Universidad del Valle de Guatemala
Facultad de Ingeniería

Diseño e implementación de la plataforma para gestión automatizada de enlaces Ethernet e IP de una empresa de telecomunicaciones.

Trabajo de Graduación en presentado por
Lucia Analy Alvarez Fernández
para optar al grado académico de Licenciada en Ingeniería Electrónica

Guatemala,

2016

Universidad del Valle de Guatemala
Facultad de Ingeniería

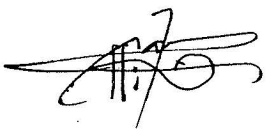
Diseño e implementación de la plataforma para gestión automatizada de enlaces Ethernet e IP de una empresa de telecomunicaciones.

Trabajo de Graduación en presentado por
Lucia Analy Alvarez Fernández
para optar al grado académico de Licenciada en Ingeniería Electrónica

Guatemala,

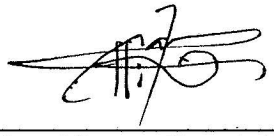
2016

Vo.Bo.:

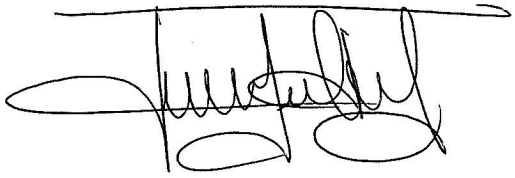


(f)_____
Carlos Alberto Esquit Hernández

Tribunal Examinador:



(f)_____
Carlos Alberto Esquit Hernández



(f)_____
Julio Ismael Vásquez Vargas

(f)_____
José Augusto Sánchez Villanueva

Fecha de Aprobación: Guatemala, 13 de junio de 2016

ÍNDICE

Página

LISTA DE CUADROS

Página

LISTA DE FIGURAS

Página

RESUMEN

Este trabajo presenta una propuesta para la implementación de una plataforma de monitoreo de enlaces Ethernet e IP. Para esto, el primer paso fue definir la clasificación general de la interface. Luego también se debió definir la manera en que constaría que los enlaces nuevos se consideran funcionales a través de la determinación de los parámetros a evaluar. Por último, se debió definir un flujo para la gestión de eventos generados en los enlaces Ethernet e IP.

La parte más relevante del trabajo consiste en la gestión de los eventos, dado que se contaba con el monitoreo de los enlaces, pero no se estaba utilizando los resultados para realizar acciones correctivas o de notificación a clientes, puesto que no existía ninguna estructura que ayudara a determinar el impacto y urgencia de los eventos presentados en los enlaces.

Se logró definir umbrales para determinar el impacto que estaban experimentando los enlaces, y se definió también una clasificación de urgencia de los enlaces dependiendo de sus características. A partir de esos dos parámetros, impacto y urgencia, se determina la prioridad del evento, lo cual a su vez determina las acciones requeridas a realizar ya sea automáticamente o manualmente por un ingeniero de soporte. En varias ocasiones las acciones manuales quedan a discreción del ingeniero que esté a cargo del monitoreo.

I. INTRODUCCIÓN

Este trabajo tiene el objetivo de realizar un diseño para implementar una plataforma de monitoreo para enlaces Ethernet e IP de una empresa de telecomunicaciones. Se pretende que la herramienta pueda gestionar los enlaces, vpns y clientes de la compañía para la que se realizó el trabajo, así como mostrar alarmas por la generación de eventos sobre dichos enlaces y realizar las acciones que sean requeridas, ya sea de manera automática o de manera manual por parte de un usuario, que sería un ingeniero de soporte técnico.

Para esto se debió realizar inicialmente la definición de la clasificación general de la plataforma, la cual quedó definida en Enlaces, VPNs, Clientes, Herramientas y Monitoreo. Esta clasificación general se definió a partir de la manera más intuitiva como generalmente se organizan los enlaces, donde es posible realizar búsquedas, documentar comentarios y encontrar todo tipo de información relevante para la gestión de los enlaces en el día a día.

En el trabajo se incluye una parte en que se definen los parámetros que se tomarán en cuenta para la aceptación de enlaces nuevos como funcionales, lo cual constituye una parte importante en la operación, puesto que es importante que conste que al entregar el enlace el mismo se encontraba en condiciones aceptables tanto para la compañía como para el cliente.

La tercera parte constituye la más relevante del trabajo, que es la definición de un flujo para la gestión de eventos generados en los enlaces Ethernet e IP, para lo cual se debió definir la manera en que se determinaría la prioridad de dichos eventos. Para esto se tomó en cuenta parámetros como la urgencia del enlace, basada en el monto de facturación, ancho de banda y utilización del enlace; y también el impacto que esté ocasionando el evento sobre el enlace.

Es importante mencionar que el monitoreo de los enlaces Ethernet e IP ya se encontraba implementado; sin embargo, no estaba siendo utilizado de ninguna manera hasta el momento para poder generar acciones a partir de los resultados del monitoreo. Fue por ello que se debió definir umbrales para poder determinar el impacto del evento, y así generar alertas que llevaran a la necesidad de realizar acciones correctivas o de notificación a clientes.

En este trabajo no se incluyó la parte de la programación para la implementación de la plataforma, dado que esto fue realizado por un otro grupo de ingenieros de la compañía para la que se realizó el trabajo, sino únicamente se trabajó el diseño de la plataforma, la definición de los umbrales para la detección de eventos, la generación de alarmas dependiendo de prioridad del evento y el flujo de los eventos para llegar a realizar acciones según se requiriera.

Se pudo concluir que la interface diseñada era funcional para el acceso a la gestión de los enlaces Ethernet e IP, se pudo definir los parámetros aceptables para que un enlace Ethernet o IP nuevo pueda considerarse funcional. Se logró determinar las condiciones suficientes para generar una alerta en el monitoreo de un enlace Ethernet e IP dependiendo de sus características y también el flujo a seguir para generar acciones a partir de una alerta disparada en un enlace Ethernet o IP. Se pudo crear una clasificación de enlaces Ethernet e IP por criticidad tomando en cuenta sus características específicas, así como un criterio de disparo de alertas según la clasificación de criticidad que tenga cada enlace Ethernet e IP.

II. OBJETIVOS

A. OBJETIVO GENERAL

Diseñar e implementar una plataforma para gestión automatizada de enlaces Ethernet e IP de una empresa de telecomunicaciones.

B. OBJETIVOS ESPECÍFICOS

1. Diseñar una interface funcional para el acceso a la gestión de los enlaces Ethernet e IP.

2. Especificar los parámetros aceptables para que un enlace Ethernet o IP nuevo pueda considerarse funcional.

3. Determinar las condiciones suficientes para generar una alerta en el monitoreo de un enlace Ethernet e IP dependiendo de sus características.

4. Determinar el flujo a seguir para generar acciones a partir de una alerta disparada en un enlace Ethernet o IP.

5. Crear una clasificación de enlaces Ethernet e IP por criticidad tomando en cuenta sus características específicas.

6. Crear un criterio de disparo de alertas según la clasificación de criticidad que tenga cada enlace Ethernet e IP.

7. Definir las acciones a realizar dependiendo de las alertas disparadas en los enlaces Ethernet e IP.

III. JUSTIFICACIÓN

Las redes de datos e internet son indispensables para la operación de múltiples compañías a nivel mundial, dado que permiten el funcionamiento de las aplicaciones y la comunicación a nivel institucional. Surgieron como una necesidad de las empresas para acceder y compartir información rápida y eficazmente. Las de redes han brindado soluciones para compartir información, hardware, software y centralización de administración y soporte.

Como es de esperarse, el funcionamiento de los enlaces de datos e internet, es crítico para la operación de las empresas, pues de otra manera no pueden comunicarse hacia el mundo exterior. Es por ello que existen centros especializados para el monitoreo de las redes, detección y resolución de fallas en las mismas. Estos centros se conocen generalmente como NOC (Network Operation Center) o Centro de Operaciones de Redes. En un NOC, el personal está enfocado en analizar problemas, realizar procesos de pruebas para detectar inconvenientes en la comunicación.

En el proceso de detección de fallas, el tiempo en que se realizan las pruebas sobre un enlace debe minimizarse tanto como sea posible, dado que esto permite disminuir el tiempo en que se realizan las acciones correctivas necesarias, y consecuentemente el tiempo en que se resuelve la falla. Es por ello que se requiere tener una plataforma que permita asegurar que los enlaces nuevos cumplen con las especificaciones requeridas para considerarse como funcionales, de esta manera evitar reporte de fallas por deficiencias en implementación, y también que sea capaz de generar alertas al detectar problemas con algún enlace y también derivar acciones para el tratamiento temprano de la falla.

En la actualidad, el NOC de la empresa de telecomunicaciones en cuestión, utiliza gran cantidad de recursos en la atención de fallas reportadas por clientes, mientras que al implementar la solución que presenta este trabajo, se pretende tener un mayor enfoque en la detección temprana y resolución de fallas proactivamente.

IV. ANTECEDENTES

Con anterioridad a este trabajo se desarrolló la implementación del monitoreo de enlaces Ethernet e IP. El monitoreo de los enlaces Ethernet se realizó a través de la lectura del estado de interfaces y VPLSs, tráfico y mac address, mientras que el monitoreo a nivel IP se realizó a través de RPM, recolectando datos como porcentajes de pérdida de paquetes, RTT y Jitter. De esta manera, se tenía implementación de dicho monitoreo; sin embargo, no se contaba con un proceso que permitiera utilizar los resultados del monitoreo para generar acciones correctivas o de notificación a clientes, ni que permitiera al equipo de ingenieros del centro de operaciones de redes, tener visibilidad del estado de los servicios de manera clara y accesible.

Adicionalmente, se contaba con la implementación de la comunicación entre el servidor de la plataforma y los equipos desde los cuales se requiere hacer las pruebas para mantener los servicios bajo monitoreo, sin embargo no se contaba con un diseño de monitoreo para poder ser implementado de manera eficaz, a manera de que permitiera mantener a la vista únicamente los eventos más relevantes a través de un análisis de los mismos, y realizar las acciones más urgentes y necesarias para la notificación y corrección de fallas.

V. METODOLOGÍA

El trabajo se dividió en tres partes importantes; la primera es la del diseño de la plataforma, la cual se realizó según las necesidades del equipo del trabajo y de acuerdo a la que se creía que era la manera más intuitiva como puede agruparse los enlaces Ethernet e IP. La primera parte implicó un análisis para la definición de la información que se presentaría en cada una de las clasificaciones generales. Para la segunda parte del trabajo, que consiste en la definición de un criterio de aceptación de enlaces Ethernet e IP nuevos para que sean considerados como funcionales, fue necesario definir los parámetros a tener en consideración y los valores aceptables para que tenga un funcionamiento adecuado, lo cual se definió dependiendo del tipo de enlace, la ubicación del punto inicial y final, y otros parámetros detallados más adelante. Para la tercera y última parte del trabajo, que consistió en diseñar y validar la implementación un proceso que permitiera utilizar el disparo de alertas generado a partir de un evento detectado en el monitoreo enlaces, para luego pasar por un análisis de la criticidad del enlace, y así determinar la acción a realizar, se definió los criterios y umbrales a utilizar. Uno de estos criterios fue el impacto del evento sobre el enlace, y otro fue la urgencia del evento, que estaba definido por la criticidad del enlace. Dichos criterios se definieron tomando en cuenta ciertas características como el ancho de banda, los costos de facturación, las aplicaciones en que se utilizan, entre otras. Como era supuesto, esta tercera parte fue la que mayor análisis requirió, dado que, utilizando los criterios previamente definidos, se debe diseñar un flujo para generar acciones a partir de una alerta disparada en un enlace. Adicionalmente se deben definir las acciones a realizar dependiendo del tipo de alerta que se genere al finalizar el flujo.

De esta manera, las actividades a realizar se dividieron en 17: definir las clasificaciones generales de la interface, definir los elementos incluidos en cada clasificación, implementar la clasificación de la interface, especificar los parámetros aceptables para que un enlace Ethernet e IP nuevo pueda considerarse funcional, diseñar la clasificación de los enlaces Ethernet e IP según sus características, implementar la clasificación de los enlaces y verificar que sea válida y totalmente incluyente, definir los valores aceptables para cada característica que se tomará en cuenta para generar una alerta en el monitoreo de un enlace Ethernet e IP, determinar el flujo a seguir para generar acciones a partir de una alerta disparada en un enlace, validar el flujo con el equipo de trabajo de monitoreo, definir cuáles son las características que se deben tomar en cuenta para

determinar la criticidad de un enlace, definir cuáles son los rangos dentro de dichas características, crear una clasificación de enlaces por criticidad tomando en cuenta sus características específicas, validar que la clasificación de enlaces por criticidad sea válida y totalmente incluyente, definir un criterio de disparo de alertas según la clasificación de criticidad que tenga cada enlace, definir las acciones a realizar dependiendo de las alertas disparadas en los enlaces, implementar las acciones a realizar dependiendo de dichas alertas, validar el proceso con el equipo de trabajo y por último, elaborar del trabajo escrito.

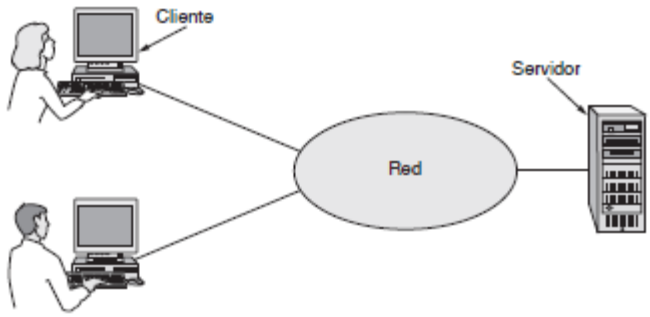
VI. MARCO TEÓRICO

Este trabajo presenta una propuesta para el diseño e implementación de una plataforma para gestión automatizada de enlaces Ethernet e IP, y para la comprensión de dicha propuesta, es necesario tener el conocimiento básico sobre redes de computadoras.

A. DEFINICIÓN DE REDES DE COMPUTADORAS

En el pasado se solía tener los llamados "centros de cómputo", donde las personas pertenecientes a cierta organización llevaban su trabajo para procesarlo. Hoy en día, este concepto es obsoleto, y ha quedado en el pasado el modelo en que existía una sola computadora para atender todas las necesidades computacionales de la organización. Dicho concepto ha sido reemplazado por uno en que un gran número de computadoras separadas, pero interconectadas realizan el trabajo. A estos sistemas se les conoce como redes de computadoras, también conocidas como redes de telecomunicaciones, o redes informáticas, y tienen múltiples aplicaciones tales como negocios, domésticas, móviles y sociales (Tanenbaum, 2012).

Figura 1. Red simple donde dos clientes se conectan a un servidor.



(Tanenbaum, 2012)

Actualmente, no existe una clasificación aceptada en la que encajen todas las redes, pero hay dos que sobresalen de manera importante: la tecnología de transmisión y la escala. En la Figura 1 se puede observar un ejemplo de una red simple.

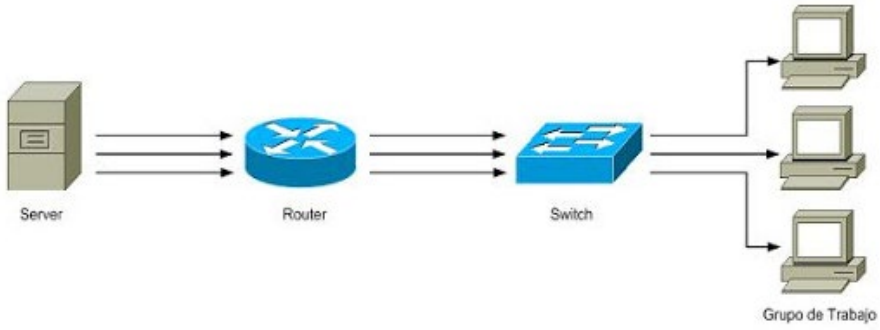
B. CLASIFICACIÓN DE REDES POR TECNOLOGÍA DE TRANSMISIÓN

En términos generales, existen dos tipos de tecnología de transmisión empleados mayormente en la actualidad: los enlaces de difusión y los enlaces de punto a punto.

1. Enlaces de punto a punto.

Estos se caracterizan porque conectan pares individuales de máquinas. Probablemente los mensajes, conocidos como paquetes, para ser transmitidos del sitio origen al destino deban pasar por alguna o algunas máquinas intermediarias. A la transmisión punto a punto, como la que se observa en la Figura 2, en donde sólo hay un emisor y un receptor se le conoce como unidifusión (Rosales, 2016).

Figura 2. Método de transmisión por unidifusión.



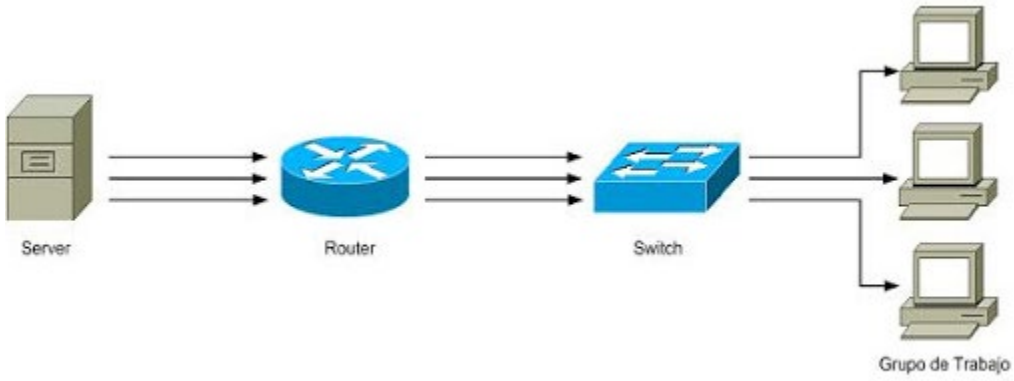
(Rosales, 2016)

2. Enlaces de difusión.

Una red de difusión se caracteriza porque todas las máquinas en la red comparten un mismo canal de comunicación y los paquetes que envía una máquina son recibidos por todas las demás, como se puede observar en la Figura 3. En este caso, existe un campo de dirección dentro de cada paquete que especifica a quién se dirige, a manera que cuando una máquina recibe un paquete, verifica el campo de dirección, si el paquete está destinado a la máquina receptora, ésta procesa el paquete; pero si el paquete está destinado para otra máquina, lo ignora. A este modo de operación se le conoce como difusión. Algunos sistemas de difusión también soportan la transmisión a un

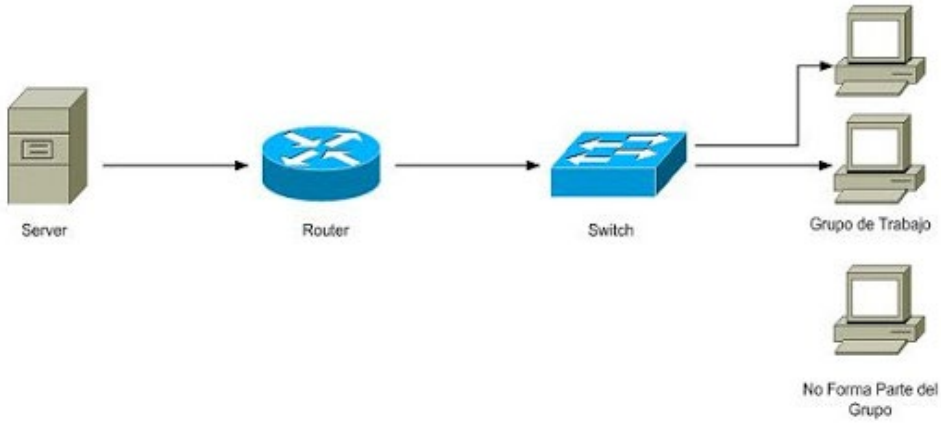
subconjunto de máquinas, como se observa en la Figura 4, lo cual se conoce como multidifusión (Tanenbaum, 2012).

Figura 3. Método de transmisión por difusión.



(Rosales, 2016)

Figura 4. Método de transmisión por multidifusión.

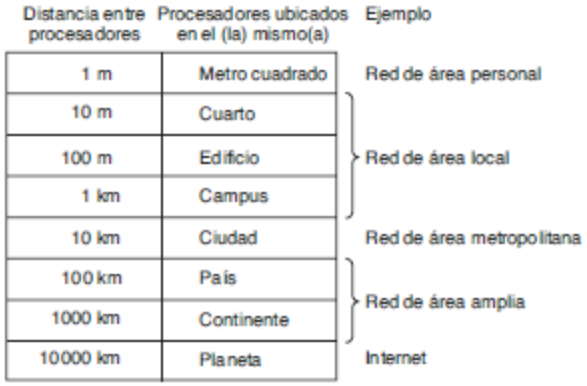


(Rosales, 2016)

C. CLASIFICACIÓN DE REDES POR ESCALA

Este es un criterio alternativo para la clasificación de las redes, y la distancia es un aspecto importante que se debe tomar en cuenta dado que las distintas tecnologías se utilizan a diferentes escalas. En la Figura 5 se puede observar la clasificación de los procesadores o computadoras con base en la escala, las cuales se pueden dividir en redes de área local, de área metropolitana y de área amplia, cada una con una escala mayor que la anterior. Adicionalmente, a la conexión de dos o más redes se le conoce como interred, y el mejor ejemplo de esto es la Internet (Tanenbaum, 2012).

Figura 5. Clasificación de los procesadores interconectados según la escala.



Distancia entre procesadores	Procesadores ubicados en el (la) mismo(a)	Ejemplo
1 m	Metro cuadrado	Red de área personal
10 m	Cuarto	Red de área local
100 m	Edificio	
1 km	Campus	
10 km	Ciudad	Red de área metropolitana
100 km	País	Red de área amplia
1000 km	Continente	
10000 km	Planeta	Internet

(Tanenbaum, 2012)

1. Redes de área personal.

Estas son también llamadas PAN por sus siglas en inglés, y permiten a los dispositivos comunicarse dentro del rango de una persona. Un buen ejemplo es una red inalámbrica que conecta a una computadora con sus periféricos. Pueden también utilizar cables para comunicar los diferentes dispositivos entre sí, y pueden abarcar espacio cerca de un metro cuadrado. (Tanenbaum, 2012).

2. Redes de área local.

Estas redes se conocen como LAN por sus siglas en inglés, y son redes de propiedad privada que funcionan dentro de un mismo campus, edificio, casa u oficina. También son llamadas redes empresariales y tal como se puede observar en la Figura 5, están generalmente limitadas a un espacio entre 10 metros y 10 kilómetros (Tanenbaum, 2012).

3. Redes de área metropolitana.

Una red de este tipo, también conocida como MAN por sus siglas en inglés, abarca el perímetro de una ciudad, o cerca de los 10 kilómetros. Un ejemplo sería las redes de televisión por cable (Tanenbaum, 2012).

4. Redes de área amplia.

Una red de este tipo abarca una extensa área geográfica, por lo general un país o continente. Son llamadas también WAN por sus siglas en inglés y puede llegar a extenderse hasta 10,000 kilómetros (Tanenbaum, 2012).

5. Interredes.

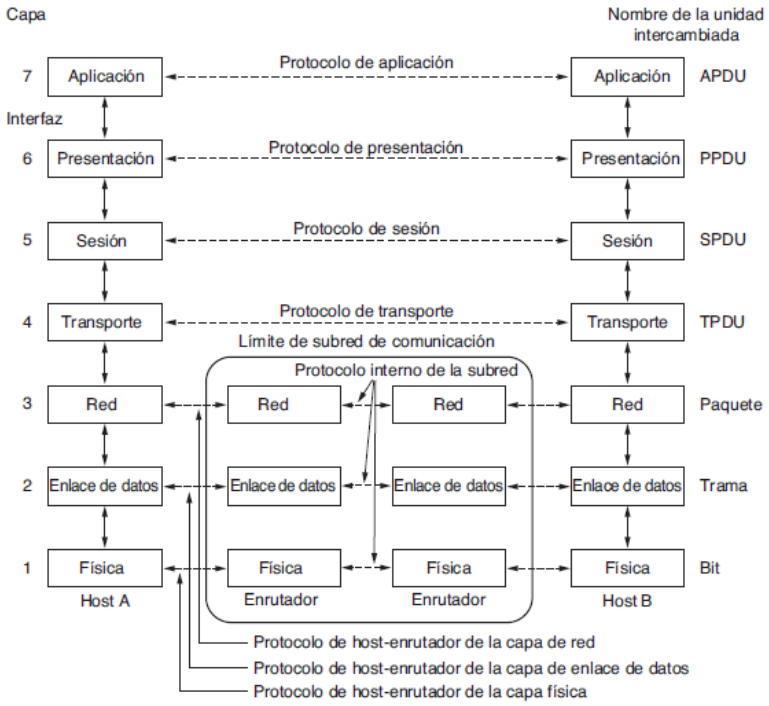
Estas redes surgen de la necesidad de las personas conectadas a una red, para conectarse a una red distinta. Para lograrlo, es necesario conectar redes distintas que con frecuencia son incompatibles. A una colección de redes interconectadas se le conoce como interred o internet. La Internet Mundial, que es una red internet específica, es un ejemplo (Tanenbaum, 2012).

Hasta este momento se ha estudiado las redes a nivel de hardware; sin embargo, es importante examinar también las redes a nivel de software puesto que ha llegado a estar muy estructurado.

D. MODELO DE REFERENCIA OSI

Para comprender la manera en que se logra la comunicación entre dos computadoras a través de una red, se debe entender el funcionamiento del modelo de interconexión de sistemas abiertos, o modelo OSI. Este modelo tiene siete niveles llamados capas, y su finalidad es delegar ciertos aspectos de la comunicación a cada una de las capas, a manera que el resto pueda desentenderse de esos detalles y enfocarse en su responsabilidad. En la Figura 6 se puede observar un diagrama explicativo del modelo OSI.

Figura 6. Modelo OSI.



(Tanenbaum, 2012)

Desde la primera capa, cada una provee un servicio a su capa superior, hasta llegar a la capa de aplicación que es con la que el usuario tiene interacción. Se explicará cada capa comenzando desde la más baja que es la capa física, hasta la más alta, que es la capa de aplicación (Arriola, 2013).

1. Capa física.

Esta capa es la encargada de transmitir las unidades binarias de información a través del medio físico de transmisión, se ocupa de las propiedades físicas y de las características eléctricas de los diversos componentes tales como la velocidad de transmisión y si esta es uni o bidireccional (simplex, dúplex o full-dúplex). También se encarga de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.

De manera general se puede decir que esta capa se encarga de la transformación de un paquete de información binaria, conocidos como cuadros, a una sucesión de impulsos que son

adecuados para el medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos, como en la transmisión por cable; electromagnéticos, como en la transmisión inalámbrica; o luminosos, como en la transmisión óptica. Cuando la acción que realiza es la recepción, el trabajo es inverso; se encarga de transformar los impulsos mencionados en paquetes de datos binarios que serán entregados a la siguiente capa, que es la capa de enlace (Ecured, 2016).

2. Capa de enlace.

Esta capa se encarga de trasladar los mensajes desde y hacia la capa física a la tercera capa, que es la capa de red. En esta capa se especifica la manera en que se organizan los datos cuando se transmiten en un medio de transmisión. En esta capa se definen cómo son los cuadros, las direcciones y las sumas de control de los paquetes Ethernet. Se encarga del direccionamiento local, la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para realizar lo mencionado, agr upa la información a transmitir en bloques, conocidos como cuadros, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son corroborados por el receptor, y en caso se detecte que algún datagrama se ha corrompido, se envía un mensaje de control al remitente solicitando su reenvío (Ecured, 2016)

Es importante realzar que en esta capa se utilizan las direcciones Media Access Control, o MAC, que también se conocen como direcciones de hardware. Estas están formadas por 48 bits normalmente representados por dígitos hexadecimales agrupados en seis parejas, cada pareja se separa de otra mediante dos puntos o un guion; los primeros 24 bits identifican el fabricante de la tarjeta, y los siguientes diferencian cada una de las tarjetas. Cada tarjeta tiene una dirección MAC única. Los protocolos Ethernet y ATM son ejemplos de esta capa (Arriola, 2013)

3. Capa de red.

En esta capa se lleva a cabo la transmisión de los datagramas (paquetes) y el encaminamiento de cada uno a la ruta adecuada. Sin embargo, no se ocupa de los errores o pérdida de paquetes, sino que únicamente define la estructura de direcciones y rutas. A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta. En esta capa también se realiza la fragmentación de los cuadros, en caso el tamaño máximo de transmisión, MTU por sus siglas en inglés, sea menor que el tamaño de los cuadros que maneja el enrutador (Ecured, 2016).

Esta capa tiene dos partes importantes; el transporte y la conmutación. En la parte del transporte, se encapsulan los datos a transmitir y utiliza los paquetes de datos. La parte de conmutación es la encargada de intercambiar información de conectividad específica de la red, y su actividad es raramente percibida por el usuario. En esta categoría se encuentra el protocolo de control de mensajes de Internet, ICMP por sus siglas en inglés; y el protocolo de Internet, IP por sus siglas en inglés (Ecured, 2016).

4. Capa de transporte.

Esta es la capa encargada de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. En esta capa se define cuándo y cómo debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa superior, que es la capa de sesión, en trozos (datagramas), los enumera correlativamente y los entrega a la capa de red para su envío (Ecured, 2016).

Esta capa también es responsable de los mensajes de confirmación, en que se asegura la entrega confiable de los paquetes y multiplexa varias secuencias de mensajes, o las sesiones en un vínculo lógico para mantener un seguimiento de los mensajes pertenecen a las sesiones, que se explicará en la capa siguiente que es la capa de sesión (Arriola, 2013).

Ejemplos de esta capa son el protocolo de control de transporte, TCP por sus siglas en inglés, y el protocolo de datagrama universal, UDP por sus siglas en inglés.

5. Capa de sesión.

Esta capa es una extensión de la capa de transporte, ofrece control de diálogo y sincronización. Debido a que en la realidad es utilizada por pocas aplicaciones, algunos autores indican que es meramente una consideración teórica de los autores del modelo sin absolutamente ninguna utilidad práctica conocida (Ecured, 2016).

Esta capa permite los procesos de aplicación en diferentes equipos para establecer, utilizar y terminar una conexión, llamada sesión. Ofrece el establecimiento, mantenimiento y terminación de la sesión, y realiza las funciones que permiten a los equipos comunicarse a través de la red de manera segura, realizar los procesos como el reconocimiento de nombre y el registro (Arriola, 2013).

6. Capa de presentación.

En esta capa a diferencia de las capas inferiores, que se enfocan principalmente en mover las unidades binarias de un lado a otro, el enfoque es en la sintaxis y la semántica de la información transmitida. Define de manera abstracta las estructuras de datos que se van a intercambiar, a manera que sea posible la comunicación entre computadoras con distintas representaciones internas de datos. La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de mayor nivel, como por ejemplo, registros bancarios (Tanenbaum, 2012). Según algunos autores, esta capa es buena candidata para implementar aplicaciones de criptografía. En esta capa se presenta los datos a la capa de aplicación cogiendo los datos recibidos y transformándolos en formatos como texto imágenes y sonido (Ecured, 2016).

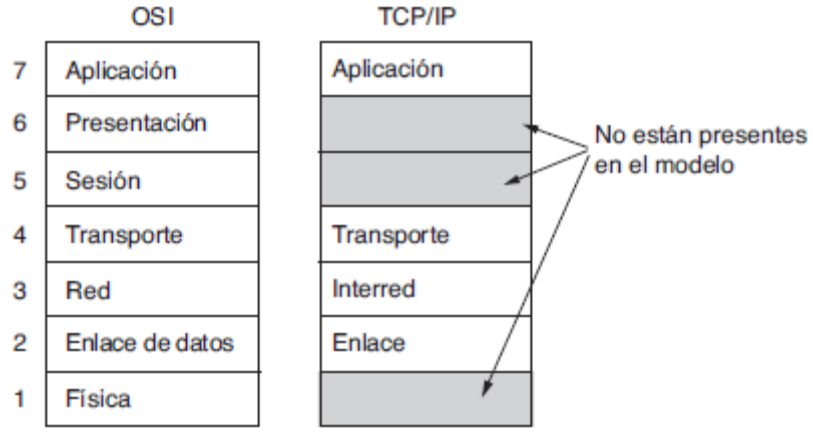
7. Capa de aplicación.

Esta capa describe como hacen su trabajo los programas de aplicación, tales como navegadores, clientes de correo, terminales remotos, transferencia de ficheros, etc. En esta capa se manejan varios protocolos utilizados con frecuencia. Un ejemplo de esto es el protocolo de transferencia de hipertexto, HTTP por sus siglas en inglés, el cual forma la base para la Internet. Cuando un navegador desea una página web, envía el nombre de la página que quiere al servidor que la hospeda mediante el uso de HTTP. Después el servidor envía la página de vuelta. Hay otros protocolos de aplicación que se utilizan para transferir archivos, enviar y recibir correo electrónico y noticias (Tanenbaum, 2012).

E. MODELO DE REFERENCIA TCP/IP

Este modelo presenta una estructura desde una perspectiva distinta al modelo OSI, como se puede observar en la Figura 7. Se dio a conocer como el Modelo de referencia TCP/IP debido a sus dos protocolos primarios. Este modelo se definió por primera vez en 1974; sin embargo, después se refinó y definió como estándar en la comunidad de Internet en 1989.

Figura 7. Diferencias entre el modelo de referencia OSI y el modelo de referencia TCP/IP.



(Tanenbaum, 2012)

1. La capa de enlace.

Debido a que se tenía la necesidad de incluir una gran cantidad de redes con diferentes medios de transmisión físicos, se llegó a la elección de una red de conmutación de paquetes basada en una capa sin conexión que opera a través de distintas redes. La capa más baja en este modelo es la capa de enlace; describe qué enlaces se deben llevar a cabo para cumplir con las necesidades de esta capa de interred sin conexión. Más que una capa, es una interfaz entre los anfitriones (hosts) y los enlaces de transmisión (Tanenbaum, 2012).

2. La capa de interred.

Esta capa tiene una correspondencia aproximada a la capa de red del modelo de referencia OSI, como se puede ver en la Figura 7. Su trabajo es permitir que los anfitriones inyecten paquetes en cualquier red y que viajen de independientemente hacia el destino, que podría estar incluso en una red distinta. Es posible inclusive que los paquetes llegasen en un orden totalmente diferente al que se enviaron, en cuyo caso es responsabilidad de las capas más altas volver a ordenarlos, si se desea una entrega en orden. El autor Tanenbaum (2012), realiza una analogía de esta capa con el sistema de correos convencional:

«Una persona puede dejar una secuencia de cartas internacionales en un buzón en un país y, con un poco de suerte, la mayoría de ellas se entregarán a la dirección correcta en el país de destino. Es probable que las cartas pasen a través de una o más puertas de enlace de correo internacionales en su trayecto, pero esto es transparente a los usuarios. Además, los usuarios no

necesitan saber que cada país (es decir, cada red) tiene sus propias estampillas, tamaños de sobre preferidos y reglas de entrega.»

Esta capa define un formato de paquete y un protocolo oficial llamado protocolo del Internet, IP por sus siglas en inglés, además de un protocolo complementario llamado protocolo de mensajes de control de Internet, ICMP por sus siglas en inglés, que le ayuda a funcionar. La tarea de la capa de interred es llevar los paquetes IP al lugar donde se supone que deben ir. Aquí el enrutamiento de los paquetes es sin duda el principal aspecto, al igual que la congestión (Tanenbaum, 2012).

3. La capa de transporte.

Esta capa funciona de manera muy similar a la del modelo OSI, puesto que está diseñada para permitir que las entidades pares, en los nodos de origen y de destino, lleven a cabo una conversación. Aquí se definieron dos protocolos de transporte entre los extremos. El primero, protocolo de control de la transmisión, TCP por sus siglas en inglés, es un protocolo confiable orientado a la conexión que permite que los datos se entreguen sin errores a cualquier otra máquina en la interred. En el destino, los mensajes deben ser ensamblados nuevamente, de manera que se conforme un flujo de salida. El TCP también maneja el control de flujo para evitar inundar a un receptor lento. El segundo protocolo en esta capa, protocolo de datagrama de usuario o UDP por sus siglas en inglés, es un protocolo sin conexión, que no es confiable para aplicaciones que no desean la asignación de secuencia o el control de flujo de TCP y prefieren proveerlos por su cuenta. Se utiliza bastante en las aplicaciones en las que es más importante una entrega oportuna que una entrega precisa, como en la transmisión de voz o video (Tanenbaum, 2012).

4. La capa de aplicación.

Este modelo no tiene capas de sesión o de presentación, puesto que en su momento no se consideraron necesarias. Las aplicaciones simplemente incluyen cualquier función de sesión y de presentación que requieran. Sobre la capa de transporte se puede encontrar la capa de aplicación, que contiene todos los protocolos de alto nivel. Entre los primeros protocolos están el de terminal virtual TELNET, transferencia de archivos FTP y correo electrónico SMTP. A través de los años se han agregado muchos otros protocolos (Tanenbaum, 2012).

F. MULTIPROTO DE CONMUTACIÓN DE ETIQUETAS

El multiprotocolo de conmutación de etiquetas, MPLS por sus siglas en inglés, reduce el procesamiento de paquetes que se requiere cada vez que un paquete ingresa a un enrutador en la red de manera significativa, lo cual mejora el desempeño de los dispositivos y del desempeño de la red en general. Este es un protocolo que se mantiene en desarrollo constante dado que en los últimos años la demanda de esta tecnología ha ido incrementando. Las capacidades más relevantes de dicho protocolo son cuatro; el soporte de calidad sobre servicio, QoS por sus siglas en inglés; ingeniería de tráfico; soporte para redes privadas virtuales, VPNs por sus siglas en inglés y, soporte multiprotocolo.

MPLS impone un marco de trabajo orientado a conexión en un ambiente de Internet, basado en el protocolo de Internet, IP (Morales, 2006).

1. Soporte de calidad de servicio.

QoS permite al administrador de la red tener un mayor control sobre los recursos de sus redes, dado que permite asignar más recursos a aplicaciones que más lo requieran, sin afectar el desempeño de las demás aplicaciones. Esto lo convierte en una herramienta para optimizar el ancho de banda y tiempos de respuesta (Morales, 2006).

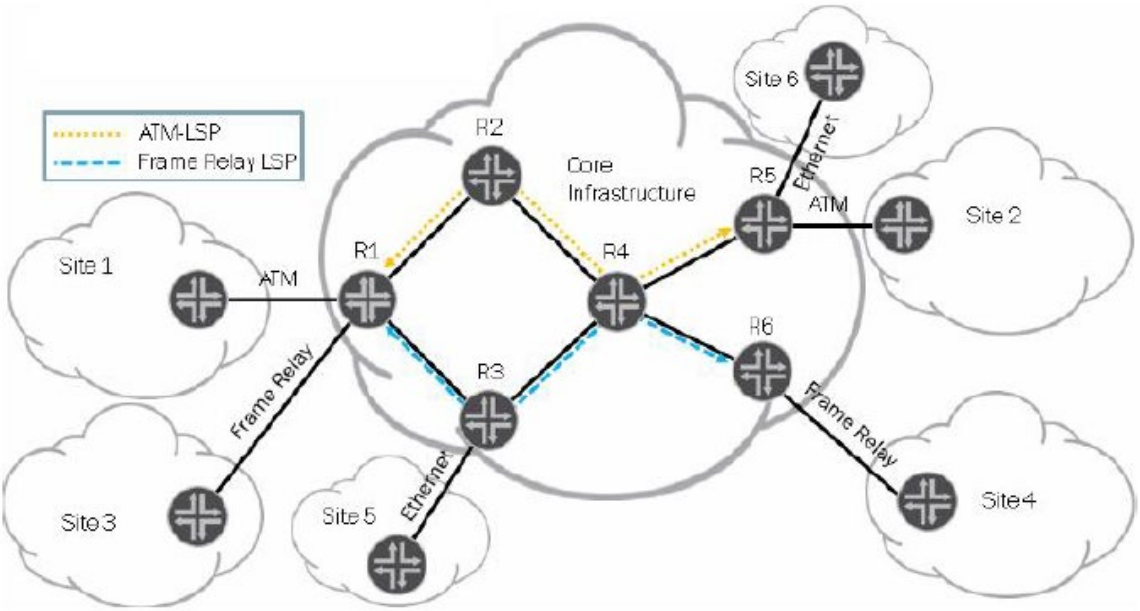
2. Ingeniería de tráfico.

Se refiere a la definición de rutas dinámicas y la planeación de la asignación de recursos según su demanda para la optimización de la red. Existen otros protocolos que permiten cambiar la ruta de los paquetes para balancear carga como IP o protocolo del Camino Más Corto Primero, OSPF por sus siglas en inglés; sin embargo, este cambio solo ocurre solo cuando hay congestión, lo cual no es deseable, y siempre se trata de evitar. A diferencia de otros protocolos como por ejemplo OSPF que ve paquete por paquete, con MPLS se puede predecir rutas en base a flujos individuales, lo cual hace posible de que existan diferentes flujos entre canales similares, pero dirigiéndose a diferentes enrutadores. Si llegase a amenazar congestión en la red, las rutas MPLS pueden ser re-ruteadas inteligentemente, de esta manera se pueden cambiar las rutas de flujo de paquetes dinámicamente conforme a las demandas de tráfico de cada flujo. En general, la ingeniería de tráfico permite evitar congestionamientos, mejorar el desempeño general y reducir la latencia y el desecho de paquetes (Morales, 2006).

3. Soporte de redes virtuales privadas.

MPLS permite manejar de manera eficiente las redes privadas virtuales, utiliza etiquetas que funcionan de manera análoga a los códigos postales con un identificador único que aísla cada red y de esta manera se reenvían paquetes a través de túneles privados. Estos caminos por los cuales se enrutan los paquetes son llamados label switched paths, o LSP's. Las VPN implementadas a través de tecnología MPLS tienen una mayor capacidad de expansión y son más flexibles en cualquier red (Arriola, 2013).

Figura 8. Ejemplo de implementación de distintas tecnologías como ATM, Frame Relay, IPSec y Ethernet, sobre una misma estructura MPLS.



(Arriola, 2013).

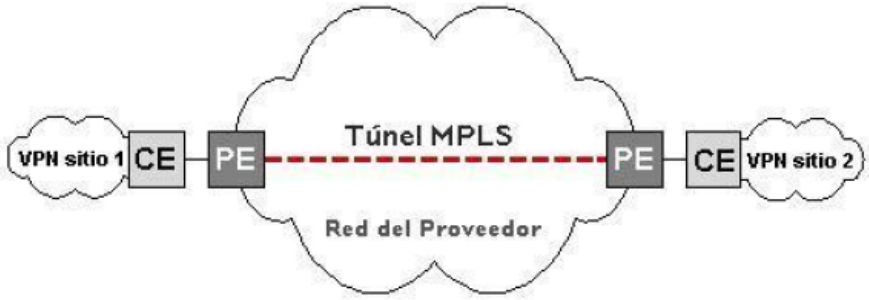
4. Soporte multiprotocolo.

Esta es una de las mayores ventajas de MPLS, ya que es posible implementar esta tecnología con otras tecnologías ya existentes, tales como IP, Internet, ATM y Frame Relay, tal como se observa en la Figura 8. No es necesario actualizar los enrutadores IP existentes, puesto que los enrutadores MPLS pueden trabajar con enrutadores IP, al igual que los switches. Es por ello que se dice que propicia la ampliación de redes sin necesidad de incurrir en grandes inversiones por la necesidad de cambiar las tecnologías implementadas previamente (Morales, 2006).

5. MPLS VPNs.

Para entender el funcionamiento de una red MPLS VPN, es necesario conocer los términos P (router interno del proveedor), PE (router de borde del proveedor) y CE (router frontera de cliente que solicita el servicio). Se entiende como sitio a las intranets de los clientes que están separados físicamente pero lógicamente unidos vía una VPN. Se puede observar de manera gráfica en la Figura 9. Una VPN en conjunto con tecnología MPLS crean servicios de eje troncal VPN IPv4 de capa 3. Una VPN IP es la base que las compañías utilizan para crear y administrar servicios de valor agregado como servicios de telefonía y de transmisión de datos para así ofrecerlos a sus clientes (Morales, 2006).

Figura 9. VPN con MPLS habilitado.



(Morales, 2006)

Cada VPN está asociada con una o más instancias de Ruteo/Reenvío Virtual llamadas VRF por sus siglas en inglés. Una VRF determina la conexión exclusiva que tiene el cliente conectado al router PE de la compañía proveedora del servicio. Cada VRF está compuesta por una tabla de ruteo IP, un grupo de interfaces que utilizan dicha tabla y un conjunto de reglas y parámetros del protocolo de ruteo que controlan la información que se incluye en la tabla de ruteo. Las VRF contienen las rutas disponibles en la VPN que pueden ser accedidas por los sitios de los clientes, cada sitio puede estar suscrito a varias VPN, pero solo a un VRF. (Morales, 2006).

G. PROTOCOLO DE INTERNET

El Protocolo de Internet, IP por sus siglas en inglés, es el protocolo utilizado para el envío de datos a través de internet desde una computadora, o equipo, llamado también host a otra. Cada

uno de estos equipos tiene una o más direcciones IP públicas, que lo identifica entre todos los demás equipos en Internet. Existen también IPs privadas, lo cual es determinado por rangos como se verá más adelante. Actualmente la versión utilizada es IP versión 4, en la cual las direcciones están formadas por 4 bytes, cada uno se muestra en forma decimal, separados por un punto de la siguiente manera: 190.127.27.4. También tiene máscara de red, la cual cumple la funcionalidad de delimitar la parte de la dirección que corresponde a la red y la que corresponde al host específico dentro de dicha red. La máscara está formada por 32 bits, y puede ser expresada de dos maneras; en la forma de 4 bytes al igual que la dirección IP de la siguiente manera: 190.127.27.4 255.255.255.252, o con el número de bits anteponiendo un símbolo de diagonal de la siguiente forma: 190.127.27.4/30, lo cual se puede observar en la Figura 10. La sección de la IP perteneciente a la red se obtiene realizando un AND lógico entre la IP y la máscara, esto nos da como resultado la red, y la sección eliminada nos indicaría el host (Arriola, 2013).

Figura 10. Ejemplo del cálculo de una red a través de la dirección IP y de su máscara

IP	192.168. 1. 8	11000000 10101000 00000001 00001000
Máscara	255.255.255. 0	11111111 11111111 11111111 00000000
Red	192.168. 1. 0	11000000 10101000 00000001 00000000

(Arriola, 2013)

Como fue mencionado anteriormente, una dirección IP puede ser pública o privada. Los bloques para redes privadas se definen de la siguiente manera: 10.0.0.0 – 10.255.255.255, 192.168.0.0 – 192.168.255.255, 172.16.0.0 – 172.31.255.255 y 169.254.0.0 – 169.254.255.255. Estas direcciones privadas son utilizadas por empresas que poseen redes con muchos equipos, y por otras organizaciones u hogares que cuentan únicamente con pocos equipos. Existen documentos donde se definen algunos aspectos del funcionamiento de Internet como protocolos, procedimientos, etc. que son publicados por el grupo de trabajo de ingeniería de Internet. Dentro de estas publicaciones, se encuentra el documento RFC 1918, donde se especifican los bloquees de IPs que corresponden a redes privadas y a redes públicas respectivamente. Este documento surgió como una medida temporal, debido a la rapidez de crecimiento de la Internet, pues se agotaron rápidamente las direcciones IP. Como una solución a largo plazo se ha planteado la utilización de IP versión 6, donde cada IP cuenta con 16 bytes (Arriola, 2013).

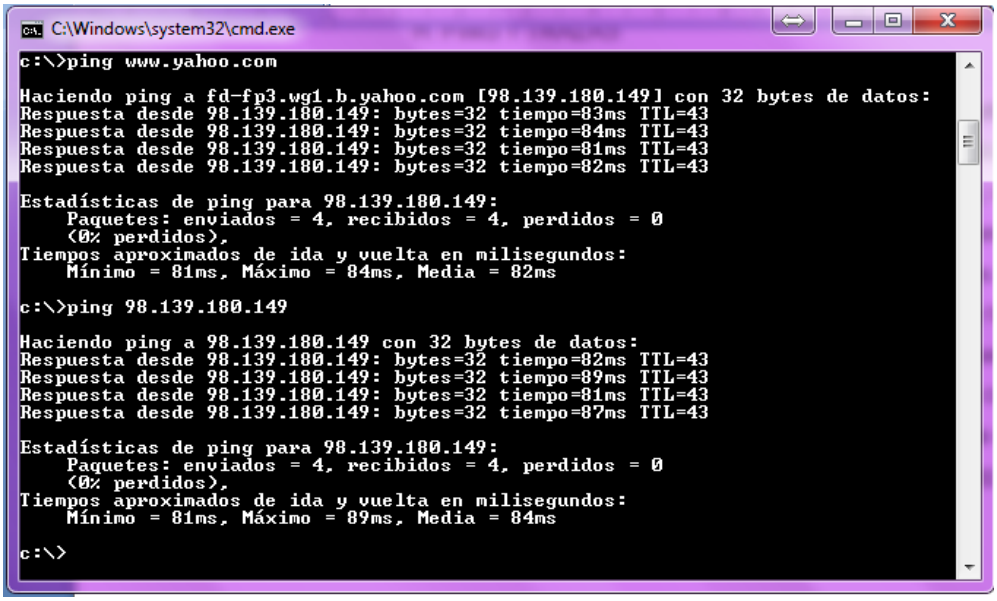
La manera en que funciona el envío de datos a través de Internet es descomponiendo dicho mensaje partes pequeñas llamadas paquetes, que contienen tanto la dirección de Internet del remitente como la del receptor. El direccionamiento de paquetes de origen a destino es realizado por enrutadores, que trabajan en la capa 3 del Modelo OSI mencionado anteriormente. Cualquier paquete para primero a un equipo de puerta de enlace, o Gateway en inglés, que comprende una pequeña parte del Internet. El dicho equipo lee la dirección de destino y envía el paquete a una puerta de enlace inmediata, que a su vez lee la dirección de destino y la envía a su puerta inmediata. Esto continúa sucediendo hasta que una puerta de enlace reconoce el paquete como perteneciente a un ordenador dentro de su vecindad inmediata o dominio, y reenvía el paquete directamente al ordenador cuya dirección se especifica. Debido a que un mensaje se divide en una serie de paquetes, cada paquete puede, si es necesario, ser enviada por una ruta diferente a través de Internet (Arriola, 2013).

Es importante recordar que en esta capa se trabaja el transporte de origen a destino, por lo que los paquetes podrían llegar en un orden diferente que el orden en que fueron enviados, y sería trabajo de la siguiente capa el ordenamiento de los paquetes, para lo cual se utiliza el protocolo de Control de Transmisión, TCP (Arriola, 2013).

H. PING Y TRAZAS

Ping y trazas son herramientas que pueden ser utilizadas para hacer pruebas de conectividad IP. La herramienta Ping generalmente es utilizada para comprobar que esté establecida una conexión y verificar la velocidad de la misma; indica cuánto tiempo un paquete de datos tarda en ir desde la computadora en la que se genera hasta un servidor específico y viceversa. Las trazas son otra herramienta útil, muestran los saltos de la ruta que sigue un paquete desde su computadora a una dirección de destino, y también muestran cómo muchas veces los paquetes están siendo retransmitidos por otros servidores hasta que llegue a su destino final. Ambas herramientas se pueden generar en una computadora con Windows desde la consola del sistema, en cuyo caso el tamaño del paquete es de 32 bytes. En la Figura 10 se observa una prueba de ping generada desde la consola del sistema Windows, el comando para generarla es la palabra ping seguida del nombre del servidor www.yahoo.com, o de la ip del host. Si la conexión está establecida al utilizar el comando se debe recibir cuatro respuestas como las de la Figura 11 (Arriola, 2013).

Figura 11. Prueba de Ping generada desde la consola del sistema Windows



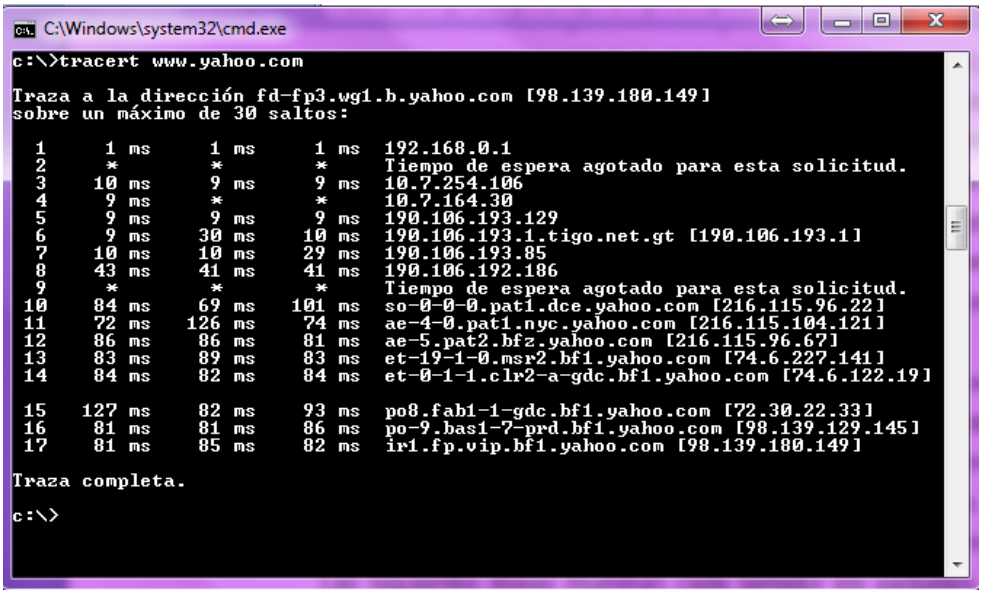
(Elaboración propia).

En el caso que el comando ping vaya seguido del nombre del servidor, la siguiente línea muestra el nombre completo del huésped. Las siguientes cuatro líneas deben mostrar si el host respondió, con la cantidad de bytes (tamaño del paquete), el tiempo de ida y vuelta (en milisegundos), y el time-to-live. Las últimas líneas muestran las estadísticas de ping al host, que incluyen el número de paquetes enviados, recibidos y perdidos, así como los tiempos de ida y vuelta y promedios. En el caso contrario, si no se reciben paquetes, se vería un mensaje que indica "Host de destino inaccesible" o "Tiempo de espera agotado". Esto puede indicar que la conexión no es correcta o bien, que por razones de seguridad, como es realizado en algunos servidores, no está permitido alcanzarlos a través de ping (Arriola, 2013).

En la Figura 12 se observa una traza utilizando la consola del sistema Windows, para lo cual se utiliza el comando tracert, seguido del nombre del servidor www.yahoo.com, o de la ip del host, al igual que con el comando ping. En la siguiente línea muestra el nombre completo del huésped y el número máximo de saltos antes de renunciar a tratar de encontrar el host. En las líneas siguientes se podrá observar cada servidor a través del cual los paquetes dan saltos para llegar al destino www.yahoo.com. Se muestra la dirección IP y el nombre de dominio real de los servidores a través de los cuáles pasan los paquetes. Las trazas son muy útiles porque pueden mostrar en qué salto se genera la falla de la conexión, lo cual permite determinar con precisión dónde se pierde un

paquete, que quedará en evidencia porque a partir de ahí, se verán únicamente asteriscos, como se observa en la Figura 12. Al igual que ping, algunos servidores no permiten ruta de seguimiento de todo el camino a ellos. Ping y trazas permiten diagnosticar problemas con las conexiones a Internet, o hacia un punto remoto en redes privadas puesto que ayudan a diagnosticar si el problema de conexión está en el equipo, fuera de la red, o en el servidor que está intentando alcanzar (Arriola, 2013).

Figura 12. Prueba de traza generada desde la consola del sistema Windows.



(Elaboración propia)

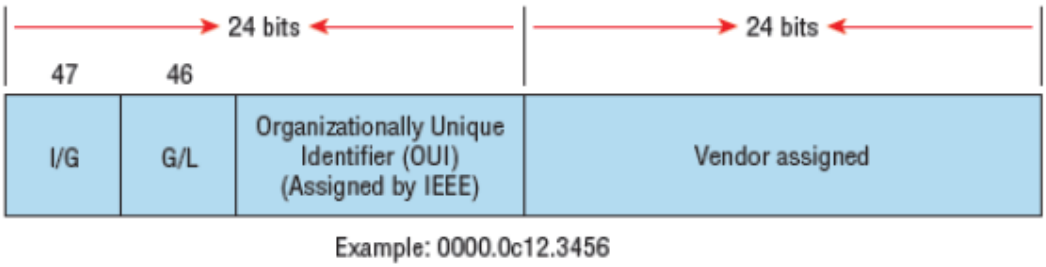
I. ETHERNET

Ethernet podría definirse como un estándar y una familia de protocolos y tecnologías dentro de la capa de enlace de datos y capa física del Modelo de referencia OSI. Se utiliza generalmente para conectar dispositivos a nivel de redes de área local (LAN), metropolitana (MAN) e incluso área amplia (WAN). Ethernet define las direcciones de control de acceso a media, MAC por sus siglas en inglés, como identificadores únicos de las tarjetas de interfaces de red, NIC por sus siglas en inglés, para cada elemento de red, tales como enrutadores, switches y hosts a nivel global. Cada interfaz de un dispositivo tiene una MAC única, y no podría repetirse en ningún otro dispositivo. Ethernet utiliza exclusivamente las direcciones MAC como método de direccionamiento para establecer conectividad entre dispositivos dentro de un mismo segmento de red o dominio de

Broadcast. A esto se le conoce como direccionamiento Ethernet o de capa 2, a este nivel el elemento principal es el switch, de manera análoga como en capa 3 lo es el enrutador (Robles, 2015).

Dentro del estándar Ethernet, una de las funciones principales que se buscan dentro del estándar Ethernet a nivel de capa 2 es el direccionamiento MAC o de hardware. Una dirección de acceso a media (MAC) está compuesta por 48 bits y, como se explicó anteriormente, se representa de manera hexadecimal. En la Figura 13, se puede apreciar la forma de asignación de una MAC. El campo OUI es asignado por la IEEE a una organización específica dedicada a la fabricación de elementos de red. El bit I/G (Individual/Group) indica qeu la MAC es única de una NIC de un elemento de red al ser 0, de lo contrario, si es 1, puede ser Mulitcast o Broadcast, es decir que hace referencia a un conjunto de NICs dentro de un dominio de difusión. El bit G/L (Global/Individual) indica que una MAC es administrada globalmente al ser 0, de lo contrario indica que es asignada por una entidad individual y para uso exclusivo de dicha entidad. De esta manera, interfaz física dentro de un elemento de red siempre tendrá una MAC única.

Figura 13. Asignación de dirección.



(Robles, 2015)

En capa 3, a la distribución de paquetes entre elementos de red se le conoce como ruteo, pero en capa 2, a la distribución de tramas entre equipos (switches) se le denomina conmutación capa 2 (Layer 2 Switching) (Robles, 2015).

Un switch de capa 2 es capaz de realizar la tarea con mayor rapidez que un enrutador dado que al no tener que determinar cuál es el siguiente salto para elegir la ruta óptima, no tiene que revisar el encabezado de capa3. Únicamente revisa la dirección física de destino de la trama previo a determinar enviarla a un puerto específico del equipo capa 2 (forwarding), a todos los puertos del equipo excepto por el cual salió, o bien, descartar la trama. La distribución de tramas a nivel de

capa 2 se compone de tres funciones básicas; aprendizaje de MACs, decisiones de envío/filtrado y prevención de bucles (Robles, 2015).

El aprendizaje de MACs es el equivalente en capa 2 a una tabla de rutas en capa de red, pero difiere en que únicamente se compone de tres elementos: la dirección MAC, el puerto lógico o físico del cual la aprende y la LAN virtual, VLAN por sus siglas en inglés, asociada. Los switches capa 2 almacenan la dirección MAC fuente en su tabla MAC al momento de evaluar el envío de una trama recibida a través de uno de sus puertos (Robles, 2015).

Las decisiones de envío/filtrado se llevan a cabo cuando una trama es recibida a través de uno de los puertos de un switch, y la MAC destino se compara con la tabla MAC. En caso que la MAC coincida, el switch envía la trama únicamente a través del puerto correspondiente, indicado por la tabla. Esto evita el envío a través de todos los puertos, y representa un ahorro de ancho de banda. A este proceso se le conoce como filtrado de tramas. En cambio, si la tabla MAC no logra asociar la MAC destino, la trama es entonces enviada al resto de puertos. Si se recibe una respuesta, la MAC es almacenada. Es importante recalcar que durante este proceso, la MAC fuente es siempre evaluada para asociarse a la tabla MAC de no tenerla en el registro (Robles, 2015).

Ethernet tiene la función de prevención de bucles dado que utiliza el protocolo Spanning Tree, que permite utilizar redundancias cuando hay múltiples conexiones entre switches (Robles, 2015). Este tema no se abordará a profundidad por encontrarse fuera del interés.

J. INSTANCIAS DE RUTEO EN JUNIPER

Una instancia de ruteo se refiere a la virtualización de un equipo físico, lo cual hace que todas sus propiedades sean independientes de otras instancias y de la configuración fuera de estas. Esto es útil porque permite emular varios equipos dentro de un mismo equipo físico, permitiendo una gran flexibilidad del dispositivo. Para cada instancia se crea una colección única y lógica de tablas de ruteo, interfaces y parámetros de protocolos de ruteo. Incluso una misma interfaz física, a través de las interfaces lógicas derivadas de ella, puede formar parte de distintas instancias de ruteo.

Con la finalidad de que la flexibilidad sea mayor, existen distintos tipos de instancias de ruteo en los equipos Juniper, que pueden ser definidas por el administrador, a manera que puedan adaptarse a la aplicación específica. Estas son:

- Forwarding: Utilizada para el envío de datos basado en filtros.
- L2VPN: Empleada para aplicaciones L2VPN. Se excluye MPLS VPLS, ya que existe un tipo de instancia dedicado.
- No-Forwarding: Su fin es separar redes grandes en entidades administrativas pequeñas.
- Virtual-router: Empleada para aplicaciones no relacionadas a conectividad VPN, como virtualización del equipo.
- Vpls: Utilizada para implementaciones LAN punto-multipunto remotas entre distintos sitios dentro de una VPN.
- Vrf (Virtual routing and forwarding): Su uso es para implementaciones L3VPN. Se muestra en la figura un ejemplo de este tipo y la configuración de la interfaz asociada.

Existen dos parámetros utilizados dentro de las instancias de ruteo que especifican conectividad por medio de una implementación VPN; Route-Distinguisher y VRF-Target. En el caso de Route-Distinguisher, este es utilizado para especificar una dirección única dentro de la red MPLS. Consta de dos partes, el primer bloque es la IP de conectividad del equipo de borde y el segundo es un identificador único de la ruta. Esto conforma la denominada dirección VPNv4. De esta forma estos equipos pueden identificar de donde proviene un paquete y a que instancia de ruteo pertenece, haciéndolo único dentro de la red MPLS. VRF-Target es útil para determinar los prefijos que pueden importarse y exportarse del equipo de borde en función de la instancia de ruteo, desde la tabla de rutas del equipo. Estos dos parámetros realizan funciones que aseguran la virtualización de los servicios (Robles, 2015).

K. MONITOREO DE DESEMPEÑO EN TIEMPO REAL

Existen infinidad de herramientas de monitoreo, las cuales son útiles para poder reducir la cantidad de tiempo de impacto de servicios, al realizar acciones correctivas de manera proactiva. RPM es una estas herramientas y puede ser implementado en equipos Juniper. Utilizando RPM es posible configurar pruebas llamadas sondas hacia una ip objetivo con el fin de monitorear una conexión, y determinar cuál es el o los factores que están afectando su comportamiento, tales como

pérdida de paquetes, el tiempo de viaje de ida y vuelta conocido como RTT, y jitter es la diferencia entre el RTT mínimo y máximo medidos durante una prueba RPM. Para la obtención de los datos pueden ser utilizadas solicitudes GET de HTTP, ICMP, TCP y UDP; sin embargo, para este trabajo son de interés únicamente las solicitudes ICMP, específicamente ICMP-ping (a través de direcciones IPv4), puesto que el interés está focalizado en garantizar la conectividad de un servicio punto a punto, donde, por lo general, los equipos destino son propiedad del cliente (Robles, 2015).

A continuación, se detallan los componentes de una configuración RPM.

- Sonda de RPM (RPM Probe): Permite obtener estadísticas de desempeño con respecto a un destino de la sonda (probe target) identificado por medio de una dirección IP o una dirección URL. Cuando el objetivo recibe la sonda, el mismo responde al dispositivo que la genera.
- Prueba de RPM (RPM Test): Una prueba RPM es parte de una sonda y monitorea un cada destino de la misma. Una sonda puede tener una prueba RPM configurada por destino a monitorear, por lo que una sonda podría definirse también como un conjunto de pruebas individuales, por ejemplo, un conjunto de pruebas de ping. Dicho esto, una prueba de RPM (test) suele contener un conjunto de probes (pruebas de ping) y una sonda (Probe) contiene un conjunto de pruebas RPM (Tests). De las pruebas RPM puede obtenerse estadísticas como desviación estándar y jitter.
- Intervalos de Pruebas RPM (Test) y de pruebas individuales (probes): Dentro de una prueba de RPM, las pruebas individuales son enviadas a intervalos de tiempo determinados y configurables en segundos. Cuando el número total de pruebas individuales es enviado dentro de los intervalos de tiempo especificados, una prueba RPM (test) se completa. El inicio de la siguiente prueba RPM (test), depende del intervalo de tiempo configurado en segundo entra cada prueba RPM (test).
- Cliente RPM: Es el dispositivo que realiza la solicitud de RPM.
- Servidor RPM: Es el dispositivo al cual se le hace la solicitud.
- Estadísticas de RPM: Al final de cada prueba RPM, el dispositivo colecciona estadísticas que permiten obtener el monitoreo de nivel. Dentro de las más importantes se encuentran RTT mínimo, RTT máximo, RTT promedio, RTT desviación estándar, Jitter, conteo de pruebas, porcentaje de pérdida, umbral y trampas RPM.

L. ITIL

Esta es la librería de información, tecnología e infraestructura, su función es definir la estructura organizacional y las habilidades requeridas de una organización de tecnologías de la información, así como establecer un conjunto de procedimientos y prácticas de gestión estándar operacional, a manera de permitir la gestión de una operación informática y su infraestructura asociada. Todos estos procedimientos y prácticas operacionales se aplican a todos los aspectos dentro de la infraestructura de informática y son independientes del proveedor. Para interés de este trabajo, es importante tener claridad en algunos conceptos que se manejarán para la parte del manejo de eventos.

1. Evento.

En términos generales, la definición de evento es algo que ha ocurrido, y en términos de informática, es algo tan simple como un cambio de estado. Se podrían mencionar algunos ejemplos como el incremento de utilización de un servicio del 50% al 60%, que una conexión se haya caído, o que una ruta haya cambiado. De estos ejemplos, podemos observar que los eventos pueden indicar algo que es usual, inusual o algo que es definitivamente una excepción. Al llevarse a cabo un evento usual, se dice que tiene una significancia informativa; uno inusual, tiene significancia de advertencia; y uno excepcional tiene significancia de un error, y está operando por debajo de los parámetros aceptables. Esto tiene un significado muy importante para la gestión de servicios, puesto que son el punto de partida para determinar la necesidad de realizar alguna acción; algunos requerirán acciones y otros, no (Agrassala, 2016).

2. Incidente.

Normalmente un incidente se conoce como algo que acontece mientras que transcurre un asunto, relato, etc., y que tiene una repercusión, alterándolo o interrumpiéndolo. Según ITIL, un incidente es una interrupción no planificada de un servicio de informática, la reducción de la calidad o la falla de un elemento de configuración CI por sus siglas en inglés, que se refiere a un servicio. De esta manera, todos los incidentes son eventos; sin embargo, no todos los eventos son incidentes (Agrassala, 2016).

3. Prioridad.

La prioridad, por definición, es la preferencia que se tiene de una cosa sobre la otra por su nivel de importancia. Según ITIL, esta se debe medir según dos parámetros: impacto y urgencia.

(Osiatis, 2016). Se puede observar la relación entre estos factores en el Cuadro 1, donde 1 es crítica, 2 es alta, 3 es moderada, 4 es baja y 5 es planeada.

.

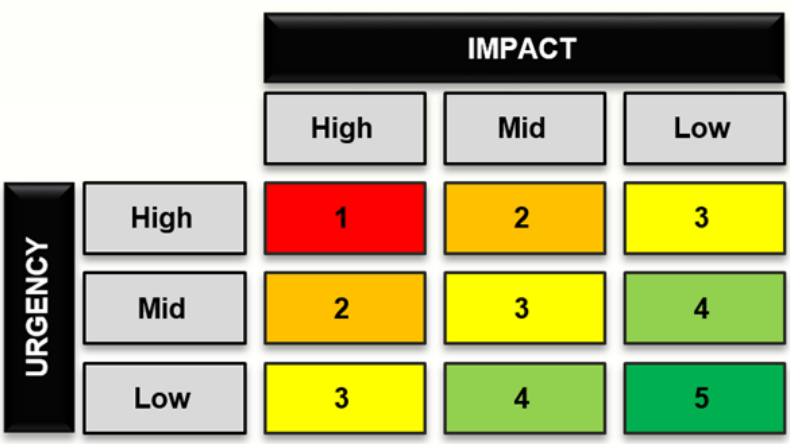
4. Impacto.

Determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados. Está relacionado al alcance de la falla, y qué tanto daño potencial podría llegar a causar. (Zitek, 2016).

5. Urgencia.

Es la medida que indica que tan rápido se requiere que sea la solución de un incidente, determinado por el acuerdo de nivel del servicio, SLA. (Zitek, 2016).

Cuadro 1. Matriz de prioridad según ITIL.

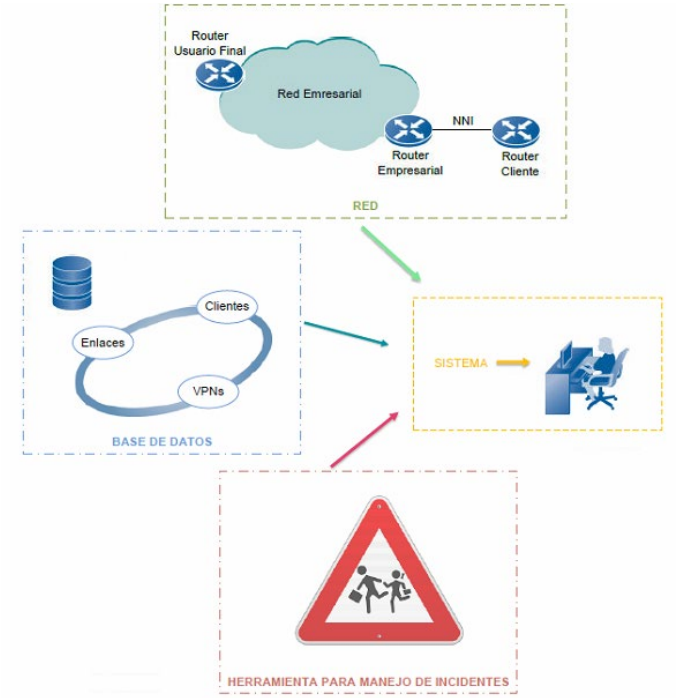


(Zitek, 2016)

VII. DISEÑO EXPERIMENTAL

El trabajo se dividió en tres partes importantes; la primera es la del diseño de la plataforma, la cual se realizó según las necesidades del equipo del trabajo y según la que se creía que era la manera más intuitiva como puede agruparse los enlaces Ethernet e IP. La primera parte implicó un análisis para la definición de la información que se presentaría en cada una de las clasificaciones generales. Para la segunda parte del trabajo, que consiste en la definición de un criterio de aceptación de enlaces Ethernet e IP nuevos para que sean considerados como funcionales, fue necesario definir los parámetros a tener en consideración y los valores aceptables para que tenga un funcionamiento adecuado. Para la tercera parte, que consiste en la parte más relevante del trabajo, se definió un proceso que permitiera utilizar el disparo de alertas generado a partir de un evento detectado en el monitoreo enlaces, para luego pasar por un análisis de la criticidad del enlace y generar acciones dependiendo de la prioridad determinada. En general, se deseaba tener un sistema que pudiese tener acceso a información de la red, de la base de datos de clientes, VPNs y enlaces, y comunicación con la herramienta de manejo de incidentes para poder facilitar el manejo de los eventos.

Figura 14. Integración de información hacia el sistema.



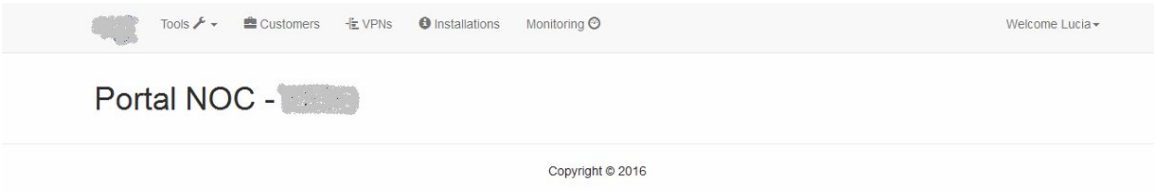
(Elaboración propia)

A continuación, se presenta la manera cómo se realizaron las tres partes.

A. CLASIFICACIÓN DE INTERFACES

La primera parte del trabajo a desarrollar consistía en la definición de las clasificaciones generales de la interface. Se definió que las mismas serían: Enlaces, VPNs, Clientes, Monitoreo y Herramientas. Para las primeras tres clasificaciones, se debió definir el diseño de la vista de búsqueda, y del elemento seleccionado mediante dicha búsqueda.

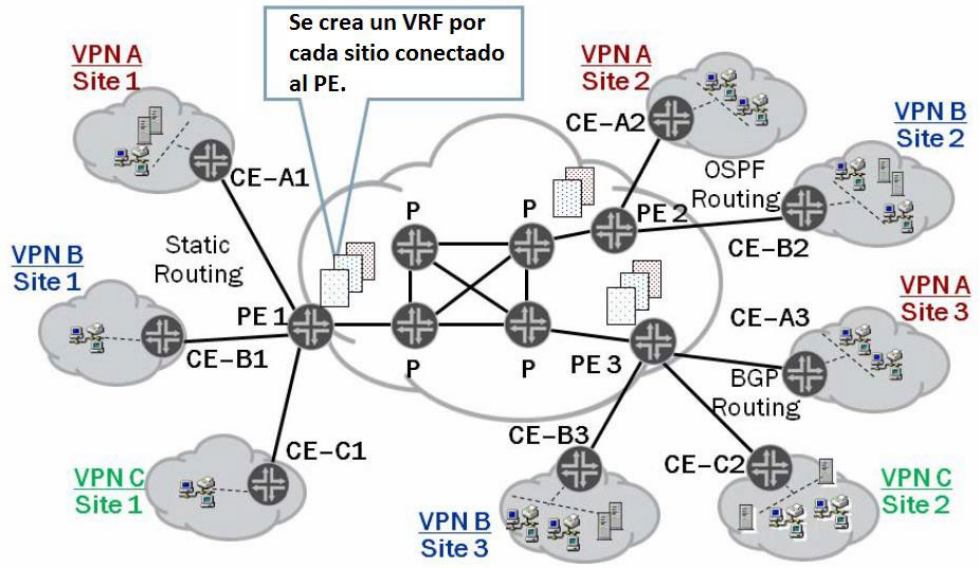
Figura 15. Clasificación de la interface.



(Elaboración propia)

Es importante tomar en cuenta que las clasificaciones de Clientes, VPNs y Enlaces están correlacionadas, dado que se provee a cada cliente diferente VPNs; cada VPN puede ser para un cliente final distinto, y puede estar formada por uno o más enlaces. Esta relación se observa en la Figura 15.

Figura 16. VPNs A, B y C para un solo cliente, donde cada VPN puede ser para diferentes clientes finales, y estar formada por uno o más enlaces.



(Arriola, 2013)

Cada clasificación aparece como una pestaña. El diseño se realizó de la siguiente manera, para cada una de las clasificaciones:

1. Enlaces.

Para esta clasificación se debía definir los elementos en las vistas de búsqueda y del enlace seleccionado mediante la misma. Para la vista de búsqueda, se definió que en el texto aparecería en la parte de arriba lo siguiente:"Búsqueda de Enlaces". Posteriormente, aparecerían las opciones para ingresar los campos de búsqueda, en el siguiente orden:

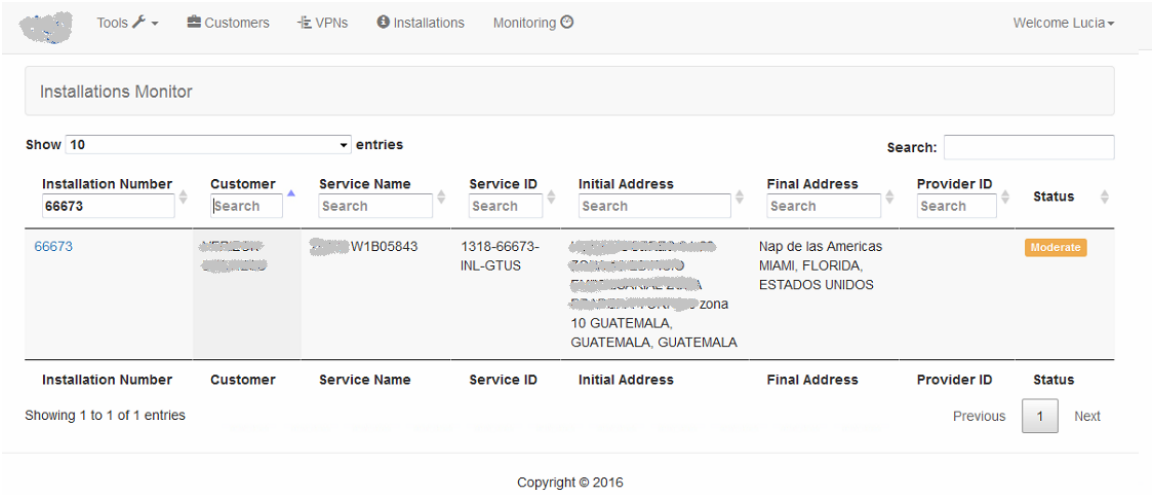
- Número de instalación
- Cliente
- Nombre del enlace
- ID del enlace
- Dirección inicial
- Dirección final
- ID Proveedor

Al realizar una búsqueda se debería mostrar, además de los parámetros para realizar una nueva búsqueda, un listado de los enlaces que coincidan con los parámetros de la búsqueda ordenados en filas. En las columnas del listado, se observaría la información en el siguiente orden:

- Número de instalación
- Cliente
- Nombre del enlace
- ID del enlace
- País inicial
- País final
- Estado

En los estados se vería el color relacionado a la alarma de impacto que se haya definido en la última lectura. Estos pueden ser: para impacto alto, color rojo; para impacto medio, naranja; para impacto bajo, amarillo; sin impacto, color verde; sin monitorear; color gris. Al colocar el cursor sobre el estado del servicio, debería aparecer información sobre el estado, indicando el nivel de impacto que tiene el servicio, o bien que no está monitoreado.

Figura 17. Vista de búsqueda de enlaces



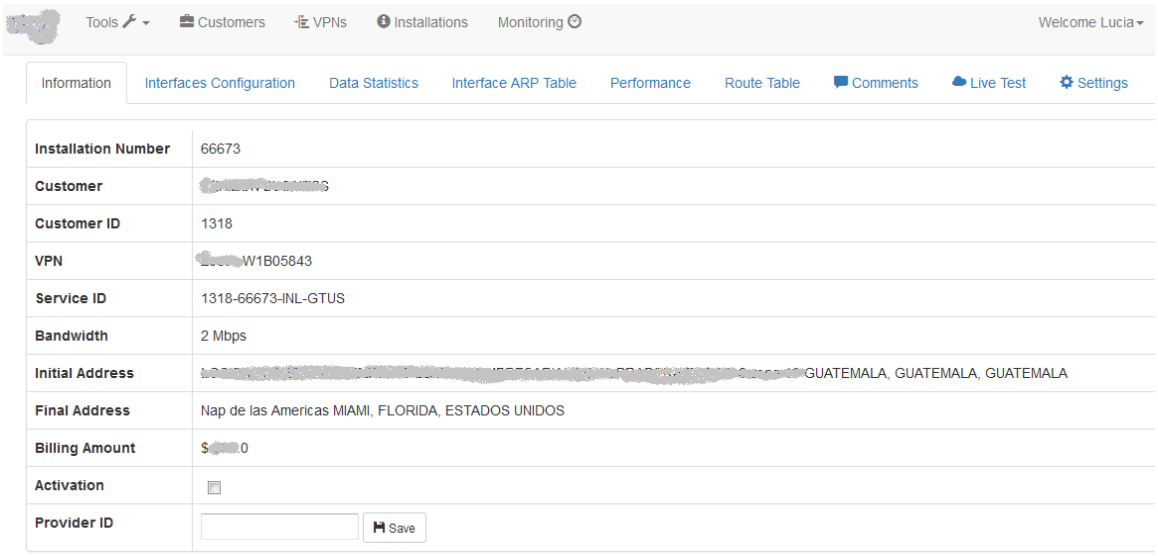
(Elaboración propia)

Al dar clic en el número de instalación de cualquier enlace en el listado, debería aparecer la vista del enlace seleccionado. En dicha vista, se observaría el número de instalación y el cliente en la parte superior. Adicionalmente debería aparecer la siguiente información:

- Número de instalación
- Cliente
- ID del cliente.
- Nombre del enlace
- ID del enlace
- Ancho de banda
- Dirección inicial
- Dirección final
- Monto de Facturación
- Activación
- ID Proveedor
- Comentarios.
- Realizar pruebas
- Abrir un *ticket*

La parte de comentarios e ID proveedor serían modificables, por lo que debería tener a la derecha una opción para editar el texto. En la parte de comentarios se mostraría los mismos en un listado de filas, donde se define la fecha y hora de la última modificación del comentario, y el usuario que lo modificó, y adicionalmente a la opción para editar, debería existir una opción para eliminar el comentario.

Figura 18. Vista del enlace seleccionado



(Elaboración propia)

2. VPN's.

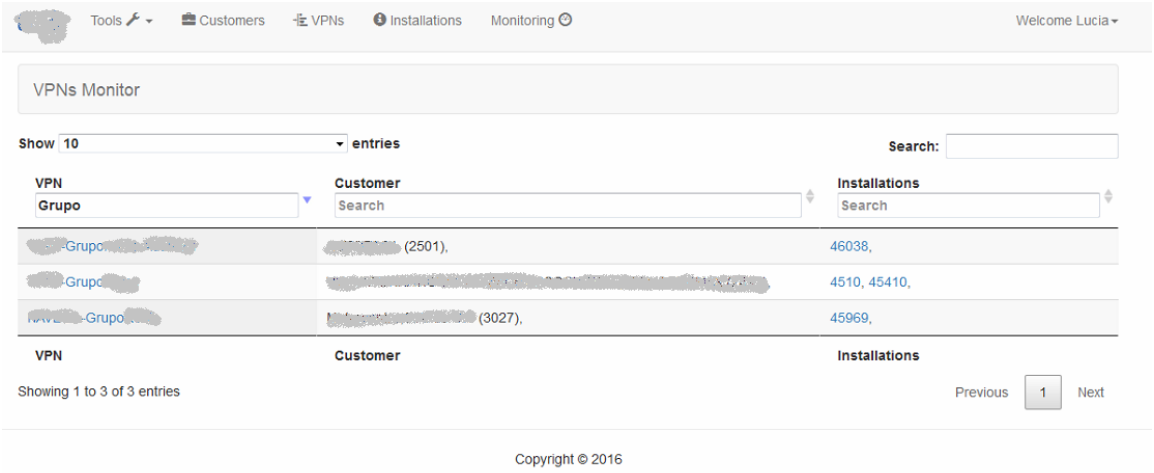
Para esta clasificación se debía definir los elementos en las vistas de búsqueda y de la VPN seleccionada mediante la misma. Para la vista de búsqueda, se definió que aparecería en la parte de arriba el texto "Búsqueda de VPN's". Posteriormente, aparecerían las opciones para ingresar los campos de búsqueda, en el siguiente orden:

- Nombre de la VPN
- Cliente
- Número de instalación asociada

Al realizar una búsqueda se deberá mostrar, además de los parámetros para realizar una nueva búsqueda, un listado de las VPN's que coincidan con los parámetros de la búsqueda ordenados en filas. En las columnas del listado, se observaría la información en el siguiente orden:

- Nombre de la VPN
- Cliente
- Números de instalaciones asociadas

Figura 19. Vista de búsqueda de VPNs.



(Elaboración propia)

Al dar clic en el nombre de cualquiera de las VPN en el listado, debería aparecer la vista de la VPN seleccionada. En dicha vista, se observaría el nombre de la VPN y el cliente en la parte superior. Adicionalmente debería aparecer la siguiente información:

- Nombre de la VPN
- Cliente
- Monto de facturación total de enlaces asociados
- Ir al listado de enlaces asociados
- Comentarios.

Figura 20. Vista de la VPN seleccionada.

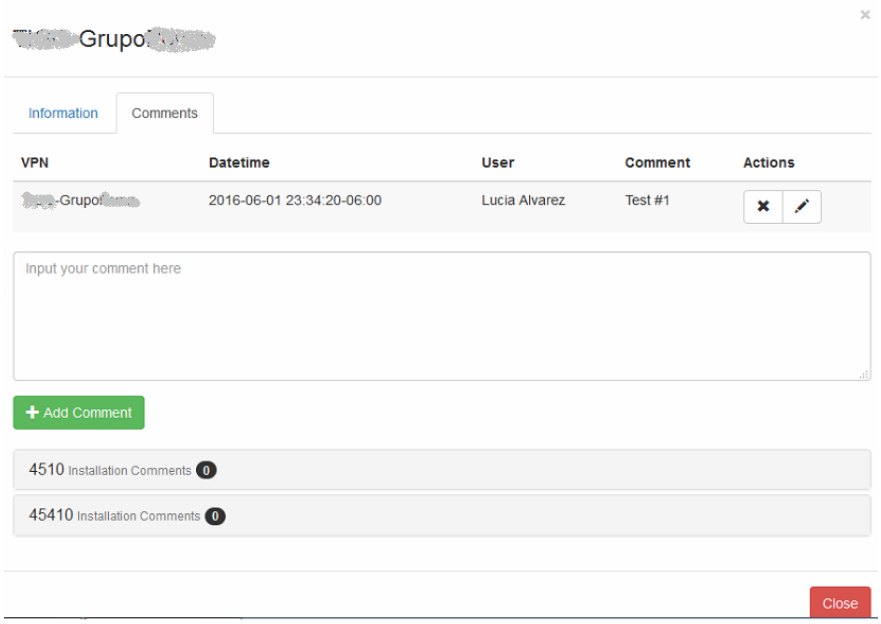
(Elaboración propia)

En la parte de ir al listado de enlaces asociados, debería abrir una ventana nueva, donde se debería mostrar un listado tal como fue definido en la clasificación de enlaces, en la vista de Búsqueda de Enlaces.

Al dar clic en el número de instalación de cualquier enlace en el listado, debería aparecer la vista del enlace seleccionado, tal como fue definido en la clasificación de Enlaces.

En la parte de comentarios se mostraría los mismos en un listado de filas, donde se define la fecha y hora de la última modificación del comentario, el usuario que lo modificó. Esta parte debería ser modificable, por lo que debería aparecer una opción para editar el comentario y otra para eliminarlo.

Figura 21. Vista de comentarios.



(Elaboración propia)

3. Clientes.

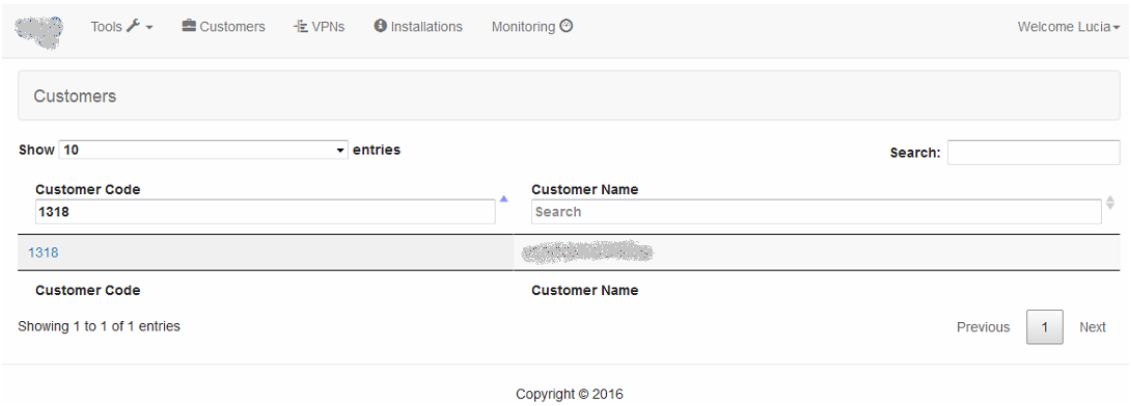
Para esta clasificación se debió definir los elementos en las vistas de búsqueda y del cliente seleccionado mediante la misma. Para la vista de búsqueda, se definió que aparecería en la parte de arriba el texto "Búsqueda de Clientes". Posteriormente, aparecerían las opciones para ingresar los campos de búsqueda en una sola columna, en el siguiente orden:

- Código de cliente
- Cliente

Al realizar una búsqueda se deberá mostrar, además de los parámetros para realizar una nueva búsqueda, un listado de los clientes que coincidan con los parámetros de la búsqueda ordenados en filas. En las columnas del listado, se observaría la información en el siguiente orden:

- Código de cliente
- Cliente

Figura 22. Vista de búsqueda de clientes.

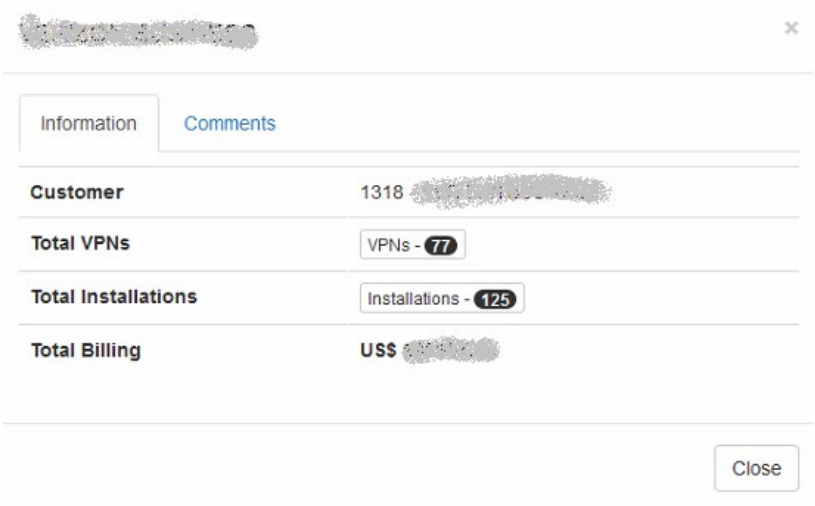


(Elaboración propia)

Al dar clic en el nombre de cualquiera de los clientes en el listado, debería aparecer la vista del cliente seleccionado. En dicha vista, se observaría el código y nombre del cliente en la parte superior. Adicionalmente debería aparecer la siguiente información:

- Cliente
- Cantidad de VPNs asociadas
- Cantidad de enlaces asociados
- Monto de facturación total de instalaciones asociadas
- Comentarios.

Figura 23. Vista del cliente seleccionado.



(Elaboración propia)

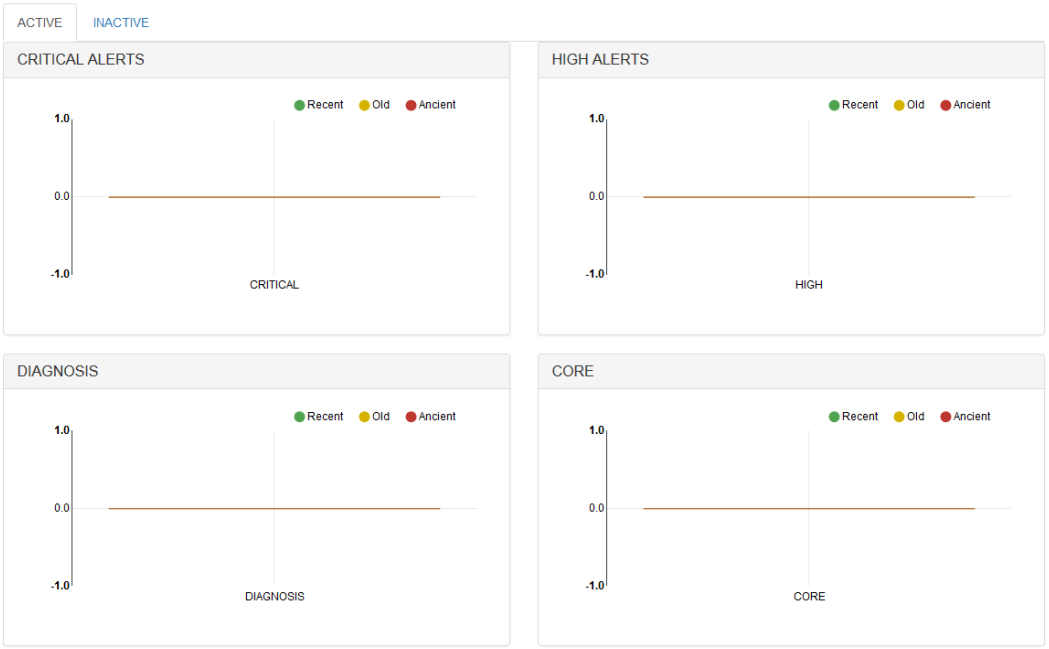
En la parte donde se muestra la cantidad de VPNs y enlaces asociados, debería abrir una ventana nueva, donde se debería mostrar un listado tal como fue definido en la clasificación de VPNs, en la vista de Búsqueda de VPNs, o bien de enlaces según corresponda.

En la parte de comentarios se mostraría los mismos en un listado de filas, donde se define la fecha y hora de la última modificación del comentario, el usuario que lo modificó. Esta parte debería ser modificable, por lo que debería aparecer una opción para editar el comentario y otra para eliminarlo.

4. Monitoreo.

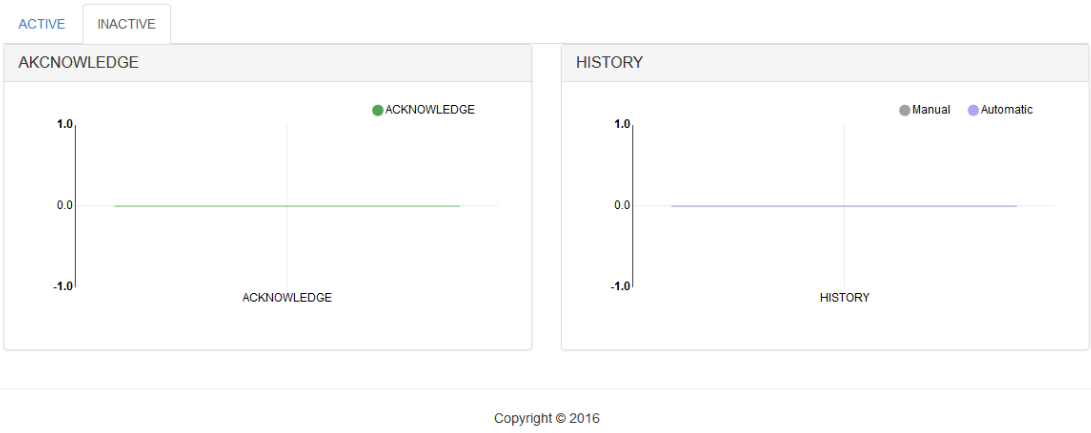
Esta clasificación debería ser un tablero donde haya seis gráficas de barras. La primera y segunda gráfica estarían en la parte superior de la pestaña principal de alarmas activas, mientras que la tercera y cuarta estarían en la parte inferior. La quinta y sexta gráfica deberían estar en la pestaña secundaria de alarmas inactivas, donde estarán las alarmas reconocidas e históricas.

Figura 24. Tablero de monitoreo en la pestaña de alarmas activas.



(Elaboración propia)

Figura 25. Tablero de monitoreo en la pestaña de alarmas inactivas.



(Elaboración propia)

a. Primera gráfica.

En esta gráfica deberían estar las alarmas nuevas con prioridad crítica. Al colocar el cursor sobre la primera gráfica, debería mostrar la descripción de dichas alarmas. Al dar clic, debería aparecer el listado de los enlaces alarmados. En dicho listado, para cada alarma, debería aparecer lo siguiente:

- Número de instalación
- Nombre del cliente
- Recurrencia. (Cantidad de alarmas en las últimas 24 horas)
- Ticket(s) asociado(s), con una "M" si es por una falla general o "C" si es core.
- Equipo origen
- Alarma origen (PCKLOS, DELAY, TRAFF, INTERF, PEER)
- Si es capa 2 o capa 3 (L2, L3).

Al dar clic derecho, deberían aparecer varias opciones en el orden indicado a continuación:

1) Ver resultados de pruebas.

Al dar clic, aparecerán los resultados en una ventana adicional, donde pueden ser seleccionados y copiados.

2) Ir a alguno de los *tickets* asociados.

Esta opción aparecerá únicamente si hay *tickets* asociados. Al dar clic, debería abrir una nueva pestaña con *ticke*t seleccionado en la plataforma de tickets.

3) Reconocer (Acknowledge en inglés).

Al dar clic aquí, debería aparecer un cuadro de diálogo, donde debería poder seleccionarse si se desea que la alerta regrese a la gráfica actual en 12 horas o más. De ser más de 12 horas, debería especificar fecha y hora. Posteriormente, debería desaparecer de esta gráfica, e ir la quinta. Existe también un botón para desactivar que la alerta pase al historial al limpiarse la alarma, y esto se utilizará en caso de que no se requiera que vuelva a realizar todo el flujo cuando se active la alarma nuevamente.

El color de la alerta debería cambiar dependiendo del tiempo que haya transcurrido sin pasar a la quinta gráfica.

t<5minutos: VERDE
5<t<10minutos: AMARILLO
t>10minutos: ROJO

En caso en la siguiente lectura se detecte que el enlace ya no está alarmado, debería ir a la sexta gráfica en color azul. En caso haya un ticket generado, se debería pegar en el ticket una notificación que indique que la alarma ya limpió.

b. Segunda gráfica.

Aquí se deberían mostrar las alertas generadas con prioridad alta. Al colocar el cursor sobre la segunda gráfica, debería mostrar la descripción de dichas alarmas. Al dar clic, debería aparecer el listado de los enlaces alarmados. En dicho listado, debería aparecer lo siguiente:

- Número de instalación
- Nombre del cliente
- Recurrencia. (Cantidad de alarmas en las últimas 24 horas)
- *Ticke*t(s) asociado(s), con una "M" si es por una falla general o "C" si es core.
- Equipo origen
- Alarma origen (PCKLOS, DELAY, TRAFF, INTERF, PEER)
- Si es capa 2 o capa 3 (L2, L3).

Al dar clic derecho, deberían aparecer las siguientes opciones:

1) Ver resultados de pruebas.

Al dar clic, aparecerán los resultados en una ventana adicional, donde pueden ser seleccionados y copiados.

2) Ir a alguno de los *tickets* asociados.

Esta opción aparecerá únicamente si hay *tickets* asociados. Al dar clic, debería abrir una nueva pestaña con *ticket* seleccionado en la plataforma de tickets.

3) Crear *ticke*t nuevo.

Al dar clic en esta opción, debería aparecer un cuadro de diálogo indicando el número de ticket creado, donde se tenga la opción de ir al ticket. Se deberían pegar en el ticket los resultados de la batería de pruebas, la alarma origen y la criticidad de la misma.

4) Iniciar revisión.

Al dar clic aquí, deberá desaparecer de esta tabla e ir la tercera gráfica.

5) Reconocer (Acknowledge en inglés).

Al dar clic aquí, debería aparecer un cuadro de diálogo, donde debería poder seleccionarse si se desea que la alerta regrese a la gráfica actual en 12 horas o más. De ser más de 12 horas, debería especificar fecha y hora. Posteriormente, debería desaparecer de esta gráfica, e ir la quinta. Existe también un botón para desactivar que la alerta pase al historial al limpiarse la alarma, y esto se utilizará en caso de que no se requiera que vuelva a realizar todo el flujo cuando se active la alarma nuevamente.

6) Asociar a un t*icke*t de Falla Core:

Al dar clic, aparece un cuadro de diálogo donde se puede ingresar el número del ticket de falla Core manualmente.

El color de la alerta deberá cambiar dependiendo del tiempo que haya transcurrido sin pasar a la tercera gráfica.

t<10minutos: VERDE
10<t<15minutos: AMARILLO
t>15minutos: ROJO

Si en la siguiente lectura se detecta que el enlace ya no está alarmado, deberá ir a la sexta gráfica en color azul. En el caso de que haya un *ticke*t generado, pegar en el *ticke*t una notificación que indique que la alarma ya limpió.

c. Tercera gráfica.

En la tercera gráfica de barras se mostrará las alertas que están en proceso de diagnóstico por parte del ingeniero. Al colocar el cursor sobre la tercera gráfica, deberá mostrar la descripción de dichas alarmas. Al dar clic, deberá aparecer el listado de los enlaces alarmados. En dicho listado, aparecerá lo siguiente:

- Número de instalación
- Nombre del cliente
- Recurrencia. (Cantidad de alarmas en las últimas 24 horas)
- *Ticke*t(s) asociado(s), con una "M" si es por una falla general o "C" si es core.

- Equipo origen
- Alarma origen (PCKLOS, DELAY, TRAFF, INTERF, PEER)
- Si es capa 2 o capa 3 (L2, L3).

Al dar clic derecho, aparecen las opciones:

1) Ver resultados de pruebas.

Al dar clic, aparecerán los resultados en una ventana adicional, donde pueden ser seleccionados y copiados.

2) Ir a alguno de los *tickets* asociados.

Esta opción aparecerá únicamente si hay *tickets* asociados. Al dar clic, debería abrir una nueva pestaña con *ticket* seleccionado en la plataforma de tickets.

3) Crear *ticket* nuevo.

Al dar clic en esta opción, debería aparecer un cuadro de diálogo indicando el número de *ticket* creado, donde se tenga la opción de ir al ticket. Se deberían pegar en el *ticket* los resultados de la batería de pruebas, la alarma origen y la criticidad de la misma.

4) Enviar correo al cliente.

En este caso se enviará el correo al cliente solicitando revisar y que nos reporte en caso encuentre algún problema: “Estimado Cliente, Se ha verificado que existe un posible problema en el enlace (NOMBRE DEL ENLACE) con ID (ID DEL ENLACE). Por favor apoyarnos realizando revisiones internamente y en caso se detecten inconvenientes con el mismo, por favor realizar un reporte a nuestro grupo de soporte técnico a (CORREO DEL NOC) o al número (NÚMERO DEL NOC).”

5) Reconocer (Acknowledge en inglés).

Al dar clic aquí, debería aparecer un cuadro de diálogo, donde debería poder seleccionarse si se desea que la alerta regrese a la gráfica actual en 12 horas o más. De ser más de 12 horas, debería especificar fecha y hora. Posteriormente, debería desaparecer de esta gráfica, e ir la quinta. Existe también un botón para desactivar que la alerta pase al historial al limpiarse la alarma, y esto se utilizará en caso de que no se requiera que vuelva a realizar todo el flujo cuando se active la alarma nuevamente.

6) Asociar a un *ticket* de Falla Core.

Al dar clic, aparece un cuadro de diálogo donde se puede ingresar el número del ticket de falla Core manualmente.

El color de la alerta deberá cambiar dependiendo del tiempo que haya transcurrido sin pasar a la quinta gráfica.

t<15minutos: VERDE
15<t<20minutos: AMARILLO
t>20minutos: ROJO

En caso en la siguiente lectura se detecte que el enlace ya no está alarmado, deberá ir a la sexta gráfica en color azul. En caso haya un ticket generado, pegar en el ticket una notificación que indique que la alarma ya limpió.

d. Cuarta gráfica.

Esta gráfica debe mostrar las alarmas que se haya detectado que están entre los dos PE. Al colocar el cursor sobre la cuarta gráfica, deberá mostrar la descripción de dichas alarmas. Al dar clic, deberá aparecer el listado de los enlaces alarmados. En dicho listado, aparecerá lo siguiente:

- Número de instalación
- Nombre del cliente
- Recurrencia. (Cantidad de alarmas en las últimas 24 horas)
- *Ticket*(s) asociado(s), con una "M" si es por una falla general o "C" si es core.
- Equipo origen
- Alarma origen (PCKLOS, DELAY, TRAFF, INTERF, PEER)
- Si es capa 2 o capa 3 (L2, L3).

Al dar clic derecho, aparecen las opciones:

1) Ver resultados de pruebas.

Al dar clic, aparecerán los resultados en una ventana adicional, donde pueden ser seleccionados y copiados.

2) Ir a alguno de los *tickets* asociados.

Esta opción aparecerá únicamente si hay tickets asociados. Al dar clic, debería abrir una nueva pestaña con ticket seleccionado en la plataforma de tickets.

3) Crear *ticket* nuevo.

Al dar clic en esta opción, debería aparecer un cuadro de diálogo indicando el número de *ticket* creado, donde se tenga la opción de ir al ticket. Se deberían pegar en el *ticket* los resultados de la batería de pruebas, la alarma origen y la criticidad de la misma.

4) Enviar correo al cliente.

En este caso se enviará el correo al cliente solicitando revisar y que nos reporte en caso encuentre algún problema: "Estimado Cliente, Se ha verificado que existe un posible problema en el enlace (NOMBRE DEL ENLACE) con ID (ID DEL ENLACE). Por favor apoyarnos realizando revisiones internamente y en caso se detecten inconvenientes con el mismo, por favor realizar un reporte a nuestro grupo de soporte técnico a (CORREO DEL NOC) o al número (NÚMERO DEL NOC)."

5) Asociar a un *ticket* de Falla Core.

Al dar clic, aparece un cuadro de diálogo donde se puede ingresar el número del *ticket* de falla Core manualmente.

6) Reconocer (Acknowledge en inglés).

Al dar clic aquí, debería aparecer un cuadro de diálogo, donde debería poder seleccionarse si se desea que la alerta regrese a la gráfica actual en 12 horas o más. De ser más de 12 horas, debería especificar fecha y hora. Posteriormente, debería desaparecer de esta gráfica, e ir la quinta. Existe también un botón para desactivar que la alerta pase al historial al limpiarse la alarma, y esto se utilizará en caso de que no se requiera que vuelva a realizar todo el flujo cuando se active la alarma nuevamente.

El color de la alerta deberá cambiar dependiendo del tiempo que haya transcurrido sin pasar a la quinta gráfica.

t<15minutos: VERDE

15<t<20minutos: AMARILLO

t>20minutos: ROJO

En caso en la siguiente lectura se detecte que el enlace ya no está alarmado, deberá ir a la sexta gráfica en color azul. En caso haya un *ticket* generado, pegar en el ticket una notificación que indique que la alarma ya limpió.

e. Quinta gráfica.

En esta gráfica aparecerán las alarmas que ya hayan sido reconocidas; que ya se haya realizado la acción que se requería y es necesario que ya no esté a la vista en la pestaña principal. Al colocar el cursor sobre la quinta gráfica, deberá mostrar la descripción de dichas alarmas. Al dar clic, deberá aparecer el listado de los enlaces alarmados. En dicho listado, aparecerá lo siguiente:

- Número de instalación
- Nombre del cliente
- Recurrencia. (Cantidad de alarmas en las últimas 24 horas)
- *Ticket*(s) asociado(s), con una "M" si es por una falla general o "C" si es core.
- Equipo origen
- Alarma origen (PCKLOS, DELAY, TRAFF, INTERF, PEER)
- Si es capa 2 o capa 3 (L2, L3).
- Usuario que reconoció la alarma.
- Criticidad de la alarma origen (CRITICAL, HIGH, MEDIUM, LOW)

Al dar clic derecho, aparecen las opciones:

1) Ver resultados de pruebas.

Al dar clic, aparecerán los resultados en una ventana adicional, donde pueden ser seleccionados y copiados.

2) Ir a alguno de los *tickets* asociados.

Esta opción aparecerá únicamente si hay *tickets* asociados. Al dar clic, debería abrir una nueva pestaña con ticket seleccionado en la plataforma de tickets.

3) Crear *ticket* nuevo.

Al dar clic en esta opción, debería aparecer un cuadro de diálogo indicando el número de *ticket* creado, donde se tenga la opción de ir al ticket. Se deberían pegar en el *ticket* los resultados de la batería de pruebas, la alarma origen y la criticidad de la misma.

4) Descartar.

Al dar clic aquí, la alerta deberá pasar a la quinta Gráfica 5.

5) Regresar a gráfica origen.

Al dar clic aquí, la alerta deberá regresar a la gráfica de origen.

f. Sexta gráfica.

Aquí se muestran las alertas que ya no están activas o bien que fueron removidas manualmente desde la Gráfica 5. Estos estarán en gris los que vienen de la quinta gráfica. Estarán en Celeste los que hayan sido removidos automáticamente. Al colocar el cursor sobre la sexta gráfica, deberá mostrar la descripción de dichas alarmas. Al dar clic, deberá aparecer el listado de los enlaces alarmados. En dicho listado, aparecerá lo siguiente:

- Número de instalación
- Nombre del cliente
- Recurrencia. (Cantidad de alarmas en las últimas 24 horas)
- *Ticket*(s) asociado(s), con una "M" si es por una falla general o "C" si es core.
- Equipo origen
- Alarma origen (PCKLOS, DELAY, TRAFF, INTERF, PEER)
- Si es capa 2 o capa 3 (L2, L3).
- Usuario que envió la alarma al historial.
- criticidad de la alarma origen (CRITICAL, HIGH, MEDIUM, LOW)

Al dar clic derecho se deben tener las siguientes opciones:

1) Eliminar del historial.

Esta opción hará desaparecer la alerta del historial.

2) Ver *tickets* asociados.

Verifica los *tickets* que se han abierto para este número de instalación. Mostrará un listado con número de *ticket,* resumen del ticket y fecha de creación.

3) Buscar historial para este servicio.

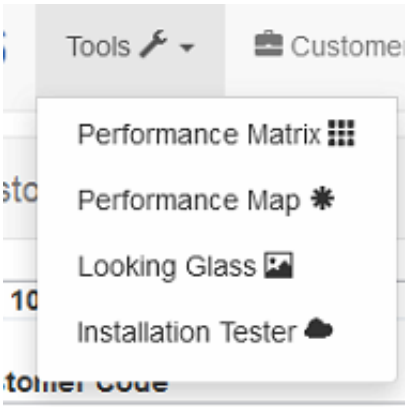
En esta opción se podrá ver las alarmas que se han generado últimamente (últimos 30 días) en la misma vista del listado de alarmas al dar clic sobre la gráfica.

5. Herramientas.

En esta parte se podría tener acceso a algunas herramientas adicionales de la plataforma tales como una matriz de desempeño (Performance Matrix), un mapa de desempeño (Performance Map) y un espejo (Looking Glass), las cuales se encuentran fuera del marco de este trabajo, pero que debían ser incluidas en la misma, por haber sido desarrolladas previamente a este trabajo.

Asimismo, dentro de estas herramientas se incluyó un generador de pruebas sobre un enlace específico, la cual sirve para hacer pruebas sobre un enlace teniendo el número de instalación.

Figura 26. Menú de herramientas.



(Elaboración propia)

B. CRITERIOS DE ACEPTACIÓN PARA ENLACES ETHERNET E IP NUEVOS

En esta parte del trabajo se deseaba establecer los parámetros aceptables para que un enlace Ethernet e IP nuevo pueda considerarse funcional al finalizar la implementación del enlace por

parte del equipo a cargo de esta función. Para esto se determinó que los parámetros a tomar en cuenta serían:

1. Tiempo de respuesta.

Estos tiempos de respuesta dependen de la distancia entre el punto desde donde se genera la prueba hacia el sitio remoto al que estamos intentando alcanzar, y dependen de cada caso en especial. Es importante que quede documentado el tiempo de respuesta al ser un enlace nuevo, puesto que, si el cliente realiza futuros reclamos, se puede utilizar como referencia. Esto deberá quedar documentado en los comentarios de la instalación.

2. Tamaño de paquetes.

Este tamaño de paquete es por default 32 bytes; sin embargo, cuando el cliente requiere utilizar cierto tamaño de paquete debido a alguna aplicación que lo requiera, esto debe ser especificado en los requerimientos del enlace en la orden de compra. Por defecto, el tamaño de paquetes máximo soportado es de hasta 1600 bytes.

3. Ancho de Banda.

Es importante la verificación de que se alcance el ancho de banda contratado debido a que los clientes generalmente tienen aplicaciones que requieren la utilización del mismo, y pueden generarse problemas en caso no se alcance, por lo que es necesario verificar que la configuración del ancho de banda sea correcta y consecuente con lo que aparezca en la información sobre el enlace.

4. Configuración de interfaces para monitoreo.

Es importante que el personal a cargo de la implementación de los circuitos realicen la configuración de la descripción de las interfaces utilizando el estándar que se ha establecido, donde la descripción de interfaces de los PE que ven hacia la central del cliente deben llevar la letra c minúscula seguida del número del cliente, y la descripción de interfaces que vean hacia el sitio remoto, deberán llevar la letra i minúscula, seguida del número de instalación, que es el identificador del circuito.

Cuando se reciba un enlace nuevo, la verificación del funcionamiento del enlace puede realizarse al ingresar a la parte de Herramientas, y luego al generador de pruebas (Installation Tester). Al verificar los parámetros de las interfaces, se deberá marcar la parte de Activación en la

vista del enlace a través de la clasificación de Enlaces, y en los comentarios deberá quedar documentado los tiempos de respuesta alcanzados, el MTU máximo soportado y el ancho de banda configurado en las interfaces.

C. MANEJO DE EVENTOS

Para el manejo de eventos, se propuso utilizar el esquema de prioridad, definido por impacto y urgencia. El impacto de los enlaces está relacionado con el tipo de evento generado, y la urgencia, con el tipo de servicio que está siendo impactado.

1. Categorías de urgencia de eventos.

Para poder determinar la urgencia de un evento, se realizó un análisis en conjunto con el equipo de trabajo, y se determinó que los parámetros a tomar en cuenta serían el ancho de banda, el monto de facturación de los enlaces y la utilización que dará el cliente final. Para esto se utilizó tres clasificaciones; Diamante para los servicios más importantes, Oro para los servicios con importancia moderada, y Plata para los servicios con menor urgencia.

A continuación, se describen estas clasificaciones.

a. Importancia alta (Diamante).

El daño podría crecer rápidamente. El trabajo que no podría ser completado por el cliente es altamente sensible al tiempo. Un incidente menor puede ser prevenido de ser un incidente mayor si se actúa rápidamente. Varios usuarios con estado VIP están siendo afectados.

b. Importancia media (Oro).

El daño potencial del evento crece considerablemente con el tiempo. Un usuario importante está afectado.

c. Importancia baja (plata).

El daño causado por el incidente, crece con el tiempo, solo marginalmente. El trabajo que no se puede realizar por el cliente no es sensible al tiempo.

2. Categorías de impacto de eventos.

Para poder determinar el impacto que se debía relacionar a cada evento, se realizó la relación con el impacto de incidentes que describe ITIL (Kempter, 2016).

A continuación, se describen los niveles de impacto definidos para los eventos.

a. Baja

El disparo del evento supone un daño potencial bajo, dado que un número mínimo de personas se verían afectadas y/o en condiciones de poder brindar un servicio aceptable con esfuerzo extra. La cantidad de clientes que se podrían ver afectados y/o con inconvenientes no es significativa. El posible impacto financiero es probable que sea bajo y el daño a la reputación del negocio es mínimo.

b. Media.

Un número moderado de personas o clientes podrían verse afectadas o bien no podrían completar su trabajo apropiadamente. El impacto financiero no sería alto, pero sí considerable, y el posible daño a la reputación del negocio es moderado.

c. Alta.

El disparo del evento supone un daño potencial alto, dado que un número extenso de personas podrían estar afectadas y no poder realizar su trabajo. Un número extenso de clientes estarían afectados y/o en una gran desventaja de alguna manera. El impacto financiero podría ser muy alto y el posible daño a la reputación del negocio es muy alto. Alguien podría resultar lastimado.

3. Pruebas en capa 3 e impacto.

Estas pruebas se basan en los resultados del RPM configurado previamente en los enlaces IP de capa 3. Los parámetros que se deben tomar en cuenta son la pérdida de paquetes y el tiempo de viaje de ida y vuelta.

A continuación, se amplía la información sobre los umbrales tomados en cuenta.

a. Pérdida de paquetes.

Al verificar que existe algún paquete perdido en el último grupo de pruebas de RPM realizadas, se procede de la siguiente manera que se observa en el Cuadro 2.

Cuadro 2. Umbrales para definir el impacto de los eventos de pérdida de paquetes.

Prueba realizada	% Pérdida de paquetes (PL)	Siguiente paso
RPM	0%<PL<=5% PL>=5%	Ninguno Realizar prueba de Ping enviando 10 paquetes.
Ping 10 paquetes	0%<PL<=5% 5%<PL<=35% 35%<PL<=99% PL=100%	Realizar prueba de Ping enviando 500 paquetes. Categorizar como evento de impacto bajo Categorizar como evento de impacto medio Categorizar como evento de impacto alto
Ping 500 paquetes	0%<PL<=5% 5%<PL<=35% 35%<PL<99% PL=100%	Realizar prueba de Ping enviando 500 paquetes. Categorizar como evento de impacto bajo Categorizar como evento de impacto medio Categorizar como evento de impacto alto

(Elaboración propia)

b. Tiempo de viaje de ida y vuelta.

Cada servicio tiene normalmente un tiempo de viaje promedio, que varía dependiendo de la distancia entre ambos puntos, donde se genera la prueba y donde finaliza. Se definieron umbrales para determinar el impacto del evento disparado por esta característica de la manera que se observa en el Cuadro 3.

Cuadro 3. Umbrales para definir el impacto de los eventos de tiempo de viaje de ida y vuelta.

Tiempo de viaje promedio (RTT) normal	Porcentaje de retraso sobre RTT normal (D)	Siguiente paso
RTT =< 30 ms	10%< D =<20% 20%< D =<50% D>50%	Categorizar como evento de impacto bajo Categorizar como evento de impacto medio Categorizar como evento de impacto alto
30 ms < RTT =< 50 ms	10%< D =<15% 15%< D =<40% D>40%	Categorizar como evento de impacto bajo Categorizar como evento de impacto medio Categorizar como evento de impacto alto
51 ms < RTT	10%< delay =<15% 15%< delay =<30% delay>30%	Categorizar como evento de impacto bajo Categorizar como evento de impacto medio Categorizar como evento de impacto alto

(Elaboración propia)

4. Pruebas en capa 2 e impacto.

Estas pruebas se basan en los resultados del monitoreo de capa 2, configurado previamente en los enlaces Ethernet de capa 2. Los parámetros que se deben tomar en cuenta son el incremento y caída de tráfico, caída de interfaces y cambios en los *peerings*.

a. Tráfico.

Este es un indicador importante, dado que generalmente al no haber tráfico, esto supone un posible problema. Sin embargo, es importante notar que, en la mayoría de los enlaces, el tráfico sube en horas hábiles, pero fuera de horario laboral se mantiene bajo. Los umbrales se definieron de la siguiente manera.

Cuadro 4. Umbrales para definir el impacto del comportamiento del tráfico.

Evento	Acción a realizar
Tráfico debajo de 100 bps	Revisar MAC Address
No hay MAC address en alguno de los extremos	Categorizar como evento de impacto alto
Tráfico sobre el 95%	Categorizar como evento de impacto bajo

(Elaboración propia)

b. Estado de interfaces.

El estado de la interface nos dice mucho acerca del estado de un enlace que esté configurado en ella. Por ello se definió que, al detectar el evento de la caída de una interface, se categorizará como un evento de impacto alto.

c. Estado de VPLS.

El estado de la VPLS determina si el servicio capa 2 está funcionando correctamente o no, de una manera muy directa. Por eso se definió que, al detectar el evento de la caída de una VPLS, se categorizará como de impacto alto.

5. Flujo de la alerta.

A partir de que se dispara un evento en un enlace, dependiendo de su impacto y urgencia se le asigna una prioridad. Dependiendo de la prioridad del evento, se definió un flujo a seguir, el cual se describe a continuación.

a. Primer paso.

Se envía un correo. En este momento aún no aparece en el tablero de monitoreo. El correo dirá lo siguiente: Estimado Cliente, Se ha detectado un posible problema en el enlace (nombre del enlace) con número de identificación (número de instalación). En estos momentos está siendo revisado por nuestro personal. En caso de encontrar algún inconveniente, le estaremos informando al respecto lo antes posible. Por cualquier consulta adicional, por favor comunicarse con nuestro grupo de soporte a (correo electrónico) o al número (número de teléfono).

b. Segundo paso.

Se genera la batería de pruebas capa 2 o capa 3 dependiendo del enlace.

c. Tercer paso.

Dependiendo de la prioridad de la alerta, se generan las siguientes acciones:

1) Prioridad crítica.

Se crea un incidente en la herramienta de manejo de incidentes con prioridad alta. Se pegan en el incidente los resultados de la batería de pruebas, la alarma origen y la criticidad de la misma. El evento se observa en la primera gráfica del tablero.

2) Prioridad alta.

El evento se observa en la segunda gráfica del tablero. Esta gráfica requiere atención inmediata de un ingeniero, quien deberá revisarla y pasarla a la tercera gráfica.

3) Prioridad moderada y baja.

En este caso, se deberá analizar si el problema está en el segmento local de cada extremo del enlace o bien en el Core. Para eso, para los servicios capa dos, se verificará si la vpls está down, si es así, se categoriza como un evento de Core. En capa 3, se deberá verificar si se alcanza el PE remoto, si no se alcanza, o tiene pérdidas, es problema de Core. Si es problema de Core, el evento deberá aparecer en la cuarta gráfica, en este punto un ingeniero debería revisar la falla para que si lo considera prudente, se genere un ticket de falla Core. De lo contrario se envía un correo al cliente con un aviso y pasa a la quinta gráfica sin realizar ninguna acción adicional.

4) Prioridad planeada.

En este caso no se realizan acciones.

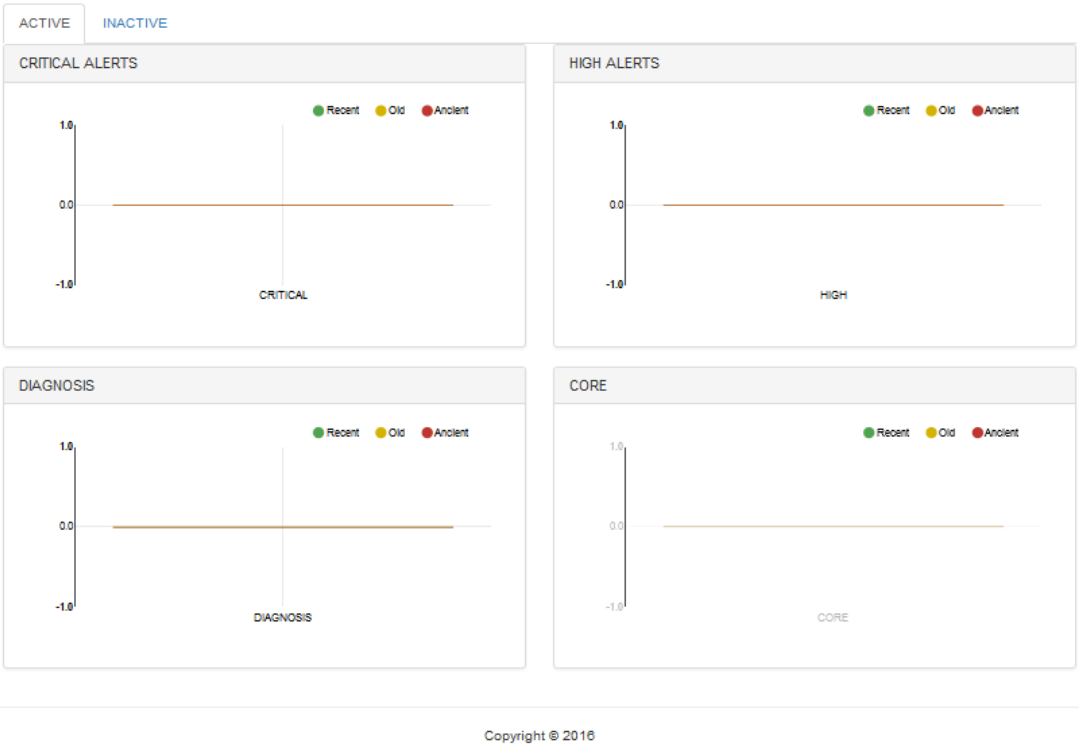
VIII. RESULTADOS

A. Clasificación de interfaces.

En la primera parte de resultados se pretende mostrar la presentación diseñada para la clasificación de la plataforma. Las cinco clasificaciones mencionadas, Enlaces, VPNs, Clientes, Herramientas y Monitoreo, se muestran en pestañas.

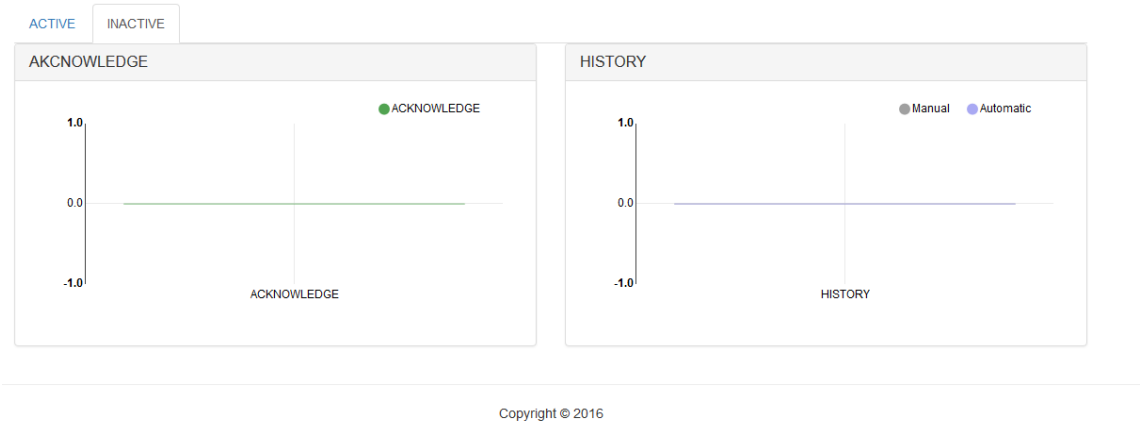
En la pestaña de monitoreo se observan las dos pestañas de alarmas activas generadas por eventos, y la de inactivas, tal como se ve en la Figura 27 y Figura 28.

Figura 27. Clasificación de monitoreo en la pestaña de alarmas activas.



(Elaboración propia)

Figura 28. Clasificación de monitoreo en la pestaña de alarmas inactivas.



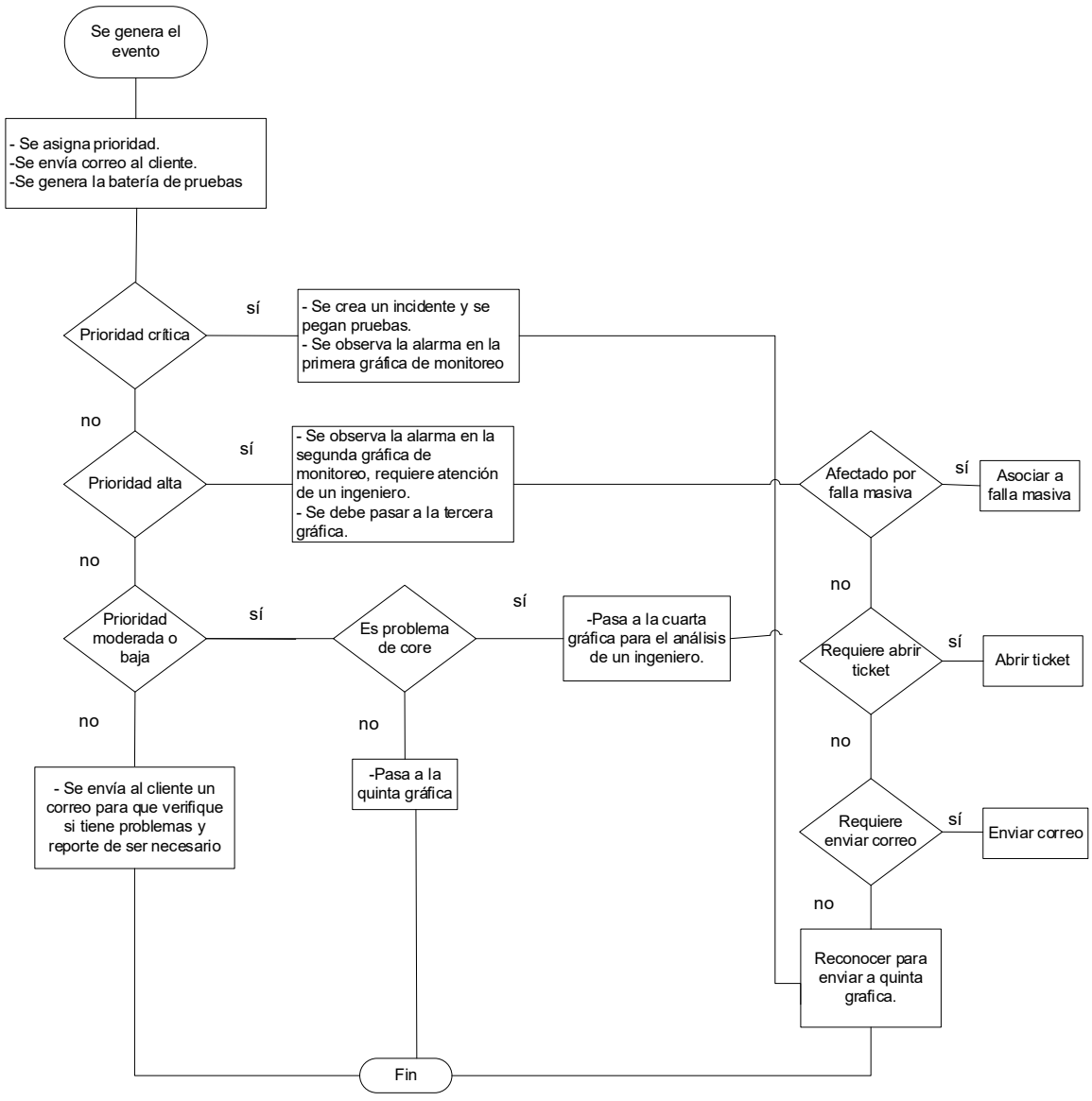
(Elaboración propia)

B. Flujo del evento.

El manejo del evento comienza desde el momento en que se genera el mismo. Al generarse, se realiza un análisis sobre el impacto del mismo y la urgencia del servicio afectado y a través de esto se asigna la prioridad del evento.

En la Figura 29 se observa el flujo de un evento.

Figura 29. Flujo de un evento.

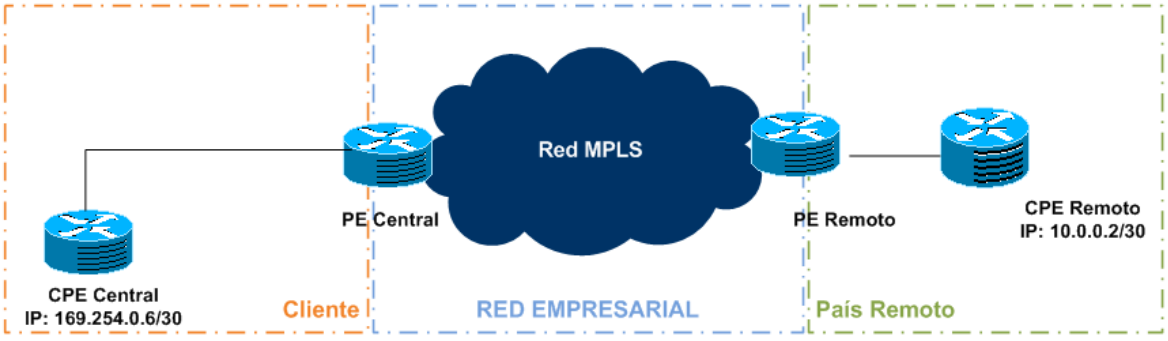


(Elaboración propia)

C. Escenario de pruebas

Con fines de pruebas, se configuró un enlace de pruebas que tiene la topología de la Figura 30.

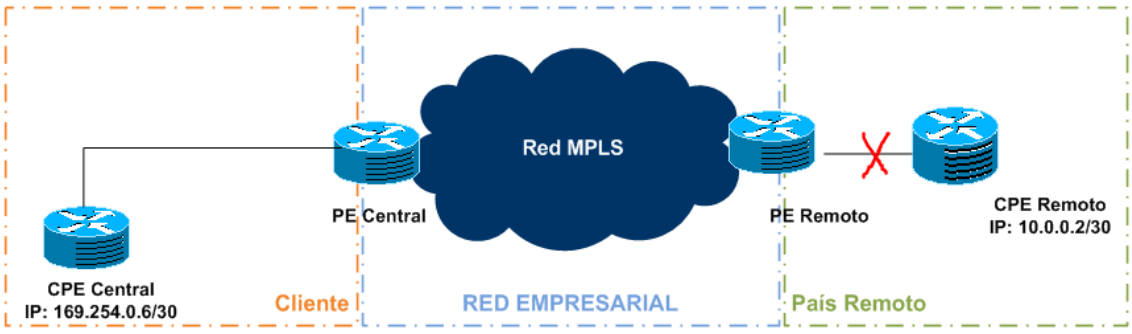
Figura 30. Topología del enlace de pruebas de capa 3.



(Elaboración propia)

Se procede a simular un corte en la parte local del punto remoto del enlace de pruebas, lo cual genera una pérdida de paquetes del 100%, evento de impacto alto.

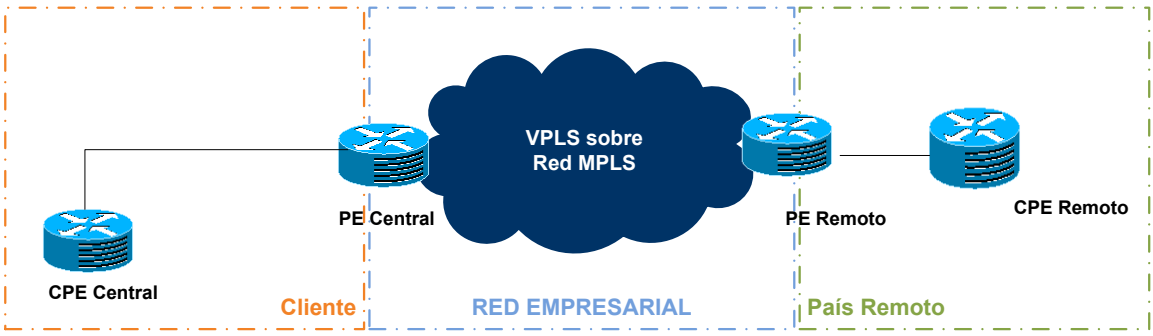
Figura 31. Muestra de escenario de prueba.



(Elaboración propia)

En el caso de un enlace de capa 2, se tiene la topología de pruebas que se observa en la Figura 32.

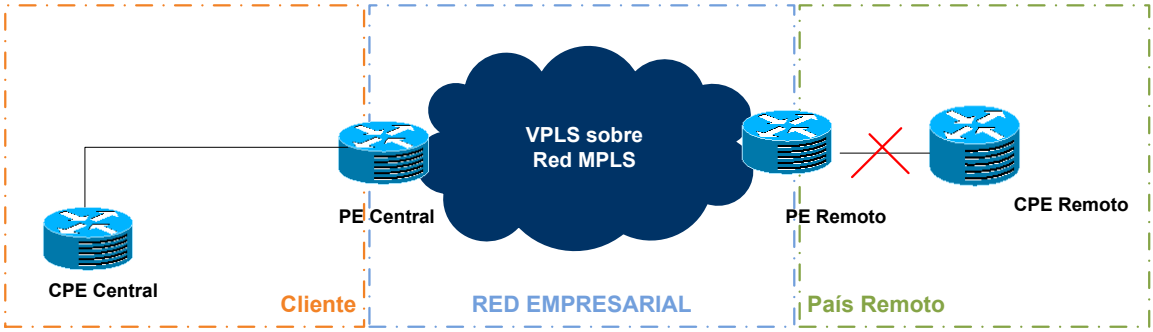
Figura 32. Topología del enlace de pruebas de capa 2.



(Elaboración propia)

Se procede a simular un corte en la parte local del punto remoto del enlace de pruebas, con lo cual dejará de aprenderse las mac address de dicho extremo, como se ve en la Figura 33.

Figura 33. Muestra de escenario de prueba.



(Elaboración propia)

Este evento representa un impacto alto debido a que no hay mac address de uno de los extremos de la VPLS.

1. Prioridad crítica.

Para poder simular un evento con prioridad crítica, se le asigna urgencia alta al enlace.

Figura 34. Urgencia del enlace.

(Elaboración propia)

Se asigna la prioridad al evento dependiendo del impacto y urgencia, en este caso, dado que el impacto del evento simulado es alto y la urgencia del enlace de pruebas es alta, se le asigna una prioridad crítica a la alarma, como se observa en el Cuadro 5.

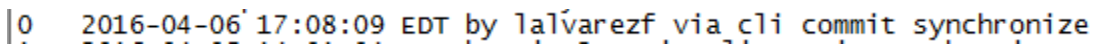
Cuadro 5. Prioridad crítica del evento.

		Impacto		
		Alto	Medio	Bajo
Urgencia	Alta	**Critica**	Alta	Moderada
	Media	Alto	Moderada	Baja
	Baja	Moderada	Baja	Planeada

(Elaboración propia)

Para el escenario de la falla en el enlace capa 3 de la Figura 31, se realizó la desconexión de la interface del equipo que simula ser el CPE Remoto, esto se realizó a las 17:08 GMT-4 del 6 de abril de 2016, como se puede observar en la Figura 24.

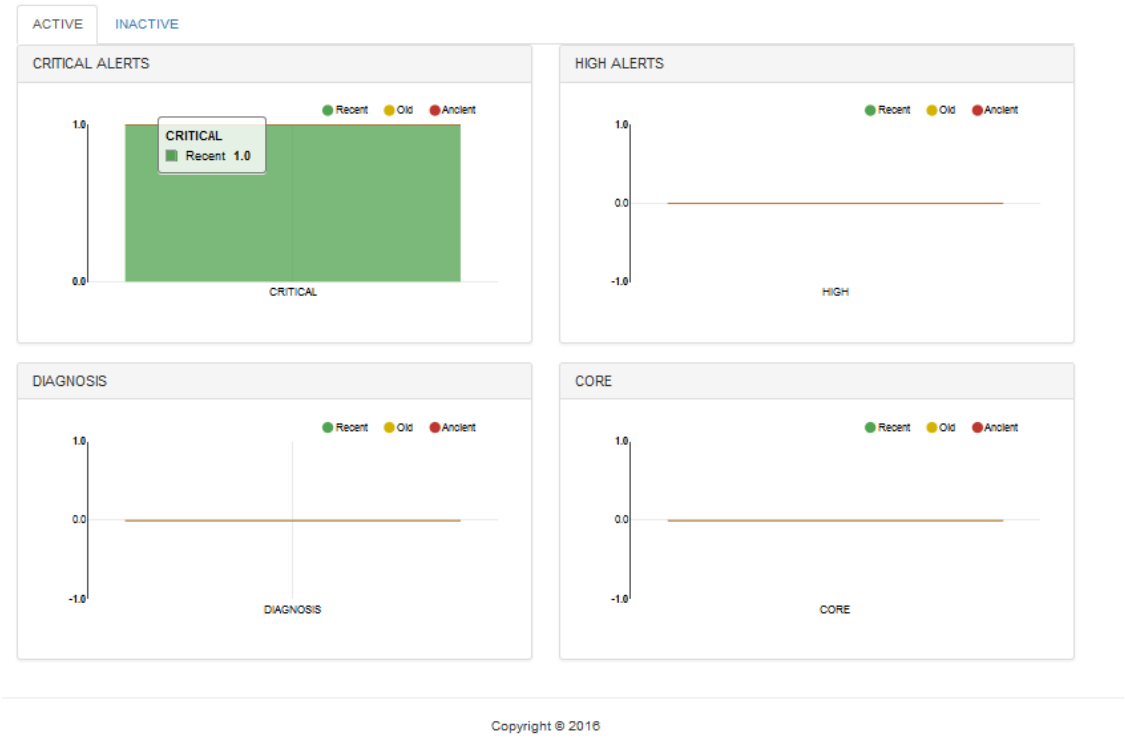
Figura 35. Log del momento en que se realizó la simulación



(Elaboración propia)

Al ser un evento de prioridad crítica, la alarma debería aparecer en la primera gráfica del tablero. Se observa que cerca de 20 minutos después de que se ha producido el evento, aparece la alarma en la primera gráfica del tablero, en color verde como se observa en la Figura 36.

Figura 36. Aparece alarma en la primera gráfica del tablero en color verde.



(Elaboración propia)

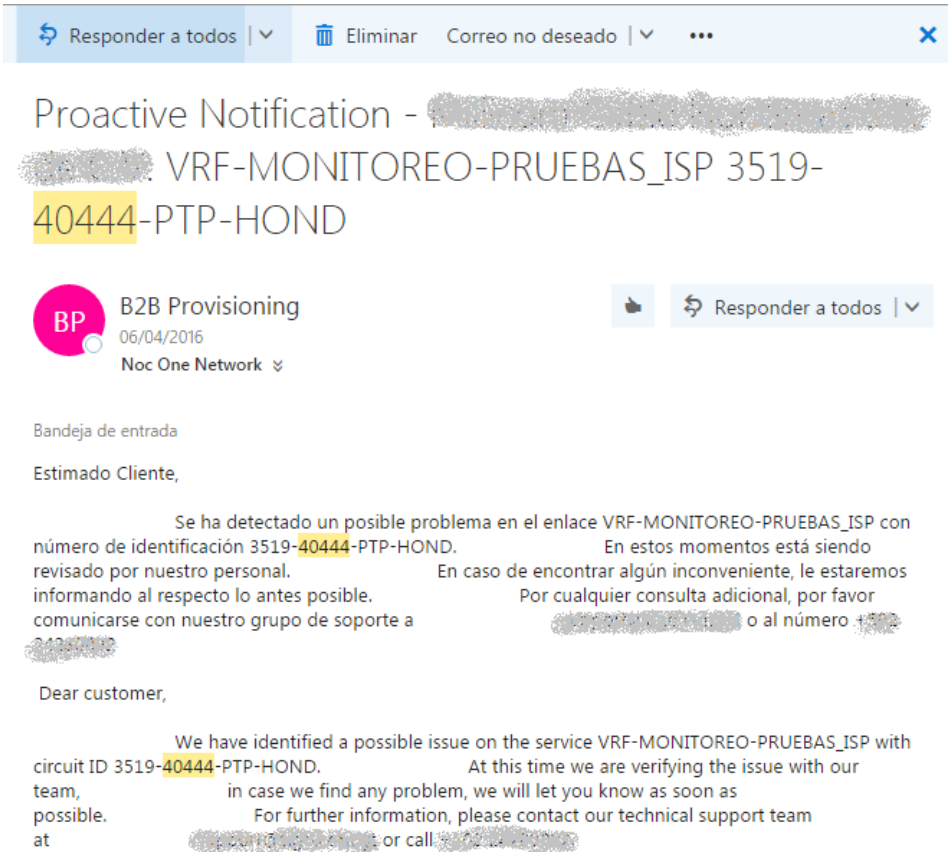
Pocos segundos después se genera el incidente en la herramienta de manejo de incidentes, en la Figura 37 se puede observar la hora de creación del incidente.

Figura 37. Se crea un incidente en la herramienta de manejo de incidentes.

(Elaboración propia)

Se observa también que ha llegado el correo con la notificación a la dirección indicada, tal como se evidencia en la Figura 38.

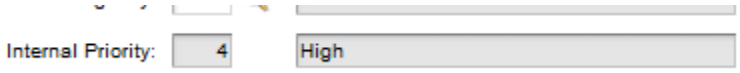
Figura 38. Correo electrónico con la notificación del inicio del incidente.



(Elaboración propia)

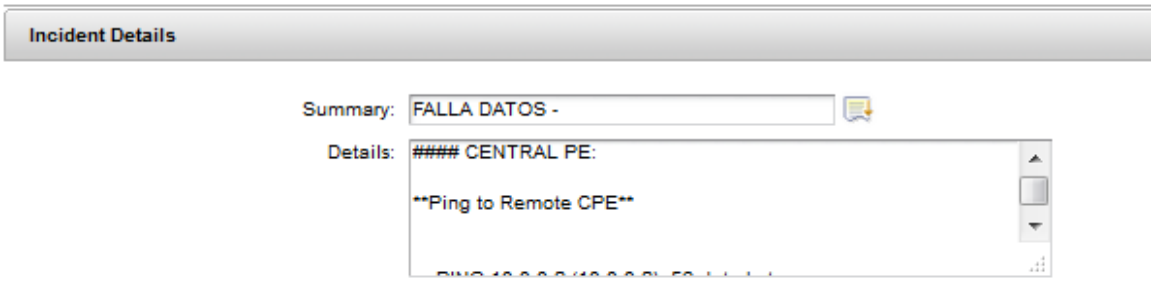
La prioridad del incidente es alta, como se observa en la Figura 32, y se pudo verificar que sí se pegaron las pruebas realizadas por el sistema en el incidente, como se ve en la Figura 39.

Figura 39. Se le asigna prioridad alta al incidente en la herramienta de manejo de incidentes.



(Elaboración propia)

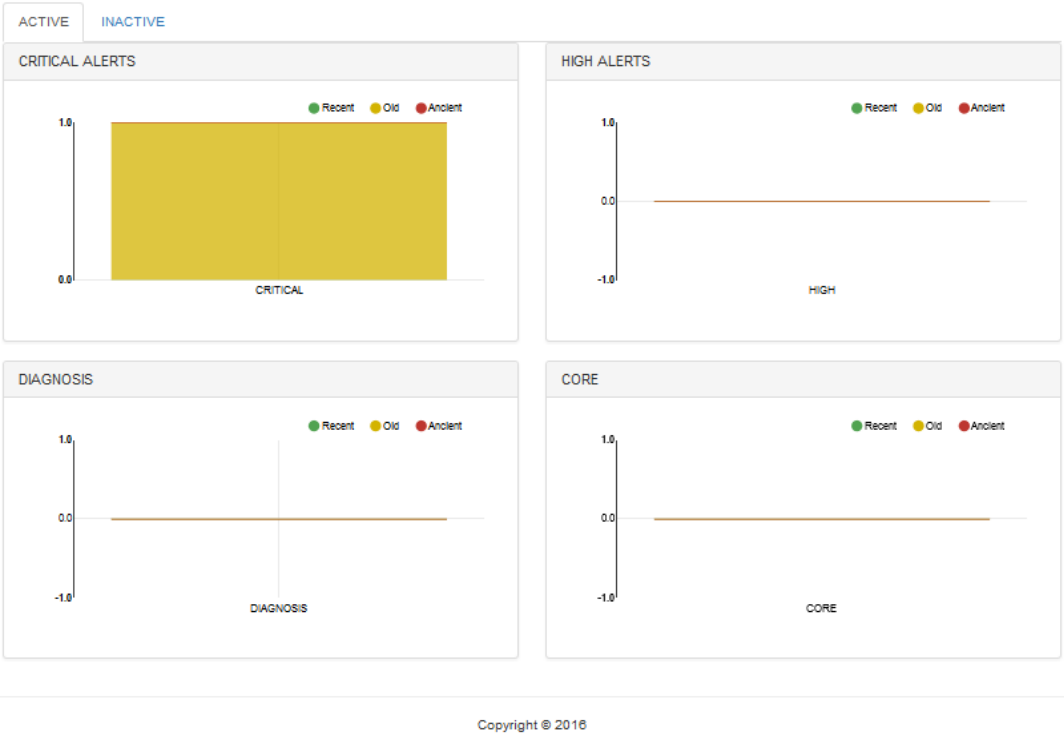
Figura 40. Evidencia de pruebas pegadas en el incidente generado.



(Elaboración propia)

Tal como fue definido, para eventos con prioridad crítica, luego de transcurridos 5 minutos, la alarma se torna de color amarillo en la gráfica, como se puede observar en la Figura 41.

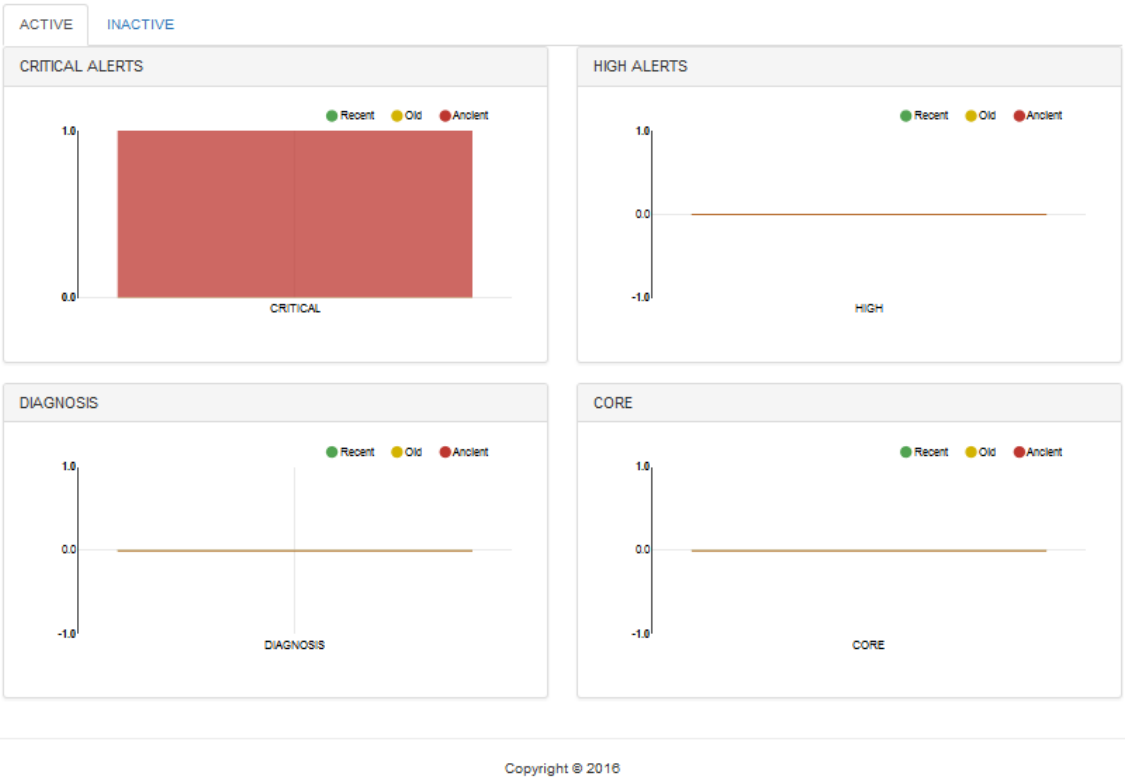
Figura 41. Alarma de evento crítico luego de pasados 5 minutos de haber aparecido en el tablero.



(Elaboración propia)

Asimismo, se observa que al pasar 10 minutos desde que se generó la alarma, sin tomar la acción necesaria, el color de la alarma cambia a rojo, como se observa en la Figura 42.

Figura 42. Alarma de evento crítico luego de pasados 10 minutos de haber aparecido en el tablero.



(Elaboración propia)

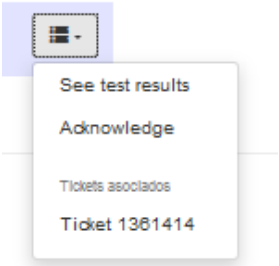
Al dar clic en la primera gráfica, se abre una nueva pestaña donde se encuentra el listado de las alarmas activas para eventos críticos como se puede ver en la Figura 43, donde se observa el ID del servicio o número de instalación, el nombre del cliente, la recurrencia, el equipo desde donde se genera la prueba, la descripción de la alarma, el tipo de servicio y las posibles acciones a realizar.

Figura 43. Listado de alarmas sobre eventos críticos.

(Elaboración propia)

Al dar clic en las acciones del botón que se encuentra a la izquierda, se puede observar que se tiene la opción de ver los resultados de las pruebas, reconocer la alarma, y muestra los incidentes asociados, tal como se observa en la Figura 44.

Figura 44. Posibles acciones de la alarma de evento crítico.

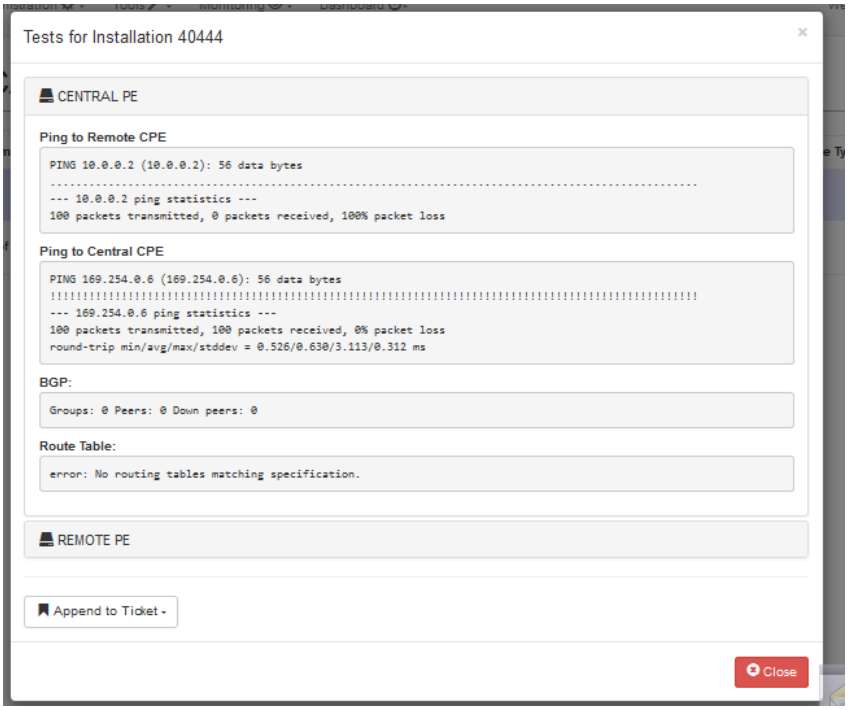


(Elaboración propia)

Si se le da clic en la opción para ver los resultados de las pruebas, se puede observar que se abre una ventana pequeña donde se pueden observar los resultados de las pruebas realizadas desde ambos PE, como se observa la Figura 45.

También se observa que hay una opción para guardar las pruebas realizadas en algún incidente existente.

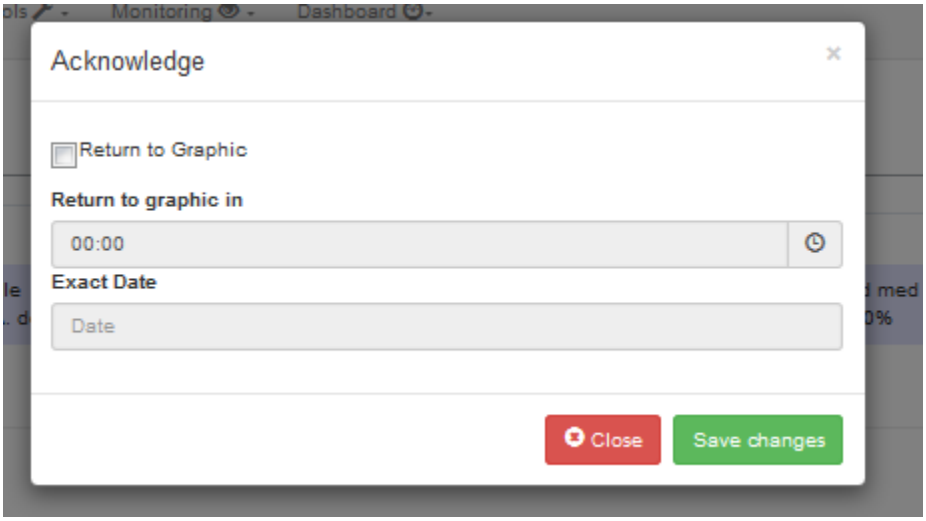
Figura 45. Resultados de pruebas sobre el enlace.



(Elaboración propia)

Al dar clic sobre la opción para reconocer la alarma, se observa que aparece una ventana como la está en la Figura 46, donde se puede seleccionar si se requiere que la alarma regrese a la gráfica de origen, y el momento en que se desea que regrese.

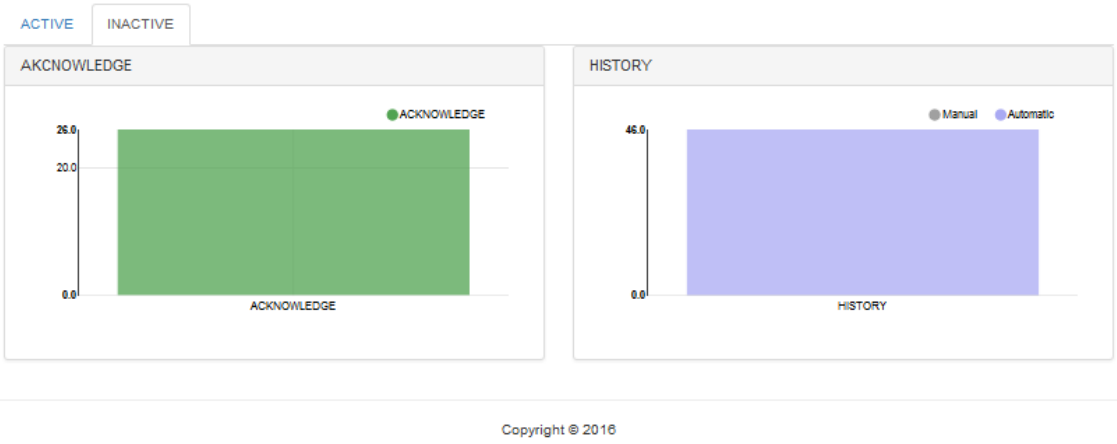
Figura 46. Resultados de pruebas sobre el enlace.



(Elaboración propia)

Al guardar los cambios, la alarma queda reconocida, y pasa a la vista de gráficas inactivas, a la quinta gráfica, como se observa en la Figura 47.

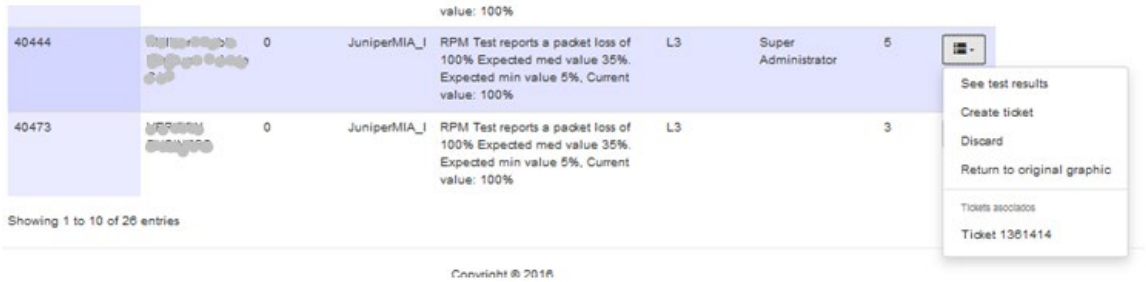
Figura 47. Alarmas reconocidas e historial.



(Elaboración propia)

Al dar clic sobre las alarmas, se abre una nueva pestaña, donde se observa el listado de alarmas reconocidas como se observa en la Figura 48.

Figura 48. Listado de alarmas reconocidas.



(Elaboración propia)

2. Prioridad alta. Para poder simular un evento con prioridad alta, se le asigna urgencia media al enlace, como se observa en la Figura 49.

Figura 49. Urgencia media del enlace.

(Elaboración propia)

De esta manera, al tener un impacto alto y urgencia media, se le asigna una prioridad alta al evento, como se observa en el Cuadro 6.

Cuadro 6. Asignación de prioridad alta para el evento.

		Impacto		
		Alto	Medio	Bajo
Urgencia	Alta	Critico	Alto	Moderado
	Media	**Alto**	Moderado	Bajo
	Baja	Moderado	Bajo	Planeado

(Elaboración propia)

Para el escenario de la falla en el enlace capa 3 de la Figura 31, se realizó la desconexión de la interface del equipo que simula ser el CPE Remoto, esto se realizó a las 21:20:37 GMT-4 del 5 de junio de 2016, como se puede observar en la Figura 50.

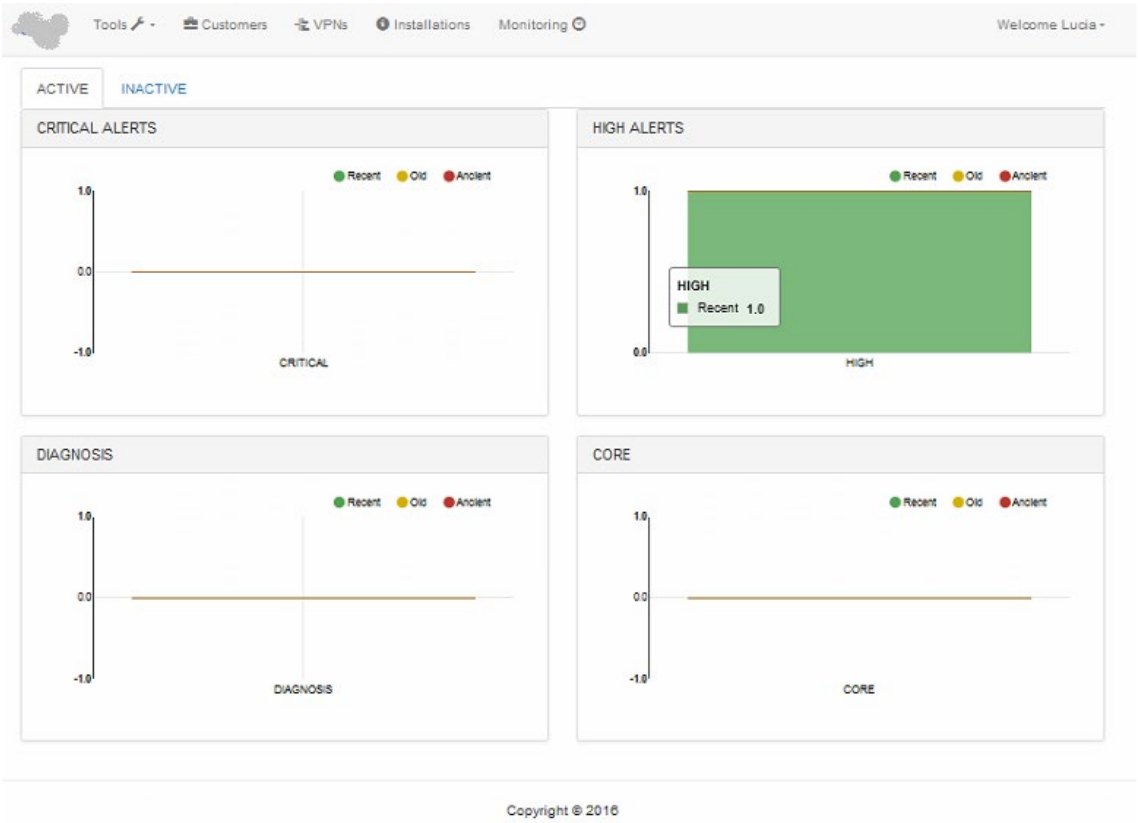
Figura 50. Log del momento en que se realizó la simulación

```
0   2016-06-05 21:20:37 EDT by bramirez via cli commit synchronize
```

(Elaboración propia)

Al ser un evento de prioridad alta, la alarma debería aparecer en la segunda gráfica del tablero. Se observa que cerca de 20 minutos después de que se ha producido el evento, aparece la alarma en la primera gráfica del tablero, en color verde como se observa en la Figura 51.

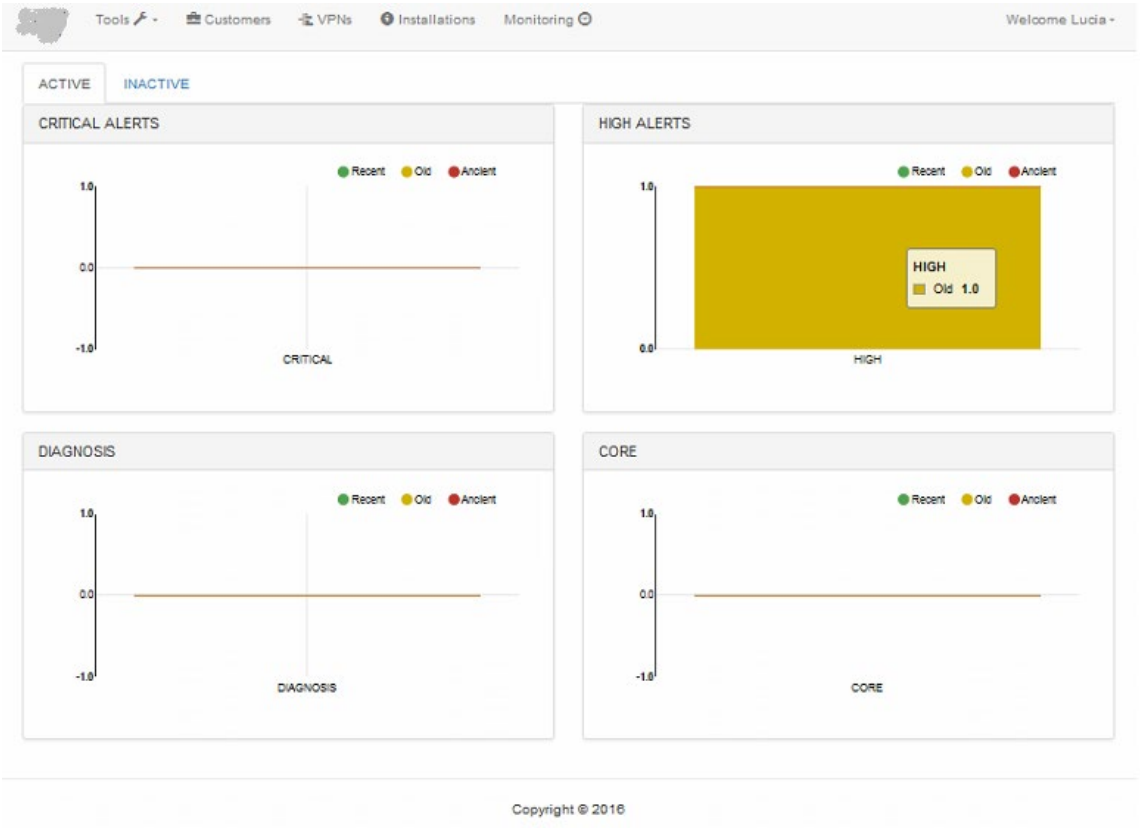
Figura 51. Aparece alarma en la primera gráfica del tablero en color verde.



(Elaboración propia)

Tal como fue definido, para eventos con prioridad crítica, luego de transcurridos 15 minutos, la alarma se torna de color amarillo en la gráfica, como se puede observar en la Figura 52.

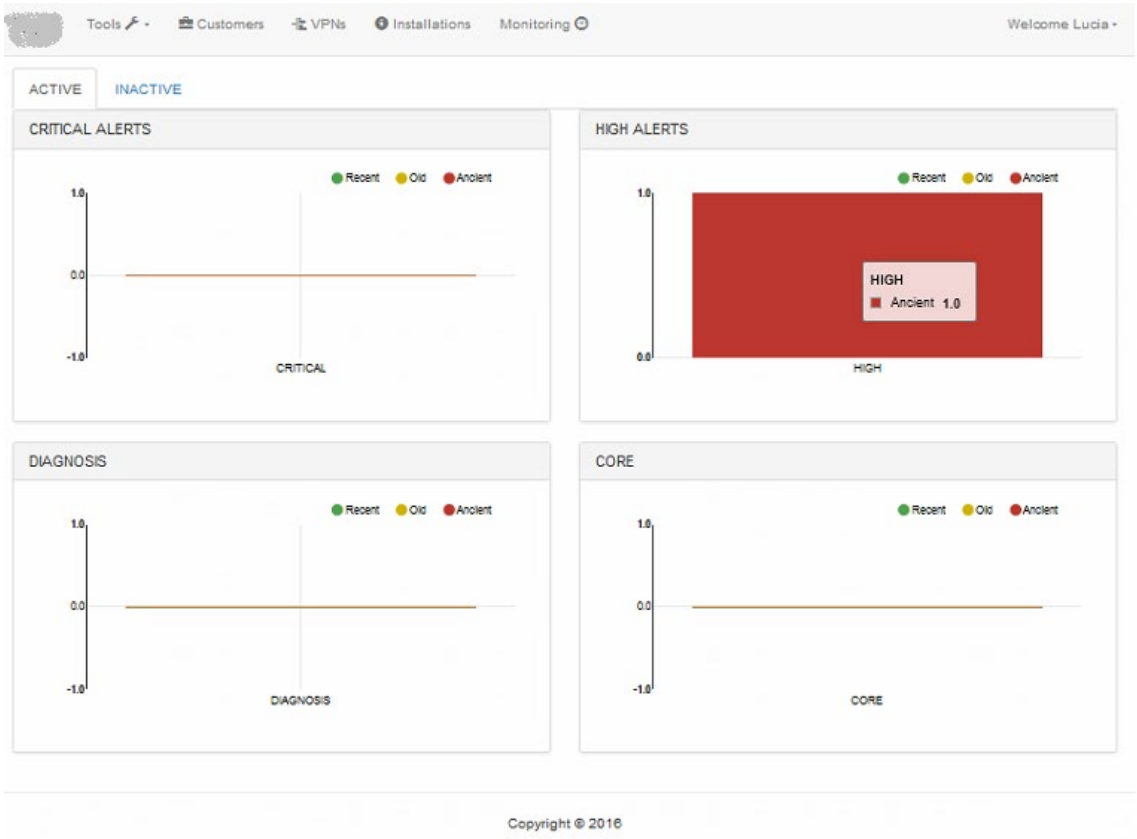
Figura 52. Alarma de evento con prioridad alta luego de pasados 10 minutos



(Elaboración propia)

Asimismo, se observa que al pasar 15 minutos desde que se generó la alarma, sin tomar la acción necesaria, el color de la alarma cambia a rojo, como se observa en la Figura 53.

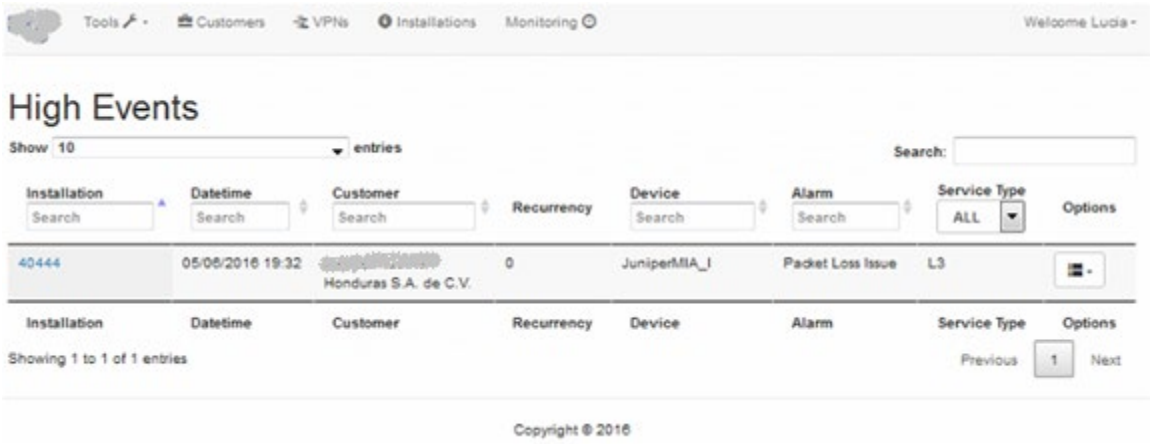
Figura 53. Alarma de evento con prioridad alta luego de pasados 15 minutos de haber aparecido en el tablero.



(Elaboración propia)

Al dar clic en la segunda, se abre una nueva pestaña donde se encuentra el listado de las alarmas activas para eventos de criticidad alta, como se puede ver en la Figura 54, donde se observa el ID del servicio o número de instalación, el nombre del cliente, la recurrencia, el equipo desde donde se genera la prueba, la descripción de la alarma, el tipo de servicio y las posibles acciones a realizar.

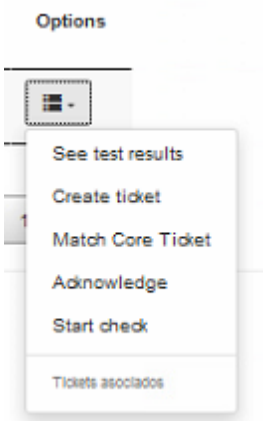
Figura 54. Listado de alarmas sobre eventos críticos.



(Elaboración propia)

Al dar clic en las acciones del botón que se encuentra a la izquierda, se puede observar que se tiene la opción de ver los resultados de las pruebas, crear un ticket, asociar con ticket Core, reconocer la alarma, comenzar revisiones y muestra los incidentes asociados, tal como se observa en la Figura 55.

Figura 55. Posibles acciones de la alarma de evento con prioridad alta.

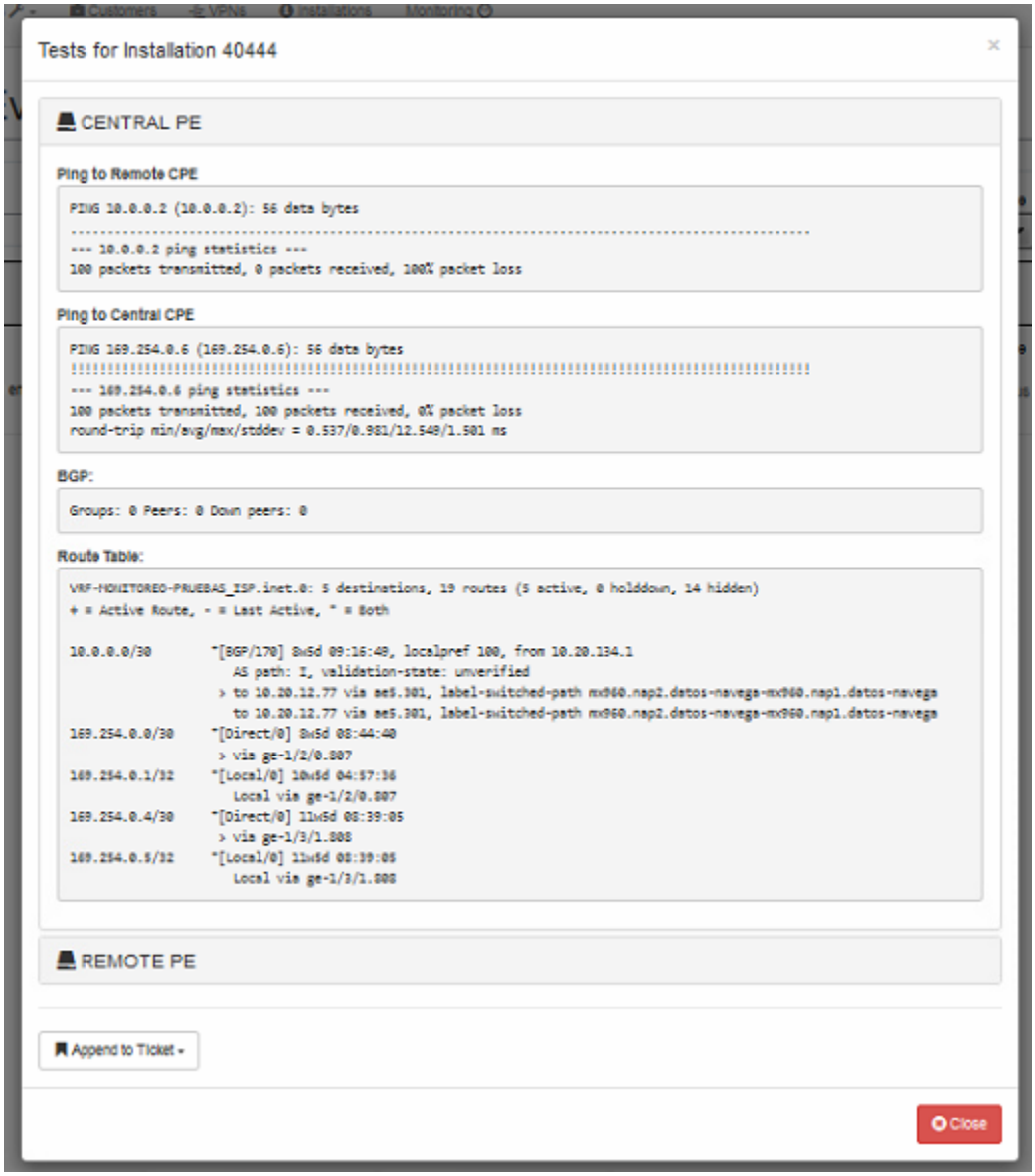


(Elaboración propia)

Si se le da clic en la opción para ver los resultados de las pruebas, se puede observar que se abre una ventana pequeña donde se pueden observar los resultados de las pruebas realizadas desde ambos PE, como se observa la Figura 56.

También se observa que hay una opción para guardar las pruebas realizadas en algún incidente existente.

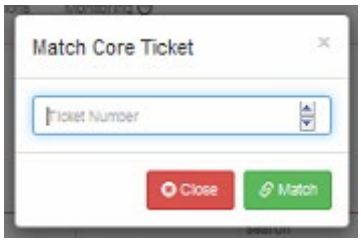
Figura 56. Resultados de pruebas sobre el enlace.



(Elaboración propia)

Al dar clic sobre la opción asociar a un ticket de falla Core, se observa que aparece una ventana como la está en la Figura 57, donde se puede ingresar el número de ticket al que se desea asociar.

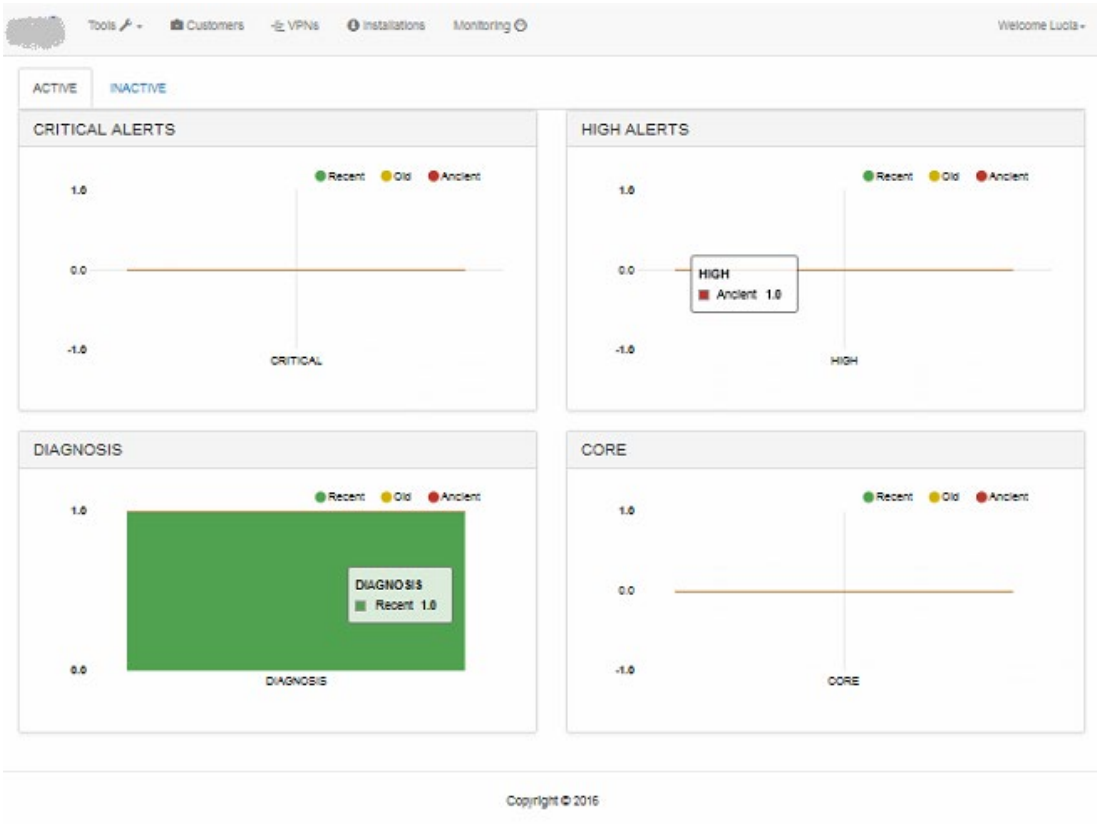
Figura 57. Ventana para asociar una alarma a un *ticket* Core.



(Elaboración propia)

Al dar clic sobre la opción para comenzar revisiones, se observa que la alarma aparece en la tercera gráfica, tal como se observa en la Figura 58.

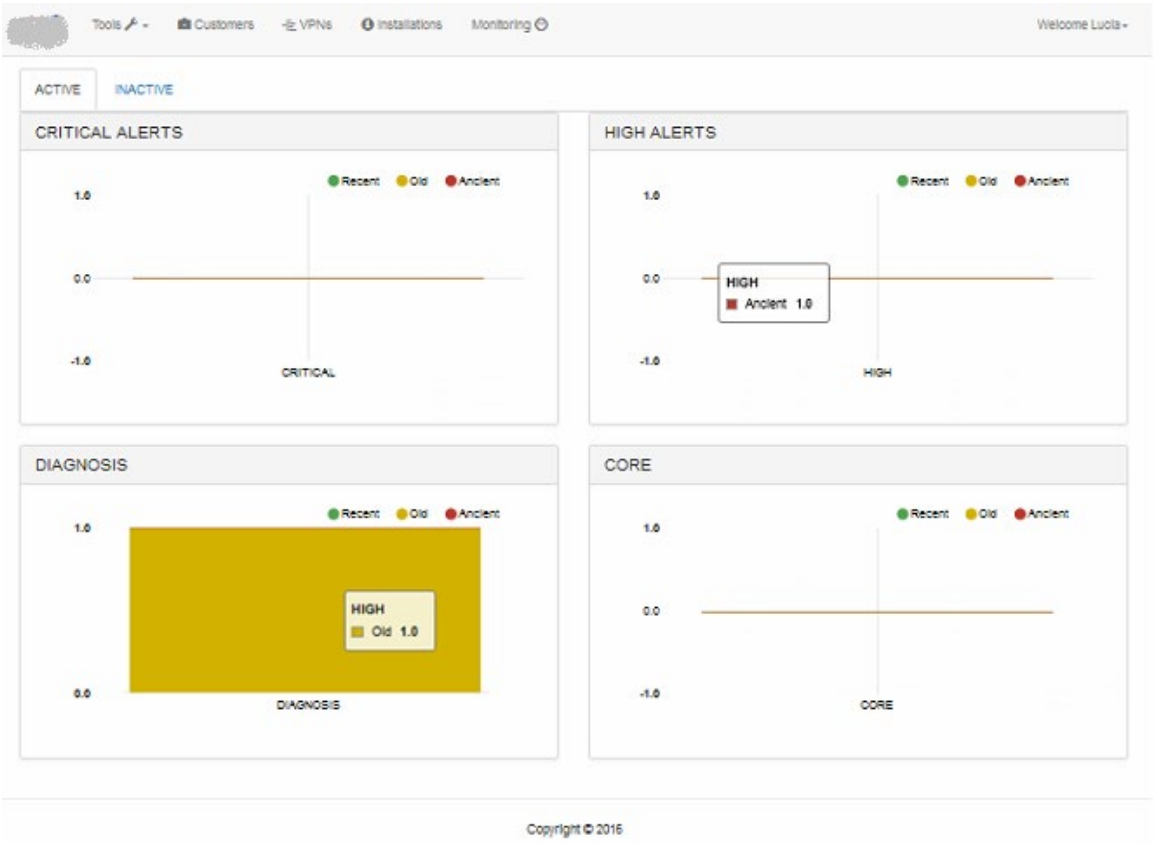
Figura 58. Tercera gráfica de alarmas en revisión en verde.



(Elaboración propia)

Tal como fue definido, para eventos de prioridad alta en revisión, luego de transcurridos 20 minutos, la alarma se torna de color amarillo en la gráfica, como se puede observar en la Figura 59.

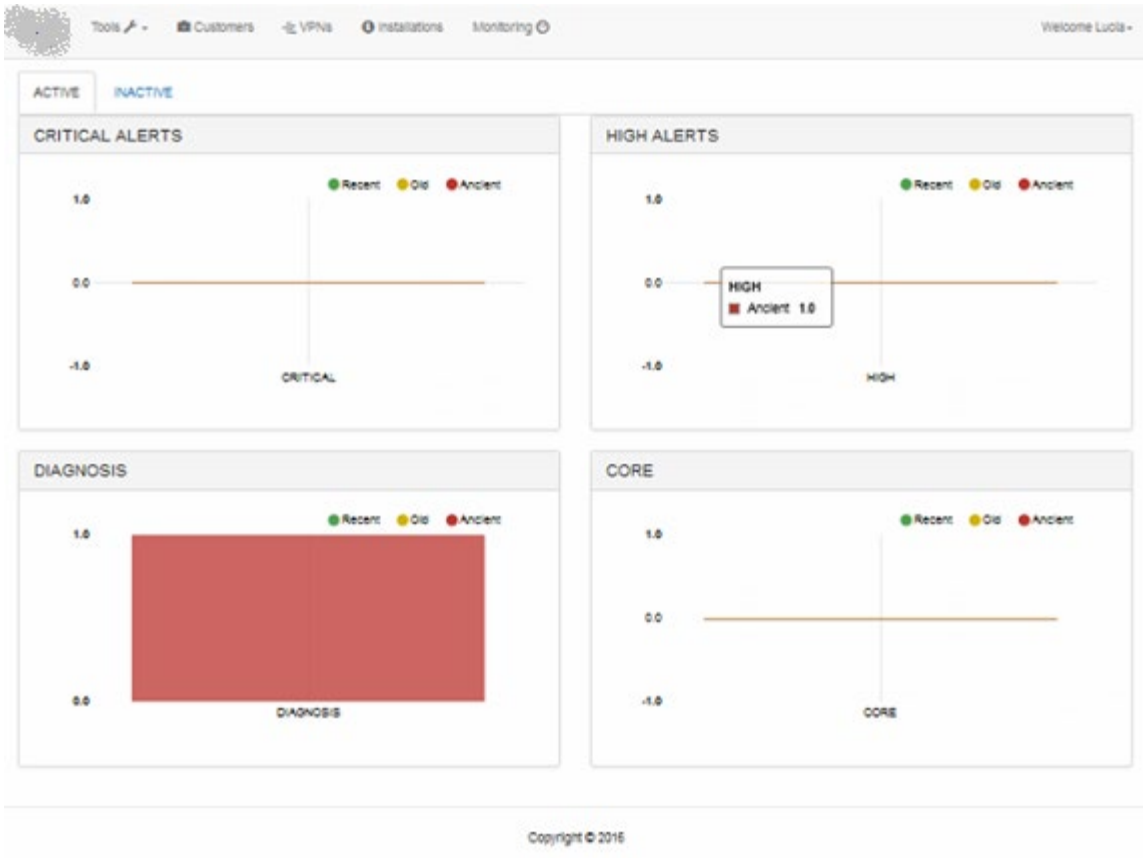
Figura 59. Gráfica de eventos con prioridad alta en revisión en amarillo.



(Elaboración propia)

Asimismo, se observa que al pasar 20 minutos desde que se generó la alarma, sin tomar la acción necesaria, el color de la alarma cambia a rojo, como se observa en la Figura 60.

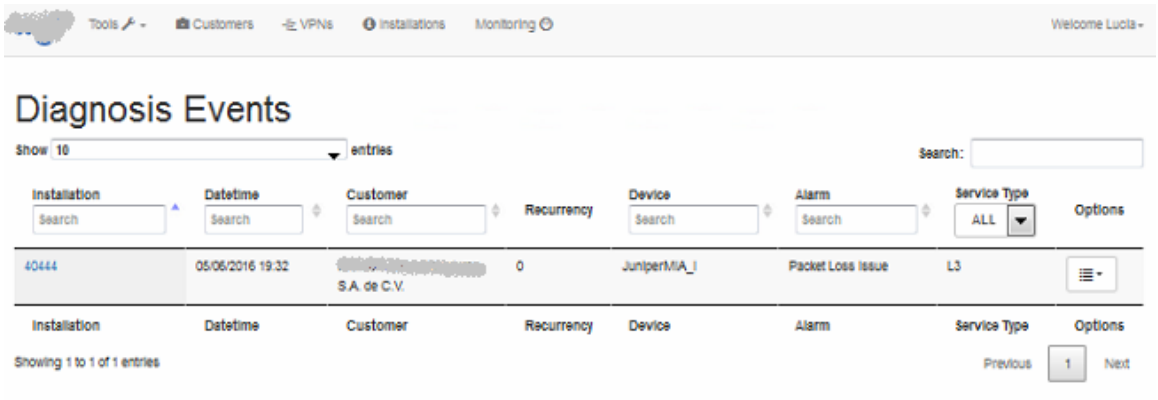
Figura 60. Gráfica de eventos con prioridad alta en revisión en rojo.



(Elaboración propia)

Al dar clic sobre la gráfica, se abre una pestaña nueva con el listado de las alarmas activas para eventos de criticidad alta en revisión, como se puede ver en la Figura 61, donde se observa el ID del servicio o número de instalación, el nombre del cliente, la recurrencia, el equipo desde donde se genera la prueba, la descripción de la alarma, el tipo de servicio y las posibles acciones a realizar.

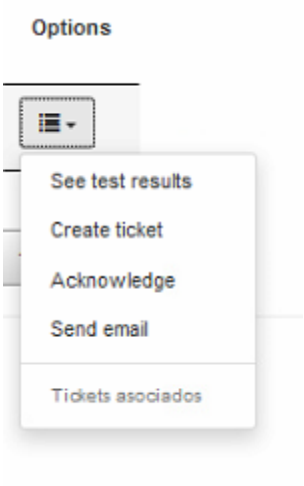
Figura 61. Listado de eventos en revisión de criticidad alta.



(Elaboración propia)

Al dar clic en las acciones del botón que se encuentra a la izquierda, se puede observar que se tiene la opción de ver los resultados de las pruebas, crear un ticket, reconocer la alarma, enviar un correo al cliente y los tickets asociados, tal como se observa en la Figura 62.

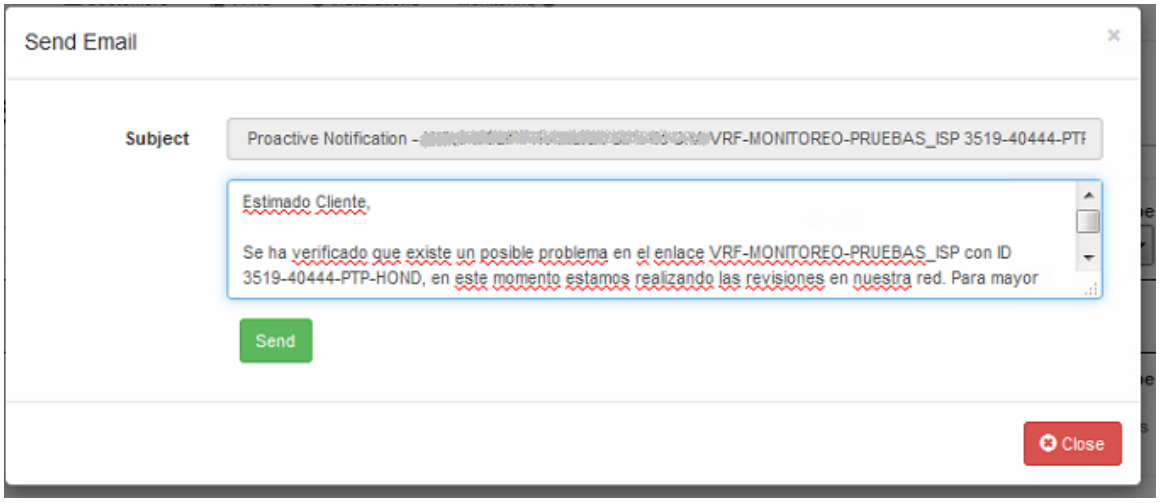
Figura 62. Opciones del evento en el listado de alarmas en revisión.



(Elaboración propia)

Al dar clic en la opción de enviar correo, aparece una ventana como la de la Figura 63, donde el asunto del correo no es modificable, pero el texto sí lo es. Al presionar "Enviar" se envía el correo al cliente.

Figura 63. Ventana para enviar un correo al cliente.



(Elaboración propia)

Se procedió a simular la finalización de la falla a las 00:02 GMT-4 del 6 de junio, como se observa en la Figura 64. Luego de esto, el evento debería ser enviado al historial.

Figura 64. Listado de alarmas reconocidas.

```
0   2016-06-06 00:02:43 EDT by bramirez via cli commit synchronize
```

(Elaboración propia)

Se observa que cerca de 20 minutos luego de que se realizó la finalización de la falla simulada, el evento pasa a la quinta gráfica, que se observa en la Figura 65.

Figura 65. Evento pasa al historial luego de que la simulación de la falla finaliza.

(Elaboración propia)

3. Prioridad moderada o baja. Para estos casos, el sistema debe determinar si la falla está en el Core de la red de la empresa. Para fines de pruebas, dado que la implementación sobre las pruebas de Core aún está en proceso, el sistema asume que el problema no está en el core, por lo que, en este caso, únicamente se envía el correo inicial al cliente, y se observa el evento en la quinta gráfica.

Para la simulación, la urgencia del servicio se define como baja, como se observa en la Figura 66.

Figura 66. Urgencia baja del enlace.

(Elaboración propia)

Dado que el evento tiene un impacto alto, y la urgencia del servicio es baja, se define que el evento tiene una prioridad Moderada, como se observa en el Cuadro 7.

Cuadro 7. Asignación de prioridad moderada del evento.

		Impacto		
		Alto	Medio	Bajo
Urgencia	Alta	Critico	Alto	Moderado
	Media	Alto	Moderado	Bajo
	Baja	Moderado	Bajo	Planeado

(Elaboración propia)

Se procede a simular una falla sobre el servicio, a las 00:47 GMT-4 del 6 de junio, como se observa en la Figura 67.

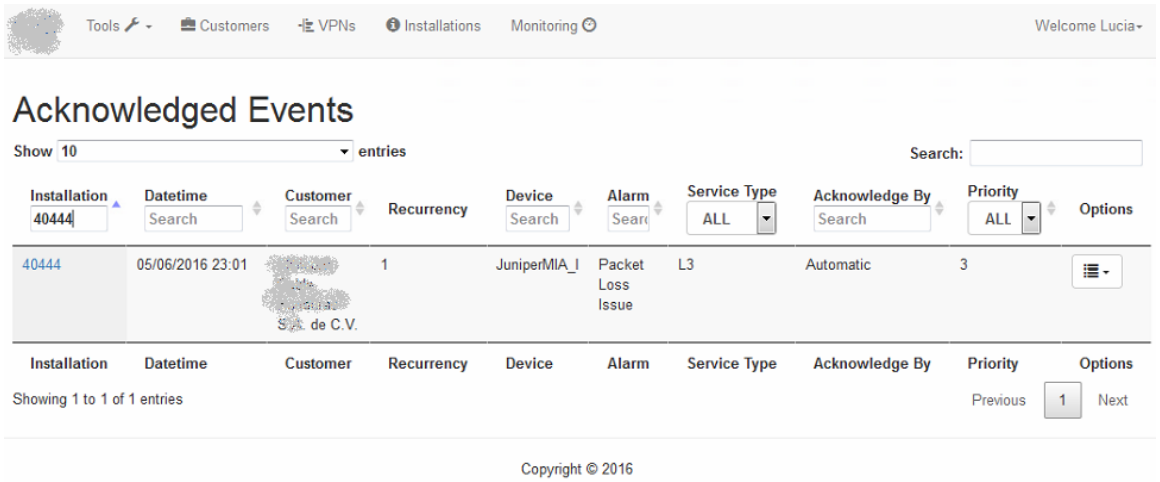
Figura 67. Hora de simulación de evento con impacto alto.

```
0    2016-06-06 00:47:42 EDT by brámirez via cli commit synchronize
```

(Elaboración propia)

Se observa que el evento ha pasado a la quinta gráfica luego de aproximadamente 20 minutos de haber sido generado, como se observa en la Figura 68.

Figura 68. Evento pasa a quinta gráfica por ser de prioridad moderada.



(Elaboración propia)

IX. ANÁLISIS DE RESULTADOS

Inicialmente se creía que la mejor manera de clasificar la interface era en tres grupos; Enlaces, VPNs, y Clientes. Sin embargo, posteriormente se validó que existían algunas herramientas adicionales que ya estaban creadas y que, por lo tanto, se encuentran fuera del marco de este trabajo, pero que aún así era necesario incluirlas. De esta manera, surgió la necesidad de crear una cuarta clasificación; Herramientas. Posteriormente se definió que podría agregarse una herramienta adicional muy útil a esta clasificación; un Generador de Pruebas de Instalaciones, en el cual al ingresar un número de instalación manualmente, realiza las pruebas sobre el enlace asociado, de la misma manera que las realiza al detectar un evento sobre algún enlace. Esta herramienta es útil cuando se recibe algún reporte directamente del cliente sobre un enlace fallido, puesto que aquí se pueden tener las pruebas de manera unificada, sin la necesidad de ir a buscar en cada equipo donde está configurado el servicio. Adicionalmente, al finalizar las pruebas se puede seleccionar guardarlas en algún incidente ya creado, o bien crear un nuevo incidente pegando las pruebas realizadas. Esto implica una gran simplificación y ahorro de tiempo, lo cual es deseable en cualquier negocio.

Respecto a las tres clasificaciones que se habían propuesto originalmente, se puede decir que es la manera más intuitiva en que se pueden clasificar los servicios, dado que la mayoría de servicios que se proveen a otras compañías en capa 3 son enlaces con configuración IP-VPN, que como su nombre lo dice, conforman VPNS. En algunas ocasiones los clientes reportan problemas entre sitios remotos, pero únicamente cuentan con el identificador de uno de los enlaces que conforman la VPN, por lo que es útil tener a la mano todos los demás identificadores para poder ahorrar tiempo en el momento que se desee realizar pruebas.

En este punto se tenían cuatro clasificaciones generales; sin embargo, no se había tomado en cuenta dónde estarían los gráficos donde se monitorearía de manera esquematizada los eventos que surgieran. Se validó que era necesario que el acceso al lugar de monitoreo fuera rápido, por lo que la opción más acertada fue crear una nueva clasificación: Monitoreo. Era deseable que la interface permitiera que las alarmas de los eventos más críticos fuesen los que más saltaran a la vista, por lo cual se decidió que hubiese dos pestañas; la de alarmas activas y la de alarmas inactivas; de esta manera se tendría visibilidad de las alertas de eventos nuevos o, sin que las alertas de eventos pasados o que ya habían sido reconocidas causaran distracción.

De este modo se había propuesto que hubiera una gráfica para cada prioridad. Sin embargo, posteriormente surgió un cambio, pues el tablero estaba planificado para que diera visibilidad de los problemas con mayor riesgo potencial. Fue por ello que se decidió hacer una gráfica para cada prioridad únicamente para las dos más altas; crítica y alta. Para los eventos de prioridad moderada y baja se pensó que lo mejor sería que no generasen una gráfica a menos que se tratara de un problema que pueda estar afectando o llegar a afectar otros enlaces. Fue por ello que se decidió que estaría la gráfica de Core, que es la gráfica donde se muestran las alarmas por eventos moderados y bajos que están afectados por alguna falla masiva en los equipos de Core, y que por lo tanto podría representar un riesgo potencial para toda la operación de los enlaces. Por supuesto que existen ocasiones en que sí será necesario realizar alguna acción, como abrir un *ticket* o enviar un correo al cliente, pero esto ya queda a discreción del ingeniero que esté a cargo, por lo que se dejó una opción tanto para abrir un ticket nuevo como para enviar un correo al cliente.

Respecto a las vistas de búsqueda de Enlaces, VPNs y Clientes, se propuso que los parámetros de búsqueda sean las características más específicas de los enlaces, esto para evitar que el resultado de búsqueda sea tan largo, que resulte no siendo práctico. Se propuso que en la vista de Enlaces estuviese un campo modificable para ingresar identificadores de circuitos de proveedores, y que se pudiese buscar enlaces a través de dicho campo. Esto es muy necesario, dado que ha sucedido de manera frecuente que cuando un proveedor notifica algún mantenimiento o algún incidente proactivo, es bastante complicado y tardado el realizar la búsqueda del enlace relacionado para poder notificarlo al respectivo cliente, con el respectivo identificador. De esta manera, se podrá tener acceso más rápido a los enlaces cuando se esté trabajando con proveedores.

Adicionalmente, tanto en la vista de Enlaces y VPNs como de Clientes, se propuso colocar un campo modificable para comentarios. Estos comentarios son útiles porque muchas veces existen algunas modificaciones temporales o anotaciones que se deben realizar y que ayudan realizar procesos de diagnóstico más eficientemente, o a saber si los casos o clientes deben ser manejados de alguna manera especial. Un ejemplo de estos casos en que existen algunos enlaces que cuando están afectados por alguna falla se debe notificar a cierto grupo de personas, adicionalmente a quien ha realizado el reporte. También hay ocasiones en que se realizan modificaciones temporales, o que quedan pendientes trabajos para realizarse la vez más próxima que exista una falla. En todos estos casos es útil tener los comentarios de los demás ingenieros, y es importante que puedan eliminarse, ya que luego de que ya no son útiles, no hay necesidad de tener referencia histórica.

Con respecto a la metodología para determinar la prioridad del evento, según ITIL, como se pudo verificar en la parte del marco teórico, existen tres tipos de eventos; usuales, inusuales y excepciones, y esto es lo que determina las acciones a realizar. Sin embargo, en el caso del presente trabajo, no se tenía únicamente un factor a tomar en cuenta para la determinación del disparo de una alarma, pues también se tienen distintos tipos de servicio, con distintos niveles de importancia. Fue por ello que se decidió tomar

como referencia el modelo para determinar la prioridad de un incidente, que consiste en la combinación del impacto y la urgencia.

De esta manera, se asoció el concepto de impacto con el tipo de evento, teniendo tres tipos; los usuales clasificados como bajos, los inusuales clasificados como medios, y las excepciones, clasificadas como eventos de impacto alto. En consecuencia, luego de determinar la urgencia de los enlaces, la determinación de la prioridad sería algo muy sencillo; y así lo fue.

En la propuesta del presente trabajo se mencionaba que se debía establecer los parámetros aceptables para que un enlace se considerara funcional. Este punto surgió como una oportunidad de mejora, puesto que en la actualidad se ha hecho necesario que exista un acuerdo entre los grupos de aprovisionamiento y soporte al poner un enlace nuevo en producción, de manera que, al llegar los reportes de falla al grupo de soporte, pueda determinarse que realmente se trata de una falla, al encontrarse el enlace en un estado distinto al que se entregó al ser puesto en producción. Hay ciertos parámetros muy importantes, y que los clientes valoran mucho en un enlace, tales son el RTT, el tamaño de paquete MTU y el ancho de banda contratado. Actualmente, al ser un enlace nuevo puesto en producción, un ingeniero de soporte da visto bueno al enlace, pero no se tenía especificado cuáles serían los parámetros que se tomarían como aceptables. Se ha definido que el ingeniero de soporte que realiza la revisión validará que los parámetros de funcionamiento sean los que están establecidos en el requerimiento del cliente, y de ser así, estará marcando la parte de la activación del enlace en la vista de enlaces, lo cual indicará que los parámetros fueron aceptados como funcionales.

De igual manera, para la implementación del monitoreo de los enlaces, se requiere que la configuración de las interfaces relacionadas tengan cierto formato. Para dar el visto bueno, también se deberá validar esto para poder aceptar el enlace como funcional, de otra manera, no tendría monitoreo implementado.

De las pruebas realizadas con el enlace de pruebas en capa 3, se observó un tiempo de aproximadamente 22 minutos entre el momento en que se generó el evento, en este caso, que se desconectó intencionalmente la interface que simula la del equipo del CPE remoto, hasta el momento en que se creó el ticket y apareció la alarma en el tablero. Este desfase se debe a que los resultados del RPM de todos los enlaces se actualiza cada 10 minutos, y debe pasar por varias pruebas antes de determinar si está realmente afectado o no. A pesar de este desfase, se pudo determinar que el tiempo de la generación de la alarma es aceptable, tomando en cuenta que es una acción proactiva, y que es preferible pasar por una serie de pruebas para determinar el impacto que tiene el enlace, a generar alarmas por cualquier evento, puesto que se perderían de vista los eventos que puedan representar una mayor afectación o riesgo de afectación.

Los datos que se obtienen a través del monitoreo enlaces de capa 3 son mucho más variadas y permiten conocer ciertos detalles que no es posible tenerlos con el monitoreo de capa 2. Por ejemplo, el

porcentaje de pérdidas y los tiempos de viaje de ida y vuelta (RTT) son factores muy importantes para el funcionamiento de un enlace para los clientes finales. Al presentarse un problema de este tipo, las causas pueden muy variadas. Según la experiencia que se ha tenido sobre lo observado en el día a día en el NOC, podría tratarse de una degradación en la ruta de transporte, una conmutación de ruta principal a ruta secundaria, errores por problemas de conexiones físicas en los puertos, o incluso saturación del enlace. De todos estos posibles problemas, el único que podría monitorearse en capa 2 es la saturación a través del análisis de tráfico, lo cual es muy limitado. Es por ello que, muchas veces, aún tratándose de un enlace capa 2, se solicita a los clientes configurar una dirección IP de pruebas en su sitio remoto, de manera que se pueda implementar monitoreo de capa 3 sobre dicho enlace.

Los tiempos de respuesta dependen mucho de la distancia entre el punto desde donde se genera la prueba y el punto remoto que se desea alcanzar, así como de cuántos equipos intermedios existan entre dichos puntos. Para la definición de los umbrales de pérdida de paquetes se realizó un análisis sobre en qué punto comienza a ser este un problema para los clientes, o bien comienza a ser percibido. Es importante mencionar que hay algunos enlaces, dependiendo de la utilización que le dé el cliente, que están sujetos a un monitoreo más estricto por parte de los clientes. Se observó que la mejor manera para definir los umbrales de pérdidas eran sobre un porcentaje de retraso respecto a los tiempos promedio de los enlaces. Esto es porque, por ejemplo, no es lo mismo que un enlace que normalmente tiene 80 milisegundos de RTT tenga un aumento de 5 milisegundos, a que un enlace que normalmente tiene un RTT de 25 milisegundos, tenga dicho aumento. En el segundo caso es más probable que la diferencia pueda llegar a ser notoria en el desempeño de las aplicaciones, que en primer caso.

Los umbrales de pérdida de paquetes se realizaron en varias fases, lo cual se realizó de esa manera para evitar que el sistema tardara demasiado en realizar las pruebas cuando la pérdida de paquetes es alta. De esta manera, al detectar demasiada alta pérdida de paquetes con diez pruebas de Ping, el sistema detectará el evento inmediatamente, pero de no ser así, realizará algunas pruebas más para cerciorarse de que se trata de un evento relevante y no de pérdidas aleatorias.

El cambio de colores en las gráficas de monitoreo es algo deseable, dado que es importante que las acciones requeridas se realicen de manera rápida. Lo ideal es que el tablero se mantenga siempre sin alarmas activas, y que la mayoría se encuentren en estado de reconocida, de manera que, al generarse un evento, pueda ser visualizado rápidamente y no perderse entre muchos otros eventos activos sobre los cuales ya se realizaron acciones en caso se requiera, y que ya fueron reconocidas.

Como se pudo observar, al reconocer una alarma se puede variar el tiempo en que debe permanecer en la clasificación de alarmas reconocidas. Esto es porque algunas veces sucede que hay algún evento en sitio del cliente final o se están realizando trabajos sobre el enlace que ya están notificados al cliente, y se desea

que el evento se mantenga oculto para evitar alertar al personal de NOC innecesariamente. Al haber transcurrido el tiempo configurado para permanecer reconocido el evento, deberá regresar a su gráfica original, para que ya se tenga visibilidad nuevamente de que el problema continúa.

Normalmente cuando el problema que disparó el evento en un inicio ha finalizado, el evento se envía de manera automática a la sexta gráfica, al historial. Luego de eso, podría generarse un nuevo evento si el problema es recurrente. Es por ello que se agregó una opción cuando se pasan los servicios a reconocidos, que permite que se mantenga en la clasificación de reconocidos aún si el problema ya ha sido resuelto, y que no pase al historial. De esta manera, si el problema vuelve a repetirse, no se generará un nuevo evento.

X. CONCLUSIONES

1. Se determinó que la forma más intuitiva para la presentación al usuario es una clasificación de interfaces por Enlaces, VPNs, Clientes, Monitoreo y Herramientas

2. Se verificó que, a través de la clasificación general de la plataforma, los usuarios pueden gestionar de manera eficiente los enlaces Ethernet e IP.

3. Se identificó que los alcances de monitoreo para los enlaces capa 3 MPLS IP-VPN y capa 2 MPLS-VPLS permiten monitorear características diferentes por tipo de enlace.

4. Se demostró que el monitoreo de enlaces capa 3 a través de RPM permite la verificación de tiempo de viaje de ida y vuelta, y pérdida de paquetes de forma satisfactoria.

5. Se demostró que el monitoreo de enlaces capa 2 utilizado permite la verificación de direcciones MAC, tráfico, estado de interfaces y estado de VPLS de forma satisfactoria.

6. Se verificó que el monitoreo de enlaces capa 3 permite tener mayor visibilidad en cuanto al desempeño del enlace, respecto a los de capa 2.

7. Se definieron los umbrales de tiempo de viaje con base en el tiempo de viaje promedio que mantiene el enlace en el historial, y el cálculo se realizó manualmente.

8. Se determinó que los parámetros a considerar en la aceptación de un enlace nuevo como funcional son tiempos de respuesta (RTT), tamaño de paquetes, ancho de banda, y configuración de interfaces para monitoreo de servicios.

9. Se definió la prioridad de un evento considerando dos parámetros; el impacto del evento y la urgencia del servicio.

10. Se definió el impacto del evento considerando el daño potencial que podría causar en la operación de un negocio.

11. Se estableció el impacto de los eventos como alto, medio o bajo basado en las repercusiones que estos pueden representar desde el punto de vista financiero y de ejecución del trabajo de los usuarios finales.

12. Se estableció una clasificación de la urgencia de los enlaces considerando el monto de facturación y ancho de banda, así como la utilización que el usuario final da al enlace.

13. Se diseñó una clasificación totalmente incluyente para la urgencia de los enlaces Ethernet e IP.

14. Se definió que la urgencia de un evento puede ser alta, media o baja dependiendo de la facturación, ancho de banda y utilización del enlace que afecta, así como si el usuario cuenta o no con un enlace de protección o redundancia.

15. Se definió el flujo de un evento para determinar las acciones a realizar tanto por el sistema como por parte de un ingeniero de soporte de manera manual.

16. Se excluyó del alcance de este trabajo el flujo de actividades a realizar luego de generarse un evento de prioridad crítica, puesto que el presente proyecto incluye únicamente el flujo para la gestión de eventos.

17. Se diseñó un flujo de manejo de eventos, tal que, al generarse un evento de cualquier tipo, se enviará al cliente automáticamente un correo informando sobre un potencial problema y solicitándole comunicarse con el grupo de soporte de requerir mayor información y apoyo.

18. Se determinó que el umbral de tráfico para identificar que un enlace está potencialmente fuera de funcionamiento es de 100 bps.

19. Se definió que en enlaces Ethernet un evento tiene impacto alto, es decir, que se encuentra fuera de funcionamiento, cuando el tráfico está por debajo de los 100 bps, y las mac address de alguno de los extremos deja de aprenderse, o bien que alguna de las interfaces esté abajo, o que la VPLS esté abajo.

20. Se definió que en enlaces Ethernet para validar que un evento tiene impacto bajo, se debe cumplir que el tráfico esté por encima del 95% del ancho de banda contratado.

21. Se definió que en enlaces IP para validar que un evento tiene impacto alto, se debió haber detectado pérdida de paquetes del 100% o porcentaje alto de incremento de RTT.

22. Se definió que en enlaces IP para validar que un evento tiene impacto medio, se debió haber detectado pérdida de paquetes por encima del 36% y debajo del 99% y porcentaje medio de incremento de RTT.

23. Se definió que en enlaces IP para validar que un evento tiene impacto bajo, se debió haber detectado pérdida de paquetes por encima del 6% y por debajo del 35%, y porcentaje bajo de incremento de RTT.

24. Se diseñó un sistema que genera cambio de colores en las distintas gráficas de monitoreo a manera que permita a los ingenieros estar atentos a las alarmas por eventos y evitar que pase mucho tiempo sin realizarse las acciones que sean requeridas.

XII. BIBLIOGRAFÍA

Agrassala, Vinod. *Events vs Incidents. – 'Too easy' and 'So confusing' at the same time.* https://vagrasala.wordpress.com/2010/03/16/events-vs-incidents-too-easy-and-so-confusing-at-the-same-time/ [Marzo 2016].

Arriola, Álvaro. 2013. «Implementación de Gestión Proactiva End-to-End para Servicios IP». Trabajo de Graduación Universidad del Valle de Guatemala. 77 págs.

Ecured. *Modelo OSI*. http://www.ecured.cu/Modelo_OSI [Marzo 2016].

Galeón. *Redes de datos*. http://redesdedatosinfo.galeon.com/enlaces2128619.html [Marzo, 2016].

Kempter, Stefan. *Checklist Incident Priority.* http://wiki.en.it-processmaps.com/index.php/Checklist_Incident_Priority [Marzo, 2016].

Morales, Luis. 2006. «Investigación de Redes VPN con Tecnología MPLS». Tesis Licenciatura Universidad de las Américas Puebla. 95 págs.

Osiatis. *ITIL®-Gestión de Servicios TI, Gestión de Incidentes, Clasificación del Incidente.* http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes/clasificacion_y_registro_de_incidentes.php [Marzo, 2016].

Robles, Jonathan. 2015. «Implementación de un sistema de monitoreo sobre servicios Ethernet e IP». Trabajo de Graduación Universidad del Valle de Guatemala. 204 págs.

Rosales, Delfino. *Métodos de Transmisión: Unicast, Multicast y Broadcast*. http://www.delfirosales.com/2009/06/metodos-de-transmision-unicast.html [Marzo 2016].

Tanenbaum, Andrew y D. Wetherall. 2012. *Redes de Computadoras*. 5ta Edición. Traducción de Alfonso Vidal Romero Elizondo. México: Pearson. 816 págs.

Wikipedia. *Networks Operations Center*. https://en.wikipedia.org/wiki/Network_operations_center [Marzo 2016].

Zitek, Neven. All *About Incident Classification*. http://advisera.com/20000academy/knowledgebase/incident-classification/ [Marzo, 2016].

XIII. ANEXOS

A. DEFINICIÓN DE BATERÍA DE PRUEBAS

1. Pruebas en Capa 3

a. En PE central.

ping <IP_CPE_REMOTO> routing instance <ROUTING_INSTANCE> rapid count 100 //Ver tiempos de respuesta y porcentaje de perdidas hacia el CPE remoto.

ping <IP_PE_NNI> routing instance <ROUTING_INSTANCE> rapid count 100 //Ver tiempos de respuesta y porcentaje de perdidas hacia la IP de la central del cliente o NNI.

show route table <ROUTING_INSTANCE> //Ver red del cliente si se conoce, verificar tiempo de conocer rutas

show services rpm probe-results test <TEST> owner <OWNER> // Ver jitter, RTT,verificar si ha habido caídas.

show bgp summary instance <ROUTING INSTANCE>; //Verificar tiempo que lleva arriba la sesión BGP hacia el NNI

b. En PE de país remoto.

ping <IP_CPE_REMOTO> routing instance <ROUTING_INSTANCE> rapid count 100 //Ver tiempos de respuesta y porcentaje de perdidas hacia el CPE remoto.

ping <IP_PE_NNI> routing instance <ROUTING_INSTANCE> rapid count 100 //Ver tiempos de respuesta y porcentaje de perdidas hacia la IP de la central del cliente o NNI.

show route table <ROUTING_INSTANCE> //Ver red del cliente si se conoce, verificar tiempo de conocer rutas

show bgp summary instance <ROUTING INSTANCE>; //Verificar tiempo que lleva arriba la sesión BGP hacia el CPE remoto.

2. Pruebas en Capa 2

a. En ambos PE

show vpls connections logical system <LOGICAL_SYSTEM> instance <ROUTING_INSTANCE> // Ver uptime de la VPLS (OMITIR "logical system <LOGICAL_SYSTEM>" en caso no esté dentro de un Sistema lógico)

show vpls connections logical system <LOGICAL_SYSTEM> instance <ROUTING_INSTANCE> //Verificar si se tienen mac address de ambos extremos (OMITIR "logical system <LOGICAL_SYSTEM>" en caso no esté dentro de un Sistema lógico)

B. ACTIVIDADES PARA EL DESARROLLO DEL TRABAJO

1. Definir las clasificaciones generales de la interface.
2. Definir los elementos incluidos en cada clasificación.
3. Implementar la clasificación de la interface.
4. Especificar los parámetros aceptables para que un enlace Ethernet e IP nuevo pueda considerarse funcional.
5. Diseñar la clasificación de los enlaces Ethernet e IP según sus características.
6. Implementar la clasificación de los enlaces y verificar que sea válida y totalmente incluyente
7. Definir los valores aceptables para cada característica que se tomará en cuenta para generar una alerta en el monitoreo de un enlace Ethernet e IP.
8. Determinar el flujo a seguir para generar acciones a partir de una alerta disparada en un enlace.
9. Validar el flujo con el equipo de trabajo de monitoreo.
10. Definir cuáles son las características que se deben tomar en cuenta para determinar la criticidad de un enlace.
11. Definir cuáles son los rangos dentro de dichas características.
12. Crear una clasificación de enlaces por criticidad tomando en cuenta sus características específicas.
13. Validar que la clasificación de enlaces por criticidad sea válida y totalmente incluyente.

14. Definir un criterio de disparo de alertas según la clasificación de criticidad que tenga cada enlace.
15. Definir las acciones a realizar dependiendo de las alertas disparadas en los enlaces.
16. Implementar las acciones a realizar dependiendo de dichas alertas.
17. Validar el proceso con el equipo de trabajo.
18. Elaboración del trabajo escrito.

C. CRONOGRAMA DE ACTIVIDADES

# Actividad	Descripción de Actividad	Fecha Inicial	Fecha Final
1	Definir las clasificaciones generales de la interface.	19/07/2015	20/07/2015
2	Definir los elementos incluidos en cada clasificación.	20/07/2015	21/07/2015
3	Implementar la clasificación de la interface.	22/07/2015	26/07/2015
4	Especificar los parámetros aceptables para que un enlace Ethernet e IP nuevo pueda considerarse funcional.	26/07/2015	27/07/2015
5	Diseñar la clasificación de los enlaces Ethernet e IP según sus caracteristicas.	28/07/2015	29/07/2015
6	Implementar la clasificación de los enlaces y verificar que sea válida y totalmente incluyente	29/07/2015	30/07/2015
7	Definir los valores aceptables para cada característica que se tomará en cuenta para generar una alerta en el monitoreo de un enlace Ethernet e IP.	01/08/2015	06/08/2015
8	Determinar el flujo a seguir para generar acciones a partir de una alerta disparada en un enlace.	07/08/2015	11/08/2015
9	Validar el flujo con el equipo de trabajo de monitoreo.	12/08/2015	15/08/2015
10	Definir cuáles son las características que se deben tomar en cuenta para determinar la criticidad de un enlace.	16/08/2015	19/08/2015
11	Definir cuáles son los rangos dentro de dichas características.	19/08/2015	23/08/2015
12	Crear una clasificación de enlaces por criticidad tomando en cuenta sus características específicas.	24/08/2015	26/08/2015
13	Validar que la clasificación de enlaces por criticidad sea válida y totalmente incluyente.	27/08/2015	30/08/2015
14	Definir un criterio de disparo de alertas según la clasificación de criticidad que tenga cada enlace.	31/08/2015	04/09/2015
15	Definir las acciones a realizar dependiendo de las alertas disparadas en los enlaces.	05/09/2015	07/09/2015
16	Implementar las acciones a realizar dependiendo de dichas alertas.	07/09/2015	09/09/2015
17	Validar el proceso con el equipo de trabajo.	10/09/2015	15/09/2015
18	Elaboración del trabajo escrito.	15/09/2015	20/09/2015

XIV. GLOSARIO

AS Autonomous System

BGP Border Gateway Protocol

CE Customer Edge

CI Configuration Item

CPE Customer Premises Equipment

CPU Central Processing Unit

DNS Domain Name System

HTTP Hypertext Transfer Protocol

ICMP Internet Control Message Protocol

IP Internet Protocol

ISP Internet Service Provider

ITIL Information Technology Infrastructure Library

L2VPN Layer2 VPN

LSP Label Switched Path

LSR Label Switching Router

MPLS Multi-Protocol Label Switching

MTTR Mean Time To Repair

MTU Maximum Transmission Unit

NOC Network Operations Center

OS Operating System

OSPF Open Shortest Path First

PE Provider Edge

RPM Real-Time Performance Monitoring

RTT Round-Trip Time

SLA Service Level Agreement

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

VPN Virtual Private Network

VPLS Virtual Private LAN Service

VRF VPN Routing and Forwarding