UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

CONTROL DE INCIDENCIAS DE REDES DE TELECOMUNICACIONES MEDIANTE UN ADMINISTRADOR DE GESTORES (MoM)

AUTOR:
Tejada Cáceres, Jaime Andrés

Trabajo de Titulación previo a la obtención del título de
INGENIERO EN TELECOMUNICACIONES

TUTOR:
Palau De La Rosa, Luis Ezequiel

Guayaquil, Ecuador

31 de Agosto del 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Tejada Cáceres, Jaime Andrés** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

_____

Palau De La Rosa, Luis Ezequiel

DIRECTOR DE CARRERA

_____

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los 31 días del mes de agosto del año 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Tejada Cáceres, Jaime Andrés**

DECLARÓ QUE:

El trabajo de titulación **"Control De Incidencias De Redes De Telecomunicaciones Mediante Un Administrador De Gestores (Mom)",** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 31 del mes de Agosto del año 2018

EL AUTOR

_____

TEJADA CÁCERES, JAIME ANDRÉS

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Tejada Cáceres, Jaime Andrés**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Control De Incidencias De Redes De Telecomunicaciones Mediante Un Administrador De Gestores (Mom)"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

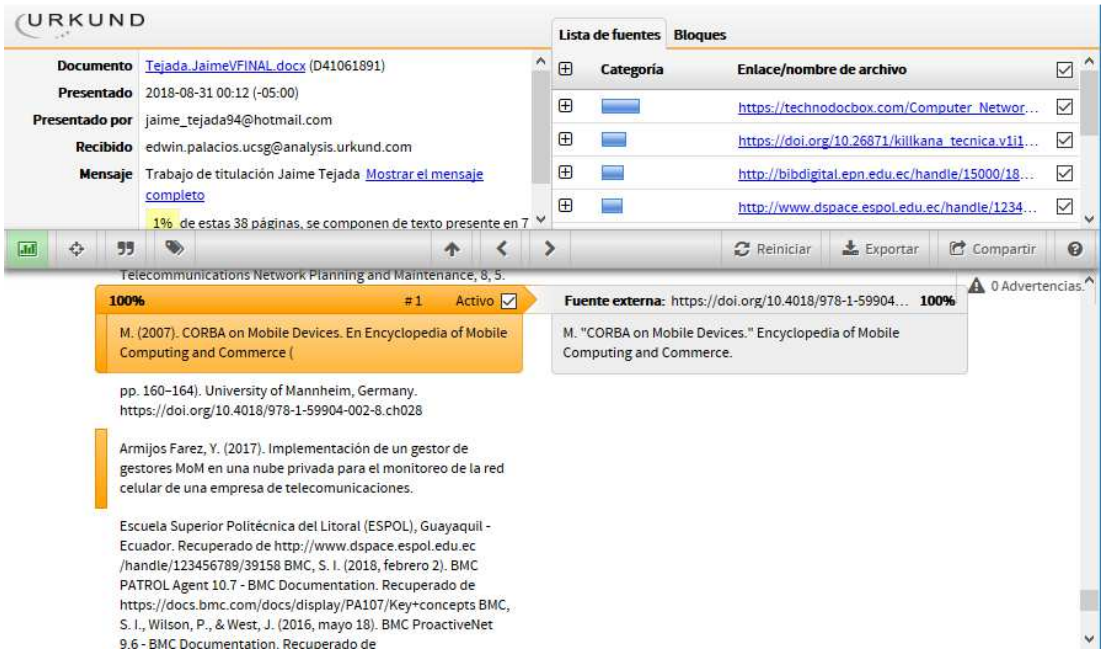
Guayaquil, a los 31 del mes de Agosto del año 2018

EL AUTOR

_____

TEJADA CÁCERES, JAIME ANDRÉS

REPORTE DE URKUND



DEDICATORIA

El presente trabajo de titulación es dedicado a mi familia quienes han otorgado todo su apoyo durante mi desarrollo como un profesional.

A mis padres por ser el pilar de mis sueños y parte fundamental en toda meta de mi vida.

EL AUTOR

_____

TEJADA CÁCERES, JAIME ANDRÉS

AGRADECIMIENTO

Agradezco a Dios por permitirme todas las posibilidades que he tenido para superarme día a día.

A mi familia por ser parte esencial para mi formación y en cada decisión que he tomado.

A todos los que me dieron su pequeño apoyo para la realización de este trabajo de titulación.

A todos les quedo enormemente agradecido.

EL AUTOR

_____

TEJADA CÁCERES, JAIME ANDRÉS

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESÚS

DECANO

f. _____

M. Sc. HERAS SANCHEZ, MIGUEL ARMANDO

DIRECTOR DE CARRERA

f. _____

M.

OPONENTE

Índice General

Índice de Figuras

Capítulo 2:

Capítulo 3:

Capítulo 4:

Capítulo 5:

Índice de Tablas

Capítulo 2:

Capítulo 3:

Resumen

Las empresas de telecomunicaciones están en constante evolución de sus servicios y de su infraestructura, creando así competitividad en el mercado presentando nuevos y mejores servicios a sus clientes. El desarrollo y aumento de tecnologías es evidente en los últimos años dentro del país, pero este va de la mano con el aumento de sistemas de red y de la exigencia de la calidad de los servicios ofrecidos. La infraestructura de las redes de telecomunicaciones es monitoreada constantemente por un área llamada NOC que poseen la tarea de monitorear la operabilidad de la red como también informar y dar soporte en las incidencias que ocurren sobre la misma, entre las incidencias se encuentran fallas en equipos, saturación de servicios, status de equipos, congestión de las redes, fallas de autenticación, etc. Que son visualizadas dentro de los Sistemas Gestores de cada proveedor. Sin embargo, el uso de diversas herramientas que poseen distinto proveedor, servicio, modelo, etc. implica que se debe ingresar a varias plataformas para poder medir el rendimiento de la red como también incrementar cantidad de empleados. Un administrador de gestores es capaz de consolidar varios tipos de redes y de tecnologías en una sola interfaz, de tal modo que el personal del NOC y directores de la empresa pueden realizar mediciones de desempeño de las redes y monitorear en tiempo real toda su infraestructura con una sola herramienta. Esto permite la toma de decisiones en un menor periodo de tiempo para solucionar o prevenir afectaciones dentro de la red, asegurando la calidad de los servicios. Esta solución facilita la optimización de recursos, tiempo y de personal en una empresa de telecomunicaciones.

En el presente trabajo de titulación se mostrará la implementación de una red de telecomunicaciones en un Administrador de gestores, dando a conocer los beneficios de estandarizar los procesos de control de redes móviles.

Palabras claves: Red móvil, Elementos de red, SNMP, Celdas remotas.

Capítulo 1: Descripción General

1.1. Introducción

Un MoM (Management of Management) es un administrador de Gestores que recolecta información de múltiples Gestores de diferentes marcas y estructuras. Satisface necesidades de control y monitoreo especialmente sobre redes de Telecomunicaciones. De tal modo que facilita la operación y mantenimiento sobre los servicios y aplicaciones que estas redes proveen, asegurando una alta disponibilidad de su uso para el cliente.

Dentro del contexto de MoM, se refiere a la integración de un conjunto de sistemas de transmisiones, sistemas de conmutación, multiplexores, terminales de señalización, bases de datos, aplicaciones, equipos, procesos y demás complementos que permiten el intercambio y procesamiento de información (digital y analógica) a través de diferentes sistemas que proporcionan una gama de capacidades a los clientes.

El objetivo principal de un MoM es proporcionar una arquitectura organizada y estandarizada, para tener un control incidencias y anomalías sobre la misma de tal modo que el área encargada de monitorear pueda identificar el problema causa raíz y derivar el problema para su solución inmediata.

1.2. Antecedentes

Las demandas de nuevos e innovadores servicios en las telecomunicaciones como VoIP, Servicios en la Nube, Video Streaming, navegaciones de alta velocidades, etc. implican un crecimiento de los

componentes y elementos que comprenden las diferentes redes. Debido a la gama de equipos que se encuentran en la infraestructura, los múltiples sistemas gestores de cada proveedor son controlados y monitoreados por áreas específicas a quienes se le responsabiliza por la operabilidad y disponibilidad de los equipos. Sin embargo, la cantidad de servicios y de equipos está directamente relacionado con los sistemas gestores. Esto causa que la cantidad de recursos y de empleados también aumenten. Lo que implica una complejidad al momento de solucionar falencias en cada uno de ellos y la visualización de problemas a nivel de toda la infraestructura.

1.3. Definición del Problema

Las operadoras móviles poseen una infraestructura muy amplia en donde existen varios elementos de las redes móviles 2G, 3G, y 4G. Así como también servidores, switches, firewalls corporativos entre otros equipos, en donde cada uno de ellos cumple una función para proveer servicios de voz, mensajería y datos a los clientes. Cada uno de estos elementos se encuentran interconectados a través de estándares y protocolos que son los encargados del traspaso de la información de un nodo a otro. La gestión de estos componentes consiste fundamentalmente en supervisar y controlar la operabilidad de cada uno de ellos. Sin embargo, el creciente uso de las comunicaciones móviles, fijas, computacionales, etc. van de la mano con el crecimiento de las redes y con el uso de múltiples herramientas de control, por lo que la gestión de la red se vuelve cada vez más compleja. Las empresas de telecomunicaciones tienen la obligación de asegurar la disponibilidad de la operabilidad de todos los equipos para satisfacer las expectativas de fiabilidad

y calidad de servicio de los usuarios, esto implica que sea necesario el uso de una sola herramienta para realizar el control de toda una infraestructura, manteniendo la operabilidad de estos equipos al 100%.

1.4. Justificación del Problema

Debido al desarrollo de nuevas tecnologías que prometen servicios innovadores en cuanto a comunicaciones móviles, internet y telefonía fija al usuario, el crecimiento de las infraestructuras de telecomunicaciones es constante. En donde nuevos sistemas de redes son agregados. Cada uno de estos sistemas cumple con una función específica y son controlados por su sistema gestor. Existen múltiples gestores dentro de las distintas áreas de telecomunicaciones, que tienen además de controlar la operabilidad, permite el monitoreo del rendimiento de todos los equipos utilizados. Sin embargo, la gran cantidad de gestores exige el acceso y el uso de muchas herramientas, diferenciadas cada una de ellas; incrementando el personal encargado para el uso de la misma. Usando un MoM que integra diferentes sistemas de red celular, es posible tener una visión general del rendimiento de todos los equipos, servicios y aplicaciones que se están ofreciendo a los usuarios. En caso de que se presenten afectaciones, un MoM es capaz de identificar la causa probable antes de que el cliente informe el problema. Priorizando los eventos que envían todos los dispositivos monitoreados.

1.5. Objetivos del Problema de Investigación

1.5.1. Objetivo General

Implementación de una infraestructura de telecomunicaciones en un sistema de control de incidencias para facilitar el monitoreo de todos los servicios.

1.5.2. Objetivos Específicos

- Integrar de varios tipos de sistemas de redes y grupos de equipos sobre un Administrador de Gestores para una alta disponibilidad de la información referente a cada componente.
- Priorizar incidencias de toda una infraestructura de telecomunicaciones para la prevención de afectaciones en los servicios.
- Consolidar varios tipos de tecnologías y sistemas de redes en una sola interfaz estandarizada para su monitoreo general.

1.6. Hipótesis

Mediante el uso de MoM se puede tener un control y una vista total de las incidencias que tiene una infraestructura completa de telecomunicaciones esto incluye Redes fijas, móviles, switches, enlaces, firewalls, servidores, elementos de red, etc. Lo que permitirá realizar análisis y control del rendimiento como también de la operabilidad de los múltiples equipos que son responsables de brindar los servicios, aplicaciones y comunicaciones en una operadora móvil. Y de proporcionar funciones de gestión en una vista general, consiguiendo interconexión entre los múltiples tipos de sistemas de redes y equipos de telecomunicaciones, utilizando una arquitectura estándar.

1.7. Metodología de Investigación

El paradigma a usarse será el empírico-analítico, debido a que, mediante la implementación de una infraestructura de redes de telecomunicaciones, se verificará de forma práctica la capacidad de un administrador de gestores, integrando diversos sistemas de redes celulares y redes informáticas para su consolidación en una sola interfaz. Posee un alcance descriptivo, porque explica la necesidad actual de contar con instrumentos factibles para mostrar las capacidades de los administradores de gestores. Además, el método será hipotético-deductivo, ya que mediante la hipótesis indicada con antelación se procura establecer una práctica generalizada.

Capítulo 2: Redes de una Infraestructura de Telecomunicaciones

Las redes de telecomunicaciones son sistemas de comunicación de difusión que disponen de activos de cómputo y telecomunicaciones específicamente, un grupo de nodos y enlaces que son capaces de llevar comunicaciones de audio, visuales y de datos. La función primordial de cualquier red de telecomunicaciones es proporcionar una transmisión eficiente de la información desde un punto de origen hasta un punto de terminación.

Las tecnologías de la información y de la comunicación (TIC) son las bases de las transformaciones en la industria de las telecomunicaciones. Las necesidades del ser humano han hecho viable la evolución constante de las formas en que la gente se comunica, entretiene, trabaja, socializa, negocia, etc. (Saló Dobarganes & Rivero Pons, 2015).

2.1. Tipos de Redes de Telecomunicaciones

Las redes de telecomunicaciones comprenden una variedad de componentes como: sistemas de acceso, sistemas de transporte, sistemas BSS (Sistemas de soporte a operaciones), sistemas electrónicos de enlaces y switches, sistemas de energía eléctrica y los controles que rigen su funcionamiento. La consolidación de todos los sistemas de redes permite la transferencia de datos y el intercambio entre múltiples usuarios.

Cuando varios usuarios de medios de telecomunicaciones desean comunicarse entre sí, deben ser organizados por medio de algún tipo de red. En teoría a cada usuario se le puede dar un enlace directo punto a punto a todos los demás usuarios, a esto se lo conoce como una topología conectada

completamente. Pero en la práctica, esta técnica es poco práctica y muy costosa por la cantidad de conexiones internas que se deben realizar para el traspaso de la información especialmente para una red grande y dispersa.

Las redes de telecomunicaciones modernas evitan problemas de latencias y pérdidas de información estableciendo una red vinculada de switches o nodos, de forma que cada usuario está conectado a uno de los nodos. Cada enlace de dicha red se le denomina canal de comunicaciones. Para lograr la comunicación entre un punto a otro se utilizan cables coaxiales, cables de fibra ópticas, enlaces satelitales y ondas de radio para diferentes canales de comunicaciones.

2.1.2. Redes 3G

La tercera generación de redes móviles 3G surgió a inicios del año 2000 e hizo obsoleto los sistemas de generaciones antecesoras ya que el desarrollo de esta tecnología se centró en la mejora de los servicios de voz con capacidades de datos, mayores anchos de banda y el apoyo de servicios multimedia, con el fin de proporcionar mayores capacidades en la red debido al aumento de suscriptores y varios avances tecnológicos (Giotopoulou, 2015).

Esta generación cumple con las especificaciones del estándar global de las Telecomunicaciones Móviles Internacionales 2000 (IMT-2000), en donde se requiere un sistema capaz de soportar rangos de datos de velocidad de 144 kpbs hasta 4 Mbps (Agrawal, Rakesh, Mor, Dubey, & keller, 2015). Opera en la banda de frecuencia 2100 Mhz y tiene un ancho de banda 15-20

Mhz que se utiliza para el servicio de internet, video chat, mensajería, etc. (Vora, 2015).

Las principales características de la red 3G son:

- Velocidades hasta 4 Mbps
- Llamadas celulares.
- Aumento de ancho de banda y velocidades de transferencia de datos para acomodar aplicaciones basadas en web y archivos de audio y video (Criollo & Javier, 2016).
- Proporciona comunicaciones con menor latencia en comparación con generaciones antecesoras gracias a la evolución de sus elementos de red (Giotopoulou, 2015).
- Mensajería entre múltiples proveedores de correo electrónico como Outlook, Gmail, Yahoo, etc.
- Aumento de seguridad en conexiones web, videoconferencias, juegos 3D, transferencias de archivos, mensajería y llamadas, aplicaciones, etc. (Agrawal et al., 2015).
- Mayor cobertura de celdas celulares, gracias a su clasificación de acuerdo a las zonas (macro celda, micro celda y pico celda). (Vora, 2015)

2.1.2.1. Infraestructura de red 3G

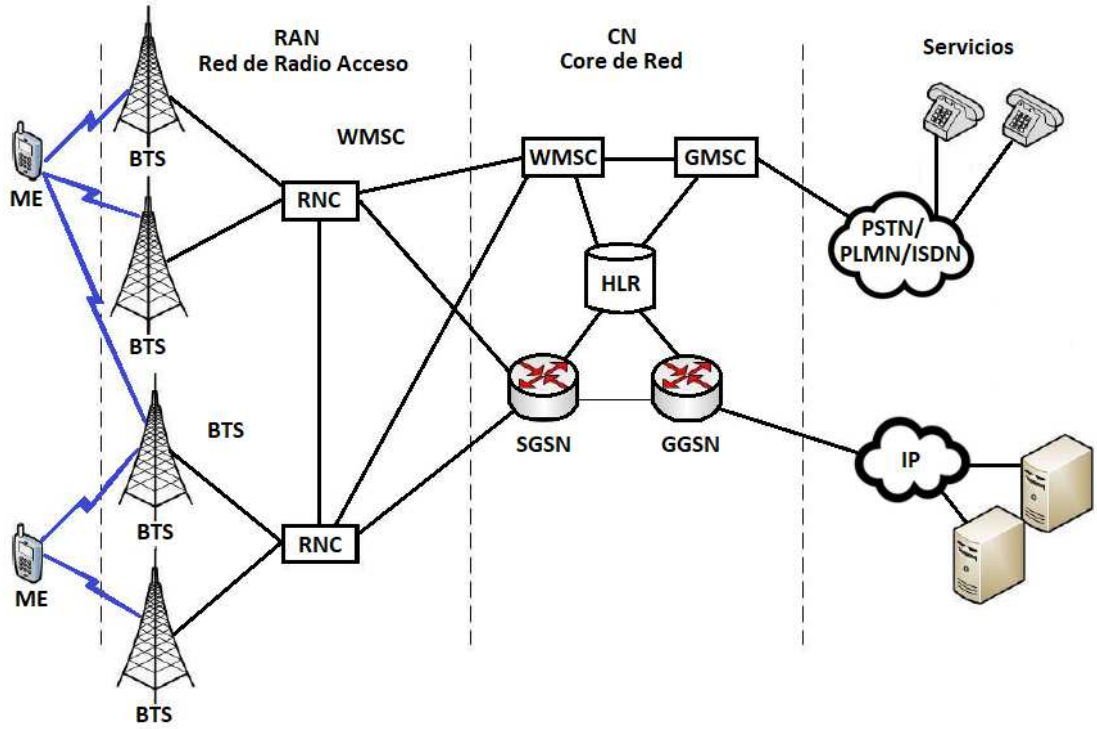


Figura 2. 1: Arquitectura de red 3G

Fuente: (Giotopoulou, 2015).

La red 3G consiste de 3 partes: ME (Equipo móvil), UTRAN (Red de Acceso Radio Terrestre UMTS) y el core de la red (CN).

ME (Equipo móvil) o UE (Equipo de usuario) se basa en el teléfono móvil y la tarjeta SIM (Módulo de identidad del suscriptor) llamada USIM (Universal SIM) que contiene datos específicos de los usuarios y permite la entrada autenticada del suscriptor en la red (Vora, 2015).

ME es capaz de trabajar en tres modos:

- Modo CS (Conmutación por circuito)
- Modo PS (Conmutación por paquetes)
- Modo CS/PS

En el modo CS, el equipo solo está conectado a la red central mientras que en el modo PS el equipo solo está conectado al dominio PS. El modo

CS/PS permite trabajar simultáneamente para ofrecer servicios tanto CS como PS (Agrawal et al., 2015).

2.1.2.2. UTRAN

Los componentes de la red de acceso de radio (RAN) son:

- Estaciones bases o nodos B, tienen como funciones controlar la potencia de bucle cerrado, codificación de canales físicos, modulación y demodulación, transmisiones de interfaz de aire y manejo de recepción y error (Giotopoulou, 2015).
- Controlador de red de radio o RNC el cual tiene las funciones de control de recursos de radio y gestión, control de energía, asignación de canal, control de admisión, cifrado, segmentación y reensamblaje (Criollo & Javier, 2016).

2.1.2.3. Core de la red o red troncal (CN)

La principal función de la red troncal es proporcionar conmutación, enrutamiento y tránsito para el tráfico de usuarios. El CN también contiene las bases de datos y las funciones de administración de la red. La arquitectura CN básica para la red 3G se basa en la red GSM con GPRS. Todos los equipos deben ser modificados para la operación y los servicios de red 3G. Se divide en los dominios CS y PS (Giotopoulou, 2015).

Los componentes de la red troncal son:

GMSC (Centro de conmutación de servicios móviles) o Gateway, que es un elemento conmutado por circuitos, se utiliza para enrutar llamadas fuera de la red móvil. En particular cuando un usuario móvil que proviene fuera de

la red móvil quiere realizar una llamada o el suscriptor quiere hacer una llamada a un usuario fuera de la red móvil la llamada se enruta a través de la GMSC (Giotopoulou, 2015).

VLR (Registro de localización del visitante) es también un elemento conmutado por circuitos, contiene la información sobre los suscriptores que vagan dentro del área de la localización del centro móvil de la conmutación (MSC). La función principal de VLR es minimizar el número de consultas que MSCS debe realizar al registro de ubicación de inicio (ELO), que contiene datos permanentes sobre los suscriptores de la red celular (Agrawal et al., 2015).

SGSN (Nodo de servicio GPRS) es un elemento de conmutación de paquetes que remite el acceso a los recursos de red en nombre de los suscriptores móviles e implementa la directiva de programación de paquetes entre diferentes clases de QoS (Calidad e servicio). Es responsable de establecer el contexto de protocolo de datos (PDP) con el GGSN (Nodo de soporte GPRS Gateway) al activarse.

GGSN (Nodo de soporte GPRS Gateway) elemento de conmutación de paquetes que es responsable de la interoperabilidad entre la red GPRS y las redes de conmutación de paquetes externas. Desde el punto de vista de las redes externas GGSN es un router a una sub-red porque recibe los datos dirigidos a un usuario específico y comprueba si el usuario está activo. GGSN reenvía los datos al SGSN que requiera el usuario móvil, pero si el usuario móvil está inactivo los datos se descartan. Asigna direcciones IP a usuarios móviles y es responsable de la facturación de los servicios ofrecidos (Criollo & Javier, 2016).

2.1.3. Redes 4G

4G LTE es completamente un sistema basado en el protocolo IP (Internet Protocol) y en conmutación de paquetes. Lo que hace posible que además de soportar voz, datos y otros servicios de la red 3G, proporcione acceso a internet de banda ancha móvil permitiendo el desarrollo de nuevas aplicaciones basadas en IP y en internet como VoIP (Voice over IP) (Giotopoulou, 2015).

Esta tecnología nació comercialmente en los años 2010 y 2011 debido al aumento de dispositivos y de la demanda de mayores servicios con altas tasas de velocidad en comparación con las redes 2G y 3G. Dado que existen disposiciones en LTE para la interoperabilidad con los sistemas existentes, existen varias rutas disponibles para conectarse a la red, es decir un operador con generaciones anteriores es capaz de conectarse a la actual red 4G LTE (Cárdenas Lino, 2016).

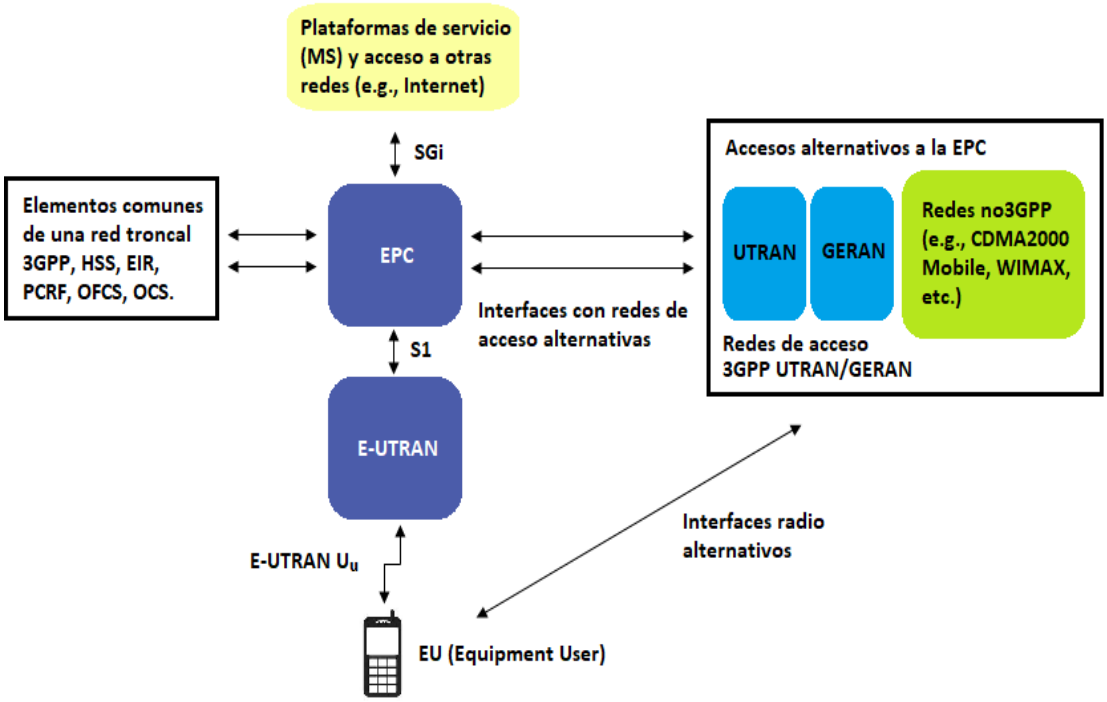


Figura 2. 2: Arquitectura de los sistemas de redes 4G LTE
Fuente: (Santacruz & Garcia, 2017)

2.1.3.1. Arquitectura de la Red 4G LTE

La arquitectura de la red 4G LTE consta de 3 partes:

1.- E-UTRAN o la red de acceso de radio terrestre UMTS evolucionada, que es la interfaz de aire del sistema de red y es la sustitución de la tecnología UMTS que se especificaron en las redes 3GPP. Consiste en UE (Equipment User) que son los dispositivos a través de los cuales el usuario se conecta a la red y los EnodeBS que son las versiones evolucionadas de NodeBS (Elemento de la red 3G) (Santacruz & Garcia, 2017).

2.- EPC o el núcleo de paquetes evolucionado que tiene como función proporcionar conectividad “Always on”, soporte de traspaso y el transporte de los paquetes de voz (González Espinoza & Morocho Lovato, 2017).

3.- Plataformas de servicios que tiene como función proporcionar los múltiples servicios de internet al usuario.

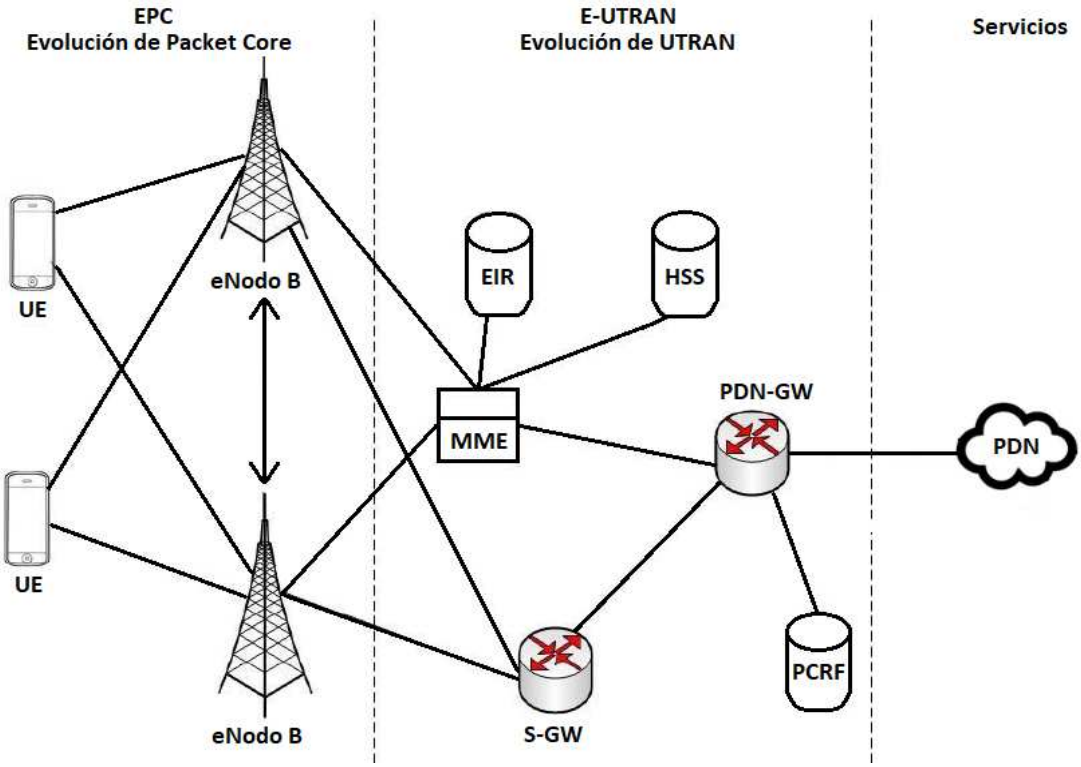


Figura 2. 3: Arquitectura de elementos de red 4G
Fuente: (Giotopoulou, 2015)

2.1.3.2. Funciones de los elementos de red

E-NodoB es una evolución del nodoB de la red 3G. La combinación con funcionalidad de controlador de radio. La combinación de estos dos componentes reduce la latencia a medida que la señalización entre el eNodoB u la red de acceso de radio se elimina. Contiene los transmisores y receptores de radio que generan: la modulación y demodulación de señales de radio, codificación delantera de la corrección de errores y todo el proceso requerido al crear y recibir la señal de radio. En particular gestiona los recursos de radio para determinar qué señales de radio deben ser asignadas y que configuración debe ser aplicada para soportar el servicio deseado (Cruz Fabian & Flores Galindo, 2017).

MME (Entidad de gestión de la movilidad) es el nodo de control que procesa la señalización entre UE y el CN. Los protocolos que se ejecutan entre la UE y el CN se conocen como protocolos de estrato sin acceso (NAS). Entre sus funciones se encuentran: funciones relacionadas con la gestión del portador que incluye el establecimiento, mantenimiento y liberación de los portadores y es manejado por la capa de administración de sesiones en el protocolo NAS; funciones relacionadas con la administración de conexiones que incluye el establecimiento de la conexión y la seguridad entre la red y el equipo del usuario UE, es manejada por la capa de conexión o administración de movilidad en la capa de protocolo NAS (Cruz Fabian & Flores Galindo, 2017).

EIR (Funcionalidad del registro de identidad del equipo) es una base de datos que contiene el IMEI de todos los teléfonos marcados como lista

negra. Esto permite a los operadores móviles evitar el uso de teléfonos robados en su red (Santacruz & Garcia, 2017).

HSS (Servidor de suscriptor de inicio) es una base de datos central manejada desde GSM y UMTS (antes llamado HLR) que contiene información acerca de todos los suscriptores de la operadora de red. También contiene información sobre la PDNs (Red de paquetes de datos) a la que el usuario puede conectarse, esto puede tomarse como un nombre de punto de acceso (APN) que es una etiqueta de acuerdo con las convenciones de nomenclatura de DNS (describen el punto de acceso a la PDN) o una dirección PDN que indica las direcciones de IP suscrita. El HSS puede integrar el centro de autenticación (AUC), el cual genera los vectores para las claves de autenticación y seguridad (Cárdenas Lino, 2016).

S-GW (Servicio de Gateway) actual como un enrutador y remite datos entre la estación base y la puerta de enlace PDN (PDN-GW). Realiza el filtrado de paquetes para los datos del usuario y marca los paquetes en el enlace ascendente y descendente introduciendo el punto de código de servicio diferenciado correcto de modo que esos paquetes puedan ser dados el tratamiento apropiado para garantizar la calidad del servicio (Giotopoulou, 2015).

PDN-GW (Gateway de la red de paquetes de datos) proporciona acceso de la entrada a PDN (puerta de enlace hacia el internet) y consulta el HSS para encontrar la ubicación real del usuario, porque en caso de que se encuentre en una red diferente, el PDN-GW tendrá que reenviar los paquetes hacia otro lugar. Es responsable de la asignación de IP al equipo del usuario. Se conecta a PCRF (Función de políticas y reglas de cobros) donde obtiene

información sobre la calidad del servicio y los servicios generales que se aprueban para un usuario en particular. Esta información se utiliza junto con el filtrado de paquetes y la inspección de paquetes profundos para que el PDN-GW pueda realmente hacer cumplir esas reglas y recopilar los datos necesarios para cobrar los servicios prestados (Giotopoulou, 2015).

PCRF (Función de control de políticas y reglas de cobros) es un componente responsable de la toma de decisiones de la aplicación de carga hacia un usuario específico. Proporciona control de políticas y decisiones de control de carga basadas en flujo. Soporta detección de flujo de datos de servicio y administra políticas para la gestión y control de la calidad del servicio (González Espinoza & Morocho Lovato, 2017).

2.1.4. Red de comunicaciones conmutadas

Una red de comunicaciones conmutada transfiere datos del origen del destino a través de una serie de nodos de red. El cambio se puede hacer de una o dos maneras. En una red de conmutación de circuitos, se establece una ruta física dedicada a través de la red y se mantiene durante el tiempo que sea necesaria la comunicación (Larsson, 2017). Un ejemplo de este tipo de red es el sistema telefónico tradicional analógico. Por otro lado, una red conmutada por paquetes encamina los datos digitales en pequeños trozos llamados paquetes, cada uno de los cuales procede de forma independiente a través de la red. En un proceso denominado almacenar y reenviar, cada paquete se almacena temporalmente en cada nodo intermedio y, a continuación, se reenvía cuando el siguiente vinculo está disponible (Criollo & Javier, 2016).

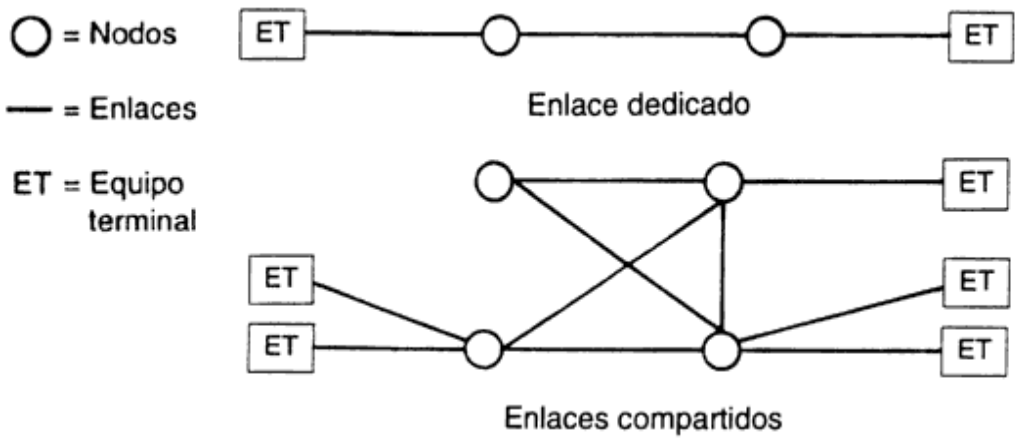


Figura 2. 4: Red conmutada
Fuente: (Criollo & Javier, 2016)

En un esquema de transmisión orientado a la conexión, cada paquete toma la misma ruta a través de la red, y por lo tanto todos los paquetes suelen llegar al destino en el orden en que se enviaron, por lo contrario, cada paquete puede tomar un camino diferente a través de la red en un esquema de datagramas o conexión. Dato que los datagramas no pueden llegar al destino en el orden en que fueron enviados, están numerados para que puedan ser correctamente reensamblados.

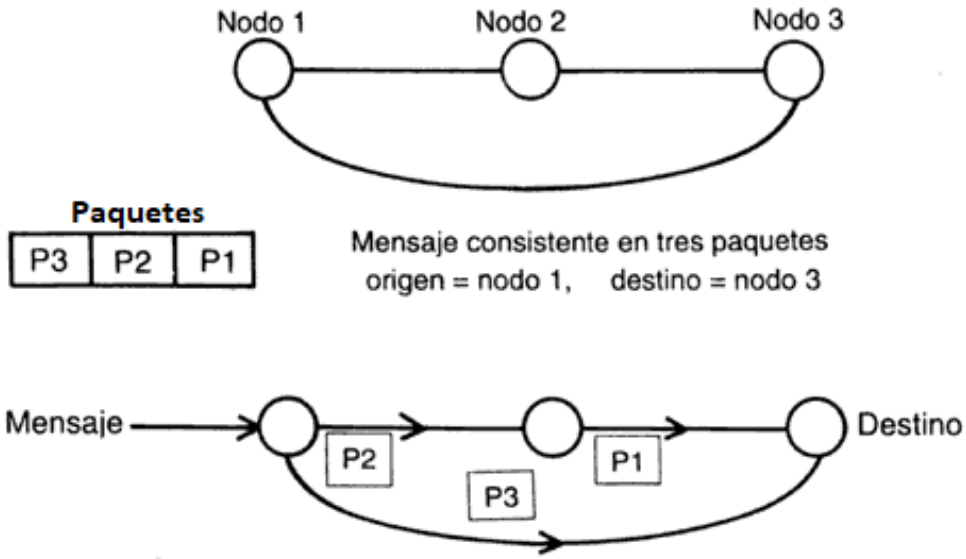


Figura 2. 5: Conmutación de paquetes
Fuente: (Criollo & Javier, 2016)

2.1.5. Redes de difusión

Una red de difusión evita los complejos procedimientos de enrutamiento de una red conmutada asegurándose de que todos los demás nodos de la red reciban las transmisiones de cada nodo. Por lo tanto, una red de radiodifusión solo tiene un canal de comunicaciones único (Larsson, 2017).

Por ejemplo, una red de área local cableada se puede configurar como una red de difusión, con un usuario conectado a cada nodo y los nodos normalmente dispuestos en una topología de bus, estrella o anillo, como se muestra en la siguiente figura. Los nodos conectados entre sí en una LAN inalámbrica pueden emitirse mediante enlaces radiofónicos u ópticos. En una escala más grande, muchos sistemas de radio por satélite son redes de difusión, ya que cada estación de tierra dentro del sistema puede normalmente escuchar todos los mensajes transmitidos por un satélite (Agubor, Chukwudebe, & Nosiri, 2015)

2.1.6. Tipos de topología de redes

Los equipos, switches y terminales interconectados por enlaces de red se denominan como nodos colectivos. El propósito del control de red es proporcionar una conexión entre los nodos que necesitan comunicarse. La disposición de los nodos y enlaces en una red se denomina topología. Una variedad de arreglos es posible, cada uno aplicado de acuerdo al ambiente en el que represente mayores beneficios. La topología de red tiene que adaptarse a la estructura de la unidad organizativa que utilizará la red (Alarcon, Javier Zorzano Mier, Jevtić, & Andina, 2008).

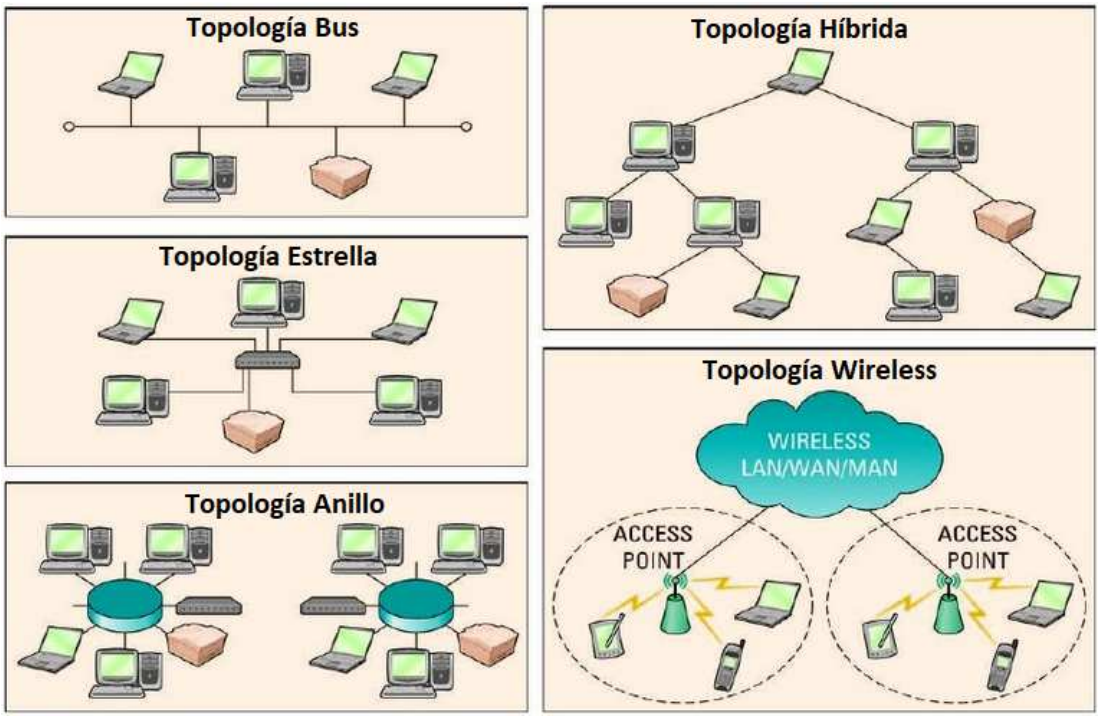


Figura 2. 6: Tipos de topologías de red
Fuente: (Alarcon et al., 2008)

2.2. Tipos de comunicación para el control de Elementos de Red

Existen varios tipos de comunicación entre los elementos que complementan una red entre ellos los más usados para su control y gestión son el protocolo SNMP y el estándar Corba.

2.2.1. Comunicación SNMP

El protocolo de administración SNMP fue propuesto por Internet Engineering Task Force (IETF) en 1998 para administrar redes IP. Sus siglas SNMP significan Protocolo simple de administración de redes y a simple se refiere a que funciona silenciosamente de manera eficiente sobre las redes típicamente encima de UPD (NSW, 2017).

Es un protocolo de capa de aplicación utilizado para administrar y supervisar dispositivos de diversos tipos de redes y sus funciones. SNMP proporciona un lenguaje común para que los dispositivos de red retransmitan

información de administración dentro de entornos de un único multiproveedor en una red de área local (LAN) o en una red de área amplia (WAN) (Kona & Xu, 2002).

Considerado uno de los protocolos más ampliamente utilizados, SNMP es apoyado en una amplia gama de hardware, desde equipos de red convencionales y móviles como Elementos de redes móviles, routers, switches, firewalls físicos, sondas, puntos de accesos inalámbricos, etc. a terminales como impresoras, escáneres, UPS, Aires, Power Plants y dispositivos IOT (Internet of things). Además de hardware SNMP puede utilizarse para supervisar servicios como el protocolo de configuración dinámica de host (DHCP) (NSW, 2017).

Los agentes de software de estos dispositivos y servicios se comunican con un sistema de administración de red (NMS), también conocido como un administrador de SNMP, a través de SNMP para retransmitir información de estado, niveles de umbrales, cambios de configuración, etc (Abdelwahab Saleh, 2017).

El uso de SNMP sobre un Gestor o NMS permite a un administrador de red gestionar y superar todos los nodos desde única interfaz, que normalmente puede soportar comandos por lotes y alertas automáticas. SNMP es descrita en el estándar de solicitud de comentario (RFC) establecido por la IEFT (Internet Engineering Task Force) (NSW, 2017).

2.2.1.1. Componentes de SNMP

El Agente SNMP, este componente se ejecuta en el hardware o servicio que se está monitoreando, recopilando datos sobre varias métricas como el

uso de ancho de banda, capacidad de celdas móviles, status de nodos, falencias de hardware y/o software, almacenamiento, etc. Cuando el administrador de SNMP lo consulta, el agente devuelve esta información al sistema de administración. Un agente también puede notificar proactivamente a los sistemas gestores si se produce un error. La mayoría de los dispositivos vienen con un agente SNMP preinstalado; normalmente solo necesita ser activada y configurada (Abdelwahab Saleh, 2017).

Recursos y dispositivos: Estos son los nodos en los que se ejecuta un agente.

El administrador SNMP (Gestor o NMS), es una plataforma de software que funciona como una consola centralizada alimentada de la información enviada por los agentes. El envío de la información puede ser constantemente o con solicitudes de intervalos regulares. Lo que el administrador de gestores puede hacer con esa información depende de su capacidad, interpretación y configuración (Abdelwahab Saleh, 2017).

La base de información gestionada (MIB), es una pequeña base de datos que contiene un archivo de texto con extensión (.MIB), detalla y describe todos los objetos utilizados por un dispositivo determinado que se puede controlar o consultar mediante SNMP. Esta base de datos debe ser publicada y cargada en cada uno de los sistemas gestores, para que pueda identificar y supervisar el estado de estas propiedades. A cada elemento MIB se le asigna un identificador de objeto (OID) (Abdelwahab Saleh, 2017).

Los identificadores de objetos (OIDs) son nada más que una etiqueta numérica que identifica un objeto específico. Un objeto es cualquier elemento de red (Autor, 2018).

2.2.1.2. Funcionamiento de SNMP

SNMP realiza una multitud de funciones, basándose en una combinación de comunicaciones “push and pull” entre los dispositivos de red y el sistema de gestión. La variedad de información que retransmite SNMP dependerá directamente de la red, dispositivo, servidor, aplicación, base de datos y de los sistemas que se estén monitoreando. Es posible la interacción del protocolo SMTP para la transferencia de correos electrónicos o mensajes de texto de alertas si se excede un umbral definido o si se detecta la pérdida de conexión con el dispositivo (Abdelwahab Saleh, 2017).

La mayoría de veces SNMP opera bajo un modelo sincrónico, con comunicación iniciada por el administrador de SNMP y el agente que envía una respuesta. Estos comandos y mensajes son típicamente transportados sobre el protocolo de datagramas de usuario (UDP) o el protocolo de control de transmisión/Protocolo de internet (TCP/IP), se conoce como unidades de datos de protocolo (PDUs) (Huawei, 2014).

Tabla 2. 1: Funciones de SNMP

GET	Generado por el administrador de SNMP y enviado a un agente para obtener el valor de una variable, identificada por su OID en un MIB.
RESPONSE	Enviado por el agente a el administrador de SNMP, emitido en respuesta a una solicitud GET. Contiene los valores de las variables solicitadas.
GETNEXT	Enviado por el administrador de SNMP al agente para recuperar los valores del OID siguiente en la jerarquía de MIB.
GETBULK	Enviado por el administrador de SNMP al agente para obtener tablas grandes de datos realizando varios cmandos GETNET.
SET	Enviado por el administrador de SNMP al agente para emitir configuraciones o comandos.
TRAP	Se ha producido una alerta asincrónica enviada por el agente al administrador de SNMP para indicar un evento significativo, como un error o un fallo.

Fuente: (NSW, 2017).

2.2.2. Comunicación por estándar CORBA

CORBA (Common Object Request Broker Architecture) es una arquitectura y especificación para crear, distribuir y administrar objetos de programas distribuidos en una red. CORBA es permitido en sistemas gestores y componentes de diferentes ubicaciones y desarrollados por diferentes proveedores para comunicarse en una red a través de un intermediario de interfaces, incluso en múltiples lenguajes de programación. De tal modo que facilita la comunicación y la convergencia de tecnologías distribuidas en entornos heretogéneos. Fue desarrollada por el grupo de gestión de objetos en la década de 1990 (Aleksy, Korthaus, & Schader, 2007).

El concepto esencial en CORBA es el ORB (Object Request Broker). El soportar ORB en una red de clientes y servidores en diferentes equipos facilita la comunicación y significa que un programa cliente (que puede ser un objeto) pueda solicitar servicios desde un programa o un objeto de servidor sin tener que conocer la ubicación en una red distribuida o cuál es la interfaz. En otras palabras, es el encargado en enviar peticiones hacia los objetos y devolver las respuestas al usuario que haya requerido sin tomar en cuenta la localización, el lenguaje de programación, estado de ejecución y mecanismo de comunicación entre los objetos (Zhen, Qixin, Lo, & Lei, 2009).

ORB es considerado un software que implementa las especificaciones de CORBA. Es el corazón del estándar y es responsable de todos los mecanismos necesarios para realizar las siguientes tareas (NSW, 2017):

- Busca la implementación del objeto para la solicitud.
- Prepara la implementación del objeto para recibir la solicitud.
- Comunicar los datos que realizan la solicitud.

2.3. Sistemas de alarmas

Los modernos y actuales equipos son capaces de emitir alarmas cada que han sufrido un cambio en su configuración o alguna afectación. Cuando el equipo supera el inconveniente de igual manera emite una alarma de cancelación. Estas alarmas son enviadas hacia las herramientas que controla su operación, función, status y disponibilidad. Un MoM recopila información de diferentes elementos que pertenecen a diversos sistemas de red para detectar anomalías, cambios o fallas. De tal manera que facilita el análisis de la infraestructura remotamente (Autor, 2018).

Capítulo 3: Administrador de Gestores (MoM)

3.1. Definición de MoM

Mom es una plataforma completa y unificada que optimiza al mismo tiempo los costos de TI (Tecnología de la información), demuestra transparencia, aumenta el valor del negocio, controla el riego y asegura la calidad del servicio. Simplifica, estandariza y controla todos los componentes de una red de telecomunicaciones de manera eficiente. (Armijos Farez, 2017)

3.2. Ventajas de la implementación de MoM

Las ventajas de la implementación de MoM sobre una infraestructura de telecomunicaciones garantiza la calidad y la alta disponibilidad de los servicios que se ofrece al cliente. Al tener un control total de las incidencias es posible prevenir y solucionar afectaciones en tiempo real.

Tabla 3. 1: Capacidad de un MoM

Gestión de impacto de eventos y servicios	Analítica de datos
▪ Monitorear, procesar y mantener eventos que se producen en recursos de telecomunicaciones. ▪ Proporciona soluciones en tiempo real para la detección y la resolución proactiva de problemas de telecomunicaciones.	▪ Utilizar los datos recolectados de la infraestructura para detectar anomalías y predecir interrupciones. ▪ Proporcionar un centro de investigación para comprender mejor, sintonizar y abordar las anomalías de las telecomunicaciones.

Fuente: (Armijos Farez, 2017)

3.3. BMC

BMC Software Inc. es una empresa de reconocimiento mundial que provee soluciones de tecnologías de la información y comunicación ofreciendo velocidad, agilidad y eficiencia desde un mainframe hasta redes móviles, fijas,

redes en Cloud y mucho más. Entre sus diversas soluciones proporciona herramientas en cuanto a Administradores de Servicios, Automatización, Operación y Mainframe (BMC, 2018).

92 de 100 Global Forbes confían en BMC para acelerar sus iniciativas digitales. Con más de 35 años siendo líderes en soluciones de administración de redes y equipos TI (BMC, Wilson, & West, 2016).

3.4. ProactiveNet

Se define como una plataforma integrada que combina administración de eventos y análisis de datos en una única solución de uso práctico que permite el control de afectaciones dentro de una red de Telecomunicaciones. La alta capacidad de la herramienta permite la integración de la mayoría de gestores, equipos de Telecomunicaciones, elementos de red, etc. Que pertenecen a una red corporativa. ProactiveNet es un administrador de gestores que consolida varios tipos de redes en una sola interfaz web lo que facilita el monitoreo de manera completa de los servicios brindadas al cliente (BMC et al., 2016).

Esta herramienta administra eventos generados de los servidores que forman parte de su infraestructura y de eventos externos que provienen de integraciones de otros fabricantes que se comunican a través del protocolo SNMP, estándar Corba, estándar ASCII (BMC et al., 2016).

Es necesario el uso de agentes y adaptadores en todos los dispositivos y servidores que brinden servicios para la comunicación con el Servidor principal ProactiveNet. Los eventos son recibidos en el servidor ProactiveNet para el análisis de los datos con el fin de detectar anomalías y desviaciones

de los patrones normales de comportamiento definidas con umbrales. Estos eventos pueden presentar afectaciones o posibles afectaciones de los servicios (Autor, 2018).

3.4.1. Requerimientos de Hardware

La siguiente tabla menciona los requerimientos de hardware que deben ser considerados cuando se determine el tamaño del ambiente de la infraestructura a monitorear. Valido para todos los servidores que conformarán la infraestructura de ProactiveNet (Servidor principal, Servidor de celdas remotas y Base de datos).

Tabla 3. 2: Requerimientos de Hardware

Ambiente	**Ítem de configuración**	**Administrador de eventos de datos y administrador de eventos con impacto**
Pequeño	Plataforma	• Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Procesador Intel Core i7. CPU: 4 vCPUs, Frecuencia: 2.2 GHz y Threads: 16 • Red Hat Enterprise Linux 6.0, 7.0, Procesador: x86-64: AMD64, Intel EM64T. CPU: 4 vCPUs de, Frecuencia: 2.2 GHz y threads: 16 • SPARC Enterprise T-Series or M-Series Servers. CPU: 4 CPUs de 3 GHz, UltraSPARC T2 y ≥ 32 threads.
	RAM	• 8 GB
	Configuración de Almacenamiento	• 200 GB (30 GB para el servidor + 170 GB para la base de datos) • 15000 RPM drive o un tier 1 SAN storage (2-4 GBps SAN con canal dedicado)
Mediano	Plataforma	• Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, (64-bit), Procesador Intel Core i7. CPU: 4 vCPUs, Frecuencia: 2.2 GHz y Threads: 16 • Red Hat Enterprise Linux 6.0, 7.0, Procesador: x86-64: AMD64, Intel EM64T.

		CPU: 4 vCPUs de, Frecuencia: 2.2 GHz y threads: 16 • SPARC Enterprise T-Series or M-Series Servers. CPU: 4 CPUs de 3 GHz, UltraSPARC T2 y ≥ 32 threads.
	RAM	• 16 GB + 4 GB adicionales requeridos para la visualización de información.
	Configuración de Almacenamiento	• 300 GB (50 GB para el servidor + 250 GB para la Base de Datos) • 15000 RPM drive o un tier 1 SAN storage (2-4 GBps SAN con canal dedicado)
Largo	Plataforma	• Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, (64-bit), Procesador Intel Core i7. CPU: 8 vCPUs, Frecuencia: 2.2 GHz y Threads: 16 • Red Hat Enterprise Linux 6.0, 7.0, Procesador: x86-64: AMD64, Intel EM64T. CPU: 8 vCPUs de, Frecuencia: 2.2 GHz y threads: 16 • SPARC Enterprise T-Series or M-Series Servers. CPU: 8 CPUs de 3 GHz, UltraSPARC T2 y ≥ 32 threads.
	RAM	• 32 GB + 8 GB adicionales requeridos para la visualización de información.
	Configuración de Almacenamiento	• 1 TB (250 GB para el servidor + 750 GB para la base de datos. • 15000 RPM drive o un tier 1 SAN storage (2-4 GBps SAN con canal dedicado)

Fuente: (BMC et al., 2016)

3.4.2. Diagrama para integración de Infrastructuras

El siguiente diagrama de solución puede ser aplicado para infraestructuras de TI y/o de Telecomunicaciones en donde determinado Gestor realiza el envío de eventos a través de SNMP o CORBA hacia el servidor de celda remota y son escuchados por un determinado puerto. Dicho servidor es monitoreado constantemente por medio del agente Patrol que mide a nivel de sistema operativo el rendimiento, CPU, status, filesystems (Particiones de discos), Memoria, entre otros, para garantizar su alta

disponibilidad. Esto es como parte del auto monitoreo que realiza el MoM sobre su misma infraestructura y las infraestructuras que se integrarán (Autor, 2018).

El servidor de celda remota contiene varias celdas, en donde cada una de ellas puede representar un gestor o determinados grupos de equipos. Para cada celda se le asigna un puerto específico. El gestor o equipo que se requiera integrar deberá apuntar el envío de eventos hacia la IP del servidor de celda remota y el puerto determinado (Autor, 2018).

La celda es la encargada de la interpretación de la información mediante una base de conocimiento denominada KB. En ella se configurarán las reglas de generación de alarmas, cancelación de alarmas, deduplicación, correlaciones, políticas, propagación, etc. Después de que el evento haya sido procesado en la celda, es propagado hacia un colector que se encargará de consolidar varias celdas (Incluso celdas de otros servidores) para una visión general de toda una infraestructura (Autor, 2018).

En la consola de operación (Interfaz Web) el usuario podrá visualizar todas las alarmas de las celdas y de los colectores. En ella se puede tener control de las incidencias como también la realización de reportes, análisis de causa raíz, búsqueda de anomalías por filtros y la visualización completa del status de toda la infraestructura integrada (Autor, 2018).

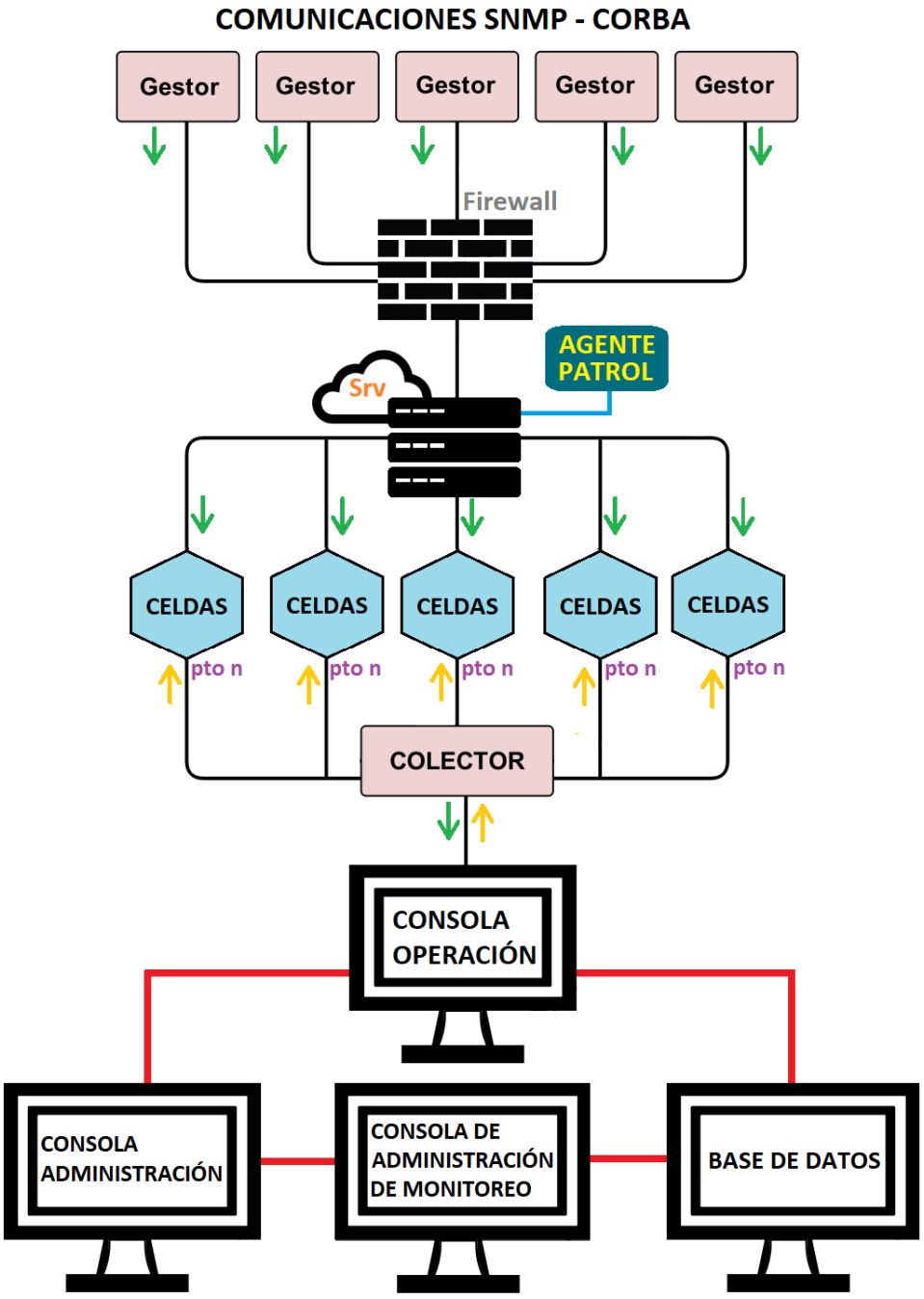


Figura 3. 1: Diagrama de solución para la infraestructura de una empresa de Telecomunicaciones
Fuente: Elaborado por el autor.

3.5. Arquitectura de ProactiveNet

La herramienta ProactiveNet tiene varios componentes esenciales para su operabilidad, como lo son (BMC et al., 2016):

- Servidor ProactiveNet

- Consola de Administración central de monitoreo.
- Servicio de integración
- Celdas
- Modelamiento de servicio
- Base de datos
- Consolas de Administración
- Consola de Operación

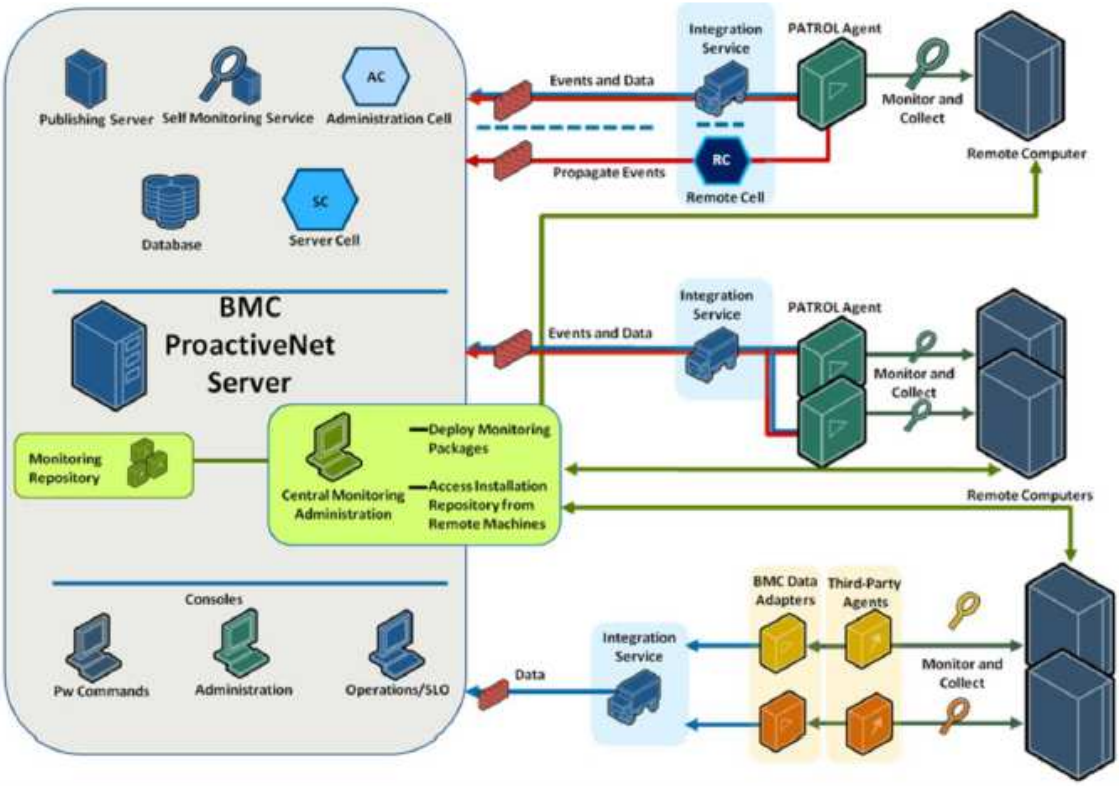


Figura 3. 2: Arquitectura y componentes ProactiveNet
Fuente: (BMC et al., 2016)

3.5.1. Servidor ProactiveNet

Es el componente principal de ProactiveNet que recibe eventos y datos de varias fuentes, que son procesados utilizando un potente motor analítico e instrucciones adicionales de procesamiento de eventos almacenados en una base de conocimientos (KB – Knowledge Base). Utiliza un modelo de servicio

para poner monitores y eventos en un contexto de servicio empresarial (BMC et al., 2016).

Entre sus funciones se tiene:

- Configura y controla los agentes de ProactiveNet para la recolección de datos de diferentes fuentes externas (BMC, 2018).
- Almacena y presenta datos recolectados en forma de gráficos, informes, vistas y eventos en la consola de operación (BMC et al., 2016).

Recibe eventos y datos de:

- Agentes PATROL
- Celdas remotas
- Eventos y datos de fuentes Third-party (Desarrollados por terceros)

Los componentes que comprenden el servidor de ProactiveNet son (BMC et al., 2016):

- Servidor de celdas
- Administración de celdas
- Consola de operación
- Consola de administración
- Base de Datos
- Servicio de Automonitoreo
- Publishing Server

3.5.2. Consola de Administración Central de Monitoreo

Se utiliza la Administración central de monitoreo para administrar la configuración de los Agentes Patrol en uno o más servidores secundarios del servidor ProactiveNet. Presenta los diagramas de arquitectura para

implementaciones de servidor único y de varios servidores que incluyen la administración total del monitoreo (BMC et al., 2016).

3.5.2.1. Agente Patrol

Patrol es un sistema, aplicaciones y una herramienta de gestión de eventos. Propociona un entorno en el que se puede supervisar el estado de cada recurso virtal en el entorno distribuido que se esté administrando, como equipos host, servidores físicos o virtuales, bases de datos, servicios y aplicativos de Windows y Unix. (BMC, 2018)

El siguiente gráfico muestra la implementación del servidor desde una perspectiva de administración central de supervisión. En donde el Servidor Central de ProativeNet será el encargado de recolectar toda la información de los servidores que están siendo monitoreados por el Agente Patrol que están integrados por medio del servicio de integración.

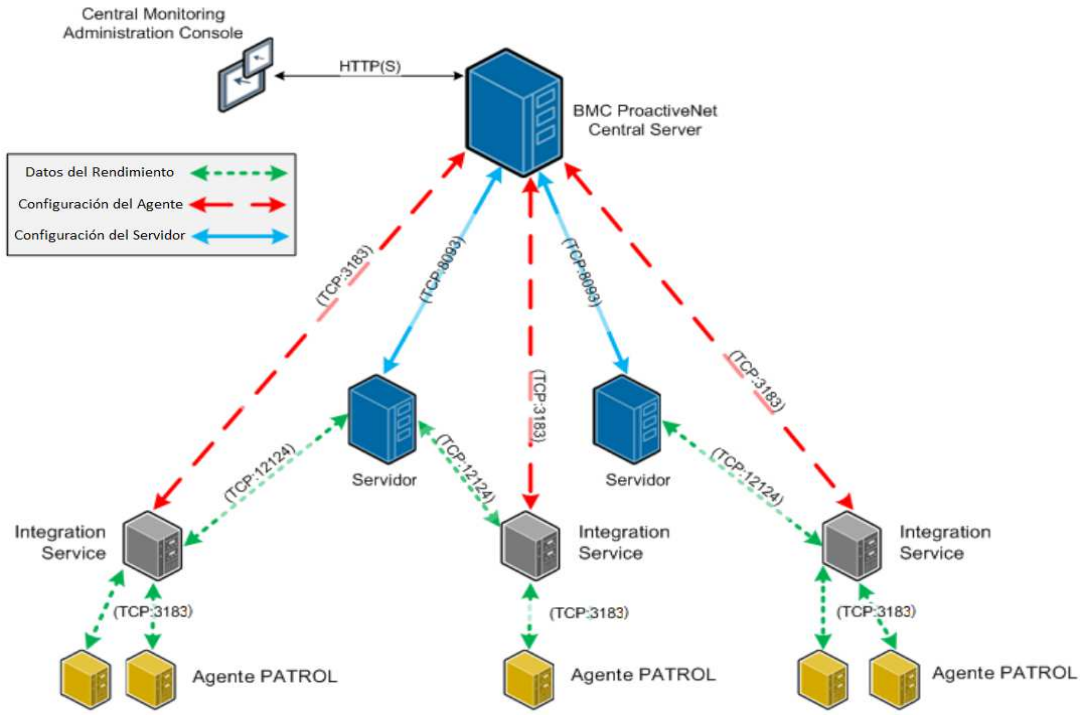


Figura 3. 3: Consola de Administración Central de Monitoreo
Fuente: (BMC, 2018)

3.5.3. Servicio de Integración

El servicio de integración permite que el servidor ProactiveNet recopile de forma remota datos estadísticos de todos los sistemas operativos soportados. El servicio de integración obtiene estos datos de Agentes Patrol, Productos HP, Microsoft, IBM y demás productos de terceros para su monitoreo (BMC et al., 2016).

Su instalación incluye los siguientes componentes:

- Adaptadores de eventos
- Administrador de eventos

3.5.3.1. Adaptadores de eventos

Los adaptadores de eventos preparan los datos del evento que son enviados de la fuente origen hasta la consola de operación para el proceso de interpretación mediante un procesador de eventos establecido para cada celda. Estos adaptadores son instalados mediante la implementación de un componente llamado BMC ProactiveNet Integration Service. Que tiene la funcionalidad de permitir la instalación y configuración de los adaptadores en los distintos servidores remotos (BMC et al., 2016).

Los adaptadores de eventos leen, monitorean e interpretan eventos de equipos, servidores, aplicaciones, servicios y demás componentes de fuentes externas que pertenecen a la infraestructura de telecomunicaciones (Autor, 2018).

Proporciona los siguientes grupos de adaptadores:

- Adaptador de eventos log, que recolectan registros provenientes de eventos logs de Windows, Unix

- Adaptadores de eventos

  - Adaptador de archivos logs en sistemas Windows, UNIX

  - Adaptador SNMP

  - Adaptadores IP

Los adaptadores se ejecutan como procesos de fondo y generan eventos de supervisión automática que se pueden visualizar desde la consola de operación. (BMC et al., 2016)

3.5.3.2. Componentes del adaptador de eventos

Cada adaptador, independientemente del tipo, consta de los siguientes componentes:

Parser (Analizador) – el analizador sintáctico separa la secuencia de datos (eventos de origen) en registros y campos mediante expresiones regulares, es decir da formato a los datos recopilados y los convierte en campos para luego pasar por el proceso de asignación de celda remota correspondiente. Cada uno de los adaptadores incluye un dedicado analizador configurado por default (BMC et al., 2016).

Map file – el archivo de mapa distingue cómo se asignan los datos analizados a los atributos de los eventos (Campos de un registro de eventos) y es quien administra la traducción entre un evento específico procedente de una fuente externa y un evento de la celda remota. Los archivos map también se utilizan para filtrar eventos no deseados y para cambiar o agregar datos en el evento de origen. Todos los adaptadores requieren de uno a diferencia de Adaptador de archivos logs de Windows y Unix (BMC et al., 2016).

Tabla 3. 3: Archivos Map predefinidos para cada Adaptador

Adaptador	Archivo map por default
Eventos logs Perl para Windows	mceventlog.map
Archivos Logs	mclogfile.map
SNMP Trap	mcsnmptrapd.map
Archivos de logs Apache	mcapache.map
Syslog de UNIX	mcsyslogd.map
Clientes TCP	mctcpclt.map
Servidores TCP	mctcpsrv.map
Telnet	mctelnet.map
Clientes UDP	mcudpclt.map
Servidores UDP	mcudpsrv.map

Fuente: (BMC et al., 2016)

Definiciones de clases de eventos: los eventos asignados deben traducirse dentro de estructuras de lenguaje C con extensión BAROC. Los datos del evento traducido se convierten en una instancia de evento de una celda.

Configuración – la configuración del adaptador define: una instancia de un tipo de adaptador, el analizador parser a utilizar, los parámetros específicos de un tipo de adaptador y la celda a la que el adaptador reenvía los eventos (BMC et al., 2016).

3.5.3.3. Características de los adaptadores de eventos

Los adaptadores de eventos pueden recopilar eventos, información de origen desde (BMC et al., 2016):

a) Adaptador de eventos/registros Perl para Windows
b) Adaptador de archivos logs
c) SNMP V1, V2 y V3 (Traps)

Todos los adaptadores vienen preconfigurados, para el registro de parámetros y establecimientos de puertos. Sin embargo, es posible modificar

los adaptadores predefinidos y las clases de eventos para implementar nuevos adaptadores de eventos (BMC et al., 2016).

Los adaptadores tienen las siguientes características:

Varias instancias del mismo tipo de adaptador pueden ejecutarse al mismo tiempo (BMC et al., 2016). Por ejemplo, dos adaptadores SNMP pueden configurarse para escuchar en varios puertos diferentes de manera similar. De este modo es posible la integración de varios gestores o grupos de equipos en una celda remota. Del mismo modo múltiples adaptadores de archivos Logs pueden monitorear simultáneamente variedad de registros con ajustes completamente diferentes (Autor, 2018).

Cada instancia de un adaptador está relacionada con un archivo map y dat, quienes son los encargados de la traducción de los eventos que llegan hacia un evento de celda remota. Consiste en un conjunto de enunciados, condiciones y asignaciones (BMC et al., 2016).

Todos los adaptadores de eventos almacenan sus configuraciones en el mismo archivo de configuración denominado mcxa.conf que pueden ser modificados en cuanto a parámetros y configuraciones predefinidas. El proceso mcxa.conf se ejecuta como un proceso en sistemas Unix y como un servicio en sistemas Windows (BMC et al., 2016).

a) Adaptador de eventos/registros Perl para Windows

Este adaptador disponible únicamente para sistemas Windows desarrollado en Perl y ejecutado en el proceso mcxa. Tiene la función de supervisar los eventos y registros del sistema, seguridad y aplicación

generados por el sistema operativo. De modo que traduce la información y la remite en forma de eventos hacia una celda (BMC et al., 2016).

BMC software recomienda utilizar el agente Patrol para una supervisión de eventos y registros más amplia ya que es compatible para sistemas Windows y Unix (BMC, 2018).

b) Adaptador de archivos logs

El adaptador de archivos logs es un lector de archivos que se puede utilizar con cualquier archivo de texto que contenga registros a nivel de sistemas operativos, redes, aplicaciones y seguridad que puedan ser reconocidos por librerías de C de expresiones regulares definidas por Perl. El adaptador puede descubrir automáticamente archivos logs alojados dentro de servidores y bases de datos. (BMC et al., 2016)

A pesar de que el adaptador de archivos logs está destinado a ser un adaptador genérico para cualquier archivo log basado en texto, se suministran configuraciones de adaptadores especiales y archivos de mapa para supervisar registros de logs en sistemas UNIX más conocido como procesos syslog como también los procesos de Apache. Cada una de estas funciones viene incluida por default en el archivo mxca.conf.

c) Adaptador SNMP

Este adaptador consiste en un servidor UDP SNMP que escucha todo tipo de tráfico que utiliza como método de envío SNMP. Incluye el administrador de configuración del adaptador SNMP que convierte la información de los archivos de la base de información gestionada (MIBs) en

las clases de la celda remota y los archivos de configuración de mapas y enumeración utilizados para formatear las capturas en eventos que se propagan hacia las celdas remotas (BMC et al., 2016).

Los archivos MIBs deben ser publicados para el adaptador SNMP antes de empezar a direccionar traps hacia la celda remota. Cuando se recibe la captura SNMP, el adaptador intenta coincidir con el OID de los traps con clases definidas en el archivo map y publica campos en el evento basados en esa definición (BMC et al., 2016).

El proceso de publicación utiliza los MIBs suministrados por default y los MIBs proporcionados por el proveedor. Estos son procesados de acuerdo a la configuración que se le establezca al adaptador para luego ser compilados por mib2map. De este modo cada MIB es procesado y cada tipo de trap dentro de la MIB se convierte en los archivos map, dat y las clases que incorporan a los archivos BAROC (Autor, 2018).

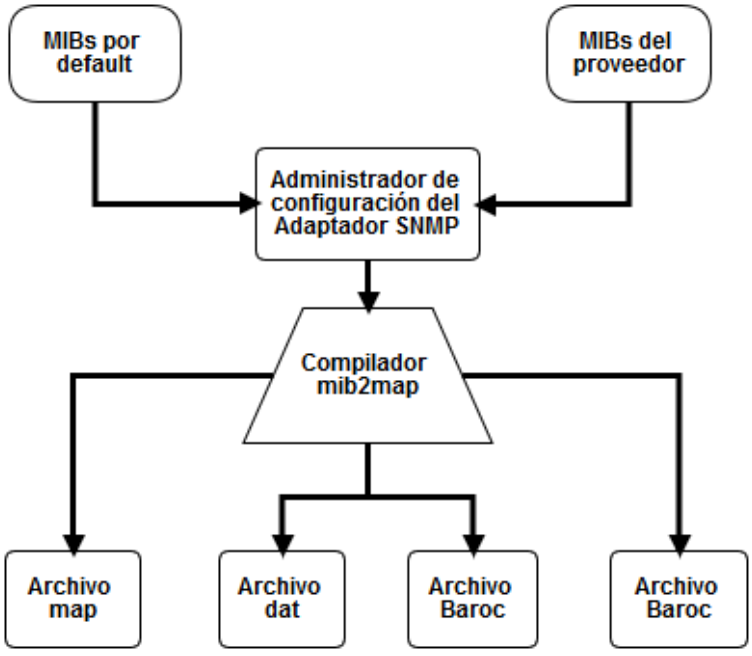


Figura 3. 4: Publicación de Bases de información gestionadas (MIBs)
Fuente: Elaborado por el autor.

3.5.4. Celdas

Las celdas de ProactiveNet son motores de procesamiento de eventos que almacenan todos los eventos y datos en la memoria, así como en el disco en tiempo real. Una celda se ejecuta como un servicio de Windows y como un proceso en UNIX, LINUX, SunOS y demás plataformas soportadas (BMC et al., 2016).

El comportamiento de una celda se rige por su base de conocimientos (KB)

Tiene las siguientes funciones:

a) Recibe datos de eventos de origen de un adaptador, integración, otra celda, API, procesador de tasas o la interfaz de línea de comandos (CLI) (BMC et al., 2016).
b) Analiza y procesa eventos según las reglas y políticas de gestión de eventos definidas en su base de conocimientos (KB).
c) Responde a los eventos ejecutando acciones, tal como se definen en scripts o programas en su base de conocimientos (KB).
d) Propaga eventos seleccionados a destinos especificados (Normalmente colectores) y actualiza los eventos propagados cuando estos se cambian en el origen del evento o en el destino de eventos (BMC et al., 2016).
e) Registra las operaciones de eventos realizadas en un evento.
f) Relaciona un evento con el componente de modelo de servicio apropiado.
g) Calcula el estado de los componentes del modelo de servicio y propaga su estado a los componentes relacionados mediante los modelos de cálculo de estado designados (BMC et al., 2016).

Tipos de Celdas

Existen diferentes tipos de celdas que son aplicados de acuerdo al ambiente de la infraestructura a integrar. Por ejemplo, en un Banco las celdas pueden representar la consolidación de servicios integrados en la misma, que monitorean el status y cambios que sufran en determinados periodos de tiempo. Pero en una red móvil o fija pueden representar celdas en la que se integran sistemas gestores para el control de incidencias sobre la red y sus componentes (Autor, 2018).

3.5.4.1. Servidor de Celda

Funciona como parte del servidor ProactiveNet para proporcionar administración de impactos de eventos y servicios locales. La celda del servidor ProactiveNet también asocia eventos con componentes del modelo de servicio y calcula los estados de los componentes (BMC et al., 2016).

3.5.4.2. Celda de administración

Una celda que se instala automáticamente como parte del servidor ProactiveNet y se mantiene por sí mismo. Su nombre de instancia de celda por default es Admin y contiene una base de conocimientos (KB) especializada (BMC et al., 2016). Esta celda acepta registro, configuración y otros eventos de componentes y aplicaciones de productos BMC.

Esta celda crea las definiciones de los componentes basándose en la información del evento. También utiliza estos eventos para mantener un modelo de servicio de la infraestructura de ProactiveNet, que se puede ver

desde la consola de administración, completa con la configuración y la información de estado real (BMC et al., 2016).

3.5.4.3. Celdas Remotas

Instaladas por separado del servidor ProactiveNet, la celda remota funciona como parte de una red distribuida más grande de celdas que propagan eventos a la celda del servidor ProactiveNet (BMC et al., 2016). Si se implementa la administración de impacto de servicio, la celda remota también asocia eventos con componentes de modelo de servicio y calcula estados de los componentes. Por otro lado, si no se implementa la administración de impacto de servicio, la celda es simplemente una celda de administración de eventos (Autor, 2018).

Las redes de celdas remotas se pueden organizar para servir a cualquier jerarquía empresarial o configurarse para resolver problemas técnicos como limitaciones de red o del sistema (BMC et al., 2016). Se puede configurar una celda remota para alta disponibilidad configurando un servidor de celda primario y un servidor de celda secundario que se usará para fallas o sobrecargas si el servidor de celda primerio sufre afectaciones.

3.5.5. Knowledge Base

Una base de conocimientos o KB define el comportamiento de una instancia de ProactiveNet (También denominada celda). Las clases KB definen que información se contiene en cada evento. Las reglas de KB definen como se procesan los eventos. Se puede modificar la KB para personalizar

su comportamiento en su entorno. Es similar a un script y la celda es el motor que ejecuta el script (BMC et al., 2016).

La KB es una colección compilada de archivos, como reglas de procesamiento de eventos, definiciones de clases y ejecutables, organizadas en una estructura de directorios. Se instalan con cada celda de ProactiveNet. Los archivos KB son cargados por una celda en la hora de inicio. Esta base de conocimientos indica a la celda como formatear datos de eventos entrantes, eventos recibidos de procesos y eventos de visualización en la consola de operaciones. Aunque muchas KBs pueden existir dentro de un entorno de celdas remotos distribuido, cada celda puede asociarse con solo una KB a la vez (BMC et al., 2016).

Durante la instalación de una celda remota, una KB es creada automáticamente para su configuración y proporciona definiciones de datos, instancia de datos, definiciones de recopiladores y reglas para un entorno completamente funcional en el que se procesan eventos y servicios de componentes (Autor, 2018).

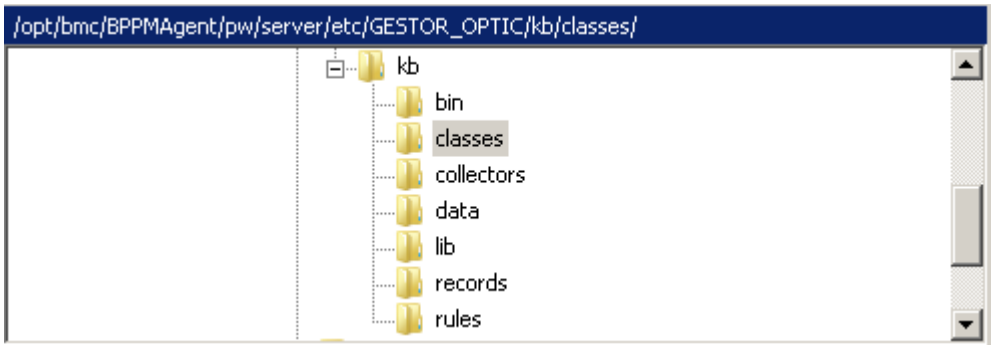


Figura 3. 5: Directorios pertenecientes a la KB de cada celda remota
Fuente: Elaborada por el autor.

3.5.5.1 Componentes de una KB

- Clases de eventos: define los tipos de eventos para aceptar y clasificar los datos del evento de origen para el procesamiento.

- Clases de datos: define las clases y las ranuras de las instancias de datos dinámicos y de los componentes del modelo del servicio.

- Datos dinámicos: funcionan como variables contextuales que pueden proporcionar valores de datos a reglas y políticas durante el procesamiento de eventos (BMC et al., 2016).

- Registros globales: variables globales estructuradas persistentes que mantienen los valores de datos en todas las fases del procesamiento de eventos.

- Reglas de gestión de eventos: instrucciones de procesamiento de eventos que utilizan los datos asociados con un evento, instancias de datos o registros para determinar si, cuándo y cómo responder a nuevos eventos o modificaciones de eventos (BMC et al., 2016).

- Políticas de gestión de eventos: uno de varios tipos de reglas genéricas que realizan acciones contra eventos que cumplen los criterios de selección especificados en un selecto de eventos asociados (BMC et al., 2016). Una política de gestión de eventos selecciona los eventos que desea procesar, define los procesos necesarios para administrar esos eventos y programarlos para cuando se procesen los eventos.

- Colectores de eventos: filtros que consultan el repositorio de eventos y muestran los resultados en una lista de eventos de las celdas remotas de una manera organizada (BMC et al., 2016).

- Acciones ejecutables: programas o scripts ejecutables que realizan una tarea automatizada en un evento particular.

3.5.6. Base de Datos

ProactiveNet suporta las siguientes bases de datos para la recopilación de información:

- Sybase ASA: es la base de datos establecida por defecto, proporcionada como complemento en la instalación del servidor ProactiveNet. No es necesario una configuración adicional (BMC et al., 2016).
- Oracle: una base de datos muy conocida y confiable, que puede ser usada en remplazo de la predeterminada. Se debe definir una instancia de base de datos dedicada para ProactiveNet (BMC et al., 2016).

Las bases de datos actúan como repositorio central para toda la configuración del monitor y los datos estadísticos en el servidor ProactiveNet, como también las siguientes funciones (BMC et al., 2016):

- Información de configuraciones, como usuarios, dispositivos, agentes Patrol y soluciones de monitor.
- Reportes/informes realizados a partir de la recopilación de alarmas.
- Datos de rendimiento como status de fylesystems, procesos, picos de CPUs, memoria Ram, etc.
- Información analizada y procesada como datos de índice y de referencia.

3.5.7 Consola de Administración

La consola de administración permite modificar el servidor ProactiveNet, los servidores de celdas remota y las áreas de administración de la red de servicios de integración mediante la adición o eliminación de usuarios, grupos, dispositivos monitoreados, aplicaciones y servicios, o el

cambio de notificaciones de eventos y umbrales. También puede administrar los componentes de infraestructura y modelos de servicios soportados. La consola de administración proporciona acceso a las directivas de administración de eventos, al editor de tablas dinámicas y al editor de servicios (BMC et al., 2016).

Es posible el uso de la consola de operación en equipos remotos. Lo que facilita la administración de la herramienta desde cualquier sitio.

La consola de operación consta de dos pestañas principales:

Administration: Se utiliza esta pestaña para la administración general de las cuentas de usuarios y otras tareas de administración de la herramienta, trabajando con las directivas de administración de eventos, trabajando con tablas dinámicos utilizando el editor de datos y la administración de la infraestructura de la herramienta, como los servicios de integración y las celdas (BMC et al., 2016).

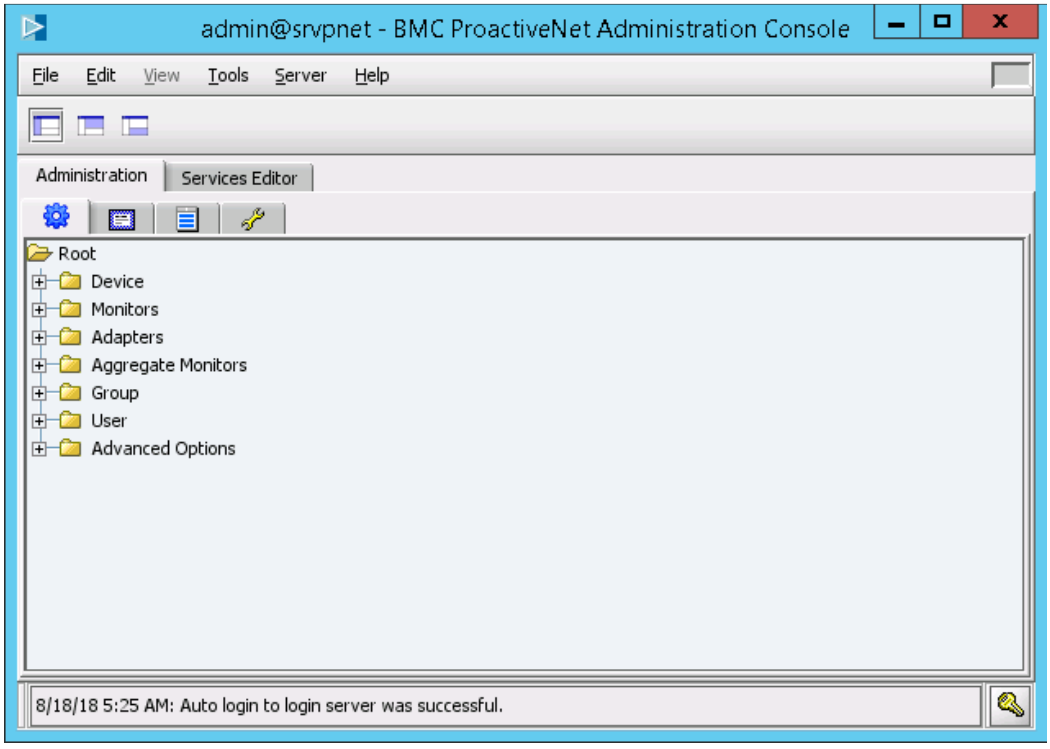


Figura 3. 6: Pestaña Administration
Fuente: Elaborado por el autor.

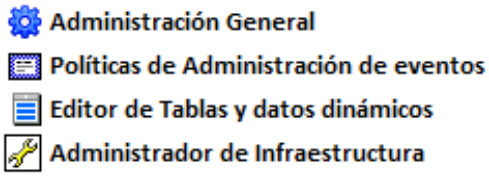


Figura 3. 7: Pestañas de Administración
Fuente: Elaborado por el autor.

Services Editor: es la vista que utilizan los administradores de servicios, supervisores de servicios y personal de operaciones de TI para ver los modelos de servicios. Los administradores de servicios pueden ver los modelos de servicios que representan los servicios empresariales de una empresa de telecomunicaciones. Son creados organizando componentes de modelo de servicio en relaciones jerárquicas que los operadores y administradores de servicios puede navegar (BMC et al., 2016).

Desde esta pestaña un administrador u operador puede identificar si un componente del modelo de servicio consume los servicios de otro componente del modelo de servicio (consumidor) o si proporciona servicio a otro componente (proveedor).

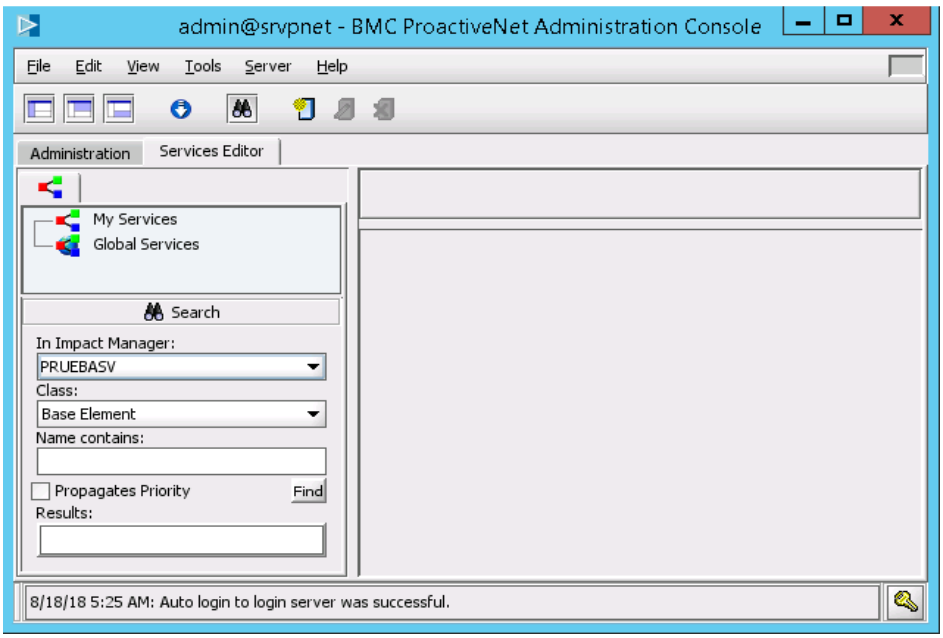


Figura 3. 8: Pestaña Editor de Servicios
Fuente: Elaborado por el autor.

3.5.8. Consola de operación

Es una aplicación basada en servicios web que proporciona opciones para navegar y ver toda la información recopilada y calculada por el servidor ProactiveNet relacionando eventos, rendimiento, servicios y aplicaciones. Las operaciones del día a día de ProativeNet se realizan mediante la consola de operación (BMC et al., 2016).

En la siguiente figura se puede observar la consola de operación, que es la consola que utiliza el usuario final para el monitoreo de sus redes. Está constituida por tres paneles:

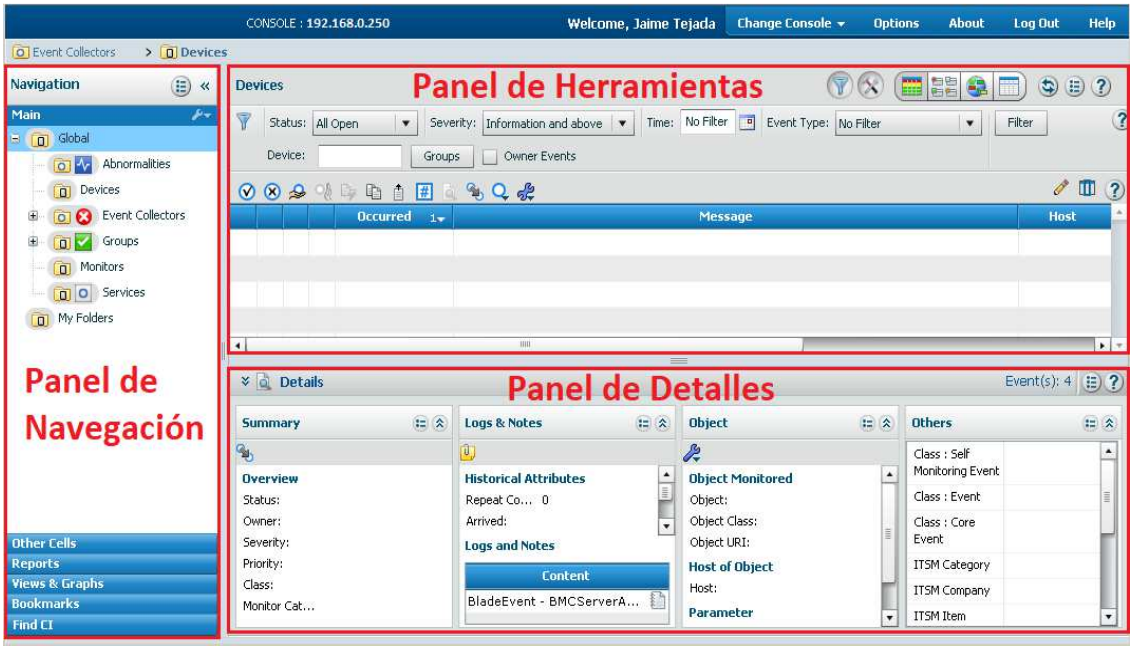


Figura 3. 9: Consola de operación vista modo eventos
Fuente: Elaborada por el autor.

3.5.8.1. Panel de navegación

En este panel se puede seleccionar y acceder a la información respectiva de cada celda remota o colector, que contienen los sistemas o grupos de equipos integrados. Para su visualización se requiere de habilitar las celdas a monitorear. (BMC et al., 2016).

Tabla 3. 4: Elementos del árbol de navegación

Elemento de navegación	Descripción
Main	Proporciona acceso a listas de eventos y muestra información de eventos y estado en base a la infraestructura de ProactiveNet.
Other cells	Enumera las celdas remotas disponibles conectadas al servidor ProactiveNet y monitoreadas por ProactiveNet.
Reports	Permite generar y administrar informes basados en datos recopilados por ProactiveNet.
Views and Graphs	Administra vistas y gráficas en la consola de operación.
Bookmarks	Permite ver, cambiar el nombre y eliminar marcadores de objetos o elementos y sus vistas relacionadas que se crean en el árbol de navegación. Las modificaciones que se realicen solo son visibles para el usuario.
Find CI	Proporciona un mecanismo de búsqueda para que pueda encontrar CIs (Items de configuración) que cumplan con los criterios de búsqueda especificados.

Fuente: (BMC et al., 2016)

3.5.8.2. Bloque Main

En esta pestaña se visualiza el auto-monitoreo de la herramienta y de su infraestructura. Constituida por dos nodos denominadas Global y My folders.

Global: Al crear carpetas bajo este nodo, todos los usuarios de ProactiveNet podrán visualizarlas y acceder a ellas. Por default vienen las siguientes carpetas creadas:

- Abnormalities: Muestra todos los eventos de anormalidad. Son alarmas informativas sobre cambios repentinos en cuanto al rendimiento de SO, CPU y memoria de los equipos. Como también el alcance de umbrales establecidos.

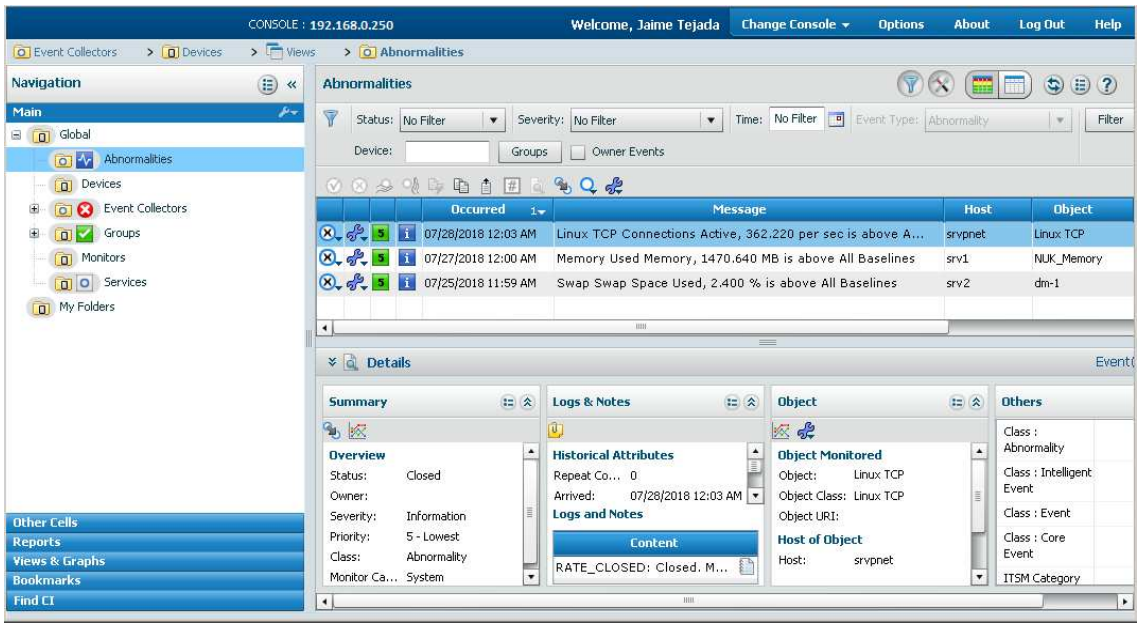


Figura 3. 10: Eventos con anormalidad de los componentes que conforman la arquitectura ProactiveNet
Fuente: Elaborado por el autor.

- Devices: Muestra todos los dispositivos y servidores integrados. Basándose en permisos, los usuarios pueden crear carpetas de eventos y componentes bajo este nodo para organizar la vista de eventos.

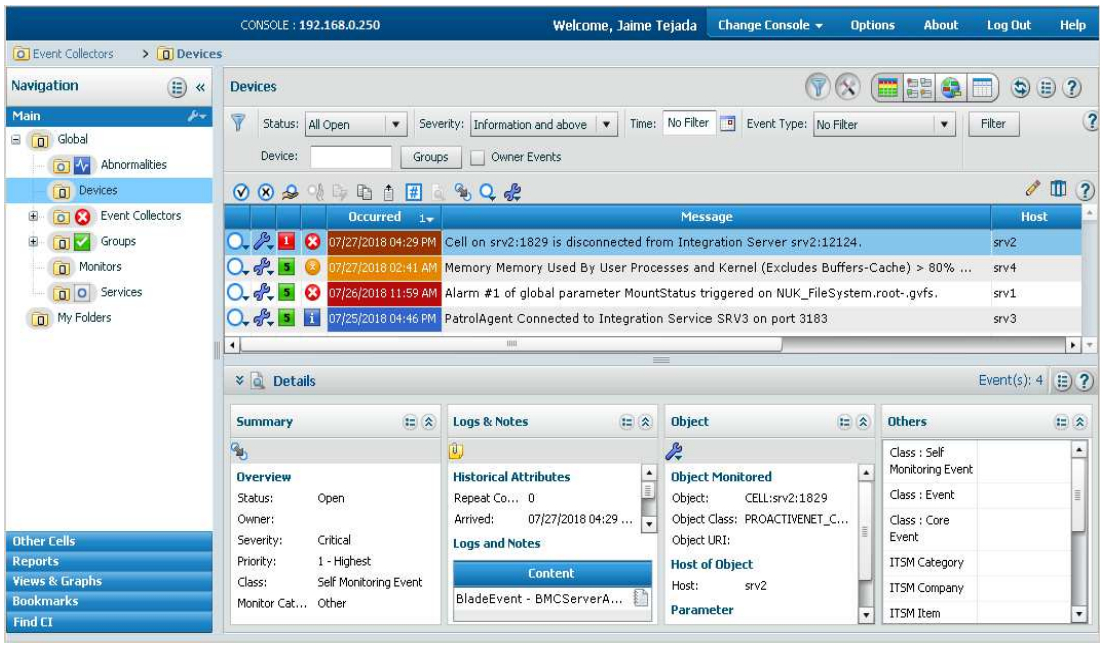


Figura 3. 11: Alarmas de dispositivos integrados en modo de vista de eventos
Fuente: Elaborado por el autor.

Como podemos visualizar en la figura 17 se encuentran activas 4 alarmas distintas respecto a los servidores de celdas remotas, que son parte de la infraestructura de la herramienta. Dentro de estos servidores se encuentra el almacenamiento de cada una de las celdas remotas a la que se les asignan y se integra un gestor o varios equipos en particular (Autor, 2018). Estas alarmas muestran el rendimiento de estos servidores a nivel de Sistema operativo, Filesystems (particiones de disco), CPU, memoria RAM y SWAP, status de: agentes, componentes y celdas implementadas. En pocas palabras se monitorea todo el funcionamiento de cada uno de ellos (BMC et al., 2016).

Figura 3. 12: Dispositivos que conforman la arquitectura ProactiveNet en modo de vista Grid
Fuente: Elaborado por el autor.

Tabla 3. 5: Opciones de la pestaña Main en Panel de navegación

Opción	**Definición**
Event Collectors	Muestra toda la jerarquía de recopiladores de eventos.
Groups	Muestra todos los grupos.
Monitors	Muestra una lista de eventos para monitores creados en los dispositivos monitoreados por ProactiveNet.
Services	Muestra todos los servicios monitoreados.

My Folders	Cuando se crean carpetas bajo este nodo, solo el usuario que las creo podrá visualizarlas y acceder a las mismas.

Fuente: (BMC et al., 2016)

3.5.8.3. Bloque Other Cells

En este bloque vamos a visualizar todas las celdas remotas que representan cada uno de los Sistemas Gestores o grupo de equipos que han sido integrados. De acuerdo al rol y el grupo que se le asigne a un usuario, podrá realizar modificaciones en cuanto a las celdas que se deseen visualizar y poder ocultar aquellas que no sean necesarias en el momento (Autor, 2018). Tal y como se muestra a continuación:

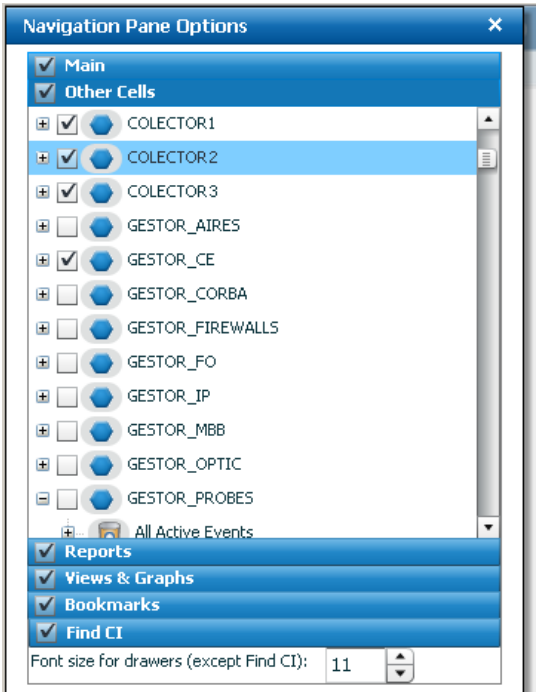


Figura 3. 13: Modificaciones en la visualización de celdas remotas
Fuente: Elaborado por el autor.

3.5.8.4. Panel de Herramientas

En este panel se muestran todas las incidencias respecto a lo seleccionado en el panel de navegación. Este panel da la comodidad de realizar filtrados de acuerdo a la manera de visualización que se requiera, por

ejemplo: en relación a su prioridad, severidad, impacto, etc. También se puede tener control sobre todas las incidencias, permitiendo el cambio de estado (Abierto, Reconocido, Asignado y Cerrado). Se puede realizar búsquedas de incidencias en base a fechas, elementos, componentes, host, etc. (BMC et al., 2016).

3.5.8.5. Modos de visualización de la información

La siguiente tabla describe las vistas proporcionadas por la consola de operación. Existe diferentes vistas disponibles, dependiendo del objeto seleccionado en el panel de navegación. Se accede a cada vista en el botón asociado de la barra de herramientas de la consola de operación (BMC et al., 2016). Si una vista no está disponible para el objeto seleccionado, simplemente el botón no se mostrará en la barra de herramientas.

Tabla 3. 6: Modos de visualización de la información

Vista de eventos	Muestra todos los eventos en forma detallada en una lista. Predeterminada por default para todos los objetos. Una de sus utilidades es permitir comprobar los detalles de las incidencias y tratar aquellos que no se están formando correctamente. También puede hacer frente a la condición incorrecta de una incidencia, invocando acciones remotas y acciones locales. Esta vista ayuda a comprobar el servicio de impacto. Disponible para los siguientes objetos: Colectores de eventos, Anormalidades, Servicios, Grupos, Dispositivos, monitores y celdas remotas en donde se integran sistemas de redes externas.	
Vista de Mosaico	Muestra una vista encapsulada de las métricas de eventos para los componentes que se están monitoreando para los componentes que se están monitoreando en su entorno. Se la utiliza para obtener un resumen del panel de actividades de eventos.	
Canvas	El modo de vista Canvas permite crear una representación gráfica de los componentes que se están monitoreando en su entorno. En donde los componentes están representados por objetos que son colocados en una imagen de fondo. Los objetos pueden ser gráficos, como imágenes o conectores, o información de métricas representadas en un mosaico.	

Vista de árbol/ gráfico	Muestra la información de un objeto seleccionado como un árbol que representa la jerarquía del objeto. Está disponible para grupos y servicios. Este modo de vista se puede utilizar para obtener una visualización interactiva en tiempo real del estado del evento y otros detalles del grupo/servicio seleccionado.	
Grid	Muestra información para el objeto seleccionado en formato tabular. Esta vista cuadrícula se puede utilizar para ver el estado del evento y otros detalles del objeto seleccionado, ya que la representación tabular de los objetos tendrá vínculos de desglose con detalles a través de gráficos, visitas y así sucesivamente.	

Fuente: (BMC et al., 2016).

3.5.8.6. Columnas de información de eventos

La información se muestra de acuerdo a los ajustes y a los campos que se elijan. Para la presentación de alarmas se tienen los siguientes campos de información:

Figura 3. 14: Campo de información de eventos
Fuente: Elaborado por el autor.

a) Status de los eventos

Proporciona información básica acerca de la actividad de repuesta del evento, muestra el estado actual del evento. Los estados de un evento pueden ser los siguientes:

Tabla 3. 7: Status de eventos

Status	**Definición**
Open	Cuando se presenta una incidencia, el equipo genera una alarma que se encuentra en estado abierto.

Assigned	Aquellas alarmas que ya fueron reconocidas y asignadas al personal correspondiente para su solución.
Acknowledge	Aquellas alarmas que ya fueron reconocidas por el personal de monitoreo.
Blackout	Este status se presenta cuando el dispositivo, componente, servidor, servicio o aplicación se encuentra apagado.
Closed	Se coloca el estado Cerrado a aquellas alarmas que el equipo envía como confirmación de que el incidente ha sido solucionado.

Fuente: Elaborado por el autor

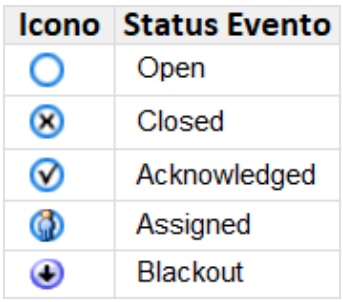


Figura 3. 15: Status de un evento
Fuente: (BMC et al., 2016)

En la siguiente figura se muestra cómo un evento de cualquier estado se ve afectado por las operaciones de los empleados que monitorean. Los círculos representan los estados del acontecimiento. Cada flecha representa una acción, con la dirección de la flecha que indica el flujo de la acción. Por ejemplo, se sufre una incidencia y se genera una alarma, el personal de monitoreo establecerá a quién asignarle dicha incidencia. La persona a la que se le asigna, debe tomar posesión o declinar la incidencia. Si toma posesión de ella, se le debe dar seguimiento hasta que la incidencia haya sido solucionada y se cerrará la alarma. En el caso de que no se tome posesión, la alarma se mantendrá abierta y se cerrará en caso de que la incidencia haya sido solucionada o por ser descartada por políticas de cerrados.

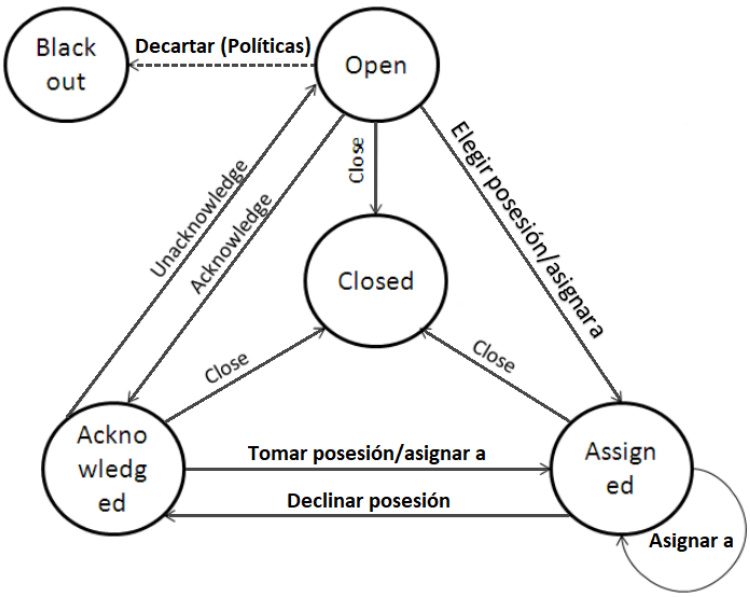


Figura 3. 16: Acciones a tomar frente a una incidencia
Fuente: Elaborado por el autor.

b) Herramientas

Permite realizar operaciones en un evento, ejecutar acciones remotas, realizar el análisis de la causa probable del incidente, recuperar el historial del dispositivo y exportar el evento (BMC et al., 2016).

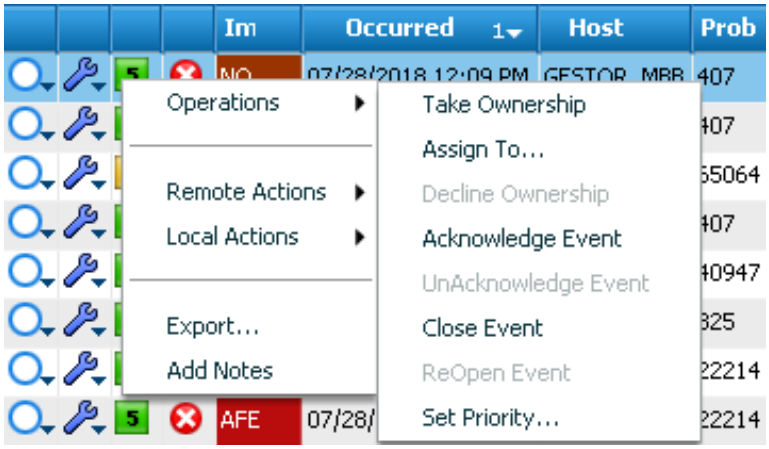


Figura 73. 17: Icono de herramientas para toma de acciones sobre los eventos
Fuente: Elaborado por el autor.

c) Prioridad del evento

Determina qué evento requiere de mayor acción de su resolución frente a los demás. Así se prioriza las incidencias (Autor, 2018).

Icono	Prioridad de evento
1	Prioridad 1 (Alta)
2	Prioridad 2
3	Prioridad 3
4	Prioridad 4
5	Prioridad 5 (Baja)

Figura 3. 18: Prioridad de un evento
Fuente: Elaborado por el autor.

d) Severidad del evento

Determina qué evento requiere de mayor acción de su resolución frente a los demás. De acuerdo al filtrado de visualización, podemos darles seguimiento a aquellas alarmas con una severidad Critica consideradas esenciales para el funcionamiento de las redes móviles (Autor, 2018).

Color	Icono en la lista de eventos	Niveles de Severidad
Rojo		Critical
Naranja Oscura		Major
Naranja Claro		Minor
Amarillo		Warning
Azul		Information
Verde		Ok
Gris		Unknown
Gris Claro		No event

Figura 3. 19: Niveles de severidad de un evento
Fuente: Elaborado por el autor.

e) Impacto

Muestra el impacto de cada una de las incidencias, de acuerdo a la recomendación del proveedor. Tienen los siguientes niveles:

Tabla 3. 8: Niveles de Impacto

Impacto	Descripción
NO	Aquellas incidencias que no representan impacto ni afectación en los servicios.
P. AFE	Aquellas incidencias que tienen una probabilidad de impacto y de afectación en caso de que no se los solucione a tiempo.
AFE	Aquellas incidencias que representan afectación en los servicios y requieren de solución inmediata.

Fuente: Elaborado por el autor.

f) Ocurred

Muestra la fecha y hora cuando una alarma que presenta una incidencia ha sido generada como también el cambio de cada uno de los estados de la alarma: Abierta, Cerrada, Acknowledge y Assigned (BMC et al., 2016).

g) Host

Muestra el host name de la incidencia, que en otras palabras es el gestor que administra los equipos que emiten las alarmas. De este modo en la vista general se todos los eventos es posible distinguir el origen de cada una de las incidencias que se presentan.

h) Probable Cause

Muestra el ID Alarm, que es un número único que identifica cada incidencia, para cada gestor se le establece un catálogo de alarmas que lo proporciona el proveedor. Con el fin de conocer las diversas alarmas que se pueden generar de acuerdo a la incidencia sufrida.

i) Alarm Text

Muestra el texto de la alarma, especifica mayor información de la incidencia. De esta manera durante una afectación del servicio, se puede conocer cuál ha sido la falla y cómo solucionarlo.

j) Elemento

Muestra el elemento o nodo del cuál haya sufrido una incidencia (Nombre de equipo y sector de su ubicación).

k) Component Affected

Muestra el componente específico el cual originó la incidencia.

l) Info Additional

Describe con mayor detalle la incidencia y muestra información sobre la ubicación del componente afectado.

3.5.8.3. Panel de detalles

El panel de detalles es muy usado para identificar información que no se visualiza en los diversos modos de visualización de los eventos. Muestra la cantidad total de los eventos que se encuentran en la celda o colector seleccionado. Es muy usada para realizar un análisis de posibles causas raíz (BMC et al., 2016).

En él se encuentra información completa respecto a cada incidencia. Constituido por 4 pestañas: Summary que muestra un resumen en cuanto a la incidencia, Logs & Notes indica los registros de cada cambio de status o modificación que haya sufrido un evento, Object muestra información en base al objeto específico que ha sufrido una afectación como su host, dirección IP, parámetros, etc (Autor, 2018).

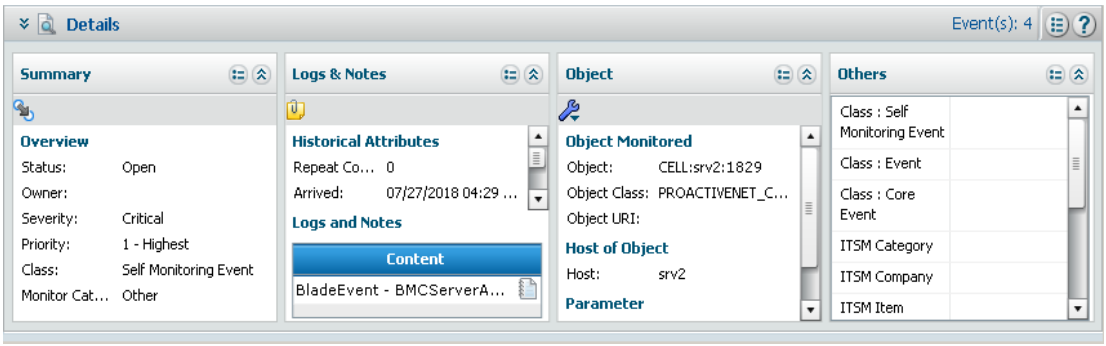


Figura 3. 20: Panel de detalles
Fuente: Elaborado por el autor.

3.6. Alcance en su implementación

- Identificar que existe un problema (o problema inminente) con una aplicación o servicio antes de que un cliente informe el problema (BMC et al., 2016). Esto incluye servicios ofrecidos en entornos Cloud.
- Solucionar en tiempo real las incidencias, mediante la identificación precisa y rápida de los componentes de red problemáticos que afectan al servicio.
- Identificar la causa probable de la interrupción de la aplicación o del servicio existente o inminente.
- Reducir los costos asociados con el reemplazo innecesario de componentes en un entorno Cloud (BMC, 2018).
- Asegurar la disponibilidad del servicio en ambientes Cloud y físicos previniendo interrupciones.
- Filtrar eventos masivos y aumenta sólo la información más relevante, enriquecida con el análisis de rendimiento y diagnósticos detallados.
- Reducir el costo de la supervisión de la infraestructura de telecomunicaciones mediante la automatización de ajustes de umbrales y mantenimiento (BMC et al., 2016).

- Reducir los recursos desperdiciados en la solución de problemas de degradación del rendimiento resultándote de cambios de infraestructura no autorizados.
- Tener en cuenta el impacto de aquellos componentes de red que son claves para la infraestructura de telecomunicaciones, los servicios críticos y priorizar los esfuerzos en consecuencia.
- Priorizar un incidente automáticamente basado en el impacto al servicio.
- Crear automáticamente un incidente enriquecido con la solución del problema y la información relevante para el NOC.
- Medir y reportar niveles de servicio.

Al unificar el monitoreo y la administración de entornos físicos, virtuales y Cloud en una única plataforma de operaciones proactivas, da soluciones como:

- Proporciona una visión consolidada de los datos del rendimiento e impacto de múltiples soluciones de monitoreo y sistemas Silos (Aquellos sistemas de gestión que no funciona con cualquier otro sistema)
- Prioriza eventos basados en el análisis de impacto de servicios predictivos.
- Ofrece alertas tempranas de problemas inminentes, al tiempo que elimina la dependencia de los umbrales reactivos.
- Indica automáticamente la causa raíz proactiva en la infraestructura, los usuarios, las aplicaciones y los servicios; como también cambios en la configuración (BMC et al., 2016).

- Mapea, monitorea y les da seguimiento a relaciones de afectaciones y el comportamiento a través de entornos físicos, virtuales y Cloud.
- Captura continuamente los diagnósticos de aplicaciones críticas para su inclusión en el análisis proactivo de la causa raíz (BMC et al., 2016).

De acuerdo a la infraestructura que se visualiza en la siguiente figura, para cada uno de los gestores de distintas marcas de proveedores corresponden a una celda específica. Estas celdas son creadas y almacenadas dentro del servidor celda (srv1, srv2, srv3, srv4), el número de celdas que se puede integrar en cada servidor dependerá de la carga de información que envíe cada gestor (Autor, 2018).

En el primer servidor srv1, posee 5 celdas correspondientes a distintos gestores pero que se relacionan entré sí debido a que sus elementos de red proveen servicios de voz y datos en redes móviles. Por ese motivo todas son consolidadas dentro de un Colector, que dispondrá toda la información en cuanto a incidencias y rendimientos de todos los equipos pertenecientes a todos los gestores integrados (Autor, 2018).

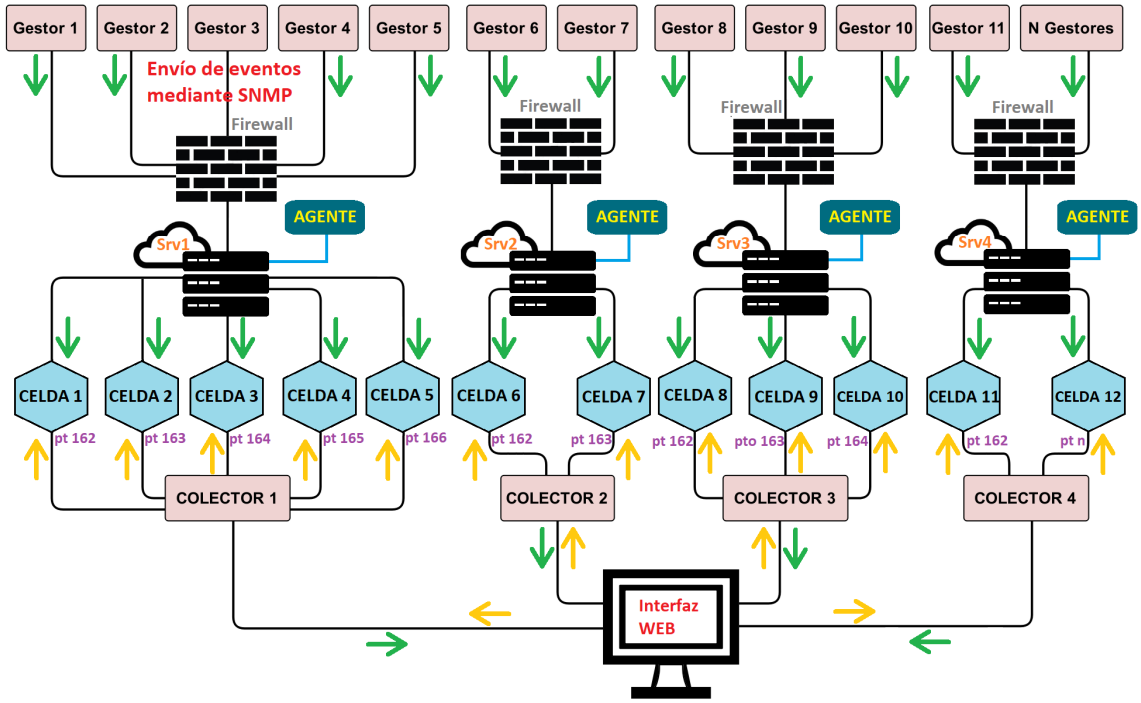


Figura 4. 1: Diagrama de comunicación entre gestores implementados en ProactiveNet
Fuente: Elaborada por el autor.

Si determinados equipos no están siendo administrados mediante alguna herramienta, ProactiveNet admite que sean integrados en una celda remota, la cual permitirá organizar una estructura que facilite la monitorización de todo dispositivo que disponga de un cable de red y una tarjeta SNMP (Autor, 2018).

4.1. Integración con un Sistema Gestor de Red 4.5G

Un sistema gestor tiene la propiedad de controlar el sistema de red y sus recursos mediante el control de su uso, el acceso a la monitorización y notificación de su estado actual e histórico. Con su uso se puede realizar pronósticos, toma de decisiones, análisis de datos y procurar mantener la calidad del servicio (Huawei, 2014).

El gestor a integrar tiene como nombre genérico Gestor_OPTIC que hace mención a un sistema de administradores de elementos de redes móviles. Específicamente para elementos de la generación 4.5G el cual provee operación centralizada y mantenimiento para la solución de cualquier afectación al servicio en cuanto a Multiplexación de ancho de banda (WDM), redes de transporte óptico, microondas, routers, switches, redes de transporte de paquetes, nodos de acceso multiservicio, equipos IP, etc. (Autor, 2018).

Este sistema gestor posee una interfaz externa para la operabilidad con otros sistemas mediante el uso de varios protocolos como SNMP, Corba (Huawei, 2014). Motivo por el cuál fue elegido para integrarse a la infraestructura de ProactiveNet.

4.2. Requerimientos

Antes de realizar la creación de una celda remota y de la integración del gestor en la misma se deben exigir los siguientes repertorios:

a) MIBs: Es la llave que permite la comunicación entre el gestor y la celda remota.
b) Manual de las arquitecturas de los OIDs.
c) Catálogo de alarmas.
d) La IP o varias IPs para la recepción de alarmas.
e) Solicitar la creación de permisos en el Firewall dependiendo la ubicación de los servidores físicos y en caso de que se encuentra en la Cloud no es necesario.
f) Solicitar que se configure el enrutamiento, en el caso de grandes arquitecturas de redes se debe establecer rutas que no hayan estado definidas para permitir la comunicación entre el gestor y ProactiveNet.

4.3. Pasos para la creación de celdas remotas en Servidor de celdas

Se crea la celda en la termina o consola dependiendo del sistema operativo. Con el siguiente comando:

“mcrtcell -n NombredeCelda -@ servidordeCeldaremota/PuertoInterno”

En donde se establece el nombre de la celda, el servidor de celda remota y el puerto de comunicación interna con el servidor ProactiveNet (Interfaz Web).

Para realizar un análisis profundo ante la caída de las celdas, es necesario activar los logs, que no son más que registros de eventos o acciones que afectan a un proceso en particular. Se lo activa con el siguiente comando:

“mcell -n NombredeCelda”

Registrar información de la celda en archivo mcell.dir ubicado en el siguiente directorio, en donde se establecen datos esenciales para la comunicación con el servidor ProactiveNet.

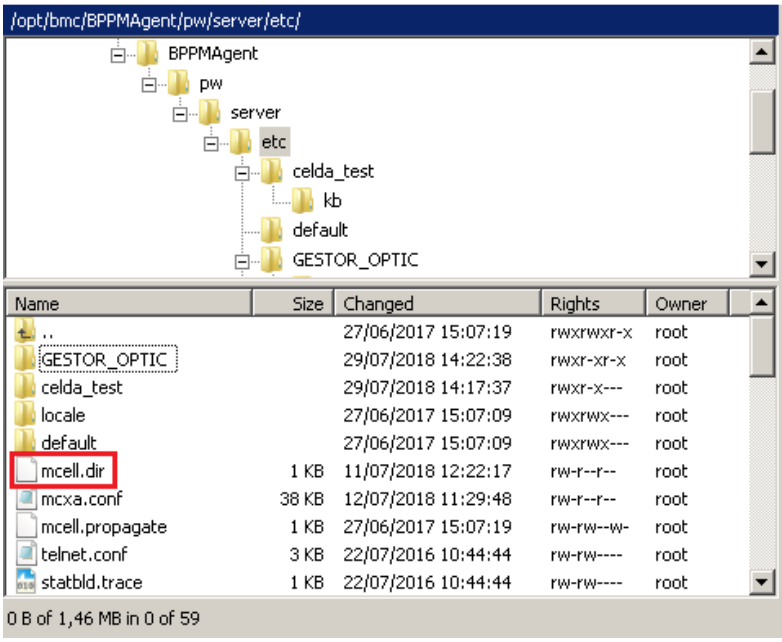


Figura 4 .2: Directorio para el registro de información sobre celdas remotas creadas en el servidor de celdas
Fuente: Elaborado por el autor.

El registro se lo realiza de la siguiente manera:

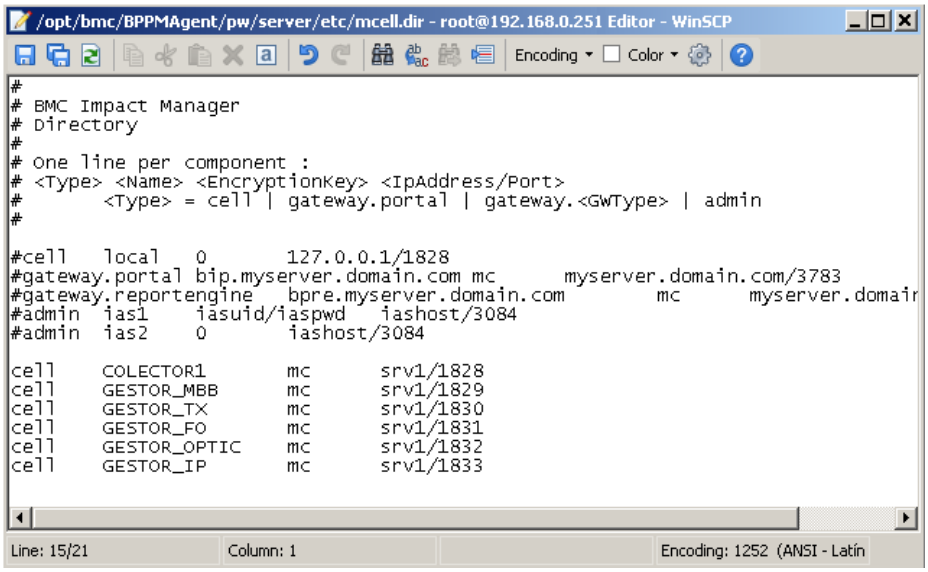


Figura 4. 3: Registro de celdas remotas creadas
Fuente: Elaborado por el autor.

Luego se debe registrar la celda remota en el servidor ProactiveNet para su visualización en la consola de operación. Se la registra con el siguiente comando:

“ladmin -ac

name=x:key=x:primaryHost=x:primaryPort=x:secondaryHost=x:secondaryPort=x:environment=x:usergroups=x”

En donde en la variable name se coloca el nombre de la celda, en primaryHost el nombre del host del servidor principal, en primaryPort se establece el puerto para la comunicación interna con el servidor principal, secondaryHost y secondaryPort se establecen para tener un sistema redundante, en environment se establece el ambiente (desarrollo o producción) y en usergroups se identifican los grupos de usuarios que serán capaces de visualizar la celda (Autor, 2018).

Es necesario registrar también la información de la celda remota creada en archivo mcell.dir del directorio ***/*etc** del servidor principal ProactiveNet donde se establecen datos esenciales para la comunicación interna entre celda remota y servidor ProactiveNet.

Luego se debe reiniciar la celda remota desde el servidor de celda remota y el servidor ProactiveNet con el siguiente comando:

“mcontrol -n NombredeCelda restart”

Para que el usuario pueda visualizar la nueva celda remota, se la debe habilitar en la consola de administración y en la consola de operación.

En la consola de administración se debe agregar la celda remota en la pestaña Impact Manager, a su servidor correspondiente, esto permitirá el uso de

consola de administración para la creación de tablas dinámicas como complemento para la interpretación de eventos.

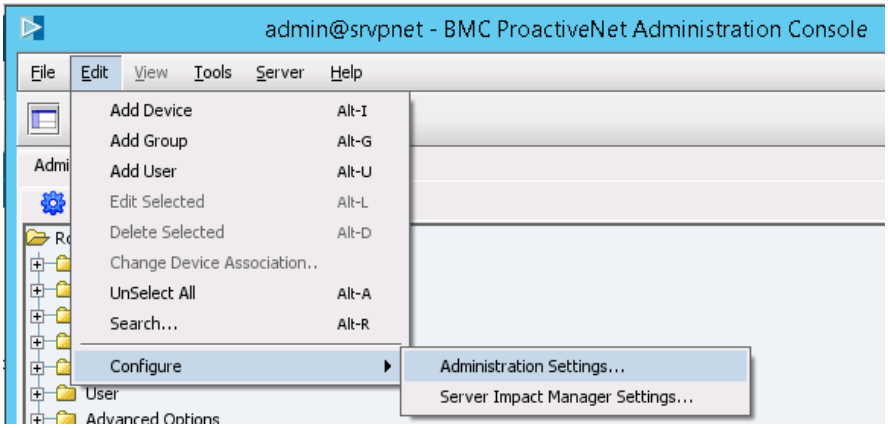


Figura 4. 4: Impact Manager en Consola de Administración
Fuente: Elaborado por el autor.

La celda remota es seleccionada dentro del servidor de celda que le corresponde. En este caso es el srv1.

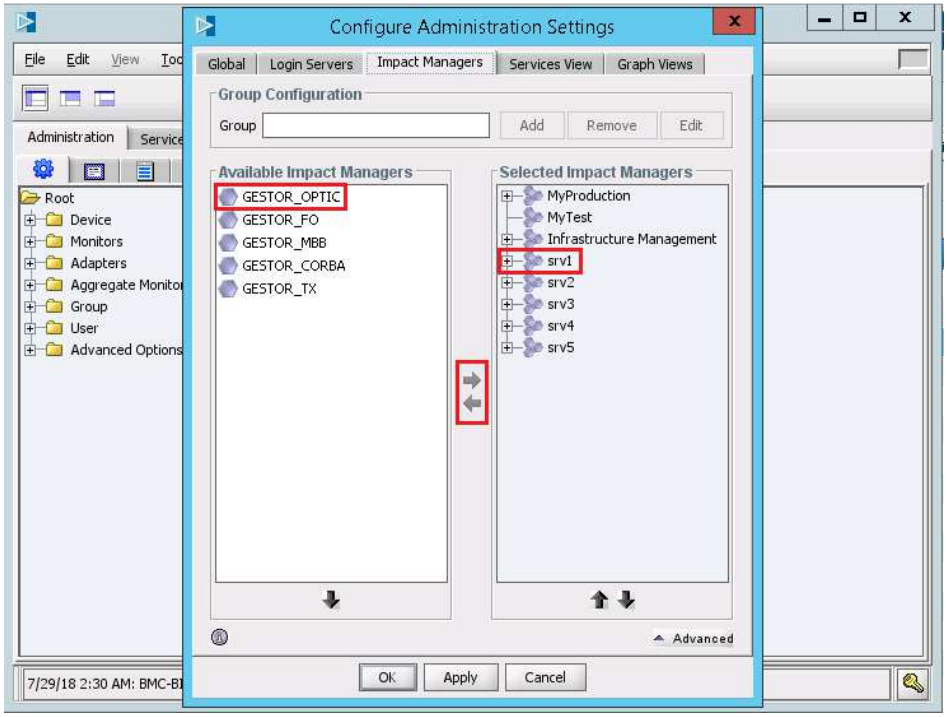


Figura 4. 5: Habilitación de celdas remotas en Impact Manager
Fuente: Elaborado por el autor.

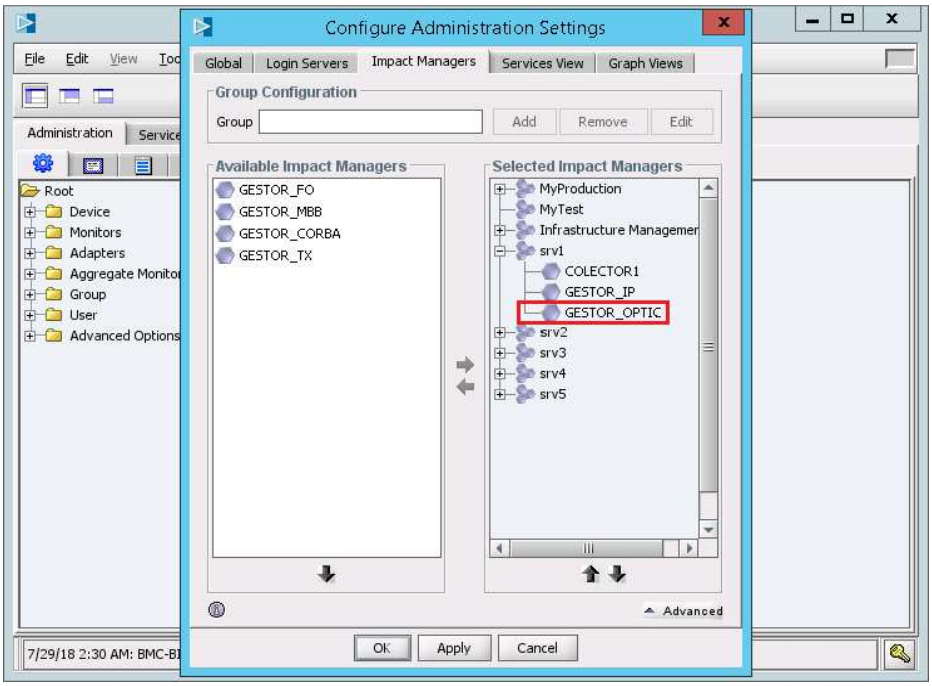


Figura 4. 6: Celda Gestor OPTIC habilitada para su visualización en la consola de operación

Fuente: Elaborado por el autor.

En la consola de operación se habilita la celda remota creada, para la visualización de incidencias respecto a la misma.

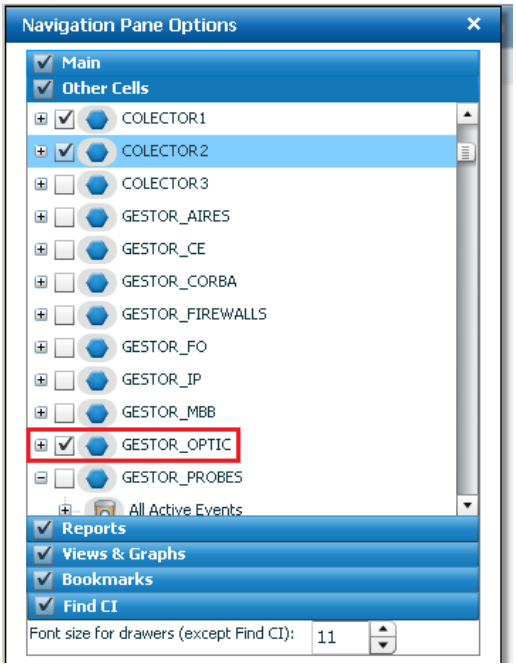


Figura 4. 7: Habilitación de celda remota en panel de navegación

Fuente: Elaborado por el autor.

Una vez habilitado, la celda estará activa, pero sin eventos ya que aún no se ha integrado el gestor.

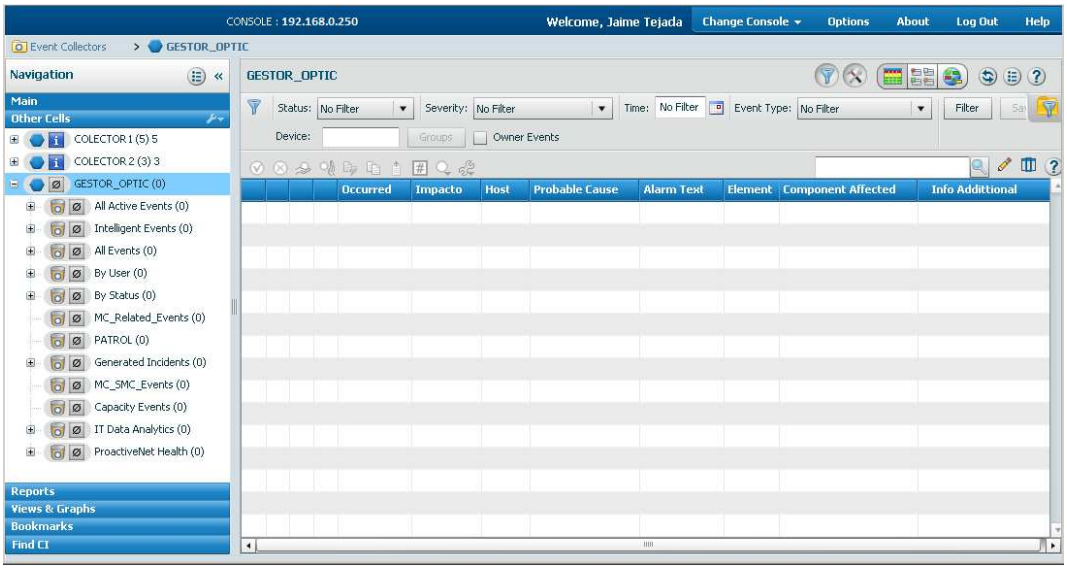


Figura 4. 8: Visualización de celda remota en consola de operación
Fuente: Elaborado por el autor.

4.4. Publicación y validación de MIBs

Cada proveedor debe proporcionar los MIBs (Base de información gestionada) de sus sistemas gestores y equipos, los cuales son compilados en la celda remota. En otras palabras, es la llave para permitir la integración del sistema en la celda remota. Sin esta, los eventos no llegarían de forma correcta al ProactiveNet y tampoco se visualizarían.En el peor de los casos, los MIBs pueden ser descargados de internet, asegurándose de que sean la versión correspondiente (Autor, 2018).

Los MIBs del proveedor deben ser compilados con los MIBs por default de ProactiveNet y se los coloca en el siguiente directorio del servidor de la celda remota.

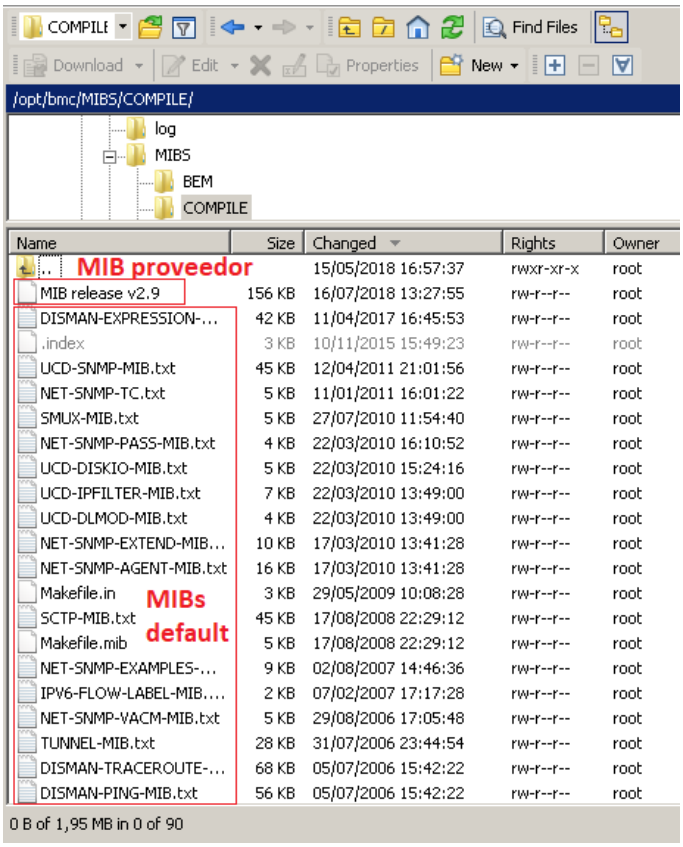


Figura 4. 9: MIBs necesarios para la publicación y validación en celda remota
Fuente: Elaborado por el autor.

El siguiente paso es la compilación utilizando una herramienta llamada mib2map.pl que se encarga de extraer la información y generar 4 archivos esenciales para el arribo de eventos a la celda remota.

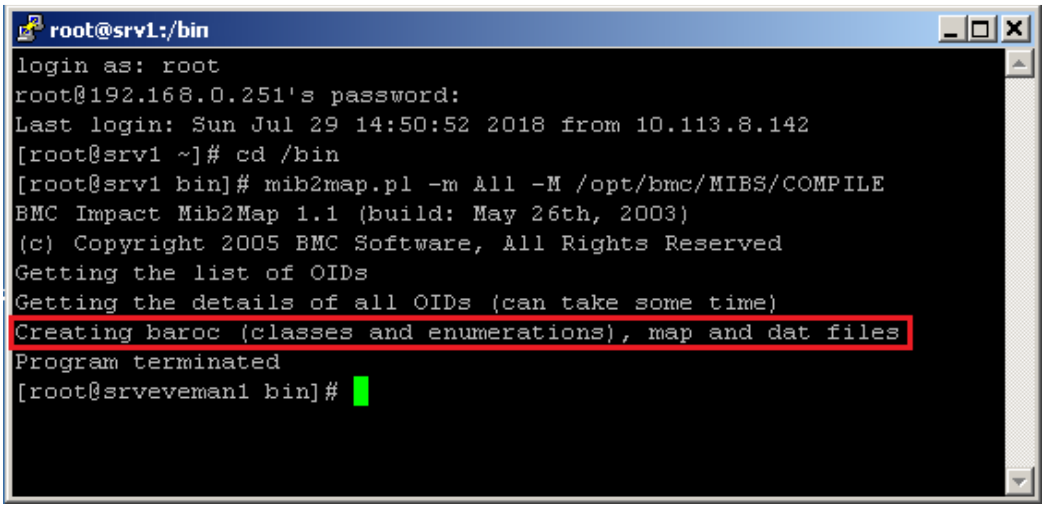


Figura 4. 10: Compilación de MIBs mediante Mib2Map
Fuente: Elaborado por el autor.

Se generaron los siguientes archivos en el directorio /bin.

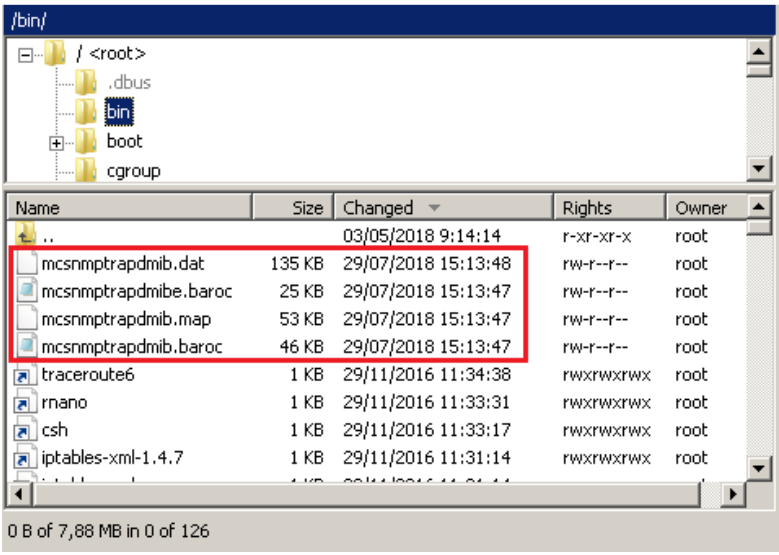


Figura 4. 11: Archivos generados producto de la publicación de MIBs
Fuente: Elaborado por el autor.

Aquellos archivos que tienen una extensión **.baroc** corresponden al directorio clases de la KB de la celda remota. Y sus nombres deben ser agregados en el archivo **.load** quien es el encargado de incluir dichos archivos cuando se compile la KB de la celda remota.

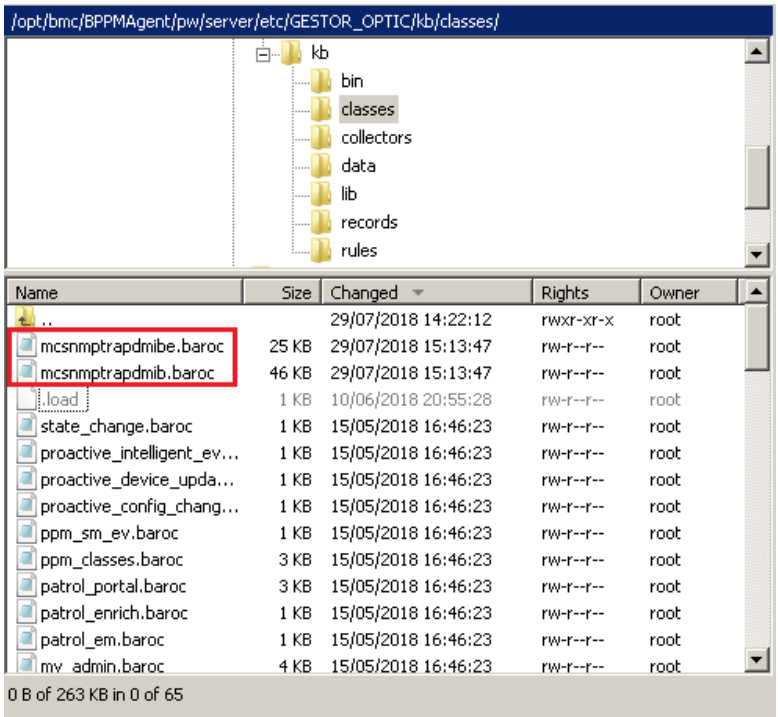


Figura 4. 12 - Directorio correspondiente para archivos con extensión baroc
Fuente: Elaborado por el autor.

Aquellos archivos que tiene una extensión .dat y .map son colocados en el siguiente directorio. Y deben ser establecidos para su uso en el adaptador SNMP que tiene como nombre mxca.conf y se encuentra en el mismo directorio /etc.

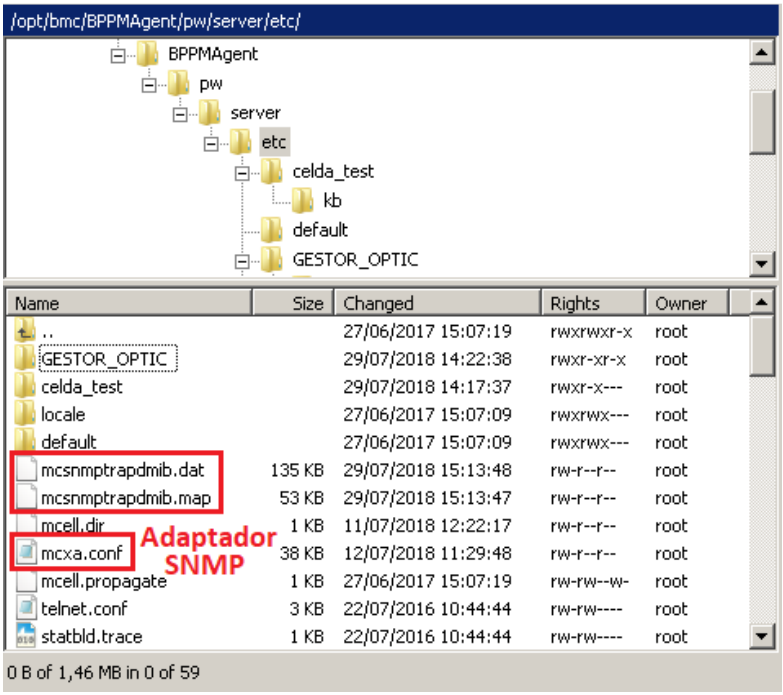


Figura 4. 13: Directorio correspondiente para archivos .dat y .map
Fuente: Elaborado por el autor.

El archivo mcxa.conf se lo configura de la siguiente manera:

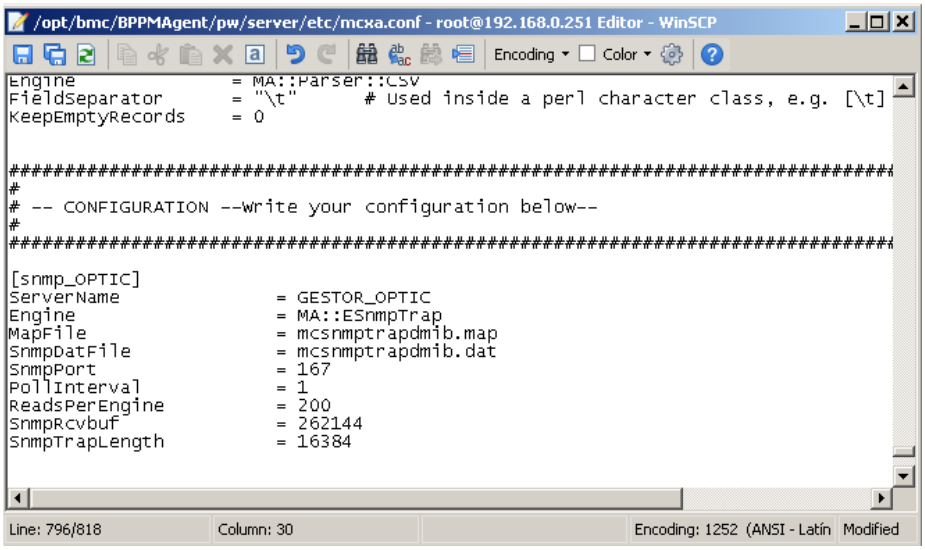


Figura 4. 14: Parámetros de adaptador SNMP
Fuente: Elaborado por el autor.

Los parámetros son predeterminados para todos los adaptadores específicos. Deben ser agregados y configurados de acuerdo a la celda remota que se integren (BMC et al., 2016). Para cada celda se le asigna un adaptador. En este caso se debe especificar el nombre de la celda remota, el módulo del motor que en este caso es MA::ESsnmpTRAP ya que permite la administración de capturas SNMP, se identifican los archivos .map y .dat generados en la compilación de los MIBs, el puerto SNMP por el cuál recibirá los eventos y los demás parámetros son por default establecidos para la mayor capacidad en la recepción de eventos (como el tamaño del buffer y tamaño de la trama de traps) (Autor, 2018).

4.5. Pruebas de comunicación

Una vez ya configurado el adaptador es necesario realizar pruebas de comunicación utilizando una herramienta llamada wireshark, que se encarga de hacer capturas del tráfico de datos enviados mediante los diversos protocolos de comunicación. Wireshark me permite descartar problemas del adaptador SNMP y problemas de red, en caso de que las vías de enrutamiento se no encuentren establecidas y/o permisos no habilitados de firewalls corporativos (solo aplica para servidores físicos), por lo que los eventos no se presentarían en la consola de operación.

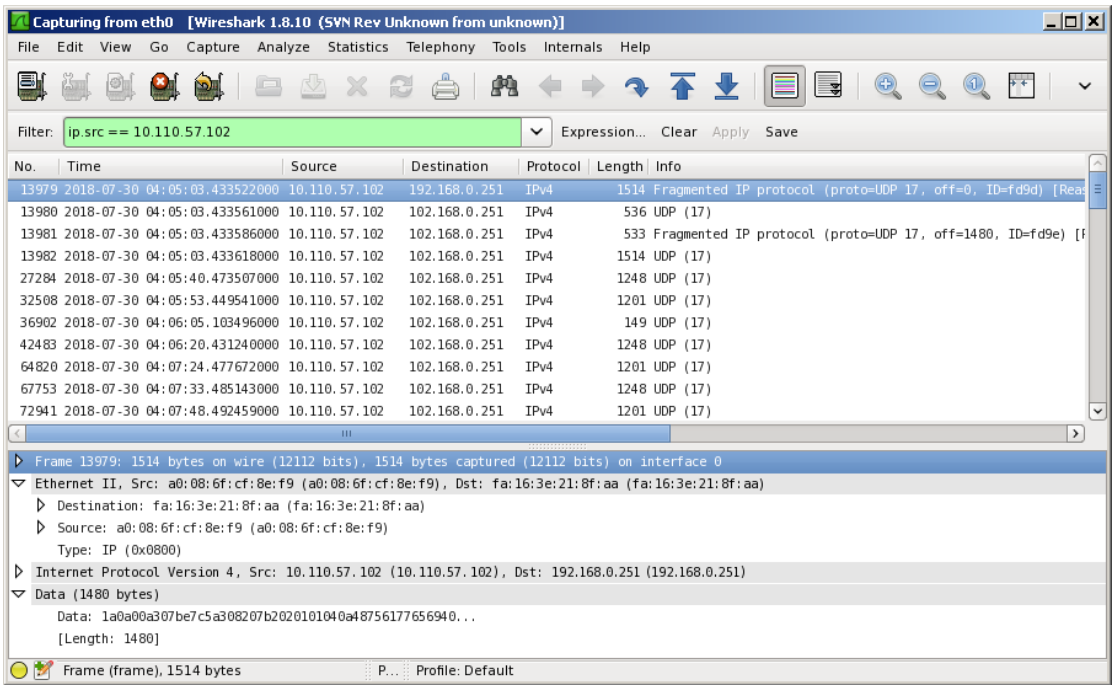


Figura 4 .15: Captura de tráfico entrante y saliente hacia los servidores de celdas mediante Wireshark
Fuente: Elaborado por el autor.

En la figura anterior, se puede apreciar que los eventos utilizan SNMP para la capa de aplicación, el protocolo UPD para la capa de transporte y toda la comunicación es sobre una red IPv4. Así como también la IP de la fuente y del destino que es el srv1 en donde se encuentra la celda remota.

Una vez ya confirmada la comunicación entre ProactiveNet y gestores. Se debe confirmar la visualización de los eventos en bruto en la consola de operación. Como se muestra en a figura a continuación, los campos determinados de los eventos que llegaron se encuentran vacíos y con una severidad OK.

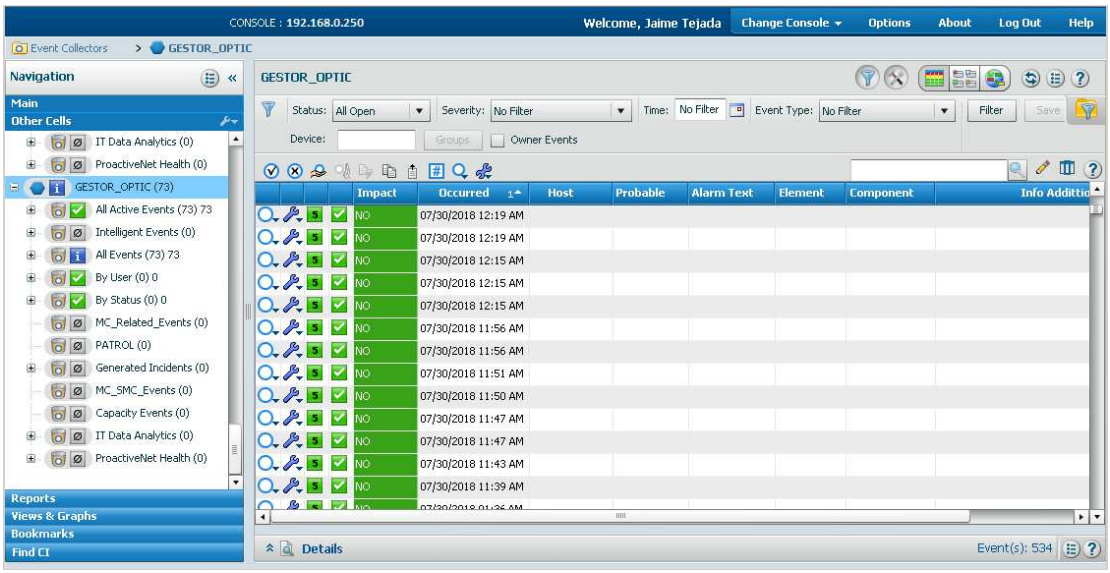


Figura 8 - Validación del arribo de eventos a la celda remota provenientes del Gestor OPTIC
Fuente: Elaborado por el autor.

Para poder analizar la estructura de los eventos que llegan, se debe establecer otros filtros de acuerdo a campos que se utilizan en comunicaciones SNMP, como Class, SNMP Enterprise, SNMP Comunity SNMP Values, SNMP OIDs. Una vez establecido un filtro o seleccionado los campos correctos se debe analizar la información para establecer los atributos a utilizar en las reglas de interpretación de eventos.

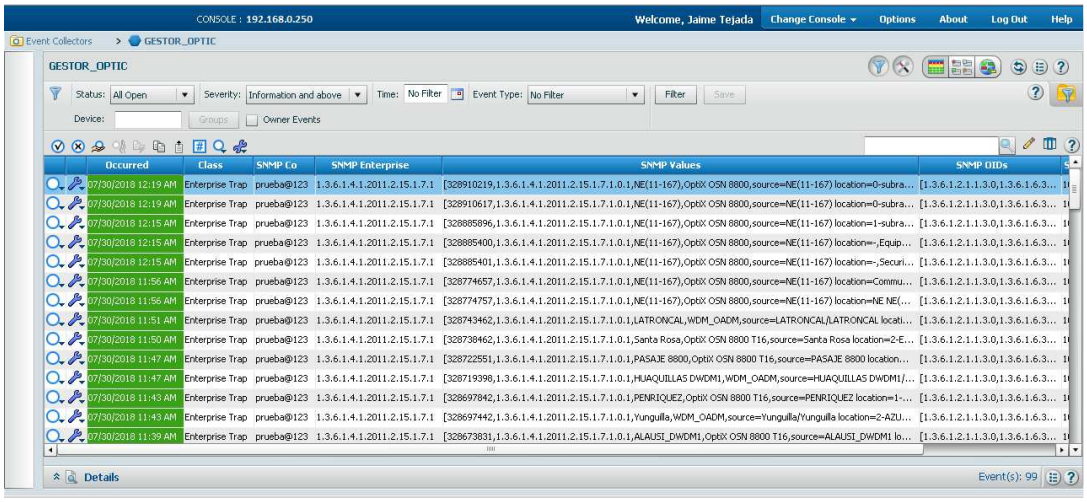


Figura 97: Información entrantes en campos de acuerdo a la clase SNMP Enterprise
Fuente: Elaborado por el autor.

Para realizar un mejor análisis, se extrae el evento y se lo edita en la herramienta Notepad++.

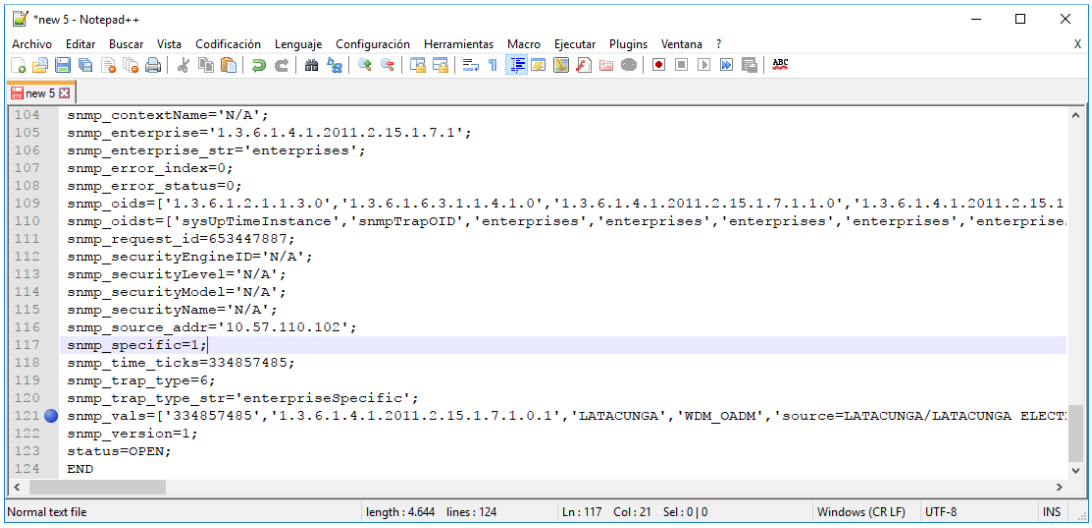


Figura 10. 18 - Atributos de la clase SNMP Enterprise
Fuente: Elaborado por el autor.

En la figura anterior, se visualizan varios atributos de 124 que tiene en total este trap. Se identifica que el atributo de la posición 121 contiene la información necesaria para la interpretación de incidencias.

El atributo snmp_vals contiene varias tramas también denominadas posiciones, cada una hace mención a información valiosa que envía cada equipo. A continuación, se detallan las posiciones a utilizar para el mapeo de información:

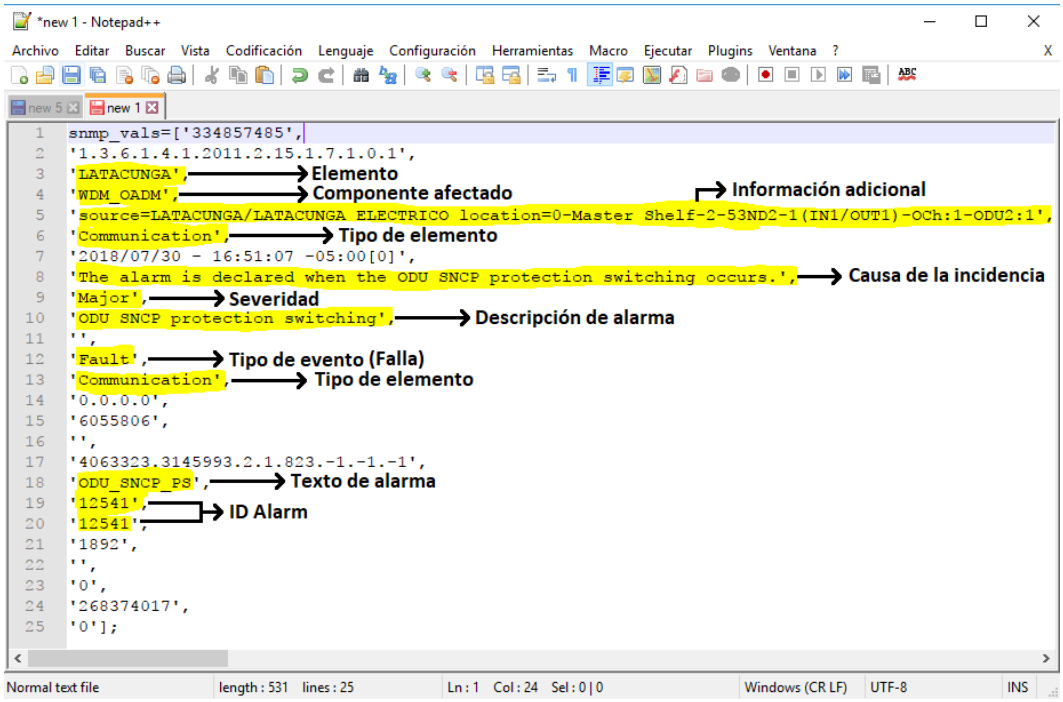


Figura 11: Estructura del atributo SNMP Vals de un evento que define una generación de alarma
Fuente: Elaborado por el autor.

En la figura 45 de acuerdo a la posición 12 del atributo snmp_vals, el trap que se analiza pertenece a una generación de alarma, ya que contiene “fault” que se traduce como “falla”. De la misma manera se debe realizar un análisis de un trap que represente el cerrado de la alarma. De esta manera se verifica si existen cambios en las posiciones de la trama y se identifica la variable que diferencie una generación de un cerrado de alarma.

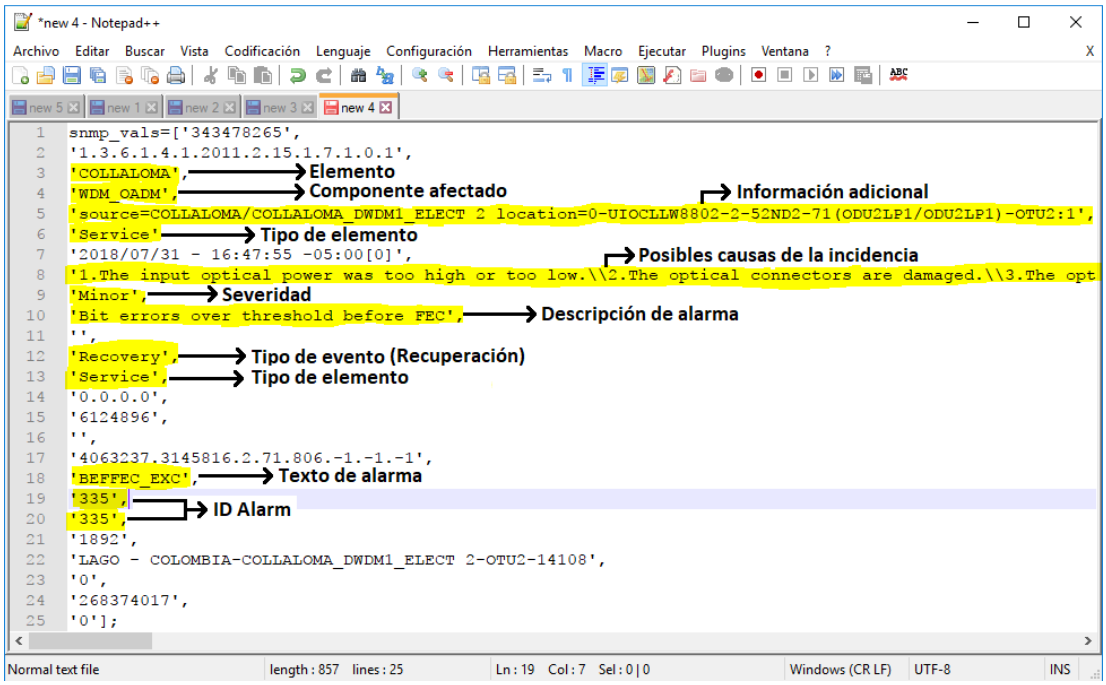


Figura 12: Estructura de Atributo SNMP Vals para un evento que define un cerrado
Fuente: Elaborado por el autor.

De acuerdo a la figura 46, este trap define un cerrado de los eventos ya que en la posición 12 del atributo snmp_vals contiene la palabra “Recovery” que hace mención a la recuperación del componente afectado. Una vez hecho el análisis se identifican los atributos a utilizar para la configuración de la KB.

4.6. Configuración de Base de Conocimiento (kb)

En el directorio Classes, vamos a identificar las clases de atributos a utilizar para la interpretación de las alarmas en la consola de operación. Se establecieron 2 clases: EVENT y CATALOGO.

En la clase EVENT se establecieron los atributos que van a contener la información que se extraen de los campos del atributo snmp_vals. De este modo la información se muestra de forma ordenada y entendible.

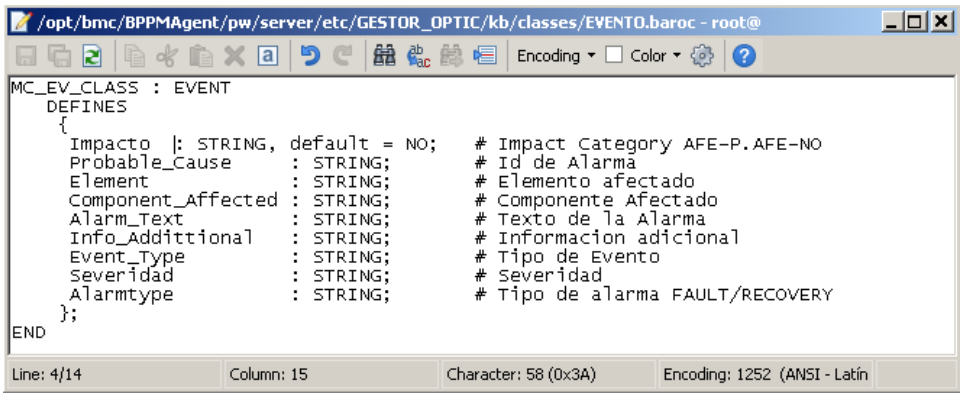


Figura 13: Atributos de la Clase EVENT
Fuente: Elaborado por el autor.

La siguiente clase será definida como tablas de datos dinámicos que representarán campos a llenar en la consola de administración. A la clase CATALOGO se le establecen atributos con campos que podrán ser editados por el administrador, estos servirán de complemento para la estructura de las alarmas. Lo que hace posible realizar configuraciones de acuerdo a las exigencias de visualización, severidad, prioridad, impacto, etc. sobrescribiendo lo que el sistema o equipo envía por default. También permite la comparación de información para prevenir campos nulos o incorrectos.

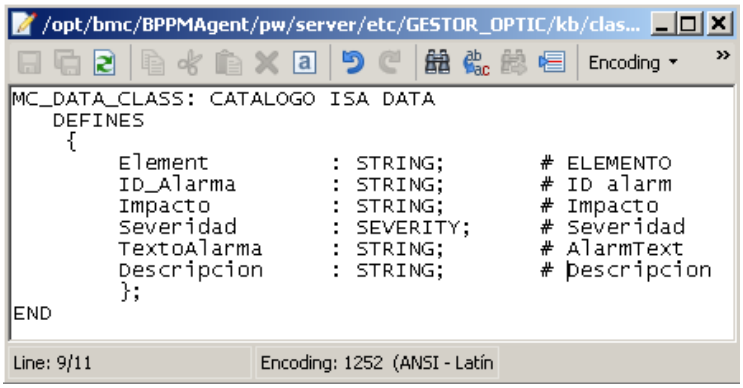


Figura 14: Atributos de la Clase CATALOGO
Fuente: Elaborado por el autor.

La siguiente figura muestra la tabla dinámica que se creó con la clase CATALOGO en el Editor de Datos Dinámicos, que contiene el catálogo de

alarmas que proporciona el proveedor. Puede ser cargado manualmente o importado mediante comandos internos de ProactiveNet.

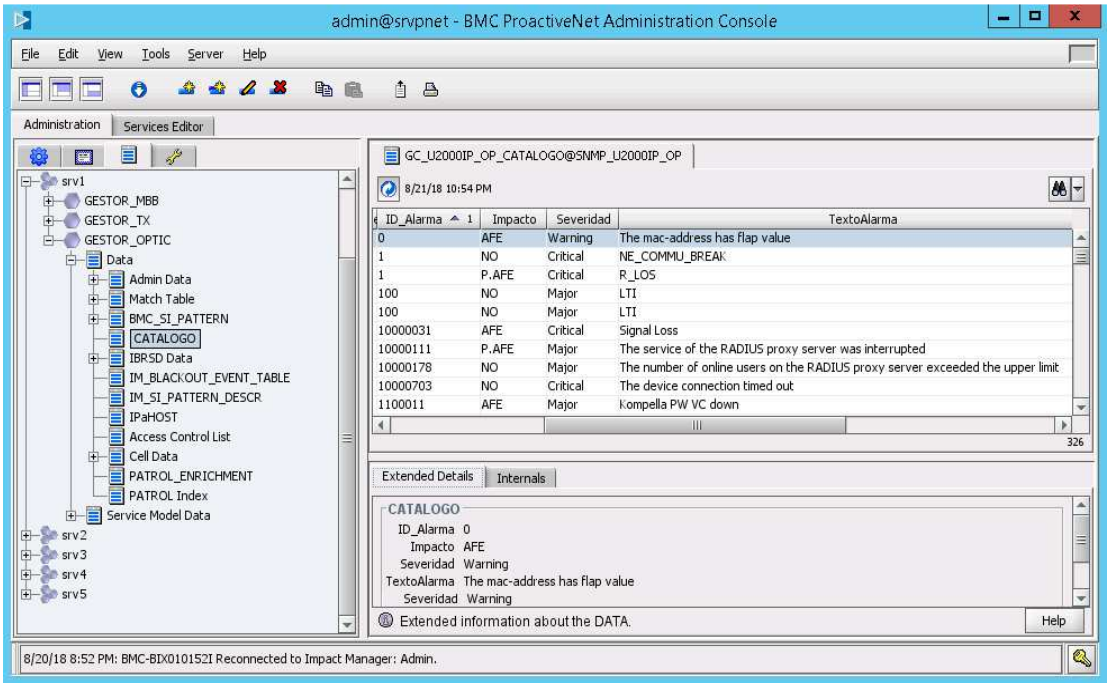


Figura 15 Catálogo de alarmas como tabla dinámica en la Consola Administrativa
Fuente: Elaborado por el Autor.

4.6.1. Reglas para la interpretación de incidencias

En el directorio rules de la KB se van a definir las reglas en base a la generación de alarmas, cerrado de alarmas, correlaciones de alarmas, filtros, propagación y deduplicación (Autor, 2018).

En siguiente figura se establecen dos reglas: ambas para la generación de alarmas, en la primera se realiza un arreglo de atributos para mostrarlos de acuerdo a la clase “EVENT” creada anteriormente con el fin de mostrar la información esencial y de forma clara. Para cada atributo se le asigna una posición del atributo snmp_vals analizado anteriormente. En la segunda regla se normalizan todos los eventos comparándolos con una tabla dinámica en donde se importa el catálogo de alarmas que pone a disposición cada proveedor. De este modo es posible hacer configuraciones de acuerdo a las

consideraciones y requerimientos del NOC en cuanto a ajustes en la severidad, prioridad, texto de alarma, etc.

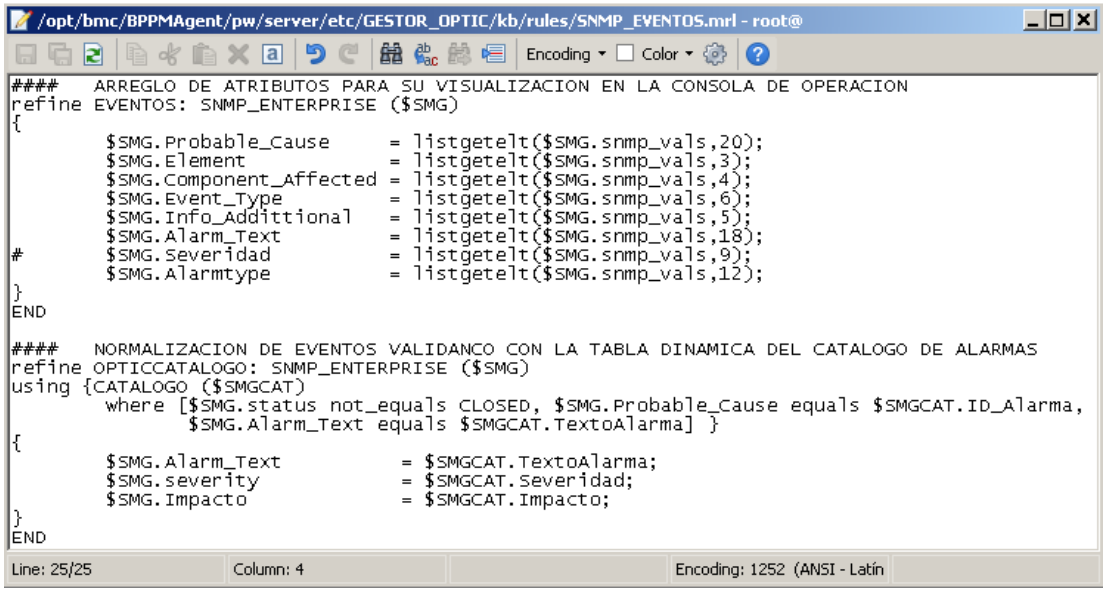


Figura 4. 24: Reglas de generación de alarmas
Fuente: Elaborado por el autor.

La siguiente regla define una regla de deduplicación que no es nada más que la comprensión de datos para depurar eventos que se identifiquen como duplicados, para esto se establece una comparación entre nuevos eventos y aquellos ya presentes. Aquellos eventos que arriben y ya se encontraban presentes serán filtrados y depurados automáticamente.

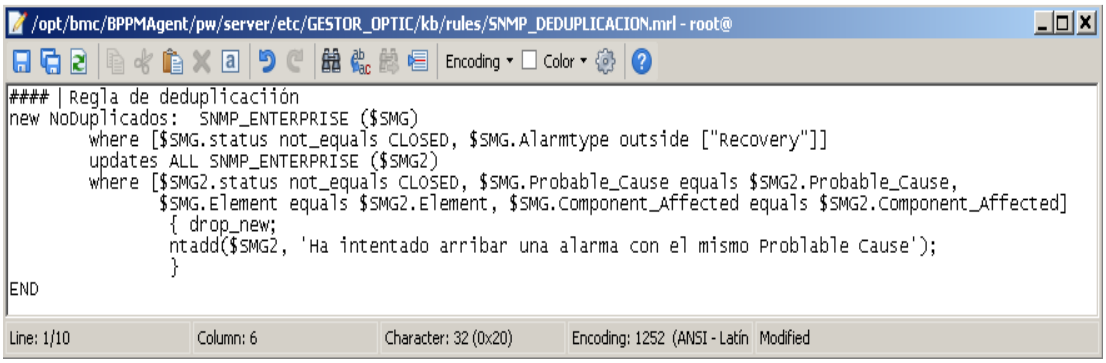


Figura 16: Regla de deduplicación
Fuente: Elaborado por el autor.

En la siguiente figura se encuentran dos reglas respecto a la cancelación de eventos. En la primera se aplica un filtro para una alarma en particular que es enviada constantemente con información no valiosa, los nuevos equipos pueden ser configurados para enviar eventos cada cierto tiempo con el objetivo de confirmar su operabilidad. En la regla se establece que no pasen a la consola de operación aquellos eventos que contengan un OID en particular en el atributo **snmp_enterprise**. En la segunda regla se establece el cerrado de los eventos cuando hayan sido solventados, el equipo automáticamente envía una alarma de tipo “Recovery” que se traduce al español como recuperación para cancelar las alarmas presentes. Para validar de que esa cancelación sea para un equipo es particular se establecen condiciones en donde se compara el Probable Cause, Elemento y componente afectado.

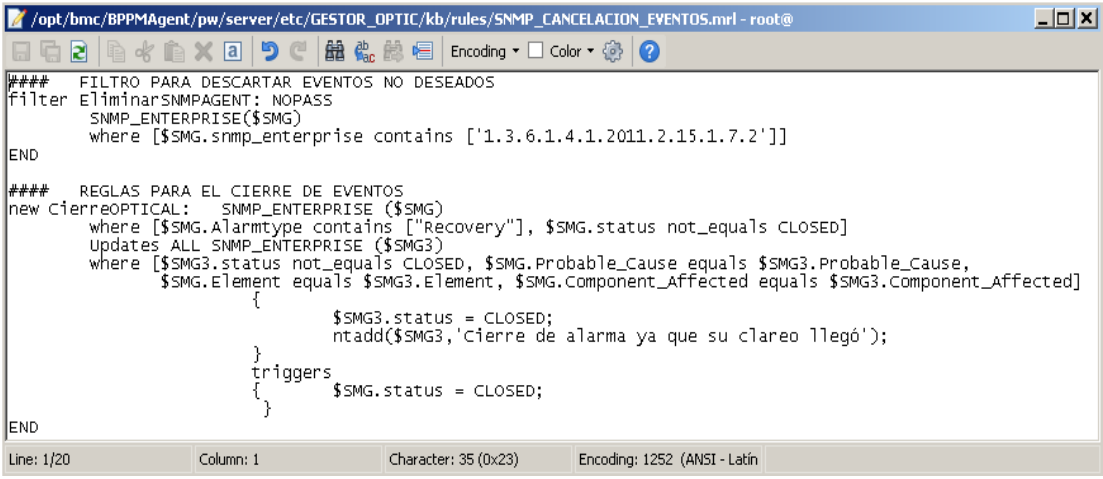


Figura 4. 26: Reglas para la cancelación de eventos
Fuente: Elaborado por el autor.

Ahora se debe establecer una regla de propagación que filtrará y reenviará las alarmas hacia un colector. En la regla se establece que aquellos eventos que cumplan con la condición de que tengan una severidad mayor a

Warning, será propagados hacia el Colector1 que consolida más celdas remotas para la visualización general de toda una infraestructura.

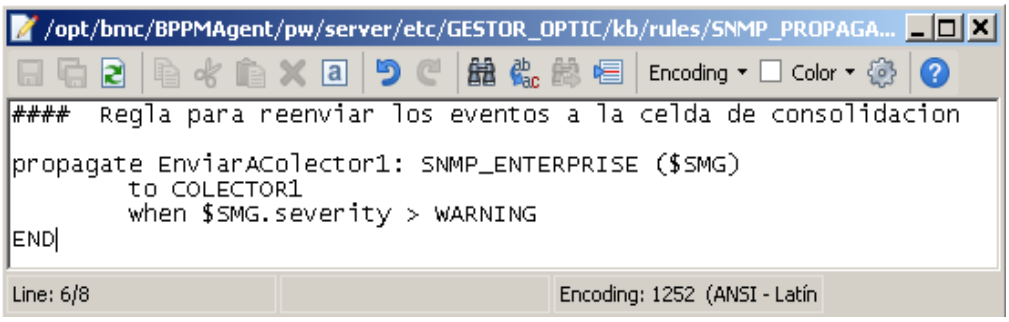


Figura 4. 177 - Regla de propagación de eventos hacia COLECTOR1
Fuente: Elaborado por el autor.

4.7. Pruebas Finales

Para culminar con una integración es necesario realizar pruebas de alarmas, en donde se generan afectaciones controlables para simular escenarios parecidos y ver el comportamiento de la herramienta.

Dentro de las áreas de una empresa de telecomunicaciones el NOC es el encargado de realizar el monitoreo de toda la estructura de Telecomunicaciones. Es esencial su presencia durante las pruebas, en conjunto con el proveedor quien generará las alarmas.

El NOC por lo general realiza pruebas como:

- Pruebas de generación de alarmas para validar que los campos se visualicen correctamente y el status sea el correspondiente.

- Pruebas de cancelación de alarmas, de este modo se valida el cerrado cuando el recovery de la alarma ha llegado.

- Pruebas de alarmas desde varios equipos de múltiples ubicaciones para validar la comunicación.

- Pruebas para validar el correcto funcionamiento de todas las reglas establecidas en la KB.

4.8. Visualización en la consola de operación

Una vez culminada la integración se establece un monitoreo en tiempo real del Sistema Gestor integrado, que administra los elementos de red que pertenecen al Core de la red móvil 4.5G, equipos de multiplexación DWDM y componentes de sistemas de fibra óptica. Cada anormalidad, afectación o cambio en la configuración de cualquiera de los dispositivos causará una alarma que se visualizará en la consola de operación.

En la siguiente figura se observan varias alarmas abiertas que representan incidencias de acuerdo al servicio o aplicación que afectan. La información básica que se muestra en cada una de las alarmas contiene los siguientes campos esenciales: Status, prioridad, severidad, fecha, impacto, probable cause, texto de alarma, elemento, componente afectado, tipo de evento e información adicional. Esto facilita que la persona encargada de la operabilidad pueda prevenir y solucionar problemas en un menor tiempo, al disponer de todos los detalles de la posible causa raíz del problema es posible mantener una alta disponibilidad de los servicios que cumple cada uno de los componentes de la red.

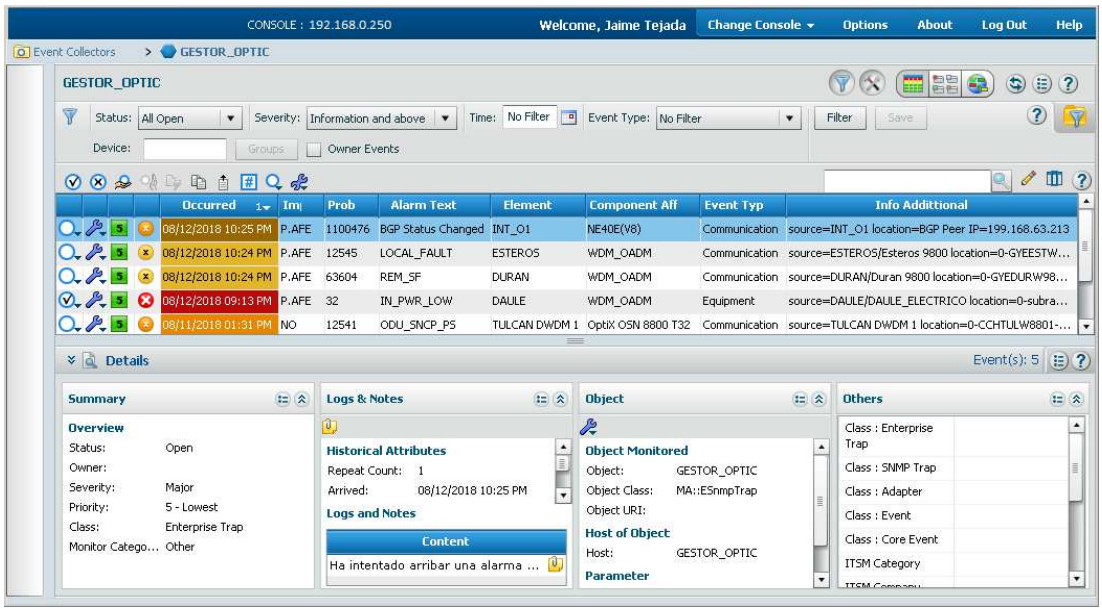


Figura 18: Alarmas activas
Fuente: Elaborado por el autor.

Cuando la incidencia ha sido solventada y la operabilidad se encuentra regularizada, los equipos son capaces de identificar su solución y envían una alarma parecida, pero con un campo distinto que contiene la palabra “Recovery” que hace mención a la recuperación del componente afectado. En la siguiente figura se pueden observar que las alarmas generas han recibido su recovery, por lo que se actualiza el status de ambas a cerrado.

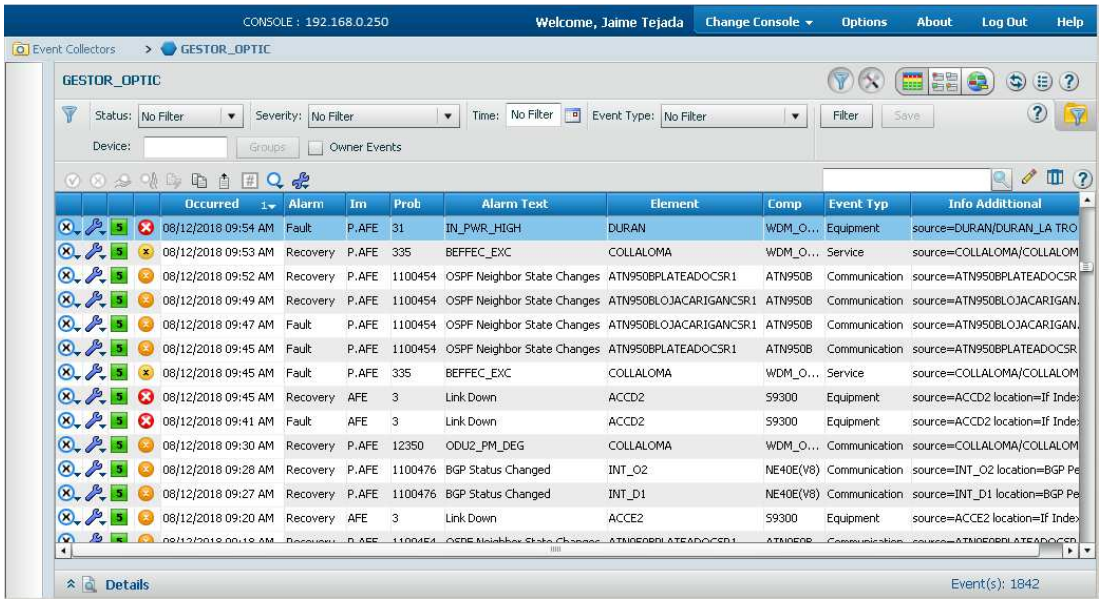


Figura 19: Cancelaciones de alarmas
Fuente: Elaborado por el autor.

De acuerdo a las posibles exigencias de visualización de la información es posible filtrar las alarmas de acuerdo a cualquiera de los campos que posee cada evento. Es decir, es posible filtrar de menor a mayor o viceversa de acuerdo a la severidad, prioridad, fecha, impacto, etc. Para prevalecer la prioridad de aquellas incidencias que necesiten una rápida solución y aplazar aquellas que no.

Las celdas también son consideradas como un histórico del status de la red y de sus componentes, lo que facilita determinar problemas que se presentan con mayor ocurrencia o buscar el detalle de las afectaciones que se tuvieron en determinados periodos de tiempo. Para ello por medio de filtros podemos realizar una búsqueda estableciendo los parámetros de la incidencia que se quieran analizar (host, componente afectado, probable cause, etc).

Para la búsqueda que se visualiza en la siguiente figura, se creó un nuevo filtro y se le asigno la clase “Enterprise Trap” ya que es comunicación SNMP. Luego se establecieron 3 condiciones de atributos: En Event type se define “equipment” para mostrar aquellas alarmas que provengan de equipos, en Status se establece que la alarma esté abierta y por último que el impacto sea Posible Afectación o afectación directa.

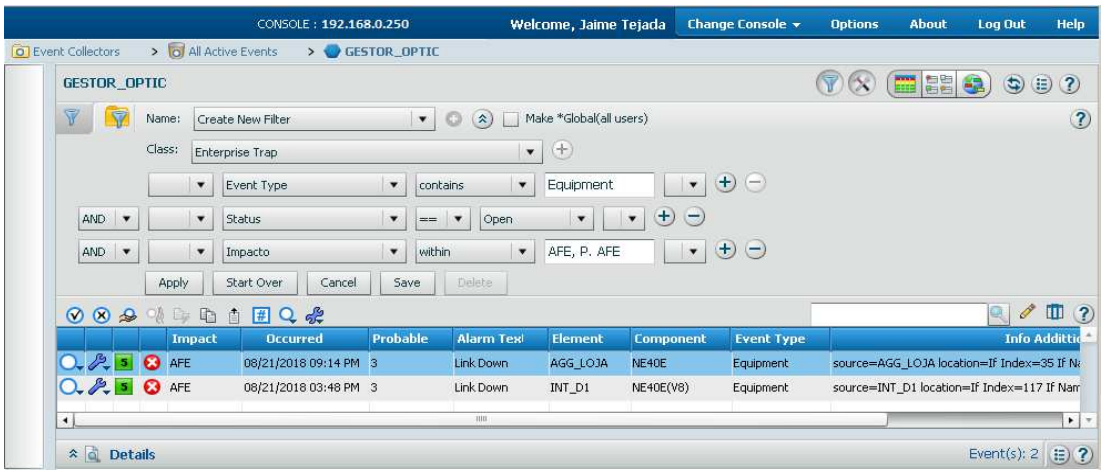


Figura 20 Búsqueda por incidencias por filtros de atributos
Fuente: Elaborado por el autor.

4.9. Colectores de celdas

La creación de un colector es igual que la creación de una celda remota. Una vez creada debe ser registrada en el directorio de celdas “mcell.dir” en el servidor de celda remota y servidor ProactiveNet. La diferencia de las otras celdas es que esta solo se encargará de consolidar otro tipo de celdas, por lo que se debe configurar la KB para crear subcolectores en donde se propaguen los eventos de cada una de las celdas remotas.

Debe crearse un archivo con extensión **.mrl** en el directorio “collectors” de la KB de la celda remota creada del Colector creado, en donde se indique la matriz de los roles de usuarios que tendrán acceso a su visualización y la condición o filtro que deberá cumplirse para la propagación de las alarmas al Colector1. A continuación se muestra la ruta del directorio del archivo y su estructura en la cual se establece que solo se filtrarán los eventos que provengan de la IP fuente del Sistema Gestor integrado:

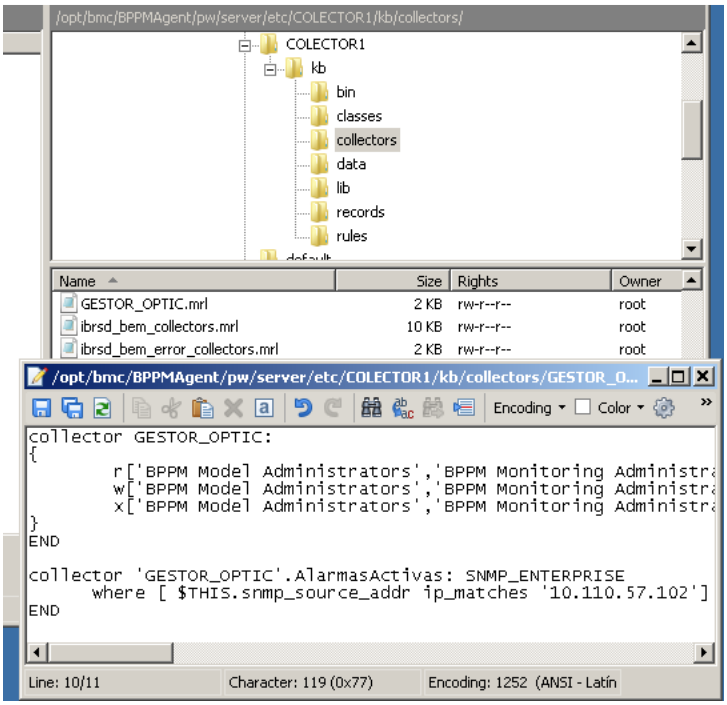


Figura 21: Regla para la aceptación de la propagación desde una celda remota hacia el Colector
Fuente: Elaborado por el autor.

4.9.1. Colector 1

En la siguiente figura se muestra el Colector 1 quien consolida varios sistemas de redes móviles. Como redes de transporte, acceso, transmisión, enlace y elementos de red que pertenecen a Comunicaciones móviles de las generaciones 2G, 3G y 4G. En ella podemos encontrar alarmas que provienen de celdas compuestas por la operación de varios elementos de red de las distintas generaciones móviles. Se puede obtener una vista general del status y de las anomalías de todas esas infraestructuras al organizarlas de manera estandarizada.

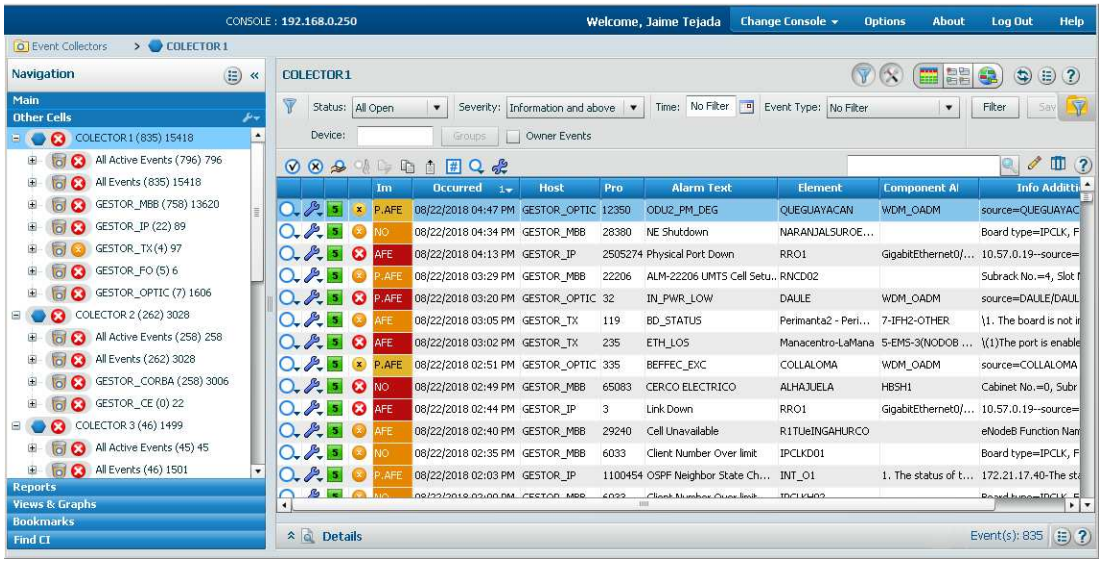


Figura 22: Colector 1 red móvil
Fuente: Elaborado por el autor.

4.9.2. Colector 2

La siguiente figura muestra el Colector 2 desde una vista de mosaico. Este consolida elementos de red móvil de GSM y UMTS que utiliza el estándar Corba como comunicación entre los nodos, además integra una aplicación que se encarga del Customer Care a través de métricas. ProactiveNet muestra un resumen total de todas las incidencias que actualmente están activas y las clasifica de acuerdo a su prioridad y a su severidad. De este

modo se puede realizar análisis de factibilidad en cuanto a las diversas estructuras que tiene una empresa, comprobando su correcta operabilidad en aquellos que tengan un menor número de incidencias.

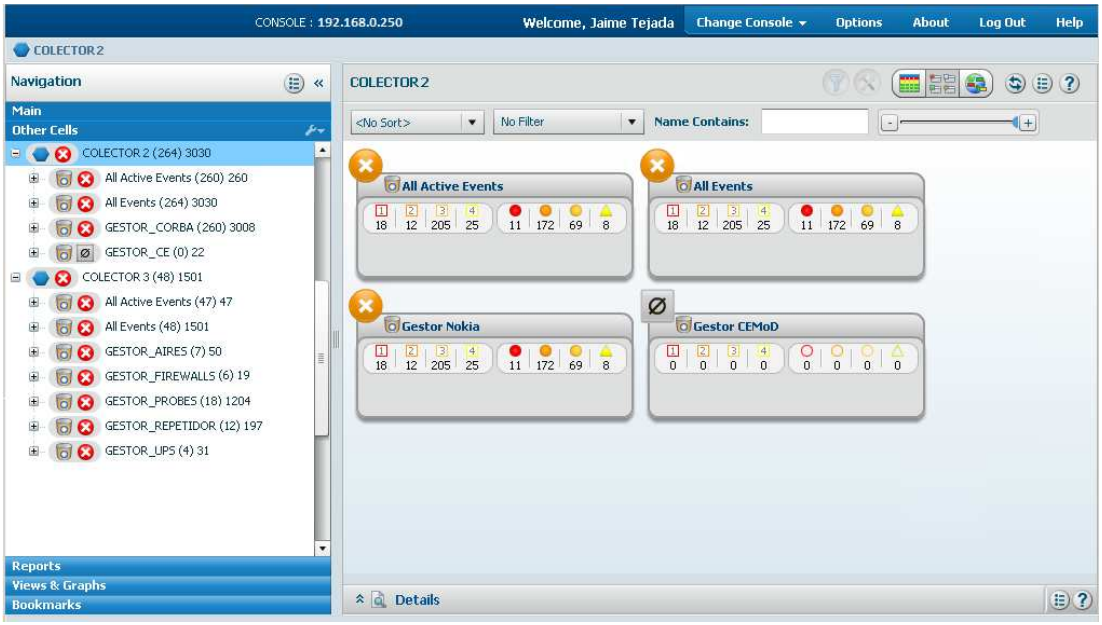


Figura 23 - Colector 2 estándar Corba sobre elementos de la red GSM y UMTS
Fuente: Elaborado por el autor.

4.9.3. Colector 3

En la siguiente figura se muestra el Colector 3 quien consolida componentes de hardware y software. Entre ellos Equipos UPS y Aires, recolectores de tráfico móvil y de voz (Probes), Sistemas Firewalls y Equipos repetidores de radiofrecuencia en zonas indoor. Además de realizar la convergencia de todos estos sistemas, es posible crear subcolectores dentro de cada Gestor que facilitan la búsqueda de incidencias al contar con una estructura totalmente configurable.

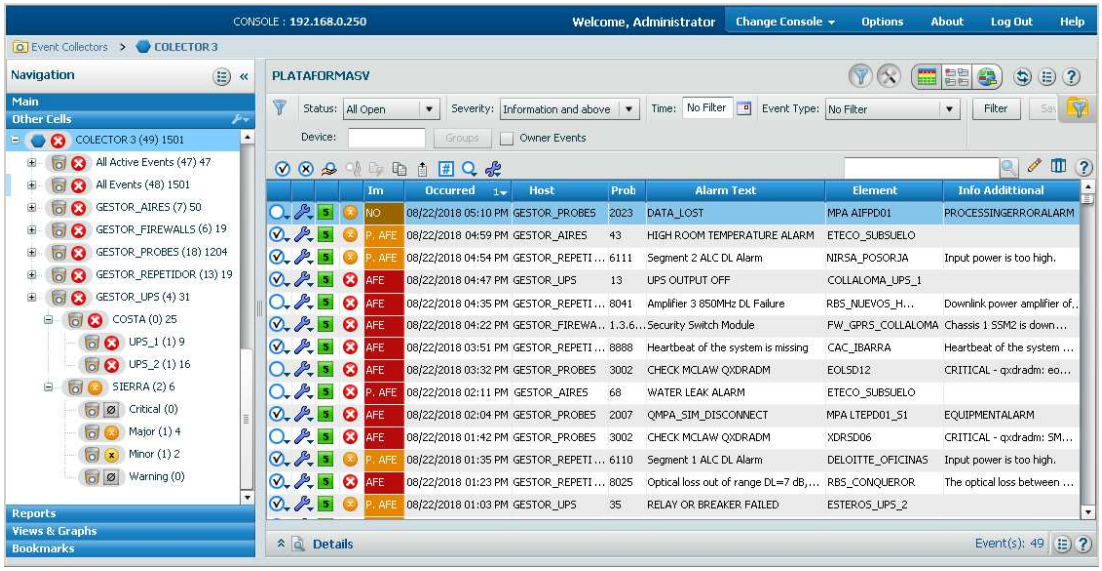


Figura 24: Colector 3 Hardware y complementos
Fuente: Elaborado por el autor.

Capítulo 5: Conclusiones

5.1. Soluciones para demás tipos, sistemas y equipos de red

En el capítulo 4 se mencionó el método de integración para un sistema de red móvil al Administrador de Gestores (MoM), en donde varios tipos de tecnologías convergen para hacerlo posible. El método para integrar otros tipos de red, sistemas gestores, elementos de red, equipos de TX y RX, etc. No es muy distinta a la que se explicó, los cambios necesarios se realizan en la configuración de la KB (Base de conocimiento) en donde es necesario realizar un análisis de todos los atributos de los traps que llegan para establecer los scripts definidos en la KB después de realizar la publicación de los MIBs y ajustar las direcciones IPs correspondientes.

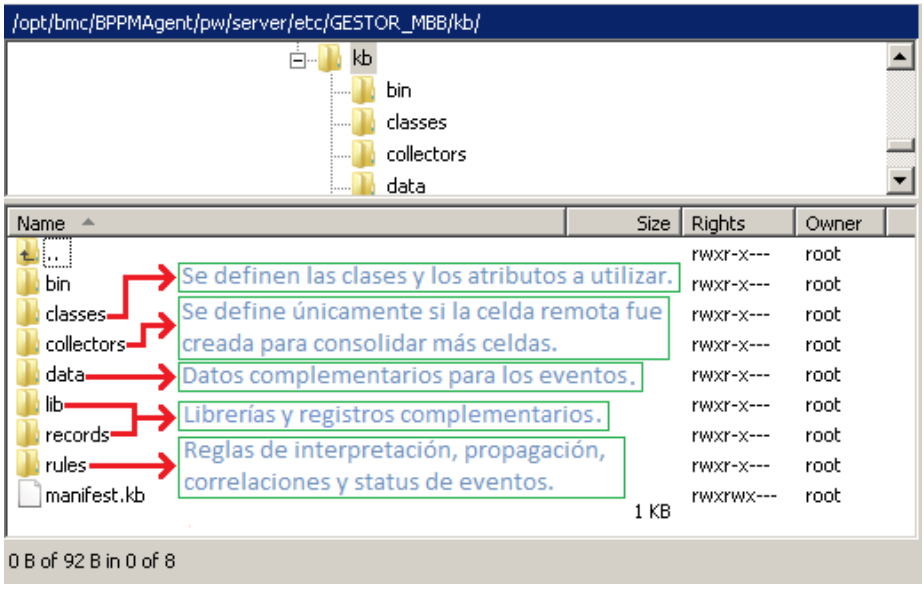


Figura 25: Configuración de kb para cada integración
Fuente: Elaborado por el autor.

Por medio del análisis de los traps se establecen los atributos a utilizar en las reglas de interpretación de los eventos y poder visualizar las alarmas en el administrador de gestores de una manera entendible. De este modo es

posible realizar integraciones de infraestructuras que dispongan de comunicaciones SNMP, Corba, ASCII. Para el caso de querer monitorear Sistemas operativos, Bases de datos, Racks, Servidores es posible la instalación de un agente dependiendo de las necesidades, uno de ellos el Agente PATROL capaz de monitorear rendimiento, almacenamiento y status.

5.2. Conclusiones

Es necesario la implementación de un Sistema MoM sobre toda la infraestructura de una empresa de Telecomunicaciones para identificar incidencias en tiempo real y realizar el análisis de su posible causa raíz. Esto permite la solución de afectaciones directas sobre los servicios y aplicaciones que se proporcionan al cliente. Asegurando así la funcionalidad de los equipos y de prevenir escenarios críticos en donde se pierden por completo los servicios de voz y datos.

Una estructura de monitoreo estandarizada reduce costos de pagos al personal que tiene la función de monitorear todas las herramientas que administran cada uno de los componentes de red. Además, la vista general y organizada de las infraestructuras integradas facilita la asignación de incidencias que le corresponden a las áreas correspondientes para su seguimiento y solución. Por medio de los filtros que provee ProactiveNet se puede prevalecer aquellas incidencias que tengan un alto nivel de impacto, severidad y prioridad.

En cuanto a redes móviles, permite la integración de los Gestores de Elementos de red de las generaciones 2G, 3G y 4G LTE. Esto facilita el monitoreo de los servicios de Voz y Datos que son proporcionados al cliente.

Además del status de repetidores que se encuentran implementados en zonas indoor por la alta atenuación de las ondas de radiofrecuencia. De este modo es posible determinar cuándo una celda móvil no se encuentra operativa además de los componentes afectados que causaron la incidencia para su solución inmediata.

En cuanto a redes fijas, la integración de equipos que pertenecen a los diferentes nodos facilita el conocimiento de anomalías y cambios que sufre la red. De tal modo que cuando se realiza un cambio no autorizado es posible identificarlo y reportarlo. Usando la información de las alarmas como respaldo, que muestra los parámetros enviados por el componente alterado.

El uso de Mom permite acceder desde dónde sea y cuándo sea para tener conocimiento del status actual de las múltiples infraestructuras consolidadas en la herramienta. Lo que facilita realizar análisis de factibilidad y operabilidad de los componentes de redes en tiempo real o en determinado tiempo. La información de cada una de las celdas remotas se encuentra disponible por meses incluso años de acuerdo a la configuración del operador. En caso de que un área de auditoría requiera de razones técnicas por el corte de servicios, es posible demostrarles técnicamente la causa raiz mediante la información de las alarmas almacenadas.

La implementación de un MoM permite la solución inmediata remotamente frente a incidencias reflejadas en la herramienta. Ya no es necesario estar en las centrales o estaciones para evidenciar las falencias de los equipos. De este modo los técnicos pueden evitar grandes afectaciones priorizando la solución de aquellos componentes que representen dependencia sobre el funcionamiento de otros.

Glosario

Archivo .mrl: Es la extensión de archivos de código fuente que contienen múltiples lenguajes de programación.

Atributos: Son campos que componen una trama de un paquete de datos.

Celdas remotas: Aquella celda que integra un sistema gestor o componentes de la red.

Colectores: Son celdas que se establecieron para consolidar celdas remotas y organizar una vista general con una arquitectura configurable.

Consola de Administración: Consola que se administran usuarios, políticas, datos dinámicos y celdas.

Consola de Administración Central de Monitoreo: Consola web que administra los agentes que monitorean los servidores.

Consola de operación: Consola web que utiliza el usuario final para la visualización y control de las incidencias.

CORBA: Estándar que permite a operabilidad de múltiples componentes con diferentes lenguajes de comunicación.

Eventos: Acontecimientos enviados por sistemas y equipos de redes.

KB: Base de conocimiento que contiene parámetros y políticas para la interpretación de la información.

MoM: Administrador de Gestores.

MIBs: Información de base gestionada, que contiene las arquitecturas y nomenclaturas de los identificadores de objetos (OIDs)

OIDs: Identificadores de objetos que contienen una arquitectura numérica que define un objeto específico.

Servidor de celdas: Servidor en el cual se almacenan celdas remotas.

Servidor ProactiveNet: Servidor principal que contiene las consolas web, administrativas y operativa. Recopila toda la información

SNMP: Protocolo simple de administración de red.

Traps: son mensajes de alertas enviadas remotamente desde algún equipo controlado por SNMP.

Bibliografía

Abdelwahab Saleh, D. M. (2017, mayo). Network Management (NETW-1001). IET-Networks, GUC. Recuperado de http://eee.guc.edu.eg/Courses/Networks/NETW1001%20Network%20Management/Lectures/Lecture9.pdf

Agrawal, J., Rakesh, P., Mor, D. P., Dubey, D. P., & keller, D. J. M. (2015). Evolution of Mobile Communication Network: from 1G to 4G, *3*, 4.

Agubor, C. K., Chukwudebe, G. A., & Nosiri, O. C. (2015). Security challenges to telecommunication networks: An overview of threats and preventive strategies. En *2015 International Conference on Cyberspace (CYBER-Abuja)* (pp. 124–129). Abuja, Nigeria: IEEE. https://doi.org/10.1109/CYBER-Abuja.2015.7360500

Alarcon, M., Javier Zorzano Mier, F., Jevtić, A., & Andina, D. (2008). Telecommunications Network Planning and Maintenance, *8*, 5.

Aleksy, M., Korthaus, A., & Schader, M. (2007). CORBA on Mobile Devices. En *Encyclopedia of Mobile Computing and Commerce* (pp. 160–164). University of Mannheim, Germany. https://doi.org/10.4018/978-1-59904-002-8.ch028

Armijos Farez, Y. (2017). *Implementación de un gestor de gestores MoM en una nube privada para el monitoreo de la red celular de una empresa de telecomunicaciones*. Escuela Superior Politécnica del Litoral

(ESPOL), Guayaquil - Ecuador. Recuperado de http://www.dspace.espol.edu.ec/handle/123456789/39158

BMC, S. I. (2018, febrero 2). BMC PATROL Agent 10.7 - BMC Documentation. Recuperado de https://docs.bmc.com/docs/display/PA107/Key+concepts

BMC, S. I., Wilson, P., & West, J. (2016, mayo 18). BMC ProactiveNet 9.6 - BMC Documentation. Recuperado de https://docs.bmc.com/docs/display/public/proactivenet96/Home?key=proactivenet96

Cárdenas Lino, C. (2016). *Simulación y análisis de desempeño de la red LTE para infraestructura de medición avanzada en Smart Grid*. Universidad de Chile, Santiago de Chile. Recuperado de http://repositorio.uchile.cl/handle/2250/141239

Criollo, R., & Javier, A. (2016). *Evolución de las redes de telecomunicaciones y calidad de servicio en redes de nueva generación NGN en el Ecuador*. Recuperado de http://repositorio.puce.edu.ec:80/xmlui/handle/22000/11111

Cruz Fabian, E., & Flores Galindo, I. (2017). *Estudio de acceso al medio para la tecnología 4G LTE.* Escuela Superior de Ingeniería Mecánica y Eléctrica, México D.F. Recuperado de http://tesis.ipn.mx:8080/xmlui/handle/123456789/21590

Giotopoulou, P. (2015). *The evolution of mobile communications: Moving from 1G to 5G, and from human-to-human to machine-to-machine*

communications. National and Kapodistrian University of Athens, Zografou - Greece. Recuperado de https://technodocbox.com/Computer_Networking/69535815-The-evolution-of-mobile-communications-moving-from-1g-to-5g-and-from-human-to-human-to-machine-to-machine-communications.html

González Espinoza, V., & Morocho Lovato, A. (2017). *Simulación y análisis del rendimiento de una red LTE mediante el software ns3 bajo condiciones de tráfico multimedia*. Escuela Politécnica Nacional, Quito - Ecuador. Recuperado de http://bibdigital.epn.edu.ec/handle/15000/18972

Huawei, T. C., Ltd. (2014, diciembre 4). Huawei iManager U2000. Recuperado de https://www.commoncriteriaportal.org/files/epfiles/Huawei%20iManager%20U2000%20Version%201%20Release%206%20Security%20Target%20v1.6.pdf

Kona, M. K., & Xu, C.-Z. (2002). A framework for network management using mobile agents. En *Proceedings 16th International Parallel and Distributed Processing Symposium* (pp. 8 pp-). https://doi.org/10.1109/IPDPS.2002.1016643

Larsson, T. (2017). Telecommunication Exchange Evolution. En J. G. Webster, *Wiley Encyclopedia of Electrical and Electronics Engineering* (pp. 1–16). Hoboken, NJ, USA: John Wiley & Sons, Inc. https://doi.org/10.1002/047134608X.W2043.pub2

NSW, T. for N. (2017, mayo 5). Telecommunication Equipment Network Management 1. Recuperado de https://www.transport.nsw.gov.au/industry/asset-standards-authority/find-a-standard/telecommunication-equipment-network-management-1

Saló Dobarganes, B., & Rivero Pons, I. (2015). *El Escenario de la 5G* (Thesis). Cujae.electrica.telemática, Habana - Cuba. Recuperado de http://tesis.cujae.edu.cu:8080/handle/123456789/1501

Santacruz, J., & Garcia, R. (2017). Convergencia de las Comunicaciones Móviles hacia Sistemas LTE y LTE-A de Cuarta Generación. *Killkana Técnica*, *1*(1), 15–22. https://doi.org/10.26871/killkana_tecnica.v1i1.16

Vora, M. L. (2015). Evolution of Mobile Generation Technology : 1G to 5G and Review of Upcoming Wireless Technology 5G. *Scientific Journal Impact Factor (SJIF)*, *2*(10), 11.

Zhen, Z., Qixin, C., Lo, C., & Lei, Z. (2009). A CORBA-based simulation and control framework for mobile robots. *Robotica*, *27*(3), 459–468. https://doi.org/10.1017/S026357470800489X

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Tejada Cáceres, Jaime Andrés** con C.C: # 092493284-1 autor del Trabajo de Titulación: **CONTROL DE INCIDENCIAS DE REDES DE TELECOMUNICACIONES MEDIANTE UN ADMINISTRADOR DE GESTORES (MOM)**previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 31 de Agosto de 2018

f. _____

Nombre: Tejada Cáceres, Jaime Andrés

C.C: 092493284-1

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Control De Incidencias De Redes De Telecomunicaciones Mediante Un Administrador De Gestores (Mom)		
AUTOR(ES)	TEJADA CÁCERES, JAIME ANDRÉS		
REVISOR(ES)/TUTOR(ES)	PALAU DE LA ROSA, LUIS EZEQUIEL		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	31 de Agosto de 2018	**No. DE PÁGINAS:**	116
ÁREAS TEMÁTICAS:	Comunicaciones Inalámbricas		
PALABRAS CLAVES/ KEYWORDS:	Redes móviles, Elementos de Red, Comunicación SNMP, Celdas remotas.		

RESUMEN/ABSTRACT (150-250 palabras):

Las empresas de telecomunicaciones están en constante evolución de sus servicios y de su infraestructura, creando así competitividad en el mercado presentando nuevos y mejores servicios a sus clientes. El desarrollo y aumento de tecnologías es evidente en los últimos años dentro del país, pero este va de la mano con el aumento de sistemas de red y de la exigencia de la calidad de los servicios ofrecidos. La infraestructura de las redes de telecomunicaciones es monitoreada constantemente por un área llamada NOC que poseen la tarea de monitorear la operabilidad de la red como también informar y dar soporte en las incidencias que ocurren sobre la red, entre las incidencias se encuentran fallas en equipos, saturación de servicios, status de equipos, congestión de las redes, fallas de autenticación etc. Que son visualizadas dentro de los Sistemas Gestores de cada proveedor. Sin embargo, el uso de diversas herramientas que poseen distinto proveedor, servicio, modelo, etc implica que se debe ingresar a varias plataformas para poder medir el rendimiento de la red como también incrementar cantidad de empleados. Un administrador de gestores es capaz de consolidar varios tipos de redes y de tecnologías en una sola interfaz, de tal modo que el personal del NOC y directores de la empresa pueden realizar mediciones de desempeño de las redes y monitorear en tiempo real toda su infraestructura con una sola herramienta. Esto permite la toma de decisiones en un menor periodo de tiempo para solucionar o prevenir afectaciones dentro de la red, asegurando la calidad de los servicios.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593983328074	E-mail: jaime_tejada94@hotmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez Edwin Fernando	
	Teléfono: +593-9-68366762	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	