UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SISTEMA DISTRIBUIDO DE ALMACENAMIENTO LOCAL DE CONTENIDOS WEB

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

JHONN NEIL SEBASTIÁN AREQUIPEÑO LA ROSA SÁNCHEZ

PROMOCIÓN
2002-II

LIMA – PERÚ
2006

SISTEMA DISTRIBUIDO DE ALMACENAMIENTO LOCAL DE CONTENIDOS WEB

Dedico este trabajo a:

Mis padres, por el apoyo brindado,

A Mis Hermanos, por la oportunidad prestada,

A mis abuelos por el camino trazado

Y a mis maestros por la esperanza aun puesta.

SUMARIO

Actualmente los usuarios del Servicio de Internet están recibiendo un servicio diferenciado gracias el amplio desarrollo de las redes que se ha venido realizando lo cual esta ayudando a contar con un servicio mas rápido y eficiente en los tiempos de acceso a los contenidos WEB, permitiendo así que desaparezca casi en su totalidad los cuellos de botella que antes existía en la salida a la red Internacional para acceder a los servidores WEB que se encuentran alrededor del mundo. De esta manera, este informe pretende mostrar sintéticamente todo el proceso que implicó el diseño e implementación del proyecto "Sistema de Caché Distribuido en la Red IP/MPLS" de Telefónica Empresas, que contribuyó enormemente a brindar un mejor servicio de acceso a Internet a sus clientes, lo cuales siempre han esperado contar con tiempos mínimos de acceso a sus contenidos WEB.

Este trabajo muestra en el capitulo I el análisis del problema. El capitulo II brinda todas los alcances teóricos - técnicos que nos fue necesario detallar para poder implementar tal solución, por lo que cada concepto mencionado se ha tratado de mostrar con el lenguaje mas sencillo posible. El capitulo III desarrolla a su vez el diseño e implementación de la solución junto con los recursos humanos y equipos que nos fue necesario contar. En el capítulo IV se muestran los resultados obtenidos de ahorro y consumo de ancho de banda los cuales comprueban que efectivamente se han alcanzado los objetivos inicialmente planteados. Finalizamos este informe colocando las conclusiones derivadas de la implementación de este proyecto.

INDICE

INTRODUCCION

EL sistema implementado se basa principalmente en una red de almacenamiento que combina equipos repositorios de contenidos como son los modelos CACHEFLOWS de la marca BLUECOAT y conmutadores de contenidos inteligentes como son los modelos CONTENT SERVICES SWITCH de la marca CISCO, los cuales son integrados a la Red IP/MPLS de 6 nodos principales y a Enrutadores puerta de salida a Internet (Red Internacional). Esta solución acelerará el reparto de contenidos y optimizará el uso del ancho de banda de la Red Internacional para un Proveedor de Servicios de Internet a la cual de ahora en adelante la reconoceremos por sus siglas PSI. La red de almacenamiento cuyo elemento principal es la Red Caché la cual se anexa a la Red IP/MPLS tiene por función el grabado y almacenado de información, donde las copias de los contenidos recientemente visitados son almacenados temporalmente sobre un conjunto de repositorios; el contenido copiado esta disponible luego para ser usado por el siguiente usuario que requiere el mismo contenido. El reparto de la información se logra a través de un conmutador de contenidos que validará que efectivamente el contenido se encuentre, y que además balanceará la carga que viene de los usuarios a los servidores caches. Cabe mencionar que tanto los conmutadores de contenidos como los servidores caches se encuentran redundados para brindar alta disponibilidad del servicio.

La integración con la red IP/MPLS se debe a que la "Red Caché" esta diseñada para funcionar interdependientemente con el Núcleo de red de un proveedor de servicios de Internet, en la que cada "Red Caché" es albergada en los nodos principales de este Núcleo de Red lo cual garantiza Redundancia y Confiabilidad en el Servicio de Caché de Contenidos. El tránsito recorrido de los contenidos almacenados va desde las Redes Caché a los usuarios finales a través de los Enrutadores de borde que manejan exclusivamente Internet, esta comunicación entre los nodos que albergan las redes caché y los Enrutadores de borde se dan a través de protocolos de enrutamiento, por lo que se tiene en todo momento una red permanentemente actualizada y por ende comunicada de un nodo a otro. Como sabemos la Red IP/MPLS, se caracteriza principalmente por su alta capacidad de procesamiento y por la diferenciación que realiza de los servicios que transitan por ella, así mismo esta red brinda una alta disponibilidad operativa por lo que si

fallara uno de los nodos que componen la red el servicio no se vería suspendido pues sería asumido por los otros nodos restantes operativos.

Aprovechando esta integración de la Red IP/MPLS con las Redes Caché es que podemos tener tiempos de respuesta bajísimos, disminución de la congestión de Internet, reducción del uso del ancho de banda de la Red Internacional y por ende reducción de costes del servicio de Internet para los usuarios y empresas, disminución también de los riesgos informáticos, y así mismo optimización en los recursos de la Red; observando esto, es que Telefónica Empresas S.A.A. decidió en Octubre del 2002 la implementación del Sistema de Almacenamiento Distribuido en su Red IP/MPLS, tal decisión se baso en el hecho de que la implementación significaría de un beneficio adicional de valor añadido en el servicio de acceso a Internet para los clientes que tenían contratado el servicio con esta PSI, así mismo esto significaría para la empresa una reducción del 20% del consumo del ancho de banda en sus enlaces Internacionales. Vistas estas ventajas se fijo el mes de Junio del año 2003 como fecha término de la implementación, pero debido a retrasos en la inversión, la primera parte del proyecto se concluyó en el mes de Setiembre del mismo año consistiendo primeramente de la puesta en producción de las Redes Caché de los nodos de San Isidro y Washington de la ciudad de Lima; la segunda Fase del Proyecto se concluyo en Noviembre del mismo año abarcando no solo los nodos de Miraflores y Monterrico sino también los de Provincia como son Arequipa y Trujillo. Cabe precisar que los nodos de Monterrico y Miraflores no contienen servidores caché pero si conmutadores de contenidos que se encargarán de redireccionar los contenidos a las demás redes caché los cuales si tienen servidores de almacenamiento.

Como parte fundamental de la consolidación del proyecto se contó con la presencia y asistencia de las empresas proveedoras de equipos como es el caso de las empresas CISCO y de INFODATA, la primera que suministro los equipos Conmutadores de Contenidos y la segunda (Representante Comercial de la compañía BLUECOAT) como proveedora de los equipos CACHE, las 2 compañías brindaron junto a sus matrices en el exterior de la suficiente información (capacitaciones, material escrito, consultoría, etc) que permitió estar capacitados durante todo el proceso que significo la implementación del proyecto. Así mismo es necesario mencionar que este desarrollo no hubiese sido factible si no hubiese tenido las bases Técnico-Científico que respaldan estos tipos de proyectos, conceptos como protocolos de enrutamiento, direccionamiento IP, lista de accesos, calidad de servicio, diferenciación de servicios, cabeceras, rutas cacheables que son usados constantemente en este informe son a su vez fundamentados en

conceptos de transmisión de paquetes, de corrección de errores, algoritmos de almacenamiento, IOS propietarios, etc, que han permitido contar con el soporte necesario para poder instalar estos diseños.

CAPITULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del Problema.- El principal problema que nos ha llevado a diseñar e implementar este proyecto ha sido el de la disminución en la calidad del servicio de Internet debido a que el tiempo de acceso a ciertos contenidos era demasiadamente alto, y esto en gran parte por la lejana ubicación geográfica de los servidores web internacionales y por el notorio congestionamiento de las salidas a las red internacional al acceder a los contenidos internacionales (Ubicadas en servidores Internacionales), por lo que se registraba un alto consumo de ancho de banda del tráfico internacional (Tráfico que es administrado por la empresa TIWS) para el servicio de Internet que continuamente usan sus clientes a través de sus servicios Unired, Cabinet e Infointernet.

1.2 Antecedentes del Problema.- Desde la aparición de Internet en los años 90 el crecimiento de las redes de transmisión de paquetes se ha dado de manera explosiva, hasta que a principios del año 2000 (Marzo - Abril) la burbuja tecnológica se contrajo debido a la llamada a la cautela de los analistas que presentaron informes que reflejaban la mala rentabilidad de las empresas IT a corto y medio plazo, y es por eso que las inversiones en TI pasan de ser inversiones de moda a inversiones inteligentes capaces de contribuir concretamente a los objetivos estratégicos de las Empresas de los diferentes mercados, visto esto es que las Empresas empiezan a adquirir los productos TI necesarios para poder seguir compitiendo en sus respectivos segmentos económicos. Así mismo debido a ese crecimiento exponencial que hubo en esa década hizo que las empresas proveedoras de Internet no tuvieran presente la planificación necesaria que considerará que en algún momento Internet pasaría de ser un servicio Estrella a un servicio diferenciado por el tiempo de acceso a una página web, en pocas palabras Internet creció y siguió creciendo hasta que las Empresas proveedoras del servicio se hicieron la pregunta de que si tal crecimiento representaba en realidad un servicio eficiente y esto por la sencilla razón de que el acceso a Internet ya empezaba a mostrarse visiblemente con signos de retardo y congestión.

1.3 Objetivos del Trabajo.-

Los objetivos a alcanzar gracias a la implantación del proyecto son las siguientes:

- Disminución de los tiempos de acceso a los contendidos web de los clientes Unired, Cabinet e InfoInternet.
- Reducción del consumo de ancho de banda de los enlace internacionales en un 20% aproximadamente.

1.4 Evaluación del Problema.- La forma de acceder a Internet (Contenidos Web Internacionales) de los usuarios de Telefónica Empresas se da a través de los enlaces de la Red Internacional de Telefónica que es administrada por la Empresa TWIS cuya puerta de acceso en nuestro país es el Compuerta de Lurín la cual se conecta a 2 nodos siendo el principal el nodo de MIAMI (ver figura 1) que es la puerta de acceso Internacional a Internet y que es considerado el NAP(Punto de Acceso a la Red) de la Américas, pues esta se encarga de conectarse con los diferentes nodos posicionadas alrededor del mundo y es debido a esta concentración de enlaces que se presenta un punto de congestión de Internet, aparte de la distancia misma los cuales causan un retardo en el acceso de los contenidos web.

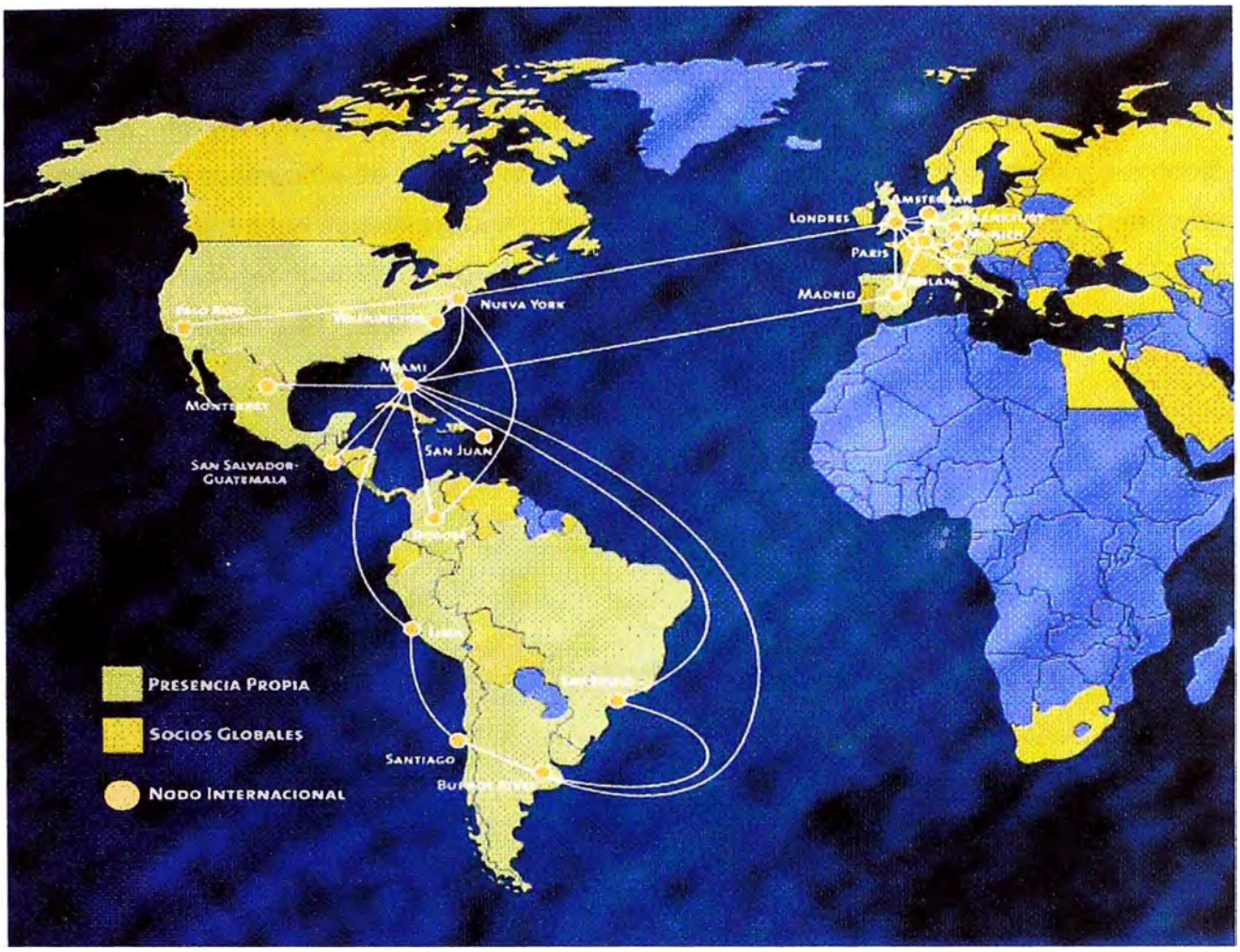


Figura 1.1 Mapa de la Red Internacional de Telefónica

Es necesario también mencionar que Telefónica Empresas a finales del año 2002 tenía 2 conexiones STM-1 (310Mbps) que se traducía en 2 enlaces que venían directamente del Núcleo de Red IP/MPLS (ver figura 1.2) los cuales están conectados a la RED Internacional vía Enrutadores de Entrada (Enrutadores TG) que son usados para acceder a Internet. Este tráfico que se ha venido usando, ha sido en manera de capacidad suficiente, pero con la consideración siempre de la existencia de los retardos considerables, que es causado por el tiempo que tarda en recorrer la distancia geográfica hacia los servidores web internacionales y por la congestión que sucede en los nodos tanto de Lurín como de Miami por ser puntos altos de concentración a nivel Nacional e Internacional respectivamente. Dicho esto es que podemos concluir que el problema que se tiene es de retardo al acceso de los contenidos Web.

La topología que tiene la red IP/MPLS mostrada en la Figura 2 muestra la arquitectura pasada de conexión a la Red Internacional, en la que se utiliza 2 enrutadores de acceso como son los Enrutadores de Entrada los cuales a su vez están conectados bajo redundancia a los Enrutadores LSR (Enrutadores P) que son 2 de los 4 elementos

centrales (Nodos de San Isidro y Washington) de la Red IP/MPLS los cuales concentran todo el tráfico internacional saliente y entrante de Internet de los clientes de Telefónica Empresas, de esta manera puede observarse en la topología de Red que hay una disposición de elementos de Red de alta capacidad de procesamiento de tráfico así como de una gran capacidad instalada para brindar el servicio de Internet, pues los Enrutadores LSR son los enrutadores que se encargan de conmutar los diferentes tipos de trafico de acuerdo a la etiqueta con la cual son enviados desde los Enrutadores LER o Enrutadores PE.

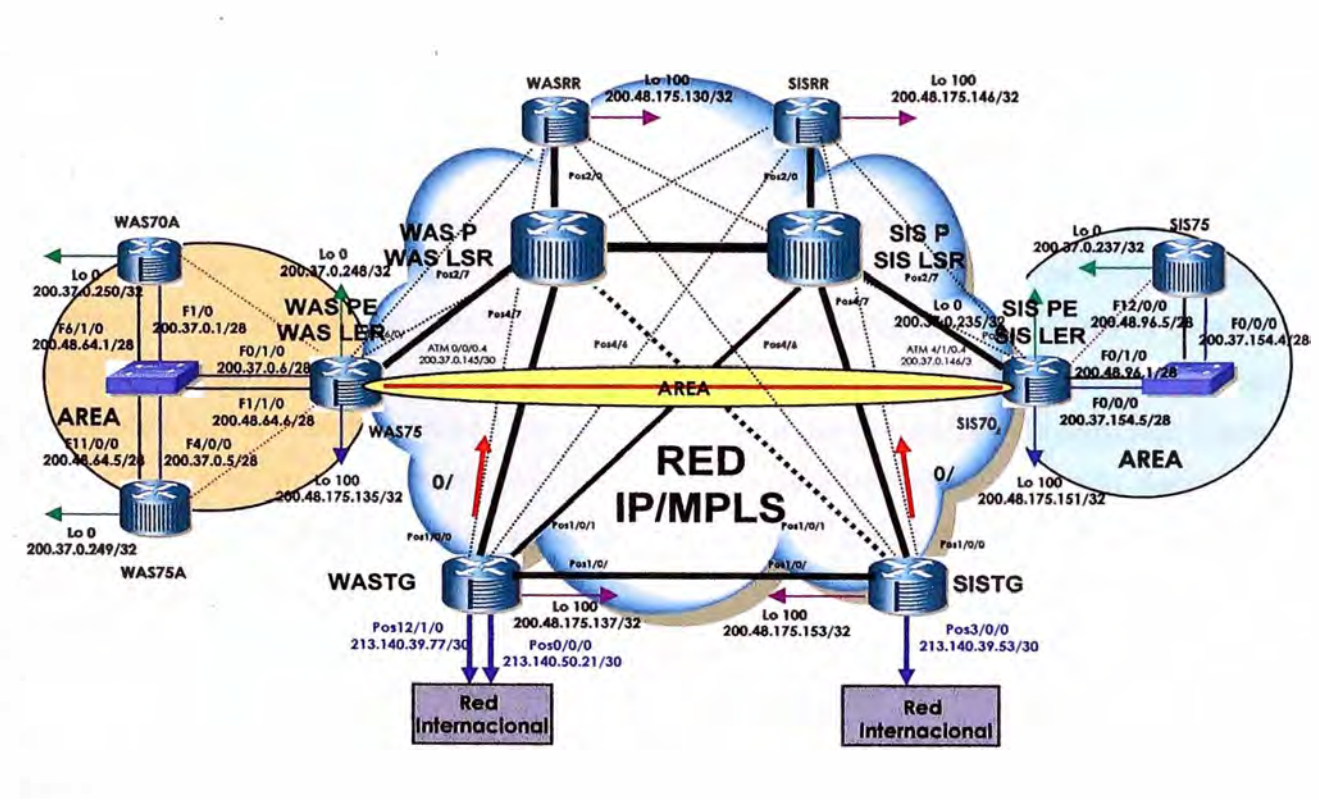


Figura 1.2 Situación Anterior del Acceso a Internet en la Red IP/MPLS de Telefónica Empresas

La arquitectura mas común que se usaba antes para acceder a Internet hacia páginas internacionales es la que se muestra en la figura 1.3 esta solución es la topología base que se uso desde el principio, pero que ha venido cambiando sobre todos en los medios y protocolos de transmisión y de comunicación respectivamente en medida que los cambios tecnológicos se han suscitado.

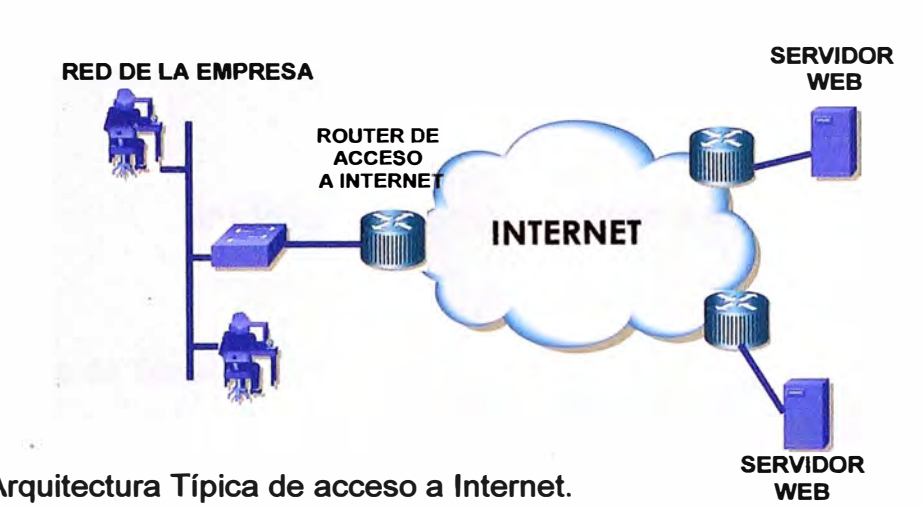


Figura 1.3 Arquitectura Típica de acceso a Internet.

1.5 Limitaciones del Trabajo.- Las principales limitaciones que se han tenido para la implementación de este proyecto, han sido principalmente de orden económico y esto debido a que este proyecto exigía una alto nivel de inversión el cual no estuvo programado dentro de los tiempos previstos lo cual origino un retraso de la puesta en producción del servicio, causando que el proyecto fuese entregado en 2 partes (Setiembre fue el mes de entrega de la primera parte del proyecto y la segunda Fase del Proyecto se concluyo en Noviembre). Exceptuando esta limitación se puede decir que los demás recursos tanto materiales y humanos estuvieron presentes a tiempo y en buenas condiciones.

1.6 Síntesis del Trabajo.- Una vez ubicado el problema de retardo de acceso a los contenidos web debido a la disposición de la red Internacional y de la distancia de los servidores web, la implementación comenzó con la selección del diseño que se ajustaba mejor para la solución del tema del retardo, una vez escogido este diseño se procedió a desarrollar la planificación respectiva, así mismo se programó la capacitación necesaria del personal involucrado y también se programó las actividades propias de configuración e instalación del equipamiento, así como del acondicionamiento del ambiente donde finalmente fueron alojado los servidores.

CAPITULO II
MARCO TEORICO CONCEPTUAL

2.1 Definiciones de Términos

2.1.1 QoS: Calidad de Servicio

Es una medida de rendimiento para un sistema de transmisión que refleja la calidad de la transmisión y la disponibilidad del servicio. El primer objetivo que satisface el QoS es el Ancho de Banda Dedicado, el desfasaje y latencia controlada; entendamos por desfasaje como la variación de la señal de su posición referencial de tiempo y por latencia como el retardo de tiempo entre que la trama de datos es recibida y reenviada. El QoS se basa en un programa desarrollado por los proveedores de equipos el cual permite a redes complejas poder controlar y soportar servicios de una variedad de aplicaciones de red y diferentes tipos de tráfico, este programa presenta también los siguientes beneficios:

- El Control de Recursos de ancho de banda, equipos, facilidades de área de cobertura, etc., que se están usando, que permitirá por ejemplo limitar el ancho de banda consumido sobre el enlace de un nodo central de una transferencia FTP o brindar la prioridad de acceso a una base de datos importante.
- Uso más eficiente de los recursos de red, mediante herramientas de administración y de contabilidad, que son herramientas que permiten conocer que una determinada red esta siendo usada para servir al más importante tráfico del negocio del cliente.
- Servicios Flexibles, en el cual utilizando los instrumentos de control y monitoreo proporcionado por QoS permite a los proveedores de servicio de Internet ofrecer niveles diferenciados de servicios a sus clientes.
- Coexistencia de aplicaciones críticas, que aseguran que una red de área amplia o red WAN esta siendo usada de manera eficiente para aplicaciones críticas que son importantes para el negocio del cliente, y que los anchos de banda y mínimos retardos requeridos están disponibles para aplicaciones multimedia y aplicaciones de voz y que otras aplicaciones que usan el enlace compartido no están interfiriendo con la utilización del tráfico crítico.

a. **Arquitectura Básica de QoS**.- La arquitectura consiste de 3 partes:
   - Calidad de Servicio con solo un elemento de red, compuesto por herramientas de encolamiento, ordenamiento y formación de tráfico.
   - Técnicas de Señalización para coordinación de la Calidad del Servicio de extremo a extremo entre elementos de la red.
   - Control y administración de extremo a extremo del tráfico que cruza por una red mediante políticas, reglas administrativas y funciones de contabilidad.

2.1.2 CoS: Clase de servicio

Es una metodología de encolamiento, el cual usa un algoritmo que permite comparar determinados campos de paquetes llamados etiquetas ToS Tipo de Servicio para poder clasificarlos y para luego asignarles de acuerdo a esta comparación diferentes prioridades. La Clase de Servicio permite diferenciar servicios tradicionales tales como protocolo hipertexto, Correo Electrónico o Transferencia de Ficheros, de otras aplicaciones mas dependientes del retardo y de la variación del mismo, como son el vídeo y la voz interactiva.

2.1.3 LSP: Ruta de Conmutación de Etiquetas

Es el camino virtual a través de la red MPLS por donde se transmitirán los paquetes, y que es determinado gracias al protocolo de enrutamiento IGP utilizado y al protocolo de señalización, este último protocolo permite distribuir las etiquetas que definirán la ruta LSP.

2.1.4 Enrutadores Proveedores (Enrutadores P)

Mejor conocidos como equipos LSR (Enrutador de Conmutación de Etiquetas) elemento que conmuta etiquetas en una red IP/MPLS, pues como su nombre lo indica se encarga de conmutar las etiquetas que contienen el parámetro LSP, y que vienen de los enrutadores de borde.

2.1.5 Enrutadores Proveedores de Borde (Enrutadores PE)

Conocidos comúnmente como equipos LER (Enrutador de Etiquetas de borde) elemento que inicia o termina la comunicación de etiquetas en una red IP/MPLS (pone y quita etiquetas), la asignación de etiquetas esta definida de acuerdo a políticas de prioridad del servicio jerarquizado que se desea brindar.

2.1.6 MPLS Multi Protocolo de Conmutación de Etiquetas

Es un método para reenviar paquetes a través de una red usando información contenida en etiquetas añadidas a los paquetes IP, donde su principal objetivo es crear redes flexibles y escalables con un incremento en el desempeño y la velocidad. Esto incluye Ingeniería de Tráfico y soporte de VPNs (Redes Privadas Virtuales), el cual ofrece Calidad de Servicio (QoS) con múltiples Clases de Servicio (CoS). Hay que resaltar que las etiquetas son insertadas entre el encabezado de capa 3 y el encabezado de capa 2 para el caso de tecnologías basadas en tramas de datos. En MPLS tan pronto un paquete es asignado a un FEC (Clase de Equivalencia de Reenvío), el análisis del encabezado ya no es realizado por los enrutadores subsecuentes, todo el reenvío es hecho basado en etiquetas.

La base del MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los caminos LSP por la red. Cada LSP se crea a base de concatenar uno o más saltos en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Enrutador LSR) a otro, a través del dominio MPLS. Un LSR no es sino un enrutador especializado en el envío de paquetes etiquetados por MPLS. Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer Enrutador (LER) que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola y son los que colocan y quitan las respectivas etiquetas, los dos están en el exterior del dominio MPLS. Los otros Enrutadores interiores son los LSRs que están dentro de dominio MPLS. Un LSR es como un enrutador que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona los protocolos de enrutamiento. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada tal como se muestra en la Figura 2.1, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LER sólo hay una etiqueta de salida en el de cabecera y otra etiqueta de entrada en el de cola).

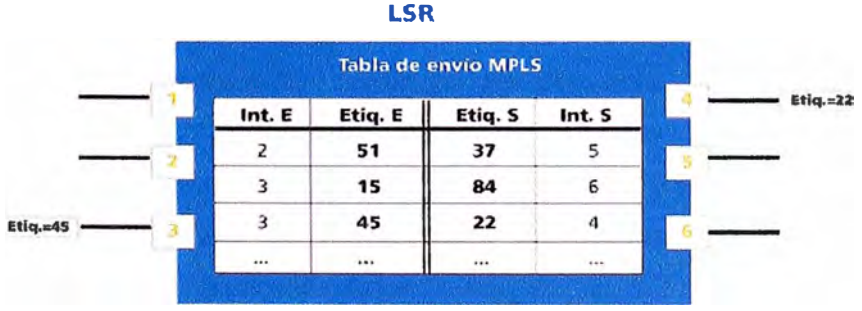


Figura 2.1 Tabla de Conmutación de Etiquetas

2.1.7 AS - Sistema Autónomo

Es un conjunto de redes bajo una administración común que comparte una estrategia de ruteo común. Los sistema autónomos son divididos por áreas y su identificación consta de un número de 16 bits asignado por IANA (Autoridad para la asignación de números Internet). A menudo la palabra dominio se utiliza con frecuencia como sinónimo de AS.

2.1.8 OSPF: Algoritmo Abierto de Primero la Trayectoria más corta

Este es un protocolo abierto de enrutamiento (lo cual índica que sus especificaciones son de dominio público) el cual esta basado sobre el algoritmo SPF. Básicamente OSPF es un protocolo que verifica el estado del enlace enviando LSA (avisos de estado del enlace) a todos los enrutadores que se encuentran en un mismo Sistema Autónomo. En las LSAs del OSPF se incluye la información de las interfaces interconectadas, las mediciones utilizadas y otras variables. Con la información de los estados de los enlaces los enrutadores utilizan el algoritmo SPF para calcular la trayectoria mas corta hacia cada nodo.OSPF puede operar dentro de una jerarquía. La entidad mas grande dentro de la jerarquía es el AS – Sistema Autónomo, OSPF es un protocolo de enrutamiento intra –AS (puerto de enlace interior), aunque puede recibir rutas de otros ASs y enviar rutas a otros ASs.

Un AS puede ser dividido en varias áreas, que son grupos de redes contiguas unidos por enrutadores, estos enrutadores llamados *enrutadores de frontera de área* llevan bases de datos topológicas separadas por cada área. Una base de datos topológica es en esencia un panorama general de las redes en relación con los enrutadores. La base de datos topológica contiene la colección de LSAs recibida de todos los enrutadores en la misma área. Debido a que los enrutadores dentro de la misma área comparten la misma información, tienen bases de datos topológicas idénticas. Una topología de área es invisible para las entidades fuera del área. Conservando cada topología de área por separado, el OSPF transfiere menos tráfico de enrutamiento del que pasaría si el AS no estuviera particionado. La partición del área genera dos tipos diferentes de enrutamiento OSPF, en función de si el origen y el destino se encuentran en la misma o en diferentes áreas. El enrutamiento intraárea se presenta cuando el origen y el destino se encuentran en la misma área; el enrutamiento interárea se presenta cuando están en áreas diferentes.

Un troncal OSPF es responsable de distribuir información de enrutamiento entre las áreas. Está formada por todos los enrutadores de frontera de área, las redes no contenidas por completo en cualquier área y sus enrutadores conectados, la troncal misma se comporta como un área OSPF.

a. **ALGORITMO SPF.-** EL algoritmo de enrutamiento SPF (Primero la trayectoria mas corta) es la base de la operación del OSFP. Cuando un enrutador SPF se enciende, inicializa sus estructuras de datos para el protocolo de enrutamiento y posteriormente espera las señales de los protocolos de las capas inferiores que indican que sus interfaces están funcionando correctamente.

   Después que el enrutador se asegura de que sus interfaces están funcionando correctamente, utiliza el protocolo "Hola" de OSPF para obtener vecinos, que son enrutadores con las interfases hacia una red común, por lo que el enrutador envía paquetes "Hola" a sus vecinos y recibe sus paquetes "Hola". Además de ayudar a obtener vecinos, los paquetes Hola también funcionan como señales de permanencia para que los enrutadores sepan que otros enrutadores están funcionando correctamente.

   En las redes multiacceso (redes que soportan más de dos enrutadores), el protocolo "Hola" selecciona un enrutador designado y un enrutador designado de respaldo. Entre otras cosas, el enrutador designado es responsable de generar LSAs para toda la red de multiacceso. Los enrutadores designados permiten que disminuya el tráfico de la red y el tamaño de la base de datos topológica. Cuando las bases de datos de estado de enlaces de 2 enrutadores vecinos están sincronizadas, se dice que los enrutadores son adyacentes. En las redes multiacceso, el enrutador designado determina que enrutadores deben ser adyacentes. Las bases de datos de topologías están sincronizadas entre pares de enrutadores adyacentes. Las adyacencias controlan la distribución de los paquetes del protocolo de enrutamiento los cuales se envían y reciben sólo a través de las adyacencias. Cada enrutador periódicamente envía un LSA para proporcionar información sobre las adyacencias de un enrutador o para informar a los demás enrutadores cuando se presente un cambio en el estado de algunos de ellos. Comparando las adyacencias establecidas con los estados de enlaces, se pueden detectar rápidamente los enrutadores que están fallando y la topología de red se puede modificar de la misma forma. Con la ayuda de la base de datos topológica que generan los LSAs, cada enrutador calcula un árbol de trayectoria mas corta, con él mismo como raíz. El árbol de trayectoria mas corta, a su vez, genera una tabla de ruteo.

2.1.9 IS-IS: Sistema Intermedio a Sistema Intermedio

Es un protocolo de enrutamiento jerárquico basado en estado de enlaces de OSI que inunda la red con información de estado de enlaces para construir un panorama

consistente de la topología de red. IS-IS utiliza 4 métricas de manera predeterminada, La métrica es una medida propia del protocolo de enrutamiento en el caso de IS-IS se define 4 métricas o costos: Valor de Trayectoria, Retardo, Gasto y Error. El primero es un valor cualquiera asignado por el administrador de la red, el segundo se refiere a la cantidad de retardo en el enlace, la métrica de Gasto refleja el costo de las comunicaciones asociado con la utilización del enlace y la métrica de Error refleja la tasa de errores del enlace, estas 4 mediciones están asociadas a la QoS que permitirá calcular las rutas a través de la red.

2.1.10 BGP: Protocolo de Puerta de Enlace Fronteriza

Es un protocolo de enrutamiento cuya función de enrutamiento involucra a 2 o más enrutadores localizados en sistemas autónomos diferentes o iguales, y que usan BGP para mantener una vista completa de las redes propias o vecinas. BGP también es usado para determinar que Enrutador será considerado como el punto de conexión para específicos sistemas autónomos externos. BGP mantiene tablas de enrutamiento, transmite actualizaciones de enrutamiento y decisiones de enrutamiento para seleccionar la mejor ruta en base a métricas de enrutamiento.

a. **Operación de BGP.-** BGP realiza tres tipos de enrutamiento:
    - El enrutamiento de sistemas interautónomos se presenta entre dos o más enrutadores BGP en sistemas autónomos diferentes. Los enrutadores equivalentes en estos sistemas utilizan BGP para mantener una vista conciente de la topología de la red. Los BGP vecinos que se comunican entre sistemas autónomos deben residir en la misma red física. La red Internet es ejemplo de una entidad que utiliza este tipo de enrutamiento ya que está compuesta de sistemas autónomos o dominios administrativos. Muchos de estos dominios representan a las diferentes instituciones, corporaciones y entidades que forman internet. El BGP se suele utilizar para determinar la trayectoria que proporcione el enrutamiento óptimo en Internet.
    - El enrutamiento del sistema intraautónomo se presenta entre dos o más enrutadores BGP localizados en el mismo sistema autónomo. Los enrutadores equivalentes dentro del mismo sistema autónomo utilizan el BGP para conservar una vista consistente de la topología del sistema. EL BGP también se utiliza para determinar que enrutador servirá como punto de conexión para los sistemas autónomos externos específicos. En este

caso Internet también representa un ejemplo del enrutamiento de sistemas interautónomos. Una organización como una Universidad podría hacer uso del protocolo BGP para ofrecer el enrutamiento óptimo dentro de su propio dominio administrativo o sistema autónomo. EL protocolo BGP puede proporcionar servicios de enrutamiento de sistemas Inter e intraautónomos.

- EL enrutamiento de sistemas autónomos de paso se presenta entre dos o más enrutadores equivalentes BGP que intercambian tráfico a través de un sistema autónomo que no corre el BGP. En un ambiente de sistemas autónomos de paso, el tráfico BGP no se origina dentro del sistema autónomo en cuestión y no está destinado a un nodo en el sistema autónomo. El BGP debe interactuar con cualquier protocolo de enrutamiento de sistema interautónomo que se esté utilizando para transportar de manera exitosa el tráfico BGP a través de ese sistema autónomo.

b. **Enrutamiento BGP.-** Igual que con cualquier protocolo de enrutamiento, el protocolo BGP lleva tablas de enrutamiento, transmite actualizaciones de enrutamiento y se basa en medidas o métricas para tomar las decisiones de enrutamiento. La función principal de un sistema BGP es intercambiar información respecto al alcance de la red, incluyendo información sobre la lista de las trayectorias de sistemas autónomos con otros sistemas BGP. Esta información se puede utilizar para construir una gráfica de la conectividad de los sistemas autónomos de la cual se pueden retirar los ciclos de enrutamiento y con la que se pueden aplicar las decisiones en cuanto a las medidas que se tomarán a nivel sistema autónomo.

   Cada uno de los enrutadores BGP lleva una tabla de enrutamiento que enlista todas las trayectorias factibles hacia una red particular. Sin embargo, el enrutador no actualiza la tabla de enrutamiento. En vez de ello, la información de enrutamiento que reciben los enrutadores equivalentes se conserva hasta que se recibe una actualización de incremento. Los dispositivos BGP intercambian información de enrutamiento en un intercambio inicial de datos y después con actualizaciones de incremento. Cuando un enrutador se conecta por primera vez a la red, los enrutadores BGP intercambian todas sus tablas de enrutamiento BGP. De manera similar, cuando se modifica la tabla de enrutamiento, los enrutadores envían la porción de su tabla de enrutamiento que se ha modificado. Los

enrutadores BGP no envían, de manera regular, actualizaciones de enrutamiento programado, y las actualizaciones de enrutamiento BGP anuncian solamente la trayectoria óptima hacia una red.

EL BGP utiliza una sola métrica de enrutamiento para determinar la mejor trayectoria hacia una determinada red. Esta métrica consta de un número arbitrario de unidades que especifica el grado de preferencia de un enlace particular. La medida BGP típicamente se asigna a cada enlace a través del administrador de la red. EL valor asignado a un enlace puede basarse en cualquier criterio, entre ellos, la cantidad de sistemas autónomos por los que pasan la trayectoria, la estabilidad, la velocidad, el retardo, y el costo.

2.1.11 Objetos:

Entiéndase por objeto a los elementos que conforman una página web y que son los elementos que se almacenan dentro de los servidores caché, los objetos mas conocidos son los gráficos con extensión bmp, jpg, jpeg, tiff; los videos con extensión mpeg, avi, wav los elementos de extensión tar, zip, txt, pdf.

2.2 Bases Teóricas.-

A continuación explicamos los diferentes elementos teóricos que es necesario considerarlos

2.2.1 La Ley de Zipf

George Kingsley Zipf (1902-1950) indica que "*La frecuencia de ocurrencia de cierto evento (P) como función del rango (i) cuando el rango viene determinado por la frecuencia de ocurrencia, es una función potencial*

$$Pi \approx \frac{1}{i^a} \quad (2.1)$$

con el exponente a cercano a la unidad"

Para este ejemplo particular de un servidor caché para la página web de Sun Microsystem, la frecuencia de ocurrencias en este caso esta determinado por el Número de Peticiones y el rango esta definido por la cantidad de objetos usados o requeridos, ver figura 2.1.

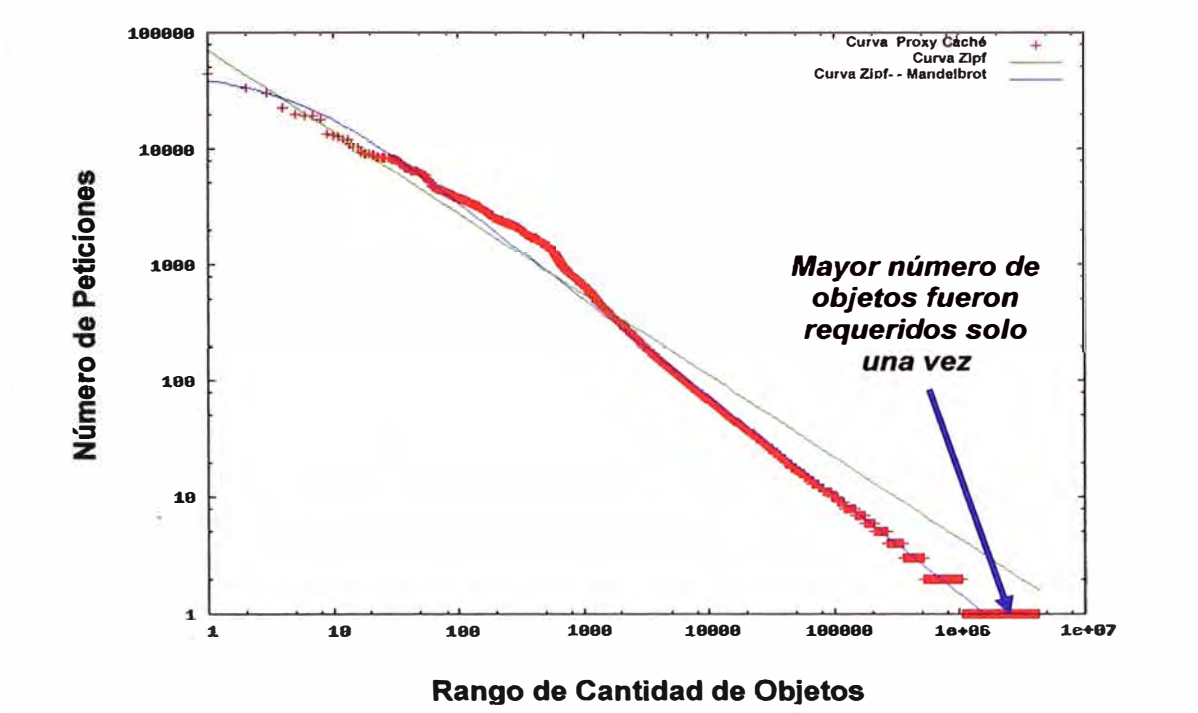


Figura 2.1 Frecuencia de ocurrencias para la web de SUN MICROSYSTEM

2.2.2 Características del Tráfico Web:

- El tráfico Web es multiprotocolo el cual incluye TCP, UDP, HTTP, FTP; pero es el tráfico HTTP el que ocupa el 80% de este tráfico.
- El tamaño medio de objeto esta entre 10 y 15 Kbytes. Abundan **objetos pequeños** aunque se encuentra una cantidad no despreciable de objetos grandes (Mbytes).
- La mayor parte de la estructura de una pagina Web esta compuesta de **objetos gráficos**, seguido de documentos html. El 1-10% son objetos dinámicos.
- Una página html tiene como media **10 imágenes** y varios enlaces a otras.
- Un 40% de objetos que componen una página web son considerados no cacheables.
- La popularidad de los objetos web es muy dispar: solo una pequeña fracción de objetos es responsable de un gran porcentaje de la demanda , la demanda de los objetos sigue la ley de Zipf
- El ritmo de encontrar objetos estáticos al acceder a las páginas webs es mucho mayor que el ritmo de encontrar objetos en modificación.
- En escala de tiempo inferior al minuto, se puede considerar al tráfico web como una transmisión de ráfagas de datos: valores medios de tráfico durante decenas de segundo.
- Un 5-10% de accesos al Web se cancelan antes de finalizar.
- Casi todos los servidores usan el puerto 80

2.2.3 Red IP/MPLS.- LA red IP/MPLS es una arquitectura de equipos conformada principalmente por enrutadores los cuales se distribuyen en Enrutadores Proveedores (EnrutadoresP) que son los que conforman el Núcleo de red y los Enrutadores Proveedores de Borde (Enrutadores PE) que se encuentran en la frontera de la red del proveedor los cuales están interconectados a los Enrutadores P mediante protocolos de enrutamiento internos IGP que pueden ser OSPF o IS-IS. Así mismo se utiliza el protocolo de enrutamiento BGP (Protocolo de entrada de Frontera) para la comunicación entre Enrutadores PE los cuales utilizan la ventaja de la tecnología MPLS para transmitir información de un nodo PE a otro nodo PE y que se traduce en el reenvío de etiquetas que contienen la ruta LSP (*Ruta de conmutación de Etiquetas*) que es el camino MPLS definido entre los Enrutadores PE, de manera que los Enrutadores intermedios conmutarán los paquetes hacia su destino gracias al LSP definido en la etiqueta. Para establecer el LSP se utilizan 2 protocolos que trabajan por separado como son el Protocolo de Enrutamiento y el Protocolo de señalización, El protocolo de enrutamiento distribuye la información de la topología de la red a través de la red para poder determinar el óptimo LSP, para esto los IGP mas usados son OSPF o IS – IS, pues las redes MPLS por lo general usan un único dominio administrativo. Los protocolos de señalización informan a los conmutadores que etiquetas y enlaces se usarán para cada LSP, lo que significará que cada vez que ingrese al conmutador una etiqueta con un determinado LSP este sabrá por que enlace derivarlo, pues lo tendría almacenado dentro de su Tabla de Conmutación; para llevar a cabo esta tarea se utilizan los Protocolos de Reservación de Recursos y el Protocolo Distribuidor de Etiquetas, el primero con la función de determinar las tablas de conmutación con características de Ingeniería de Tráfico y de calidad de servicio para el flujo de datos y el segundo con la misión de asociar o distribuir la etiqueta con la LSP correspondiente. Visto esto es que por lo menos se debe activar LDP y MPLS en los Enrutadores P y PE, para aprovechar las ventajas del etiquetado de tráfico. Para mejor entendimiento de la arquitectura podemos revisar la figura 2.1.

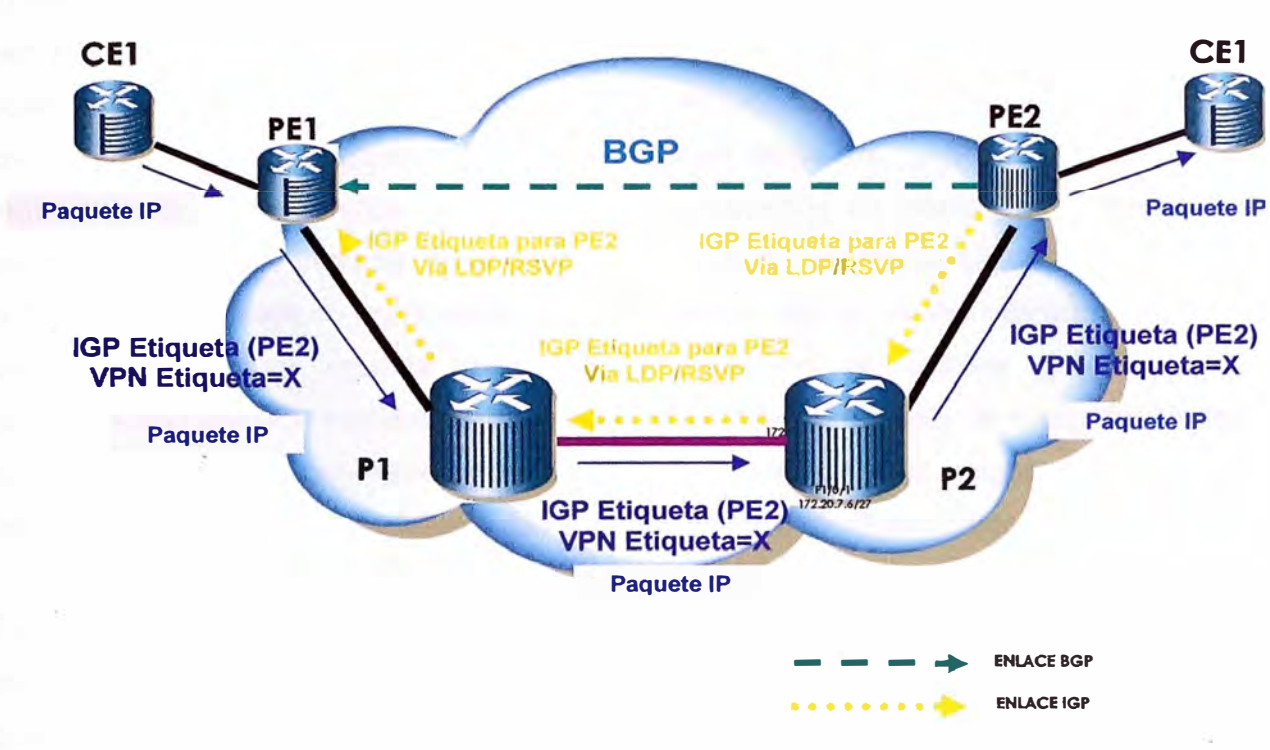


Figura 2.2 Transmisión de Etiquetas en la Red IP/MPLS

2.2.4 Red Caché.- Red Caché son los equipos interconectados localmente que permiten el copiado y almacenamiento de información en una red local. Las copias de contenidos recientemente visitados son almacenadas temporalmente en repositorios que se encuentran en ubicaciones topológicas, este almacenamiento ofrece tiempos de respuesta reducidos, reducción de la congestión de Internet, conservación del ancho de banda de la red, reducción de costos de servicios por reducción del tráfico internacional y optimización de los recursos de la red.

Existen actualmente 3 escenarios para desarrollar Redes de almacenamiento o redes Caché, el cual esta en función de la aplicación que se le quiera dar a los repositorios y de sus respectivos conmutadores en una red WAN, estos son:

- Almacenamiento Proxy. Que requiere tener ubicado los servidores caché dentro de su propia red corporativa pero que representa una solución muy cara para las empresas.
- Almacenamiento Transparente. Ubica a los servidores caché dentro de la red WAN de las empresas proveedoras de Internet PSI y que significa una inversión estratégica, por ser esta parte del Núcleo del negocio de la empresa.
- Almacenamiento Proxy Inverso. Utiliza los servidores caché para ampliar su capacidad de almacenamiento de los servidores web de las compañías cuyos contenidos web tienen mucha demanda de acceso.

El escenario que se ha usado para este caso es el de almacenamiento transparente por ser el diseño que se ajusta a una Empresa Proveedora de Servicios de Internet PSI, pues en esta solución los elementos de almacenamiento llámese repositorios y conmutadores están alojados dentro de la red WAN de la PSI por lo que cada requerimiento de contenidos generados por los usuarios es interceptado por las redes caché (RC), quienes verifican si guardan una copia del contenido solicitado, si no es así la RC visita el contenido en el servidor web y realiza una copia del mismo dentro de sus servidores caché y reenvía este mismo contenido al usuario que lo requirió, subsecuentemente los requerimientos de otros usuarios adquirirán la copia del contenido que se encuentra en los repositorios lo cual es mas rápido y no consume mas ancho de banda de Internet que el necesario, las figuras 2.1 y 2.2 explican mejor estos escenarios:

En la figura 2.3 observamos la topología que muestra el proceso que proporciona el contenido al cliente cuando el contenido no existe en los servidores caché, donde vemos que se intenta de conseguir el contenido una sola vez para de ahí grabarlo en los caches.

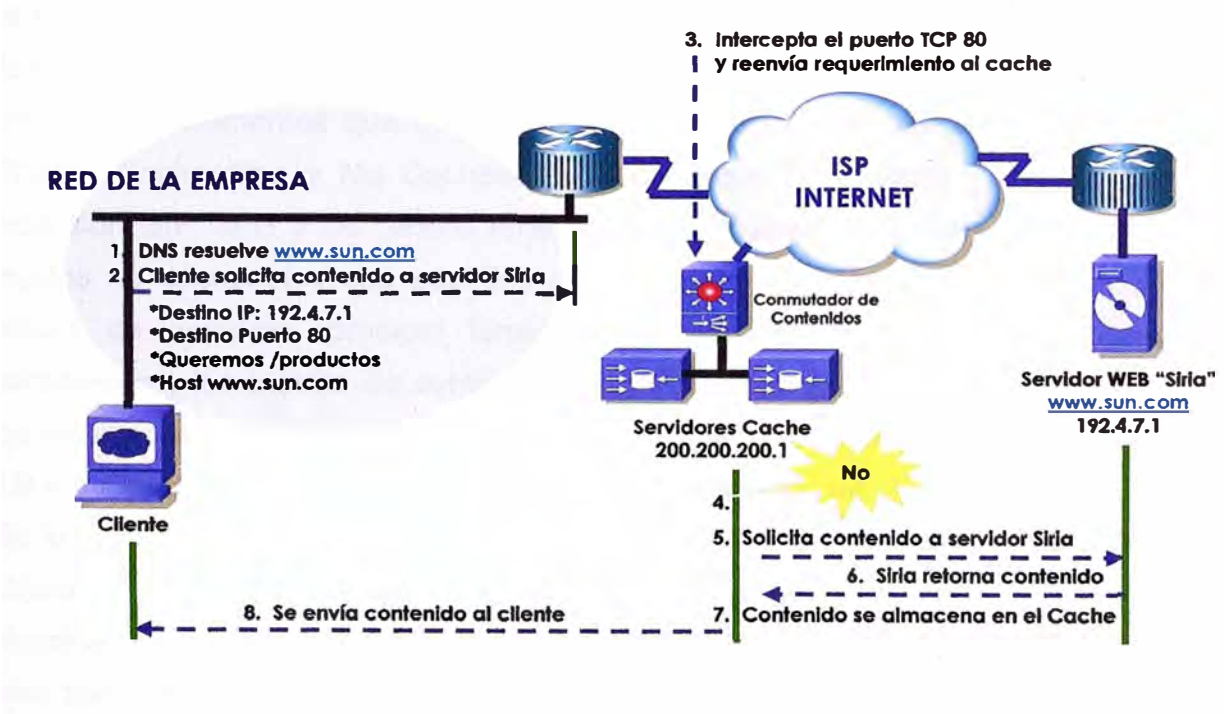


Figura 2.3 Esquema cuando el contenido no existe en el servidor caché

En la figura 2.4 observamos la topología que muestra el proceso que proporciona el contenido al cliente cuando el contenido existe en los servidores caché y lo simple que se torna entregar el requerimiento al cliente.

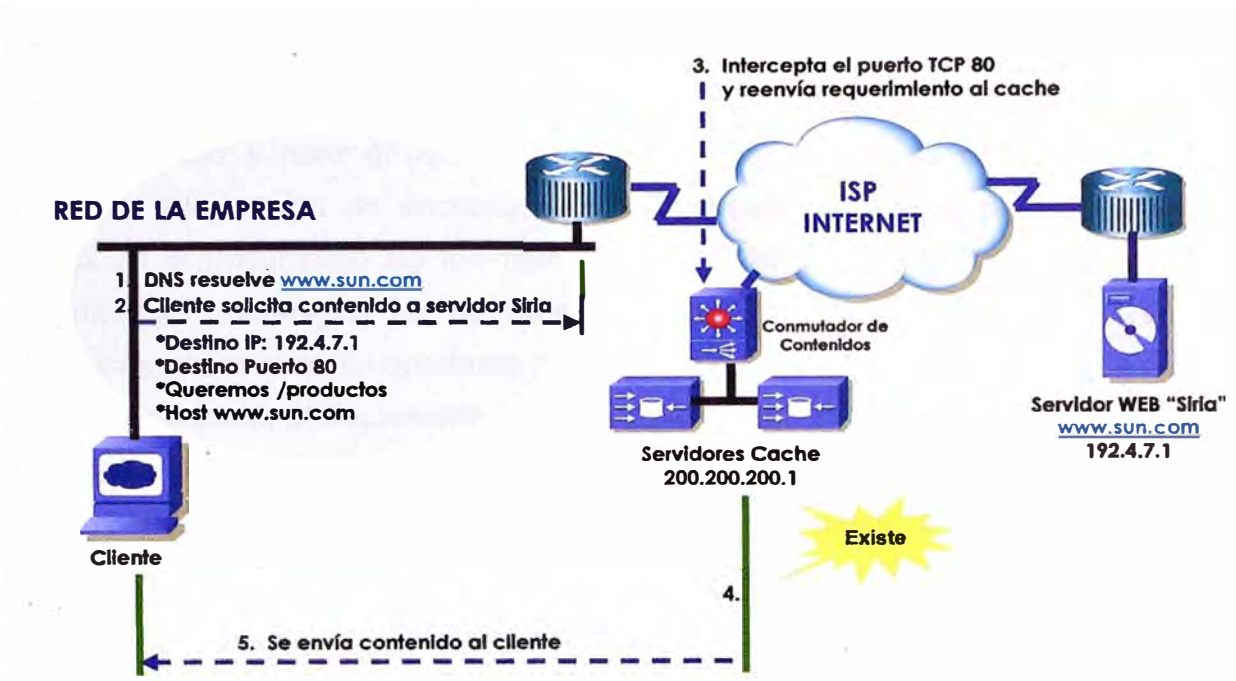


Figura 2.4 Esquema cuando el contenido existe en el servidor caché

La forma en que se da el copiado caché viene dado por un establecimiento de reglas que determinan cuando se brindará un objeto si este se encuentra disponible (entiéndase por objeto a los elementos que conforman una página web los cuales podemos dividir en Objetos Cacheables y No Cacheables, los objetos Cacheables son los gráficos de extensión GIF, JPG y los textos HTML que son grabados en los servidores caché, los objetos no cacheables son aquellos de contenido dinámico como son los objetos de bolsas de compras, precios; también está aquellos cuyo resultado depende de parámetros y los objetos de contenidos seguros o encriptados que no son grabados en los servidores caché). Algunas de estas reglas son establecidas en los protocolos HTTP 1.0 y 1.1 y otras son definidas por el administrador del caché.

En lo que respecta al copiado caché podemos mencionar de 2 tipos de estados de los objetos: RECIENTE Y CONSEGUIR Un objeto de caché es considerado RECIENTE (que significa capaz de ser enviado a un cliente sin la comprobación del servidor origen) si este tiene un tiempo de expiración o otra directiva establecida de control de antigüedad, que esta apto dentro del periodo de servicio. Para asegurar que las copias copiadas permanezcan actualizadas, HTTP fuerza la expiración de un objeto mediante una Cabecera de Expiración que especifica el día de expiración del objeto. Cuando es esencial que un objeto obtenido esté actualizado, se debe contactar al servidor remoto por cada requerimiento CONSEGUIR. Para solucionar el problema que provoca tener que

obtener el documento del servidor remoto por cada acceso al mismo, el protocolo HTTP incluye una cabecera de nombre *Modificado-desde-entonces* al requerimiento, haciendo posible un requerimiento CONSEGUIR condicional. Mediante esta cabecera, que contiene el día y hora en que el documento fue modificado por última vez, puede obtenerse información de encabezado del documento en lugar del documento en sí mismo. Si el documento no fue modificado a partir del día y hora contenidos en la cabecera, el documento no se retorna desde el servidor remoto, sólo se retorna información de cabecera importante del documento, tal como nueva fecha de expiración. Si, por el contrario, el documento fue modificado luego del día y hora de la cabecera, se retornará el documento como si se tratase de un requerimiento GET tradicional.

El CONSEGUIR condicional tiene varias utilidades más eficientes, como por ejemplo, puede ser usado por el software de espejado que regularmente tiene que refrescar un gran número de archivos. Además podría ser útil para que un servidor caché refresque su caché durante períodos de inactividad de los clientes. Si el servidor HTTP remoto no soporta requerimientos CONSEGUIR condicionales, ignora la cabecera, enviando en todos los casos el documento completo. Afortunadamente, la mayoría de los servidores HTTP soportan la cabecera del CONSEGUIR condicional.

Si un objeto es antiguo, el servidor del origen será preguntado para validar el objeto, o dirá al servidor caché que la copia que tiene sigue aún siendo buena y si el intervalo de tiempo de la cabecera *Modificado-desde-entonces* o de la cabecera de expiración es crítico, la pagina almacenada puede enviar un requerimiento CONSEGUIR con la definición de que el objeto es no cacheable.

En ausencia de una Cabecera de Expiración, los agentes proxy estiman un día de expiración para un documento basándose en datos disponibles. Por ejemplo, un documento que ha cambiado recientemente (dato obtenido de la cabecera *Modificado-desde-entonces*) se puede asumir que es importante actualizarlo frecuentemente, la carencia de accesos puede provocar la expiración de un objeto, también se pueden copiar al cache las imágenes por un tiempo mayor que el que usa en los de texto. Las cabeceras de expiración son especialmente funcionales para realizar el copiado a los caché de imágenes estáticas (como barras y botones de la navegación) por el hecho de que no cambian mucho, es así que se puede fijar un tiempo de vencimiento extremadamente largo para estos objetos, permitiendo de esta manera que la Página Web aparezca con mucha más disponibilidad para los usuarios, pero además las cabeceras de expiración son también útiles para controlar el almacenamiento de una página que cambia regularmente, por ejemplo, si usted pone al día una página de noticias

a las 6am, usted puede fijar el objeto para expirar en un determinado tiempo, es así que los servidores caché sabrán cuándo conseguir una copia fresca.

Cabe destacar que en HTTP/1.1 existe un conjunto más rico de cabeceras de control que en HTTP/1.0, incluyendo controles sobre la edad máxima de documentos, directivas de caché públicas y privadas, etc. Es para notar que muchas de las funciones que brinda el servidor de caché dependen del tiempo, por eso es muy importante que el servidor y la página web usen correctamente el tiempo GMT.

Diferentes páginas web y agentes proxy aplican diferentes heurísticas para determinar qué documentos pueden ser cacheados, mientras que de la especificación de HTTP derivan algunas reglas, tales como:

- No pueden ser cacheados documentos que requieran autorización.
- No pueden ser cacheados los documentos no cacheables.
- Los documentos con tiempo de expiración de momento, con un día de expiración ya vencido o un día de expiración ilegal, tampoco pueden ser cacheados.

CAPITULO III
METODOLOGIA DE SOLUCION DEL PROBLEMA

3.1 Alternativas de Solución.-

Ante este problema del retardo de acceso a los servidores web, las PSI (Proveedoras de Servicios de Internet) han considerado un abanico de alternativas de solución, las cuales van desde la ampliación de la capacidad de ancho de banda a la salida Internacional así como de la colocación de repositorios para determinados clientes que generen mayor congestión. La presente solución no solo responde a una solución promedio sino que sobre todo responde a un fundamento técnico que ha de considerar las condiciones de red existente de acceso a Internet que tiene Telefónica Empresas y a la disposición de la red IP/MPLS que posee, teniendo en cuenta esto es que se ha optado por implementar redes caché del tipo Transparente (tema que fue explicado en el subtítulo 2.2.4) en cada nodo de la Red IP/MPLS con el objetivo de tener un servicio redundante y confiable que pueda satisfacer la expectativa del cliente, por lo que dicha solución no solo contribuirá a que los clientes se beneficien con la percepción de tiempos de acceso mínimos a las páginas web sino que también contribuiría a que la empresa pueda ahorrar una cantidad considerable de ancho de banda que podría destinar para que sean usados por otros clientes, lo cual se revertiría en mayores beneficios económicos para la empresa. Si bien es cierto que la inversión que se realizó para implementar este proyecto de inicio a fin fue muy considerable, es cierto también que dicha inversión permitió y permite generar grandes ahorros en plazos muy cortos, lo cual justifica completamente las decisiones de inversión que se tomaron en un inicio para la ejecución de este ambicioso proyecto.

3.2 Solución del Problema: Diseño e Implementación.-

3.2.1 Diseño.- El diseño de la solución parte del dato de la velocidad de acceso a la Red Internacional que se tiene contratado, pues este dato permitirá determinar la capacidad de almacenamiento de los servidores cuyo tamaño deberá soportar a los actuales usuarios como a los futuros clientes del servicio por un determinado periodo de tiempo, considerando además que la red IP/MPLS de Telefónica esta compuesta por 6 nodos de los cuales 4 contendrán una red caché (compuesto por repositorios caché y

conmutadores). El tráfico contratado que se usa de acceso a Internet esta fijado en 3 STM-1 (465Mbps) y que se ha repartido en los 4 nodos de acuerdo a la tabla 3.1, recordando que esta distribución promedio se ha obtenido en función del total de los servicios de Internet contratados por los clientes asignados por cada nodo (Aquí están contenidos los usuarios de InfoInternet, Cabinet Y Unired), por lo que se puede observar en esta tabla que hay mayor demanda del servicio por el lado de los nodos de Washington y San Isidro los cuales han sido considerados críticos por lo que se ha previsto que deben disponer de redundancia a nivel de almacenamiento por lo que se colocará 2 servidores de caché o de almacenamiento con las mismas características y capacidades para soportar la carga de la otra en caso de que una de ellas falle, así mismo se ha optado por elegir un método de balanceo de carga de manera que no se tenga capacidad tecnológica instalada ociosa dentro de las Redes Caché, de esta manera la elección de la forma de balanceo estará supeditada al elemento principal que se desea balancear que en este caso son los objetos que conforman las páginas web, tal como mencionamos en el punto 2.2 (Redes Caché), en donde tenemos la posibilidad de administrar los contenidos web con ayuda de las cabeceras HTTP, vista esta ventaja es que se necesita contar con un equipo que aparte de balancear también nos permita conmutar los contenidos, pues de los comúnmente ya conocidos que operan en los niveles OSI tal como L2, L3 y L4, también nos deberá permitir balancear y conmutar los contenidos usando dichas cabeceras HTTP cuyo tratamiento corresponde únicamente a la capa de aplicación L7 de la estructura OSI, pero sin olvidar que deberá de cumplir también con los requisitos de procesamiento de tráfico y de velocidad de transmisión; además que deberá utilizar un módulo inteligente que se encontrará permanentemente comunicado a otro equipo similar redundante, en caso que suceda una falla en uno de ellos. De esta manera nuestra red caché estará formada por 2 Servidores caché y 2 Conmutadores de contenidos en los nodos de Washington y San Isidro; de 1 Servidor caché y Conmutador de contenidos en los nodos de Arequipa y Trujillo y de 1 Conmutador de contenidos en los nodos de Monterrico y Miraflores. De esta manera tendremos continuidad y respaldo del servicio en caso de fallas tanto de Servidores Caché así como de Conmutadores de Contenidos.

Tabla 3.1 Tabla por Nodos del Consumo de Ancho de Banda de Internet de la Red IP/MPLS en la Red Internacional.

NODO	% VELOCIDAD TOTAL	Velocidad (465M)
WASHINGTON	36	168M
SAN ISIDRO	36	168M
AREQUIPA	7	33M
TRUJILLO	7	33M

Las distintas empresas proveedoras de equipamiento han elaborado tablas de correspondencia en base a la velocidad total de acceso a la red, para el caso de los servidores de almacenamiento mostramos la matriz de relación de los servidores de modelo CacheFlows de la marca BlueCoat en la tabla 3.2:

Tabla 3.2 Tabla de Capacidades de los Servidores de Almacenamiento Caché Flow

MODELO	6000	5000	2000	1000	500	100
EMPRESA	SI	SI	SI	SI	SI	SI
ISP	SI	SI	SI	SI	SI	NO
TRAFICO	155 - 310Mb/s	155Mb/s	155Mb/s	155Mb/s	6Mb/s	1Mb/s
DISCO	640G	243G	54G	25G	18G	2G
MEMORIA	256M a 4G	1M a 4G	768M a 1G	256M a 512M	256M a 384M	128M

También mostramos en la tabla 3.3 la matriz de relación de los equipos Conmutadores de Contenidos de la marca CISCO, que son equipos que manejan la conmutación de contenidos en niveles OSI L4 y L7

Tabla 3.3 Tabla de Características de los Content Switch

	CISCO CSS11501	CISCO CSS11503	CISCO11506
Ranuras Modulares	0 (Configuración Fija)	3	6
Incluida en la configuración base	Control Conmutador con 8puertos 10/100 Ethernet y 1 puerto Giga Ethernet (GBIC)	Módulo Control Conmutador con 2 puertos Giga Ethernet (GBIC)	Módulo Control Conmutador con 2 puertos Giga Ethernet (GBIC)
Número Máximo de Puertos Gigabit Ethernet	1	6	12
Número Máximo de Puertos 10/100 Ethernet	8	32	80
Terminación SSL	No	Si	Si
Modulo de 2 puertos Gigabit Ethernet de Entrada y Salida		Máximo de 2	Máximo de 5
16 puertos Ethernet 10/100 de Entrada y Salida		Máximo de 2	Máximo de 5
8 puertos Ethernet 10/100 de Entrada y Salida		Máximo de 2	Máximo de 5
Módulos SSL		Máximo de 2	Máximo de 4
Módulos Aceleradores de Sesión		Máximo de 2	Máximo de 5
Características de Redundancia	* Redundancia de sesiones adaptivas de Nivel 5 * Redundancia de direcciones IP virtuales	* Redundancia de sesiones adaptivas de Nivel 5 * Redundancia de direcciones IP virtuales	* Redundancia de sesiones adaptivas de Nivel 5 * Redundancia de direcciones IP virtuales * Modulo de Control de Conmutación Activo Redundante * Modulo mallado de conmutación redundante * Fuentes de Energía Redundante
Ancho de Banda Agregado	6 Gbps	20 Gbps	40 Gbps
Opciones de Almacenamiento	512MB Disco Duro o 256MB de Disco de Memoria Flash	512MB Disco Duro o 256MB de Disco de Memoria Flash	512MB Disco Duro o 256MB de Disco de Memoria Flash
Energía	Corriente Alterna Integrada	Corriente Alterna y Directa Integrada	Hasta 3 fuentes AC o 3 fuentes DC

Vista las características de los equipos podemos comprobar que algunos de los modelos que se nos presentan satisfacen las necesidades propuestas, es por esto que se ha confeccionado una matriz (ver tabla 3.3) colocando los modelos que cumplen de los Servidores de Almacenamiento y los Conmutadores de Contenidos versus los datos de la tabla 3.1.

Tabla 3.3 Tabla de Correspondencia

Servidor Caché			
PARAMETROS	**REQUERIMIENTOS**	**Modelo CA6085**	**Cumple**
Velocidad de Acceso	168Mbps	155 - 310Mbps	SI
Disco	Esta en función de los velocidad acceso	640G	SI
Memoria	Esta en función de la velocidad de acceso	256M a 4G	SI
Puertos	2 puertos FastEthernet para el caché	3 puertos 10/100Mbps	SI
Protocolos	Que soporte HTTP	Soporta HTTP 1.0 y 1.1	SI
Redundancia	de fuentes de alimentación	2 fuentes AC	SI
Otros Protocolos o Servicios		SSL Tunneling FTP RIP SNMP ICP NTP SOCKS TELNET	SI
Conmutador de Contenidos			
PARAMETROS	**REQUERIMIENTOS**	**Modelo CSS 11506**	**Cumple**
Velocidad de Acceso	168Mbps	40Gbps	SI
Disco	Esta en función de los velocidad acceso	512MB	SI
Memoria	Esta en función de la velocidad de acceso	256MB	SI
Puertos	10 puertos FastEth con 2 puertos GigaEth de FO	2 puertos GigaEth, 14 puertos Fast Ethernet	SI
Redundancia	En fuentes de alimentación	2 fuentes AC	SI
Manejo Contenidos	L4-L7	Content Intelligence	SI
Protocolos	Que soporte HTTP	Soporta HTTP 1.0 y 1.1	SI
Módulos de Control	01 modulo	Modulo de Control de Conmutación	SI
Otros Protocolos o Servicios		Análisis Completo de URL TCP UDP SSL VLAN 802.1Q SSH SNMP GUI RIP OSPF	SI

Así mismo debido a la gran cantidad de procesamiento que ha de originarse debido a este servicio de Internet es que se ha colocado Enrutadores de mayor capacidad en interfaces y procesamiento que soportarán la carga de este tráfico, por lo que se deberá escoger un Enrutador que maneje casi las velocidades del Conmutador de Contenidos que en este caso es de **40Gbps**, este Enrutador de Distribución de Internet deberá además tener redundancia de procesadores y redundancia de hardware, así mismo deberá soportar servicios críticos como QoS (Calidad de Servicio), MPLS (Conmutación de Etiquetas de Multiprotocolo), agregaciones de banda ancha y control de lista de accesos. Visto esto es que se ha elegido el Enrutador 10008 marca CISCO.

Tabla 3.4 Tabla de Características del Enrutador Cisco 10008

Especificaciones	Cisco 10008
Ranuras Modulares	* 8 ranuras para tarjetas * 16 ranuras para tarjetas medianas * 2 ranuras para módulos de Enrutamiento (1 activo, 1 redundante)
Capacidad de Velocidad (bps)	51.2 Gbps

a. **Funcionalidades Adicionales de los Equipos Seleccionados**: Los equipos seleccionados aparte de cumplir las condiciones necesarias de diseño ya presentadas, ostentan también propiedades muy importantes que es necesario mencionar:

Funcionalidades del Conmutador de Contenidos:

- Balanceo de Carga: Esta funcionalidad es aprovechada mediante las cabeceras HTTP las cuales son examinadas y luego redireccionadas junto con sus contenidos a los servidores designados, para esta redirección se usan palabras claves contenidas en las cabeceras HTTP que se asociarán a los servidores caché. Usando balanceo de carga mediante cabeceras HTTP se elimina la necesidad de duplicar varias formas de los mismos contenidos lo que permitirá tener mayor espacio disponible.
- Seguridad: Los ataques que puede sufrir un Conmutador de Contenidos son del tipo DoS (Negación de Servicio) y dentro de estos están contenidos lo ataques LAND que son aquellos paquetes que tienen idéntica dirección fuente y destino, también tenemos los ataques SMURF que son el envío de sesiones de conexión (PING) con destino a todas las direcciones, también tenemos los ataques SYN que son conexiones TCP

que son iniciadas por una fuente pero que no son seguidos por una trama ACK para completar el conocido triple paso TCP.

- Redundancia: Esta solución se da en el caso de que se cuente con mas de un conmutador de contenidos, y se da en el caso de que uno de los equipos falle, por lo que se tendrá que uno de los conmutadores asumirá el servicio y el otro se encontrará en modo de respaldo en un lapso de 3 a 7 segundos lo que significará un mínimo impacto del servicio. La comunicación del aviso de que se realizará tal conmutación del servicio se realiza a través del protocolo VRRP (Protocolo Virtual de Redundancia de Enrutadores) el cual utilizará una VLAN dedicada para tal sentido el definirá cual de los equipos será usado como Master.

Funcionalidades del Servidor Caché:

- Control Adaptivo de renovación de contenidos
- Administración óptimo del rendimiento del disco
- Remapeo automático de URLs para discos que se extraen en caliente
- Integración con Conmutadores Nivel 4 ante fallas.
- Equipo tolerantes a una o mas fallas de disco.

3.2.2 Implementación.- La implementación de este proyecto se desarrollo en 2 fases, la primera fase que cubrió los meses de Enero a Setiembre del 2003 y la segunda fase que cubrió los meses de Setiembre a Noviembre del mismo año.

a. Primera Fase

En la primera fase del proyecto se implementó las Redes Caché en los nodos de Washington y San Isidro, esta implementación se inicio con la instalación de la planta externa, del cableado estructurado y del acondicionamiento del local donde quedaron ubicados los equipos (ver figura 3.1 y 3.2).

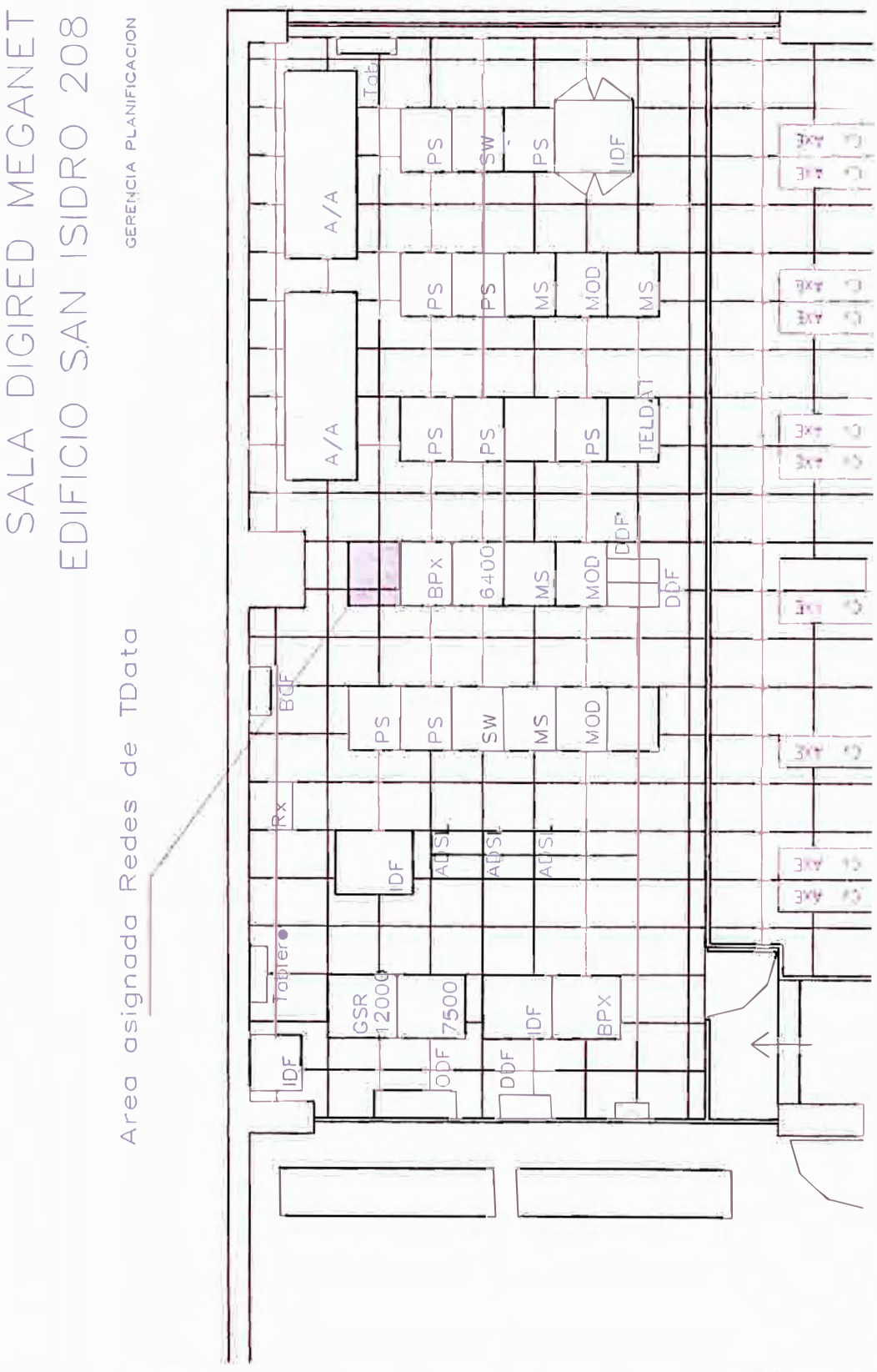
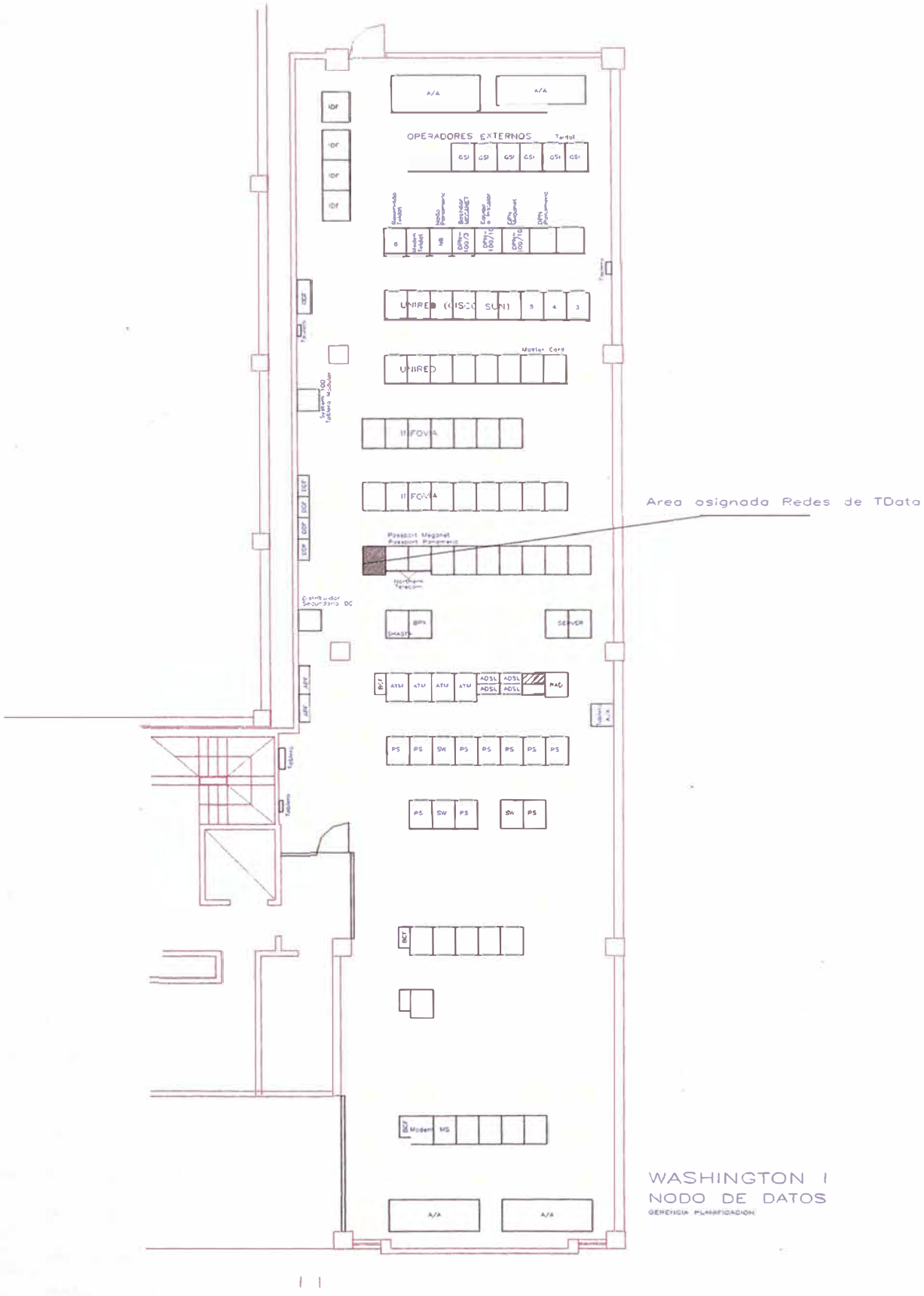


Figura 3.1 Plano de Ubicación de la Red Caché en el Nodo San Isidro



igura 3.2 Plano de Ubicación de la Red Caché en el Nodo Washington

Después de la ubicación final de los equipos se procedió a configurar los mismos. La implementación de la red de los nodos de San Isidro y Washington quedo tal como se puede observar en las topologías de las figuras 3.3 y 3.4, y cuyo proceso de instalación y configuración describimos a continuación:

- Interconexión del Enrutador Distribuidor de Internet (SISDI1 o WASHDI1) con el Enrutador Proveedor (SISP1 o WASHP1) mediante una conexión Optica POS STM -1.
- Interconexión del Enrutador Distribuidor de Internet (SISDI1 o WASHDI1) con los Conmutadores de Contenidos (CSS) redundados mediante 2 enlaces Opticos Gigabit Ethernet, aquí se utilizaron 2 enlaces uno que va al Conmutador de Contenidos Maestro y el otro que va al Conmutador de Contendidos Esclavo. En los CSS tanto el enlace Maestro como el Esclavo utilizan la misma VLAN cuando se conectan al Enrutador Distribuidor y a los Enrutadores Internet (RI).
- Las VLAN´s que tiene definido los CSS son 4: VLAN de Agregación (que se encarga de conectar al Enrutador Distribuidor de Internet (SISDI1 o WASHDI1) y al Enrutador de Internet (SISRI o WASHRI)). VLAN de Gestión (Que se encarga de la administración de la red caché), VLAN de Caches que se encarga de la conexión con los Servidores Caché y la VLAN de Replicación que sirve para transmitir el aviso del Conmutador de Contenidos Maestro al Esclavo para que intercambien funciones o conmuten.
- Se ha definido Enrutamiento OSPF en los Conmutadores de Contenidos para trasladar las rutas contenidas en los Enrutadores de Internet (SISRI o WASHRI) al Enrutador Distribuidor (SISDI1 o WASHDI1).
- Se estableció sesiones IBGP en los Enrutadores (SISDI1 o WASHDI1) para encaminar el tráfico que viene de los CSS hacia los Enrutadores Puerta de Salida (SISTG o WASHTG) a través del AS 6147 (Sistema Autónomo) de la Red IP/MPLS.
- Así mismo se han establecido sesiones IBGP en los Enrutadores Puerta de Salida (SISTG o WASHTG) para encaminar el tráfico hacia todos los Enrutadores DI definidos, para que estos luego lo deriven a los Enrutadores RI.
- En los Enrutadores DI se ha configurado de tal manera que respete las etiquetas asignadas en los Enrutadores RI, estas etiquetas permiten diferenciar en velocidad y valores reales los servicios de Internet contratados por los clientes, esta diferenciación de los servicios se establece en las políticas de prioridad definidas en la Red IP/MPLS.

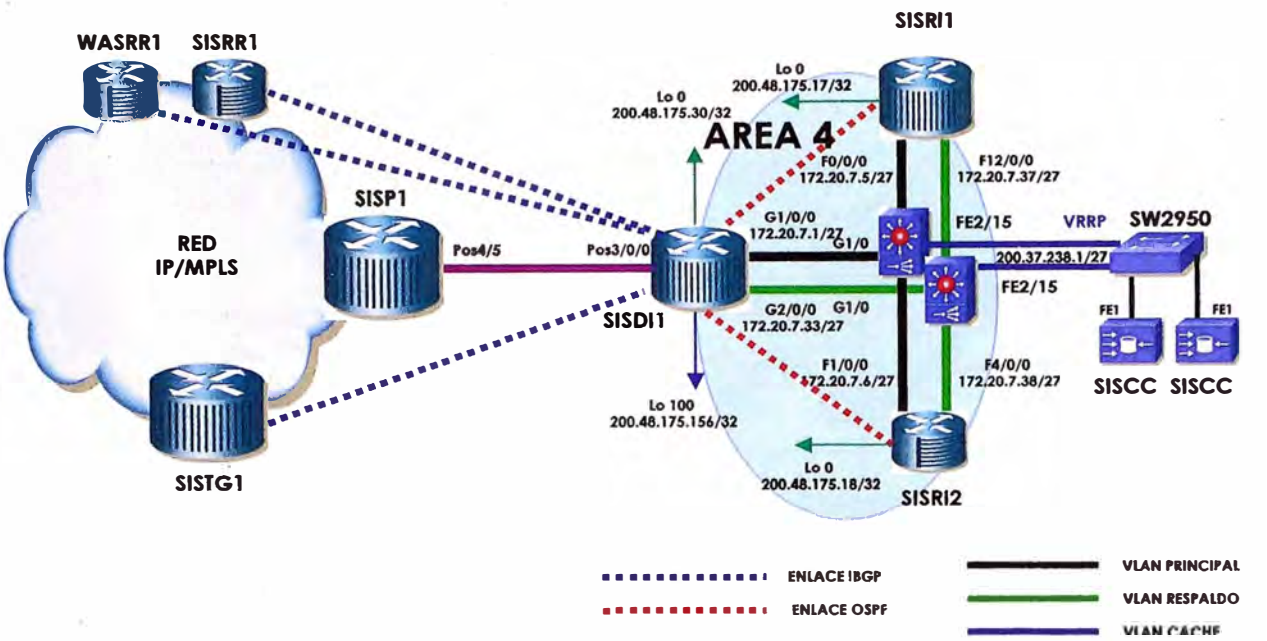


Figura 3.3 Topología Final de la Red Caché en el Nodo de San Isidro

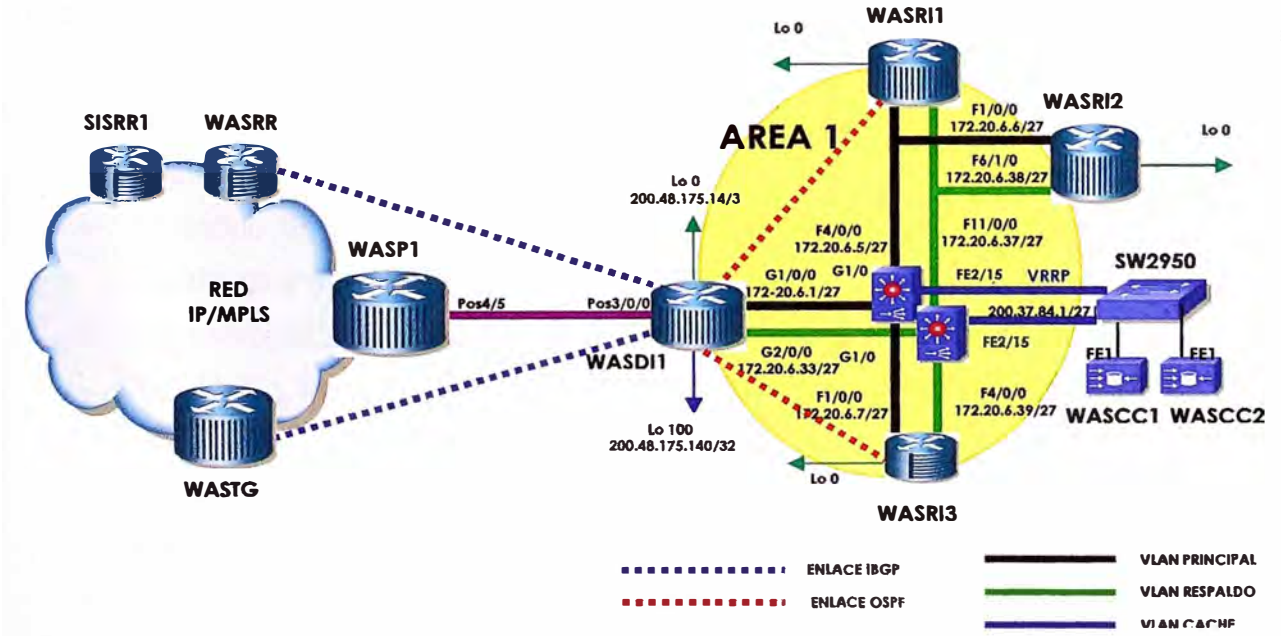


Figura 3.4 Topología Final de la Red Caché en el Nodo de Washington

Una vez implementada las redes caché en los nodos mencionados, se tuvo como primer cliente a la Empresa Telefónica del Perú (Operador de Telefonía Fija) quien contrató a TEmpresas 80Mbps de ancho de banda para brindar el servicio de Internet a sus usuarios Residenciales, los cuales fueron repartidos entre los nodos de Washington y San Isidro. La figura 3.5 muestra como quedo topológicamente establecida las conexiones

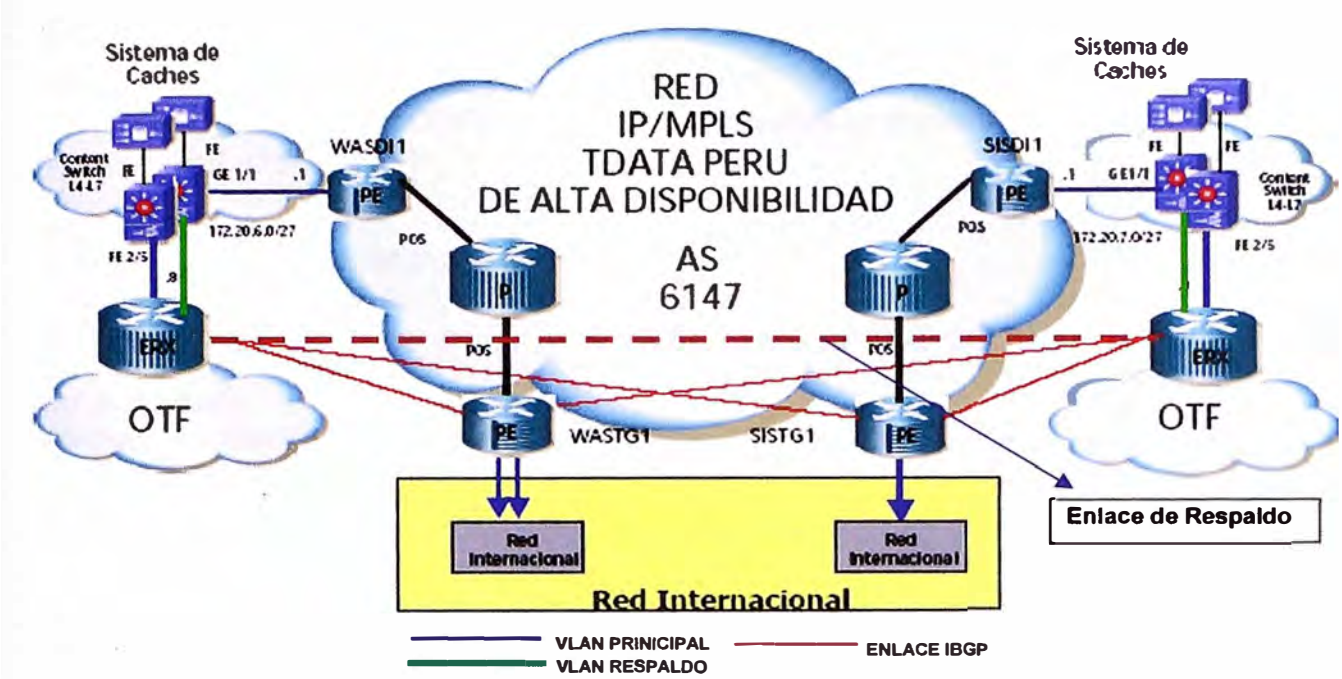


Figura 3.5 Topología de Acceso a Internet de OTF – Sistema de Caché Distribuido

Los pasos que tuvieron que seguirse para ejecutar esta implementación fueron:

- Se interconectaron los enrutadores ERX de OTF a los Conmutadores de Contenidos de los nodos de Washington y San Isidro mediante enlaces FastEthernet.
- El trafico IP que OTF provee a la Red IP/MPLS es de 40MB por el Nodo de Washington y 40 MB por el nodo de San Isidro.
- Se estableció en forma redundante sesiones IBGP en los enrutadores ERX de Telefónica del Perú para encaminar el trafico IP hacia la Red IP/MPLS de AS 6147.
- Se implemento un enlace STM-1 POS o FE Internodal de respaldo entre los nodos de Washington y San Isidro ante una posible contingencia.
- Se encaminará tráfico de subida y bajada a Internet.
- Todo trafico IP que OTF encamina en forma local es a través de los actuales enlaces STM-1 ATM.

Los equipos instalados en la red caché (Conmutador de Contenidos y Servidores Caché), así como el Enrutador DI, y TG han quedado configurados de acuerdo a su Sistema Operativo propietario, recordando que estos deben tener configurado tanto los servicios de los clientes de TEmpresas como el servicio Speedy para el cliente Telefónica del Perú. A manera de ejemplo presentamos la configuración de los equipos que conforman la Red caché del nodo de San Isidro:

Configuración de los CSS:

```
!************************** GLOBAL **************************
***Aquí se define el área OSPF en el que se encuentra el Conmutador de Contenidos que en este caso es de área 4

ospf as-boundary
ospf advertise 200.37.84.0 255.255.255.224
ospf router-id 172.20.7.2
ip redundancy
no restrict web-mgmt
no restrict xml
persistence reset remap
bypass persistence disable
ospf area 0.0.0.4
ospf enable
sntp server 192.168.102.101 version 1
snmp trap-source specified 192.168.101.106
virtual authentication primary tacacs
acl enable
snmp trap-type enterprise
snmp auth-traps
snmp community mplschimu read-only
snmp community mplschavin read-write
snmp contact "Centro Gestion de Red"
snmp location "Nodo San Isidro - Av. Camino Real 208 4to. piso"
snmp trap-host 192.168.102.10 mplschimu
logging buffer 4096
logging commands enable
logging subsystem redundancy level notice-5
logging subsystem ospf level notice-5
logging subsystem chassis level notice-5
ip route 1.1.1.1 255.255.255.255 blackhole
ip route 192.168.101.0 255.255.255.0 192.168.102.100 1
tacacs-server 192.168.102.10 51 primary
tacacs-server 192.168.101.10 51
tacacs-server 192.168.101.15 51
tacacs-server key qhhfseodrfddddcg
tacacs-server account non-config
tacacs-server account config
tacacs-server authorize config
tacacs-server timeout 3

!************************ INTERFACE ************************
***Aquí definimos las interfaces que irán conectados a la VLAN de agregación
interface 1/1
bridge vlan 2
description " --- SISDI1 GE1/0/0 --- "
redundancy-phy
interface 2/5
phy 100Mbits-FD
bridge vlan 2
description "ERX 14400 OTF"
```

```
!************************** CIRCUIT **************************
***Aquí definimos las VLANs de Agregación, Gestión, Caché y de Replicación
circuit VLAN2
redundancy
description "VLAN DE AGREGACION"
ip address 172.20.7.2 255.255.255.224
ospf
ospf priority 0
ospf enable
ospf area

circuit VLAN5
description "VLAN DE GESTION"
ip address 192.168.102.106 255.255.255.0

circuit VLAN3
description "VLAN DE CACHES"
redundancy
ip address 200.37.84.1 255.255.255.224

circuit VLAN4
description "VLAN DE REPLICACION"
ip address 192.168.90.1 255.255.255.252
redundancy-protocol

!************************** SERVICE **************************
***Definición de Direcciones IP, puertos y protocolos de los Servidores Caché, así mismo
definición del repositorio donde serán enviados los VIRUS informáticos que detecten los
Conmutadores de Contenidos.
service SISCF1
type transparent-cache
ip address 200.37.84.2
port 80
protocol tcp
active

service SISCF2
type transparent-cache
ip address 200.37.84.3
port 80
protocol tcp
active

service TACHO-VIRUS
ip address 1.1.1.1
keepalive type none
active
!************************** EQL **************************
***Aquí se define las extensiones de los objetos que serán copiados en los servidores
caché
eql CACHEABLE
description "This EQL contains extensions of cacheable content"
extension pdf "Acrobat"
extension fdf "Acrobat Forms Document"
```

```
extension au "Sound audio/basic"
extension bmp "Bitmap Image"
extension z "Compressed data application/x-compress"
extension gif "GIF Image image/gif"
extension html "Hypertext Markup Language text/html"
extension htm
extension js "Java script application/x-javascript"
extension mocha
extension jpeg "JPEG image image/jpeg"
extension jpg
extension jpe
extension jfif
extension pjpeg
extension pjp
extension mp2 "MPEG Audio audio/x-mpeg"
extension mpa
extension abs
extension mpeg "MPEG Video video/mpeg"
extension mpg
extension mpe
extension mpv
extension vbs
extension m1v
extension pcx "PCX Image"
extension txt "Plain text text/plain"
extension text
extension mov "QuickTime video/quicktime"
extension tiff "TIFF Image image/tiff"
extension tar "Unix Tape Archive application/x-tar"
extension avi "Video for Windows video/x-msvideo"
extension wav "Wave File audio/x-wav"
extension gz "application/x-gzip"
extension zip "ZIP file application/x-zip-compressed"

!********** NQL **********
***Definición de los grupos de IPs que acceden a la red Caché (nql de Caches, POP Local, Remoto y de Servicios) . También se definen los grupos de IPs Asimétricos que serán encaminados directamente a los servidores web internacionales..

nql ASIMETRICO
description "IPs CLIENTES BYPASS"
ip address 200.60.91.0 255.255.255.224


nql CACHES
description "IPs de CACHES"
ip address 192.168.101.0 255.255.255.0
ip address 192.168.102.0 255.255.255.0
ip address 200.37.84.0 255.255.255.224
ip address 200.37.238.0 255.255.255.224

nql GESTION
ip address 192.168.101.0 255.255.255.0
ip address 192.168.102.0 255.255.255.0
```

ip address 200.37.10.128 255.255.255.192
ip address 200.48.10.0 255.255.255.192
ip address 10.125.25.0 255.255.255.0

nql POPs-LOCAL
ip address 200.37.195.0 255.255.255.0
ip address 200.48.97.0 255.255.255.0
ip address 200.48.79.0 255.255.255.0
ip address 200.10.75.0 255.255.255.0

nql POPs-REMOTOS
ip address 200.37.0.0 255.255.0.0
ip address 200.48.0.0 255.255.0.0
ip address 200.60.0.0 255.255.0.0
ip address 200.106.0.0 255.255.128.0
ip address 200.107.128.0 255.255.128.0
ip address 199.229.76.0 255.255.255.0
ip address 200.0.110.0 255.255.255.0
ip address 200.0.169.0 255.255.255.0
ip address 200.0.170.0 255.255.254.0
ip address 200.0.172.0 255.255.254.0
ip address 200.4.192.0 255.255.192.0
ip address 200.10.64.0 255.255.224.0
ip address 200.10.130.0 255.255.254.0
ip address 200.10.188.0 255.255.255.0
ip address 200.11.48.0 255.255.240.0
ip address 200.16.0.0 255.255.248.0
ip address 206.138.104.0 255.255.248.0
ip address 207.17.216.0 255.255.248.0
ip address 207.79.208.0 255.255.240.0

nql SERVICIOS
ip address 172.20.7.0 255.255.255.224
ip address 172.20.6.0 255.255.255.224

*!********** HEADER FIELD GROUP **********
***Definición de los nombres y extensión de los objetos a rechazar que irán al repositorio de VIRUS*

header-field-group .ida
header-field .ida request-line contain ".ida"

header-field-group cmd.exe
header-field .ida request-line contain "cmd.exe"

header-field-group default.ida
header-field .ida request-line contain "default.ida"

header-field-group root.exe
header-field .ida request-line contain "root.exe"

header-field-group x.ida
header-field .ida request-line contain "x.ida"

```
!************************** OWNER **************************
***Definición de las 2 alternativas de obtener una pagina web (ya sea directamente al
servidor web mediante la propiedad BYPASS o mediante el servidor CACHE), también se
define las reglas contra virus y sus extensiones como objetos.

owner CACHE
content BYPASS
application bypass
protocol tcp
port 80
url "/*"
active

content CACHEABLE
protocol tcp
port 80
url "/*" eql CACHEABLE
add service SISCF2
balance domainhash
add service SISCF1
active

owner RULE-VIRUS

content block_.ida
protocol tcp
port 80
url "/*"
header-field-rule .ida weight 0
add service TACHO-VIRUS
active

content cmd.exe
protocol tcp
port 80
url "/*"
header-field-rule cmd.exe weight 0
add service TACHO-VIRUS
active



content default.ida
protocol tcp
port 80
url "/*"
header-field-rule default.ida weight 0
add service TACHO-VIRUS
active

content root.exe
protocol tcp
port 80
```

url "/"*
header-field-rule root.exe weight 0
add service TACHO-VIRUS
active

content x.ida
protocol tcp
port 80
url "/"*
header-field-rule x.ida weight 0
add service TACHO-VIRUS
active

*!*********** **ACL** **********
Definición de las listas de acceso a nivel de TCP , IP y de aplicación.
acl 10
clause 10 bypass tcp nql ASIMETRICO destination any
clause 15 bypass tcp any destination nql ASIMETRICO
clause 40 permit tcp any destination content RULE-VIRUS/block_.ida
clause 41 permit tcp any destination content RULE-VIRUS/default.ida
clause 42 permit tcp any destination content RULE-VIRUS/root.exe
clause 43 permit tcp any destination content RULE-VIRUS/cmd.exe
clause 44 permit tcp any destination content RULE-VIRUS/x.ida
clause 50 permit tcp any destination content CACHE/BYPASS
clause 81 deny tcp nql POPs-LOCAL destination nql CACHES eq http
clause 82 deny tcp nql POPs-LOCAL destination nql CACHES eq https
clause 83 deny tcp nql POPs-LOCAL destination nql CACHES eq smtp
clause 84 deny tcp nql POPs-LOCAL destination nql CACHES eq ftp
clause 86 deny tcp any destination nql CACHES eq http
clause 87 deny tcp any destination nql CACHES eq https
clause 88 deny tcp any destination nql CACHES eq smtp
clause 89 deny tcp any destination nql CACHES eq ftp
clause 90 deny tcp any destination nql CACHES eq 8080
clause 95 bypass tcp nql POPs-LOCAL destination nql POPs-REMOTOS
clause 96 permit tcp nql POPs-LOCAL destination content CACHE/CACHEABLE
clause 99 permit any any destination any
apply circuit-(VLAN2)

acl 30
clause 10 permit any any destination any
apply circuit-(VLAN3)

acl 40
clause 10 permit any any destination any
apply circuit-(VLAN4)

acl 50
clause 10 permit any nql GESTION destination nql CACHES
apply circuit-(VLAN5)

Configuración del SISDI1:

SISDI1#sh conf

```
version 12.0
no service pad
service tcp-keepalives-in
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname SISDI1

!Definimos aquí los accesos a la red por parte de los administradores de red
boot system flash disk0:c10k-p10-mz.120-25.S1.bin
boot system flash slot0:c10k-p10-mz.120-25.S1.bin
boot system flash c10k-p10-mz.120-25.S1.bin
boot bootldr bootflash:c10k-eboot-mz.120-25.S1.bin
redundancy
mode sso
logging rate-limit console all 10 except critical
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication login CGR local enable
aaa authentication enable default none
aaa authorization exec default tacacs+ none
aaa authorization commands 1 default tacacs+ none
aaa authorization commands 15 default tacacs+ none
aaa accounting exec default start-stop tacacs+
aaa accounting commands 1 default start-stop tacacs+
aaa accounting commands 15 default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
enable secret 5 $1$3GwZ$fF7THTdweHdUhQlL1urNN.
!
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
!
Definimos aquí las interfaces de red
card 1/0 1gigethernet-1
card 2/0 1gigethernet-1
card 3/0 6oc3pos-1
ip subnet-zero
no ip domain-lookup
!
Indicamos aquí las clases y accesos de los enrutadores ORX de Telefónica del Perú
class-map match-all D_ERX-SIS-OTF
match access-group name D_SIS-OTF
class-map match-all A_ERX-SIS-OTF
match access-group name A_SIS-OTF
!
Definimos aquí las politicas y clases de servicio de los Enrutadores ERX de OTF
policy-map D_INTERNET
class A_ERX-SIS-OTF
police 40000000 71680 107520 conform-action transmit exceed-action drop violate-action
drop
policy-map A_INTERNET
```

```
class D_ERX-SIS-OTF
police 40000000 71680 107520 conform-action transmit exceed-action drop violate-action
drop
!
no tag-switching ip propagate-ttl
tag-switching tdp router-id Loopback100
!
interface Loopback0
ip address 200.48.175.30 255.255.255.255
no ip directed-broadcast
!
interface Loopback100
ip address 200.48.175.156 255.255.255.255
no ip directed-broadcast
ip router isis BACKBONE
!
A partir de aquí configuramos las Interfaces de Red
interface FastEthernet0/0/0
description *** SW2924 FE0/12 ***
ip address 192.168.102.105 255.255.255.0
no ip directed-broadcast
full-duplex
cdp enable
!
interface GigabitEthernet1/0/0
description *** SISCS1 interface 1/1 ***
ip address 172.20.7.1 255.255.255.224
ip verify unicast reverse-path
no ip redirects
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
cdp enable
service-policy input A_INTERNET
service-policy output D_INTERNET
!
interface GigabitEthernet2/0/0
description *** SISCS2 interface 1/1 ***
ip address 172.20.7.33 255.255.255.224
ip verify unicast reverse-path
no ip redirects
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
cdp enable
!
interface POS3/0/0
description --- ENLACE STM-1 POS SISP1 4/5 ---
ip address 172.20.1.62 255.255.255.252
no ip directed-broadcast
ip router isis BACKBONE
encapsulation ppp
tag-switching ip
crc 32
```

```
cdp enable
pos framing sdh
pos flag s1s0 2
!
Definimos aquí los protocolos de  enrutamiento que será necesario usar para distribuir las solicitudes y entregas de las páginas web.
router ospf 6147
router-id 200.48.175.30
log-adjacency-changes
redistribute static subnets route-map STATICS
redistribute bgp 6147 subnets route-map REDES_OTF
network 172.20.7.0 0.0.0.31 area 4
network 172.20.7.32 0.0.0.31 area 4
network 200.48.175.0 0.0.0.127 area 4
default-information originate always
!
router isis BACKBONE
redistribute static ip route-map NET_LOOPBACKS
net 47.0000.c830.af9e.0200.00
is-type level-2-only
domain-password tdat9186
area-password tdat8130
metric-style wide
no hello padding point-to-point
log-adjacency-changes
!
router bgp 6147
no synchronization
bgp router-id 200.48.175.156
bgp log-neighbor-changes
bgp redistribute-internal
network 200.37.84.0 mask 255.255.255.224
network 200.60.31.96 mask 255.255.255.224
network 200.107.128.0
timers bgp 10 30
neighbor 200.48.175.130 remote-as 6147
neighbor 200.48.175.130 update-source Loopback100
neighbor 200.48.175.130 next-hop-self
neighbor 200.48.175.130 soft-reconfiguration inbound
neighbor 200.48.175.137 remote-as 6147
neighbor 200.48.175.137 update-source Loopback100
neighbor 200.48.175.137 next-hop-self
neighbor 200.48.175.137 soft-reconfiguration inbound
neighbor 200.48.175.137 route-map NETs_OTF in
neighbor 200.48.175.146 remote-as 6147
neighbor 200.48.175.146 update-source Loopback100
neighbor 200.48.175.146 next-hop-self
neighbor 200.48.175.146 soft-reconfiguration inbound
neighbor 200.48.175.146 route-map DEFAULT-ROUTE in
neighbor 200.48.175.153 remote-as 6147
neighbor 200.48.175.153 update-source Loopback100
neighbor 200.48.175.153 next-hop-self
neighbor 200.48.175.153 soft-reconfiguration inbound
neighbor 200.48.175.153 route-map NETs_OTF in
```

```
no auto-summary
!
ip classless
ip route 10.3.1.254 255.255.255.255 172.20.7.8
ip route 172.22.128.10 255.255.255.255 172.20.7.9
ip route 192.168.101.0 255.255.255.0 192.168.102.100
ip route 200.48.172.50 255.255.255.255 172.20.7.8
ip route 200.48.225.29 255.255.255.255 172.20.7.8
ip route 200.107.128.0 255.255.255.0 Null0 220 permanent
ip tacacs source-interface Loopback100
!
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/32
!
ip prefix-list IP_LOOPBACKS seq 5 permit 200.48.225.29/32
ip prefix-list IP_LOOPBACKS seq 10 permit 172.22.128.10/32
!
ip prefix-list REDES_OTF_SIS seq 5 permit 200.37.195.0/24
!
ip prefix-list TEMPO_OTF seq 5 permit 200.107.129.0/24 le 32
!
ip access-list extended A_SIS-OTF
permit ip any 200.37.195.0 0.0.0.255
permit ip any 200.107.129.0 0.0.0.255
ip access-list extended D_SIS-OTF
permit ip 200.37.195.0 0.0.0.255 any
permit ip 200.107.129.0 0.0.0.255 any
!
Definimos aquí los accesos de lista mediante IPs.
logging trap debugging
logging facility local1
logging source-interface Loopback100
logging 192.168.102.10
access-list 5 permit 10.125.25.0 0.0.0.255
access-list 5 permit 192.168.101.0 0.0.0.255
access-list 5 permit 192.168.102.0 0.0.0.255
access-list 5 permit 200.48.175.0 0.0.0.255
access-list 5 deny any
access-list 97 permit 192.168.101.14
access-list 97 permit 192.168.101.16
access-list 97 permit 10.3.1.254
access-list 97 deny any
access-list 98 permit 192.168.101.15
access-list 98 permit 192.168.102.10
access-list 98 permit 192.168.101.10
access-list 98 deny any
access-list 99 permit 192.168.101.15
access-list 99 permit 192.168.101.14
access-list 99 permit 192.168.102.10
access-list 99 permit 192.168.101.10
access-list 99 permit 192.168.101.28
access-list 99 permit 192.168.101.17
access-list 99 permit 192.168.101.16
access-list 99 permit 192.168.101.18
access-list 99 deny any
```

```
Definimos las políticas y jerarquías de envío de mensajes de gestión CDP (Protocolo de
Descubrimiento de Equipos Cisco) propietaria de CISCO
cdp run
route-map NETs_OTF permit 10
match ip address prefix-list REDES_OTF_SIS
set weight 200
!
route-map NETs_OTF permit 15
match ip address prefix-list TEMPO_OTF
set weight 200
!
route-map NETs_OTF deny 20
!
route-map DEFAULT-ROUTE permit 10
match ip address prefix-list DEFAULT
set local-preference 125
!
route-map DEFAULT-ROUTE permit 20
!
route-map NET_LOOPBACKS permit 10
match ip address prefix-list IP_LOOPBACKS
!
route-map REDES_OTF permit 10
match ip address prefix-list REDES_OTF_SIS
!
route-map REDES_OTF permit 15
match ip address prefix-list TEMPO_OTF
!
route-map DEFAULT permit 10
match ip address prefix-list DEFAULT
!
route-map STATICS permit 10
match ip address prefix-list IP_LOOPBACKS
!
Definimos aquí los traps o avisos SNMP que serán direccionados a los diferentes
elementos de Gestión
snmp-server view IPQosPol cbQosCMPostPolicyBitRate.1039.1040 included
snmp-server view IPQosPol cbQosCMPostPolicyBitRate.1047.1048 included
snmp-server community mplschimu RO 99
snmp-server community mplschavin RW 98
snmp-server community commOTFro view IPQosPol RO 97
snmp-server ifindex persist
snmp-server trap-source FastEthernet0/0/0
snmp-server location Jorge Basadre 592 6to Piso Oficina 609
snmp-server contact Jefatura de Planificacion
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps atm subif
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps syslog
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
```

```
snmp-server enable traps msdp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps bgp
snmp-server enable traps alarms
snmp-server host 192.168.102.10 mplschimu
snmp mib persist expression
tacacs-server host 192.168.102.10 key ipvpn
tacacs-server host 192.168.101.10 key ipvpn
tacacs-server host 192.168.101.15 key ipvpn
tacacs-server timeout 3
tacacs-server key ipvpn
!
line con 0
exec-timeout 30 0
login authentication CGR
line aux 0
exec-timeout 30 0
password 7 071F2D1E1E594B5545
login authentication CGR
line vty 0 4
access-class 5 in
exec-timeout 30 0
password 7 0831401C5949574740
length 0
!
ntp clock-period 17181169
ntp source Loopback100
ntp peer 200.48.175.129 prefer
ntp peer 200.48.175.145
end
```

Configuración del SISTG1:

```
SISTG1#sh conf
no tag-switching ip propagate-ttl
tag-switching tdp router-id Loopback100
!
Configuración de las intefaces de red
interface Loopback100
ip address 200.48.175.153 255.255.255.255
no ip directed-broadcast
ip router isis BACKBONE
!
interface FastEthernet0/0/0
ip address 192.168.102.102 255.255.255.0
no ip directed-broadcast
cdp enable
!
interface POS1/0/0
description --- ENLACE STM-1 POS SISP1 4/7 ---
ip address 172.20.1.54 255.255.255.252
```

```
no ip directed-broadcast
ip router isis BACKBONE
encapsulation ppp
tag-switching ip
crc 32
cdp enable
pos framing sdh
pos flag s1s0 2
!
interface POS1/0/1
description --- ENLACE STM-1 POS WASP1 4/6 ---
ip address 172.20.0.58 255.255.255.252
no ip directed-broadcast
ip router isis BACKBONE
encapsulation ppp
tag-switching ip
crc 32
cdp enable
pos framing sdh
pos flag s1s0 2
!
interface POS1/0/3
description --- ENLACE POS STM-1 GRTLIMLU1 POS3/0/0 ---
ip address 213.140.39.54 255.255.255.252
ip access-group ACLIN in
ip access-group VIRUSOUT3 out
no ip redirects
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
crc 16
pos framing sdh
pos flag s1s0 2
!
interface POS1/0/5
description --- ENLACE POS STM-1 WASTG1 POS1/0/5 ---
ip address 172.20.0.194 255.255.255.252
no ip directed-broadcast
encapsulation ppp
crc 32
cdp enable
pos framing sdh
pos flag s1s0 2
```

Definición de los protocolos de ruteo OSPF y BGP con sus respectivas rutas a considerar.

```
router isis BACKBONE
net 47.0000.c830.af99.0200.00
is-type level-2-only
domain-password tdat9186
area-password tdat8130
metric-style wide
no hello padding point-to-point
log-adjacency-changes
!
```

```
router bgp 6147
no synchronization
table-map RUTAS-AS6147
bgp router-id 200.48.175.153
bgp log-neighbor-changes
network 199.229.76.0
network 200.0.110.0
network 200.0.170.0 mask 255.255.254.0
network 200.0.172.0 mask 255.255.254.0
network 200.4.192.0 mask 255.255.224.0
network 200.4.224.0 mask 255.255.224.0
network 200.10.64.0 mask 255.255.224.0
network 200.10.130.0 mask 255.255.254.0
network 200.10.188.0
network 200.11.48.0 mask 255.255.240.0
network 200.16.0.0 mask 255.255.248.0
network 200.37.0.0 mask 255.255.224.0
network 200.37.32.0 mask 255.255.224.0
network 200.37.64.0 mask 255.255.224.0
network 200.37.96.0 mask 255.255.224.0
network 200.37.125.0
network 200.37.128.0 mask 255.255.224.0
network 200.37.160.0 mask 255.255.224.0
network 200.37.192.0 mask 255.255.224.0
network 200.37.224.0 mask 255.255.224.0
network 200.48.0.0 mask 255.255.224.0
network 200.48.32.0 mask 255.255.224.0
network 200.48.64.0 mask 255.255.224.0
network 200.48.96.0 mask 255.255.224.0
network 200.48.128.0 mask 255.255.224.0
network 200.48.160.0 mask 255.255.224.0
network 200.48.192.0 mask 255.255.224.0
network 200.48.224.0 mask 255.255.224.0
network 200.60.0.0 mask 255.255.224.0
network 200.60.32.0 mask 255.255.224.0
network 200.60.64.0 mask 255.255.224.0
network 200.60.96.0 mask 255.255.224.0
network 200.60.128.0 mask 255.255.224.0
network 200.60.160.0 mask 255.255.224.0
network 200.106.48.0 mask 255.255.240.0
network 200.107.128.0 mask 255.255.224.0
network 200.107.160.0 mask 255.255.224.0
network 206.138.104.0 mask 255.255.248.0
network 207.17.216.0 mask 255.255.248.0
network 207.79.208.0 mask 255.255.240.0
neighbor BGP_VPN peer-group
neighbor BGP_VPN remote-as 6147
neighbor BGP_VPN update-source Loopback100
neighbor BGP_VPN version 4
neighbor BGP_VPN next-hop-self
neighbor BGP_VPN default-originate
neighbor BGP_VPN soft-reconfiguration inbound
neighbor BGP_VPN route-map RUTACERO out
neighbor 200.48.175.130 peer-group BGP_VPN
```

```
neighbor 200.48.175.140 remote-as 6147
neighbor 200.48.175.140 update-source Loopback100
neighbor 200.48.175.140 route-reflector-client
neighbor 200.48.175.140 soft-reconfiguration inbound
neighbor 200.48.175.140 route-map NORUTAS in
neighbor 200.48.175.140 route-map NETs_OTF_WAS out
neighbor 200.48.175.146 peer-group BGP_VPN
neighbor 200.48.175.156 remote-as 6147
neighbor 200.48.175.156 update-source Loopback100
neighbor 200.48.175.156 route-reflector-client
neighbor 200.48.175.156 soft-reconfiguration inbound
neighbor 200.48.175.156 route-map NORUTAS in
neighbor 200.48.175.156 route-map NETs_OTF_SIS out
neighbor 200.48.225.28 remote-as 6147
neighbor 200.48.225.28 update-source Loopback100
neighbor 200.48.225.28 next-hop-self
neighbor 200.48.225.28 soft-reconfiguration inbound
neighbor 200.48.225.28 route-map SET_LP_OTF in
neighbor 200.48.225.28 route-map NORUTAS out
neighbor 200.48.225.29 remote-as 6147
neighbor 200.48.225.29 update-source Loopback100
neighbor 200.48.225.29 next-hop-self
neighbor 200.48.225.29 soft-reconfiguration inbound
neighbor 200.48.225.29 route-map SET_LP_OTF in
neighbor 200.48.225.29 route-map NORUTAS out
no auto-summary
!
Definiciones de las rutas estaticas
ip classless
ip route 0.0.0.0 0.0.0.0 213.140.39.53 100
ip route 10.111.222.1 255.255.255.255 Null0
ip route 10.111.222.2 255.255.255.255 Null0
ip route 192.168.101.0 255.255.255.0 192.168.102.100
ip route 199.229.76.0 255.255.255.0 Null0 210 permanent
ip route 200.0.110.0 255.255.255.0 Null0 210 permanent
ip route 200.4.192.0 255.255.224.0 Null0 210 permanent
ip route 200.4.224.0 255.255.224.0 Null0 210 permanent
ip route 200.10.64.0 255.255.224.0 Null0 210 permanent
ip route 200.10.130.0 255.255.254.0 Null0 210 permanent
ip route 200.10.188.0 255.255.255.0 Null0 210 permanent
ip route 200.11.48.0 255.255.240.0 Null0 210 permanent
ip route 200.16.0.0 255.255.248.0 Null0 210 permanent
ip route 200.37.0.0 255.255.224.0 Null0 210 permanent
ip route 200.37.32.0 255.255.224.0 Null0 210 permanent
ip route 200.37.64.0 255.255.224.0 Null0 210 permanent
ip route 200.37.96.0 255.255.224.0 Null0 210 permanent
ip route 200.37.128.0 255.255.224.0 Null0 210 permanent
ip route 200.37.160.0 255.255.224.0 Null0 210 permanent
ip route 200.37.192.0 255.255.224.0 Null0 210 permanent
ip route 200.37.224.0 255.255.224.0 Null0 210 permanent
ip route 200.48.0.0 255.255.224.0 Null0 210 permanent
ip route 200.48.32.0 255.255.224.0 Null0 210 permanent
ip route 200.48.64.0 255.255.224.0 Null0 210 permanent
ip route 200.48.96.0 255.255.224.0 Null0 210 permanent
```

```
ip route 200.48.128.0 255.255.224.0 Null0 210 permanent
ip route 200.48.160.0 255.255.224.0 Null0 210 permanent
ip route 200.48.192.0 255.255.224.0 Null0 210 permanent
ip route 200.48.224.0 255.255.224.0 Null0 210 permanent
ip route 200.60.0.0 255.255.224.0 Null0 210 permanent
ip route 200.60.32.0 255.255.224.0 Null0 210 permanent
ip route 200.60.39.255 255.255.255.255 Null0
ip route 200.60.64.0 255.255.224.0 Null0 210 permanent
ip route 200.60.96.0 255.255.224.0 Null0 210 permanent
ip route 200.60.128.0 255.255.224.0 Null0 210 permanent
ip route 200.60.142.146 255.255.255.255 Null0
ip route 200.60.160.0 255.255.224.0 Null0 210 permanent
ip route 200.60.174.22 255.255.255.255 Null0
ip route 200.106.48.0 255.255.240.0 Null0 210 permanent
ip route 200.107.128.0 255.255.224.0 Null0 210 permanent
ip route 200.107.160.0 255.255.224.0 Null0 210 permanent
ip route 206.138.104.0 255.255.248.0 Null0 210 permanent
ip route 207.17.216.0 255.255.248.0 Null0 210 permanent
ip route 207.79.208.0 255.255.240.0 Null0 210 permanent
ip tacacs source-interface Loopback100
!
ip prefix-list REDES_OTF_SIS seq 5 permit 200.37.195.0/24
ip prefix-list REDES_OTF_SIS seq 10 permit 200.4.245.0/24
ip prefix-list REDES_OTF_SIS seq 15 permit 200.48.226.0/24
ip prefix-list REDES_OTF_SIS seq 20 permit 200.48.228.0/24
ip prefix-list REDES_OTF_SIS seq 25 permit 200.48.231.0/24
!
ip prefix-list REDES_OTF_WAS seq 5 permit 200.48.34.0/24
ip prefix-list REDES_OTF_WAS seq 10 permit 200.48.97.0/24
ip prefix-list REDES_OTF_WAS seq 15 permit 200.37.30.0/24
ip prefix-list REDES_OTF_WAS seq 20 permit 200.48.29.0/24
ip prefix-list REDES_OTF_WAS seq 25 permit 200.48.79.0/24
!
Definición de la lista de acceso en base a la IP y Puerto TCP
logging trap debugging
logging facility local1
logging source-interface Loopback100
logging 192.168.102.10
access-list 1 permit 0.0.0.0
access-list 1 deny any
access-list 5 permit 200.37.10.155
access-list 5 permit 192.168.101.0 0.0.0.255
access-list 5 permit 200.48.10.0 0.0.0.31
access-list 5 permit 200.37.145.96 0.0.0.31
access-list 5 permit 200.48.175.0 0.0.0.255
access-list 5 permit 206.138.105.64 0.0.0.31
access-list 5 permit 200.60.107.96 0.0.0.15
access-list 5 permit 200.37.10.128 0.0.0.63
access-list 5 permit 192.168.102.0 0.0.0.255
access-list 5 permit 10.125.25.0 0.0.0.255
access-list 5 deny any
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 deny 172.16.0.0 0.15.255.255
access-list 10 deny 192.168.0.0 0.0.255.255
```

```
access-list 10 deny 192.0.2.0 0.0.0.255
access-list 10 deny 224.0.0.0 31.255.255.255
access-list 10 deny 127.0.0.0 0.255.255.255
access-list 10 permit any
access-list 98 permit 192.168.101.15
access-list 98 permit 192.168.102.10
access-list 98 permit 192.168.101.10
access-list 98 deny any
access-list 99 permit 192.168.101.15
access-list 99 permit 192.168.101.14
access-list 99 permit 192.168.102.10
access-list 99 permit 192.168.101.10
access-list 99 permit 192.168.101.28
access-list 99 permit 192.168.101.17
access-list 99 permit 192.168.101.16
access-list 99 permit 192.168.101.18
access-list 99 permit 192.168.101.35
access-list 99 permit 200.48.10.26
access-list 99 permit 200.60.107.101
access-list 99 permit 200.60.107.98
access-list 99 deny any
access-list 180 deny ip 200.10.64.0 0.0.31.255 any
access-list 180 deny ip 207.79.208.0 0.0.15.255 any
access-list 180 deny ip 200.4.192.0 0.0.63.255 any
access-list 180 deny ip 200.37.0.0 0.0.255.255 any
access-list 180 deny ip 200.48.0.0 0.0.255.255 any
access-list 180 deny ip 200.16.0.0 0.0.7.255 any
access-list 180 deny ip 200.10.130.0 0.0.1.255 any
access-list 180 deny ip 200.11.48.0 0.0.15.255 any
access-list 180 deny ip 200.10.188.0 0.0.0.255 any
access-list 180 deny ip 200.1.177.0 0.0.0.255 any
access-list 180 deny ip 200.1.178.0 0.0.1.255 any
access-list 180 deny ip 200.1.180.0 0.0.3.255 any
access-list 180 deny ip 200.0.110.0 0.0.0.255 any
access-list 180 deny ip 200.0.170.0 0.0.1.255 any
access-list 180 deny ip 200.0.172.0 0.0.1.255 any
access-list 180 deny ip 199.229.76.0 0.0.0.255 any
access-list 180 deny ip 200.60.0.0 0.0.255.255 any
access-list 180 deny ip 200.106.32.0 0.0.31.255 any
access-list 180 permit ip any any
```

Definimos las políticas y jerarquías de envío de mensajes de gestión CDP (Protocolo de Descubrimiento de Equipos Cisco) propietaria de CISCO

```
cdp run
route-map SET_LP_OTF permit 10
set weight 200
!
route-map NETs_OTF_WAS permit 10
match ip address prefix-list REDES_OTF_WAS
set ip next-hop 172.20.6.8
!
route-map NETs_OTF_WAS deny 30
```

```
!
route-map NETs_OTF_SIS permit 20
match ip address prefix-list REDES_OTF_SIS
set ip next-hop 172.20.7.8
!
route-map NETs_OTF_SIS deny 30
!
route-map NORUTAS deny 10
!
Definimos aquí los traps o avisos SNMP que serán diseccionados a los diferentes
elementos de Gestión
snmp-server community mplschimu RO 99
snmp-server community mplschavin RW 98
snmp-server trap-source Loopback100
snmp-server location Nodo San Isidro Piso 4
snmp-server contact Centro Gestion de Red
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps atm subif
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps syslog
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps msdp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps bgp
snmp-server enable traps alarms
snmp-server host 192.168.102.10 mplschimu
tacacs-server host 192.168.101.10 key ipvpn
tacacs-server host 192.168.102.10 key ipvpn
tacacs-server host 192.168.101.15 key ipvpn
tacacs-server timeout 3
tacacs-server key ipvpn
!
ntp clock-period 17181139
ntp source Loopback100
ntp peer 200.48.175.129 prefer
ntp peer 200.48.175.145
end
```

b. Segunda Fase

En la Segunda fase del proyecto se implemento las Redes Caché en los nodos de Trujillo, Arequipa, Miraflores y Monterrico, esta implementación también consistió de la instalación de la planta externa, del cableado estructurado y del acondicionamiento del local donde quedaron ubicados los equipos (ver figura 3.6 y 3.7). La implementación de la red tanto en los nodos de Trujillo y Arequipa es muy similar tal como se puede observar en las topologías de las figuras 3.8 y 3.9, y cuyo proceso de instalación y configuración se describen a continuación:

- Interconexión del Enrutador proveedor de borde PE (AREPE1 o TRUPE1) con el enrutador proveedor (AREP1 o TRUP1) de cada ciudad con un enlace de fibra STM-1 para de ahí establecer 2 enlaces E3 hacia los enrutadores proveedores de los nodos de San Isidro y Washington (WASP1 y SISP1).
- Interconexión del Enrutador PE (AREPE1 o TRUPE1) con el Conmutador de Contenidos mediante enlaces redundados PortChannel (E1). Aquí se utilizaron 2 enlaces que van a un único Conmutador de Contenidos que se ha instalado denominado Maestro. En este Conmutador de Contenidos el enlace Maestro utiliza una única VLAN cuando se conectan a los Enrutadores de Internet (ARERI o TRURI) que es la VLAN de Agregación.
- Las VLAN´s que tiene definido el Conmutador de Contenidos en estas ciudades son 2: VLAN de Agregación (Que contiene a los Enrutadores PE (AREPE1 o TRUPE1) y a los Enrutadores RI (ARERI o TRURI)) y VLAN de Caches que se encargarán de la conexión con los Servidores Caché.
- Se ha definido Enrutamiento OSPF en el Conmutador de Contenidos para trasladar las rutas contenidas en los Enrutadores de Internet (ARERI o TRURI) al Enrutador PE (AREPE1 o TRUPE1).
- Se estableció sesiones IBGP en los Enrutadores PE (ARQPE1 o TRUPE1) para encaminar el trafico que viene de los Conmutadores de Contenidos hacia los Enrutadores Puerta de Salida (SISTG o WASHTG) a través del AS 6147 (Sistema Autónomo) de la Red IP/MPLS.
- Así mismo se han establecido sesiones IBGP en los Enrutadores Puerta de Salida (SISTG o WASHTG) para encaminar el tráfico hacia todos los Enrutadores PE (ARQPE1 o TRUPE1) para que estos luego lo deriven a los Enrutadores RI (ARERI o TRURI).
- Los Enrutadores PE (ARQPE1 o TRUPE1) se han configurado de tal manera que se respete las etiquetas asignadas en los Enrutadores RI, estas etiquetas permiten diferenciar en velocidad y saturación los servicios de Internet

contratados por los clientes, esta diferenciación de los servicios se establece también en las políticas de prioridad definidas en la Red IP/MPLS.

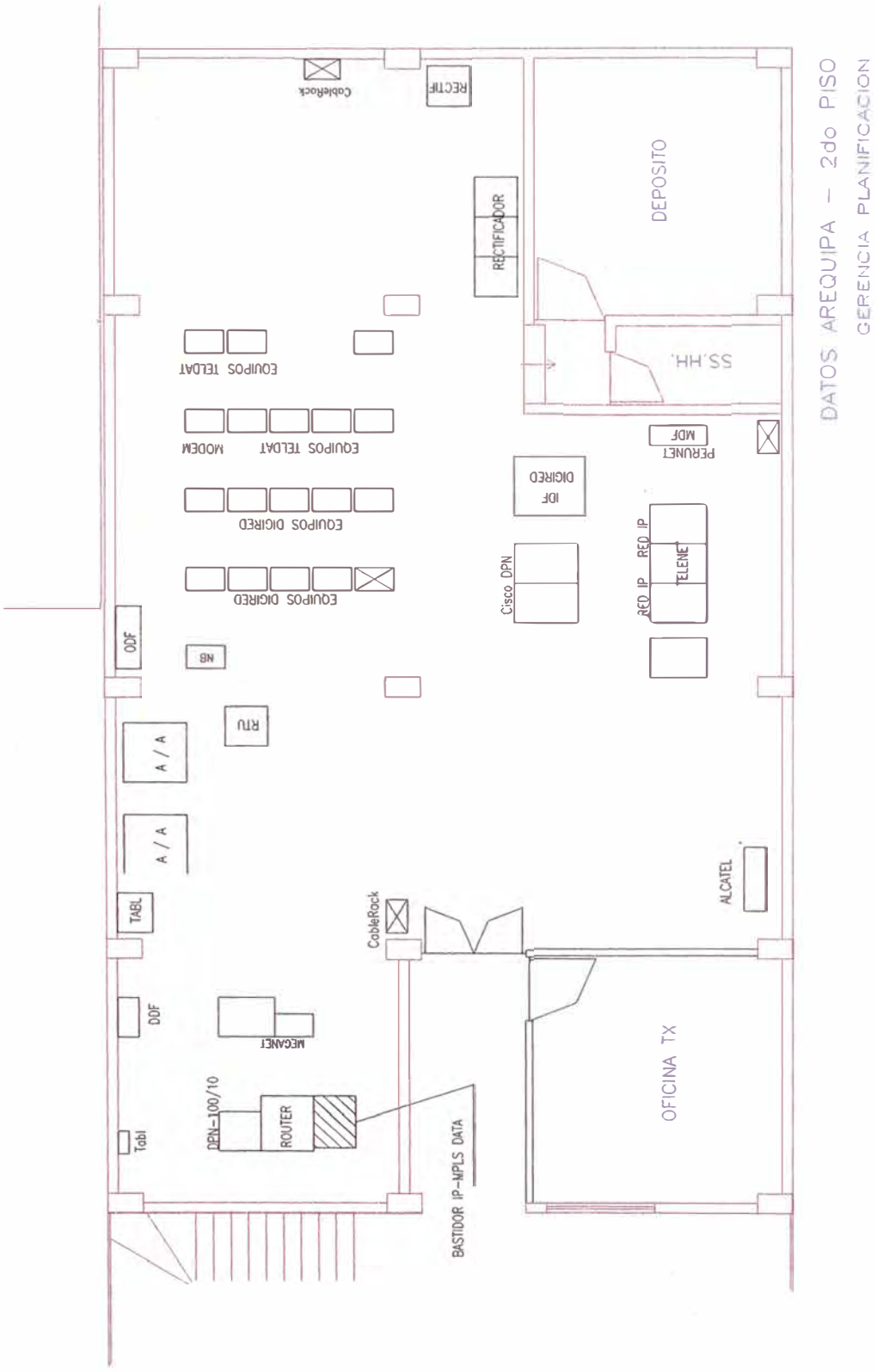


Figura 3.6 Plano de Ubicación de la Red Caché en el Nodo de Arequipa

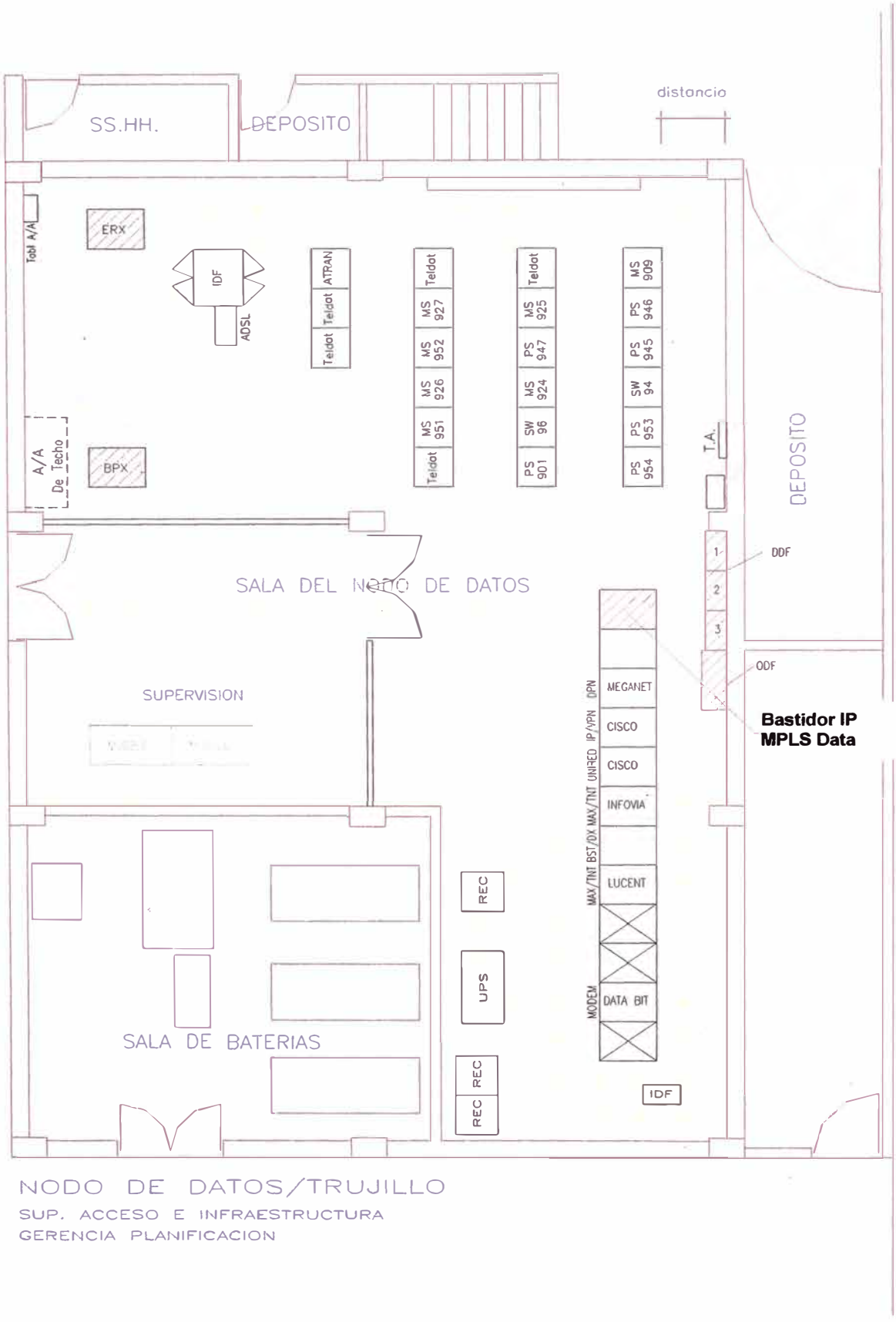


Figura 3.7 Plano de Ubicación de la Red Caché en el Nodo de Trujillo

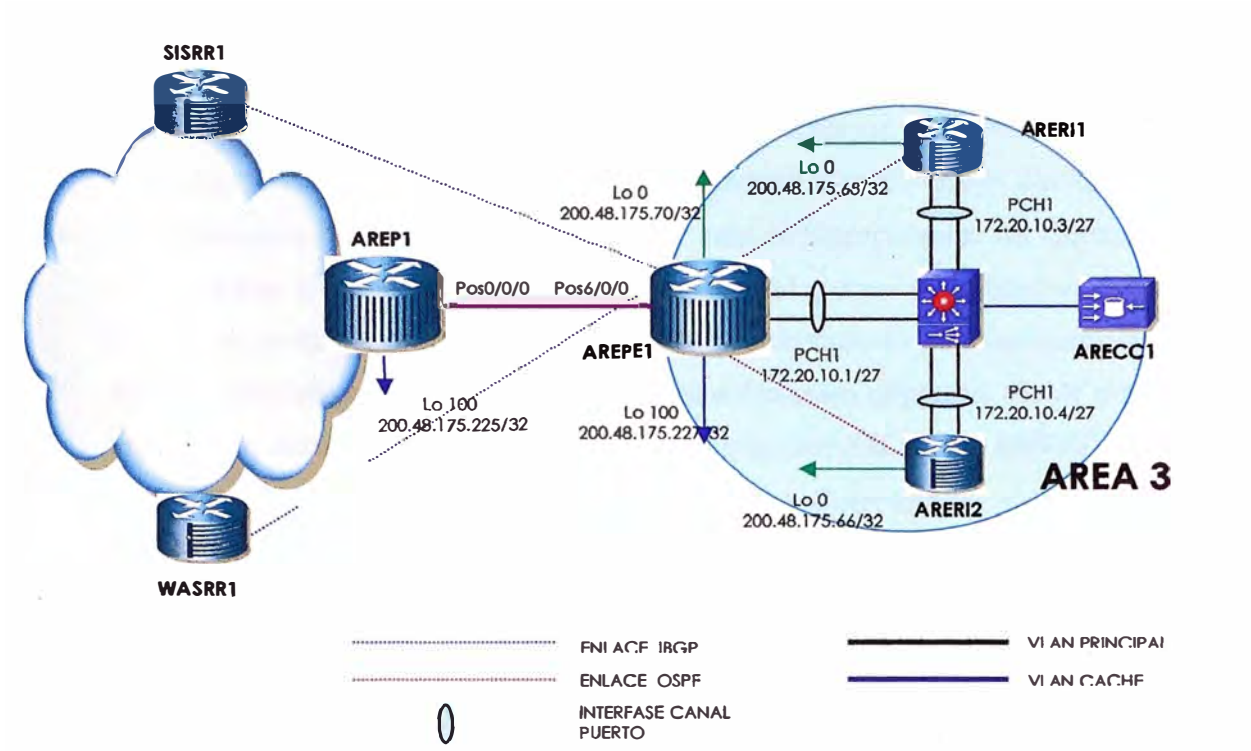


Figura 3.8 Topología Final de la Red Caché en el Nodo de Arequipa

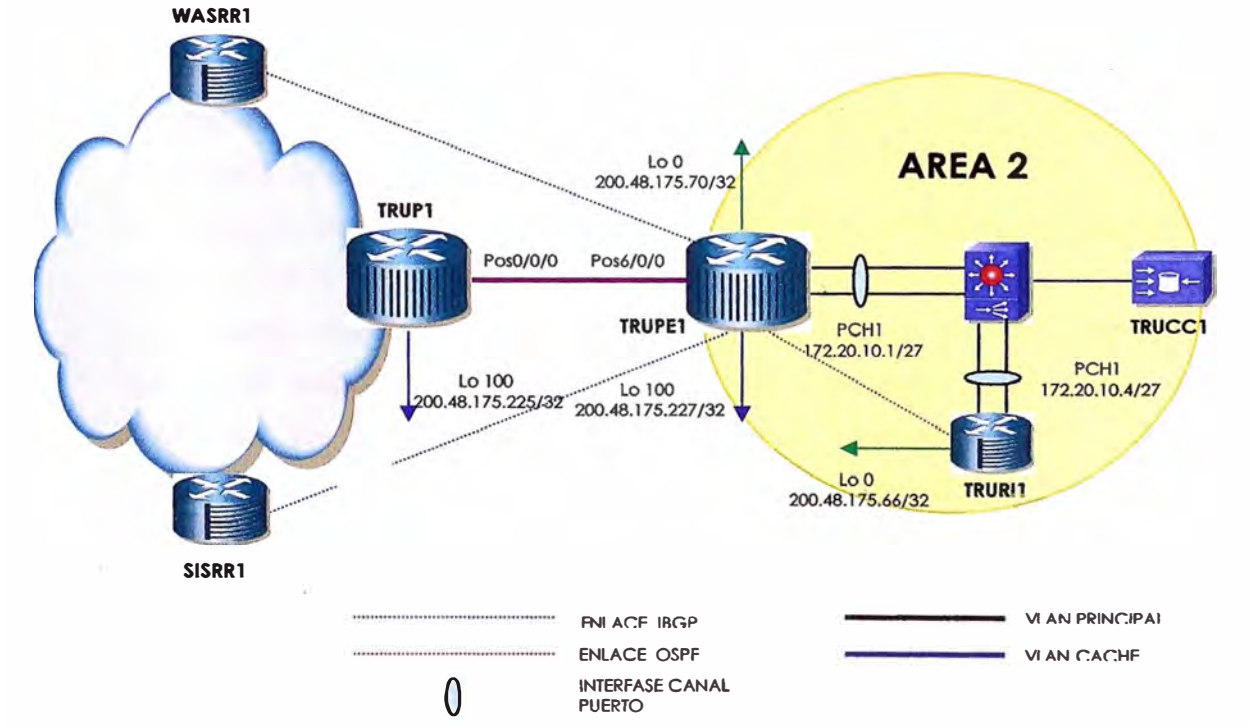


Figura 3.9 Topología Final de la Red Caché en el Nodo de Trujillo

La implementación de la red de Monterrico y Miraflores quedo tal como se puede observar en las topologías de las figuras 3.10 (la topología de estos nodos son iguales), y cuyo proceso de instalación y configuración se describen a continuación:

- Interconexión del Enrutador Distribuidor de Internet (MONDI o MIRDI) con el Enrutador Proveedor (MONP o MIRP) mediante una conexión Optica POS STM -1
- Interconexión del Enrutador Distribuidor con el Conmutador de Contenidos (CSS) redundados mediante enlaces PortChannel (E1), aquí se utilizaron 2 enlaces que van a un único Conmutador de Contenidos instalado denominado Maestro. En este Conmutador de Contenidos el enlace Maestro utiliza la VLAN de Agregación cuando se conectan a los Enrutadores de Internet (MONRI o MIRRI).
- La única VLAN que esta configurada en este Conmutador de Contenidos es la VLAN de Agregación (Que conecta a los Enrutadores de Internet (MONRI o MIRRI)) y esto debido a que en este nodo no existe servidores caché, ni redundancia en el Conmutador de Contenidos, en este caso todas las direcciones de los clientes alojados en estos nodos son reenviados a las redes caché de San Isidro y Washington.
- Se ha definido Enrutamiento OSPF en el Conmutador de Contenidos para trasladar las rutas contenidas en los Enrutadores de Internet (MONRI o MIRRI) al Enrutador Distribuidor (MONDI o MIRDI).
- Se estableció sesiones IBGP en los Enrutadores Distribuidor (MONDI o MIRDI) para encaminar el trafico que viene de los Conmutadores de Contenidos hacia los Enrutadores Puerta de Salida (SISTG y WASHTG) a través del AS 6147 (Sistema Autónomo) de la Red IP/MPLS.
- Así mismo se han establecido sesiones IBGP en los Enrutadores Puerta de Salida (SISTG y WASHTG) para encaminar el tráfico de entrada hacia todos los Enrutadores Distribuidor de San Isidro y Washington (SISDI y WASHDI), para que estos luego lo deriven a sus propios servidores caché, que luego de almacenar los contenidos reenviaran dichos contenidos a los Enrutadores Distribuidor de Miraflores y Monterrico (MONDI o MIRDI) para que de ahí sean derivados a los Enrutadores de Internet respectivos(MONRI o MIRRI).
- En los Enrutadores Distribuidor (MONDI o MIRDI) se ha configurado de tal manera que respete las etiquetas asignadas en los Enrutadores RI. Estas etiquetas permiten diferenciar en velocidad y saturación los servicios de Internet contratados por los clientes, esta diferenciación de los servicios se establece en las políticas de prioridad definidas en la Red IP/MPLS.

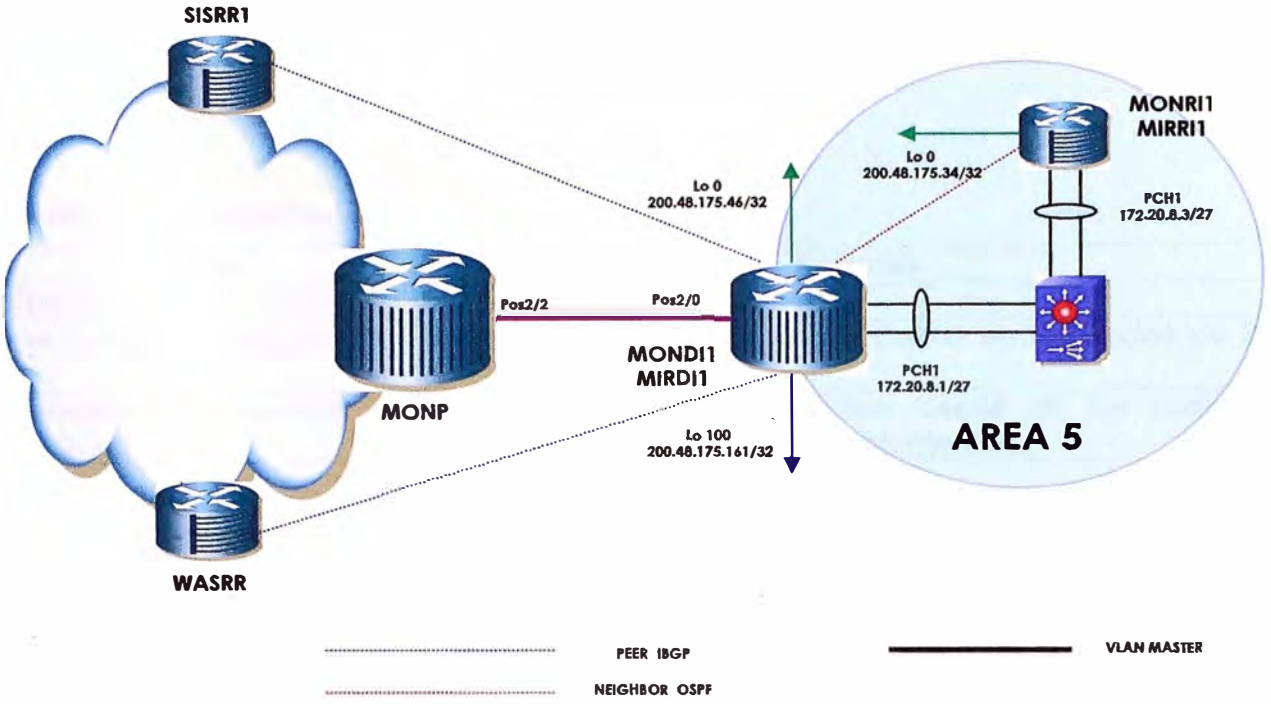


Figura 3.10 Topología Final de la Red Caché en los Nodos de Monterrico y Miraflores

3.3 Recursos Humanos:

Para la implementación de este proyecto se contó con la ayuda de Ingenieros de Telefónica Empresas capacitados en las Areas de Planificación de Red en los niveles CCNP y CCIEE, así mismo para la elaboración de las estadísticas de monitoreo se tuvo el apoyo de Ingenieros programadores de páginas web expertos en PHP, Mysql y PERL, para lo cual adjuntamos sus nombres y cargos respectivos en la tabla

Para la implementación de la planta externa y cableado estructurado se tuvo el valioso apoyo de las Empresas de instalación contratadas por Telefónica Empresas.

Tabla 3.5 Relación del Personal de TEmpresas

Nombres y Apellidos	Cargo
Luis Quispe Oncoy - Jefe de Proyecto	Ingeniero Planificador de Red, experto en Redes CISCO
Juan Espinoza Borda	Ingeniero Planificador de Red, experto en instalación de redes de datos
Juan Ernesto Higa	Ingeniero Programador de aplicativos web para redes de datos
Jhonn Arequipeño La Rosa Sánchez	Becario en el área de Planificación de Red y Nuevos Servicios

3.4 Tiempo de Ejecución

La implementación de este proyecto se desarrollo en 2 fases, tal como lo indica la siguiente tabla:

Tabla 3.6 Cronograma General de Implementación

Fechas	Labores
Enero – Febrero 2003	Provisión de Equipos
Marzo a Setiembre 2003	Implementación de las Redes Caché en los Nodos de San Isidro y Washington.
Setiembre a Noviembre del 2003	Implementación de las Redes Caché en los nodos de Arequipa, Trujillo, Miraflores y Monterrico.

Se podrá encontrar mayor detalle técnico del direccionamiento IP y de las VLANs de las redes caché implementadas en el ANEXO A del informe.

CAPITULO IV
VERIFICACION DE RESULTADOS

4.1 Análisis y Supervisión de Variables y Resultados

Analizando los objetivos por cumplir de este proyecto encontramos que el parámetro de retardo de acceso a las páginas iba a ser un parámetro muy difícil de medir debido a que este se encontraba en un rango de tiempo cercanos a los milisegundos, así que hemos decidido por conveniente analizar el parámetro de consumo de ancho de banda, para lo cual se ha desarrollado interfaces web de monitoreo para poder observar si es que se llega a ahorrar el 20% de ahorro propuesto.

Como podemos observar en este gráfico se llega a comprobar el ahorro propuesto que se encuentra en un promedio del 15%, tal como podemos observar en la figura 4.1, este ahorro es el total de los 6 nodos caché implementados.

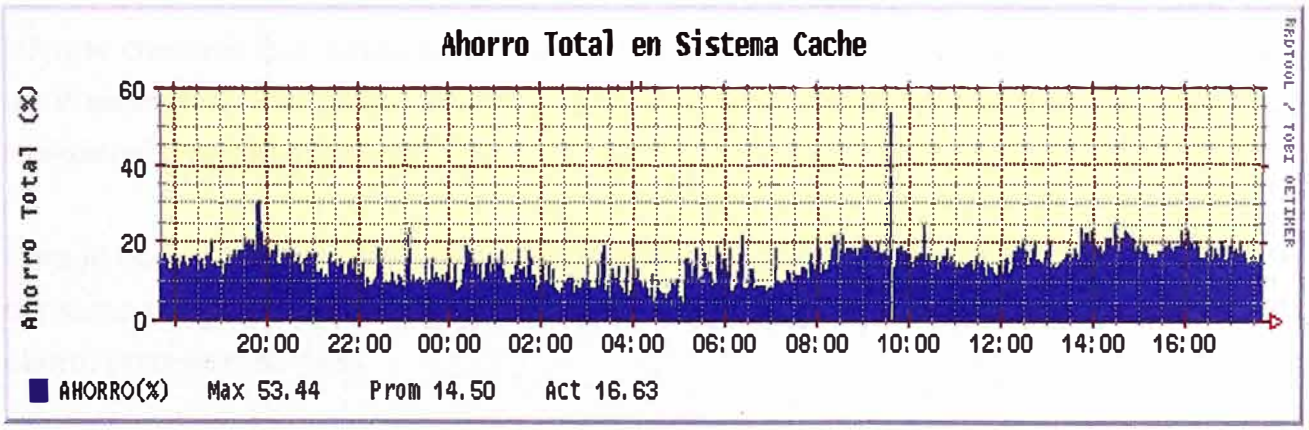


Figura 4.1 Ahorro Total de todos los Nodos Caché

Este resultado se obtiene de la división del tráfico en tiempo real total cursado en el enlace Enrutador DI – Conmutador de Contenidos de todos los nodos caché entre el tráfico en tiempo real cursado de todos los servidores caché de todos los nodos (Enlace Conmutador de Contenidos – Servidor Caché) tal como se muestra en la fórmula 4.1

$$Porcentaje\ Ahorro = \frac{TráficoServidorCaché\ \&\ ConmutadorContenido_{Tiempo\ Real}}{TráficoEnrutadorDI\ \&\ ConmutadorContenidos_{Tiempo\ Real}} x100\% \quad \textbf{(4.1)}$$

En el gráfico 4.2 (izquierdo) podrán observar el consumo total de ancho de banda a nivel de todos los enlaces que hay entre el Enrutador DI y su respectivo Conmutador de Contenidos. El gráfico 4.2 de la derecha muestra el consumo total de ancho de banda que hay entre el conmutador de contenidos y los servidores caché, de la división de estas 2 cantidades podemos saber el total ahorrado que se muestra en la figura 4.1.

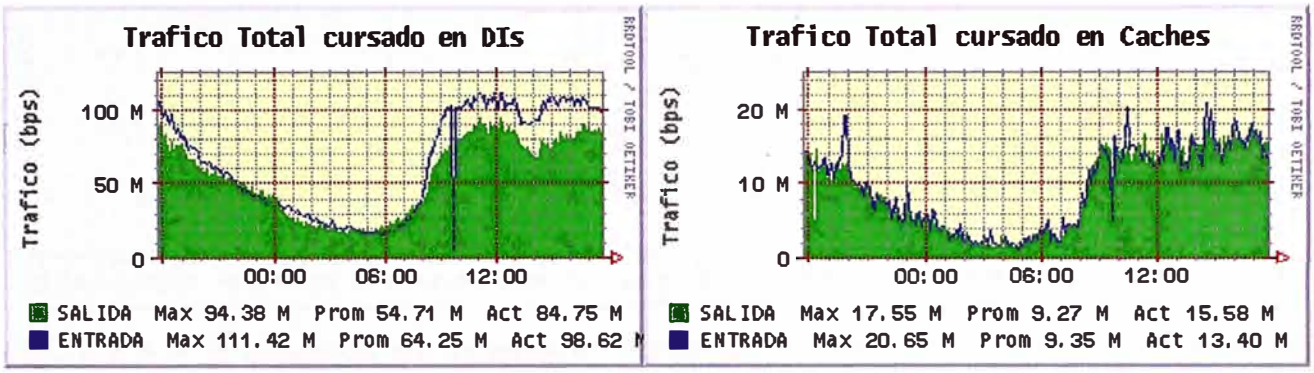


Figura 4.2 Consumo de Ancho de Banda de los enlaces DI y de los Enlaces de los servidores caché.

En los gráficos anteriores hemos mostrado el ahorro del total realizado por las redes caché, pero también debemos observar el ahorro sucedido en cada nodo, para este informe creemos que bastará con colocar los consumos de ancho de banda de los nodos de Washington, San Isidro, Trujillo y Arequipa pues al final de todo son los nodos que realizan el proceso de caché.

Para el nodo de Washington, podemos observar las 3 figuras siguientes: La de ahorro del consumo del ancho de banda de este nodo (Fig. 4.3), en la que observamos que hay un ahorro promedio de 15%.

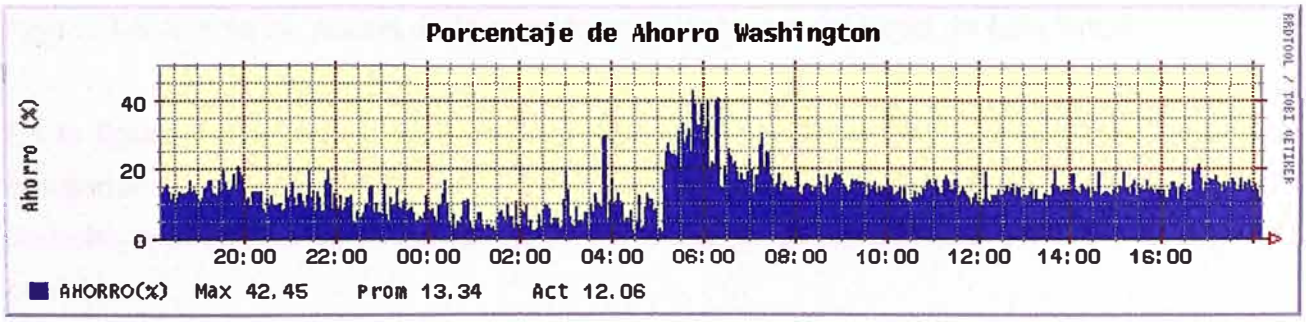


Figura 4.3 Ahorro de Ancho de Banda de la Red Caché del nodo de Washington

En la figura 4.4 al lado izquierdo observamos el consumo de ancho de banda entre el enrutador distribuidor WASDI y el Conmutador de Contenidos WASCS, mientras que al lado derecho mostramos el tráfico entre el conmutador de contenidos WASCS y el servidor caché.

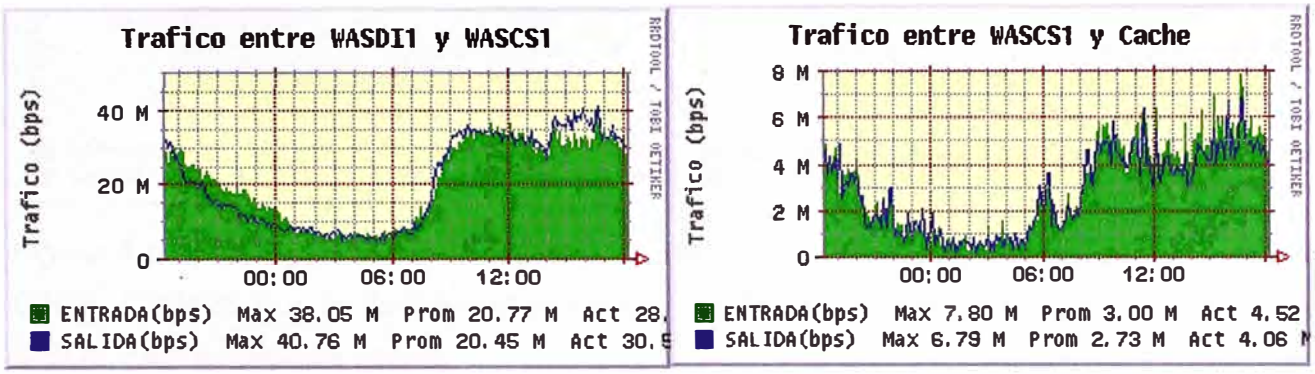


Figura 4.4 A la izquierda se muestra el Consumo de Ancho de Banda de los enlaces WASDI y WASCS y a la derecha consumo del Ancho de banda de los Enlaces entre WASCS y los servidores caché.

Para el nodo de San Isidro, podemos observar las 3 figuras siguientes: La de ahorro del consumo del ancho de banda de este nodo (Fig. 4.5), en la que observamos que hay un ahorro promedio de 13%.

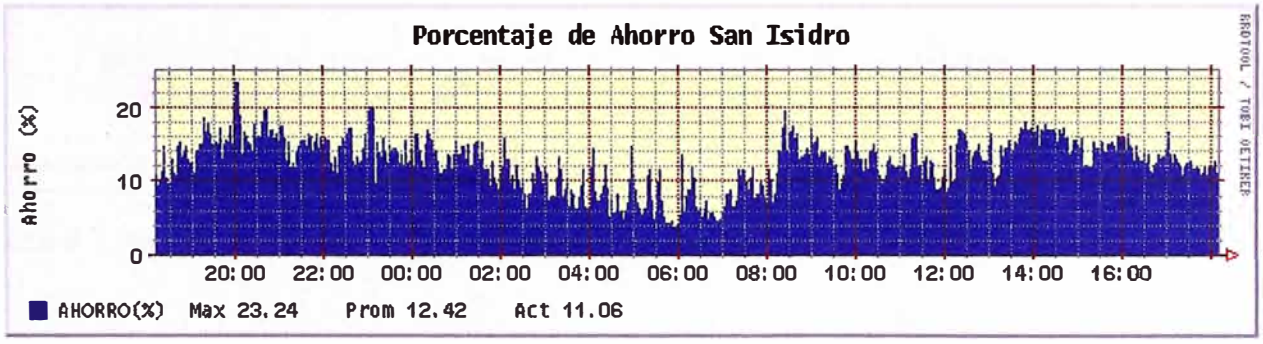


Figura 4.5 Ahorro de Ancho de Banda de la Red Caché del nodo de San Isidro.

En la figura 4.6 al lado izquierdo observamos el consumo de ancho de banda entre el enrutador distribuidor SISDI y el Conmutador de Contenidos SISCS, mientras que al lado derecho mostramos el tráfico entre el conmutador de contenidos SISCS y el servidor caché.

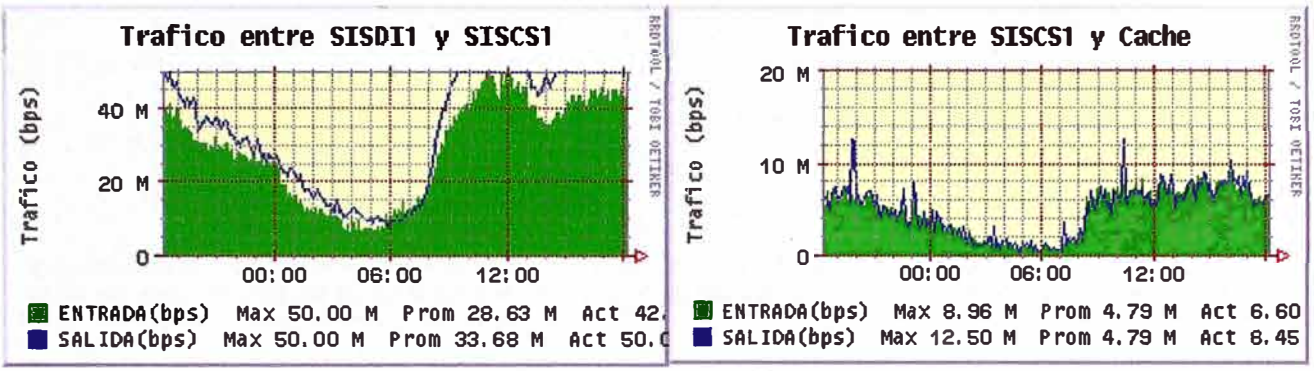


Figura 4.6 A la izquierda se muestra el Consumo de Ancho de Banda de los enlaces SISDI y SISCS y a la derecha el consumo del Ancho de banda de los Enlaces entre SISCS y los servidores caché.

Para el nodo de Arequipa, podemos observar las 3 figuras siguientes: La de ahorro del consumo del ancho de banda de este nodo (Fig. 4.7), en la que observamos que hay un ahorro promedio también de 13%.

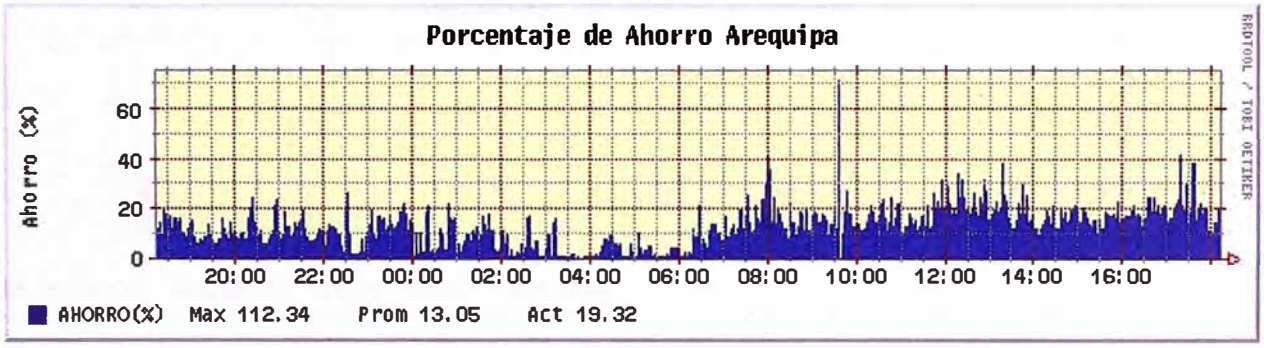


Figura 4.7 Ahorro de Ancho de Banda de la Red Caché del nodo de Arequipa.

En la figura 4.8 al lado izquierdo observamos el consumo de ancho de banda entre el enrutador distribuidor AREDI y el Conmutador de Contenidos ARECS, mientras que al lado derecho mostramos el tráfico entre el conmutador de contenidos ARECS y el servidor caché.

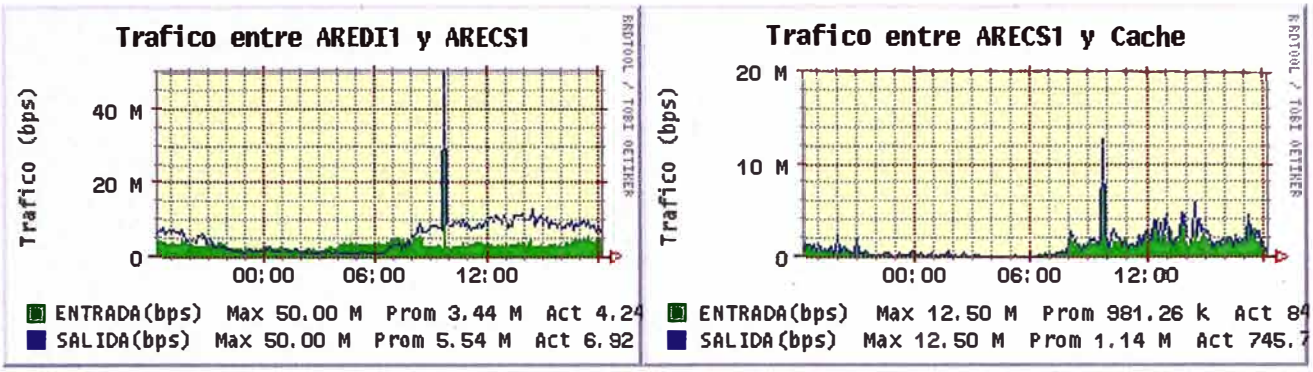


Figura 4.8 A la izquierda se muestra el Consumo de Ancho de Banda de los enlaces AREDI y ARECS y a la derecha el consumo del Ancho de banda de los Enlaces entre ARECS y los servidores caché.

Para el nodo de Trujillo, podemos observar las 3 figuras siguientes: La de ahorro del consumo del ancho de banda de este nodo (Fig. 4.9), en la que observamos que hay un ahorro promedio también de 10%.

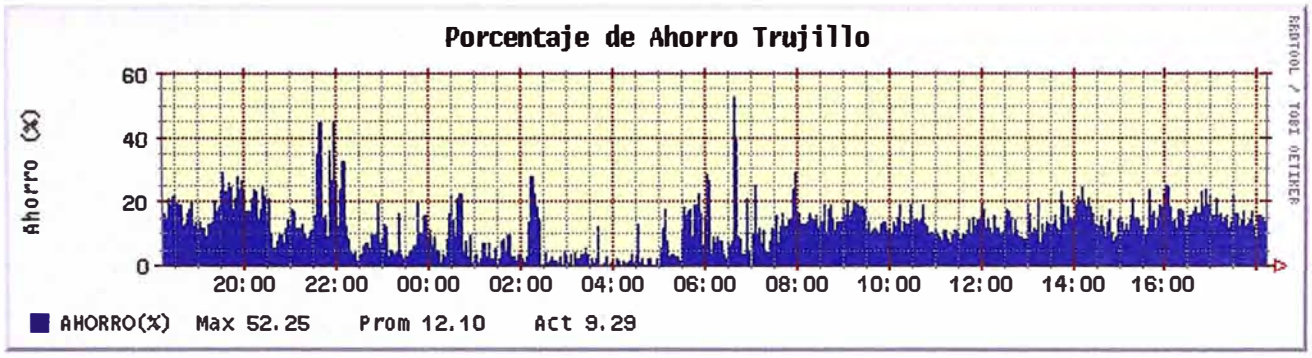


Figura 4.9 Ahorro de Ancho de Banda de la Red Caché del nodo de Trujillo.

En la figura 4.10 al lado izquierdo observamos el consumo de ancho de banda entre el enrutador distribuidor TRUDI y el Conmutador de Contenidos TRUCS, mientras que al lado derecho mostramos el tráfico entre el conmutador de contenidos TRUCS y el servidor caché.

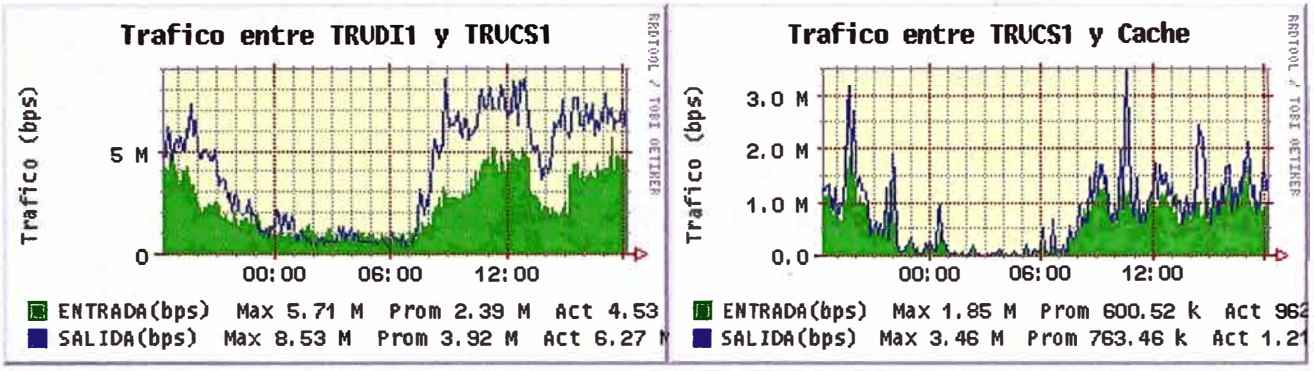


Figura 4.10 A la izquierda se muestra el Consumo de Ancho de Banda de los enlaces TRUDI y TRUCS y a la derecha el consumo del Ancho de banda de los Enlaces entre TRUCS y los servidores caché.

En todos los gráficos presentados se puede observar un ahorro promedio del 15% tanto en el ahorro total como en los ahorros parciales, lo cual verifica que la solución implementada ha logrado disminuir el consumo de ancho de banda internacional para fines de Internet.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se ha comprobado que utilizando servidores de almacenamiento inteligentes se puede obtener un gran ahorro del ancho de banda, generando a su vez menores costos para las PSI (Proveedores De Servicios Internet) debido a que el ancho de banda que no se usa simplemente no se paga.
2. La selección de los equipos y servidores de almacenamiento se ha logrado gracias al dato del consumo total de tráfico Internet que existe en cada nodo y que viene a ser la suma del ancho de banda usado por todos los clientes que acceden a Internet.
3. Es necesario mencionar que la solución de almacenamiento distribuido ha sido posible de implementar gracias a que ya se contaba con una Red IP/MPLS ya implementada y operativa, por lo que la inserción de las Redes Caché a la RedIP/MPLS ha significado no solo un acceso mas rápido a los contenidos sino también la permanencia de la diferenciación de servicio del tráfico de Internet que cruzaba la Red IP/MPLS de Telefónica Empresas.
4. Gracias a la implementación de este proyecto se observan menores cuellos de botella o menor congestión en el acceso a las páginas Web internacionales debido a que las páginas más usadas se encuentran almacenadas en los servidores caché implementadas en los nodos principales de la Red IP/MPLS. Esta reducción en la congestión también ha permitido disminuir los retardos de acceso a páginas internacionales de uso muy continúo debido a que ahora las Web´s se almacenan en repositorios inteligentes locales que trabajan de manera distribuida y redundante.
5. El retorno de la inversión realizada en este proyecto se ha traducido a la larga en mejores beneficios económicos para las PSI y en una mejor percepción de los servicios por parte de los clientes, pues ahora se tiene un servicio mas rápido, eficiente y seguro; sin que por ello se pague mas pues el servicio implementado es considerado un Servicio de Valor Añadido.

RECOMENDACIONES

1. La implementación del proyecto no hubiese sido posible si es que no se hubiese contado permanentemente con la dirección de un Jefe de Proyecto quién durante la elaboración y ejecución del mismo ha cumplidos funciones de coordinación, seguimiento y provisión de recursos.
2. Se debe tener el cuidado necesario con los plazos de ejecución de inversión durante la implantación del proyecto pues un retraso de este item puede causar una demora considerable en su fecha de culminación.
3. La seguridad de que se contaba con el equipo humano preparado ha sido una base sólida que ha permitido solucionar problemas críticos en los momentos oportunos.
4. Un proyecto de esta envergadura siempre debe contar con el respaldo decidido de una Gerencia Central para facilitar la provisión de recursos y flexibilización de procedimientos.
5. El seguimiento periódico del proyecto ha permitido que todas las Áreas involucradas trabajen de manera ordenada y sincronizada.

ANEXO A

DIRECCIONAMIENTO IP DE LAS REDES CACHE IMPLEMENTADAS

Mostramos a continuación tablas importantes que han sido de mucha utilidad para poder implementar este proyecto.

Tabla A-1 Tabla de Asignación de Direccionamiento IP de las VLANs definidas.

Nodo San Isidro	Networks	Tipo
VLAN2	172.20.7.0/27	Agregación
VLAN3	200.37.238.0/27	Caching
VLAN4	192.168.90.0/30	Redundancia
VLAN5	192.168.102.0/24	Gestión

Nodo Washington	Networks	Tipo
VLAN2	172.20.6.0/27	Agregación
VLAN3	200.37.84.0/27	Caching
VLAN4	192.168.90.0/30	Redundancia
VLAN5	192.168.101.0/24	Gestion

Nodo Arequipa	Networks	Tipo
VLAN2	172.20.7.0/27	Agregación
VLAN3	200.107.139.224/27	Caching
VLAN4	192.168.90.0/30	Redundancia
VLAN5	192.168.106.0/24	Gestion

Nodo Trujillo	Networks	Tipo
VLAN2	172.20.6.0/27	Agregación
VLAN3	200.106.63.224/27	Caching
VLAN4	192.168.90.0/30	Redundancia
VLAN5	192.168.105.0/24	Gestion

Tabla A-2 Tabla de Asignación de Direccionamiento IP de las Interfaces de Red de los Equipos de cada Red Caché

Nodo Washington	Puerto Consola	Servicio	Looback100 - ISIS	Loopback0 - OSPF	MASTER	SLAVE	Interfaz	Interfaz	Lan Gestión	AREA
WASDI1	42		200.48.175.140/32	200.48.175.14/32	172.20.6.1/27	172.20.6.33/27	GE 1/0/0	GE 2/0/0	192.168.101.105/24	AREA 1
WASCS1	49	200.37.238.1/27		172.20.6.2	172.20.6.2/27		GE 1/1		192.168.101.106/24	
WASCS2	50			172.20.6.34		172.20.6.34/27	GE 1/1		192.168.101.107/24	
WASRI1	46			200.48.175.1/32	172.20.6.5/27	172.20.6.37/27	FE1/0/0	FE4/0/0	192.168.101.108/24	
WASRI2				200.48.175.2/32	172.20.6.6/27	172.20.6.38/27	FE1/0/0	FE6/1/0	192.168.101.109/24	
WASRI3				200.48.175.3/32	172.20.6.7/27	172.20.6.39/27	FE4/0/0	FE11/0/0	192.168.101.110/24	
ERX-WAS					172.20.6.8/27	172.20.6.40/27				
WASCC1	51	200.37.238.2/27							192.168.101.111/24	
WASCC2	52	200.37.238.3/27							192.168.101.112/24	
SW2924	53								192.168.101.254/24	
SW2950	54								192.168.101.253/24	
Nodo San Isidro	**Puerto Consola**	**Servicio**	**Looback100 - ISIS**	**Loopback0 - OSPF**	**MASTER**	**SLAVE**	**Interfaz**	**Interfaz**	**Lan Gestión**	**AREA**
SISDI1	42		200.48.175.156/32	200.48.175.30/32	172.20.7.1/27	172.20.7.33/27	GE 1/0/0	GE 2/0/0	192.168.102.105/24	AREA 4
SISCS1	49	200.37.84.1/27		172.20.7.2	172.20.7.2/27		GE 1/1		192.168.102.106/24	
SISCS2	50			172.20.7.34		172.20.7.34/27	GE 1/1		192.168.102.107/24	
SISRI1				200.48.175.17/32	172.20.7.5/27	172.20.7.37/27	FE0/0/0	FE12/0/0	192.168.102.108/24	
SISRI2	46			200.48.175.18/32	172.20.7.6/27	172.20.7.38/27	FE 1/0/0	FE 4/0/0	192.168.102.109/24	
ERX-SIS					172.20.7.8/27	172.20.7.40/27				
SISCC1	51	200.37.84.2/27							192.168.102.111/24	
SISCC2	52	200.37.84.3/27							192.168.102.112/24	
SW2924	53								192.168.102.254/24	
SW2950	54								192.168.102.253/24	

Nodo Arequipa	Puerto Consola	Servicio	Looback100 - ISIS	Loopback0 - OSPF	MASTER	SLAVE	Interfaz	Interfaz	Lan Gestión	AREA
AREPE1	1		200.48.175.227/32	200.48.175.70/32	172.20.7.65/27	172.20.7.97/27	FE1/0/0	FE4/0/0	192.168.106.1/24	AREA 3
ARECS1	3	200.107.139.225/27		172.20.7.66	172.20.7.66/27		FE2/1		192.168.106.106/24	
ARECS2	4			172.20.7.98		172.20.7.98/27	FE2/1		192.168.106.107/24	
ARERI1	5			200.48.175.65/32	172.20.7.67/27	172.20.7.99/27	FE0/1	FE2/0	192.168.106.108/24	
ARECC1	6	200.107.139.226/27							192.168.106.111/24	
ARESW1									192.168.106.254/24	
Nodo Trujillo	**Puerto Consola**	**Servicio**	**Looback100 - ISIS**	**Loopback0 - OSPF**	**MASTER**	**SLAVE**	**Interfaz**	**Interfaz**	**Lan Gestión**	**AREA**
TRUPE1	1		200.48.175.195/32	200.48.175.62/32	172.20.6.65/27	172.20.6.97/27	FE 5/0/0	FE 1/0/0	192.168.105.1/24	AREA 2
TRUCS1	3	200.106.63.225/27		172.20.6.66	172.20.6.66/27		FE2/1		192.168.105.106/24	
TRUCS2	4			172.20.6.98		172.20.6.98/27	FE2/1		192.168.105.107/24	
TRURI1	5			200.48.175.57/32	172.20.6.67/27	172.20.6.99/27	FE0/1	FE2/0	192.168.105.108/24	
TRUCC1	6	200.106.63.226/27							192.168.105.111/24	
TRUSW1									192.168.105.254/24	

TERMINOLOGIA

POS: Paquetes sobre SONET/SDH

VLAN: Red Virtual de Area Local

VPN: Red Privada Virtual

WASCC1: Servidor Caché del Nodo de Washington

WASCS1: Conmutador de Contenidos del Nodo de Washington

WASP1: Enrutador Proveedor del Nodo de Washington

WASRR1: Enrutador Reflector del Nodo de Washington

WASDI1: Enrutador Distribuidor del Nodo de Washington

WASRI1: Enrutador de Internet del Nodo de Washington

BGP: Protocolo de Puerta de Enlace Fronteriza

IBGP: Protocolo Interno de Puerta de Enlace Fronteriza

EBGP: Protocolo Externo de Puerta de Enlace Fronteriza

OSPF: Algoritmo Abierto de Primero la Trayectoria más corta

IS-IS: Sistema Intermedio a Sistema Intermedio

MPLS: Multiprotocolo de Conmutación de Etiquetas

AS: Sistema Autónomo

DoS: Denegación del Servicio

BIBLIOGRAFIA

1. Steve Spanier, "Manual de Content Services Switch Serie 15000"
   Editorial CISCO 2001

2. Jeff Doyle – Jennifer Carroll, "Routing TCP/IP"
   Editorial CISCO PRESS 2001

3. Catherine Packet – Diane Teare, "Building Scalable Cisco Networks"
   Editorial CISCO PRESS 2001

4. Merilee Ford – H. Kim Lew, "Tecnologías de Interconectividad de Redes"
   Editorial Prentice Hall Hispanoamérica S.A. 1998

5. Tim Redjaian, "Manual de Servidores Caché CHACHEFLOW Series 6000/7000
   Editorial CacheFlow Inc 2001