UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CONTROL DE CALIDAD Y MONITOREO DE MANTENIMIENTO PARA ESTACIONES BASE DE UNA RED DE TELEFONÍA MÓVIL

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero Eléctrico Electrónico

P R E S E N T A

Samuel Montiel López

ASESOR DE INFORME

M. en C. Edgar Baldemar Aguado Cruz

Ciudad Universitaria, Cd. Mx., 2017

Tabla de Contenido

Informe de Trabajo Profesional

Control de calidad y monitoreo de mantenimiento para estaciones base de una red de telefonía móvil

Introducción y Objetivo:

El objetivo del presente informe es exponer las diferentes actividades que realizo en mi empleo, las cuales, para el proyecto en el que participo (RSA/SNTT) se dividen en dos tareas principales, antes de explicar estas dos tareas es preciso definir quién es el cliente para el cual trabajamos.

Ericsson, como empresa de telecomunicaciones brinda servicios y soluciones, así como equipo para redes telefónicas a sus clientes, En este caso uno de sus clientes es Sprint, una empresa estadounidense de telefonía celular que brinda cobertura de 3g y 4g a sus usuarios en el territorio de Estados Unidos y Hawái.

Entre los proyectos que tiene la empresa con Sprint está RSA/SNTT del cual formo parte y en el que realizo dos tareas principales:

- **RSA (Remote Site Acceptance)** Aceptación remota de sitios

En este punto es preciso definir un término que será muy usado durante todo el reporte, este es el término "sitio", el cual se usa para referirse de otra manera a una radio base o "cell site" sitio celda de una red celular.

Retomando la explicación de las actividades para la parte de RSA, estas son, como su acrónimo indica, la aceptación de manera remota de sitios que son los nodos de acceso a la red, se realizan una serie de verificaciones correspondientes a la configuración que un sitio debe tener, como son; visibilidad de alarmas, alarmas activas, registro correcto en la base de datos, configuración de hardware y software correcta, capacidad de procesamiento de datos y llamadas, verificación de backhaul (la parte de transporte en la red), y por último la verificación general, la cual solo será exitosa si todas y cada una de las verificaciones anteriores son correctas, lo que significa que, en este caso el producto entregado, el sitio, cumple con los requerimientos de calidad necesarios para ser dado de alta y pueda brindar el servicio a los usuarios.

Más adelante se explicará a fondo cada una de las verificaciones efectuadas.

La finalidad de esta parte del proyecto es brindar un servicio de control de calidad al cliente, ya que el equipo comprado por el cliente, el cual como producto final es un sitio o estación base, debe tener las especificaciones y características antes mencionadas, en el caso en el que alguna o varias verificaciones falle, el producto tendrá que ser corregido por el fabricante en cuestión y devuelto para su nueva revisión hasta que este cumpla con los estándares necesarios.

- **SNTT (Sprint Network Touch Tracking)** Seguimiento de mantenimientos a la red de Sprint

En este segundo punto lo que hago es un registro de entrada y salida de técnicos que realizan mantenimientos a sitios de la red, comparando el estado del sitio antes de que el técnico comenzara a trabajar y después de que este ha terminado, esto con la finalidad de garantizar que la persona encargada de realizar el mantenimiento no deje un sitio más afectado o con una mayor cantidad de alarmas que como estaba antes de comenzar a trabajar. Esto se explicará a fondo más adelante.

Descripción de la empresa

Breve historia de la empresa

La comunicación es una necesidad humana básica, esa fue la simple visión de Lars Magnus Ericsson cuando abrió su taller de elaboración y reparación de telégrafos en 1876 en Estocolmo Suecia, sin embargo, cuando la gente iba con Lars, él ve una oportunidad estupenda y comienza a fabricar teléfonos con su propio diseño, un ingeniero con una visión, cuyos diseños pronto capturan la imaginación del público.

Lars Magnus Ericsson
CEO 1876 – 1900.

En 1883, forma una sociedad que será la realización de su empresa. Henrik Thore Cedergren es un empresario que, así como Lars Magnus, ve el potencial del teléfono. El objetivo de la sociedad es proveer de líneas telefónicas a cada edificio y a todos los inquilinos que habitan en este, a un precio más económico.

Ellos construyen un armazón de andamios con 1200 líneas en el techo de la central telefónica, la cual es capaz de mantener a más de 3000 suscriptores. El resultado de esto es que para 1885 Estocolmo tiene más suscriptores telefónicos que cualquier otro lugar en el mundo, volviéndose el teléfono en algo esencial para la vida.

Con una demanda global que aumenta a una gran velocidad, las operaciones de la empresa se expanden alrededor del mundo. En Rusia, China, México, los cables se extienden a través de los países, y en las ciudades los cielos se oscurecen con ellos.

En 1903 cuando Lars Magnus se retira, su empresa es una de las principales proveedoras de teléfonos a nivel mundial con centrales telefónicas presentes en más de 100 países.
Esta escala global probaría ser un recurso definitivo para darse cuenta de la visión de conectar personas hasta nuestros días.

Ericsson en México

En 1905, la empresa obtuvo una concesión para operar la red telefónica en la Ciudad de México y las zonas periféricas. Cuatro años más tarde, una filial de Ericsson, Mexeric, se hizo cargo de estas operaciones.

México, 1930,
Robot telefónico de madera.

Después ITT había adquirido la empresa de la competencia Mexicana en 1925, las dos compañías se enfrentaron con fuerza para convertirse en el líder, y preferiblemente el único operador de telecomunicaciones en México

Axel Wenner-Gren estaba viviendo en México y tenía mucho capital después de tener acciones vendidas en la compañía de productos forestales suecos SCA. Las negociaciones entre él, Ericsson y Mexeric dieron lugar a un nuevo acuerdo que se firmó entre las partes en 1947, que crearon una nueva compañía. Fue nombrada Teléfonos de México S A y fue llamada Telmex.

Después de algún tiempo, los propietarios no estaban de acuerdo sobre el futuro de Telmex. En 1953, Ericsson compró a Axel Wenner-Gren, y se llegó a un acuerdo en el que Ericsson e ITT haría cada uno su propia mitad del capital social de Telmex.

Con el gobierno tomando un papel activo en la industria, fue considerado mejor transferir a Telmex a los intereses de México. Un grupo de empresario mexicano compró las acciones de Ericsson e ITT. Telmex fue finalmente asumida por el Estado.

Es así como la empresa decide invertir en manufactura en el país y en 1989, se instala el primer sistema de telefonía móvil AMPS en México con Ericsson como proveedor.

México. 1930, Inauguración de una línea telefónica.

Cuando la primera línea telefónica internacional de la empresa con Estados Unidos y Canadá había sido oficialmente inaugurada, la primera llamada fue hecha entre el famoso piloto coronel mexicano Roberto Fierro y su esposa e hija.

Hoy en día la empresa es un líder mundial en el ambiente rápidamente cambiante de las tecnologías de comunicación, proporcionando equipo, software y servicios para permitir la transformación a través de la movilidad, también es de las pocas empresas que ofrecen soluciones end-to-end para los estándares de comunicaciones móviles. La comunicación está cambiando la forma en que vivimos y trabajamos. La compañia juega un papel importante en esta evolución.

Proporciona redes de comunicación, servicios de telecomunicaciones y soluciones, haciendo más fácil para las personas alrededor del mundo comunicarse, sirviendo a clientes en más de 180 países. Aproximadamente 40% del tráfico móvil del mundo pasa a través de equipo de red suministrado por la empresa.

Cuenta con 37.000 patentes concedidas, que comprende uno de los portafolios más fuertes de la industria.

ERICSSON

Actual Logo Ericsson.

Visión

La visión de la empresa es la de una Sociedad Conectada, donde todas las personas e industrias estén habilitadas para alcanzar su máximo potencial.

Creemos que se formará un mundo mejor y más sostenible cuando todas las personas estén conectadas. Desde hace tiempo que ha previsto la llegada de una Sociedad Conectada: una en la que, la conectividad acerque aún más a las personas, en donde la colaboración forme parte de la vida diaria y donde todas las personas e industrias estén habilitadas para alcanzar su máximo potencial.

Misión

Dirigimos la transformación a través de la movilidad. El potencial de la Sociedad Conectada se encuentra en la transformación a través de la movilidad. La transformación es la manera en que las personas organizan sus vidas y llevan a cabo tareas vitales. La transformación es la forma en que trabajamos, la forma en que compartimos información y la forma en que hacemos negocios. La transformación es la forma en que consumimos y la forma en que creamos.

Valores fundamentales

Respeto. Profesionalismo. Perseverancia. Estos son los valores fundamentales que definen la cultura de la empresa y nos guían en nuestro trabajo diario y en la forma en que hacemos negocios. Nos guían en nuestro compromiso con nuestros clientes, un compromiso que está ligado a la confianza, la innovación y el desempeño.

GSC México

GSC MX (Global Services Center Mexico) es uno de los cuatro GSC en el mundo cuyo principal objetivo es fomentar la eficiencia de escala con el fin de proporcionar, a través de las regiones, costes menores de servicios con el apoyo más eficiente, utilizando las herramientas adecuadas, la mejora de los procesos y la escala.

Global Network Operations Center (GNOC) México dentro del GSC México es una organización que ofrece operaciones de servicios gestionados a una amplia gama de operadores multi-proveedor y multi-tecnología con diferentes tamaños e infraestructura de complejidad a importantes operadores de telecomunicaciones de todo el mundo.

MS OPS (Managed Services Operations) es la organización responsable de operar, gestionar y monitorear telecomunicaciones e infraestructura de tecnologías de información (servicios y recursos) de los clientes y los servicios proporcionados a sus usuarios finales, conforme al alcance de un contrato MS. El alcance de la organización cubre tres unidades principales.

El alcance de la organización abarca: Cumplimiento, 1er nivel de Operaciones, 2º nivel de operaciones, incidencias, problemas y gestión de cambio y Service Desk.

Descripción del puesto de trabajo

El puesto de trabajo es ingeniero de primer nivel de operaciones, el cual es responsable de la coordinación, apoyo, gestión y ejecución de actividades de mantenimiento proactivas y reactivas de primer nivel para asegurar que el servicio entregado a los clientes este continuamente disponible y realizado por los niveles de desempeño del Acuerdo de Nivel de Servicio (SLA) por sus siglas en inglés, agrupando las actividades que requieren la ejecución 24x7.

Este puesto de trabajo debe estar alineado con la función de servicio "1st Level Operations".
La función de servicio está compuesta por un número de elementos de servicios y actividades que definen el ámbito de trabajo de acuerdo a la oferta de servicios gestionados MS de la empresa.

Se lleva a cabo recurso continuo, estado del servicio y la supervisión del rendimiento para detectar proactivamente los posibles fallos y actuar sobre ellos para asegurar la restauración y reparación de primer nivel. Es responsable de manipular los informes de problemas o las llamadas recibidas desde el Centro de atención al cliente del operador o Service Desk y garantizar 1er nivel de resolución de incidentes. También es responsable de la gestión del ciclo de vida del incidente, siendo responsable de dar seguimiento a TT (Trouble tickets) desde su creación hasta que el incidente ha sido resuelto y el TT esté cerrado.

Da seguimiento a la ejecución de cambio, aprobando el comienzo de la ejecución de actividades y asegurando que la actividad no ha tenido efectos negativos en la infraestructura del cliente. También es responsable de involucrar a un proveedor externo en caso de que forme parte del servicio afectado o parte de la escalación funcional.

Competencias conductuales

- Obtención de resultados y satisfacción de las expectativas del cliente
- Seguimiento de Instrucciones y Procedimientos
- Análisis
- Trabajar con personas

Proceso aplicable conectado con el puesto de trabajo

Gestión de eventos
Gestión de Incidentes
Gestión de cambio
Gestión de Acceso
Actividades del Proceso operativo

Descripción de elementos de servicio

1er Nivel de Aseguramiento de Actividades de Apoyo (1st Level Assurance Support Activities)

Monitoreo y apoyo de introducciones de cambios en el entorno real del cliente (operador) como parte del proceso de Gestión de Cambio.

Conceder autorización para el grupo que lleve a cabo un cambio previsto para iniciar actividades de acuerdo a la petición de cambio, asegurando que el impacto en los servicios se encuentre dentro de los límites acordados y que la ejecución se lleva a cabo dentro de plazo aprobado.
Apoyo al mantenimiento de campo cuando se requiere la asistencia debido a la naturaleza del mantenimiento especificado o si el personal de mantenimiento de campo enviado necesita ayuda para resolver situaciones problemáticas durante el mantenimiento.
Responsable de recopilar información y preparar informes de KPI (Key Performance Indicator) de acuerdo a las plantillas acordadas.

Tareas principales:

Apoyo a ejecución de mantenimiento preventivo de operaciones de Campo
Autorización de inicio de ejecución de cambio
Monitoreo de cambio planeado de la hora de finalización
1er nivel de ejecución de mantenimiento preventivo
Colección de datos de informe

Gestión de eventos (Event Management)

Permitir la estabilidad de entrega de servicios mediante el control de todos los eventos que se producen en toda la infraestructura del operador con el fin de asegurar que los servicios y recursos están operando a un rendimiento regular y dentro de SLA acordado, y para detectar y escalar excepciones. También proporciona el punto de entrada para la detección de cualquier notificación procedente de Gestión de Problemas del Cliente (ya sea desde el Centro de atención al cliente del operador o del service Desk de la empresa). Proporciona una forma de comparar el desempeño actual y el comportamiento frente a las normas de diseño y SLA, una base de rendimiento e informes de KPI y las iniciativas de mejora continua del servicio.

Tareas principales:

Supervisión del rendimiento de los recursos
Supervisión del rendimiento del servicio
Monitoreo de eventos de seguridad
La identificación de incidentes
Apoyo de investigación de capacidad y desempeño

Gestión de incidencias de 1er nivel (1st Level Incident Management)

Representa las actividades llevadas a cabo en el 1er nivel de operaciones para restaurar el servicio normal tan pronto como sea posible y minimizar el impacto adverso en las operaciones comerciales, asegurando así que el SLA acordado se mantenga. Es el punto inicial de escalación funcional para todas las incidencias detectadas en el entorno del operador y se encarga de acoplar el correcto nivel de competencia en el tiempo de respuesta correcta. En caso de incidentes críticos (y, opcionalmente, mayores) se inicia y apoya la función de gestión de incidentes. Es responsable del análisis de incidencia inicial y para la aplicación de error conocido o soluciones de incidentes.

Es el responsable fin a fin de la administración de tickets de incidentes y para su notificación e informes de estado.

Tareas Principales:

Resolución 1er nivel de incidencia
Notificación de incidentes e informes de estado
Cierre de incidente

Marco Teórico

Telefonía celular

Las redes móviles hoy en día juegan un papel muy importante en las comunicaciones, ha habido a lo largo de la historia una evolución en la tecnología de telefonía celular hasta ser como la conocemos ahora.

La tecnología se ha transformado del sistema analógico inicial, a las redes digitales de mayor capacidad que usamos hoy en día, cada generación sucesiva ha tenido capacidades más altas, puede albergar más señales en una cantidad de espectro dada y soporta características y funciones adicionales.

Las redes móviles están basadas principalmente en estándares de segunda, tercera y cuarta generación, estándares adicionales que son transiciones entre generaciones son 2.5, 3.5 y precuarta generación o 3.9.

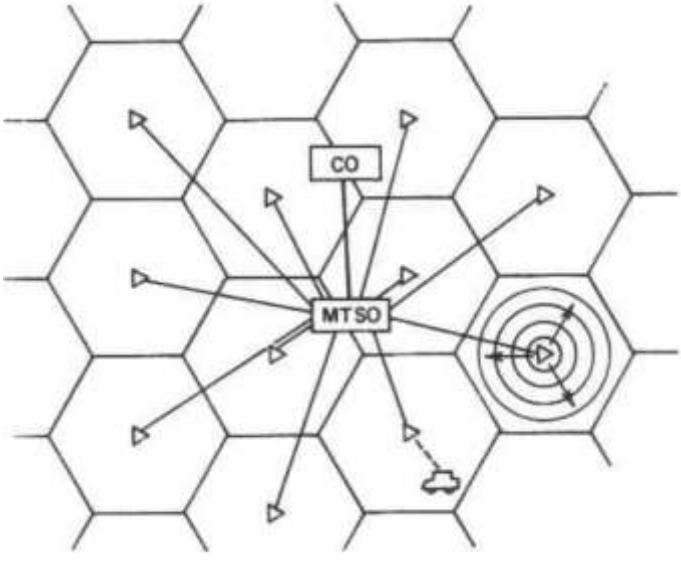
Se compone de switches y bases de datos interconectados, la única parte de la red que es en realidad inalámbrica es entre el usuario y las antenas, las señales transmitidas de y hacia las antenas viajan a través de líneas terrestres hacia el Core centralizado de la red.

El equipo en la parte de core proporciona conexión con sistemas de facturación, bases de datos, y *Gateways,* entre otras. Los *Gateways* son la entrada a redes fijas y a redes externas como lo es Internet.

La telefonía celular se compone de radio estaciones base RBS conectadas a una oficina de conmutación digital, también llamada oficina de conmutación de telefonía móvil (MTSO) por sus siglas en inglés, la cual está conectada a la parte de Core centralizado.

A medida que el usuario se mueve de una celda a otra, el MTSO hace el cambio de conexión a la estación base correspondiente con el fin de mantener una conexión continua para no perder la comunicación mientras el usuario se encuentra en movimiento, este procedimiento se conoce como *handover*.

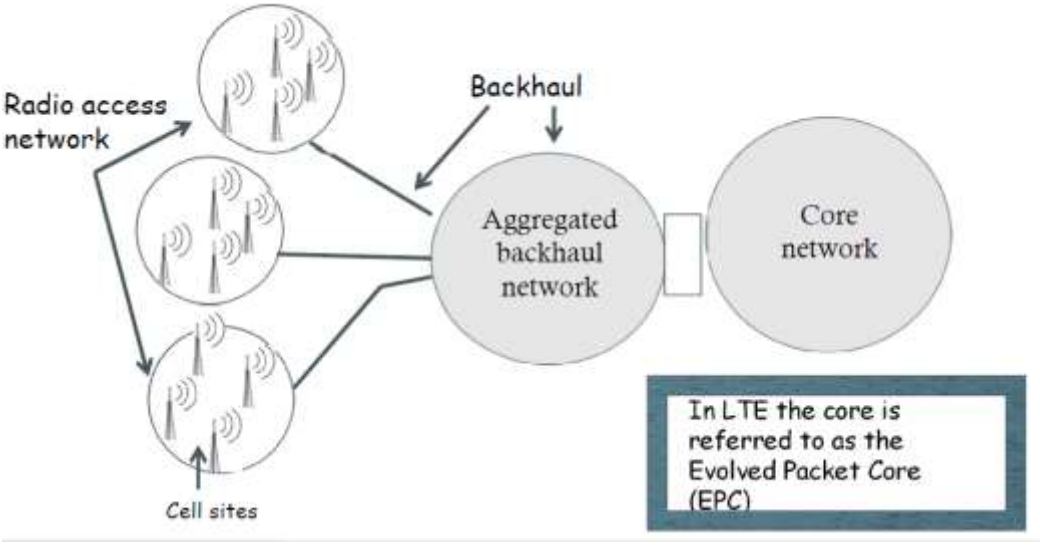
Se denomina celular ya que el espectro se aloja en un área geográfica llamada celda, las celdas una junto a otra usan diferentes frecuencias, esto para evitar interferencia, las celdas no contiguas reutilizan o repiten frecuencias.



Topologia de una red celular movil.

Red Agregada Backhaul

La parte de la red que conecta la parte de radio acceso con la parte de core, se denomina *Backhaul*, existen diferentes tipos los cuales pueden ser cableados, como lo es la fibra óptica, o inalámbricos, como lo son las microondas, esta es la parte de transporte de datos de la redo red de transporte.



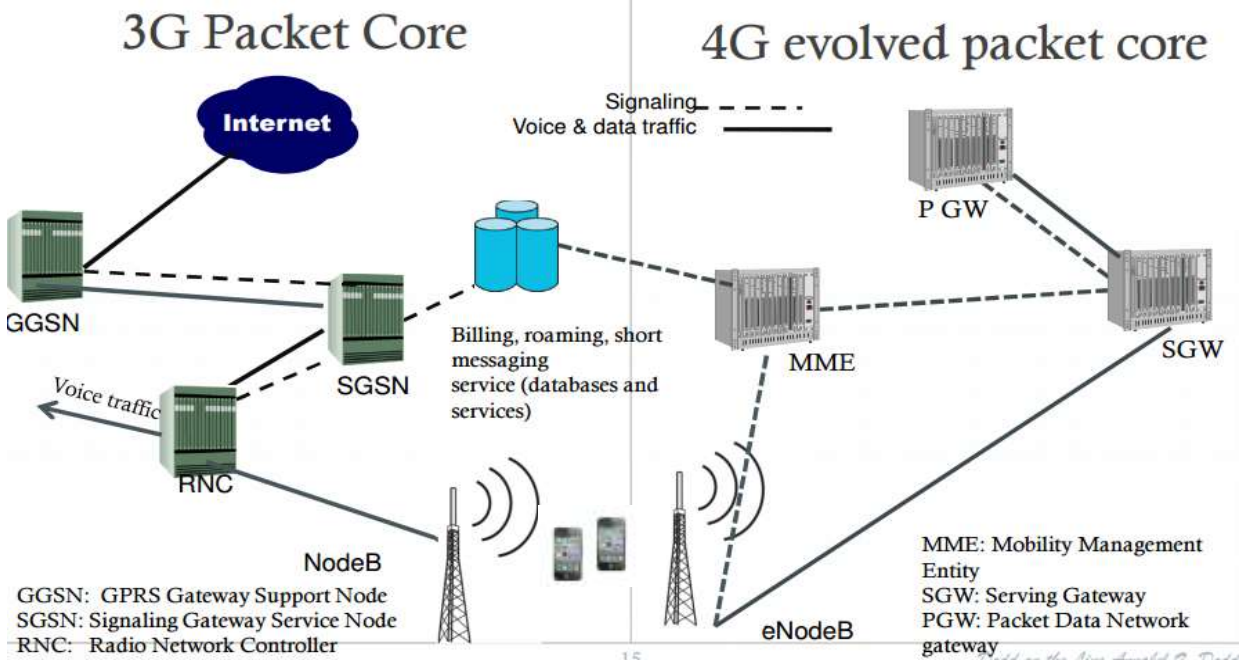
La red agregada consolida el tráfico de múltiples celdas antes de ser enviadas hacia el Core.

Dependiendo de la cantidad de tráfico, la red de Backhaul usa lo siguiente:

- T1/E1 (1.54Mbps/2.05Mbps) con cable de cobre
- Microondas (un servicio de transmisión inalámbrico) (44Mbps/34.4Mbps)

- Gigabit Ethernet y MPLS (Multiprotocol Label Switching) (10Gbps con capacidades de QoS) con cable de fibra optica.

Arquitectura de red 3G y 4G LTE



Arquitectura 3G y 4G

La red 3G usa tecnología *packet-switched* para datos, mientras que la voz es llevada de manera separada usando tecnología *circuit-switched*. En contraste a la cuarta generación (4G), la cual utiliza *packet-switched* tanto para voz como para datos.

Todo dispositivo inalámbrico contiene radios. Los radios en las redes móviles extraen señales de radiofrecuencia del aire y las convierten en pequeños bits de frecuencia compatibles con los dispositivos, los radios convierten las señales a las frecuencias usadas en la red celular y transmiten esas señales inalámbricas por el aire.

Las estaciones base son la porción más extensa de una red móvil, los llamados NodeB's, nombre que reciben las radio bases para la tercera generación, contiene antenas y radios que traducen de radiofrecuencias (señales que viajan por el aire) a señales digitales para poder ser procesadas y viceversa, después se encuentra la (**RNC**) Radio Network Controller que controla los *handovers* de llamadas a otras radio bases o sitios celda, está conectada a dichos sitios y a otros controladores.

GPRS Gateway Support Node (**GGSN**) convierte los paquetes de UMTS (Univelsal Mobile Telecommunications System) a aquellos compatibles con GPRS, Internet y otras redes de datos y vice versa.

Signaling Gateway Service Node (**SGSN**) Transmite datos entre RNC y las bases de datos de la red, aplicaciones, y sistemas de facturación, también comunica con el GPRS Gateway.

LTE (4G) usa menos protocolos y requiere menos equipo en su red Core que las arquitecturas de 2g y 3G, incluso distribuye algunas funciones encontradas en la red Core de la arquitectura de 3G a equipo en el sitio celda.

El **eNodeB** (Evolved NodeB) es la estación base, junto con las antenas, amplificadores y es usado para acceder a la red, constituye el Radio Access Network (RAN), la función de la RNC de las arquitecturas anteriores es ahora migrada a el eNodeB

Las funciones dentro de la red Core de LTE está dividida en tres elementos principales.

Mobility Management Entity (**MME**) - Este realiza la función de señalización en el IP Core. Envía y recibe información de señalización necesaria para direccionar llamadas al eNodeB y al Serving Gateway. Además, contiene los protocolos de seguridad, autenticación y autorización.

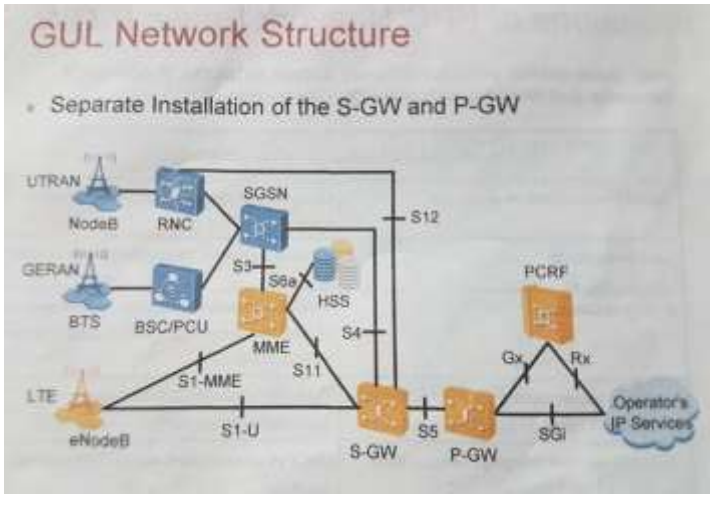
Serving Gateway (**SGW**) - Reenvía los paquetes de datos en caminos de canales entre el eNodeB y el PGW. Maneja la conversión de protocolos entre dispositivos LTE y sistemas 2Gy 3G.

Packet Data Network Gateway (**PGW**) – Almacena la direction IP de los usuarios. Puede clasificar paquetes con requerimiento de calidad de servicio (QoS), también genera medidas de uso de voz y tráfico para propósitos de facturación.

Estructura de Red GUL

La estructura de red GUL (GSM-2G,UMTS-3G,LTE-4G), es una estructura unificada de las tres generaciones digitales de telefonía celular, las cuales se interconectan entre si para brindar servicios de las tres generaciones en una misma red, es el sistema implementado actualmente en el cual coexisten las tres tecnologías, los beneficios sonlos siguientes:

- Simplifica el manejo y desarrollo de la red.
- Disminuye el gasto en señalización y reenvio de paquetes, lo cual reduce en gran medida el tiempo de respuesta.
- Disminuye el costo de implementación para operadores de red.

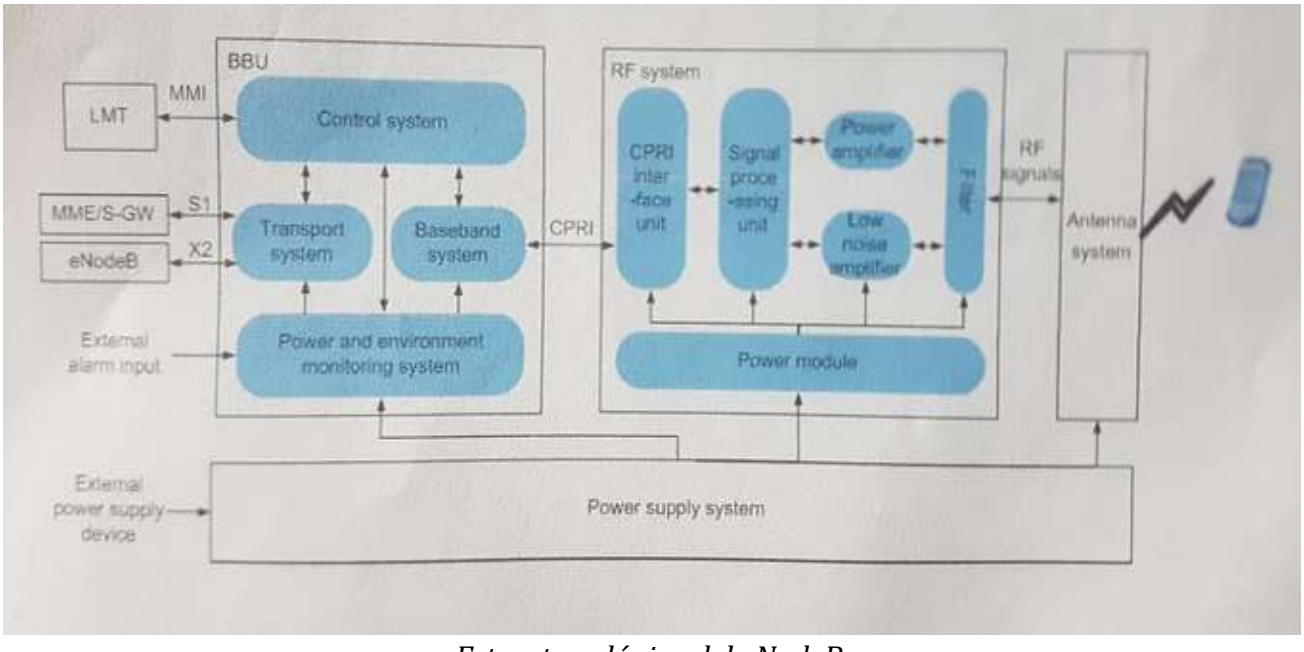


Sistema GUL, nodos e interfaces, S-GW y P-GW pueden ser implementados en un mismo equipo.

Descripción estación base eNodeB

Las estaciones base pueden clasificarse en single o multi-mode de acuerdo con el servicio dado que el cliente necesite para la radio base (2G, 3G, 4G).

Un EnodeB esta diseñado con base en una arquitectura distribuida. Cada radio base consiste en dos tipos básicos de componentes: La unidad de banda base BBU, y la unidad de Radio Frecuencia RF RRU o RRH. Los nombres de estos varian con respecto a los diferentes fabricantes



Estructura lógica del eNodeB.

La BBU (Base Band Unit) inplementa elprocesamiento de señalización, y el manejo de recursos de radio, proporciona los puertos de comunicación entre el eNodeB y el MME y SGW, además de los puertos CPRI (Common Public Radio Interface) para la comunicación entre el BBU y los radios, también los puertos para monitoreo de alarmas.

El módulo BBU se encarga del procesamiento de señal digital en banda base, para después pasar por el puerto CPRI hacia los radios, donde se hace un acondicionamiento de señal, utilizando radiofrecuencia para que la información pueda viajar en la interfaz de aire por medio de las antenas, esto cuando la radio base esta transmitiendo, el proceso inverso ocurre cuando las antenas se encargan de recibir información de los usuarios.

Los RRU's realizan la modulación y demodulación, procesamiento de datos, y amplificación de señales en bandabase y de radiofrecuencia, soporta diferentes anchos de banda para la transmisión.

Centro de Operaciones y herramientas utilizadas

Construir, actualizar y mantener una red celular requiere grandes esfuerzos, requiere sitios celda o radio bases, equipo de switcheo, y conexión a otras redes.

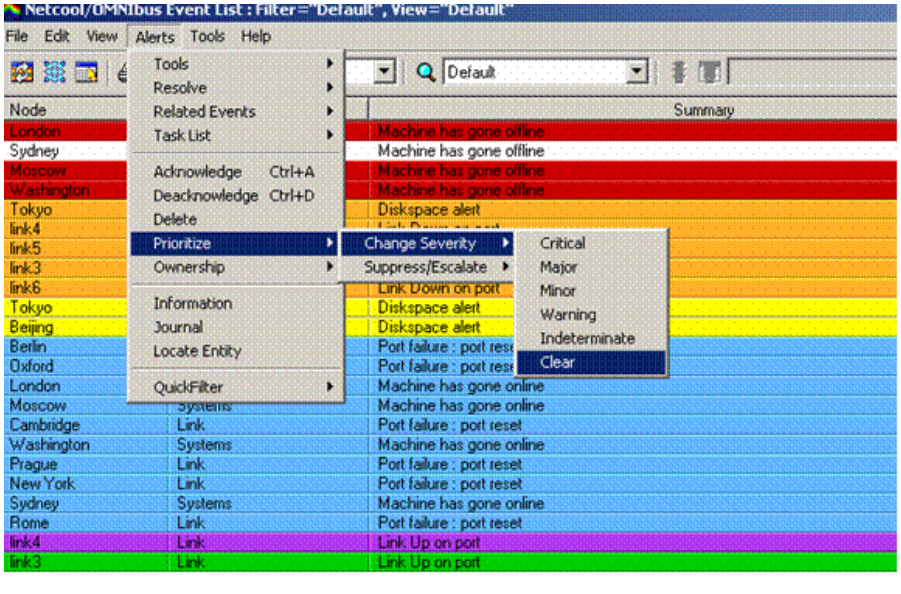
En un centro de operaciones de red se encarga de mantener, monitorear y detectar fallos, esto se realiza mediante una herramienta integrada de gestión de red llamada Netcool, que proporciona supervisión y visualización centralizada y en tiempo real de eventos o incidentes de entornos de red complejos, que pueden superar los millones de sucesos al dia, para mejorar la disponibilidad y eficiencia de la red, creando un diagnostico avanzado.

Netcool cuenta con diferentes filttros de visualización para una mejor gestión e identificación de correlacion de eventos relacionados, para la reducción del tiempo de respuesta.

Podriamos definir una alarma como una indicación de alerta de una condición que puede tener impacto potencialmente negativo en el estado del recurso o servicio monitoreado, mientras que, un evento es un cambio de estado que tiene significancia para la gestión de un recurso o servicio, a su vez, un incidente es una interrupción no planeada del servicio o la reducción en la calidad del mismo.

Una alarma es un poco similar a un evento, de hecho podemos considerar que una alarma siempre es un evento, aunque el caso contrario no siempre es cierto, ya que no todos los eventos son alarmas.

Dentro de Netcool existen diferentes severidades de alarmas indicadas con un código de colores como se muestra en la siguiente figura, cada alarma se muestra con un color diferente según el impacto que tiene:



Código de colores para severidades de alarmas:

Critical – *Rojo*
Major – *Naranja*
Minor – *Amarillo*
Warning – *Azul*
Indeterminate – *Morado*
Clear – *Verde.*

Sin embargo no en todos los casos las alarmas que aparecen en Netcool están en tiempo real, es por eso que para asegurarse, se debe verificar mediante el gestor de elementos de cada provedor, o bien Secure CRT, la cual es una terminal que permite realizar conecciones SSH a los elementos de un swith mediante la dirección IP, y en la cual la interface también difiere entre cada provedor, en esta herramienta se puede acceder en tiempo real al estado de un sitio celda, ver alarmas activas o historiales de alarmas.

Otra herramienta muy importante en un centro de operaciones es la herramienta de creación de tickets de informe, en el caso de Sprint, esta herramienta se llama TRAMS(Ticket Research Analysis and Management Systems).

Dentro del entorno de TRAMS se crean tickets de diferente severidad de acuerdo a el tipo de alarmas que se va a reportar. Cada ticket debe tener un titulo, en el cual se resume información importante acerca del sitio y el tipo de problema que se reporta, asi como notas donde se agrega información mas detallada sobre el diagnostico, y el estado de alarmas completo para su mejor comprensión y mas pronta resolución, se envía a la agencia encargada de solucionar los fallos en la red asegurando una mejor calidad en el servicio evitando lo mas posible la perdida del mismo.

Antecedentes del proyecto:

Para poder explicar los procesos que realizo en el trabajo y su utilidad se deben definir las necesidades del cliente, así como todo proyecto de ingeniería se crea como solución a una necesidad, en este proyecto surge por dos necesidades del cliente, y surge con un grupo de gente en Estados Unidos del estado de Kansas, el cual después fue reubicado a la ciudad de México.

Una de las necesidades fue darle un seguimiento a los cambios que se hacían a la infraestructura de la red, es decir, controlar y monitorear cualquier ejecución de mantenimiento programada para los elementos de red. Ya que no se contaba con un control sobre esto, podrían surgir problemas debido a que no existía alguna agencia o departamento encargado de supervisar estos trabajos, en los cuales surgían afectaciones en el servicio o en la infraestructura directamente debido a malas prácticas o trabajos que se dejaban inconclusos por parte de los técnicos o ingenieros encargadas de realizar los trabajos.

Para evitar este tipo de daños a la red del cliente, se crea la parte de SNTT, la cual se encarga de supervisar los trabajos de mantenimiento así evitando cualquier tipo de alarmas adicionales que pudieran surgir después de haberse realizado un mantenimiento en un elemento de red como una radiobase, y si es que surgieran, notificarlo inmediatamente para afectar lo menos posible el servicio y calidad de la red solucionándolo cuanto antes, ya sea por la misma persona que realizo el mantenimiento o por alguna otra persona calificada para hacerlo.

Otra de las necesidades que existían era tener un control de calidad sobre el equipo adquirido por el cliente, es decir, los componentes que forman una radiobase, como son radios, antenas, tarjetas, etc., por parte de los diferentes proveedores, ya que antes de existir el proyecto, los sitios eran aceptados en la red sin verificación de estado operacional.

Esta parte del proyecto surge para asegurar que el OEM (Original Equipment Manufacturer) entregue un sitio que este funcionalmente en un nivel superior a los estándares del cliente para poder ser aceptado en su red.

Estos estándares tienen que ver con el estado operacional del elemento de red, si es apto para procesar tráfico de voz y datos, si esta dado de alta de manera correcta en la base de datos, si tiene comunicación con los gestores de elementos para poder monitorear cualquier tipo de alerta que se presente, etc,

Si existe algún problema se debe reportar para que el proveedor se encargue de solucionarlo.

Metodología utilizada y contexto de la participación profesional

A continuación explicaré por separado el procedimiento a seguir para las dos partes del proyecto:

Proceso Remote Site Acceptance (RSA)

¿Por qué realizamos RSA?

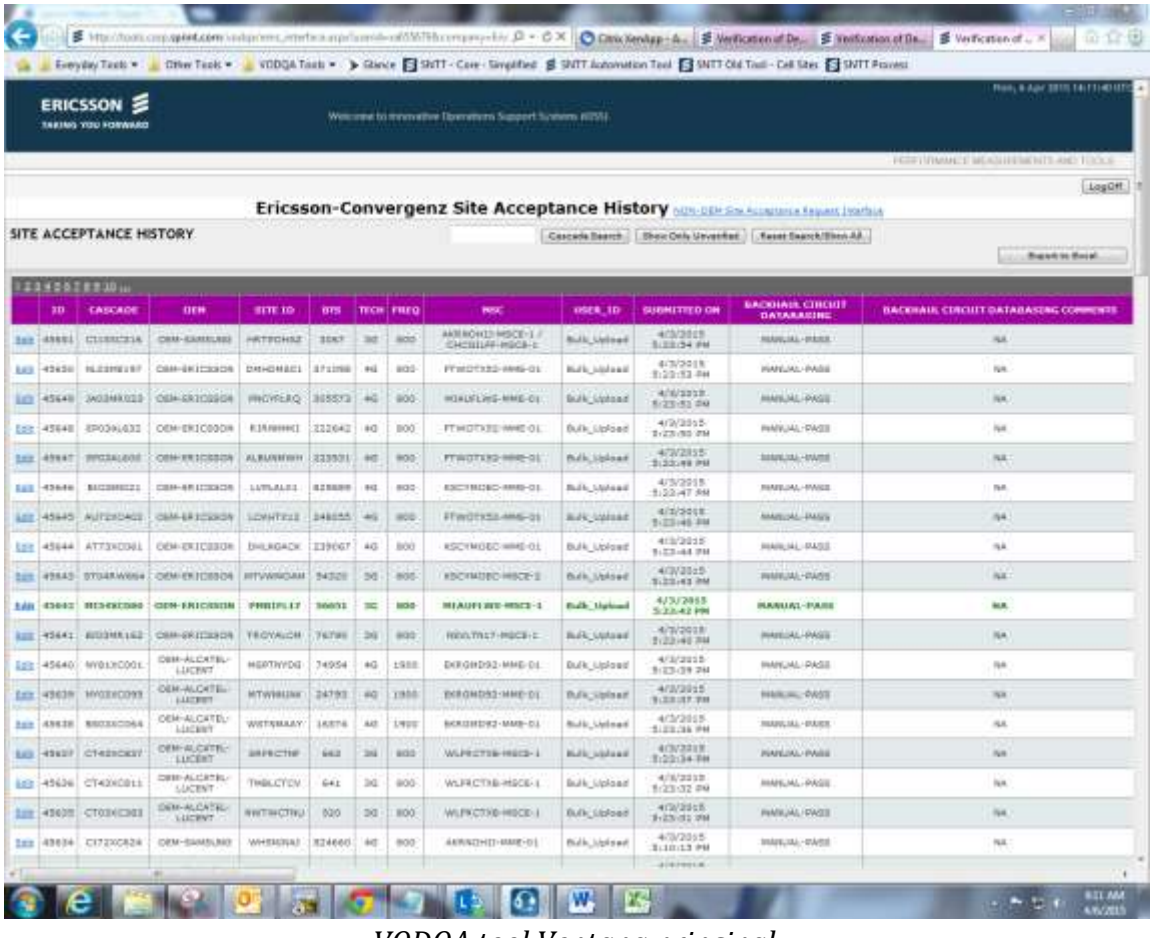
Antes de nuestro equipo, los sitios son aceptados dentro de la red sin verificación de estado operacional.

Este procedimiento es realizado para asegurar que el OEM (Original Equipment Manufacturer) ha entregado un sitio funcionando a un nivel por encima de las normas establecidas por Sprint para poder ser aceptado en su red.

VODQA (Verification of Deployment Quality Automation)

VODQA tool es la herramienta utilizada para registrar la verificación de un sitio, en la cual se verifican seis campos para poder ser aceptado en la red. Cada entrada VODQA tiene un ID único, una entrada VODQA es un sitio dado de alta por el OEM para su verificación en la cual se registrará qué campos cumplen con los requerimientos acordados.

Cada renglón representa una entrada VODQA, para comenzar a trabajar una de estas, selecciono la opción Edit en letras azules subrayadas con lo cual se abrirá en una nueva pestaña cada uno de los campos a verificar y su estado inicial, más adelante explicaré los estados de los campos.



VODQA tool Ventana principal.

Campos en la herramienta

- **ID:** Número ID especifico a una entrada VODQA
- **Cascade Id:** Cascada asociada a una entrada VODQA
- **OEM:** Original Equipment Manufacturer
- **Site ID:** Site ID asociado a una entrada VODQA
- **BTS Number:** Número de BTS asociado con la entrada VODQA.

ID	CASCADE_ID	OEM	SITE_ID	BTS_NUMBER
45660	NY54XC978	OEM-ALCATEL-LUCENT	NYCQNYQC	74055

- **Technology:** 3G o 4G
- **Frequency:** 800, 1900, 2500Mhz
- **MSC:** Ubicación del elemento (Switch)
- **User ID:** Id del usuario que introdujo la entrada VODQA
- **Time Stamp:** Hora en GMT en la cual se introdujo la entrada

TECHNOLOGY	FREQUENCY	MSC	USER_ID	TIME_STAMP
4G	800	EKRGMD92-MME-01	Bulk_Upload	4/6/2015 3:48:44 PM

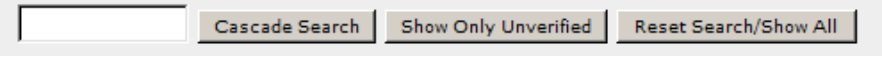
Tipos diferentes de herramientas VODQA

- VODQA NV (Network Vision)
  - Esta herramienta consiste en los sitios de Ericsson, Samsung, y Alcatel Lucent 3G y 4G 800Mhz y 1900Mhz. Esta será la forma más genérica de VODQA tool.

- VODQA 2.5 es el proceso RSA en sitios de 2500 MHz para LTE
  - Esta herramienta consiste en sitios de Nokia, Samsung, y Alcatel Lucent 2.5Ghz
  - Se puede notar que *Ericsson* está excluido en este tipo de VODQA y remplazado por *Nokia*
  - VODQA 2.5 usa casi todas las verificaciones realizadas para NV excepto *"Backhaul Circuit Databasing"* ya que para estos se omite esta parte debido a que para que un sitio tenga 2.5 GHz ya debe tener 1900 MHz y 800 MHz instalado y estos a su vez ya tienen instalado y verificado equipo correspondiente al Backhaul.
  - También se tendrá que hacer una verificación adicional en la parte de configuración la cual es "Golden Parameters" para este proceso, estos son parámetros de configuración con los que deben de contar los sitios para su funcionamiento.

- VODQA Ocean
  - Esta herramienta consiste en todas las nuevas construcciones de sitios en la red (Ericsson, Nokia, Samsung, Alcatel Lucent 3G y 4G 800Mhz, 1900Mhz, y 2500Mhz)
  - Las verificaciones en este proceso reflejan la contraparte en NV/2.5
    Ej.: 4G 1900 Samsung en Ocean es el mismo proceso que 4G 1900 en NV

Los siguientes botones son de gran ayuda para navegar en la herramienta, a continuación se explica su utilidad



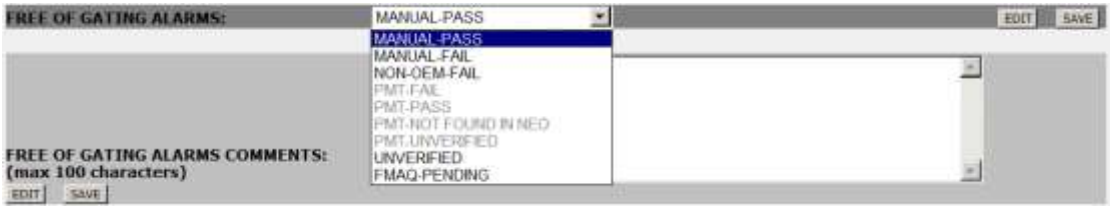
Cascade Search: Se utiliza para buscar una entrada o varias asociadas a un cascade ID de un sitio, es muy útil cuando se requiere localizar una entrada específica trabajada.

Show Only Unverified: Muestra solamente las entradas sin verificar para saber cuáles son las que se tienen que trabajar, una vez que una entrada se acabó de verificar por completo, esta desaparece de esta vista al volver a dar clic en el botón Show Only Unverified indicando que se ha terminado de trabajar dicha entrada.

Reset Search/Show All: Muestra todas las entradas ordenadas por ID de mayor a menor estén verificadas o no.

Edición de campos

Para editar un campo se debe de dar clic en el botón *EDIT* y desplegar el menú que contiene las opciones se tiene que seleccionar de acuerdo si el campo pasa o falla la opción adecuada para posteriormente seleccionar el botón *SAVE*, a continuación explico cada una de estas opciones:



- MANUAL-PASS

Se utiliza cuando cumple con la especificación requerida para ese campo, generalmente no se necesita agregar un comentario cuando se selecciona esta opción solo para casos especiales.

- MANUAL-FAIL

Cuando no se cumple con las especificaciones necesarias, esta es la opción que se selecciona, para esta opción se requiere siempre en la parte de comentarios (máximo 100 caracteres) indicar la causa de la falla, dependiendo de qué campo sea, existe una lista de comentarios estandarizados para esta parte, la cual contiene comentarios para cada campo verificado, esto es importante indicarlo para que el OEM, que se encarga de solucionar estos fallos, sepa precisamente cuál es el error y lo pueda resolver de mejor manera, un ejemplo seria para la parte de alarmas, agregar el nombre de la alarma que está causando que el campo verificado falle, o el error o problema en la configuración, más adelante se explicaran más ejemplos para cada campo.

- NON-OEM-FAIL

Esta opción puede utilizarse cuando algo fallo en la verificación, pero no es algo directamente falla del EOM, generalmente

- PMT-FAIL

La VODQA tool es una herramienta automatizada ya que puede agregar estados a algún campo, las opciones PMT son las asignadas por la herramienta automáticamente, debido a eso no las podemos seleccionar como se muestra en la figura anterior, estas opciones se dan gracias a que la herramienta VODQA tiene comunicación con la NEO Database, que es la base de datos de todos los sitios, y comunicada también con Netcool, por lo que puede saber si puede existir alguna alarma activa para ese sitio, por ejemplo, al ser dado de alta un sitio en la herramienta para su revisión esta asigna un valor pmt si tiene algún tipo de información de algún campo, como puede ser "gating alarms", (más adelante se explican las verificaciones de cada campo), y así determinar si el campo pasa o falla, sin embargo las opciones PMT pueden y en algunos casos deben ser modificadas. En el caso de PMT-FAIL siempre debe ser modificado, puede que la herramienta haya fallado automáticamente un campo, pero debe ser verificado de todas maneras y ser cambiado ya sea a MANUAL-PASS o a MANUAL-FAIL.

- PMT-PASS

Este es otro estado automático de la herramienta, es el único que puede no ser modificado, es decir no seleccionar una opción manual, sin embargo, en algún caso especial (gating alarms) si debe ser verificado y si falla se debe cambiar a MANUAL-FAIL si no es el caso se puede dejar como PMT-PASS o modificarlo a MANUAL-PASS.

- PMT-NOT FOUND IN NEO

Esta es la opción automática que selecciona la herramienta cuando no encuentra información del sitio en la NEO database la cual solo puede estar en los campos donde se necesita información de la base de datos, los cuales son databased correctly y alarm visibility.

- PMT UNVERIFIED

Esta opción automática no nos proporciona ningún tipo de información, y se debe verificar de forma usual para determinar si falla o pasa.

- UNVERIFIED

Esta, a diferencia de la anterior, es la opción manual de un campo sin verificar, cuando algún campo no se ha verificado y se sepa que esta sin verificar.

- FMAQ PENDING

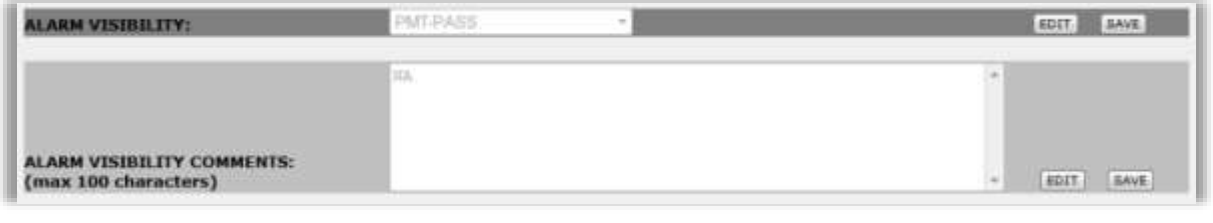
Esta opción solo es válida para el campo de Alarm visibility cuando esta falla, más adelante se explicará su función.

Campos a verificar y por qué

Alarm Visibility (Visibilidad de Alarmas)

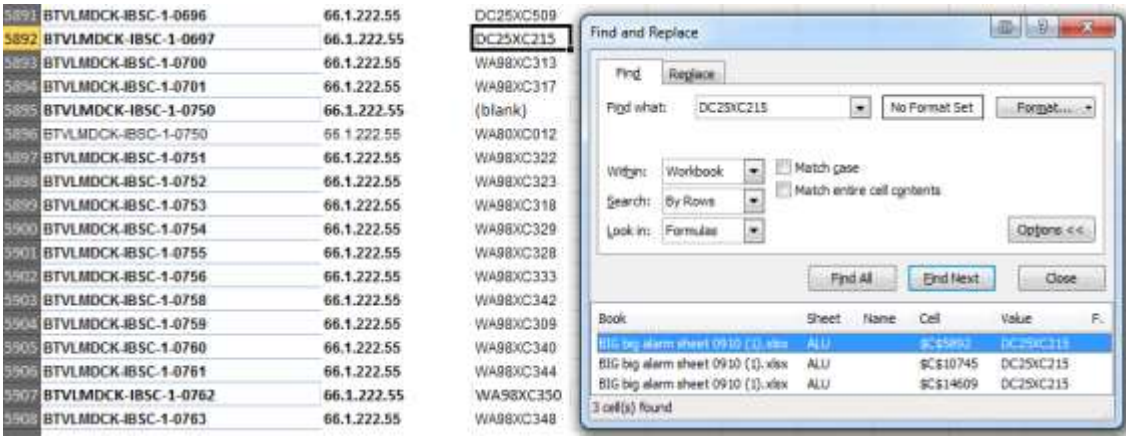
Realizo esta verificación para asegurar que el elemento tenga comunicación con Netcool, esto con la finalidad de que se pueda tener un monitoreo óptimo para este sitio, es decir, si algún problema se presenta y llega a aparecer una alarma sea notificado oportunamente por las herramientas de monitoreo, en este caso Netcool, para su pronto tratamiento y resolución.

Verifico esto revisando una hoja de verificación de alarmas y la herramienta automática VODQA.



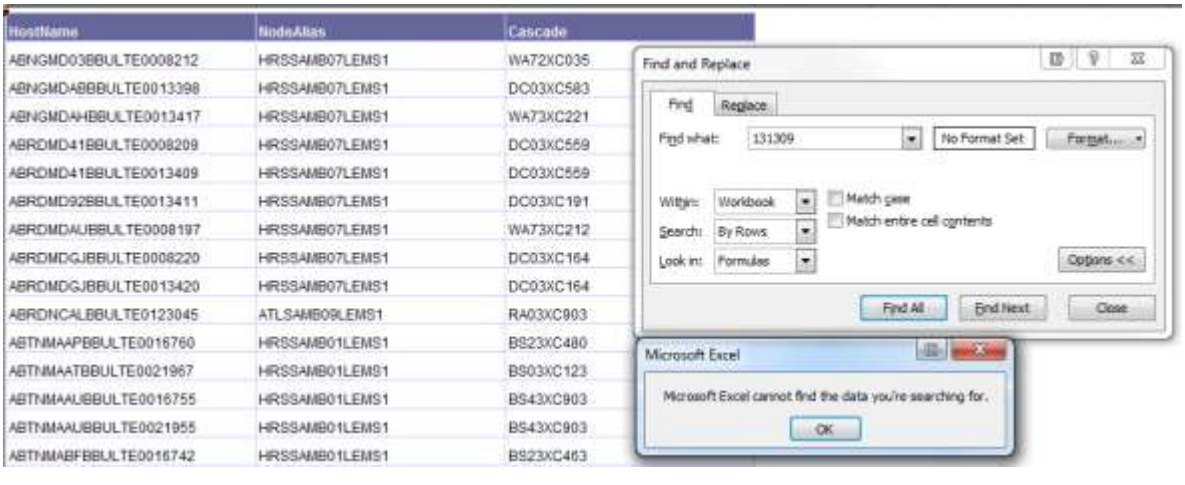
Se cuenta con dos hojas de verificación, una de ellas se actualiza diariamente, la recibimos por correo de parte de gente de Sprint que se encarga de actualizar la lista de sitios que han presentado alarmas y enviándonosla por correo. Para hacerlo presiono la combinación ctrl + F para buscar en todo el libro la búsqueda se realiza por cascada o por site ID o BTS ID ya que en

algunos casos no aparece con la cascada asociada como en la siguiente figura donde para la BTS 750 en la columna Cascade aparece como (blank), si se encuentra el eNodeB o la BTS en cuestión verificando que si corresponde, entonces se considera como pass para el campo alarm visivility, en la siguiente figura se muestra un ejemplo de un sitio encontrado en la hoja de verificación.



En la siguiente figura se muestra un ejemplo de cuando no es posible encontrar un Site ID en la hoja de verificación.

Para estos casos existen otros pasos a seguir para verificar este campo, recordemos que estamos buscando que nuestro sitio tenga comunicación con la herramienta de monitoreo, lo cual se puede verificar mediante otras opciones.

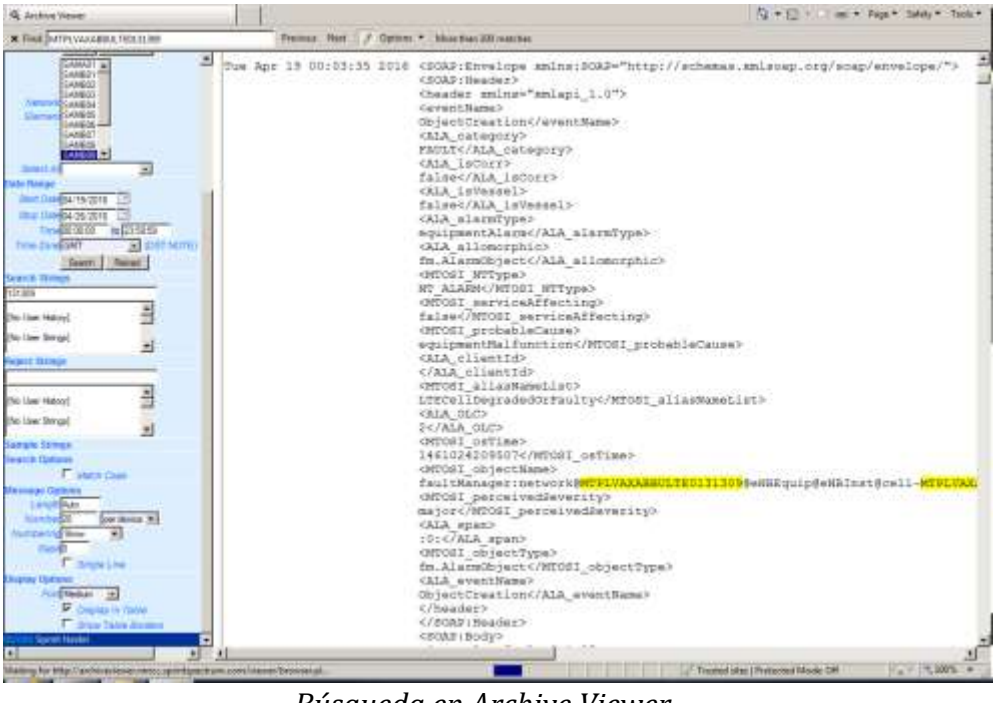


La siguiente opción, después de no encontrar la BTS o eNodeB es buscar directamente en Netcool, de acuerdo a la tecnología y el provedor del sitio con los filtros que tiene netcool, los cuales están divididos en 3G, 4G, y uno para cada provedor, hago una búsqueda parecida a la realizada en la hoja de verificación con la combinación ctrl + F dentro de netcool y buscando ya sea por cascada, site ID o BTS ID, si muestra algún resultado exitoso para la BTS o EnodeB, es decir, Netcool es capaz de mostrar alarmas para dicho sitio significa pass para alarm visibility.

Si aún no tengo éxito con estas dos verificaciones anteriores tengo otras opciones más.

La siguiente opción es buscar entradas previas para ese sitio, si existen y tienen pass para el campo de alarm visibility automáticamente es un pass para la entrada en la que estoy trabajando, por el contrario, si hay entradas previas y se fallaron para alarm visibility o no existe tal entrada previa paso a la siguiente opción de verificación.

Procedo a una más de las verificaciones en caso de que aún no tenga éxito con las anteriores, esta es con una herramienta llamada Archive Viewer donde puedo acceder a registros históricos de datos de alarmas del servidor por switch, buscando por determinado periodo de tiempo alarmas relacionadas a un site ID especifico, en la siguiente imagen se muestra un ejemplo, donde se aparece la fecha de inicio y de fin de la búsqueda, el switch en cuestión y el elemento que se desea encontrar, con la herramienta find busco si en los datos que arroja la herramienta se encuentra algo relacionado al sitio, en la imagen encontré un eNodeB del cual se encontraron datos de alarmas por fechas, también se muestra el número de coincidencias encontradas, con esto puedo asegurar que se puede obtener datos de alarmas de dicho sitio y con el cual obtengo un pass para alarm visibility.



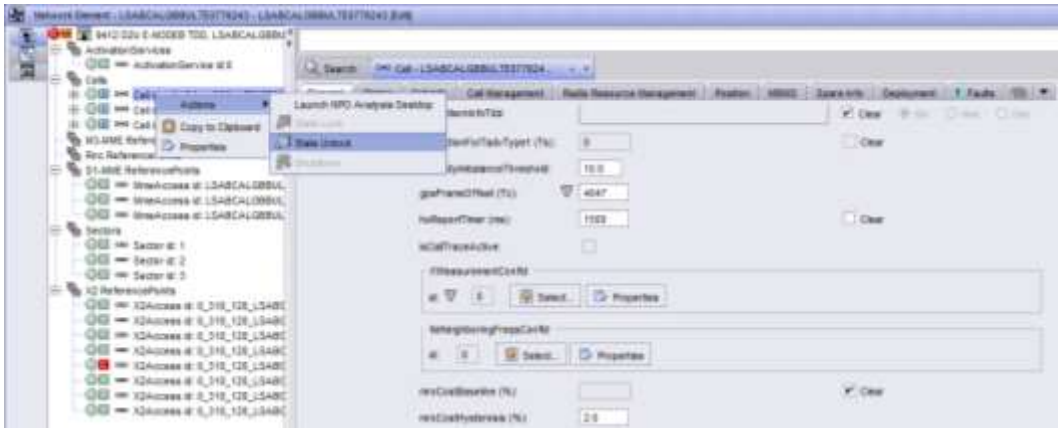
Búsqueda en Archive Viewer.

Este es un caso en el cual se debe de agregar un comentario para este campo indicando que se encontró registro en Archive viewer para ese sitio.

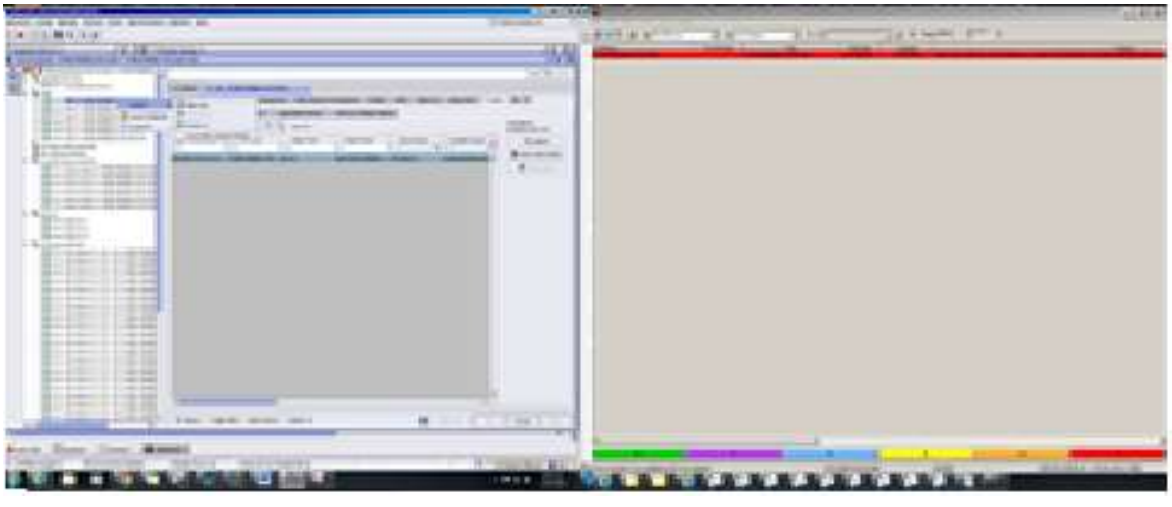
Sin embargo hay casos en los que tampoco es posible encontrar registros en Archive viewer, la siguiente opción solo aplica para sitios que no están al aire aun, es decir, que aún no brindan servicio, ya que se trata de disparar manualmente alarmas desde las herramientas de gestión, no aplica para sitios que ya están al aire debido a que no puedo causar ningún tipo de alarma que afecte la continuidad del servicio en una radio base, si se requiere hacerlo para un sitio que ya este al aire se debo programar una ventana de mantenimiento nocturna para no afectar demasiado el servicio, con esa ventana de mantenimiento obtengo el permiso de Sprint para poder deshabilitar el servicio momentáneamente, asegurando que se restaurará al termino del mantenimiento.

El proceso para disparar alarmas es muy sencillo, generalmente se hace con equipo de ALU para 1900 MHz, 800 MHz o 2.5 GHz , este consiste en bloquear algún radio de uno de los sectores y continuar desbloqueando la celda de ese sector y volviéndola a bloquear aproximadamente 7 veces, esto disparara una alarma critica para ese sector al desbloquearlo, deshabilitándolo y habilitándolo nuevamente, haciendo esto se debe verificar que nuestra alarma aparezca en Netcool con lo que se logra el pass para alarm visibility, al final se debe regresar el sector afectado a su estado inicial, sin alarmas.

Bloqueo del radio del sector Alfa.



Desbloqueo de la celda alfa para generar una alarma crítica.



Alarma disparada y vista con el filtro de Netcool.

Si tampoco se tuvo éxito con este proceso solo queda una opción la cual es crear un ticket de TRAMS porque el Archive Viewer no presenta datos, dicho ticket deberá mandarse a la queue de FMAQ para su resolución, con lo cual el equipo de FMAQ pueda revisar y obtener de otra herramienta algún registro de alarmas de ese sitio y notificárnoslo para poder pasar el VODQA para alarm visibility.

Mientras el ticket es enviado y se espera la resolución debo seleccionar la opción FMAQ PENDING y agregar el comentario "Trams ticket ******* routed to FMAQ. Pending results for Alarm Verification" con el número de ticket en el campo de alarm visibility.

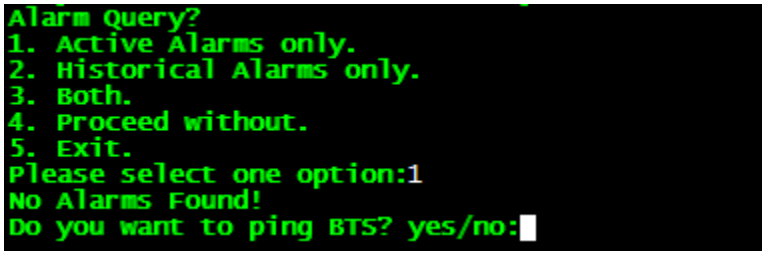
Cuando el equipo de FMAQ regrese el ticket con el historial de alarmas que encontró, verificare si coincide con el site ID y BTS ID correspondiente, si es así cerraré el TRAMS ticket y daré MANUAL-PASS al VODQA para visibilidad de alarmas. En el anexo a se explica con un diagrama de flujo todo este proceso.

Free of Gating Alarms (Libre de alarmas que afecten el servicio)

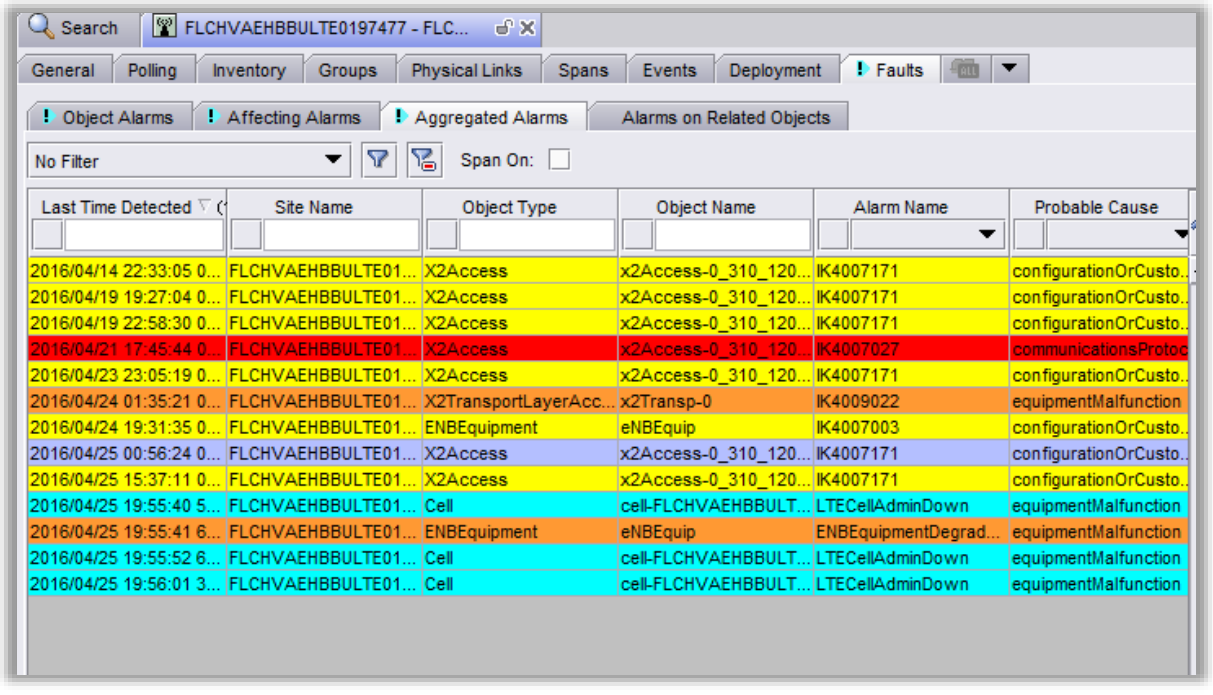
Verifico que el equipo esté libre de alarmas causantes de impacto en el servicio, es decir, que causen una interrupción o afectación en el tráfico de voz o datos.

Esto se verifica obteniendo el estado de alarmas del elemento y comparándolo con la lista de Gating Alarms.

En las siguientes imágenes muestro estados de alarmas de elementos de diferentes proveedores con sus respectivas interfaces:



Alarmas no encontradas para un sitio Ericsson 3g.



Alarmas activas para un sitio ALU 4G.

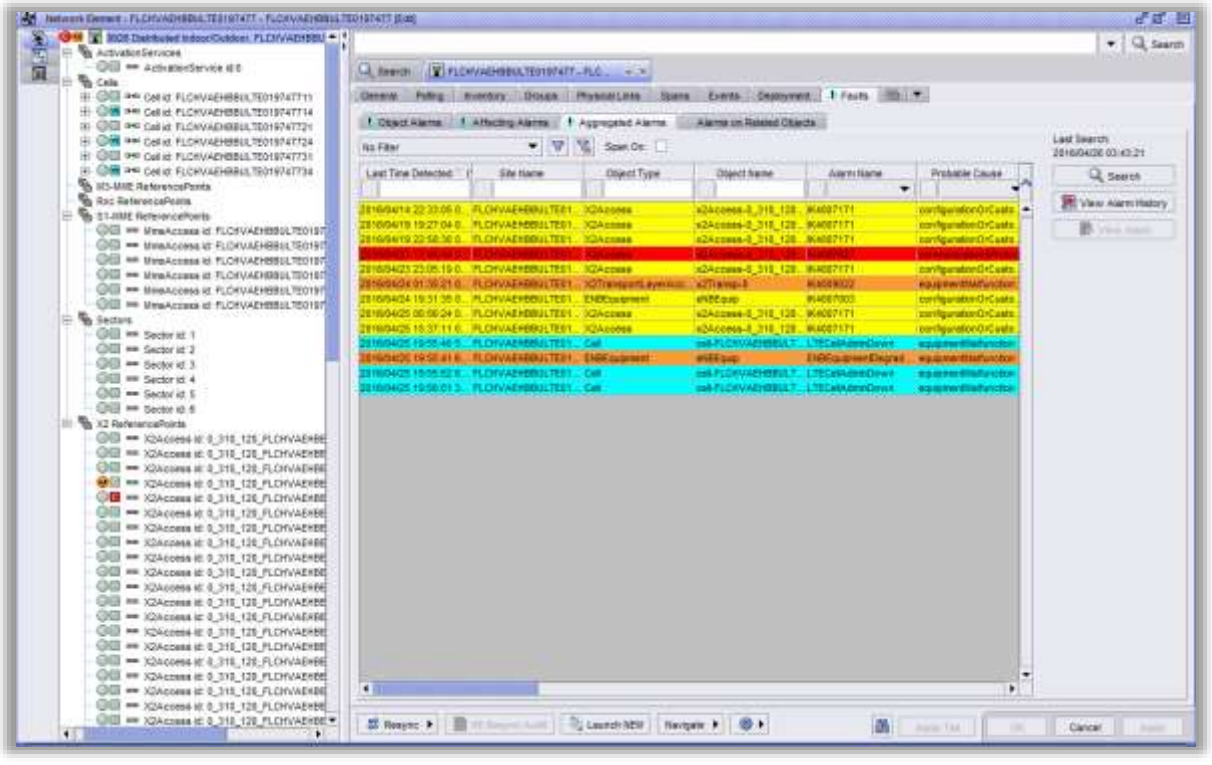
En esta última se muestran alarmas activas, debo revisar cada una para saber si existe alguna alarma que pueda afectar o causar perdida de servicio, para lo cual existe una lista de alarmas clasificadas como gating o no gating en la que busco si alguna alarma es gating o no, realizo la búsqueda con el nombre de la alarma "Alarm name" con la herramienta de búsqueda en la hoja de Excel de la lista de alarmas, si no encuentro la alarma en cuestión o aparee como NON-Gating significa que no hay problema con esa alarma y procedo a seleccionar MANUAL-PASS.

Por el contrario, si esta alarma aparece como gating entonces es una alarma que puede afectar al servicio, si este es el caso busco en la lista de excepciones si esta alarma corresponde a alguna de las excepciones propuestas por cada OEM.

Cada OEM cuenta con su propia lista de excepciones, entre las cuales se encuentran alarmas NON-Gating o alarmas causadas por algún estado administrativo de un sitio como por ejemplo ENBEQUIPMENTADMINDOWN una alarma causada cuando un equipo aun no es puesto al aire y se deja abajo o down a propósito.

Si la alarma encontrada es gating, no se encuentra en la lista de las excepciones y además el sitio NO está al aire aun para la frecuencia que estoy trabajando entonces se falla el campo alarm visibility, en cualquiera de los casos agrego las alarmas activas en los comentarios del campo.

Si un sitio ya se encuentra al aire, automáticamente pasa por gating alarms y por configuración aunque tenga alarmas activas o que falle algo en la configuración, esto es debido a que al estar un sitio ya al aire, este ya es responsabilidad directa de Sprint en cuanto a alarmas y se deberán de trabajar por gente de campo de Sprint directamente, ya no será responsabilidad de OEM, recordemos que estas verificaciones se hacen con relación a fallas que son responsabilidad de los EOM y que solo ellos pueden corregir.



Alarmas activas para un sitio ALU LTE.

Databased Correctly (NEO Databasing) (Dado de alta de manera correcta en la base de datos)

Después de verificar la visibilidad de alarmas para un sitio donde se verificó que si aparece alguna alarma esta sea visible con las herramientas de monitoreo para su pronta resolución ahora verificaré que se pueda abrir un ticket para reportar alguna alarma que se pueda presentar, esto lo hacemos directamente en TRAMS.

Verifico que este dada de alta correctamente la información de este sitio en la "neo database" que es la base de datos que utiliza Trams para obtener la información de un sitio. Así como TRAMS, muchas de las herramientas obtienen la información de los sitios a través de la *neo database* como Netcool, por eso es importante verificar que este dado de alta de manera correcta.

En esta verificación veo si el sitio tiene IPA (IP Aggregator) Backhaul dado de alta en TRAMS y si se muestra el número de ENodeB / BTS proporcionado por OEM a través de la VODQA tool.

La herramienta automática PMT compara con la base de datos de NEO, si encuentra el sitio, será PMT-Pass, si no es capaz de identificar todos los componentes será PMT-Fail, en este último caso se deberá revisar manualmente desde Trams si es posible crear un ticket para tal sitio (que este dado de alta correctamente) y se pueda crear un ticket para Backhaul.

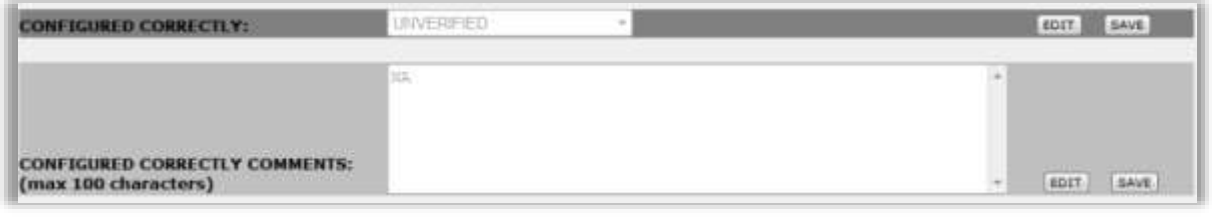
Realizo una búsqueda de elementos con la cascade ID, se mostrará una lista de los elementos de dicha cascada y se deberá buscar la parte de Backhaul del sitio indicada como "BHRS", y que la BTS o eNodeB ID este listada, si se encuentran ambas partes se pasa el campo Databased Correctly, de lo contrario lo fallo indicando en los comentarios la parte faltante.

Configured Correctly (Configurado correctamente)

En este campo verifico lo siguiente:

- Estado operacional y administrativo del equipo
- Software más actualizado
- Configuración de RRH's, RET's, tarjetas, etc…
- Golden Parameters (Solo para 2.5 GHz)

Esto lo verifico a través de los gestores de elementos de cada tecnología.



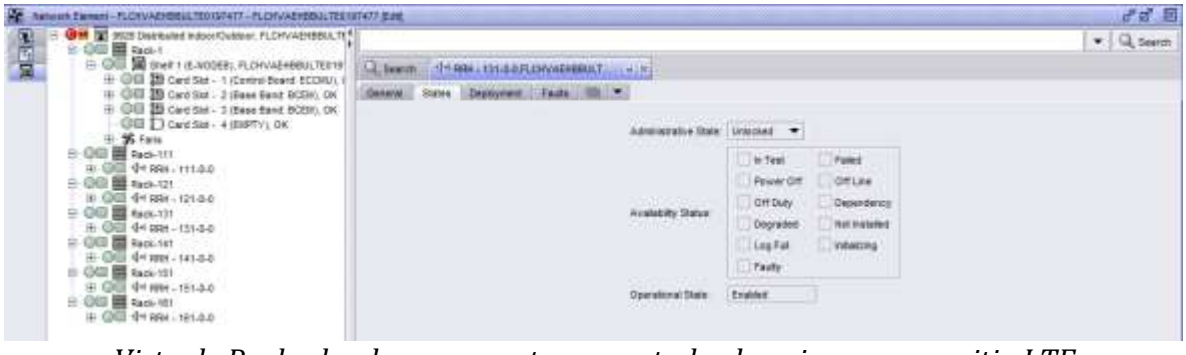
En la siguiente figura se muestra el estadio operacional y administrativo de un radio RRH (Remote Radio Head), el estado administrativo puede ser locked o unlocked (bloqueado o desbloqueado), y el estado operacional puede ser enabled o disabled (habilitado o deshabilitado), la diferencia entre estos dos estados es que solo uno de ellos se puede modificar manualmente, este es el estado administrativo, se puede bloquear o desbloquear un sector por ejemplo dando click derecho en la RRH del sector en cuestión y seleccionando ya sea locked o unlocked, a diferencia del estado operacional el cual no puede ser modificado, es propio del equipo, si está en buen estado o no.

El estado administrativo puede ser modificado bloqueado en todos los sectores en el caso que el sitio aún no se encuentre al aire, o cuando alguien realiza un mantenimiento y se necesite bloquear alguno de los sectores a la vez.

Si el estado administrativo es bloqueado, el estado operacional debe ser deshabilitado, y si el estado administrativo es desbloqueado, el estado operacional debe ser habilitado.

Por lo anterior, la única combinación de estados que causaran una falla será cuando el estado administrativo sea Unlocked y el estado operacional sea Disabled, lo que significa que, al

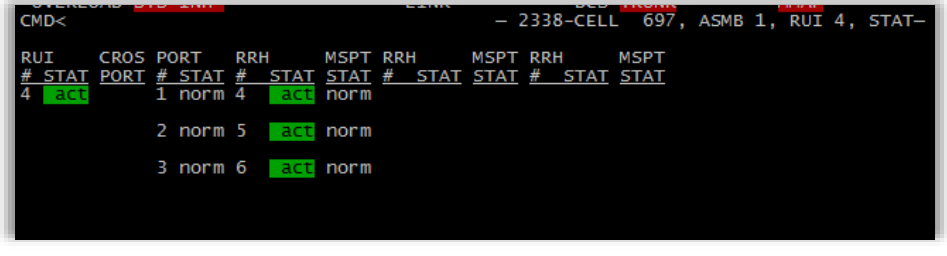
desbloquear administrativamente, el estado operacional debe ser habilitado automáticamente, si no es así entonces el equipo está dañado y tiene que ser reparado ya que no podrá ser capaz de procesar tráfico.



Vista de Racks donde se encuentra conectado el equipo para un sitio LTE.

En algunos casos también debo verificar que se encuentren montadas las tarjetas de control y de banda base, como se muestra en la figura anterior en el Rack 1, ya que sin estas tarjetas no es posible el procesamiento de las señales, lo que causaría un Fail en la configuración.

En la siguiente figura se muestra otro ejemplo de estados de RRH de la verificación de configuración para un sitio 3G, cuando una RRH se encuentra fuera de servicio se muestra en la parte de STAT subrayado en rojo con letras blancas OOS (Out of service) con lo que fallaría la configuración, también es importante identificar cuales RRH's corresponden a la banda de frecuencia que estoy trabajando 1900 MHz, 800 MHZ o 2.5 GHz.



Estado de RRH's para un sitio 3G ALU.

También existe el caso en el que solo tenga dos o una RRH montadas, en cuyo caso debo de verificar con cuantos sectores está configurado el sitio, puede que sea un sitio de solo dos sectores o solo un sector como puede ser una small cell o un DAS que son sistemas indoors o para interiores, montados generalmente en casas, edificios o supermercados, lugares donde la demanda de usuarios es mucha y donde se necesita mayor cobertura y rendimiento.

Si se confirma el número de sectores con en el número de RRH's la configuración es la correcta, de lo contrario causará un Fail.

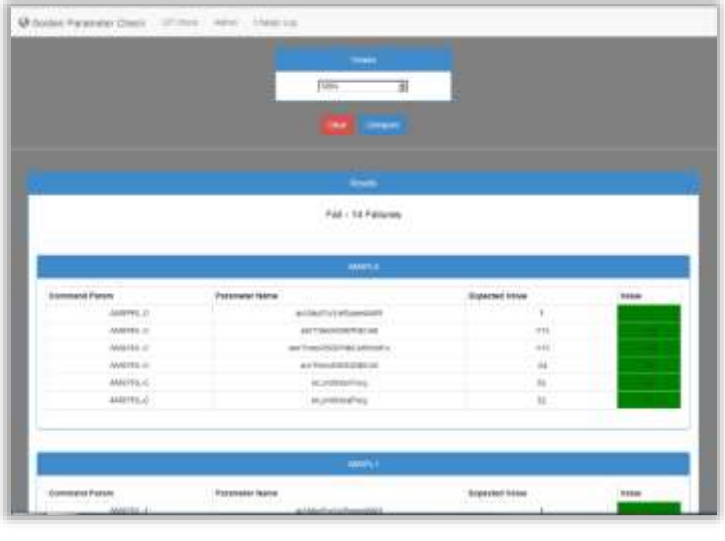
Ejemplo de verificación de un sitio que cuenta con un solo sector.

El siguiente paso, uno de los más importantes es revisar el software cargado, el cual debe ser el más actual, para verificarlo se tiene una hoja emitida por sprint con la lista de software organizador por tecnología y con fechas de periodo de gracia, la cual se actualiza cada día, contiene las versiones de software que se debe tener cargada en un sitio, si la versión cargada no coincide con la indicada en el documento entonces fallará la configuración.

La última verificación es (Golden Parameters) solo aplica para sitios LTE de la banda de 2.5 GHz.

Para realizarlo debo correr un archivo con una serie de comandos desde la interfaz de comandos, estos comandos se ejecutan uno tras otro verificando parámetros de LTE como, niveles de interferencia, estados de equipo, entre muchos otros, al terminar de ejecutar todos los comandos copio los resultados y los pego en una herramienta llamada Golden Parameter Check, la cual se encargará de comparar valores esperados de dichos parámetros con los valores obtenidos de la ejecución de los comandos.

Si todos los valores obtenidos coinciden con los valores esperados, la herramienta muestra cero fallas en los parámetros, de lo contrario muestra el número de fallas marcadas en rojo en la lista de parámetros, en la siguiente figura se muestra un ejemplo de verificación de parámetros.



Verificación de parámetros Golden con fallas.

Al dar click en el botón *Compare* después de haber pegado los resultados de la ejecución de comandos saldrán los resultados de la comparación con el número de fallas y la lista de parámetros comparados indicando los valores esperados y los valores obtenidos, mostrando las fallas sombreadas en rojo.

En el menú de selección *Vendor* se puede elegir entre *NSN (Nokia Siemens Network)* o *Samsung* de primero o segundo carrier, ya que también reviso entradas VODQAS correspondientes al segundo carrier, en los cuales lo único diferente es esta parte de *Golden Parameters*, donde se ejecutan comandos solo para comparar la configuración del segundo carrier.

Si no aparecen fallos en los parámetros, entonces significa que los parámetros son los correctos, si no fallo el campo de configuración agregando los parámetros que fallaron en los comentarios del campo.

Al haber terminado todos los pasos anteriores para este campo, este solo pasara si todas y cada una de las verificaciones de los pasos anteriores pasó, es decir, si alguna de esas verificaciones falló, entonces fallo el campo *configured correctly* agregando en los comentarios la parte de configuración que falló.

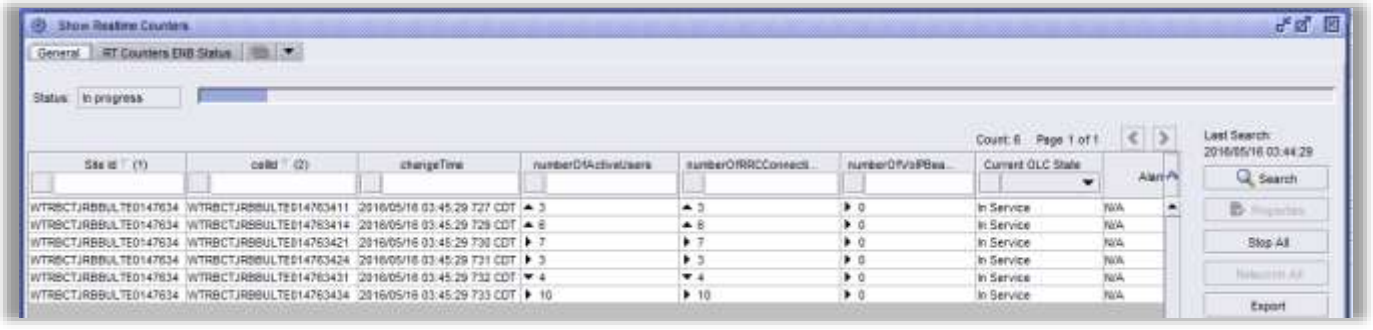
Igual que en el caso de *gating alarms*, si un sitio ya está al aire, automáticamente pasa para configuración, aunque se tengan fallas, la razón de esto se explicó en la parte de *gating alarms.*

Calls/Data Processing/In service (Procesamiento de voz y datos)

En este campo se verificará la habilidad del sitio de procesar tráfico. Esta categoría casi siempre pasa. Debido a la manera de operar del proceso, cada problema o falla en un sitio solo puede ser registrado en una categoría.

Si hay una falla que pueda impactar el procesamiento de voz o datos, la puede ya haber registrado en otra categoría y no ser duplicada en *Data Processing*.

Con el procesamiento de llamadas, tengo que confirmar si hay un problema de bloqueo de llamadas si no veo procesamiento de tráfico, un sitio puede no tener llamadas activas, pero ser completamente funcional, por ejemplo, si no se encuentra aún al aire, en esta situación no puedo fallar el campo. En la siguiente figura se muestra un ejemplo con usuarios activos por sector para un sitio LTE 800/1900 MHz.



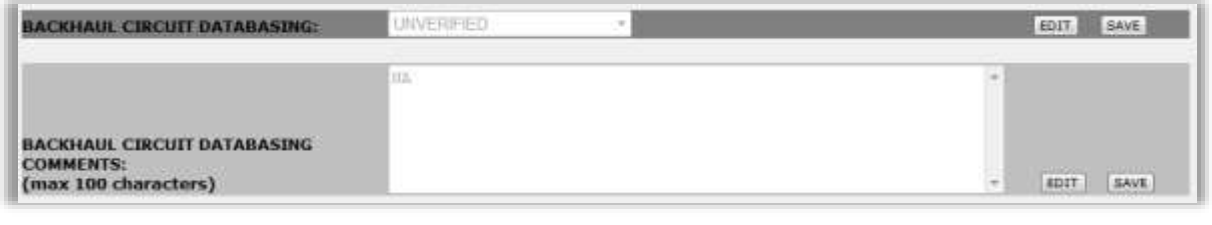
Usuarios activos para una radio base de LTE 800/1900MHz.

Sin embargo, si hay un problema que cause bloqueos o caídas en las llamadas, usualmente es relacionado a alguna alarma de hardware, en cuyo caso solo puede fallarse en una sola categoría, ya sea *Free of Gating Alarms* o *Configured Correctly*. En estas categorías, si existe algo que pueda evitar que el sitio opere correctamente puede ser clasificado como FAIL.

Hay muchos ejemplos de qué es aceptable y qué no lo es, es aquí donde debo usar mi mejor criterio profesional o referirme a algún compañero para asistencia o aclaración y tomar la decisión más acertada.

Backhaul Circuit Databasing (Comprobación del circuito de Backhaul en la base de datos)

En esta categoría verificaré la posibilidad de crear tickets relacionados con backhaul, revisando que el circuito de Backhaul se encuentre en la base de datos.



Esto se verifica buscando en las hojas de cálculo de reportes de Backhaul para Sprint RSA, esta hoja es enviada diariamente al correo de RSA.

Una vez que tenga la hoja de cálculo, con la herramienta find <Ctrl+F> busco la cascada, el sitio se mostrara seleccionado si se encontró alguna coincidencia en el archivo, como se muestra en la siguiente figura.

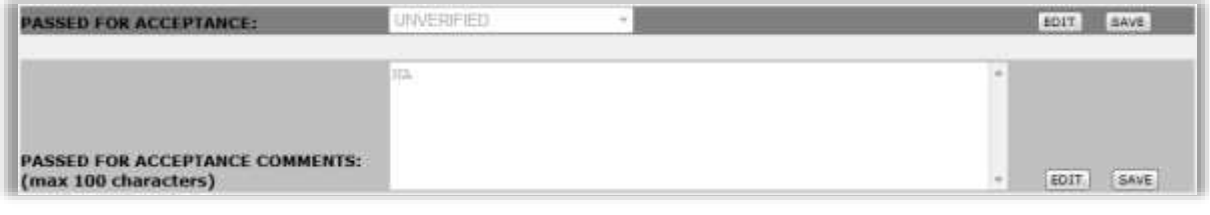
• Si la cascada se encontró listada en el informe de Sprint RSA BH, el sitio sería aprobado para la categoría de "backhaul Circuit databasing"

• Si la cascada no se encontró en el informe de Sprint RSA BH, el sitio se fallaría para "backhaul Circuit databasing" con el comentario correspondiente.

Passed For Acceptance (Pase de aceptación)

Esta es la verificación general de la entrada VODQA para el sitio, si hay algún comentario en los campos fallados, tendrán que ser combinados en la sección de comentarios de este campo general, si algún campo falló entonces fallara toda la entrada VODQA, con los comentarios correspondientes, cambiando este campo a MANUAL-FAIL.

Todos los campos deberán haber sido PASS para que este campo sea cambiado a MANUAL-PASS.



Verificación completada

Después de que he completado la verificación de los pasos cualquier cosa listada en la herramienta VODQA como PMT-FAIL o MANUAL-FAIL será proporcionado de nuevo a la OEM, lo cual pueden ver a través de su propia interfaz utilizándola herramienta VODQA. El OEM es entonces responsable de corregir el problema (s) listado(s).

Una vez que el OEM los haya completado entonces tendrán la posibilidad de volver a presentar una solicitud para que el sitio se compruebe de nuevo. Se debe tener en cuenta que una vez que el OEM ha vuelto a presentar una solicitud, sólo deberá ser necesario comprobar los campos que figuraban originalmente como PMT-FAIL o MANUAL-FAIL. Sin embargo, si se nota algo que estaba en la lista original como PMT-PASS o MANUAL-PASS y algo nuevo se encontró entonces la sección debe ser actualizada y aparece como MANUAL-FAIL y enumerar un comentario que describe por qué ha fallado

Proceso SNTT (Sprint Network Touch Tracking)

Esta parte del proyecto está dentro del proceso de *Change Management* o gestión de cambio el cual es responsable de controlar los cambios en la infraestructura del cliente, con el objetivo de asegurar que cualquier modificación necesaria a la red sea hecha de manera correcta, siguiendo procedimientos y resultando en mínimo o ningún impacto en el servicio al usuario final.

La autorización para comenzar una ejecución de cambio y su monitoreo es realizado como parte de las actividades de 1er Nivel de Aseguramiento de Actividades de Apoyo, dentro de la función de servicio de 1er nivel de operaciones.

Esta gestión se aplica a eventos de mantenimiento realizados por ingenieros o técnicos de campo de los diferentes OEM o por gente directamente de sprint a los elementos de la red en una o múltiples radio bases.

El control de entrada y salida de técnicos de campo se hace mediante una herramienta automática llamada SNTT Automation Tool, en la cual registro manualmente check-ins y check-outs, al inicio y al final del mantenimiento respectivamente.

La persona que llama para realizar un check-in inmediatamente antes de comenzar a trabajar o realizar cualquier cambio en la infraestructura de la red es responsable de cualquier alarma que acurra mientras realiza trabajo en la radio base, esto para asegurar que el sitio este en el mismo estado, o idealmente mejor que cuando comenzaron las actividades del mantenimiento.

Si hay alguna alarma en el sitio después de recibir la llamada de check-out por parte del técnico, se le dará una oportunidad para resolverla, si no es posible arreglarla entonces el check out seria fallido o FAIL y será reportada a Sprint vía la creación de un TRAMS ticket.

Si no se realiza un check-out después de que el trabajo se completó, se considerara como non-compliant o sin cumplimiento, seguido de un correo enviado a las partes apropiadas dentro de las organizaciones de OEM, la empresa y el cliente.

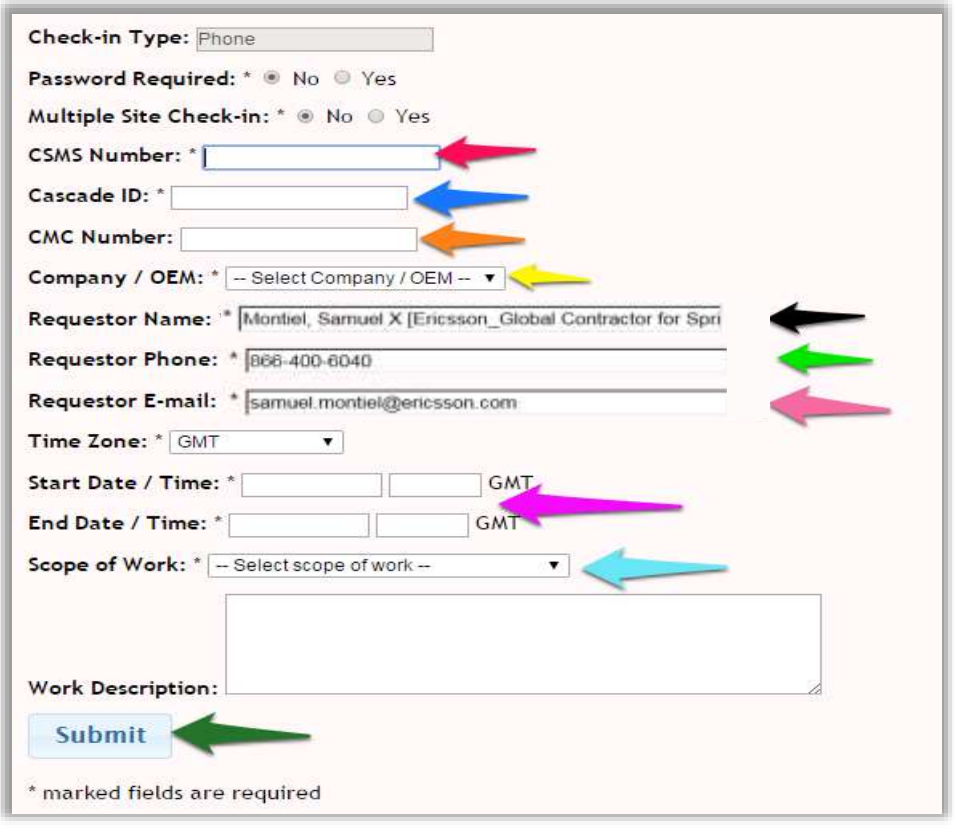
Para que se pueda llevar a cabo este proceso, cualquier cascada de una radio base a la que se le dará mantenimiento se debe documentar requiriéndose un ticket CSMS (Cell Site Maintenance Scheduler), la herramienta donde se programan los eventos de mantenimiento, para prevenir que

el NOC (Network Operations Center) vea alguna alarma en el sitio debido a la actividad de mantenimiento, si no es creado un CSMS ticket, no habrá supresión de alarmas y el personal de monitoreo de alarmas podrá ver la alarma y tomar acción, lo cual no es deseado ya que como se mencionó antes, cualquier tipo de alarma generada durante la ventana de mantenimiento es responsabilidad de la persona que realiza el mantenimiento y es la misma que tiene que repararla, más adelante se explicara a detalle este proceso.

Proceso de registro de entrada (Check-In)

Antes de contactar a SNTT y comenzar con el proceso de check in, debe existir un ticket u orden de trabajo CSMS/CMC (Change Management Control) abierto y aprobado para la fecha en que se realizara el mantenimiento, importante, solo puede haber una actividad a la vez en un sitio, es decir, no podrá haber múltiples CSMC válidos para el mismo sitio al mismo tiempo.

Para comenzar el trabajo de mantenimiento, el implementador debe contactar al equipo de SNTT por teléfono o vía email para solicitar un check in, debe proporcionar un CSMS válido, la cascada asociada, la información de contacto, nombre completo, número de teléfono y correo electrónico, y la actividad que se va a realizar, a continuación, el formato a llenar para el registro (Check-In Data Entry) dentro de la SNTT automation tool.



CHECK-IN Data Entry.

Check In Type: Tipo de Check In procesado.

Phone – Solicitado por teléfono.

Web – Solicitado manualmente por la persona que realiza el mantenimiento desde la aplicación web con un dispositivo móvil.

Password Required: Si la persona requiere una contraseña de acceso a herramientas para trabajar de manera remota.

Multiple Site Check In: Si el individuo realizara mantenimiento en múltiples sitios a la vez.

CSMS Number (Flecha roja): Este número lo obtengo del técnico de campo, debo verificar la validez del ticket y su vigencia, así como comparar este número con la cascada proporcionada los cuales deben de coincidir, de no cumplirse esto o no contar con este número, debo pedir al técnico solicite un número valido, vigente y correspondiente a la cascada en cuestión.

Cascade (Flecha azul): Introduzco la cascada correcta en este campo.

CMC Number (Flecha naranja): Este número aplica solo para Golden BTS's (sitios con la prioridad más alta P1) y solo cuando el trabajo a realizar tendrá un impacto en el servicio al usuario, este número debe ser obtenido del técnico, si no cuenta con él, deberá solicitarlo con su manager y volver a llamar.

Company / OEM (Flecha amarilla): Compañía/OEM para la que trabaja el técnico, al dar click se despliega un menú de opciones (Ericsson, ALU, Samsung, Sprint).

Requestor Name (Flecha negra): Nombre y apellido del técnico.

Requestor Phone Number (Flecha verde claro): Número de teléfono del técnico en caso de haber necesidad de contactarlo.

Requestor E-mail (fleche rosa): Correo electrónico del técnico, al cual se le enviará automáticamente un correo de notificación al realizar el check in.

Time Zone: Se puede seleccionar de entre 7 diferentes zonas horarias de un menú desplegable, por defecto se utilizará la Hora Media de Greenwich (GMT).

Start Date / Time (Flecha Morada): Hora a la que el técnico comenzará el trabajo.

End Date / Time (Flecha Morada): Hora a la que el técnico terminará el trabajo.

Scope of Work (Flecha azul cielo): Este es el tipo de trabajo que realizara el técnico, se mostraran algunas opciones en el menú, si se trata de una actividad diferente de estas se debe agregar una pequeña descripción en la parte de *work description*.

Submit Button: (Flecha verde obscuro): Este botón va a evaluar el check in y avisar al usuario mediante una ventana emergente si el check in pasa o falla y la razón por la cual está fallando si es el caso.

Al haber registrado la entrada del técnico exitosamente en la herramienta, esta manda un correo de confirmación automático a la dirección de correo indicada en el campo correspondiente con la información del sitio, la duración de la ventana de mantenimiento y un ID único que será el número de referencia para realizar posteriormente el check out, este número es el SNTT ID.

Además, la función automática de la herramienta toma un registro del estado de alarmas del sitio en ese momento de Netcool para después compararlas al momento de hacer el check out, idealmente debe ser menor el número de alarmas que había al momento de hacer el check in, antes de comenzar su trabajo.

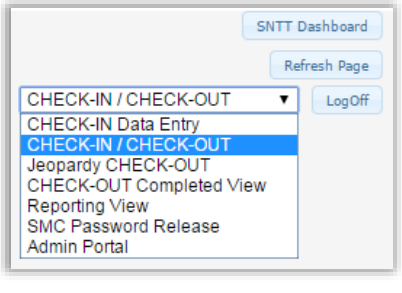
Es importante destacar en este punto que existen días del calendario durante los cuales no está permitido realizar cualquier tipo de mantenimiento en ciertas radiobases o en cualquier equipo físico ya sea local o remoto los cuales son llamados "MAINTENANCE FREEZE", estos se realizan en eventos de especiales como el superbowl, partidos de baseball, carreras de Nascar o en fechas importantes en los Estados Unidos, como el día de la independencia o el día de acción de gracias, etc. Se realizan a lo largo de todo el año ya sea a nivel nacional o en ciertas regiones del país, esto para restringir cualquier tipo de trabajo que pueda afectar el rendimiento de la red y entregar el mejor servicio posible durante esas fechas, por lo que no se permite la entrada al técnico a un sitio para estos casos.

Proceso de registro de Salida (Check-Out)

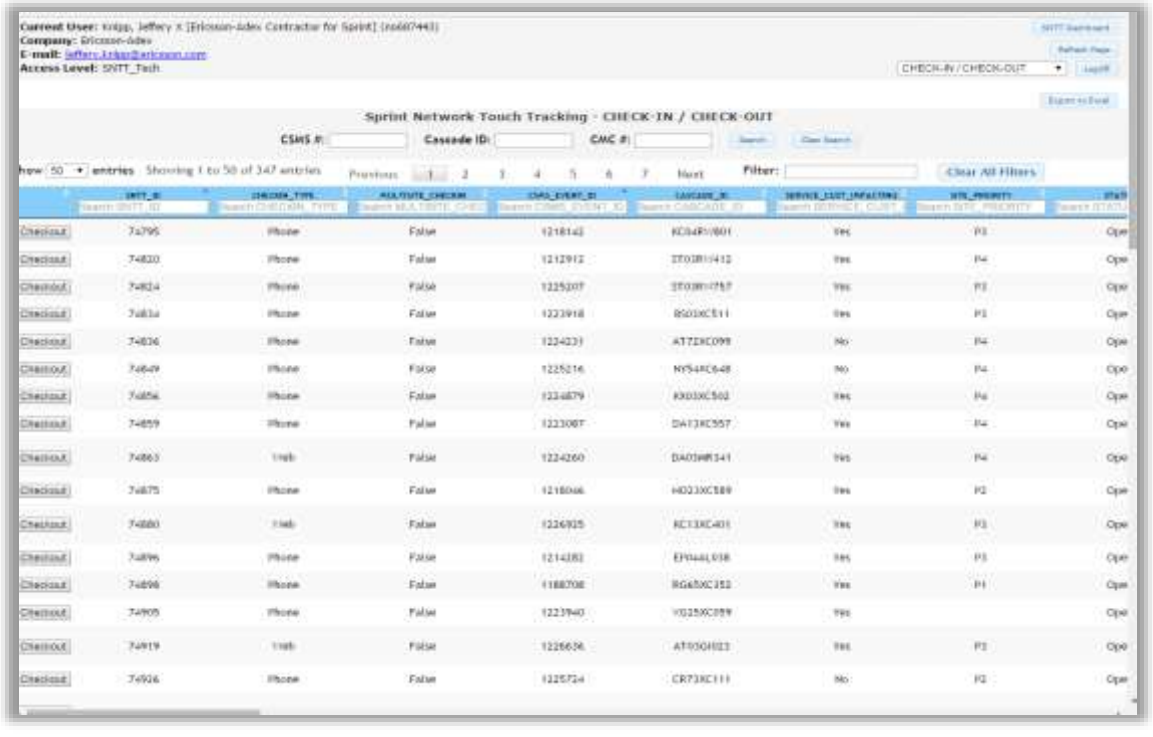
Después de completado el trabajo programado y/o antes de dejar la ubicación física o después del termino de un trabajo remoto, el implementador de cambio tiene que registrar su salida a través del equipo de SNTT.

Página Check-In/Check-Out

La primera página a la cual ingreso en el proceso de Check-out o registro de salida es la página "Check-In/Check-Out", a la cual se accede seleccionando "Check-In/Check-Out" del menú desplegable de la esquina superior derecha de la "sntt automation tool".

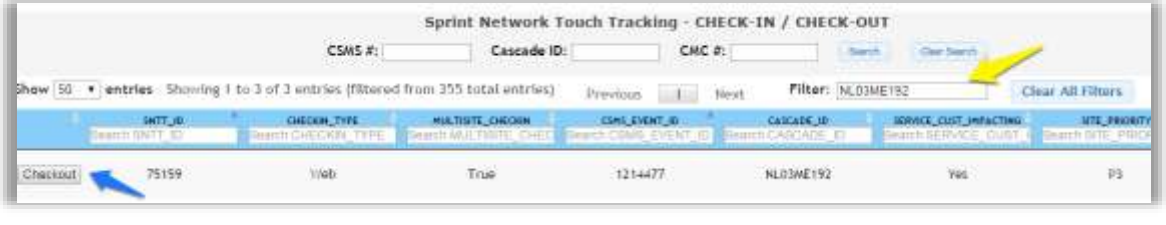


En esta vista se encuentran todos los check ins que se han hecho en el día con toda la información de los mismos, como se muestra en la siguiente figura.



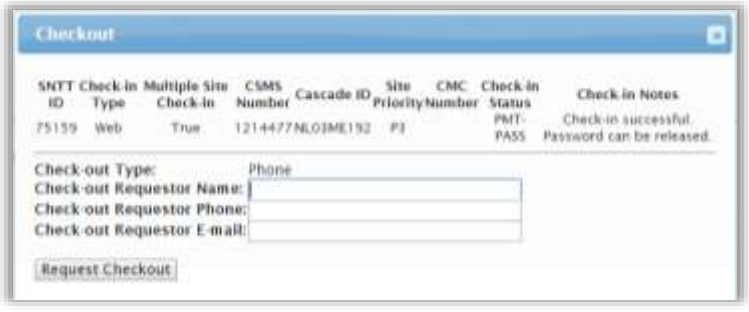
Ventana principal "Check-In/Check-Out".

Al momento que el técnico contacta a SNTT para solicitar un check out, el trabajo debe estar terminado y le solicito alguna referencia para encontrar su registro en la anterior ventana filtrando la información proporcionada, esta referencia puede ser cascada, SNTT ID, CSMS, CMC o cascada, también tengo la opción de buscar por cualquier campo escribiendo una palabra clave en el campo "*Filter*".



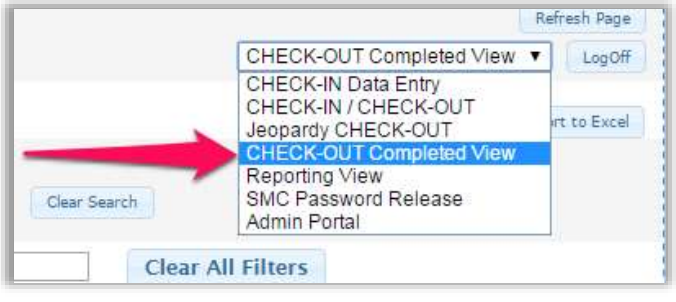
Una vez encontrado el "SNTT ID" correspondiente, corroboro la información del técnico, así como la del sitio, que sea la cascada y CSMS correspondientes, habiendo hecho esto doy clic en botón "Checkout" localizado a la izquierda de cada entrada.

Aparecerá una ventana emergente donde lleno la información necesaria del técnico que solicita su salida.

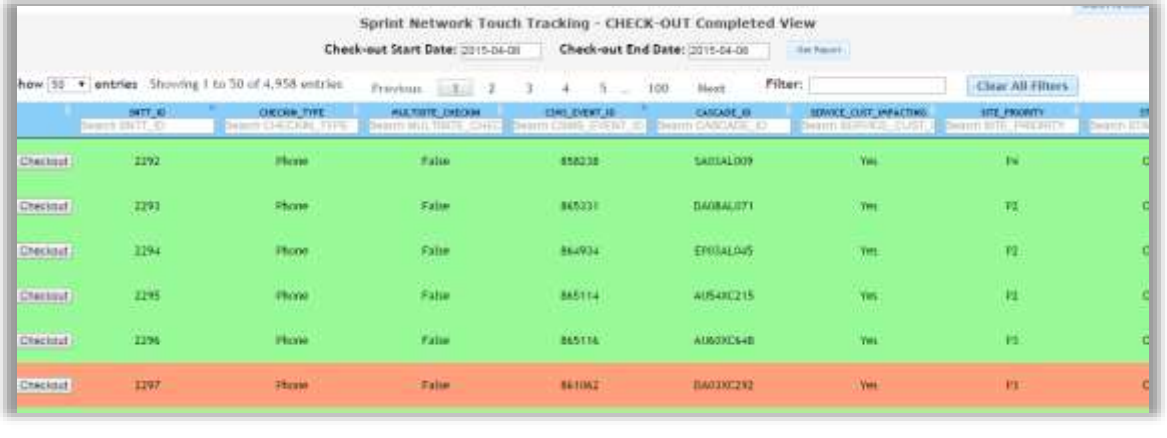


Página Check Out Completed View

Una vez procesado el Check Out, puedo ver los resultados en la página "Check Out Completed View"



Lo que redirigirá a la siguiente vista, donde se encuentran todos los Check Outs procesados:



Ventana principal "Check Out Completed View".

Ese en este punto donde la herramienta automática hace la comparación del estado de alarmas en el sitio, obtiene un reporte de alarmas de netcool al procesarse el check out, el cual es comparado con el que obtuvo al procesarse el check in, esto tarda aproximadamente uno o dos minutos en los cuales actualizo la página hasta que arroje el resultado del check out el cual aparecerá ya sea de color verde o de color rojo al filtrar por cualquiera de los campos para encontrar el check out en cuestión.

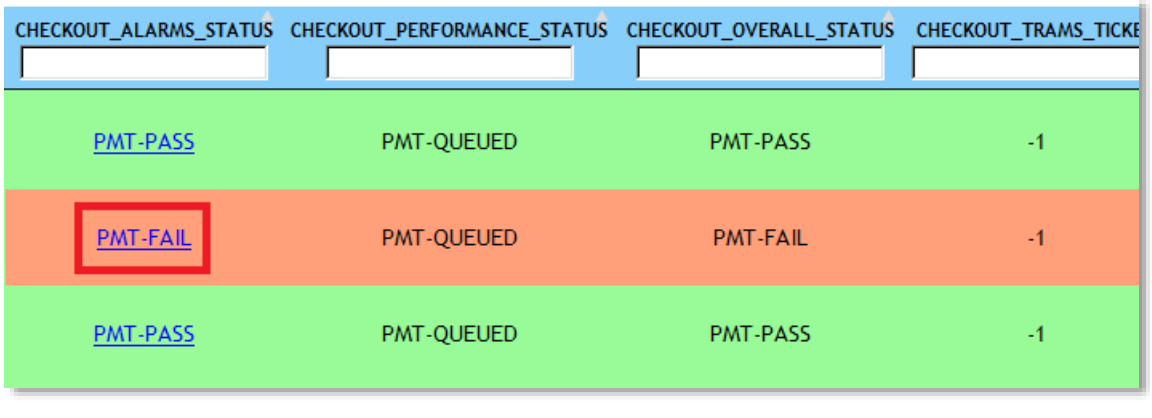
Significado del color resultante en un Check Out

Color Verde **–** El Check Out es "PMT-PASS", la herramienta automática no encontró alarmas adicionales en Netcool y el técnico puede ya salir del sitio sin problema, su trabajo está terminado y el proceso de registro de entrada y salida se completó exitosamente, el estado se queda como "PMT-PASS".

Color Rojo- El Check Out es "PMT-FAIL", la herramienta automática encontró alarmas adicionales durante la ventana de mantenimiento, los pasos a seguir al presentarse este resultado son los siguientes:

– Verifico que las alarmas sean válidas y estén realmente activas

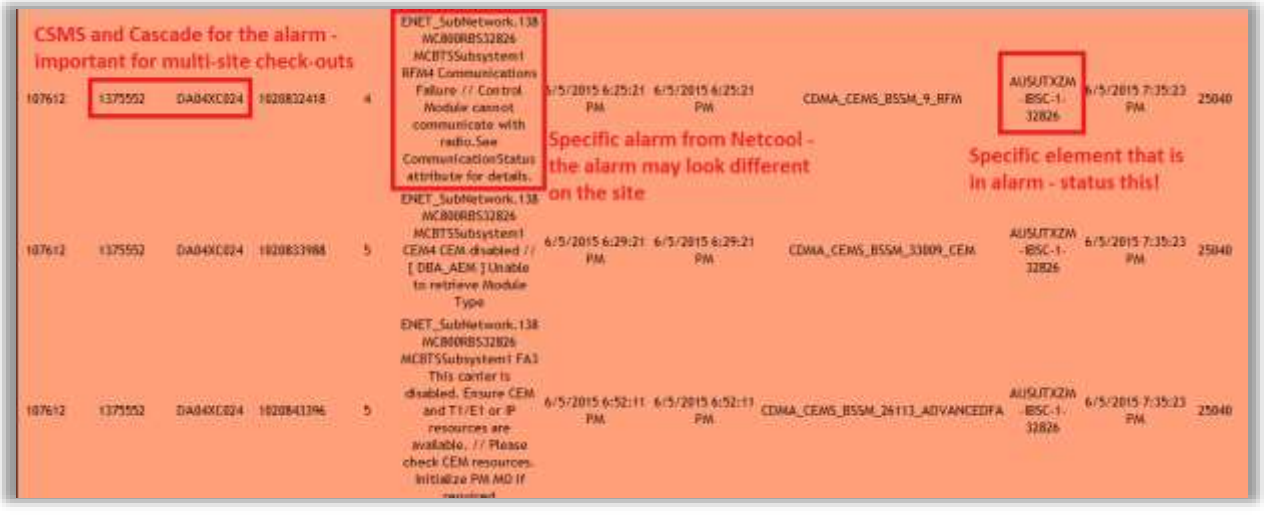
Debajo de la columna *"Check Out Alarms Status",* como se muestra en la figura, se encuentra un hiperlink el cual al dar click se muestran las alarmas que causan que el check out falle, estas serán las alarmas que debo verificar que estén realmente activas, esto se verifica en cada una de las herramientas de verificación de estado de cada tecnología, las mismas ocupadas para los tickets VODQA en la parte de "FREE OF GATING ALARMS".



CHECKOUT_ALARMS_STATUS	CHECKOUT_PERFORMANCE_STATUS	CHECKOUT_OVERALL_STATUS	CHECKOUT_TRAMS_TICKE
PMT-PASS	PMT-QUEUED	PMT-PASS	-1
PMT-FAIL	PMT-QUEUED	PMT-FAIL	-1
PMT-PASS	PMT-QUEUED	PMT-PASS	-1

- Si la(s) alarma(s) no se encuentra(n) activa(s), es posible que el check out haya fallado debido al retraso de Netcool con respecto de la herramienta en tiempo real, cambio el

estado del Check Out a MANUAL-PASS y agrego una nota de que no se encontraron alarmas activas, con esto se concluye el proceso de manera exitosa y el técnico puede dejar el sitio.



- Si la(s) alarma(s) esta(n) activa(s), notifico al técnico a qué están relacionadas las alarmas activas y preguntarle si es capaz de arreglarla(s).

Nota: Antes de notificar al técnico que existen alarmas activas verifico que el elemento reportado se encuentre al aire para dicha banda de frecuencia, en algunos casos podrán aparecer alarmas relacionadas con la frecuencia de 800 MHz cuando es instalada, pero si aún no está al aire debo proceder a cambiar el estado a MANUAL-PASS.

También verifico el historial de alarmas de la radio base ya que es posible que se trate de una alarma pre existente mostrada como una nueva alarma durante el check out.

- Si el técnico está dispuesto a repararlas, cambio el estado del Ckeck Out a "MANUAL-FAIL" y escribo las anotaciones pertinentes en la sección de "Check-out Notes" del botón de Checkout, espero a que vuelva a llamar para volver a verificar.

- Si no le es posible reparar las alarmas, y no tiene apoyo remoto para poder resolverlo, creo un ticket TRAMS para un seguimiento de dichas alarmas y lo envío a la agencia adecuada para su correcto tratamiento y solución.

Determinación del tipo correcto de ticket a crear

Si el técnico ya ha intentado solucionar las alarmas sin éxito, le pregunto ahora si terminó su trabajo en el sitio para ese día o regresará al siguiente día para seguir trabajando con otra ventana de mantenimiento para el mismo sitio como continuación del trabajo que estuvo realizando.

- Si regresará al siguiente día, creo un ticket de TRAMS llamado “multiday”, esto para evitar que se cree algún otro ticket por las alarmas que pudieran estar presentes en el sitio y se mande a otra persona a repararlas, muchas veces hay mantenimientos programados para cierta cantidad de días consecutivos durante los cuales se mantienen alarmas activas intencionalmente, al término de los trabajos de multiples días, estas alarmas debes de estar ya clareadas y dejar el sitio en igual o mejores condiciones que como estaba el primer día que comenzaron los trabajos de mantenimiento.

  Para poder crear el multiday ticket es requerido que el técnico proporcione el número de ticket CSMS con el que va a registrar su entrada al sitio el siguiente día, para asegurar que el técnico está enterado que es responsable de regresar al sitio y continuar con su trabajo.

- Si ya terminó con el trabajo y no regresara a trabajar en la radio base al día siguiente, debo crear un ticket de TRAMS (Ticket Research Analysis and Management Systems) llamado “Failed Check Out”.

  Verifico que ya no exista CSMC para el siguiente día y no exista algún otro ticket para el mismo problema, si existe un ticket multiday se debe cerrar para crear el ticket Failed Check out.

  Agrego una explicación clara del problema en el ticket con la evidencia de las alarmas activas para su fácil detección y solución. Dependiendo del problema envío el ticket ya sea a OEM o a gente de campo de Sprint para resolver el problema, si se trata de alarmas con impacto en el servicio lo envío a campo de lo contrario lo envío con alguno de los diferentes OEM. En el anexo b se explica con un diagrama de flujo todo este proceso.

Resultados y aportaciones:

En ambas actividades realizadas se requiere de procedimientos y técnicas de análisis, evaluación y resolución de problemas como principales herramientas para poder desarrollar un buen trabajo.

Dentro del proceso de gestión de eventos realizo un procedimiento de detección e interpretación de ocurrencias de manera eficiente, esto es, identificar que evento repercute en la infraestructura del cliente evaluando su dimensión e impacto para una correcta apreciación de problemas o inconvenientes e iniciar una apropiada acción de control y solución. Para este procedimiento requiero conocer el estado de la infraestructura y detectar cualquier desviación de los niveles operacionales normales o esperados.

Este proceso depende de sistemas eficientes de monitoreo y control, las cuales generen alertas en caso de detección de alguna falla operacional.

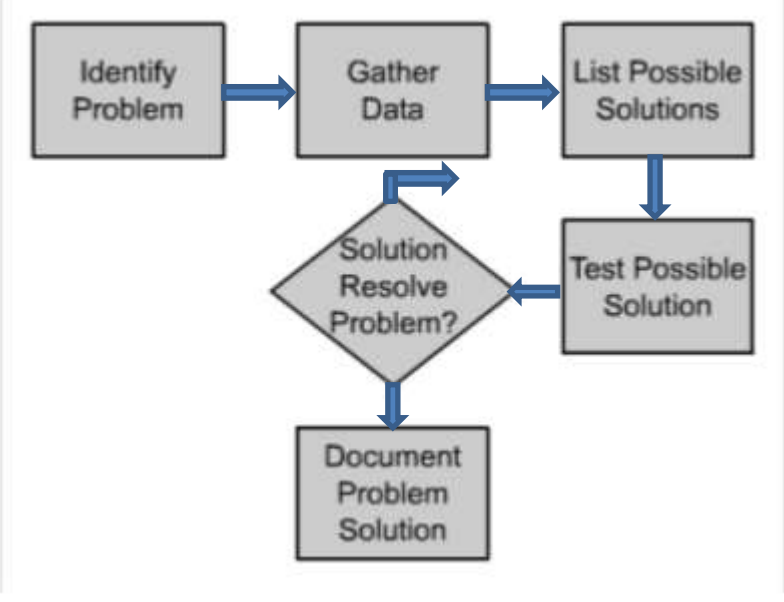
Al ser detectadas estas alertas debo evaluar su causa y consecuencia, así como su impacto y darle un correcto seguimiento, en caso de ser necesario, lo reporto al departamento correspondiente para su pronta solución creando un ticket, proporcionando todos las características y causas del problema después de analizar todos los factores, este es el procedimiento que más utilizo para la solución de problemas, también llamado *troubleshooting*.

Al final, después de identificar el problema y resolverlo verifico con una prueba de estado, descartando que el problema persiste en su totalidad y corroborando la solución del mismo, cerrando el ticket hasta que cualquier alerta sea solucionada.

Es importante en este punto identificar diferentes tipos de problemas y darle una solución a la vez, es decir, si se cuenta con varias alertas, saber distinguir si son relacionadas al mismo problema, o a la misma falla, o se trata de problemas distintos, solucionándolos de manera separada y organizada, siendo esta la manera más eficiente.

Este proceso se resume mediante los siguientes pasos:

a. Identificar el problema
b. Obtener y analizar datos
c. Proponer posible(s) solución(es)
d. Implementar solución
e. ¿Se resolvió el problema?
f. Documentar la resolución



Las habilidades de análisis y resolución de problemas aprendidas en la carrera me han permitido desempeñarme de mejor manera en el ámbito laboral, si bien día con día se presentan nuevos retos o inconvenientes, como lo es cuando alguna de nuestras herramientas principales de monitoreo deja de funcionar, he podido pensar en otras alternativas para solucionarlo y aplicar un criterio profesional para determinar posibles soluciones y ejecutar un plan de acción.

También es importante destacar los conocimientos teóricos adquiridos en la facultad, los cuales han sido útiles para el mejor entendimiento de los sistemas de telecomunicaciones con los que trabajo y para comprender mejor los cursos de capacitación que me proporcionaron, con los que he logrado un mejor desempeño.

Conclusiones:

A lo largo de este tiempo trabajando para esta empresa he aprendido muchísimas cosas, desde las primeras capacitaciones, aprendí cosas sobre las redes celulares que no sabía, dado que no era mi área de especialización, sin embargo, es un área que me interesó aprender y saber cómo funcionan los sistemas de telefonía celular, ahora tengo un panorama diferente al que tenía sobre las telecomunicaciones y en específico las redes.

Después de esa capacitación teórica y un poco práctica, se me asigna a un proyecto en específico, RSA/SNTT junto con un grupo de colegas, algunos con la misma experiencia laboral que yo y algunos que ya tenían años trabajando con otros proyectos en el GNOC.

El proyecto se llevaba a cabo en el estado de Kansas en Estados Unidos por un equipo de la empresa en ese país, donde se localizan las oficinas de Sprint.
Sprint decidió trasladar el proyecto a la ciudad de México para continuar la operación en el GNOC México.

Así comenzó la capacitación del proyecto y todos los procesos ya explicados en la parte del desarrollo del presente reporte, las personas que nos capacitaron fueron el manager y un líder de equipo del anterior grupo de Estados Unidos.

Desde el primer día trabajando en la empresa, en la presentación y bienvenida, he desarrollado una mejor comprensión del lenguaje inglés, escuchando gente de diferentes nacionalidades, ahora puedo entablar una conversación en inglés y poder entender muchas más cosas que antes, eso ha sido para mí un gran cambio y avance en mi experiencia profesional.

Debido a mi poca experiencia con redes, y como complemento a los cursos de capacitación de la empresa, tome algunos cursos de certificación para comprender mejor sobre este campo, tome el curso de certificación HCNA-LTE impartido en la facultad de Ingeniería por el doctor Victor Rangel Licea, un curso sobre redes LTE para certificación por parte de Huawei, y otro curso en una institución externa para la certificación CCNA de Cisco, con estos dos cursos pude comprender mejor lo que realizo en el trabajo.

Los conocimientos adquiridos hasta ahora, junto con la experiencia que llevo, buena conducta y puntualidad me han ayudado a obtener buenos resultados en mi revisión de IPM (Individual Performance Management) que se realiza dos veces al año, en la cual se evalúan ciertos puntos y se definen objetivos a conseguir con el manager del proyecto, de esta manera he podido conseguir aumentos de sueldo.

Bibliografía:

Fuentes bibliográficas :

- DOOD Annabel Z. (2001). *The Essential Guide to Telecommunications*. New Jersey: Prentice Hall PTR.

- BELLAMY John C. (2000). *Digital Telephony (Wiley Series in Telecommunications and Signal Processing)*. New York: Wiley-Interscience.

- Roger L. Freeman. (1999). Fundamentals of Telecommunications. New York: John Wiley & Sons, Inc.

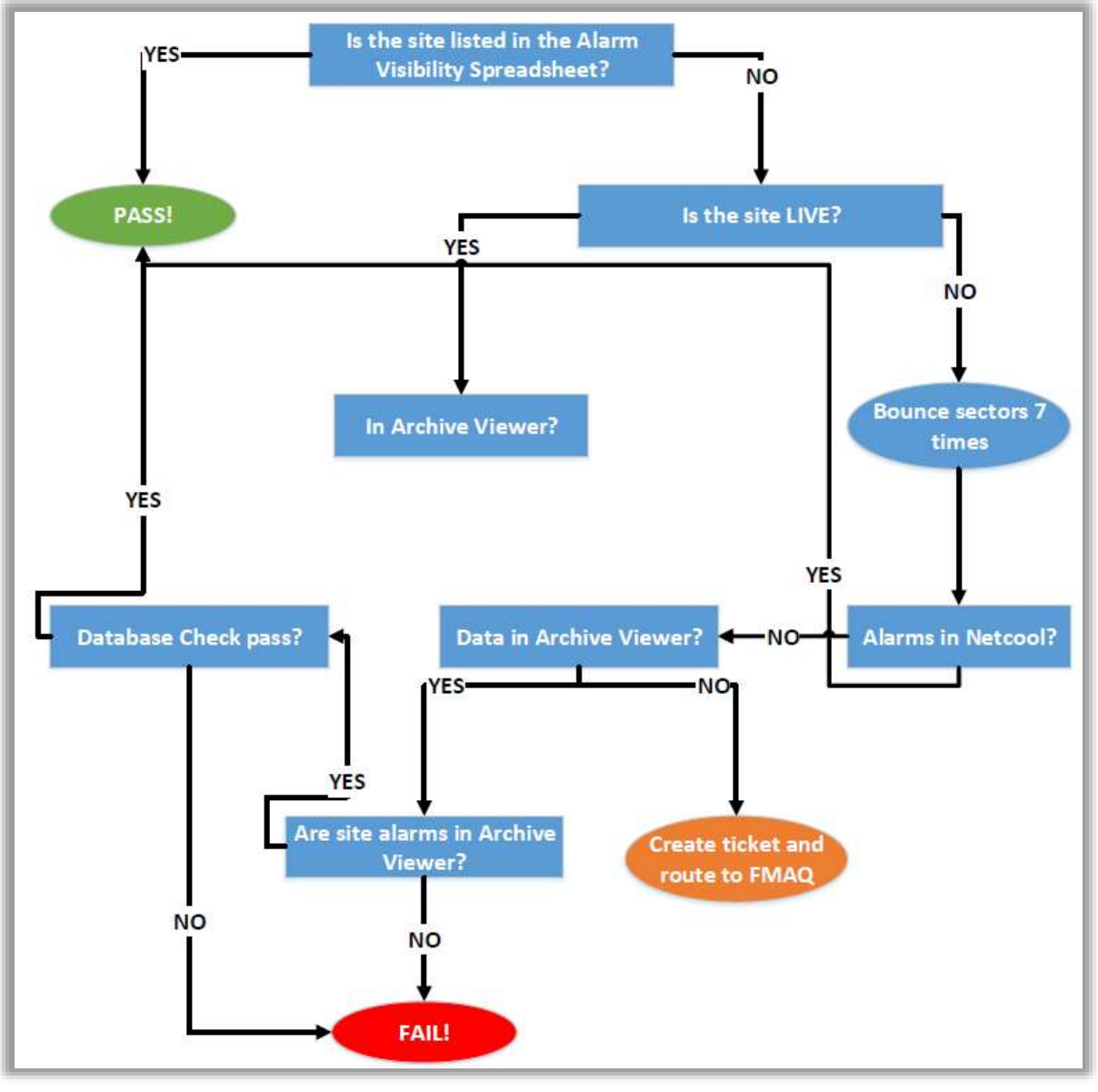
Fuentes Digitales:

- http://www.ericssonhistory.com/

- http://www.ericsson.com/cr/news/2012-12-20-line-es_3377875_c

Anexos:

a. Troubleshooting alarm visibility



b. Diagrama de flujo Failed Checkout