UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE BACKBONE PARA LA PLATAFORMA DE LA RED DE DATOS EN UNA ENTIDAD FINANCIERA

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

RICARDO JUSTINIANO BENDITA LARICO

PROMOCIÓN
2006-I

LIMA-PERÚ
2013

DISEÑO DE BACKBONE PARA LA PLATAFORMA DE LA RED DE DATOS DE UNA ENTIDAD FINANCIERA

A mi madre, porque con su fortaleza y perseverancia
me demostró que ante muchos problemas que pueda tenerse
en la vida, siempre existe una forma de poder salir adelante,
gracias mamá por esforzarte tanto y hacer de tu pequeño hijo un profesional.
Quiero que sepas que tengo y tendré grabado en mi mente
aquella noche en la que pude presenciar tan grande tristeza en tu rostro, al
enterarte que el mayor de tus hijos no ingresaba a la
Universidad, desde pequeño llevo una fotografía de ese
instante en mi mente y me sirvió todo este tiempo, ante las adversidades,
poder seguir adelante, y así intentar regalarte una sonrisa.
Y como no mencionar a la persona que durante estos últimos
meses me brindo su apoyo incondicional, y aquella amistad especial que
toda persona desearía tener en su vida, en verdad Gracias!.
Tengan por seguro que cada paso que doy lo hago pensando
en ustedes, tenga por seguro que nunca los defraudaré.

SUMARIO

El presente trabajo describe el diseño de backbone para la plataforma de la red de datos de una entidad financiera basado en equipamiento de altas prestaciones en rendimiento, disponibilidad y escalabilidad.

La solución es requerida por la necesidad de proporcionar una plataforma para la red de datos que este acorde con las aplicaciones de hoy en día, las cuales demandan un alto rendimiento de los diferentes equipos de comunicaciones que conforman la plataforma de red para las diferentes aplicaciones, comenzando desde la parte de acceso, distribución y llegando así a la parte de Core, además se ve en el backbone de la plataforma de la red de datos actual, la necesidad de homologar el equipamiento de comunicaciones utilizado, para así evitar incompatibilidades de funcionamiento, operación y gestión entre los diferentes equipos de comunicaciones que conforman la backbone de la entidad financiera.

Para prestar un alto rendimiento y disponibilidad en el proceso de conmutación y enrutamiento de tráfico, en el backbone se hace uso de la línea modular de switches de marca Juniper Networks, que proveen de un alto rendimiento, disponibilidad, y escalabilidad, requerida hoy en día por las diferentes aplicaciones de la entidad financiera y de esta forma también soportar cualquier tipo de aplicación futura, así como, el de proporcionar una respuesta inmediata ante cualquier requerimiento en la prestación de servicios.

La solución propuesta considera distribuir el equipamiento en diferentes ubicaciones físicas, de tal forma no solo contar con una redundancia local (cluster), sino también con una redundancia geográfica del data center, para lo cual los equipos distribuidos se interconectaran entre sí mediante enlaces redundantes de fibra óptica, de esta forma se estará disminuyendo al máximo la interrupción de los servicios.

El esquema topológico y lógico es aplicable a cualquier plataforma de red que requiera contar con altas prestaciones, y con tiempos de respuesta óptimos, garantizando una operatividad continua de la plataforma de red instalada, y no afectando los servicios prestados por las diferentes aplicaciones de uso común por la entidad financiera, ya que un requisito fundamental de la solución es conseguir una alta disponibilidad en hardware y software.

ÍNDICE

INTRODUCCIÓN

La solución desarrollada en el presente informe surge de la necesidad de diseñar e implementar la infraestructura de Backbone para la plataforma de red de datos de una entidad financiera, de esta manera tener una plataforma sobre la cual se transporte el tráfico de las aplicaciones de uso actual, como las que se vendrán adquiriendo durante los próximos dos años que durará la renovación tecnológica.

También se considera brindar una arquitectura robusta que permita ser resistente ante la falla de cualquier componente que conforma la solución requerida, de esta forma evitar la interrupción del servicio en alguna de las aplicaciones de uso de la entidad financiera.

La solución se implementa haciendo uso de la línea de switches modulares de alto rendimiento EX8200 de la marca Juniper Networks, los cuales son plataformas de muy altas prestaciones, diseñados para Data Centers y entornos de redes de Core. La robustez es lograda por la utilización de múltiples switches configurados en alta disponibilidad, los cuales trabajan de manera distribuida y simultánea, logrando reducir al mínimo la probabilidad de falla de la comunicación.

El diseño presentado tiene tres ámbitos totalmente diferenciados, análisis de la plataforma actualmente instalada y en uso, planteamiento de un rediseño total de la red de Backbone, y plan de trabajo de la solución propuesta. El análisis de la plataforma actualmente instalada duró un mes, y la elaboración del diseño y la planificación de la implementación fué de dos meses.

La disponibilidad tecnológica fué de fácil solución por cuanto los equipos se encontraban disponibles comercialmente, homologados y no se requería de importaciones especiales. La alta disponibilidad ofrecida como parte de la solución propuesta, asegura un grado absoluto de continuidad operacional.

Aunque la configuración de cada uno de los switches de Core que conforman el Backbone pueden ser administrados a través de una conexión vía telnet, http o cable serial (línea de comandos), para hacer mucho más eficiente la gestión de los equipos y de manera centralizada, dentro de la solución propuesta se ha contemplado el uso de un programa de administración de red propietario Network & Security Manager (NSM) mucho más amigable e intuitivo. Se analizó la situación de la necesidad requerida por el

entidad financiera, y se identificaron las opciones de mejora y de diseño de la solución de Backbone, durante el periodo de un mes se trabajo de forma conjunta con el equipo de TI de la entidad financiera, estudiando así a detalle la plataforma actualmente instalada, pudiendo conocer los procedimientos y arquitectura de la backbone actual. El equipo estaba conformado por jefes de proyecto, administradores de red y otros en una visión común.

La bibliografía utilizada en este trabajo es variada en cuanto a la teoría (Juniper), para la parte de diseño se contó con toda la documentación técnica requerida.

El presente informe de suficiencia, se divide de la siguiente manera: En el primer capítulo se expone el problema de ingeniería, haciendo hincapié en el objetivo y los alcances de la solución propuesta, en el segundo capítulo se exponen los conceptos necesarios que sustentan la explicación para la solución propuesta, en el tercer capítulo se describe la metodología de la solución, exponiendo los estudios preliminares realizados para la red de Backbone propuesta, alta disponibilidad, y demás aspectos técnicos. En el capítulo final se hace un compendio de la programación de trabajos, el equipamiento usado, y los costos de dicha solución

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema, para ello primeramente se describe el problema y luego se expone el objetivo del trabajo, también se evalúa el problema y se precisan los alcances del informe, para finalmente presentar una síntesis del diseño presentado.

1.1 Descripción del problema

Existe un deficiente servicio prestado por la plataforma actual sobre la cual se transportan múltiples aplicaciones de uso diario por la entidad financiera, ya que para el crecimiento continuo de usuarios y el avance en la tecnología de las aplicaciones las cuales cada vez son más robustas por sus propias prestaciones, la plataforma actual no es lo suficientemente sólida y robusta para soportar nuevas aplicaciones y el crecimiento continuo a la cual la entidad financiera tiene como objetivo, dentro del objetivo trazado se encuentran los siguientes puntos:

a) Falta de alta disponibilidad a nivel de acceso, no se cuenta con enlaces redundantes desde las salas de comunicaciones a los switches de Core.

b) Falta de alta disponibilidad a nivel de Core, no se cuenta con una redundancia a nivel físico y lógico entre los equipos de conmutación de paquetes de la oficina principal y contingencia respectivamente.

c) Ausencia de herramientas de seguridad a nivel de conmutación de paquetes, que puedan servir como facilidades de protección ante cualquier tipo de ataque de seguridad a nivel de conmutación.

d) La plataforma de la red de Core actual cuenta con un limitado número de facilidades de diagnóstico de red, que puedan servir como herramientas de análisis ante algún evento de falla sobre la plataforma actual.

1.2 Objetivos del trabajo

Diseñar y proponer un diseño de Backbone para la plataforma de red de datos de la entidad financiera, que proporcione una alta disponibilidad, confiabilidad, y escalabilidad para las diferentes aplicaciones actuales y de uso futuro de la entidad financiera.

La solución se logrará mediante el uso de la línea de switches modulares EX8200 de Juniper Networks de altas prestaciones, trabajando de una manera coordinada y

simultánea, de esta forma se permite optimizar sus recursos ofrecidos, situándolos en la ubicación más conveniente de la red de datos, y haciendo posible el control y operación de todo el núcleo corporativo.

En el caso de falla de algún enlace y/o elemento que conforma la solución propuesta, el servicio brindado por el diseño de switches de la solución propuesta, no deberá verse interrumpido, el objetivo es tener una plataforma que preste una confiabilidad absoluta como plataforma de red de datos de forma tal que los diferentes servicios y aplicaciones corporativas de la entidad financiera no se vean afectados, la solución propuesta deberá incluir el equipamiento necesario para tener una redundancia geográfica del Data Center actual, cuya oficina de respaldo se denomina sede de contingencia, existiendo enlaces punto a punto mediante fibra óptica oscura entre ambos Data Centers (principal y contingencia).

1.3 Evaluación del problema

La plataforma actual utilizada como Backbone, si bien es cierto soporta el tráfico generado por las aplicaciones corporativas y dirigido hacia Internet, según las proyecciones de la entidad financiera se tendrá un crecimiento importante del trafico IP, por el uso de nuevas aplicaciones en la parte de acceso y transporte, ha ocasionado un deterioro en el rendimiento de la red, viéndose afectadas aplicaciones corporativas muy críticas, y en algunos casos deteniendo por completo la transmisión de trafico critico e importante para la entidad financiera, en el anexo A se describen los eventos críticos que han ocasionado problemas en la red.

El no usar una red dedicada en su totalidad para el tráfico de gestión para los diferentes equipos de comunicaciones que conforman la red de datos de la entidad financiera, ha llevado en muchos casos una pérdida y ausencia de orden en la gestión de tales equipos.

El no tener una contingencia ante la falla de un elemento que conforma la Backbone de la red de datos que sirve como medio de transporte del trafico originado por los usuarios y dirigidos a las aplicaciones corporativas o a Internet, tiene como resultado la pérdida de la calidad del servicio por un tiempo no determinado, que en algunos casos ha llegado a ser de horas, y originando así una mala imagen ante el cliente, y de una considerable pérdida de dinero para la entidad financiera, el Anexo A describe que por lo se presentaban de por lo menos dos problemas críticos en la red, los cuales pudieron ser evitados por mecanismos de protección a nivel de conmutación de paquetes.

El tema del alcance de la facilidad de gestión del equipamiento que conforman la Backbone actual, fue constituyéndose en otro problema, dado a la falta de capacidad en conocimientos de administración de equipamiento, así como de la ausencia de

actualizaciones de software del equipamiento actual.

A lo expuesto, el personal de TI de la entidad financiera no suelen ser alertados con mensajes de advertencia de posibles inconvenientes que se presenten dentro de la plataforma de red instalada, por lo cual se ve la necesidad de inclusión dentro de la solución propuesta de un componente de red que tenga la capacidad de poder almacenar y alertar al personal de TI de problemas inminentes que tengan como resultado la paralización o interrupción de los servicios prestados a la red.

El incluir dentro de la solución, equipamiento que proporcione altas prestaciones en funcionalidad con configuraciones de alta disponibilidad, las cuales tengan la capacidad de poder reducir al mínimo la probabilidad, de detener los servicios prestados a la red por medio de las aplicaciones de uso común con las que cuenta la entidad financiera, y así conseguir lo propuesto con la solución.

1.4 Alcance del trabajo

Se diseña e implementa el Backbone para la plataforma de red de datos en alta disponibilidad local y geográfica, proporcionando una redundancia absoluta a la red de acceso de la entidad financiera y a su Data Center principal.

El diseño presentado abarca tres emplazamientos:

Estudio de la plataforma actualmente instalada.

El diseño de una nueva solución como plataforma de red que ofrezca a la entidad financiera una garantía en uso completo a todo momento de sus aplicaciones.

La planificación e implementación de la solución propuesta.

La capacidad de contar con equipos de conmutación central en una configuración activo/activo, diseñada especialmente para Data Centers y con redundancia en todos sus elementos principales, proporciona una confiabilidad de 99,999%.

1.5 Síntesis del trabajo

Para el diseño de la infraestructura de Backbone de la red de datos, como primer paso se realizó un estudio de los diferentes componentes físicos que comprendían la solución del Backbone instalado, incluyendo las diferentes interconexiones en fibra y cobre, entre el Core y las salas de comunicaciones existentes en los pisos, incluyendo la interconexión con la sede de contingencia, para así tener un esquema topológico de la red actual instalada, de esta forma siguiendo con el análisis lógico de la red, llegando así a obtener toda la información referente al direccionamiento IP, información de enrutamiento IP, y configuración actual de los equipos.

Después de realizado el análisis, se procedió a la detección de "Zonas Oscuras", es decir zonas con mucha interferencia, o a las que no llega el servicio debido a obstáculos,

que influirán en la calidad de la red. Con esta información se determinó el lugar óptimo de emplazamiento de los puntos de accesos Inalámbricos para asegurar una cobertura adecuada a todos los usuarios.

Una vez determinado la topología física y lógica de la plataforma de datos en uso por la entidad financiera, se procedió a realizar un diseño acorde con las necesidades que estableció la entidad financiera como solución adecuada para sus propósitos, para lo cual se requirió realizar un consolidado de la información obtenida con la información proporcionada por la entidad financiera que consistía en tipo de conmutadores de datos, diagrama de distribución de red, y sus ubicaciones físicas por nivel (wiring closet). Como resultado de la consolidación de información se pudo determinar que la topología de red, cuya topología de red desplegada en la entidad financiera tiene una configuración estrella y un entorno de red diferenciado en dos etapas de red (ver figura B.1 del anexo B): 1) Etapa acceso y 2) Core (núcleo).

1. En la etapa de acceso los equipos de comunicación son de fabricación variada como Alcatel y Nortel. Estos equipos manejan VLAN (Redes virtuales de área local), cuentan con 24 o 48 puertos, enlaces de fibra y también tienen la capacidad de manejo de etiquetas, también conocido cómo Tagging (IEEE 802.1Q)
2. La etapa de Core de la red es de una topología en estrella y es el centro de la plataforma instalada, a esta llegan los enlaces de fibras procedentes de los distintos armarios de telecomunicaciones (wiring closet) repartidos por todo el edificio de la entidad financiera. El Core esta compuesta por dos switches en configuración activo/pasivo con balanceo de carga.

Una vez entendida la topología de red se procedió a la configuración de los equipos de red, bajo las siguientes condiciones:

a) El Backbone para la plataforma de red de datos, tiene como finalidad brindar acceso continuo e ininterrumpido a Internet y a la Intranet corporativa de la entidad financiera, para lo cual se dispondrá de cuatro switches ubicados en pares en dos ubicaciones geográficas distintas, considerando que cada par de switches funcionaran en una configuración de alta disponibilidad (cluster) activo/activo, balanceando así la carga de trafico originado desde la red y hacia la red corporativa.

b) Cada par de switches funcionaran como una única entidad de red (Virtual Chassis).

c) En cada ubicación física, en la cual se instalen los pares de switches se dispondrá de dos XRE200 trabajando en alta disponibilidad, los cuales permiten a un par de switches

secundaria, ambas sedes se interconectaran a través de una topología full-mesh, con una configuración de Link Aggregation con enlaces de fibra óptica redundantes de 10Gbit Ethernet, llegando a un total de 40Gbps de velocidad entre ambas oficinas.

e) Ya concluida la interconexión y configuración de los switches que forman la Backbone de la plataforma de datos de la entidad financiera, se proseguirá a la integración entre la red actual a la nueva plataforma instalada, con fines de migración.

f) Culminando con la instalación, se instalará y configurará la solución de consolidación de eventos, este con el objetivo de consolidar los eventos, flujos de información de red y seguridad de la solución propuesta, y que interactué con el equipamiento de switching de la solución propuesta.

g) Como procedimiento final a la implementación de la solución propuesta e instalada, se brindará un servicio de post-soporte durante los siguientes sesenta días laborables, una vez instalada la solución, además se consideró el soporte anual de un ingeniero certificado y capacitado, quien cumplirá labores como ingeniero de soporte residente, cuyo horario se regirá en el modo de 8x5horas a la semana, con fines de poder finiquitar, solucionar y dar el soporte necesario ante cualquier detalle y/o requerimiento técnico que sea solicitado referente a la implementación integral de la solución instalada, dando así el soporte técnico necesario.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen los conceptos esenciales más importantes que faciliten el entendimiento de la solución descrita en el presente documento. Los temas a tratar son:

Introducción a las redes Ethernet.

Estándares Ethernet.

Conceptos de networking.

Servicios de red.

VLAN (Red de área local virtual).

LACP (Link Aggregation Control Protocol).

Junos OS (Junos Operation System).

VC (Virtual Chassis).

Alta disponibilidad.

Arquitectura de backbone.

Sistema de gestión centralizado.

2.1 Introducción a las redes Ethernet

La comunicación, como hecho integral de intercambio de información, se ha vuelto hoy en día un aspecto muy importante en la vida cotidiana de las personas al igual que en las diferentes organizaciones, de esta manera poder mantenerse competitivos en este escenario actual en el cual la tecnología avanza a pasos agigantados. Por este motivo es inconcebible que cualquier compañía no posea conexión a Internet, redes de computadores, centrales telefónicas propias y tampoco les haya brindado un adecuado servicio de correo electrónico para sus funcionarios.

A lo anterior, se eligió un protocolo que pueda soportar sin problema alguno las diferentes formas de comunicación y diferentes aplicaciones que permitan aumentar la productividad de las organizaciones. Por tal motivo es que Ethernet se ha convertido en el medio de acceso más conocido para equipos de comunicaciones, utilizado ya sea en entornos de redes pequeñas a grandes.

En el presente Ethernet, permite velocidades de entre 10Mbps a 100Gbps, Ethernet es hoy una tecnología omnipresente que dota de conectividad a más del 90% de

dispositivos de red de todo el mundo. Si bien es cierto el origen de Ethernet fue para poder comunicar un conjunto de estaciones de red, en la actualidad se puede utilizar Ethernet para una extensa gama de aplicaciones, tipos de usuarios y tipos de redes.

El auge de Ethernet en el sector de Telecomunicaciones se explica por la necesidad de los proveedores y operadores de servicios de migrar sus actuales infraestructuras a redes Ethernet e IP de nueva generación. Una tendencia a la que contribuyen los menores costes de Ethernet, su ubicuidad tanto en las redes privadas como públicas y el conocimiento universal sobre su tecnología y despliegue. Por tal motivo para lograr la implementación de sistemas de telecomunicaciones eficientes que permitan cubrir la demanda actual, es importante considerar dos objetivos claros: 1) mantenerse a la vanguardia de la tecnología y 2) reducir los costos, y Ethernet cumple con tales objetivos. Es por tal motivo que se convierte en favorito inmediato para el uso de nuevas tecnologías.

2.1.1 Visión general

Una Red de Área Local Ethernet permite la interconexión entre dos o más dispositivos, nodos o estaciones de red, haciendo uso de un método de acceso a la red conocido como CSMA/CD, de esta forma poder intercambiar información, comunicarse y a acceder a diversos servicios. Para lograr el intercambio de información existen diferentes mecanismos de comunicación o protocolos que establecen reglas que permiten el flujo confiable de información entre nodos. Por ejemplo, el conjunto de protocolos TCP/IP utilizado en redes de computadoras como Internet, permite que cualquier computadora que los implemente pueda comunicarse con otra que se encuentre conectada a la misma red.

Durante muchos años, la industria de las redes ha promovido el concepto de convergencia, a saber, una única red que admita servicios de voz, video y dato. Como ejemplo la conocida tecnología ATM se diseño con este propósito, previendo que una única red de datos convergida reduciría drásticamente sus gastos de explotación, prácticamente en su momento la mayoría de empresas de telecomunicaciones implantaron la tecnología ATM en sus redes troncales. Estas empresas intentaron imponer la tecnología ATM como el estándar de facto para redes en los servicios que prestaban a clientes de empresa, tanto para redes WAN como LAN. Debido al alto coste financiero y operativo de la tecnología ATM, esta nunca fue implantada por los clientes de empresa en su red LAN. Prácticamente todas las LAN de empresas están basadas en la tecnología Ethernet y utilizan el protocolo de Internet (IP) en sus aplicaciones.

2.2 Estándares Ethernet

Los estándares tal como lo define la ISO son acuerdos documentados que contienen

especificaciones técnicas u otros criterios precisos para ser utilizados consistentemente como reglas, guías o definiciones de características para asegurar procesos y servicios cumplan con su propósito, sin importar el tipo de dispositivo o las diferencias en su fabricación. Los estándares facilitan además la interoperabilidad entre componentes aunque estos tengan características diferentes. Existen diferentes organismos internacionales que originan estándares; en el área de telecomunicaciones se encuentran, por ejemplo, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por su sigla en inglés) y la Unión Internacional de Telecomunicaciones (UIT).

La especificación IEEE para Ethernet es la 802.3, que define que tipo de cableado y cuáles son las características de la señal que transporta. La especificación 802.3 original utilizaba un cable coaxial grueso de 50ohm, que permite transportar una señal de 10Mbps a 500m. Posteriormente se añadió la posibilidad de utilizar otros tipos de cables, como el cable coaxial delgado, pares de cables trenzados, y fibra óptica.

Para los diferentes tipos de medio se definieron diversos estándares, por ejemplo para el cable coaxial se definieron los estándares IEEE 802.3 y 802.3a, para la fibra óptica se definió el estándar 802.3j y 802.3u, y para el cable de par trenzado se definieron los estándares 802.3i, 802.3u, 802.3ae, etc.

Hoy en día ya existen tecnologías de 40 y 100 Gigabit Ethernet definidos en el estándar aprobado IEEE 802.3ba en Junio del 2010, la aprobación de 40 y 100 Gigabit Ethernet constituyen un paso más en la versatilidad y adaptabilidad de Ethernet a los nuevos requisitos de capacidad de las redes de datos basadas en IP, debido al crecimiento en el trafico de la VoIP, la IPTV con HDTV y 3D, el VoD, la videoconferencia y tele presencia IP, etc.

40 Gigabit está pensado para ser utilizado para backplanes[1] de equipos y para redes de almacenamiento, conectividad de servidores, cluster de computación de alto rendimiento, servidores blade, etc. Por otro lado 100 Gigabit Ethernet será empleado en la red de switching, routing y agregación en centro de datos, redes metropolitanas y troncales de los operadores y grandes empresas, etc.

2.3 Conceptos de networking

Al implementar una solución de redes se debe identificar los diversos elementos que conformaran la solución, así como los servicios y las alternativas de integración que presentan los dispositivos para realizar una configuración. Para el caso de la implementación del Backbone de datos de la entidad financiera, se tienen que diferenciar conceptos y funciones que pueden tenerse en los diferentes elementos que conforman la solución. Los aspectos que serán explicados a continuación son: a) Red de

computadoras, b) Configuración de la red, c) Clasificación de las redes y d) Componentes básicos de una red.

a. Red de computadoras

Una red de computadoras es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a Internet, e-mail, chat, juegos), etc.

b. Configuración de la red

Para que un equipo determinado pueda acceder a la red y a Internet, es necesario configurar el acceso a la red. Algunos datos de acceso a la red deben ser suministrados por el ISP (Internet Service Provider), que es la entidad con la que se tenga contratados los servicios de acceso a Internet.

Para conectarse a un LAN y a Internet, es necesario tener correctamente configurado el protocolo TCP/IP, en las propiedades de la conexión a la red. La dirección IP de un ordenador debe ser única dentro de la red a la que pertenece. Las direcciones IP que se tienen dentro de una LAN son privadas y las que comunican la LAN con Internet son públicas.

c. Clasificación de las redes

Las redes se pueden clasificar de acuerdo al área de cobertura en la que prestan servicios:

1. LAN (Local Area Network).- Son pequeñas redes como por ejemplo las que podemos crear en nuestro propio domicilio entre varios ordenadores. Son redes en las que cada equipo puede comunicarse con el resto de manera rápida debido a las pequeñas distancias que ha de recorrer la información. Son redes de uso privado.
2. MAN (Metropolitan Area Network).- De tamaño superior a las LAN, pueden abarcar una ciudad entera y la distancia entre puntos no sueles superar la decena de kilómetros. Un ejemplo sería la de que podría crearse una para unir varios comercios o entidades públicas de una ciudad.
3. WAN (Wide Area Network).- Redes de amplio alcance capaces de cubrir distancias de hasta miles de kilómetros. Las WAN puedes ser de tipo privado o público. De tipo privado puede ser la WAN de una empresa que permite la comunicación entre sucursales situadas en ciudades diferentes.
4. Internet.- Es una inmensa red de redes informáticos que están unidas entre si a nivel mundial.

[1] Placa de circuito impreso en la parte posterior de un switch que forma un BUS.

d. Componentes básicos de una red

Los componentes básicos para una red local:

1. Estaciones de Trabajo: Se entiende por estación de trabajo como un microordenador de altas prestaciones destinado para trabajo técnico o científico, en las redes de datos se entiende a una estación de trabajo como una computadora a través del cual facilita a los usuarios el acceso a los servidores y periféricos de red, suele utilizarse el termino nodo para referirnos a una computadora.
2. Servidor: Es una computadora utilizada para poder prestar un determinado servicio, por ejemplo, un servidor de archivos, es aquella computadora que publica archivos para su uso a la red, de la misma forma puede existir servidores de impresión, servidores web, servidores de correo, servidores de impresión y demás servicios que se puedan prestar a los diferentes elementos de la red instalada.
3. Medio de transmisión (Cableado): Permite la interconexión de dispositivos de red para la comunicación entre ellos y la transmisión de datos.
4. NIC o adaptador de red Ethernet: Permite el acceso de una computadora a una red. Cada adaptador de red posee una dirección física conocida como Media Access Control MAC que la identifica en la red y es única.
5. Concentrador o HUB: Funciona como un repetidor, permite la interconexión de múltiples nodos, con la peculiaridad que cada mensaje que es enviado por un nodo es repetido en cada uno de los puertos del HUB.
6. Conmutador o switch: Funciona como el bridge, pero permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado que un HUB. Los switches pueden tener otras funcionalidades, como redes LAN virtuales y mecanismos de seguridad en el acceso de los nodos a la red, siendo así mucho más eficientes que los concentradores.
7. Enrutador o router: Es aquel dispositivo que permitirá la interconexión de red entre ordenadores de red que operan a nivel de red, de esta forma se encargara de seleccionar el camino a seguir para la comunicación entre los nodos de red.

2.4 Servicios de red

En esta sección se describirán los diferentes servicios de red vinculados a la solución propuesta en este informe; a) HTTP, b) SNMP, c) Telnet y d) SSH.

a. HTTP (Hypertext Transfer Protocol)

Es un protocolo de transferencia de hipertexto, es el método más común de intercambio de información en la World Wide Web, y mediante el cual se transfieren las páginas web a un ordenador, el servicio brindado se realiza a través del puerto 80 TCP,

todas las páginas web que se consultan a través de Internet están escritas en lenguaje de hipertexto HTML (Hyper-text Markup Language), el protocolo trabajo en un esquema petición-respuesta entre un cliente y un servidor, al cliente que efectúa la solicitud se le conoce como agente del usuario el cual podría ser cualquier navegador web, a la información transmitida se le llama recurso y se le identifica mediante una dirección llamada URL (Uniform Resource Locator).

El servicio web prestado por los switches que conforman la solución, es utilizado vía el protocolo HTTP para poder administrar de manera independiente vía web a los switches que conforman la backbone de datos de la entidad financiera.

b. SNMP (Simple Network Management Protocol)

Es un protocolo desarrollado para gestionar y administrar dispositivos en una red IP, de esta manera poder supervisar el funcionamiento de la red, buscar y resolver sus problemas, las versiones de SNMP mas utilizadas son SNMPv1 y SNMPv2, siendo la última versión SNMPv3 el cual posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad.

En una red administrada vía SNMP consiste de tres componentes claves, los dispositivos administrados, agentes y sistemas administradores de red (NMS), un dispositivo administrado es un nodo de red que contiene un agente SNMP, estos recolectan y almacenan la información de administración, la cual es puesta a disposición de los NMSs usando SNMP, los dispositivos administrados, podrían ser estaciones de red, servidores, hubs, switches, routers, etc.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Para poder realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a conexión (UDP) cuyos puertos de comunicación comúnmente utilizados son el 161 y 162, para enviar un conjunto de pequeños mensajes PDUs entre los NMSs y los agentes.

Las diferentes variables que determinan que información será administrada de un dispositivo a través del agente instalado, es definida mediante las MIB's (Management Information Base) el cual es un conjunto de variables organizadas de forma jerárquica y son accedidas usando un protocolo de administración de red como SNMP.

En nuestra solución propuesta se contempla el uso de un NMS propietario a través del cual se monitoreara los diferentes aspectos de los equipos que conforman la solución.

c. Telnet (Telecommunication Network)

Es un protocolo de red cliente-servidor que sirve para acceder mediante una red a otro nodo conectado a la red, el servicio brindado se realiza a través del puerto 23 TCP,

de modo que podamos tener control remoto a través de una terminal, es decir, sin grafico, el problema de este protocolo es la seguridad, ya que toda la comunicación a través de este protocolo viaja a través de la red en texto plano (cadenas de texto sin cifrar), lo cual permite que cualquiera que espié el trafico de red pueda obtener información confidencial como credenciales de autenticación, por tal motivo hoy en día no es el mecanismo común que se utiliza para la administración remota a través de terminales.

Hoy en día en casos muy puntuales se utiliza este mecanismo de administración ya que al no utilizar un mecanismo de cifrado de la información lo hace más ligero en conexiones de red muy congestionadas, por otro lado en la solución propuesta no se hará uso alguno de este tipo de conexión, por lo contrario se utilizará un mecanismo de control remoto a través de una terminal utilizando una conexión segura, conocida como SSH la cual se detalla en el siguiente punto, durante el desarrollo e implementación del proyecto no se ha contemplado por ningún motivo el uso de esta herramienta por su inseguridad.

d. SSH (Secure Shell)

Es un protocolo de red cliente-servidor que permite el intercambio de datos usando un canal seguro entre dos dispositivos conectados a una red, el servicio brindado se realiza a través del puerto 22 TCP, es el sucesor del protocolo Telnet, dado que realiza las mismas funciones pero con las ventajas en seguridad que proporciona, SSH hace uso de técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y así no se pueda interceptar información confidencial.

La versión actual es SSHv2, la cual para mejorar la seguridad hace uso de Diffie-Hellman Key Exchange y una fuerte verificación de la integridad de la información a través de códigos de autenticación de mensajes.

Múltiples aplicaciones como SFTP (Secure File Transfer Protocol) y SCP (Secure Copy), los cuales son utilizados para transferencia de archivos, se basan en el código base del protocolo SSHv2 para poder realizar las transferencias de los archivos de manera segura.

Este protocolo se utilizará como uno de los métodos de acceso para la administración remota de los diferentes elementos de red que conforman la solución propuesta en el presente informe.

2.5 VLAN (Red de área local virtual)

Como se sabe una red de área local, es un conjunto de estaciones de trabajo interconectadas físicamente entre sí, las cuales comparten el ancho de banda disponible y el dominio de "broadcast[2]" al que pertenecen, en este esquema no se podría optimizar

[2] Transmisión de un paquete que será recibido por todos los dispositivos en una red.

el ancho de banda, ni se podría conseguir un nivel de confidencialidad ya que el medio es compartido por todos los nodos que comprenden la red, a lo anterior se suma, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Una VLAN es una red de área local (o LAN) que agrupa un conjunto de equipos de manera lógica y no física, el uso de VLAN's nos proporciona una mayor flexibilidad en la administración y en los cambios de la red, los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de la red, las redes LAN virtuales pueden restringir los "broadcast" a los dominios lógicos donde han sido generados. Además añadir usuarios a un determinado dominio o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros. Las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparte el dominio de "broadcast" con los dispositivos que pertenezcan a la misma red LAN virtual.

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma.

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico o VLAN.

En el caso de la familia EX de switches del fabricante Juniper, es en todos sus modelos de switches que se soporta la creación de LAN virtuales VLAN's.

2.6 LACP (Link Aggregation Control Protocol)

LACP está definido en la especificación IEEE 802.3ad (Aggregation of Multiple Link Segments), LACP es un método de agrupación de varias interfaces físicas para formar una interface lógica, el intercambio de mensajes LACP los cuales son conocidos como LACPDUs se realiza entre la interface con LACP habilitado y el extremo del enlace.

LACP ha sido diseñado para lograr la agregación y eliminación automática de enlaces individuales al conjunto de interfaces agrupadas que suelen recibir el nombre de Link Aggregation Group LAG sin intervención alguna del usuario, además de monitorear el enlace para así verificar si ambos extremos del LAG están conectados a el grupo correcto. Este funciona enviando LACPDUs por todos los enlaces que tienen el protocolo LACP habilitado, este encontrara un dispositivo en el extremo del enlace que también tenga el protocolo LACP habilitado, y es así que este ultimo también empezara a responder a los mensajes LACPDUs sobre los mismos enlaces y es así que el protocolo LACP combinara estos enlaces en un único enlace lógico.

Con la configuración de LAGs se consigue un incremento del ancho de banda, incremento de la disponibilidad del enlace, balanceo de carga ya que el tráfico se distribuye a través de los múltiples enlaces minimizando así la probabilidad que un simple enlace se vea saturado, y de la reutilización de hardware existente.

2.7 Junos OS (Junos Operating System)

Junos es un confiable, sistema operativo de red de alto rendimiento para enrutamiento, switching, y seguridad, de Juniper Networks. Junos es un sistema, diseñado para reformular por completo la forma en la cual trabajan las redes. Junos funcionalmente es un sistema compartimentado en múltiples procesos de software. Donde cada proceso maneja una porción de la funcionalidad del dispositivo. Cada proceso se ejecuta en su propio espacio de memoria protegido, de esta forma asegurándose que un proceso no puede interferir directamente con otro. Cuando un simple proceso falla, el sistema entero no necesariamente falla. Esta modularidad también asegura que las nuevas características puedan ser adicionadas con menos probabilidad de alguna ruptura en la funcionalidad actual, por estos motivos es que se resalta que Junos es un sistema operativo robusto, modular y escalable.

La forma en la cual está diseñado la arquitectura de Junos está basado en la separación del plano de control y el plano de forwarding, como se muestra en la Figura 2.1.

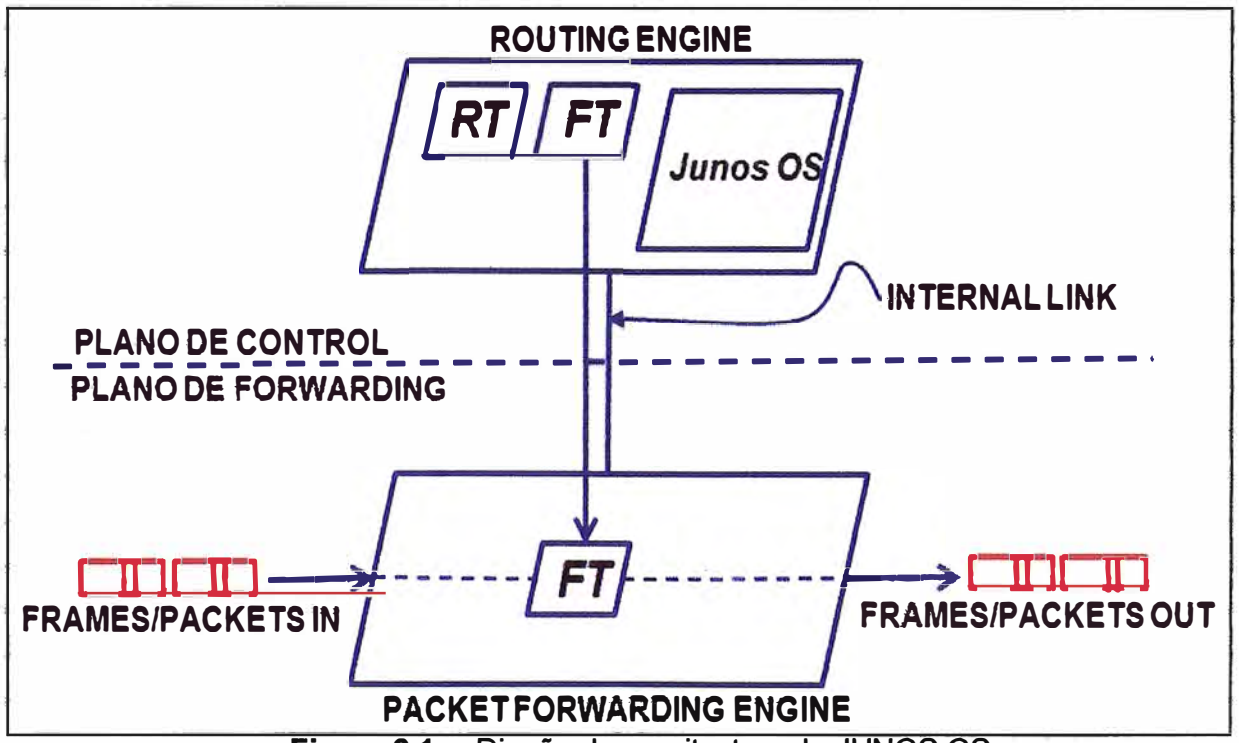

Figura 2.1 Diseño de arquitectura de JUNOS OS

Los procesos que controlan los protocolos de enrutamiento y de switching están completamente separados de los procesos que realizan el forwarding de frames,

paquetes, o ambos a través del dispositivo sobre el cual se ejecuta Junos OS. La separación de los planos de control y de forwarding es una de las razones clave porque el Junos OS puede soportar diferentes plataformas de un común código base. En el plano de control se ejecuta el Routing Engine (RE). El RE es el corazón de la plataforma; este es responsable de realizar las actualizaciones de los protocolos y de la administración del sistema. El RE mantiene la tabla de enrutamiento, tabla de bridging, y la tabla principal de forwarding, y se conecta al Packet Forwarding Engine (PFE) a través de un enlace interno, el PFE se ejecuta en un hardware separado y es responsable del forwarding del trafico de transito a través del dispositivo. En muchas plataformas el PFE hace uso de Application Specific Integrated Circuits (ASICs) para incrementar el rendimiento de la plataforma, debido a que esta arquitectura separa las operaciones de control de las operaciones de forwarding, las plataformas que ejecutan el Junos OS pueden entregar un rendimiento superior y una alta confiabilidad en su operación. El PFE recibe la tabla de forwarding (FT) del RE por medio del enlace interno.

El PFE es el componente de procesamiento central del plano de forwarding. El PFE sistemáticamente reenvía tráfico basado en una copia local de la tabla de forwarding del plano de control.

2.8 VC (Virtual Chassis)

Un sistema de Virtual Chassis es una colección de interconectados entre sí, que son administrados como un único switch. Un virtual chassis consiste de uno a diez switches modelos EX4200 de la familia EX de switches de marca Juniper proporcionando así una flexibilidad en el crecimiento de puertos según las necesidades, los cuales son conocidos como switches miembros, los miembros trabajan de manera conjunta para proporcionar una alta densidad de puertos, que al trabajar de manera individual.

Un sistema de Virtual Chassis simplifica las tareas de administración, por ejemplo las actualizaciones de software, ya que en un sistema de Virtual Chassis solo el switch Master debe tener el sistema operativo actualizado. Sin embargo, si todos los miembros funcionan como switches independientes, todos los miembros individuales deben actualizar su sistema operativo de manera separada. También, en un escenario de Virtual Chassis, no existe la necesidad de ejecutar Spanning Tree Protocol (STP) entre los miembros individuales debido a que en todos los aspectos funcionales, un sistema de Virtual Chassis es un simple dispositivo.

En una configuración de Virtual Chassis, el sistema nos proporciona redundancia en el plano de control, donde uno de los switches miembro es elegido como el switch master y un segundo switch miembro es escogido como un switch backup. Este enfoque de diseño nos proporciona una redundancia en el plano de control y es un requerimiento en

muchos entornos empresariales.

Un Virtual Chassis consiste de cualquier combinación de modelos de switches de la familia de switches EX4200 (EX4200-24T, EX4200-24P, EX4200-48T, EX4200-48P), cada switch EX4200 tiene dos a tres Packet Forwarding Engine (PFEs) dependiendo de la plataforma, todos los PFEs son interconectados ya sea a través de conexiones internas o a través de los Virtual Chassis Ports (VCPs) ubicados en la parte posterior de la plataforma EX4200. De forma colectiva los PFEs y sus conexiones constituyen el backplane del Virtual Chassis, la Figura 2.2 muestra los diferentes escenarios de implementación de un Virtual Chassis.

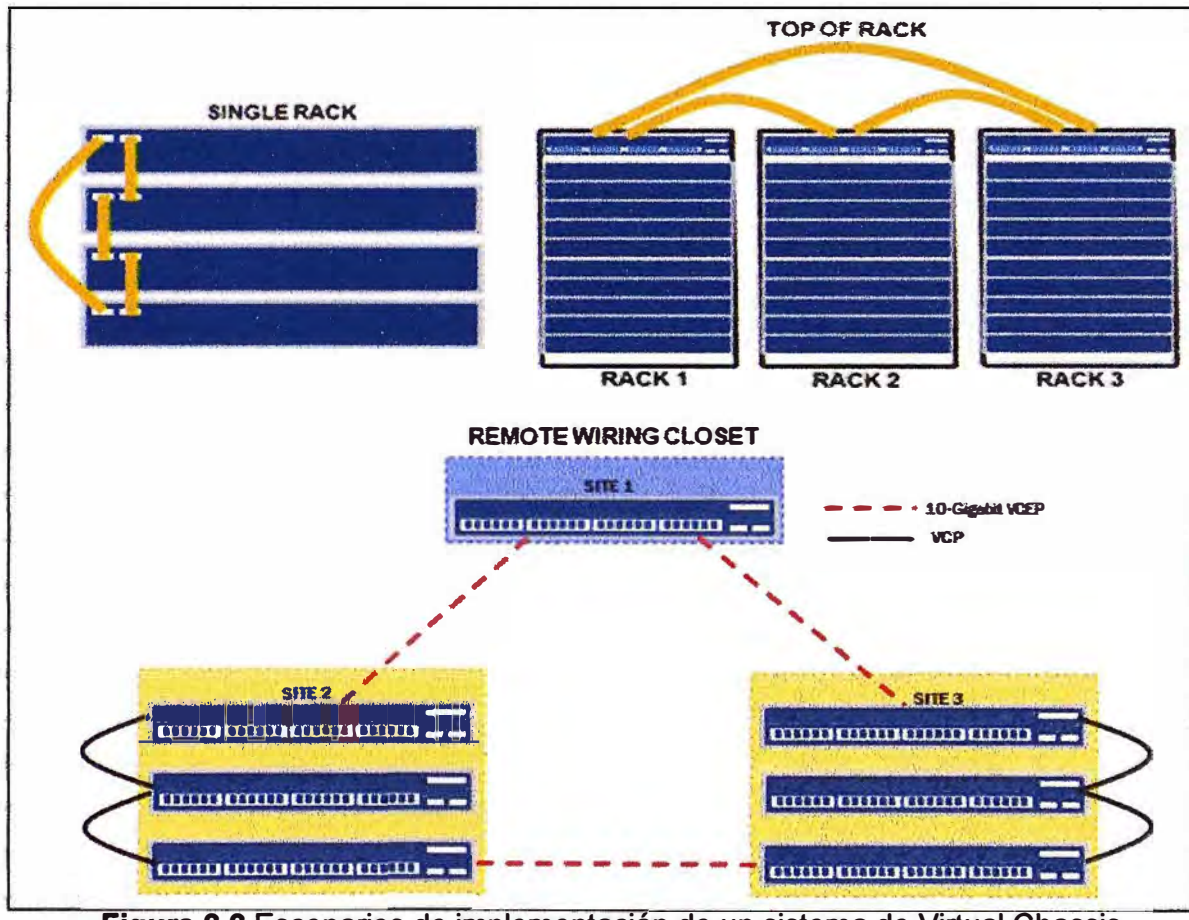

Figura 2.2 Escenarios de implementación de un sistema de Virtual Chassis.

Un sistema de Virtual Chassis tiene dos componentes; a) Virtual Chassis Port (VCP), b) Virtual Chassis Extender Ports (VCEP).

a. VCP (Virtual Chassis Port)

Usa cables propietarios de marca Juniper Virtual Chassis Backplane (VCB) para conectar los switches miembros, los VCPs son ubicados en la parte posterior de los switches EX4200, para su funcionamiento no se quiere configuración alguna.

b. VCEP (Virtual Chassis Extender Port)

Usa fibra óptica para conectar switches miembros remotos, se requiere de módulos de 10 Gigabit Ethernet como módulos uplink, el VCEP debe ser habilitado manualmente. Entre

los modos comunes de implementación incluyen, Single-rack el cual se extiende a menos de cinco metros, Top-of-rack el cual puede expandirse hasta los quince metros, y el Remote Wiring Closet, en el cual se hace uso de los VCEPs para interconectar switches distribuidos físicamente en salas de comunicaciones remotas, logrando extenderse hasta los 500 metros.

2.9 Alta disponibilidad

A medida que el tiempo transcurre, la importancia de las comunicaciones incrementa exponencialmente, por lo que los sistemas informáticos y las plataformas de redes actuales deben implementarse con el diseño que pueda asegurar que no exista interrupciones en la comunicación.

La Alta disponibilidad consiste en una serie de medidas tendientes a garantizar la disponibilidad de uno o varios servicios prestados, es decir, asegurar la continuidad del servicio.

Para el fabricante Juniper Networks las plataformas de switching ejecutando Junos OS, la alta disponibilidad hace referencia a los componentes en hardware y software que proporcionan redundancia y confiabilidad a las comunicaciones basadas en paquetes, la familia de switches del fabricante Juniper Network, soporta las siguientes características de alta disponibilidad; a) VRRP, b) Graceful Protocol Restart, c) Redundant Routing Engines, d) Virtual Chassis, e) Graceful Routing Engine Switchover, f) Link Aggregation, g) Nonstop Active Routing, y h) Nonstop Software Upgrade.

a. Virtual Router Redundancy Protocol VRRP

La habilitación de esta facilidad le permite a un switch actuar como una plataforma de enrutamiento virtual, de esta forma permite a las estaciones de trabajo de una red LAN hacer uso de una plataforma de enrutamiento redundante sobre esta red LAN sin requerir más que una configuración estática de una simple puerta de enlace predeterminada en los nodos.

Las plataformas de enrutamiento comparten la dirección correspondiente a la puerta de enlace predeterminada configurada en los nodos, en cualquier instante, una de las plataformas de enrutamiento es el master(activo) y el resto son backups. Si la plataforma de enrutamiento master falla, una de las plataformas backup se convierte en el nuevo master.

b. Graceful Protocol Restart

En una implementación estándar de protocolos de enrutamiento, cualquier servicio de interrupción requiere en un switch a poder recalcular adyacencias con los switches vecinos, restaurando las entradas de la tabla de enrutamiento, y actualizando información específica de otros protocolos. El beneficio principal de Graceful Protocol Restart son el

ininterrumpido Packet Forwarding y la supresión temporal de todas las actualizaciones de protocolos, de esta forma permite a un switch a pasar a través de estados de convergencia intermedias que son ocultas para el resto de la red.

c. Redundant Routing Engines

La redundancia consiste en contar con dos Routing Engine en un switch. Cuando un switch tiene dos Routing Engines, uno funciona como master, mientras que el otro funciona como backup ante la falla del Master Routing Engine. El Master Routing Engine recibe y transmite información de enrutamiento, construye y mantiene la tabla de enrutamiento, se comunica con las interfaces y el Packet Forwarding Engine del switch, y tiene un completo control sobre el plano de control del switch. El Backup Routing Engine se mantiene en sincronización con el Master Routing Engine en término de estado de protocolos, tablas de forwarding, y demás.

d. Virtual Chassis

Un Virtual Chassis es la interconexión de múltiples switches que operan como una única entidad de red. Las ventajas de múltiples conexiones de switch en un Virtual Chassis, incluye una mejor gestión de ancho de banda en la capa de red, configuración y mantenimiento simplificado debido a que múltiples switches pueden ser administrados como un único dispositivo.

e. Graceful Routing Engine Switchover

Al habilitar esta funcionalidad en un switch con un redundante Routing Engine o en un Virtual Chassis, permite controlar con una mínima interrupción en las comunicaciones de red del Master Routing Engine a el Backup Routing Engine. Es en este escenario que el Backup Routing Engine automáticamente sincroniza con el Master Routing Engine para preservar información de estado del kernel y estado de la tabla de Forwarding, cualquier actualización en el Master Routing Engine se replica en el Backup Routing Engine tan pronto como sucedan.

f. Link Aggregation

Se puede combinar múltiples puertos Ethernet físicos para formar un enlace lógico punto a punto, conocido como Link Aggregation Group (LAG) o bundle. Un LAG nos proporciona más ancho de banda y redundancia en la red balanceando el trafico de red a través de todos los enlaces disponibles, si uno de los enlaces falla, el sistema automáticamente balancea el trafico a través de los enlaces restantes.

g. NSR (Nonstop Active Routing)

Proporciona alta disponibilidad en un switch con redundante Routing Engine permitiendo una transparente conmutación del Routing Engine sin requerir reiniciar los protocolos de enrutamiento soportados, ambos Routing Engine están completamente

activos en el procesamiento de sesiones, siendo que cada uno pueda hacerse cargo del otro. La conmutación es transparente a los dispositivos de enrutamiento vecinos, los cuales no detectan que un cambio ha ocurrido.

h. NSSU (Nonstop Software Upgrade)

Esta facilidad se encuentra disponible en los switches EX8200 con redundante Routing Engine y en un Virtual Chassis con redundante Routing Engine externos. NSSU toma ventaja del Graceful Routing Engine Switchover y Nonstop Active Routing para permitir actualizar la versión de Junos OS en un switch o Virtual Chassis con ninguna ruptura en el plano de control.

2.10 Arquitectura del Backbone

El diseño e implementación de una red de Backbone exige incluir diversos criterios que permiten poner en funcionamiento el diseño propuesto. A continuación se describen: 1) Switch Fabric, 2) Backplane, 3) Supervisora, 4) Tasa de procesamiento, 5) Modulo SRE, 6) External Routing Engine, 7) Modulo SF, 8) Tarjetas de línea, 9) Sistema de enfriamiento, y 10) Fuentes de energía.

2.10.1 Switch Fabric

Es el elemento de conmutación del switch, cuya estructura interna es similar a una matriz de conmutación interna que conecta todos los puertos del switch, cuyo componente permite la conmutación de los paquetes entre los diferentes puertos del switch. Su capacidad de conmutación se mide en Gbps.

2.10.2 Backplane

Viene a ser la placa de circuito impreso en la parte posterior del switch que conecta entre si las diferentes tarjetas formando un bus. Es un elemento pasivo por tanto no se toma en cuenta para el cálculo de la capacidad de procesamiento o conmutación en el equipo conmutador, ya sea un switch y/o otro dispositivo.

2.10.3 Tarjeta supervisora

También conocida como tarjeta controladora o Engine, es la tarjeta principal de procesamiento del switch, la cual aloja al switch fabric.

2.10.4 Tasa de procesamiento

La tasa de procesamiento de paquetes o Layer 2 Forwarding Rate, define cuantos paquetes son enviados por segundo, siendo sus unidades de medición en Mbps.

2.10.5 Modulo SRE

La funcionalidad de switching, administración del sistema, y función de control del sistema de un switch modelo EX8208 son realizados por un modulo Switch Fabric and Routing Engine (SRE). Un modulo SRE contiene un Routing Engine y un Switch Fabric, siendo este ultimo el sinónimo del Packet Forwarding Engine.

En un switch modelo EX8208 se pueden instalar uno o dos módulos SRE, en cuyo caso de tener dos módulos SRE, uno modulo SRE funciona como el master y el otro funcionaria como el backup, si el master SRE falla o es removido, el modulo backup asume el rol de master. El modulo SRE backup automáticamente sincroniza la configuración y el estado actual con el modulo master.

2.10.6 External Routing Engine XRE

Un External Routing Engine es usado para crear un Virtual Chassis compuesto de switches Ethernet EX8200 de Juniper Networks, y a su vez reemplazan el papel que cumple un modulo SRE para el Virtual Chassis.

Para poder formar el Virtual Chassis a través del XRE se conectan los Virtual Chassis Ports (VCP) del XRE, los cuales pertenecen a los módulos Virtual Chassis Control Interface (VCCI), la cual está compuesta por 4 interfaces 10/100/1000Base-T, estos son conectados a los puertos de administración (MGMT) de cada uno de los Internal Routing Engine de los switches que pertenecerán al Virtual Chassis, el Virtual Chassis es formado automáticamente cuando estas conexiones son establecidas. Un segundo XRE podría ser adicionado a la configuración, para así proporcionar redundancia al Virtual Chassis.

El Internal Routing Engine y el External Routing Engine se comunican a través del protocolo propietario Virtual Chassis Control Protocol (VCCP).

2.10.7 Modulo SF

El modulo de Switch Fabric, trabaja con el modulo SRE, proporciona la funcionalidad necesaria de switching para una configuración del switch EX8208. En una configuración redundante el modulo SF proporciona una redundancia del switch fabric, este modulo adicional de switch fabric proporciona una completa configuración 2 + 1 redundante de switch fabric, en los modelos de switches EX8200 se puede adicionar un modulo SF en todo el chassis.

2.10.8 Tarjetas de línea

El switch EX8208 al ser modular, proporciona los diferentes tipos de interfaces a la red a través de tarjetas de línea, los cuales tienen la facilidad de poder ser removidos o insertables sin necesidad del apagado del switch, entre los diferentes tipos de tarjetas de línea se tienen desde las que proveen de interfaces Ethernet 10/100/1000Base-T hasta tarjetas de linean que proveen interfaces de 10 Gigabit Ethernet. Estas dentro del chassis se encuentran tienen posiciones especificas para su instalación, la cual debe ser tenida en cuenta para su correcto funcionamiento.

2.10.9 Sistema de enfriamiento

El sistema de enfriamiento en los switches EX8208 consiste de una bahía de ventiladores que puede ser removido o insertado sin necesidad de apagar el switch, la

bahía contiene un total de doce ventiladores, la cual se instala de manera vertical, por la parte frontal izquierda del chassis y así proporcionar una ventilación de lado a lado al chassis, un sistema de enfriamiento es muy importante en todo equipo de comunicaciones más aun tratándose de un equipo que se compone de múltiples elementos que requieren de energía para su funcionamiento, como las tarjetas de línea, fuentes de energía, los módulos SRE, modulo SF, etc.

2.10.10 Fuentes de energía

Las fuentes de energía en los switches EX8208 son completamente redundantes, balancean su carga, y pueden ser removidos o insertados sin necesidad del apagado del switch, cada una de las fuentes de energía se conecta al Backplane del chassis, el cual distribuye la energía de salida producida por las fuentes de energía a los diferentes componentes del switch, una configuración N+1 de energía es requerida para tener una redundancia en fuentes de energía, en esta configuración, si una fuente de energía falla o es removida en el tiempo de operación del switch, las fuentes de energía restantes aun continúan suministrando la energía suficiente y requerida por el sistema, la Figura 2.3 muestra una el detalle de los componentes del switch EX8208.

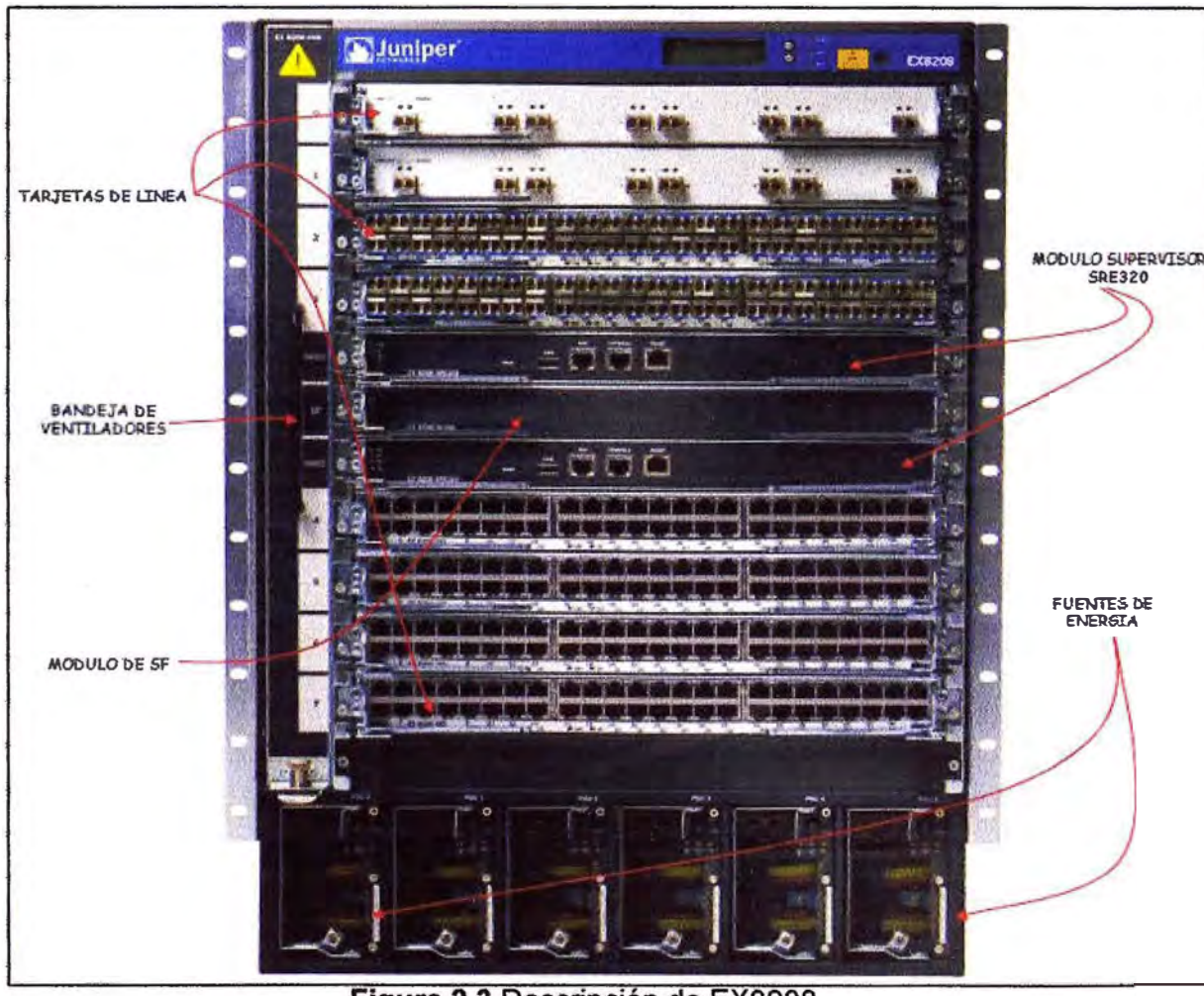

Figura 2.3 Descripción de EX8208

CAPÍTULO III
ANALISIS Y DISEÑO DE LA SOLUCION TECNOLOGICA

En el presente capítulo se describe el análisis y la descripción de la solución tecnológica propuesta a la entidad financiera. Se exponen los diferentes aspectos que han relevantes para la toma de decisión de la renovación tecnológica, así como los aspectos técnicos tenidos en cuenta para el diseño de la solución, de esta manera poder explicar el estudio del pre-diseño y post-implementación de la solución propuesta, mostrando seguidamente el aspecto conceptual del diseño y el equipamiento usado.

3.1 Análisis de la problemática:

Con el propósito de diseñar y proponer una plataforma de Backbone para la red de datos de alta disponibilidad para una entidad financiera, se realizó una serie de procedimientos con el objetivo de analizar, identificar y describir los diferentes frentes que degradan la calidad de la plataforma de red actual de la entidad financiera, las cuales se resumen en los siguientes puntos:

3.1.1 Topología física

Para poder obtener la información exacta del diseño actual de la plataforma de la red de datos de la entidad financiera, se requirió comparar la información suministrada por el cliente, la cual consistía de un diagrama topológico desactualizado indicando solo parte de los diferentes elementos de red, siendo esta información actualizada con la información recabada durante el periodo previo a la presentación de la propuesta técnica económica como parte de la etapa de pre venta de la solución, habiendo realizado este último proceso en múltiples visitas de manera periódica durante un mes, obteniendo asi el detalle de la topología física actual de la entidad financiera, y por consiguiente identificando equipamiento como conmutadores y repetidores que degradaban el rendimiento de la red, además de identificar conexiones de anillos usando tecnologías Ethernet y Fast Ethernet de manera combinada que el cliente no tenía conocimiento de su existencia en su red, y por último se pudieron determinar múltiples loops físicos existentes en los diferentes elementos de red que por motivos de falta de identificación y conocimiento tecnológico existían en la red, dado que el equipamiento de la red del cliente consistía en un 80% de su totalidad de equipos de marca Nortel, la tarea de análisis se llevó a cabo mediante una herramienta llamada Enterprise Switch Manager

ESM, del mismo fabricante, de esta forma se pudo obtener una información más fiable de la topología actual como la detección de los diferentes inconvenientes a nivel topológico.

3.1.2 Topología lógica

Para poder determinar la topología lógica de la cual consistía la red de la entidad financiera, de primera instancia nos concentramos en los nodos principales que manejaban el enrutamiento entre los diferentes segmentos de red, seguido realizamos múltiples procesos de trazas y escaneos de red con herramientas como traceroute y nmap que nos ayudaron a obtener una mejor comprensión de la red lógica, y por último nos reunimos con las diferentes áreas de la entidad financiera para consultar y coordinar por los segmentos de red que manejaban, siendo este último de gran utilidad para poder identificar segmentos de red nulos, de la información consolidada se detectó direccionamiento IP cuyas mascaras de red llegaban a una capacidad 2^{16}-2 estaciones de red de los cuales solo se usaban el 3% o 4% de su capacidad, por otro lado también se determinaron subnets que no estaban en uso, subnets no identificadas por el cliente y subnets de capacidad de 2^{7}-2 de estaciones de red en los que se requería de una mayor capacidad de estaciones de red, en conclusión, de manera lógica no existe un mecanismo de separación del dominio de broadcast de toda la red, además de existir una adecuada segmentación de red que se adecue a la cantidad de estaciones según la demanda.

3.1.4 Saturación de enlaces principales

Dado que la infraestructura de red de la entidad financiera consiste de una red distribuida en diferentes ubicaciones físicas cuyos enlaces de interconexión entre oficinas principales estaban comprendidas por enlaces cuyas capacidades de caudal bordeaban los 300Mbps en promedio, era común presentar inconvenientes de saturación en los enlaces principales dada la necesidad de uso de nuevas aplicaciones corporativas que exigen un mayor ancho de banda y por la ausencia de contar con algoritmos de control de congestión, encolamiento de tráfico, y priorización de paquetes que permitan que las aplicaciones no puedan ser manipuladas de manera adecuada.

3.1.4 Gestión unificada

La ausencia de un sistema de gestión unificado que pueda provisionar cada uno de los elementos de red, gestionar los diferentes parámetros de configuración del equipo y monitorear las diferentes alarmas de rendimiento, interfaces, saturación, nivel de procesamiento, calidad de servicio, niveles de voltaje, niveles de temperatura, funcionamiento adecuado de los ventiladores, y demás parámetros a monitorear en los múltiples elementos de red originaban que no se identifique y pueda tomarse acciones inmediatas ante algún inconveniente sobre la plataforma de red.

3.1.5 Obsolescencia tecnológica

En base al inventario que se realizó de toda la plataforma de red se pudo determinar que el 75% de equipos contaban con versiones de software obsoletas con inconvenientes a nivel funcional, además de encontrar equipos los cuales el fabricante Nortel ya no proveía soporte a nivel de software y hardware por la antigüedad de los mismos, por lo que la entidad financiera demando una renovación tecnológica dejando atrás los equipos obsoletos y poder mantener una única línea de versión de software recomendada por el fabricante y que provea lo último en funcionalidades de red a la solución propuesta.

3.2 Propuesta de solución tecnológica

En esta sección se expondrán las necesidades propias de la entidad financiera para la utilización de la solución implementada, además de describir a la entidad financiera y sus principales requisitos técnicos.

3.2.1 Aspectos técnicos de la entidad bancaria

La entidad financiera tiene implementado una configuración de alta disponibilidad con dos switches de marca Nortel, cuya configuración no tiene una redundancia geográfica (Data Center de contingencia), el cual es un requerimiento necesario y obligatorio para toda entidad bancaria hoy en día, de esta manera mejorar el modelo de distribución de su plataforma de red, y así aumentar la confiabilidad y disponibilidad de las diferentes aplicaciones de uso corporativo.

La organización tiene un objetivo claro de sus necesidades en lo que respecta a maximizar el tiempo operacional de la plataforma de la red de Backbone, así como el de tener la red operativa, eficiente, segura, y constantemente monitoreada; para poder lograr este objetivo la entidad financiera optó en su momento por una plataforma cuya tecnología no era escalable, y con el paso del tiempo no ha podido soportar las necesidades técnicas que se han presentado. En lo que respecta a disponibilidad, el banco ha sufrido caídas del servicio en su Core, debido a la falta de funcionalidades como detección de lazos físicos de red, mecanismos de seguridad a nivel de conmutación de paquetes, los cuales puedan evitar que toda la plataforma de red se vea afectada ante algún evento que afecte a las aplicaciones de uso corporativo, en ocasiones también se ha visto afectada la red por el incremento en las tasas de transferencia de información que demanda las nuevas aplicaciones de uso interno a la entidad financiera, como por ejemplo aplicaciones de video en tiempo real, y aplicaciones que hacen uso de tráfico Multicast.

El diseño de red lógico/físico simplificado de esta organización es definido en el diagrama siguiente (Figura 3.1) y corresponde a la situación actualmente implementada. Un mayor detalle es mostrado en la Figura B.1 del Anexo B “Diagramas del sistema”.

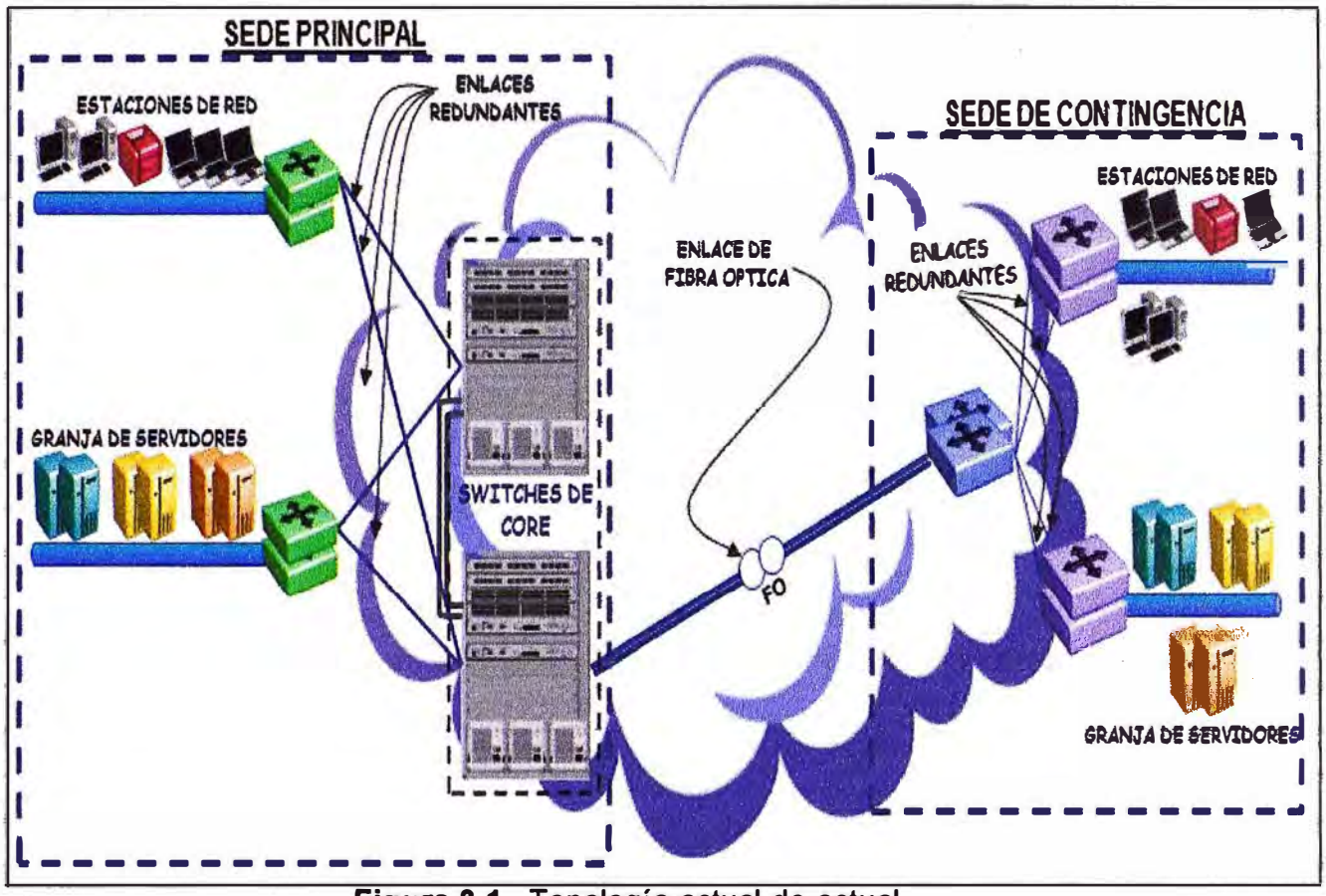

Figura 3.1 Topología actual de actual.

La figura anterior incluye la oficina principal y la oficina de contingencia. En virtud de la claridad, sólo se muestran algunos servidores y clientes.

3.2.2 Criterios para el diseño

Los criterios seguidos para la propuesta de la solución son los siguientes: a) Experiencia certificada, b) Instalación y soporte técnico, c) Cumplimiento de especificaciones técnicas, d) Rendimiento, e) Redundancia, f) Resistencia, g) Calidad de servicio, y h) Seguridad de redes.

a) Experiencia certificada

La entidad proveedora local de la solución deberá estar certificada por el fabricante para las labores de diseño, implementación y soporte técnico; y contar como mínimo con cinco años de experiencia en la marca ofertada. Para lo cual deberá presentar una carta de representación del fabricante, copias de certificaciones oficiales, copias de de facturas o contratos, y copia simple de su constitución de la empresa.

El personal técnico asignado al proyecto deberá contar con las certificaciones oficiales del fabricante que lo habiliten para realizar labores de instalación, configuración y mantenimiento de la solución ofertada.

b) Instalación y soporte técnico

Comprende la gestión, atención, ejecución de servicios, suministros, materiales y

soporte técnico por parte de la entidad proveedora local de la solución propuesta, para el fiel cumplimiento y total funcionamiento de la solución y los requerimientos de la entidad financiera, dentro del ámbito y condiciones de la implementación de la solución, para lo cual:

1) El proveedor local de la solución, se compromete en brindar a la entidad financiera el servicio de mantenimiento integral de los switches de Core – Sede principal, incluyendo limpieza de todos los componentes como CPU's, tarjetas periféricas, y Backplane, de acuerdo a las recomendaciones del fabricante.

2) El proveedor local de la solución, deberá realizar el Upgrade de hardware y software del Core existente en la sede principal a la última versión vigente, de acuerdo a las recomendaciones del fabricante.

3) El proveedor local de la solución, deberá realizar el servicio de instalación, configuración y puesta en funcionamiento de cuatro switches de Core tipo chassis modular, de los cuales dos serán para la sede principal, y los restantes para la sede de contingencia.

4) Dentro de los servicios de integración y optimización de las funcionalidades del Backbone de la entidad financiera, se involucra la distribución de tarjetas, balanceo de enlaces de fibra óptica, funcionalidad de redundancia y alta disponibilidad habilitada, creación de VLANs de usuarios, creación de VLANs de administración, y habilitación del software de administración.

5) El proveedor local de la solución, también deberá incluir en su propuesta técnica economía el contrato de soporte directo a fabrica, para todo el equipamiento ofertado, vigente durante doce meses, contados a partir de la puesta en marcha, y que involucre el soporte, update y upgrade del software, con reemplazo de hardware al siguiente día útil de reportado la falla.

6) Se deberá ofertar también un periodo de gestión y soporte local de la red implementada, realizada a través de un (01) ingeniero residente on site, no menor de (06) meses.

7) El postor deberá presentar un plan de trabajo, considerando equipo de trabajo, cronograma de actividades, protocolos de prueba y entregables.

8) La ejecución de los servicios deberá realizarse en un plazo no mayor de 45 días calendario, y deberá incluirse un periodo de soporte de post-instalación de 15 días para monitorear y garantizar el correcto funcionamiento de la solución implementada.

9) Finalizada la puesta en servicio, el postor presentará en informe impreso y digital, con la memoria descriptiva, indicando el hardware suministrado, el software, licencias y

configuraciones realizadas, se deberá entregar además un CD backup de la ultima configuración de las sedes.

10) Finalmente, el postor deberá dejar óptimamente funcionando los switches de Core para la integración y mejora del Backbone de la entidad financiera, con todo el hardware, software y servicios que se requieran, según las disposiciones de la entidad financiera, para lograr el objetivo sin costo adicional para la entidad financiera.

c) Cumplimiento de especificaciones técnicas

El proveedor local de la solución, deberá ofertar la cantidad necesaria de equipamiento por sede (oficina principal y de contingencia), suministrará la cantidad y tipo de interfaces que se requieran para el funcionamiento correcto y completo de la solución propuesta, considerando las características, funcionalidades, y su cumplimiento para todo el equipamiento propuesto dentro de la solución:

1) Ampliación en sede principal

Se requiere realizar el upgrade de los dos (2) switches de Core existentes y configurados en alta disponibilidad, puestos en producción a la última versión de software recomendada por el fabricante.

La nueva solución propuesta deberá componerse de dos (2) switches de Core existentes, para que trabajen como Cluster[3] redundante en una configuracion activo-activo, los cuales deberán ser del tipo chassis modular, con inteligencia de capa 2 a 7, cada Core deberá contener dos (02) CPU's, 96 puertos 10/100/1000 BaseT Ethernet, 96 puertos 100FX/1000Base-X, 8 puertos 10Gb Ethernet, y fuentes de energía redundantes, deberá soportar interna de filtrado de paquetes, capacidad de poder crear cluster a terabit. Capacidad de poder escalar hasta 384 puertos Gigabit Ethernet y 64 puertos 10Gb Ethernet, así como el de permitir conectividad 40Gb y 100Gb Ethernet para uso futuro.

Siendo la configuración mínima de la oferta en hardware y software instalada y operativa, para cada uno de los switches de Core, la siguiente:

a) 2 tarjetas supervisoras o CPU/Switch Fabric por cada switch de Core.
b) Fuentes de alimentación redundante de 100-240VAC en configuración N+1.
c) 1 tarjeta de ocho puertos 10Gb Ethernet para cada uno de los switches de Core.
d) 1 tarjeta de 48 puertos 10/100/1000 BaseT Ethernet, para cada uno de los switches de Core.
e) 1 tarjeta de 48 puertos 100FX/1000Base-X Ethernet, para la instalación en cada uno de los switches de Core.

---

[3] Agrupación de switches conectados entre si para formar una única entidad.

f) La capacidad de Backplane del switch modular deberá de ser de por lo menos de 4Tbps.

g) El Throughput de cada uno de los switches deberá ser de por lo menos de 600Mbps por sistema.

h) El equipo deberá ser instalado en un rack de 19 pulgadas.

2) Core – Sede de contingencia

Es en la sede de contingencia en la cual se tiene toda una plataforma de servidores, los cuales forman una réplica de las diferentes aplicaciones de uso de la entidad financiera, por lo cual con la propuesta de instalación de la Backbone del Core de la entidad financiera, se contempla la replicación exacta en switches de Core para la oficina de contingencia, por lo cual el requerimiento en equipamiento deberá ser el mismo que en la sede principal, el cual sería como sigue:

a) 2 tarjetas supervisoras o CPU/Switch Fabric por cada switch de Core.

b) Fuentes de alimentación redundante de 100-240VAC en configuración N+1.

c) 1 tarjeta de ocho puertos 10Gb Ethernet para cada uno de los switches de Core.

d) 1 tarjeta de 48 puertos 10/100/1000 BaseT Ethernet, para cada uno de los switches de Core.

e) 1 tarjeta de 48 puertos 100FX/1000Base-X Ethernet, para la instalación en cada uno de los switches de Core.

f) La capacidad de Backplane del switch modular deberá de ser de por lo menos de 4Tbps.

g) El Throughput de cada uno de los switches deberá ser de por lo menos de 600Mbps por sistema.

d) Rendimiento

1) El atraso máximo deseable para un paquete medido entre una puerta de entrada y una puerta de salida a carga completa no deberá ser mayor de 10milisegundos.

2) La matriz de conmutación (Switching Fabric) debe ser del tipo no bloqueante y del tipo "Full Duplex).

3) El equipamiento debe ser capaz de procesar el tráfico generado por todas las interfaces requeridas, con 100% de utilización de paquetes de 64bytes, inclusive con los mecanismos de calidad de servicio habilitados.

4) La falla La falla de cualquier unidad de procesamiento el de una unidad matriz de conmutación, reloj, etc. no debe afectar la performance del equipamiento.

e) Redundancia

El equipamiento deberá soportar redundancia en hardware de los siguientes módulos:

1) Fuentes de alimentación.
2) Ventiladores.
3) Interfaces.

f) Resistencia

1) El equipamiento debe soportar In-service Upgrade redundancia.
2) El equipamiento debe soportar Nonstop Forwarding (NSF) para IS-IS.
3) El equipamiento debe soportar Nonstop Forwarding (NSF) para OSPF.
4) El equipamiento debe soportar Nonstop Forwarding (NSF) para MPLS LDP.
5) El equipamiento debe soportar Nonstop Forwarding (NSF) para MPLS VPN L2.
6) El equipamiento debe soportar Nonstop Forwarding (NSF) para Multicast IGMP.

g) Calidad de servicio

7) El equipamiento debe permitir el tratamiento del tráfico por interface y subinterface.
8) El equipamiento debe realizar tratamiento de filas en todas las interfaces para poder implementar calidad de servicio.
9) El oferente debe informar si el equipamiento dispone de la facilidad de reserva de banda, para aplicaciones de ruteo de voz.
10) El equipamiento debe ser capaz de implementar Per Hop Behavior de acuerdo con el modelo DiffServ.
11) El equipamiento debe ser capaz de clasificar paquetes de acuerdo con los siguientes campos:

- Campo CoS del frame Ethernet
- Campo ToS del encabezado IPv4
- Campo DSCP del encabezado IPv4
- EXP bits en el encabezado MPLS
- Dirección IP Origen
- Dirección IP Destino
- Protocolo
- 8) Puerto TCP/UDP de origen
- 9) Puerto TCP/UDP de destino
- Interface de entrada

6) De acuerdo con la clasificación local el router deberá definir las filas de salida asociadas a cada paquete.
7) El equipamiento deberá soportar por lo menos 8 filas diferentes, cada una con 4 umbrales diferentes de descarte para prevención de congestión, en cada interfaz (interfaz up-link).
8) El equipamiento deberá soportar por lo menos 4000 colas lógicas por interfaz de

acceso.

9) El equipamiento deberá soportar por lo menos 8 colas lógicas por subinterface de acceso.

10) Para cada fila deberá ser posible atribuir una ponderación directamente relacionada con la proporción de banda disponible en la interface que será alocada para la fila.

11) El equipamiento deberá soportar las siguientes filas en las interfaces de salida:

- Custom Queueing
- Strict Priority Queueing
- Weighted Fair Queueing
- Class Based Weighted Fair Queueing
- Low Latency Queueing

12) El equipo deberá implementar limitadores de banda de entrada y salida para cada interface lógica. El tráfico en exceso podrá ser marcado con prioridad de descarte, podrá ser directamente descartado el apenas contabilizado.

13) El equipo deberá implementar políticas de WRED para cada fila. El WRED deberá considerar paquetes con diferentes prioridades de descarte.

14) El equipo deberá ser capaz de reescribir los bits de precedencia de paquetes saliendo del equipamiento.

15) El equipamiento deberá ser capaz de mapear CoS en DSCP, DSCP en CoS, CoS en EXP, EXP en CoS, DSCP en EXP y EXP en DSCP.

16) Rate limiting bidireccional, por VLAN, en por lo menos, 4096 interfaces lógicas sobre una misma interface física.

17) Filtrado de paquetes bidireccional en velocidad de línea por VLAN en por lo menos 4096 interfaces lógicas sobre una misma interface física.

h) Seguridad de redes

Con el objetivo de ofrecer mayor seguridad y control sobre el tráfico, el router debe presentar las siguientes funcionalidades:

1) El equipamiento deberá proveer la funcionalidad de filtrado de paquetes permitiendo descartar paquetes indeseados.
2) El equipamiento deberá permitir la configuración de listas de control de acceso (access control lists) standard y extendidas, que realizen el filtrado basedo en criterios como: dirección de origen del paquete, número de puerto, etc.
3) Las listas de control de acceso deben ser aplicables por interface.
4) Debe permitirse la configuración de las listas de control de acceso especificándose el sentido (entrada o salida) a que se aplica.
5) Es deseable que se permita la aplicación de ACLs de acuerdo con la hora del día.

6) Será evaluada en forma positiva la posibilidad del router de poseer funcionalidad de firewall, protegiendo la red del cliente contra accesos no autorizados. El proveedor debe informar si está funcionalidad es opcional, pudiendo ser adquirida o no.
7) La funcionalidad de firewall debe permitir la detección y prevención de ataques de diversos tipos, proveer alarmas en tiempo real, etc.
8) En caso de atendimiento de este item, El proveedor debe especificar cuáles son las funcionalidades soportadas por el firewall integrado al router.
9) El equipamiento deberá proveer los siguientes mecanismos de autenticación:
10) Autenticación PAP (Password Authentication Protocol) que permite la autenticación de peers PPP (RFC 1661).
11) Autenticación CHAP (Challenge Handshake Authentication Protocol) (RFC 1661 e RFC 1994).
12) Soporte de L2TP (Layer 2 Tunneling Protocol).

3.2.3 Propuesta de diseño de la red:

Como propuesta estaba compuesta por cuatro switches EX8208 de Juniper Networks, formando la red de Backbone de la entidad financiera, se procedió a la configuración de estos, bajo las siguientes condiciones:

a) Dos switches EX8208 se ubicaran físicamente en el Data Center principal, y dos en el Data Center backup, los cuales se encuentran separados unos 40km en promedio, entre ambas sedes existe pares de fibra óptica oscura.

b) En los cuatro switches que formaran la plataforma de Backbone se actualizarán a la última versión de Junos OS recomendada por el fabricante.

c) Cada par de switches serán configurados en modo activo/activo dentro de un mismo Virtual Chassis, es gracias a los dos XRE200 distribuidos en el Data Center principal y dos en la Data Center secundario los cuales se encuentran configurados en alta disponibilidad HA que los pares de switches EX8208 de Core pueden funcionar como un único elemento de red o también denominado Virtual Chassis, para tal propósito se siguió las recomendaciones del fabricante en lo que respecta a la interconexión entre los EX8208 y los XRE200, y así reducir al mínimo las probabilidades de falla que puedan originar una paralización en la comunicación. La Figura 3.2 ilustra la interconexión que se realizó entre cada uno de los switches y los XRE200 para conseguir una configuración en alta disponibilidad funcionando en modo activo/activo.

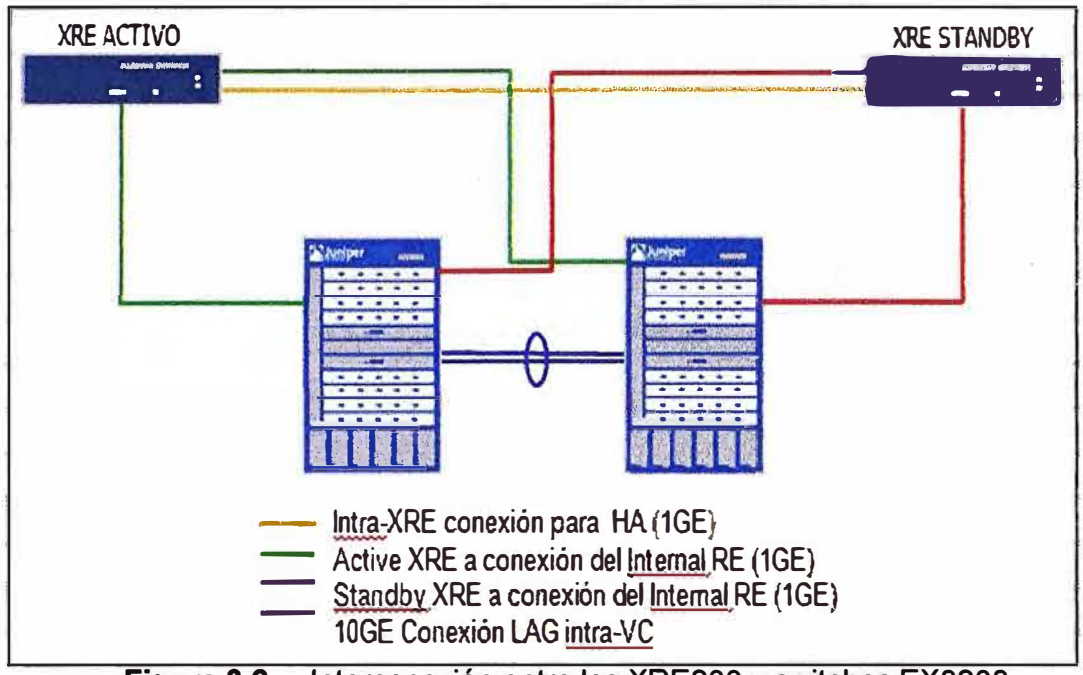

Figura 3.2 Interconexión entre los XRE200 y switches EX8208

d) Una vez instalado y configurado cada uno de los Virtual Chassis en el Data Center principal y de contingencia respectivamente, se realizará la configuración e interconexión entre los dos Virtual Chassis de ambos Data Centers mediante un único enlace LAG, el cual estará formado por cuatro enlaces de fibra óptica oscura, siendo cada uno de ellos de 10 Gigabit Ethernet, comportándose de forma lógica como un único enlace de 40Gigabit Ethernet entre ambos Data Centers, los enlaces de fibra óptica oscura ya se encuentran instalados entre ambas sedes, la topología física de interconexión será del tipo full-mesh[4]. En este diseño ambos Data Centers se compondrán de una única entidad de conmutación, el cual sería el Virtual Chassis formado por los dos XRE200 y dos EX8208 asignados para cada uno de los Data Centers, la comunicación entre los Virtual Chassis será mediante el LAG configurado de 40Gigabit Ethernet entre ambos Data Centers. La Figura 3.3 muestra la interconexión física entre los Virtual Chassis.

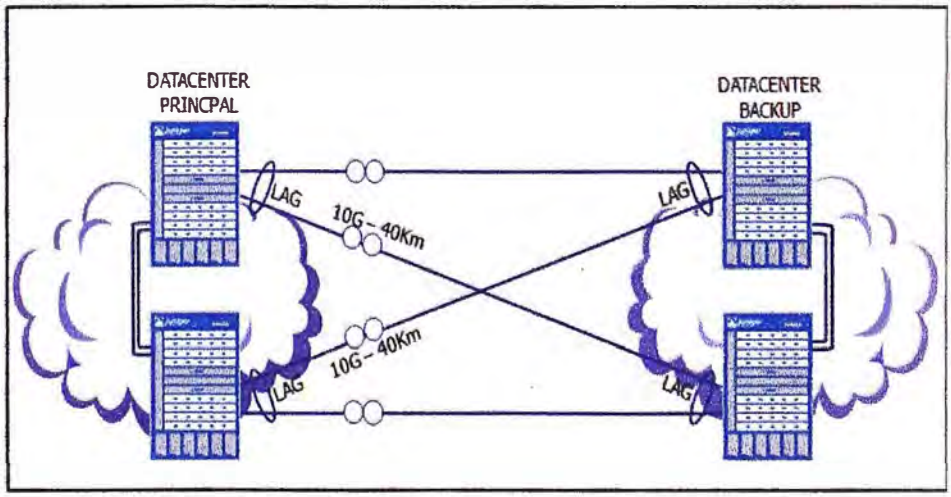

Figura 3.3 Interconexión física entre los Virtual Chassis.

[4] Interconexión física de nodos en redundancia total.

e) Una vez realizada la configuración e interconexión mostrada en la Figura 3.2, se configurará la integración entre la red actualmente operativa en la entidad financiera y la nueva Backbone de datos, cuyo enlace consistirá de un LAG de 8 miembros, sumando un total de 8Gigabit Ethernet de throughput. La Figura 3.4 muestra la interconexión entre los switches de Core existentes y la nueva plataforma de Backbone instalada.

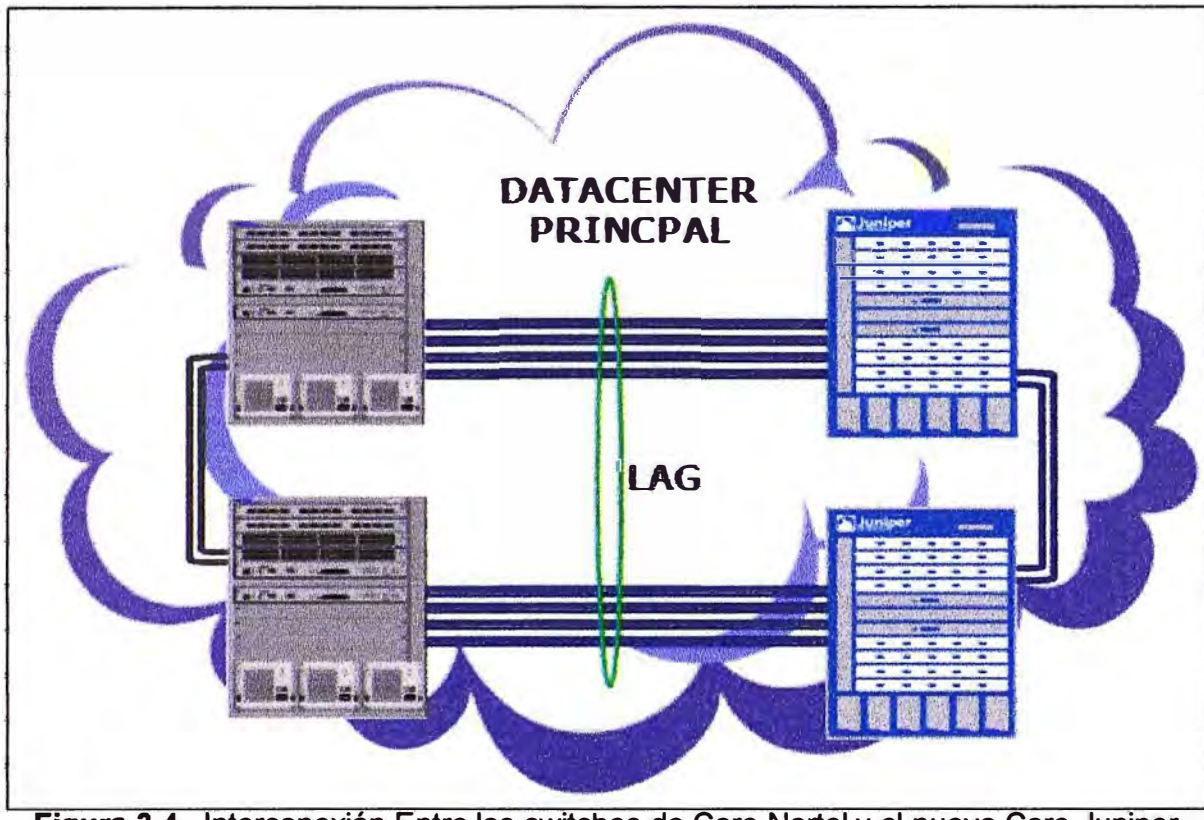

Figura 3.4 Interconexión Entre los switches de Core Nortel y el nuevo Core Juniper.

f) Una vez realizada la interconexión entre ambas plataformas de red, se empezará con la migración de los diferentes enlaces provenientes de las salas de comunicaciones existentes en la sede principal, de las conexiones que existen en el Data Center backup, finalizando con las conexiones remotas existentes.

g) Una vez migradas las diferentes conexiones físicas a la nueva plataforma de red, se procederá a la migración del direccionamiento IP, cuya información se obtuvo en el estudio de la plataforma de red actual del cliente.

El diagrama de la Figura 3.5 muestra como se implementara la Backbone de la red de datos, servidores físicos e Internet, como se vincularan y como se distribuirán entre los diferentes sitios de la entidad financiera.

Es necesario recalcar que el número de servidores que se muestran en el diagrama de diseño de la red constituye una generalización, y no la cantidad exacta de servidores, switches, y los diferentes equipos que forman parte de la plataforma de red de la entidad financiera.

Un diagrama con mayor detalle es mostrado en la Figura B.2 del Anexo B. Sin

embargo en los siguientes ítems: a) Sede Principal y b) Sede Contingencia, se muestra de forma más detallada la infraestructura de cada sede. Ambas sedes se encuentran enlazadas por fibra óptica.

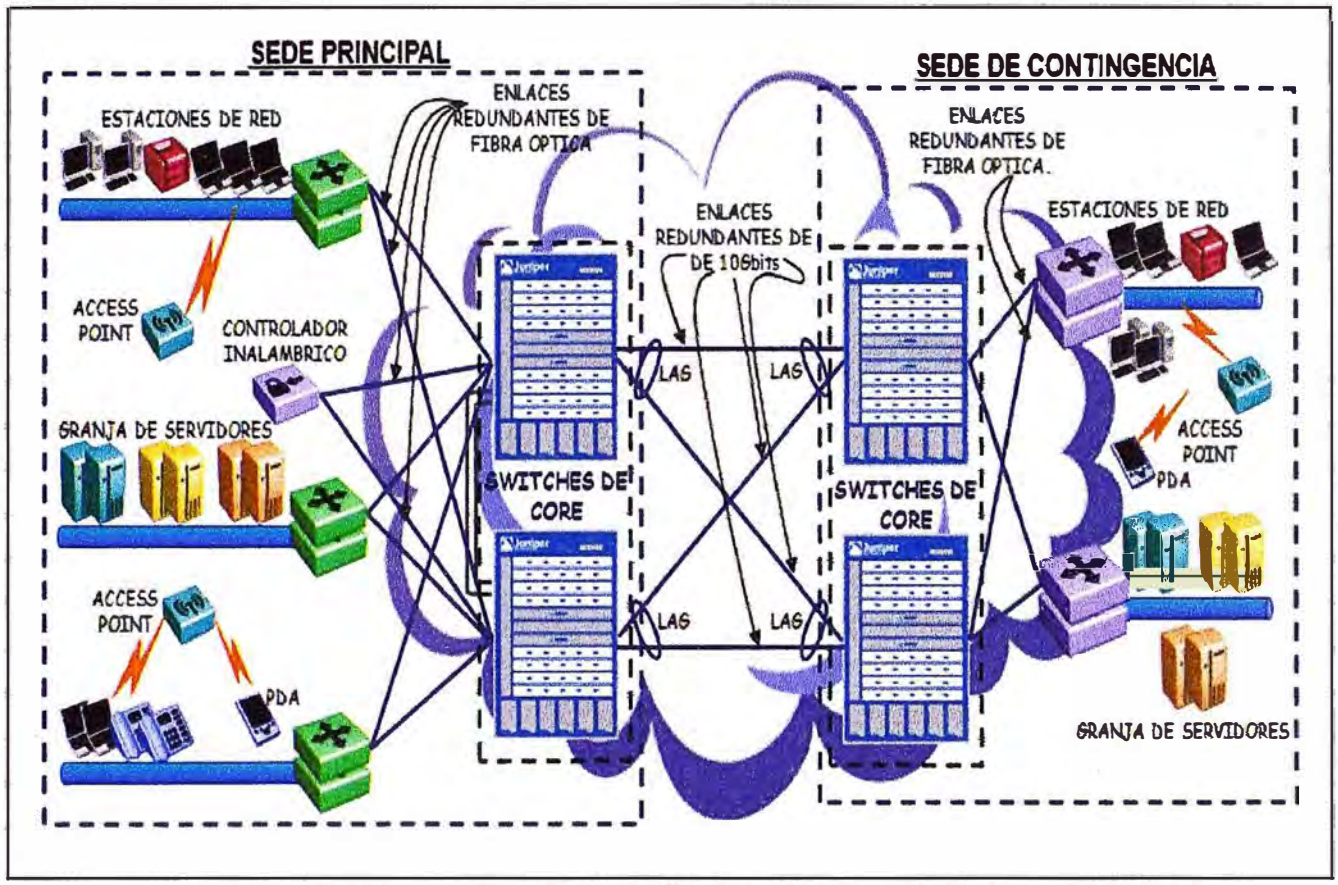

Figura 3.5 Topología de Backbone de la red de datos final

a) Sede principal

La figura 3.6 ilustra la implementación del Backbone para la red de datos de la entidad financiera y los diferentes componentes de red que comprenden sede principal.

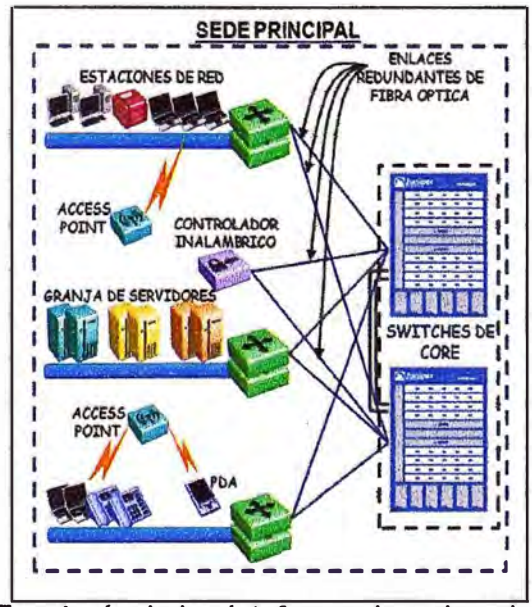

Figura 3.6 Topología de la plataforma de red en la sede principal

b) Sede de contingencia

La Figura 3.7 ilustra la implementación del Backbone para la red de datos de la Entidad financiera en la sede de contingencia y sus componentes de red.

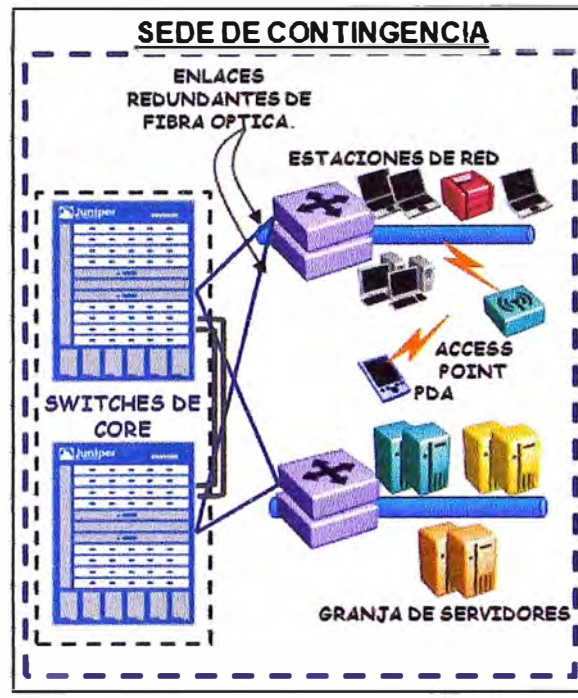

Figura 3.7 Topología de la plataforma de red en la sede de contingencia.

3.2.4 Estrategia de escalabilidad

La solución es compatible con una amplia gama de implementaciones a un costo apropiado para cada uno. Por ejemplo, una implementación de una plataforma para la cantidad de sesiones originadas por 500 usuarios debería costar proporcionalmente menos que una implementación para 5000 usuarios, la Figura 3.8 muestra la interconexión de las oficinas remotas a la nueva solución.

La complejidad de la implementación y administración también debe ser realista para esta gama de organizaciones. En la figura anterior se muestra cómo el diseño de la solución puede escalarse en forma ascendente para abarcar una gran cantidad de usuarios en la sede principal y proveer de conectividad a más sedes remotas, con una facilidad de integración a la solución implementada.

La reutilización de los componentes existentes en aplicaciones futuras es un criterio clave en el diseño. Tanto los componentes como los servidores que prestan distintos servicios a la plataforma de red, pueden rehusarse para proporcionar servicios para diversas aplicaciones.

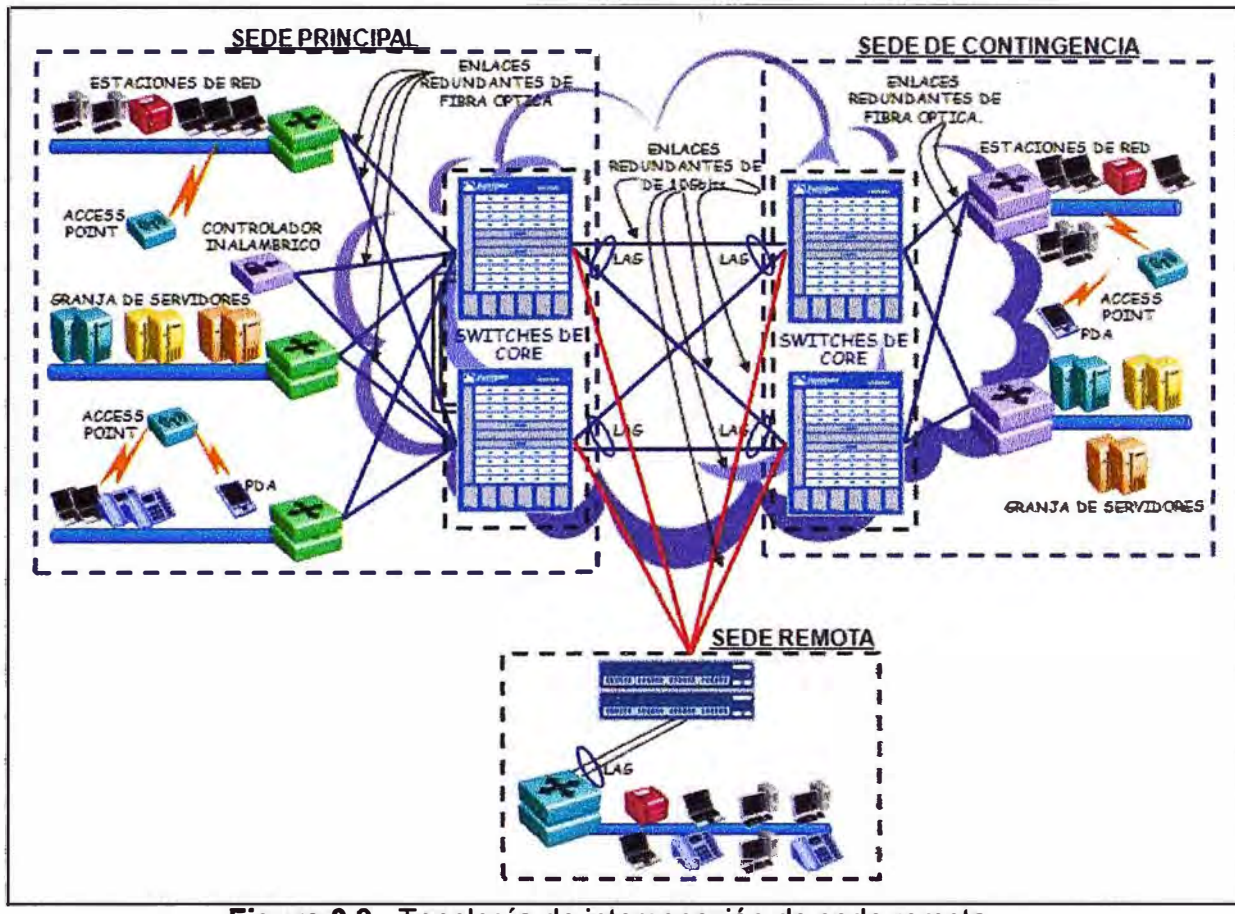

Figura 3.8 Topología de interconexión de sede remota.

3.2.5 Planificación de migración

En base a la información obtenida, se planificó la migración de las interconexiones existentes de los dispositivos de forman el Core actual, a la nueva plataforma Backbone de la red de datos que está conformado por cuatro switches modelo 8200 de marca Juniper Networks. De la información consolidada se pudo identificar que la topología física de la red en la oficina principal tiene una topología física del tipo estrella. Su entorno de red esta diferenciada en una etapa de Core y acceso, conformándose esta ultima de múltiples salas de comunicaciones (wiring closet) las cuales se interconectan a los switches de Core mediante enlaces de fibra óptica. En la etapa de Acceso los equipos de comunicación eran de fabricantes variados como Alcatel y Nortel. Estos equipos manejan VLAN, cuentan con una densidad de 24 o 48 puertos de red, así como de la capacidad de soportar el estándar IEEE 802.1Q.

En la etapa de Core se tiene instalado dos switches de Core en una configuración de alta disponibilidad con protocolos propietarios del fabricante Nortel, así como la concentración en un mayor porcentaje de los enlaces de fibra óptica provenientes de las salas de comunicaciones, de los dos pares de fibra óptica provenientes de las salas de comunicaciones, uno de ellos se conectaba a un switch de Core y el restante al segundo switch de Core, que conformaban el Core principal de la plataforma de red de la entidad financiera.

De esta manera se coordinó con personal IT de la entidad financiera que una vez configurado los cuatro switches que conformarían la nueva Backbone de la red de datos, se daría comienzo a la migración de los diferentes enlaces remotos y locales que conforman la plataforma de red, siendo esta una migración gradual que consistirá en una primera etapa en la integración de los nuevos switches de Core a los switches de Core existentes, y así proceder con una migración gradual de toda la plataforma de red existente.

3.3 Arquitectura de la solución

En la presente sección se realizará una descripción de la arquitectura de la solución.

Los objetivos de esta sección son los siguientes:

1) Proporcionar una descripción conceptual del funcionamiento de una solución de Backbone para una plataforma de red, así como de los componentes principales de este tipo de solución.

2) Definir el diseño de la solución para el diseño lógico y las fases posteriores del diseño técnico detallado.

3) Producir un diseño lógico coherente que constituya la base para el diseño detallado

4) Explicar la forma en que puede modificarse la solución para cumplir los requisitos de organización de diferentes tamaños.

5) Explicar en detalle algunas de las formas en que puede ampliarse el diseño propuesto o utilizarlo como base para generar otras soluciones de acceso de red.

6) Examinar el proceso de diseño detallado para cada uno de los componentes principales del diseño lógico de la Backbone para la plataforma de datos de la entidad financiera y poner la solución en funcionamiento.

3.3.1 Diseño conceptual

La solución necesita contar con las características siguientes:

1) Poder so portar la densidad de tráfico, y tenga la capacidad suficiente para poder soportar los requerimientos de aplicaciones de uso futuro dentro de la entidad financiera.

2) Proveer de alta disponibilidad, redundancia y confiabilidad, en los puntos críticos dentro de la plataforma instalada, de esta forma reducir al mínimo la posibilidad de verse afectado en los servicios de red, por algún posible problema en hardware o software.

3) Dada que la solución requerida presenta contingencia en hardware y software para la sede principal, así como el de tener una redundancia geográfica en la parte de Core, se espera que el tiempo de conmutación de las funcionalidades de algún elemento de red que presente un problema dentro de la solución propuesta, este debería ser el mínimo posible, de tal forma que la percepción que deberá tener el personal operativo de la entidad financiera ante un problema en la plataforma instalada, no deba ser catalogado

como una paralización de en los servicios prestados a la red.

4) El sistema no solo debe proporcionar redundancia en software y hardware, sino también el de soportar una interconexión física activo-activo entre la sede principal y la sede de contingencia, la cual debe soportar la densidad de tráfico actual, de esta forma si un enlace físico redundante dejase de funcionar, todo el trafico activo en tal enlace deberá conmutar al enlace restante.

3.3.2 Componentes principales

La Figura 3.9 muestra el diagrama conceptual de la solución con los elementos principales: a) Dispositivo de acceso, b) Aplicaciones, c) Red de acceso, y d) Backbone de la red.

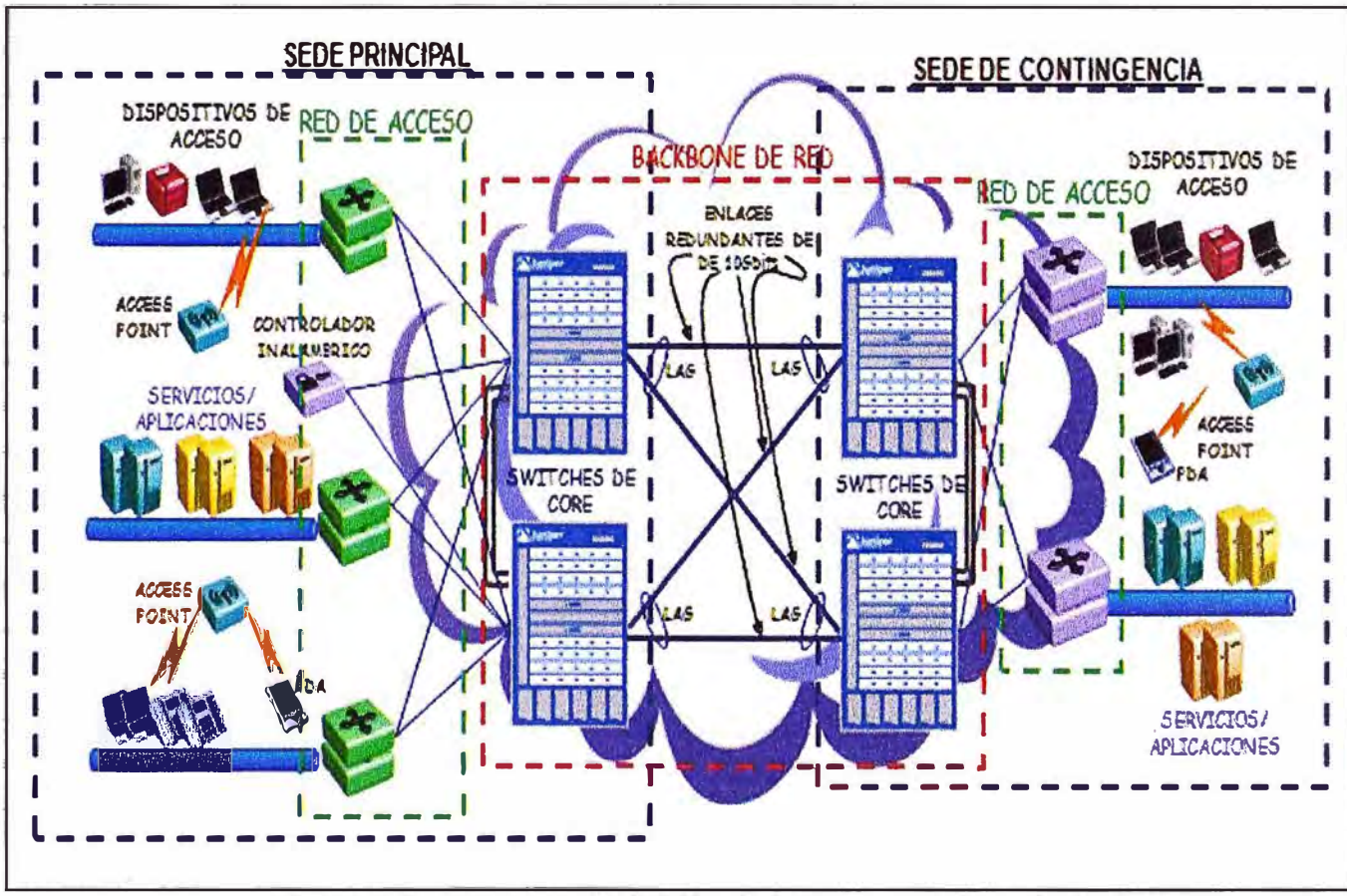

Figura 3.9 Esquema de división de los componentes principales

a. Dispositivo de acceso

Se trata de un equipo o dispositivo el cual ejecuta aplicaciones que requieren el acceso a los recursos de red, debiendo ser el acceso a estos recursos de manera no interrumpida, evitando así inconvenientes en el desempeño y productividad del usuario.

b. Aplicaciones

Vienen a ser el núcleo principal y soporte de los diferentes procedimientos de servicios administrativos y de gestión importantes para la entidad financiera.

c. Red de acceso

Es dentro de la red de acceso, que se pueden englobar todos los elementos encargados de llevar todo el tráfico de acceso de las diferentes aplicaciones de uso de la entidad financiera hasta el usuario, y atender las peticiones de este por el canal de retorno.

d. Backbone de la red

La red de Backbone es una parte de la infraestructura de red informática que interconecta varias partes de la red, proporcionando el camino para el intercambio de información entre las diferentes redes de área local.

3.4 Equipamiento utilizado

En esta sección se detallará al equipamiento (hardware y software) utilizado en el proyecto descrito: a) EX8200, b) XRE200, y c) STRM Series Security Response Managers

3.4.1 EX8200

EX8200 viene a ser la línea de switches que ofrece flexibilidad, una plataforma modular que entrega una alta densidad de puertos, escalabilidad, y alta disponibilidad requeridas por la demanda de hoy en día que se tiene para data centers y entornos de campus de Core.

la familia de switches EX8200 es la línea más alta en prestaciones de conmutación que ofrece el fabricante Juniper Networks, y es de esta familia, de la cual el modelo EX8208 se adecua a los requerimientos de la entidad financiera, y será la que se utilizó para la implementación de la solución de Backbone instalada en la entidad financiera. Ver Figura 3.10.

a) Especificaciones técnicas generales:

1. Capacidad de backplane: la capacidad por cada tarjeta de línea es de 320Gbps (full dúplex).

2. Data Rate: La rapidez con la que se trasmite los datos depende del tipo de modulo, el modulo EX8200-48T: 96Gbps, EX8200-48F: 96Gbps, EX8200-8XS: 160Gbps, y EX8200-40XS: 80Gbps.

3. Throughput: por tarjeta de línea es de 120Mbps y de 960Mbps por todo el sistema EX8208.

4. Densidad de puertos: la densidad de puertos son provistas por las diferentes tarjetas de línea, las cuales varían por la cantidad y tipo de puertos, 48 puertos 10/100/1000Mbps

en una tarjeta de línea EX8200-48T, 48 puertos de fibra 1000Mbps en una tarjeta de línea EX8208-48F.

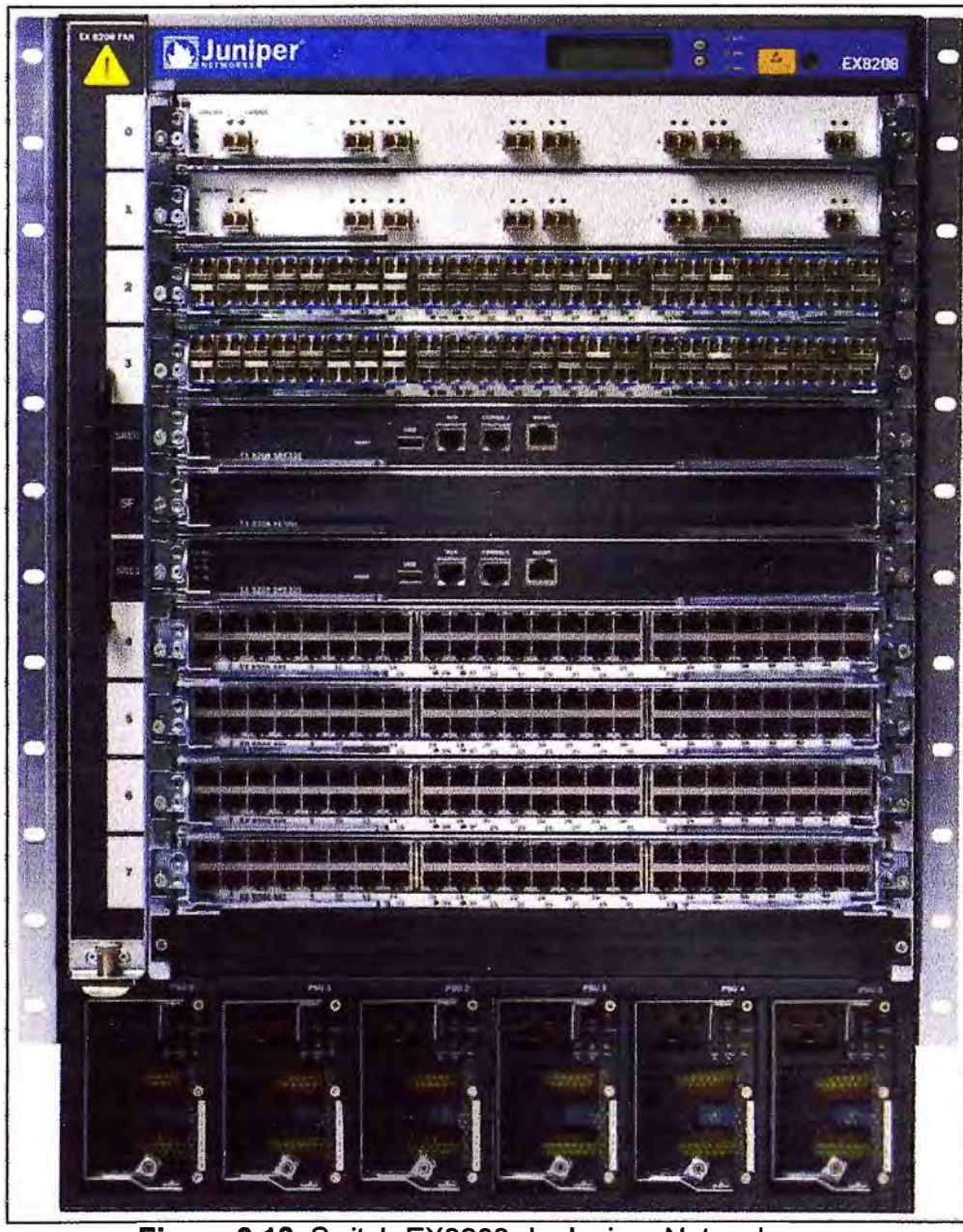

Figura 3.10 Switch EX8208 de Juniper Networks

5. Resistencia

Soporta un total de seis fuentes de energía, en una configuración redundante N+1 o N+N, estas fuentes pueden ser reemplazables aun teniendo el switch en operación, sin afectar la operatividad del Switch.

6. Opciones de energía

Soporta dos tipos de fuente de energía, los de 1200W los cuales cuentan con la auto funcionalidad de reconocimiento de energía requerida, llegando a un total de 6000W por Chassis, por otro lado se tiene las fuentes de energía de 3000W llegando a obtener hasta 15000W por Chassis.

7. **Entradas ARP**

   El sistema modular es capaz de soportar hasta 100,000 entradas de ARP.

8. **Número de VLANs**

   La cantidad de VLANs soportada por el equipo es hasta 4,096 de VLANs.

b) Especificaciones técnicas complementarias

b.1) Dimensiones y condiciones ambientales

1) **Dimensiones:** 43.82cm de ancho, 61.6cm de altura, y 53cm de profundidad.
2) **Espacio en rack:** 14 unidades de rack.
3) **Peso máximo:** 149Kg.
4) **Temperatura de operación:** 0 °C a 40 °C.
5) **Temperatura de almacenamiento:** -40 °C a 70 °C.
6) **Humedad relativa de operación:** 10% a 95% sin condensación

b.2) Cumplimiento de estándares

1) **IEEE 802.1AB:** Link Layer Discovery Protocol (LLDP)
2) **IEEE 802.1D-2004:** Spanning Tree Protocol (STP)
3) **IEEE 802.1p:** Class-of-service (CoS) prioritization
4) **IEEE 802.1Q-2006:** VLAN tagging
5) **IEEE 802.1s:** Multiple instances of Spanning Tree Protocol (MSTP)
6) **IEEE 802.1w:** Rapid reconfiguration of Spanning Tree Protocol (RSTP)
7) **IEEE 802.3:** 10BASE-T
8) **IEEE 802.3u:** 100BASE-T
9) **IEEE 802.3ab:** 1000BASE-T
10) **IEEE 802.3z:** 1000BASE-X
11) **IEEE 802.3ae:** 10-Gigabit Ethernet
12) **IEEE 802.3x:** Pause Frames/Flow Control
13) **IEEE 802.3ad:** Link Aggregation Control Protocol (LACP)

b.3) Seguridad y electromagnética

Se rige de acuerdo a los siguientes estándares:

1) FCC Part 15, UL 60950
2) IC Part 15, CSA 22.2 N0-950, RSS-139-1 and RSS-210
3) ETS 300-328 (2.4 GHz) and 301-893 (5 GHz), EN 301-489-17
4) R&TTE Directive 1999/5/EC
5) TELEC, ARIB T66
6) GBT-15941-1995, GBT-16841-1997

7) LP0002

3.4.2 XRE200

El XRE200 External Routing Engine es un servidor del tipo appliance que trabaja con el Internal Routing Engine externalizando la funcionalidad del plano de control y separando a este del plano de datos en el actual switch fabric. El XRE200 es una solución de diseño altamente confiable que incluye no solo un único punto de falla, como resultado se obtiene una solución escalable que proporciona un procesamiento adicional requerido para administrar un Virtual Chassis basado en la línea de switches EX8208, la Figura 3.11 muestra el XRE200.

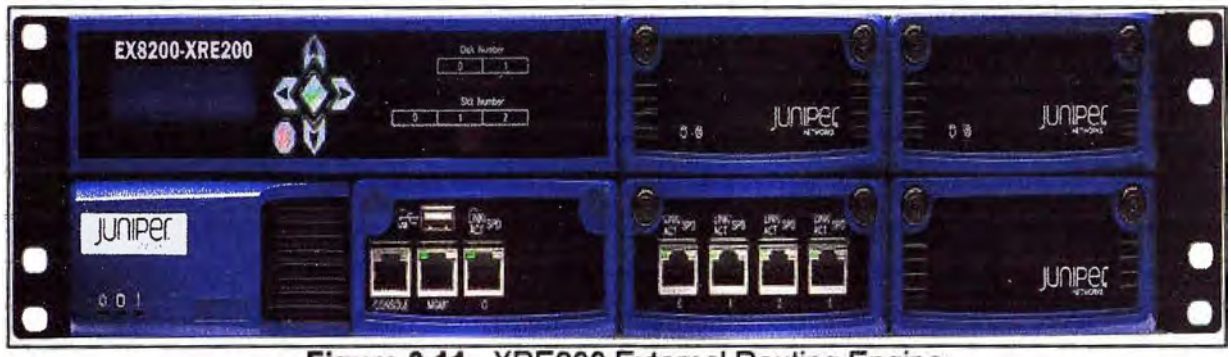

Figura 3.11 XRE200 External Routing Engine

a) Características y beneficios

Además de la escalabilidad del plano de control que provee el XRE200, el XRE200 provee la funcionalidad que si uno o mas switches en la configuración de VC pierde conectividad a los chassis adyacentes, el acceso a los switches que pertenecen al Virtual Chassis de EX8200 no pierden la conectividad a la red.

b) Descripción del producto

El XRE200 es un dispositivo de dos unidades de rack, el cual incluye dos ranuras para los módulos de interfaces de 1GbE identificados como Virtual Chassis Control Interface (VCCI), en la parte frontal del panel el XRE200 incluye una pantalla LCD para reportar el estado del dispositivo o realizar una configuración al dispositivo a través de un menú de opciones, tiene una serie de puertos 10/100/1000Base-T RJ-45 que son de uso dedicado para la conexión de XRE-a-XRE o XRE-a-Virtual Chassis, un puerto consola para la administración del equipo, así como de un puerto USB para el almacenamiento de archivos y restauración del sistema operativo.

c) Layer 2 switching

1) GVRP
2) Physical port redundancy: redundant trunk group (RTG)*
3) STP/RSTP (802.1D-2004)
4) VSTP (Compatible with PVST+)

5) STP enable/disable per port
6) MSTP (802.1Q-2003)
7) Number of MST instances supported: 64
8) Link Layer Discovery Protocol (LLDP)*
9) RVI (Routed VLAN Interface)*

d) Caracteristicas de capa 3

1) Routing protocols: RIPv1/v2, OSPF v2, BGP, IS-IS
2) Static routing
3) Routing policy
4) Bidirectional Forwarding Detection
5) Layer 3 redundancy: VRRP
6) Layer 3 sub-interfaces
7) IP directed broadcast

3.4.3 STRM (Series Security Response Managers)

El STRM es una solución de administración de seguridad ideal para pequeñas, medianas y grandes empresas, esta solución de administración de seguridad de red puede ser implementada como un dedicado Qflow Colector para la colección de flujos de red.

El modelo STRM500 es la opción propuesta para la solución, el enfoque integrado de la serie STRM usado en conjunto con la colección de datos, análisis, correlación y capacidades de auditoría, permite a las organizaciones a rápida y fácilmente implementar una solución de administración corporativa que entrega las mejores prácticas como administración de mensajes de información, y administración de alertas que puedan anticipar al personal de IT de un posible problema en algún elemento de la red, la Figura 3.12 muestra el STRM500.

Figura 3.12 STRM500

a) Características físicas

i. 2 discos duros de 500 GBPS Raid 1.
ii. 8 Gb de memoria RAM.

iii. Fuente de energía redundante.

iv. Dos ventiladores redundantes del tipo hot swap.

v. Dos puertos de trafico 10/100/1000Base-T RJ-45.

vi. Un puerto de consola RJ-45.

vii. Espacio requerido de 2 unidades de rack.

b) Facilidades

1) 500 eventos por segundo.

2) 15,000 flujos por segundo.

3) Análisis de tráfico en capa 7.

4) Recolección de eventos y flujos.

5) Procesamiento de eventos, flujos,

6) Correlación.

7) Análisis.

8) Reportes.

9) Monitorización de eventos en tiempo real.

10) Data warehousing.

11) Gestión de comportamiento de ataques.

CAPÍTULO IV
ANÁLISIS DE COSTOS

En el presente capítulo se detallan los aspectos relacionados a los costos y al cronograma del sistema implementado.

4.1 Estimación de costos

En la estimación de costos se considera todo el equipamiento que involucra la solución propuesta, así como el costo que involucra contar con el soporte local y el de fabrica directamente, ya que por la envergadura del proyecto y lo que implica el tener un tiempo de respuesta mínimo ante posibles fallas posteriores al periodo de instalación, se requiere contar con un contrato directo al fabricante, el detalle de lo indicado en este punto es mostrado en la Tabla 4.1.

4.1.1 Elementos no considerados en la estructura de costos

No son considerados dentro de la estructura de costos lo descrito en los aspectos que se describen a continuación:

a. Costo de hospedaje y alimentación

El alcance del proyecto se limita a ser realizado dentro de los límites que involucran la provincia Lima, fuera de este límite no se contempla gasto alguno en lo que respecta a alimentación, y hospedaje, los cuales deberían ser cubiertos en el caso que se requiriesen por la entidad financiera.

b. Costo de la instalación, puesta en operación y soporte local

Es parte de la propuesta técnica económica que sólo es manejada por el departamento comercial de la entidad proveedora de la solución y que es considerada confidencial por la entidad bancaria.

c. El costo de capacitación del personal técnico

También es parte de la propuesta técnico económico, la cual será brindada a un grupo de 10 personas, cuyas personas serán designadas por la entidad financiera, de esta manera se pueda contribuir con la sostenibilidad de esta solución, ya que el post-soporte de primer nivel de la solución propuesta pueda ser personal de IT de la misma entidad financiera.

4.1.2 Elementos considerados en la estructura de costos

Las características de los elementos considerados en el presupuesto son mostradas

en la Tabla 4.1.

4.2 Cronograma de tareas

La Tabla 4.2 muestra el cronograma de tareas realizadas para la implementación del proyecto. El diagrama de Gantt correspondiente, dado su tamaño y detalle, es mostrado en el Anexo C "Diagrama de Gantt".

Tabla 4.1 Presupuesto

Cantidad	Numero de parte	Descripción	Precio unitario	Precio total
4	EX8208-REDUND-AC	Redundant EX8208 system bundle: 8-slot chassis with passive backplane and 1x fan tray, 2x routing engine with switch fabric, 1x switch fabric module, 6x 2000W AC PSUs with power cords, and all necessary blank panels.	$64,000	$256,000.00
4	EX-XRE200-AC	EX 8200 Virtual Chassis External Routing Engine 200 includes dual AC power supplies, dual fans, 2 160GB HDD and one 4 port 10/100/1000 BASE-T RJ-45 IO card.	$20,000	$80,000.00
4	EX-XRE200-AFL	XRE200 Advanced Feature License for EX8200.	$10,000	$40,000.00
4	EX8200-8XS	8-port 10GbE SFP+ line card; requires SFP+ optics sold separately.	$40,000	$160,000.00
16	EX-SFP-10GE-USR	SFP+ 10 Gigabit Ethernet Ultra Short Reach Optics, 850 nm for 10m on OM1, 20m on OM2, 100m on OM3 multi-mode fiber.	$750	$12,000.00
4	EX8200-48T	48-port 10/100/1000BASE-T RJ-45 line card.	$24,000	$96,000.00
4	EX8200-48F	48-port 100FX/1000BASE-X SFP line card; requires SFP optics sold separately.	$32,000	$128,000.00
64	EX-SFP-1GE-SX	Small Form Factor Pluggable 1000Base-SX Gigabit Ethernet Optics.	$500	$32,000.00
4	SVC-SD-EX8208	Juniper Care SameDay Support for EX8208 Chassis (includes PS, RE, SFB).	$5,930	$23,720.00
4	SVC-SD-EX-XRE200	Juniper Care SameDay Support for EX-XRE200.	$2,750	$11,000.00
1	STRM500-ADD-250E-7500F	STRM in a All in One architecture. Threat Management License to Add EPS=250, Flows=7.5K Qflows/SFlows (15K J/NetFlows); Devices=250.	$10,450	$10,450.00
1	JA-STRM500-A2-BSE	STRM 500 Base HW Appliance Series II Only.	$7,000	$7,000.00
			COSTO TOTAL:	$856,170.00

Tabla 4.2 Cronograma de tareas

Nombre de Tarea	Tiempo	Comienza	Fin
Proyecto Backbone en entidad financiera.	46 días	01/10/2010 9:00	17/11/2010 18:00
Planificación del proyecto.	3 días	28/09/2010 9:00	30/09/2010 18:00
Designación de responsables	0.25 días	03/10/2010 9:00	03/10/2010 11:00
Recopilación de información de la infraestructura actual.	5 días	03/10/2010 9:00	07/10/2010 18:00
Entrega de equipamiento.	2 días	10/10/2010 9:00	11/10/2010 18:00
Instalación y configuración de los switches de Core EX8208 en sede principal.	4 días	12/10/2010 9:00	15/10/2010 18:00
Instalación y configuración de XRE's en sede principal.	1 día	16/10/2010 9:00	16/10/2010 18:00
Pruebas de funcionalidad de los EX8208 en sede principal.	2 días	17/10/2010 9:00	18/10/2010 18:00
Instalación y configuración de los switches de Core EX8208 en sede de contingencia.	4 días	19/10/2010 9:00	22/10/2010 18:00
Instalación y configuración de XRE's en sede de contingencia.	1 día	23/10/2010 9:00	23/10/2010 18:00
Pruebas de funcionalidad de los EX8208 en sede de contingencia.	2 días	24/10/2010 9:00	25/10/2010 18:00
Interconexión entre la sede principal y la redundante.	1 día	26/10/2010 9:00	26/11/2010 18:00
Integración entre los EX8208 y la infraestructura actual.	0.5 días	27/11/2010 9:00	27/11/2010 18:00
Migración física de los enlaces provenientes de las salas de comunicaciones, al nuevo Core en la sede principal.	5 días	28/11/2010 9:00	01/11/2010 18:00
Migración lógica de la plataforma de la entidad financiera.	2 días	02/11/2010 9:00	03/11/2010 18:00
Monitoreo de la solución instalada.	5 días	04/11/2010 9:00	08/11/2010 18:00
Preparación del informe de la solución instalada.	2 días	09/11/2010 9:00	10/11/2010 18:00
Presentación de la solución instalada.	1 día	11/11/2010 9:00	11/11/2010 18:00

En el cuadro anterior en el punto de entrega de equipamiento, no se está considerando el tiempo que demora la importación del equipamiento, más si, solo el tiempo de entrega local de los almacenes del proveedor local a los almacenes de la entidad financiera.

ANALISIS Y PRESENTACION DE RESULTADOS

1. La figura B.2 del Anexo B muestra la topología final actualmente en operación, en el presente los switches de Core de marca Nortel se vienen utilizando para proveer de conectividad redundante a los servidores de la entidad financiera.

2. El siguiente cuadro describe el protocolo de pruebas expuesto al personal de IT días previos a la puesta en producción de la nueva red de Backbone.

Tabla 4.3 Protocolo de pruebas

SWITCH DE CORE			
Nro	**VERIFICACION**	**PROCEDIMIENTO**	**RESULTADO**
1	Verificación de CPUs y fuentes redundantes.	Identificación de los CPUs y fuentes de energía redundantes.	correcto
2	Operatividad de fuentes redundantes.	Se procedió al apagado de una fuente de energía, y el switch se mantuvo operativo, de este modo se confirmo la operatividad de la redundancia de las fuentes de energía.	correcto
3	Operatividad de CPU's redundantes.	Se procedió al retiro de un CPU, y el switch se mantuvo operativo, de este modo se confirmo la operatividad de la redundancia de los CPUs.	correcto
4	Operatividad de XRE200 redundantes.	Se procedió al apagado del XRE200 principal, no percibiendo perdida de comunicación de comunicación alguna en la red.	correcto
5	Operatividad de XRE200 redundantes.	Se procedió al apagado del XRE200 en standby, no percibiendo perdida de comunicación de comunicación alguna en la red.	correcto
6	Verificación de los enlaces físicos al XRE200.	Se encuentran activos todos los enlaces redundantes de los switches de Core a los XRE200 redundantes.	correcto
7	Operatividad de los enlaces redundantes entre los switches y los XRE200.	Se desconecto uno de los enlaces físicos que interconecta el switch de Core y el XRE200, no percibiendo problema alguno en la red, este mismo procedimiento se realizo con el resto de conexiones redundantes entre los switches de Core y los XRE redundantes.	correcto
8	Operatividad de los enlaces entre switches de Core.	Se desconecto uno de los enlaces de fibra óptica que interconecta los switches de Core, no percibiendo problema alguno en la red, este mismo procedimiento se realizo con el resto de conexiones redundantes entre los switches de Core de la oficina principal y redundante.	correcto

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El Backbone para la plataforma de red de datos implementada en la entidad financiera ha demostrado desde el inicio de su operatividad un alto desempeño y alta disponibilidad brindando los niveles de accesibilidad y continuidad de las aplicaciones corporativas para los empleados y usuarios foráneos.
2. Durante las pruebas de contingencia realizadas antes y durante la implementación de la solución se forzó la falla de uno de los switches de Core perteneciente al Virtual Chassis de la oficina principal, la respuesta del switch restante ha sido sumamente eficiente y rápida, no habiéndose generado falla alguna en las comunicaciones de los usuarios.
3. El uso de una tecnología que provea de una alta disponibilidad en una configuración activo/activo dentro de un Virtual Chassis como tecnología propietaria del fabricante Juniper Networks, ayuda a simplificar la complejidad de gestión y configuración de la solución por el personal de IT, evitando el uso de protocolos de enrutamiento, o protocolos de alta disponibilidad.
4. La solución de red implementada en el Data Center ofrece la más completa solución; hoy en día el acceso a servidores de red en el mercado a una velocidad de 10Gbps, es ideal para organizaciones que vienen tratando de optimizar la conectividad Ethernet a través de cluster de plataformas virtualizadas y aplicaciones distribuidas.
5. Con la solución instalada se logró un servicio clave requerido por el personal de IT de la entidad financiera, el cual es la administración y monitoreo centralizado de los diferentes elementos de red como switches, firewall's, y demás dispositivos, reduciendo el tiempo y los gastos requeridos para configurar y administrar los dispositivos de red. Adicionalmente, el tráfico de red puede ser fácilmente analizado con este sistema, optimizando el rendimiento de la red.
6. El uso de la tecnología de virtualización (Virtual Chassis) facilita el incremento del ancho de banda de disponible entre ambas sedes, de los 40Gbps hasta un total de 80Gbps sin necesidad de interrupción en el servicio brindado a la red.
7. La adopción de comunicaciones unificadas que incluyen voz, video, y servicio de

datos, va en aumento. Según las estadísticas la mayoría de organizaciones corporativas tienen instalados sistemas de telefonía IP local y remota. Soluciones como estas tienen un impacto directo en los requerimientos de alto rendimiento y alta disponibilidad de una solución de Core para una red de área local, la solución implementada desde los inicios de su diseño ha sido pensada para poder soportar el trafico corporativo y no corporativo de la entidad financiera, así como de cualquier otro tipo de trafico que pueda originarse como un nuevo requerimiento de alguna aplicación que se adquiera en un futuro.

8. Se realizó un análisis de los diferentes tipos de equipos existentes en el mercado y se procedió a la elección de la mejor alternativa tomando en cuenta aspectos técnicos y económicos, teniendo como premisa la solicitud de la entidad financiera, el cual es contar con una solución con un desempeño del 99,999% en disponibilidad y totalmente redundante.

9. Finalmente se concluye que el presente proyecto se perfila como una solución que se ajusta perfectamente a la realidad de nuestro medio, brindando soluciones con costos de inversión admisibles, satisfaciendo a los usuarios y permitiéndose a la entidad financiera en la medida de lo posible, ir a la par de los desafíos que representan los nuevos y sofisticados servicios de transporte de información.

Recomendaciones

1. Que el personal IT de la entidad financiera realice periódicamente (cada seis meses) pruebas de alto desempeño a efectos de determinar aquellos elementos que puedan estar causando un bajo rendimiento en la plataforma instalada.

2. Que el personal de soporte IT se mantenga capacitado y entrenado para las labores de soporte y reparación de eventualidades en la plataforma de acceso inalámbrico de alta disponibilidad.

3. Para los usuarios que necesiten instalar software se deben establecer políticas para definir los tipos de software permitidos, y las reglas que deben cumplir en cuanto a licencias. Además se debe planificar un intervalo de tiempo para la realización del mantenimiento del software de las estaciones de trabajo, con el fin de mantener los equipos libres de virus y espías informáticos (cada seis meses).

4. Es recomendable que el personal IT capacite periódicamente al personal de la entidad bancaria en cuanto a las políticas de seguridad por cuanto no es parte de la solución desarrollada (cada seis meses).

5. La administración de la red es la suma de todas las actividades de planeación y control, enfocada a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, y seguridad, por lo que se debe contar con

un buen sistema de administración, ya que esto ayudará a mantener la operatividad de los recursos y el buen estado de los mismos.

6. Se recomienda evaluar la actualización de software de los diferentes equipos que conforman la solución, con el fin de poder evitar posibles inconvenientes que originen una disminución en el desempeño de la solución.

7. Para este diseño se ha seleccionado los equipos del fabricante Juniper Networks, ya que por sus características técnicas, rendimiento y garantías expuestas, están dentro de las necesidades y objetivos de la red, solicitadas por la entidad financiera.

8. En la entidad financiera, los datos con los que se trabajan son confidenciales, por lo cual las aplicaciones de uso corporativo usan sistemas de autenticación y encriptación de información, que exigen un alto rendimiento de la red, siendo este punto la base del diseño de la solución, se recomienda hacer mediciones de ancho de banda en los enlaces troncales con el fin de tener un estado actualización de consumo de ancho de banda.

9. Es importante que existan equipos de protección contra sobrecargas y picos de tensión, como es el UPS, que además de brindar protección sirve como fuente de poder cuando existe algún corte de energía eléctrica, proveyendo durante algunos minutos energía para los elementos constitutivos de la red.

ANEXO A
EVENTOS DE LA RED

ITEM	FECHA	DESCRIPCION DE EVENTO
1	07/01/2009	Se detecto lentitud en la red originado por una infección de virus en el servidor de monitoreo, el cual enviaba un nivel muy alto de paquetes broadcast a toda la red, teniendo como resultado caída de toda la red.
2	12/01/2009	Caída del SMLT 5 PP8600 Master (4/5) y PP8600 Backup(4/5) donde está conectado el switch 425-48T para servidores 130.30.1.128, originando la caida del resto de SMLTs.
3	16/01/2009	Caída del SMLT 12 PP8600 Master (4/10) y PP8600 Backup(4/10) donde está conectado el switch 325-24T ubicado en el piso 10, originando la caida del resto de SMLTs.
4	13/02/2009	Problema en la transición de VRRPs entre los switches de Core, el cual fue originado por la alta transferencia de trafico de tipo Multicast entre servidores, originando una lentitud en la red.
5	26/02/2009	Caída del SMLT 7 PP8600 Master (4/3) y PP8600 Backup(4/2) donde está conectado el ERS2526T ubicado en el piso 8, originando la caída del resto de SMLTs.
6	05/03/2009	Se percibió lentitud en la red durante las 8:30am a 11:00am.
7	17/03/2009	Caída del SMLT 3 Puertos PP8600 Master (4/15) y PP8600 Backup(4/18) donde está conectado el switch ERS5520 ubicado en la sala de comunicaciones del piso 6, originando la caída del resto de SMLTs.

Figura A.1 Eventos de la red de nivel crítico.

ANEXO B
DIAGRAMAS DEL SISTEMA

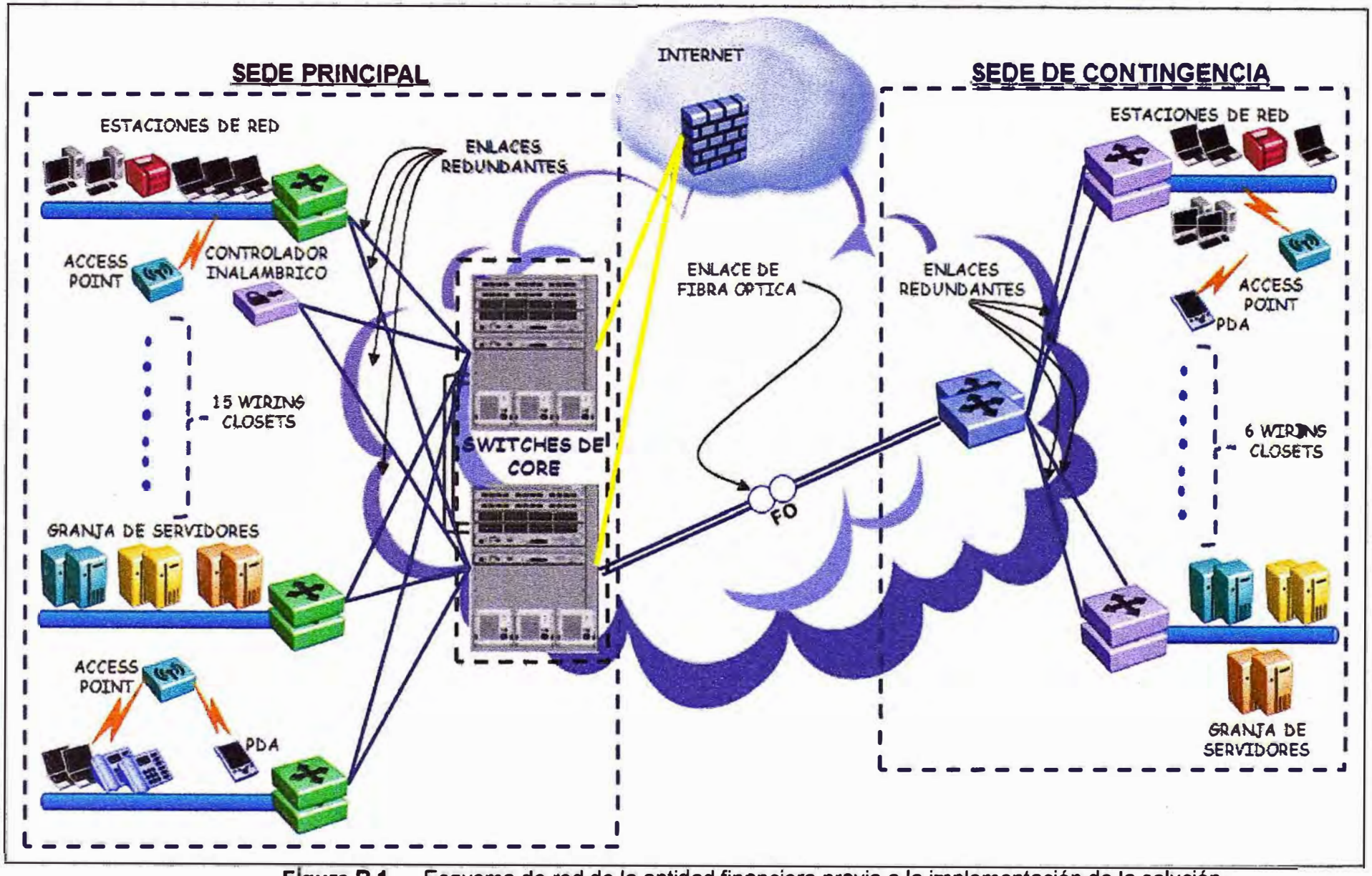

Figura B.1 Esquema de red de la entidad financiera previa a la implementación de la solución.

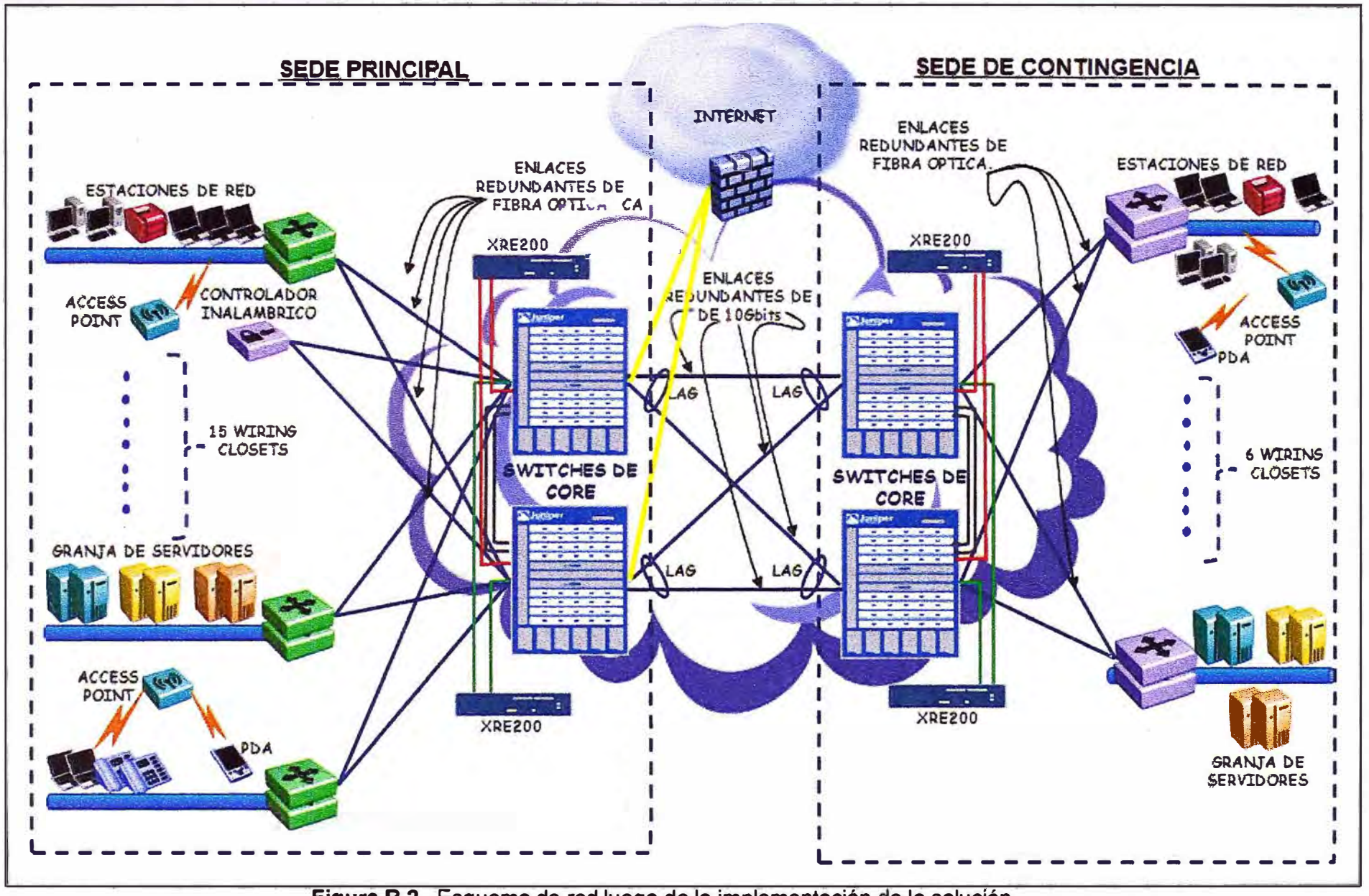

Figura B.2 Esquema de red luego de la implementación de la solución.

ANEXO C
DIAGRAMA DE GANTT

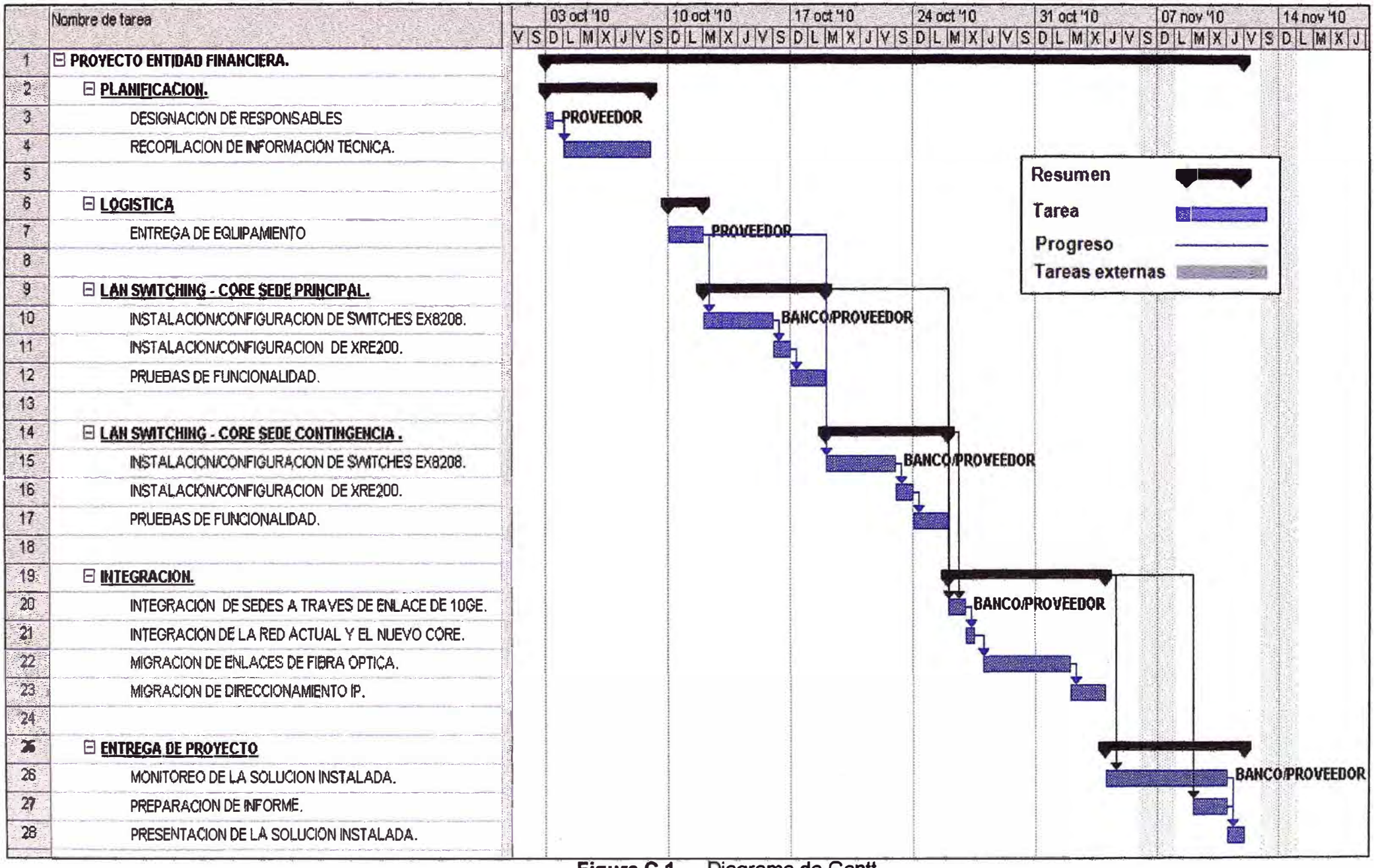

Figura C.1 Diagrama de Gantt

ANEXO D
GLOSARIO DE TÉRMINOS

ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
CLI	Interfaz de línea de comandos
CORE	Conjunto de componentes de conforman la red central
CPU	Central Processing Unit
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
EX	Enterprise switching
HA	High Availability
HUB	Concentrador
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ISO	International Organizational for Standardization
ISP	Internet Service Provider
JUNOS	Juniper Operating System
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAG	Link Aggregation Group
LAN	Local Area Network
MAN	Metropolitan Area Network
MIB	Management Information Database.
NIC	Network Interface Card
NMS	Sistema de administración de red.
NSR	Nonstop Active Routing
NSSU	Nonstop Software Upgrade
PDU	Packet Data Unit
PFE	Packet Forwarding Engine
PIM	Physical Interface Module VRRP
POE	Power over Ethernet
RE	Routing Engine
RFC	Request for Comments

SCP	Secure Copy
SF	Switch Fabric
SFP	Small Form-Factor Pugglable
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SRE	Switch Fabric and Routing Engine
STP	Spanning Tree Protocol
STRM	Series Security Response Managers
TCP/IP	Transmission Control Protocol/ Internet Protocol
TELNET	Telecommunication Network
IT	Information Technology
UIT	Unión Internacional de Telecomunicaciones
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VC	Virtual Chassis
VCB	Virtual Chassis Backplane
VCCI	Virtual Chassis Connector Interface
VCEP	Virtual Chassis Extender Port
VCP	Virtual Chassis Port
VLAN	Redes virtuales de área local
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
XRE	External Routing Engine

BIBLIOGRAFÍA

[1] Junos OS for EX Series Ethernet Switches, Release 11.2: EX8200 Virtual Chassis, http://www.juniper.net/techpubs/en_US/junos11.2/information-products/topic-collections/ex-series/software-all/book-software-ex8200-series-virtual-chassis.pdf

[2] EX8200 Ethernet Switches – Modular Ethernet Solutions – Juniper Networks
http://www.juniper.net/us/en/products-services/switching/ex-series/ex8200/

[3] Understanding Link Aggregation into an EX8200 Virtual Chassis - Technical Documentation - Support
http://www.juniper.net/techpubs/en_US/junos11.1/topics/concept/virtual-chassis-ex8200-lag-into.html

[4] IEEE P802.3ad Link Aggregation Task Force
http://www.ieee802.org/3/ad/public/index.html

[5] Junos Security: A Guide to Junos for the SRX Services Gateways & Security Certification "Junos Security Orelly".

[6] Junos High Availability: Best Practices for High Network Uptime "Junos High Availability".

[7] Junos Enterprise Switching: A Practical Guide to Junos Switches and Certification "Junos Enterprise Switching".

[8] Junos Enterprise Routing 2nd Edition "Junos Enterprise Routind"

[9] Richard Stevents. Addison- Wesley, "TCP/IP Ilustrated", volumen 1.

[10] Cisco, "Programa de certificacion CCNA" ver 4.0, 2007.

[10] Data Center LAN Migration Guide
http://www.juniper.net/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/design-guides/7100128-en.pdf

[11] Data Center LAN Connectivity Design Guide
http://www.juniper.net/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/design-guides/8020010-en.pdf

[12] Campus LAN Design Guide
http://www.juniper.net/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/design-guides/8020001-en.pdf

[13] Cloud-Ready Data Center Reference Architecture
http://www.juniper.net/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/reference-architectures/8030001-en.pdf

[14] Datasheets EX8208 Ethernet Switch
http://www.juniper.net/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/datasheets/1000261-en.pdf