UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA MECÁNICA, ELECTRÓNICA Y AMBIENTAL

CARRERA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"DISEÑO DE LA ARQUITECTURA Y OPERACIÓN DE UNA RED LAN EN SUS CAPAS DE ACCESO, DISTRIBUCIÓN Y SEGURIDAD PARA UNA EMPRESA DE SUMINISTRO ELÉCTRICO"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

FAUSTOR CASTRO, DANIEL JONATHAN

Villa El Salvador
2015

DEDICATORIA

La presente tesis se la dedico a mi familia especialmente a mis padres, que gracias a su apoyo pude concluir mi carrera. También a mis hermanas por su apoyo y su confianza que pusieron en mí para poder cumplir mis objetivos como persona y estudiante y a mi novia por el constante apoyo en este largo camino.

AGRADECIMIENTO

Mi más profundo agradecimiento a mi asesores, por sus consejos y recomendaciones para poder elaborar la presente tesis, sin su incondicional aporte en brindarme sus conocimientos y/o experiencias, no podría haber sido posible, en este proceso de elaboración de mi proyecto de tesis**.**

INDICE

LISTADO DE FIGURAS

Capítulo 3

LISTADO DE TABLAS

INTRODUCCIÓN

El presente trabajo tiene la finalidad de dar evidencia de una arquitectura de red de una empresa que no cuenta con alta disponibilidad de enlaces a nivel de capa acceso, distribución y capa de nucleó, lo que hoy en día al ritmo que crece la tecnología se le puedo denominar acceso fiable hacia internet.

Mostrar las características de los equipos que actualmente presenta la Empresa, de su diseño actual y no escalable en algunos términos de contingencia de enlaces, mediante el uso de diagramas de red demostrar los puntos de falla de los equipos y conexiones.

Finalmente dar a conocer una arquitectura estable a nivel de enlaces redundantes en los noveles de acceso, distribución y nucleó basados en este trabajo como red interna y red externa. Verificar el diseño mediante diagramas que dan evidencia de un diseño estable y las características de los equipo de acceso para poder realizar una innovación tecnológica basado en alta disponibilidad, seguridad perimetral en los equipos mencionados en la nueva arquitectura para la Empresa

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

En el mundo en el que nos desarrollamos y convivimos en la actualidad, la comunicación es un medio muy importante por el cual podemos tener intercambio de expresiones (recepción y transmisión) de elementos de la comunicación.

Para lo cual al vivir en un mundo tan versátil, donde la forma de recibir y transmitir datos a gran velocidad es un proceso que conlleva la necesidad de no tener perdida (latencia), pérdidas de paquetes y la información. Donde los elementos que están presentes en este proceso (receptor / emisor), no se encuentren perjudicados al momento de realizar este proceso. En la actualidad una entidad, empresa (privada y/o pública), buscan la interconexión con el mundo vía internet, que es un medio por el cual las masas pueden realizar diversas acciones como (enviar archivos, carpetas comprimidas, fotos, videos) información muy importante para las entidades que utilizan este medio de comunicaciones problema se presenta al momento que esta información se ve interrumpida por factores ya sea

por hardware y/o software de los equipos encargados de realizar la transmisión y recepción de la comunicaron (Internet). Al ser un medio de vital importancia y con un porcentaje de disponibilidad que no se puede ver afectada.

Hoy por día existen centros de trabajos (privados y públicos), que no cuentan con infraestructura muy acorde con el cambio tecnológico en los equipos de comunicación vía internet como lo son conmutadores y equipos de capa de transporte y acceso hasta llegar hacia el usuario final, tener el criterio de que los trabajadores no se ven afectados en sus labores cotidianas (distintas áreas de un centro laboral). El problema se denota con mayor intensidad cuando dicha entidad, no tiene acceso hacia internet donde se encuentran servicios publicados, páginas web, páginas de correos, páginas de archivos compartidos, acceso hacia la red vía remota, acceso interno hacia servidores donde se encuentran servicios de usuarios locales, que se pueden ver afectados por equipos con un tiempo de disponibilidad ya muy elevado, para la comunicación actual.

1.2. Justificación del Problema

Ante la necesidad de tener comunicación hacia internet y sin la presencia de pérdidas hacia dicho medio, así como la de controlar a los usuarios finales hacia el acceso hacia internet(trabajadores de la entidad), y poder presentar un diseño de arquitectura de red que sea estable y contar con equipos de capa 2 que tengan la funcionalidad de ser configurados en capa 3 y lograr optimizar una red tal sentido, para que los enlaces de internet que presente la entidad o institución no se vean afectados, ante la caída de equipos por diversos factores sea

(humanos y/o artificiales), manipulación inadecuada de equipos de red y/o fallas eléctricas, para los equipos que intervienen en el proceso de comunicación como lo son los switches (interruptores) , Router (conmutadores) , equipos de seguridad como firewall que son herramientas hardware y software que mantienen una red protegida ante ataques desde internet, hasta equipos que controlen el flujo del ancho de banda en los usuarios finales con el acceso hacia internet.

1.3. Delimitación del Proyecto

1.3.1. Delimitación espacial: Se considera para el diseño de la red con alta disponibilidad de enlaces, seguridad en la red de datos de una empresa dedicada al rubro de energía en toda su infraestructura de equipos de comunicación de datos. (Datacenter y gabinetes).

1.3.2. Delimitación Temporal: El diseño de la arquitectura y fundamentos se llevó acabo en el mes de marzo del 2015.

1.4. Formulación del Problema

1.4.1. Problema principal

¿Cómo la innovación tecnológica en equipamiento para acceso de internet puede contribuir para una mejora en el acceso de comunicación a una empresa pública y/o privada, manteniendo sus enlaces de internet en alta disponibilidad, capas de acceso, distribución y seguridad en la red LAN?

1.5. Objetivos.

1.5.1. Objetivo General

Dar a conocer una solución de alta disponibilidad de enlace de internet, capas de acceso, distribución y seguridad en la red LAN, ante eventuales fallas, (humanas o artificiales) para una empresa eléctrica en su red de datos.

1.5.2. Objetivos Específicos

1. La contribución de un arquitectura estable a nivel de enrutamiento, seguridad y administración de ancho de banda, contribuyen para que una empresa mediante estas herramientas de hardware y software pueda saber administrar sus servicios y/o recursos, ante la demanda de atención, para los procesos generados como institución y dar a conocer mediante el desarrollo del presente trabajo la alta disponibilidad de los equipos para la satisfacción de los usuarios finales (trabajadores de la entidad, institución pública y/o privada).

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

En la tesis elaborada con el nombre Infraestructura de comercio electrónico en

Alta disponibilidad de José Christian Bradna Villanueva [1] donde encontramos definición de alta disponibilidad y las características de un equipo establecido como clúster entre el flujo y envió de datos. Internet, una red de datos que une al mundo, proporciona gran diversidad de servicios a sus usuarios. Internet abre nuevas oportunidad, y crean nuevos retos, los negocios pueden llegar a un número mayor de clientes, y mantener servicio a las mismas 24 horas al día 365 días al año, en forma continua, alrededor del globo terrestre. Todo esto apoya por tecnología de punta y en la cual se requieren altos niveles de disponibilidad.

[1] José Christian Bradna Villanueva con el título “Infraestructura de comercio electrónico en Alta disponibilidad “ Guatemala, octubre 2,004(tesis), Universidad de San Carlos de Guatemala Facultad de Ingeniería

Una solución de comercio electrónica, tiene tres características claves desde el punto de vista de la infraestructura, que son: alta disponibilidad, escalabilidad, y seguridad. Estas características deben observarse en toda la arquitectura de la solución en cada una de sus capas de hardware y software. La alta disponibilidad es la habilidad para proveer acceso continuo a los servicios de comercio electrónico para los clientes. Un requisito fundamental para los negocios en Internet disponible 24 horas al día.

Examinaremos las opciones que ofrece el mercado para alta disponibilidad a nivel de redes de datos, servidores, sistemas operativos, y bases de datos, también se examina qué se ofrece en las herramientas de administración de redes fundamental para completar la arquitectura de alta disponibilidad.

Por último, se tocarán los procedimientos necesarios para asegurar la alta disponibilidad, basados en las mejores prácticas y recomendaciones de los proveedores líderes en el mercado. Lo mejor en hardware y software no podrán asegurar la alta disponibilidad de un sitio de comercio electrónico, si no son correctamente administrados [2]

[2] José Christian Bradna Villanueva con el título “Infraestructura de comercio electrónico en Alta disponibilidad “ Guatemala, octubre 2,004(tesis), Universidad de San Carlos de Guatemala Facultad de Ingeniería

De la tesis con el título “Análisis, diseño y optimización de una red local con Intervlan troncalizadas y seguridad de acceso mediante la aplicación de acls” de Pedro José Solís Sánchez y María Auxiliadora Desiderio Rodrigo [3], se diseña una red local con 3 Vlans, las cuales se comunican entre ellas de manera troncalizada, para este propósito el autor emplea un router que permite la comunicación entre ellas. Realiza pruebas de conectividad entre los distintos dispositivos que conformaron nuestra red, aplicando cada uno de los protocolos de enrutamiento, emplea una comunicación escogimos en base a la escalabilidad y convergencia, sobre la configuración de los routers con el protocolo seleccionado se aplicaron ACLS a las interfaces tanto físicas como virtuales de los routers, con lo cual comprobamos el correcto funcionamiento de las ACLS.También el autor efectúa pruebas de redundancia aplicando Etherchanel, tecnología propietaria de CISCO, y simula caídas de enlace, verificando de esta manera la continuidad de la conectividad de nuestra red.

[3] Pedro José Solís Sánchez y María Auxiliadora Desiderio Rodrigo con el título Análisis, diseño y optimización de una red local con Intervlan troncalizadas y seguridad de acceso mediante la aplicación de acls” ESCUELA SUPERIOR POLITECNICA DEL LITORAL Facultad de Ingeniería en Electricidad y Computación 2005.

2.2 Bases Teóricas

Se desarrolla bajo este concepto los siguientes temas, modelo OSI, alta disponibilidad, seguridad perimetral y todos sus componentes y administrador de ancho de banda, equipos switch como acceso y Core toda aplicación y modelos de funcionamiento para el entendimiento en este sentido.

2.2.1 El modelo OSI

Durante las últimas dos décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Muchas de ellas sin embargo, se desarrollaron utilizando implementaciones de hardware y software diferentes. Como resultado, muchas de las redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder comunicarse entre sí. Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984.

2.2.1.1 El modelo de referencia OSI

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos.

Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

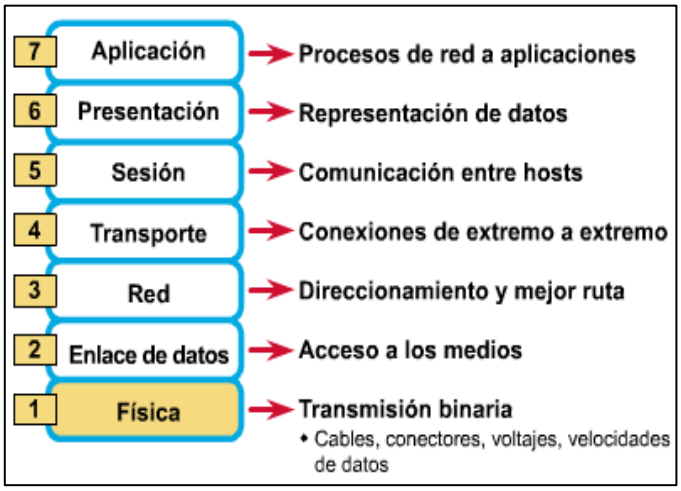


Figura 2.1 Capas del Modelo OSI

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aun cuando el transmisor y el receptor tengan distintos tipos de medios de red. En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina división en capas. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

2.2.1.2 Las siete capas del modelo de referencia OSI

El problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo.

Las siete capas del modelo de referencia OSI son:

Capa 7: La capa de aplicación La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y

establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Capa 6: La capa de presentación La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Capa 5: La capa de sesión Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Capa 4: La capa de transporte La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos. La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de

implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

Capa 3: La capa de red La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Capa 2: La capa de enlace de datos La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Capa 1: La capa física La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física.

2.2.2. Alta disponibilidad

En un mundo tan globalizado en donde los sistemas de comunicación siempre están transmitiendo datos a gran velocidad, y con llegada a usuarios finales, mediante el manejo de equipos componentes de estos sistemas (vía internet, comunicación satelital, voz , datos y demás medios por el cual se puede compartir información), pero esto no solo se basa en recibir y poder transmitir datos, la necesidad del ser humano de siempre presentar una disponibilidad o continuidad de un servicio sin ser afectado directamente , es lo que se busca con la alta disponibilidad.

La Alta Disponibilidad se puede entender de la siguiente manera, se refiere a la capacidad de un conjunto y/o agrupación de usuarios finales (personas que disponen de un componente que le brinda la facilidad de comunicación e interacción con otro medio), para acceder a un sistema donde se encuentran recursos para sus labores cotidianas. Mientras que los usuarios no pueden acceder a los recursos o sistemas necesarios, se le denomina de forma general tiempo de inactividad.

Por ende la forma de como poder mencionar el porcentaje de alta disponibilidad por un determinado periodo ya establecido, se basa por la actividad de disponibilidad de los equipos, cabe resaltar que funcionamiento no es una definición de mencionar a un sistema disponible, ya que pueden estar equipos o sistemas funcionando correctamente, pero a su vez no disponibles en caso de presentar fallas de los equipos de red.

La alta disponibilidad se aplica a toda la gama de soluciones que sostienen los sistemas de información de las empresas: bases de datos, cortafuegos, servidores web, etc. Si bien, los mecanismos que se emplean pueden ser distintos en función del entorno, los modelos actuales permiten tener equipos dedicados para determinar la disponibilidad y mantener un funcionamiento continuo con todos los sistemas sin perjudicar al usuario final.

Para determinar el modo de procedimiento, se tienen los siguientes conceptos:

2.2.2.1 Activo-Pasivo

El criterio de poder establecer un modo de funcionamiento, contando con todos los servicios que componen el sistema de información al que denominaremos Activo, y el otro nodo que se denominará Pasivo en el que se encuentran duplicados todos estos servicios, pero detenidos a espera de que se produzca un fallo.

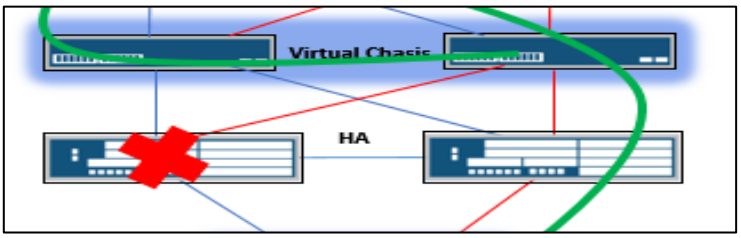


Figura 2.2 Equipo que representa el estado activo pasivo ante una falla.

2.2.2.2 Activo-Activo

La configuración de "alta disponibilidad" en activo-activo es muy similar a la de activo-pasivo, aunque en este caso los dos nodos comparten los servicios de una

manera activa, normalmente balanceados, consiguiendo una disponibilidad mayor ya que los servicios se entregan antes.

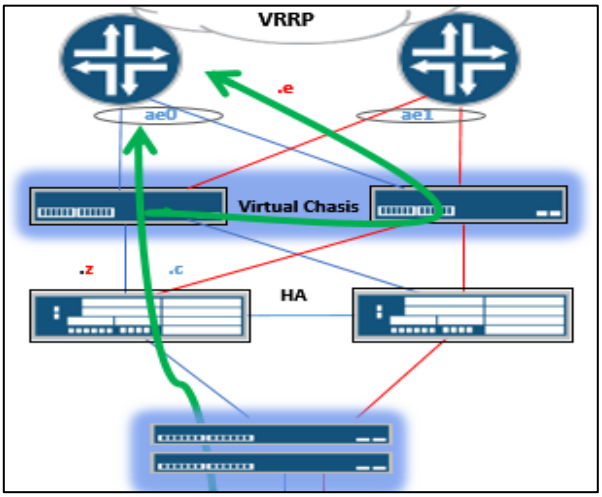


Figura 2.3 Equipos configurados que representa el estado activo activo.

2.2.2.3 Conjunto de servidores

Normalmente orientado a servicios web, servicios computacionales que se entregan de forma masiva, como puedan ser servicios terminales. En estas configuraciones no solo es importante la fiabilidad, también es importante contar con un sistema muy disponible por lo que se suelen colocar un gran número de máquinas haciendo una tarea común. Esta configuración siempre nos va a permitir que en caso de que un nodo deje de hacer su función otro asuma su rol.

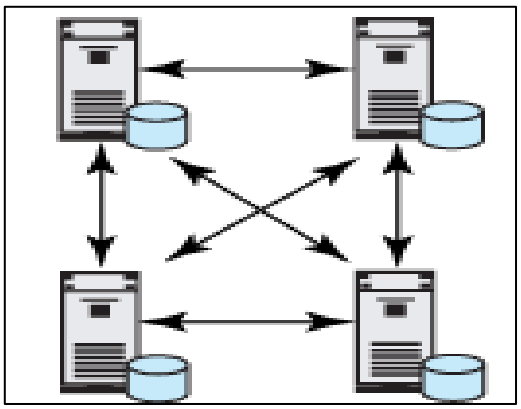


Figura 2.4 Servidores en alta disponibilidad

Los principios básicos de la alta disponibilidad que normalmente y muy a menudo es expresado en medio de las telecomunicaciones con las siglas H.A qué significa High availability, de lo cual los siguientes conceptos básicos para su respectivo entendimiento:

Fiabilidad.- Marca la medida en la que un dispositivo computacional se mantiene activo.

Disponibilidad.- La medida en la que un sistema de información está preparado para su uso.

Confiabilidad.-Grado de eficacia del sistema de información.

Failover.- Configuración de mínimo dos nodos en el que, en un momento dado y debido a cierta casuística, un nodo continua activo en vez del otro.

TakeOver.- Failover automático, cuando un fallo es detectado a partir de una monitorización.

2.2.3. Seguridad de la red de datos

En la actualidad la seguridad e integridad informática de una empresa es primordial. Los ataques por red y pérdidas de información ocasionan un gran trastorno y no solo la imagen si no también el funcionamiento y progreso de una empresa se ven afectados.

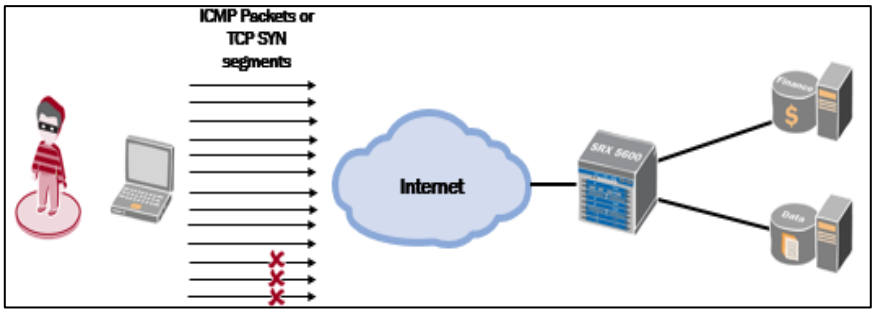


Figura 2.5 Atacantes y su intento de ingreso a una red

Todo lo que se realiza en base para la seguridad de la información en las empresas de distintos sectores públicos y privados, se manifiesta en equipos que brinden este fortalecimiento en la red, en todos los sectores los administradores de red tratan de resguardar información, por ese motivo la factibilidad que realizan en su red interna un escaneo de las vulnerabilidades, desde tener un equipo en su red interna que genere lentitud, que genere mucho tráfico hasta un dispositivo periférico como usb (dispositivo de almacenamiento portátil), que pueden tener presencia de malware que se puede propagar en la red.

Una red que presente estos síntomas nos indica la posible presencia de los siguientes factores de infección y los dispositivos que son generadores desde la red interna como la red externa.

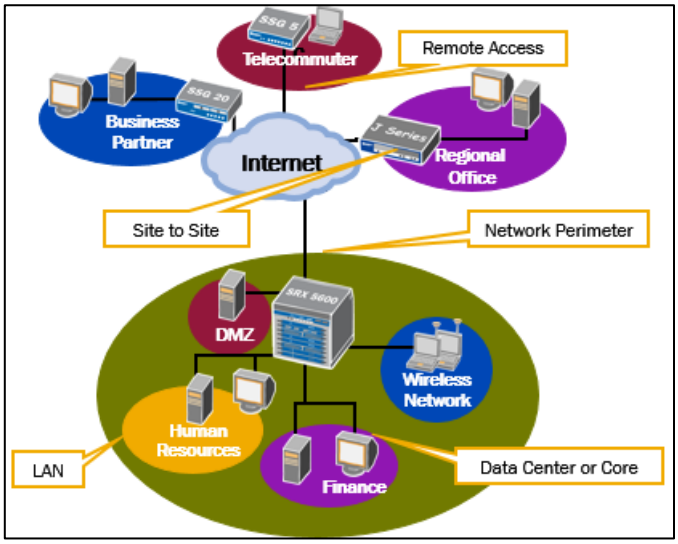


Figura 2.6 Las distintas áreas en una red que se ven amenazadas ante problemas de seguridad perimetral

Como definición de la coyuntura de infección en una red interna se tiene que mencionar los siguientes virus que perjudican a todos los usuarios de una institución que se ven en la necesidad de tener acceso hacia internet o una red interna.

Se define lo antes mencionado de la siguiente manera:

Malware: que es la definición de todo sistema que tenga mala reputación en la red mediante el acceso a información no permitida, su abreviatura se da razón como malicious software, término que define para todo tipo de programa o código informático malicioso cuya función dañar, dejar sin funcionamiento a un sistema.

Dentro de la cantidad se sistemas que pueden causar estos sistemas en la red se menciona los siguientes términos.

Virus: es la definición de programas maliciosos que su objetivo principal es de intentar o lograr infectan a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo denominado como víctima , que puede ser archivos compartidos, mediante descargas, (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección. Su nombre lo adoptan de la similitud que tienen con los virus biológicos que afectan a los humanos, donde los antibióticos en este caso serían los programas Antivirus.

Adware: es un software que despliega publicidad de distintos productos o servicios todo esto incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario. Generalmente, agregan ícono gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo, la cuales tienen palabras claves predefinidas para que el usuario llegue a sitios con publicidad, sea lo que sea que esté buscando.

Backdoors: son programas diseñados para abrir una “puerta trasera” en nuestro sistema de modo tal de permitir al creador de esta aplicación tener acceso al sistema y hacer lo que desee con él. El objetivo es lograr una gran cantidad de

computadoras infectadas para disponer de ellos libremente hasta el punto de formas redes como se describen a continuación.

Botnet: es un malware del tipo bot es aquel que está diseñado para armar botnets los cuales constituyen una de las principales amenazas en la actualidad. Una Botnet es una red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cuando una computadora ha sido afectado por un malware de este tipo, se dice que es un equipo es un robot o zombi.

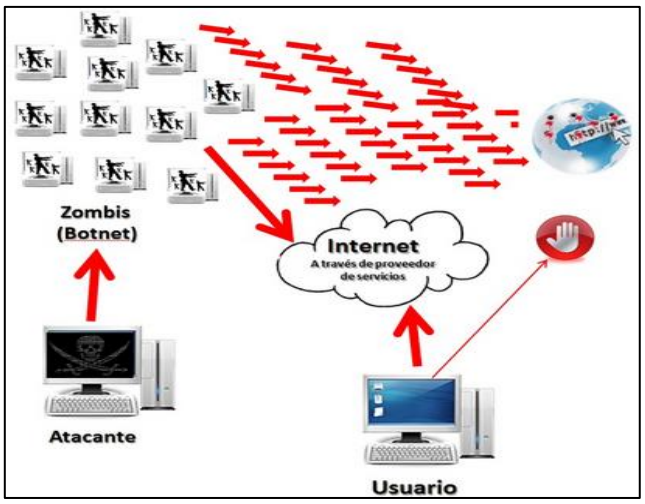


Figura 2.7 Ataques de denegación de servicio

Gusanos: Los gusanos son en realidad un sub-conjunto de malware. Su principal diferencia con los virus radica en que no necesitan de un archivo anfitrión para seguir vivos. Los gusanos pueden reproducirse utilizando diferentes medios de comunicación como las redes locales, el correo electrónico, los programas de mensajería instantánea, redes P2P, dispositivos USBs y las redes sociales.

Hoax: es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores, que algo falso es real. A diferencia de otras amenazas, como el phishing o el scam; los hoax no poseen fines lucrativos, por lo menos como fin principal.

Hijacker: son los encargados de secuestras las funciones de nuestro navegador web (browser) modificando la página de inicio y búsqueda por alguna de su red de afiliados maliciosos, entre otros ajustes que bloquea para impedir sean vueltos a restaurar por parte del usuario. Generalmente suelen ser parte de los Adwares y Troyanos. Uno de los principales factores de robo de información es mediante los procesos de cifrado de contraseñas, que son usadas por el usuario para acceso a correo, aplicaciones internas y archivos confidenciales para la empresa.

Keylogger: Aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado (Capturadores de Teclado). Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.

Phishing: consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

PUP: (Programa potencialmente no deseado) que se instala sin el consentimiento del usuario y realiza acciones o tiene características que pueden menoscabar el

control del usuario sobre su privacidad, confidencialidad, uso de recursos del ordenador, etc.

Rogue: software es básicamente un programa falso que dice ser o hacer algo que no es. Con la proliferación del spyware estos comenzaron a surgir como un importante negocio para los ciberdelincuentes en formato de “Falso Antispyware”. Con el tiempo fueron evolucionando creando desde “Falsos Optimizadores” de Windows, y en los más extendidos “Falsos Antivirus”.

Riskware: Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas.

Rootkit: Los rootkits son la cremé de la cremé de malware, funcionando de una manera no muy diferente a las unidades de elite de las fuerzas especiales: colarse, establecer comunicaciones con la sede, las defensas de reconocimiento, y el ataque de fuerza. Si se detectan y se hacen intentos por eliminarlas, todo el infierno se desata. Cada removedor de rootkit que se precie advierte que la eliminación del rootkit podría causar problemas para el sistema operativo, hasta el punto de donde no podrá arrancar.

Eso es porque el rootkit se entierra profundamente en el sistema operativo, en sustitución de los archivos críticos con aquellos bajo el control del rootkit. Y cuando los archivos reemplazados asociados con el rootkit se retiran, el sistema operativo puede ser inutilizado.

Otro generador de infección en una red viene dado por los correos spam que ingresan hacia la bandeja de entrada de un usuario, este tipo de infección es común para en robo de contraseñas bancarias, mediante publicidad falsa, el termino spam lo explicamos de la siguiente manera.

Spam: se denomina spam al correo electrónico no solicitado enviado masivamente por parte de un tercero. En español, también es identificado como correo no deseado o correo basura.

Troyano: un troyano no es virus, ya que no cumple con todas las características de los mismos, pero debido a que estas amenazas pueden propagarse de igual manera, suele incluírselos dentro del mismo grupo. Un troyano es un pequeño programa generalmente alojado dentro de otra aplicación (un archivo) normal. Su objetivo es pasar inadvertido al usuario e instalarse en el sistema cuando este ejecuta el archivo “huésped”. Luego de instalarse, pueden realizar las más diversas tareas, ocultas al usuario. Actualmente se los utiliza para la instalación de otros malware como backdoors y permitir el acceso al sistema al creador de la amenaza. Algunos troyanos, los menos, simulan realizar una función útil al usuario a la vez que también realizan la acción dañina. La similitud con el “caballo de Troya” de los griegos es evidente y debido a esa característica recibieron su nombre.

Spyware: es un software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas.

Normalmente, este software envía información a sus servidores, en función a los hábitos de navegación del usuario. También, recogen datos acerca de las webs que se navegan y la información que se solicita en esos sitios, así como direcciones ip y urls que se visitan. Esta información es explotada para propósitos de mercadotecnia, y muchas veces es el origen de otra plaga como el spam, ya que pueden encarar publicidad personalizada hacia el usuario afectado. Con esta información, además es posible crear perfiles estadísticos de los hábitos de los internautas. Ambos tipos de software generalmente suelen “disfrazarse” de aplicaciones útiles y que cumplen una función al usuario, además de auto ofrecer su descarga en muchos sitios reconocidos.

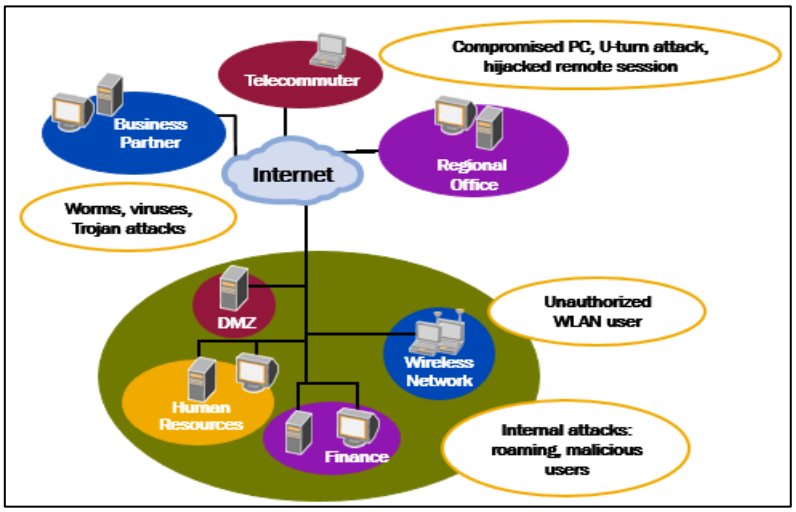


Figura 2.8 Red vulnerable a los ataques mencionados

2.2.4 Firewalls y/o Cortafuegos

Un problema de seguridad que afecta a los datos que mantienen en sus sistemas privados así como aquellos que son enviados a sitios remotos de la red. Los

firewalls ofrecen una solución a estos problemas y ha surgido una amplia variedad de tecnologías y estrategias de entre las cuales se encuentran, como innovación de los últimos tiempos, los Cortafuegos distribuidos, que permiten establecer políticas más flexibles y robustas que los sistemas convencionales que dependen fuertemente de la topología de la red sobre la cual se implementen.

Un firewall es la combinación de diferentes componentes: dispositivos físicos (hardware), programas (software) y actividades de administración, que, en conjunto, permitirán aplicar una política de seguridad de una red, haciendo efectiva una estrategia particular, para restringir el acceso entre ésta red y la red pública a la cual esté conectada. El objetivo es protegerla de cualquier acción hostil proveniente de un host externo1 a la red.

La función de un firewall es tal que todo el tráfico de entrada y salida de la red privada debe pasar a través de él; el tráfico permitido por el firewall es autorizado mediante su evaluación en base a la política de seguridad.

El enfoque de firewalls está basado en el concepto de permitir a los usuarios locales el uso de todos los servicios de red internos a su red local y otros servicios ofrecidos por Internet, controlando, además, el acceso de los usuarios externos a los recursos de la red local.

2.2.4.1 Necesidad de seguridad

La gran demanda de controlar a los usuarios hacia los recursos internos de la empresa y/o institución mediante aplicativos como servidores, intranet todo esto es posible mediante el uso de los ordenadores que se han convertido en la herramienta esencial para el manejo de información en nuestra vida cotidiana y más aún en la actividad diaria de una empresa. Como consecuencia ha surgido una necesidad de compartir información entre usuarios y entre estos y organizaciones o empresas. Esta necesidad ha sido dirigida por dos fuerzas: los laboratorios y proyectos de investigación, que ante la necesidad de colaboración necesitaron compartir información entre diferentes grupos situados en lugares remotos y desarrollaron protocolos y métodos para transferir datos (como por ejemplo TCP/IP); y por otro lado los intereses de las empresas, la necesidad de mejorar el intercambio de información corporativa entre oficinas o edificios llevó al desarrollo de varios protocolos desarrollados para estos fines.

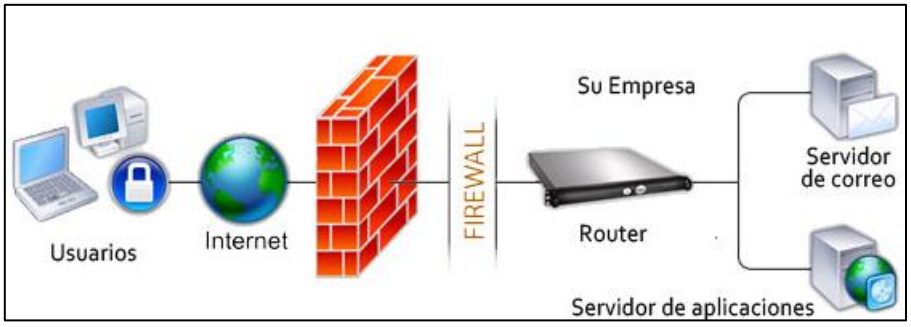


Figura 2.9 Representación de un equipo de seguridad

Posteriormente, la necesidad de comunicación se extendió a grandes áreas y surgieron nuevas industrias en la manipulación de routers, gateway y otros dispositivos para posibilitar tal transmisión de datos. Así mismo se estableció una tendencia al uso de protocolos estándares de uso común entre multitud de organizaciones que les permitiría intercomunicarse de forma apropiada.

La necesidad de empresas de poder comunicarse entre sucursales la necesidad de encontrar una solución de poder brindar acceso y controlar redes desde una zonal, la creación de usuarios, gestionar los aplicativos, la publicación de servicios hacia internet, dar acceso a la red interna, controlar al usuario final, actualización de equipos que permiten que una red permanezca estable, mediante software y herramientas de navegación.

A la par de este crecimiento surgieron varios aspectos importantes como lo es el de la seguridad de la información. La mayor parte de las compañías utilizan Internet como herramienta clave para realizar sus negocios y dependen de ella para continuar existiendo, lo que puede llevar a exponer información privada poniendo en peligro la confidencialidad de sus operaciones. Muchas organizaciones ofrecen servicios mediante sus sistemas de comunicación, la efectividad de tales servicios requiere el acceso a recursos críticos del sistema de información de la empresa (archivos, dispositivos de almacenamiento, líneas telefónicas, etc.). Dichos recursos deben ser protegidos contra el uso indiscriminado y malicioso por parte de usuarios no deseados. Si un sistema de comunicación es vulnerable a estos tipos de ataques, el riesgo de pérdida de

datos es importante. Este riesgo potencial de seguridad aumenta junto con el nivel de dependencia en tecnología de información, lo que requiere el uso sistemas de seguridad más confiable y robusta.

Actualmente la vulnerabilidad de la red se puede resumir de los siguientes aspectos muy importantes y que influyen en el manejo de todos los servicios:

- Existen muchos puntos vulnerables desde donde puede ser lanzado un ataque (red interna / red externa).
- El perímetro físico del sistema de comunicación se ha extendido, existiendo mensajes de entrada y salida, manteniendo contacto con todos los otros sistemas conectados a la red,
- Las redes ofrecen múltiples servicios de conexión, cada uno con un punto de acceso propio. Cada uno de estos requiere una protección adecuada contra intrusos y cada una ofrece una complejidad y dificultad propia.

Las organizaciones poseen un conjunto de ordenadores conectadas a la red propia y al exterior, que deben ser capaces de establecer comunicaciones fiables con cualquier dispositivo en la red. Puesto de esta forma, parece ser una tarea bastante complicada en lo que a seguridad se refiere. Afortunadamente, la red puede ser configurada de manera que solo un ordenador necesite comunicarse con el exterior (un gateway) y suele ser el principio de un plan de seguridad.

2.2.4.2 Requerimientos funcionales de una solución de seguridad

La implementación de un buen sistema de seguridad requiere el uso de ciertas funciones que permitirán asegurar la confidencialidad e integridad de los recursos de nuestra red contra las intrusiones. Con este planteamiento, surgen algunas cuestiones previas a la elección de las tecnologías a utilizar, que deberán ser resueltas al momento de implementar un mecanismo de seguridad efectivo para una red:

Cuando nos referimos al cuidado o la seguridad de la red tenemos que mencionar la seguridad externa y/o interna, lo podemos mencionar como un determinado host posee ciertos recursos y tiene acceso a otros recursos de la red. Deben determinarse qué recursos son críticos para la organización y deben, por lo tanto, ser protegidos contra el acceso de intrusos. Tales recursos pueden ser archivos confidenciales, dispositivos de almacenamiento u otro tipo, líneas de conexiones, etc. Estas decisiones determinarán las medidas a tomar o estrategia que asegurarán la aplicación de los permisos de acceso a los recursos para cada posible usuario (host confiable o no); por ejemplo, si queremos proteger todos esos recursos, debemos efectuar un control en un punto previo a la entrada a la red local.

Estas decisiones deben tomar en consideración otra cuestión referida a dónde se originan los problemas de seguridad, es decir contra quién defendemos nuestros sistemas .Es posible que un intruso asuma la identidad de un host confiable para

la red y tenga acceso a recursos que de otra forma no tendría. Además debemos tener en cuenta qué tan severo sería que la seguridad sea quebrada y los recursos de la red sean accedidos por usuarios no deseables.

El objetivo es que esto nunca suceda por lo que podríamos decidir implementar una estrategia severa con mecanismos de alta calidad, pero estamos dejando de lado otro importante factor. Esto se relaciona, en cierta forma, con que tan deseables son los recursos de nuestra organización para los usuarios de la red externa, aunque es una cuestión un tanto discutible y muy relativa.

El objetivo de una solución de seguridad es “aislar” el segmento de la red local del resto de Internet y controlar el tráfico que llega y sale de ella. De aquí surgen dos aspectos básicos a cubrir por una solución de seguridad para redes, seguridad en tránsito y regulación de tráfico, los cuales, cuando son combinados, ayudan a garantizar que la información correcta sea entregada de forma segura al lugar correcto. Existe también la necesidad de asegurar que los hosts que reciban la información, la procesen apropiadamente, de aquí surge el espectro completo de seguridad de los hosts.

2.2.4.3 Funciones principales de un Firewall

Un firewall permite proteger una red privada contra cualquier acción hostil, al limitar su exposición a una red no confiable2 aplicando mecanismos de control para restringir el acceso desde y hacia ella al nivel definido en la política de

seguridad. Generalmente un firewall es utilizado para hacer de intermediario entre una red de una organización e Internet u otra red no confiable.

Estos mecanismos de control actúan sobre los medios de comunicación entre las dos redes, en particular, sobre la familia de protocolos utilizada para la comunicación de sistemas remotos. La más comúnmente usada es TCP/IP ya que dispone de amplios desarrollos de mecanismos estándares para su uso en varios aspectos, incluyendo en seguridad.

La tarea de un firewall consiste en inspeccionar y controlar todo el tráfico entre la red local e Internet. De esta forma se intenta detectar y rechazar todo el tráfico potencialmente peligroso antes de que alcance otras partes de la red interna, en algunos casos también se efectúan registros de tales actividades. La determinación de qué es peligroso para la red local, es especificada en la política de seguridad adoptada por el sitio.

La protección que provee un firewall es de diferentes tipos:

- Bloqueo de tráfico no deseado
- Redirección de tráfico de entrada a sistemas internos de más confianza
- Ocultar sistemas de Internet
- Registro de tráfico desde y hacia la red privada

- Ocultar información como ser nombres de sistemas, topología de la red, tipos de dispositivos de red, e identificadores de usuarios internos de Internet

El firewall permite lograr esta protección aislando el segmento de la topología correspondiente a la red local del resto de Internet, controlando todo el tráfico que llega y sale de la misma.

Un firewall ayuda a manejar una variedad de aspectos en el punto de acceso a la red pública manteniendo a los intrusos fuera, mientras permite a la red interna concentrarse en ofrecer sus servicios. La idea básica es permitir a los usuarios de una red protegida acceder a una red pública y al mismo tiempo hacer disponibles a la red pública los servicios y productos de la compañía, ofrecidos por esta red protegida.

El control de acceso que ofrece un firewall a un sistema de red permite que algunos servidores pueden hacerse disponibles desde la red externa, mientras otros puedan ser cerrados del acceso externo no deseado. Previniendo, de esta forma, que los servicios inseguros o vulnerables sean explotados por atacantes externos, es posible el uso de estos servicios con un riesgo reducido de exposición ya que solo algunos protocolos seleccionados serán capaces de pasar a través del firewall.

2.2.4.4 Estrategia de un firewall

Generalmente un firewall se encuentra situado en los puntos de entrada a la red que protege. Este es un enfoque tradicional que surge a partir de la forma más simple de conexión de una red privada a Internet: mediante un único enlace. Aunque es posible utilizar otros enfoques para diferentes topologías de interconexión. Pero en cada caso, cada conexión (punto de acceso) de la red local a Internet estará equipada con un firewall.

Todo el tráfico que es entrante desde internet, su único camino para alcanzar dicha conexión es el firewall que se puede considerarse como el foco de todas las decisiones de seguridad. Concentrando las defensas en este punto, es posible reducir la sobrecarga de seguridad del sistema interno ya que el esfuerzo se limita a unos pocos dispositivos de toda la red (los que forman parte del firewall). De esta forma, un firewall centraliza el control de acceso. Los usuarios remotos pueden acceder a la red interna de forma controlada y segura, pasando a través del firewall.

Un firewall será transparente a los usuarios si no advierten su existencia para poder acceder a la red. Los firewalls generalmente son configurados para ser transparentes para los usuarios de la red interna, mientras que para los usuarios de la red externa.

2.2.4.5 Fundamento de los firewalls

La mayoría de empresas y/o instituciones dependen de Internet para publicitar sus productos y servicios. Por lo que es necesario proteger los datos, transmisiones y transacciones de cualquier incidente, ya sea, causado por actos maliciosos o no intencionales. En el caso de una red local directamente conectada a Internet sin un firewall, la red entera está sujeta a ataques. La experiencia práctica muestra que es muy difícil asegurar que todo host de la red esté protegido. Una contraseña mal elegida puede comprometer la seguridad de toda la red. La gran cantidad de equipos de seguridad que son destinados para la protección de servidores, equipos internos host o computadoras portátiles, celulares, y todo aquel dispositivo electrónico que tenga acceso hacia internet este destinado al uso de este mencionado para tener interacción entre el usuario y el acceso de este recurso que es el internet.

Si la red local está protegida por un firewall, solo existe acceso directo para un conjunto seleccionado de hosts y la zona de riesgo es reducida al firewall en sí mismo o a un conjunto seleccionada de hosts de la red interna.

2.3 Marco Conceptual

1. Arquitectura de red

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término

arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

2. Tolerancia a fallas

La expectativa de que Internet está siempre disponible para millones de usuarios que confían en ella requiere de una arquitectura de red diseñada y creada con tolerancia a fallas. Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo.

Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia. Ésta es la premisa básica de la arquitectura de redes actuales.

3. Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicio se conectan a Internet cada semana. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar disrupción en toda la red. Los desarrollos tecnológicos aumentan constantemente las capacidades de transmitir el mensaje y el rendimiento de los componentes de la estructura física en cada capa. Estos desarrollos, junto con los nuevos métodos para identificar y localizar usuarios individuales dentro de una red interna y externa.

4. Seguridad

Internet evolucionó desde el uso en las organizaciones gubernamentales y educativas estrechamente controladas a un medio ampliamente accesible para la transmisión de comunicaciones personales y empresariales. Como resultado, cambiaron los requerimientos de seguridad de la red. Las expectativas de privacidad y seguridad que se originan para intercambiar información empresarial crítica y confidencial exceden lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red. Como resultado, se está dedicando un gran esfuerzo a esta

área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.

5. Arquitectura de red escalable

El hecho de que Internet se expanda a esta velocidad, sin afectar seriamente el rendimiento de usuarios individuales, es una función del diseño de los protocolos y de las tecnologías subyacentes sobre la cual se construye. Internet, hecho de una colección de redes públicas y privadas interconectadas, tiene una estructura jerárquica en capas para servicios de direccionamiento, designación y conectividad. En cada nivel o capa de la jerarquía, los operadores de red individual mantienen relaciones entre pares con otros operadores en el mismo nivel. Como resultado, el tráfico de redes destinado para servicios regionales y locales no necesita cruzar a un punto central para su distribución. Los servicios comunes pueden duplicarse en diferentes regiones, manteniendo el tráfico de las redes Backbone de nivel superior.

Aunque no existe una organización que regule Internet, los operadores de las diferentes redes individuales que proporcionan la conectividad de Internet cooperan para cumplir con los protocolos y estándares aceptados.

La adherencia a los estándares permite a los fabricantes de hardware y software concentrarse en las mejoras del producto en áreas de rendimiento y capacidad, sabiendo que los nuevos productos pueden integrarse y mejorar la infraestructura existente. La arquitectura de Internet actual, altamente escalable, no siempre

puede mantener el ritmo de la demanda del usuario. Los nuevos protocolos y estructuras de direccionamiento están en desarrollo para cumplir con el ritmo acelerado al cual se agregan los servicios y aplicaciones de Internet.

6. Provisión de seguridad de red

La infraestructura de red, los servicios y los datos contenidos en las computadoras conectadas a la red son activos comerciales y personales muy importantes. Comprometer la integridad de estos activos puede ocasionar serias repercusiones financieras y comerciales.

- Algunas de las consecuencias de la ruptura en la seguridad de la red son:
- Interrupciones de red que impiden la realización de comunicaciones y de transacciones, con la consecuente pérdida de negocios,
- Fallido direccionamiento y pérdida de fondos personales o comerciales,
- Propiedad intelectual de la empresa (ideas de investigación, patentes o diseños) que son robados y utilizados por la competencia, o
- Detalles de contratos con clientes que se divulgan a los competidores o son hechos públicos, generando una pérdida de confianza del mercado de la industria.

La falta de confianza pública en la privacidad, confidencialidad y niveles de integridad de los negocios puede derivar en la pérdida de ventas y, finalmente, en la quiebra de la empresa. Existen dos tipos de cuestiones de seguridad de la red que se deben tratar a fin de evitar serias consecuencias: seguridad de la infraestructura de la red y seguridad del contenido. Asegurar la infraestructura de

la red incluye la protección física de los dispositivos que proporcionan conectividad de red y evitan el acceso no autorizado al software de administración que reside en ellos.

La seguridad del contenido se refiere a la protección de la información contenida en los paquetes que se transmiten en la red y la información almacenada en los dispositivos conectados a ésta. Al transmitir la información en Internet u otra red, los dispositivos y las instalaciones por las que viajan los paquetes desconocen el contenido de los paquetes individuales.

Se deben implementar herramientas para proporcionar seguridad al contenido de los mensajes individuales sobre los protocolos subyacentes que rigen la forma en que los paquetes se formatean, direccionan y envían. Debido a que el re-ensamblaje y la interpretación del contenido se delegan a programas que se ejecutan en sistemas individuales de origen y destino, muchos de los protocolos y herramientas de seguridad deben implementarse también en esos sistemas.

Las medidas de seguridad que se deben tomar en una red son:

- Evitar la divulgación no autorizada o el robo de información,
- Evitar la modificación no autorizada de información, y
- Evitar la Denegación de servicio.

Los medios para lograr estos objetivos incluyen:

- Garantizar la confidencialidad,

- Mantener la integridad de la comunicación, y
- Garantizar la disponibilidad.
- Garantizar la confidencialidad

La privacidad de los datos se logra permitiendo que lean los datos solamente los receptores autorizados y designados (individuos, procesos o dispositivos).

Un sistema seguro de autenticación de usuarios, el cumplimiento de las contraseñas difíciles de adivinar y el requerimiento a los usuarios para que las cambien frecuentemente ayudan a restringir el acceso a las comunicaciones ya los datos almacenados en los dispositivos adjuntos de la red. Cuando corresponda, el contenido encriptado asegura la confidencialidad y reduce las posibilidades de divulgación no autorizada o robo de información.

7. Mantener la integridad de las comunicaciones

La integración de datos significa que la información no se alteró durante la transmisión de origen a destino. La integración de datos puede verse comprometida cuando al dañarse la información, ya sea en forma intencional o accidental, antes de que el receptor correspondiente la reciba. La integridad de origen es la confirmación de que se validó la identidad del emisor. Se compromete la integridad del origen cuando un usuario o dispositivo falsifica su identidad y proporciona información incorrecta al destinatario.

El uso de firmas digitales, algoritmos de hash y mecanismos de checksum son formas de proporcionar integridad de origen y de datos a través de la red para evitar la modificación no autorizada de información

8. Garantizar disponibilidad

La garantía de confidencialidad e integridad son irrelevantes si los recursos de red están sobrecargados o no disponibles. Disponibilidad significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados. Los recursos pueden no estar disponibles durante un ataque de Denegación de servicio (DoS) o por la propagación de un virus de computadora. Los dispositivos firewall de red, junto con el software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y solidez del sistema para detectar, repeler y resolver esos ataques. La creación de infraestructuras de red completamente redundantes, con pocos puntos de error, puede reducir el impacto de esas amenazas.

El resultado de la implementación de medidas para mejorar tanto la calidad del servicio como la seguridad de las comunicaciones de red es un aumento en la complejidad de la plataforma de red subyacente. Debido a que Internet continúa expandiéndose para ofrecer más y nuevos servicios, su futuro depende de las nuevas y más sólidas arquitecturas en desarrollo que incluyen estas cuatro características: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

CAPÍTULO III: DISEÑO

3.1 Análisis de la arquitectura de red de datos

3.1.1 Diseño de redes jerárquicas

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez. El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general.

La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo.

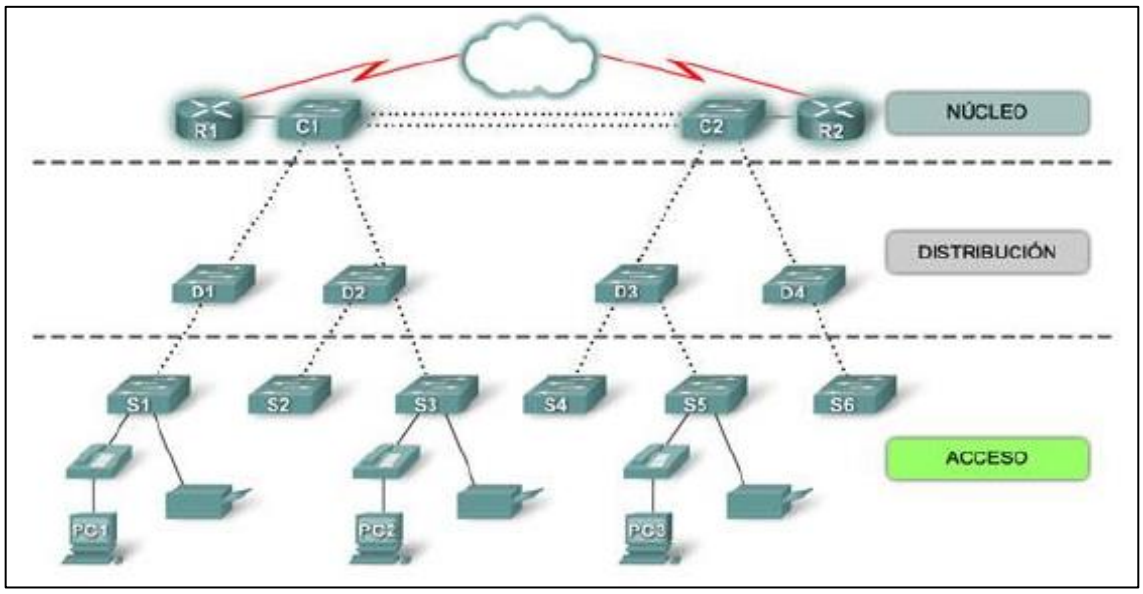


Figura 3.1 Capas de acceso, distribución y núcleo representados

Capa de acceso

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

Capa de distribución

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las

funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso. Las VLAN permiten al usuario segmentar el tráfico sobre un switch en subredes separadas. Por ejemplo, en una universidad el usuario podría separar el tráfico según se trate de profesores, estudiantes y huéspedes.

Normalmente, los switches de la capa de distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad.

Capa núcleo

La capa núcleo del diseño jerárquico es la Backbone de alta velocidad de la internet y se tiene que capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente.

3.1.2 Análisis de la arquitectura de red actual

Nuestro desarrollo para una arquitectura de red redundante y de alta disponibilidad, se enfoca en el observado en las tres capas antes mencionadas, acceso, distribución y de núcleo. Por tales características nos vamos a relacionar con cada concepto en el desarrollo. Se tiene para esta arquitectura dos sedes una principal y otra sede secundaria, que a su vez todas se comunican con sedes remotas.

Capa de acceso y Capa de distribución, en la este escenario la empresa a que hacemos mención tiene una gran dificultad a no tener visibilidad de los equipos instalados, tanto como switches de acceso como principal o de Core, no tener administración de la mayoría de equipos.

La dificultad radica en la topología actual a nivel de acceso, donde se muestra una red plana o de cascada, lo cual para su desarrollo diario en actividades como acceso hacia internet, acceso a archivos compartidos, aplicaciones, servidores se ve interrumpido, por los siguientes eventos y la observación que se llegó al momento de analizar la red.

Se tiene actualmente tiene en su sede los siguientes equipos definidos de la siguiente manera y con las características que hacen una red vulnerable ante fallas a nivel de arquitectura

1. Una red con muchos puntos de fallo, ya que se observa conexión de equipos en su data center (Switch Core), los cuales asumen la importancia de ser el nexo entre todos los equipos, estar asumiendo el papel de Master y Backup de una forma errónea y que no garantiza redundancia esto conlleva a que cualquier fallo en uno de los Switches de acceso, se lleve consigo la conectividad hacia las demás áreas conectadas a él.

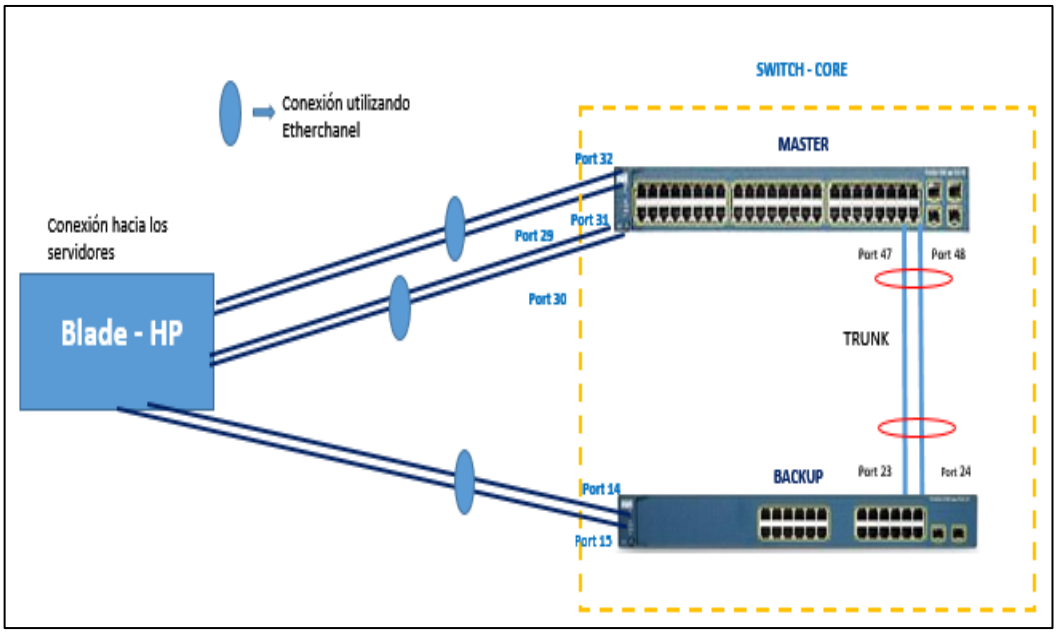


Figura 3.2 Conexión con el switch principal, donde se aprecia la no contingencia de enlaces. Fuente: Elaboración propia

2. Se tiene switches actuando de Core, el primero un Cisco 3560 y Cisco 2690 actuando como Layer 3 (Master) para toda la red y el segundo un Cisco 3560 como Layer 3 (Backup) y el cual maneja vlans de las distintas áreas de su sede para la comunicación de servidores y usuarios finales.

3. Se tiene configurado para toda la red una única vlan tráfico de datos, tráfico de voz y conexión hacia los equipos de acceso inalámbrico, y otra vlan tráfico de servidores, que es compartida con el área de soporte.

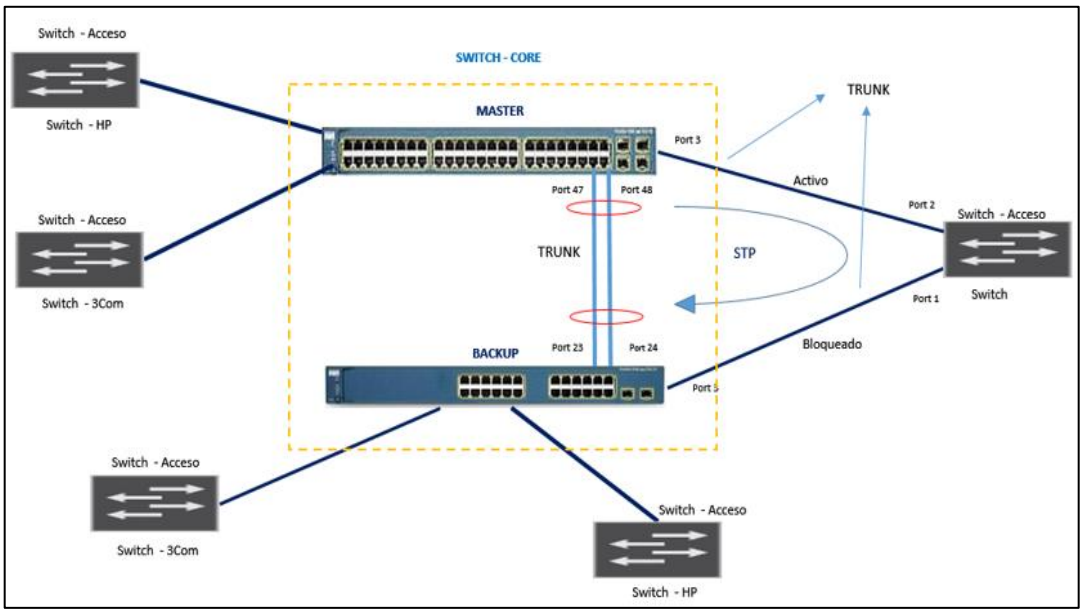


Figura 3.3 Representación de la comunicación entre switches en la red LAN y la generación de bucles. Fuente: Elaboración propia

- El esquema mostrado nos indica las conexiones del equipo configurado como Switch Core y los Switches de acceso, lo cual conlleva a no tener redundancia de conexiones entre ambos equipos, como ejemplo el equipo switch – acceso tiene una conexión troncal hacia el switch Core (Master y Backup), pero al tener configurado STP (*Spanning Tree Protocol),* para evitar la generación de bucles en la red y no ocasionar perdida de gestión y malestar entre los usuarios (servicios finales – navegación- telefonía /digital-analógica – servidores - etc.). Pero que actualmente por lo anterior mencionado y al no haber redundancia las prioridades genera cambios de root entre todos los equipos.

4. La agrupación actual de las vlan no brinda un ordenamiento a la red, y la no administración de la conexión entre el Switch Core (Master y Backup), no dan redundancia a la red por estar solamente conectados con enlace troncal y tener configurados Lacp pero al no tener contingencia en la conexión. Por tal motivo la generación de bucles en la red al no conocer quien asume el papel de root entre los Switches de acceso y el Switch Core.

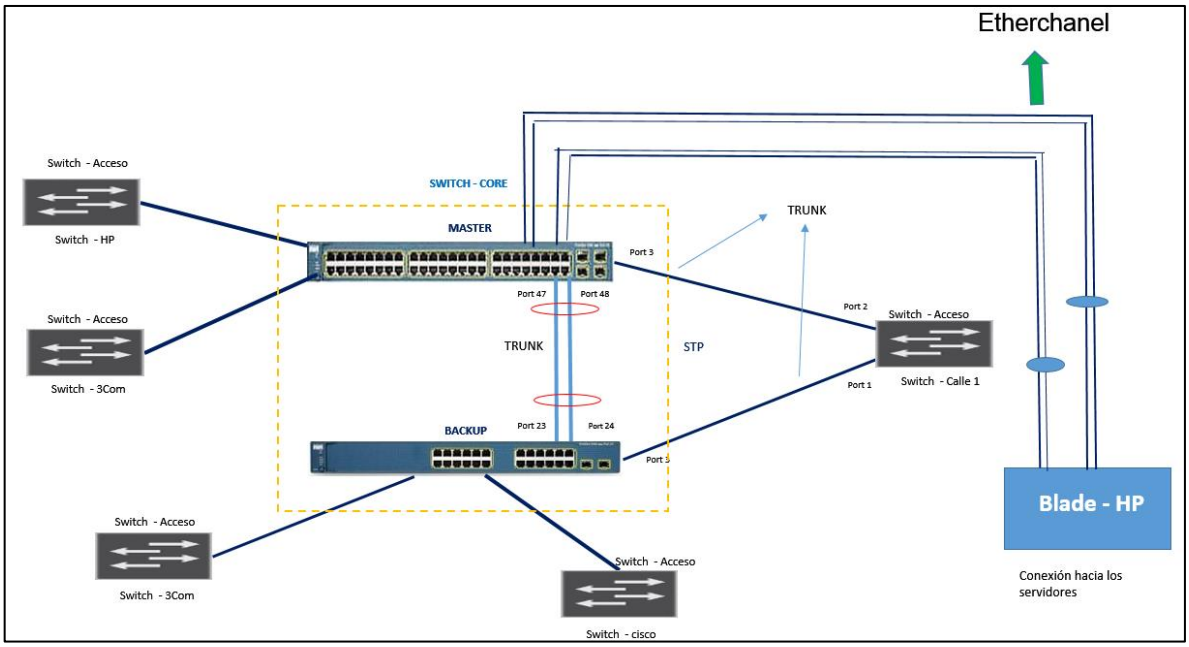


Figura 3.4 Conexión entre el switch principal y los servidores, lo cual no garantiza la redundancia de enlaces. Fuente: Elaboración propia

5. Se tiene una red que opera a 100Mbps Full Dúplex, sin redundancia de enlaces. La conexión del Switch Core hacia los Servidores no tiene enlaces redundantes. Si bien está configurado mediante Etherchanel, éste no se tiene redundancia en la conexión.

6. Si nos referimos al protocolo Spanning Tree, éste se encuentra habilitado, pero con problemas con lo anterior mencionado y además de carecer de roles definidos (root bridge, root designated, etc.).

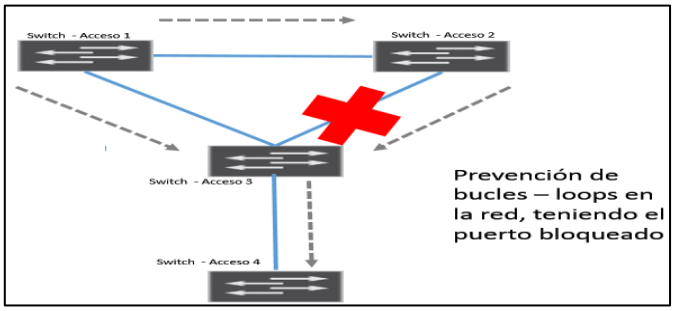


Figura 3.5 Generación de loops en una red, lo cual es perjudicial para los administradores de red. Fuente: Elaboración propia

Ante la problemática de tener actualmente estas conexiones, las que se aprecian en la gráfica.

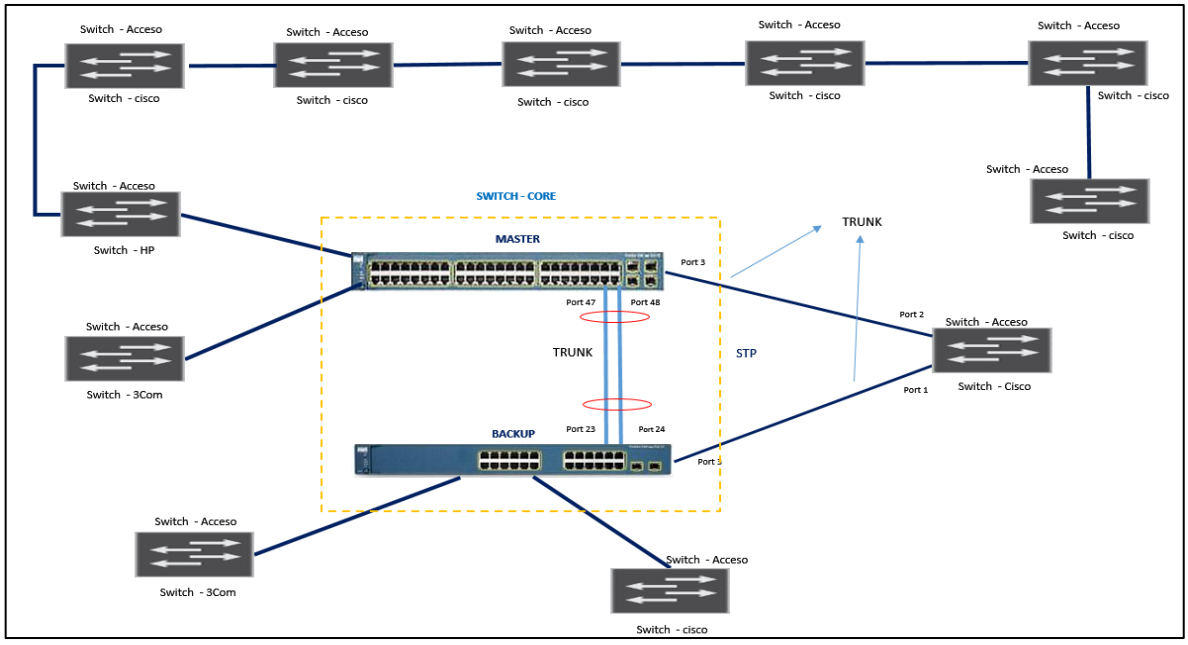


Figura 3.6 Se representa mediante el diagrama de red, la arquitectura interna entre todos los switches y se puedes observar la comunicación en cascada. Fuente: Elaboración propia

Como observamos en la topología inicial de la empresa a la que se hace referencia, se tiene lo siguiente:

- Una red con muchos puntos de fallo, ya que se observa cascada de switches, esto conlleva a que cualquier fallo en uno de los switches de acceso, se lleve consigo la conectividad hacia las demás áreas conectadas a él.

- Se tiene 2 switches actuando de Core, el primero un Cisco 3560 actuando como Layer 3 para toda la red y el segundo un Cisco 3560R actuando sólo como Layer 2 y como servidor de vlans (VTP).

- Se tiene una misma vlan para tráfico de datos y tráfico de voz, ya que carece de segmentación. Esto resulta en el agotamiento de direcciones IPs asignadas a los dispositivos de red (Pc, teléfonos IP, impresoras, etc.) ya que inicialmente se usaban segmentos de red de máscara /24.

- La conexión del Switch Core hacia los Servidores no tiene enlaces redundantes. Si bien está configurado mediante Etherchanel, éste no se encuentra activo.

- Si nos referimos al protocolo Spanning Tree, éste se encuentra habilitado por default con una versión antigua como lo es PVST, además de carecer de roles definidos (root bridge, root designated, etc.).

- La Gestión de los equipos se realiza utilizando direcciones IPs del segmento de datos, esto hace que se agote aún más el direccionamiento dedicado a la red de datos, voz y/o etc.

En la capa de núcleo, se tiene las siguientes características que dan evidencia la no redundancia de enlaces, al igual que la capa de acceso y la capa de distribución. Los equipos que comparten el acceso hacia internet (red externa), tienen la particularidad que solo tienen un enlace hacia internet, mientras que en los extremos solo tiene un enlace, los equipos de seguridad no cuentan con ningún tipo de soporte actual, la navegación no es controlada por ningún tipo de filtrado web, y las conexiones al tener enlaces activo / activo, no son utilizadas de la forma correcta, por lo cual el uso adecuado de una reestructuración al nivel de tecnología tanto en internet y equipos de seguridad.

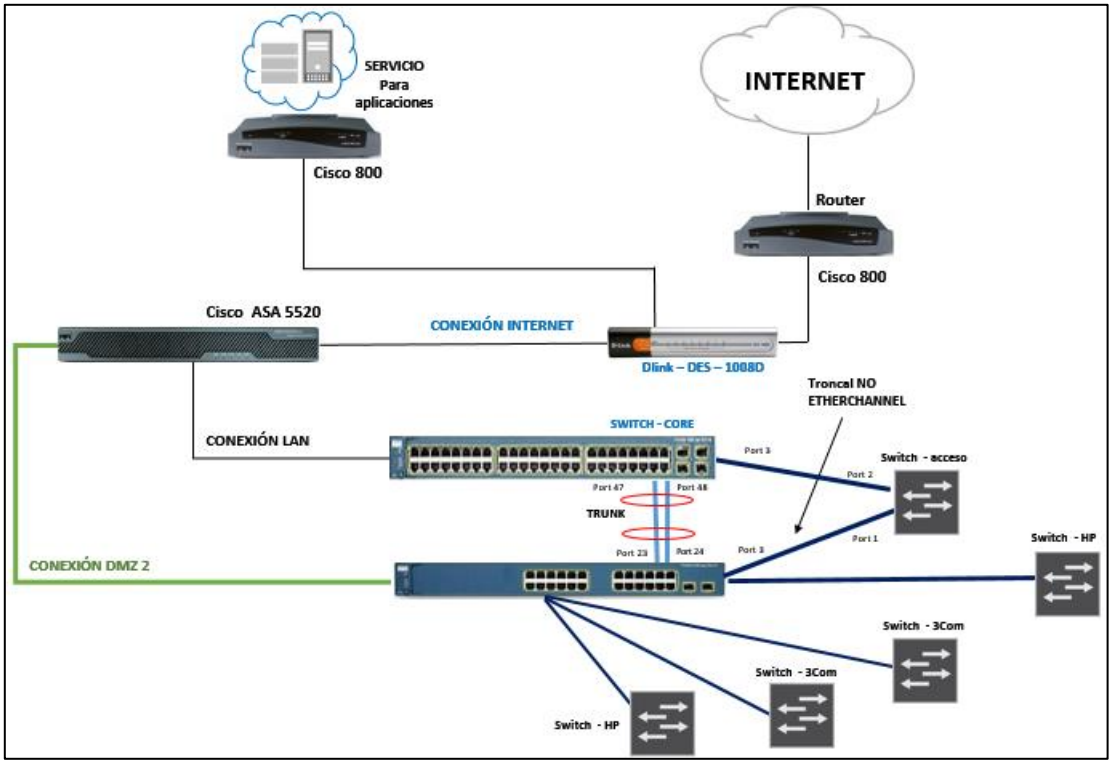


Figura 3.7 Diagrama lógico de la conexión entre la red interna y red externa, donde la comunicación de dependen solo un equipo hacia internet. Fuente: Elaboración propia

El esquema actual no presenta contingencia ante fallas del equipo ya sea por software o hardware, se muestra los siguientes casos: Ante la caída del equipo Dlink DES-1008D utilizado como switch layer 2 para interconectar la zona DMZ con el firewall, ante esta falla se pierde su conectividad.

Lo mencionado anteriormente la utilización de equipos de irradiación inalámbrica por medio de sistemas autónomos de acceso wireless, y tener la dificultad de contar con el direccionamiento ip para la mayoría de equipos en su red interna.

Al no tener un equipo dedicado de filtrado web, el consumo de ancho de banda en todas las sedes se ve reducida, por no tener visibilidad de los usuarios en su entorno de trabajo, la nulidad de no poder apreciar en tiempo real estos mensajes de consumos., para su respectivo registro hacen muy dificultoso y laborioso el control de toda la red interna de todas las sedes asociadas a la sede principal.

Se muestra la topología de la arquitectura de red de la empresa, con lo cual se muestra la forma de cascadas con los equipos de acceso y distribución con las sedes remotas.

Un gran inconveniente es el uso del acceso remoto el cual no utiliza ningún elemento de seguridad, para acceder a la red interna desde cualquier sede, se realiza con el uso de software libres, que pueden ser un generador de robos de información en la red de la empresa.

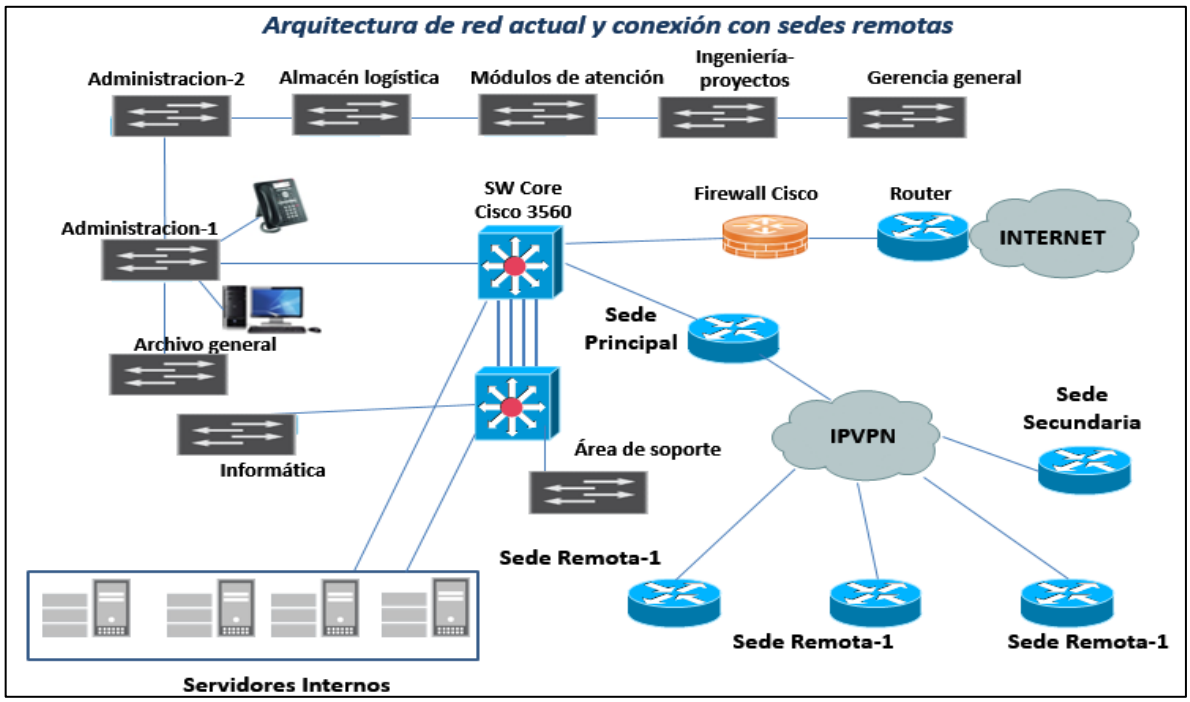


Figura 3.8 Arquitectura de red donde se observa las conexiones con las sedes remotas y los switches, donde no hay redundancia de enlaces.

Fuente: Elaboración propia

3.1-Diseño de la arquitectura de red de datos

Se presenta los siguientes criterios para el diseño de una arquitectura a nivel de capa de acceso, distribución y nucleó. Como las evidencia de tener una arquitectura a red interna y red externa deficientes, en este proceso de renovación tecnológica en todos los equipos se utilizara para este propósito equipos Juniper como routers, firewalls y Switches por su gran estabilidad y por tener las siguientes características que hacen a una red estable y en ambos aspectos tener una red redundante en conexiones hacia los switches de acceso, principales, el

manejo de filtrado web, para el control de usuarios y en una red remota el control de ancho de banda por el uso de un equipo administrador de ancho de banda.

En este proceso comenzaremos a definir los beneficios y características de los equipos que se utilizan en la capa de acceso y distribución.

Equipos Juniper en la capa de acceso y distribución

El Nuevo Switch Core de la Empresa y los demás Switches de acceso comprenden las siguientes funcionalidades:

3.2.1 Virtual Chassis (VC):

Los equipos Juniper a nivel de switches tienen la característica de poder formar equipos modulares, la gran ventaja de esta tecnología es que está conformada por un plano de control y un plano de envió el cual permite tener alta redundancia de enlaces y como característica general es que todos los equipos de esta gama comparten el mismo sistema operativo Junos.

Junos es un sistema operativo confiable y de alto rendimiento para sistemas de enrutamiento, conmutación y seguridad. Reduce el tiempo necesario para desplegar nuevos servicios y disminuye los costos de operación de la infraestructura de red. Junos es un sistema, diseñado para redefinir completamente la manera en que una red funciona.

- Un único sistema operativo para los Enrutadores, Conmutadores y Firewalls Juniper: Reduce el tiempo y esfuerzo para planificar, implementar y operar la infraestructura de red.
- Una única versión de sistema operativo: Proporciona la entrega estable de nuevas funcionalidades en una cadencia constante (cada 3 meses) de nuevas versiones de SO.
- Una arquitectura de software modular: Proporciona alta disponibilidad y escalabilidad de software que se encarga de las necesidades cambiantes a corto y a largo plazo.

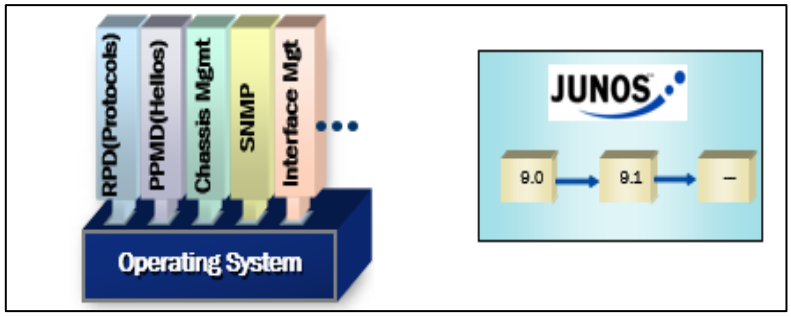


Figura 3.9 Sistema operativo y el inicio de sus versiones

La ejecución de Junos en la red mejora la confiabilidad, el rendimiento y la seguridad de las aplicaciones existentes. Automatiza las operaciones de red en un sistema simplificado, lo que permite más tiempo para centrarse en el despliegue de nuevas aplicaciones y servicios. Y es escalable tanto hacia arriba como hacia abajo, proporcionando un sistema constante, confiable y estable para los desarrolladores y operadores.

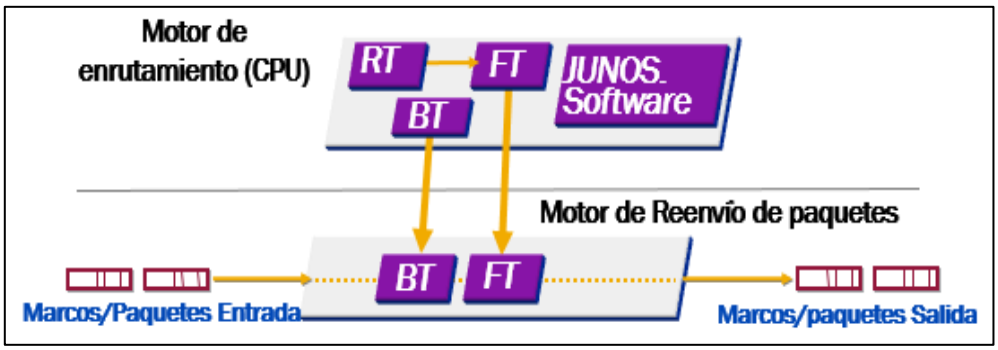


Figura .3.10 Representación del plano de control donde está el motor de enrutamiento (protocolos, tabla se sesión, etc.) y el plano de reenvió de paquetes donde solo recibe datos de entrada y salida sin la necesidad de procesar. Fuente: Elaboración propia

Mediante ella, se puede crear un chasis virtual (con todas las ventajas que conlleva), hasta 10 equipos, independientemente del tipo de enlace, local o extendido. Nos permite por tanto, simplificar el diseño y operación de nuestra red de múltiples maneras:

Las características de alta capacidad de reenvío de paquetes, performance, calidad de servicio, VLANs, entre otras funcionalidades avanzadas de conmutación. Permitirá contar con maniobrabilidad en la configuración y diseño final de red de acceso.

- En una red de hasta 480 puertos (con 10 switches), podríamos trabajar como si de un sólo equipo se tratara.

- Podemos dimensionar nuestro crecimiento, de forma totalmente gradual, así nos adaptamos a crecimientos inesperados de usuarios por área.

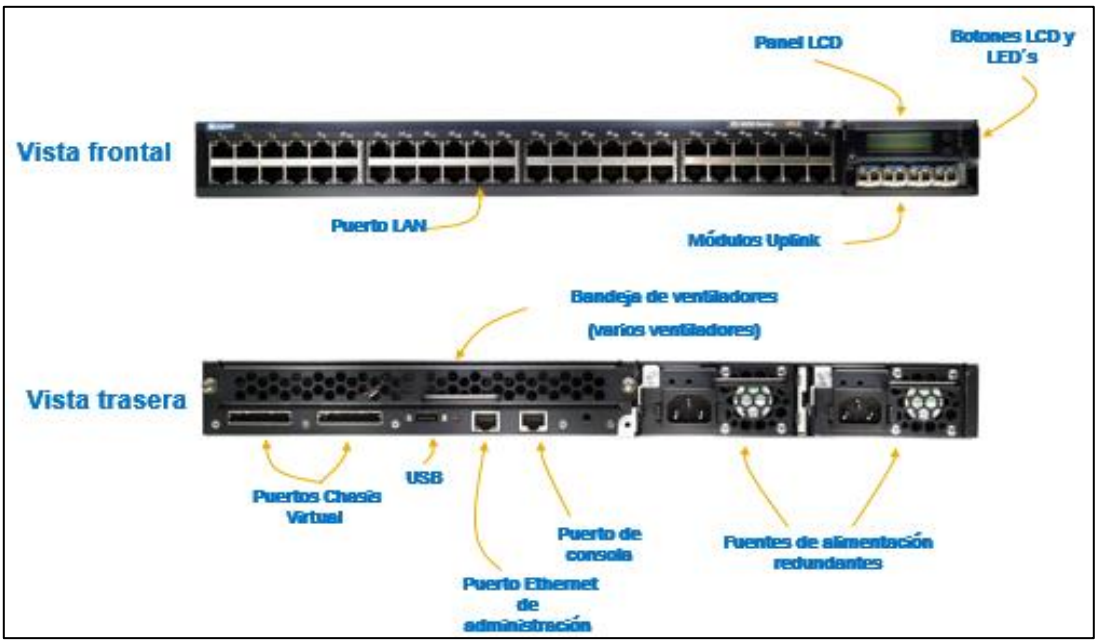


Figura 3.11 Equipos y sus características físicas. Fuente: Elaboración propia

- Al poder conectar los diferentes enlaces a una única entidad lógica, podemos ahorrarnos los mecanismos tradicionales de control de bucles de red, como el Spanning-Tree, y tener fácilmente una arquitectura totalmente redundante, y balanceada, de elevado rendimiento, velocidad, y sin pérdida de servicio.

La topología de la empresa está compuesta por un Virtual Chassis de 4 miembros (Nodo 0 al Nodo 3), donde se tienen los siguientes roles:

- Nodo 0: Routing Engine Master >>>>>>> EX4200-24F

- Nodo 1: Routing Engine Backup >>>>>>> EX4200-24F

- Nodo 2: Line Card >>>>>>>>>>>>>>> EX4200-48P

- Nodo 3: Line Card >>>>>>>>>>>>>>> EX4200-48P

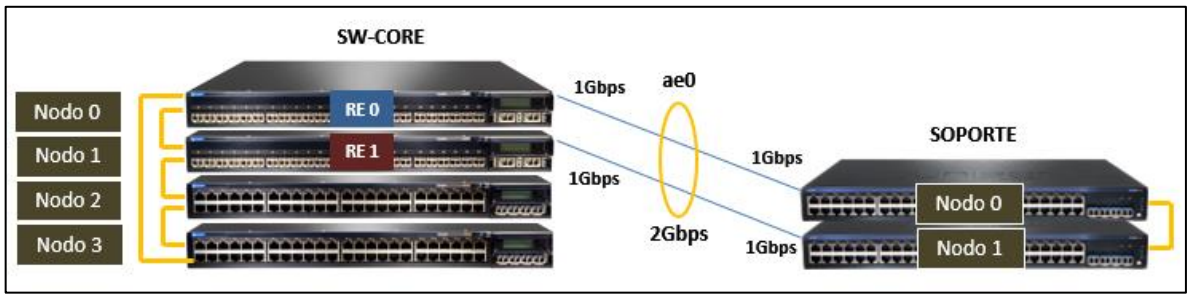


Figura 3.12 Se representa un equipo con la tecnología virtual chassis y las características de alta redundancia de enlaces. Fuente: Elaboración propia

Los equipos que son utilizados en la capa de distribución son los equipos EX4200 con puertos de conexión de fibra y conexión cobre. La tecnología de utilizar los equipos en virtual chassis es que el equipo designado como master es el router-engine (motor de enrutamiento) y los demás equipos mantienen una copia de esta características ante cualquier caída de equipo ya sea por nodo la alta disponibilidad de los enlaces hacen posible la continuidad de la funcionalidad de los equipos y de la red.

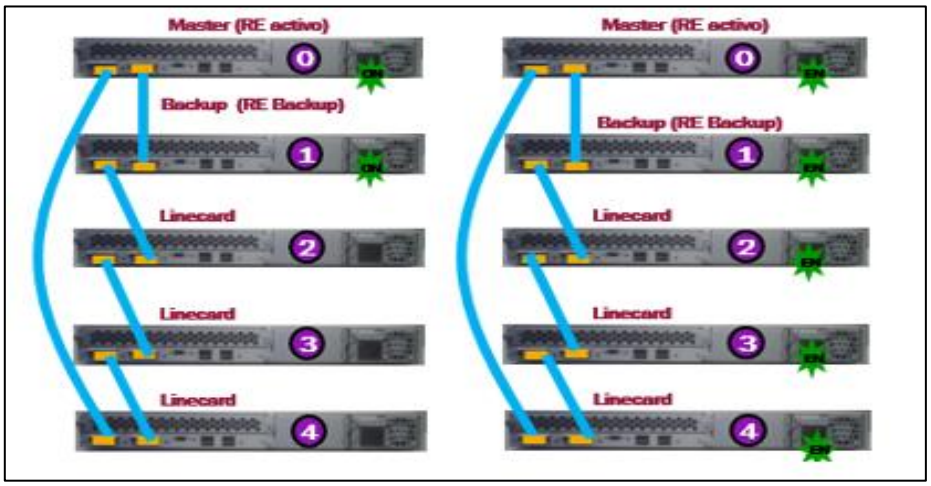


Figura 3.12 Encendido de equipos en virtual chassis y sus conexiones entre cada equipo. Fuente: Elaboración propia

Definimos prioridades para los miembros que actuarán como Routing-Engine:

Para formar el VC, procedemos a encender el Switch que deseamos que sea member 0 y le asignamos una prioridad de 255, este valor asegura que siempre sea Master. Seguidamente encendemos el segundo Switch y le asignamos la prioridad de 254, con ello el Member 1 actuará como routing-engine de Backup. Los demás dispositivos actuarán como Line Cards (sólo interfaces físicas).

```
virtual-chassis {
    member 0 {
        mastership-priority 255;
    }
    member 1 {
        mastership-priority 254;
    }
}
```

Figura 3.13 Configuración y prioridades entre equipos miembros al ser configurados en virtual chassis. Fuente: Elaboración propia

3.2.2 VLANs y Routed Vlan Interface (RVI) – Intervlan Routing

Una RVI es una interfaz virtual configurada en un switch multilayer. Se puede crear una RVI para cualquier VLAN que exista en el switch. Una RVI se considera virtual porque no hay un puerto físico dedicado a la interfaz. Puede realizar las mismas funciones para la VLAN que una interfaz de router y puede configurarse de manera similar a una interfaz tal (es decir, dirección IP, ACL de entrada y de salida, etc.).La RVI para la VLAN proporciona procesamiento de capa 3 para los

paquetes que provienen de todos los puertos de switch asociados a dicha VLAN o que se dirigen a ella. Algunos de los motivos para configurar una RVI son:

- Proporcionar un gateway a una VLAN a fin de poder enrutar el tráfico dentro o fuera de ella.

- Proporcionar conectividad IP de capa 3 al switch.

- La latencia es mucho menor, porque no hace falta que salga del Switch para conectividad entre vlans.

3.2.3 Enrutamiento Estático

El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una red origen a una red destino. Switches L3 y routers son dispositivos que se encargan de transferir paquetes de una red a otra. Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que los protocolos de routing dinámico.

3.2.4-Link Aggregation

La agregación virtual de enlaces (LAG), es una característica de nivel 2, que une puertos físicos en un único enlace de datos de mayor ancho de banda; de este modo se aumenta la capacidad del enlace y se crean enlaces redundantes. Si falla un enlace, la carga se redistribuye entre los enlaces restantes, con lo que el funcionamiento es continuo.

Un ejemplo es cuando tenemos muchos servidores que salen por un único enlace troncal donde puede que el tráfico colapse el enlace, y una de las soluciones más prácticas es el uso de Link Aggregation más conocido como Lacp.

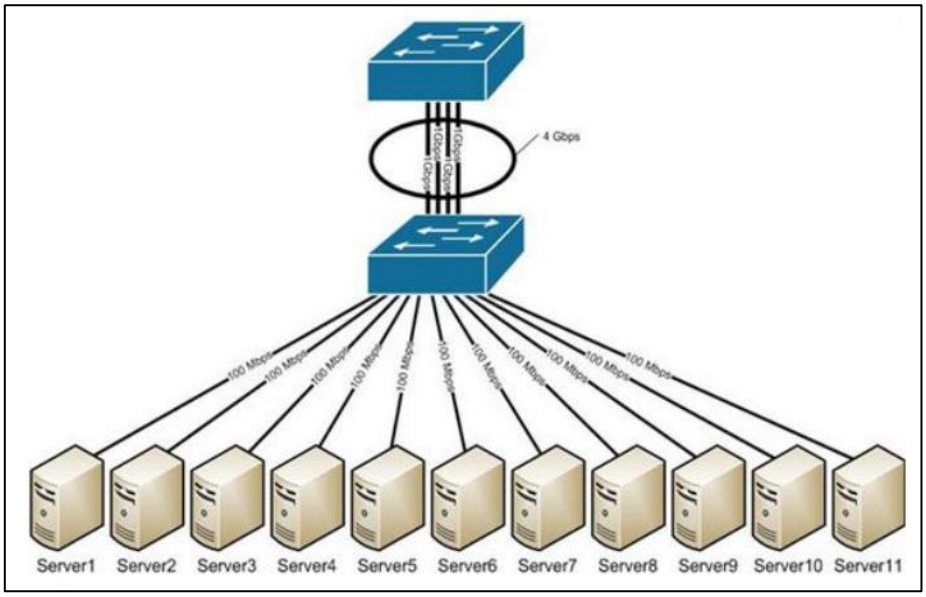


Figura 3.14 El enlace virtual formado tiene la nomenclatura de aen, donde "n" es el número de enlace virtual creado.

Para el escenario de la Empresa, se crearon LAGs hacia el Switch de cada área. Estos están compuestos de 2 interfaces ópticas de 1Gbps cada una, la cual al estar agregadas forman un solo enlace de 2Gbps. Para asegurar la continuidad del enlace, se han formado los link aggregations tomando como miembros una interface de cada Switch como se muestra en la figura:

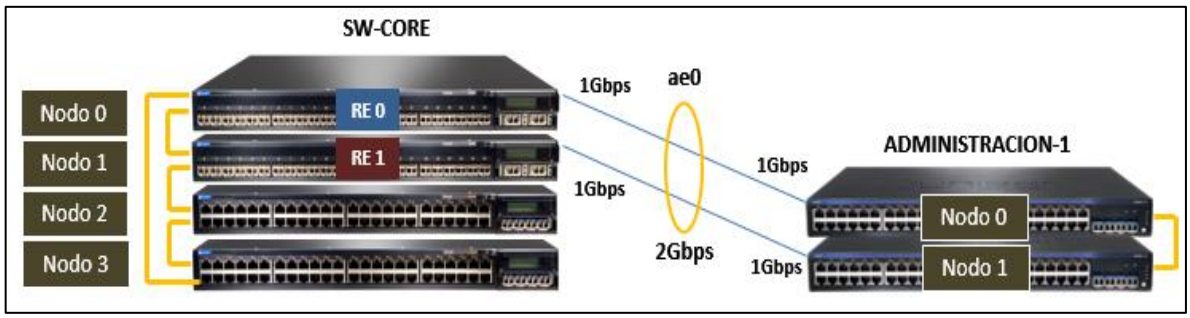


Figura 3.15 Conexión entre el switch principal y un switch de acceso, mediante Lacp en sus conexiones, lo cual garantiza alta redundancia.

Fuente: Elaboración propia

3.2.5 DHCP Server y DHCP Relay

Se configuró un servicio DHCP con Pool 172.16.114.0/24 para la conectividad de los Access Point con el Wireless LAN Controller (WLC100). Estos APs reciben todos los parámetros necesarios para registrarse en el WLC y En el caso de DHCP Relay (Reenvío de solicitudes DHCP hacia los servidores designados) Como ejemplo el diagrama para el área de Administracion-1

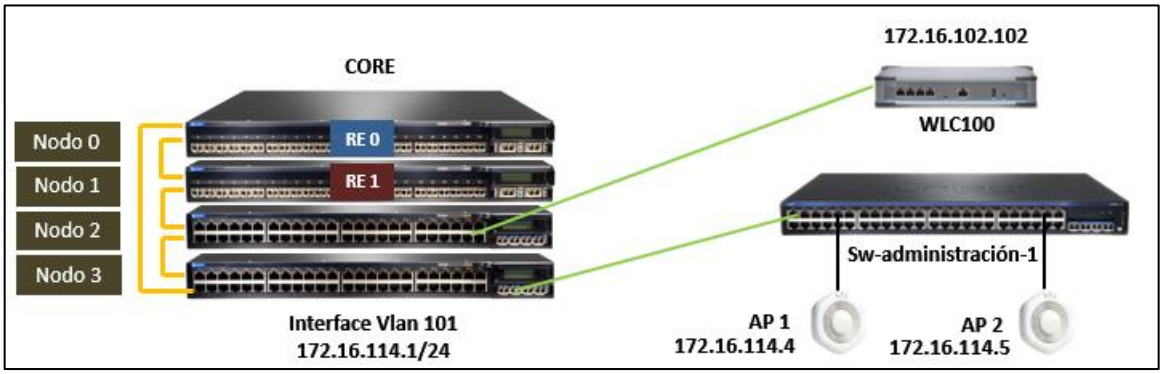


Figura 3.16 Conexión de los equipos y la administración de pertenecer a otras vlan para la conexión inalámbrica y separarlos de la vlan de datos.

Fuente: Elaboración propia.

3.2.6-Firewall Filters

Los filtros de firewall nos permiten realizar filtrado de tráfico de paquetes en sentido entrante o saliente, de manera similar a los Access lists de Cisco.

Para la Empresa, se configuraron filtros de acceso a la gestión de equipos, es decir sólo tendrán acceso a la administración de equipos instalados los administradores de red. Los accesos son vía telnet, SSH, Web Seguro.

3.2.7-Power over Ethernet (PoE+)

PoE son la iniciales de Power Over Ethernet y permite la transmisión de electricidad y datos a través de cable UTP/STP. Es útil en aquellas situaciones en las que se necesita instalar un dispositivo de red (como puede ser un Acceso Point, un teléfono IP, una cámara IP o cualquier dispositivo de red que admita este sistema y no haya disponible una toma de electricidad.

Power over Ethernet se implementa siguiendo las especificaciones de la norma IEEE std. 802.3af. Permite alimentar dispositivos para que utilicen niveles de voltaje entre 44–57 V DC (el voltaje nominal es 48 V, sobre dos de los cuatro pares de un cableado estructurado con una corriente entre 10–350 mA.

3.2.8-Spanning Tree RSTP, VSTP

Cuando se introduce la redundancia en un diseño de la Capa 2, pueden generarse bucles y tramas duplicadas. Los bucles y las tramas duplicadas pueden tener

consecuencias graves en la red. El protocolo spanning tree (STP) fue desarrollado para enfrentar estos inconvenientes.

STP asegura que exista sólo una ruta lógica entre todos los destinos de la red, al realizar un bloqueo de forma intencional a aquellas rutas redundantes que puedan ocasionar un bucle. Un puerto se considera bloqueado cuando el tráfico de la red no puede ingresar ni salir del puerto. Esto no incluye las tramas de unidad de datos del protocolo de puentes (BPDU) utilizadas por STP para evitar bucles.

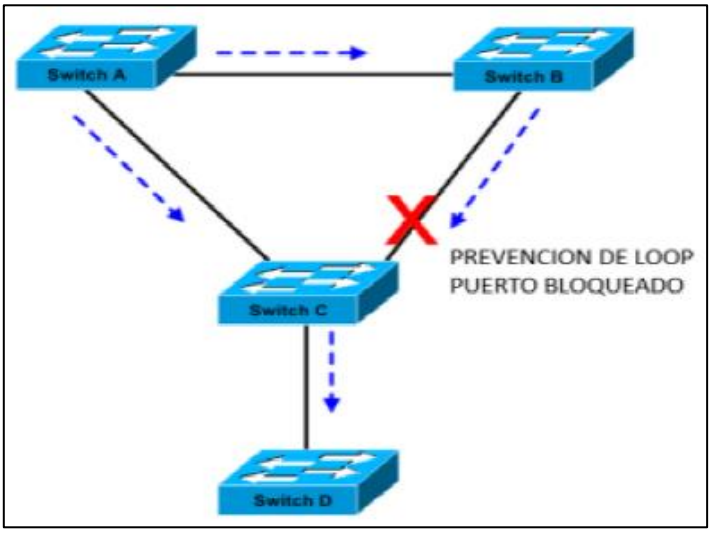


Figura 3.17 Switches sin la aplicación de saber quién es el de mayor prioridad lo cual genera bucles en la red.

A manera de asegurar que el switch Core sea la raíz de toda la topología de la Empresa, se ha configurado con prioridad 0 el chassis virtual, esto evita que cualquier otro switch que se coloque posteriormente se convierta en la raíz de toda la red.

```
    protocols {
        igmp-snooping {
            vlan all;
        }
        vstp {
            vlan all {
                bridge-priority 0;
            }
        }
        lldp {
            interface all;
        }
        lldp-med {
            interface all;
        }
}
```

Figura 3.18 Configuración del switch y la aplicación de prioridad en el equipo principal, Fuente: Elaboración propia

3.2.9-Protocolo de Descubrimiento de enlaces LLDP, LLDP-MED

LLDP es un Protocolo de Descubrimiento de Vecinos, alternativo a CDP que ha sido diseñado para dispositivos de redes como switches y routers. Dicho protocolo solo trabaja en Layer-2. Uno de los mayores usos es para identificar los teléfonos VoIP, Access Point, Parámetros Poe, etc. A continuación una imagen que detalla el funcionamiento de LLDP:

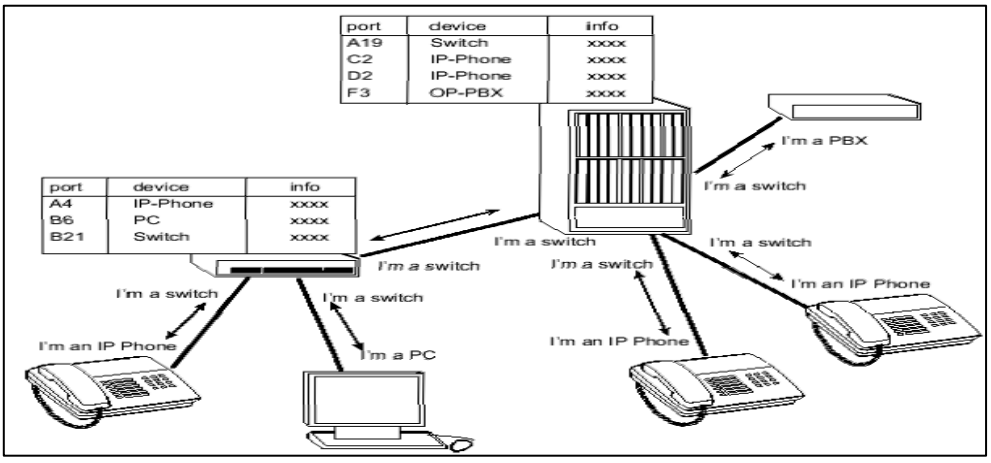


Figura 3.19 LLDP se habilita en la jerarquía protocolos, distintas conexiones.

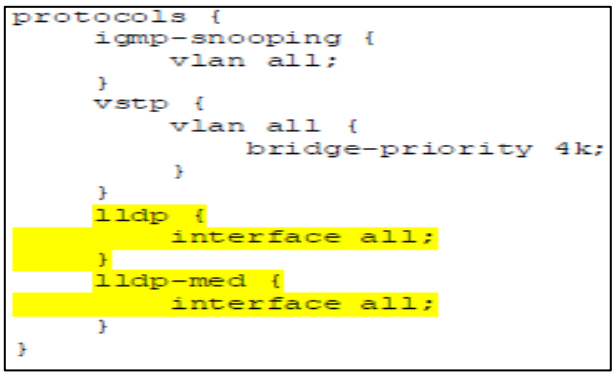


Figura 3.20 Configuración para el descubrimiento de conexiones hacia los equipos principales, se aplica entre los equipos de acceso y distribución
Fuente: Elaboración propia

3.2.10 Bidirectional Forwarding Detection (BFD)

El protocolo BFD (Bidireccional Forwarding Detection) es un protocolo diseñado para permitir la detección rápida de caídas en enlaces de comunicación de datos entre dos equipos. La detección rápida permite establecer caminos alternativos en un tiempo menor que utilizando los mecanismos de “Hello” de los protocolos de routing existentes. El mejor tiempo de detección de los protocolos de routing no es inferior a 1 segundo. Este tiempo es excesivo para ciertas aplicaciones y supone una pérdida de datos excesiva a tasas de transferencia de gigabit. El objetivo de BFD es la detección rápida generando muy poca sobrecarga y ocupando la línea durante muy poco espacio de tiempo.

La detección se realiza en el enlace que une dos equipos adyacentes, detectando problemas no sólo en la línea, sino también en los interfaces y en el propio forward de cada router. También el protocolo BFD pretende estandarizar los métodos de

detección, de forma que sirva para todo tipo de medios, enlaces y protocolos, con tiempos de detección programables y adaptables a las posibilidades de los equipos de routing.

Básicamente el protocolo BFD consiste en la transmisión de paquetes con una cadencia continua entre los dos equipos de los extremos del enlace que se monitoriza. Se detecta una incidencia cuando se dejan de recibir paquetes en uno de los extremos durante un tiempo determinado. Por cada enlace que se monitoriza se crea una nueva sesión BFD, y sólo una única sesión por enlace.

Durante la negociación entre los dos equipos para el establecimiento de la sesión BFD, ambos equipos establecen sus limitaciones a la hora de transmitir y recibir paquetes. De esta forma el equipo más rápido se adapta al equipo más lento y se definen los tiempos de transmisión y detección para cada equipo.

Los protocolos de routing se registran en la sesión BFD que monitoriza el enlace en el que estén interesados. La sesión notifica los cambios de estado del enlace a los protocolos de routing que se hayan registrado en la sesión. De esta forma sólo existe una sesión BFD por cada enlace a monitorizar

Después de lo mencionado se tiene el diseño de red para las sedes remotas y la sede principal en diagramas de red a nivel de capa de acceso y distribución aplicando los criterios mencionados de las características de los equipos Juniper Switches a nivel de renovación tecnológica y dar una alta disponibilidad y redundancia de enlaces.

Arquitectura de red en una sede remota a nivel de capa de acceso y distribución y la alta disponibilidad presente en el diseño.

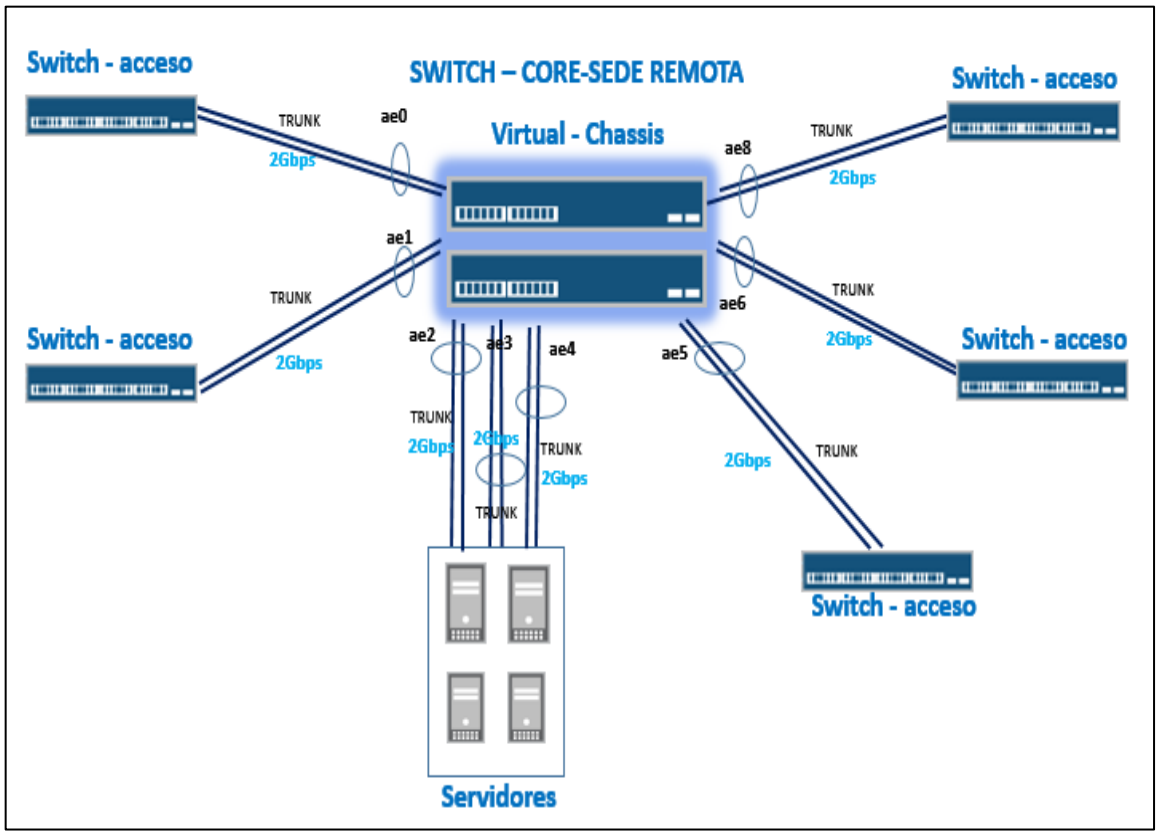


Figura 3.21 Diseño de red, de una sede secundaria donde se aprecia la alta redundancia de enlaces desde los switches de acceso y servidores con comunicación entre el equipo principal. Fuente: Elaboración propia

Sede principal y el diseño de la nueva red donde se aprecia la redundancia de enlaces entre el equipo Swicth-Core y los Switches de acceso, también se puede apreciar los criterios antes mencionados como el diseño de la red aplicando Lacp entre todo los enlaces conectados al equipo principal.

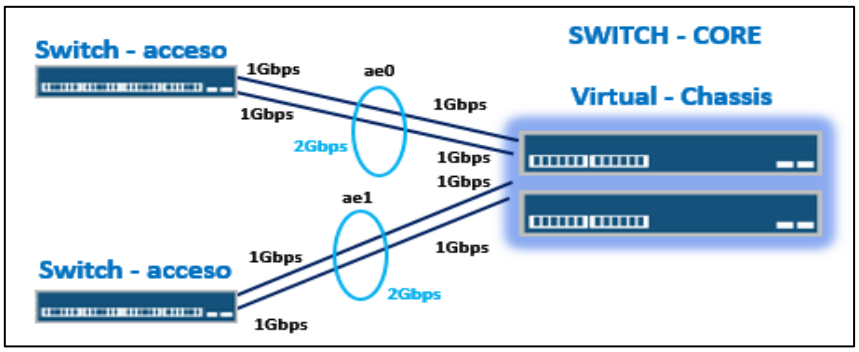


Figura 3.22 Conexión entre un switch principal y un equipo de acceso, con la aplicación de virtual chassis en un extremo y configuración de Lacp entre ambos equipos. Fuente: Elaboración propia

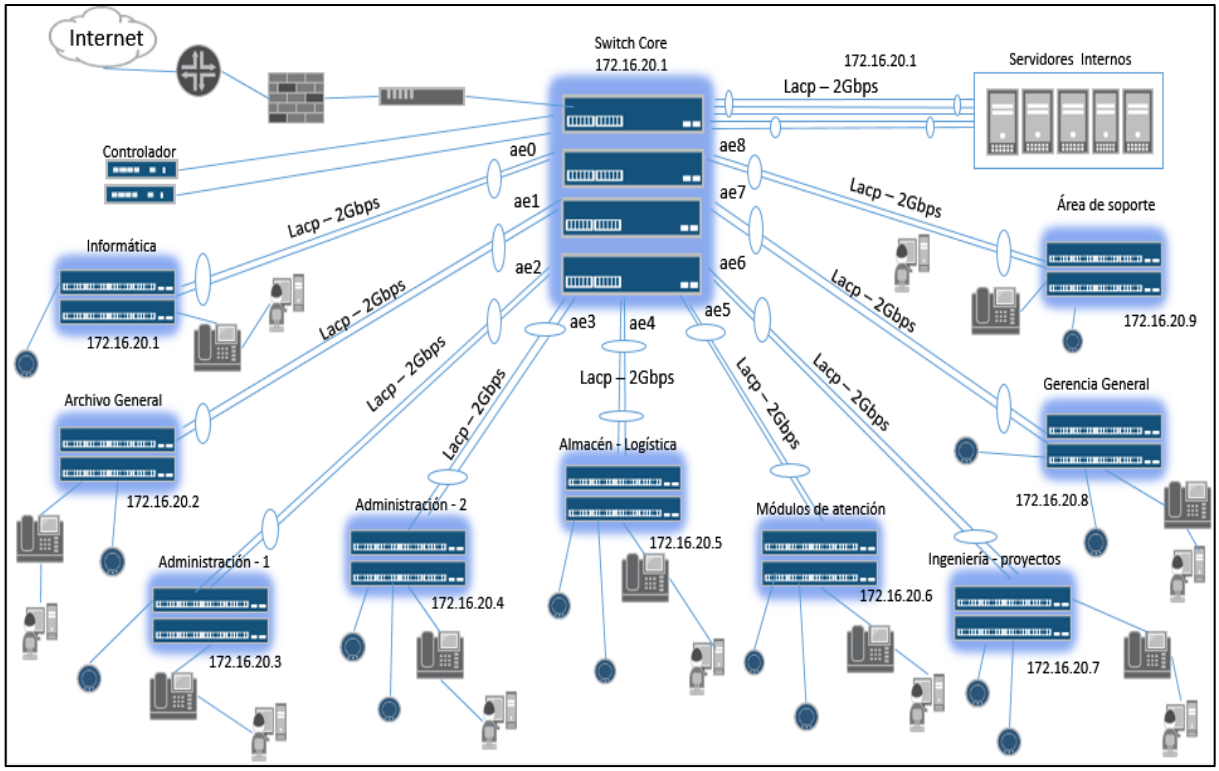


Figura 3.23 Diseño de la arquitectura de red a nivel de capa de acceso y distribución los cual garantiza alta redundancia de enlaces entre todos los equipos de la red. Fuente: Elaboración propia

Se analizó la arquitectura y se dio una solución óptima a nivel de capa de acceso y distribución**,** ahora el siguiente paso es poder diseñar una red estable y en alta disponibilidad con salida hacia internet, actuablemente se tiene en las sede remotas un enlace y en la sede principal enlaces de internet activo / activo, cabe mencionar de todas las sedes remotas hay una sede que viene hacer la sede secundaria que en un futuro tendrá enlaces activo / pasivo , y aunque la arquitectura actual no permite el enlace se presentó la siguiente solución, con los siguientes resultados y pruebas de protocolos en la etapa de navegación sin tener problemas en la red.

Como la renovación de tecnología y la capacidad de poder brindar una redundancia hacia la red externa (internet), se presentan los equipos Juniper en la gama de seguridad que son los srx como firewalls y routers y las siguientes características.

3.2.11 Puertas de Enlace SRX

Se ofrece como solución de Seguridad Perimetral las puertas de enlace de servicios SRX son soluciones de seguridad de red de alto rendimiento para empresas y proveedores de servicios que incluyen alta densidad de puertos, seguridad avanzada y conectividad flexible en plataformas de fácil gestión.

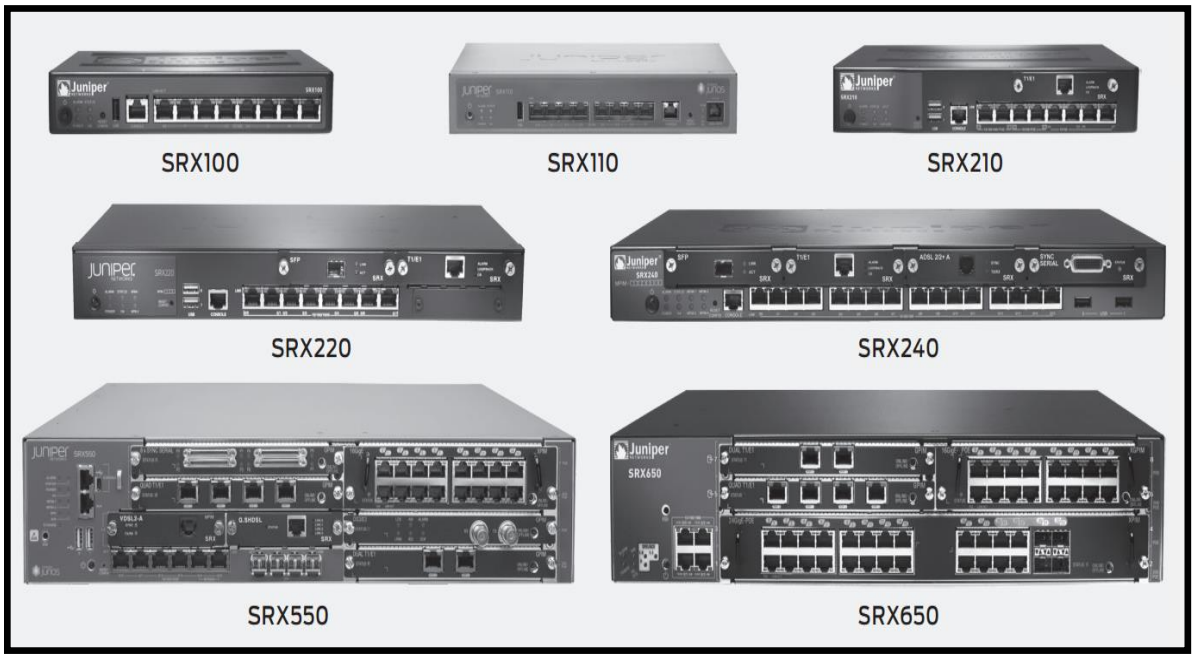


Figura 3.24 Representación de los equipos juniper srx. Fuente: Elaboración propia

Estas soluciones versátiles y rentables admiten operaciones rápidas, seguras y de alta disponibilidad de los centros de datos y las sucursales, y aportan un rendimiento incomparable para ofrecer una relación calidad-precio que se encuentra entre las mejores del sector de redes de datos y solución de seguridad interna y/o externa.

Los equipos Juniper SRX550 Gateway es un todo en uno. Se presenta en forma de un dispositivo con dos unidades de rack integrado de seguridad, enrutamiento, conmutación y conectividad WAN. Es compatible con un firewall para un rendimiento máximo de 5,5 Gbit/s, un rendimiento de VPN IPSec de hasta 1 Gb/s e IPS con un rendimiento de hasta 800 Mbit /s. También incluye la función UnifiedThreat Management (UTM) que consiste en: antivirus, seguridad de

aplicaciones, IPS, filtrado Web anti-spam y avanzado. Los Servicios SRX550 Gateway es ideal para asegurar las medianas y grandes filiales.

La seguridad, los servicios de protección y las capacidades de enrutamiento enriquecido de la serie SRX se basan en Dynamic Services Architecture del sistema operativo Junos., el cual incrementa la eficiencia a nivel de operación del dispositivo. Junos es un sistema operativo confiable y de alto rendimiento para sistemas de enrutamiento, conmutación y seguridad. Reduce el tiempo necesario para desplegar nuevos servicios y disminuye los costos de operación de la infraestructura de red.

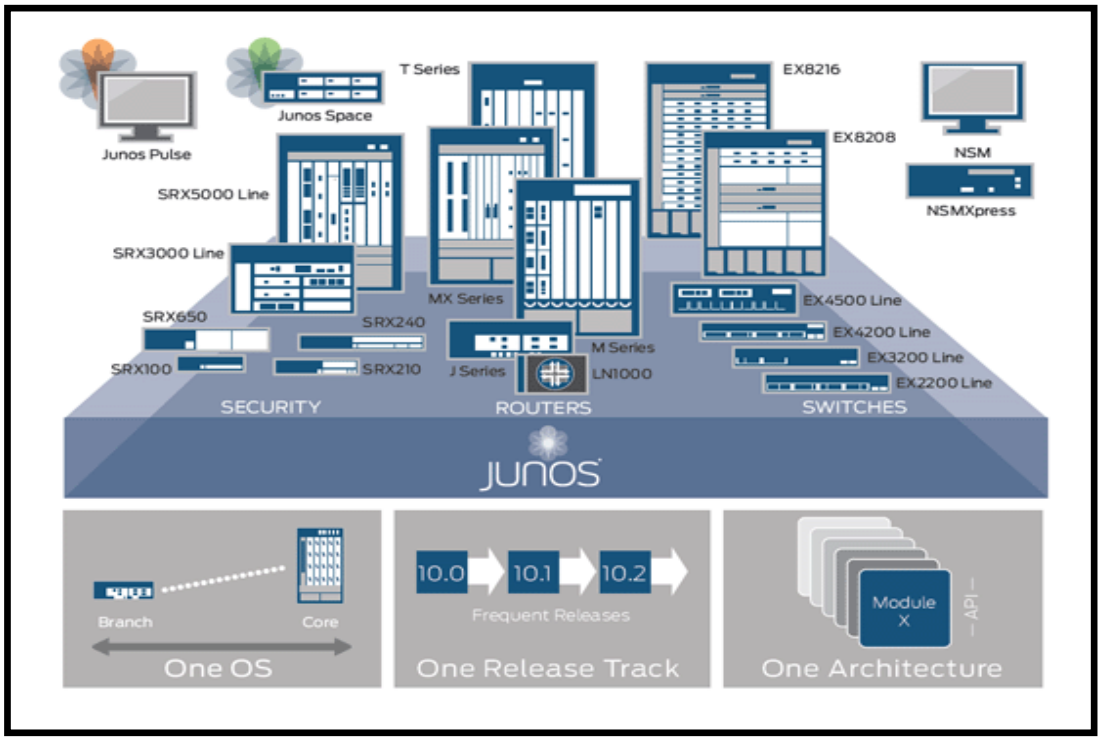


Figura 3.25 Representación de los equipos de seguridad y las versiones de sistema operativo. Fuente: Elaboración propia

Junos es un sistema diseñado para redefinir completamente la manera en que una red funciona. La ejecución de Junos en la red mejora la confiabilidad, el rendimiento y la seguridad de las aplicaciones existentes.

Adicionalmente Junos automatiza las operaciones de red en un sistema simplificado, lo que permite más tiempo para centrarse en el despliegue de nuevas aplicaciones y servicios. Así mismo, Junos es escalable tanto hacia arriba como hacia abajo, proporcionando un sistema constante, confiable y estable para los desarrolladores y operadores.

Junos posee una arquitectura única, con software modular y separación de recursos que permita brindar seguridad, estabilidad, alta disponibilidad y rapidez.

Los Equipos Juniper Networks SRX proporcionan:

Gestión unificada de amenazas (UTM) completamente integrada, la cual permite a las empresas utilizar el nivel adecuado de seguridad necesario en un emplazamiento determinado, en lugar de desplegar una solución para varios dispositivos. Incluye los siguientes sistemas:

- Antivirus
- Prevención de Intrusiones (IPS)
- Filtrado Web
- Antispam

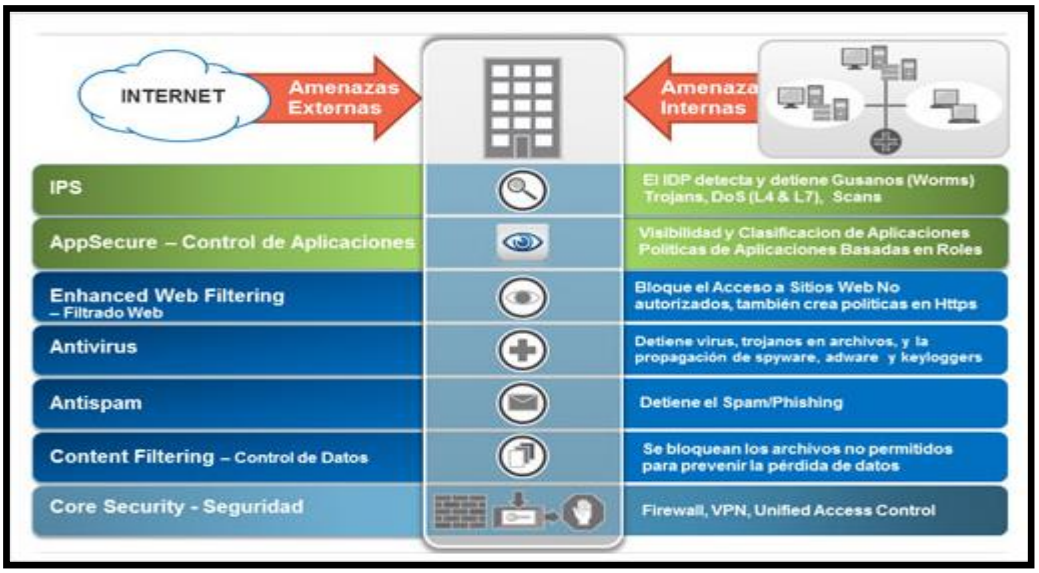


Figura 3.26 Características de los equipos srx aplicados como firewall para la seguridad perimetral. Fuente: Elaboración propia

- Rendimiento escalable: El Acelerador de seguridad de contenido puede procesar amenazas secuencialmente mediante IPS y ExpressAV, de modo que las empresas puedan desplegar la seguridad sin los costes y la complejidad asociados a dispositivos independientes.
- Resistencia de la red y del sistema: Fiabilidad de clase portadora basada en funciones que varían desde hardware y componentes redundantes al software Junos.
- Segmentación de la red: La zona de seguridad, las LAN virtuales (VLAN) y los enrutadores virtuales permiten a los administradores personalizar la seguridad y las políticas de red para varios subgrupos internos, externos y de zona desmilitarizada (DMZ).

- Flexibilidad de interfaces: Configuración de E/S flexible y escalabilidad de E/S independiente para adaptarse a las necesidades de prácticamente cualquier entorno de red.
- Sólido Motor de Procesamiento: El potente procesador de los equipos SRX proporciona separación física y lógica de datos y planos de control con el fin de permitir la implementación de dispositivos de enrutamiento y seguridad consolidados y garantizar la seguridad de las infraestructuras de enrutamiento.
- Exhaustiva protección ante amenazas: Las funciones y servicios de seguridad integrados incluyen un cortafuego de varios gigabits, detección y prevención de intrusiones, denegación de servicio, conversión de direcciones de red y calidad del servicio.

El equipo dispone de los siguientes mecanismos de seguridad que, a nivel de capa 3 del modelo OSI, permite mantener la integridad y disponibilidad del servicio:

- Detección de ataques a la red
- Protección contra ataques DoS (Negación de Servicios) y DDoS.
- Protección frente a la fragmentación y re-ensamblado de paquetes TCP
- Ataques de Fuerza Bruta
- SYN cookie protection
- Protección frente a paquetes mal deformados
- Zone-based IP spoofing

A nivel de capa de nucleó, donde se encuentran todos aquellos equipos que hacen posible la comunicación hacia internet a gran velocidad de tiene la siguiente solución.

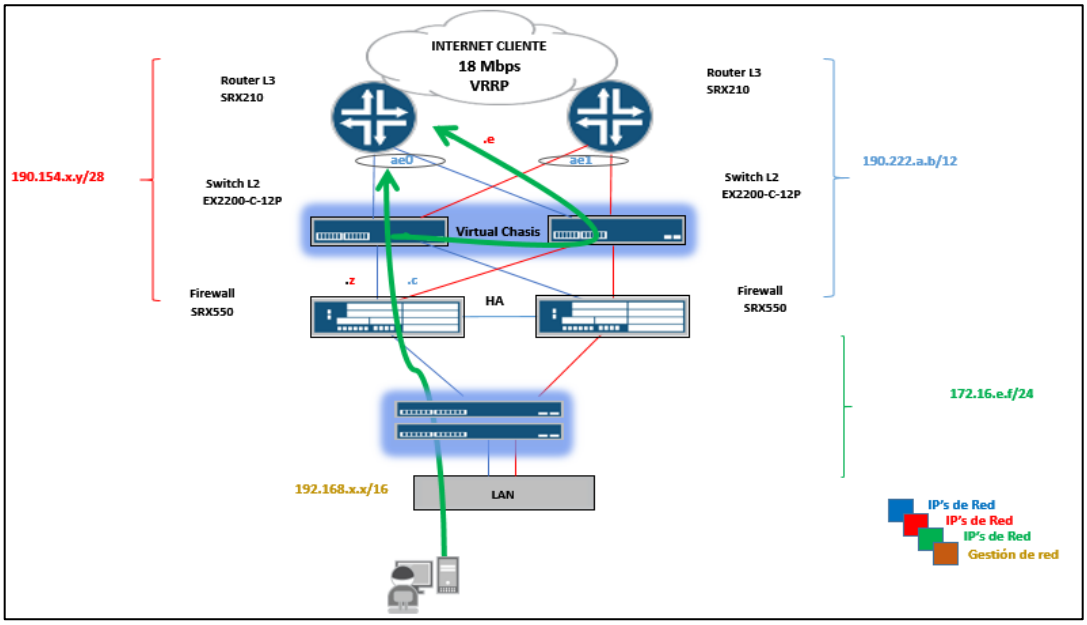


Figura 3.27 Diseño de red, para la alta disponibilidad de enlaces desde la red externa hacia la red interna en la sede secundaria Fuente: Elaboración propia

La arquitectura de red mostrada representa a la sede principal, al tener los enlaces de internet activo / activo, se utiliza switches en la capa de acceso entre los routers y el equipo de seguridad para poder brindar alta disponibilidad de enlaces, al utilizar en el equipo de seguridad configurado en clúster, al estar en este modo de configuración este equipo detecta las caídas de sesiones, ya sea udp y/o tcp. La tecnología en Juniper en poder configurar equipos en alta disponibilidad nos dan la gran ventaja de poder realizar redes redundantes, en todos los niveles.

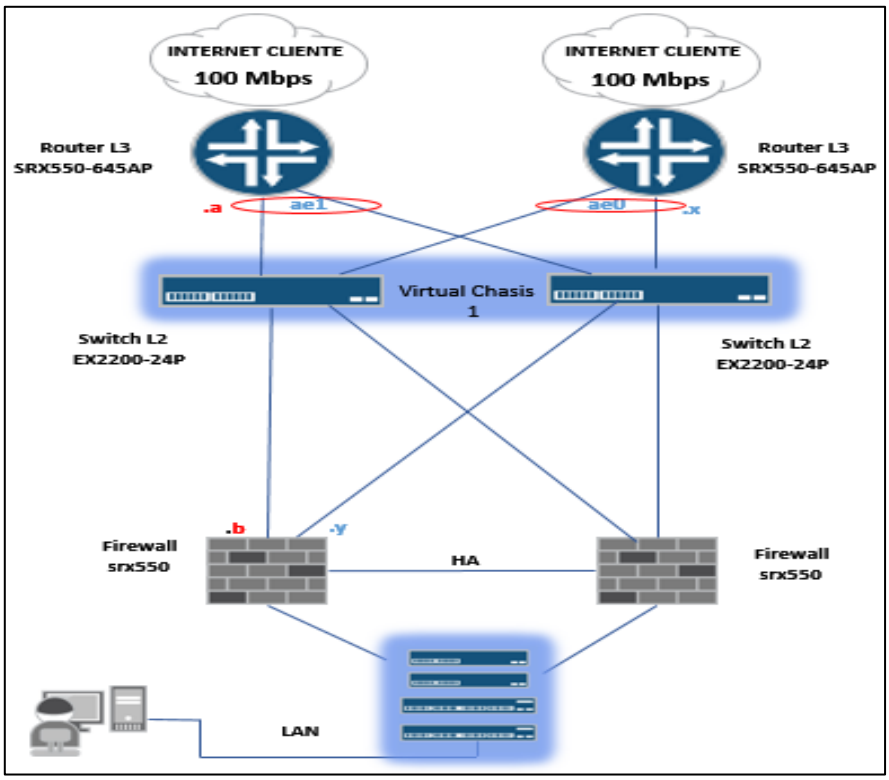


Figura 3.28 Diseño de red de arquitectura de la sede principal y donde se aprecia la alta disponibilidad y las conexiones en alta redundancia entre todos los equipos participantes. Fuente: Elaboración propia

El diseño de red en esta escala utilizamos Lacp entre los routers y los equipos que interconectan los equipos de seguridad, para ante cualquier falla de software o hardware exista la alta disponibilidad de enlaces. Al final se tendrá una configuración entre todas las sedes remotas a nivel de nucleó, y como se explicó anteriormente la conexión entre sedes mediante software que no dan seguridad de red, la gran disponibilidad de los equipo en cada sede de la gama de los srx se pueden aplicar y configurar vpn para interconectar ambos extremos con seguridad encriptado, y dar confiabilidad a la red interna y externa mediante la autenticación de usuarios.

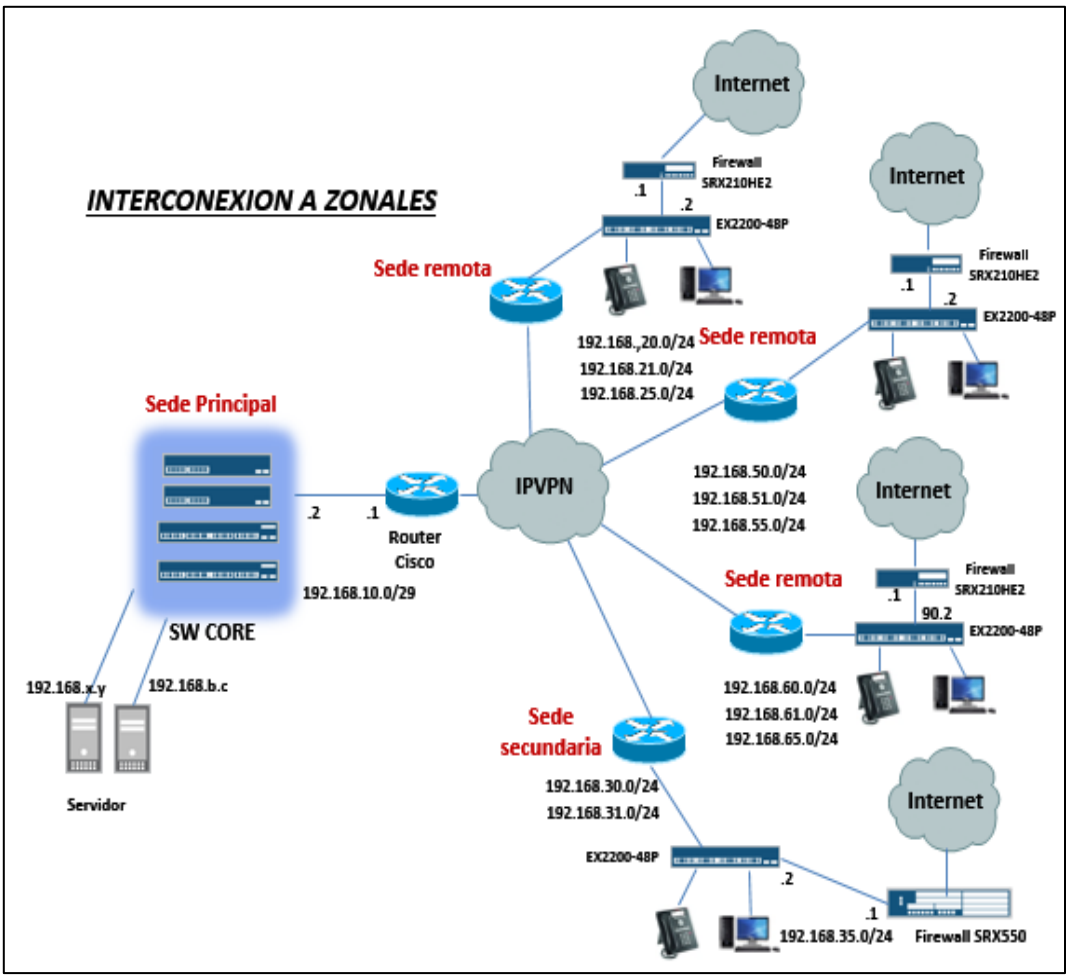


Figura 3.29 Diseño de arquitectura de red, con los equipos juniper en todas las sedes. Fuente: Elaboración propia

La aplicación de filtrado web como característica principal de los equipos juniper srx, en todas las sedes para garantizar la navegación por perfiles, urls y destinos permitidos por el administrador de red y así poder garantizar la administración del ancho de banda toda la red interna y seguridad a todo nivel.

Capa de acceso y distribución:

La realización de la configuración de los equipos es de la siguiente forma, se tomara como inicio del diseño las características del swicth de la Sede principal y como se encuentra estructurado por cada jerarquía, el benefició de los equipos Juniper es la estructura de su entorno de comandos de interfaces de línea (cli).

SEDE	***PRINCIPAL***
DIRECCION IP	192.168.40.0/24
VLANS	VLAN-GENERAL
	VLAN-VOZ
	VLAN-WIFI
SEDE	**SECUNDARIA**
DIRECCION IP	192.168.30.0/24
VLANS	VLAN-GENERAL
	VLAN-VOZ
	VLAN-WIFI
SEDE	**REMOTA-1**
DIRECCION IP	192.168.20.0/24
VLANS	VLAN-GENERAL
	VLAN-VOZ
	VLAN-WIFI
SEDE	**REMOTA-2**
DIRECCION IP	192.168.50.0/24
VLANS	VLAN-GENERAL
	VLAN-VOZ
	VLAN-WIFI
SEDE	**REMOTA-3**
DIRECCION IP	192.168.60.0/24
VLANS	VLAN-GENERAL
	VLAN-VOZ
	VLAN-WIFI

Tabla 1.- Segmentación de la red LAN por sedes remotas

Para realizar una estructuración de la configuración de la actual sede se tiene la siguiente tabla de direcciones ip que desarrollara en esta sede de la empresa donde la gran mayoría de los equipos se encontraban en capa 2 y todos conectados en cascada. La sede de la empresa tenía la siguiente estructura a nivel de direcciones ip y vlan creadas por lo cual se evidencia la necesidad de realizar una segmentación de vlan, para que la red sea estable, para el administrador y todo el entorno de la empresa. La vlan de servidores en la sede principal comparte la misma dirección de red lo cual hace muy dificultoso la asignación de direcciones a usuarios, hay equipos que tienen dirección ip estática y otros que reciben la dirección de red por un servidor dhcp. El problema crece cuando al momento de tener los problemas de la red, por navegación, acceso hacia internet para un nuevo usuario, repercute en que las direcciones ip se agotan. El diseño de un solo segmento en la sede principal hace que la red sea inestable, al no saber qué dirección de red que son asignados a usuarios y telefonía. La problemática de no tener visibilidad, no tener los equipos con una vlan de administración o de gestión hace que se evidencia problemas de ancho de banda. Las demás sede no tienen este problema de inconveniente de escasez de direcciones de re, pero también surge la necesidad de tener una sede remota con diferentes vlan y control de usuarios. Para determinar el nuevo diseño comenzaremos a establecer las direcciones de red para los equipos que estarán presentes en todas las sede, estableciendo la dirección de red de gestión, para que el administrador de red no tenga problemas de asignar una dirección de su red de datos, voz, wifi y servidores. La siguiente tabla, nos representa la

asignación de direcciones de red para cada equipo y su sede correspondiente, usuario y el puerto 22 que hace referencia a ssh.

SEDES	EQUIPOS	IP	Puerto	User
SEDE-PRINCIPAL	*Firewall Sede Principal*	192.168.40.1	22	soporte
	Switch Core-principal	172.16.20.1	22	
	Switch acceso- Informática	172.16.20.2	22	
	Switch acceso- Archivo General	172.16.20.3	22	
	Switch acceso- Administración -1	172.16.20.4	22	
	Switch acceso- Administración -2	172.16.20.5	22	
	Switch acceso- Almacén - Logística	172.16.20.6	22	
	Switch acceso- Módulos de atención	172.16.20.7	22	
	Switch acceso- Ingeniería Proyectos	172.16.20.8	22	
	Switch acceso- Gerencia General	172.16.20.9	22	
	Switch acceso - Área de soporte	172.16.20.10	22	
	controlador-1	172.20.20.4	4343	
	controlador-2	172.20.20.5	4343	
SEDE-SECUNDARIA	*Firewall Sede Principal*	192.168.1.1	22	
	Switch Core-principal	192.168.1.2	22	
SEDE REMOTA-1	*Firewall Sede Principal*	192.168.2.1	22	soporte
	Switch Core-principal	192.168.2.2	22	
SEDE-REMOTA-2	*Firewall Sede Principal*	192.168.3.1	22	
	Switch Core-principal	192.168.3.2	22	
SEDE-REMOTA-3	Firewall Sede Principal	192.168.4.1	22	
	Switch Core-principal	192.168.4.2	22	

Tabla 2.- Direcciones de red de gestión de los equipos en todas las sedes.

La asignación de direcciones de red se explicara dentro de la configuración de la sede principal de la siguiente forma y la creación de vlan en capa 3, para que todas la red este segmentada. En el equipo Juniper el Swicth principal esta designado de la siguiente forma, ya que en este tipo de tecnología las jerarquías

están separadas entre vlan, interfaces, usuarios. Comenzaremos con la creación de usuarios para la sede principal en la jerarquía system, se configura el nombre del equipo, zona horaria y el usuario, el usuario root en los equipos juniper es el que viene por defecto de fábrica, de ahí la necesidad de crear una red segura y establecer usuarios es este caso como se observa se configura un usuario soporte y una de las características de la creación de usurarios es: Se pueden configurar usuarios de total acceso. Super-user y también creación de usuarios de solo lectura y restringir a usuarios al ingreso a solo algunas jerarquías.

```
{master:0}[edit]
admin@Sw-sede-pricipal# show
version 12.3R8.7;
system {
    host-name Sw-sede-pricipal;
    time-zone America/Lima;
    root-authentication {
        encrypted-password "$1$htYP/YMY$QIAn8qb1jANYLf1"; ## SECRET-DATA
    }
    login {
        user soporte {
            uid 2017;
            class super-user;
            authentication {
                encrypted-password "$1$r/hXhQuKSNdqKHmOnVtfi."; ## SECRET-DATA
            }
        }
    }
    services {
        ssh {
            max-sessions-per-connection 32;
        }
        telnet;
        netconf {
            ssh;
        }
        web-management {
            http;
            https {
                system-generated-certificate;
            }
        }
        dhcp {
            traceoptions {
                file dhcp_logfile;
```

Figura 3.30.- Configuración de usuarios y servicios de acceso externo y/o interno. Elaboración propia.

La configuración de la contraseña es encriptado por el equipo y por eso se visualiza de la forma siguiente en la creación de usuarios.

```
login {
    user soporte {
        uid 2017;
        class super-user;
        authentication {
            encrypted-password "$1$r/hXhQuKSNdqKHmOnVtfi."; ## SECRET-DATA
        }
    }
}
```

Figura 3.31.- Configuración de usuarios para acceso del equipo. Elaboración propia.

En este entorno también se habilitan los servicios de los cuales podemos tener gestión de los equipos como son telnet, ssh configurado con un número máximo de conexiones y el acceso vía web para los equipos esta configuración es como el administrador de red este de acuerdo de cómo realizar la gestión de sus equipos.

```
    unit 70 {
        description "INTERFACE RED DE VOZ";
        family inet {
            address 192.168.70.1/24;
        }
    }
    unit 80 {
        description "INTERFACE RED DATOS-1";
        family inet {
            address 192.168.80.1/24;
        }
    }
    unit 81 {
        description "INTERFACE RED DATOS-2";
        family inet {
            address 192.168.81.1/24;
        }
    }
    unit 82 {
        description "INTERFACE RED INTRANET";
        family inet {
            address 192.168.82.2/24;
        }
    }
    unit 83 {
        description "INTERFACE RED SCADA";
        family inet {
            address 192.168.83.1/24;
        }
    }
    unit 84 {
        description "INTERFACE RED_ DATOS";
        family inet {
            address 192.168.84.1/22;
        }
    }
```

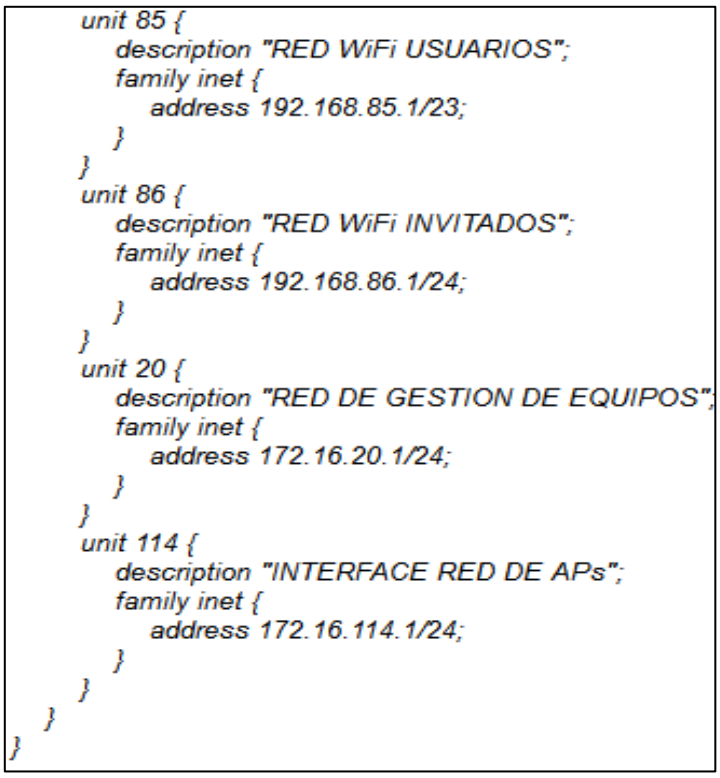


Figura 3.32.- Configuración de las interfaces y segmento de red en capa 3. Elaboración propia.

La configuración de vlan en capa tres en un equipo juniper es de la siguiente forma la característica es de que juniper divide la configuración de capa 2 y 3 en la siguiente forma la opción family inet describe el tipo de vlan capa 3 y la opción Ethernet-switching hace referencia a una vlan de capa 2, en modo acceso y/o troncal.

```
ge-3/0/0 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members DATOS-1;
            }
        }
    }
}
ge-3/0/1 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members DATOS-2;
            }
        }
    }
}
```

Figura 3.33.- Configuración de las interfaces y asociación de vlan en modo acceso y troncal. Elaboración propia.

Después de haber asignado la vlan a los puertos se tiene configurado las vlan en capa 3 y capa 2 de la siguiente forma.

```
{master:0}[edit]
admin@Swicth-sede principal# show
APs {
    vlan-id 114;
    l3-interface vlan.114;
}
DATOS-1 {
    vlan-id 80;
    l3-interface vlan.80;
}
DATOS-2 {
    vlan-id 81;
    l3-interface vlan.81;
}
GESTION_RED {
    vlan-id 20;
    l3-interface vlan.20;
}
INTRANET {
    vlan-id 82;
    l3-interface vlan.82;
}
SCADA {
    vlan-id 83;
    l3-interface vlan.83;
}
```

Figura 3.34.- Configuración de las vlans en capa 3. Elaboración propia.

La configuración de la redundancia de enlaces, se realiza de la siguiente de la siguiente forma, esta configuración nos garantiza la redundancia de enlace, para eso utilizamos Lacp en los switches de acceso y distribución para garantizar la redundancia, para tener interfaces agregadas, ingresamos en la jerarquía que se muestra en la configuración.

Recordar que un ae soporta 8 interfaces lo cual es la suma de cada interface, no solamente en conexión física sino en cantidad de velocidad de transmisión.

La jerarquía es chassis y muestra los siguientes parámetros:

```
chassis {
    aggregated-devices {
        ethernet {
            device-count 11;
        }
    }
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
    auto-image-upgrade;
}
```

Figura 3.35.- Configuración de las interfaces agregadas. Elaboración propia.

Y las interfaces agregadas se crean como una interfaz lógica como son los ae, los cuales son agrupaciones de interfaces físicas, esta configuración se realización e interconexión de los switches de acceso con el swicth principal, mediante la conexión de cada interfaz lógica configurado a 1Gbps y cómo se va a tener configurado dos enlaces por swicth de acceso entonces nos da resultado de un enlace de 2Gbps.

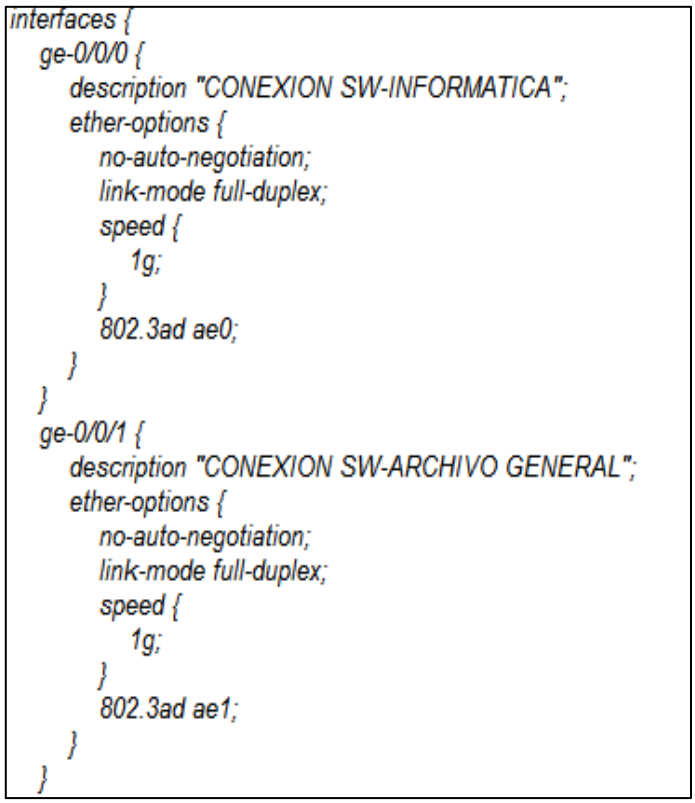


Figura 3.36.- Configuración de las interfaces y asociación de enlace agregados para la redundancia de enlaces. Elaboración propia.

Como se observa la configuración de las interfaces agregadas para generar alta redundancia en los equipos de la empresa en la capa de acceso y distribución.

```
ge-0/0/2 {
    description "CONEXION  SW-ADMIN-1";
    ether-options {
        no-auto-negotiation;
        link-mode full-duplex;
        speed {
            1g;
        }
        802.3ad ae2;
    }
}
ge-0/0/3 {
    description "CONEXION  SW-ADMIN-2";
    ether-options {
        no-auto-negotiation;
        link-mode full-duplex;
        speed {
            1g;
        }
        802.3ad ae3;
    }
}
ge-0/0/4 {
    description "CONEXION SW-ALM-LOGISTICA";
    ether-options {
        no-auto-negotiation;
        link-mode full-duplex;
        speed {
            1g;
        }
        802.3ad ae4;
    }
}
```

Figura 3.37.- Configuración de las distintas áreas de la empresa y su enlace agregado para la redundancia de enlaces. Elaboración propia.

Las interfaces agrupadas de la siguiente manera nos brindan alta redundancia de enlace y se puede evidenciar de la siguiente forma.

Se puede observar que las interfaces agregadas desde una interfaz agregada se encuentra activo, en los equipos juniper en la gama de switches se ingresa hacia la jerarquía run show vlan este comando nos muestra los ae y las interfaces, con lo cual se concluye que vlan es la que está aprendiendo, una característica es poder observar en signo asterisco encima de la interfaz agregada (lógica) y la interfaz física con su número de puerto correspondiente.

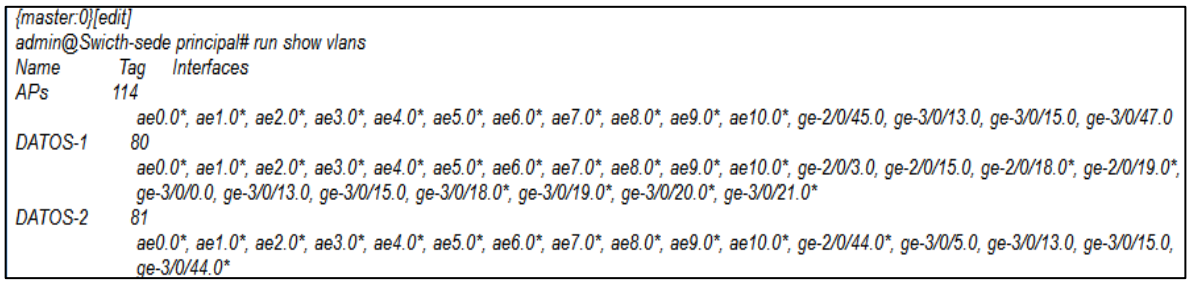


Figura 3.38.- Estado de las interfaces y asociación a la vlan que corresponde y/o aprende. Elaboración propia

Las interfaces en los equipos juniper están representados como se muestra en la imagen donde como por ejemplo: ge-0/0/1 el primer número indica el FPC l cual significa el equipo físico, el swicth como caja, el segundo nos indica la posición de los puertos, en un equipo con 48 puertos , sería el Slot 0 , pero si el switch presenta un módulo de conexión hacia fibra ese módulo de puertos seria conocido como slot 1 y la configuración seria ge-0/1/1, el ultimo indica el número de puerto de la del swicth, en los equipos juniper la numeración es desde el puerto ge-0/0/0 hasta el puerto ge-0/0/47, con todos los números pares en la parte superior y los impares en la parte inferior. En nuestro equipo los puertos que son utilizados para que dos equipos formen uno solo es la tecnología virtual chassis, como antes explicado se puede garantizar la redundancia y alta disponibilidad de equipos., si tenemos un solo equipo la representación de puertos es la siguiente:

- ge-0/0/47 un solo equipo nos indica el primer número de la izquierda.
- ge-1/0/47 dos equipos nos indica el primer número de la izquierda.
- ge-2/0/47 tres equipos nos indica el primer número de la izquierda.
- ge-3/0/47 cuatro equipos nos indica el primer número de la izquierda.

Finalmente podemos observar el estado de los puertos mediante el siguiente comando, que se muestra en la figura, la opción admin es la conexión de hardware de los puertos y que se encuentra activas, si esta opción está en down se tendría que revisar el puerto físicamente y la opción link nos indica la conexión de un puerto y su estado operativo.

También se puede observar que nos indica el tipo de family es si pertenece a un puerto en capa 2 o en capa 3

```
{master:0}[edit]
admin@Swicth-sede principal# run show inerfaces terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/0                up    up
ge-0/0/0.0              up    up   eth-switch
ge-0/0/1                up    up
ge-0/0/1.0              up    up   eth-switch
ge-0/0/2                up    up
ge-0/0/2.0              up    up   inet     192.168.80.1/24
ge-0/0/3                up    up
ge-0/0/3.0              up    up   eth-switch
ge-0/0/4                up    down
ge-0/0/4.0              up    down eth-switch
ge-0/0/5                up    up
ge-0/0/5.0              up    up   eth-switch
ge-0/0/6                up    up
ge-0/0/6.0              up    up   eth-switch
ge-0/0/7                up    up
ge-0/0/7.0              up    up   eth-switch
ge-0/0/8                up    up
ge-0/0/8.0              up    up   eth-switch
ge-0/0/9                up    up
ge-0/0/9.0              up    up   eth-switch
ge-0/0/10               up    down
ge-0/0/10.0             up    down eth-switch
```

Figura 3.39.-Estado de las interfaces operativas y no activas. Elaboración propia

Para garantizar la gestión delos equipos por personal de soporte y/o administrador de red, se configura en el equipo un filtro de seguridad en la jerarquía firewall, esto configuración nos garantiza que solo el personal de gestión de los equipos switches pueda tener acceso a los equipos mediante, telnet, ssh y la interfaz web.

```
firewall {
    family inet {
        filter Filtro-Gestion-Red {
            term Permit-Gestion {
                from {
                    source-address {
                        192.168.41.12/32;
                        192.168.42.12/32;
                        192.168.62.12/32;
                        192.168.21.12/32;
                        192.168.50.12/32;
                        192.168.30.12/32;
                        192.168.41.16/32;
                        192.168.42.16/32;
                        192.168.41.6/32;
                        192.168.40.6/32;
                    }
                    protocol tcp;
                    destination-port [ ssh telnet http https ];
                }
                then accept;
            }
            term Deny-Gestion {
                from {
                    protocol tcp;
                    destination-port [ ssh telnet http https ];
                }
                then {
                    discard;
                }
            }
            term Default-Term {
                then accept;
            }
        }
```

Figura 3.40.- Configuración de filtros para la administración de los equipos. Elaboración propia

Donde solo se asigna en este filtro las direcciones ip del personal encargado, las demás direcciones de red, denegarle el acceso y/o descartar el acceso a personal no autorizado. Con lo cual se realizan filtros para que distintas vlan en capa 3 no

puedan tener comunicación entre ellas, con este resultado nos garantiza que el usuario que se encuentre en la vlan de datos no tenga acceso a la vlan de servidores, donde se le deniega el acceso por icmp.

La siguiente configuración nos muestra el estado de dos equipos configurados de virtual chasis en un equipo de acceso en la sede principal donde la jerarquía donde se configura esta plataforma es la de virtual chassis, y los equipos son dos designados como miembro 0 que es el equipo master y el equipo miembro 2 designado como miembro 1 backup, que ante cualquier falla del equipo master este asumirá dicha característica.

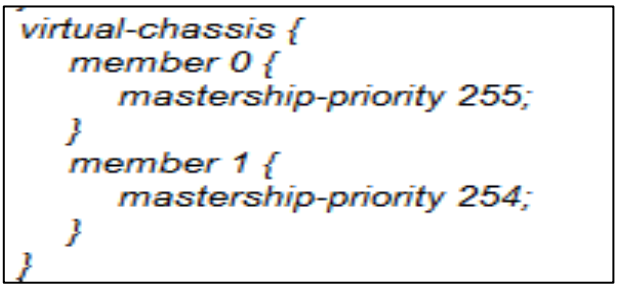


Figura 3.41.- Configuración del estado dl virtual chassis en el equipo.
Elaboración propia

Las prioridades son importantes porque nos indican que los equipos están, tanto el master y el backup, con prioridad 255 y 254, que función tiene y que característica cumplen es la que si el master por índoles fallas tienden tener problemas automáticamente el backup asume este rol de master, pero una vez solucionado, se desea agregar el equipo en la funcionalidad de virtual chasis, con esto el equipo por tener una prioridad mayor a la del equipo configurado backup, recupera

el rol de master. Todas las características y configuración son replicadas en los equipo tanto de acceso y distribución como el caso de los equipos asignados en la empresa como swicth principal y swiches de acceso.

```
ae0 {
    description "LINK AGGREGATION INFORMATICA";
    aggregated-ether-options {
        lacp {
            active;
        }
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ GESTION-RED VOZ DATOS-1 DATOS-2 APs WiFi_Usuarios  ];
            }
        }
    }
}
ae1 {
    description "LINK AGGREGATION SW-ARCHIVO GENERAL";
    aggregated-ether-options {
        lacp {
            active;
        }
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ GESTION-RED VOZ DATOS-1 DATOS-2 RED-DATOS  APs WiFi_Usuarios ];
            }
        }
    }
}
```

Figura 3.42.- Configuración de filtros para la administración de los equipos. Elaboración propia

Solo el equipo asignado como swicth principal es que comparte la vlan en capa 3 y es distribuido a los otros equipos mediante enlaces troncales donde se distribuyen todas las vlan, que son datos, voz y gestión de red, solo los switches de acceso tienen una ruta configurada que todos tienen como destino al equipo principal , ya que pertenecen a la vlan de gestión, el los equipos de wifi comparten una vlan de

wifi , la cual para los equipos Access point deben tener una vlan de ap. entonces el equipo de la sede principal le designa mediante dhcp a los equipos inalámbricos y los demás usuarios reciben ip desde el servidor dhcp, pero se configura en el equipo para que mediante un dhcp-Relay las consultas sean directamente consultados hacia el servidor.

```
    dhcp {
        traceoptions {
            file dhcp_logfile;
            level all;
            flag all;
        }
        pool 172.16.114.0/24 {
            address-range low 172.16.114.10 high 172.16.114.60;
            router {
                172.16.114.1;
            }
            option 43 byte-stream "105 112 58 49 55 50 48 49 54 46 49 48 48 46 46 48 53";
        }
        pool 192.168.86.0/24 {
            address-range low 192.168.86.20 high 192.168.86.220;
            name-server {
                192.168.70.8;
                192.168.20.10;
            }
            router {
                192.168.70.1;
            }
        }
    }
}
```

Figura 3.43.- Configuración del servicio dhcp. Elaboración propia

La consultas de asignar dhcp están, directamente relacionadas al servidor dhcp pero los equipos inalámbricos reciben dhcp desde el mismo equipo principal, la asignación de separar la vlan de Access point con la vlan de red wifi es la siguiente el controlador de acceso inalámbrico con la que tiene la empresa reconoce los equipos, pero al tener una mala distribución, no se puede segmentar en una sola vlan de default, por tal motivo se crea vlan de usuarios internos e

invitados para después el controlador se configure un enlace troncal y sea conectado al controlador, de esta manera si se puede configurar las vlan provenientes del controlador y poder tener la vlan ap. como una vlan creada para la gestión de los Access point.

La configuración de los protocolos para la no generación de bucles entre los equipos de acceso y distribución viene dado de la siguiente manera, asumiendo el equipo principal el papel root, que los términos de spanning tree, es un rol muy importante.

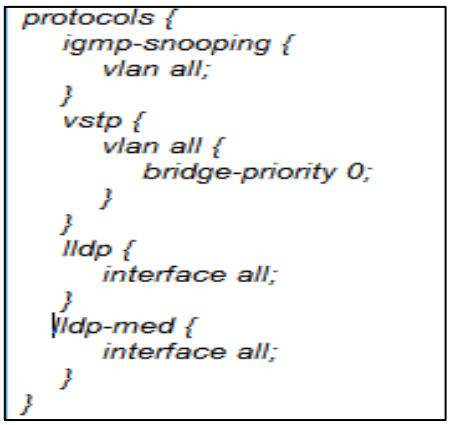


Figura 3.44.- Configuración de los protocolos de descubrimiento de los equipos. Elaboración propia

También se configura en esta jerarquía el descubrimiento de vecinos en los equipos lo cual para realizar un descarte en la red es muy importante por ya al tener creado la vlan de gestión y asignarle una ruta en cada equipo de acceso, con destino hacia el principal nos permite realizar saltos desde cualquier equipo hacia el swicth configurado como principal.

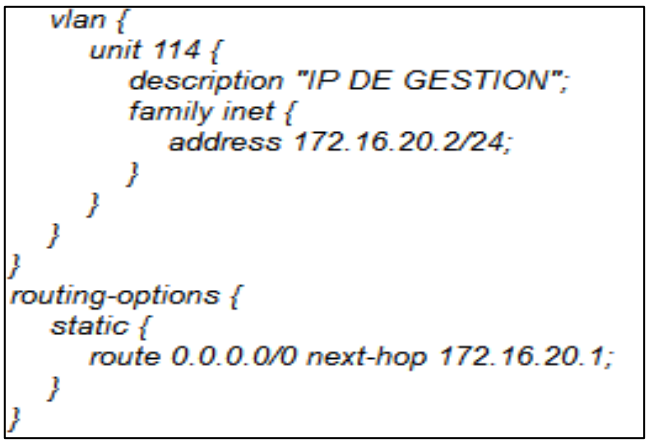


Figura 3.45.- Configuración de la vlan de gestión y el enrutamiento estático. Elaboración propia

Con esta configuración, se tiene acceso a los equipos con la vlan de gestión. Y el problema de la telefonía era que compartían la misma vlan tanto teléfonos y computadoras de los usuarios, para esto se crearon distintas vlan, vlan de datos y vlan de voz, la particularidad de los equipos juniper es que tienen una jerarquía donde el mismo puerto, es designado como puerto para los teléfonos asociados con su respectiva vlan, esta vlan llega al teléfono y después es la misma interfaz está asociada a la vlan de datos.

Este resultado nos garantiza que la conexión proveniente del swicth de acceso va directamente al teléfono con su respectiva vlan de voz y del teléfono una conexión hacia la computadora o portátil con la respectiva vlan de datos.

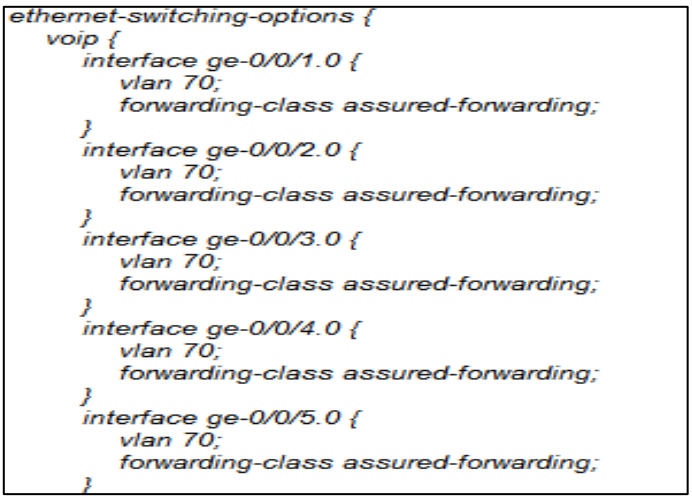


Figura 3.46.- Configuración de las interfaces aplicados como vlan de voz. Elaboración propia

Asociada a su respectiva vlan de datos y voz (en cada interface) y la configuración admite los equipos que se energizan mediante PoE, y también mediante comandos se puede deshabilitar esta opción para dispositivos no PoE. Solo en los switches de capa de acceso se configuran vlan de capa 2.

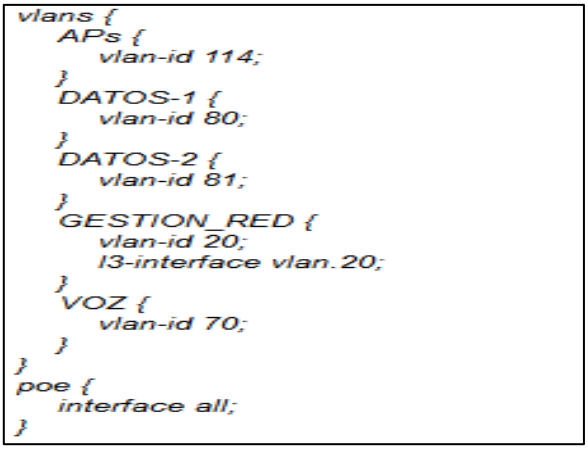


Figura 3.47.- Configuración de vlans en capa 2 y 3. Elaboración propia

Y poder verificar el estado de los equipos mediante comandos, desde la temperatura de funcionamiento, el consumo de memoria y estado si es equipo master o backup.

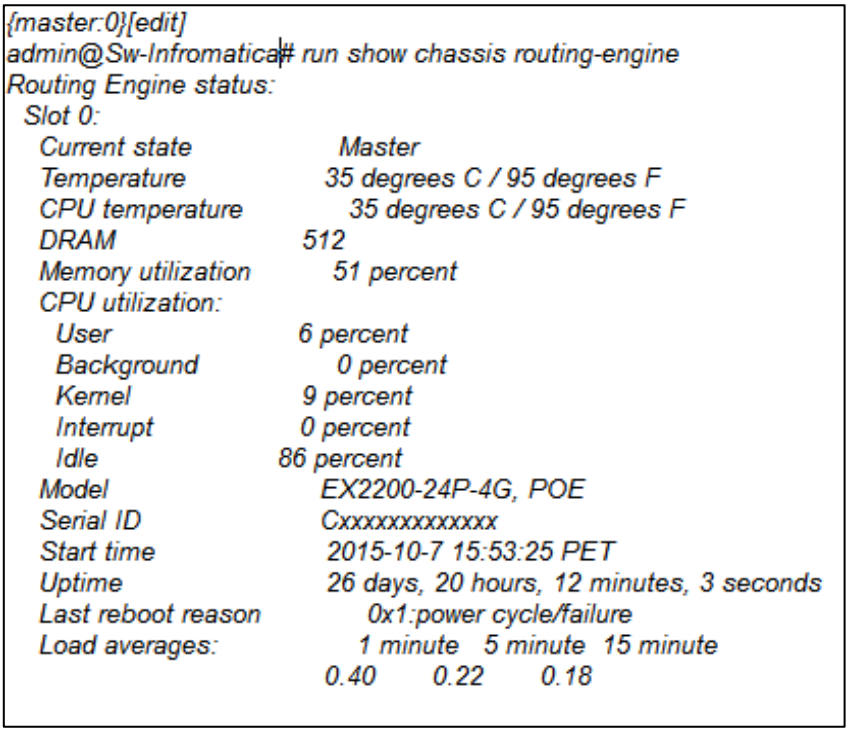


Figura 3.47.-Verfificacion del estado físico del equipo. Elaboración propia

Los equipo configurados en virtual chassis, tienen la particularidad que mediante la consola de gestión se puede ingresar al equipo configurado como master, cada vez que el fabricante realice una actualización del sistema operativo, no es necesario realizarlo en cada equipo, sino solamente realizarlo en el equipo designado como master y replicarlos mediante comando a todos los miembros del virtual chasis. Por ultimo de muestra las conexiones físicas de los equipos juniper en el laboratorio antes de realizar cualquier implementación. Recordar que para

configurar un equipo en virtual chassis tienen que tener la misma versión del sistema operativo y realizar unos comandos que permiten armar el virtual chassis entre todos los equipos configurados con esta última opción realizada, particularidad de los equipos juniper, y llegar a una tener un plano de control del equipo configurado como master y una copia activa entre los demás miembros del virtual chassis, con esto garantizamos la alta redundancia y disponibilidad de los equipos y conexiones. Las imágenes que se muestran son de los equipos juniper, de la gama de los switches.

Figura 3.48.- Equipo juniper instalado en el laboratorio donde se realizaron pruebas de armado de virtual chassis. Elaboración propia

Figura 3.49.- Conexiones de los cables de alimentación. Elaboración propia

Los switches, y los tres puertos que están hacia la izquierda, son de administración, consola y entrada USB para realizar las actualizaciones, que también se pueden realizar mediante ftp (transferencia de archivos) y entorno web.

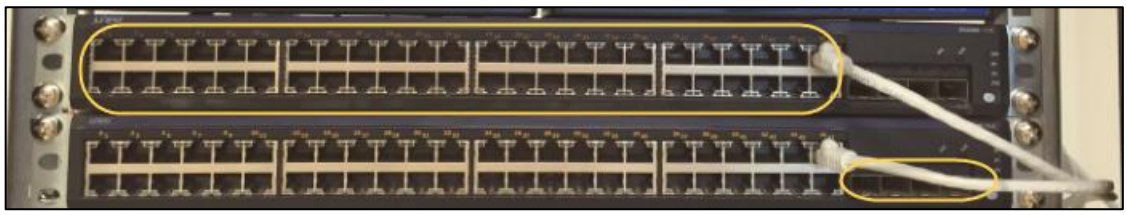


Figura 3.50.- Indica el slot 0 y la captura más pequeña el slot 1. Elaboración propia

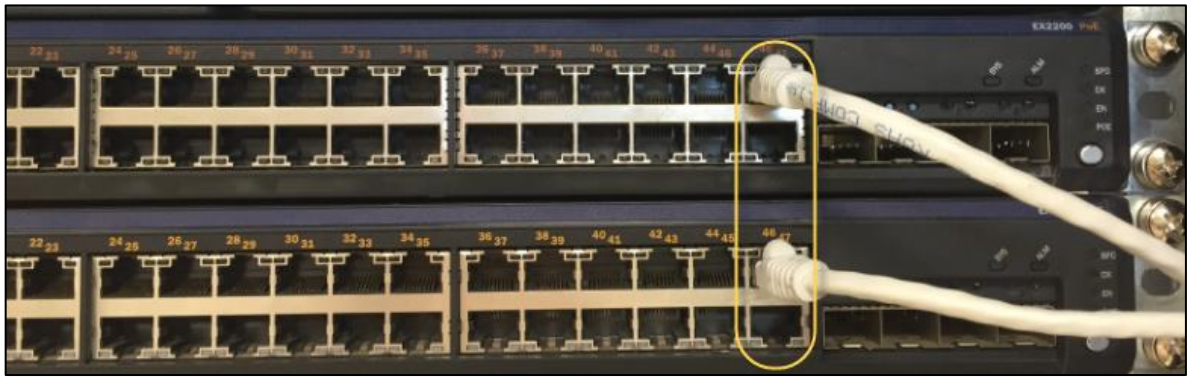


Figura 3.51.- Puertos designados para la configuración de virtual chassis, recomendable los últimos dos puertos de cada swicth.

Después tenemos las conexiones de los puertos asignados a las vlan correspondientes

Figura 3.51.- Encendido de los equipos y sus conexiones. Elaboración propia

En encendido del equipo y el estado de los puertos que indican que el equipo esta funcionamiento**.**

El estado de los puertos está en operación como se observa, en la prueba de laboratorio.

Figura 3.52.- Equipos configurados en virtual chassis, uno representa al equipo de capa de acceso otro de capa de distribución. Elaboración propia

Figura 3.53.- Equipo swicth configurado como equipo principal. Elaboración propia

Figura 3.54.- Equipo configurado como swicth de acceso y sus conexiones en el equipo juniper. Elaboración propia

Las pruebas de configuración se realizaron con pruebas de alta disponibilidad con los equipos de seguridad que serán explicados en el siguiente paso.

Figura 3.55.- Conexión de los equipos juniper con laptops asociadas a distintas vlan. Elaboración propia

Figura 3.56.- Pruebas de laboratorio y las conexiones de los equipos juniper mediante cable consola para ingresar al modo de configuración. Elaboración propia.

Capa de núcleo (acceso hacia internet)

En la capa de acceso y distribución de puede observar la alta redundancia de los equipos, mediante la utilización de enlaces agregados, aplicación de vlan en capa 3 (vlan de usuarios, acceso inalámbrico y de voz), el uso de filtros para la gestión de red, y que las demás vlan de capa 3 no tengan comunicación entre los usuarios de las distintas áreas.

La tecnología y el crecimiento de un red, se ve reforzada por equipos robustos, entorno a la seguridad perimetral, los cuales por ser en algunos casos equipos que no vienen en uno solo, sino equipos que son independientes como son los equipos IPS (sistemas de prevención de intrusión), que protegen a una red de los ataques provenientes desde la red externa, filtros dedicados para el control de la navegación, configuración que se realiza en línea de comandos y con la aplicación de equipos que necesitan de una tarjeta y/o modulo externo.

Para todos estos sistemas que preocupan a los administradores de red, como son los ataques de denegación de servicio, infección en la red, no disponibilidad de sus servicios, la saturación de su red, sin saber las causas y/o mala administración por parte del personal de soporte o área de tecnología de la información.

Un diseño de arquitectura de red, debe de tener alta disponibilidad, en software (sistema operativo en la que funciona el equipo) y hardware (arquitectura interna del equipo, circuitos electrónicos), todo aquello es lo que resume a un equipos en alta disponibilidad, que los servicios estén fallidos ante un error humano y/o artificial.

El inconveniente principal de la arquitectura que presentaba la empresa es tener un equipo que su función principal era de brindar seguridad en la red, en el equipo presentaba las siguientes características:

Cisco ASA 5520	
Fabricado para entornos	Empresas pequeñas
Resumen de rendimiento	
Capacidad máxima de procesamiento (Mbps) del firewall	**450**
Capacidad máxima de procesamiento (Mbps) de VPN 3DES/AES	**225**
Cantidad máxima de sesiones de usuario de VPN de sitio a sitio y de acceso remoto	**750**
Cantidad máxima de sesiones de usuario de VPN SSL1	**750**
Cantidad máxima de conexiones	**280000**
Cantidad máxima de conexiones /segundo	**9000**
Paquetes por segundo (64 bytes)	**320000**

Tabla 3.- Características técnicas del equipo antiguo. Elaboración propia.

Las características mostradas, representan la actualidad de la empresa, se puede observar un número determinado de conexiones, concurrentes en una red que puede soportar el equipo, también el máximo número de conexiones mediante el uso de VPN (conexiones seguras y/o red privada virtual).

Las características de hardware, que para la demanda creciente de la tecnología y el acceso hacia las aplicaciones, demandan de mucho consumo de memoria y necesitan conexión con puertos de giga-Ethernet,

Resumen técnico	
Memoria (MB)	512
Memoria flash del sistema (MB)	64
Puertos integrados	4-10/100/100--1-10/100
Cantidad máxima de interfaces virtuales (VLAN)	150
Ranura de expansión SSC/SSM	SI (SSM)

Tabla 4.- Características técnicas del equipo antiguo. Elaboración propia.

Las aplicaciones y/o módulos externos (equipos modulares), mediante la utilización de tarjetas externas, licencias para cada característica como filtrado URLs. Filtrado de contenidos, Antispam, etc. Todo lo mencionado hace que una red sea más vulnerable en todos los aspectos, seguridad y alta disponibilidad.

Cambio de la capa de núcleo (acceso hacia internet y seguridad perimetral)

Lo citado anteriormente, nos presenta las dificultades de la red en términos de seguridad y alta disponibilidad.

Se presenta como solución una arquitectura de red confiable, las características se pueden observar en el siguiente cuadro, con la cantidad de conexiones

Juniper srx550	características
Junos OS sistema operativo	Junos OS 12.1
Capacidad máxima de procesamiento (máx.)	5.5 Gbps
IPS performance (NSS 4.2.1)	800 Mbps
AES256+SHA-1 / 3DES+SHA-1 conexiones VPN	1.0 Gbps
Cantidad máxima de conexiones	375,000
Nuevas sesiones/por segundo(TCP)	27,000
Máximo seguridad de políticas	7,256

Tabla 5.- Características técnicas del equipo juniper SRX. Elaboración propia.

Si se realiza un comparativo, entre las dos tecnologías antes usadas se puede observar la ventaja del procesamiento, y lo resaltado en la cantidad máxima de conexiones de los dos equipos. En la empresa se dispone implementar un equipos Juniper srx550, con la características de disponer dos equipos para realizar alta disponibilidad (la configuración de Cluster), el equipo anterior un cisco 5520, por ser un equipo que el fabricante ya no produce y la necesidad del administrador de red de poder brindar una renovación tecnológica en los equipos tanto de seguridad, acceso y distribución, se menciona los siguientes criterios de diseño.

- **Seguridad perimetral (uso de dos equipos Juniper srx550), configurados en Cluster /alta disponibilidad.**

Para tener una red estable y ante puntos de falla, mencionados, se dispone de dos equipos de seguridad del fabricante juniper, modelo srx550, por su máximo número de conexiones, capacidad de poder ser utilizado mediante Cluster,

activo/activo y/o activo/pasivo. La integración de filtrado web, filtrado de contenidos, seguridad IPS, configuración de VPN site to site y/o dinámicas mediante la adquisición de licencia la última mencionada, creación de Nat (traducción de direcciones de red), creación de políticas en un entorno de líneas de comandos, entorno web (guide), y la aplicación de filtros de seguridad, y la funcionalidad de screen, que es una protección adicional que tiene los equipos juniper en la gama de seguridad.

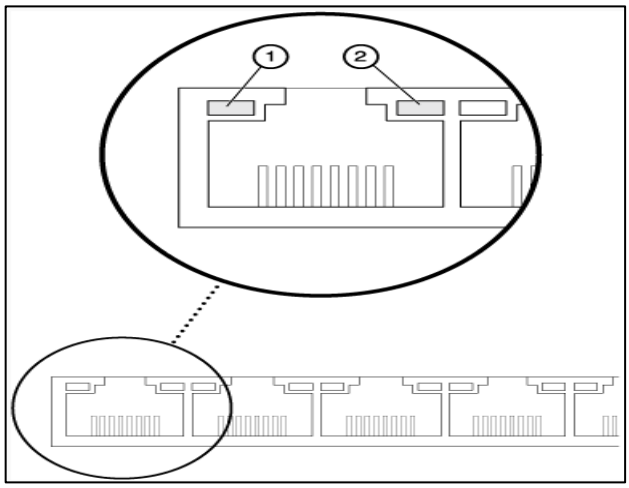
Ante los criterios antes mencionados se resume el funcionamiento de la configuración del equipo de seguridad y su acceso hacia la red externa, para la seguridad de la empresa. Estatus del panel frontal.

Componente	Descripción	Uso
LED de alarma	• Rojo fijo indica una alarma importante. • Luz ámbar fija indica una alarma menor. • Desactivado indica que el dispositivo se está iniciando. Nota: Cuando el sistema está en marcha y funcionando, si el LED de alarma está apagado, indica que no hay alarmas presentes en el dispositivo.	El LED de alarma se puede utilizar para recoger información sobre las alarmas mayores o menores, o para determinar si el dispositivo está funcionando normalmente.
LED de status	• Verde fijo indica que el dispositivo está funcionando normalmente. • Luz ámbar fija indica que el dispositivo se está iniciando. • Rojo fijo indica que el	El LED de status se puede utilizar para determinar si el dispositivo se está iniciando, está funcionando normalmente, o ha fallado.

	dispositivo ha fallado	
LED Mini-PIM	• Verde fijo indica que el Mini-PIM está funcionando normalmente. • Apagado indica que el Mini-PIM no está presente o no detectada por el dispositivo.	El LED Mini-PIM puede ser utilizado para determinar si el Mini-PIM está presente y detectado por el dispositivo
LED de Power	• Verde fijo indica que el dispositivo está funcionando normalmente. • Luz ámbar fija indica que el botón de encendido ha sido presionado y liberado rápidamente. • Desactivado indica que el dispositivo no está recibiendo alimentación.	El LED de alimentación se puede utilizar para determinar si el dispositivo está recibiendo alimentación.
LED HA	• Verde fijo indica que todas las conexiones HA están disponibles. • Rojo fijo indica que las conexiones HA no están funcionando como se esperaba. • Luz ámbar fija indica que algunos enlaces de HA no están funcionando como se esperaba. • Apagado indica que HA no está habilitada.	El LED de HA se puede utilizar para determinar si la alta disponibilidad está activada en el dispositivo.

Tabla 6.- Características de encendido del equipo SRX. Elaboración propia.

LED de puerto Ethernet: se adjunta tabla donde se muestra el estado del led.



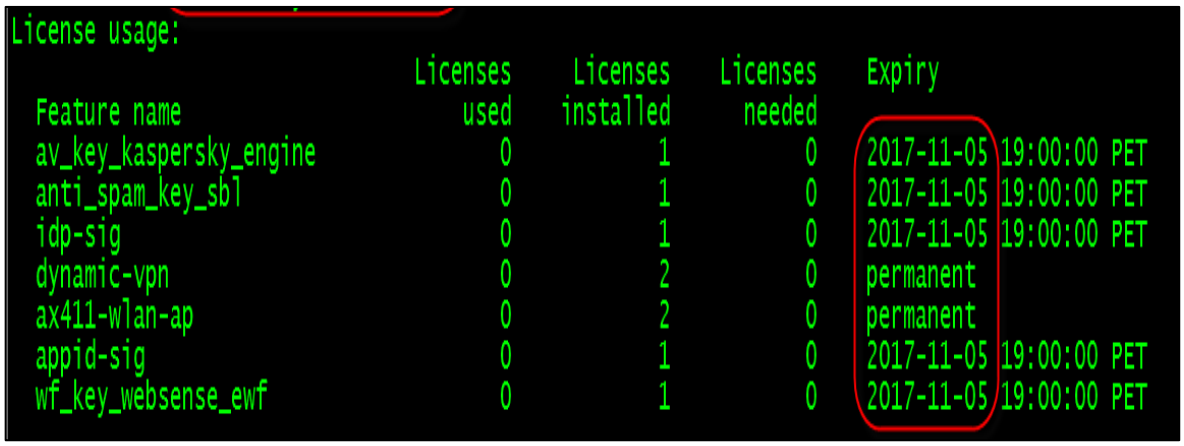
Puerto Ethernet (comportamiento y estado de LEDs)**:**

Número	Función	Color	Status	Descripción
1		Verde	parpadeo	Enlace está activo. La comunicación de datos está en proceso
			estable	Enlace está activo. No hay comunicación
		Apagado	Apagado	Enlace está inactivo.
2		Verde	Estable	Alimentación a través de Ethernet está encendido y el dispositivo de alimentación conectado está recibiendo alimentación.

Tabla 7.-Estado de led de encendido del equipo SRX. Elaboración propia.

La funcionalidad del equipo permite configurar distintos perfiles a nivel de seguridad de navegación, controlar a los usuarios por perfiles predeterminados por el filtro, permite configurar reglas que el equipo juniper en la gama de seguridad. La herramienta de filtrado, esta funcionalidad se llama web-Filtering, un motor de

aplicaciones e inspección de contenido de navegación, mediante enlace con un servidor en la nube websense, nos permite controlar todas estas aplicaciones, que mediante la actualización de firmas nos permite tener una red estable, a lo referente de control de navegación por usuario y contenido, ya que la creación de perfiles nos permite individualizar, agrupar y gestionar la navegación, mediante la activación de firmas ya predefinidas, todo esto es posible con la agregación de licencias para este propósito, no hay necesidad de tener que agregar equipos modulares y/o tarjetas, equipos de la gama alta tienen esta funcionalidad mediante la activación de licencias, como es el equipo que para el funcionamiento se utiliza un srx 550, las licencias de ips (sistema de prevención de intrusos), antivirus utilizando la plataforma de karpesky y lo referido a el correo malicioso como aliado a el motor de la nube shopos.



License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine	0	1	0	2017-11-05 19:00:00 PET
anti_spam_key_sbl	0	1	0	2017-11-05 19:00:00 PET
idp-sig	0	1	0	2017-11-05 19:00:00 PET
dynamic-vpn	0	2	0	permanent
ax411-wlan-ap	0	2	0	permanent
appid-sig	0	1	0	2017-11-05 19:00:00 PET
wf_key_websense_ewf	0	1	0	2017-11-05 19:00:00 PET

Figura 3.57- Configuración del Perfil y respectivo Web Filtering con las categorías respectivas. Elaboración propia.

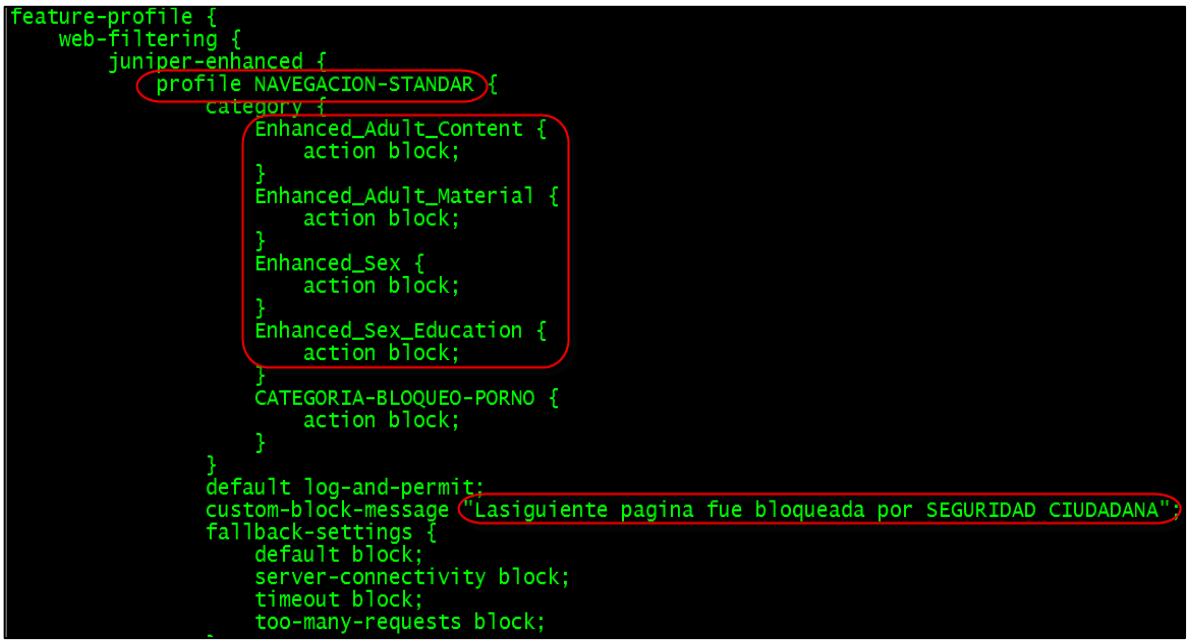


Figura 3.58- Configuración del Perfil y respectivo Web Filtering con las categorías respectivas. Elaboración propia.

La configuración del filtrado por perfiles nos permite, agrupar diferentes categorías de contenido de navegación con la estructura de poder generar perfiles, de lista blanca (sitios de navegación permitidos), listas negras (navegación a sitios web con mala reputación y/o que los administradores de red no permitan a los usuarios finales en su red interna).

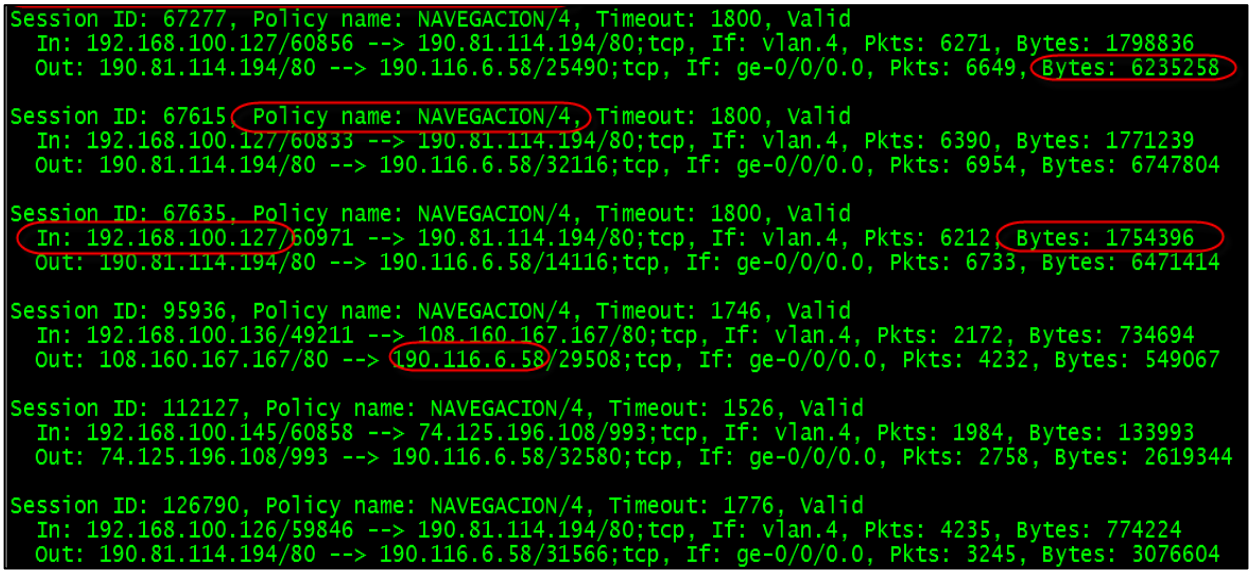
El esquema de configuración se muestra de la siguiente forma, perfil con el nombre del grupo de usuarios de la red interna, que al momento de que el motor de control de filtrado web sea utilizado, muestra el mensaje de bloqueo y/o no autorización en la red por la empresa.

Todo esto es posible si en la política de la zona interna red LAN, se le asocia este perfil configurado en la jerarquía utm (en el equipo juniper).

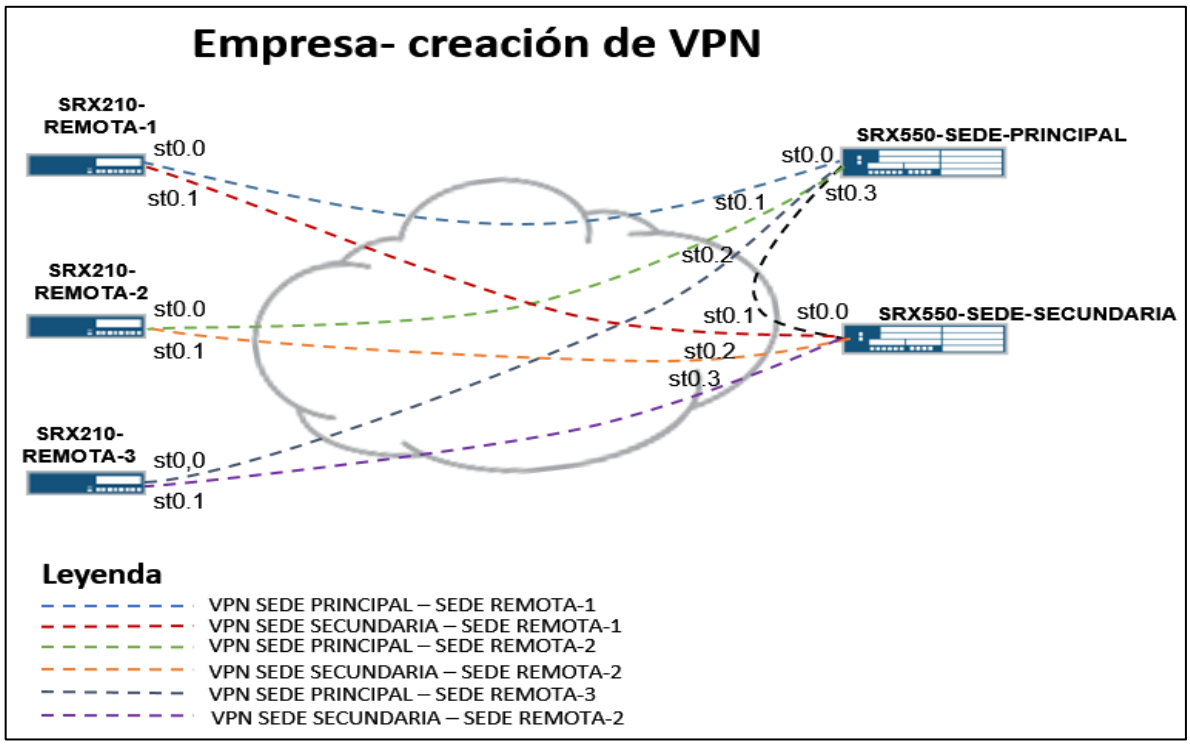
```
security {
    utm {
        custom-objects {
            url-pattern {
            }
        }
        feature-profile {
            web-filtering {
                juniper-enhanced {
                    profile NAVEGACION-STANDAR {
                        category {
                            Enhanced_Adult_Content {
                                action block;
                            }
                            Enhanced_Adult_Material {
                                action block;
                            }
                            Enhanced_Sex {
                                action block;
                            }
                            Enhanced_Sex_Education {
                                action block;
                            }
                            CATEGORIA-BLOQUEO-PORNO {
                                action block;
                            }
                        }
                        default log-and-permit;
                        custom-block-message "La siguiente página fue bloqueada por EMPRESA";
                        fallback-settings {
                            default block;
                            server-connectivity block;
                            timeout block;
                            too-many-requests block;
                        }
                    }
                }
            }
        }
        utm-policy UTM-BLOQUEO {
            web-filtering {
                http-profile NAVEGACION-STANDAR;
            }
        }
    }
        rule-set Navegacion {
            from zone LAN;
    policies {
        from-zone LAN to-zone WAN {
            policy NAVEGACION {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
```

```
                utm-policy UTM-BLOQUEO;
            }
        }
    }
}
}
```

Se muestra las sesiones de los usuario de la Zona LAN, política activa NAVEGACION y tipo de filtrado.



Cuando nos referimos de seguridad y alta disponibilidad tenemos que afrontar dos obstáculos, saber si los equipos presentan estas características y la estabilidad que me puede brindar en la red. El equipo que la empresa tiene como seguridad hacia internet es un equipo que se encuentra configurado en Cluster, asociación de dos equipos en alta disponibilidad uno activo y el otro pasivo. Con lo cual nos permite



La configuración de vpn (redes privadas virtuales) entre las sedes, para tener interconexión con todas las sedes remotas y mantener una conexión estable, gráficamente se representa el túnel establecido en ambos sentidos, ya que el túnel es preparado con métodos de encriptación en ambos extremos.

```
{primary:node0}[edit]
admin@FW-EMPRESA# run show version
node0:
--------------------------------------------
Hostname: FW-EMPRESA
Model: srx550
JUNOS Software Release [12.1X46-D35.1]

node1:
--------------------------------------------
Hostname: FW-EMPRESA
Model: srx550
JUNOS Software Release [12.1X46-D35.1]

{primary:node0}[edit]
adminT@FW-EMPRESA#
```

La versión del equipo juniper, sistema operativo que se renueva por el fabricante cada tres meses.

Configuración de un chasis clúster en el equipo srx 550 el cual se puede observar, los puertos asociados hacia cada nodo, al ser un equipo configurado en activo /pasivo, y con la opción de poder conmutar mediante caídas de interfaces.

```
{primary:node0}[edit chassis]
admin@FW-EMPRESA# show
cluster {
    reth-count 7;
    redundancy-group 0 {
        node 0 priority 200;
        node 1 priority 150;
    }
    redundancy-group 1 {
        node 0 priority 200;
        node 1 priority 150;
        preempt;
        gratuitous-arp-count 4;
        interface-monitor {
            ge-6/0/0 weight 255;
            ge-6/0/1 weight 255;
            ge-6/0/2 weight 255;
            ge-6/0/4 weight 255;
            ge-6/0/5 weight 255;
            ge-15/0/0 weight 255;
            ge-15/0/1 weight 255;
            ge-15/0/2 weight 255;
```

Representación de los nodos en un equipo configurado en clúster (alta disponibilidad)

```
{primary:node0}[edit]
admin@FW-EMPRESA# run show chassis cluster status
Monitor Failure codes:
    CS  Cold Sync monitoring         FL  Fabric Connection monitoring
    GR  GRES monitoring              HW  Hardware monitoring
    IF  Interface monitoring         IP  IP monitoring
    LB  Loopback monitoring          MB  Mbuf monitoring
    NH  Nexthop monitoring           NP  NPC monitoring
    SP  SPU monitoring               SM  Schedule monitoring

Cluster ID: 1
Node   Priority Status          Preempt Manual   Monitor-failures

Redundancy group: 0 , Failover count: 1
node0  200      primary         no      no       None
node1  150      secondary       no      no       None

Redundancy group: 1 , Failover count: 19
node0  200      primary         yes     no       None
node1  150      secondary       yes     no       None

{primary:node0}[edit]
```

Cantidad de sesiones que presenta el equipo, mediante el uso de comandos de interface de línea

```
{primary:node0}[edit]
admin@FW-EMPRESA# run show security flow session summary
node0:
--------------------------------------------------------------------------
Unicast-sessions: 1360
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1376
  Valid sessions: 1359
  Pending sessions: 0
  Invalidated sessions: 17
  Sessions in other states: 0
Maximum-sessions: 524288

node1:
--------------------------------------------------------------------------
Unicast-sessions: 1387
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1473
  Valid sessions: 1381
  Pending sessions: 0
  Invalidated sessions: 92
  Sessions in other states: 0
Maximum-sessions: 524288
```

La configuración muestra el uso de inspección de intrusiones, en un equipo srx mediante la activación en las zonas donde se desea proteger de ataques, por ser una zona vulnerable la zona externa, se aplica en la zona WAN, en la configuración admite varias reglas de protección para servidores, paquetes que se pueden ver afectados por ataques externos.

```
{primary:node0}[edit security idp]
admin@FW-EMPRESA# show
idp-policy IDP-EMPRESA {
    rulebase-ips {
        rule 1 {
            /* This rule is designed to protect your networks against important TCP/IP attacks. */
            match {
                from-zone WAN;
                to-zone any;
                application default;
                attacks {
                    predefined-attack-groups [ "[Recommended]IP - Critical" "[Recommended]IP - Minor"
"[Recommended]IP - Major" "[Recommended]TCP - Critical" "[Recommended]TCP - Minor"
"[Recommended]TCP - Major" ];
                }
            }
            then {
                action {
```

```
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 2 {
        /* This rule is designed to protect your network against important ICMP attacks. */
        match {
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]ICMP - Major" "[Recommended]ICMP -
Minor" ];
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 3 {
        /* This rule is designed to protect your network against important HTTP attacks. */
        match {
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]HTTP - Critical" "[Recommended]HTTP -
Major" "[Recommended]HTTP - Minor" ];
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 4 {
        /* This rule is designed to protect your network against important SMTP attacks. */
        match {
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]SMTP - Critical" "[Recommended]SMTP -
```

```
Major" "[Recommended]SMTP - Minor" ];
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 5 {
        /* This rule is designed to protect your network against important DNS attacks. */
        match {
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]DNS - Critical" "[Recommended]DNS -
Minor" "[Recommended]DNS - Major" ];
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 6 {
        /* This rule is designed to protect your network against important FTP attacks. */
        match {
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]FTP - Critical" "[Recommended]FTP -
Minor" "[Recommended]FTP - Major" ];
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 7 {
        /* This rule is designed to protect your network against important POP3 attacks. */
        match {
```

```
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]POP3 - Critical" "[Recommended]POP3 -
Minor" "[Recommended]POP3 - Major" ];
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 8 {
        /* This rule is designed to protect your network against important IMAP attacks. */
        match {
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]IMAP - Critical" "[Recommended]IMAP -
Major" ];
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
    rule 9 {
        /* This rule is designed to protect your network against common internet malware. */
        match {
            from-zone WAN;
            to-zone any;
            application default;
            attacks {
                predefined-attack-groups [ "[Recommended]TROJAN - Critical"
"[Recommended]TROJAN - Major" "[Recommended]TROJAN - Minor" "[Recommended]VIRUS -
Critical" "[Recommended]VIRUS - Major" "[Recommended]VIRUS - Minor"
"[Recommended]WORM - Critical" "[Recommended]WORM - Major" "[Recommended]WORM -
Minor" ];
            }
        }
        then {
            action {
                recommended;
            }
```

```
            notification {
                log-attacks;
            }
        }
    }
  }
}
active-policy IDP-EMPRESA;

{primary:node0}[edit security idp]
admin@FW-EMPRESA#
```

Mediante comandos tenemos un resumen de los ataques que ha detectado el equipo, y se puede tener una breve descripción del evento, que se realizo o detecto el equipo la cantidad de hits, son los intentos que se produjeron en ese evento.

```
{primary:node0}[edit]
admin@FW-EMPRESA# run show security idp attack table
node0:
--------------------------------------------------------------------
IDP attack statistics:

  Attack name                                   #Hits
  HTTP:CGI:BASH-CODE-INJECTION                  140
  HTTP:PHP:PHPMYADMIN:SETUP-SCAN                106
  HTTP:PHP:WP-SLIDER-REV-AFD                    17
  HTTP:SQL:INJ:CHAR-ENCODE                      12
  HTTP:SQL:INJ:DECLARE-EXEC                     12
  HTTP:SQL:INJ:MS-SQL-FUNCTIONS                 12
  HTTP:SQL:INJ:PROC-GENERIC                     12
  HTTP:SQL:INJ:SYSOBJECTS                       12
  HTTP:SQL:INJ:UNION-SELECT                     12
  HTTP:PHP:PHP-CGI-CMD-LINE-RCE                 10
  HTTP:PHP:WP-INCLUDES-ACCESS                   8
  HTTP:PHP:CMD-INJ                              2
  HTTP:DLINK-AUTHENTICATION-BO                  1
  HTTP:EXPLOIT:ILLEGAL-HOST-CHAR                1
  HTTP:REQERR:NULL-IN-HEADER                    1

node1:
--------------------------------------------------------------------

{primary:node0}[edit]
admin@FW-EMPRESA#
```

```
{primary:node0}[edit]
admin@FW-EMPRESA# run show security idp attack description HTTP:CGI:BASH-CODE-INJECTION
Description: This signature detects attempts to exploit a known vulnerability against GNU Bash. A
             successful attack can lead to arbitrary code execution.

{primary:node0}[edit]
admin@FW-EMPRESA# run show security idp attack description HTTP:PHP:PHPMYADMIN:SETUP-SCAN
Description: This signature detects attempts to access the setup.php script of a PHPMyAdmin enabled
             website.  Generally, this script is only enabled on an unconfigured installation of
             PHPMyAdmin , and is disabled after first use.  If you are setting up PHPMyAdmin for the first
             time, you may trigger this signature non-maliciously.  Otherwise, this is most likely an
             attempt to find an unconfigured PHPMyAdmin instance in your network.  A successful attack
             could result in arbitrary code execution.

{primary:node0}[edit]
admin@FW-EMPRESA# run show security idp attack description HTTP:PHP:WP-SLIDER-REV-AFD
Description: This signature detects attempts to exploit known flaws in the Slider Revolution Responsive
             WordPress plug-in.  A successful attack could result in arbitrary files being downloaded from
             the server, including sensitive system files containing system configuration files,
             administrative credentials, and server databases.

{primary:node0}[edit]
admin@FW-EMPRESA# run show security idp attack description HTTP:SQL:INJ:CHAR-ENCODE
Description: This signature detects SQL commands with character conversion within a URL. The char()
             function converts hexadecimal and decimal values into characters to be interpreted by the SQL
             engine.  By encoding common injection variables, attackers can attempt to evade detection.
             Because SQL commands are not normally used in HTTP connections, this can indicate a SQL
             injection attack. However, it can be a false positive.  To reduce false positives, it is
             strongly recommended that these signatures only be used to inspect traffic from the Internet
             to your organization's Web servers that use SQL backend databases to generate content and not
             to inspect traffic going from your organization to the Internet.

{primary:node0}[edit]
admin@FW-EMPRESA#
```

Breve descripción de los eventos, que nos indica que tipo de evento y/o ataque ha presentado el equipo, todo esto se puede reservar mediante log para su respectivo análisis, y se muestra la versión la seguridad mediante ips en el equipo juniper.

```
{primary:node0}[edit]
admin@FW-EMPRESA#
 run show security idp security-package-version
node0:
--------------------------------------------------------------------------

  Attack database version:2525(Wed Oct 09 17:11:36 2015 UTC)
  Detector version :12.6.160150609
  Policy template version :2527

node1:
--------------------------------------------------------------------------

  Attack database version:2525(Wed Oct 09 17:11:36 2015 UTC)
  Detector version :12.6.160150609
  Policy template version :2527
```

Se puede realizar mediante línea de comando, la representación del plano de control, el cual maneja la tabla de enrutamientos, protocolos, procesamiento de políticas, inspección de filtrado web y la temperatura que trabaja el equipo, también se puede observar el estado de los ventiladores de la fuente de alimentación del equipo por cada nodo activo y pasivo.

```
{primary:node0}[edit]
admin@FW-EMPRESA# run show chassis environment
node0:
--------------------------------------------------------------------------
Class Item                           Status     Measurement
Temp  Routing Engine                 OK         27 degrees C / 80 degrees F
      Routing Engine CPU             OK         27 degrees C / 80 degrees F
      Routing Engine                 Absent
      Routing Engine CPU             Absent
Fans  SRXSME Chassis Fan 0           OK         Spinning at normal speed
      SRXSME Chassis Fan 1           OK         Spinning at normal speed
      SRXSME Chassis Fan 2           OK         Spinning at normal speed
      SRXSME Chassis Fan 3           OK         Spinning at normal speed
Power Power Supply 0                 OK
      Power Supply 1                 Absent

node1:
--------------------------------------------------------------------------
Class Item                           Status     Measurement
Temp  Routing Engine                 OK         24 degrees C / 75 degrees F
      Routing Engine CPU             OK         24 degrees C / 75 degrees F
      Routing Engine                 Absent
      Routing Engine CPU             Absent
Fans  SRXSME Chassis Fan 0           OK         Spinning at normal speed
      SRXSME Chassis Fan 1           OK         Spinning at normal speed
      SRXSME Chassis Fan 2           OK         Spinning at normal speed
      SRXSME Chassis Fan 3           OK         Spinning at normal speed
Power Power Supply 0                 OK
      Power Supply 1                 Absent

{primary:node0}[edit]
admin@FW-EMPRESA#
```

La configuración de protección de pantalla, es muy favorable en un entorno de seguridad en cual realiza un escaneo de todos los ataques que provienen de redes externas, mediante el análisis de paquetes, que pueden ocasionar una denegación de servicio (Dos y/o Ddos).

```
{primary:node0}[edit security screen]
admin@FW-EMPRESA# show
ids-option SCREEN-EMPRESA {
    icmp {
        ip-sweep threshold 1000;
        fragment;
        large;
        flood threshold 200;
        ping-death;
    }
    ip {
        bad-option;
        stream-option;
        spoofing;
        strict-source-route-option;
        unknown-protocol;
        tear-drop;
    }
    tcp {
        syn-fin;
        tcp-no-flag;
        syn-frag;
        port-scan threshold 1000;
        syn-ack-ack-proxy threshold 500;
        syn-flood {
            alarm-threshold 500;
            attack-threshold 500;
            source-threshold 50;
            destination-threshold 1000;
            timeout 10;
        }
        land;
        winnuke;
        tcp-sweep threshold 1000;
    }
    udp {
        flood threshold 500;
        udp-sweep threshold 1000;
    }
    limit-session {
        source-ip-based 1000;
    }
}

{primary:node0}[edit security screen]
admin@FW-EMPRESA#
```

Se muestra una configuración muy robusta, entorno a parámetros que permite analizar este contenido de paquetes provenientes de la red externa, todo esto es posible realizar un monitoreo mediante líneas de comando, el cual nos da

evidencia de la cantidad de paquetes analizados en la zona de ingreso del equipo de seguridad, todo esto se aplica en la zona Wan, a diferencia de idp que puede ser aplicado entre zonas internas, la aplicación de protección de pantalla realiza protección externa.

Mediante registros o log, con la configuración de files y/o carpetas donde se puede mencionar a que tipo de evento realiza mención en un determinado tiempo, para su respectivo análisis para el administrador de red, o para mitigar un ataque.

```
node0:
--------------------------------------------------------------------------
Screen object status:

Name                                        Value
  ICMP flood threshold                      200
  UDP flood threshold                       500
  TCP winnuke                               enabled
  TCP port scan threshold                   1000
  ICMP address sweep threshold              1000
  TCP sweep threshold                       1000
  UDP sweep threshold                       1000
  IP tear drop                              enabled
  TCP SYN flood attack threshold            500
  TCP SYN flood alarm threshold             500
  TCP SYN flood source threshold            50
  TCP SYN flood destination threshold       1000
  TCP SYN flood timeout                     10
  IP spoofing                               enabled
  ICMP ping of death                        enabled
  TCP land attack                           enabled
  TCP SYN fragment                          enabled
  TCP no flag                               enabled
  IP unknown protocol                       enabled
  IP bad options                            enabled
  IP strict source route option             enabled
  IP stream option                          enabled
  ICMP fragmentation                        enabled
  ICMP large packet                         enabled
  TCP SYN FIN                               enabled
  TCP SYN-ACK-ACK proxy threshold           500
  Session source limit threshold            1000
```

Aplicación para la protección de pantalla en el equipo de seguridad, en la zona WAN.

```
{primary:node0}[edit security zones]
admin@FW-EMPRESA# show
security-zone WAN {
    screen SCREEN-EMPRESA;
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth0.0;
    }
}
security-zone DMZ {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth2.0;
    }
}
security-zone LAN {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth1.0;
    }
}
```

La configuración de zonas en el equipo de seguridad, nos permite separar lógicamente zonas destinados a servidores, grupos de trabajos, y desarrollar comunicación entre diferentes usuarios con restricción de puertos mediante la configuración de políticas de seguridad entre zonas.

```
from-zone WAN to-zone DMZ {
    policy SEGURIDAD-DMZ {
        match {
            source-address 172.16.20.40;
            destination-address any;
            application [ junos-http junos-https TCP_8888 junos-icmp-all junos-ftp ];
        }
      then {
            permit {
                application-services {
                    idp;
                }
            }
        }
    }
    policy   policy SEGURIDAD-DMZ-1 {
        match {
            source-address 172.16.20.45;
            destination-address any;
            application [ junos-http junos-https TCP_8888 junos-icmp-all junos-ftp ];
        }
      then {
            permit {
                application-services {
                    idp;
                }
            }
        }
    }
    policy   policy SEGURIDAD-DMZ -2{
        match {
            source-address [ WEB-1    TEST-1  WEB-2 ];
            destination-address any;
            application [ junos-http junos-https TCP_8888 junos-icmp-all junos-ftp ];
        }
      then {
            permit {
                application-services {
                    idp;
                }
            }
        }
```

```
    }
 policy   policy SEGURIDAD-DMZ-3 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            denny;
        }
    }
```

Las opciones de carpeta que nos permite almacenar registros y/o log de eventos, aunque el equipo almacene estos log de forma ya predefinida, lo que se realiza aquí es poder mencionar que carpeta pertenece a cada sistema de protección se requiere analizar.

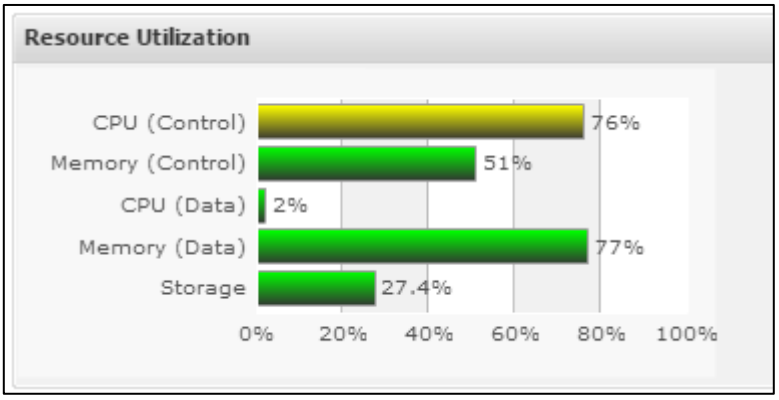
```
{primary:node0}[edit system syslog]
admin@FW-EMPRESA# show
archive size 100k files 3;
user * {
    any emergency;
}
host 10.0.0.101 {
    any any;
    port 1302;
}
file messages {
    any critical;
    authorization info;
    archive size 1000k files 5 no-world-readable;
    structured-data {
        brief;
    }
}
file FLOW-DENY {
    any any;
    match RT_FLOW_SESSION_DENY;
    archive size 1000k files 10 world-readable;
    structured-data {
        brief;
    }
}
file FLOW-PERMIT {
    any any;
    match RT_FLOW_SESSION_CREATE;
```

```
    archive size 1000k files 10 world-readable;
    structured-data {
        brief;
    }
}
file FLOW-CLOSE {
    any any;
    match RT_FLOW_SESSION_CLOSE;
    archive size 1000k files 10 world-readable;
    structured-data {
        brief;
    }
}
file interactive-commands {
    interactive-commands error;
}
file IDP {
    any any;
    match IDP_ATTACK_LOG_EVENT;
    archive size 3m files 15 world-readable;
    structured-data {
        brief;
    }
}
file SCREEN-MESSAGES {
    any any;
    match RT_SCREEN_IP;
    archive size 1000k files 5 world-readable;
    structured-data {
        brief;
    }
}

{primary:node0}[edit system syslog]
admin@FW-EMPRESA#
```

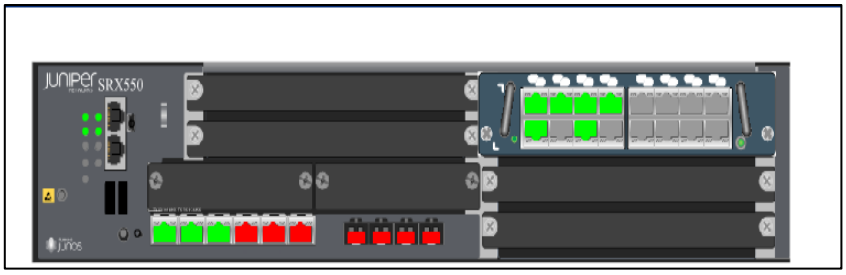
Y mediante líneas de comandos podemos determinar la cantidad de paquetes en la zona externa del equipo de seguridad, como es inundación por paquetes icmp y udp, para poder realizar una denegación de servicio.

```
admin@FW-EMPRESA# run show security screen statistics zone WAN
node0:
--------------------------------------------------------------------------
Screen statistics:

IDS attack type                              Statistics
  ICMP flood                                 12005
  UDP flood                                  66987368
  TCP winnuke                                0
  TCP port scan                              0
  ICMP address sweep                         0
  TCP sweep                                  1765
  UDP sweep                                  0
  IP tear drop                               0
  TCP SYN flood                              5288
  IP spoofing                                0
  ICMP ping of death                         0
  IP source route option                     0
  TCP land attack                            0
  TCP SYN fragment                           0
  TCP no flag                                0
  IP unknown protocol                        0
  IP bad options                             0
  IP record route option                     0
  IP timestamp option                        0
  IP security option                         0
  IP loose source route option               0
  IP strict source route option              0
  IP stream option                           0
  ICMP fragment                              0
  ICMP large packet                          345
  TCP SYN FIN                                0
  TCP FIN no ACK                             0
```

El equipo y su representación gráfica mediante la interfaz web, los puertos mostrados de color rojo son los puertos que o se usan, los puertos de color verde son los que actualmente están en funcionamiento y por ultimo por un tema de protección y no se realice un error se realizó el apagado de los puertos que no so utilizados y se muestran de color plomo.



Los puertos en operación y los que se encuentran desactivados por un tema de protección.



3.2-REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS

Se han configurado los equipos de tal manera que el tráfico valla por el enlace señalado, cuando exista caída de conexión del router hacia la nube.

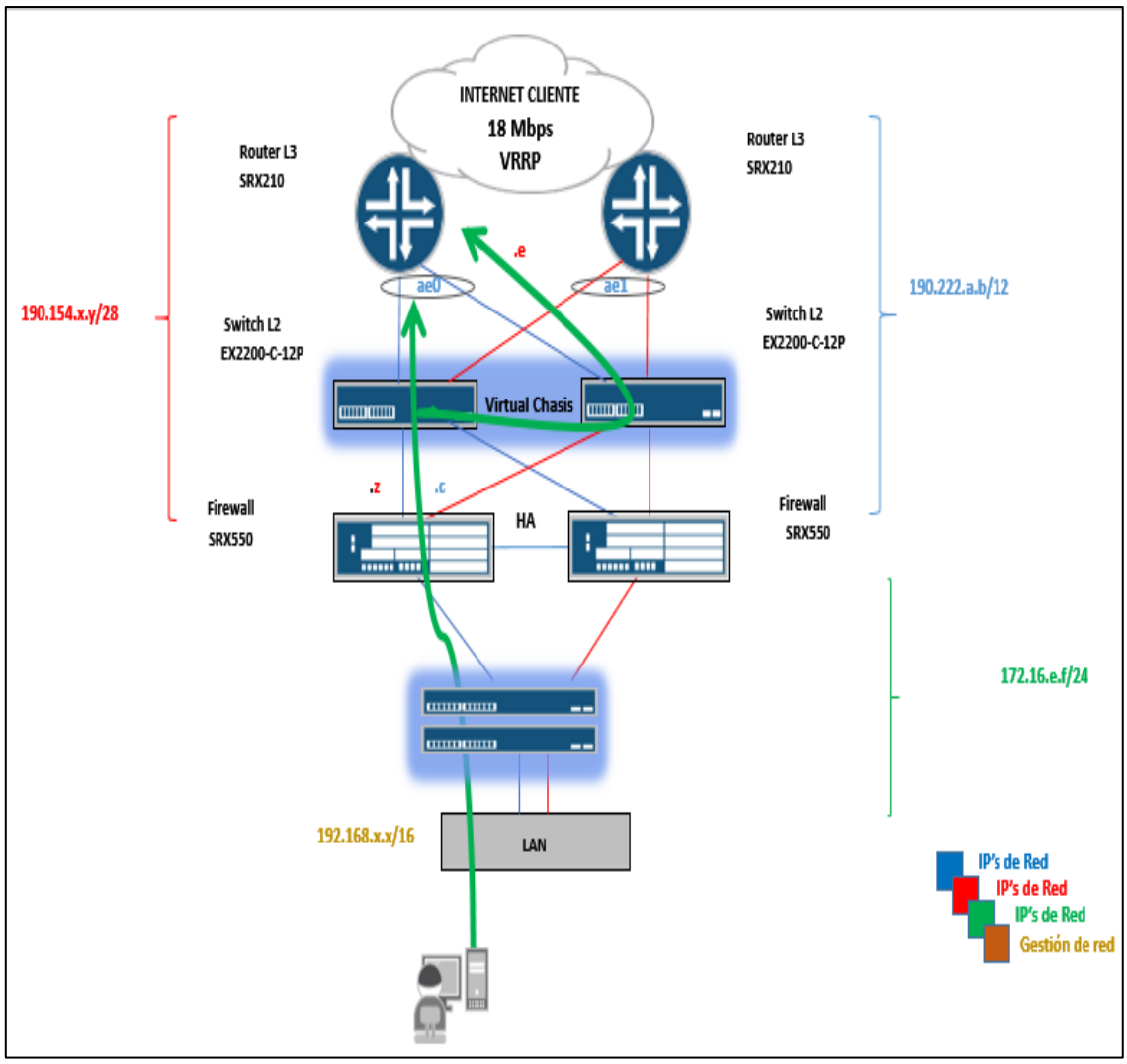


Figura.3.81 -Se muestra la funcionalidad de los equipos administrados ante fallas de conexión del router hacia la nube (internet), Fuente: Elaboración propia

Se observa en la gráfica, que ante la caída de un enlace (conexión srx550-router) con el equipo EX2200 switch se mantiene conectividad y el flujo de tráfico no se ve interrumpido ante esta eventualidad, por la redundancia de la solución brindada.

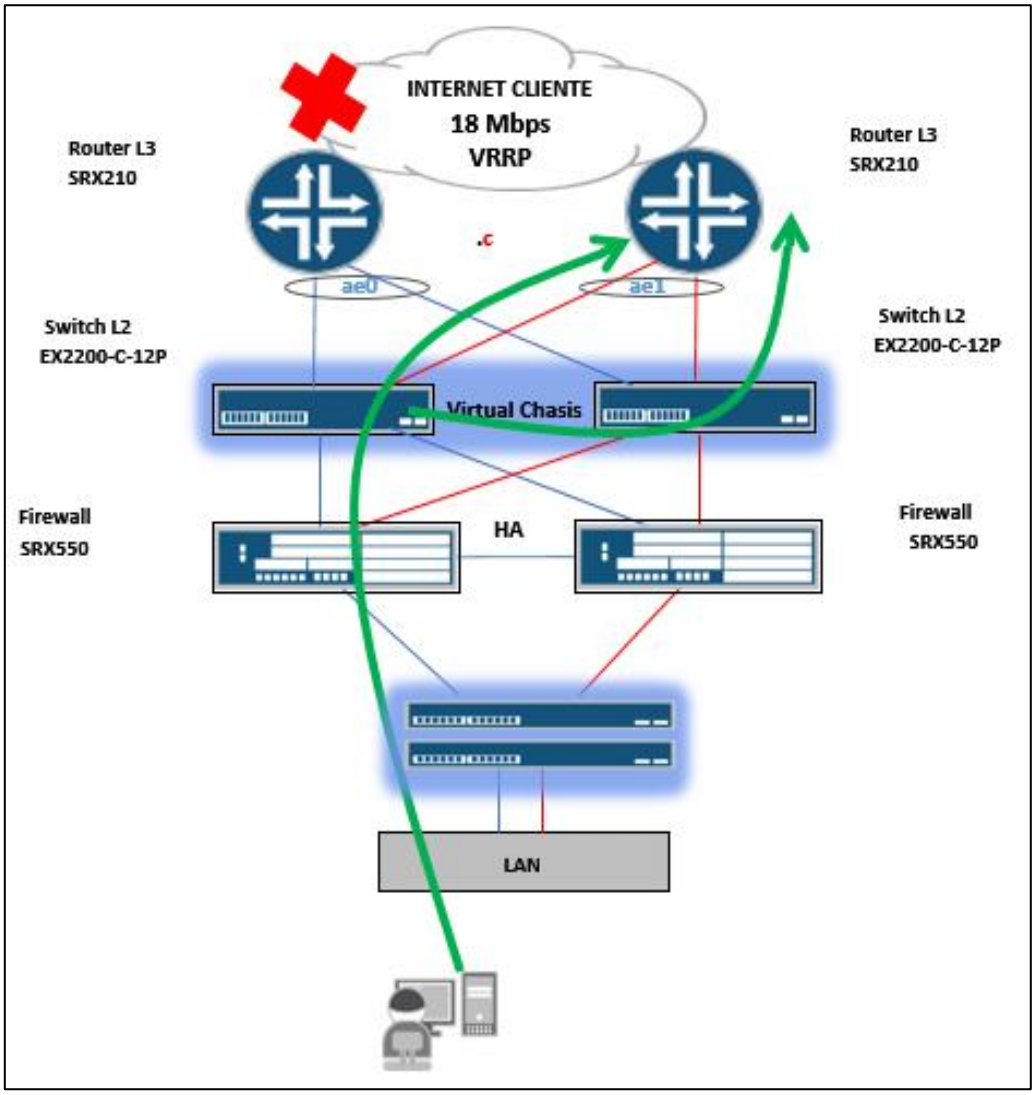


Figura.3.82 -Conexión caída de un enlace router – switch, contingencia de flujo de tráfico mediante Lacp (configurado en ambos equipos). Fuente: Elaboración propia

La falla eléctrica del equipo switch EX2200 en el esquema actual del cliente se observa la contingencia de los dos equipos configurados en virtual chassis, se aprecia que ante la caída del equipo configurado como Master, el equipo contiguo que forma parte del virtual chasis, brinda redundancia y el equipo Backup asume el nuevo papel de activo, sin presentar inconvenientes en la red, garantizando la navegación.

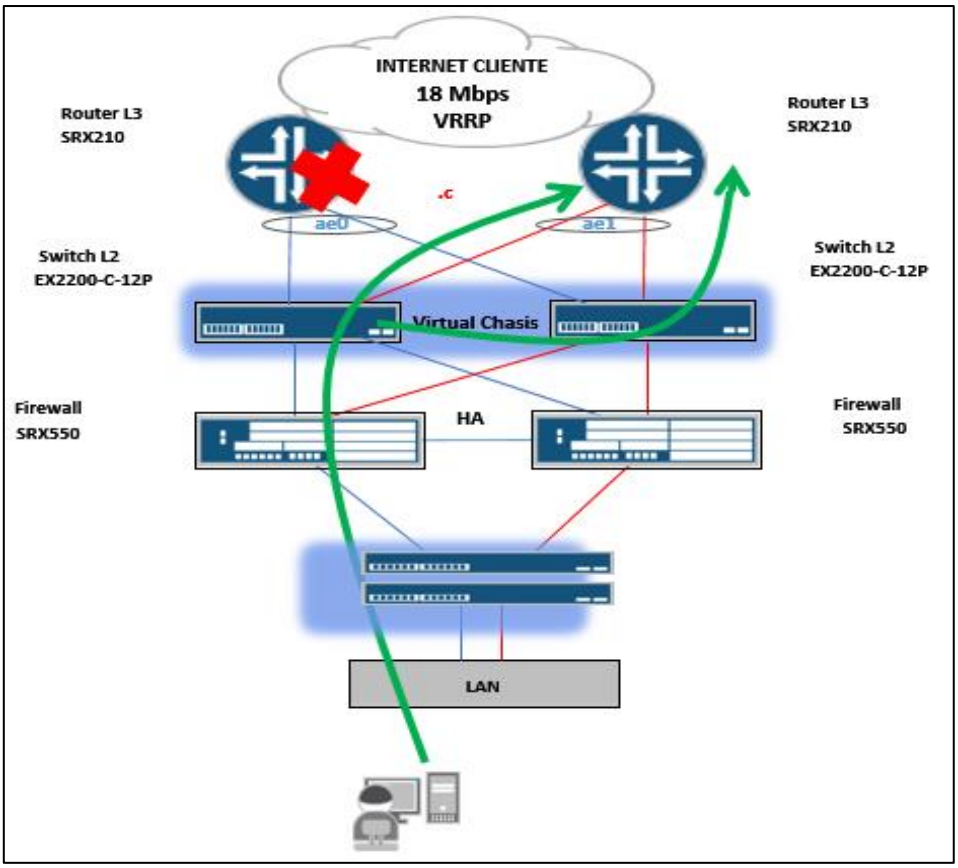


Figura.3.83 - Falla eléctrica del equipo Master (virtual chassis), se observa el tráfico se mantiene para garantizar la navegación en la sede de la empresa.
Fuente: Elaboración propia

En el siguiente diagrama se visualiza que ante la caída del equipo EX2200 configurado y/o que mantiene un estado de backup no se pierde conectividad sin interrupción de la navegación ante la caída física del equipo. Ya que el primer equipo configurado en virtual chassis asume el papel de master.

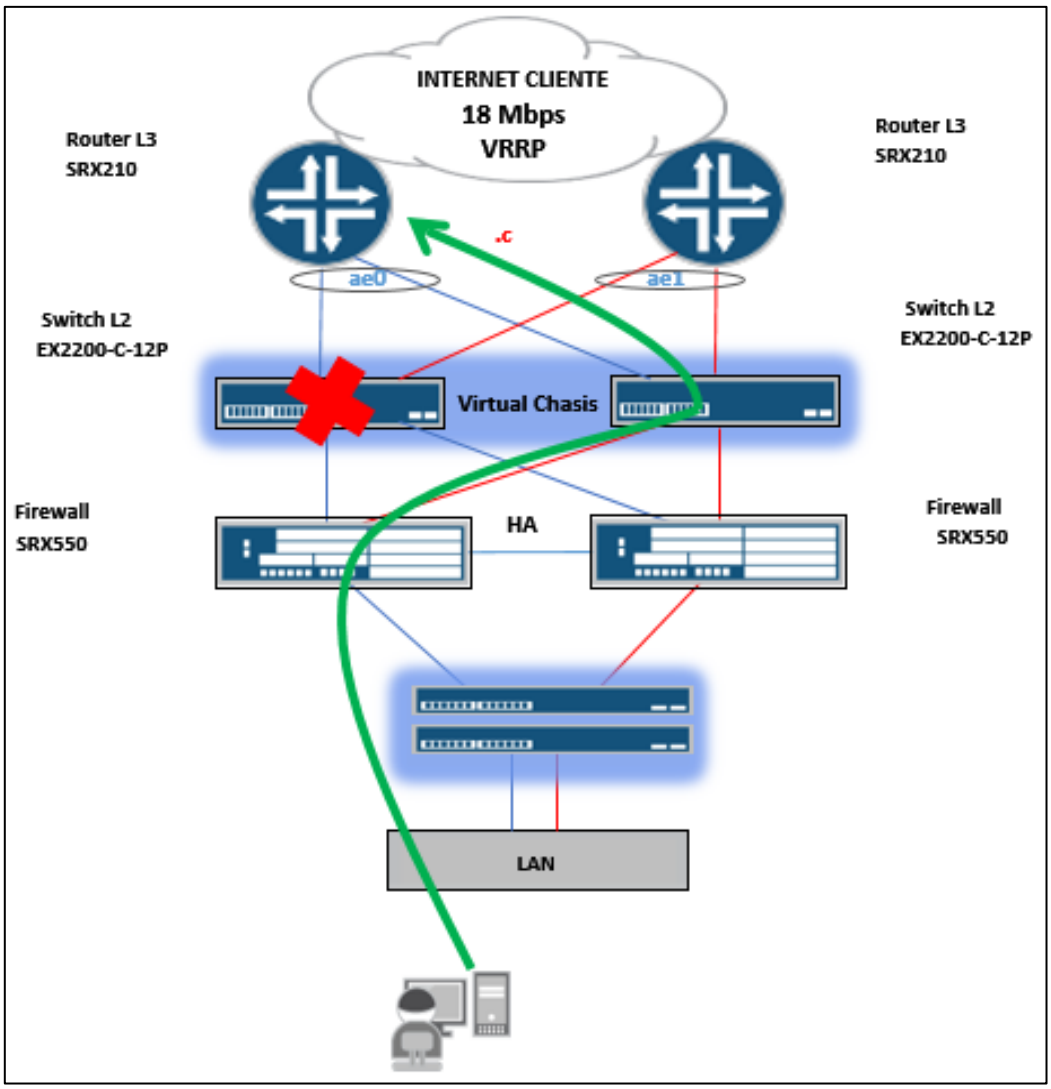


Figura.3.84-Caída física del equipo EX2200 quien asume el rol de backup.
Fuente: Elaboración propia

Los equipo SRX550 están configurados en clúster (nodo 0 y nodo 1), cual nos indica que los equipos se encuentran pasivo / activo, por tal motivo como se muestra en la gráfica. Cuando existe una falla el nodo 0 quien tenía el rol de activo, automáticamente detecta la caída de las sesiones en este nodo 0 y quien asume el nuevo rol de activo es el equipo configurado en nodo 1 o backup. Con lo cual se garantiza la navegación y la alta disponibilidad que brinda los equipos configurados en HA (High Availability).

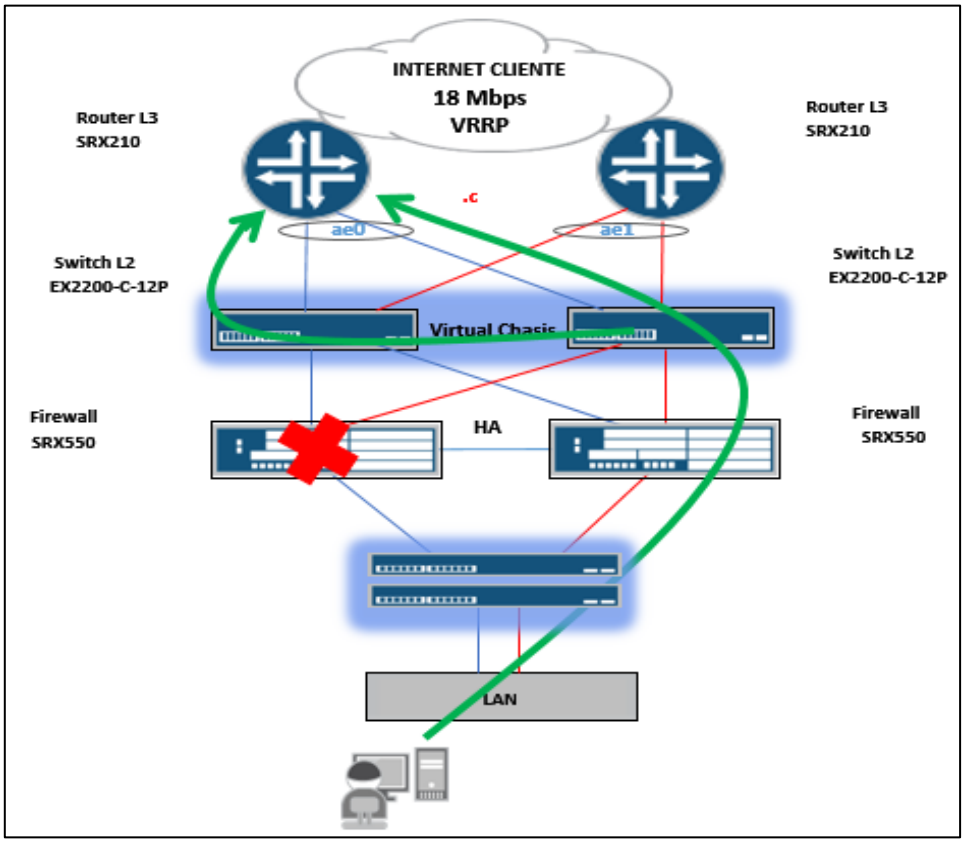


Figura.3.85- Se muestra la caída del equipo SRX550 –nodo 0 / activo y la alta disponibilidad de la solución brindada al cliente. Fuente: Elaboración propia

El equipo SRX550 configurado como nodo 1 / pasivo, ante cualquier falla como se observa en la gráfica, la solución brindad no presentaría problemas ya quien asume todo la navegación en el equipo activo /nodo 0 y así lograr la alta disponibilidad del enlace.

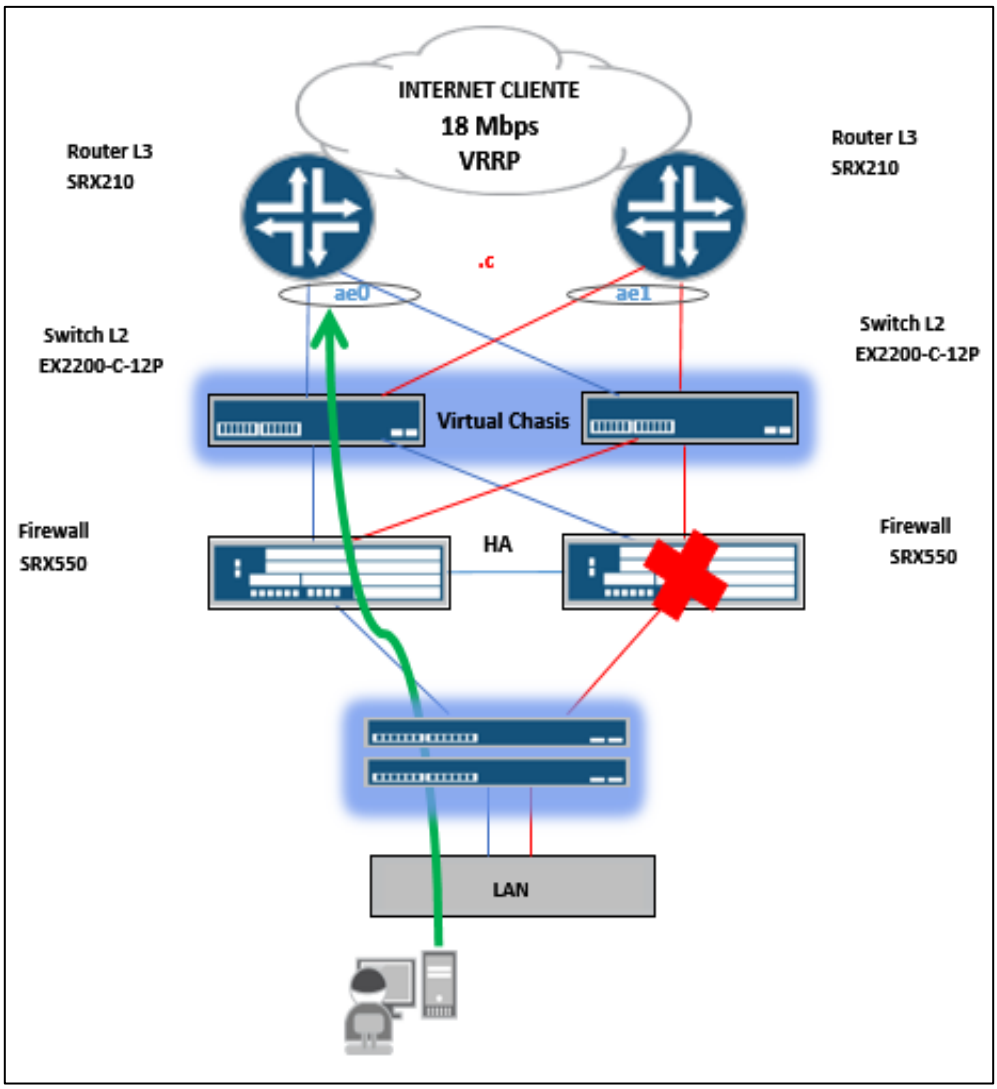


Figura.3.86- EL tráfico no se ve interrumpido ante la caída del equipo configurado como nodo 1 / pasivo. Fuente: Elaboración propia

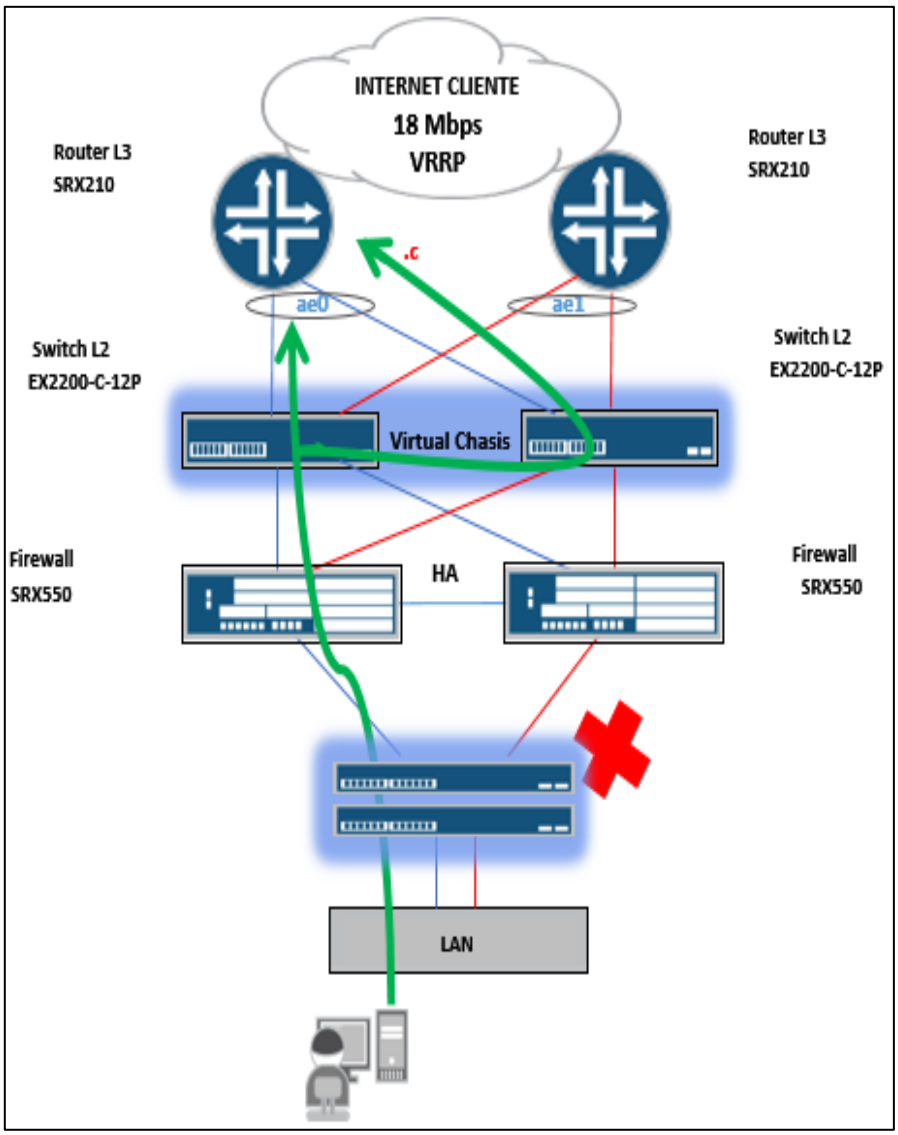


Figura.3.87- Caída física del equipo Switch –Core y la funcionalidad de Virtual Chassis ante la mencionado anteriormente, sin afectar la funcionalidad de la solución perimetral de la Empresa. Fuente: Elaboración propia

Además se tiene la funcionalidad de realizar ante cualquier evento de mantenimiento de los equipos y poder evitar que se dañen los sistemas operativos la función de programar los apagados de estos mediante una tarea programada, se muestra la configuración correspondiente.

CONCLUSIONES

1.- El siguiente trabajo tiene como conclusión poder garantizar la alta disponibilidad de enlaces desde la red externa hacia la red interna, mediante la utilización de equipos juniper, que soportan configuración de Lacp y la tecnología de virtual chassis que es la agregación de equipos, lo cual nos da una redundancia de enlaces ante la caída de un equipo por hardware y/o software, ya que toda la gama de los equipos juniper comparten el mismo sistema operativo junos.

2.- Mediante la aplicación de configuración de equipos en alta disponibilidad en la red externa, mediante enlaces redundantes y la aplicación de clúster activo / pasivo en los equipos de seguridad perimetral, garantizan una red estable ante fallos, una característica que evidencia una red estable.

3.- Un fácil manejo de los equipos administrados en todas las sedes mediante el uso de vlan de voz, datos y gestión de los equipos, para poder tener una red segmentada.

4.- La gestión de la política de seguridad empresarial se ha convertido en una tarea extremadamente compleja. El crecimiento en el tráfico de red, incluyendo el tráfico móvil y el procedente de los dispositivos personales, así como el desarrollo de los servicios de tecnología de cloud, se han combinado para dar lugar a una nueva gama de posibilidades para los hackers.

5.- La gestión de la seguridad es una tarea que puede resultar propensa a errores y requerir mucho tiempo si las soluciones de gestión son lentas o difíciles de utilizar, o bien la granularidad de control es restringida. Los errores de configuración resultantes pueden dar lugar a una vulnerabilidad de la empresa de cara a amenazas, así como a un incumplimiento de normativas y políticas.

RECOMENDACIONES

1.- La elaboración del siguiente trabajo tiene recomendación dar a conocer una tecnología que puede ser aplicado con la utilización de equipos juniper, para conseguir una performance, hacia la conexión a una red externa y/o interna, como recomendación para toda empresa, institución, sector publico y/o privado que tenga la necesidad de proteger su red ante tanta vulnerabilidad que existe hoy.

2.- Mediante una arquitectura de red con base sólida de diseño que garantiza una alta disponibilidad hacia los servicios, y sea alcanzable por los usuarios, dentro y fuera de la empresa, mantener una red estable mediante el uso de equipo de seguridad perimetral y equipos de acceso y distribución con características que hacen que la funcionalidad de la red no se vean afectados.

3.- Cuando se implementa o se diseña una red de datos se debe tener segmentadas las vlan de gestión, para que sean muy distintas a las vlan de datos y voz, para tener una gestión centralizada de los equipos de red en las capas de acceso y distribución.

4.-Tener una gestión centralizada de los equipos en toda la red, la unificación de capas de acceso, distribución y núcleo lo cual para los administradores de red tienen una mejor visibilidad de una arquitectura estable.

5.- Se presenta la implementación de políticas de seguridad y la configuración de zonas para tener un red distribuida en políticas y la aplicación de medidas de

seguridad mediante la protección ante ataques externos y realizar una red estable mediante el uso de equipo configurados en clúster, que brinda disponibilidad de enlace y que el usuario final no presente problemas en la navegación, por ende la aplicaciones de filtros y/o políticas de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

1. Ordóñez Galiano, Felipe Andrés (2012). Solución de Firewall con alta disponibilidad para redes corporativas utilizando Vyatta con virtualización. Carrera de Ingeniería en Electrónica, Redes y Comunicación de Datos. ESPE. Sede Sangolquí.
2. Helm Bank (2012) Clúster de balanceo de carga y alta disponibilidad para servicios web y mail.
3. Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS of Juniper Networks (2010), JNCIA-Junos Study Guide—Part 1.Inc. in the United States
4. Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS of Juniper Networks (2010), JNCIA-Junos Study Guide—Part 2.Inc. in the United States
5. Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS of Juniper Networks (2010), JNCIS-SEC Study Guide—Part 1. in the United States
6. Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS of Juniper Networks (2010), JNCIS-SEC Study Guide—Part 2. in the United States
7. Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS of Juniper Networks (2010), JNCIS-ENT Study Guide—Part 1. in the United States

8. Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS of Juniper Networks (2010), JNCIS-ENT Study Guide—Part 2. in the United States

9. SRX Configure Chassis Cluster (High Availability) on a SRX550 device. http://kb.juniper.net/InfoCenter/index?page=content&id=KB25889
10. EX Configure Virtual Chassis on EX4200 and EX2200 http://www.juniper.net/documentation/en_US/junos13.2/topics/task/configuration/virtual-chassis-ex4200-cli.html.
11. Cisco CCNA Exploration 4.0 Aspectos Básico de Interworking(2011)
12. Cisco CCNA Exploration 4.0 Aspectos Básico de Interworking- Introducción al diseño de la red LAN.(2011)
13. Configuration vlan layer 2 and layer 3 in the swicth juniper family EX http://www.juniper.net/documentation/en_US/junos14.2/topics/concept/layer-2-services-bridging-overview-l2.html

ANEXO

ANEXO A. Equipos Juniper de la gama de seguridad:

Product Comparison

	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650
Maximum Performance and Capacity							
Junos OS version tested	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15	Junos OS 11.4R5	Junos OS 12.1	Junos OS 11.4R5
Firewall performance (large packets)	700 Mbps	700 Mbps	850 Mbps	950 Mbps	1.8 Gbps	5.5 Gbps	7 Gbps
Firewall performance (IMIX)	200 Mbps	200 Mbps	250 Mbps	300 Mbps	600 Mbps	1.7 Gbps	2.5 Gbps
Firewall + routing PPS (64 Byte)	70 Kpps	70 Kpps	95 Kpps	125 Kpps	200 Kpps	700 Kpps	850 Kpps
Firewall performance[3] (HTTP)	100 Mbps	100 Mbps	290 Mbps	350 Mbps	830 Mbps	1.5 Gbps	2 Gbps
IPsec VPN throughput (large packets)	65 Mbps	65 Mbps	85 Mbps	100 Mbps	300 Mbps	1.0 Gbps	1.5 Gbps
IPsec VPN tunnels	128	128	256	512	1,000	2,000	3,000
AppSecure firewall throughput[3]	90 Mbps	90 Mbps	250 Mbps	300 Mbps	750 Mbps	1.5 Gbps	1.9 Gbps
IPS (intrusion prevention system)	75 Mbps[4]	75 Mbps	65 Mbps	80 Mbps	230 Mbps	800 Mbps	1 Gbps
Antivirus	25 Mbps (Sophos AV)	25 Mbps (Sophos AV)	30 Mbps (Sophos AV)	35 Mbps (Sophos AV)	85 Mbps (Sophos AV)	300 Mbps (Sophos AV)	350 Mbps (Sophos AV)
Connections per second	1,800	1,800	2,200	2,800	8,500	27,000	35,000
Maximum concurrent sessions	32 K[1]	32 K[1]	64 K[1]	96 K[1]	256 K[1]	375 K	512 K
DRAM options	2 GB DRAM	2 GB DRAM	2 GB DRAM	2 GB DRAM	2 GB DRAM	2 GB DRAM	2 GB DRAM
Maximum security policies	384	384	512	2,048	4,096	7,256	8,192
Maximum users supported	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Network Connectivity							
Fixed I/O	8 x 10/100	8 x 10/100 VDSL/ ADSL2+ WAN (Annex A or B)	2 x 10/100/1000 BASE-T + 6 x 10/100	8 x 10/100/1000 BASE-T	16 x 10/100/1000 BASE-T	6 x 10/100/1000 BASE-T + 4 SFP	4 x 10/100/1000 BASE-T
I/O slots	N/A	N/A	1 x SRX Series Mini-PIM	2 x SRX Series Mini-PIM	4 x SRX Series Mini-PIM	2 x SRX Series Mini-PIM, 6 x GPIM or multiple GPIM and XPIM combinations	8 x GPIM or multiple GPIM and XPIM combinations
Services and Routing Engine slots	No	No	No	No	No	No	2[2]
WAN/LAN interface options	N/A	N/A	See ordering information	See ordering information	See ordering information	See ordering information	See ordering information
Maximum number of PoE ports (PoE optional on some SRX Series models)	N/A	N/A	Up to 4 ports of 802.3af with maximum 50 W	Up to 8 ports of 802.3af/ at with maximum 120 W	Up to 16 ports of 802.3af/ at with maximum 150 W	Up to 40 ports of 802.3af/ at with maximum 247 W	Up to 48 ports of 802.3af/ at with maximum 247 W
USB	1	2	2	2	2	2	2 per SRE

IPsec VPN							
Concurrent VPN tunnels	128	128	256	512	1,000	2,000	3,000
Tunnel interfaces	10	10	64	64	128	456	512
DES (56-bit), 3DES (168-bit) and AES (256-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MD-5, SHA-1 and SHA-2 authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Manual key, Internet Key Exchange (IKE v1+v2), public key infrastructure (PKI) (X.509)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy (DH Groups)	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5	1, 2, 5
Prevent replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic remote access VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPsec NAT traversal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Redundant VPN gateways	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of remote access users	25 users	25 users	50 users	150 users	250 users	500 users	500 users

Flash and Memory							
Memory (DRAM)	2 GB (SRX100H2)	2 GB (SRX110H2)	2 GB (SRX210HE2)	2 GB (SRX220H2)	2 GB (SRX240H2)	2 GB (SRX550)	2 GB (SRX650)
Memory slots	Fixed memory	Fixed memory	Fixed memory	Fixed memory	Fixed memory	2 DIMM	4 DIMM
Flash memory	2 GB	2 GB CF, externally accessible	2 GB	2 GB CF, externally accessible	2 GB	2 GB CF internal	2 GB CF internal on SRE, external slot empty, up to 2 GB CF supported
USB port for external storage	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dimensions and Power							
Dimensions (W x H x D)	8.5 x 1.4 x 5.8 in (21.6 x 3.6 x 14.7 cm)	11.02 x 1.72 x 8.385 in (28 x 4.37 x 21.3 cm)	11.02 x 1.73 x 7.12 in (28.0 x 4.4 x 18.1 cm)	14.31 x 1.73 x 7.11 in (36.3 x 4.4 x 18.1 cm)	17.5 x 1.75 x 15.1 in (44.4 x 4.4 x 38.5 cm)	17.5 x 3.5 x 18.2 in (44.4 x 8.8 x 46.2 cm)	17.5 x 3.5 x 18.2 in (44.4 x 8.8 x 46.2 cm)
Weight (device and power supply)	2.5 lb (1.1 kg)	6.7 lb (3.06 kg)	3.3 lb (1.5 kg) non-PoE / 4.4 lb (2 kg) PoE No interface modules	3.43 lb (1.56 kg) non-PoE No interface modules	For LM and HM-AC: 11.2 lb (5.1 kg) For HM - DC: 12.56 lb (5.7 kg) / 12.3 lb (5.6 kg) PoE No interface modules	21.96 lb (9.96 kg) No interface modules 1 power supply	24.9 lb (11.3 kg) No interface modules 1 power supply
Rack-mountable	Yes, 1 RU	Yes, 1 RU	Yes, 1 RU	Yes, 1 RU	Yes, 1 RU	Yes, 2 RU	Yes, 2 RU
Power supply (AC)	100-240 VAC, 30 W	100-240 VAC, 60 W	100–240 VAC, 60 W non-PoE/ 150 W PoE	100–240 VAC, 60 W non-PoE / 200 W PoE	150 W for LM and HM 190 W for HM with DC 360 W for PoE	100–240 VAC, single 645 W or dual 645 W	100–240 VAC, single 645 W or dual 645 W
Maximum PoE power	N/A	N/A	50 W	120 W	150 W	247 W redundant, or 494 W non-redundant	247 W redundant, or 494 W non-redundant

ANEXO B. Equipos Juniper de la gama de capa de acceso y distribución:

Product Options

Eight EX4200 switch models are available (see Table 1 below).

Table 1: EX4200 Line of Ethernet Switches

Model	Access Port Configuration	PoE Ports*	Height	POE Budget	Power Supply Rating
EX4200-24T**	24-port 10/100/1000BASE-T	8 PoE	1 RU	130 W	320 W AC
EX4200-24PX	24-port 10/100/1000BASE-T	24 PoE+	1 RU	740 W	930 W AC
EX4200-48T**	48-port 10/100/1000BASE-T	8 PoE	1 RU	130 W	320 W AC
EX4200-48PX	48-port 10/100/1000BASE-T	48 PoE+	1 RU	740 W	930 W AC
EX4200-24F**	24-port 100/1000BASE-X (SFP)	N/A	1 RU	N/A	320 W AC
EX4200-24T-DC**	24-port 10/100/1000BASE-T	0	1 RU	N/A	190 W DC
EX4200-48T-DC**	48-port 10/100/1000BASE-T	0	1 RU	N/A	190 W DC
EX4200-24F-DC**	24-port 100/1000BASE-X (SFP)	N/A	1 RU	N/A	190 W DC

* All PoE ports 802.3af-compliant @ 15.4W. All PoE+ ports on EX4200-24PX/48PX models 802.3at compliant @ 30 W subject to maximum PoE budget.

** NEBS certified

- 10GbE XFP optic/connector type: 10GE XFP LC connector, SR (multimode), LR (single-mode), ER (single-mode) or ZR (single-mode)
- 10GbE SFP+ optic/connector type: 10GE SFP+ LC connector, SR (multimode), USR (multimode), LR (single-mode), ER (single-mode), LRM (multimode) and DAC (direct-attach copper)

Physical Layer

- Time Domain Reflectometry (TDR) for detecting cable breaks and shorts: 24P/24T and 48P/48T only
- Auto MDI/MDIX support: 24P/24T and 48P/48T only (all ports)
- Port speed downshift/setting max advertised speed on 10/100/1000BASE-T ports: 24P/24T and 48P/48T only, on all ports
- Digital optical monitoring for optical ports

Packet Switching Capacities (Maximum with 64 Byte Packets)

- 24P/24T: 88 Gbps
- 48P/48T: 136 Gbps
- 24F: 88 Gbps

Aggregate Switch Capacities (Maximum with 64 Byte Packets)

- 24P/24T/24F: 216 Gbps
- 48P/48T: 264 Gbps

- IEEE 802.1X: Port Access Control
- IEEE 802.1ak: Multiple Registration Protocol
- IEEE 802.3: 10BASE-T
- IEEE 802.3u: 100BASE-T
- IEEE 802.3ab: 1000BASE-T
- IEEE 802.3z: 1000BASE-X
- IEEE 802.3ae: 10 Gigabit Ethernet
- IEEE 802.3af: Power over Ethernet
- IEEE 802.3x: Pause Frames/Flow Control
- IEEE 802.3ad: Link Aggregation Control Protocol
- IEEE 802.3ah: Ethernet in the First Mile
- Metro
  - PVLAN support
  - IEEE 802.1ag connectivity fault management
  - ITU-T G803.2
  - ITU-T Y.1731
  - IEEE 802.1ad Q-in-Q
  - Multicast VLAN routing

Layer 3 Features: IPv4

- Max number of ARP entries: 16,000
- Max number of IPv4 unicast routes in hardware: 16,000
- Max number of IPv4 multicast routes in hardware: 8,000
- Routing protocols: RIPv1/v2, OSPF, BGP, IS-IS
- Static routing
- Routing policy

EX4200 Specifications

Physical Specifications

- Backplane: 128 Gbps Virtual Chassis interconnect to combine up to 10 units as a single logical device
- Uplink module options:
  - 4-port GbE module with pluggable SFP optics
  - 2-port 10GbE module with pluggable XFP optics
  - Dual-mode 2-port 10GbE SFP+ / 4-port GbE SFP module with pluggable SFP+/SFP optics
  - Dual-mode 2-port 10GbE SFP+ / 4-port GbE SFP module with pluggable SFP+/SFP optics and MACsec support

Power Options

- Power supplies: Autosensing; 100-120 V / 200-240 V; AC 320 W, 600 W and 930 W dual load-sharing hot-swappable internal redundant power supplies
- Maximum current inrush: 50 amps
- DC power supply: 190 W DC, input voltage range 36 V - 72 V, dual input feed, dual load-sharing hot-swappable internal redundant power supplies
- Minimum number of PSUs required for fully loaded chassis: 1 per switch

Dimensions (W x H x D)

- 17.41 x 1.72 x 16.43 in (44.21 x 4.32 x 41.73 cm)
- [1]Desktop installation width noted above, rack-mount width is 17.5 in (44.5 cm)
- [2]Height: 1 RU
- [3]Depth with 320 W AC PSU and 190 W DC PSU noted above, 18.8 in (47.8 cm) with 600/930 W AC PSU

System Weight

- EX4200-24T with 320 W AC PSU: 16.5 lb (7.5 kg)
- EX4200-24P with 600 W AC PSU: 17.2 lb (7.8 kg)
- EX4200-24PX with 930 W AC PSU: 18 lb (8.16 kg)
- EX4200-48T with 320 W AC PSU: 17.1 lb (7.8 kg)
- EX4200-48P with 930 W AC PSU: 18.2 lb (8.3 kg)
- EX4200-48PX with 930 W AC PSU: 19 lb (8.61 kg)
- EX4200-24F with 320 W AC PSU: 16.1 lb (7.3 kg)
- EX4200-24T-DC with 190 W DC PSU: 16.5 lb (7.5 kg)
- EX4200-48T-DC with 190 W DC PSU: 17.1 lb (7.8 kg)
- EX4200-24F-DC with 190 W DC PSU: 16.1 lb (7.3 kg)

Environmental Ranges

- Operating temperature: 32º to 113º F (0º to 45º C)
- Storage temperature: -40º to 158º F (-40º to 70º C)
- Operating altitude: up to 10,000 ft (3,049 m)
- Non-operating altitude: up to 16,000 ft (4,877 m)
- Relative humidity operating: 10% to 85% (noncondensing)
- Relative humidity non-operating: 0% to 95% (noncondensing)

Cooling

- Field-replaceable fan tray with multiple blowers (3)
- Switch remains operational even if one blower fails
- Airflow: 20.3 cfm

Hardware Specifications

- Switching Engine Model: Store and forward
- DRAM – 1 GB with ECC
- Flash – 1 GB
- CPU – 1 GHz PowerPC CPU
- GbE port density per system:
  - 24P/24T/24F: 28 (24 host ports + four-port GbE uplink module)
  - 48P/48T: 52 (48 host ports + four-port GbE uplink module)
- 10GbE port density per system (all models): 2 (uplink module)

Optics

- 100 Mbps optic/connector type: LC SFP fiber supporting 100BASE-FX SFP (multimode), LX (single-mode) and BX (single-strand)
- 10/100/1000BASE-T connector type: RJ-45
- GbE SFP optic/connector type: RJ-45 or LC SFP fiber supporting 1000BASE-T SFP, SX (multimode), LX (single-mode), LH/ZX (single-mode) and BX (single strand)