan)#name VLAN_FINANCIERO
SW-PRIMARIO(config-vlan)#exit
SW-PRIMARIO(config)#vlan 40
SW-PRIMARIO(config-vlan)#name VLAN_IMPRESORAS
SW-PRIMARIO(config-vlan)#exit
SW-PRIMARIO(config)#vlan 50
SW-PRIMARIO(config-vlan)#name VLAN_VIDEOVIGILANCIA
SW-PRIMARIO(config-vlan)#exit
SW-PRIMARIO(config)#vlan 60
SW-PRIMARIO(config-vlan)#nam
SW-PRIMARIO(config-vlan)#name VLAN_ADMINISTRATIVA
SW-PRIMARIO(config-vlan)#
SW-PRIMARIO(config-vlan)#exit
SW-PRIMARIO(config)#vlan 70
SW-PRIMARIO(config-vlan)#name VLAN_SERVIDORES
SW-PRIMARIO(config-vlan)#exit
SW-PRIMARIO(config)#vlan 80
SW-PRIMARIO(config-vlan)#name VLAN_VISITANTES
SW-PRIMARIO(config-vlan)#exit
```

8.1.10. Asignación de direcciones IP a las interfaces de VLAN’s en el servidor VTP

```
SW-PRIMARIO#configure terminal
SW-PRIMARIO(config)#interface vlan 10
SW-PRIMARIO(config-vlan)#ip address 192.168.1.1 255.255.255.0
SW-PRIMARIO(config-vlan)#exit
```

8.1.11. Configuración de enlaces troncales en los switches Núcleo/Distribución

SW-PRIMARIO #configure terminal
SW-PRIMARIO (config)#interface range fastethernet 0/1-5
SW-PRIMARIO (config-if-range)#switchport trunk encapsulation dot1q
SW-PRIMARIO (config-if-range)#switchport mode trunk
SW-PRIMARIO (config-if-range)#switchport trunk allowed vlan all
SW-PRIMARIO (config-if-range)#end

8.1.12. Configuración de enlaces troncales en los switches de la capa de acceso

Switch#configure terminal
Switch(config)#interface range gigabitEthernet 0/1-2
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan all
Switch(config-if-range)#end

8.1.13. Asignación de los puertos de los switches de acceso a sus respectivas VLAN's

SW-ACCESO_1#configure terminal
SW-ACCESO_1(config)#interface range fastEthernet 0/1-48
SW-ACCESO_1(config-if-range)#switchport mode access
SW-ACCESO_1(config-if-range)#switchport access vlan 20
SW-ACCESO_1(config-if-range)#switchport voice vlan 10
SW-ACCESO_1(config-if-range)#switchport trunk allowed vlan 10,20
SW-ACCESO_1(config-if-range)#end

8.1.14. Configuración de seguridad en los puertos de los switches de acceso

SW-ACCESO_1#configure terminal
SW-ACCESO_1(config)#interface range fastEthernet 0/1-24
SW-ACCESO_1(config-if-range)#switchport port-security maximum 1
SW-ACCESO_1(config-if-range)#switchport port-security violation protect

SW-ACCESO_1(config-if-range)#switchport port-security mac-address sticky
SW-ACCESO_1(config-if-range)#end

SW-ACCESO_1#show port-security interface fastEthernet 0/1 //Verificar la seguridad

8.2. Configuración de Calidad de Servicios QoS

8.2.1. Creación de las clases de servicios

SW-PRIMARIO#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-PRIMARIO(config)#class-map VOIP
SW-PRIMARIO(config-cmap)#match protocol udp
SW-PRIMARIO(config-cmap)#match protocol rtp
SW-PRIMARIO(config-cmap)#match protocol h323
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO(config)#class-map ALTA-PRIORIDAD
SW-PRIMARIO(config-cmap)#match protocol ftp
SW-PRIMARIO(config-cmap)#match protocol telnet
SW-PRIMARIO(config-cmap)#match protocol ssh
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO(config)#class-map MEDIA-PRIORIDAD
SW-PRIMARIO(config-cmap)#match protocol http
SW-PRIMARIO(config-cmap)#match protocol snmp
SW-PRIMARIO(config-cmap)#match protocol syslog
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO(config-cmap)#class-map BAJA-PRIORIDAD
SW-PRIMARIO(config-cmap)#match protocol pop3
SW-PRIMARIO(config-cmap)#match protocol smtp
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO#show class-map // Verificar la creación de las clases

8.2.2. Configuración para el marcado de las clases creadas

SW-PRIMARIO#configure terminal
SW-PRIMARIO(config)#policy-map MARCADO
SW-PRIMARIO(config-pmap)#class VOIP
SW-PRIMARIO(config-pmap-c)#set ip dscp ef // Marcar con muy alta prioridad
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO(config-pmap)#class ALTA-PRIORIDAD

SW-PRIMARIO(config-pmap-c)#set ip dscp af41
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO(config-pmap)#class MEDIA-PRIORIDAD
SW-PRIMARIO(config-pmap-c)#set ip dscp af31
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO(config-pmap)#class BAJA-PRIORIDAD
SW-PRIMARIO(config-pmap-c)#set ip dscp af21
SW-PRIMARIO(config-pmap-c)#exit

8.2.3. Aplicación de las políticas de marcado en las interfaces de entrada de paquetes de la capa de núcleo/distribución.

SW-PRIMARIO#configure terminal
SW-PRIMARIO(config)#interface range fastEthernet 0/1-5
SW-PRIMARIO(config-if-range)#service-policy input MARCADO

8.2.4. Creación de clases para las políticas de salida

SW-PRIMARIO#configure terminal
SW-PRIMARIO(config)#class-map VOIP-OUT
SW-PRIMARIO(config-cmap)#match ip dscp ef
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO(config)#class-map ALTA-PRIORIDAD-OUT
SW-PRIMARIO(config-cmap)#match ip dscp af41
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO(config)#class-map MEDIA-PRIORIDAD-OUT
SW-PRIMARIO(config-cmap)#match ip dscp af31
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO(config)#class-map BAJA-PRIORIDAD-OUT
SW-PRIMARIO(config-cmap)#match ip dscp af21
SW-PRIMARIO(config-cmap)#exit
SW-PRIMARIO#show class-map // Verifica la creación de las clases

8.2.5. Configuración de las políticas asignación de prioridades a las clases de salida creadas

SW-PRIMARIO(config)#policy-map QoS-OUT
SW-PRIMARIO(config-pmap)#class VOIP-OUT
SW-PRIMARIO(config-pmap-c)#priority 120 6000
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO(config-pmap)#class ALTA-PRIORIDAD-OUT

```
SW-PRIMARIO(config-pmap-c)#bandwidth percent 20
SW-PRIMARIO(config-pmap-c)#random-detect dscp-based
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO(config-pmap)#class MEDIA-PRIORIDAD-OUT
SW-PRIMARIO(config-pmap-c)#bandwidth percent 15
SW-PRIMARIO(config-pmap-c)#random-detect dscp-based
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO(config-pmap)#class BAJA-PRIORIDAD-OUT
SW-PRIMARIO(config-pmap-c)#bandwidth percent 10
SW-PRIMARIO(config-pmap-c)#random-detect dscp-based
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO(config-pmap)#class class-default
SW-PRIMARIO(config-pmap-c)#fair-queue 16
SW-PRIMARIO(config-pmap-c)#queue-limit 20
SW-PRIMARIO(config-pmap-c)#random-detect
SW-PRIMARIO(config-pmap-c)#exit
SW-PRIMARIO#show policy-map          // Verifica la creación de las políticas
```

8.2.6. Aplicación de las políticas QoS en las interfaces de salida

```
SW-PRIMARIO#configure terminal
SW-PRIMARIO(config)#interface range gigabitEthernet 0/1-2
SW-PRIMARIO(config-if-range)#service-policy output QoS-OUT
SW-PRIMARIO(config-if-range)#exit
SW-PRIMARIO(config)#interface range fastEthernet 0/6-7
SW-PRIMARIO(config-if-range)#service-policy output QoS-OUT
SW-PRIMARIO(config-if-range)#exit
SW-PRIMARIO#show queue gigabitEthernet 0/1          // Verificación de
la aplicación de las políticas a las interfaces de salida
```

8.2.7. Configuración del root primario y secundario del STP

```
SW-PRIMARIO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-PRIMARIO(config)#spanning-tree vlan 10-80 root primary
SW-PRIMARIO(config)#end
```

SW-SECUNDARIO #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-SECUNDARIO(config)#spanning-tree vlan 10-80 root secondary
SW-SECUNDARIO(config)# end

8.2.8. Configuración de la tecnología Etherchannel

SW-PRIMARIO#configure terminal
SW-PRIMARIO(config)#interface fastEthernet 0/7
SW-PRIMARIO(config-if)#channel-group 1 mode on
SW-PRIMARIO(config-if)#interface fastEthernet 0/8
SW-PRIMARIO(config-if)#channel-group 1 mode on
SW-PRIMARIO(config-if)#exit

8.3. Configuración de seguridad en el Firewall

8.3.1. Configuración de la interface VLAN 2 de salida de la red

ASA5500#configure terminal
ASA5500 (config)#interface vlan 2 //Interface
ASA5500 (config-if)#nameif outside //Nombre de la interface
ASA5500 (config-if)#security-level 0 //Nivel de seguridad
ASA5500 (config-if)#ip address 198.51.100.100 255.255.255.0 // IP Pública
ASA5500 (config-if)#no shutdown
ASA5500 (config-if)#end
ASA5500#write memory

8.3.2. Configuración de la interface VLAN 1 de entrada a la red

ASA5500#configure terminal
ASA5500 (config)#interface vlan 1
ASA5500 (config-if)#nameif inside
ASA5500 (config-if)#security-level 100
ASA5500 (config-if)#ip address 192.168.1.1 255.255.255.0 //IP Privada
ASA5500 (config-if)#no shutdown
ASA5500 (config)#end
ASA5500#write memory

8.3.3. Creación de una nueva interfaz VLAN para la DMZ

ASA5500 (config-if)#interface Vlan 3
ASA5500 (config-if)#nameif dmz
ASA5500 (config-if)#security-level 50
ASA5500 (config-if)#ip address 192.68.0.1 255.255.255.0 //IP de la DMZ
ASA5500 (config-if)#end
ASA5500#write memory

8.3.4. Asignación de la VLAN Inside a la interfece Ethernet 0/1

ASA5500#configure terminal
ASA5500 (config)#interface ethernet 0/1
ASA5500 (config-if)#switchport access vlan 1
ASA5500 (config-if)#end
ASA5500#write memory

8.3.5. Asignación de la interfece Ethernet 0/2 a la VLAN dmz

ASA5500 (config)#interface ethernet 0/2
ASA5500 (config-if)#switchport access vlan 3
ASA5500 (config-if)#no shutdown
ASA5500 (config-if)#end

8.3.6. Creación del objeto de red DNS para la traducción

ASA5500 (config)#object network dns-server
ASA5500 (config-network-object)#host 192.168.1.53
ASA5500 (config-network-object)#exit

8.3.7. Creación del objeto de red WEB EXTERNA para la traducción

ASA5500 (config)#object network webserver-external-ip
ASA5500 (config-network-object)#host 198.51.100.101
ASA5500 (config-network-object)#exit

8.3.8. Creación del objeto de red WEBSERVER para la traducción

ASA5500 (config)#object network webserver
ASA5500 (config-network-object)#host 192.168.0.100
ASA5500 (config-network-object)#nat (dmz,outside) static 198.51.100.101 service tcp www www

8.3.9. Creación del objeto de red DMZ para la traducción

ASA5500 (config)#object network dmz-subnet
ASA5500 (config-network-object)#subnet 192.168.0.0 255.255.255.0
ASA5500 (config-network-object)#nat (dmz,outside) dynamic interface
ASA5500 (config-network-object)#end

8.3.10. Creación del objeto de red INSIDE para la traducción

ASA5500 (config)#object network inside-subnet
ASA5500 (config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA5500 (config-network-object)#nat (inside,outside) dynamic interface
ASA5500 (config-network-object)#exit

8.3.11. Creación de listas de acceso ASA5500

(config)#access-list outside_acl extended permit tcp any object webserver eq www

(config)#access-list dmz_acl extended permit udp any object dns-server eq domain

(config)#access-list dmz-acl extended deny ip any object inside-subnet

(config)#access-list dmz_acl extended permit ip any any

8.3.12. Asignación de ACL's a las interfaces

ASA5500 (config)#access-group outside_acl in interface outside
ASA5500 (config)#access-group dmz_acl in interface dmz

8.3.13. Creación de la ruta estática de salida

ASA5500(config)#route outside 0.0.0.0 0.0.0.0 198.51.100.1

8.3.14. Proforma general del proveedor

Technology Services Del Ecuador
Soluciones Tecnológicas

RUC: 0912724325001

Sauces 6 Mz. 317 Solar 2 Telf. Fax +593-4-2967463 +593-084-354353

COTIZACION

Cliente				**Varios**	
Empresa:	Ing. Andrés Quilumba			Fecha	16 de febrero de 2016
Dirección				Nº de pedido	1602161137
Email.		Telf:		Representante	Douglas De La Torre
Contacto:		Ciudad:	Guayaquil	Codigo del Cliente	tsc-1011

Cantidad	Descripción	Precio unitario	TOTAL
2	Rack de piso 32 UR 60x80x160	$759,00	$ 1.518,00
120	Pacth cord 3fts cat 6A	$ 4,51	$ 541,20
8	Patch panel modular 24 puertos cat 6A	$ 23,10	$ 184,80
20	Jack de patch panel cat 6A	$ 4,81	$ 96,20
15	Organizador horizontal 2UR	$ 12,89	$ 193,35
50	Blank negro	$ 0,32	$ 16,00
1	Multitoma Eléctrica	$ 26,84	$ 26,84
1	Rack de pared_12 UR 600x450x635mm	$ 189,75	$ 189,75
72	Pacth cord 3fts cat 6A	$ 4,51	$ 324,72
3	Patch panel modular 24 puertos cat 6A	$ 23,10	$ 69,30
168	Jack de patch panel cat 6A	$ 4,81	$ 808,08
5	Organizador horizontal 1UR	$ 10,16	$ 50,80
1	Multitoma Eléctrica	$ 26,85	$ 26,85
2	Servidor HP Prolyant DL380P G9	$ 7.200,00	$ 14.400,00
1	Firewall asa 5512	$ 2.693,00	$ 2.693,00
2	Switch 24 puertos (capa 3) ws-c3850T-L	$ 4.256,00	$ 8.512,00
3	Switch 48 puertos (acceso)	$ 4.708,00	$ 14.124,00
2	Switch 24 puertos (acceso)	$ 2.688,00	$ 5.376,00
1	Central Telefónica IP 8 lineas	$ 920,00	$ 920,00
2	UPS Apc 3KVA	$ 1.145,10	$ 2.290,20
410	Bandejas/Rejillas metálicas Mts 30x5x3 mts	$ 24,16	$ 9.905,60
3	Tuberia de Ø 50mm mts	$ 2,56	$ 7,68
2	Codos de Ø 50mm	$ 0,63	$ 1,26
410	Canaleta mediana 2 canales mts 60x40	$ 4,93	$ 2.021,30
32	Face Plate simple	$ 1,39	$ 44,48
63	Face Plate doble	$ 1,57	$ 98,91
158	Patch cord cat 6A 7 fts	$ 6,33	$ 1.000,14
158	Jack cat 6A	$4,81	$ 759,98
158	Caja sobrepuesta	$1,54	$ 243,32
3	Multitoma eléctrica	26,85	$ 80,55
16	Cable UTP CAT 6A	327,53	$ 5.240,48
		Subtotal	$ 71.764,79
		Envío	
	Impuestos	12,00%	$ 8.611,77
		TOTAL	**$ 80.376,56**

Medio de pago	Cheque
Comentarios	Cheque a Nombre Douglas De La Torre
Garantia	1 año contra defecto de Fabrica
Tiempo del Entrega:	Confirmar stock
Caducidad	15 Dias
Forma de Pago	50% Anticipo 50% contra entrega

www.techservi.com

Condiciones Comerciales: