UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ALTA DISPONIBILIDAD Y MEJORA
DE LA SEGURIDAD DEL CENTRO DE SERVICIOS
DE UN PROVEEDOR DE SERVICIO DE INTERNET

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ÁLVARO ENRIQUE PÉREZ UNZUETA

PROMOCIÓN
2008-I

LIMA-PERÚ
2011

ALTA DISPONIBILIDAD Y MEJORA DE LA SEGURIDAD DEL CENTRO DE SERVICIOS DE UN PROVEEDOR DE SERVICIO DE INTERNET

A mis padres, Magda y Enrique
por su cariño y dedicación
en todos estos años

SUMARIO

El presente informe describe el diseño e implementación de la alta disponibilidad y mejora de la seguridad del centro de servicios de un proveedor de servicio de Internet, mediante la reestructuración de la topología, con la finalidad de hacerla más robusta.

Esta solución de ingeniería de redes era necesaria debido a que la infraestructura presentaba un único punto de falla a nivel de enlace, y carecía por completo de redundancia a nivel de balanceadores DNS (servidores de resolución de nombres) y Firewall; adicionalmente los usuarios y atributos eran almacenados localmente (en dispositivos de red), todo ello la hacía más insegura e ineficiente.

La solución se enfoca en el servicio DNS, procurando un desempeño óptimo a través de estrategias de redundancia a nivel de enlaces, firewall, balanceadores de carga, granjas de servidores, y mediante la incorporación de un servidor de control de acceso, también en alta disponibilidad.

En el informe se presenta el análisis de la situación inicial evaluando sus vulnerabilidades para luego proponer diversas configuraciones de mejora de la topología. Luego de ello se presenta la infraestructura y topología de la solución en detalle, describiendo su funcionalidad y configuración para el modo normal así como para el modo de contingencia.

El informe se complementa con la descripción del equipamiento, la estructura de costos y de tiempo, así como con las pruebas realizadas.

ÍNDICE

INTRODUCCIÓN

El objetivo del trabajo descrito en el presente informe es hacer más robusta la infraestructura y los servicios de red del Proveedor de Servicios (ISP) mediante la implementación de alta disponibilidad y mejora de la seguridad en los Centros de Servicio y Core IP (red de transporte). Se busca así que la red se mantenga óptimamente funcional ante la falla de algunos dispositivos o la falla de los enlaces, del mismo modo, se trata de eliminar las vulnerabilidades a nivel de seguridad de acceso y tráfico de datos.

La solución se enfoca en el servicio de los servidores de resolución de nombres (DNS) encargados de proporcionar al usuario una dirección IP adonde realizar la petición de información de determinada web la cual es escrita en formato de texto (por ejemplo http://www.orce.uni.edu.pe = 208.70.188.28).

La solución se logra a través de estrategias de redundancia a nivel de enlaces (agregación de enlaces), firewall (cortafuegos), balanceadores de carga (para el reparto de las solicitudes), granjas de servidores (conteniendo la base de datos), y mediante la incorporación de un servidor de control de acceso (para mejora de la seguridad).

La solución se realiza para las dos sedes del proveedor de servicios, una de ellas en Lima y la otra en San Isidro. Cada una de ellas se enlaza a la nube Internet a través de un router Cisco 7206 en donde se implementa el protocolo HSRP (se explica en el marco teórico), un switch Catalyst 6513 en donde se actualiza el firewall, un switch Catalyst 6509 en donde se mejora el balanceador de carga y se incorpora el servidor de control de acceso (todo en alta disponibilidad). A esto se añade la redundancia de los enlaces entre switches del mismo tipo, así como entre los switches de la misma sede.

El desarrollo del proyecto de ingeniería se basa principalmente en la documentación técnica del equipamiento utilizado, proveniente de Cisco System Inc. También se ha consultado diversa bibliografía en los temas de seguridad de redes. El informe de ingeniería fue realizado gracias a la experiencia adquirida durante tres años en proyectos similares de ingeniería de telemática.

El informe se divide en cuatro capítulos:

- Planteamiento de ingeniería del problema.- Se describe el problema y los objetivos, se explica la justificación de la solución, se determina el alcance del proyecto y finalmente se hace una síntesis del informe.
- Marco teórico.- En él se exponen las bases teóricas conceptuales relacionadas con la

solución. En este capítulo se desarrollan los siguientes temas: Servidores de resolución de nombres (DNS), protocolos y características relacionadas con la alta disponibilidad, seguridad informática, cálculos de disponibilidad.

- Metodología para la solución del problema.- Este capítulo describe la ingeniería del proyecto de reestructuración de la topología del Centro de Servicios del ISP. Primeramente se realiza el análisis preliminar para determinar la solución a implementar, posteriormente se explica la solución implementada y finalmente, se hace una descripción técnica del equipamiento utilizado.

- Análisis y presentación de resultados.- En él se presenta la estructura de costos del proyecto, el cronograma de trabajos así cómo las pruebas realizadas.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema. Se describe el problema y se expone el objetivo del trabajo. Se hace una evaluación del problema y se precisan los alcances del informe; para concluir, se presenta una síntesis de la solución.

1.1 Descripción del Problema

Deficiente disponibilidad y seguridad del centro de servicios de un proveedor de servicio de Internet.

La infraestructura presentaba un único punto de falla a nivel de enlace, y carecía por completo de redundancia a nivel de balanceadores DNS y Firewall; los usuarios y atributos eran almacenados localmente (dispositivos de red).

1.2 Objetivos del trabajo

Hacer más robusta la infraestructura y los servicios de red del Proveedor de Servicios (ISP) mediante la implementación de alta disponibilidad y mejora de la seguridad en los Centros de Servicio y Core IP.

Esto es logrado mediante la reestructuración de la topología, para lo cual se reemplaza, incorpora, actualiza y/o reconfigura los dispositivos de comunicaciones, equipos de balanceo de aplicaciones, equipos firewall (corta fuegos), servidores de control de acceso y granjas de servidores DNS.

1.3 Evaluación del problema

El colapso de las comunicaciones sufrido durante el terremoto de 2007, puso en evidencia la deficiencia de los centros de servicio de los proveedores de Internet, los cuales, ante la saturación de servicios, los usuarios finales (domésticos y empresariales) veían afectado su capacidad de navegar en la Internet.

Uno de los principales factores correspondía a los servidores DNS. El DNS (Servidor de Resolución de Nombres) es una base de datos distribuida y jerárquica, la cual almacena información que asocia los nombres de dominio en redes como Internet con una dirección IP (p. ej. www.google.com → 74.125.229.115). Es claro que si el servidor DNS no existe o se encuentra saturado, los usuarios no podrán resolver a dónde dirigir su requerimiento de navegación.

Para el caso de estudio se disponía de una topología en donde los servicios de DNS

se manejaban a través de dos centros de servicio, uno situado en San Isidro y otro en Lima Cercado, interconectados mediante un enlace de fibra óptica. En esta topología la granja de servidores de cada sede se turnaban para brindar el servicio de DNS (200.48.225.130 y 200.48.225.146).

Cuando cualquier dispositivo de la infraestructura de red de uno de los DNS dejaba de dar servicio por cualquier motivo, se reestablecía manualmente el servicio afectado, configurando los dispositivos de ambos centros de servicios de forma que se comunican ante un único enlace de fibra óptica. Este único enlace era crítico y ponía en riesgo la disponibilidad del servicio de DNS.

El balanceo de carga de solicitudes de DNS se realizaba a través de una única granja, la cual, mediante el proceso llamado "round robin" (circular), distribuía la carga a cada uno de los servidores físicos. No se tenía respaldo para cada servidor de la granja, esto quiere decir que si uno de los servidores fallaba, entonces el proceso de balanceo se hacía deficiente, esto podía continuar hasta saturar el servicio, esto era crítico teniendo en cuenta que solamente un DNS estaba activo a la vez.

A nivel de Firewall el servicio era satisfactorio, sin embargo, si se estimaba una mejora proporcionando redundancia a diversos niveles en el centro de servicios, esta facilidad también debía ser mejorada.

Tener los atributos de seguridad de los usuarios almacenados en los dispositivos de red representaba un alto riesgo, por cuanto las estrategias para ingresar a una red restringida se basaban en el aprovechamiento de las vulnerabilidades de la red. El almacenamiento local hacía ineficiente la administración de los usuarios y por consecuencia también ponía en riesgo la seguridad, no se podía determinar quién había modificado una configuración ni por cuánto tiempo había permanecido activa.

Las deficiencias descritas líneas arriba, ponían en evidencia un mal servicio para el usuario, lo cual afectaba a la empresa proveedora, no sólo como imagen, sino también ante la posibilidad de ser multada por OSIPTEL.

Todos los argumentos expuestos en esta sección, sustentaban el robustecimiento de la infraestructura.

1.4 Alcance del trabajo

El informe desarrolla la solución de alta disponibilidad y mejora de la seguridad del centro de servicios de un proveedor de servicio de Internet en sus dos sedes de Lima.

La solución se enfoca en el servicio DNS, procurando un desempeño óptimo a través de estrategias de redundancia a nivel de enlaces, firewall, balanceadores de carga, granjas de servidores, y mediante la incorporación de un servidor de control de acceso, también en alta disponibilidad.

1.5 Síntesis del trabajo

En el informe se explica la metodología para cumplir con los requerimientos, el dimensionamiento del equipamiento y de las aplicaciones a ejecutar; se muestran y explican, tanto la topología previa como la topología implementada; además se describe de manera resumida los aspectos técnicos del nuevo equipamiento (Cuadro 1.1).

Se hace un análisis de costos del proyecto y un análisis de la gestión de tiempo (responsabilidades, trabajos, tareas realizadas, tiempos), mediante un diagrama de Gantt. También se describen las pruebas y resultados. El informe se complementa con los aspectos técnicos conceptuales de la solución implementada (Cuadro 1.2).

Análisis preliminar	Descripción situacional de la topología Centro de Servicios Alternativas de solución Comparación de alternativas Dimensionamiento de la solución propuesta
Infraestructura y topología de la solución	Descripción de la infraestructura Funcionamiento de la topología Configuración
Equipamiento	Router Cisco 7206VXR Switches Cisco familia Catalyst WS-C6500-E (6513 y 6509) Módulo de firewall FWSM (Firewall Service Module) Módulo de ACE (Application Control Engine Module) Servidor de control de acceso ACS1113

Cuadro 1.1 Cuadro sinóptico de la Metodología de Solución del Problema

Servidores de Resolución de nombres (DNS)	Generalidades Granjas de servidores Balanceo de carga
Protocolos y características relacionadas con la alta disponibilidad	Redes de Área Local Virtuales (VLAN) Troncales Protocolo de agregación de enlaces (LACP) Protocolo para redundancia de capa 3 (HSRP) Contextos Failover Protocolo de redundancia para balanceador de carga
Seguridad informática	Generalidades Tipos de ataque Las tres principales metas de seguridad de red Firewall (corta fuego) Administración de usuarios Inspección de protocolos de aplicación Listas de acceso
Disponibilidad	Disponibilidad individual Disponibilidad de sistema Disponibilidad y seguridad

Cuadro 1.2 Cuadro sinóptico del Marco Teórico

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen las bases teóricas conceptuales directamente relacionadas con la solución desarrollada en este informe de suficiencia. El capítulo consta de los siguientes tópicos: Servidores de Resolución de Nombres (DNS), protocolos y características relacionadas con la alta disponibilidad, seguridad informática, disponibilidad individual y de sistema.

2.1 Servidores de Resolución de Nombres (DNS)

DNS son las siglas de Domain Name System. En esta sección se desarrollan los aspectos generales del DNS, el concepto granja de servidores y finalmente, lo referente al balanceo de carga de tráfico de datos.

2.1.1 Generalidades

El DNS asigna nombre a equipos y servicios de red [1]. El DNS se estructura de manera jerárquica. La asignación de nombre se utiliza en redes TCP/IP, de manera que localiza dispositivos y servicios con nombres descriptivos (por ejemplo cuando un usuario final escribe www.google.com el DNS podrá traducir el nombre en una dirección IP). A continuación se presentan los principales componentes (Figura 2.1) para la operación práctica de un DNS.

- **Cliente DNS** Un cliente DNS es un proceso informático que se ejecuta en un ordenador o dispositivo de red y que genera peticiones respecto a un nombre específico en Internet a un servidor DNS para que resuelva el nombre pedido con una dirección IP correspondiente
- **Servidor DNS** Es un servidor que contiene una extensa base de datos y responden las peticiones de los clientes DNS.

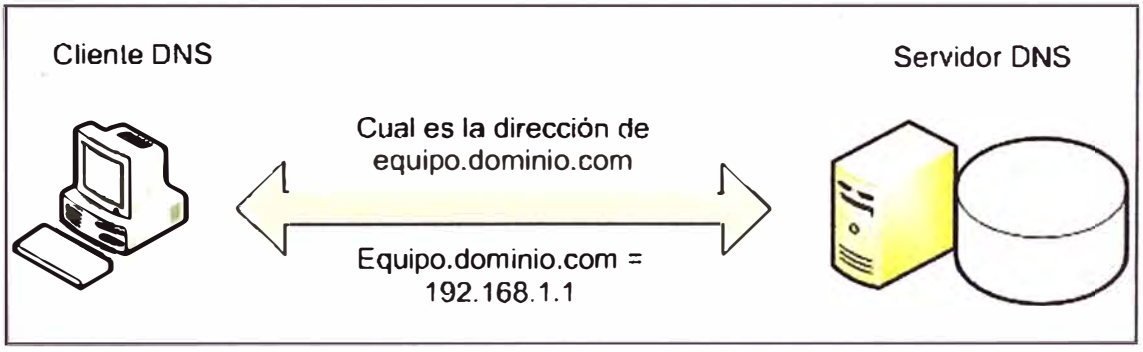

Figura 2.1 Componentes principales del DNS (Fuente: elaboración propia)

2.1.2 Granjas de servidores

Para definir este concepto, primeramente se debe conocer lo que son los servidores reales. Los servidores reales [2] son en sí servidores físicos de gran capacidad de procesamiento con amplia memoria y que ejecutan aplicaciones cliente/servidor, es decir, que deben atender de manera dedicada los requerimientos de los dispositivos de red que se lo solicitan; para el caso de estudio se habla de servidores DNS, como ya se explicó líneas arriba, sin embargo otras aplicaciones son el HTTP (Hypertext Transfer Protocol) y el FTP (File Transfer Protocol).

Las granjas de servidores son grupos de servidores reales que contienen el mismo contenido y típicamente residen en la misma ubicación física en un centro de datos. Los sitios web ofrecen a menudo grupos de servidores configurados en una granja de servidores. El software de balanceo de carga distribuye las peticiones de los clientes, contenido y servicios a los servidores reales.

La disponibilidad de un servidor en un sistema de balanceo de carga comprende varios factores, por ejemplo, si uno deja de funcionar, entonces otro puede tomar el lugar y continúa ofreciendo el mismo servicio y contenido a los clientes que envían peticiones.

2.1.3 Balanceo de carga

Es el proceso de decidir cuál servidor podría enviar una respuesta de un servicio a un cliente [2]. Por ejemplo, un cliente podría realizar una petición que consiste de un comando HTTP (HyperText Transport Protocol) para una página Web o FTP (File Transfer Protocol) para descargar un archivo. El trabajo del balanceador de carga es seleccionar el servidor que puede responder satisfactoriamente y en un tiempo corto sin sobrecargar ningún servidor como sea posible. Ver Figura 2.2

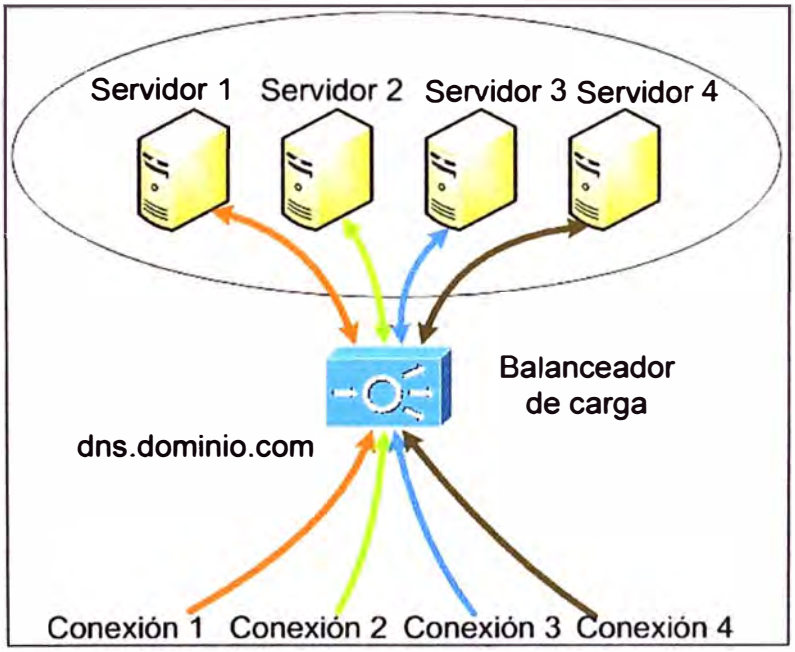

Figura 2.2 Granja de servidores y balanceo de carga (Fuente: Elaboración Propia)

2.2 Protocolos y características relacionadas con la alta disponibilidad

En esta sección se desarrollan los siguientes tópicos: LAN virtual (VLAN), troncales, protocolo de control de agregación de enlaces, protocolo para redundancia de capa 3, contextos, Failover, y protocolo de redundancia para balanceador de carga

2.2.1 Redes de Área Local Virtuales (VLAN)

Es una agrupación lógica de ordenadores y dispositivos de red. Las VLAN se agrupan por función o por ubicación física, sin importar la ubicación real de los usuarios finales [3].

El flujo de datos entre las VLAN está restringido. Los Switches envían tráfico de datos unicast, multicast y broadcast (a un solo punto, a un grupo determinado, y a todos, respectivamente) sólo en segmentos de red que pertenezcan a la misma VLAN a la que pertenece el tráfico de datos. En otras palabras, los dispositivos que pertenecen a una VLAN sólo se comunican con los dispositivos que pertenecen a la misma VLAN.

Las VLAN mejoran el rendimiento de la red agrupando a los dispositivos y recursos de forma lógica. Las empresas a menudo usan las VLAN como una forma de garantizar que un conjunto de dispositivos se agrupen lógicamente más allá de su ubicación física. Las VLAN permiten a los usuarios finales compartir la misma ubicación física, pero pertenecer a redes diferentes, a pesar de estar usando los mismos dispositivos de red (Figura 2.3).

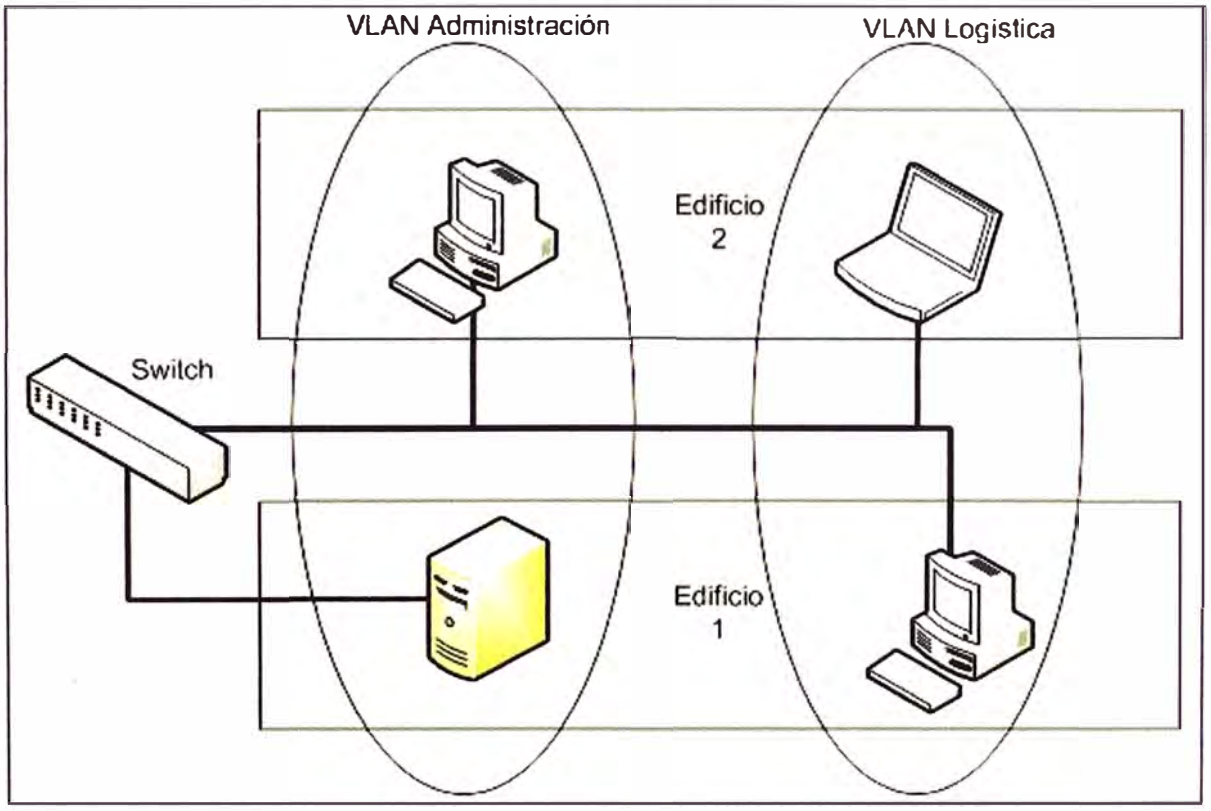

Figura 2.3 Ejemplo de VLAN (Fuente: Elaboración Propia)

Por ejemplo, los usuarios del departamento de Administración se ubican en la VLAN de Administración, mientras que los usuarios del Departamento de Logística se ubican en la VLAN de Logística, a pesar de que sus miembros se encuentren en pisos y hasta

edificios distintos. Las VLAN pueden mejorar la escalabilidad, seguridad y gestión de red.

2.2.2 Troncales

Una troncal es una conexión física que transporta enlaces lógicos [3]. En el contexto LAN, un enlace troncal es un enlace punto a punto entre dos Switches que soporta y transporta varias VLAN. El propósito de un enlace troncal es ahorrar puertos al crear un enlace entre dos Switches que implementan VLAN.

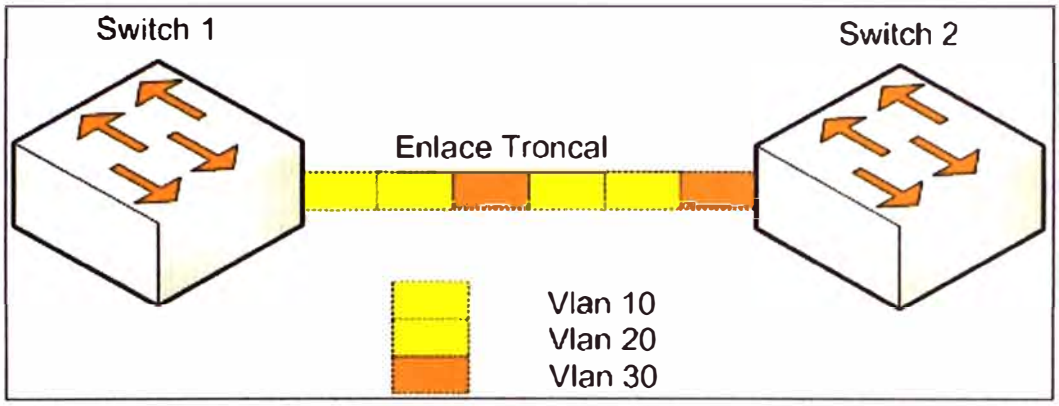

Figura 2.4 Troncal (Fuente: Elaboración propia)

2.2.3 Protocolo de agregación de enlaces (LACP)

Siglas de Link Aggregation Control Protocol, definido por el IEEE 802.3ad. Ofrece un método de agregación de múltiples enlaces Ethernet en un simple canal lógico (Figura 2.5). Esta propiedad ayuda a mejorar el costo efectivo de los dispositivos, incrementando el ancho de banda acumulativo sin requerir una actualización de dispositivos [4]. En adición, IEEE 802.3ad ofrece una capacidad de provisión dinámica, administración y monitoreo de varios enlaces de agregación y habilita la interoperabilidad entre dispositivos de diferentes marcas.

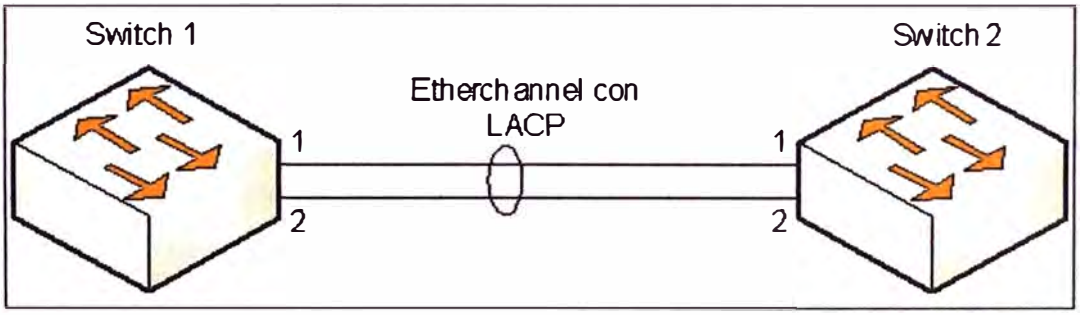

Figura 2.5 Enlace Etherchannel con LACP (Fuente: Elaboración propia.)

Gigabit Etherchannel es una tecnología Ethernet de alto desempeño (Cisco) que ofrece tasas de transmisión en Gigabit por segundo. Una agrupación Gigabit Etherchannel es un enlace lógico que ofrece ancho de banda agregado que llega hasta 8 enlaces físicos. Todos los puertos en cada Etherchannel deben tener la misma velocidad y deberán ser configurados como puertos Ethernet capa 2 o puertos capa 3.

Cuando un enlace perteneciente al Etherchannel falla, el tráfico previamente llevado

sobre el enlace que presentó falla es redistribuido en el Etherchannel, también cuando ocurre una falla, se envía un mensaje que identifica el dispositivo Etherchannel y el enlace que falló.

LACP soporta creación automática de Etherchannel intercambiando paquetes LACP entre los puertos LAN. Los paquetes LACP son intercambiados solamente entre puertos en modo pasivo y activo. El protocolo aprende la capacidad de agrupar dinámicamente puertos LAN e informar a los otros puertos LAN, después LACP identifica correctamente los enlaces Ethernet de cada extremo.

Ambos modos, pasivo y activo, permiten a LACP negociar entre puertos LAN y determinar si pueden formar un Etherchannel, basado en el criterio de velocidad de puertos y estado trunk (troncal).

Los puertos LAN pueden formar un Etherchannel cuando son compatibles con el modo LACP, según los siguientes ejemplos:

- Un puerto LAN en modo activo puede formar un Etherchannel con otro puerto LAN en modo activo.
- Un puerto LAN en modo activo puede formar un Etherchannel con otro puerto LAN en modo pasivo.
- Un puerto LAN en modo pasivo no puede formar un Etherchannel con otro puerto LAN que es también en modo pasivo porque ninguno inicia negociación.

La IEEE 802.3ad ofrece los siguientes beneficios:

- Incremento de la capacidad de la red sin cambiar físicamente las conexiones o actualizando los dispositivos de red.
- Ahorro de costos, resulta del uso de dispositivos existentes y funcionalidades adicionales de software.
- Es una solución estándar que habilita la interoperabilidad de los dispositivos de red.
- Puertos de redundancia sin intervención de usuarios cuando los puertos fallan.

2.2.4 Protocolo para redundancia de capa 3 (HSRP)

De sus siglas Hot Standby Routing Protocol; es un protocolo propietario de Cisco desarrollado para permitir varios routers (o Switches multicapa) que representan una simple dirección IP. Básicamente, cada uno de los routers que ofrecen redundancia es configurado en un grupo HSRP. Un router es elegido como primario, o router activo; el otro es elegido como router espera. Los routers intercambian mensajes "hola" HSRP en intervalos regulares de tiempo [5].

Un grupo HSRP puede ser asignado arbitrariamente, desde el 0 al 255. HSRP elige el router activo en base a un valor de prioridad (0 a 255) que es configurado en cada router en el grupo. Por defecto, la prioridad es 100. El router con mayor valor de prioridad (255

es el más alto) se convierte en el router activo del grupo; si todos los routers poseen la misma prioridad o está configurado por defecto, entonces el router que tiene mayor dirección IP en la interfaz que participa en el grupo HSRP se vuelve router activo. Ver Figura 2.6.

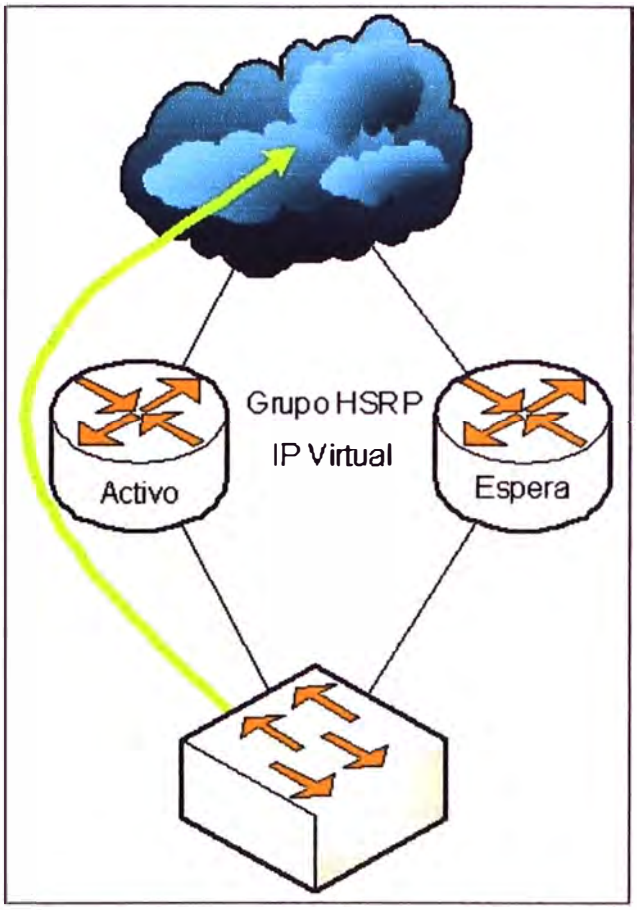

Figura 2.6 Router activo y de espera enrutando tráfico a nube WAN (Fuente: Elab. Prop.)

Solamente el router en espera monitorea al router activo con mensajes "hola". Por defecto, los mensajes "hola" son enviados cada 3 segundos. Si los mensajes "hola" se pierden durante el tiempo de espera (por defecto 10 segundos, o 3 veces el tiempo de envío del mensaje "hola"), el router activo es supuesto como caído. El router en espera entonces asume el rol de activo.

Normalmente, después que el router activo falla y el router espera se vuelve activo, el router original activo no puede inmediatamente volverse activo cuando es restaurado. En otras palabras, si un router todavía no está activo, no puede volverse activo nuevamente hasta que el router activo actual falle, aun si su prioridad sea más alta que la del router activo actual. Se puede configurar un router para que retorne o inmediatamente tome el rol de activo si su prioridad es la más alta.

2.2.5 Contextos

Un dispositivo se puede dividir en múltiples dispositivos virtuales, conocidos como contextos. Cada contexto tiene sus propias políticas, interfaces, y administradores. Los

contextos son similares a tener múltiples dispositivos independientes. Muchas características de los dispositivos físicos son soportadas en el modo contexto múltiple, incluyendo tablas de enrutamiento, políticas, propiedades, y administración. Algunas propiedades no son soportadas.

El administrador del sistema agrega y administra los contextos a través de un único contexto denominado contexto admin, en este contexto se configura y agrega cada contexto, asignando interfaces, y recursos a estos. El contexto admin es como cualquier contexto, excepto cuando un usuario ingresa, entonces se puede decir que es el administrador del sistema y puede acceder a otros contextos. El contexto admin no se restringe de ninguna manera y puede ser usado como un contexto regular, sin embargo, el contexto admin garantiza los privilegios sobre todos los otros contextos.

2.2.6 Failover

Es la capacidad de conmutar automáticamente a un dispositivo redundante o en espera. El failover se ejecuta sin intervención humana y generalmente sin peligro. Los sistemas de failover requieren continua disponibilidad y alta confiabilidad [7]. El failover toma lugar automáticamente usando un mensaje "pulso", este mensaje es enviado y recibido mediante el enlace que interconecta ambos dispositivos. Mientras el mensaje "pulso" continua entre el dispositivo principal y secundario, el dispositivo secundario no iniciará la conmutación. El dispositivo secundario iniciará la conmutación tan pronto como detecte una alteración en el sistema de alta disponibilidad.

Algunos sistemas de manera intencionada no realizan la conmutación automática, sino que requiere de la intervención humana. Esta conmutación se realiza con la aprobación del administrador del sistema ejecutándose automáticamente una vez que el administrador lo haya aprobado.

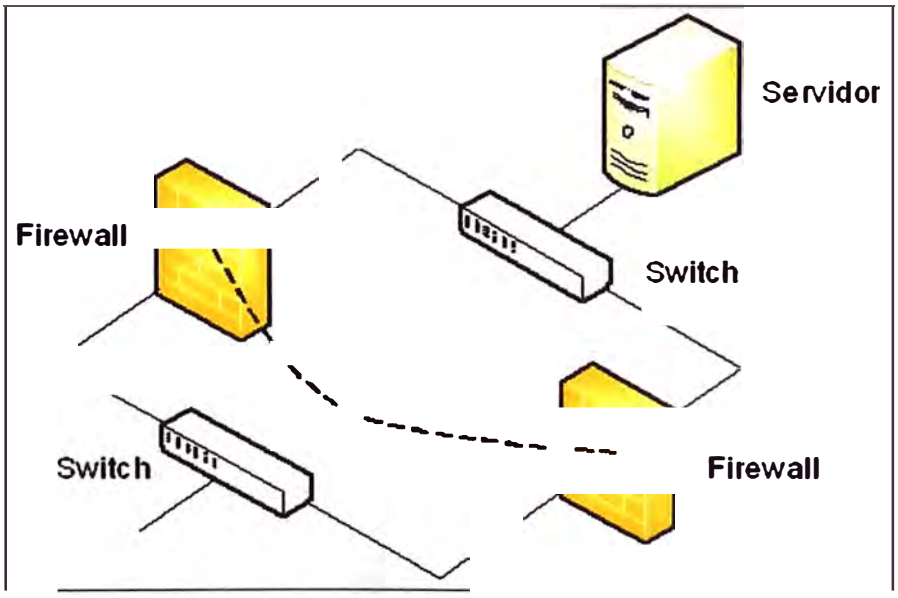

Figura 2.7 Ejemplo de Failover entre dos dispositivos Firewall (Fuente: Elab. prop.)

2.2.7 Protocolo de redundancia para balanceador de carga

El balanceador de carga ACE (Application Control Engine - Cisco) usa un protocolo propietario que habilita la configuración de redundancia de dos ACE. Se puede configurar como máximo dos ACE en un mismo Switch Cisco Catalyst 6500 o en dos diferentes chasis para redundancia. Cada módulo ACE puede contener uno o más grupos de tolerancia de falla (FT Group - Fault Tolerance Group). Cada FT group consiste en dos miembros: un contexto activo y el otro contexto en espera.

Una dirección MAC virtual (VMAC) es asociada con cada FT group. El formato de la VMAC es 00-0b-fc-fe-1b-groupID. Porque una VMAC no puede cambiar hasta que conmuten. El cliente y la tabla ARP (protocolo de resolución de direcciones) del servidor no requieren actualización. El ACE selecciona una VMAC desde un grupo de direcciones MAC virtuales disponibles. Se puede especificar el grupo de direcciones MAC que el ACE local y ACE en espera usa.

Cada FT group actúa como una instancia redundante independiente. Cuando ocurre la conmutación, el miembro activo del FT group se vuelve un miembro en espera y el miembro original en espera se vuelve miembro activo. Una conmutación puede ocurrir por las siguientes razones:

- Un miembro activo no responde
- Puede realizar la conmutación manualmente forzando que ocurra la conmutación.
- Un dispositivo, interfaz o grupo HSRP que falla.

2.3 Seguridad informática

Para la comprensión de la seguridad informática [9], la cual también es incluida en la solución desarrollada en este informe, esta sección se divide en los siguientes ítems: Generalidades, tipos de ataque, principales metas de seguridad de red, Firewall (corta fuego), administración de usuarios (AAA), inspección de protocolos de aplicación y finalmente listas de acceso (ACL).

2.3.1 Generalidades

A medida que las redes crecen y se interconectan con otras redes, incluido Internet, estas redes son expuestas a un gran número de riesgos de seguridad informática. No solamente el número de potenciales atacantes ha crecido a lo largo de toda la red, sino que además las herramientas disponibles de estos potenciales atacantes se vuelven más sofisticadas.

Una red siempre es un blanco. Nuevas vulnerabilidades y nuevos métodos de ataques son descubiertas, un usuario que no posea herramientas relativamente sofisticadas puede enviar un ataque contra una red no protegida. Los ataques de red involucran sofisticados y habilidosos métodos que evaden la detección; los ataques se

vuelven cada vez más específicos y tienen mayores consecuencias financieras para sus víctimas.

2.3.2 Tipos de ataque

Al conectarse a una red externa como Internet, se introduce la posibilidad que atacantes externos aprovechen las debilidades de la red, tal vez robando información o impactando el desempeño de la red, por ejemplo, introduciendo virus; sin embargo, aun si la red estuviera desconectada de la red externa, las amenazas de seguridad seguirán existiendo.

Específicamente, acorde al Computer Security Institute (CSI) en San Francisco, California, aproximadamente 60 al 80% de los incidentes de red son originados desde la misma red, por consiguiente, aunque el aislamiento de la red no es factible para negocios que tienen ambientes informáticos (negocios electrónicos), incluso el aislamiento físico de la red no garantiza la seguridad de la red.

Basados en estos factores, los administradores de red deben considerar ambas amenazas: internas y externas.

a. Amenazas internas

Son aquellas amenazas que son originadas dentro de la red, estas amenazas tienden a ser más serias que las amenazas externas. A continuación se exponen algunas razones de la severidad de amenazas internas:

- Los usuarios internos ya conocen la red y sus recursos disponibles.
- Los usuarios internos típicamente tienen algunos niveles de acceso por la naturaleza de su trabajo.
- Los mecanismos de seguridad de red, tales como sistemas de prevención de intruso (IPS) y firewall (corta fuegos), no son efectivos contra muchos problemas de red originados internamente.

b. Amenazas Externas

Los atacantes externos probablemente no tengan conocimiento de la red, y esto es lógico porque no tienen las credenciales de acceso, sus ataques tienden a ser de naturaleza técnica.

Por ejemplo, un atacante podría realizar un barrido de comando ping en una red e identificar la dirección IP que responde a la serie de pings. Entonces, las direcciones IP podrían ser sujetas a una revisión de puertos TCP/IP de los servicios que estén abiertos de los dispositivos descubiertos.

Si el atacante gana control del dispositivo, él podría usar ese punto como un trampolín para atacar toda la red. Afortunadamente, los administradores de red pueden mitigar muchas amenazas expuestas a atacantes externos.

2.3.3 Las tres principales metas de seguridad de red

La mayor parte de los días de una red corporativa, son en su mayoría referidas a los requerimientos y demandas del comercio electrónico y contacto con el cliente; estas dos requieren de conectividad interna entre la red externa (Internet) y red interna, desde el punto de vista de seguridad, hay dos supuestos básicos en las redes empresariales modernas [9], las cuales se exponen a continuación:

- Las redes corporativas de hoy en día son grandes, se interconectan con otras redes, y corren protocolos propietarios.
- Los dispositivos y aplicaciones se conectan y usan en redes corporativas que continuamente incrementan en complejidad.

La mayoría (si no son todas) de las redes corporativas requieren seguridad de red, se considera como las tres metas principales de la seguridad de red: la confidencialidad, la integridad y la disponibilidad. Estas son desarrolladas a continuación.

a. Confidencialidad

La confidencialidad de la información implica mantener la privacidad de la información. Esta privacidad podría ser físicamente o lógicamente de acceso restringido a la información sensible o a la encriptación de tráfico de red. Una red que ofrece confidencialidad podría hacer lo siguiente:

- Los mecanismos de seguridad de red (por ejemplo, firewalls y listas de control de acceso) previenen el acceso no autorizado a los recursos de red.
- Requiere de credenciales apropiadas (por ejemplo, usuarios y contraseñas) para acceder a recursos de red específicos.
- Tráfico encriptado, de manera que el atacante no pueda descifrar cualquier tráfico que capture desde la red.

b. Integridad

La integridad de la información asegura que los datos no han sido modificados en tránsito. También se considera una solución de integridad de información la autenticación que verifica que el tráfico originado desde el origen es el enviado. Ejemplo que incluye violación de la integridad es lo siguiente:

- Modificar la página web corporativa.
- Interceptar y alterar las transacciones de comercio electrónico.
- Modificar los estados financieros que son almacenados electrónicamente.

c. Disponibilidad

La disponibilidad de la información es una medida de la accesibilidad de la data, por ejemplo, si un servidor estuviera inactivo solamente 5 minutos por año, podría tener una disponibilidad de 99.999%. A continuación se muestra un par de ejemplos de cómo un

atacante podría intentar comprometer la disponibilidad de la red:

- Se podría enviar información de formato inadecuando a los dispositivos de red, resultando un error de excepción no manejable por el dispositivo de red.
- Se podría inundar la red con una cantidad excesiva de tráfico o requerimientos. Esto consumiría procesamiento de los recursos del sistema y podría responder previniendo con varios requerimientos verdaderos. Este tipo de ataque es llamado denegación de servicio (DoS).

2.3.4 Firewall (corta fuego)

Es un dispositivo o conjunto de dispositivos diseñados para permitir o denegar direcciones de red basado en reglas y frecuentemente usado para proteger redes de acceso no autorizado mientras que permite comunicación legítima [10].

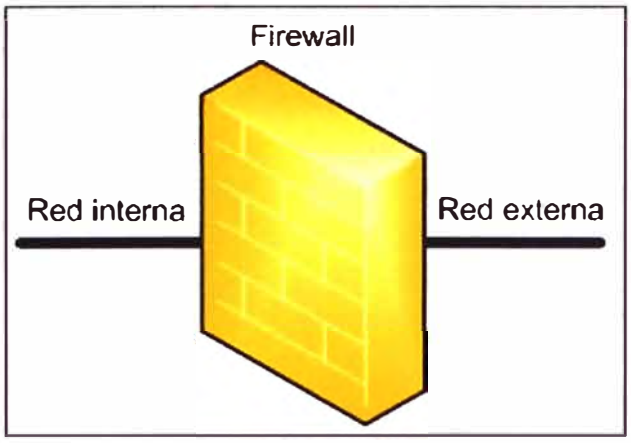

Figura 2.8 Representación de Firewall (Fuente: Elab. prop.)

Los firewalls actuales reúnen características avanzadas, sin embargo, es necesario mencionar las capacidades que tuvieron los firewalls durante su evolución tecnológica.

a. Primera generación de firewalls (filtrado de paquetes):

Este tipo de filtrado de paquetes no presta atención si un paquete es parte de un flujo de tráfico. En lugar de esto, filtra cada paquete basado solamente en información contenida en su propio paquete (más comúnmente usando una combinación de paquete con dirección de origen y destino, protocolo, y el número del puerto TCP y UDP).

Los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) constituyen la mayor comunicación sobre Internet; por convención el tráfico TCP y UDP usan puertos conocidos para un tipo de tráfico en particular.

Los firewalls con filtrado de paquete funcionan principalmente en las tres primeras capas del modelo OSI.

b. Segunda generación de firewalls (capa de aplicación)

La clave del beneficio del filtrado de capa de aplicación es que puede entender ciertas aplicaciones y protocolos (tal como FTP, DNS, o Web), y puede detectar si un protocolo no deseado está oculto a través de puertos no estándares.

Un firewall de aplicación es mucho más seguro y confiable comparado con firewalls de filtrado de paquetes porque funciona en las siete capas del modelo OSI, desde la capa 1 (físico). Esto es similar a un firewall de filtrado de paquete, pero aquí se puede filtrar información en base al contenido. Un firewall de aplicación puede filtrar protocolos de capa alta como FTP, Telnet, DNS, DHCP, HTTP, TCP, UDP y TFTP.

c. Tercera generación de firewalls (filtros de estado)

Combina la primera y segunda generación de firewalls, además de añadir la inspección del estado del paquete, así como al mantenimiento las conexiones que pasa a través del firewall. El firewall es capaz de determinar si un paquete empieza una nueva conexión, una parte de una conexión existente, o es un paquete inválido.

2.3.5 Administración de usuarios

El acceso no autorizado a una red crea potenciales intrusos que pueden ganar acceso a los equipos de red y servicios sensibles. La arquitectura AAA (Authentication, Authorization, Accounting) [9][11] ofrece un medio para hacer frente a estas amenazas a través de la seguridad sistemática y el acceso escalable. En efecto, los usuarios finales y los posibles intrusos no son los únicos que traten de acceder a la red. Los administradores de red también tienen acceso a dispositivos de red, y AAA ofrece un medio seguro que proporciona esto.

La arquitectura AAA ofrece un acceso y administración en ambientes de red, referente a la red de campus, dialup, o acceso a internet, basado en una arquitectura modular que es compuesta por tres componentes funcionales. Autenticación, Autorización, y Contabilidad.

- **Autenticación**: la autenticación es el proceso por el cual los usuarios y administradores prueban que ellos son quienes dicen ser. En ambientes de red varían los mecanismos para comprobar la autenticación, incluyendo el uso de usuarios y contraseñas, tarjetas token, etc.
- **Autorización**: después que el usuario o administrador ha sido autenticado, la autorización sirve para decidir a qué recurso se es permitido acceder, de manera que la operación se puede realizar.
- **Contabilidad y auditoría**: después que la autenticación y autorización han sido realizadas, el usuario o administrador empieza a acceder a la red. Es el rol de la contabilidad y auditoría grabar qué es lo que el usuario o administrador actualmente hace con este acceso, a qué accede, y por cuánto tiempo accede.

TACACS+ y RADIUS son los protocolos AAA más usados, también son los más populares, cada uno tiene propiedades que hacen que sean apropiados para diferentes situaciones. RADIUS es un protocolo AAA estándar, mientras que TACACS+ es un

protocolo propietario de Cisco que encripta la información y reemplaza las viejas versiones de TACACS y XTACACS.

TACACS+ funciona en TCP, y RADIUS opera en UDP. Por otro lado, TACACS+ puede controlar los niveles de autorización de los usuarios, pero RADIUS no puede. A diferencia de RADIUS, TACACS+ también separa la autenticación y la autorización. Esta propiedad permite el uso de TACACS+ para la autorización y la contabilidad, ofreciendo flexibilidad para implementar diferentes métodos de autenticación.

La arquitectura AAA para dispositivos Cisco ofrece tres maneras para implementar AAA.

a. Solución de seguridad de Servidor de Control de Acceso

En esta implementación, AAA funciona sobre el servidor de control de acceso, el cual actúa como un guardián de acceso que protege recursos, contactando el servidor de control de acceso para la autenticación de usuarios y administrador. El servidor de control de acceso es un dispositivo que contiene un agente de seguridad. Este puede ser fácilmente aprovechado por algunas organizaciones. El administrador del ACS podría también tomar pasos para bloquear el acceso a ciertos usuarios.

b. Solución de servidor de control de acceso (ACS) para Servidores Windows

Este software puede ser usado para la autenticación de usuarios y administradores, el administrador del ACS podría también tomar pasos para bloquear el acceso a ciertos usuarios.

c. AAA local

AAA también puede funcionar en un dispositivo de red implementado, de forma que la autenticación resida en el mismo dispositivo.

Comúnmente en las implementaciones de AAA se usa la autenticación de usuarios para acceder a la red corporativa a través de una conexión remota, tal como dialup o vía Internet sobre una red privada virtual (VPN). Otra implementación es cuando un administrador quiere acceder a un dispositivo de red por el puerto consola vía Telnet o SSH (Secure Shell).

El control de acceso mediante AAA es soportado por los dispositivos Cisco usando usuario y contraseña o a través de servidores de seguridad con base de datos. Que ofrecen acceso a pequeños grupos de usuarios de red; una base de datos de seguridad puede ser configurada en un dispositivo de red usando un usuario y contraseña.

Un servidor de seguridad remoto puede también ser usado. Esta implementación usa una base de datos de seguridad en un servidor separado, corriendo un protocolo de seguridad AAA. Este puede ofrecer servicios AAA a múltiples dispositivos de red y gran número de usuarios.

2.3.6 Inspección de protocolos de aplicación

Algunas aplicaciones requieren de un manejo especial de una porción de datos de un paquete. La inspección de los protocolos de aplicación [12] ayuda a verificar el comportamiento de los protocolos de aplicación e identificar que tráfico malicioso no se quiere que pase a través de los dispositivos de seguridad y balanceo de carga. Basado en las especificaciones de las políticas de tráfico, el dispositivo de seguridad y balanceo de carga acepta o rechaza los paquetes asegurando que las aplicaciones y servicios estén a salvo.

Los dispositivos de seguridad y balanceo de carga inspeccionan aplicaciones como DNS, FTP, HTTP, ICMP (Internet Control Message Protocol), RTSP (Real Time Streaming Protocol), SCCP (Skinny Client Control Protocol), ILS (Internet Locator Service), y SIP (Session Initiation Protocol).

Como primer paso antes de que los paquetes pasen al servidor destino, la inspección de aplicaciones ayuda a identificar la localización de la información embebida en las direcciones IP en el flujo TCP o UDP. Esta inspección permite al dispositivo de seguridad y balanceo de carga trasladar las direcciones embebidas y actualizar cualquier suma de revisión u otro campo que son afectados en la traslación.

La traslación de direcciones IP embebida en el cuerpo de los protocolos es especialmente importante para el NAT y el balanceo de carga. La inspección de aplicaciones también monitorea sesiones TCP o UDP que determina el número de puertos alternativos. Algunos protocolos abiertos de TCP o UDP mejoran el desempeño. La sesión inicial de los puertos conocidos es usada para negociar dinámicamente los puertos asignados. La inspección de protocolos de aplicación tiene la función de monitorear estas sesiones, identificar el puerto dinámico asignado, y permite intercambiar información en estos puertos durante la sesión.

a. Inspección de DNS

La inspección de DNS desempeña las siguientes tareas:

- Monitorea los mensajes intercambiados de forma que aseguren que el identificador del paquete de respuesta del DNS posea una comparación correcta con el paquete de petición del DNS.
- Permite al DNS responder cada paquete de petición DNS en una conexión UDP. El dispositivo de seguridad y balanceo de carga remueve las sesiones DNS asociadas con la petición DNS tan pronto como la respuesta del DNS sea reenviada.
- Traduce el DNS a una base de grabación en la configuración del NAT (Network Address Translation). Solamente las búsquedas enviadas son traducidas usando NAT; el dispositivo de seguridad y balanceo de carga no administra los estados de conexión.

- Realiza la revisión del tamaño del paquete de respuesta del DNS y toma acción si sobrepasa el tamaño.
- Despliega un número de revisión de seguridad de la siguiente manera: Verifica que la longitud máxima de la etiqueta no es mayor a 63 bytes, Verifica que la longitud máxima del nombre del dominio no sea mayor 255 bytes.

b. Inspección de ICMP

La inspección de ICMP permite al trafico ICMP tener una sesión que pueda ser inspeccionada similarmente que el trafico TCP y UDP. Si no se usa la inspección de ICMP, se recomienda no crear listas de acceso que permitan el paso del trafico ICMP que pase a través del dispositivo de seguridad y balanceo de carga.

Sin la inspección, ICMP puede ser usada para atacar la red. La inspección ICMP asegura que hay solamente una respuesta por cada paquete de petición ICMP, y que el número de secuencia es correcto.

La inspección ICMP realiza las siguientes tareas para los paquetes de solicitud ICMP o paquetes de respuestas de mensajes ICMP:

- Crea una sesión bidireccional o estado de conexión. La clave en la búsqueda del reenvío de la dirección IP, es la dirección IP origen, dirección IP destino, tipo de protocolo ICMP, identificador ICMP, y VLAN.
- Verifica que el estado de la conexión contenga una ventana con un número de secuencia que especifique la lista de los números de secuencia de los paquetes de solicitudes pendientes de manera que los paquetes de respuesta estén pendientes.
- Verifica que los estados de conexión tengan un tiempo límite, entonces las conexiones inactivas pueden ser reusadas por otros flujos y pueden proteger la red interna contra paquetes ICMP fraudulentos.
- La respuesta del paquete es permitida solamente si una conexión es válida y previene la respuesta de paquetes que pasan a través de una ACL (lista de acceso) nuevamente si la conexión existe.
- Crea un estado de conexión para los paquetes de solicitudes y respuestas ICMP y también para los paquetes direccionados hacia o desde el dispositivo de seguridad y balanceo de carga.

2.3.7 Listas de acceso

Las listas de acceso filtran tráfico de red controlando que paquete es reenviado o bloqueado en las interfaces de un router, switch, dispositivo de seguridad y balanceo de carga, y firewall. Los dispositivos de red determinan si se reenvía o rechaza los paquetes, basados en los criterios especificados en las listas de acceso [13].

El criterio de la lista de acceso podría ser por dirección origen, dirección destino, por

protocolo de capa superior, o por otra información. Se debe notar que los usuarios avanzados algunas veces evaden satisfactoriamente las listas de acceso básicas, porque no se requiere autenticación.

Hay varias razones para configurar listas de acceso, por ejemplo, se puede usar listas de acceso para restringir contenido de actualización de protocolo de enrutamiento, u ofrecer control de flujo de tráfico de datos. Pero una de las más importantes razones para configurar listas de acceso es ofrecer seguridad a la red.

Se debería usar las listas de acceso para ofrecer un nivel básico de seguridad para acceder a una red. Si no se configura listas de acceso en los dispositivos de red, todos los paquetes que pasan a través de estos dispositivos podrían permitir el acceso a cualquier parte de la red.

Por ejemplo, las listas de acceso pueden permitir que una estación acceda a una parte de la red, y previenen que otra estación acceda a la misma área. En la Figura 2.9 la estación A esta permitida para acceder a la red de recursos humanos y la estación B no tiene acceso a la red de recursos humanos.

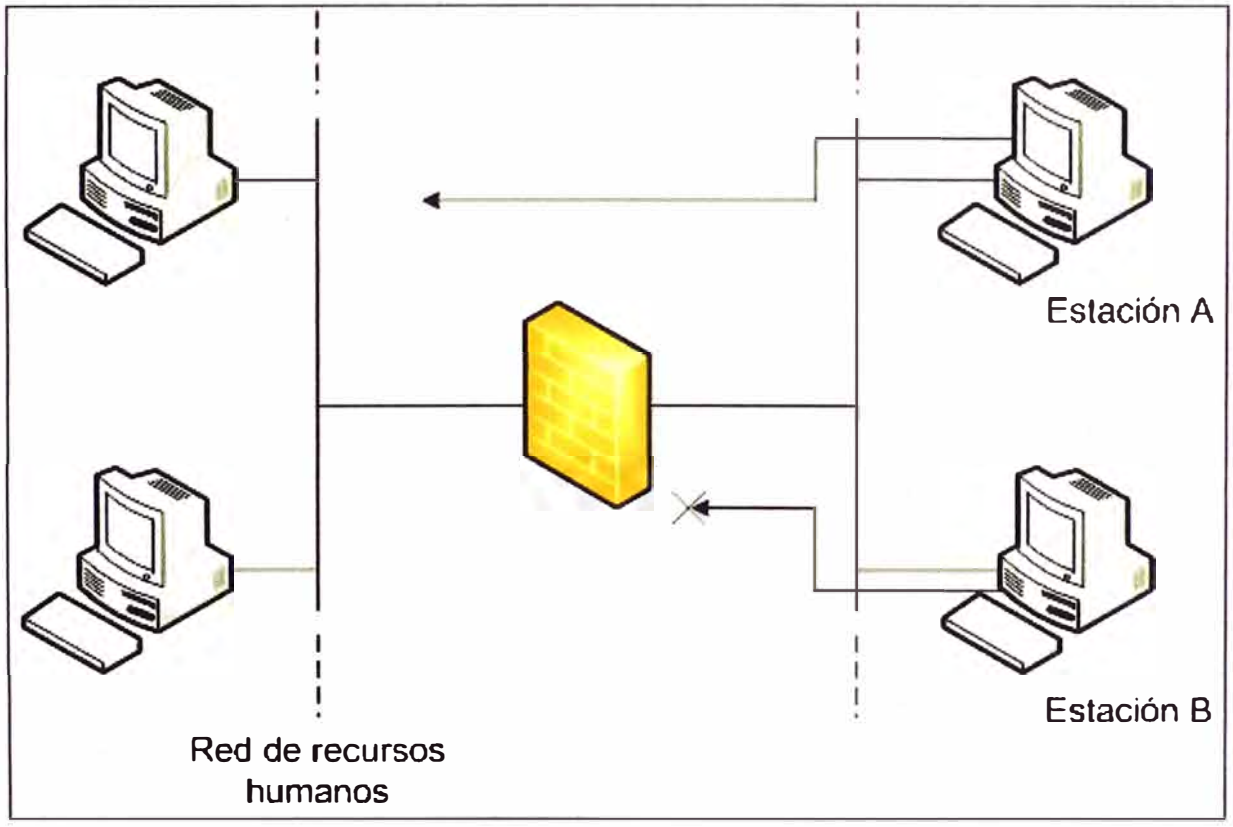

Figura 2.9 Ejemplo de listas de acceso (Fuente: Elaboración propia)

Las listas de acceso deberían ser usadas en firewalls, los cuales son colocados entre una red interna y una red externa, tal como internet. Se puede usar listas de acceso en un router posicionándolo entre dos zonas de la red, para controlar el tráfico entrante o saliente en una parte especifica de la red interna.

Para aprovechar los beneficios de seguridad de la red, las listas de acceso deben ser configuradas mínimamente en los routers de borde, routers situados en la parte externa de la red. Esto ofrece un mayor control desde un área de menos control a la red interna o a la parte más sensible de la red.

En estos routers, se debe configurar listas de acceso para cada protocolo de red configurado en las interfaces del router. Se puede configurar listas de acceso con orientación de flujo entrante o con orientación de flujo saliente o en ambas direcciones.

2.4 Disponibilidad

Las empresas de hoy en día requieren que su red sea altamente disponible para asegurar que sus aplicaciones de misión crítica estén disponibles. El incremento de la disponibilidad se traslada en la alta productividad, incrementando ingresos económicos, y ahorrando costos. La disponibilidad significa que el sistema está listo para ser usado inmediatamente.

2.4.1 Disponibilidad individual

Los factores que afectan la disponibilidad son el MTTR (mean time to repair) y MTBF (mean time by failure) [14][15].

- MTTR es el tiempo que toma un dispositivo en recuperarse de una falla,
- MTBF es el tiempo que pasa entre falla de un dispositivo.

Cuando decrece el MTTR y/o se incrementa el MTBF entonces incrementa la disponibilidad.

$$\text{Disponibilidad} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \tag{2.1}$$

Por ejemplo, para el cálculo de la disponibilidad para una fuente de alimentación: el MTBF de la fuente de alimentación es 40,000 horas y el MTTR es 8 horas. Reemplazando los valores en la fórmula 2.1 se obtiene:

$$\text{Di} = \frac{40000}{40000 + 8} = 99.98\%$$

2.4.2 Disponibilidad del sistema

Para el cálculo de la disponibilidad de un sistema (Ds) en serie se debe multiplicar la disponibilidad de cada uno de los componentes (Di) del sistema [16]. Figura 2.10

$$\text{Ds} = \prod_{i=1}^{n} D_i \tag{2.2}$$

Para el cálculo de la disponibilidad de un sistema (Ds) en paralelo se debe restar a 1 el producto de las disponibilidades de los complementos respecto a 1 de todos los componentes del sistema. Figura 2.11

$$\text{Ds} = 1 - \prod_{i=1}^{n} (1 - D_i) \tag{2.3}$$

Donde n el número de componentes del sistema.

Figura 2.10 Sistema en serie (por ejemplo con disponibilidad Dx).

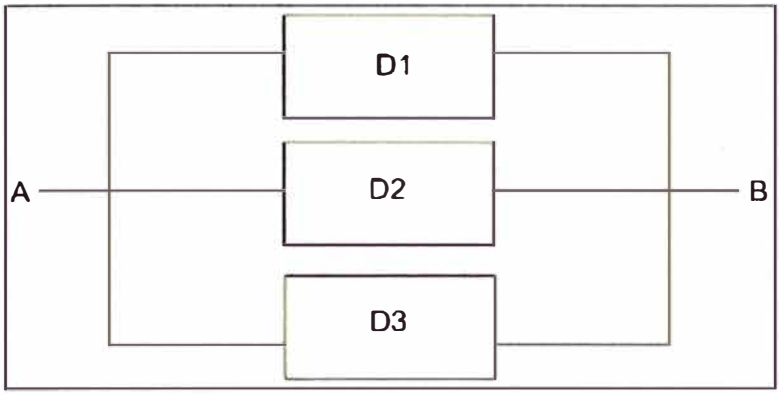

Figura 2.11 Sistema en paralelo (Por ejemplo con disponibilidad Dy)

Para el ejemplo de la Figura 2.10 la disponibilidad sería Dx=D1.D2. Para el ejemplo de la Figura 2.11 la disponibilidad sería igual a Db= 1-(1-D1).(1-D2).(1-D3). Para sistemas combinados se hace el tratamiento individual por partes. Por ejemplo si los sistemas Dx y Dy se colocan:

- En paralelo, entonces la disponibilidad sería Df = 1-(1-Dx).(1-Dy)
- En serie, entonces la disponibilidad sería Df = Dx.Dy

Existe un caso especial del calculo de disponibilidad para sistemas llamados puente Figura 2.12.

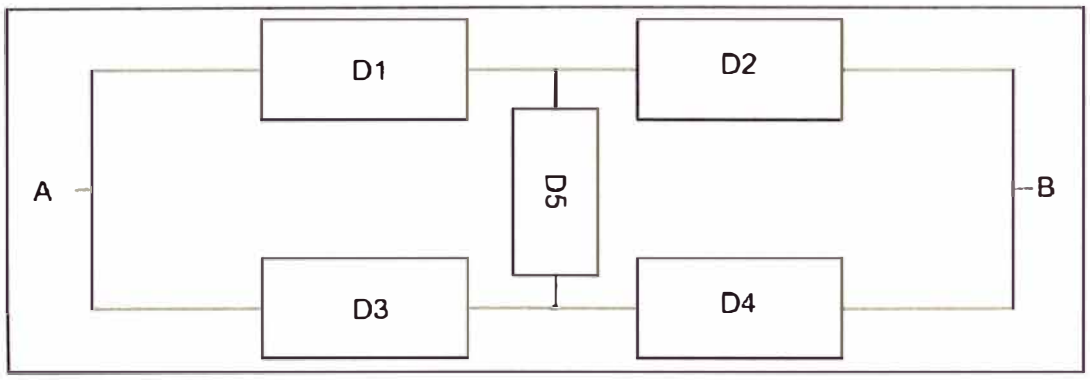

Figura 2.11 Sistema en puente (Por ejemplo con disponibilidad Dz)

La disponibilidad de este caso se resuelve creando cuatro susbsistemas series:

- Dserie1= D1.D2
- Dserie2= D3.D4
- Dserie3= D1.D5.D4
- Dserie4= D3.D5.D2

Estos sistemas luego son colocados en paralelo y la disponibilidad obtenida se calcula finalmente Df = 1- (1-Dserie1). (1-Dserie2) (1-Dserie3) (1-Dserie4). Figura 2.12.

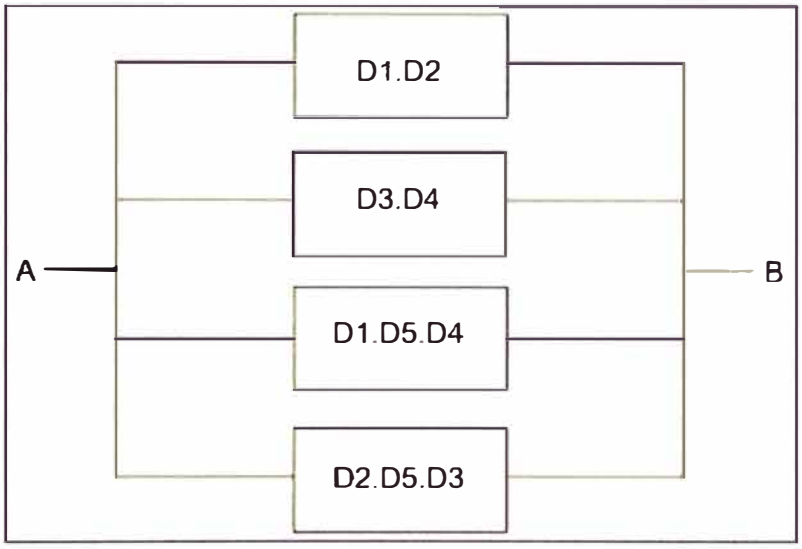

Figura 2.12 Sistema en puente equivalente

2.4.3 Disponibilidad en la red de datos

La teoría expuesta anteriormente se aplica a un sistema en general. Para el caso de las redes de datos, los componentes no son solo los dispositivos de comunicaciones, sino también los propios enlaces (Figura 2.13)

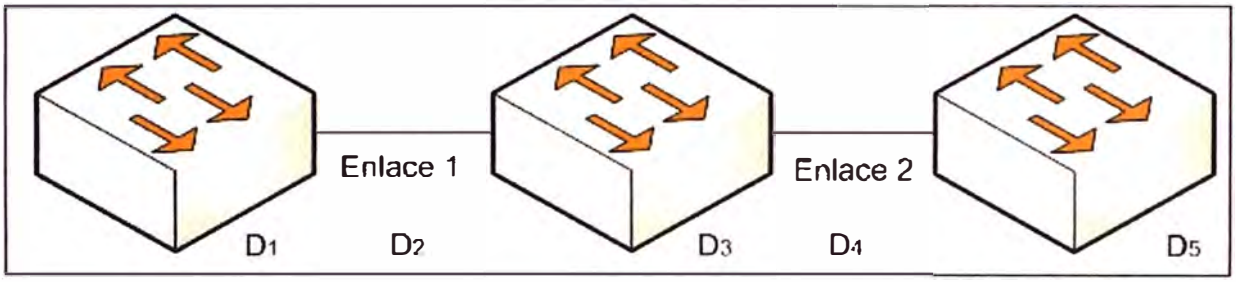

Figura 2.13 Esquema ejemplo de los componentes del sistema en serie

Teniendo como ejemplo la Figura 2.13, la disponibilidad del sistema Ds = D1.D2.D3. D4.D5. Si a la topología mostrada se realiza una modificación que permita incrementar la disponibilidad de uno de los componentes, entonces la disponibilidad obtenida es mayor. Como ejemplo se muestra la Figura 2.14. Para este caso se ha realizado la agregación de un enlace entre los dos primeros dispositivos de comunicaciones; esta agregación se considera redundante, es decir que si un enlace falla el otro enlace permite la continuidad de las comunicaciones, **la disponibilidad D2 es ahora mayor** (puede considerarse = 1 o calcularse como 1-(1-Denlace1).(1-Denlace2))

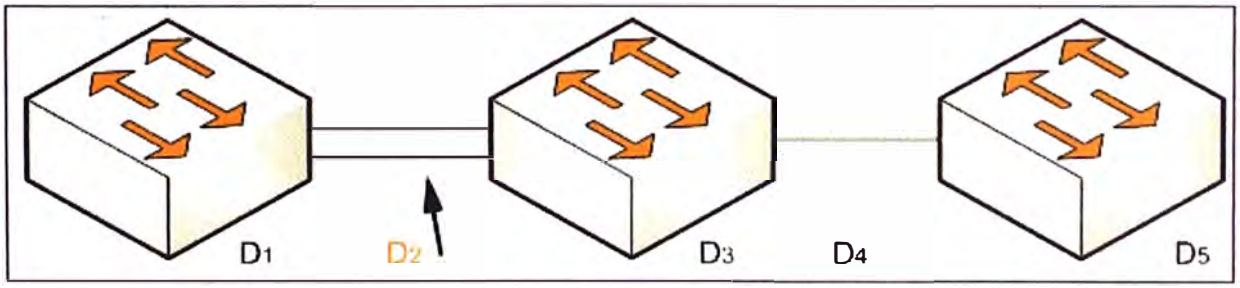

Figura 2.14 Esquema de los componentes del sistema en serie modificado

Para la evaluación, a nivel de disponibilidad, de las diversas topologías para un mismo sistema, no es tan importante saber los valores de disponibilidad individual sino más bien realizar un análisis comparativo. Por ejemplo si Ds1 = D1.D2.D3.D4.D5, y Ds2 = D1.**1**. D3.D4.D5 (se asume D2=1) se concluye que Ds2 > Ds1. Es por ello que, incluso desconociendo los valores de disponibilidad individuales, se puede realizar el análisis de que topología es la mejor.

Es necesario notar que la inclusión de un dispositivo (sin redundancia) destinado a realizar una tarea específica (antes no soportada) mejora el desempeño del sistema pero debilita la disponibilidad del sistema, ya que introduce un factor (<1).Ver D6 Figura 2.15.

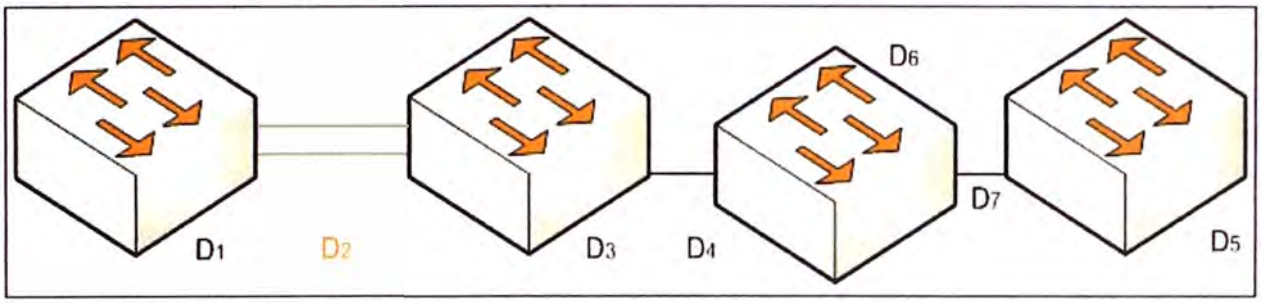

Figura 2.15 Aumento de desempeño del sistema

En la Figura 2.15 se ha incluido un dispositivo de comunicaciones entre los enlaces de los últimos dispositivos, para ello también se ha aumentado un enlace, entonces la disponibilidad del sistema Ds3 = D1.1.D3.D4.D5.**D6.D7**

La disponibilidad no se circunscribe a los dispositivos físicos, también son consideradas las aplicaciones que mantienen funcional un sistema, en este rango se incluyen a los sistemas de seguridad ya mencionados que evitan que el sistema sea paralizado (antivirus, ataques de denegación de servicio, etc.).

Por ejemplo si para efectos comparativos de dos sistemas de topologías iguales, se considera que en uno no existe una aplicación o módulo de seguridad, mientras que en otro no (o de menores prestaciones), entonces el cálculo de la disponibilidad queda modificado si se utiliza como ejemplo la Figura 2.16 entonces la disponibilidad del sistema es Ds = D1.D2.D3.**Dap**; donde Dap es la disponibilidad de la aplicación o el módulo de seguridad.

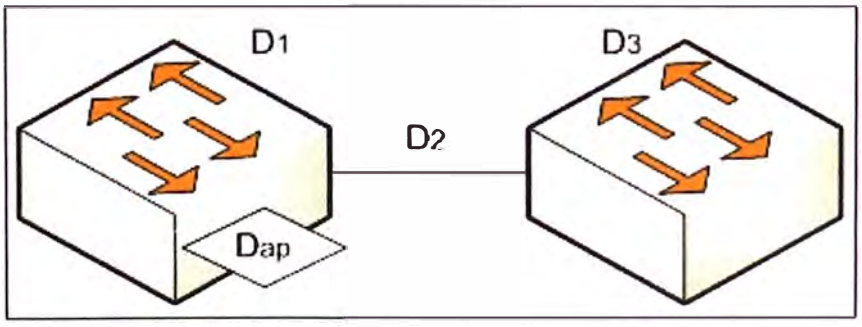

Figura 2.16 Aumento de desempeño del sistema

De lo mostrado, si para un sistema 2 el valor de la disponibilidad de su módulo de seguridad es mayor que la del sistema 1 (Dap1<Dap2), entonces se concluye que la disponibilidad del sistema 2 es mayor que la del sistema 1 (Ds2>Ds1)

2.4.4 Análisis comparativo

Para el análisis comparativo de la disponibilidad de varias topologías, se debe considerar la totalidad de los elementos que se incluyen en el sistema más robusto. En el caso que algunas topologías no posean ciertos elementos que aseguren la disponibilidad del sistema, se deberán incluir en el cálculo de disponibilidad un factor menor al de la topología que si lo tenga (como en el ejemplo mostrado en la figura 2.15). Solo así se asegura un análisis comparativo real de la disponibilidad (se deben incluir los aspectos descritos en las secciones 2.2 y 2.3).

Como ya fue mencionado, para la evaluación de diversas alternativas de solución deben considerarse también los aspectos de desempeño que cumplan los requerimientos estipulados (más capacidad de tráfico, de almacenamiento, etc.)

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se describe la ingeniería del proyecto de reestructuración de la topología del Centro de Servicios del ISP. Se realiza el análisis preliminar para determinar la solución a implementar, posteriormente se explica la solución implementada y finalmente se hace una descripción técnica del equipamiento utilizado.

3.1 Análisis preliminar

En esta sección se describe la situación inicial (previa a la solución implementada) del Centro de Servicios, a fin de analizar sus puntos débiles; luego se evalúan las posibles configuraciones de solución; y para concluir, se hace el dimensionamiento de la solución propuesta.

3.1.1 Descripción situacional de la topología Centro de Servicios

En esta subsección se describe la situación del Centro de Servicios del proveedor de servicios de internet (ISP) antes de la solución implementada.

El Centro de Servicios consta de dos centros de datos que funcionan simultáneamente (uno es respaldo del otro), éstos interconectados a través de un enlace Gigabit Ethernet entre los dos Switches WS-C6509-E.

Para comprender las debilidades de la infraestructura es necesario conocer diversos aspectos, tales como su topología, su funcionamiento en modo normal y el procedimiento de contingencia. El resumen del análisis situacional, es decir, los puntos débiles o desventajas de la situación inicial, es expuesto al final de esta sección, a fin de evaluar las mejores alternativas de solución en la sección siguiente.

a. Topología

La Figura 3.1 muestra el esquema de la topología inicial. En el se puede apreciar a dos ramificaciones que parten de la nube WAN que son simétricas para las sedes de Lima y San Isidro.

En general, esta estructura de datos consta de los siguientes equipos de comunicaciones: un router Cisco 7206VXR, un Switch WS-C6513-E, un módulo de servicio de Firewall (FWSM) integrado al Switch WS-C6513-E, un Switch WS-C6509-E, un Switch de contenido de servicios CSS11506, y una granja de servidores DNS. La única diferencia es que en la sede Lima la granja de servidores consta de 8 servidores mientras que la de San Isidro consta de 7 servidores.

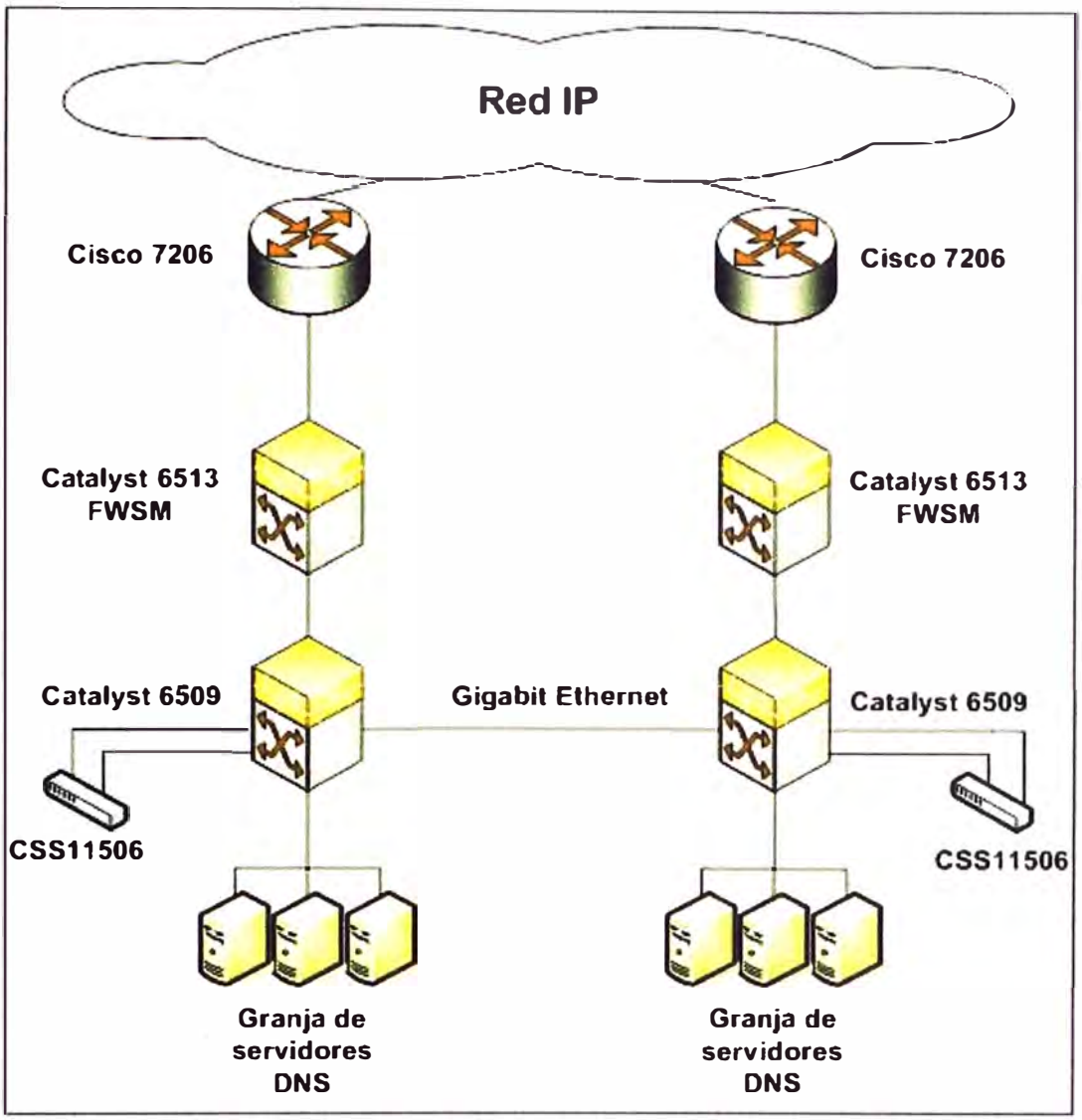

Figura 3.1 Topología de la infraestructura de red inicial (Fuente: Elab. Propia)

b. Funcionamiento en modo normal

Dada la similitud de ambas sedes en su funcionamiento, se describe de manera general los dispositivos de una de las ramificaciones. Para el funcionamiento general se debe hacer referencia a lo desarrollado en la sección 2.1 del marco teórico en lo que respecta al DNS, a las granjas de servidores y al balanceo de carga.

b.1 Balanceador de carga (CSS11506)

Tiene la función de decidir qué servidor real de la granja de servidores de la sede asumirá las peticiones y respuestas DNS. En el CSS11506 se encuentran declarados 7 servidores para San Isidro y 8 para Lima. Los servidores de Lima pertenecen a la red 10.5.1.0/24, mientras que los de San Isidro a la red 10.5.2.0/24.

Cada servidor tiene un "peso" asignado. Se asignan pesos de 10 y de 20. El peso significa que al momento de hacer el balanceo los servidores con un peso de 10 tienen menos carga que los servidores con peso 20, es decir los de mayor peso tienen mayor desempeñó al asumir mayor carga de trabajo en el proceso de balanceo round robin (por

cada 10 conexiones en un servidor peso 10, se realiza después 20 conexiones a un servidor peso 20). Para San Isidro la configuración de "peso" es de 6 a 1 (seis con peso 10 y uno con peso 20), mientras que la sede de Lima es de 6 a 2.

La granja de servidores está representada a través del balanceador de carga por una IP virtual (200.48.225.130 Lima y 200.48.225.146 para San Isidro). El balanceador de carga esta interconectado mediante dos puertos Fast Ethernet al Switch WS-C6509-E.

b.2 Switch WS-C6509-E

La función que tiene este equipo es extender el número de servidores declarados en el balanceador de carga, configurándolos en una VLAN de manera que estén confinados a esa red y mediante otro puerto (en la misma VLAN) se comuniquen al balanceador de carga. Para la sede de Lima la VLAN es la 61 y para la sede San Isidro es la 60.

Por otro lado, la dirección IP 200.48.225.130 pertenece a una VLAN que es interconectado al FWSM (módulo de firewall) integrado al Switch WS-C6513-E por un puerto trocal que lleva esta VLAN (74 para Lima y 54 para San Isidro).

b.3 Switch WS-C6513-E

La función que tiene este Switch es entregar el tráfico de red que sale del balanceador de carga (CSS11506) a una VLAN que está integrada al módulo de Firewall (FWSM) interconectado vía interfaces internas del Switch (placa madre) y el FWSM.

Después que el FWSM filtra el tráfico permitido (o sea el DNS), este mismo Switch envía el tráfico al Router de salida a Internet mediante un enlace Gigabit Ethernet.

b.4 Firewall (FWSM)

La función que tiene el módulo de Firewall es permitir solo las peticiones y respuestas DNS hacia la IP que representa a la granja de servidores DNS y el protocolo ICMP a esta misma IP, otro tipo de protocolo o servicio no será permitido, de manera que se asegure un control en capa 3 y de estado de conexiones.

El FWSM está interconectado al Switch WS-C6513-E mediante interfaces internas que tiene el Switch (placa madre) y el FWSM.

b.5 Router Cisco 7206VXR

La función de este equipo es publicar los DNS a través de Internet de manera confiable y segura.

b.6 Administración de equipos

La administración de los equipos se hace localmente utilizando un usuario y contraseña por equipo.

c. Procedimiento de contingencia

En esta sección se hablará acerca del procedimiento de contingencia ante un evento inesperado, falla de hardware o la caída del enlace en el Centro de Datos de Lima o San

Isidro. Dada que la topología es simétrica, se explicará este procedimiento sólo con una de las ramificaciones. Para los esquemas de explicación, SIS representa a la sede de San Isidro y LIM representa a sede de Lima.

c.1 Falla de enlace y hardware del balanceador de carga

Está representada por la Figura 3.2. En esta falla se consideran dos escenarios:

- **Falla de enlace entre balanceador de carga y Switch WS-C6509-E**.- Ante una falla en el enlace entre el balanceador de carga y el WS-C6509-E el servicio DNS con IP 200.48.225.130 se ve afectado, dejando solo al DNS con IP 200.48.225.146 para que haga la resolución de nombre de todos los clientes corporativos y abonados.

- **Falla de hardware CSS11506**.- Ante una falla de hardware del balanceador de carga el servicio DNS con IP 200.48.225.130 se ve afectado, dejando solo al DNS con IP 200.48.225.146 para que haga la resolución de nombre de todos los clientes corporativos y abonados.

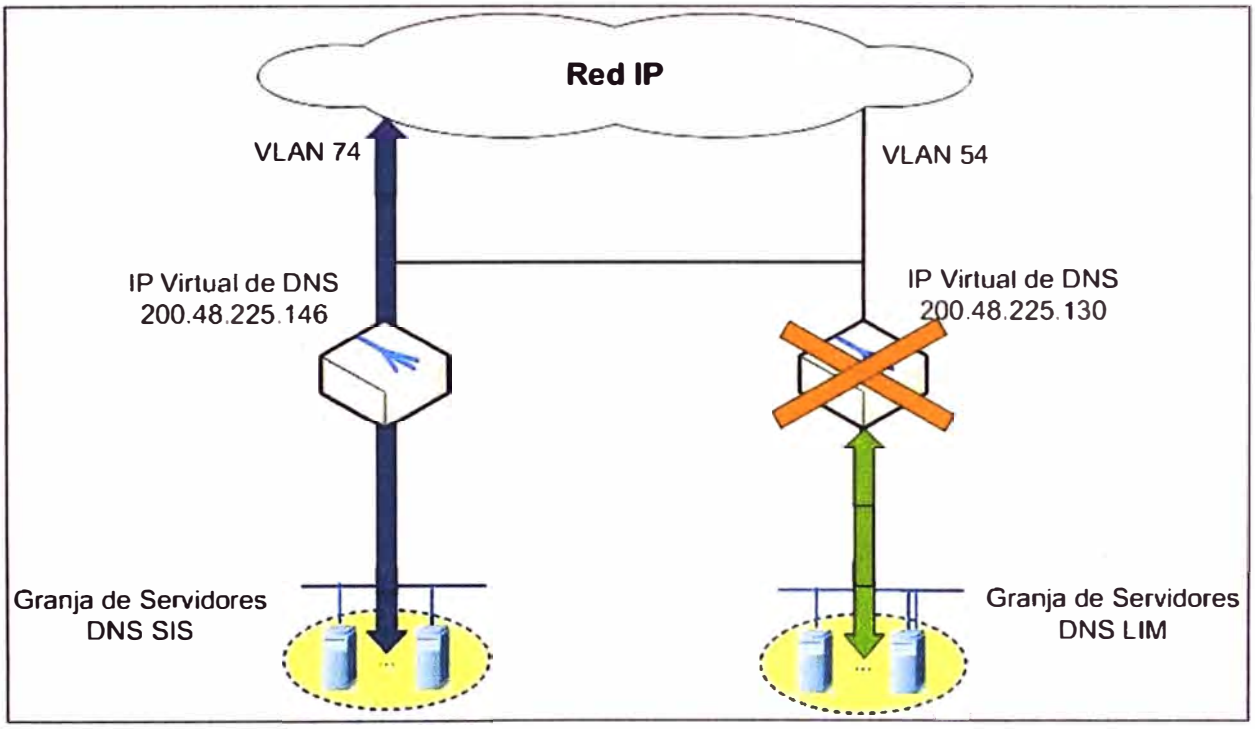

Figura 3.2 Falla de enlace y hardware del balanceador de carga (Fuente: Elab. Propia)

c.2 Falla del FWSM Lima

En este punto se indicará el evento ocasionado por la falla de hardware FWSM instalado en el Switch WS-C6509-E Lima. El procedimiento es el siguiente:

- **Falla de hardware FWSM**.- Ante una falla de hardware del Firewall Service Module el servicio DNS con IP 200.48.225.130 se ve afectado, dejando solo al DNS con IP 200.48.225.146 para que haga la resolución de nombre de todos los clientes corporativos y abonados. Ver Figura 3.3

- **Reactivación manual del servicio**.- Es la medida de contingencia a esta falla. Se

procede a configurar manualmente el FWSM San Isidro de manera que las políticas de filtrado de petición y respuesta de la dirección IP 200.48.225.130 son aplicadas por el FWSM San Isidro.

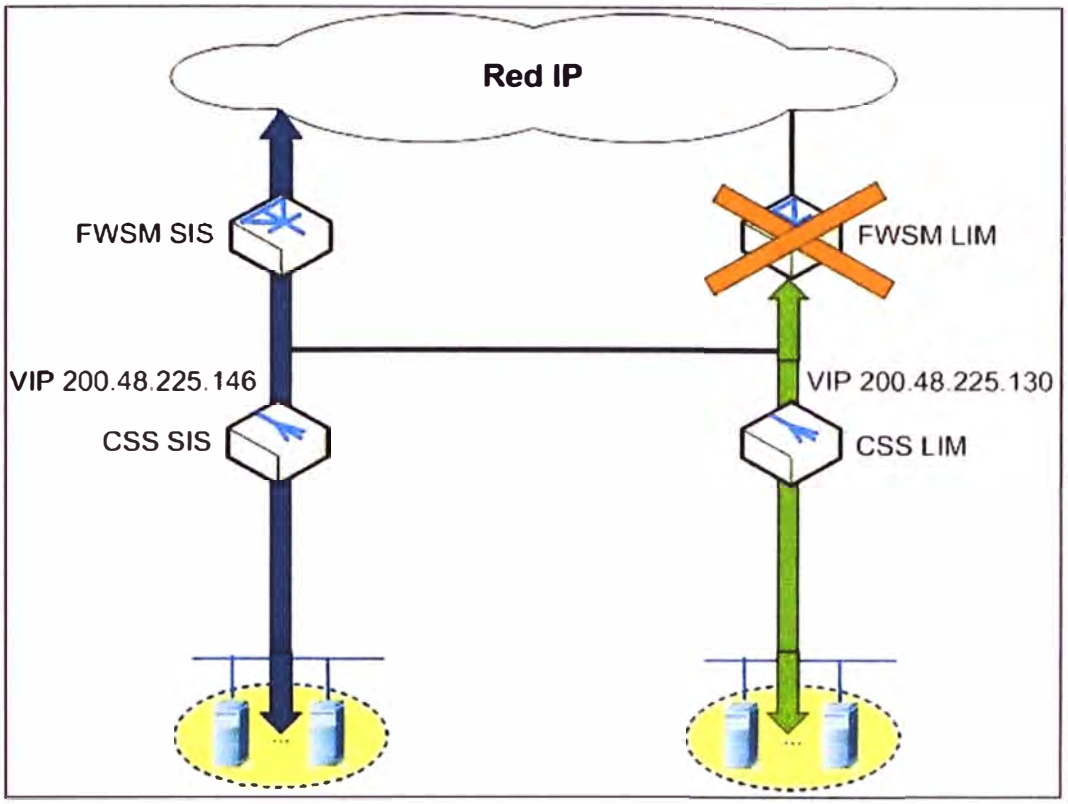

Figura 3.3 Falla del hardware FWSM (Fuente: Elaboración propia)

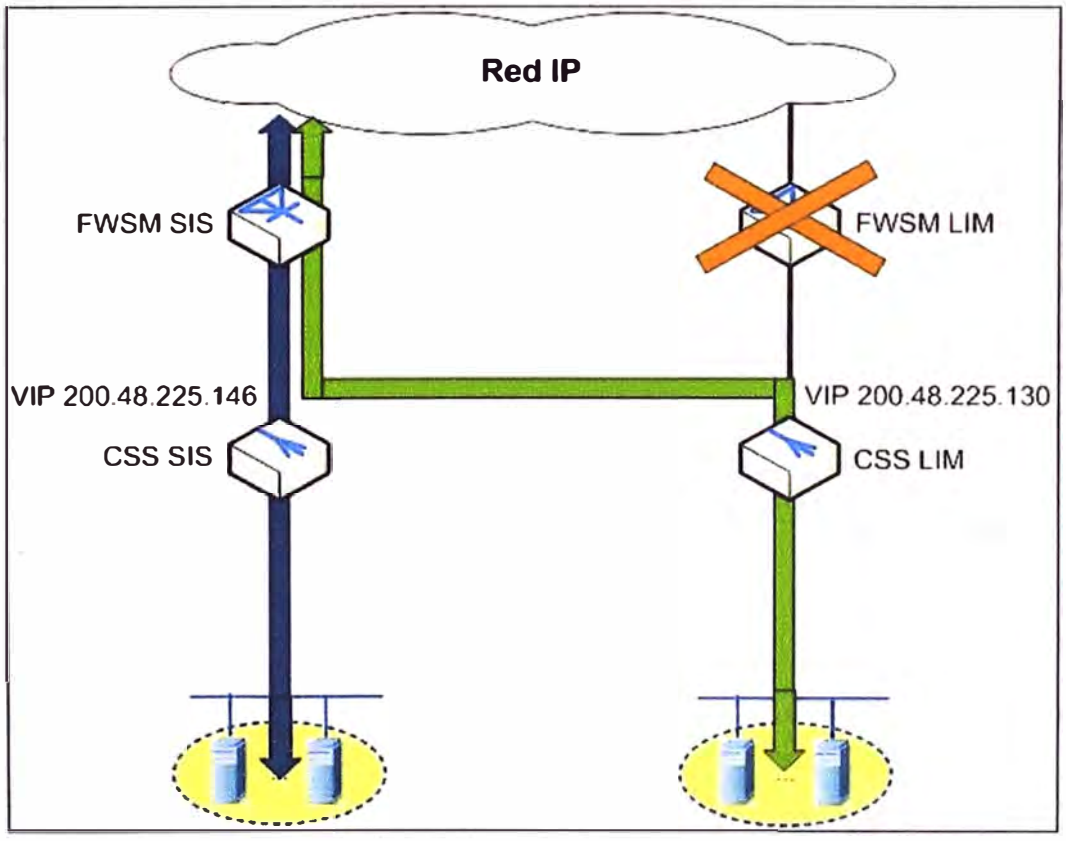

Figura 3.4 Contingencia (Fuente: Elaboración propia)

c.3 Falla de enlace entre Switches WS-C6509-E Lima y WS-C6509-E San Isidro

Está representada por la Figura 3.5. Estos Switches funcionan de manera independiente, sin afectarse el servicio, a menos que además se presente una falla en el Switch WS-C6513-E, Router, o Firewall de la sede, como se explicó en el anterior acápite.

Es necesario señalar que el tráfico que envía el balanceador de carga es enviado al WS-C6509-E, luego este tráfico es analizado y procesado por el WS-C6513-E y el firewall para ser enviado al Router. Todo este proceso en la misma sede, es decir, cada ramificación maneja el tráfico independientemente.

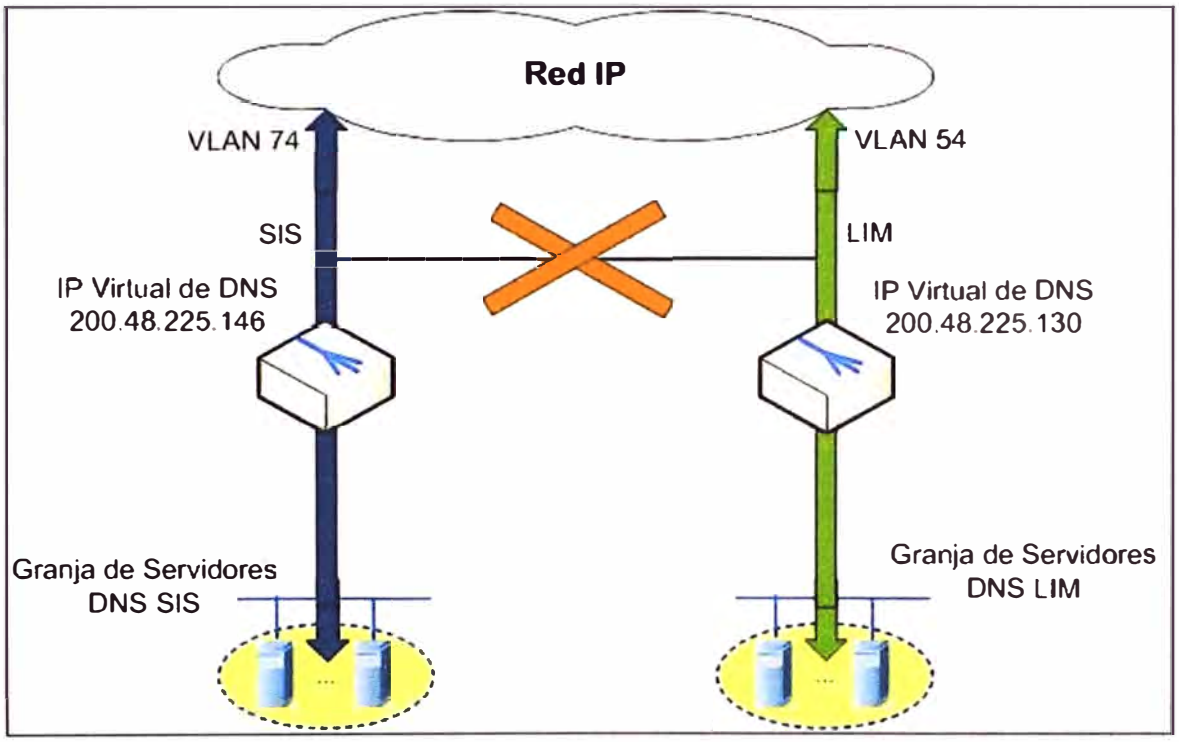

Figura 3.5 Falla enlace entre Switches C6509 (Fuente: Elaboración propia)

c.4 Falla del Router Lima

En este punto se indicará el evento ocasionado por la falla del Router Lima. El procedimiento es el siguiente:

- **Falla de hardware o enlace de Router**.- Ante una falla de hardware o enlace del Router, el servicio DNS con IP 200.48.225.130 se ve afectado, dejando solo al DNS con IP 200.48.225.146 para que haga la resolución de nombre de todos los clientes corporativos y abonados (Figura 3.6).

- **Reactivación manual del servicio**.- Como consecuencia de la falla de hardware o enlace del Router Lima, se procede a configurar manualmente el Router San Isidro, de manera que enrute las peticiones y respuestas de la dirección IP 200.48.225.130 aplicadas al Router San Isidro (Figura 3.7). Esta configuración manual es estrictamente enfocada a las tablas de enrutamiento que tenía configurado el Router afectado.

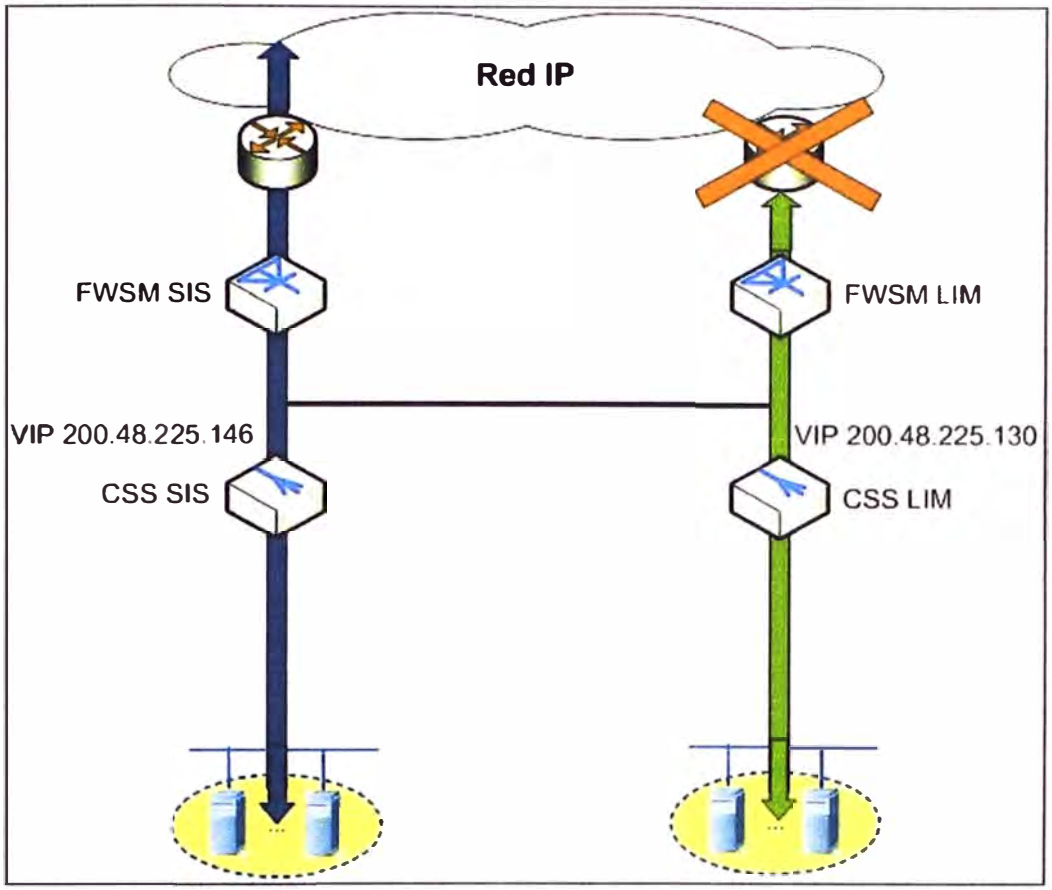

Figura 3.6 Falla hardware y enlace del router (Fuente: Elaboración propia)

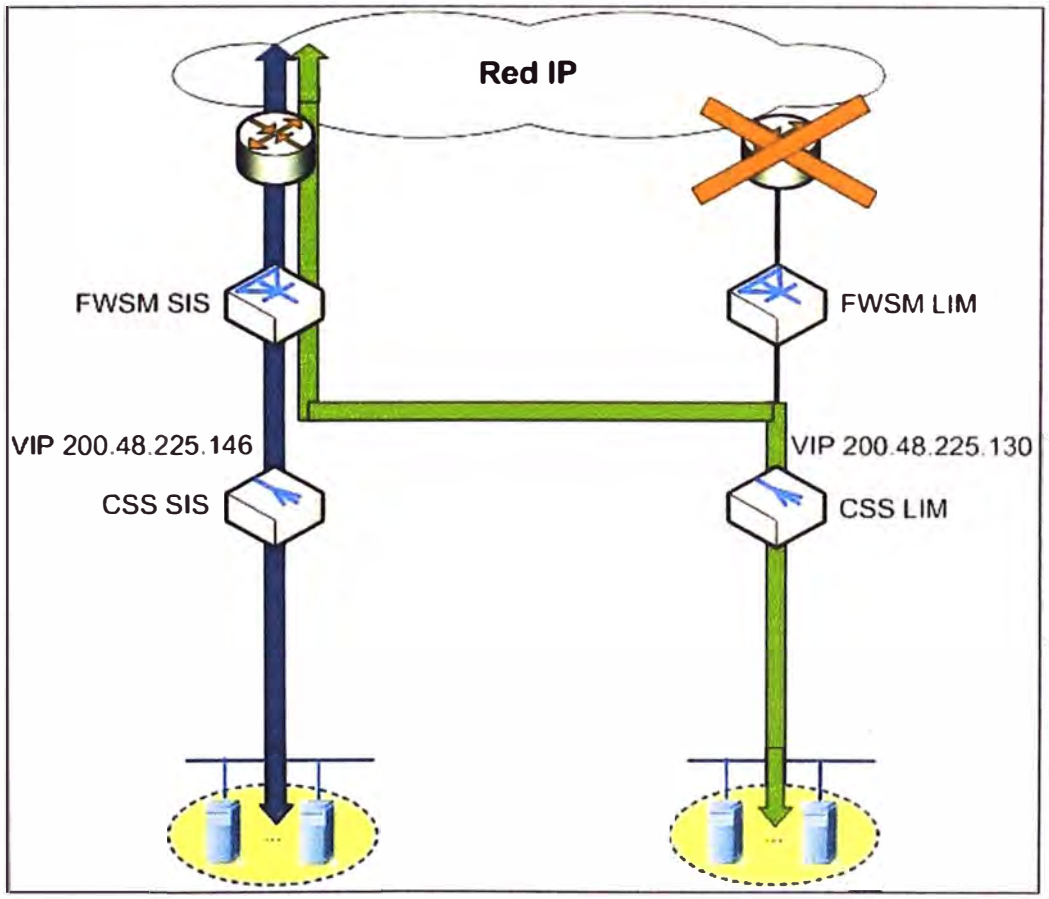

Figura 3.6 Contingencia (Fuente: Elaboración propia)

d. Desventaja de la situación inicial

En este ítem se resume los puntos débiles de la situación actual, enfocado en la disponibilidad del servicio y en la seguridad informática.

- **Balanceador de carga (CSS11506)**.- Los balanceadores de carga no soportan la creación de contextos, alta disponibilidad activo/activo, solo soportan alta disponibilidad activo/espera, no ofrece inspección de los protocolos DNS e ICMP.
- **Switches WS-C6509-E y WS-C6513-E**.- La interconexión entre los centros de datos tiene un punto de fallo desde el punto de vista de enlace y equipamiento, la velocidad de conexión entre los centros de datos está limitada por un solo enlace 1Gbps, no se tiene redundancia de enlace entre los Switches WS-C6509-E y WS-C6513-E y entre las sedes.
- **Firewall (FWSM)**.- El FWSM instalado en el Switch WS-C6513-E no soporta contextos, alta disponibilidad activo/activo, ni AAA.
- **Router Cisco 7206VXR**.- Los Routers no tienen configurado protocolos de alta disponibilidad de capa 3 (HSRP) y no conmutan de forma automática en caso falla de hardware o enlace.
- **Administración de equipos**.- Los equipos no tienen ningún mecanismo de autenticación, autorización, contabilidad y auditoría, los usuarios se almacenan localmente, no hay control de los niveles de permiso de los usuarios de administración, monitoreo, de quien ingreso a los equipos, que tiempo permaneció en cada uno de ellos y que acciones se realizaron.

3.1.2 Alternativas de solución

En esta sección se describe las alternativas de mejora a la situación inicial del Centro de Servicios. Es necesario notar que la alternativa n presentada es una mejora de la alternativa n-1. Para entender las posibles soluciones a aplicar, deben tomarse como referencia la sección 2.2 y la sección 2.3.

a. Alternativa 1

En este ítem hace mención de las mejoras que se van a realizar en la infraestructura de red de uno de los centros de datos, debe tenerse en cuenta que solo se describe una de las ramificaciones, debido a la simetría de la topología de red del ISP.

En la Figura 3.7 se puede apreciar la mejora en la alta disponibilidad de los balanceadores de carga (activo/espera), la aplicación de protocolo de alta disponibilidad capa 3 (el HSRP), la implementación de un enlace entre los Switches WS-C6513-E, la actualización (upgrade) del módulo de firewall FWSM de manera que pueda soportar alta disponibilidad, y la implementación de un servidor de control de acceso a la red (ACS).

A continuación se explica con mayor detalle las mejoras del centro de servicio y se revisa cada componente del nuevo esquema.

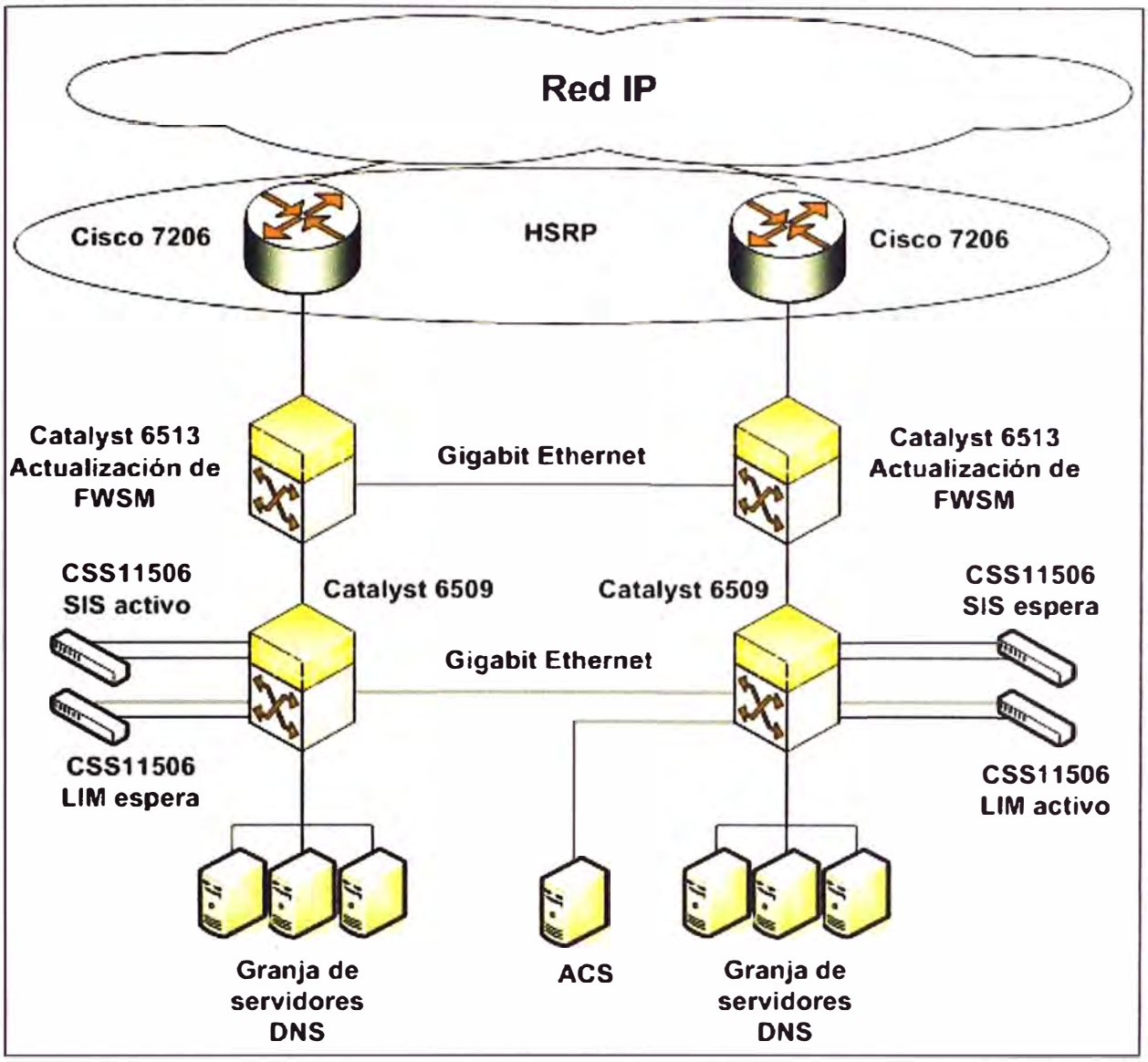

Figura 3.7 Alternativa 1 (Fuente: Elaboración propia)

a.1 Balanceador de carga (CSS11506)

Para mitigar el corte de servicio de uno de los DNS es necesario configurar en una de las ramificaciones un segundo balanceador que tenga el rol de espera, de manera que se vuelva activo si la otra sede deja de enviar paquetes "hola". Este segundo balanceador es configurado físicamente igual al balanceador activo en la sede.

a.2 Switch WS-C6513-E

Para evitar que el enlace entre los Switches WS-C6509-E (parte inferior del esquema) sea el único punto de falla, se implementa un enlace de 1Gbps entre los Switches WS-C6513-E (parte superior), de manera que si hay una falla en el enlace que une los dos Switches WS-C6509-E, éste sea reemplazo del otro. Además es necesario mencionar que este nuevo enlace debe estar configurado en modo troncal.

a.3 Router Cisco 7206VXR

Para evitar la configuración manual de las rutas del DNS de la otra ramificación, se

configura un protocolo de alta disponibilidad de capa 3 entre los Routers, el HSRP (como referencia véase la sección 2.2.4).

a.5 Administración de equipos

Se coloca un servidor de control de acceso a la red debido a que no se tenía control de los usuarios que administran los equipos de comunicaciones, es decir no se sabe quién ha ingresado a un equipo determinado, tampoco qué ha hecho durante un lapso de tiempo y qué actividades realizó. Este servidor le da un valor agregado a la seguridad de acceso, ya que los usuarios de administración están centralizados en un solo servidor de red, de manera que al existir un ataque directo a un equipo de comunicación crítico, éste no se verá afectado porque el usuario y contraseña están alojados en este servidor.

b. Alternativa 2

Una segunda alternativa es mostrada en la Figura 3.8. Se mantienen las mejoras de la alternativa 2, pero se implementa la agregación de enlaces configurando el protocolo LACP, y además se añade un segundo ACS que reside en la otra sede.

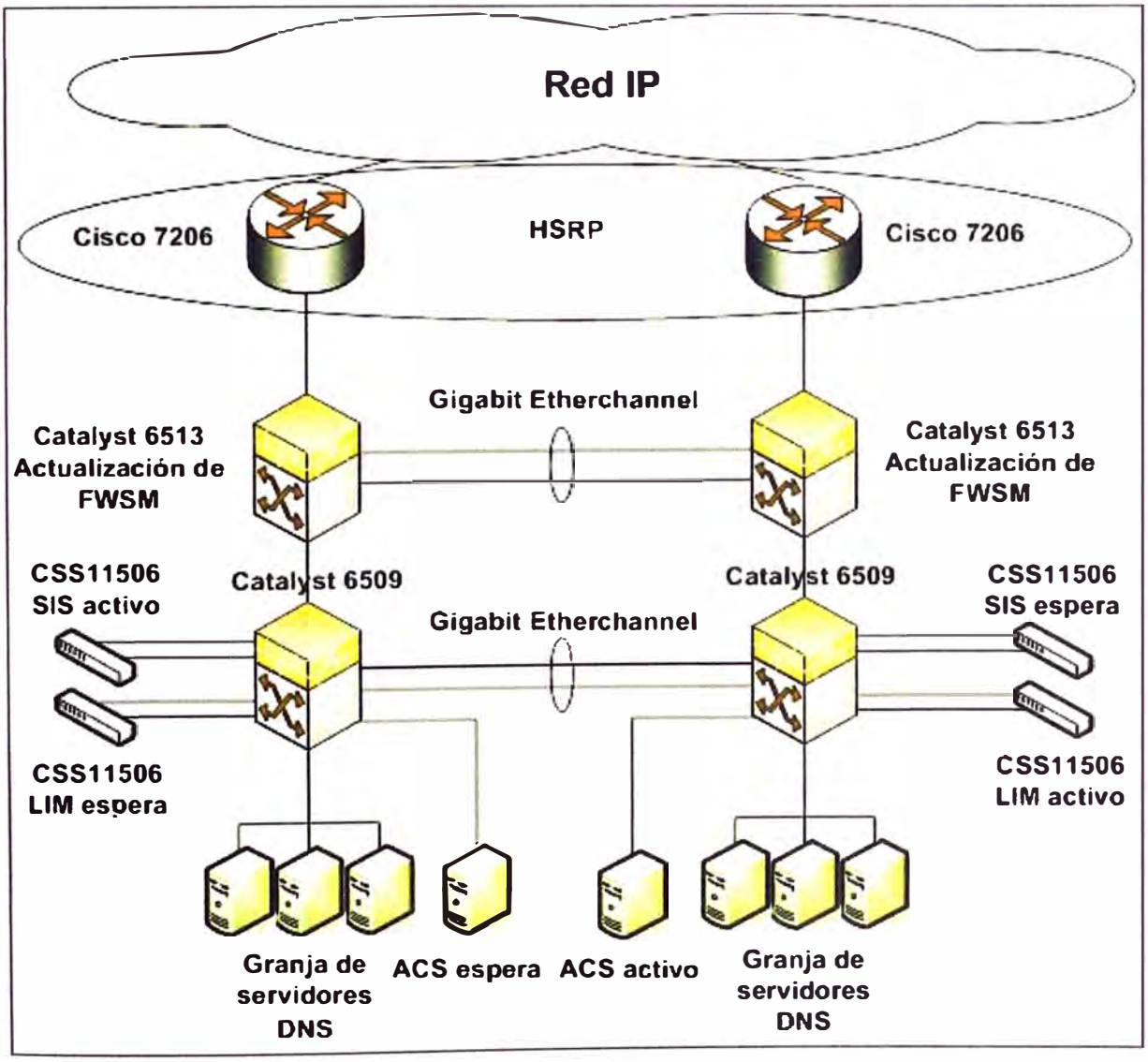

Figura 3.8 Alternativa 2 (Fuente: Elaboración propia)

b.1 Mejora de enlace entre Sedes

Para dar mayor disponibilidad al centro de servicio se, implementa en cada Switch el protocolo LACP. Dos puertos físicos representan a un solo enlace lógico (referencia sección 2.2.3).

LACP utiliza dos puertos de 1Gbps, lo cual aumenta de 1Gbps a 2Gbps la tasa de transferencia (bit rate). La implementación de LACP en cada ramificación está en modo troncal, es decir, todas las VLAN son enviadas a través de los enlaces.

b.2 Administración de equipos

Esta solución ofrece alta disponibilidad de servidores de control de acceso a la red, siendo una de las ventajas la sincronización de la base de datos de los ACS y balancear las peticiones de autenticación, autorización, conteo y auditoria.

c. Alternativa 3

En esta alternativa se reemplaza los balanceadores de carga en cada sede por un módulo ACE por ramificación (ver 2.2.7) y se implementa LACP entre los Switches de una misma ramificación. La Figura 3.9 muestra esta topología.

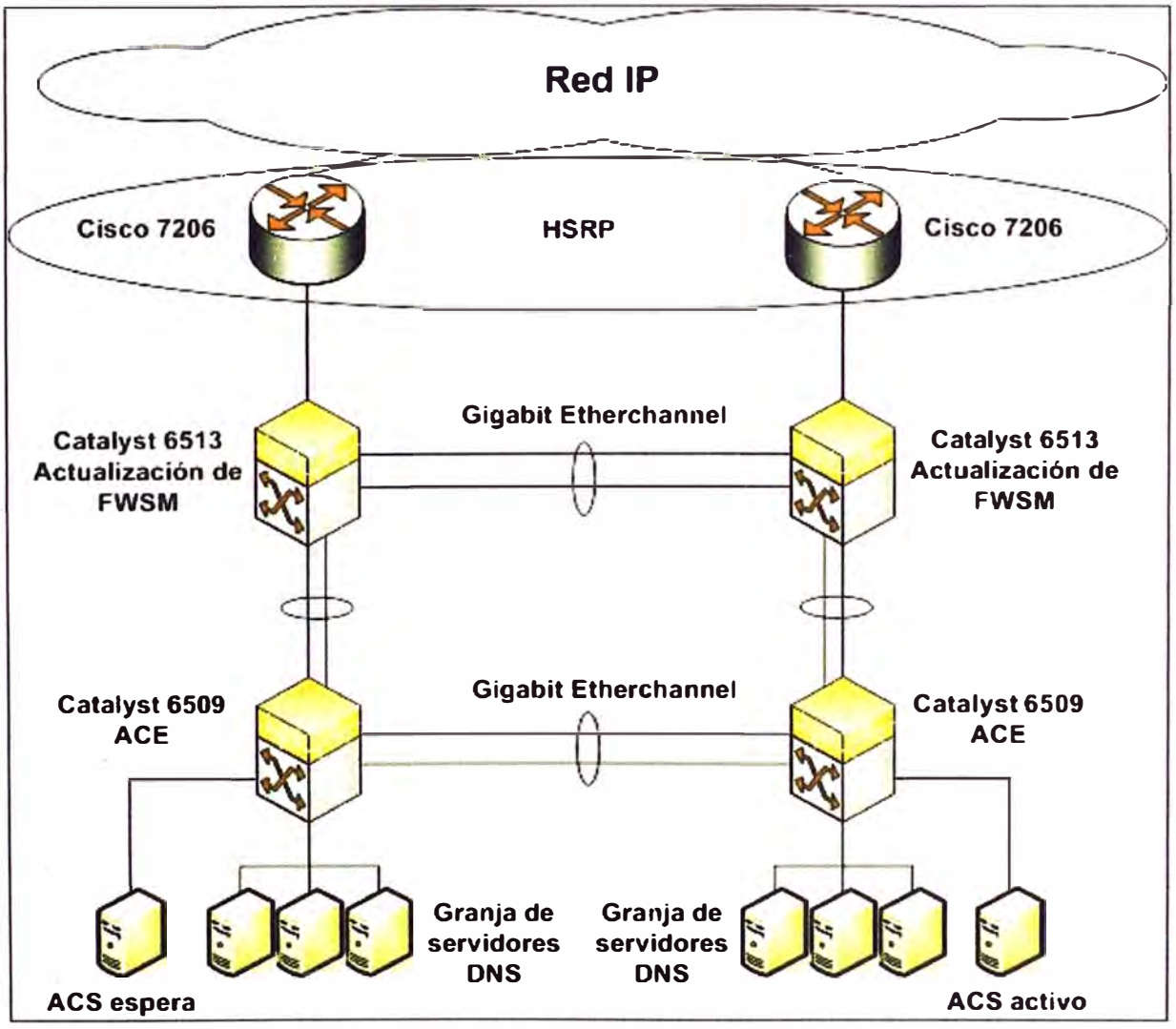

Figura 3.9 Alternativa 3 (Fuente: Elaboración propia)

c.1 ACE (Application Control Engine)

La mejora que añade el ACE es la división lógica de un dispositivo físico en dos (un ACE virtual para San Isidro y otro para Lima), de manera que en las dos ramificaciones se tiene un esquema activo/activo; uno activo de una sede y el otro en espera y viceversa. Otra mejora que ofrece el ACE es la inspección del protocolo DNS e ICMP (ver sección 2.3.6).

c.2 LACP entre Switch WS-C6509-E y WS-C6513-E

La implementación del protocolo LACP entre los Switches en la misma ramificación mejora la disponibilidad y aumenta la tasa de transferencia entre el módulo ACE y el módulo de firewall, de manera que no representa un cuello de botella el enlace conformado por dos enlaces físicos.

3.1.3 Comparación de alternativas

Como se indicó en la sección 2.4.4, para el análisis comparativo de la disponibilidad de varias topologías, se debe considerar la totalidad de los elementos que se incluyen en el sistema más robusto (o que contiene más componentes). La Figura 3.10 muestra el esquema de la alternativa 3 en la cual se indica las disponibilidades individuales.

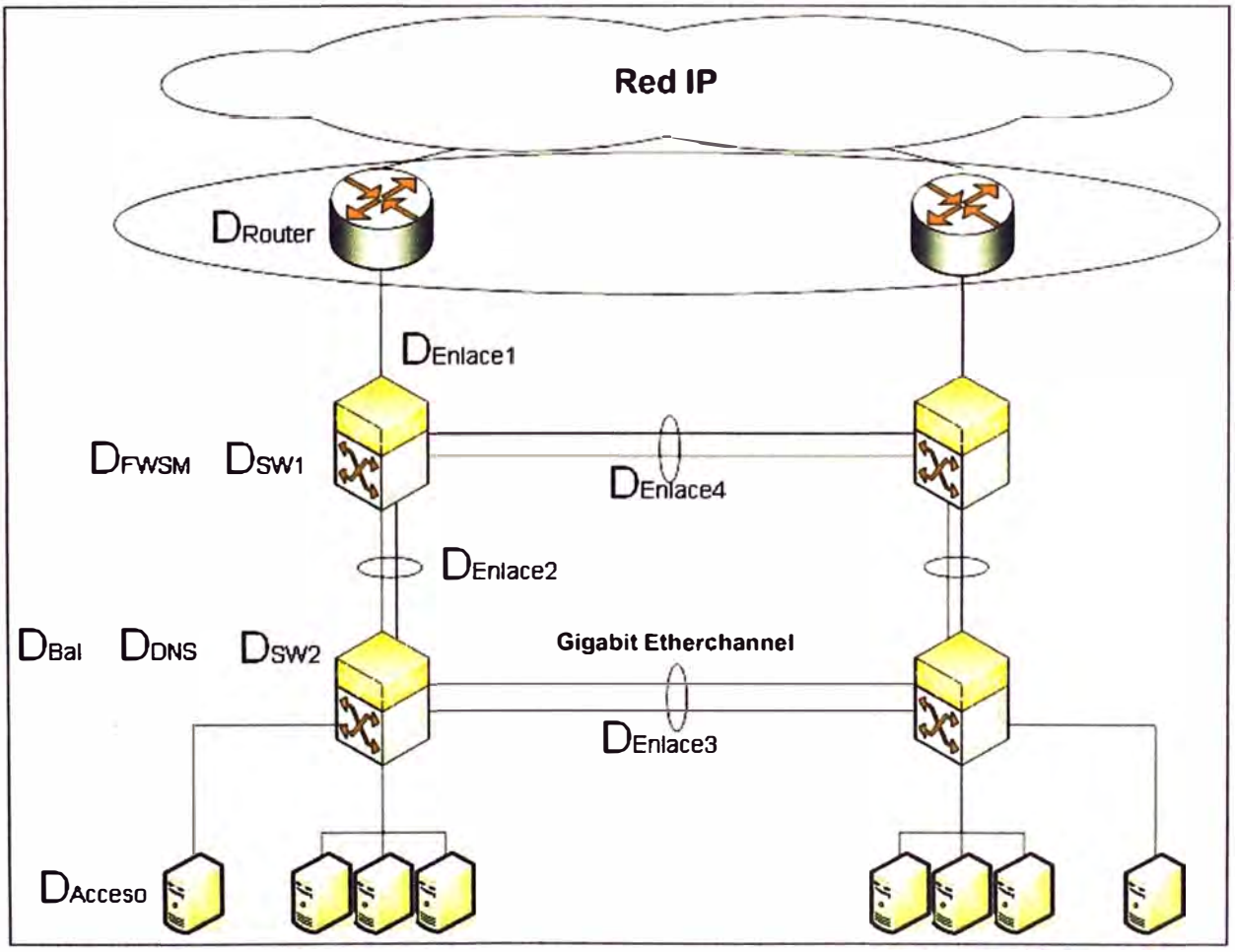

Figura 3.10 Variables de disponibilidad (Topología alternativa 3)

La disponibilidad a nivel de equipos (Drouter, Dsw1, Dsw2) no cambia para ninguna

de las alternativas, tampoco la del enlace 1, por lo que en el análisis comparativo podrían no considerarse. Sin embargo, si deben considerarse en el análisis las demás variables, incluso en las que no existían estos componentes. La Figura 3.11 muestra a las mismas variables para la situación inicial; en rojo (y subrayado) se presentan a las que no existían en dicha topología.

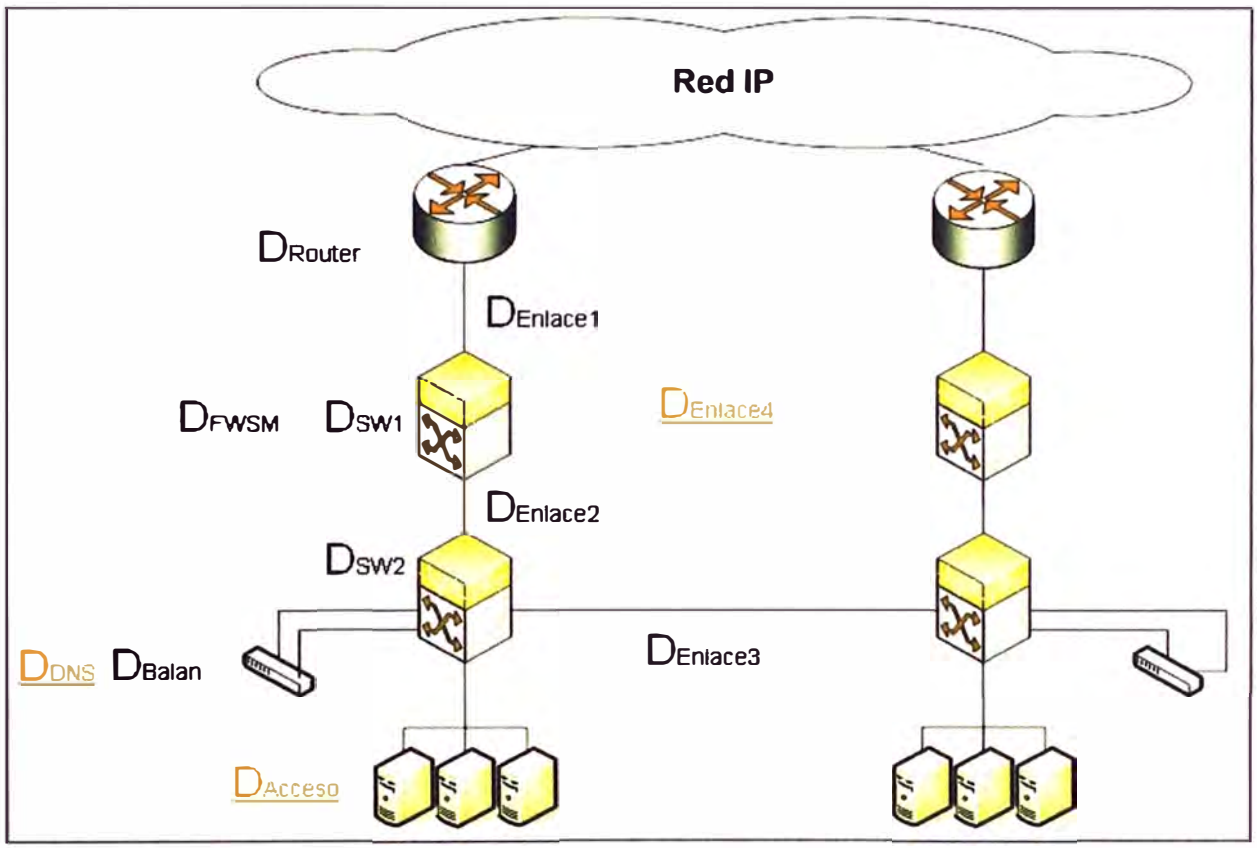

Figura 3.11 Variables de disponibilidad para situación inicial

En esta sección, de manera similar a la presentación de la solución inicial y de las alternativas, se analiza a nivel de disponibilidad las mejoras para cada variable (componente) considerada. (Ver anexo A).

a. Disponibilidad de Firewall

La variable es DFWSM. Se analizan los cuatro casos:

a.1 Situación inicial

En la situación inicial la disponibilidad (DFWSM) es menor que 1 debido a que si falla alguno de los firewall. Se procede manualmente a configurar todas las políticas de filtrado de paquete DNS.

a.2 Primera, segunda y tercera alternativa

En estas alternativas la disponibilidad (DFWSM) es considerada igual a uno por existir redundancia, ya que se ha actualizado y virtualizado el firewall de cada sede. Permitiendo la conmutación automática en caso que algún firewall falle, por lo que se mitiga el tiempo de interrupción de operación del sistema.

b. Disponibilidad del balanceador

La variable es D_{BAL}. Se analizan los cuatro casos:

b.1 Situación inicial

En la situación inicial la disponibilidad (D_{BAL}) es menor que 1 porque ante una falla en el balanceador de cualquier sede se pierde el servicio.

b.2 Primera y Segunda alternativa

En estas alternativas la disponibilidad (D_{BAL}) es considerada igual o superior a la anterior porque existe redundancia activo/espera, es decir ante la falla del balanceador activo de una de las sedes, entra a reemplazarlo el balanceador en espera de la otra sede, mitigándose así la pérdida del servicio DNS.

b.3 Tercera alternativa

En esta alternativa, la disponibilidad del balanceador (D_{BAL}) es considerado superior a la anterior, porque en vez de usar dispositivos físicos, se reemplaza por un solo dispositivo (módulo ACE) que virtualiza los balanceadores de ambas sedes, permitiendo alta disponibilidad activo/activo. El módulo ACE trae como ventaja adicional la posibilidad de mitigar los ataques por denegación de servicio. Esto se trata en el siguiente ítem.

c. Disponibilidad de servicio DNS

La variable es D_{DNS}. Se analizan los cuatro casos para la aplicación que mantiene funcional al sistema contra ataques diversos (denegación de servicio, etc.):

c.1 Situación inicial, primera y segunda alternativa

En la situación inicial, además de en la primera y segunda alternativa, la disponibilidad del DNS (D_{DNS}) es mucho menor que 1, porque ante un ataque de denegación de servicio se pierde servicio DNS; es decir no hay protección contra estos ataques y el tiempo de reposición es indeterminado.

c.2 Tercera alternativa

En esta alternativa, la disponibilidad del DNS (D_{DNS}) es considerada casi 1 porque el ACE agrega la funcionalidad de analizar los paquetes en tránsito.

d. Disponibilidad de enlaces

Las variables son $D_{ENLACE2}$, $D_{ENLACE3}$ y $D_{ENLACE4}$. Se analizan los cuatro casos:

d.1 Situación inicial

En la situación inicial las disponibilidades de los enlaces antes mencionados ($D_{ENLACE2}$ y $D_{ENLACE3}$) son menores que 1, ya que si falla alguno de los enlaces antes mencionados, se pierde el servicio DNS. Cabe mencionar que el enlace 3 tiene el riesgo de saturación. El enlace 4 no existe (no está disponible).

d.2 Primera alternativa

En esta alternativa las disponibilidades ($D_{ENLACE2}$, $D_{ENLACE3}$ y $D_{ENLACE4}$) son menores

que 1 debido a que no existe redundancia de ellas.

d.3 Segunda alternativa

En esta alternativa las disponibilidades ($D_{ENLACE3}$ y $D_{ENLACE4}$) se consideran cercanos a 1 por que se ha configurado LACP (agregación de enlaces) entre los switches de ambas sedes (WS-C6509E y WS-C6513E), pero la disponibilidad del enlace 2 se mantiene en su valor menor que 1 por no tener redundancia. Esto significa que ante la falla de este enlace se perdería el servicio DNS.

d.4 Tercera alternativa

En esta alternativa se mantiene el esquema del enlace 3 y 4, pero se mejora la disponibilidad del enlace 2 ($D_{ENLACE2}$ redundante). Por lo que se mitiga la pérdida de servicio DNS por la mejora antes mencionada.

e. Disponibilidad de AAA

La variable relacionada al ACS es D_{ACCESO}. Se analizan los cuatro casos:

e.1 Situación inicial

La falta de un control centralizado de la administración de los equipos de comunicación, potencialmente puede provocar una interrupción en la operación de los equipos de comunicación, debido a una mala maniobra en la configuración de alguno de ellos.

Cuando se manipula inadecuadamente la configuración de un dispositivo y no se realiza un control y registro de esto, al ocurrir un problema en la red, la mitigación del problema (reposición del servicio) tarda un mayor tiempo al no saber dónde se han hecho los cambios, qué cambios se han hecho y quién hizo los cambios. De esto se concluye que $D_{Acceso\_0} < 1$.

e.2 Primera alternativa

En esta alternativa, la disponibilidad de AAA (D_{Acceso_1}) es superior a la situación inicial (D_{Acceso_0}), ya que la inclusión de un ACS mejora la administración de los dispositivos de comunicaciones y reduce el tiempo de restauración del servicio ante algún incidente. El valor menor a uno en esta alternativa se debe también a que si este equipo falla, entonces existe el riesgo que ocurra un incidente durante el tiempo de reposición del equipo y se dilate el tiempo de restauración del sistema.

e.3 Segunda y tercera alternativa

En la segunda y tercera alternativa, la disponibilidad de AAA (D_{Acceso}) es redundante (aprox 1) porque se añade un ACS (redundante activo/espera) para mitigar el tiempo de interrupción del proceso de aseguramiento de administración de los dispositivos de red.

En este caso, si un ACS fallara, el que está en espera asume el control de la administración mejorando así la disponibilidad final del sistema.

f. Conclusión del análisis

Durante el análisis se presentaron todas las variables que influyen en la disponibilidad del sistema. Cada variable ha sido analizada, tanto para la topología inicial como para las alternativas presentadas. Los valores de D_{FWSM}, D_{BAL}, D_{DNS}, $D_{ENLACE2}$, $D_{ENLACE3}$, $D_{ENLACE4}$, y D_{ACCESO} para la tercera alternativa son superiores a la situación inicial, así como a las demás alternativas. Según lo mostrado en el anexo A, se concluye que la alternativa 3 es la que brinda la mejor disponibilidad al sistema: $D_{INICIAL} < D_{ALT1} < D_{ALT2} < D_{ALT3}$ (98.2336298 % < 99.1009488 % < 99.1128786 % < 99.9984552 %). Además, cumple con lo indicado en el anexo G de estándar EIA/TIA-942 [22] (subsección G 2.9.5) y lo indicado por el Uptime Institute [23] para el nivel de disponibilidad Tier IV (99.995% de disponibilidad) [24]. La alternativa 1 y 2 no cumplen con este estándar dentro de los marcos de disponibilidad de Tier I, II, III, y IV de acuerdo al Uptime Institute.

En si la redundancia puede ser extendida a cada elemento del sistema, por ejemplo: grupos electrógenos redundantes, e incluso usar la energía eléctrica de dos proveedores distintos. Otras mejoras de redundancia se mencionarán en las recomendaciones.

3.1.4 Dimensionamiento de la solución propuesta

Luego de evaluada las tres alternativas, se opta por la última, ya que es la que presenta la mejor solución de alta disponibilidad y mejora de seguridad. En resumen, la nueva topología consta de las siguientes mejoras:

a. A nivel de enlaces

Se implementa LACP en los enlaces entre sedes o switches del mismo nivel (entre 6513 y entre 6509). Adicionalmente, se implementa LACP entre los switches de distinto nivel pero de la misma ramificación (sede).

b. A nivel de virtualización

Los Firewalls y balanceadores ACE son virtualizados, permitiendo ahorro de energía y escalabilidad. La virtualización permite también esquemas de alta disponibilidad activo/activo; esto quiere decir que ante la caída de una de las ramificaciones, en un mismo módulo de firewall o ACE se pueden tener instancias de firewall o ACE independientes una de la otra de manera que dan servicio a los dos DNS.

c. A nivel de acceso

Se centraliza en un solo servidor de red la base de datos de los usuarios, para una mejora de seguridad. El ACS permite un registro exhaustivo de la actividad de cada usuario, lo cual es de gran ayuda en las auditorías de seguridad informática.

d. A nivel de routers

Ya no se configura manualmente las rutas del DNS de la otra ramificación, esto es logrado al configurar HSRP como protocolo de alta disponibilidad de capa 3 entre los

Routers.

e. A nivel de flujo DNS

El ACE permite ahora inspeccionar los protocolos de la capa aplicación, de manera que identifica actividad irregular en el flujo de datos hacia los DNS.

f. A nivel de conexiones

La cantidad de conexiones concurrentes en Lima (durante la situación previa a la solución) hacia este servicio es típicamente 100 mil y durante la caída de la otra sede ha llegado hasta un valor de 300 mil conexiones; por otro lado, la cantidad de conexiones concurrentes en San Isidro hacia este servicio es típicamente 80 mil y durante incidentes ha llegado hasta un valor de 180 mil conexiones. El Firewall y el ACE deben ser capaces de manejar este nivel de conexiones con proyección a un futuro crecimiento.

Se debe tener un módulo de FWSM dedicado para este servicio en Lima y San Isidro, en el peor de los casos (caída de uno de los módulos FWSM y ocurrencia de un incidente) un módulo soportaría la carga de este servicio para ambas sedes, llegando en caso de algún incidente hasta 480 mil conexiones concurrentes, dejando una tasa de sobrecarga de hasta 100 % (1 millón de conexiones es el límite de conexiones para el módulo FWSM).

Respecto al ACE, el tipo de módulo seleccionado maneja hasta 4 millones de conexiones concurrentes, para el caso (activo/activo) maneja dos millones de conexiones concurrentes para cada ACE virtual.

3.2 Infraestructura y topología de la solución

La Figura 3.12 muestra la topología de la solución implementada. En ella se agrupan (dentro de líneas punteadas) los módulos correspondientes a cada switch; por ejemplo, para el 6513 está el módulo de Firewall (aparecen los dos virtualizados) y para el 6509 está el módulo ACE.

3.2.1 Descripción de la infraestructura

En adición a lo mencionado en la sección 3.1.3, en esta sección se describe los aspectos más importantes de la configuración de la nueva infraestructura de datos.

a. Routers

Los routers tienen rutas de las redes públicas 200.48.225.128/28 y 200.48.225.144/28 apuntando hacia las direcciones IP activas de cada par de contextos de Firewall respectivamente. ".C" (en mayúscula) representa la dirección IP del Firewall activo en Lima y ".c" (minúscula) representa la dirección IP en San Isidro.

b. FWSM

Los contextos de Firewall de Lima tienen como puerta de enlace predeterminada (default-gateway) la dirección IP virtual del grupo HSRP de Lima.

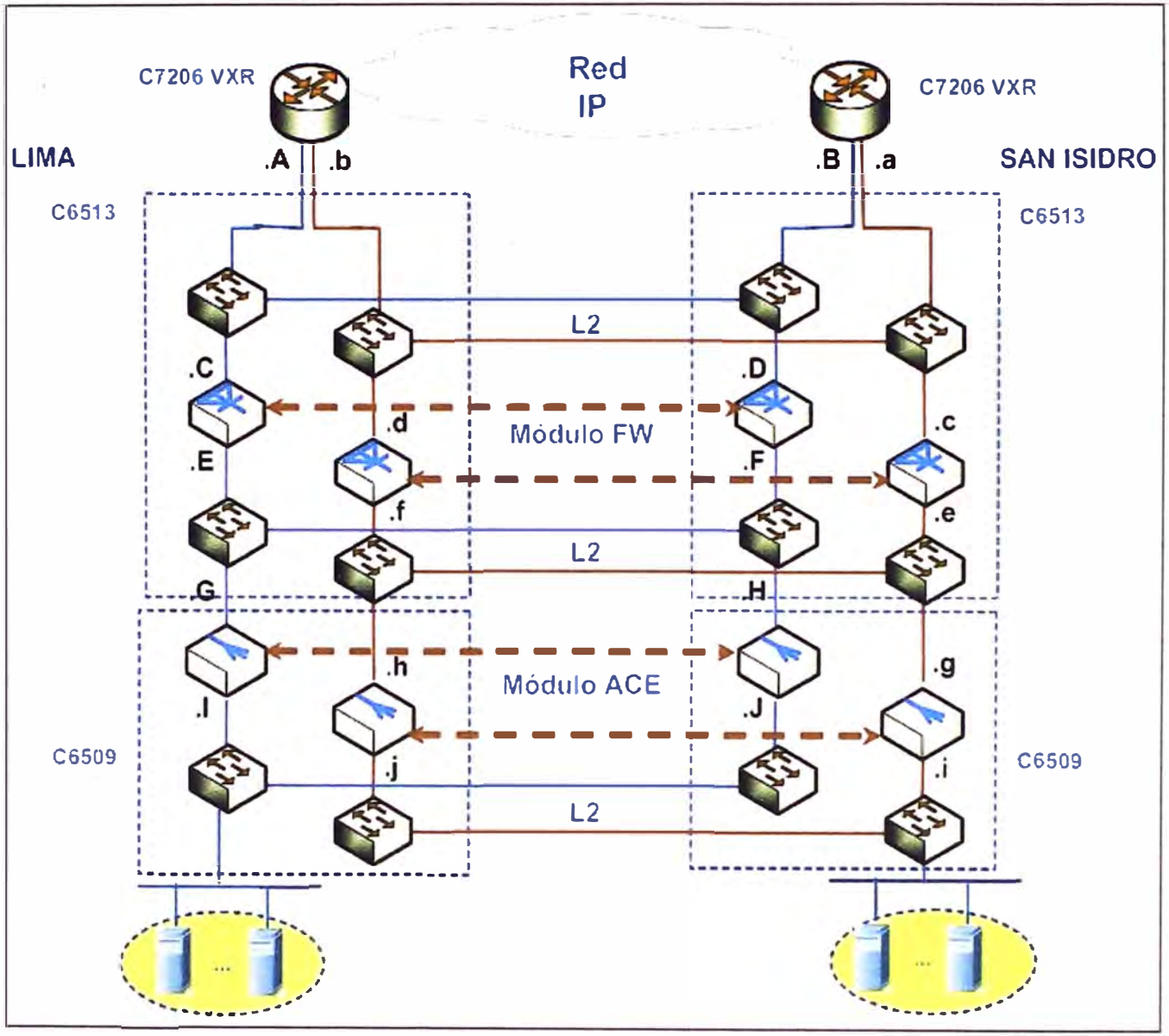

Figura 3.12 Topología de la solución (Fuente: Elaboración propia)

Los contextos de Firewall de San Isidro tienen como puerta de enlace predeterminada la dirección IP virtual del grupo HSRP de San Isidro. Los dos pares de contextos de Firewall para este servicio están alojados en los módulos FWSM, ubicados en la ranura (slot) 5 de los Switches 6513 de Lima y San Isidro.

Los contextos de Firewall de Lima y San Isidro tienen rutas de las redes públicas 200.48.225.128/28 y 200.48.225.144/28, apuntando hacia la IP del FT Group del contexto ACE de Lima y San Isidro respectivamente.

c. ACE

Los contextos ACE de Lima y San Isidro tienen como puerta de enlace predeterminada la dirección IP activa de los contextos Firewall de Lima y San Isidro, respectivamente. (.G en Lima y .g en San Isidro). Los servidores DNS de Lima y San Isidro tendrán como puerta de enlace predeterminada la dirección IP del FT Group del contexto ACE de Lima y San Isidro, respectivamente.

3.2.2 Funcionamiento de la topología

La topología de la solución está preparada para enfrentar los siguientes escenarios asegurando alta disponibilidad:

- Falla en el módulo ACE San Isidro.- Contempla el restablecimiento de los servicios mediante el contexto correspondiente del módulo ACE en Lima.
- Falla en el módulo ACE Lima.- Contempla el restablecimiento de los servicios mediante el contexto correspondiente del módulo ACE en San Isidro.
- Falla en el módulo FWSM San Isidro.- Contempla el restablecimiento de los servicios mediante el contexto correspondiente del módulo FWSM de Lima.
- Falla en el módulo FWSM Lima.- Contempla el restablecimiento de los servicios mediante el contexto correspondiente del módulo FWSM de San Isidro.
- Falla en el Router 7200 San Isidro.- Contempla el restablecimiento de los servicios de routing a través del Router de Lima.
- Falla en el Router 7200 Lima.- Contempla el restablecimiento de los servicios de routing a través del Router de San Isidro.
- Falla del enlace entre Red Núcleo-R7200 / R7200-FWSM / FWSM-ACE.- Contempla el restablecimiento de los servicios por rutas alternativas en la medida de lo posible, también se establecen rutas con doble conectividad (Etherchannel) para tener alta disponibilidad en enlaces críticos para la arquitectura y funcionalidad del diseño.
- Falla de ACS activo.- contempla la falla del servidor de control de acceso activo en una de las sedes. Este comportamiento se replica para la otra sede.

a. Flujo normal

La Figura 3.13 muestra el esquema funcional de la topología en modo normal.

Para el funcionamiento modo normal, ambas sedes del centro de servicio brindan servicio DNS de manera independiente, es decir, cada componente de la solución cumple su función (balanceo, filtrado, y enrutamiento). A continuación se explica una de las ramificaciones, esto debido a la simetría topológica.

Las peticiones DNS son recibidas a través de cada router para luego ser enviadas al Switch WS-C6513-E, que contiene el módulo firewall. Una vez que el firewall filtra todo el tráfico que no es DNS (deja pasar solo tráfico DNS) lo envía a la IP que representa al DNS a través del Switch WS-C6509-E que tiene integrado el módulo ACE. Éste toma la decisión de enviar el tráfico al servidor real según el peso asignado a cada uno.

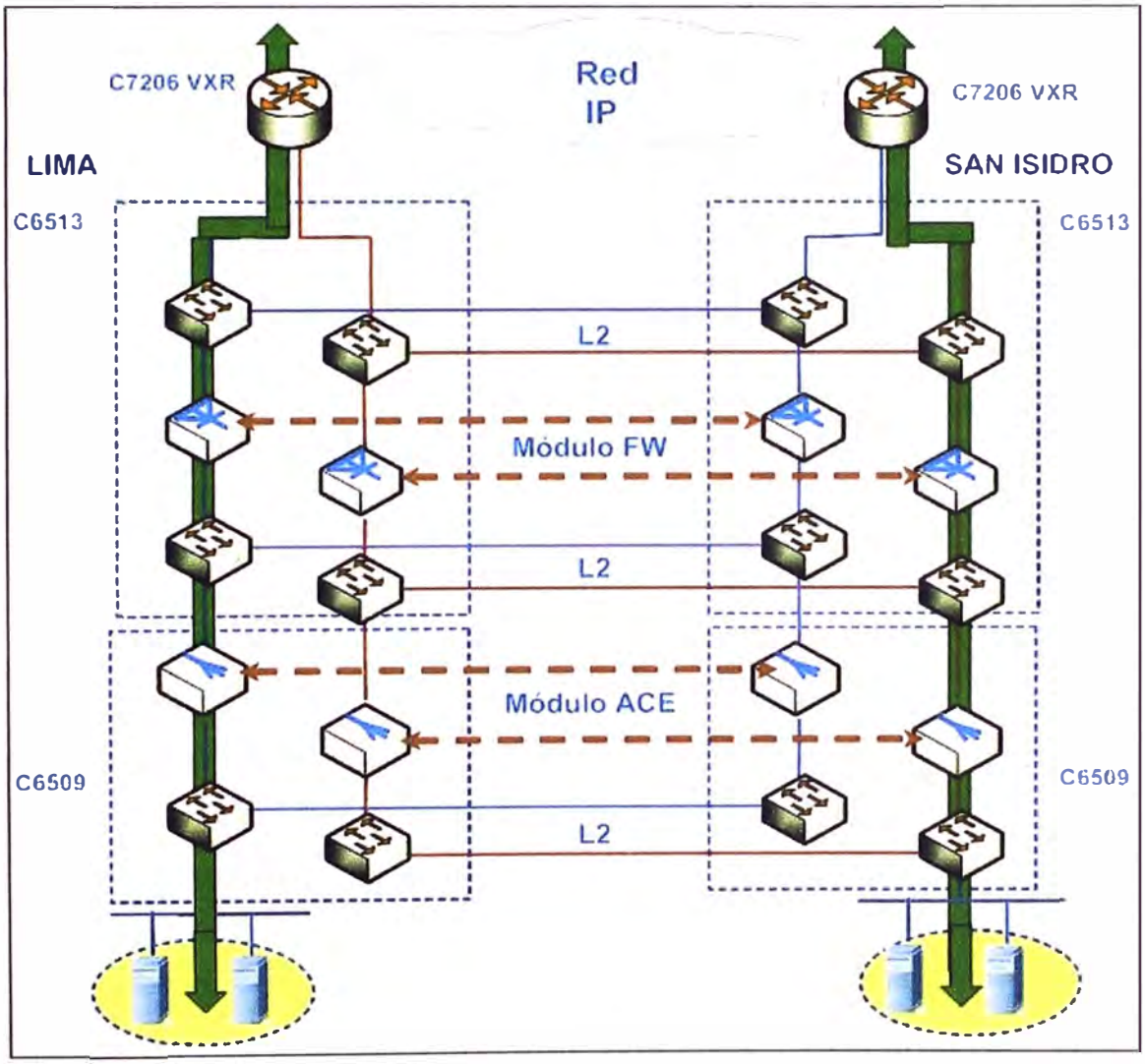

Figura 3.13 Flujo Normal

b. Falla en el módulo ACE San Isidro y de Lima

Las Figuras 3.14 y 3.15 muestran el esquema del funcionamiento de la topología cuando falla el módulo ACE de San Isidro y el de Lima, respectivamente. Sólo se explica lo relacionado a la Falla de la sede de Lima por existir simetría topológica.

Cuando falla el módulo ACE de la sede de Lima (marcado con aspa), el flujo de tráfico (de los servidores hacia el router) es reenviado automáticamente a través del enlace

Etherchannel (ver línea en azul) entre los Switches WS-C6509-E de las sedes; el contexto de la sede Lima en espera (situado en San Isidro) del módulo ACE del Switch WS-C6509-E asume todo el balanceo de carga de los servidores ubicados en Lima, luego de realizado el balanceo, el tráfico es enviado al Switch WS-C6513-E de la sede San Isidro para luego regresarlo a la sede Lima para que el módulo firewall filtre el tráfico DNS.

Luego de esta corrección el flujo de tráfico sigue con el comportamiento autónomo que se tenía en la situación normal (hacia el router).

c. Falla en el módulo FWSM San Isidro y Lima

Las Figuras 3.16 y 3.17 muestran el esquema del funcionamiento de la topología cuando falla el módulo FWSM de San Isidro y de Lima, respectivamente. Sólo se explica lo relacionado a la falla de la sede de Lima por existir simetría topológica.

Ante la caída del módulo firewall de la sede Lima, el contexto en espera de la sede Lima (situado en San Isidro) toma el control del filtrado de trafico DNS de la sede Lima. Esto se hace mediante el envío de trafico desde el Switch WS-C6513-E de Lima al de San Isidro vía enlace Etherchannel (ver línea en azul); luego de que este contexto filtra el trafico DNS, lo regresa nuevamente al Switch WS-C6513-E de la sede Lima para continuar el flujo del funcionamiento normal de las sedes (hacia el router).

d. Falla en el Router 7200 San Isidro y Lima

La Figura 3.18 y 3.19 muestra el esquema del funcionamiento de la topología cuando falla el router 7200 de San Isidro y de Lima, respectivamente. Sólo se explica lo relacionado a la falla de la sede de Lima por existir simetría topológica.

Ante la falla del Router Lima el trafico saliente del módulo firewall se envía al Switch WS-C6513-E San Isidro (vía Etherchannel) para que este lo reenvíe al Router San Isidro y pueda responder satisfactoriamente al requerimiento DNS de los clientes (línea azul).

e. Falla del enlace entre FWSM-ACE / R7200-FWSM

Los ítems anteriores explicaban la manera de dar alta disponibilidad al sistema en caso que fallen los dispositivos de comunicaciones y/o módulos. Estos hacían uso de los módulos o contextos disponibles existentes en la otra sede, y mediante un enlace Etherchannel se redirigía el flujo para asegurar la continuidad del servicio. De la misma manera que se hizo con los dispositivos de comunicaciones ante una falla, se resuelven las fallas de los enlaces respectivos.

Para ilustrar este comportamiento, se explican la falla del enlace entre los Switches WS-C6509-E y WS-C6513-E de la misma sede (representado por FWSM-ACE), cuyo procedimiento de contingencia equivale a la falla del módulo ACE de la sede Lima, lo cual fue explicado en el ítem b de esta sección. Por otro lado, la falla del enlace entre el router

y el módulo firewall (representado por R7200-FWSM) equivale a la falla del módulo FWSM descrito en el ítem c de esta sección.

- **Falla del enlace entre los Switches WS-C6509-E y WS-C6513-E de la misma sede**.- Las Figuras 3.20 y 3.21 muestran el esquema del funcionamiento de la topología cuando falla el enlace FWSM-ACE. Sólo se explica lo referente a la sede Lima por existir simetría topológica. El tráfico es enviado a través del enlace Etherchannel entre los Switches WS-C6509-E de las sedes Lima y San Isidro. Después de ser balanceado por el módulo ACE de la sede San Isidro, esto se hace de manera que este mismo trafico se reenvía nuevamente desde el Switch WS-C6513-E de San Isidro al de Lima y luego lo filtra el módulo firewall de la sede Lima para comportarse como si las sedes estuvieran separadas independientemente.

- **Falla del enlace entre el Switch WS-C6513-E y el router de la misma sede**.- Las Figura 3.22 y 3.23 muestran el esquema del funcionamiento de la topología cuando falla el enlace R7200-FWSM. Sólo se explica lo referente a la sede Lima por existir simetría topológica. Ante la caída del módulo firewall de la sede Lima, el contexto en espera de la sede Lima toma el control del filtrado de trafico DNS de la sede Lima. Esto se hace mediante el envío de trafico desde el Switch WS-C6513-E de Lima al de San Isidro vía enlace Etherchannel; luego de que este contexto filtra el trafico DNS, lo regresa nuevamente al Switch WS-C6513-E de la sede Lima para continuar el flujo del funcionamiento normal de las sedes.

f. Falla de ACS activo

La Figura 3.24 muestra el esquema del funcionamiento del ACS en modo normal, mientras que la Figura 3.25 cuando falla el ACS activo. Ante una falla del ACS activo, la base de datos del ACS activa es replicada o sincronizada con el ACS de3 espera que se tiene en la otra sede, de manera que en la configuración de los equipos de comunicación se tiene configurado los dos ACS. De esta manera, la caída de uno de los ACS no afecta la seguridad en el acceso a estos dispositivos.

3.2.3 Configuración

Los dispositivos de comunicaciones (y sus módulos respectivos) son configurados mediante lo que se conoce como plantilla de configuración. La plantilla de configuración es un documento de texto que contienen todos los comandos que normalmente se ingresan al dispositivo mediante una CLI (Command Line Interface) o línea de comandos.

Los comentarios empiezan con "!". Estos ayudan al personal al entendimiento de la programación realizada. Las plantillas son extensas y además contienen información confidencial, por ello se omitirá su inclusión en el informe de suficiencia. Sin embargo en esta sección se describe la configuración para cada dispositivo de manera resumida.

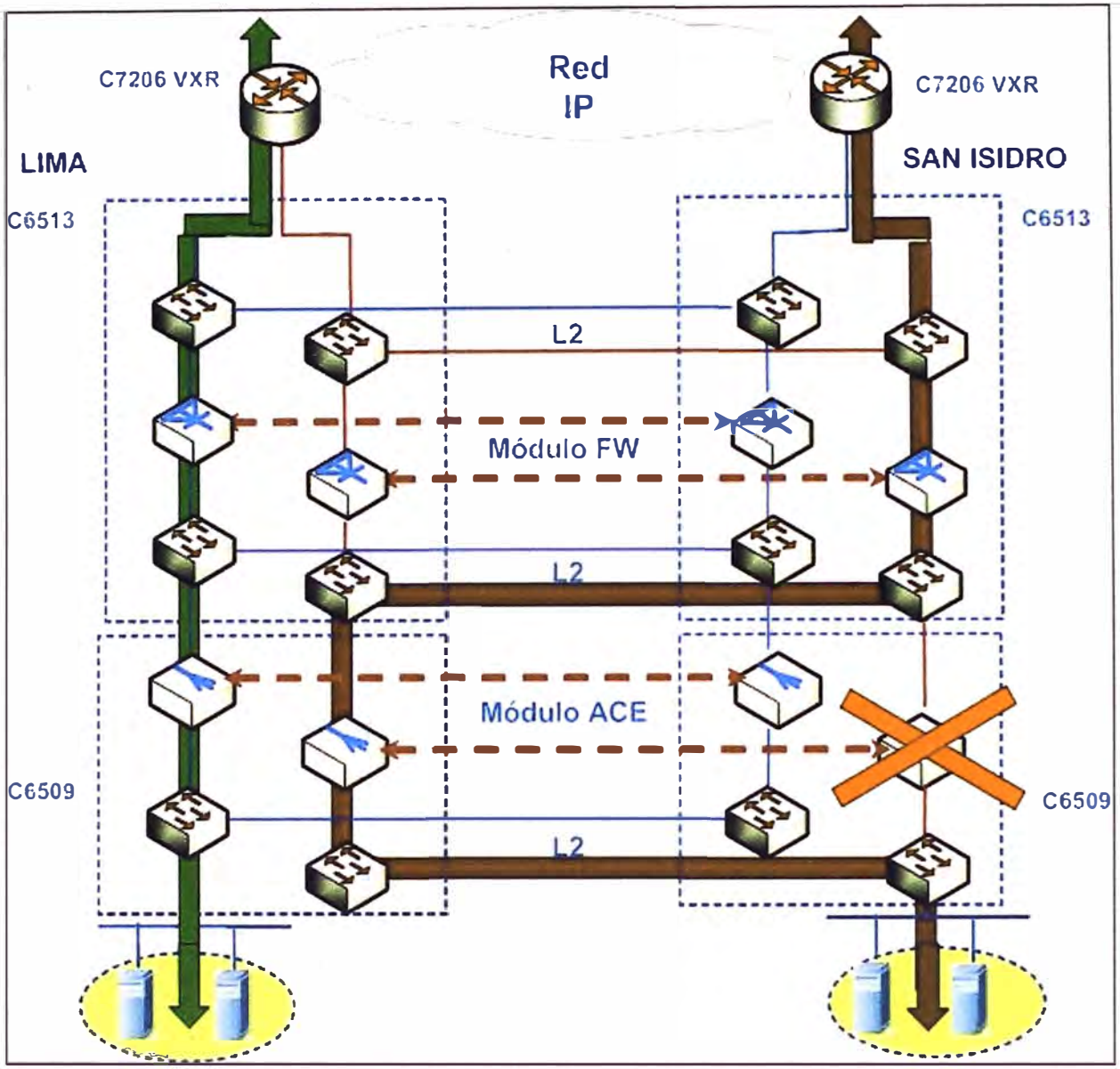

Figura 3.14 Falla en el módulo ACE San Isidro (Fuente: Elaboración propia)

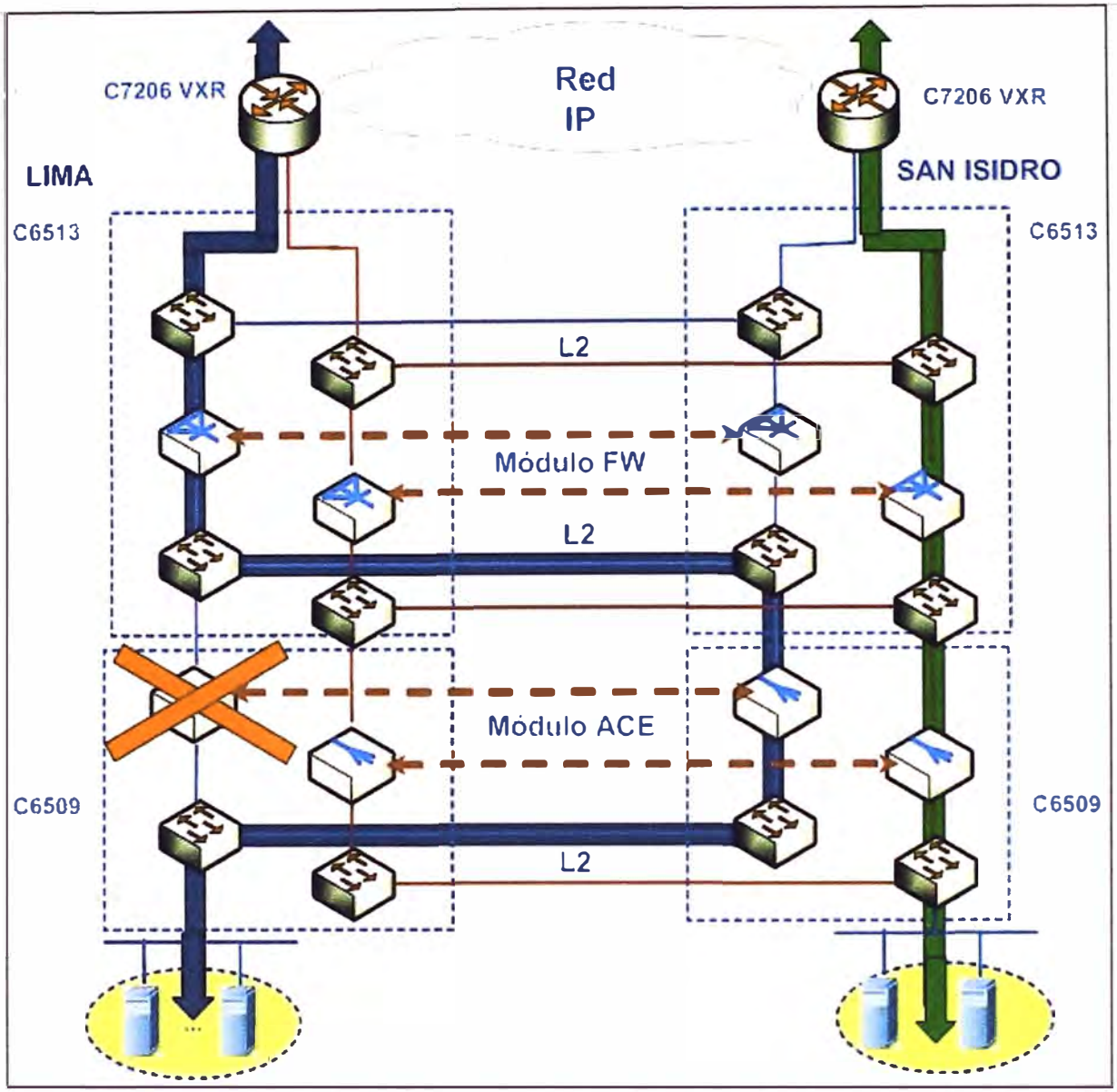

Figura 3.15 Falla en el módulo ACE Lima (Fuente: Elaboración propia)

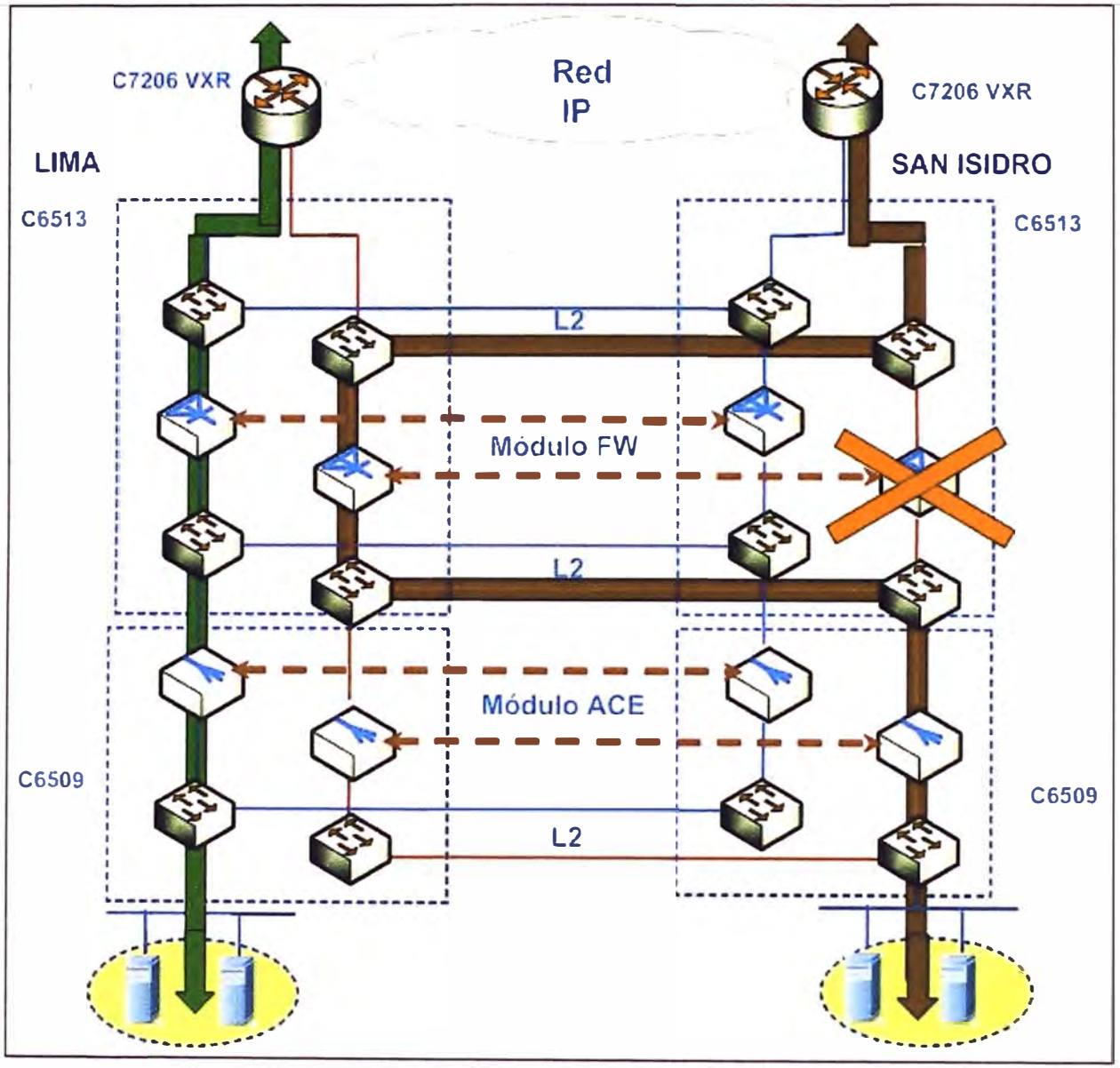

Figura 3.16 Falla en el módulo FWSM San Isidro (Fuente: Elaboración propia)

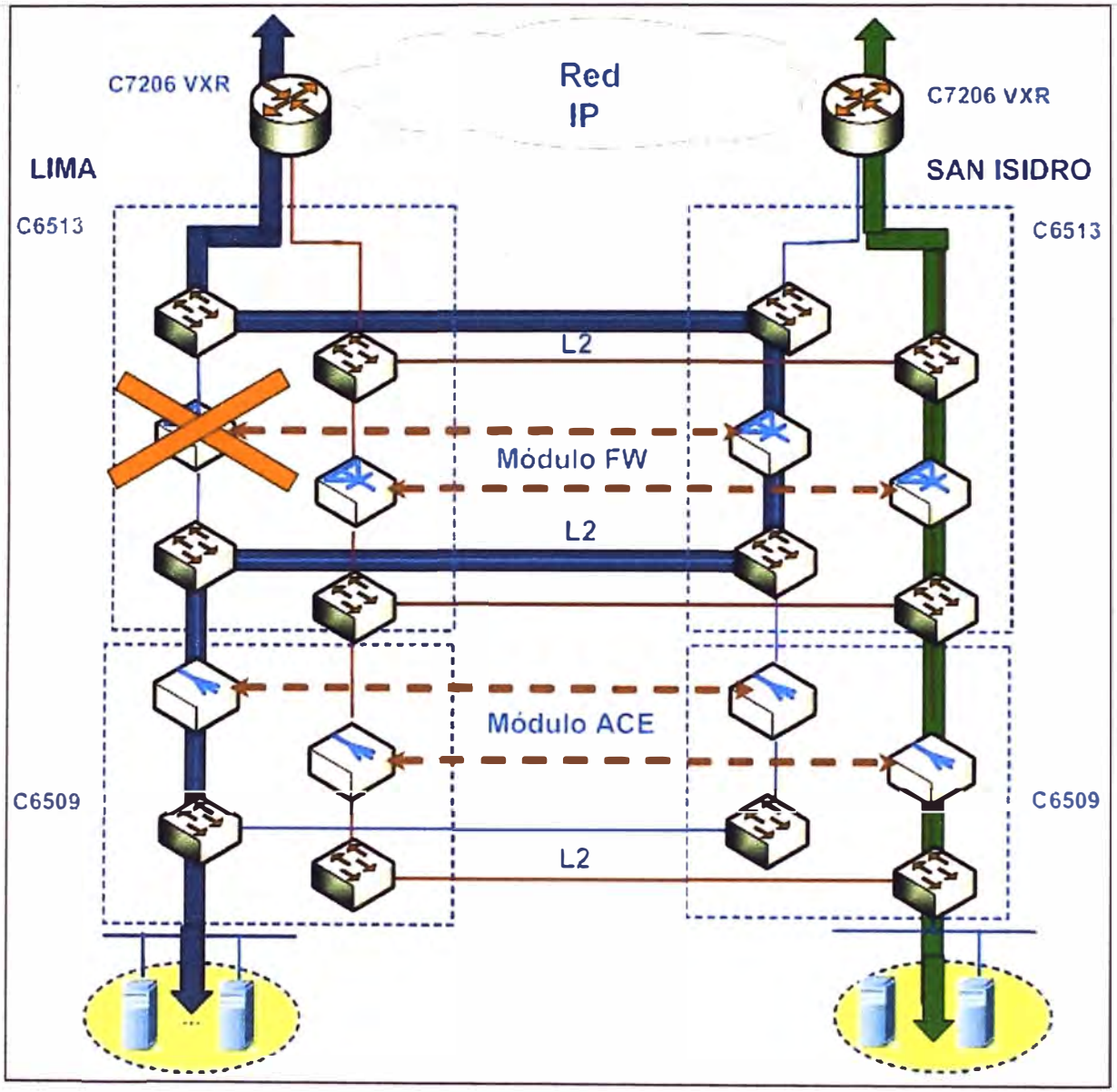

Figura 3.17 Falla en el módulo FWSM Lima (Fuente: Elaboración propia)

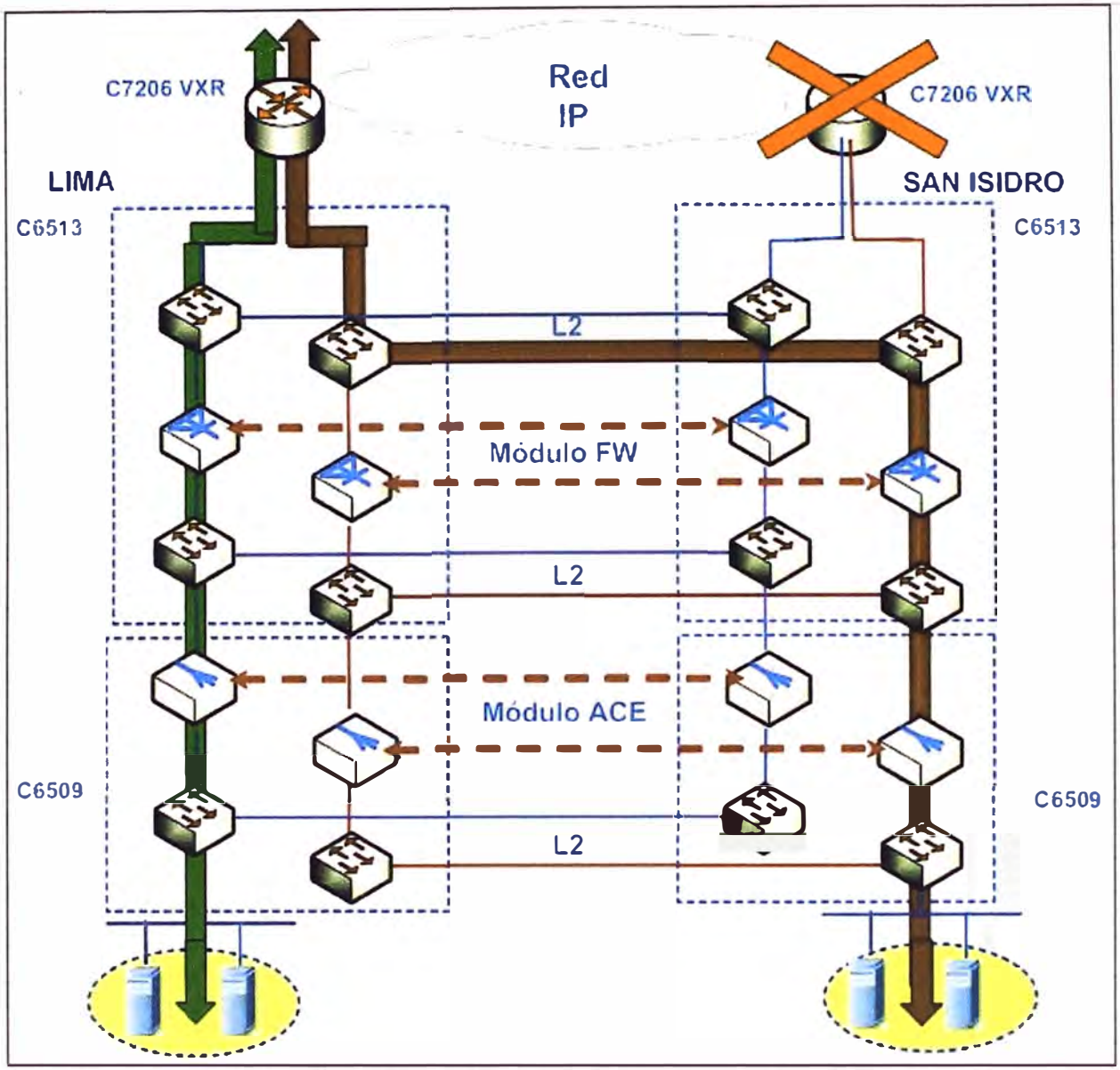

Figura 3.18 Falla en el Router 7200 San Isidro (Fuente: Elaboración propia)

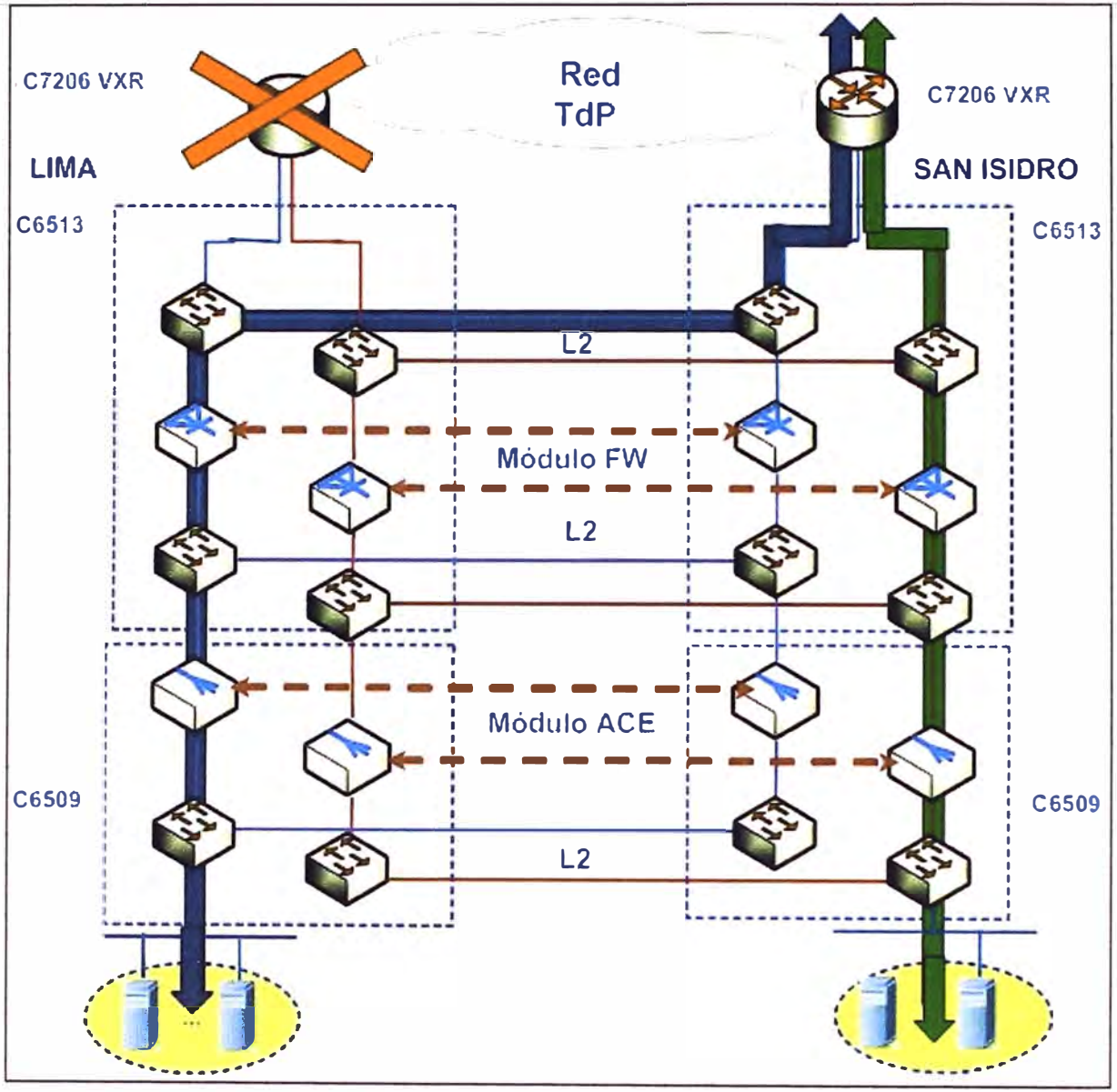

Figura 3.19 Falla en el Router 7200 Lima (Fuente: Elaboración propia)

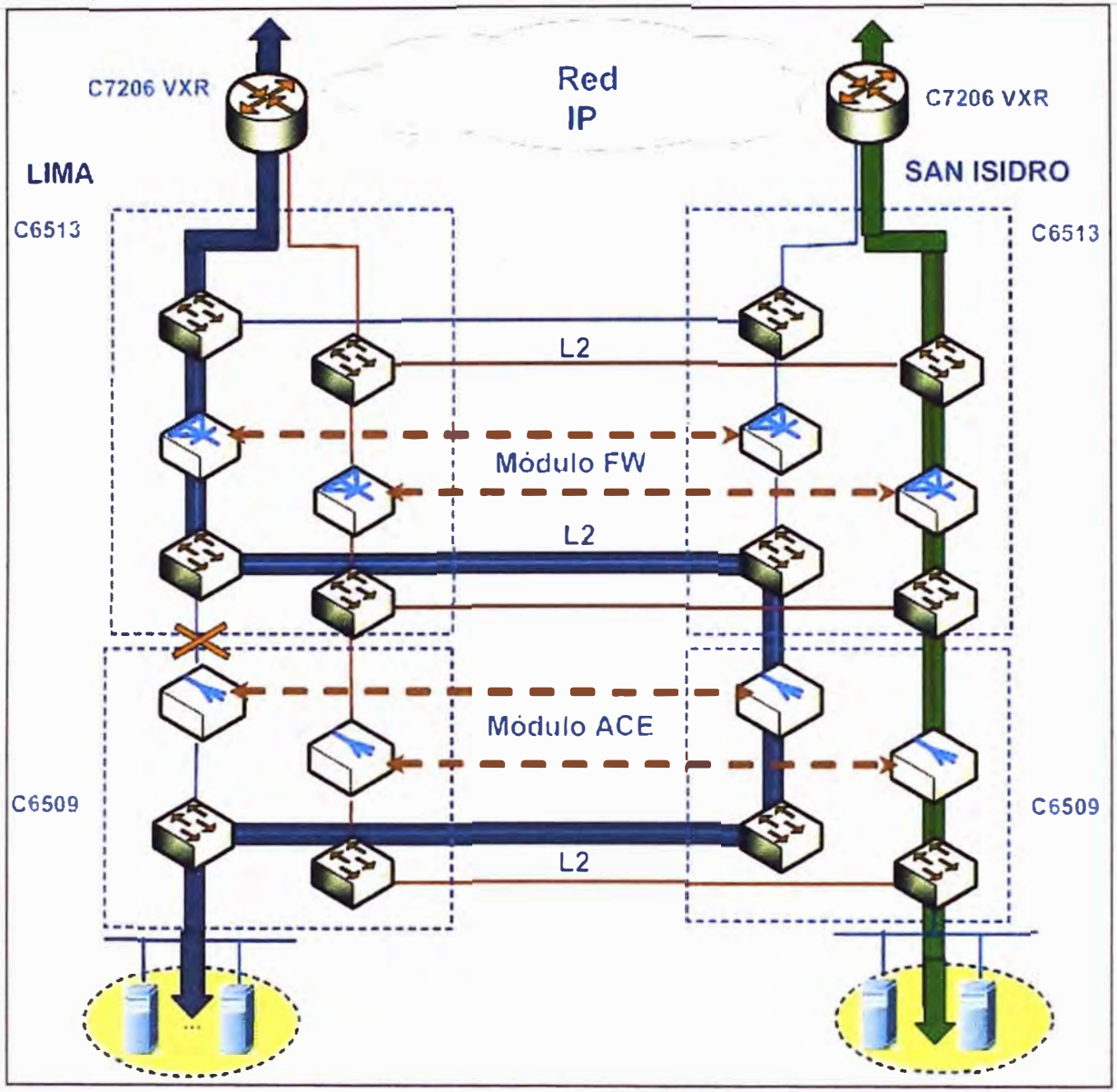

Figura 3.20 Falla del enlace entre FWSM-ACE Lima (Fuente: Elaboración propia)

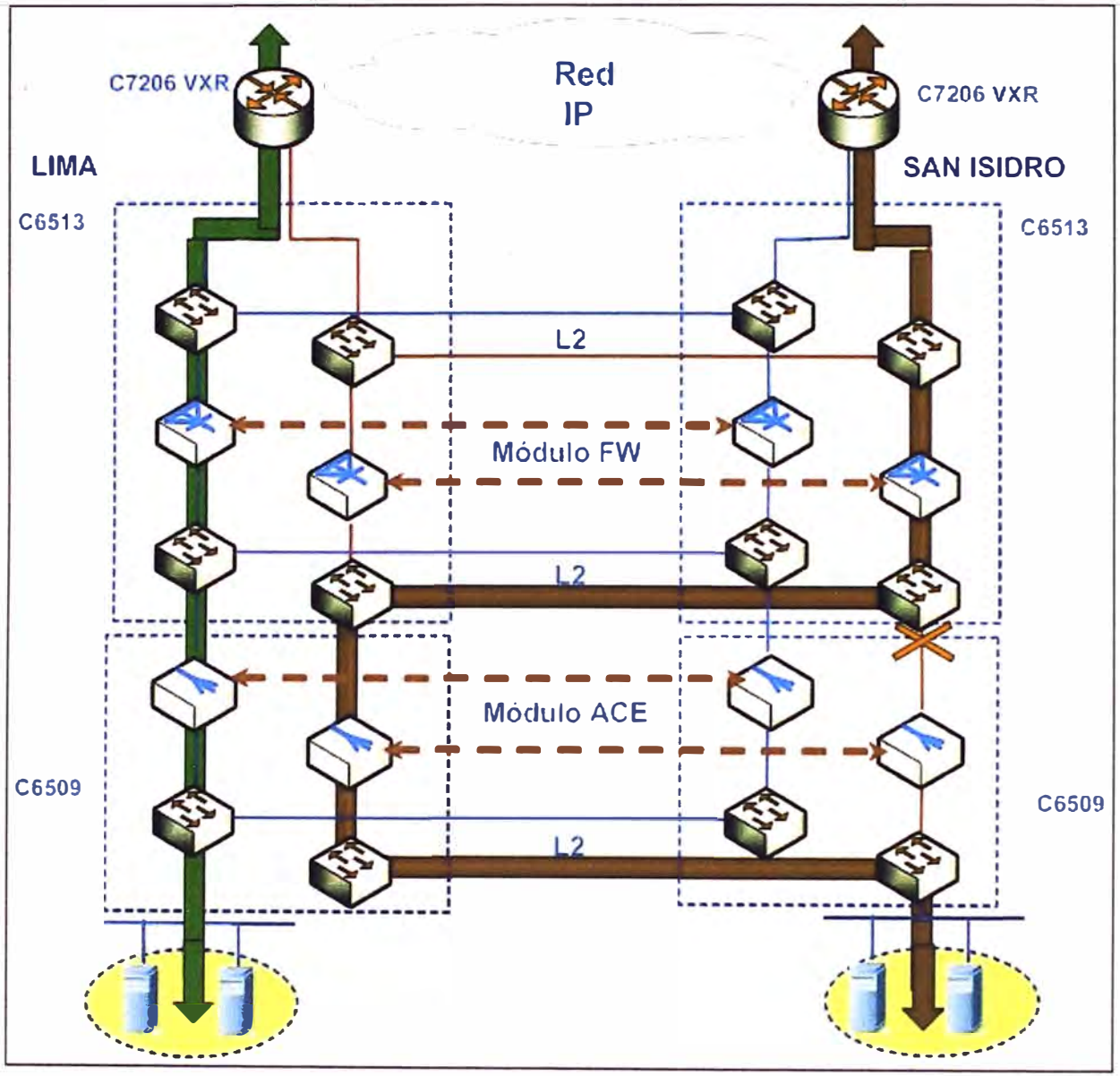

Figura 3.21 Falla del enlace FWSM-ACE San Isidro (Fuente: Elaboración propia)

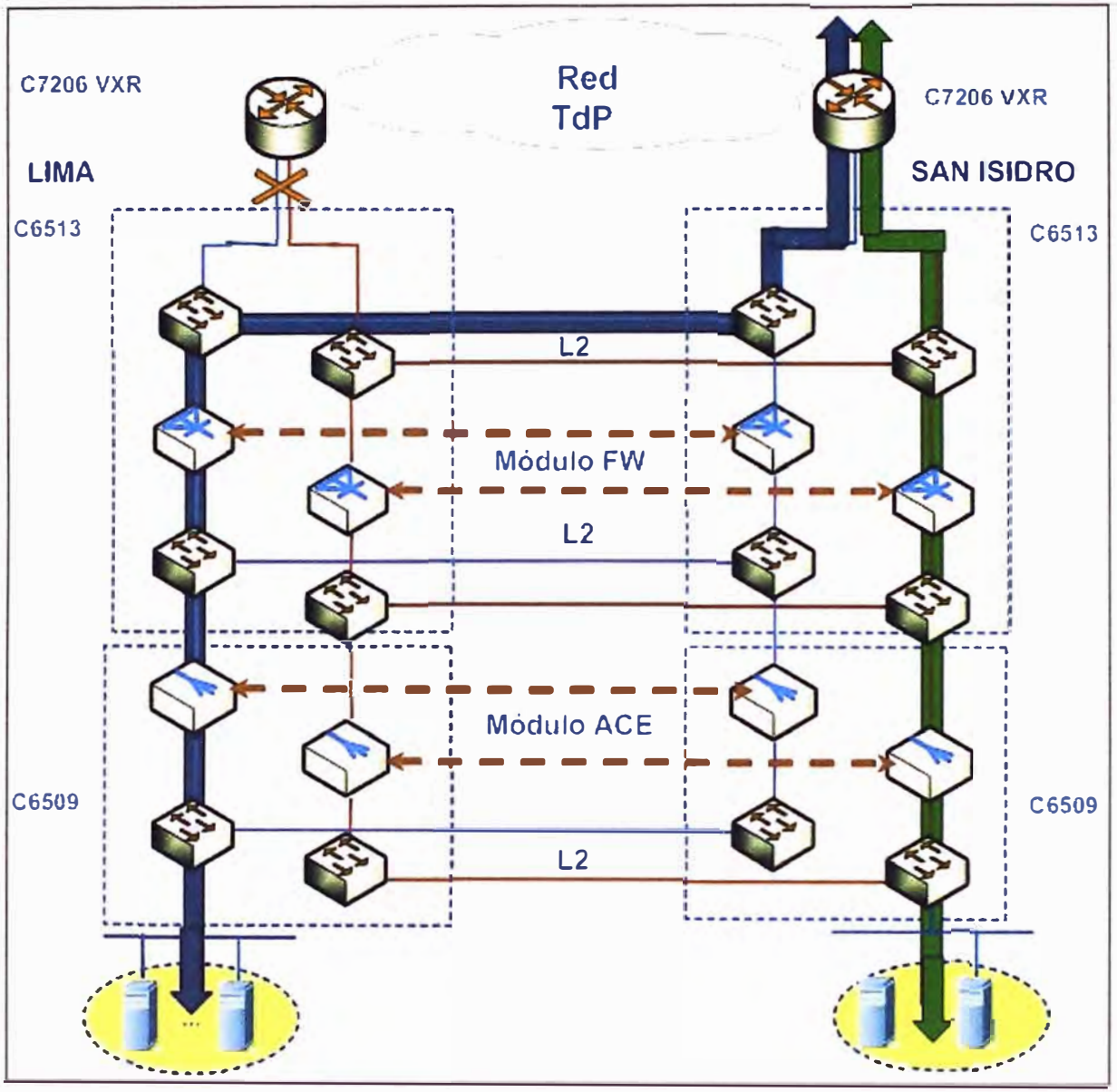

Figura 3.22 Falla del enlace entre el Switch WS-C6513-E y el router de la misma sede (Lima) (Fuente: Elaboración propia)

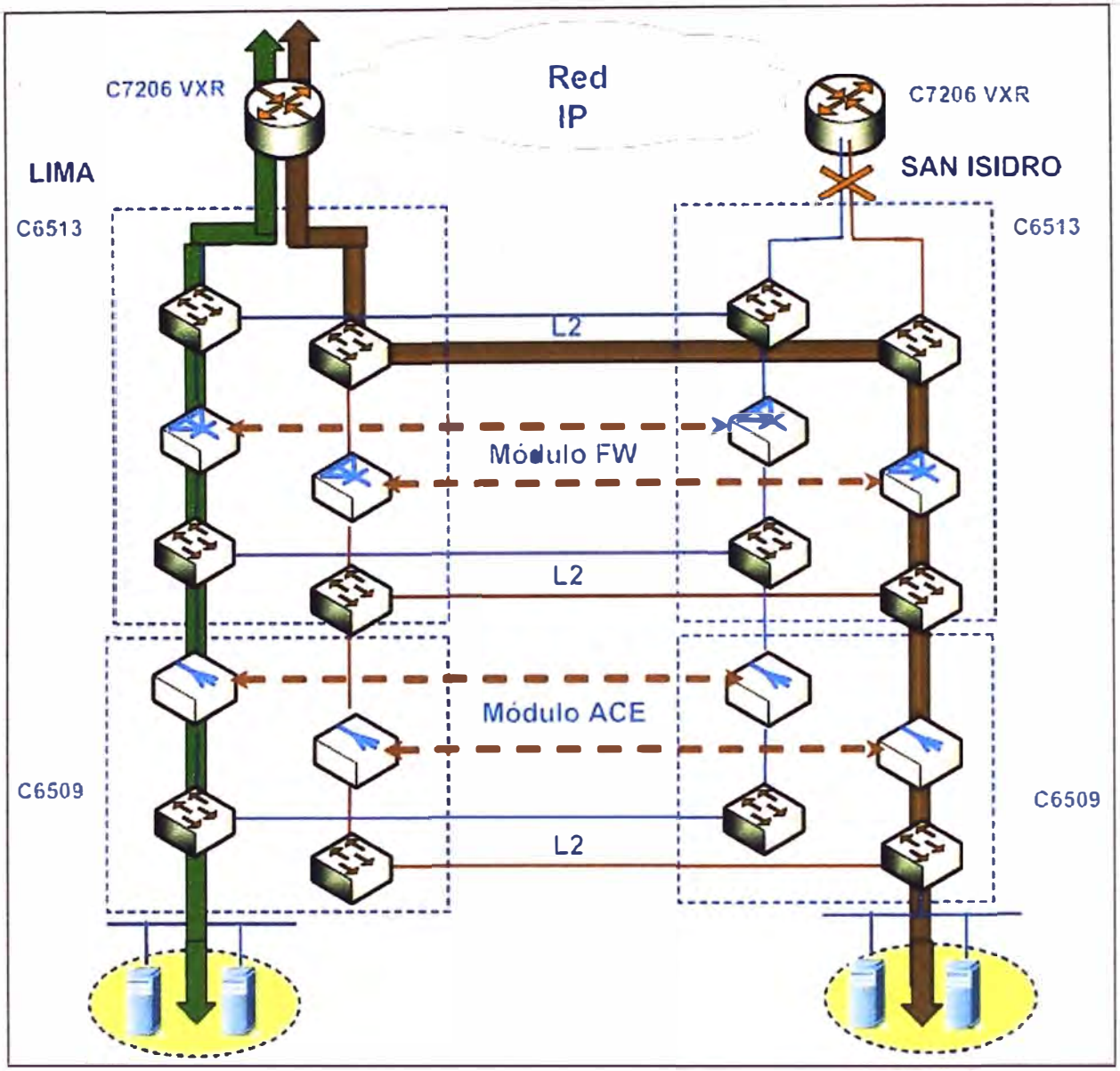

Figura 3.23 Falla del enlace entre el Switch WS-C6513-E y el router de la misma sede (San Isidro) (Fuente: Elaboración propia)

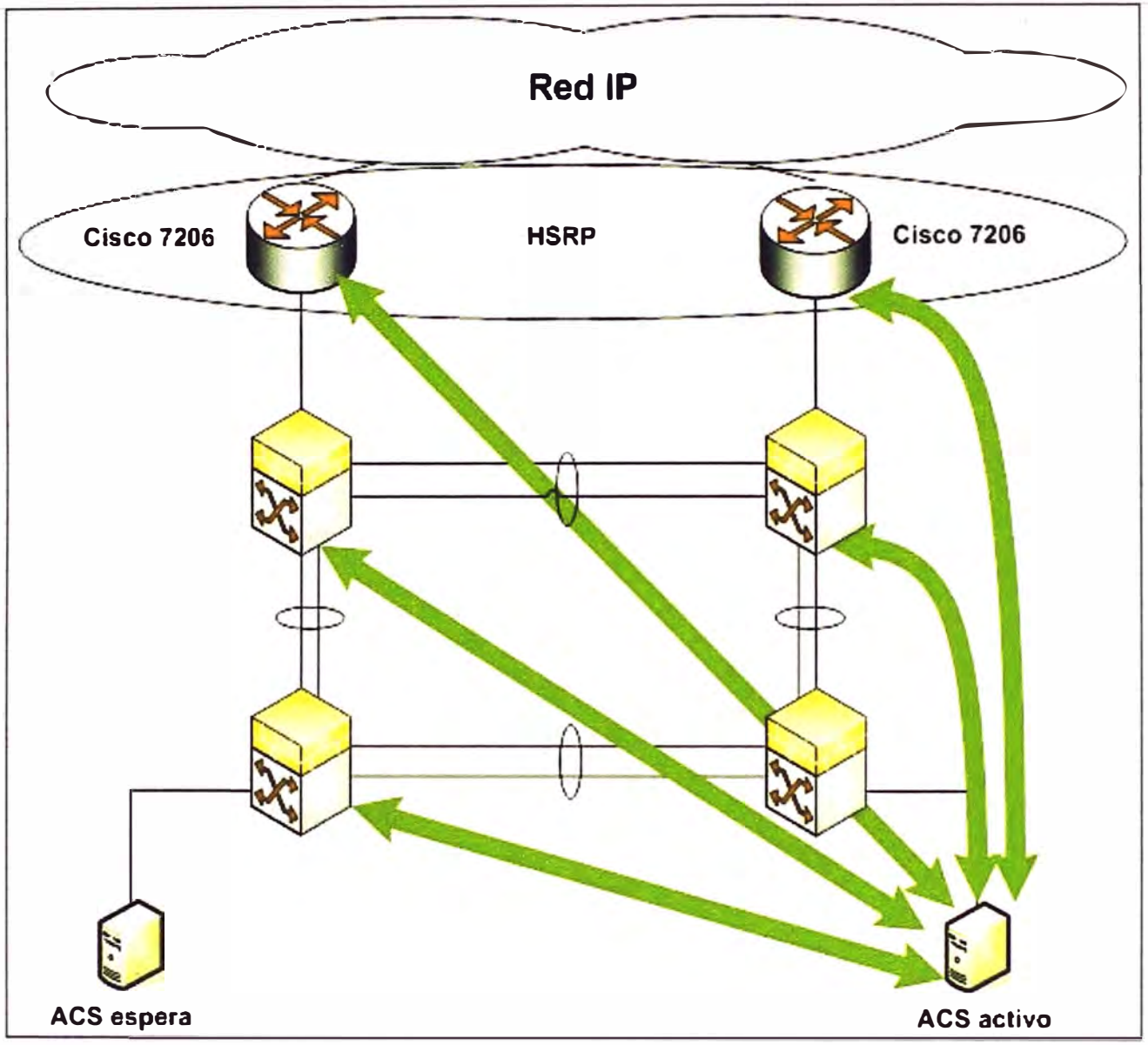

Figura 3.24 Funcionamiento del ACS en modo normal (Fuente: Elaboración propia)

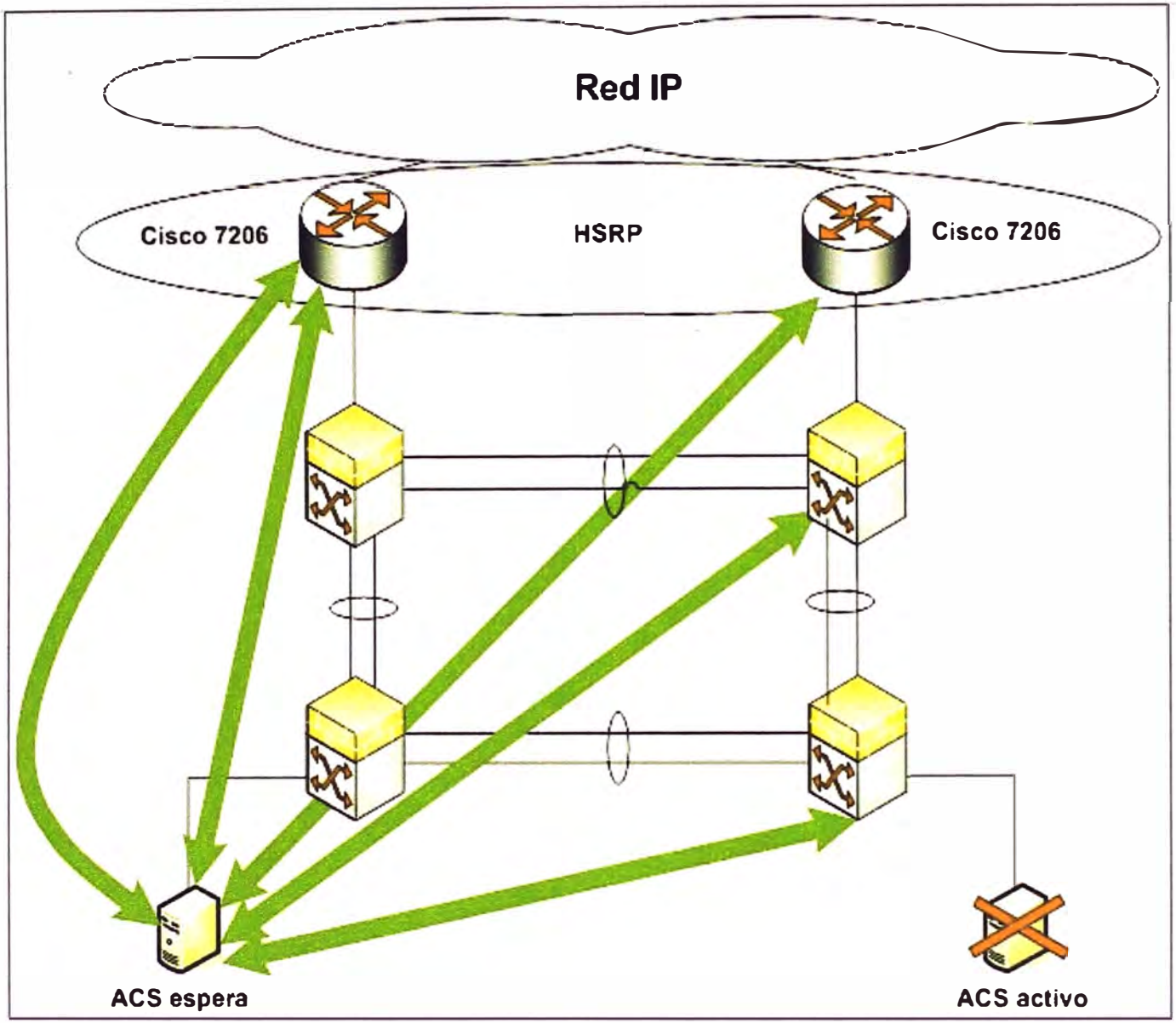

Figura 3.25 Funcionamiento del ACS durante falla (Fuente: Elaboración propia)

a. Configuración del ACE

El módulo ACE se encuentra situado en el Switch WS-C6509-E. Este módulo es el encargado de tomar la mejor decisión para el balanceo de acuerdo a las prioridades (peso) de los servidores. Para configurar este módulo primeramente debe ser accedido mediante el comando: "*6509# session slot 2 processor 0*".

Una vez tomado el control del módulo, se crean los contextos LIM y SIS correspondientes a Lima y San Isidro, respectivamente, y además se asocian a las VLAN correspondientes como se muestra en la Tabla 3.1. Debe tenerse en cuenta que este procedimiento se realiza en una sede (mismo dispositivo). Para la explicación se tiene como referencia a la sede de Lima. De manera recíproca se realiza el mismo procedimiento para la otra sede.

Tabla 3.1 Comandos de configuración de contextos

Contexto Lima	Contexto San Isidro
(config)# context LIM	*(config)# context SIS*
(config-ctx)# allocate-interface VLAN 50	*(config-ctx)# allocate-interface VLAN 65*
(config-ctx)# allocate-interface VLAN 74	*(config-ctx)# allocate-interface VLAN 64*
(config-ctx)# allocate-interface VLAN 220	*(config-ctx)# allocate-interface VLAN 240*

Luego de ello se crean los Fault Tolerance Groups (FT Groups) 1, 21 y 11. Ver Tabla 3.2

Tabla 3.2 Comandos de creación de FT Groups

1(Administración)	21 (Contexto San Isidro)	11 (Contexto Lima)
ft group 1	*Ft group 21*	*ft group 11*
peer 1	*peer 1*	*peer 1*
priority 200	*priority 150*	*priority 200*
peer priority 150	*peer priority 200*	*peer priority 150*
associate-context ADMIN	*associate-context SIS*	*associate-context LIM*
inservice	*inservice*	*inservice*

Después de ello se debe configurar la interfaz Fault Tolerance mediante el comando "*ft interface vlan 144*".con la finalidad de configurar las direcciones IP local y remota de los enlaces contra tolerancia de fallas. Hasta este punto el ACE ha sido virtualizado por lo cual está listo para:

- La creación de granja de servidores.
- Configuración de pesos.
- Configuración de inspección de protocolos de aplicación.
- Configuración de IP Virtual

Para ingresar a cada contexto (SIS o LIM) y luego configurarlos, se debe introducir el comando "*changeto LIM*". Una vez realizado ello se deben crear los diez servidores reales mediante el comando "*rserver host DNS1*", que se repite usando en cada caso un

valor distinto que va desde el 1 al 10. Luego de creados los servidores reales, cada uno es configurado con su propia dirección IP (10.5.1.0/24) y se le asignan los pesos respectivos. Con esta información completada se procede a crear la granja de servidores.

Para la configuración de inspección de protocolos de aplicación se debe crear listas de acceso, luego una clase y la política respectiva de inspección, la que se encarga de verificar que el tamaño máximo de los paquetes DNS sea de 512 bytes.

Para la configuración de IP Virtual (el que va a representar a toda la granja) se debe configurar una clase especificando la IP virtual y puerto UDP del DNS, y a continuación la política respectiva dando la directiva de balancear.

En las Tablas 3.3 y 3.4 se muestra la distribución de carga de tráfico hacia los servidores en este servicio:

Tabla 3.3 Granja San Isidro

VIP:	200.48.225.146		
IP:	10.5.2.0		
Mask:	255.255.255.0		
Servidor1	DNS 1	Peso	10
Servidor2	DNS 2	Peso	10
Servidor3	DNS 3	Peso	10
Servidor4	DNS 4	Peso	10
Servidor5	DNS 5	Peso	10
Servidor6	DNS 6	Peso	10
Servidor7	DNS 7	Peso	20

Tabla 3.4 Granja Lima

VIP:	200.48.225.130		
IP:	10.5.1.0		
Mask:	255.255.255.0		
Servidor1	DNS 1	Peso	10
Servidor2	DNS 2	Peso	10
Servidor3	DNS 3	Peso	10
Servidor4	DNS 4	Peso	10
Servidor5	DNS 5	Peso	10
Servidor6	DNS 6	Peso	10
Servidor7	DNS 7	Peso	10
Servidor8	DNS 8	Peso	10
Servidor9	DNS 9	Peso	20
Servidor10	DNS 10	Peso	20

b. Configuración del Switch WS-C6509E y WS-C6513E

Las tareas que comprende la configuración de estos dispositivos son: creación de VLAN, asignación de VLAN a servidores reales, asociación de módulo ACE al WS-C6509E, asociación de módulo firewall al WS-C6513E, y finalmente la configuración de

Etherchannel entre Switches de la misma sede y Switches de distintas sedes. Esto se desarrolla a continuación.

b.1 Creación de VLAN

En los Switch WS-C6509E y WS-C6513E (de Lima y San Isidro) se crean las VLAN correspondientes según la función que desempeñan. Su número es de 5 VLAN por cada switch y su composición se describe a continuación:

- **WS-C6509E**.- Se crea la VLAN de Failover utilizando el comando "*6509(config)# vlan 144*", de esta manera se crean sucesivamente las VLAN para los servidores reales de las sedes de Lima y San Isidro (VLAN 220 para contexto SIS y VLAN 240 para contexto LIM), así como para la VLAN de la red que representa la granja de servidores de cada sede (VLAN 64 para LIM y VLAN 74 para SIS). En total cinco VLAN.
- **WS-C6513E**.- Se crea la VLAN de Failover utilizando el comando "*6513(config)# vlan 111*" , del mismo modo se crean sucesivamente las VLAN de las zonas internas (VLAN 64 para contexto LIM y VLAN 74 para contexto SIS) y externa (VLAN 44 para LIM y VLAN 54 para SIS) del firewall de las sedes de Lima y San Isidro. En total cinco VLAN.

b.2 Asignación de VLAN a servidores reales

Para la asignación de VLAN de los servidores reales de Lima y San Isidro se configura cada interfaz con el siguiente comando "*6509(config-if)# switchport access vlan 240*" para la sede Lima y "*6509(config-if)# switchport access vlan 220*" para la sede San Isidro. Para la sede Lima se configuran 10 interfaces y para San Isidro se configuran 7 interfaces.

b.3 Asociación de módulo ACE al WS-C6509E

Para asociar el módulo ACE al Switch, primero se deben definir las VLAN que son parte de cada contexto.

Para el Failover se asigna la VLAN 144, para el contexto SIS están asignadas las VLAN 74 y 220, y para el contexto LIM están asignadas las VLAN 64 y 240. Después de esto se ubica la posición en la que está instalado el módulo ACE.

Luego de la definición de VLAN y ubicación del módulo ACE, se asignan las VLAN al grupo 1 mediante el comando *"6509(config)# svclc vlan-group 1 64,74,144,220,240*", luego de esto se asocia el grupo 1 al WS-C6509E mediante el comando "*6509(config)# svclc module 2 vlan-group 1".*

b.4 Asociación de módulo firewall al WS-C6513E

Para asociar el módulo firewall (FWSM) al Switch, primero se deben definir las VLAN que son parte de cada contexto.

Para el Failover se asigna la VLAN 111, para el contexto SIS están asignadas las VLAN 44 y 64, y para el contexto LIM están asignadas las VLAN 54 y 74. Después de

esto se ubica la posición en la que está instalado el módulo firewall.

Luego de la definición de VLAN y ubicación del módulo firewall, se asignan las VLAN al grupo 2 mediante el comando *"6513(config)# firewall vlan-group 2 44,54,64,74,111"*, luego de esto se asocia el grupo 2 al WS-C6513E mediante el comando "*6513(config)# firewall module 5 vlan-group 2".*

b.5 Configuración de Etherchannel

La configuración del Etherchannel es entre los Switches WS-C6509E de Lima y San Isidro, y entre los Switches WS-C6509E y WS-C6513E de la misma sede. Previamente a la configuración del Etherchannel se definen los puertos que son miembros.

- **Etherchannel entre WS-C6509E Lima y WS-C6509E San Isidro**.- Se configuran los puertos GigabitEthernet3/1 y GigabitEthernet3/2 de los Switches de cada sede en modo troncal, permitiendo solo las VLAN 144, 220 y 240. Este comando es aplicado en la interfaz utilizando la sentencia "*6509(config-if)# switchport mode trunk" y "6509(config-if)# switchport trunk allowed vlan 144,220,240".* Para configurar el Etherchannel se *tiene que configurar en los puertos que son miembros del enlace lógico el comando "6509(config-if)# channel-group 2 mode desirable",* luego de esta configuración se crea la interfaz Port-channel 2, este puerto tiene la misma configuración que cada puerto individual (GigabitEthernet3/1 y GigabitEthernet3/2).

- **Etherchannel entre WS-C6513E Lima y WS-C6513E San Isidro**.- Se configuran los puertos GigabitEthernet4/1 y GigabitEthernet4/2 de los Switches de cada sede en modo troncal permitiendo solo las VLAN 44, 54, 64, 74, y 111. Este comando es aplicado en la interfaz utilizando la sentencia "*6513(config-if)# switchport mode trunk" y "6513(config-if)# switchport trunk allowed vlan 44,54,64,74,111".* Para configurar el Etherchannel se *tiene que configurar en los puertos que son miembros del enlace lógico el comando "6513(config-if)# channel-group 2 mode desirable",* luego de esta configuración se crea la interfaz Port-channel 2, este puerto tiene la misma configuración que cada puerto individual (GigabitEthernet4/1 y GigabitEthernet4/2).

- **Etherchannel entre WS-C6509E Lima y WS-C6513E de la misma sede**.- Se configuran los puertos GigabitEthernet3/4 y GigabitEthernet3/4 del Switch WS-C6509E y los puertos GigabitEthernet4/4 y GigabitEthernet4/5 del Switch WS-C6513E, todos estos puertos en modo troncal permitiendo solo las VLAN 1, 64, y 74. Esto es realizado aplicando los comandos "*(config-if)# switchport mode trunk" y "(config-if)# switchport trunk allowed vlan 1,64,74"* en las interfaces del WS-C6509E y WS-C6513E. Para configurar el Etherchannel se configuran los puertos que son miembros del enlace lógico mediante el comando *"(config-if)# channel-group 1 mode desirable*", luego de esta configuración se crea la interfaz Port-channel 1 en cada Switch. Este puerto tiene la misma configuración

que los puertos individuales GigabitEthernet3/3, GigabitEthernet3/4, GigabitEthernet4/4, y GigabitEthernet4/5.

c. Configuración de Cisco 7206VXR

La configuración del protocolo HSRP tiene lugar en las interfaces Gigabit Ethernet 0/2 de los Routers de Lima y San Isidro. En esta interfaz se crea el grupo HSRP y se configura la dirección IP virtual mediante el comando "*7206(config-if)# standby 1 ip virtual-ip*", también se configura la prioridad más alta en la sede Lima y la ruta de regreso (en caso se restablezca la interfaz caída) mediante el comando "7206(config-if)# standby 1 priority 150". Para la sede San Isidro se configura una prioridad de 120.

La habilitación de rastreo se hace mediante la sentencia "*7206(config-if)# standby 1 priority preempt*" y finalmente se configura el rastreo en la interfaz Gigabit Ethernet 0/1 utilizando este mismo comando en el Router principal "*7206(config-if)#standby 1 track GigabitEthernet0/1 60*".

d. Configuración del FWSM

El módulo firewall está instalado en el Switch WS-C6513E. Este módulo es el encargado de dejar pasar el flujo de tráfico de datos relacionado con los DNS. Para configurar este módulo, inicialmente se debe acceder mediante el comando: "*6513# session slot 5 processor 1*".

Una vez tomado el control del módulo, se crean las interfaces VLAN de los contextos a crear, delimitados por la VLAN 44 y 64 para el contexto LIM, y VLAN 54 y 74 para el contexto SIS.

A manera de ejemplo se explica la configuración de las interfaces VLAN, esto se hace mediante el comando "*FWSM(config)# interface vlan 64*" para la zona interna y "*FWSM(config)# interface vlan 44*" para la zona externa del contexto Lima y "*FWSM(config)# interface vlan 111*" para Failover.

Los contextos LIM y SIS se asocian a las VLAN correspondientes como se muestra en la Tabla 3.5. Debe tenerse en cuenta que este procedimiento se realiza en una sede (mismo dispositivo). Para la explicación se tiene como referencia a la sede de Lima. De manera recíproca se realiza el mismo procedimiento para la otra sede. Para lograr el Failover Activo/Activo se crean dos grupos Failover asociados a cada contexto.

Tabla 3.5 Comandos de configuración de contextos

Contexto Lima	Contexto San Isidro
(config)# context LIM	*(config)# context SIS*
(config-ctx)# allocate-interface VLAN 44	*(config-ctx)# allocate-interface VLAN 54*
(config-ctx)# allocate-interface VLAN 64	*(config-ctx)# allocate-interface VLAN 74*
(config-ctx)# join-failover-group 1	(config-ctx)# join-failover-group 2

Luego de ello se configura el Failover (Failover Groups) 1, y 2. Ver Tabla 3.6

Tabla 3.6 Comandos de creación de Failover y Failover Groups

Sede Lima	Sede San Isidro
(config)# failover	*(config)# failover*
(config)# failover lan unit primary	*(config)# failover lan unit secondary*
(config)# failover lan interface fover Vlan111	*(config)# failover lan interface fover Vlan111*
(config)# failover link fover Vlan111	*(config)# failover link fover Vlan111*
(config)# failover group 1	*(config)# failover group 1*
(config)# failover group 2	*(config)# failover group 2*
(config)# secondary	*(config)# secondary*

Después de ello se debe configurar la interfaz Failover mediante el comando "*failover interface ip failover IP1 [máscara] standby IP2*" con la finalidad de configurar las direcciones IP activa (IP1) y de espera (IP2) de los enlaces Failover. Hasta este punto el FWSM ha sido virtualizado por lo cual está listo para la creación de zonas, la configuración de las listas de acceso para filtrar las peticiones DNS, y el enrutamiento estático.

Para ingresar a cada contexto (SIS o LIM) y luego configurarlos, se debe introducir el comando "*changeto context LIM*". Una vez realizado esto se crean las zonas en cada interfaz VLAN mediante el comando "*FWSM/LIM(config-if)# security-level 0*" para la zona externa (VLAN 44) y "*FWSM/LIM(config-if)# security-level 100*" (VLAN 64) para la zona interna, este procedimiento se repite en el otro contexto. Luego de creadas las zonas, cada una es configurada con su propia dirección IP y dirección IP de espera.

Para la configuración de las listas de acceso se debe filtrar solo los puertos TCP/IP de DNS, luego se aplican estás listas de acceso a la interfaz externa de cada contexto.

Para la configuración del enrutamiento se debe configurar una ruta por defecto (0.0.0.0/0) con puerta de enlace predeterminada a la dirección IP Virtual del grupo HSRP. Esto se hace mediante el comando "*route outside 0.0.0.0 0.0.0.0 [ip-default-gateway]*" en el FWSM.

e. Configuración de la seguridad de administración de equipos de red

Ciertos dispositivos de red cuentan con una interfaz de usuario basada en un entorno web, es decir, una pantalla de una página web como cualquiera de las disponibles en Internet. Esto facilita la administración del dispositivo sin tener que conectarse físicamente a él y ejecutar un programa especial o línea de comandos.

La Figura 3.26 es la pantalla de configuración del ACS la cual se ejecuta en un entorno web. En los párrafos siguientes se omitirá algunas partes de esta pantalla. El entorno presentado muestra tres partes principales, la primera es aquella en donde se coloca la dirección del dispositivo de red, en este caso es el ACS; la segunda es una serie de botones pertenecientes a un menú que al ir seleccionándolos mostrarán otras pantallas en el entorno de configuración.

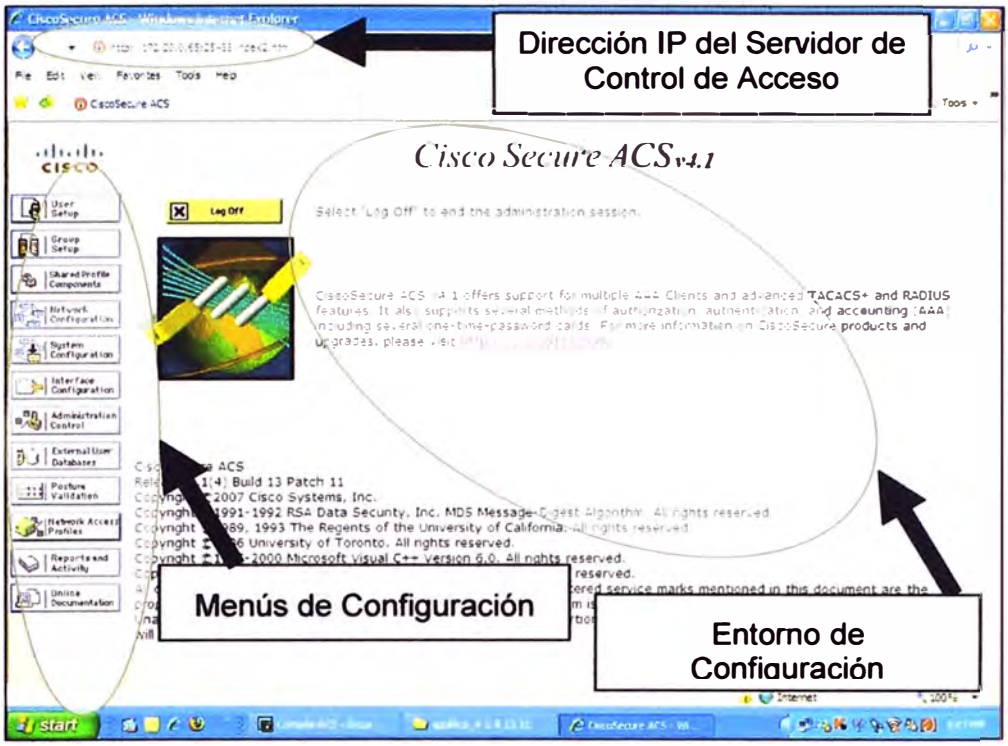

Figura 3.26 Pantalla de trabajo del ACS (Fuente: Elaboración propia)

La Figura 3.27 es un ejemplo de configuración de entorno web en donde se debe introducir la dirección IP del Cliente AAA, la clave compartida y el tipo de autenticación. Las opciones de este entorno se encuentran en inglés, para efectos explicativos han sido cambiados al castellano.

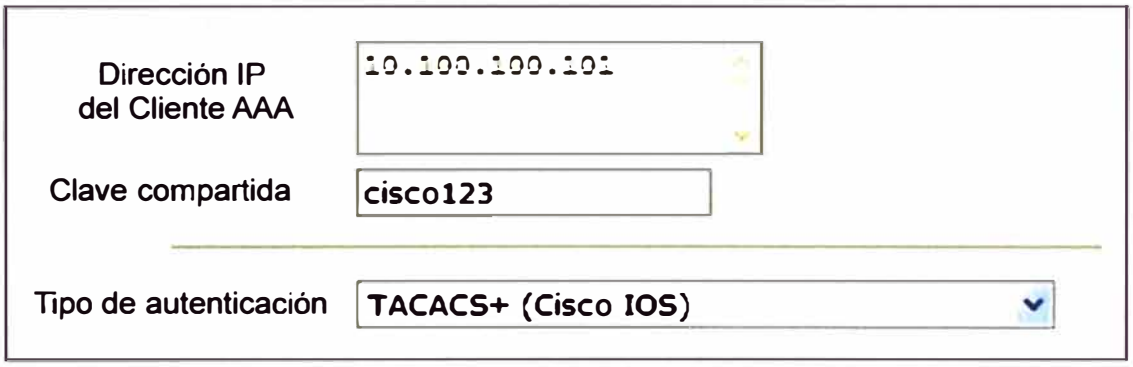

Figura 3.27 Detalle de configuración (Fuente: Elaboración propia)

En el entorno de configuración ACS debe asignarse una cuenta (usuario) y contraseña a cada cliente.

Otra parte de la configuración del ACS es habilitar la alta disponibilidad entre sedes. La Tabla 3.7 muestra los componentes seleccionados para ello.

Tabla 3.7 Alta disponibilidad de ACS

Componente	Enviar	Recibir
Base de datos de usuarios		X
Configuración de equipos		X
Configuración de interfaz		X

De manera complementaria a la configuración del ACS, es necesario configurar los

dispositivos de red (cuatro switch y dos routers) para que conozcan quién es el servidor que atenderá sus requerimientos de administración. Deben ser introducidos una serie de comandos de línea en cada dispositivo de red; estos se agrupan en:

- aaa authentication.- Se define quién puede acceder
- aaa authorization.- Se define qué puede hacer
- aaa accounting.- se habilita la inspección de actividades (qué hizo y a qué hora)
- tacacs-server.- dirección ip del servidor de control de acceso (ACS)

3.3 Equipamiento

En esta sección se hace la descripción del equipamiento de la solución:

- Router Cisco 7206VXR
- Switches Cisco de la familia Catalyst WS-C6500-E (6513 y 6509)
- Módulo de firewall FWSM (Firewall Service Module)
- Módulo de ACE (Application Control Engine Module)
- Servidor de control de acceso ACS1113

3.3.1 Router Cisco 7206VXR

La serie de Routers Cisco 7200 VXR [17] entrega un alto desempeño, precio competitivo, modularidad y escalabilidad de manera compacta con un gran despliegue de opciones (Figura 3.28).

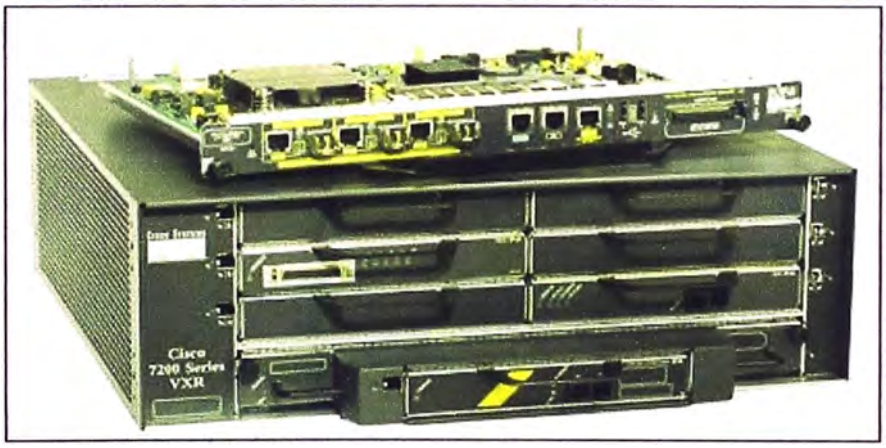

Figura 3.28 Router Cisco 7206VXR (Fuente: Cisco System Inc.)

Posee una velocidad de procesamiento de hasta 2 millones de paquetes por segundo, lo cual lo hace ideal para servicios de agregación WAN de empresas y proveedores de servicio de Internet, el cual despliega cualquier solución:

- WAN - propiedades de desempeño de calidad de servicio
- MPLS (Multiprotocol Label Switching)
- Integración de Voz/Video/Datos
- VPN (Virtual Private Network)

Este dispositivo dirige los requerimientos de las soluciones integrando las funciones previamente desempeñadas por separado en una sola plataforma. A través de esta

integración, también ofrece un costo efectivo para la plataforma que soporta:

- Alta densidad de interfaces LAN y WAN
- Terminaciones de voz, data, y video E1/T1
- Alta disponibilidad multicanal E3/T3 y E1/T1 con unidades de canales de servicio integrado y unidades de servicio de data (CSU/DSU)
- Alta densidad de tarjetas Ethernet de conmutación

Esta serie ofrece un gran grupo de capacidades que direccionan los requerimientos, desempeño, densidad, alta confiabilidad, disponibilidad, servicios, y administración.

3.3.2 Switches Cisco de la familia Catalyst WS-C6500-E (6513 y 6509)

El Cisco Catalyst 6500 [18] es un switch modular con capacidad de entregar paquetes a alta velocidad. Los Switches Cisco Catalyst 6500 comprende dos fuentes de poder, una o dos supervisoras, tarjetas de puertos Gigabitethernet, TenGigabitethernet y módulos de servicio (como ACE Application Control Engine Module y FWSM Firewall Service Module).

Un chasis puede tener 3, 4, 6, 9 o 13 slots cada uno (en los modelos Catalyst 6503-E, 6504-E, 6506-E, 6509-E, o 6513-E respectivamente) con opción a uno o dos fuentes de poder. La supervisora engine ofrece procesamiento y envío de información centralizada; hasta dos de estas tarjetas pueden ser instaladas en un chasis que ofrece failover activo/espera. Las tarjetas ofrecen conectividad de puertos y los módulos de servicios permiten dispositivos integrados en el switch. La Figura 3.29 muestra el chasis de la familia 6500-E.

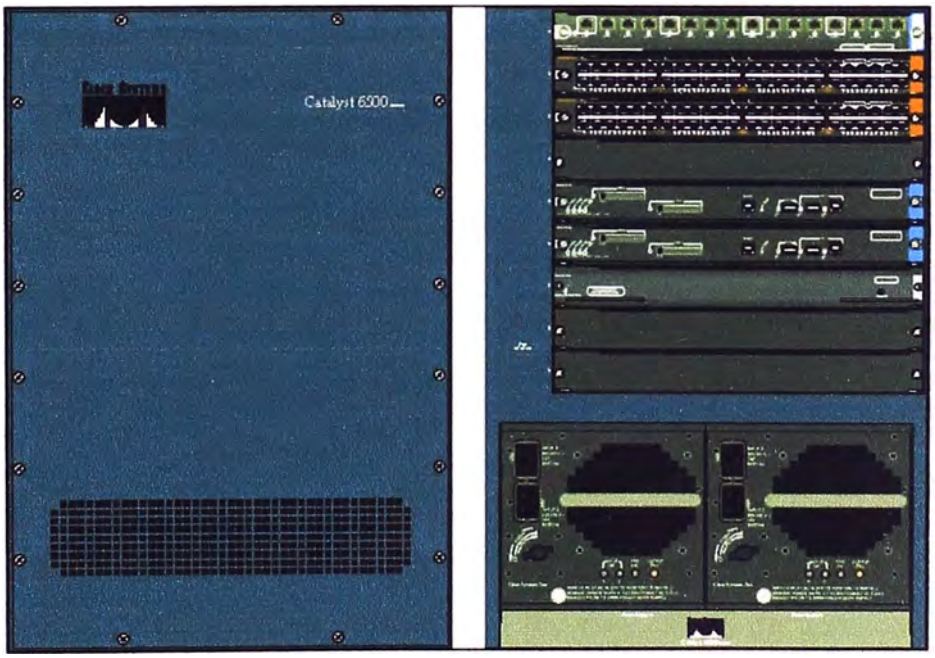

Figura 3.29 Vista Frontal y posterior del Switch de la serie 6500-E (Fuente: Elab prop)

3.3.3 Módulo de firewall FWSM (Firewall Service Module)

El FWSM [19] es un módulo de firewall de alta disponibilidad integrado para Switches

Cisco Catalyst 6500. Ofrece un rápido manejo de datos en la industria, soportando 5Gbps de rendimiento de procesamiento, 100,000 conexiones por segundo, y 1 millón de conexiones concurrentes.

Hasta 4 FWSMs (Figura 3.30) pueden ser instalados en un sólo chasis, ofreciendo una escalabilidad de hasta 20 Gbps por chasis. El Cisco FWSM ofrece una alta capacidad de procesamiento, confiabilidad, y rendimiento.

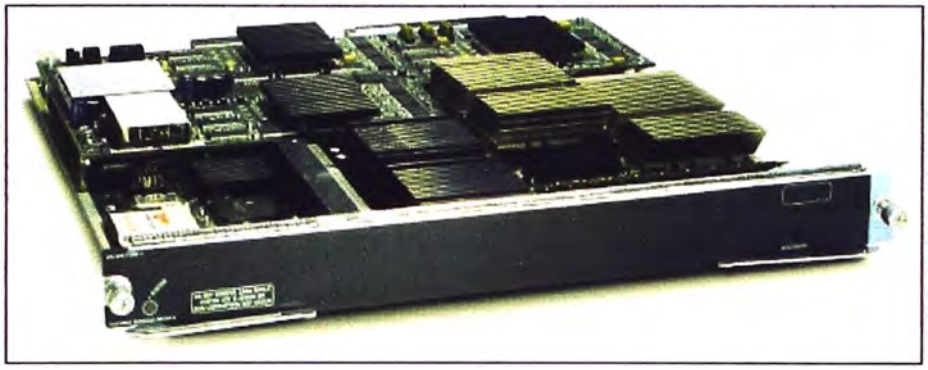

Figura 3.30 Módulo FWSM (Fuente: Cisco System Inc.)

El Cisco FWSM incluye un número de características asociadas que reducen costos y complejidad de operación mientras se habilitan la organización para administrar múltiples firewalls desde la misma consola de administración de la plataforma.

El Cisco FWSM ofrece un módulo integrado Instalado en un Switch Cisco Catalyst 6500, el FWSM permite que cualquier puerto del dispositivo opere como un puerto del firewall e integra la infraestructura de seguridad de un firewall en la topología de red. La Tabla 3.8 muestra las características de capacidad y rendimiento del FWSM

Tabla 3.8 Capacidad y rendimiento de FWSM

Desempeño	• 5.5 Gbps rendimiento de procesamiento por módulo • Hatsa 4 FWSMs (20 Gbps) por Switch Catalyst 6500 con VLAN estáticas. • 2.8 Mpps • 1 millón de conexiones concurrentes. • 256,000 traslaciones concurrentes de NAT o PAT
Interfaces VLAN	• 1000 por módulo • 256 VLAN por contexto en modo router • 8 VLAN por contexto en modo transparente
Listas de Acceso	Hasta 80,000 Listas de Acceso en un Firewall sin contextos.
Firewalls Virtuales (Contextos)	Licencia para 20, 50, 100, y 250 contextos por FWSM

3.3.4 Módulo de ACE (Application Control Engine Module)

El Cisco ACE Application Control Engine Module para Switches Cisco Catalyst 6500 [20] (Ver Figura 3.31) es la nueva generación de dispositivos de balanceo de carga y entrega de soluciones el cual ayuda con las siguientes tareas:

- Ayuda con la continuidad del negocio, incrementando de esa manera la disponibilidad de las aplicaciones.

- Mejora la productividad de los negocios, acelerando las aplicaciones y mejorando el rendimiento de los servidores
- Reduce el consumo de energía, espacio y circulación de flujo de aire a través de una arquitectura de virtualización
- Disminuye los costos asociados al aprovisionamiento y escalamiento de las aplicaciones.

Se alcanzan todas estas metas a través de un balanceo de carga inteligente e integrando tecnología de Switches de contenido con aceleración y seguridad. Una arquitectura virtualizada y basada en roles de administración ayuda a aprovisionar y entregar múltiples aplicaciones con un sólo módulo, de manera que incrementa la escalabilidad de los centro de datos.

El ACE mejora la eficiencia de las aplicaciones y servidores. Este módulo incrementa la disponibilidad de las aplicaciones, el módulo usa los mejores algoritmos de conmutación de aplicaciones y los mejores métodos de alta disponibilidad. Se puede manejar hasta 16Gbps de trafico de aplicación en un solo módulo, y hasta 64Gbps con cuatro módulos, en un solo Switch Cisco Catalyst 6500. La Tabla 3.9 muestra sus características

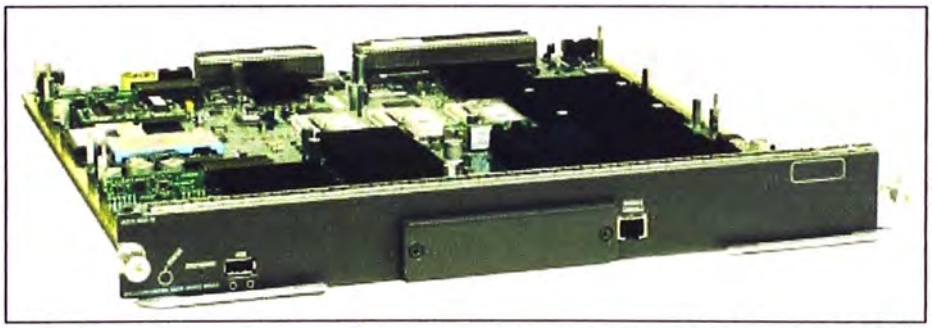

Figura 3.31 Módulo ACE (Fuente: Cisco System Inc.)

Tabla 3.9 Rendimiento y configuración

Propiedades	Máximo desempeño y configuración
Rendimiento de procesamiento	Hasta 16 Gbps
Contextos	Hasta 250
Máximo número de conexiones L4 por Segundo	500,000 transacciones completas
Máximum número de conexiones L7 por segundo	200,000 transacciones completas
Conexiones concurrentes	4 millones

3.3.5 Servidor de control de acceso ACS1113

El Cisco Secure Access Control Server (ACS) [21] ofrece inteligencia en las soluciones de control de acceso e identidad, integración y control de administración en empresas, administradores, y recursos de infraestructura de red.

El ACS (Figura 3.32) está disponible en gabinetes de comunicación exclusiva para

tareas específicas o en software que funcionan sobre Windows 2000 y 2003. Ambos productos ofrecen seguridad, y AAA para empresas.

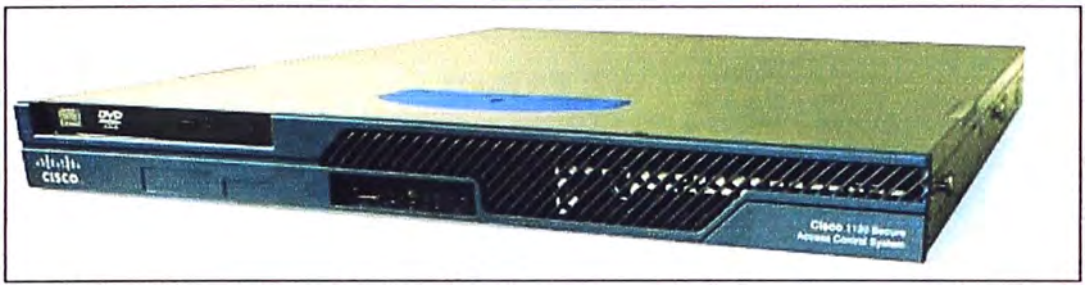

Figura 3.32 Servidor ACS1113 (Fuente: Cisco System Inc.)

Es altamente escalable y de alto desempeño. Realiza el control de acceso centralizado como servidor RADIUS y TACACS, extendiendo el acceso de seguridad, combinando autenticación, acceso de usuarios, y administración con políticas de control centralizadas en soluciones de identidad, permitiendo gran flexibilidad y movilidad, incrementando seguridad, y ganando productividad en los usuarios. El ACS se integra con soluciones de red cableada, inalámbrica, VPN y soluciones de administración de equipamiento.

Los principales beneficios del ACS son los siguientes:

- Fácil uso: una interfaz web basada en usuario simplifica y distribuye la configuración, perfiles, grupo de perfiles, y la configuración del ACS.
- Escalabilidad: El ACS ha sido construido para soportar amplios ambientes de red con el soporte de redundancia, base de datos remotas, y replicación de base de datos.
- De fácil extensión: soporta la extensión de autenticación de base de datos externas, tales como directorios activos.
- Manejo: Windows Active Directory soporta la consolidación de usuarios y contraseñas Windows que son administrados y usados para la administración.
- Administración: Diferentes niveles de acceso para cada administrador del ACS, y la habilidad de agrupar dispositivos de red fácilmente y con flexibilidad de facilitar los cambios de políticas de administración en todos los dispositivos de red.
- Flexible: porque Cisco IOS viene embebido en el ACS, puede ser usado en TACACS y RADIUS. Cisco ACS está disponible en software y en una caja a medida del cliente (personalizada=customized).
- Soporte de terceros: Cisco ACS ofrece integración con RSA, OTP (One Time Password) y con dispositivos multimarca.
- Control: El ACS ofrece control de inicio de sesiones.

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

En el presente capítulo se tocan los temas involucrados a las pruebas realizadas, al presupuesto y al cronograma del proyecto de ingeniería.

4.1 Pruebas realizadas y resultados obtenidos

En esta sección de presentan las pruebas realizadas a la solución y los resultados obtenidos, los cuales se analizan en los distintos módulos.

4.1.1 Pruebas

Para las pruebas de alta disponibilidad de la solución se provocaron fallas en los diversos enlaces, así como en los dispositivos de red. En cada una de estas fallas provocadas se pudo asegurar el servicio debido a la adecuada respuesta del sistema. Los dispositivos en espera asumieron el control o la carga del tráfico de datos.

Para las pruebas de seguridad, se puso a prueba el servidor ACS mediante ataques diversos (diccionario de usuario y contraseña, ataque de fuerza bruta, etc.), en ningún caso se pudo vulnerar el acceso a los dispositivos de red.

4.1.2 Resultados obtenidos

Esta sección se enfoca en el análisis de la información proporcionada por los distintos dispositivos y módulos de la solución, tanto en modo normal así como cuando existen fallas

a. Estadísticas de conexiones de módulos ACE y FWSM

En esta subsección se menciona el número de conexiones concurrentes en los módulos ACE y FWSM en las sedes Lima y San Isidro, así como el análisis de estas conexiones en cada contexto. Finalmente, se compara el número de conexiones concurrentes con respecto al valor de fábrica de Cisco System Inc.

La Tabla 4.1 y la Tabla 4.2 contienen las estadísticas de conexiones del módulo ACE en el contexto LIM de la sede Lima y en el contexto SIS de la sede San Isidro en modo normal; los datos mostrados son: el número de conexiones (columna 1), las peticiones de las direcciones IP origen a cada DNS (columna 2), el balanceo de carga (columna 3), y el estado de las conexiones (columna 4).

Se puede observar que el número total de conexiones concurrentes no supera los 4 millones de conexiones concurrentes del módulo ACE, según se indica en la hoja de fabricación del módulo. En caso que uno de los módulos ACE de Lima o San Isidro falle

el ACE está preparado para soportar ambos números de conexiones al mismo tiempo.

Tabla 4.1 Estadísticas de conexiones de ACE de contexto LIM en sede Lima

Identificador de conexiones	Origen	Destino	Estado
94732	120.100.8.21	200.48.225.130	Establecido
94731	10.5.1.10	120.100.8.21	Establecido
94730	200.30.2.20	200.48.225.130	Establecido
94729	10.5.1.11	200.30.2.20	Establecido

Tabla 4.2 Estadísticas de conexiones de ACE de contexto SIS en sede San Isidro

Identificador de conexiones	Origen	Destino	Estado
76811	161.220.56.2	200.48.225.146	Establecido
76810	10.5.2.10	161.220.56.2	Establecido
76809	201.180.3.19	200.48.225.146	Establecido
76808	10.5.2.11	201.180.3.19	Establecido

La Tabla 4.3 y la Tabla 4.4 contienen las estadísticas de conexiones del módulo FWSM para el contexto LIM de la sede y contexto SIS de la sede San Isidro. Los datos mostrados son; el número de conexiones concurrentes, la dirección IP origen, y la dirección IP destino.

Se puede observar que el número de conexiones de los contextos LIM y SIS funcionando al mismo tiempo en un mismo módulo no supera el número máximo de conexiones que el fabricante Cisco System Inc indica (1 millón de conexiones).

Tabla 4.3 Estadísticas de conexiones de FWSM de contexto LIM en sede Lima

Conexiones	Origen	Destino
193772	205.29.2.56	200.48.225.130
193771	162.1.11.77	200.48.225.130
193770	190.31.22.4	200.48.225.130
193769	205.29.2.56	200.48.225.130

Tabla 4.4 Estadísticas de conexiones de FWSM de contexto SIS en sede San Isidro

Conexiones	Origen	Destino
166550	190.41.12.2	200.48.225.146
166549	201.19.1.33	200.48.225.146
166548	196.13.20.9	200.48.225.146
166547	201.19.1.33	200.48.225.146

b. Estadisticas de inspección de DNS del ACE de Lima y San Isidro

La Tabla 4.5 y la Tabla 4.6 contienen las estadísticas del número de veces que la política INSPECCIÓN-DNS detecta que el tamaño de las peticiones DNS excedió los 512 bytes. Las fuentes del resultado de las políticas INSPECCIÓN-DNS son tomadas de las

sedes Lima y San Isidro en funcionamiento normal o falla.

Tabla 4.5 Estadísticas de inspección de DNS de Lima

Número de paquetes	Tamaño de paquete DNS	Concordancia con política
126332	512 bytes	364

Tabla 4.6 Estadísticas de inspección de DNS de San Isidro

Número de paquetes	Tamaño de paquete DNS	Concordancia con política
100574	512 bytes	298

c. Resultado de alta disponibilidad del ACE de Lima y San Isidro

La Tabla 4.7 y la Tabla 4.8 contienen los estados de alta disponibilidad de los contextos LIM y SIS del módulo ACE de la sede Lima y del módulo ACE de la sede San Isidro en modo normal. A continuación se explica el estado de cada contexto.

En la sede Lima el contexto Admin y LIM están activos y el contexto SIS está en espera. De la misma forma la sede San Isidro el contexto Admin y LIM están en espera y el contexto LIM está activo.

Tabla 4.7 Estado de cada contexto del ACE de la sede Lima

Contexto	Admin	LIM	SIS
Estado	Activo	Activo	Espera

Tabla 4.8 Estado de cada contexto del ACE de la sede San Isidro

Contexto	Admin	LIM	SIS
Estado	Espera	Espera	Activo

En caso de falla o caída de enlace relacionado a la inactividad del módulo ACE de la sede Lima o San Isidro (Tabla 4.9), el módulo ACE de la otra sede asume el control del DNS de dicha sede. Debido a la simetría del comportamiento en la falla de cualquiera de los módulos ACE se muestra solo la sede Lima.

Tabla 4.9 Resultado de falla del módulo ACE de San Isidro en la sede Lima

Contexto	Admin	LIM	SIS
Estado	Activo	Activo	Activo

d. Resultado de alta disponibilidad del FWSM de Lima y San Isidro

La Tabla 4.10 y la Tabla 4.11 contienen los estados de alta disponibilidad de los contextos LIM y SIS del módulo FWSM de la sede Lima y del módulo FWSM de la sede San Isidro en modo normal. A continuación se explica el estado de cada contexto.

En la sede Lima el contexto Admin y LIM están activos y el contexto SIS está en espera. De la misma forma la sede San Isidro el contexto Admin y LIM están en espera y el contexto LIM está activo.

Tabla 4.10 Estado de cada contexto del FWSM de la sede Lima

Contexto	Admin	LIM	SIS
Estado	Activo	Activo	Espera

Tabla 4.11 Estado de cada contexto del FWSM de la sede San Isidro

Contexto	Admin	LIM	SIS
Estado	Espera	Espera	Activo

En caso de falla o caída de enlace relacionado a la inactividad del módulo firewall de la sede Lima o San Isidro (Tabla 4.12). El FWSM de la otra sede asume el control de la protección del DNS de dicha sede. Debido a la simetría del comportamiento en la falla de cualquiera de los FWSM se mostrará la sede Lima.

Tabla 4.12 Resultado de falla del FWSM de San Isidro en la sede Lima

Contexto	Admin	LIM	SIS
Estado	Activo	Activo	Activo

e. Resultado de alta disponibilidad del Router 7206VXR de Lima y San Isidro

La Tabla 4.13 contiene el estado de los grupos HSRP configurados en los Routers 7206VXR de la sede Lima y San Isidro en funcionamiento normal. El grupo 1 permite que el DNS envíe todo el tráfico a través del Router de Lima. El grupo 2 en esta sede pone en estado en espera el tráfico DNS de la sede San Isidro. De manera similar el grupo 2 permite que el DNS envíe todo el tráfico a través del Router de San Isidro.

Tabla 4.13 Estado de cada grupo de los Routers de la sede Lima y San Isidro

Sede/Grupo	Grupo 1	Grupo 2
Lima	Activo	Espera
San Isidro	Espera	Activo

La Tabla 4.14 contiene el estado de los grupos HSRP en caso el Router de la sede San Isidro falle o el enlace relacionado a uno de los dispositivos conectados, el router de la sede Lima asume el tráfico del DNS de Lima y San Isidro.

Tabla 4.14 Estado de cada grupo del Router de la sede Lima por falla en San Isidro

Sede/Grupo	Grupo 1	Grupo 2
Lima	Activo	Activo
San Isidro	Falla	Falla

f. Resultado de Etherchannel de los Switches WS-C6500E de Lima y San Isidro

La Tablas 4.15, 4.16, y 4.17 contienen las agrupaciones lógicas de los puertos que conforman los Etherchannel entre los Switches WS-C6509E de la misma sede, Switches WS-C6513E de la misma sede, y entre los Switches WS-C6509E y WS-C6513E de la misma sede, respectivamente. Estos puertos se encuentran en funcionamiento normal.

Tabla 4.15 Equipos y puertos que conforman el Etherchannel en Lima

Etherchannel/Equipo	WS-C6509E (Lima)	WS-C6513E (Lima)
Port-channel 1	Gi3/4 y Gi3/5	Gi4/4 y Gi4/5

Tabla 4.16 Equipos y puertos que conforman el Etherchannel entre sedes (6509E)

Etherchannel/Equipo	WS-C6509E (Lima)	WS-C6509E (San Isidro)
Port-channel 2	Gi3/1 y Gi3/2	Gi3/1 y Gi3/2

Tabla 4.17 Equipos y puertos que conforman el Etherchannel entre sedes (6513E)

Etherchannel/Equipo	WS-C6513E (Lima)	WS-C6513E (San Isidro)
Port-channel 2	Gi4/1 y Gi4/2	Gi4/1 y Gi4/2

En el caso que falle uno de los puertos pertenecientes a uno de los Etherchannel de la sede Lima entre los equipos WS-C6509E o entre los equipos WS-C6509E y WS-C6513E de la misma sede, el enlace restante asume toda la carga de tráfico (Tabla 4.18) convirtiéndose este enlace en un posible cuello de botella.

Tabla 4.18 Falla del puerto Gi3/5 del WS-C6509E en la sede Lima

Etherchannel/Equipo	WS-C6509E (Lima)	WS-C6513E (Lima)
Port-channel 1	Gi3/4	Gi4/4 y Gi4/5

g. Resultado de seguridad de acceso a dispositivos (AAA y ACS)

La Tabla 4.19 contiene los resultados de acceso a los equipos WS-C6509E y C7206VXR de la sede Lima. Los datos mostrados son: el usuario almacenado en el ACS de una de las sedes, los comandos ingresados en el equipo monitoreado, el tiempo el cual estuvo conectado y el nivel de acceso que tiene dicho usuario.

Tabla 4.19 Resultado de acceso a WS-C6509E y C7206VXR de la sede Lima

Usuario	Comandos realizados	Tiempo	Equipo
José	Configuración	32 minutos	6509 Lima
Roberto	Revisión	25 minutos	7206 Lima

En el caso de alta disponibilidad de los ACS de la sede Lima y San Isidro, el servidor ACS de Lima es el activo y el servidor ACS de la sede San Isidro es el dispositivo en espera. Para el caso en el que el ACS de Lima falle (Tabla 4.20), el ACS de San Isidro asume todo el control de la seguridad de acceso.

Tabla 4.20 Falla de servidor ACS de sede Lima

Situación/ACS	Servidor ACS Lima	Servidor ACS San Isidro
Situación normal	Activo	Espera
Situación falla	Falla	Activo

g. Resultado de disponibilidad

En el análisis de la situación inicial se obtuvo los resultados mostrados en la Tabla 4.21. Estos datos corresponden al año 2007. La disponibilidad anual es calculada mediante la ecuación 4.1, es decir, la sumatoria de las disponibilidades de cada mes

durante todo un año y dividida entre 12.

$$\text{Disponibilidad} = \frac{\sum_{i=1}^{i=12} D_i}{12} \qquad (4.1)$$

Donde Di es la disponibilidad de un mes que está dentro de los meses del año 2007.

Tabla 4.21 Datos de año 2007

Mes	Horas totales al mes (Ht)	Tiempo de corte en horas (Tc)	Porcentaje Ht/(Ht +Tc))x100
1	720	2	99.72
2	720	2	99.72
3	720	6	99.17
4	720	0	100
5	720	0	100
6	720	14	98.09
7	720	8	98.90
8	720	10	98.63
9	720	8	98.90
10	720	4	99.44
11	720	4	99.44
12	720	0	100

De los resultados obtenidos en la Tabla 4.21 la disponibilidad anual es 99.33%

En el análisis de la solución actual se obtuvo los resultados mostrados en la Tabla 4.22. Estos datos corresponden al año 2008. La disponibilidad del año 2008 es obtenida de igual forma (media aritmética de los 12 meses del año):

Tabla 4.22 Datos de año 2008 (Después de implementada la solución)

Mes	Horas totales al mes	Tiempo de corte (horas)	Disponibilidad	Porcentaje (%)
1	720	0	1.0000	100.00
2	720	0	1.0000	100.00
3	720	0	1.0000	100.00
4	720	0	1.0000	100.00
5	720	0	1.0000	100.00
6	720	0	1.0000	100.00
7	720	0	1.0000	100.00
8	720	0	1.0000	100.00
9	720	0	1.0000	100.00
10	720	0	1.0000	100.00
11	720	0	1.0000	100.00
12	720	0	1.0000	100.00

De los resultados obtenidos en la Tabla 4.22, la disponibilidad anual de la solución actual es 100.00%, demostrándose la efectividad de la solución implementada.

4.2 Estimación de costos

La Tabla 4.23 contiene el presupuesto de adquisición de los módulos ACE y servidores ACS e implementación de la solución (se incluye IGV).

Tabla 4.23 Presupuesto de módulos ACE, servidores ACS, e implementación

Rubro	Unidad	Cantidad	Precio unitario S/.	Precio total S/.
Módulo ACE	c/u	2	73,353	148,705
Servidor ACS	c/u	2	24,061	48,122
Implementación	Horas hombre	832	135	112,320
Total				309,047

4.3 Estimación de tiempos

La gestión del tiempo del proyecto ha sido dividida en las siguientes tareas:

- Análisis de la solución. Consta del análisis preliminar y del diseño de la solución.
- Elaboración del presupuesto.- Que contiene el equipamiento y la implementación.
- Aprobación del presupuesto.- Consta de la evaluación económica y su sustento.
- Actividades previas a la implementación.- Involucra la revisión de las configuraciones de los dispositivos y módulos.
- La implementación.
- Las pruebas.

La Tabla 4.24 es un resumen del cronograma de implementación.

Tabla 4.24 Resumen del cronograma de actividades del proyecto

Descripción del Proyecto	Tiempo
Proyecto de Alta Disponibilidad y Reforzamiento de Seguridad	48 días
Análisis de la solución	8 días
Elaboración de presupuesto	7 días
Aprobación de presupuesto	7 días
Actividades previas a la implementación	4 días
Implementación - Lima - San Isidro	9 días
Pruebas	13 días

El Anexo B contiene el diagrama de gantt del proyecto.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se ha logrado hacer más robusta la infraestructura y los servicios de red del Proveedor de Servicios (ISP) mediante la implementación de alta disponibilidad y mejora de la seguridad en los Centros de Servicio y Core IP.

2. A nivel de alta disponibilidad la topología de red ahora posee una arquitectura robusta en la que se ha implementado mecanismos automáticos que mitigan las fallas físicas de equipos y enlace. En resumen: se ha implementado el protocolo LACP en los switches (WS-C6509E y WS-C6513E), se ha implementado el protocolo de alta disponibilidad de capa 3 HSRP en los router (7206VXR), se han virtualizado los firewall (creando contextos) y se ha implementado failover activo/activo, de manera que si algún firewall falla el otro asume todo el control de ambos servicios DNS, se han virtualizado los balanceadores (ACE) en dos contextos; además se ha implementando la tolerancia de fallas entre los contextos, finalmente, también se ha implementado la redundancia de los servidores de control de acceso (ACS).

3. A nivel de seguridad de acceso, ahora se tiene una estructura de seguridad para la administración de los equipos del Centro de Servicios (Switches y Routers) centralizando la base de datos de usuarios y contraseña en un solo servidor de control de acceso, auditando las actividades que se hacen en los dispositivos de red y restringiendo las actividades realizadas por ciertos usuarios.

4. A nivel de protocolos, ahora se inspecciona las peticiones DNS para asegurar que los requerimientos enviados a los DNS tengan un comportamiento adecuado a una petición normal desde el Internet.

5. A nivel de velocidad de la red núcleo (Switches y Router), se ha incrementado la velocidad de trasferencia de 1Gbps a 2Gbps (Etherchannel), esto con la finalidad de no provocar un cuello de botella, además de múltiples caminos en caso se presente un evento físico o lógico.

Recomendaciones

1. Proveer cuatro servidores físicos adicionales a cada granja de servidores de las

sedes de Lima y San Isidro. Esto evitaría la sobrecarga en los servidores físicos actuales, especialmente cuando algún servidor físico falle.

2. Añadir un puerto físico a todos los enlaces Etherchannel de las sedes de Lima y San Isidro. Esto con la finalidad de aumentar la capacidad de transmitir datos y evitar que, debido a la caída de un puerto, en el puerto restante se origine un cuello de botella.

3. Añadir la seguridad de acceso también al módulo ACE y al módulo firewall, de manera que se refuerza la seguridad de los módulos de servicio.

4. Separar la administración de los equipos de la solución creando un grupo de administración para los equipos de seguridad y balanceo y un grupo de administración para los Routers y Switches.

5. Implementar Etherchannel también entre los Routers 7206 VXR de cada sede y los Switches WS-C6513E, mediante la adición de una interfaz Gigabit Ethernet.

6. Replicar las granjas de servidores de la sede de Lima y San Isidro en cada sede, es decir, implementar una granja de servidores adicional en cada sede para desplegar un plan de recuperación de desastres.

ANEXO A
ECUACIONES DE DISPONIBILIDAD DEL SISTEMA

Este anexo se basa en los diagramas de las topologías de la situación inicial y las alternativas de solución. Se toma en cuenta la teoría de la sección 2.4.2 a 2.4.4., así como la sección 3.1.3 (comparación de alternativas).

A.1 Sistema Inicial

El diagrama de bloques de la Figura A.1 resume los elementos considerados en el cálculo de disponibilidad del sistema inicial

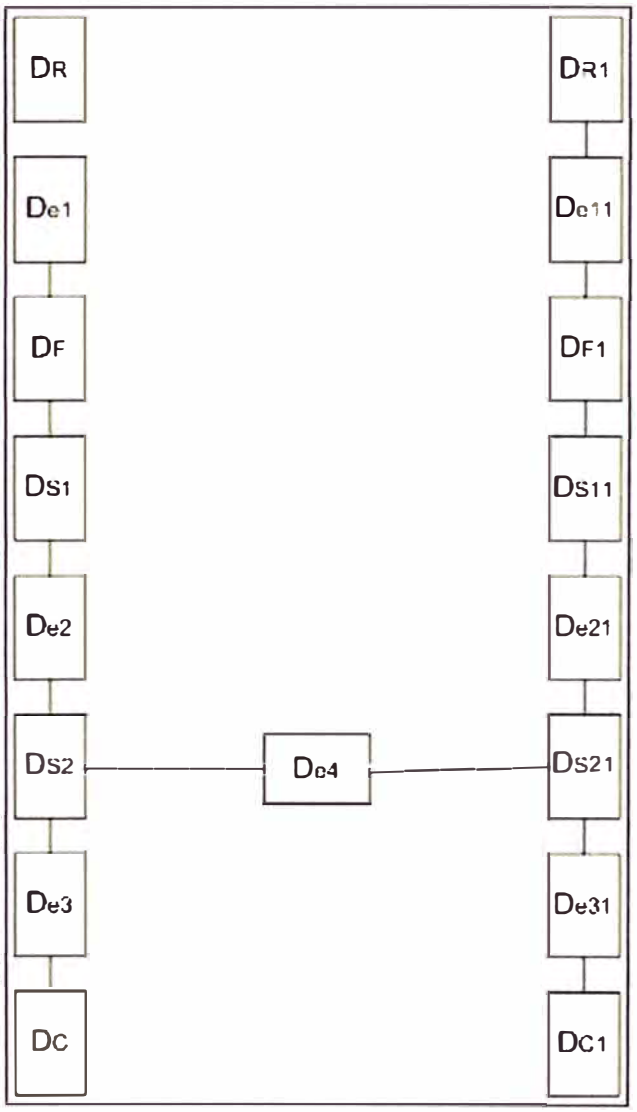

Figura A.1 Sistema inicial

Se consideran cuatro tramos serie, de D_{T1} a D_{T4}., los que luego son calculados en paralelo. Las ecuaciones (A.1 a A.4) de la disponibilidad de cada tramo (en serie) describen también los componentes considerados:

$$D_{T2} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e31} \times D_{C1} \quad (A.1)$$

$$D_{T2} = D_{R1} \times D_{e11} \times D_{F1} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e31} \times D_{C1} \quad (A.2)$$

$$D_{T3} = D_{R1} \times D_{e11} \times D_{F1} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e4} \times D_{S2} \times D_{e3} \times D_C \quad (A.3)$$

$$D_{T4} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e4} \times D_{S21} \times D_{e31} \times D_{C1} \quad (A.4)$$

Luego las disponibilidades serie son calculadas como si todas estuvieran en paralelo. Esto se refleja en la fórmula (A.5).

$$D_S = 1-(1-D_{T1})\times(1-D_{T2})\times(1-D_{T3})\times(1-D_{T4}) \quad (A.5)$$

Lo que se resume en la fórmula (A.6)

$$D_S = 1-\prod_{i=1}^{4}(1-D_{Ti}) \quad (A.6)$$

En el caso de las ecuaciones de disponibilidad de denegación de servicio y seguridad de administración las disponibilidades son D_d y D_a lo cual se introduce en serie a la disponibilidad del sistema; ecuación (A.7).

$$D_{Inicial} = D_S \times D_d \times D_a \quad (A.7)$$

A.2 Alternativa 1

El diagrama de bloques de la Figura A.2 resume los elementos considerados en el cálculo de disponibilidad de esta alternativa.

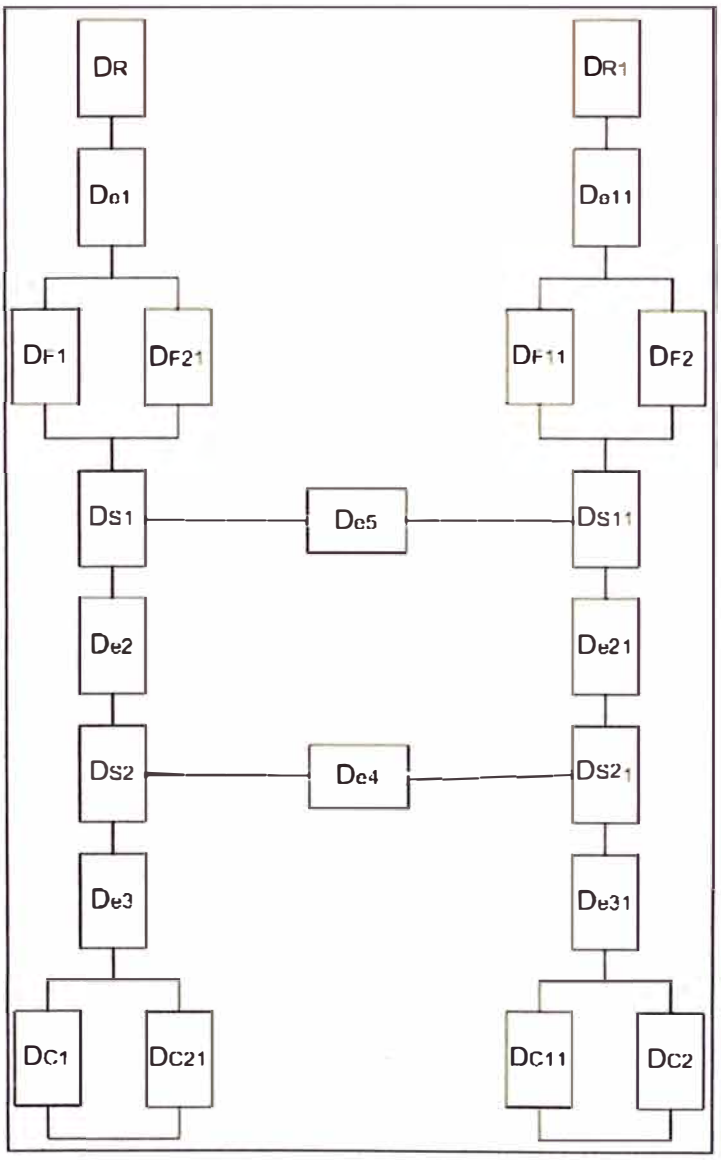

Figura A.2 Primera alternativa

Primero se considerarán las disponibilidades de los elementos en redundancia (en paralelo) mediante las siguientes fórmulas (A.8 a A.11).

$$D_F = 1-(1-D_{F1})\times(1-D_{F21}) \quad (A.8)$$

$$D_{FF} = 1-(1-D_{F11})\times(1-D_{F2}) \quad (A.9)$$

$$D_C = 1-(1-D_{C1})\times(1-D_{C21}) \quad (A.10)$$

$$D_{CC} = 1-(1-D_{C11})\times(1-D_{C2}) \quad (A.11)$$

Luego con estos valores de determinan los ocho tramos equivalentes para las topología tipo puente (Fórmulas A.12 a A.19).

$$D_{T1} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e3} \times D_C \quad (A.12)$$

$$D_{T2} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e31} \times D_{CC} \quad (A.13)$$

$$D_{T3} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{e5} \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e3} \times D_C \quad (A.14)$$

$$D_{T4} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e5} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e31} \times D_{CC} \quad (A.15)$$

$$D_{T5} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{e5} \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e4} \times D_{S21} \times D_{e31} \times D_{CC} \quad (A.16)$$

$$D_{T6} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e5} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e4} \times D_{S2} \times D_{e3} \times D_C \quad (A.17)$$

$$D_{T7} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e4} \times D_{S2} \times D_{e3} \times D_C \quad (A.18)$$

$$D_{T8} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e4} \times D_{S21} \times D_{e31} \times D_{CC} \quad (A.19)$$

Luego con las disponibilidades seriales se calcula la disponibilidad del sistema (paralela una a otra). Esta disponibilidad se expresa en la ecuación (A.20) y se resume con la ecuación (A.21).

$$D_{A1} = 1-(1-D_{T1})\times(1-D_{T2})\times(1-D_{T3})\times(1-D_{T4})\times(1-D_{T5})\times(1-D_{T6})\times(1-D_{T7})\times(1-D_{T8}) \quad (A.20)$$

$$D_{A1} = 1-\prod_{i=1}^{8}(1-D_{Ti}) \quad (A.21)$$

En el caso de las ecuaciones de disponibilidad de denegación de servicio y seguridad de administración las disponibilidades son D_d y D_a, lo cual se introduce en serie a la disponibilidad del sistema. En este caso la disponibilidad de la seguridad de administración de dispositivos se considera la inclusión de un ACS. El subsistema en la siguiente ecuación:

$$D_a = D_{enlace} \times D_{ACS} \quad (A.22)$$

Finalmente la ecuación de la alternativa 1 es la siguiente:

$$D_{Alternativa1} = D_{A1} \times D_d \times D_a \quad (A.23)$$

A.3 Alternativa 2

El diagrama de bloques de la Figura A.3 resume los elementos considerados en el cálculo de disponibilidad de esta alternativa.

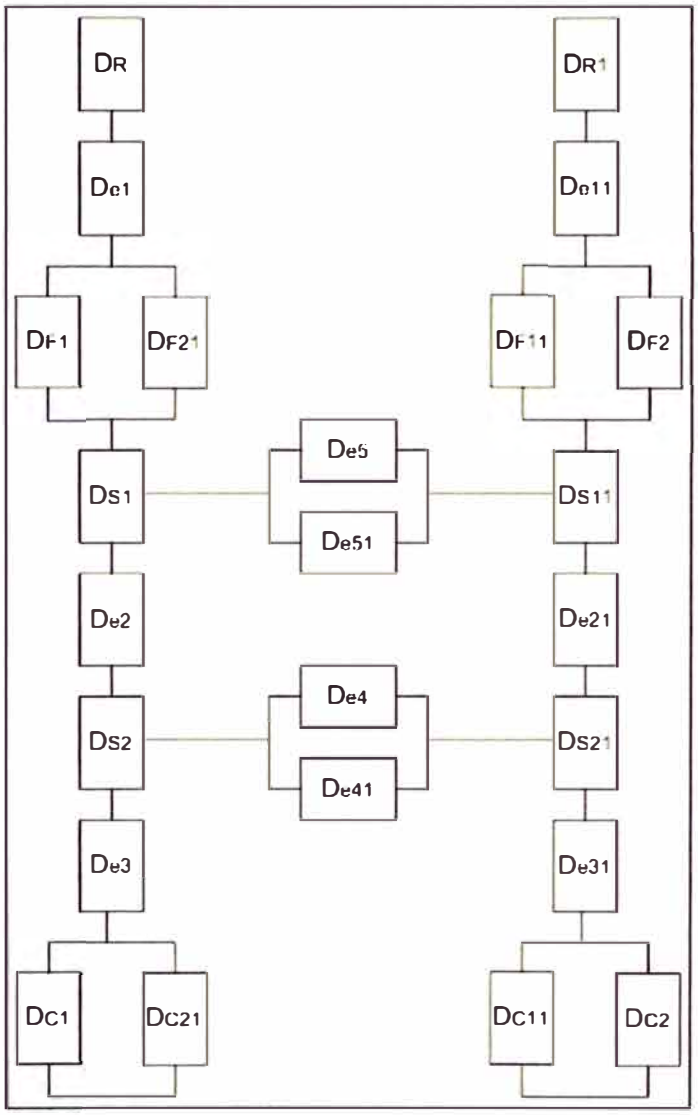

Figura A.3 Segunda alternativa

Primero se considerarán las disponibilidades de los nuevos elementos en redundancia (en paralelo) mediante las fórmulas (A.24) y (A.25). Se consideran las ecuaciones A.8 a A.11 para los restantes elementos redundantes.

$$D_E = 1-(1-D_{e5})\times(1-D_{e51}) \quad \text{(A.24)}$$

$$D_{EE} = 1-(1-D_{e4})\times(1-D_{e41}) \quad \text{(A.25)}$$

Luego con estos nuevos valores se actualizan los ocho tramos equivalentes para las topología tipo puente (Fórmulas A.26 a A.33).

$$D_{T1} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e3} \times D_C \quad \text{(A.26)}$$

$$D_{T2} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e31} \times D_{CC} \quad \text{(A.27)}$$

$$D_{T3} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_E \times D_{S1} \times D_{e2} \times D_{S2} \times D_{e3} \times D_C \quad \text{(A.28)}$$

$$D_{T4} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_E \times D_{S11} \times D_{e21} \times D_{S21} \times D_{e31} \times D_{CC} \quad \text{(A.29)}$$

$$D_{T5} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_E \times D_{S1} \times D_{e2} \times D_{S2} \times D_{EE} \times D_{S21} \times D_{e31} \times D_{CC} \quad \text{(A.30)}$$

$$D_{T6} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_E \times D_{S11} \times D_{e21} \times D_{S21} \times D_{EE} \times D_{S2} \times D_{e3} \times D_C \quad \text{(A.31)}$$

$$D_{T7} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{e21} \times D_{S21} \times D_{EE} \times D_{S2} \times D_{e3} \times D_C \quad (A.32)$$

$$D_{T8} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{e2} \times D_{S2} \times D_{EE} \times D_{S21} \times D_{e31} \times D_{CC} \quad (A.33)$$

Luego con las disponibilidades seriales se calcula la disponibilidad del sistema (paralela una a otra). Esta disponibilidad se expresa en la ecuación (A.34) y se resume con la ecuación (A.35).

$$D_{A2} = 1-(1-D_{T1}) \times (1-D_{T2}) \times (1-D_{T3}) \times (1-D_{T4}) \times (1-D_{T5}) \times (1-D_{T6}) \times (1-D_{T7}) \times (1-D_{T8}) \quad (A.34)$$

$$D_{A2} = 1 - \prod_{i=1}^{8} (1-D_{Ti}) \quad (A.35)$$

En el caso de las ecuaciones de disponibilidad de denegación de servicio y seguridad de administración las disponibilidades son D_d y D_a lo cual se introduce en serie a la disponibilidad del sistema. En este caso la disponibilidad de la seguridad de administración de dispositivos se considera la inclusión de otro ACS en alta disponibilidad del subsistema en la siguiente ecuación:

$$D_a = 1-(1-D_{enlace} \times D_{ACS}) \times (1-D_{enlace1} \times D_{ACS1}) \quad (A.36)$$

Finalmente la ecuación de la alternativa 2 es la siguiente:

$$D_{Alternativa2} = D_{A2} \times D_d \times D_a \quad (A.37)$$

A.4 Alternativa 3

El diagrama de bloques de la Figura A.4 resume los elementos considerados en el cálculo de disponibilidad de esta alternativa. Primero se considerarán las disponibilidades de los nuevos elementos en redundancia mediante las fórmulas (A.38) y (A.39). Se consideran las demás ecuaciones ya definidas para los restantes elementos redundantes.

$$D_{E1} = 1-(1-D_{e2}) \times (1-D_{e22}) \quad (A.38)$$

$$D_{EE1} = 1-(1-D_{e21}) \times (1-D_{e212}) \quad (A.39)$$

Luego con estos nuevos valores se actualizan los ocho tramos equivalentes para las topología tipo puente (Fórmulas A.40 a A.47).

$$D_{T1} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{E1} \times D_{S2} \times D_C \quad (A.40)$$

$$D_{T2} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{EE1} \times D_{S21} \times D_{CC} \quad (A.41)$$

$$D_{T3} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{E1} \times D_{S1} \times D_E \times D_{S2} \times D_C \quad (A.42)$$

$$D_{T4} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_E \times D_{S11} \times D_{EE1} \times D_{S21} \times D_{CC} \quad (A.43)$$

$$D_{T5} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_E \times D_{S1} \times D_{E1} \times D_{S2} \times D_{EE} \times D_{S21} \times D_{CC} \quad (A.44)$$

$$D_{T6} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_E \times D_{S11} \times D_{EE1} \times D_{S21} \times D_{EE} \times D_{S2} \times D_C \quad (A.45)$$

$$D_{T7} = D_{R1} \times D_{e11} \times D_{FF} \times D_{S11} \times D_{EE1} \times D_{S21} \times D_{EE} \times D_{S2} \times D_C \quad (A.46)$$

$$D_{T8} = D_R \times D_{e1} \times D_F \times D_{S1} \times D_{E1} \times D_{S2} \times D_{EE} \times D_{S21} \times D_{CC} \quad (A.47)$$

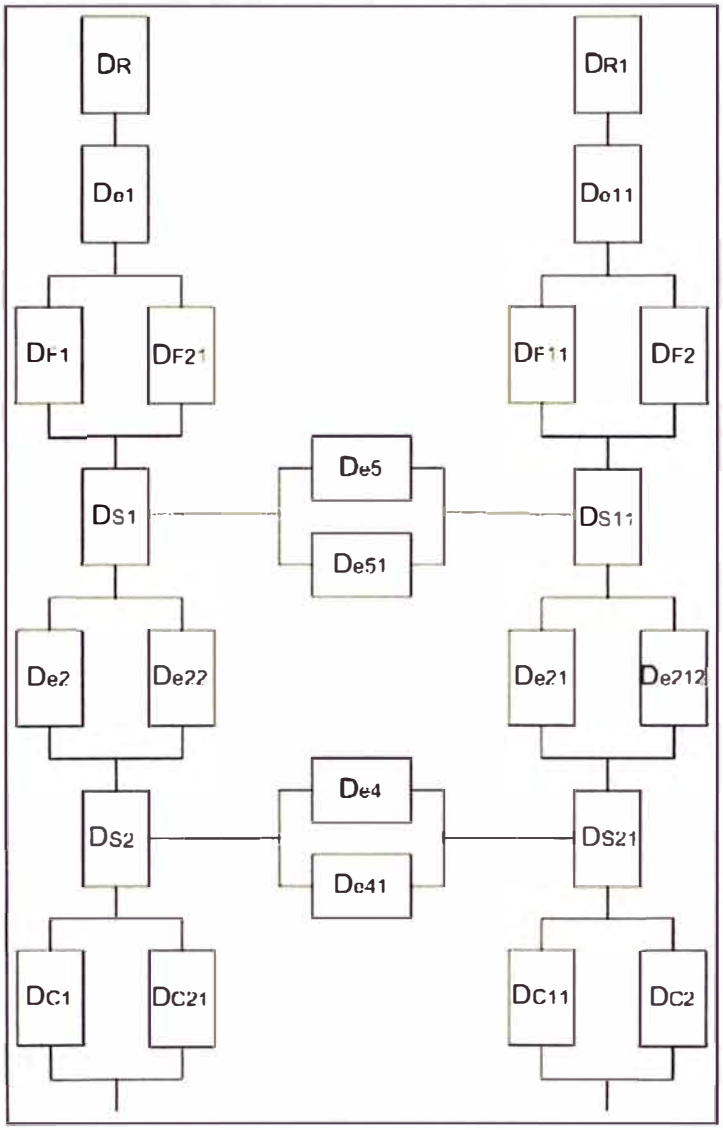

Figura A.4 Tercera alternativa

Luego con las disponibilidades seriales se calcula la disponibilidad del sistema (paralela una a otra). Esta disponibilidad se expresa en la ecuación (A.48) y se resume con la ecuación (A.49).

$$D_{A3} = 1-(1-D_{T1})\times(1-D_{T2})\times(1-D_{T3})\times(1-D_{T4})\times(1-D_{T5})\times(1-D_{T6})\times(1-D_{T7})\times(1-D_{T8}) \quad (A.48)$$

$$D_{A3} = 1-\prod_{i=1}^{8}(1-D_{Ti}) \quad (A.49)$$

Para el caso de la disponibilidad de denegación de servicio (Dd) por la inclusión del ACE esta sube. Se puede asumir un valor mayor que el de la disponibilidad sin el ACE.

Para la seguridad de administración la disponibilidad (Da) es planteada mediante la ecuación (A.50):

$$D_a = 1-(1-D_{enlace}\times D_{ACS})\times(1-D_{enlace1}\times D_{ACS1}) \quad (A.50)$$

Finalmente la ecuación de la alternativa 3 es la siguiente:

$$D_{Alternativa3} = D_{A3}\times D_d \times D_a \quad (A.51)$$

A.5 Evaluación de topologías en cuanto a disponibilidad

De la situación inicial y las alternativas planteadas. La evaluación se hace referente al MTBF de los equipos equivalentes y a los componentes del sistema [25][26][27][28][29][30][31]. En la tabla A.1 se considera el MTTR igual a 4 horas para los dispositivos y enlaces. Para la denegación de servicio se hace referencia a la sección 4.1.2 a la Tabla 4.21.

Tabla A.1 MTBF, MTTR, y disponibilidad de equipos equivalentes y componentes.

Componente	MTBF (horas)	MTTR (horas)	Disponibilidad
WS-C6500E	61320	4	0.999935
Firewall	65576	4	0.999939
Balanceador	259173	4	0.999985
Enlace	175200	4	0.999977
Router	61320	4	0.999935
ACS	41000	4	0.999902
Denegación de servicio (2007)	6480	58	0.991128
Administración de acceso (2007)	6480	58	0.991128

Sistema inicial

Las disponibilidades son calculadas según las ecuaciones A.1 a A.4. El valor de D_{T1} y D_{T2} es igual a 0.999659448, y para D_{T3} y D_{T4} es igual a 0.999571421. Reemplazando estás ecuaciones en la ecuación A.6 el valor de D_S es igual a 1.

Las disponibilidades Dd y Da son iguales a 0.991129, entonces la disponibilidad de la situación inicial es:

$$D_{Inicial} = 98.2336298\%$$

Alternativa 1

Las disponibilidades son calculadas según las ecuaciones A.8 a A.19. El valor de D_F y D_{FF} es igual a 0.999999996279707 y D_{CC} y D_C es igual a 0.999999999761808, para D_{T1} y D_{T2} es igual a 0.998967072, y para D_{T3}, D_{T4}, D_{T5}, D_{T6}, D_{T7}, y D_{T8} es igual a 0.999647817. Reemplazando estos valores en la ecuación A.20, el resultado de D_{A1} es igual a 1.

Considerando Dd igual 0.991129 y Da = 0.99987962 según la ecuación A.22, entonces la disponibilidad de la alternativa 1 es:

$$D_{Alternativa1} = 99.1009488\%$$

Alternativa 2

Las disponibilidades son calculadas según las ecuaciones A.26 a A.33. El valor de D_E y D_{EE} es igual a 0.999999999478767, para D_{T1} y D_{T2} es igual a 0.99973585, para D_{T3}, D_{T4}, D_{T7}, y D_{T8} es igual a 0.99967064, y para D_5, D_6 es igual a 0.999605433. Reemplazando estos valores en la ecuación A.34, el resultado de D_{A2} es igual a 1.

Considerando Dd igual 0.991128 y Da igual a 0.999999986 según la ecuación A.36, entonces la disponibilidad de la alternativa 2 es:

$$D_{Alternativa2} = 99.1128786\%$$

Alternativa 3

Las disponibilidades son calculadas según las ecuaciones A.38 a A.47 El valor de D_{E1} y D_{EE1} es igual a 0.999999999478767, para D_{T1} y D_{T2} es igual a 0.9997815, para D_{T3} y D_4, 0.999716287 D_5, y D_6 es igual a 0.999651077, y para D_7 y D_8 es igual a 0.999716287. Reemplazando estos valores en la ecuación A.48, el resultado de D_{A3} es igual a 1.

Considerando D_d igual 0.999985 y D_a = 0.999999986 según la ecuación A.50 entonces la disponibilidad de la alternativa 3 es:

$$D_{Alternativa3} = 99.9984552\%$$

ANEXO B
DIAGRAMA DE GANTT

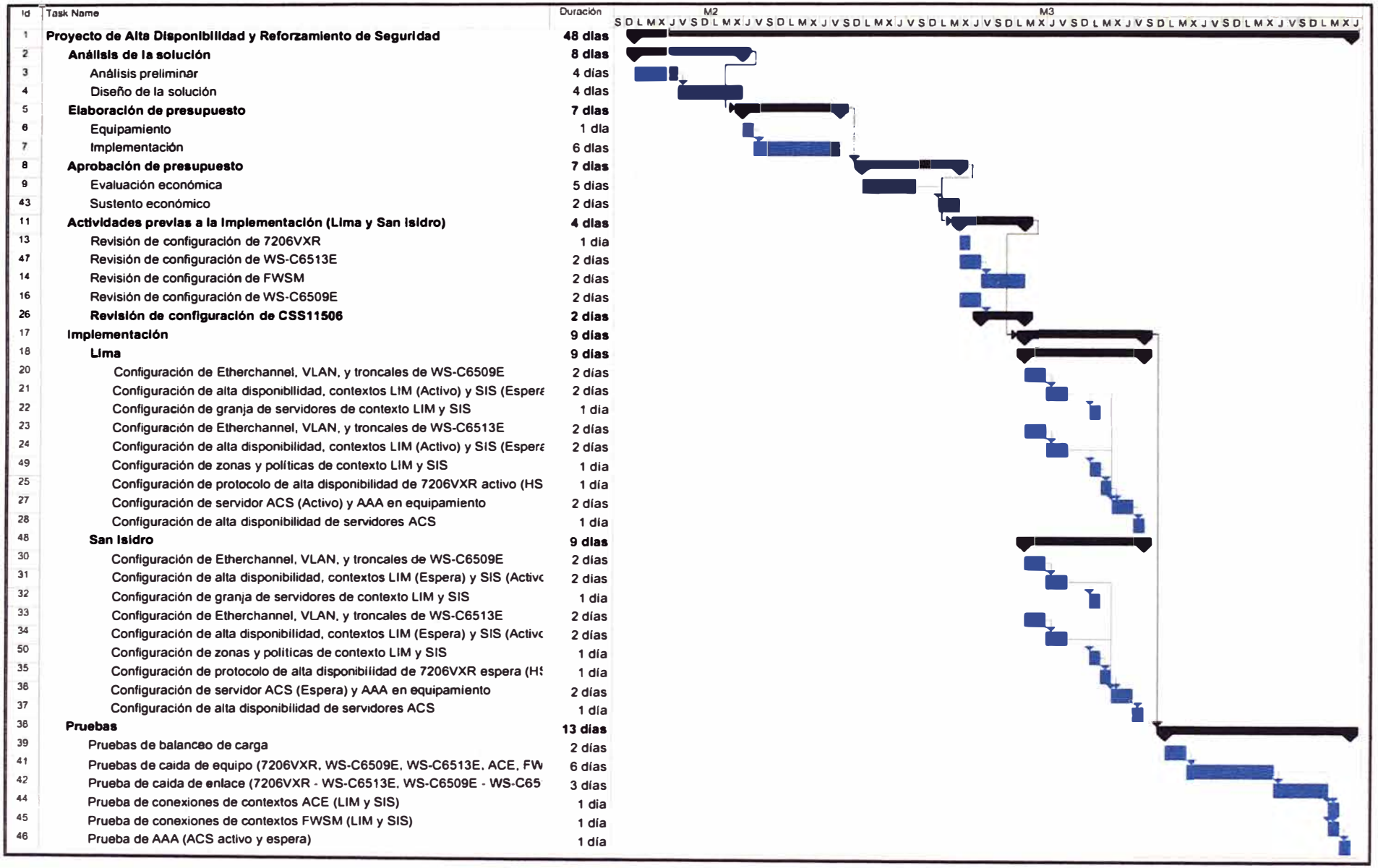

Figura B.1 Diagrama de Gantt

ANEXO C
GLOSARIO DE TÉRMINOS

AAA	Authentication, Authorization, Accounting
ACE	Application Control Engine
ACL	Access Control List
ACS	Access Control Server
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HSRP	Hot Standby Routing Protocol
HTTP	Hypertext Transport Protocol
ICMP	Internet Control Message Protocol
ILS	Internet Locator Service
IP	Internet Protocol
IPS	Intrusion Prevention System
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
NAT	Network Address Translation
RADIUS	Remote Authentication Dial-In User Server
RTSP	Real Time Streaming Protocol
SCCP	Skinny Client Control Protocol
SIP	Session Initiation Protocol
SSH	(Secure Shell)
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

BIBLIOGRAFÍA

[1] Microsoft, "Definición DNS - Windows Server 2003 Ayuda del Producto", 2011, http://technet.microsoft.com/es-es/library/cc787920(WS.10).aspx

[2] Cisco, "Cisco Application Control Engine Module Server Load-Balancing Configuration Guide", Cisco Systems, Inc., 2009 http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA2_3_0/configuration/slb/guide/slbgd.pdf

[3] Cisco, "Academia de Networking de Cisco System: Guía del segundo año CCNA 3 y 4", Cisco Press, 2005.

[4] Cisco, "IEEE 802.3ad Link Bundling", Cisco Systems, 2007. http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sbcelacp.pdf

[5] David Hucaby, "CCNP SWITCH 642-813, Official Certification Guide", Cisco Press", 2010. http://motorola.wirelessbroadbandsupport.com/fp/downlink.php?id=a3ce20684bee2cecba6cf22c42d6098b

[6] Cisco, "Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services - Module Configuration Guide", Cisco Systems Inc., 2007. http://www.cisco.com/en/US/docs/security/fwsm/fwsm32/configuration/guide/fwm32cfg.pdf

[7] David Hucaby, "Cisco ASA, PIX, and FWSM, Firewall Handbook, 2nd Edition", Cisco Press, 2008.

[8] Cisco, "Cisco Application Control Engine Module, Administration Guide", Cisco Systems Inc., 2009, http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA2_3_0/configuration/administration/guide/ace_adgd.pdf

[9] Kevin Wallace, "CCNA Security Official Exam Certification Guide", Cisco Press, 2008.

[10] Matthew Strebe, Charles Perkins, "Firewalls 24Seven, Second Edition", SYBEX Inc., 2002.

[11] Kwok T. Fung, "Network Security Technologies", CRC Press-Auerbach Publications, 2005.

[12] Cisco,"Cisco Application Control Engine Module, Security Configuration Guide", Cisco Systems Inc., 2009.

[13] Cisco, "Security Configuration Guide-Access Control Lists: Overview and Guidelines", http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/scacls.pdf

[14] Noria Latín América, "Proceso de Análisis Integral de Disponibilidad y Confiabilidad como Soporte para Mejoramiento Continuo de las empresas", Noria. 2006. http://www.noria.com/sp/rwla/conferencias/mem/Paper%20Rosendo.pdf

[15] Keith Hutton, Amir Ranjbar, "CCDP Self-Study: Designing Cisco Network Architectures (ARCH)", Cisco Press, 2007.

[16] Dr. Primitivo Reyes Aguilar, "Curso de Confiabilidad", 2006. www.icicm.com/files/CURSO_CONFIABILIDAD.doc

[17] Cisco, "Cisco 7200 VXR Series Routers Overview", Cisco Systems, 2008. http://www.cisco.com/en/US/prod/collateral/routers/ps341/product_data_sheet09186a008008872b.pdf.

[18] Cisco, "Cisco Catalyst 6500 and 6500-E Series Switch", Cisco Systems, 2009. http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916.pdf

[19] Cisco, "Cisco Firewall Services Module for Cisco Catalyst 6500 Series and Cisco 7600 Series", Cisco Systems, 2010. http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps4452/product_data_sheet0900aecd803e69c3.pdf

[20] Cisco, "Cisco ACE Application Control Engine Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers", Cisco Systems, 2010. http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6906/product_data_sheet0900aecd8045861b.pdf

[21] Cisco, "Cisco Secure Access Control Server 4.1", Cisco Systems. 2006. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps2086/ps7032/product_data_sheet09186a00800887d5.pdf

[22] ANSI, "ANSI/TIA-942-2005 Telecommunications Infrastructure Standard for Data Centers", ANSI. 2005 http://www.tiaonline.org/standards/catalog/search.cfm?standards_criteria=TIA-942

[23] Uptime Institute, Sección 3.1 de "Datacenter Site Infraestructure Tier Standard: Topology", Uptime Institute, LLC, 2010

[24] http://uptimeinstitute.org/component/option,com_docman/task,doc_download/gid,90/Itemid,418/

[25] Anixter, "The Purpose of ANSI/TIA/EIA-942 Telecommunications Infrastructure Standard for Data Centers", Anixter. 2009.

[26] http://www.anixter.com/AXECOM/AXEDocLib.nsf/(UnID)/09DF0A00E09C409886257177006611B4/$file/ANSI-TIA-EIA-942.pdf

[27] Cisco, "Cisco Catalyst 6504-E Chassis", Cisco System, 2010. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/ps6771/product_data_sheet0900aecd802b647c.pdf

[28] Juniper, "ISG Series Integrated Security Gateways", Juniper Network, 2010. http://www.juniper.net/us/en/local/pdf/datasheets/1100036-en.pdf

[29] F5, "BIG-IP 6900, 3600, and 1600 FAQ", F5 Networks, 2008. www.firewallsystems.com.au/docs/FAQ_6900_3600_1600_NA.pdf

[30] F5, "sol7407: The mean time between failure (MTBF) for Cavium FIPS cards", F5 Networks, 2011.

[31] http://support.f5.com/kb/en-us/solutions/public/7000/400/sol7407

[32] Siemon, "MapIT G2 Smart Patch Panel", Siemon, 2010.

[33] http://files.siemon.com/int-download-product-specsheets-us/mapit_mapit-g2-smart-patch-panel_ss.pdf

[34] Cisco, "Cisco 7606 Chassis", Cisco System, 2010.
http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps371/product_data_sheet09186a0080088773.pdf

[35] Cisco, "Technical Specifications for the Cisco 1113", Cisco System, 2009.
http://www.ciscosystems.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2.1/Installation_Guide/solution_engine/spcsap.pdf