DISEÑO DE LA RED CORPORATIVA QUICOM S.A. Y YABELKO S.A.

LEÓN ESTEBAN GONZÁLEZ RIVERA
DAVID ZULUAGA ELJACH

UNIVERSIDAD EAFIT
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
MEDELLÍN, COLOMBIA
2011

DISEÑO DE LA RED CORPORATIVA QUICOM S.A. Y YABELKO S.A.

LEÓN ESTEBAN GONZÁLEZ RIVERA
DAVID ZULUAGA ELJACH

TRABAJO DE GRADO

JOSE LUÍS MONTOYA PAREJA
ASESOR

UNIVERSIDAD EAFIT
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
MEDELLÍN, COLOMBIA
2011

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Medellín, 4 de Noviembre de 2011

AGRADECIMIENTOS

Muchas gracias a mis amigos y familia por todo su apoyo durante el desarrollo de mi carrera, gracias a ellos soy la persona que soy y he logrado llegar a este punto. Son un soporte incondicional.

A mi madre María Melva Rivera, la mujer más trabajadora y dedicada que conozco. Sin ella hoy yo no sería nadie, es mi apoyo y mi soporte y gracias a su esfuerzo hoy estoy escribiendo estas páginas.

A mi compañero y amigo de proyecto, hemos estado juntos desde el colegio y ahora terminamos un ciclo más de nuestra vida, juntos.

LEÓN ESTEBAN GONZÁLEZ RIVERA

Quiero agradecer a mis padres, por el apoyo incondicional, por siempre creer en mí y por ser mi modelo de vida. Quiero también agradecerle a mi compañero y amigo León, por dar lo mejor de sí para el proyecto y querer compartir conmigo este logro.

DAVID ZULUAGA ELJACH

DEDICATORIA

Quiero dedicar este trabajo y todo el trabajo realizado durante mi carrera a la memoria de mi padre, Hugo León González Bedoya (Q.E.P.D). Su ejemplo fue mi modelo a seguir, y ahora puedo decir que soy como él, como siempre quise desde pequeño.

LEÓN ESTEBAN GONZÁLEZ RIVERA

Le dedico a mi abuelita Nelly Muñoz, mis esfuerzos, logros y conocimiento adquirido. Sé que de todo corazón has querido que alcance mis ideales y por eso te has convertido en una razón más para lograrlos.

DAVID ZULUAGA ELJACH

CONTENIDOS

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

***Access Point*:** Un *Access Point* es un dispositivo que envía y recibe información hacia y desde los hosts de una red inalámbrica. En la mayoría de los casos, sirve como el punto de conexión entre una red inalámbrica y una red alámbrica. Múltiples *Access poínos* pueden hacer parte de una misma red inalámbrica, de manera que se pueda brindar conexión con una amplia cobertura.

Dominio de *Broadcast*: Es una división lógica de nodos de red, en la cual todos éstos pueden alcanzarse entre sí a nivel de capa de enlace de datos mediante *broadcast* (transferencia de información a todos los destinatarios simultáneamente) .

***Firewall*:** Consiste en un conjunto de funcionalidades de un equipo ubicado como puerta de enlace de una red, las cuales protegen los recursos de una red privada de usuarios de otras redes. Por lo general son usados en las empresas, cuando a los empleados se les brinda acceso a internet, para prevenir intrusiones y controlar los recursos externos a los cuales los empleados pueden tener acceso.

Un *firewall* trabaja junto con el enrutamiento, examinando cada uno de los paquetes de la red para determinar si este debe ser enviado o no a su destino, el firewall normalmente funciona de forma separada del resto de los equipos de red de tal manera que no sea posible acceder directamente a los recursos de la red. Un *firewall* puede validar los paquetes de datos de muchos métodos, pero la forma más básica es por medio del tipo de protocolo o nombre de dominio.

Hipertexto: Es un conjunto de unidades de información conectada a través de vínculos (hipervínculos), que puede contener texto, imágenes, tablas, entre otras cosas. Es la base de la *World Wide Web*. Es la manera más común de difundir información a través de internet.

Hipervínculo: Es un vínculo contenido dentro de un documento de hipertexto, que lleva hacia otro documento completo o alguna información específica dentro del documento. Sirve para navegar a través de varios documentos de hipertexto.

HTTP (*Hypertext Transfer Protocol*): Es un protocolo que define una serie de reglas para transferir documentos de hipertexto desde un servidor hacia un cliente. Básicamente, funciona enviando mensajes de petición de información desde un cliente hacia un servidor, el cual responde a ésta petición con la información requerida.

Intranet: Una red privada de una compañía. Se comporta como una versión privada de internet, para compartir documentos e información entre los mismos usuarios de la

compañía. A través de túneles, se pueden crear intranets a través de redes públicas y de esta manera extender la intranet a lugares remotos.

IPS (*Intrusion Prevention System*): Aplicación de seguridad que monitorea todo el tráfico de la red con el objetivo de prevenir intrusiones (accesos indeseados a la red) basándose en las reglas y políticas definidas por el administrador de la red.

Generalmente funciona bloqueando todo el tráfico de cierta dirección IP o puerto del cual un paquete proveniente se cataloga como malicioso, o analizando y detectando patrones en el tráfico y así evitando futuros ataques y posibles intrusiones.

ISP (*Internet Service Provider*): Es una compañía que provee servicio de conexión a internet y, en muchos casos, otros servicios como telefonía y televisión a particulares y empresas. Tienen la infraestructura necesaria para poner un punto de presencia en donde se requiera dentro del área geográfica de cobertura.

KDS (*Kitchen Display System*): Sistema de Pantallas de Cocina: Subsistema de MICROS que permite administrar y mostrar en cocina la información de los pedidos que realizan los clientes al restaurante, en tiempo real y de la manera eficiente, monitoreando los tiempos y los estados de dichos pedidos.

Mensajería Instantánea: Es un modo de mensajería en tiempo real basada en mensajes de texto enviados a través de internet, entre dos o más personas conectadas a través de un computador u otro dispositivo como un *Smartphone* o *tablet*. Inicialmente, era necesario contar con un software especializado para esto, pero hoy en día se puede acceder a este servicio a través de sitios WEB.

MICROS *Workstation* (Estación de trabajo de MICROS): Es una solución de hardware de MICROS para punto de venta basada en PC, con pantalla táctil y completamente integrada a las labores administrativas. Son operadas por personal del restaurante para atención al cliente.

Navegador WEB: Es una aplicación que sirve para acceder a la información de los documentos contenidos en la *World Wide Web*. Utiliza el protocolo HTTP para obtener los documentos, normalmente escritos en lenguaje HTML el cual el navegador puede interpretar.

***Patch panel*:** Es un dispositivo de red pasivo, que consiste en un conjunto de conectores de red al cual llegan las conexiones de los hosts y de allí las lleva al dispositivo al cual deben ir conectados, normalmente un *switch.* Es un dispositivo pasivo porque no realiza ningún tipo de proceso sobre los datos que viajan por él, se usa como organizador de conexiones.

***Phishing*:** Consiste en un fraude vía E-mail en el cual se envía a la víctima un correo aparentemente legitimo con el objetivo de conseguir información personal y financiera, el mensaje parece ser enviado por páginas de bancos, entidades financieras, redes sociales, páginas de comercio electrónico, etc. Se basa en la inocencia de la víctima para que esta misma sea quien provea de la información que se quiere obtener.

PoP (*Point of Presence*): Punto de presencia es el sitio físico específico dentro de un lugar, desde el cual un ISP ofrece salida a internet.

POS (*Point Of Sale*): Es el punto donde ocurre una transacción de venta al público. Es el equivalente a una caja registradora, pero con más funciones como el almacenamiento de información, generación de reportes e impresión de facturas.

QoS (*Quality of Service*): Calidad de servicio consiste en la idea de establecer un flujo de datos por una red de tal manera que se le dé prioridad a ciertas características que dicho flujo de datos debe contar en particular. Las características más importantes de calidad en los flujos de datos son: confiabilidad (evitar bits incorrectos en la transferencias de datos), retardo (minimizar el tiempo que toma la transferencia), fluctuación (evitar que los paquetes de datos llegan de manera desordenada) y ancho de banda (capacidad para enviar simultáneamente la mayor cantidad de datos posible). Algunas aplicaciones necesitan prioridad en unas características más que en otras dependiendo del tipo de aplicación, por lo general las que funcionan en tiempo real necesitan mayor prioridad en el retardo y fluctuación que en la confiabilidad.

***Router*:** Es un dispositivo físico o, en algunos casos, un software de computador que se encarga de decidir el siguiente paso de un paquete que va de una red hacia otra red. Un *router* debe estar conectado a un mínimo de dos redes entre las cuales decide el destino de los paquetes que viajan por él, basado en una tabla de enrutamiento que contiene ésta información. Se localiza en medio de dos redes y en todo punto de presencia de internet.

Sistema Autónomo: Es una red o un conjunto de redes que comparten una misma política de enrutamiento, controlada por un administrador o grupo de administradores para el beneficio de una misma entidad (Universidad, corporación, negocio, etc.). Un sistema autónomo a veces se define como un dominio de enrutamiento.

***Smartphone*:** Teléfono móvil que contiene funciones extras a las de un teléfono móvil convencional, entre las que se encuentran multimedia, navegación en internet, GPS, cámaras fotográficas y de video, entre otras.

***Spyware*:** Es un programa que logra alojarse en el computador de la víctima de forma secreta como virus o por medio de la instalación de cualquier otra aplicación, espiando y

obteniendo información de una persona u organización y reportándola a quienes perpetran el espionaje.

***Switch*:** Es un dispositivo que se encarga de recibir el tráfico de múltiples puntos de red y enviarlo por el puerto correspondiente para que llegue a su destino. Todo dispositivo que se encuentra conectado a una red, su primer punto de conexión no pasivo es en un *switch*.

***Tablet*:** Dispositivo móvil con funciones similares a las de un computador portátil, pero con la característica principal que su medio de interacción es a través de su pantalla táctil. Sirve principalmente para navegación en internet, edición de documentos, multimedia y juegos.

Telefonía IP: También conocida como VoIP (*Voice over Internet Protocol* - Voz sobre Protocolo de Internet) es un conjunto de tecnologías y estándares que permiten la difusión de voz sobre redes basadas en IP, como el internet.

UTM (*Unified Threat Management*): Equipo de seguridad de red que incluye protección contra múltiples amenazas, generalmente incluye de forma integrada las funcionalidades de firewall, antivirus y filtros de contenido. La ventaja principal de los equipos UTM es la facilidad para el administrador de red de gestionar todos los programas de seguridad de forma unificada.

VLSM (*Variable Length Subnet Mask*): Es una técnica usada para la creación de subredes, que consiste en la variación de los bits de la máscara de subred de una dirección IP, de manera que los bits de hosts sean suficientes para cubrir el direccionamiento de una LAN, sin que se desperdicien direcciones, de manera que todas las direcciones puedan ser usadas de forma eficiente.

***Web Filter*:** Programa que analiza las páginas Web entrantes con el fin de determinar si es permitido o no mostrarla al usuario completa o parcialmente, esta decisión es tomada basándose en el conjunto de reglas definidas por el usuario y generalmente basándose en las normas establecidas por la organización. Los objetivos de establecer esta característica de seguridad en una organización son: evitar contenidos indebidos para los usuarios de la red y evitar posibles fuentes de virus y spyware. La forma de funcionamiento de un Web Filter se basa en filtros de contenido, llevando a cabo ciertas acciones dado el caso que alguna cadena de texto sea coincidente con las reglas establecidas.

WWW(*World Wide Web*): Es un servicio de documentos de hipertexto al cual se accede a través de internet. También es conocido como la *WEB* (Red en inglés). A través de un navegador *WEB*, se puede acceder a texto, música, videos, noticias y otros servicios

multimedia mediante hipervínculos que se encuentran contenidos en estos documentos. Actualmente la WWW se encuentra expandida por todo el mundo, y se está convirtiendo en el modo de acceso no sólo para contenido multimedia, sino también para aplicaciones que ofrecen diversos servicios, como compartir archivos, sesiones de escritorio remotas y conversión de diferentes tipos de archivos.

1. INTRODUCCIÓN

1.1. DEFINICIÓN DEL PROBLEMA

Quicom S.A. y Yabelko S.A. son dos empresas encargadas del manejo de dos importantes franquicias de comida rápida en Colombia respectivamente. Ambas empresas son administradas por Quicom S.A.

La empresa, aunque cuenta con tecnología de gran capacidad y funcionalidad, tiene una red poco estructurada que actualmente cumple con sus funciones básicas pero no suple todas las necesidades que el negocio demanda, debido a sus altas expectativas de crecimiento. Por este motivo se hace necesario diseñar e implementar un mejoramiento a la red actual, que soporte dicho crecimiento, tanto en términos de servicios como de seguridad. Una red que sea la plataforma ideal para implementar soluciones a los diferentes tipos de problemas que se le presentan actualmente tanto al personal administrativo, como al operativo y que permita sacar el máximo provecho a la tecnología ya mencionada.

Se desea entonces tener una red organizada, estructurada y esquematizada, que no sólo solucione las necesidades inmediatas del negocio, sino que también sirva de base para el futuro crecimiento del departamento de TI, evitando mayores problemas que se puedan presentar cuando la red no pueda dar abasto a las operaciones del negocio y sea necesaria una solución rápida y costosa, que pueda generar un impacto grande en la compañía e incluso llegar a verse afectada su productividad operacional.

1.2. OBJETIVOS

1.2.1. Objetivo General

Adecuar el área de tecnología para el diseño de una red estructurada para la compañía, que cumpla con todas las necesidades que demanda el negocio y sus expectativas de crecimiento.

1.2.2. Objetivos Específicos

- Mejorar la arquitectura de la red corporativa.
- Diseñar una infraestructura de red que soporte el crecimiento de la compañía.
- Diseñar un esquema de direccionamiento para la red.

- Implementar un nivel de seguridad sobre la red que permita su confiabilidad, confidencialidad e integridad de la información.

1.3. ALCANCE Y PRODUCTOS

El alcance enmarca al proyecto entre la concepción inicial de la propuesta, análisis y diseño de la red según las necesidades propias del negocio, hasta la gestión de los proveedores de tal manera que en cualquier momento la empresa pueda seleccionar el que implementará la solución basada en el diseño previamente hecho. La gestión de adquisición de un servidor y los servicios necesarios sobre la red también se incluyen dentro del alcance del proyecto.

El entregable del proyecto es el diseño de la red, que contiene:

- Esquema de arquitectura de red, con la distribución de las sedes administrativas y los locales, a nivel nacional (Colombia).
- Esquema de arquitectura de red detallado de las ciudades, incluyendo detalle dentro de los locales y sedes administrativas.
- Esquema detallado de direccionamiento IP.
- Especificaciones técnicas de la red (anchos de banda, descripción de equipos, tipos de cableado).
- Aspectos tenidos en cuenta para la preselección de proveedores.
- Entrega de información de los proveedores que mejor satisfacen las necesidades de la implementación del proyecto y sus propuestas de infraestructura.

1.4. METODOLOGÍA

La metodología a seguir se basa principalmente en identificar el estado de la red actual de la compañía, definir los requerimientos para el nuevo diseño, realizar el diseño, preseleccionar y contactar proveedores y presentar propuestas a la compañía.

1.4.1. Estado actual de la red

Es necesario determinar el estado de la red actualmente, de manera que se puedan identificar problemas en la misma y que consideraciones se deben tener en cuenta para el diseño final de la red. En este proceso se deben tener en cuenta:

- Estado de conectividad de los restaurantes con la oficina principal.

- Estado de la conectividad dentro de los restaurantes
- Estado de la conectividad dentro de la oficina principal
- Equipos existentes en la red y su estado.
- Servicios y aplicaciones existentes que hacen uso de la red.

1.4.2. Requisitos para el nuevo diseño

Una vez determinado el estado de la red actual, se pueden establecer los requisitos para el nuevo diseño. Es necesario tener varias consideraciones para la nueva red:

- Necesidades de conectividad
- Servicios y aplicaciones que hacen uso de la red, en los restaurantes, en la oficina y entre los restaurantes y la oficina.
- Niveles de seguridad en la red.
- Posibles servicios y aplicaciones futuras que hagan uso de la red.
- Crecimiento de la compañía.

1.4.3. Diseño de la red

Después de establecer los requisitos, se puede realizar el diseño de la red con todas las consideraciones hechas. El diseño de la red incluye:

- Diseño general de la red, con soluciones de conectividad.
- Diseño de red de los restaurantes.
- Diseño de red de la oficina principal.
- Direccionamiento IP.
- Especificaciones técnicas de la red.

1.4.4. Proveedores y propuestas

Una vez realizado el diseño de la red, es necesario conseguir proveedores aptos para realizar la implementación, se definen entonces unos parámetros mínimos que deben cumplir estos proveedores para ser preseleccionados, dichos parámetros se establecen en base a las características del escenario de la empresa y las características del diseño de la red, Finalmente se contactan a los proveedores preseleccionados para solicitarles sus propuestas.

1.5. IMPORTANCIA DEL PROYECTO

Se considera que el problema presentado en este proyecto es idóneo para poner en práctica y demostrar los conocimientos adquiridos durante la carrera de Ingeniería de Sistemas y más específicamente, los conocimientos adquiridos en la línea de énfasis en Telemática. En general los temas tenidos en cuenta para la implementación de la solución son:

- Gestión de proyectos informáticos.
- Redes LAN.

Aunque el proyecto no requiere ningún tipo de desarrollo de software, se pueden tomar elementos prestados de la ingeniería de software como lo es la disciplina para la definicion del problema y el análisis de su solución.

2. MARCO TEÓRICO

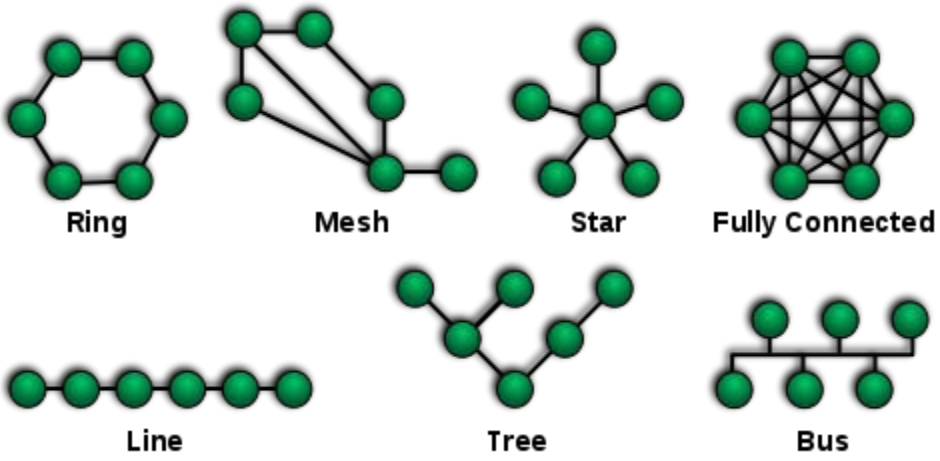
2.1. REDES LAN

Las redes de área local LAN (por sus siglas en inglés, *Local Area Network*), son redes de propiedad privada que tienen por objetivo conectar computadores personales y estaciones de trabajo dentro de una misma empresa o fábrica, para de esta manera compartir recursos como servicios e impresoras, e intercambiar información. Su despliegue es limitado hasta algunos kilómetros. Normalmente, se considera una red LAN aquella que va desde una red doméstica hasta la red de un campus con varios edificios, como una universidad o una fábrica.

Las redes LAN también están delimitadas por su tecnología de transmisión. Actualmente las velocidades de transmisión en una red LAN son de 10/100 Mbps siendo Ethernet por par trenzado la tecnología más utilizada, aunque los nuevos diseños que se están implementando llegan hasta los 1000 Mbps y 10000 (10 Gbps) gracias a tecnologías como la fibra óptica. También se usa la tecnología inalámbrica 802.11 que puede funcionar a velocidades desde 54 Mbps hasta 600 Mbps (802.11n). Se profundizará más adelante en cada uno de estos temas. Estas velocidades siempre son conocidas, por lo que es posible realizar un diseño que permita un mejor uso de los servicios optimizando éstos canales de transmisión.

La topología de red es otra de las características de una red LAN. Una topología de red es la disposición de interconexiones de los nodos en una red. Un nodo no siempre tiene que ser un equipo, ya que estas topologías pueden ser físicas o lógicas (por ej. Lógicas mediante el uso de VLAN). Existen diferentes tipos de topologías, ente las más comunes se encuentran: topología en anillo, en bus, en estrella, en malla, en árbol, etc.

Figura 1. Topologías de redes LAN



Fuente: WIKIMEDIA FOUNDATION, INC. Wikipedia, La enciclopedia libre.

Actualmente las redes LAN constituyen para las empresas un importante activo en su patrimonio, ya que es de vital importancia la interconexión de sus estaciones de trabajo, oficinas y sedes, con el objetivo de brindarles a sus clientes un mejor servicio. Anualmente las empresas invierten grandes sumas de dinero en el mantenimiento y modernización de sus redes, con la que esperan obtener beneficios en muchas de sus áreas.

2.2. REDES WAN

En contraste con las redes de área local LAN, las redes de área amplia WAN (por sus siglas en inglés, *Wide Area Network*), son redes que abarcan espacios geográficos mucho más grandes que las redes LAN, a nivel nacional e incluso continental. Utilizan tecnologías diferentes y son con frecuencia, usadas para interconectar otras LAN entre sí. Normalmente, los proveedores de servicios de internet, telefonía, telefonía móvil y televisión son quienes cuentan con este tipo de redes a nivel nacional, y prestan sus servicios a empresas para que éstas puedan interconectar sus sedes remotas para la compartición de servicios e información.

Las tecnologías usadas en las redes WAN son diferentes de las usadas en las redes LAN, aunque ya se está usando Ethernet para redes más amplias que las LAN. Entre las tecnologías que se usan en las redes WAN se encuentran Frame Relay, ATM, PPP etc. No se entrará en detalle en estas tecnologías, ya que no hacen parte de temas a tratar dentro del proyecto.

2.3. MODELO OSI

El modelo OSI es un modelo de referencia creado por la ISO para definir las capas que debe tener todo sistema de comunicación. Sus siglas significan Interconexión de Sistemas Abiertos (*Open Systems Interconnection* por sus siglas en inglés), y se diseñó para poder permitir la comunicación entre sistemas diferentes, estandarizando en capas las funciones que deben cumplirse para permitir dicha comunicación. El modelo OSI no es una arquitectura de red, es decir, no tiene una implementación propia, es más una guía para nuevos modelos como TCP/IP, que es el modelo en el cual está basado internet.

El modelo OSI consta de 7 capas. Cada capa inferior presta un servicio a su capa inmediatamente superior. Éstas son las capas del modelo:

Figura 2: Capas del modelo OSI

Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

Capa física: Es el nivel más bajo del modelo OSI y, en general, de cualquier modelo o arquitectura de red. En este nivel se define cómo es la transmisión de bits por el medio físico, a nivel eléctrico y mecánico. A este nivel, se deben definir reglas como:

- Niveles de voltaje para representar 1's y 0's.
- Tiempo de duración de un bit (nanosegundos).
- Codificación de la señal eléctrica.
- Disposición y uso de los pines de un adaptador de red.
- Establecimiento de la conexión física entre un punto físico y otro.

Capa de enlace de datos: En este nivel, los datos que se transmiten son divididos en tramas por el emisor, quien las envía organizadas al receptor. Esto se hace con el fin de convertir esta transmisión en un canal de comunicación controlado, en el que se hace control de flujo y de errores. Esta capa debe garantizar que se envíe y reciba el mensaje

original, sin errores, para así poderlo entregar a la capa superior (red) y así se puedan procesar los datos de manera correcta. A este nivel operan los conmutadores.
En este nivel existe un direccionamiento físico que identifica el hardware de red con el que el dispositivo se conecta a ésta, de manera que se puedan entregar las tramas que son destinadas para él. Todas estas operaciones son a nivel de red local, siendo el direccionamiento a nivel de redes diferentes una tarea de la capa superior.

Capa de Red: En este nivel, se realiza direccionamiento entre hosts pertenecientes a redes diferentes, y a veces heterogéneas. Los datos se organizan en paquetes, los cuales deben ser enrutados desde el host de origen hasta el host de destino, no importa la ubicación en que se encuentre cada uno. A este nivel operan los enrutadores, quienes utilizan protocolos y tablas de enrutamiento para asegurarse de que los paquetes lleguen a su destino. En este nivel, se realizan las siguientes tareas:

- Enrutamiento de paquetes.
- Fragmentación: algunas veces los paquetes pueden ser muy grandes para el receptor, por lo que se deben fragmentar los paquetes de manera que puedan ser recibidos.
- Desfragmentación: así como los paquetes algunas veces se pueden fragmentar, deben ser desfragmentados en el destino para su correcta recepción.
- Control de congestión: Factores como la velocidad de transmisión y fragmentación, hace que se presenten cuellos de botella. Estos cuellos de botella causan cogestión en los dispositivos encargados de enrutar los paquetes, por lo que se debe contar con control de congestión.
- Direccionamiento: En este nivel opera el direccionamiento IP (del protocolo TCP/IP), el cual es un esquema no jerárquico de direccionamiento para realizar el transporte de los paquetes del origen al destino.

En este nivel, se establecen conexiones entre enrutadores hasta que los paquetes lleguen a su destino. Hasta esta capa, las conexiones se realizan entre los equipos y sus vecinos inmediatos. El enlace que se realiza de extremo a extremo entre origen y destino se realiza a nivel de transporte y en las capas superiores.

Capa de transporte: Como se menciona anteriormente, en este nivel es donde se realiza la conexión de extremo a extremo. Un programa en un equipo se comunica con un programa en otro equipo de manera bidireccional y éstos necesitan comunicarse por medio de mensajes. La capa de transporte es la encargada de realizar esta conexión, tomando los datos que vienen de sus capas superiores y empaquetándolos (fragmentándolos si es necesario) y enviándolos a la capa de red para que ésta realice el enrutamiento de dichos paquetes, asegurándose de que éstos lleguen al otro extremo libre de errores. Son tareas de la capa de transporte:

- Establecer la conexión de extremo a extremo y mantenerla.

- Segmentar y des-segmentar la información que viene/va a las capas superiores.
- Realizar control de flujo y control de errores.
- Es la capa que aísla a las capas superiores de la tecnología que se está usando, de manera que para ellas sea transparente la conexión sin importar lo que haya más abajo.

A este nivel operan los llamados puertos TCP y UDP (protocolos comunes en esta capa), los cuales veremos con más detalle en el modelo TCP/IP.

Existen protocolos orientados y no orientados a la conexión. La diferencia entre ambos es que los primeros se preocupan por establecer una conexión entre origen y destino, controlar los errores y reenviar paquetes que no se reciben. Se utilizan para aplicaciones que deben transmitir datos de manera confiable y segura, sin importar mucho la velocidad (ya que es más demorado por el reenvío de paquetes perdidos). Los segundos, son protocolos que envían los mensajes sin confirmar si llegan o no al destino. No mantienen una conexión abierta como si lo hacen los protocolos orientados a la conexión. Este tipo de protocolos se utilizan para aplicaciones en tiempo real, como voz por IP.

Capa de sesión: Es la capa encargada de establecer conexiones entre máquinas en diferentes extremos mediante sesiones. Las sesiones deben ofrecer servicios como control de dialogo, control de *token* y sincronización.

Capa de presentación: Es la encargada de presentar los datos a la capa de aplicación, de manera que ésta las entienda. Maneja la sintaxis y semántica de la información que se transmite, haciendo un mapeo de manera que aplicaciones que usan diferentes sintaxis y semántica se puedan comunicar. Esta capa transforma los datos en la información que requiere la aplicación.

Capa de aplicación: Es la capa más cercana al usuario. Es la aplicación con la que el usuario interactúa, como lo es por ejemplo un browser web, un gestor de descargas o un sistema de mensajería instantánea. Es la última capa del modelo OSI y es la que genera la información que se envía por la red, así mismo como es quien usa esta información. Existen varios protocolos para esta capa, como lo son el HTTP, FTP y RSS.

2.4. MODELO TCP/IP

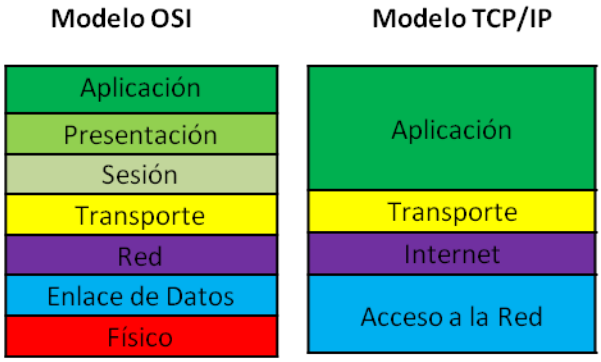
A diferencia del modelo OSI, el modelo TCP/IP es una arquitectura que si tiene una implementación y unos protocolos definidos. Su nombre se da por los dos protocolos más importantes que hacen parte de su arquitectura: TCP (*Transmission Control Protocol* – Protocolo de Control de Transmisión) e IP (*Internet Protocol* – Protocolo de Internet). Fue

inventado en 1970 por DARPA (*Defense Advanced Research Projects Agency* – Agencia de Investigación de Proyectos Avanzados de Defensa, agencia del departamento de defensa de los Estados Unidos encargada del desarrollo de nuevas tecnologías para uso militar) mediante la creación de ARPANET (*Advanced Research Projects Agency Network* – Red de la Agencia de Investigación de Proyectos Avanzados), una red creada para interconectar universidades y centros de investigación de los Estados Unidos. Fue la primera red de conmutación de paquetes creada, cuyo objetivo era interconectar múltiples redes de una manera confiable. Hoy en día el modelo TCP/IP es la base de la gran mayoría de redes en el mundo, incluyendo la Internet.

Una de las razones principales por la cual TCP/IP se convirtió en el estándar mundial de redes, se debe a que provee sus servicios independiente de la conexión que se utilice, es decir, no importa que tecnología se esté usando, ya que TCP/IP funciona sobre todas estas tecnologías.

El modelo se divide en 4 capas, entre las cuales se distribuyen los servicios de las capas que presenta el modelo de referencia OSI. Se puede hacer la equivalencia entre ambos protocolos así:

Figura 3: Comparación modelo OSI - TCP/IP



Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

Las tareas de las capas de aplicación, presentación y sesión del modelo OSI se ejecutan en la capa de aplicación del modelo TCP/IP. Las capas de transporte y red de OSI se corresponden con las capas de transporte e internet de TCP/IP respectivamente. Las tareas de enlace de datos y de nivel físico del modelo OSI se ejecutan en la capa de acceso a la red del modelo TCP/IP. Las capas del modelo TCP/IP se explican a continuación.

Capa de acceso a la red: Esta capa es la encargada de poner los paquetes TCP/IP en el medio de la red y de recibir los paquetes TCP/IP del medio de la red. Dado que estos

protocolos fueron diseñados para funcionar sobre cualquier tecnología, no importa que protocolos, codificación o medios de transmisión se usen en este nivel. Dado que en esta capa se cumplen las mismas tareas que en los niveles físico y enlace de datos del modelo OSI, y en el conjunto TCP/IP puede funcionar cualquier protocolo o tecnología en este nivel, no se explicará más a fondo esta capa.

Capa de internet: Corresponde con las tareas del nivel de red del modelo OSI. Su principal objetivo, es inyectar los paquetes en la red para que estos puedan ser enviados a las redes destino. A este proceso de envío de paquetes de la red de origen a la red de destino, se le conoce como enrutamiento, el cual hace parte de esta capa. Además, esta capa es responsable del empaquetamiento de datos y del direccionamiento de los hosts.

Para realizar estas tareas, la capa se vale del protocolo de internet IP (*Internet Protocol* por sus siglas en inglés), uno de los dos principales protocolos de este modelo. Además, existen a este nivel otros protocolos como ARP, RARP, ICMP, RIP etc. Algunos de estos se explican a continuación, pero nos centraremos más en el protocolo IP. Los protocolos de enrutamiento se explicarán mejor en la sección de enrutamiento, más adelante en este documento:

- ARP (*Address Resolution Protocol* – Protocolo de Resolución de Direcciones): Es el protocolo responsable de la conversión de direcciones IP a las direcciones MAC de la interface de red.
- RARP (*Reverse Address Resolution Protocol* – Protocolo Inverso de Resolución de Direcciones): Realiza la tarea opuesta del protocolo ARP, convierte las direcciones físicas MAC en direcciones IP.
- ICMP (*Internet Control Message Protocol* – Protocolo de Mensajes de Control de Internet): Este protocolo proporciona mensajes de diagnóstico y reporte de errores referente a la entrega de los paquetes IP.
- RIP (*Routing Information Protocol* – Protocolo de Información de Enrutamiento): Protocolo que utilizan los enrutadores () para realizar la tarea de enrutamiento de paquetes entre redes, intercambiando información con otros enrutadores.
- OSPF (*Open Shortest Path First* – Abrir Primero el Camino más Corto): Protocolo de enrutamiento alternativo a RIP, el cual no se basa en número de saltos, sino asociando un costo a cada ruta.

El protocolo IP (v4): Es el protocolo principal de la capa de internet del modelo TCP/IP. Se encarga de enrutar los paquetes del host de origen al host de destino utilizando únicamente la dirección IP. Es el protocolo principal de la Internet, y actualmente todos los hosts que se conectan a la red tienen cada uno una dirección IP. Las características principales de este protocolo son:

- Es no orientado a la conexión, lo que quiere decir que no establece comunicación punto a punto para garantizar la entrega de paquetes, por lo que pueden ocurrir pérdidas de los mismos.
- Su función principal es la entrega de paquetes.
- Realiza fragmentación cuando es necesario.
- Se encarga del direccionamiento IP. Actualmente se usa IPv4 que son direcciones de 32 bits, divididas en 8 octetos. Se representa mediante decimales con puntos para separar los octetos.

Las direcciones IP se utilizan para identificar los hosts en una red. Actualmente la gran mayoría de los hosts que se conectan a la Internet tienen asignada una dirección IP.

Capa de transporte: Corresponde con las tareas de la capa de transporte del modelo OSI. Su tarea es que los hosts establezcan una comunicación para el intercambio de mensajes enviados por la capa de aplicación. Esta encargada de ofrecer una conexión de extremo a extremo y mantenerla hasta el final de la conversación. En esta capa hay dos protocolos principales, TCP (*Transmission Control Protocol* – Protocolo de Control de Transmisión) y UDP (*User Datagram Protocol* – Protocolo de Datagramas de Usuario).

Protocolo TCP: Es un protocolo orientado a la conexión, lo que quiere decir que es un mecanismo de comunicación confiable ya que crea una conexión entre hosts y mantiene esta comunicación hasta el final, mediante el uso de mensajes de control que le permiten saber el estado de la comunicación, cuando se entregaron paquetes, cuando llegaron bien y cuando llegaron con errores. Mediante este control, es posible reenviar paquetes perdidos o dañados durante la transmisión. También realiza un control de flujo para que los emisores rápidos no saturen los receptores lentos con demasiados mensajes. Entre algunas de sus características se encuentran:

- Crea una conexión lógica llamada circuito virtual para garantizar la entrega de mensajes.
- Permite conexiones full dúplex.
- No trabaja con broadcast ni multicast.
- En sus puntos extremos utiliza dirección y puerto, lo que permite tener varias conexiones TCP abiertas al mismo tiempo.
- Realiza control de flujo mediante ventanas deslizantes: Protocolo que controla el tamaño de mensajes enviados al receptor de manera que este no se sature con más mensajes de los que puede recibir.
- Utiliza números de secuencia para transmitir los datos de extremo a extremo de manera ordenada.
- Utiliza un direccionamiento de la siguiente manera: Dirección de puerto de 16 bits, socket que es dirección IP y dirección de puerto.

Protocolo UDP: Es un protocolo no orientado a la conexión, lo que quiere decir que no garantiza la entrega de mensajes al no mantener una comunicación entre hosts. A diferencia del protocolo TCP, el protocolo UDP no realiza ningún control sobre los mensajes que envía, por lo que se pueden duplicar, perder o llegar sin orden. Es problema de la aplicación realizar este control. El hecho que no realice tantos controles como TCP, hace que este protocolo sea óptimo para aplicaciones de tiempo real, como transmisión de video o voz (telefonía IP).

Capa de aplicación: La capa de aplicación corresponde a las capas de sesión, presentación y aplicación del modelo OSI. Cumple las mismas funciones definidas en éste modelo.

2.5. DIRECCIONAMIENTO IP

El direccionamiento IP es parte primordial dentro de un diseño de red ya que, como hemos dicho antes, el protocolo IP es el protocolo principal de la capa de internet del modelo TCP/IP, dado que es el que permite que los paquetes sean entregados a su destino mediante enrutamiento por direcciones IP.

Una dirección IP (versión 4) es un conjunto de 32 bits divididos en 4 octetos, cuya función es identificar un host dentro de una red de computadoras que use el protocolo de internet (IP) para comunicarse. Los 4 octetos se separan mutuamente por puntos, y cada octeto se escribe en formato decimal para una manera más fácil de ser leído e interpretado. Mundialmente, todo equipo que se conecte a la red de Internet, debe tener asignada una dirección IP que lo identifique, y de esta manera pueda enviar y recibir tráfico a las demás redes.

Un ejemplo de dirección IP es el siguiente:

10000000 00001010 00000010 00011110, en notación decimal se escribiría: 128.10.2.30

Las direcciones IP se componen de dos partes: Identificador de Red e Identificador de Host. El identificador de red, como su nombre lo indica, identifica la red de la cual hace parte el host. El identificador de host identifica el host dentro de esa red.

Las direcciones IP se clasifican en clases de acuerdo a los bits más significativos de la dirección. Son 5 clases, las primeras 3 se utilizan para direccionamiento individual (una dirección por host), otra para direccionamiento multicast y otra son direcciones reservadas:

Tabla 1. Rango de direcciones IP por clase.

Clase	Dirección más baja	Dirección más alta
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.0.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Las direcciones clase A utilizan el primer octeto para definir la dirección de red, y los otros 3 octetos para definir el host. Por lo tanto, las direcciones clase A tienen pocas redes (2^7=128) y muchos hosts (2^{24}=16, 777,216).

Las direcciones clase B utilizan los dos primeros octetos para definir la dirección de red, y los otros 2 octetos para definir el host. Por lo tanto, las direcciones clase B tienen más o menos redes (2^{14}=16,384) y más o menos hosts (2^{16}=65,536)

Las direcciones clase C utilizan los 3 primeros octetos para definir la dirección de red, y el octeto restante para definir el host. Por lo tanto, las direcciones clase C tienen muchas redes (2^{21}=2, 097,152) y muy pocos hosts (2^8=256).

Las direcciones clase D, se utilizan para direccionamiento multicast y las direcciones clase E están reservadas para investigación y pruebas.

Existen algunas direcciones especiales dentro del direccionamiento IP:

- Las direcciones IP cuyos bits de host se encuentran en 0, se usan para referirse a la red misma.
- Las direcciones IP cuyos bits de host se encuentran en 1, son direcciones broadcast, y se utilizan para enviar información a todos los hosts de la red.
- La dirección 127.0.0.0 es una dirección de *loopback*, y se utiliza para realizar pruebas locales de aplicaciones TCP/IP, y para comunicación de procesos internos de la máquina.

Subred y máscara de subred: Las subredes se utilizan para poder identificar redes dentro de las redes, es decir, con las redes definidas en las clases de direcciones IP no es suficiente, dado que con una sola dirección de red sólo se puede cubrir una dirección física de red, por lo que se hace necesario definir redes dentro de estas redes, ya que, por ejemplo, las empresas pueden tener muchas redes distribuidas, por lo que se hace necesario que tengan más de una dirección física de red.

Por este motivo se creó el concepto de subred y máscara de subred, con el objetivo de crear el siguiente esquema: RED-SUBRED-SUBRED…HOST. La máscara de subred, es

una “dirección IP” que identifica la parte de subred de una dirección IP. Se caracteriza por tener los bits más significativos en 1’s, en las posiciones que determinan cuáles de los bits de la dirección IP que acompañan identifican la subred a la que pertenecen. De esta manera, las máscaras por defecto para las direcciones clase A, B, y C son:

A: 11111111.00000000.00000000.00000000 = 255.0.0.0
B: 11111111.11111111.00000000.00000000 = 255.255.0.0
C: 11111111.11111111.11111111.00000000 = 255.255.255.0

Las máscaras de subred se asignan de acuerdo a cuántos hosts se quieran tener dentro de la misma red, de manera que no se desperdicien direcciones IP asignando direcciones de red con mucha más capacidad de hosts de la requerida.

2.6. ENRUTAMIENTO

El enrutamiento es el proceso mediante el cual se seleccionan los caminos para enviar los paquetes IP a través de una red. Se lleva a cabo tanto en redes de datos como en redes telefónicas. En las redes electrónicas de datos se utiliza un proceso llamado conmutación de paquetes, que consiste en la agrupación de los datos transmitidos en bloques más pequeños llamados paquetes, y los envía por la red basado en ciertas reglas para la optimización del envío. El enrutamiento se basa en el protocolo IP.

Existen dos tipos de enrutamiento: estático y dinámico. En el enrutamiento estático, se especifica dentro del *router* una tabla de enrutamiento, en la que se especifica que hacer con los paquetes cuando éstos pasan por el equipo. Éste tipo de direccionamiento es poco usado, ya que se deben que tener en cuenta todas las posibles redes desde y hacia las que se generen tráfico, de manera que no se pierdan paquetes. En el enrutamiento dinámico, las tablas de enrutamiento se actualizan automáticamente a través de protocolos.

Existen varios protocolos de enrutamiento que se basan en reglas como costo y/o vector distancia, de manera que el enrutamiento se realice lo más eficiente posible. Los protocolos de enrutamiento más usados son:

- RIP (*Routing Information Protocol* - Protocolo de Información de Enrutamiento): Es un protocolo que funciona mediante vector distancia, calculando los saltos que debe dar para enviar el paquete a su destino. El máximo de saltos que permite es 15. Funciona mediante el envío de actualizaciones de los que se encuentran conectados y configurados en RIP, de manera que cada *router* envía la información a los demás de

las redes que conoce y a las que puede llegar, propagándose así toda la información de enrutamiento entre todos los.

- OSPF (*Open Shortest Path First*): Es un protocolo que funciona mediante el cálculo de la ruta más corta posible, basado en un "costo" de envío de paquete por esa ruta. El protocolo realiza un mapa de la topología de red y, basado en esta topología, crea la tabla de enrutamiento para tomar decisiones en base únicamente a la dirección IP. El "costo" es determinado por políticas como estado de un enlace, distancia entre un *router* y otro, disponibilidad y confiabilidad de un enlace. Es un protocolo que funciona únicamente para sistemas autónomos.
- BGP (*Border Gateway Protocol* - Protocolo de Borde de Puerta): Es un protocolo diseñado para enrutamiento entre sistemas autónomos, por lo tanto, es el protocolo usado para el enrutamiento en internet. Se basa en el intercambio de información de enrutamiento entre los de borde de los sistemas autónomos.

2.7. ETHERNET

Es una tecnología para redes LAN, actualmente la más difundida y usada en todo el mundo dada su versatilidad y velocidad (que actualmente en hogares, alcanza 1 Gbps). Está especificada en el grupo de estándares IEEE 802.3, el cual contiene todos los estándares que definen y modifican la tecnología Ethernet.

La tecnología Ethernet se caracteriza por funcionar sobre cualquier medio (fibra, cable coaxial, par trenzado), aunque en la actualidad su medio de transmisión más usado es sobre cobre par trenzado, conocido como UTP. Los estándares más conocidos son:

- 10BASE-T: Alcanza velocidades de hasta 10 Mbps sobre par trenzado. También puede ser implementado sobre cable coaxial y fibra óptica.
- 100BASE-T: También conocido como *Fast Ethernet,* alcanza velocidades de hasta 100 Mbps sobre par trenzado y fibra óptica. Es actualmente el más usado, aunque está siendo reemplazado por 1000BASE-T.
- 1000BASE-T: Conocido como *Gigabit Ethernet*, alcanza velocidades de hasta 1 Gbps sobre par trenzado. Es el estándar que actualmente se está extendiendo en el mercado.
- 10GBASE-T: Conocido como *10 Gigabit Ethernet*, alcanza velocidades de hasta 10 Gbps sobre par trenzado, en longitudes de cable de hasta 100 metros.

2.8. INTERNET

Es un conjunto descentralizado de redes de computadores globalmente interconectadas, que se basa en el modelo TCP/IP para su funcionamiento. Actualmente sirve a billones de personas en todo el mundo, las cuales hacen parte de redes privadas, públicas, académicas, de negocios y gubernamentales, comunicadas a través de una compleja red de conexiones electrónicas, ópticas e inalámbricas. En ella se ofrecen múltiples servicios, desde documentos hasta multimedia, entre los que se encuentran:

- World Wide Web.
- Correo Electrónico.
- Telefonía
- Televisión.
- Películas por demanda.
- Noticias.
- Compras.
- Mensajería Instantánea.

Comenzó como una red impulsada por el departamento de defensa de los Estados Unidos para comunicar Universidades y centros de investigación del país, pero rápidamente fue creciendo a medida que nuevas universidades y empresas se fueron uniendo a la red, para compartir información. Actualmente, el gobierno de internet es descentralizado y se encuentra difundido por todo el mundo, salvo dos entidades que se encargan de administrar dos aspectos claves del funcionamiento de la red: El espacio de direccionamiento IP y el sistema de nombres de dominio DNS, ambos controlados por la ICANN (*Internet Corporation for Assigned Names and Numbers* - Corporación de Internet para Nombres y Números Asignados). Actualmente el número de usuarios de internet supera los 2 billones[1] en todo el mundo.

2.9. CORREO ELECTRÓNICO (*E-MAIL*)

El servicio de correo electrónico es un método para intercambiar mensajes digitales, generados desde un remitente hacia uno más destinatarios. Su nombre de "correo" viene del sistema de correo físico estándar, en el cual está basado éste servicio de correo

[1] Internet World Stats. MINIWATTS MARKETING GROUP. All Rights Reserved Worldwide. [Online] URL: http://www.internetworldstats.com/stats.htm

electrónico. Así, un mensaje de correo electrónico se compone principalmente de 3 elementos:

2.10. CABLEADO ESTRUCTURADO

Son un conjunto de normas y estándares que existen para los sistemas de cableado en campus y edificios. Se compone de elementos más pequeños llamados subsistemas, los cuales cada uno tiene sus normas y reglamentaciones para que el cableado pueda cumplir con las exigencias requeridas. Típicamente, el cableado estructurado se compone de:

- Punto de demarcación: El punto a donde llegan los servicios al cliente, típicamente datos mediante internet, y voz, la cual puede ser también sobre internet (telefonía IP) o sobre la red de telefonía convencional.
- Cuarto de telecomunicaciones: El cuarto donde se guardan todos los equipos que brindan servicios a la red, tanto de conectividad como de aplicaciones. Pueden ser *switchs, gateways,* servidores, etc.
- Cableado vertical: Es el cableado que conecta los diferentes cuartos de telecomunicaciones en un campus o edificio.
- Cableado horizontal: Es el cableado que se extiende desde los cuartos de telecomunicaciones hasta los puntos de trabajo, típicamente a través de canaletas, cielo falsos, tuberías y/o ventilas de aire.
- Componentes de área de trabajo: Se compone de los elementos que conectan las estaciones de trabajo con el cableado horizontal, como *faceplates* y *jacks.*

Existen varias normas internacionales para el cableado estructurado. La norma más común es la que rige el cableado estructurado para edificios comerciales, la TIA/EIA-568-B.

2.11. REDES INALÁMBRICAS Y WI FI(802.11)

Las redes inalámbricas son redes en las cuales un usuario móvil se puede conectar a la red a través de un enlace inalámbrico de radio. El grupo de estándares 802.11 de la IEEE definen todos los aspectos que contiene una red inalámbrica. Actualmente es el competidor directo de Ethernet, ya que no necesita cableado y puede alcanzar velocidades mayores a las de Fast Ethernet. Además, con el aumento en el uso de equipos portátiles como *tablets, laptops* y *smartphones* que hacen uso de esta tecnología, se ha aumentado el uso de redes inalámbricas en todo el mundo.
El estándar más reciente, 802.11n, especifica entre otras, las siguientes características:

- Mejora la velocidad de transferencia, hasta 600 Mbps
- Permite el uso de antenas múltiples de entrada y salida.
- Puede operar en la banda de los 5 GHz

Existe una alianza llamada" *Wi-Fi Alliance*" (*Wide Fidelity* - Amplia Fidelidad), dueña del logo "*Wi-Fi Certified*", que se encarga de la certificación de los dispositivos inalámbricos. Actualmente, se mal utiliza el término "*Wi-Fi*" para referirse a la presencia de redes inalámbricas en algún lugar, sin saber que Wi-Fi se refiere a la certificación que se le realiza a los dispositivos. Todos los fabricantes que desean que sus dispositivos tengan el logo "*Wi-Fi Certified*", deben someterlos a pruebas rigurosas con altos estándares, tanto en transmisión de datos como en seguridad y calidad de servicio. Ésta certificación garantiza interoperabilidad entre todos los dispositivos que la poseen.

2.12. VPN (*VIRTUAL PRIVATE NETWORK*)

Consiste en una red privada que hace uso de la salida a internet para proveer, a alguna sede o usuario, de acceso seguro a dicha red. Por lo general usa sistemas de autenticación de usuarios y encriptación tanto de la comunicación establecida como del origen y destino de los datos, los protocolos más usados para la encriptación de los túneles VPN son:

IPSec (*Internet Protocol Security* – Protocolo de seguridad en Internet): Protocolo de internet usado en IPv4 como protocolo de seguridad capa 2 en el modelo TCP/IP cuyo diseño cumple con las características de seguridad de integridad, confidencialidad y autenticación. Funciona enmarcando un paquete IP dentro de otro paquete y encriptando su origen.

SSL/TLS (*Secure Sockets Layer* / *Transport Layer Security* – Capa de Protección Segura / Seguridad de Capa de Transporte): Protocolo que permite brindar seguridad a una conexión completa, puede funcionar en ambientes donde el protocolo IPSec puede presentar problemas con *firewalls* o traducciones de direcciones de red. Usa métodos de encriptación asimétrica, o sea que el método usado para cifrar no es el mismo que el usado para descifrar.

VPN Sitio a Sitio (*Site to Site*): Es una VPN que se establece entre dos IP fijas específicas, utilizada para brindar conexión permanente entre dos sitios, sin necesidad de establecer la conexión cada vez que se requiera.

VPN Móviles (también llamadas *Client-to-Site* – Cliente-a-Sitio): A diferencia de las *Site-to-site* – Sitio-a-Sitio, consisten en una conexión VPN que no se establece a una IP fija específica, lo cual le permite la libertad de cambios de redes al usuario.

2.13. VLAN

Una VLAN (*Virtual Local Area Network* - Red de Área Local Virtual) es una separación de dominios de *broadcast* en una misma red física. Mediante el uso de VLAN se pueden crear redes locales lógicas dentro de una red local física, con el objetivo de agrupar estaciones de trabajo sin la necesidad de estar físicamente conectados a un mismo concentrador. Los VLAN tienen las siguientes ventajas:

- Segmentación lógica, permitiendo movilidad de hosts entre segmentos físicos sin perder la conectividad a su segmento lógico.
- Creación de diferentes esquemas de direccionamiento en un mismo segmento físico, de manera que se puedan ocultar unos hosts de otros sin necesidad de moverlos de lugar.
- Ofrecimiento de servicios diferenciados a hosts conectados a la misma red física.

3. ESTADO ACTUAL DE LA RED

Este capítulo abarca todo el estudio previo realizado a la red actual de la compañía, necesario para poder determinar las necesidades reales de la misma. Inicialmente se hizo una visita a los restaurantes ubicados en la ciudad de Medellín, para revisar su estado en cuanto a equipos y conexiones. Dado que son los más antiguos en la cadena de restaurantes que maneja la compañía, su arquitectura e infraestructura de red son las más deficientes dado el poco o nulo diseño que se hizo de las mismas, debido a que la empresa no contaba con personal especializado en sistemas que la asesorara en éstos temas. Ésta situación causa que elementos como la organización de cableado y de equipos en los racks se conviertan en un gran inconveniente a la hora de solucionar problemas de conectividad en la red, sin mencionar los problemas que se pueden presentar en un futuro cuando los equipos empiecen a fallar o el cableado se empiece a deteriorar, no sólo por su uso, sino también por el pobre cuidado que se tiene de éstos elementos.

Así mismo, se solicitó a los empleados de los restaurantes ubicados en las otras ciudades que enviaran registros fotográficos del estado de los racks, y un inventario de equipos tanto de red como estaciones de trabajo y demás tipos de equipos que se conectan a la red, como datáfonos y *KDS*. En estos restaurantes, la desorganización de los equipos de red no es tan crítica como en las primeras aperturas de puntos de venta de la compañía.

3.1. INFRAESTRUCTURA

En todos los restaurantes de la compañía, existe una gran heterogeneidad de equipos dispuestos en toda la red, pues cuentan con diferentes marcas y modelos, que se han ido adquiriendo a medida que se abren los restaurantes y, dado que no se ha tenido una planeación, se adquiere cualquier equipo que permita conectividad dentro de la sede sin pensar en las necesidades de conectividad con la oficina principal ubicada en Medellín. Básicamente, al abrir un nuevo restaurante se piensa en tener un *switch* que comunique los equipos dentro de la red, y un pequeño *router* que se conecte con los equipos del proveedor de servicio y dé salida a internet al computador de gerencia. En ningún restaurante ni tampoco en la sede principal, hay *firewalls* que protegen de ataques externos, o que permitan una conexión segura a internet. En general, la gran mayoría de equipos de red que se tienen son básicos, y no le proveen a la compañía los niveles de seguridad y confiabilidad que necesita para la operación de su negocio. A continuación, se especifica el estado de la infraestructura en las sedes. Se omiten marcas en los equipos ya que no es necesario especificarlas, simplemente se especifica el tipo de

equipo con el que se cuenta, haciendo énfasis en el número de puertos en los *switchs* y en los servicios de los *routers*.

3.1.1. Restaurante 1

Es uno de los restaurantes más desordenados de todos. Tiene *switchs pequeños* conectados en cascada, cableado sin ordenadores, enmendaduras en el rack y, en general, todo se encuentra ubicado caóticamente adentro de éste. El cableado no tiene etiquetas, por lo que es muy difícil revisar conexiones cuando se presenta algún inconveniente. Todos éstos elementos ponen en riesgo la integridad de la infraestructura de red, ya que por estar ubicados de la manera en que lo están y el tipo de equipos que se usan, la red puede colapsar en cualquier momento y su arreglo puede ser muy costoso y traumático para las operaciones de venta del restaurante, ya que encontrar la causa del problema y solucionarlo puede tomar mucho tiempo. Los equipos de red que se tienen actualmente en éste restaurante son:

- Un *switch* de 6 puertos 10/100 Ethernet pequeño, no administrable, para hogares.
- Dos *switchs* de 8 puertos 10/100 Ethernet pequeños, no administrables, para hogares.
- Un *patch panel* de 19 puertos.
- Un *router* con soporte para VPN y firewall pequeño 10/100 Ethernet, para hogares.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el siguiente:

- Los *switchs* se encuentran conectados en cascada. La razón de esta conexión, es que al principio se adquirió un *switch* pequeño para los equipos iniciales. A medida que se fueron adicionando equipos a la red, se hicieron necesarios más puertos para conectarlos, por lo que se adquirieron nuevos *switchs* pequeños para suplir esta necesidad.
- Las conexiones entre los equipos se encuentran desorganizadas. El cableado se encuentra enredado, ya que los equipos se conectaron y se guardaron en el rack sin orden alguno. No se usa un organizador de cableado.
- Dado que los equipos son pequeños, no hay manera de unirlos al rack para que estén un poco más organizados, por lo que todo dentro de éste se encuentra convertido en una especie de "nido" de cableado, con todos los equipos en el interior y por esta razón, es muy difícil identificar conexiones y equipos, ya que muchos de éstos no son fácilmente visibles.
- El cableado que va desde el rack y se distribuye por todo el restaurante no está debidamente marcado, ni en el *patch panel,* ni en los *faceplates.* Esto imposibilita una eficiente solución de problemas de conectividad de red.

- El cableado que llega hasta los KDS que se encuentran encima de las pantallas de cocina se encuentra muy desorganizado y enredado. Es la misma situación que se presenta en el rack.
- El rack no es lo suficientemente grande para alojar los equipos necesarios y tener óptimas condiciones de ventilación.

Figura 4. Foto de Rack Restaurante 1

Fuente: de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.1.2. Restaurante 2

Al igual que Restaurante 1, se encuentra en un alto estado de desorden. Tiene todos los mismos problemas de éste restaurante: conexiones en cascada, desorden en el cableado, falta de espacio, etc. Los equipos de red que se tienen actualmente en este restaurante son:

- Dos *switchs* de 8 puertos 10/100 Ethernet pequeños, no administrables, para hogares.
- Un *router* con soporte VPN y firewall pequeño 10/100 Ethernet, para hogares.
- Un *patch panel* de 24 puertos.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el mismo que el de Restaurante 1. Tiene un problema más, y es que el rack tiene un pequeño orificio en la parte inferior por la que ingresan cables de red y de energía. Un problema no solamente estético sino también funcional, dado que no sólo los cables no se encuentran organizados como deberían, sino que el orificio que tiene el rack tiene cortes afilados que deterioran los mismos.

Figura 5. Foto de Rack Restaurante 2

Fuente: de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.1.3. Restaurante 3

Este restaurante no tiene tantos problemas como los dos restaurantes arriba explicados. Su rack esta mejor organizado y, por ser más espacioso, no tiene los problemas de aglomeración de equipos y cableado que tienen los otros restaurantes. Los equipos de red que se tienen actualmente en este restaurante son:

- Un *switch* de 8 puertos 10/100 Ethernet pequeño, no administrable, para hogares.

- Un *switch* de 16 puertos 10/100 Ethernet mediano, no administrable, para Pymes.
- Un *router* pequeño 10/100 Ethernet, para hogares.
- Un *patch panel* de 24 puertos.
- Un organizador de cableado.
- Un *multiservice gateway* propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el siguiente:

- Se tienen dos *switchs* para conectar los equipos a la red. Sin embargo, aun no es claro por qué se tienen ambos, ya que sólo con el *switch* de 16 puertos se puede fácilmente suplir la necesidad de los equipos que se tienen.
- Las conexiones entre los equipos se encuentran un poco más organizadas que en los restaurantes antes mencionados. Se utiliza el organizador de cable para cumplir ésta función. Aún así, los cables no se encuentran completamente organizados ya que los excesos de éstos se encuentran desplegados en todo el rack, pero es más fácil solucionar problemas de conectividad aquí que en otros restaurantes.
- El cableado se encuentra sin marcar, tanto en el rack como en los *faceplates* y algunos *patch cords* tienen sus conectores quebrados, por lo cual se desconectan fácilmente.
- Los equipos son muy pequeños para asegurarlos al rack, por lo que es difícil ordenarlos dentro del mismo, lo que dificulta encontrar conexiones entre los equipos.
- Es desorganizado y enredado el cableado que llega hasta los KDS que se encuentran encima de las pantallas de cocina.

Figura 6. Foto de Rack Restaurante 3

Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.1.4. Restaurante 4

Es el restaurante más organizado de todos los de Medellín. Es el modelo de organización de infraestructura mínimo al que se desea llegar, con cableado y equipos ordenados. La razón por la que este restaurante se encuentra en tan buen estado, es porque la empresa ya contaba con una persona encargada de sistemas la cual diseñó un cuarto de telecomunicaciones apropiado, con un rack, equipos y cableado apropiado. Los equipos de red que se tienen actualmente en este restaurante son:

- Un *switch* de 48 puertos 10/100 Ethernet, administrable, para Pymes.
- Un *router* con soporte VPN y firewall pequeño 10/100 Ethernet, para hogares.
- Un Access *point*.
- Un *patch panel* de 48 puertos.
- Un organizador de cableado.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

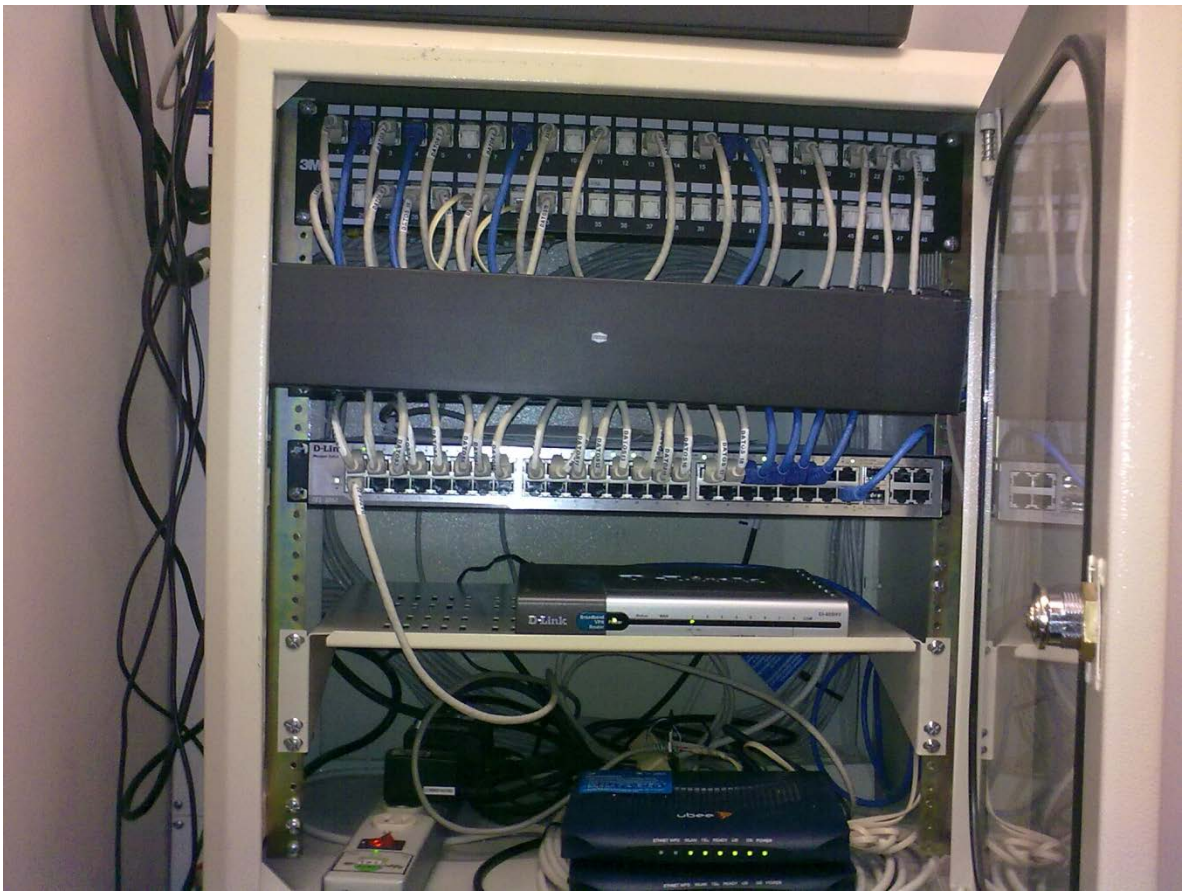
El estado de la infraestructura es el siguiente:

- Todas las conexiones se encuentran perfectamente organizadas y marcadas. Se utiliza el organizador de cables y etiquetas para este fin. Las etiquetas diferencian las

diferentes conexiones en el *switch, patch panel* y *faceplate.* Gracias a estas etiquetas, se pueden solucionar problemas de conectividad fácilmente.

- Los equipos se encuentran perfectamente organizados dentro del rack. El *switch* es del tamaño estándar para poder fijarlo a este. Aunque el *router* y los equipos del ISP no pueden ser fijados al rack, se encuentran debidamente ubicados y organizados dentro del mismo.
- Los excesos de cable se encuentran organizados en la parte trasera del rack.
- Se tiene un *Access point* mediante el cual se ofrece internet inalámbrico gratis a los clientes. Sin embargo, no cuenta con restricciones de ningún tipo y se encuentra directamente conectado a la red sin separación física o virtual, tampoco hay seguridad como un *firewall* que controle el tráfico. Es una gran brecha de seguridad.
- Todos los equipos de red se encuentran ubicados en un cuarto de telecomunicaciones, destinado únicamente para éste propósito. El cuarto cuenta con aire acondicionado para mantener los equipos a una temperatura adecuada.

Figura 7. Foto de Rack Restaurante 4



Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.1.5. Restaurante 5

Restaurante ubicado en la ciudad de Cali, su estado es muy similar al de los restaurantes 1 y 2. El tamaño del rack no es suficiente para almacenar todos los equipos, el cableado se encuentra enredado sin organizador y también consta de varios *switchs* pequeños conectados en cascada. Los equipos de red que se tienen actualmente en este restaurante son:

- Tres *switchs* de 8 puertos 10/100 Ethernet pequeños, no administrables, para hogares.
- Un *router* con soporte VPN y firewall pequeño 10/100 Ethernet, para hogares.
- Un *patch panel* de 24 puertos.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el siguiente:

- Se tienen tres switchs conectados en cascada de manera muy desorganizada y se hace extremadamente difícil el monitoreo y la solución de problemas.
- No se cuenta con ningún tipo de seguridad contra las amenazas a las que se expone una red con salida a internet.
- El cableado distribuido por el restaurante no se encuentra debidamente etiquetado y algunos *faceplates* están en mal estado.
- Los equipos están expuestos a temperaturas altas debido al espacio reducido del rack, el polvo acumulado y la temperatura del ambiente, pues el aire acondicionado no tiene un flujo correcto.

3.1.6. Restaurante 6

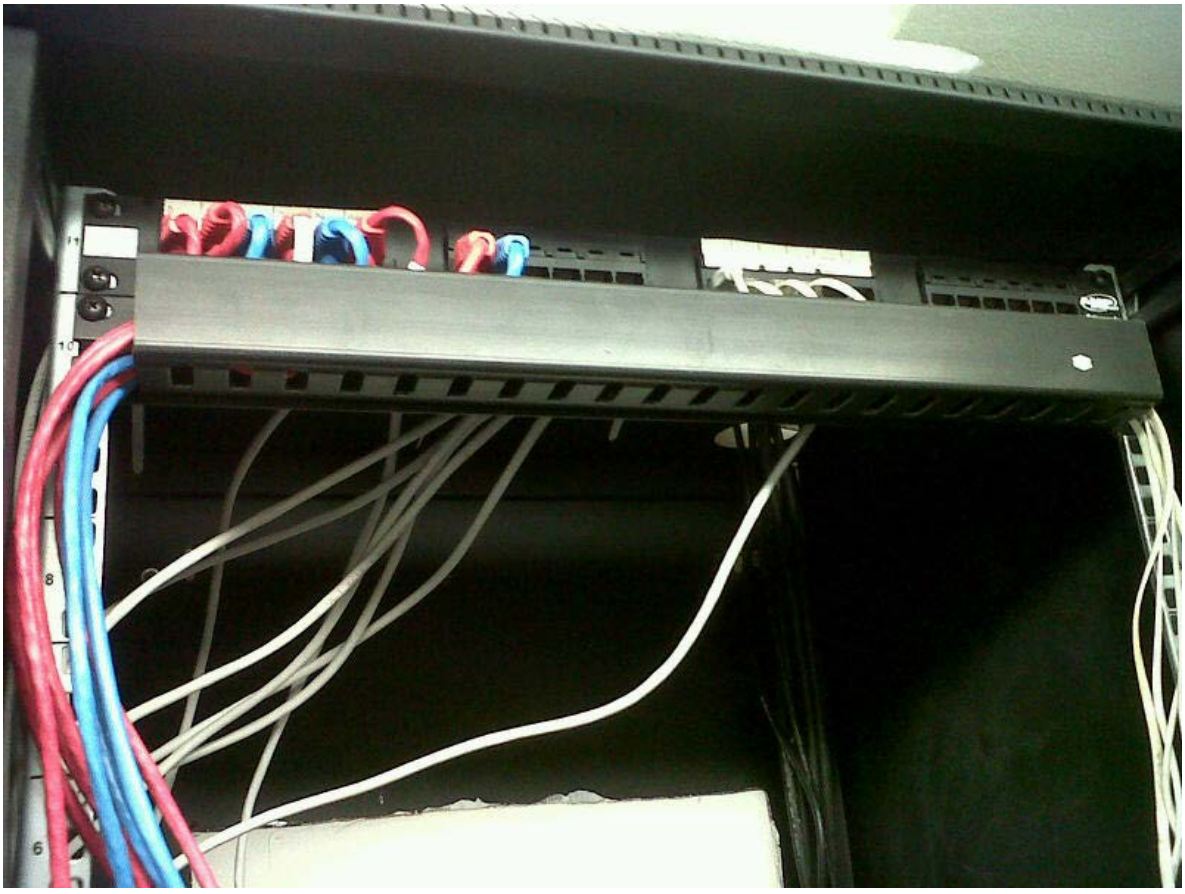
Se encuentra ubicado en la ciudad de Barranquilla, en este caso el rack de telecomunicaciones es sobredimensionado para los equipos que aloja, el *switch* a pesar de ser adecuado para la cantidad de puntos de red necesarios, no se encuentra debidamente fijado a los soportes del rack, se cuenta con un organizador de cableado pero no se usa correctamente, pues no todos los cables pasan por éste y el servicio de internet brindado por el ISP llega directamente al computador gerencial del restaurante. Los equipos de red que se tienen actualmente en este restaurante son:

- Un *switch* de 16 puertos 10/100 Ethernet mediano, no administrable, para Pymes.
- Un *router* pequeño 10/100 Ethernet, para hogares.
- Un *patch panel* de 24 puertos.
- Un organizador de cableado.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el siguiente:

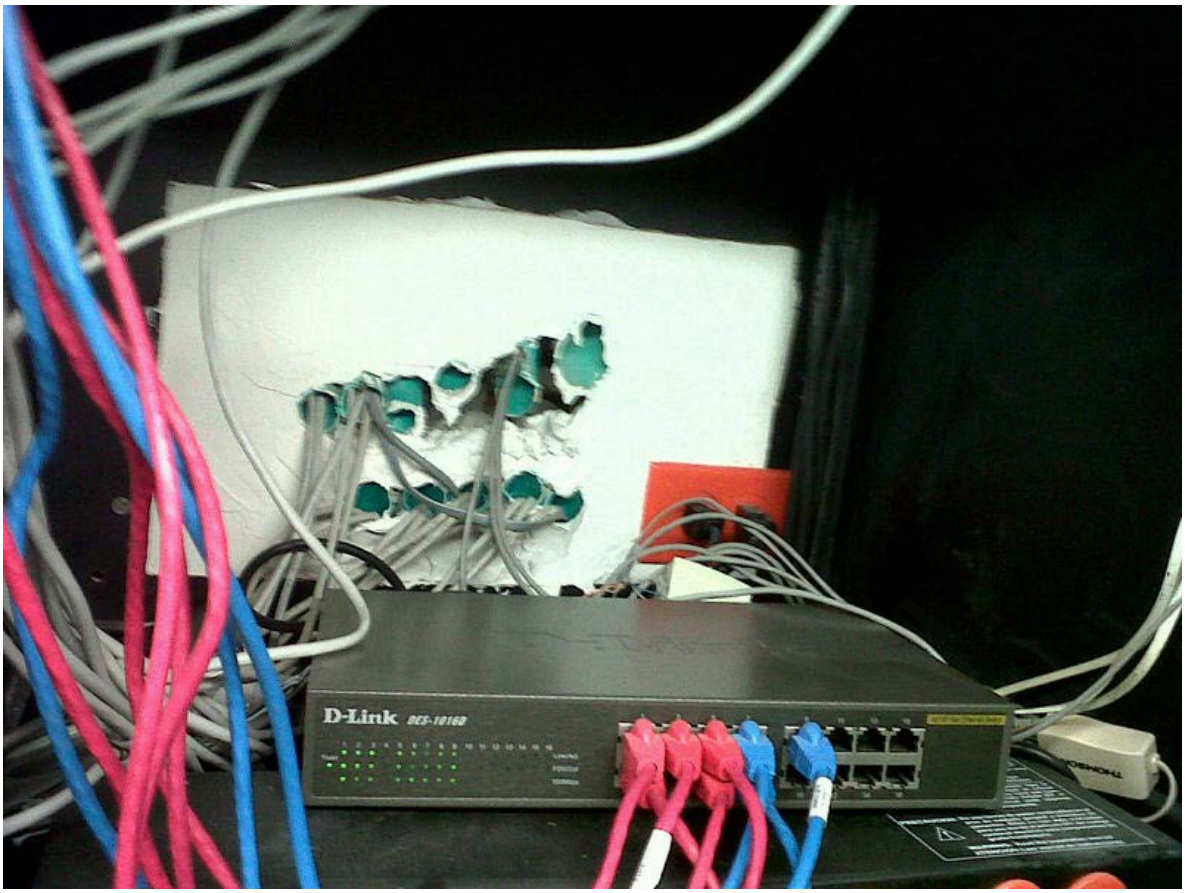
- La red LAN no cuenta con salida a internet, únicamente tiene salida el computador gerencial, el cual cuenta con 2 tarjetas de red para conectarse respectivamente a la red LAN y a internet.
- Un pequeño router para hogares va conectado entre el enlace de internet y el computador gerencial, este router no cuenta con ningún tipo de seguridad.
- Aunque la distribución del cableado se encuentra en buen estado, ni los *faceplates* ni el *patch panel* se están debidamente marcados.

Figura 8. Foto 1 de Rack Restaurante 6



Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

Figura 9. Foto 2 de Rack Restaurante 6



Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.1.7. Restaurante 7

Se encuentra ubicado en la ciudad de Bogotá, cuenta con una red organizada, un cableado debidamente certificado y los equipos necesarios para que la red LAN funcione correctamente. Los equipos de red que se tienen actualmente en este restaurante son:

- Un *switch* de 48 puertos 10/100 Ethernet, administrable, para Pymes.
- Un *router* con soporte VPN, firewall pequeño 10/100 Ethernet y *Access point* integrado, para hogares.
- Dos *patch panel* de 48 puertos, uno para voz y otro para datos.
- Un organizador de cableado.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el siguiente:

- El switch y los Patch Panel son sobredimensionados en la cantidad de puertos para los puntos de red con los que cuenta el restaurante.
- El patch panel para voz es innecesario debido a que solo se cuenta con 1 línea telefónica en el restaurante y no existirá la necesidad de instalar líneas adicionales.
- Por medio del Access point integrado del router, se conectan algunos computadores portátiles del personal gerencial del restaurante, pero también se brinda a los clientes este servicio de manera gratuita sin ninguna restricción ni seguridad, al igual que Restaurante 4.

Figura 10. Foto de Rack Restaurante 7

Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.1.8. Restaurante 8

Es el restaurante más nuevo de la compañía, ubicado en el Centro comercial Gran Estación en la ciudad de Bogotá. Cuenta con un correcto cableado, un rack de tamaño adecuado para los equipos almacenados y con buena ventilación. Los equipos de red que se tienen actualmente en este restaurante son:

- Un *switch* de 24 puertos 10/100 Ethernet, no administrable, para Pymes.

- Un *router* con soporte VPN y firewall pequeño 10/100 Ethernet, para hogares.
- Dos *patch panel* de 24 puertos, uno para voz y otro para datos.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el siguiente:

- No se cuenta con ningún equipo que brinde un adecuado nivel de seguridad de red en el restaurante.
- El switch del restaurante es adecuado para la cantidad de puntos de red con los que este cuenta.
- Todo el cableado se encuentra debidamente ordenado y marcado.
- Por medio del *Access point* integrado del router, se conectan algunos computadores portátiles del personal gerencial del restaurante.
- Al igual que en Restaurante 7, también se considera innecesario el patch panel de voz.

Figura 11. Foto de Rack Restaurante 8

Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.1.9. Oficina Central

Ubicada en la ciudad de Medellín, es el lugar donde se encuentra todo el personal administrativo de la compañía. Su infraestructura de red se encuentra en buen estado, organizada y bien mantenida. Los equipos de red que se tienen actualmente aquí son:

- Un *switch* de 16 puertos 10/100 Ethernet, no administrable, para Pymes.
- Un *router* con soporte VPN, *wireless* y *firewall* pequeño 10/100 Ethernet, para hogares.
- Un *patch panel* de 48 puertos.
- Un organizador de cableado.
- Un *multiservice Gateway*, propiedad del ISP.
- Un equipo empalme de fibra óptica, propiedad del ISP.
- Un equipo para telefonía, propiedad del ISP.

El estado de la infraestructura es el siguiente:

- El *switch* de 16 puertos no soporta el crecimiento de la oficina, actualmente se encuentra lleno y es imposible añadir nuevos puntos de red en la oficina dado que no hay puertos disponibles.
- El cableado se encuentra organizado en el rack y bien distribuido por toda la oficina, pero aun no se encuentra marcado, dificultando esto el monitoreo y la solución de problemas.
- Se brinda servicio de internet inalámbrico dentro de la oficina para los mismos empleados que trabajan con equipos portátiles, de manera que tengan movilidad dentro de la misma.
- La telefonía entra como telefonía IP al equipo del ISP y de allí se distribuye en 6 líneas análogas al PBX.

Figura 12. Foto de Rack Oficina Central

Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

3.2. CONECTIVIDAD

Una de las razones principales para este proyecto es la necesidad de la compañía de mejorar la conectividad de la oficina central con sus restaurantes, de manera que puedan obtener información importante de una manera rápida, fácil y segura. Para esto, se hizo un diagnóstico de como es actualmente ésta conectividad, revisando los siguientes aspectos tanto en los restaurantes como en la oficina central: conexiones existentes, información que se intercambia y servicios que se ofrecen en la red. Fue importante identificar que tan crítico es para la compañía cada uno de éstos aspectos, para así poder hacer un diagnóstico real.

3.2.1. Conexiones Existentes

Tanto la oficina central como los restaurantes se comunican mediante conexión a internet. A pesar de que se tienen *routers* con soporte para VPN en algunas sedes, éstas no están configuradas ya que en la oficina central no se cuenta con un equipo lo suficientemente robusto para soportar todas las conexiones que se necesitan. Todos los restaurantes tienen una conexión a internet de 2 Mbps de *downstream* y 3 Mbps de *upstream*. La oficina central cuenta con una conexión de 4 Mbps de *downstream* y 3 Mbps de *upstream.* A través de internet se obtiene la información financiera de los restaurantes en la oficina central, pero sin una conexión segura que permita el traspaso de información de manera confiable.

3.2.2. Información que se intercambia

Existe cierta información que se requiere en la oficina central para la administración de la compañía. Esta información que proviene de los restaurantes se recopila día a día, y debe ser consultada de manera regular para el correcto funcionamiento de la empresa. La encargada de generar todos estos datos es la aplicación principal del negocio, que se encuentra instalada tanto en la oficina central como en los restaurantes. Para obtener esta información de los restaurantes, actualmente se utiliza una aplicación que corre sobre internet llamada *LogMeIn®,* la cual se comporta como un Escritorio Remoto de Microsoft® que permite tomar control del computador de gerencia del restaurante que se necesita, y generar los reportes para después entregarlos a quien los requiere. Ésta aplicación es usada por el personal de sistemas. Adicionalmente existe una portal llamado MyMicros, que permite consultar gran cantidad de reportes vía web, lo que le facilita la tarea al personal administrativo ya que no requiere de el área de sistemas para obtenerlos.

Aparte de la información que se obtiene de los restaurantes, también existe información que se envía de la oficina central a los restaurantes. Según el modelo de funcionamiento de la aplicación Micros® cada configuración se debe realizar en el servidor principal ubicado en la oficina central, en vez de realizar la misma configuración en cada uno de los restaurantes de manera local. Esta tarea es realizada por el personal de sistemas que se encuentra ubicado en la misma oficina central. Cuando se realiza un cambio, éste es generado en un archivo especial que debe ser distribuido a los equipos de gerencia de todos los restaurantes destinatarios del cambio, para que luego puedan ser aplicados a las estaciones de trabajo. Esta distribución se realiza mediante una aplicación que corre sobre internet llamada *Dropbox*®, la cual permite transferir archivos de un equipo a otro realizando una compartición de carpetas a través de internet. El archivo del cambio es generado, luego es copiado a la carpeta que se comparte para que sea recibido en el restaurante, y posteriormente mediante *LogMeIn*® se accede al computador de gerencia para copiar el archivo de la carpeta compartida a la carpeta de la aplicación central y así, aplicar el cambio a las estaciones de trabajo del restaurante.

Como se pudo observar, este intercambio de información es un poco demorado y puede ser simplificado si se cuenta con los enlaces WAN apropiados que comuniquen los restaurantes con la oficina central.

3.2.3. Servicios que se ofrecen en la red

Este punto fue solamente evaluado en la oficina central, ya que por no tener enlaces WAN los servicios que se ofrecen sobre esta red no se hacen extensibles a los restaurantes, aunque esto es lo que se quiere obtener con el nuevo diseño de red que se plantea en este documento. Los servicios que se ofrecen en la red son servicios de DNS para ingresar al dominio de la red y de Directorio Activo para la autenticación de los usuarios de la oficina central.

4. CONSIDERACIONES PARA EL DISEÑO DE RED

Para realizar el diseño de la red corporativa se tienen en cuenta las necesidades y requerimientos de la compañía, ya que son éstas las que finalmente definirán el diseño de la red. A continuación se explican éstas necesidades y requerimientos.

Se desea contar con enlaces de red entre la oficina y todos los puntos de venta en el país, con los objetivos de:

- Permitir la propagación de los servicios del servidor de la oficina a todos los puntos de venta.
- Brindar acceso a las bases de datos de todos los restaurantes desde la misma oficina central, la aplicación *Ocean* requiere realizar consultas a dichas bases de datos con el fin de obtener la información que requiere el usuario.
- Facilitar el acceso remoto a los restaurantes desde la oficina para funciones de configuración y soporte.

En la oficina central, el enlace a internet es crítico, tanto para las labores administrativas cotidianas como para mantener en funcionamiento las conexiones VPN establecidas con los restaurantes.

Tanto la oficina central como los restaurantes deben contar con cierto nivel de seguridad, pues información como ventas, costos, mercadeo y datos financieros es de carácter confidencial, además las operaciones de venta diarias de los restaurantes se basan de manera esencial en la tecnología y su correcto funcionamiento, lo que hace indispensable mantener bajo control las amenazas de virus, intrusiones y ataques vía Web.

Se pretende brindar servicio de internet inalámbrico a los clientes en los restaurantes, por lo que se hace necesario separar la red corporativa de dicho servicio de internet a clientes.

Se debe considerar la posibilidad de servicio de telefonía IP para su implementación en un futuro.
En cuanto al esquema de direccionamiento:

- Se deben reservar suficientes direcciones de host para la oficina principal, teniendo en cuenta un futuro crecimiento, el cual se espera que llegue a un máximo de 50 usuarios simultáneos.
- Se deben reservar suficientes direcciones de host para cada restaurante, teniendo en cuenta que un restaurante en sí no puede crecer mucho, pero la compañía si crecerá en número de restaurantes.

- Se debe tener un direccionamiento para la red inalámbrica de los clientes diferente al de la red corporativa, el mismo que podría ser utilizado en todos los restaurantes.

En la tabla 1 se muestra la cantidad de puntos de red que debe tener disponible cada una de las sedes de la compañía (oficina y restaurantes).

Tabla 2. Puntos de red por sede

	R1	R2	R3	R4	R6	R7	R8
Workstation POS	3	3	3	5	4	3	3
KDS	2	2	3	3	3	6	6
Servidor	1	1	1	1	1	1	1
Equipo Menú digital	0	1	1	1	1	1	1
Equipo Cámaras de seguridad	1	1	1	1	1	1	1
Access Point	1	1	1	1	1	1	1
Salida Internet	1	1	1	1	1	1	1
Datafonos por internet	3	2	3	5	4	3	3
Teléfono IP(Posibilidad)	1	1	1	1	1	1	1
Total Puntos de red	13	13	15	19	17	18	18

5. DISEÑO DE LA NUEVA RED

Para realizar el diseño, fue necesario separar dos esquemas similares dentro de un gran esquema general, ya que para los restaurantes hay requerimientos diferentes que para la oficina central. Fue importante separar estos dos esquemas tanto para efectos funcionales como para efectos de infraestructura, ya que los equipos que se necesitan para los restaurantes son diferentes a los que se necesitan para la oficina central.

5.1. ESQUEMA DE RED GENERAL

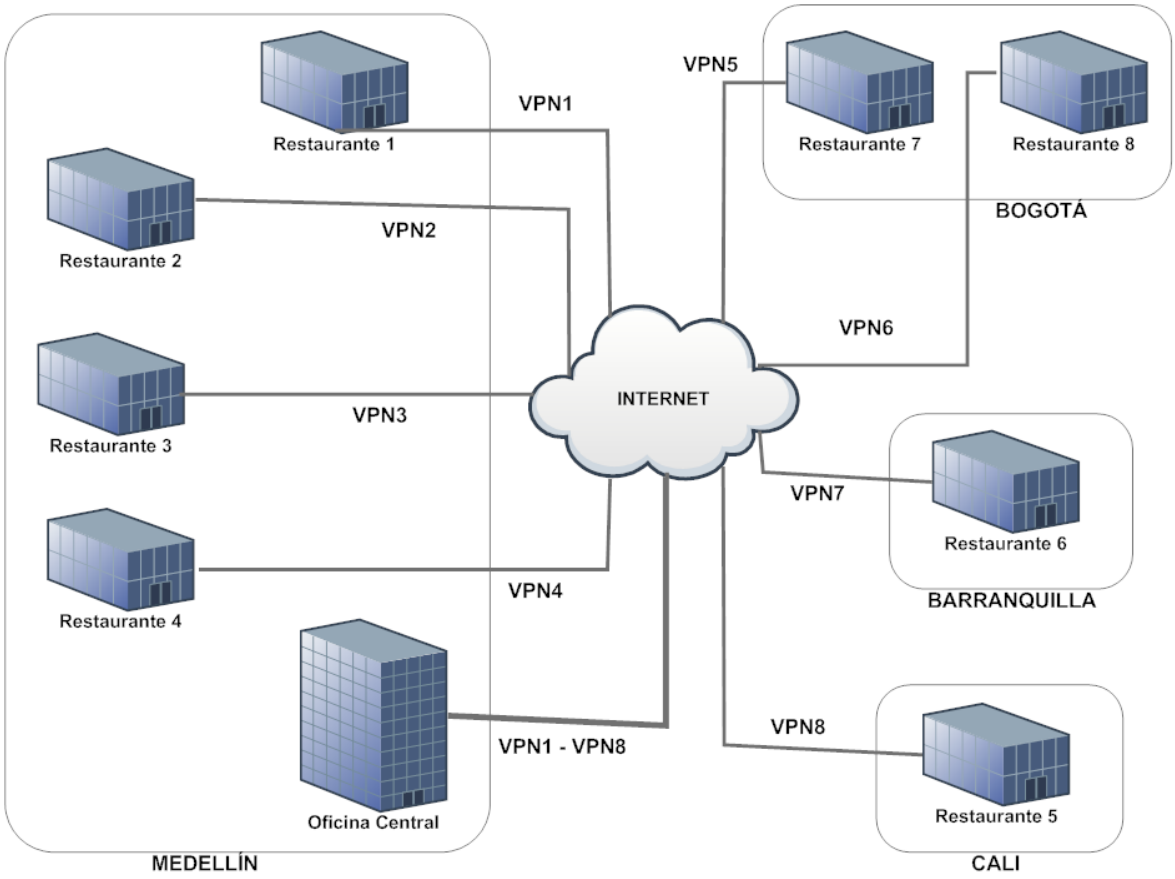
Como visión general de la red, se tienen unos restaurantes ubicados por todo el territorio nacional y una oficina central ubicada en la ciudad de Medellín. Como no es necesario conectar los restaurantes entre sí, se considera idónea la topología de estrella extendida, donde todos los *routers* de los restaurantes se conectan con un *router* en la oficina central. Toda la administración se realiza en esta oficina, por lo que toda la información de los restaurantes debe llegar a la misma cuando sea requerido. Para esto se pensó en un enlace WAN por medio de VPN: una VPN entre cada restaurante y la oficina central. Las razones por las cuales se tomó esta decisión son las siguientes:

- Cada restaurante cuenta con conexión a internet con alta disponibilidad, lo cual es requisito básico para la implementación de los túneles VPN.
- En caso de que el acceso a internet falle, los restaurantes pueden seguir funcionando normalmente mientras el servicio se restablece ya que la aplicación principal no es centralizada y se encuentra instalada tanto en la oficina central como en el equipo de gerencia de los restaurantes. La información es recopilada y luego obtenida por medio de reportes.
- El tráfico de datos entre los restaurantes y la oficina central no es muy alto: sólo se necesita para enviar pequeños paquetes de información, realizar algunas pocas consultas en las bases de datos de los restaurantes, algunas sesiones de escritorio remoto. En un futuro se puede necesitar para telefonía IP, pero dado que en cada restaurante sólo habrá una extensión telefónica, el tráfico de voz será muy pequeño.
- Al utilizar un equipo que soporte VPN en la oficina central se pueden ofrecer conexiones privadas a los gerentes de la compañía, de manera que puedan tener acceso a la información desde cualquier punto que cuente con servicio de internet.
- En comparación con la otra opción de enlace WAN que son los enlaces dedicados, la VPN ofrece la mejor relación costo - beneficio para lo que necesita la compañía. Un enlace dedicado es muy costoso y se usa para conexiones críticas que requieren una muy alta disponibilidad porque de él dependen aplicaciones muy importantes, pero para éste caso es un lujo innecesario ya que la VPN ofrece una muy buena seguridad, aprovechando el canal de internet como medio de comunicación, tanto para la

conexión privada como para la navegación en internet de los empleados y la red de clientes.

El esquema general de la red a nivel nacional es el siguiente:

Figura 13. Esquema de enlaces WAN



Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

Como se puede apreciar en la Figura 13, todos los enlaces VPN conectan los restaurantes con la oficina central. Cada línea representa una conexión a internet. Sobre cada una de éstas conexiones se crea un túnel, a excepción de la conexión de la oficina central que tiene tantos túneles como restaurantes tenga la compañía. Actualmente tiene 8 restaurantes, pero se esperan tener muchos más en los próximos años, por lo que el equipo que soporta las VPN debe ser lo suficientemente robusto para mantener las conexiones simultáneas garantizando calidad en el servicio y estabilidad en la conexión.
Esta conectividad es necesaria para mejorar el proceso mediante el cual se realiza el intercambio de información entre las sedes (ver capítulo 1 para detalles sobre el proceso

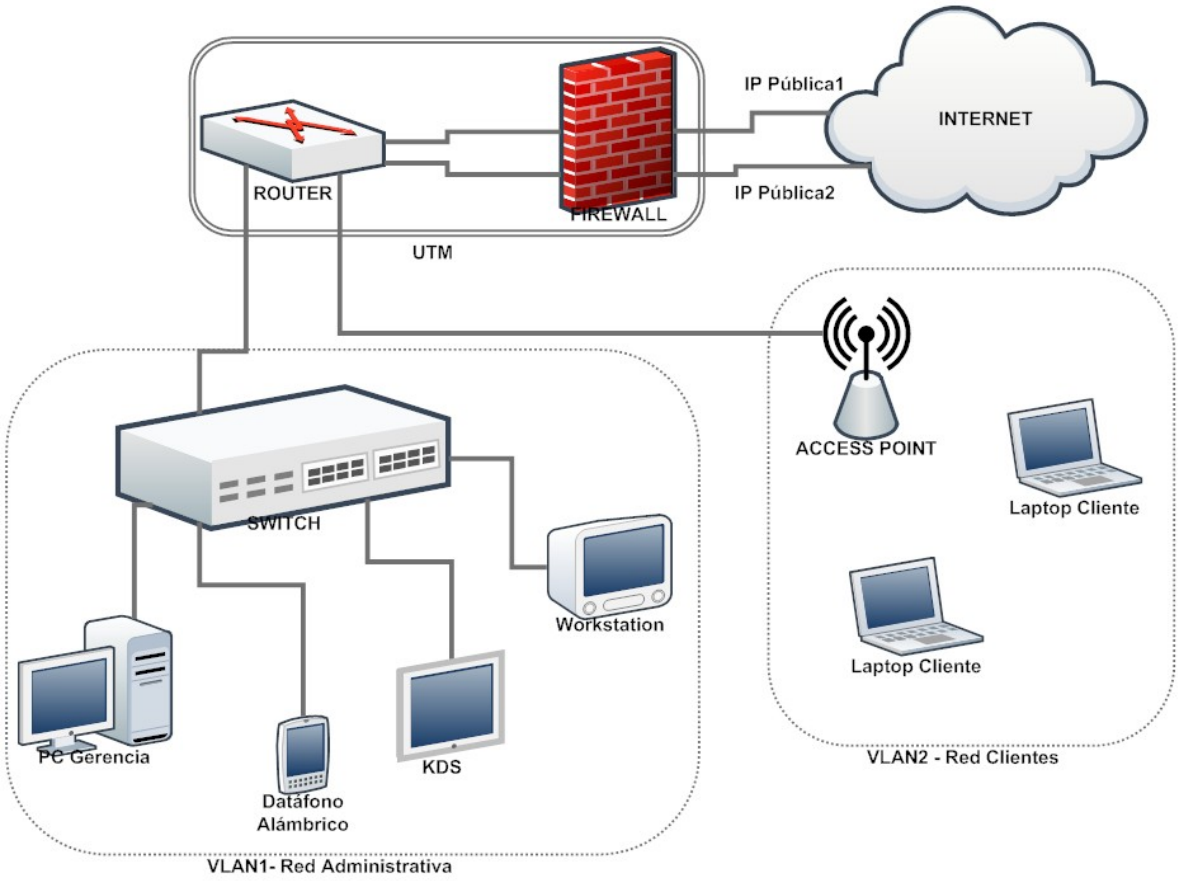
actual), de manera que todas se vean como una gran red en la que se puede compartir información fácilmente. Con las VPN se espera poder compartir los archivos de la aplicación principal Micros® de manera transparente, tan fácil como copiar un archivo de una carpeta a otra dentro de la misma LAN. Además, se espera poder acceder a las bases de datos de los restaurantes de manera simple, realizando consultas como si fuera en la misma LAN, de forma rápida y segura, mediante la aplicación Ocean.

Dentro de este esquema general se encuentran dos esquemas similares para sus sedes: un esquema para los restaurantes y otro esquema para la oficina central. Entre ambos hay ciertas diferencias que hacen que sea necesario separar el diseño para garantizar la seguridad en la red.

5.2. ESQUEMA DE RESTAURANTES

La siguiente figura muestra el diseño de red para los restaurantes. Se debe tomar como una plantilla para usarla en cada uno de los mismos, homogeneizando así la arquitectura e infraestructura de red de las sedes, lo cual significa mayor facilidad en configuraciones, soporte e implementaciones, ya que se puede realizar de manera estándar para todos los restaurantes.

Figura 14. Esquema LAN de los restaurantes



Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

En este esquema se identificaron dos subredes diferentes: una subred administrativa y otra subred de clientes. Como se puede observar, se utiliza una topología en estrella extendida donde todos los equipos de la red administrativa se conectan a un concentrador principal, el *switch,* quien a su vez se conecta al *router*. Este a su vez, tiene conectado un *Access point* del cual se conectan todos los equipos de la red de clientes. Esto es debido a que la compañía desea ofrecer servicio de internet inalámbrico a sus clientes, por lo que se deben separar ambas subredes para efectos de seguridad.

Las razones para separar las subredes es que, primero, existe el riesgo de que algún cliente que se conecte al servicio de internet inalámbrico tenga conocimientos en redes y *hacking* y que además tenga intenciones de hacer estragos en la red administrativa, por lo que es importante que esta red no sea visible para los clientes. Segundo, es imposible controlar los equipos que se conectan a la red, ya que se pretende que sea un servicio gratuito y libre, por lo que existe el riesgo de que se conecten computadores infectados con virus, troyanos, gusanos y toda clase de elementos informáticos dañinos que se

pueden propagar por una red, por lo que es necesario aislar los equipos administrativos de este tipo de riesgos.

Por estas razones se decidió separar las dos subredes mediante VLAN, lo cual provee una separación lógica de las subredes sobre una misma red física. Estas VLAN permiten que exista un esquema de direccionamiento IP independiente para la red de clientes y de esta manera separar los servicios que sobre ésta se ofrecen, además que oculta los equipos administrativos de la vista de los clientes ya que no pertenecen a la misma subred.

Adicional a la separación lógica de las redes, se decide usar una segunda dirección IP pública en cada restaurante, con el fin de separar el tráfico de la VPN y el tráfico de internet, de modo que ningún paquete que se origine de la red de clientes sea enrutado hacia la red privada que tiene como destino la oficina central y, de esta manera, evitar que el enrutamiento se convierta en una brecha de seguridad.

Dado que la seguridad es un tema de suma importancia para la compañía, se deben adicionar *firewalls* robustos a la red. Estos *firewalls* son los encargados de establecer las VPN y mantenerlas conectadas de manera confiable y segura, para así garantizar la transmisión de información. Actualmente ninguna sede cuenta con un *firewall* de este tipo y es necesario adicionarlo al nuevo diseño de red. Este equipo debe estar acompañado de un *router,* encargado de encaminar los paquetes hacia el destino correcto. Dado que se optó por disponer de dos direcciones IP públicas, el equipo debe soportar doble WAN, y de esta manera poder hacer uso de este recurso para separar el tráfico administrativo del tráfico de clientes. Se sugiere para este diseño incorporar a la infraestructura equipos UTM (*Unified Treath Management* - Administración Unificada de Amenazas) que cumplen ambas funciones, tanto de *router* como de *firewall,* simplificando la arquitectura, la administración y el soporte de la red. Además de las anteriores características, el equipo UTM debe tener la capacidad de generar VLAN para la separación lógica de la red administrativa y la red de clientes.

5.2.1. Red administrativa

La red administrativa es la red a la que pertenecen todos los equipos necesarios para el funcionamiento del restaurante: el computador de gerencia, las estaciones de trabajo (*workstations*), los KDS y los datáfonos alámbricos. Todos estos equipos son los esenciales y, sin ellos, el restaurante se ve obstaculizado en su operación diaria. Los equipos funcionan de la siguiente manera:

- Todos los equipos van conectados al *switch* principal.
- La aplicación principal de Micros® se encuentra alojada en el computador de la gerencia. Las estaciones de trabajo se comunican con éste para guardar la

información de las operaciones que se realiza en cada una de ellas. Sin ésta conexión, las estaciones pueden almacenar muy poca información en su memoria flash, (aproximadamente 200 transacciones), por lo que se vuelve crítica la disponibilidad del computador de gerencia para las estaciones de trabajo.

- Los KDS se comunican con las estaciones de trabajo de manera que cuando se realiza un pedido en la estación, éste aparece inmediatamente en uno de los monitores ubicados en la cocina para que vaya siendo despachado. Sin los KDS, los empleados de cocina no saben qué tienen que preparar en el instante, por lo que se vuelve un cuello de botella para garantizar la velocidad en la entrega de las órdenes. Además, sin estos KDS, aumentan considerablemente las probabilidades de cometer errores en la preparación de los productos.
- Los datáfonos alámbricos funcionan a través de internet, por lo que se debe garantizar conectividad a éste servicio para éstos equipos. Sin embargo, no son tan críticos en el funcionamiento de los restaurantes, ya que también se cuenta con datáfonos inalámbricos por GPRS (*General Packet Radio Service* - Servicio General de Paquetes de Radio) en forma de respaldo, que no dependen de la red interna sino de la red de telefonía celular en la que operan.

5.2.1.1. Políticas de seguridad

Es necesario aplicar políticas de seguridad en el *firewall* de manera que se pueda restringir el tráfico que se genera en la red, sobre todo desde y hacia internet. Se debe hacer esto para garantizar que el computador de la gerencia se utilice para los propósitos a los que está asignado y no usado para otros fines y tenga acceso restringido a sitios de poca confiabilidad que puedan significar una amenaza para la integridad y seguridad de la red. Éste computador se necesita para:

- Alojar la aplicación principal Micros® del negocio en el restaurante y su base de datos.
- Consultar y hacer pedidos a sitios WEB de proveedores. Además se le permite a los gerentes consultar ciertos portales WEB de entidades financieras y correo electrónico. Los sitios WEB que actualmente se pueden consultar son (definidos por la normatividad de la empresa en conjunto con el personal de sistemas de la compañía):
  - http://www.validargroupon.com
  - http://www.google.com
  - http://www.hotmail.com
  - http://vinson.aviacarga.com.co/jbolivar/jsp/administracion/autenticacion/login.jsf
  - http://www.arpsura.com
  - http://www.papyser.com
  - http://www.grupobancolombia.com
- Crear reportes, documentos, llevar registros y toda clase de tareas administrativas necesarias para un punto de venta, todas llevadas a cabo por el gerente de punto.

Existen además ciertas reglas para los dominios que se deben definir en el *firewall* para bloquear completamente ciertos tipos de páginas que generan distracción en el personal, tales como redes sociales, páginas de juegos y de entretenimiento para adultos. Las políticas son (definidas por la compañía):

- Bloquear las redes sociales como: Facebook, Myspace, Hi5, Google+, Flickr, Taringa, Twitter, etc.
- Bloquear sitios de multimedia como: YouTube, Megavideo, Cuevana, Vimeo, Vevo, etc.
- Bloquear sitios de *filehosting* como: Megaupload, Rapidshare, Fileserve, Mediafire, Hotfile, etc.
- Bloquear sitios de juegos y entretenimiento para adultos.

Esta lista es incremental y se van adicionando políticas a medida que se descubren nuevos sitios.

Además de los sitios que se desean bloquear, se deben limitar los puertos abiertos a unos pocos, los necesarios para las funcionalidades que requiere la red. El tráfico de cada puerto es separado entre la IP de internet y la IP de la VPN, según el protocolo que haga uso del puerto. Se definió entonces una lista de los puertos que se deben dejar abiertos, la cual se muestra en la siguiente tabla:

Tabla 3. Puertos abiertos en el *firewall* de los restaurantes para la red administrativa

Puerto	Descripción	Puerto	Descripción
13	Daytime protocol	543	Kerberos
20	FTP Transfer	544	Kerberos
21	FTP Control	636	LDAPS
22	SSH	647	DHCP Failover
25	SMTP	749	Kerberos Administración
37	Time Protocol	843	Flash Player
42	WINS	847	DHCP Failover
53	DNS	860	iSCSI
80	HTTP	989	FTPS
88	Kerberos	990	FTPS
110	POP3	992	TELNET
118	SQL	993	IMAPS
123	NTP	995	POP3S
143	IMAP	1293	IPSec
161	SNMP	2967	Symantec
162	SNMP	4500	IPSec NAT

Tabla 3. (Continuación)			
220	IMAP3	5500	VNC
401	UPS	6101	Backup Exec
443	HTTPS	8008	HTTP Alternativo
445	Active Directory	8080	HTTP Alternativo
464	Kerberos Password	10000	Backup Exec
465	SMTP sobre SSL	17500	Dropbox
520	RIP	32976	LogMeIn ®

5.2.2. Red de clientes

La red de clientes se compone de todos los equipos de quienes se conectan a la red inalámbrica del restaurante. Su función es brindar servicio de internet gratuito a los clientes, para que puedan navegar en internet mientras consumen productos de la empresa. El servicio fue pensado por la compañía como una forma de mercadeo como valor agregado al negocio, dado que cada vez existen más usuarios de equipos con conexión inalámbrica y, al brindar una opción de conexión a internet gratis, más consumidores se acercarían atraídos por este servicio. Dado que se cuenta con un canal de internet de alta velocidad en cada sede, se vio viable la opción de ofrecer este servicio, de manera que pueda limitarse su uso como la compañía lo desee, ofreciendo en este caso, únicamente acceso a portales WEB, correo electrónico y mensajería instantánea.

Para crear la red inalámbrica se adicionó al esquema de red un *Access Point* conectado al equipo enrutador o, en este caso, UTM, el cual, por medio de VLAN, divide este segmento de red de manera lógica, permitiendo direccionamientos diferentes e independientes, lo que garantiza dicha separación.

Para conectarse a la red inalámbrica, se hará uso de una clave de acceso, la cual será brindada a cada cliente que solicite el servicio. La compañía no garantiza ninguna calidad de servicio ni de seguridad, dado que es un servicio libre y gratuito.

5.2.2.1. Políticas de seguridad

Por ser un servicio gratuito de internet, se optó por dejar todas las páginas y dominios abiertos y limitar puertos de manera que se restrinja el tráfico a sitios WEB, correo electrónico y mensajería instantánea. La siguiente es la lista de puertos permitida a la red de clientes:

Tabla 4. Puertos abiertos en el *firewall* de los restaurantes para la red de clientes

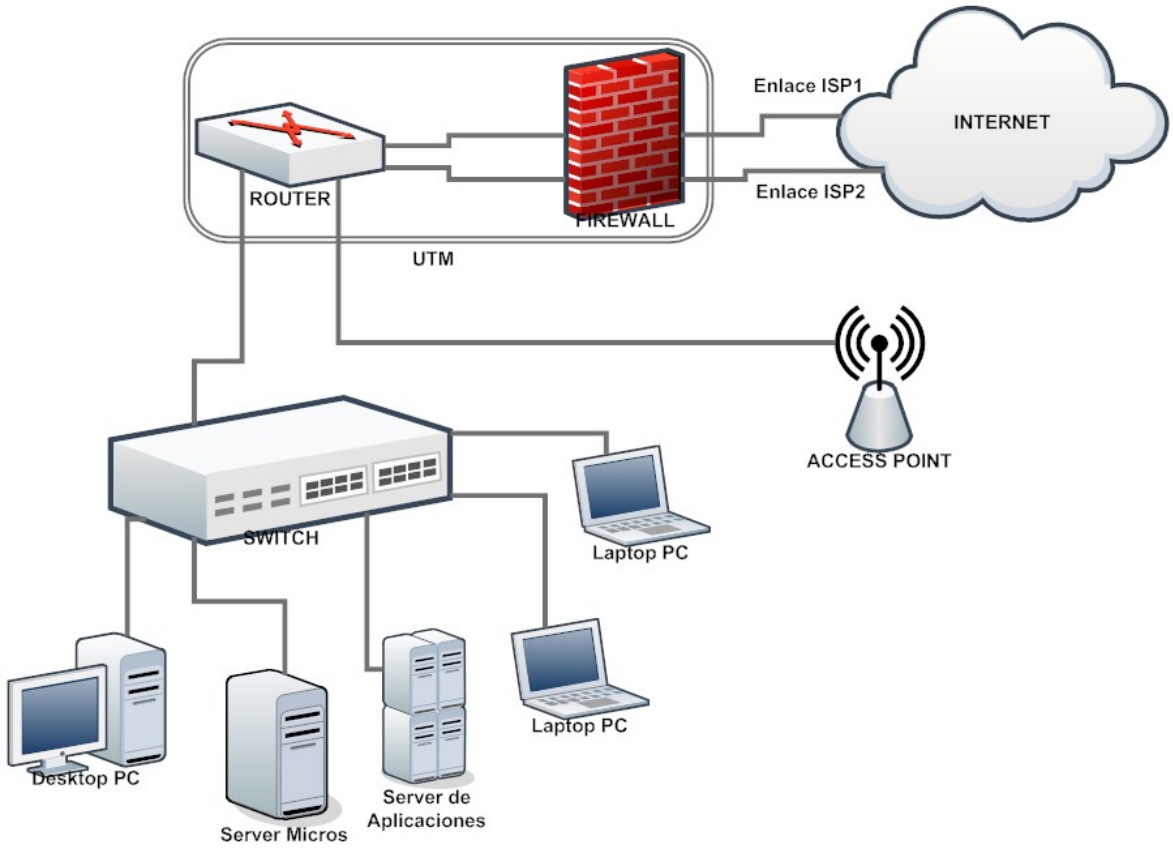
Puerto	Descripción	Puerto	Descripción
25	SMTP	847	DHCP *Failover*
53	DNS	993	IMAPS
80	HTTP	995	POP3S
110	POP3	8008	HTTP Alternativo
143	IMAP	8080	HTTP Alternativo
161	SNMP	1503	Windows Live MSN
162	SNMP	6901	Windows Live MSN
220	IMAP3	23399	Skype
443	HTTPS	19294	Google Talk, voz y video
465	SMTP sobre SSL	19295	Google Talk, voz y video
647	DHCP *Failover*	19302	Google Talk, voz y video
843	Flash Player		

La lista puede ser modificada según las necesidades que vaya teniendo en la compañía. Las políticas se definieron para brindar seguridad a toda la red, de usuarios mal intencionados que se conecten a la red de clientes.

5.3. ESQUEMA DE RED DE LA OFICINA CENTRAL

La siguiente figura muestra el diseño de red para la oficina central:

Figura 15. Esquema LAN de la oficina central



Fuente: Diseño de la red corporativa Quicom S.A. y Yabelco S.A. GONZALEZ RIVERA, León Esteban - ZULUAGA ELJACH, David. 2011.

Aunque a primera vista el esquema es bastante parecido al de los restaurantes, éste es diferente en varios aspectos. El primero y más grande de todos, es que en este caso no tenemos dos redes diferentes sino una gran red general. Esto es debido a que la red inalámbrica es exclusivamente para el personal administrativo y se tiene como opción de movilidad para los equipos portátiles, además que se usa como contingencia en caso de que el *switch* pueda fallar, de manera que los equipos portátiles puedan seguir conectados a internet (sin acceso a los servidores). El diseño presenta una topología en estrella, con todos los equipos conectados a un concentrador, el *switch,* garantizando así conectividad para cada uno de ellos sin depender del funcionamiento de otro, además de control de flujo y colisiones en la red. El caso es el mismo para la red inalámbrica usando el *Access point* como concentrador.

Se tomó como punto central en el diseño de red de la oficina, el hecho de que aquí es a donde convergen todas las VPN de todos los restaurantes, por lo que los niveles de seguridad y confiabilidad en los equipos y el software deben ser mayores. Al igual que en los restaurantes, se debe adicionar un *firewall* robusto al esquema de red, de manera que

todas las VPN que se levantan desde éste punto se mantengan arriba ofreciendo un servicio confiable y seguro.

El servicio de internet es un punto crítico en el esquema de la oficina central dado que los túneles de las VPN se crean a través de este canal, por lo que si falla la conexión a internet en la oficina, se pierde la comunicación con todos los restaurantes provocando un corte en el flujo de la información que se recibe de los mismos, afectando las tareas administrativas que se realizan con esta información. Además por medio de internet se llevan a cabo actividades financieras, se da soporte a restaurantes, se revisan correos, se coordinan reuniones, etc. Por este motivo, se incluyó en el diseño un doble canal de internet, cada uno contratado con un ISP diferente, de manera que mientras ambos funcionen correctamente, se puedan utilizar para balancear las cargas de la salida a internet de la oficina y el establecimiento de las VPN y, en caso de que falle alguno de los dos enlaces, se tiene el otro como contingencia para mantener la conectividad de las sedes funcionando. Para poder lograr esto, es necesario que el *router* que se instale aquí soporte doble enlace WAN. Así como en los restaurantes, se sugirió utilizar un equipo UTM que se encargue de todas las tareas del *router* y el *firewall* (...véase numeral 5.5.2.2...).

Todos los equipos se encuentran conectados físicamente a un *switch* central. Los equipos que se conectan son: Un servidor de la aplicación principal Micros®, un servidor de otras aplicaciones (DNS, Directorio Activo, Ocean), computadores de escritorio, datáfonos alámbricos vía internet, computadores portátiles y en un futuro se espera tener teléfonos IP para los empleados. Todos los computadores se autentican contra el directorio activo alojado en el servidor de aplicaciones, además todos tienen acceso a internet poco restringido, por lo que se requiere de un buen canal de internet para permitir todo el tráfico que se necesita: enlaces VPN, sitios WEB y correo electrónico consultado por los empleados. Los computadores portátiles, además, se conectan a la misma red de forma inalámbrica mediante un *Access point* conectado al equipo enrutador (en este caso al UTM) ofreciendo así una solución de movilidad para éstos computadores cuando sea necesario desplazarlos.

5.3.1. Políticas de seguridad

Se tuvieron en cuenta dos aspectos importantes a la hora de definir las políticas de seguridad en la oficina central. El primero y más importante es que todos los túneles VPN llegan aquí, donde se guarda toda la información de los restaurantes. Además, es en donde se encuentra el laboratorio de la aplicación principal Micros® en el cual el personal de sistemas realiza todos los cambios necesarios a la misma, como actualización de precios, descuentos, combos, etc. El segundo aspecto es que los empleados de la oficina tienen acceso ilimitado y poco restringido a internet y, ya que son empleados de confianza, pueden: acceder a muchos más sitios WEB, descargar contenido, entrar a sitios de entretenimiento, entrar a redes sociales, revisar correo electrónico, usar

mensajería instantánea, ver videos en línea y muchos otros servicios que no se les permite a los empleados de los restaurantes.

Por estas razones, se definió una lista de puertos que son los que van a estar abiertos para garantizar seguridad en la red y, al mismo tiempo, permitir libertad a la hora de navegar en internet:

Tabla 5. Puertos abiertos en el *firewall* de la oficina central

Puerto	Descripción	Puerto	Descripción
13	Daytime protocol	647	DHCP Failover
20	FTP Transfer	749	Kerberos Administración
21	FTP Control	843	Flash Player
22	SSH	847	DHCP Failover
25	SMTP	860	iSCSI
37	Time Protocol	989	FTPS
42	WINS	990	FTPS
53	DNS	992	TELNET
80	HTTP	993	IMAPS
88	Kerberos	995	POP3S
110	POP3	1293	IPSec
118	SQL	2967	Symantec
123	NTP	4500	IPSec NAT
143	IMAP	5500	VNC
161	SNMP	6101	Backup Exec
162	SNMP	8008	HTTP Alternativo
220	IMAP3	8080	HTTP Alternativo
401	UPS	10000	Backup Exec
443	HTTPS	17500	Dropbox
445	Active Directory	32976	LogMeIn ®
464	Kerberos Password	1503	Windows Live MSN
465	SMTP sobre SSL	6901	Windows Live MSN
520	RIP	23399	Skype
543	Kerberos	19294	Google Talk Voz & Video
544	Kerberos	19295	Google Talk Voz & Video
636	LDAPS	19302	Google Talk Voz & Video

En cuanto a dominios y sitios WEB específicos, no se creó ninguna regla, de manera que se brinde libertad a los empleados para consultar lo que deseen. Esta decisión fue

tomada por la empresa ya que los empleados de la oficina son considerados empleados de confianza.

5.4. DIRECCIONAMIENTO IP

El direccionamiento IP es un punto importante en el diseño de esta nueva red. Actualmente es desorganizado, desperdicia direcciones ya que no hace uso de herramientas de *subnetting* y se repiten segmentos de red en diferentes restaurantes, lo cual sería un impedimento para el correcto funcionamiento de las conexiones VPN. Se definió un esquema de direccionamiento IP privado teniendo en cuenta las consideraciones hechas para el diseño de la red (...véase capítulo 4...). Las características de este nuevo esquema de direccionamiento son:

- Para la red corporativa, se utilizaron direcciones privadas clase B, tomando como base la dirección 172.16.0.0 con máscara 255.255.0.0, y realizando *subnetting* mediante VLSM.
- Para la oficina se definieron direcciones IP con máscara de subred 255.255.255.0, teniendo así 254 hosts disponibles.
- Para la red de los restaurantes, se definieron direcciones IP con máscara de subred 255.255.255.192, teniendo así 62 *hosts* por restaurante. Con este *subnetting* de 10 bits, tenemos una posibilidad de 1024 direcciones de red, cada una para asignarla a un restaurante.
- Para los enlaces punto a punto de las VPN, se usó como base la dirección IP 172.17.0.0 con máscara de subred 255.255.0.0. Realizando *subnetting* y asignándole a las direcciones IP de esta red una máscara de subred 255.255.255.252, se obtienen 16384 direcciones de red para asignar a enlaces punto a punto como nuevas VPN.
- Para la red inalámbrica de los clientes se usó direccionamiento clase C privado, tomando como base la dirección IP 192.168.0.0 con máscara de subred 255.255.255.0. Esto resulta en un total de 254 hosts por restaurante, siendo mucho más que suficiente para la demanda de clientes usuarios de internet de cada uno. Este mismo direccionamiento se usa en todos los restaurantes, ya que cada uno es independiente y no se comporta como una gran red entre todos los restaurantes, sino que es una pequeña red para cada restaurante. Para la salida a internet de los clientes, se hace uso de NAT (*Network Address Translation* - Traducción de Dirección de Red).

En las siguientes tablas, se especifica el direccionamiento IP tanto para las redes LAN de los restaurantes y la oficina central, como para los enlaces punto a punto de las VPN.

Tabla 6. Direccionamiento IP para las redes LAN

Ubicación	Número de Hosts	Dirección de Red	Dirección de Broadcast	Máscara de Subred
Oficina	254	172.16.0.0	172.16.0.255	255.255.255.0
R1	62	172.16.1.0	172.16.1.63	255.255.255.192
R2	62	172.16.1.64	172.16.1.127	255.255.255.192
R3	62	172.16.1.128	172.16.1.191	255.255.255.192
R4	62	172.16.1.192	172.16.1.255	255.255.255.192
R5	62	172.16.2.0	172.16.2.63	255.255.255.192
R6	62	172.16.2.64	172.16.2.127	255.255.255.192
R7	62	172.16.2.128	172.16.2.191	255.255.255.192
R8	62	172.16.2.192	172.16.2.255	255.255.255.192

Tabla 7. Direccionamiento IP para los enlaces VPN

VPN	Dirección de Red	Dirección de Broadcast	Máscara de Subred
VPN1 R1 - Oficina	172.17.0.0	172.17.0.3	255.255.255.252
VPN2 R2 - Oficina	172.17.0.4	172.17.0.7	255.255.255.252
VPN3 R3 - Oficina	172.17.0.8	172.17.0.11	255.255.255.252
VPN4 R4 – Oficina	172.17.0.12	172.17.0.15	255.255.255.252
VPN5 R5 – Oficina	172.17.0.16	172.17.0.19	255.255.255.252
VPN6 R6 – Oficina	172.17.0.20	172.17.0.23	255.255.255.252
VPN7 R7 - Oficina	172.17.0.24	172.17.0.27	255.255.255.252
VPN8 R8 - Oficina	172.17.0.28	172.17.0.31	255.255.255.252

5.5. RECOMENDACIONES TÉCNICAS MÍNIMAS DE INFRAESTRUCTURA

Para que el diseño de red realizado pueda funcionar, existen una serie de especificaciones mínimas de infraestructura que permitan el buen despliegue, funcionamiento y mantenimiento de la red diseñada. Es importante que en el momento de la implementación de este diseño de red, se cumplan éstas recomendaciones en los equipos que se van a adquirir, para así cumplir con los objetivos planteados en este proyecto. En el capítulo siguiente de los proveedores, se especifican los equipos cotizados y que se le sugiere utilizar a la compañía. Sin embargo, ésta es libre de usar los

equipos que crea sean más pertinentes tanto para sus necesidades futuras y actuales como para sus finanzas.

5.5.1. Cableado estructurado

Estas son las recomendaciones mínimas para el cableado estructurado, basadas en las falencias encontradas en el cableado actual:

- Para el cableado, se recomienda utilizar cable UTP categoría 5e para voz y UTP categoría 6 para datos, que es el estándar actual del mercado. Éste tipo de cable funciona con tecnología Ethernet 100BASE-TX y 1000BASE-T, alcanzando velocidades de hasta 1 Gbps
- Los cables que vayan a quedar expuestos, canalizarlos por tuberías para mantenerlos organizados, y protegerlos de factores externos como humedad y calor. Evitar juntar cables de energía con cableado de datos, para que no se genere ruido en la señal. Si es completamente necesario mantener todo el cableado junto, usar cable UTP blindado para evitar ruido en la señal.
- Aumentar el tamaño de los racks en los restaurantes de 1 y 2 a unos de 12U y 19" (igual al rack de Restaurante 4), ya que los que actualmente tienen son muy pequeños para los equipos que necesitan guardar allí.
- Utilizar *patch panel* de 24 puertos y organizador de cableado en todos los restaurantes, de manera que se pueda tener ordenado todo el cableado. Así mismo, tener marcado el *patch panel* y los *faceplates* distribuidos por todo el restaurante de manera que se puedan identificar las conexiones en el rack.
- Para la construcción y adecuación de los nuevos restaurantes, se aconseja destinar un espacio únicamente para el cuarto de telecomunicaciones que cuente con ventila de aire acondicionado para mantener una temperatura adecuada en los equipos, con el objetivo de extender su vida útil y de tenerlos funcionando a su capacidad máxima.

5.5.2. Equipos

Estas son las especificaciones mínimas que deben tener los equipos que se adquieran para la implementación de este diseño de red. Como las funcionalidades de los restaurantes y la oficina principal son diferentes, se especifican por separado equipos para restaurante y equipos para la oficina central.

5.5.2.1. Switch

- El promedio de equipos para conectar a la red en todos los restaurantes es de 16 equipos, más o menos 3. Dado este escenario, se recomienda usar *switchs* de 24 puertos en todos los restaurantes, pensando en futuro crecimiento de la red. Aunque se definió que los restaurantes no crecen mucho en sí mismos, es importante tener

una holgura en la disponibilidad de puertos, ya que existe la posibilidad de que nuevos equipos que se adicionen a la red, así como nuevas tecnologías que puedan hacer uso de la misma, como telefonía IP.

- Dado que los equipos de los restaurantes no requieren de tecnología avanzada para operar ni se espera una evolución drástica en términos de hardware, no es necesario que los *switchs* sean más de 10/100 Fast Ethernet, ya que equipos como las estaciones de trabajo y los KDS no funcionan a velocidades mayores a estas.
- Es aconsejable que los *switchs* sean de 19" de ancho, para que puedan ser fijados al rack y de esta manera mantener un orden dentro del mismo.
- Es importante que estos equipos cuenten con QoS (*Quality of Service* - Calidad de Servicio) para futura implementación de telefonía IP.
- En la oficina central el *switch* debe ser de 48 puertos, ya que es el lugar con mayor proyección de crecimiento, tanto en personal como en equipos. Debería ser 10/100/1000 ya que actualmente la gran mayoría de computadores, tanto de escritorio como portátiles, vienen con tarjetas Giga-Ethernet, por lo que tener un *switch* que trabaje a estas velocidades optimiza el rendimiento de la red local.
- El *switch* de la oficina central debe tener QoS y PoE (*Power over Ethernet* - Energía sobre Ethernet) para futura implementación de telefonía IP.

5.5.2.2. UTM

Los equipos UTM son la pieza fundamental de todo este diseño de red. Se optó por esta opción en vez de *router* y *firewall* por separado por las siguientes razones:

- Complejidad reducida al haber un sólo equipo para administrar de un sólo fabricante, además de ser una misma solución integrada de seguridad.
- Simplicidad ya que no se requiere instalación de gran cantidad de software por separado, todo viene instalado de fábrica y sólo requiere configuración.
- Su manejo es sencillo, es *Plug & Play*, con interfaz gráfica fácil de manejar.
- Son equipos robustos que ofrecen lo que la compañía necesita.

Para los restaurantes, el UTM que se instale debe tener las siguientes características mínimas:

- Capacidad para un mínimo de 3 VPN: Una que siempre se encuentra conectada a la oficina central, la segunda para usarla cuando se desee establecer conexión al restaurante desde afuera de la red corporativa y la tercera para brindar conexión al proveedor de la aplicación Micros® que facilite el soporte remoto en caso de necesitarlo.
- Doble enlace WAN para las dos IP públicas que se van a tener, de manera que se pueda dividir el tráfico de internet y las VPN.

- Soporte para crear un mínimo de 2 VLAN: una para la red administrativa y otra para la red de clientes.
- Capacidad QoS para futura telefonía IP
- Es importante que para todos los restaurantes sea el mismo equipo UTM, ya que implica que el personal de sistemas de la compañía esté capacitado en el manejo de un sólo equipo y pueda solucionar los problemas que se presenten de manera rápida.

Para la oficina central, el UTM que se instale debe tener las siguientes características mínimas:

- Capacidad para un mínimo de 50 VPN, dado que la compañía tiene altas expectativas de crecimiento y por cada restaurante nuevo que se abra es un túnel VPN más que se conecta. Además, los gerentes de la empresa se podrán conectar mediante conexiones bajo demanda, por lo que se debe tener disponibilidad de túneles.
- Doble enlace WAN para el doble canal de internet que se tendrá, cada uno de un ISP diferente. Por tal motivo, para aprovechar estos enlaces es necesario que el equipo cuente además con balanceo de cargas. Además, debe estar en la capacidad de levantar las VPN desde un canal y, cuando este se caiga, hacer el cambio automático al otro canal de internet, para mantener la conectividad con los restaurantes.
- Capacidad QoS para futura telefonía IP.

Aparte de estas características, ambos equipos deben tener servicios de seguridad como *anti-virus,* filtro WEB y control de aplicaciones, entre otros. Éstos servicios son necesarios para poder configurar las políticas de seguridad establecidas (...véanse numerales 5.2.1.1, 5.2.2.1 y 5.3.1...).

5.5.2.3. Access Point

Tanto en los restaurantes como en la oficina central hay instalados *Access points* para crear redes inalámbricas. Dado que en los restaurantes la seguridad es controlada desde el equipo UTM, no es necesaria ninguna característica especial en el *Access point.* Sólo se requiere que tenga seguridad mínima de clave pre compartida.

En la oficina central, el *Access point* es para la red inalámbrica de soporte y contingencia y, como es sólo para los empleados, sólo se requiere que tenga seguridad de clave pre compartida.

5.5.3. Anchos de banda de Internet

La conexión a internet en este diseño es muy importante, por lo que los anchos de banda, sobre todo en la oficina central, deben ser suficientes para satisfacer la demanda. El ancho de banda para cada uno de los canales de internet de la oficina central, no debería

ser menor a 4 Mbps de *downstream* y 2 Mbps de *upstream*, que, combinados, en el mejor de los casos debería trabajarse a 8 Mbps de *downstream* y 4 Mbps de *upstream*.

En los restaurantes la situación es similar, ya que al ofrecerse servicio de internet gratuito a los clientes se debe tener un ancho de banda que permita el flujo de las VPN y el flujo de internet sin ningún inconveniente. Por eso, es recomendable un ancho de banda de 3 Mbps de *downstream* y 1 Mbps de *upstream* como mínimo, para todo el tráfico de información que se genera.

5.6. PLAN DE CONTINGENCIA

En todo diseño de red, es muy importante tener un plan de contingencia en caso de que alguno de los elementos de la red falle. Es importante identificar los puntos críticos dentro del diseño y tratar de reducir el impacto cuando algo malo ocurra. En la siguiente tabla se especifican los elementos críticos del diseño, en que podrían fallar y cuál es la criticidad del fallo. Así mismo presenta una solución como plan de contingencia.

Tabla 8. Elementos críticos del diseño y plan de contingencia.

Elemento	Fallo	Criticidad	Solución
Canal de Internet de la Oficina	Caída	Alta	Doble canal de internet con diferente ISP para garantizar disponibilidad, ya que el internet es muy importante en la oficina.
Enlace VPN	Caída	Baja	Los restaurantes pueden funcionar sin conectividad a la oficina central. Se puede acceder a la información de los restaurantes por medio de MyMicros y paquetes de datos totales EM.
UTM de la oficina central	Caída - Daño	Alta	El UTM de la oficina principal es el equipo al que llegan todas las VPN de los restaurantes, por lo que se caerían todos los enlaces. Sin embargo lo más crítico es que se perdería la salida a internet de la oficina, por lo que es necesario contar con un contrato de soporte de este equipo como respaldo y guardar *routers* viejos para conectar en caso de que falle el UTM.
Switch de la oficina central	Caída - Daño	Alta	Se deben guardar *switchs* viejos de los que serán reemplazados, de manera que se puedan conectar los computadores de escritorio y los servidores. Los computadores portátiles pueden seguir con conexión a través del *Access point.*

Tabla 8. (Continuación)			
Canal de internet de los restaurantes	Caída	Media - baja	Sin internet, los restaurantes no pueden hacer pedido a proveedores ni conectarse a las VPN, sin embargo pueden seguir facturando y guardando información. La información que sea requerida por el personal administrativo, puede ser extraída físicamente o impresa y enviada a la oficina central. El servicio de internet a los clientes es gratuito, por lo que no importa que no se brinde.
UTM de restaurante	Daño - Caída	Media - baja	Sin el equipo UTM se pierde la conectividad a internet y se caen las VPN. Para garantizar conectividad a internet del computador de gerencia se debe guardar un *router* de los reemplazados.
Switch de restaurante	Daño - Caída	Muy Alta	Es el peor de los escenarios, ya que las estaciones de trabajo sólo pueden facturar por un promedio de 2 horas si no tienen conexión con el computador de gerencia. Es necesario guardar *switchs* pequeños de 8 puertos para conectar los equipos críticos para el funcionamiento del restaurante: estaciones de trabajo, computador de gerencia y KDS.

6. PROPUESTAS DE IMPLEMENTACION

6.1. PRESELECCIÓN DE PROVEEDORES

Para realizar una selección apropiada de proveedores es indispensable tener siempre presentes y claras las características con las cuales estos proveedores deben de contar, determinadas por el tipo de negocio de la empresa. Se definen entonces unos parámetros de preselección de proveedores necesarios para participar en el proceso:

- Cobertura a nivel nacional: La compañía actualmente cuenta con restaurantes en las ciudades de Medellín, Cali, Barranquilla y Bogotá, se espera que se lleve a cabo otras aperturas en otras de las ciudades más importantes de Colombia. Debido a esto, se busca un proveedor que pueda brindar la misma calidad de servicios sin importar el lugar del país donde se requiera.
- Capacidad para brindar solución completa como servicio de tercerización: No solo se busca un proveedor de equipos de red, se busca un proveedor que lleve a cabo tanto la instalación como la configuración, soporte y administración de la misma infraestructura de red.
- Capacidad de adaptación al diseño de red establecido: El proveedor debe tener el conocimiento y los medios necesarios para implementar la red según el diseño que se le indique.
- Posibilidad de arrendamiento de equipos: Se busca contar con la posibilidad de arrendamiento debido a que este evita que aumenten los activos de la empresa.

Además de estos parámetros indispensables, se establecen otros que brindarían valor agregado al proveedor que los cumpla:

- Soporte por contrato: El proveedor debe estar en capacidad de brindar el soporte que se necesite basándose en un contrato claramente definido.
- Casos de éxito y clientes: Se desea contratar un proveedor que tenga suficiente experiencia y haya trabajado en negocios similares al de la compañía, por esta razón es importante conocer sus clientes y casos de éxito.
- Tiempo de implementación: Es importante poder disponer de una solución de implementación en cualquier caso extremo de plazo muy corto de tiempo para esta etapa en una futura apertura de un restaurante.
- Claridad en la propuesta de infraestructura y plan de implementación: Una propuesta clara y un plan bien definido demuestra que tan comprometido y ordenado es el proveedor.

Finalmente, es la empresa quien selecciona el proveedor más adecuado para la implementación del proyecto basándose en las propuestas económicas, ya que por medio de estas se hace posible establecer la relación entre el costo y el beneficio de cada proveedor.

Entre todas las posibilidades de proveedores en el mercado, se preseleccionaron 2 opciones. Con ambas empresas se realizan reuniones presenciales para aclarar desde ambas partes las generalidades del proyecto.

Tabla 9. Comparación de proveedores

	Proveedor 1	**Proveedor 2**
Parámetros necesarios		
Cobertura a nivel nacional	Personal en Medellín y Bogotá con posibilidad de viaje a cualquier ciudad.	Personal ubicado en las principales ciudades de Colombia.
Solución completa como servicio de tercerización	Instalación completa o capacitación al personal de la empresa para realizar instalaciones, lo mismo para el soporte.	Implementación completa y servicio de administración de equipos.
Capacidad de adaptación al diseño de red	Aporta al diseño de red con sus propios enfoques, brindando y buscando solución.	Se adapta fácilmente al diseño que establece la empresa.
Posibilidad de arrendamiento de equipos	Posibilidad de arrendamiento a un término mínimo de 1 año.	Posibilidad de arrendamiento a un término mínimo de 1 año.
Parámetros de valor agregado		
Soporte por contrato	no ofrece contrato de soporte.	Contrato de soporte 8 x 5 x NBD.
Casos de éxito, clientes	McDonald's, Renting Bancolombia, Cooperativa John F Kennedy, Grupo EMI, Andi.	No entregado.
Tiempo Implementación	A corto plazo.	A un plazo de 45 días como mínimo.
claridad en la propuesta y plan de implementación	La propuesta es poco clara y no brindan un plan de implementación.	Plan de implementación y propuesta de infraestructura detallada y clara.

6.2. PROPUESTAS DE INFRAESTRUCTURA Y PLAN DE IMPLEMENTACIÓN

6.2.1. Propuesta de infraestructura Proveedor 1

Se propone implementar en la red equipos UTM marca Fortigate, uno en cada sede, se sugiere también mayor robustez del UTM de la oficina con respecto al de los restaurantes debido a la topología de la red a implementar. Algunas de las características más relevantes para nuestro caso, con las que cuentan los UTM Fortigate son:

- *Firewall*: Funcionalidad de seguridad que evita intrusiones y ataques a nivel de aplicación.
- *Router*: a pesar de ser un equipo de seguridad, el UTM cumple con la función de enrutamiento, lo que nos evita la necesidad de equipo *Firewall* y equipo *Router* por aparte.
- VPN Ipsec /SSL: Proporciona conexiones seguras entre redes, aplicando simultáneas características de seguridad sobre las VPN que necesitamos establecer.
- *Application Control*: funcionalidad que permite definir políticas sobre las aplicaciones que hacen uso de la red.
- Antivirus/*Antispyware*: cuenta con su propio sistema anti-malware, controlando dichas amenazas antes de que puedan causar daños.
- IPS (I*ntrusion Prevention System* – Sistema de Prevención de Intrusiones): Análisis de las actividades de la red con el fin de prevenir y bloquear amenazas, ataques e intrusiones.
- *Web Filter* (Filtro WEB): funcionalidad para evitar ataques de tipo Web y aplicar políticas de acceso web a los usuarios de la red.
- QoS: Calidad de servicio, permite definir prioridades del servicio a diferentes aplicaciones y flujos de datos, es necesario contar con esta característica por si se va a implementar en un futuro telefonía IP.
- Doble WAN: doble puerto WAN, en la oficina se usa para función de balanceo de cargas y redundancia en la conexión a internet, en los restaurantes se usa para separar el flujo de información de las VPN respecto al resto de flujo de información a internet.

En los restaurantes se propone un equipo Fortigate 50B-BDL, en la oficina se propone un equipo Fortigate 60C-BDL, la cantidad de sesiones VPN que permite establecer cada uno de estos equipos justifica dicha diferencia entre el UTM de los restaurantes y el de la oficina.

Este proveedor propone implementar *switchs* administrables.

6.2.2. Propuesta de Infraestructura Proveedor 2

La solución ofrecida por este proveedor consta de equipos Cisco ASA 5505 en los restaurantes y un equipo Cisco ASA 5510 en la oficina central, estos equipos de seguridad permiten establecer conexiones VPN IpSec *Site-to-Site* (Sitio-a-Sitio) sobre los enlaces de internet de cada una de las sedes. Las características más relevantes de los equipos Cisco ASA son (Ficha técnica de la familia ASA 5500 anexa):

- *Firewall*: Permite el flujo de información valido para el negocio mientras mantiene bloqueado el flujo de datos indeseado. Dentro de esta característica de Firewall se incluye control de aplicaciones.
- *Market-leading content security capabilities* (Capacidades de Seguridad en Contenido de Líderes de Mercado): dentro de esta característica, Cisco establece un perímetro de seguridad exhaustiva lo cual enmarca las características: Antivirus, *Anti-spam*, *Anti-phishing*, protección Web en tiempo real, filtro de contenidos (correo electrónico y WEB), etc.

Los *switchs* requeridos para esta propuesta son No Administrables, puesto que las VLAN se configuran directamente sobre el ASA 5505, el cual cuenta con 8 puertos *Fast Ethernet* 10/100 con capacidad de hasta 3 VLAN.

Todos los equipos tienen garantía y servicio de soporte con la modalidad 8 x 5 x NBD (*Next Business Day* – Siguiente Día de Negocio) (8 horas correspondientes a las laborales diarias, 5 días de la semana correspondientes a los laborales semanalmente y reemplazo de equipos al siguiente día laboral en caso de ser necesario).

7. CONCLUSIONES

- Se lograron identificar problemas y necesidades que tiene la compañía en cuanto a la planificación e implementación de sus redes. La empresa antes de éste proyecto, no contaba con un esquema de planeación para el despliegue de las redes de sus nuevos restaurantes causando que la infraestructura de red fuera desordenada y poco confiable.
- Al analizar en profundidad el escenario para el cual se implementaría la red junto con sus características particulares y después de tener presente diversas opciones de diseño, se ha logrado acoplar los conceptos y técnicas consideradas válidas para realizar una futura implementación de manera idónea.
- Se han presentado dos propuestas de infraestructura y dos proveedores para la implementación de éstas respectivamente. Para obtener dichas propuestas de infraestructura se ha llevado a cabo una preselección de proveedores por medio de parámetros de comparación, los cuales podrían también ser la base para toma de decisiones de la compañía respecto a implementación.
- Tanto para el diseño de red como para las propuestas de infraestructura, se ha tenido como enfoque el futuro crecimiento y evolución del escenario para el cual fue propuesto dicho diseño, garantizando así una red que soporte las operaciones de la compañía a través del tiempo.

BIBLIOGRAFÍA

BRAZZIEL, Dominique. *SearchTelecom: switch.* TechTarget. [Online]. URL: http://searchtelecom.techtarget.com/definition/switch. 2000

CAYMAEX, Olivier. *SearchNetworking: autonomous system (AS).* TechTarget. [Online]. URL: http://searchnetworking.techtarget.com/definition/autonomous-system. 1999

COLLINS, Terrance. KEELEY, Ron. WAYE, Dean. *SearchEnterpriseWan: virtual private network (VPN).* [Online]. URL: http://searchenterprisewan.techtarget.com/definition/virtual-private-network. 2000

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Documentación, presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta actualización. Bogotá D.C. 2008. ICONTEC. NTC 1486.

KROON, Daniel. *SearchNetworking: OSI (Open Systems Interconection)*. TechTarget. [Online]. URL: http://searchnetworking.techtarget.com/definition/OSI. 2006

MICROS SYSTEMS INC. *Kitchen Display Systems.* [Online]. URL: http://www.micros.com/Products/RestaurantSolutions/RestaurantOperations/KitchenDisplaySystems/

--------. *POS Hardware*. [Online]. URL: http://www.micros-fidelio.es/es-ES/Solutions/Products-N-Z/POS-Hardware.aspx

--------. *Restaurant Enterprise Solution.*[Online] URL: http://www.micros-fidelio.es/es-ES/Solutions/Products-N-Z/Restaurant-Enterprise-Solution.aspx

--------. *Workstation*. [Online]. URL: http://www.micros-fidelio.es/es-ES/Solutions/Products-N-Z/~/media/Files/micros-fidelio/Brochures/EU/Workstation%204LX.ashx

RHODES, David. *SearchNetworking: router.* TechTarget. [Online]. URL: http://searchnetworking.techtarget.com/definition/router. 2000

RYLAND, Don. *SearchNetworking: 10BASE-T.* TechTarget. [Online]. URL: http://searchnetworking.techtarget.com/definition/10BASE-T. 2000

TANENBAUM, Andrew S. Redes de Computadoras, 4ta Edición. Ámsterdam, Holanda: Universidad Libre (*Vrije Universiteit*).Pearson Education. 2003.

TECHTARGET. *SearchMobileComputing: access point.* [Online] . URL: http://searchmobilecomputing.techtarget.com/definition/access-point.2003

--------, *SearchMobileComputing: IEEE 802 Wireless Standards: Fast Reference.* [Online]. URL: http://searchmobilecomputing.techtarget.com/definition/IEEE-802-Wireless-Standards-Fast-Reference. 2004

--------, *SearchMobileComputing: wireless LAN (WLAN or Wireless Local Area Network.* [Online]. URL: http://searchmobilecomputing.techtarget.com/definition/wireless-LAN. 2008

--------, *SearchNetworking: 100BASE-T.* [Online]. URL: http://searchnetworking.techtarget.com/definition/100BASE-T. 1997

--------, *SearchNetworking: 1000BASE-T.* [Online]. URL: http://searchnetworking.techtarget.com/definition/1000BASE-T. 2001.

--------, *SearchNetworking: Ethernet.* [Online]. URL: http://searchnetworking.techtarget.com/definition/Ethernet. 2000

--------. *SearchNetworking: patch panel.* [Online]. URL: http://searchnetworking.techtarget.com/definition/patch-panel. 2000

--------, *SearchNetworking: TCP/IP (Transmission Control Protocol/Internet Protocol)*. [Online]. URL: http://searchnetworking.techtarget.com/definition/TCP-IP. 2000

--------, *SearchNetworking: variable-length subnet mask (VLSM).* [Online]. URL: http://searchnetworking.techtarget.com/definition/variable-length-subnet-mask. 2007

--------, *SearchWinDevelopment: browser.* [Online]. URL: http://searchwindevelopment.techtarget.com/definition/browser. 2006

--------, *SearchWinDevelopment: HTTP (Hypertex Transfer Protocol)* [Online]. URL: http://searchwindevelopment.techtarget.com/definition/HTTP. 2000

TECHTARGET, *SearchWinDevelopment: intranet.* [Online]. URL: http://searchwindevelopment.techtarget.com/definition/intranet. 2000

--------, *SearchWinDevelopment: ISP (Internet Service Provider).* [Online]. URL: http://searchwindevelopment.techtarget.com/definition/ISP. 2000

WIKIMEDIA FOUNDATION, INC. *Wikipedia, the free encyclopedia: Border Gateway Protocol.* [Online]. URL: http://en.wikipedia.org/wiki/Border_Gateway_Protocol. 2011

--------, *Wikipedia, the free encyclopedia: Broadcast Domain*. [Online]. URL: http://en.wikipedia.org/wiki/Broadcast_domain. 2011

--------, *Wikipedia, the free encyclopedia: Ethernet.* [Online]. URL: http://en.wikipedia.org/wiki/Ethernet. 2011

--------, *Wikipedia, the free encyclopedia: Hyperlinks.* [Online]. URL: http://en.wikipedia.org/wiki/Hyperlinks. 2011

--------, *Wikipedia, the free encyclopedia: Hypertext.* [Online]. URL: http://en.wikipedia.org/wiki/Hypertext. 2011

--------, *Wikipedia, the free encyclopedia: IEEE 802.11n - 2009.* [Online]. URL: http://en.wikipedia.org/wiki/IEEE_802.11n-2009. 2011

--------,*Wikipedia, the free encyclopedia: IP Address.* [Online]. URL: http://en.wikipedia.org/wiki/IP_address. 2011

--------. *Wikipedia, the free encyclopedia: Instant Messaging*. [Online] URL: http://en.wikipedia.org/wiki/Instant_messaging. 2011

--------, *Wikipedia, the free encyclopedia: Internet.* [Online]. URL: http://en.wikipedia.org/wiki/Internet. 2011

--------, *Wikipedia, the free encyclopedia: Open Shortest Path First.* [Online]. URL: http://en.wikipedia.org/wiki/Open_Shortest_Path_First. 2011

WIKIMEDIA FOUNDATION, INC. *Wikipedia, the free encyclopedia: OSI Model.* [Online]. URL: http://en.wikipedia.org/wiki/Osi_model. 2011

--------. *Wikipedia, the free encyclopedia: Point Of Sale.* [Online]. URL: http://en.wikipedia.org/wiki/Point_of_sale. 2011

--------, *Wikipedia, the free encyclopedia: Public-key cryptography.* [Online]. URL: http://en.wikipedia.org/wiki/Public-key_cryptography. 2011.

--------, *Wikipedia, the free encyclopedia: Routing Information Protocol.* [Online]. URL: http://en.wikipedia.org/wiki/Routing_Information_Protocol. 2011

--------, *Wikipedia, the free encyclopedia: Smartphone*. [Online]. URL: http://en.wikipedia.org/wiki/Smartphone. 2011

--------, *Wikipedia, the free encyclopedia: Structured Cabling.* [Online]. URL: http://en.wikipedia.org/wiki/Structured_cabling. 2011

--------, *Wikipedia, the free encyclopedia: TCP/IP Model.* [Online]. URL: http://en.wikipedia.org/wiki/TCP/IP_model. 2011

--------, *Wikipedia, the free encyclopedia: Transport Layer Security.* [Online]. URL: http://en.wikipedia.org/wiki/Transport_Layer_Security. 2011

--------, *Wikipedia, the free encyclopedia: Virtual LAN.* [Online]. URL: http://en.wikipedia.org/wiki/Virtual_LAN. 2011

-------, *Wikipedia, the free encyclopedia: Virtual Private Network.* [Online]. URL: http://en.wikipedia.org/wiki/Virtual_private_network. 2011

--------, *Wikipedia, the free encyclopedia: Voice over Internet Protocolo.* [Online]. URL: http://en.wikipedia.org/wiki/Voice_over_Internet_Protocol. 2011

--------, *Wikipedia, the free encyclopedia: VPNs in mobile environments.* [Online]. URL: http://en.wikipedia.org/wiki/Virtual_private_network#VPNs_in_mobile_environments. 2011

--------, *Wikipedia, the free encyclopedia: Wi-Fi Alliance*. [Online]. URL: http://en.wikipedia.org/wiki/Wi-Fi_Alliance. 2011