UNIVERSIDAD AMERICANA DE ACAPULCO

EXCELENCIA PARA EL DESARROLLO

FACULTAD DE INGENIERIA EN COMPUTACION
INCORPORADA A LA UNIVERSIDAD
AUNTONOMA DE MEXICO
INCORPORACION 8852-16

ENLACE REMOTO ENTRE DOS REDES: CASO HOTEL ACAPULCO RADISSON

T E S I S

QUE PARA OBTENER EL TITULO DE :
INGENIERO EN COMPUTACION

PRESENTA :

ORLANDO GONZALEZ SANTOS

DIRECTOR DE TESIS

ING. GONZALO TRINIDAD GARRIDO

ACAPULCO, GRO AGOSTO 2006

DEDICATORIA

Quiero empezar agradeciendo a Dios por guiarme, darme la sabiduría y poder ver culminada una parte en mi vida académica.

De igual forma a mis padres Catalina y Bernabé, por darme la bendición de la vida, por enseñarme que la humildad es una parte importante del éxito en las metas que me proponga, gracias por que he aprendido a valorar las cosas y saber disfrutar aquello que te da la vida, por el apoyo que siempre he tenido de ustedes, el cual me motiva a seguir superándome día tras día, finalmente, por que siempre he tenido el acierto de sus consejos, para mi formación personal y académica. Gracias a toda mi familia por su apoyo.

Gracias, por enseñarme que en todo momento se debe de vivir al máximo y no desaprovechar la oportunidad de ser feliz, por que gracias a ti la palabra *vida,* tiene un significado especial, gracias por siempre mostrarme el mejor e increíble lado bueno, de las situaciones adversas, siempre agradeceré el poder haber compartido un poco de mi vida a tu lado. Está dedicado con mucho amor y esfuerzo para ti hermano. Gracias *Carlitos* †.

A ti 'nena', que ante todo has sido una excelente amiga, por que me has inyectado de tu optimismo en todo momento, por tu amor, cariño y comprensión, por ser un gran apoyo en mi vida. Gracias por compartir mis triunfos y apoyarme en mis tropiezos. Gracias Kary[710].

Siendo una parte importante en todo este proceso, a todos mis amigos, que me han brindado su amistad y apoyo incondicionalmente, por haberme permitido disfrutar tantos momentos a su lado, por confiar en mi y en mi amistad, omitiré nombres, por que seria larga la lista, pero ustedes saben que les tengo un cariño especial en donde quiera que se encuentren.

Gracias a ti mi gran amigo, con el cual tuve el privilegio de compartir muchas experiencias inolvidables y a su vez me dejaste grandes enseñanzas. Donde quiera que estés. Con cariño para ti *Ponchito* †.

Orlando González Santos

AGRADECIMIENTOS

- A la Universidad Americana de Acapulco.
  Por permitir que llevara a cabo mis estudios.

- Al rector C.P. Israel Soberanis Nogueda.

- A la Facultad de Ingeniería en Computación.
  Por el gran apoyo que he recibido en lapso de mi licenciatura.

- Al Ing. Gonzalo Trinidad Garrido director de la Facultad.
  Por formar parte importante en este trabajo, agradecerle su disposición en todo momento y aportar sus conocimientos.

- A todos mis maestros, que con su gran capacidad y profesionalismo, fueron pieza clave para el desarrollo de este proyecto y por todos los conocimientos adquiridos.

- Al Ing. Javier Saavedra Lluck.
  Por sus invaluables aportaciones a este trabajo, sus consejos y ser un gran amigo.

- Al hotel Radisson Acapulco.
  Por todas las facilidades, así como el apoyo brindado, para el análisis y estudio de este trabajo, gracias al área de sistemas y representantes del hotel.

INDICE

CAPITULO 4. ANÁLISIS DEL PROBLEMA

CAPITULO 5. CONEXIÓN OMAHA – ACAPULCO

INTRODUCCION

Las sociedades en cualquiera de sus diferentes épocas, se vieron en la necesidad de crear formas y lenguajes para subsistir. Hoy en día, esa misma necesidad, es la que mueve a las grandes compañías de Telecomunicaciones y en general a todas las empresas que están el ámbito de desarrollo de comunicaciones, a seguir diversificando la manera en que nos comunicamos. Conforme se hacen mejoras, y se vuelven eficientes los dispositivos que utilizamos para establecer comunicación entre los demás individuos, se agregan aplicaciones que nos permiten acceder a espacios de entretenimiento o interactuar entre ellos.

Es por ello, que en este trabajo se aborda una opción más de comunicación, la cual esta aplicada al Hotel Radisson Acapulco, basada en el ahorro, en cuanto a costo, para mantener un enlace entre el anterior y el corporativo, que se encuentra en Estados Unidos.

En el capitulo 1, se describen las transformaciones por las que han pasado las primeras redes, pasando por los tipos de enlaces que se manejaban, así como una breve reseña de cómo han evolucionado las redes en México.

En el capitulo 2, se enfoca la importancia y auge que ha tenido el protocolo TCP/IP, cuales son los servicios que provee, como se puede administrar una red de computadoras con dicho protocolo y finalmente como esta compuesto.

En el capitulo 3, se analizan las redes virtuales privadas, las principales ventajas que nos ofrecen, sus alcances. También se analiza una parte importante en una red privada virtual, que es el túnel. Para finalmente, ver los mecanismos de seguridad que se emplean para el mismo.

En el capitulo 4, se analizará la problemática del hotel, cuales son las necesidades en cuanto a procesos que se deben establecer con el corporativo y las posibles soluciones que se plantean.

En el capitulo 5, se analizan los elementos que intervienen, de tipo hardware/software, la implementación de la solución, que se deriva del análisis con la premisa de reducción de costos, así como los parámetros que componen la red privada virtual.

PLANTEAMIENTO DEL PROBLEMA

Desde que la tecnología arribó al área laboral, a significado una ayuda a la cual no todas las empresas pueden alcanzar porque, desafortunadamente, la tecnología cuesta, y más, si es la de vanguardia. Esto a propiciado que entre empresas, se vea claramente, quien esta teniendo éxito y quien no, todo esto al calor de uno de los mejores termómetros, la tecnología. Además de todo esto, el tipo de actividad que ellas desarrollan, es preponderante para determinar la cantidad de ingreso podrán obtener y sobre todo, lo que podrán reinvertir en ellas para el mejoramiento de productos y servicios.

Es bajo este tenor, que las comunicaciones, y en particular los enlaces dedicados (servicios digitales en la actualidad, pero antes analógicos), juegan un papel importantísimo entre la interacción de empresas con matrices y sucursales. En los años 60´s y 70´s , solo algunas actividades como los bancos, las líneas aéreas y grandes cadenas hoteleras podían darse el “lujo” de tener comunicación vía enlaces dedicados, los cuales eran verdaderamente caros, que solo empresas con un nivel de ingresos anuales importantes, podían utilizar esta forma de comunicación, que pienso, debieron haberla visto no tanto como un gasto o inversión, si no más bien, como un punto de oportunidad, sobre todo para eficientar la operación, la concatenación y actualización de la información en “tiempo real”.

Esto no quiere decir que el resto de las empresas, no tuvieran la necesidad de realizar esta misma operación, pero tomando en consideración la actividad económica, el ingreso anual neto, dejaba sin posibilidades de poder ni siquiera en tomar en consideración realizar estas actualizaciones en “tiempo real”.

Este tipo de situaciones incrementaban su costo, si pensábamos en realizar conexiones transnacionales, ahora, no se diga en conexiones intercontinentales. Las líneas privadas, los enlaces dedicados analógicos, posteriormente los enlaces E1 o T1 (según sea el caso de EU y México) y sus enlaces descanalizados DS0, hasta en la actualidad son servicios muy costosos.

En la actualidad, se pueden utilizar innumerables servicios dentro de la red telefónica pública, y uno de ellos es la famosa nube de Internet, la cual puede ser accesada desde cualquier parte del mundo, siempre que se cuente con un servicio de acceso a esta nube, no importa el país en el que nos encontremos.

Pudiéramos pensar en contratar un enlace dedicado desde Acapulco al Distrito Federal, otro desde Acapulco a cualquier parte de Estados Unidos y otro entre dos puntos diferentes en Acapulco. Nos debe de quedar claro que definitivamente el más barato será el que realicemos en la misma ciudad, después el que enlaza a dos ciudades del mismo país y finalmente, el más caro, será el enlace internacional.

¿Por qué no usar la nube de Internet, ya ahí crear un corredor o túnel que solo podamos acceder personas autorizadas, y así, conectar dos redes a través de un medio público sin la necesidad que este enlace sea verdaderamente costoso?

La necesidad particular del Hotel Acapulco Radisson Resort, es de poder conectar un segmento de su red directamente y de manera constante con su similar en la ciudad de Omaha, en los Estados Unidos. Para llevar acabo dicha tarea, ellos tienen dos alternativas, una es un enlace dedicado internacional (verdaderamente costoso), y la otra es habilitar una VPN utilizando en acceso a la nube de Internet, con un proveedor local de Internet, ya que en Omaha, ellos ya cuentan con acceso a la nube de Internet.

OBJETIVOS

- Analizar las necesidades especificas del hotel para realizar la conexión
- Determinar bajo que rubro se hará la conexión (hardware-software)
- Definir las limitantes de este tipo de tecnología
- Construir un túnel seguro para la actualización de los datos

HIPOTESIS

La utilización de las nuevas tecnologías en enlaces, dando como resultado ventaja sobre los enlaces convencionales.

CAPITULO 1. ANTECEDENTES

En medio de tantos avances tecnológicos y al mismo tiempo el rápido crecimiento que conlleva, considero importante hacer una retrospectiva, de lo que han sido, las primeras formas de comunicación a distancia, dando un panorama de cómo se ha ido desarrollado este proceso, que es el de estar comunicados, pero principalmente el medio o la herramienta sobre la cual se basa este estudio y que en la actualidad nos permite estar en comunicación “permanente y de manera casi instantánea”, definitivamente I*nternet,* a su vez introduciéndonos en su creación, y el desarrollo que se ha venido dando en nuestro país.

1.1 Historia

Desde los inicios de la humanidad, el hombre tuvo que empezar a desarrollar diferentes formas y métodos para poder subsistir, quizás una de las propiedades que a través de la evolución ha tenido y que ha sido parte medular en el desarrollo de la sociedad como hasta hoy la conocemos, es la forma en como nos comunicamos. Desde que nuestros antepasados comenzaron a dibujar formas y figuras que a final de cuenta era información, se plasmaba sobre casi cualquier tipo de superficie, de esa manera, era como la información podía de alguna manera ser heredada para las generaciones siguientes. Era inherente en las sociedades de aquellos tiempos, la necesidad de almacenar información, en las condiciones que ya todos conocemos.

Quizás cuando la comunicación con sonidos empezó a emplearse, fue de más utilidad ya que se podían dar mensajes a

distancia (ejemplo, dando avisos de peligro, de una colina a otra), perceptibles para el oído humando y no era necesario tener “presente” al individuo que debería recibir dicho mensaje. Es así como fueron cambiando las cosas y la manera de cómo hacíamos llegar la información a él o los destinatarios deseados, bien cabe mencionar el ejemplo de las señales de humo. Los documentos escritos que esta ahora seguimos empleando, fueron experimentando cambios en cuanto a su forma de hacerse llegar, como sabemos era muchas las formas que se originaron para realizar dicho evento, desde recorrer grandes distancias caminando, con la ayuda de algún animal para poder aminorar el desgaste y el tiempo de recepción del documento, pasando por los grandes descubrimientos como son el telégrafo, el teléfono y muchas otras cosas que ya nos estaban dejando ver que el hecho de querer estar en contacto con alguien más, no iba a requerir demasiado esfuerzo.

De todas esas formas primitivas se pudieron llegar a grandes invenciones que dieron poco a poco al mundo un giro y la pauta para el desarrollo de alta tecnología que hoy tenemos a nuestro alcance, procesos que hasta la fecha todavía utilizamos como son la comunicación vía marítima, aérea, terrestre y lo que esta en boga: el medio electrónico.

En los tres siglos pasados estuvieron relacionados de alguna forma con el progreso de la tecnología en su respectiva época. En el siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la

máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información.

Dejando de lado un poco la versión histórica de lo que ha sido la comunicación a través de las generaciones y acercarnos más al panorama que son las redes, de lo cual se pretende que sea la base de este estudio, es necesario tomar en cuenta los cambios y necesidades que, época tras época, se han ido dando. Quizás las nuevas generaciones no se han dando cuenta que se han estado dando sucesos muy revolucionarios en prácticamente todo nuestro entorno. Como se menciono anteriormente, hemos pasado desde los inventos para comunicarnos a distancia sin mucho esfuerzo como lo es el telégrafo, por el teléfono, la radio y la televisión, hasta el enorme crecimiento que han tenido las redes hasta nuestros días.

Definitivamente cuando hablamos en el sentido estricto de redes, no necesariamente nos referimos a redes de computo, en realidad el concepto de redes poco a poco se ha ido ampliando y podemos identificarlo en casi cualquier lugar en donde nos encontremos, por citar algunos ejemplos, existen redes tipo hidráulicas, redes que transmiten el servicio eléctrico, incluso las empresas que pueden tener franquicias a nivel internacional llámese tiendas departamentales, compañías de refrescos, en fin, un sin numero de ejemplos que podríamos seguir nombrando.

De tal manera estas grandes invenciones han dado lugar a una revolución de la información, por llamarla así, que es la que estamos

experimentando en estos momentos. Conforme va transcurriendo el tiempo se van mejorando y creando nuevos estándares de calidad y de mejor desempeño, en los ámbitos económico, político, social y cultural, así como sé esta buscando una simplificación y hacer cada vez más sencillo el hecho de estar en comunicación con nuestros seres queridos.

Sin duda alguna, sé esta dando una convergencia de la tecnología que utilizamos en la actualidad hacia cualquier rubro de nuestra vida. También se percibe una diferencia en la manera de cómo se realiza la captura, transporte almacenamiento y procesamiento de información las cuales están evolucionando con rapidez.

En lo que se refiere al desarrollado de las computadoras, estas han tenido un progreso evolutivo demasiado veloz, hace 40 años no nos hubiéramos imaginado que iban a existir diversas opciones que nos permitieran una comunicación y no solo eso, si no enviar diferentes tipos de comunicación.

El antiguo esquema que sé tenia de que una computadora “central”, controlara o administrara a un grupo finito de computadoras en una empresa, se ha esta sustituyendo por el de varios equipos interconectados haciendo los mismos procesos, pero claro esta con un aumento considerable en los tiempos y la eficiencia que representa esto, es de ahí de donde se deriva el concepto de redes de computadoras.

Es por eso que considero valido hacer mención un poco sobre el inicio y desarrollo de Internet hasta nuestros días.

1.1.1 Internet

Antes de empezar a hacer mención sobre los enlaces, quisiera recordar un poco los orígenes de estos. Haciendo un poco de historia sabemos que el origen de Internet surgió de la necesidad de establecer una comunicación entre computadoras localizadas en distintos puntos geográficos, este fue el problema que tenia que resolver las oficinas militares de los Estados Unidos.

"A comienzos de la década del 60 A.R.P.A. emprendió la tarea de desarrollar un sistema militar de comunicaciones en red diseñado específicamente para interconectar computadores en forma descentralizada cuyo objetivo principal debía ser continuar operando aun en el caso de alguno o varios de sus nodos de comunicaciones fueran destruidos durante un ataque enemigo."[1]

En 1969 la Advanced Research Projects Agency (ARPA) del Pentágono creó la primera red llamada ARPAnet, la cual constaba sólo de cuatro computadoras conectadas, una en la Universidad de California en los Ángeles (UCLA), otra en el Instituto de Investigaciones de Stanford (SRI), una más en la Universidad de California en Santa Bárbara (UCSB) y la última en la Universidad de UTHA.

[1] Fuente: http://www.paralibros.com/passim/p20-tec/pg2058dr.htm

Un par de años más tarde se fueron agregando otros nodos hasta llegar a un total de 40. Después, en el año de 1974 Vint Cerf y Robert Kahn, elaboraron un documento llamado A protocol for Packet Network Internetworking, en el cual daba una solución al problema de cómo se comunicaban diferentes tipos de maquinas. Exactamente 8 años mas tarde se crea el TCP / IP (Protocolo de Control de Transmisión / Protocolo de Internet) que fue tomado como estándar por el Departamento de los Estados Unidos. Así, ese mismo año el Departamento de la Defensa se separo de ARPAnet y creo su propia red llamada MILnet.

"Esto permitió al ejército empezar a compartir la tecnología DARPA basada en Internet y llevó a la separación final entre las comunidades militares y no militares. En 1983 ARPANET estaba siendo usada por un número significativo de organizaciones operativas, de investigación y desarrollo en el área de la defensa."[2]

En definitiva el protocolo TCP/IP se ha hecho un estándar en lo que se refiere a la comunicación entre equipos de cómputo siendo este el más utilizado en todo el mundo. Mas adelante podremos hablar del con mas detalle.

Con la separación de la parte militar, se permitió el acceso a otras instituciones no nada más de Estados Unidos si no de todo el mundo, siempre y cuando fuera para fines académicos o de investigación.

[2] Fuente: http://www.ati.es/DOCS/internet/histint/histint1.html

En la actualidad el concepto que tenemos de Internet, es como un conjunto de redes que estas a su vez forman una gran red, una red mundial. Cada red de la que esta compuesta Internet, esta diseñada de acuerdo a su entorno especifico y requerimientos de las empresas o instituciones que las crean, no existen restricciones en los tipos de red que pueden ser incorporadas, ni tampoco importa donde se encuentren localizadas.

Retomando la evolución de las redes y de la manera en como intercambiamos información, la actividad en nuestro país comenzó también como un proyecto académico, involucrando primeramente universidades.

1.1.2 Internet en México, la red BITNET

"BITNET es una red digital internacional de telecomunicación que enlaza a más de 1 000 organizaciones de investigación e instituciones educacionales en los Estados Unidos, Canadá y Europa. Cada institución participante contribuye con computadoras, líneas de comunicación arrendadas, personal y programas de comunicación. El propósito primordial de BITNET es el de facilitar el intercambio de información no comercial en apoyo a la misión en la investigación o la educación de la institución miembro. Existen compuertas de acceso (*gateways*) entre BITNET y otras redes, tales como INTERNET, ARPANET NSFNET y JANET."[3]

[3] Fuente: http://www.bvs.sld.cu/revistas/aci/vol2_2_94/aci02294.htm

“En 1986, el Campus Monterrey del Tecnológico de Monterrey (ITESM) ya recibía, por medio de líneas conmutadas, la información electrónica que circulaba a través de la red BITNET. El 15 de junio de 1987, el ITESM Campus Monterrey estableció una conexión de carácter permanente hacia esa importante red de información electrónica. Posteriormente, en octubre de 1986, la Universidad Nacional Autónoma de México también se conectó a la red BITNET.

El 28 de febrero de 1989, el Tecnológico de Monterrey Campus Monterrey se convirtió en la primera institución mexicana que logró establecer un enlace a Internet, a través de una línea analógica privada de cinco hilos de nueve mil 600 bits por segundo.

El acceso a Internet se estableció por medio de un enlace hacia la Escuela de Medicina de la Universidad de Texas, en San Antonio, Estados Unidos (UTSA). En 1989, el ITESM ya disponía de tres líneas de acceso. Todas las formas de enlace se realizaban a través de la UTSA. El Campus Monterrey estableció el primer nodo de Internet en México y en consecuencia lógicamente dispuso del primer name server para el dominio (.mx).

La UNAM fue la segunda institución que consiguió establecer un acceso a Internet, conformando un segundo nodo entre el Instituto de Astronomía –ubicado en la Ciudad de México– y el Centro Nacional de Investigación Atmosférica (NCAR) –en Boulder, Colorado, Estados Unidos–. Ese enlace digital se estableció vía satélite a 56 Kbps. La UNAM y el Tecnológico de Monterrey Campus Monterrey entonces

mantenían un enlace común a través de la red de la información BITNET, mediante líneas analógicas privadas.

La tercera institución que consiguió conectarse a Internet fue el ITESM Campus Estado de México. Tal conexión también fue posible a través de la NCAR."[4]

Tiempo más tarde, surgió otro organismo denominado MEXNET que reunía representantes legales de cada institución, el cual incluía a varias universidades de distintos lugares del país. Dicha organización, en 1992, establece una salida de 56 kbps al Backbone de Internet. En 1993 la CONACyT se conecta a Internet mediante un enlace satelital al NCAR (Centro Nacional de Investigación Atmosférica) al igual que el ITAM, la UAM, en ese mismo año, se establece como el primer NAP (Network Access Point), al intercambiar tráfico entre dos diferentes redes. A finales de este año en México ya se contaba con distintas redes: MEXnet, Red UNAM, Red ITESEM, RUTyC (desaparece el mismo año), BAJAnet, Red total CONACyT y SIRACyT. Fue en 1994, con la fundación de la Red Tecnológica Nacional (RTN), integrada por MEXnet y CONACyt, que se generó un enlace a 2 Mbps (E1).

En 1996, se registran cerca de 17 enlaces E1 contratados con TELMEX para uso privado, asimismo se consolidan los principales ISP's (proveedores de servicios de Internet) en el país, de los casi ya 100 ubicados a lo largo y ancho del territorio nacional. Para el año de 1997 existen más de 150 ISP's, ubicados en los principales centros

[4] Fuente: http://www.mexicanadecomunicacion.com.mx/Tables/FMB/foromex/apuntes.html

urbanos: Cd. de México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Laredo, Saltillo, Oaxaca, entre otros.

A partir de estas etapas por las que pasábamos conjuntamente con otros países que o bien ya contaban con esa infraestructura o iban empezando a adoptar todos esos mecanismos de comunicación, al mismo tiempo se estaba construyendo en nuestro país las bases, para lo cual hoy tenemos al alcance las herramientas que conocemos.

1.2 Tipos de Enlaces

Los Enlaces Digitales representan la evolución natural de los servicios de datos, orientados a las necesidades internas de comunicación de las empresas, basadas en las nuevas tecnologías construidas alrededor de Internet, conservando las características especiales de estos servicios, tales como calidad, seguridad, control y gestión de cliente.

Básicamente los enlaces con los que contamos ya sea de tipo punto a punto, **Frame Relay** o **ATM**, por lo que encontrará su principal aplicación en el ámbito empresarial. Su mercado objetivo son las grandes corporaciones y las PyMES con necesidad de conectar puntos dispersos geográficamente con conexiones permanentes la Red IP.

Los Enlaces Digitales se pueden combinar conjuntamente con el **Servicio Dial-Up**, para ofrecer una solución integral a las comunicaciones de empresa, incrementando la capacidad de acceso a los trabajadores remotos vía la Red de Telefonía Básica.

También se cuenta actualmente, con los llamados *Servicios Digitales*, estos proporcionan capacidad de manejar información de manera digital, ya sea voz, imaginen y datos. Estos servicios, permiten tanto a hogares como a cualquier empresa prácticamente, tener integrado, en una misma línea física, diferentes servicios.

Los Enlaces Digitales están dirigidos a aquellas empresas que tienen distintas sedes situadas en lugares separados geográficamente, que dispongan de redes de área local y que tengan la intención de unir dichas LAN's para formar una intranet, haciendo uso de las tecnologías IP.

Una forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (*Internet*). Como por ejemplo, el tan conocido por todos, *correo electrónico* (e-mail), que se envía desde una terminal, a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías e imágenes.

1.3 La importancia de los Enlaces a través de los tiempos

Las grandes empresas que hoy en día conocemos y de las cuales algunos somos consumidores, han experimentado un crecimiento muy notable a través del tiempo, poco a poco han visto sus aumentos de ganancias, desarrollos en sus maquinarias, aumento en su planta de empleados y es todo esto a su vez en otras sedes, las cuales se empezaron a situar en distancias relativamente cercanas, después en provincias y posteriormente en todo el mundo. Esta distribución de pequeñas sedes en otros países, ha permitido optimizar

y reducir costos en muchos de los aspectos con los que cuentan las empresas, otra de las ventajas es que le ayuda a reducir costos de entrega de sus productos, en muchos casos la propia manufactura de sus productos dentro de algún país determinado, definitivamente el éxito de a empresa depende de la calidad de su producto y/o en dado caso que la empresa preste un servicio, obviamente la atención que se le de al cliente, cualquiera que sea el caso, el objetivo se enfoca al cliente y su principal preocupación es la satisfacción que este pueda tener.

Una parte vital de cualquier empresa es la forma en como esta realiza una conexión ya sea matriz-sucursal, sucursal-matriz o sucursal-sucursal, pudiendo existir más variantes, todo esto dando como resultado el intercambio de cualquier información. Prácticamente es estos tiempos es imprescindible que alguna empresa por pequeña que esta sea, ya cuente o este pensando en adquirir un equipo o sistema de comunicación, para el funcionamiento adecuado y la optimización de recursos con los que cuente dicha empresa. Por ejemplo, procesos como el estar en contacto con un distribuidor o proveedor, permiten el reabastecimiento oportuno de algún producto que haya sido demandado.

Muchos de nosotros seguramente en algún momento nos preguntamos, ¿cómo es que los establecimientos que visito frecuentemente puedan tener (en la mayoría de los casos) los productos que compro? Quizás lo que menos nos preocupe es como le hacen para levantar un pedido, para elaborar un reporte, para hacer

una reservación, pero sin embargo sabemos que intervienen muchos factores, tanto humanos como recursos tecnológicos, siendo estos últimos los que nos permitan establecer comunicaciones hacia otro lugar, con un departamento en algún piso hasta alguna oficina en el otro lado del mundo, otra forma de ver el alcance de las comunicaciones es que desde unas decenas o cientos de metros hasta miles de kilómetros de distancia, podemos establecer comunicación casi inmediatamente con uno o muchos quizás a la vez. La necesidad de estar comunicados ya sea por la actividad y mejoramiento de un país, ha hecho que la tecnología este presente en muchos de los ámbitos cotidianos.

Se pueden seguir citando infinidad de ejemplos en donde se involucren los distintos medios de comunicación, así como la forma en como se realiza dicha conexión entre distintas entidades. Es muy importante tener claro y definidos los objetivos reales de la empresa y que partes son las que tienen más prioridad o son más vulnerables. Una vez analizados los datos y presentado la solución o las propuestas que hagamos, para resolver un problema como el que se pretende abordar en este documento, podremos tener una idea mas clara y emitir un juicio más preciso, de que es lo que necesitaremos para resolver eso. De entre los factores que intervendrán para poder llegar a una solución optima, nos podemos encontrar, el de tipo monetario, quizás el tiempo de implementación, así como el material humano que estará a cargo, de entre otras instancias más.

1.4 Accesos remotos seguros

En la actualidad es común que cualquier usuario de Internet necesite de cierta privacidad para algunos servicios que nos pueda ofrecer la WWW. En aplicaciones tan utilizadas como el correo electrónico, por citar algún ejemplo, un usuario para poder acceder a este servicio, requiere de un *nombre de usuario* y una *contraseña,* de lo contrario no se podremos utilizarlo. Este *nombre de usuario* y esta *contraseña* nos servirán para tener el servicio de correo electrónico cuantas veces lo deseemos, ya que estos elementos serán la forma de identificarnos dentro de la red en que nos encontremos. La principal desventaja radica en que el sistema o servicio del cual estemos haciendo uso, no podrá detectar si en realidad, el que esta utilizando el servicio es la persona indicada, pero es aquí en donde se pueden apreciar diferentes mecanismos y métodos que se han ido descubriendo a través del tiempo, dentro de los cuales principalmente son de manera remota.

Hoy en día este rubro (el de las comunicaciones seguras), se ha puesto de moda, por decirlo de alguna manera, ya que se han visto mas presentes los ataques desde o hacia, llámesele usuarios, empresas de todos tamaños, hasta instituciones gubernamentales o educativas. Aunque cabe destacar que el problema no es nuevo y así como evolucionó la forma de interconectarse, también hubo cabida a detalles de pérdida o modificación de la información por otras entidades. Por lo tanto, se han desarrollado políticas internas dentro de las instituciones para que este problema, permita un funcionamiento y desarrollo de las empresas como se pretende. Pero ¿por qué hablar de políticas internas

y demás? Considero, y se puede constatar en la mayoría de las empresas, en donde cada una empleará criterios y reglamentos a utilizar para el uso correcto de la información y otras aplicaciones. A lo que se ha llegado es a que cada día resulte más difícil a las o grupos de personas no autorizadas, el acceso a los datos de cualquier entidad, aun así seamos *simples* usuarios de Internet.

Las posibilidades de comunicación que nos ofrece Internet y los diferentes protocolos de comunicación, son muy extensas, y día a día los estamos comprobando. Lo más importante remarcar, es que es un medio versátil que nos permite estar en contacto con casi cualquier parte o persona, ubicada geográficamente en otro lugar, aunque claro muchas de ellas tienen sus puntos en contra, como podría ser la velocidad en las transmisiones, la intercepción de la información que estemos enviando, el costo del servicio que utilicemos, es decir todo tendrá un precio.

Pero a lo que se pretende llegar es que mientras nosotros no podamos garantizar una conexión segura, es decir utilizando las herramientas adecuadas (software/hardware según sea el caso) entre dos o más puntos que se requiera dicha conexión y suponiendo que nosotros tengamos la responsabilidad de realizar esta tarea, muy probablemente nos podría costar nuestro puesto, si no le damos la importancia a esta parte de la comunicación.

Cabe hacer notar que no será suficiente con estar protegidos, de los ataques de los cuales pudiéramos ser objetos. Si no que debemos asegurar la calidad y facilidad para que los usuarios que deseen acceder a nuestro sistema se lleve a cabo de manera eficiente y segura, de manera que no se violen las políticas que tenga establecida la organización en cuestión.

CAPITULO 2.
PROTOCOLO TCP/IP DE INTERNET

Conocido de manera oficial como el grupo de protocolos Internet TCP/IP, pero llamado más comúnmente TCP/IP (siglas provenientes de sus dos principales estándares) el nombre TCP / IP proviene de dos de los protocolos más importantes de la familia de protocolos de Internet, el *Transmission Control Protocol* (TCP) e *Internet Protocol* (IP), éste puede utilizarse para comunicarse a través de cualquier grupo de redes interconectadas. Por ejemplo, algunas empresas utilizan el TCP/IP para interconectar todas las redes dentro de la corporación, aun cuando las empresas no tengan una conexión hacia redes externas. Otros grupos utilizan el TCP/IP para comunicarse entre sitios geográficamente alejados uno del otro. La arquitectura TCP / IP transfiere datos mediante el ensamblaje de datos en paquetes. Cada paquete comienza con una cabecera que contiene información de control seguida de los datos. He aquí una breve descripción:

- *Internet Protocol* (IP), un protocolo del nivel de red del modelo OSI, permite a las aplicaciones ejecutarse de forma transparente sobre las redes interconectadas. De esta forma, las aplicaciones no necesitan conocer qué *hardware* esta siendo utilizado en la red y, por tanto, la misma aplicación puede ejecutarse en cualquier arquitectura de red.
- *Transmission Control Protocol* (TCP), un protocolo del nivel de transporte de OSI, asegura que los datos sean entregados, que lo que se recibe corresponde con lo que se envió y que los

paquetes sean reensamblados en el orden en que fueron enviados.

2.1 Servicios de Internet

A continuación se revisan de manera breve los servicios de una red de redes, resaltando los servicios que la mayoría de los usuarios utiliza.

El análisis de los servicios se enfoca en estándares llamados *protocolos*. Protocolos como el TCP y el IP proporcionan las reglas para la comunicación. Contienen los detalles referentes a los formatos de los mensajes, describen como responde una computadora cuando llega un mensaje y especifican de que manera una computadora maneja un error u otras condiciones anormales. En cierto sentido, los protocolos son para las comunicaciones lo que los algoritmos para la computación. Un algoritmo permite especificar o entender un cómputo aunque no se conozcan los detalles de un juego de instrucciones de CPU. De manera similar, un protocolo de comunicaciones permite especificar o entender la comunicación de datos sin depender de un conocimiento detallado de una marca en particular de hardware de red.

Existen dos tipos de servicios: *Servicios de Internet a nivel aplicación y Servicios de Internet a nivel red.*

2.2 Servicios de Internet a nivel aplicación

Desde el punto de vista de un usuario, una red de redes TCP/IP aparece como un grupo de programas de aplicación que utiliza la red para llevar a cabo tareas útiles de comunicación. Los programas de aplicación de Internet muestran un alto grado de interoperabilidad, refirámonos a *interoperabilidad*, como la habilidad que tienen diversos sistemas de computación para cooperar en la resolución de problemas computacionales. Algunos de los servicios de aplicación de Internet más populares son:

- ***Correo electrónico***: Al utilizar el TCP/IP se logra que la entrega sea más confiable debido a que no se basa en computadoras intermedias para distribuir los mensajes de correo. Un sistema de entrega de correo de TCP/IP opera al hacer que la maquina del transmisor contacte directamente la maquina del receptor. Por lo tanto, el transmisor sabe que, una vez que el mensaje salga de su maquina local, se habrá recibido de manera exitosa en el sitio de destino.
- ***Transferencia de archivos***: Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo esta diseñado principalmente para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación de transferencia de archivos, el cual permite que los usuarios envíen o reciban archivos arbitrariamente grandes de programas o de datos. Por ejemplo, al utilizar el programa de transferencia de archivos, se puede copiar de una maquina a otra una gran base

de datos que contenga imágenes de satélites, un programa escrito en C++, o un diccionario del idioma ingles.

- ***Acceso remoto***: El acceso remoto permite que un usuario que este frente a una computadora se conecte a una maquina remota y establezca una sesión interactiva. El acceso remoto hace aparecer una ventana en la pantalla del usuario, la cual se conecta directamente con la maquina remota al enviar cada golpe de tecla desde el teclado del usuario a una maquina remota y muestra en la ventana del usuario cada carácter que la computadora remota genere. Cuando termina la sesión de acceso remoto, la aplicación regresa al usuario a su sistema local.

2.3 Servicios de Internet a nivel de Red

Un programador o empresa, que desarrolla aplicaciones para diversas problemáticas, las cuales tiene como base el protocolo TCP/IP, y en general cualquier otro protocolo que se utilice, tiene la prioridad de estudiar los distintos métodos y formas de representación de los problemas y una vez estudiados todos los casos, dan como resultado un Programa (software), el cual ayuda al usuario final, a resolver sus requerimientos de manera transparente y eficiente. En el nivel de red, una red de redes proporciona dos grandes tipos de servicio que todos los programas de aplicación utilizan.

- ***Servicio sin conexión de entrega de paquetes***: Este servicio forma la base de todos los otros servicios de red de redes. La entrega sin conexión es una abstracción del servicio que la

mayoría de las redes de conmutación de paquetes ofrece. Simplemente significa que una red de redes TCP/IP rutea mensajes pequeños de una maquina a otra, basándose en la información de dirección que contiene cada mensaje. Debido a que el servicio sin conexión rutea cada paquete por separado, no garantiza una entrega confiable y en orden.

- ***Servicio de transporte de flujo confiable***: La mayor parte de las aplicaciones necesitan mucho más que solo la entrega de paquetes, debido a que requieren que el software de comunicaciones se recupere de manera automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable resuelve dichos problemas. Permite que una aplicación en una computadora establezca una “conexión” con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si ésta fuera permanente y directa del hardware. Debajo de todo esto, por supuesto, los protocolos de comunicación dividen el flujo de datos en pequeños mensajes y los envían, uno tras otro, esperando que el receptor proporcione un acuse de recibe de la recepción.

Diferenciación de los servicios TCP/IP de los otros:

- ***Independencia de la tecnología de red.*** Ya que el TCP/IP esta basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en

particular. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada *datagrama*, y especifican cómo transmitir los datagramas en una red en particular.

- ***Interconexión universal.*** Una red de redes TCP/IP permite que se comunique cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una *dirección* reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de su fuente y su destino. Las computadoras intermedias de conmutación utilizan la dirección de destino para tomar decisiones de ruteo.
- ***Acuses de recibo punto-a-punto.*** Los protocolos TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre maquinas sucesivas a lo largo del camino, aun cuando las dos maquinas no estén conectadas a la misma red física.
- ***Estándares de protocolo de aplicación.*** Además de los servicios básicos de nivel de transporte (como las conexiones de flujo confiable), los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto.

2.4 Denominación a una computadora en TCP / IP

Es importante que se establezca la identificación de la estación de trabajo de una forma que evite su duplicidad dentro de todas las computadoras que puedan conectarse. Para ello, en TCP / IP, se utiliza el nombre de usuario y el nombre de dominio de la red. Para identificar al usuario es necesario nombrarlo evitando que pueda haber dos con el

mismo nombre y produzca confusiones al servidor de la red. Para identificar a la red se utiliza el concepto de dominio. La estructura del dominio se asemeja a un árbol invertido (el tronco se encuentra en la parte superior y las ramas en la parte inferior) y cada hoja corresponde a un dominio.

La identificación de un dominio está formada por varios apartados separados por un punto (por ejemplo, RED1.MEC.EDU). Cada uno de ellos recibe el nombre de subdominio. El subdominio situado más a la derecha es el de carácter más general y recibe el nombre de dominio de nivel alto.

El nombre de un dominio completamente calificado (*Full Qualified Domain Name*) ha de empezar por el nombre de la estación de trabajo (HOST), un punto, y el nombre de la red (DOMINIO).

2.5 Direcciones IPv4

Las direcciones IP consiguen que el envío de datos entre computadoras se realice de forma eficaz, de forma parecida a como se utilizan los números de teléfono en las llamadas telefónicas.

Actualmente, las direcciones *IP* de la versión actual (*IPv4*) tienen 32 bits, formados por cuatro campos de 8 bits (octeto), cada uno, separados por puntos. Por tanto, las direcciones IP están en representación binaria. Normalmente y debido a la dificultad del sistema binario, la dirección *IP* se representa en decimal.

Los cuatro octetos de la dirección *IP* componen una dirección de red y una dirección de equipo que están en función de la clase correspondiente.

2.5.1 Tipos de Clases

Existen cinco clases de redes: A, B, C, D o E (esta diferenciación viene dada en función del número de computadoras que van a tener la red).

- La **clase A** contiene 7 *bits* para direcciones de red (el primer *bit* del octeto siempre es un cero) y los 24 bits restantes representan a direcciones de equipo. De esta manera, permite tener un máximo de 128 redes (aunque en realidad tienen 126, ya que están reservadas las redes cuya dirección de red empieza por cero y por 127), cada una de las cuales pueden tener 16,777,216 computadoras (aunque en realidad tienen 16,777,214 computadoras cada una, ya que se reservan aquellas direcciones de equipo, en binario, cuyos valores sean todos ceros o todos unos). Las direcciones, en representación decimal, estarán comprendidas entre 0.0.0.0 y 127.255.255.255 y la máscara de subred será de 255.0.0.0.
- La **clase B** contiene 14 *bits* para direcciones de red (ya que el valor de los dos primeros *bits* del primer octeto ha de ser siempre 10) y 16 *bits* para direcciones de equipo, lo que permite tener un máximo de 16,384 redes, cada una de las cuales pueden tener 65,536 computadoras (aunque en realidad tienen 65,534 computadoras cada una, ya que se reservan aquellas

direcciones de equipo, en binario, cuyos valores sean todos ceros o todos unos). Las direcciones, en representación decimal, estarán comprendidas entre 128.0.0.0 y 191.255.255.255 y su máscara de subred será de 255.255.0.0.

- La **clase C** contiene 21 *bits* para direcciones de red (ya que el valor de los tres primeros *bits* del primer octeto ha de ser siempre 110) y 8 bits para direcciones de equipo, lo que permite tener un máximo de 2,097,152 redes, cada una de las cuales pueden tener 256 computadoras (aunque en realidad tienen 254 computadoras cada una, ya que se reservan aquellas direcciones de equipo, en binario, cuyos valores sean todos ceros o todos unos). Las direcciones, en representación decimal, estarán comprendidas entre 192.0.0.0 y 223.255.255.255 y su máscara de subred será de 255.255.255.0.
- La **clase D** se reserva todas las direcciones para multidestino (multicasting), es decir, una computadora transmite un mensaje a un grupo específico de computadoras de esta clase. El valor de los cuatro primeros *bits* del primer octeto ha de ser siempre 1110 y los últimos 28 *bits* representan los grupos multidestinos. Las direcciones, en representación decimal, estarán comprendidas entre 224.0.0.0 y 239.255.255.255.
- La **clase E** se utiliza con fines experimentales únicamente y no está disponible para el público. El valor de los cuatro primeros *bits* del primer octeto ha de ser siempre 1111 y las direcciones, en representación decimal, estarán comprendidas entre 240.0.0.0 y 255.255.255.255.

2.5.2 Segmentación de la Red

Actualmente debido al uso masivo de aplicaciones cliente-servidor y multimedia que requieren la transmisión de grandes volúmenes de información, la tecnología de redes de área local, que en algunos casos data de desde hace unos 20 años, se ha visto en la necesidad de transmitir un gran volumen de datos y con mayor rapidez. Esta necesidad ha obligado a buscar tecnologías que permitan aumentar el ancho de banda y mejorar, e incluso intentar asegurar, los tiempos de respuestas.

Cuando en una red se empiezan a presentar problemas de transmisión de los datos, como las colisiones y pérdidas de los mismos además dando como resultado reducción en el ancho de banda, una posible solución es dividir la red en segmentos separados que se conectaran mediante puentes (*bridges*), procurando reducir el trafico entre dichos segmentos al mínimo, pues el puente sólo dejará pasar de un segmento a otro, aquellos paquetes que vayan dirigidos específicamente a algún nodo en el segmento destino. Cuanto más segmentada esté la red, mejor será su rendimiento pues cada uno de los segmentos tendrá menos estaciones y una probabilidad mucho menor de producirse colisiones.

2.5.3 Mascara de la Subred IP

Una dirección de subred se crea “pidiendo bits prestados” del campo host y designándolos como un campo de subred. El número de bits prestados varía y está especificado por la máscara de subred.

Las máscaras de subred utilizan el mismo formato y técnica de representación que las direcciones IP. Sin embargo, la máscara de subred tiene 1’s binarios en todos los bits, los cuales especifican los campos de red y subred y 0’s binarios en todos los bits que especifican el campo de host.

Los bits de la máscara de subred deben provenir de los bits de orden superior (los que están más a la izquierda) del campo de host.

CAPITULO 3.
TECNOLOGÍAS DE VPN

Habiendo mencionado un poco de la importancia de los métodos que se usaron para comunicarse en épocas pasadas y el progreso que se ha dado hasta nuestros días, enfoquémonos más a ver las herramientas con las que pretendemos atacar este problema, que para efectos de este trabajo son las *Redes Virtuales Privadas*, es decir, ver otra opción y hacer uso de uso de esa enorme “red de redes”, el cual es el objetivo de este trabajo, así mismo identificar los elementos, características y los procedimientos que se requieren para poder construir una red de este tipo.

3.1 REDES VIRTUALES PRIVADAS (Virtual Private Network)

Una red privada virtual (Virtual Private Network) es una red privada que se extiende, mediante un proceso de encapsulación, y en su caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

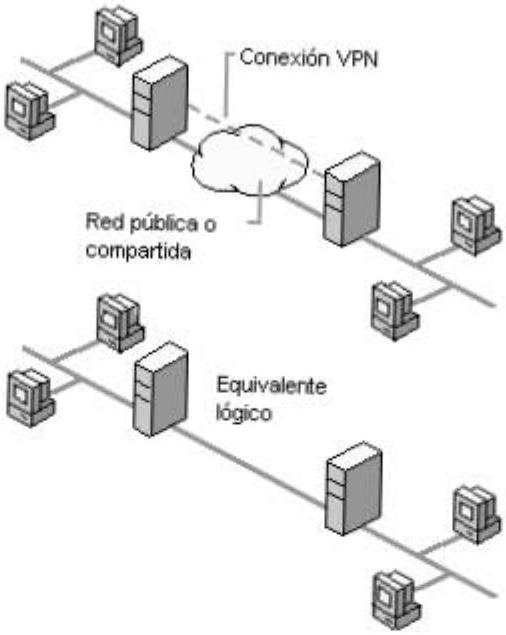

Figura 1.

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su computadora remota las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público:

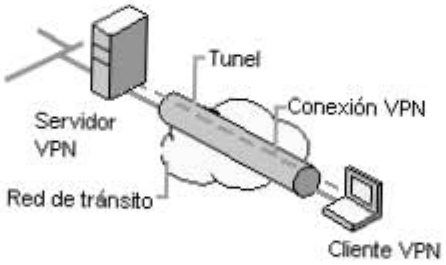

Figura 2.

3.1.1 Tipos de Redes Virtuales Privadas

Las redes privadas virtuales se dividen en 3 categorías distintas dependiendo del servicio de conectividad que brindan:

VPN de Acceso: Provee acceso remoto a la Intranet o Extranet corporativa a través de una infraestructura pública manteniendo las mismas políticas (seguridad, calidad de servicio, etc.) que en la red privada. La VPN de Acceso permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o simplemente IP para la conexión segura de usuarios móviles, Telecommuters o sucursales remotas a los recursos corporativos.

VPN de Intranet: Vincula la oficina remota o sucursal a la red corporativa a través de una red pública, mediante enlace dedicado al Proveedor de Servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio, disponibilidad, etc.

VPN de Extranet: Permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública.

3.1.2 Calidad de Servicio en las VPN

La calidad de servicio, permite la asignación eficiente de los recursos de la red pública a las distintas VPN para que estas puedan tener un rendimiento predecible. A su vez las VPN asignarán distintas políticas de calidad de servicio a sus usuarios, aplicaciones o servicios.

Los componentes básicos de la tecnología de Calidad de Servicio son:

Clasificación de Paquetes: asignación de prioridades a los paquetes basados en la política corporativa. Se pueden definir hasta 7 clases de

prioridades utilizando el campo de IP precedente dentro del encabezado del paquete IP.

Committed Access Rate (CAR): garantiza un ancho de banda mínimo para aplicaciones o usuarios basándose en la política corporativa.

Weighted Fair Queuing (WFQ): determina la velocidad de salida de los paquetes en base a la prioridad asignada a estos, mediante el encolado de los paquetes.

Weighted Random Early Detection (WRED): complementa las funciones de TCP en la prevención y manejo de la congestión de la red, mediante el descarte de paquetes de baja prioridad.

Generic Traffic Shaping (GTS): reduce la velocidad de salida de los paquetes con el fin de reducir posibles congestiones de la red que tengan como consecuencia el descarte de paquetes.

3.1.3 Capacidades de una VPN

A continuación, se mencionan las principales tareas que una VPN en particular, debe realizar:

- Identificación de Usuario. La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN, a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien accesó, que información y cuando.

- Administración de Direcciones. La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.
- Codificación de Datos. Los datos que se van a transmitir a través de la red pública, deben ser previamente encriptados, para que no puedan ser leídos por clientes no autorizados de la red.
- Administración de Claves. La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.
- Soporte a Protocolos Múltiples. La VPN debe ser capaz, de manejar los protocolos más comunes que se utilizan en la red pública. Estos incluyen, el Protocolo de Internet (IP), el Intercambio de Paquete de Internet (IPX), entre otros.

3.1.4 Componentes de una VPN

Básicamente, los componentes que intervienen en la creación de una Red Privada Virtual, son tan casi comunes, como los que se utilizan en la elaboración de redes, de las grandes empresas. La principal característica en una VPN, es que las empresas tengan la capacidad, de poder ser accesadas por distintas entidades, llámense clientes, proveedores, sucursales, etc., claro esta, debidamente configurados, teniendo como prioridad, la disminución de costos, en tener líneas dedicadas.

Estas herramientas son las siguientes:

- Un Gateway VPN
- Software
- Firewall
- Router
- Dispositivos con un software y hardware especial para proveer de capacidad a la VPN.

Cabe destacar, que si estamos trabajando sobre una plataforma PC o Workstation, el software desempeñará y optimizará todas las funciones de la VPN.

3.1.5 Ventajas de una VPN

- Unen oficinas remotas a través de Internet.
- La ubicación de las oficinas es indiferente; pueden estar a ambos lados de una calle, en la misma ciudad o en cualquier lugar del mundo.
- Se utiliza encriptación de alto nivel IPSec.
- La conexión a Internet puede ser ADSL, Cable o RDSI, podemos acceder con prácticamente cualquier medio a Internet.
- Ahorro de grandes sumas de dinero en líneas dedicadas.
- Escalabilidad: soportan múltiples túneles simultáneos.
- Flexibilidad: Las oficinas remotas pueden configurarse rápidamente.
- Uniones remotas de carácter temporal pueden establecerse con facilidad.

Por otra parte, la principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican 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, etc. a través de un acceso público.

De entre los inconvenientes podemos citar: una mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una mayor relentización de la mayoría de conexiones. También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).

3.1.6 Funcionamiento de una VPN

En esta parte, se muestra una visión en general, sobre el funcionamiento de una Red Privada Virtual.

Cuando se realiza la conexión de una VPN, el software de los extremos contacta el acceso a la VPN, por ejemplo, al Router de Ethernet de una oficina. Este acceso, generalmente, verifica si es un

usuario aprobado verificando el password. Luego, el mismo software crea el túnel y agrega un encabezado al paquete de datos que el Internet pueda interpretar. Cuando el paquete llega hacia el punto de acceso (es decir hacia la entrada de la otra red o de la PC), dicho acceso, lo direcciona hacia el destino final.

A lo largo de este texto, hemos encontrado términos como túnel y encriptación, a continuación se explicara un poco de ellos.

3.2 TUNEL EN UNA VPN

Una VPN crea un túnel a través de Internet, esto es, una unión punto a punto que utiliza una fuerte encriptación. De esta manera, aunque el túnel utilice una red pública como es Internet, los datos que circulan por el túnel están encriptados. Fuera del túnel, los dos ruteadores utilizan direcciones IP públicas (estáticas o dinámicas, según sean proporcionadas por el proveedor de servicios), pero dentro del túnel las redes locales utilizan rangos de direcciones privados (por ejemplo 192.168.3.1 a 192.168.3.254) que no son accesibles desde Internet.

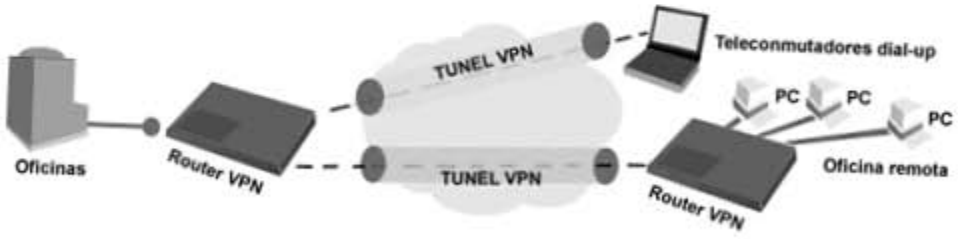

Figura 3.

3.2.1 Protocolos de comunicación en túneles

Para la creación de túnel existen tres diferentes tipos de protocolos:

- **Point to Point Tunneling Protocol (PPTP):** PPTP es una especificación de protocolo desarrollada por varias compañías. Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP. La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su fallo a elegir una única encriptación y autentificación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

- **Layer Two Tunneling Protocol (L2TP):** El principal competidor de PPTP en soluciones VPN fue L2F, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP. L2TP existe en el nivel de enlace del modelo OSI. L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

- **Internet Protocol Security (IPsec):** IPsec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec existe en el nivel de red en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet.
- **SOCKS Networks Security Protocol:** El sistema SOCKS proporciona otra alternativa a los protocolos de VPN. SOCKS se aloja en el nivel de sesión de OSI. Como SOCKS trabaja en un nivel OSI más alto que los protocolos anteriores, permite a los administradores limitar el tráfico VPN.

PPTP y L2PT pueden verificar el ID de un usuario y mezclar la información utilizando la criptografía básica, que encripta un archivo entero de una vez. Este nivel de seguridad es capaz de satisfacer a las necesidades de seguridad de cualquier empresa, pero la verdadera seguridad está dada por el IPSec que hace el proceso un poco más detallista, verificando y encriptando cada paquete de datos para asegurar una privacidad máxima.

IPsec es un conjunto de protocolos y algoritmos que nos permite garantizar comunicaciones seguras y privadas sobre redes IP, proporciona a los datos:

- *Integridad mediante los mecanismos de Hashing*
- *Confidencialidad aplicando el algoritmo de encriptación correspondiente*

- *Autenticidad mediante la Firma Digital*

3.2.2 Proceso de comunicación en las tecnologías de túneles

El túnel lleva datagramas entre PAC Y PNS. Muchas sesiones son multiplexadas sobre un mismo túnel.

PAC: (*PPTP ACCESS CONCENTRATOR*) Concentrador de acceso PPTP. Dispositivo que asocia una o más líneas capaces de soportar PPP (Point to Point Protocol) y manejo del protocolo PPTP. PAC necesita solamente TCP/IP para pasar sobre el tráfico de una o más PNS.

PNS: (*PPTP Network Server*) Es el servidor para red de PPTP. Sirve para operar sobre computadoras de propósito general y plataformas de servidores. PNS dirige la parte del servidor del protocolo PPTP mientras PPTP confía completamente TCP/IP y es independiente de la interfaz de Hardware, el PNS puede usar cualquier combinación de hardware de interfaz IP, incluyendo dispositivos LAN y WAN.

PPTP está implementado para PAC y PNS. Existen actualmente relacionados muchos PAC Y PNS, un PAC puede proveer servicio a muchos PNS. Por ejemplo un proveedor de servicio Internet puede elegir PPTP para un número de clientes de red privada y crear VPN's para ellos. Cada red privada podrá operar uno o más PNS's. Un PNS podrá asociarse con muchos PAC's para concentrar el tráfico desde muchos sitios de diferente ubicación Geográfica.

PPTP usa una forma parecida a GRE (*Generic Routing Encapsulation*) para llevar los paquetes PPP de usuario. Permite a bajo nivel controlar la congestión y flujo que va a llevarse a través de los túneles usados para llevar los datos de usuario entre PAC y PNS. Este mecanismo permite la eficiencia del uso del ancho de banda disponible para los túneles y evita retransmisiones innecesarias y desbordamiento en los buffers.

PPTP requiere el establecimiento de un túnel para cada comunicación PNS- PAC. Este túnel es usado para llevar todos los paquetes PPP de sesión de usuario participando un par determinado de PNS y PAC. Una llave está presente en el encabezado GRE indicando a cual sesión en particular pertenece el paquete PPP. De esta manera los paquetes PPP son multiplexados y demultiplexados sobre un túnel simple entre el PNS y PAC dado. El valor a usar en el campo de la llave es establecido por la llamada, estableciendo el procedimiento mediante el cual toma el control de la conexión.

El encabezado GRE también contiene la secuencia de información que ha sido usada para desempeñar algún nivel de control de congestión y detección de errores sobre el túnel. Luego la conexión de control es usada para determinar la tasa y los parámetros de almacenamiento temporal que han sido usados para regular el flujo de paquetes PPP para una sesión particular sobre el túnel.

3.3 SEGURIDAD

Definitivamente un punto que bajo cualquier contexto computacional, siempre resulta preponderante no importando la complejidad, llámese sistema o una red cualquiera que sean sus características. Veremos algunos puntos en materia de seguridad, que intervienen y están inmersos en los procesos de comunicación con el mundo exterior (Internet).

3.3.1 Algoritmos de Encriptación

La encriptación, protege a los datos durante su paso a través de redes IP ó redes públicas como Internet, de tal forma que si un intruso escucha esos datos le resulte ininteligible y que sólo sean claros para el destinatario al cual van dirigidos.

Los algoritmos de encriptación que se pueden emplear son:

DES (*Data Encryption Standard*)

- Usa una clave de 56 bits para encriptar datagramas de 64 bits.

3DES (*Triple Data Encryption Standard*)

- Se basa en DES, pues encripta los datos tres veces seguidas apoyándose en este algoritmo.
- Para encriptar puede utilizar dos claves distintas, obteniendo una clave de 112 bits ó tres claves distintas, obteniendo en este caso una clave de 168 bits.

Debido a que en los últimos años se ha producido una gran evolución en los PC's que existen en el mercado tanto en capacidad de procesamiento como de memoria, se dispone de máquinas muy poderosas que pueden llegar a vulnerar una clave DES, por lo que se están desarrollando nuevos algoritmos de encriptación como AES (Advanced Encryption Standard) que en los próximos años se convertirá en un algoritmo estándar de encriptación desplazando a DES.

3.3.2 Firmas Digitales

La Firma Digital, garantiza la identidad de los extremos durante su transporte sobre redes privadas IP ó públicas como Internet, es decir autentica la identidad de la persona que envía esos datos ó que los firma. Consiste en un mecanismo de intercambio de claves entre los dos extremos. Se utiliza una clave privada secreta para la generación de la firma y una clave pública para verificar en el otro extremo que esa persona es quien dice ser.

La Firma Digital suele ir ligada al concepto de compendio ya que aparte de garantizar la autenticidad de los extremos se asegura la integridad de los mismos en su paso a través de Internet ó de las redes privadas IP.

3.3.2.1 Algoritmos de Firma Digital

Los algoritmos de Firma Digital que existen son:

RSA (*Rivest, Shamir, Adelman*)

- Es el algoritmo de Firma más popular, puede ser utilizado tanto para firmar los datos como para encriptarlos aunque es mucho más lento que DES.

DSA (*Digital Signature Algorithm*)

- Es el algoritmo estándar de Firma Digital. Genera una clave de 512 ó 1024 bits por lo que es más lento que RSA.

Si el número de usuarios ó oficinas remotas que se tienen que autenticar aumenta considerablemente, la gestión de las claves se complica bastante; por lo que el mecanismo que se aconseja para autenticar los extremos son los Certificados Digitales en lugar de la Firma Digital.

CAPITULO 4.
ANALISIS DEL PROBLEMA

Hacia esta parte del documento, hemos visto el entorno en que se va a resolver este problema, así como el medio que se va utilizar para llevar a cabo la solución de este problema, ahora lo que se describe en este capitulo, es conocer de que manera se aplicará la tecnología antes mencionada conforme a nuestro actor principal, que es el hotel *Radisson Acapulco*, finalmente se conocerán de forma detallada como se encontraba el hotel y las nuevas necesidades que han surgido, todo esto en el ámbito informático.

4.1 Grupo Carlson

El objetivo de este análisis, como se ha mencionado anteriormente es, proporcionar una comunicación, desde Estados Unidos hacia el “Hotel Radisson Acapulco”, a través de un “túnel” en Internet, lo suficientemente estable y confiable para el desempeño de la LAN, que se va a implementar.

Considero importante, hacer mención que la parte a la cual nos vamos a enfocar, es a la resolución de la VPN por parte del “Hotel Radisson”.

CARLSON

(OMAHA, E.U.A)

Carlson es un conjunto de empresas que se fundo en el estado de Minneapolis, Minnesota, E.U.A., por el empresario Curtis L. Carlson (Julio 9, 1914-Febrero 19, 1999), el cual inicio con Gold Bond Stamp Company, y posteriormente fue expandiéndose, hasta lo que se conoce ahora.

Al grupo *Carlson*, tiene a su cargo diferentes empresas, como Hoteles, Cruceros, Restaurantes, etc. Estas oficinas se han ido colocando en distintas partes de Estados Unidos, y sus franquicias en distintas partes del mundo. Una de esas oficinas, que llamaremos Corporativo Carlson, el cual necesitan tener conexión permanente (o las veces que sea requerido).

El problema que se va a resolver, es respecto a la reservación de habitaciones, la cuestión aquí es que no se tiene un permanente refresco de la ocupación que se da en el Hotel Radisson Acapulco, desde el portal de Carlson (www.carlson.com) y esto refleja una deficiencia y al mismo tiempo, molestia de los clientes al tener que esperar un cierto tiempo, para poder saber si existen habitaciones disponibles.

La filosofía del grupo Carlson, siempre ha sido brindar un servicio de la más alta calidad en todas sus (“Socios”). Es por eso que la solución que se esta llevando a cabo conlleva grandes beneficios y

ahorro de costos. Debido a que, en esta ciudad se concentra la información de la mayor parte del grupo Carlson referente al hotel.

Por parte de Omaha, se tiene un enlace y un ruteador, el cual provee la infraestructura necesaria para poder realizar la VPN en cuestión; para efectos prácticos nos limitaremos a solo mencionar, las direcciones IP, con las que estaremos trabajando para realizar el túnel.

4.2 Hotel Radisson Acapulco

El Radisson es un lujoso hotel localizado en la exclusiva "Playa Guitarrón". Posee una espléndida vista de la bahía de Acapulco. Radisson Acapulco Resort, 4 estrellas. Este hotel ofrece a sus huéspedes la posibilidad de disfrutar de un confortable spa, gimnasio, diversión en sus albercas, así como una gran variedad de deportes acuáticos en su playa privada. 197 habitaciones con 15 hermosas suites distribuidas en 13 villas pequeñas. Todas las habitaciones están equipadas con teléfono, aire acondicionado, radio, TV vía satélite, minibar, balcones privados, vista al mar o al jardín, y habitaciones disponibles para discapacitados o no fumadores.

4.2.1 Necesidades del Hotel

Básicamente el hotel *Radisson* Acapulco, tiene que resolver un problema, el cual es, tener única y exclusivamente información disponible referente a la ocupación que presente el hotel, en determinado momento que llegue a ser requerida, en este caso, dicha petición será solicitada desde Omaha, la cual esta designada como, *Central Mundial de Reservaciones*.

El hotel cuenta con una propia red *interna*, la cual, permite estar en contacto con diferentes departamentos, algunos de ellos son : *Contabilidad, Recursos Humanos, Ventas, Compras, etc.,* cabe hacer notar, que la comunicación y funcionamiento que se da entre estas áreas, es independiente de la información que se va a manejar en el *túnel,* es decir la información de la parte administrativa del hotel, no es relevante para el enlace hacia la central que esta en Omaha, por esa razón no se entrará en detalles, sobre la organización y comportamiento del hotel.

4.2.2 Requerimientos del Grupo Carlson hacia el Hotel Radisson

El hotel Acapulco Radisson Resort, tiene ciertas especificaciones para poder realizar diversas tareas como son la realización de reservaciones principalmente vía web, la verificación del nivel de ocupación con que cuenta el hotel, así como de información adicional para el cliente acerca del hotel y los servicios que ofrece.

Para esta franquicia, el hotel debe contar con la infraestructura a nivel cómputo, necesaria para poder realizar todas las operaciones, como las antes mencionadas y muchas otras más.

El grupo Carlson le da al hotel Radisson Acapulco las especificaciones para poder soportar todos los servicios que ofrecen. Es por eso que a continuación se harán mención de los elementos que intervienen para llevar a acabo dichas operaciones.

- El hotel debe contar con un servidor, en el cual se le montara el sistema FIDELIO, siendo este el principal gestionador de la mayoría de las aplicaciones y tareas que el hotel necesitara realizar. A su vez este servidor fungirá como PDC (*Primary Domain Controller, Controlador de Dominio Primario*), el cual será capaz de administrar los demás servicios y aplicaciones con que cuenta la estructura Carlson. Así mismo será el servidor en donde se firmen los diferentes usuarios a las aplicaciones en las cuales, tengan los permisos necesarios.
- Otro elemento que se encuentra inmerso dentro de la solución integral que se esta manejando, es el sistema FIDELIO, este sistema esta enfocado a la administración de los hoteles, por lo cual es común encontrarlos en la mayoría de ellos. FIDELIO de entre sus múltiples características, permite un control eficiente de los usuarios que tienen permitidos ciertos servicios, así como un monitoreo de los mismos. También permite una interacción a cerca de las operaciones del área de Recepción, Ama de Llaves, Reservaciones, entre otras.
- Otro de los requerimientos del Grupo Carlson, es la estación de trabajo HDBM, esta estación de trabajo es enviada por el Grupo Carlson, como requisito indispensable para el funcionamiento de la franquicia, este llega al hotel, debidamente configurado. Básicamente el funcionamiento de esta estación de trabajo, permite una administración y monitoreo de las reservaciones que se lleven a cabo en sitio, así como las que se realicen vía la WWW.

- También existe una estación de trabajo llamada INTERFASES, la cual permitirá a la red del hotel, conectarse tanto al conmutador general del hotel (específicamente el tarificador de llamadas), como al servidor con la aplicación MICROS. La función de esta estación de trabajo es la traducción de ambas aplicaciones antes mencionadas con el sistema FIDELIO.

4.2.3 Soluciones

En el momento en que se pretende atacar un problema, de esta naturaleza, suelen surgir un sin número de opciones, por supuesto cada una con sus características y limitantes debidamente definidas, por ende, empezamos un proceso de evaluación de las distintas tecnologías, analizando así, sus principales ventajas y los inconvenientes que estas pudieran presentar.

Como se da en todos los casos, cada empresa decide que tipo de recursos destinará para sus soluciones de comunicación. Aunque en la mayoría de los casos, siempre se verá limitada por el presupuesto de cada compañía. Por supuesto no es el único factor que interviene en el análisis y toma de decisiones, para determinar que tecnología es la que se manejará, que componentes son requeridos, la información que se va a manejar, la cuestión geográfica es muy importante, tanto como el personal que deberá estar a cargo para el funcionamiento óptimo de la integración de los puntos antes mencionados.

Existen diferentes tecnologías, que pueden satisfacer, la necesidad de enlazarnos hacia prácticamente cualquier parte del mundo. Aunque definitivamente no todas se ajusten o tengamos al alcance. De entre las soluciones que podemos emplear para solucionar esto, tenemos las siguientes:

Existen los enlaces de baja velocidad: dicho de otra manera los enlaces más convencionales, ya que es el acceso a la red de redes, de la mayoría de las personas que trabajan en casa, con esto no pretendo afirmar que es la única forma que se pueda utilizar, para llevar a cabo dicha conexión. Al primero que me estoy refiriendo y que aun es utilizado por muchas compañías para realizar algún tipo de transferencia, es al acceso por Dial Up, que son las cuentas que contratamos con el proveedor 'X' de Internet y que a demás nos venden la velocidad de navegación de 56K, que ya es sabido que es falso. Aunque el propósito de esto no es analizar las velocidades de conexión. Volviendo a las diferentes de conectarnos, muy probablemente nuestro proveedor 'X' tiene otra opciones de conexión, dependiendo de que tantas necesidades tengamos, ahora bien, no solo aplica a nuestro hogar, en ya la mayoría de los negocios se esta integrando este tipo de servicios. Como un ejemplo de este servicio serian las líneas DSL con velocidades desde los 64 Kbps. Otra opción que esta al alcance es el Cable MODEM.

Tenemos los enlaces digitales y de alta velocidad: Como los, Enlaces DS0, DS1, DS3, E1, E3, T1, T2, T3., por mencionar algunos. Los cuales nos permiten diferentes capacidades de *Upstream* y

Downstream (el termino *upstream* se le denomina a la transmisión que se realiza desde un usuario final, hacia un servidor; y *downstream* se refiere a la transmisión desde un servidor, hacia un usuario final), brindando como resultado, la posibilidad de montar sobre estos enlaces, múltiples servicios digitales, los cuales nos darán un uso eficiente del tiempo y la información que necesitemos transmitir. Este tipo de tecnología muy probablemente ya la podamos adquirir en nuestro ISP más cercano o con la compañía telefónica de nuestra elección, definitivamente esta decisión dependerá de las necesidades reales que como empresa u hogar tengamos y que a su vez este ISP nos pueda ofrecer.

.

CUADRO COMPARATIVO DE LOS DIFERENTES ENLACES DEDICADOS

Cuadro (a)

ENLACE	***VELOCIDAD***	***CARACTERÍSTICAS*** (*Canales Digitales*)
E0	64 Kbps [1]	Es utilizado para referirse a los canales de ISDN de 64 Kbps en estándar americano.
E1	2.048 Mbps [5]	Es utilizado principalmente para la transmisión de datos.
E3 (Sin Descanalizar)	34.368 Mbps [2]	Canal de comunicación digital para datos.
E3 (Descanalizado)	2.048 Mbps [6]	Canal de comunicación digital para datos.
T1	1.54 Mbps [3] Estándar en E.U.A, 24 canales digitales	Velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 1.54 Mbps a través de una red telefónica.
T2	6.32 Mbps [7]	Línea digital interna de las compañías telefónicas que no se ofrecen a las empresas privadas.
T3	44.736 Mbps [7]	Línea de transmisión de datos utilizada en Internet. (Requiere de Fibra Óptica)
T4	274,176 Mbps [7]	Principalmente utilizada en E.U.A.
DS0	64 Kbps [4]	Enlace de comunicación dedicado sencillo.
DS1	1.544 Mbps [8]	Canal de comunicación digital de señal tipo 1; puede ser E1 de 1.44 Mbps en Estados Unidos o T1 de 2.108 Mbps en el estándar Europeo.
DS2	6.31 Mbps [8]	Un enlace DS2, se vale de 96 canales por Codificación de Modulación de Pulso, utilizada principalmente para voz.
DS3 (Sin Descanalizar)	44.736 Mbps [6]	Canal de comunicación digital de señal tipo 3, se utiliza en líneas T3 de ISDN.
DS3 (Descanalizado)	2.048 Mbps [6]	Canal de comunicación digital de señal tipo 3.
DS4	274.1 Mbps [8]	Canal de comunicación digital de señal tipo 4, de 274 Mbps en el estándar de Bell.

[1] Fuente : http://www.cft.gob.mx/cofetel/html/4_tar/metrored/metrored1.shtml
[2] Fuente : http://www.cft.gob.mx/cofetel/html/4_tar/telereunion/capitulo01.shtml
[3] Fuente : http://www.pcta.com/about/glossary.php?page=t

El cuadro anterior, muestra los enlaces dedicados frecuentemente utilizados por las empresas, como se puede apreciar, existe diferencia entre estos enlaces, y van desde velocidad, costo, objetivos más concretos y países en los que son utilizados.

De estos enlaces, se pusieron bajo propuesta, los que cubrieran la funcionalidad, en la cual radica el problema. Pero desafortunadamente, otro de los factores primordiales es, disminuir costos.

Es por eso que los directivos del hotel descartaron estas soluciones, para poder dar paso a la implantación sobre Internet. Se plantearon y analizaron diversas posibilidades para la solución de conectividad entre los dos puntos y finalmente se opto bajo el esquema de disminución costos que lo mas viable era “viajar” por Internet tomando en cuenta los diferentes riesgos y delimitando perfectamente el factor vulnerabilidad en la información.

4.3 Designación de Dispositivos

Por otra parte, se harán notorias tres etapas por las que pasa el hotel, debido a cambios y nuevos requerimientos en la nueva administración.

En un principio el hotel en el cual se ha desarrollado esta solución de conexión remota, no contaba con la infraestructura necesaria, debido a que el nombre del hotel y por ende la

[4] Fuente : http://es.wikipedia.org/wiki/T-carrier

administración era completamente diferente, este vistazo que se pretende dar, es con relación a la tecnología y sistemas que se estén manejando en su momento, para satisfacer las necesidades en cuestión de comunicación que exista entre el hotel y el exterior.

4.3.1 Condiciones iniciales del Hotel Radisson

Haciendo un poco de historia, trataré de dar un panorama en general, sobre las características con las que contaba el hotel (en su franquicia inicial) en aquellos momentos. Podemos mencionar que:

- El hotel manejaba sus operaciones de administración de cuartos con un servidor Unisys bajo plataforma UNIX, y corriendo una aplicación en cobol.
- Controlaba sus operaciones de Restaurante con el sistema MICROS.
- También contaba con una aplicación llamada AVANTE para el sistema contable.
- Así mismo, poseía un tarificador el cual ejercía un control sobre las llamadas realizadas.
- Tenía conexiones tipo interfase serial para la conexión de las estaciones de trabajo.

De manera muy somera, estas eran las principales características con las que contaba el hotel. Posteriormente se lleva a cabo el establecimiento de la nueva franquicia (Radisson Acapulco).

En la transición que se realiza, se diseña una nueva propuesta, la cual incluye una nueva estructura y nuevos lineamientos que se tendrán que seguir a partir de esta nueva etapa.

4.3.2 Planteamiento de una nueva propuesta

Para este momento, la franquicia tiene asignados los nuevos requerimientos a los que se tendrá que apegar para el desempeño adecuado de las labores del hotel, esto en materia de comunicación. Como se ha mencionado anteriormente, en el acondicionamiento de nuevas tareas y procesos que se deben llevar a cabo, es necesario tener las herramientas necesarias, en este caso, tanto en *Hardware* como en *Software*. Algunas herramientas se pudieron integrar a la solución que en ese momento se estaba planteando.

- Se continúo utilizando el sistema MICROS, para las operaciones de los restaurantes.
- Así mismo se siguió utilizando la aplicación llamada AVANTE para el sistema contable.
- También se mantuvo funcionado el *Call* (Tarificador).
- Se solicitan los servicios de la aplicación FIDELIO, que puede correr en cualquier estación de trabajo, para dicho evento se envía una petición al servidor que contiene FIDELIO, el cual es un Servidor Compaq Proliant, más adelante se detallará, sobre estos componentes.

- Otro elemento importante en la solución, es la estación de trabajo HDBM, la cual se encarga de gestionar el nivel de ocupación, ya sea vía Web o de manera local.
- Se cuenta con la estación de trabajo INTERFACES, la cual tiene una tarjeta de emulación del puerto RS232, a la cual se le agrega un conector llamado “Pulpo”, el cual posee 8 conectores RS232 y por medio de este conector, la estación de trabajo INTERFACES controla el flujo de información del *Tarificador*, MICROS y AVANTE con el sistema de administración hotelera FIDELIO.

Es importante hacer mención que el Grupo Carlson, ha designado un segmento de red, para que el Hotel, pueda designar a los respectivos dispositivos, las IP’s correspondientes y así tener el acceso y los permisos pertinentes.

4.3.3 Situación Actual (DESEADA)

Actualmente el hotel, cuenta con los dispositivos antes mencionados, solo que se ha agregado una característica más, a parte de que existe la necesidad de tener información de reservaciones, siendo esta accesada vía remota. Este último requerimiento, es el principal objetivo de este estudio.

- Se continúo utilizando el sistema MICROS, para las operaciones de los restaurantes.
- Así mismo se siguió utilizando la aplicación llamada AVANTE para el sistema contable.

- También se mantuvo funcionado el *Call* (Tarificador), el cual trabaja en conjunción con el *Conmutador*.
- Se mantienen funcionando los servicios de la aplicación FIDELIO, que puede correr en cualquier estación de trabajo.
- Otro elemento importante en la solución, es la interfaz HDBM, esta cuenta con una aplicación llamada CURTIS, la cual se encarga de gestionar el nivel de ocupación, ya sea vía Web o de manera local.
- Se cuenta con la misma estación de trabajo INTERFASES.
- Se incorpora en esta solución el servidor MAIN, que viene a actuar como Primary Domain Controller, al mismo tiempo se configura, el servidor FIDELIO para que sea Backup Domain Controller.

Con la adición de este dispositivo, se podrán controlar los accesos a los diferentes departamentos, así como se tendrá más confiabilidad en los datos, debido a que el servidor MAIN se encargara de administrar los Usuarios, y si existiera algún problema, se contaría con un respaldo.

CAPITULO 5
CONEXIÓN OMAHA – ACAPULCO

Ya conocimos tanto las condiciones iniciales de la infraestructura informática del Hotel Radisson Acapulco al inicio de este análisis, como los lineamientos, normatividad y equipamiento sugeridos por el grupo Carlson, así como las adquisiciones que el Hotel Radisson Acapulco realizó en miras a su preparación para la fusión de las operaciones a la normatividad de grupo Carlson.

Continuaré, ahora, con la parte de implementación de la solución encontrada para realizar:

1.-Conexión de la red bajo la trama de Ethernet (al 100%)
2.- Levantar dos servidores bajo la tecnología Windows 2000 server
3.- Configuración de un PDC y un BDC
4.- Conexión a Internet y compartirla a toda la trama Ethernet
5.- Dar de alta los servicios de ruteo en el Contivity 100 de Nortel Networks
6.- Levantar el túnel para la comunicación entre Omaha-Acapulco y así poder alcanzar todos los objetivos trazados en este proyecto.

5.1 Equipo Activo

Independientemente de la importancia que existe en la elección del hardware, tanto en el equipo de cómputo como en el equipo activo, es este segundo él que tendrá la responsabilidad de encargarse de la transferencia de datos entre los dos sites (Omaha-Acapulco). Es por eso, que grupo Carlson manda un router VPN modelo Contivity 100 de

la marca Nortel Network, el cual es por normatividad del grupo, el equipo que se utiliza en cada uno de los hoteles de la cadena.

Como parte de la “receta” que el grupo Carlson tiene cocinada para este tipo de conexiones, esta la contratación de una línea dedicada internacional (en este caso, por obvias razones) con la compañía MCI, socio tecnológico de grupo Carlson. Al igual que Nortel Network (por el lado de ruteo), MCI (en cuestión de enlaces dedicados) provee de la señal necesaria y acceso al Internet actualmente (ya que anteriormente, solo suministraba señal directa al enlace dedicado, subiendo los costos de manera dramática) para que se pueda realizar una VPN entre Acapulco y Omaha.

Realizaré el análisis del equipo activo en dos partes, ***la parte de la red de área local*** del Hotel Radisson Acapulco, y por otra parte, el equipo necesario para ***la conexión a Omaha***, tanto el ruteador VPN, como el equipo utilizado para el servicio de Internet.

En la parte de ***la red de área local***, se cuentan solo con switches de la marca 3Com, uno que es administrable (SuperStack 3 Switch 3300 TM), el cual nos servirá para nombrarlo MainSwitch, el switch que controla a toda la red de área local. Este switch cuenta con un puerto Gigabit, pero para nuestros efectos, no será necesario utilizarlo, ya que los switches restantes (3 SuperStack 3 Switch no administrables) se encargaran de la parte horizontal del cableado, mientras que la conexión del backbone dependerá exclusivamente del MainSwitch.

DIAGRAMA FISICO DE LA RED DEL HOTEL
RADISSON ACAPULCO

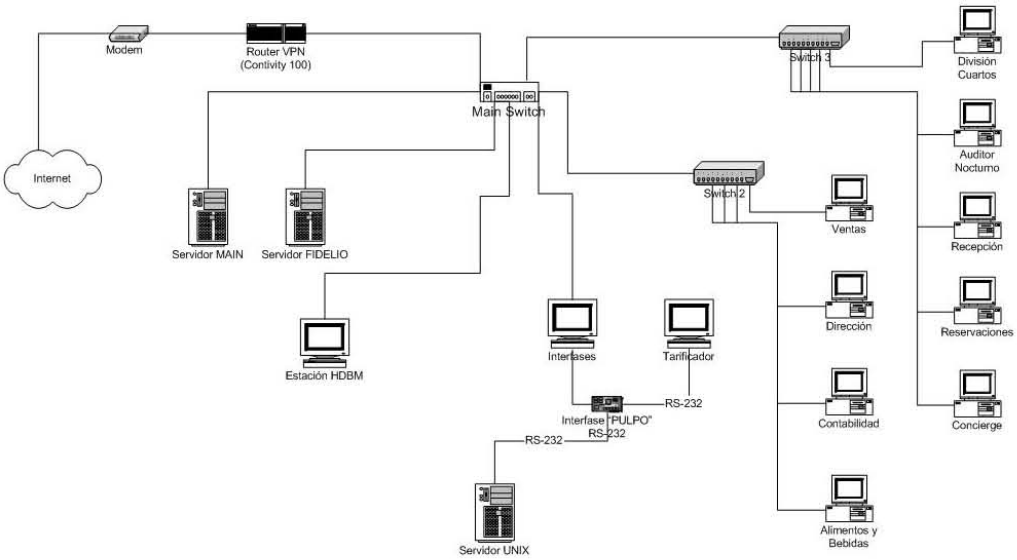

Figura 4.

5.2 Implementando la Propuesta

En la conexión del backbone, se conectan los diferentes Switches secundarios (los que proporcionan servicio al cableado horizontal) al MainSwitch, además el equipo que tiene que estar de primera mano al core, como servidores, estaciones de trabajo de propósito específico (estación de trabajo HDBM, Interfaces, etc.) y ruteadores.

Aquí nos encontramos con la primera diferencia del modelo tradicional del grupo Carlson con respecto a los demás hoteles de la

cadena, en referencia a la topología, segmentos de red y diseño lógico del tramado Ethernet utilizados.

Dos aspectos importantes de esta variación, *los servidores y la segmentación de la red*. Normalmente, se deja solo un servidor (él cual lleva por nombre FIDELIO, y es el PDC), en donde se montan las aplicaciones de MICROS FIDELIO, software de administración y seguimiento del control del hotel (en el se llevan la relación de cuartos, su ocupación, módulos de ama de llaves, reservaciones, recepción, etc.), todo esto montado sobre un sistema operativo de red Windows 2000 server en versión de idioma ingles (ya que los técnicos de Omaha no hablan español). Por lo que respecta al segmento de red, el grupo Carlson asigna un grupo de direcciones de su segmento 172.29.0.0 (de la 172.29.245.128 a la 172.29.245.157 dándonos un total de 30 direcciones IP) esto para que el servidor FIDELIO, y las estaciones de trabajo de administración como INTERFASES y HDBM puedan ser vistos de forma natural por ellos, al igual que las estaciones de trabajo de recepción y reservaciones. Como generalmente los franquiciarios no montan mucha infraestructura informática, a diferencia de este caso en particular, en donde la infraestructura informática es mucho mayor.

Continuando con ***la parte de la red de área local,*** y regresando al funcionamiento de los switches secundarios, estos se dividen en y le dan servicios a los diferentes departamentos de la siguiente manera:

Switch no. 1:

- Dirección

- Ventas
- Contabilidad
- Alimentos y Bebidas
- Grupos y Convenciones

Switch no. 2:

- Reservaciones
- Recepción
- Auditoria Nocturna
- División Cuartos
- Concierge

Switch no. 3:

- Recursos Humanos
- Chef
- Compras
- Ama de Llaves
- Almacén
- Atención proveedores
- Seguridad

Por consiguiente, tenemos los tres primeros puertos del MainSwitch ocupados con estas conexiones de los switches secundarios, más la conexión de los dos servidores *Compaq Proliant*, uno para montar a la aplicación FIDELIO con sistema operativo windows 2000 server en ingles y dejándolo como BDC (es el server con el cual interactuarán la gente de soporte técnico del grupo Carlson) y el otro para el servidor *Compaq Proliant* identificado como MainServer con sistema operativo windows 2000 server en español (este servidor

tendrá toda la configuración de seguridad de usuarios que necesita el grupo Carlson, más las directivas que el franquiciario guste añadir). Tres puertos más ocupados, dos para los equipos de estación de trabajo administrativa, la HDBM, equipo proporcionado por grupo Carlson, corriendo windows NT-Workstation 4.0 en ingles, la aplicación CURTIS, necesaria para la administración y auditoria remota, además de llevar el control de reservaciones mundiales del grupo Carlson; y el otro es utilizado para el equipo para la administración y el monitoreo de la red. Quedan los puertos disponibles para la conexión del ruteador, Internet, etc.

Es necesario hacer notar que la modificación que se realizó para este proyecto, llevó al Hotel a cambiar al 100% su tendido de red, ya que solo se contaba con una incipiente red de datos vía RS-232 con terminales tontas en recepción, auditoria nocturna, división cuartos, ama de llaves y las terminales de punto de venta en los centros de consumo. El hotel decidió no quitar dicha infraestructura y se monto la nueva infraestructura tomando en cuenta a la ya existente, como se puede apreciar en el diagrama físico de la red.

Al analizar la parte de ***la conexión a Omaha,*** nos encontramos que con relación al equipo activo de la red, estamos utilizando el MainSwitch, y los switches secundarios 1 y 2. Aquí es donde la parte medular del equipo activo será colocada, me refiero al ruteador Contivity 100 VPN de NortelNetworks, el cual deberá tener una señal de Internet directamente a él, así como se tendrá que conectar a la red de área local del hotel.

A continuación, veremos los porque de las adecuaciones y cambios a la receta general de grupo Carlson, y las reacciones del personal técnico al planteamiento del Hotel a esta situación.

5.2.1 Conexión de la Red Bajo la Trama de Ethernet (AL 100%)

Ya vimos que la red de área local tiene dos tramas, la trama Ethernet (nueva, en Cat 5e) y la trama RS-232 – ver diagrama físico de red – la cual nos sirve para poder seguir teniendo comunicación con las terminales de punto de venta de los centros de consumo, sistema que se encuentra residente en un servidor Unix (sistema MICROS de punto de venta).

Se tenía planeado montar una tarjeta de red al servidor Unix, para así tener una segunda opción de comunicación, y no solo tener comunicación por la trama RS-232 para los equipos del departamento de contabilidad que realizan accesos a este servidor, pero a la conclusión de este documento, no se había implementado dicha situación.

Como se comentó anteriormente, el grupo Carlson designa 30 direcciones IP para la operación de la parte de control del hotel en el aspecto de reservaciones, recepción, facturación y atención de los huéspedes. El hotel actualmente cuenta con 56 equipos (todos con conexión a la red de área local) y pretende crecer su infraestructura computacional a 20 equipos más al finalizar el 2003. Es por esta razón, que se piensa en comprar dos servidores (en lugar de uno que requería

el grupo Carlson) y en segmentar la trama Ethernet a dos segmentos de red.

¿Qué fue lo que paso? ¿Por que este cambio? ¿En verdad se mejoró a la propuesta original?

Lo primero que vemos es que 30 direcciones no eran suficientes para el hotel, el grupo Carlson no podía dar más direcciones IP al segmento que estaba proporcionándole al hotel, así que nos vemos en la necesidad de utilizar otro segmento de red. Ahora bien, con respecto a los servidores, de primera instancia se pensó en adquirir los dos para utilizar uno de espejo (respetando la propuesta original del grupo Carlson), pero a la necesidad naciente de un segmento de red, se pensó en tener un servidor primario controlando los servicios de red y un segundo servidor asignado a dar servicio a la aplicación que se estaba por montar (MICROS FIDELIO). Desde el primer momento, el personal técnico de MICROS FIDELIO les gusto la propuesta, claro, no dejando de hacer algunas observaciones de la interrelación entre el sistema operativo de red y el sistema mismo, de esto hablaremos con más profundidad en los puntos 4.2.2 y 4.2.3.

Con respecto a la trama Ethernet y a la utilización de dos segmentos de red con diferente IP (por dos razones, la fácil identificación de los segmentos, y la necesidad de utilizar el segmento proporcionado por el grupo Carlson), nos lleva a utilizar dos tarjetas de red en cada uno de los servidores, por definición del grupo Carlson, el servidor donde se encuentra la aplicación debe llamarse FIDELIO (luego veremos la importancia de esto en el apartado 4.2.2), además debe tener la

dirección IP 172.29.245.146 (asignada a una de las dos tarjetas de red) que llamaremos IP del segmento Carlson o Ethernet 1. Las demás direcciones IP del segmento Carlson son:

- HDBM 172.29.245.145
- INTERFACES 172.29.245.147
- Recepción de la 172.29.245.148 a la 172.29.245.157 vía DHCP
- Reservaciones de la 172.29.245.148 a la 172.29.245.157 vía DHCP
- Libres de la 172.29.245.128 a la 172.29.245.143
- Router VPN 172.29.245.144

El otro segmento de red, el cual le dará servicio al resto de la red local, lo llamaremos segmento Acapulco, es el que utilizaremos para compartir Internet con toda la red (en sus dos segmentos), así como poder ver al servidor FIDELIO pero por la segunda tarjeta de red, la cual será conocida como Ethernet 0.

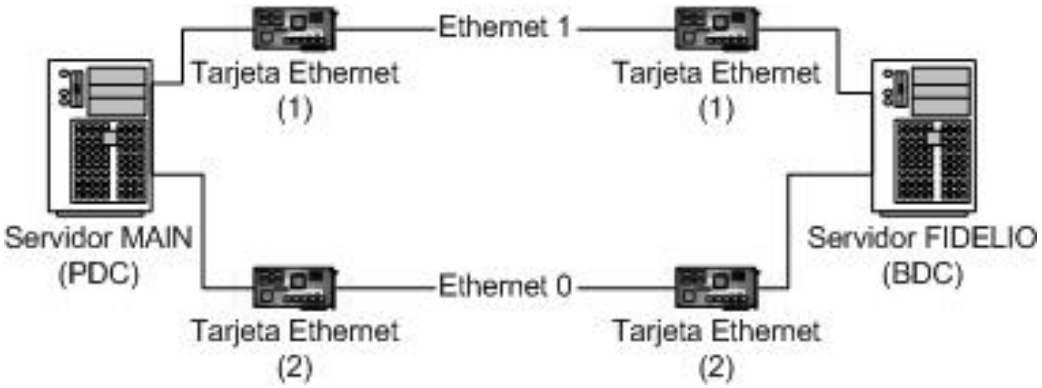

Figura 5.

Debido a que existe una tarjeta de red en el servidor FIDELIO con una IP del segmento Acapulco (Ethernet 0), todo aquel equipo que necesite correr la aplicación de MICROS FIDELIO y que se encuentre en dicho segmento, lo podrá ejecutar sin problemas. Aunque la estación de trabajo se firma al servidor MAIN, en él existen los permisos y los script (archivo en cual están contenidas las rutas, para el acceso de las carpetas correspondientes a dicha aplicación) de conexión a unidades de red remotas. Una mejora sustancial de este nuevo esquema en relación con la propuesta inicial del grupo Carlson, es que en caso de que tengamos alguna falla en el servidor MAIN, el servidor FIDELIO, por ser un BDC, puede firmar a los usuarios a la red y seguir dándole el servicio de la aplicación MICROS FIDELIO hasta que el servidor MAIN vuelva a ser levantado.

¿Qué ganamos con esto? Bueno, en el esquema original, si tengo un problema con el servidor por servicios de red, me voy para abajo, el dar de baja el servidor (inclusive, solo para reiniciar) me obliga a suspender el servicio de la aplicación por un tiempo. Mientras que en este esquema final, no importa si necesitas reiniciar al servidor MAIN para lo que sea, toda estación de trabajo que este firmada a la red y trabajando con la aplicación MICROS FIDELIO, seguirá trabajando aun y cuando el servidor MAIN ya no se encuentre arriba. Como estamos hablando del mismo segmento de red, la estación de trabajo, la cual leyó un *script* de enrutamiento de unidades de red direccionadas al servidor FIDELIO, sigue teniendo comunicación con dicho servidor, y no importa que salga de la aplicación, podrá volver a entrar a ella cuantas veces quiera, siempre y cuando no termine su sesión de red. Ahora, si estando el

servidor MAIN abajo, una estación de trabajo desea entrar, el servidor FIDELIO por ser BDC le da acceso al dominio, además contiene un script de enrutamiento de unidades de red, pero en a diferencia del script en el servidor MAIN, este apunto a su disco duro local (el aplicativo MICROS FIDELIO, necesita que las estaciones de trabajo direccionen a sus diferentes carpetas de trabajo vía unidades de red lógicas).

Concluimos que:

- Un segmento de red en Clase B (Ethernet 1) con 30 IP preasignadas
- Un segmento de red en Clase C (Ethernet 0) con 254 IP para ser usadas por el hotel
- Dos servidores con conexiones a ambos segmentos
- Ethernet 1 para grupo Carlson y para la conexión VPN
- Ethernet 0 para el resto del hotel y sus diferentes departamentos

5.2.2 Levantar Dos Servidores bajo tecnología WIN 2000 SERVER

Dentro de la normatividad de grupo Carlson, el servidor FIDELIO (el que corre a aplicación MICROS FIDELIO) debe ser instalado bajo el sistema operativo windows 2000 server en su versión en ingles. Esto se debe a que como parte del soporte técnico de grupo Carlson, y gracias a la VPN entre Omaha y Acapulco, los técnicos de grupo Carlson puedan moverse a través de las diferentes máquinas del segmento Carlson (Ethernet 1) sin la necesidad de estar traduciendo de

otro idioma que no sea su idioma nativo. De hecho, todo el equipo que se instala en el segmento Carlson, deberá estar con su sistema operativo y sus aplicaciones en versiones en ingles.

En nuestro caso, se le da seguimiento a la normatividad del grupo Carlson, solo que el servidor MAIN se instala con una versión en español del windows 2000 server.

Los equipos HDBM, INTERFASES, las estaciones de trabajo de recepción y las de reservaciones, se les instalo el sistema operativo en versión inglesa.

Como la instalación del sistema operativo Windows 2000 Server, ya sea en su versión en español o en ingles no es el motivo de este estudio, solo listaré los parámetros necesarios para su correcta instalación.

- Un servidor de dominio (MAIN)
- Un servidor de respaldo
- Solo protocolo TCP/IP en las interfaces de red
- El PDC corriendo servicios de DHCP
- Un BDC corriendo la aplicación principal
- Base de usuarios bajo norma Carlson
- Usuarios adicionales bajo criterio de Acapulco

Además del idioma utilizado en cada uno de los servidores, el otro aspecto importante a resaltar son las interfaces de red que se montan en cada uno de ellos. Como se explicó con antelación, en el servidor FIDELIO se colocaron dos tarjetas de red, una se configura en la clase B asignada por grupo Carlson (172.29.245.146/16) y la otra en la clase C de uso exclusivo de Acapulco (X.X.X.2/24), y solo se levanta el protocolo de comunicación TCP/IP para cada una de las interfaces. De la misma manera, el servidor MAIN lleva dos tarjetas de red, la que se le asigna una IP de la clase B, la cual se tomo de una de las IP libres de la normatividad de grupo Carlson (172.29.245.143/16) y la otra en la clase C (X.X.X.1/24).

5.2.3 Configuración de un PDC y un BDC

Como parte de la normatividad de grupo Carlson, no esta contemplado el esquema de un servidor como BDC (Backup Domain Controller). Pero para efecto de nuestro caso, lo tomaremos en cuenta para poder beneficiarnos de él y así poder tener un esquema más sólido de acceso para la red.

Aquí el por que; en el esquema original de grupo Carlson, el servidor FIDELIO es configurado como un PDC (Primary Domain Controller) él cual se encarga tanto de levantar los servicio de red, así como la interacción de la aplicación MICROS FIDELIO. En nuestro esquema, el servidor FIDELIO será un BDC del dominio del hotel (por cierto, el nombre del dominio es también propuesto por grupo Carlson, RDACMX) y nuestro servidor MAIN (anexado para esta propuesta) será el PDC.

Ya tenemos más elementos para analizar. Primero el servidor MAIN, con sistema operativo en español (ya que no se necesitará el soporte técnico en este servidor, una vez que este dada de alta la base de datos de usuarios y sus características) y encargándose de todos los servicios de red, en él, se quiso levantar el servicio de DHCP para la parte de estaciones de trabajo en el segmento Carlson, solo que se decidió montar dicho servicio en el servidor FIDELIO. En segundo lugar, el servidor FIDELIO, como BDC, cuenta con la copia de usuarios, permisos y relaciones de confianza del resto de la red, corre el aplicativo MICROS FIDELIO, y da servicios de DHCP a las diferentes estaciones de trabajo que están así consideradas en el esquema original de grupo Carlson (recepción y reservaciones), se monto el servicio de DHCP en este servidor por que es el que esta en ingles y solo equipos del segmento Carlson necesitarán este servicio, así que los técnicos de necesiten hacer cualquier verificación, solo estarán interactuando con equipo en su idioma.

Hagamos un paréntesis para explicar que para poder trabajar con el aplicativo MICROS FIDELIO, es necesario que la estación de trabajo tenga las rutas o asignaciones de las carpetas de trabajo en el servidor (script). Esto no es otra cosa más que conectar a unidades remotas (en el servidor) y asignarle una letra para trabajar como otro disco duro de manera local. Cada servidor contiene un archivo *script* con el mismo nombre, el cual me garantiza que siempre habrá un *script* disponible para leer, en caso que el PDC no se encuentre disponible, el BDC firmará a la estación de trabajo y tendrá disponible un script para enrutar las unidades remotas. Cada estación de trabajo cuenta con un

archivo en lote dentro de su *autoexec.bat* el cual contiene la instrucción de leer el script dependiendo cual servidor este presente (si esta presente el MAIN, lo carga desde la ubicación de él, de no estar presente, lo carga de FIDELIO).

La parte más interesante de esta combinación entre PDC y BDC, es que:

Caso no.1 Firmándose a la red, con PDC arriba: cualquier estación de trabajo, ya sea del segmento Carlson o del segmento Acapulco, se firma vía PDC, y el enrutamiento lo realizan vía un *script* existente en el directorio raíz del servidor MAIN, el equipo entonces conoce a las carpetas referenciadas del servidor FIDELIO y entonces se puede utilizar el aplicativo MICROS FIDELIO. A esto lo conoceremos como *login* Normal.

Caso no.2 Login Normal, y ya en el aplicativo, PDC se cae: Me he firmado de manera normal y logré entrar al aplicativo MICROS FIDELIO, ya trabajando en él, el PDC por *X* motivo se cae, gracias al esquema implementado, la estación de trabajo sigue sin problemas conectada al servidor FIDELIO aún sin el MAIN arriba.

Caso no.3 Login Normal vía PDC, ya en el aplicativo (MICROS), salir del aplicativo y volver a entrar (PDC abajo): Una vez que se ha firmado la estación de trabajo de manera normal (por PDC) al sistema operativo, y se hace uso del aplicativo (MICROS), y en un lapso "*X*" de tiempo el PDC falla y se requiere salir del mismo, al

momento que deseemos utilizar nuevamente el aplicativo, no se tendrá ningún problema, debido a que la estación de trabajo, ejecutara el *script* que automáticamente le brindará el acceso, a las unidades lógicas del servidor de respaldo (BDC), dando como resultado que el usuario no se percate de dicho movimiento.

Caso no.4 Login Normal vía PDC, ya en el aplicativo (MICROS), salir del aplicativo y volver a entrar, salir de la red y realizar un relogin (PDC abajo): Tomando como referencia el caso anterior, en donde se explica una serie de entradas y salidas del aplicativo, para este caso, existe una variante que es la de salir de la red (terminar la sesión) y posteriormente hacer un relogin de la estación de trabajo, y en estos momentos falla el PDC, cuando sucede esto, la estación de trabajo, buscará el *script* que se encuentra en el servidor BDC, debido a que el servidor MAIN (PDC) se encuentra fuera de servicio, una vez hecho lo anterior, la estación de trabajo continuara funcionando de manera normal, sin necesidad de que PDC este funcionando.

Caso no.5 Login a la red, cuando PDC se encuentra fuera de servicio: Este proceso, se lleva a cabo de manera normal, es decir, al estar la estación de trabajo en su proceso de inicialización, detecta que esta fuera de servicio el PDC, y va a leer el *script* que se encuentra en BDC, procede a realizar un login con el BDC con su respectivo nombre de usuario y password, y el BDC comprobará y proporcionará los servicios y permisos que tenga asignados dicho usuario, para posteriormente trabajar con el aplicativo (MICROS) de forma local, si

así lo requisitaza el usuario, cabe destacar que el script ya no se ve obligado a ‘conectarse’ a las unidades lógicas, debido a que se encuentra inicializado en el servidor.

Caso no.6 BDC se encuentra fuera de servicio: Este escenario sería una excepción y al mismo tiempo representaría perdidas en muchos aspectos, ya que se estarían deteniendo prácticamente todas las operaciones del hotel, para poder resolver esto, será necesario levantar un servidor de respaldo con las mismas características del BDC, y posteriormente ponerlo en funcionamiento.

5.2.4 Conexión a Internet y compartir a la trama Ethernet

En un primer paso, y con lo que respecta a la conexión a Internet, se ha seleccionado como proveedor del servicio a Telmex, con su servicio Prodigy Infinitum de 512 Kbps en la modalidad de direccionamiento de IP estática, proporcionando al hotel un equipo de modem DSL/ROUTER. Este equipo tiene la facilidad o ventaja de proporcionar un servicio de DHCP, liberando así al servidor MAIN de un servicio más levantado y administrado por él. Esto, en el sentido de dar a los equipos del hotel que no entran directamente en la trama o segmento de grupo Carlson el acceso a Internet, y a su ves, tener acceso a la aplicación FIDELIO.

Ahora bien, ya tenemos resuelto la primera parte, el segmento del hotel, la trama ethernet X.X.X.0/24 ya cuenta con salida a Internet, utilizando como puerta de salida predeterminada la IP del modem DSL/ROUTER, la cual cuenta con parte de su segmento con

direcciones IP estáticas (como la X.X.X.1 y la X.X.X.2 correspondientes a los servidores MAIN y FIDELIO respectivamente, así como la destinada a la IP de la compuerta de salida) y con direcciones dinámicas.

Tenemos entonces que el segmento del grupo Carlson por el momento no tiene salida, esto debido a que la IP de la compuerta de salida predeterminada no se encuentra en el mismo segmento que Carlson.

Lo siguiente es conectar el modem DSL/ROUTER al Contivity 100 para que él se encargue de recibir la conexión a Internet y administrarla (poder crear el túnel entre Omaha-Acapulco), para ello existen dos conectores de puerto ethernet en la parte trasera del Contivity 100, un puerto montado en una ranura de expansión y otro fijo al chasis del ruteador. Se debe conectar el modem DSL/ROUTER por el puerto ethernet del spot, ya que el puerto fijo al chasis es utilizado para conectar con el segmento de red local.

5.2.5 Ruteador Contivity 100 de NORTEL NETWORKS para VPN

El switch-ruteador Contivity 100 ofrece una amplia capacidad para VPN sobre IP sitio a sitio y otras características más, incluyendo acceso seguro a Internet a través de túneles, protección de firewall, características de autenticación y encriptación de datos.

Características:

- **Seguridad en el túnel.** El Contivity 100 soporta IPSec en los túneles – cada uno envuelto en una corriente de datos dentro del formato del protocolo IPSec, de tal modo que permitan las comunicaciones corporativas atravesar una ruta privada a través de Internet.
- **Protección contra Hackers.** El Contivity 100 tiene capacidades de firewall por proxy. Esta técnica en la cual un servidor concentra las peticiones de todos los usuarios hacia y desde Internet. No abriendo una trayectoria directa entre dos redes, firewall por proxy previene al hacker obtener direcciones internas y detalles de la red privada y sus usuarios.
- **Acceso solo para usuarios autorizados.** El Contivity 100 acepta trafico entrante con autenticado, para conexiones de túnel. La autenticación del usuario es provista por SHA-1 (Secure Hash Algorithm-1) o MD5 (Message Digest 5) – algoritmos que crean firmas digitales. Los usuarios del contivity 100 pueden escoger el método de autenticación que mejor se adecue a los requerimientos de su aplicación.

Además las funciones de administración y actualización para el contivity 100 son protegidas por PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol). Ambos métodos implican el acceso a una tabla de ID's (identificadores) de usuarios y passwords en un servidor, para verificar en que momento ingresaron los usuarios. CHAP provee

un incremento en la seguridad mediante la encriptación de los ID's de usuarios y los passwords antes de que sean transmitidos al servidor de verificación.

- **Encriptación avanzada a la protección del tráfico de datos privados.** Todas las conexiones del contivity 100 son encriptadas para privacidad, utilizando ambos algoritmos DES (Data Encription Standard) y triple DES con llaves pre-compartidas. DES es un método eficiente que utiliza una llave de encriptación de 56 bits. Triple DES ofrece considerablemente más seguridad utilizando múltiples llaves que encriptan, deencriptan y encriptan nuevamente.

ESPECIFICACIONES TÉCNICAS

Componentes:

Procesador y memoria

- 1 Procesador Pentium 300 Mhz (expandible)
- 16 Mb en memoria RAM
- 8 MB en memoria flash

Opciones de interfase

- Dos puertos 10/100 Ethernet LAN
- Un puerto serial (DB9)
- Puerto sencillo o dual análogo ISDN

COMPATIBILIDAD

Protocolos de túnel

- PPTP
- L2F
- L2TP
- IPSec (incluyendo autenticación de encabezado)
- ESP
- IKE.

Protocolos de ruteo

- RIP1
- RIP2
- OSPF
- VRRP

Servicios de autenticación

- LDAP (interno/externo)
- RADIUS
- Tarjeta Token Integration via Security Dynamics and AXENT
- Certificado Digital de Autenticación vía Entrust y VeriSign

Encriptación

- Soporta hasta 192-bit de longitud de de llave o separados en llaves de 64-bit
- DES

- 3DES
- RC4
- FIPS 140-1 Level 2
- IPSec/ICSA certification

Requerimientos de Sistema

- Windows 95/98/2000/NT4.0 o más adelante

Figura 6.

5.2.6 Túnel entre OMAHA-ACAPULCO

A continuación se describirán los procesos y resultados, los cuales derivan de la creación y el funcionamiento del túnel, con el cual trabaja nuestra VPN.

Una de las propuestas de este trabajo y el punto en donde se ha hecho énfasis, es en la *disminución* de costos, siempre y cuando esta reducción, este justificada por la estructura y lineamientos del hotel, dando como resultado el optimo rendimiento de los procesos que demanda el Hotel. Todo esto en las áreas en donde sea viable dicha disminución de costos.

¿Porqué decidir entre una IP Estática o una IP Dinámica?

Retomando el texto anterior, comencemos por preguntarnos ¿Cuál es el principal beneficio que conlleva el uso de una IP dinámica en esta propuesta? Siendo esta (IP), la cual participa en la creación del túnel, que proveerá el enlace entre el *corporativo* (Omaha E.U.A) y el Hotel Radisson (Acapulco). La respuesta a la pregunta anterior es simple, la IP dinámica representa un ahorro sustancial en materia de *costo* del servicio.

Es en esta parte del estudio, podemos deducir claramente, una de las principales ventajas de este análisis, en el cual se recomienda la utilización de una dirección IP dinámica, debido a que en primer lugar, no hay limitantes por parte del hotel, también se hace el comparativo en referencia a costos del servicio, y definitivamente es más conveniente el uso de la IP dinámica, ya que nos brinda el mismo objetivo en cuanto a funcionalidad.

Veamos el siguiente comparativo.

Cuadro (b).

Prodigy Infinitum	Velocidad vs Dial Up	Velocidad de Bajada	Velocidad de Subida	Computadoras en Red*	Renta mensual IP Dinámica	Renta mensual IP Fija
256	Hasta 8 veces más rápido	De 128 hasta 256 kbps	Hasta 128 kbps	Hasta 16	$349.00	$1,349.00
512	Hasta 16 veces más rápido	De 256 hasta 512 kbps	128 kbps	Hasta 32	$599.00	$1,599.00
1,000	Hasta 33 veces más rápido	De 512 hasta 1000 kbps	256 kbps	Hasta 48	$999.00	$1,999.00
2,000	Hasta 66 veces más rápido	2000 kbps	512 kbps	Hasta 64	$4,599.00	$5,599.00

Fuente: http://www.prodigy.com.mx/infinitum_adsl
*Sugeridas

Refirámonos a los elementos que intervienen en esta propuesta de infraestructura tecnológica, los cuales son inherentes al momento de llevar a cabo la conexión *VPN*. Para efectos de este estudio dividámoslo en *elementos de tipo servicio*, *elementos de tipo hardware.*

El *elemento tipo servicio*, que básicamente es el servicio encargado de proveer una "salida" hacia la red de redes (*Internet*), siendo mas concreto, estamos hablando de una conexión ADSL, compuesta básicamente por un dispositivo *modem*, una cuenta de usuario y respectivamente la puesta a punto de los parámetros en el modem para realizar la conexión a Internet.

Dentro de los elementos de tipo *hardware*, contamos con una par de dispositivos que realizan el trabajo de enlace entre las dos oficinas remotas. Teniendo el mayor grado de importancia (que en un sentido estricto sabemos que no es así, puesto que un componente de tipo hardware o software, dependerán entre sí para realizar una tarea con éxito).Nos referimos específicamente al VPN Router Contivity 100 de Nortel Networks, el cual es totalmente administrable, con características que le permiten crear conexiones seguras y eficientes. También se cuenta como se hizo mención en el párrafo anterior, con un modem Speed Stream 5200 de Siemens, el cual debidamente configurado provee una conexión a Internet.

5.2.6.1 Creación del Túnel

Tomando en cuenta los dispositivos anteriores y entendiendo uno de los procesos, que finalmente permite hacer el "enlace" entre los dos

puntos, que a su vez esta asociado con el ruteador Contivity, me refiero al proceso NAT (Network Address Translation/Traducción de Dirección de Red), podemos discernir lo siguiente.

Una vez mencionado los elementos que se requieren (*hardware-software*) para la creación del túnel a través de Internet, analicemos como el *ruteador* Contivity permite la funcionalidad de trabajar con NAT.

Partamos del Router Contivity, el cual nos dará la pauta para la creación del túnel. Bien, una vez identificados los elementos de tipo hardware, echemos un vistazo al funcionamiento de NAT.

5.2.6.2 ¿ Que es NAT (Network Address Translation)? Traducción de direcciones de red

Una definición nos dice que, NAT es un estándar de Internet, que permite a una red local (LAN-Local Area Network) usar un conjunto de direcciones IP para el tráfico interno y un segundo conjunto de direcciones IP para el tráfico externo. Esto quiere decir que NAT, permite a un dispositivo (router) poder comunicar una red “local”, con algún otro dispositivo a través de Internet.

De NAT se destacan tres ventajas fundamentales.

- Simular una especie de cortafuegos (*firewall*), el cual oculta las direcciones IP que son internas.
- Permitir a una compañía utilizar más direcciones IP internas. Puesto que si se utilizan solo de manera interna, no habrá

posibilidad de que existan conflictos con otras direcciones IP, utilizadas por otras compañías u organizaciones.

- Finalmente permite utilizar múltiples conexiones ISDN (Integrated Services Digital Network, Red de Servicios Integrados), dentro de una conexión a Internet.

Desarrollado por Cisco, NAT es utilizado por un dispositivo (*cortafuegos, ruteador o una computadora*) que se sitúa entre una red interna y el resto del mundo (*Internet*).NAT tiene muchas formas y puede trabajar de diferentes maneras:

- **NAT Estática.** Se "traduce" una dirección IP no registrada a una dirección IP registrada, en una relación uno-a-uno. Particularmente es utilizada, cuando un equipo necesita estar accesible desde fuera de la red.
- **NAT Dinámica.** Se traduce una dirección IP no registrada a una dirección IP registrada de un grupo de direcciones IP registradas. Es decir, se le asigna una dirección IP registrada de un rango definido a una dirección IP no registrada.
- **Sobrecargar (Overloading).** Una forma de NAT *dinámica* que traduce múltiples direcciones IP no registradas a una sola dirección IP registrada utilizando diferentes puertos. A esto también se le conoce como PAT (Port Address Translation). Es decir cuando una dirección IP no registrada pretende "salir", la traducción ocurre a la misma dirección IP registrada, cambiando solo el puerto.

- **Traslapar (Overlapping).** Cuando la dirección IP usada en una red interna es una dirección IP registrada y esta siendo utilizada en otra red, el ruteador debe mantener una tabla de búsqueda de esas direcciones para que pueda interceptarlas y reemplazarlas con las únicas direcciones IP registradas. Es importante hacer notar, que el ruteador NAT debe traducir las direcciones "internas" a direcciones únicas registradas así como traducir las direcciones "externas" registradas a direcciones que solo utilice la red privada.

Ahora veamos como trabaja NAT en esta propuesta.

NAT como mencione, puede ser configurado de diferentes maneras, el ruteador Contivity es configurado para traducir direcciones IP no-registradas (internas) que residen en la red privada (Hotel Radisson) a direcciones IP registradas.

Esto pasará siempre que un dispositivo en nuestra red (hotel) con direccionamiento estático (no-registrada), necesite comunicarse a través de la red pública (Internet), con el corporativo ubicado en Carlson (E.U.A), tomando en cuenta que existe una conexión a Internet y que la red este funcionando en su normalidad.

- En primer término, se cuentan con los servicios de un ISP que nos entrega una conexión ADSL, que resulta en un acceso a Internet por medio de una dirección IP pública (dinámica).

- Por otro lado tenemos un segmento de direcciones IP que manejamos por parte de la red privada (Hotel).
- Teniendo los elementos antes mencionados y dada la configuración en el ruteador *Contivity* que posee la funcionalidad NAT, el proceso resulta ser muy transparente, es decir, cuando un host (*pc*), que tiene definidos ciertos privilegios y requiere hacer una transferencia de datos fuera de la red del Hotel, la petición de dicho *host* llega al ruteador *Contivity*, el ruteador verifica en su tabla de ruteo si hay una entrada disponible para la dirección destino, si existe, el ruteador traduce entonces el paquete de información y crea una entrada para el, en la tabla de traducción de direcciones (como ya sabemos, para identificar y validar cualquier *host* en una red, normalmente se hace por medio de la dirección IP), además de que el ruteador Contivity hace la gestión, validando la información del host (*fuente*) en la tabla del ruteador, así como la de realizar el proceso NAT, accediendo a la creación del túnel, en caso de que el host en cuestión tenga los permisos y privilegios debidos, dando como resultado, que la información del host (fuente) pueda ser enviada a través del túnel y se pueda concretar la VPNet (*red privada virtual*) hacia el ruteador *destino*.
- Existe el caso, en que el host de la red *local* (Hotel), necesita establecer comunicación con un host de la red *externa* (Corporativo), se lleva a cabo todo el proceso de validación y cuando finalmente el ruteador detecta que el host no se encuentra en la tabla de ruteo, lo que hace es desecharse del paquete de información que se pretendía enviar.

Finalmente, hemos visto aplicado usos y variantes que tiene *NAT*, así como destacar esta funcional herramienta, que es el ruteador Contivity 100, el cual provee una eficiente administración de los procesos en cuanto a conectividad se refiere, ya que como se ha dicho, tiene aplicaciones tipo *firewall*, previniendo posibles intrusiones hacia la red del Hotel, así mismo de manera interna, se puede llevar a cabo un control detallado de las conexiones que existan hacia cualquier punto (fuera de la red), no dejando de lado la gestión de trafico y filtrado de información que existe entre los diferentes host (externos).

Haciendo un breve resumen para poder aterrizar lo dicho anteriormente y ver que esta sucediendo con la interacción de los elementos antes mencionados, recordemos lo siguiente.

A nivel infraestructura (física):

- Se cuenta con una LAN (UTP Cat 5e) por parte del Hotel Radisson.
- Conjunto de servidores que proveen los servicios a la LAN tanto interna como externamente.
- Un ruteador de la marca Nortel Networks.
- Modem Speed Stream 5200.

CONCLUSION Y RECOMENDACIONES

Uno de los objetivos que han sido prioridad en este estudio, es el de mostrar al lector el desarrollo y aplicación de una solución en base a requerimientos de la empresa, que en este caso en particular hacemos referencia a una empresa prestadora de servicios, la cual se rige por altos estándares de calidad. Así mismo, su misión es la de proveer a sus clientes la mejor de las estancias, valiéndose de los servicios e infraestructura con que el hotel cuente. Teniendo el hotel como principal punto a satisfacer, el carácter recreativo así como de confort hacia sus huéspedes. Todo esto y sin dejar de lado la estructura tecnológica, que es de suma importancia para poder brindar a sus huéspedes las facilidades para hacer uso de las instalaciones del hotel y así como de los servicios con que cuenta. Por citar un ejemplo; desde hacer una reservación, cuando nos encontramos en una agencia de viajes u oficina autorizada que no se encuentre geográficamente cerca del hotel, para llevar a cabo dicha tarea.

También se pretende incentivar a todos aquellos compañeros profesionistas que se encuentren en el ramo de la administración, protección y mejor flujo de la información, a realizar propuestas que conlleven a una disminución de costos considerable, en los puntos en donde pueda aplicarse, todo esto sin sacrificar la eficiencia y productividad entre los sistemas de cómputo, que pueda resultar un producto o servicio de baja calidad.

Se ha ejemplificado para este estudio en particular, el uso de las VPN’s como una herramienta que permite de manera eficaz una

reducción en costos de comunicación de enlaces digitales, con la ventaja principal de que no estamos haciendo una inversión representativa, para prácticamente cualquier empresa, tomando en relación otras soluciones más robustas. Siendo reiterativos en tomar en cuenta las necesidades y requerimientos de cada empresa, ya que dependiendo de estos parámetros, adquirirá mayor complejidad la solución que pretendamos plantear.

Para el hotel Radisson Acapulco es de gran importancia poner especial atención en los rubros de seguridad así como de integridad de sus datos, para lo cual se analizan profundamente los flujos de información tanto de manera interna en el hotel, así como la transmisión y recepción de la misma, que se haga desde el exterior. Todo esto lográndose por medio del establecimiento de directivas de seguridad, tanto del usuario como del hardware o software en cuestión.

El trabajo futuro que se pudiera realizar a este proyecto, seria no perder aspectos fundamentales como lo es la *seguridad*, ya que esta significa una parte medular en el entorno tecnológico que hemos estado tratando, ya que si bien no es un sistema de misión critica propiamente, la corrupción de información representaría perdidas en ventas y un deplorable servicio al cliente. Otro punto es la verificación en cuanto a compatibilidad de los diferentes dispositivos que en un momento dado se pudieran adicionar a esta solución, tomando en cuenta que esta propuesta (como todo ciclo computacional), tiene un tiempo de vida, para poder realizar algún cambio radical o no.

Sin duda actualmente, al encender nuestro aparato televisor, dar un vistazo en la portada de una revista en materia de innovaciones tecnológicas, o simplemente recibir varios mensajes publicitarios (en la mayoría de la ocasiones, bombardeos de POP-UP's), alusivos a productos o servicios, al momento de revisar nuestro correo electrónico, podemos palpar una nueva etapa en el manejo de la información, así como el incesante surgimiento de tecnologías, las cuales repercuten indudablemente en la sociedad, la cual que se ve obligada a modificar la forma de interactuar entre los demás individuos, denotando cierta clasificación de tipo social-tecnológica, entre la misma sociedad, paralelamente en las empresas, que adopten dichas tecnologías, cambiaran dependiendo del grado de integración de las tecnologías, algunos procesos y diferentes formas, para el tratamiento de la información.

Existe un periodo de renovación y descubrimiento de nuevas tecnologías cada determinado tiempo. Y muchos de nosotros, han experimentado esta etapa de obsolencia de las herramientas y dispositivos que, mayormente facilitan nuestras labores diarias y que muchas veces pensamos que seria "casi imposible" realizarlas sin ellas. Este patrón, ha obligado de alguna forma, a que las personas que están expuestas a estos constantes cambios, apliquen estas nuevas formas de comunicación, entretenimiento y constante proceso de actualización. A últimos años, es común toparnos en la calle a personas que poseen dispositivos de toda clase, como teléfonos celulares, PALM's, reproductores MP3's, equipos de radio comunicación, los cuales son capaces de establecer comunicación entre personas de distintos

países, solo por mencionar algunos, dichos dispositivos con el tiempo sufren mejoras, en cuanto a capacidad de almacenamiento, perfeccionamiento en sus funciones, calidad y seguridad en el manejo de información, por citar algunos adelantos.

De igual manera, las empresas se ven enfrentadas a esta tecnología entrante, esto no quiere decir que todo el desarrollo tecnológico que este emergiendo, aplique para todas las empresas, mucho menos sea viable y adaptable a los esquemas e infraestructura con las que cuente. Es por eso que considero, en caso del Hotel Radisson Acapulco, analizar detalladamente cada área y servicio en el cual se pretenda dar un mejor rendimiento, tanto en los procesos internos del hotel, como los servicios que se ofrecen a los clientes, todo esto evaluando diversas opciones y tecnologías las cuales estén vigentes en ese lapso que se pretenda alguna mejora, siempre y cuando cumplir con los estándares que rigen la calidad del hotel.

GLOSARIO

3DES. (*Triple Data Encryption Standard*) Se basa en DES, pues encripta los datos tres veces seguidas apoyándose en este algoritmo. Para encriptar puede utilizar dos claves distintas, obteniendo una clave de 112 bits ó tres claves distintas, obteniendo en este caso una clave de 168 bits.

Acceso remoto. Propiamente dicho es la capacidad de conectarse a una red que geográficamente esta distante. Generalmente, esto implica una computadora, un módem, y un cierto software de acceso remoto para poder conectarse con la red.

ADSL. (Asymmetric Digital Subscriber Line) es una nueva tecnología que permite el envío de más datos ser enviados a través de las líneas telefónicas de cobre.

AES. (Advanced Encryption Standard) que en los próximos años se convertirá en un algoritmo estándar de encriptación desplazando a DES.

ARPA. Pos sus siglas en ingles, Advanced Research Projects Agency algo así como la Agencia de Investigaciones de Proyectos Avanzados.

ARPAnet. Una de las primeras redes que utilizó el pentágono de Estados Unidos.

ATM. (Asynchronous Transfer Mode) por sus siglas en ingles. Modo de transferencia asíncrono. Una tecnología de red basada en la transferencia de células o paquetes de un tamaño fijo.

Backbone. Se refiere a las conexiones principales de las cuales se compone Internet.

Bit. Es la mínima unidad de información que se maneja en una maquina. Un simple bit solo puede tener dos tipos de valores, 0 o 1. En su mayoría las computadoras se clasifican en números de bits que pueden procesar de una sola vez o por el número de bits que utilizan para representar direcciones.

BITNET. (Because It's Time NETwork) que constituye una red con fines educativos y de investigación para conectar centros de ordenadores a lo largo del mundo usando líneas alquiladas de 9600 bps. Utiliza un protocolo llamado NJE (Network Job Entry).

Bridges (Puentes). Es un dispositivo que conecta dos redes de área local (LAN's) o dos segmentos de una misma red LAN que usan el mismo protocolo.

Cable. Conexión a Internet de alta velocidad que se hace a través de fibra óptica.

CAR. (Committed Access Rate) Componente básico de la calidad de servicio en una VPN. El cual se encarga de garantizar un ancho de banda mínimo para aplicaciones o usuarios basándose en la política corporativa.

CPU (Central Processing Unit). Unidad Central de Proceso. Se refiere al cerebro de una computadora. A veces se refiere solamente como procesador o procesador central. El CPU es en donde se llevan a cabo la mayoría de los cálculos.

DES. (*Data Encryption Standard*) Usa una clave de 56 bits para encriptar datagramas de 64 bits.

DHCP. (Dynamic Host Configuration Protocol) Configuración Dinámica de Protocolo de Host. Es un protocolo que se utiliza para asignar direcciones IP de manera dinámica en una red. Con el direccionamiento

dinámico, un dispositivo puede tener diferentes direcciones IP cada vez que se conecta a una red.

Dial-Up. Conexión vía modem telefónico el cual se encarga de enviar y transmitir señales analógicas a través de cobre.

Dominio. Un dominio es un grupo de computadoras y dispositivos en una red, que son administrados como una unidad, teniendo en común reglas y procedimientos. Dentro de Internet, los dominios son definidos por direcciones IP.

Downstream. Contrario a *upstream*, es la transmisión que se lleva a cabo desde un servidor hacia un usuario final. Ejemplo de una transmisión *downstream* se refleja con la señal que envía un proveedor de televisión por cable hacia un cliente.

DS0. Enlace dedicado de comunicación sencillo, con una velocidad de 64 Kbps.

DS1. Canal de comunicación digital sencillo tipo, con una velocidad de 1.544 Mbps.

DS3. Canal de comunicación digital de señal tipo 3, con velocidades que van desde los 2.048 Mbps hasta los 44.736 Mbps.

DSA. (*Digital Signature Algorithm*) Es el algoritmo estándar de Firma Digital. Genera una clave de 512 ó 1024 bits por lo que es más lento que RSA.

E1. Enlace dedicado que se utiliza principalmente para la transmisión de datos, con una velocidad de transmisión de 2.048 Mbps.

E3. Canal digital de comunicación utilizado para la transmisión de datos, con velocidades desde 2.048 Mbps hasta 34.368 Mbps.

E-mail. Comúnmente llamado correo electrónico, son los mensajes que se transmiten sobre redes de comunicaciones. Los mensajes pueden

ser notas entradas desde el teclado o archivos almacenados en un disco.

Encriptación. Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor. Se usa para evitar el robo de información sensible, como números de tarjetas de crédito.

Enlace Analógico. Tipo de enlace que maneja una velocidad de hasta 9,600 Kbps y se asocia al uso de transmisión de voz.

Enlace dedicado. Se refiere a una solución de conectividad permanente que maneja distintas velocidades y que son utilizados comúnmente por empresas según sus necesidades.

Enlace Digital. Transmisión que se puede llevar a cabo desde un ISP hacia un hogar o negocio, el cual contiene datos expresados con valores numéricos discretos (dígitos binarios o bits) de unos y ceros que la máquina puede interpretar.

Ethernet. Es una arquitectura desarrollada por la compañía Xerox, la cual se implementa principalmente en redes de área local, la cual consiste en un bus o una topología tipo estrella y soporta una tasa de transferencia de 10 Mbps.

Extranet. Se refiere a una Intranet que es parcialmente accesible por usuarios externos. Mientras que un Intranet reside detrás de un cortafuego y es accesible solamente por miembros de la misma compañía u organización, un extranet proporciona varios niveles de accesibilidad a los usuarios externos.

FIDELIO. Sistema esta enfocado a la administración en hoteles.

Firewall. Un sistema diseñado para prevenir accesos no autorizados hacia o desde una red privada. Los cortafuegos se pueden implementar

tanto en software como en hardware o como una combinación de ambos.

Firma Digital. La Firma Digital, garantiza la identidad de los extremos durante su transporte sobre redes privadas IP ó públicas como Internet, es decir autentica la identidad de la persona que envía esos datos ó que los firma.

Frame Relay. Es un protocolo de conmutación de paquetes que se utiliza para conectar dispositivos en una Red de Área amplia (WAN). En Estados Unidos, Frame Relay soporta velocidades de transmisión desde un T1 de 1.54 Mbps hasta un T3 de 45 Mbps.

Gateway. Un nodo en una red que sirve como entrada a otra red.

GRE. (*Generic Routing Encapsulation*) permite llevar los paquetes PPP de usuario. Permite a bajo nivel controlar la congestión y flujo que va a llevarse a través de los túneles usados para llevar los datos de usuario entre PAC y PNS.

GTS. (Generic Traffic Shaping) Componente básico de la calidad de servicio en una VPN. Reduce la velocidad de salida de los paquetes con el fin de reducir posibles congestiones de la red que tengan como consecuencia el descarte de paquetes.

Hashing. Es la acción de producir valores hash para acceder a datos o por seguridad. Un valor hash (o simplemente hash), también llamado *resumen del mensaje*, es un numero generado de una cadena de texto.

HDBM. Es una estación de trabajo, que tiene como objetivo principal, la administración y monitoreo de las reservaciones que se lleven a cabo en sitio, así como las que se realicen vía WWW.

HOST. Se puede interpretar como una computadora que es accesada por un usuario que esta trabajando en una localidad remota.

Usualmente el término es usado cuando dos computadoras son conectadas por medio de módems y líneas telefónicas.

Internet. Conjunto de redes de ordenadores creada a partir de redes de menos tamaño, cuyo origen reside en la cooperación de dos universidades estadounidenses. Es la red global compuesta de limes de redes de área local (LAN) y de redes de área extensa (WAN) que utiliza TCP/IP para proporcionar comunicaciones de ámbito mundial a hogares, negocios, escuelas y gobiernos.

Intranet. Una red basada en protocolos TCP / IP, los cuales pertenecen a una organización, usualmente una corporación, accesible únicamente por miembros de la organización, empleados u otros con autorización.

IPSec. Es un conjunto de protocolos desarrollados por el IETF (Internet Engineering Task Force) para el soporte de la seguridad en el intercambio de paquetes en la capa IP. IPSec ha sido desarrollado ampliamente para implementarse en VPN's.

IPv4. Creado hace más de veinte años, el snack TCP/IP ha probado tener un diseño poderoso y flexible. Pero representa ya algunas limitaciones al funcionamiento de las redes actuales. Por ejemplo, inminente saturación del espacio de direcciones, se requiere soportar aplicaciones de videoconferencia y multimedia en tiempo real, se requieren mecanismos de seguridad en la capa de red.

IPX. (Internetwork Packet Exchange) Es un protocolo para establecer una red, el cual es usado por los sistemas operativos Novell Netware.

ISP. (Internet Service Provider) Por sus siglas en ingles (Proveedor de Servicio de Internet). Se refiere a la compañía que provee el acceso a Internet. Por una tarifa mensual, el proveedor brinda al usuario un

paquete de software (según sea el caso), un nombre de usuario y una contraseña así como el numero de acceso telefónico.

Kbps. Kilo bits por segundo, es una medida de velocidad para trasferencia de datos. Por ejemplo los módems miden su velocidad en Kbps.

L2TP. Por sus siglas en ingles Layer Two Tunneling Protocol, Protocolo de Túnel en capa dos, es una extensión del protocolo PPP que habilitan los proveedores de Internet para operar una red privada virtual.

LAN (Local Area Network). Red de Área local, Se llama así a una red de computadoras que se comunican entre si en una área relativamente pequeña.

MAIN. Con este servidor se pueden controlar los accesos a los diferentes departamentos, así como se tendrá más confiabilidad en los datos, debido a que el servidor MAIN se encargara de administrar los Usuarios, y si existiera algún problema, se contaría con un respaldo.

Mascara de Subred. También conocida como mascara de dirección. Cifra de 32 bits que específica los bits de una dirección IP que corresponde a una red y a una subred. Las direcciones de bits no cubiertas por la máscara corresponden a la parte del host.

MEXNET. Organismos que se crea el 20 de enero de 1992 en la Universidad de Guadalajara y por iniciativa de varias universidades como –Sistema ITESM, Universidad de Guadalajara, Universidad de las Américas, ITESO, Colegio de Postgraduados, LANIA, CIQA, Universidad de Guanajuato, Universidad Veracruzana, Instituto de Ecología, Universidad Iberoamericana e Instituto Tecnológico de Mexicali–, el cual se encargaría de coordinar los esfuerzos de las instituciones de educación superior interesadas en propiciar y contribuir al desarrollo de Internet en México.

MICROS. Estación de trabajo que lleva a cabo una traducción entre la estación de trabajo INTERFASES y el tarificador, para poder emitir un reporte al sistema FIDELIO.

NAP. (Network Access Point) Una red publica que facilita el intercambio, en donde los ISP's pueden conectarse con algún otro mediante arreglos pares. Los NAP's son los componentes claves de los *backbone* de Internet, porque las conexiones dentro de ellos determinan como el trafico será enrutado.

OSI. Que significa Sistema de Interconexión Abierto, junto con la ISO, se encargan de definir el marco de una red para implementar protocolos en las siete capas.

PAC. (*PPTP ACCESS CONCENTRATOR*) Concentrador de acceso PPTP. Dispositivo que asocia una o mas líneas capaces de soportar PPP (Point to Point Protocol) y manejo del protocolo PPTP. PAC necesita solamente TCP/IP para pasar sobre el tráfico de una o más PNS.

PDC. (Primary Domain Controller) *Controlador de Dominio Primario*. Servidor capaz de administrar los servicios y aplicaciones con que cuenta la estructura Carlson. Así como permite a los usuarios firmarse a las diferentes aplicaciones.

PNS. (*PPTP Network Server*) Es el servidor para red de PPTP. Sirve para operar sobre computadoras de propósito general y plataformas de servidores. PNS dirige la parte del servidor del protocolo PPTP mientras PPTP confía completamente TCP/IP y es independiente de la interfaz de Hardware, el PNS puede usar cualquier combinación de hardware de interfaz IP, incluyendo dispositivos LAN y WAN.

PPTP. Por sus siglas en ingles Point to Point Tunneling Protocol, Protocolo de Túnel punto a punto, una nueva tecnología que se utiliza para crear redes virtuales privadas, desarrollada por Microsoft, U.S. Robotics y muchos proveedores de accesos remotos.

PROXY. Es un servidor que se sitúa entre una aplicación cliente, como puede ser un *navegador,* y el servidor verdadero.

RDSI (ISDN-Integrated Services Digital Network). Red Digital de Servicios Integrados. Es un tipo de red que agrupa distintos servicios anteriormente distribuidos a través de soportes distintos, siempre que se utilice tecnología digital: telefonía (con centralitas digitales), videoconferencia, teleinformática, videotex, mensajería electrónica, sonido, datos, imágenes, etc.

Ruteador (Router). Es un dispositivo que remite paquetes de datos a lo largo de redes.

RS - 232. Se trata del principal medio por el cual se conecta un ordenador a un periférico (sobretodo el modem). La interfase tiene 25 conexiones denominadas DB25, aunque existe otro de sólo nueve, denominado DB9. Es un estándar de Electronic Industry Association (EIA). Es también conocido como: IEEE-448.

RSA. (*Rivest, Shamir, Adelman*) Es el algoritmo de Firma más popular, puede ser utilizado tanto para firmar los datos como para encriptarlos aunque es mucho más lento que DES.

Script. Es una lista de comandos que pueden ser ejecutados sin la interacción de un usuario.

Segmentación. En términos de redes, es una sección que esta perfectamente delimitada por puentes, ruteadores o switches. Por

ejemplo. Dividiendo una Ethernet en múltiples segmentos es una de las formas más comunes de incrementar el ancho de banda en una Lan.

Servidor. Se entiende como una computadora o un dispositivo que administra los recursos de una red.

Software. Cualquier cosa que pueda ser almacenada electrónicamente se le considera *software.*

Switch. En términos de una red, dispositivo que filtra y distribuye paquetes entre segmentos de una red LAN.

T1. Canal de comunicación digital utilizado en Estados Unidos, el cual maneja una velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 1.54 Mbps a través de una red telefónica.

T2. Línea digital interna de las compañías telefónicas que no se ofrecen a las empresas privadas. Con una velocidad de 6.32 Mbps.

T3. Línea de transmisión de datos utilizada en Internet. (Requiere de Fibra Óptica). Con una velocidad de 44.736 Mbps.

TCP/IP. Protocolo de Control de Transmisión / Protocolo de Internet. Uno de los protocolos más utilizados en la redes, para la transmisión de datos.

Tunneling. (Túnel)Una tecnología que permite a una red enviar datos mediante conexiones a otras redes.

UNIX. Sistema operativo con propiedades de *multiusuario* y *multitareas* desarrollado por los laboratorios Bell a principios de 1970.

Upstream. Se refiere a la transmisión que se lleva a cabo desde un *usuario final* a un servidor. Una transmisión *upstream* se puede dar en forma de una señal que es transmitida desde una estación de trabajo hacia un servidor a través de una red, como por ejemplo una LAN.

VPN (Virtual Private Network). Una red que es construida usando el cableado publico para conectar nodos.

WFQ. (Weighted Fair Queuing) Componente básico de la calidad de servicio en una VPN. Determina la velocidad de salida de los paquetes en base a la prioridad asignada a estos, mediante el encolado de los paquetes.

Workstation. Un tipo de computadora usada en aplicaciones de ingeniería, diseño de publicidad, desarrollo de software y otro tipo de aplicaciones que requieren una gran cantidad de recursos y relativamente alta calidad en el manejo de gráficos.

WRED. (Weighted Random Early Detection) Componente básico de la calidad de servicio en una VPN. Complementa las funciones de TCP en la prevención y manejo de la congestión de la red, mediante el descarte de paquetes de baja prioridad.

WWW (World Wide Web). Es un sistema de servidores de Internet que soportan especialmente documentos en un formato específico. Estos documentos están formateados bajo un lenguaje llamado HTML (*HyperText Markup Language*) que soporta ligas a otros documentos, así como graficas, audio y archivos de video.

BIBLIOGRAFÍA

- Titulo: Redes globales de información con Internet y TCP/IP
  Autor: Douglas E. Comer
  Tercera Edición
  Editorial: Pearson
- Titulo: Como construir una Intranet con Windows 2000 Server
  Autor: José Luis Raya, Laura Raya
  Primera Edición
  Editorial: RA-MA Editorial

Referencias en Internet

- http://ciberhabitat.com/museo/cerquita/ic05.htm
- www.webopedia.com
- www.glosarium.com
- www.red.com.mx
- http://computer.howstuffworks.com/