UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

ESTUDIO Y DISEÑO DE UNA RED DE INTERCONEXIÓN ENTRE LAS SEDES DE ONLYTICKET EVENTOS CARACAS, PUERTO ORDAZ Y PANAMÁ.

TRABAJO ESPECIAL DE GRADO

Presentada ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR Evangelia Charcotsicas Tsantarliotou
Adriana Giménez Silva

TUTOR Ing. Luis Molner

FECHA Febrero 2012

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

ESTUDIO Y DISEÑO DE UNA RED DE INTERCONEXIÓN ENTRE LAS SEDES DE ONLYTICKET EVENTOS CARACAS, PUERTO ORDAZ Y PANAMÁ.

TRABAJO ESPECIAL DE GRADO

Presentada ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR Evangelia Charcotsicas Tsantarliotou
Adriana Giménez Silva

TUTOR Ing. Luis Molner

FECHA Febrero 2012

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

ESTUDIO Y DISEÑO DE UNA RED DE INTERCONEXIÓN ENTRE LAS SEDES DE ONLYTICKET EVENTOS CARACAS, PUERTO ORDAZ Y PANAMÁ.

Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado:

_____

J U R A D O E X A M I N A D O R

Firma: Firma: Firma:

Nombre: _____ Nombre: _____ Nombre: _____

REALIZADO POR Evangelia Charcotsicas Tsantarliotou
Adriana Giménez Silva
TUTOR Ing. Luis Molner.
FECHA Febrero de 2012

DEDICATORIA

En primer lugar queremos dedicarle este logro a Dios y a la Virgen María por guiarnos en este camino transcurrido, por siempre iluminarnos y escuchar nuestras suplicas semestre tras semestre.

Este Trabajo Especial de Grado está dedicado a nuestras familias, nuestros padres y hermanos, que nos ayudaron, nos apoyaron con sus palabras de aliento y buenos consejos en los momentos difíciles, y que siempre confiaron en nosotros.

Evangelia Charcotsicas y Adriana Giménez

AGRADECIMIENTOS

Deseamos agradecer a nuestro Dios por habernos bendecido y servirnos de guía durante toda la carrera, permitiéndonos culminar la misma con éxito.

De igual manera agradecemos a nuestros padres, por su apoyo incondicional, sus consejos, ayuda y palabras de aliento los cuales nos dieron fuerza y coraje para nunca perder vista de nuestro objetivo. Esto es un logro tanto nuestro como de ustedes.

También deseamos agradecer enormemente al Ing. Luis Molner el cual nos brindó su tutela durante toda la elaboración de este proyecto, orientándonos, aportando sugerencias y valiosas ideas.

No podemos dejar de agradecer al personal de OnlyTicket Eventos por abrirnos las puertas de su empresa y permitirnos realizar este importante proyecto.

Por último, pero no menos importantes deseamos agradecer a nuestros amigos y compañeros de carrera que siempre estuvieron ahí para animarnos, ofrecernos su incondicional ayuda, apoyo y aportes para que este proyecto pudiese culminarse exitosamente. A todos mil gracias.

RESUMEN

ESTUDIO Y DISEÑO DE UNA RED DE INTERCONEXIÓN ENTRE LAS SEDES DE ONLYTICKET EVENTOS CARACAS, PUERTO ORDAZ Y PANAMÁ.

Charcotsicas, Evangelia
evacht88@gmail.com

Giménez, Adriana
adrigs12@gmail.com

OnlyTicket Eventos es una empresa importante en el mundo del entretenimiento en Venezuela, destacándose en la planificación y elaboración de eventos y conciertos. Lamentablemente, no cuenta con la tecnología necesaria para hacer posible una conexión entre sus sedes.

Por dicha razón, en este trabajo especial de grado se propone diseñar una red de interconexión que permita el intercambio de información entre las tres sedes ubicadas en Caracas, Puerto Ordaz y una en Panamá, además de una sede móvil. Para ello, se definió una arquitectura detallando características como tecnologías, topología y equipos a utilizar basándose en diversas fuentes bibliográficas, que sirvieron de guía para el diseño de dicha red.

Posterior a esto, se hizo una estimación de costos, con el fin de presentarle a la empresa un presupuesto estimado de solución propuesta. Además, se realizaron simulaciones para así poder verificar el correcto funcionamiento del diseño planteado.

Una vez culminados los pasos mencionados anteriormente, se obtuvo un diseño de red eficiente, que garantiza la transmisión y recepción de voz, datos y video.

Palabras claves: red, diseñar, simulación.

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INDICE DE ABREVIATURAS

ANSI: *American National Standards Institute*

EIA: *Electronics Industries Alliance*

HTTP: *Hypertext Transfer Protocol*

IDF: *Intermediate Data Facility*

IP: Internet Protocol

IPv4: Protocolo de internet versión 4

IPv6: Protocolo de internet versión 6

MDF: *Main Data Facility*

OSI: Organización Internacional para la Estandarización

POP3: *Post Office Protocol v3*

SIP: *Session Initiation Protocol*

TIA: *Telecommunications Industry Association*

TCP: Protocolo de control de transmisión

UPS: *Uninterrupted Power System*

UTP: *Unshielded twisted pair*; Par trenzado no blindado

VLSM: *Virtual Local Area Network*

VPN: *Virtual Private Network*

INTRODUCCIÓN

En Venezuela actualmente hay diversas empresas que organizan eventos de entretenimiento, teniendo varias sedes en el territorio nacional. Tal es el caso de OnlyTicket Eventos, contando con dos sedes en Venezuela y una internacional ubicada en Panamá, así como también una sede móvil en la locación donde se realizan los eventos.

Dicho esto, el gran problema de OnlyTicket Eventos es la falta de una plataforma que permita dicha comunicación entre sus sedes. Esto ocasiona que los encargados de esta empresa, tengan que movilizarse entre ellas para organizar y monitorizar los *shows* montados. Por tal motivo, se requiere un sistema de tecnología de punta, que permita obtener en tiempo real la información de sus sedes, es decir, que permita la transmisión de datos, video y voz.

Con lo expresado anteriormente, se plantea como objetivo general del proyecto diseñar una red que permita conectar las sedes de OnlyTicket Eventos Caracas, Puerto Ordaz y Panamá donde se intercambie información necesaria entre esas localidades. Para el desarrollo de este objetivo general, se dividió en los objetivos específicos descritos a continuación.

En primer lugar, realizar un estudio de la red existente entre los centros, así como los requerimientos básicos de la empresa. Para cumplir con este objetivo, se visitará la sede de la empresa en Caracas (sede principal), donde se explicará a detalle las características de las tecnologías con la que cuentan actualmente, realizando consultas y recogiendo opiniones de gente con experiencia en el área.

En segundo lugar, se presentan el reconocimiento de los elementos y aplicaciones necesarios para la realización del sistema y definición de los mismos.

Para poder alcanzar este objetivo, una vez investigadas las tecnologías existentes en las sedes, se hará una revisión bibliográfica para elegir los componentes esenciales que permitirán llevar a cabo con éxito el proyecto planteado. Posterior a esto, se hará el diseño de la arquitectura de red que soporte la transmisión de voz, datos y video.

En tercer lugar, una vez realizado el diseño, se identificará el *software* de simulación a utilizar. Luego de esto, se pasará a simular la red diseñada, con el fin de comprobar si en efecto se puede implementar en la empresa.

Por último, se tiene la elaboración de un estudio tecno-económico que permita a la empresa tomar la decisión para su implementación tomando en cuenta tanto el costo de implementación como el de mantenimiento.

CAPÍTULO I

PLANTEAMIENTO DEL PROYECTO

En este capítulo se describe el problema que motivó la realización del Trabajo Especial de Grado, también se presenta el objetivo general, los objetivos específicos, y finalmente los alcances y limitaciones del proyecto.

I.1 Planteamiento del Problema

OnlyTicket Eventos es una empresa importante en el mundo del entretenimiento en Venezuela destacándose en la planificación y elaboración de eventos y conciertos.

Sus centros operativos se encuentran en las ciudades de Caracas, Puerto Ordaz y una internacional ubicada en Panamá. Estas sedes se encargan de la gestión de la empresa, teniendo departamentos de publicidad y mercadeo, finanzas y tecnología principalmente.

Adicionalmente, esta empresa cuenta con sedes móviles, en las cuales se lleva a cabo eventos como exposiciones o conciertos. Dichos eventos se organizan en estos lugares de modo que gente ubicada en distintos sitios tengan la oportunidad de disfrutarlos.

Sin embargo, los centros antes mencionados no cuentan con la tecnología para crear un medio que permita la interacción entre usuarios de distintas sedes. El hecho de no estar conectadas significa que cada sede maneja la información de manera desordenada siendo un obstáculo para la toma de decisiones corporativas (tomando en cuenta que Caracas es la sede principal). De igual manera, se presentan grandes inconvenientes como carencia de monitoreo externo en las sedes móviles, falta de correo interno corporativo, duplicidad de datos y graves problemas de seguridad a nivel de red tales como: privacidad, resguardo de la información, autenticación del usuario y seguridad lógica de los equipos.

Cabe destacar, que las sedes de Caracas y Panamá tienen un servicio de internet con una tasa de bits limitada (1024 kbps) el cual no le proporciona la velocidad adecuada para realizar sus procesos administrativos, ocasionando que la red no pueda soportar el tráfico que se genera en un momento determinado. Las sedes móviles cuentan con una conexión a internet del proveedor de servicios donde se realicen los eventos (centros comerciales), pero solo para fines internos y administrativos sin tener una comunicación externa. En cuanto a la sede de Puerto Ordaz, ésta no posee una conexión a internet lo que causa dificultad de su funcionamiento interno y la comunicación hacia las otras sedes de la empresa. Dichos argumentos imposibilitan óptimos servicios de gestión entres los centros operativos y sedes móviles.

En este sentido, a solicitud de OnlyTicket Eventos, se presentó la oportunidad de aprovechar este trabajo especial de grado para desarrollar la propuesta de diseñar una red de interconexión entre sus sedes, obteniendo grandes beneficios al estar al tanto de lo que sucede en ellas, resolviendo los problemas mencionados anteriormente.

Para poder llevar a cabo este proyecto, se requiere la instalación de una plataforma que permita la transmisión de datos, video y voz, logrando así la interconexión entre las distintas sedes brindando un servicio que proporcione un eficiente funcionamiento de la empresa, originando su consolidación en el mercado latinoamericano.

I.2. Objetivos

I.2.1 Objetivo General

Diseñar una red que permita conectar las sedes de OnlyTicket Eventos Caracas, Puerto Ordaz y Panamá.

I.2.2 Objetivos Específicos

- Realizar el estudio de la red existente en la sede de Caracas, Puerto Ordaz y Panamá.
- Proponer un diseño de una red de comunicaciones que permita la interoperabilidad entre las redes de voz, dato y video.
- Conocer los elementos y aplicaciones requeridas por la empresa para dimensionar la red.
- Identificar el *software* que permita realizar la simulación del diseño propuesto.
- Elaborar un estudio técnico-económico con el fin de tener un estimado monetario de inversión.

I.3 Limitaciones y Alcances

Con el presente Trabajo Especial de Grado se pretende diseñar una red que permita la interconexión de las distintas sedes de la empresa OnlyTicket Eventos, tomando como premisa que la empresa solicitó realizar una propuesta basado en una estructura física de cuatro pisos, para la sede de Caracas, Panamá y Puerto Ordaz en donde se defina el cableado estructurado, que permita organizar usuarios por departamentos, así como también la instalación de un *software* de videoconferencia con el cual ya cuenta la empresa. Por último, independizar los servicios administrativos fundamentales para el cumplimiento de su misión como son: sistema de nomina y administración, correo electrónico, web y boletería.

Esta red se debe diseñar tomando en cuenta que la empresa está buscando crecer por lo que es importante que presente escalabilidad.

Existe una limitante al momento de realizar el reconocimiento de las tecnologías y equipos de cada sede, debido a que solo se pudo acceder físicamente a la sede ubicada en Caracas. La información de las sedes de Puerto Ordaz, Panamá y

las sedes móviles fueron proporcionadas directamente por los gerentes de operaciones de la empresa.

Con respecto a la sede móvil es importante mencionar que la misma estará sujeta cambios en su estructura física debido a que depende del tipo de eventos que se realicen y su ubicación.

En cuanto al dimensionamiento de la red en lo que se refiere al cálculo del ancho de banda, se debe tener presente que el mismo será solo una estimación puesto que no existe un modelo que permita realizar un cálculo específico de este requerimiento. Esto es debido a que el ancho de banda aumenta o disminuye de acuerdo a la cantidad de usuarios conectados y la carga que tenga la red.

El trabajo estará basado netamente en el diseño de la red, el cual permitirá a la empresa tener una idea del costo del proyecto al momento de ser implementado en un futuro.

I.4 Justificación

Las empresas de entretenimiento, siempre buscan expandirse a lo largo del territorio nacional, a modo de ofrecer sus servicios en otras regiones, obteniendo una mayor clientela. Crecer de manera exitosa implica que las diferentes sedes de una empresa se comuniquen entre sí, logrando estar al tanto de las actividades que se encuentren desarrollando en cada localidad, teniendo un control sobre las mismas.

Para obtener lo mencionado anteriormente, es necesario hacer el diseño de una red convergente y escalable que permita, en caso de ser necesario, la fácil comunicación y un monitoreo constante sobre sus eventos.

Debido a que la empresa OnlyTicket Eventos se encuentra en la situación en la cual tiene varias sedes y carece de una red que las interconecte, el desarrollo de este Trabajo Especial de Grado será de gran beneficio para optimizar su proceso productivo.

CAPÍTULO II
MARCO TEÓRICO

En este capítulo se presentan los conceptos y definiciones esenciales sobre los cuales se fundamenta el proyecto del Trabajo Especial de Grado, cubriéndose principalmente temas de redes. La figura 1 presenta un esquema de la teoría más relevante para la investigación.

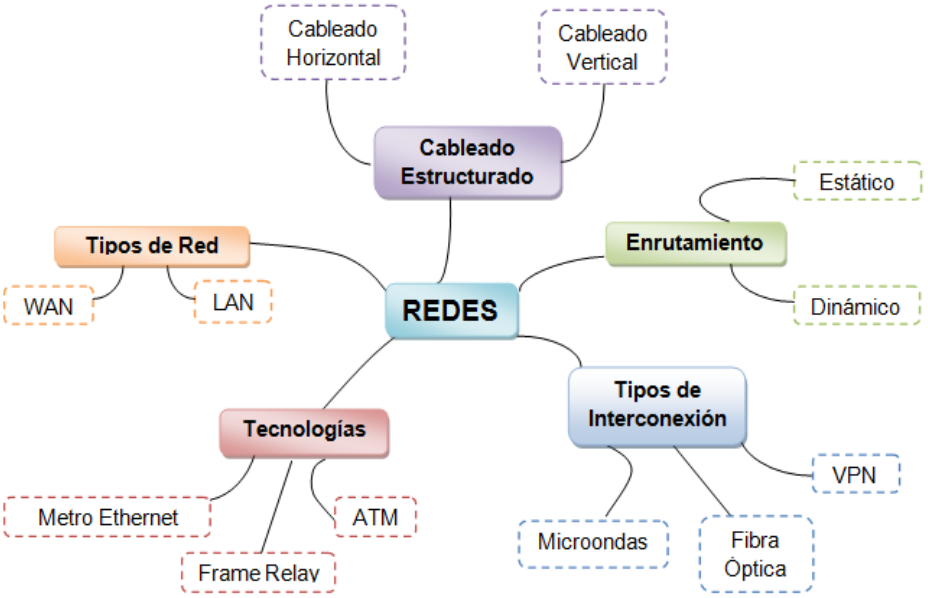


Figura 1. Mapa mental de los conceptos teóricos.

Fuente: Elaboración propia.

II.1 REDES

Una red es un conjunto de dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por

otros nodos de la red. Los enlaces conectados con los dispositivos se denominan a menudo canales de comunicación. (1)

Actualmente, cuando se habla de redes, se suele hablar de tres clases principales: redes de área local, redes de área metropolitana y redes de área amplia. (1)

Una red de área local (LAN, *Local Area Network*) suele ser una red de propiedad privada que conecta enlaces de una única oficina, edificio o campus. Dependiendo de las necesidades de la organización donde se instale y del tipo de tecnología utilizada, una LAN puede ser tan sencilla como dos PC y una impresora situadas en la oficina de la casa de alguien; o se puede extender por toda una empresa e incluir periféricos de voz, sonido y vídeo. Actualmente, el tamaño de las LAN está limitado a unos pocos kilómetros.

Las LAN están diseñadas para permitir compartir recursos entre computadoras personales o estaciones de trabajo. Los recursos a compartir pueden incluir *hardware* (por ejemplo, una impresora), *software* (por ejemplo, un programa de aplicación) o datos. Un ejemplo frecuente de LAN, que se encuentra en muchos entornos de negocios, enlaza un grupo de trabajo de computadoras relacionadas con una cierta tarea, como, por ejemplo, estaciones de trabajo de ingeniería o PC de contabilidad.

Además del tamaño, las LAN se distinguen de otros tipos de redes por su medio de transmisión y su topología. En general, una LAN determinada usará un único medio de transmisión. Las topologías más frecuentes de las LAN son el bus, el anillo y la estrella. (1)

II.1.1 REDES DE ÁREA AMPLIA

Una red de área amplia (WAN, *Wide Area Network*) proporciona un medio de transmisión a larga distancia de datos, voz, imágenes e información de vídeo sobre grandes áreas geográficas que pueden extenderse a un país, un continente o incluso al mundo entero.

Una WAN puede ser tan compleja como las troncales que conectan Internet o tan simple como la línea telefónica que conecta una computadora casera a Internet. Normalmente se denomina a la primera WAN conmutada y a la segunda WAN punto a punto. La WAN conmutada conecta los sistemas terminales, que habitualmente incluyen un enrutador (dispositivo de conexión entre redes) que conecta a otra LAN o WAN. La WAN punto a punto es normalmente una línea alquilada a un proveedor de telefonía o TV por cable que conecta una computadora casera a una LAN pequeña o a un proveedor de servicios de Internet (ISP, *Internet Service Provider*). Este tipo de WAN se usa a menudo para proporcionar acceso a Internet. (1)

II.1.3 VLAN (*Virtual Local Area Network*)

Las VLANs permite la creación de redes lógicamente independientes dentro de una misma red física, agrupando los puertos de un switch de forma que se comporten como si fuesen un switch independiente. De esta manera se permite la existencia de varias redes y subredes IP en una misma red conmutada.

Para crear las VLANs se tienen dos opciones: la primera la lleva a cabo el administrador directamente asignando los puertos a la VLAN correspondiente, este tipo es conocido como VLAN estática. En segundo lugar, se presentan las VLAN dinámicas en las cuales se requiere de un servidor de administración como *VLAN Management Policy Server* (VMPS), que con la dirección MAC (*Media Access Control*) asocia un puerto no asignado a la VLAN en consideración. (2)

Las VLANs extienden el dominio de difusión limitado por un router tradicional a un dominio de difusión limitado por VLAN, y generan un dominio de difusión con características que pueden definirse y limitarse mediante *switches* dentro de la red, reduciendo así el tráfico innecesario y aumentando en consecuencia su rendimiento.

Los puertos de los switches se pueden configurar básicamente en dos modos:

- *Modo acceso:* un puerto configurado en modo "access" indica que al puerto está conectada una única VLAN.
- *Modo troncal:* un puerto configurado en modo "trunk" sirve como puerta de salida a todas las VLAN. A pesar de que lógicamente son distintas subredes, físicamente tienen acceso al router a través de un mismo puerto, por ende transportan la información de VLANs distintas por medio del protocolo IEEE 802.1Q. (2)

II.1.3.1 TIPOS DE VLANs

Las VLANs son asociadas con un conjunto de puertos de switch en el dominio de difusión, de tal manera, que una VLAN se define por los puertos de acceso asignados a ella. Algunos tipos de LAN están definidos por el tipo de tráfico que soportan, y otros por las funciones específicas que llevan a cabo. Los principales tipos de VLAN son: las de datos, la predeterminada, la nativa y la de administración.

1. **VLAN de datos:** Está configurada para transportar únicamente tráfico generado por el usuario, también se le denomina VLAN de usuario.

2. **VLAN predeterminada:** Es aquella a la cual todos los puertos de *switch* se asignan cuando el dispositivo se reinicia con los valores predeterminados de fábrica. Si todos los puertos del *switch* son miembro de la VLAN predeterminada, todos ellos son parte del mismo dominio de difusión, lo que permite que los dispositivos conectados al mismo se comuniquen entre sí.

3. **VLAN Nativa:** está asignada a un puerto de enlace troncal IEEE 802.1Q, el cual admite el tráfico que llega de una VLAN (tráfico etiquetado) y también el que no llega de las VLANs (tráfico no etiquetado). Se establece para mantener la compatibilidad con el tráfico no etiquetado de los escenarios LAN.

4. **VLAN de administración:** Es configurada por el administrador del *switch* como medio para acceder a las capacidades de administración del mismo. A la VLAN

de administración se le asigna una dirección IP y una máscara de subred, debido a que un *switch* puede ser administrado vía http, Telnet, SSH (*Secure SHell*) o SNMP (*Simple Network Management Protocol*). (3)

II.2 METRO ETHERNET NETWORK

Es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN *(Metropolitan Area Network)* y WAN *(Wide Area Network)* de nivel 2, a través de UNIs *(Users Network Interface)* Ethernet. Estas redes denominadas *"multiservicio"*, soportan una amplia gama de servicios y aplicaciones, contando con mecanismos donde se incluye soporte a trafico "RTP" (Protocolo Tiempo Real), como puede ser telefonía IP y video IP, este tipo de trafico resulta especialmente sensible al retardo, al *jitter*. (4)

Los beneficios que Metro Ethernet ofrece son:

- Presencia y capilaridad prácticamente "universal" en el ámbito metropolitano, en especial gracias a la disponibilidad de las líneas de cobre, con cobertura universal en el ámbito urbano.
- Muy alta fiabilidad, ya que los enlaces de cobre certificados Metro Ethernet, están constituidos por múltiples pares de líneas de cobre (MAN BUCLE) y los enlaces de Fibra Óptica, se configuran mediante *Spanning tree* (activo-pasivo) o LACP (caudal Agregado).
- Fácil uso: Interconectando con Ethernet se simplifica las operaciones de red, administración, manejo y actualización.
- Economía: los servicios Ethernet reducen el capital de suscripción y operación de tres formas:
- Amplio uso: se emplean interfaces Ethernet que son la más difundidas para las soluciones de *Networking.*
- Bajo costo: Los servicios Ethernet ofrecen un bajo costo en la administración, operación y funcionamiento de la red.

- Ancho de banda: Los servicios Ethernet permiten a los usuarios acceder a conexiones de banda ancha a menor costo.
- Flexibilidad: Las redes de conectividad mediante Ethernet permiten modificar y manipular de una manera más dinámica, versátil y eficiente, el ancho de banda y la cantidad de usuarios en corto tiempo.

El modelo básico de los servicios Metro Ethernet, está compuesto por una Red switcheada MEN (*Metro Ethernet Network*), ofrecida por el proveedor de servicios; los usuarios acceden a la red mediante CEs (*Customer Equipment*), CE puede ser un router; Bridge IEEE 802.1Q (*switch*) que se conectan a través de UNIs (*User Network Interface*) a velocidades de 10Mbps, 20Mbps, 34Mbps, 100Mbps, 1Gbps y 10Gbps. (5)

A continuación, ventajas e inconvenientes que aporta Metro Ethernet frente a ATM o *Frame Relay*:

Ventajas:

• Bajo Coste: los costes para implementar la infraestructura (cables, conectores, tarjetas, equipos de interconexión, etc.) son menores, además los costes de mantenimiento y configuración de una red Ethernet también son menores que los de una red ATM o *Frame Relay*, debido a que Ethernet solo requiere conectar los equipos sin más configuración.

• Configuración rápida bajo demanda: una red sobre SDH no es fácilmente ampliable, sin embargo, Ethernet si permite esta flexibilidad, ofreciendo una gran variedad de velocidades de transmisión, (desde 10 Mbps hasta 10 Gbps), en intervalos de hasta 1 Mbps o incluso menos.

• Fácil de interconectar con otras redes: debido a que el 98% de las LAN están implementadas sobre Ethernet, no es necesaria una conversión de protocolos entre LAN y MAN, lo que facilita enormemente la integración de redes LAN en la red MAN.

Inconvenientes:

• La distancia: era una gran limitación puesto que las redes Ethernet sobre cobre podían solo cubrir una extensión de 100 metros antes de que el retardo de propagación causara una degradación seria en la comunicación.

• La fiabilidad y la redundancia*:* las redes Ethernet no eran consideradas tan fiables como las redes TDM. De hecho, los mecanismos de redundancia y recuperación ante fallos de Ethernet, como *Spaning Tree*, eran sumamente lentos e ineficientes.

• La capacidad de crecimiento*:* hechos como el continuo *broadcast* o la necesidad de aprendizaje de direcciones físicas (*MAC*) de todos los usuarios en todos los nodos de la red, ponían en entredicho la capacidad de crecimiento de la tecnología.

• La seguridad*:* Ethernet se consideraba una tecnología de medio compartido en el que los usuarios fácilmente podían acceder al tráfico de otros.

Hoy en día la tecnología proporciona las herramientas necesarias para superar dichas limitaciones, de esta manera se puede afirmar que:

• La distancia ya no es una limitación, debido a que las tecnologías ópticas nos permiten transportar Ethernet a decenas e incluso centenares de kms.

• La fiabilidad y la redundancia han dejado de ser un problema y hoy en día los fabricantes de equipamiento Ethernet aportan soluciones tan fiables como las de telefonía tradicional TDM, con tiempos de protección similares.

• La capacidad de crecimiento de las redes Ethernet se ha incrementado en varios órdenes de magnitud, gracias a modificaciones de la tecnología.

• La seguridad y la separación entre usuarios se ha reforzado gracias a tecnologías de tunelización. (5)

II.3 PROTOCOLO IP

Este protocolo implementa la capa red, es un protocolo no orientado a conexión, que se usa en una red de paquetes conmutados, garantiza la mejor ruta. Los

paquetes pueden llegar dañados, duplicados, en otro orden o no llegar, tiene direccionamiento y enrutamiento.

Direccionamiento es como se asigna las direcciones y como se dividen en redes, subredes y subsubredes.

Enrutamiento consiste en encontrar el mejor camino entre dos redes. (6)

II.4 PROTOCOLOS DE ENRUTAMIENTO

II.4.1. Protocolo de Enrutamiento de Vector Distancia

Los protocolos de enrutamiento de vector distancia que utilizan algoritmos conocidos con el nombre de Bellman-Ford y permiten transmitir el contenido de sus tablas de enrutamiento a sus vecinos, a menudo de forma periódica. Los enrutadores que usan este tipo de protocolo de enrutamiento no conocen la topología física de una red. Sólo tienen en su tabla de enrutamiento datos respecto a una red de destino, a la que se asocia una métrica que indica la "mejor" ruta. Cuando un enrutador recibe una tabla de enrutamiento de un enrutador vacío, la compara con su propia tabla. Si le proporciona nuevas rutas, las añade a su tabla de enrutamiento incrementado la métrica. Si conoce una ruta con una métrica superior o igual a la definida, no tiene en cuenta la información. Por el contrario, si recibe una ruta con una métrica menor que la que conoce, actualizará su tabla de enrutamiento por el nuevo camino.

Debido a que los protocolos de enrutamiento de vector distancia transmiten únicamente a sus vecinos sus tablas de enrutamiento de forma periódica, los tiempos de convergencia en una red que use este tipo de protocolo pueden ser largos. Se dice que la red ha convergido cuando todos los enrutadores poseen una tabla de enrutamiento al día y correcta.

A mayor número de enrutadores, más larga será la convergencia en caso de modificación de la topología. Puede ser que algunos enrutadores en un momento dado, posean datos de enrutamiento incoherentes, lo que entraña la pérdida de

paquetes IP. Para combatir este problema, cada protocolo de enrutamiento implementa una o más de estas soluciones para regular los problemas de bucle.

- Métrica máxima: utilizar un valor de métrica máximo antes de definir una ruta no válida.
- Horizonte cortado: con esto no se envía información de ruta en la misma dirección que la que la permitido aprender la ruta.
- Inversión del veneno: cuando un enrutador descubre una ruta no válida, pone en su tabla de enrutamiento una información respecto a esta red con un coste infinito y el tiempo que la red converja progresivamente. Esta técnica se emplea con un temporizador de retención
- Temporizadores de retención: cuando una ruta no es válida, el enrutador coloca un temporizador que permite al enrutador "retener" las rutas durante un cierto lapso de tiempo. Cuando un enrutador recibe de un enrutador vecino una información de ruta no válida, aplica un temporizador de retención y marca la ruta como inaccesible. Si durante este tiempo recibe una información del mismo vecino que indica que la red es de nuevo accesible, el temporizador se suprime y la ruta se marca de nuevo como válida. (7)

II.4.2 Protocolo de Enrutamiento de Estado de Enlace

Los protocolos de enrutamiento de estado de enlace mantienen una tabla de enrutamiento que funcionan con un algoritmo SPF (*Short Path First*). Los enrutadores que implementan este tipo de protocolo de enrutamiento disponen de una vista completa de una red. No se intercambian tablas de enrutamiento, sino los datos que permiten construir dicha tabla, Los protocolos de enrutamiento de estado de enlace utilizan paquetes de estado de enlace (LSP, *Link State Package*), una base de datos topológica, un algoritmo SPF que permite construir un árbol de la red mediante paquetes SPF recibidos y una tabla de enrutamiento que indica los caminos para alcanzar redes de destino.

Este tipo de protocolos convergen muy rápido, y utilizan métricas sofisticadas basadas generalmente en el coste de una conexión que, a su vez, se basa en la velocidad de conexión.

Aunque este protocolo sea más potente y rápido que el protocolo de enrutamiento de vector de distancia, es más complejo de comprender e implementar, y consume más recursos del sistema. El protocolo de enrutamiento de estado de enlace transmitirá LSP, que habrá que analizar con un algoritmo SPF y volver a transcribir en una tabla de enrutamiento, lo cual entraña un fuerte consumo de ancho de banda. (7)

II.4.3 RIP (*Routing Information Protocol*)

Es un protocolo de enrutamiento de vector distancia. RIP transmite toda la tabla de enrutamiento a todas las interfaces activas cada 30 segundos. RIP lleva una cuenta de saltos solo para determinar la mejor vía hacia una red remota, pero tiene un máximo de 15 saltos permitidos por defecto. Esto quiere decir que una red cuyos paquetes pueden llegar a atravesar 16 enrutadores para alcanzar su destino no pueden usar este protocolo. RIP funciona bastante bien en redes pequeñas, pero es ineficiente en redes más grandes con enlaces WAN lentos o en redes que tengan muchos enrutadores. (8)

RIP versión 1 utiliza solamente enrutamiento por clases, que significa que todos los equipos en una red deben tener la misma máscara de subred. Esto sucede porque RIP versión 1 no manda *updates* con máscara de subred.

RIP versión 2 en cambio trabaja con enrutamiento sin clases, quiere decir que sí envía información sobre la máscara de subred cuando envía *updates* porque soporta VLSM (*Variable Length Subnet Mask*). Otra ventaja que ofrece RIPv2 sobre RIPv1, sería que es capaz de usar un mecanismo de autenticación. (7)

RIP, además de tener el problema de máximo 15 saltos, también tiene un problema de conteo al infinito (dado que se basa en el algoritmo de Bellman-Ford).

Este problema puede surgir en situaciones atípicas en las cuales se puedan producir bucles, ya que estos bucles pueden producir retardos e incluso congestión en redes en las cuales el ancho de banda sea limitado. Aparte también utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependan de parámetros a tiempo reales como por ejemplo retardos o carga del enlace. (8)

II.4.4 OSPF (*Open Short Path First*)

OSPF soporta tres tipos de conexiones y redes:

- Las líneas punto a punto exactamente entre dos enrutadores
- Redes de multiacceso con difusión
- Redes de multiacceso sin difusión

Una red multiacceso es la que puede tener múltiples enrutadores, cada uno de los cuales se puede comunicar directamente con todos los demás.

OSPF funciona hacienda una abstracción del conjunto de redes, enrutadores y líneas en un grafo dirigido en el que a cada arco se le asigna un costo. Entonces calcula la trayectoria más corta con base en los pesos de los arcos. Una conexión en serio entre dos enrutadores se representa por un par de arcos, uno en cada dirección. Sus pesos pueden ser diferentes. Una red multiacceso se representa con un nodo para la red en sí más un nodo para cada enrutador. Los arcos del nodo de la red a los enrutadores tienen peso 0 y se omiten del grafo.

Cada sistema autónomo tiene un área de red dorsal, llamada 0. Todas las áreas se conectan a la red dorsal, posiblemente por túneles, de modo que es posible entrar desde cualquier área en el sistema autónomo a cualquier otra área en el sistema autónomo mediante la red dorsal. Cada enrutador que se conecta a dos o más áreas es parte de la red dorsal. Como con otras áreas, la topología de la red dorsal no es visible fuera de ésta.

Dentro de un área, cada enrutador tiene la misma base de datos del estado del enlace y ejecuta el mismo algoritmo de la ruta más corta.

OSPF distingue cuatro clases de enrutadores:

- Enrutadores internos que están totalmente dentro de un área.
- Enrutadores de límite de área que conectan dos o más áreas.
- Enrutadores fronterizos de sistemas autónomos que se comunican con los enrutadores de otros sistemas autónomos.

OSPF trabaja intercambiando información entre enrutadores adyacentes, que no es lo mismo que entre enrutadores vecinos. En particular, es ineficaz tener cualquier enrutador en la LAN que se comunica con cualquier otro enrutador en la LAN. Para evitar esta situación, se elige un enrutador como enrutador designado. Se dice que es adyacente a todos los demás enrutadores en su LAN, e intercambia información con ellos. Los enrutadores vecinos que no son adyacentes no intercambian información entre sí. Un enrutador designado como respaldo siempre se guarda actualizado, para facilitar la transición en caso de que el primer enrutador designado se cayera y necesitara ser reemplazado de manera inmediata. (9)

II.5 CALIDAD DE SERVICIO (QoS)

La calidad de servicio (QoS) es el rendimiento de extremo a extremo de los servicios electrónicos tal como lo percibe el usuario final. Los parámetros de QoS son: el retardo, la variación del retardo y la pérdida de paquetes. Una red debe garantizar un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros.

La implementación de Políticas de Calidad de Servicio se puede enfocar en varios puntos según los requerimientos de la red, los principales son:

- Asignar ancho de banda en forma diferenciada

- Evitar y/o administrar la congestión de la red
- Manejar prioridades de acuerdo al tipo de tráfico
- Modelar el tráfico de la red (10)

La calidad de servicio de la red depende básicamente de dos aspectos: que existan suficientes recursos en la red y que los mecanismos para manejar el tráfico utilicen eficientemente los recursos disponibles. Proporcionar en una red QoS basada en servicios diferenciados será más complicado que en una red basada en el mejor esfuerzo, ya que en entornos *multicast* puede haber receptores heterogéneos con requerimientos diferentes de QoS. La QoS se define con base en los parámetros de transmisión que describen la métrica de un modelo de QoS y con base en el alcance para delimitar la QoS. (11)

II.6 SEGURIDAD

La seguridad en su forma más sencilla, se ocupa de garantizar que los curiosos no puedan leer, o peor aún, modificar mensajes dirigidos a otros destinatarios. Tiene que ver con la gente que intenta acceder a servicios remotos no autorizados.

Los problemas de seguridad de las redes pueden dividirse en términos generales en cuatro áreas interrelacionadas: confidencialidad, autenticación, no repudio y control de integridad. La confidencialidad consiste en mantener la información fuera de las manos de usuarios no autorizados. La autenticación se encarga de determinar con quién se está hablando antes de revelar información delicada o hacer un trato de negocios. El no repudio se encarga de las firmas. Por último ¿Cómo puede asegurarse de que un mensaje recibido realmente fue enviado, y no algo que un adversario malicioso modificó en el camino o cocinó por su propia cuenta?

Todos estos temas, son pertinentes también en los sistemas tradicionales, pero con algunas diferencias importantes. La confidencialidad y la integridad se logran usando correo certificado y poniendo bajo llave los documentos. (8)

Una técnica muy usada actualmente para la seguridad es la criptografía.

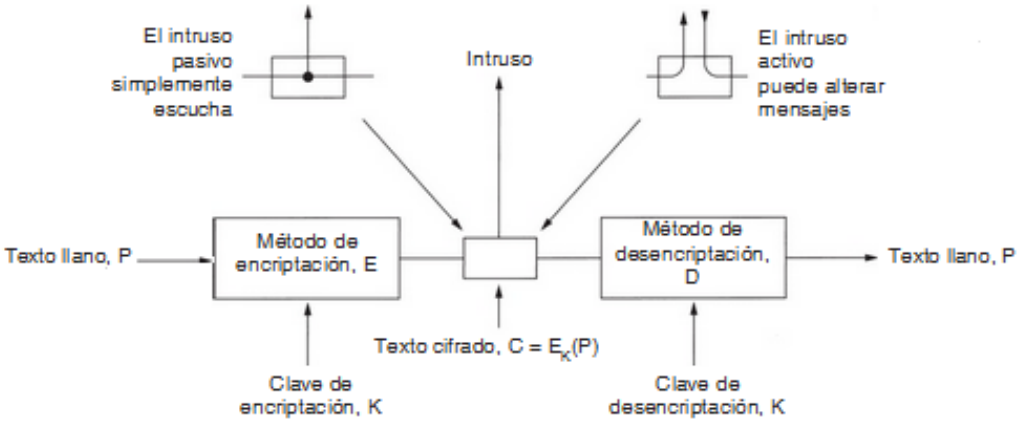


Figura 2. El modelo de cifrado **(8)**

Los mensajes por cifrar, conocidos como texto llano, son transformados por una función parametrizada por una clave. El resultado del proceso de cifrado, conocido como texto cifrado, se transmite a continuación. Si un intruso desea escuchar y copiar todo el texto cifrado, no conocerá la clave de descifrado y no podrá descifrar con facilidad el texto cifrado.

Los métodos de cifrado han sido divididos históricamente en dos categorías:

- Cifrados pos sustitución: cada letra o grupo de letras se reemplazan por otra letra o grupo de letras para disfrazarla. El sistema general de sustitución por símbolo se llama sustitución monoalfabética, siendo la clave la cadena de 26 letras correspondiente al alfabeto completo. Si se cuenta con una cantidad pequeña de texto cifrado, puede descifrarse fácilmente. El ataque básico aprovecha las propiedades estadísticas de los lenguajes naturales.

- Cifrados por transposición: reordenan las letras pero no las disfrazan. La clave del cifrado es una palabra o frase que no contiene letras repetidas. El propósito de la clave es numerar las columnas, estando las columnas bajo la letra más cercana al inicio del alfabeto, y así sucesivamente. El texto llano se escribe horizontalmente, en filas, las cuales se rellenan para completar la matriz si es necesario. El texto cifrado se lee por columnas, comenzando por la columna cuya letra clave es la más baja. (8)

II.6.1. FIREWALL

Un *firewall* es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un *firewall* es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el *firewall* examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el *firewall* decide si lo permite o no. Además, el *firewall* examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un *firewall* puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del *firewall* que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un *firewall* puede ser un dispositivo *software* o *hardware*, es decir, un aparato que se conecta entre la red y el cable de la conexión a Internet, o bien un programa

que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con *software*s específicos que lo único que hacen es monitorizar las comunicaciones entre redes. (12)

II.7 VPN

Una red privada virtual (VPN) es una red privada construida dentro de una infraestructura de red pública, tal como la red mundial de Internet. Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet económicos proporcionados por terceros, en vez de costosos enlaces WAN dedicados o enlaces de marcación remota de larga distancia.

Las organizaciones pueden usar redes privadas virtuales para reducir los costos de ancho de banda de redes WAN, y a la vez aumentar las velocidades de conexión a través de conectividad a Internet de alto ancho de banda, tal como DSL, Ethernet o cable. (13)

Las VPNs trabajan en diferentes capas del modelo ISO/OSI, siendo la capa 2 (enlace) y capa 3 (red) las más usadas. La VPN menos usada, como una alternativa a la usada en capa 2 y capa 3, opera en la capa 4 (transporte).

Las VPNs que operan en capa 2 pueden operar con una red pública de *frame relay*, donde la red depende de equipos de acceso de frame relay y enrutadores o switches conectado mediante canales. LA VPN se establece configurando circuitos virtuales permanentes, los cuales son visto como una porcion de la capacidad del canal. De este modo, un VPN formada sobre un frame relay puede conectar dos sitios remotos, una ciudad A con una ciudad B, o bien, estas dos con una tercera ciudad C. La seguridad normalmente no es un asunto particularmente importante cuando se trabaja con frame relay dado que los circuitos virtuales permanentes, representan rutas configuradas previamente a través de la red para clientes ya definidos. De esta

manera, a menos que el operador de la red se encuentre haciendo algo indebido, hay una mínima posibilidad que un cliente de la red obtenga información sobre otro. (14)

Muchas empresas han incrementado la mobilidad de sus trabajadores logrando una comunicación para los empleados, y a su vez estos, al viajar tienen la necesidad de estar conectados a las redes de la compañía. Por esta razón, surgio una VPN que funciona por acceso remoto, permitiendo el acceso a través de internet a las redes corporativas. Este tipo de VPN utiliza un diseño cliente/servidor que sigues los siguientes pasos:

- Un *host* o cliente remoto que desee acceder a la red de la compañía debe conectarse primero a un ISP (proveedor de servicio de internet) público.
- Posteriormente, el *host* inicia una conexión VPN al servidor VPN de la compañía. Dicha conexión se logra mediante un servidor VPN instalado en el *host* remoto.
- Una vez establecida la conexión, el cliente remoto puede comunicarse con el sistema interno de la compañía a través de la internet, como si fuera un *host* local. (15)

Una VPN muy usada es la llamada *site-to-site* la cual trabaja en capa 3 y conecta dos sitios a traves de una red pública como la internet. Este tipo de VPN es utilizada en su mayoría para conectar múltiples clientes en una oficina a computadoras corporativas ubicadas en una región o en la casa matriz. Asimismo, clientes en una casa matriz o region pueden tener acceso a las computadoras en una determinada sucursal.

Montar una VPN requiere saber que servicio se ofrecerá y asi poder adaptarse a ello, usando solamente *software* o *software* con un *hardware* adicional. Si no se necesita mucho ancho de banda se puede trabajar exclusivamente con *software* sobre los clientes para establecer una conexión de VPN a un servidor. Por otro lado, si el desempeño de un servidor se vuelve deficiente cuando un número de clientes quiere acceder al mismo, es recomendable añadir un *hardware* acelerador de cifrado. Si en cambio se quiere conectar dos o mas sitios con una gran cantidad de clientes con

conexiones VPN individuales a uno o más lugares determinados, se deberá utilizar un VPN de *hardware*. Usar un enrutador con un acelerador VPN o un *gateway* VPN eliminaría la carga tanto en el cliente como en el servidor. (15)

II.7.1. AUTENTICACIÓN Y CIFRADO

La autenticación representa el proceso de identificar al usuario, la ubicación del usuario o la computadora. Una manera de autentificar a nivel de computadora cuando se ha usado un VPN de capa dos, es un intercambio de certificado de computadoras o PSK (*preshared key*) mientras se establece el protocolo de seguridad de internet (IPSec). A nivel de usuario, se utiliza el protocolo *point-to-point*. (19)

El cifrado de un VPN se puede realizar de dos formas que son transporte y *tunneling.* El cifrado por transporte establece un *link* cifrado, seguro a través de internet, y cifra la data (*payload*) que se está enviando al otro sitio. El cifrado es invisible al usuario, apartando la contraseña o una tarjeta especial para conectarla a la computadora, el usuario no tiene que cifrar o descifrar en ningún momento. Toda la información o data que se está enviando es protegida de manera que no pueda ser vista. Sin embargo, el cifrado por transporte tiene un defecto grande, a pesar que la información que se transmite esta oculta, sus respectivas cabeceras se mandan sin protección alguna. Al mandar las cabeceras de la data de esta manera, quedan a la vista para cualquier intruso que tenga acceso. (16)

El cifrado por *tunneling*, no sólo establece un enlace cifrado y seguro entre dos sitios, sino que además cifra las cabeceras de los datos. Existen varios protocolos de *tunneling*, los más comunes son los siguientes:

- *Point-to-point tunneling protocol (PPTP):* permite cifrar tráfico multiprotocolo para luego encapsularlo en una cabecera IP y mandarlo en una red IP o una red IP pública, como internet. Este tipo de cifrado de utiliza para una VPN *site-to-site* o de acceso remoto. PPTP emplea una conexión TCP para manejo de túneles y una versión modificada de encapsulamiento por enrutamiento genérico (GRE) para encapsular marcos PPP para la data tunelizada.

- *Layer two tunnelig protocol* (L2TP): es muy vinculada a PPTP, permite cifrar tráfico multiprotocolo y mandarlo bajo cualquier medio que soporte entrega de datagrama *point-to-point*, tal como IP o ATM. Se apoya en IPsec para servicios de cifrado en el modo transporte. Para poder usar este tipo de cifrado, el cliente y servidor VPN deben soportar L2TP e IPsec. La encapsulación consiste de dos capas, en la capa uno (encapsulación L2TP) y en la capa dos (encapsulación IPsec).
- *Secure Socket Tunneling Protocol (SSTP):* es un nuevo protocolo que utiliza el protocolo HTTPS y el puerto TCP 443 para que pase el tráfico a través del proxy *firewall* que podrían bloquear tráfico PPTP y L2TP/IPsec. Provee un mecanismo para encapsular tráfico PPP sobre el *Secure Sockets Layer* (SSL). Cuando un cliente intenta establecer una conexión VPN basada en SSTP, SSTP primero establece una capa HTTPS bidireccional con el servido SSTP. Sobre esta capa HTTPS, los paquetes del protocolo fluyen como la carga útil (*payload).* (17)

II.7.2 VENTAJAS DE UNA VPN

Una VPN es una solución para establecer una red segura a larga distancia y por lo general son implementadas por negocios u organizaciones. Es una solución cuya principales ventajas son el ahorro en costos (mantenimiento de bajo costo) y la escalabilidad.

Antes de la implementación de las VPN, las empresas tenían que alquilar la capacidad de red, como líneas T1 para lograr una conexión segura y completa entre sus oficinas. Con una VPN, se puede utilizar internet o alguna otra red pública para hacer la conexión y entrar a la red virtual a través de líneas locales alquiladas de un costo mucho más bajo, o una conexión banda ancha a un ISP cercano.

En el pasado era común usar servidores de acceso remoto y una conexión por línea telefónica de larga distancia para poder acceder al intranet de la compañía al momento de viajar. Establecer una VPN sustituye la necesidad de lo anterior, dado que el cliente solo necesita conectarse al *access point* más cercano (lo cual es por lo usual es local).

Cuando no se utiliza una VPN sino cualquier otra alternativa o recurso, ocurren problemas a medida que la red vaya creciendo con más personas por oficinas. Este problema de escalabilidad se elimina cuando se utiliza una VPN dado que simplemente entran a las líneas y redes públicas que tengan capacidad disponible. (15)

II.8 FIBRA ÓPTICA

La fibra óptica es una nueva tecnología de cable que se utiliza para la instalación de redes locales. Consiste en un núcleo central muy delgado de vidrio con alto índice de refracción de la luz. Alrededor de este núcleo hay un revestimiento también a base de vidrio pero con índice de refracción más bajo que protege al núcleo de contaminación y provoca el fenómeno de refracción interna, es decir, que cuando un rayo de luz (información) entra por un extremo del cable no se disipa hacia el exterior sino que mediante reflexiones sucesivas dentro del núcleo se propaga hasta el otro extremo de la fibra. (18)

Ventajas

El uso de las fibras ópticas como medio de transmisión luminoso presenta muchas ventajas. Algunas de ellas son las siguientes:

- Son muy delgadas. Un cable de fibra óptica tiene un diámetro mucho más pequeño que un cable de cobre con la misma capacidad de transmisión, por lo que pueden agregarse fácilmente a instalaciones existentes, donde ya hay cables (por ejemplo, en las tuberías usadas en el *backbone* de la red).
- Son livianas, en comparación con los cables metálicos.
- No conducen electricidad, por lo tanto, su uso carece de riesgos eléctricos.
- Transmiten la información en forma segura. Mientras que las señales de comunicación vía satélite o por radio se pueden interferir fácilmente, las señales transmitidas por las fibras ópticas no son fácilmente interferibles.

Además, las posibles interferencias se detectan en forma sencilla con un detector de señales ópticas. Esta ventaja es muy importante para mantener la confidencialidad de la información.

- Duran mucho tiempo. No son afectadas por condiciones externas como la temperatura y la humedad (incluso pueden usarse en cables subacuáticos). No se dañan por cortocircuitos o sobretensiones eléctricas.
- Son compatibles con la tecnología digital. (18)

Desventajas

- Necesitan conversores, *transceiver*, para que la fibra óptica transmita la señal, el cual debe transformarla de eléctrica a luminosa; al llegar a destino nuevamente debe transformarse en señal eléctrica. Estas conversiones hacen más cara la comunicación.
- Son frágiles.
- No se reparan fácilmente. En caso de que un cable de fibra óptica se dañe, se requiere de personal especializado para repararlo. (18)

II.9 APLICACIONES

II.9.1 Videoconferencia

Se puede definir una videoconferencia como la interacción en tiempo real entre dos o más participantes remotos que intercambian señales de audio y vídeo. (19)

Los participantes se pueden escuchar unos a otros y pueden verse en vídeo. También pueden compartir documentos o archivos entre los participantes. Un sistema de videoconferencia puede proveer casi todas las opciones de presentación e intercambio de información que se realizan en una reunión cara a cara.

Un sistema de videoconferencia es una herramienta que representa un arma estratégica en un mercado de información de alta competitividad. Efectivamente,

compartir información de manera eficaz y económica es un requisito para sobrevivir en todas las áreas de la industria, negocios, gobierno, educación y entretenimiento. (19)

La videoconferencia ofrece hoy en día una solución accesible a esta necesidad de comunicación con sistemas que permiten el transmitir y recibir información visual y sonora entre puntos o zonas diferentes evitando así los gastos y pérdida de tiempo que implican el traslado físico de la persona, todo esto a costos cada vez más bajos y con señales de mejor calidad. Estas ventajas hacen a la videoconferencia el segmento de mayor crecimiento en el área de las telecomunicaciones. (19)

II.9.2 Estándares

Los siguientes estándares usados en el campo de la Videoconferencia. Están definidos dentro del conjunto de normas UIT H.320 y H.323:

G.711: *bit-rate* de 56 o 64 Kbps.
G.722: *bit-rate* de 48, 56 o 64 Kbps.
G.723: *bit-rate* de 5,3 o 6,4 Kbps.
G.728*: bit-rate* de 16 Kbps.
G.729: *bit-rate* de 8 o 13 Kbps.

Diversos Códecs admiten diversas velocidades para adecuarse a la capacidad de transmisión de las redes de comunicación subyacentes. Solamente G.711 debe implementarse obligatoriamente en un sistema de videoconferencia H.32x. (19)

II.9.3 Voz Sobre IP

La telefonía de voz sobre IP y el Protocolo de Internet (IP) cada vez son más populares entre empresas y consumidores. La voz sobre IP proporciona a su empresa una base para ofrecer aplicaciones de comunicaciones unificadas más avanzadas,

incluyendo videconferencias y conferencias en línea, que pueden transformar su forma de hacer negocios. (20)

II.9.4 Session Initiation Protocol (SIP)

El protocolo de señalización de inicio de sesión, del inglés Session Initiation Protocol (SIP), fue desarrollado por el IETF, es responsable de establecer las llamadas del resto de funciones de señalización. Cuando se habla de señalización en el contexto de llamas de voz, se está hablando de la indicación de la línea ocupada, los tonos de llamada o que alguien ha contestado del otro lado de la línea.

SIP hace tres cosas importantes:

- Encargarse de la autentificación.
- Negociar la calidad de una llamada telefónica (Una de las grandes diferencias entre la telefonía tradicional y la IP es que la calidad de servicio de una conversación se puede negociar).
- Intercambiar las direcciones IP y puertos que se van a utilizar para enviar y recibir las "conversaciones de voz".

II.9.5 Ventajas de la voz sobre IP

La voz sobre IP y las comunicaciones unificadas le permiten:

- Reducir los gastos de desplazamiento y formación, mediante el uso de videoconferencias y conferencias en línea.
- Actualizar su sistema telefónico de acuerdo a sus necesidades.
- Tener un número de teléfono que suena a la vez en varios dispositivos, para ayudar a sus empleados a estar conectados entre sí y con sus clientes.
- Reducción de gastos telefónicos.
- Utilizar una sola red para voz y datos, simplificando la gestión y reduciendo costes.

- Acceder a las funciones de su sistema telefónico en casa o bien en las oficinas de sus clientes, en aeropuertos, hoteles o en cualquier parte donde haya una conexión de banda ancha. (20)

II.9.6 Terminología útil relacionada con voz sobre IP

- Por **voz sobre IP** (VoIP) se entiende el método utilizado para transportar llamadas telefónicas sobre una red IP de datos, ya sea que se trate de Internet o de la red interna de una organización. Una de las principales ventajas de la voz sobre IP es la posibilidad de reducir gastos ya que las llamadas telefónicas se transportan por la red de datos en lugar de a través de la red de la compañía telefónica.
- La **telefonía IP** incluye el conjunto completo de servicios habilitados por VoIP, como la interconexión de teléfonos para comunicaciones; servicios relacionados como facturación y planes de marcación; y funciones básicas que pueden incluir conferencias, transferencia de llamadas, reenvío de llamadas y llamada en espera.
- **Las comunicaciones IP** admiten funciones como la mensajería unificada, los centros de atención y manejo de contactos integrados y conferencias multimedia con voz, datos y vídeo.
- Las **Comunicaciones Unificadas** elevan a las comunicaciones IP a un nivel superior al utilizar tecnologías SIP (Protocolo de inicio de sesión), junto con soluciones de movilidad, con el fin de unificar y simplificar todas las formas de comunicación, con independencia del lugar, tiempo o dispositivo. (21)

II.9.7 Servicios de voz por IP

Las funciones de voz sobre IP están disponibles en una variedad de servicios. Algunos servicios básicos y gratuitos de voz sobre IP requieren que todas las partes estén en sus computadores para recibir llamadas. Otros admiten llamadas desde un aparato telefónico tradicional e incluso de un teléfono móvil a cualquier otro teléfono.

Equipos de voz sobre IP

Para voz sobre IP, es necesario tener una conexión a Internet de banda ancha, además de un teléfono tradicional y un adaptador, o un teléfono habilitado para voz sobre IP o *software* de voz sobre IP en el computador.

Calidad de servicio y seguridad de la voz sobre IP

La mayoría de los servicios de voz sobre IP para el consumidor utilizan Internet pública para realizar llamadas. Pero muchas empresas utilizan voz sobre IP y comunicaciones unificadas a través de sus redes privadas. Eso se debe a que las redes privadas proporcionan una seguridad más robusta y una mejor calidad de servicio que Internet. (20)

II.10 CABLEADO ESTRUCTURADO

En la actualidad se puede observar como los edificios son dotados de diferentes servicios que implican un mayor o menor nivel tecnológico, servicios como aire acondicionado, seguridad y megafonía permiten dotar a la infraestructura con comodidades y beneficios que hacen la experiencia del usuario más amena y sencilla. El desarrollo actual de las comunicaciones hace necesario el empleo de un sistema de cableado estructurado capaz de soportar los sistemas de red requeridos por los usuarios.

Algunas de las ventajas que ofrece el cableado estructurado son:

- Debido a que el sistema de cableado es independiente de la aplicación y del proveedor, los cambios en la red y en el equipamiento pueden realizarse utilizando la estructura de cableado existente.

- Pueden hacerse modificaciones de topología en los nodos finales de la red sin necesidad de alterar el cableado.

- La administración de la red se simplifica de forma considerable.

El cableado estructurado implica que todos los servicios en el edificio para las transmisiones de voz y datos se hacen conducir a través de un sistema de cableado en común. En 1991, la asociación de las industrias electrónicas desarrollaron el estándar comercial de telecomunicaciones designado "EIA/TIA568", este estándar especifica una gran variedad de parámetros de cableado para edificios, desde el cable de *Backbone,* usado para conectar los closets de comunicación con los equipos de trabajo, hasta el cableado horizontal, utilizado para el cableado desde cada usuario individual al closet de comunicaciones, también se definen las características de desempeño del cableado, así como el tipo de conectores y cables. (22)

II.11 SUBSISTEMAS DE CABLEADO ESTRUCTURADO

Existen siete subsistemas relacionados con el sistema de cableado estructurado, como se ve en la Figura 3. Cada subsistema realiza funciones determinadas para proveer servicios de datos y voz en toda la planta de cables: (23)

- Punto de demarcación (demarc) dentro de las instalaciones de entrada (EF) en la sala de equipamiento.
- Sala de equipamiento (ER)
- Sala de telecomunicaciones (TR)
- Cableado *backbone*, también conocido como cableado vertical
- Cableado de distribución, también conocido como cableado horizontal.
- Área de trabajo (WA)
- Administración

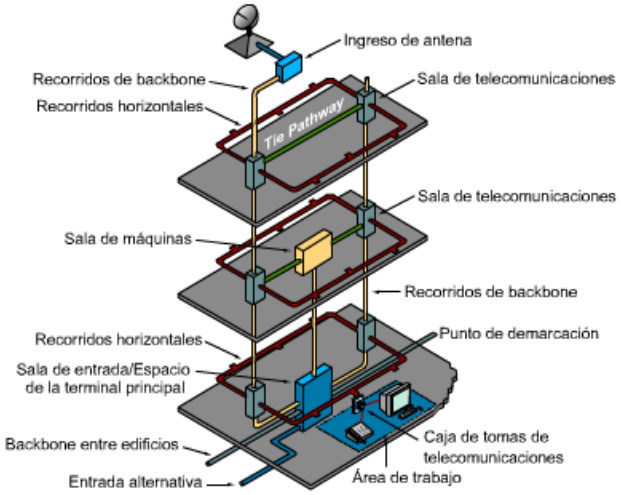


Figura 3. Subsistemas de cableado estructurado **(23)**

II.11.1. EIA/TIA568

Dentro de este estándar se definen dos estructuras principales:

- **Cableado Vertical o de *Backbone:*** Cualquier cableado instalado entre la conexión cruzada principal (MC) y otra sala de telecomunicaciones (TR) se conoce como cableado *backbone*. Es el encargado de la interconexión entre cuartos de entrada de servicios, cuartos de equipos y cuartos de telecomunicaciones. (23)

El estándar EIA/TIA568 define los medios que pueden ser utilizados para este tipo de cableado, estos se pueden observar en la siguiente tabla:

Tabla 1. Medios utilizados para el Backbone **(22)**

Medio	Distancia Máxima Cable
100 ohm UTP	800 metros
150 ohm STP	700 metros
50 ohm cable coaxial grueso	500 metros
50 / 125 µ fibra óptica multimodal	2500 metros

El cableado Horizontal: Es la conexión cruzada horizontal (HC) va desde la sala de telecomunicaciones más cercana, hasta las áreas de trabajo. La HC, es un panel de conexión o un bloque de inserción a presión, puede contener dispositivos de *networking* como repetidores, *hubs* o *switches.* Puede estar montada en un bastidor en una habitación o gabinete. Dado que un sistema de cableado horizontal típico incluye varios tendidos de cables a cada estación de trabajo, puede representar la mayor concentración de cables en la infraestructura del edificio. Un edificio con 1,000 estaciones de trabajo puede tener un sistema de cableado horizontal de 2,000 a 3,000 tendidos de cable. (23)

CAPÍTULO III
METODOLOGÍA

Este capítulo abarca los procedimientos y procesos utilizados para poder alcanzar el cumplimiento de los objetivos tanto generales como específicos, que se han planteado para realización de este Trabajo Especial de Grado.

Se propone un plan de investigación compuesto por varias fases, las cuales se describen a continuación en la figura 4:

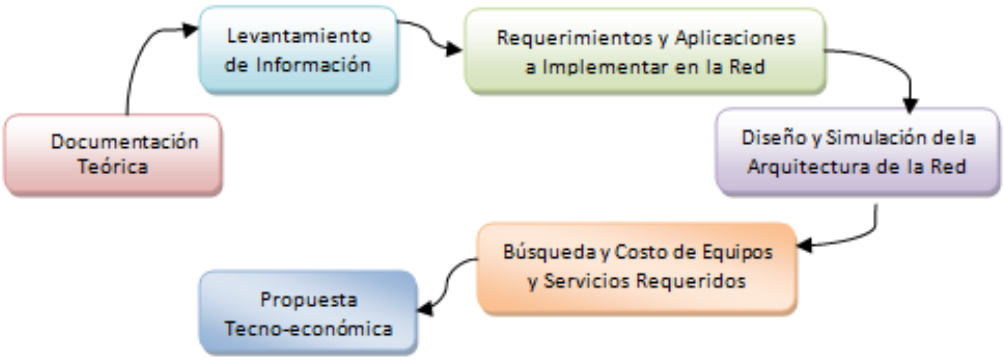


Figura 4. Fases Metodológicas.

Fuente: Elaboración propia.

III.1 Documentación Teórica

En esta primera fase se realizó el estudio de las diferentes tecnologías de transporte de datos actuales, medios físicos de transporte, topologías de redes, servicios de datos (videoconferencia, correo electrónico, video *stream* entre otras).

III.2 Levantamiento de Información

En esta fase se realizó el levantamiento de información de cada una de las sedes que conforman la empresa OnlyTicket Eventos.

Para los fines de obtener la mayor información posible acerca del funcionamiento de las distintas sedes, se llevo a cabo una reunión con los directivos y operadores de red, donde se obtuvieron los distintos elementos que conforman la red actual y se hizo un reconocimiento de la estructura física de la empresa.

Así mismo, se dieron a conocer los requerimientos, aplicaciones y servicios que la empresa desea que sean incluidos en el desarrollo de este proyecto.

III.3 Requerimientos y Aplicaciones a Implementar en la Red

Esta fase consistió en la clasificación de los servicios requeridos por la empresa, tomando en cuenta aspectos como costos, retardo, consumo de ancho de banda, instalación, mantenimiento, velocidades de transmisión, entre otros. La clasificación, se realizó de la siguiente manera:

En primer lugar, se encuentran los Servicios de Seguridad, en segundo lugar, se encuentran los Servicios de Gestión, dirigidos a los operadores de red, y en tercer lugar, se encuentran las aplicaciones específicas con las que debe contar cada una de las sedes para realizar sus funciones y para mantener la interoperabilidad entre ellas.

III.4 Diseño y Simulación de la Arquitectura de la Red

El desarrollo de esta fase se llevó a cabo a través de las siguientes etapas:

III.4.1 Dimensionamiento de la Red (Ancho de Banda y estimación de tráfico)

Luego de definir las aplicaciones y servicios a implementar en la red, fue necesario determinar el tráfico generado por cada uno de ellos, para así determinar el ancho de banda y velocidad mínimos requeridos por el sistema.

Para realizar la estimación del tráfico y ancho de banda generado por cada una de las aplicaciones se efectuó un análisis, el cual se encuentra reflejado en el siguiente Capítulo.

III.4.2 Selección de la Tecnología a Implementar

Para la ejecución de esta etapa, es necesario tomar en cuenta los siguientes parámetros:

- Sistemas de transporte de alta velocidad y alto consumo de ancho de banda.
- Interoperabilidad entre las redes de dato y video.
- Enlaces de redundancia.
- Escalabilidad de la red.
- Comunicación de forma libre y segura entre redes remotas.

III.4.3 Diseño de la Topología.

En esta etapa se llevo a cabo el diseño de la topología con la que contaría la red a diseñar, tomando en cuenta la tecnología elegida anteriormente y el mecanismo de protección y respaldo de los datos.

III.4.4 Direccionamiento IP.

Para llevar a cabo la etapa de direccionamiento fueron elegidas direcciones IP privadas y públicas, estáticas y dinámicas. La distribución y asignación de las direcciones será especificado en el Capítulo IV.

III.4.5 Cableado Estructurado

Esta etapa se basa en la escogencia de los elementos más eficientes necesarios a la hora de conectar los equipos dentro de los distintos departamentos de la empresa.

III.4.6 Simulación.

Una vez realizado el diseño de la red de comunicaciones, se procedió a la elección del *software* utilizado para poder realizar la simulación de los distintos elementos presentes en el diseño.

III.5 Búsqueda de Equipos y Servicios Requeridos

Luego de elaborar el diseño y la simulación de la red, se realizó una búsqueda de los distintos equipos que cumplieran con las necesidades de la red. Se consultaron costos, los cuales fueron proporcionados por distintos proveedores. Adicionalmente, se consultó el costo de la implementación de las tecnologías elegidas, mediante la empresa escogida proveedora de dichos servicios.

III.6 Propuesta técnico-económica

En esta fase, habiendo realizado un estudio sobre la red a implementar y teniendo el precio de cada uno de los equipos y servicios, se procedió a realizar un presupuesto con los costos de equipos más económicos encontrados, que se adaptaran a las características de la red.

CAPÍTULO IV
DESARROLLO Y RESULTADOS

A continuación se hace una descripción detallada referente a los pasos y métodos para cumplir cada una de las fases mostradas en la metodología, con el fin de poder concluir el diseño de la red de interconexión de OnlyTicket Eventos.

IV.1 Documentación Teórica

La investigación teórica se basó en el estudio de los conceptos fundamentales para el desarrollo de este proyecto como lo son las tecnologías de transporte, medios físicos de transporte, topologías de redes y otros conceptos referentes al tema. Las fuentes consultadas de donde se obtuvieron todas las informaciones y conceptos previamente descritos, fueron libros, trabajos especiales de grado, de diversos países, así como también fuentes electrónicas, documentos encontrados en la web, siendo este uno de los principales medios, ya que el tema central se encuentra en constante evolución debido a su importancia en las telecomunicaciones.

Los resultados de esta fase, se presentan con la realización del marco teórico, el cual abarca el Capítulo II de este Trabajo Especial de Grado, logrando así tener los conceptos y definiciones que dan basamento a este proyecto.

En la figura 5 se muestra un esquema en el que se mencionan los conceptos principales que forman parte del marco teórico.

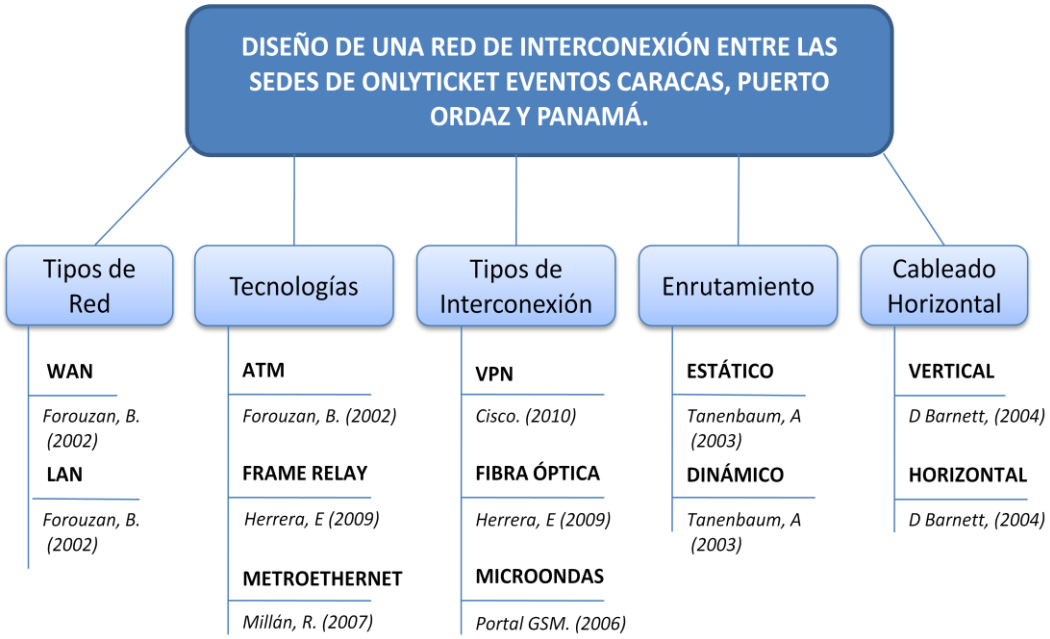


Figura 5. Mapa conceptual de los contenidos que conforman el Marco Teórico.

Fuente: Elaboración propia

IV.2 Levantamiento de Información

El levantamiento de información realizado fue tanto de la topología de la red presente así como de la estructura física y organizativa de OnlyTicket Eventos.

Se realizaron visitas a la sede de Caracas en donde se obtuvo la información referente a la estructura de red de la empresa, como el estado actual del cableado, presencia de los cuartos de telecomunicaciones y cableado estructurado. Debido a la distancia a la que se encuentran el resto de las sedes, la información fue facilitada por los directivos y operadores de red de la empresa.

IV.2.1 Infraestructura física de la Empresa OnlyTicket Eventos.

La empresa OnlyTicket tiene una estructura física en cada sede fija que consta de cuatro pisos donde se encuentran los distintos departamentos y oficinas. La

distribución de cada uno de los pisos es departamental estando repartidas de la siguiente manera:

- **Tecnología (piso 1):** encargado principalmente de dar soporte técnico, administración y monitoreo de la red.
- **Publicidad y Mercadeo (piso 2):** encargado de posicionar en el mercado todos los eventos y servicios que ofrece la empresa.
- **Finanzas (piso 3):** encargado de llevar la logística del punto de vista económico y el control de personal.
- **Presidencia (piso 4):** piso en el que se encuentra el presidente o gerente regional (en el caso de Panamá y Puerto Ordaz) y donde se lleva a cabo conferencias para tomas de decisiones corporativas.

A pesar de que la estructura física de las sedes fijas es semejante, en lo referente al número de pisos y departamentos, la cantidad de equipos (teléfonos IP, impresoras conectadas en red y computadoras) es distinta en cada sede debido a la cantidad de usuarios presentes. En Caracas, como es la sede principal es donde se concentran la mayor cantidad de usuarios, por tanto de equipos. En las sedes de Panamá y Puerto Ordaz se tienen menos usuarios y equipos debido a que estas son más recientes. Estas sedes poseen estructuras de 4 pisos debido a que la empresa se encuentra en crecimiento y desea tener gran presencia en el mercado del entretenimiento, por lo que en un futuro pretende ampliar el número de usuarios y equipos.

En cuanto a las sedes móviles, normalmente cuentan con una dimensión de (80 x 40)m pero estas son adaptables a las localidades y espacios en donde se desarrollen cada uno de los eventos. Asimismo también sufrirá variaciones dependiendo del tipo de evento que se realice ya sean conciertos, exposiciones, teatro, eventos corporativos, entre otros. Por lo general estas se encuentran en espacios abiertos en los centros comerciales. Existe una taquilla que se encarga de la boletería

y la administración referente a entradas vendidas y los ingresos obtenidos por las mismas.

IV.2.2 Estructura de red de la Empresa OnlyTicket Eventos.

Los elementos identificados en cada una de las sedes de OnlyTicket Eventos son los siguientes:

OnlyTicket Caracas:

- Tecnología de acceso a internet: ADSL, proporcionada por la empresa CANTV.
- No presenta cuarto de telecomunicaciones ni gabinetes.
- No presenta cableado estructurado en sus instalaciones.
- Cuentan con alrededor de 15 equipos de computación.
- Las PC no se encuentran conectadas en red.
- No existen puntos de acceso inalámbricos.
- Poseen 4 *switch* modelo Tp-Link TL-WR642G.
- Existencia de un servidor web.

En la figura 6 se muestra la estructura actual de la sede de Caracas.

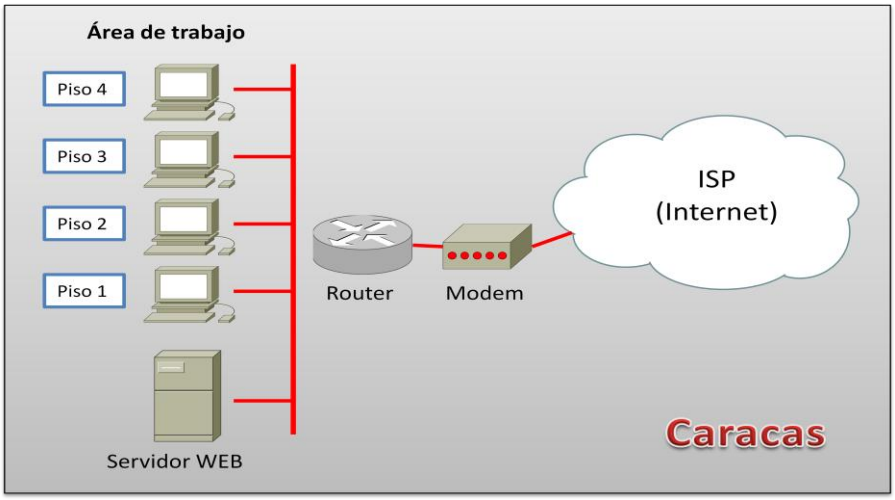


Figura 6. Situación Actual de la sede de Caracas

Fuente: Elaboración Propia

OnlyTicket Puerto Ordaz:

- Poseen 5 equipos de computación.
- No tienen acceso a internet.
- No presentan cuarto de telecomunicaciones ni gabinetes.
- No presenta cableado estructurado.
- Las PC no se encuentran conectadas en red.

En la figura 7 se muestra la estructura actual de la sede de Puerto Ordaz.

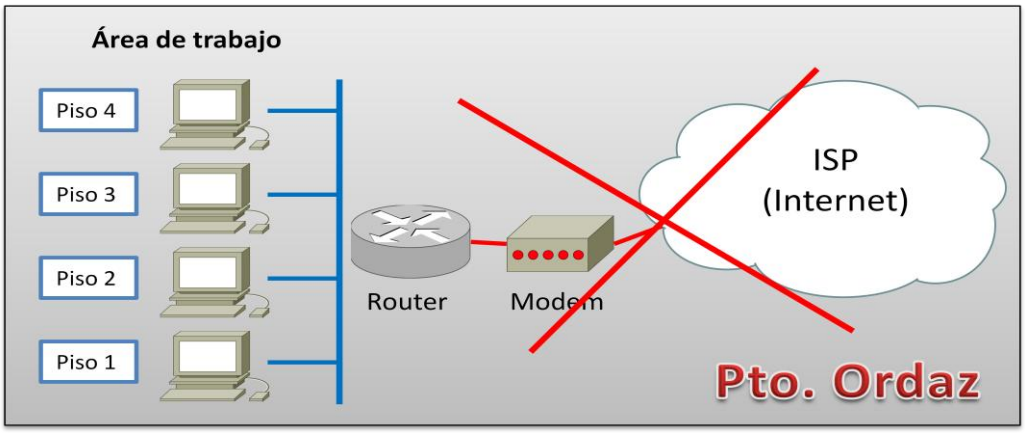


Figura 7. Situación Actual de la sede de Puerto Ordaz.

Fuente: Elaboración Propia.

OnlyTicket Panamá:

- Tecnología de acceso a internet: ADSL.
- No poseen cableado estructurado.
- Poseen 7 equipos de computación
- Las PC no se encuentran conectadas en red.
- Poseen 4 *switch*
- No poseen servidor web.
- No presenta cuarto de telecomunicaciones.

En la figura 8 se muestra la estructura actual de la sede de Panamá.

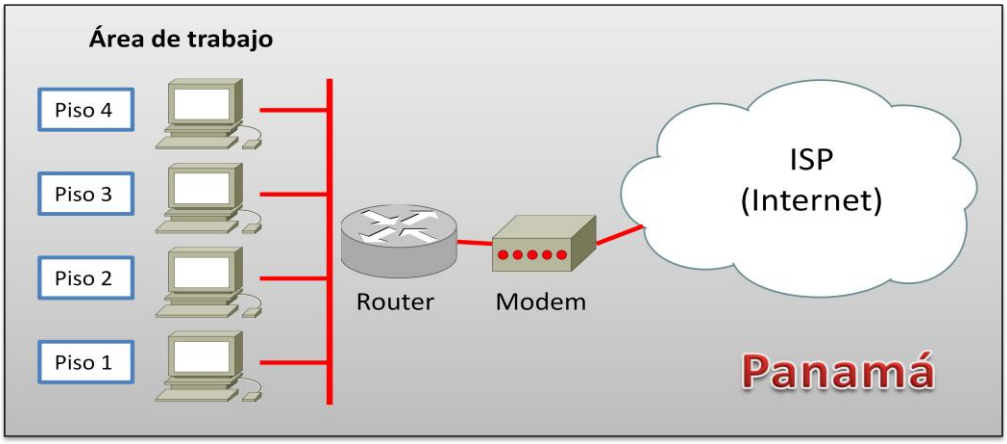


Figura 8. Situación Actual de la sede de Panamá.

Fuente: Elaboración Propia

Como se observa en las figuras anteriores las sedes de Caracas, Panamá y Puerto Ordaz actualmente no se encuentran conectadas entre sí, siendo una limitante al momento de centralizar la información así como también la toma de decisiones es inoportuna causando pérdidas económicas y de tiempo en cuanto a la solución de una problemática dada en alguno de los eventos en un momento determinado. Además, ninguna de estas sedes posee el cableado necesario para mantener las computadoras en red por lo que el intercambio de información entre usuarios de la misma sede es más complicado. Igualmente, la carencia de equipos de seguridad como *firewall* crea grandes problemas con la privacidad y protección de la información.

Por último, las sedes de Caracas y Panamá presentan una conexión a Internet de 1024 Kbps que únicamente permite cumplir funciones administrativas, entre las que resaltan el envío de correo electrónico donde los usuarios de esta empresa utilizan correos personales bajo dominios comerciales (Gmail, Hotmail y Yahoo) lo que viola el principio básico de la privacidad de la información de la empresa en su plan de mercadeo y promociones de eventos.

Sedes móviles:

Las sedes móviles no se encuentran comunicadas con ninguna de las sedes fijas, únicamente cuentan con cámaras de seguridad ubicadas en distintos puntos internos de las localidades donde se realizan los eventos, permitiendo a la seguridad tener un control de lo que sucede en el mismo.

El sistema encontrado se basa en un servidor que controla un grupo de cámaras unidireccionales. Este servidor presenta una calidad de video deficiente, que únicamente puede ser visualizado por los operadores que se encuentran en la sala de operaciones dentro del recinto ya que este no posee salida hacia Internet, por esta razón las imágenes no pueden ser monitoreadas por operadores de red externos a dicho recinto. Estas sedes, tienen una conexión a Internet dada por el proveedor de servicio presente en el lugar donde se realicen los eventos a nivel interno para fines administrativos sin contar con comunicación hacia otras sedes de la empresa.

IV.3 Aplicaciones y Requerimientos a implementar en la red.

Para establecer las aplicaciones y requerimientos, previamente se definieron dos tipos de servicios, los servicios de seguridad y los servicios de gestión, junto con las diversas aplicaciones.

IV.3.1 Servicios de Seguridad

Son considerados como uno de los elementos más importantes de la configuración y realización de este Trabajo Especial de Grado, ya que en la nueva plataforma de comunicaciones viajará cierta información, considerada privada, la cual no debería ser detectada por usuarios ajenos a dicha plataforma. Por lo tanto, se tomaron en cuenta métodos y equipos de prevención que permitan realizar dichas restricciones.

Firewall

Con el fin de resguardar la información que transita por la red diseñada se definió en la configuración, el uso de *Firewall*, el cual permite realizar este tipo de restricciones. Se considera el *Firewall* como un equipo de *hardware*, que se encuentra entre el *router* y el modem con el fin de filtrar todo acceso no autorizado a la red.

VLANs

Con el fin de intercomunicar lógica y no físicamente los distintos departamentos que conforman la empresa, además de realizar un mejor uso del ancho de banda, se propone el empleo de VLANs, ya que permite segmentar lógicamente la infraestructura física de una LAN en distintas subredes, creando así redes independientes dedicadas a funciones específicas por departamento.

Cada uno de los departamentos que conforman la empresa, serán identificados con un número y nombre de VLAN, de acuerdo a cada uno de ellos, lo que permitirá asignarle los recursos y servicios de red de acuerdo a sus funciones lo que posibilita el mejor rendimiento de la red. Se llevó a cabo también la configuración de la VLAN Administrativa puesto que es la que por defecto permite la configuración del *switch*.

Con relación al tipo de VLAN que se propone utilizar, se escogió la VLAN por tipo de puerto, ya que permite la selección física de un puerto en el respectivo *switch*; de esta manera la red se torna más eficiente puesto que las tramas *unicast*, *multicast* o *broadcast* son enviadas directamente a la VLAN correspondiente.

De esta manera, se plantea una alternativa a futuro permitiendo mantener la red física diseñada en este trabajo Especial de Grado y únicamente modificar, la configuración lógica de los equipos que la conforman.

La siguiente tabla presenta el VLAN ID para cada uno de los departamentos así como servicios que se presentan.

Tabla 2. Definición de las VLANs
Fuente: Elaboración Propia.

DEPARTAMENTOS	VLAN
Presidencia	10
Finanzas	20
Publicidad	30
Tecnología	40
Administrativa	1
Video	60
Voz	50

Es necesario configurar enrutamiento entre VLANs, puesto que los usuarios van a intercambiar información de una red a otra. Este proceso permite reenviar el tráfico de la red de una VLAN a otra mediante un enrutador, pero manteniendo el control de dominio de *broadcast*. Este enrutamiento se realizó mediante la conexión de diferentes subinterfaces lógicas en una misma interfaz física del enrutador, así como también, en el puerto que configura el *switch* con el mismo, se habilitó modo troncal basado en el etiquetado 802.1q, el cual permitirá que diferente VLANs puedan transmitir tráfico por este puerto por medio de un proceso de multiplexación evitando así el uso de puertos innecesarios en el *switch.*

Mando Centralizado.

La sede de Caracas será la encargada de controlar y supervisar toda la red de comunicaciones. Esto se debe a que Caracas es la sede principal de la empresa OnlyTicket Eventos, donde se encuentran los directivos y desde donde desean tener el control y supervisión de los distintos eventos.

Así mismo, Caracas será el punto central desde donde se darán las ordenes, administrativas y gerenciales de la empresa, así como también la toma de decisiones. En esta sede, es donde se ubicaran los servidores WEB, DHCP, DNS, nomina y administración, boletería y correo electrónico, por lo tanto en ella se concentrará la mayor parte del tráfico e información circulante de toda la red.

Cámaras IP

Este tipo de cámaras representan el sistema de vigilancia empleado en las distintas sedes móviles con el fin de mantener la seguridad de dichas instalaciones en todo momento. Este sistema presenta una salida enrutable a Internet, la cual permite que un usuario debidamente autorizado pueda acceder y visualizar el desenvolvimiento del evento.

IV.3.2 Servicios de Gestión

Este tipo de servicios, engloba la comunicación entre los operadores de red y los distintos departamentos dentro de la empresa, con el fin de garantizar la comunicación y el buen funcionamiento de cada una de las áreas que conforman dicha empresa. Para el control del personal que labora en las distintas sedes, habrá un sistema de control de acceso a la red. Adicionalmente, se tendrá a disposición de los clientes un medio desde el cual podrán acceder vía internet, y consultar los distintos eventos que ofrece la empresa ya sea con fines informativos o de reservación.

Los servicios de gestión se componen de los siguientes elementos:

Servidor Web

Para este diseño se decidió remplazar el servidor existente en la sede de Caracas debido a que no contaba con las características necesarias para satisfacer los requerimientos planteados. Por esta razón, se plantea la adquisición de un nuevo servidor web dedicado basado en hardware. Se determinó que la mejor ubicación para este equipo es el Cuarto de Servicios ubicado en la parte baja del edificio.

Servidor DNS

Al OnlyTicket Eventos contar con una página web es necesario un equipo que sea capaz de traducir una dirección IP asociada a un servidor web, con el nombre

www.onlyticket.net. Así como también el nombre de *host* de cada dispositivo, lo que permitirá una fácil administración.

En la sede de Caracas contara con una serie de servidores que permitirán la centralización de los datos, estos servidores son los siguientes:

Servidor de Correo

Este tipo de servidor va permitir definir buzones de correo electrónico dentro de un dominio llamado OnlyTicket.com, asignándole a cada trabajador un nombre de usuario con su respectiva contraseña. De esta manera se garantiza que la distribución de los correos internos se haga de manera inmediata, ya que los correos no tienen que salir a Internet. Lo más recomendado es instalar este servicio en un servidor único, asegurando la confiabilidad de la información y la escalabilidad futura.

Servidor de Nomina y Administración

Este servidor permitirá a la empresa una forma organizada y eficiente de administración. Este servidor contara con el sistema adquirido por la empresa llamado *Profit Plus*, el cual permite el correcto funcionamiento de los procesos de la empresa a nivel de negocios, una eficiente gestión administrativa, la cooperación entre los empleados de la empresa. Además este sistema facilita la centralización de la información para el mejor manejo de esta, en el instante que sea necesario.

Control de Acceso

El control de acceso se establece mediante la creación de niveles de autorización según las tareas de cada empleado. Los usuarios tendrán perfiles establecidos que les permitirán o no acceder a distintos niveles de configuración. Estos perfiles serán programados según un controlador de dominios por medio del *software Active Directory.*

Venta de boletos

La venta de boletos está establecida en las sedes móviles donde se realizan los eventos, en ella se encuentran los elementos necesarios para el cobro e impresión de las entradas. La base de datos de la boletería de todos los eventos estará ubicada en la ciudad de Caracas, no obstante en la sede móvil se ubicarán taquillas que tendrán acceso de manera remota desde su ubicación hacía Caracas, esto permitirá tener un mejor control del estatus de la venta de boletería.

Todos los servidores antes mencionados tendrán como característica técnicas las siguientes: marca HP Proliant MI110 G6 4 Quad de 8Gb de memoria Ram y 500 Gb de disco duro.

IV.4 Diseño y Simulación de la Arquitectura de la Red

Con el desarrollo de las fases anteriores se muestra la deficiente estructura de comunicaciones existente dentro de la empresa OnlyTicket Eventos. Por esta razón la plataforma de comunicaciones debe sufrir modificaciones en lo referente a tecnologías de comunicación, protocolos y medios de comunicación, con la finalidad de garantizar una estructura de comunicaciones robusta que permita lograr un enlace óptimo de las distintas sedes con Caracas.

IV.4.1 Dimensionamiento de la Red.

Los elementos necesarios a la hora de realizar el dimensionamiento de la red son la estimación de tráfico y el ancho de banda requerido.

La tabla 3, muestra el ancho de banda de las aplicaciones que debe soportar la red a diseñar, esta estimación del ancho de banda se muestra por usuario.

Tabla 3. Estimación de ancho de banda por aplicación. (26)

Aplicación	Ancho de banda/Usuario	Características
Correo Electrónico	1 – 100 Kbps	El correo electrónico es asincrónico e intermitente, por lo tanto va a tolerar la latencia. Los grandes archivos adjuntos, los virus y el correo no deseado aumentan significativamente la utilización del ancho de banda.
Navegador WEB	50 -100 Kbps	Los navegadores web solo usan la red cuando se solicitan datos, la comunicación es asincrónica.
Flujo de audio *(Streaming)*	96 – 160 Kbps	Cada usuario de un servicio de flujo de audio va a utilizar una cantidad constante de una relativamente gran cantidad de ancho de banda, durante el tiempo que este activo. Puede tolerar algo de latencia pasajera mediante la utilización de mucha memoria de almacenamiento temporal en el cliente (buffer).
Flujo de video (*Streaming*)	64 – 200 Kbps	El flujo de video requiere de alto rendimiento y baja latencia para trabajar correctamente.

Al momento de calcular el ancho de banda, cabe destacar que no existe una metodología establecida para el cálculo del mismo. Tampoco se tienen estadísticas por consumo motivado a que el ancho de banda no es finito para las aplicaciones ni para los usuarios, pudiendo aumentar o disminuir aleatoriamente, de acuerdo a la demanda. Además, éste se ve afectado por la cantidad de usuarios y carga de datos en la red mediante su tasa de transferencia.

Por lo anteriormente señalado, se evaluaron tres posibles escenarios que permitirán estimar un ancho de banda adecuado teniendo en cuenta las aplicaciones utilizadas por la empresa y la cantidad de usuarios en cada una de las sedes que se conectarán hacia Caracas, que es donde se centraliza la información en cuanto a los sistemas administrativos, videoconferencia, correo electrónico y web.

Como se mencionó anteriormente, las sedes se encuentran divididas por departamentos (presidencia, finanzas, publicidad y mercadeo y tecnología), cada una teniendo su propia VLAN. Adicionalmente, se estima el ancho de banda tomando

como premisa que en Caracas hay 30 usuarios, 20 en Panamá, 20 en Puerto Ordaz y 11 en las sedes móviles. Se definió esta cantidad de usuarios que difieren de la cantidad de equipos que se encuentran en la fase de levantamiento de información debido a que los equipos iniciales describen la situación actual y esta cantidad de usuarios refleja el diseño propuesto en este Trabajo Especial de Grado.

Para el desarrollo de los siguientes cálculos se tomaron en cuenta tres posibles escenarios, que nos permitirán tener una estimación del ancho de banda necesario de los enlaces de interconexión entre las distintas sedes. Para ello se tomo como referencia, el tráfico de mayor de consumo de ancho de banda es cual es generado por la aplicación de videoconferencia adquirida por la empresa con anterioridad, la cual presenta un tráfico mínimo requerido de 384kbps. Este tráfico se basa en las especificaciones brindadas por el fabricante (las cuales pueden ser visualizados en el anexo C), el cual define que soporta sesiones simultáneas remotas con alta calidad y sin pérdida utilizando un CÓDEC H.264 y H.261.

- **ESCENARIO 1. Cálculo de ancho de banda basado en aplicaciones de mayor prioridad.**

Para el desarrollo de este cálculo se tomo en cuenta la aplicación y el servicio que presenta mayor prioridad. Este servicio es el de videoconferencia el cual al ser en tiempo real demanda un compromiso de entrega de los paquetes con el mínimo retraso posible.

En base a lo explicado anteriormente, y bajo la condición de que las sedes presentan una estructura común se utilizó como prueba piloto para este estudio la conexión entre Caracas y Panamá por tener una estructura con condiciones a Puerto Ordaz y la móvil.

Se tomó la decisión de estimar en el peor de los casos, que se establezcan cuatro sesiones abiertas, las cuales serán definidas en Caracas hacía cada uno de los departamentos de las sedes estimando un tráfico de 384 kbps por sesión. Al momento

de realizar los cálculos, serán estimados para cinco sesiones, esto debido a que si llegara a darse esta situación (4 sesiones simultáneas), estos 384kbps adicionales serían destinados de holgura para el tráfico requerido por el resto de las aplicaciones siempre y cuando se presente esta condición.

BW= 5 sesiones*384kbps=1,9Mbps

En base a este cálculo el ancho de banda estimado para este escenario sería de 2 Mbps.

- **ESCENARIO 2. Cálculo de ancho de banda basado en un mínimo requerido por usuario.**

A pesar que la aplicación con mayor tráfico es la de videoconferencia, no todos los usuarios demandarán este servicio en un mismo instante de tiempo, por lo que en este escenario se plantea usar el 50% del tráfico generado por esta aplicación destinado a cada usuario. Esto garantiza que al momento de que un usuario desee establecer una conexión vía conferencia sólo se negocie 192kbps disponible dentro de la red.

BW= 20 usuarios *192kbps=3,84Mbps

En base a este cálculo el ancho de banda estimado para este escenario sería de 4 Mbps, para las sedes de Panamá y Puerto Ordaz.

Para la sede móvil el ancho de banda requerido será de 2 Mbps.

$BW_{(móvil)}$= 11 usuarios*192kbps = 2,122 Mbps

- **ESCENARIO 3. Cálculo del ancho de banda basado en videoconferencia de alta calidad.**

Esta opción se basa en la asignación de un ancho de banda dedicado a cada sede de 1 Mbps para uso exclusivo de videoconferencia. Se propone 1 Mbps debido a que esta es la velocidad de transmisión requerida por la aplicación a utilizar en la empresa para establecer una videoconferencia que cumpla con los parámetros de alta calidad.

Adicionalmente, dado que el resto de los usuarios están haciendo uso de distintas aplicaciones (correo electrónico y/o navegador web), basándose en la tabla 3 que establece la velocidad de transmisión promedio de dichas aplicaciones. Se dedica para cada uno de los usuarios (20 usuarios) una velocidad de transmisión dedicada de 100 kbps (50 kbps de correo electrónico y 50 kbps de navegador web).

BW= (19 usuarios *100 kbps) + 1000 kbps= 2,9 Mbps

En base a este cálculo el ancho de banda estimado para este escenario sería de 3 Mbps.

Tomando en cuenta los datos antes señalados, se debe elegir una solución que integre los tres escenarios posibles, de tal manera de garantizar el funcionamiento adecuado, de acuerdo a la demanda de las aplicaciones y cantidad de usuarios en las sedes. Dado lo anterior, se concluye que el ancho de banda a utilizar será el de 4Mbps (4096 kbps), el cual además le proporciona escalabilidad a la red.

IV.4.2 Selección de la Tecnología a Implementar

Basándose en la información recolectada en el Capítulo II, se realizó una comparación de las posibles tecnologías a implementar en la realización de este Trabajo Especial de Grado.

A continuación se muestra una tabla resumen de las posibles tecnologías a implementar.

Tabla 4. Comparación Tecnologías.

Fuente: Elaboración propia.

ATM	• Permite la transmisión de aplicaciones síncronas y asíncronas de voz, video y datos, a diversas velocidades, en direcciones múltiples, con diferentes grados de calidad y servicios. • Permite manejar el ancho de banda de manera flexible e inteligente asignándolo solo cuando las aplicaciones lo demandan. • Presenta capacidades mínimas de control de error y flujo.
Frame Relay	• Bajo retardo de red y alta conectividad. • Eficiente utilización del ancho de banda. • No soporta aplicaciones sensibles al tiempo. • No garantiza la entrega de los datos. • Definido para velocidades de hasta 1,544/2,048 Mbps.
Metro Ethernet	• Permite modificar y manipular de una manera más dinámica, versátil y eficiente, el ancho de banda y la cantidad de usuarios en corto tiempo. • Ofrece un bajo costo en la administración, operación y funcionamiento de la red. • Facilidad de uso e instalación.

Al analizar y comparar las posibles tecnologías que garanticen calidad de servicio en la transmisión de datos entre las distintas sedes físicas que conforman la empresa OnlyTicket Eventos, se considera que la tecnología para dicha implementación es Metro Ethernet Network dado que es la más eficiente para este proyecto. Esta tecnología presenta la mejor relación beneficio-costo ya que se considera una tecnología realmente económica y netamente escalable permitiendo la expansión del ancho de banda de acuerdo a los requerimientos de la empresa y sus distintas sedes.

Metro Ethernet está destinado a brindar servicios de internet de alta velocidad a las distintas sedes que conforma la empresa OnlyTicket Eventos, cumple con las condiciones para aplicaciones solicitadas para la empresa, transmisión de datos *multicast*, servicios de voz, transmisión de audio y video en tiempo diferido y tiempo real.

En la siguiente tabla 5 se detalla la el ancho de banda requerido para cada enlace, siendo estos simétricos (con la misma tasa de transferencia de subida que de bajada).

Tabla 5. Ancho de Banda requerido por enlace
Fuente: Elaboración Propia

ENLACE	ANCHO DE BANDA
Caracas-Panamá	4 Mbps
Caracas-Puerto Ordaz	4 Mbps

De igual manera, en contraste con la investigación teórica realizada se tiene la siguiente tabla donde se muestran las comparaciones con respecto a los distintos tipos de interconexión entre las distintas sedes.

Tabla 6. Tipos de Interconexión.

Fuente: Elaboración propia.

	REQUERIMIENTOS – VENTAJAS	LIMITACIONES
MICROONDAS	• El camino entre el receptor y el transmisor debe tener una altura mínima sobre los obstáculos en la vía. • Zona de Fresnel, ya que aumenta o disminuye el nivel de intensidad de la señal recibida.	• No deben existir obstáculos entre el transmisor y receptor. • Distancias limitadas entre el transmisor y receptor.

VPN *(Virtual Private Network)*	• Ahorro en costos (mantenimiento de bajo costo) y la escalabilidad. • Puede utilizar internet o alguna otra red pública para hacer la conexión y entrar a la red virtual a través de líneas locales.	• Se deben establecer correctamente las políticas de seguridad y de acceso.
FIBRA ÓPTICA	• No resulta afectada por condiciones externas. • Pueden colocarse fácilmente en las distintas instalaciones debido a su contextura delgada.	• Alta fragilidad. • Necesidad de conversores de señal.

Entre las tecnologías evaluadas se decidió como medio de redundancia de la red el uso de VPN, ya que permite una forma de comunicación entre las partes de la red privada a través de la red pública; esto se realiza estableciendo túneles virtuales entre dos puntos de la red, donde se usan métodos de encriptación y autentificación para asegurar la confiabilidad de los datos transmitidos dentro de la red.

Al hablar de VPN es necesario destacar el método a utilizar para proteger los datos IP cuando estos viajen de una sede a otra. Por esta razón, en este Trabajo Especial de Grado se plantea el uso de VPN IPsec.

IPsec se refiere al conjunto de protocolos que aseguran las comunicaciones sobre IP, autenticando y cifrando cada paquete IP. El utilizar IPsec la VPN puede ser considerada segura ya que proporciona: confidencialidad de los datos, integridad de los datos, autenticación del origen de los datos y anti- repetición.

La VPN al ser realizada a través de Internet, muchos de los datos que transiten por ella podrían ser interceptados y examinados. La confidencialidad de los datos lleva de la mano la encriptación; los paquetes son encriptados y solamente podrán ser interpretados por el receptor. La autentificación es necesaria para validar el origen en la VPN IPsec, esto se realiza en cada uno de los extremos de la VPN, para asegurar que el otro extremo es el que debe estar conectado. La anti-repetición es importante ya que asegura que los paquetes no estén duplicados dentro de la VPN, esto se lleva a

cabo a través del número de secuencia de los paquetes y de un sistema de ventanas deslizantes en el receptor.

IV.4.3 Diseño de la Topología.

Al momento de realizar el diseño de la topología de la red se deben tomar en cuenta las distintas características de cada una de las posibles topologías a implementar, para luego tomar la decisión que produzca la mayor cantidad de beneficios dentro de la red de telecomunicaciones diseñada.

La tabla 7, presenta las características de las posibles topologías a implementar.

Tabla 7. Topologías de red

Fuente: Elaboración Propia

TOPOLOGÍA	VENTAJAS	DESVENTAJAS
TIPO ESTRELLA	• Si un PC se desconecta o se rompe el cable solo queda fuera de la red ese PC. • Facilidad al reconfigurar la arquitectura. • Fácil de prevenir daños o conflictos. • Centralización de la red.	• Si el nodo central falla, toda la red deja de transmitir. • Es costosa, ya que requiere más cable que las topologías bus o anillo. • El cable viaja por separado del concentrador a cada computadora.
TIPO ANILLO	• Camino unidireccional cerrado que conecta todos los nodos. • El control de acceso está distribuido por toda la red. • Se puede operar a grandes velocidades, y los mecanismos para evitar colisiones son sencillos.	• El canal usualmente se degradará a medida que la red crece. • Difícil de diagnosticar y reparar los problemas. • Si una estación o el canal falla, las restantes quedan incomunicadas.
TIPO BUS	• Facilidad de implementación y crecimiento. • Simplicidad en la arquitectura.	• Complejidad de reconfiguración y aislamiento de fallos. • Limitación de las longitudes físicas del canal. • El desempeño se disminuye a medida que la red crece. • Altas pérdidas en la transmisión debido a colisiones entre mensajes.

La red ha sido diseñada tomando como premisa que cada una de las sedes debe estar conectada con la sede de Caracas, buscando la centralización de la información. Partiendo de este hecho se decidió el uso de una topología tipo estrella donde cada nodo estaría conectado directamente con el nodo central (Caracas).

La ventaja principal de este tipo de topología, es que permite que todos los demás nodos se comuniquen entre sí de manera conveniente.

La figura 9 muestra la topología de la red a diseñar, los servicios estarán centralizados en la sede de Caracas, permitiendo que las sedes de Panamá y Pto.Ordaz puedan interconectarse con Caracas y acceder a estos servicios.

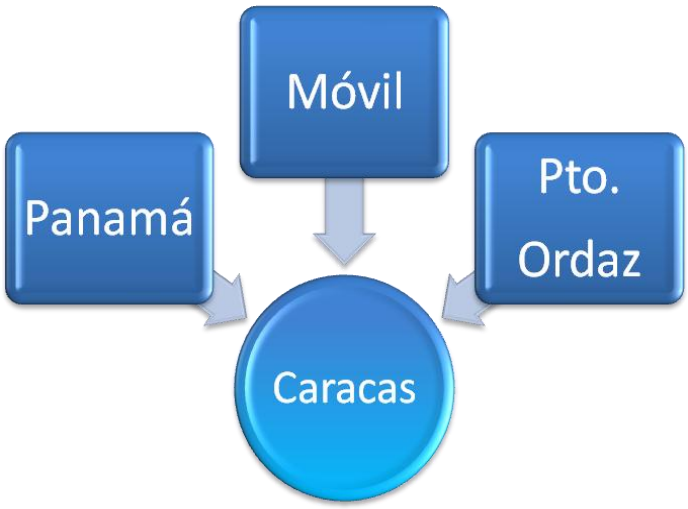


Figura 9. Topología de la Red.

Fuente: Elaboración Propia.

IV.4.4 Direccionamiento IP

Al momento de realizar la asignación de direcciones a cada uno de los equipos se debe tomar en cuenta, la clasificación y características de cada una de ellas. Para ello fue necesario realizar la tabla 8:

Tabla 8. Clasificación Direccionamiento IP.

Fuente: Elaboración Propia

DIRECCIONAMIENTO IP	
ESTÁTICO	**DINÁMICO**
• Gestionado manualmente por el administrador de red. • Ausencia de tolerancia a fallos. • Fácil de configurar en redes pequeñas.	• Asignada mediante un servidor DHCP. • Reduce los costos de operación a los proveedores de servicios de Internet (ISP). • Reduce la cantidad de IP asignadas (de forma fija) inactivas.

Se determinó el uso de un servidor DHCP *(Dynamic Host Configuration Protocol)*, el cual asignara una dirección IP a cada equipo que conforma la red.

Se definió que el mecanismo más adecuado para esta red es el direccionamiento dinámico, ya que la asignación por usuario se realiza de forma temporal, es decir, permite la reutilización de un rango de direcciones IP que se encuentran disponibles, las cuales serán asignadas posteriormente a otro usuario.

Solo a excepción de los servidores en el cual el mecanismo más adecuado es el direccionamiento estático ya que estas direcciones deben permanecer constantes para mantener un equilibrio dentro de la red de Telecomunicaciones a diseñar.

Aunque se haga uso de un servidor DHCP, es necesario asignar el rango de direcciones a utilizar para que el servidor se encargue de asignar a cada equipo la dirección correspondiente. El direccionamiento IP se realizó haciendo uso de VLSM (*Variable Length Subnet Masking*), partiendo de la familia de direcciones privadas 172.16.0.0, para así definir las subredes que conforman la red de telecomunicaciones diseñada (ver anexo b).

Para realizar la asignación de las subredes y correspondientes máscaras, se tomaron en cuenta la cantidad de direcciones IP necesarias en cada sede, sin dejar de tomar en cuenta la escalabilidad futura de la red.

IV.4.5 Enrutamiento

Con respecto al enrutamiento, el mismo se propuso hacerlo de manera estática debido a que existen pocas subredes (ver anexo d). Para ello, las rutas serían establecidas manualmente por el administrador de red, actualizando su ruta en caso de existir un cambio en la topología. Esto posee ventajas sobre el enrutamiento dinámico ya que consume menos recursos del enrutador y la red al no tener que estar constantemente calculando rutas, ahorra ancho de banda, procesamiento y memoria del enrutador. Esto permite mayor seguridad debido a que el administrador define el flujo de datos entrantes y salientes.

IV.4.6 Cableado Estructurado

El diseño de un cableado estructurado que enrute, proteja, identifique y determine los medios de comunicación de manera apropiada, es esencial para el funcionamiento eficiente de la red. Es necesario para el cableado horizontal, utilizar un par trenzado de cobre UTP, en conjunto con conectores RJ45. Las categorías de cableado UTP se muestran a continuación en la tabla 9.

Tabla9. Tipos de Cable UTP

Fuente: Elaboración Propia

Categoría	Características
Categoría 5	Transmisión de datos a velocidades de hasta 100 Mbps. O 100 BaseT.
Categoría 5e	Transmisión de datos con un ancho de banda de (125MHz) 250 Mbps.
Categoría 6	Redes de alta velocidad hasta 1Gbps (Equipos)
Categoría 6 a	Cuenta con parámetros de transmisión de datos mejorados, apoya 10GBase-T y todas las aplicaciones digitales de banda ancha.

Al realizar el sistema de cableado estructurado, se deben tomar en cuenta los distintos elementos:

- **Cuarto de Servicios o MDF**: se encuentra en la parte baja del edificio, en este cuarto es donde se conecta el cableado del proveedor con el cableado de la red a diseñar.
- **Sala de Telecomunicaciones o IDF:** en esta sala se producen las conexiones entre las transiciones del cableado vertical *(backbone*) y el cableado horizontal.

El cableado estructurado se dividió en dos partes las cuales se encuentran a continuación.

IV.4.6.1 Cableado Vertical.

Se propone implementar como tecnología para el *backbone* el uso de fibra óptica multimodo 50/125 micrones la cual se colocará en la ala derecha del edificio por dentro del ducto de los ascensores. En el primer piso del edificio se encontrará el MDF (*Main Distributoin Frame*) que luego estará conectado mediante fibra a los IDF (*Intermediate Distribution Facility*) en los pisos restantes.

Al momento del extendido de la fibra, es necesario que esta sea colocada dentro de ductos de 4 pulgadas (100 x 100 mm). Estos deben ser corrugados en la superficie externa de modo de hacerlos aptos para el traslado de la fibra óptica y dicha fibra, cubierta para ser protegida de agentes externos.

IV.4.6.2 Cableado Horizontal

Una vez realizado el diseño del *backbone,* se consideraron todos los parámetros necesarios para el desarrollo del cableado horizontal, el cual será proveniente de cada IDF o MDF (en caso del primer piso) y luego a cada estación de trabajo (siendo tanto telefonía como datos).

Para esta implementación, teniendo en cuenta el estándar ANSI /TIA/ EIA-568-C ha sido actualizada, se propone el uso del cable UTP categoría 6a

el cual ofrece escalabilidad y mayores velocidades frente al 5e, logrando un óptimo desempeño de la plataforma de comunicaciones.

Con respecto a la red telefónica, se decidió utilizar un sistema basado en Voz sobre IP con el fin de integrar telefonía con datos en una sola red y aprovechar de mejor manera el cableado.

En la figura 10 se propone el tipo de cableado que sería utilizado por las tres sedes. Los pisos tendrán una altura de 4,20m cada uno.

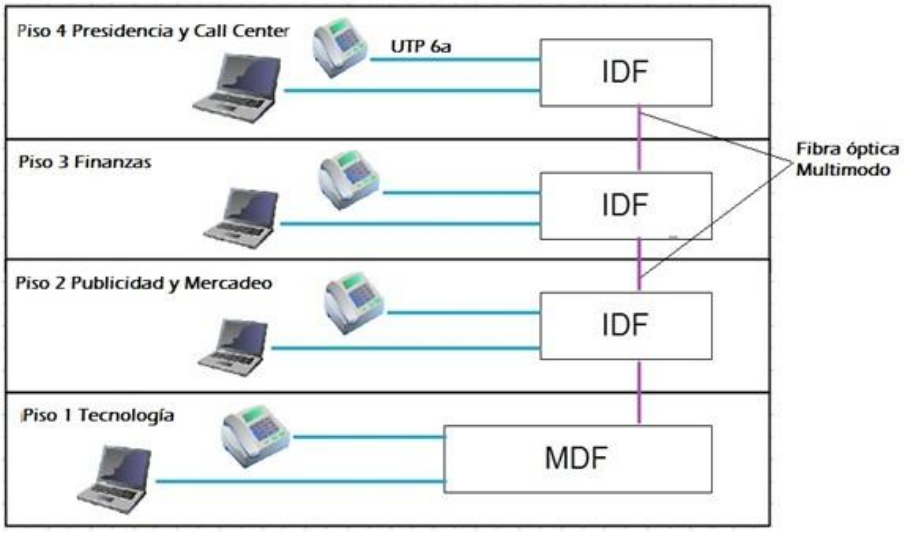


Figura 10. Estructura del cableado propuesta.

Fuente: Elaboración propia.

La distribución principal se hace a partir del MDF donde se halla el *patch panel* tanto de voz como de datos y luego hacia los equipos requeridos llevándose por medio de escalerillas de soporte aéreo y canaletas de doble canal de 75x50 mm. Los IDF tendrán una dimensión de 3x3m y tendrán piso falso a modo de facilitar la instalación del cableado, acceso y mantenimiento, deberán tener una temperatura de aproximadamente 21º C y humedad entre 30% y 45%. Además, contarán con dos gabinetes cada uno los cuales brindan una mayor protección contra interferencias electromagnéticas y resguardo

para equipos, agrupando las unidades de conmutación y *transceivers* que recibirían cableado. Los MDF tendrán una dimensión de 5,5x4,5m, bajo las mismas condiciones, pero teniendo un rack adicional para conmutadores, enrutadores y servidores.

Finalmente, tanto los MDF como los IDF deben contar con un sistema de potencia ininterrumpida UPS *(Uninterrumpible Power Supply)*, la cual generara ventajas a la red que contara con un respaldo de energía, como consecuencia su funcionamiento no se verá afectado ante cualquier inconveniente eléctrico.

La figura 11, ejemplifica la distribución de tanto del cableado vertical como el horizontal en el edificio donde funciona la empresa.

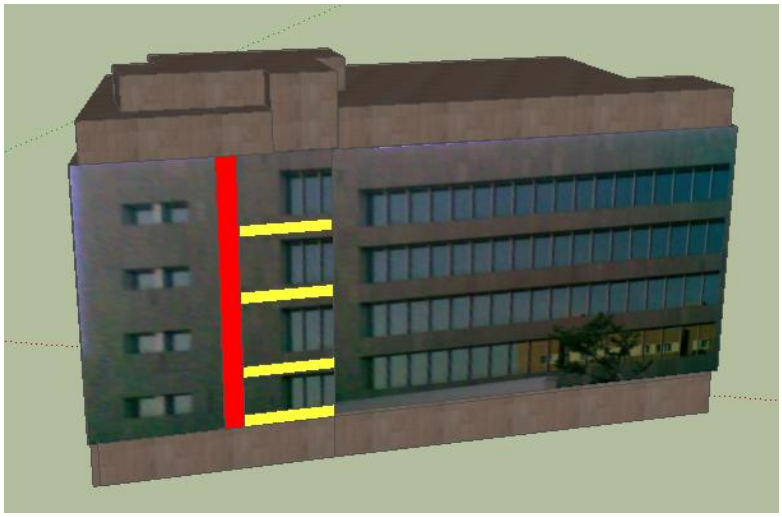


Figura 11. Distribución del Cableado en el Edificio.

Fuente: Elaboración Propia.

Con respecto a las sedes móviles, donde se hacen los eventos, las mismas no contarán con esta estructura de cableado, puesto que solo constan de un piso, por lo que solo tendrá un cuarto principal en el cual se coloque el servidor de video de alta calidad, un switch y un router.

IV.4.7 Diseño propuesto

Luego de haber hecho el levantamiento de información, y conocer el tipo de enrutamiento, direccionamiento, tecnología, topología de red y cableado estructurado adecuado para esta empresa se presenta en la figura 12 el diseño propuesto.

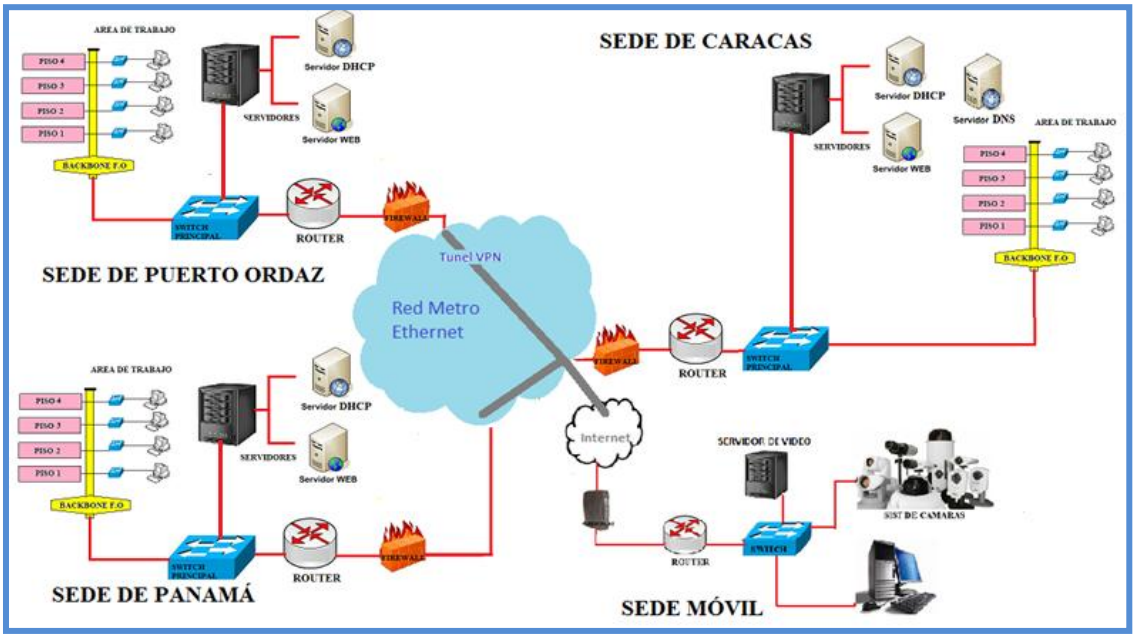


Figura 12. Diseño Final dela conexión entre las sedes fijas y móviles
Fuente: Elaboración Propia

Como se puede observar las sedes fijas se encuentran conectadas mediante la tecnología Metro Ethernet y como redundancia VPN, contando cada una con su propio *firewall* para resguardo de la información transitando en la red. La sede de Caracas cuenta con servidores de correo, boletería, DHCP, DNS, nómina y administración y web mientras que las de Puerto Ordaz y Panamá tienen solo servidores DHCP y DNS. También se presenta el *backbone* del cableado estructurado, el cual representa la interconexión entre el cuarto de servicios y los cuartos de telecomunicaciones ubicados en cada piso, proporcionando la conectividad a cada uno de los equipos y usuarios.

Con respecto a las sedes móviles, se observa que estas cuentan con cámaras IP y su respectivo servidor de video y además debido a que cuentan con acceso a internet del proveedor de servicios (ABA Empresarial), se encuentran conectadas mediante VPN con la sede de Caracas, a modo de poder monitorizar externamente las situaciones que se puedan presentar.

Los equipos y servicios necesarios para lograr este diseño se encuentran explicados de manera detallada más adelante en la fase de búsqueda de servicios y equipos requeridos.

IV.4.8 Simulación.

La simulación realizada en este Trabajo Especial de Grado, permite la configuración y verificación de la conectividad de los enlaces, así como también el funcionamiento del protocolo de enrutamiento seleccionado. Adicionalmente permite reconocer el funcionamiento de algunos elementos que componen el diseño de la red.

Con respecto al software de simulación a utilizar se consideró en un primer plano, *OPNET GURU ACADEMIC EDITION*, pero se descartó debido a que la versión existente presenta límites con respecto a la cantidad de eventos aceptados al momento de correr la simulación, las cuales no eran suficientes para este diseño.

El software que se utilizó fue *PACKET TRACER*, propiedad de CISCO SYSTEMS. Este software es un simulador de redes gráfico, que permite realizar el diseño de topologías, la configuración de dispositivos de red, protocolos de enrutamiento, así como la detección y corrección de errores en los sistemas de comunicaciones. La gran ventaja de este simulador es que permite el análisis de los procesos ejecutados de acuerdo a la capa del modelo OSI que interviene en dicho proceso. Packet Tracer, ofrece también una interfaz amigable, basada en ventanas que ofrece facilidades para el modelado, configuración y simulación de redes. Otra de las razones por las que decidió usar este software es que la empresa proveedora de servicios basa parte de su plataforma de comunicaciones en equipos CISCO, y los equipos de enrutamiento y conmutación seleccionados para este diseño pertenecen a

esta empresa. Con este software se podrá plantear las interfaces y configuración de los equipos elegidos.

La siguiente figura, muestra la topología de la red de telecomunicaciones diseñada; en ella se presentan las sedes de Caracas, Panamá y Puerto Ordaz, así como la conexión de ellas con el proveedor de servicios.

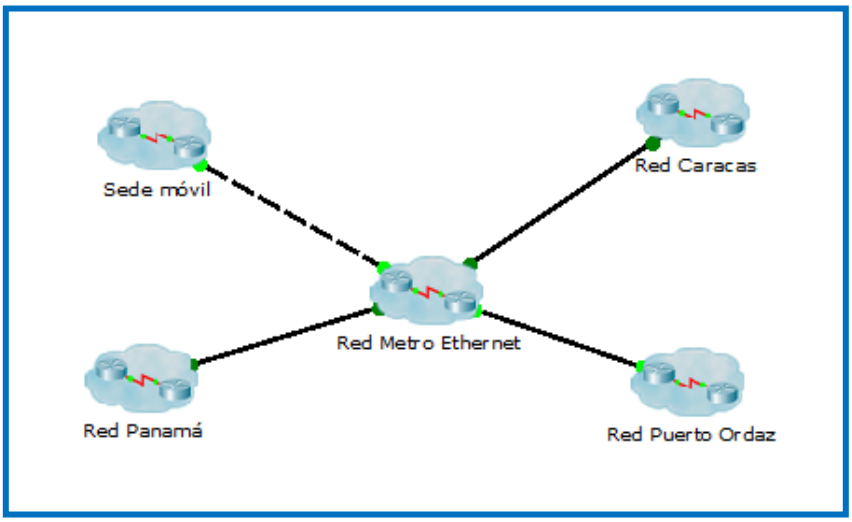


Figura 13. Red simulada en Packet Tracer.

Fuente: Elaboración Propia.

En la simulación se pueden evidenciar los elementos que conforman cada nodo (sede) de la red. A continuación en las siguientes figuras muestran dichos elementos.

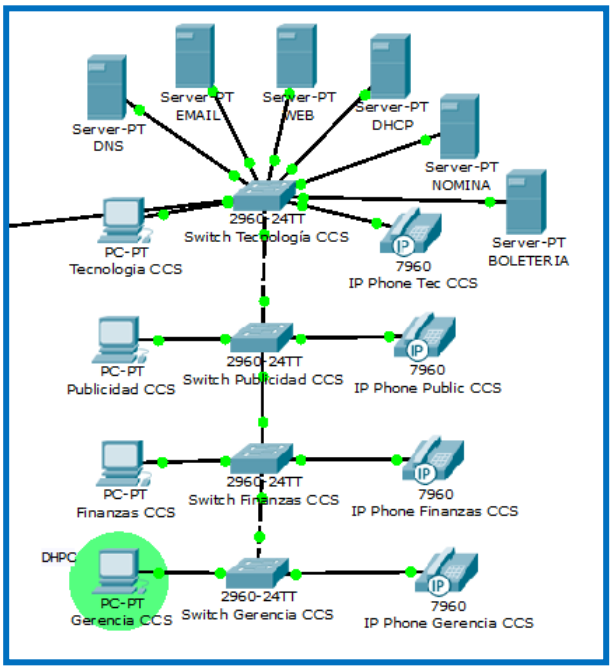


Figura 14. Sede Caracas

Fuente: Elaboración Propia.

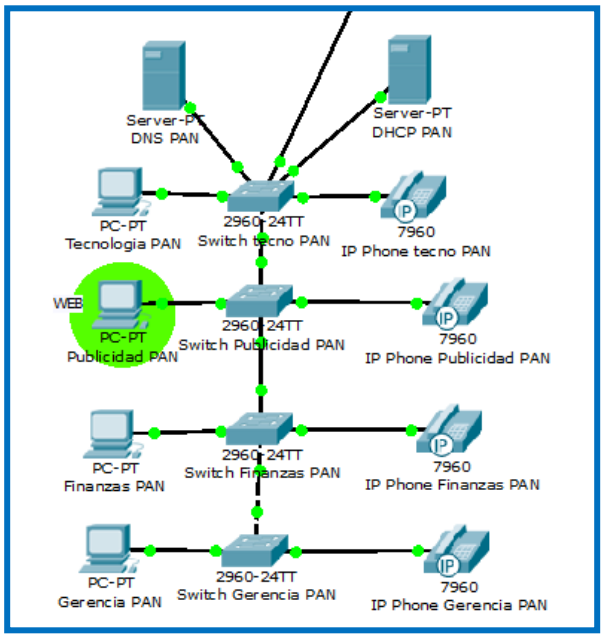


Figura 15. Sede Panamá

Fuente: Elaboración Propia.

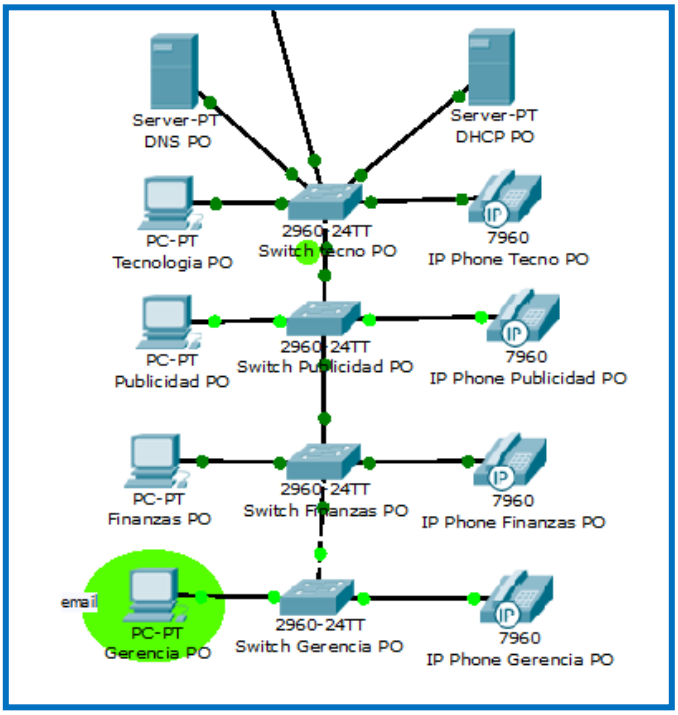


Figura 16. Sede Puerto Ordaz

Fuente: Elaboración Propia.

Cabe destacar que la conexión física entre las sedes fue simulada mediante el uso de fibra óptica emulando la velocidad contratada al proveedor de servicios. Esto debido, a que el ISP posee numerosos enlaces para poder prestar los diversos servicios que ofrece y no es posible conocer exactamente los equipos utilizados por ellos en su topología para prestar el servicio contratado.

En las Figuras 14, 15 y 16 se puede observar que cada una de las sedes presenta un router conocido como router frontera, el cual conecta hacia el resto de la red. Los *switches* mostrados presentan configuradas las distintas VLANs que identifican los servicios.

El sistema de datos está representado por computadores que poseen acceso a Internet y correo electrónico, a través de los servidores de email y WEB ya que estos trabajan con protocolos como HTTP, SMTP y POP3. Estos protocolos se encuentran involucrados en el envío y recepción de correo electrónico, funcionando en la capa 7

(aplicación) del modelo OSI. A continuación se muestra la visualización desde un PC cualquiera, la vista de la página web perteneciente al servidor web ubicado en Caracas.

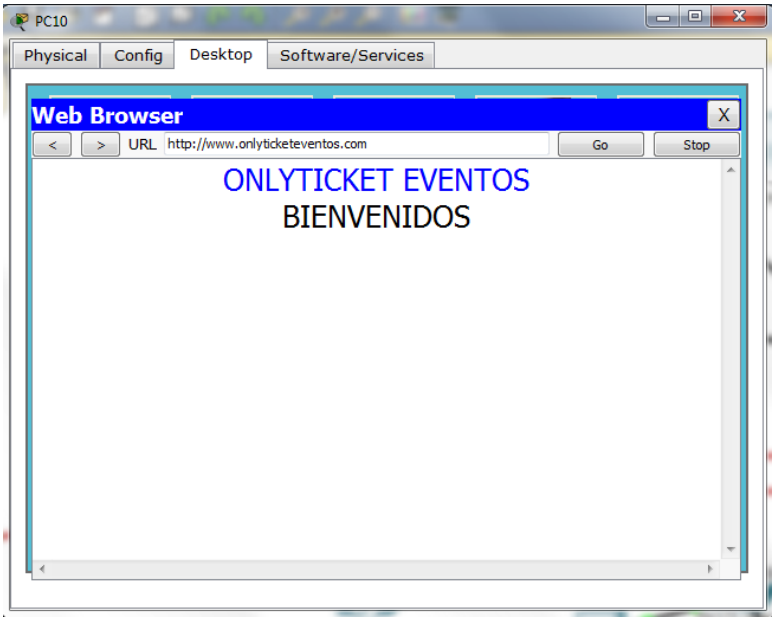


Figura 17. Configuración Página web

Fuente: Elaboración propia

Con respecto al direccionamiento IP, fueron asignadas las direcciones IP estáticas a los servidores de cada uno de los nodos; mientras que a los distintos *host* son asignadas de forma dinámica por el servidor DHCP.

Fueron utilizados teléfonos IP para así simular el uso de estos y su configuración con el fin de ejemplificar el sistema de Voz sobre IP.

IV.5 Búsqueda de Equipos y Servicios Requeridos y Costo de Equipos y Servicios Requeridos

Luego de elaborar el diseño de la red, se hizo una lista de los equipos requeridos en cada una de las sedes. Esta fase se dividió en dos etapas, constando de búsqueda de servicios, y la otra sección de búsqueda de equipos.

V.5.1 Servicios Requeridos

Para el enlace de Metro Ethernet, se buscaron diversas empresas que pudieran ofrecer este tipo de conexión a las sedes. Luego de una búsqueda con compañías como Movistar, CANTV o Intercable, las cuales no ofrecían el servicio deseado en todas las sedes, se encontró una empresa internacional, Global Crossing, la cual, como se puede ver en la figura 18, brinda enlaces de Metro Ethernet a diferentes regiones en el mundo, como lo sería en este caso Caracas, Puerto Ordaz y Panamá siendo ideal para lo requerido en este proyecto.

Esta empresa sería la escogida para proporcionar los enlaces simétricos de conexión entre las distintas sedes (Caracas-Panamá y Caracas – Puerto Ordaz), con un ancho de banda de 4 Mbps de enlace, siendo suficiente para soportar las aplicaciones planteadas anteriormente y asignándoles 1 IP pública a cada sede.

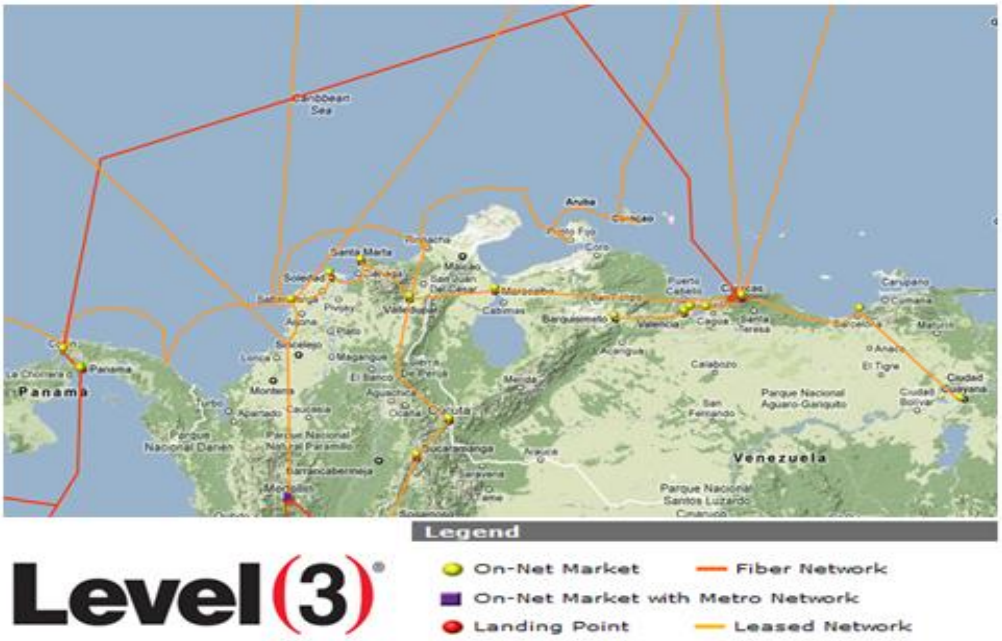


Figura 18. Mapa de Conexiones Global Crossing. **(28)**

V.5.2 Equipos Requeridos

Considerando que se trata de una interconexión y cableado estructurado para las sedes fijas, hay una cantidad de equipos que se requieren para lograr este fin. También existen las sedes móviles, las cuales también requieren de equipos con el fin de lograr monitorizar los eventos. A continuación se presentan las etapas llevadas a cabo para definir los equipos necesarios para el diseño:

V.5.2.1 Equipos para la red de datos

Para la red de datos, es necesario contabilizar la cantidad de puntos de red que hay en cada edificio en total. Hay un aproximado de 30 hosts para cada una de las sedes por lo que la distribución de los puntos de red quedaría de la manera mostrada en la tabla 10.

Tabla 10. Distribución de puntos de Red.

Fuente: Elaboración propia

PISOS	PUNTOS DE RED	EQUIPO
Piso 1	11	*Patch Panel* 24 puertos
Piso 2	11	*Patch Panel* 24 puertos
Piso 3	11	*Patch Panel* 24 puertos
Piso 4	11	*Patch Panel* 24 puertos

En el cableado horizontal se necesitarían conectores tipo Jack RJ 45 de cuatro pares (8 pines) y placas de pared con dos puntos de acceso cada uno como mínimo. A pesar que hay tan solo 11 puntos de red en cada piso, se utiliza un *patch panel* de 24 puertos, tomando en cuenta que es una empresa en crecimiento, permitiéndole escalabilidad.

Con respecto a los equipos de enrutamiento y conmutación, se decidió utilizar un *switch* marca Cisco modelo 2960 de 48 puertos y luego uno de 24 puertos por cada piso (4 en total por cada sede) y un *router* por cada sede marca Cisco modelo 2811.

El cableado vertical, requiere de un panel de distribución de fibra óptica, para separar cables de múltiples fibras y garantizar que solo el personal autorizado tenga acceso al mismo. Así como en el cableado horizontal, en este cableado también se dispondrá de un *patch panel* de fibra óptica de 24 puertos, organizando la interconexión entre el *backbone* y los equipos de enrutamiento y conmutación. En cuanto a los conectores, siguiendo al ANSI/TIA/EIA 568-C, se eligió el SC (*Set and Connect*), debido a que es el recomendado y de fácil instalación. Por último, es necesario que cada piso tenga un *transceiver* actuando como interfaz entre un determinado dispositivo de red y el cableado en fibra. El que tiene mayor difusión es el GBIC (G*igabit Interface Converter*), siendo compatible con la mayoría de equipos disponibles en el mercado.

V.5.2.2 Equipos para voz

En la infraestructura requerida para soportar el servicio de voz sobre IP en la empresa, se debe disponer de una central PBX funcionando como foco para el tipo de comunicaciones. Se recomienda el uso de una central del tipo *software* código abierto como ASTERISK, reduciendo costos de instalación y mantenimiento. Este tipo de central tiene la ventaja que trabaja con varios protocolos de VoIP, siendo los más usados H.323, SIP y MGCP. Debido a la cantidad de usuarios, se tiene un aproximado de 20 líneas por sede, pero se tiene que tomar en cuenta la capacidad de agregar extensiones, en caso de incorporación de nuevos usuarios en un futuro, por lo que

se eligió un *patch panel* de 24 puertos por piso, como se puede observar en la siguiente tabla 11.

Tabla 11. Patch Panels para voz.
Fuente: Elaboración propia.

PISOS	EQUIPOS	CANTIDAD
Piso 1	*Patch Panel* 24 puertos	11
Piso 2	*Patch Panel* 24 puertos	11
Piso 3	*Patch Panel* 24 puertos	11
Piso 4	*Patch Panel* 24 puertos	11

Como se quiere conectar los servicios de telefonía IP con la telefonía tradicional, se precisa de adaptadores (ATA) que permitan conectar de manera convencional un teléfono tradicional a una computadora, es decir para la conmutación hacia la red telefónica pública. Estos adaptadores han de ser colocados en cada estación de trabajo de los usuarios. Adicionalmente, se debe contar con puertos FXO, a modo de asegurar agregación de otros servicios en un futuro, así como la compatibilidad con la red de telefonía tradicional.

La central de voz sobre IP estará ubicada en el MDF en el primer piso, para luego ser distribuido hacia diferentes usuarios en la empresa.

V.5.2.3 Equipos para sedes móviles

Para las sedes móviles se utilizarán cámaras IP, la cuales serán conectadas a un servidor de video el cual a su vez estará conectado a un *switch* con el fin de darle acceso a dicho servidor a cualquier operador de red encargado de la seguridad ubicado dentro del recinto, asimismo dicho *switch* estará conectado a un *router* que permitirá

entrada y salida a internet con el fin de poder monitorear dichas cámaras desde redes externas a las sedes móviles.

Se puede apreciar en la figura 19 una estructura general de las sedes móviles, aunque como es explicado anteriormente, estará sujeta a cambios. Los puntos azules representan las cámaras IP (alámbricas) las cuales estarán conectadas a la sala de operaciones donde se encuentra el personal encargado de supervisar la red, el *switch*, *router* y servidores.

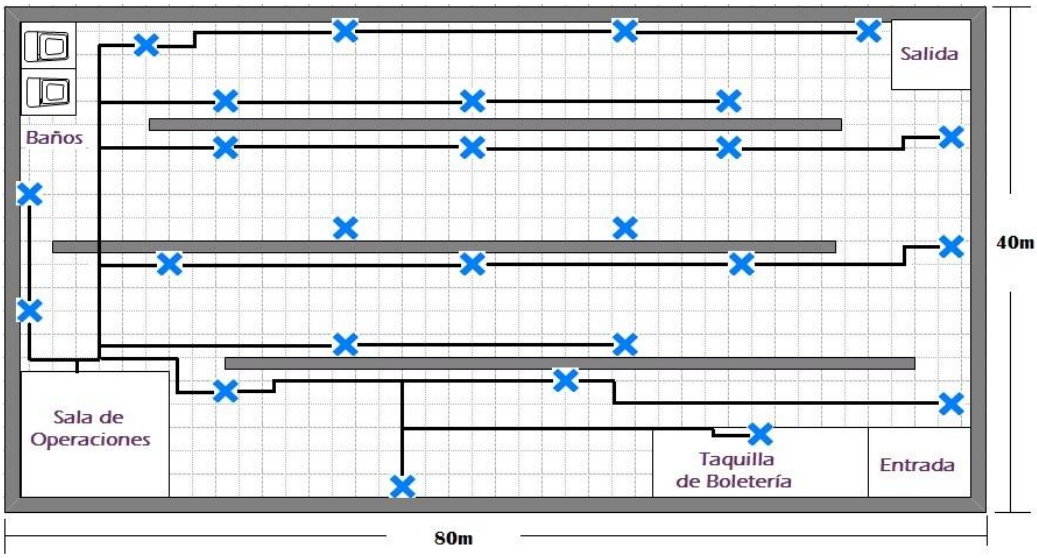


Figura 19. Distribución de los equipos en las sedes móviles

Fuente: Elaboración Propia.

V.5.3 Costo de los Servicios y Equipos requeridos

Se realizó el cómputo métrico del cable para determinar la cantidad de cable necesario para el cableado vertical y horizontal. Se hizo el cálculo del cableado vertical teniendo en cuenta la altura de los pisos, el bucle de servicios, el MDF y el IDF. Para el cableado horizontal se tomó en cuenta las

dimensiones de cada una de los pisos (30x25m) y la distancia del techo a los puntos de red. Los cálculos de dicho cable se muestran la tabla 12 y tabla 13.

Tabla 12. Cálculo para el cableado vertical.

Fuente: Elaboración propia

Pisos	Metros
Altura piso 1 (4,20m x 2) + bucle de servicio (2m) + MDF (5m)	15,4
Altura piso 2(4,20m x 2) + bucle de servicio (2m) + IDF (3m)	13,4
Altura piso 3(4,20m x 2) + bucle de servicio (2m) + IDF (3m)	13,4
Altura piso 4(4,20m x 2) + bucle de servicio (2m) + IDF (3m)	13,4
Total fibra multimodo 50/125micrones	**55.6**

Tabla 13. Cálculo para el Cableado Horizontal.

Fuente: Elaboración Propia.

Pisos	Metros
Cableado horizontal piso 1 (60m) + distancia al punto de red (1,5m x 11)	76,5
Cableado horizontal piso 2 (60m) + distancia al punto de red (1,5m x 11)	76,5
Cableado horizontal piso 3 (60m) + distancia al punto de red (1,5m x 11)	76,5
Cableado horizontal piso 4 (60m) + distancia al punto de red (1,5m x 11)	76,5
Total cable UTP 6ª	**306**

Se contactó a la empresa Global Crossing con sede en Caracas, con el fin de pedirle una cotización para el enlace deseado y se investigó a fondo los precios de los diferentes equipos necesarios. En la tabla 14 se muestran los costos de cada equipo y del servicio de Metro Ethernet.

Tabla 14. Costos de cada Equipo y Servicio.

Fuente: Elaboración propia.

Equipos	**Costo Unitario (USD)**
Patch Panel 24 puertos	33,4
Conectores RJ 45 Macho	1,32
Conectores RJ 45 Hembra	2,13
Rack	4549
Patch cord cat 6ª	1,95
Placas de Pared	380
Cable UTP 6ª	2
Fibra óptica 50/125 micrones	4,25
Panel de distribución de fibra	59
Patch panel fibra 24 puertos	92,4
Patch cord SC	11,5
Transceiver	83,4
Estaciones de voz	380
Hardphones	116
ATA	29
Router	1025
Switch 48 puertos	1515
Switch 24 puertos	422
Cámaras IP	97,80
Enlace Metro Ethernet	2070
UPS	160
Firewall	560
Servidor	470

IV.6 Propuesta técnico-económica

Una vez obtenidos los costos de los equipos y servicios se evaluó la mayor rentabilidad, que permita un equilibrio entre los costos y beneficios, buscando la mayor cantidad de beneficios al menor costo posible. Esta propuesta, permitirá a la empresa poseer la idea de la inversión necesaria para implementar el proyecto en un futuro. Para la conversión de bolívares a dólares, se utilizó la actual tasa de cambio de Bs 4,30 por cada dólar.

No se consideró un presupuesto en fibra óptica para el cableado horizontal puesto que es mucho más costoso que el cable UTP 6ª. De igual modo, solo se hicieron los cálculos de costos de los equipos pero no los costos de la instalación.

Las tablas que se muestran a continuación detallan los costos de los equipos y servicios necesarios en cada una de las sedes de la empresa.

Tabla 15. Costo Cableado Horizontal.

Fuente: Elaboración Propia.

CABLEADO HORIZONTAL					
Equipos	**Cantidad**	**Precio/ unidad (USD)**	**Precio/ Unidad (Bs)**	**Precio Total (USD)**	**Precio Total (Bs)**
Cable UTP 6a	306m	2	8.6	612	2.631.6
Patch Panel 24 puertos	4	33.4	143.62	133.6	574.5
Conectores RJ45 macho	50	1.32	5.805	66	283.8
Conectores RJ45 hembra	50	2.13	9.16	106.5	457.95
Patch cord cat 6a	96	1.95	8.385	187.2	804.96
Rack	9	4549	19561	40941	176046.3
Placas de pared	50	380	1634	19000	81700
Switch 24 puertos	4	422	1814,6	1688	7258,4
Total				**62.734,3**	**269.757,5**

Tabla 16. Costo Cableado Vertical.
Fuente: Elaboración Propia

CABLEADO VERTICAL					
Equipos	**Cantidad**	**Precio/ unidad (USD)**	**Precio/ Unidad (Bs)**	**Precio Total (USD)**	**Precio Total (Bs)**
Fibra óptica multimodo 50/125 micrones	55.6m	4.64	18	257.984	1109.33
Panel de Distribución de Fibra	4	59	253.7	236	1014.8
Patch Panel fibra 24 puertos	4	92.4	397.32	369.6	1589.3
Patch cord sc	8	11.5	49.5	92	395.6
Transceiver GBIC	4	83.4	358.62	333.6	1434.5
Router	1	1025	4407,5	1025	4407,5
Switch 48 puertos	1	1515	6514,5	1515	6514,5
Total				**3.829,18**	**16.465,53**

Tabla 17. Costo Equipos Estructura para voz
Fuente: Elaboración Propia.

EQUIPOS ESTRUCTURA PARA VOZ					
Equipos	**Cantidad**	**Precio/ unidad (USD)**	**Precio/ Unidad (Bs)**	**Precio Total (USD)**	**Precio Total (Bs)**
Patch Panel 24 puertos	4	33.4	143.62	133.6	574.48
Conectores RJ45 macho	50	1.32	5.676	66	283.8
Conectores RJ45 hembra	50	2.13	9.159	106.5	457.95
Patch cord cat 6a	50	1.95	8.385	97.5	419.25
Estaciones de voz	4	380	1634	1520	6536
Hardphones	35	116	498.8	4060	17458
ATA	40	29	124,7	1160	4988
Total				**7.143,6**	**30.717,55**

La tabla 18, muestra los equipos y costos de las sedes móviles.

Tabla 18. Costo Equipos Sedes Móviles

Fuente: Elaboración Propia.

SEDES MÓVILES					
Equipos	**Cantidad**	**Precio/ Unidad (USD)**	**Precio/ Unidad (Bs)**	**Precio Total (USD)**	**Precio Total (Bs)**
Router	1	1025	4407,5	1025	4407,5
Switch 48 puertos	1	1515	6514,5	1515	6514,5
Cámaras IP	30	97,80	420,54	2934	12616,2
Total				**5.474**	**23.538,2**

Finalmente, luego de haber segmentado los distintos servicios y equipos necesarios, la tabla 19 muestra los costos asociados a todo el proyecto, incluyendo las tres sedes fijas y una sede móvil.

Tabla 19. Presupuesto Final
Fuente: Elaboración Propia

ONLYTICKET Eventos					
Servicio	**Cantidad**	**Precio/ unidad (USD)**	**Precio/ Unidad (Bs)**	**Precio Total (USD)**	**Precio Total (Bs)**
Cableado Horizontal	3	62.734,3	269.757,5	188202,9	809272,5
Cableado Vertical	3	3829,18	16465,53	11487,54	49396,59
Equipos Estructura de Voz	3	7143,6	30717,55	21430,8	92152,44
Equipos Sedes Móviles	3	5474	23538,2	16442	70614,6
Enlace Metro Ethernet		-	-	-	16450
Servidores	12	470	2021	5640	21252
Total				**246.304,216**	**1.059.138,14**

Adicionalmente, la empresa Global Crossing, proporcionó los cargos mensuales por el enlace de 4Mbps hacia las sedes, referentes al alquiler de los equipos, el mantenimiento preventivo, correctivo y actualización tecnológica. En la tabla 20 se muestran los costos mensuales, teniendo en cuenta que este servicio está propuesto para una duración de 36 meses.

Tabla 20. Gasto Mantenimiento Mensual por Ambos Enlaces

Fuente: Elaboración Propia

GASTO MENSUAL POR MANTENIMIENTO		
Servicio	**Meses**	**Gasto/ Mensual (Bs)**
Enlace Metro Ethernet (4Mbps, ambos enlaces)	1	12662,60

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

VI.1 Conclusiones

En este Trabajo Especial de Grado, se diseñó satisfactoriamente la red de telecomunicaciones que permite interconectar las sedes de la Empresa OnlyTicket Eventos. Con la realización de este diseño se permite la integración de servicios y tecnologías que representan el crecimiento futuro de la empresa.

Para el diseño de la red de interconexión, se realizó un análisis de la situación actual de la empresa en donde se evaluaron las características físicas del proyecto, donde se pudo determinar que la misma requiere de una red para lograr la eficiente comunicación entre sus sedes, logrando centralizar la información a su sede principal en Caracas. Seguidamente se procedió con las etapas de investigación, definición de las aplicaciones y requerimientos necesarios en la red.

Es importante señalar que en el cálculo del ancho de banda para el dimensionamiento de la red, no existe un modelo definido que proporcione el cálculo exacto del mismo, sino un estimado que servirá de referencia, tomando en cuenta las aplicaciones usadas y cantidad de usuarios presentes en la red.

La tecnología de Metro Ethernet brinda a la empresa la velocidad de transmisión y capacidad necesaria, puesto que ofrece diversas combinaciones entre velocidades y medios de transmisión, permitiendo escoger la mejor opción para la red. Además, esta tecnología es compatible con la topología física utilizada.

Se escogieron equipos marca Cisco debido a que la empresa proveedora de Metro Ethernet, Global Crossing, opera con equipos de esta marca. Asimismo, el *software* de simulación fue Packet Tracer por ser el usado por Cisco.

Las simulaciones realizadas fueron de mucha utilidad para verificar el funcionamiento del enrutamiento estático, direccionamiento IP y la configuración de las VLANs. Adicionalmente se observaron algunas características como el envío y

recepción de correos electrónicos, páginas web, y telefonía IP ejemplificando así algunos de los servicios requeridos en la red diseñada.

A través de un análisis y comparación de precios, se buscó un equilibrio entre los costos y los beneficios obtenidos, buscando siempre la mayor cantidad de beneficios al menor costo posible.

Finalmente, la realización de este Trabajo Especial de Grado permitió llevar a la práctica los conocimientos teóricos adquiridos durante los estudios cursados, siendo estos la base para estudiar las distintas alternativas presentes hoy día en el mercado tecnológico y tomar las decisiones con un criterio técnico y teórico, lo que dio como resultado la red de interconexión diseñada.

VI.2 Recomendaciones

En vista de la economía inestable que existe actualmente en el país, se recomienda iniciar lo antes posible la ejecución del proyecto, a los fines de cumplir con el monto de la inversión presupuestado.

Es de vital importancia el mantenimiento y la administración de la red propuesta, refiriéndose a los equipos que existen dentro de la misma, de esta manera se garantiza siempre el óptimo funcionamiento de la empresa y sus diferentes sedes.

Hay que tener presenta la situación actual del protocolo Ipv4, por lo que se recomienda estudiar un plan de migración hacia el protocolo Ipv6, donde se tome en cuenta el direccionamiento y distribución lógica de la red.

BIBLIOGRAFÍA

1. **Forouzan, B.** *Transmisión de Datos y Redes de Comunicaciones.* Madrid : Mc Graw Hill, 2002.

2. **Arcesio.** Arcesio. [En línea] 2011. http://www.arcesio.net/switches/switches1a.ppt.

3. **Lewis, W.** *Red Inalambrica y Conmutada.* Madrid : Pearson, 2009.

4. **Millán, R.** *Redes de Datos y Convergencia IP.* Madrid : Copyright S.L., 2007.

5. **Chonchi Aller Tomillo, Jorge Rabadán y J. Javier Pastor.** COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN. [En línea] Febrero de 2005. [Citado el: 26 de Febrero de 2011.] http://coit.es/publicaciones/bit/bit149/64-66.pdf.

6. **Muñoz, O.** Diseño y construcción de un sistema para controlar el movimiento de una cámara IP. [En línea] Julio de 2009. [Citado el: 26 de Febrero de 2011.]

7. **Martínez, MAría Julieta Goitia y David Luis.** *Protocolos de Enrutamiento Simulador de Tráfico de Redes.* s.l. : Universidad Nacional de Nordeste.

8. **Tanenbaum, Andrew S.** *Redes de Computadoras.* Mexico : Pearson Prentice Hall, 2003.

9. **Cisco.** Manual Cisco CCNA Protocolos de Enrutamiento. [En línea] Cisco, 17 de Marzo de 2008. [Citado el: 07 de Febrero de 2011.] http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx..

10. **red, Es la.** Práctica 4-Análisis de Tráfico, QoS. [En línea] Es la red, 2004. [Citado el: 07 de Marzo de 2011.] www.eslared.org.ve/walc2004/apc-aa/archivos-aa/.../Practica_QoS.doc..

11. **Xavier, Antoni Barba y.** *Inteligencia de red.* Barcelona : Ediciones UPC, 2002.

12. **Alvarez, Miguel Angel.** Firewall. [En línea] 2008. [Citado el: 05 de Junio de 2011.] www.desarrolloweb.com.

13. **Cisco.** VPN. [En línea] 2010. [Citado el: 02 de Junio de 2011.] http://www.cisco.com/web/ES/solutions/es/vpn/index.html.

14. **Held, Gilbert.** *Virtual Private Networking.* s.l. : John Wiley & Sons, Ltd, 2001.

15. **Mitchell, Bradley.** VPN Tutorial. [En línea] [Citado el: 02 de Junio de 2011.] http://compnetworking.about.com/od/vpn/a/vpn_tunneling.htm..

16. **Cobb, Chey.** *Part I: Crypto Basics & What You Really Need to Know.* 2004.

17. **Microsoft.** VPN Tunneling Protocols. [En línea] 2010. [Citado el: 02 de Junio de 2011.] http://technet.microsoft.com/en-us/library/cc782786(v=ws.10).aspx..

18. **Herrera, E.** *Tecnologías y Redes de Transmisión de Datos.* Mexico : Limusa, Noriega Editores, 2009.

19. **Villacrés, W.H.** *Estudio comparativo de plataformas alternativas de videoconferencia basadas en software en el backbone de la ESPOCH.* 2010 : Escuela Politécnica de Chimborazo.

20. **Cisco.** Voz sobre IP. [En línea] 2010. [Citado el: 05 de Junio de 2011.] http://www.cisco.com/web/ES/solutions/es/voice_over_ip/index.html..

21. **GSM, Portal.** Grupo de tecnología de las Telecomunicaciones. [En línea] 2006. [Citado el: 05 de Junio de 2011.] http://portalgsm.com/documentacion_extendida/104_0_17_0_C/..

22. **D Barnett, D. Groth & J. McBee.** *Cabling: The complete guide to networking.* Alameda : Sybex, 2004.

23. *Suplemento sobre cableado estructurado.* **Systems, Cisco.** 2003.

24. **Global Crossing.** Global Crossing- Level 3. [En línea] 2012. http://www.globalcrossing.com.

25. Informatica moderna. [En línea] 2009. [Citado el: 2 de 7 de 2011.] http://www.informaticamoderna.com/Pantalla_LCD.htm.

26. **Flickenger, R.** *Redes Inalámbricas en los Países en Desarrollo.* 2007.

27. **Lammle, Todd.** *CCNA: Cisco Certified Network Associate.* Indianapolis : Wiley Publishing, 2007.

28. **Microsoft.** Authentication of VPN clients. [En línea] 2010. [Citado el: 02 de Junio de 2011.] http://technet.microsoft.com/en-us/library/cc782786(WS.10).aspx.

29. **Sierra, E.** Proyecto de Metro Ethernet en Medellín-Antioquiía. [En línea] [Citado el: 25 de febrero de 2011.]

ANEXOS

Anexo A

Las siguientes figuras, muestran las distintas oficinas presentes en cada uno de los pisos que conforman las sedes de la empresa y la distribución del cableado horizontal.

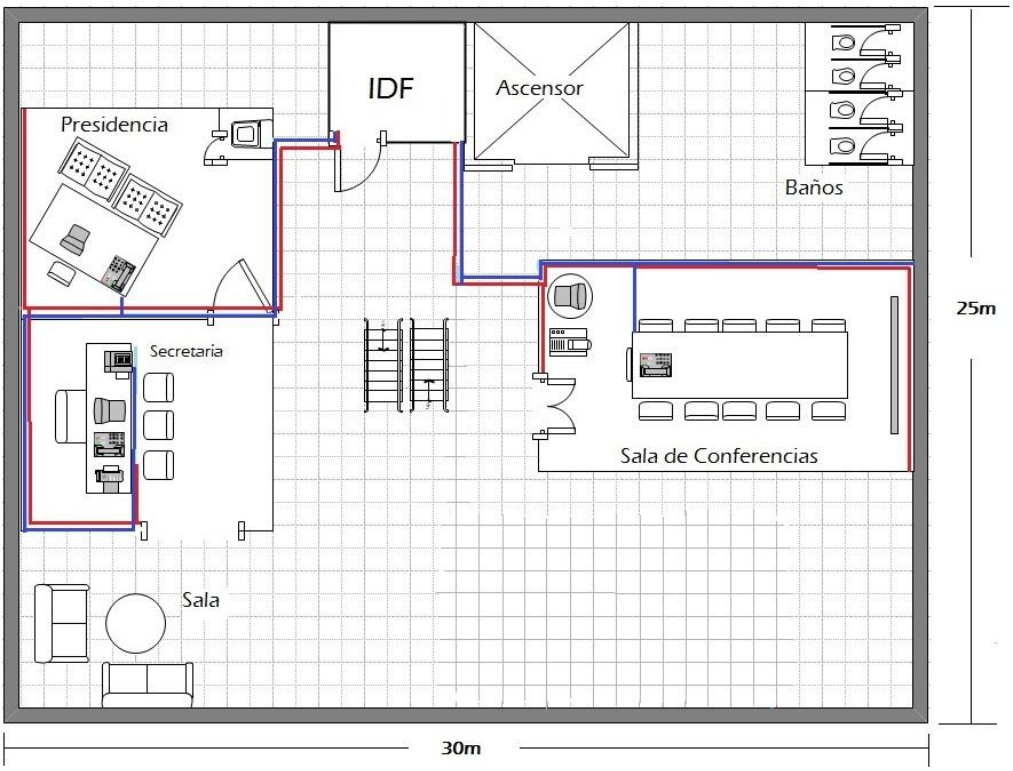


Figura 20. Presidencia

Fuente: Elaboración Propia.

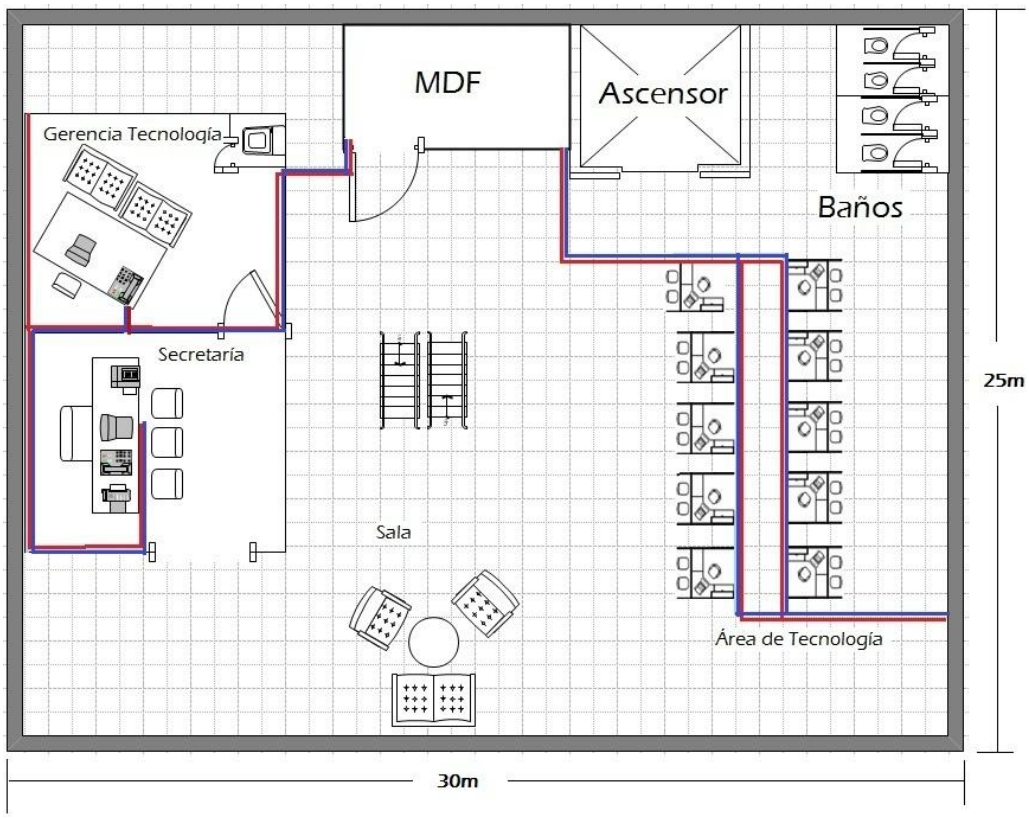


Figura 21. Departamento de Tecnología

Fuente: Elaboración Propia

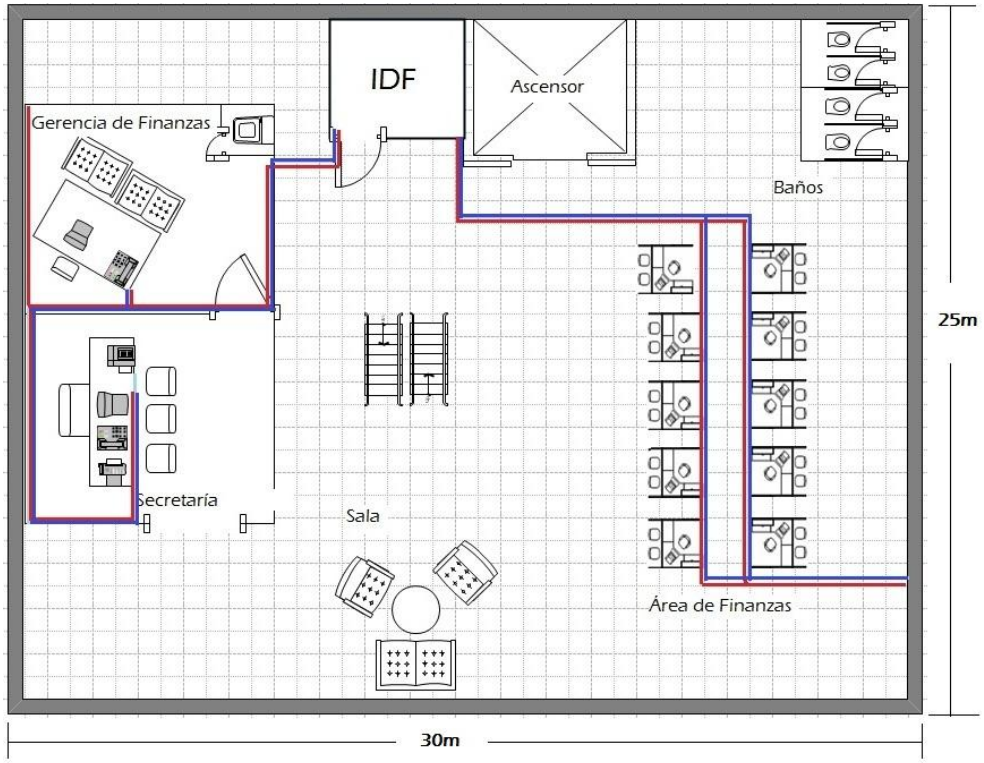


Figura 22. Departamento de Finanzas

Fuente: Elaboración Propia

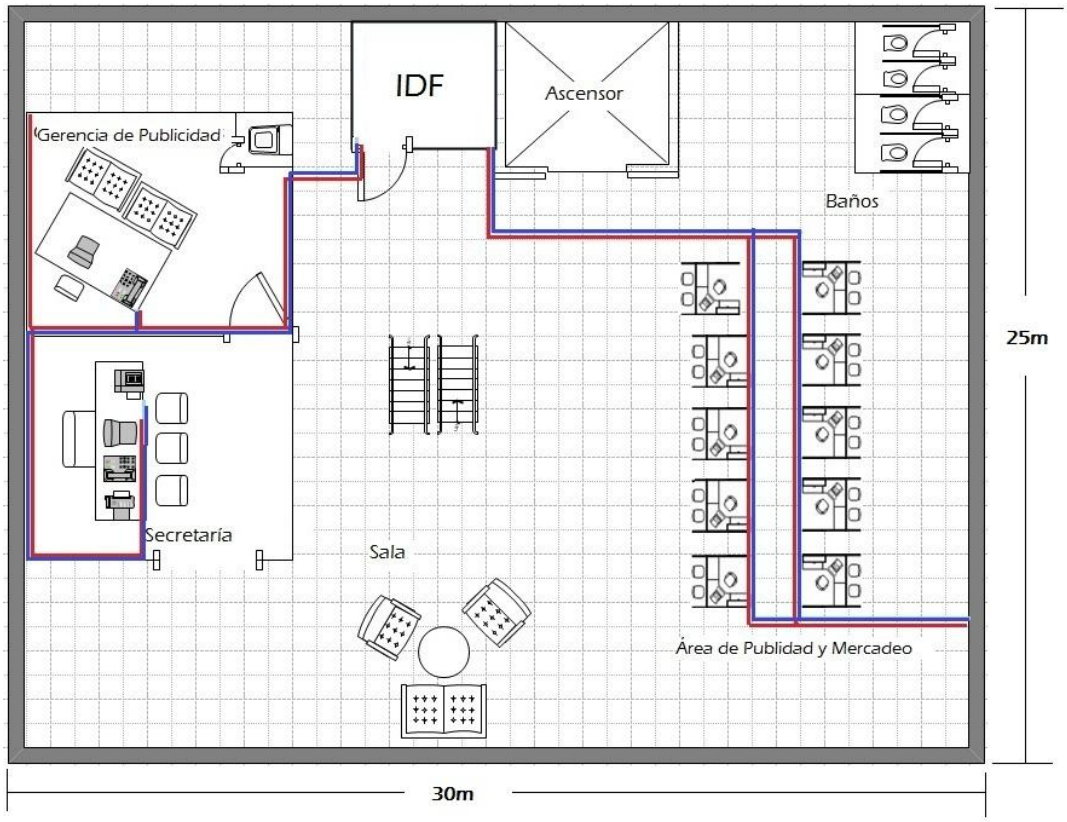


Figura 23. Departamento de Publicidad y Mercadeo

Fuente: Elaboración Propia

Anexo B

A continuación se presenta la tabla 21 correspondiente al direccionamiento IP de la red, siendo distribuido por sede y sus respectivos departamentos. Se observa además la escalabilidad en cada una de las VLANs, en caso de introducirse nuevos equipos en un futuro.

Tabla 21. Tabla de Direccionamiento

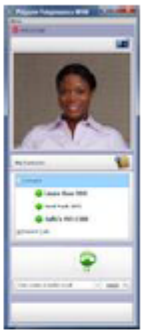
Fuente: Elaboración Propia

Dirección Sub-Red	1er Host	Ultimo Host	Broadcast	Mascara		Ubicación	Número de VLAN	Host Totales	Host Utilizados	Host Disponibles
172.16.0.64	172.16.0.65	172.16.0.126	172.16.0.127	255,255,255,192	/26	VLAN Video (Móvil)	60	62	31	31
172.16.0.128	172.16.0.129	172.16.0.190	172.16.0.191	255,255,255,192	/26	VLAN voz (CCS)	50	62	30	32
172.16.0.192	172.16.0.193	172.16.0.222	172.16.0.223	255,255,255,224	/27	VLAN Voz (PAN)	50	30	17	13
172.16.0.224	172.16.0.225	172.16.0.254	172.16.0.255	255,255,255,224	/27	VLAN Voz (PO)	50	30	17	13
172.16.1.0	172.16.1.1	172.16.1.14	172.16.1.15	255,255,255,240	/28	VLAN Publicidad (CCS)	30	14	13	1
172.16.1.16	172.16.1.17	172.16.1.30	172.16.1.31	255,255,255,240	/28	VLAN Tecnología (CCS)	40	14	11	3
172.16.1.32	172.16.1.33	172.16.1.46	172.16.1.47	255,255,255,240	/28	VLAN Tecnología (PAN)	40	14	7	7
172.16.1.48	172.16.1.49	172.16.1.62	172.16.1.63	255,255,255,240	/28	VLAN Tecnología (PO)	40	14	7	7
172.16.1.64	172.16.1.65	172.16.1.78	172.16.1.79	255,255,255,240	/28	VLAN Tecnología (Movil)	40	14	7	7
172.16.1.80	172.16.1.81	172.16.1.94	172.16.1.95	255,255,255,240	/28	VLAN Administrativa (CCS)	1	14	6	8
172.16.1.96	172.16.1.97	172.16.1.110	172.16.1.111	255,255,255,240	/28	VLAN Administrativa (PAN)	1	14	6	8
172.16.1.112	172.16.1.113	172.16.1.126	172.16.1.127	255,255,255,240	/28	VLAN Administrativa (PO)	1	14	6	8
172.16.1.128	172.16.1.129	172.16.1.142	172.16.1.143	255,255,255,240	/28	VLAN Finanzas (Móvil)	20	14	6	8
172.16.1.144	172.16.1.145	172.16.1.158	172.16.1.159	255,255,255,240	/28	VLAN Finanzas (CCS)	20	14	5	9
172.16.1.160	172.16.1.161	172.16.1.174	172.16.1.175	255,255,255,240	/28	VLAN Finanzas (PAN)	20	14	5	9
172.16.1.176	172.16.1.177	172.16.1.190	172.16.1.191	255,255,255,240	/28	VLAN Finanzas (PO)	20	14	5	9
172.16.1.192	172.16.1.193	172.16.1.206	172.16.1.207	255,255,255,240	/28	VLAN Publicidad (PAN)	30	14	5	9
172.16.1.208	172.16.1.209	172.16.1.222	172.16.1.223	255,255,255,240	/28	VLAN Publicidad (PO)	30	14	5	9
172.16.1.224	172.16.1.225	172.16.1.230	172.16.1.231	255,255,255,248	/29	VLAN Administrativa (Móvil)	1	6	3	3
172.16.1.232	172.16.1.233	172.16.1.238	172.16.1.239	255,255,255,248	/29	VLAN Voz (Móvil)	50	6	3	3
172.16.1.240	172.16.1.241	172.16.1.246	172.16.1.247	255,255,255,248	/29	VLAN Presidencia (CCS)	10	6	3	3
172.16.1.248	172.16.1.249	172.16.1.254	172.16.1.255	255,255,255,248	/29	VLAN Gerencia Regional (PAN)	10	6	3	3
172.16.2.0	172.16.2.1	172.16.2.6	172.16.2.7	255,255,255,248	/29	VLAN Gerencia Regional (PO)	10	6	3	3
172.16.2.8	172.16.2.9	172.16.2.14	172.16.2.15	255,255,255,248	/29	VLAN Gerencia Regional (Movil)	10	6	3	3
172.16.2.16	172.16.2.17	172.16.2.17	172.16.2.18	255,255,255,252	/30	VLAN Publicidad (Movil)	30	2	2	0

Anexo C

Polycom Customer FAQ

Polycom® Telepresence m100™



The standards-based Telepresence m100 raises the bar on mobile video communications. By allowing users to easily connect between desktop and mobile devices to millions of telepresence video conferencing systems in use today, the Telepresence m100 also drives broad adoption. Polycom delivers mobile telepresence within a Unified Communications experience.

Telepresence m100 is the perfect solution for a small to medium business. Utilizing industry standards, Telepresence m100 delivers high-quality audio, video and content at up to HD resolution. The software client is easily downloaded, installed, and running in just a few minutes. Users can then place point-to-point calls or even multipoint calls through a video bridge.

Polycom Telepresence m100 provides features such as:

- High-quality audio, video, and content sharing
- Organizational directory search
- Click-to-call for ease of use
- Compatibility within existing video conferencing hardware and software, including mobile, room and immersive telepresence systems
- Constant Clarity™ for high-quality audio and video over less than optimal internet connections.
- Low total cost of ownership with dual-protocol support for both H.323 and SIP networks in a single application.

FAQ
Q: Where can I buy the Telepresence m100?
A: You can buy Telepresence m100 from your Polycom authorized partner.

Q: What are the PC hardware requirements?
A: See requirements below:

- Basic (up to QVGA):1.5 GHz P4, 1.2 GHz Pentium M/AMD Turion or higher
- Standard (up to CIF, People+Content): 2.0 GHz P4, Pentium M/AMD Turion 1.4GHz
  Premium (up to VGA, People+Content): 3.2 GHz Pentium, Pentium M/AMD Turion 2.0 GHz
- HD (up to 720p): Quad Core Duo 2.0 GHz
- RAM: XP – 1GB, Vista – 2GB
- Windows XP, Windows Vista, and Windows 7 – 32bit
- Storage: 30MB

POLYCOM

1

- 256 MB video RAM recommended for Vista
- Display: XGA, 16-bit color or higher

Q: What types of cameras will work with Telepresence m100?
A: USB 2.0 Web Cameras: Microsoft HD-5000, Microsoft LifeCam Cinema, LifeCam HD-6000, Logitech C100, Logitech C210, Logitech C310, Logitech Webcam Pro 9000, Logitech Webcam C905

Q: Do I need a keycode to activate my Telepresence m100 software? If so, how do I get it?
A: Yes. A keycode can be purchased from your Polycom representative or certified partner.

Q: Each time I start the application I am asked to activate my software. How can I hide this message?
A: After you purchase, enter your activation key and this dialog will no longer appear.

Q: Does Telepresence m100 include service?
A: The client price includes one year of service. You can extend this period by purchasing additional years through your Polycom representative.

Q: I can't seem to get two-way both audio and video. What can I do?
A: Telepresence m100 supports H.460 firewall traversal. However, you are likely experiencing a port blocking on one or more call signaling ports. Please consult your IT representative for further information.

Q: Can the Telepresence m100 be used for chat?
A: No, not at this time.

Q: Does the Telepresence m100 support presence?
A: No, not at this time.

Q: Can a PVX license be converted into a Telepresence m100 license?
A: No.

Q: Can an m100 license be converted into a Polycom CMA Desktop license?
A: No, they are two distinct products.

Q: Is there recommended network bandwidth availability (and call speed) for the Telepresence m100?
A: Based on your network environment, one of the recommended speeds below is appropriate:
Corporate LAN: 1929 kbps
Premium Broadband: 768 kbps
Residential Broadband: 384 kbps-512 kbps

POLYCOM

2

Q: Can I install Telepresence m100 on a computer that has Polycom CMA Desktop installed?
A: Yes. Make sure Polycom CMA Desktop is not running before you install Telepresence m100.

Q: Can I have both the CMA Desktop and the Telepresence m100 running at the same time on the same computer?
A: No.

Q: Can I dial into meeting rooms or endpoints from outside the network without a VPN?
A: Yes. If you are not on the VPN and want to call use the appropriate Polycom® Video Border Proxy™(VBP®). Enter the address in this format: IP_Address ##E.164. For example, 11.12.13.14##1000.

Q: Can I use the Telepresence m100 like a Voice-Over IP (VOIP) phone?
A: Telepresence m100 is capable of placing calls without the use of a camera. However, the call is not a traditional VOIP call that is capable of calling PSTN phones.

Q: Can I use Telepresence m100 over VPN?
A: Yes. We support a Juniper Virtual Private Network (VPN) solution but it is not required for call connection into the organization. Telepresence m100 operates much like a video conferencing system dialing from the public internet.

Q: During installation I saw an opportunity to use SIP, should I have a SIP address?
A: SIP signaling protocol is supported, but not necessary. Contact your IT representative for SIP registration purposes.

Q: Can the Telepresence m100 register to a standards-based H.323 Gatekeeper?
A: Yes. An excellent choice would be the Polycom CMA™ 4000 or 5000 if available.

Q: What is the difference between the Telepresence m100 and theTelepresence m500?
A: The primary difference is that the Telepresence m100 is for PC-based operating systems such as Windows while the Telepresence m500 is for mobile operating systems such as Android.

Q: How do I contact Polycom technical support?
A: www.support.polycom.com

Tips and Tricks

1. When using over the public internet limit call rates to between 384k and 512k unless you can guarantee higher call speeds through fiber or similar business class connections.
2. Never sit with your back to a window. Backlighting causes the camera iris to close and make your image dark and unrecognizable.
3. Use only approved USB cameras unless you are using ones embedded inside the laptop frame.

POLYCOM®

3

Anexo D

En el siguiente Anexo se muestra el enrutamiento realizado para las sedes de Caracas, Puerto Ordaz y Panamá

Tabla 22. Enrutamiento Caracas

Fuente: Elaboración Propia

Dirección IP Red	Máscara	Dirección IP destino
172.16.0.64	255.255.255.192	200.1.1.2
172.16.1.128	255.255.255.240	200.1.1.2
172.16.1.224	255.255.255.248	200.1.1.2
172.16.1.232	255.255.255.248	200.1.1.2
172.16.2.8	255.255.255.248	200.1.1.2
172.16.2.16	255.255.255.252	200.1.1.2
172.16.0.192	255.255.255.224	200.2.2.2
172.16.1.32	255.255.255.240	200.2.2.2
172.16.1.96	255.255.255.240	200.2.2.2
172.16.1.160	255.255.255.240	200.2.2.2
172.16.1.192	255.255.255.240	200.2.2.2
172.16.1.248	255.255.255.248	200.2.2.2
172.16.0.224	255.255.255.2224	200.3.3.1
172.16.1.48	255.255.255.240	200.3.3.1
172.16.1.112	255.255.255.240	200.3.3.1
172.16.1.176	255.255.255.240	200.3.3.1
172.16.1.208	255.255.255.240	200.3.3.1
172.16.2.0	255.255.255.248	200.3.3.1

Tabla 23. Enrutamiento Panamá.

Fuente: Elaboración Propia

Dirección IP red	Máscara	Dirección IP destino
172.16.1.80	255.255.255.240	200.2.2.1
172.16.1.0	255.255.255.240	200.2.2.1
172.16.1.144	255.255.255.240	200.2.2.1
172.16.1.16	255.255.255.240	200.2.2.1
172.16.0.128	255.255.255.192	200.2.2.1
172.16.1.240	255.255.255.248	200.2.2.1

Tabla 24. Enrutamiento Puerto Ordaz.

Fuente: Elaboración Propia

Dirección IP red	Máscara	Dirección IP destino
172.16.1.80	255.255.255.240	200.3.3.1
172.16.1.0	255.255.255.240	200.3.3.1
172.16.1.144	255.255.255.240	200.3.3.1
172.16.1.128	255.255.255.192	200.3.3.1
172.16.0.240	255.255.255.248	200.3.3.1
172.16.1.16	255.255.255.240	200.3.3.1