UNIVERSIDAD POLITÉCNICA SALESIANA

FACULTAD DE INGENIERÍAS
SEDE QUITO-CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

Análisis de Factibilidad para la Implementación de un Sistema Integral de Interconexión entre la Dirección Nacional De Servicios Educativos (DINSE) y sus respectivas Unidades Administrativas Regionales a través de una red privada virtual reutilizando la infraestructura existente

TESIS PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO DE SISTEMAS

ANGEL DARWIN GUALOTUÑA NIETO

DIRECTOR: ING. MARLON J. CARTAGENA

QUITO, AGOSTO 2010

DECLARACIÓN

Yo, Angel Darwin Gualotuña Nieto, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la ley de propiedad intelectual, por su reglamento y por la normatividad institucional vigente.

_____

A. Darwin Gualotuña Nieto

CERTIFICACIÓN

Certifico que el presente trabajo, fue desarrollado por Angel Darwin Gualotuña Nieto, bajo mi dirección.

_____

Ing. Marlon J. Cartagena Andrade

DEDICATORIA

Quiero dedicar el presente trabajo, a toda mi familia y a quienes considero parte la misma, quienes ha estado siempre apoyándome, independientemente de mis decisiones, especialmente a mi mami Loly, papi Angel y a mis hermanas Edith, Marianela, y mi sobrinita Brigithe y muy especialmente a mi hermana Gladys quien hizo posible con su incondicional apoyo, que pueda alcanzar una meta mas.

AGRADECIMIENTOS

Agradezco a todos quienes de alguna manera aportaron para la realización del presente trabajo, especialmente al personal de la DINSE y en particular al Ing. Pablo Rengifo, Eco. Patricio Puente y Sr. Vicente Soria por su predisposición para brindarme su desinteresado apoyo.

Agradezco a mi tutor Ing. Marlon por su paciencia, compresión, estimulo y guía, para hacer posible la presente tesis.

De manera especial, agradezco a la Universidad Politécnica Salesiana porque gracias los conocimientos adquiridos en ella, he alcanzado logros personales y profesionales.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo, es un análisis de las ventajas de implementar alternativas económicas, de interconexión de redes geográficamente distantes, para brindar acceso a los recursos tecnológicos, de una institución como la DINSE que tiene una Matriz centralizada en la ciudad de Quito, y cuenta con unidades administrativas regionales para cubrir todo el territorio nacional y canalizar la ejecución de obras de infraestructura escolar. Se muestra también que es una excelente alternativa el tener una infraestructura mixta, entre equipos de alto costo inicial, software licenciado y equipos robustos pero más accesibles, y software de código abierto, reutilizando parte de los equipos existentes.

Por este motivo, se diseño la solución de tal manera que permita el acceso transparente a los recursos y servicios de la unidad Matriz y la administración en tiempo real, al resto de unidades administrativas de manera segura, confiable amigable y económica.

CAPÍTULO 1: REDES CORPORATIVAS

1.1 INTRODUCCIÓN (RESEÑA HISTÓRICA)

La industria de la Computación es relativamente joven, comparada con otras industrias, aun en el área de las Telecomunicaciones, como por ejemplo la telefonía. La rapidez del crecimiento y el abaratamiento de los costos[1] hacen que hoy en día las Computadoras estén al alcance de la gran mayoría de personas y de prácticamente todas las empresas.

En el presente trabajo se ha visto conveniente realizar una reseña histórica de los principales acontecimientos que permitieron la implementación y desarrollo de las redes Corporativas en el Ecuador y la computación en general.[2]

Adelanto importante en estudios: En 1978 la Escuela Politécnica del Ejército crea el Instituto de Informática, cuyos estudios se extienden por seis semestres. De esta manera inició una carrera profesional que despuntaría en el futuro.[3]

El primer computador IBM: En 1978 Filanbanco instaló el primer computador IBM 4331 con teleproceso, uno de los primeros en Sudamérica con el Sistema Operativo DOS USE, igualmente primero en el país.

Creación de Entidad Gubernamental: En agosto de 1978 el Gobierno Nacional[4] crea la Comisión Nacional de Informática, ente que se encargaría de brindar el soporte necesario para el desarrollo de esta área.

Nuevos Equipos IBM: En 1979 IBM lanza al mercado ecuatoriano una nueva línea de equipos de dictado, que incorpora como medio de registro discos magnéticos que se encuentra en cartuchos, con un máximo de 25 discos por cartucho.

---

[1] El abaratamiento de los costos se da principalmente debido a la gran oferta existente, la producción en serie y la Globalización del conocimiento.
[2] PCWorld, "303 Números en 30 años", *PC WORLD*, año XXX, Nº 303, Ecuador, Mayo 2008
[3] www.pcwla.com
[4] Triunvirato encabezado por Luis Leoro Franco.

Normas que impulsaron la Informática: En febrero de 1979 se publica el reglamento interino de la Comisión Nacional de la Informática, cuya finalidad es impulsar la actividad informática en el País, esta comisión tuvo listo el reglamento en 6 meses luego de su creación.

IBM y Microsoft: Estos dos gigantes se debaten el mercado en 1981 el Computador personal de IBM revolucionó el mercado con su precio competitivo y accesible para el usuario medio, su precio era de 1565 USD. En este año También entro en escena Microsoft con su Sistema Operativo MS - DOS.

Las primeras Portátiles: En 1981 sale a la venta el primer Computador portátil *Osborne* 1 a 1795 USD. La Gavilán SC fue la primera Computadora que se comercializó como "*laptop*" en 1983 a 4000 USD.

IBM presenta su PC: En agosto de 1981, IBM lanzó la primera PC con microprocesador Intel 8088 de 4,77 *Mhz* de velocidad, lo más avanzado de su época. La disquetera ofrecía 160 Kilobytes de almacenamiento, aproximadamente 50 páginas escritas a máquina, con monitor a color y sistema Operativo DOS.

Las primeras Redes: El área bancaria fue pionera en redes, en septiembre de 1981, el presidente Oswaldo Hurtado, presidió una ceremonia en la que trece Bancos del País se conectaron a la red mundial de Telecomunicaciones Bancarias que opero la SWIFT –Society World Interbanks Financial Telecomunications- (Sociedad para Telecomunicaciones Financieras Interbancarias Mundiales). Ecuador fue el Segundo país en hacerlo después de Chile en Latinoamérica.

La primera feria de Computación: En Octubre de 1982 se organiza la primera feria Exposición de Informática y afines, Compu 82 en el círculo Militar de Quito.

Apple inicia con el Mundo gráfico en Sistemas Operativos: En 1981 el Computador de Apple, Lisa, se marca como el principio de la desaparición de programas basados solo en texto para dar paso a los gráficos a un precio de 9995 USD. A partir de este punto muchos cambios se suscitan principalmente por la competitividad entre Apple y Microsoft.

Los primeros Clones: En vista del alto costo de los computadores , la empresa Compaq lanza en Enero de 1983 su primer clon de computadores, lo que le generó grandes ganancias debido a la baja de precios a la mitad de lo que se ofertaba.

TV por suscripción: En 1985 los Sistemas de Audio y Video por suscripción inician su operación con la primera empresa registrada como proveedora del servicio, Tele-Cable. Casi simultáneamente se concesiona este servicio a TV Max, ambas empresas se fusionaron y dieron cabida a TVCable.

Creación del CONADE: En junio de 1985 se disuelve la Comisión Nacional de Informática por el Gobierno de León Febres-Cordero, encargando estas funciones al CONADE -Consejo Nacional de Desarrollo -.

El fax reemplaza al Télex: En 1986 baja la popularidad del télex (Sistema automático de comunicación) con la llegada al país del Fax (facsímil), sistema que permite transmitir a distancia por la línea telefónica escritos o gráficos (telecopia).

IETEL digitalizado: En junio de 1986, el IETEL -Instituto Ecuatoriano de Telecomunicaciones-, adquirió la primera central Telefónica Digital, gracias a un acuerdo alcanzado con la compañía Sumitomo Corporation de Tokio, Japón.

El primer paso de Ethernet: En junio de 1986 se instala en la Cooperativa de Ahorro y Crédito Oscus, el primer sistema en el Ecuador de Ethernet (Data Communications Lan Ethernet), con computadores Data General.

Conteo de Votos Computarizado: En julio de 1986 como dependencia de la presidencia de la República, la Secretaria Técnica Nacional de Informática, por primera vez en la historia electoral del país, trabajo conjuntamente con la secretaría Nacional de Información Pública en la recolección y conteo de votos como parte del proceso electoral del país.

Alcatel se Instala en Quito: A partir de Julio de 1987 la empresa Telenorma fundada en 1958 toma el nombre de Alcatel del Ecuador, para brindar al país hardware, software y servicios para proveedores de telecomunicaciones.

Acuerdo entre Apple y *Digital Equipment*: En abril de 1988 Apple y *Digital Equipment Corporation* llegan a un acuerdo para integrar los equipos de ambas empresas y sus respectivas redes de comunicación.

Internet al Área empresarial: En 1991 Ecuanex, un nodo de Internet establecido por la corporación Interinstitucional de Comunicación Electrónica, Intercom, ofreció sus servicios al Ecuador a nivel corporativo. Pero a partir de Octubre de 1992 el Internet llego al común de los usuarios, gracias a un segundo nodo, Ecuanet, que fue establecido en el país por la Corporación Ecuatoriana de Información, auspiciada por el banco del pacífico, la ESPOL, la Universidad Católica Santiago de Guayaquil y otras entidades.

Nace EMETEL: En agosto de 1992, se reestructuró el sector de las telecomunicaciones cuando el congreso Nacional aprobó la ley especial de Telecomunicaciones, por la que IETEL se transformó en EMETEL -Empresa Estatal de Telecomunicaciones-. Otro aspecto importante fue la creación de la SUPTEL -Superintendencia de Telecomunicaciones- como organismo de regulación y control.

Ayuda Tecnológica a No-Videntes: En septiembre de 1992, Xerox instaló en Ecuador el primer equipo de lectura para ciegos.- Inventado por el científico y empresario *Raymond Kurzweil*, el lector personal introdujo material impreso a un computador mediante un scanner y luego lo tradujo en voz sintetizada.

Eficiencia en Telecomunicaciones: En Octubre de 1992 Alcatel lanzó al país el nuevo Centro de Atención Automatizada, el nuevo equipo mejoró la producción y eficiencia de las empresas en comunicaciones, al suministrar información, optimizar la recepción de mensajes direccionándolos al correo de voz y agilizar la transferencia de llamadas.

Microsoft: Microsoft abre sus puertas en Ecuador en vista de las proyecciones de desarrollo tecnológico.

Inicio la telefonía Celular: En 1993 las empresas *Otecel* y *Conecel* fueron escogidas para operar con telefonía celular en país. *Conecel* con su nombre comercial Porta, firma primero un contrato de concesión de servicios de

telecomunicaciones con el Estado Ecuatoriano por un periodo de 15 años en Agosto. En tanto en noviembre *Otecel* firma un contrato parecido bajo el nombre de celular Power, que luego fue BellSouth y actualmente Movistar de Telefónica de España. El primer celular fue Motorola.

Transformación de entes gubernamentales: En agosto de 1995 EMETEL se transformó en la sociedad anónima -EMETEL S.A.- Se crea el CONATEL-Consejo Nacional de Telecomunicaciones-, para administrar y regular las Telecomunicaciones; la Secretaria Nacional de Telecomunicaciones -SENATEL- es designada para ejecutar políticas de Telecomunicaciones y la Superintendencia de Telecomunicaciones como ente de control.

Impsat conecta al Ecuador con 4 países: En noviembre de 1995 Impsat (después de su creación en Julio de 1993) crea la primera super-autopista de la información latinoamericana con el Telepuerto que conecto a Argentina, Colombia, México, Venezuela y Ecuador con una red neuronal de las telecomunicaciones y la información que permitió a los latinoamericanos entrar al mundo globalizado.

Festival de la Canción Computarizada: En octubre de 1993. Cosideco doto de red computacional al festival OTI de la Canción capitulo Ecuador. La empresa diseño un programa computacional para contabilizar el puntaje otorgado a cada participante. El sistema estuvo basado en una red Novell, constituida por diez estaciones de trabajo.

Tarjeta inteligente para el Área bancaria: En diciembre de 1995 Filanbanco incorpora la tarjeta inteligente para sus servicios, incluía un micro chip para realizar más de un transacción bancaria y portar documentos electrónicos y hasta información importante para el portador. La tecnología se respaldo en HCMOS, con un CPU de 8 bits.

La Banca siempre innovando: En febrero de 1997, el banco de préstamos fue la primera entidad que introdujo el sistema *Cobis* completamente en todas sus fases y aplicaciones. Este software desarrollado por la empresa nacional Macosa cuenta con una tecnología abierta de Cliente – Servidor.

Fin de EMETEL: En noviembre de 1997 de conformidad con la ley reformatoria a la ley especial de telecomunicaciones se inscribió en el registro Mercantil la escritura de escisión de EMETEL en dos compañías operadoras Andinatel con sede en Quito y Pacifictel con sede en Guayaquil. En el mismo periodo inicia el primer intento de venta de las operadoras, pero no se realiza; en 1998 se vuelve a intentar pero falla debido a movilizaciones populares, sumadas a conflictos de intereses de los posibles compradores.

Mayor control en Telecomunicaciones: En Marzo de 1998 la SUPTEL inauguró el SICOTE -Sistema Nacional de Comprobación Técnica de Emisiones Radioeléctricas-, cuya finalidad era permitir un control eficiente de los servicios públicos y privados de telecomunicaciones.

Backbone Andino: En 1999 se crea el Sistema Andino de Internet. La empresa Impsat como miembro de la ASETA -Asociación de Empresas Estatales de Telecomunicaciones del Acuerdo Subregional Andino- colaboró junto con Colombia y Venezuela. Para crear un Backbone Andino para que el tráfico que sale a EEUU pase por este Backbone.

Internet de Andinatel: En 1999 Andinatel expande sus servicios a Internet, al utilizar el cable Panamericano que inició operaciones en el país en el mismo año. Parte desde Arica (Chile), va a Lurín (Perú), Punta carnero (Ecuador), Ciudad de Panamá (Panamá), Barranquilla (Colombia), Punto fijo (Venezuela), *Baby Beach* (Aruba), Saint Croix (Islas Vírgenes EEUU) y termina en *Saint Thomas* (Islas Vírgenes EEUU). La capacidad contratada por Pacifictel y Andinatel es de 40 E-1, actualmente saturado se estima que la demanda actual es de 250 E-1.

Internet Móvil: En enero de 2001, BellSouth propone una nueva dimensión de servicios móviles al fusionar el mundo móvil y el mundo de la información, al establecer el portal inalámbrico. El Internet móvil permitió optimizar tiempo y recursos, además de acceder, actualizar, controlar y revisar, desde cualquier punto donde se encuentre el usuario, la agenda personal, la lista de contactos o información requerida.

La Tecnología en la Educación: En junio de 2001 se lanzo el proyecto digital “Educanet” del Municipio de Quito, con el objetivo de promover la inclusión y

participación de las escuelas y colegios de la Ciudad en la vida tecnológica del país, dotándoles de equipos y centros de computo a los alumnos, y capacitación informática a los maestros.

Agenda de Conectividad: En agosto 2001, se aprueba el reglamento especial a la ley de telecomunicaciones y el uso del espectro radioeléctrico. Además se presento la Agenda Nacional de Conectividad para garantizar un acceso democrático a los beneficios y oportunidades de la Sociedad del Conocimiento, cuyos puntos se replantearon años mas tarde con la presentación del "libro blanco", estructurado por Juan Carlos Solines en ese entonces presidente del CONATEL. En septiembre de ese mismo año se aprueba el reglamento para la provisión de Segmento Espacial de Sistemas de Satélites Geoestacionarios, a fin de regular y establecer los requisitos y procedimientos para facilitar servicios de telecomunicaciones en el país o en conexión con el exterior.

ADSL el nuevo Internet: En diciembre del 2001, Andinatel y Alcatel presentaron la tecnología de Internet ADSL, que permitió una conexión similar a la de banda ancha con la diferencia que no necesita de fibra óptica o líneas dedicadas, sino que utiliza los cables de cobre que están instalados en la mayor parte del país.

Pago por Internet y Libre competencia de Telecomunicaciones: En el 2002 la Empresa Metropolitana de Agua Potable y Alcantarillado de Quito, ofreció a través de su página web pagos por Internet a los usuarios. En enero de este mismo año se hizo oficial la Apertura del Mercado de las Telecomunicaciones que inicia la libre competencia con el proceso de subasta de las redes de acceso inalámbrico de tecnología Wireless Local Loop (WLL).

Internet en PDA: En febrero de 2002 BellSouth, Wireless Solutions e Internet móvil juntaron su tecnología para ofrecer a los usuarios el servicio de Internet móvil PDA. El servicio permite que los usuario se conecten a través de un dispositivo de bolsillo a la red sin computadores o líneas telefónicas, solo utilizando CDPD para el manejo de datos en forma inalámbrica; pero solo se podía acceder a ciertas paginas.

Ley de Comercio Electrónico: En abril del 2002 el Congreso Nacional aprobó la ley de Comercio electrónico, firmas electrónicas y mensajes de datos. El

documento original fue presentado por la corporación Ecuatoriana de Comercio Electrónico CORPECE.

Internet con Cable Panamericano: En el 2003 inicia el uso de fibra óptica internacional, a través de telefónica Perú. Hasta entonces Internet se valía de enlaces satelitales. Otro enlace se abrió por el norte con Trasnnexa-Internexa de Colombia.

Planes de Masificación de Internet: En enero del 2003 el CONATEL, aprobó la tarifa plana para permitir la masificación del uso de Internet, bajo dos modalidades: tarifa plana ilimitada y la tarifa plana restringida. Lastimosamente, nunca llegó a implementarse.

Alegro la empresa Celular del Estado: En abril del 2003 Andinatel y Pacifictel crearon la compañía de telecomunicaciones móviles del Ecuador Telecsa. Inicialmente su capital estaba 50% en manos de cada compañía, pero Andinatel siempre mantuvo el control mayoritario. Actualmente, la Corporación Nacional de Telecomunicaciones, mantiene el total del paquete accionario de la empresa.

Ecuador y Colombia Interconectados: En julio del 2003 Transelectric inauguró oficialmente la subestación Pomasqui que permitió la interconexión eléctrica entre Ecuador y Colombia. El proyecto tuvo una inversión de 35 millones de USD y permitió exportar energía y cubrir las necesidades eléctricas de los dos países.

Tv en Internet: En junio de 2005 la empresa GameproTV presentó la primera televisión Online de videojuegos en español totalmente gratuita. De esta manera inició otra manera de entender Internet.

Popularización de redes Inalámbricas: En el 2006 comienza el abaratamiento de la tecnología. Unificación de redes a Ethernet e IP a través de medios guiados (fibra, cobre) o inalámbricos como WiFi, Wi-Max para acceso a Internet sin cables, y tecnología digital de telefonía móvil (CDMA y GRPS). En octubre del mismo año el CONATEL y la SENATEL, presentaron la Norma de Calidad de Servicio de valor agregado de Internet en Ecuador, para brindar una mejor prestación y apoyar al usuario en el respeto de sus derechos.

Cable Submarino en Ecuador: En noviembre del 2007 después de un año de gestiones, se suscribió el acta entre la Superintendencia de Telecomunicaciones y TIWS -Telefónica Internacional Wholesale Services Ecuador S.A.-, por 20 años. La operación del Sistema de Cable Submarino se ubicó en la estación de amarre, localizada en la parroquia José Luis Tamayo, vía a Punta Carnero. En operación, el enlace tiene una capacidad de 10 Gb., para permitir una rápida conectividad; además se promueve una baja en los costos para el acceso a Internet en al menos 30%.

Decreto Sobre Software libre: El presidente de la república, Rafael Correa, mediante decreto del 10 de abril del 2008, establece como política pública para las entidades de la administración pública central la utilización de Software Libre en sus Sistemas y equipamientos informáticos.

CNT: Mediante escritura pública otorgada ante el Notario Décimo Séptimo del Cantón Quito, se procedió a efectuar la fusión de las compañías ANDINATEL S.A. y PACIFICTEL S.A. y la creación de la Corporación Nacional de Telecomunicaciones CNT, inscrita en el Registro Mercantil el 30 de octubre de 2008.

1.2 CONCEPTOS PREVIOS

1.2.1 CONCEPTO DE REDES CORPORATIVAS

Las redes corporativas son un conjunto de computadores conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos que comparten información[5] en puntos dispersos geográficamente, pudiendo también estar ubicados en el mismo edificio. Un claro ejemplo de una red corporativa es un Banco donde la Matriz, esta intercambiando constantemente información con agencias ubicadas en otros sectores conocidas como Sucursales. En un sentido más simple seria la Interconexión de Redes de Área Local.

[5] Se puede además compartir recursos y servicios. Pero no tendría sentido hacerlo por que se saturaría innecesariamente el enlace ya que se los puede compartir localmente dentro de la LAN.

1.2.2 DIRECCIONAMIENTO

El direccionamiento, es parte fundamental en el Internet ya que ayuda al protocolo TCP/IP a ocultar los detalles de las redes físicas y hace que el Internet parezca una sola red uniforme. Para que el Sistema de Comunicaciones sea Universal, se necesita de un método aceptado de manera global para identificar cada computadora que se conecta a él (Identificadores Universales). Esto se consigue con el direccionamiento IP. *"En el protocolo IP se especifica un punto de unión en la red llamado interfaz .Una máquina puede tener múltiples interfaces, teniendo una dirección IP por cada una de ellas , las interfaces son por lo general conexiones físicas distintas, pero también pueden ser conexiones lógicas compartiendo una misma interfaz"*[6].

1.2.3 INTERCONEXIÓN DE REDES DE ÁREA LOCAL

En muchas ocasiones es necesario interconectar redes de Área Local, para sacar el máximo rendimiento de sus capacidades. Para conseguir esto la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar que características posean.

El objetivo de la Interconexión de Redes (*internetworking*) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios[7].

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.

---

[6] Tomado de www.gfc.edu.ec
[7] www.monografias.com

- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

Los problemas que suelen presentarse en las redes Tradicionales son:

- Recursos compartidos
- Rendimiento depende del número de usuarios
- No hay seguridad
- Broadcast y Multicast

La solución a este problema es segmentar[8] la red, utilizando una de las siguientes opciones:

- Bridging
- Switching
- Routing

1.2.3.1 Dominios

En una *Internetwork* se definen dos tipos de Dominios:

- Dominios de Colisión.
- Dominio De Broadcast

1.2.3.1.1 Dominios De Colisión

Trabaja en la capa de Enlace, es aplicable para redes que utilizan el método de acceso al medio CSMA/CD (Carrier sense Multiple Access with Collision Detection).

Define al grupo de equipos conectados a un medio físico (bus de datos) que se ven directamente afectados por una colisión del canal.

[8] Dividir un Dominio

1.2.3.1.2 Dominios De Broadcast

El control del Broadcast es uno de los principales problemas a solucionarse ya que suele llegar hasta la capa de Aplicación (procesador).

Trabaja en capa red, indica el alcance que tiene el tráfico de Broadcast en una red o subred lógica.

Por lo general, estos dominios se hallan limitados por enrutadores.

Un mismo Dominio de Broadcast puede estar formado por varios dominios de colisión, conectados entre sí mediante un Bridge (o un switch).

1.2.3.2 Bridging

Es una tecnología que permite interconectar segmentos de redes de Área local (LAN), con el propósito de simular un único segmento más grande.

- El equipo que interconecta los segmentos se denomina **Bridge** (puente).
- Esta tecnología trabaja en las dos capas inferiores del Modelo OSI, es decir la capa Física y la capa de Enlace, lo cual le hace independiente de cualquier estructura lógica de una red y de la acción y condiciones de los protocolos enrutados.
- Ya que trabajó en la capa Enlace, utiliza como información para los procesos que realiza las direcciones físicas; específicamente, las direcciones MAC.
- Al dividir una red Ethernet en varios segmentos, se consigue reducir la cantidad de tráfico en cada uno de ellos, disminuyendo las colisiones, e incrementando el ancho de banda estadístico para cada elemento.
- Al dividir una red Token Ring en varios anillos, se reducen los tiempos de espera.

Tipos de Bridging: Un enrutador puede utilizar varios tipos de Bridging, los cuales le permitirán transmitir la información de un protocolo no enrutado de un puerto a otro del equipo. Estas alternativas están relacionadas directamente con

las características físicas de los puertos y con ciertas funciones que podría realizar un enrutador en capa de red.

- Transparent Bridging (TB)
    - Utilizado para conectar segmentos Ethernet u 802.3
    - La operación del Bridge es transparente para los equipos de la red, pudiendo considerarse que ellos se encuentran conectados por un canal físico contiguo.
    - Esta solución mejora el rendimiento de un dominio de Broadcast, reduciendo la cantidad de colisiones del canal.
    - Los equipos de la red no tiene conocimiento de la existencia del Bridge.
- Integrated Routing and Bridging (IRB)
    - Permite agrupar a todos los puertos del enrutador que realizan funciones del Bridging, y dotarles de presencia ante una red lógica.
- Source-route Bridging (SRB)
    - Desarrollado por IBM para las redes Token Ring.
    - El camino completo hacia un destino es determinado por equipo origen previo a que los datos sean transmitidos a la red.
- Source-route Transparent Bridging (SRT)
    - Realiza tares de TB y SRB.
    - El tráfico que tiene la información de una ruta es manejado con SRB, y el que no tiene esta información, con TB.
    - Este método no realiza traslación.
- Source-route Translation Bridging (SR/TLB)
    - Permite interconectar redes Ethernet con Token Ring.

- Hace traslación de tramas.

- Encapsulated Bridging

  - Utilizado para conectar de segmentos de red mediante canales independientes de datos, por ejemplo FDDI o enlaces seriales.

  - En el caso de los enlaces seriales, estos pueden utilizar, a nivel de Capa enlace cualquier protocolo de encapsulación, por ejemplo HLC, Frame Relay, etc.[9]

1.2.3.2.1 Transparent Bridging[10]

La operación de esta tecnología involucra las siguientes etapas o funciones:

1. Aprendizaje de los equipos de conectados a los puertos del Bridge.
2. Transmisión (e inundación) de tramas
3. Administración de lazos en topologías cerradas.

1.- Aprendizaje:

Cuando un Bridge es conectado por primera vez a una red, o es encendido, no tiene conocimiento alguno de la red. Por lo mismo. La primera tarea que realiza es elaborar una tabla de direcciones la cual relaciona las direcciones MAC de los equipos, con el puerto del Bridge al cual se halla conectados, esto lo logra revisando el campo de la dirección origen de todas las tramas que le llegan, el equipo actualiza el contenido de la tabla cada vez que recibe una trama de un equipo desconocido, cada entrada en la tabla se encuentra relacionada con un temporizador, el temporizador de una entrada se encera cada vez que el Bridge recibe una trama del equipo al que hace referencia dicha entrada, si un equipo deja de enviar información durante un tiempo, el Bridge elimina su dirección de la tabla, esta información es utilizada en los procesos de la transmisión.

---

[9] Lo referente a Bridging ha sido tomado de un manual de ”Uniplex” de un curso de configuración de Switch administrables que lo recibí en la DINSE

[10] Debido a que los equipos concentradores en la DINSE soportan Transparente Bridging, es necesario profundizar en este tema.

2.- Transmisión e Inundación

La transmisión es el proceso por el cual un Bridge copia una trama que recibió por uno de sus puertos, en otro.

La transmisión sigue un procedimiento conocido como Store and Fordward.

En este, el bridge recibe primero toda la trama antes de transmitirla.

Una vez que la trama ha ingresado completamente al equipo, este revisa si hay algún error en ella. En caso de encontrar problemas con el campo FCS, desecha la trama.

Si el FCS es el correcto, revisa la dirección MAC de destino para determinar que acción debería tomar.

Este proceso introduce un retardo igual al tiempo de llegada de la trama, mas el procesamiento de transmisión. Por lo general este último valor se encuentra en el orden de los cinco microsegundos.

Hay tres posibilidades al momento de decidir la transmisión, todas relacionadas con el contenido de la tabla de direcciones:

a) Si la dirección MAC destino de la trama no se halla en la tabla.

- El Bridge transmite la trama por todos los puertos, con excepción del puerto por el cual fue recibida.
- Este proceso se conoce como **flooding.**
- El Bridge espera que el equipo que origino la trama reciba una respuesta del destino desconocido para poder determinar el puerto al que se halla conectado, con lo cual no es necesario realizar nuevamente el flooding.
- En este caso se encuentran todos los paquetes de Broadcast que se generen en la red, ya que su dirección MAC de destino es igual a 0*FFFF,FFFF,FFF; la cual nunca se hallara en una trama como dirección física de origen.

b) Si la dirección MAC destino de la trama se halla en la Tabla, y está relacionada con un puerto diferente al puerto de ingreso de datos.

- El Bridge copia la trama en el puerto donde se encuentra el equipo de destino.

c) Si la dirección MAC destino de la trama se halla en la tabla, y está relacionada con el mismo puerto de ingreso de datos.

- El Bridge desecha la trama.
- Este proceso se denomina filtrado.

3.- Administración de lazos

Topología de lazo cerrado

Una topología de lazo cerrado es aquella en la cual existen dos o más caminos disponibles, para llegar a un mismo segmento.

- Este tipo de Topologías es utilizado fundamentalmente para dotar de redundancia a los enlaces con lo cual se mejora la confiabilidad.
    - Si una red no dispone de redundancia, en el momento en que uno de los equipos deja de trabajar, el enlace se cae y se pierde la conectividad.
- Sin embargo la redundancia puede convertirse en un problema si no hay una forma de controlar el proceso de transmisión del Bridge.
    - Por ejemplo, si un paquete generado en el equipo B tiene como destino el C, al pasar por los equipos redundantes se generaran dos copias del mismo mensaje.
    - Esta duplicación trae como principal desventaja el consumo de recursos, tanto en el canal del dominio de colisión de destino, como en el CPU del equipo, el cual tendrá que procesar el duplicado, aunque luego o deseche.

- Un problema aun más grave que la duplicación del mensaje de red de destino, es el desencadenado por los paquetes de Broadcast.
    - Cuando un Broadcast aparece en uno de los segmentos y llega a un Bridge, este lo transmitirá por todos los puertos.
    - Una vez en los otros segmentos, el paquete llegara a los equipos redundantes, los cuales los copiaran otra vez en el resto de sus puertos.
    - Nuevamente, en los siguientes segmentos, donde ocurrió la segunda copia, se repetirá el proceso de transmisión y así sucesivamente.
    - Este error se conoce como **Broadcast Storm,** en estas condiciones, se puede llegar a saturar tanto los recursos de los canales, como el procesador de los equipos de la red, ya que un Broadcast es procesado en la Capa de Aplicación.
    - Para corregir el Broadcast Storm se desarrollo el protocolo **Spanning Tree** el cual permite que los Bridges negocien automáticamente con el fin de eliminar los caminos redundantes deshabilitando puertos de los equipos.
    - En este escenario si el Bridge que conecta dos segmentos de red (esto es, el que tiene habilitados todos sus puertos) llega a fallar, el camino redundante se habilita automáticamente, manteniendo la conexión entre segmentos.

Protocolo Spanning Tree

A grandes rasgos, el comportamiento del Spanning Tree es el siguiente:

- El protocolo selecciona a un equipo raíz, basándose en el valor de un identificador.
    - El Bridge con el menor identificador será la raíz.

  - El identificador consta de ocho bytes. Los primeros dos bytes pueden ser configurados por el administrador. Los últimos seis contienen la dirección MAC de alguna de la interfaces del equipo.
  - Si el administrador decide configurar el campo de prioridad (los dos bytes mencionados), debería escoger como raíz a un equipo que se encuentre lo más cerca del centro de la red. Con esto se consigue incrementar la eficiencia de la Topología.

- Cada Bridge selecciona el camino de menor costo hacia el equipo raíz.
- Los interfaces para los caminos alternos son deshabilitados.

Estados de puertos en STP (Spanning Tree Protocol)

- Bloqueado (Blocked)
  - Al iniciar el switch
- Escuchando (Listening)
  - Esperando mensajes STP para asegurarse de que no hay bucles de que no hay bucles
- Aprendiendo (Learning)
  - Recibiendo tramas y guardando direcciones MAC en la tabla
- Reenviando (Forwarding)

En otras palabras la meta es apagar puertos redundantes y formar un árbol jerárquico.

1.2.3.3 Switching

El Switching es la evolución del Bridging, es el uso de un dispositivo (Switch) que trabaja en a nivel de Capa 2, se puede decir que es un Bridge multipuerto.

Ventajas

- Rápido

    - Switch implementa los algoritmos en ASICS
    - ASIC: Application- -Specific Integrated Circuit
    - No inspecciona el paquete IP
    - No modifica la trama
- Permite combinar enlaces distintos
    - Mayores velocidades para tráfico agregado
- Reducción del Dominio de Colisión.
    - Cada puerto es un Domino de Colisión
    - Las tramas se envían solo a través del puerto correspondiente.
    - Aumento del ancho de banda disponible a cada estación.
    - Reducción de la carga innecesaria del CPU de las estaciones
    - Seguridad ya que no permite ver el tráfico de otros usuarios.

Limitaciones

- No limita el Domino de Broadcast
- No limita el tráfico multicast
    - Actualmente existen soluciones que permiten solucionar estos inconvenientes, aunque originalmente el Switching no lo permitía.
    - IGMP Snooping
    - PIM Snooping
- Susceptible a bucles
    - Esto se resuelve utilizando Spanning Tree
        - Esto aumenta la complejidad
        - Puede tener convergencia lenta.

Funciones básicas

- Aprendizaje de direcciones
- Tabla de direccionamiento vacía al inicio
- Cada dirección MAC origen nueva se agrega a la tabla, indicando el puerto donde se recibió la trama.
- Reenvío (Fordwarding)
    - Se inspecciona la dirección destino en cada trama.
    - Si la dirección se encuentra en la tabla, la trama se reenvía solamente a través del puerto correspondiente.
    - Si no, la trama se reenvió a través de todos los puertos
    - Cuando el destinatario responde, su dirección origen se agrega a la tabla.
- Control de bucles
    - Pueden darse por dos razones:
        - Error Humano (confusión con el cableado)
        - Para proveer redundancia
    - Si no hubiera un mecanismo de control
        - Broacast Storm
        - Imposibilidad de aprendizaje de Direcciones.

1.2.3.3 Routing

Entre las funciones que tiene el Routing, la principal seria que permite conectar redes lógicas, como pueden ser Vlan’s. Redes de diferente direccionamiento.

Características

- Trabaja en la capa de Red
- Utiliza como información direcciones lógicas: IP, IPX, Apple Talk.
- Permite:
    - Realizar la transmisión con mejor rendimiento
    - Aislar dominios de Broadcast
    - Interconectar redes LAN de diferentes características
    - Mayor control y administración
    - Implementar funciones de control de flujo, errores, fragmentación, tiempo de vida del tráfico.
    - Mantener varios caminos alternos.

Tipos de Enrutamiento

- Enrutamiento Estático
    - Rutas ingresadas por el administrador
- Enrutamiento dinámico
    - Utilización de protocolos de enrutamiento para generar Tablas de Rutas.

Conmutación

Una red completamente aislada de otra red TCP/IP requiere solo de rutas mínimas. Las rutas mínimas son creadas por el comando ifconfig al momento de configurar una interfaz. Las rutas mínimas son: la ruta de red local y la ruta para loopback. En linux es necesario crear la interfaz y la ruta.[11]

---

[11] Tomado BERT HUBERT, Msc. "Enrutamiento avanzado y control de tráfico en Linux"
Asumiendo que una de las alternativas seria la implementación con Linux, se hace necesaria esta aclaración.

1.2.4 RFC

Las Request For Comments —petición de comentarios— son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Se abrevian como RFC.

Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

Cualquiera puede enviar una propuesta de RFC a la IETF, pero es ésta la que decide finalmente si el documento se convierte en una RFC o no. Si luego resulta lo suficientemente interesante, puede llegar a convertirse en un estándar de Internet.

Cada RFC tiene un título y un número asignado, que no puede repetirse ni eliminarse aunque el documento se quede obsoleto.

Cada protocolo de los que hoy existen en Internet tiene asociado un RFC que lo define, y posiblemente otros RFC adicionales que lo amplían. Por ejemplo el protocolo IP se detalla en el RFC 791, el FTP en el RFC 959, y el HTTP (escrito por Tim Berners-Lee, entre otros) el RFC 2616.

Existen varias categorías, pudiendo ser informativos (cuando se trata simplemente de valorar por ejemplo la implantación de un protocolo), propuestas de estándares nuevos, o históricos (cuando quedan obsoletos por versiones más modernas del protocolo que describen).

Las RFC se redactan en inglés según una estructura específica y en formato de texto ASCII.

Antes de que un documento tenga la consideración de RFC, debe seguir un proceso muy estricto para asegurar su calidad y coherencia. Cuando lo consigue, prácticamente ya es un protocolo formal al que probablemente se interpondrán pocas objeciones, por lo que el sentido de su nombre como petición de comentarios ha quedado prácticamente obsoleto, dado que las críticas y

sugerencias se producen en las fases anteriores. De todos modos, el nombre de RFC se mantiene por razones históricas[12].

1.3 TIPOS DE REDES

Se puede clasificar las redes en cuanto a las dimensiones de la tecnología de transmisión y del tamaño.

1.3.1 RED PÚBLICA

Una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica[13].

1.3.2 RED PRIVADA

Una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

1.3.2.1 Red Privada Física

Una red privada física, es una conexión a través de un enlace "contratado" que permite enlazar dos puntos distantes geográficos de manera controlada. Uno de los ejemplos que podríamos citar son los servicios que ofrecen, los proveedores de transmisión de datos, únicamente para grandes empresas, como canales dedicados. En este caso el acuerdo de nivel de servicio garantiza un ancho de banda predefinido y no el servicio únicamente.

1.3.2.2 Red Privada Virtual

La Red Privada Virtual (Virtual Private Network) (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de

---

[12] Tomado de http://es.wikipedia.org/wiki/
[13] Tomado de TOBY SCANDIER, "Guía del estudio de redes, cuarta edición"

soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

1.3.3 RED DE ÁREA PERSONAL (PAN)

(Personal Area Network) es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las PDA) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales del mismo usuario (comunicación intrapersonal), o para conectar con una red de alto nivel y el Internet (un up link)[14]. Las redes personales del área se pueden conectar con cables, con los buses de la computadora tales como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.

1.3.4 LAN –LOCAL AREA NETWORK- (RED DE ÁREA LOCAL)

Una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización.

1.3.5 CAN -RED DEL ÁREA DEL CAMPUS-

Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

1.3.6 MAN -RED DE ÁREA METROPOLITANA-

Es una red que conecta las redes de un área (dos o más redes locales juntas) pero no se extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Los enrutadores múltiples, los switch y los hubs están conectados para crear una MAN.

---

[14] Con esta opción es la que se pretende implementar el proyecto OLPC (One laptop per children), para que estos PC tengan conectividad entre si y a su vez acceso a Internet.

1.3.7 WAN –WIDE AREA NETWORK- RED DE ÁREA EXTENSA

Es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

1.3.7.1 Tipos De Redes Wan

1.3.7.1.1 Centralizada

Una WAN centralizada consiste en una computadora central que esté conectada con las terminales nodos y/u otros tipos de dispositivos del Terminal.

1.3.7.1.2 Distribuida

Una WAN distribuida consiste en dos o más computadoras en diversas localizaciones y puede también incluir conexiones a los terminales nodos y a otros tipos de dispositivos del Terminal.

1.3.8 REDES INALÁMBRICAS

Los computadores portátiles son el segmento más rápido de crecimiento en la industria de la computación. Los usuarios móviles de estos pequeños computadores quieren estar conectados en línea a su base de operaciones y necesitan obtener datos para sus aplicaciones sin estar atados a las comunicaciones terrestres. En algunos casos el obtener una conexión por cable es imposible, el ejemplo típico es un automóvil, por lo tanto se encuentra su interés en las redes inalámbricas.

Se basan en el principio de conectar una antena a un circuito eléctrico en donde las ondas electromagnéticas se difunden para captarse en un receptor a cierta distancia.

Las redes inalámbricas son de gran importancia para los transportadores de carga pesada y pasajeros, vehículos de servicios público, personas que efectúen

reparaciones en sitios de difícil acceso, y para las organizaciones militares, entre otras.

La instalación de redes inalámbricas es relativamente fácil, pero presentan algunas desventajas como su velocidad de transmisión y recepción, la cual es mucho más lento que en las redes de área local y redes de largo alcance. En algunas ocasiones las redes inalámbricas presentan interferencias de comunicaciones.

Algunas de las características más notables de este tipo de RED son:

- Una red inalámbrica usa radio, microondas, satélites, infrarrojo, u otros mecanismos para comunicarse.
- Se pueden combinar las redes inalámbricas con los computadores móviles, pero los dos conceptos son distintos.

CAPITULO 2: REDES PRIVADAS VIRTUALES (VPN)

2.1 CARACTERÍSTICAS

La integración de Redes Locales, es posible gracias al costo accesible de las conexiones a Internet, sumado actualmente a la disponibilidad de alta velocidad en la transmisión de datos. Una solución práctica y relativamente a bajo costo es el uso de VPN`s –Virtual Private Network-(Red Privada Virtual).

2.1.1 DEFINICIÓN

Una Red Privada Virtual consiste en la Interconexión de redes dispersas existentes "…*utilizando sus enlaces a Internet con una relación de confianza (Configurable) entre las mismas, y niveles de autenticación y cifrado*"[15].

"*Es una Red de carácter privado, perteneciente a una organización, que se extiende usando medios cuya propiedad o explotación corresponde a otras redes/entidades de ámbito público, codificando el tráfico que ha de transitar por esos intermediarios.*[16]"

La VPN permite ver a la red resultante como algo homogéneo y simple, y lo más importante transparente a los usuarios finales y las aplicaciones, con la Seguridad de que la información transportada no está comprometida.

Para conseguir esa privacidad virtual, una VPN transfiere los datos entre dos redes a través de una red intermedia, mediante la encapsulación de los paquetes de datos dentro de otro protocolo, que en el caso de Internet se trata de TCP/IP.

Hoy en día las VPN's han añadido una nueva dimensión en la encapsulación utilizando métodos de encriptación.

2.1.2 FUNCIONAMIENTO

Una Red Privada Virtual se basa en un protocolo denominado Protocolo de Túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.

---

[15]Tomado VICENTE JOSÉ AGUILAR, Ing. "Implementación de Redes Privadas Virtuales"
[16] Tomado de JUAN BLÁZQUEZ MARTIN, Msc. "Redes Privadas Virtuales: Poner puertas al campo"

La palabra túnel se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran en la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que cifra y descifra los elementos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la VPN, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y este envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

2.1.3 TÚNEL

Un túnel es un canal virtual, configurado entre dos sistemas remotos que se encuentran en diferentes redes, sobre una conexión real que involucra más de un nodo intermedio.

La VPN utiliza técnicas de *tuneling* encapsulando unos datos que son encriptados, de tal forma que esa información resulta imposible de interpretar por quien no es parte de esa VPN establecida; así, los datos pueden enrutarse por Internet con garantías suficientes de que solo podrán ser interpretados en el destino, en donde los paquetes de datos serán extraídos y traducidos a su formato original. Los procedimientos de autentificación que se implementan en esta tecnología, refuerzan la seguridad frente a intrusos y usuarios no autorizados, proporcionando además, los mecanismos de control necesarios para su total gestión.

La técnica de *tuneling* consiste básicamente "*en encapsular un mensaje de un protocolo dentro de sí mismo aprovechando ciertas propiedades del paquete externo con el objetivo de que el mensaje sea tratado de forma diferente a como habría sido tratado el mensaje encapsulado. De esta forma el paquete puede saltar la topología de una red. Por ejemplo, un túnel puede ser usado para evitar*

un firewall (con los peligros consecuentes de esta decisión). Esta es una consideración a tener en cuenta al configurar un túnel[17]*."*

El túnel es creado encapsulando un protocolo de red dentro de los paquetes del mismo protocolo, que serán llevados por la red real. Adicionalmente, el paquete encapsulado es encriptado por el emisor, en acuerdo con el receptor (el sistema que se encuentra del otro lado del túnel) de manera que solo ambos extremos puedan acceder a los datos transportados. Éste tipo de comunicación solo es posible si el protocolo soporta esta facilidad, denominada modo túnel. La otra modalidad posible, modo transporte, provee protección solo para protocolos de la capa superior.

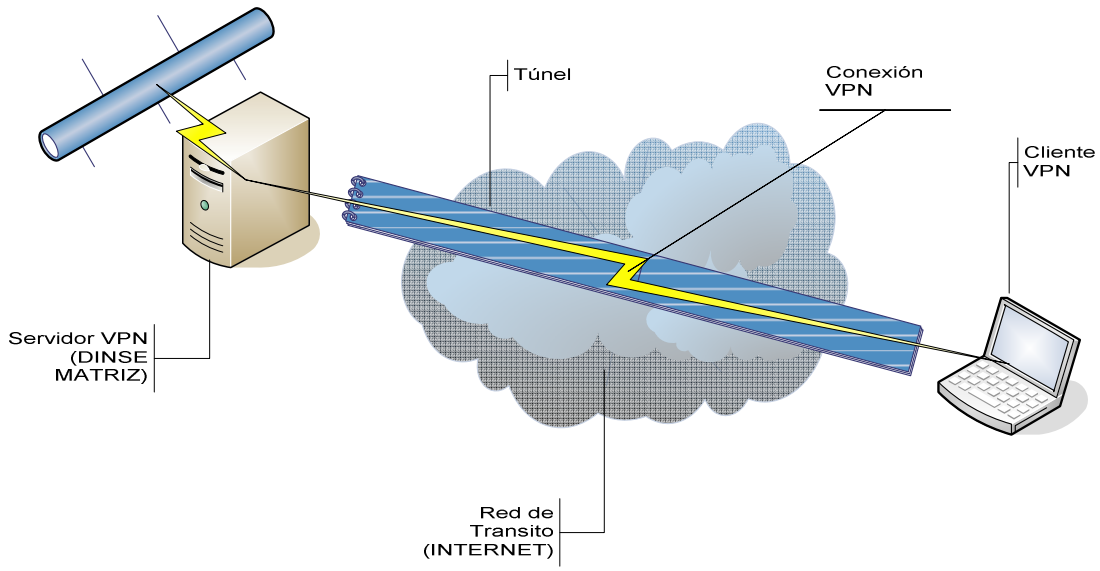

Figura 2.1 Ilustración Concepto de Tuneling

De esta forma, el túnel es simplemente la ruta que toman los paquetes encapsulados (y encriptados), dentro de un paquete del mismo protocolo, entre las dos redes (Fig. 2.1). Un atacante puede interceptar los mensajes que viajen por el túnel, pero los datos encapsulados están encriptados y solo pueden ser recuperados por el destinatario final.

[17] Tomado de http://es.wikipedia.org/wiki/Red_privada_virtual.

Con el uso del modo túnel, el encabezado IP interno (encapsulado) es encriptado, ocultando la identidad del destinatario y del origen del tráfico. Los mismos servicios pueden ofrecerse a un usuario móvil al cual se le asigna una IP dinámicamente para una conexión de acceso telefónica: se establece un canal en modo túnel al firewall del ISP funcionando como un Gateway de seguridad. Es decir permite evitar el firewall del ISP pero a su vez el túnel está configurado de tal manera que la seguridad que brinda al tráfico está garantizada comportándose como una pasarela de seguridad del ISP.

"En relación con una conexión o canal seguro, cabe introducir un concepto importante: el de Asociación de Seguridad (Security Asociation - SA). Una asociación de seguridad (AS) es una instancia de una política de seguridad junto con componentes claves. Las SAS son identificadas de forma única por una dirección de destino, un protocolo de seguridad y un índice de parámetros de seguridad o SPI (un conjunto de atributos se seguridad). Las SAS son independientes entre ellas. Una conexión de datos protegida necesita un conjunto de SAS, una por cada dirección y protocolo. Las SAS pueden actuar en una dirección o en ambas. Una SA en modo túnel es una SA aplicada a un túnel, por ejemplo, un túnel IP.

Siempre que en una asociación de seguridad esté involucrado un gateway de seguridad, dicha SA debe operar en modo túnel; de otra forma, si sólo están involucrados sistemas finales (o gateways de seguridad que no actúen como tales –no transporte tráfico de datos, por Ej. comandos SNMP para administración de red –), puede operar también en modo transporte. Por esto, un sistema final (un host) también debe soportar ambos modos de operación, transporte y túnel (ya que puede comunicarse con un gateway, que operará en modo túnel)."[18]

[18] Tomado de http://es.wikipedia.org/wiki/Red_privada_virtual

2.1.3.1 Tipos De Túnel

Entre los requerimientos básicos con los que debe cumplir un protocolo de túnel se tiene:

1. Autenticación de usuario.
2. Asignación dinámica de direcciones
3. Compresión de datos
4. Encriptación de datos
5. Administración de llaves
6. Soporte multiprotocolo

2.1.3.1.1 Túneles Voluntarios

Un usuario o una estación de trabajo cliente puede emitir una petición de conexión a la VPN para configurar y crear un túnel voluntario. En este caso, el usuario es un terminal del túnel y actúa como el cliente del mismo.

2.1.3.1.2 Túneles Compulsivos

Una VPN con servidor con capacidad de acceso por llamada, configura y crea un túnel, donde el usuario no es un terminal del mismo. Otro dispositivo, el RAS –remote access server-(Servidor de acceso remoto), entre la computadora usuario y el servidor de túnel es la terminal del túnel y actuara como cliente.

2.1.3.2 Protocolos De Túnel

Para la implementación de VPN se utilizan protocolos que trabajan a nivel de capa 2 y capa 3, se establece la conexión entre los dos puntos y se crea un túnel entre ellos como si fueran parte de la misma red.

2.1.3.2.1 Pptp -Point To Point Tuneling Protocol- (Protocolo De Túnel Punto A Punto)

Es una especificación de protocolo de capa 2 desarrollado por Microsoft, 3Com, *Ascend*, US *Robotics* y ECI *Telematics*. Se suele asociar a este protocolo con Microsoft, ya que Windows soporta este protocolo. La principal característica de PPTP es su habilidad para soportar protocolos no IP. Sin embargo, el principal

inconveniente es su fallo a elegir una única encriptación y autentificación estándar; dos productos que acceden utilizando PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

Lo que hace posible el PPTP es una extensión del acceso remoto del PPP (Protocolo punto a punto).[19] PPTP encapsula los paquetes PPP en datagramas IP para su trasmisión bajo redes basadas en TCP/IP.

PPTP soporta la implementación de VPN y una característica dentro de esto es que soporta VPN sobre RTPC (Red Telefónica Publica Conmutada), que comúnmente se los llama acceso telefónico a redes.

PPTP es una solución del acceso remoto para usuarios en continuo desplazamiento ya que proporciona seguridad y comunicaciones encriptadas sobre estructuras de área de trabajo existentes como RTPC o Internet.

En una distribución típica de PPTP comienza por un PC remoto o portátil[20] que será el cliente PPTP. Este cliente PPTP necesita acceso a la red privada utilizando un proveedor de servicios de Internet ISP (fig. 2). Los clientes que utilicen el SO Windows usaran el *dial – up networking* y el protocolo PPP para conectarse a su ISP. Al tener establecida la conexión el cliente tiene la capacidad para extraer datos de Internet. Los NAS – *Network Access Server* – (servidores de acceso a la red) usan el protocolo TCP/IP para el mantenimiento de todo el tráfico.

[19] El PPP esta definido en el RFC 1171
[20] Son también conocidos como Front – End Processors (FEP's) o Point-Of-Presence servers (POP's).

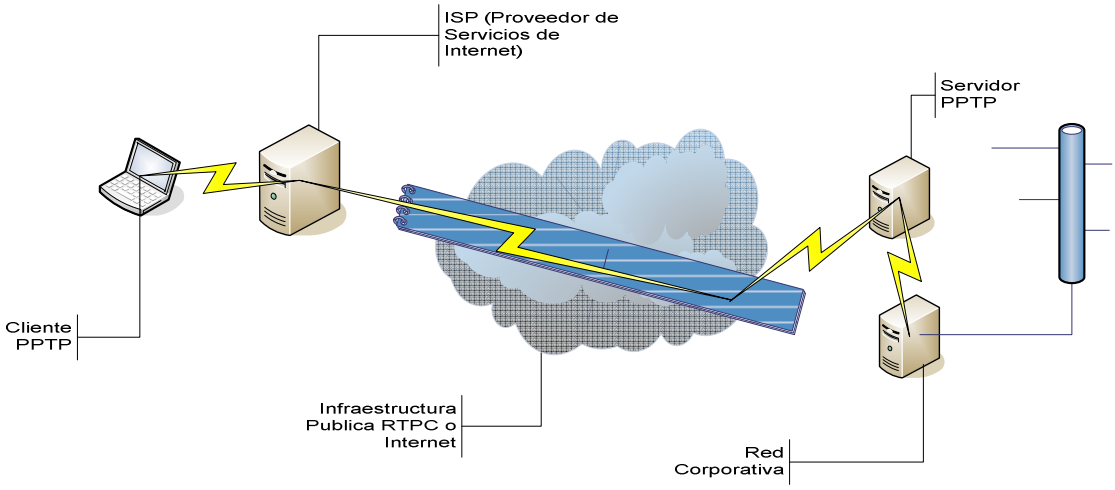

Figura 2.2 Ilustración Protocolo PPTP

Luego de que el cliente ha realizado la conexión PPP inicial al ISP, la segunda llamada Dial-up es hecha a través de la conexión PPP ya establecida. Los datos enviados usando la segunda conexión VPN a un servidor PPTP en la red privada de la compañía. Esto es el túnel propiamente dicho.

El tuneling activa el enrutamiento de la red para transmitir el paquete a un ordenador intermediario, como un Servidor PPTP. Este servidor está conectado a ambas, a la red privada de la compañía y a la red de enrutamiento que en este caso es el Internet.

Cuando el servidor PPTP recibe un paquete de la red de enrutamiento (Internet) lo envía a través de la red privada hasta el host de destino. El servidor PPTP hace esto procesando el paquete PPTP para obtener el nombre del PC de la red privada o la información de la dirección que esta encapsulada en el paquete PPP.

El paquete PPP encapsulado puede contener datos multi-protocolo como TCP/IP, IPX/SPX, NetBEUI. Debido a que el servidor PPTP está configurado para comunicar a través de la red privada usando protocolos de esta red privada, es capaz de entender multi-protocolos.

PPTP encapsula encriptado y comprimido el paquete PPP en datagramas IP para su transmisión a través de Internet. Estos datagramas IP son enrutados a través

de Internet como un paquete PPP y después son desencriptados usando el protocolo de red de la VPN.

Para establecer una comunicación segura usando PPTP son necesarios tres procesos, interrelacionados entre sí de tal manera que cada uno necesita de la ejecución del proceso anterior: Control y comunicación, Control de Conexión y *Tuneling* de datos.

Conexión y Comunicación PPTP: Un cliente PPTP utiliza PPP para conectarse a un ISP usando una línea telefónica normal o una línea RDSI. Esta conexión usa el protocolo PPP para establecer la conexión y encriptar los paquetes de datos.

Control de Conexión PPTP: Los mensajes de control son enviados dentro de los paquetes de control en un datagrama TCP. Una conexión TCP es activada entre el cliente PPTP y el servidor. Este path es usado para enviar y recibir mensajes de control. El datagrama contiene una cabecera PPP, una TCP, un mensaje de control PPTP y sus apropiadas reglas (Fig. 3).

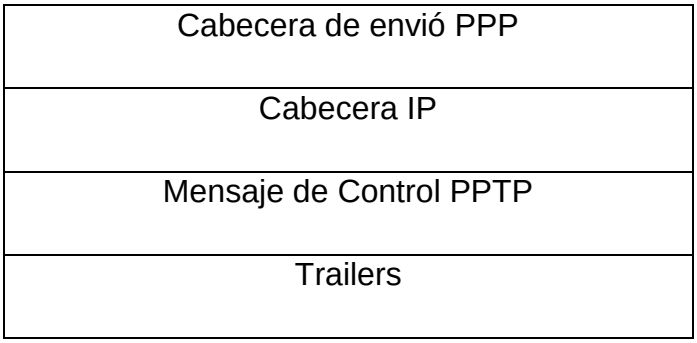

Figura 2.3 Estructura Datagrama TCP

Tuneling de datos PPTP: El protocolo PPTP crea datagramas IP conteniendo paquetes PPP encriptados que son enviados a través del túnel PPTP al PPTP servidor. El servidor PPTP desensambla los datagramas IP y desencripta los paquetes PPP, y reencamina los paquetes desencriptados a la red privada.

Transmisión de datos PPTP: Los datos son enviados en datagramas IP conteniendo paquetes PPP. El datagrama IP es creado usando una versión del protocolo GRE[21] –Generic Routing Protocol-.

Cabecera de envío del PPP
Cabecera IP
Cabecera GRE
Cabecera PPP
Cabecera IP
Cabecera TCP
Datos

Figura 2.4 Estructura del Datagrama IP

La seguridad con el PPTP utiliza la estricta autentificación y encriptación que se encuentra en los ordenadores que corren RAS (S.O. Windows Server).La autentificación inicial en la petición de conexión puede ser requerida por un ISP de NAS. Un servidor PPTP sería un gateway a nuestra red, y necesita la base estándar para ingresar usando un nombre de usuario y contraseña validos. Todos los clientes PPTP deben proporcionar un nombre de usuario y una contraseña. Dicho de otro modo loguearse de modo remoto es prácticamente igual a que un PC lo haga en una LAN.

La encriptación de los datos con PPTP se lo realiza usando el proceso de encriptación RAS *shared secret*[22] . El nombre de usuario y el password está disponible al servidor y sustituida por el cliente. Una llave de encriptación es generada usando una mínima parte del password situados en el cliente y el servidor. Esta llave es después usada para encriptar y desencriptar todos los datos transmitidos entre el servidor PPTP y el cliente. Los datos en los paquetes

[21] Protocolo definido en el RFC 1701-2
[22] Se lo conoce como *shared-secret* por que ambos terminan la conexión “compartiendo” la clave de encriptado.

PPP son encriptados. El paquete PPP que contiene un bloque de datos encriptados es después insertado en un datagrama IP para su enrutamiento.

La seguridad se mejora considerablemente activando el filtro PPTP en el servidor PPTP. Cuando el filtro PPTP esta activado, el servidor PPTP en la red privada acepta y encamina solo paquetes PPTP. Esto permite filtrar los paquetes de la red externa[23].

2.1.3.2.2 Ipsec –Internet Protocolo Security-

Este protocolo es en realidad una recolección de múltiples protocolos relacionados, un conjunto de estándares del IETF[24] para incorporar servicios de seguridad en IP. Tal es así que se lo puede usar como una solución de implementación completa de VPN o únicamente como un esquema de encriptación para LPT2 o PPTP.

Proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (como TCP y UDP). Al no ser un protocolo propietario proporciona un nivel de seguridad común y homogénea para todas las aplicaciones, además de ser totalmente independiente de la tecnología física que se emplee. Se integra en la versión Ipv4 y se encuentra por defecto en Ipv6.

Cumple con los requerimientos para la implementación de una VPN, confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de *hash* (MD5, SHA-1) y certificados digitales X509v3.

Aplicando IPsec se tiene acceso seguro y transparente de un nodo IP remoto, y permite la construcción de una red corporativa segura sobre redes públicas.

Se puede distinguir los siguientes componentes:

Dos protocolos de seguridad: IP *Authentication Header* (AH) e *IP encapsulating Security Payload* (ESP) que proporcionan los mecanismos de seguridad para mantener protegido al tráfico IP.

---

[23] El tráfico de datos PPTP utiliza el puerto 1723
[24] Internet Engineering Task Force --

Un protocolo de gestión de claves *Internet Key Exchange* (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión utilizando AH o ESP.

AH (Fig. 2.5): Es básicamente un protocolo que garantiza la integridad y autenticación de los datagramas IP excepto los campos variables[25]: TOS, TTL, *flags, offst, checksum*. Es una autenticación que se inserta entre la cabecera IP estándar y los datos transportados que puede ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo.

[25] Si garantiza (autenticidad e integridad) los datos transportados y la cabecera IP excepto lo mencionado.

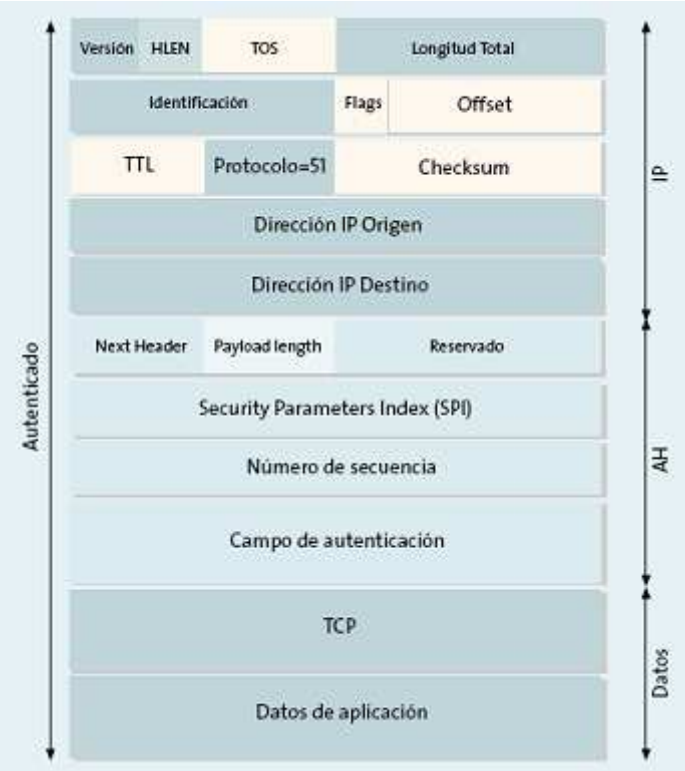

Figura 2.5 Estructura del Protocolo AH[26]

El emisor calcula (Fig. 2.6) un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete. Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado.

[26] Fuente: http://www.scribd.com/doc/34037219/Protocolos-VPN

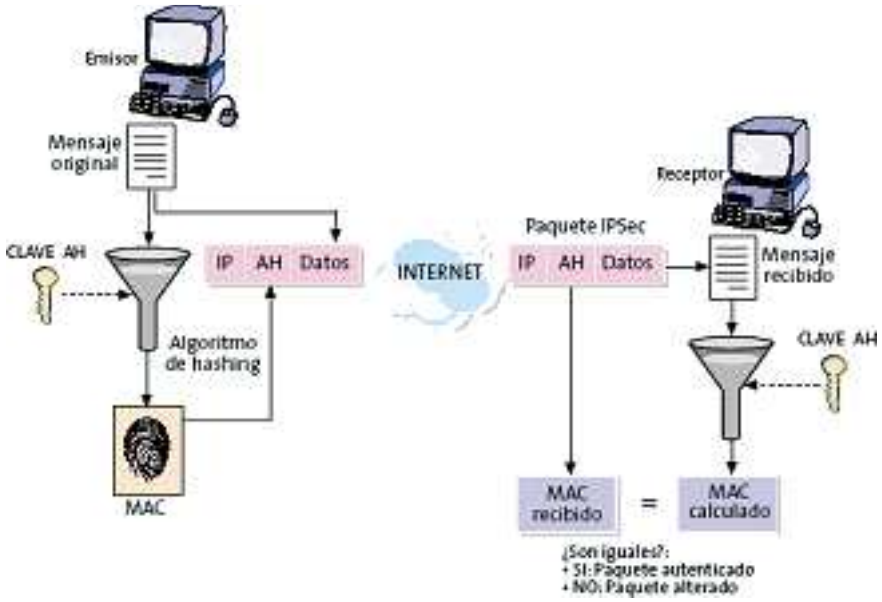

Figura 2.6 Funcionamiento del Protocolo AH[27]

ESP (Fig. 2.7): Sirve para proporcionar confidencialidad, para esto especifica el modo de cifrar los datos que se desean enviar y la forma en que este contenido cifrado se incluye en un datagrama. La cabecera así como la carga útil, están cifrados, un atacante que intercepte el paquete no podrá saber si el contenido es TCP o UDP. La función de cifrado es desempeñada por un algoritmo de clave simétrica.

[27] Fuente: http://www.scribd.com/doc/34037219/Protocolos-VPN

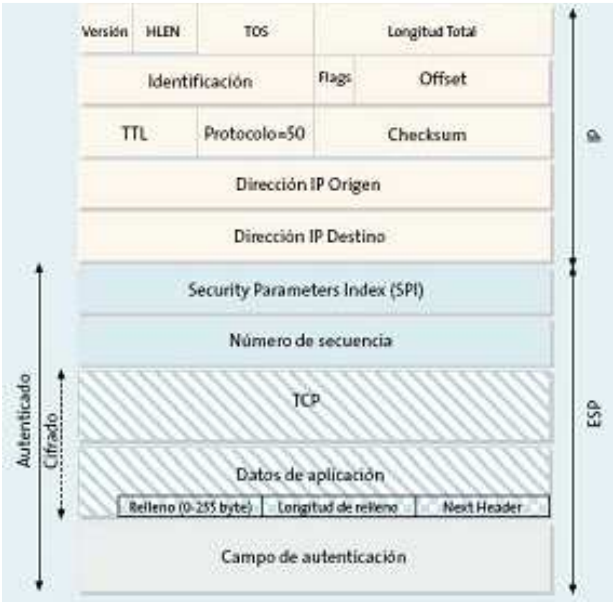

Figura 2.7 Estructura del Protocolo ESP

El funcionamiento de ESP es de la siguiente manera (Fig. 2.8): El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. La seguridad de este protocolo radica en la robustez del algoritmo de cifrado.

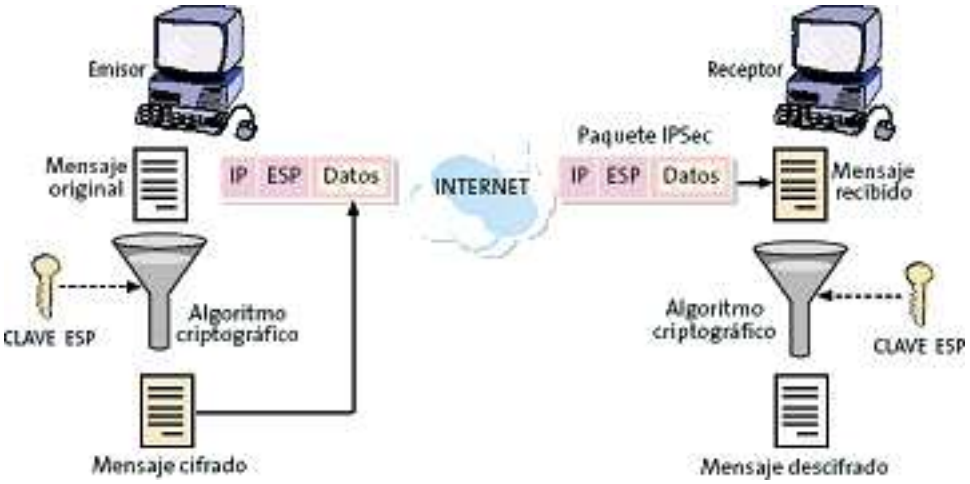

Figura 2.8 Funcionamiento del Protocolo ESP[28]

[28] Fuente: http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

El protocolo ESP puede funcionar en modo transporte así como en modo túnel. El modo transporte (Fig. 2.9) consiste en que, el contenido transportado dentro de un datagrama AH o ESP son datos de la capa transporte (TCP o UDP). La cabecera IPsec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. La ventaja del modo transporte es que asegura la comunicación extremo a extremo, para ello requiere que ambos extremos entiendan el protocolo IPsec.

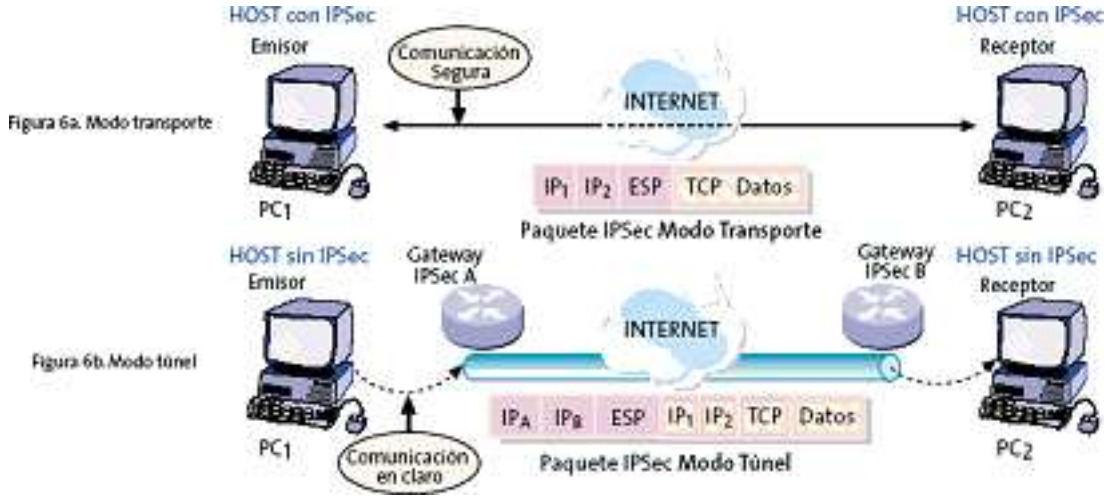

Figura 2.9 Modo Transporte y Túnel del Protocolo ESP[29]

Al utilizar en modo túnel (Fig. 2.9) el protocolo ESP, el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se le añade una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. Este modo de funcionamiento se lo utiliza cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones.

Protocolo de Control IKE: Un concepto introducido en IPsec es el de asociación de seguridad (SA), esto es esencial ya que SA es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al

[29] Fuente: http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

identificar únicamente un canal unidireccional, una conexión IPsec se compone de dos SAs, una por cada sentido de la comunicación.

La negociación de SA consiste en una configuración manual o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios como: los algoritmos criptográficos a emplear así como en los parámetros de control.

Una característica muy importante del protocolo IKE es que no se limita su utilidad a IPsec, ya que es un protocolo estándar de gestión de claves que se lo podría utilizar en otros protocolos como: OSPF[30] o RIPv2[31].

Este protocolo es el resultado de la integración de dos protocolos: ISAKMP y Oakley. ISAKMP define de forma general el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, en tanto que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente. Esquema de obtención de la clave de sesión (Fig. 2.10).

Figura 2.10 Obtención de la Clave de sesión[32]

[30] OSPF: -*Open Shortest Path First*- Protocolo de enrutamiento Jerárquico que calcula la ruta mas corta posible.
[31] RIP: -*Routing Information Protocol*- (Protocolo de encaminamiento de Información)
[32] Fuente: http://www.scribd.com/doc/34037219/Protocolos-VPN

Integración de IPsec con una PKI –*Public Key Infraestructure*- (Infraestructura de clave pública).

El uso de una PKI aparece en IPsec por la necesidad de un procedimiento que permita autentificar de forma fiable a un conjunto numeroso de nodos que desean comunicarse mediante IPsec. El uso de PKI en IPsec tiene ventajas que deben ser aprovechadas, como la centralización de alta y baja de usuarios, además de que posibilita la introducción de tarjetas inteligentes para soportar los certificados y con esto facilita la aplicación de IPsec en entornos de usuarios móviles o trabajadores remotos.

Al utilizar IPsec en una VPN se garantiza un acceso seguro de los usuarios remotos. La tecnología IPsec permite comunicar al usuario remoto a las maquinas del centro corporativo

2.1.3.2.3 L2tp –Layer 2 Tuneling Protocol-

Es un protocolo estándar aprobado por el IETF en oposición al protocolo propietario de Microsoft PPTP. Gracias a su estandarización es soportado por la totalidad de firmas del mercado de la comunicación de datos, incluyendo a Microsoft y Cisco. En L2TP se fusionan las mejores características de de otros protocolos de túnel como el PPTP de Microsoft y el L2F (*Layer 2 Forwading*) de Cisco Systems.

L2PT encapsula las tramas del protocolo punto a punto (PPP) que van a enviarse a través de redes IP, X25, *Frame Relay,* o ATM. Cuando L2TP está configurado para utilizar IP como su transporte, se lo puede utilizar como protocolo de túnel VPN en Internet. L2TP utiliza el puerto UDP 1701, para el mantenimiento del túnel incluye mensajes de control L2TP. Utiliza UDP para enviar tramas PPP encapsuladas se pueden cifrar o comprimir.

Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPsec (utilizándolo en modo transporte). Mediante la utilización de PPP, L2TP obtiene compatibilidad multiprotocolo para protocolos como IPX y Appletalk.

Así también L2TP proporciona una amplia gama de opciones de autenticación de usuario, incluidos CHAP, MS-CHAP, MS-CHAPv2 y el Protocolo de autenticación

extensible EAP "*Extensible Authentication Protocol*" que admite mecanismos de autenticación de tarjetas *token* y tarjetas inteligentes. Por lo tanto proporciona tuéneles bien definidos e interoperables, con la "…*seguridad de alto nivel e interoperabilidad de IPsec.*"[33]

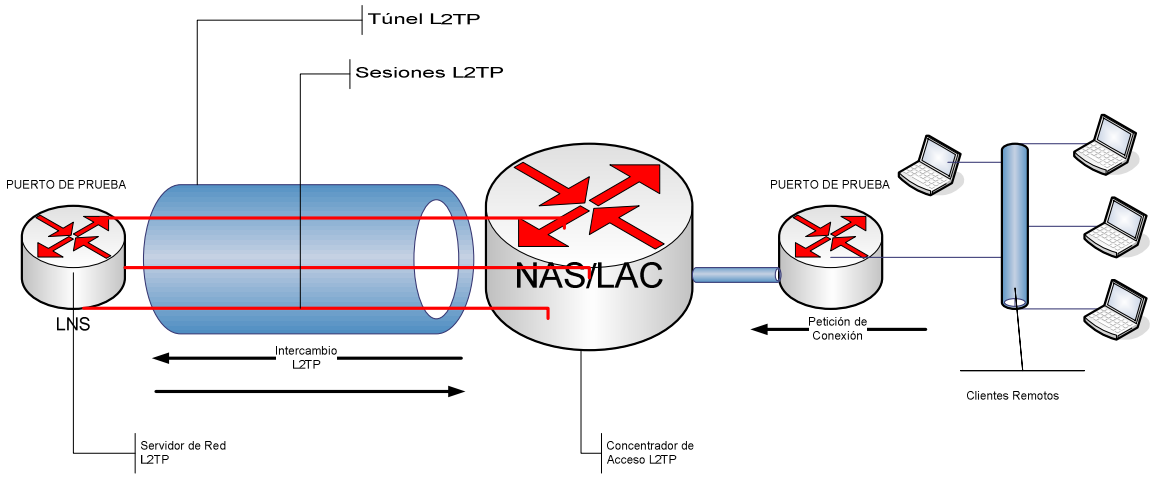

Figura 2.11 Elementos del Protocolo L2TP

LAC (Fig. 2.11)-*L2TP Access Concentrator*- (Concentrador de Acceso L2TP): Es un dispositivo físico que se añade a los elementos de interconexión de la red conmutada; como la red telefónica publica conmutada, o se coloca con un Sistema de terminación PPP capaz de gestionar el protocolo L2TP. Una LAC solo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o más LNS (L2TP *Network Server*).

LNS (fig 2.11) -*L2TP Network Server*- (Servidor de Red L2TP): Opera sobre cualquier plataforma con capacidad de terminación PPP. Gestiona el lado del servidor del protocolo L2TP, ya que L2TP se apoya sobre el medio al que llegan los túneles L2TP, LNS solo puede tener una interfaz única WAN o LAN, aunque es capaz de terminar todas las llamadas entrantes en cualquiera de la amplia

[33] LUIS GUERRERO RAMIREZ, Ing. "Seguridad en Redes Telemáticas"

gama de las interfaces PPP LAC. Al LNS se lo conoce también como *Home Gateway* (HGW).

NAS - *Network Access Server*- (Servidor De Acceso A La Red): Este dispositivo proporciona a los usuarios acceso temporal a la red bajo demanda. Este acceso es punto a punto, de uso típico en líneas de la red telefónica convencional o RDSI. En la implementación Cisco, un NAS sirve como LAC.

La autentificación de un usuario ocurre en 3 fases en L2TP:

En la primera fase, el ISP puede usar el número de teléfono de la llamada recibida, el número llamado o el nombre del usuario determinado que el servicio de L2TP requiere y entonces iniciar un túnel de conexión al servidor de red apropiado. Cuando un túnel está establecido, el Concentrador de Acceso (LAC) del ISP asigna un nuevo ID de llamada para identificar la conexión con el túnel e inicia una sesión para devolver la información autentificada.

El servidor de red corporativa emprende la segunda fase de autentificación para decidir si acepta o no la llamada. La llamada comienza indicando al ISP si incluir CHAP, PAP, EAP o la información de la autentificación de otros, el servidor de red usará esta información para decidir si acepta o rechaza la llamada.

Después que la llamada ha sido aceptada, el servidor de red puede iniciar la tercera fase de autentificación a la capa de PPP.

A través de estas 3 fases de autentificación L2TP garantiza que el usuario final, ISP y el servidor de red están conectados con quien dicen ser.

Los componentes de mayor importancia son aquellos que definen el punto final de un túnel basado en este protocolo, entre los cuales se encuentra el concentrador de acceso L2TP (LAC) como parte del equipamiento del ISP, y el servidor de red L2TP (LNS). En el caso de los ISPs además del hardware implementado en el mismo se tiene en cuenta el software necesario requerido que puede ser reducido para el enlace de los clientes móviles, los cuales necesitaran negociar en la primera fase de autentificación de usuarios. Por otro lado, el LNS deberá ser atendido y mantenido por el personal de la empresa, mientras que estas actividades son responsabilidad del ISP con relación al LAC.

Internet sólo puede transportar tráfico TCP/IP; sin embargo, con la técnica de túneles del protocolo L2TP, los datos no TCP/IP pueden ser transportados a través de Internet sin el precio de conexiones telefónicas directas. Si ambos extremos, la red corporativa y una red de la sucursal por ejemplo, usan equipos que incluyan soporte L2TP, cada uno de ellos puede originar un túnel sobre el otro; dicho túnel es totalmente transparente al proveedor de Internet, y evita la necesidad de gestionar cualquier configuración o contrato especial con el proveedor de Internet.

VPN NAT: Algunas organizaciones utilizan la traducción de direcciones (NAT) a pesar de no ser exclusivamente VPN. Los dispositivos de VPN se ven afectados directamente por estos procesos de NAT. El proceso consiste en cambiar la dirección IP interna por una IP pública.

Salida: Todo el tráfico que viene de la VPN se dirige hacia el dispositivo de NAT para cambiar al usuario que lo solicite por una IP pública con la capacidad de ser enrutable. Luego el dispositivo NAT envía el paquete al dispositivo de VPN que se encarga de la encriptación del mismo. El paquete es enviado al router extremo y de ahí al destino final.

Entrada: Los paquetes entrantes deben dirigirse al dispositivo de VPN correspondientes, se realiza la carga de encriptación y se revisan los privilegios de autenticación como la autenticación del usuario. Luego el paquete se envía al dispositivo de traducción de direcciones para remitirlo al usuario correspondiente. El dispositivo envía el paquete hacia su destino.

2.2 TIPOS DE VPN

Las formas en que pueden implementar las VPNs pueden ser basadas en *Hardware* o a través de *Software*, pero lo más importante es el protocolo que se utilice para la implementación.

Las VPNs basadas en *Hardware* utilizan básicamente equipos dedicados como por ejemplo los routers[34], son seguros y fáciles de usar, ofreciendo gran

[34] O también Switch administrables como el 3Com 4500 que posee la Dinse.

rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios, en síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son PROPIETARIOS.

Básicamente se puede diferenciar tres tipos de arquitecturas para la implementación de VPN.

2.2.1 VPN DE ACCESO REMOTO

Actualmente es considerado el modelo más usado, y consiste en usuarios o proveedores que se conectan con la red corporativa desde sitios distantes geográficamente de la ubicación física de la empresa (red corporativa), estos sitios remotos pueden ser: oficinas comerciales, domicilios, hotel, incluso aviones preparados con este servicio. Utilizando Internet como vinculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura –dial up- (modems y líneas telefónicas). Aunque en muchas empresas por razones de contingencia conservan aun sus viejos modems y enlaces telefónicos.

2.2.2 VPN PUNTO A PUNTO

Esta arquitectura se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que esta enlazado permanentemente a Internet, acepta las conexiones entrantes vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, para su funcionalidad la conexión a Internet debería ser de banda ancha. Esto permite reducir considerablemente los costos que representan los vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

2.2.3 VPN INTERNA A WLAN

Este esquema es el menos difundido y por lo tanto el menos utilizado, pero uno de los más poderosos para utilizar dentro de la empresa. Es básicamente una variable del tipo “Acceso Remoto” pero en lugar de utilizar Internet como medio de conexión, emplea la misma LAN de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad los hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicados detrás de un equipo VPN, el cual provee autenticación adicional mas el agregado del cifrado, haciendo posible que solo el personal de recursos humanos habilitado pueda acceder a la información.

2.3 TIPOS DE CONEXIÓN

2.3.1 CONEXIÓN DE ACCESO REMOTO

Una conexión de acceso remoto es realizada por un cliente o un usuario de un computador que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y este se autentica al servidor de acceso remoto, y el servidor se autentica ante el cliente. Necesariamente la dirección IP para el cliente tiene que ser asignada dinámicamente.

2.3.2 CONEXIÓN VPN A ROUTER A ROUTER

Una conexión VPN de esta característica es decir de router a router es realizada como no podría ser de otra manera por un router, y este a su vez se conecta a una red privada, En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentica ante el router que responde y a su vez se autentica ante el router que realiza la llamada y también sirve para la Internet.

2.3.3 CONEXIÓN VPN FIREWALL ASA A FIREWALL ASA

Una conexión VPN firewall ASA a firewall ASA es realizada por un firewall ASA, y este a su vez se conecta a una red privada. En este tipo de conexión, los

paquetes enviados desde cualquier usuario en Internet llegan al firewall ASA que realiza la llamada, se autentica ante el firewall ASA que responde y este a su vez autentica ante el firewall ASA que realiza la llamada.

2.4 IMPLEMENTACIÓN

Existen diferentes tecnologías para implementar VPNs[35].

DLSW: Data Link Switching(SNA over IP)

IPX for Novell Netware over IP

GRE: Generic Routing Encapsulation

ATMP: Ascend Tunnel Management Protocol

IPSEC: Internet Protocol Security Tunnel Mode

PPTP: Point to Point Tuneling Protocol

L2TP: Layer To Tuneling Protocol

Las diferentes tecnologías que se tienen para implementar VPN se las debe considerar ya que de esto dependerá de hacerlo por Software o por Hardware, de acuerdo a las necesidades y recursos de la empresa. Al momento de tomar la decisión se analiza los protocolos que los equipos soportan, (de hacerlo por hardware) y el software (S.O. y software VPN) tanto cliente como servidor (de hacerlo por Software)

2.4.1 VPN POR HARDWARE (CAJA NEGRA)

Son dispositivos que utilizan algoritmos de tecnología VPN. Algunos de ellos implementan encriptación como DES de 40 bits. Estos elementos con capaces de cumplir con la tarea de encriptación y desencriptación más rápidamente que los servidores de VPN.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software.

---

[35] Los mas usados en el medio han sido analizados previamente en el sub capitulo 2.2

Dentro de esta familia se tiene a los productos de WatchGuard, Nortel, Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, D-link, etc.

Estos dispositivos se pueden colocar después del firewall o en caso contrario paralelo a este. En el primer caso los paquetes que pasen por el firewall llegan al servidor de VPN y de ahí a la red, en este trayecto pueden ser encriptados o no dependiendo de la configuración. En el segundo caso permite al servidor de VPNs crear múltiples túneles. El dispositivo d VPN solo se encarga del tráfico que es propio de la VPN y el resto pasa por el firewall.

2.4.2 VPN POR SOFTWARE

La implementación de VPN por Software, consiste en que únicamente intervienen dispositivos de la red corporativa, sin otro dispositivo de hardware adicional. Es decir se carga el software en el servidor corporativo y en el cliente.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en las implementaciones por hardware. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general

Los Sistemas operativos Windows Server, permiten la implementación de VPN con el protocolo PPTP activando el Servidor RAS[36], y luego el mismo protocolo PPTP. En el caso del cliente, el acceso telefónico a redes o conexión a Internet de otro tipo permite el acceso a la VPN.

En el caso de LINUX, en su distribución Red Hat Enterprise 9.0 ya viene instalado el IPsec para permitir la implementación. De no ser así se puede usar Software como OpenVPN, StrongsWAN, FreeS/WAN y hay versiones para la gran mayoría de distribuciones[37] de Linux.

Como se habia indicado anteriormente, independientemente de la manera en como vayamos a implementar la VPN (por Software o Hardware) lo principal a tener en consideración es el protocolo a usar.

---

[36] Servidor de acceso remoto
[37] Una distribución de Linux es una versión con características diferentes entre si.

Para la Implementación propiamente dicha se debe tener en cuenta lo siguiente:

1. La Arquitectura.
2. El protocolo.
3. Direcciones IP públicas por cada recurso que interviene en la VPN.
4. Una conexión a Internet banda ancha para el servidor y por supuesto una conexión a Internet en cada uno de los lugares remotos, igualmente de preferencia banda ancha.
5. Una dirección IP estática para el servidor.
6. Configuración de tal manera que la asignación de direcciones IP, para los PCS remotos, sea dinámica.
7. Un Proxy que se ejecute en el servidor, para permitir o denegar el acceso según sea el caso.
8. Un adaptador virtual de la red instalado en el Pc remoto o Cliente.
9. Instalar y configurar el Software en el servidor.
10. Instalar y configurar el Software en el Cliente.

En el siguiente ejemplo propuesto, se necesita conectar una sucursal a la Matriz ya que se encuentran geográficamente distantes. Se tiene un servidor que utiliza la distribución linux Centos 5.0 y una PC con Windows y acceso a Internet en la Matriz y el cliente (Fig. 2.11).

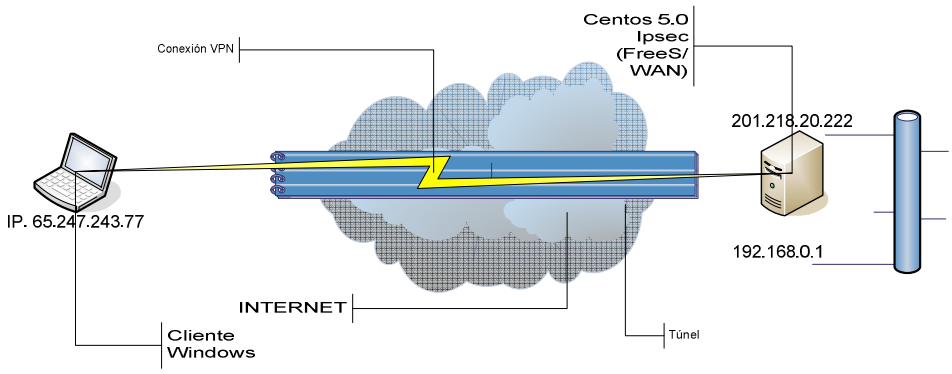

Figura 2.12 Ejemplo de Implementación de VPN por Software

- La Arquitectura que permite realizar esto es la VPN de acceso remoto.
- El protocolo a usar es el IPsec.
- Se tiene al menos una dirección IP pública (201.218.20.222) para el servidor, y una para el cliente (65.247.243.77).
- La dirección IP estática del servidor es 192.168.0.1
- El equipo servidor con linux (Cualquier distribución para servidores) puede servir dinámicamente las direcciones IP (DHCP).
- El Squid es un Proxy que viene por defecto en la distribución Linux Centos, este permite crear listas de control de acceso permitiendo o denegando URL, puertos, etc.
- El protocolo escogido es IPsec así que para implementar la VPN se necesitará FreeS/WAN que es un software de implementación libre de IPsec para sistemas operativos Linux. Para el cliente Windows se necesitará una versión de FreeS/WAN para sistemas operativos de Microsoft.

CAPITULO 3: ESTUDIO Y ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA TI[38] DE LA DINSE

3.1 REDES LAN EXISTENTES

La DINSE -Dirección Nacional de Servicios Educativos- es una entidad pública, Unidad Ejecutora del Ministerio de Educación, su accionar abarca a todo el País es así que tiene siete Unidades Administrativas Regionales distribuidas de la siguiente manera: Frontera Norte No.1 (*Ibarra*), Centro Norte No. 2 (*Tena*), Centro No. 3 (*Riobamba*), Litoral Norte No. 4 (*Manta*), Litoral Centro No5 (*Guayaquil*), Austro No. 6 (*Cuenca*), Frontera Sur No. 7 (*Loja*)[39].

Las oficinas en las Unidades administrativas: Ibarra, Loja, Manta, Tena y Riobamba, únicamente se encargan de receptar los requerimientos de infraestructura escolar de las provincias que abarcan, estas a su vez envían a la DINSE Matriz. La recepción es exclusivamente de documentos físicos, básicamente lo que receptan son oficios dirigidos al Director Nacional de Servicios Educativos, o al Ministro de Educación y este los remite a la DINSE Matriz.

Y esto es porque la infraestructura en estas dependencias se limita a una pequeña oficina sin acceso a TI.

---

[38] Tecnología Informática,

[39] Actualmente, las unidades administrativas, que no están enlazadas en el diagramase debe a quew no poseen la infraestructura de TI para poder estar en la VPN.

Unidades Administrativas

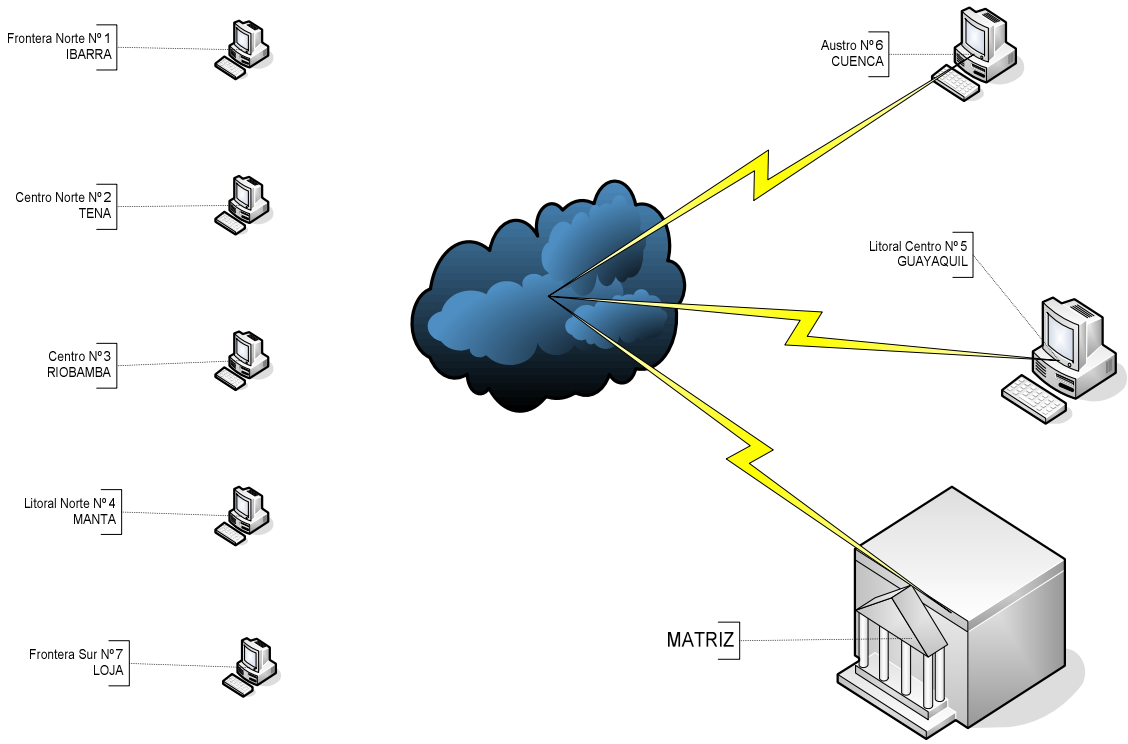

Figura 3.1 Distribución Administrativa DINSE

Frontera Norte Nº 1 (Sede Ibarra)

- Carchi
- Imbabura
- Esmeraldas
- Orellana

Centro Norte Nº 2 (Sede Tena)

- Napo
- Pichincha
- Cotopaxi
- Sucumbíos

Centro Nº 3 (Sede Riobamba)

- Chimborazo
- Tungurahua
- Pastaza

Litoral Norte nº 4 (Sede Manta)

- Manabí
- Sto. Domingo de los Tsachilas
- El Oro
- Galápagos

Litoral Centro Nº 5 (Sede Guayaquil)

- Guayas
- Sta. Elena
- Los Ríos
- Bolívar

Austro Nº 6 (Sede Cuenca)

- Azuay
- Cañar
- Morona Santiago

Frontera Sur Nº 7 (Sede Loja)

- Loja
- Zamora Chinchipe

3.1.1 MATRIZ

El edificio matriz de la DINSE (a la fecha 2009-09-15) se encuentra ubicado en la Av. 10 de agosto y N34-566 y Juan Pablo Sanz Edificio “Paseo Carolina”.

La estructura civil del edificio matriz[40], consta de cinco plantas divididas en departamentos y con divisiones modulares para cada funcionario, constituida de la siguiente manera:

En la planta 5 (piso 3) se encuentran los siguientes departamentos:

- Dirección Nacional
- Asesoría Jurídica
- Financiero (Caja, Contabilidad, Presupuesto, Coordinación Financiera).
- Comunicación

En la Planta 4 (piso 2) se encuentran los siguientes departamentos:

- Estudios y Proyectos
- Fiscalización
- Planificación
- Infraestructura

En la Planta 3 (piso 1) se encuentran los siguientes departamentos:

- Gestión Tecnológica
- RR.HH.
- Dirección Administrativa
- DIMCOME (Dirección de imprenta y Comercialización).

[40] Los planos del edifico matriz se encuentran en el Anexo 1.

En la Planta 2 (planta baja) se encuentran los siguientes departamentos:

- Servicios Institucionales
- Dpto. Medico
- Archivo
- Recepción

En el subsuelo se encuentra el cuarto de Telecomunicaciones.

3.1.1.1 Diagrama Lógico De La Red

La infraestructura para la transmisión de datos en la matriz se encuentra centralizada, básicamente es una topología tipo estrella. Ubicándose en los extremos los terminales, sean estos estaciones de trabajo, servidores, etc., y en el centro un dispositivo concentrador Switch 3Com administrable. Esta configuración se presenta en el anexo 2.

3.1.1.2 Descripción Del Cableado

Como se puede visualizar en el Anexo 1 la DINSE, posee actualmente la siguiente infraestructura para la transmisión de datos:

Item	Elemento	Numero	Detalle
1	Puntos de Datos	110	Categoría 5e, certificados
2	Servidor Hp Proliant 370	1	Sistema Operativo Windows 2003 Server Enterprise, como DNS y Servidor de Antivirus.
3	Servidor Hp Proliant 170	1	Sistema Operativo Windows 2003 server Bussines Servidor de aplicaciones
4	Pc HP dc 1200	1	Sistema Operativo Centos 5.0, como proxy.

Item	Elemento	Numero	Detalle
5	Swich 3Com 4500	3	Interconectan los puntos de datos en cada piso
6	Switch 3Com 5500	1	Interconecta los Switch 4500

Tabla 3.1: Listado de los elementos de TI en matriz

Adicionalmente cuenta con el cableado correspondiente de 100 puntos de voz, pero no cuenta con el resto de la infraestructura (central telefónica digital) que permita la trasmisión de voz.

En el subsuelo se encuentra la sala de servidores, por lo que la troncal se distribuye desde esta planta hacia las plantas superiores. En cada piso hay un área destinada a los equipos concentradores.

3.1.2 GUAYAQUIL

La regional Litoral Centro, tiene su sede en Guayaquil en la Av. Esmeraldas s/n y Piedrahita (esquina). Esta Unidad administrativa abarca a las provincias de Guayas, Los Ríos, Santa Elena y Bolívar. Considerando que únicamente existe oficinas y por lo tanto infraestructura tecnológica en Guayaquil[41].

[41] No existe en las provincias de Los Ríos, Sta. Elena ni en Bolívar oficinas de la DINSE, por esta razón, se canaliza a través de la unidad GYE.

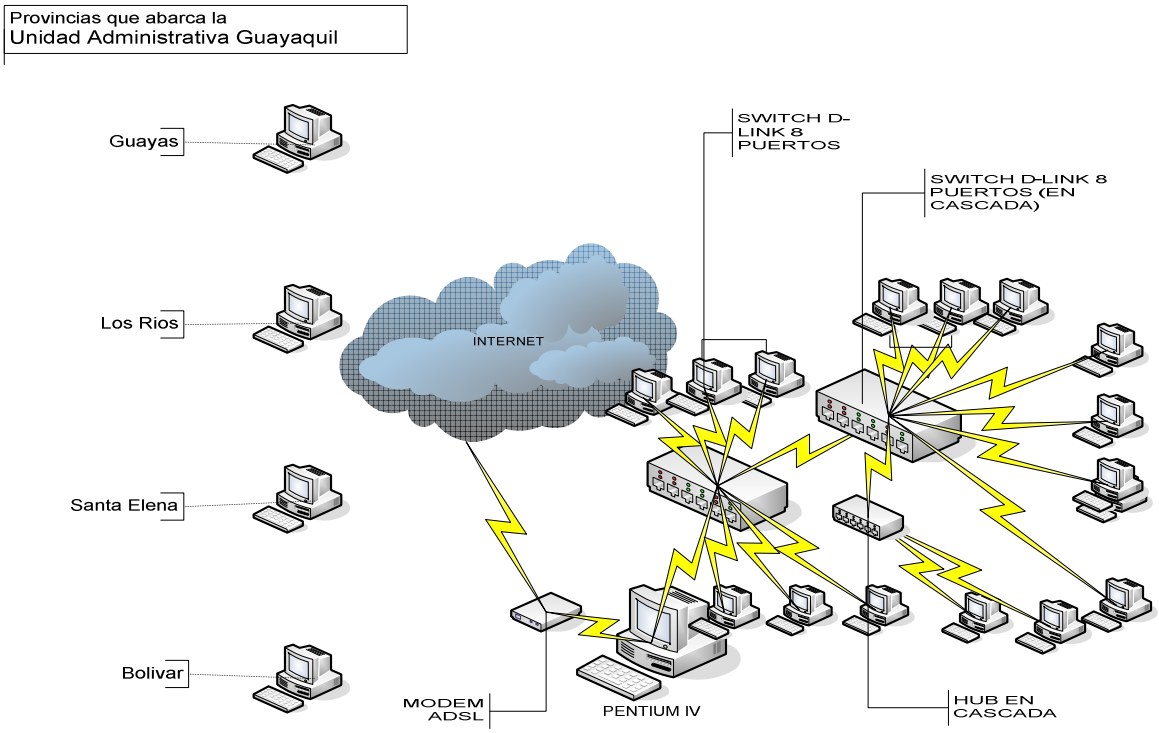

Figura 3.2 Unidad Administrativa GYE

En las unidades administrativas regionales, la situación varía considerablemente respecto a la Matriz, ya que el cableado se lo ha ido instalando de manera antitécnica, sin considerar el crecimiento de los diferentes departamentos y por lo tanto de la necesidad de acceder a los recursos de la DINSE Gye. Esto ha provocado que los dispositivos como impresoras, unidades de almacenamiento, se encuentren subutilizados y su disponibilidad sea mínima.

La administración actual ha realizado una readecuación del Cableado, sin embargo no cuenta con certificación de los puntos de red.

3.1.2.1 Diagrama Lógico De La Red

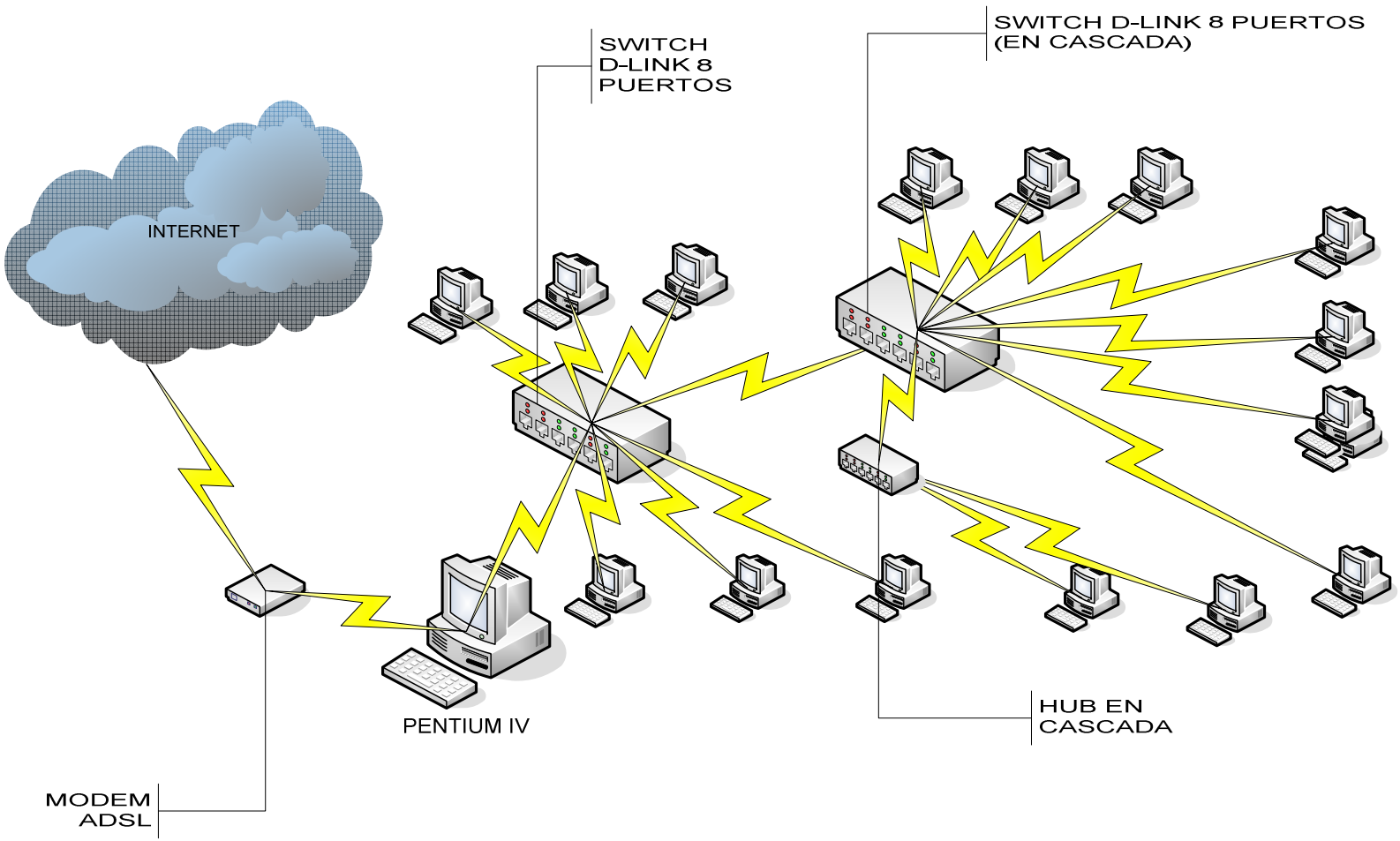

Figura 3.3 Diagrama lógico de la red GYE

3.1.2.2 Descripción Del Cableado

La regional Litoral, actualmente cuenta con la siguiente infraestructura para la transmisión de datos:

Item	Elemento	Numero	Detalle
1	Pc PIV	1	Servidor Proxy
2	Puntos de datos	16	Categoría 5e, sin certificación.
3	Switch D-Link 8 puertos	2	Concentrador datos
4	Hub C-NET	1	8 Puertos

Tabla 3.2 Listado de los elementos de TI en Gye.

3.1.3 CUENCA

La regional Austro con sede en la Ciudad de Cuenca está ubicada en la calle Guayacanes s/n y Av. Ordóñez Lazo diagonal al edificio Astudillo. Coordina la ejecución de obras y entrega de material escolar en las provincias de Azuay, Cañar y Morona Santiago[56].

[56] Esto es debido a que no existen oficinas de la DINSE en las provincias mencionadas.

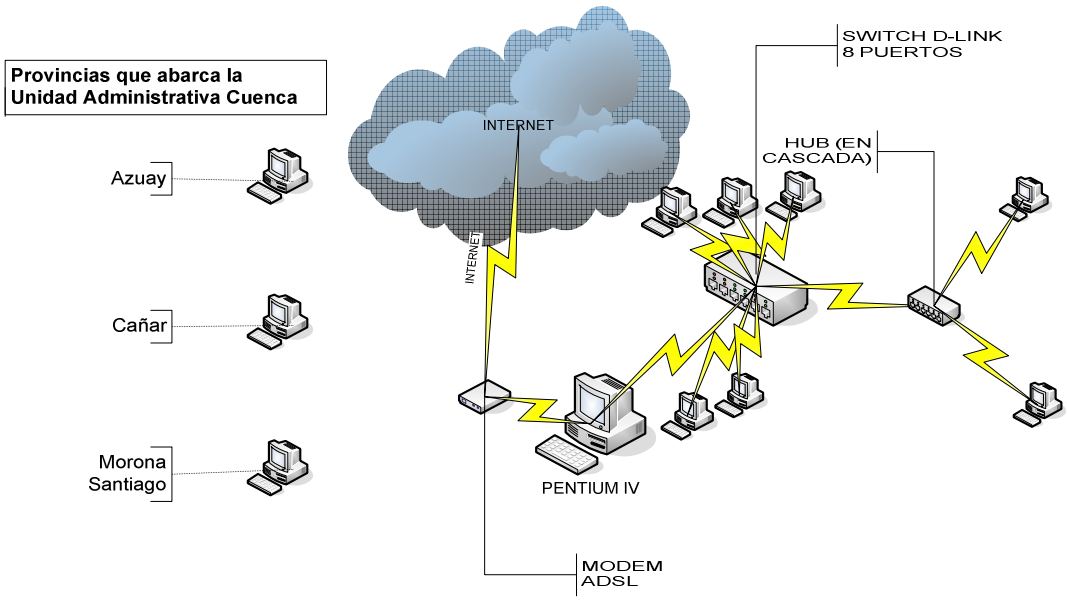

Figura 3.4 Unidad Administrativa CUE

En esta sede las condiciones no varían respecto a la regional Litoral Centro, ya que no existía la distribución del Internet, únicamente contaba con este servicio el departamento financiero.

Actualmente cuenta con 15 puntos de datos con las especificaciones técnicas debidas, aunque hay solo nueve usuarios permanentes.

3.1.3.1 Diagrama Lógico De La Red

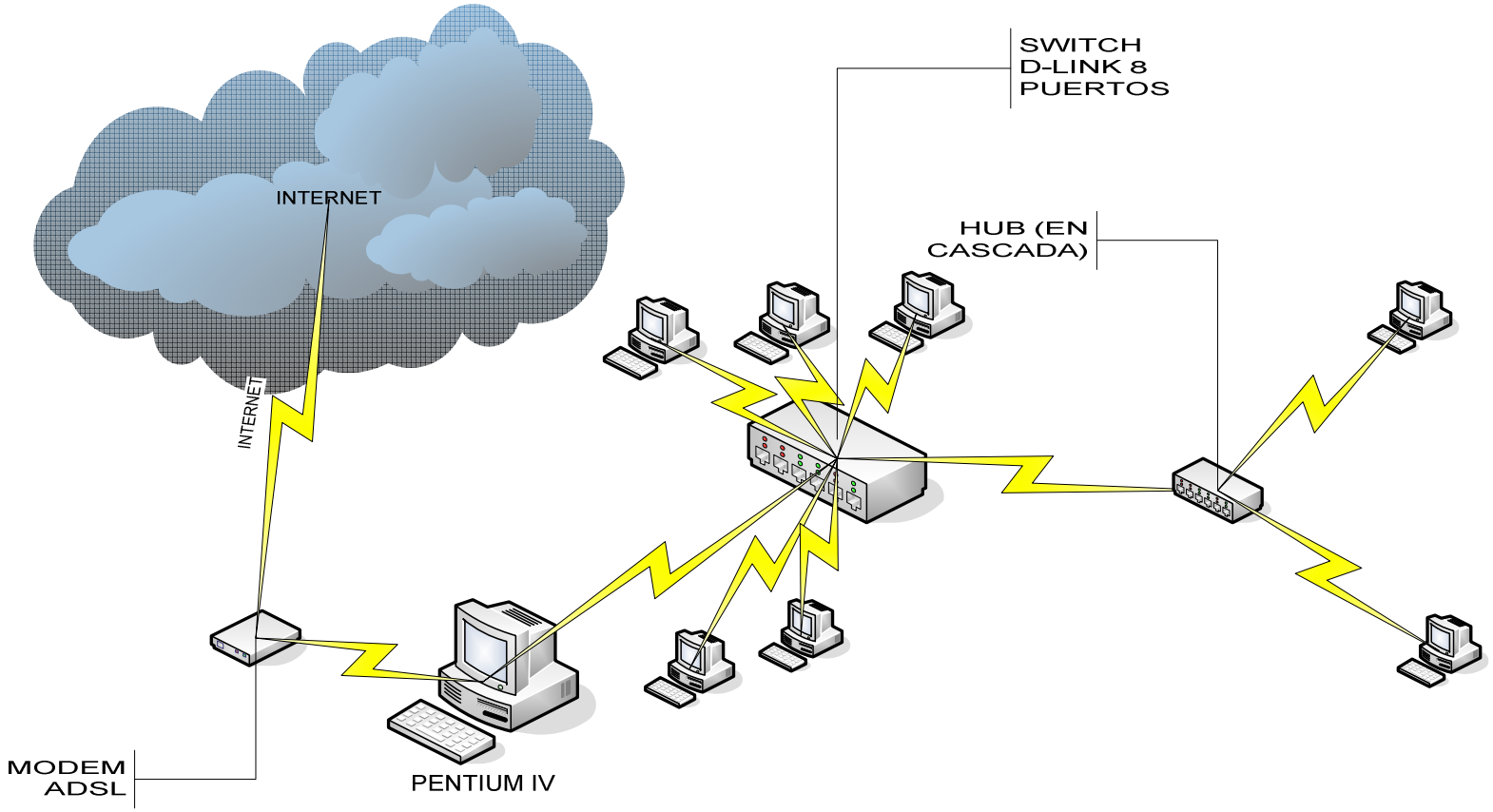

Figura 3.5 Diagrama Lógico de la Red CUE

3.1.3.2 Descripción Del Cableado

La regional Austro, actualmente cuenta con la siguiente infraestructura para la transmisión de datos:

Item	Elemento	Numero	Detalle
1	Pc PIV	1	Servidor Proxy
2	Puntos de datos	15	Categoría 5e, sin certificación.
3	Switch D-Link 8 puertos	1	Concentrador datos, 8 Puertos
4	Hub C-NET	1	8 Puertos

Tabla 3.3 Listado de los elementos de TI en matriz

3.2 ACCESO A INTERNET

Actualmente la empresa *Brightcell* ofrece el servicio de Internet a la DINSE con las siguientes características de Operación.

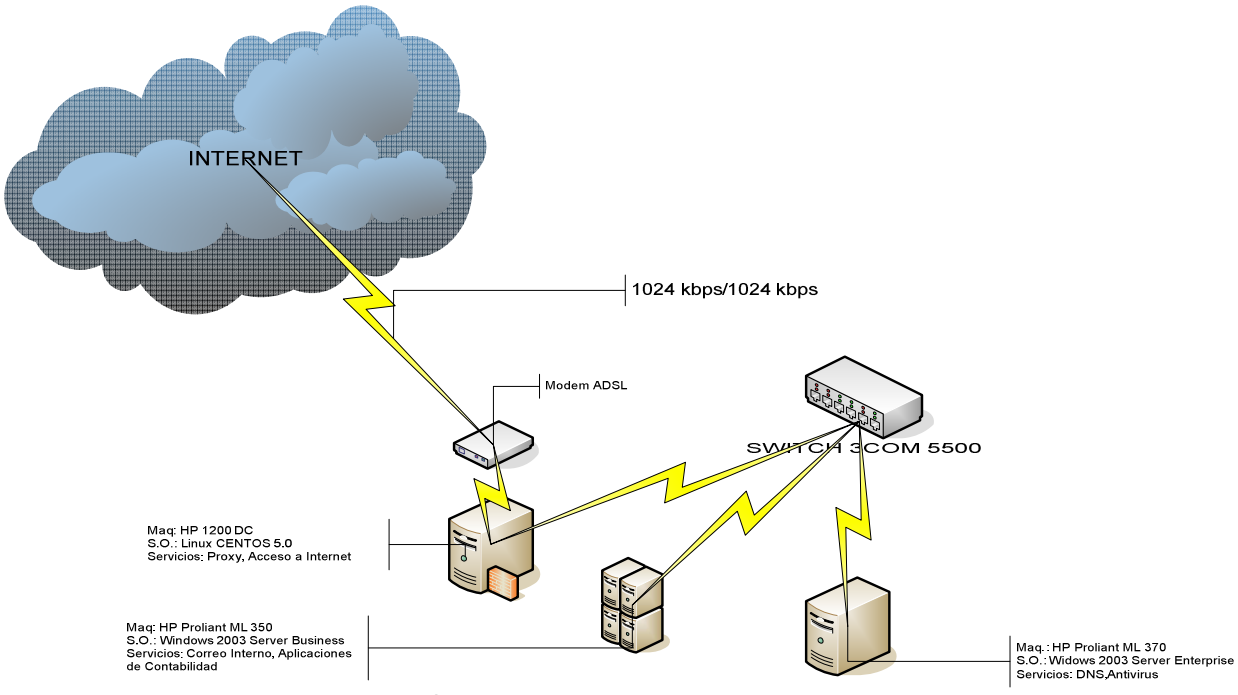

Figura 3.6 Acceso a Internet

La especificación técnica del servicio de Internet banda ancha, contratado con "*Brightcell*." es la siguiente:

- Servicio de acceso a Internet Corporativo Simétrico 1024 kbps para subida de información.
- El circuito proporcionado será un canal de 1024 Kbps uplink, que podrá crecer a en pasos de nx64, el ancho de banda es garantizado sea o no requerido por las aplicaciones del usuario. Este circuito permite la integración de tráfico multimedia (voz, datos y video), de acuerdo con el hardware del cliente.
- 1024 kbps para bajada de información.
- El circuito proporcionado será un canal de 1024 Kbps downlink, que podrá crecer a en pasos de nx64, el ancho de banda es garantizado sea o no requerido por las aplicaciones del usuario. Este circuito permite la integración de tráfico multimedia (voz, datos y video), de acuerdo con el hardware del cliente.
- *Brightcell* entregara un bloque de 8 direcciones IP reales, sin costo adicional alguno. Las direcciones IP proporcionadas por *Brightcell*, son direcciones de red públicas, registradas tanto en NIC como en Arin. En el caso de requerir direcciones IP adicionales, se requiere una comunicación escrita por parte de la DINSE.
- La velocidad contratada se garantizara a través de un equipo administrador de ancho de banda Packeteer 4500 ISP, asegurando así niveles de compartición desde el lado del proveedor de Internet, por lo cual la relación USUARIO/CANAL será de 2 a 1 hasta los NAP's en los Estado Unidos.
- *Brightcell* cuenta con un software especializado para la administración y monitoreo de canales y equipos por medio del protocolo SNMP[43] las 24 horas del día los 7 días de la semana, los 365 días del año, para los cual

[43] Simple Network Manager Protocol –Protocolo Simple de Manejo de red de trabajo-

se utiliza el Sistema CISCO Works con SNMPc de Castle Rock, el mismo que permite manejar alarmas tanto en cortes de última milla como en problemas en el acceso remoto al Internet, estas alarmas son enviadas a beepers o pagers garantizando así la oportuna asistencia y corrección de errores que puedan presentarse.

- Adicionalmente al Sistema de monitoreo detallado de Brightcell podrá instalar en el servidor la plataforma de control y monitoreo NAGIOS la cual se ejecutara sobre plataforma Linux (Red Hat 9, Fedora Core 2 o superior) la que permitirá determinar oportunamente cortes o caídas del enlace, con generación de alarmas que pueden ser direccionadas al personal técnico que trabaja en la Institución por medio de correo electrónico o mensajes SMS a teléfono celular.

Características del Proveedor de Servicios de Internet:

- *Brightcell* actualmente cuenta con un canal principal de enlace internacional por medio de F.O (fibra óptica).

- El primero va a través de la plataforma de TRANSNEXA que se conecta por medio de Ethernet sobre SDH con su filial en Colombia, INTERTEXA, que presta los servicios de operador de cabeza del cable submarino de fibras ópticas Arcos 1 y una conexión de fibra óptica en Tolú para la interconexión con cable Maya. INTERXA a su vez se interconecta con 3 proveedores de Internet en USA ofreciendo redundancia a la salida internacional.

- El segundo por medio de FO, es el mismo que utiliza un canal E3 de Microonda de Andinatel desde Quito hasta Tulcán y ahí se interconecta con la FO de Telecom, utilizando un circuito independiente a la ciudad de Bogotá, a través de Cable Maya para alcanzar la red de OPEN TRANSIT en el NAP de Atlanta permitiendo la interconexión con los principales NAPs de USA, este canal tiene la capacidad de 8 E1s.

- Este esquema de conexión permite mantener una disponibilidad del 99,8% de servicio y garantiza la conectividad permanente al Internet.

- Up time Anual Ultima Milla:
- El enlace de última milla tiene una disponibilidad anual de 99,6%

3.3 CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS DE NETWORKING DE LA DINSE

Los equipos de *Networking* utilizados para la interconexión de la red LAN, con los que cuenta la DINSE son los siguientes:

3.3.1 SWITCH 3COM 4500/5500 - 26 PORT (MATRIZ)

La DINSE cuenta actualmente con 4 switches de este tipo, ubicados en el cableado horizontal de las plantas que componen el edificio. Este tipo de dispositivo es apilable para aplicaciones de extremo, responde a las necesidades más exigentes de redes convergentes seguras.

Este dispositivo ofrece switching de Capa 2 y routing dinámico de capa 3 con una amplia variedad de características, en una plataforma competitiva de alto rendimiento. Es posible apilar hasta 8 switches mediante puertos Gigabit Ethernet, por lo que toda una pila puede administrarse como una única entidad de administración IP.

Seguridad[44]: El control de acceso de red basado en el estándar 802.1.X[45] combinado con la autenticación RADIUS[46] garantiza acceso seguro a los recursos. Además, el RADA (acceso a dispositivo autentificado mediante RADIUS) permite la autenticación de los dispositivos conectados mediante la dirección MAC.

Las listas de control de acceso (ACLs) basado en puerto habilitan de forma efectiva políticas de uso en cada punto de acceso a la red mediante el switch.

---

[44] Fuente: Uniplex empresa calificada como Proveedora de equipos de telecomunicaciones por la DINSE
[45] 802.1X es una norma del IEEE para el control de acceso a la red basada en puertos, permite a la autenticación de dispositivos conectados a un puerto LAN
[46] Es un protocolo de autenticación para aplicaciones de acceso a la red o movilidad IP

El soporte de SSHv2 –Secure Shell Versión 2- y SMNPV3 garantiza un acceso de administración seguro a los switches mediante la autenticación y encriptación del tráfico de administración.

Voz sobre IP dinámica: La exclusiva funcionalidad de VLAN de voz detecta la presencia de teléfonos IP, y asigna dinámicamente puertos de switching a la VLAN de voz, permitiendo así una configuración y priorización automatizadas del tráfico VoIP. Esta potente funcionalidad permite minimizar los costes y la complejidad asociados con la instalación adicional o el traslado de teléfonos IP.

Rendimiento: Capacidad agregada de switching de hasta 8,8 Gbps. Los uplinks Gigabit duales en cada unidad de switching permiten establecer conexiones de alta velocidad con la red troncal, o con los servidores conectados localmente.

Priorización y administración de ancho de banda: Las ocho colas de prioridad por puerto posibilitan funciones de Clase de Servicio / Calidad de Servicio (CoS/QoS) 802.1p. Las capacidades de limitación de velocidad de ancho de banda y de filtrado de protocolos permiten a la familia Switch 4500 aplicar controles en cada puerto, para un uso eficiente de los recursos de la red y una priorización de las aplicaciones empresariales fundamentales o sensibles al tiempo, incluyendo la voz sobre IP (VoIP).

Flexibilidad y escalabilidad: Cada puerto Gigabit ofrece una selección de medios de cobre o fibra: 1000Base-T (mediante RJ45), o 1000Base-X (mediante módulos opcionales de transceptor "SFP", o de pequeño factor de forma conectables).

La capacidad de apilamiento permite combinar hasta 8 unidades en una misma pila administrada, pudiendo escalarse a hasta 384 puertos 10/100. Un completo conjunto de funcionalidades de switching, incluyendo filtrado multicast y soporte de protocolo Rapid Spanning Tree, actúa para mejorar aún más la escalabilidad y disponibilidad de los recursos de la red.

Administración y control: La familia Switch 4500 funciona con el sistema operativo de 3Com, el mismo software comprobado y compartido por los switches

empresariales de primera clase de 3Com, incluyendo las familias Switch 5500, Switch 7700, y Switch 8800.

Las funcionalidades de configuración y control de red son accesibles mediante interfaz de línea de comando[47] (CLI), o bien usando software de administración SNMP, como por ejemplo 3Com Enterprise Management Suite (EMS) y 3Com Network Director.

Facilidad de uso: El routing dinámico con RIP (protocolo de información de routing) permite la actualización automática de topologías de red de Capa 3. La velocidad y el modo duplex en todos los puertos se negocian automáticamente, evitando así la posibilidad de configuración inadecuada. Los switches detectan y ajustan las conexiones de cables cruzados o directos mediante la funcionalidad "Auto MDI/MDIX", eliminado así la necesidad de emplear distintos cables para interconectar dispositivos de red.

3.3.2 SWITCH D-LINK 8 PUERTOS

Este dispositivo lo utilizan tanto en la regional Administrativa Guayaquil, como en la sede Cuenca.

Este equipo no permite la interconexión de redes diferentes que es básicamente lo que se pretende con la VPN Quito - Guayaquil - Cuenca. Enlazar redes LAN distantes a través del Internet.

3.4 ANÁLISIS DE LA TI DE LA DINSE

Ya que los equipos concentradores Switch 3Com se encuentran con todos sus puertos utilizados, además que el tráfico de la LAN se va incrementando a medida que los usuarios respaldan sus datos más importantes en unidades mapeadas en el servidor de aplicaciones, debido al contenido y tamaño de los archivos (archivos de CAD y GIS), se corre el riesgo de saturar la red interna.

[47] La línea de comandos mediante Telnet

Se puede recomendar la adquisición de un Equipo router Cisco 1751 para la matriz y un router Cisco 1721[48] para cada una de las unidades regionales (Guayaquil y Cuenca) que formara parte de la VPN, conformada por redes con ubicación geográfica diferente.

Ya que estos dispositivos cumplen con las principales características para la implementación de la VPN como son:

- Protocolo de Transporte.
- Protocolo de direccionamiento
- Algoritmo de cifrado.
- Protocolo de Gestión Remota.

El incremento en el tráfico es fácilmente demostrable ya que han ingresado nuevos funcionarios a la DINSE matriz, con requerimientos de acceso a los recursos como son:

- Correo Electrónico,
- Aplicación Delphos,
- Impresoras de Red,

Además de acceso permanente a los portales:

- www.educarecuador.com (Ministerio de Educacion)
- www.edufuturo.com (Prefectura de Pichincha)

Si bien el Switch 3Com 5500 que se tiene instalado actualmente, puede realizar el encaminamiento de los paquetes (ruteo) su capacidad llegaría al umbral de máximo rendimiento, y se encuentran ocupados la gran parte de los puertos. Y en cuanto a soporte y homogeneidad de la VPN, se optaría por una marca mucho más recomendable.

En las unidades administrativas regionales Litoral Centro y Austro, los puntos de red no están certificados, pero de la constatación física realizada en el mes de

[48] La justificación para la selección de los routers, es que se consiguió estos equipos re-manufacturados el cual consta en la proforma en el Anexo 7 “Proforma de Equipos”

diciembre de 2007[49], se ha determinado que si cumplen con las condiciones necesarias (distancias máximas, curvaturas, distribución de pines, uso de componentes apropiados) para soportar el tráfico, luego de su reestructuración, por lo que el diseño que se presenta en el capítulo IV, puede ser implementado sin inconvenientes al interior de la DINSE.[50]

[49] En el anexo 3 se adjunta la información que respalda la constatación a la que se hace referencia

[50] Pese a que la investigación garantiza el funcionamiento de la propuesta que se plantea, en el capítulo de conclusiones y recomendaciones, se sugerirá que en el corto plazo se implemente un proyecto de certificación del Sistema de Cableado Estructurado en las unidades administrativas regionales para la optimización de recursos y el mejor funcionamiento de la red.

CAPITULO 4: DISEÑO DE LA SOLUCIÓN E IMPLEMENTACIÓN

4.1 ESTUDIO DE LA CAPACIDAD PARA IMPLEMENTAR VPN EN LA MATRIZ Y EN LAS REGIONALES.

4.1.1 CAPA ACCESO

Es el punto en el que cada usuario se conecta a la red. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. "*El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales. En la capa de acceso se puede encontrar múltiples grupos de usuarios con sus correspondientes recursos*"[51]. Actualmente en la DINSE se tienen implementados el siguiente equipamiento para la capa de acceso.

Dpto.	**Elemento**
Quito (Matriz)	Swich 3Com 4500
Guayaquil	Switch D-Link 8 puertos
Cuenca	Switch D-Link 8 puertos

Tabla 4.1 Definición de Capa de Acceso

4.1.2 CAPA DISTRIBUCIÓN

Esta capa marca el punto medio entre la capa de acceso y los servicios principales de la red. El enrutamiento, filtrado y acceso a WAN, son funciones primordiales de esta capa.

Dependiendo del lugar a implementarse puede cumplir con las siguientes funciones:

[51] ARIGANELLO ERNESTO, Ing. "Redes CISCO: Guía de estudio para la certificación CCNA 640-802"

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de *Broadcast*.
- Traducir los diálogos entre los diferentes tipos de redes.

La capa de Distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuando y como los paquetes pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso a servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo. La capa de núcleo podrá entonces transportar la petición al servicio apropiado[52].

Actualmente en la DINSE se tienen implementados el siguiente equipamiento para la capa de Distribución.

Dpto.	**Elemento**
Quito (Matriz)	Swich 3Com 5500
Guayaquil	Switch D-Link 8 puertos (mismo dispositivo)
Cuenca	Switch D-Link 8 puertos (mismo dispositivo)

Tabla 4.2 Definición de Capa de Distribución

4.1.3 CAPA *CORE* -NUCLEO-

La capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios.

[52] La capa de distribución se la identifica por se donde se encuentran establecidas las políticas como por ejemplo ACLs.

Estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia.
Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo. Actualmente en la DINSE se tienen implementados el siguiente equipamiento para la capa de Core.

Dpto.	**Elemento**
Quito (Matriz)	Switch 3Com 5500 (podría cumplir las funciones de CORE)
Guayaquil	No dispone
Cuenca	No dispone

Tabla 4.3 Definición de capa de Core

Como se puede observar en las tablas 4.1, 4.2 y 4.3, la DINSE no cuenta con equipos que permiten definir las capas del modelo jerárquico; en este sentido, es necesaria la adquisición de equipos que permitan identificar las diferentes capas, con el objetivo de administrar de mejor manera los servicios de red.

Por ejemplo: se tiene que los mismos equipos de la capa de distribución en el caso de las unidades regionales (Cuenca y Guayaquil) son los mismos equipos que para la capa de acceso.

4.2 ANÁLISIS DEL FLUJO DE INFORMACIÓN ENTRE LA MATRIZ Y LAS REGIONALES

Debido a la declaratoria de emergencia en las Construcciones Escolares[53], el flujo de información entre la DINSE matriz y sus unidades regionales, se ha

[53] Decreto Nº 188: “Declaración en estado de emergencia al sector educativo”

incrementado[54]. Se estima que diariamente se envían y se reciben a través del correo convencional entre 50 y 80 fojas[55] útiles de documentos[56] y aproximadamente 200 correos electrónicos personales diarios de entre 30 Kb y 5 Mb. Con la implementación de una VPN, se prevé que el flujo de información se incrementaría de manera exponencial, debido al uso de este medio para enviar y recibir información como archivos de los fiscalizadores, que principalmente son de diseño asistido por computador y archivos de sistemas de información geográfica, y convirtiéndose en una alternativa al uso del correo tradicional.

4.2.1 CORREO ELECTRÓNICO

El uso de correo personal es principalmente para el envió-recepción de: informes (Archivos de Texto 20 KB), planillas (hojas de cálculo 40 KB) y un grupo definido de usuarios (Área Técnica 1 MB) planos y mapas.
Si se toma en cuenta que:

- Los informes tienen que ser diarios (al menos uno al día).
- Las planillas son por detalle de obra (2 semanales en promedio).
- Los planos y archivos de información geográfica son un caso aparte, se estima que cada funcionario (de Planificación o de Infraestructura y Equipamiento) tiene una asignación de dos obras por año, si consideramos que cada plano va a tener dos correcciones serian 6 planos anuales y 2 de información geográfica.

Se ha determinado que el tamaño promedio de los correos electrónicos es de 700 KB, lo cual está justificado con el análisis anterior de los archivos de intercambio.
Realizando una aproximación, se puede determinar que se revisa un promedio de 2 correos en una hora, lo cual nos permite calcular:

$$\text{Uso e-mail} = \frac{700\ \text{KB}}{\text{e-mail}} \times \frac{8\ \text{bits}}{1\ \text{BYTE}} \times \frac{2\ \text{e-mail}}{1\ \text{hora}} \times \frac{1\ \text{hora}}{3600\ \text{seg}} = 3{,}11\ \text{kbps}$$

Figura 4.1 (Calculo demanda de AB de e-mail)

[54] Se ha incrementado el flujo de información en formato físico , es decir; oficio, cartas, tramites, etc.
[55] Hoja de papel en un proceso.
[56] Fuente: Dinse unidad de archivo Eco. Patricio Puente

Ahora bien si se tiene un escenario en el cual el 20% de los usuarios[57], es decir 40 de un total de 200, utilizaría simultáneamente el e-mail, se tiene:
Entonces: (#usuarios) 40* (demanda de AB e-mail) 3,11=124,4 kbps
La demanda de AB para e-mail será aproximadamente de 124,4 kbps.

4.2.2 NAVEGACIÓN WEB

Para realizar la estimación de los requerimientos de AB, se ha considerado que una página web tiene un tamaño aproximado de 50 KBytes[58] y que un usuario accede a la web y revisa un promedio de 20 enlaces en una hora[59] se tiene:

$$\text{Uso web} = \frac{50\ KB}{Web} X \frac{8\ bits}{1\ BYTE} X \frac{20\ enlaces}{1\ hora} X \frac{1\ hora}{3600\ seg} = 2{,}22\ kbps$$

Figura 4.2 (Calculo demanda de AB web)

Ahora bien, en el mismo escenario se tiene que el 50 % de los funcionarios es decir 100, utilizaran el servicio al mismo tiempo, lo que nos da:
AB Acceso web=2,22 kbps * 100=222,22 kbps
Y se tiene que es necesario 222,22 kbps para el uso de servicios y portales web.

4.2.3 MULTIMEDIA

Aunque por política general dentro de una institución[60] la descarga de archivos de video, música, etc., está restringida, también es limitada en las listas de control de acceso del Proxy. Sin embargo esto está supeditado a las consideraciones de la Dirección General la cual puede solicitar la activación de ciertos “sites” a ciertos funcionarios que así lo requieran para su desempeño. Considerando esto se tiene que es necesario un AB de 128[61] kbps para poder tener video en línea (on-line) con calidad aceptable.

---

[57] Administrativos que requieren acceso a e.mail para sus funciones.
58 Tomado de: http://www.guiaweb.gob.cl/guia/capitulos/tres/accesorapido.htm
59 Considerando el acceso a las páginas y servicios de las instituciones de las cuales la DINSE forma parte o, necesita para intercambiar información, como por ejemplo el ministerio de Finanzas y el Ministerio de Educación.
[60] Todo lo que no esta expresamente permitido, esta prohibido
[61] Mínimo requerido para video on—linem fuente: http://blog.espol.edu.ec/ylambert/2010/08/05/kbps-vs-kb-%C2%BF128-256-512-kbps-%C2%BF1mbps-valores-que-nos-confunde-pero-cual-es-la-velocidad-real-de-internet/

4.2.4 APLICACIONES WEB

Se tiene además las aplicaciones Web a las cuales se les puede considerar como páginas web de tamaño normal, ya que muchos de los servicios son consultas a bases de datos[62] las cuales dependen del servicio a brindar.

Por ejemplo en caso del licenciamiento en red, el servicio Web es una consulta cifrada[63] simple, lo mismo ocurre con el Servicio de Nombres de dominios (DNS[64]) y administración centralizada de Antivirus[65].

Con lo expuesto anteriormente y tomando en cuenta que las aplicaciones en la Matriz se encuentran en la red local, se puede decir que el uso de AB en aplicaciones web es equivalente a la demanda para el acceso a web en la matriz, es decir 222,22 kbps.

4.2.5 CAPACIDAD DEL CANAL PARA ACCESO A INTERNET

Únicamente se debe realizar la suma de todos los servicios que se va a brindar a través del Internet para tener un aproximado:

Canal Internet= e-mail+web+multimedia+aplicaciones web

Donde: 124,4+ 222,22+ 128+ 222,22= 696,84 kbps (estandarizando se tendría 1024 kbps)

4.3 ALTERNATIVAS PARA LA IMPLEMENTACIÓN

Con los equipos que posee la DINSE, actualmente y por el costo Operativo, no se contempla la implementación de una solución alternativa a través de Software, pues con este tipo de implementación, -el rendimiento es menor y la configuración más delicada, pues se suma el sistema operativo y la seguridad del equipo en general.

Una solución específicamente para la DINSE seria la implementación en el servidor Proxy con Sistema Operativo Linux CENTOS 5.0, sin embargo como se

---

[62] Las consultas a bases de datos dependen de la cantidad de registros, mas que de el tamaño mismo de la base.

[63] Cifrada de fabrica por cuestiones propias del licenciamiento.

[64] Para la aplicación de políticas a nivel nacional.

[65] La herramienta antivirus de la DINSE es actualmente NOD32, la cual permite tener la administración centralizada.

detalla anteriormente esto implicaría el soporte permanente[66] por parte del personal de TI de la DINSE, el cual es reducido y no cuenta con el conocimiento sobre distribuciones Open Source.

Con los enlaces a Internet que se disponen se pueden ubicar equipos de tecnología similar, que soporten los protocolos para la Implementación de la VPN a través de Hardware.

Se recomienda la adquisición (en cualquiera de sus formas) de equipos CISCO o 3Com por su garantía, confiabilidad y soporte.

4.3.1 METODOLOGIA DE DISEÑO PPDIOO

La metodología PPDIOO es de un estándar de CISCO[67] para el diseño e implementación de redes.

- Baja el costo total de propiedad por validación de requerimientos de tecnología y planeamiento para cambios de infraestructura y requerimientos de recursos.
- Incrementa la disponibilidad de la red por la producción de un sólido diseño de red y validaciones en las operaciones.
- Mejora la agilidad de negocios estableciendo requerimientos y estrategias tecnológicas.
- Velocidad de acceso para aplicaciones y servicios, mejorando disponibilidad, fiabilidad, seguridad, escalabilidad y performance[68].

Contempla las siguientes fases:

- Preparar
- Planificar
- Diseñar

---

[66] Open Source es una excelente alternativa, gracias a la gran comunidad de desarrolladores y colaboradores, el inconveniente radica en su permanente actualización y la aplicación de parches de mejora, es decir; sin actualización en pequeños intervalos de tiempo se vuelve obsoleta en insegura la versión implementada en un inicio.

[67] El soporte, el diseño de soluciones generales en el ámbito de las TIC y NTIC demuestran claramente que CISCO es líder en su ámbito y por lo tanto un referente y consecuentemente un estándar.

[68] Fuente: “Cisco Press 642-825 CCNP ISCW Official.Exam.Certification.Guide.Jul.2007”

- Implementar
- Operar
- Optimizar

Se procederá definir e identificar las diferentes fases en el caso específico de la DINSE.

4.3.1.1 Preparar

Esta fase crea un caso de negocios para establecer una justificación financiera para la estrategia de red. La identificación de la tecnología que soportará la arquitectura.

Por la importancia del tema y la aplicabilidad en el desarrollo institucional, se ha conseguido que la "Dirección Nacional de Servicios Educativos" (DINSE), brinde su auspicio para el desarrollo de la investigación, análisis, estudio y diseño del presente proyecto, adicionalmente que la DINSE correrá con los costos del equipamiento necesario para la instalación[69].

La tecnología a utilizar es una ***VPN site to site IPSec***, la cual soporta la arquitectura tipo estrella que es básicamente la conexión de todos los dispositivos de red a través de un dispositivo único[70].

4.3.1.2 Planificar

Identifica los requerimientos de red realizando una caracterización y evaluación de la red, realizando un análisis de las deficiencias contra las buenas prácticas de arquitectura. Un plan de proyecto es desarrollado para administrar las tareas, parte responsables, hitos y recursos para hacer el diseño y la implementación. Este plan de proyecto es seguido durante todas las fase del ciclo.

En el análisis de la Infraestructura de TI de la DINSE se determino que es necesaria la adquisición de equipos y administración/monitoreo de la VPN.

---

[69] Justificación en el "Plan de Proyecto de Titulación"

[70] Esto se cumple a plenitud debido a que la comunicación para el usuario final es transparente y la VPN actúa como una red única.

4.3.1.3 Diseñar

El diseño de la red es desarrollado basado sobre los requerimientos técnicos y de negocios, obtenidos desde las fases anteriores. Esta fase incluye diagramas de red y lista de equipos. El plan de proyecto es actualizado con información más granular para la implementación. Después de esta fase aprobada empieza la implementación.

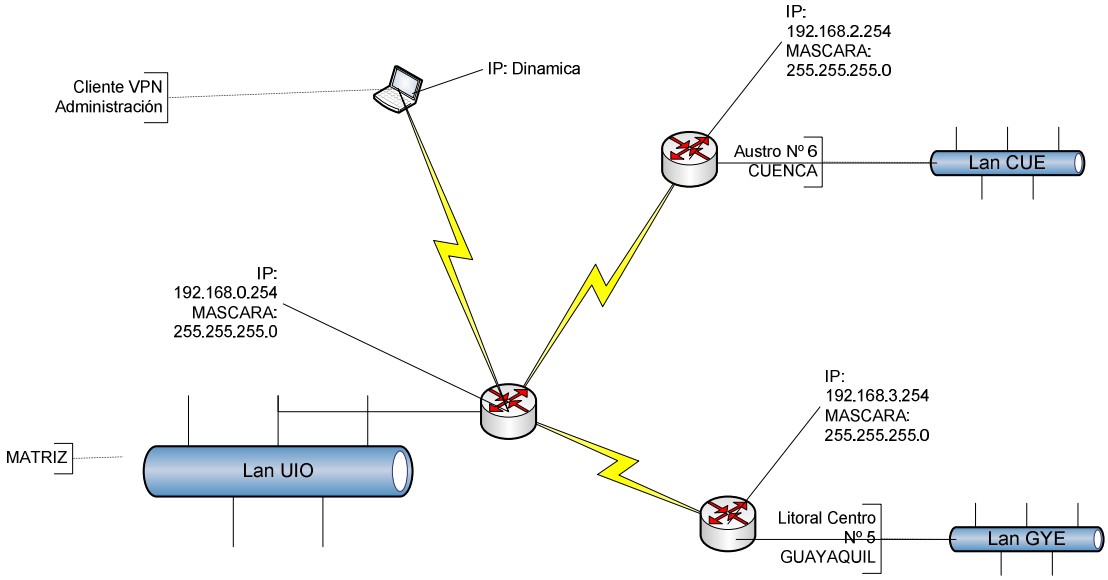

Figura 4.3 VPN PROPUESTA

DATOS CONCENTRADOR VPN-UIO

- Tipo de servicio: Internet
- Equipo VPN: Router CISCO 1751
- DIRECCIONAMIENTO IP:

ETH0/0 192.168.0.240
MASCARA: 255.255.254.0
FASTETHERNET0/0 208.19.69.67
MASCARA: 255.255.255.248

Tabla 4.4

DATOS VPN-GYE

- Tipo de servicio: Internet
- Equipo VPN: Router CISCO 1751
- DIRECCIONAMIENTO IP:

ETH0/0 192.168.2.254
MASCARA: 255.255.255.0
FASTETHERNET0/0 190.95.191.170
MASCARA: 255.255.255.252

Tabla 4.5

DATOS VPN-CUE

- Tipo de servicio: Internet
- Equipo VPN: Router CISCO 1721
- DIRECCIONAMIENTO IP:

ETH0 192.168.3.254
MASCARA: 255.255.255.0
FASTETHERNET0 190.95.200.66
MASCARA: 255.255.255.252

Tabla 4.6

4.3.1.4 Implementar

El nuevo equipamiento es instalado y configurado en esta fase. El plan de proyecto es seguido durante esta fase. Los cambios deben ser comunicados en una reunión de control de cambios, con la necesaria aprobación para proceder. Cada paso en la implementación debe incluir una descripción, guía de implementación, detallando tiempo estimado para implementar, pasos para rollback[71] en caso de falla e información de referencia adicional.

4.3.1.4.1 Introducción

La VPN site to site tiene 5 pasos en el ciclo de vida, de los cuales no se ha detallado anteriormente[72] el primero que es el de "Especificar el tráfico interesante", al cual se hace referencia a continuación.

Paso 1: Especificar el tráfico interesante.

Se debe especificar el tráfico que resulta interesante de ser capturado, por lo cual se debe cifrar (proteger por IPsec VPN), para que únicamente en los extremos de la VPN se pueda acceder a su contenido. Cuando existe un túnel VPN IPsec entre dos sitios, el tráfico que es considerado "interesante" se envía de forma segura a través de la VPN a la ubicación remota. Una vez dentro de la VPN, los datos se encuentran seguros dentro hasta llegar al otro extremo del túnel. El concepto de tráfico interesante implica, que el tráfico que no está catalogado como interesante no goza de los beneficios de la IPsec VPN, estos no están protegidos ni cifrados de alguna manera, este tráfico puede viajar a su destino incluso al destino remoto donde termina el túnel VPN.

Una lista de control de acceso extendida (ACL), se usa para especificar el tráfico interesante. El tráfico que es permitido por esta ACL debe tener una aplicación adecuada de la política de seguridad-.

Paso 2: Fase IKE 1

Paso 3: Fase IKE 2

Paso 4: Transferencia segura de datos

Paso 5: Terminación del túnel IPsec

---

[71] En términos generales, es el procedimiento que permite regresar a un estado determinado, en caso de algún fallo.

[72] Los 4 pasos restantes ya fueron señalados en el Capitulo 2

4.3.1.4.2 Implementación Por Cli[73] –Comand Line Interfaz- (Interfaz De Línea De Comandos)

La implementación se la ha realizado con una herramienta de simulación de CISCO a través de líneas de comando.

La herramienta utilizada es GNS3 con IOS "C1700-Sv3y7-Mz_20122-13_20Zh.bin", la cual permite la configuración de los equipos y simular un entorno real del diseño propuesto.[74]

4.3.1.4.3 Reseña De Implementación Por Sdm[75] –Secure Device Manager- (Administrador Seguro De Dispositivos)

SDM Es una herramienta de mantenimiento, basada en una interfaz web propietaria CISCO, es una herramienta java accesible a través del navegador mediante la cual se puede reemplazar el CLI de cisco, por una interfaz gráfica mediante http más amigable y sencilla.

SDM soporta un amplio número de routers CISCO IOS, actualmente se encuentran pre-instalados en las familias de Routers nuevos, y se puede ejecutar desde el PC o del mismo dispositivo.

Se puede acceder desde el vínculo en la PC si se encuentra instalado o a través de un navegador Web si está instalado únicamente en el dispositivo (Router o Switch).

La figura 4.4 muestra la pagina principal de SDM:

---

[73] IOS CLI: Internetwork Operative System Comand Line Interface, proporciona un sistema fijo de comandos de varias palabras, el sistema disponible es determinado por el "modo" y el nivel de privilegio del usuario.

[74] En el anexo 4 se puede apreciar el código fuente de la simulación

[75] Herramienta de mantenimiento, alternativa CLI

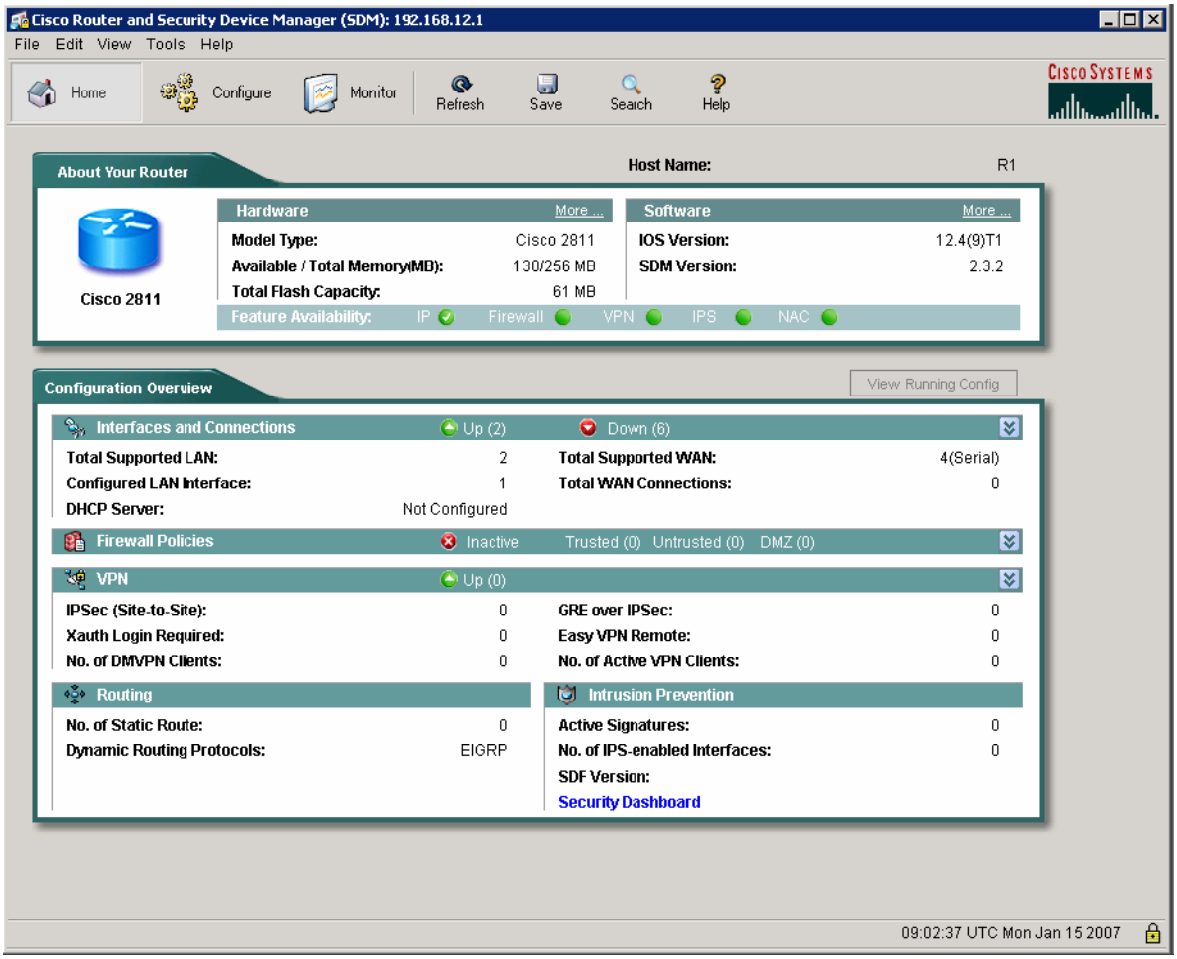

Figura 4.4[76] Pantalla principal de SDM

Como se puede observar, las posibilidades son varias, desde monitorear los dispositivos asociados al equipo y reiniciar los servicios hasta implementar nuevos y modificar los ya implementados.

En la parte de “configure” se puede acceder a un asistente (wizard) de configuración para implementar nuevos servicios

[76] **Imagen de**: CCNP: Implementing Secure Converged Wide-area Networks v5.0 - Lab 3-4

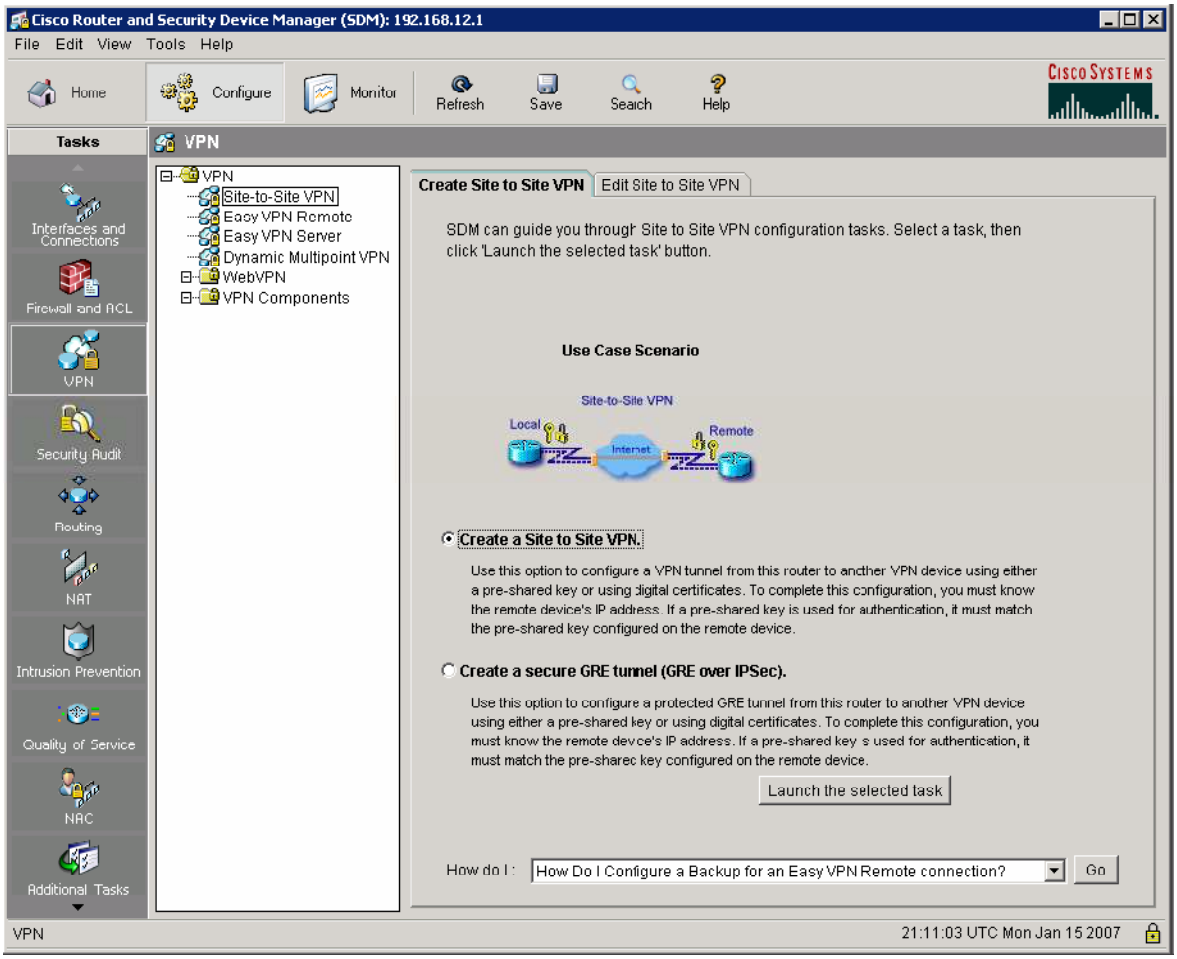

Figura 4.5 Asistente de creación de VPN

Básicamente SDM cumple las mismas funciones de CLI y los parámetros a configurar son exactamente los mismos, lo que varia es la forma de acceder al dispositivo. De la misma manera se puede configurar los clientes.

4.3.1.5 Operar

Esta fase mantiene el estado de la red día a día. Esto implica administración y monitoreo de los componentes de la red, manteniendo el ruteo, administración de actualizaciones, administración del desempeño, e identificación y corrección de errores, esta fase es la prueba final del diseño.

En esta fase se puede y se debe aprovechar las facilidades que proporciona la interfaz grafica SDM ya que tiene un modulo de administración y uno de monitoreo permanente. Se pueden además utilizar herramientas como

"Wireshark[77]" que permite capturar paquetes para poder analizarlos y encontrar extraños fragmentos que pueden deberse a vulnerabilidades de la red, además sirve para ver si esta encapsulando el tráfico mientras está establecida la VPN.

En la figura 4.6 se puede observar los paquetes capturados por "Wireshark" mientras está establecida la VPN en una oficina remota. Como se puede observar, los paquetes están encapsulados por ESP que proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete.

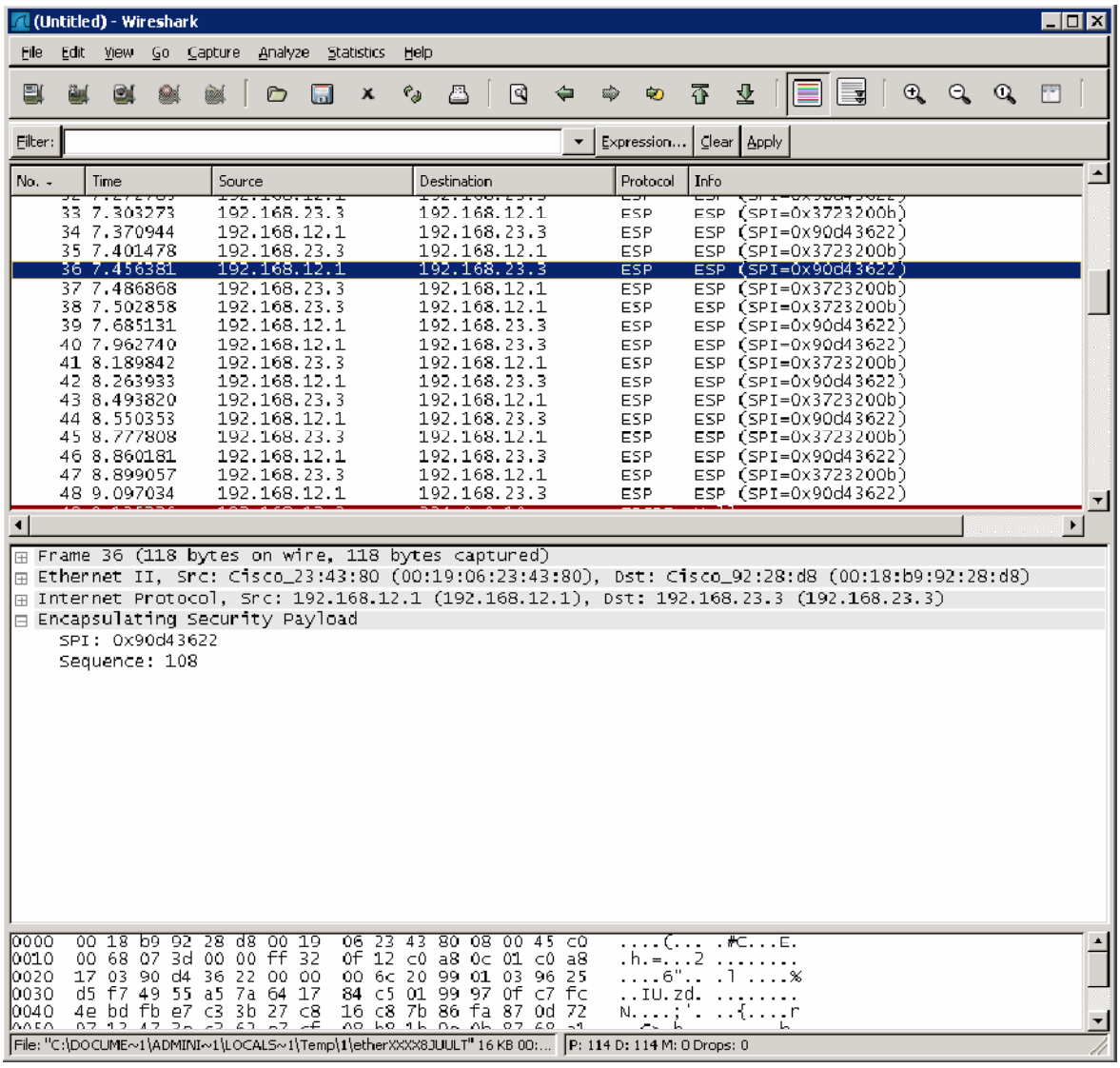

Figura 4.6 Captura de Paquetes de VPN con Wireshark

[77] Wireshark es la nueva versión de Ethereal, el cual es un analizador de protocolos que es utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para el desarrollo de software y protocolos. Es una herramienta de Software Libre.

En la figura 4.7 se puede observar una captura del tráfico de un cliente de una VPN (teletrabajador), y se puede mirar en la fila señalada la cual muestra la captura del tráfico de una sesión SSH[78], la misma que está cifrada por el protocolo sshv2, cabe mencionar que se puede acceder a la línea de comandos de CISCO (CLI IOS) a través de una sesión SSH.

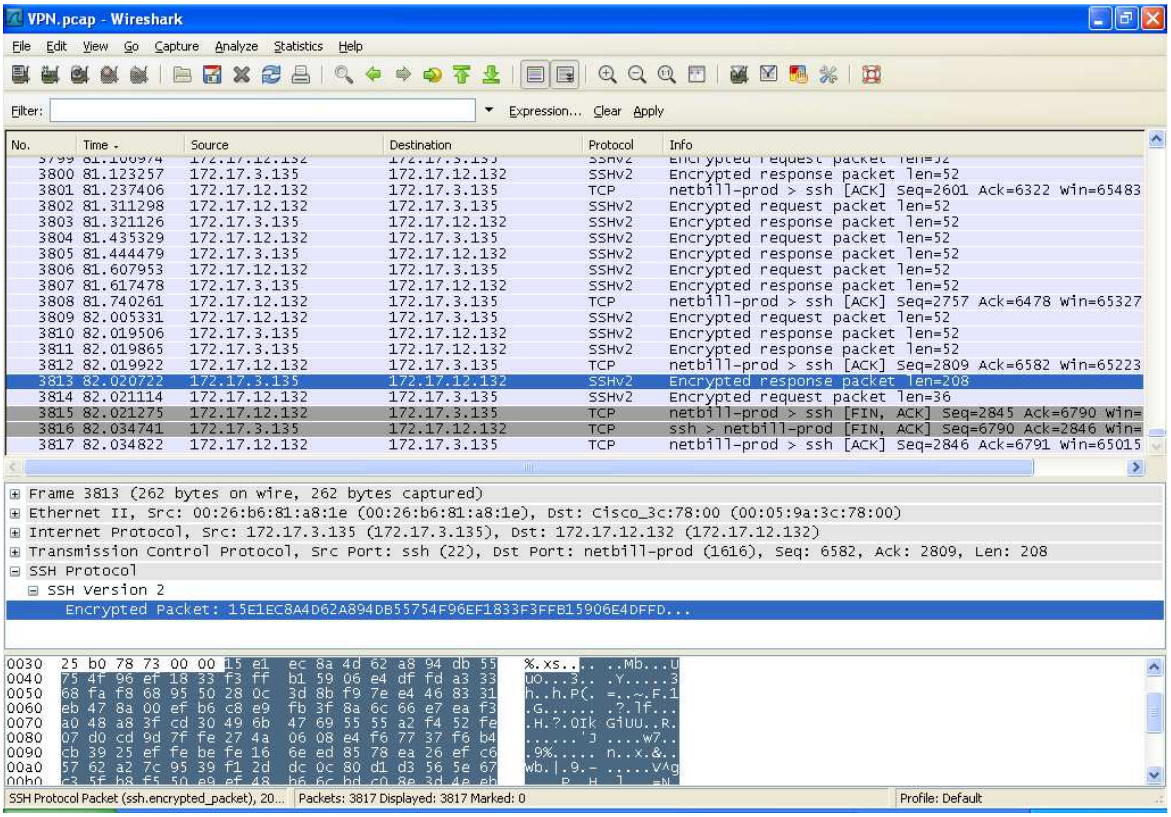

Figura 4.7 Captura de Tráfico de Cliente VPN

Como se puede observar en la siguiente captura, incluso se puede observar que lo que se transmite vía MSN “Protocolo de mensajería instantánea” no se cifra y basta con filtrar el tráfico correcto y se puede ver incluso en texto plano la captura (texto marcado).

[78] Secure Shell: Interprete de comandos seguro

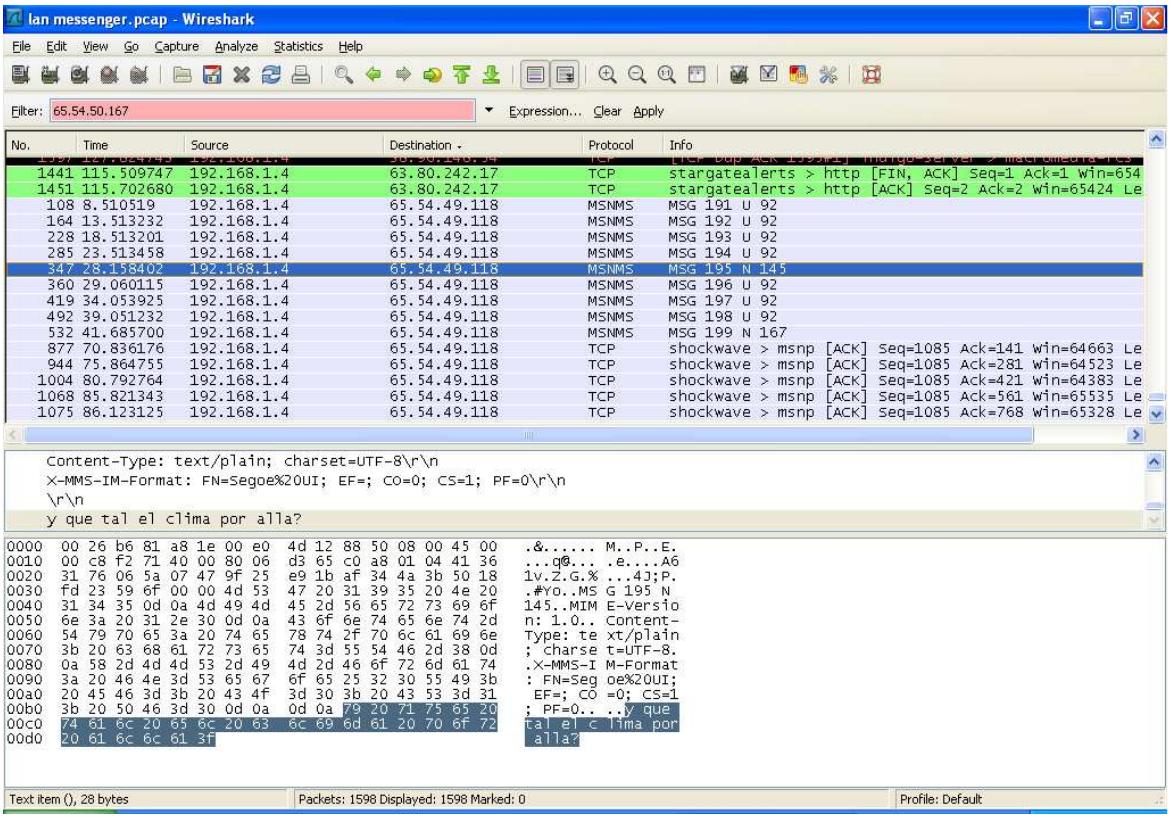

Figura 4.8 Captura tráfico MSN[79]

4.3.1.6 Optimizar

Esta fase envuelve una administración pro-activa, identificando y resolviendo cuestiones antes que afecten a la red. Esta fase puede crear una modificación al diseño si demasiados problemas aparecen, para mejorar cuestiones de desempeño o resolver cuestiones de aplicaciones.

La metodología de diseño PPDIOO, es cíclica por lo tanto va en constante cambio para optimizar, tomando consideraciones principalmente sobre la capa de Core que utilice correctamente la latencia para que sea mínima y optimice la provisión de servicios.

[79] Protocolo de mensajeria instantánea de Microsoft

4.4 PROTOCOLO DE PRUEBAS Y RESULTADOS

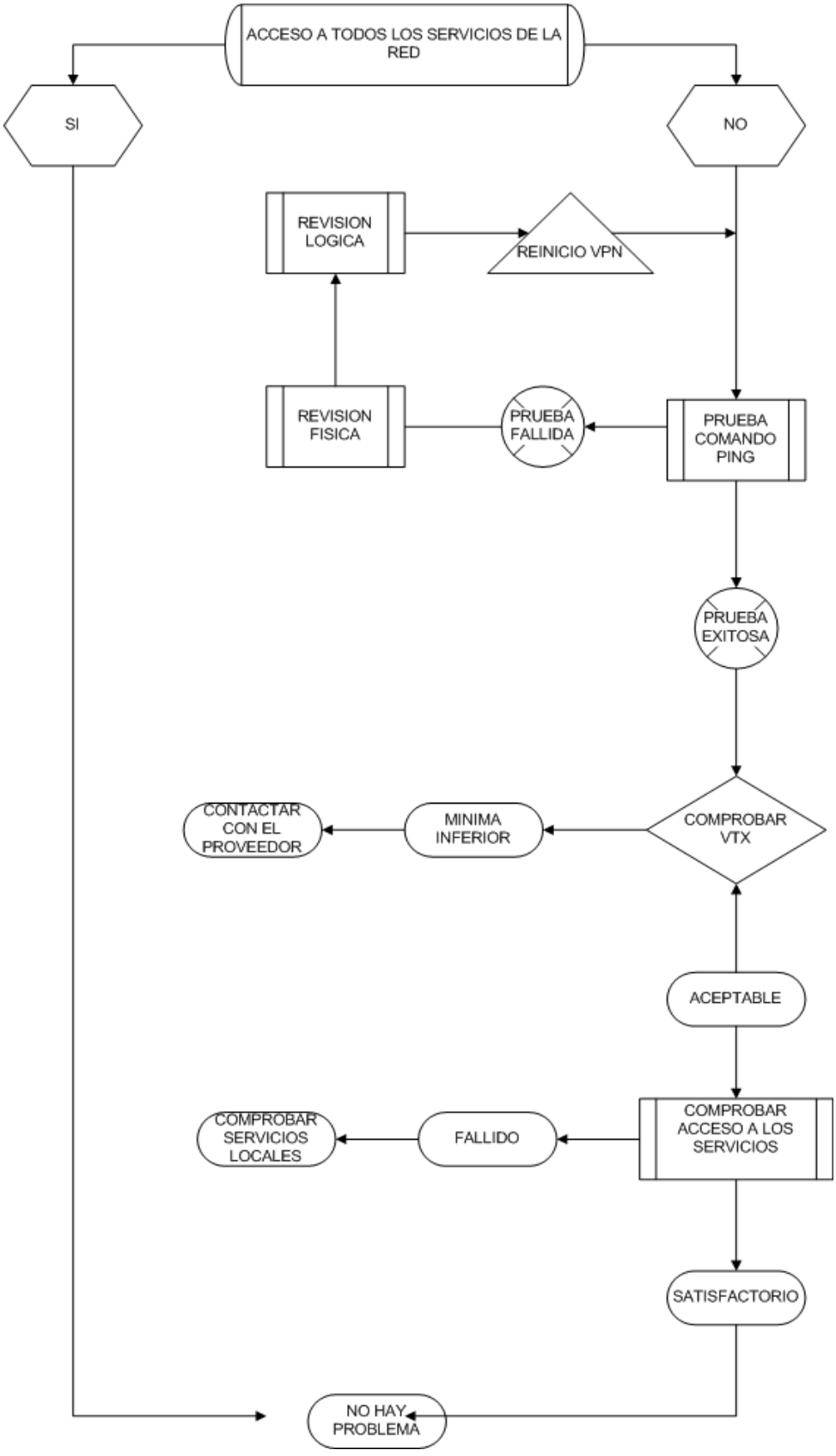

Figura 4.9 Diagrama del Protocolo de pruebas y resultados

Las pruebas que se deben realizar para comprobar la comunicación entre dos dispositivos (sea cual fuere su ubicación geográfica) es recurrir a la utilidad PING.
La utilidad PING permite comprobar el estado de la conexión con uno o varios dispositivos (equipos) remotos, por medio de los paquetes de solicitud de eco y de respuesta de eco, esto permite determinar si un sistema IP especifico es accesible en una red. En resumen cuando se realiza un “PING” a una dirección IP, lo que hace el sistema es enviar a esa dirección una serie de paquetes (por defecto 4) de un tamaño total de 64 bytes a menos que se especifique otro tamaño del paquete y queda en espera del reenvió de estos (eco), por lo que es útil para medir el tiempo que tardan en comunicarse dos puntos geográficamente distantes.
Para el caso de prueba especifico, se va a realizar un “PING” local en primer lugar, con lo que se comprueba que la interfaz funciona correctamente.

>ping 192.168.0.254
Luego con la respuesta exitosa (paquetes recibidos), se procede a realizar un “PING” a una dirección IP pública, para comprobar su conexión con el Internet.
>ping 79.50.61.250
Y seguidamente una prueba de “PING” con una terminal en la otra LAN (GYE).

Con estas pruebas realizadas se puede comprobar la conectividad entre los dos puntos.
Para realizar una prueba de la Vtx se puede realizar un sencillo cálculo para determinar este importantísimo parámetro:

$$Vtx = \frac{\text{Tamaño archivo (bits)}}{\text{Tiempo de descarga (s)}} = bps$$

Figura 4.10 Formula Vtx

Con estas pruebas se puede determinar si la velocidad de la conexión se encuentra dentro los parámetros normales o si tiene algún retardo anormal en la comunicación.

4.5 MANUAL DE USUARIO (ADMINISTRADOR)

El usuario final de la VPN, va a ver todo el proceso de conexión y acceso a la misma, de manera tranparente, en el diseño propuesto[80] se contempla la posibilidad de utilizar un enlace a Internet exclusivo para la VPN, de esta manera no interferiría con el acceso a Internet de los usuarios.

La transparencia en el uso se debe a que, para el usuario final va a ser como acceder a una red local, compartir ficheros, recursos, etc, etc.

Para el administrador[81] de la red en general, su administración se reduciría a las pruebas de conectividad en caso da fallas o tomando como referencia el sub-capitulo siguiente, en el cual se detallan lineamientos a seguir en el caso de fallas o averías. A más de este particular la administración de usuarios remotos (tele-trabajadores) debe estar claramente definida en las políticas de seguridad informática de la Institución.

[80] Grafico 4.12, pagina 96
[81] En el Anexo 5 se encuentra el manual del Administrador

4.6 GESTIÓN DE FALLOS Y AVERÍAS

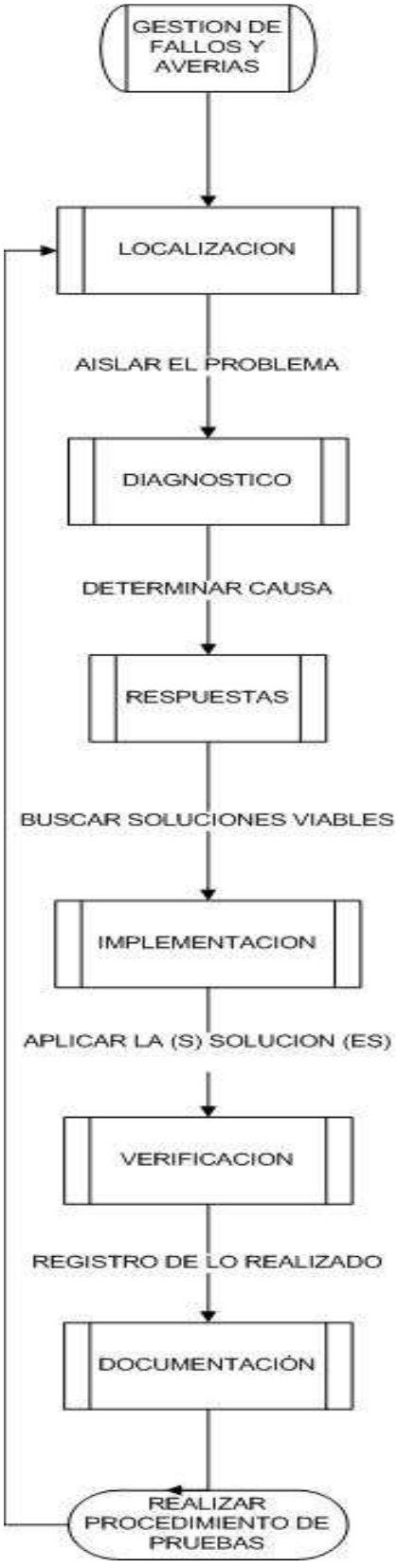

Figura 4.11 Diagrama de Gestión de fallos y averías

Al momento de diagnosticar y resolver fallos en redes IP, es de suma importancia utilizar un procedimiento sistemático que permita cubrir de modo ordenado las diferentes posibilidades que pueden provocar una falla de servicio en una red IP.

4.6.1 LOCALIZACIÓN

Se debe aislar el área de la red en que se genera el fallo, y enseguida se puede realizar los siguientes pasos.

- Verificar la conectividad completa extremo a extremo utilizando la línea de comandos, intentar conectar con telnet o simplemente hacer un eco (*ping*).
- Si existe conectividad extremo a extremo se debería trazar la ruta (tracert) para identificar en que punto de la red comienza la falla.
- Es muy importante durante este proceso verificar las tablas de enrutamiento, un problema de conectividad a nivel de capa 3 o inferior provoca la falta de entradas en la tabla de enrutamiento.
- Localizada el área de la red en la que comienza el fallo, se debe ubicar en el primer dispositivo accesible para comenzar a partir de allí la fase de diagnostico.

4.6.2 DIAGNOSTICO

Determinar con precisión cuál es la causa de la interrupción del servicio. Es importante seguir un orden coherente en el proceso de diagnostico para no descartar equivocadamente ninguna posibilidad. Para esto, el procedimiento habitual es tomar como base las 7 capas del modelo OSI, en orden ascendente, es decir empezando por la capa física.

- En este proceso se debe utilizar los comandos de visualización (show) y relevamiento de actividad (debug) de los dispositivos involucrados.
- Una vez determinada la causa del fallo, se puede proseguir con la fase de elaboración de una respuesta.

4.6.3 RESPUESTA

Una vez establecida la causa del fallo, se debe elaborar una estrategia de solución acorde.

Lo más importante en este punto debe ser la búsqueda de una solución y pruebas de una solución definitiva al problema, la ventaja que tiene el IOS del Cisco es que se puede sacar una imagen con las configuraciones en un estado de pruebas satisfactoria, de esta manera se puede volver a cargar el IOS probado para que funcione antes del fallo, sin embrago la identificación del problema supondría la mejora o el parcheo de una posible falla en este IOS y crearla para cargarla posteriormente.

4.6.4 IMPLEMENTACIÓN

Se implementa la respuesta, la cual puede significar el cambio de partes de equipamiento, la corrección de cableado defectuoso o modificaciones de configuración.

En el peor de los casos puede suponer el cambio del equipo, ventajosamente la garantía y soporte por parte del fabricante es muy extendido.
Cabe recalcar que no se debe realizar ninguna modificaron en la red mientras no se tenga un diagnostico claro. Modificar un elemento que no es la causa del fallo puede complicar aun más la situación y traducirse en una prolongación innecesaria del tiempo de caída del servicio de la red.

4.6.5 VERIFICACIÓN

Se debe verificar que se hayan restablecido los servicios, con una prueba de conectividad extremo a extremo.
Diagrama de flujo

- Si la prueba es exitosa: el problema ha sido superado.
- Si la prueba no es exitosa, se verifica que la capa del modelo OSI que tenía problemas se encuentre operativa. Si no lo está, la solución no fue adecuada, y se debe retomar el proceso desde el principio para proveer una nueva estrategia de solución.
- Si la capa que tenía dificultades se encuentra operativa; ha solucionado el problema que se diagnostico, pero hay otro fallos en una capa superior del modelo OSI, se debe volver a retomar el proceso para identificar este nuevo problema y dar una solución.

4.6.6 DOCUMENTACIÓN

Se debe documentar, cada uno de los pasos seguidos en la Gestión de fallos y averías, desde el momento mismo en el que se localiza el fallo hasta la verificación de la implementación de la solución.

Este es un procedimiento tan importante como la misma solución de la falla, ya que en un caso posterior se tendría un registro de lo realizado independientemente del recurso humano que haya participado en cualquiera de las fases.

Se recomienda que sea un formato siguiendo el grafico de las fases de Gestión y Averías (Grafico 4.11), sin omitir pasos por dispensables que puedan parecer.

4.4 DISEÑO FINAL

El diseño final contempla la adquisición de un nuevo enlace de Internet con el objetivo de que se garantice el acceso a los recursos sin que se sature el canal y con la posibilidad de brindar VoIP en el futuro.

Esto se puede hacer utilizando el canal de la VPN que necesitaría de 16[82] kbps por cada usuario concurrente de la telefonía y correría, sin el peligro de que se sature el canal para el acceso al resto de servicios.

Con nuevo enlace de Internet se necesitaría el acceso a correo electrónico institucional y las aplicaciones web que suman 346,62 y si se desearía gozar de los beneficios de la VoIP sería recomendable que este nuevo canal sea de 1024 kbps.

El enlace de Internet de 1024 sería utilizado para los otros servicios como multimedia, Web correo electrónico público, etc., de esta manera entre los usuarios competirían por el ancho de banda, con la posibilidad de administrar el mismo desde herramientas tanto en software (Squid con delay pools) como en hardware (packetshaper o los mismos Switch 3Com).

---

[82] Recomendación del fabricante de equipos para VoIP, fuente; http://www.cisco.com/en/US/products/pss6655/index.html

En el presente diseño se ha logrado la reutilización de los equipos en cuanto a la capa de acceso y distribución, la infraestructura existente soporta la implementación de la VPN con las adquisiciones de routers indicadas y justificadas, acorde con el alcance del proyecto que plantea la interconexión entre las regionales Guayaquil y Cuenca con la Matriz (Quito), se cumple con el objetivo del presente tema de investigación.

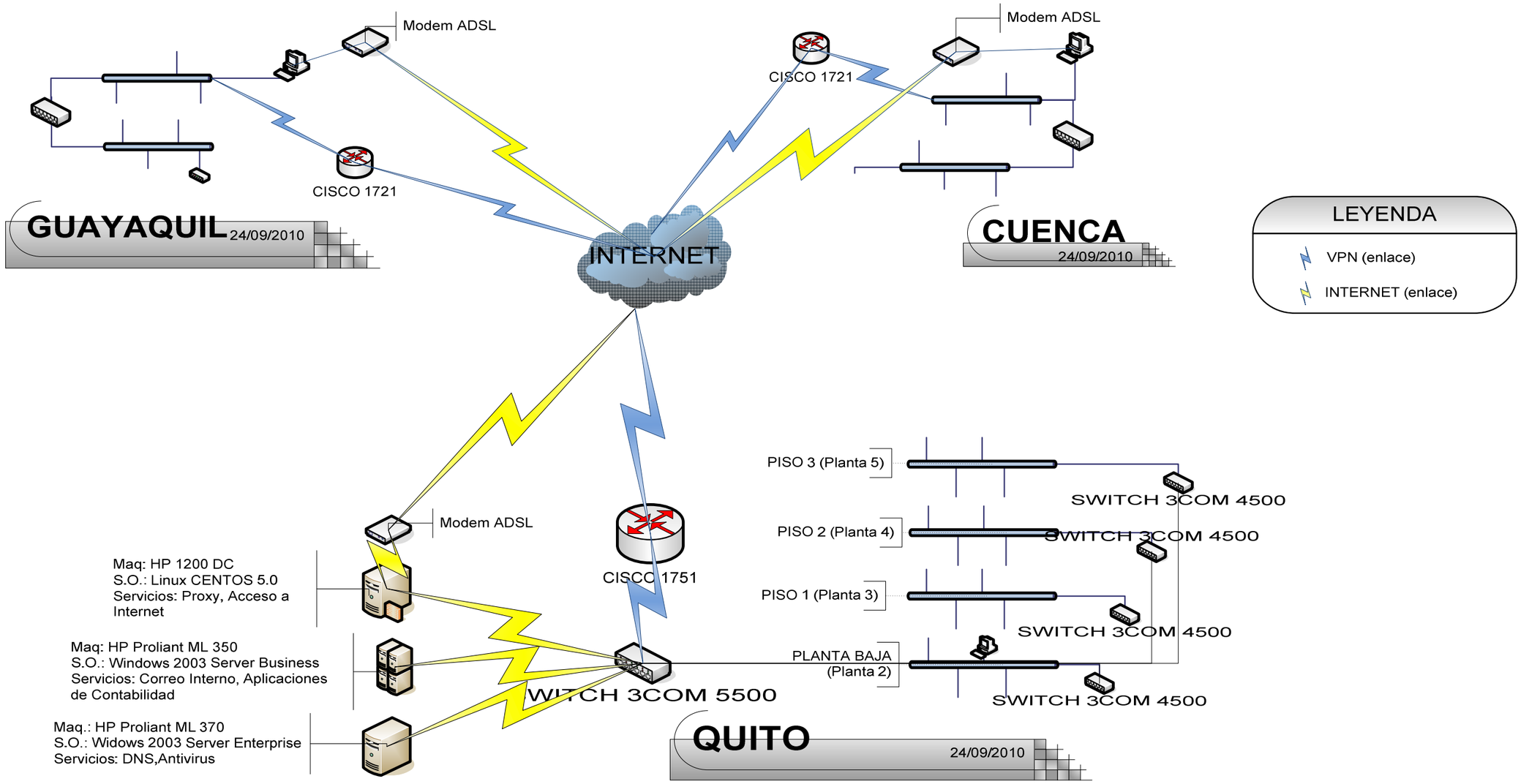

Figura 4.12 Diseño Solución VPN DINSE

CAPITULO 5: ANÁLISIS DE COSTOS

Uno de los retos al implementar nuevas tecnologías, es precisamente los costos propios de la Tecnología y derivados de esta.

"El proceso de diseño de una red involucra analizar y comprender la situación actual de la organización o Empresa, antes de proponer un cambio en la red de comunicación. Para esto, el diseñador debe conocer tanto el estado actual de la empresa (factores internos) como el mercado actual (factores externos)"[83].

Bajo esta reseña, en la propuesta presente se tiene clara la situación de la red en la actualidad y de toda la infraestructura de Tecnología Informática de la DINSE, pero además, se considera la utilidad que tendrá esta propuesta en vista de la tendencia actual del mercado, las cuales se detallan (dos de las más importantes que se involucran directamente con el proyecto) a continuación.

i) Arrendamiento de Equipos:

El equipamiento de Tecnología Informática, es sumamente costoso esa es una realidad evidente y palpable. Por esta razón una de las alternativas viables es el arrendamiento de los equipos (o los equipos en comodato), los cuales vienen además de la garantía del fabricante, con soporte 7x24x365 (7 días a la semana, las 24 horas al día, los 365 días del año) por parte del distribuidor o "dueño" del equipo.

"EL modelo de Acuerdo de Nivel de Servicios (Service Level Agreement, SLA) consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc.

Los principales puntos a cubrir deben ser:

- *Tipo de servicio.*

---

[83] Mejías Acevedo: **Estimación de Costos de una Red de Computadores en la Etapa de Diseño**, PC World Centro América

- *Soporte a clientes y asistencia.*
- *Provisiones para seguridad y datos.*
- *Garantías del sistema y tiempos de respuesta.*
- *Disponibilidad del sistema.*
- *Conectividad.*
- *Multas por caída del sistema.*

Estos puntos son importantísimos a la hora de formalizar de forma contractual una operación.

Implantación de acuerdos de nivel de servicio con proveedores

Para implantar con éxito un SLA han de tenerse en cuenta una serie de factores clave, de los que va a depender en gran medida la obtención de los resultados deseados:

- ***Aspectos críticos***

Los aspectos más críticos, son la definición de procedimientos estándares y los mecanismos de evaluación y seguimiento.

- ***En la implantación de un SLA se deben seguir una serie de puntos***

1. Definición de Objetivos: mejora de la eficacia, reducción de costes, formalización de la relación

2. Identificar expectativas: qué es lo que espera la organización de este acuerdo

3. Adecuada planificación temporal

4. Optimización/rediseño de procesos (revisar los procesos si el SLA no asegura ningún cambio o como mínimo formalizarlos)

- ***Errores más frecuentes en la implantación***
    - *Definir niveles de servicio inalcanzables*
    - *Regulación excesiva*

- *Error en la definición de prioridades*
- *Complejidad técnica*
- *Irrelevancia (si un SLA no tiene ningún efecto sobre el cliente, el objetivo no tiene sentido).”*[84]

ii) Licenciamiento en Red

La tendencia actual del mercado, también está enfocada al licenciamiento de productos de Software a través de un servidor de Licencias, debido a la creciente piratería en todos los ámbitos (y de manera sorprendente en el de Software), se hacen necesarios mayores controles en la autenticación de usuarios del mismo. Uno de los mecanismos que se avizora como el futuro en cuanto a licenciamiento es el licenciamiento en red, que ya lo vienen usando desde hace algún tiempo empresas como Autodesk©[85], y permite múltiples soluciones al licenciamiento dentro de una red de Pc's.

“El licenciamiento de red es una herramienta potente para administrar sus licencias. Es importante determinar qué tipo de licenciamiento es el más apropiado para sus usuarios. Usted puede mantener la mayor parte de las licencias como usuarios autónomos, a la vez que realiza un proyecto piloto con licenciamiento de red, o puede transferir la mayoría de las licencias a un servidor de licencias al tiempo que mantiene algunas licencias autónomas que resultan críticas para los usuarios clave.

La mayoría de las compañías que implementan el licenciamiento de red también cuentan con algunas licencias autónomas para casos especiales.”[86]

Con una VPN se puede licenciar el software sin que necesariamente los equipos se encuentren dentro del mismo lugar. Precisamente todo funcionario del Dpto. Técnico de la DINSE utiliza algún producto Autodesk©.

---

[84] Tomado de: http://www.contratosinformaticos.com/sla/, en el Anexo 6 se muestra un ejemplo de SLA
[85] Proveedor líder de soluciones de diseño en 2D y 3D, creación de contenido digital, y project collaboration software tools.
[86] Tomado de: http://www.autodesk.com

Software de estadística (SPSS[87]) en incluso el licenciamiento de Windows server 2008, tiene *Client Access Licence* (Licencia de Acceso de Cliente), la cual le permite acceder a los recursos de la red y es necesario el licenciamiento a través de esta.

5.1 ANALISIS DE COSTO INICIAL

De acuerdo a lo demostrado en el Capítulo III y sugerido en el Capítulo IV, se deben adquirir nuevos equipos, en el presente Capitulo se realizara una aproximación real de los costos de inversión para la implementación de la VPN, únicamente se considerara los costos de los equipos, costos de implementación y configuración de la red. No se tomaran en cuenta los costos que involucra el diseño, ya que es parte de un proyecto de titulación.

Una de las principales metas en la implementación de nuevos equipos, es "*lograr el equilibrio perfecto, entre los costos iníciales del equipo y los costos operativos del rendimiento a largo plazo*"[88]

Las redes de computadores tienen costos asociados. Desde la amortización de los equipos, pasando por los costos de utilización de servicios hasta los propios costos de la administración.

5.1.1 COSTOS DE LOS EQUIPOS

Los equipos según la tendencia y la disponibilidad de recursos, pueden ser propios o arrendados. En el caso de los equipos propios, existe un costo de amortización, generalmente prorrateado[89] en un periodo estimado como el de vida útil del equipo. Los equipos arrendados tienen un costo mensual prefijado.

Se recomendó[90] la adquisición de 3 routers que cumplen con las características necesarias:

---

[87] Software propietario
[88] Tomado de: http://www.adc.com/us/en/Library/Literature/103633LA.pdf
[89] Costo compartido cliente-proveedor
[90] Capitulo IV

- **Matriz Router CISCO 1751**

Ficha técnica:[91]

CARACTERISTICAS ROUTER CISCO 1751	
General	
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular
Anchura	28.4 cm
Profundidad	22.1 cm
Altura	10 cm
Peso	1.6 kg
Procesador	
Tipo	Motorola MPC860 48 MHz
Memoria	
Memoria RAM	96 MB (instalados) / 128 MB (máx.)
Memoria Flash	32 MB (instalados) / 32 MB (máx.)
Conexión de redes	
Tecnología de conectividad	Cableado
Velocidad de transferencia de datos	100 Mbps
Formato Frames	ANSI T1.413
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, serial
Red / Protocolo de transporte	TCP/IP, AppleTalk, L2TP, IP/IPX, IPSec, PPPoE, L2F, AAL5
Protocolo de direccionamiento	OSPF, EIGRP, HSRP, GRE
Protocolo de gestión remota	SNMP, Telnet
Características	Diseño modular, protección firewall, auto-sensor por dispositivo, soporte de NAT, soporte VLAN, mitad modo dúplex, modo dúplex completo
Cumplimiento de normas	IEEE 802.1Q, X.509
Comunicaciones	
Tipo	Módem DSL
Protocolo de señalización digital	ADSL
Protocolos y especificaciones	ITU G.992.1 (G.DMT)
Expansión / Conectividad	
Total ranuras de expansión (libres)	4 Ranura de expansión

[91]Tomada de la pagina de cisco:
http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet.html

CARACTERISTICAS ROUTER CISCO 1751	
Interfaces	1 x red - Ethernet 10Base-T/100Base-TX - RJ-45
	1 x red - ADSL - RJ-11 (WAN)
	4 x red - FXS
	1 x gestión - auxiliar - RJ-45
	1 x gestión - consola - RJ-45
Diverso	
Algoritmo de cifrado	DES, Triple DES
Método de autentificación	RADIUS, PAP, CHAP, certificados X.509, TACACS+
Cumplimiento de normas	CISPR 22 Class B, EN 60950, IEC 61000-3-2, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, NOM, VCCI-II, IEC 60950, EN55024, EN55022 Class B, AS/NZ 3548 Class B, FCC Part 15 B, ACA TS001, AS/NZS 3260, FCC Part 68, CS-03, UL 1950 Third Edition, CSA 22.2 No. 950 Third Edition, EN 60555-2
Alimentación	
Dispositivo de alimentación	Adaptador de corriente - externa
Voltaje necesario	CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento	20 vatios
Parámetros de entorno	
Temperatura mínima de funcionamiento	0 ℃
Temperatura máxima de funcionamiento	40 ℃
Ámbito de humedad de funcionamiento	10 - 85%

Tabla 5.1 Características 1751

- **Unidades Administrativas Gye y Cue ROUTER CISCO 1721[92]**

Ficha técnica:

CARACTERISTICAS ROUTER CISCO 1721	
General	
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular
Anchura	28.4 cm
Profundidad	22.1 cm
Altura	10 cm
Peso	1.6 kg
Procesador	
Tipo	Motorola MPC860 48 MHz
Memoria	
Memoria RAM	96 MB (instalados) / 128 MB (máx.)
Memoria Flash	32 MB (instalados) / 32 MB (máx.)
Conexión de redes	
Tecnología de conectividad	Cableado
Velocidad de transferencia de datos	100 Mbps
Formato Frames	ANSI T1.413
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, serial
Red / Protocolo de transporte	TCP/IP, AppleTalk, L2TP, IP/IPX, IPSec, PPPoE, L2F, AAL5
Protocolo de direccionamiento	OSPF, EIGRP, HSRP, GRE
Protocolo de gestión remota	SNMP, Telnet
Características	Diseño modular, protección firewall, auto-sensor por dispositivo, soporte de NAT, soporte VLAN, mitad modo dúplex, modo dúplex completo
Cumplimiento de normas	IEEE 802.1Q, X.509
Comunicaciones	
Tipo	Módem DSL
Protocolo de señalización digital	ADSL
Protocolos y especificaciones	ITU G.992.1 (G.DMT)
Expansión / Conectividad	
Total ranuras de expansión (libres)	4 Ranura de expansión

[92] Como se puede observar claramente, únicamente varia respecto del router 1751 en sus interfaces, ya que son de la misma familia (1700)

CARACTERISTICAS ROUTER CISCO 1721	
Interfaces	1 x red - Ethernet 10Base-T/100Base-TX - RJ-45
	1 x red - ADSL - RJ-11 (WAN)
	1 x gestión - auxiliar - RJ-45
	1 x gestión - consola - RJ-45
Diverso	
Algoritmo de cifrado	DES, Triple DES
Método de autentificación	RADIUS, PAP, CHAP, certificados X.509, TACACS+
Cumplimiento de normas	CISPR 22 Class B, EN 60950, IEC 61000-3-2, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, NOM, VCCI-II, IEC 60950, EN55024, EN55022 Class B, AS/NZ 3548 Class B, FCC Part 15 B, ACA TS001, AS/NZS 3260, FCC Part 68, CS-03, UL 1950 Third Edition, CSA 22.2 No. 950 Third Edition, EN 60555-2
Alimentación	
Dispositivo de alimentación	Adaptador de corriente – externa
Voltaje necesario	CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento	20 vatios
Parámetros de entorno	
Temperatura mínima de funcionamiento	0 ℃
Temperatura máxima de funcionamiento	40 ℃
Ámbito de humedad de funcionamiento	10 - 85%

Tabla 5.2 Características Router CISCO 1721

Precios referenciales[93]:

EQUIPO	CANTIDAD	COSTO UNITARIO	TOTAL
Router Cisco 1751	1	205	205
Router Cisco 1721	2	230	460
		Total	665

Tabla 5.3 Precios referenciales Equipos

5.2.2 ENLACE A INTERNET

Es evidente que si se dispone de un enlace únicamente para la VPN su funcionamiento no dependerá del uso del Internet en la Institución.

Internet corporativo: 1024 kbps nivel de compartición 1:1, para la Matriz

Precio referencial: 250 USD mensuales[94]

Internet corporativo: 512 kbps nivel de compartición 1:1, para cada unidad administrativa.

Precio referencial 150 USD mensuales

5.2.3 COSTO DE IMPLEMENTACION

Este valor hace referencia a los costos de la mano de obra para el montaje y configuración de los equipos; instalación y configuración de la VPN. Estos costos no se deben estimar ya que el personal de TI de la DINSE pudiera implementarlo de manera sencilla con el respaldo del IOS configurado con anterioridad.

Sin embargo en el menos favorable de los casos, se tendría que pedir los servicios de un especialista ajeno a la institución, considerando que la hora

[93] Proformas en el Anexo 7
[94] Propuesta de servicio Anexo 8

trabajo en promedio para el soporte senior[95] de TI esta en 20 USD y el estimado del tiempo de implementación del proyecto se ha calculado en dos días laborables (16 horas[96]), el costo sería de 320 USD.

COSTOS DE IMPLEMENTACION				
DESCRIPCION	**NUMERO DE TRABAJADORES**	**HORAS DE TRABAJO**	**VALOR POR HORAS DE TRABAJO**	**TOTAL**
Personal de soporte TI senior	1	8	20	320
Supervisión por parte de TI de la DINSE	1	8	nomina	nomina

Tabla 5.4 Costos de Implementación

5.2.4 COSTO TOTAL DEL PROYECTO

El costo total del proyecto es la suma de los costos de los equipos, enlaces y de implementación.

Todos los precios son referenciales y están sujetos a variaciones de acuerdo al comportamiento del mercado (oferta demanda), tal es así que las proformas que emiten los diferentes distribuidores de equipos de TI, tienen una validez máxima de 45 días.

[95] Ingeniería de soporte con especialidad en Tecnología Informática, a nivel de soluciones empresariales.
[96] Al cumplir con todos los requerimientos previos, únicamente se haría una prueba con los dispositivos a nivel local y luego su instalación en física seria simplemente interconectar los dispositivos.

COSTOS TOTAL PARA LA IMPLEMENTACION DE LA SOLUCION VPN PARA LA DINSE	
DESCRIPCION	TOTAL USD
COSTO EQUIPOS	665
COSTO IMPLEMENTACION	320
COSTOS MENSUAL ENLACE	150
TOTAL	1135

Tabla 5.5 Costo total referencial

5.3 ANÁLISIS COSTO OPERACIONAL.

El costo operacional, implica los recursos económicos utilizados para continuar el normal y optimo funcionamiento, de la solución para la interconexión de la Matriz con sus unidades administrativas regionales en la Dirección Nacional de Servicios Educativos DINSE a través de una VPN.

Son los gastos que surgen, de las actividades actuales de la solución ya implementada, en un determinado periodo de tiempo. Tales como recursos humanos, servicios básicos, arrendamiento, etc., es decir todo lo que está relacionado de alguna manera con el proyecto.

En este contexto, la principal motivación del uso y difusión de esta tecnología (VPN) es la reducción de los costos de comunicaciones directos, tanto en líneas dial-up como en vínculos WAN dedicados. Los costos se reducen drásticamente en estos casos:

- En el caso de accesos remotos, llamadas locales a los ISP (Internet Service Provider) en vez de llamadas de larga distancia a los servidores de acceso remoto de la organización o institución. O también mediante servicios de banda ancha.

- En el caso de conexiones punto a punto, utilizando servicios de banda ancha para acceder a Internet, y desde Internet llegar al servidor VPN de la organización. Todo esto a un costo sensiblemente inferior al de los vínculos WAN dedicados.

Los costos de servicios básicos (energía eléctrica en este caso) son despreciables, ya que el consumo es equivalente a lo que consume una radio[97] cualquiera.

Ahora bien se ha contemplado que una alternativa viable seria el arrendamiento de equipos, este tendría un costo mensual y tiene la ventaja de que se puede renovar por una cifra bastante baja, si en lugar de esto se tiene los equipos propios (adquiridos por la DINSE) existe siempre el riesgo por mínimo que sea, de que sufra un daño irrecuperable y se tenga que adquirir uno nuevo.

Para este proyecto específico se ha referido la compra de los equipos, que se han recomendado a la Unidad de Gestión Tecnológica.

En la gran mayoría de contratos de arrendamiento de equipos, prestación de servicios o incluso compra de equipos, se detalla un mantenimiento mínimo de dos veces al año de los equipos.

Esto obedece a que los equipos: están plenamente probados, cumplen con la garantía de reposición de ser el caso y está asegurado su funcionamiento en un periodo de dos años sin inconvenientes. La tendencia en el mercado también apunta a que se vendan equipos con mantenimiento preventivo (2 veces) en el primer año, sin costo adicional, con la seguridad de que terminado el año se va a comprar el mantenimiento a este mismo proveedor. Adicionalmente existe el seguro de equipos es decir a parte de adquirir el equipo se compra un seguro del proveedor (en algunos casos[98] el propio fabricante) el cual consiste en la reposición inmediata del equipo, si este llegara a sufrir algún daño inesperado incluso abarca percances como incendios, sobrecarga de voltaje, etc.

---

[97] De acuerdo a lo detallado en las “features” características del producto.
[98] Como por ejemplo en los equipos de video conferencia Polycom

Con lo analizado y detallado anteriormente, y estimando que el periodo de tiempo para calcular el costo operacional, es de un año, se tiene el siguiente escenario:

- Será necesario el soporte senior de TI por lo menos dos veces por año, por cuestiones de mantenimiento[99] y eventualmente "upgrade[100]". El cual no excederá la hora de trabajo.

- El enlace a Internet es un caso especial ya que tiene un costo mensual y está sujeto a las condiciones del mercado.

COSTOS OPERACIONALES			
DESCRIPCION	**CANTIDAD**	**VALOR UNITARIO**	**TOTAL USD**
Personal de soporte TI señor (2 horas x año)	1	20	40
Enlace a Internet (x 1 año)	1	150	1800
		TOTAL	1840

Tabla 5.6 Costos Operacionales

5.4 ANALISIS DEL COSTO TOTAL DEL PROYECTO

Es necesario realizar una evaluación del proyecto, para así determinar su viabilidad, considerando los aspectos que permitan determinar en qué medida el proyecto va a ser rentable.

El presente proyecto de Investigación no tiene como objetivo el reducir costos, tiene como objetivo ofrecer soluciones reales a necesidades evidentes de los funcionarios de una Institución como la DINSE, que está presente de alguna[101] manera en todo el territorio ecuatoriano y considerando que la Institución está

[99] Si no existiere ningún percance o particularidad el mantenimiento se lo puede hacer sin contratiempos de manera remota.
[100] Actualización del IOS.
[101] Si bien no dispone de oficinas en cada provincia del Ecuador, tiene Unidades administrativas regionales que abarcan las provincias mas cercanas cubriendo así el territorio nacional.

ligada intrínsecamente con la Educación que es el pilar fundamental del consecuente desarrollo de las naciones.

Sin embargo de lo expuesto anteriormente, si existe un incuestionable ahorro de recursos.

Para corroborar lo citado se toma de ejemplo del uso de medios impresos para compartir información utilizando el correo tradicional.

Si se envían un promedio de 75[102] fojas útiles diariamente a través del correo tradicional a un costo referencial estimado de 15 dólares diarios se tiene:

15 USD diarios x el número de días laborables 246[103]= 3690 USD

Y si con la implementación del proyecto se logra reducir en un 50% el uso del correo tradicional, se tendría un ahorro de 1845 USD aproximadamente.

Lo cual es coincidencialmente equivalente al costo operacional del proyecto en un año.

Y esto es únicamente si se logra la reducción del envió-recepción de correos tradicionales[104], si se considera el licenciamiento en red, la administración y soporte remoto, la compartición de archivos en tiempo real, y con este canal de Internet incluso se puede lograr implementar VoIP[105] sin inconvenientes de acuerdo a lo demostrado en el Capítulo IV.

En el peor de los casos la inversión estaría plenamente justificada en el lapso de un año y con un sistema de cableado estructurado se contempla que el proyecto sea de al menos 5 años sin cambios radicales.

---

[102] Capítulo IV Pág. 54
[103] Si se considera que existen 23 días laborables al mes, por eliminación de sábados y domingos.
[104] Uno de los objetivos que si esta contemplado, es precisamente el uso de una herramienta de seguimiento de procesos de trabajo "workflow" a nivel nacional, para eliminar sistemáticamente el uso de correo tradicional, al menos para documentos internos.
[105] Si bien el costo de las llamadas nacionales están por el momento al mismo precio que las llamadas locales, el ahorro sigue siendo por utilizar un canal que estaría disponible sin costo adicional.

CAPITULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- El desarrollo y la implementación de las redes corporativas y la computación en general, en el Ecuador ha debido recorrer un gran camino para estar acorde a las nuevas Tecnologías de la Información.

- El evidente alto costo de los servicios de telecomunicaciones en el país, se debe principalmente a que no se contempló el acceso al cable submarino de fibra panamericano, y aunque ya se tiene acceso[106], aun se debe subarrendar canales con Colombia y Perú, para garantizar la disponibilidad del servicio.

- Uno de los decretos del actual gobierno se refiere a la utilización de Software libre en las entidades de administración del estado, si bien se lo ha venido aplicando en la parte de plataformas y desarrollo de las aplicaciones (Java/php/Joomla frente a .net, adobe, etc.) aun no hay establecida ni a manera de plan piloto, lineamientos que permitirán la migración de los usuarios finales a un Sistema Operativo de código abierto.

- Las redes Privadas Virtuales son una solución viable a distintos problemas que se suscitan al tener dos oficinas geográficamente distantes, entre los beneficios que se obtienen evidentemente se contemplan los económicos, por ejemplo en el caso de que se desee realizar una conexión entre dos sedes de empresas, tan distantes geográficamente como una en Japón y la otra en Ecuador, sería muy costoso (rayaría en lo inexplicable pero valido para el ejemplo) el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque solo se hace uso de Internet que es un conjunto de redes conectadas entre sí. Pero observándolo desde el punto de vista de los usuarios particulares de Internet, como son los estudiantes o investigadores que utilizan el Internet como un medio de comunicación,

[106] Telefónica, tiene acceso al cable submarino desde Julio del 2007

de compartimiento de información, este tipo de redes perjudican este desarrollo, debido a varios factores como son, el consumo de ancho de banda y el consumo de direcciones IP[107].

- El protocolo IPsec responde a la necesidad creciente de garantizar un nivel de seguridad imprescindible para las comunicaciones entre empresas, instituciones y comercio electrónico.

- Las nuevas aplicaciones distribuidas y sofisticadas han provocado un movimiento abrupto en los administradores de redes, donde los usuarios con cierto grado de conocimientos avanzados requieren un ambiente apropiado para su desarrollo.

- La técnica de switcheo cada vez más avanzada proporciona soluciones óptimas para la segmentación del tráfico de información en las redes locales controlando los costos y manteniendo una curva costo-efectividad aceptable para los clientes. Tomar en cuenta todos los escenarios posibles, permite instalar una sola vez la infraestructura física, y aun servir para los requerimientos de la institución, todavía fuera del horizonte actual. Los traslados, adiciones, o cambios ya no requieren más el tendido de nuevos cables, excepto cuando el espacio físico crezca.

- El uso de emuladores, permite la detección en tiempo real de fallas en el diseño o la implementación, ya que a diferencia de un simulador, no solo trata de reproducir el comportamiento de un programa, sino que trata de modelar de forma precisa el dispositivo que esta emulando, además de que un emulador está en capacidad de usar las mismas plataformas que el dispositivo físico real.

- Es prácticamente indispensable estar en permanente contacto con las unidades administrativas en instituciones que dependen directamente del gobierno central[108].

---

[107] Con el uso de IPV6 esto no tendría sentido

- El uso de Líneas de Comando (CLI) para la configuración de equipos CISCO es recomendable en lugar de hacerlo por SDM (Servicio de Administración del Dispositivo) ya que SDM consume muchos más recursos del dispositivo y pudiera interferir en el normal funcionamiento del mismo.

- La importancia del acuerdo con el distribuidor sobre la disponibilidad del enlace de Internet (Acuerdo de Nivel de Servicio) es primordial ya que garantiza el trasporte de datos (texto, voz, video etc.) y únicamente se debe preocupar del óptimo funcionamiento de los equipos de la institución.

- Con la implementación del proyecto se lograra reducir el uso del correo tradicional, y hacer posible el acceso al correo institucional de manera fácil y confiable a todas las unidades administrativas que componen la DINSE.

- El presente diseño va a permitir acceder a las nuevas formas de licenciamiento, de manera totalmente transparente para el usuario, y de fácil gestión para el administrador de la red y de la distribución de las licencias.

---

[108] Esto debido a que actualmente, esta centralizada la asignación de recursos a través del Ministerio de Finanzas

6.2 RECOMENDACIONES

- Implementar un sistema de cableado estructurado en las Unidades regionales administrativas, para optimizar los recursos y mejorar el funcionamiento de la red.

- La contratación inmediata de un enlace de Internet independiente del servicio que actualmente disponen, ya que los usuarios del Internet competirían entre si por el ancho de banda sin perjudicar la VPN.

- Realizar inmediatamente la actualización de las políticas de seguridad informática contemplando el nuevo escenario que es contar con una VPN.

- Se recomienda la utilización de un Software antivirus que permita la administración centralizada, en el caso de la matriz las actualizaciones del mismo serian a través de una consola central y en las unidades administrativas localmente pero con la implementación de las mismas políticas que en la Matriz.

- Se recomienda la implementación de un servidor de actualizaciones para software ya que el intercambio permanente de información es un riesgo de seguridad por la filtración de *malewares*.

- Diseñar una solución de migración al menos en la parte mas viable, a soluciones de software libre para usuarios finales, ya que el gobierno central ha declarado la necesidad del uso de esta alternativa para las entidades publicas

- Mantener los equipos en un armario de telecomunicaciones diferente, para que la identificación de los dispositivos de conexión estén plenamente definidos y no haya el peligro de errores involuntarios.

- Que en el mediano plazo, se contemple la posibilidad de implementar VoIP aprovechando las ventajas que ofrece la VPN, como es la administración centralizada de redes LAN distantes, haciendo posible la implementación

de este servicio, para lo cual se debe re-calcular las necesidades de AB del enlace de internet

- Socializar y de ser posible capacitar a los usuarios, en lo que tiene que ver con los beneficios de contar con una VPN.
- Implementar un sistema de aire acondicionado[109], para los equipos que se encuentran en el cuarto de telecomunicaciones, para no tener inconvenientes futuros debido a que las especificaciones de la temperatura en estos dispositivos, es estricta. Tal es así que, al momento que se sobre pase del límite indicado, el equipo empezara a tener funcionamiento no deseado.
- Motivar a los funcionarios de los diferentes departamentos, a utilizar el correo electrónico en lugar del correo tradicional.
- Realizar un manual de datos para que, los más sensibles puedan ser respaldados durante el día localmente en cada ciudad y realizar una subrutina que permita el almacenamiento en una unidad de cintas en la Matriz durante la noche, así no interferiría con el canal de Internet.
- Realizar un estudio que permita ver la posibilidad de usar el canal de Internet como respaldo para la VPN y viceversa.

[109] Actualmente la DINSE Matriz, cuenta con ventiladores que si bien cumplen su objetivo, son anti técnicos y no permiten ningún tipo de administración.

BIBLIOGRAFÍA

- BERT HUBERT, Msc. “Enrutamiento avanzado y control de tráfico en Linux”
- TOBY SCANDIER, “Guía del estudio de redes, cuarta edición”
- VICENTE JOSÉ AGUILAR, Ing. “Implementación de Redes Privadas Virtuales”
- JUAN BLÁZQUEZ MARTIN, Msc. “Redes Privadas Virtuales: Poner puertas al campo”
- LUIS GUERRERO RAMIREZ, Ing. “Seguridad en Redes Telemáticas”
- ARIGANELLO ERNESTO, Ing. “Redes CISCO: Guía de estudio para la certificación CCNA 640-802”
- ANDREW TANENBAUM, “redes de computadoras”
- PCWorld, “303 Numeros en 30 años”, *PC WORLD,* año XXX, Nº 303, Ecuador, Mayo 2008
- Manual de Curso Uniplex, “redes DINSE 2007”
- RFC 1171 (Referente a PPP)
- RFC 1701-2 (Referente al protocolo GRE)
- Cisco Press 642-825 CCNP ISCW Official.Exam.Certification.Guide.Jul.2007
- CCNP: Implementing Secure Converged Wide-area Networks v5.0 - Lab 3-4
- Mejías Acevedo: Estimación de Costos de una Red de Computadores en la Etapa de Diseño, PC World Centro América

INTERNET

- www.pcwla.com
- http://es.wikipedia.org/w/index.php?title=Redes_de_datos&redirect=no
- www.gfc.edu.ec
- www.monografias.com

- *www.ecualinux.com*
- http://es.wikipedia.org/wiki/
- www.ecualug.org
- http://www.garciagaston.com.ar/
- www.cisco.com/web/ES/
- http://www.dric.com.mx/seguridad/di/di4.php
- http://www.guiaweb.gob.cl/guia/capitulos/tres/accesorapido.htm
- http://www.contratosinformaticos.com/sla/
- http://www.autodesk.com
- http://www.adc.com/us/en/Library/Literature/103633LA.pdf
- http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet.html
- http://blog.espol.edu.ec/ylambert/2010/08/05/kbps-vs-kb-%C2%BF128-256-512-kbps-%C2%BF1mbps-valores-que-nos-confunde-pero-cual-es-la-velocidad-real-de-internet/

ANEXOS

ANEXO 1

PLANOS CABLEADO ESTRUCTURADO DINSE MATRIZ

ANEXO 2

DIAGRAMA LOGICO DINSE MATRIZ

ANEXO 3

DOCUMENTO QUE CERTIFICA LA CONSTATACIÓN FÍSICA DE LA RED DE GUAYAQUIL

ANEXO 4

CODIGO FUENTE IMPLEMETACION SIMULADOR GNS3

!--- Creamos la configuración de la política IKE "define una combinación de parámetros de seguridad que serán usados durante la negociación IKE"[110] (definición del intercambio de llaves). Cada Política se identifica por su numero de prioridad (de 1 a 10000; 1 la prioridad mas alta)

uio(config)# crypto isakmp policy 1

!--- Especificamos el algoritmo de encriptación que se va a utilizar, en este caso 168-bit Triple DES –Data Encryption Standar- (Estándar de Cifrado de datos)

uio(config-isakmp)# encryption 3des

!--- Escogemos el algoritmo de hash[111] a usar, en este caso SHA –Secure Hash Algoritm- (Algoritmo hash seguro)

uio(config-isakmp)# hash sha

!--- Determinar el método de autenticación, este puede ser: pre-shared keys (pre-share), RSA1 encrypted nonces (rsa-ener), o RSA signaturas (rsa-slg)

uio(config-isakmp)# pre-share

!--- Especificamos el identificador del grupo Diffie-Hellman[112]: 768-bit Diffie-Hellman (1) o 1024-bit Diffie-Hellman (2)

uio(config-isakmp)# group 2

!--- Determinar el tiempo de vida de la asociación de seguridad (IKE-SA) en segundos (86400 s= 1 Dia)

uio(config-isakmp)# lifetime 86400

!--- Volvemos al modo de configuración global

uio(config-isakmp)# exit

---

[110] Technical Support & Documentation CISCO, Document ID 46242
[111] Hash, se refiere a una función para generar claves que representan de manera casi univoca a un documento, resumir o identificar un dato a través de la probabilidad
[112] Es un protocolo que permite el intercambio secreto de claves entre dos partes, que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada)

!--- En la Matriz: elegimos la identidad ISAKMP (address o hostname) que el router usara en las negociaciones IKE.

uio(config)# crypto isakmp identity address

!--- En la Matriz: establecer el secreto compartido que se usara con el router de la oficina remota

uio(config)# crypto isakmp key 1223334444 192.168.2.254

!--- En la oficina remota (Gye): se elige la identidad ISAKMP (address o hostname) que el router usara en las negociaciones IKE.

gye(config)# crypto isakmp identity address

!--- En el router gye: establecer el secreto compartido que se usara con el router de la oficina central.

gye(config)# crypto isakmp 1223334444 192.168.0.240

!--- para comprobar los valores de cada parámetro de seguridad de la politica IKE se puede ejecutar el comando

uio# show crypto isakmp policy

Configuramos IPsec en los dos extremos:

- Creamos una Crypto ACL

Las Crypto ACL se usan para definir el tráfico que será protegido mediante cifrado.

!--- En la Matriz: ciframos todo el tráfico IP que salga de la oficina central (uio) hacia la oficina remota (gye)

uio(config)# access-list 109 permit ip 192.168.0.240 192.168.2.254

!--- En la oficina remota (gye): ciframos el tráfico IP que sale de hacia la Matriz (uio)

gye (config)# access-list 109 permit ip 192.168.2.254 192.168.0.240

!--- Se puede verificar la Crypto ACL con el siguiente comando

uio# show access-list 109

- Definimos los transforms Sets (conjuntos a transformar)

!--- Establece la políticas de seguridad IPSEC que se usaran en las comunicaciones, eligiendo el modo transporte (AH) o túnel (ESP).

uio(config)# crypto ipsec transform-set STRONG esp-3des esp-sha-hmac

!--- Verificamos el Transform set

uio# show crypto ipsec transform-set

- Configuramos Crypto Map

!--- Se crea un Crypto Map de nombre QUITO, se establece el numero de secuencia de entrada, obligando a usar IKE para establecer Sas (Asociaciones de Seguridad).

uio(config)# crypto map QUITO 1 ipsec-isakmp

!--- De los transforms sets que se haya definido, especificar cual se usara en esta entrada del crypto-map

uio(config-crypto-map)# set transform-set STRONG

!--- Activar Perfect Forward Secrecy(Proveee seguridad adicional en la solicitud de SA)

uio(config-crypto-map)# set pfs group 2

!--- Defnir la direccion del host remoto (gye)

uio(config-crypto-map)# set peer 192.168.2.254

!--- Establecer el tráfico que se va a cifrar, que esta previamente definido en una ACL.

uio(config-crypto-map)# match address 109

!--- Volvemos al modo privilegiado

uio(config-crypto-map)# exit

!--- Verificamos la configuracion del Crypto Map

uio(config)# show crypto map

!--- Entrar al modo de configuración de la interfaz donde se aplicara el crypto map

uio(config)# interface fastethernet0/0

!--- Se aplica el crypto map a la interfaz física.

uio(config-if)# crypto map QUITO

!--- Volvemos al modo privilegiado

uio(config-if)# exit

!--- Verificación de la asociación de la interfaz y el crypto map

uio# show crypto map interface fastethernet0/0

!--- Verificación de la asociación de seguridad (SA)

uio# show crypto ipsec sa

!--- Guardamos los cambios

uio# write

Configuración de un cliente remoto o teletrabajador:

!--- Creamos una política IKE fase 1

uio(config)# crypto isakmp policy 1

!--- Seleccionamos 3des el tipo de encriptacion

uio(config-isakmp)# encryption 3des

!--- El algoritmo de hash será MD5

uio(config-isakmp)# hash md5

!--- La clave de encriptacion pre-share

uio(config-isakmp)# authentication pre-share

!--- Especificamos el identificador del grupo Diffie-Hellman: 768-bit Diffie-Hellman (1) o 1024-bit Diffie-Hellman (2)

uio(config-isakmp)# group 2

!--- Regresamos a la configuración global

uio(config-isakmp)# exit

!--- Creamos un grupo de clientes de la VPN

uio(config)# crypto isakmp client configuration group VPNGROUP

!--- Usamos la clave 1223334444

uio(config-isakmp-group)# key 1223334444

!--- Las direcciones de los clientes se definen en el pool de direcciones VPNPOOL

uio(config-isakmp-group)# pool VPNPOOL

!--- Direccionamos al Servidor de Nombres de Dominio DNS

uio(config-isakmp-group)# dns 192.168.1.1

!--- Regresamos a la configuración global

uio(config-isakmp-group)# exit

!--- Se crea un trasnform set para la política IKE fase 2

uio(config)# crypto ipsec transform-set TRANSFORM-1 esp-3des espsha-hmac

!--- regresamos al modo de configuración global

uio(cfg-crypto-trans)# exit

!--- Iniciamos el servicio de autenticación AA

uio(config)# aaa new-mode1

!--- Verificamos la autenticación de logeo para el grupo por defecto, usando el usuario local de la base de datos

uio(config)# aaa autentication login default local

!---- Verificamos la autenticación para el grupo VPNAUTH usando el usuario local dela base de datos.

uio(config)# aaa autentication login VPNAUTH local

!--- Verificamos la autorización de ejecutar para el grupo por defecto usando el usuario local de la base de datos.

uio(config)# aaa autorization exec default local

!--- Verificamos la autorización de acceso a la red para el grupo VPN AUTH con el usuario local de la base de datos.

uio(config)# aaa autorization network VPNAUTH local

!--- Creamos el usuario para la autenticación de la VPN

uio(config)# username prengifo secret password1

uio(config)# username asistente secret password2

!--- Creamos un Crypto map dinámico

uio(config)# crypto dynamic-map DYNAMAP 1

!--- Definimos el transform set debe coincidir con el cliente

uio(config-crypto-map)#set transform-set
TRANSFORM-1

!--- Añade un retorno de ruta en la table de enrutamiento

uio(config-crypto-map)# reverse-route

!--- Salimos del modo crypto-map

uio(config-crypto-map)# exit

!--- Configuración IKE extendida (xauth) para el grupo de la VPN VPNAUTH

uio(config)# crypto map CRYPTOMAP client authentication list VPNAUTH

!--- Confirurar la clave de IKE de busqueda del servidor AAA para el grupo VPNAUTHOR

uio(config)# crypto map CRYPTOMAP isakmp authorization list VPNAUTHOR

!--- Habilitar el router para aceptar peticiones de direcciones IP de cualquier punto.

uio(config)# crypto map CRYPTOMAP client configuration address respond

!--- Usos IKE para establecer IPsec Sas tal como se especifica por el Crypto map DYNAMAP

uio(config)# crypto map CRYPTOMAP 65535 ipsec-isakmp dynamic DYNMAP

!--- Ingresamos a la configuración de la interfaz

uio(config)# interface ethernet 2/0

!--- Aplicamos el Crypto map CRYPTOMAP

uio(config-if)# crypto map CRYPTOMAP

!---- Salimos del modo privilegio

```
uio(config-if)# end
```

ANEXO 5

MANUAL DE USUARIO

MANUAL DE USUARIO

Para trabajar en un escenario en el cual ya esta implementado una VPN con equipos CISCO, es recomendable hacerlo por SDM ya que el ambiente es mucho más amigable debido a su potente interfaz grafica.

Se configura el Router para permitir el acceso via SDM:

- Configuramos un usuario y un password,

```
UIO(config)# username ciscosdm privilege 15 password 0 ciscosdm
```

- Se debe configurar el acceso via http y https a el router

```
UIO(config)# ip http server
UIO(config)# ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Augus 14 20:19:45.310: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Augus 14 20:19:46.406: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue
"write memory" to save new certificate
UIO(config)# ip http authentication local
```

- Finalmente se configura la terminal vitual del ROUTER para autenticar al usuario, y permitir el ingreso virtual a través de telnet y SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet ssh
```

Configurados ya los accesos se continua con las direcciones IP:

- Para el acceso se necestia configurar la interfaz o interfaces,

```
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

- De igual manera se debe asignar un IP al PC que se encuentre dentro de la misma red, para lo cual nos vamos a las propiedades de las conexiones de red y seleccionamos el ítem de “Protocolo TCP/IP”, Figura 1

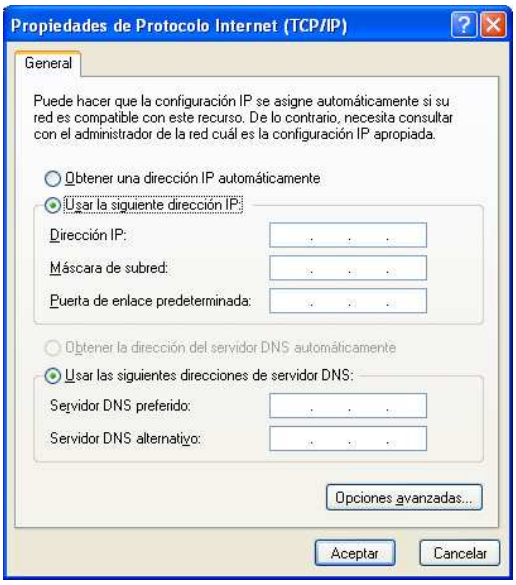

Figura 1

Enseguida se procede con la descarga del fichero que contiene el instalador del SDM:

Se realiza doble click en el ejecutable “setup.exe” y enseguida sale la siguiente pantalla con el asistente.

Figura 2

Realizamos clic en siguiente (next)

Figura 3

Aceptamos los términos del acuerdo de la licencia y presionamos siguiente.

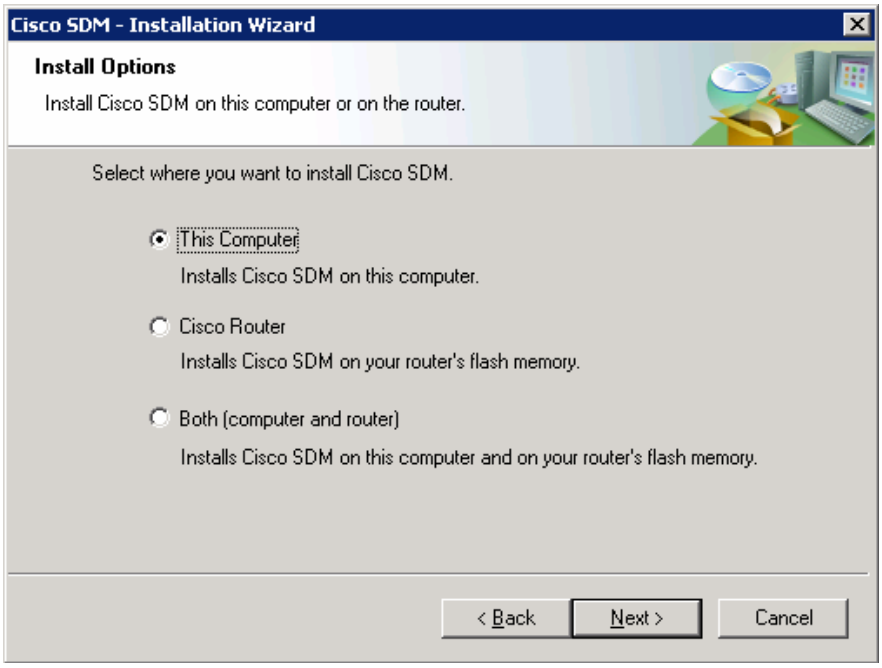

Figura 4

En esta pantalla (figura 4) se tiene la posibilidad de escoger entre las diferentes opciones, escogemos la opción 1 “This Computer”, para que se intale localmente en el PC monitor.

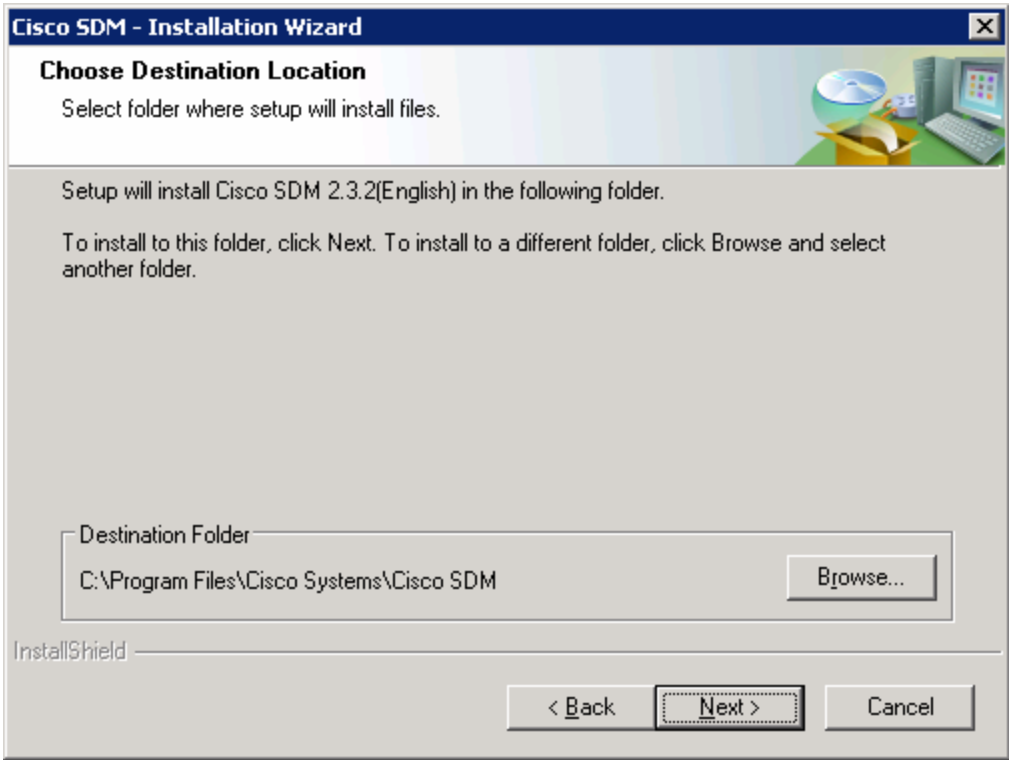

Figura 5

Se escoge la opción de siguiente para que se instale en el directorio por defecto.

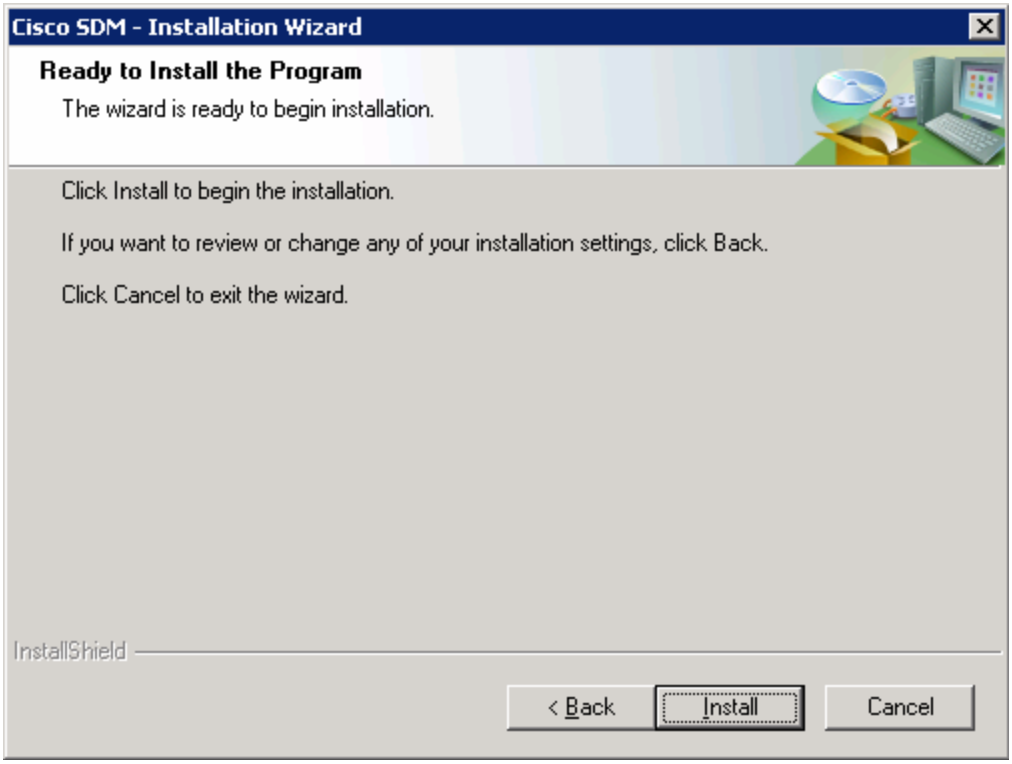

Figura 6

En la siguiente pantalla (Figura 6) se coloca la opción “install” y listo, se debe esperar que termine el proceso.

Figura 7

Se procede a pulsar “finish” y se ejecutara el programa ya que esta habilitada la opción de que se ejecute al terminar la instalación.

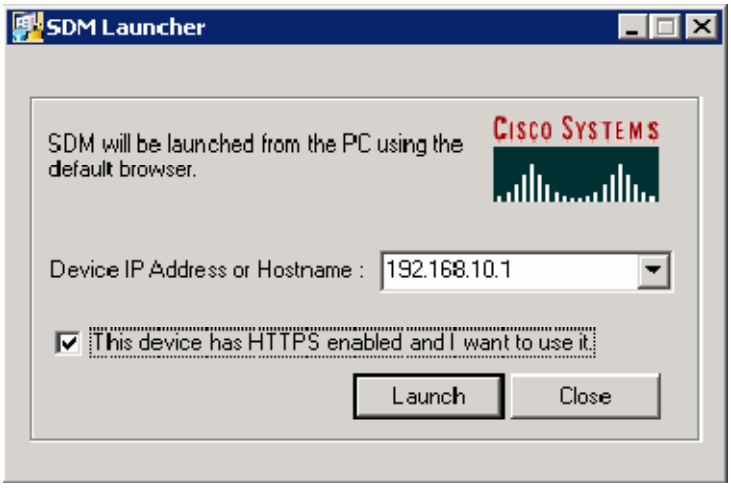

Figura 8

En la siguiente pantalla le damos clic en ”launch” ya que no se tiene que escoger el dispositvo, por que se asume que es el único, o caso contrario escoger por la dirección IP del dispositivo.

Figura 9

Se autentica con el usuario y el password definido previamente para conectarse via http.

Figura 10

Alerta de seguridad del Navegador (Internet Explorer)

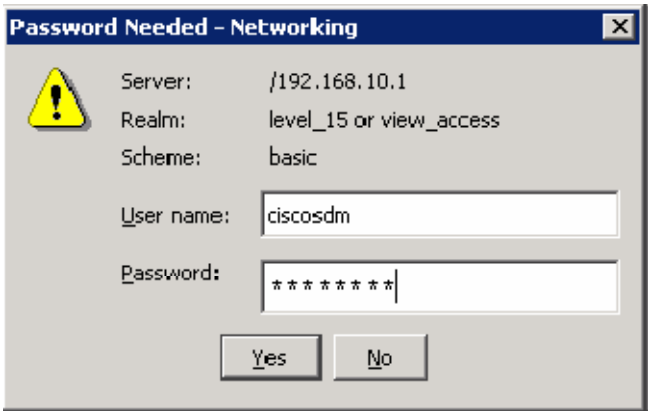

Figura 11

Cuadro de autenticación de SDM, de la misma manera se procede a colocar el usuario y password creados.

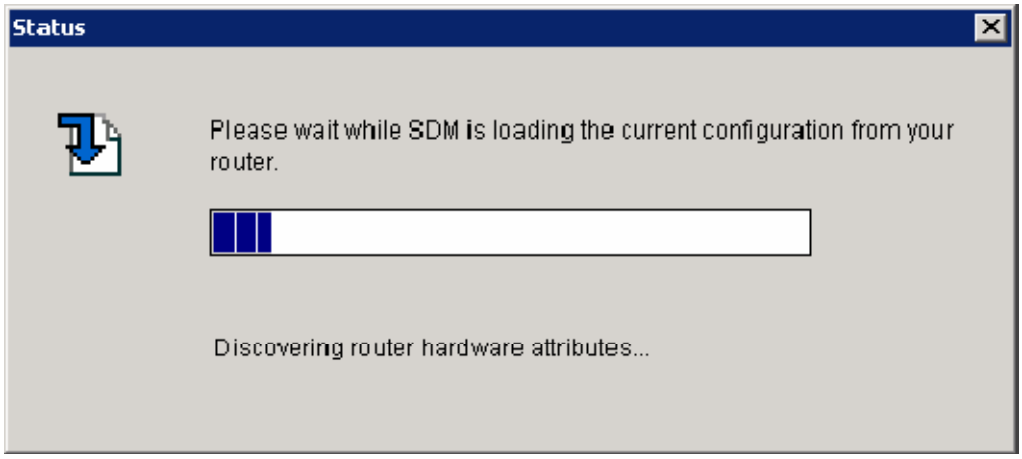

Figura 12

Barra de avance de carga de la configuración del dispositivo.

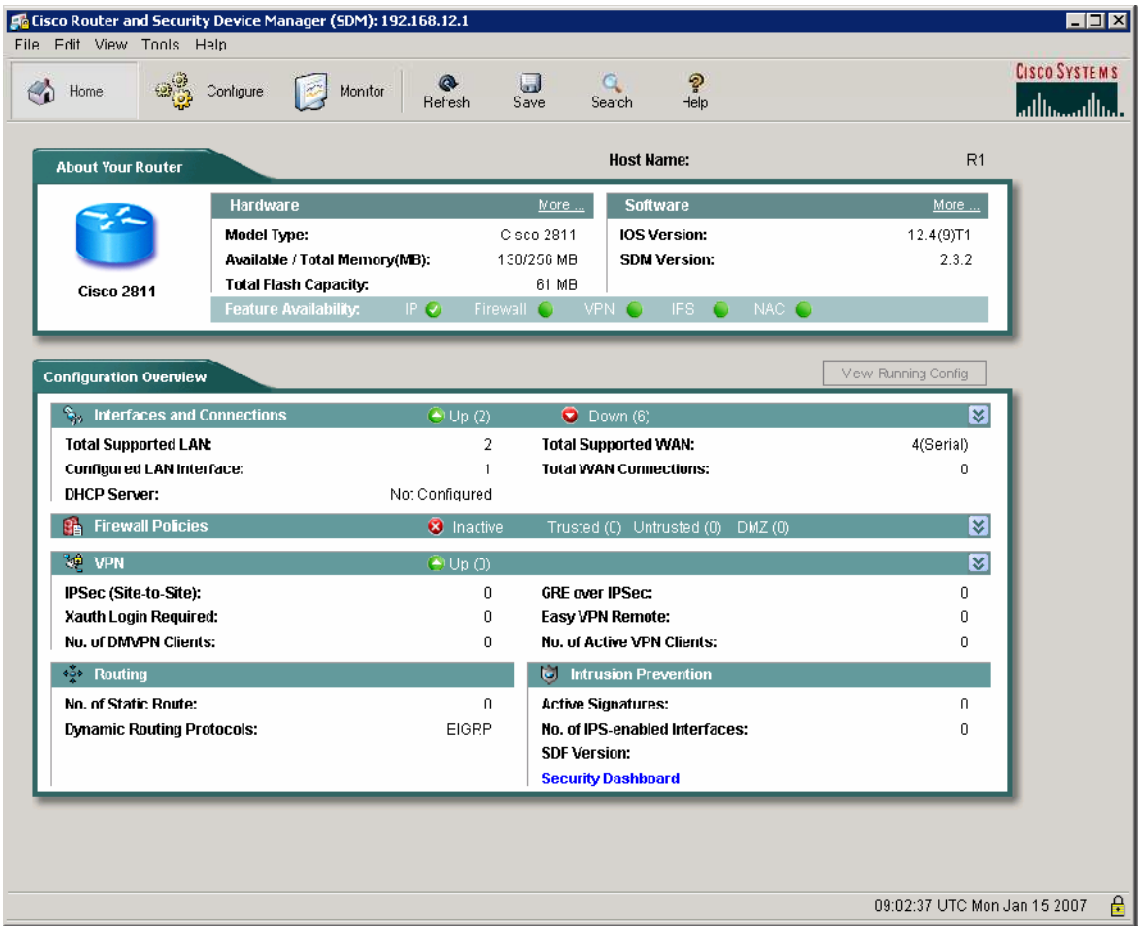

Figura 13

Pantalla de bienvenida del SDM

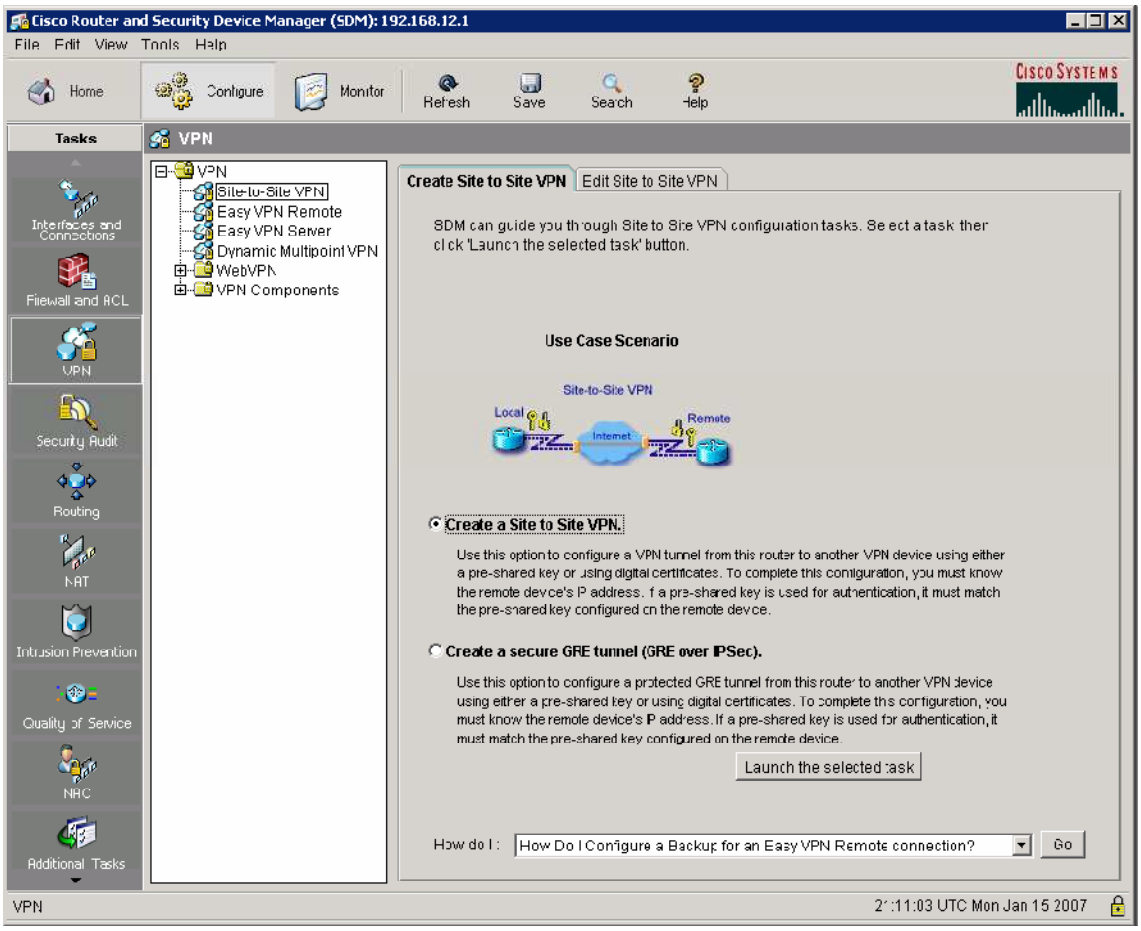

Figura 14

Se selecciona el icono de configuración (configure),

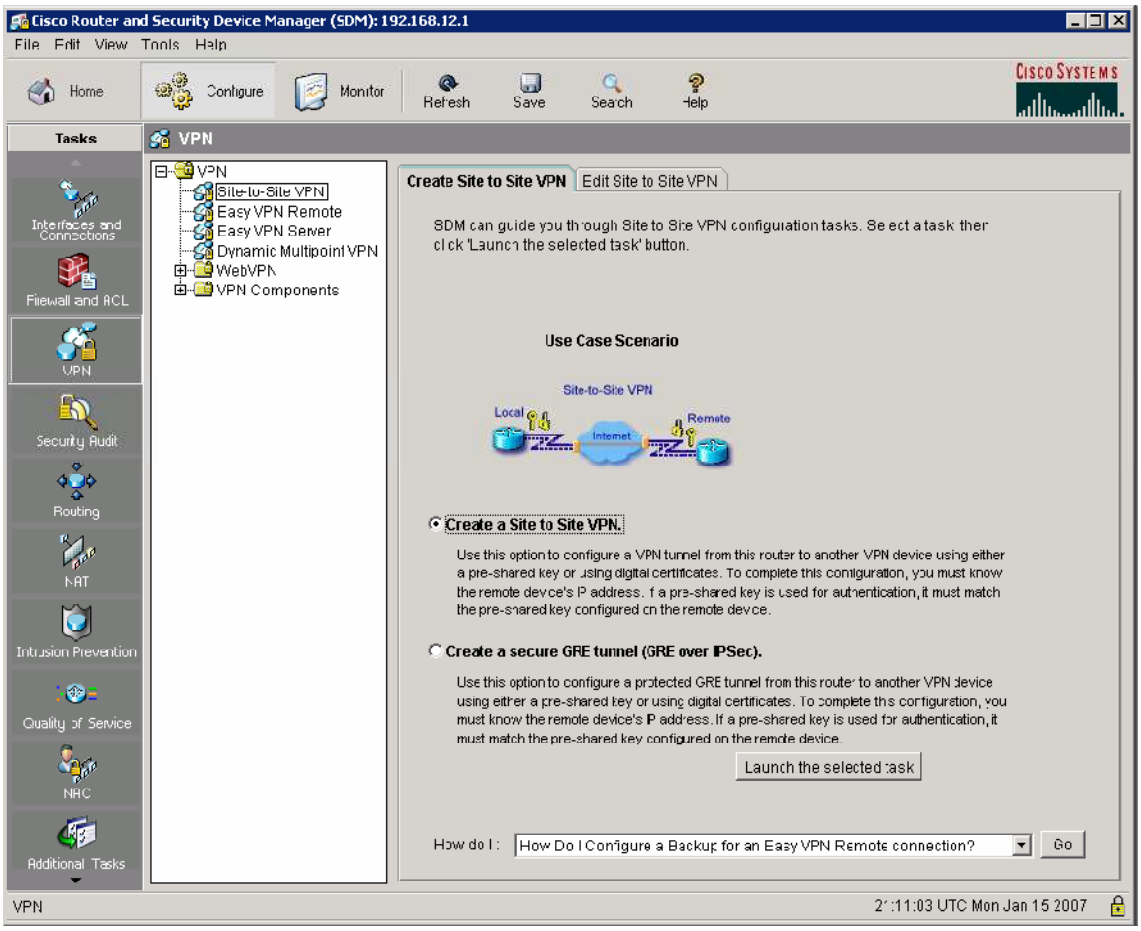

Figura 15

Para el caso de estudio, escogemos la opción de “Create Site to Site VPN”

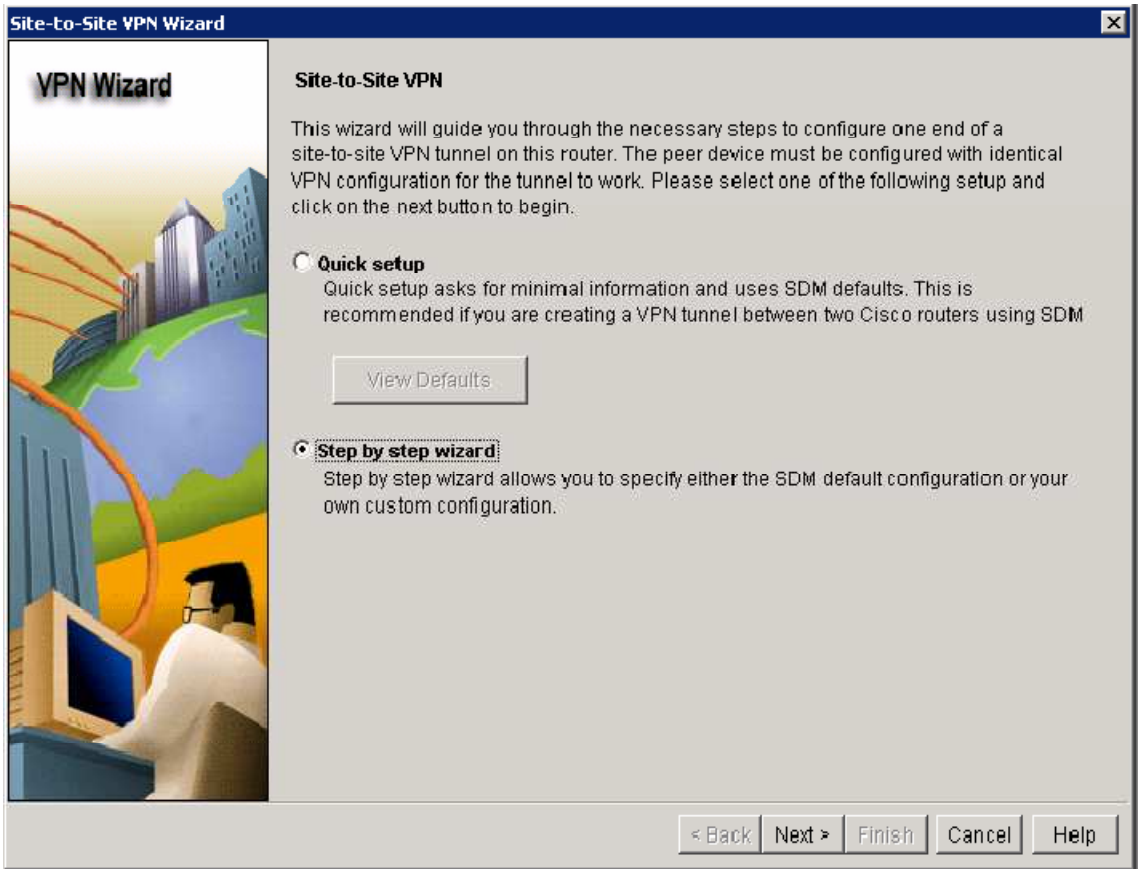

Figura 16

En la siguiente pantalla se debe escoger la opción de “Step by step wizard” (asistente paso a paso), para ir seleccionando las opciones deseadas.

Para trabajar con equipos de alto costo como los ROUTER, es necesario contar con un simulador, o de preferencia un emulador, ya que se pueden probar previamente los comandos a utilizar y de esta manera no perder el tiempo ni correr el riego de cometer errores en el equipo físico.

Una excelente opción en Software libre, es GNS3 que permite emular dispositivos concentradores, e incluso permite probar las mismas imágenes de CISCO, y de esta manera se pueden mitigar las fallas humanas.

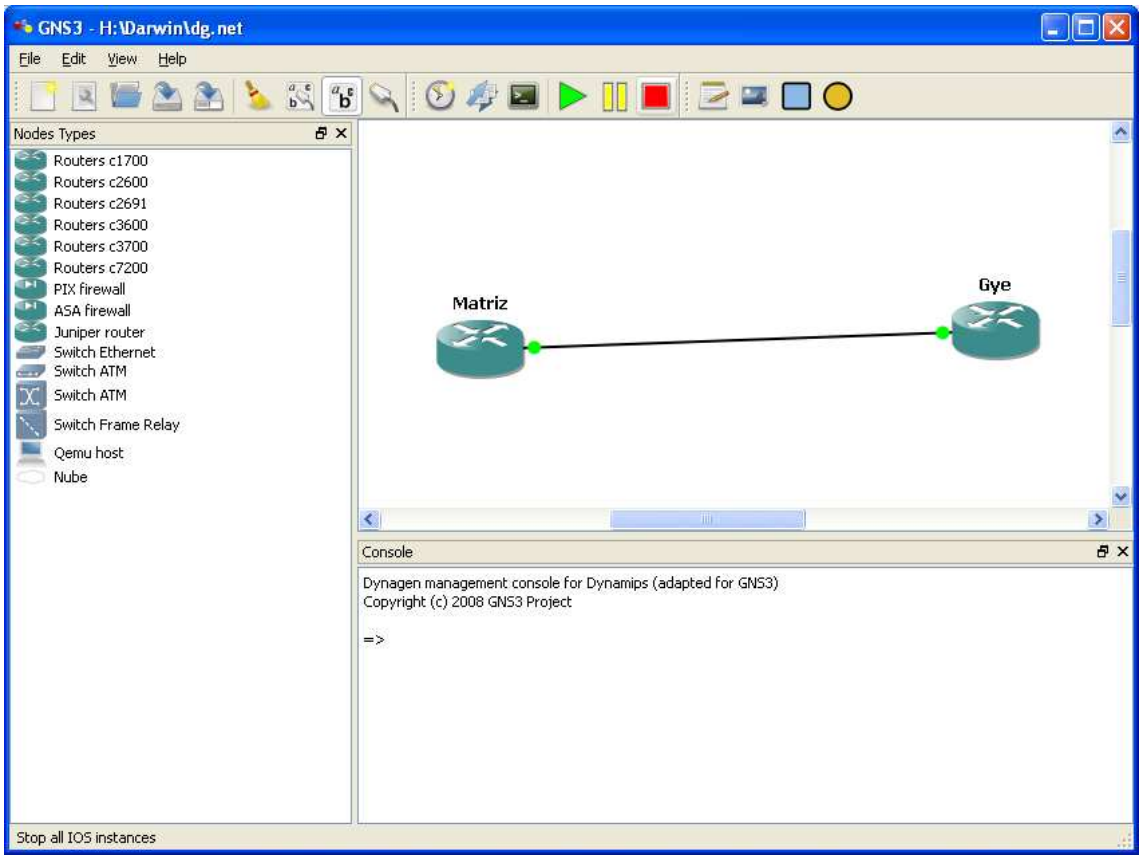
GNS3 - H:\Darwin\dg.net
File
Edit
View
Help
Nodes Types
Routers c1700
Routers c2600
Routers c2691
Routers c3600
Routers c3700
Routers c7200
PIX firewall
ASA firewall
Juniper router
Switch Ethernet
Switch ATM
Switch ATM
Switch Frame Relay
Qemu host
Nube
Matriz
Gye
Console
Dynagen management console for Dynamips (adapted for GNS3)
Copyright (c) 2008 GNS3 Project
=>
Stop all IOS instances

Figura 17

En este software se puede cargar las imágenes de CISCO, y probarlas antes de su instalación en el equipo fisco.

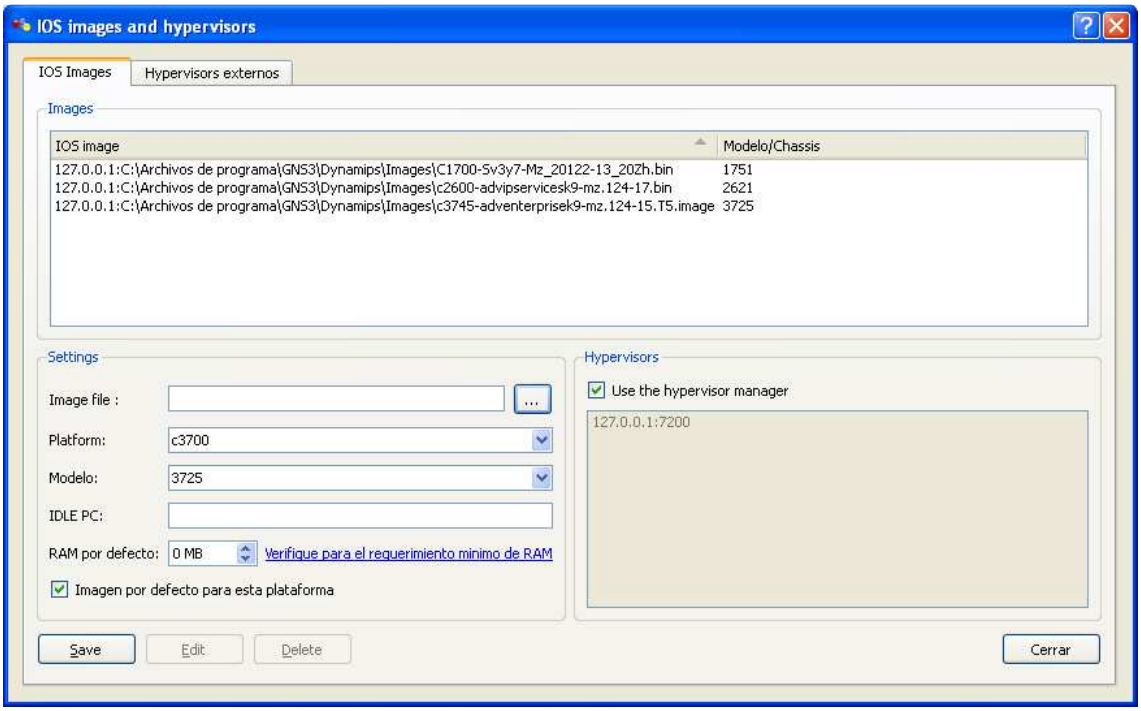

Figura 18

La interfaz de GNS3, es bastante intutiva, en esta pantalla, se puede observar que se carga una imagen y se observan las familias de modelos de equipos CISCO que soportan, de la misma manera se puede añadir las líneas de comando necesarias, la configuración del equipo por líneas de comando se encuentran en el Anexo 4, detallando cada paso únicamente referente a la configuración de VPN sobre IPsec.

ANEXO 6
ACUERDO DE NIVEL DE SERVICIO

INTRODUCCIÓN

PROPÓSITO

El presente documento tiene como finalidad definir el Acuerdo de Niveles de Servicio (SLA – Service Level Agreement) entre BRIGHTCELL S.A. y LA DINSE, que en lo posterior lo denominaremos CLIENTE y que describe de común acuerdo los objetivos de desempeño y disponibilidad de los enlaces que BRIGHTCELL S.A., ofrecerá al CLIENTE.

Los objetivos de desempeño y disponibilidad serán los parámetros mensurables de la relación BRIGHTCELL/CLIENTE, y podrán ser sujetos a revisiones continuas.

Responsabilidades / Funciones de BRIGHTCELL S.A.:

Administrar los segmentos de red dentro de su dominio. El límite de cada dominio está determinado por los puntos de conexión, generalmente en lugares de propiedad del CLIENTE.

Monitoreo continuo de cada dominio y generación de reportes en caso de problemas.

Establecer procesos internos que sirvan de soporte a los requerimientos del presente SLA.

DISPONIBILIDAD Y CALIDAD DEL SERVICIO DE RED

DISPONIBILIDAD

La disponibilidad ofrecida por BRIGHTCELL S.A., para los enlaces para el CLIENTE cumplirá con lo estipulado en las recomendaciones Internacionales dadas por la ITU, es decir 99.7%. Se entiende por Disponibilidad el tiempo medido en horas en que el servicio está disponible en un determinado canal.

Se debe cumplir con una disponibilidad igual o superior a la contratada, del tiempo de duración de un periodo para los enlaces ofrecidos por BRIGHTCELL S.A.

El porcentaje de disponibilidad será calculado y medido respecto a cada canal digital provisto de acuerdo con la siguiente fórmula:

D = (A/B) x 100, donde:

A = Número de horas en las cuales cada canal estuvo disponible, información que BRIGHTCELL S.A. obtendrá de los reportes generados por su centro de gestión.

B = Número de horas que debería estar disponible cada canal, cuyo valor es veinticuatro (24) horas por el número de días del periodo de observación.

D = Porcentaje de disponibilidad.

Los tiempos de fallas en el servicio generados por los motivos que se describen a continuación se excluirán del cálculo de la Disponibilidad.

Periodos de mantenimiento programados: BRIGHTCELL S.A., dispondrá de veinticuatro (24) horas al año, para el mantenimiento de cada canal ofrecido, sin que esto afecte el servicio.

Periodo de mejoramiento: BRIGHTCELL S.A., dispondrá de veinticuatro (24) horas al año para los trabajos de mejora de red, sin afectar el servicio.

Motivos de fuerza mayor tales como desastres naturales, atentado, asonada, hurto, vandalismo, accidente, incendio, alteración del orden público, etc., que afecten las instalaciones, equipos y/o facilidades de BRIGHTCELL S.A., y/o CLIENTE

La evaluación de los parámetros de disponibilidad se realizará de forma conjunta entre BRIGHTCELL S.A., y el CLIENTE mensualmente.

INDISPONIBILIDAD

Se define como Indisponibilidad, el tiempo en horas durante el cual un canal se encuentra en condición de fuera de servicio, o cuando los sitios a los cuales esta conectado, son incapaces de establecer el enlace e intercambiar información, por falta o falla en el enlace correspondiente en cualquiera de los sitios, debido a problemas en la red de BRIGHTCELL S.A.

La indisponibilidad de servicio no aplica cuando:

BRIGHTCELL S.A., requiere realizar una prueba de enlace, aunque no se hubiese detectado o reportado falla. En este caso debe notificar por escrito con antelación de por lo menos cuarenta y ocho (48) horas.

El enlace es modificado y/o alterado de cualquier manera por requerimiento escrito específico del CLIENTE.

Por falla del CLIENTE en no darles a los funcionarios de BRIGHTCELL S.A., o a quién este designe, acceso a los equipos que brindan el servicio, luego de la solicitud por escrito presentada por BRIGHTCELL S.A., o por quien designe, con el propósito de investigar y rectificar cualquier problema.

El CLIENTE requiere realizar una prueba de enlace, independiente de haberse detectado o reportado falla. En este caso debe informar al personal de turno de BRIGHTCELL S.A., del particular con por lo menos veinticuatro (24) horas de anticipación.

El enlace es modificado y alterado de cualquier manera por requerimiento escrito específico del CLIENTE.

Se produce una falla atribuible, a los equipos y aplicaciones del CLIENTE.

PERIODO DE ESTABILIZACIÓN

Se establece un periodo de estabilización para cada enlace o conjunto de enlaces de siete (7) días calendario, contados a partir de la fecha de firma del acta de entrega del canal al CLIENTE por parte del BRIGHTCELL S.A. Durante este periodo se realizarán todos los ajustes necesarios a los equipos para su óptimo funcionamiento y que servirán de base para medir la calidad del servicio y del soporte, que permitirá a BRIGHTCELL S.A., tomar las acciones correctivas para lograr los niveles de servicio pactados.

Durante el Periodo de Estabilización del servicio se realizaran mediciones de disponibilidad de estos enlaces, que no serán consideradas para la evaluación de la disponibilidad.

FACTOR DE CALIDAD DE SERVICIO

El parámetro factor de calidad del servicio (FCS) es un índice determinado por el porcentaje de disponibilidad de un enlace en un periodo de un mes.

Se utilizará la tabla siguiente para definir el factor de calidad del servicio:

% DISPONIBILIDAD		Número Máximo de Horas	Factor de Calidad
DESDE	HASTA	Sin Servicio al mes.	Del Servicio
100.00	99.70	2,16	1.00
99.69	99.20	5,76	0,95
99.19	98.50	10,8	0,90
98.49	93.50	46,8	0,85
93.49	89.50	75,6	0,75
89.49	84.50	111,6	0,50
84.49	75.00	180	0,25
74.99	0.00	720	0.00

Tabla 2.1 Factor de Calidad de Servicio

El valor mensual a pagar por el CLIENTE se calculará basándose en la siguiente fórmula:

VMP=VMC x FCS

Donde:

VMP= Valor del mes a pagar por el CLIENTE por el servicio de un canal.

VMC= Valor mensual contractual correspondiente al servicio de un canal.

FCS= Factor de Calidad del Servicio.

Los costos en los que CLIENTE incurra por el reemplazo del servicio serán asumidos por BRIGHTCELL S.A.; deducibles del último pago pendiente por parte del CLIENTE a este.

REPORTES

Mensualmente, junto con las facturas para el pago del servicio, BRIGHTCELL S.A., entregará un resumen de los enlaces que mantiene con el CLIENTE en el cual debe constar lo siguiente:

Ancho de Banda de enlace.

Disponibilidad mensual y acumulada por canal.

Tasa de errores por canal (umbrales recomendados, medición, reporte, procedimiento de medida).

PROVISIÓN DE SERVICIOS

LIMITES DE RESPONSABILIDAD

BRIGHTCELL S.A., será responsable de la instalación, puesta en operación y mantenimiento de todos los equipos con los cuales ofrecerá el servicio al CLIENTE, hasta el punto de conexión con los equipos del CLIENTE.

De acuerdo al contrato con el CLIENTE, este se constituye en custodio de los equipos que le brindan servicio instalados en sus dependencias. En tal condición, deberá mantenerlos en buen estado y usarlos de conformidad con el destino y finalidad para los que fueron fabricados e instalados y será responsable de todo daño o menoscabo distintos del deterioro natural. Sin perjuicio de su responsabilidad, el CLIENTE comunicará a BRIGHTCELL S.A., sobre todo daño que sufra el equipo instalado, dicha comunicación deberá efectuarse por escrito dentro de las veinticuatro (24) horas inmediatas siguientes a la ocurrencia del suceso.

En caso de que el centro de monitoreo de los enlaces determine que uno o todos los enlaces están operativos, y el CLIENTE no tuvieren servicio y se requiera asistencia de un técnico de soporte del BRIGHTCELL S.A., y se verificare que efectivamente el enlace estuviere en pleno funcionamiento, BRIGHTCELL S.A., presentará al CLIENTE un informe técnico indicando la razón por la cual no se advertía el servicio.

INTERFACES

Salvo cualquier excepción previamente justificada y aprobada por las partes, las interfaces de red que estarán disponibles en las dependencias del CLIENTE serán:

V.35/V (EIA/TIA RS-449), con conector estándar M34 (Winchester). BRIGHTCELL S.A., deberá ofrecer un conector tipo “hembra” y de características funcionales y operativas DTE.

G.703, cable coaxial de 75 ohmios y de características funcionales y operativas DTE o

Ethernet RJ45 10/100 Mbps

SEGURIDAD

Debido a la naturaleza del tráfico de datos, BRIGHTCELL S.A., no podrá sin previa autorización del CLIENTE, realizar las siguientes acciones:

Utilizar herramientas para analizar el tráfico del CLIENTE que atraviesa los canales de datos provistos.

Ingresar a las consolas de los equipos del CLIENTE para modificar configuraciones.

Administrar claves de acceso de los equipos de enrutamiento.

ACTIVIDADES DE MANTENIMIENTO

Las actividades de Mantenimiento incluyen trabajos planificados, solución de problemas técnicos y administración de desempeño de la red.

Los problemas presentados en la red se los ha clasificado de acuerdo a la severidad de los mismos:

Crítica: Existe una indisponibilidad total de cualquier segmento de la red. Esto provoca una reducción sustancial en la capacidad de la red, e incapacidad de los terminales para efectuar sus transacciones.

Mayor: Existe una degradación del servicio, la cual se refleja en niveles de BER mayores a los permitidos, pérdida de paquetes y tiempos de respuestas altos, próximos a un corte de servicio.

Menor: Existe una condición mínima de falla que degrada el servicio y que puede incurrir en alarmas considerables.

En todos los casos, BRIGHTCELL S.A., brindará un soporte técnico apropiado capaz de superar cualquier problema o inconveniente que se presente en la red de acceso y enlace de última milla, motivo de este SLA.

El soporte técnico entregado por BRIGHTCELL S.A., será de 7 X 24 (permanente). Para horario de oficina en días laborables se dispondrá de personal técnico en sus oficinas, para hora fuera de horarios de oficina, fines de semana y feriados, dispondrá igualmente de personal técnico de turno, cuyos contactos serán localizados en base a provisiones previamente notificadas al CLIENTE.

MANTENIMIENTO PLANIFICADO

Las actividades de mantenimiento planificado serán efectuadas previa coordinación y acuerdo mutuo entre BRIGHTCELL S.A., y el CLIENTE. Dichas tareas podrían en determinados casos provocar degradación o indisponibilidad de uno o varios segmentos de la red, por lo que es importante la comunicación de las 2 partes.

La finalidad del Mantenimiento Planificado será evitar problemas que pudiesen afectar el desempeño y la calidad de la red de transporte de datos.

En todos los casos, la comunicación oficial de las tareas a realizarse será reportada al CLIENTE con 48 horas de anticipación como mínimo.

RESPUESTA A PROBLEMAS

Para alcanzar los objetivos de desempeño y calidad, es muy importante que los problemas en la red sean resueltos de manera rápida y apropiada.

Las acciones tomadas y tiempos de reparación estarán determinados por la severidad del problema.

Una vez detectado el problema por parte del personal de BRIGHTCELL S.A., o del CLIENTE, comunicaran vía telefónica para coordinar el ingreso a las oficinas de propiedad del CLIENTE.

Los tiempos de respuesta que se aplicarán para la solución de problemas se detallan a continuación:

Tiempo de atención a llamadas de soporte técnico menor o igual a 10 minutos.

Tiempo de valoración del problema menor o igual a 1 hora.

Tiempo de solución del problema (GYE/UIO) menor o igual a 2 horas.

Tiempo de solución del problema (Provincias) menor o igual a 10 horas.

Tiempo de solución del problema (Provincias de Oriente y Galápagos) menor o igual a 72 horas.

PROCEDIMIENTO PARA SOLUCIÓN DE PROBLEMAS

Reportes de problemas podrán originarse desde CENTRO DE MONITOREO o desde las dependencias del CLIENTE. Los reportes se pueden generar basados en los sistemas de supervisión de alarmas de la red y monitoreo del desempeño de la misma.

El CENTRO DE MONITOREO de BRIGHTCELL S.A., deberá tener la facilidad de discriminar y conocer si el problema se encuentra en el dominio de BRIGHTCELL S.A., o el dominio del CLIENTE. Todo esto, con finalidad de encontrar una solución inmediata al inconveniente presentado, a través de las áreas responsables de los diferentes dominios.

Una NOTA de mantenimiento será emitida en todos los casos de reporte de problemas para hacer un seguimiento del mismo desde su inicio hasta su solución definitiva. A través de ello, se podrá contar con estadísticas que permitan tomar acciones tendientes a un mejoramiento continuo de la red y de la calidad del servicio.

ANEXO 7

PROFORMA DE EQUIPOS

ANEXO 8

PROPUESTA DE SERVICIOS

Quito, 04 de agosto del 2010

Señores

DINSE

Presente.-

El que suscribe, en atención a la convocatoria efectuada por usted, para la cotización de Provisión de Servicios de Internet y Transmisión de Datos, luego de examinar los requerimientos precontractuales, al presentar esta propuesta la Compañía BRIGHTCELL S.A., declara que:

Entregará los servicios ofertados completos, listos para su uso, de conformidad con las características detalladas en las Especificaciones Técnicas de sus requerimientos indicados.

Garantiza la veracidad y exactitud de la información y las declaraciones incluidas en los documentos de la propuesta, formularios y otros anexos, al tiempo que autoriza a efectuar acciones para comprobar u obtener aclaraciones e información adicional sobre las condiciones técnicas y económicas del proponente.

BRIGHTCELL S.A., declara también que en caso de recibir la adjudicación del contrato, nos comprometemos a entregar los servicios, en las condiciones técnicas impuestas, en un plazo máximo de veinte y uno (21) días calendario en el caso de Fibra Optica y de ocho (8) días calendario en el caso de Radio o Cobre, previo el envío formal de una carta de adjudicación o firma del contrato.

Atentamente,

Lcda. Erika Mora

BRIGHTCELL S.A.

RUC BRIGHTCELL: 1791741471001

Mail: emora@brightcell.net

Telf: 223-2329 / 223-2619

Móvil: 096-381 289 095-070 039

www.brightcell.net

Enlace de Internet – Propuesta Económica

Precio Mensual del Servicio de Internet

SERVICIO	CARACTERISTICAS	CANTIDAD	PRECIO
INTERNET	1024 Kbps DOWN x 1024 Kbps UP 1:1	1	150
		TOTAL	150

NOTA: * Nuestros precios no incluyen IVA

Valores Agregados

- Se entregará y publicará las direcciones IP, necesarias para la utilización del servicio, de acuerdo a las especificaciones de contratación, *para este caso puntual se asignará el rango que requieran sin costo alguno.*
- *El enlace permitirá la transmisión ilimitada y sin ningún tipo de restricción.*
- *Permitirá la ejecución de toda aplicación en Internet existente.*

PLAZOS Y FORMA DE PAGO

La oferta económica contempla un período de contratación del servicio por un año, el pago del servicio se realizará contra factura mensual que se entregará los primeros cinco días del mes siguiente al que se esté facturando.

El plazo de Instalación del servicio será de veinte y un (21) días laborables, que serán contados a partir de la fecha de entrega del anticipo para gastos de instalación del sistema.

VALIDEZ DE LA OFERTA

La oferta tiene una validez de sesenta (60) días contados a partir de la fecha de presentación de esta propuesta.

INTRODUCCIÓN

BRIGHTCELL S.A., Empresa con altos estándares de seguridad y eficiencia en sistemas de telecomunicaciones para instituciones. Parte de una iniciativa de personas y capitales del ámbito privado ecuatoriano, especializados en telecomunicación gubernamental y corporativa, que provee de tecnología de avanzada y organización para el mejor funcionamiento y transparencia de las organizaciones, tiene el agrado de darles a conocer esta propuesta de servicios de Internet, diseñada contemplando las necesidades de su organización y específicamente enfocada al mercado Corporativo.

Desde el inicio de nuestra operación la intención ha sido ofrecer soluciones que respondan a las necesidades de un mercado sujeto a un cambio permanente y en rápida evolución, manteniendo una excelente relación con nuestros socios de negocios, nuestros clientes.

La oferta que presentamos a continuación fue elaborada a partir de los requerimientos solicitados y en base a nuestra experiencia en soluciones de alta disponibilidad, confiabilidad y de calidad.

SERVICIOS DISPONIBLES:

BRIGHTCELL S.A., instala enlaces de Ultima Milla sobre medios de Fibra Óptica, cobre y wireless, dedicada desde las instalaciones del cliente hasta el Nodo más cercano de acceso a nuestro Backbone de Fibra Optica de acceso a Internet. Este acceso es de tecnología digital.

Call Center: Centro de Atención al Cliente de las Unidades de Negocios de BRIGHTCELL S.A. Es un centro encargado de proveer asistencia a los clientes sin costo

las 24 horas del día, los 365 días del año. El número telefónico de asistencia del Call Center es (593)-2-232329 (593)-9-6248932 E-mail: techsupport@brightcell.net

Centro de Gestión: Centro de Operaciones de Backbone de la red de datos. Es un centro técnico de última tecnología de asistencia permanente a los requerimientos generados por el Call Center, el cual provee asistencia permanente las 24 horas del día, los 365 días al año.

Para la gestión y mantenimiento de la red, se utiliza los sistemas de gestión NAGIOS y EGROUPWARE basados en protocolos estándares TMN y SNMP, de manera que la gestión de la red se realiza sobre una plataforma de administración centralizada que permite monitorear, configurar y diagnosticar el estado de los equipos, interfaces y circuitos de prácticamente todos los elementos activos de la red, recopilando información con la que se pueden obtener estadísticas del desempeño de los circuitos de comunicación en base a los principales parámetros de funcionamiento y calidad, incluyendo algunos asociados a los elementos pasivos como son los medios de transmisión.

El sistema consiste de un set de funciones las cuales tienen una interfase hacia el usuario y funciones de servicio que corren 24 horas al día recopilando y actualizando la información de la red en un SYSLOG SERVER y sobre este opera un conjunto integrado de herramientas para la gestión de red, brindando estadísticas tales como:

- Diagramas de Red
- Prueba de Circuitos en Loop
- Sistema de Gestión de Alarmas
- Calculadora de Capacidad de Red
- Simulador de Fallas
- Administración de Usuarios
- Archivo de Problemas y Soluciones
- Administrador de Unidades de Software
- Administración de Cuentas.

Además con la información que se recopila en los diferentes servidores y que se almacena en una base de datos, esta es procesada y se obtiene los siguientes servicios:

- Comunicación con los elementos de la red
- Recuperación de los canales de control
- Poleo de fallas
- Monitoreo en tiempo real
- Colección de estadísticas de funcionamiento
- Monitoreo de consistencia entre la información de los nodos y la base de datos.

Contingencia: BRIGHTCELL S.A., cuenta con un NOC[113] ALTERNO DE OPERACIÓN Y GESTION ubicado en un sitio geográfico diferente, construido bajo normas y estándares de seguridad y diseño como ISO 17799 y ANSI/TIA 942 para garantizar y proveer de alta disponibilidad y continuidad del negocio a sus clientes, minimizando inconvenientes ante eventuales desastres naturales o subversivos.

En el CORE de infraestructura se encuentra implementados dispositivos de seguridad eficientes como Firewall-Shorewall, IDS\IPS-Snort (Detección y Prevención de Intrusiones), Antivirus-Clamav, Antispam-SpamAssassin y otros elementos de seguridad como servidores con configuraciones de alta disponibilidad, sistemas de climatización y suministro de energía, etc.

Servicio de Ruteo: Se incluye un CPE[114]; como equipo de terminación del enlace, el cual es administrado por BRIGHTCELL S.A.

Sobre el equipo de terminación el cliente conectará sus propios equipos para la conexión de su Red.

---

[113] *NOC (Network Operations Center)* Centro de Operaciones de Red; grupo que administra una red

[114] *CPE (Client Point Equipment)* Equipo de Punto del Cliente, Son equipos terminales que cuentan con los protocolos necesarios para que sean supervisados y controlados por el sistema de gestión de la red a la cual estén conectados.

Servicio de Mantenimiento: Se incluye el servicio de mantenimiento tanto preventivo como correctivo, el cual posee la **provisión de equipos y stock de backup (1+1) para el reemplazo inmediato** y para la conservación de los equipos de propiedad de BRIGHTCELL S.A, instalados para el servicio solicitado.

El Mantenimiento Preventivo.- Se realiza regularmente dos veces al año y comprenden tareas de mantenimiento y mejoras de servicios tanto de infraestructura de red como de los equipos y programas del NOC. Estas tareas se coordinan fuera de los horarios laborales y de operación del cliente con el objeto de no impactar la operación de los mismos.

Mantenimiento Correctivo.- Servicio y soporte a clientes con cobertura nacional. Los usuarios del servicio, cuentan aquí con distintos niveles de asistencia técnica, de acuerdo al tipo de falla ocurrida y procedimientos de escalamiento de reclamos.

Estadísticas y Reportes: BRIGHTCELL S.A., entregará El Reporte Mensual de operación a solicitud del cliente, del seguimiento de la operación de sus circuitos, el cual especificará:

- Disponibilidad mensual de oficinas y enlaces.
- Cambios planificados y no planificados a la configuración de la red.
- Problemas encontrados por BRIGHTCELL S.A., y problemas reportados por el cliente.
- Recomendaciones para evitar incidir en los mismos problemas en el siguiente mes.
- Reportes adicionales o con distinta periodicidad solicitados por el cliente que deberán ser acordados de manera puntual entre las partes.

NIVELES DE SERVICIO GARANTIZADOS

La calidad del servicio que BRIGHTCELL S.A., garantiza a sus clientes es mayor o igual a 99.7% de disponibilidad, y esta regulada a través de un Acuerdo de Calidad de

Servicio SLA[115], por un porcentaje igual o mayor al seleccionado en el contrato, que se firmará con el cliente en el momento de la contratación.

Considerando el tipo de servicio que BRIGHTCELL S.A., presta al cliente y puesto que no existe la transferencia de propiedad de los procesos de negocios del cliente hacia BRIGHTCELL S.A., se ha considerado los siguientes aspectos para garantizar un nivel de servicio adecuado.

Redundancia en Conexiones del Backbone Internacionales: La conexión Internacional a Internet se realiza a través de múltiples proveedores internacionales a través de Cable Arcos, Cable Maya, Cable Panamericano y Satmex 5 (SATELITAL).

Por Colombia:

Transelectric y Transnexa F.O., cruza hasta el Caribe y accede al cable ARCOS

Con Andinatel F.O. hasta Tulcán, repetidor Troya, luego vía radio con Telecom hasta el Caribe donde existen los cables: MAYA, GLOBAL CROSSING y ARCOS.

Por Perú:

Microonda de empresas privadas hasta Huaquillas, cable de fibra óptica de Telefónica del Perú desde Aguas Verdes hasta LURIN

---

[115] *SLA (Service Level Agreement)* Es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a prestar el mismo bajo unas determinadas condiciones y con unas prestaciones mínimas

Desde LURIN existe acceso a cables: GLOBAL CROSSING, EMERGIA, PANAMERICANO

Los circuitos internacionales son provistos a través de enlaces terrestres o marítimos por fibra óptica, se garantiza un tiempo de respuesta de 60-80ms para enlace Ecuador-USA, medido con un ping estándar y en condiciones normales de tráfico sobre el canal. Se excluye fallas originadas por daño, tiempo de procesamiento en equipos del cliente o por eventos de fuerza mayor que afecten la estabilidad del enlace. No aplica para destinos cubiertos con enlaces satelitales.

Redundancia en Conexiones del Backbone Nacional: Las Ciudades Principales, como Quito, Guayaquil, Cuenca, etc., cuentan con Redes SDH[116] en anillo, permitiendo contar con una redundancia proporcionada por el anillo a todos los Nodos del mismo, manteniendo el tráfico en toda la Red siempre activo aún en presencia de un corte físico en el anillo. Adicionalmente todos los circuitos de clientes que cursan por la red son configurados con una ruta alternativa, de tal forma que en caso de una falla, ruptura o sobrecarga del circuito principal, el enlace permanece con el máximo performance gracias a su ***conmutación automática*** al circuito secundario. Esto lo realiza en forma totalmente transparente el sistema de Administración de la Red.

Adicional se cuenta con contratos de reventa del servicio portador en donde se puede contar con topologías de redes full mesh sobre fibra óptica permitiendo altos niveles de Uptime.

En Todas las Ciudades, los Nodos cuentan con circuitos redundantes, para mantener el máximo Uptime de los clientes.

---

[116] *SDH (Synchronous Digital Hierarchy)* Jerarquía Digital Sincrónica **SDH** y el equivalente norteamericano SONET son las tecnologías dominantes en la capa física de transporte de las actuales redes de fibra óptica de banda ancha. Su misión es transportar y gestionar gran cantidad de tipos de tráfico sobre la infraestructura física.

SLA (Acuerdo de Calidad de Servicio): En cada contrato, BRIGHTCELL S.A. firma un anexo de Calidad de Servicio, donde figuran los valores comprometidos para diversos parámetros, que permiten garantizar el servicio que cada cliente recibe.

BER[117] (Bit Error Rate): En caso de contratación de enlaces transparentes (TDM)[118], se garantiza una tasa de error de BIT menor que (BER <= 1x10 E-08), medida durante un período no menor a 24 horas. Será medida previo a la entrega del circuito al cliente final.

Futuras mediciones podrán ser solicitadas por el cliente, y serán realizadas generando una orden de trabajo y un cargo en la siguiente factura.

SERVICIOS OPCIONALES:

Servicio DNS: Facilita el uso de sus servidores de DNS primarios y secundarios para la resolución de nombres de usuarios del servicio. El servicio de registro y mantenimiento de nombres de dominios propios de la organización es un servicio que deberá gestionarse en forma adicional.

Direcciones IP públicas: El servicio comprende la asignación de direcciones IP públicas necesarias para el uso del servicio. BRIGHTCELL S.A. entregará y publicará esta numeración IP de acuerdo a las especificaciones de contratación del mismo ***para este caso puntual se asignará el rango que requieran a un costo de cero dólares***.

REQUERIMIENTOS PARA UN ÓPTIMO SERVICIO

---

[117] *BER (Bit Error Rate)* Es el parámetro fundamental que determina la calidad de la señal demodulada "trama de transporte" de los sistemas digitales. Cuantifica el número de errores de bit de una trama sea cual fuere el origen del error

118 *TDM (Time Division Multiplexing)* Multiplexación por División de Tiempo TDM, es el nombre que identifica a una red de alta velocidad que facilita **enlaces dedicados** mediante circuitos "punto a punto" local, metropolitano e internacional lo que le permite confiabilidad las 24 horas del día.

Requisitos: El cliente deberá cumplir con las siguientes condiciones en sus instalaciones:

- Espacio suficiente para los equipos (interno y externo).
- Ductería para el paso del cableado.
- Instalaciones eléctricas independientes para los equipos de comunicaciones.
- Red de conexión a tierra.
- Suministro de energía regulada permanente.
- Rack estándar de comunicaciones con ventilación forzada.
- Definición de un mecanismo efectivo para conceder el acceso a personal de BRIGHTCELL S.A., a cualquier oficina, cualquier día y a cualquier hora.

Escalabilidad

Para la instalación de nuevas aplicaciones o modificaciones a las existentes, incrementos de ancho de banda, priorizar el tráfico, etc., el trabajo deberá realizarse en conjunto entre el cliente y BRIGHTCELL S.A., con pruebas pilotos de rendimiento en los casos necesarios.

El sistema propuesto permite flexibilidad y la capacidad de ampliar el canal de transmisión en múltiplos de 64 KBPS hasta los niveles antes señalados, sin que implique cambios en la infraestructura física de servicios y costos adicionales por instalación o inscripción.

Cualquier incremento de nuevos enlaces se mantendrá dentro del esquema del Contrato el mismo que permitirá disponer de los costos y los impuestos.

Confiabilidad del Enlace

- Redundancia de Internet en el nodo de BRIGHTCELL S.A.
- Monitoreo y control del enlace las 24 horas al día
- Servicio de Soporte 7x24x365 (7 días a la semana, las 24 horas al día, los 365 días del año)
- Redundancia en todos los Equipos 1+1

- Reacción inmediata frente a fallas o peticiones de servicio menor o igual a dos horas. (Ver Anexo No.1 SLA)
- Reportes mensuales de disponibilidad del servicio.