UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

MODELO DE SERVICIO DE SEGURIDAD PERIMETRAL EN LA NUBE DEL OPERADOR DE INTERNET PARA CLIENTES CORPORATIVOS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

WILLIAM LUIS UCHARIMA

PROMOCIÓN
2009-II

LIMA-PERÚ
2013

MODELO DE SERVICIO DE SEGURIDAD PERIMETRAL EN LA NUBE DEL OPERADOR DE INTERNET PARA CLIENTES CORPORATIVOS

Dedicatoria

Dedicado a mis amados padres Auria y Roberto por su confianza y amor.

A mi hermano Rigoberto por su apoyo constante.

A dios por darme la felicidad de tener a mis seres queridos a mi lado.

SUMARIO

El objetivo de este informe es el de realizar un diseño para implementar un servicio de seguridad perimetral desde la red del operador de Internet, es decir en la red WAN.
Este servicio de seguridad perimetral tendrá como objetivo brindar seguridad a la red LAN de los clientes corporativos del operador de Internet para ofrecer un servicio con el cual el cliente no tendrá la necesidad de contar con infraestructura, equipos y personal calificado para la operación y mantenimiento de una solución de seguridad óptima y eficiente.
Uno de los objetivos del presente trabajo es aportar información sobre cómo realizar el diseño de un servicio de seguridad en la nube desde el equipamiento a considerar hasta cuales serían sus funcionalidades. Además se brindara información acerca de las tendencias actuales de los servicios de telecomunicaciones los cuales son llevados a la nube.
Finalmente se expondrá las conclusiones a las cuales se llegara después del presente trabajo. También se realizaran una serie de recomendaciones acerca de los servicios en la nube.

ÍNDICE

INTRODUCCION

En la actualidad la sociedad se encuentra en un momento decisivo respecto del uso de la tecnología para extender y potenciar las comunicaciones mediante el uso de las tecnologías de información y comunicación. La globalización de Internet se ha producido más rápido de lo que cualquiera hubiera imaginado. El modo en que se producen las interacciones sociales, comerciales, políticas y personales cambia en forma continua para estar al día con la evolución de esta red global. En la próxima etapa de nuestro desarrollo, los innovadores usarán Internet como punto de inicio para sus esfuerzos, creando nuevos productos y servicios diseñados específicamente para aprovechar las capacidades de la red. Mientras los desarrolladores empujan los límites de lo posible, las capacidades de las redes interconectadas que forman Internet tendrán una función cada vez más importante en el éxito de esos proyectos.

Así como el Internet es una herramienta que se ha convertido en el medio idóneo para enseñanza permitiendo a los organismos gubernamentales brindar programas de educación a los pueblos más alejados y de menores recursos económicos. Las empresas pueden realizar una publicidad más enfocada a un determinado público consumidor. Los bancos ofrecen servicios de pagos desde un portal web. Las personas lo usan como medio de comunicación o entretenimiento.

Ante este uso masivo del Internet también se crea oportunidades para los delincuentes informáticos conocidos como HACKERS quienes utilizan los medios informáticos y el conocimiento sobre su funcionamiento como herramientas para delinquir y obtener algún beneficio económico.

Los Hackers vulneran la seguridad de servidores web, correos, base de datos, etc. Una vez habiendo vulnerado la seguridad del servidor pueden provocar la caída del servicio, cambios en la página web, robo de información confidencial, etc.

Adicionalmente al peligro de los Hackers, que es una amenaza externa a la empresa debemos mencionar los ataques que provienen desde el interior de la empresa y las causas que originan estos ataques. Los códigos maliciosos o malware, constituyen también una de las principales amenazas para cualquier Institución u Organizaciones y aunque parezca un tema trivial suele ser motivo de importantes pérdidas económicas.

Actualmente, casi el 80% de los ataques informáticos llevados a cabo por códigos maliciosos, se realizan a través de programas troyanos. Este tipo de malware ingresa a un sistema de manera completamente subrepticia activando una carga dañina que despliega las instrucciones maliciosas que eliminan archivos, monitorean tráfico de la red, destruyen particiones de disco, etc.

Los Hackers suelen usar troyanos para realizar sus ataques pero estos troyanos poseen un requisito particular que debe ser cumplido para que logren el éxito: necesitan la intervención del factor humano, en otras palabras, tiene que ser ejecutados por el usuario. Es por ello que estas amenazas se diseminan por medio de diferentes tecnologías como dispositivos USB, mensajería instantánea, redes P2P, e-mail, etcétera; a través de alguna metodología de engaño, aparentando ser programas inofensivos.

Estos programas maliciosos es una de las principales amenazas desde el interior de la empresa y son los usuarios los que provocan su ejecución.

Después de describir las amenazas externas e internas debemos mencionar las contramedidas para evitar estos ataques. Para controlar las amenazas externas se usa el firewall que es un dispositivo que funciona como cortafuegos permitiendo o denegando las transmisiones. Un uso típico es situarlo entre la red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Como contramedida para las amenazas internas radican principalmente en la implementación de programas antivirus que operen bajo mecanismos de detección avanzados que permitan monitorear, controlar y administrar de manera centralizada cada uno de los nodos involucrados en la red, junto a planes y programas de educación orientados a crear conciencia en el personal sobre los riesgos de seguridad que representan los códigos maliciosos.

CAPITULO I
PLANTEMIENTO DEL PROBLEMA

Este capítulo se desarrolla con la finalidad de presentar de una manera clara y concisa el escenario bajo el cual nace la motivación de este informe y a qué necesidad responde.
Se definen también cuáles son los alcances y aportes del mismo. Finalmente se dedica un punto a la síntesis de este informe.

1.1 Descripción del problema

En la última década Internet se ha convertido en una herramienta necesaria e indispensable para las empresas. Esta herramienta hace posible que las empresas puedan realizar diferentes actividades como compartir información o realizar campañas de publicidad desde un sitio web.
El uso de Internet lleva a que las empresas abran una puerta a un mundo virtual en cual existen muchos peligros como el hurto de información o la baja productividad de sus empleados al ingresar a sitios web de entretenimiento, esto impacta en la rentabilidad de la empresa, por tal motivo el personal de TI busca soluciones de seguridad para tomar medidas correctivas a estos peligros.
En la búsqueda de estas soluciones de seguridad se necesita una fuerte inversión de dinero en cuanto a personal técnico calificado como de infraestructura. Esto lleva muchas veces a que las empresas tengan de enfocarse en una tarea en la cual no son expertos y terminan realizando labores que no son propias de su negocio.

1.2 Objetivos Generales

El objetivo de este trabajo es realizar el diseño de red para brindar una solución para implementar un servicio de seguridad perimetral desde la red del operador de Internet.

1.3 Objetivos Específicos

El presente trabajo tiene como objetivo específico brindar una solución para las empresas que desean contar con un servicio de seguridad perimetral para la red LAN que cumpla con ser eficiente, escalable y económica. Se plantea brindar a los clientes corporativos de un proveedor de Internet una solución con la cual no tendrán la necesidad de contar con la infraestructura, equipos y personal especializado para poder operar y mantener de manera eficiente un servicio de seguridad. Esto ayudara a la empresa a minimizar gastos en compra de equipos y pagos a personal especializado.

1.4 Evaluación del problema

En la actualidad muchas empresas sufren de ataques por hackers, estos vulneran la seguridad de las empresas y roban información o causan daño a sus sistemas.

Actualmente incluso portales web de entidades de gobierno sufren ataques de los hackers. Este problema lleva a la empresa a contar con personal calificado capaces de evitar y corregir los daños causados por los hackers. Además del personal calificado, se debe contar con el equipamiento y la infraestructura necesaria para implementar una solución de seguridad de alto nivel.

Por otra parte hoy en día existe una necesidad de llevar todos los servicios a la nube o Internet. Muchas empresas ofrecen servicios alojados en data centers y que cumplen con prestar servicios de equipamiento, infraestructura y personal calificado para brindar distintos servicios.

Ante este modelo de servicio se plantea realizar una solución de seguridad para una red LAN montada en la nube del operador de Internet.

1.5 Alcance del trabajo

Este trabajo constituye una guía para aquellas personas que se encuentren investigando nuevas opciones para realizar una solución de seguridad en una red de área local (LAN).

El aporte de este informe será brindar una visión general de cómo se realizar una solución de seguridad considerando el equipo físicamente instalado en la sede del cliente. Posteriormente se realizara un análisis detallado de una solución de seguridad instalando los equipos en la nube del operador de Internet. Analizaremos las ventajas que se obtiene con respecto a una solución con equipos en la sede del cliente.

Se brindara las características que debe cumplir todo el equipamiento considerado en este diseño de seguridad perimetral.

Finalmente se detallara un procedimiento de pruebas para la validación del correcto funcionamiento de la solución de seguridad perimetral en la nube.

1.6 Síntesis del trabajo

Se exponen los fundamentos teóricos que permitan comprender los protocolos involucrados en la comunicación de una red privada con la red de Internet.

Se presenta un análisis de las características de hardware y software del equipo de seguridad. Se exponen lineamientos y recomendaciones a tener en cuenta en el proceso de diseño, implementación y operación de la seguridad en la nube.

Finalmente, se indicaran las ventajas, conclusiones y recomendaciones que se obtienen en una solución de seguridad en la nube frente a una solución de seguridad con equipos instalados en la sede de cliente.

CAPITULO II
MARCO TEORICO CONCEPTUAL

2.1 Bases teóricas

En el presente capitulo se brindaran fundamentos teóricos básicos para entender la solución de seguridad en la nube.

2.1.1 Descripción de una Red

Entender los beneficios de una red de computadoras y como ellas funcionan es importante para mejorar las formas de comunicación entre los usuarios. Una red es un grupo de dispositivos conectados, como computadoras, servidores, tabletas, teléfonos móviles, etc. Estos dispositivos pueden comunicarse uno con otros. Las redes transportan información entre distintos ambientes como hogares, pequeñas empresas, grandes empresas, etc. En el caso de grandes empresas con un gran número de ubicaciones posiblemente necesiten ser conectadas unas con otras, y puede describirse estas ubicaciones en términos de donde se encuentran localizados los usuarios.

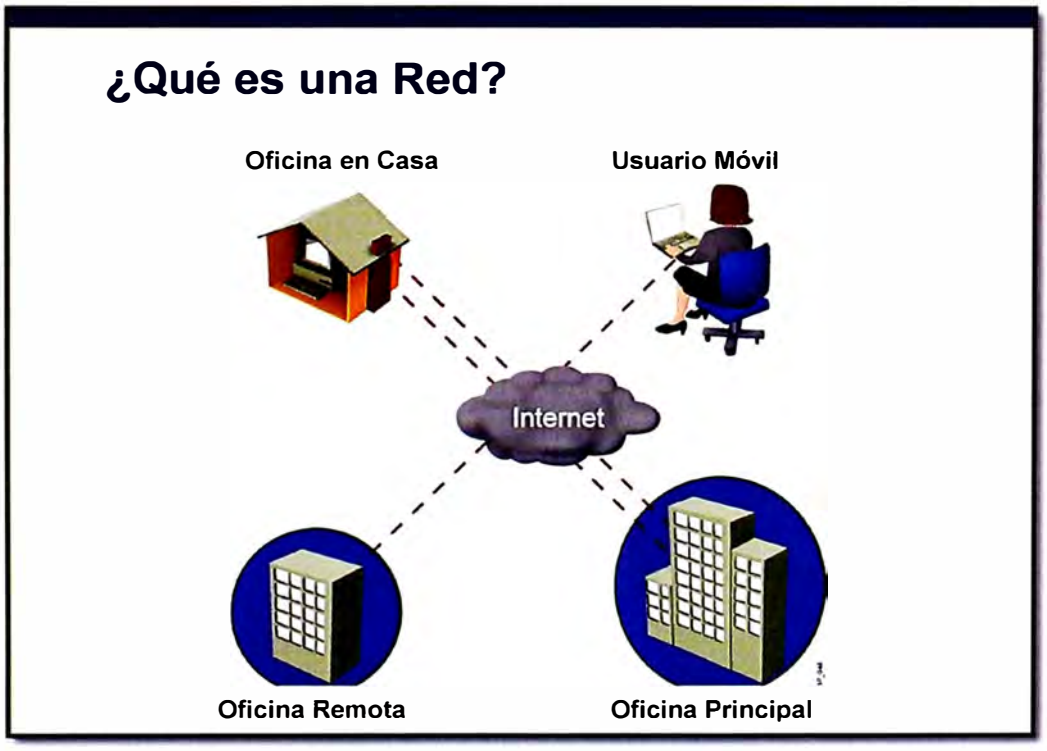


Figura 2.1 Escenario Común de Conexión de Red

a.- Oficina Principal: Una oficina principal es un sitio donde todos los usuarios están conectados por una red y donde gran parte de la información de la empresa se encuentra

localizada. Una oficina principal puede tener cientos de usuarios quienes dependen de una red para acceder a sus labores diarias. Una oficina principal podría usar muchas redes las cuales pueden conectar varios pisos en un edificio de oficinas o extenderse sobre un campus con varios edificios de oficinas.

b.- Ubicaciones Remotas: Una gran variedad de ubicaciones remotas usan alguna red para conectarse con la oficina principal.

Oficina Remota: En una oficina remota, un grupo pequeños de personas trabaja y se comunica con otras oficinas usando una red. Aunque alguna información de la corporación puede almacenarse en la oficina remota es más recomendable que esta información se almacene en la oficina principal. Equipos como impresoras si pueden estar ubicadas en la oficina remota.

Hogar de Trabajo: Algunas personas trabajan en casa, esta ubicación se conoce también como Home Office. Estos usuarios requieren de una conexión para tener acceso a archivos almacenados en la oficina principal o remota.

Usuarios Móviles: Los usuarios móviles se conectan a la oficina principal o remota desde un dispositivo también móvil cuando se encuentran en un viaje o lugar fuera de la corporación.

2.1.2 Componentes físicos comunes de una red

Se describen los componentes físicos comunes de una red, incluyendo enrutadores, conmutadores, interconexiones y computadoras. En la figura 2.2 se pueden observar estos componentes.

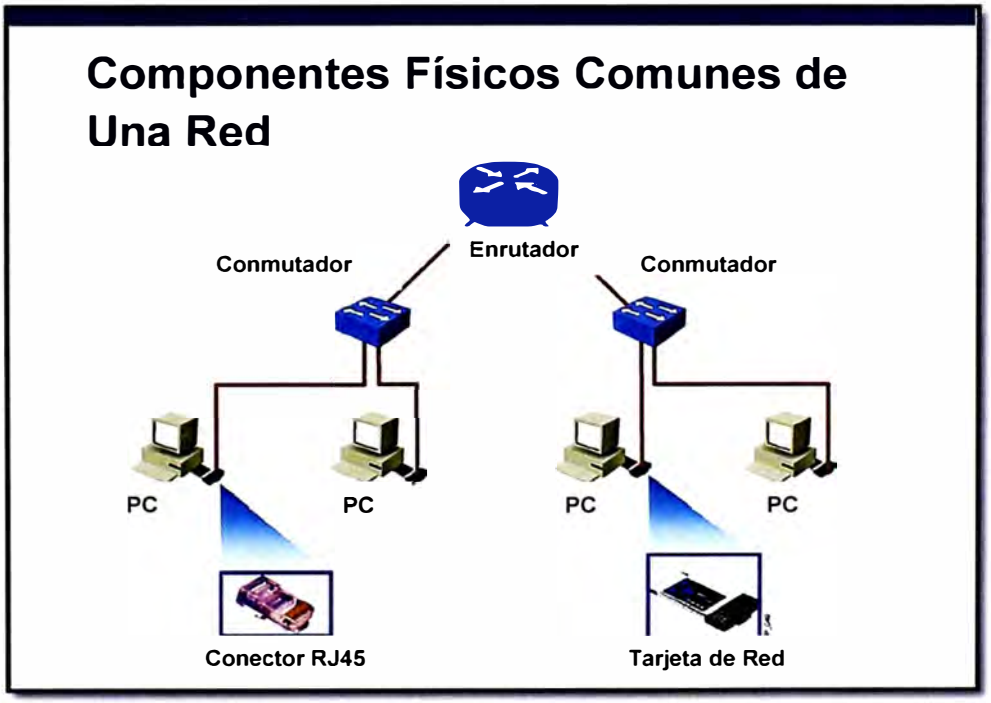


Figura 2.2 Componentes Físicos en una Red

Estos son las cuatro categorías de componentes físicos en una red de computadoras:

a.- Computadoras Personales: Las computadoras sirven como puntos finales en la red, recibiendo y enviando datos.

b.- Interconexiones: Las interconexiones consisten de un componente que provee un medio para que viaje la información de un punto a otro punto de la red. Esta categoría incluye componentes como los siguientes:

Tarjetas de red, que traslada los datos producidos por una computadora a un formato que pueda ser codificado y transmitido sobre una red local.

Medio de Red, tal como los cables o medios inalámbricos que proveen de un medio para que una señal viaje de un dispositivo de red a otro.

Conectores, proveen puntos de conexión con el medio de red.

c.- Conmutadores: Los conmutadores o switches son dispositivos que proveen de un acoplamiento a los dispositivos finales y la inteligencia para la conmutación de datos de un punto a otro punto en la red local.

d.- Enrutadores: Los enrutadores o routers son dispositivos que interconectan redes e intercambian los mejores caminos entre redes.

2.1.3 Interpretación de un Diagrama de Red

Describiremos los iconos típicos usados para representar los componentes de una red, incluyendo computadoras, conmutadores y enrutadores. Se puede observar la figura 2.3 en la cual se notara algunos iconos de mayor uso cuando se esquematiza una red.

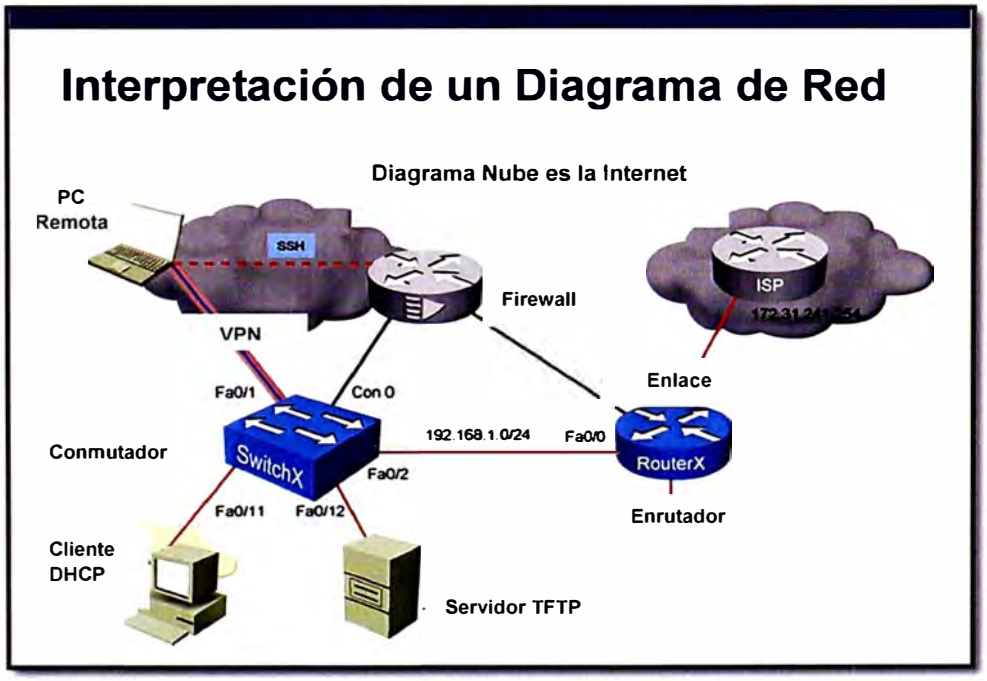


Figura 2.3 Diagrama de Interpretación de Red

El diagrama de red es usado para capturar información de forma grafica de los equipos y la conexión entre ellos en una red. La topología de red es comúnmente representada por una serie de líneas e iconos.

2.1.4 Funcionalidades y Beneficios de Compartir Recursos

Las redes permiten a los usuarios finales compartir recursos de información y equipos. La mayoría de recursos que se comparten en una red de computadoras es la siguiente:

a.- Datos y Aplicaciones: Cuando los usuarios están conectados a la red, ellos pueden compartir archivos y programas de aplicación, haciendo del intercambio de información más fácil y promoviendo la colaboración entre los trabajadores de un proyecto.

b.- Recursos: Los recursos que pueden estar compartidos pueden ser dispositivos como cámaras, impresoras, etc.

c.- Almacenamiento de red: Actualmente hay muchas formas en que la red hace accesible a los usuarios a dispositivos de almacenamiento. Dispositivos de almacenamiento directamente conectados a las computadoras o DAS (Direct Attached Storage). Dispositivos de almacenamiento conectados a la red, como un servidor al cual varios usuarios hacen uso de este, conocido como NAS (Network Attached Storage). Finalmente se puede mencionar a las redes de almacenamiento o SAN (Storage Area Network), es una red de almacenamiento integral.

d.- Equipos de reserva: Una red también puede incluir dispositivos de reserva, que proveen de un punto central para salvar información de múltiples computadoras.

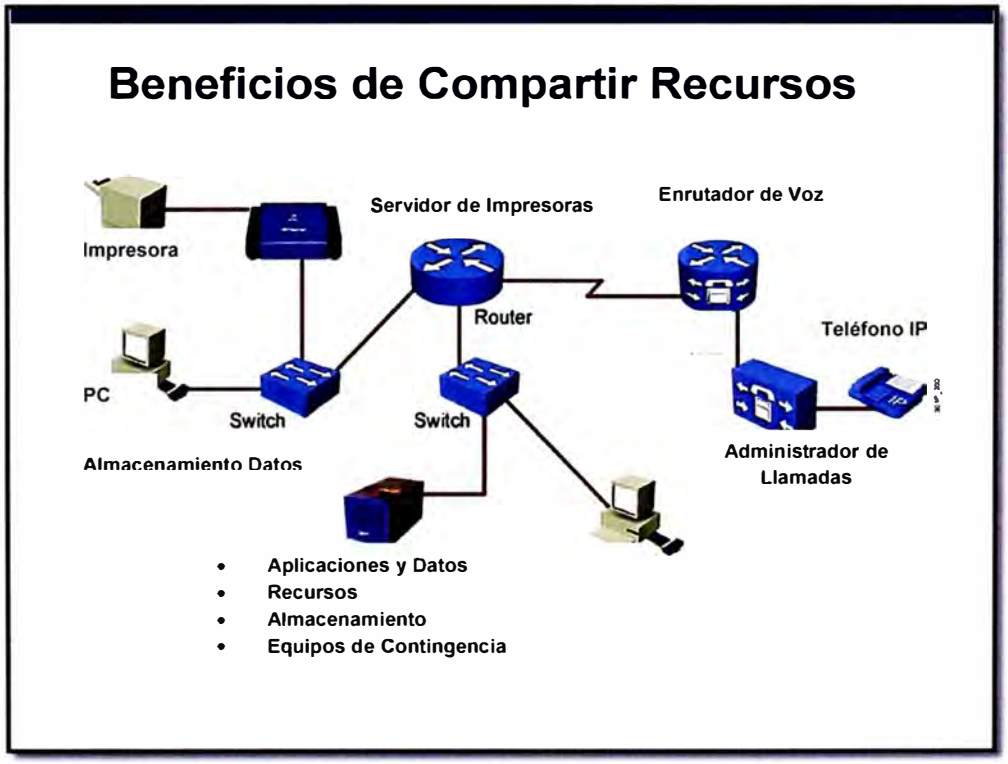


Figura 2.4 Recursos que se comparten en la Red

El conjunto de beneficios a los usuarios que se conectan a una red brinda eficiencia a la operación compartiendo componentes como impresoras, archivos compartidos, dispositivos de almacenamiento, etc. Esta eficiencia resulta en aumentar la productividad y reducir gastos.

2.1.5 Aplicaciones de Usuarios

Hay muchas aplicaciones de usuarios en una red, algunas son comunes y cercanas a todos los usuarios aquí mencionaremos estas aplicaciones. Las más comunes son las siguientes:

a.- Correo Electrónico: El correo es la aplicación más valorada por los usuarios en la red. Los usuarios pueden comunicarse electrónicamente enviando mensajes o archivos en un tiempo corto y no únicamente con usuarios en la misma red sino con otros usuarios de otras redes.

b.- Navegadores Web: Un navegador web es un programa que permite acceder a Internet a través de un lenguaje común. Internet provee abundante información la cual puede convertirse en vital para la productividad de usuarios de un hogar domestico o empresa. Los navegadores más comunes son Microsoft Internet Explorer, Mozila Firefox, Google Crome, etc.

c.- Mensaje Instantáneo: Los mensajes instantáneos se realiza en un ambiente de usuario a usuario. Es beneficioso para el mundo corporativo como para usuarios domésticos.

d.- Colaboración: Trabajar juntos entre grupos o individuos es beneficioso y productivo para la culminación de un proyecto, cuando sobre una red se instala software o hardware para la colaboración. Un software de colaboración conocido es WebEx que permite el uso compartido de presentaciones, archivos de voz, video. Estableciendo reuniones desde cualquier lugar.

e.- Base de Datos: Este tipo de aplicaciones permite a usuarios sobre una red almacenar información en un punto central por lo tanto otros usuarios de la red pueden acceder a esta misma información.

2.1.6 Características de una Red

Existen características de una red las cuales son comúnmente usadas para compararlas y establecer la eficiencia de esta red. Las redes pueden ser descritas y comparadas de acuerdo a su estructura y eficiencia, como las siguientes:

a.- Velocidad: La velocidad muestra que tan rápido los datos son transmitidos en la red. Este es un punto crítico en cuanto a la experiencia de usuario en el uso de la red.

b.- Costo: El costo indica el costo general de equipos, instalación, mantenimiento y operación de la red.

c.- Seguridad: La seguridad indica que tan segura es la red, incluyendo cuando los datos son transportados sobre la red. El tema de seguridad es realmente importante y está constantemente evolucionando. El administrador de la red debe considera la seguridad en cualquier cambio en la red.

d.- Disponibilidad: En términos generales, la disponibilidad se define como la relación entre el tiempo en que la red es funcional y el tiempo total.

e.- Escalabilidad: Indica que tan buena es la red para acomodarse a los cambios como más usuarios, nuevos equipos de red, mayores anchos de banda, etc. Si una red es diseñada teniendo en cuanta solo las necesidades iniciales podría resultar costoso y difícil de realizar un crecimiento en la red.

f.- Confiabilidad: La confiabilidad indica la confianza de los equipos que componen la red. Es medido como una probabilidad de falla o tiempo medio entre fallas.

g.- Topología: En una red, hay dos tipos de topologías: La topología lógica, es la disposición de cables, dispositivos de red, computadoras, servidores. Y la topología lógica, es el camino que la señal recorre por la topología física.

2.1.7 Topología Física y Lógica

a. Topología Física

La topología física hace referencia a la disposición física de equipos y cableado en la red. Se debe considerar la compatibilidad entre el cableado que será instalado y la topología física, los más usados son: cableado de par trenzado, coaxial, fibra óptica, etc. Hay tres categorías de topologías físicas, como se muestra en la figura 2.5:

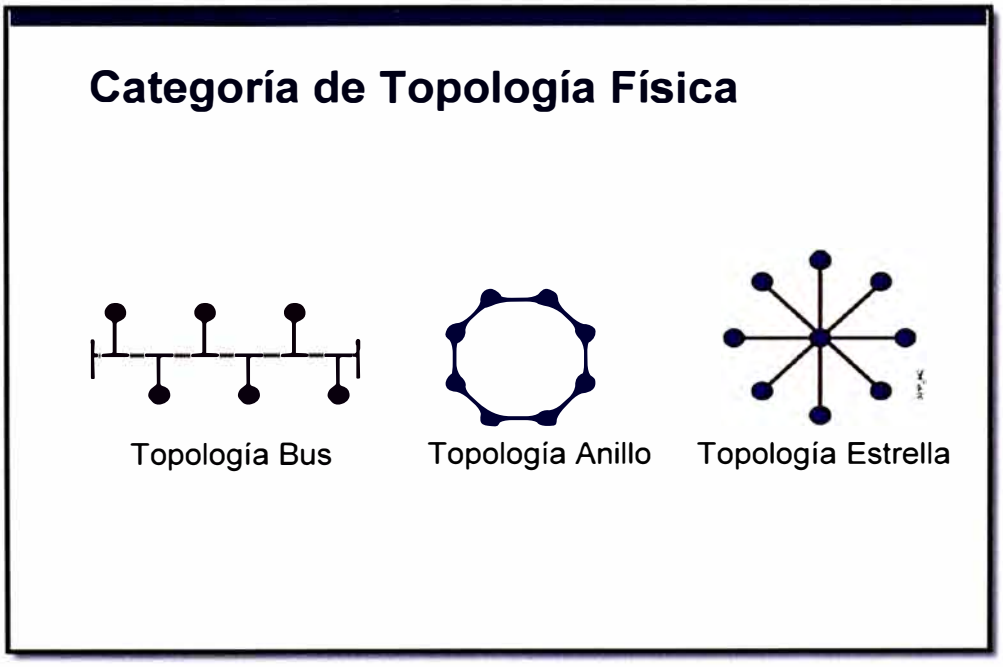


Figura 2.5 Tipos de Topología Física de Red

1.- Bus: En esta topología, todos los nodos están conectados a cable común o compartido. Es decir cuando un equipo envía un paquete de datos todos los equipos reciben el paquete. Las redes Ethernet usan esta topología.

2.- Anillo: En esta topología, todos los nodos se conectan entre sí formando un lazo cerrado, de manera que cada nodo se conecta a otros dos dispositivos.

3.- Estrella: En esta topología, cada nodo se conecta directamente a un concentrador central. En una topología de estrella todos los datos pasan a través del concentrador antes de alcanzar su destino. Este es una común tanto en redes Ethernet como inalámbricas.

b. Topología Lógica

La topología lógica de una red referencia el camino que usa la señal para ir de un punto de la red a otro. La topología lógica y física de una red puede ser la misma. Por ejemplo, en una topología física de bus la señal viaja por la longitud del cable. Por lo tanto, la topología lógica de bus es igual con la topología física de bus.

Por otro lado, una red puede tener una topología lógica y física algo diferente. Por ejemplo, una topología física en estrella, en la cual todos los segmentos de cables conectan las computadoras a un concentrador central, pueden tener una topología lógica en anillo. Por lo tanto, no siempre es posible predecir como viajan los datos a través de una red simplemente observando la disposición física de los equipos.

c. Topología Bus

Esta topología es representada como una línea, todos los dispositivos sobre la topología de bus son conectados sobre un único cable.

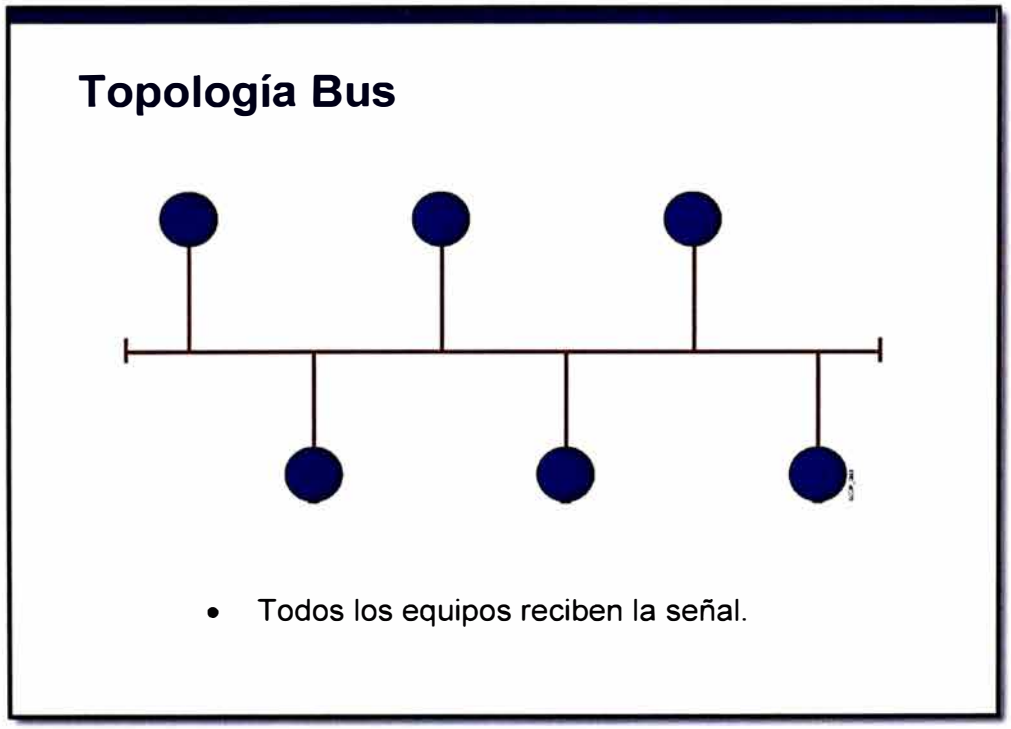


Figura 2.6 Diagrama de Topología en Bus

Como se ilustra en la figura, en una topología de bus un cable va desde un computador a la siguiente, al igual que un autobús de línea de una ciudad a otra.

Con una topología en bus física, el segmento de cable principal debe finalizar con un terminador que absorba la señal cuando ésta alcanza el final de la línea o cable. Si no

hay un terminador, la señal eléctrica que representa los datos rebotara al otro extremo del cable, provocando errores.

d. Topología Estrella

La topología en estrella, es la topología física más frecuente en las LAN Ethernet. La topología en estrella está constituida por un punto de conexión central que es un dispositivo donde se encuentran todos los segmentos de cable. Cada uno de los dispositivos en la red está conectado al dispositivo central por su propio cable. Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador, un conmutador o un concentrador siguen esta topología. El nodo central en este tipo de redes seria el enrutador, conmutador o concentrador por donde pasa todo el tráfico de datos.

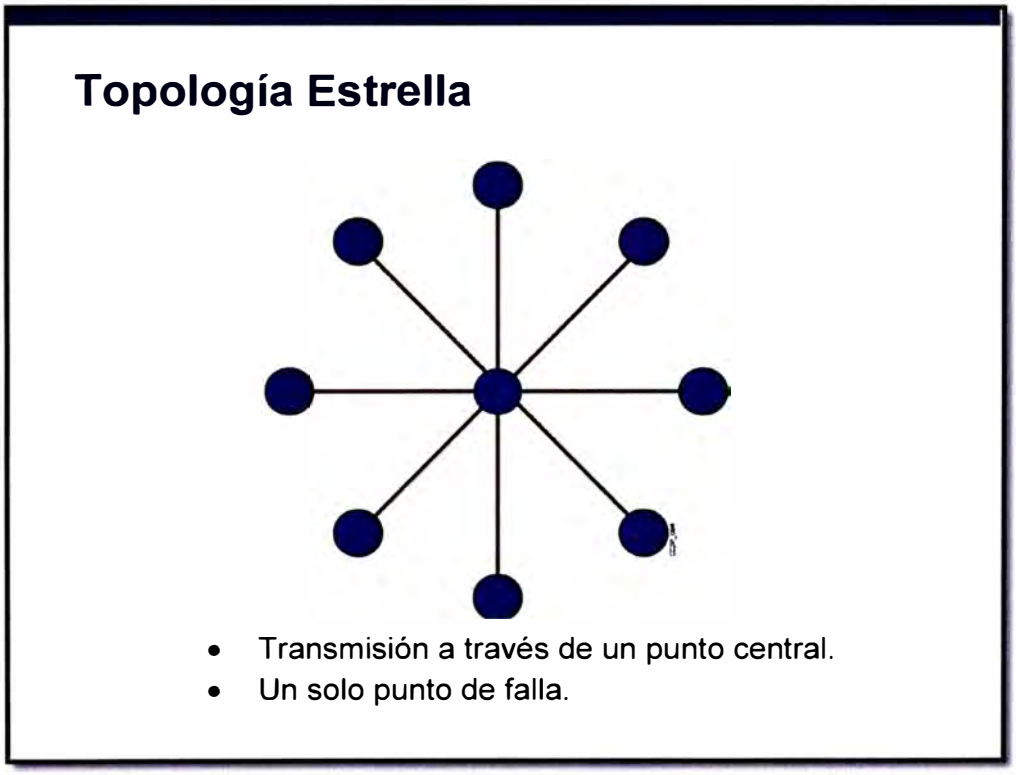


Figura 2.7 Diagrama de Topología en Estrella

e. Topología en Malla Completa y en Malla Parcial

La topología en malla completa conecta todos los dispositivos con todos los demás para conseguir redundancia y tolerancia a fallos, como muestra la figura 2.8.

El cableado en una topología en malla tiene diferentes ventajas e inconvenientes. La ventaja es que cada nodo está conectado físicamente con todos los demás, creándose una conexión redundante. Si falla cualquier de los enlaces, la información puede fluir por otros muchos enlaces para alcanzar su destino. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada nodo tiene sus propias conexiones con todos los demás nodos.

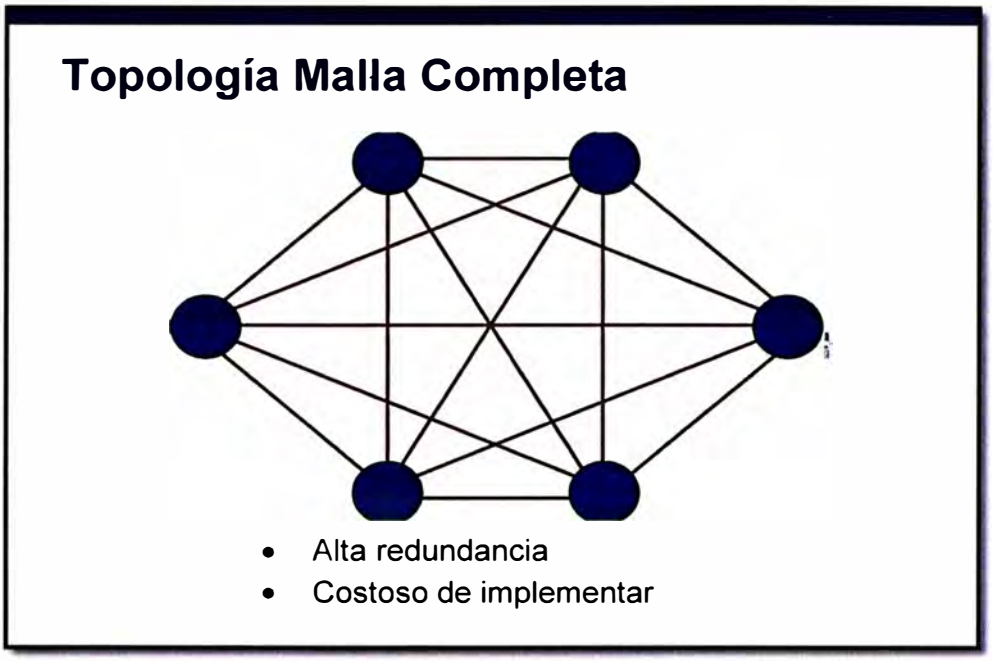


Figura 2.8 Diagrama de Topología de Malla Completa

El principal inconveniente es que para algo más que un pequeño número de nodos, la cantidad de medios para los enlaces y el número de conexiones en las líneas puede ser abrumador. La implementación de una topología en malla es costosa y compleja.

En una topología de malla parcial, al menos uno de los dispositivos mantiene múltiples conexiones con otros sin estar mallado por completo, como se muestra en la figura 2.9. Una topología en malla parcial todavía proporciona redundancia al contar con varias rutas alternativas. Si una ruta no se puede utilizar, los datos toman otra diferente, aunque sea más larga.

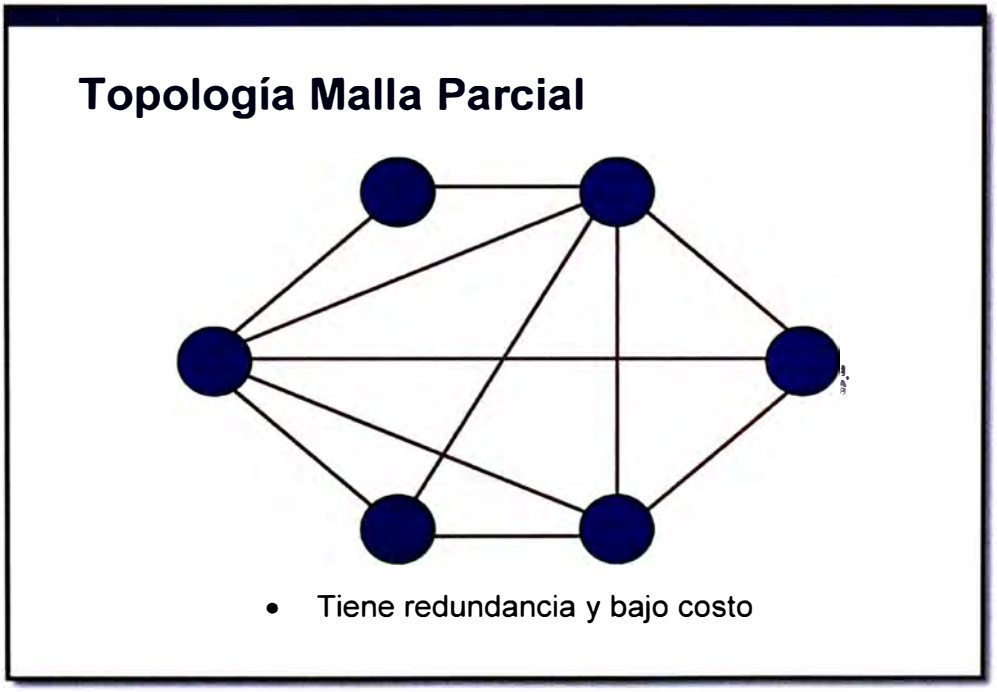


Figura 2.9 Diagrama de Topología de Malla Parcial

2.2 Fundamentos de MPLS

MPLS (Multi Protocol Label Switching) es una tecnología preferida para llevar datos a alta velocidad y voz digital en una sola conexión. Es una tecnología que puede brindar calidad de servicio priorizando tráfico de tiempo real frente a otro tipo de tráfico que no se ve afectado por el retardo. MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costos generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP. MPLS es colocado entre la Capa 2 y Capa 3 del Modelo OSI. En la figura 2.10 se puede observar la ubicación de la Capa MPLS dentro del Modelo OSI.

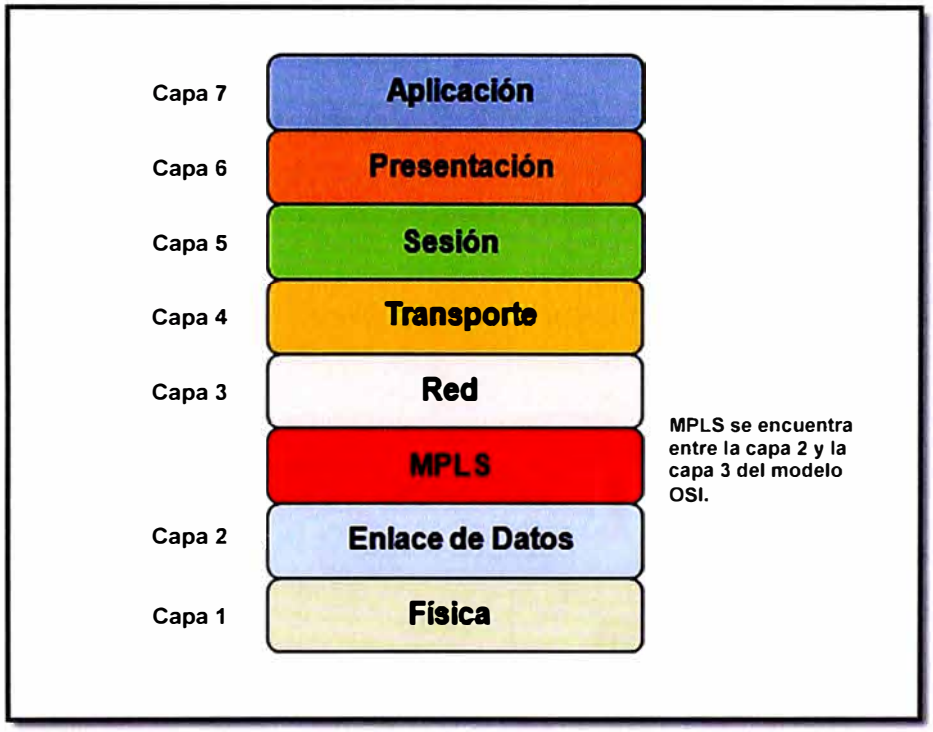


Figura 2.10 MPLS dentro del Modelo OSI

2.2.1 Características de MPLS

a. MPLS es usado sobre múltiples tecnologías.

b. Mecanismo para manejar el flujo de tráfico de tamaños variados (Flow Management).

c. Es independiente de protocolos de capa 2 y 3.

d. Mapea direcciones IP a etiquetas de longitud fija.

e. Interconecta a protocolos de existentes (RSVP, OSPF).

f. Soporta ATM, Frame-Relay y Ethernet.

2.2.2 Arquitectura MPLS

Elementos en una arquitectura MPLS. Podemos mencionar a los siguientes, figura 2.11: **LER (Label Edge Router)**: elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada

se conoce como **Ingress Router** y uno de salida como **Egress Router**. Ambos se suelen denominar Edge Label Switch Router ya que se encuentran en los extremos de la red MPLS.

LSR (Label Switching Router): elemento que conmuta etiquetas. Un LSR es como un enrutador que funciona a base de intercambiar etiquetas según una tabla de envió. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control.

LSP (Label Switched Path): nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.

LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.

FEC (Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

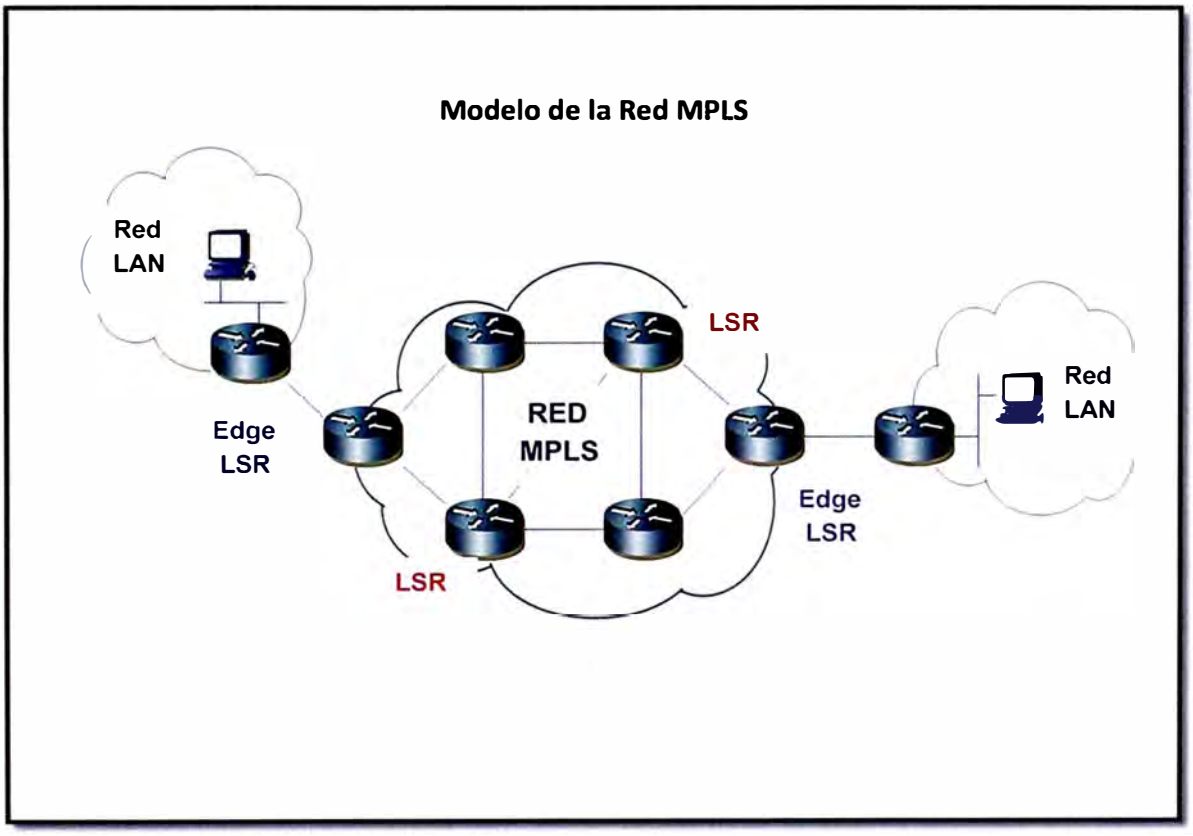


Figura 2.11 Diagrama de una Red MPLS

2.2.3 Cabecera MPLS

Las etiquetas que utiliza MPLS pueden ir en los campos para etiquetas de ATM o Frame Relay, o si se transmiten sobre cualquier otra tecnología en una cabecera que se sitúa entre la capa 2 y capa 3 del modelo OSI. En la figura 2.12 se observa el campo Label que es la etiqueta de 20 bits.

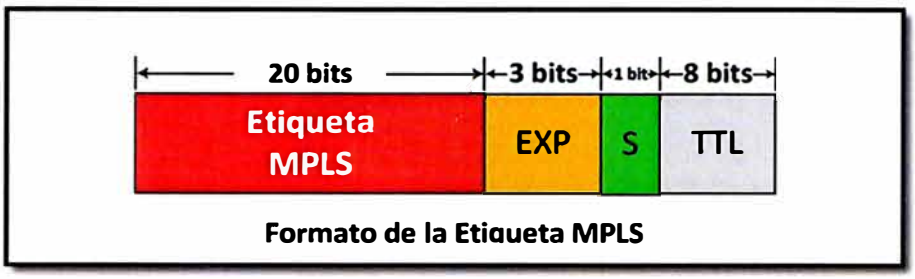


Figura 2.12 Diagrama de la Etiqueta MPLS

El campo Label es la etiqueta. Los tres bits Exp están reservados para uso experimental. El bit S se utiliza para apilamiento. El campo TTL, para mantener la funcionalidad del campo TTL de IP, ya que en la red MPLS no se accede a la cabecera IP y no puede haber decremento del campo TTL contenido en ella.

2.2.4 Operación en MPLS

La operación del MPLS se basa en la creación, distribución de etiquetas. La fuente envía datos a un destino. En un dominio MPLS, no todo el tráfico es necesariamente transportado por el mismo camino. Dependiendo de las características de tráfico, diferentes LSPs podrían ser crear diferentes paquetes con requerimientos de CoS. Ahora debemos seguir los siguientes pasos para que un paquete de datos sea transportado a través de una red MPLS:

1. Creación y distribución de etiquetas.
2. Creación de tablas en cada router.
3. Creación de label switched path (LSP).
4. Inserción de etiquetas y acceso en tablas.
5. Envió de paquetes.

a. Creación y distribución de etiquetas

Antes que el tráfico comience los routers deciden asociar un label a un FEC (Forward Equivance Class) y construir sus tablas. En LDP (Label Distribution Protocol), los routers inician la distribución de labels y la asociación label/FEC. Luego las características relacionas con el tráfico y capacidades MPLS son negociadas usando LDP. Un protocolo de transporte confiable debería ser usado para el protocolo de señalización.

b. Creación de tablas en cada router

Bajo recepción de la asociación de label, cada LSR (Label Switching Router) crea entradas en una base de información de labels (label information base - LIB), el cual puede verse en la figura 2.13. El contenido de la tabla especifica el mapeo entre un label y un FEC. Mapeo entre la puerta y label de entrada y la puerta y label de salida. Las entradas son actualizadas en cada renegociación asociando label y FEC. La asignación de labels durante todo el recorrido de la Red MPLS puede ver en la figura 2.13.

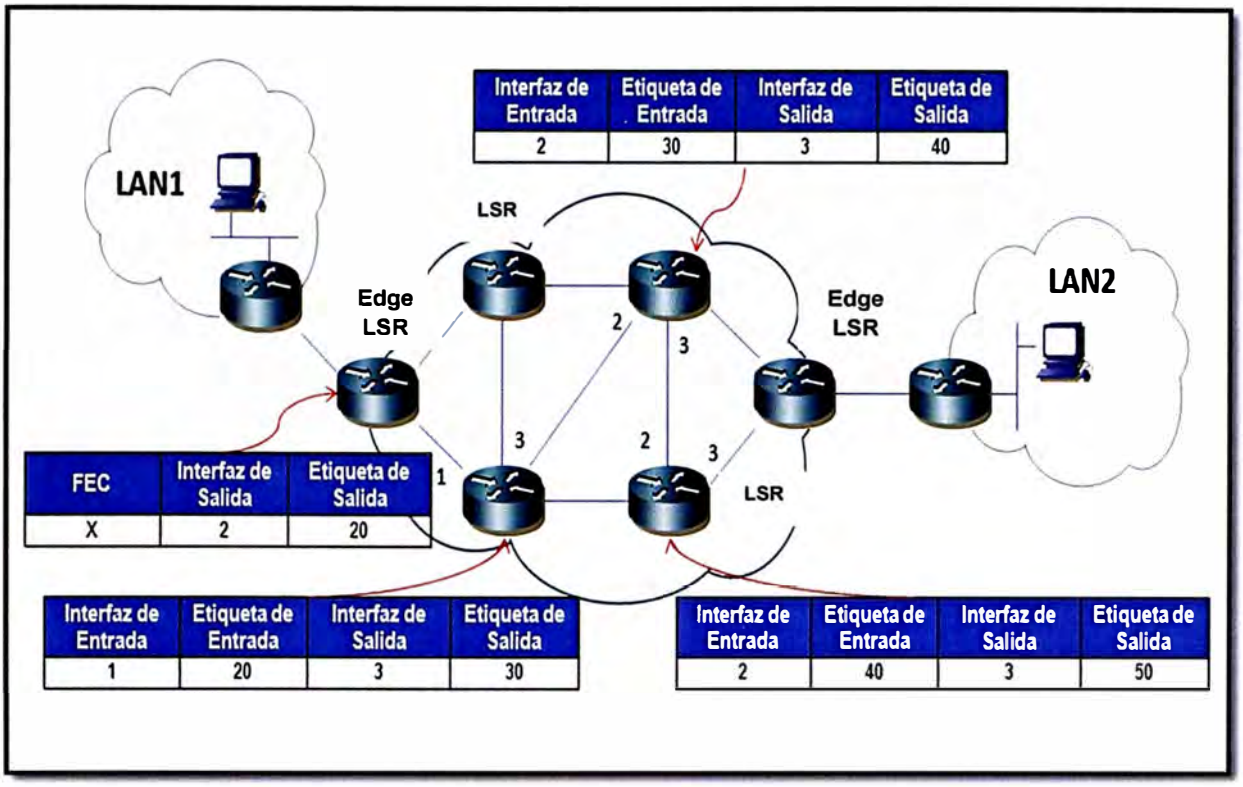


Figura 2.13 Asignación de Etiquetas en el recorrido de la Red MPLS

c. Creación de Label Switched Path (LSP)

Antes de enviar la información por el flujo es necesario establecer un Camino de Conmutación de Etiquetas (LSP) entre los routers que van a transmitir la FEC. Los LSPs son creados en dirección inversa a la creación de entradas en el LIBs. Dichos LSP sirven como túneles de transporte a lo largo de la red MPLS e incluyen los parámetros QoS específicos del flujo.

Estos parámetros sirven para determinar dos cosas:

La cantidad de recursos a reservar al LSP.

Las políticas de desechado y la cola de procesos en cada LSR.

Para lograr los puntos anteriores se utilizan dos protocolos para intercambiar información entre los routers de la red. Se le asignan etiquetas a cada flujo FEC particular para evitar el uso de etiquetas globales que dificultan el manejo y la cantidad de las mismas. Por esta razón las etiquetas sólo hacen referencia al flujo específico. La asignación de nombres y rutas se puede realizar manualmente o bien se puede utilizar el Protocolo de Distribución de Etiquetas (LDP).

d. Inserción de Etiquetas y Acceso en Tablas

El primer router (LER1) usas la tabla LIB para encontrar el próximo hop y requerir un label para un FEC específico. Los router subsecuentes sólo usan la tabla para encontrar el próximo hop. Una vez que el paquete llega al LSR de egreso (LER4), el label es removido y el paquete es entregado al destino.

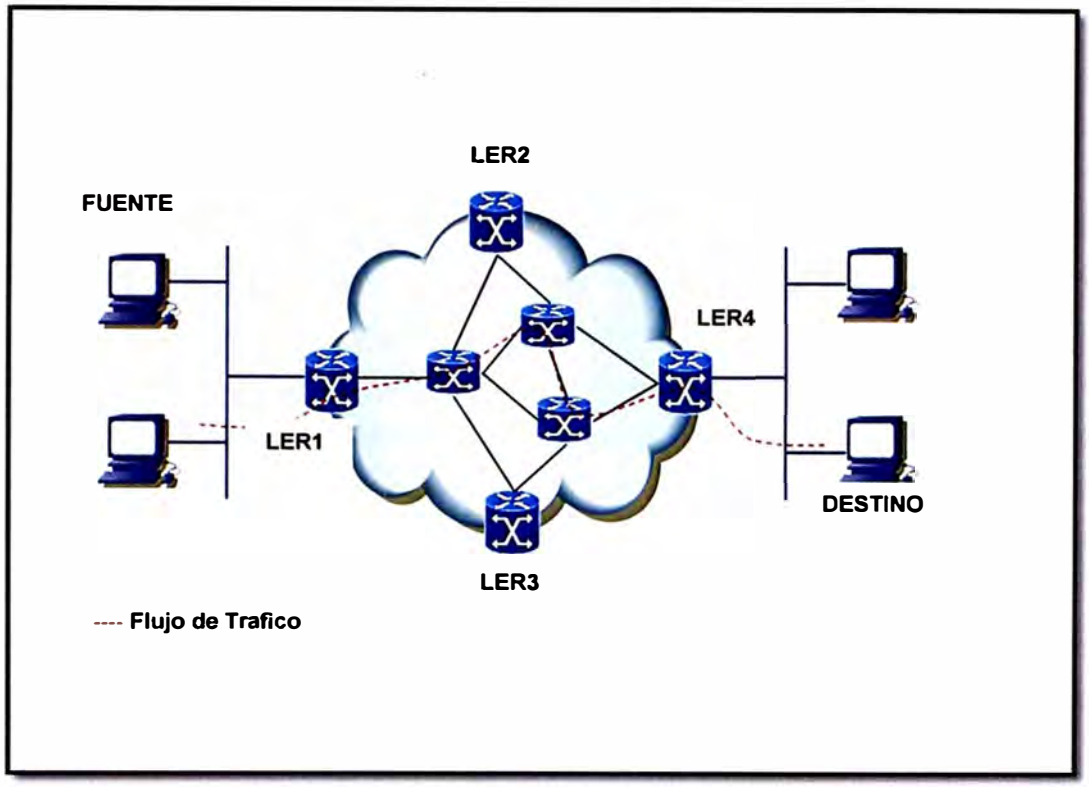


Figura 2.14 Diagrama donde se muestra LER1 y LER4 en el proceso de inserción y retiro de etiquetas

2.2.5 Calidad de Servicio QoS

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ (Servicios Diferenciados) del IETF (Internet Engineering Task Force o Fuerza de Tareas de Ingeniería de Internet). Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros para los que el retardo no es crítico, de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por

ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort.

2.2.6 Ingeniería de Tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios

Especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

2.3 MPLS L2 VPN punto-multipunto: VPLS

VPLS, también conocido como servicio de LAN transparente es una VPN punto a multipunto de capa dos que permite conectar múltiples sitios de usuario a través de la

simulación de una red de área local (LAN, del inglés, *Local Area Network*) *Ethernet*. Todos los sitios del cliente pertenecientes a una entidad VPLS parecen estar en la misma LAN, sin importar sus localizaciones, tal y como si estuvieran interconectadas a través de un gran conmutador *Ethernet*.

VPLS se basa en el re-envío de tramas *Ethernet*. La red del proveedor de servicios, por tanto, puede re-enviar la información basándose solamente en sus direcciones MAC o teniendo en cuenta además las etiquetas de LAN virtual. Es por ello que los enrutadores PE deben soportar todas las prestaciones "clásicas" *Ethernet*, como aprendizaje de direcciones MACs, inundación de tramas, etc. Desde un punto de vista funcional, esto implica que los PEs deben implementar un puente o *bridge* (según su denominación en inglés) por cada instancia VPLS. Este es conocido como puente virtual (VB, del inglés, *virtual bridge*). La funcionalidad virtual bridge se lleva a cabo en el PE mediante la asignación de una tabla virtual de re-envió (VFT, del inglés, Virtual Forwarding Table) para cada entidad VPLS.

Los elementos necesarios para constituir una entidad VPLS, como es de esperar, son los mismos que componen una MPLS L2 VPN de manera general: una red central MPLS, *routers* CEs y PEs, circuitos de conexión (AC), puentes virtuales (VB, del inglés, *Virtual Bridge*), túneles y pseudowires. Los puentes virtuales no son más que las tablas virtuales de re-envío (VFT) anteriormente mencionadas. Por otra parte, la definición de pseudowires es utilizada para denominar a una entidad bidireccional de conexión entre enrutadores PEs compuesta por dos circuitos virtuales (VC) o LSPs unidireccionales y de sentidos opuestos. El resto de la nomenclatura mantiene su mismo significado.

El circuito que posibilita dicha conexión puede ser tanto un enlace Ethernet físico o lógico, un PVC ATM transportando tramas Ethernet o incluso un pseudowires Ethernet. Con esto se simplifica la frontera LAN/WAN y se logra un aprovisionamiento rápido y flexible del servicio. La figura 2.15 muestra la estructura descrita anteriormente.

El núcleo de la red IP/MPLS interconecta los PEs que intervienen en la entidad VPLS en cuestión pero no participa realmente en su funcionalidad. El tráfico en este segmento se conmuta simplemente basándose en etiquetas MPLS. Para el intercambio de información entre dos enrutadores PEs se establecen dos circuitos virtuales (LSPs), uno en cada dirección. Estos túneles internos son los mencionados pseudowires. La arquitectura pseudowire está normalizada por Grupo de Trabajo para PWE3 (Pseudowire Emulation Edge to Edge).

Para cada entidad VPLS se crea una malla completa de túneles internos entre todos los PEs que participan en la entidad VPLS. Gracias a estos, las tramas pueden ser transmitidas directamente desde el PE de entrada hacia el de salida sin pasar por ningún

otro PE intermedio. No es necesario entonces implementar ningún protocolo de prevención de bucles, como el Spanning Tree Protocol (STP, por sus siglas en inglés), Multiple Spanning Tree Protocol (MSTP). Con la aplicación de una simple regla conocida como "Split Horizon" se prevé cualquier lazo que pueda ocurrir en una entidad VPLS. Dicha regla plantea que ningún PE debe re-enviar a través de un pseudowire el tráfico que haya recibido a través de otro pseudowire. En el PE es donde el VPLS comienza y termina y donde se establecen todos los túneles necesarios para conectar con todos los otros PEs. Sus funcionalidades quedan divididas en dos planos.

Plano de re-envío: realiza el encapsulado, re-envío y desencapsulado de las tramas Ethernet desde que entran a la red del proveedor y hasta que salen de la misma respectivamente.

Plano de control: En este plano se lleva a cabo el descubrimiento de miembros de una entidad VPLS, el cual puede ser implementado a través de una configuración manual o de forma automática a través de la utilización de determinados protocolos. Dicho plano además, se encarga de la señalización, a través de la cual establece, mantiene y elimina los pseudowires entre PEs pertenecientes a una entidad VPLS. Estas funciones pueden implementarse mediante la utilización de dos protocolos: el BGP (Border Gateway Protocol) y el LDP (Label Distribution Protocol).

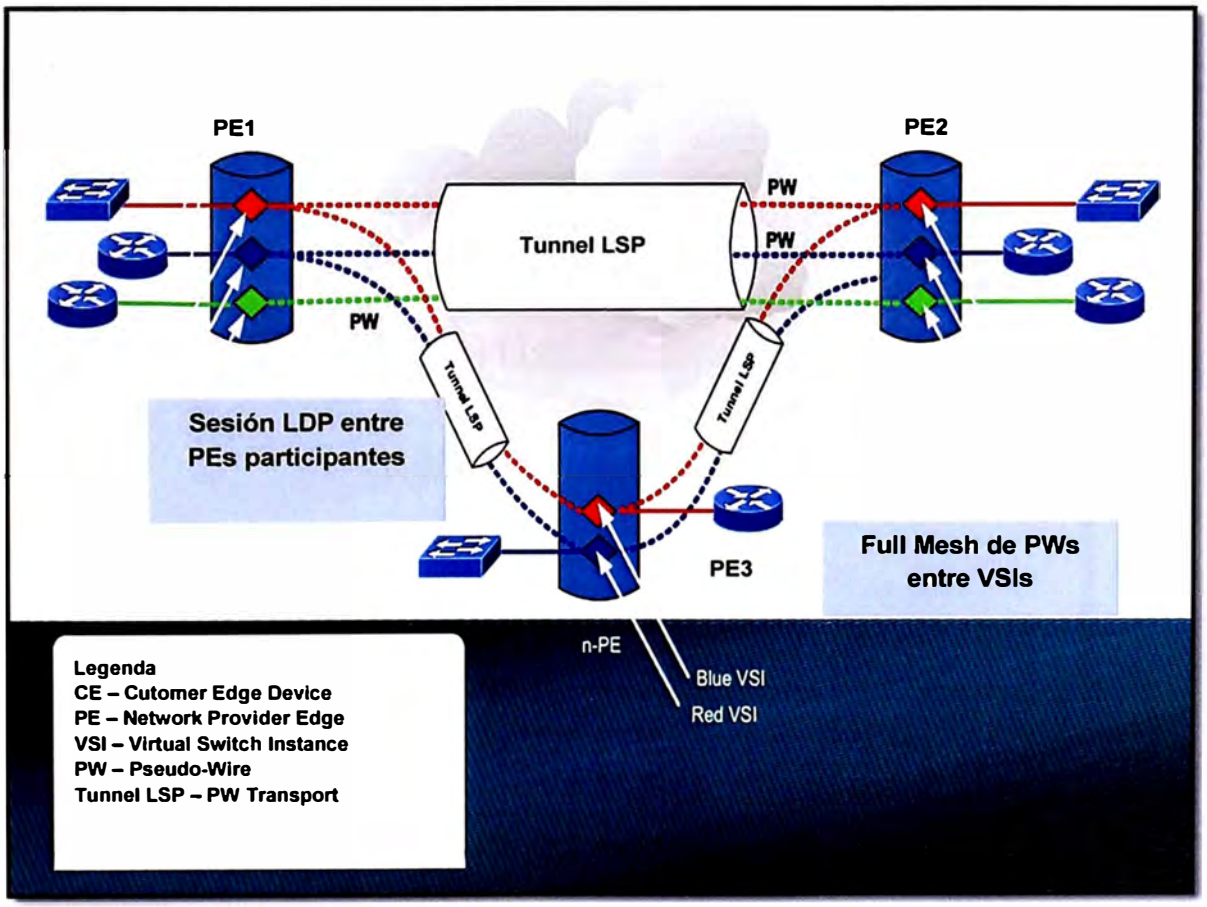


Figura 2.15 Estructura de una Red VPLS

2.4 Computación en la Nube

En la actualidad el concepto más nuevo es el de **computación en la nube** que es la tendencia de disponer de archivos y aplicaciones directamente en la Web. El termino cloud computing literalmente al español es "computación en la nube".

En los últimos 10 años la tendencia de guardar en algún lugar donde almacenar información es la contaste de las empresas, por eso cada vez la distancia se acorta entre el usuario y la red de redes. Cada usuario que usa un ordenador tendrá que usar algún tipo de aplicación de ofimática y utilidades que probablemente no tenga instalado en su computador, por lo cual esta teoría viene a revolucionar el mundo de la información.

Desde los primeros tiempos se ha graficado la noción de Internet como una nube hacia donde se conectan todas las computadoras del mundo. Lo cierto es que Internet es un concepto más complejo, ya que se trata de computadoras individuales que conforman redes, las cuales a su vez se agrupan para conformar conglomerados de redes. Estos conglomerados se interconectan conformando una red de redes, que denominados Internet. Es por eso que para simplificar esta explicación, se muestra en la figura 2.16 Internet como una nube, hacia la cual se conecta cada dispositivo para utilizar los servicios y aplicaciones que todos conocemos.

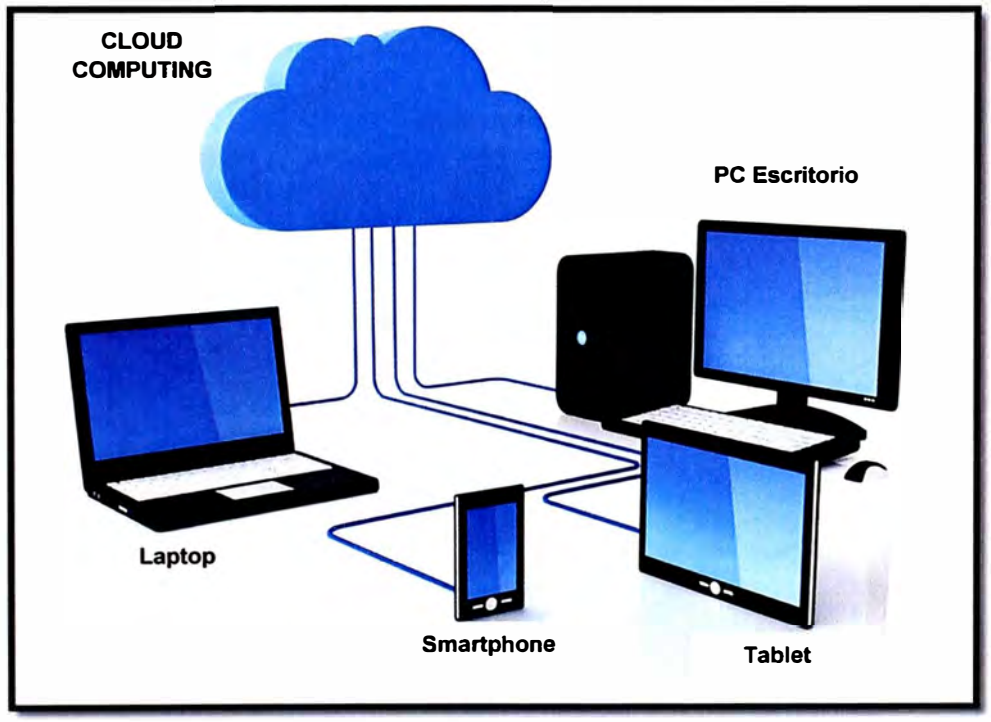


Figura 2.16 Escenario de Cloud Computing

2.4.1 Aplicaciones de Computación en la Nube

Es una tecnología que permite acceder a servicios y aplicaciones a través de Internet mediante un navegador convencional. En este tipo de sistema, el usuario puede acceder a todo tipo de servicios sin la necesidad de instalar un software en su ordenador.

Un ejemplo sencillo de servicios en la nube son los servicios de correo electrónico, muchas personas tienen cuentas en Hotmail, Gmail, yahoo etc. Estas casillas de correo permiten enviar, recibir y almacenar nuestros mensajes en servidores alojados en la nube, el usuario accede a este servicio a través de un navegador web.

Todos estos mensajes no llegan a descargarse en nuestra computadora personal, por tal motivo el usuario puede acceder a esta información desde cualquier dispositivo, desde cualquier lugar y en cualquier momento

Estas facilidades de acceso a la información alojados en la nube han provocado una tendencia tecnológica de llevar todo el servicio a la nube. Actualmente podemos hacer uso de servicios de video para ver películas online hasta servicios que nos permiten editar documentos y hojas de cálculo.

Otros servicios de bastante uso son los servicios de alojamiento de archivos multiplataforma en la nube conocidos como Cloud Storage. Estos servicios permiten a los usuarios almacenar, compartir archivos con otros usuarios. Podemos mencionar a Dropbox y SkyDrive como ofertantes de este tipo de servicios.

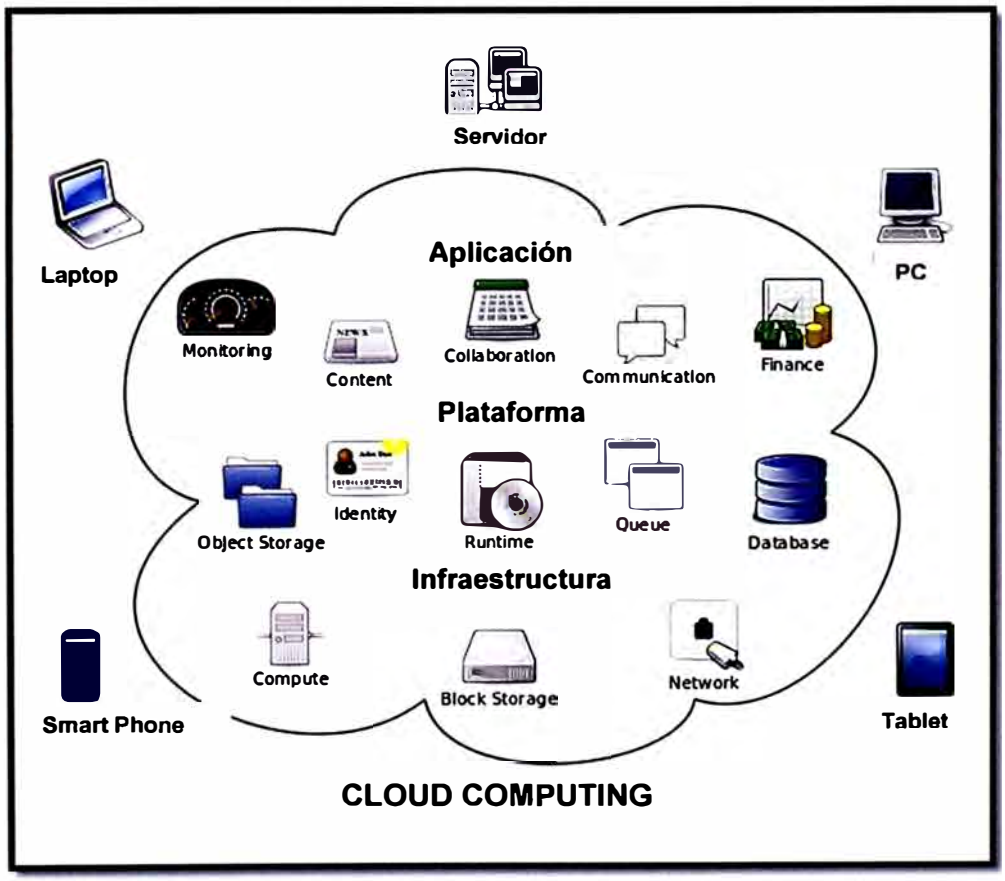


Figura 2.17 Tipos de Aplicaciones en el concepto Cloud Computing

2.4.2 Clases de Computación en la Nube

Computación en la Nube o Cloud Computing se ha convertido en un concepto muy usado y que puede referirse a muchas cosas. Se puede usar en múltiples contextos para

referirse a cosas de lo más dispares. Pero parece que hay consenso respecto a las tres clases fundamentales del Cloud Computing.

Software como Servicio: (en inglés Software as a Service, SaaS). Modelo de distribución de software donde una empresa sirve el mantenimiento, soporte y operación que usará el cliente durante el tiempo que haya contratado el servicio. El cliente usará el sistema alojado por esa empresa, la cual mantendrá la información del cliente en sus sistemas y proveerá los recursos necesarios para explotar esa información.

Infraestructura como Servicio: (en inglés Infrastructure as a Service, IaaS). Modelo de distribución de infraestructura de computación como un servicio, normalmente mediante una plataforma de virtualización. En vez de adquirir servidores, espacio en un centro de datos o equipamiento de redes, los clientes compran todos estos recursos a un proveedor de servicios externo.

Plataforma como Servicio: (en inglés Platform as a Service, PaaS). Este modelo de distribución de un ambiente de desarrollo y el empaquetamiento de una serie de módulos o complementos que proporcionan normalmente una funcionalidad horizontal. De esta forma, un tipo de plataforma como servicio podría consistir en un entorno conteniendo una pila de básica de sistemas o componentes pre-configurados y listas para integrarse sobre una tecnología concreta de desarrollo.

En la figura 2.18 se muestra las tres clases de computación en la nube.

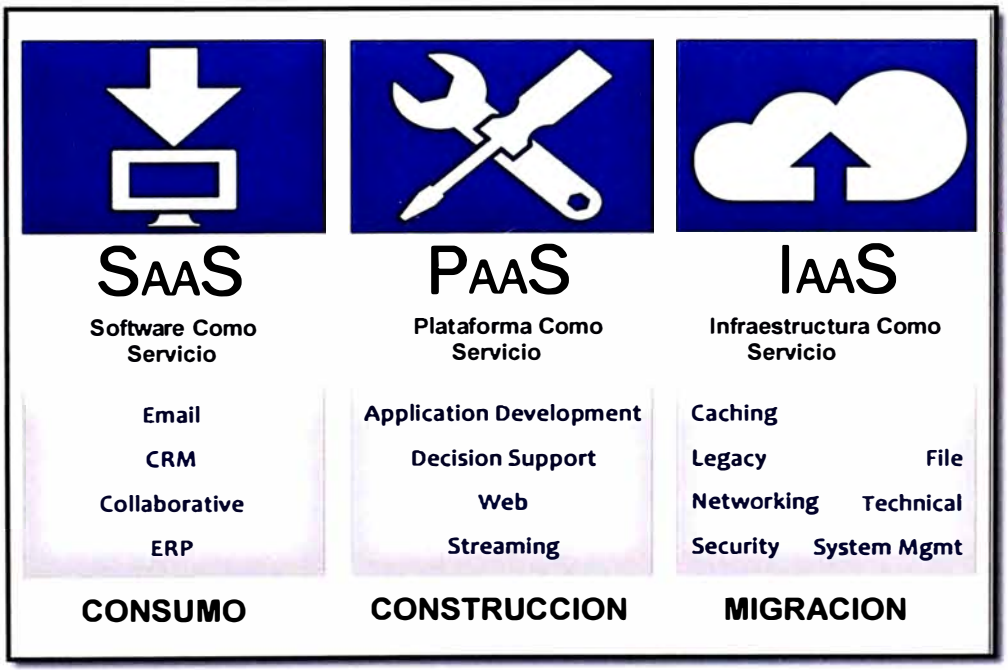


Figura 2.18 Clases de Servicios en Cloud Computing

2.4.3 Ventajas y Desventajas de Computación en la Nube

Entre las ventajas de los servicios en la nube podemos mencionar son los siguientes:

1. Acceso a la información y los servicios desde cualquier lugar.

2. Disponibilidad del servicio y/o aplicación web 24h/7dias/365dias.
3. Accesibilidad mediante diferentes tecnologías compatibles, tales como: tablets, móviles, laptops, computadora de escritorio, etc.
4. Servicios gratuitos y de pago según las necesidades del usuario.
5. No saturación del uso del disco duro en el ordenador o aplicación que se usa, debido a que solo se necesita un navegador web, e Internet.
6. Empresas con facilidad de escalabilidad.
7. Capacidad de procesamiento y almacenamiento sin instalar máquinas localmente.

Entre las desventajas podemos mencionar las siguientes:

1. Acceso de toda la información a terceras empresas.
2. Dependencia de los servicios en línea.
3. En ocasiones, puede que debido a una catástrofe natural o error humano, dicho servicio quede fuera de servicio, con las malas repercusiones a los clientes.
4. Guardar datos privados, fotos, videos, o información mucho más privada en estos servicios.
5. Descontrol del manejo, almacenamiento y uso de esta información.
6. Mayor dependencia de proveedores de Internet, y de la velocidad contratada en el servicio de Internet. Posibilidad de que delincuentes cibernéticos rompan la seguridad del servicio y se hagan con datos privados.

CAPITULO III
METODOLOGIA PARA LA SOLUCION DEL PROBLEMA

3.1 Alternativas de Solución

Después de haber detallado los retos que debe afrontar el área de tecnologías de información (TI) de una empresa para mantener segura la red corporativa de agentes externos e internos, debemos buscar la mejor solución para brindar este servicio de seguridad de red.

Para la solución propuesta debemos considerar los costos involucrados en las etapas de diseño, implementación, mantenimiento y optimización del proyecto, por tal motivo se tendrá en consideración los costos de los dispositivos de seguridad involucrados así como sus características técnicas asegurando futuros crecimientos en la red como usuarios, anchos de banda, etc. Otro punto importante a considerar son los costos del personal técnico calificado dedicados a la operación de la solución propuesta, este punto es importante pues contar con un personal técnico con experiencia y certificaciones en redes asegura el correcto funcionamiento de la solución y que tendrán la experiencia para realizar cambios y configuraciones sobre los dispositivos de seguridad.

Además debemos de tener en cuenta el factor humano, actualmente muchos colaboradores de una empresa o institución llevan al trabajo su propio dispositivo como laptops, notebooks, tablets, etc. Estos usuarios de la red deben estar sujetos a la administración del acceso a Internet sin importar desde que dispositivo accedan.

Por lo antes mencionado debemos diseñar una solución que entregue seguridad en la navegación y control sobre el flujo de datos, desde y hacia Internet, a través de Firewall, IPS, Antivirus, Antispam y Filtro de Contenidos. Con estas herramientas se podrá administrar el acceso de los empleados a sitios Web específicos, para maximizar su productividad y aumentar el rendimiento de la red. Además esta solución de seguridad debe poder ofrecer protección a los datos de la organización y bloquear el acceso a personas y programas externos.

3.1.1 Primera Alternativa de Solución

Para brindar un servicio de seguridad de red, la primera opción es instalar un dispositivo de seguridad en la red LAN. Este tipo de soluciones en la de mayor uso por el personal de tecnología de información (TI) de una empresa. Se debe considerar un ambiente

adecuado para la instalación de estos equipos de comunicaciones, como pueden ser cuartos de comunicaciones, un gabinete, energía estabilizada, cableado de red, etc.
Por otro lado, también se debe considerar el personal técnico adecuado para brindar soporte de mantenimiento y configuración sobre estos equipos de seguridad.
Por estas consideraciones la empresa debe de asignar un presupuesto para cubrir los costos de implementación de esta solución así como el sueldo de la persona o grupo de personas que se encargaran de brindar el soporte de los equipos de seguridad.

3.1.2 Segunda Alternativa de Solución

Por lo expuesto acerca de los servicios en la nube, podemos considerar una solución que integre el servicio de Internet y la seguridad, como un solo servicio. En este escenario el proveedor de servicio de Internet será el ejecutor de los trabajos de instalación, mantenimiento y optimización de la solución de seguridad. Por considerarse la seguridad como un servicio integral al servicio de Internet, la empresa no tendrá que adquirir ningún dispositivo de seguridad.

Para los trabajos de instalación el operador debe brindar el espacio donde se instalaran los equipos, este espacio se puede considerar un gabinete en el Data Center del proveedor, con esto la empresa no tendrá que preocuparse por buscar un espacio en sus oficinas. El operador será el responsable de contar con un grupo de personas calificadas para brindar soporte y mantenimiento al servicio de seguridad.
La empresa o cliente solo deberá comunicarse con el operador para solicitar cambios en la configuración. Por ser un servicio, será el operador quien tendrá que preocuparse por que los equipos puedan soportar los cambios que solicite el cliente, como pueden ser: mayores anchos de banda en el acceso a Internet, crecimiento en cantidad de usuarios, etc.

3.2 Solución del Problema

De ambas alternativas de solución, la mejor opción para el cliente es un escenario en el cual no tenga que adquirir equipos ni contratar personal dedicado para labores de mantenimiento de los equipos de seguridad. Por lo tanto, se desarrollara un diseño en el cual se considera una solución de seguridad en la nube del operador de Internet.

3.2.1 Objetivo de Solución

El objetivo de esta solución será realizar un guía de diseño y configuración para implementar un escenario de servicio de seguridad en la nube del operador de Internet.

3.2.2 Consideraciones de la Solución

Para la solución de seguridad en la nube debemos considerar lo siguiente:

a. La disponibilidad de recursos físicos y lógicos en la red del operador, como hilos de fibra óptica, puertos físicos, direcciones IP privada y pública, etc.

b. Debemos considerar las características técnicas de los equipos involucrados en la solución.
c. La solución de un servicio de seguridad en la nube se planteara sobre una red IP/MPLS del operador de Internet.
d. Disponibilidad de recursos lógicos y de procesamiento en el equipo firewall instalado en la nube del operador.

3.2.3 Descripción del servicio de Internet

En el presente informe se describirá las características del servicio de Internet y de la plataforma de red sobre la que este implementada.

El servicio Accedo Dedicado a Internet, debe ser un servicio orientado para el segmento corporativo que a través de una plataforma única, convergente y multiservicios proporcione conectividad a Internet. Estos servicios además de conectividad a Internet deberán incluir el soporte técnico y mantenimiento necesarios para mantener la continuidad operativa de sus servicios, a través de acuerdos de nivel de servicios.

a. Características del Servicio de Internet

Capacidad, de manejar diferentes tasas de velocidad desde 128Kbps hasta 100Mbps. Opciones superiores estarán fuera de los alcances de este informe.

Métricas de calidad, diferenciadas para asegurar el cumplimiento de los objetivos de desempeño y las expectativas del cliente. Estos servicios de Internet deben incluir herramientas que le permitan al cliente observar el consumo de ancho de banda en tiempo real.

Fibra óptica, que compone la red y el backbone al 100%. Se debe entender que la red de acceso, distribución y core debe ser en fibra óptica.

Convergencia: Una sola infraestructura 100% IP, basada en arquitectura MPLS (Multiprotocol Label Switching).

Confiabilidad: El servicio Acceso Dedicado a Internet del operador de Internet debe contar con un alto nivel de disponibilidad, 99.98% en el acceso y 99.5% en la última milla. Se debe entender como última milla la acometida del cable de fibra óptica desde la red del operador hasta la sede del cliente.

Escalabilidad: Gran flexibilidad para implementar anchos de banda, prioridades, nuevos servicios y aplicaciones de valor agregado.

Soporte calificado: Atención y asesoría con personal calificado 7x24 los 365 días del año.

Los servicios de Internet que ofertan los proveedores se diferencian principalmente por la tasa que garantiza un mínimo del ancho de banda en horarios de tráfico alto. Esto es más conocido por el termino **overbooking**.

Otra definición de overbooking, es el nivel de sobreventa de un enlace es decir cuántos usuarios van a estar compartiendo los recursos de un enlace.

En el presente informe se realizara considerando un enlace de Internet con el 100% de ancho de banda garantizado y simétrico. Es decir que un único cliente usa los recursos de un enlace.

Los anchos de banda a ser considerados en el acceso a Internet en el presente informe se muestran en la siguiente tabla 3.1:

Tabla 3.1 Anchos de Banda para el Internet en el Servicio Seguridad en la Nube

	Anchos de Banda
Ancho de Banda de Internet	1M, 1.5M, 2M, 2.5M, 3M, 4M, 5M, 6M, 7M, 8M, 9M, 10M, 15M

b. Componentes del Servicio de Internet

Los componentes del servicio se muestran en la figura 3.1.

Internet: Es el caudal de acceso a Internet, que es ofrecido según el plan específico.

Acceso a la Red: Corresponde a los elementos físicos y lógicos necesarios para conectar la sede del cliente al punto de atención más adecuado.

Enrutador: Es el equipo terminar instalado en la sede del cliente, que permite conectar la red del cliente al servicio de Internet.

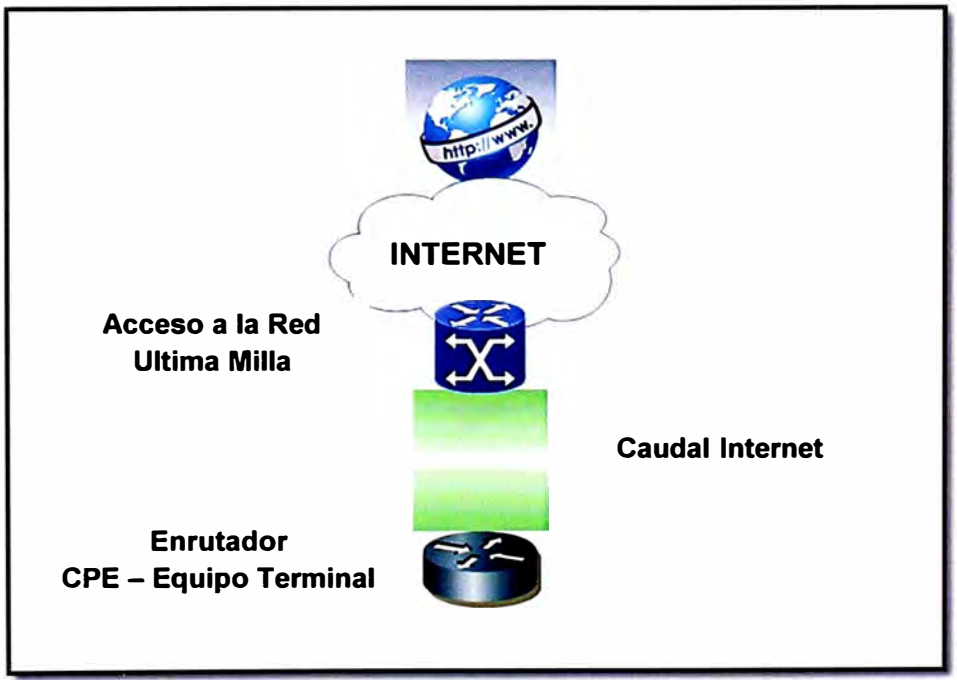


Figura 3.1 Componentes básicos en el acceso a Internet

3.2.4 Arquitectura del servicio de Internet – Seguridad en la Nube

a. Elementos del servicio de Internet

El servicio de Internet esta soportado sobre una red IP/MPLS con los siguientes elementos en la red.

Red IP/MPLS y Acceso Metro Ethernet

La figura 3.2 muestra los elementos de red sobre la cual se soportara el servicio de Internet – Seguridad en la nube. Se puede observar los equipos enrutadores como son los CPE y PE. Las ubicaciones de estos equipos son en la sede del cliente y en el NODO de la red del operador de Internet. Además se puede observar el equipo de conmutación de tráfico o switch ubicado en el POP o punto de presencia más cercano al cliente de parte del operador de Internet.

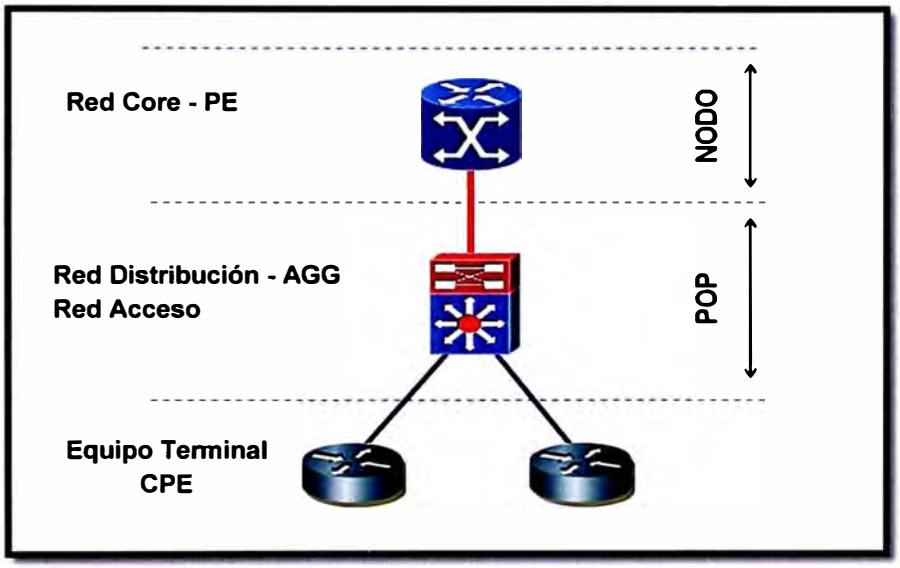


Figura 3.2 Elementos de Red IP/MPLS

Elementos del servicio de Internet – Seguridad en la nube

La figura muestra los elementos a considerar para el servicio de Internet – Seguridad en la nube.

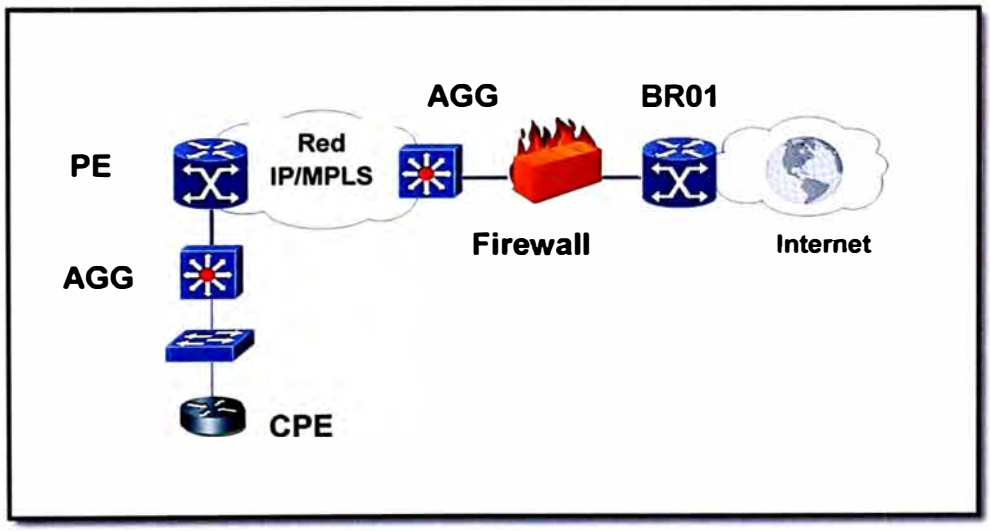


Figura 3.3 Elementos del Servicio de Internet – Seguridad en la nube

El servicio de Internet - Seguridad en la nube debe ser implementado sobre una Red IP/MPLS con Acceso Metro Ethernet. En la siguiente figura 3.4 se muestra el detalle de la Red de Acceso y la Red de Core del operador.

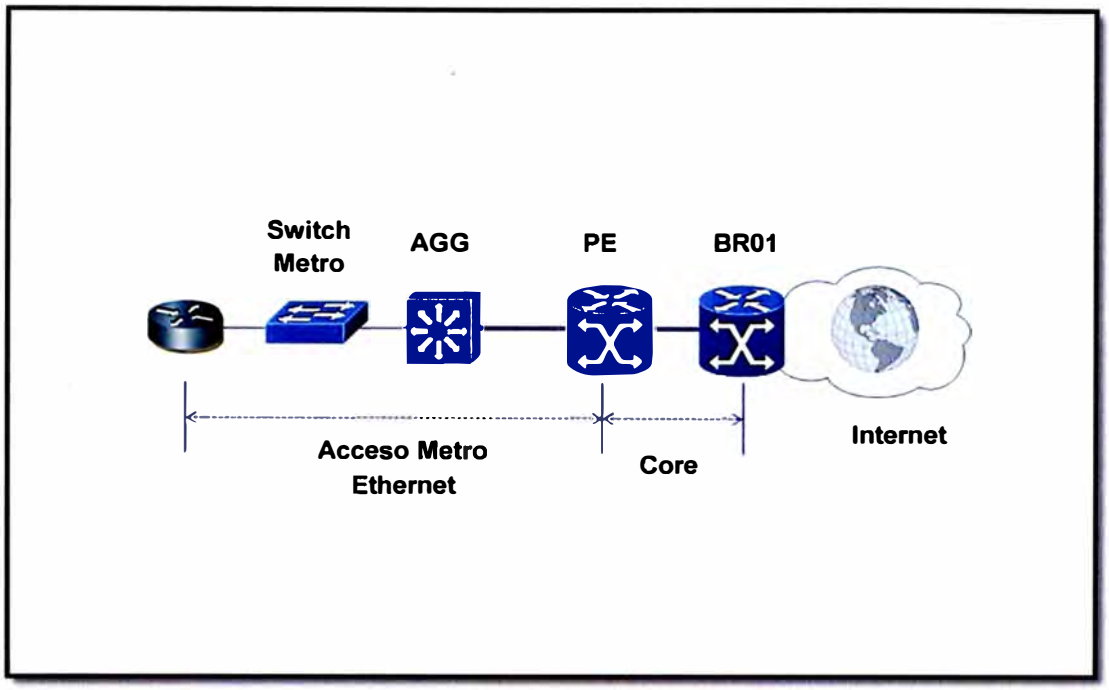


Figura 3.4 Arquitectura de la Red IP/MPLS

Anchos de Banda para la Plataforma Metro Ethernet

Los anchos de banda para la plataforma Metro Ethernet se detallan en el siguiente cuadro son:

Tabla 3.2 Anchos de Banda en el Acceso Metro Ethernet

	Anchos de Banda
Anchos de Banda Acceso Metro Ethernet	1M, 1.5M, 2M, 2.5M, 3M, 4M, 5M, 6M, 7M, 8M, 9M, 10M, 15M, 20M, 25M,30M, 35M, 40M, 50M, 60M, 70M, 80M, 90M, 100M

Arquitectura de la Red de Acceso Metro Ethernet

La arquitectura de la Red IP/MPLS con Acceso Metro Ethernet estará comprendido por equipos de marca Cisco instalados en distintos puntos del departamento de Lima, estos puntos son conocidos como POP (Punto de Presencia).

En la Red de Acceso del operador estará compuesta por switches Metro Ethernet de marca Cisco. Estos equipos son utilizados para brindar conexión al CPE ubicado en la sede del cliente. En la tabla 3.3 se muestran los equipos Cisco Catalyst Serie 4500 a considerar en la red de acceso.

En la Red de Distribución del operador estará compuesta por los equipos Cisco Serie 7200, estos equipos se usaran para agregar múltiples equipos Catalyst Serie 4500 de la red de acceso. En la tabla 3.3 se muestran estos equipos.

En la Red de Core del operador estará compuesta por los siguientes equipos Serie ASR 9000 y Serie GSR 12000 según la tabla 3.3.

Tabla 3.3 Relación de equipos en la Red IP/MPLS

Hardware	Características	IOS
Cisco ASR 9000	Proveedor de Servicios	c9kprp-p-mz.125-29-S5.bin
Cisco GSR 12406	Proveedor de Servicios	c12kprp-p-mz.120-31-S6.bin
Cisco 7206 VXR - NPE 400	Proveedor de Servicios	c7200-p-mz.123-21.bin
Cisco 7206 VXR - NPE G1	Proveedor de Servicios	c7200-p-mz.123-21.bin
Cisco 7206 VXR - NPE G2	Proveedor de Servicios	c7200p-spservicesk9-mz.124-4.bin
Cisco Catalyst 4510R	Mejorado L3 3 (OSPF, EIGRP, IS-IS)	cat400-i5s-mz.122-25.EWA2.bin
Cisco Catalyst 4506	Mejorado L3 (OSPF, EIGRP, IS-IS)	cat400-i5s-mz.122-25.EWA2.bin

En la figura 3.5, se muestra la arquitectura de la Red IP/MPLS con acceso Metro Ethernet con este modelo se basa el presente informe y es un tipo de red que cumplen muchos operadores de servicio de Internet en el Perú. Por lo expuesto en el marco teórico la red MPLS ofrece muchas características que brindan al operador ofrecer muchos servicios sobre una misma infraestructura de red.

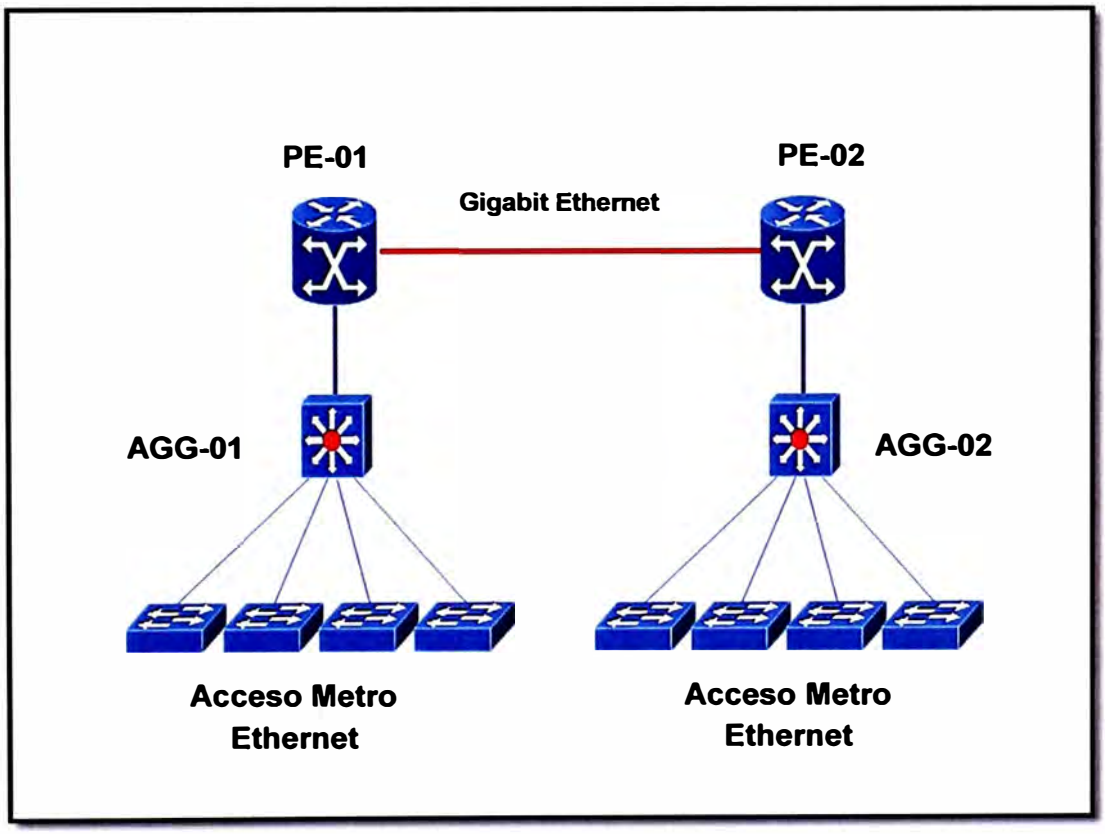


Figura 3.5 Arquitectura de Red IP/MPLS con Acceso Metro Ethernet

Características de los equipos en el local del cliente

Los equipos en el local del cliente (CPE), es un equipo de telecomunicaciones usado para encaminar o terminar la comunicación. Este equipo será el encargado de tener la configuración necesaria para permitir la conectividad hacia Internet. En la tabla 3.4 y tabla 3.5 se muestran algunos equipos validados para el servicio de Internet – Seguridad en la nube.

Tabla 3.4 Relación de Equipos CPE – CISCO

Series de Equipo	Versión de IOS	BW Soportado	FLASH	DRAM
Cisco881	15.0.1	16Mbps	28MB	128MB
Cisco1921	15.0.1	80Mbps	64MB	128MB
Cisco2901	15.0.1	120Mbps	64MB	256MB
Cisco2921	15.0.1	150Mbps	64MB	256MB
Cisco2941	15.0.1	200Mbps	64MB	256MB
Cisco3901	15.0.1	340Mbps	64MB	256MB
Cisco871	12.4	6Mbps	28MB	128MB
Cisco2801	12.4.8	20Mbps	64MB	128MB

Tabla 3.5 Relación de Equipos CPE - JUNIPER

Series de Equipo	Versión SO	BW Soportado	FLASH	DRAM
Juniper SRX100	JUNOS OS	60M	2GB	2GB
Juniper SRX110	JUNOS OS	100M	2GB	2GB
Juniper SRX210	JUNOS OS	180M	2GB	2GB

Características del Equipo de Seguridad

Este dispositivo será instalado en la nube del operador. En este equipo se configurara las funcionalidades de seguridad y protocolos de enrutamiento necesarios para brindar el servicio de seguridad en la nube.

Este dispositivo debe tener las características de seguridad, enrutamiento, conmutación y conectividad WAN. Las características la gestión unificada de amenazas (UTM) se incluye lo siguiente: Antivirus, seguridad de aplicaciones, IPS, antispam y filtrado web. El dispositivo que cumple estas características es la serie SRX de la marca Juniper. En el diseño para la solución de seguridad en la nube se realizara con el equipo SRX650 cuyas características se muestran en la tabla 3.6.

Tabla 3.6 Características del equipo Juniper SRX650

SRX650 Services Gateway
Four fixed ports 10/100/1000 Ethernet LAN ports, 8 GPIM slots or multiple GPIM and XPIM combinations.
Support for T1, E1, DS3/E3, Ethernet ports; supports up to 52 Ethernet ports including SFP; 48 switch ports with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af (or 52 non-PoE 10/100/1000 Copper ports), 10GbE.

Content Security Accelerator hardware for faster performance of IPS and ExpressAV.
Full UTM; antivirus, antispam, enhanced Web filtering, and intrusion prevention system, AppSecure.
Unified Access Control and content filtering.
Modular Services and Routing Engine; future internal failover and hot-swap.
2 GB DRAM default, 2 GB compact flash default, external compact flash slot for additional storage.
Optional redundant AC power; standard AC power supply that is PoE-ready; PoE power up to 250 watts single power supply or 500 watts dual power supply.

3.2.5 Proceso de Diseño e Implementación del servicio

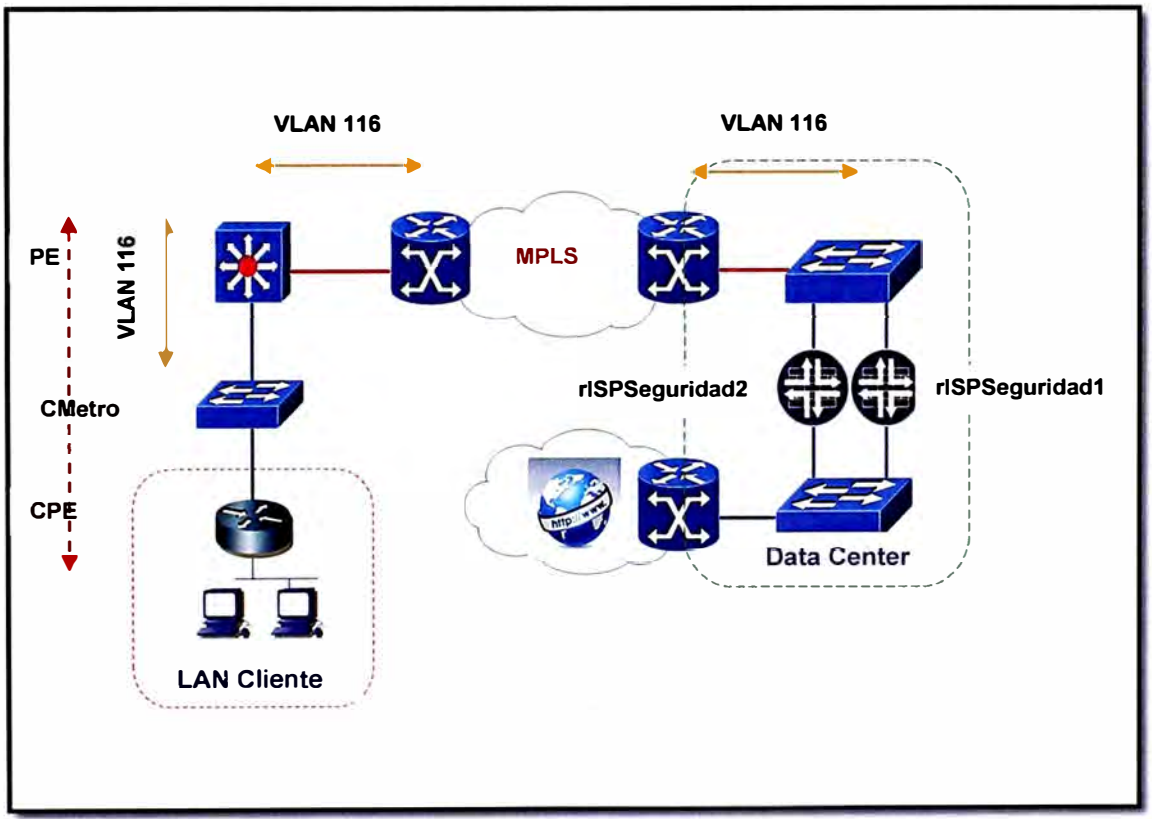


Figura 3.6 Arquitectura de red del Servicio Seguridad en la Nube

Consideraciones de Diseño

La solución plantea la creación de un circuito de Capa 2 punto a punto, donde por cada servicio se dispone de una VLAN a la cual se le asigna una subnet /30 para la conexión CPE-Router de Acceso, través de la red Metro Ethernet.

Para este propósito se debe crear una VPN L2 para el transporte del tráfico (VPLS) de todos los clientes del servicio de seguridad en la nube.

El servicio cuenta con el equipamiento SRX650 Juniper, este dispositivo será el encargado de brindar la seguridad a la red LAN del cliente final.

En el presente diseño se considera una solución de activo – contingencia en los equipos de seguridad Juniper para brindar redundancia ante la caída de uno de ellos.

En la figura 3.6 se muestra la arquitectura de acceso a través de la red IP/MPLS del servicio seguridad en la nube.

Se deben tener en cuenta las siguientes características para el diseño e implementación:

Se debe considerar un acceso Metro Ethernet. Para habilitar el presente servicio, se ha considerado configurar VPLS con Bridge Domain 116, este número se usara como solo como referencia para el presente trabajo, asociado a la VLAN ID 116, en la red IP/MPLS, para el transporte del servicio en una VPN L2.

Se debe crear la VLAN 116 en todos los equipos de acceso Metro Ethernet donde se habilitará el servicio. En la puerta de acceso del equipo Metro Ethernet que da acceso al cliente, deberá configurarse QinQ, para el transporte de modo transparente de las VLANs de acceso del cliente. Las VLANs de los CPE de acceso, serán terminadas en el equipo rUTMSeguridad vía una sub-interface con tagging 802.1Q habilitado.

El CPE debe soportar 802.1Q en la interface WAN, el cual debe ser habilitado dentro de una sub-interface. En el equipo rUTMSeguridad se utilizará tagging 802.1Q, la asignación de sub-interfaces se realizara de la manera indicada en el procedimiento de configuración tabla 3.10.

Sobre el equipo rUTMSeguridad, se debe habilitar el enrutamiento estático para tener alcance de la red LAN asignada a los clientes.

Escenario del Servicio de Seguridad en la Nube en la sede del Cliente

Actualmente muchos clientes solicitan diseños de red para asegurar la disponibilidad del servicio contratado. Este tipo de soluciones se logra realizando dos enlaces de acceso a Internet en la sede del cliente, uno funciona como primario y el otro como secundario. Cuando el enlace de conexión primario se pierde, la conexión secundaria se activara de inmediato y actuara como la reserva, sustituyendo la posición de la primaria. La conexión secundaria se actuara como el enlace activo hasta que la conexión primaria se reconecte, para entonces la conexión secundaria regresara a su función de reserva.

Primer escenario – Un Enlace de Internet Seguridad en la Nube

Este escenario será ideal para clientes que solo quieren contar con un solo enlace de Internet y no deseen redundancia o alta disponibilidad en el acceso a la red del operador. Debemos recordar que el servicio de seguridad en la nube se brinda por dos equipos Juniper SRX650 configurados en alta redundancia para asegurar la disponibilidad del servicio de Seguridad en la Nube.

La figura 3.7 muestra el diagrama en bloques de la arquitectura con un solo enlace de acceso a la red del operador para el servicio de Internet.

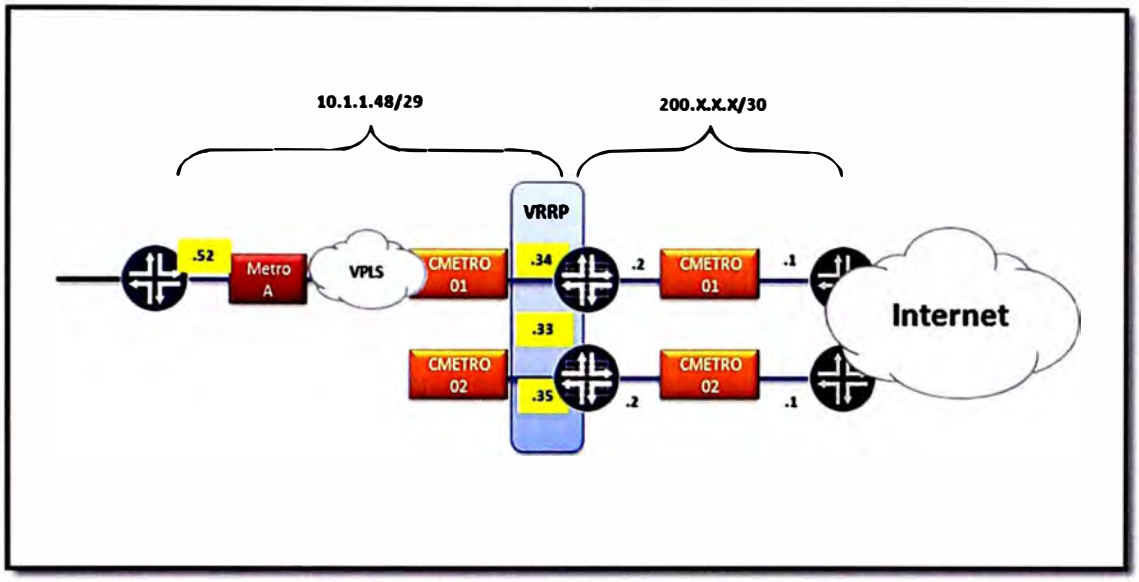


Figura 3.7 Arquitectura de un enlace como acceso a la Red

Segundo Escenario – Dos enlaces de Internet Seguridad en la Nube

En este escenario está diseñado para clientes que deseen tener dos enlaces de acceso a la red del operador para tener una mayor disponibilidad del servicio de Internet Seguridad en la nube.

En la figura 3.8 se muestra el diagrama en bloques de la arquitectura con dos enlaces de acceso a la red del operador para el servicio de Internet.

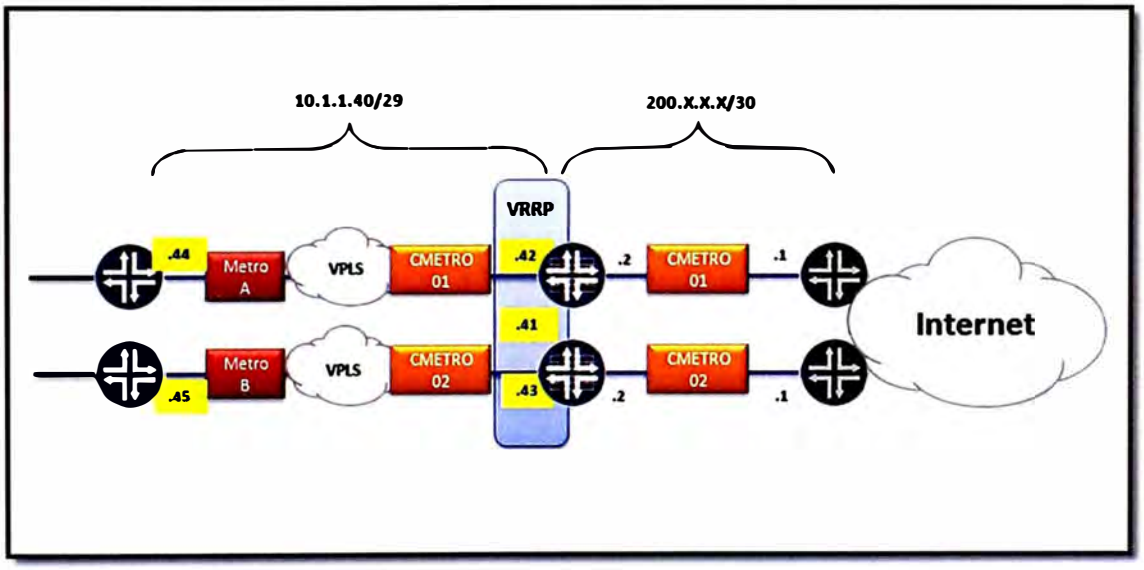


Figura 3.8 Arquitectura de dos enlaces como acceso a la Red

3.2.6 Asignación de Recursos Lógicos

Asignación de VLANs

Para el CPE y PE rUTMSeguridad, se deberá considerar la siguiente asignación de VLANs de acuerdo al equipo Metro Ethernet. Para el presente trabajo se ha considerado

un escenario donde existe ocho equipos de acceso Metro Ethernet en la ciudad de Lima y considerando la siguiente repartición cuatro en el distrito de San Isidro y cuatro en el distrito de Cercado de Lima.

Tabla 3.7 Asignación de VLAN por cada acceso Metro Ethernet

PE	Agregador	Equipo Metro	VLAN CPE
rMPLSSanIsidro	cAGREGADORIsidro	Chinchon	20 - 49
		Saladium	50 - 99
		Aviacion	100 - 149
		Arriola	150 - 199
rMPLSLima	cAGREGADORLima	Cotabambas	200 - 249
		Colonial	250 - 299
		Ingenieria	300 - 349
		Tacna	350 - 399

Asignación de direcciones IP Publicas

El proveedor de Internet debe contar con un guía de operación donde se tenga asignado las direcciones de IP públicas que serán configurados en cada PE de la red del operador. Para el presente trabajo se asignara un grupo de direcciones de acuerdo al escenario de red considerado.

Direcciones IP a usar a nivel LAN

Se asigna un grupo de direcciones IP públicas a ser usadas en la red LAN del cliente, estas direcciones serán usadas por los clientes para publicar servidores correo, web, ftp, etc.

Tabla 3.8 Asignación de direcciones IP públicas por cada PE en la LAN-Cliente

Equipo	Rango
rMPLSSanIsidro	190.223.45.0/24
rMPLSLima	190.223.46.0/24

Direcciones IP a usar a nivel WAN

Se asigna un grupo de direcciones IP públicas a ser usadas en la red WAN es decir estas direcciones se usaran dentro de la red del operador.

Tabla 3.9 Asignación de direcciones IP públicas por cada PE en la WAN-Cliente

Equipo	Rango
rMPLSSanIsidro	190.116.116.0/24
rMPLSLima	190.116.117.0/24

3.2.7 Procedimiento de Configuración

La asignación de sub-interfaces en el puerto Giga Ethernet del equipo rUTMSeguridad se realizara de la forma que indica el cuadro.

Tabla 3.10 Asignación de sub-interfaces en rUTMSeguridad

Servicio	Acceso	ID	Sub Interface	Valor=abcd
Internet	Metro Ethernet	54	GE1/0/0.54abcd	VLAN

De igual forma la asignación de sub-interface en el CPE se debe realizar según la tabla:

Tabla 3.11 Asignación de sub-interfaces en CPE

Servicio	Acceso	ID	Sub Interface	Valor=abcd
Internet	Metro Ethernet	54	FE x/y.116	VLAN

Configuración de CPE

En el CPE se realizará el tagging 802.1Q bajo una sub interface.

```
interface FastEthernetx/y.116
 description Red WAN Internet
 encapsulation dot1Q [VLAN_ID_ACCESO]
 ip address [DIR-IP-CPE/30]
 load-interval 30
 full-duplex
```

Configuración de Equipo Metro Ethernet

El equipo Metro Ethernet delimita la frontera de servicio donde se adiciona el segundo tagging 802.1Q. Es en los equipos de acceso Metro Ethernet donde recibirá una VLAN asignada al cliente según la tabla 3.7 esta VLAN será enmascara en una VLAN del servicio de seguridad en la nube. Esta técnica es conocida como QinQ consiste en hacer un túnel, el cual permite que usando como transporte una única VLAN transportar todas las VLAN de un cliente. Esto permite al operador usar una única VLAN para el transporte del tráfico perteneciente al servicio de seguridad en la nube, permitiendo escalabilidad y seguridad al separar a los clientes en una VLAN independiente.

```
interface GigabitEthernet x/y
 description IDE XXXXX
 switchport access vlan 116
 switchport mode dot1q-tunnel
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
 service-policy input Policer_IN_EJEMPLO
 service-policy output Policer_OUT_EJEMPLO
 logging event link-status
 load-interval 30
```

3.2.8 Disponibilidad del servicio

La disponibilidad del servicio mensual se calculara mediante la siguiente fórmula:

$$\frac{\text{(Tiempo total – Tiempo total no disponible)*100}}{\text{Tiempo total}}$$

Este cálculo no debe ser menor a 99.95% cuando el cliente contrate un solo enlace a Internet. El proveedor debe garantizar este nivel de disponibilidad tomando en cuenta que existe redundancia en los equipos de seguridad y un solo acceso a Internet.

En los casos que el cliente contrate dos enlaces de Internet, la disponibilidad no debe ser menor a 99.99%.

Tiempo total: es la cantidad total de tiempo de cada enlace activo del CLIENTE. Suponiendo que el 100% de disponibilidad es de 60 minutos por hora, 24 horas por día, 7 días a la semana, el servicio pudo haber estado disponible durante un período de un mes

Tiempo total no disponible: es la cantidad total de tiempo no disponible del enlace activo del CLIENTE durante un mes

No se contabilizarán dentro del tiempo de no disponibilidad las interrupciones de servicio que pudieran producirse por causas imputables al CLIENTE o ajenas al proveedor.

3.2.9 Reportes y Atención de Averías

El proveedor deberá describir el *"Sistema de Atención de Averías"*, en el que deberá detallar como mínimo:

1. La organización del Sistema de Atención de Averías
2. Tiempo medio de reparación (MTTR)
3. Recursos humanos dedicados para las solución de averías: personal de turno en el centro de operaciones, y personal asignado a reparación en el campo
4. Procedimiento de atención de fallas
5. Método de emisión de la boleta o código de avería: pro-activo (a iniciativa del proveedor de servicio), o por comunicación del cliente.

Con respecto a los reporte el proveedor deberá suministrar reportes mensuales de averías registradas con detalles de tiempos sin servicio y solución aplicada por cada una de ellas. Adicional a esto deberá suministrar una página web para verificar eventos ocurridos en el equipo de seguridad. Este acceso deberá tener un usuario y clave para cada cliente que contrate el servicio.

El cliente podrá observar en esta página web, los intentos de abrir páginas prohibidas, los virus que se detectaron, los intentos de descarga video o música.

CAPITULO IV
PROCEDIMIENTO DE PRUEBAS DEL SERVICIO DE SEGURIDAD EN LA SUBE

Este capitulo tiene por objetivo realizar el procedimiento de validacion de la topologia a implementar en el servicio de Seguridad en la Nube a nivel de enrutamiento de los enlaces de Internet. Se verificara el escenario II, donde los cliente soliciten dos enlaces de Internet en un escenario de Activo – Contingecia. El procedimiento de pruebas para el escenario I sera un caso particular del escenario II.

4.1 Diagrama Topologico para las pruebas

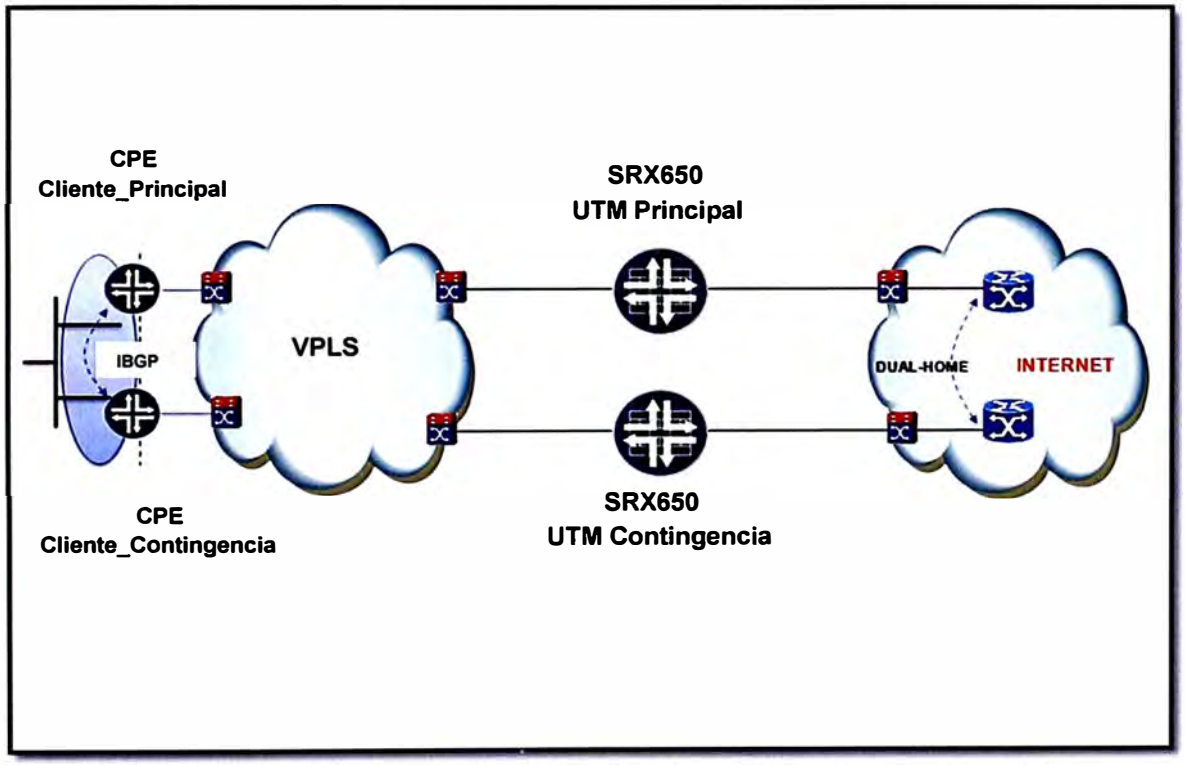


Figura 4.1 Topología Internet seguridad en la nube para pruebas

LAN CLIENTE: 190.223.45.112/28

WAN PRINCIPAL CLIENTE: 10.1.1.4/30 (Enlace Principal)

WAN CONTINGENCIA CLIENTE: 10.1.1.5/30 (Enlace Secundario)

ENLACE UTM-CLIENTE PRINCIPAL: 10.1.1.2/30 (Enlace Principal)

ENLACE UTM-CLIENTE CONTINGENCIA: 10.1.1.3/30 (Enlace Secundario)

ENLACE UTM-INTERNET PRINCIPAL: 190.81.138.246/30 (Enlace Principal)

ENLACE UTM-INTERNET CONTINGENCIA: 190.223.7.242/30 (Enlace Secundario)

4.2 Consideraciones para las pruebas

Para este escenario se usara el CPE Juniper SRX100B. Se utilizará la RED **LAN 190.223.45.112/28,** para la interconexión de equipos router y switch con una IP Flotante 190.223.45.113 para el uso de VRRP. En caso de que el enlace principal caiga el tráfico se direccionará automáticamente por el enlace de contingencia. El enlace de contingencia solo entrara a trabajar cuando el enlace principal se ve afectado. Se considera alta disponibilidad para los equipos UTM (Equipos de Seguridad) en los cuales se aplicará el protocolo VRRP para su respectiva función.

4.3 Protocolo de Pruebas

Se procede a configurar los equipos SRX-100B, las configuraciones serán las rutas y el protocolo no propietario VRRP, definido en el RFC 3768. Una vez terminada la configuración se valida el correcto funcionamiento de los equipos.

De manera similar se debe configurar las rutas y el protocolo VRRP en el equipo de seguridad Juniper SRX650.

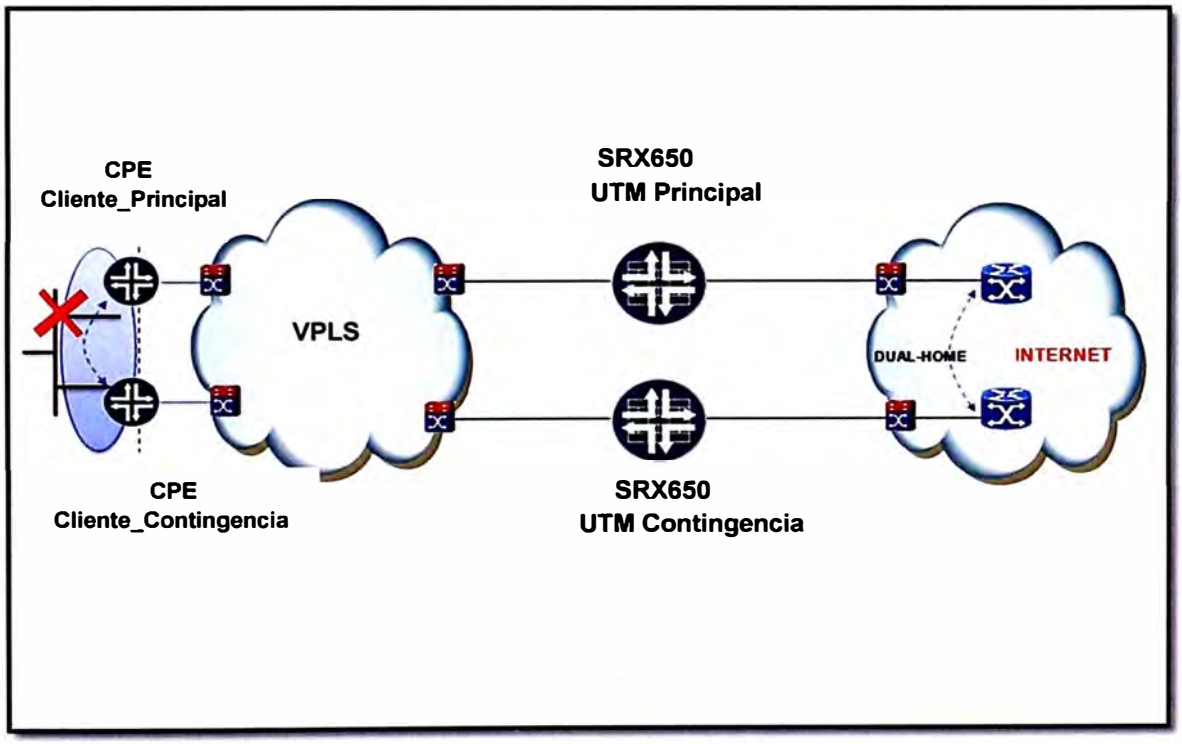


Figura 4.2 Topología simulando la caída de la red LAN en el CPE principal

Terminada la configuración de los equipos se procederá a realizar las pruebas de contingencia.

Primer Paso: Comenzamos simulando la caída de la interface LAN del enlace principal del cliente, mediante la desconexión del cable conectado al switch en la LAN:

Previo a la desconexión del cable, se debe realizar una prueba de PING EXTENDIDO con fuente la red LAN del cliente y con destino a www.google.com o cualquier otro destino en Internet. Se observara que todos los paquetes llegan pero uno se pierde por el

retardo en la conmutación al enlace de contingencia. En la figura 4.3 se muestra lo descrito anteriormente.

```
Haciendo ping a www.google.com [74.125.235.20] con 32 bytes de datos:

Respuesta desde 74.125.235.20: bytes =32 tiempo=321 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=314 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=316 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=319 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=318 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=322 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=313 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Tiempo de espera agotado para esta solicitud.
Respuesta desde 74.125.235.20: bytes =32 tiempo=316 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=320 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=321 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=319 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=317 TTL=48
```

Figura 4.3 Pruebas de PING EXTENDIDO desde la red LAN

También se debe considerar realizar una prueba de traza a Internet, con destino www.google.com desde la red LAN.

Se debe verificar el estado VRRP del router principal, el cual debería de estar inactivo. Se muestra en la figura 4.4 lo siguiente:

```
CLIENTE_PRINCIPAL# run show  vrrp
Interface        state     Group   VR state   VR Mode   Timer   Type   Address
fe-0/0/1.0       down      1       init       Active    N       lcl    190.223.45.114
                                                                 vip    190.223.45.113
```

Figura 4.4 Verificación de estado VRRP en CPE Principal

Inmediatamente se debe verificar el estado VRRP del enrutador de contingencia, en este equipo debería estar activo.

```
CLIENTE_CONTINGENCIA# run show  vrrp
Interface        state     Group   VR state   VR Mode   Timer   Type   Address
fe-0/0/1.0       up        1       master     Active    A       lcl    190.223.45.115
                                                                 vip    190.223.45.113
```

Figura 4.5 Verificación de estado VRRP en CPE Contingencia

Una vez validado el funcionamiento de la contingencia, se procede a realizar la reconexión del enlace principal. De igual manera que el primer paso se debe realizar una prueba de ping hacia el destino www.google.com y se obtendrá lo siguiente, según se muestra en la figura 4.6.

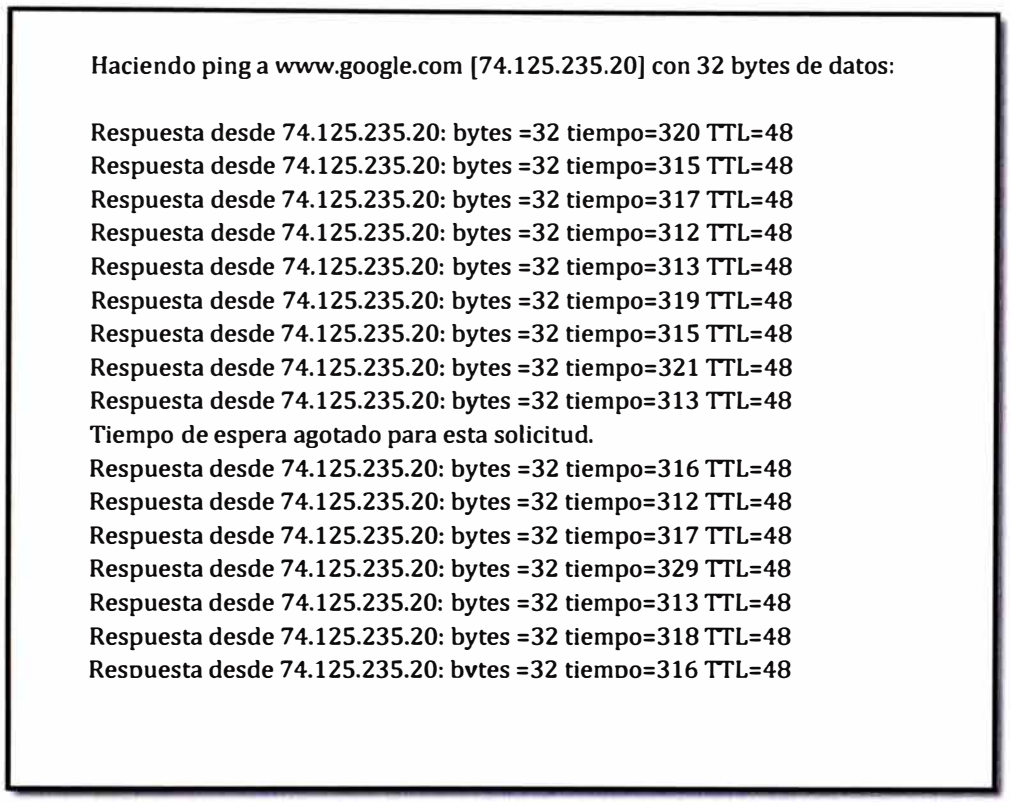
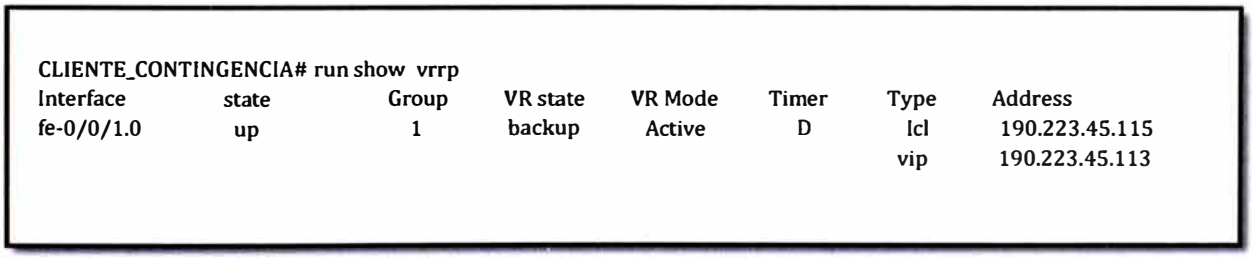


Figura 4.6 Pruebas de PING EXTENDIDO desde la red LAN

De igual forma que se verifico el estado VRRP en el primer caso, ahora se debe verificar estos estados, en la figura 4.7 se muestra el estado VRRP del enrutador de contingencia.

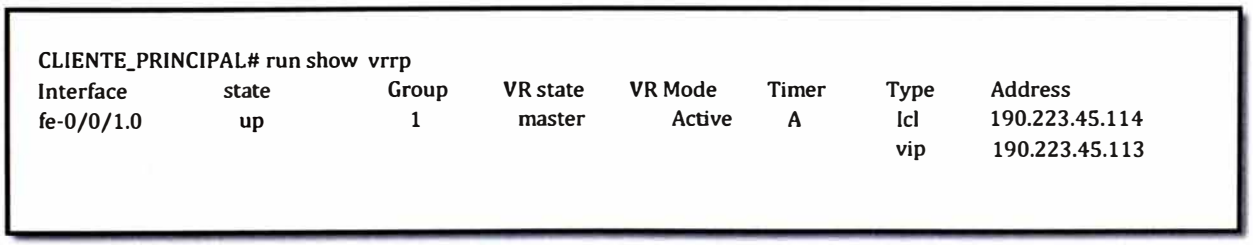


CLIENTE_CONTINGENCIA# run show vrrp

Interface	state	Group	VR state	VR Mode	Timer	Type	Address
fe-0/0/1.0	up	1	backup	Active	D	lcl	190.223.45.115
						vip	190.223.45.113

Figura 4.7 Verificación de estado VRRP en CPE contingencia

Ahora debemos verificar el estado VRRP del enrutador principal, en la figura 4.8 se muestra el siguiente resultado:



CLIENTE_PRINCIPAL# run show vrrp

Interface	state	Group	VR state	VR Mode	Timer	Type	Address
fe-0/0/1.0	up	1	master	Active	A	lcl	190.223.45.114
						vip	190.223.45.113

Figura 4.8 Verificacion de estado VRRP en CPE principal

Segundo Paso: Se procederá a simular la caída de la interface WAN del enlace principal del cliente, mediante la desconexión del cable conectado a la red VPLS.

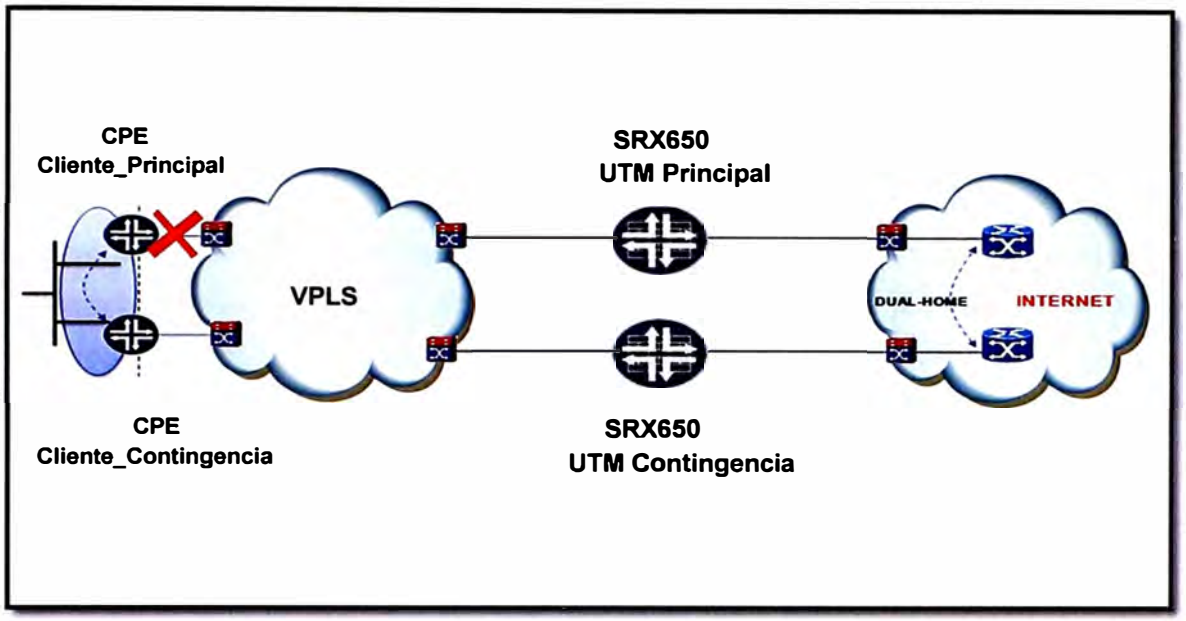


Figura 4.9 Topología simulando la caída de la red WAN en el CPE principal

Se realiza pruebas de PING al destino www.google.com de manera similar al primer paso se verificaran los estados VRRP en cada enrutador.

```
Haciendo ping a www.google.com [74.125.235.20] con 32 bytes de datos:

Respuesta desde 74.125.235.20: bytes =32 tiempo=320 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=317 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=313 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Tiempo de espera agotado para esta solicitud.
Respuesta desde 74.125.235.20: bytes =32 tiempo=316 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=317 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=329 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=321 TTL=48
```

Figura 4.10 Pruebas de PING EXTENDIDO desde la red LAN

```
CLIENTE_PRINCIPAL# run show  vrrp
Interface        state       Group     VR state    VR Mode     Timer    Type     Address
fe-0/0/1.0       up          1           backup      Active      D        lcl      190.223.45.114
                                                                          vip      190.223.45.113
```

Figura 4.11 Verificacion de estado VRRP en CPE principal

```
CLIENTE_CONTINGENCIA# run show vrrp
Interface        state    Group   VR state   VR Mode   Timer   Type   Address
fe-0/0/1.0       up       1       master     Active    D       lcl    190.223.45.115
                                                                vip    190.223.45.113
```

Figura 4.12 Verificacion de estado VRRP en CPE contingencia

Una vez validado el funcionamiento de la contingencia, se procede a realizar la reconexión del enlace principal, obteniendo resultados similares al primer paso. Es decir se verificara el paso a inactivo del enlace contingencia y el paso a activo del enlace principal. En una prueba de PING el resultado será similar a la figura 4.6.

Tercer Paso: Como siguiente prueba, se simulara la caída de la interface del equipo UTM correspondiente al enlace UTM-Cliente Principal, este caso simulara una caída física local en el equipo UTM y una caída lógica para el enrutador principal en la sede del cliente. Esta prueba se realizara desconectando el cable que en el equipo UTM Principal a continuación se verificara que el equipo UTM contingencia asume la carga de tráfico del servicio de seguridad en la nube.

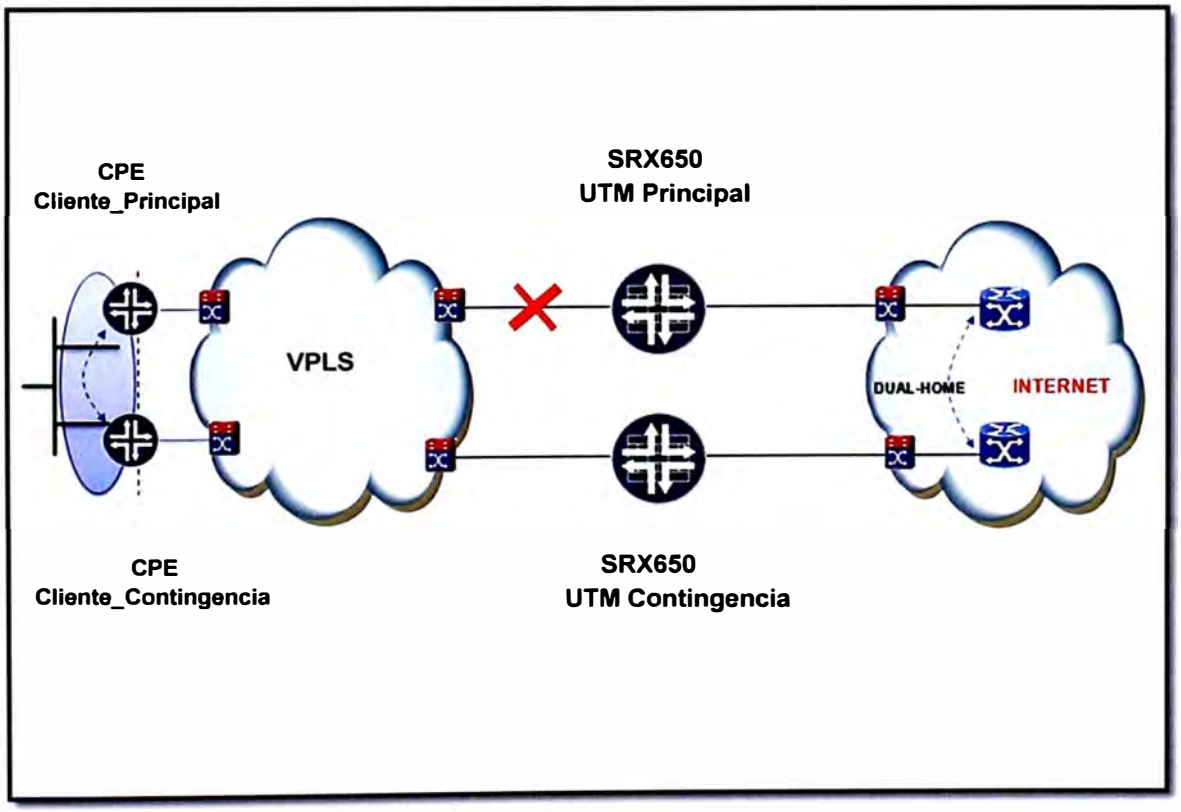


Figura 4.13 Topología simulando la caída de la interface con el CPE principal

Se procede a realizar pruebas de PING EXTENDIDO hacia el destino www.google.com, usando como fuente la red LAN del cliente. En la figura 4.14 se muestra los resultados que se deberían obtener:

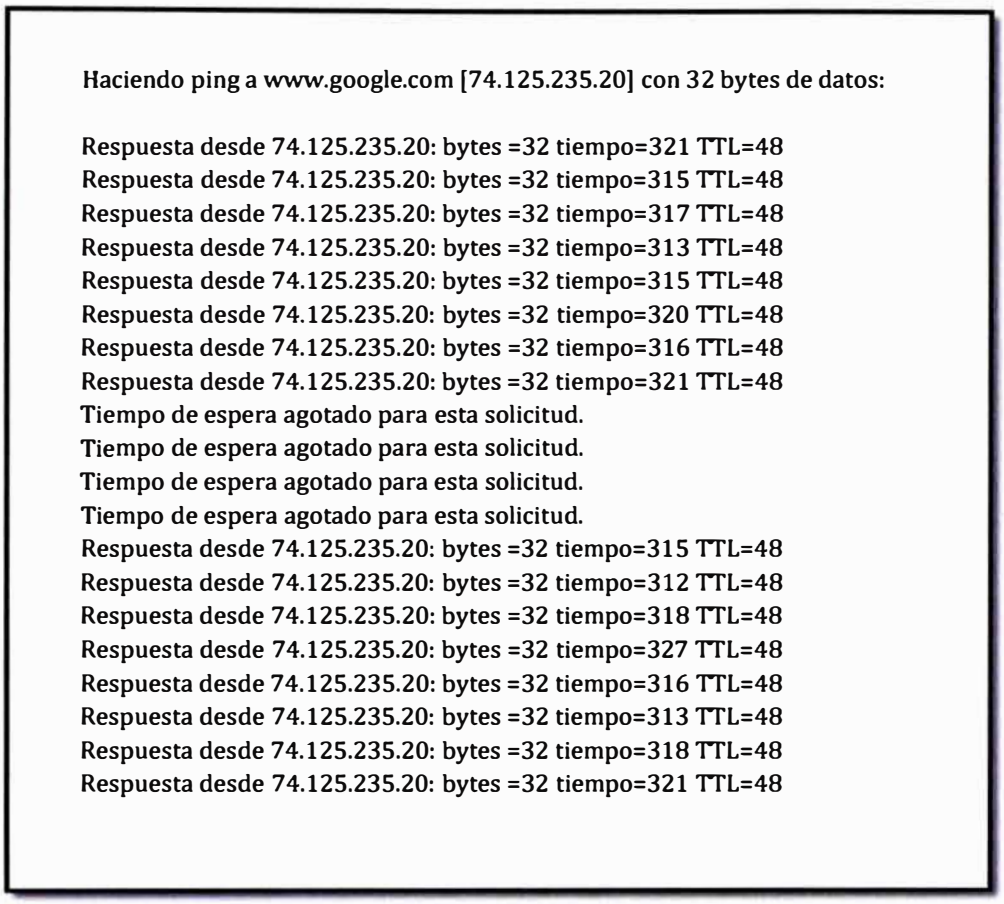


Figura 4.14 Pruebas de PING EXTENDIDO desde la red LAN

El resultado muestra una mayor pérdida de paquetes que en las pruebas de caída del enrutador ubicado en el cliente, esto es por los servicios de seguridad que se encuentran configurados en el equipo de seguridad Juniper y este equipo en contingencia requiere de un tiempo para iniciar el proceso de análisis de los paquetes de datos. Una vez terminado este proceso, todos los servicios de seguridad continúan funcionando.

Una vez validado el funcionamiento del enlace de contingencia, se procede a realizar la reconexión del enlace principal. Esta etapa el equipo de seguridad principal retomara sus funciones y el equipo de seguridad contingencia pasa a un estado inactivo. Se verifica el estado VRRP para el equipo UTM Principal, observándose lo mostrado en la figura 4.15.

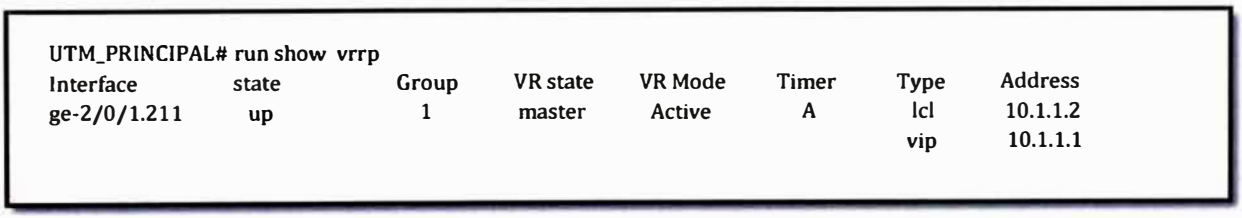


Figura 4.15 Verificación de estado VRRP en UTM principal

Cuarto Paso: Como siguiente prueba se simulara la caída de la interface del equipo UTM correspondiente al enlace UTM-INTERNET PRINCIPAL, este caso simularía una caída física local para el equipo UTM y una caída lógica para el enrutador principal en la sede

del cliente. En la figura 4.16 se muestra la caída del enlace que usa el rISPSeguridad principal para salir a Internet.

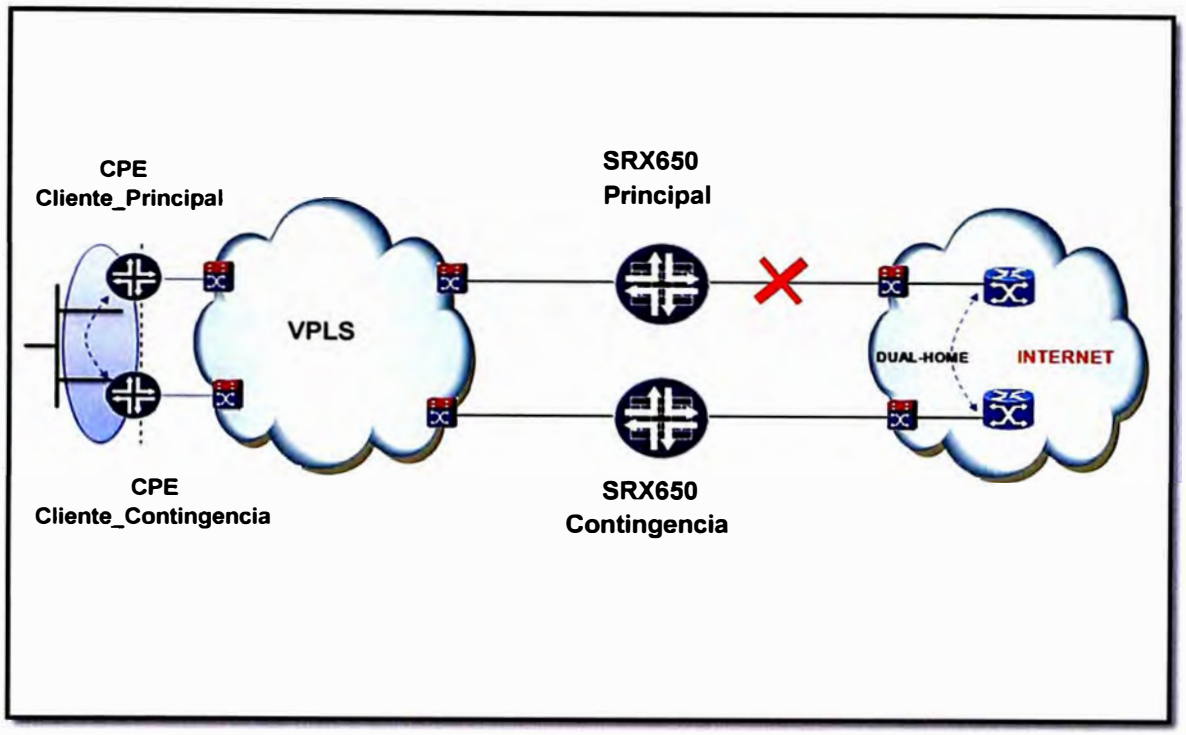


Figura 4.16 Topología simulando la caída de la interface con el Internet Principal

Se realizan las pruebas de PING EXTENDIDO desde una PC en la LAN del cliente con destino a www.google.com, se muestran los resultados en la figura 4.17.

```
Haciendo ping a www.google.com [74.125.235.20] con 32 bytes de datos:

Respuesta desde 74.125.235.20: bytes =32 tiempo=321 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=317 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=313 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=320 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=316 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=321 TTL=48
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=318 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=327 TTL=48
```

Figura 4.17 Pruebas de PING EXTENDIDO desde la red LAN

Ahora debemos verificar el estado VRRP del enrutador principal, en la figura 4.18 se muestra el siguiente resultado:

```
UTM_CONTINGENCIA# run show vrrp
Interface        state    Group   VR state   VR Mode   Timer   Type   Address
ge-2/0/1.211     up       1       master     Active    A       lcl    10.1.1.3
                                                                vip    10.1.1.1
```

Figura 4.18 Verificacion de estado VRRP en UTM contingencia

Una vez validado el funcionamiento del enlace de contingencia, se procede a realizar la reconexión del enlace principal, en la figura 4.19 se muestra que no se pierde ningún paquete de datos en este proceso:

```
Haciendo ping a www.google.com [74.125.235.20] con 32 bytes de datos:

Respuesta desde 74.125.235.20: bytes =32 tiempo=321 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=314 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=316 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=311 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=313 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=314 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=317 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=319 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=312 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=313 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=316 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=315 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=314 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=310 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=317 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=320 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=313 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=316 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=311 TTL=48
Respuesta desde 74.125.235.20: bytes =32 tiempo=317 TTL=48
```

Figura 4.19 Pruebas de PING EXTENDIDO desde la red LAN

También se verifica el estado VRRP en los equipos de seguridad Juniper. En la figura 4.20 se muestra el resultado:

```
UTM_CONTINGENCIA# run show  vrrp
Interface          state       Group    VR state    VR Mode    Timer    Type    Address
ge-2/0/1.211       up          1        backup      Active     D        lcl     10.1.1.3
                                                                         vip     10.1.1.1
```

Figura 4.20 Verificación de estado VRRP en UTM contingencia

En la siguiente figura 4.21 se muestra el resultado del estado VRRP del equipo UTM-Principal.

```
UTM_PRINCIPAL# run show  vrrp
Interface          state       Group    VR state    VR Mode    Timer    Type    Address
ge-2/0/1.211       up          1        master      Active     A        lcl     10.1.1.2
                                                                         vip     10.1.1.1
```

Figura 4.21 Verificación de estado VRRP en UTM principal

4.4 Validación de los servicios de Seguridad

Las pruebas realizadas para la validación del servicio, se dieron bajo el esquema ACTIVO-CONTINGENCIA de los equipos de seguridad, por lo que se valida el funcionamiento del servicio ante alguna caída del enlace principal.

Ahora se procederá a la validación de los servicios de seguridad del equipo principal, para esta prueba no se simulara la caída del enlaces principal.

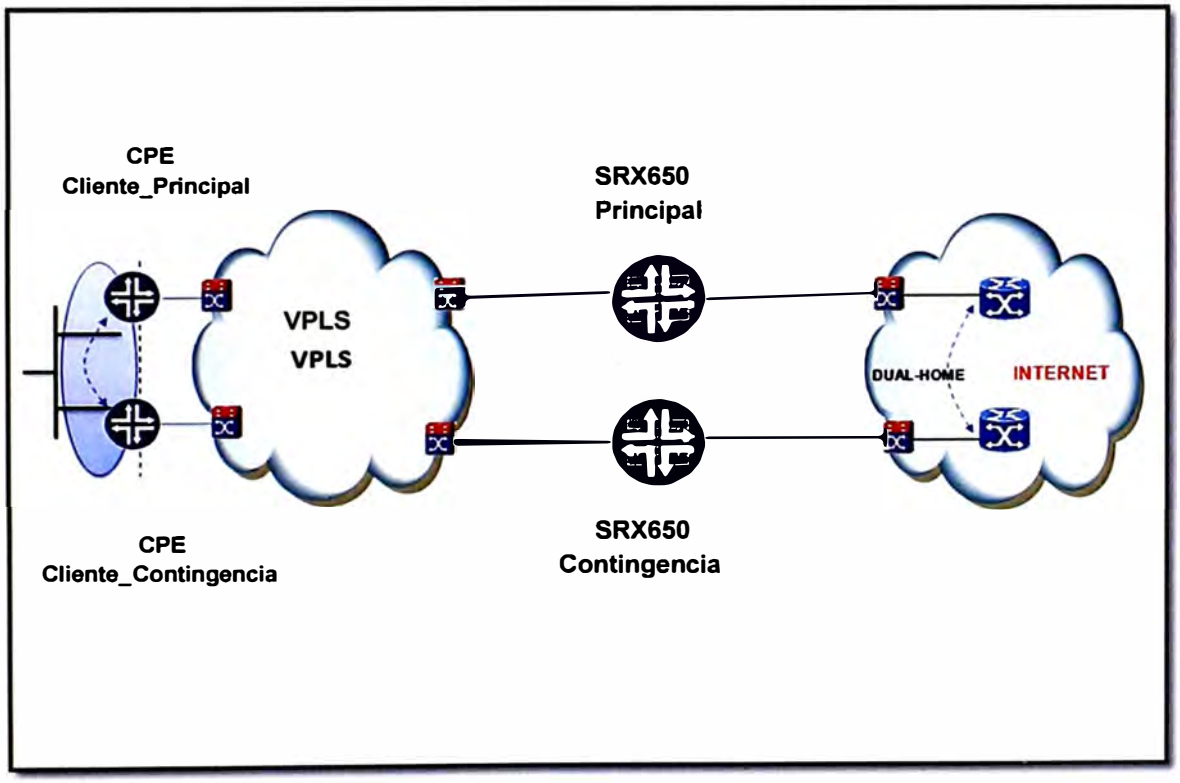


Figura 4.22 Topología del servicio de Internet Seguridad en la Nube

Se valida el escenario ante un correcto funcionamiento del UTM-PRINCIPAL. Para el escenario mostrado usaremos como programa de navegación de Internet el software Internet Explorer.

Se realiza una prueba realizando una consulta a la página www.google.com.pe. Esta prueba se puede realizar con cualquier otra página web, el objetivo es verificar el servicio de Internet.

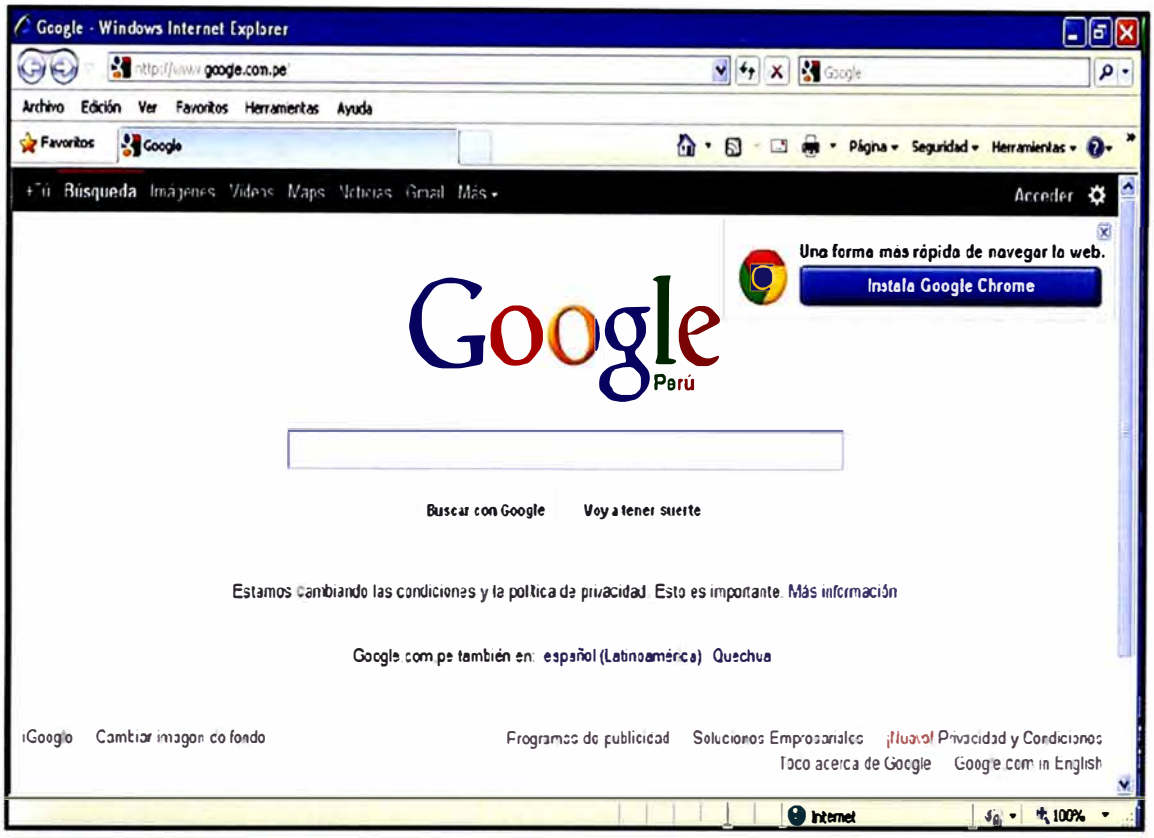


Figura 4.23 Verificación del servicio de Internet

Validación del servicio Antivirus

Para realizar esta validación se usara el test de prueba EICAR es una prueba desarrollada por el Instituto Europeo para la Investigación de Antivirus Informáticos y para probar la respuesta de los programas antivirus en el equipo. La razón detrás de esto es permitir a las personas, empresas y programadores de antivirus, probar su software sin tener que utilizar un verdadero virus informático que pudiera causar daño real al no responder el antivirus correctamente.

El Instituto Europeo para la Investigación de los Antivirus Informáticos, compara el uso de un virus vivo para probar el software antivirus como el establecimiento de un fuego en un cubo de basura para poner a prueba una alarma de incendio, y promueve el archivo de prueba EICAR como una alternativa segura.

La prueba EICAR consiste en un archivo que sirve para comprobar hasta dónde analizan los programas antivirus, o si estos están en funcionamiento. La ventaja que tiene sobre

otras comprobaciones es que el equipo queda libre de riesgos. Se trata de un inofensivo archivo de texto.

En la dirección http://www.rexswain.com/eicar.html se puede descargar los archivos para realizar la prueba segura de test de antivirus. Este sistema es usado por muchas personas dedicadas a labores de TI.

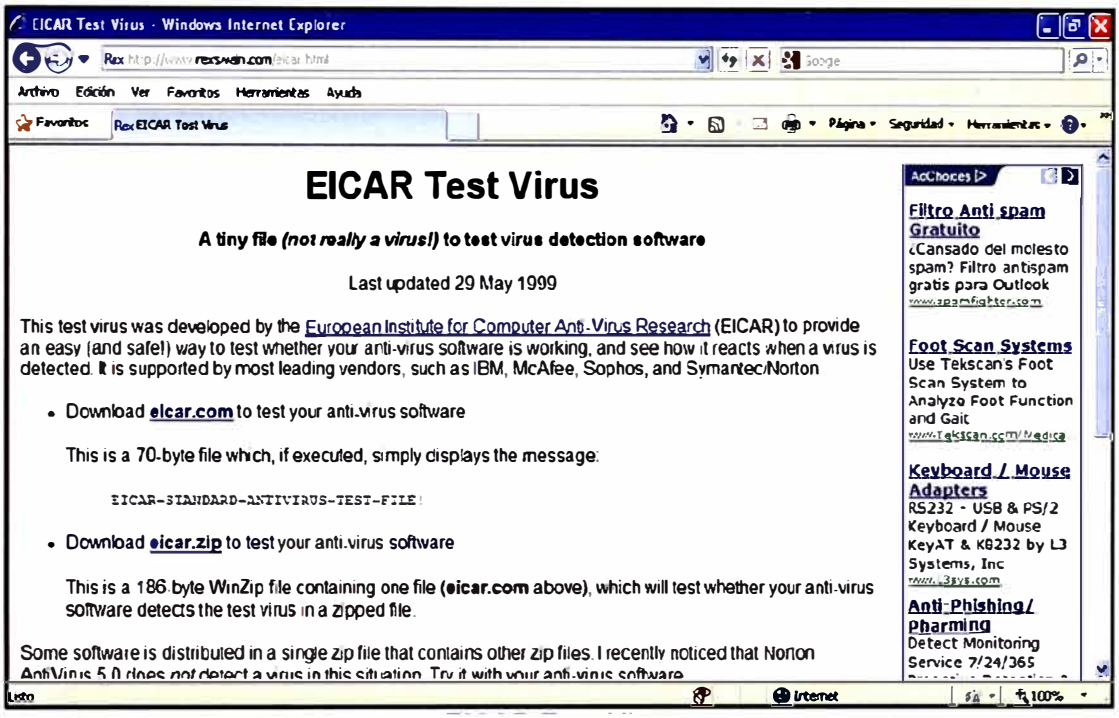


Figura 4.24 Prueba con EICAR Test Virus

Luego se inicia la prueba descargando el archivo, inmediatamente el equipo de seguridad debe de enviar un mensaje de advertencia.

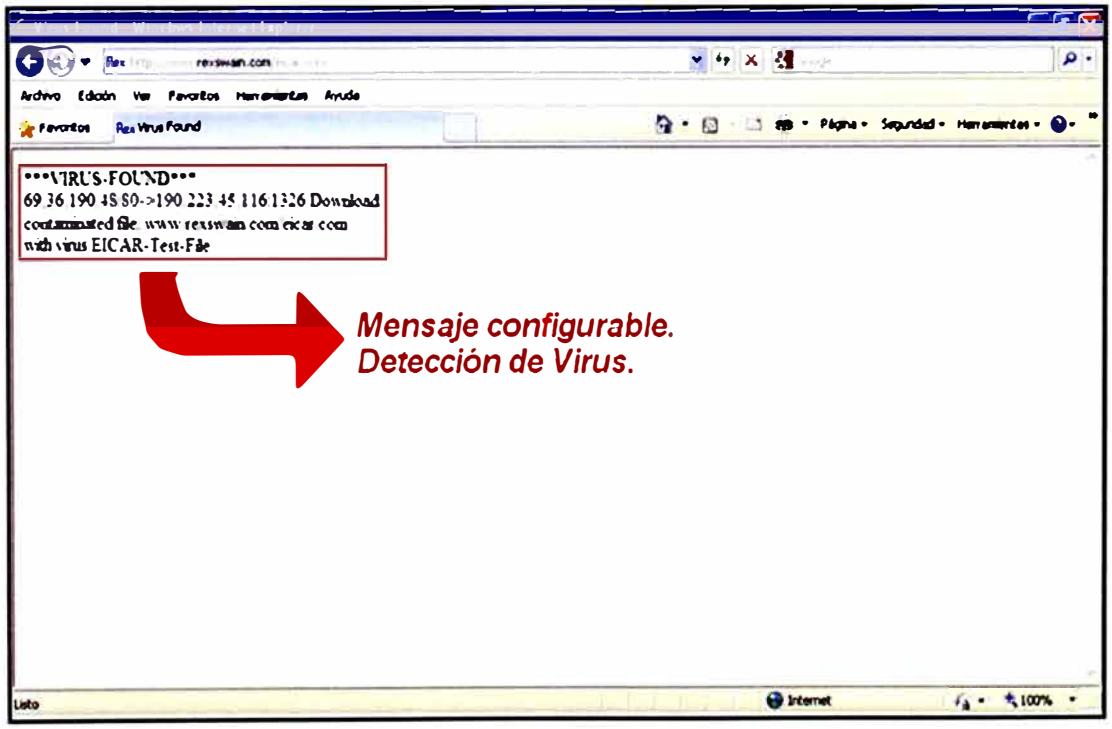


Figura 4.25 Verificación del servicio de Antivirus del UTM Juniper

Validación del Servicio Filtro de Contenidos

Se realiza una prueba intentando descargar un archivo de cualquier sitio web. Esta prueba se realizara intentando descargar el programa PUTTY.

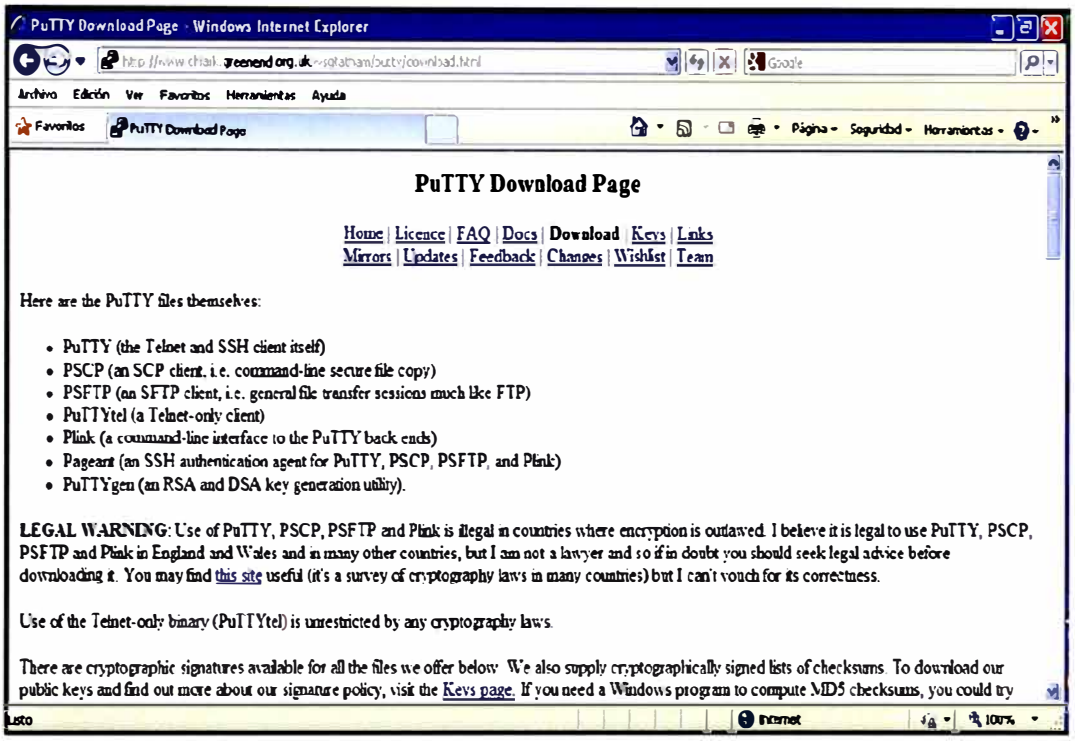


Figura 4.26 Prueba de descarga de software

El equipo de seguridad Juniper detectara la descarga de aplicación y aplicara la política de seguridad prohibiendo el tráfico. En la figura 4.27 se muestra el resultado al intentar realizar la descarga de un software.

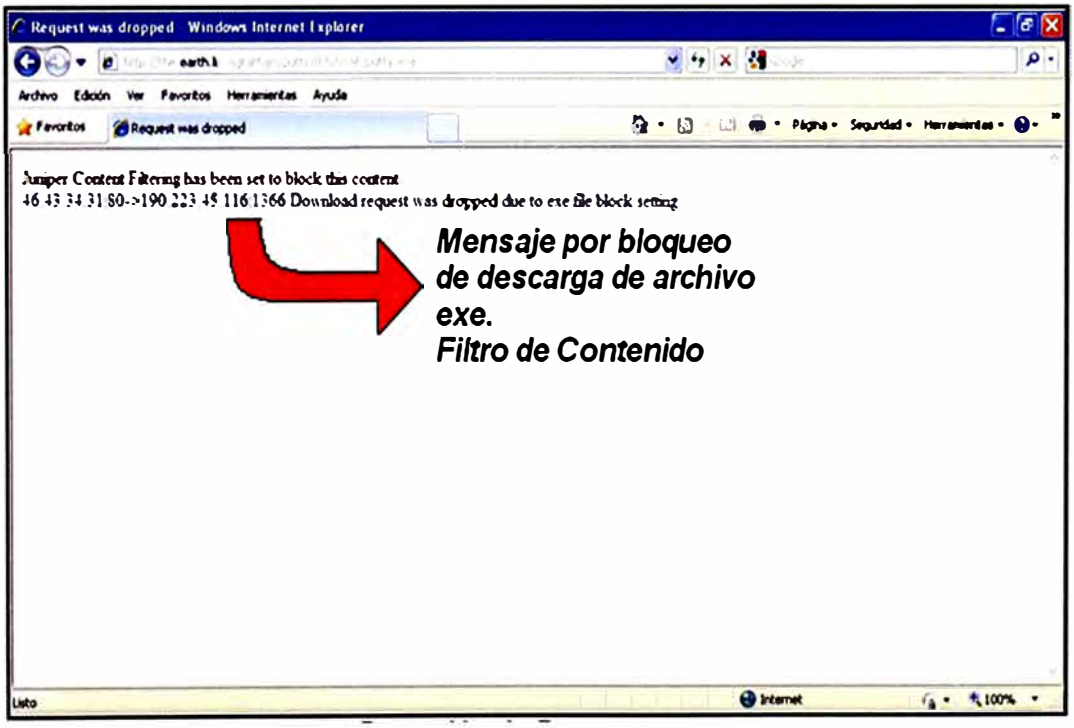


Figura 4.27 Verificación del servicio de filtro de contenidos

Validación de Servicio Filtro Web

El servicio permite realizar el filtro para permitir o negar determinadas páginas web. En la figura 4.28 se muestra la apertura de la página de Facebook.

Figura 4.28 Prueba de navegación de una página permitida

En la siguiente figura 4.29 se muestra la negación a la página web www.sexo.com. Esta es una página bloqueada por el equipo de seguridad.

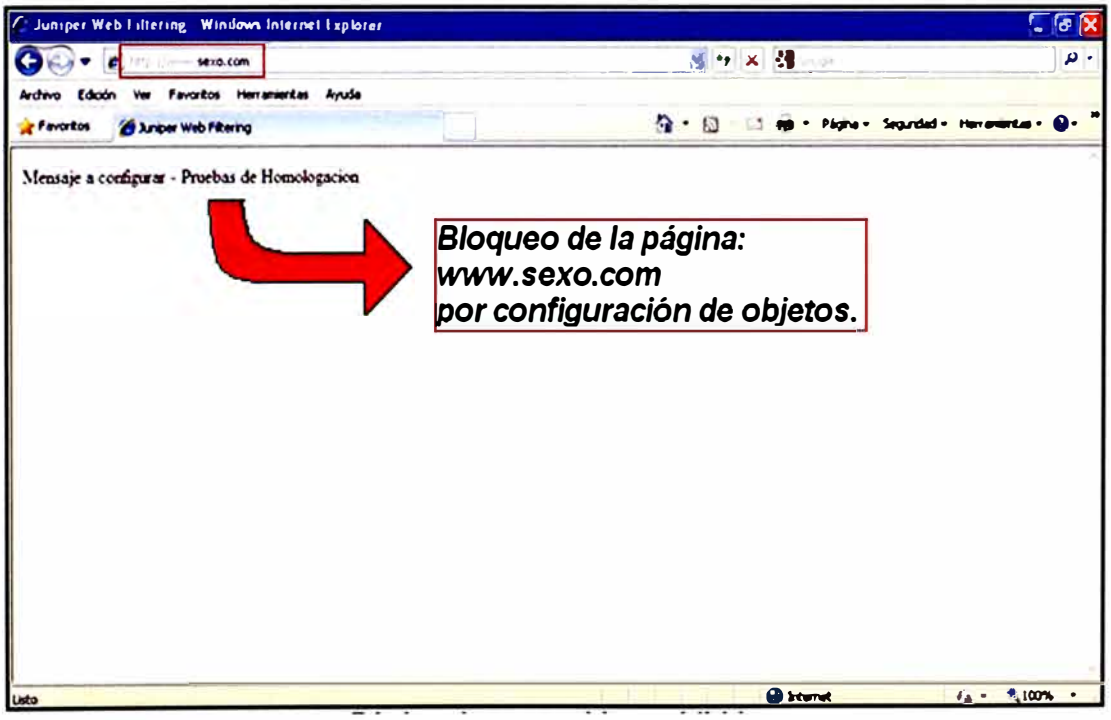


Figura 4.29 Verificación del servicio filtro WEB

CONCLUSIONES Y RECOMENDACIONES

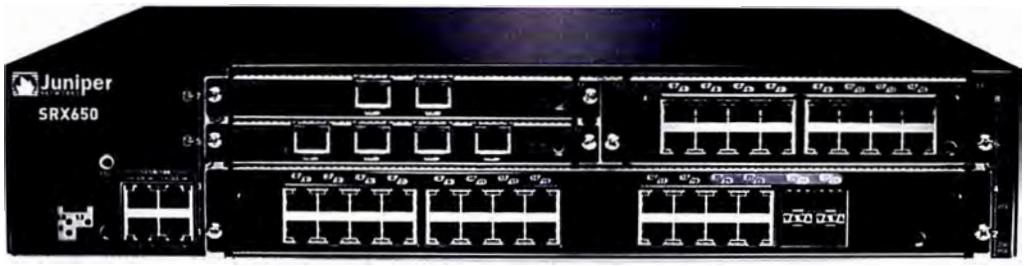
1. Se considera implementar el servicio de Seguridad en la Nube sobre una plataforma MPLS-VPLS, donde se permita configurar sobre una única VLAN el servicio de seguridad en la nube y la VLAN de cada cliente será encapsulado sobre la VLAN del servicio. Esto permitirá el ahorro en la asignación de recursos lógicos como la asignación de una VLAN individual por cliente.
2. Para el diseño de la solución Seguridad en la Nube se debe considerar dos equipos de seguridad en activo – contingencia, con esto aseguramos la disponibilidad del servicio a nivel de la red. Suponiendo que uno falle el segundo equipo asumiría la función del equipo principal brindando continuidad al servicio de forma transparente al usuario.
3. Los equipos de seguridad que se deberán considerar en la solución de Seguridad en la Nube deben tener la capacidad de trabajar en la capa 3 del modelo OSI, es decir deben soportan protocolos de enrutamiento. Estas funcionalidades de enrutamiento permitirán realizar configuraciones de VRRP y crear las rutas para la salida a Internet con el enrutador de borde en la red del operador de Internet.
4. Para el servicio de Internet que se instalara en la sede del cliente se podrá considerar un escenario en el cual se brinde dos enlaces de Internet para asegurar la disponibilidad del servicio. Esto se lograra configurando los enrutadores (CPE) en un escenario de Activo – Contingencia.
5. El CLIENTE deberá solicitar como la disponibilidad del servicio, reportes y accesos web para verificar el buen funcionamiento del servicio.
6 Para el proceso de diseño del servicio de seguridad en la nube se recomienda que el operador debe contar con una red IP/MPLS. Por otra parte, el operador debe contar con mínimo dos salidas a Internet a través de operadores TIER 1. Las salidas a Internet deben estar ubicadas en dos lugares distintos, estos requisitos son necesarios para asegurar la disponibilidad del servicio de Internet.
7. Además del punto anterior debemos asegurar la disponibilidad del servicio de seguridad en la nube, por este motivo en la etapa de diseño se debe considerar dos equipos de seguridad configurados con un protocolo de redundancia. El protocolo de redundancia no debe ser propietario, es decir no debe pertenecer a una marca.

8. Los equipos recomendados para implementar el servicio de seguridad en la nube son los equipos Juniper serie SRX650, estos equipos tienen funcionalidades de enrutadores y firewall. Estas características ofrecen la posibilidad de configurar un protocolo de redundancia y las funcionalidades de UTM.
9. En la etapa de implementación se debe seguir el procedimiento de pruebas para asegurar el correcto funcionamiento del servicio antes de la entrega al cliente.
10. Se debe asegurar un nivel de servicio con el cliente. Los niveles de servicio pueden cubrir cualquier escenario desde una simple monitorización, creación de informes y notificación de amenazas, hasta la respuesta manual desde el SOC del operador para cambios en la configuración o actualizaciones.

ANEXO A
JUNIPER – SERIE SRX650

Es esta sección se muestra el equipo Juniper SRX650. Juniper Networks SRX Series Services Gateways son equipos de seguridad que proveen capacidades de conexión, seguridad y administración, estas sedes pueden ser de pocos o cientos de usuarios. Mediante la consolidación de conmutación rápidas y de alta disponibilidad, seguridad, enrutamiento y capacidades de aplicaciones en un solo dispositivo, las empresas pueden ofrecer económicamente nuevos servicios, conectividad segura, y una experiencia de usuario satisfactoria.

Toda la serie SRX incluye productos escalables en oficinas remotas, oficinas principales, campus y data center. Juniper Network Junos OS el sistema operativo probado que ofrece consistencia sin igual, un mejor rendimiento con los servicios y la protección de infraestructura superior a un costo total de propiedad más bajo.



SRX650

Especiaciones Técnicas

Protocols

IPv4, IPv6, ISO Connectionless Network Service (CLNS)

Routing and Multicast

- Static routes
- RIPv2 +v1
- OSPF/OSPFv3
- BGP
- BGP Router Reflector2
- IS-IS
- Multicast (Internet Group Management Protocol (IGMPv1/2/3), PIM-SM/DM/SSM, Session Description Protocol (SDP), Distance Vector Multicast Routing Protocol (DVMRP), source-specific, Multicast inside IPsec tunnel), MSDP
- MPLS (RSVP, LDP, Circuit Cross-connect (CCC), Translational Cross-connect (TCC), Layer 2 VPN (VPLS), Layer 3 VPN, VPLS, NGMVPN)

IP Address Management

• Static

• DHCP, PPPoE client

• Internal DHCP server, DHCP Relay

Address Translation

• Source NAT with Port Address Translation (PAT)

• Static NAT

• Destination NAT with PAT

• Persistent NAT, NAT64

L2 Switching

• 802.1D, RSTP, MSTP, 802.3ad (LACP)

• 802.1x, LLDP, 802.1ad (Q-in-Q), IGMP Snooping

• Layer 2 switching with high availability

Traffic Management Quality of Service (QoS)

• 802.1p, DSCP, EXP

• Marking, policing, and shaping

• Class-based queuing with prioritization

• Weighted random early detection (WRED)

• Queuing based on VLAN, data-link connection identifier (DLCI), interface, bundles, or multi-field (MF) filters

• Guaranteed bandwidth

• Maximum bandwidth

• Ingress traffic policing

• Priority-bandwidth utilization

• DiffServ marking

• Virtual channels

Security

Firewall

• Firewall, zones, screens, policies

• Stateful firewall, stateless filters

• Network attack detection

• Screens denial of service (DoS) and provides distributed denial of service (DDoS) protection (anomaly-based)

• Prevent replay attack; Anti-Replay

• Unified Access Control

-- TCP reassembly for fragmented packet protection

-- Brute force attack mitigation

-- SYN cookie protection

-- Zone-based IP spoofing

-- Malformed packet protection

UTM1

• Intrusion Prevention System (IPS)

-- Protocol anomaly detection

-- Stateful protocol signatures

-- Intrusion prevention system (IPS) attack pattern obfuscation

-- User role-based policies

• Customer signatures creation

• Daily and emergency updates

• AppSecure

-- AppTrack (application visibility and tracking)

-- AppFW (policy enforcement by application name)

-- Custom signatures

-- Dynamic signature updates

-- User-based application policy enforcement

• Antivirus

-- Express AV (stream-based AV, not available on SRX100 and SRX110)

-- File-based antivirus

›› Signature database

›› Protocols scanned: POP3, HTTP, SMTP, IMAP, FTP

›› Antispyware

›› Anti-adware

›› Antikeylogger

-- Cloud-based antivirus

• Antispam

• Integrated enhanced Web filtering

-- Category granularity (90+ categories)

-- Real time threat score

• Redirect Web filtering

• Content Security Accelerator in SRX210 high memory, SRX220, SRX240, SRX550, and SRX6501

• ExpressAV option in SRX210 high memory, SRX220 high memory, SRX240, SRX550, and SRX6501

• Content filtering

-- Based on MIME type, file extension, and protocol commands

High Availability

• VRRP

• JSRP

• Stateful failover and dual box clustering

• SRX550/SRX650:

-- Redundant power (optional)

-- GPIM hot swap

-- Future internal failover and SRE hot swap (OIR) on SRX650

• Backup link via 3G/4G LTE wireless or other WAN

• Active/active—L3 mode

• Active/passive—L3 mode

Administration

• Juniper Networks Network and Security Manager support (NSM)

• Juniper Networks Junos Space Security Director support

• Juniper Networks STRM Series Security Threat Response Managers support

• Juniper Networks Advanced Insight Solutions support

• External administrator database (RADIUS, LDAP, SecureID)

• Auto-configuration

• Configuration rollback

• Rescue configuration with button

• Auto-record for diagnostics

• Software upgrades (USB upgrade option)

• Juniper Networks Junos® Web

• Command-line interface

ANEXO B
GLOSARIO DE TERMINOS

LAN (Local Area Network): Una red de área local, red local es la interconexión de uno o varios dispositivos en un área cercana.

WAN (Wide Area Network): Es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales, llamadas LAN, por lo que sus miembros no están todos en una misma ubicación física.

DHCP (Dynamic Host Configuration Protocol): Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

VPN (Virtual Private Network): Una tecnología de red que permite extender la red local sobre una red pública.

ISP (Internet Service Provider): Siglas para indicar al proveedor del servicio de Internet.

PC (Personal Computer): Computadora de escritorio.

OSI (Open System Interconnection): Es el modelo que hizo la Organización Internacional para la Estandarización (ISO) para estandarizar la interconexión de sistemas abiertos.

MPLS (Multi Protocol Label Switching): Es una tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. La conmutación de paquetes se realiza por etiquetas esto permite mayor velocidad en el reenvió de tráfico.

VPLS (Virtual Private LAN Service): Es una forma de proporcionar Ethernet multipunto a multipunto basado en la comunicación sobre redes IP / MPLS.

RSVP (Resource Reservation Protocol): Es un protocolo de la capa de transporte diseñado para reservar recursos de una red bajo la arquitectura de servicios integrados (IntServ).

OSPF (Open Shortest Path First): Es un protocolo de enrutamiento desarrollado para Internet Protocol (IP).

ATM (Asynchronous Transfer Mode): Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Frame Relay: Es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual.

Ethernet: Es un estándar de redes de área local para computadores con acceso al medio por contienda (CSMA/CD).

TI: Tecnologías de la Información, es aquella herramienta y métodos empleados para recabar, retener, manipular o distribuir información.

VRRP: Virtual Router Redundancy Protocol, es un protocolo de redundancia no propietario definido en el RFC 3768 diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a la misma red.

BIBLIOGRAFÍA

[1]. Alberto Ureaña, Annie Ferrari, David Blanco, Elena Valdecasa "Cloud Computing Retos y Oportunidades".
http://www.ontsi.red.es/ontsi/sites/default/files/1_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf (fecha de acceso: 06/07/2013).

[2]. Jesús Enrique Vázquez Reina "Cloud Computing".
http://campusv.uaem.mx/cicos/imagenes/memorias/7mocicos2009/Articulos/p11%20%20Cloud%20Computing.pdf (fecha de acceso: 20/07/2013).

[3]. Ivan Pepelnjak, Jim Guichard "MPLS and VPN Architectures".

[4]. Cisco Systems Inc, "Virtual Private LAN Service".
http://www.cisco.com/application/pdf/en/us/guest/tech/tk891/c1482/ccmigration_09186a00801ed3ea.pdf (fecha de acceso: 03/08/13).

[5]. Juniper Networks, "Especificaciones de SRX650".
http://www.juniper.net/es/es/products-services/security/srx-series/srx650/ (fecha de acceso: 03/08/13)

[6]. "Guía para la seguridad de aéreas criticas de atención en cloud computing".
https://cloudsecurityalliance.org/ (fecha de acceso: 26/07/13).

[7]. Thomas Erl, Ricardo Puttini, Zaigham Mahmood "Cloud Computing: Concepts, Technology & Architecture".