UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TESIS

"PROPUESTA DE IMPLEMENTACIÓN DE COMUNICACIONES UNIFICADAS CON LA INTEGRACIÓN DE TELEFONÍA IP EN LA EMPRESA TECPROTEL"

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN **"COMPUTACIÓN"**

PRESENTAN:

Jesús García Argüello
Marco Apolo Muñoz Paul

DIRECTORA DE TESIS

Ing. Gabriela Camacho Villaseñor

CIUDAD UNIVERSITARIA 27 /11/ 2014

ÍNDICE

Agradecimientos

Jesús García Argüello

Quiero empezar agradeciendo obviamente a mis padres, mis hermanos y familiares que siempre me han apoyado a lo largo de mi vida en cualquier proyecto que he tenido pero sin duda este ha sido es el más importante.

Agradecer infinitamente a la profesora Gabriela Camacho, al Ingeniero Daniel Figueroa y a Marco Apolo Muñoz por su valioso tiempo, paciencia y sabiduría para ayudarme a realizar juntos este sueño.

Mi gratitud más sincera para Amanda Lozada porque siempre me ha animado a seguir hacia adelante.

A la Universidad Nacional Autónoma de México, en especial a la Facultad de Ingeniería por permitirme estudiar dentro de sus instalaciones y ser mi segundo hogar durante muchos años.

A todos mis profesores porque cada uno dejo un legado de conocimientos y enseñanzas que me ayudaron a terminar mi carrera.

Al señor Lino Reza y familia por brindarnos su tiempo y escuchar nuestra propuesta para este proyecto.

A mis amigos y compañeros en especial a Mayra Angélica, Rubén Guevara, Luis Felipe Cano, Fabián Martínez, Carlos Alberto Silva, Verónica Pereira, Miguel Estrada.

A los amigos de mi generación del CCH Azcapotzalco.

Y sobre todo quisiera agradecer a cada uno de mis sobrinos que han sido una fuente de inspiración, espero que en un futuro ellos también puedan vivir un momento como este, se los deseo de corazón.

Gracias Totales...

Marco Apolo Muñoz Paul

A mi madre, mis hermanas Christian, Elisa, María Concepción y toda mi familia por su amor y ser mi felicidad.

A nuestros guías en este proyecto Gabriela Camacho y Daniel Figueroa por su paciencia y enseñanzas.

A Yaret, Aideé y a todos mis amigos que me han apoyado en mi trayectoria y en mi vida.

A Jesús García por permitirme realizar este proyecto junto a él para conseguir esta meta.

A Enrique Niño por darme la oportunidad de medir mis habilidades, aprender y aplicar mi conocimiento en la Escuela Nacional de Trabajo Social.

A la Facultad de Ingeniería de la UNAM, sus aulas y profesores por darme las herramientas, el conocimiento y sabiduría y así poder lograr este objetivo personal, académico y profesional.

A todas las personas que he conocido a lo largo de la vida y han ayudado para que con sus enseñanzas crezca como persona, y por darme las oportunidades para mejorar día a día.

A la *luz* por guiarme en el camino de la vida, iluminarme en los momentos de mayor obscuridad, ayudarme a cumplir mis sueños, metas y liberarme de mi ego.

Prefacio

El presente trabajo surge en respuesta a los cambiantes estilos de trabajo de la actualidad y a la necesidad de colaboración en tiempo real no solamente entre el personal que está en la empresa o fuera de sus lugares de oficinas, sino, en general entre todos los empleados, lo cual permite obtener información actualizada y ágil, es así como TECPROTEL busca herramientas integradas de productividad que permitan a los usuarios comunicarse desde cualquier lugar, de manera segura y rentable.

Por otra parte, el terminar esta tesis, si bien es un aspecto importante en la vida, y resulta de suma trascendencia, es en realidad el inicio de algo nuevo, lo que como seres humanos aspiramos a ser mejores cada día.

El trascender en la vida, es el resultado cuando nos damos cuenta de que el esfuerzo rindió frutos y valió la pena, este trabajo lo vale no solamente por el hecho de terminar y cumplir con un simple trámite, si no que al final del día deja como resultado, un entendimiento de las nuevas tecnologías que podemos utilizar, y comenzar con una interesante etapa en las comunicaciones del ser humano, llamas Comunicaciones Unificadas.

Esta tesis sirvió también para afirmar que, al final de cuentas, hacer las cosas por el gusto de hacerlas, sin pensar obsesivamente en los resultados, es lo más importante, igualmente haber llegado hasta este momento es motivo para expresar algunos agradecimientos, cuyas específicas palabras no comprenderán la amplitud de mis sentimientos.

Agradezco la invitación de la Ing. Gabriela Camacho Villaseñor, para iniciar mis pininos en esta nueva faceta de dirección de tesis.

A mi alma Mater la Universidad Nacional Autónoma de México, por la formación y dicha de poder regresar un poco de lo mucho que me dio.

Jesús y Marco por su paciencia y dedicación en la elaboración del presente y aceptación de los comentarios y sugerencias de un servidor.

Daniel Figueroa Sánchez

Introducción

Como en la mayoría de las empresas en la actualidad, sus empleados tienen la necesidad de salir a reuniones, viajan, o trabajan desde casa si así lo requieren; además de esto el personal de TECPROTEL proporciona servicios en sitio o salen a tomar capacitaciones; en consecuencia constantemente están fuera de la empresa; y para todo directivo se ha vuelto una prioridad el poder localizar a sus subordinados sin importar el lugar donde se encuentren; derivado de esto surge la necesidad de encontrar diferentes canales de comunicación que sean fáciles de utilizar y permitan hacer llegar la información al empleado; sin embargo no se cuenta con una infraestructura óptima que permita tener una comunicación eficiente y con ello lograr optimizar los procesos de negocio de la compañía.

La presente tesis tiene como propósito, el proponer una solución basada en Comunicaciones Unificadas para la empresa TECPROTEL apoyado en la infraestructura AVAYA e integrando las funcionalidades de Microsoft Lync, aprovechando las fortalezas y características de cada sistema para proveer una solución robusta, confiable y flexible para que los servicios que se prestan sean más fiables, seguros y rápidos, en la empresa y hacia los clientes.

En el **Capítulo 1 Antecedentes** en este apartado comenzamos con la base de conocimientos teóricos sobre las redes, durante el desarrollo de éste se explicará sobre los elementos necesarios y como es el funcionamiento de una red. Es muy importante el entendimiento estos conceptos ya que estos serán utilizados durante el desarrollo de esta tesis. Se explican los conceptos de red y redes de computadoras, la forma en que se hace la conexión con los estándares OSI y TCP/IP y los medios de transmisión que se utilizan para hacer los enlaces y la transmisión de datos.

Una vez comprendido el funcionamiento de los sistemas de redes de datos presentamos el **Capítulo 2 Telefonía IP**; en donde empezaremos hablando del tema de la telefonía tradicional describiendo la forma en cómo la comunicación vía telefónica ha ido evolucionando constantemente hasta la época actual en donde ahora se maneja la telefonía IP con funcionalidades mucho más completas, haciendo énfasis en los principales protocolos que se utilizan y la estructura básica de una red de telefonía, las cuales nos dan la pauta para la integración con las redes de datos.

Así es como nos adentramos en el **Capítulo 3 Comunicaciones Unificadas** (UC) donde se explica cada una de las funciones que componen a las UC, los requerimientos, los factores que involucran, como los servicios, tecnologías, estándares y protocolos que sirven para su implementación.

Adentrados en la temática en el **Capítulo 4 Seguridad en las Comunicaciones Unificadas** es en donde abordamos la forma más viable en la cual se deben gestionar los posibles problemas que podrían influenciar la forma de diseñar o poner en práctica la nueva estrategia de CU por lo cual se muestra cómo podemos hacerle frente para garantizar y optimizar cada uno de los servicios de manera confiable y segura para mantener los riesgos en la organización en los niveles más bajos, además de obtener los parámetros necesarios para el diseño de la solución y los servicios a implementarse.

El **Capítulo 5 Fases de la Propuesta a Implementar** es la parte medular de esta tesis en él cual presentamos la estrategia de planeación, diseño y fases de nuestra propuesta de implementación Comunicaciones Unificadas con telefonía IP en la empresa TECPROTEL se explica la metodología haciendo la elección entre diferentes alternativas y propuestas de solución.

Una vez realizada la elección se realiza la integración y configuración de la propuesta con Microsoft Lync 2010 y la tecnología de AVAYA, aclarando las dudas y la transferencia del conocimiento y el método de operación.

Y para finalizar en la parte de **Conclusiones.** Se pretende afinar la solución con un conjunto de conclusiones, recomendaciones, aportaciones y observaciones pertinentes a cada una de las fases que se llevaron a cabo en las diferentes etapas de la propuesta y sobre todo a la integración de las Comunicaciones Unificadas en la empresa TECPROTEL.

Objetivo

Integración de Microsoft Lync 2010 con Telefonía IP AVAYA como solución de Comunicaciones Unificadas para la empresa TECPROTEL.

Objetivos particulares

1. Utilizar la infraestructura existente para optimizar el uso de recursos de la Empresa
2. Integrar la Telefonía IP en el esquema de la solución de Microsoft Lync
3. Presentar una solución óptima de acuerdo a las necesidades de la Empresa

Capítulo 1 Antecedentes

1 Redes de cómputo

1.1 Concepto de Red

Una Red es un Sistema de comunicación el cual permite que un grupo de computadoras y otros dispositivos que están conectados unos a otros puedan comunicarse y compartir información o recursos entre sí a través de un medio de transmisión.

1.1.1 Clasificación de las Redes de Computadoras

Las redes de comunicaciones actualmente se clasifican en dos grandes grupos: LANs, WANs.

1.1.1.1 LAN (Local Área Network), Red de Área Local

Una LAN conecta varios dispositivos de red en una área de corta distancia (decenas de metros) delimitadas únicamente por la distancia de propagación del medio de transmisión [coaxial (hasta 500 metros), par trenzado (hasta 90 metros) o fibra óptica (decenas de metros), espectro disperso o infrarrojo (decenas de metros)].

Una LAN podría estar delimitada también por el espacio en un edificio, un salón, una oficina, hogar pero a su vez podría haber varias LAN en esos mismos espacios. En redes basadas en IP, se puede concebir una LAN como una subred, pero esto no es necesariamente cierto en la práctica. Las LAN comúnmente utilizan las tecnologías Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface “Interfaz de Datos Distribuida por Fibra”) para conectividad, así como otros protocolos tales como el Apple talk, DECnet, IPX (Internetwork Packet Exchange “Intercambio de Paquetes Interred”).

1.1.1.2 WAN (Wide Area Network), Red de Área Local

Una WAN es una colección de LAN´s dispersadas geográficamente cientos de kilómetros una de otra. El router es el dispositivo capaz de conectar LAN´s a una WAN.

1.2 Topologías de Red

1.2.1 Topologías Físicas de Red

Es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (habitualmente denominados nodos). En la figura 1 se muestran las topologías físicas actuales más usadas.

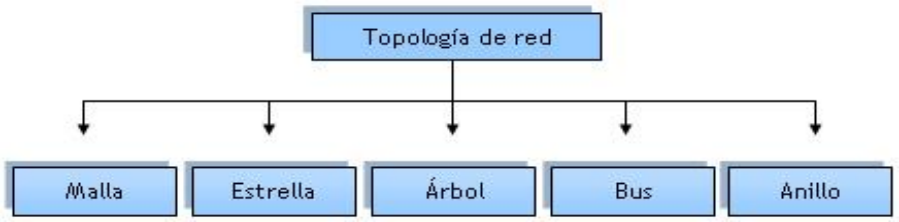

Figura 1 Topología Red

1.2.1.1Topología de Bus

Una topología de bus es multipunto. Un cable largo actúa como una red troncal que conecta todos los dispositivos en la red.

Los nodos se conectan al bus mediante cables de conexión y sondas. Un cable de conexión es una conexión que va desde el dispositivo al cable principal. Una sonda es un conector que, o bien se conecta al cable principal, o se pincha en el cable para crear un contacto con el núcleo metálico. En la figura 2 se muestra la topología de bus.

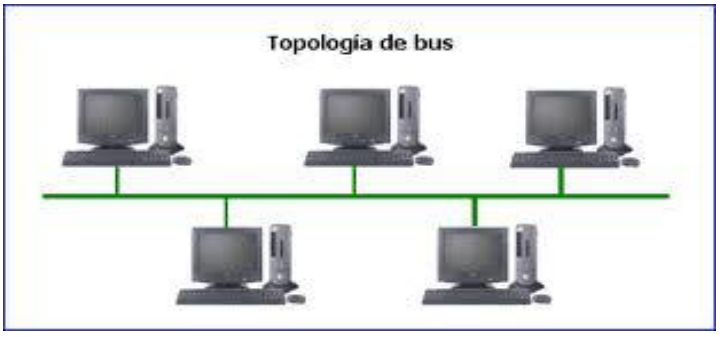

Figura 2 Topología Bus.

Entre las ventajas de la topología de bus se incluye la sencillez de instalación. El cable troncal puede tenderse por el camino más eficiente, después, los nodos se pueden conectar al mismo

mediante líneas de conexión de longitud variable. De esta forma se puede conseguir que un bus use menos cable que una malla, una estrella o una topología en árbol.

1.2.1.2Topología de malla

En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta.

Por tanto, una red en malla completamente conectada necesita n(n-1)/2 canales físicos para enlazar N dispositivos. Para acomodar tantos enlaces, cada dispositivo de la red debe tener sus puertos de entrada/salida (E/S). En la figura 3 se muestra la topología de malla.

Figura 3 Topología de Malla.

Una red en malla ofrece varias ventajas sobre otras topologías de red. En primer lugar, el uso de los enlaces dedicados garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos. En segundo lugar, una topología en malla es robusta. Si un enlace falla, no inhabilita todo el sistema.

Otra ventaja es la privacidad o la seguridad. Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado. Las fronteras físicas evitan que otros usuarios puedan tener acceso a los mensajes.

1.2.1.3 Topología estrella

En la topología en estrella cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central, habitualmente llamado concentrador. Los dispositivos no están directamente enlazados entre sí.

A diferencia de la topología en malla, la topología en estrella no permite el tráfico directo de dispositivos. El controlador actúa como un intercambiador: si un dispositivo quiere enviar datos a otro, envía los datos al controlador, que los retransmite al dispositivo final.

Figura 4 Topología de Estrella.

Una topología en estrella es más barata que una topología en malla. En una red de estrella, cada dispositivo necesita solamente un enlace y un puerto de entrada/salida para conectarse a cualquier número de dispositivos, como se muestra en la figura 4.

Este factor hace que también sea más fácil de instalar y reconfigurar. Además, es necesario instalar menos cables, y la conexión, desconexión y traslado de dispositivos afecta solamente a una conexión: la que existe entre el dispositivo y el concentrador.

1.2.1.4 Topología anillo

En una topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino. Cada dispositivo del anillo incorpora un repetidor. En la figura 4 se muestra la topología anillo.

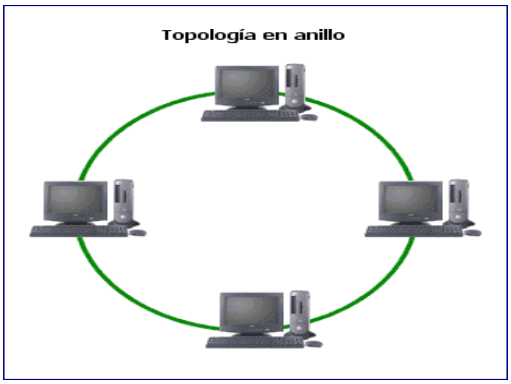

Figura 5 Topología de Anillo.

Una red en anillo es relativamente fácil de instalar y reconfigurar. Cada dispositivo está enlazado solamente a sus vecinos inmediatos (bien físicos o lógicos). Para añadir o quitar dispositivos, solamente hay que mover dos conexiones.

Las únicas restricciones están relacionadas con aspectos del medio físico y el tráfico (máxima longitud del anillo y número de dispositivos). Además, los fallos se pueden aislar de forma sencilla. Generalmente, en un anillo hay una señal en circulación continuamente.

1.2.1.5 Topología de árbol

La topología en árbol es una variante de la de estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central.

Figura 6 Topología de Árbol.

El controlador central del árbol es un concentrador activo. Un concentrador activo contiene un repetidor, es decir, un dispositivo hardware que regenera los patrones de bits recibidos antes de retransmitidos. Un ejemplo grafico se muestra en la figura 6.

Retransmitir las señales de esta forma amplifica su potencia e incrementa la distancia a la que puede viajar la señal. Los concentradores secundarios pueden ser activos o pasivos. Un concentrador pasivo proporciona solamente una conexión física entre los dispositivos conectados.

1.2.2 Topologías Lógicas de Red

Hay dos tipos de topologías lógicas: Bus y anillo. Se definen por el seguimiento del flujo de datos en la red.

1.2.2.1 Topología de anillo

En una topología lógica de anillo, los datos se van transmitiendo desde una computadora a otra hasta que llegan a la computadora de destino. El cable transfiere una trama de datos completa permitiendo un bit por vez en el cable. Para enviar datos, las computadoras deben aguardar hasta que se les notifique que es su turno. La topología lógica de anillo también se conoce como una topología activa, ya que cada computadora regenera la señal antes de pasarla. La topología lógica de anillo se utiliza en fabricaciones donde, muchas veces, resulta crítico poder predecir el tiempo que se tardará en transmitir un mensaje desde una fuente determinada hasta su destino.

1.2.2.2 Topología de bus

Por el contrario, una topología lógica de bus se conoce como una topología pasiva, ya que las computadoras no regeneran la señal ni la pasan, como lo hacen en una de anillo. En cambio, son necesarios dispositivos de red especiales, como los repetidores, para regenerar las señales a través de grandes distancias. Otra diferencia es que las estaciones de trabajo en una topología lógica de bus deben lograr obtener el derecho de transmisión. A diferencia de las transmisiones en un anillo lógico, todas las computadoras reciben los datos. Las computadoras miran la dirección de destino en los datos. Si esa dirección no está destinada a ellas, las computadoras descartan los datos.

1.3 Arquitectura TCP/IP

A finales de los años sesenta, el Departamento Defensa de los Estados Unidos creó la red ARPANET (Advanced Research Projects Agency Network “Agencia de Investigación de Proyectos Avanzados”) para poder investigar la comunicación de paquetes. DARPA (Defense Advanted Research projects Agency “Agencia de Proyectos de Investigación Avanzados de Defensa”) fue el organismo que promovió el desarrollo de ARPANET, red que llego a interconectar en 1972 bases militares, centro de investigación, universidades y laboratorios gubernamentales.

En 1982 se especificó un nuevo conjunto de protocolos para ARPANET que fue referenciado por TCP/IP. Se suministraron implementaciones con las versiones 4.1 y 4.2 BSD de Unix, lo cual facilito la expansión. Y en 1983 el TCP/ se adoptó como estándar en ARPANET. A su vez una segunda red llamada MILNET, dedicada exclusivamente a aspectos militares se separó de ARPANET y así fue como empezó a formarse la red de redes mejor conocida como el “INTERNET”

Podemos definir entonces al modelo TCP/IP como una familia de protocolos desarrollados para permitir la comunicación entre cualquier par de computadores de cualquier red o fabricante, respetando los protocolos de cada red individual.

1.3.1 Las capas del modelo TCP/IP

El modelo TCP/IP está formado por capas, en cada una de las cuales se emplean protocolos de comunicación distintos. A continuación describiremos las capas definidas en la arquitectura TCP/IP:

Capa de acceso a la red. Define las características del medio, su naturaleza, el tipo de señales, la velocidad de transmisión, la codificación, específica la forma en la que los datos deben transmitirse sea cual sea el tipo de red utilizado.

Capa de Internet. Se superpone a la red física ya que permite crear un servicio de red virtual independiente de aquella. No es fiable ni orientado a conexión. Es responsable de encapsular el paquete de datos (datagrama).

Capa de Transporte. Se encarga de suministrar a las aplicaciones servicios de comunicaciones de extremo a extremo utilizando dos tipos de protocolo: TCP (Protocolo de Control de Transmisión), fiable y orientado a conexión y UDP (Protocolo de Datagrama de Usuario), no fiable y no orientado a conexión. Su función es brindar los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión.

Capa de Aplicación. En este nivel se encuentran las aplicaciones disponibles para los usuarios una aplicación es un proceso de usuario que está cooperando con otro proceso de usuario en una misma máquina o en máquinas diferentes (Telnet, SMTP, FTP, etc.)

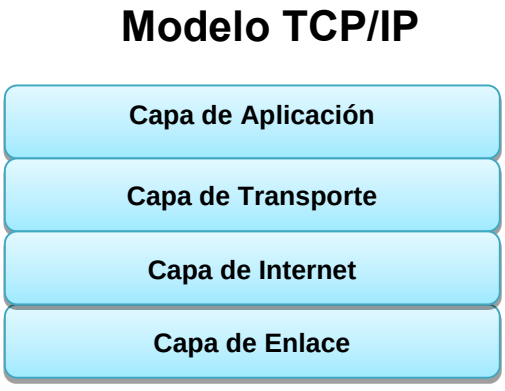

Figura 7 Modelo TCP/IP.

1.4 El Modelo OSI (Open System Interconection “Interconexion de Sistemas Abiertos”)

El modelo de referencia OSI. Es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red.

Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ejemplo, hojas de cálculo, documentos, etc.), a través de un medio de red (por ejemplo, cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aun cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica, de la cual se señalan las siguientes características:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

El problema de trasladar información entre computadores se divide a su vez en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo.

1.4.1 Las capas del modelo de referencia OSI

- Capa 7: Aplicación.
- Capa 6: Presentación.
- Capa 5: Sesión.
- Capa 4: Transporte.
- Capa 3: Red.

- Capa 2: Enlace de datos.
- Capa 1: Física.

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, presentamos una breve descripción de cada capa del modelo de referencia OSI.

Empezando desde la capa 7 que es la más tangible. La figura 8 hace una representación gráfica de forma apilada de las capas del modelo OSI.

Capa 7: La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias.

Capa 6: La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Capa 5: La capa de sesión. Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Capa 4: La capa de transporte segmenta los datos originados en el host emisor y los reensamblan en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte. Si desea recordar a la Capa 4 en la menor cantidad de palabras posible, piense en calidad de servicio y confiabilidad.

Capa 3: La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas, con el crecimiento de la Internet se ha incrementado el número de usuarios que tienen acceso a la información alrededor del mundo. La capa de red es la que se encarga de administrar la conectividad de estos usuarios al proporcionarles el direccionamiento lógico.

Capa 2: La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico) la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Capa 1: La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física.

Figura 8 Modelo OSI.

Comparación del Modelo OSI con el Modelo TCP/IP

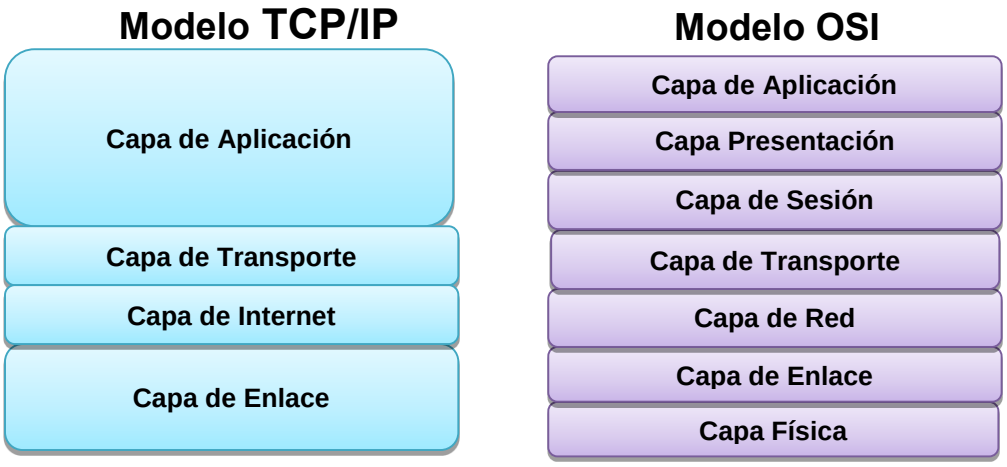

Figura 9 Comparación Modelo OSI vs Modelo TCP/IP.

Como podemos ver en la figura 9 existen ciertas similitudes entre ambos modelos como el hecho de tener una estructura jerárquica pero también existen algunas diferencias OSI se fundamenta en los conceptos de servicios interfaces y protocolos mientras que en TCP/IP estos son obvios en conclusión podemos decir que el modelo OSI es una referencia teórica pero que no es válida en la práctica debido a que OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente.

1.5 Redes Inalámbricas

Una red inalámbrica es, como su nombre lo indica, una red en la que dos o más terminales se pueden comunicar sin la necesidad de una conexión por cable (por ejemplo, computadoras, portátiles, agendas electrónicas, etc.). Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya sea que se encuentren a unos metros de distancia o bien a varios kilómetros (WiMax). Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las

paredes para pasar cables ni de instalar porta cables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.

Por otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

1.5.1 Tipos de Redes Inalámbricas

Hoy en día existe una gran variedad de estándares que nos permiten la comunicación con los dispositivos móviles es por ello que muchos de las computadoras o dispositivos cuenten con soporte para diferentes estándares lo cual permite que se genere mayor operatividad entre ellos en los últimos años estos tipos de redes han ido creciendo en infraestructura en nuestro país debido a la facilidad con las que se puede crear una.

Esto nos ha permitido poder compartir recursos de cómputo y tecnologías de una manera más fácil y simple aunque no tan segura como pude ser en una red cableada, sin embargo otra de las ventajas que ofrece una red inalámbrica es que se puede ahorrar el costo de una red debido a que no necesita conectores o cables y pueden ser más fácil de administrar.

Existen una gran variedad de tipos de Redes Inalámbricas como ya hemos mencionado, estás dependen de un estándar para poder establecer comunicación con otros dispositivos, así que deben de ser compatibles. Y entre los distintos tipos de red ponemos mencionar algunos muy conocidos como son: Bluetooth, Asociación de datos Infrarrojos (Infrared Data Association, IrDA “Asociación de Datos Infrarrojos”), Radiofrecuencia (Home Radio Frecuency Home RF) y los estándares de IEEE 802.11, los cuales nos permiten que exista comunicación entre diferentes dispositivos.

1.5.1.1 WLAN y WPAN

Existen las redes inalámbricas WLAN y WPAN, las primeras (Wireless Local Área Network) están delimitadas por la distancia de propagación del medio y de la tecnología empleada, en interiores hasta 100 metros y en exteriores varios kilómetros, como se muestra en la figura 10.

Las WLAN utilizan tecnologías tales como IEEE 802.11a, 802.11b, 802.15, HiperLAN2, HomeRF, etc. para conectividad a través de espectro disperso (2.4 GHz, 5 GHz).

Las WPANs (Wireless Personal Área Network) están delimitadas en distancia aún más que las WLANs, desde los 30 metros hasta los 100 metros bajo condiciones óptimas en interiores. Las WPAN utilizan tecnologías tales como IEEE 802.15, Bluetooth, HomeRF (Frecuencia de Radio), 802.11b para conectividad a través de espectro disperso o con infrarrojo.

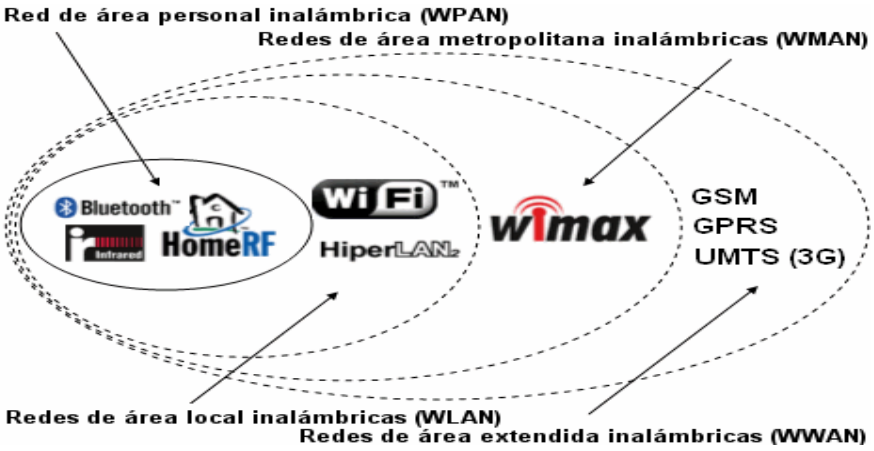

Figura 10 Modelo redes WLAN y WPAN.

1.5.1.2 WMAN Y WWAN

Las redes inalámbricas de área metropolitana WMAN (Wireless Wide Area Network “Las redes inalámbricas de área extensa”) también se conocen como bucle local inalámbrico (WLL, Wireless Local Loop “El Bucle Local inalámbrico”). Las WMAN se basan en el estándar IEEE 802.16. Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones.

La mejor red inalámbrica de área metropolitana es WiMAX (Worldwide Interoperability for Microwave Access “Interoperabilidad Mundial para Acceso por Microondas”), que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros.

Las redes inalámbricas de área extensa (WWAN) tienen el alcance más amplio de todas las redes inalámbricas. Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa. Las tecnologías principales son:

- GSM (Global System for Mobile Communication “Sistema Global para las comunicaciones Móviles”)
- GPRS (General Packet Radio Service “Servicio General de Paquetes vía Radio)
- UMTS (Universal Mobile Telecommunication System “Sistema Universal de Telecomunicaciones Móviles”)

1.5.1.3 Bluetooth

Bluetooth es una especificación tecnológica para redes inalámbricas que permite la transmisión de voz y datos entre distintos dispositivos mediante una radiofrecuencia segura (2,4 GHz). Esta tecnología, por lo tanto, permite las comunicaciones sin cables ni conectores y la posibilidad de

crear redes inalámbricas domésticas para sincronizar y compartir la información que se encuentra almacenada en diversos equipos.

El término [1]Bluetooth ("Diente azul" en inglés, aunque el nombre proviene del rey danés y noruego Harald Blatand, traducido como Harold Bluetooth) es la denominación comercial y popular del estándar de comunicación inalámbrica IEEE 802.15.1. La primera empresa en investigar esta tecnología fue Ericsson, encargada de liderar un grupo que, con el tiempo, sumó a IBM, Nokia, Microsoft, Motorola y otras compañías que apoyaron el estándar.

1.5.1.4 IrDA (Infrared Data Association "Asociación de Datos Infrarrojos")

Es un estándar para la transmisión de datos mediante un puerto de infrarrojos las velocidades de transferencia son más o menos lo mismo que los puertos paralelos tradicionales. La conectividad por infrarrojos es una tecnología inalámbrica de edad utiliza para conectar dos dispositivos electrónicos. Se utiliza un haz de luz infrarroja para transmitir la información y por lo tanto requiere línea de vista directa y opera sólo a corta distancia.

IR fue sustituida por Bluetooth, que tiene la ventaja de operar a distancias más largas (alrededor de 30 pies) y de ser omni-direccional.

1.5.1.5 HomeRF (Home Radio Frecuency "Frecuencia de Radio")

Home RF (Home Radio Frequency) proporciona interconexión entre productos electrónicos de consumo dentro del hogar, para diferentes aplicaciones. Utiliza también la misma banda de 2,4 GHz, pero no interfiere con Bluetooth gracias al método de salto de frecuencia (Protocolo de Acceso Inalámbrico Compartido) en este caso es de 50 por saltos por segundo, en vez del Direct Sequence empleado en otras tecnologías y la potencia de los transmisores es de tan sólo 100 mW.

Las principales aplicaciones que encuentra Home RF están en la conexión inalámbrica de un PC a otros dispositivos electrónicos de consumo, como son vídeos, electrodomésticos, juguetes avanzados, impresoras, centralitas, teléfonos inalámbricos, etc.; con un rango de distancia que alcanza hasta los 50 metros.

Al igual que Bluetooth, Home RF utiliza el salto de frecuencia para evitar interferencias; admite la comunicación de datos hasta 2 Mb/s y permite conectar hasta un total de 127 dispositivos. Soporta comunicación de voz y datos, permitiendo hasta 6 conversaciones. El grupo de trabajo The HomeRF Working Group (HRFWG), formado en marzo de 1998 por compañías como COMPAQ, Ericsson, Hewlett-Packard, IBM, Intel, Microsoft y Motorola, entre más de 100, ha desarrollado el protocolo SWAP (Shared Wireless Access Protocol), basado en el estándar IEEE 802.11 para datos y en DECT para voz, que se usará en esta aplicación. SWAP puede

[1] http://definicion.de/bluetooth/

soportar todo tipo de servicios enfocados a la transmisión de datos, tipo TCP/IP, así como protocolos para voz, tipo DECT/GAP, en redes domésticas.

1.5.1.6 Wi-Fi

Wi-Fi es una marca de la Wi-Fi Alliance (Anteriormente la Wireless Ethernet Compatibility Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x. Cuando hablamos de Wi-Fi nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día. Wi-Fi, también llamada WLAN (Wireless LAN, red inalámbrica) o estándar IEEE 802.11.

En la actualidad podemos encontrarnos con tres tipos de comunicación Wi-Fi:

- 802.11b, que emite a 11 Mb/s,
- 802.11g, más rápida, a 54 MB/s.
- 802.11n, transferencia de datos de 2 a 5 veces más que una antena Wi-Fi 802.11 a/g, mejoras sustanciales en cobertura y calidad de conexión. El Wi-Fi 802.11n fue diseñado para reemplazar por completo la actual tecnología alámbrica Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet.

1.5.1.7 Wimax

(Worldwide Interoperability for Microwave Access “Interoperabilidad Mundial para Acceso por Microondas” Interoperabilidad Mundial para Acceso por Microondas), es la marca que certifica que un producto está conforme con los estándares de acceso inalámbrico IEEE 802.16 Estos estándares permiten conexiones de velocidades similares al ADSL o al cable módem, sin cables, y hasta una distancia de 50-60 km. Este estándar es compatible con el de Wi-Fi (IEEE 802.11).

Wimax supone una solución económica al problema tecnológico de la última milla para ofrecer servicios de gran ancho de banda a múltiples usuarios y es una alternativa viable a la instalación de fibra óptica hasta el usuario o a la adaptación de los sistemas de televisión por cable para ofrecer servicios de banda ancha.

Wimax forma parte de la familia de estándares 802.16 del IEEE e HyperMAN de la ETSI y utiliza bandas licenciadas y no licenciadas.

Dependiendo de la implementación puesta en práctica, Wimax ofrece un servicio de hasta 70 Mbps y accesos concurrentes de hasta 48Km de radio en algunas ciudades de Estados Unidos se comienzan a desplegar velocidades entre 34 Mbit/s y 1 Gbit /s.

En la actualidad encontramos tres tipos de comunicación Wimax:

- 802.16, frecuencia de 10-66 GHz Alcance de 2-5 Km
- 802.16a, frecuencia de 11 GHz Alcance de 5-10Km
- 802.16b, frecuencia de 6 GHz Alcance de 2-5 Km.

Figura 11 Modem Wimax.

1.5.1.8 Tecnologías 3G y 4G

Sistemas de Tercera Generación o (3G) Hoy en día en los últimos celulares se está empezando a implementar las tecnología 3G, igualmente ya se está empezando a usar la nueva tecnología 4G, está tecnología principalmente está pensada para que los celulares hagan todo lo que hace una computadora, video llamadas, juegos en tiempo real y ver videos en web. También mejorara mucho la comunicación entre celulares y muchas novedades que aún están por descubrirse.

Una de las principales cosas que se mejoran en esta nueva tecnología es el ancho de banda de la misma, ya que actualmente el ancho de banda utilizado ronda los 14 Mbps máximo, se actualizara primero a 326 Mbps en una tecnología 3.9 G que es una intermedia entre la 3G y la 4G, haciendo que finalmente cuando llegue el 4G se llegue a la velocidad de 1 Gbps.

Esta tecnología también incluirá en la mayoría de los celulares Wi-Max y LTE, estas son dos tecnologías parecidas, que ya se han actualizado en algunos lugares. Principalmente se refieren redes Wi-Fi pero con mucha más potencia.

Antes de la tecnología 4G hubo algunas intermedias como principalmente la 3.9 G, que se inauguró por Verizon en 2010, en el país de EE.UU.

Súper 3G. Esta Súper 3G, fue una tecnología intermedia antes de dar paso a la 4G, transmite datos unas diez veces más rápido que los 3G normales.

Sistemas de Cuarta generación o (4G) Long Term Evolution “Evolución a Largo Plazo”

Algunas empresas de telefonía ya han desarrollado redes 4G que permiten la descarga de hasta 150 megas. Por ejemplo, la compañía de telecomunicaciones TeliaSonera, ha desarrollado este tipo de red en el norte de Europa, convirtiéndose en el primer operador mundial en ofrecer esta innovadora conexión a finales del año 2009. Las redes 4G son las más rápidas del mercado de la telefonía móvil, con velocidades que pueden ser hasta diez veces mayores que las extendidas redes 3G. Las primeras ciudades en gozar de esta tecnología que acelera la transferencia de datos en los móviles han sido Oslo y Estocolmo.

En México fue apenas en el año 2012 que las compañías telefónicas como América Móvil Telefónica Movistar y Iusacell lanzaran este tipo de red para el año 2013 con velocidades de descarga hipotéticas de hasta 100 Mb/s de bajada y 80 Mb/s de subida

1.5.2 Estándar IEEE 802

El primer estándar que surge es el 802.11 (1997), el cual sienta las bases tecnológicas para el resto de la familia. No tuvo mucha relevancia en su momento por la baja velocidad binaria ("bitrate") que alcanzaba, cerca de 2 Mbps, además de la carencia de mecanismos de seguridad de las comunicaciones. Muy poco después se publica el 802.11b, el cual es acogido con un gran éxito comercial. Opera en la banda de los 2.4 GHz y permite alcanzar velocidades binarias teóricas de 11 Mbps mediante el empleo de mecanismos de modulación de canal y protección frente a errores bastante robustos, aunque en la práctica es difícil superar un ancho de banda efectivo de 7 Mbps Cuando el canal de transmisión es ruidoso, posee un mecanismo de negociación que reduce la velocidad binaria en escalones predefinidos, aumentando paralelamente la robustez de los mecanismos de protección frente a errores.

Para complementar su operativa, incorpora un protocolo de seguridad de las comunicaciones, el WEP o (Wired Equivalent Privacy "Privacidad Equivalente a Cableado"), habida cuenta de la imposibilidad de confinar las emisiones en un medio más protegido como es el cable en el caso de las redes fijas. Desafortunadamente, el pretencioso nombre no se corresponde a la realidad, pues muy poco después de su publicación se descubrieron importantes defectos que permitían la intrusión en las comunicaciones con escaso esfuerzo y un equipo convencional.

Las especificaciones del estándar 802 definen estándares para:

- Tarjetas de red (NIC).
- Componentes de redes de área global (WAN, Wide Area Networks).
- Componentes utilizadas para crear redes de cable coaxial y de par trenzado.

En la tabla 1 veremos más a detalle a que se refiere cada uno de estos estándares.

Estos estándares se dividen principalmente en 16 categorías, como se muestra en la tabla 1.

Especificación	Descripción
802.1	Establece los estándares de interconexión relacionados con la gestión de redes.
802.2	Define el estándar general para el nivel de enlace de datos. El IEEE divide este nivel en dos subniveles: los niveles LLC y MAC. El nivel MAC varía en función de los diferentes tipos de red y está definido por el Estándar IEEE 802.3
802.3	Define el nivel MAC para redes de bus que utilizan Acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD, Carrier-Sense Multiple Access with Collision Detection). Éste es el Estándar Ethernet.
802.4	Define el nivel MAC para redes de bus que utilizan un mecanismo de Paso de testigo (red de área local Token Bus).
802.5	Define el nivel MAC para redes Token Ring (red de área local Token Ring).
802.6	Establece estándares para redes de área metropolitana (MAN, Metropolitan Area Networks), que son redes de datos diseñadas para poblaciones o ciudades. En término de extensión geográfica, las redes de área metropolitana (MAN) son más grandes que las Redes de área local (LAN), pero más pequeñas que las redes de área global (WAN). Las redes de área metropolitana (MAN) se caracterizan, normalmente, por conexiones de muy alta velocidad utilizando cables de fibra óptica u otro medio digital.
802.7	Utilizada por el grupo asesor técnico de banda ancha (Broadband Technical Advisory Group).
802.8	Utilizada por el grupo asesor técnico de fibra óptica (Fiber-Optic Technical Advisory Group).
802.9	Define las redes integradas de voz y datos.
802.10	Define la seguridad de las redes.
802.11	Define los estándares de redes sin cableen la capa física y la capa de enlace.
802.11b	Ratificado el 16 de Septiembre de 1999, proporciona el espaldarazo definitivo a la normativa estándar inicial, ya que permite operar a velocidades de 11 Mbps y resuelve carencias técnicas relativas a la falta de itinerancia, seguridad, escalabilidad, y gestión existentes hasta ahora.
802.11n	Este estándar viene sustituyendo al 802.11b y 802.11g que es intermedio entre estos que hace uso de la banda de 2,4 Ghz y 54 Mbps (aun en uso) actualmente el 802.11n maneja la banda de 5 Ghz con velocidades de transmisión que pueden llegar a los 300 Mbps.
802.12	Define el acceso con prioridad por demanda (Demand Priority Access) a una LAN, 100BaseVG-AnyLAN.
802.13	No utilizada.(se cree que por superstición no se le da un uso)
802.14	Define los estándares de módem por cable.
802.15	Define las redes de área personal sin cable (WPAN, Wireless Personal Area Networks).
802.16	Define los estándares sin cable de banda ancha. Como la Tecnología WiMax

Tabla 1Estándares WiMax

1.5.3 Mecanismos de acceso al medio

La multiplexación por división de frecuencia, también denominada FDMA (Frequency Division Multiple Access “Acceso Múltiple por División de Frecuencia”) permite compartir la banda de frecuencia disponible en el canal de alta velocidad, al dividirla en una serie de canales de banda más angostos, de manera que se puedan enviar continuamente señales provenientes de diferentes canales de baja velocidad sobre el canal de alta velocidad.

Este proceso se utiliza, en especial, en líneas telefónicas y en conexiones físicas de pares trenzados para incrementar la velocidad de los datos.

El estándar IEEE 802.3 especifica el método de control del medio (MAC) denominado CSMA/CD por las siglas en ingles de acceso múltiple con detección de portadora y detección de colisiones (carrier sense multiple access with collision detection). CSMA/CD opera de la siguiente manera:

1. Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.
2. Si el medio está tranquilo (ninguna otra estación está transmitiendo), se envía la transmisión.
3. Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.
4. Cuando se produce una colisión, todas las estaciones receptoras ignoran la transmisión confusa.
5. Si un dispositivo de transmisión detecta una colisión, envía una señal de expansión para notificar a todos los dispositivos conectados que ha ocurrido una colisión.
6. Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión.
7. Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

En CSMA/CA cuando una estación que quiere transmitir realiza una serie de pasos:

- Escuchar en el canal correspondiente.
- Si el canal está libre envía la trama.
- Si el canal está ocupado espera un tiempo aleatorio denominado contención y vuelve a intentarlo.
- Transcurrido el tiempo de contención vuelve a repetir todo el proceso hasta que pueda enviar la trama. Hasta lograr RTS/CTS también conocido como sondeo de portadora virtual

Se puede presentar un problema en una red inalámbrica cuando dos estaciones asociadas al mismo punto de acceso no se ven entre sí. Cuando intenten transmitir ninguna de ellas detectará a la otra por lo que pueden transmitir simultáneamente, lo que origina una corrupción de datos en el resto de las estaciones. Para solucionar este problema se puede establecer un mecanismo para que cada estación notifique al punto de acceso que va a transmitir.

Las funciones request-to send y clear-to-send (RTS/CTS) permiten al punto de acceso controlar el uso del medio de las estaciones activando RTS/CTS. Si el adaptador activa RTS/CTS, entonces primero enviará una trama RTS al punto de acceso antes de enviar una trama de datos. El punto de acceso responde con una trama CTS indicando que el adaptador puede enviar la trama de datos. Con la trama CTS el punto de acceso envía un valor en el campo de duración de la cabecera de la trama que evita que otras estaciones transmitan hasta que el adaptador que haya iniciado RTS pueda enviar su trama de datos.

Este proceso de solicitud de envío evita colisiones entre nodos ocultos. El saludo RTS/CTS continúa en cada trama mientras que el tamaño de la trama exceda del umbral establecido en el adaptador correspondiente. En la mayoría de adaptadores de red los usuarios pueden fijar un umbral máximo de tamaño de trama para que el adaptador de red active RTS/CTS. Por ejemplo, si establecemos un tamaño de trama de 1.000 bytes, cualquier trama de un tamaño superior a 1.000 bytes disparará RTS/CTS. De esta forma el proceso sólo afectaría a las tramas más grandes y más costosas de retransmitir pero las más pequeñas es mejor arriesgarse.

Finalmente el ACK o Acknowledgement: Es la estación receptora que chequea el paquete recibido por si tiene algún error. Si lo encuentra correcto envía un "ACK", con lo cual el remitente sabe que el paquete llegó bien, pues si no, debe ser enviado otra vez. Una vez que las demás estaciones "captan" el ACK, saben que el canal está libre y que ya pueden intentar ellas enviar sus paquetes. Si el emisor no recibe el ACK, enviará el paquete nuevamente.

1.5.4 Topología de Redes Inalámbricas

Como hemos visto las redes Inalámbricas son un conjunto de dispositivos lógicos interconectados a través de un medio de propagación para compartir información lo que se conoce como un Conjunto de Servicio Básico el cual consta de un área definida para poder trabajar entre sí. Dicho espacio dependerá de cómo se propague la información, las topologías más conocidas son: BSS, IBSS y ESS

IEEE 802.11b dispone de 2 modos de radio posibles: BSS e IBSS, incompatibles entre sí.

1.5.4.1 Red de Infraestructura BSS (Basic Service Sets)

Es el modo de operación en el que un punto de acceso actúa como puerta de enlace entre una red inalámbrica y una red cableada, los nodos que pertenecen a la red inalámbrica, los clientes de BSS, establecen la comunicación con el punto de acceso y éste, actúa como un puente entre las dos tecnologías de red. En la figura 12 se muestra un gráfico de este proceso.

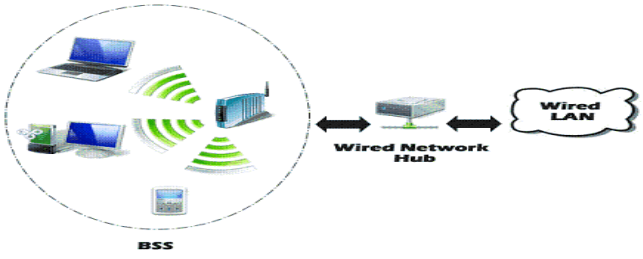

Figura 12 Red de Infraestructura BSS.

1.5.4.2 Áreas de Servicio Extendidas ESS (Extended Service Sets)

Son un conjunto extendido de BSS, es decir, los servicios que se ofrecen cuando existe más de un punto de acceso de tal forma que los clientes pueden unirse a cada punto de acceso permitiendo la movilidad, dicho de otra forma, como se muestra en la imagen de la figura 13.

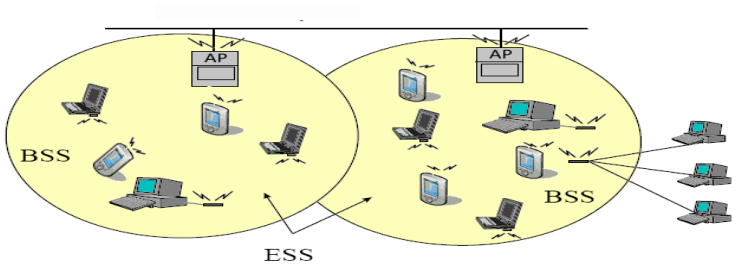

Figura 13 Áreas de Servicio Extendidas ESS.

1.5.4.3 Redes Independientes IBSS (Independent Basic Service Sets)

Es un servicio básico entre iguales, en este modo dos clientes se pueden comunicar entre sí, sin necesidad de que exista un punto de acceso, basta que ambos dispongan de tarjetas de red compatibles para lograr la comunicación, sería el equivalente a conectar dos PC's con tarjetas de red Ethernet mediante un cable cruzado, no se necesitan, hubs, switches ni otros dispositivos, la figura 14 ejemplifica lo anterior explicado.

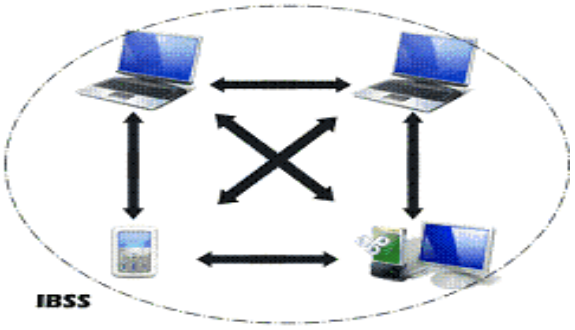

Figura 14 Redes Independientes IBSS.

Además si uno de los clientes que operan en IBSS dispone de conexiones con otras redes, puede proporcionar acceso a las mismas actuando como reenviador o puente de conexión.

Es necesario configurar el protocolo 802.11b para trabajar en BSS o IBSS, pero no se puede trabajar en los dos modos de forma simultánea se usa uno o el otro, pero no los dos a la vez.

Tanto BSS como IBSS admiten el cifrado y codificación WEP de clave compartida.

Lo más habitual es disponer de topologías con uno o varios BSS que brindan conectividad a sus respectivos clientes.

Una limitación de las comunicaciones IBSS, aparte de que sólo pueden comunicarse dos nodos entre sí, es que si usamos tarjetas de diferentes fabricantes, pueden existir incompatibilidades, si bien, con la expansión de las redes 802.11b, cada fabricante han contribuido en la compatibilidad con el protocolo y podemos decir que hoy en día se certifica la conectividad de tarjetas que operan en 802.11b.

Podrás encontrar también el modo IBSS como modo Ad-Hoc o Ad-Hoc Demo, son otras formas de llamar al modo de operación IBSS.

1.5.5 Componentes de una red Inalámbrica

Para poder establecer comunicación en una red como hemos visto se necesitaba de un cable que nos permitía la transferencia de información entre ellos pero la tecnología ha ido evolucionando y también ha cambiado ese aspecto tanto así que hoy en día existen diferentes dispositivos que nos van a permitir tener comunicación entre varios periféricos por medio de ellos como veremos a continuación.

1.5.5.1 Antenas de red

La definición formal de una antena es un dispositivo que sirve para transmitir y recibir ondas de radio. Convierte la onda guiada por la línea de transmisión (el cable o guía de onda) en ondas electromagnéticas que se pueden transmitir por el espacio libre.

El ancho de banda de la antena se define como el rango de frecuencias sobre las cuales la operación de la antena es "satisfactoria". Esto, por lo general se toma entre los puntos de media potencia, pero a veces se refiere a las variaciones en la impedancia de entrada de la antena.

Ancho de Banda de la Antena: El ancho de banda de la antena se define como el rango de frecuencias sobre las cuales la operación de la antena es "satisfactoria". Esto, por lo general se toma entre los puntos de media potencia, pero a veces se refiere a las variaciones en la impedancia de entrada de la antena.

Cada subconjunto o banda de frecuencias dentro del espectro electromagnético tiene propiedades únicas que son el resultado de cambios en la longitud de onda. Por ejemplo, las frecuencias medias (MF, Medium Frequencies) que van de los 300 kHz a los 3 MHz pueden ser radiadas a lo largo de la superficie de la tierra sobre cientos de kilómetros, perfecto para las estaciones de radio AM (Amplitud Modulada) de la región.

Las estaciones de radio internacionales usan las bandas conocidas como ondas cortas (SW, Short Wave) en la banda de HF (High Frequency) que va desde los 3 MHz a los 30 MHz. Este tipo de ondas pueden ser radiadas a miles de kilómetros y son rebotadas de nuevo a la tierra por la ionosfera como si fuera un espejo, por tal motivo las estaciones de onda corta son escuchadas casi en todo el mundo. Los estaciones de FM (Frecuencia Modulada) y TV (Televisión) utilizan las bandas conocidas como VHF (Very High Frequency) y UHF (Ultra High Frequency) localizadas de los 30 MHz a los 300 MHz y de los 300 MHz a los 900 MHz, este tipo de señales debido a que no son reflejadas por la ionosfera cubren distancias cortas, una ciudad por ejemplo. La ventaja de usar este tipo de bandas de frecuencias para comunicaciones locales permite que docenas de estaciones de radio FM y televisoras " en ciudades diferentes " puedan usar frecuencias idénticas sin causar interferencia entre ellas.

1.5.5.2 Tarjeta de Red NIC (Network Interface Card)

Comúnmente mejor conocido como NIC es un dispositivo el cual permite que las computadores en una red LAN puedan estar interconectadas, las computadoras en una red de trabajo se comunican entre sí mediante protocolos para transmitir paquetes de datos entre diferentes maquinas conocidos como nodos. La Tarjeta de red sirve como un intermediario entre ellas para enviar y recibir datos en la LAN.

Regularmente el lenguaje o protocolo más usado para las redes LAN es el Ethernet o algunas veces se hace referencia al IEEE 802.3, en ocasiones también se puede hacer mención del protocolo Token Ring. Las tarjetas de red deben ser instaladas en cada una de las computadoras y todas las tarjetas deben ser de la misma arquitectura para evitar conflictos. Un Ethernet de red interfaz de la tarjeta se instala en una ranura libre en el interior del equipo. El NIC asigna una dirección única llamada dirección MAC (Media Access Control) de la máquina. Las MACs en la red se utilizan para dirigir el tráfico entre los equipos.

Un PCMCIA tarjeta de red, o tarjeta de PC, permite a los ordenadores portátiles conectarse a Internet y a redes de área local (LAN) a través de un CAT-5 Ethernet de cable o de radio inalámbrica. Una tarjeta de red PCMCIA abarca una multitud de tecnologías de red, incluyendo un módem, fax, Ethernet y adaptadores inalámbricos. Al usar una tarjeta de red PCMCIA, las computadoras pueden comunicarse con otros dispositivos conectados a la red y acceder a la Web. Las tarjetas de red facilitan una variedad de funciones, incluyendo la transferencia de archivos, navegación web y uso compartido de recursos entre sistemas.

Figura 15 Puntos de acceso.

1.5.5.3 Access Point (AP)

Un punto de acceso (AP, o también "WAP" para "punto de acceso inalámbrico") es un nodo responsable de la formación de una red inalámbrica a través de la conexión entre los dispositivos de comunicación inalámbricos. Actúa como un transmisor central y receptor de señales de radio inalámbricas, y se configura a través de un protocolo de Internet (IP).

Los modelos más antiguos de los puntos de acceso sólo pueden soportar un máximo de 10 a 20 clientes, mientras que los modelos más recientes son capaces de soportar hasta 255 clientes. El punto de acceso es capaz de transmitir datos entre dispositivos inalámbricos y dispositivos de cableado, y también es capaz de conectarse a una red de área local de cable (LAN)

El uso de dispositivos WAP también ofrecen una mayor movilidad que el uso de ordenadores cableados a la pared.

Figura 16 Puntos de acceso

WAP tiene sus desventajas. La seguridad que manejan en una principio era un cifrado WEP el cual sus contraseñas han pasado a ser vulnerables y fáciles de obtener actualmente ya la mayoría de dispositivos manejan Cifrado WPA y WPA2 que es más robusto, más seguro y más difícil de vulnerar. Por otro lado los primeros Access Point tenían algunos problemas de interferencias, ya que muchos dispositivos, como teléfonos inalámbricos y hornos de microondas, operan a una frecuencia de 2,4 GHz Esta interferencia puede obstaculizar la fuerza de la señal en una red inalámbrica actualmente ya pueden trabajar en dual Band a 2.4 y 5 GHz.

1.6 Cableado Estructurado

Es el cableado de un edificio o una serie de estos, el cual permite interconectar un conjunto de equipos activos de igual o diferente tecnología permitiendo la optimización e integración de diferentes servicios que dependen del tendido de los cables como el video, datos, audio o la voz. Su objetivo principal es cubrir las necesidades de los usuarios para que en la medida que esté en dicho edificio no se tenga que hacer ninguna modificación y así evitar más gastos.

Ventajas del Cableado estructurado

- Modularidad: Capacidad de integrar varias tecnologías sobre el mismo cableado: voz, datos, video.
- Fácil Administración: El cableado estructurado se divide en partes manejables que permiten hacerlo confiable y perfectamente administrable, pudiendo así detectar fallas y repararlas fácilmente.
- Menores Costos: El costo inicial de un sistema de cableado estructurado puede resultar alto, pero este hará ahorrar dinero durante la vida útil del sistema.

Organismos y Normas

ANSI: (American National Standards Institute. Organización "Instituto Nacional Estadounidense de Estándares"): Es una Organización Privada sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización voluntaria del sector privado de los Estados Unidos.

EIA: (Electronics Industry Association "Alianza de Industrias Electrónicas"): Fundada en 1924. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.

TIA: (Telecommunications Industry Association "Asociación de la Industria de las Telecomunicaciones"). Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.

ISO: (International Standards Organization "Organización Internacional de Normalización"). Organización no gubernamental creada en 1947 a nivel Mundial, de cuerpos de normas nacionales, con más de 140 países.

IEEE: (Institute of Electrical and Electronics Engineers "Instituto de Ingenieros Eléctricos y de Electrónica"). Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet, 802.5 Token Ring, ATM y las normas de Giga bit Ethernet.

Todas estas Instituciones se encargan de regular y aprobar las normas para poder hacer un estándar posteriormente y así facilitar la implementación de algún cableado.

Normas

ANSI/TIA/EIA-568-B Nos indica como instalar cableado. (Cableado de Telecomunicaciones en Edificios Comerciales).

TIA/EIA 568-B1 Requerimientos generales.

TIA/EIA 568-B2 Componentes de cableado mediante par trenzado balanceado.

TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.

ANSI/TIA/EIA-569-A Nos indica cómo enrutar el cableado

Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales

ANSI/TIA/EIA-570-A

Normas de Infraestructura Residencial de Telecomunicaciones.

ANSI/TIA/EIA-606-A

Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales

ANSI/TIA/EIA-607

Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.

ANSI/TIA/EIA-758

Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

Normas ISO de Cableado:

- ISO/IEC 118011: Sistemas de cableado genéricos
- ISO/IEC 14763-1: Administración y documentación
- ISO/IEC 14763-2: Planificación e Instalación.
- ISO/IEC 14763-3: Mediciones de cableado de fibra óptica.
- IEC 61935-1: Especificaciones para las mediciones de cableado de comunicaciones balanceado

Componentes del cableado estructurado:

- Área de trabajo.
- Cableado horizontal.
- Armario de telecomunicaciones (racks, closet).
- Cableado vertical.
- Sala de equipos.
- Backbone de Campus.

En conjunto, a todo el cableado de un edificio se llama SISTEMA y a cada parte en la que se subdivide se llama Subsistema. Se llama estructurado porque obedece a esta estructura definida.

1.6.1 Medios de Transmisión

Uno de los aspectos más importantes que todo administrador de sistemas o redes, debe conocer plenamente son todos los detalles de cada uno de los medios de comunicaciones empleados en redes ya que sin el buen conocimiento de causa, sería muy fácil perderse en todo lo que concierne a los términos y productos de una red.

Ancho de Banda: Es la medida de la capacidad de un sistema de transmisión. El ancho de banda se mide en Hertz

Atenuación: propiedad física del medio de tx, que disminuye los diferentes componentes de frecuencia (cn) en distinto grado, causando distorsión.

Tasa de Señalización: o de Modulación (Baud Rate: r en Baudios o pulsos/s), cantidad veces por segundo que la señal cambia su valor, no siempre igual a Rb.

Tasa de Datos o de Bits (Bit Rate): Rb en bits/s o bps, tasa a la que se transmiten los datos, según esquema de codificación de los niveles discretos de voltaje.

1.6.1.1 Cable Coaxial

El cable coaxial es la forma de cableado preferida desde hace tiempo por el simple hecho de que es barato y fácil de manejar (debido a su peso, flexibilidad, etc.). Un cable coaxial está compuesto por un hilo de cobre central (denominado núcleo) que está rodeado por un material aislante y luego, por una protección de metal trenzada.

Gracias a la protección, el cable coaxial se puede utilizar para cubrir grandes distancias y a altas velocidades (a diferencia del cable par trenzado). Sin embargo, se suele utilizar con mayor frecuencia para instalaciones básicas.

1.6.1.2 Par trenzado

En su forma más simple, el cable de par trenzado consiste en dos hilos de cobre trenzados dentro de un cordón y cubiertas por un aislante.

Generalmente se reconocen dos tipos de cables de pares trenzados:

- Par trenzado protegido (STP, por sus siglas en inglés (Shielded Twisted Pair)),
- Par trenzado no protegido (UTP, por sus siglas en inglés (Unshielded Twisted-Pair)).

Habitualmente, el cable está compuesto por varios pares trenzados agrupados todos juntos dentro de una funda de protección. La forma trenzada elimina el ruido (interferencia eléctrica) debido a pares adyacentes u otras fuentes de interferencia (motores, relés, transformadores).

Por lo tanto, el par trenzado es adecuado para una red local que tenga pocos nodos, un presupuesto limitado y una conectividad simple. Sin embargo, en distancias largas y a altas velocidades, no garantiza la integridad de los datos (es decir, que no haya pérdida en la transmisión de datos).

Para cableado estructurado de edificios comerciales, se definen varias categorías de cables de par trenzado.

- Cat.1: Cable telefónico tradicional con velocidades de 512 Kb/s.
- Cat.2: Certificado para transmitir datos hasta 4 Mbps UTP.
- Cat.3: Se utiliza en redes 10Base-T y puede transmitir datos a velocidades de hasta 10 Mbit/s.
- Cat.4: Se utiliza en redes Token Ring. Puede transmitir hasta 16 Mbps.
- Cat.5: Puede transmitir datos a velocidades de hasta 100 Mbit/s
- Cat.6: Redes de alta velocidad hasta 1 Gbit/s.
- Cat.6A: Redes de alta velocidad hasta 10 Gbit/s
- Cat.7: Fue creado para permitir 10 Gigabit Ethernet sobre 100 metros de cableado de cobre.

1.6.1.3 Fibra Óptica

El cable de fibra óptica tiene numerosas ventajas:

- Poco peso
- Inmunidad al ruido
- Baja atenuación
- Soporta una transferencia de datos que ronda el orden de los 100 Mbps
- Ancho de banda que va desde decenas de Mega Hertz hasta varios Giga Hertz (fibra mono modo)

La capacidad de transmisión de información que tiene una fibra óptica depende de tres características fundamentales:

a) Del diseño geométrico de la fibra
b) De las propiedades de los materiales empleados en su elaboración. (Diseño óptico)
c) De la anchura espectral de la fuente de luz utilizada. Cuanto mayor sea esta anchura, menor será la capacidad de transmisión de información de esa fibra.

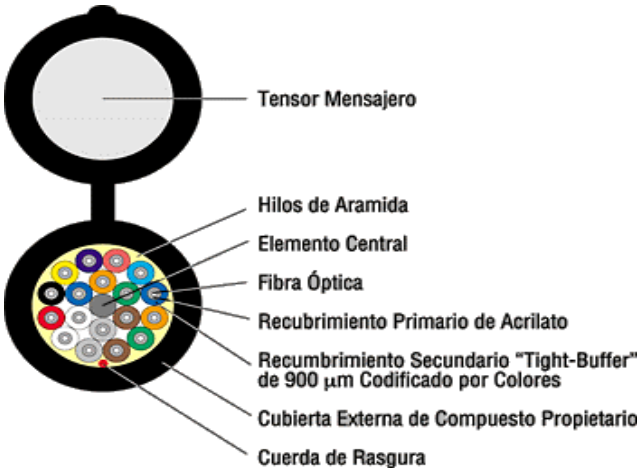

Figura 17 Componentes de la Fibra Óptica.

El cableado de fibra óptica es particularmente apropiado para conexiones entre distribuidores (una conexión central con varias construcciones, conocida como columna vertebral) ya que permite conexiones a través de grandes distancias (desde unos pocos kilómetros hasta 60 km., en el caso de la fibra de modo único) sin necesitar una conexión a tierra. Además, este tipo de cable es muy seguro ya que resulta extremadamente difícil perforarlo.

Sin embargo, a pesar de su flexibilidad mecánica, este tipo de cable no es apropiado para conexiones de redes locales ya que es muy difícil de instalar y además es muy costoso. Por este motivo, se prefieren pares trenzados o cables coaxiales para conexiones cortas.

1.6.1.3.1 Tipos de fibra óptica

Las fibras ópticas se clasifican de acuerdo al modo de propagación que dentro de ellas describen los rayos de luz emitidos. En esta clasificación existen tres tipos.

Mono modo: En este tipo de fibra, los rayos de luz transmitidos por la fibra viajan linealmente. Este tipo de fibra se puede considera como el modelo más sencillo de fabricar, y sus aplicaciones son concretas.

Multimodo de Índice Gradiente Gradual: Estos tipos de fibras son más costosas, y tienen una capacidad realmente amplia. Tienen una banda de paso que llega hasta los 500MHz por kilómetro La tecnología de fabricación de las mismas es realmente importante. Sus costos son elevados ya que el índice de refracción del núcleo varía de más alto, hacia más bajo en el recubrimiento. Este hecho produce un efecto espiral en todo rayo introducido en la fibra óptica, ya que todo rayo describe una forma helicoidal a medida que va avanzando por la fibra.

Multimodo de índice escalonado: Este tipo de fibra, están fabricadas a base de vidrio, con una atenuación de 30 dB/km, o plástico, con una atenuación de 100 dB/km. Tienen una banda de paso que llega hasta los 40 MHz por kilómetro. La producción de las mismas resulta adecuada en cuanto a tecnología y precio se refiere. No tiene una capacidad tan grande, pero

la calidad final es alta. El índice de refracción del núcleo es uniforme para todo el mismo, en realidad describe la forma general de la fibra óptica

1.6.2 Componentes de una Red

Dentro de la infraestructura de red existen diversos componentes que la integran y hacen posible que funcione en óptimas condiciones los cuales detallaremos brevemente en este apartado.

1.6.2.1 Hub

También conocido como concentrador se encarga de tomar los paquetes que llegan hasta una de sus entradas y enviarlos por el resto, de manera que las estaciones que se encuentran a la escucha las reciban. El inconveniente es que llegan hasta todas ellas los paquetes y no sólo hasta la interesada. Esto hace que se ocupen todas las líneas de paquetes que no se aprovechan en general y disminuye el ancho de banda de la transmisión. Un Hub trabaja en la capa 1 del modelo OSI debido a que trabajan como repetidores.

1.6.2.2 Switch

Realiza la misma tarea que un Hub, sin embargo ellos permiten segmentar los dominios de colisiones de una LAN, en pequeños dominios de colisiones. Cada puerto del switch representa un dominio de colisión separado que proporciona los medios completos para el nodo o nodos que están conectados en ese puerto. Los switches conectan segmentos de red de una LAN, usan una tabla de direcciones MAC para determinar el segmento al cual serán enviados los datos. Aunque su finalidad principal es garantizar la interconexión de dos segmentos de red hoy en día ya podemos encontrar switches con la capacidad de poder actuar como un Router o hacer VLAN y trabajar en la capa 3, incluso ya existen algunos con la capacidad de implementar políticas y filtros.

1.6.2.3 Router

Traducido significa ruteador o encaminador lo que podemos interpretar como simplemente guía. Se trata de un dispositivo inteligente, en el cual cuando recibe un paquete hacia un destinatario, la primera vez lo envía por todos los caminos posibles, y cuando recibe la verificación de por dónde se encuentra el destinatario, "se anota el camino", y en las veces sucesivas lo envía solamente por el camino correcto y no por todos los posibles. El Router permite la interconexión de redes LAN y su función es la de guiar los paquetes de datos para que fluyen hacia la red correcta e ir determinando que caminos debe seguir para llegar a su destino, básicamente para los servicios de Internet, los cuáles recibe de otro dispositivo como un módem del proveedor de

Internet de banda ancha. El Router trabaja en la capa de red del modelo OSI es decir que trabaja a nivel de IP´s. Existen diferentes protocolos de enrutamiento los cuales proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes routers de la red. Podemos decir que existen dos principales tipos de enrutamiento: el estático y el dinámico, el primero se configura manualmente a diferencia del dinámico, que se intercambian las tablas de enrutamiento mediante actualizaciones periódicas. La diferencia principal entre ellos es que el enrutamiento dinámico es escalable y adaptable

Clasificación de protocolos de enrutamiento dinámico

Los protocolos de enrutamiento se pueden clasificar en diferentes grupos según sus características. Los protocolos de enrutamiento que se usan con más frecuencia son:

• RIP: un protocolo de enrutamiento interior vector distancia.

• OSPF: un protocolo de enrutamiento interior de link-state.

• EIGRP: el protocolo avanzado de enrutamiento interior vector distancia desarrollado por Cisco.

• BGP: un protocolo de enrutamiento exterior vector ruta.

1.6.2.4 Gateway

También conocida como puerta de enlace. Es un dispositivo el cual nos permite tener interconexión entre distintas redes sin importar que sean de protocolos distintos o de arquitecturas diferentes este tipo dispositivo es el encargado de hacer la traducción entre diferentes dispositivos, por lo cual admite que las maquinas en una red Local puedan tener acceso a una red exterior mediante una traducción de IP´s o también conocido como NAT en la cual se aplica la técnica de enmascaramiento de ir que es regularmente usada para que los propios equipos de la red local compartan una única conexión a internet a través de una misma dirección.

1.6.2.5 Firewall

Es un sistema de hardware o software que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros los cuales generalmente vienen desde internet. Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Este tipo de aparatos también nos sirven como Gateway; como ya hemos mencionado nos permiten interconectar distintas redes.

1.6.2.6 Servidores

Es uno de los principales y más importantes componentes que forman parte de una red ya que es el encargado de proveer servicios a otros computadores denominados clientes los cuales son aquellos que hacen las peticiones al servidor de un determinado recurso para poder realizar alguna actividad, el servidor generalmente siempre está en espera de estas peticiones cuando esta llegue al puerto esperado y si se ajusta a las condiciones del protocolo, entonces autoriza para poder ejecutar un servicio. Debido a esto existe una gran diversidad de tipos de servidores a continuación hablaremos de algunos de los más importantes.

1.6.2.6.1 Tipos de Servidores por Funcionalidad

Servidores FTP (File Transfer Protocol "Protocolo de Transferencia de Archivos"). Es un protocolo de transferencia que nos permite mover archivos de manera rápida y fiable entre distintas computadoras proporcionando seguridad. Emplea los puertos 20 para Transferir datos. Y 21 para el envío de órdenes. Es de los servicios con mayor tiempo en Internet. Los servidores ftp soportan SSL/TLS y utilizan el mismo tipo de cifrado presente en los sitios web seguros.

Servidor de Base de datos: Aunque su función de almacenamiento y administración de una base de datos parezca muy simple es muy importante contar con un servidor de este tipo ya que nos permiten almacenar información en grandes cantidades de manera jerárquica, segura y ordenada.

Servidores de Correo. Sin duda es uno de los tipos de servidores más conocidos y más importantes dentro de una organización en él se gestionan y almacenan los correos electrónicos ya sea a través de una red local o por medio del internet, con independencia de la red que los usuarios utilicen para ello se basa en diferentes Protocolos como: el SMTP el POP3 y IMAP.

Servidores Proxy. Los servidores proxy generalmente se ubican entre un programa del cliente el cual normalmente es un navegador y un servidor externo que habitualmente es otro servicio web el Proxy entonces nos ayudara para filtrar peticiones, poder mejorar el funcionamiento y también compartir conexiones.

Servidores Web: De manera general, un servidor web o web hosting sirve como contenido estático a un navegador, el cual básicamente está a la espera de una petición para entregar como resultado información o una página web a través de un navegador a un usuario final. El protocolo que maneja este tipo de servicio es el HTTP el cual es el encargado de ser el intérprete entre el usuario y el servidor.

Servidor RAS: Un servidor RAS es una computadora especialmente dedicada para el acceso remoto de igual modo responden llamadas telefónicas entrantes o reconocen la petición de la

red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red.

1.6.2.6.2 Tipos de Servidores según su Arquitectura

Servidor Clúster. A diferencia de los servidores de datos este tipo de servidores es un conjunto de servidores que trabajan como uno un solo sistema que está dedicado y especializado de igual forma para el almacenamiento de información; de gran capacidad con la ventaja de que nos permiten evitar pérdida de información por problemas de otro servidor

Blade. Este tipo de servidores son de los más recientes básicamente podemos decir que es un tipo de computadora la cual ha sido diseñada para los bastidores y en ellos aprovechar el espacio, reducir el consumo, simplificar la administración debido a que en él podemos alojar diversos servidores; cada servidor blade es una delgada tarjeta que contiene únicamente microprocesador, memoria y buses.

Entre sus principales usos y ventajas de un blade es para uso en instalaciones de entornos de virtualización, en clúster y para web hosting.

1.7 Redes Virtuales

Las redes virtuales hoy en día suponen una gran ventaja para cualquier empresa ya que además de poder compartir información nos permiten obtener grandes ahorros no solo económicos ya que también nos ayudan a ahorrar espacios además de facilitar la administración, disminuir el tráfico en la red y aumentar la seguridad dentro de nuestros sistemas.

Es bien sabido que la Internet es una red pública y abierta, su transmisión de los datos se realiza a través de la creación de túneles criptográficos para que las organizaciones puedan establecer conexiones de red seguras de un lado a otro.

1.7.1 VPN (Virtual Private Network “Red Privada Virtual”)

La tecnología VPN nos proporciona conectividad de acceso remoto desde casi cualquier lugar con conexión a Internet. Existen diferentes protocolos para conectar una VPN generalmente a través de un cliente, entre los principales protocolos y más conocidos encontramos a IPSec, SSL, PPT, L2TP o bien los túneles GRE que es propietario de Cisco.

La función principal de implementar este tipo de tecnología es que reduce gastos en la infraestructura, es más fácil de escalar que una red WAN tradicional y nos proporciona mayor seguridad.

1.7.1.1 Ventajas de una VPN

Como ya hemos dicho la principal ventaja de usar una VPN es que nos permite disfrutar de una conexión a red con todas las características de la red privada a la que queremos acceder. Nuestro cliente VPN va a adquirir totalmente la condición de miembro de esa red, con lo cual podemos aplicarle todas las directivas de seguridad y permisos de un ordenador en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, e información en general se desee compartir a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizaran usando los recursos y conexiones que tenga la red privada.

1.7.1.2 Clasificación de las Redes Privadas Virtuales:

- VPN´s dé Sitio a Sitio: Son el sucesor de las redes de área extensa (WAN) y se utilizan entre puntos fijos, que están conectados permanentemente.
- VPN's dé Acceso Remoto: La evolución del servicio de acceso remoto (RAS) mediante módem, permiten el acceso a la red de la empresa desde cualquier lugar del mundo por el precio de una llamada local.
- VPN's Mixtas: Son el caso más normal, redes con usuarios fijos, conectados siempre a ellas, como empresas con delegaciones dispersas, y con usuarios móviles, como consultores, que necesitan trabajar con los datos corporativos en cualquier lugar del mundo, pero a un coste moderado.

1.7.2 VLAN´s (LAN´s Virtuales)

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física es decir que a pesar de estar interconectados en diferentes equipos o zonas pertenecen a la misma red.

Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, o limitaciones de dirección, ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo.

1.7.2.1 Tipos de VLAN

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

- La VLAN de nivel 1 (También denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador;
- La VLAN de nivel 2 (También denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación;
- La VLAN de nivel 3: existen diferentes tipos de VLAN de nivel 3:

La VLAN basada en la dirección de red conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

La VLAN basada en protocolo permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

Capítulo 2 Telefonía IP

2.1 Telefonía

La telefonía a lo largo de los años ha sufrido bastantes cambios; la historia nos dice que desde mediados del siglo XIX Antonio Santi Giuseppe Meucci hiciera las primeras pruebas de lo que hoy conocemos como el Teléfono en aquel entonces conocido como teletrófono el cual surgió debido a que su esposa estaba enferma y Meucci necesitaba mantener comunicación con ella desde su laboratorio hasta su dormitorio en ese entonces ya se contaba con el telégrafo en donde se trasmitían impulsos eléctricos y letras para enviar mensajes en largas distancias en ese entonces; el reto seria trasmitir la voz humana con esas señales eléctricas a través de cableado; para 1871 ya tenía perfeccionado este dispositivo pero por falta de dinero y de interés de la compañía Western Unión en el año de 1874 quienes no se interesaron en ese proyecto; debido a esto no pudo darle seguimiento y es así que dos años más tarde Alexander Graham Bell patentara este descubrimiento es por ello que mucha gente le atribuyera el invento del teléfono pero también hay quienes dicen que fue Antonio Meucci el verdadero inventor del teléfono. En la figura 18 se muestra el diseño de Meucci.

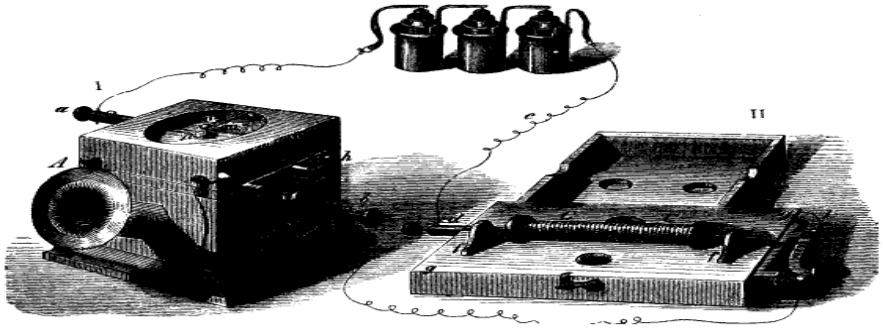

Figura 18 Teléfono de Antonio Meucci

Sin embargo el gran reto del teléfono seria la interconexión de diferentes aparatos fue en el año de 1878 que se gestó la primera conexión publica en los Estados Unidos cuando una central telefónica o de comunicación era la que hacia manualmente la distribución de las llamadas de diferentes usuarios lo que hoy en día conocemos como conmutación y que actualmente se hace de forma automática.

Otra característica importante que se tiene que analizar dentro del rubro de la telefonía son las distancias ya que como hemos mencionado en un principio solo se utilizaban cables para poder llevar la voz a través de ellos cuando se trataba de distancias cortas; actualmente cuando se

trata de largas distancias se suele utilizar la radio o satélites artificiales para lograr la comunicación.

Pero sin duda uno de los avances más importantes que ha surgido dentro del ámbito de las comunicaciones telefónicas es el haber logrado realizar que estos aparatos fueran autónomos y por medio de una batería logran emitir señales que se han vuelto electromagnéticas; estos aparatos mejor conocidos como celulares han revolucionado la industria telefónica y finalmente otro de los grandes avances es el hecho de hacer posible la comunicación por internet y el envío de paquetes de voz a través de redes de datos que es lo que llamamos Voz sobre IP (VoIP) todo esto y más lo iremos viendo a lo largo de este capítulo.

2.1.2 Arquitecturas de las redes telefónicas tradicionales existentes

Los sistemas de telefonía tradicional están guiados por un sistema muy simple pero ineficiente denominado conmutación de circuitos. La conmutación de circuitos ha sido usada por las operadoras tradicionales por más de 100 años. En este sistema cuando una llamada es realizada la conexión es mantenida durante todo el tiempo que dure la comunicación. Este tipo de comunicaciones es denominado "circuito" porque la conexión está realizada entre 2 puntos hacia ambas direcciones. Estos son los fundamentos del sistema de telefonía convencional.

La Red Telefónica Básica (RTB) fue creada para transmitir la voz humana. Tanto por la naturaleza de la información a transmitir, como por la tecnología disponible en la época en que fue creada, es de tipo analógico.

La tecnología que se utiliza hoy en día para transportar voz en las redes telefónicas se conoce como «conmutación de circuitos». Se basa en el principio de reservar un recurso (circuito) para una llamada desde el momento de su establecimiento hasta su conclusión. El tamaño de este recurso, expresado como una velocidad binaria desde la digitalización de las redes telefónicas, es 64 kbps. Este límite fue escogido en su momento porque permitía la digitalización eficaz de las muestras de la voz humana, cuyo espectro va de 300 a 3400 Hz.

Cada línea RTB tiene asignada una numeración específica (su número telefónico) y está físicamente construida por dos hilos metálicos (conocidos como par de cobre), que se extienden desde la central telefónica hasta la instalación del abonado (se conoce también como bucle de abonado). Cada central atiende las líneas de abonado de un área geográfica determinada. A su vez, las centrales telefónicas están unidas entre sí por sistemas más complejos y basados en tecnología digital. Esta unión de centrales constituye el sistema telefónico nacional que a su vez está enlazado con los restantes del mundo. Ejemplo de 6arquitectura RTB se muestra en la figura 19.

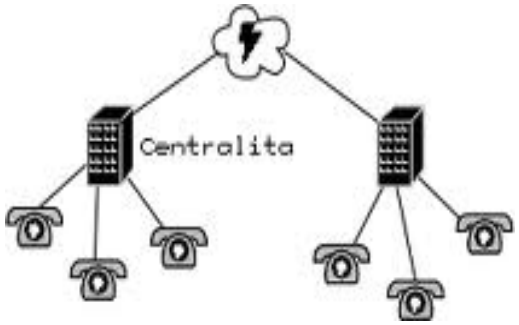

Figura 19 Arquitectura RTB

En los años 60 las centrales telefónicas, mayoritariamente analógicas, fueron transformando su tecnología a digital. Ello solventó diversos problemas, como los relacionados con la degradación de la señal de voz y la imposibilidad de manejar gran cantidad de llamadas. Del mismo modo, la intención fue también digitalizar el bucle local pero por motivos meramente económicos el bucle local continuó siendo analógico.

Finalmente, la medida que se adoptó fue la de digitalizar la comunicación entre las centralitas telefónicas, manteniendo el bucle local analógico, y obteniéndose así los beneficios de la telefonía digital a un precio razonable. Esta medida dio lugar a lo que se conoce como RDI "Red Digital Integrada".

La situación actual para la RTB puede clasificarse como híbrida; lo normal es que la transmisión sea todavía analógica en los bucles de abonado de ambos extremos y digital en su tráfico entre centrales (esto requiere una doble conversión, analógico-digital y digital analógico).

Para su digitalización, la señal analógica es muestreada a 8.000 veces por segundo

(8 KHz.). El valor de cada muestra puede ser un valor entre 0 y 255 (puede ser representado por 1 byte -octeto-) lo que supone un flujo de datos de 8 KB/s o 64 Kb/s, lo cual se denomina calidad de sonido telefónico

2.1.3 Red Digital de Servicios Integrados ISDN

Se define la RDSI (Red Digital de Servicios Integrados, en ingles ISDN Integrated Services for Digital Network) Está definida por la normalización de interfaces de usuario aportada por la ITU-T, y se implementa como un conjunto de conmutadores digitales y caminos admitiendo un amplio rango de tipos de tráfico y suministrando servicios de procesamiento de información que presta conexiones extremo a extremo a nivel digital y es capaz de ofertar diferentes servicios como son télex, voz, conmutación de circuitos, videoconferencia, conexión a Internet, opciones como llamada en espera, identidad del origen conmutación de paquetes con una transmisión digital que integra señales analógicas mediante la transformación analógico-digital que ofrece una comunicación a 64 kbps con este tipo de red permite la conexión de múltiples dispositivos

Con líneas analógicas resulta necesario disponer de una línea por cada dispositivo del usuario, si estos se quieren emplear simultáneamente por ello resulta muy caro enviar datos (archivos o vídeo) mientras se mantiene una conversación hablada. Por otra parte, se requieren diferentes interfaces para emplear diferentes dispositivos al no existir estándares al respecto. Con la RDSI es posible combinar diferentes fuentes de datos digitales y hacer que la información llegue al destino correcto.

Como la línea es digital, es fácil controlar el ruido y las interferencias producidos al combinar las señales. Además, las normas de la RDSI especifican un conjunto de servicios proporcionados a través de interfaces normalizados.

En una conexión RDSI, la llamada se establece enviando un paquete de datos especial a través de un canal independiente de los canales para datos. Este método de llamada se engloba dentro de una serie de opciones de control de la RDSI conocidas como señalización, y permite establecer la llamada en un par de segundos. Además informa al destinatario del tipo de conexión (voz o datos) y desde que número se ha llamado, y puede ser gestionado fácilmente por equipos inteligentes como un ordenador.

Actualmente la RDSI ha evolucionado a RDSI de Banda ancha ofreciendo velocidades de 2 Mbps y hasta los 200 Mbps en México (servicio otorgado por Axtel) con lo cual permite aumentar en gran medida el número de servicios que la red puede ofrecer.

2.1.4 ADSL Asymmetric Digital Subscriber Line

También conocida como Línea de abonado digital asimétrica es una tecnología para módems, que proporciona un acceso asimétrico y de alta velocidad a través de un par simétrico de cobre actualmente podemos verlo instalado en oficinas y casas de los usuarios de la RTB (o bien de la RDSI, con la cual también es compatible) como ya hemos visto el hecho de poder acceder a diferentes servicios integrados ha traído como resultado que estos sean insuficientes para una conexión a internet de los usuarios con lo cual requieren mayor ancho de banda y así disfrutar de los contenidos multimedia; debido a que es una tecnología que proporciona acceso a internet de banda ancha con velocidades mayores a las de un modem ya que estos utilizaban la banda de voz con lo cual se obstruía el servicio de voz mientras este en uso o viceversa esta es una de las principales ventajas de esta tecnología ya que permite que los usuarios de ADSL pueden utilizar simultáneamente el teléfono e Internet con ayuda de un micro filtro que ayudan a eliminar los posibles ruidos que puedan generar otros dispositivos.

Las velocidades de transmisión depende de la calidad de los cables de cobre tradicionalmente se manejaba que eran de 1,5 Mbps sobre distancias de 6 Km, y de hasta 8 Mbps para distancias de 3 km.

Las velocidades máximas descendentes (desde el usuario a la central), iban de 16-640 Kbps actualmente existen mejoras sobre este servicio ofreciendo velocidades que pueden alcanzar hasta 40 Mbps de bajada y 8 Mbps de subida lo que ahora se conoce como el ADSL2+ con capacidad de suministro de televisión y video de alta calidad por el mismo par telefónico. Como podemos ver este tipo de transmisión es asimétrica se diseñó así porque generalmente los usuarios reciben más información de la que envían sin embargo esto analizaremos más adelante.

2.2 Central de Comunicación

Las primeras centrales telefónicas, y así fue durante mucho tiempo, constaban de una mesa de conexiones en la que cada uno de los conectores correspondía a un abonado. Cuando una abonado quería llamar a otro, generaba una señal mediante una manivela en su teléfono y una operadora le respondía desde la central. El abonado indicaba con qué otro abonado deseaba hablar y la operadora conectaba un latiguillo entre los conectores de ambos abonados, cerrándose el circuito. En el caso de conferencias de larga distancia, se conectaban las centrales en cadena y una operadora comunicaba a la siguiente el destino de la llamada hasta cerrarse el circuito completo. En la figura 20 se observa el trabajo de las operadoras en esos años.

Figura 20 Operadoras en Central de comunicación

Posteriormente se diseñaron lo sistemas de conmutación de discos, que eran complejos sistemas electromecánicos de discos que giraban para hacer contacto entre los pares apropiados para cerrar los circuitos entre el abonado llamante y el llamado. En la actualidad el sistema es electrónico y la conmutación, aunque continúa siendo física se realiza de forma no mecánica. A un nivel más profundo, las comunicaciones entre centrales han dejado en muchos casos de ser analógicas para ser digitales de forma que con un menor despliegue material pueden establecerse muchas más llamadas simultáneas. Es lo que se conoce como multiplexación de un medio.

Con todos estos elementos ya disponemos de lo que se conoce como PSTN (Public Switched Telephone Network “Red Telefónica Pública Conmutada”)

Hoy en día resulta difícil de creer que una empresa pueda operar sin una central telefónica privada debido a todas las ventajas que esta proporciona.

2.2.1 Conmutador

Un centro de conmutación involucra un centro de transmisión, es decir, el equipo de conmutación se encarga de establecer las conexiones apropiadas para enrutar o dirigir la comunicación, a través de la red telefónica, hacia su destino correcto por la vía más adecuada; mientras que, el equipo de transmisión se encarga del envío de las señales de control y supervisión, así como del mensaje, asignándole a esta información un canal de comunicación que generalmente se proporciona mediante sistemas de onda portadora para las comunicaciones de larga distancia.

Los conmutadores locales reciben las líneas de abonado que van directamente a la casa u oficina. Entre conmutadores van conectadas varias líneas llamadas troncales que son un conjunto de enlaces para establecer las llamadas entre diferentes zonas. En total existen los conmutadores locales que conmutan la llamada dentro de la zona, conmutadores tándem que administran los circuitos entre varias centrales locales y conmutadores especiales para llamadas con tarifas y cargos extras al cliente.

Los conmutadores constan de un módulo administrador que se encarga de la tarificación, la traslación de la llamada, el ruteo entre troncales y otras especificaciones. Cada conmutador digital o ESS, utiliza switches y programas de control de almacenamiento según el tipo de servicio que esté prestando a la red. Algunos utilizan multicanalización en espacio, otros en tiempo y otros en frecuencia. La concentración de líneas para cada conmutador varía según la demanda. Los conmutadores reciben canales modulados a 64 kbps y transmiten entre ellos en canales de 2.56 Mbps. Existen conmutadores conectados por fibra óptica multimodo llevando consigo 32.768 Mbps.

2.2.2 Tipos de Conmutadores

Conmutadores de Pequeña Capacidad: En la actualidad podemos encontrar conmutadores o para aplicaciones muy pequeñas 3 x 8 es decir (3 Líneas 8 Extensiones), 1232 (12 Líneas 32 Extensiones) algunos de estos modelos pueden ser expandibles al máximo de su capacidad y son usados comúnmente en pequeñas compañías como Restaurantes, Puntos de Ventas, Tiendas departamentales, Moteles, Oficinas y Casas Habitación y/o condominios, Edificios departamentales. La mayoría de estos equipos siguen siendo Analógicos aunque en la actualidad los podemos encontrar digitales o bien híbridos.

Conmutadores de Media Capacidad

Los conmutadores de capacidades con más de 12 Líneas y 30 Extensiones ya se consideran de mediana capacidad las necesidades son diferentes por obvias razones en ellos nos encontramos con más tráfico de llamadas, entrantes e internas además de las salientes.

Los conmutadores recomendados para estos casos en su mayoría solían ser equipos digitales pero hoy en día la tecnología se empieza a inclinar a los conmutadores IP aunque algunas marcas están fabricando equipos híbridos que son Digital/IP otros le apuestan 100% a la tecnología IP. Las capacidades de estos equipos pueden llegar desde un E1 (30 líneas con 100 Números telefónicos) 600 extensiones, y son recomendados en Edificios comerciales como: Hospitales, oficinas, corporativos, entre otros.

Conmutadores de Alta Capacidad.

Estos conmutadores son capaces de manejar más de un E1 y pueden manejar miles de extensiones son básicamente usados en Campos industriales, Pequeñas ciudades, Complejos Turísticos, Plazas comerciales, oficinas gubernamentales o con varios edificios, al igual que los equipos de mediana capacidad son equipos digitales con tendencias a IP que como veremos más adelante manejan los protocolos SIP y H323.

2.3 Red Telefónica Pública Conmutada (RTPC) Public Switched Telephone Network (PSTN)

La red telefónica pública conmutada (PSTN, Public Switched Telephone Network) es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real. Cuando se llama a alguien, se cierra un conmutador al marcar y se establece así un circuito con el receptor de la llamada. La PSTN garantiza la calidad del servicio (QoS) al dedicar el circuito a la llamada hasta que se cuelga el teléfono. Independientemente de si los participantes en la llamada están hablando o en silencio, seguirán utilizando el mismo circuito hasta que la persona que llama cuelgue, existen 600 millones de usuarios alrededor del mundo. En la figura 21 se muestra un diagrama de lo que se explica de una PSTN

La infraestructura necesaria para ofrecer servicios de larga distancia son una red telefónica pública conmutada y los sistemas, procesos, y recursos humanos necesarios para explotar dicha red. La red es pública porque cualquier abonado debería poder suscribirse al Operador de la red, y éste a su vez debería poder completar llamadas a cualquier parte del mundo.

La red es telefónica porque sólo está diseñada para conectar circuitos de voz entre dos aparatos telefónicos. La transmisión de datos analógicos, por cierto, viene por añadidura, sin compromiso

ni obligaciones. Los circuitos sin conexión permanente típicamente no forman parte de la RTPC aunque la tecnología ATM (Asynchronous Transfer Mode “Modo de Transferencia Asíncrona”) puede encontrar rápidamente candidatos que sí lo justifican, por ejemplo, videoconferencia bajo demanda. Finalmente, la red es conmutada porque como ya hemos dicho los circuitos de voz se establecen mediante Centrales Telefónicas que conmutan los recursos de la red para establecer conexiones temporales a bajo costo para los usuarios.

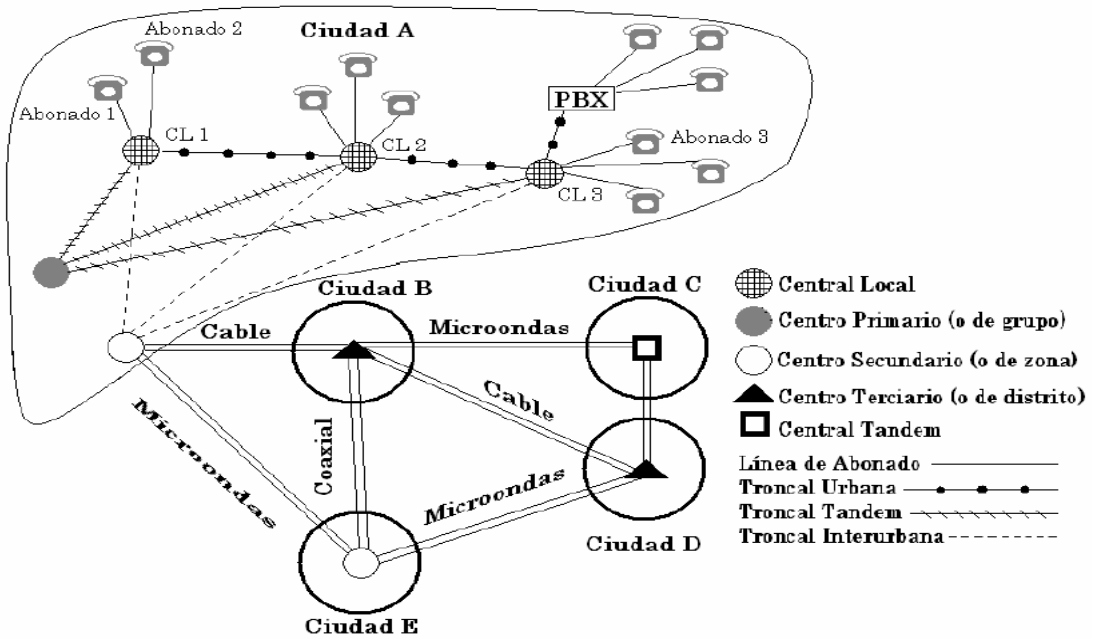

Figura 21 Diagrama de una RTPC.

Los elementos de conmutación cumplen una función muy sencilla en concepto: establecer una trayectoria de comunicación entre dos abonados.

Las Centrales Telefónicas frecuentemente recurren a equipos periféricos que agregan inteligencia o servicios a la red básica, por ejemplo, plataformas de operadoras, de tarjetas telefónicas, de detección de fraude, de red inteligente SCP (Service Control Point “Puntos de Control de Servicio”).

La señalización es el lenguaje que las centrales telefónicas utilizan para hablarse entre sí y para hablar con los equipos terminales de los abonados.

La transmisión se entiende como el medio físico que conduce las señales portadoras de voz o datos por la red así como también los equipos electrónicos del medio. El medio físico de transmisión puede ser aire, cable coaxial, fibra óptica, satélite, etc.

Los equipos electrónicos (sistemas) de transmisión optimizan el uso del ancho de banda disponible en el medio.

Los elementos de gestión mantienen vigilancia ininterrumpida sobre los elementos de red; proporcionan mecanismos automatizados, centralizados, y amigables para configurar los elementos de red; optimizan la administración de los recursos de conmutación y transmisión, y hacen eficiente el mantenimiento preventivo y reactivo de la red.

Los equipos terminales son propiedad de los abonados: desde los aparatos telefónicos, los equipos de fax, las estaciones de trabajo, computadoras personales o los conmutadores residenciales, hasta los complicados sistemas de telefonía privada de las grandes empresas. Mientras más robusto sea el sistema de telefonía privada de una empresa, menos servicios requiere la empresa del Operador telefónico

2.3.1 PBX

Un conmutador empresarial, también conocido como PBX (Prívate Branch Exchange, por las siglas en inglés) dimensionado a su máxima capacidad puede fácilmente dar servicio de larga distancia por sí solo, con un conjunto sustancial de características de procesamiento. La robustez del PBX se mide, por ejemplo, en el tratamiento de llamadas entrantes; el PBX puede mantener una cola de llamadas en espera si todas las líneas están ocupadas; puede desbordar llamadas a otro PBX si se exceden parámetros razonables de tiempo de espera; puede reproducir anuncios grabados en el contexto específico de cada llamada; puede ofrecer identificación de llamadas; puede ser interconectado con otros PBX, mediante enlaces privados, para crear una red privada con atributos deseables como marcación abreviada, buzón de mensajes de voz, códigos de autorización, ya hemos dicho que es la encargada de conmutar las llamadas pero además de eso tiene otras utilidades que a continuación describiremos, un PBX es una Central Telefónica que se conecta directamente a una red pública de telefonía a través de líneas troncales y se encarga de establecer conexiones entre terminales de una misma empresa, además de enlazar llamadas del interior con el exterior o bien tener acceso a una línea exterior.

Entre las principales funciones que realiza un PBX tenemos:

- Transferencia de llamadas
- Conferencias Permite que una llamada del exterior hable con varias extensiones
- Llamada en espera Permite que el sistema haga esperar si una extensión está ocupada hasta que esta quede libre
- Permite conocer el estado de las extensiones
- Desvió de llamadas en dado caso que no se encuentren en su lugar

2.4 Telefonía IP

La Telefonía sobre Internet o Telefonía IP, es un servicio de telecomunicaciones que posibilita a cualquier usuario efectuar llamadas telefónicas sobre redes que utilizan el protocolo de comunicación IP, es decir el protocolo por el cual la red Internet conecta las computadoras entre sí.

Estas comunicaciones desarrolladas a través de la red Internet son posibles gracias a un sofisticado mecanismo que permite que la voz (emitida por el usuario) sea digitalizada y empaquetada, como si fueran paquetes de texto, enviándose por la red y finalizando la comunicación en el destinatario final de la misma (a través de un proceso de desempaquetando y digitalizado para convertirlos nuevamente en voz.) Un ejemplo se muestra en la figura 22.

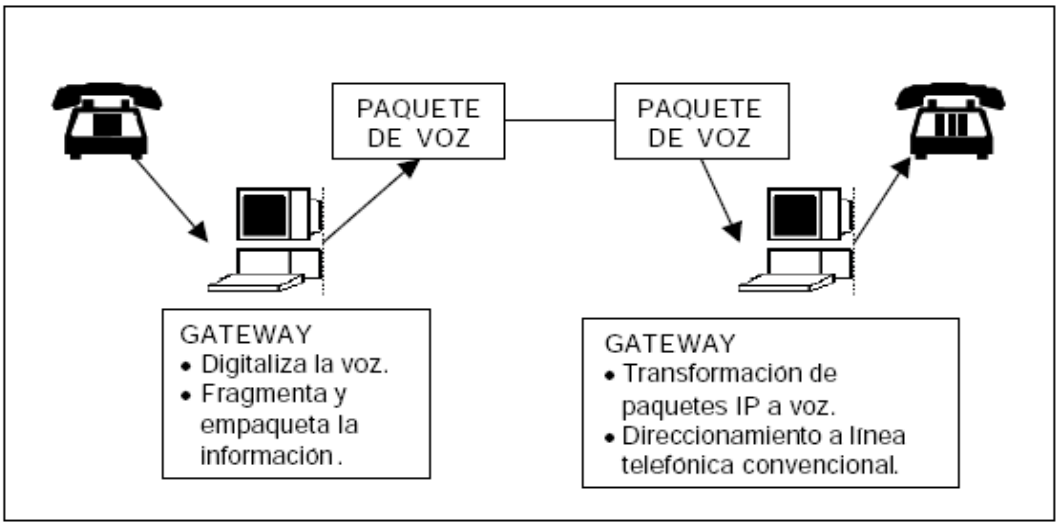

Figura 22 Transmisión de Voz-IP, IP-Voz.

La telefonía IP se compone de dos categorías: la transmisión de voz y la de datos. Se basan principalmente en transportar la voz convertida previamente en datos entre dos destinos distantes. Las redes que se han desarrollado a lo largo de los años para transmitir voz tales como CDMA (Code Division Múltiple Access “Multiplexación por División de Código”), TDMA (Time Division Multiple Access “Multiplexación por División de Tiempo”) GPRS (General Packet Radio Service “Servicio General de Paquetes vía Radio”) y ATM (Asynchronous Transfer Mode “Modo de Transferencia Asíncrona”), las cuales se basan principalmente en la conmutación de circuitos, es decir, para establecer una comunicación entre dos puntos se requiere mantener un circuito físico durante el tiempo de la llamada. Los recursos utilizados en una llamada no pueden ser usados en otra hasta que la primera no finalice. En la figura 23 se ejemplifica el proceso de la telefonía IP.

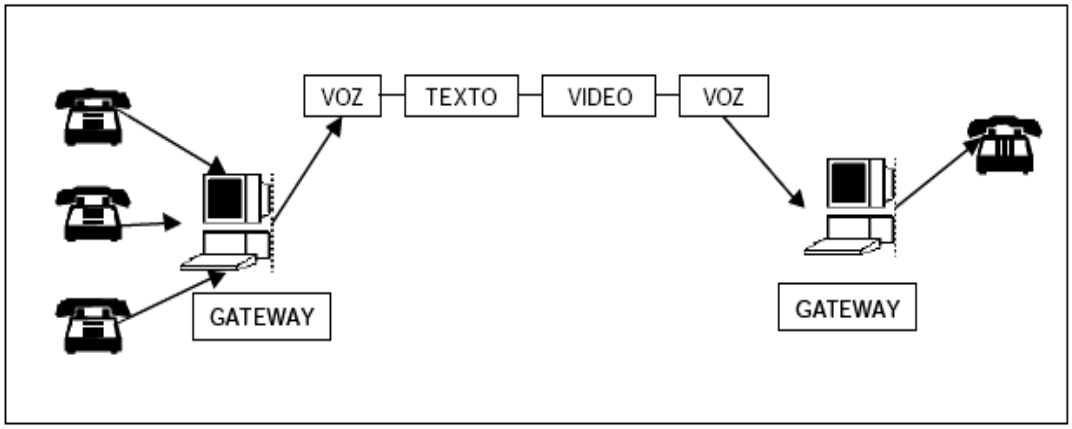

Figura 23 Transmisión de datos telefonía IP.

Por otro lado existen las redes de datos, la cuales se basan en el concepto de conmutación de paquetes, en otras palabras, se realiza un mismo enlace el cual contiene diferentes caminos entre el origen y el destino durante el tiempo que dura la llamada, mientras los recursos que intervienen en una conexión pueden ser utilizados por otras conexiones que se efectúen al mismo tiempo.

2.4.1. Clases de Telefonía IP

La telefonía IP a modo didáctico puede ser clasificada en base A:

La Naturaleza de Red IP: Tomando en cuenta la naturaleza de la Red IP se puede clasificar la Telefonía IP en Telefonía por Internet y VoIP. La primera utiliza principalmente la Internet Pública, mientras que la segunda utiliza redes privadas basadas en el IP.

Los medios utilizados:

De PC a PC conectados a Internet: Mediante el uso de computadoras multimedia, y con software compatibles que les permita a cada usuario directamente digitalizar y empaquetar la información cuando la envía, así como desempaquetarla y convertirla nuevamente en voz cuando la recibe, lográndose con ello entablar una conversación con otra similar ubicada en cualquier parte del planeta.

De PC a teléfono: el usuario que esté utilizando la PC requiere de un programa, o estar conectado a un Gateway que le permita digitalizar y empaquetar la voz, sin importar que el segundo esté conectado o sepa que se está utilizando el Internet para recibir la llamada.

De Teléfono a Teléfono: conecta una línea convencional de teléfono a un Gateway el cual digitaliza, fragmenta y empaqueta la voz, enrutándola a través de Internet hacia su destino, el

mismo que también cuenta con un Gateway que transforma los paquetes IP a voz y lo direcciona a la línea telefónica convencional.

Muestra de la comunicación entre diferentes dispositivos IP se observan en la figura 24.

Figura 24 Comunicación entre diferentes dispositivos IP.

En la telefonía IP existen diferentes elementos que son fundamentales para una conexión exitosa, tales como el Gateway, gatekeeper, señalización y codificación los cuales describiremos a continuación.

2.4.2.1 Gateway de Voz sobre IP

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI (Red Digital de Servicios Integrados). Podemos considerar al Gateway como una caja que por un lado tiene un interface LAN y por el otro dispone de uno o varios de los siguientes interfaces:

- FXO. Para conexión a extensiones de centralitas o a la red telefónica básica.
- FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
- E&M. Para conexión específica a centralitas.
- BRI. Acceso básico RDSI (2B+D)
- PRI. Acceso primario RDSI (30B+D)
- G703/G.704. (E&M digital) Conexión específica a centralitas a 2 Mbps

Los distintos elementos pueden residir en plataformas físicas separadas o también se puede encontrar varios elementos conviviendo en la misma plataforma.

2.4.2.2 Gatekeeper

EL Gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCU. El gatekeeper puede ofrecer también

otros servicios a los terminales Gateway y MCUs tales como gestión del ancho de banda y localización de los gateways

2.4.2.3 Señalización

La señalización es necesaria en cualquier sistema de telefonía debido a que en el momento en el cual un usuario marca un número de teléfono, se determine el estado a quién se llama (libre u ocupado) y se establezca la llamada. Dentro de estos protocolos se enmarcan el H.323 y el SIP (Session Initiation Protocol "Protocolo de Inicio de Sesión"), y el SS7 que es el que se encarga de la red PSTN (Public Switched Telephone Network).

2.4.2.4 SS7 Sistema de Señalización No. 7

Es un conjunto de protocolos utilizados para la Red Telefónica Pública Conmutada. En Telefonía "señalización" es el proceso de conexión y finalización de llamadas. La señalización SS7 se realiza fuera de la banda, lo que significa que los mensajes de señalización SS7 se transportan sobre una conexión de datos independiente, con lo cual se pueden comunicar grandes cantidades de información durante una llamada lo que permitió el desarrollo de diversos servicios relacionados con la llamada. Desvío de llamadas, llamada en espera, correo de Voz, visualización del número, identificador de llamadas y filtrado de llamadas son algunos de estos servicios.

2.4.2.5 Codificación

El proceso que nos permite hacer posible todo ese intercambio de información es la codificación sin ella no sería posible la comunicación de la voz humana, ya que la comprime y convierte en paquetes de datos para enviarlos por una red IP

2.5 Voz sobre IP (VoIP)

El VoIP (del inglés Voice Over Internet Protocol) se define como el envío de canales de voz en un tiempo real mediante diferentes redes utilizando el protocolo de Internet (IP), es decir, permite tener conversaciones con diferentes personas usando la red de Internet, la cual a través de los años se ha incrementado los anchos de banda permitiendo enviar mayor cantidad de información simultánea y rápidamente.

La función principal del VoIP es dividir en paquetes los flujos de audio para poder transportarlos sobre redes basadas en IP. Estos protocolos originalmente no fueron diseñados para la transmisión por lo tanto, se crearon otros cuyo mecanismo abarca una serie de transacciones

de señalización entre terminales que cargan dos flujos de audio para cada dirección de la conversación.

VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional.

Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- **Direccionamiento:**

1. RAS (Registration, Admission and Status “Registro Admisión y Estado”). Es un protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.

2. DNS (Domain Name Service”Servicio de Resolución de Nombres”) es el que nos traduce en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS

- **Señalización:**

1. Señalización inicial de llamada.

2. H.225 Este protocolo nos ayuda Control de llamadas: señalización, registro y admisión, empaquetamiento/sincronización del flujo de voz.

3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para flujos de voz.

- **Compresión de voz:**

1. Requeridos: G.711 y G.723.

2. Opcionales: G.728, G.729 y G.722

- **Transmisión de voz:**

1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

2. RTP (Real Time Transport Protocol “Protocolo de Transporte de Tiempo Real”). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción

- **Control de la transmisión:** RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

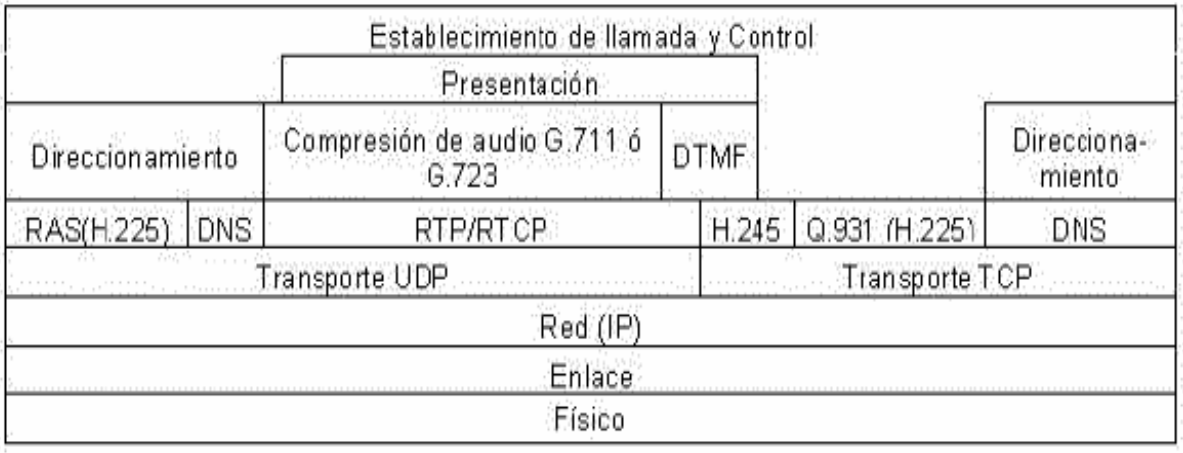

Figura 25 Trama de protocolo

El hecho de que VoIP se apoye en un protocolo de nivel 3, como es IP, permite una flexibilidad en las configuraciones que en muchos casos está todavía por descubrir, en la figura 25 se muestra la trama de este protocolo. Una idea que parece inmediata es que el papel tradicional de la centralita telefónica quedaría distribuido entre los distintos elementos de la red VoIP. En este escenario, tecnologías como CTI (Computer Telephony Integration "Integración de Telefonía Informática") tendrán una implantación mucho más simple. Será el paso del tiempo y la imaginación de las personas involucradas en estos entornos, los que irán definiendo aplicaciones y servicios basados en VoIP.

2.5.1 Proveedores de Servicios

Proveedor ISP: Un proveedor de servicios Internet (ISP) es una compañía que ofrece acceso a Internet, normalmente por una cuota. Normalmente, la conexión con el ISP tiene lugar a través de una conexión de acceso telefónico (línea telefónica) o una conexión de banda ancha (cable o ADSL). Muchos ISP ofrecen servicios adicionales, como cuentas de correo electrónico, exploradores web y espacio para crear un sitio web propio.[2]

Proveedores VoIP: La función de los proveedores de VoIP es la de ofrecer una infraestructura que pueda desviar y conectar las llamadas que originan tu sistema con los números de teléfono de otras infraestructuras (IP o PSTN).

[2] http://windows.microsoft.com/es-XL/windows-vista/What-is-an-Internet-Service-Provider-ISP

Proveedores SIP: Un SIP carrier es una cuenta ofrecida por el proveedor de VoIP que comunica con el estándar del SIP. El SIP es actualmente el protocolo más popular de VoIP en Internet, usado para conectar millones de redes y dispositivos.

2.5.2 VoIP-DID

El servicio VoIP-DID te permitirá no sólo realizar llamadas, sino recibir llamadas desde cualquier teléfono del mundo en tu VoIP fijo, móvil. La marcación Directa de Entrada (DID por sus siglas en inglés) es un número telefónico válido fijo de tu ciudad, que está enlazada con tu número VoIP. Actualmente un número VoIP solamente puede recibir llamadas de números VoIP de la misma empresa proveedora del servicio VoIP, pero con la tecnología DID, un número VoIP puede recibir además llamadas desde la red fija (PSTN) o red móvil. Además, puedes tener muchos números fijos enlazados a tu número VoIP.

2.6 Protocolos en la telefonía IP

Un protocolo es un conjunto de reglas y acuerdos que los computadores y dispositivos deben seguir para que puedan comunicarse entre ellos. Más concretamente, un protocolo de señalización es el que se encarga de gestionar los mensajes y procedimientos utilizados para establecer una comunicación.

Para VoIP existen varios protocolos de señalización, tales como, H323, MGCP, SCCP, SIP y IAX2. Sin embargo, los tres protocolos más extendidos son SIP, IAX2, y H323. Aunque H323 ha estado muy extendido, ha sido muy utilizado y ha sido el que ha permitido el despegue de la VoIP, existiendo gran variedad de hardware que lo soporta.

2.6.1 H323

Básicamente H323 es un protocolo cliente-servidor en el que básicamente intervienen dos tipos de señalización: Señalización de control de llamada (H225) y Señalización de control de canal (H245), la primera se encarga del registro y localización y la segunda del establecimiento de llamadas.

2.6.2 MGCP

MGCP (Media Gateway Control Protocol “Protocolo de Control de Dispositivos”), es un protocolo del tipo cliente-servidor, y ya ha quedado obsoleto, aunque IAX2 ha adoptado parte de su estructura de funcionamiento.

2.6.3 SCCP

SCCP (Skinny Client Control Protocol), es un protocolo propietario de Cisco, basado en un modelo cliente servidor que deja toda la inteligencia en manos del servidor, llamado “call manager”, este protocolo se encuentra en activo en muchas corporaciones debido a la garantía y respaldo que Cisco proporciona.

2.6.4 IAX

El protocolo IAX (Inter-Asterisk Exchange Protocol) fue diseñado para conmutadores virtuales especialmente el Asterisk para protocolo abierto, es decir, que se puede descargar y desarrollar libremente. Este protocolo ha sido desarrollado para solucionar problemas de NAT (Network Address Translation “Traducción de Dirección de Red”) y mejorar el trunking entre sistemas basados en este protocolo. En las comunicaciones basadas en IAX, el Asterisk puede operar de dos formas diferentes:

- Servidor: El Asterisk admite registros de clientes IAX, pudiendo ser estos clientesHardware, Software u otros como Asterisk.
- Cliente, Asterisk puede registrarse en otros Asterisk o en operadores IP que utilicen este protocolo.

2.6.5 SIP (Session Initiation Protocol)

Este protocolo está más integrado con las aplicaciones y servicios de Internet, posee mayor flexibilidad para incorporar nuevas funciones y su implementación es mucho más simple que H323, incluso es parecido a los protocolos HTTP y SMTP.

Las aplicaciones SIP usan el puerto 5060 con UDP (User Datagram Protocol) o TCP (Transmission Control Protocol), para información de señalización y normalmente el protocolo RTP para la transmisión de voz mediante la elección de un número par al azar para el puerto, más concretamente se usan dos puertos por canal de comunicación.

SIP se ha propuesto como sistema genérico para el soporte de mecanismo de señalizaciones de servicio de telefonía IP. SIP soporta cinco elementos funcionales para el establecimiento y terminación de comunicaciones multimedia:

- Localización de Usuarios.
- Intercambio y negociación de capacidades de los terminales.
- Disponibilidad de Usuarios.
- Establecimiento de llamadas.
- Mantenimiento de llamadas.

SIP es un protocolo basado en el modelo cliente-servidor. Los clientes SIP envían peticiones a un servidor, el cual una vez procesada contesta con una respuesta. Los terminales SIP, también pueden establecer llamadas de voz directamente sin la intervención de elementos intermedios, al igual que en el caso de H323, funcionando como “peers independientes”.

El protocolo SIP define principalmente seis tipos de solicitudes:

- INVITE: establece una sesión.
- ACK: confirma una solicitud INVITE.
- BYE: finaliza una sesión.
- CANCEL: cancela el establecimiento de una sesión.
- REGISTER: comunica la localización de usuario (nombre de equipo, IP).
- OPTIONS: comunica la información acerca de las capacidades de envío y recepción de teléfonos SIP.

Y seis clases de respuestas:

- 1xx: respuestas informativas, tal como 180, la cual significa teléfono sonando.
- 2xx: respuestas de éxito.
- 3xx: respuestas de redirección.
- 4xx: errores de solicitud.
- 5xx: errores de servidor.
- 6xx: errores globales.

Normalmente una comunicación tendrá las siguientes fases:

Registro → Establecimiento → Comunicación mediante RTP → Finalización.

2.7 Codecs en la telefonía IP

La señal de audio ha de ser digitalizada, comprimida y codificada antes de ser transmitida por la red IP. Para ello se utilizan algoritmos matemáticos implementados en software llamados códec (acrónimo de codificador-decodificador, aunque principalmente se utilizan como compresores-descompresores).

Existen diferentes códec de audio utilizados en VoIP, y dependiendo del algoritmo escogido en la transmisión variara la calidad de la voz, el ancho de banda necesaria, y la carga computacional. El objetivo principal de esta tecnología es encontrar un equilibrio entre eficiencia y calidad de voz.

Aunque el sistema auditivo humano es capaz de captar las frecuencias comprendidas entre 20 Hz y 20 kHz, la gran mayoría de códec procesan aquella información dentro de la banda de 400 Hz a los 3,5 kHz ya que con esto es suficiente para reconstruir la señal original. A continuación se enumeran algunos de los códec más comunes:

2.7.1 G.711

Principal códec de la PSTN estandarizado por la ITU (Internacional Telecommunication Union "Unión Internacional de Telecomunicaciones") en 1972. Este estándar muestrea a una frecuencia de 8 kHz y utiliza PCM (Pulse Code Modulation "Modulación por Puntos Codificados"), para comprimir, descomprimir, codificar y decodificar. Existen dos subtipos:

- μlaw: codifica cada 14 muestras en palabras de 8 bits. Usado en EE.UU y Japón.
- A-Law: codifica cada 13 muestras en palabras de 8 bits. Usado en el resto del mundo.

Al entregar ambas palabras de 8 bits requiere un ancho de banda de 64 Kbps. Este es el algoritmo más simple y de menos carga computacional, ya que no realiza compresión en la codificación y es la base del resto de estándares.

2.7.2 G.726

Este estándar de la ITU, también conocido como ADPCM (Adaptive Differential Pulse Code Modulation "Modulación por Codificación de Impulsos Diferencial Adaptativa"), sustituyo al obsoleto standard G.721 en 1990.

Permite conseguir un ancho de banda de 16 Kbps, 24 Kbps, y 32 Kbps La ventaja de este códec es la disminución del ancho de banda sin incrementar la carga computacional.

2.7.3 G.723.1

Este algoritmo, estandarizado en 1995 por la ITU, puede operar a 6,3 Kbps o 5,3 Kbps Este códec debe ser licenciado para poder ser usado.

2.7.4 G.729a

Este códec desarrollado por diferentes empresas privadas necesita un ancho de banda de 8 Kbps, y su carga computacional es elevada. También es necesaria una licencia para su uso. No puede transportar tonos como DTMF, o fax, pero es el que menor tasa de bits proporciona (8 Kbps).

2.7.5 GSM (RPE-LPT)

Este códec aunque conocido popularmente por GSM, por ser usado en este tipo de redes, su nombre original es: Regular Pulse Excitación-Long Term Predicción. Este códec codifica a 13 Kbps con una carga computacional media, y no requiere el pago de licencia.

2.7.8 ILBC (Internet Low Bit-Rate Codec)

Códec de baja tasa de bits para internet. Este códec muestrea cada 8 KHz, y utiliza para la codificación (LPC) y codifica a 15.2 Kbps o 13.3 Kbps Este códec es libre, y no necesita ser licenciado.

2.7.9 SPEEX

Es un códec de comprensión de audio que implementa un algoritmo capaz de variar la velocidad de transmisión dependiendo de las condiciones actuales de la red. El ancho de banda puede variar desde 2.15 a 22.4 Kbps usado principalmente para VoIP.

Capítulo 3 Comunicaciones Unificadas

3 Comunicaciones Unificadas

La historia de las comunicaciones unificadas es relativamente reciente sin embargo su evolución ha sido muy rápida podemos decir que esta tecnología la cual incluye una combinación de software, hardware y los recientes servicios en la nube; este crecimiento es obviamente paralelo al avance de las tecnologías que lo soportan. Podríamos decir que su desarrollo comenzó a finales de los años noventa con la proliferación de las centralitas privadas conectadas a la red pública (PBX), las cuales primero fueron analógicas, luego digitales, actualmente también IP y los sistemas telefónicos de teclas a principios de los ochenta. Todo ello aceleró la migración desde sistemas de conmutación telefónicos electrónicos tradicionales manuales y automatizados. Estos sistemas PBX y sistemas de teclas hicieron más funcional a las empresas u oficinas individuales permitiendo realizar conexiones entre los teléfonos internos, además de conectarlos con la red de teléfono pública Public Switching Telephone Network (PSTN), operada por empresas de telefonía locales. Además de que proporcionan las capacidades de llamada deseadas tales como marcación de extensiones, devolución de llamadas, uso de grupo de búsqueda y el buzón de voz.

Es así que las Comunicaciones Unificadas nos permiten obtener grandes ventajas para los usuarios ya que pueden mantenerse en contacto con cualquier persona, donde quiera que estén y en tiempo real ayudando a:

1. Aumentar la Productividad de los Empleados
2. Aumentar la Calidad de Atención al Cliente
3. Optimizar los Recursos de un Sistema de Comunicaciones.

Las soluciones de comunicaciones unificadas integran las tecnologías de información existentes entre los teléfonos y equipos de computadora, el correo electrónico, correo de voz, faxes, mensajería instantánea y calendario convergiéndolos a todos en un solo lugar: la bandeja de entrada y con una interfaz familiar para la PC, web o gadget para hacerlo fácil de usar, independientemente de la ubicación en donde se encuentre la persona, esto hace que las comunicaciones sean más ágiles y fáciles, aumentando la productividad y reduciendo los costos.

Las Comunicaciones Unificadas incluyen servicios como son: telefonía, presencia, mensajería instantánea, conferencias, videoconferencia, colaboración, movilidad, transferencia de archivos, mensajería unificada, buzón de voz y correo electrónico.

Las Comunicaciones Unificadas representan la evolución de las tecnologías de comunicación, un aumento de la efectividad de las empresas, un ahorro de tiempo y de costos. Hace que la

administración y el mantenimiento sean más fáciles, rápidos y sencillos; permitiendo que el usuario se sienta informado, contento y maravillado por todas las posibilidades que tiene de estar comunicado y mantener una ubicuidad de manera real a cualquier hora.

Cada día se ha vuelto más sencillo unificar y centralizar todos los medios de comunicaciones que se utilizan en el día a día empresarial como lo veremos a lo largo de este capítulo.

3.1 Requerimientos de las Comunicaciones Unificadas

En cuanto a los costos, su espectro es tan amplio como las alternativas o perfiles que se requieran para un empleado, un grupo o un departamento ya hemos dicho que las Comunicaciones Unificadas son un conjunto de software, hardware y servicios. Sin embargo, conocer los valores reales y ocultos de estos servicios y poder estimar el retorno de la inversión estimado en un año promedio, son datos más que relevantes al momento de implementar las CU.

Podemos decir que las comunicaciones unificadas integran las tecnologías de comunicación con las herramientas de colaboración, aunque algunas herramientas poseen características de ambas (en definitiva, no hay colaboración sin comunicación), todo esto visto globalmente como servicios de comunicaciones.

Dentro de las herramientas de comunicación tenemos:

- Teléfonos fijos
- Teléfonos móviles
- Video
- Mensajería de voz
- Correo electrónico
- Chat.

Dentro de las herramientas de colaboración están las siguientes:

- Calendarios
- Conferencias y Videoconferencias web
- Salas de reuniones
- Compartir documentos (Escritorio Compartido)
- Telepresencia
- Aplicaciones Móviles
- Atención al Cliente

Existen diferentes alternativas de soluciones de Comunicaciones Unificadas que se ofrece el mercado en la actualidad, las hay hosteadas lo que se conoce como el Cloud o servicios en la

nube y también existen las que son dedicadas. Obviamente en cualquiera de los dos escenarios la propuesta de unificación deberá siempre ajustarse a los perfiles de los empleados, al presupuesto y a los requerimientos específicos de cada empresa.

Las alternativas como los servicios y las otras, como instalación de infraestructura de comunicaciones. En el primer caso, la contratación basta. Para el segundo, se requiere de una estrategia de implementación, para lo cual la planificación es de suma importancia. Se debe realizar un análisis del estado de la infraestructura, un plan de implementación y crecimiento, y hasta de capacitación del personal.

En el análisis de la red, se debe tomar en cuenta la infraestructura actual y determinar si es necesaria una actualización o como lo mencionamos anteriormente optimizar los recursos con los que se cuenta.

De acuerdo a los objetivos y la visión de la empresa se deben considerar los servicios que se necesiten y la infraestructura que lo soporte como son:

- Cableado estructurado
- Telefonía IP
- Servicio de Internet (Enlace Dedicado)
- Servidores capaces de alojar los servicios que se requieren prestar.
- Un ancho de banda Simétrico
- Asegurarnos de contar con corriente regulada
- La ventilación y temperatura adecuada para los equipos de cómputo.

Se deberá considerar requerimientos técnicos específicos que tienen que garantizar la calidad de los servicios. La infraestructura de la red debe contar con routers/switches que soporten tanto la calidad de servicio QoS, VLAN´s, seguridad y alimentación eléctrica en sus puertos POE (Power Over Ethernet “Alimentación sobre Ethernet”).

El costo para este tipo de proyectos es un factor determinante en el análisis que se debe hacer para implementar CU.

A continuación describiremos los servicios que incluyen algunos proveedores dentro de las soluciones para Comunicaciones Unificadas.

3.1.1 Movilidad

La movilidad es parte del día a día laboral y se entiende como estar trabajando sin estar en el escritorio de la empresa, poder ir donde quiera y aun así aportar a los trabajos y proyectos que se necesitan en tiempo real. Las CU proporcionan todavía más capacidades para la movilidad, incluyendo:

Teléfonos de banda múltiple de dos y tres modos: Con las CU los teléfonos inteligentes se pueden cambiar indistintamente entre redes Wi-Fi corporativas y redes móviles.

Clientes móviles de CU: El uso de un cliente móvil permite manejar visualmente los mensajes de correo electrónico y de voz, acceder al directorio corporativo, y extender características PBX corporativas como la transferencia, la conferencia y otras hasta los dispositivos móviles.

Texto a voz: Se puede hacer que la aplicación lea los mensajes de correo electrónico mientras se accede a los mensajes de voz. En algunos casos, incluso que se lea el documento adjunto.

Reconocimiento de voz: El reconocimiento de voz se adapta a la perfección a los usuarios móviles. Proporciona acceso independiente de voz con ojos libres y manos libres para realizar llamadas y participar en conferencias, usar el correo electrónico y el correo de voz, el calendario, y la lista de tareas.

Los teléfonos celulares actuales llamados Smartphone o recientemente denominados como superphones tienen todo el hardware y software necesario para realizar estas actividades, con las comunicaciones unificadas y las aplicaciones para estos se puede lograr y aumentar las capacidades de los dispositivos.

3.1.2 Escritorio Convergente

Utilizando Comunicaciones Unificadas se obtiene un escritorio “unificado” o “convergente” (“Converged Desktop”). Este concepto apunta a consolidar las interfaces informáticas y telefónicas, manteniendo ambas, pero permitiendo un alto grado de integración y unificación. Mediante la utilización de técnicas de CTI, integradas o embebidas en las aplicaciones de escritorio, es posible:

Recibir notificaciones de llamadas telefónicas en el escritorio: Mediante la presentación de pantallas emergentes (“screenpopups”), la información de las llamadas entrantes se despliegan de manera similar a la recepción de un nuevo correo electrónico, o de un mensaje instantáneo.

Controlar el teléfono desde el escritorio: Las llamadas pueden ser atendidas u originadas desde las aplicaciones de escritorio, integrando la libreta de direcciones corporativa. Mediante “un clic” sobre el nombre de la persona es posible iniciar una llamada, a su interno, a su celular, a su trabajo, etc.

Activar desvíos “inteligentes” de llamadas: En forma integrada al calendario de reuniones, o al estado de presencia, es posible activar desvíos de llamadas, al correo de voz, al celular, etc.

Combinar los sistemas de mensajería instantánea y presencia a las actividades telefónicas: Automáticamente el estado de presencia se cambia a “El teléfono” cuando se está en una llamada.

Adicionalmente, con Comunicaciones Corporativas Unificadas una llamada establecida, se puede iniciar una sesión de mensajería instantánea para intercambiar archivos, o compartir el escritorio

3.1.3 Presencia

La “presencia” es una indicación del estado de disponibilidad de una persona para comunicarse con otras. Los sistemas de presencia basan su desarrollo en las recomendaciones del RFC 2778 donde se definen las siguientes entidades:

- Presentity: Una entidad descrita por su información de presencia. Generalmente esta “entidad” es una persona, y su estado se mantiene en un servidor de presencia.
- Watcher: Quienes solicitan información de presencia de otras personas al servidor de presencia.
- Fetcher: Un “watcher” que solicita el estado actual de presencia de algún “Presentity” a través del servidor de presencia.
- Subscriber: Un “watcher” que solicita notificaciones del servidor de presencia cuando algún “presentity” cambia de estado.
- Poller: Una clase especial de “Fetcher” que solicita los estados de presencia en forma regular.

En el contexto de las Comunicaciones Unificadas, diversos tipos de aplicaciones pueden conocer y presentar el estado de presencia de las personas. Típicamente la presencia es indicada en sistemas de mensajería instantánea. Sin embargo, el estado de presencia puede ser muy útil en otro tipo de aplicaciones. En los clientes de correo electrónico, conocer el estado de presencia del remitente brinda la posibilidad de decidir en el mismo momento el medio por el cual contestar su solicitud. Si la persona está presente y disponible, puede ser más eficiente llamarlo que responderle en forma escrita. Aplicaciones de procesadores de texto y planillas electrónicas, así como aplicaciones de gestión CRM Customer Relationship Management “Administración de las Relaciones con los Clientes”), ERP (Enterprise Resource Planning “Sistema de Planificación de Recursos Empresariales”), también pueden mostrar el estado de presencia de las personas involucradas en el documento o proceso, mejorando de esta manera la comunicación organizacional cooperativa

3.1.4 Mensajería Instantánea

Originalmente los sistemas de mensajería instantánea fueron definidos para entregar mensajes de texto cortos y simples en forma inmediata a otros usuarios que estén conectados en línea. Con el tiempo los sistemas fueron mejorados para soportar intercambios de archivos, conversaciones de voz y video, y otras funciones como conversaciones en grupo.

La Mensajería Unificada combina mensajes de voz y mensajes de correo electrónico en una única infraestructura de mensajes.

Correo de voz único: Se tienen un solo sistema de correo de voz al cual pueden acceder desde cualquier lugar.

Los indicadores de correo de voz aparecen tanto en los teléfonos de la oficina como en los móviles, así como en otras aplicaciones en las computadoras de escritorio.

Repuesta en medios cruzados: En lugar de infraestructuras de mensajería separadas para el correo electrónico, el correo de voz y los mensajes de texto, una sola infraestructura soporta la mensajería y responde en varios medios, incluidos:

- Respuestas de correo de voz hacia el correo electrónico.
- Respuestas de correo electrónico o texto hacia correo de voz.

Mensajería instantánea federada: Las CU hacen posible los ambientes de mensajería instantánea entre organizaciones y proveedores que permiten a las personas contactar a otros por medio de la mensajería instantánea, sin importar el servicio de IM que cada uno esté usando.

3.1.5 Conferencias

Características que ofrecen las CU para las conferencias son:

Independencia de dispositivos: Los participantes pueden unirse a una conferencia por medio de cualquiera de estos dispositivos: teléfono móvil de solo audio, teléfono inteligente, o portal web de PC.

Llamada para iniciar la conferencia: El sistema de conferencia llama al anfitrión de la reunión y a los participantes, en lugar que todos tengan que hacer la llamada. Las reuniones pueden comenzar con más prontitud. No hay que buscar números para realizar la llamada: solo tiene que responder el teléfono cuando éste suena.

Adaptabilidad de medios: Una conferencia que inicia en un modo puede fácil y rápidamente agregar otros modos.

Horario integrado: Cuando alguien organiza una conferencia, los calendarios de los participantes invitados se actualizan automáticamente. El organizador puede, con solo presionar un botón (está bien, es más bien, digitando una URL en el buscador), agregar información acerca de la conferencia para un invitado, de manera que sus participantes no tendrán que descifrar cómo unirse a la conferencia a la hora definida.

Control visual y auditivo de la conferencia: Los organizadores de la conferencia pueden en tiempo real controlar aspectos de video y audio de la conferencia.

Esto permite que una conferencia rica en medios sea más inteligente con respecto a las capacidades de los participantes.

Los participantes que cuentan con capacidades enriquecidas en sus medios pueden ver el video, el audio, la aplicación para compartir y así sucesivamente, si sus terminales son capaces, mientras los participantes en terminales más livianas como los dispositivos móviles pueden recibir las partes de la conferencia que permiten sus dispositivos.

3.1.5.1 Videoconferencias

La videoconferencia tiene un rol cada vez más importante, a medida que las organizaciones se han vuelto más distribuidas y móviles, proporcionan una experiencia más personal que admite la creación eficaz de equipos. Las interfaces complejas, los altos costos y las funciones limitadas han reducido la adopción de la videoconferencia para la mayor parte de los recursos. Al incorporar vídeo en el cliente unificado se puede agregar programaciones a una conferencia en línea con vídeo o elevar el vídeo espontáneamente a una videoconferencia es un proceso directo y fácil.

Con el fin de proporcionar la experiencia de comunicación más inmersiva posible hay una gran variedad de opciones de videoconferencia. Se facilita la adición de vídeo a una llamada telefónica estándar con tan solo hacer un clic. Con compatibilidad para dispositivos de audio y vídeo, los usuarios pueden configurar un video llamada de manera sencilla y mejorar la colaboración entre compañeros de trabajo y clientes.

3.1.6 Colaboración

El concepto de Colaboración involucra a múltiples personas trabajando en conjunto para lograr un objetivo en común.

Diversas herramientas de colaboración forman parte de las Comunicaciones Unificadas. Entre ellas, se destacan:

Vistas compartidas: Permiten compartir documentos o el escritorio de una o varias personas entre varias personas. Entre las herramientas de vistas compartidas se incluye la pizarra electrónica.

Navegación Web compartida: Permite que los participantes de una conferencia multimedia puedan navegar en forma conjunta por páginas de Internet. Esto complementa las vistas compartidas, con aplicaciones que realizan esta función de los navegadores de Internet de cada participante, no mediante una vista compartida del navegador de uno de los participantes.

Transferencia de Archivos: Permite que un usuario envíe un archivo a uno o varios colaboradores.

Una de las máximas que proporciona la colaboración es el hecho de poder trabajar donde sea que se encuentren a la hora que sea, con cualquier dispositivo, accediendo a cualquier tipo de contenido con los controles de políticas apropiados; lo cual al parecer es el nuevo modelo de negocios para las empresas.

3.1.7 Federación

Las Comunicaciones Unificadas han significado la oportunidad para que aparezca un nuevo modelo comunicaciones federadas. Éste concepto tecnológico nace gracias al internet, donde el ruteo y direccionamiento del tráfico se basa en servidores de dominio o lo que se conoce como los Domain Name Server. (DNS) para convertir el nombre de un dominio en una dirección IP y así hacer posible el enrutamiento de una petición de página web hacia el servidor web correcto.

La federación les permite a los usuarios o trabajadores comunicarse de una manera más rápida y eficiente con otros usuarios que estén dentro o fuera de la organización. Con la federación por ejemplo se puede ampliar Lync Server 2010 a través de Internet con clientes, proveedores, socios y otros participantes es un plus con el que cuenta Microsoft respecto de otras tecnologías de UC.

Características y funcionalidad clave

- Se puede Federar con socios de confianza. Los administradores pueden habilitar la federación con otra organización que cuente también con Lync Server 2010 u otras versiones anteriores, incluidos Office Communications Server y Live Communications Server.
- Manténgase en contacto más fácilmente. Una vez habilitados, los usuarios de una organización pueden agregar a los usuarios de otra a sus listas de contactos, así como enviarles mensajes instantáneos y consultar su información de presencia.
- Experimente las capacidades completas de las comunicaciones unificadas. Los usuarios pueden elegir la mejor forma de comunicarse según la tarea que estén realizando (voz, vídeo, etc.), y pueden pasar fácilmente de conversaciones entre dos personas a conferencias con varios participantes.
- Ahorre dinero. Las comunicaciones federadas usan Internet y no la red telefónica pública, lo que contribuye a reducir el gasto de dinero en facturas telefónicas y servicios de conferencias de terceros.
-

3.1.8 Operadora Automática

La operadora automática es una de las funcionalidades de respuesta instantánea que les permite a las recepcionistas y otros administradores de atención al público tener un mayor control de las llamadas y así mismo lograr una mayor satisfacción con los clientes además de que vincula la presencia lo cual permite llevar a cabo una mejor interacción en tiempo real ya que como vimos antes con la presencia podemos saber la disponibilidad de la persona y así poder elegir el medio adecuado para contactar a la persona que nos interesa.

Generalmente este servicio se brinda a través de una interfaz gráfica en donde la operadora tiene la oportunidad de determinar cuál es el mejor método para establecer una comunicación ya sea verbal o escrita: Les permite tener acceso al directorio y así mismo hacer transferencias, llamadas o incluso iniciar una conferencia con un solo clic, en la misma página nos permite la opción de regresar a un operador en cualquier momento en caso de necesitar más ayuda, básicamente aquí hablamos que para poder utilizar esta herramienta existe toda una plataforma en donde se le añade esta opción por medio de un software.

3.1.9 Correo de Voz

El correo de voz es una herramienta con la cual a través de ella podemos almacenar, y registrar las llamadas entrantes que no pueden ser contestadas en el momento en el que son realizadas por medio de mensajes que se van registrando y almacenando en un teléfono o bien en un servidor.

Si quisiéramos que en cualquier momento se nos pueda contactar y no perder ninguna llamada que pudiera ser importante y que al menos nos dejen un recado telefónico en caso de no estar presentes; el correo de voz es una buena opción es un sistema centralizado el cual nos permite almacenar mensajes de voz en cualquier momento que no estemos presentes, o bien de que nuestra línea o extensión no se encuentre disponible y no podamos contestar por la razón que sea; actualmente muchas de las compañías telefónicas ofrecen este servicio por un costo adicional o como parte de un paquete.

Debido a la importancia que ha cobrado el hecho de no perder llamadas que puedan ser relevantes, algunos conmutadores vienen con correo de voz integrado quizá de manera muy escueta pero con la capacidad de adaptarse a un correo de voz más completo que pueda contar con las siguientes características:

- Operadoras automáticas para requisitos específicos de la empresa
- Herramienta intuitiva de diseño para configurar los flujos y el enrutamiento de llamadas
- Integración con varios sistemas de correo electrónico, que incluyen Microsoft Exchange y mensajes de correo electrónico del proveedor del servicio

- Sistemas interactivos de cliente automáticos (aplicaciones IVR) con la capacidad para leer la información a la persona que llama.

3.1.10 Telepresencia

Comunicarse mediante video sigue siendo una de las tendencias principales en telecomunicaciones, como se evidencia por el fuerte crecimiento del mercado del video para empresas. La Telepresencia es uno de los servicios más nuevos dentro de las comunicaciones unificadas se podría decir que es un sistema más avanzado de lo que son las videoconferencias la cual nos ayuda para evitar desplazamientos innecesarios, acelerar los procesos de decisión y mejorar las comunicación es por lo cual es una excelente herramienta de comunicaciones de video empresarial la cual obviamente entre sus ventajas principales es el ahorro del tiempo. Por medio de una sencilla conexión entre dos o más sedes, que pueden encontrarse separados por algunos metros o bien por miles de kilómetros de distancia unas de otras, los sistemas de Telepresencia permiten establecer una comunicación bidireccional o multi-direccional, más directa, y que a la vez pueda ser fluida y flexible, con niveles de calidad sorprendentes.

También nos permite ver y escuchar al interlocutor como si estuviera a pocos metros de distancia, con una gran calidad de audio y video. Además, no solo se mantiene una comunicación oral y gestual, sino que al mismo tiempo se pueden compartir la visualización simultánea del interlocutor con una imagen de la pantalla de un ordenador donde realizar presentaciones, ver gráficos, etc.

Cisco es el que hasta ahora más le ha invertido a este tipo de tecnología y cuanta con diferentes soluciones como el TelepresenceSX200, Polycom con el TelepresenceM100, Avaya recientemente adquirió Radvision para ingresar en la competencia de los servicios de Videoconferencia y Telepresencia una de sus plataformas es el Scopia XT Telepresence. Estos son algunos proveedores que hoy en día tienen más desarrollo en este tipo de solución Un estudio realizado en 2011 por Infonetics estima que el gasto en videoconferencias y Telepresencia se duplicará para 2015 así que hablar de que esto sea el futuro de las comunicaciones ya no suena tan descabellado, más bien ya solo es cuestión de tiempo para que sea una realidad.

3.1.11 Aplicaciones Móviles

Las aplicaciones móviles son extensiones informáticas para dispositivos portátiles, las cuales inicialmente comenzaron con los asistentes digitales personales (PDA). Y actualmente debido a su crecimiento se encuentran alojadas en un “mercado” (tiendas online) restringido para su descarga por medio de los teléfonos inteligentes Smartphone. La mayoría de estas aplicaciones se han desarrollado en lenguajes como C y C++, Java y Visual. Existen diferentes fabricantes de teléfonos móviles como: Apple, BlackBerry, Nokia, Sony, Samsung etc. que a través de sus

sistemas operativos entre los que sobresalen IOS, Android, Windows Mobile y RIM, permiten que al día de hoy existan en el mercado millones de aplicaciones debido a que cada vez es más competitivo.

Sin embargo a pesar de que existe una gran variedad de aplicaciones no todas son multiplataforma, lo cual representa un obstáculo en el desarrollo de las mismas; lo cual es un tema aparte, lo que nos interesa en este caso es que debido a la creación de estas aplicaciones nos proporcionan generalmente funcionalidades de presencia y mensajería instantánea, correo de voz y obviamente telefonía en las CU por medio de un Smartphone con aplicaciones como One-X Mobile (Avaya), en el caso del cliente de Lync (Microsoft) y el Jabber (Cisco) también nos proporciona videoconferencia, y escritorio compartido, en la figura 26 se muestra las apps para smartphones que están actualmente en el mercado.

Lync **Jabber** **One-x Mobile**

Figura 26 Aplicaciones para móviles.

3.1.12 Proveedores de Comunicaciones Unificadas

Hoy en día existen diferentes competidores en el mercado que ofrecen este tipo de tecnología como son: Cisco, Avaya, Microsoft, IBM, Polycom entre otros sin embargo ninguno lo hace de la forma tan estrechamente integrada como lo hace Microsoft. El mayor competidor de Lync es Cisco, pero su suite de UC tiende a ser más cara es una buena opción para empresas grandes. Y la de IBM, Sametime, carece del componente de voz. Aunque dispone de conferencia Web e IM, para telefonía depende de las PBX de otros fabricantes.

En el cuadrante mágico que Gartner ha publicado desde el 2009 sobre el mercado de las Comunicaciones Unificadas ha reconocido como líderes a Microsoft, Cisco, Avaya, Alcatel-Lucent y Siemens Enterprise Communications entre otros.

Gartner Inc. es una empresa consultora y de investigación de las tecnologías de la información, cada año hace estudios sobre cómo van evolucionando diferentes tecnologías a continuación

podemos ver la parte que nos interesa sobre Comunicaciones Unificadas en donde Cisco Y Microsoft se han peleado la punta en los últimos años como se muestra en las siguientes imágenes.

Como podemos observar desde 2010 en las figuras 27, 28, 29 y 30 existen diferentes alternativas de proveedores, sin embargo solo nos enfocaremos en Lync debido y Avaya, debido a que ya se cuenta con infraestructura de esta última y a que muchos ya están familiarizados con soluciones de Microsoft, Cisco se descarta porque es una solución basada en hardware lo cual lo hace más costoso y su integración con otras tecnologías es más difícil de realizar.

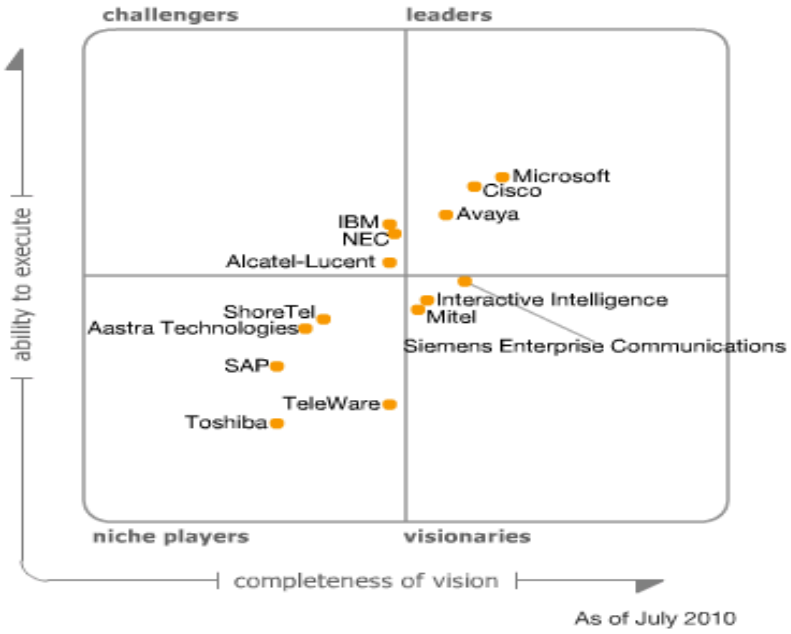

Figura 27 Cuadrante Mágico UC 2010

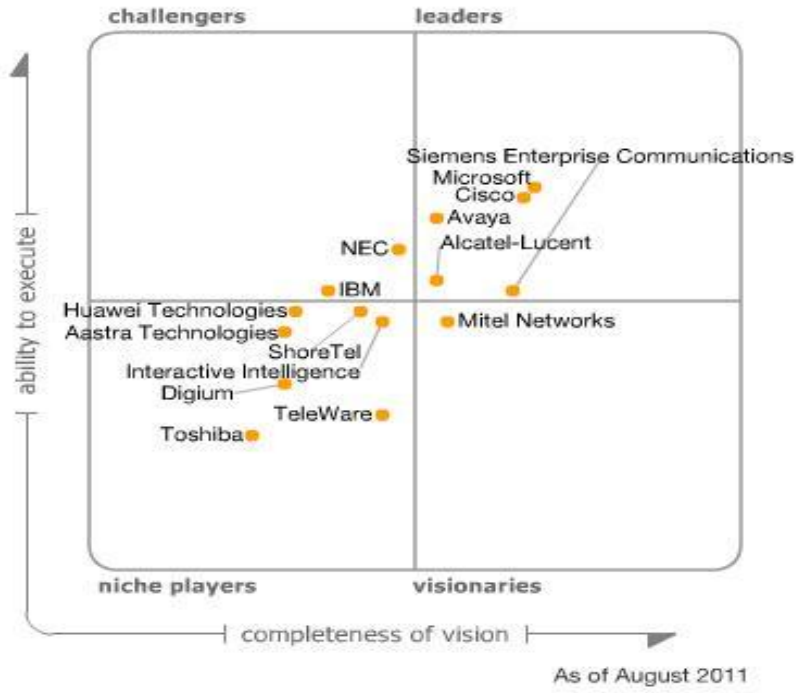

Figura 28 Cuadrante Mágico UC 2011

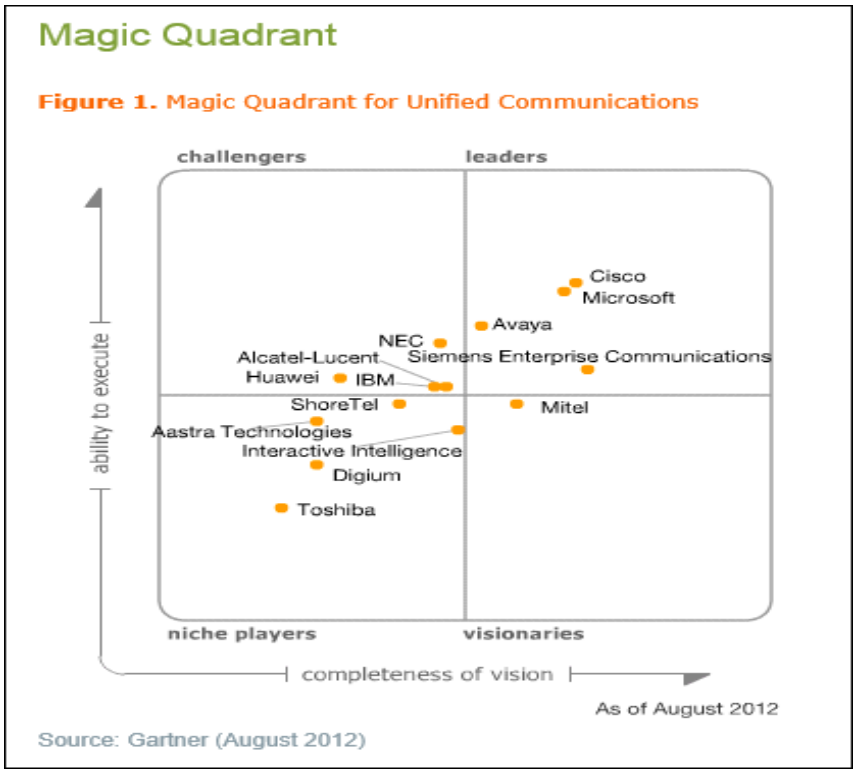

Figura 29 Cuadrante Mágico UC 2012

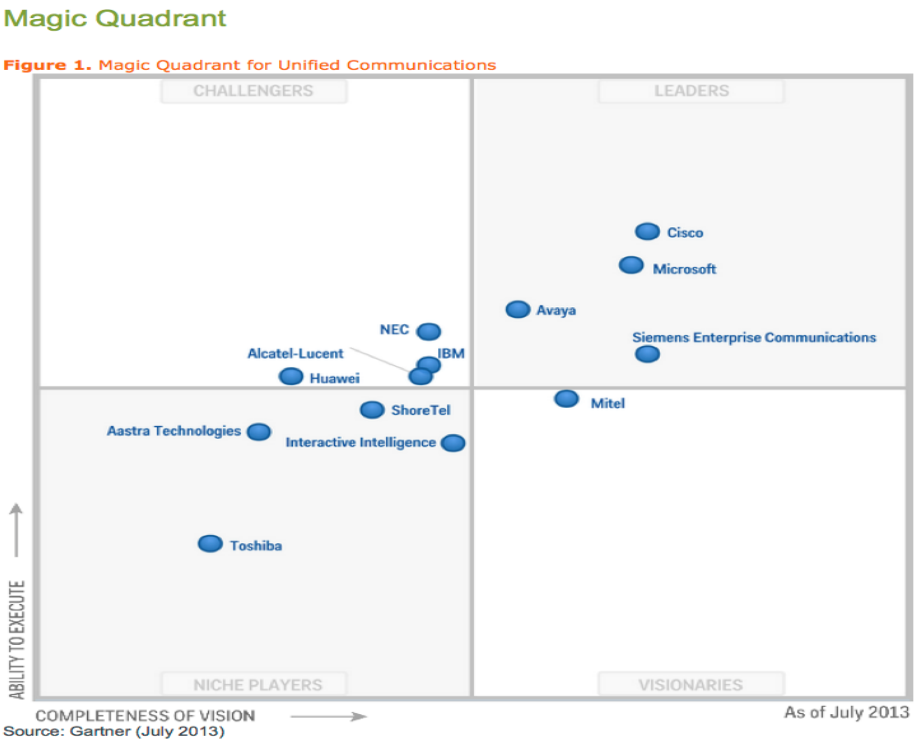

Figura 30 Cuadrante Mágico UC 2013

Capítulo 4 Seguridad en las Comunicaciones Unificadas

4 Seguridad en las Comunicaciones Unificadas

La seguridad en las Comunicaciones Unificadas es un tema muy importante para cualquier empresa que pretenda implementar este tipo de tecnología, debido a que tanto los datos como la voz son medios de información la cual es el activo de mayor envergadura que se posee y que será transportado a través de la red; es por ello que se debe contar con una estrategia y técnicas para protegerlos adecuadamente.

Es sumamente importante entender que con este tipo de tecnología en donde estamos integrando diferentes servicios y que además están vinculados con otras herramientas que bien pueden ser por medio de software o hardware se lleve a una planeación y estrategia de seguridad apropiada, de manera conveniente no solo hay que enfocarse en la relación costo-beneficio en este tipo de tecnología, y de manera minuciosa hay que ir cuidando todos y cada uno de los activos que iremos integrando a nuestro sistema. Para ello hablaremos de seguridad en este capítulo en tres apartados, empezando por la seguridad física en donde explicaremos como resguardar los activos y el manejo adecuado de los mismos.

Seguidamente veremos la parte de seguridad lógica en donde como mencionábamos antes se ocupa cuando se requiere de implementar técnicas para la protección de los activos y cuando la seguridad física ha sido rebasada.

Y Finalmente la seguridad perimetral que como veremos es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de aseguramiento en el perímetro externo de la red y a diferentes niveles. Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Si bien es verdad que algunas organizaciones no le dan el valor adecuado a los inconvenientes que se puedan llegar a presentar al integrar los servicios no debemos ver esto como un tema aparte si no como un complemento de las UC Como veremos a lo largo de este capítulo existen diversos, ataques, amenazas y riesgos que pueden hacer que nuestra red sea vuelva vulnerable, y con ello comprometer nuestros servicios o funcionalidades de las CU afectando la productividad de los usuarios, sin embargo trataremos de reducir y controlar en la medida de lo posible con algunas implementaciones o planes de contingencia y métodos que veremos en este apartado que nos ayudaran para poder disminuir los diferentes problemas que se pueden presentar en la implementación de las Comunicaciones Unificadas.

4.1 Seguridad Física

La Seguridad Física es todo lo relacionado con la seguridad y salvaguarda de los bienes tangibles de los sistemas computacionales de la empresa, tales como el hardware, periféricos, y equipos asociados, las instalaciones eléctricas, las instalaciones de comunicación y de datos.

Igualmente la Seguridad Física incluye todo lo relacionado con la seguridad y salvaguarda de las construcciones, el mobiliario y equipo de oficina, así como la protección a los accesos al centro de cómputo o Site. En sí, podemos decir que es todo lo relacionado con la seguridad, la prevención de riesgos y protección de los recursos físicos informáticos de la empresa. En pocas palabras podríamos decir que la seguridad física son los mecanismos de control en el entorno de un sistema informático, en la figura 31 se muestran ejemplos de herramientas de estos mecanismos.

Figura 31 Seguridad Física.

4.1.2 Controles de eventos en la Seguridad Física

Al hablar de Seguridad forzosamente tenemos que hablar de mecanismos de control que se tienen que implementar para el resguardo y protección de los bienes.

Controles necesarios para la seguridad física del área:

- Inventario del hardware, mobiliario y equipo.
- Resguardo del equipo de cómputo.
- Bitácoras de mantenimiento y correcciones.
- Controles de acceso del personal al área de sistemas.
- Control del mantenimiento a instalaciones y construcciones.
- Seguros y fianzas para el personal, equipos y sistemas.
- Contratos de actualización, asesoría y mantenimiento del hardware.

Control de accesos físicos del personal al área de cómputo.

Es el establecimiento de las medidas tendiente a controlar el acceso de las personas que tengan que entrar al centro de cómputo.

Dichas medidas van desde registros en bitácoras o libretas, uso de gafetes y credenciales magnéticas, hasta la vigilancia estrecha de visitantes, áreas y pasillos por medio de circuito cerrado, así como la revisión física del personal que entra y sale del área de sistemas.

4.1.3 Análisis de Riesgos

Se considera a las posibles causales de riesgos en el área donde se desempeña el personal y para ello se deben de contar con el equipo adecuado y con el personal capacitado para el manejo de los recursos.

Los desastres naturales, incendios accidentales, humedad e inundaciones así como amenazas ocasionadas involuntariamente por personas o bien acciones hostiles deliberadas como robo, fraude o sabotaje son tipos de amenazas que pueden poner en riesgo nuestra estrategia de implementación en las Comunicaciones Unificadas por ello debemos enfocarnos en los siguientes puntos.

- Se deberá revisar el número de extintores que están disponibles en el área, su capacidad, que sean de fácil acceso, que tenga el peso indicado y si el tipo de producto que utiliza es el adecuado además de contar con un plan de mantenimiento para su recarga.
- Contar con detectores de humo que indiquen la posible presencia de fuego.
- Capacitar al personal para el uso adecuado de los equipos contra incendio.
- Verificar que las salidas de emergencia estén libres y puedan ser utilizadas.
- Los ductos del aire acondicionado deben de estar limpios.
- Se debe tener equipo de fuente no interrumpible y contar con corriente regulada.
- Contar con un sistema de tierra física, para las posibles descargas de corriente eléctrica.
- De ser posible contar con un banco de capacitores y supresor de picos.
- Restringir el acceso a los centros de cómputo sólo al personal autorizado.
- Definición y difusión de las horas de acceso al centro de cómputo.

Se debe indicar si se cuenta con controles y procedimientos para:

- Clasificación y justificación del personal con acceso a los centros de cómputo del negocio y a las oficinas donde se encuentra papelería o accesorios relacionados con informática.
- Definir la aceptación de la entrada a visitantes.
- Manejo de bitácoras especiales para los visitantes de los centros de cómputo.

Figura 32 Análisis de Riegos

4.1.4 Seguridad en el Personal

La Seguridad Física también incluye el control del Personal quienes van a controlar y administrar los recursos físicos y lógicos de la empresa. El objetivo principal de la auditoría de la seguridad del personal es evitar, hasta donde humanamente sea posible, los accidentes acaecidos en el trabajo que constituyen los riesgos de trabajo y así en mayor medida evitar los daños involuntarios.

Controles necesarios para la seguridad física del área

- Controles administrativos del personal de informática.
- Seguros y fianzas para el personal de sistemas.
- Planes y programas de capacitación.
- Planes de contingencia definidos para el personal que labora en el área.

4.1.5 Planes de contingencia

- Es el control de las contingencias y riesgos que se pueden presentar en el área de sistemas.
- Estas contingencias se pueden evitar a través de planes y programas preventivos específicos, en los que se detallan las actividades antes, durante y después de alguna contingencia.

En estos planes se incluyen los simulacros de contingencias, los reportes de actuaciones y las bitácoras de seguimiento de las actividades y eventos que se presenten en el área de sistemas.

Seguros y fianzas para el personal, equipos y sistemas:

- Son las medidas preventivas para garantizar la reposición de los activos informáticos de la empresa en caso de ocurrir alguna contingencia.
- Estas medidas se establecen para asegurar la vigencia de las pólizas de los activos informáticos asegurados, así como sus coberturas.

- Igual ocurre al afianzar la participación del personal y usuarios del área de sistematización de la empresa, ya sea para salvaguardar su fidelidad, o para protegerse de su ausencia por cualquier motivo.

Un plan de contingencia debe contar con lo siguiente:

- Un plan de emergencia: en el cual se pretende contener el daño. Es el plan para limitar el daño causado por un desastre. Debe contemplar todos los desastres naturales y eventos que son mal intencionados.
- El plan de respaldo: Proporciona continuidad a partes críticas entre el desastre y la terminación de la Recuperación. Contempla el mantenimiento de partes críticas entre la pérdida del servicio o recurso y su recuperación.
- El plan de recuperación: Restauración temporal o permanente de la capacidad de operación. Recuperación: Es la restauración temporal o permanente de una capacidad operacional crítica. Usualmente es responsable del proveedor del servicio.
- El programa de registros vitales: Proteger datos esenciales y preservar aquellos registros necesarios para restablecer las operaciones.

4.1.6 Objetivos de la Seguridad Física

La Seguridad Física es algo que conforme ha pasado el tiempo se ha vuelto algo de mayor envergadura y así con ello poder contar con un mayor control para evitar accidentes y saber reaccionar ante situaciones críticas es por ello que su finalidad sería:

- Verificar que existan los planes políticas y procedimientos relativos a la seguridad dentro de la organización.
- Confirmar que exista un análisis costo-beneficio de los controles y procedimientos antes de ser implantados.
- Comprobar que los planes y políticas de seguridad y de recuperación sean difundidos y conocidos por la alta dirección.
- Asegurar la disponibilidad y continuidad del equipo de cómputo el tiempo que requieran los usuarios para el procesamiento oportuno de sus aplicaciones.
- Evaluar el grado de compromiso por parte de la alta dirección, los departamentos usuarios y el personal de informática con el cumplimiento satisfactorio de los planes, políticas y procedimientos relativos a la seguridad.
- Constatar que se brinde la seguridad necesaria a los diferentes equipos de cómputo que existen en la organización.
- Comprobar que existen contratos de seguro necesarios para el hardware y software de la empresa.

Si logramos llevar esto a buenos términos y conseguimos establecer políticas y procedimientos para evitar las interrupciones prolongadas del servicio de procesamiento de datos y continuar en un medio de emergencia hasta que sea restaurado el servicio completo habremos puesto los cimientos para proteger nuestros recursos informáticos, lugar de trabajo, y el personal adecuado.

4.2 Seguridad Lógica

La seguridad lógica son las técnicas que empleamos para la protección del acceso y el resguardo de los datos garantizando que solo tengan acceso las personas autorizadas dentro de un sistema informático para hacerlo como ya lo habíamos mencionado anteriormente la seguridad lógica entra en función cuando la seguridad física se ve rebasada o bien para fortalecerla o cuando los mecanismos empleados son insuficientes para el resguardo de la información es decir que se vuelve un complemento de ella; en el rubro de seguridad informática se dice que "todo lo que no está permitido debe estar prohibido" y bajo esta regla no escrita la seguridad lógica se plantea analizar los siguientes puntos.

Restringir el acceso a programas y archivos mediante claves y/o encriptación.

- Asignar las limitaciones correspondientes a cada usuario del sistema informático. Esto significa, no darle más privilegios extras a un usuario, sino sólo los que necesita para realizar su trabajo.
- Asegurarse que los archivos y programas que se emplean son los correctos y se usan correctamente. Por ejemplo, el mal uso de una aplicación puede ocasionar agujeros en la seguridad de un sistema informático.
- Control de los flujos de entrada/salida de la información. Esto incluye que una determinada información llegue solamente al destino que se espera que llegue, y que la información llegue tal cual se envió.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. En la figura 33 se muestra el acceso como un acceso protegido por un password.

Figura 33 Seguridad Lógica.

4.2.1 Causas de la inseguridad

Se pueden definir una gran cantidad de causas que nos conlleven a tener un sistema que no sea seguro como veremos en este capítulo ningún sistema es 100% seguro pero si existen métodos para robustecer la seguridad de nuestra red entre las principales causas que podemos identificar dentro de una red:

- La deficiencia en los equipos respectivos de soporte. Son aquellos que no cuentan con antivirus, actualizaciones o parches para tener un mejor rendimiento.
- La “Ingeniería social” La cual es una técnica que permite a usuarios que no están autorizados tener acceso a algún sistema por medio de engaños para realizar algún acto que perjudique a una persona o institución.
- El espionaje industrial o el robo de Información. Como hemos venido diciendo dentro de un sistema informático lo más importante es la información es por ello que existe personas dedicas a obtener de manera ilícita la información de personas u organismos.
- La deficiencia en la administración de una red. Sin duda esta es una de las principales causas que vuelve a un sistema inseguro si no se cuenta con el equipo indicado y con el personal capacitado esto hará que el sistema se vuelva vulnerable y fácil de alterar.
- Los virus, gusanos, troyanos. Son aquellas amenazas que están Internet ya sea por medio de programas o herramientas de algún programa que mediante algún código malicioso pretenden alterar y manipular el funcionamiento de un equipo o bien corromper nuestro sistema y dejarlo expuesto.
- Fallos en la seguridad de programas. Es muy importante contar con programas que cuenten con sus licencias para garantizar las actualizaciones y con ello tener un mejor funcionamiento de estos.
- Los vándalos virtuales o también conocidos como cibercriminales. Las deficiencias o vulnerabilidades mencionadas anteriormente son aprovechadas por este tipo de

personas que de manera oportunista buscan algún hueco de inseguridad en un sistema para penetrar en este y realizar algún ataque o robo de información.

4.2.1 Control de accesos

En cuanto a este tipo de controles existen estándares de seguridad para el procedimiento de determinar un acceso autorizado como se menciona por parte del NIST (National Institute for Standars and Technology “Instituto Nacional de Normas y Tecnología”). Los cuales veremos a continuación

Identificación y Autentificación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- Algo que solamente el individuo sabe: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- Algo que la persona tiene: por ejemplo una tarjeta magnética un símbolo de seguridad.
- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura el control por voz.
- También existe la autenticación mediante dos factores "algo que tengo" la llave + "algo que sé" un número de PIN (token criptográfico)
- Autenticación triple factor "algo que tengo" el dispositivo criptográfico + "algo que sé" una clave de autenticación tipo PIN (al token criptográfico) + "quién soy" la huella dactilar que me permite autenticarme al dispositivo de forma unívoca.

Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

- Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

- Limitaciones a los Servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

Modalidad de Acceso

Ubicación y Horario El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

4.2.2 Barreras Informáticas

Como ya hemos visto al igual que la seguridad física, la seguridad lógica pretende evitar el robo de información para ellos existen diferentes métodos para que no se vea del todo comprometida nuestra información, en este apartado mencionaremos algunos de ellos.

Segmentar las redes de los servidores, es uno de los más importantes métodos en la seguridad lógica que nos permite poner una barrera de contención; el simple hecho de tener nuestro servidores en subredes diferentes, nos permitirá aislarlos y si alguno de ellos llega a ser comprometido los otros se mantendrían a salvo con ello se reduciría el tiempo en el que se puede realizar un ataque.

Mantener actualizado el Software de nuestros equipos. Esta quizá parece la tarea más fácil sin embargo muchas veces no se le da la importancia adecuada y por falta de negligencia, tiempo, decidía o incluso desconocimiento. Al ser una labor manual esto a menudo no se lleva a cabo,

sin darse cuenta que esto es una de los métodos más prácticos que existen y que nos ayudan a mantener funcional nuestros sistemas.

Conexión Restringida a Internet Para nadie es un secreto que la red más insegura que existe es el Internet por ello se debe tener cuidado con los accesos que se tienen en los servidores, ya que si no estarían más expuestos a algún tipo de ataque, lo más conveniente es que ni siquiera tuvieran acceso hacia el exterior.

Antivirus Dentro de nuestro sistema de cómputo es importante contar con antivirus obviamente que estos estén habilitados, actualizados y trabajando en tiempo real.

Si es posible se deberán programar por lo menos dos análisis por mes esto de algún modo nos ayudara a proteger nuestro servidor de virus informáticos y en algunos casos de rootkits, gusanos y virus.

Todos estos métodos se podrían resumir en lo que se conoce como Hardening (palabra en ingles que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, deshabilitar los puertos USB, dar privilegios a usuarios, como lo hemos mencionado anteriormente. Es decir todo aquello que es innecesario en el sistema así como cerrando puertos que tampoco estén en uso además de muchas otros métodos. Este método consiste en hacerles el acceso más difícil a los atacantes, es bien sabido que ninguno sistema es 100% seguro pero con el hardening de lo que trata es de asegurarlo lo más posible que se pueda. En otras palabras se podría decir que es un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo. Su propósito, es entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad. Esto no quiere decir que el sistema se vuelva invulnerable, sino que simplemente lo hace más difícil de penetrar, en la figura 34 hace referencia a perpetradores de la información.

Figura 34 Barreras Informáticas.

4.2.3 Intrusión y Ataques

Para llevar a cabo una intrusión en un sistema; previamente el atacante o intruso debió haber burlado nuestro sistema de seguridad o simplemente ya estar dentro de él. Una vez que ha logrado acceder al mismo puede hacer uso de los recursos y causar algún daño si así lo quisiera o bien robar información al estar infiltrado se puede llevar a cabo un ataque informático y de esta forma intentara desestabilizar el sistema o en el peor de los casos controlarlo.

4.2.3.1 Intrusiones al sistema

Existen diversas formas para poder acceder a un sistema

- Física. El atacante logra acceder al sistema por medio de engaños “Ingeniería Social” o bien logra infiltrarse dentro de una organización haciéndose pasar por un empleado e incluso puede ser gente de limpieza o algo similar.
- Por sistema. Si el intruso se encuentra dentro de un organización y ya ha logrado ganarse la confianza del personal o bien si es un empleado inconforme o resentido y que ya tiene acceso al sistema de igual forma puede causar daño
- Remota. Este método es el más difícil de detectar debido a que pueden tener acceso de manera no presencial y quizá no darnos cuenta de ello, existen diversos programas para manipular un equipo de manera remota y con ellos acceder a un sistema.

4.2.3.2 Técnicas utilizadas

Barrido de puertos. Es una técnica, en la cual el intruso pretende obtener una lista de equipos activos dentro de un rango de direcciones y conocer los puertos abiertos que cada máquina tiene. Cada sistema puede tener un total de 65535 puertos disponibles. Los atacantes usan a menudo esta técnica para encontrar puntos de acceso debilitados para penetrar en los sistemas informáticos por ello es importante solo mantener abiertos los puertos que ocupemos en nuestro sistema para ello podemos apoyarnos de un equipo firewall que nos ayude a bloquear los puertos que no utilizamos.

Bugs. Son los errores que se pueden cometer al desarrollar un programa y la manera en las que nos pueden afectar depende desconcertantes, como que un fichero no pueda imprimirse, o errores graves que afecten a la seguridad de tu PC. Cuando esto es así se convierten en verdaderos agujeros por los que cualquier intruso puede colarse. Es por ello que muchas veces un atacante busca estas vulnerabilidades en los sistemas para invadir ordenadores ajenos como ya lo mencionamos es importante mantener actualizados nuestros programas ya que muchas veces las actualizaciones van corrigieron fallos en el programa.

Backdoors: Es esencialmente cualquier programa o configuración deliberada diseñada para permitir el acceso remoto a un sistema los Troyanos, rootkits, e incluso programas legítimos pueden utilizar para instalar una puerta trasera.

Algunos tipos de puertas traseras pueden incluir programas legítimos como:

- Escritorio remoto de Microsoft,
- Virtual Network Computing (VNC)
- LogMeIn Hamachi
- Teamviewer.

Los programas maliciosos escritos específicamente para proporcionar de nuevo la puerta de acceso como BackOrifice, SubSeven y T0rnki.

4.2.3.3 Esquema del comportamiento

Fase 1: Reconocimiento. Esta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet (buscadores) para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el sniffing.

Fase 2: Exploración. En esta segunda etapa se utiliza la información obtenida en la primera fase para sondear el objetivo y tratar de obtener la mayor información posible sobre el sistema víctima las cuales pueden ser direcciones IP, nombres de host, o datos de autenticación.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

Fase 3: Obtener acceso. En esta etapa comienza a efectuarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración.

Las técnicas que un atacante generalmente puede utilizar son ataques de Buffer Overflow, Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session. Hijacking.

Fase 4: Mantener el acceso. Una vez que se ha conseguido acceder al sistema, el atacante buscará implantar herramientas que le permitan regresar para acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Fase 5: Borrar huellas. Después de que el atacante logró obtener y mantener el acceso al sistema, lógicamente la intención es no dejar rastros para ello tendrá que ir borrando los registros que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS) o del Sistema de Prevención de Intrusos (IPS).

4.2.4 Consecuencias de la falta de Seguridad lógica

El hecho de contar con los controles antes mencionados nos puede ayudar a identificar individualmente a cada usuario y sus actividades en el sistema, y restringe el acceso a datos, a los programas de uso general, de uso específico, de las redes y terminales pero la falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

- Cambio de los datos antes o cuando se le da entrada a la computadora.
- Copias o Robo de programas y/o información.
- Código oculto en un programa
- Entrada de virus

La seguridad lógica puede evitar una afectación de perdida de registros, y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

Un método eficaz para proteger sistemas de computación es mediante software de control de acceso. Los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden al usuario una contraseña antes de permitirle el acceso a la información confidencial. Sin embargo, los paquetes de control de acceso basados en componentes pueden ser eludidos por delincuentes sofisticados en computación, por lo que no es conveniente depender de esos paquetes por si solos para tener una seguridad adecuada.

4.2.4.1 Formas de controlar

Existen diversos técnicas o métodos para controlar los ataques generalmente todas ellas van acompañados de algún dispositivo o programa para tratar de hacer más difícil el acceso a nuestra red o sistema y como lo hemos mencionado es importante hacer uso de todos esos recursos y de esta forma hacer más complicado el acceso para los atacantes y así evitar que los daños o perdida de información sean menores. En los siguientes puntos veremos cómo podemos realizar esto.

4.2.5 Direccionamiento

El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (Ipv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Diseñar, implementar y administrar un plan de direccionamiento IPv4 efectivo asegura que las redes puedan operar de manera eficaz y eficiente

4.2.5.1 Subnetting

El subnetting hace referencia a cómo están direccionadas las redes IP. Se realiza en la capa 3 del modelo de referencia OSI, una dirección en capa de red tiene dos partes: Red: Identifica un grupo de dispositivos individuales.

Host: Identifica los dispositivos individuales de un grupo.

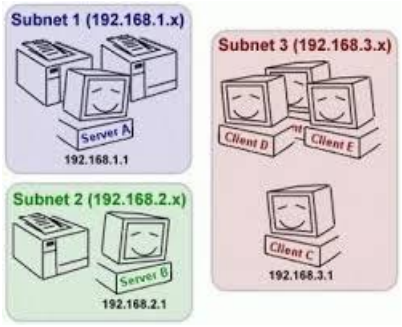

Figura 35 Subneteo de redes.

La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

El Subneteo permite una mejor administración, control del tráfico y seguridad al segmentar la red por función. También, mejora la performance de la red al reducir el tráfico de broadcast de nuestra red.

El subneteo reside en tomar prestado de la parte de los hosts, para la parte de red y así crearemos una subred, en cada clase de IP solo hay determinados bits para tomar prestados. Así a medida de que se aplican más host a la red, se crearan más subredes.

Existen dos fórmulas para calcular el número de subredes y de host por subred, son las siguientes:

Numero de Host x Subred = (2 elevado al número de bits usados de host)-2

Numero de Subredes = (2 elevado al número de bits usados para subnetear)-2

Para aplicar el subneteo solo necesitamos saber la dirección de la red y broadcast de cada subred, para eso tenemos que restarle 225 a la máscara de subred, ejemplo:

255-192 = 63 de manera que la Dirección de red de la Primera subred es 64

Y para saber la dirección de la segunda subred, solo tenemos que sumarle a la primera subred el resultado que nos dio anteriormente, que en este caso es 64, y nos resultara 128 esa será la dirección de la segunda subred, y así sucesivamente para cada una de las subredes.

4.2.5.1 VLAN's como una forma de seguridad lógica.

Una Virtual Local Área Network (VLAN) o red de área local virtual es un grupo flexible de dispositivos que se encuentran en cualquier ubicación de una red de área local pero que se comunican como si estuvieran en el mismo segmento físico.

Con las VLANs se puede segmentar la red sin restringirse a las ubicaciones o conexiones físicas.

Las ventajas que nos pueden aportar las VLANs son entre otras:

- Mayor flexibilidad y mejor gestión de recursos, al facilitar el cambio y movimiento de los dispositivos en la red.
- Facilidad de localización y aislamiento de averías.
- Mejora en cuanto a seguridad, debido a la separación de dispositivos en distintas VLANs.
- Control de tráfico de broadcast.
- Separación de protocolos.

Se pueden implementar atendiendo a diversos criterios como puertos de un switch a los que se conectan los host, direcciones MAC, etc.

4.2.5.1.1 Generaciones de VLAN

Basadas en puertos y direcciones MAC

Internet Working; se apoya en protocolo y dirección capa tres.

De aplicación y servicios: aquí se encuentran los grupos multicast y las VLAN definidas por el usuario.

Servicios avanzados: Una vez que se cumple con los tres criterios antes de realizar alguna asignación a la VLAN; se puede efectuar por medio de DHCP (Dynamic Host Configuration Protocol “Protocolo de Configuración Dinámica”) o bien mediante una AVLAN (Authenticate Virtual Local Area Networks “Redes Virtuales Autenticadas de Área Local”).

VLAN por Puerto

Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN, el problema se presenta cuando se quieren hacer VLAN por MAC ya que la tarea es compleja. Aquí el puerto del switch pertenece a una VLAN, por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN amarilla, el servidor estará en la VLAN amarilla.

VLAN por MAC

Se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación.

Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que meterse con las direcciones MAC y si no se cuenta con un software que las administre, será muy laborioso configurar cada una de ellas.

VLAN por Protocolo

Lo que pertenezca a IP sé enrutara a la VLAN de IP e IPX se dirigirá a la VLAN de IPX, es decir, se tendrá una VLAN por protocolo. Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectara automáticamente a la VLAN correspondiente.

VLAN por subredes de IP o IPX

Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión dentro de este para que el usuario aunque esté conectado a la VLAN del protocolo IP sea asignado en otra VLAN subred que pertenecerá al grupo 10 o 20 dentro del protocolo.

VLAN definidas por el usuario

En esta política de VLAN se puede generar un patrón de bits, para cuando llegue el frame. Si los primeros cuatro bits son 1010 se irán a la VLAN de ingeniería, sin importar las características del usuario protocolo, dirección MAC y puerto.

Si el usuario manifiesta otro patrón de bits, entonces se trasladara a la VLAN que le corresponda; aquí el usuario define las VLAN.

VLAN Binding

Se conjugan tres parámetros o criterios para la asignación de VLAN: si el usuario es de un puerto x, entonces se le asignara una VLAN correspondiente.

También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN.

VLAN por DHCP

Aquí ya no es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente. Esta política de VLAN es de las últimas generaciones.

4.3 Seguridad Perimetral

Las empresas y organizaciones que están conectadas a internet se encuentran en riesgo de a ataques o infiltraciones, y aún más hay incremento con el crecimiento de la red y de los dispositivos móviles. Existen mecanismos, medidas, dispositivos que deben formar parte de un plan de seguridad y que deben ser imprescindibles y responsables del resguardo de la red. Los objetivos son prevenir, detener y bloquear ataques externos, dentro de la organización a diferentes áreas internas y sobre todo el control para el uso adecuado del internet.

La seguridad perimetral permite una gestión más fácil ya que centra la administración en puntos estratégicos que reforzamos con las herramientas indicadas y debe estar acompañado de políticas de seguridad. La falta o debilidad de seguridad perimetral abre un agujero de seguridad en la red y origina que un intruso pueda aprovecharse de ello.

4.3.1 Firewall

Dispositivo que tiene un conjunto de reglas para especificar que tráfico se acepta y se deniega, además de bloquear y habilitar el tráfico. Los firewalls son diseñados de forma que todo lo que no es expresamente autorizado, es prohibido por defecto.

Un firewall protege la red interna de una organización, al hacerlos invisibles de los usuarios que residen en redes externas. Un firewall permite el paso entre las dos redes a sólo los paquetes de información autorizados. Los firewalls pueden ser usados internamente, para formar una barrera de seguridad entre diferentes partes de una organización. Ejemplo gráfico de cómo se interpreta un firewall, se muestra en la figura 36.

Figura 36 Firewall.

Un firewall puede mejorar significativamente el nivel de seguridad en la red y reducir los riesgos filtrando la falta de seguridad inherente en los servicios de Internet.

Hay básicamente tres técnicas aproximadas a la arquitectura de firewall: Packet Filter, Stateful Packet Inspection y Application Gateway.

- Packet Filter es muy usado frecuentemente para describir firewalls que bloquean o pasan tráfico, comparando con la información encontrada en el encabezado de cada paquete de salida o entrada contra una tabla de reglas de control de acceso. Los firewalls Packet Filtering son rápidos, debido a que operan en la capa de red y hacen solamente verificaciones superficiales de la validez de una conexión dada.

- Application Gateway es un programa de aplicación que corre sobre un sistema de firewall entre dos redes denominado proxy. Cuando un programa cliente establece una conexión a través de un Gateway a un servicio destino, primero establece una conexión directamente al programa de Gateway en el servidor.
  El cliente entonces negocia con el Gateway para que establezca una conexión en su nombre hacia el servicio destino. Si es satisfactorio, entonces se regeneran dos conexiones: una entre el cliente y servidor Gateway y otra entre el servidor Gateway y el servicio destino. Una vez establecida, el gateway recibe y envía tráfico en forma de dos vías entre el cliente y el servicio.

- Stateful Packet Inspection. (SPI) Basado en la tecnología de Packet Filtering, el modelo de SPI agrega más verificaciones de seguridad en un intento para simular las verificaciones de seguridad de un firewall de Application Gateway.

  En lugar de simplemente ver las direcciones de cada paquete de entrada, el firewall de SPI intercepta los paquetes de entrada en la capa de red hasta que se tiene la suficiente información para hacer algunas determinaciones sobre el estado del intento de conexión.

4.3.2 Router de perímetro

Un router es un componente de la red, que permite la interconexión entre dos o más redes no necesariamente de la misma tecnología física. El router por concepto se conoce que trabaja hasta la capa de red del modelo de referencia OSI. Dentro de un esquema de seguridad perimetral de Internet, el router juega el papel de proveer el acceso a la Internet, así como de representar la primera línea de defensa en contra de intrusos. También representa un punto de separación entre los recursos propios de la organización y los que no le pertenecen, normalmente del proveedor de Servicio Internet.

4.3.3 Honeypot

Un Honeypot es un sistema de hardware y software que está colocado en una red en la que se espera habrá ataques desde redes desconocidas como Internet y que ha sido configurado para resistir cualquier tipo ataques. Con frecuencia, los honeypot son utilizados como plataforma para firewalls, Gateway de aplicaciones internas, para servidores de servicios de acceso público tales como Web, FTP, DNS, SMTP, o mediadores de servicios de Internet para hosts internos. Normalmente, un honeypot está ejecutando alguna aplicación sobre un sistema operativo de propósito general.

Un honeypot es colocado en los perímetros de red más cercanos a Internet, lo que lo hace más vulnerable de ataques, para ello la seguridad de sus servicios del sistema de red y aplicaciones se encuentran afinados lo mejor posible.

4.3.4 Servidor proxy

Un proxy server es una computadora sencilla cuyo propósito es concentrar los servicios de aplicación. Típicamente una computadora sencilla que actúa como un proxy server para una variedad de protocolos (Telnet, SMTP, FTP, HTTP, etc.) aunque existen computadoras individuales para un solo servicio.

En lugar de conectarse directamente a un servidor externo, el cliente se conecta al proxy server el cual deja iniciar una conexión al servidor externo solicitado. Dependiendo del tipo de proxy server usado, es posible configurar los clientes internos para hacer esta redirección de forma automática, sin conocimiento para el usuario, otro pueden requerir que usuario se conecte directamente al proxy server y luego inicie la conexión a través del formato especificado, en la figura 37 se muestra un ejemplo de este esquema.

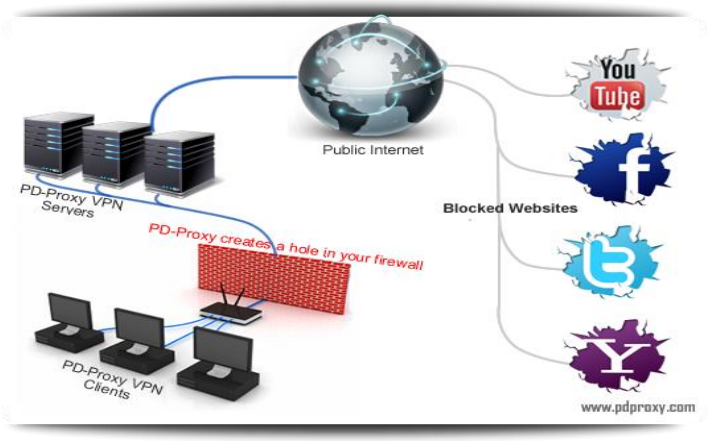

Figura 37 Proxy Server.

4.3.5 Sistema de detección de intrusos

Los sistemas de detección de intrusos o IDS (Intrusion Detection Systems) actúan como una segunda línea de defensa contra cualquier actividad que no haya sido identificada por los sistemas de seguridad tradicionales como firewalls. El objetivo de la detección de intrusos es identificar en tiempo real cualquier actividad sospechosa, mal uso o abuso de los sistemas informáticos, tanto si tienen su origen en usuarios de la red interna, como si se trata de ataques externos. El nivel de sofisticación en la identificación de ataque varía desde violaciones aisladas, sucesos que a lo largo del tiempo acaban constituyendo una violación, y hechos secuenciales que suponen una violación.

La detección de intrusos supone un gran reto debido a la proliferación de los tipos de conexiones entre redes e Internet, la mezcla de sistemas operativos, la variedad de protocolos y la diversidad de aplicaciones de dominio público y privadas.

Los sistemas de detección de intrusos pueden categorizarse, en un primer nivel, de la siguiente manera:

- NIDS: sistemas que analizan el tráfico de la red completa.
- HIDS: sistemas que analizan el tráfico sobre un servidor o estación de trabajo.

4.3.6 Sistema de Prevención de Intrusos

Un Sistema de Prevención de Intrusos a menudo es considerado como una extensión de los IDS debido a que en ambos monitorean nuestro sistema sin embargo esto no es correcto ya que se le debe considerar como otro método de control de accesos diferente; su función principal en ambos casos es detectar cualquier actividad maliciosa que implique algún riesgo, de igual modo nos ayuda a identificar y reportarla.

Un IPS al igual que un IDS funciona por medio de módulos, pero la diferencia entre ellos es que un IDS alerta al administrador ante la detección de un posible intruso, pero generalmente es cuando ya se encuentra dentro de nuestro sistema mientras que en un Sistema de Prevención de Intrusos se puede establecer políticas de seguridad para proteger al sistema o la red de algún ataque; en resumen se puede decir que un IPS protege nuestra red de manera proactiva mientras que un IDS lo hace de manera reactiva.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Firmas, como lo hace un antivirus.
- Detección Basada en Políticas, el IPS Requiere que se declaren muy específicamente las políticas de seguridad.
- Detección Basada en Anomalías, Funcionan con el patrón de comportamiento normal de Tráfico.

Detección Basada en Firmas: Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto, y entonces lanza una alerta. Como este tipo de detección funciona parecido a un Antivirus, el Administrador debe verificar que las firmas estén constantemente actualizadas.

Detección Basada en Políticas: En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

Detección Basada en Anomalías: Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición ‘normal’. En este tipo de detección se clasifica de la siguiente manera:

Detección Estadística de Anormalidades: El IPS analiza el tráfico de red en un determinado periodo de tiempo y en base a eso crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.

Detección No Estadística de Anormalidades: En este tipo de detección, es el administrador quien define el patrón ‘normal’ de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

4.3.7 Zona desmilitarizada

Uno de los aspectos más importantes de seguridad asociados con la conexión de redes privadas en Internet es la contención. Se necesita separar cada sistema y servicio para prevenir la corrupción o compromiso de unos de llevar a la corrupción o compromiso de otros. La solución

es una zona de amortiguado controlada entre los servicios extremos y el entorno interno. Esta es la razón por la cual se define la zona desmilitarizada o DMZ

La DMZ es una red aislada que contiene servicios que están directamente accesibles de Internet. La DMZ es un amortiguador entre la red corporativa y el mundo externo. La DMZ tiene un único número de red que es diferente del número de red corporativo. Solamente la red DMZ es visible al mundo externo.

Un lado está conectado a Internet, mientras el otro está conectado a la red interna. Ambos lados están protegidos por firewalls, los cuales están configurados para limitar los protocolos, direcciones origen y destino de paquetes que pasan entre todas las redes, en la figura 38 se muestra un ejemplo de una configuración de un DMZ.

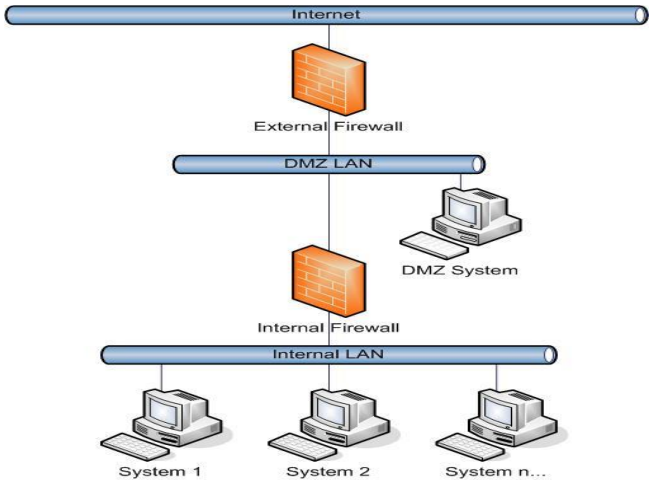

Figura 38 Zona Desmilitarizada.

4.3.8 Proceso de seguridad

Una vez vistos los conceptos básicos de la seguridad de redes, se debe aplicar un conjunto de pasos iterativos que permitan definir el ciclo de vida del modelo de seguridad que se desea implementar en la empresa. Básicamente, estos pasos constituyen el proceso de seguridad de la empresa. Habitualmente consta de cuatro pasos, tal y como se muestra en la Figura 39:

1. Estimación. Preparación de los elementos asociados al resto de pasos del proceso. En este caso se ocupa de hacer un estudio de las políticas, procedimientos, leyes y reglamentos que se deben cumplir para garantizar la protección de los recursos.
2. Protección. Se define como la aplicación de medidas para reducir la probabilidad de compromiso del recurso a proteger. Se puede decir que es equivalente a prevención, pero hay que recordar que uno de los axiomas que se comentaron antes es que la prevención fracasará.

3. Detección. Se perfila como el paso en el que se produce la identificación de intrusiones. Las intrusiones se pueden definir como violaciones de la política de seguridad (definida en el paso 1) o incidentes de seguridad en un ordenador.
4. Respuesta. Proceso de verificar los resultados de la detección y de dar pasos necesarios para remediar las intrusiones. Una de las técnicas más usadas consiste en la "vuelta atrás" mediante la recuperación del estado del recurso (por ejemplo una copia de seguridad de una base de datos) en un momento anterior.

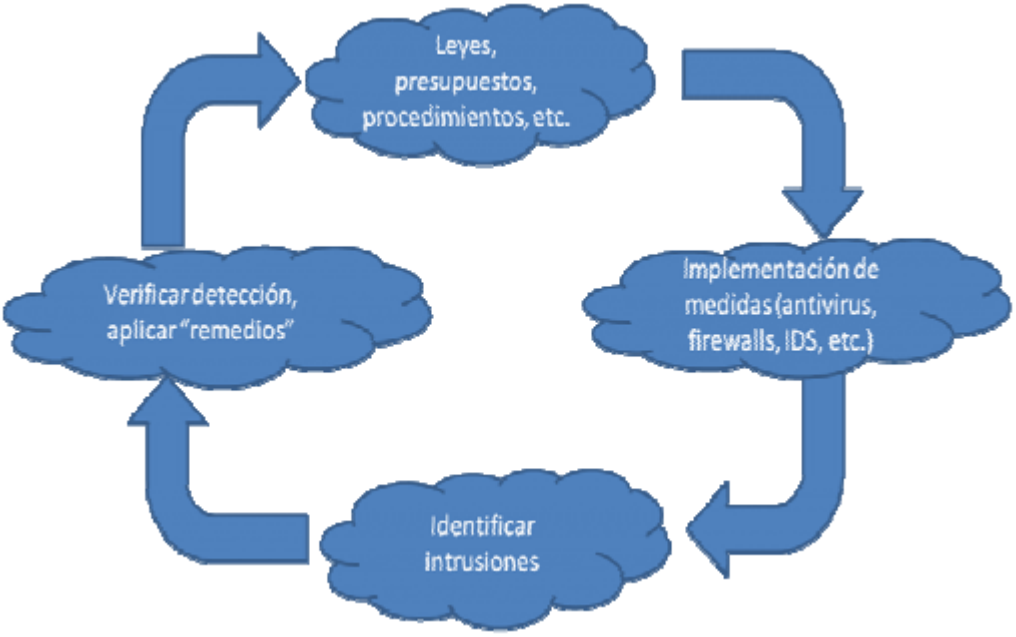

Figura 39 Proceso de Seguridad.

Capítulo 5 Propuesta de implementación

El desarrollo de este capítulo, describe la propuesta de implementación de Microsoft Lync con la integración de telefonía IP en la Empresa Tecprotel.

5.1 Descripción de la Empresa

Técnicos Profesionales en Telefonía S.A. de C.V. a quien en lo sucesivo llamaremos TECPROTEL Nace en 1989 gracias a la vocación de servicio en telefonía y a la visión de su fundador el Sr. Lino Reza Cornejo quien vio la oportunidad de crear una empresa que pudiera satisfacer de servicios, mantenimiento, instalaciones, cableado de voz y ahora de datos entre otros, al mercado de las telecomunicaciones ya que dichos servicios solamente los proporcionaba de manera monopólica y con muchas deficiencias la empresa Teléfonos de México (TELMEX) cuando ésta era administrada por el gobierno.

Sus principales retos inician en los noventas cuando en 1992 TELMEX deja de ser un monopolio y el gobierno permite la competencia de nuevos proveedores como Alestra (AT&T), Avantel (ahora Axtel), Maxcom, y más recientemente Iusacell y Cablevisión. De esta manera TECPROTEL se enfrenta a una fuerte competencia que antes no existía ya que el nacimiento de estos nuevos “carriers” genera la creación de más empresas que serán sus competidores directos en esta Área.

Al llegar al siglo XXI con él llegaron nuevos retos fue en el año 2002 cuando logran demostrar a TELMEX que se cuenta con la experiencia, instalaciones y capacitación para su personal técnico y así poder ser representante autorizado de la misma y se firma un convenio para poder ofrecer a sus clientes servicios como: venta de líneas telefónicas convencionales, digitales, internet infinitum, Internet Dedicado Empresarial (IDE) así como enlaces dedicados, al mismo tiempo esto permite que empresas que solicitan a TELMEX atención personalizada de servicios de telecomunicaciones específicos y que esta no proporciona, refiera a estos clientes con TECPROTEL para que esta los atienda ampliando así su cartera de clientes y teniendo mayor protagonismo.

Este hecho cambia el paradigma de las comunicaciones y genera nuevas metas como: la expansión, innovación, integración y capacitación en nuevas tecnologías, empieza a penetrar con mucha fuerza la tecnología IP (Internet Protocol) en el ramo de las comunicaciones y la telefonía tradicional que usualmente solía ser analógica y digital empieza a migrar hacia las comunicaciones unificadas (integración de las fuentes de información más utilizadas como los mensajes de voz, fax y e-mail), esto hizo necesario el aprender tecnologías de redes y datos que antes no eran requeridos o solicitados por los clientes lo cual le ha venido a dar un nuevo rumbo a la empresa para poder integrar de la manera más óptima las redes de datos con la telefonía y por ello ahora es necesario ofrecer soluciones de voz y datos en conjunto.

Actualmente debido a las necesidades de los clientes y los avances tecnológicos a nivel mundial cada vez son más los requerimientos de los clientes hoy en día la VoIP, la movilidad, la colaboración, la telefonía IP, la mensajería unificada, las redes inalámbricas, las redes virtuales son algunas de las peticiones más recurrentes para la empresa es por ello que sea ha vuelto una prioridad contar con personal capacitado para el manejo de las Comunicaciones Unificadas.

5.2 Fase I Planeación

Dentro de la metodología utilizada la primera fase que se aborda es la planeación, donde el objetivo es convertir la solución conceptual en diseños y planes tangibles para que se puedan compilar en un seguimiento de la propuesta.

5.2.1 Problemática Actual

La empresa Técnicos Profesionales en Telefonía S.A. de C.V. También conocida como TECPROTEL es un Bussines Partner de AVAYA y representante autorizado de Teléfonos de México su especialidad son las telecomunicaciones, diseño, instalación e implementación de soluciones de voz y datos.

Como en la mayoría de las empresas en la actualidad, sus empleados tienen la necesidad de salir a reuniones, viajan, o trabajan desde casa si así lo requieren; además de esto el personal de TECPROTEL proporciona servicios en sitio o salen a tomar capacitaciones; en consecuencia constantemente están fuera de la empresa; y para todo directivo se ha vuelto una prioridad el poder localizar a sus subordinados sin importar el lugar donde se encuentren; derivado de esto surge la necesidad de encontrar diferentes canales de comunicación que sean fáciles de utilizar y permitan hacer llegar la información al empleado; sin embargo no se cuenta con una infraestructura óptima que permita tener una comunicación eficiente y con ello lograr optimizar los procesos de negocio de la compañía.

La tecnología que se maneja hoy en día por parte de TECPROTEL difiere mucho de los requerimientos necesarios en la actualidad en el mundo de las telecomunicaciones y de las mismas necesidades de la empresa; es por ello que analizando las deficiencias nos propusimos presentar una propuesta de modernización para implementar comunicaciones unificadas con telefonía IP.

Actualmente TECPROTEL maneja su telefonía con la tecnología de AVAYA a través de un IP Office 406, se cuenta con un módulo E1 para 30 extensiones telefónicas también algunos de los empleados cuentan con radio Nextel para la comunicación cuando están fuera de la

empresa; el resto de los empleados cuentan con su propio plan de datos o por saldo para comunicarse cuando salen de visita con los clientes.

La red actual se encuentra centralizada manejando voz y datos por separado, siendo el enlace a Internet a través de 2 modems infinitum de 2 y 6 MB respectivamente y por medio de un switch 3COM; dentro del cual se encuentra un Access Point para la red inalámbrica, el Gateway se lleva a cabo por medio de un firewall Wacthguard XTM 550e.

El servidor es de 32 bits con 2 Gb en RAM maneja la plataforma de Microsoft Windows Server Standard 2008 en donde se aloja el directorio activo en el que están integrados los usuarios para otorgar medidas de control y de seguridad. Los equipos de cómputo cuentan con sistemas operativos. XP y Windows 7 predominando Windows 7.

En lo que se refiere a la administración del correo electrónico está basada en un servidor de correo electrónico con plataforma Linux Parallels Plesk Control Panel el cual está asociado con Microsoft Outlook 2007 para que los usuarios puedan tener intercambio de mensajes dentro y fuera de la empresa.

Debido a que TECPROTEL tiene planes de crecimiento a corto y mediano plazo se evalúa la posibilidad de modernizar su infraestructura básica de telecomunicaciones; es por ello que con base a nuestra propuesta de tesis deseamos presentar una solución aprovechando los recursos y la tecnología de AVAYA existentes, implementar Comunicaciones Unificadas con integración de Telefonía IP y así lograr la convergencia de múltiples tecnologías en una sola solución que sea fácil de manejar sin que esto represente grandes costos, le otorgarán una herramienta integral con los servicios más utilizados y funcionales para mejorar desempeño de la empresa.

5.2.2 Actividades que debe desarrollar “TECPROTEL”

El personal técnico especializado de **“TECPROTEL”** (servicio), será el responsable para realizar las tareas de apoyo en el proyecto **“Plataforma de Colaboración con Lync Server 2010”,** teniendo como visión: Implementar una Solución que permita la comunicación confiable, segura y flexible en TECPROTEL, mediante un cliente de uso intuitivo y fácil en el cual convergen las tecnologías más utilizadas para comunicación; Mensajería Instantánea, Telefonía y Correo electrónico.

En la figura 40 se muestra un diagrama de la red física de datos que actualmente se encuentra en operación.

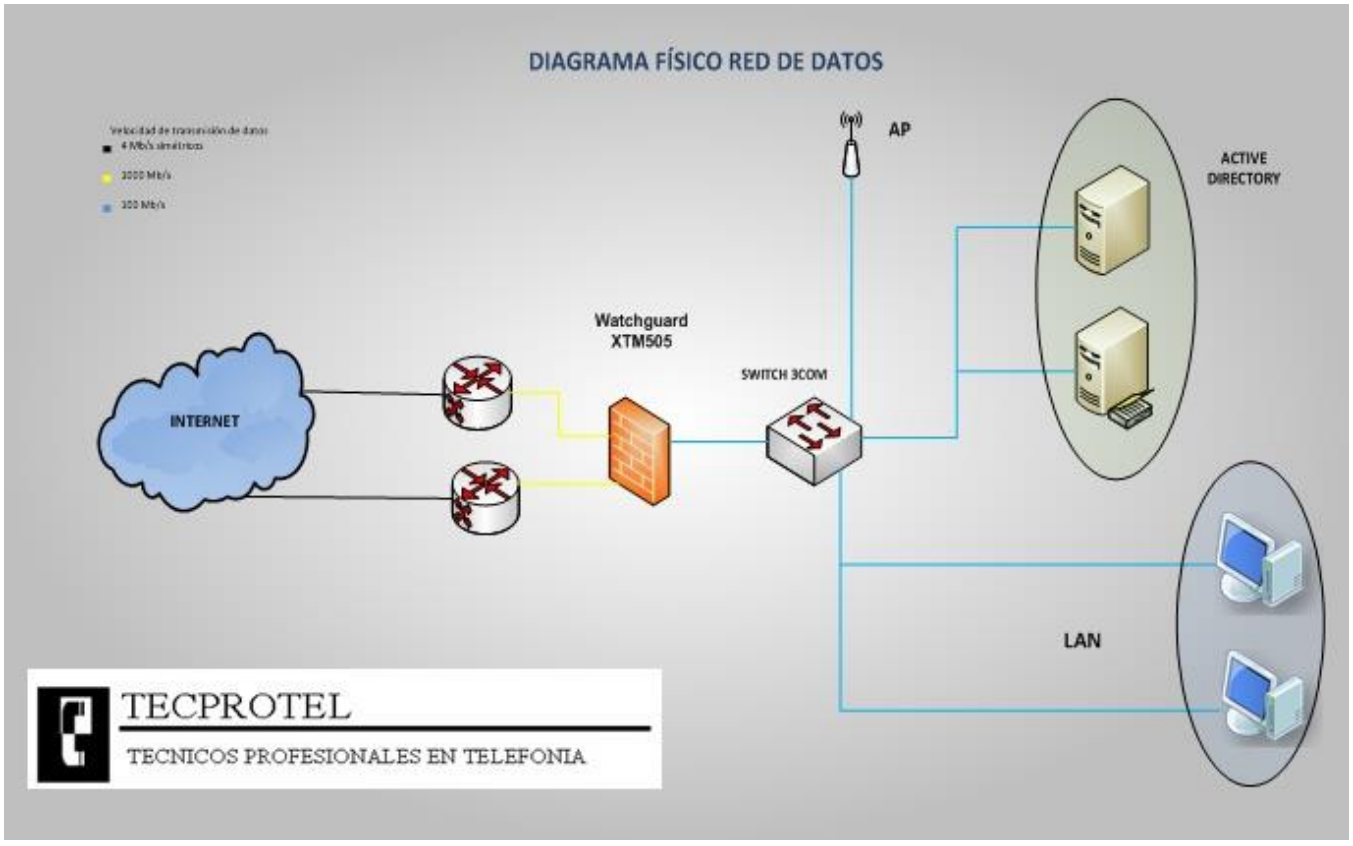

Figura 40 Diagrama Físico de la Red de Datos de TECPROTEL

La figura 41 muestra la red telefónica que opera actualmente en Tecprotel.

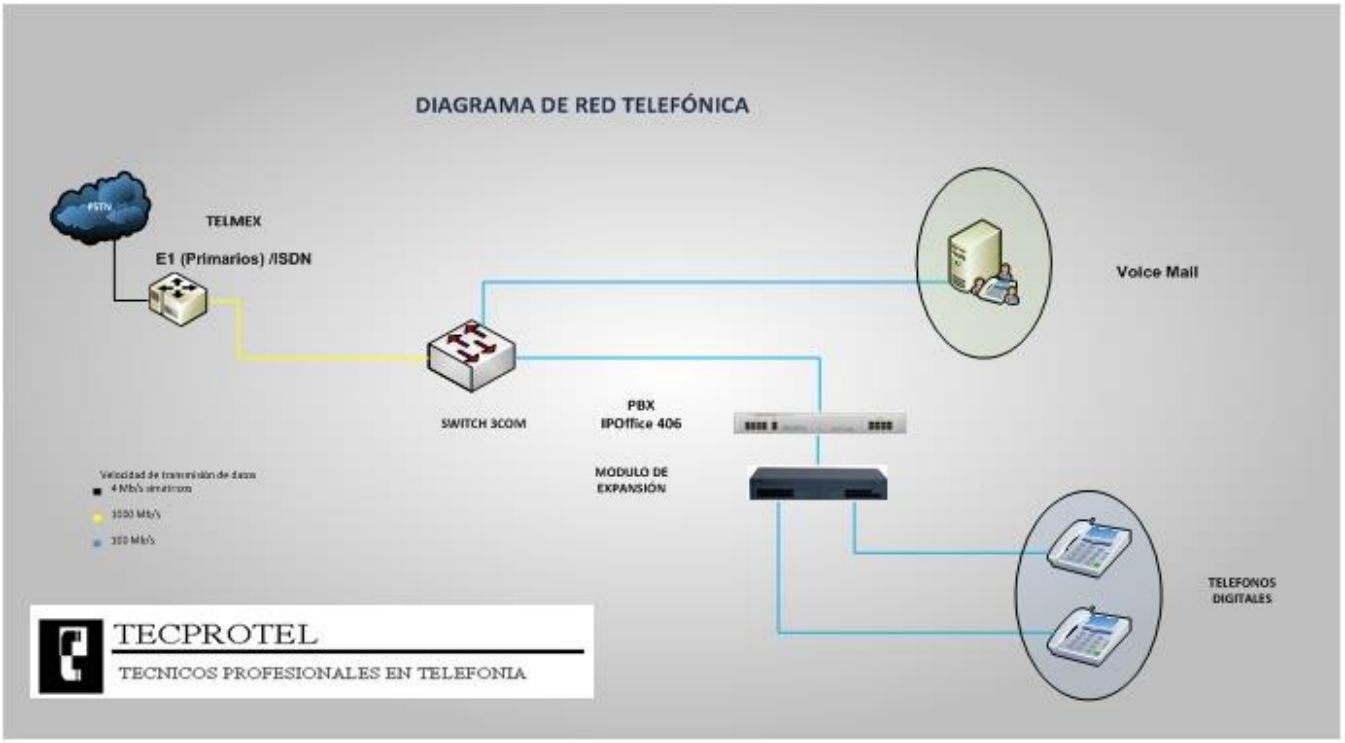

Figura 41 Diagrama de Red Telefónica

El diagrama lógico de la red de datos de Tecprotel se muestra en la 42.

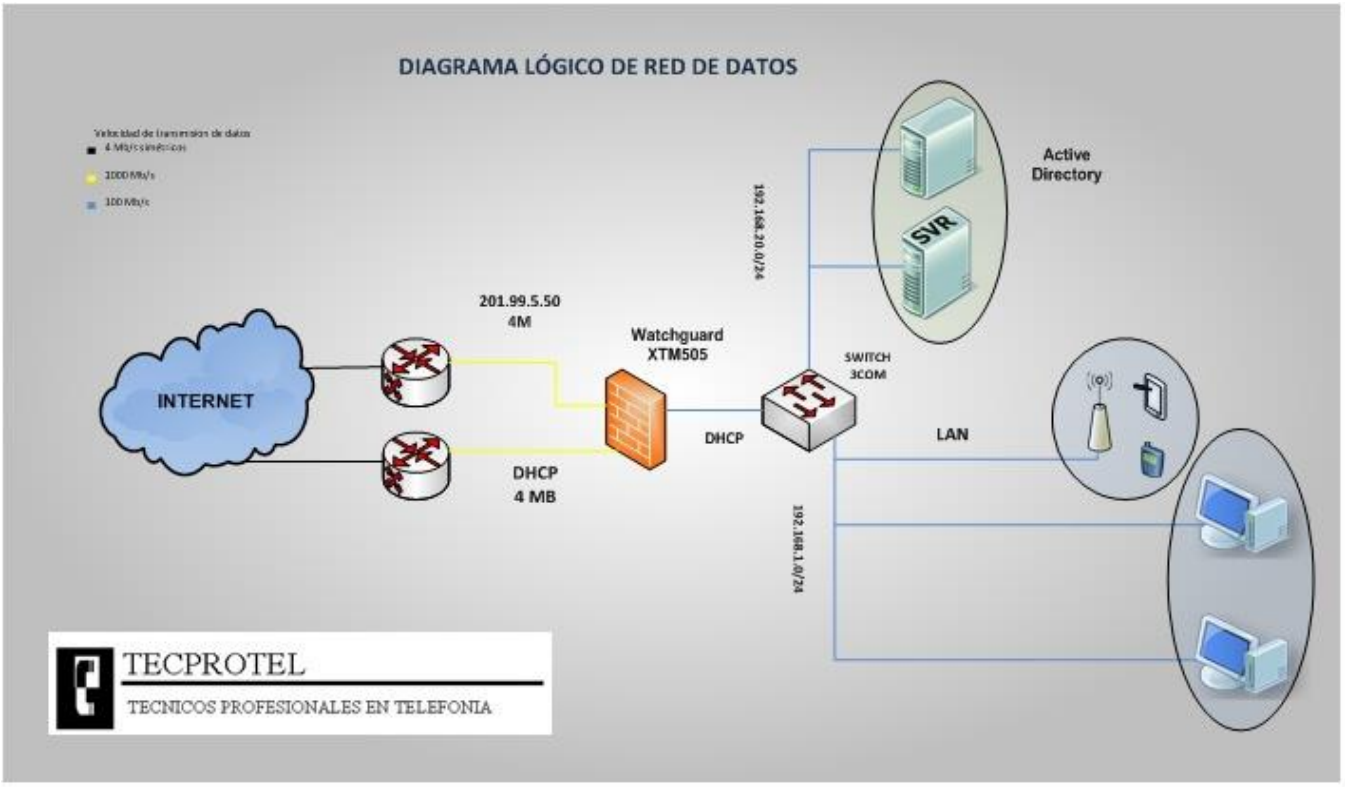

Figura 42 Diagrama Lógico de red de Datos

5.2.2.1 Actividades previas

I. Realizar un levantamiento de equipo de cómputo y telefonía con la que cuenta Tecprotel.
II. Identificación de usuarios y servicios.
III. Realizar un levantamiento de equipo de cómputo y telefonía.

Respecto a la red actualmente trabaja con un cableado no certificado de categoría 5e tanto para la red de datos y la de telefonía digital.

Se cuenta con un switch de capa 2 no gestionable; el cual es una desventaja ya que no cuenta con mecanismos de seguridad en la red y cualquiera puede conectarse a sus puertos además de no poder configurar VLAN´s en este dispositivo lo cual representa una desventaja y se dificulta su administración.

En cuanto al ruteo el dispositivo encargado de hacer esto. Es un firewall Watchguard que además es el encargado de brindar seguridad a la red ya que cuenta con la tecnología de UTM (SpamBlocker, WebBlocker, Gateway Antivirus, Intrusion Prevention Service). Cuenta con licencias activas para UTM y para actualización de software, el equipo permite 5 conexiones vpn móviles con crecimiento de hasta 55 conexiones, las cuales son controladas por medio de licencias; para conexiones de sitio a sitio permite hasta 50; además de esto nos permite hacer hasta 55 VLAN's, por otra parte además tiene integrada la licencia para MultiWAN con ella se puede trabajar con dos enlaces de internet.

Para la parte administrativa se cuenta con 3 servidores los cuales se ocupan principalmente de las siguientes tareas.

1. Servidor de almacenamiento y gestión del directorio activo y otros aplicativos (Tptserv).
2. Servidor para la mensajería instantánea y la presencia (OnexPortal).
3. Y servidor para el correo de voz y tarificador de llamadas (VoiceMail).

A la fecha se está trabajando con tres enlaces de Telmex con 4 MB asimétricos cada uno, uno de ellos trabaja con una IP fija para poder realizar conexiones remotas hacia la oficina.

En la parte de telefonía se tienen contratadas troncales digitales (E1) con 10 canales, 3 líneas, un conmutador IPOffice 500 v2 junto con un módulo de extensiones digitales los teléfonos son únicamente digitales aunque se cuenta con Licencias para poder trabajar con Teléfonos IP (5) en esta parte es importante mencionar que el equipo está preparado para tener un crecimiento de hasta 384 extensiones digitales o extensiones IP estas últimas requieren Licencias y las digitales por medio de tarjetas o módulos de expansión tienen su crecimiento, también mediante

licencias se puede aprovechar la parte de correo de voz para mensajería unificada, también dicho conmutador puede trabajar a través de una Small Community Network en red con otro en alguna otra sucursal si así lo exigiera la carga de trabajo igualmente con Licencias.

Cabe mencionar que no se cuenta con un espacio adecuado donde se puedan concentran los recursos necesarios para el procesamiento de la información de la organización es decir que el Site no reúne los requerimientos necesarios para un buen funcionamiento como son:

- Contar con corriente regulada.
- Contar con planta de emergencia para casos de interrupción de energía eléctrica de las líneas principales.
- Tener un espacio dedicado y exclusivo para el funcionamiento de los servidores y equipos de comunicación.
- Contar con una refrigeración para mantener la temperatura de los dispositivos en condiciones de funcionamiento óptimos.
- Contar con equipos extintores.
- Contar con controles de acceso.

Para la parte de respaldos se cuenta con un disco duro externo de 1TB y manualmente se hacen los respaldos de los archivos importantes.

La parte de red inalámbrica está compuesta con dos Access point Linksys wrt54g y wg54g los cuales se pueden considerar como obsoletos a pesar de que manejan un cifrado WPA no pueden generar multiSSID para mayor seguridad ni son capaces de generar VLAN's.. Por otro lado como ya hemos mencionando antes la tecnología 802.11g ha sido reemplazada por la 802.11n hace ya algunos años.

Finalmente hablaremos respecto a los equipos de cómputo.

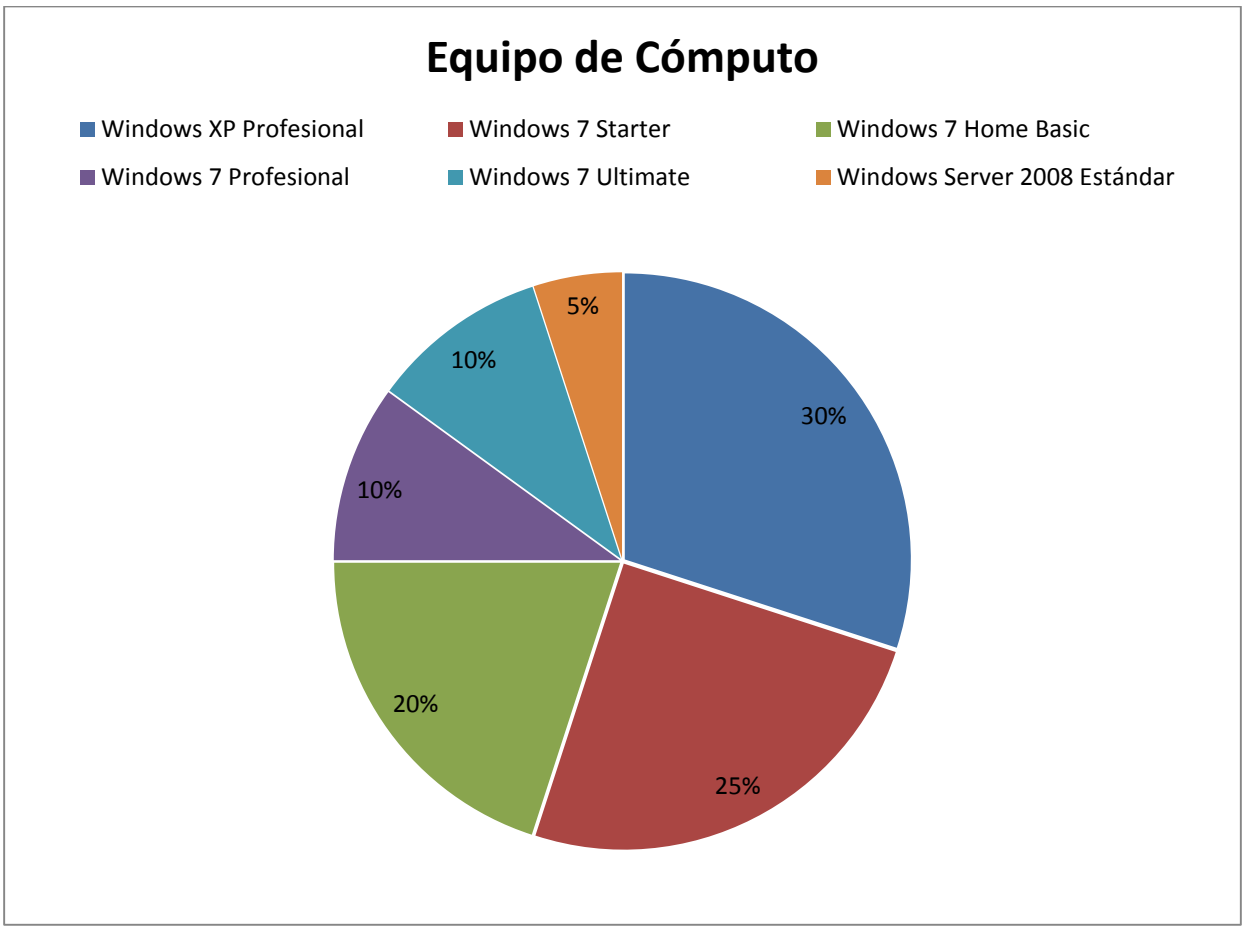

Figura 42 Porcentaje de equipos de cómputo

Como podemos observar en la Figura 42 la mayoría de ellos todavía trabajan con un sistema operativo Windows XP (un sistema que ya va de salida y que Microsoft anuncio que le ha dejado de brindar soporte).Los siguientes sistemas operativos que se manejan dentro de la empresa sin Windows 7 en sus versiones Basic o starter.

A continuación se muestra la relación del equipamiento con la que cuenta la empresa Tecprotel:

En la siguiente figura se hace referencia a los usuarios y servicios con los que se plantea esté operando el sistema.

II. Identificación de usuarios y servicios.

TECPROTEL	
Características habilitadas	**Configuración de capacidad**
• Mensajería instantánea y presencia • IPv4 • Conferencia A/V • Conferencia web • Lync Web App • Chat persistente • Supervisión • Archivado • Movilidad • Integración de archivado de Exchange • Grupo de respuesta • Servicio de anuncio • Servicio de estacionamiento de llamadas • Anuncio de conferencia • Servicio de operador de conferencia • Conferencia de acceso telefónico local • Control de admisión de llamadas • Acceso de usuarios externos • Alta disponibilidad para usuarios externos • Telefonía IP empresarial • Mensajería unificada de Exchange • Integración de Office Web Apps Server	• 100% de usuarios de archivado • 40% de usuarios de notificación • 50% de usuarios de Lync Web App • 20% de usuarios de chat persistente • 100% de usuarios de voz • 65% de llamadas de omisión de medios • 60% de llamadas de UC a RTC • 0.05% de usuarios del servicio de estacionamiento de llamadas • 0.15% de usuarios del grupo de respuesta • 4 llamadas por hora • Línea de red E1 • Ningún PBX implementado • Puerta de enlace de 4 puertos • 30% de conferencias simultáneas • 30% de conferencias de acceso telefónico local simultáneas • 75% de conferencias web con voz simultáneas • 50% de conferencias de mensajería instantánea en grupo simultáneas • 50% de usuarios de mensajería unificada de Exchange • 30% de usuarios externos

Tabla 3 Características habilitadas y Capacidad de configuración

A continuación se hace una descripción más detallada con los siguientes componentes de la solución por perfiles de usuario

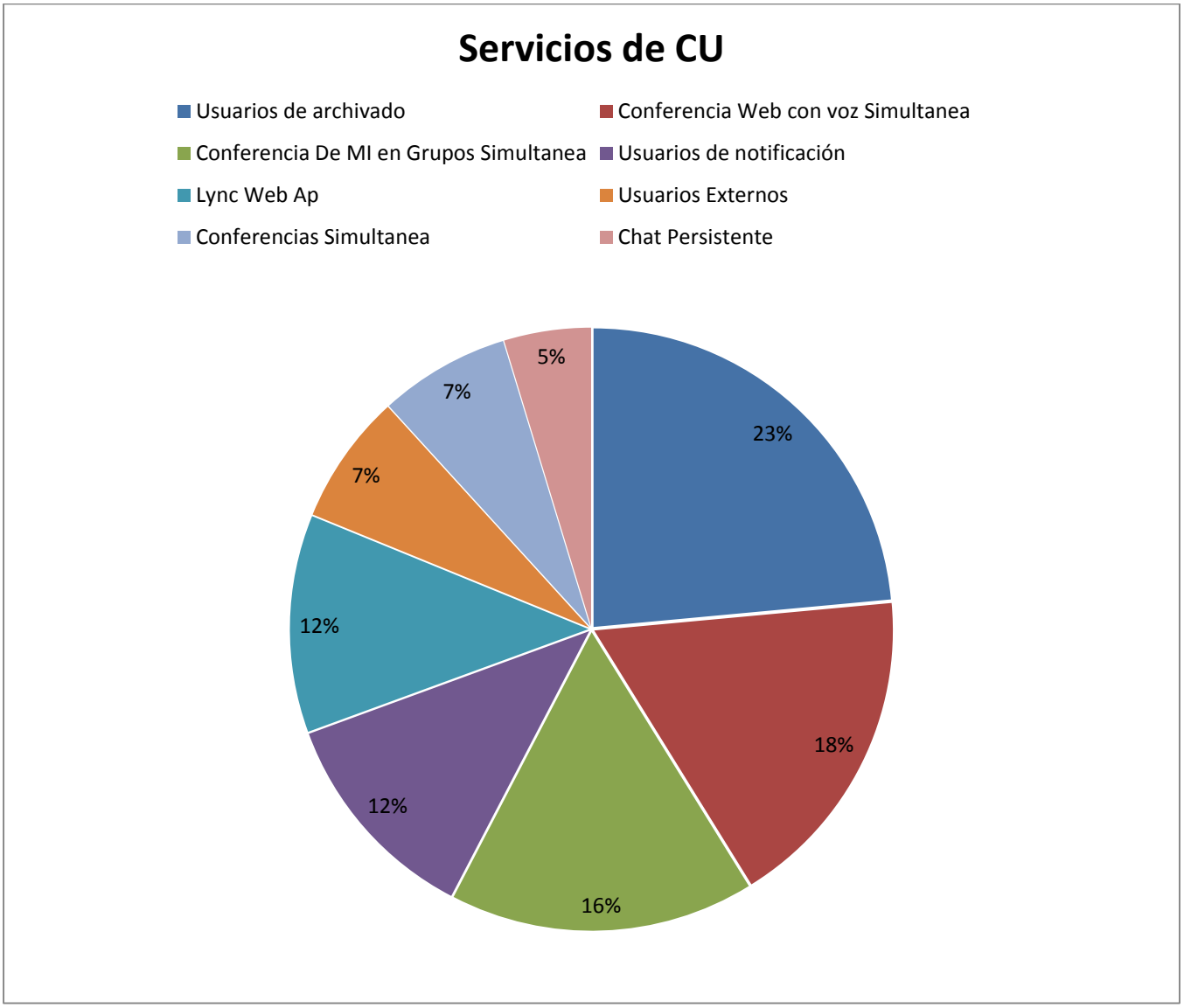

Figura 43 Perfiles de Usuario.

En la figura 43 podemos observar una clasificación de los servicios que se les va otorgar a cada usuario de acuerdo a su perfil y función que realiza en la empresa. Como podemos observar el servicio de Archiving es el que más solicitaron ya que les permite almacenar las conversaciones del Chat y de las conferencias. Los servicios de Conferencia por Mensajería Instantánea (IM) y Conferencia Web fueron los siguientes en los que más se interesaron.

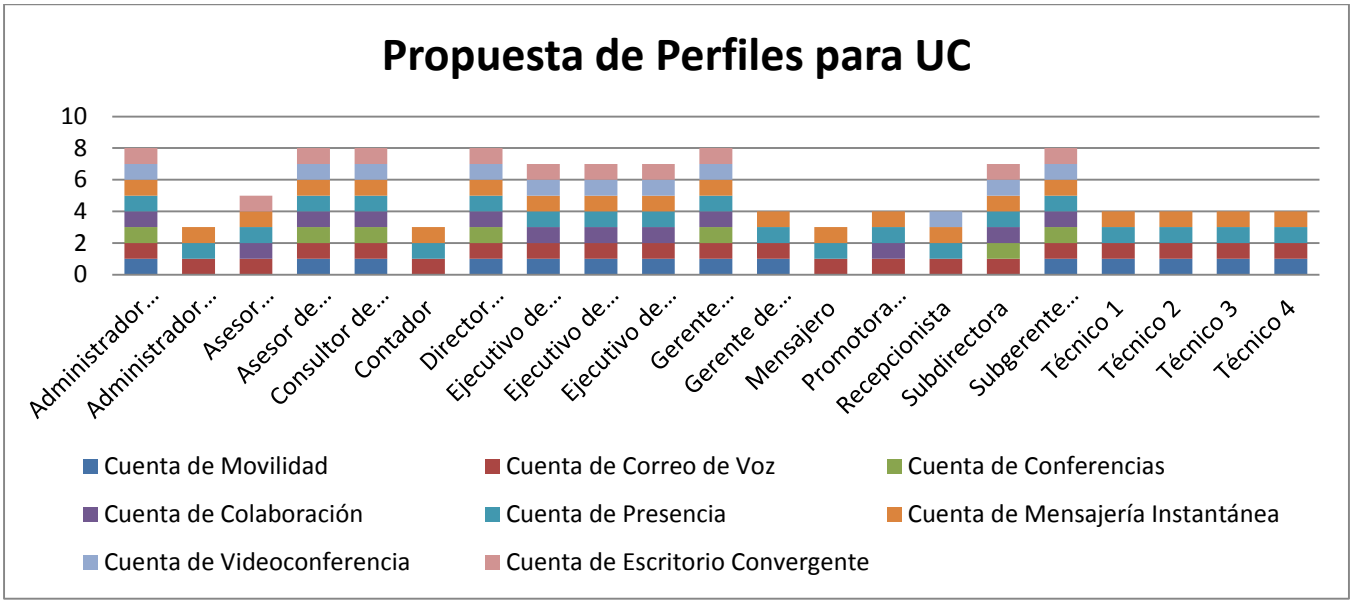

Figura 44 Servicios por perfil.

En esta grafica se muestra el resumen del porcentaje de servicios que se habilitara en cada perfil de los usuarios.

Directivos: Presencia, Mensajería Instantánea, Conferencia de voz y video, Conferencias en línea y con la funcionalidad de compartir contenido y grabar sesiones, Lync Mobile, Telefonía, Información de presencia con integración entre Lync y el calendario de Outlook, Acceso a Outlook desde cualquier dispositivo, Llamadas telefónicas entre usuarios Lync.

Ingenieros de operación: Presencia, Mensajería Instantánea, Conferencia de voz y video, Conferencias en línea y con la funcionalidad de compartir contenido y grabar sesiones, Lync Mobile, Telefonía, Publicación de servicios de Lync hacia internet, Federación, Información de presencia con integración entre Lync y el calendario de Outlook, Acceso a Outlook desde cualquier dispositivo, Reportes de conversación entre usuarios de mensajería instantánea, Llamadas telefónicas entre usuarios Lync.

Vendedores: Presencia, Mensajería Instantánea, Conferencia de voz y video, Conferencias en línea y con la funcionalidad de compartir contenido y grabar sesiones, Lync Mobile, Telefonía, Información de presencia con integración de Lync y el calendario de Outlook, Llamadas telefónicas entre usuarios Lync.

Personal administrativo-secretarial: Presencia y con la funcionalidad de compartir contenido, Mensajería Instantánea, Telefonía, Información de presencia con integración de Lync y el calendario de Outlook, Llamadas telefónicas entre usuarios Lync.

Clientes: Llamar a extensiones Lync desde cualquier teléfono, realizar llamadas hacia el PSTN desde el cliente.

5.2.2.2 Alcances de la solución

"TECPROTEL" obtendrá al término del proyecto los siguientes beneficios inmediatos de la solución propuesta:

- ✓ Definición de estructura de la organización.
- ✓ Definición de la infraestructura de red (diagramas LAN y WAN).
- ✓ Definición y diagrama de la infraestructura telefónica.
- ✓ Descripción del Firewall y las restricciones de red.
- ✓ Instalación de dos servidores de Front-End de Lync Server 2010
- ✓ Integración de Lync Server 2010 con PBX.
- ✓ Configuración del servidor de UM de Exchange Server.
- ✓ Integración de Exchange Server con Lync Server 2010.
- ✓ Instalación de dos servidores de Edge en alta disponibilidad.
- ✓ Instalación del Clúster de SQL Server para los servicios alojados.
- ✓ Ejecución de pruebas en piloto controlado.
- ✓ Verificación y demostración de la operación correcta de los componentes claves contemplados en la implementación.
- ✓ Memoria técnica.
- ✓ Integración con AVAYA IPOffice 500 V2

5.2.3 Requerimientos de la solución

Un servidor físico host con sistema operativo Windows Server Datacenter a 64 bits que alojara Lync y los roles de servidor.

Un servidor físico host con los servicios de DNS, AD, DHCP, Exchange.

Hardware:

- 2 Servidores físicos y 13 servidores virtuales para Lync con las siguientes características.

Resumen		Perfil de uso			
		Número total de usuarios para todos los sitios	50		
Número total de sitios	1	**Nombre del sitio**	**Número de usuarios**	**Características habilitadas**	**Configuración de capacidad**
		TECPROTEL	50	Mensajería instantánea y presencia,IPv4,Conferencia A/V, Conferencia web, Lync Web App, Chat persistente, Supervisión, Archivado, Movilidad, Integración de archivado de Exchange, Grupo de respuesta, Servicio de anuncio, Servicio de estacionamiento de llamadas, Anuncio de conferencia, Servicio de operador de conferencia, Conferencia de acceso telefónico local, Control de admisión de llamadas, Acceso de usuarios externos, Alta disponibilidad para usuarios externos, Telefonía IP empresarial, Mensajería unificada de Exchange, Integración de Office Web Apps Server	100% de usuarios de archivado,40% de usuarios de notificación,50% de usuarios de Lync Web App,20% de usuarios de chat persistente,100% de usuarios de voz,65% de llamadas de omisión de medios,60% de llamadas de UC a RTC,0.05% de usuarios del servicio de estacionamiento de llamadas,0.15% de usuarios del grupo de respuesta,4 llamadas por hora, Línea de red E1,Ningún PBX implementado, Puerta de enlace de 4 puertos,30% de conferencias simultáneas,30% de conferencias de acceso telefónico local simultáneas,75% de conferencias web con voz simultáneas,50% de conferencias de mensajería instantánea en grupo simultáneas,50% de usuarios de mensajería unificada de Exchange,30% de usuarios externos

Tabla 3 Resumen de características y capacidad de la solución

Perfil de servidor		
	Número total de servidores físicos en todos los sitios	13
Nombre del sitio	**Rol de servidor**	**Número de servidores**
TECPROTEL	Servidor Standard Edition	1
TECPROTEL	Proxy inverso	1
TECPROTEL	Servidor perimetral	2
TECPROTEL	Director	2
TECPROTEL	Servidor Office Web Apps	1
TECPROTEL	Servidor de mensajería unificada de Exchange	1
TECPROTEL	Servidor de chat persistente	1
TECPROTEL	Base de datos SQL de chat persistente	1
TECPROTEL	Puerta de enlace	1
TECPROTEL	Dirección IP virtual de equilibrio de carga	2

Tabla 5 Perfil de hardware de la soluci

Requisitos Previos para Instalar Lync
Revisión del Cableado
Análisis de los nodos necesarios y levantamiento de Información
Definición de las aplicaciones a emplear hoy en día y en los próximos años
Planificación del cambio de cableado (Opcional)
Realizar un diseño de la red a instalar considerando (Costos de instalación y satisfacción de las necesidades de comunicación y mantenimiento de la estética de la Empresa)
Retirar el cableado existente en caso de que acepten el cambio
Instalación del nuevo Cableado solo en caso de que sea aprobado hacer el cambio.
Pruebas de comunicación y verificación de la funcionalidad
Optimización del Directorio Activo
Revisión General del Directorio Activo actual
Levantamiento y revisión de la información de la Infraestructura actual proporcionada
Identificación y ubicación de usuarios, computadoras, servidores y grupos
Realización de respaldo del Dominio origen File system y System State de un DC
Identificación de perfiles de funciones de la base de datos
Definición del segmento que va a utilizar el dominio.
Creación de Unidades Organizacionales
Creación de Directivas de grupo
Configuración de Políticas de Dominio
Configuración de Políticas de Grupo
Configuración de equipos al dominio (5)
Pruebas de conectividad al Dominio
Correo electrónico
Detección y Análisis de la situación Actual
Definición del Servidor en donde se llevara a cabo la instalación
Definir Políticas de Antispam y Filtrado de contenido
Determinar las capacidades para cada buzón de voz
Definir capacidad de tamaño máximo en Mb. de envío y recepción
Definir un plan de respaldos
Instalación de Microsoft Exchange 2010
Definición y solicitud de los Puertos utilizados por Directorio Activo, DNS, Exchange Server y el cliente
Creación de cuentas de correo electrónico (5 usuarios)
Creación de las bases de datos para los buzones
Pruebas de Respaldo y Restauración
Creación de usuarios y buzones de todo el personal de Tecprotel
Notificación a todo el personal sobre la actualización del dominio
Configuración de los DNS
Obtener el nombre de dominio aprobado por Internic
Solicitar la dirección IP y el nombre de host del servidor para el que se desea proporcionar resolución de nombres.
Configuración del Servidor DNS en Windows Server
Pruebas de comunicación y resolución de nombres
Pruebas de la incorporación de una estación de trabajo al dominio tecprotel.com.mx
Pruebas de comunicación y Servicios en el dominio tecprotel.com.mx

Identificación de Aplicaciones dependientes del dominio
Revisión del registro de configuración del servidor
Preparación, Instalación y configuración, Servidor Lync Server Edición
Se deberá contar con un Servidor con 32 GB en RAM, quad core, con 2 GHz o superior, 200 Gb de disco duro y con un puerto de red, de preferencia 2.
Instalar las licencia de Windows Server, Lync Server y las CAL´s
Descargar las actualizaciones del Sistema Operativo
Definir las características, funciones y roles que se van a implementar en el Servidor
Instalar el software VMWare para la implementación de máquinas virtuales
Determinar las máquinas virtuales que deben ser instaladas para los servidores
Instalar los certificados de SAN y Wildcard. El certificado SAN para nuestros servidores EDGE y el Wildcard para nuestros Front-END y sus servicios Web.
Instalar las nuevas funciones o roles dentro del servidor
Realizar pruebas de comunicación
Preparación de Equipos de Cómputo para la nueva Implementación
Revisión de Hardware y Software en Equipos de Computo
Actualización de Sistema Operativo para 14 equipos
Instalación de las actualizaciones para 14 equipos
Migración de equipos de cómputo al Dominio tecprotel.com.mx
Pruebas de funcionalidad dentro del dominio de la empresa
Identificación y resolución de problemas documentando cada uno de ellos.
Optimización del Servidor que aloja el AD para la instalación de hardware y lograr su expansión de características
Actualización de equipo Servidor que aloja el directorio activo
Enlaces de Internet para la implementación de Lync 2010
Para la implementación de Lync se recomienda tener un enlace dedicado
El enlace se recomienda que sea como mínimo de 2 MB simétricos
Actualmente se cuenta con 3 ADSL, se sugiere quedarse solo con uno de ellos que sirva para mantener la supervivencia del sistema en caso de falla
Se realizó un estudio de mercado acerca de los diferentes proveedores de Internet
Entre los principales Proveedores se encuentran (Telmex, Axtel, Iusacell, Alestra, Cablevisión, BBS Red de México)
Como parte del estudio se tomaron en cuenta principalmente los costos, la velocidad, y el soporte.
Se hicieron pruebas con algunos proveedores como BBS Red de México
Se determinó que la mejor opción para esta solución será contar con un Enlace Dedicado de 4 MB y un pool de 10 IP´s Fijas
Se sugiere conservar uno de los enlaces ADSL para tener al menos un equipo de respaldo
Configuración del Firewall
Definir los segmentos de red que se van a utilizar en la implementación de Lync
Configuración de los enlaces para la salida a Internet
Ubicar a los usuarios en diferentes Perfiles de acuerdo a lo que se ha definido para el sistema Lync
Liberar los puertos que se van a ocupar en nuestra solución
Definir los usuarios que tendrán acceso remoto hacia la red cuando estén fuera de la oficina
Creación de la VPN para el acceso remoto de los usuarios mediante cliente VPN para laptop o celular
Configurar Políticas para brindarle mayor seguridad a la red y optimizar los recursos para el consumo de ancho de banda

Tabla 5 Requisitos previos para Instalar Lync

5.3 Fase II Desarrollo y Metodología

La metodología de trabajo a seguir será Microsoft Solutions Framework (MSF) es una metodología que nos permite llevar el control y el adecuado seguimiento del proyecto.

MSF provee un conjunto de modelos, principios y reglas a seguir para el diseño y desarrollo de soluciones empresariales de tal manera que se asegure que todos los elementos del proyecto tales como las personas involucradas, procesos y herramientas puedan ser administradas de manera exitosa.

MSF también provee las mejores prácticas probadas para la planeación, diseño, desarrollo y distribución exitosa de soluciones empresariales.

Tabla 6 Metodología Microsoft Solutions Framework (MSF)

A pesar de que nos basaremos en el uso de esta herramienta hacemos hincapié que ha sido ajustada de acuerdo a nuestros objetivos y los requerimientos de la Empresa TECPROTEL. Al usar la metodología desarrollada por Microsoft la implementación de Comunicaciones Unificadas se integra perfectamente a Lync.

Se establecen las adecuaciones que se deben de llevar acabo para que la PROPUESTA DE IMPLEMENTACION DE COMUNICACIONES UNIFICADAS CON INTEGRACIÓN DE TELEFONÍA IP EN LA EMPRESA TECPROTEL cumpla con los requerimientos necesarios y así poder garantizar un buen funcionamiento. Es importante señalar que las siguientes modificaciones están basadas:

1. En el levantamiento que se realizó previamente
2. Los alcances pactados en este proyecto
3. Los requerimientos y necesidades de la empresa,
4. En el modelo operativo del negocio
5. Con ayuda de la herramienta de Microsoft Planning Tools.

Licenciamiento: Para la implementación de la propuesta se requiere que todos los sistemas operativos en los equipos clientes trabajen con versiones profesionales, de preferencia nosotros recomendamos Windows 7 ya que a la versión de XP se le dejara de dar soporte el 14 de Abril de 2014[3]**.** Y en parte también porque para la versión de Windows 8 todavía se tiene desconocimiento de uso por parte de los usuarios.

En relación a los alcances que puede tener el proyecto nos tocó entrevistarnos con el personal Administrativo y con la gente de Sistemas informándonos que se estima un crecimiento en el personal de hasta 30 usuarios en los próximos dos años como consecuencia de que es una empresa integrada principalmente por gente de confianza, o bien porqué en su mayoría está compuesta por familiares. Debido a esto es que sería recomendable adquirir 30 licencias (CAL) en su versión standard de acuerdo a los requerimientos y necesidades de la empresa para las funcionalidades de LYNC 2010.

Como lo hemos visto en la solución propuesta para este proyecto y a un análisis que se hizo de la infraestructura con la que se cuenta observamos que será necesaria la adquisición de la Licencia Lync Server Standard Edition 2010, para poder integrarla junto con uno de los servidores en el cual podremos también virtualizar algunos otros para complementar nuestra solución de una mejor manera.

Cableado: Uno de los principales movimientos que se deberían de realizar ya que en un futuro podría ser una limitante es el cambio de cableado y así tener un mejor rendimiento para ello es prioritario considerar la migración a la categoría 6, ya que como vimos en el levantamiento se trabaja con categoría 5e (CAT 5e) y La razón más básica por la cual sería recomendable un cambio es que la categoría 6 (CAT 6) proporciona significativamente un mejor canal de transmisión que CAT 5e. Además de que la presente propuesta tiene como expectativa tener una red con Gigabit Ethernet ya que dentro de los servicios que se van a utilizar en la empresa esta las videoconferencias. Otro aspecto importante por el cual se ha considerado utilizar este cableado es el hecho que el grosor del cable y las mejoras de torsión con CAT 6 ofrece menos pérdidas de inserción, un mejor rendimiento de diafonía y una mejor señal al radio de ruido que el cable estándar CAT 5e anterior. En lo que respecta a los conectores para los cables CAT 5e y CAT 6 son idénticos. Ambas normas (A y B) utilizan conectores RJ45, lo que significa que la velocidad de la red de los dos cables es completamente intercambiable. Los conectores RJ45 de 8 pines coinciden con el número de cables en ambos estándares. Los conectores RJ45 son muy fáciles y fiables de usar así que además del cable se debe considerar el cambio de conectores.

Es importante aclarar que el cambio del cableado solo se presenta como una propuesta de mejora para el intercambio de información ya sea de datos o de voz, pues con el cableado que se tiene actualmente en categoría 5e se podría implementar la Tecnología de Lync pero si

[3] http://www.microsoft.com/es-es/windows/endofsupport.aspx

debemos recalcar que si existe una gran diferencia entre uno y otro por lo cual dejamos esto a criterio de la Empresa.

Servidores: Debido a que ya se tenía configurado el Active Directory (AD) solo se procedió como principio de cuentas a realizar un respaldo de la configuración actual y realizar algunos ajustes respecto a los usuarios del AD. Debido a que algunas contraseñas no coincidían con los respectivos usuarios. Lo cual dio como resultado que se actualizará la contraseña de cada usuario y después probar cada una de ellas. También se realizó una reestructuración en cuanto al diseño del bosque y dominio para identificar los perfiles y funciones dentro de la base de datos.

DHCP: Se determinó el segmento de Red 192.168.1.0 para la implementación del sistema y se configuro el Servidor agregándole la función de DHCP para que se pueda administrar a los usuarios de una manera más eficiente, para ello se precedió a verificar que el servidor contara con una IP estática para poder activar la funcionalidad de DHCP.

Microsoft Exchange 2010: Para la parte de correo electrónico se configuró Microsoft Exchange Server 2010 ya que es parte importante de la solución de Comunicaciones Unificadas de Microsoft, es una herramienta que ha sido la elección de varias empresas para facilitar una colaboración avanzada y tener mayor productividad entre sus usuarios. La versión de Exchange 2010 se basa en estos precedentes para ofrecer:

- Costes más bajos en TI con una plataforma de mensajería flexible y fiable.
- Una mayor productividad proporcionando acceso desde cualquier lugar a las comunicaciones de la empresa.
- Una mejor gestión del riesgo, al salvaguardar su empresa con capacidades de protección y cumplimiento.

El uso de esta herramienta no solo se limita a la revisión de correos. Adicional a esto es que con la configuración que permite realizar con el conmutador se puede implementar la Unificación del correo electrónico con el buzón de voz y de este modo podríamos garantizar que las llamadas que se tienen si por alguna razón no se encuentra presente la persona que se localiza siempre exista algún medio para contactarlos siempre y cuando quien hace la llamada haga uso del buzón.

Switch: Se integró a la infraestructura un Switch Avaya capa 2 Modelo 2526T-PWR y en este se configuraron tres VLAN de la siguiente manera:

VLAN 2 Red de Datos.

VLAN 3 Red de Voz.

VLAN 4 Red para Servidores.

Firewall: Como se ha mencionado es el dispositivo encargado de la seguridad dentro de una empresa por lo tanto es sumamente importante contar con un equipo que nos proteja de

amenazas o ataques que vengan no solo desde el exterior sino que además nos ayude a protegernos internamente y a la vez nos brinde un mayor control de los equipos en nuestra red y de nuestros usuarios.

Debido a una promoción que le ofrecieron a la empresa TECPROTEL en el presente año es que pudo renovar su dispositivo de seguridad y ahora cuenta con un "WatchGuard XTM modelo 330" con licencias de security bundle incluidas de UTM para la seguridad y de livesecurity para garantía y actualizaciones del equipo todo ello es de gran utilidad. Una vez más reiteramos que con ayuda de este equipo podremos administrar nuestra red de una manera más eficiente, creando diferentes segmentos para otorgar mayor seguridad, quizá será necesario crear una DMZ en donde podamos aislar nuestros servidores para brindar una mayor protección, cabe mencionar que este equipo cuenta con una licencia que nos permite hacer un balanceo de carga y tener alta disponibilidad para la navegación web debido a que se cuenta con dos enlaces de internet y así garantizar el mayor tiempo posible la conexión a internet.

Otro punto importante que nos ayudara el contar con este equipo Firewall. Es el hecho de poder configurar VPN´s para tener acceso remoto ya sea desde un dispositivo móvil o desde una computadora para aprovechar los recursos de la empresa como pueden ser las extensiones móviles.

Enlaces: Actualmente se cuenta con dos enlaces ADSL con un ancho de banda de 4 MB, por lo que su velocidad de subida es diferente a la de bajada. Se recomienda que para la implementación de Lync se cuente con dos enlaces; uno de ellos se sugiere que sea un enlace dedicado simétrico; dado que el Internet de Banda Ancha dedicado-simétrico varia de las conexiones tradicionales DSL o asimétricas, por lo que la velocidad de subida de datos, será la misma que la de bajada en todo momento lo cual es muy importante y por otra parte el tiempo de respuesta que se maneja en estos enlaces en caso de existir alguna falla es de un máximo de 4 horas contra 72 horas en un enlace convencional, ya que es importante mantener el mayor tiempo posible se tenga el acceso a internet.

Como lo hemos mencionado hoy en día existen diferentes proveedores de este servicio, Por lo tanto se tienen diferentes opciones de donde podemos escoger. Por lo tanto podríamos tener un enlace con un proveedor y otro con uno diferente, ya que el Firewall nos lo permite.

Resumiendo sería importante contar con servicio de internet con un enlace dedicado empresarial ya sea de Telmex, Axtel, o BBS Red. Ya que nos ofrecen paquetes a partir de 2 MB y hasta 10 MB simétricos o bien contratar otro proveedor de servicios de Internet (Iusacell, Total Play, Cablevisión etc.) que nos puedan proporcionar IP's públicas que sean fijas pagando una renta mensual por cada una de ellas, esto es muy importante si queremos tener acceso desde internet a la plataforma sin tener que conectarnos mediante VPN. También es cierto que cuantos menos servicios desde el exterior se requiera, menos IP's Públicas nos hacen falta. Si solo se quiere IM con una IP Pública es suficiente.

El otro servicio de internet podría ser alguno de los que se tiene actualmente o ver la posibilidad de contratar uno con mayor ancho de banda para contar con una alternativa en caso de que falle uno debido a que los servicios como la videoconferencia consumen mayor ancho de Banda.

Capacitación de Usuarios: Uno de los aspectos más importantes que se tiene que considerar y que muchas veces no se le pone el interés necesario o bien se omite cuando se pretende implementar una nueva solución es el hecho de no contar con la preparación o la capacitación adecuada del personal es por ello que debemos de poner mucho énfasis en la capacitación del usuario para qué este a su vez se adapte de una manera más óptima, rápida y eficiente a la nueva tecnología y con ello se facilite el proceso de implementación.

Una de las principales razones por las cuales decidimos que la Tecnología de Comunicaciones Unificadas se lleve a cabo con Lync 2010; es porque la suite de Office era algo con lo que ya se contaba, el hecho de ser un producto Multiplataforma y que este respaldado por Microsoft; representa una gran ventaja debido a que la mayoría de los usuarios están familiarizados con los productos de Microsoft como la suite de Office, o algunos otros aspectos con la mensajería Instantánea, el correo de Voz, entre otros, por ello a pesar de que detectamos que dentro del personal que integra a la Empresa Tecprotel carece de una constante preparación, no sería tan complicado el Integrar esta Tecnología ya que se vuelve muy ágil e Intuitiva para el usuario al momento de usarla.

PBX: El conmutador de la empresa también se ha actualizado cambiando el gabinete a su versión de IP Office 500V2 Preferred Edition una de las tres versiones disponibles para este tipo de conmutadores, (las otras dos Essential Edition y Advaced Edition) cuenta con el release 8.1.69; este equipo es una versión Demo que cuenta con varias licencias para realizar pruebas en él; se cuenta con diferentes licencias entre las que destacan: Endpoint IP para teléfono IP, Voicemail Pro License para hacer uso del correo de Voz, Networking License, para interconectar dos conmutadores, y algunas otras para tener usuarios móviles.

Es un equipo diseñado para las pequeñas y medianas empresas el cual es escalable hasta 384 extensiones, (Digitales, IP o Analógicas), cuenta con una Interfaz de enlace troncal: 204 enlaces troncales analógicos, 8 enlaces troncales PRI (240 canales), 16 enlaces troncales BRI (32 canales), 128 enlaces troncales SIP Conferencias de 2 x 64 participantes, conferencias “Meet-Me”Compatible con hasta 1000 empleados en 32 ubicaciones. Además de que cuenta con capacidad de admitir módulos de expansión para ampliar aún más todas estas capacidades.

Parte de las actividades que se han llevado acabo, para la configuración del equipo ha sido la migración de la versión IP Office 406 a esta nueva versión en donde se llevó a cabo primeramente un respaldo del equipo y la base de datos para instalarlo en el nuevo, posteriormente se realizaron las actualizaciones correspondientes, la configuración de las líneas, y nuevamente se dieron de alta las extensiones y los usuarios con el archivo de respaldo, para que finalmente se realizaran pruebas de llamadas Internas y posteriormente llamadas hacia el exterior con el nuevo conmutador.

Movilidad: Para la parte de movilidad la empresa tendrá que adquirir en su renovación de equipos en la compañía Nextel otros dispositivos con lo que puedan tener una mayor oportunidad de aprovechar más las ventajas del plan de datos contratado ya que actualmente solo usan los aparatos para comunicarse por medio del radio, pero carecen de servicios como el internet, mensajería instantánea o bien una cuenta de correo y obviamente realizar llamadas telefónicas, es importante detenernos un momento en esta parte ya que esta es un rubro en el cual le puede ayudar a la empresa a obtener mayores beneficios con la implementación de Lync, debido a que la mayor parte del tiempo el personal se encuentra fuera de la oficina y con ello podemos mejorar la comunicación entre los integrantes de la empresa, y a la vez se reducirán los viajes, o bien se tendrá la capacidad de poder tener mayor colaboración en tiempo real por parte de diferentes áreas así que será importante, contar con ciertos requisitos para tener mayor provecho de esta tecnología.

- Como principio de cuenta los teléfonos deberán ser Smartphone.
- Descargar la App de Lync de Microsoft la cual está disponible en Android, IOS, o bien Windows Phone,
- Una cuenta de correo en Microsoft Exchange 20 10 en este caso.
- Una conexión Wi-Fi o como lo decíamos contar con plan de datos.

5.4 Fase III Implementación

Al haber cumplido con los requisitos previos descritos en la fase de planeación y siguiendo la metodología MSF descrita anteriormente.

La instalación consta de varias etapas que debemos seguir en un orden concreto que se enuncian a continuación en la siguiente tabla.

Implementación de Microsoft Lync Server en TECPROTEL		
ID	**TAREA**	**DURACIÓN (Días)**
1	**I Upgrade AD / Implementación de Mycrosoft Lync Server**	**7**
2	Instalación (física y SO) de servidor	0
3	Preparación del Ambiente (Schema) y revisión de servidores	1
4	Implementación de Microsoft SQL Server Back End	1
5	Implementación de Microsoft Lync Server Front End	1.5
6	Implementación de Microsoft Lync Server Director (2 Servidores	2
7	Configuración de políticas y servicios sobre Lync	1
8	Pruebas de funcionalidad y estabilización - usuarios	0.5
9	**I - A Instalación de Lync para usuarios (10 usuarios)**	**2**
10	Definición de Calendario de migración	0
11	Alta de cuentas de usuarios; deploy de cliente Lync para 10 usuarios	1
12	Recomendaciones para distribuir el cliente Lync	1
13	**II Instalar Archiving Y Monitoring**	2
14	Instalación (Virtual) de servidor	0
15	Instalación y configuración para Archiving	1
16	Configuración de políticas y servicios sobre Lync	0.5
17	Pruebas de funcionalidad	0.5
18	**III Publicar servicios a Internet - Edge**	**5**
19	Instalación y configuración de Lync Edge	1
20	Configuración de Reverse Proxy / Firewall	1
21	Configuración de certificados públicos	1
22	Pruebas de funcionalidad (Edge y Web Ext)	2
23	**IV Integración de servicios de telefonía**	**4**
24	Instalación y configuración de Mediation	1
25	Configuración de Marcación y plan de políticas	1
26	Configuración de Gateway - Localidad Central (E1 con Avaya)	1
27	Pruebas de funcionalidad	1
28	**V Servicio de correo de Voz**	**3**
29	Instalación y configuración de Exchange UM	1
30	Configuración de Dial plan y pruebas de funcionalidad	1.5
31	Asignar Correo de voz a usuarios	0.5
32	**VI Entrega de servicios**	**1**
33	Memoria Técnica	1

Tabla 7 Implementación de Microsoft Lync

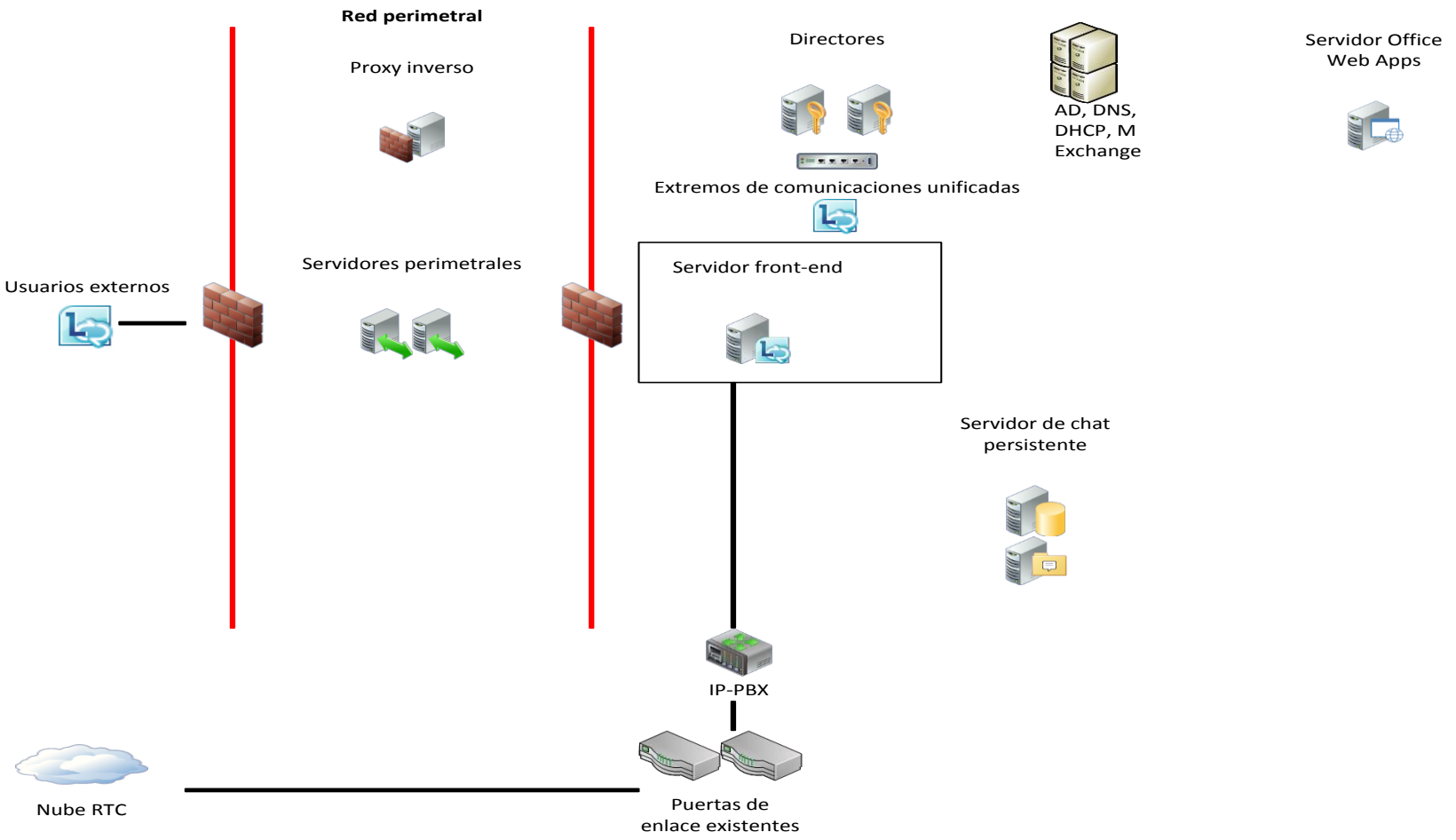

Figura 43 Diagrama de roles y servidores Lync.

Los roles de servidor que se utilizan en la solución para TECPROTEL y que son configurados dentro del Servidor Standard Edition, junto con la infraestructura existente y la integración de la telefonía IP de Avaya.

FRONT-END: Es el rol del servidor principal y ejecuta muchas funciones de Lync Server básicas.
El servidor front-end incluye:

- Registro y autenticación de usuarios
- Información de presencia e intercambio de tarjetas de contacto
- Servicios de libreta de direcciones y ampliación de la lista de distribución
- Funcionalidad de MI, incluidas las conferencias de MI de varios participantes
- Conferencia web, conferencia de acceso telefónico local
- Servicios de hospedaje de aplicaciones para las dos aplicaciones incluidas en Lync
- Recopilar información de uso en forma de registros de detalles de las llamadas (CDR) y registros de errores de las llamadas (CER)
- Componentes web para las tareas basadas en web compatibles
- Archivado, para archivar comunicaciones de MI y contenido de reuniones con fines de cumplimiento
- Servicios web de chat persistente para la administración de salones de chat y para la carga y descarga de archivos.

SERVIDOR PERIMETRAL: El servidor perimetral permite a los usuarios comunicarse y colaborar con usuarios externos a los firewall de la organización.

SERVIDOR DE MEDIACIÓN: El servidor de mediación es necesario para la implementación de Telefonía IP empresarial y la conferencia de acceso telefónico local. El servidor de mediación convierte la señalización y los medios entre la infraestructura interna de Lync Server y la puerta de enlace de una red telefónica conmutada (RTC) pública, un sistema IP-PBX o un enlace troncal de Protocolo de inicio de sesión (SIP).

SERVIDOR DIRECTOR: Los directores pueden autenticar solicitudes de usuario de Lync Server, sin hospedar cuentas de usuario ni proporcionan servicios de presencia o conferencia. Mejoran la seguridad.

SERVIDOR DE CHAT PERSISTENTE: El chat persistente permite a los usuarios participar en conversaciones con varios participantes sobre un tema en particular que persisten a lo largo del tiempo.

PROXY INVERSO: Se configura el proxy inverso HTTPS en la red perimetral para que los clientes externos puedan acceder a los servicios web de Lync Server 2010 en el director y el grupo principal del usuario.

Configuración lógica de la red perimetral que se configura para implementar la solución de Microsoft Lync

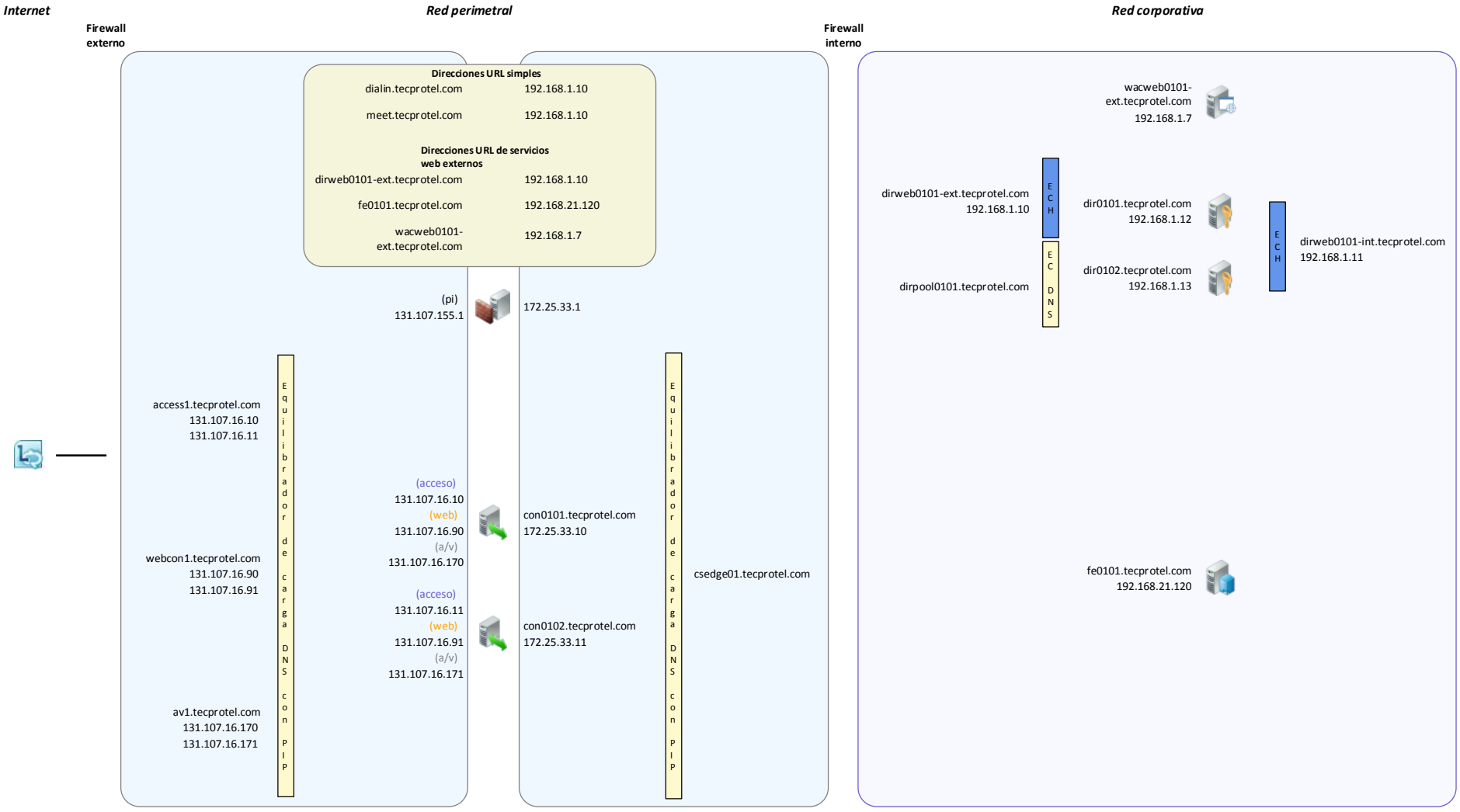

Figura 44 Descripción de la Red Perimetral

Requisitos de puertos			
Rol de servidor	**Puertos habilitados**	**Equilibrio de carga de DNS**	**Equilibrador de carga de hardware**
Servidor Standard Edition	80/TCP para tráfico de los servidores front-end a los FQDN de la granja de servidores web	No	Sí
	135/DCOM/RPC usado para operaciones basadas en DCOM, como mover usuarios, sincronización del replicador de usuarios y sincronización de la libreta de direcciones	Sí	Sí
	443/TCP para tráfico HTTPS de los servidores front-end a los FQDN de la granja de servidores web	No	Sí
	444/TCP para tráfico HTTPS entre el foco y los servidores de conferencia	Sí	No
	445/TCP usado para la replicación desde el servidor de administración central a los servidores de Lync Server	No	No
	448/TCP usado para el servicio de directivas de ancho de banda de Lync Server	Sí	No
	4443/TCP usado para IIS externo para el servidor de libreta de direcciones y uso compartido de diapositivas	No	Sí
	5060/5061/TCP/MTLS para toda la comunicación interna	Sí	No
	5062-5065 para conferencias de mensajería instantánea, conferencias A/V, conferencias de telefonía y uso compartido de aplicaciones	No	No
	5066/TCP - para puerta de enlace E-9-1-1 saliente	No	No
	5067/TCP/TLS usado para las solicitudes SIP entrantes de la puerta de enlace de RTC	Sí	No
	5068/TCP usado para las solicitudes SIP entrantes de la puerta de enlace de RTC	Sí	No
	5069/TCP: para el agente QoE en el servidor front-end	Sí	No
	5070/TCP usado para escuchar el tráfico SIP del servicio de mediación	Sí	No
	5071-5074 para el grupo de respuesta, el operador de conferencia y el anuncio de conferencia	Sí	No
	5075/TCP usado para las solicitudes SIP entrantes del servicio de estacionamiento de llamadas	Sí	No
	5076/TCP usado para las solicitudes SIP entrantes del servicio de prueba de audio	Sí	No
	5080/TCP usado para el servicio de directivas de ancho de banda de Lync Server	Sí	No
	8057/TLS para escuchar conexiones PSOM de Live Meeting	No	No
	8080/TCP usado para IIS externo para el servidor de libreta de direcciones y uso compartido de diapositivas	No	Sí
	8404 para las comunicaciones internas entre servidores (comunicación remota a través de MTLS) para el grupo de respuesta	No	No
	49152-57500/TCP/UDP para las solicitudes multimedia de audioconferencia en todos los servidores internos. Lo usan todos los servidores que terminan audio.	No	No
	49152-65335/TCP: se usa para el intervalo de puertos de uso compartido de aplicaciones	No	No
	57501-65335/TCP/UDP: se usa para el intervalo de puertos multimedia	No	No
	5063/TCP usado para conferencias AV	No	No
	57501-65335/TCP/UDP: se usa para el intervalo de puertos multimedia	No	No
	135 para MSMQ	No	No

Proxy inverso	80/TCP usado para la conexión de ISA a Servicios web internos	No	No
	8080/TCP usado para IIS externo para el servidor de libreta de direcciones y uso compartido de diapositivas	No	No
	443/TCP usado para escuchar en la interfaz externa las solicitudes entrantes de usuarios externos de información de componentes web, descargas de archivos, expansión de distribución e información de la libreta de direcciones.	No	No
	4443/TCP usado por el proxy inverso para la expansión del grupo de distribución	No	No
Servidor perimetral	3478/UDP (interfaces interna y externa) para las comunicaciones STUN/UDP multimedia entrantes y salientes	Sí	No
	443/TCP (interfaz externa) para las comunicaciones SIP/TLS de usuarios externos que tienen acceso a conferencias web internas, y las comunicaciones STUN/TCP multimedia entrantes y salientes para el acceso a sesiones multimedia y de A/V internas	Sí	No
	4443/TCP usado para dirigir datos de configuración del servidor de administración central al servidor perimetral. Este puerto debe estar abierto en cada uno de los servidores perimetrales y no en el equilibrador de carga.	No	No
	5061/TCP (interfaz interna y externa) para la comunicación SIP/MTLS para el acceso de usuarios remotos o federación	Sí	No
	5062/TCP (interfaz interna) para la autenticación SIP/MTLS de comunicaciones de mensajería instantánea salientes a través del firewall interno	Sí	No
	5209/TCP (interfaz interna y externa) para la comunicación XMPP para el acceso de usuarios remotos o federación	Sí	No
	8057/TCP (interfaz interna) para las comunicaciones PSOM/MTLS del servidor que usa el servicio de conferencia web en la interfaz interna de dicho servicio	No	No
	50.000-59.999/RTP/TCP usado para la transferencia multimedia entrante y saliente a través del firewall externo	No	No
Director	5060/5061/TCP/MTLS para toda la comunicación interna	Sí	No
Servidor Office Web Apps	443/TCP para el tráfico HTTPS desde servidores front-end para la detección	No	Sí
	443/TCP para el tráfico HTTPS desde clientes de Lync Server para direcciones URL internas	No	Sí
	443/TCP para el tráfico HTTPS desde el proxy inverso de la red perimetral para direcciones URL externas	No	Sí
	808/TCP para las comunicaciones de servidor internas entre los servidores Office Web Apps (es decir, los servidores front-end y back-end)	No	Sí
	809/TCP para las comunicaciones de servidor internas entre los servidores Office Web Apps (es decir, los servidores front-end y back-end)	No	No
Servidor de chat persistente	HTTP/SSL 443	No	No
	8010-8011 para sincronización de servidores del mismo nivel/puertos WCF para el servidor de búsqueda y el servidor de canal	No	No
	5041 usado para el puerto de escucha de servidor SIP del Servicio de canal	No	No
	SIP/TLS 5061 usado para la comunicación con servidores internos	No	No
	49152-65535: 10 puertos de sesión SIP elegidos de forma dinámica 010-8011 para sincronización de servidores del mismo nivel/puertos WCF para el servidor de búsqueda y el servidor de canal	No	No

Tabla 8 Requisitos de puertos

Informe de resumen-TECPROTEL			
Ubicación	**FQDN / Dirección IP**	**Tipo**	**Comentarios**
Informe del servidor perimetral consolidado			
Servidor			
FQDN de Servidor interno	con0101.tecprotel.com con0102.tecprotel.com	Red perimetral	Servidor de grupo de trabajo en la red perimetral que hospeda los servicios perimetrales de acceso, conferencia web y conferencia A/V.
FQDN de Servidor perimetral de acceso externo	access1.tecprotel.com	Red perimetral	
FQDN de Conferencia web externo	webcon1.tecprotel.com	Red perimetral	
FQDN de Conferencia A/V externo	av1.tecprotel.com	Red perimetral	
NIC			
Nodo del servidor perimetral de acceso interno, conferencia web y conferencia A/V	172.25.33.10 172.25.33.11		Una dirección IP está enlazada a cada nodo interno del servidor perimetral de acceso combinado y conferencia web. Si estos adaptadores de red no están la misma red que el director o el grupo de servidores front-end, configure una ruta persistente estática desde esta red a la red que contiene el director o grupo de servidores en cada nodo del servidor perimetral combinado. Ejemplo: ruta a la red interna 10.0.0.0 desde la red perimetral 192.168.253.0: route add –p 10.0.0.0 mask 255.0.0.0 192.168.253.1.
Interfaz de Servidor perimetral de acceso externa	131.107.16.10 131.107.16.11		Estas direcciones IP se asignan a la interfaz externa en la red perimetral y se colocan detrás del equilibrador de carga. Pueden no estar en DNS, pero se utilizan para NAT. El rol de servidor de Servidor perimetral de acceso se puede colocar detrás de un firewall de enrutamiento de puertos o NAT.
Interfaz de Conferencia web externa	131.107.16.90 131.107.16.91		Estas direcciones IP se asignan a la interfaz externa en la red perimetral y se colocan detrás del equilibrador de carga. Pueden no estar en DNS, pero se utilizan para NAT. El rol de servidor de Conferencia web se puede colocar detrás de un firewall de enrutamiento de puertos o NAT.
Interfaz de Conferencia A/V externa	131.107.16.170 131.107.16.171		Direcciones IP asignadas a la interfaz externa en la red perimetral y detrás de un equilibrador de carga de hardware. El rol de servidor perimetral A/V debe tener una dirección IP direccionable públicamente (si se encuentra detrás de un firewall de enrutamiento de puertos o ejecuta Firewall de Windows, pero no puede estar habilitado para traducción de direcciones de redes). Nota: todos los nodos del servidor perimetral A/V junto con las direcciones VIP del equilibrador de carga de hardware a las que están asociados deben tener direcciones IP direccionables públicamente.

Informe del proxy inverso			
Servidor			
FQDN de Proxy inverso externo	rp0100.tecprotel.com	Red perimetral	Servidor de grupo de trabajo en la red perimetral que hospeda el proxy inverso.
NIC			
Interfaz de Proxy inverso interna	172.25.33.1		Una dirección IP enlazada a la interfaz interna de ISA Server.
Interfaz de Proxy inverso externa	131.107.155.1		Una dirección IP enlazada a la interfaz externa de ISA Server. Nota: el proxy inverso puede estar detrás de un firewall de enrutamiento de puertos o NAT.
Dirección IP pública			
Interfaz de Proxy inverso externa	131.107.155.1		Dirección IP pública externa enlazada a la interfaz externa del proxy inverso.
Informe del servidor del próximo salto			
Servidor			
FQDN de Grupo de servidores interno	dirpool0101.tecprotel.com	Interno	
NIC			
Interfaz de Grupo de servidores interna	192.168.1.12 192.168.1.13	Interno	Adaptador de red del próximo salto de Lync.
Dirección IP virtual			
Direcciones VIP - IP de grupo internas	192.168.1.11	Interno	

Tabla 9 Informe Configuración de servidores.

Informe de certificados-TECPROTEL				
Nombre de sujeto	**Entradas/orden de nombre alternativo de sujeto**	**CA**	**EKU**	**Asignar a:**
Servidor perimetral consolidado ampliado				
access1.tecprotel.com	webcon1.tecprotel.com sip.tecprotel.com	Pública	Servidor/cliente (solo EKU de cliente para la federación AOL)	Asignar a los siguientes roles de servidor perimetral en cada servidor del grupo de servidores perimetrales: Interfaz externa: Servidor perimetral de acceso; Servicio perimetral de conferencia web; Interfaz interna: Servicio de autenticación de medios (usando Asistente para certificados de Lync Server para una única asignación de certificado);
csedge01.tecprotel.com	N/D	Interno	Servidor	Asignar al siguiente rol de servidor perimetral: Interfaz interna: Servidor perimetral (usando Asistente para certificados de Lync Server para una única asignación de certificado);
Proxy inverso				
rp0100.tecprotel.com	dialin.tecprotel.com meet.tecprotel.com dirweb0101-ext.tecprotel.com wacweb0101-ext.tecprotel.com	Pública	Servidor	Reglas de publicación del servicio de libreta de direcciones, DGX e IP. El nombre alternativo del sujeto contiene todas las URL simples.
Grupo/director del próximo salto				
dirpool0101.tecprotel.com	sip.tecprotel.com admin.tecprotel.com dialin.tecprotel.com meet.tecprotel.com dirweb0101-int.tecprotel.com dirpool0101.tecprotel.com dir0101.tecprotel.com dir0102.tecprotel.com	Interno	Servidor	Asignar a los siguientes servidores y roles del grupo de servidores del próximo salto: Director 01 en Director1; Director 02 en Director1; Etc...; (usando Asistente para certificados de Lync Server para una única asignación de certificado)

Tabla 10 Informe de Configuración de Certificados

Informe de firewall-TECPROTEL							
Rol del servidor perimetral	**Dirección IP de origen**	**Puerto de origen**	**Dirección IP de destino**	**Puerto de destino**	**Transporte**	**Aplicación**	**Comentarios**
Configuración de los puertos del firewall externo							
Interfaz externa (NODO 1)							
Acceso	131.107.16.10	Cualquiera	Cualquiera	80	TCP	HTTP	
Acceso	131.107.16.10	Cualquiera	Cualquiera	53	UDP	DNS	
Acceso	Cualquiera	Cualquiera	131.107.16.10	443	TCP	SIP (TLS)	Tráfico SIP del cliente al servidor para el acceso de usuarios externos
Acceso	Cualquiera	Cualquiera	131.107.16.10	5061	TCP	SIP (MTLS)	Para la conectividad de mensajería instantánea federada y pública mediante SIP
Acceso	131.107.16.10	Cualquiera	Cualquiera	5061	TCP	SIP (MTLS)	Para la conectividad de mensajería instantánea federada y pública mediante SIP
Acceso	131.107.16.10	Cualquiera	Cualquiera	5269	TCP	XMPP	
Conferencia web	Cualquiera	Cualquiera	131.107.16.90	443	TCP	PSOM (TLS)	
Audio y vídeo	131.107.16.170	50000 - 59999	Cualquiera	Cualquiera	TCP	RTP	Solo es necesario para compartir el escritorio y para la federación con los socios que ejecutan Office Communications Server 2007 u Office Communications Server 2007 R2. Se requiere también para compartir aplicaciones y para la transferencia de archivos con usuarios federados de Lync que utilizan sesiones de A/V con Skype.
Audio y vídeo	131.107.16.170	50000 - 59999	Cualquiera	Cualquiera	UDP	RTP	Solo es necesario para la federación con los socios que aún ejecutan Office Communications Server 2007.
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.170	50000 - 59999	TCP	RTP	Solo es necesario para la federación con los socios que aún ejecutan Office Communications Server 2007.
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.170	50000 - 59999	UDP	RTP	Solo es necesario para la federación con los socios que aún ejecutan Office Communications Server 2007.
Audio y vídeo	131.107.16.170	Cualquiera	Cualquiera	3478	UDP	STUN/MSTURN	El tráfico saliente 3478 se utiliza para determinar la versión del servidor perimetral Lync con el que se establece la comunicación y también para el tráfico multimedia de un servidor perimetral a otro. Se requiere para la federación con Office Communications Server 2007 R2 y también si se implementan varios grupos de servidores perimetrales en una compañía.
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.170	3478	UDP	STUN/MSTURN	
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.170	443	TCP	STUN/MSTURN	

Interfaz externa (NODO 2)							
Acceso	131.107.16.11	Cualquiera	Cualquiera	80	TCP	HTTP	
Acceso	131.107.16.11	Cualquiera	Cualquiera	53	UDP	DNS	
Acceso	Cualquiera	Cualquiera	131.107.16.11	443	TCP	SIP (TLS)	Tráfico SIP del cliente al servidor para el acceso de usuarios externos
Acceso	Cualquiera	Cualquiera	131.107.16.11	5061	TCP	SIP (MTLS)	Para la conectividad de mensajería instantánea federada y pública mediante SIP
Acceso	131.107.16.11	Cualquiera	Cualquiera	5061	TCP	SIP (MTLS)	Para la conectividad de mensajería instantánea federada y pública mediante SIP
Acceso	131.107.16.11	Cualquiera	Cualquiera	5269	TCP	XMPP	
Conferencia web	Cualquiera	Cualquiera	131.107.16.91	443	TCP	PSOM (TLS)	
Audio y vídeo	131.107.16.171	50000 - 59999	Cualquiera	Cualquiera	TCP	RTP	Solo es necesario para compartir el escritorio y para la federación con los socios que ejecutan Office Communications Server 2007 u Office Communications Server 2007 R2. Se requiere también para compartir aplicaciones y para la transferencia de archivos con usuarios federados de Lync que utilizan sesiones de A/V con Skype.
Audio y vídeo	131.107.16.171	50000 - 59999	Cualquiera	Cualquiera	UDP	RTP	Solo es necesario para la federación con los socios que aún ejecutan Office Communications Server 2007.
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.171	50000 - 59999	TCP	RTP	Solo es necesario para la federación con los socios que aún ejecutan Office Communications Server 2007.
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.171	50000 - 59999	UDP	RTP	Solo es necesario para la federación con los socios que aún ejecutan Office Communications Server 2007.
Audio y vídeo	131.107.16.171	Cualquiera	Cualquiera	3478	UDP	STUN/MSTURN	El tráfico saliente 3478 se utiliza para determinar la versión del servidor perimetral Lync con el que se establece la comunicación y también para el tráfico multimedia de un servidor perimetral a otro. Se requiere para la federación con Office Communications Server 2007 R2 y también si se implementan varios grupos de servidores perimetrales en una compañía.
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.171	3478	UDP	STUN/MSTURN	
Audio y vídeo	Cualquiera	Cualquiera	131.107.16.171	443	TCP	STUN/MSTURN	
Proxy inverso							
N/D	Cualquiera	Cualquiera	131.107.155.1	80	TCP	HTTP	Opcional: se puede usar para redirigir el tráfico HTTP a HTTPS.
N/D	Cualquiera	Cualquiera	131.107.155.1	443	TCP	HTTPS	

Tabla 11 Informe de Configuración firewall.

Configuración de los puertos del firewall interno							
Interfaz interna (NODO 1)							
Acceso	172.25.33.10	Cualquiera	192.168.1.12 192.168.1.13	5061	TCP	SIP (MTLS)	El destino será el servidor o servidores del próximo salto. En el caso de una arquitectura de referencia, serán las direcciones IP de los dos servidores front-end del grupo.
Acceso	192.168.1.12 192.168.1.13	Cualquiera	172.25.33.10	5061	TCP	SIP (MTLS)	El origen será el servidor o servidores del próximo salto. En el caso de una arquitectura de referencia, serán las direcciones IP de los dos servidores front-end del grupo.
Acceso	192.168.21.120	Cualquiera	172.25.33.10	4443	TCP	HTTPS	Lo utiliza el agente de replicación para la replicación de bases de datos de almacenamiento de administración central e incluye todos los servidores front-end.
Conferencia web	Cualquiera	Cualquiera	172.25.33.10	8057	TCP	PSOM (MTLS)	
Audio y vídeo	192.168.21.120	Cualquiera	172.25.33.10	5062	TCP	SIP (MTLS)	Incluir todos los servidores front-end que usan este servicio de autenticación A/V en concreto.
Audio y vídeo	Cualquiera	Cualquiera	172.25.33.10	3478	UDP	STUN/MSTURN	
Audio y vídeo	Cualquiera	Cualquiera	172.25.33.10	443	TCP	STUN/MSTURN	
Interfaz interna (NODO 2)							
Acceso	172.25.33.11	Cualquiera	192.168.1.12 192.168.1.13	5061	TCP	SIP (MTLS)	El destino será el servidor o servidores del próximo salto. En el caso de una arquitectura de referencia, serán las direcciones IP de los dos servidores front-end del grupo.
Acceso	192.168.1.12 192.168.1.13	Cualquiera	172.25.33.11	5061	TCP	SIP (MTLS)	El origen será el servidor o servidores del próximo salto. En el caso de una arquitectura de referencia, serán las direcciones IP de los dos servidores front-end del grupo.
Acceso	192.168.21.120	Cualquiera	172.25.33.11	4443	TCP	HTTPS	Lo utiliza el agente de replicación para la replicación de bases de datos de almacenamiento de administración central e incluye todos los servidores front-end.
Conferencia web	Cualquiera	Cualquiera	172.25.33.11	8057	TCP	PSOM (MTLS)	
Audio y vídeo	192.168.21.120	Cualquiera	172.25.33.11	5062	TCP	SIP (MTLS)	Incluir todos los servidores front-end que usan este servicio de autenticación A/V en concreto.
Audio y vídeo	Cualquiera	Cualquiera	172.25.33.11	3478	UDP	STUN/MSTURN	
Audio y vídeo	Cualquiera	Cualquiera	172.25.33.11	443	TCP	STUN/MSTURN	
Proxy inverso							
N/D	172.25.33.1	Cualquiera	192.168.1.7	443	TCP	HTTPS	Regla de enrutamiento de Office Web Apps para acceso externo

Tabla 12 Informe configuración de puertos de firewall

Informe de DNS-TECPROTEL				
Ubicación	**Tipo**	**FQDN**	**Dirección IP**	**Asignar a / Comentarios**
Servidor perimetral consolidado ampliado				
DNS externo	A	access1.tecprotel.com	131.107.16.10/24	Interfaz externa del servidor perimetral de acceso (NODO 1)
	A	access1.tecprotel.com	131.107.16.11/24	Interfaz externa del servidor perimetral de acceso (NODO 2)
	A	webcon1.tecprotel.com	131.107.16.90/24	Interfaz externa del servidor perimetral de conferencia web (NODO 1)
	A	webcon1.tecprotel.com	131.107.16.91/24	Interfaz externa del servidor perimetral de conferencia web (NODO 2)
	A	av1.tecprotel.com	131.107.16.170/24	Interfaz externa del servidor perimetral A/V (NODO 1)
	A	av1.tecprotel.com	131.107.16.171/24	Interfaz externa del servidor perimetral A/V (NODO 2)
	SRV	_sip._tls.tecprotel.com	access1.tecprotel.com	Interfaz externa del servidor perimetral de acceso (access1.tecprotel.com) Necesaria para que la configuración automática de Lync funcione externamente
DNS interno	A	csedge01.tecprotel.com	172.25.33.10/24	Interfaz interna del servidor perimetral consolidado (Equilibrador de carga de DNS)
	A	csedge01.tecprotel.com	172.25.33.11/24	Interfaz interna del servidor perimetral consolidado (Equilibrador de carga de DNS)
	A	con0101.tecprotel.com	172.25.33.10/24	Interfaz interna del servidor perimetral consolidado (NODO 1)
	A	con0102.tecprotel.com	172.25.33.11/24	Interfaz interna del servidor perimetral consolidado (NODO 2)
Proxy inverso				
DNS externo	A	dialin.tecprotel.com	131.107.155.1/24	La URL simple de acceso telefónico redirige a una página con números de acceso telefónicos (usados de forma interna y externa)
	A	meet.tecprotel.com	131.107.155.1/24	La URL simple de reunión es la URL de unión a la reunión (usada interna y externamente)
	A	dirweb0101-ext.tecprotel.com	131.107.155.1/24	La interfaz web externa del grupo de directores realiza ABS y DLX
	A	wacweb0101-ext.tecprotel.com	131.107.155.1/24	Interfaz externa del servidor Office Web Apps que usan los clientes externos de Lync Server para visualizar archivos de PowerPoint
Grupo/director del próximo salto				
DNS interno	A	dirpool0101.tecprotel.com	192.168.1.12/24	dirpool0101 (Equilibrador de carga de DNS)
	A	dirpool0101.tecprotel.com	192.168.1.13/24	dirpool0101 (Equilibrador de carga de DNS)
	A	dirweb0101-ext.tecprotel.com	192.168.1.10/24	dirpool0101 (VIP)
	A	dir0101.tecprotel.com	192.168.1.12/24	dirpool0101 servidor de director (NODO 1)
	A	dir0102.tecprotel.com	192.168.1.13/24	dirpool0101 servidor de director (NODO 2)
	A	sip.tecprotel.com	192.168.1.10/24	Necesario para que la configuración automática de Lync funcione internamente
	A	dialin.tecprotel.com	192.168.1.10/24	Conferencia de acceso telefónico local publicada internamente
	A	meet.tecprotel.com	192.168.1.10/24	Reuniones en línea publicadas internamente
	A	admin.tecprotel.com	192.168.1.10/24	UI de administración publicada internamente
	SRV	_sipinternaltls._tcp.tecprotel.com	dirpool0101.tecprotel.com	Necesario para que la configuración automática de Lync funcione internamente
	SRV	_ntp._udp.tecprotel.com	timeServerFQDN	Origen NTP necesario para los dispositivos de Lync Phone Edition
	A	wacweb0101-ext.tecprotel.com	192.168.1.7	Servidor o granja de servidores de Office Web Apps

Tabla 13 Informe de Configuración de DNS.

5.5 Fase IV Pruebas y verificación

En esta etapa se pretende mostrar algunas de las pruebas que se realizaron previamente en diferentes sectores antes de pasar todo a un ambiente de producción

Pruebas de funcionalidad de M Lync e integración de Telefonía IP
Pruebas de Conectividad
Comprobación de conexión física de todos los dispositivos
Conexión de Firewall Watchward a ISP de proveedor
Comunicación entre servidores, switch y firewall
Comunicación entre IPOffice Avaya con Servidor M Lync
Pruebas de rendimiento y velocidad de la red
Pruebas de servidores, roles y servicios
Prueba de M Exchange, DNS, AD
Prueba de respuesta de dominio interna y de respuesta a Internet
Prueba de usuarios aleatorios dados de alta en el Directorio Activo
Envío y recepción de correo de prueba interno y con otro proveedor de correo electrónico
Prueba de roles de servidor M Lync
Conexión de IP's Publicas en Internet
Acceso a Office Web App
Entorno de aplicación en el cliente de Lync
Conversación de mensajería entre dos y más clientes
Cambio de presencia en clientes
Inicio y recepción de llamadas local y externa a la RTP
Comprobación de desvío de llamada y almacenamiento de correo de voz
Iniciar y recibir video llamada interna y externa con cliente externo
Calidad de video en sesiones grupales
Compartición de escritorio, programas, presentaciones
Envío y recepción archivos
Programación de reuniones de chat, audio y video
Utilidades de conferencia y reuniones
Programación de calendario
Pruebas de apps de dispositivos móviles, Android, Ipad y Iphone
Comprobación de almacenamiento
De archivado de mensajería
De almacenamiento de detalles de llamada
De audio y videoconferencias
Almacenamiento de archivos y documentos
De logs de información de errores y datos relevantes
Pruebas de estrés
Carga de red de audio y video
Usuarios conectados al servidor internos y externos concurrentemente

Tabla 14 Pruebas de funcionalidad de Microsoft Lync

5.6 Fase V Transferencia de conocimientos y operación

La transferencia de conocimientos se realiza en base a los perfiles creados anteriormente establecidos.

Se hace conforme a la llamada “marcha blanca” en periodo de prueba con los servicios de Lync en funcionamiento y con la telefonía IP totalmente integrada y de posibles errores o dudas comunes acerca de la operación de parte de algunos de los usuarios.

La operación se quedará a cargo de las personas responsables del área de sistemas de la empresa a la cual:

1. Se le hace entrega de la memoria técnica
2. Capacitación básica de funcionamiento y el soporte de post-instalación a administradores, técnicos de las consolas y equipos de administración
3. Capacitación a los usuarios e integración de personal no técnico al uso de las capacidades y usos de las herramientas de Microsoft Lync

Se hace un análisis del funcionamiento de usuarios técnicos y administradores y de usuarios no técnicos, se monitorea el desempeño del sistema y si fuera el caso se da alguna recomendación y se da por terminado la última fase del proyecto.

6 Conclusiones

El propósito de esta tesis fue presentar una propuesta de implementación en la empresa TECPROTEL S.A de C.V., a partir de las necesidades de la empresa por ofrecer a los clientes del negocio con la experiencia propia la de establecer un marco de trabajo para la integración de telefonía IP en este caso de la marca AVAYA (que en cualquier escenario se pudiera presentar otra infraestructura establecida) con la solución de Comunicaciones Unificadas ofrecida por Microsoft Lync. Esta tesis surgió de la problemática que representaba el poder ofrecer este modelo de Tecnologías de la Información a los clientes del negocio en base estándares actuales y la tendencia de converger las distintas tecnologías existentes.

Para lograr el propósito de la tesis se desarrolló un trabajo de investigación sobre las distintas soluciones de Comunicaciones Unificadas en el mercado, a partir del análisis de los diferentes rubros en que se encuentra inmersa la empresa TECPROTEL S.A de C.V. y funcionamiento. Así mismo se estudiaron las directrices generales a que se sujetan las TI que participan de este proceso, y particularmente de la infraestructura de red y de Telefonía IP. Por otro lado se determinó mediante un análisis tecnológico, organizacional y financiero, como implementar Microsoft Lync en la empresa TECPROTEL S.A de C.V.

Finalmente se desarrollaron los aspectos fundamentales sobre el proceso de integración de las diferentes tecnologías y las ventajas que presenta la solución para contribuir al crecimiento del negocio y enfrentar los retos de convergencia de las nuevas tecnologías que se presenten en la empresa.

Se debe reconocer que requiere conocimientos en algunos casos especializado en la implementación, es importante rodearse de las personas capaces para poder visualizar la solución de manera integral, sin duda son diferentes temas y áreas en las que se debe trabajar con sumo cuidado sin dejar de perder de vista lo obvio.

Se encuentran numerosas ventajas en la Unificación de las comunicaciones hoy en día, es indispensable tener conocimiento básico de todo lo que involucra el hacer converger los medios y servicios otorgados hacia los clientes que finalmente son los que le darán uso diariamente.

De lo ya expuesto en que beneficia a las empresas las CU cabe destacar:

- La integración de las diferentes tecnologías en el día a día, poder utilizar varias maneras de poder contactarnos y así poder romper la barrera de la incomunicación y tener información a todo momento con personal, proveedores y clientes en cualquier lugar y en todo momento.
- Sin duda hay una inversión importante a la implementación de la solución sin embargo los ahorros son tangiblemente sustanciales al poco tiempo de la puesta en marcha.

- La fácil administración y mantenimiento que ofrece Microsoft Lync para monitorizar las aplicaciones y eventual falla la rápida localización del evento y sin duda una rápida solución.
- El uso de distintos dispositivos que van desde PC de escritorio, laptops, hasta Smartphones que permiten la interacción sencilla desde cualquier lugar en cualquier momento.
- La familiarización del usuario con los servicios de Microsoft como la paquetería Office el mensajero instantáneo y el mismo sistema operativo que hace que sea amigable y fácil de uso.

Es una apuesta que requiere una visión tecnológica y que engloba a todo el personal de la empresa, que sin duda debe operar en mutuo beneficio entre negocio y de manera humana.

El avance tecnológico hace que muchos nuevos desarrollos tengan tiempos de vida cortos pero el uso de las comunicaciones unificadas va en amplitud para la realización de esta tesis no se contempla el uso de los servicios en la nube pero que sin duda acarrea un beneficio mayor para implementación y en algunos casos de costes. Es importante señalar que se pueden implementar híbridos (algunos servicios en sitio y otros en la nube).

En las diferentes marcas que hay en el mercado y que plantean diferentes soluciones para las Comunicaciones Unificadas encontramos diferencias grandes ya que los desarrollos tienen diferentes vertientes, posiblemente las soluciones que no van orientadas a software como lo es Lync tengan un mejor desempeño con el hardware implementado el cual implica una mayor inversión por dispositivos necesarios.

El encontrarse con un escenario en el que la infraestructura posiblemente no sea la idónea constituye un reto para la implementación el hacer converger las comunicaciones requiere un estudio a fondo de la situación actual de la empresa y su problemática, encontrar una solución para integrar lo existente con lo nuevo requiere de la habilidad e ingenio, para poder optimizar la utilización de la infraestructura de telefonía IP de Avaya que es la que por cuestiones de negocio se utiliza y Microsoft Lync que después de una evaluación y facilidad de conocimiento es como mejor planteamos la solución.

Los proyectos se mejoran día a día con nuevas ideas, aportes y el avance de la misma tecnología, este proyecto como nació se volvió en un proyecto de mejora constante y se estableció una base para trabajar pero si hay importantes mejoras que se pueden realizar.

Mantener los servicios siempre disponibles es una prioridad de la seguridad informática.

Por el objetivo y los alcances se decidió por la propuesta que ofrecía confiabilidad y soporte por Microsoft Lync 2010, en el momento de desarrollar las conclusiones se ha mostrado una sustancial mejoría para implementar Microsoft Lync 2013, el soporte sin duda ha crecido, el

número de modelos compatibles con teléfonos IP, con PBX que se adaptan mejor y que requieren menor configuración.

La propuesta fue planteada con la versión Standard de Lync y sin duda la seguridad ofrecida por la versión Enterprise, que dentro de las ventajas ofrece alta disponibilidad y prevención de desastres, además de incrementar el número de usuarios que pueden interactuar con los servicios incentiva a decantarse por esta versión.

Dentro del mismo diseño se propone un solo servidor que cumpla los roles lo que es suficiente para ofrecer los servicios, como buena práctica lo recomendable es implementar un segundo servidor que se tendría como espejo por si esta fuera de línea por los mantenimientos o ante una eventual contingencia.

Es posible implementar los servicios en distintos servidores esto ayuda en que en el momento de que un servicio no esté disponible los demás no se vean afectados y si es posible reparar el error lo ante posible o como se mencionó otro servidor de respaldo así se ofrecería la alta disponibilidad, en todo momento.

Respecto a los servicios que desean implementar dentro de la Empresa se destaca que es el de Archiving el que más se piensa usar por lo cual en lo que se refiere al almacenamiento de las conversaciones y los registros de las conferencias se recomienda tener como alternativa un disco de almacenamiento externo o en su defecto ir eliminando periódicamente aquellas que ya no se consideren útiles.

La empresa TECPROTEL S.A. de C.V. no cuenta con planta de emergencia ante interrupciones o falta de energía eléctrica, por lo cual se hizo la observación que se debe tomar como medida de seguridad para ofrecer una verdadera alta disponibilidad en cuanto al diseño de la solución.

Todo esto sin duda es una inversión que debe de considerarse como alta prioridad, la seguridad de la información, los servicios disponibles, íntegros, confiables y la satisfacción de los clientes son bienes intangibles que repercuten en el éxito de las organizaciones y uno de los principales objetivos de la Computación hoy en día.

Índice de Figuras

Índice de Tablas

Bibliografía

1. -Budris Paula, (2007), Administrador de Redes Manuales users.
2. -Interconnecting Cisco Networking Devices Part 1 y 2 Cisco System 2013.
3. Carballar Jose Antonio, (2007) VOIP la Telefonía de Internet, Paranifo, Madrid España.
4. Comer, Douglas E., (2000) Interconectividad de Redes con TCP/IPDiseño e Implementación Vol II 3a. edición México Prentice Hall.
5. - Craig Zacker and John Rourke (2001), PC Hardware Manual de Referencia Osborne McGraw-Hill.
6. Forouzan, Behrouz A. (2002) Transmisión de Datos y Redes de Comunicaciones 2a. edición España McGraw-Hill.
7. - GarcíaTomás Jesús, Raya Cabrera José Luis (2002), Alta Velocidad y Calidad de servicio en Redes IP Alfa omega Ra-Ma.
8. -Himanshu Dwivedi, (2009) "Hacking VoIP" Protocols, Attacks, and Countermeasures.
9. Huidobro José Manuel, (2006), Tecnología VOIP y Tecnología IP: La telefonía por Internet Creaciones Copyright.
10. -Hunt, Craig (2002)TCP/IP Network Administration, 3th edition [s.l.i.] USA O'Reilly & Associates Inc.,
11. -King, Todd, (2002)Security + Training Guide USA, Que.
12. -Geier, Jim (2002), Wireless LAN´s Second Edition, Sams Publishing, Indianapolis, Indiana, USA.
13. -Pahlavan, Kaveh, Krishnamurthy, Prashant, IEEE 802.11 WLANs, Principles of Wireless, Networks: A Unified Approach, New Jersey, Prentice Hall.
14. Patil, Basavaraj, Saifullah, Yousuf, Faccin, Stefano, Monomen Risto (2002)IP in Wireless Networks, USA, Prentice Hall.
15. - Peter H. Gregory (2012)Comunicaciones Unificadas for Dummies Edicion Especial de Avaya.
16. - Strassberg E. Keith, Gondek R., Rollie G., (2013), Firewalls Manual de Referencia, Mc Graw Hill.
17. -Tanenbaum, Andrew S., (2003) Redes de Computadoras 4a. edición México Pearson Educación.
18. - Wesley Pub Co Inc. (2014), The Tao of Network Security Monitoring Richard Bejtlich Beyond Intrusion Detection Addison; Edición: New. (1 de julio de 2004)
19. -AVAYA (Septiembre 2013- Febrero2014) http://www.ipofficeinfo.com/
20. -AVAYA 2013http://www.ipofficeinfo.com/docs/ip_office_product_description_en_R5%20020610.pdf
21. -Cervera Carlos, Seguridad en redes inalámbricas, (2005), http://www.uv.es/~montanan/redes/trabajos/SeguridadWLANs.pdf
22. -Guía Lync 2013, (Enero-Diciembre 2013), http://blog.asirsl.com/Paginas/guialync.aspx
23. -Joancomartí, Aspectos avanzados de seguridad en redes (2004), http://www.uv.es/~montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf
24. Lehembre Guillaume (2006) Seguridad Wifi – WEP, WPA y WPA2 http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
25. Manual de seguridad en redes, (1998), http://www.redes-linux.com/manuales/seguridad/manual_de_seguridad.pdf
26. -Primera Guía de Instalación de Lync Server 2013 en Español, (Diciembre 2013), http://blog.asirsl.com/Lists/EntradasDeBlog/Post.aspx?List=9cdf87d5-c7fe-4376-998f-c7b0e3ae1a52&ID=464&Web=2947a181-12bd-4c3f-b12a-19ac0ce9566b
27. -Seguridad en VOIP: Ataques, amenazas y riesgos (2013) http://www.uv.es/~montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf
28. -Serviciod de voz sobre IP Macgraw-hill (2013) http://www.mcgrawhill.es/bcv/guide/capitulo/8448171330.pdf

29. -Technet Microsoft (2013), Microsoft Lync Server 2010, http://technet.microsoft.com/es-es/library/gg398616(v=ocs.14).aspx
30. -Technet Microsoft (2014), Implementar Lync Server 2013, http://technet.microsoft.com/es-mx/library/gg412892.aspx
31.- Revista Seguridad UNAM http://revista.seguridad.unam.mx/

Glosario

FDDI (siglas en inglés que se traducen como interfaz de datos distribuida por fibra) es una tecnología de acceso a redes a través líneas de fibra óptica. De hecho, son dos anillos: el anillo "primario" y el anillo "secundario", que permite capturar los errores del primero

ATM El modo de transferencia asíncrona o ATM (Asyncronous Transfer Mode) es un estándar adoptado por la ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) en 1985 para soportar la red digital de servicios integrados de banda ancha.

WDM La multiplexación por división de longitud de onda (WDM, del inglés Wavelength Division Multiplexing) es una tecnología que multiplexa varias señales sobre una sola fibra óptica mediante portadoras ópticas de diferente longitud de onda, usando luz procedente de un láser o un LED

ISDN Se define la RDSI (Red Digital de Servicios Integrados, en ingles ISDN) como una evolución de las Redes actuales, que presta conexiones extremo a extremo a nivel digital y capaz de ofertar diferentes servicios.

Frame Relay Es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones

TCP Es un protocolo orientado a conexión. Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de datos, y confirma su buena recepción

UDP Es un protocolo no orientado a conexión. Es decir cuando una maquina A envía paquetes a una maquina B, el flujo es unidireccional**.** El destinatario recibirá los datos sin enviar una confirmación al emisor

TELNET Se refiere a la conexión remota a un ordenador, esto es posible en Internet gracias al TELNET Protocol. Es habitual usar la expresión "hacer un TELNET", con ello estamos expresando que vamos a realizar una conexión en modo terminal remoto con una máquina en la que estamos autorizados.

FTP. Es el servicio de transferencia de ficheros a través de Internet, conectándonos con servidores dentro de la red que nos facilitan dichos archivos.

SMTP Simple Mail Transfer Protocol (SMTP), o protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos.

ADSL Abreviación de Asymmetric Digital Subscriber Line, el ADSL es un método de transmisión de datos a través de las líneas telefónicas de cobre tradicionales a velocidad alta. Los datos pueden ser descargados a velocidades de hasta 1.544 Megabits por segundo y cargados a velocidades de hasta

128 Kilobits por segundo. Esa es la razón por la cual se le denomina asimétrico. Esta tecnología es adecuada para el web, ya que es mucho mayor la cantidad de datos que se envían del servidor a un ordenador personal que lo contrario.

Ancho de banda
El ancho de banda es la máxima cantidad de datos que pueden pasar por un camino de comunicación en un momento dado, normalmente medido en segundos. Cuanto mayor sea el ancho de banda, más datos podrán circular por ella al segundo.

Backbone Un backbone es enlace de gran caudal o una serie de nudos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red. Por ejemplo, NSFNET fue el backbone, la columna o el eje principal de Internet durante muchos años.

Bps Es una abreviación de bits per second, bits por segundo, una medida de la velocidad a la cual son transmitidos los datos. Bps se utiliza normalmente para describir la velocidad de los modems o la velocidad de una conexión digital.

Cliente Un cliente es un programa que utiliza los servicios de otro programa. El programa cliente se utiliza para contactar y obtener datos u obtener un servicio a partir del servidor.

Cortafuegos (Firewall) Un cortafuego es un equipamiento, combinación de hardware y software que muchas empresas u organizaciones instalan entre sus redes internas y el Internet. Un cortafuegos permite que sólo un tipo específico de mensajes pueda entrar y/o salir de la red interna. Esto protege a la red interna de los piratas o hackers que intentan entrar en redes internas a través del Internet.

Dirección IP Una dirección IP es un código numérico que identifica a un ordenador específico en Internet. Las direcciones de Internet son asignadas por un organismo llamado InterNIC. El registro incluye un nombre (whitehouse.gov), nombre de dominio, y un número (198.137.240.100), dirección o número IP.

FTP Siglas de File Transfer Protocol. Método muy común para transferir uno o más ficheros de un ordenador a otro. FTP es un medio específico de conexión de un sitio Internet para cargar y descargar ficheros. FTP fue desarrollado durante los comienzos de Internet para copiar ficheros de un ordenador a otro. Con la llegada del World Wide Web, y de los navegadores, ya no se necesitan conocer sus complejos comandos; se puede utilizar FTP escribiendo el URL en la barra de localización que se encuentra en la parte superior de la pantalla del navegador. Por ejemplo, al escribir ftp://nombre.del.sitio/arpeta/nombredelfichero.zip se transfiere el fichero nombredelfichero.zip al disco duro del ordenador. Al escribir ftp://nombre.del.sitio/carpeta/ da una lista con todos los ficheros disponibles en esa carpeta. Cuando un navegador no está equipado con la función FTP, o si se quiere cargar ficheros en un ordenador remoto, se necesitará utilizar un programa cliente FTP. Para utilizar el FTP, se necesita conocer el nombre del fichero, el ordenador en que reside y la carpeta en la que se encuentra. La mayoría de los ficheros están disponibles a través de "anonymous FTP", lo que significa que se puede entrar en el ordenador con el nombre de usuario "anónimo" y utilizar la dirección de correo electrónico propia como contraseña.

HTTP Http son las siglas de HyperText Transfer Protocol, el método utilizado para transferir ficheros hipertexto por Internet. En el World Wide Web, las páginas escritas en HTML utilizan el hipertexto para enlazar con otros documentos. Al pulsar en un hipertexto, se salta a otra página web, fichero de sonido, o imagen. La transferencia hipertexto es simplemente la transeferencia de ficheros hipertexto de un

ordenador a otro. El protocolo de transferencia hipertexto es el conjunto de reglas utilizadas por los ordenadores para transferir ficheros hipertexto, páginas web, por Internet.

IRC Siglas de Internet Relay Chat. El IRC es un programa que permite desarrollar conversaciones en línea en tiempo real con gente de todo el mundo escribiendo mensajes por Internet. Se puede participar en grupos o de manera más privada con sólo una persona. El IRC consiste de "canales" que están dedicados a temas específicos. Cualquiera puede crear un "canal" y cualquier mensaje escrito en un canal dado es visto por todos las personas que estén en dicho canal.

ISP Un proveedor de acceso es el sistema informático remoto al cual se conecta el computador personal del usuario y a través del cual se realiza la conexión con Internet. Es la empresa que provee el acceso a Internet, y en algunos casos una cuenta en línea en su sistema informático

ISDN Siglas de Integrated Services Digital Network. Las líneas ISDN son conexiones realizadas por medio de líneas telefónicas ordinarias para transmitir señales digitales en lugar de analógicas, permitiendo que los datos sean transmitidos más rápidamente que con un módem tradicional.

POP Siglas de Point of Presence. Un POP es el punto de acceso a Internet de un usuario.

PPP Siglas de Point-to-Point Protocol. Es un protocolo de comunicaciones utilizado para transmitir datos de la red a través de las líneas telefónicas. Este tipo de conexión permite comunicar directamente con otros ordenadores de la red por medio de conexiones TCP/IP.

Protocolo Un protocolo es una serie de reglas que utilizan dos ordenadores para comunicar entre sí. Cualquier producto que utilice un protocolo dado debería poder funcionar con otros productos que utilicen el mismo protocolo

Puerto Adaptador de un ordenador al cual se fijan las unidades periféricas, como la impresora o el módem.

Servidor Un servidor es un ordenador que trata las peticiones de datos, el correo electrónico, la transferencia de ficheros, y otros servicios de red realizados por otros ordenadores (clientes).

Sitio web Conjuntos de servicios de red, ante todo documentos HTML, que están enlazados juntos y que existen en el Web en un servidor específico.

SMTP Siglas de Simple Mail Transfer Protocol. Protocolo utilizado para encaminar el correo electrónico por Internet

TCP/IP Son las siglas de Transmission Control Protocol/Internet Protocol, el lenguaje que rige todas las comunicaciones entre todos los ordenadores en Internet. TCP/IP es un conjunto de instrucciones que dictan cómo se han de enviar paquetes de información por distintas redes. También tiene una función de verificación de errores para asegurarse que los paquetes llegan a su destino final en el orden apropiado.

IP Internet Protocol, es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino. TCP, o Transmission Control Protocol, se asegura de que los paquetes lleguen correctamente a su destino. Si TCP determina que un paquete no ha sido recibido, intentará volver a enviarlo hasta que sea recibido correctamente.

PPTP Protocolo de túnel punto a punto (PPTP) Permite que el tráfico multiprotocolo se cifre y se encapsule en un encabezado IP para que, de este modo, se envíe a través de una red IP o una red IP pública, como Internet. PPTP puede utilizarse para el acceso remoto y las conexiones VPN entre sitios. Cuando se usa Internet como la red pública de una VPN, el servidor PPTP es un servidor VPN habilitado para PPTP con una interfaz en Internet y una segunda interfaz en la intranet.

L2TP Protocolo de túnel de capa dos. L2TP permite cifrar el tráfico multiprotocolo y enviarlo a través de cualquier medio compatible con la entrega de datagramas punto a punto, como IP o ATM (modo de transferencia asincrónico). L2TP es una combinación de PPTP y L2F (reenvío de nivel 2), una tecnología desarrollada por Cisco Systems, Inc. L2TP presenta las mejores características de PPTP y L2F.

SSL SSL (Secure Sockets Layer) traducido al español significa Capa de Conexiones Seguras. Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet. Recientemente ha sido sustituido por TLS (Transport Layer Security) el cual está basado en SSL y son totalmente compatibles.

IPSec Es un conjunto de servicios de protección y protocolos de seguridad basados en criptografía. Como no requiere cambios en las aplicaciones o en los protocolos, IPSec se puede instalar fácilmente en las redes existentes. IPSec proporciona autenticación en el nivel de equipo y cifrado de datos para conexiones VPN que utilicen el protocolo L2TP. La negociación de IPSec se realiza entre el equipo y un servidor VPN basado en L2TP antes de establecerse una conexión L2TP. Esta negociación protege las contraseñas y los datos.

Carrier Tiene dos acepciones principalmente en su significado de portadora, es una señal o pulso transmitido a través de una línea de telecomunicación; también se le llama así a una empresa que opera en el sector de las telecomunicaciones ofreciendo servicios de telefonía

Central Telefonica Privada (PBX Private Branch Exchange) Es un sistema telefónico dentro de una empresa que se encarga de conmutar las llamadas entre los usuarios de la misma empresa (también llamadas extensiones) y al mismo tiempo permite que todos los usuarios compartan cierto número de líneas externas (también llamadas troncales)

Codec (comprensión-descompresión). En VoIP, algoritmo de compresión-descompresión que define la relación de compresión de voz, la calidad de voz una vez descomprimida y los requerimientos de capacidad de procesamiento. El códec más popular en VoIP es 6.729(AB) aunque también existe el G 723.1

CTI Computer Telephony Integration (Integracion Telefonia-Computo). Software, hardware y programación necesarios para integrar las computadoras y los teléfonos de manera que puedan funcionar en conjunto sin discontinuidades y en forma inteligente

DECT Digitally Enhanced Cordless Telecommunications (Protocolo Digital de Telefonía Inalámbrica). Es una tecnología para enlazar equipos móviles inalámbricos con telefonía IP

IVR También denominada “unidad de respuesta de voz (VRU)” o “unidad de respuesta de sonido (ARU)”. La unidad IVR responde a los dígitos ingresados por el cliente o reconoce la voz del mismo modo que una computadora responde a las teclas oprimidas desde el teclado o el clic del mouse. Cuando la unidad IVR está integrada con computadoras con bases de datos, los clientes pueden interactuar con esas bases de datos para verificar la información actual (por ejemplo, saldos de cuentas) y realizar transacciones (por ejemplo, hacer transferencias entre cuentas)

Mensajería Unificada Solución de software que integra que integra los servicios de voz, fax, agenda y correo electrónico en un solo buzón, permitiendo acceso desde cualquier teléfono, pc o explorador basado en web

PoE (Power Over Ethernet) Es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones del dispositivo alimentado y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

QoS Calidad de servicio. Medida de desempeño para un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

Radius (Remote Authentication Dial-In User Service). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.