UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE LA RED CORPORATIVA
DE UNA EMPRESA DE TELECOMUNICACIONES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

AUGUSTO FRANCISCO CANGAHUALA TORRES

PROMOCIÓN
2004-I

LIMA-PERÚ
2011

DISEÑO DE LA RED CORPORATIVA DE UNA EMPRESA DE TELECOMUNICACIONES

SUMARIO

En un mundo en el que día a día las empresas incursionan en nuevos mercados, es indispensable diseñar una nueva red corporativa acorde a las nuevas exigencias del mercado que permita agilizar la comunicación entre sus diferentes sedes para transmitir información sobre ventas o estrategias de negocio, o cualquier otro fin; este tipo de crecimiento empresarial ha dado lugar a que se desarrollen tecnologías convergentes que satisfagan las necesidades del cliente o usuario en el sentido de velocidad, disponibilidad y seguridad de su comunicación.

Es por ello que en el presente informe se recoge estas necesidades y se plantea una red con mayor ancho de banda, baja latencia, redundancia geográfica hacia Internet, con calidad de servicio para priorizar el tráfico de las aplicaciones principales y secundarias de las diferentes áreas de negocio.

Asimismo, al desarrollar un nuevo diseño, este permitirá agilizar los servicios ofrecidos por las diferentes áreas y así estar al nivel de las nuevas aplicaciones; dejando de lado la preocupación por el retardo de la información, la saturación de los enlaces hacia las sedes remotas, pérdida de conectividad etc.

Por lo tanto, se puede decir que esta nueva red con visión innovadora gestionará una comunicación fluida entre todas las partes involucradas tanto a nivel de usuario como cliente buscando una mayor productividad a todo nivel.

“Dedico este trabajo a mi familia
por su amor, comprensión, apoyo y paciencia
que contribuyeron a culminar mi carrera”

ÍNDICE

PRÓLOGO

El diseño de Redes de Telecomunicaciones es una actividad que ha ganado considerable atención en la medida que las nuevas tecnologías han acelerado la convergencia de voz, datos, imágenes y vídeo, y agregado prestaciones que incluyen una creciente movilidad. Al no existir tecnologías claramente dominantes en los entornos multimedia, la superposición y el transporte de información sobre redes heterogéneas caracterizan al entorno de las telecomunicaciones en la actualidad y explica gran parte de su complejidad.

Las Redes MultiServicio prometen una mayor racionalidad y homogeneidad pero todavía se encuentran en una fase temprana de desarrollo e implementación. En consecuencia, el diseño de redes enfrenta a cada momento el desafío de lograr establecer parámetros y criterios sobre los cuales diseñar una red maximizando sus prestaciones, su eficiencia en costos, su rentabilidad en el tiempo y asegurando a la vez una adecuada evolución futura.

El diseño de redes debe ser un proceso completo, que asocie las necesidades del negocio a la tecnología disponible, para generar un sistema que maximice el éxito de una organización.

El presente informe conformado por cuatro capítulos describe el diseño de la red corporativa de una empresa de Telecomunicaciones.

En el primer capítulo se explican los conceptos de una red VPN sobre la MPLS, su valor agregado como tecnología calidad de servicio QoS (Quality of Service) las ventajas que se tienen al implementar Calidad de Servicio para controlar las aplicaciones y tipos de tráfico en red.

En el segundo capítulo se plantea la determinación de necesidades de la actual red corporativa.

En el tercer capítulo se detalla el diseño de la red corporativa: Arquitectura de la red a implementar, especificaciones técnicas del equipamiento, software de gestión y dimensionamiento del proyecto.

En el cuarto capítulo se consolida el detalle del costo del proyecto.

Finalmente, se exponen las conclusiones y recomendaciones. Por último se adjunta el anexo de especificaciones técnicas y la bibliografía.

CAPÍTULO I
MARCO TEÓRICO

1.1 Modelo de Referencia OSI

El modelo de interconexión de sistemas abiertos, también llamado OSI (Open System Interconnection) es el modelo de red descriptivo, creado por la Organización Internacional para la Estandarización ISO en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. La Organización Internacional para la Estandarización ISO tiene como función principal buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

Este modelo de red se define en base a siete capas, desde la capa número uno en el nivel inferior de la pila de capas, hasta la capa número siete ubicada en el nivel superior. Como se puede apreciar en la figura 1.1, describiendo de abajo hacia arriba, la capa o nivel inferior es fisco denominado también capa 1 y así sucesivamente por último la capa más alta es el 7 el de aplicación.

Figura 1.1 Modelo de referencia OSI (Fuente: Propio)

1.2 Generalidades de enrutamiento

Se entiende por enrutamiento al proceso que permite la interconexión de redes. Se puede efectuar mediante switch o router de acuerdo con el tipo de redes involucradas. El switch se prefiere por el mínimo retardo; bajo costo; pocas conexiones y mínimo planeamiento. Mientras que el router se prefiere para protocolos aislados en cada segmento y flexibilidad futura; requiere configuración para interpretar la dirección IP de capa 3.

El switch y router son elementos que "aprenden de la red". Como analizan la dirección de cada paquete pueden formar una tabla de direcciones. Cuando se conecta un nuevo terminal a la red LAN este envía un paquete indicando la activación con lo que puede integrarse a la tabla de direcciones. La dirección MAC es el número de hardware (grabado en EPROM) asignado por IEEE-ISO. El router debe poseer un set de direcciones IP. Tiene la capacidad de enrutamiento para optimizar el camino del paquete de datos (analiza el costo; retardo de tránsito; congestión de red y distancia en número de Router en el trayecto). La tabla de ruta (Routing table) contiene solo el "próximo paso" en la red1). Se han definido 2 tipos de protocolos para Router: el interior y el exterior al sistema autónomo. Se denomina sistema autónomo AS (sistema interior o dominio) a un conjunto de sub-redes y router que utilizan el mismo protocolo y el mismo control administrativo.

La métrica es una norma o standard de medida que permite efectuar las operaciones de enrutamiento denominado también routing. Entre las métricas se encuentra por ejemplo, la longitud del trayecto en número de routers utilizado en RIP (El primer protocolo de enrutamiento).La tabla de rutas es la responsable del enrutamiento del paquete en la red. Esta tabla realiza un mapa de la topología de la red para determinar el próximo paso hacia el destino final. La métrica para una ruta particular es el agregado de varias características asignadas a un enlace. Existen diversos tipos de métricas; algunos protocolos de enrutamiento utilizan solo una de ellas mientras que otros usan varias alternativas. Algunas posibles métricas de los protocolos de enrutamiento son las siguientes:

Calidad del enlace: Referido a la existencia de errores en el trayecto.

Longitud del trayecto: Referido al número de saltos o routers intermedios en la red. Es el caso más común.

Retardo de tránsito: Referido al tiempo de propagación (Medible mediante un Ping de ICMP).

Ancho de banda del enlace: Referido a la capacidad de tráfico disponible entre routers.

Disponibilidad: Referido al grado de ocupación del CPU del router.

Costo: Toma en cuenta el valor de conexión de la ruta.

1.2.1 Características de los algoritmos de enrutamiento

a. Características de clasificación

Estático/dinámico: Esta característica se refiere a la posibilidad de fijar una ruta determinada en el caso estático o enrutamiento variable para una adaptación en tiempo real.

Simple/múltiple: Referido a la posibilidad de permitir la multiplexación por varias líneas. Cuando es posible el múltiple-trayecto las vías para distribuir los paquetes son dos: balance por paquete (Distribuidos de acuerdo con la métrica) y balance por destino (Se asignan rutas por cada nuevo destino).

El balance por paquete es similar al esquema round-robin(todos-contra-todos; con el mismo nivel de métrica frente a los demás) para rutas de igual costo.

El balance por destino tiende a preservar el orden de los paquetes. TCP acomoda en orden los paquetes pero puede degradarse la performance. Si bien IP es un protocolo orientado sin-conexión, los routers que implementan el enrutamiento preservan en lo posible la ruta.

Plano/jerárquico: En la topología plana todos los routers tienen igual jerarquía; en la jerárquica los routers forman un backbone para el tráfico principal. Los protocolos OSPF y IS-IS son ejemplos de protocolos de enrutamiento que utilizan estructura jerárquica.

Hardware: Referido al tipo de hardware utilizado. Es realizado por host o router inteligentes.

Dominio: Los protocolos de enrutamiento son distintos si trabajan en el mismo dominio (intra-dominio) o entre dominios (inter-dominio).

Algoritmo: Se disponen de dos tipos de algoritmos para obtener las tablas de rutas.

RIP utiliza el algoritmo "vector-distancia" originario de Bellman-Ford. Requiere de datos sobre el número de saltos y el costo. El costo puede indicar un valor en $/min o bien preferencia (ponderación debido a retardo: por ejemplo un peso de 1 para 128 kb/s y de 10 para 64 kb/s). Es usado en RIP, Hello y BGP.

SPF que es utilizado se denomina Dijkstra Algorithm. Es un protocolo de estado de enlace **LSA** (Link State Advertisements). Acumula información que es usada por el algoritmo **SPF** (Shortest Path First) para reconocer el camino más corto a cada nodo. Es usado en OSPF y IS-IS. El protocolo IGRP (de Cisco) utiliza un algoritmo híbrido.

b. Características de Selección

Eficiencia: La eficiencia es la habilidad para seleccionar la mejor ruta con una utilización del CPU mínima.

Sumarización: La sumarización de ruta se refiere a la posibilidad de estructurar la tabla de rutas con sets de rutas sobre un mismo enlace. Esto permite reducir sustancialmente la capacidad de memoria utilizada por la tabla.

Simplicidad: Se refiere al software mínimo requerido y el uso del encabezado de paquete. Debe tenerse presente que el protocolo utiliza una parte de las reservas de enlace. De esta forma, protocolos como el RIP realizan actualizaciones periódicas, mientras que el OSPF o IS-IS lo hacen solo en caso de falla. Son más complejos pero solo ocupan al CPU en caso necesario. En funcionamiento normal minimiza la ocupación del ancho de banda.

Robustez: La robustez se refiere a la habilidad para soportar fallas de hardware, condiciones de pérdidas de paquetes e implementación incorrecta. Algunos protocolos trabajan directamente sobre IP mientras que otros lo hacen sobre TCP o UDP.

Flexibilidad: Se refiere a la adaptación a diversas circunstancias.

Convergencia: Es la velocidad de actualización del enrutamiento. Tabla cuando se requiere una actualización (re-cálculo de rutas para optimización). El problema es la formación de lazo (loop), de rutas en caso de disponer de una convergencia lenta. El tiempo de convergencia depende de la velocidad de detección de cambios en la red, selección de la ruta y propagación de los cambios. Los cambios realizados en un router y que por el momento no generan cambios en otros routers, pueden provocar loop de enrutamiento. Algunos problemas son detectados rápidamente como la interrupción (pérdida de portadora) de una línea serial. En cambio sobre una Ethernet no existe indicación de interrupción (semejante a la pérdida de carrier). Si sobre un router se efectúa un reinicio (reset) tampoco se dispone de una indicación inmediata. Una forma de detectar problemas es mediante la ventana de temporización luego de un mensaje Hello.

Escalabilidad: La escalabilidad de la red: se refiere a la posibilidad de crecimiento. Normalmente la escalabilidad se encuentra limitada por razones operacionales más que técnicas.

Seguridad: Referido al uso de medios para protección de la información de enrutamiento. El mecanismo de autentificación reduce potenciales inestabilidades

1.3 Calidad de Servicio (QoS)

La calidad de Servicio (QoS, Quality of Service) garantiza que se transmitirá cierta cantidad de datos en un tiempo dado (throughput). Esto permite que los proveedores de servicios garanticen a sus clientes que el retardo de extremo a extremo no excederá un nivel específico de tiempo. Además que en los servicios satelitales se tiene una nueva

perspectiva en la utilización del ancho de banda, dando prioridades a las aplicaciones de extremo a extremo con una serie de reglas.

Una red IP está basada en paquetes de datos, estos paquetes tienen una cabecera que contiene información sobre el resto del paquete. Existe una parte del paquete que se llama TOS, en esta parte se lleva banderas o marcas. Lo que se hace para darle prioridad a un paquete sobre el resto es marcar una de esas banderas, esto lo realiza el router mediante una configuración realizada. El equipo que genera el paquete, por ejemplo un gateway de voz IP, coloca una de esas banderas en un estado determinado y los dispositivos por donde pasa ese paquete luego de ser transmitido tienen (generalmente) la capacidad para poder discriminar los marcados para darle prioridad sobre los que no fueron marcados. Este esquema de QoS se muestra en la Figura 1.2 que se muestra a continuación.

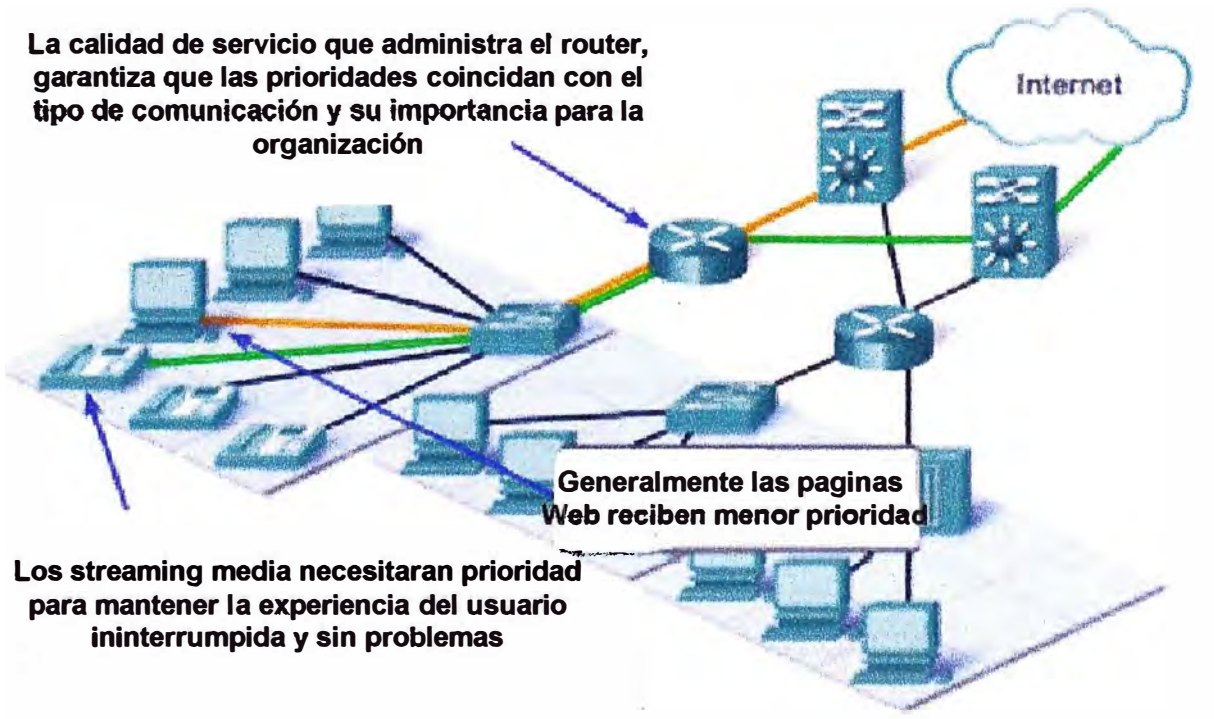

Figura 1.2 Calidad de Servicio (QoS) en un Router
(Fuente http://cisco.netacad.net/cnams/home/StudentClass.jsp)

Del uso de la Calidad de Servicio pueden beneficiarse todas las redes que deseen eficiencia óptima, sin importar que estas pertenezcan a pequeñas, medianas o grandes empresas que tienen sus propios requerimientos de QoS. Las redes empresariales deben proporcionar soluciones con calidad de servicio de extremo a extremo (usuarios) a través de diferentes plataformas que son partícipes de ellas, proporcionando soluciones para plataformas mixtas que a menudo requieren que se tomen diferentes aproximaciones en lo que concierne a implementación de QoS para cada tecnología utilizada en una red

heterogénea. Un claro ejemplo son las empresas que hoy en día manejan aplicaciones de datos de misión crítica y experimentan elevado tráfico multimedia Web, sintiendo la necesidad de que los equipos que ofrecen QoS prioricen el tráfico asegurando que se obtenga el nivel de servicio que cada aplicación requiere.

1.3.1 Ventajas

Las ventajas que se tiene al implementar Calidad de Servicio para controlar las aplicaciones y tipos de tráfico en redes, se refleja en las siguientes características:

a. Control sobre Recursos:

Se tiene control sobre recursos utilizados (ancho de banda, equipamiento, entre otros). Se puede limitar el consumo de ancho de banda sobre un enlace de núcleo o backbone para lo que es FTP, o también se puede dar prioridad al acceder a una importante base de datos.

b. Servicios Diferenciados

Un proveedor de servicios que controla y proporciona QoS puede gestionar los servicios de los clientes diferenciándolos en niveles o en clases.

c. Coexistencia de Aplicaciones de Misión Crítica

Las características de QoS hacen posibles las siguientes condiciones:

Que el enlace entre el cliente y el proveedor (WAN) sea utilizado eficientemente por las aplicaciones de misión crítica que son muy importantes para los negocios.

Que el ancho de banda y mínimo retardo requerido por aplicaciones de voz y multimedia sensible al tiempo de respuesta estén disponibles.

Que las otras aplicaciones utilizando el enlace, obtengan sus servicios

1.4 Protocolo MPLS

MPLS (Multi-Protocolo Label Switching) es un protocolo que se encapsula por encima de los protocolos de nivel de enlace, pero por debajo de IP. Básicamente lo que se consigue es decrementar el tiempo de resolución del "next- hop" o próximo salto para los paquetes IP. Para lograr esto se utilizan etiquetas añadidas a los paquetes, estas etiquetas definen un circuito virtual por toda la red, inicialmente se plantearon dos métodos diferentes de etiquetamiento, o en capa 3 o en capa 2. La opción de capa 2 es más interesante, porque es independiente de la capa de red o capa 3 y además permite una conmutación más rápida, dado que la cabecera de capa 2 esta antes de la capa 3.

La principal razón para usar MPLS en una red no es realmente la velocidad de conmutación de los paquetes a través de las etiquetas, ya que actualmente con la electrónica existente en el mercado se podría conseguir una velocidad similar usando:

Enrutamiento tradicional. El punto fuerte de MPLS es el ahorro de recursos en el núcleo, los dispositivos de transito no tienen la necesidad de conocer las rutas de los clientes o tener una tabla completa de las rutas de Internet ahorrando así gran cantidad de recursos.

MPLS proporciona características adicionales tales como:

VPN de capa 2 y 3 sin importar el tipo de tecnología que se use en cada una de las sedes de los clientes o incluso si es necesario atravesar otros ISP para interconectar diferentes sitios remotos.

Ingeniería de Trafico (Traffic Engineering TE), que es una manera de encaminar trafico MPLS en la red aprovechando enlaces que estén poco usados o de respaldo, así como responder de manera efectiva y rápida a posibles cortes en algún enlace.

1.4.1 RSVP (Resource Reservation Protocol)

El protocolo de señalización usado para MPLS es RSVP (Resource Reservation Protocol, Protocolo de Reserva de Recursos), este protocolo es un estándar en Internet. Con RSVP se pueden reservar anchos de banda mínimos, se permite la gestión del tráfico según su origen y según su tipo. Actualmente representa la forma más completa y sencilla de implementación de técnicas de ingeniería de tráfico. RSVP también permite técnicas de protección de los caminos MPLS, con lo que a pesar de la caída de algún enlace del backbone del proveedor, no se apreciará la pérdida de conectividad en ningún instante siempre y cuando exista un camino físico alternativo en el backbone. En la Figura 1.3 se muestra este protocolo.

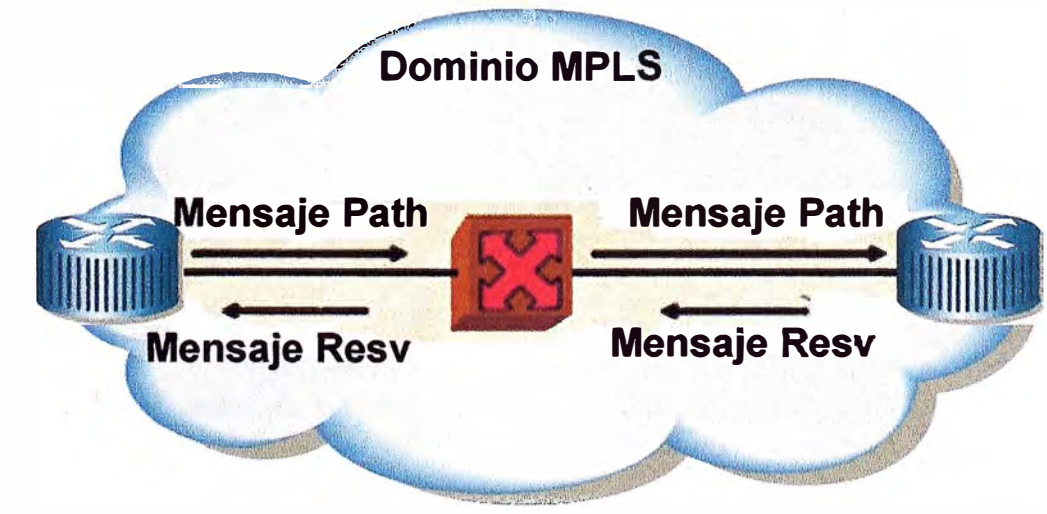

Figura 1.3 Protocolo RSVP
(Fuente Propia)

En la figura 1.3 se aprecia los mensajes del protocolo RSVP

1.4.2 VPN sobre MPLS

Las Redes Privadas Virtuales (VPN) implementadas con MPLS se aplican al backbone del proveedor de servicios, esto significa que el cliente sólo tiene que solicitarla y el proveedor se encarga de aprovisionarla y de hacerla activa. Las VPNs implementadas sobre una red MPLS contaran con una latencia baja. El protocolo MPLS basa las VPN en la creación de una tabla de rutas distintas para cada VPN, esto permite el solapamiento de direcciones y por tanto la reutilización del espacio de direcciones. Para los clientes esto añade una ventaja más ya que puede crear una VPN sin necesidad de cambiar el direccionamiento de sus equipos.

1.4.3 Arquitectura MPLS

La creación de una tabla de rutas por VPN separa el tráfico de diferentes VPN de forma lógica, esto se denomina una arquitectura de una VPN sobre MPLS. Esta arquitectura se forma cuando un sitio cliente está conectado a la red del proveedor de servicios (ISP) por una interfaz. El ISP asocia la interfaz a una tabla de enrutamiento y envío VPN denominada VRF (Virtual Routing and Forwarding, enrutamiento y envío virtual) en un PE (Enrutador de borde del proveedor). En una arquitectura VPN sobre MPLS se distinguen 3 tipos de dispositivos los cuales son el CE, PE y P. Un ejemplo de esta arquitectura de red MPLS se muestra en Figura 1.4.

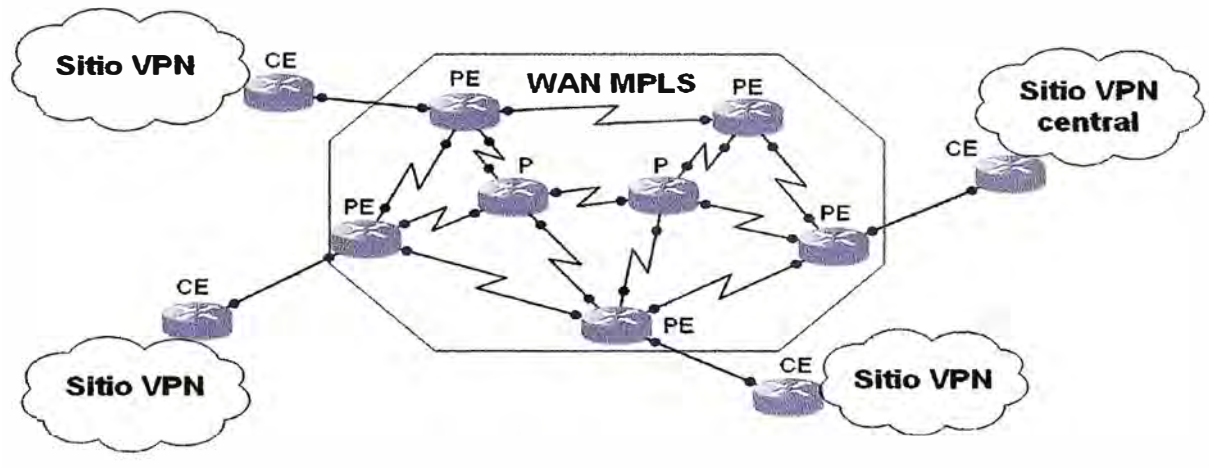

Figura 1.4 Arquitectura de una red MPLS
(Fuente: E. C. Rosen and Y. Rekhter, "BGP/MPLS IP VPNs", draft-ietf-l3vpnrfc2547bis-01.txt, Septiembre 2003)

a. CE (Equiment Customer o Equipo Cliente):

Es un router que establece adyacencia con el equipo del proveedor PE directamente conectado. Después de establecer adyacencia el enrutador CE anuncia la rutas locales del sitio VPN y aprende rutas remotas desde el PE. Este router pertenece a la red del

cliente.

b. PE (Equiment Provider o Equipo de Proveedor):

El router de borde (PE) del proveedor de servicios intercambia información de enrutamiento con el enrutador CE. Para intercambiar la información de enrutamiento se puede usar enrutamiento estático a algún protocolo de enrutamiento dinámico como RIP, OSPF, EIGRP o BGP. Cada enrutador PE mantiene una VRF para cada uno de los sitios directamente conectado.

c. P (Provider o Proveedor):

El router interno de proveedor (P) es cualquier enrutador en la red del proveedor que no une a los equipos clientes CEs. Los enrutadores P funcionan enviando y conmutando etiquetas.

1.4.4 Principales aplicaciones de MPLS

MPLS ofrece niveles de rendimiento diferenciados y priorización del tráfico, como aplicaciones de voz y multimedia, todo ello en una red.

MPLS permite funciones de ingeniería de tráfico, en general a los flujos de cada usuario se les asocia una etiqueta diferente.

MPLS también puede basar el etiquetado de los paquetes en función a criterios de prioridad y/o calidad de servicio (QoS). La idea de MPLS es realizar la conmutación de los paquetes o data gramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por el QoS, independientemente de la red sobre la que se implemente.

Conmutación veloz de paquetes usando etiquetas y no direcciones IP destino.

Troncales MPLS con dimensionamiento óptimo.

Utilización óptima del ancho de banda en accesos.

Es multi-protocolo tanto hacia arriba (L3) como hacia abajo (PWE3).

En la Figura 1.5 se muestra las principales aplicaciones de MPLS.

En resumen no olvidar que MPLS, es el Estándar del IETF (Grupo Especial sobre Ingeniería de Internet / Internet Engineering Task Force) que surgió a mediados de los años 90, a partir de propuestas brindadas por distintos proveedores de equipos de comunicaciones, para resolver los problemas de comunicación eficiente en el núcleo de una red de datos.

Finalmente MPLS utiliza lo mejor de dos arquitecturas, el enrutamiento de direcciones IP de la arquitectura IP y la velocidad de conmutación de paquetes en la arquitectura ATM. sobre una red MPLS, los proveedores de servicios establecen dos servicios, el de acceso a Internet y el de redes privadas virtuales, utilizando túneles para este último.

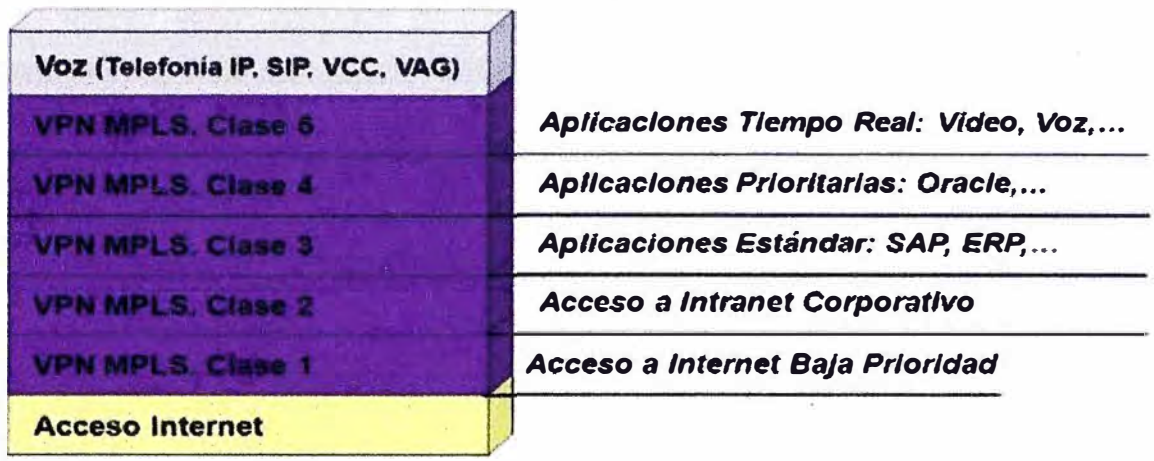

Figura 1.5 Clases de servicio para una red
(Fuente http://tic-tac.teleco.uvigo.es/profiles/blogs/las-redes-mpls-son-la-solucion)

En la figura 1.5 Se han definido siete clases de servicio para una red (VoIP/TolP, Internet y 5 clases de MPLS) para las aplicaciones

1.5 Protocolo de enrutamiento BGP

BGP (Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos. Por ejemplo, los ISP (Proveedores de servicio) registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP para el intercambio de información.

Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP, este intercambio de información de enrutamiento se hace entre los routers externos de cada sistema autónomo y estos routers deben soportar BGP. Este protocolo es el más utilizado para redes con intención de configurar un Protocolo de Gateway Exterior EGP (External Gateway Protocol). La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo, cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP).

BGP es un ejemplo de protocolo de gateway exterior (EGP) ya que BGP intercambia información de enrutamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles, además BGP es principal protocolo de publicación de rutas utilizado por las compañías más importantes de ISP en Internet. BGPv4 (BGP versión 4) es la primera versión que admite enrutamiento entre dominios sin clase (CIDR) y agregado de rutas. BGP, a diferencia de los protocolos de Gateway internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda, o retardo. BGP toma decisiones de enrutamiento basándose en políticas de la red o reglas

que utilizan varios atributos de ruta BGP. En la Figura 1.6 se muestra de manera esquemática como el protocolo BGP interconecta sistemas autónomos.

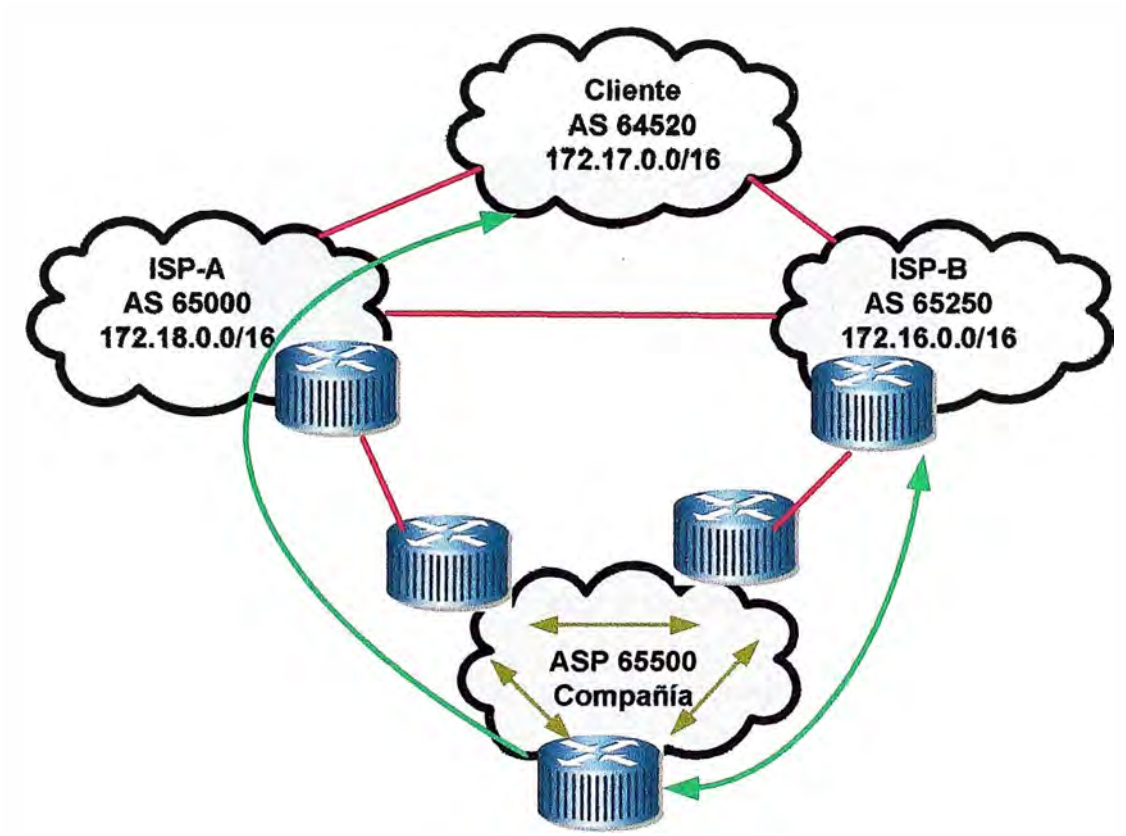

Figura 1.6 El protocolo BGP interconecta sistemas autónomos AS
(Fuente: http://cisco.netacad.net/cnams/home/StudentClass.jsp)

1.5.1 Modo de operación

El protocolo BGP se utiliza para intercambiar información de enrutamiento, este intercambio de información en la red se realiza mediante el establecimiento de una sesión de comunicación entre los routers de borde (PE) de los sistemas autónomos. Para conseguir una entrega fiable de la información se hace uso de una sesión de comunicación basada en TCP en el puerto número 179, esta sesión debe mantenerse conectada debido a que ambos extremos de la comunicación periódicamente intercambian y actualizan información, de modo que al inicio cada router envía al vecino toda su información de enrutamiento y después únicamente se enviarán las nuevas rutas, las actualizaciones o la eliminación de rutas transmitidas con anterioridad. Además periódicamente se envían mensajes para garantizar la conectividad.

Cuando una conexión TCP se interrumpe, cada extremo de la comunicación está obligado a dejar de utilizar la información que ha aprendido por el otro lado. Esta sesión TCP sirve como un enlace virtual entre dos sistemas autónomos vecinos y la falta de medios de de comunicación indica que el enlace virtual se ha caído, esa unión virtual

puede tener más de un enlace físico (redundancia).

En la Figura 1.7 se muestra el modo de operación del protocolo BGP donde se debe distinguir entre External BGP (EBGP) e Internal BGP (IBGP).

En dicha figura se muestra tres sistemas autónomos:

AS:AS 65101, AS6502 y AS65103.

a) EBGP hace referencia al intercambio de información entre sistemas autónomos.

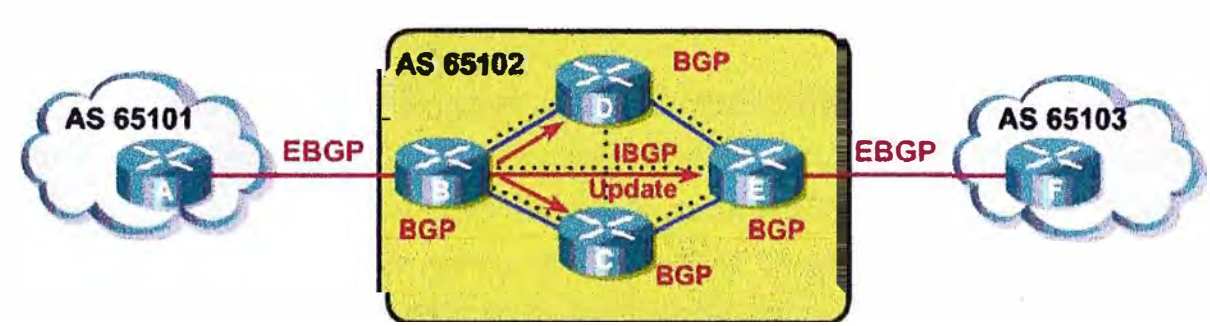

Figura 1.7 El modo de operación de BGP
(Fuente: http://cisco.netacad.net/cnams/home/StudentClass.jsp)

b) IBGP hace referencia al intercambio de información dentro de un sistema autónomo.

1.5.2 Tipos de mensajes:

Existen cuatro tipos de mensajes. Estos mensajes son:

Open,

Keepalive,

Update y

Notification.

a. Open: Se utiliza para el establecimiento de una sesión BGP una vez que se haya establecido la conexión TCP (puerto 179). Se suelen negociar ciertos parámetros que caractericen a esa sesión, por ejemplo es posible que los miembros de la sesión no tengan la misma versión de BGP por lo que es importante indicar el número de versión en este mensaje.

b. Update: Es un mensaje de actualización, es un mensaje clave en las operaciones de BGP ya que contiene los anuncios de nuevos prefijos. Se generarán mensajes de actualización cada vez que se determine una nueva mejor ruta para cierto destino o haya una modificación sobre alguna existente.

c. Keepalive: Una vez que la sesión BGP está activa, se envía periódicamente un mensaje KEEPALIVE para confirmar que el otro extremo sigue estando activo en la sesión BGP. Generalmente se acuerda un tiempo máximo de espera (hold time) durante el intercambio inicial de mensajes OPEN. El mensaje KEEPALIVE suele ser

aproximadamente una vez cada tercio del tiempo de espera, pero no más de una vez cada segundo. Los mensajes KEEPALIVE no se deben generar si el tiempo de espera es cero ya que en ese caso se entiende que la sesión es completamente fiable.

d. Notification: Se envía al cerrar una sesión BGP, esto sucede cuando ocurre algún error que requiera el cierre de la misma. De modo que es un mensaje que permite informar de los errores.

1.5.3 Atributos de BGP

El modo en que se gestiona la red utilizando el protocolo BGP es a partir de los atributos con los que cuenta dicho protocolo para satisfacer determinadas características o imposiciones de un escenario BGP. Se definen características para el tráfico saliente y para el entrante, siendo este último algo más difícil de controlar. De modo que esta gestión de la red se hace a partir de la selección de las rutas que cualquier router va a propagar en una red y de las rutas que va a escoger como preferentes y alternativas. Para ello se cuenta con un conjunto de atributos que dan información para la toma de decisión de filtrar o seleccionar rutas. Se describen los principales atributos.

a. Origen: Identifica el mecanismo por el cual se anunció el prefijo IP por primera vez. Se puede especificar como IGP (0), EGP (1) o INCOMPLETO (2). IGP indica que el prefijo IP se aprendió por un protocolo interior al sistema autónomo como por ejemplo OSFP. EGP indica que el prefijo IP se aprendió por un protocolo exterior como podría ser BGP, por ejemplo puede ser debido a que se ha realizado agregación. Generalmente si el ORIGEN es INCOMPLETO es porque se ha aprendido de forma estática. Si se quisiera decidir una selección de rutas en base a este prefijo se escoge la que tiene un valor de ORIGEN más bajo, es decir, se prefieren las rutas aprendidas por IGP antes que las de EGP y éstas últimas antes que INCOMPLETO.

Tabla 1.1 Atributo ORIGEN (Fuente propia)

VALOR	DESCRIPCION
IGP	Ruta originada dentro del AS
EGP	Ruta originada por Exterior Gateway Protocol (Descontinuado)
Incompleto	Otro medio, por ejemplo redistribución

b. As-Path: Este atributo almacena una secuencia de números de AS que identifican la ruta de AS's por los que ha pasado el anuncio. Cada vez que un router de borde propaga una ruta hacia otro lado añade a este atributo su número de AS constituyendo así la lista de AS's que se pretendía tener. La lista permanece intacta si se usa IBGP, es decir, si no

se sale del sistema autónomo. Si se quisiera utilizar el AS-PATH como método de selección de rutas se escogería el que tuviera una lista AS-PATH más pequeña. Esto es una forma de medir que haya menos saltos hacia el destino aunque no es exactamente así porque no se tienen en cuenta los posibles saltos debidos a los routers dentro de un sistema autónomo, tal como muestra la Figura 1.8.

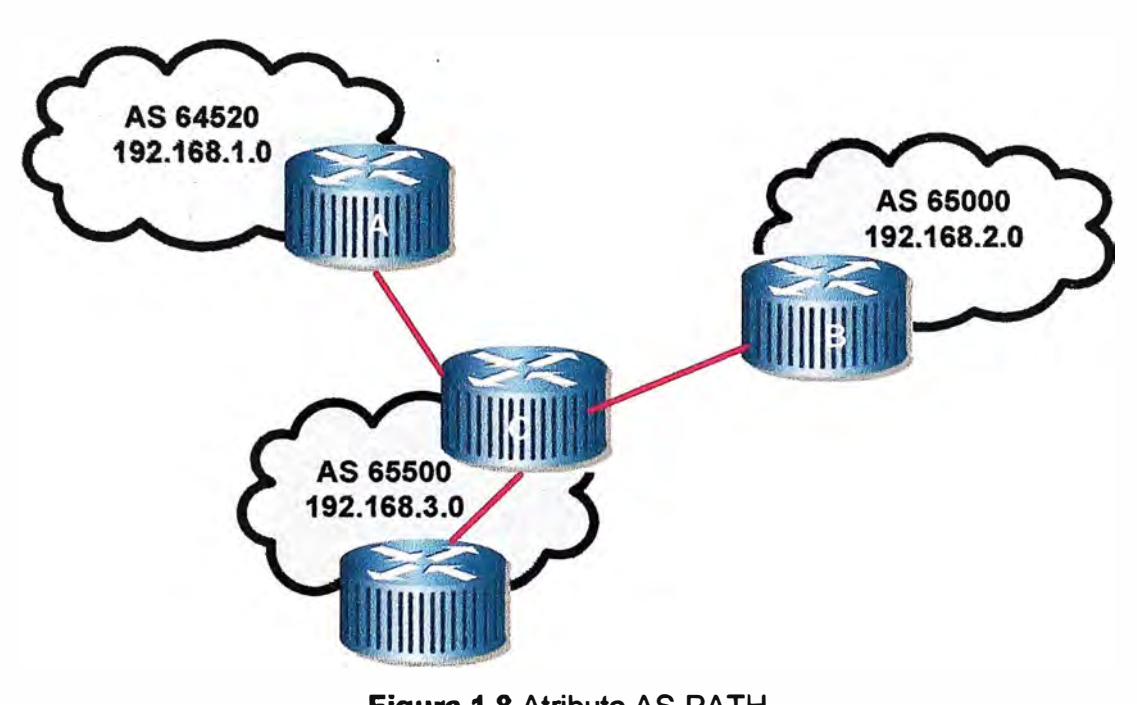

Figura 1.8 Atributo AS-PATH
(Fuente: http://cisco.netacad.net/cnams/home/StudentClass.jsp)

Observación: Los ASN (AS Number Los números de los sistemas autónomos) son asignados por el ARIN American Registry for Internet Numbers es el Registro Regional de Internet, van desde el 1 hasta el 65535. A partir del 64512 los ASN son de uso privado.

En resumen AS-Path es una secuencia de números de AS que se forma conforme una ruta se va propagando. Mientras más corto sea el AS-Path, la ruta se considerará más cercana. También sirve para evitar 'loops',(lazos) si un router ve su propio AS en un update, inmediatamente lo desecha.

c. Next-Hop: El siguiente salto identifica la dirección IP del router correspondiente al siguiente salto hacia el destino.

Se debe tener en cuenta que un prefijo IP se anuncia fuera de un sistema autónomo, por lo que el next-hop es el destino que se conoce y al que hay que enviar el tráfico de los usuarios que quieran llegar a un destino final.

La información del NEXT-HOP se procesa con los datos de tabla de enrutamiento IP. Ahora se contará con una tabla IP (con la que ya se contaba anteriormente) y con una tabla BGP que contendrá el NEXT-HOP para cada destino.

Se obtendrá una ruta hacia el destino BGP pasando por los saltos que indique la tabla de enrutamiento IP. Si se quisiera seleccionar una ruta por este atributo se seleccionaría la que suponga menor costo hacia el NEXT-HOP, es decir menor número de saltos hacia el NEXT-HOP. Este atributo se muestra en la Figura 1.9.

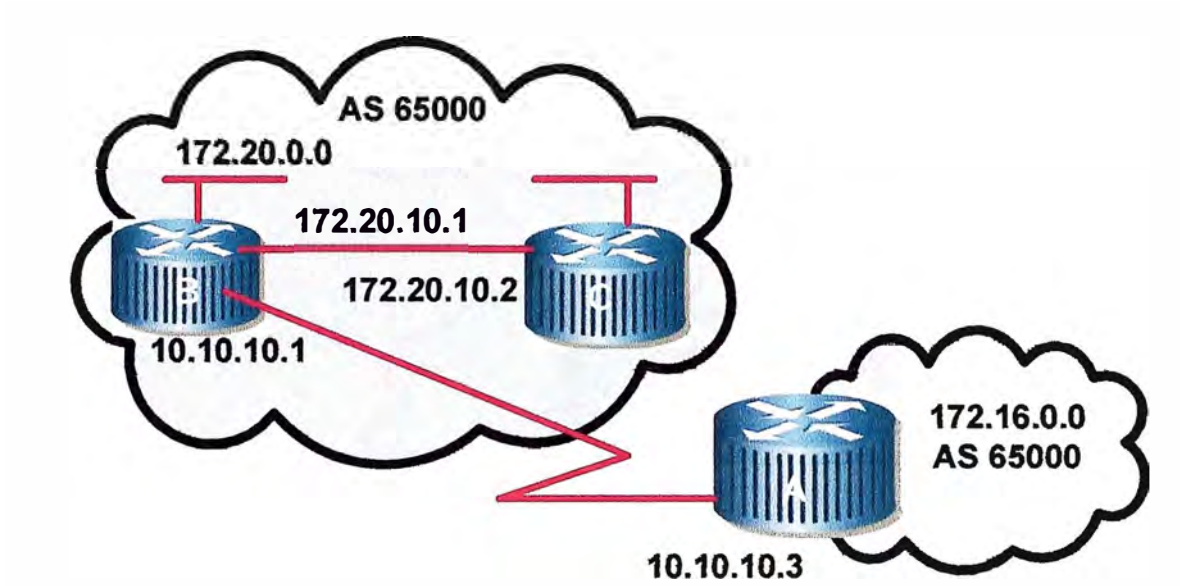

Figura 1.9 Atributo NEXT-HOP
(Fuente: http://cisco.netacad.net/cnams/home/StudentClass.jsp)

En la figura 1.9 el próximo salto (Next-Hop) del router A seria la dirección IP:
10.10.10.1

d. Multi Exit Discriminator (MED): Multi salida discriminador es un indicador diseñado para ser utilizado cuando desde un sistema autónomo existen múltiples enlaces hacia un mismo sistema autónomo, es decir desde un mismo sistema autónomo se realizan dos enlaces a otro sistema autónomo. Este atributo se puede utilizar para balanceo de carga, de modo que hacia unos prefijos se tenga un valor de MED que haga preferente cierto prefijo y hacia otros prefijos se haga preferente otro diferente.

Esta métrica es local entre dos sistemas autónomos, no se propaga fuera de ese ámbito. Si se quisiera seleccionar una ruta por medio de este atributo se consideraría preferida la que tuviese un valor de MED menor. Este atributo se observa en la Figura 1.10.

e. Local Preference: Este atributo (Ver figura 1.11) es útil en un escenario en el que un sistema autónomo tiene conectividad con múltiples sistemas autónomos, de manera que pueda haber múltiples rutas hacia un mismo destino. Este atributo dará preferencia al envío de tráfico por un enlace en concreto, por tanto solo tendrá sentido dentro de un mismo sistema autónomo, luego solo se transmite por IBGP. Se escogerá el envío de datos por el enlace que tenga un local preference más alto, siendo el valor por defecto (default) igual a 100.

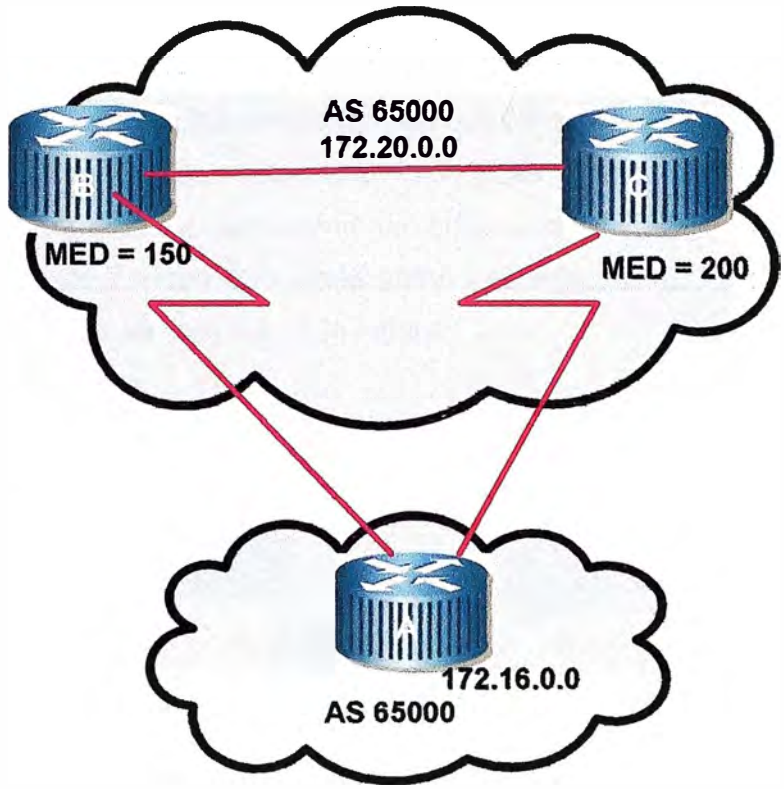

Figura 1.10 Atributo MED
(Fuente:Propia)

El atributo MED Sirve para influenciar el tráfico que ingresa al AS, siendo el menor valor el preferido. Este valor pasa de un AS a otro directamente conectado, pero no es propagado a un tercer AS.

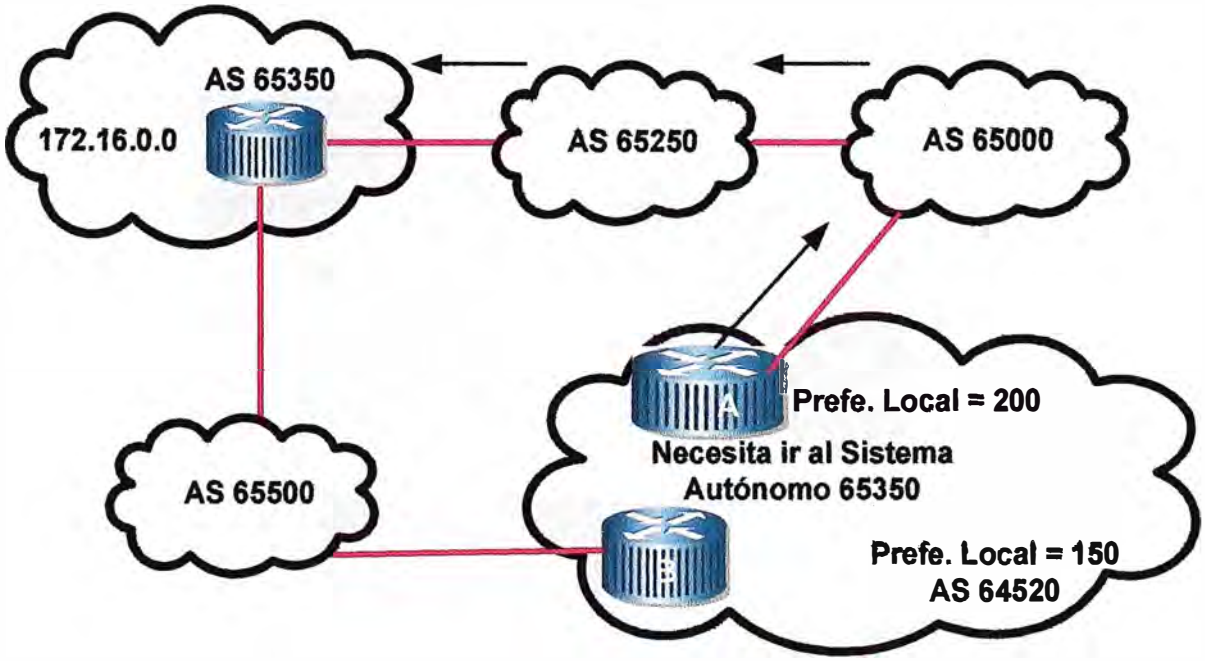

Figura 1.11 Atributo Local Preference
(Fuente Propia)

f. Community: Se puede gestionar la distribución de información de enrutamiento a un grupo de destinatarios llamados COMMUNITIES. La idea es que una vez suscrito a un grupo de destinatarios se les pueda aplicar una política de enrutamiento concreta, de ese modo se simplifica el trabajo agregando información de enrutamiento así como se proporciona una herramienta para tener un entorno más vigilado en la red, esto se consigue mediante un número que actúa como una etiqueta que califica a la ruta. Un ejemplo de este atributo se muestra en la Figura 1.12.

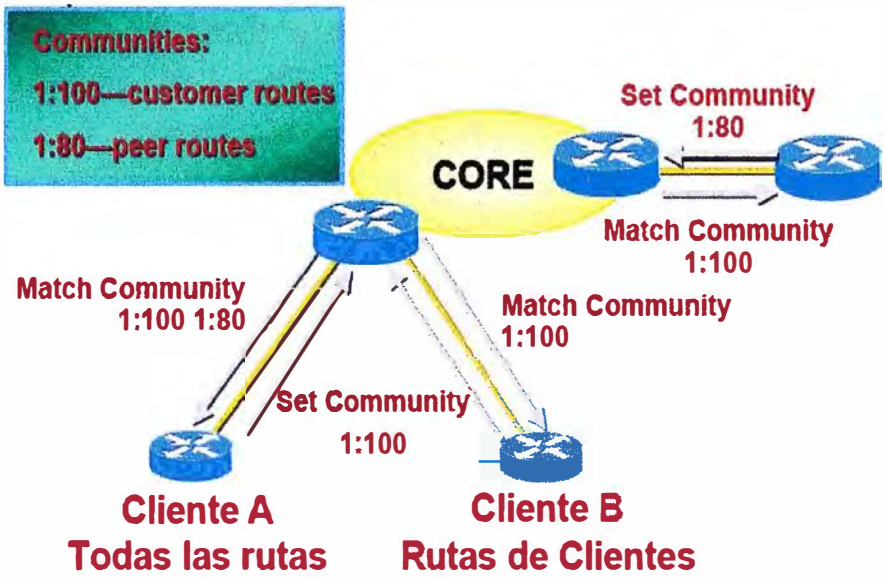

Figura 1.12 Atributo Community(Fuente: http://cisco.netacad.net/cnams/home/StudentClass.jsp)

1.5.4 Selección de rutas

Todos estos atributos pueden ser utilizados conjuntamente para la selección de rutas, sin embargo se debe imponer un orden de preferencia de manera que si se tienen varias rutas que pueden ser preferente solo se elija una. Se recorrerá la siguiente lista y se eliminarán las rutas que no empatan en el mejor valor de cada uno de los criterios. Se ha de tener en cuenta que los criterios de decisión de enrutamiento que incluyen normas de desempate se aplican a cada prefijo IP o conjunto de prefijos IP destino.

Si el siguiente NEXT-HOP no está disponible se ignora la ruta.

Eliminar las rutas con menor LOCAL-PREF.

Eliminar las rutas con AS-PATH más largo.

Eliminar las rutas con ORIGIN más alto.

Eliminar las rutas con mayor MED.

Eliminar las rutas aprendidas por IBGP si las hay aprendidas por EBGP.

Eliminar las rutas con mayor coste hacia el NEXT-HOP.

Preferir la ruta que ha anunciado el router con menor identificador BGP.

Preferir la ruta recibida desde el interfaz con menor dirección para el vecino.
Las últimas dos entradas de la lista son una forma de selección de rutas de alguna manera arbitrarias ya que no indican una política regulada como tal por un administrador. Sin embargo es una manera que propone BGP para que, el caso en que no se pueda decidir, se seleccione alguna ruta.

1.6 Protocolo IS IS

Es un protocolo de gateway interior IGP desarrollado en 1980 por DEC y estandarizado por la ISO como un protocolo de enrutamiento para el modelo de referencia OSI. El protocolo IS-IS es un enlace, o SPF (shortest path first), por lo cual, básicamente maneja una especie de mapa con el que se fabrica a medida que converge la red.
Este protocolo fue descrito por el RFC 1142. En este se refiere a que IS-IS fue creado con el fin de crear un acompañamiento a CNS (Protocol for providing the Connection less-mode Network Service).En un principio fue diseñado con la idea de crear una serie de protocolos que pudieran competir con TCP/IP. La idea original que genero la creación de IS-IS responde a los siguientes criterios:

- Crear un protocolo no propietario.
- Que sea escalable y jerárquico.
- Eficiente, que permita una rápida y eficaz convergencia sin sobrecargar la red.
- Con el transcurso del tiempo a IS-IS se le fueron añadiendo extensiones con el fin de competir y reemplazar a TCP/IP en Internet. Pero finalmente no obtuvo el resultado que se esperaba prevaleciendo TCP/IP entre ambos protocolos. A este IS-IS con extensiones se le llamo IS-IS Integrado, descrito por el RFC 1195. Actualmente simplemente se le llama IS-IS y es así como se tratara en este informe. Recientemente IS-IS está resurgiendo aumentando su popularidad debido a que se trata de un protocolo independiente, escalable y que define tipos de servicios.

1.6.1 Las características principales de Integrated IS-IS

a. Protocolo de tipo estado-enlace (link-state) cuyos mensajes usan el formato tipo, longitud, valor de tiempo de vida (TLV), lo que lo hace bastante flexible a cambios y nuevas implementaciones.
b. Forma adyacencias con los routers directamente conectados mediante el intercambio de Hellos, estas adyacencias pueden ser de tipo Level-1 o Level-2.
c. Las publicaciones de rutas (updates) usan mensajes IS-IS llamados LSPs (Link StatePDUs).
d. Su distancia administrativa es de 115.

e. El intercambio de tramas IS-IS (hellos, LSPs, etc) se hace a nivel de capa 2, solo las interfaces con IS-IS habilitado son capaces de entender y procesar estos mensajes.

f. Es 'classless', soporta autenticación, sumarización y división en áreas.

g. La métrica usada para comparar rutas depende del costo de cada enlace (se define manualmente).

1.6.2 Terminología IS-IS

Cuando se habla en terminología OSI, un router es definido como un sistema intermediario (IS) y una PC como un sistema final (ES), por tanto el protocolo IS-IS es un sistema router -a- router. Al implementar IS- IS es fundamental interpretar el direccionamiento OSI, el CLNS (Connectionless network Service), OSI soporta cuatro niveles de enrutamiento, en este caso IS-IS ocupa lo sgtes niveles:

- Nivel1, utilizado para intercambiar rutas de una área.
- Nivel2, es el núcleo, core o backbone entre áreas.

Los routers que ejecutan IS-IS pueden estar en el nivel 1, en el nivel 2 o en ambos. Estos ultimos conectan áreas al backbone. Estos niveles emplean el algoritmo de Dijkstra SFP para converger rápidamente.

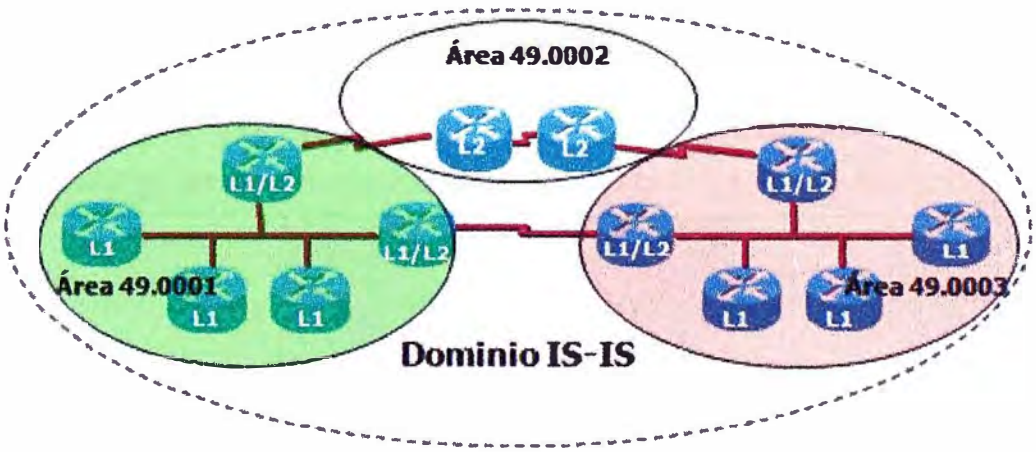

Figura 1.13 Area en IS IS
(Fuente: http://cisco.com)

CAPÍTULO II
DETERMINACIÓN DE NECESIDADES

El diseño abarca la reorganización de los servicios, así como todos los elementos que intervienen; plataforma de servidores, infraestructura de telecomunicaciones y telefonía.
Para ello se necesita diseñar una red con la última tecnología disponible en el mercado, integrando el conjunto en una solución global y compatible.
La red corporativa de la empresa transnacional de telecomunicaciones permite la interconexión entre sus diferentes áreas de negocio: red fija, red móvil, intranet, extranet, seguridad perimetral, área de administración, área de recursos humanos, centro de atención de ventas entre otras, con la finalidad de accesara las aplicaciones compartidas y no compartidas: Servidor antivirus, servidor DHCP, servidor Proxy, equipos de seguridad perimetral que se encuentran centralizados en un data center principal.
Se necesita definir la nueva infraestructura de la red corporativa desde las soluciones de comunicación internas de cada sede hasta los equipos de interconexión, accesos y los medios de transmisión a utilizar para interconectar, de manera robusta y con garantías de Calidad de Servicio, las diferentes sedes de Lima y provincias de la corporación.

Redes de Voz y Datos activas, separadas
WAN saturada iempo de respuesta deficiente
Dificultades para mantenerse al día con la seguridad
Movilidad limitada, recuperación de desastres limitada
Soluciones disparejas entre sucursales y oficinas principales

Figura 2.1 Situación de la redes actuales
(Fuente: http://www.slideshare.net/gugarte/integracin-de-servicios-de-redes-de-voz-y-datos-presentation)

Al diseñar esta nueva red es necesario considerar qué tipo de datos se van a transmitir a través de ella. Una red no es más que una herramienta, y hay un viejo axioma de los mecánicos según el cual para cada tarea debe usarse la herramienta indicada. Un análisis exhaustivo de los usos que va a tener asegurará que el desempeño de la red sea satisfactorio.

Las necesidades de ancho de banda son dictadas por las aplicaciones que se utilizarán en la red. Hay dos requisitos específicos de las aplicaciones que deben ser considerados: el caudal de tráfico y la latencia. El primero es la velocidad con que se transfieren los datos y se mide en bits por segundo; el segundo es la demora o retraso en la transmisión de los datos.

Algunas aplicaciones como bajar programas, navegar en la Internet y usar el correo electrónico regional pueden trabajar bien con un poco de latencia. Como se indicó antes, las aplicaciones "en tiempo real", como la VoIP o la Telefonía IP, no requieren mucha velocidad de transferencia de datos, pero sí una baja latencia.

También es importante la forma en que se conectan los puntos de acceso al eje troncal.

Aunque hay alguna validez en el argumento de que la seguridad puede manejarse eficazmente por encima de la capa física, la realidad es que un cable físico es más seguro que una señal de radio, cuyas limitaciones físicas son inexistentes. La intercepción de datos, la penetración de la red y el uso inapropiado de los recursos de la red por personas no autorizadas pueden exponer una red corporativa al robo de la información y del ancho de banda. Estos riesgos, sin embargo, pueden reducirse mediante la implementación de aplicaciones tales como SSL/SSH, VPN, 802.11i y Network Access/Admission Control en las redes inalámbricas.

Por lo expuesto anteriormente las necesidades de la red corporativa en detalle se pueden clasificar en seis grandes grupos:

- Necesidades de la Red de Core.
- Necesidades de las sedes remotas.
- Necesidades del Data Center.
- Necesidades de Seguridad Perimetral.
- Necesidades de Telefonía IP.
- Necesidades de Mecanismos de Monitorización.

2.1 Necesidades de la red de Core.

En la estructura de redes convergentes actuales, los equipos de núcleo o core son de vital importancia.

A través de ellos transita el grueso de información y datos de las empresas de Telecomu-

nicaciones y es en ellos donde se pone especial atención en la redundancia y la alta disponibilidad.

Se requiere que la conmutación de paquetes sea rápida, en el core, se busca contar con un protocolo de enrutamiento interior no propietario y estandarizado que soporte IPv6, que se tenga referencias o casos anteriores con éxito es decir experiencia en la implementación y que reemplace al protocolo propietario EIGRP de Cisco que se tiene actualmente.

Por lo expuesto, se debe contar con una Red de Core moderna, simple, escalable, disponible, gestionable e interoperable; preparada para soportar las nuevas aplicaciones de las diferentes áreas de negocio, del presente y del futuro, buscando que sea escalable, con redundancia geográfica hacia internet para prevenir cualquier eventualidad de la naturaleza como terremotos y de esta manera evitar tener una red no propia, antigua, con equipos de tecnología obsoleta y compleja que depende de otras áreas.

2.1.1 Parámetros de la nueva red de core:

Medio de Transmisión: Fibra óptica canalizada y subterránea.

Disponibilidad mayor a 99.99%.

(Ver tabla 2.1)

Interoperabilidad: Soporte de los protocolos ISIS, BGP, MPLS.

Equipamiento: Nuevo, de última generación.

Gestión: Propia, independiente de todos los equipos.

Escalabilidad: Se necesita equipos que soporten interfaces de 10GE.

Tabla 2.1 Disponibilidad expresado en Porcentaje

Disponibilidad	Duración del tiempo de inactividad anual
97%	11 días
98%	7 días
99%	3 días y 15 horas
99.9%	8 horas y 48 minutos
99.99%	53 minutos
99.999%	5 minutos
99.9999%	32 segundos

2.2 Necesidades de las sedes remotas.

Las diferentes sedes remotas de Lima y provincias presentan actualmente saturación en los enlaces hacia el data center, debido a que los anchos de banda son insuficientes para

las necesidades actuales. La necesidad de un mayor ancho de banda no cesa, debido al incremento de nuevos aplicaciones y usuarios.

El equipamiento de red que vienen a ser los dispositivos electrónicos que soportan la estructura lógica de comunicaciones y dan servicio de red a todos los equipamientos PC usuarios, servidores, impresoras.Se necesita realizar una renovación tecnológica total de los equipos de comunicaciones, en especial los routers, ya que presentan obsolescencia tecnológica, es decir antigüedad, y sin garantía o garantía vencida.

Se requiere que los nuevos routers de los nodos así como los routers clientes deben contar con redundancia de energía eléctrica, conectados a diferentes bastidores de energía.

Por lo expuesto, la solución de conectividad para las sedes remotas (Lima y provincias) debe ser de tecnología actual, simple, económica, disponible, y gestionable; preparada para soportar las necesidades actuales de acceso a las aplicaciones del negocio en tiempo real y de crecimiento futuro.

2.2.1 Parámetros de la solución de conectividad para las sedes remotas:

Medio de Transmisión: Fibra óptica canalizada y subterránea.

Disponibilidad mayor a 99.9%.

Interoperabilidad: Soporte de los protocolos BGP y MPLS.

Equipamiento: Nuevo, de vigencia tecnológica.

Gestión: Propia, independiente y centralizada desde el data center principal.

Escalabilidad: Se necesita equipos que soporten interfaces de 1GE.

2.2.2 Facilidades de infraestructura

También en cada sede remota de Lima y provincia se requiere contar con las siguientes facilidades de infraestructura para la instalación de los routers:

a. Área de la Sala.

Es necesario proveer un espacio razonable para la instalación de los equipos de comunicaciones con la finalidad de facilitar el acceso para realizar la operación y mantenimiento. Además en la parte posterior de cada equipo se deberá tener espacio para posibilitar los trabajos de conexionado de los cables de interfaces.

Los equipos deberán estar ubicados en un ambiente con buena ventilación y aislados del polvo y la exposición directa a la luz solar.

b. Sistema de Aire Acondicionado.

La sala deberá contar con un sistema 1+1 de aire acondicionado con controles automáticos de temperatura y humedad, estos equipos tendrán sensores distribuidos en La sala además de contar con un secuenciador para gobernar sus funciones.

La capacidad de los mismos dependerá de la carga de los equipos.

Temperatura de sala menor a 24º. C

Rango de tolerancia de Humedad Relativa: 5 a 95% no condensado

c. Energía de la Sala.

La energía comercial deberá llegar a un tablero de distribución equipado con una llave para proporcionar alimentación estabilizada y exclusiva a los equipos de comunicaciones y cómputo.

Esta red de alimentación será independiente de los otros sistemas de alimentación para luminarias, ventiladores, aire acondicionado, equipos de limpieza, entre otros.

Frecuencia de la red eléctrica de 60Hz.

Tablero de energía estabilizada de 220 VAC, con salida a través de interruptor térmico cuyas características dependerán de la carga de cada sistema.

Consumo de potencia de los equipos terminales de red, de acuerdo a lo indicado en las especificaciones suministradas con el equipamiento por el fabricante.

Las características de las llaves dependerán de la carga para cada sistema.

Se deberá contar con sistemas de protección de sobre tensión, y disparadores para prevenir cualquier sobrecarga o en lo posible instalar un transformador de aislamiento, el que podrá recibir cualquier tipo de configuración (delta o estrella).

Adicionalmente se debe contar con sistema de alimentación ininterrumpida UPS (Uninterruptible Power Supply,) y grupo electrógeno para las áreas críticas como:

Área de atención al cliente y centro de cobros,

d. Sistema de Tierra

Se deberá contar con un pozo para puesta a tierra con una calidad recomendable menor o igual a 5 ohmios, desde el cual se tomara la referencia para la tierra de la red de alimentación.

La toma de alimentación de energía deben estar debidamente polarizados (0 y 220 Vac) con respecto al punto de tierra y las conexiones de los equipos a la barra de tierra se harán directas e independientes.

2.3 Necesidades del Data Center.

Asegurar la continuidad operativa de un data center es para las empresas un tema crítico, pues allí radica información vital tanto para su negocio, como para el negocio de sus clientes en el caso de los proveedores de este servicio. Una caída del sistema, independiente de la causa, podría resultar todo un desastre, implicando pérdida de información; daños en los equipos; improductividad de los empleados; malestar entre los clientes, en síntesis, pérdidas para la compañía.

En el Data Center de la Red Corporativa, viene brindando servicios de hosting, housing, almacenamiento de información y comunicaciones IP a las diferentes unidades de negocios de la empresa. Los usuarios de la Red Corporativa a nivel nacional se comunican a nivel IP a los diferentes contenidos y plataformas alojados en el Data Center principal. Los equipos que soportan las comunicaciones, plataformas y servicios del Data Center ya fueron renovados en su totalidad. Debido a su importancia y criticidad de los servicios, actualmente se necesita interconectar en alta disponibilidad el nuevo data center principal hacia la red corporativa, también se necesita interconectar el data center de respaldo ubicado estratégicamente por temas de disaster recovery en Granados Trujillo.

En la actualidad se tiene implementado los siguientes servicios los cuales son:

- Business Continuity
- Clustering
- Virtualization
- Load Balancing
- Disaster Recovery

Figura 2.1 Data Center Principal de la empresa
(Fuente: http://computerservicenow.wordpress.com/2011/07/21/obama-administration-shutting-down-800-data-centers/)

Estos servicios no funcionan eficientemente dado que el ancho banda del data center principal hacia la red corporativa es insuficiente, esto fue demostrado por los continuos reportes de saturación de los usuarios a mesa de ayuda Helpdesk y comprobados por el centro de gestión.

Actualmente no se cuenta con alta disponibilidad del data center hacia la red corporativa, lo cual perjudicial para los diferentes negocios.

2.3.1 Parámetros de conectividad al Data Center principal y secundario:

Medio de Transmisión: Fibra óptica canalizada y subterránea.

Disponibilidad mayor a 99.999% con disaster recovery

Interoperabilidad: Soporte de los protocolos ISIS, BGP, MPLS.

Equipamiento: Nuevo, de vigencia tecnológica.

Gestión: Propia, independiente de todos los equipos de la red corporativa y centralizada en el mismo Data Center

Escalabilidad: Se necesita equipos que soporten interfaces de 10GE.

2.4 Necesidades de seguridad perimetral

Actualmente la información y los sistemas que lo soportan, se han convertido en activos fundamentales de las organizaciones. Las empresas dependen cada vez más de ellas para la operativa diaria, continuidad del negocio y toma de decisiones, pero al mismo tiempo estos sistemas se vuelven más complejos haciendo su administración más crítica, sobre todo cuando se refiere a su protección.

La gestión de la seguridad de información permite tomar acción consciente y ordenada sobre los riesgos que pueden ocasionar un impacto económico, operativo o sobre la imagen de la empresa.

La Internet es una red abierta, no segura y predispuesta a ataques de todo tipo, como denegación de servicios, código malicioso, amenazas, riesgos, virus, spam, troyanos, etc. Por tanto se necesita implementar una solución de seguridad para proteger el acceso a internet de la red corporativa.

Generalmente las soluciones de seguridad se basan en equipos firewalls con servicios adicionales (UTM).

2.4.1 Parámetros de la solución de seguridad perimetral:

Funcionalidades: Filtro web, con modulo de prevención de intrusos, antispam, antivirus, VPN, trafic shapping.

Disponibilidad: solución en alta disponibilidad (HA).

Gestión: Centralizada.

Sistema de reporte, análisis y almacenamiento de bitácoras: Que incluye capacidades de correlación y análisis de vulnerabilidades en la red para dispositivos de Administración Unificada de Amenazas.

Cantidad de interfaces de red: 12 puertos GE y 2 puertos SPF.

En la tabla 2.2 se muestra la cantidad de puertos utilizados en el firewall actual, asi como los puertos disponibles que vienen a ser 3, este firewall actual no dispone de puertos con modulo de fibra óptica SFP.

Tabla 2.2 Actuales puertos del Firewall

INTERFACE	RED
eth0	Administración
eth1	Rango Proxy
eth2	Red Interna Segura
eth3	Libre
eth4	DMZ1
eth5	DMZ2
eth6	Libre
eth7	Internet Publico
eth8	Ebussiness1
eth9	Teletrabajo
eth10	Ebussiness 2
eth11	Ebussines 3
eth12	DMZ_VPNs
eth13	Libre

2.4.2 Antivirus

Referente al antivirus se necesita contar con un servidor de antivirus corporativo, con una administración inteligente, centralizada y una automatización de procesos que ayude a acelerar la respuesta ante amenazas, que permita actualizar las versiones, definiciones de antivirus, realizar escaneos proactivos de los clientes y servidores de la empresa.

Figura 2.3 Diversos antivirus en el mercado
(Fuente: http://jonaescalante93.blogspot.com/)

Funciones claves que debe tener el servidor antivirus:

Detección proactiva de amenazas: Detección de malwares nuevos y que cambian rápidamente, debe detener el comportamiento malicioso, inclusive las amenazas nuevas.

Protección contra virus y spyware: Debe protege contra virus, gusanos, troyanos, spyware, bots, etc.

Consideraciones en la elección del Servidor Antivirus:

El servidor debe ser líder en la tecnología de detección proactiva y soporte en línea en temas de amenazas y virus. Debe contar con un escalamiento de soporte técnico 7x24x365. Que tenga adicionalmente soporte en habla hispana, que tenga bastante literatura en español e inglés lo cual permitirá gestionar de manera eficiente el tema del servidor antivirus. Que tenga soporte en línea, es decir por teléfono y Webex.

2.5 Necesidades de Telefonía IP.

Uno de los requerimientos impuestos en este proyecto es la convergencia de las comunicaciones, este hecho unido a la tendencia actual en materia de telefonía, impone un rediseño de este servicio acorde con una plataforma moderna, funcional y que permita un ahorro de costes. La telefonía IP cumple con estos requisitos, aportando una arquitectura preparada para nuevas funcionalidades impuestas por la tendencia del sector y permitiendo abrirse a los estándares del mercado.

Figura 2.4 Teléfonos IP
(Fuente:http://www.almerimatik.es/productos/centrales+digitales+voz+ip)

La red a diseñar debe contar con calidad de servicio para priorizar la voz (Telefonía IP), datos críticos (aplicación SAP y correo regional) y el best effort (Mejor esfuerzo)

Esta solución, permitirá tener un control detallado del registro de llamadas salientes de los trabajadores de las empresas, sobre todo para llamadas a celulares de otros proveedores y de larga distancia.

Actualmente ya se cuenta en producción y funcionamiento el Call Manager de Cisco, solo algunos usuarios de gerencia tienen telefonía IP, sin calidad de servicio. El nuevo diseño permitirá implementar paulatinamente la telefónica IP en todas las sedes remotas de las empresas y negocios que conforman la red corporativa.
Cabe mencionar que ya se tiene instalado un sistema de tarificación de llamadas.

2.5.1 Parámetros de la Telefonía IP:

Calidad de Servicio: En cada router se debe configurar los respectivos caudales de prioridad de ancho de banda.

2.6 Necesidades de mecanismos de monitorización:

Una red corporativa debe contar con un sistema de administración porque hay que asegurar a los usuarios: su utilización, la monitorización del tráfico y la calidad de servicio, evitar problemas, dar una solución rápida y eficaz.
Se necesita contar con una herramienta o software que permite administrar redes gestionando el ancho de banda y fallos de la red en tiempo real. Adicionalmente se necesita monitorear la carga de CPU, utilización de memoria, y espacio en disco disponible de los diferentes servidores.
Para cumplir los actuales desafíos y nuevos servicios expuestos anteriormente es necesario la compra e implementación de un software de monitoreo cuyos parámetros serán:
Costo: Económico.
Soporte del proveedor: 24x7x365.
Escalable: Por medio de licencias
Configuración: Fácil.
Reportes: Personalizables y fácil exportación a formatos pdf y Word.
Alarmas: Envió de alarmas vía SMS a celulares y correo electrónico.
En resumen:
La red corporativa actual presenta problemas de comunicación, los enlaces de comunicación de las sedes remotas continuamente se saturan por la creciente demanda de las aplicaciones, estos enlaces no están preparados por la demanda de trafico que solicitan las diferentes áreas de negocio, los costos del mantenimiento de la actual red son elevados por tener enlaces seriales .La red actual no es eficiente es decir, en la actualidad no se garantiza, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP, en resumen es una red best effort (La red hace lo posible por transmitir la información de la manera más rápida y fiable posible).

Se necesita diseñar e implementar una red basada en MPLS es decir el ahorro de recursos en el núcleo o core de la red, ágil y simple, que converja rápidamente: Es decir que todos los routers tengan información completa y precisa sobre la red, ante cualquier cambio o modificación en el menor tiempo posible).

A nivel de las sedes remotas se debe diseñar enlaces con ancho de banda que permita y asegure el flujo adecuado de la comunicación de voz, recursos multimedia y datos priorizando las aplicaciones críticas, secundarias y no criticas.

CAPÍTULO III
DISEÑO DE LA RED

3.1 Arquitectura de la red a implementar:

3.1.1 Diseño de la red de Core:

Se propone que el core, el backbone o núcleo estará conformada por 6 nodos, ubicados estratégicamente y geográficamente Estos nodos serán:

•En Lima:

Nodo Miraflores.

Nodo Santa Anita.

Nodo Cercado de Lima.

Nodo San Isidro.

•En Provincia:

Nodo Cusco.

Nodo Trujillo.

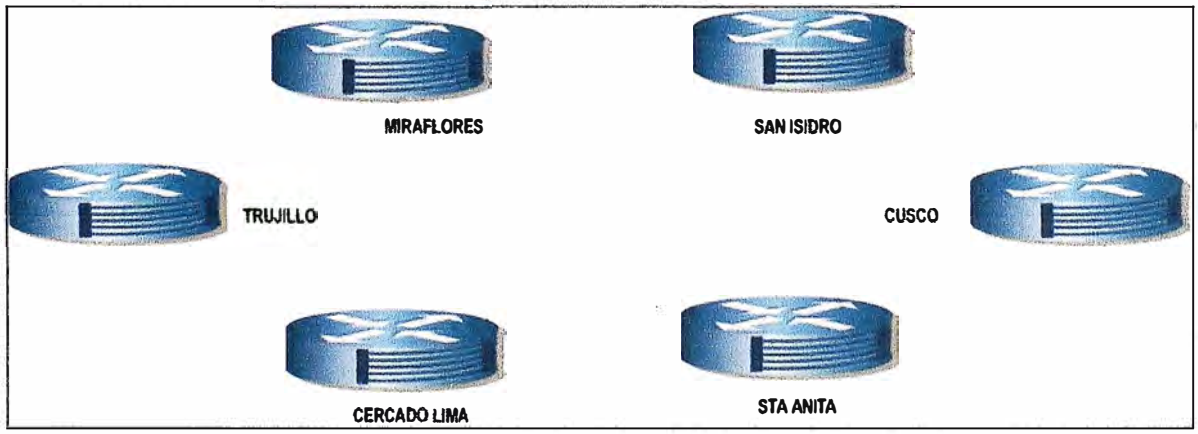

Figura 3.1 Esquema de los 6 nodos propuestos (Fuente: propia).

En la figura 3.1 se observa que se dispondrá de 2 nodos en provincia: Trujillo y Cusco.

a. Medio de Transmisión:

La conexión entre los nodos será a través de conexiones de fibra óptica canalizada y subterránea, ya instalas a la fecha por el área de Transmisiones. El tipo de fibra a utilizarse es del tipo monomodo dado por las distancias que se tiene entre nodos.

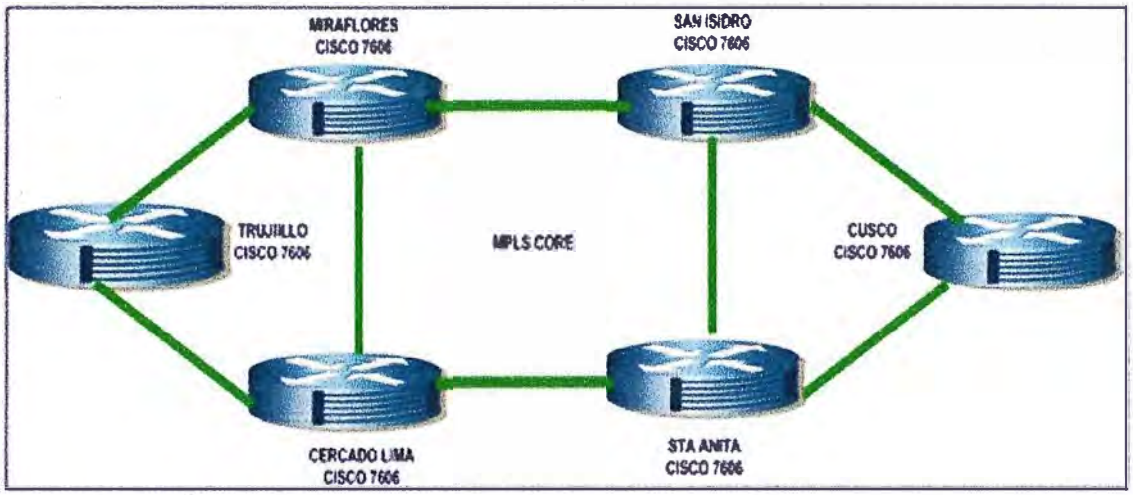

Figura 3.2 Esquema de conexión por fibra óptica de los seis nodos (fuente propia)

La fibra en cada local fue terminada en un bastidor de fibras denominado ODF (Distribuidor de Fibra Óptica).

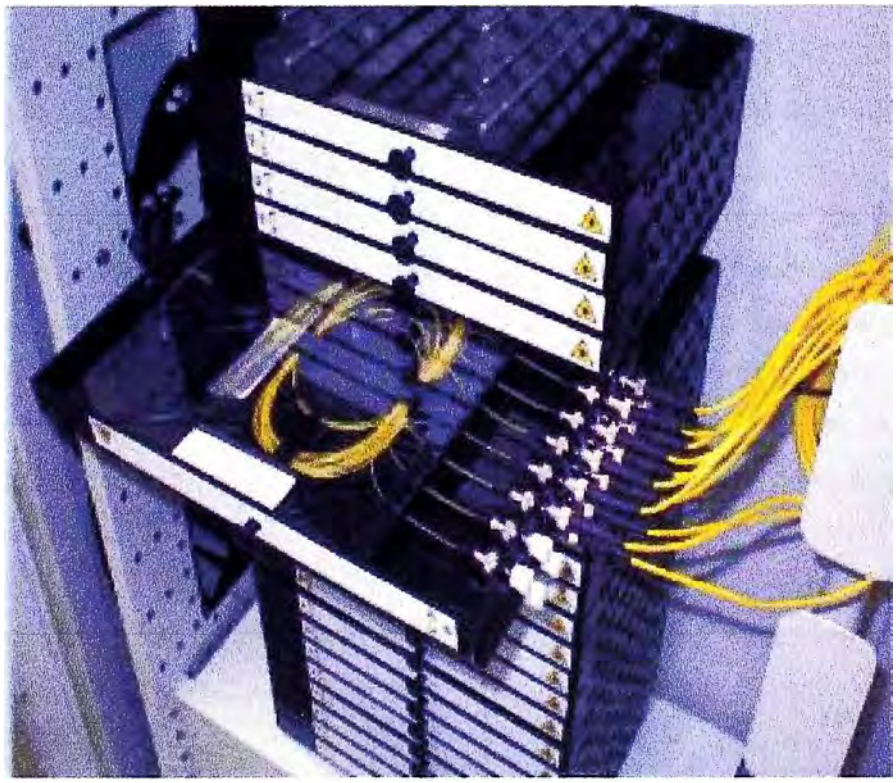

Figura 3.3 Esquema del ODF (Distribuidor de Fibra óptica)
(Fuente: http://www.revenga.com/np/upload/pdf-fic-20080617125432.pdf)

En la figura 3.3 se muestra las bandejas. La alta capacidad del distribuidor se consigue con bandejas organizadoras de 8 fibras y con diferentes tamaños de subracks. En las bandejas se realiza la interconexión de fibras externas y los patch cords de fibra.
Estos patch cords como se muestra en la figura 3.4 se conectaran con sus

correspondientes nodos. (Router de Core).

Figura 3.4 Patch Cord (Fuente: http://www.formosa-cables.com/products/)

Se usara conexiones de patch cords monomodo que son más fáciles de encontrar en el mercado que los mutimodo para conectar el respectivo ODF con router nodo. Los patch cords serán entregados por la área de transmisiones.

La interconexión de los nodos será a través de fibra óptica, canalizada y subterránea ya implementada por el área de transmisiones.

El data center principal donde se encuentra ubicado las aplicaciones de los diferentes negocios, los sistemas que permiten la gestión de los servicios que brinda la empresa a persona, empresas y corporaciones, estará interconectado a los nodos de San Isidro y Miraflores para tener redundancia, ante cualquier evento que podría suceder.

El data center secundario de Granados se conectara directamente a través de fibra óptica hacia el Nodo de Trujillo. Para proveer temas de disarter recovery, a través de un router de borde.

Adicionalmente aparte de tener alta disponibilidad de acceso a internet, se contara con redundancia geográfica hacia internet. El enlace secundario se conectara al data center secundario de Granados en Trujillo.

b. Ancho de Banda:

El ancho de banda del core propuesto es de 10Gbps.

c. Equipamiento:

Por lo expuesto en 2.1 el equipo para cada nodo seria el router Cisco 7606.El Router Cisco 7606 es compacto y con alto desempeño, especialmente diseñado con 6 slot para desarrollar todo el potencial de la nueva red, donde se requiere un desempeño robusto y switcheo IP/Multiprotocolo MPLS donde es necesario ambos requerimientos.

La elección de este router habilita proveer servicios mediante Ethernet, para crear infra-

estructuras de redes avanzadas que soporten el rango triple play IP de video, voz y datos.

Por alianza estratégica entre Cisco y la empresa de Telecomunicaciones, temas de descuentos preferenciales a nivel transnacional, experiencia previas se determino la elección de esta marca.

En la figura 3.5 se muestra que el router Cisco 7606 tienes 6 slots o ranuras .Los 2 slots de la parte inferior son las tarjetas procesadoras,

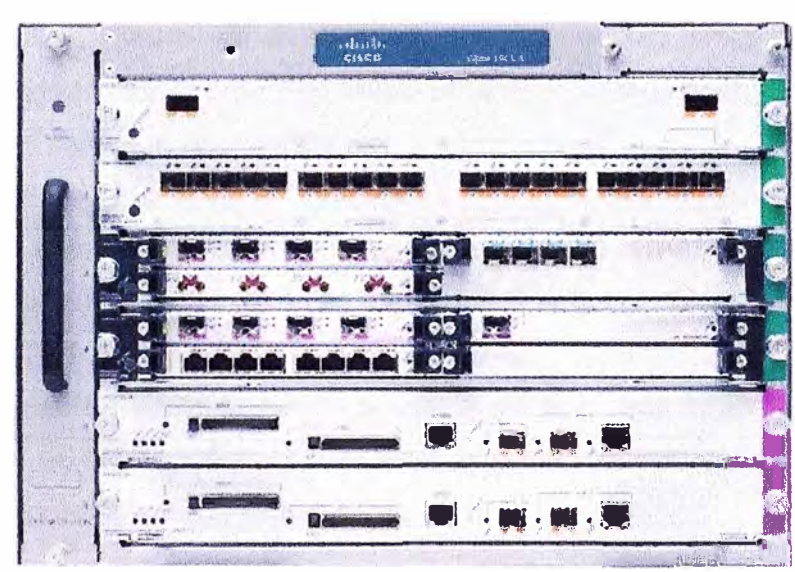

Figura 3.5 Imagen del router 7606
(Fuente ucts/hw/routers/ps368/ps371/index.html)

Entre otras Características del Router Cisco 7606 que se puede citar tenemos:

Rendimiento total: 480Gbps

Siete-RU (12.25-in.) chassis compacto, hasta 6 chassis por 7-pie rack

Network Equipment Building Standards (NEBS) Conformidad Nivel 3

Capacidad de protección route procesador: 1 + 1

Suministro de Energía opción de protección, AC o DC: 1 + 1

d. Interoperatibilidad:

Para el núcleo o core el protocolo elegido para cumplir las necesidades expuestas en el capítulo 2.2 el protocolo para una conmutación rápida entre los nodos será MPLS y para el enrutamiento se usa el protocolo ISIS que cumple con las necesidades expuestas en el capítulo 2, de ser un protocolo no propietario, escalable a IPv6 mas fácilmente que OSPF jerárquico, eficiente, que permita una rápida y eficaz convergencia sin sobrecargar la red.

3.1.2 Diseño de las sedes remotas:

a. Medio de transmisión

La conexión entre los routers de las sedes remotas con el core será a través de la red Metro Ethernet con la que cuenta la empresa.

Cabe resaltar que la red Metro Ethernet que se usara es la que actualmente dispone la empresa para sus clientes externos.

Finalmente la red Metro Ethernet a utilizar tiene redundancia en el propio anillo metro Ethernet o también usando otro anillo Ethernet.

Un dato importante es que el tiempo de convergencia de la red Metro Ethernet en la vida real es aproximadamente de 200ms.

La razón utilizar la red Metro Ethernet de ela empresa es por temas de redundancia y costos. Es más barato utilizar esta Red Metro Ethernet que mantener y solicitar usar una interfaces seriales para la implementación.

b. Ancho de Banda

De acuerdo a datos estadísticos, alcanzados por el área de administración y mantenimiento de la red corporativa se determino que la concurrencia de voz es 10%, datos críticos es 70% e internet y otros servicios 40%.

Se realizara calidad de servicio, siendo la voz el servicio más importante, en segundo lugar el servicios de datos críticos y finalmente el último servicio será el internet y otras aplicaciones no contempladas anteriormente.

A continuación se muestra el procedimiento de diseño del ancho de banda de cada sede y negocio de la empresa:

Para todos los casos de la sedes de Lima y provincia.

$$\text{BW total i} = \text{Usuarios} * \text{BW(Kbps)i} * \text{C}$$

Donde:

BW total i = ancho de banda de voz, datos críticos o internet

C = concurrencia de usuarios a la vez promedio expresado en %.

BWi = Ancho de banda promedio de voz, datos críticos o internet.

i = voz, datos críticos o internet.

Sede Surquillo:

Tabla 3.1 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%) bps	Caudales
Voz	760	64	10	4864	5836.8	6Mbps
Datos Criticos	310	80	70	17360	20832	21Mbps
Internet, otros	1100	80	40	35200	42240	Best Effort
				BW Total + margen (20%) bps	68908.8	
				BW SOLICITADO	70 Mbps	

Por tanto el ancho de banda propuesto para la sede de surquillo sería de 70 Mbps.

También se muestran los caudales de voz datos críticos, e internet

Sede Surco:

Tabla 3.2 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%) bps	Caudales
Voz	500	64	10	3200	3840	4 Mbps
Datos Criticos	250	80	70	14000	16800	17Mbps
Internet, otros	500	80	40	16000	19200	Best Effort
				BW Total + margen (20%) bps	39840	
				BW SOLICITADO	40Mbps	

Por tanto el ancho de banda propuesto para la sede de Surco sería de 40 Mbps.

Sede Begonias:

Tabla 3.3 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%) bps	Caudales
Voz	800	64	10	5120	6144	8 Mbps
Datos Criticos	400	80	70	22400	26880	14Mbps
Internet, otros	1000	80	40	32000	38400	Best Effort
				BW Total + margen (20%) bps	71424	
				BW SOLICITADO	60Mbps	

Por tanto el ancho de banda propuesto para la sede de Begonias sería de 60 Mbps.

Sede Lince:

Tabla 3.4 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%)	Caudales
Voz	65	64	10	416	499.2	500 Kbps
Datos Criticos	30	80	70	1680	2016	1.4 Mbps
Internet, otros	80	80	40	2560	3072	Best Effort
				BW Total + margen (20%) bps	5587.2	
				BW SOLICITADO	6Mbps	

Por tanto el ancho de banda propuesto para la sede de Lince sería de 6 Mbps.

Sede Callao:

Tabla 3.5 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%) bps	Caudales
Voz	50	64	10	320	384	400 kbps
Datos Criticos	40	80	70	2240	2688	1.4 Mbps
Internet, otros	70	80	40	2240	2688	Best Effort
				BW Total + margen (20%) bps	5760	
				BW SOLICITADO	6 Mbps	

Por tanto el ancho de banda propuesto para la sede del Callao sería de 6 Mbps.

De la Tabla 3.5 se observa el caudal para voz seria de 400Kbps.

Sede La Victoria:

Tabla 3.6 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%) bps	Caudales
Voz	200	64	10	1280	1536	1.6Mbps
Datos Criticos	100	80	70	5600	6720	7 Mbps
Internet, otros	200	80	40	6400	7680	Best Effort
				BW Total + margen (20%) bps	15936	
				BW SOLICITADO	16 Mbps	

Sede La Molina:

Tabla 3.7 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%) bps	Caudales
Voz	50	64	10	320	384	400 Kbps
Datos Criticos	80	80	70	4480	5376	6 Mbps
Internet, otros	150	80	40	4800	5760	Best Effort
				BW Total + margen (20%) bps	11520	
				BW SOLICITADO	12 Mbps	

Sede Arequipa:

Tabla 3.8 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%)	Caudales
Voz	100	64	10	640	768	800 Kbps
Datos Criticos	60	80	70	3360	4032	4.2 Mbps
Internet, otros	120	80	40	3840	4608	Best Effort
				BW Total + margen (20%) bps	9408	
				BW SOLICITADO	10 Mbps	

Sede Puno

Tabla 3.9 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%)	Caudales
Voz	30	64	10	192	230.4	300 Kbps
Datos Criticos	15	80	70	840	1008	1.1 Mbps
Internet, otros	45	80	40	1440	1728	Best Effort
				BW Total + margen (20%) bps	2966.4	
				BW SOLICITADO	3 Mbps	

Sede Chiclayo:

Tabla 3.10 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%)	Caudales
Voz	75	64	10	480	576	500 Kbps
Datos Criticos	50	80	70	2800	3360	1.5 Mbps
Internet, otros	95	80	40	3040	3648	Best Effort
				BW Total + margen (20%) bps	7584	
				BW SOLICITADO	5 Mbps	

Vitarte:

Tabla 3.11 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%)	Caudales
Voz	70	64	10	448	537.6	500 Kbps
Datos Criticos	85	80	70	4760	5712	1.5 Mbps
Internet, otros	170	80	40	5440	6528	Best Effort
				BW Total + margen (20%) bps	12777.6	
				BW SOLICITADO	13 Mbps	

Piura:

Tabla 3.12 Dimensionamiento de Ancho de Banda (Fuente propia)

Servicio	Usuarios	BW (kbps)	Concurrencia %	BW Total Kbps	BW + margen (20%)	Caudales
Voz	70	64	10	448	537.6	600 Kbps
Datos Criticos	45	80	70	2520	3024	3.2 Mbps
Internet, otros	95	80	40	3040	3648	Best Effort
				BW Total + margen (20%) bps	7209.6	
				BW SOLICITADO	8 Mbps	

Por tanto el Ancho de Banda solicitado para cada sede dimensionados seria:

Tabla 3.13 Resumen del Ancho de Banda de las sedes remotas (Fuente propia)

SEDE	USUARIOS	BW Mbps
Lince	80	6
Begonias	1000	72
Surco	500	40
Surquillo	1100	70
Callao	70	6
La Victoria	200	16
La Molina	150	12
Arequipa	120	10
Puno	45	3
Chiclayo	95	8
Vitarte	170	13
Piura	95	8

c. Equipamiento.

Para cumplir con los parámetros de solución, de la misma manera por las necesidades expuestas en el capítulo 2.2 el router propuesto es el router Cisco modelo 3845

Este router como se observa en la figura 3.6 posee 2 fuente redundantes de energía en la parte frontal ubicados en la parte inferior. También se puede observar la presencia de 2 interruptores.

Las interfaces de este equipo 3845 se encuentran en la parte posterior

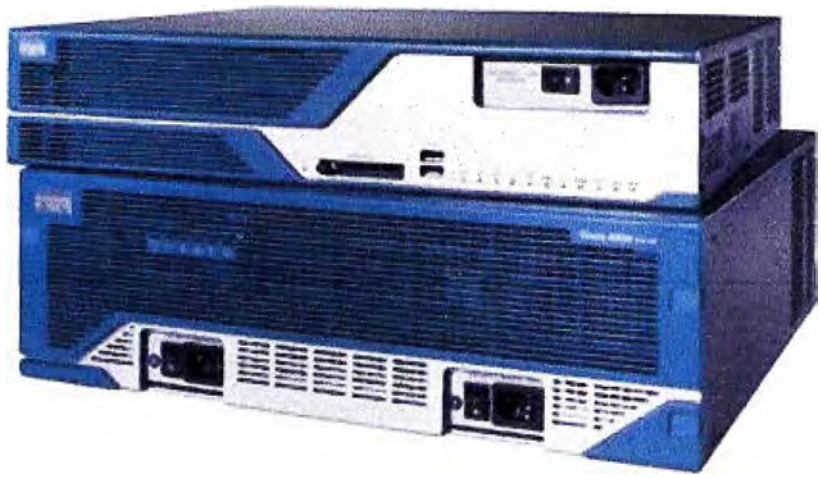

Figura 3.6: Serie Cisco 3800
(Fuente:router-switch.com/cisco3845-p-258.html)

d. Interoperabilidad:

Para las sedes remotas BGP (Boarder Gateway Protocol) será el protocolo a utilizar para anunciar las redes de cada sede remota de Lima y provincias.

Se decidió utilizar BGP debido a que es el protocolo más utilizado por las empresas y proveedores de servicio en Internet; algunas de sus ventajas principales son garantizar el enrutamiento libre de bucles y resúmenes de ruta (CIDR).

3.1.3 Diseño de conexión del Data Center principal

a. Medio de transmisión

En el data center principal de Corpac donde se encuentra ubicado las aplicaciones de los diferentes negocios, persona, empresas y corporaciones, estará interconectado a la red corporativa a través de los nodos de San Isidro y Miraflores en alta disponibilidad, por medio de fibra óptica (fibra oscura) por la alta importancia de los negocios.

b. Ancho de Banda:

El ancho de banda será de 1Gbps este dato se obtuvo por los estudios previos y datos estadísticos en los ultimos 6 meses realizado por el centro de gestión.

c. Equipamiento

El equipo a utilizar será el router Cisco modelo 7201.

El router Cisco 7201 permitirá mejorar la eficiencia operativa.

Además, incorpora un procesador de 1,7 GHz e incluye cuatro interfaces GE con cuatro interfaces ópticos SFP, también cuenta con una tarjeta de 64 MB Compact Flash y puertos auxiliares y de consola y sobre el chasis cuenta con un diseño compacto de una unidad de rack(1U) .

Como se pueda visualizar en la figura 3.7

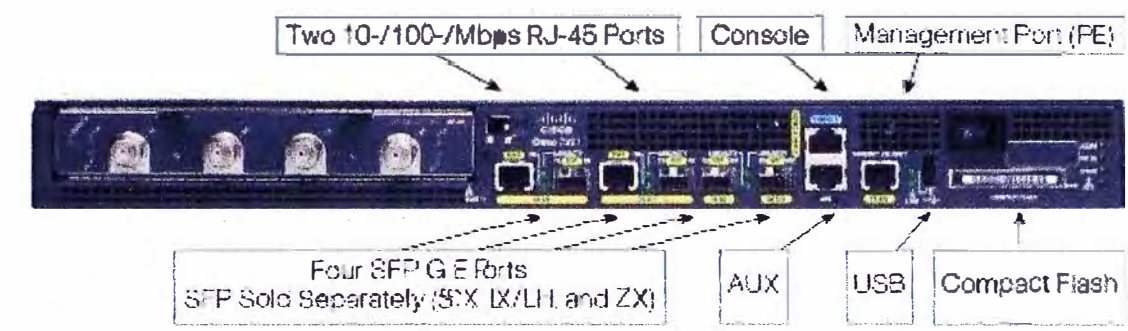

Figura 3.7 Router Cisco 7201
(Fuente:http://www.cisco.com/en/US/prod/collateral/routers/ps341/ps7253/product_data_sheet0900aecd80630b58.html)

En el gráfico 3.7 se visualiza que el router Cisco 7201 tiene 4 puertos SFP y 2 puertos 10/100Mbps RJ45, también presenta un puerto de gestión (Management)

El data center principal de Corpar estará conectado a los nodos de Miraflores y San Isidro con esto se tendrá redundancia de enlace.

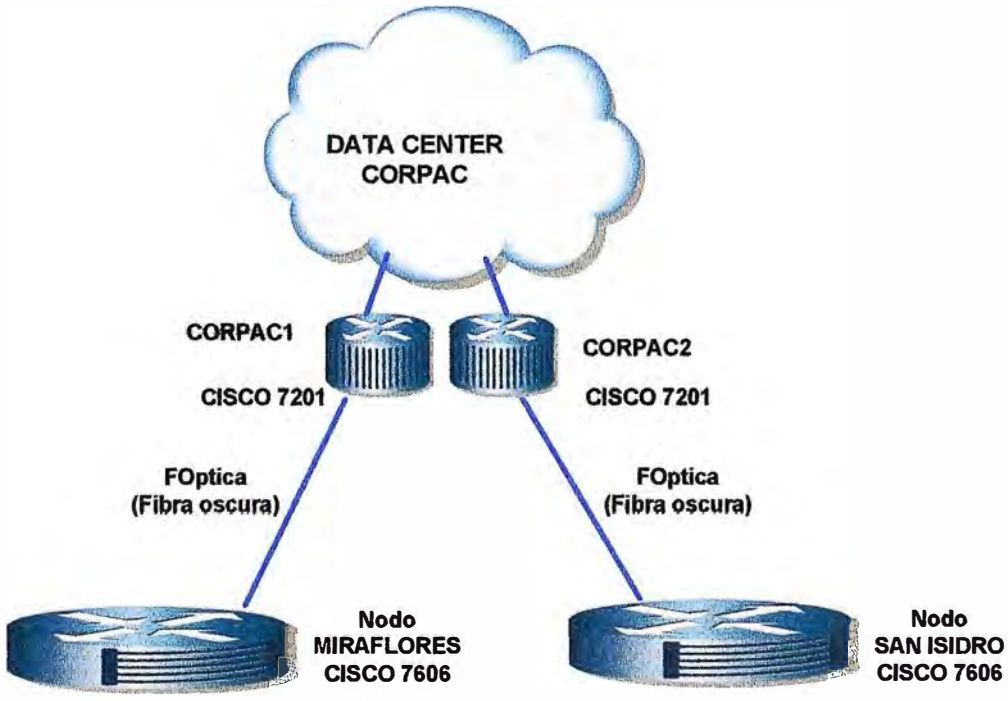

Figura 3.8 Esquema de conexión al data center principal (Corpac) a la red corporativa (Fuente propia)

d. Interoperatibilidad.

Al igual que las sedes remotas el protocolo a usar para el enrutamiento será BGP.

3.1.4 Diseño de conexión del Data Center secundario

Medio de transmisión:

La conexión del data center secundario Granados Trujillo hacia el nodo de Trujillo será a través de fibra óptica canalizada y subterránea.

Existen diferentes riesgos que pueden impactar negativamente las operaciones normales de una organización. Una evaluación de riesgo debería ser realizada para ver que constituye el desastre y a que riesgos es susceptible a la empresa

Esto permitirá tener un plan de recuperación ante desastres (Disaster Recovery Plan) que viene a ser un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que los negocios de la empresa puedan a comenzar de nuevo sus operaciones en caso de las siguientes situaciones:

Catástrofes.

Fuego.

Fallos en el suministro eléctrico.

Ataques terroristas.

Interrupciones organizadas o deliberadas.

Sistema y/o fallos del equipo.

Error humano.

Virus informáticos.

Cuestiones legales.

Huelgas de empleados

Figura 3.9 Incendio del data center de una empresa (Disaster Recovery)
(Fuente: http://www.wareprise.com/category/disaster-recovery/)

Ancho de Banda.

El ancho de banda propuesto será de 50Mbps

Equipamiento

El equipo a utilizar será el router Cisco modelo 7201.

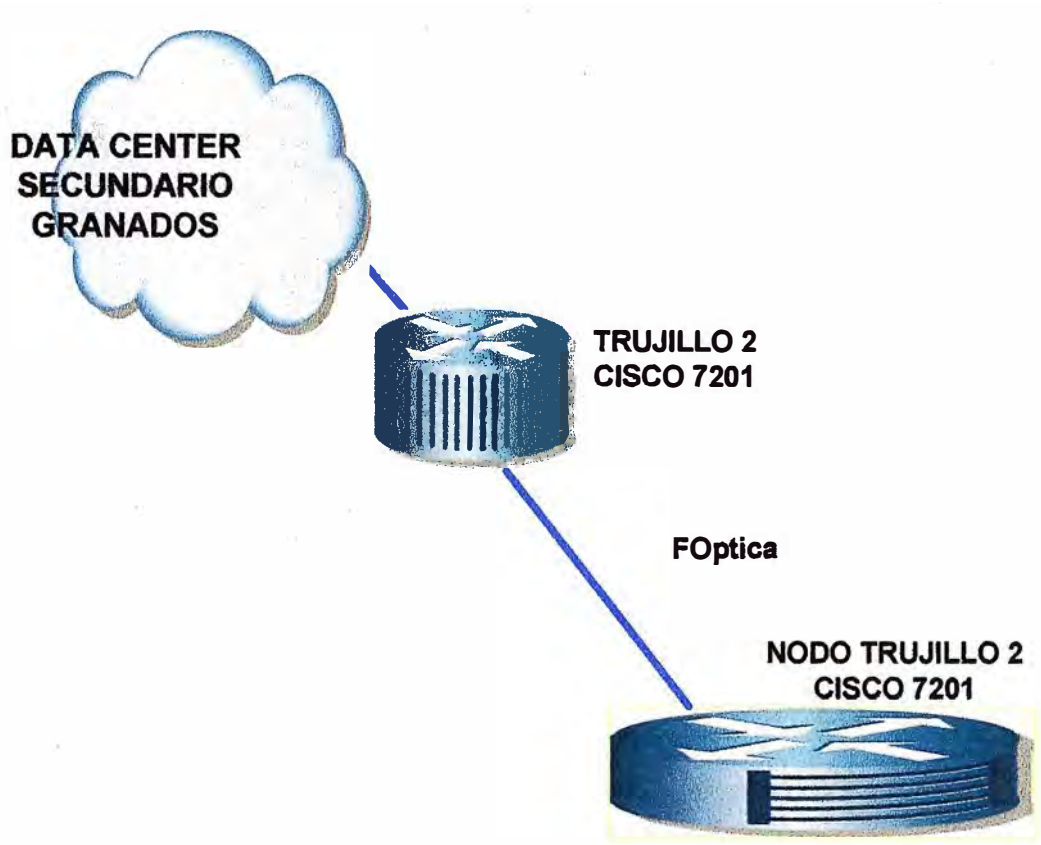

Figura 3.10 Esquema de conexión del data center secundario a la red corporativa (Fuente propia)

3.1.5 Diseño de conexión hacia Internet (enlace principal)

Medio de Transmisión

El acceso a internet (Enlace principal) ser a través de 2 enlaces hacia el proveedor de servicios de internet 1 ISP 1.

Los 2 routers se conectaran a diferente nodo del ISP 1 para garantizar la alta disponibilidad.

El medio de transmisión será por fibra óptica proveído por le ISP 1.

Ancho de Banda

El ancho de banda solicitado al ISP 1 será de 100Mbps.

Equipamiento

El equipo solicitado será el router Cisco modelo 7201. Debido a que se necesita tener interfaces de fibra óptica SFP (Transceiver).

En la figura 3.11 se visualiza el esquema final del diseño de acceso a Internet. También Se implementara HSRP (Hot standby router protocol) en la parte LAN.

Esto permitirá tener redundancia automática entres los dos routers de manera rápida y fiable. Que no exige a los dispositivos ningun tipo de cmabio en sus configuraciones ni ejecutar ningún tipo de software especial. También se observa que las conexiones hacia

el ISP 1 serán a través de la interface G0/1

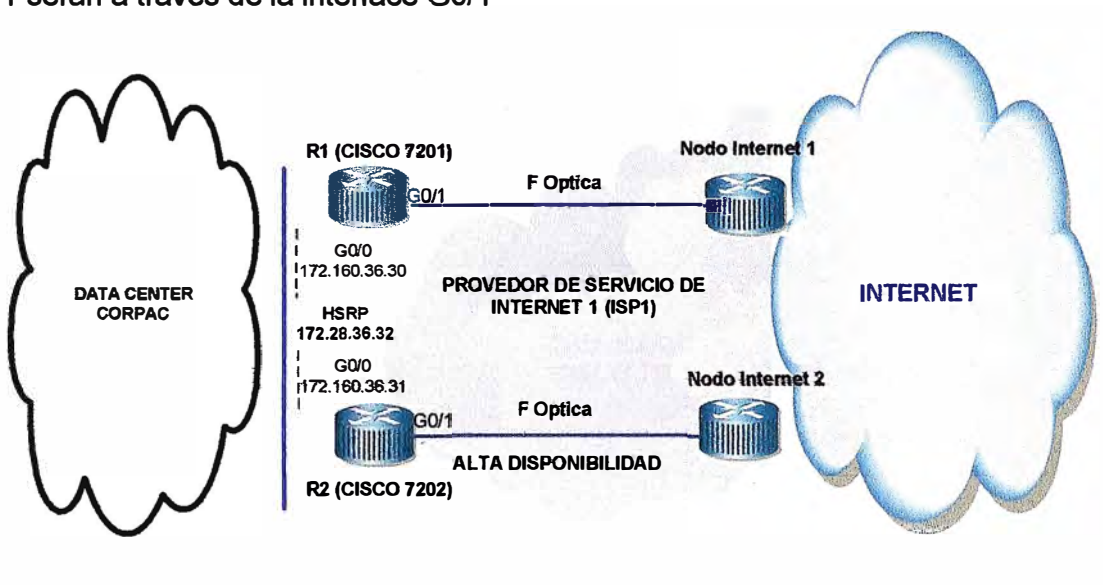

Figura 3.11 Esquema final del diseño de Internet (Enlace Principal)
(Fuente propia)

3.1.6 Diseño de conexión hacia Internet (enlace secundario)

Medio de Transmisión

El acceso a internet (Enlace secundario) será través de 1 enlaces hacia el proveedor de servicios de internet 2.

El medio de transmisión sera por fibra óptica proveído por le ISP 2.el cual terminará en el ODF de la sede denominado Trujillo 1.

Ancho de Banda

El ancho de banda solicitado al ISP 2 será de 50Mbps.

Equipamiento

El equipo solicitado al Proveedor de Servicio de Internet 2 (ISP2) será el router Cisco modelo 7201. Debido a que se necesita tener interfaces con modulo de fibra óptica SFP (Transceiver).

Figura 3.12 SFP (Fuente www.cisco.com)

En la figura 3.13 se observa que la conexión hacia internet enlace secundario será a

través de un router de borde (Trujillo 2) conectado al Nodo Trujillo de la red corporativa.

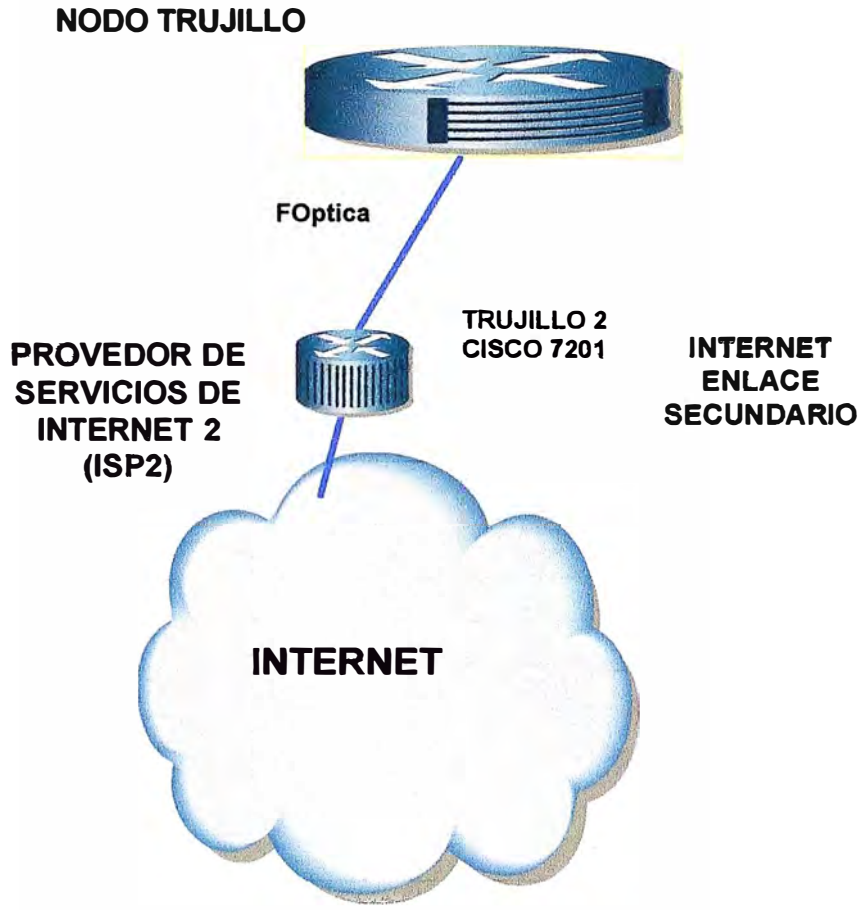

Figura 3.13 Esquema de conexión hacia internet (Enlace secundario) (Fuente Propia)

3.1.7 Diseño de la seguridad perimetral:

Para dimensionamiento del firewall se tiene que tomar en cuenta la cantidad de conexiones concurrentes de los usuarios hacia internet.

Típicamente el 40% de los usuarios acceden a internet concurrentemente.

Cada usuario en promedio tiene de 10 a 15 conexiones simultáneas.

Entonces el total de conexiones concurrentes seria:

$$TCcs = U.Ccs.C. \quad .....(A)$$

Donde:

U= Cantidad total de usuarios.

Ccs = Cantidad de conexiones simultaneas por usuario.

C= Cantidad de sesiones concurrentes de usuarios a internet (%)

Como sabemos TCcs= U.Ccs.C, entonces:

Para nuestro caso, tenemos los siguientes datos:

De la tabla 3.14 se obtiene que cantidad total de usuarios de la empresa.

Después se reemplazara en la formula (A).

Tabla 3.14 Número de usuarios de todas las sedes (Fuente propia)

SEDE	USUARIOS
Lince	80
Begonias	1000
Surco	500
Surquillo	1100
Callao	70
La Victoria	200
La Molina	150
Arequipa	120
Puno	45
Chiclayo	95
Vitarte	170
Piura	95
Total Usuarios	3625

Finalmente:

U= 3 625

Ccss= 15

C= 0,4

Reemplazando en (A):TCcs= U.Ccs.C.= 21 750 (Total de conexiones concurrentes).

Otra manera de dimensionar es por la cantidad de puertos físicos que se requieren.

Según el capitulo 2.4 se requiere contar con un firewall con modulo de fibra óptica.

Adema se necesita escalar en puertos para futuros requerimientos.

Revisando la tabla 3.15 se observa que el equipo que cumple con las necesidades de puertos (interfaces) de GE y SFP es el 1240B.

Por las razones expuestas, se propone el reemplazo del firewall actual por el un nuevo firewall Fortigate 1240B de Fortinet en alta disponibilidad.

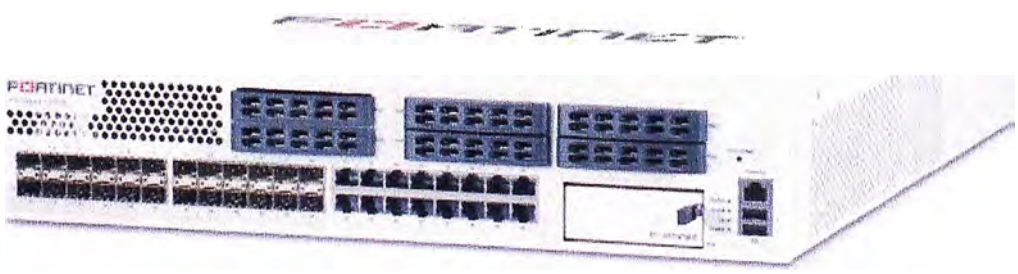

Figura 3.16 Firewall Fortigate 1240B
(Fuente: http://www.avfirewalls.com/FortiGate-1240B.asp)

Tabla 3.15 de Equipos Fortigate (Fuente www.fortinet.com)

ENTERPRISE APPLIANCES

Product	Firewall Throughput (512 Byte)	IPSec VPN Throughput	Concurrent Sessions	Sessions Per Sec	Antivirus Throughput (Proxy)	Intrusion Prevention Throughput	10/100 Interface	GbE Interface	SFP Interface	SFP+ (10GbE) Interface	Modular Expansion Slots	Base System Storage	Hot-Swappable Power Supplies	vDOMs (Max)
FortiGate-3950B (with FMC)	20 Gbps (120 Gbps)	8 Gbps (48 Gbps)	10 M	175 K	1.5 Gbps	(16 Gbps)	0	2 (100)	4 (160)	2 (12)	5 FMC, 0 FSM	0	Yes	Up to 250
FortiGate-3810A (with AMC)	7 Gbps (55 Gbps)	1 Gbps (23 Gbps)	2 M	40 K	500 Mbps	4 Gbps (UDP)	0	8	2	0	2 SW and 2 DW AMC	0	Yes	Up to 250
FortiGate-3600A (with AMC)	6 Gbps (10 Gbps)	800 Mbps (3.8 Gbps)	1.1 M	40 K	400 Mbps	3 Gbps (UDP)	0	8	2	0	1 SW AMC	0	Yes	Up to 250
FortiGate-3140B / 3040B	55 / 40 Gbps	22 / 17 Gbps	4 M	100 K	1.2 Gbps	7 / 6 Gbps	0	2	10	10 / 8	4 FSM	64 GB	Yes	Up to 250
FortiGate-3016B (with AMC)	16 Gbps (20 Gbps)	12 Gbps (15 Gbps)	1.1 M	25K	300 Mbps	2 Gbps (UDP)	0	2	16	0	1 SW AMC	0	Yes	Up to 250
FortiGate-1240B (with AMC)	40 Gbps (44 Gbps)	16 Gbps (18.5 Gbps)	2 M	100 K	900 Mbps	5 Gbps	0	16	24	0	1 SW AMC and 6 FSM	64 GB	Yes	Up to 25
FortiGate-800 / 800F	1 Gbps	200 Mbps	800 K	10 K	150 Mbps	600 Mbps (UDP)	4	4 / 0 (800F)	0 / 4 (800F)	0	No	0	No	10
FortiGate-621B / 621B-DC	16 Gbps	12 Gbps	1 M	25 K	350 Mbps	2.5 Gbps	0	20	0	0	No	64 GB	Opt. Ext. PS	10
FortiGate-620B / 620B-DC (with AMC)	16 Gbps (20 Gbps)	12 Gbps (15 Gbps)	1 M	25 K	350 Mbps	2.5 Gbps	0	20 (24)	0	0	1 SW AMC	0	Opt. Ext. PS	10
FortiGate-310B / 310B-DC FortiGate-311B (with AMC)	8 Gbps (12 Gbps)	6 Gbps (9 Gbps)	600 K	20 K	160 Mbps	800 Mbps	0	10	0	0	1 SW AMC 2 FSM (311B)	1 x 64 GB (311B)	Yes Opt. (310B) Yes (311B)	10
FortiGate-300C	8 Gbps	4.5 Gbps	1 M	35 K	200 Mbps	1.2 Gbps	0	10	0	0	No	32 GB	Opt. Ext. PS	10
FortiGate-200B / 200B-POE	5 Gbps	2.5 Gbps	500 K	15 K	95 Mbps	600 Mbps	8	8	0	0	1 FSM	0	No	10
FortiGate-224B	150 Mbps	70 Mbps	400 K	4 K	30 Mbps	100 Mbps	26	0	0	0	No	0	No	10

Figura 3.17 El dashboard del Firewall Fortigate de Fortinet (Fuente: http://www.fortinet.com)

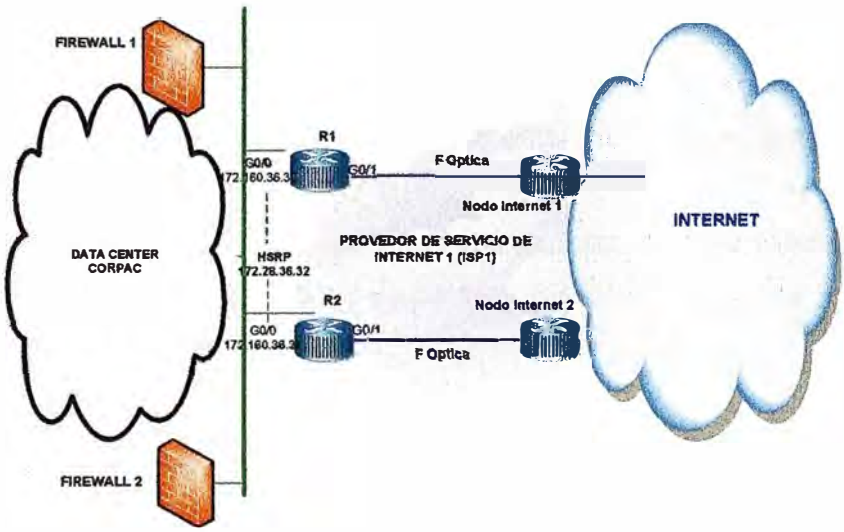

Figura 3.18 Esquema de conexión del Firewall en alta disponibilidad (Fuente propia)

Para temas de virus, se recomienda la compra del software Endepoint Protection (EP) de Symantec.

Endpoint Protection es una solución de seguridad rápida y eficaz, ofrece una defensa avanzada contra todo tipo de ataques tanto para sistemas físicos como virtuales. Gracia a la perfecta integración de las herramientas de seguridad que se necesita en un único agente de alto rendimiento con una única consola de administración, Endpoint Protection ofrece protección líder sin disminuir el rendimiento del equipo. El software SEP, propuesto cubre las necesidades expuestas en el capítulo 2.4

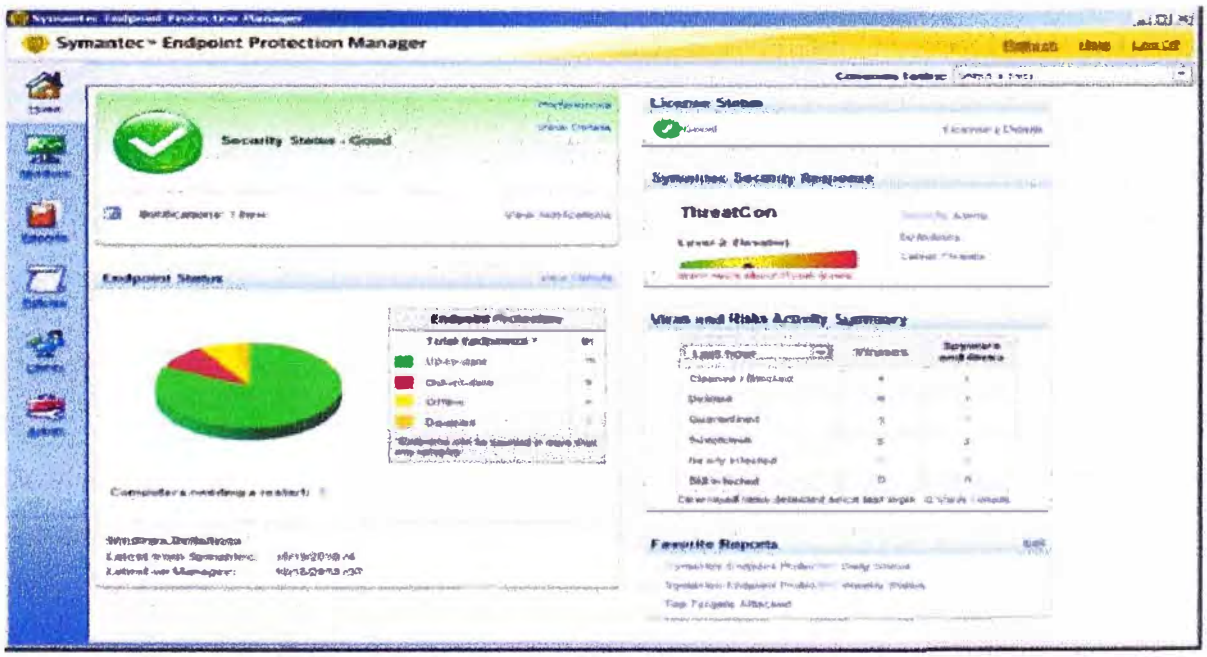

Figura 3.19 EndpointProtection Manager EPM (Consola Antivirus) (Fuente http://www.symantec.com/content/es/mx/enterprise/fact_sheets/Datasheet_SEP-12_1-GA-Version_spanish.PDF)

Se propone la compra del software del Endpoint Protection Manager, por experiencias anteriores de servicio 24x7x365, soporte en Español e Inglés, presentar documentación y literatura de diversos casos y sobre todo que Symantec es líder mundial en soluciones de seguridad, almacenamiento y administración de sistemas que nos permitirá proteger y administrar nuestra información.

Una de la ventajas importantes es que se podrá generar reportes rápidos de riesgos: equipos infectados, resumen de acciones de detección, entre otras muchas opciones mas y actuar de manera proactiva y no reactiva.

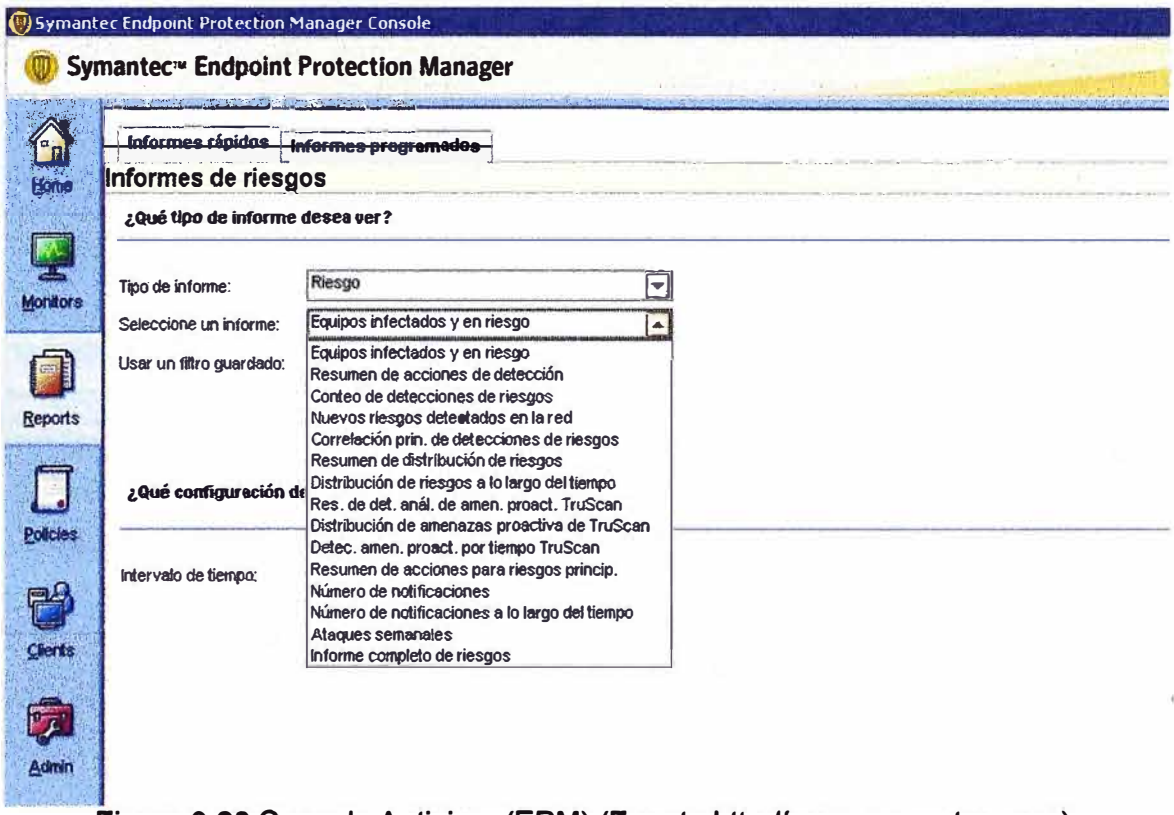

Figura 3.20 Consola Antivirus (EPM) (Fuente http://www.symantec.com)

En la figura 3.20 se observa la pantalla principal del Administrador de Antivirus EPM de Symantec, donde se destaca la facilidad e realizar informes rápidos.

3.2 Software de gestión:

Se recomienda la compra del siguiente software de monitoreo: Orion NPM de Solaris Winds. La adquisición de este software permitirá facilitar procesos rápidos de detección, diagnóstico y resolución de problemas de rendimiento en redes dinámicas. Brindar tableros y vistas en tiempo real que le permiten rastrear visualmente el rendimiento de red de manera inmediata.

Además, con nuestros nuevos mapas de topología de red que se actualizan automáticamente y las funciones de detección automática de redes, puede mantener el

ritmo de evolución de la red sin dificultad. Orion NPM es el producto más fácil de usar y mantener en su clase, lo cual significa que podrá dedicar más tiempo a la administración de redes.

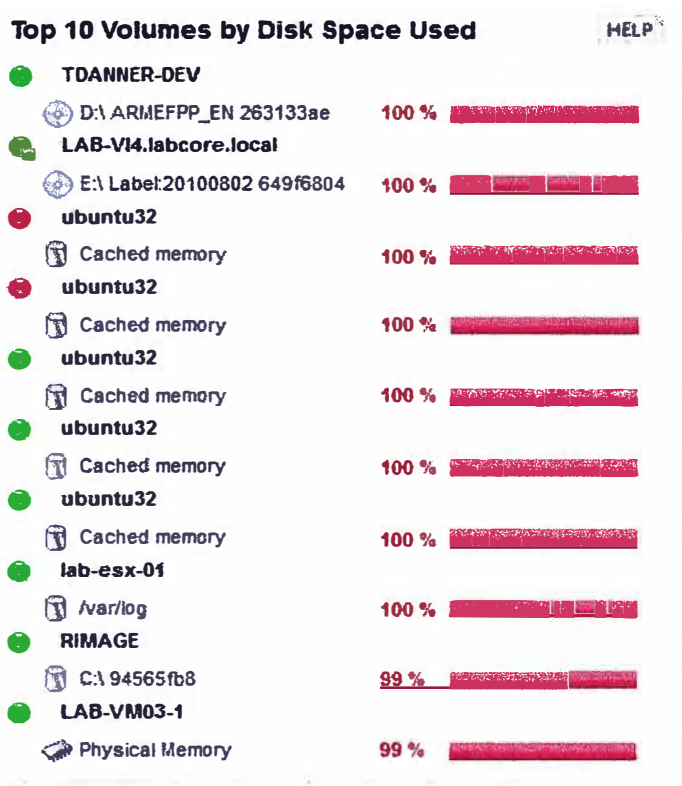

Figura 3.21 Dashboard (Tablero de comandos del Orion NPM) (Fuente:http://oriondemo.solarwinds.com/Orion/Login.aspx?RetumUrl=%2fOrion%2fSummaryView.aspx)

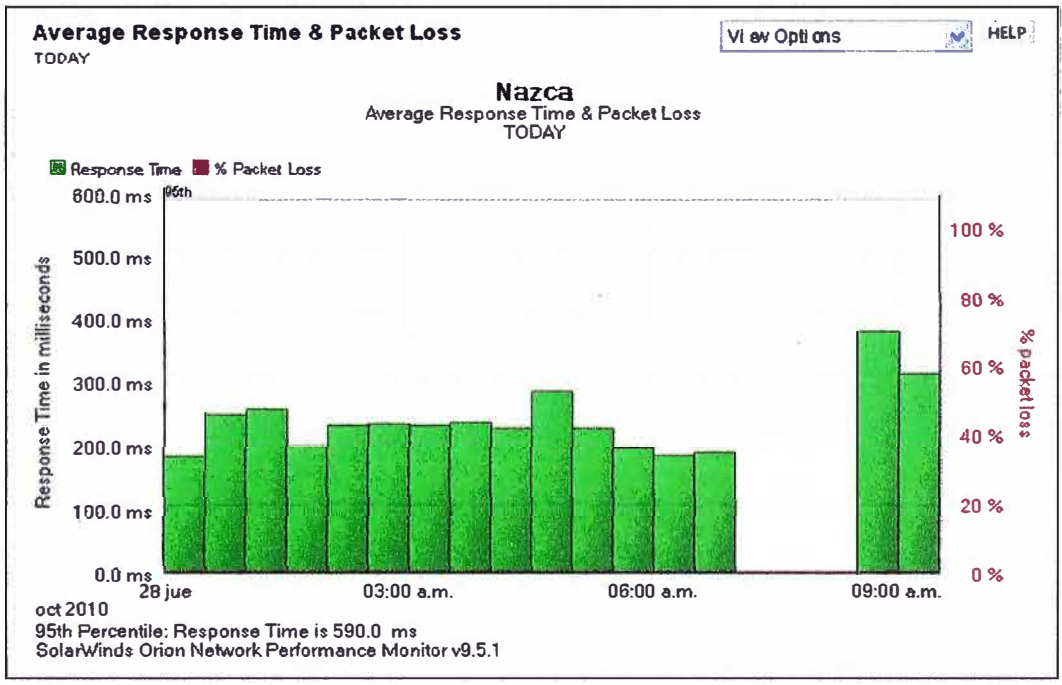

Figura 3.22: Monitoreo del tiempo de respuesta de un equipo de comunicación (Router) (Fuente propia)

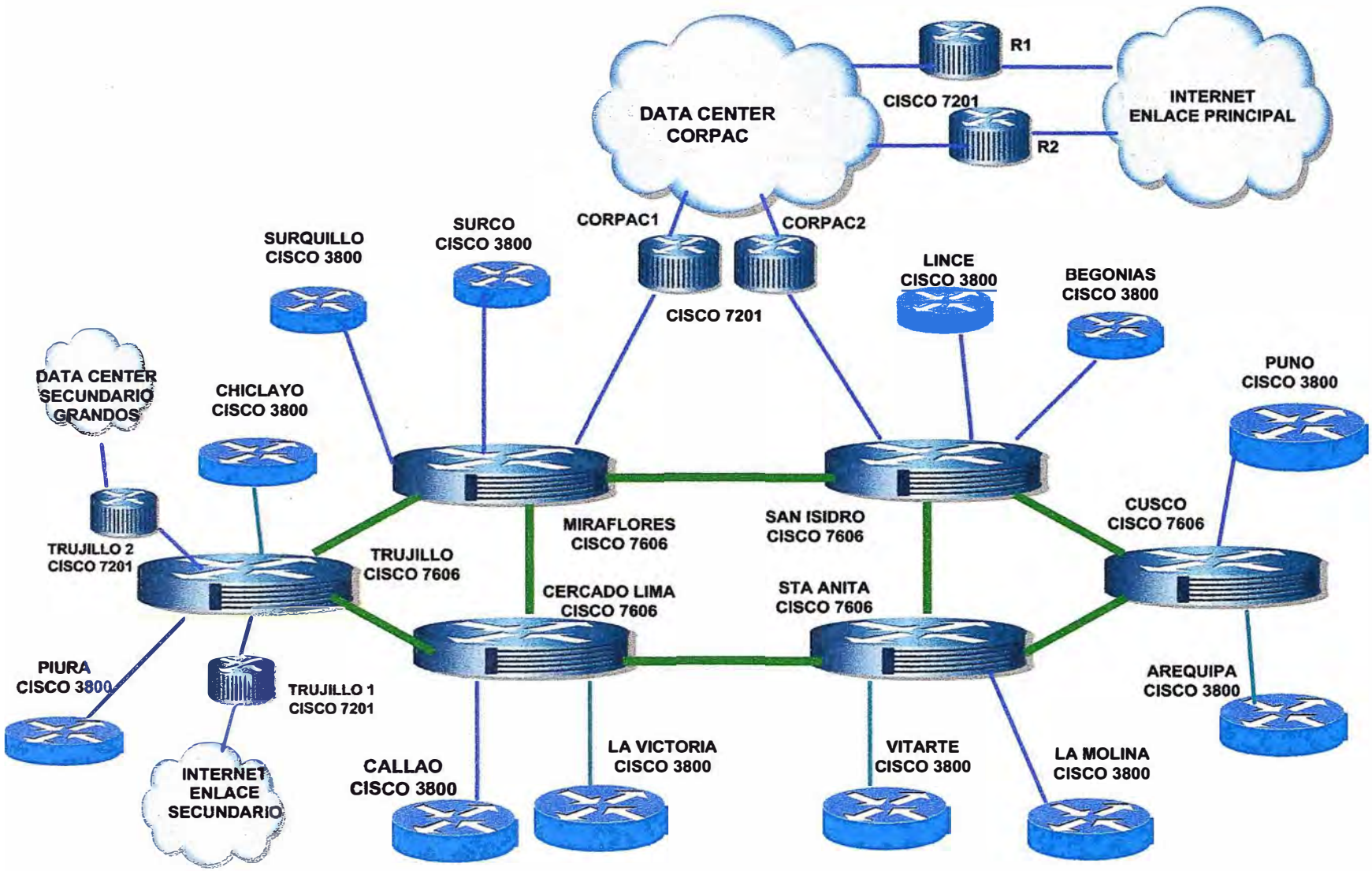

Figura 3.17 Topología del Diseño Completo de la Red Corporativa donde se muestra todos los equipos del diseño (Fuente propia)

CAPÍTULO IV
COSTO DEL PROYECTO:

Costo del equipamiento y software del diseño

En esta parte se detalla el costo de los equipos a utilizar en el diseño de la red propuesta.

Tabla 5.1 Router Cisco 3845

Producto	Descripcion	Cantidad	Precio Unitario	Precio $
CISCO3845-SEC/K9	3845 Security Bundle,Adv Security,64F/256D	12	10412.79	124953.48
PWR-3845-AC/2	Cisco3845 redundant AC power supply	12	500	6000.00
GLC-LH-SM	GE SFP, LC connector LX/LH transceiver	12	520.2	6242.40
			Precio Parcial	137195.88

Tabla 5.2 Router Cisco 7201

Producto	Descripcion	Cantidad	Precio Unitario	Precio $
Cisco 7201	Cisco 7201 router	6	13275.63	79653.78
PWR-7201-AC	Cisco 7201 redundant AC power supply	6	745.5	4473.00
GLC-LH-SM	GE SFP, LC connector LX/LH transceiver	12	520.2	6242.40
			Precio Parcial	90369.18

Tabla 5.3 Router cisco 7606

Producto	Descripcion	Cantidad	Precio Unitario	Precio $
CISCO7606-S	Cisco 7606-S Chassis	6	0	0.00
FAN-MOD-6SHS	High Speed Fan Module for CISCO7606-S Chassis	6	0	0.00
7606S-RSP720CXL-R	Cisco 7606S Chassis,6-slot,Redundant System,2RSP720-3CXL,2PS	6	43964	263784.00
MEM-RSP720-CF512M	C7600 RSP720 Compact Flash memory	6	470.44	2822.64
S764AIK9-12233SRD	Cisco 7600-RSP720 IOS ADVANCED IP SERVICES SSH	6	4727	28362.00
76-ES+BASIC-LIC	ES+ Basic License with IPv6 (no MVPN/6vPE/MPLS VPN)	6	0	0.00
WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	6	7091	42546.00
			Precio Parcial	337514.64

Tabla 5.4 FirewalFortigate 1240B, Software Orion NPM y Software EP de Symantec

Producto	Descripcion	Cantidad	Precio Unitario	Precio $
FORTIGATE 1240B	Firewall de Fortinet	2	13275.63	26551.26
Orion NPM	Software de Solariswinds (100 elementos)	1	3000	3000.00
SEP Symantec	Antivirus Empresarial	3500	45	157500.00
			Precio Parcial	187051.26

Por tanto el costo total ascienda a $752 130,96 dólares americanos. Por lo general por ser una empresa de Telecomunicaciones transnacional siempre se goza de un descuento del 30% Por tanto el costo de implementación del diseño de la nueva red corporativa de Lima y provincias asciende a $ 526 491,672

Este monto será asumido por todos los centros de costos de todos los negocios que conforman la empresa de Telecomunicaciones.

Los costos de diseño e implementación de los enlaces de fibra oscura que unirán los nodos fueron realizados y asumidos por el área de transmisiones.

La instalación y configuración de los equipos routers estará a cargo del proveedor Cisco y del área de operaciones y mantenimiento de la empresa...

La instalación y configuración de los equipos de seguridad: firewalls routers estará a cargo del proveedor Fortinet y del área de operaciones.

La instalación y configuración de los software: Orion NPM (Network Performance Monitor es decir del software de monitoreo del rendimiento de la red) y EPM (Endepoint Protection Manager, es decir de la consola Antivirus, de Symantec estará a cargo del área de plataforma de servidores.

CONCLUSIONES Y OBSERVACIONES:

Conclusiones

1. El diseño y la posterior implementación de la red corporativa permitirá tener una red modema, simple, escalable, disponible, gestionable e interoperable; preparada para soportar las nuevas aplicaciones de las diferentes áreas de negocio, del presente y del futuro.

Es decir esta nueva red será ágil y rápida con mayor y mejor flujo de comunicaciones de voz, datos, permitirá a los empleados de las diferentes áreas de negocio trabajar, realizar transacciones, consultas de las aplicaciones correspondientes sin ninguna dificultad. (De lentitud, de que el sistema se fue, no carga o no abre).

2. Se tendrá acceso a internet en alta disponibilidad y con la ventaja adicional de tener redundancia geográfica. Es decir siempre se contara con acceso a internet de manera segura y rápida.

3. Esta nueva red permitirá asegurar la conectividad operativa en redundancia hacia el data center.

4. El data center principal brindara servicios de hosting, housing, almacenamiento de información y comunicaciones IP a las diferentes unidades de negocios de la empresa y clientes externos sin problemas de saturación y retardo.

5. Se tendrá conectividad al data center secundario, contando con un plan de recuperación ante desastres (Disaster Recovery)..

6. Esta nueva red permitirá la fácil y exitosa expansión de las sedes remotas actuales y futuras a crearse.

7. Se tendrá gestión total de todos los equipos a través del Network Performance Monitor NPM de Orion.

8. Se tendrá una gestión centraliza en temas de antivirus a través de Endepoint Protection Manager de Symantec.

9. Finalmente se tendrá una red más eficiente, dinámica y económica por los costos de mantenimiento preparada para retos del presente y futuro que la Telecomunicaciones imponen, en resumen por eficiencia y costos operativos se ganara con la puesta en marcha del diseño de la red corporativa.

Observaciones

1. Se debe coordinar con el área de transmisiones para realizar trabajos de mantenimiento preventivo, cada 5 meses.
2. La nueva red estará preparada para la implementación progresiva de nuevos servicios
3. Se debe restringir el acceso a los ambientes donde se instalaran los equipos solo el personal de operaciones de red debe tener acceso a estos ambientes.
4. El proceso de implementación estará a cargo del área de Instalaciones en coordinación con los proveedores de los equipos que se compraran.
5. Se sugiere realizar el acta de aceptación cuando el diseño se entregue a la área de instalaciones para su implementación.
6. Ante alguna eventualidad en la instalación del software de Symantec llamar a soporte en línea de Symantec para nuestro caso al número 080051508.
7. En horario de oficina la red será gestionada por personal de operaciones. En horario nocturno y fin de semana el monitoreo estará a cargo del personal de mantenimiento.
8. Se sugiere realizar implementar la gestión fuera de banda de los equipos de core
9. Se recomienda etiquetar correctamente los 2 pares adicionales de fibra óptica monomodo que fueron instalados como reserva en el core o backbone MPLS (Plan de contingencia).
10. Tomar en cuenta que el retraso de esta implementación perjudicara a la empresa pues estará en desventaja comparada con otras empresas de la competencia.

ANEXO A
ESPECIFICACIONES TÉCNICAS

ESPECIFICACIONES ROUTER CISCO 7201.

A continuación se detalla las especificaciones del router Cisco 7201.

Product	Specifications
Processor	1.67-GHz Motorola Freescale 7448 processor
Performance	2,000,000 pps or more
LAN ports	4 Gigabit Ethernet ports
Gigabit Ethernet Optics	SFP • Short wave (SX) • Long wave/long haul (LX/LH) • Extended wavelength (ZX) • RJ-45 copper SFP
DRAM	1 GB default (2 GB maximum)
Compact Flash	64 MB default (256 MB maximum)
Cisco IOS Software Release	12.2(31)SB4, 12.4XD7, and 12.4PI6

ESPECIFICACIONES DE ALIMENTACIÓN ELÉCTRICA:

Dual AC power supply information	Dual AC Power Supply Information
Input power	150W maximum
Typical input power	85W
Input voltage rating	100 to 240 VAC wide input with power factor correction
Input current rating	2A maximum
Typical input current	0.85A at 100 VAC 0.35A at 240 VAC
Input frequency rating	50/60 Hz
Input cable	Use only Cisco agency approved power cords

ESPECIFICACIONES FÍSICAS Y AMBIENTALES

Feature	Specification
Physical Specifications	
Dimensions (H x W x D)	1.75 x 19 x 16.9 in. (4.44 x 48.26 x 42.93 cm)
Weight	Chassis fully configured with a port adapter ~16.5 lb (7.48 kg)
Heat Dissipation	290 Btu/hr at 85W typical input power 512 Btu/hr at 150W maximum input power
Environment Specifications	
Operating Temperature	32 to 104°F (0 to 40°C)
Storage Temperature	-4 to 149°F (-20 to 65°C)
Operating Humidity	10 to 90% non-condensing
Storage Relative Humidity	5 to 95%
Operating Altitude	60 to 2000m

ESPECIFICACIONES DEL FIREWALL FORTIGATE 1240B

De hasta 44 Gbps de rendimiento de firewall protege la red de las últimas amenazas sin afectar la productividad del usuario final

Veinticuatro (24) GbE SFP y doce (12) interfaces GbE permitir que el FortiGate-1240B para escalar fácilmente con el rápido crecimiento de negocios

De seguridad flexible y bahías de expansión de almacenamiento permiten la personalización de los resultados y el enfoque de seguridad para protección contra amenazas y la máxima eficiencia. Amplio conjunto de funciones para proteger las redes.

ESPECIFICACIONES TÉCNICAS ROUTER CISCO 7606

Articulo	Especificación
Ambiental	
Temperatura, ambiente de operación	32 ° F (0 ° C) a 104 ° F (40 ° C)
Temperatura fuera de funcionamiento ambiental y de almacenamiento	-40 ° F (-40 ° C) a 158 ° F (70 ° C)
Humedad (RH), ambiente (sin condensación) que operan	10% a 90%
Humedad (RH), ambiente (sin condensación) no operativos y de almacenamiento	5% a 95%
Altitud, que operan	Del nivel del mar a 10.000 pies (3048m) [1]

Caracteristicas fisicas	
Dimensiones (H x W x D)	12.20 x 17.25 x 21.50 pulgadas (30.98 x 43.81 x 54.61 cm). Chasis requiere 7 RU [2]
Peso	Sólo chasis: 40,8 libras (17,2 kg) Chasis totalmente configurado con el motor de un supervisor de los módulos 5 y 2 AC-entrada de las fuentes de alimentación: 133.2 libras (60.42 kg). FAN-MOD-6SHS, 7.7 lb (3.5 kg), incluye una bandeja de ventiladores.
Fuente de alimentación	2700 W de potencia AC o DC de entrada de alimentación opcional-segunda fuente de alimentación puede ser instalado en el chasis
El flujo de aire	CFM a través del montaje del ventilador del sistema 540
Sonoridad	65,3 a 73,6 dB. Organización Internacional de Normalización (ISO) 7779: posición del acompañante de funcionamiento a una temperatura ambiente de 86 ° F (30 ° C).

CARACTERÍSTICAS DEL SYMANTEC ENDPOINT PROTECTION

Requisitos del sistema Symantec Endpoint Protection para cliente de Windows:

Requisitos mínimos:

Windows® XP, Windows® Vista, Windows® 7, Windows Server® 2003, Windows Server® 2008, Windows® Small Business Server 2003,Windows® Small Business Server 2008, Windows® Essential Business Server 2008 o Windows® Small Business Server 2011.

Procesador de 32 bits: 1-GHz Intel Pentium III o equivalente como mínimo (Intel Pentium 4 o equivalente recomendado).

Procesador de 64 bits: Pentium 4 de 2 GHz o equivalente como mínimo (no se admiten procesadores Itanium).

512 MB de RAM o superior según los requisitos del sistema operativo (se recomienda 1 GB de RAM).

700 MB de espacio en disco

Procesador de 64 bits: 2-GHz Pentium 4 o equivalente como mínimo.

Requisitos del sistema Symantec Endpoint Protection Manager

Requisitos mínimos

Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Small Business Server 2003,

Windows Small Business Server 2008, Windows Essential Business Server 2008 o Windows Small Business Server 2011

Microsoft® SQL Server™ 2000 SP4 o SQL Server 2005 SP2 o SQL Server 2008 (opcional).Procesador de 32 bits: 1-GHz Intel Pentium III o equivalente como mínimo (Intel Pentium 4 o equivalente recomendado).

CARACTERÍSTICAS DEL ORION NPM

Licencia de Orion Network Performance Monitor

Orion NPM puede recoger datos e información detallada de cualquiera de sus dispositivos con SNMP de la versión 3 o anterior, incluyendo routers, conmutadores, cortafuegos y servidores. Orion NPM tiene licencia de la mayor cantidad de los tres siguientes tipos de objetos de red supervisados:

Nodos: Los nodos incluyen dispositivos enteros, por ejemplo, routers, conmutadores, servidores virtuales y físicos, puntos de acceso y módems.

Interfaces

Las interfaces incluyen puertos de conmutador, interfaces físicas, interfaces virtuales, subinterfaces, VLAN y cualquier otro punto único de tráfico de red.

Volúmenes

Los volúmenes son equivalentes a las unidades lógicas que supervisa.

La siguiente lista le muestra los diferentes tipos de licencias Orion disponibles:

- Hasta 100 objetos (SL100)
- Hasta 250 objetos (SL250)
- Hasta 500 objetos (SL500)
- Hasta 2000 objetos (SL2000)
- Objetos ilimitados (SLX)

El tamaño de la base de datos aumenta con la adición de objetos gestionados. Dependiendo del número de objetos y de la cantidad de tráfico que fluya a través de los objetos que están en su red, la gestión exitosa de más de 8.000 objetos puede requerir de la adición de más motores de sondeo. Para obtener más información sobre los motores de sondeo, consulte "Managing Orion NPM Polling Engines" en SolarWinds Orion Network Performance Monitor Administrator Guide.

Requisitos

SolarWinds recomienda la instalación de Orion NPM en su propio servidor, con la base de datos de Orion alojado independientemente, en su propio SQL Server.

Las tablas a continuación enumeran los requisitos mínimos para su servidor Orion, para Diferentes licencias

Hardware	SL100, SL250 o SL500	SL2000	SLX
Velocidad de CPU	2 GHz	2,4GHz	3 GHz
Espacio de disco duro	2 GHz	5 GHz	20 GHz
Memoria	3GB	4GB	4GB

Nota: se recomienda un disco RAID 1 para el sistema operativo del servidor, la instalación de Orion NPM y los archivos tempdb. El instalador de Orion necesita 1 GB de espacio en el disco donde se almacenan las variables temporales del sistema o usuario de Windows. Según los estándares de Windows, puede que sea necesario instalar algunos archivos comunes en el mismo disco del sistema operativo del servidor.

Puertos de Aplicaciones:

161/SNMP y 443/SNMP. Los servidores VMware ESX/ESXi son sondeados en 443.

17777/TCP abierto para el tráfico del módulo Orion

17778/ HTTPS abierto para acceder al API de servicio de información de SolarWinds

Continuación de los requisitos mínimos.

En la siguiente tabla se detalla las características que deb tenet el sistema operativo a usar.

Software	Requisitos
Sistema operativo	Windows Server 2003 o 2008, incluido R2, con IIS en modo de 32 bits. El IIS debe estar instalado. SolarWinds recomienda que los administradores de Orion NPM dispongan de privilegios de administrador local para garantizar la completa funcionalidad de las herramientas locales de Orion NPM. Las cuentas limitadas para uso de la consola web no requieren privilegios de administrador. Nota: SolarWinds permite evaluaciones pero no admite las instalaciones de Orion NPM en Windows XP, Windows Vista SP2 o Windows 7 en entornos de producción.
Servidor web	Microsoft IIS, versión 6.0 y superior, en modo de 32 bits. Las especificaciones de DNS requieren que los nombres de anfitrión estén formados por caracteres alfanuméricos (A-Z, 0-9), el signo de restar (-) y puntos (.). No se permiten caracteres de guión bajo (_). Para obtener más información, consulte *RFC 952.* Nota: SolarWinds no recomienda ni admite la instalación de Orion NPM en el mismo servidor ni el uso del mismo servidor de base de datos que un servidor de Blackberry Research in Motion (RIM).
.NET Framework	Versión 3.5. Se recomienda .NET Framework 3.5 SP1.
SNMP Trap Services	Componente de herramientas de supervisión y administración del sistema operativo de Windows.
Web Console Browser	Microsoft Internet Explorer versión 6 o superior con secuencia de comandos Firefox 3.0 o superior.

ESPECIFICACIONES TÉCNICAS ROUTER CISCO 3845

A continuación se muestra las especificaciones físicas.

Cisco 3800 Series Características	Cisco 3825/3825-NOVPN	Cisco 3845/3845-NOVPN
Especificaciones físicas		
Dimensiones (H x W x D)	• 3,5 x 17,1 x 14,7 pulgadas • 2 unidades de rack (2U)	• 5,25 x 17,25 x 16 pulgadas • 3RU
Peso (mínimo)	£ 23	£ 35
Para montaje en rack	Sí, 19 - y 23-in. opciones	Sí, 19 - y 23-in. opciones
Para montaje en pared	No	No

Especificaciones eléctricas:

Voltaje de entrada CA	100-240 VAC, autoajustable	100-240 VAC, autoajustable
Frecuencia de entrada CA	47-63 Hz	47-63 Hz
Corriente de entrada	• 3A (110) • 2A (230) • Inicio de la corriente máxima 50A (un ciclo)	• 4A (110) • 2A (230) • Inicio de la corriente máxima 50A (un ciclo)
Entrada de CA IP actual	• 8A (110V) • 4A (230) • Inicio de la corriente máxima 50A (un ciclo)	• 8A (110V) • 4A (230) • Inicio de la corriente máxima 50A (un ciclo)
DC voltaje de entrada	24-60 VDC, rango automático positivo o negativo	24-60 VDC, rango automático positivo o negativo
Corriente de entrada	• 12A (24V) • 5A (60V) • 50 A de corriente de arranque <10 ms	• 18A (24V) • 7A (60V) • 50 A de corriente de arranque <10 ms

Obs: La columna de la derecha corresponde al router Cisco 3845 para todas las tablas.

En la página siguiente se continúa con la descripción de los detalles eléctricos.

Finalmente también se detalla las especificaciones ambientales.

Salida	• AC o DC: • 210W para el sistema • Fuente de alimentación AC IP: • 210W para el sistema • 360W para los teléfonos IP (-48V)	• AC o DC: • 300W para el sistema • Fuente de alimentación AC IP: • 300W para el sistema • 360W para los teléfonos IP (-48V)
Fuente de alimentación redundante (RPS)	Externo solamente (Cisco RPS 675 Redundant Power System)	Interna AC, AC IP, o RPS DC
Recomendado RPS unidad	Cisco RPS 2300 (recomendado) y RPS 675 Redundant Power System	-
Disipación de energía		
Disipación de potencia típica (sin módulos)	52 W (177 BTU / hr)	79W (269 BTU / hr)
CA sin soporte telefónico IP	300 W (1025 BTU / hr)	435W (1485 BTU / hr)
AC con soporte telefónico IP: El sistema sólo	370 W (1262 BTU / hr)	555W (1890 BTU / hr)
AC con soporte telefónico IP: teléfonos IP	360 W (1128 BTU / hr)	360 W (1128 BTU / hr)

Especificaciones Ambientales:

Especificaciones ambientales		
Temperatura de funcionamiento	32 a 104 ° F (0 a 40 ° C)	32 a 104 ° F (0 a 40 ° C)
Temperatura sin funcionamiento	-40 A 158 ° F (-40 a 70 ° C)	-40 A 158 ° F (-40 a 70 ° C)
Humedad relativa (sin condensación)	5-85% sin condensación	5-85% sin condensación
Temperatura máxima de funcionamiento en la altura	40 ° C a nivel del mar 40 ° C a 6.000 pies (1.800 m) 30 ° C a 13.000 pies (4.000 m) 27.2 ° C a 15.000 pies (4.600 m) Nota: Reducir la capacidad en 1,4 ° C por cada 1.000 pies por encima de 6.000 pies	40 ° C a nivel del mar 40 ° C a 6.000 pies (1.800 m) 30 ° C a 13.000 pies (4.000 m) 27.2 ° C a 15.000 pies (4.600 m) Nota: Reducir la capacidad en 1,4 ° C por cada 1.000 pies por encima de 6.000 pies
Nivel de ruido (como mínimo)	50 dBA máximo, 53 dBa	56 dBA, 58 dBa máximo

BIBLIOGRAFIA

[1] Cisco Net Academy [en línea] [fecha de acceso 10 de octubre de 2011]; URL zdisponible en:cisco.netacad.net/cnams/home/StudentClass.jsp

[2] Garcia Tomas, Jesús; Raya Cabrera, José Luís; Raya, Víctor Rodrigo "Alta Velocidad y Calidad de Servicio en Redes IP"; Alfaomega; 2002; p.519

[3] BCE Nexxia A Bell Canada Company MC[en línea] [fecha de acceso 10 de octubre de 2011]; URL disponible en: http://www.bcenexxia.com

[4] E. C. Rosen and Y. Rekhter, "BGP/MPLS IP VPNs", draft-ietf-l3vpnrfc2547bis-01.txt, Septiembre 2003

[5] Pepelnjak, Iván; Guichard, Jim. Arquitectura MPLS y VPN.

[6] Tic Tac TIC (Tecnoloxías Información e Comunicacións) Redes MPLS [en línea] [fecha de acceso 15 de octubre de 2011]; URL disponible en: http://tic-tac.teleco.uvigo.es/profiles/blogs/las-redes-mpls-son-la-solucion

[7] McGraw-Hill Profesional, "Guía Completa de Protocolos de Telecomunicaciones", España, 2002.

[8] Ernesto Ariganello, Enrique Barrientos Sevilla, "Redes Cisco CCNP a Fondo",Alfaomega, Mexico 2010.

[9] Ernesto Ariganello,"Técnicas de configuración de RouterS CISCO" ,Ra-Ma, España 2008

[10] Antonio Gallego de Torres, "Router CISCO", Añaya Multimedia,
España 2010

[11] Cisco Products & Services [en línea] [fecha de acceso 15 de octubre de 2011]; URL disponible en: www.cisco.com/en/US/products/index.html

[12] Fortinet Product [en línea] [fecha de acceso 15 de octubre de 2011]; URL disponible en: www.fortinet.com

[13] Orion Performance Manager (NPM) [en línea] [fecha de acceso 15 de octubre de 2011]; URL disponible en: www.solarwinds.com

[14] Symantec.Confidence in a connected world. [en línea] [fecha de acceso 15 de octubre de 2011]; URL disponible en: www.symantec.com/business/endpoint-protection