UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN
DEPARTAMENTO DE SISTEMAS DIGITALES Y TELECOMUNICACIONES

Trabajo Monográfico para optar al Título de
Ingeniero en Electrónica

ESCENARIOS PARA EL RESTABLECIMIENTO DE FALLAS DE HARDWARE EN LAS TECNOLOGÍAS W-CDMA Y LTE EN NICARAGUA

Autores: **Br. Gerson Rafael Suárez Gúnera** **Carnet: 2010-33067**
Br. Jeneski de Jesús Marenco Martínez **Carnet: 2009-29679**

Tutor: **Msc. Ing. Cedrick Dalla-Torre**

Managua, Nicaragua
Marzo 2023

DEDICATORIA

Dedico éste trabajo en primer Lugar a Dios por darme la fortaleza para finalizarlo, por darme salud e iluminarme para cumplir todos mis objetivos durante mi etapa de estudiante y ahora durante mi fase como profesional por abrirme puertas y permitir mostrar mis capacidades.

Dedico muy especialmente a mi madre, quien ha dado todo su esfuerzo y ha sacrificado su tiempo y momentos en familia para darme la oportunidad de estudiar y culminar ésta carrera, a ella que tuvo migrar a un país diferente, dejando atrás a sus amistades, familiares, a sus padres quienes hoy descansan en paz, todo por darme estabilidad económica y que pudiera junto a mis hermanos finalizar los estudios, ejercer la carrera profesional y dejarme la mayor herencia que un padre puede dar a un hijo, buenos valores y un medio para defenderme en la vida, quiero decirte Gracias, éste trabajo es para ti.

GERSON RAFAEL SUAREZ GUNERA

Dedico mi tesis principalmente a Jehová Dios, por dar la sabiduría y la fuerza necesaria para culminar esta meta.

A mis padres, por todo su amor, su apoyo incondicional y por motivarme e inculcarme buenos valores y seguir hacia adelante. También a mi hermano, por brindarme su apoyo y motivación para estudiar esta carrera profesional.

Y, finalmente, a nuestro tutor monográfico Msc.Cedrick Dallatorre por su paciencia y conocimientos que nos brindó en nuestra carrera y trabajo monográfico.

JENESKI DE JESUS MARENCO MARTINEZ

AGRADECIMIENTOS

Doy Gracias a Dios en primer lugar por darme la vida, por poder desarrollarme personal, académica y profesionalmente, por haberme dado la fuerza, paciencia y entusiasmo para finalizar este trabajo, que hemos concluido tras muchas dificultades.

Agradezco a mis padres Elsa Gúnera Pérez y Jorge Suárez Padilla por haberme brindado los medios necesarios para poder culminar mis estudios, a mi tía Luisa Amanda Gúnera Pérez por brindarme un hogar durante la mayor parte de mi vida estudiantil, al departamento de bacas de la Universidad Nacional de Ingenieria por acogerme en el internado de la UNI durante la última etapa como estudiante.

Muy agradecido con todo el personal profesional especialista en el tema de radio bases que dieron su aporte a este trabajo desde su experiencia en campo y optimización de red móvil: Ing. Abelson Blandino, Ing. Ariel Ramirez e Ing. Danilo Ramirez y a la Ing. Lissette Palma por darme el espacio para desarrollar el tema desde el enfoque del trabajo que realizan en su área de especialización NOC.

GERSON RAFAEL SUAREZ GUNERA

Doy gracias en primer lugar a nuestro padre celestial jehová y nuestro señor Jesus, por habernos permitido finalizar el presente trabajo, el cual logramos realizarlo por el apoyo, comprensión, cariño y sobre todo el amor de nuestros padres, familiares y amigos que día a día fueron parte de nuestra fuerzas, ánimos y voluntad de alcanzar esta meta.

Agradecemos muy especialmente por su ayuda, asesoría y buena voluntad a nuestro tutor monográfico Msc. Cedrick Dallatorre, quien además nos brindó su confianza y motivación, al permitirnos la realización de este trabajo monográfico para los futuros estudiantes de nuestra facultad electrotecnia y computación.

Además, deseamos reconocer el esfuerzo directo e indirecto de todas aquellas personas que siempre han estado a nuestro lado apoyándonos y aportando su granito de arena en la realización de este tema como lo son las telecomunicaciones, para que nos preparemos como buenas personas y profesionales a la vez de nuestro país todos ellos muchas gracias.

JENESKI DE JESUS MARENCO MARTINEZ

RESUMEN

El presente trabajo monográfico consiste en el desarrollo de guías procedimentales para atender fallas en la red móvil de acceso celular (RAN, por sus siglas en inglés Radio Access Network). Es dirigido a lectores con interés en las telecomunicaciones, estudiantes de Ingenierías a fines a sistemas de telecomunicaciones y profesionales del sector que se interesen en aprender un modelo de trabajo para atención de fallas de equipos radio base (RBS, por sus siglas en inglés Radio Base Station).

Inicialmente se exponen conceptos básicos de telefonía celular referentes a la evolución de las tecnologías móviles, se le muestra al lector la arquitectura de la red móvil: Core y acceso, para que darnos una idea de en qué parte de la red se enfocará el desarrollo de las guías con procedimientos para restablecer los servicios móviles y se explica el modelo de organización y distribución de trabajo actual en las empresas operadoras de telefonía: NOC – Campo, (NOC por sus siglas en inglés Network Operation Center) así mismo, se detallan las herramientas más usadas y la importancia que tienen sobre las atenciones de fallas en la red, como sistemas de monitoreo para radio base, plataforma de procesamiento de alarmas y plataformas de gestión de incidencias.

El contenido de la guía explica la forma de atender alarmas que se reciben en los sistemas de monitoreo de la red móvil, se escogieron cinco principales grupos de alarmas que tienen una mayor frecuencia de reincidencias y que impactante sobre el servicio de telefonía celular que los operadores brindan al usuario final.

Por cada grupo de alarmas seleccionado, se realizará una explicación del cableado de la alarma o de la topología de conexión de los elementos que intervienen en el proceso y que por tanto pueden fallar al recibir la alerta. En los casos que aplica, se explica cómo realizar la configuración de las alarmas que recibirán en los gestores nativos. Se marcan los procedimientos más importantes del trabajo de monitoreo remoto, los tipos de alertas que se reciben, el troubleshooting que se realiza para intentar resolver problemas sin despachar personal y se expone los criterios para la movilización de personal técnico a sitio para atender los eventos. Finalmente explicamos las pruebas que se hacen para determinar la falla en el Hardware en sitio, los procedimientos de atención desde campo y algunos procedimientos especiales para la resolución de problemas.

INDICE

I. INTRODUCCIÓN 1
II. OBJETIVOS 2
2.1. Objetivo General: 2
2.2. Objetivos Específicos: 2
III. JUSTIFICACIÓN 3
IV. CAPITULO I: GENERALIDADES DE LA TELEFONIA CELULAR 5
4.1. GENERACIÓN 4G 6
4.2. PROVEEDORES DE TELEFONIA MOVIL 7
4.2.1. ERICSSON 8
4.2.2. HUAWEI 9
4.2.3. NOKIA 10
4.3. OPERADORAS TELEFONICAS EN NICARAGUA 11
V. CAPITULO II: ESTRUCTURA RED MOVIL 13
5.1. Arquitectura de la red móvil 13
5.1.2. Red UMTS 13
5.1.2.2. Red de acceso de radio RAN 16
5.1.3 Red LTE 25
5.2. Arquitectura de RBS 30
5.2.1. RBS 6000 31
VI. CAPITULO III: MONITOREO Y ATENCION DE ALARMAS RAN 44
6.1. Modelo NOC - Campo 44
6.1.1 Network Operation Center (NOC) 45
6.1.2. Operación y Mantenimiento (O&M) 49
6.2. Herramientas de Monitoreo y Gestión de alarmas 50
6.2.1. OSS 51
6.2.2. ENM 55
6.3. Monitoreo de Alarmas 56
6.4. TeMIP 58
6.5. Herramientas de gestión de Incidencias 59
6.6. Validación de Incidencias y Atención de alarmas. 60
6.7. Tipos de fallas 65
6.7.1. Fallas de energía. 65
6.7.2. Fallas de Hardware/Software RBS. 68

6.7.3. Fallas de transporte 70
VII. RESULTADOS – ATENCIÓN DE FALLAS RBS 72
7.1. Fallas más recurrentes en RBS 73
7.2. Escenarios de restablecimiento. 74
7.2.1. Fallas de energía AC 74
7.2.1.1. Cableado de alarmas externas 74
7.2.1.2. Configuración lógica de alarmas externas 79
7.2.1.3. Monitoreo Remoto de la red 83
7.2.1.4. Trabajo de campo 89
7.2.2. Fallas de energía DC 92
7.2.2.1. Conexión de alarmas internas de energía DC 92
7.2.2.2. Monitoreo Remoto 94
7.2.2.3. Trabajo de campo 98
7.2.3. Fallas de sectores 100
7.2.3.1. Conexiones físicas de RRU 100
7.2.3.2. Monitoreo y Troubleshooting remoto 102
7.2.3.3. Trabajo de campo 107
7.2.4. Fallas de diversidad 109
7.2.4.1. Conexión física de RRU 109
7.2.4.2. Monitoreo Remoto 110
7.2.4.3. Trabajo de campo 116
7.2.5. Fallas de Hardware/Software DU/BB 117
7.2.5.1. Conexiones Física de la Transmisión hacia la RBS 117
7.2.5.2. Monitoreo remoto 120
7.2.5.3. Trabajo de campo 127
IX. CONCLUSIONES 146
X. RECOMENDACIONES 147
XI. BIBLIOGRAFÍA 148
XII. ANEXOS 151

CONTENIDO DE ILUSTRACIONES

Figura 1. Generaciones Móviles 6
Figura 2. Logo ERICSSON 8
Figura 3. Logo HUAWEI 9
Figura 4. Logo NOKIA 10
Figura 5. Espectro y Tecnología en Nicaragua 12
Figura 6. Arquitectura redes 3G 14
Figura 7. Equipamiento de Usuario 15
Figura 8. UTRAN 16
Figura 9. Interfaz IUB 18
Figura 10. Network Switching Subsystem (NSS) 22
Figura 11. PS Core Network 23
Figura 12. ARQUITECTURA 4G 25
Figura 13. EUTRAN 26
Figura 14. Conexiones EPC 28
Figura 15. Comparativa E-UTRAN vs UTRAN 29
Figura 16. RBS 2000 30
Figura 17. Familia RBS 6000 32
Figura 18. RBS 6201 33
Figura 19. Arquitectura hardware RBS 6102 34
Figura 20. Estante de radio 35
Figura 21. Sistema de energía RBS 39
Figura 22. BBS 40
Figura 23. Estante de transporte 41
Figura 24. Monitoreo NOC 46
Figura 25. Citrix MetaFrame 52
Figura 26. Herramientas OSS Citrix Metaframe 54
Figura 27. Terminal Moshell OSS Citrix 54
Figura 28. Winfiol. 55
Figura 29. Ericsson Network Manager 55
Figura 30. Winfiol desde ENM 57
Figura 31. TeMIP 58
Figura 32. HP Service Manager 59
Figura 33. BMC Remedy 59
Figura 34. Flujo de Alarmas 60
Figura 35. Bandeja de Incidentes BMC Remedy 61
Figura 36. Interface CLI ENM - Información de un Nodo B. 63
Figura 37. ENM Alarm Monitor 64
Figura 38. ENM Alarm Search - Filtro Alarmas Internas 66
Figura 39, ENM CLI - Revisión de elementos de energía 66
Figura 40. ENM CLI - Alarmas Externas 67
Figura 41. ENM GUI - Alarmas Externas 67
Figura 42. Alarma Hw Partial Fault 69
Figura 43. Revisión de HW de RRU 69
Figura 44. Red de transporte [31] 70
Figura 45. Nodo B afectado por falla en red Tx 71

Figura 46. Alarmas Externas - Conexiones OVP 75
Figura 47. Conexión de alarmas externas - Borneras 76
Figura 48. Conexión Bornera SUP hacia OVP 76
Figura 49. Alarmas Externas sitio sin MG 77
Figura 50. Conexiones alarmas externas hacia las DU 78
Figura 51. Verificación lógica de puertos de alarmas 80
Figura 52. Bloqueo de alarmas externas 81
Figura 53. Configuración de Slogan Alarmas Externas 81
Figura 54. Activación de alarmas externas 82
Figura 55. Alarmas Externas Corte AC + MG Operando. GUI - CLI 84
Figura 56. Alarmas Externas Corte AC + Baterías en descarga. GUI - CLI 85
Figura 57. Alarma Externa Falla de MG. GUI. 87
Figura 58. Alarmas Internas Comercial Power Failure . Running on Battery. GUI. 88
Figura 59. Conexión de alarmas internas hacia las DU 93
Figura 60. Verificación de elementos energía DC. ENM CLI 95
Figura 61. Mediciones energéticas elementos DC RBS - ENM CLI 96
Figura 62. Validación de Operatividad de los elementos de energía DC. ENM CLI 97
Figura 63. Conexión RRU Aéreo hacia Gabinete RBS 101
Figura 64. Validación de alarmas de sectores. ENM CLI 104
Figura 65. Diagrama de bloques BB - RRU. ENM CLI 105
Figura 66. Información de la Alarmas SDIC. ENM - CLI 106
Figura 67. Conexión RRU hacia antena 109
Figura 68. Pérdida de retorno RL (VSWR) 111
Figura 69. Medición del nivel de Perdida de retorno (RL) VSWR 112
Figura 70. Medición VSWR (RL) comando cabx 113
Figura 71. Medición RSSI pmr 114
Figura 72. Medición RSSI cabx 114
Figura 73. Conexiones equipos Transmisión y RBS 118
Figura 74. Revisión de puerto TN configurados 121
Figura 75. Revisión de negociación en Puertos TN 121
Figura 76. Revisión de modelo de SFP, comando sdic 122
Figura 77. Prueba de ping hacia la SIU 124
Figura 78. Conexión SSH con una SIU 124
Figura 79. Revisión de alarmas de una SIU 125
Figura 80. Revisión de Puertos de una SIU 125
Figura 81. Revisión de tráfico y estado tarjeta DUW 126
Figura 82. Alarma local DUW 128
Figura 83, Conexión hiperterminal 129
Figura 84. Búsqueda del archivo del Software a cargar en la tarjeta 131
Figura 85. Búsqueda del archivo del CV a cargar en la tarjeta 131
Figura 86. Configurar ruta estática en PC hacia BB 132
Figura 87. Baseband Emergency Access 133
Figura 88. Ejecución de Board Restore 134
Figura 89. Carpeta en Disco C con archivos para restoring 134
Figura 90. Configuración de ruta mini-sfp-core 135
Figura 91. Configuración ruta CV en Recovery Summary 135
Figura 92. Configuración ruta SW en Recovery Summary 136

Figura 93. Configuración menú Autointegration BB 137
Figura 94. Porcentaje de descarga de archivos en la BB 137
Figura 95. Activación de la opción Integrate - proceso de instalación SW - CV 138

CONTENIDOS DE TABLAS

Tabla 1. ALARMAS EXTERNAS SITIOS CON MG.....74
Tabla 2. ALARMAS EXTERNAS SITIOS SIN MG.....77

I. INTRODUCCIÓN

Actualmente en este mundo digital, las telecomunicaciones móviles tienen un peso significativo en lo que respecta al desarrollo económico y social. Debido a que promueven diferentes tipos de servicios, tanto el acceso a comunicarse por voz, como también servicios de datos, con el acceso a datos se tiene la oportunidad de navegar en internet y de hacer uso de distintas aplicaciones, tanto móviles como de escritorio que generan valor a las vidas de los usuarios de este tipo de servicio.

En el presente trabajo monográfico, se tiene como objetivo general, la realización de guías procedimentales para la restauración de servicios de telefonía móvil, lo que tendrá un impacto positivo para las empresas operadoras, ya que actualmente no se dispone de un documento que contengan los pasos y configuraciones que se requieren para el restablecimiento de los servicios móviles. Esta propuesta, es de carácter aplicado y empírico, ya que se basa en la experiencia de los ingenieros de campo que hacen este tipo de tareas en empresas operadoras en todo el territorio nicaragüense. Por otro lado, se pretende que con esta guía se optimice tiempo y recursos, ya que no se necesitará de la presencia de ingenieros seniors en las diferentes estaciones bases. Debido a que un ingeniero junior, con el seguimiento paso a paso del contenido de la propuesta de guía podrá restablecer los servicios de las RBS enfocado a asegurar el cumplimiento de KPI’s.

Por tanto, las operadoras podrán disponer de documentación que servirá para reducir los tiempos con que normalmente se restablecen los servicios de comunicaciones móviles en las estaciones bases, de esta manera se tendrá menos riesgo que permanezcan por mucho tiempo caídos los servicios que estas empresas operadoras ofrecen a la sociedad. Además, con la culminación de este trabajo se pretende que los estudiantes de telecomunicaciones y carreras afines puedan disponer de un documento que les ilustre el modo de operar de las empresas que serán un posible destino laboral, conocer parte de red celular, sus fallas y la atención oportuna de cada caso que será expuesto en el presente trabajo que servirá de referencia académica, profesional y que pretende que ayude a acotar la curva de aprendizaje de los Ingenieros asignados a este tipo de labor.

II. OBJETIVOS

2.1. Objetivo General:

Realizar un estudio de escenarios más frecuentes de alarmas que se presentan en una empresa de telefonía móvil para tecnologías W-CDMA y LTE en Nicaragua.

2.2. Objetivos Específicos:

- Realizar una investigación documental respecto a los estándares W-CDMA y LTE.

- Dar a conocer la arquitectura física de los dispositivos que conforman una estación base en tecnologías W-CDMA y LTE para facilitar la comprensión de su funcionamiento.

- Analizar los escenarios de fallas más frecuentes en tecnologías W-CDMA y LTE en Nicaragua.

- Desarrollar guías procedimentales que briden la solución a las alarmas identificadas con recurrencia en tecnologías W-CDMA y LTE en Nicaragua.

III. JUSTIFICACIÓN

La educación superior en Nicaragua aborda de manera conceptual la mayor parte del contenido de la red celular, no se cuenta con procedimientos prácticos específicos y no se tienen equipos de redes en producción de operadores de telefonía para prácticas de laboratorio actualizadas, por lo cual el estudiante que se perfila a trabajos relacionados con la telefonía celular tienen poco conocimiento práctico sobre la visualización de alarmas y toma de para la atención de fallas que ocurren con mayor frecuencia en las empresas operadoras que serán sus posibles destinos laborales.

Por otro lado, las empresas operadoras por lo general tienen que capacitar al personal nuevo asumiendo que no tienen conocimiento alguno del trabajo que llegaran a realizar a determinada área dentro de la organización, esto recae en una prolongación de la curva de aprendizaje que impacta en el servicio al consumidor final al extenderse los tiempos de atención y resolución de fallas, muchas veces por la falta de conocimiento técnico, toma de malas decisiones y puesta en marcha de procedimientos que ayuden a optimizar la solución de problemas.

En una Operadora de telecomunicaciones se necesita tener personal con el conocimiento necesario para afrontar los problemas que se presenten en la red, además realizar estudios internos de los rubros que afectan mayormente los KPI, es decir que la red nos retroalimente sus necesidades para crear estrategias de para minimizar impactos.

Mediante un estudio de recurrencias de fallas proporcionado por una empresa de telecomunicaciones en Nicaragua, hemos detectado que durante el 1er cuatrimestre del año 2019 se contabilizó que las fallas que afectan la disponibilidad en la red móvil en la tecnología W-CDMA y LTE que se gestionan desde alarmas remotas se disgregan de la siguiente manera: el 31% se debe a fallas de energía en sitios sin respaldo de Motor Generador, 25% son afectados por cortes de Fibra Optica, el 16% a fallas de Motor Generador, un 8% a falla en los equipos RBS, el 3% a falla sistemas de energía internos de las Radio Base (Tarjetas rectificadoras) y el otro 17% a diferentes causas (Trabajos Programados de crecimiento a la red, respaldos, Falla en los equipos de Transporte, combustible, mantenimientos preventivos, entre otros). En el caso de los sitios LTE, hemos contabilizado que el 50% de las fallas se debe a cortes de energía en sitios sin respaldo de Motor Generador, el 21 % a cortes de fibra óptica, el 8% a fallas en los equipos RBS, un

5% a falla de Motor Generador, el 2% falla en sistemas de energía internos de las Radio Base (Tarjetas rectificadoras) y el otro 14% a diferentes causas.

Debido a que la mayor cantidad de fallas tanto en tecnología W-CDMA como en LTE se debe principalmente a fallas de energía (en sitios con/sin motor generador para el respaldo energético en caso de cortes AC), en la tecnología W-CDMA el 47% y en LTE el 55%, es necesario tener claro la importancia del monitoreo de las alarmas relacionada con Fallas de energía que afectan la disponibilidad como una caída total del servicio, ya sean alarmas de forma externa o interna en los equipos RBS, sin quitar importancia a las alarmas generadas por las estaciones base que impactan en temas de calidad del servicio como alarmas de RSSI, VSWR o que puntualicen fallas en algún punto de conexión interno o tarjeta, lo cual actualmente es realizado en Nicaragua principalmente mediante la herramientas proporcionadas por los proveedores, en este caso Ericsson, el cual proporciona a los operadores gestores de monitoreo remoto como el OSS-ERICSSON (Operation Support Sistem) y ENM (Ericsson Network Manager). En otros operadores brindan soluciones alternas para temas de monitoreo con menos herramientas pero que cumple su acometido: alertar de las fallas de manera preventiva en la red.

Por ello, vemos la importancia de desarrollar una documentación que explique el modo operandi en las empresas de telecomunicaciones para atender fallas en la red celular a nivel de acceso, de modo que los estudiantes y los trabajadores nuevos en las operadoras puedan hacerse de una idea más clara de que se encontraran en sus trabajos y la importancia de tener guías procedimentales para darle resolución a los escenarios que más impactan los servicios de los clientes que consumen este producto. Explicaremos un listado de escenarios de posibles fallas y según la importancia abordaremos a mayor detalle las fallas de mayor recurrencia que impactan mayormente la disponibilidad de la red, delimitaremos nuestro estudio a equipos de acceso en de la red móvil (RBS).

IV. CAPITULO I: GENERALIDADES DE LA TELEFONIA CELULAR

La telefonía es el servicio más utilizado de los que ofrecen los sistemas de comunicaciones móviles. Todos los sistemas tienen la función de telefonía incorporada.

Si bien la telefonía móvil empezó siendo analógica, en la actualidad todo el servicio es digital. Esta telefonía móvil digital, que también recibe la denominación de celular en algunos países, se basa en el concepto de celda o célula. [17]

La clasificación más comúnmente usada para referirse a los sistemas de comunicaciones móviles es la siguiente:

- Primera generación 1G o analógicos (AMPS, NTM, TACS...)
- Segunda generación 2G o digitales (GSM).
- Segunda generación avanzada 2.5G (GPRS) y 2.75G (EGPRS).
- Tercera generación 3G (UMTS).
- Tercera generación avanzada 3.5G (HSDPA), 3,75G (HSUPA) y 3.8G - 3.85G (HSPA+).
- Cuarta generación 4G (LTE), 4G+ (LTE Advanced).
- Quinta generación 5G.

La primera generación de telefonía móvil (1G), se caracterizó por ser análoga y brindar únicamente servicio de comunicación de voz [6], luego con la implementación de la segunda generación (2G) y sus evoluciones (GPRS, EGPRS) se logra brindar al usuario tanto servicio de voz y datos a velocidades limitadas pero que cumplían el propósito del momento [3]. Más adelante con la implantación de la tercera generación (3G) y sus evoluciones se tuvo una mejora significativa en las velocidades de conexión por lo que permitió el desarrollo de servicios como streaming multimedia, transferencias de archivos pesados y video-conferencia a una gran variedad de dispositivos, entre ellos teléfonos celulares, PDAs y computadoras portátiles [4].

Las primeras generaciones actualmente son utilizadas en un porcentaje muy reducido a nivel mundial, sin embargo, dieron paso a las siguientes etapas del desarrollo de la tenía celular. A continuación, se explica con un poco más de detalle las mejoras para el usuario con el nacimiento de la tecnología 4G.

4.1. GENERACIÓN 4G

LTE significa **Long Term Evolution** es un estándar de comunicaciones móviles desarrollado por la 3GPP, la asociación que desarrolló y mantiene GSM y UMTS. El interfaz radio (nivel físico) del sistema LTE es algo completamente nuevo, así que LTE es una nueva generación respecto a UMTS (tercera generación o 3G) y a su vez GSM (segunda generación o 2G). Véase en la figura 1 la línea de tiempo aproximada del despliegue de las tecnologías móviles. [5]

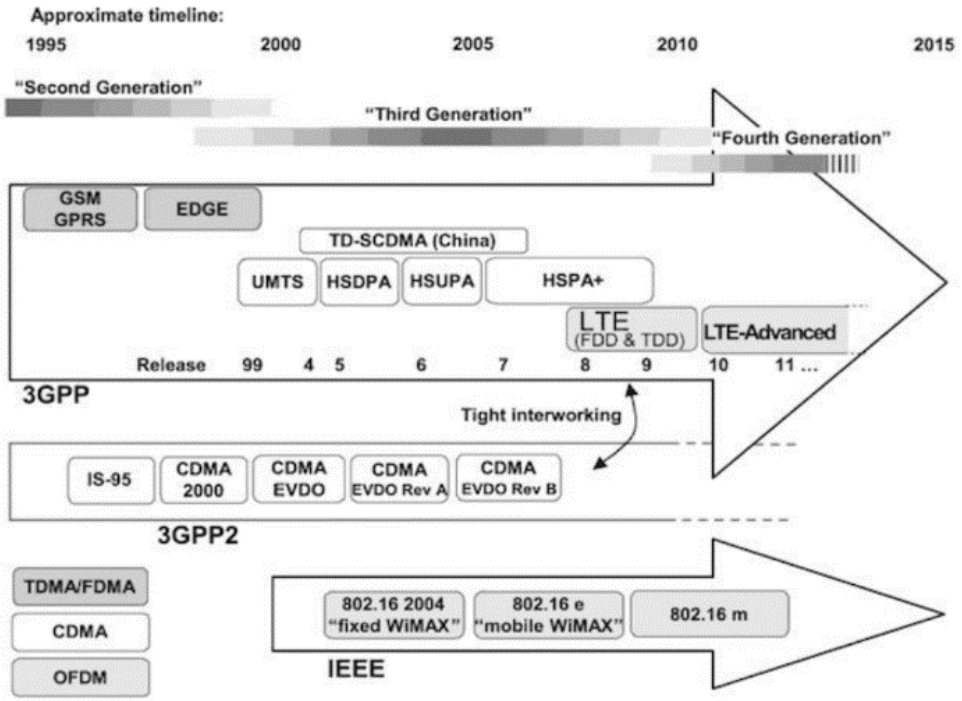


Figura 1. Generaciones Móviles [5]

LTE nació pensando en cubrir principalmente las siguientes necesidades:

- Los usuarios quieren una conexión de datos que descargue y suba a más velocidad
- Los fabricantes y operadores quieren un estándar menos complejo y que reduzca los costes
- Hay que asegurar la competitividad del 3G en el futuro frente, por ejemplo, a WiMAX

CARACTERÍSTICAS DE LTE

LTE es una tecnología muy buena y estable con tres características principales: permite altas tasas de bits con baja latencia, es barato y fácil de desplegar por los operadores, y evita la fragmentación por el tipo de duplexación. [5]

Las tasas de descarga y subida, que es lo que más interesa de esta tecnología, puede alcanzar velocidades de pico de 173 Mbps de bajada y 86 Mbps de subida, con 2 antenas en la estación base y 2 en el terminal (y hasta 300 Mbps de bajada con 4×4 antenas).

Respecto a que sea una red fácil de desplegar, la clave está en que los servicios de LTE sólo utilizan conmutación de paquetes. LTE no puede gestionar SMS o llamadas a la antigua, con conmutación de circuitos; de eso se seguirán encargando las redes GSM y demás, con la consiguiente optimización de los costes en infraestructura, una nueva solución a este problema fue el despliegue de VoLTE para poder hacer llamadas sobre LTE.

El sistema de switching de paquetes de LTE está muy optimizado, para un mundo en el que cada vez hacemos más cosas sobre IP (voip en lugar de llamadas, whatsapps en lugar de SMS…)

Por último, LTE también está pensado para evitar la fragmentación de los terminales a nivel mundial por el tipo de duplexación, ya que las últimas revisiones del estándar son compatibles tanto con FDD (Frequency Division Duplex) que utiliza varias zonas del espectro y TDD (Time Division Duplex) que ocupa una sola zona.

4.2. PROVEEDORES DE TELEFONIA MOVIL

Los principales desarrolladores de tecnología RAN (redes móviles de acceso radioeléctrico) a nivel mundial son Ericsson, Huawei y Nokia, los cuales ocupan la mayor parte del mercado, venden su Hardware y dan soporte profesional al mismo. Los Operadores de cada país deciden con que proveedor implementar la tecnología que deseen instalar, modernizar o ampliar según las necesidades de cada uno.

4.2.1. ERICSSON

Telefonaktiebolaget LM Ericsson, comúnmente conocida como Ericsson (véase su logo en la figura 2), es una compañía multinacional Sueca dedicada a ofrecer equipos y soluciones de telecomunicaciones, principalmente en los campos de la telefonía, la telefonía móvil, las comunicaciones multimedia e internet. [7]

Figura 2. Logo ERICSSON [7]

La compañía fue fundada en 1876 por Lars Magnus Ericsson, originalmente como un taller de reparación de equipos de telegrafía. En los años 1990, Ericsson se convirtió en el fabricante líder de teléfonos celulares.

Actualmente, el grupo Ericsson se compone de tres unidades de negocio:

- Redes
- Servicios
- Multimedia

Ericsson ha reforzado su posición en varios países como principal suministrador de redes para los operadores móviles y ha enriquecido su oferta de soluciones —IMS (Internet Multimedia Subsystem; Softswitch), IP/Ethernet— para la evolución de las redes de los operadores de telecomunicaciones hacia entornos totalmente Internet y con nuevas estructuras que permitirán la evolución más eficiente hacia las redes de nueva generación.

4.2.2. HUAWEI

Huawei Technologies Co., Ltd. (véase su logo en la figura 3), es una empresa tecnológica multinacional China con sede en Shenzhen, provincia de Cantón, que provee infraestructuras de tecnologías de la información y la comunicación (TIC), equipos de telecomunicación, productos electrónicos de consumo, además de varios teléfonos inteligentes propios.

La compañía fue fundada en 1987 por Ren Zhengfei. Inicialmente centrada en la fabricación de conmutadores telefónicos, Huawei ha ampliado su negocio para incluir la construcción de redes de telecomunicaciones, proporcionando servicios operativos y de consultoría y equipos a empresas dentro y fuera de China, y la fabricación de dispositivos de comunicación para el mercado de consumo. [8]

Figura 3. Logo HUAWEI [8]

Huawei provee redes de telefonía fijas y móviles, comunicaciones de datos, redes ópticas, software & servicios y terminales telefónicos, incluyendo módems conmutadores, redes de acceso integradas, NGN, xDSL, transporte óptico, redes inteligentes, GSM, GPRS, EDGE, W-CDMA, CDMA2000, una serie completa de routers y conmutadores IP, videoconferencia y equipamiento a otros campos clave de la tecnología de telecomunicaciones.

Las soluciones de red centrales de Huawei que ofrecen softswitches móviles y fijos, además del registro de ubicación de origen de próxima generación y los subsistemas multimedia de protocolo de Internet (IMS). Huawei vende xDSL, red óptica pasiva (PON) y PON de última generación (NG PON) en una sola plataforma. La compañía también ofrece infraestructura móvil, acceso de banda ancha y enrutadores y conmutadores de proveedores de servicios (SPRS).

4.2.3. NOKIA

Nokia Corporation (véase su logo en la Figura 4), es una empresa multinacional de telecomunicaciones y tecnología con sede en el distrito de Keilaniemi, Espoo, Finlandia, presidida por Pekka Lundmark (presidente y director ejecutivo). Está integrada por dos grupos de negocios: Nokia Networks (Redes de telecomunicaciones) y Nokia Technologies.

Anteriormente era una empresa orientada principalmente a la fabricación de teléfonos móviles, siendo líder mundial en este sector entre 1998 y 2013. Sin embargo, sufrió una disminución de la participación del mercado como resultado de la creciente utilización de los teléfonos inteligentes de otros proveedores. [10]

Figura 4. Logo NOKIA [10]

Nokia además del desarrollo de dispositivos móviles, actualmente se dedica al desarrollo de tecnologías de comunicación móvil a nivel RAN, para ello fundo Nokia Networks.

Nokia Networks provee equipos de comunicaciones móviles para todo mercado considerable y protocolo, incluyendo TDMA, GSM, CDMA, W-CDMA, LTE y 5G.

Nokia Solutions and Networks proporciona la red inalámbrica y fija de infraestructura, comunicaciones y plataformas de servicios de redes, así como servicios profesionales a los operadores y proveedores de servicios. Se centra en redes de acceso de radio GSM, EDGE, 3G/W-CDMA, LTE, WiMAX y 5G.

4.3. OPERADORAS TELEFONICAS EN NICARAGUA

En Nicaragua existen principalmente 3 empresas operadoras que brindan servicio de telefonía móvil al consumidor: Claro, Tigo y Cootel y entre ellas 2 dominan el mercado Nacional Nicaragüense (Claro y Tigo). El Proveedor del servicio al Operador en estas 2 compañías es Ericsson. En Nicaragua predominan las estaciones base con tecnología Sueca, Ericsson realiza la instalación, modernización y soporte a la infraestructura Movil en Nicaragua.

La privatización del monopolio público de telecomunicaciones fue presentada como una solución al problema de las demandas de indemnización de propiedades confiscadas por el gobierno sandinista. Entre 1992 y 1994 Nicaragua logro la más alta tasa de inversión y modernización de las telecomunicaciones en toda Centroamérica, de tal forma que el patrimonio del operador público era de los más modernos de la región. [11]

En el año de 1992 surge Movistar como Nicacel, en marzo de 1997 Nicacel fue vendida a Bellsauth, utilizando el nombre legal de telefonía celular de Nicaragua y opero en condiciones de exclusividad hasta a finales del año dos mil dos; el 29 de octubre del 2004 Telefónica móviles cierra la adquisición del 100% de las operadoras de telefonía móvil de Bellsauth en Ecuador, Guatemala, Panamá, Venezuela, Colombia, Perú, Uruguay y Nicaragua. En enero de 2005 Telefónica Móviles cierra la compra de todas las operadoras de Bellsouth en Latinoamérica y en abril de ese mismo año unifica su imagen en 13 países bajo la marca Movistar.

En el país se aprueban nuevas Leyes de telecomunicaciones y se crearon organismos reguladores especializados, previos al proceso de privatización. En Nicaragua se optó por privatizar un monopolio horizontal y verticalmente integrado, con una cláusula de exclusividad por un periodo de 3 años, que incluía larga distancia nacional e internacional y la posibilidad de adquirir una licencia de telefonía móvil; la empresa ganadora estaría obligada a expandir la red y mejorar la calidad del servicio, así como también crear plataforma tecnológica.

A finales del año 2001 se entrega el 40% al consorcio sueco hondureño Telia Swedfel abm egatel EMCZ por un periodo de 20 años; en el 2004 el gobierno vende paquete de acciones restantes adjudicándolo sin proceso de licitación a la empresa mexicana America móvil del grupo Carso, en paralelo la misma empresa adquirió Megatel de honduras, convirtiéndose en la única accionista de enitel y en un operador con dos licencias en telefonía celular (Enitel y la de Sercom PCS); provocando reducción de manera significativa la intensidad de la competencia.

La inexistencia en ese entonces de una agencia de competencia capaz de haber puesto como condición a la compra de enitel, que América móvil se deshiciera de una de las licencias móviles represento un serio problema para el desarrollo de la competencia global en telecomunicaciones con relación a la evolución de tarifas en telefonía móvil, se trata en general de un mercado abierto a la competencia y en consecuencia normalmente sin obligación de informar tarifas.

En 2020, Nicaragua casi alcanzó los 6 millones de líneas móviles en un mercado del que solo participan Claro y Tigo, siendo esta última la que domina con 53 por ciento de participación, según los datos del Instituto Nicaragüense de Telecomunicaciones (Telcor). [12]

El país ha logrado una buena cobertura de los servicios móviles, con el 100 por ciento de los municipios con algún tipo de tecnología, el 85 por ciento de la población con cobertura de Internet móvil y el 45 por ciento de los municipios con LTE. En la Figura 5, se muestra la distribución de servicios y espectros de frecuencias que actualmente operan las compañías America Movil y Millicom bajo las marcas comerciales Claro y Tigo.

TELEFONÍA MÓVIL

Operador	Propietario	Servicios	Tecnología y Espectro
Claro	América Móvil	Telefonía y Banda ancha Móvil	700MHz UMTS/HSPA+ 850 MHz GSM/GPRS/EDGE 1900 MHz LTE 1700-2100 MHz
Tigo	Millicom	Telefonía y Banda ancha Móvil	1800 MHz GSM/GPRS/EDGE 850 MHz GSM/GPRS/EDGE - UMTS/HSPA+ - LTE 1900 MHz 1700-2100 MHz

Figura 5. Espectro y Tecnología en Nicaragua [12]

Es muy claro el monopolio en el marcado de Claro y Tigo y ya que ellos trabajan de la mano con Ericsson, este trabajo se centrará en brindar información y explicar procesos de atención de fallas sobre las RBS Ericsson.

V. CAPITULO II: ESTRUCTURA RED MOVIL

5.1. Arquitectura de la red móvil

A nivel de arquitectura de red, GSM (2G) y UMTS (3G) tienen muchas similitudes, el bloque de acceso cambia en sus Nodos Controladores, en el caso de GSM los recursos de las BTS son administrados por una BSC (Base Station Controller), en el caso de la red UMTS los recursos se administran por una RNC (Radio Network Controller), a nivel de estación base, en GSM se tiene como acceso a la red móvil una BTS (Base Transceiver Stations), en el caso de la red UMTS se conocen como Nodos B, sin embargo en el bloque del CN (Core Network) la infraestructura es básicamente la misma, se utiliza una MSC (Mobile Services Switching Center) para controlar la conmutación de circuitos para el establecimiento de las llamadas y se utiliza el SGSN (Serving GPRS Support Node) para enrutar los paquetes de datos a los diferentes usuarios que en cada momento se encuentra conectados, a continuación explico a grandes rasgos la función que tiene cada uno de los elementos dentro de una arquitectura de red celular.

A nivel de GSM el sistema de estación base (BSS) es responsable de garantizar todo lo relacionado con el correcto funcionamiento de la señal de radio. Es su responsabilidad lograr que el sistema de conmutación se abstraiga de los problemas relacionados con la atención al móvil. [13]

Sin embargo, no se profundizará en arquitectura GSM, sino en generaciones posteriores UMTS y LTE, que son la mayor implementación en la actualidad.

5.1.2. Red UMTS

A grandes rasgos, el sistema UMTS está dividido en dos grandes bloques lógicos:

- El núcleo de red (Core Network, CN) desempeña labores de control de tráfico, señalización, conmutación y encaminamiento. Además, hace posible la conexión de UMTS con otras redes de comunicaciones. Reutiliza varios elementos ya presentes en la arquitectura 2G y soporta tanto conmutación de paquetes como conmutación de circuitos.
- La red de acceso radio (UTRAN) se encarga de los aspectos de comunicaciones, tales como la gestión de los recursos radio, el control de potencia y el traspaso de llamadas. Sus elementos principales son los controladores de red (RNC), que se

encargan de gestionar una o varias estaciones base que dan cobertura a los terminales de usuario

Dado que la CN hereda elementos de la arquitectura 2G, es frecuente ver estaciones base GSM y UMTS coexistiendo dentro de una misma red móvil [14].

Una red UMTS pude ser visualizada desde varios ángulos, ya sea desde el punto de vista del usuario, desde el plano de gestión de red, o desde la función de cada uno de sus subsistemas explican María Victoria Farías y Diego Lucas Fernández en su trabajo titulado ANALISIS DE LA IMPLEMENTACION DE IUB FULL IP [15] para la Universidad de Aeronáutica de la Ciudad de Córdoba, Argentina. Justamente de este último punto se puede describir la red UMTS haciendo foco en cada uno de los diferentes elementos que la componen. La red UMTS puede ser dividida en 4 subsistemas:

- Equipamiento del usuario
- Red de Acceso de Radio (RAN)
- Red Core, incluidos los elementos de red para los distintos grupos de servicios (CN)
- Subsistema de gestión de red

La Figura 6 muestra a grandes rasgos las interfaces de conexión entre los distintos elementos que componen la red móvil a nivel RAN y los dos elementos del CORE: conmutación de circuitos (CS) y de conmutación de paquetes (PS)

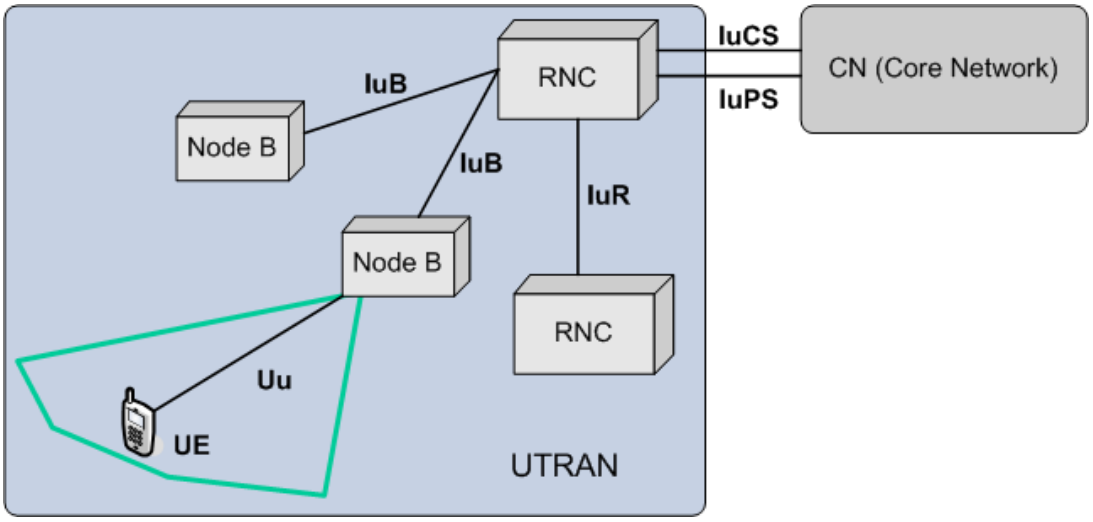


Figura 6. Arquitectura redes 3G [14]

5.1.2.1. Subsistema Equipamiento de Usuario (UE)

El equipamiento del usuario tiene a su vez una sub-estructura. La tarjeta universal que contiene el circuito integrado (UICC) similar a la SIM en GSM. Esta se ubica en el equipo móvil (ME) el cual es independiente del cliente. Tradicionalmente el UE o equipamiento de usuario era una única pieza, la red UMTS nos brinda la posibilidad de que un UE contenga interconectadas varios ME compartiendo la misma UICC, como, por ejemplo, una red de laptops [15].

La transmisión de radio, el control del recurso de radio, el soporte de QoS de datos son funciones que corresponden al Terminal Móvil (MT) el cual puede o no estar integrado del teléfono móvil o formar parte de la misma UICC (Universal Integrated Circuit Card), permitiendo a una laptop, Tablet, PC con USB 3G o Smartphone adoptar las funciones de UMTS. La UICC contiene información del cliente para varias tecnologías: para aplicaciones de GSM (igual que la tarjeta SIM), para aplicaciones UMTS e información de identidad necesaria para el servicio multimedia IP. Una característica importante de la UICC es la inaccesibilidad por parte del cliente a los datos contenidos en la tarjeta, pudiendo ser manipuladas únicamente por el operador que vende la UICC.

En la figura 7 se muestra los posibles terminales que conforman el equipamiento de usuario UE y su conexión hacia la red de acceso.

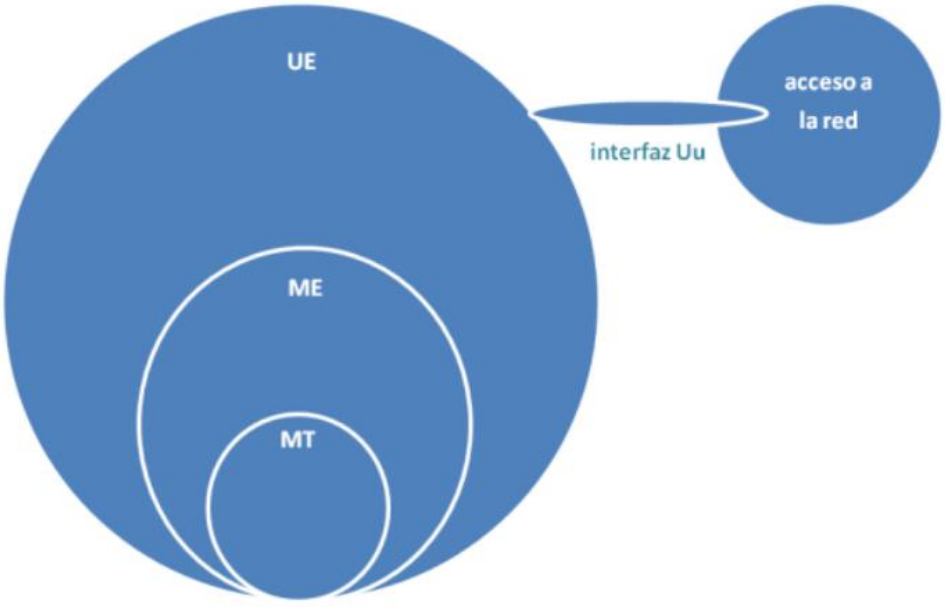


Figura 7. Equipamiento de Usuario [15]

5.1.2.2. Red de acceso de radio RAN

UTRAN

La UTRAN es la red de acceso para la tecnología 3G, se encuentra compuesta por los RNC (Radio Network Controller) y los Nodos B o Estación Base, los cuales, a como se muestra en la figura 8, se interconectan entre sí a través de la interfaz Iub. La interfaz de aire Uu permite a los UE poder ingresar a los servicios de red. Este conjunto recibe el nombre de RNS (Radio Network Sub-system).

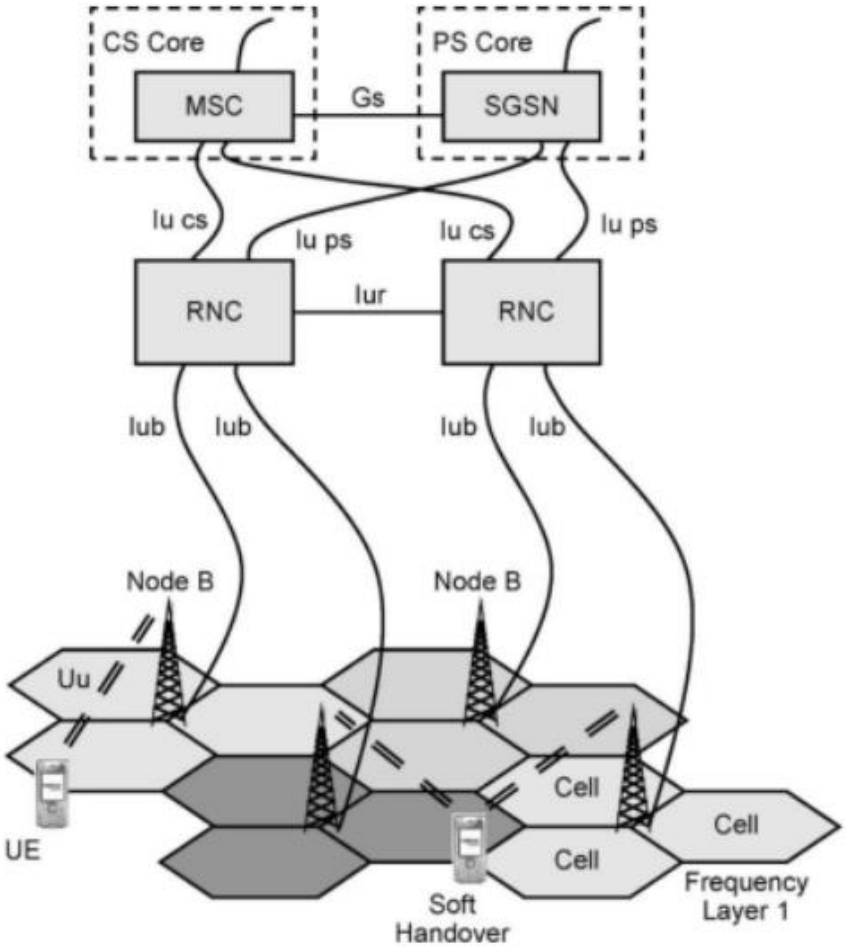


Figura 8. UTRAN [15]

Interfaz de aire Uu.

Esta interfaz es la localizada entre el equipo terminal y un nodo B. Por lo tanto, el medio de transmisión se encuentra basado en señales electromagnéticas a través del aire, utilizando técnica de acceso múltiple a fin de poder compartir el espacio radioeléctrico.

CDMA es una técnica de Acceso Múltiple por División de Códigos. Su origen proviene del entorno militar y se desarrolló a modo de optimizar otras dos técnicas de acceso que se basaban en la división de frecuencias (FDMA) y en la división de tiempos (TDMA). CDMA básicamente permite que se use todo el ancho de banda disponible, todo el tiempo requerido para cada canal, diferenciando estos últimos por diferencia de códigos. Se dio a conocer a WCDMA como solución de "espectro ensanchado" (la W de la sigla significa width – ancho). Este espectro fue generado a partir de la señal de banda base y una señal moduladora de un ancho de banda superior al de la banda base, utilizando un código de expansión que permite separar entre diferentes comunicaciones que comparten una misma portadora. En este caso el ensanchamiento se consiguió multiplicando la señal digital en banda base por una secuencia conocida por los extremos en comunicación. Esta secuencia posee una velocidad mucho mayor a la de banda base.

En WCDMA la información comparte todo el espectro de frecuencia con el resto de los canales (se pueden digitalizan entre 8 y 10 llamadas como máximo), diferenciándose a través de un código único. Esta tecnología se creó para el tratamiento de datos.

Nodo B

Un Nodo B puede dar servicio a una o más células a fin de conectar a los dispositivos de los usuarios, a través de la interfaz de aire Uu, con la red. Posee otras funciones como la realización de mapeos de la información, tanto de aquella que provienen de los terminales de usuarios en términos del ancho de banda y Qos (calidad de servicio), como aquella que definen los recursos de la interfaz Iub.

Interfaz Iub

A diferencia de la interfaz Uu que trata de una conexión directa a través de ondas radioeléctricas, la interfaz Iub es mucho más compleja ya que nunca un nodo B se conecta directamente a una RNC, dicha interfaz Iub es una interfaz lógica para

interconexión del Nodo B y los componentes de la RNC de UTRAN y en la cual intervienen varios protocolos a nivel de trasmisión de datos y señalización móvil a como se aprecia en la figura 9.

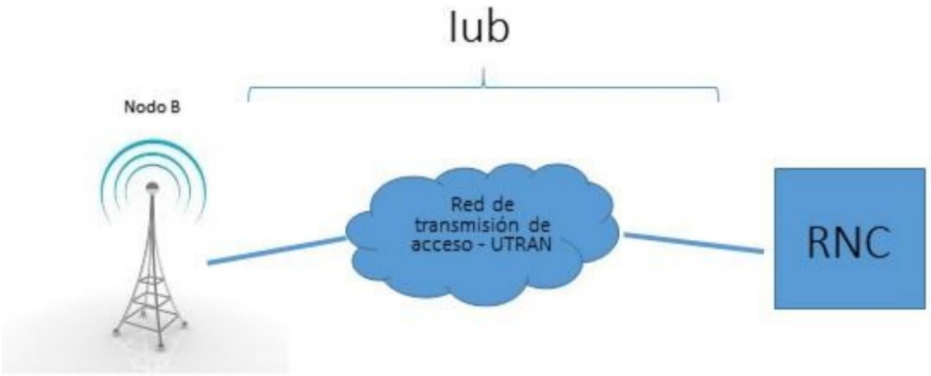


Figura 9. Interfaz IUB [15]

Es muy común que una sola RNC controle cientos de nodos B. Las RNCs suelen estar ubicadas en los centros de conmutación de las operadoras, mientras los Nodos B se encuentran repartidos en todo el territorio al que se le quiere dar servicio UMTS. Esta aclaración es validad para demostrar que en muchos casos existen grandes distancias entre un componente y otro, lo que requiere el despliegue de una red de transporte/transmisión de área extensa (WAN) que una a cada nodo B con su respectiva RNC. A esta red se le llama Red de Trasmisión de Acceso o UTRAN

Una de las características de la Iub, es que utiliza como tecnología de trasporte ATM o IP. Respecto a esto el grupo 3GPP publicó en la Release 99 (año 2000) la primera red UMTS juntos con todas sus características, y en una posterior especificación (UMTS Core Network based on ATM Transport – Spen 23925) se definió como núcleo de red a la tecnología ATM como así también la tecnología de transporte. Sin embargo, a partir de la Release 5, se permitió utilizar tanto ATM como IP para transportar los datos de usuarios y la señalización del Nodo B proveniente de la RNC a través de la interfaz Iub. Dicha interfaz permite transportar 2 tipos de información, la información Móvil-Red correspondiente a la señalización o tráfico de usuario, la cual intercambian los móviles y nodos de ingreso al CORE (pueden ser MSC para el caso CS o SGSN para el caso PS); la señalización UTRAN que abarca la información entre NBs - RNCs, y entre RNCs - CORE Network y entre las mismas RNCs.

RNC – Radio Network Controller

La RNC es la Unidad Central de Control de una RNS. Se encuentra conectada a través de distintas interfaces basadas en tecnología ATM. La interfaz Iub conecta con los Nodo B mientras que la Interfaz Iur conecta hacia otras RNC. Por último, utilizó la interfaz Iu para conectar con el Core Network (CN), que puede ser dividida en Iu-PS y Iu-CN. [16]

Algunas de las funciones que cumple la RNC son:

- Mantenimiento de conexión móvil-red troncal: La red de acceso se encarga de transportar los datos de usuario y señalización entre el móvil y la red troncal. Un aspecto importante es la gestión de los recursos de la red de radio para brindar garantía de calidad de servicio extremo a extremo requerida por los usuarios. Para esto, la red se encarga de traducir los parámetros de calidad de servicios del usuario (por ejemplo, tasa de bit, retardo), a parámetros de calidad de servicio del enlace radio (por ejemplo, intervalos de transmisión, tamaño del bloque de radio, esquema de codificación), que la red de acceso debe cumplir para garantizar la calidad.
- Control de acceso al medio: La red de acceso de radio, en conjunto con el móvil son los encomendados a realizar el control de acceso de acuerdo a las reglas de la red troncal.
- Gestión de recursos radio: A través de las funciones de control de potencia, handover, gestión de la asignación de canales/códigos, la red radio se logra asignar y mantener de forma óptima los recursos de radio utilizados por el móvil. Estos recursos dependen principalmente de la aplicación a utilizar, ya sea voz, datos o video. Tradicionalmente, han existido canales de radio dedicados y compartidos, los cuales se utilizaban dependiendo del tipo de comunicación (voz/datos/video) y de los parámetros de calidad de servicio que ésta requería. Las mejoras e introducciones de nuevos canales radio son constantes en la evolución de estas redes, con el objeto de mejorar la eficiencia espectral y la calidad de servicio.
- Movilidad de radio: La red de radio es la encargada de gestionar la movilidad, como parte de la gestión de recursos radio, cuando el móvil está conectado a la red, a través de procedimientos de registro, gestión de los estados de movilidad, paging, traspasos, de forma tal de mantener al usuario conectado y utilizar sólo los recursos necesarios de acuerdo a su perfil de movilidad y actividad.
- Manejar los recursos de transporte de la interfaz Iu.
- Manejo de la información del sistema y de los horarios de la información del sistema.

- Manejo de tráfico en los canales comunes.
- Combinación en la Macro diversidad y división de las tramas de datos transferidas sobre muchos Nodos B.
- Asignación de códigos de canalización en el enlace de bajada.
- Control de admisión.
- Manejo del tráfico en los canales compartidos.

5.1.2.3. Core Network (CN) o Red Troncal

La red troncal debe gestionar la información tanto de voz como de datos que genera la red de acceso. Gracias al protocolo SS7 denominado MAP (Mobile Application Part) UMTS pudo utilizar los mismos estándares que GSM dentro de la red troncal, es decir, las redes troncales GSM, UMTS y GPRS pudieron comunicarse entre sí para ofrecer servicios a los usuarios. El CN se encuentra compuesto de 2 grandes dominios, la MSC (Mobil Swiching Center) y SGSN (Serving GPRS Support Node). Tanto RNS y BSS conectan a la misma MSC. Ambas son piezas centrales para la conmutación de circuitos y conmutación de paquetes respectivamente.

El MSC cuenta con diferentes interfaces para conectar a la red PSTN y a través de esta se transporta el tráfico como señalización.

La MSC es la pieza central de la red basada en conmutación de circuitos. A ella se puede conectar tanto la red GSM como UMTS hacia la red Fija. El MSC es el responsable de realizar la trasmisión de voz, datos y servicios de fax así como Servicios de Mensajes Cortos (SMS) y desvío de llamadas.

Para el caso de GSM, la información de datos y fax debe ser enviada una vez codificada digitalmente al MSC. En este último la señal se debe convertir a señal "analógica" (señal PCM de 64 kbit/s). La GMSC (Gateway MSC) se puede ubicar entre la PSTN y el resto de los MSCs de la red y su función consiste en rutear las llamadas entrantes al MSC correcto.

SGSN es una pieza central que se encuentra basada en la conmutación de paquetes, y conectado a la UTRAN mediante la interfaz Iu-PS y a la GSM-BSS mediante la interfaz Gb. Su responsabilidad es la entrega de paquetes de datos desde y hacia las estaciones móviles dentro de su área de servicio geográfica. Es además el encargado de enrutar y transferir paquetes, la gestión de movilidad (conexión / desconexión), y la gestión de enlace lógico, autenticación y funciones de carga.

GGSN (Gateway GPRS Support Node), es el encargado de traducir los paquetes que recibió de la red de internet u otras redes privadas. Los paquetes originados por móviles son encaminados a la red correcta por el GGSN.

Interfaces Iu

Esta interfaz se encuentra conectada a la red troncal con la red de acceso de radio UMTS (UTRAN). Es la interfaz central y la más importante para la 3GPP. Puede tener dos diferentes instancias físicas para conectar dos diferentes elementos de la red, dependiendo si se trata de una red basada en conmutación de circuitos (Iu-CS) o basada en conmutación de paquetes (Iu-PS). En el primer caso, a la interfaz Iu-CS, le corresponde servir de enlace entre la UTRAN y el MSC, mientras que la interfaz Iu-PS es debe encargar de conectar la red de acceso de radio con el SGSN de la red central.

Interfaz Iur

Es la interfaz destinada a unir las diferentes RNC entre sí y cuyo propósito es trasmitir datos de soft handover.

Network Switching Subsystem NSS

NSS es un subsistema a nivel del Core móvil que está conformado por elementos que interactúan entre sí para lograr la funciones que se le exigen a un sistema de telefonía móvil, como el establecimiento de la llamada, registro de la llamada, autenticación de usuarios y supervisión de la red, a continuación, detallo cada uno de estos elementos y su rol en la red:

- MSC (Mobile Services Switching Center): Es el componente central del NSS y se encarga de realizar las labores de conmutación dentro de la red, así como de proporcionar conexión con otras redes.

- GMSC (Gateway Mobile Services Switching Center): es un dispositivo traductor (puede ser software o hardware) que se encarga de interconectar dos redes haciendo que los protocolos de comunicaciones que existen en ambas redes se entiendan, por ejemplo, con la telefonía fija.

- AuC (Authentication Center): se encarga de la autentificación de los usuarios (utilizando el IMSI del módulo SIM).

- EIR (Equipment Identity Register): proporciona seguridad a nivel de equipos válidos. Contiene una base de datos con los IMEI de todas las MS autorizadas en la red. Si una MS cuyo IMEI no está en el EIR trata de hacer uso de la red se le rechaza.

- GIWU (GSM Interworking Unit): sirve como interfaz de comunicación entre diferentes redes para comunicación de datos.

- OSS (Operation Support Subsystem): controla y monitoriza la red GSM

- Home Location Register (HLR): base de datos distribuida (única por red GSM) que contiene información sobre localización y características de los usuarios conectados a cada MSC.

- Visitor Location Register (VLR): contiene toda la información sobre un usuario de otra red necesaria para que dicho usuario acceda a los servicios de red (información extraída del HLR y MSC).

En la figura 10, se muestra todas las conexiones mencionadas hacia la MSC en un esquema GSM, el mismo es replicado para UMTS, con la salvedad que la red de acceso UTRAN estará compuesta por el Nodo Controlador RNC y el Nodo B como último elemento de control a nivel de acceso antes del usuario.

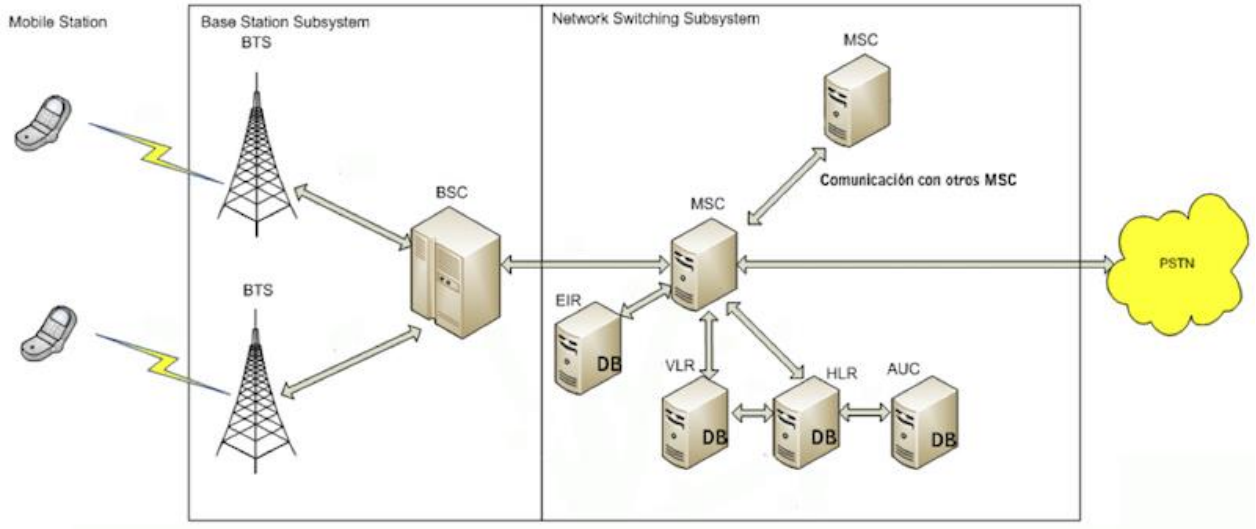


Figura 10. Network Switching Subsystem (NSS) [17]

PS Core Network

La red central PS consta de dos partes, la red central tradicional del Servicio general de paquetes de radio (GPRS) y la nueva red central del Sistema de paquetes evolucionado (EPS). La red central de PS conecta suscriptores móviles a redes de paquetes de datos (PDN), como Internet, redes corporativas o redes de servicios de operadores. [18]

En figura 11, se muestra un diagrama de los elementos que conectan hacia SGSN para generar el flujo de tráfico de datos hacia la red móvil:

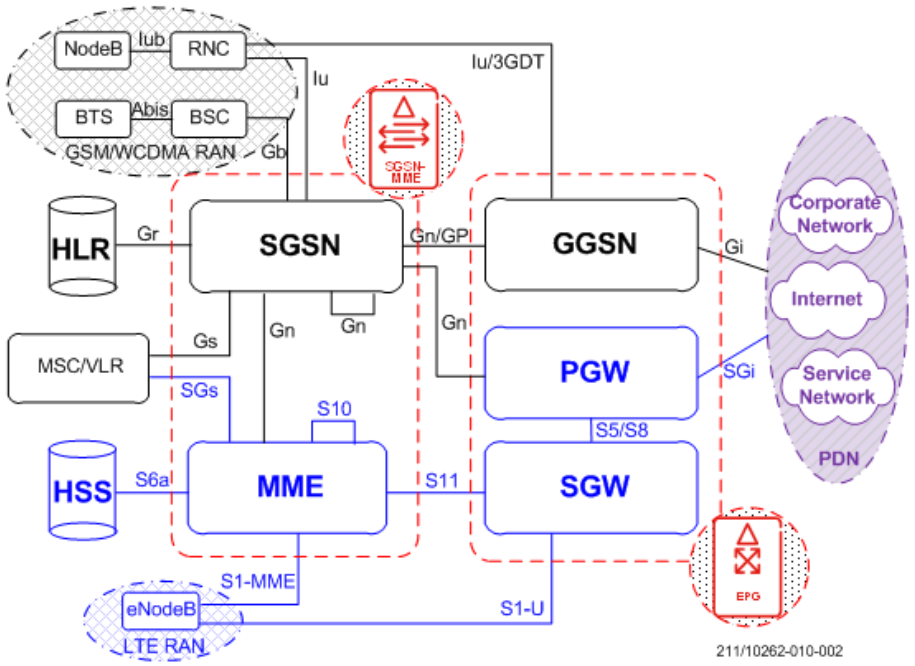


Figura 11. PS Core Network [18]

Las entidades lógicas y las interfaces se muestran en negro y forman una red 2G/3G, mientras que los recuadros azules y las líneas en la Figura muestran las partes relacionadas con LTE/EPC. La red LTE/EPC puede considerarse como una extensión y evolución de las redes 2G/3G existentes. Desde la perspectiva de la implementación del nodo, no existe un límite estricto entre las dos redes. Las entidades lógicas correspondientes de las redes GPRS y EPS se pueden implementar simultáneamente en los nodos centrales de Ericsson PS, como SGSN-MME y EPG; estos están marcados en rojo. Además, los nodos GPRS de Ericsson se pueden actualizar con la funcionalidad EPC solo mediante software.

La evolución de la red es compatible con los siguientes productos principales de Ericsson PS.

- Nodo de soporte de servicio GPRS: Entidad de gestión de movilidad (SGSN-MME) - El SGSN-MME actúa como SGSN para la red central GPRS, o como MME para la red EPC, o como una combinación de SGSN y MME.
- Evolved Packet Gateway (EPG) - EPG permite la combinación simultánea de las funciones de Gateway GPRS Support Node (GGSN), Serving Gateway (SGW) y PDN Gateway (PGW) en un nodo físico.
  Como parte de la evolución de EPC, la arquitectura de control de política y cobro (PCC), es proporcionada principalmente por la función de reglas de política y cobro (PCRF), la función de aplicación de política y cobro (PCEF), la función de aplicación (AF) y las entidades del Sistema de cobro en línea/fuera de línea (OCS y OFCS). La solución Service-Aware Charging and Control (SACC) de Ericsson proporciona funciones de PCC completas y validadas basadas en los siguientes productos principales de Ericsson PS:
- Controlador de políticas consciente del servicio (SAPC): SAPC implementa la función PCRF tal como se describe en los estándares 3GPP PCC.
- Nodo de soporte consciente del servicio (SASN): SASN es una entidad PCEF independiente y se puede implementar en la interfaz Gi/SGi entre las funciones EPG y Internet Security y Gateway.
- EPG: como plataforma de puerta de enlace combinada para GGSN, SGW y PGW, la EPG contiene una función PCEF para la arquitectura PCC. La función de conocimiento del servicio en la solución SACC se basa en una inspección avanzada de paquetes disponible integrada en EPG o independiente en SASN.

5.1.3 Red LTE

La arquitectura de 4G es conocida como la Evolved Packet System (EPS). La EPS es una evolución de la arquitectura de GPRS con una arquitectura simplificada y una red todo IP (all IP network, AIPN). El sistema EPS está implementado por una parte radio, la LTE y la core network, la System Architecture Evolved (SAE). [19]

Al igual que en GSM y W-CDMA, en el LTE coexisten 2 subsistemas que se encargan de controlar todo el flujo de tráfico móvil: RAN (red de acceso conocida en LTE como E-UTRAN) y CORE (EPC), cada uno de ellos con elementos que cumplen funciones específicas e indispensables en la red.

En la figura 12 muestra los dos subsistemas de la red LTE: E-UTRAN para el acceso y el EPC para el Core, así como las interfaces lógicas de conexión entre cada elemento.

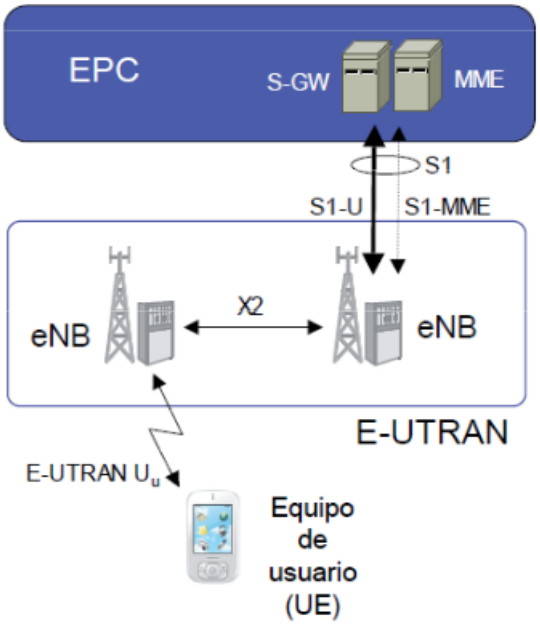


Figura 12. ARQUITECTURA 4G [19]

La red de acceso E-UTRAN está conformada por: User Equipment (UE), Evolved Node B (eNodeB).

La core network (EPC), está compuesta por: Mobility Management Entity (MME), Serving gateway (SGW), Packet Data Network (PDN) gateway (PGW), Policy and Charging Rules Function (PCRF)

E-UTRAN

EUTRAN consta solo de eNodeB en el lado de la red. El eNodoB realiza tareas similares a las realizadas por los nodosB y el RNC (controlador de red de radio) juntos en UTRAN. El objetivo de esta simplificación es reducir la latencia de todas las operaciones de interfaz de radio. Los eNodeB están conectados entre sí a través de la interfaz X2 y se conectan a la red central de conmutación de paquetes (PS) a través de la interfaz S1. [20]

Sus elementos son:

- User Equipment (UE): el terminal de usuario.
- Evolved Node B (eNodeB): Estación que se encarga de proporcionar la interfaz radio.

La interfaz entre la eNodeB y la core network se realiza mediante el protocolo S1-U para los datos de usuario y S1-MME para información de control (handovers, paging, mensajes Non-Access Stratum).

También hay conexión directa entre diferentes eNodeB mediante la interfaz X2 como se muestra en la figura 13.

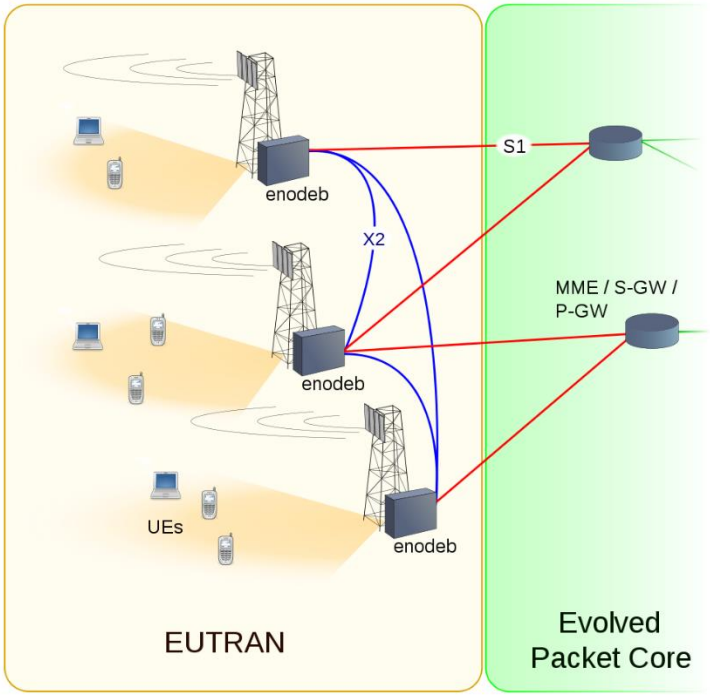


Figura 13. EUTRAN [20]

EPC

EPC es una innovación que depende de las tecnologías GSM/EDGE y UMTS/HSPA, puede aumentar la capacidad y la velocidad utilizando una interfaz de radio diferente junto con mejoras en la red central. EPC se refiere a una arquitectura de red central que agrega redes de acceso que incluyen LTE, 3G o 2G. Tiene los siguientes elementos que lo conforman:

- Mobility Management Entity (MME): Nodo principal de control que tiene asignadas multitud de funciones como el tracking del UE o paging entre otras, es un componente clave del Evolved Pack Core (EPC) definido por estándares para LTE. Proporciona gestión de sesiones de movilidad para la red LTE y admite autenticación de suscriptor, roaming y traspasos a otras redes.
- Serving gateway (SGW): Está en la frontera entre el Radio Access Network (RAN) y la core network y se encarga de gestionar la movilidad. Este Nodo maneja el tráfico de datos del usuario, pero no es responsable de los datos de señalización utilizados. Transporta datos IP desde los UE a la red principal LTE. La SGW también enruta los paquetes IP entrantes y salientes para una mejor colaboración del sistema y sirve como ancla para el UE cuando se mueve de un eNodeB a otro.
- Packet Data Network (PDN) gateway (PGW): Da servicio y conectividad con redes de paquete externas. es el nodo de red que conecta el EPC a redes IP externas. Lo que hace el PGW es enrutar paquetes hacia y desde redes IP externas. Más allá de eso, también asigna una dirección IP a todos los UE y aplica diferentes políticas con respecto al tráfico de usuarios de IP, como el filtrado de paquetes.
- Policy and Charging Rules Function (PCRF): Se encarga de tarifar. Es el nodo de software designado en tiempo-real para determinar reglas de políticas en una red multimedia. El PCRF es la parte de la arquitectura de red que reúne información desde y hacia la red, los sistemas de soporte operacional, y otras fuentes (como portales) en tiempo real, permitiendo la creación de reglas y luego tomando decisiones de política automáticamente para cada suscriptor activo en la red. Tal red podría ofrecer servicios múltiples, niveles de calidad de servicio (QoS), y reglas de tasación.

  El PCRF puede proporcionar una solución agnóstica a la red (para redes cableadas e inalámbricas) y también puede habilitar enfoques multi-dimensionales que ayuden a crear una plataforma lucrativa e innovadora para los operadores, se puede integrar con plataformas diferentes como facturación, tasación, índice de audiencia y base de datos de suscriptor o también puede ser desplegado como entidad autónoma. [21]

PCRF juega una función clave en VoLTE como mediador de recursos de red para las redes IP Sistemas Multimedia para establecer las llamadas y asignar el ancho de banda al originador de la llamada con atributos configurados. Esto habilita al operador a ofrecer servicios de voz diferenciados a su(s) usuario(s) cobrando una prima.

Los operadores también tienen la oportunidad de utilizar PCRF para priorizar las llamadas a números de emergencia en las redes de siguiente generación.

En la red troncal, a como es mostrado en la figura 14, el PGW está conectado con el SGW mediante la interfaz S5 si es del mismo operador o S8 si es de un operador diferente. En este interfaz se implementa el protocolo GTP-U (GPRS Tunnelling Protocol-User) para transportar datos del PGW al SGW. También existe el túnel GTP-C el cual transporta información de control.

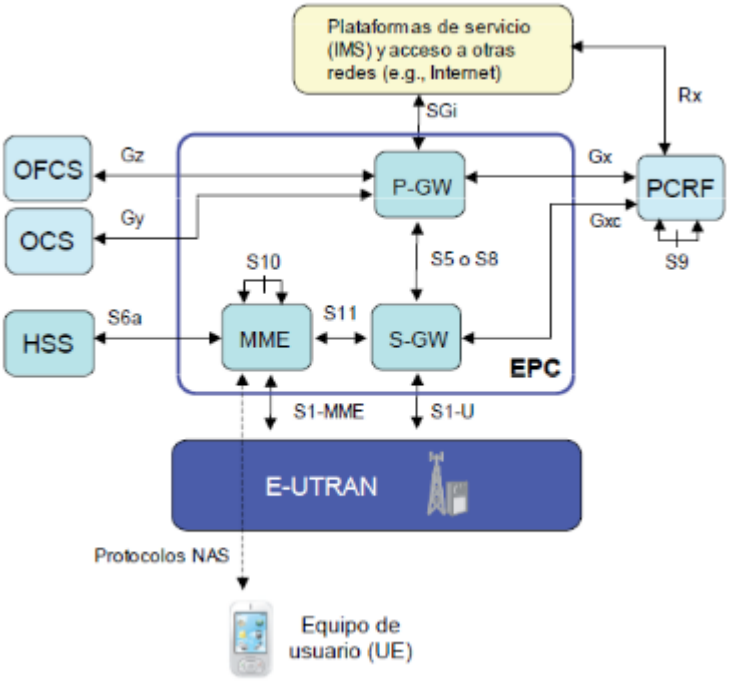


Figura 14. Conexiones EPC [19]

En EPC existe una entidad llamada Home Subscriber Service (HSS), que reune funcionalidades de los sistemas predecesores como el Home Location Register (HLR) y el Authentication Center (AuC).

El HSS está conectado con el MME para el mantenimiento de la información de gestión de la información o la autorización de acceso a la red LTE entre otras. La interfaz S6a que se utiliza para conectar el MME con el HSS, utiliza el protocolo

Diameter orientado a conexión (como TCP) y que es una evolución del protocolo RADIUS.

EPS tiene una red cuya transmisión es orientada a conexión, por lo que necesita de una conexión virtual entre dos puntos. Esta conexión virtual se llama EPS Bearer el cual provee de un servicio con una cierta calidad (QoS).

La figura 15 muestra una comparación a nivel del subsistema Core en las redes UMTS y LTE. En ambos casos se puede apreciar el nivel de redundancia. Para UMTS cada nodo controlador se debe conectar a ambos Core (CS y PS), en el caso de LTE como no existe un controlador a nivel de RAN, todos los eNode B se conectan directamente a los MME de la red.

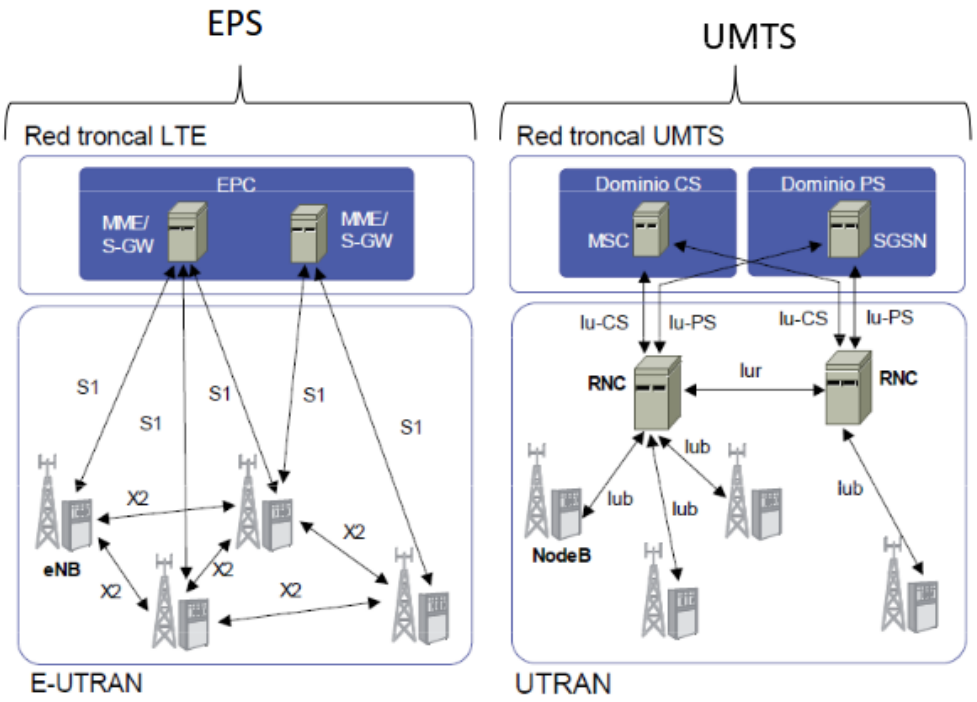


Figura 15. Comparativa E-UTRAN vs UTRAN [19]

5.2. Arquitectura de RBS

La estación base de radio (RBS) es el nombre comercial dado a la familia de estaciones base desarrolladas por Ericsson, que normalmente constituyen una parte importante de la red de acceso de radio (RAN). La estación base de radio también es el nombre genérico que se utilizará en lugar de BTS (estación transceptora base), que generalmente denota la tecnología de estación base de radio de la era GSM. Para otros proveedores, se utilizan nombres de equipos específicos, como Huawei DBS (por ejemplo, Huawei DBS3900. "DBS" significa estación base distribuida) o estaciones base NSN Flexi. [22]

A lo largo de los años, todas las Estaciones Base de Telefonía Móvil desarrolladas por la multinacional (las tecnologías soportadas van desde IS136-TDMA hasta UMTS) se han vendido con este nombre, aunque el concepto de Radio Base es el de un transceptor que está destinado principalmente a servir como un enlace troncalizado.

Ericsson ha desarrollado a lo largo del tiempo tres principales grupos de RBS:

- Familia RBS2000
- Familia RBS3000
- Familia RBS6000

La figura 16, muestra los tipos de gabinetes de la familia RBS2000 [23], se caracterizó principalmente por manejar trafico GSM (2G).

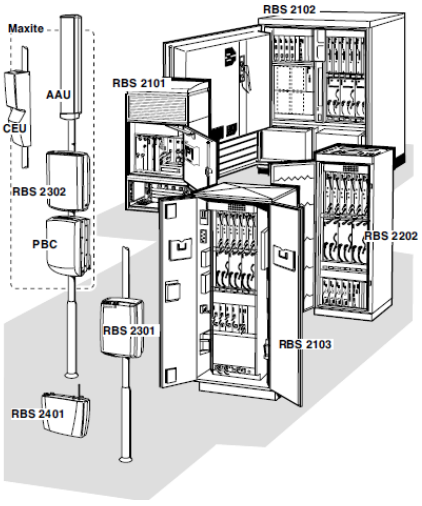


Figura 16. RBS 2000 [22]

El principal inconveniente de las familias de RBS2000 era que en su diseño las unidades de radios DTRU estaban ubicadas en el gabinete de la RBS y subía una línea de cobre (feeder) por la torre hasta llegar a conectarse al elemento pasivo (la antena), ello conllevaba mucho desgaste e inversión al momento de solventar fallas. Actualmente esta tecnología está en desuso en Nicaragua por lo que no se entrará en detalle en este trabajo monográfico.

Luego la surgió la implementación de RBS3000 [24], la cual fue una implementación para la tecnología UMTS (3G), inicialmente se diseñó bajo el mismo esquema de unidades de radio dentro del gabinete, sin embargo, se expandió gabinetes micros, sistemas indoor (edificios) y outdoor (sitios postes) y ello el principio de las unidades de radio fuera del gabinete, que luego será explotado en la siguiente generación de RBS. La generación de RBS3000 tiene un uso muy reducido en la actualidad, tampoco se entrará en mucho detalle.

Más adelante surge la familia de RBS6000, las más reciente y actualmente en uso en el territorio nicaragüense, se puede utilizar para GSM (GERAN) con tarjetas DUG, UMTS (UTRAN) con tarjetas DUW y LTE (eUTRAN) con tarjetas DUL/DUS.

El sitio RBS se puede interconectar con el resto de la RAN con una tarjeta SIU (Unidad de integración del sitio) que utiliza backhaul eléctrico, de microondas u óptico con el resto de la RAN y también proporciona conectividad Abis sobre IP para la estación base GSM.

5.2.1. RBS 6000

La familia de estaciones base RBS 6000 fue diseñada para satisfacer las necesidades y desafíos complejos que enfrentan los operadores hoy en día. RBS 6000 está construido con la tecnología del mañana y al mismo tiempo proporcionar compatibilidad con versiones anteriores con las altamente exitosas líneas de productos RBS 2000 y RBS 3000. [25]

Son Gabinetes en los que se pueden incluir tarjetas de la generación anterior como las DUG, DUW, DUS y tarjetas de nueva gama como las Base Band y equipos intermediarios como las SIU. Es el tipo de gabinete más utilizado en la actualidad, ya que da posibilidad de ampliación aprovechando los mismos recursos en cuanto a energía, clima y espacio en el gabinete.

Características clave de la serie RBS 6000:

- Camino a la sostenibilidad: la serie RBS 6000 garantiza una migración sin problemas a nueva funcionalidad y nuevas tecnologías con sitios y gabinetes existentes, proporcionando así un camino hacia ingresos y ganancias sostenidos.
- Energía bajo demanda: reingeniería de la fuente de alimentación e integración completa en el sistema fueron objetivos clave en el diseño de la serie RBS 6000. La fuente de alimentación inteligente proporciona energía bajo demanda que coincide exactamente a lo que se necesita en cada momento, asegurando así que el consumo se mantiene al mínimo absoluto.
- Multiestándar: Todas las estaciones base RBS 6000 admiten múltiples tecnologías de radios.
- Simplicidad integrada: Nuevos armarios polivalentes, una práctica común innovadora de construcción para todos los componentes, diseño modular y un nivel extremadamente alto de integración.

Figura 17. Familia RBS 6000 [25]

RBS 6201

La RBS 6201 es una estación base macro para interiores que forma parte de la familia RBS 6000 multiestándar de última generación que también incluye dos macro estaciones base, micro estación base, una configuración principal-remota y varias Unidades de Radio Remota (RRU).

Emplea un diseño de gabinete simplificado y un edificio modular innovador práctico, el RBS 6201 integra un sitio completo de alta capacidad en un solo gabinete. El gabinete contiene dos estantes para radio y todos los dispositivos de alimentación, transporte red y equipo de apoyo.

Los dos estantes para radio RBS 6201 se pueden equipar con prácticamente cualquier combinación de GSM, WCDMA y LTE, que están disponibles para todas las frecuencias. Un solo estante de radio puede proporcionar hasta 3 × 8 GSM o 3 × 4 MIMO WCDMA o 3×20 MHz MIMO LTE o una combinación de los estándares anteriores. Proporcionar un sitio multiestándar completo en un solo gabinete es posible gracias a la práctica de la construcción modular y un altísimo grado de integración.

Simplemente hay menos piezas, que se comparten en todas las tecnologías, haciendo que el sitio sea más fácil de instalar, administrar y mantener.

El concepto de sitio en gabinete está diseñado para soportar todas las tecnologías en prácticamente cualquier combinación a como es presentado en la figura 18. Esto significa que el tiempo en la expansión de la red es menos crítico y que hay menos riesgo en las decisiones de inversión, ya que la capacidad puede agregarse según sea necesario para la tecnología que está en demandando.

Figura 18. RBS 6201 [25]

Al igual que los demás miembros de la familia RBS 6000, el RBS 6201 proporciona espacio para 3U adicionales para una solución de red de transporte común que admite una amplia gama de tecnologías, incluidas IP nativa, Ethernet, Modo de transferencia asíncrono (ATM) y PDH/SDH.

Estrechamente integrado en el RBS 6201 hay una red y gestión de sitios que va mucho más allá de los sistemas tradicionales de operación y mantenimiento. Esto incluye la radio gestión de red para todas las tecnologías, red de transporte y sitio gestión con sistema de antena y control de potencia del sitio a través de un solo usuario interfaz, aumentando así aún más la sencillez para el cliente.

La fuente de alimentación completamente rediseñada para el sitio está completamente integrada en el RBS 6201. La energía se suministra bajo demanda utilizando algoritmos inteligentes para asegurar que la fuente de alimentación produzca solo la energía necesaria en cualquier momento dado y que las unidades se pueden apagar cuando no se necesitan, mejorando la eficiencia y disminuyendo el consumo de energía.

La figura 19 muestra a arquitectura de hardware flexible permite una variedad de implementaciones de sitios y consta de los siguientes componentes principales:

- Estante de radio: combinación de unidades de radio (RU) y unidades digitales (DU).
- Estante de alimentación - Unidades de fuente de alimentación (PSU) dimensionadas para el sitio.
- Estante de transporte: para equipos de red de transporte de hasta 3U de altura.
- Enclosures, incluido el sistema de climatización.

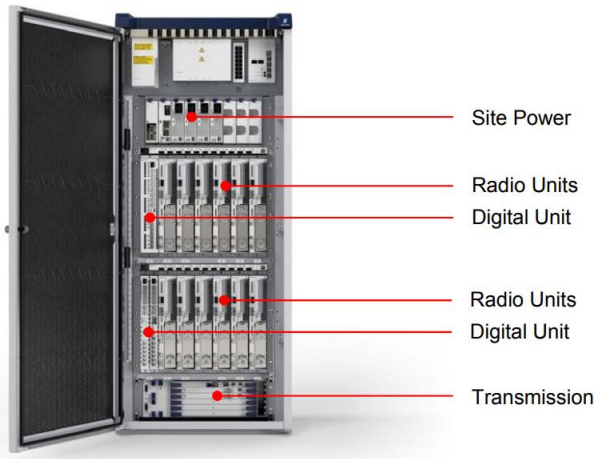


Figura 19. Arquitectura hardware RBS 6102 [25]

Estante de Radio

La familia RBS 6000 utiliza los siguientes componentes de radio principales para GSM,
WCDMA y LTE.

- RU – Unidad de Radio
  - Transceptor (TRX)
  - Amplificación del transmisor (TX)
  - Dúplex de transmisor/receptor (TX/RX)

- Filtrado de TX/RX
- Soporte de supervisión de antena

- DU – Unidad Digital
  - Procesamiento de controles
  - Distribución del reloj
  - Sincronización desde red de transporte i/f o GPS
  - Procesamiento de banda base
  - Interfaz de red de transporte
  - Interconexiones RU
  - Red de área local (LAN) del sitio e interfaz de mantenimiento

El estante de radio en las estaciones base RBS 6000 admite una amplia variedad de RU y DU para todas las bandas de frecuencia principales y cualquier combinación de Radiofrecuencia (RF) tecnologías (GSM, WCDMA o LTE). Cada estante de radio admite hasta 6 RU como el que se muestra en la figura 20 y un RBS 6201 completamente configurado pueden albergar hasta 12 RU.

Figura 20. Estante de radio [25]

Unidad de Radio

La Unidad de radio consta de un filtro y un amplificador de potencia multiportadora. La radio tiene un hasta 20 MHz de ancho de banda y hasta 60 W de potencia de salida, disponible con claves de activación de hardware en pasos de 20 W. El sistema de antena interactúa con un puerto TX/RX y un puerto RX. La radio (RUS) puede transmitir dos estándares simultáneamente.

La RU contiene puertos de coubicación, por ejemplo, para antena GSM/WCDMA compartición y conexión cruzada que minimiza el número de alimentadores si hay más se utiliza más de una RU por sector. El cable puente de la antena que conecta la RU debe tener un ángulo de 90 grados. curva conectora 7/16.

Unidad Digital

La Unidad Digital es la tarjeta principal de control en una RBS, por cada tecnología móvil cambia el nombre, pero la función es la misma, establecer un control sobre todas las interfaces que se conectan a los distintos periféricos que interactúan para hacer trabajar la RBS.

DUG

La Unidad Digital GSM (DUG) puede controlar hasta 12 portadoras GSM, Si se requieren más de 12 TRX, luego se puede instalar un DUG adicional en la radio estante y sincronizado con los otros DUG en el gabinete.

El DUG viene en dos variantes: DUG 10 es compatible con RUG, mientras que DUG 20
admite RUS y RRUS. El DUG admite la conexión cruzada de intervalos de tiempo individuales a específicos TRXs y extrae la información de sincronización del Pulse-Code
Enlace de modulación (PCM) para generar una referencia de temporización para el RBS.

La DUG contiene:
• Interfaz de transmisión E1/T1
• Procesamiento de banda base (DUG 20)
• Procedimientos de acceso al enlace en la concentración del canal D (LAPD) / multiplexación
• Doble banda, p. 3x2 900 + 3x2 1800 con un DUG
• Optimización Abis
• Multipunto (en cascada)
• Red de radio sincronizada, a través de un receptor GPS externo
• Sincronización de grupo de transceptores (TG)
• LAN del sitio

Para manejar IP, combinación con equipos opcionales como SIU, MINI-LINK u OMS.

DUW

La Unidad Digital WCDMA (DUW) viene en tres variantes, dependiendo de la demanda de capacidad. El DUW contiene la banda base, el control y la conmutación, así como las interfaces Iub y Mub. El DUW puede manejar diferentes mezclas de tráfico variables en el tiempo que consisten en datos de conmutación de circuitos de voz, conmutación de paquetes y datos de alta velocidad, como el acceso a paquetes de alta velocidad (HSPA).

Los recursos de banda base se agrupan en el DUW y el número de canales. Los elementos (CE) y la capacidad de datos de alta velocidad se pueden optimizar para adaptarse al operador requisitos por tipo de usuario y número de servicios.

La capacidad de banda base se agrupa independientemente de los sectores y frecuencias, y pueden existir hasta dos grupos de banda base (dos unidades DUW) en el mismo nodo.

La banda base cumple con los estándares 3GPP y está completamente integrada con el mismo sistema de operación y mantenimiento (O&M) que la familia RBS 3000. El software se puede descargar a través del Sistema de soporte de operaciones para Interfaces de Radio y Core (OSS-RC), ya sea localmente o a través de Radio Controlador de Red (RNC) y se almacena en la memoria no volátil del RBS.

La plataforma de software de la familia RBS 6000 brinda soporte genérico para el software de aplicación e incluye una plataforma de ejecución con sistema, ATM y transporte IP, e infraestructura O&M.

El DUW estabiliza la señal del reloj extraída de la red de transporte conexión o equipo GPS externo opcional y lo utiliza para sincronizar la RBS.

El DUW proporciona:

- Conectividad ATM
- Interfaz Gigabit Ethernet o (100/1000 Base-T Ethernet)
- Interfaz de red de transporte STM-1 canalizada
- Cuatro puertos E1/T1/J1 compatibles con IMA

Las interfaces adicionales y las configuraciones de la red de transporte están disponibles como opciones

DUL

La Unidad Digital para LTE (DUL) viene en una variante. El DUL contiene la banda base, control y conmutación, así como las interfaces S1 y Mub para LTE. El DUL admite diferentes mezclas de tráfico variables en el tiempo a través de la interfaz de datos de alta velocidad.

La capacidad de banda base se agrupa independientemente de los sectores y frecuencias, y pueden existir hasta dos grupos de banda base (dos unidades DUL) en el mismo nodo.

La banda base cumple con los estándares 3GPP y está completamente integrada con el
mismo sistema de operación y mantenimiento que la familia RBS 3000. El programa se puede descargar a través del OSS-RC, ya sea localmente o a través de una puerta de enlace de acceso, y es almacenados en la memoria no volátil de la RBS.

La plataforma de software de la familia RBS 6000 brinda soporte genérico para la software de aplicación e incluye una plataforma de ejecución con sistema, transporte IP e infraestructura de operación y mantenimiento.

El DUL estabiliza la señal del reloj extraída de la red de transporte conexión o equipo GPS externo opcional y lo utiliza para sincronizar la RBS.

El DUL proporciona:

- Conectividad IP total
- Una interfaz de red de transporte Gigabit Ethernet

Las interfaces adicionales y las configuraciones de la red de transporte están disponibles como opciones.

Sistema de energía RBS

El sistema de energía RBS es una solución moderna y eficiente para entregar energía a la RBS y en la evolución el sistema también podrá entregar energía a otros equipos en el sitio. El sistema utiliza Unidades de distribución de energía de alta densidad (PDU) controladas por disyuntores. Los algoritmos de software pueden apagar Unidades de CA y CC y otros componentes temporalmente fuera de uso para ahorrar energía y aumentar la capacidad de la batería.

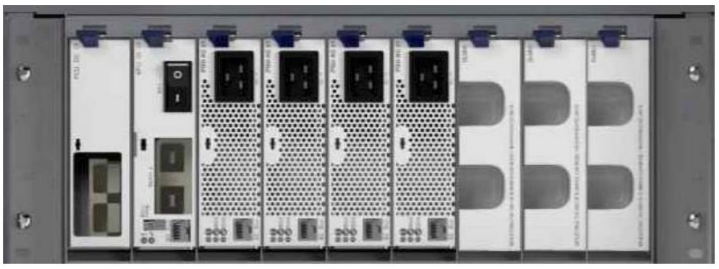


Figura 21. Sistema de energía RBS [25]

En la figura 21 se muestra un ejemplo de sistema de energía de un sitio, la cual elimina la necesidad de un sistema de energía por planta separada, este sistema puede cargar baterías.

El sistema de alimentación RBS puede utilizar alimentación de CA o CC. En corriente alterna, el sistema puede controlar la energía a unidades seleccionadas por medio de aplicaciones. Los rectificadores tolerantes (PSU AC) permiten grandes variaciones de voltaje, lo que elimina la necesidad de estabilizadores de tensión externos.

El RBS puede funcionar directamente con −48 V CC o mediante convertidores CC/CC (PSU CC), en +24 V CC o −60 V CC.

La eficiencia energética se ha mejorado mediante:

- Nuevo sistema de energía RBS con una eficiencia mejorada
- Funcionamiento en espera inteligente de una o más fuentes de alimentación
- Apagado selectivo de unidades

Las siguientes soluciones de respaldo de batería están disponibles para el RBS 6201.

BBU 6201

En caso de necesidades moderadas de respaldo de batería, se puede instalar una pequeña unidad de respaldo de batería ubicada bajo el RBS. Esto significa que un sitio completo, incluido el transporte el equipo de red, la energía y el respaldo, se administra en un RBS normal. La capacidad de la batería del sistema va desde 48V/40 Ah hasta 48V/190ah.

La BBU actúa como un marco base de la RBS y, por lo tanto, agrega muy poco trabajo a
la instalación del sitio. La BBU está preparada para una rápida y fácil conexión a el RBS.

BBS 6201

Para requisitos de respaldo exigentes, se recomienda un bastidor de batería más grande (tamaño RBS) privilegiado como el que se muestra en la figura 22. El BBS 6201 puede admitir hasta 680 Ah (−48 V) en un gabinete. 680 Ah da hasta 18 h de tiempo de respaldo. Varios gabinetes RBS pueden compartir la capacidad de un BBS.

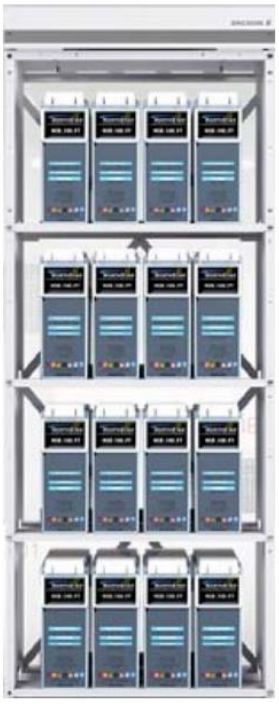


Figura 22. BBS [25]

Sistema de clima

El principio básico para el sistema climático es que cualquier unidad que necesite refrigeración tiene que solicitarlo a la Unidad de Control de Soporte (UCS). La principal ventaja de esto es que los ventiladores en el sistema de enfriamiento siempre funcionan a un nivel optimizado, lo que significa que, para cualquier

condición operativa dada, el RBS tiene un mínimo Consumo de energía con mínima generación de ruido.

La SCU tiene las siguientes funciones:

- Control de la velocidad y el estado del ventilador
- Interfaz para detector de humo, alarmas externas, lámpara de gabinete, interruptor de puerta y calentadores.
- Generar señal de arranque en frío
- Memoria del gabinete
- Puertos de bus EC protegidos contra transitorios para conexiones externas

La SCU se comunica a través del bus EC.

Estante de transporte

Con la introducción de la familia RSB 6000, hay soporte totalmente integrado para cualquier tipo de medio de red de transporte (microondas, fibra óptica o cobre) en combinación con varias tecnologías (IP/Ethernet, ATM, PDH/SDH, next gen SDH, xDSL, etc.), esquemas de redundancia, métodos de agregación y otras funcionalidades que soportan la elección de solución del Operador.

En figura 23 se muestra el espacio dentro del gabinete definido para la instalación de los equipos de transmisión.

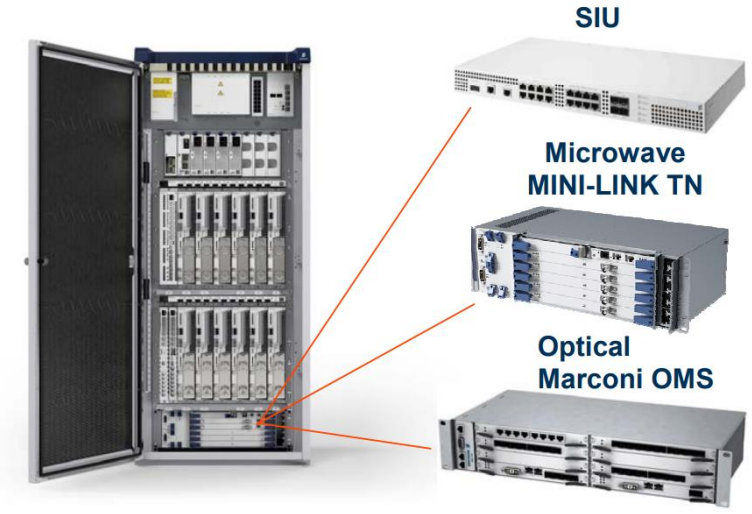


Figura 23. Estante de transporte [25]

Dado que la solución de backhaul móvil del operador suele ser única y depende de los requisitos del Operador y las condiciones del mercado, el RBS 6000 se

proporciona con espacio extra que se puede equipar con una amplia gama de alternativas soluciones de transporte mediante la cartera RAN-Transport de Ericsson. Unidad de Integración de sitio (SIU), MINI-LINK y Marconi OMS. Estos productos son parte de Solución IP RAN de Ericsson.

El SIU es un enrutador de sitio móvil de 1U de alto y 19 pulgadas de ancho. La Unidad de Integración del Sitio (SIU) actúa como una puerta de enlace del sitio celular que combina y optimiza todo el tráfico del sitio para maximizar el uso de los recursos de backhaul. Además, admite la conexión de vigilancia moderna basada en Ethernet, alarma y otros equipos del sitio sin requiere una línea adicional al sitio. Hacia la red de backhaul que soporta Redes Ethernet, IP y PDH con circuitos simples y redundantes.

Ejemplos de aplicaciones para la SIU son:

- Conectividad Local Abis

Todo el tráfico de voz GSM local se conmuta localmente en SIU, lo que reduce ancho de banda de backhaul con 100% para este tráfico.

- Transporte compartido

Todos los RBS (GSM, WCDMA y LTE) en el sitio comparten dinámicamente el ancho de banda de backhaul disponible. Esto permite al Operador lanzar servicios HSPA con un aumento mínimo de la capacidad de backhaul.

- IP sobre E1/T1

Hace posible implementar WCDMA Iub IP y LTE en todas partes en la red, incluso cuando los servicios Ethernet no están disponibles. Conjunto con Transporte compartido esto proporciona una manera muy eficiente de lanzar HSPA y LTE en todas partes.

- Puerta de enlace de seguridad

Protege todo el tráfico del sitio con IPSec. También permite la tunelización eficiente de tráfico a través de la red de proveedores de servicios.

- Enrutador de sitio celular

Capacidad de enrutamiento y VLAN para priorizar el tráfico habilitado con QoS sobre red de retorno.

MINI-LINK TN tiene una oferta completa con unidades interiores para respaldar todo lo necesario configuraciones de sitio desde pequeños nodos de borde hasta agregaciones más complejas nodos. La solución es flexible para llevar cualquier

protocolo (Ethernet, ATM, SDH y PDH) e integrado con potentes mecanismos de protección. Como resultado, el MINI-LINK TN combina bien con la familia RBS 6000 en capacidad y funcionalidad.

Ericsson complementa su tecnología de microondas con una presencia líder en el mercado de redes ópticas. La familia Marconi OMS permite al Operador para construir una infraestructura de transporte robusta donde esté disponible la fibra oscura. Se admite una amplia gama de topologías de red, desde estrella hasta en malla.

Los productos OMS 800 (Access-Edge) y 1400 (Metro-Edge) son dispositivos multiservicio (basados en tecnología Ethernet y TDM) para aseo y transporte de tráfico de paquetes de datos y voz (TDM) en una Red de Acceso Metro.

Los productos OMS 800 son soluciones pequeñas y compactas (1U) con transporte de enlace ascendente basado en NG-SDH con Ethernet. OMS 1410 es una solución híbrida compacta (2U) que puede tener un enlace ascendente basado en SDH o Ethernet.

VI. CAPITULO III: MONITOREO Y ATENCION DE ALARMAS RAN

6.1. Modelo NOC - Campo

Cuando los Operadores de telefonía móvil tienen una red en producción, es vital importancia mantenerla operando con el mayor índice de disponibilidad, esto significa que se brinde el mejor servicio posible el mayor tiempo posible para que la experiencia del usuario final sea acorde a sus expectativas o incluso mejor y mantenga preferencia y fidelidad sobre otros operadores.

Es por ello es que resulto de vital importancia crear un modelo en el cual las fallas que produzcan en la red sean atacadas rápidamente, con soluciones inteligentes y que se mejoren las debilidades de la misma en cada oportunidad. Para ello el Modelo más utilizados es tener un Centro de Control de red sobre el cual recae la supervisión y monitoreo de la red en busca de fallas potenciales, fallas menores y fallas críticas, lo que hoy en día se conoce como NOC (Network Operation Center) también llamado Centro de Operación de red o Centro de Control de red (CCR) y adicional al monitoreo remoto se tienen la necesidad de atacar en campo las fallas detectadas por el NOC, corregir las averías luego del reporte para conseguir un restablecimiento oportuno de la señal, para ello se creó un área conocida en los operadores telefónicos como Operación y Mantenimiento a la red (O&M).

Las responsabilidades que tiene cada una de las áreas indicadas (NOC, O&M) difiere de cada Operador según sus propios modelos y asignación de tareas. El objetivo siempre es reducir los tiempos de atención de fallas, es por ello que se trata de optimizar los recursos y automatizar los procesos mediante herramientas de gestión de incidencias que ayudan a ambas áreas a detectar fallos.

En Nicaragua Existen dos Operadores principales y un tercero con menor desarrollo en el servicio de telefonía móvil, todos utilizan un Modelo NOC – Campo para atención de averías, de acuerdo a sus políticas internas algunos se exigen más para el cumplimento de los KPI de su red, otros administran sus recursos y atienden las averías bajo protocolos un poco más aplazados, pero el objetivo es el mismo, mantener la operatividad de la red.

6.1.1 Network Operation Center (NOC)

El centro de operaciones de red (NOC) se refiere a una ubicación centralizada donde se lleva a cabo el monitoreo y la gestión de eventos que afectan los servicios tecnológicos y la infraestructura las 24 horas del día, los 7 días de la semana, la cual puede ser administrada por el proveedor de servicios directo, o por un tercero subcontratado.

Los NOC se originaron por primera vez a fines de la década de 1970 por los proveedores de servicios de telecomunicaciones para mostrar el estado de los conmutadores, el enrutamiento y los circuitos.

El NOC actual no solo se limita a monitorear equipos de red (enrutadores, conmutadores, servidores), sino también aspectos relacionados con la nube, la energía, el medio ambiente y el servicio. Los dos trabajos principales son el monitoreo y la gestión de eventos, dentro de sus responsabilidades tenemos:

- Análisis de tráfico
- Supervisión de todos los elementos críticos de la red
- Identificación de fallas y degradaciones de la red con un enfoque tanto reactivo como proactivo
- Determinación de la disponibilidad y el rendimiento de la red.
- Gestión de eventos e incidentes, incluidas escalaciones para acelerar la restauración de fallas
- Gestión de cambios y configuraciones
- Documentación de todas las fallas y problemas de rendimiento
- Informes sobre posibles escenarios de optimización basados en tendencias

La gestión de eventos se centra en aquellos cambios de estado monitorizados definidos por la organización como un evento, determinando su significado, identificando e iniciando la respuesta correcta a los mismos. La información sobre eventos también se registra, almacena y proporciona a las partes relevantes.

El ingeniero NOC es un personal de primera línea que se espera que sepa cómo funcionan las cosas y sea capaz de identificar de dónde provienen los problemas, utilizando tanto la experiencia como el análisis.

Actualmente en Nicaragua se buscan perfiles de Ingenieria o licenciaturas a fines a Telecomunicaciones, Electrónica, Informática, Sistemas. Que tengan manejo de sistemas informáticos y por lo general algún conocimiento básico de redes con el

fin de agilizar la curva de aprendizaje al momento de ubicarlo en su área de supervisión.

El alcance del trabajo de un ingeniero de NOC puede ser bastante amplio según las ofertas de servicios y el diseño de la infraestructura del proveedor de servicios.

Un NOC está divido en muchas áreas con el fin de segmentar el trabajo, existen áreas de transporte según el tipo de tecnología por ejemplo radio enlaces, equipos de fibra óptica SDH/PDH, red sobre IP, MPLS, otras áreas de servicios como Telefonía fija, Telefonía móvil, Tv HFC, DTH, incluso dentro del área móvil deben existir otras áreas que analicen y monitoreen la red desde una parte puntual de su arquitectura, como por ejemplo el Core PS, Core CS, RAN. Es decir que un egresado del perfil de nuestra carrera tiene un abanico de posibilidades de ingresar a un NOC y desenvolver alguna de las funciones descritas. En la figura 24 se aprecia un operador del NOC en monitoreo de varios sistemas de gestión remota.

Figura 24. Monitoreo NOC [30]

Vigilancia de la red.

La vigilancia de la red es la primera y más importante función respaldada por un NOC. El personal del NOC realiza un monitoreo continuo de todos los elementos de la red, utilizando las herramientas disponibles, como un sistema de monitoreo de red o mediante los diferentes sistemas de administración de elementos (EMS) proporcionados por los proveedores de equipos. [25]

Para aquellas alarmas de red o de rendimiento detectadas, el personal del NOC realizará un filtrado preliminar (como correlación, alarmas por trabajo planificado, etc.), abrirá el ticket de problema (TT) correspondiente, monitoreará las advertencias de alarma, categorizará/priorizará la gravedad de la alerta y manejará la escalada del problema de acuerdo con los procedimientos definidos. Durante esta etapa, una comunicación constante entre los NOC conducirá a una mejor categorización, filtrado y evitación de TT innecesarios.

La función de vigilancia de la red normalmente incluye las siguientes actividades:

- Supervisión de alarmas en tiempo real del estado de salud de la red.
- Monitoreo de alarmas en tiempo real de todas las alarmas disponibles.
- Categorización apropiada de las alarmas para su resolución.
- Filtrar alarmas resultantes de eventos programados o trabajos de mantenimiento
- Combinar y agrupar alarmas (alarmas correlacionadas) con motivos de fallo comunes.
- Registrar y recopilar información de fallas e iniciar la solicitud de tickets de problemas para la gestión de fallas.
- Iniciar acciones de recuperación y procedimientos de notificación.
- Escalar los TT al soporte de segundo nivel de NOC o cualquier otra área involucrada, de acuerdo con el nivel de servicio definido
- Interfaz con proveedores de servicios externos o portador/operador de interconexión (por ejemplo, proveedor de línea arrendada, red fija o portador de señalización internacional) para informes relacionados con fallas.

La vigilancia de la red es la función más crítica en el NOC. Dado que esta es la función que monitorea las alarmas y eventos entrantes en la red, es el primer punto de entrada para el estado de la red y permite respuestas de manera oportuna, lo que se traduce en una mejora general de los tiempos de restauración.

Las métricas típicas utilizadas para evaluar el desempeño de esta función son:

- Porcentaje de alarmas reconocidas frente al total de alarmas: mide la cantidad de alarmas que el NOC recibe e identifica positivamente.
- Identificación positiva de alarmas relacionadas con el mantenimiento: mide que todas las alarmas identificadas como parte del mantenimiento/trabajo planificado se correlacionaron de manera correcta.

- Tiempo de respuesta de alarma: Mide el tiempo que tarda el NOC en identificar y responder a una alarma, obteniendo el porcentaje de alarmas con tiempo de respuesta dentro de un tiempo objetivo y predefinido.

Gestión de fallas

La función de gestión de fallas incluye análisis de fallas, mantenimiento correctivo de primer nivel, y gestión de incidentes. El propósito es filtrar y resolver la mayoría de los casos sin intervención en el sitio o recursos adicionales dentro del marco de tiempo especificado por los niveles de servicio. [26]

Las funciones de gestión de averías incluyen las siguientes tareas:

- Acuse recibo de tickets de red, mantenimiento preventivo, gestión del rendimiento.
- Clasifique la gravedad de la falla para cumplir con los requisitos del nivel de servicio. Las gravedades pueden definirse como crítica/mayor/media/menor.
- Llevar a cabo el aislamiento, el diagnóstico y la solución de fallas en el equipo afectado.
- Correlación del TT con los existentes o creación de uno nuevo
- Escalar o asignar el TT
- Acciones correctivas remotas si el problema se puede abordar sin intervención en el sitio
- Cuando se requieran actividades en el sitio, escalar al equipo de mantenimiento de campo para despachar a la fuerza laboral
- Para fallas complejas, escalar el TT al soporte de segundo nivel (nivel 2)
- Realizar un seguimiento del estado de TT y realizar una escalada de gestión si no se resuelve dentro del marco de tiempo acordado

La función de gestión de fallas es la segunda función más vital dentro de un NOC. El grupo que ejecuta esta función asegura que las alarmas reconocidas en el paso anterior se solucionen y finalmente se resuelvan, lo que contribuye al rendimiento general de la red y, como resultado, tiene un impacto en la satisfacción del cliente.

Las métricas más comunes utilizadas para evaluar esta función son:

- Apertura de ticket: mide el tiempo en el que se abre un ticket, generalmente comparado con cada categoría de gravedad (crítica, mayor, media, menor).

- Identificación eficaz de la gravedad de la falla: mide que los tickets se abren con la gravedad correcta de acuerdo con las definiciones predefinidas para la categorización.
- Tiempo de escalación: mide el tiempo promedio que dedica el equipo de administración de fallas al aislamiento y diagnóstico inicial de fallas antes de escalar el ticket al agente de reparación correspondiente.

Despacho a campo

El despacho de campo cubre la coordinación de las intervenciones in situ que se ejecutan en la red. Las actividades realizadas incluyen:

- Envío de la orden de trabajo
- Preparación de la intervención de campo – por ejemplo: recolección de repuestos y autorización de acceso al sitio.
- Ejecución de la orden de trabajo.
- Informar el resultado al solicitante (y la devolución de las piezas de repuesto, si corresponde)

La función de despacho de campo es otra función crítica periférica de un NOC, ya que el equipo resuelve todas las intervenciones en el sitio, incluidas las tareas de mantenimiento correctivo y preventivo. Esta función específica se tratará con mucho más detalle en el módulo Gestión de la fuerza de campo.

6.1.2. Operación y Mantenimiento (O&M)

El área de Operación y Mantenimiento a la red (O&M) está compuesta por ingenieros del mismo perfil que el NOC, tienen dos tareas principales: Brindar o supervisar los mantenimientos a los sitios celulares para que operen en ópticas condiciones y se eviten fallas y atender las averías reportadas por el NOC.

La función de actividades del técnico de campo es la función más importante que cuenta con el apoyo de la organización de la fuerza de campo. Los técnicos de campo se hacen cargo de las atenciones de emergencias las 24 horas del día y los 365 días del año, realizando tareas de resolución de averías, asistencia con soporte disponible en los esfuerzos de solución de problemas junto con los Ingenieros del NOC o con contratas que atienden áreas puntuales como temas de energía o fibra óptica.

La configuración más común es tener un equipo de técnicos de campo que consta de al menos dos técnicos de campo trabajando en un sitio en un momento dado; esto es para facilitar el trabajo en altura y por cuestiones de salud y seguridad en áreas remotas, normalmente este equipo se conforma por un Ingeniero de O&M en conjunto con personal especializado en altura que puede ser interno o contrata externa a la institución. Adicional el Operador puede considerar tener solo un técnico en el sitio para tareas simples de mantenimiento preventivo que no requieran trabajo en altura.

La función de técnico de campo generalmente incluye las siguientes actividades:

- Recepción de la orden de trabajo.
- Preparación de la Intervención de Campo – por ejemplo: recolección de repuestos y autorización de acceso al sitio.
- Ejecución de la Orden de Trabajo.
- Validación de alarma con el Centro de Operación de la Red.
- Informar el resultado al solicitante; y la devolución de las piezas de repuesto (si procede)

Las métricas más comunes utilizadas para evaluar esta función son:

- Tiempo medio para aceptar la orden de trabajo: Mide el tiempo promedio que tarda el técnico de campo en aceptar una orden de trabajo.
- Porcentaje de tiempo en el sitio: Porcentaje de veces que el Técnico de Campo llega a tiempo al sitio en comparación con el total de visitas al sitio.
- Tiempo medio de resolución de la orden de trabajo: Mide el tiempo promedio que el técnico resuelve las averías.

6.2. Herramientas de Monitoreo y Gestión de alarmas

Los Operadores de telefonía necesitan de herramientas para el monitoreo y gestión de su red en producción para que el Ingeniero NOC pueda detectar eventos y gestionar atenciones con el personal de campo. Estas herramientas consisten en un conjunto de aplicativos combinados que facilitan la detección, comprensión, correlación y análisis de todos los sucesos en la red y en base a esta información tomar decisiones para atender de forma remota o con personal de campo.

En Nicaragua las operadoras telefónicas principales trabajan con tecnología desarrollada por Ericsson para la implementación RAN y Core, es por ello que el Sistema de Soporte a la Operación para monitoreo remoto es brindado por éste proveedor.

Conforme se implementan nuevos equipos y tecnologías, Ericsson ha ido cambiando su propuesta para la gestión remota de la red, sin embargo, los 2 servicios que ha ofrecido a sus clientes tienen las mismas características de modo que el Ingeniero NOC este familiarizado con el entorno y pueda realizar una transición rápida al nuevo gestor. Hay Operadores que incluso utilizan ambos Sistemas de Soporte para la red en simultaneo, a nivel de RAN comparten ambos medios, a nivel de Core permanecen o prefieren uno mientras se crean las condiciones para la migración al siguiente nivel.

Ericsson propone los softwares OSS y ENM para la gestión del monitoreo remoto en RAN. Ambos tienen interfaces CLI (Comand Line Interface) y GUI (Grafical User Interface) para la supervisión y ejecución de acciones correctivas, cada una con sus propios beneficios, la utilización de una u otra depende del Ingeniero NOC a cargo de la supervisión de la red.

6.2.1. OSS

Operations support systems - Sistemas de soporte a las operaciones (también llamados operational support systems u OSS) hacen referencia a sistemas de información empleados por las empresas operadoras de telecomunicaciones. El término OSS por lo general describe a los "sistemas de red" que están directamente vinculados a la red de telecomunicaciones misma, por ejemplo: procesos de soporte para el mantenimiento del inventario de red, servicios de aprovisionamiento, configuración de los elementos de red y software para la gestión de fallas. [27]

En general un OSS cubre al menos las siguientes áreas de aplicación:

- Network management systems - (Sistemas de gestión de red)
- Service delivery - (Plataforma de despliegue de servicios)
- Service fulfilment (Cumplimiento del servicio), incluyendo el inventario de red, activación y aprovisionamiento
- Service assurance - (Aseguramiento del servicio)
- Customer care - (Servicio al cliente)

OSS ERICSSON para sistema de gestión de la red tiene dos presentaciones: interfaz GUI mediante Citrix Metaframe basado en UNIX para visualizar y ejecutar procesos de forma gráfica y una interfaz CLI mediante un cliente desarrollado por Ericsson como Winfiol, o configurado en una terminal libre como Putty, Secure CRT, entre otros.

Citrix Metaframe

Citrix Virtual Apps (anteriormente WinFrame, MetaFrame, Presentation Server y XenApp) es un software de virtualización de aplicaciones producido por Citrix Systems que permite acceder a las aplicaciones de Windows a través de dispositivos individuales desde un servidor compartido o un sistema en la nube. [28]

CITRIX Metaframe, permite gestionar de forma centralizada aplicaciones heterogéneas y ofrece acceso a cualquier estación de trabajo, cualquier dispositivo como un portátil o teléfono móvil conectados a Internet pueden ser usados para acceder de manera transparente cualquier software instalado en el Servidor.

En resumidas palabras "puesto de trabajo virtual". Esto da lugar a un entorno seguro tanto para el acceso del empleado como el cifrado de datos mientras están en uso. Los administradores de servidores que utilizan este tipo de software, lo pueden configurar de forma colaborativa para ejecutar a través de estas conexiones remotas. [29]

Citrix MetaFrame no es en sí mismo un software de colaboración, pero sí un sistema para facilitar el acceso remoto. La Figura 25 muestra una interfaz de conexión hacia Citrix MataFrame.

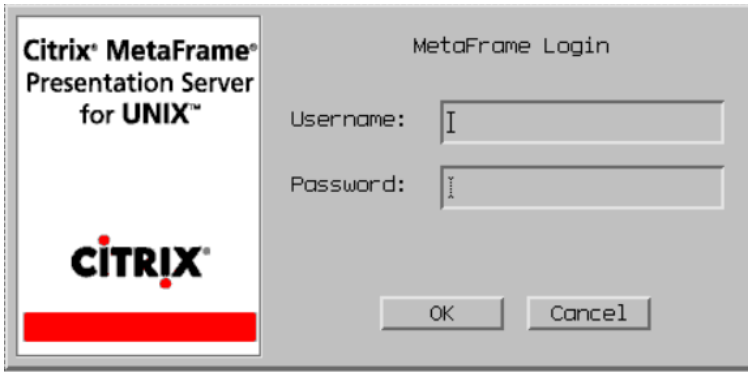


Figura 25. Citrix MetaFrame

Dentro de los aplicativos más utilizados de Citix Metaframe para OSS Ericsson para el monitoreo RAN tenemos las siguientes Herramientas:

- OSS Common Explorer: Permite al Ingeniero NOC visualizar la topología de la red, las BSC, RNC con cada elemento configurados dentro de ellas es decir cada BTS o Nodo B, al igual que los eNB, también se observa el estado de celda, alarmas del Nodo de forma gráfica con las opciones Status View, Alarm View y otras opciones de visualización de algún dato de interés del Ingeniero en monitoreo de la red. En esta herramienta también se pueden encontrar otros elementos de verificación muy útiles, principalmente el Element Manager que tienen muchos usos a nivel de Troubleshooting.
- Element Manger: Permite al Ingeniero NOC efectuar acciones de Troubleshooting correctivos como reset a los ManagedElement (función central de cada Nodo), recarga de CV (archivo de configuración de cambios en el Nodo).
- Cabinet Viewer: Permite visualizar de forma gráfica el hardware, número de producto instalado de los sectores, antenas, RRU, CBU, FCU.
- Alarm Estatux Matrix: Permite al ingeniero NOC visualizar en forma de matriz la cantidad de alarmas, con sus criticidades para elemento de Control como una RNC o una central Core como una MSC, sin embargo, no brinda a detalle la alarma generada, para ello para obtener más información se sincroniza con la siguiente herramienta de visualización: el alarm list viewer.
- Alarm List Viewer: Permite al ingeniero NOC visualizar un listado de las alarmas generadas en los elementos CORE y de control RAN, Incluso por cada elemento de acceso BTS, Nodo B o eNode B, de igual forma se puede configurar a gusto del usuario para visualizar o filtrar de acuerdo a prioridades.
- Alarm log Browser: Permite al Ingeniero NOC visualizar log de alarmas por cada elemento de la red móvil filtrado dentro la herramienta, con ellos observara un listado de alarmas generadas en el periodo de tiempo configurado según sea el interés.

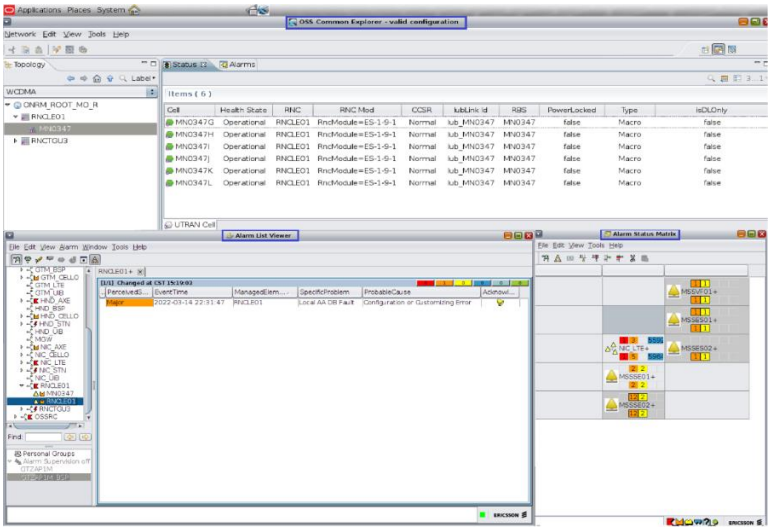


Figura 26. Herramientas OSS Citrix Metaframe

La figura 26 muestra un ejemplo de la interfaz gráfica del OSS Citrix Metaframe tomada desde un gestor en operación, se observa la visualización del OSS Common Explorer, en el cual se visualizan las opciones de Topology mediante la cual se puede navegar por los elementos configurados dentro de la red del operador, y las opciones Status cell para identificar el estado de operación de cada celda por sitio seleccionado, así mismo las alarmas que tienen al momento de la revisión.

Adicional a las herramientas gráficas, Citrix brinda la posibilidad de conectar a una terminal, la cual permite conexión a distintos elementos de red para realizar revisiones vía comando (CLI), con la instrucción AMOS se pueden conectar cualquier nodo B o eNode B configurado en el OSS, se pueden hacer conexiones ssh hacia una SIU, verificaciones ping y ejecutar cambio de contraseña desde esta misma terminal. Es una opción muy útil desde la aplicación Citrix ya que algunas instrucciones de verificación solo pueden ser revisadas desde la CLI. La figura 27 muestra una terminal dentro del OSS para revisión vía CLI.

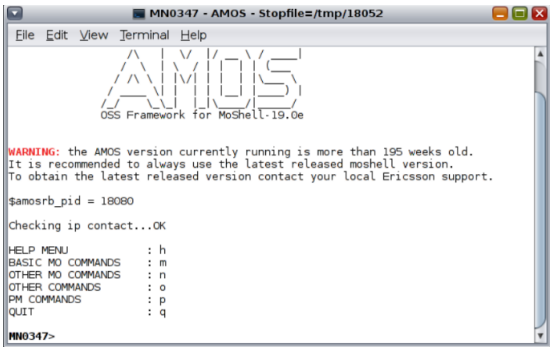


Figura 27. Terminal Moshell OSS Citrix

Winfiol

La conexión vía CLI para el OSS Ericsson se realiza preferiblemente desde la aplicación Winfiol de Ericsson, en la figura 28 se muestra la venta inicial del aplicativo tomado desde el gestor en operación, con él es posible conectarse a las BSC, RNC o MSC, aunque también lo es desde otros Software libres como el Putty o SecureCRT, pero la comandaría utilizada para la revisión es propia de Ericsson, se utiliza en su mayoría para revisiones GSM en RAN y MSC en Core.

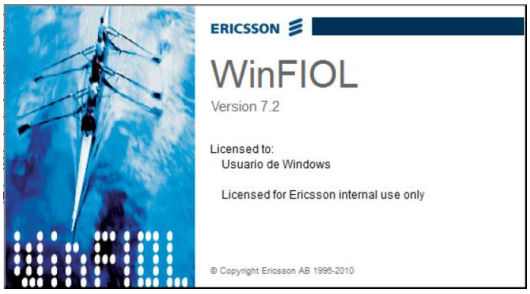


Figura 28. Winfiol.

6.2.2. ENM

Ericsson Network Manager (ENM) es el aplicativo más reciente de Ericsson que diferencia de las herramientas previas, es de fácil conectividad, ya que no requiere instalación de software en una computadora, se maneja en un entorno WEB y brinda flexibilidad de extremo a extremo, lo que permite una operación eficiente y sin inconvenientes entre redes y capas de red, así como un conjunto de aplicaciones y herramientas unificadas para administrar el acceso de radio, el transporte y las redes centrales. El entorno operativo uniforme de Ericsson Network Manager incluye una colección de funciones de gestión consolidadas basadas en una plataforma de software lista para la nube y ofrece casi cero tiempos de inactividad durante las actualizaciones de software, lo que garantiza la visibilidad y el control total de las redes. La figura 29 muestra las vistas iniciales del ENM y las opciones que brinda al operador.

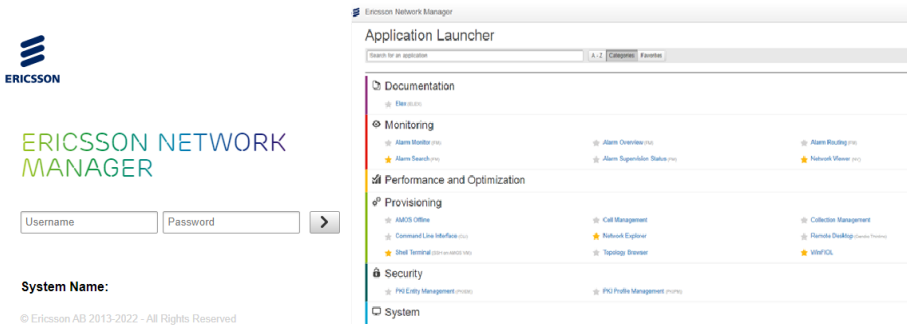


Figura 29. Ericsson Network Manager

ENM Ofrece los siguientes beneficios:

- Uniformidad del entorno, con un conjunto común de aplicaciones para permitir la gestión de todas las tecnologías accesibles a través de una vista única con control seguro.
- Gestión de todas las tecnologías y su evolución, manejando tecnologías clásicas listas para usar desde el primer día, así como todas las tecnologías basadas en la nube de la misma manera uniforme (preparado para manejar el cambio de 4G a 5G y actualizado continuamente para estar listo para la próxima ola de tecnología).
- Gestión de funciones de red virtual (VNFM), combinada con análisis y capacidades de escalado automático basadas en políticas que interactúan con varias distribuciones estándar
- Escalabilidad, brinda alta capacidad a través de una implementación escalable flexible que permite la consolidación de sitios OSS existentes para crecer o administrar una mayor complejidad y consolida una cantidad de sitios OSS existentes.
- Automatización que garantiza la mejor eficiencia operativa, un rendimiento superior de la red, un tiempo de comercialización rápido y una gestión avanzada de incidentes. Las funciones de análisis en tiempo real también se presentan para el monitoreo, la detección de anomalías, la predicción y resolución.
- Integración abierta y fácil, proporcionando un conjunto de puntos de integración abiertos y fáciles de usar en entornos OSS existentes.
- Independencia de la versión, con integración de nodos basada en modelos para proporcionar capacidades de paso rápido, lo que permite implementar un nuevo software de red móvil sin actualizar el sistema de gestión de red.
- Flexibilidad y agilidad de implementación, lo que permite a los proveedores de servicios implementar el sistema de gestión de red como un sistema de hardware integrado o como una aplicación en el entorno de nube del proveedor de servicios.

6.3. Monitoreo de Alarmas

Los ingenieros NOC encargados del monitoreo de la red móvil, lo realizan mediante herramientas de visualización muy prácticas en el ENM, mismas que se pueden encontrar en el OSS, su uso depende de donde esté integrado el elemento de red a validar. Ericsson Network Manager ofrece las siguientes herramientas:

- Network Explorer: Brinda opción de búsqueda de un elemento de red especifico, puede ser un Nodo B o una RNC, también desde esta opción se puede llamar a una colección (grupo de Nodos) previamente configurada, lo que ayuda con las revisiones generales de la red.
- Alarm Monitor: Brinda opciones de visualización grafica de alarmas por cada elemento de red, se pueden aplicar filtros a los diferentes campos con el objetivo de visualizar un tipo de alarma especifica.
- Alarm Seach: Brinda opción de visualización grafica de alarmas activas y log (historial) por cada elemento de red seleccionado.
- Cell Management: Brinda opción de visualización grafica del estado de las celdas por cada sitio configurado, también se pueden realizar acciones como bloqueo y desbloqueo manual de las celdas.
- Shell Terminal: Es una herramienta del ENM que permite la conectividad vía CLI con los elementos de la red, se pueden hacer conexiones hacia SIU y pruebas de ping como parte de troubleshooting para diagnosticar fallas.
- Winfiol: ENM trae el aplicativo de Winfiol para hacer revisiones a nivel de GSM, actualmente consta de una consola principal donde se cargan por pestañas cada una de las BSC del operador, también posee una Scrip Terminal para ejecución de comando de validación y correctivos.

La Figura 30 muestra una toma desde un gestor en operación de la opción Winfiol dentro del entorno Web del ENM.

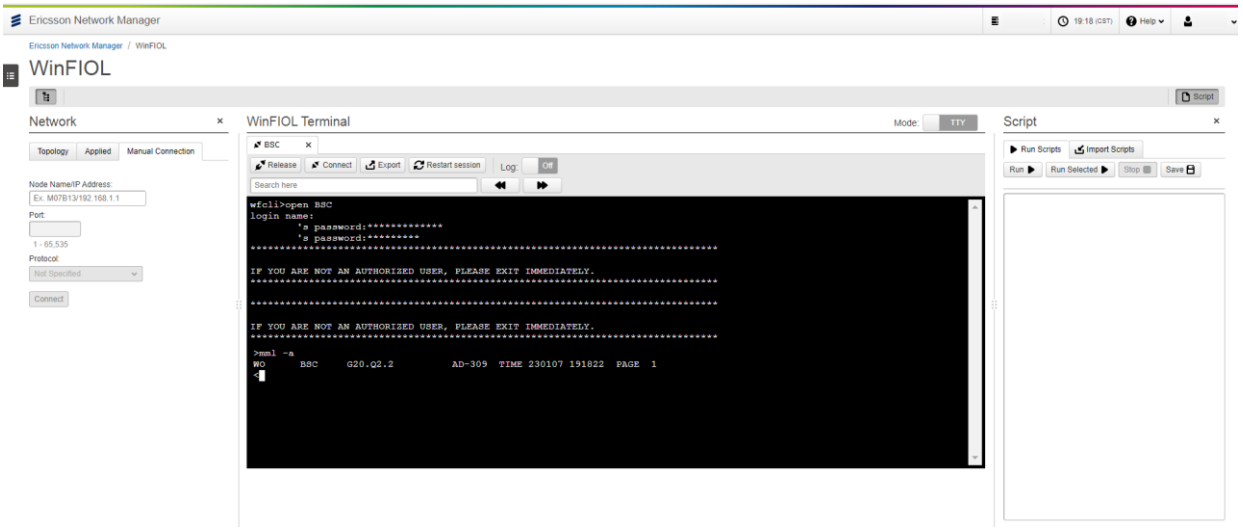


Figura 30. Winfiol desde ENM

6.4. TeMIP

En busca de optimizar los recursos y reducir el porcentaje de error durante el monitoreo de alarmas, los operadores optan por automatizar los procesos, para ello utilizan plataformas de aperturas de Incidentes, sin embargo, este tipo de plataformas necesitan una fuente de alimentación de información, es decir una conexión hacia el gestor nativo, los operadores por lo general tienen múltiples tecnologías y diferentes etapas de la red que requieren supervisión, no solo a nivel móvil RAN, sino también a nivel de Core, etapas de transporte y otros servicios, es por ello, que se necesita centralizar a las alarmas, aplicar filtrado y enviar orden de aperturar Incidentes en una cantidad que pueda ser manejable por el Ingeniero NOC responsable de la validación de estos tickets, de modo que minimice el rango de error en las atenciones de fallas.

TeMIP es una solución de administración de fallas altamente automatizada que brinda a los operadores una vista única de todos los elementos y sistemas en múltiples tipos de redes, ayuda con la gestión de redes multifabricante y ofrece funcionalidades de gestión integrada de fallos, así como un marco para la adición de nuevas aplicaciones para ampliar su funcionalidad. Igualmente, TeMIP permite al personal de operaciones controlar todos los elementos de la red con un sólo sistema, recogiendo y procesando información de eventos y alarmas de múltiples dispositivos. La funcionalidad interna de TeMIP aborda las funciones de gestión de fallos de telecomunicaciones, incluyendo registro de eventos, gestión de alarmas y etiquetado de problemas para luego enviar a generar Incidentes. HP y DEC (Digital Equipment Corporation) son empresas que brindan soluciones TeMIP a los operadores de telecomunicaciones. La figura 31 muestra un entorno de trabajo bajo el uso de TMIP.

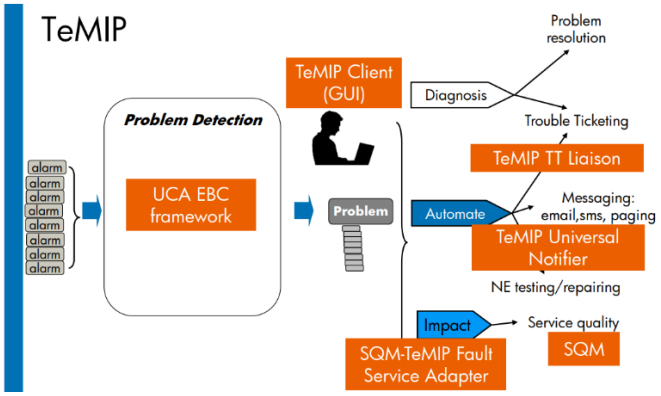


Figura 31. TeMIP

6.5. Herramientas de gestión de Incidencias

Las herramientas de gestión de Incidencias se utilizan para la documentación de todas las incidencias, problemas y cambios que se están trabajando en la red en un momento dado. Puede considerarse una de las principales herramientas utilizadas por el NOC, ya que permite que todo el equipo tenga un mecanismo adecuado para documentar todas las actividades relacionadas con cada incidente, problema o ticket de cambio.

Una herramienta adecuada para la documentación ayuda al equipo, ya que pueden saber exactamente cuál es el estado de cualquier ticket, cuáles son los próximos elementos a resolver y qué necesita seguimiento. También permite la generación de informes, que sirven como base para las revisiones del desempeño del NOC, KPI y SLA.

Una herramienta de gestión incorpora módulos para la gestión de incidentes (tickets de incidentes), gestión de problemas (tickets de problemas) y gestión de cambios (tickets de cambio). A la hora de elegir la herramienta adecuada, un punto a tener en cuenta es el esquema de colaboración entre el NOC y otra entidad que trabaje de la mano con ellos como una contrata encargada de algún servicio, deben elegirse herramientas que puedan sincronizarse y agilizar el trabajo conjunto. Algunas Herramientas de gestión de Incidentes son: BMC Remedy ITSM como el que se muestra en figura 33, ITSM ServiceNow, HP Service Manger como el mostrado en la figura 32 o Local Admin Ticket en dependencia de las preferencias del operador.

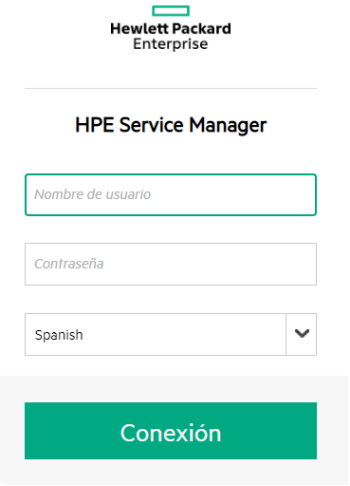


Figura 32. HP Service Manager

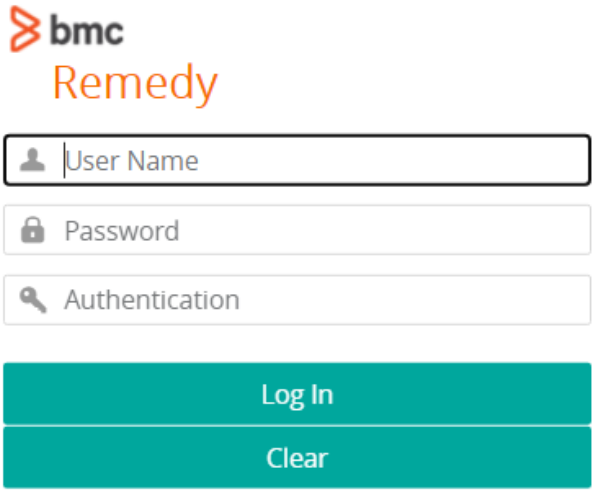


Figura 33. BMC Remedy

6.6. Validación de Incidencias y Atención de alarmas.

Un NOC necesita un medio para supervisar las alarmas, lo que se logra mediante un sistema de administración de fallas de red y un sistema de monitoreo de red, ambas herramientas son el corazón de cualquier organización NOC. Estas herramientas habilitan la función de vigilancia de la red, ya que las alarmas son monitoreadas y observadas por los técnicos del NOC y, por lo tanto, se emiten tickets para su resolución siguiendo los procesos de gestión de eventos e incidentes.

La figura 34 muestra un diagrama del flujo de procesamiento de las alarmas desde la aparición en el gestor nativo hasta la evaluación por el NOC.

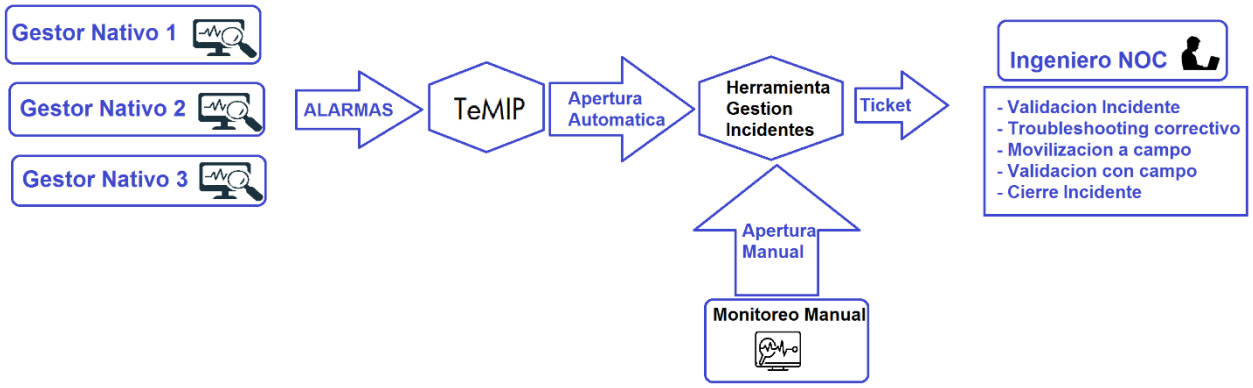


Figura 34. Flujo de Alarmas

El ingeniero NOC encargado de atender las fallas en la red tendrá dos fuentes de información para saber el estado de la red y en base a ello tomar decisiones para atender los eventos.

En primera instancia posee una herramienta de gestión de Incidentes la cual idealmente genera de forma automática ticket con alarmas que deben ser tratadas. En segunda instancia, pero de igual importancia, deben tener acceso a un sistema de monitoreo que permita aplicar filtros a conveniencia de eventos que están sucediendo en la red.

El primer nivel de atención consiste en validación de Incidentes (tickets de falla) lo cuales son emitidos por la Herramienta de gestión de Incidentes del Operador, esta herramienta tiene dos formas de generar falla. La primera inicia desde el gestor nativo (la herramienta de monitoreo de la tecnología de interés),

normalmente los operadores tienen muchos gestores Nativos, a nivel móvil pueden operar con el OSS Ericsson, ENM Ericsson, U2020 Huawei, ENM Netnumen Zte, a nivel de transporte monitoreo sobre redes IP Cisco, Huawei, equipos DWDM Nokia, Huawei, equipos de radio enlaces, Ericsson (SOEM), Huawei, Alcatel, etc. Lo que significa que deben condensar, unificar estas multiplataforma en un solo sistema, para ello tienen el TeMIP, todas las alarmas de los gestores nativos llegan a TeMIP, acá se aplican métodos de filtrado de alarmas, se dan prioridades, se aplica políticas para dar la orden de apertura de ticket, luego se generan los tickets que caen en las bandejas de los Ingenieros NOC que los validaran.

El otro método para generar tickets consiste en la apertura manual del Incidente, que se puede efectuar desde la propia herramienta de gestión de Incidentes o desde el mismo TeMIP enviando una orden de apertura semiautomática, estas opciones se trabajan en paralelo a las aperturas automáticas, se hace cuando se tiene algún tipo de alarma que es muy complicada de tratar y que genera Incidentes de forma descontrolada que no son manejable por los Ingenieros NOC.

El administrador del NOC debe garantizar un área interna responsable de la supervisión y generación de Incidentes semiautomático o manuales, normalmente conocida como Front Office.

La figura 35 es una muestra de Incidentes asignados al NOC en la plataforma Remedy para evaluación y atención de fallas en la red del operador.

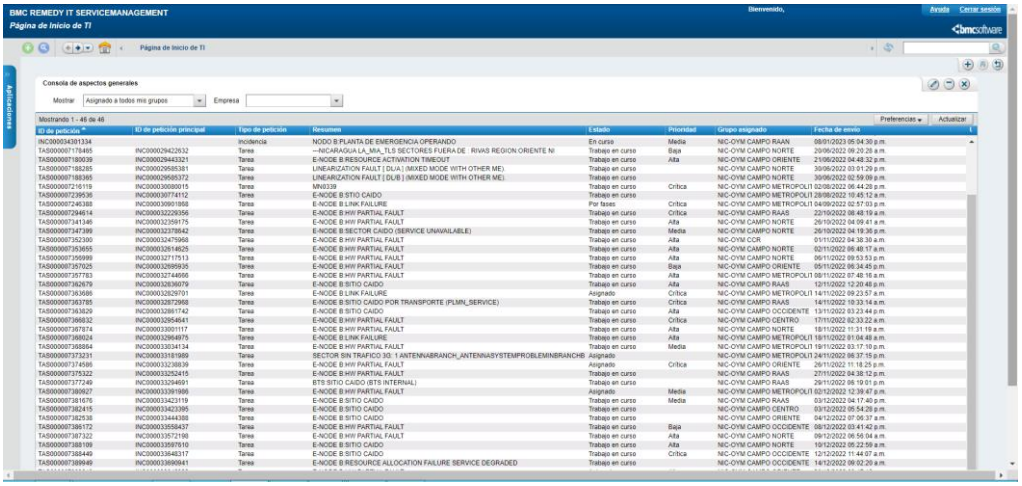


Figura 35. Bandeja de Incidentes BMC Remedy

Una vez se tiene un ticket generado, el NOC debe validar la información que trae el Incidente, que tipo de alarma es, a que gestor nativo pertenece, con que

prioridad de debe trabajar (emergencia, alta, media, baja), si tiene o no afectación de servicio.

Luego de identificar el tipo de falla y tomar decisiones sobre su trato, el Ingeniero NOC debe ejecutar acciones correctivas remotas si aplica el evento, como un reset a la RBS, recarga de CV, activación de licencia de emergencia, reset a la SIU, revisión del medio de transmisión, acción correctiva sobre el medio de transporte como: reset a puertos, balanceo de tráfico, limpieza de errores, reset a radio canales, cambios de negociación entre las diferentes etapas de la red, entre otros.

Si no es posible una acción remota correctiva, el siguiente paso a tomar en cuanta tras todas las pruebas realizadas es seleccionar el personal de campo que atenderá el evento según el área de Operación que este siendo afectada. Es deber del Ingeniero NOC brindar toda la información necesaria al Ingeniero de campo respecto al tipo de alarma que presenta el elemento de red afectado, con el objetivo que éste se prepare adecuadamente para iniciar la atención, busque repuestos, busque personal de altura y suministros necesarios para su viaje.

Si la falla es a nivel RAN, el ingeniero NOC se apoya de los gestores nativos para buscar la información como tipo de alarma, modelo de RRU, modelo de Antena, modelo de SFP, valores de RSSI, valores VSWR, niveles de imbalance en los puertos de las DU (unidades digitales), tipo de tarjeta, valor de temperatura del controlador, temperatura de los transiver, tipo de Sotfware CV, tipo de Release instalado, entre otras muchas variables que pueden ser de utilidad para simplificar la resolución de la falla.

En la figura 36 podrá visualizar mediante la Interfaz CLI del ENM información que es de relevancia cuando se tiene fallas a nivel de hardware en una radio base, brinda un diagrama de las conexiones de la DU hacia los RRU, en ella se pueden observar las celdas configuradas para cada puerto de cada RRU del sitio, de modo que el Ingeniero NOC puede indicar con certeza el espacio físico afectado cuando alguno de los CPRI Links o puertos de los RRU están alarmados, Si algún link presenta alarma, esta se visualiza textualmente en los campos que manejan información del producto afectado, adicional se pueden ver el tipo de Hardware instalado por elementos que conforma la RBS, virtualmente conocidos como MO. Toda esta información, combinada con un conjunto de pruebas previamente realizadas dan un diagnostico fiable para que el Ingeniero de campo resuelva la falla rápidamente.

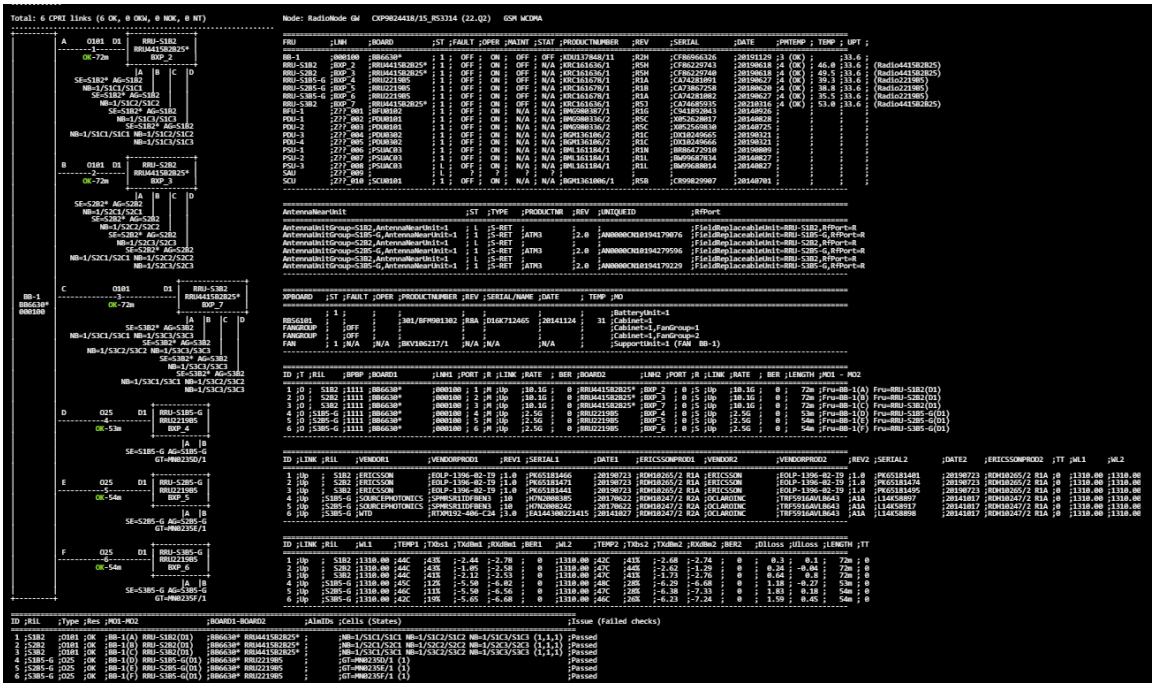


Figura 36. Interface CLI ENM - Información de un Nodo B.

El segundo nivel de atención consiste en un monitoreo eficaz sobre el gestor nativo, existen ciertos tipos de alarmas que conviene revisarlas directamente del gestor y no desde la herramienta de gestión de Incidentes. Por ejemplos las alarmas relacionadas con eventos de energía.

En un país como Nicaragua que la energía no es estable y se tienen cortes de AC prolongados en muchas zonas del país, los incidentes estarán generándose en cantidades altas no manejables por el operador, y muchas de ellas son catalogadas como caídas potenciales, pero realmente no tienen alto riesgo de afectación.

Si en una región se tiene un corte de energía y el 60% de los sitios tienen respaldo de motor generador, significa que este porcentaje de la red alarmada en esta zona no tiene un riesgo de caída de servicio o menos que el sistema de respaldo de Motor Generador (MG) falle en el transcurso del tiempo del corte de energía y conviene centrar esfuerzos en monitorear y priorizar atenciones sobre el 40% restante de la red que esta con respaldo de baterías, ya que el servicio se afectara cuando las baterías agoten carga.

En este escenario la herramienta de gestión de Incidencias generara un 100% de los tickets de los sitios en los que se tengan alarmas de corte de energía, lo que supone una alta carga de validaciones para el equipo de Ingenieros NOC, es por

ello que conviene filtrar directamente en el gestor nativo cuales son los sitios que están en baterías y concentrase en atender estas caídas realmente potenciales a como se presenta en la figura 37, en la cual nos enfocamos directamente en el texto de la alarma BATERIAS EN DESCARGA.

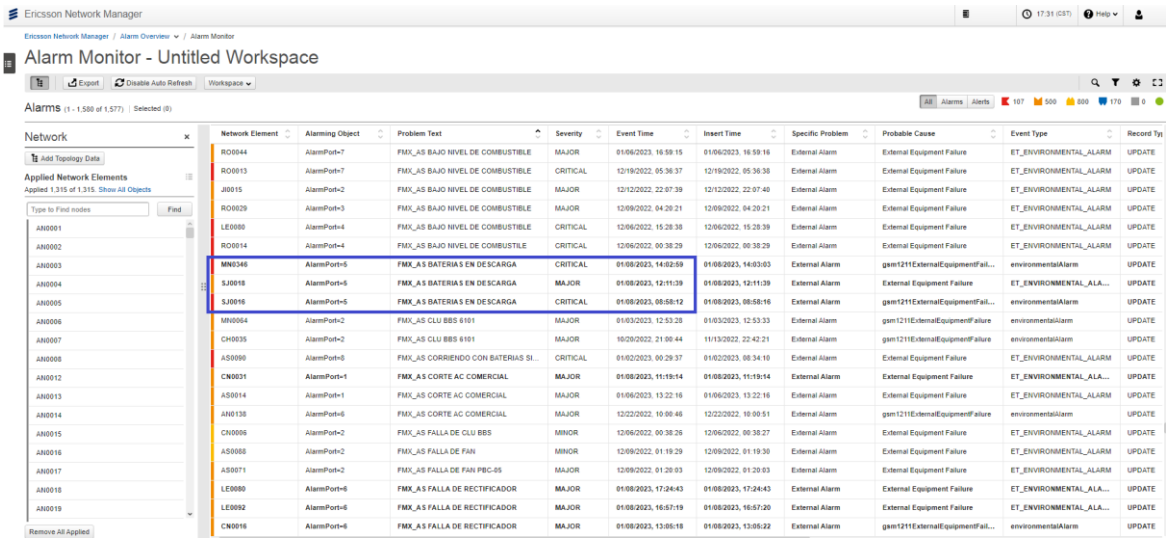


Figura 37. ENM Alarm Monitor

Ambas formas de revisión son correctas, es importante definir protocolos internos que ayuden a tomar decisiones sobre las prioridades al momento de supervisar la red, para evitar afectaciones en el servicio, minimizar los tiempos de atención de fallos y mantener en meta los KPI y SLA definidos para cada área.

6.7. Tipos de fallas

Una RBS puede afectar o degradar el servicio bajo 3 eventos principales:

- Fallas de energía
- Fallas Hardware/Software RBS
- Fallas de transporte

El ingeniero NOC debe ser capaz de identificar el origen de la afectación del servicio, para cada uno de los eventos tienen métodos de trabajo remoto, formas distintas de movilización de recursos y lógicas de funcionamiento diferentes. A continuación, se explicará los tipos de escenarios bajo los cuales operan los sitios celulares y el tipo de revisión que realiza dependiendo de la situación.

6.7.1. Fallas de energía.

Las RBS tienen 2 formas de captar los eventos de energía: mediante alarmas internas propias del gabinete y mediante alarmas externas que se captan por medio de módulos de alarmas que se conectan a las Unidades Digitales de control.

Las alarmas internas son captadas desde las DU por falla en los módulos que se conectan directamente a la tarjeta de control como las PSU, BFU, rectificadores y todo tipo de elemento que energice al gabinete o por falla en el suministro eléctrico. Las alarmas internas de energía que normalmente se visualizan en una RBS son:

- Comercial Power Failure (Loss of Mains)
- Running on Battery Supply (Battery Descarching)
- Battery Disconnected

Estas alarmas nos indican si falla el suministro eléctrico que energiza el gabinete de la RBS, también pueden fallar las unidades PSU, algún otro elemento interno, sin embargo, cuando ello sucede, se visualiza cual el elemento afectado en el campo Alarman Object de la GUI, misma información puede ser visualizada desde la CLI.

En la figura 38 se aplica un filtro sobre una red WRAN en la cual se visualizan las alarmas de energía internas, en el campo Specific Problem se visualiza el Loss of Mains, en el campo Alarm Object se observa si hace referencia a una alguna de las PSU y cuando tiene el texto Power Supply es la alimentación eléctrica de la red comercial.

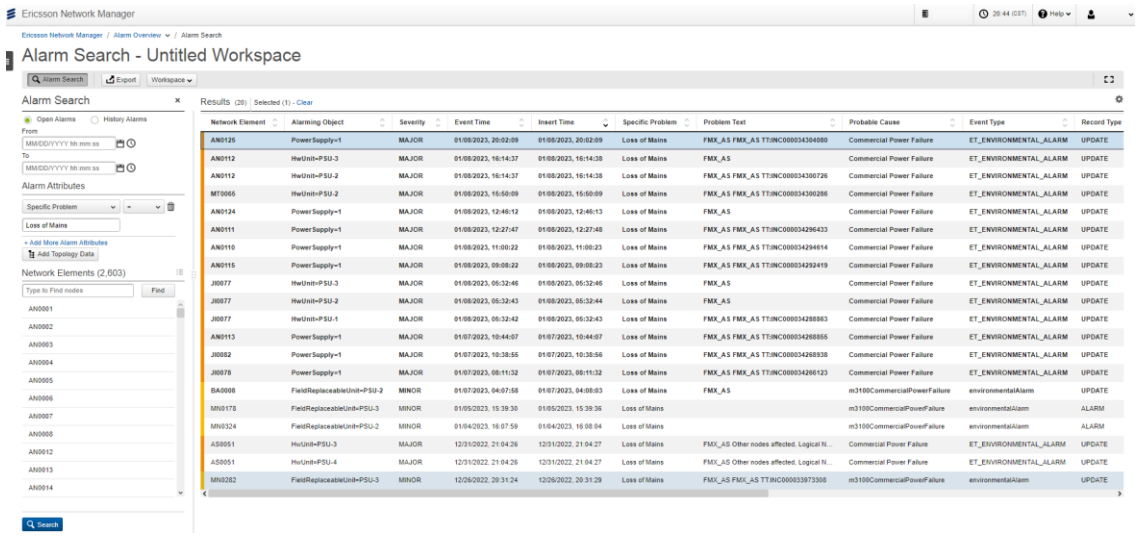


Figura 38. ENM Alarm Search - Filtro Alarmas Internas

Si algún elemento interno de energía de la RBS presenta alarma, se puede visualizar mediante la interfaz CLI los niveles de energía y características de dicho elemento con el comando ***get***, previamente identificado su MO con el comando ***lpr energy***. En el caso de las PSU a como muestra la figura 39, se visualizan las corrientes, voltajes y potencia de entrada y salida del elemento y se determina si está dañado u operacional.

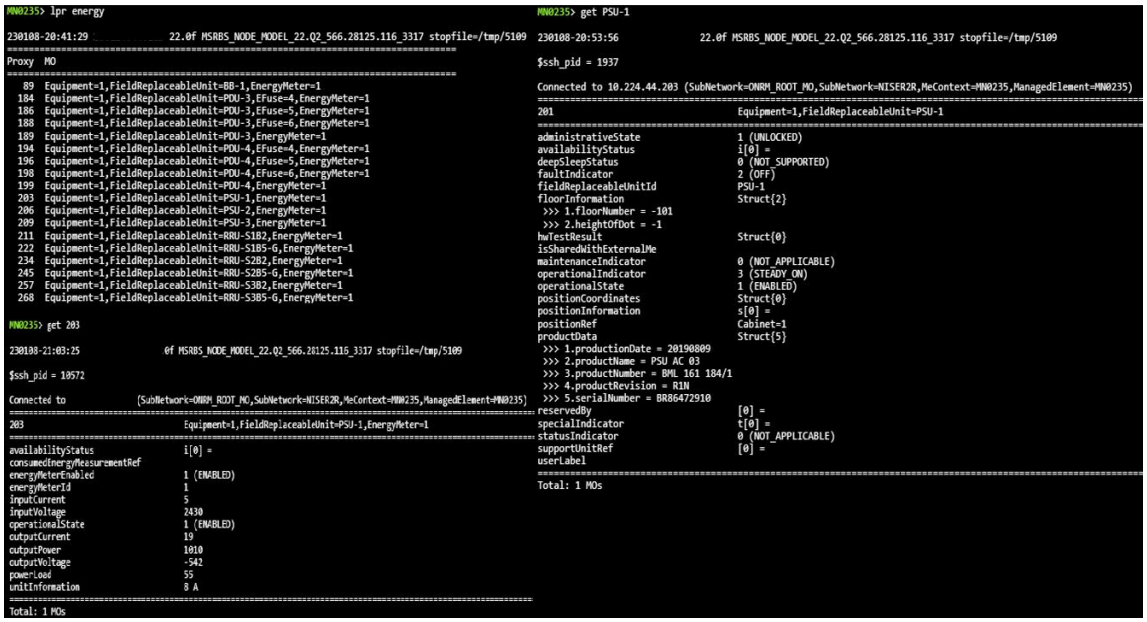


Figura 39, ENM CLI - Revisión de elementos de energía

Las alarmas externas son reconocidas en una RBS mediante un módulo intermediario de alarmas OVP, el cual se conecta a las Unidades digitales de control, reciben pulsos eléctrico provenientes del elemento que se desea censar,

como la red comercial, falla de motor generador, baterías en descarga, bajo nivel de combustible.
En la Figura 40 muestra cómo se visualizan las alarmas desde la CLI por medio del comando ***alt***, y en la Figura 41 como se muestra la mima alarma con la opción alarm monitor de la interfaz GUI del ENM.

```
AS0046> ALT

230108-22:00:56              0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/14928

Collecting Alarms...

================================================================================================================================
Date & Time (UTC)   S Specific Problem                    MO (Cause/AdditionalInfo)
--------------------------------------------------------------------------------------------------------------------------------
2022-12-12 11:57:06 M External Alarm                      FieldReplaceableUnit=SUP-1,AlarmPort=6 (FALLA DE RECTIFICADOR)
2023-01-09 03:39:19 M External Alarm                      FieldReplaceableUnit=SUP-1,AlarmPort=1 (CORTE DE AC COMERCIAL)
2023-01-09 03:39:52 M External Alarm                      FieldReplaceableUnit=SUP-1,AlarmPort=2 (MG OPERANDO)
>>> Total: 3 Alarms (0 Critical, 3 Major)
```

Figura 40. ENM CLI - Alarmas Externas

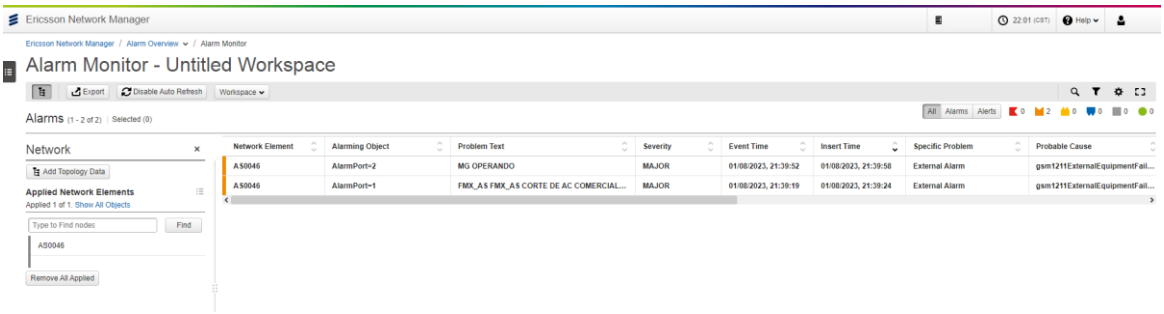


Figura 41. ENM GUI - Alarmas Externas

Una vez se tenga identificada la alarma de energía, la gestión de movilización dependerá de la infraestructura del sitio, es decir se debe tomar encuentra si el sitio trabaja únicamente con red comercial, si utiliza un sistema de paneles solares, si tiene un sistema hibrido, si tiene motor generador de respaldo y si únicamente cuenta con banco de baterías o si tienen un algún sistema de optimización de MG con baterías. Todas estas variables que debe conocer el Ingeniero NOC junto con las alarmas que visualiza en el gestor nativo, ayuda a la toma de decisión de movilización de recursos para atender fallas por caídas potenciales o afectación de servicio por temas de energía.

6.7.2. Fallas de Hardware/Software RBS.

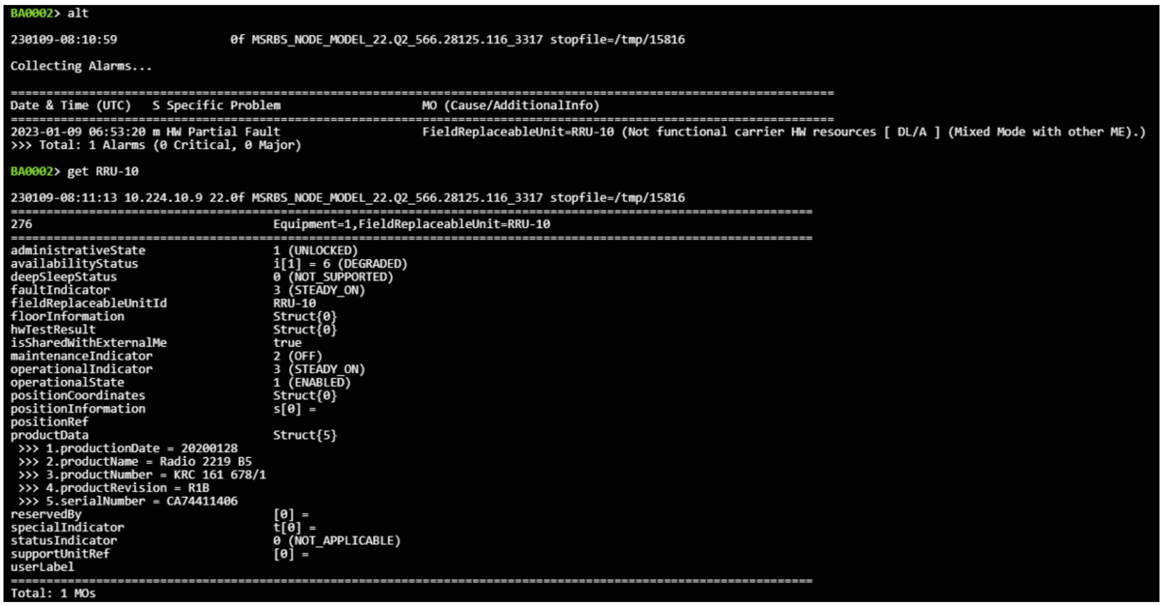
Una RBS puede presentar falla en su Hardware en cualquiera de sus tarjetas o periféricos o daño en el software que requieran acciones de cambio o reinstalación (restore), si se tiene gestión del Nodo afectado lo más recomendable es hacer una revisión vía CLI de las alarmas y el Hardware presente. Si no se tiene gestión del Nodo se deberá hacer una validación en campo del tipo de afectación. Algunas alarmas que se presentan son:

- Hardware Partial Fault RRU-X
- HW Error
- RX Diversity Lost
- RX Branch Imbalance Fault
- FanGroup=X Failure
- Link Degraded (RiLink=X)
- Linearization Disturbance Performance Degraded
- Fan Power Supply Failure
- AuxPlugInUnit_CommunicationLostWithRet
- Antenna General Problem
- SW error
- Emergency Unlock of Software
- Emergency Unlock Reset Key Required

Es importante que el Ingeniero NOC brinde la mayor cantidad de información posible al Ingeniero de campo, producto de Hardware afectado, configuración en la RBS por ejemplo si el RRU alarmado tiene configurada varias portadoras, si está en mixed mode con otra tecnología, si alguno de los puertos presenta imbalance en el Rx, si los valores fiber UL/DL están dentro del rango, si las SFP tienen las mismas capacidades tanto en la DU como el RRU.

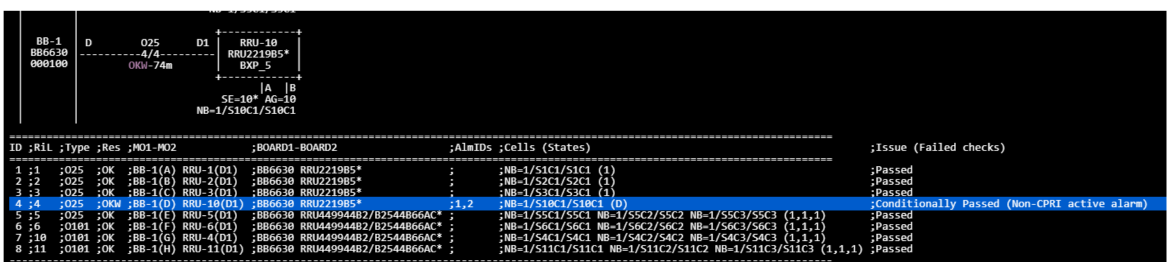
En la figura 42, se muestra un ejemplo de sitio WCDMA que tiene alarmas de falla de Hardware del RRU, esta alarma degrada el servicio, puede que impacte la disponibilidad como afectación total de RRU o que se presenten cortes de servicio de manera intermitente, para ello es conveniente revisar el log de alarmas del Nodo y evaluar el comportamiento la misma. Con el comando ***alt*** se visualizan las alarmas activas en los Nodos, en este ejemplo podemos observar que el sitio tiene el RRU-10 con alarma de HW Partial Fault y un mensaje que india que está en configuración Mixed Mode con otro elemento, es decir se genera afectación en 2 tecnologías. Se verifica el tipo de radio alarma con el comando ***get***, para que el Ingeniero de campo busque repuesto del producto correcto. Tambien podemos evaluar si el RRU alarmado presenta otro tipo de afectación por ejemplo fiber loss,

Rx imbalance, en la Figura 43, se muestra parte de un diagrama de bloques y alarmas más específicas en los cuales se observa que para este mismo ejemplo que el RRU-10 solo tiene configurada una celda, y que la única afectación del link es producto de la falla en el RRU, se pueden dar ocasiones que la falla no sea en el radio, sino en la fibra, los jumperes, SFP. A nivel de HW se verán alarmas y se compararán los niveles de los paramentos a evaluar según los rangos definidos por el proveedor Ericsson o por el área de calidad móvil o RF.



```
BA0002> alt

230109-08:10:59             0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/15816

Collecting Alarms...

==========================================================================================================
Date & Time (UTC)   S Specific Problem                   MO (Cause/AdditionalInfo)
==========================================================================================================
2023-01-09 06:53:20 m HW Partial Fault                   FieldReplaceableUnit=RRU-10 (Not functional carrier HW resources [ DL/A ] (Mixed Mode with other ME).)
>>> Total: 1 Alarms (0 Critical, 0 Major)

BA0002> get RRU-10

230109-08:11:13 10.224.10.9 22.0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/15816
=======================================================================================================
276                                Equipment=1,FieldReplaceableUnit=RRU-10
=======================================================================================================
administrativeState                1 (UNLOCKED)
availabilityStatus                 i[1] = 6 (DEGRADED)
deepSleepStatus                    0 (NOT_SUPPORTED)
faultIndicator                     3 (STEADY_ON)
fieldReplaceableUnitId             RRU-10
floorInformation                   Struct{0}
hwTestResult                       Struct{0}
isSharedWithExternalMe             true
maintenanceIndicator               2 (OFF)
operationalIndicator               3 (STEADY_ON)
operationalState                   1 (ENABLED)
positionCoordinates                Struct{0}
positionInformation                s[0] =
positionRef
productData                        Struct{5}
 >>> 1.productionDate = 20200128
 >>> 2.productName = Radio 2219 B5
 >>> 3.productNumber = KRC 161 678/1
 >>> 4.productRevision = R1B
 >>> 5.serialNumber = CA74411406
reservedBy                         [0] =
specialIndicator                   t[0] =
statusIndicator                    0 (NOT_APPLICABLE)
supportUnitRef                     [0] =
userLabel
=======================================================================================================
Total: 1 MOs
```

Figura 42. Alarma Hw Partial Fault



```
  BB-1   | D        025       D1 |   RRU-10   |
 BB6630  |----------4/4----------| RRU2219B5* |
 000100  |        OKW-74m        |   BXP_5    |
                                 +------------+
                                      |A  |B
                                  SE=10* AG=10
                               NB=1/S10C1/S10C1

==========================================================================================================
ID ;RiL ;Type ;Res ;MO1-MO2            ;BOARD1-BOARD2                 ;AlmIDs ;Cells (States)                                          ;Issue (Failed checks)
==========================================================================================================
 1 ;1    ;O25  ;OK  ;BB-1(A) RRU-1(D1)  ;BB6630 RRU2219B5*             ;       ;NB=1/S1C1/S1C1 (1)                                      ;Passed
 2 ;2    ;O25  ;OK  ;BB-1(B) RRU-2(D1)  ;BB6630 RRU2219B5*             ;       ;NB=1/S2C1/S2C1 (1)                                      ;Passed
 3 ;3    ;O25  ;OK  ;BB-1(C) RRU-3(D1)  ;BB6630 RRU2219B5*             ;       ;NB=1/S3C1/S3C1 (1)                                      ;Passed
 4 ;4    ;O25  ;OKW ;BB-1(D) RRU-10(D1) ;BB6630 RRU2219B5*             ;1,2    ;NB=1/S10C1/S10C1 (D)                                    ;Conditionally Passed (Non-CPRI active alarm)
 5 ;5    ;O25  ;OK  ;BB-1(E) RRU-5(D1)  ;BB6630 RRU449944B2/B2544B66AC* ;       ;NB=1/S5C1/S5C1 NB=1/S5C2/S5C2 NB=1/S5C3/S5C3 (1,1,1)     ;Passed
 6 ;6    ;O101 ;OK  ;BB-1(F) RRU-6(D1)  ;BB6630 RRU449944B2/B2544B66AC* ;       ;NB=1/S6C1/S6C1 NB=1/S6C2/S6C2 NB=1/S6C3/S6C3 (1,1,1)     ;Passed
 7 ;10   ;O101 ;OK  ;BB-1(G) RRU-4(D1)  ;BB6630 RRU449944B2/B2544B66AC* ;       ;NB=1/S4C1/S4C1 NB=1/S4C2/S4C2 NB=1/S4C3/S4C3 (1,1,1)     ;Passed
 8 ;11   ;O101 ;OK  ;BB-1(H) RRU-11(D1) ;BB6630 RRU449944B2/B2544B66AC* ;       ;NB=1/S11C1/S11C1 NB=1/S11C2/S11C2 NB=1/S11C3/S11C3 (1,1,1) ;Passed
----------------------------------------------------------------------------------------------------------
```

Figura 43. Revisión de HW de RRU

6.7.3. Fallas de transporte

Una RBS presenta falla a nivel de transporte cuando alguna de las etapas en toda la ruta de transmisión de datos falla, como se muestra en la figura 44, una red de transporte puede ser multiplataforma, hasta ciertas etapas majarse con fibra Optica, otras por medio de radio enlaces, a su vez cada plataforma puede fallar según el tipo de tecnología instalada, la red puede tener muchos radio enlaces de distintos proveedores, fibra óptica que pasa un muchos equipos conversores o repetidores y los equipos ultimas millas también pueden ser de distintos proveedores, sin embargo cuando cualquier etapa del transporte falla, el resultado es una afectación en los equipos RBS por caída completa de la tecnología Movil involucrada.

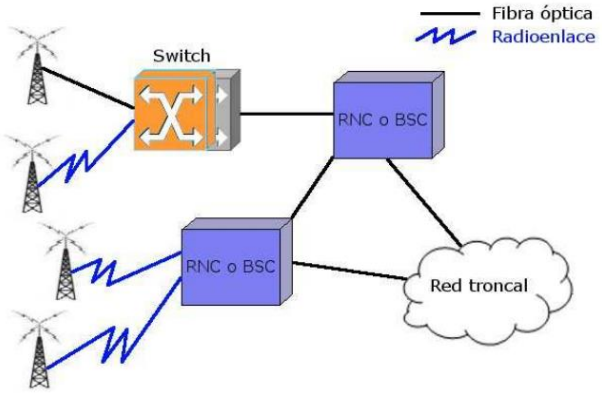


Figura 44. Red de transporte [31]

El ingeniero NOC debe estar claro del escenario que se le presenta para movilizar adecuadamente al personal de campo que hará la restauración del servicio. Un sitio que tiene instalada 3 tecnologías móviles GSM, WCDMA, LTE, se puede dar la posibilidad que la afectación sea solamente en alguna de ellas, y que no sea un problema local en la radio base, puede haber un puerto dañado en el equipo última milla de transmisión, puede haber falla en la negociación únicamente hacia la tecnología involucrada, se puede tener problemas de capacidad en la red troncal y por políticas de preferencia dejar fuera la VLAN de algún servicio. La alarma más común cuando falla el medio Tx es Hearbeat Failure, sin embargo, no necesariamente va estar presente, y cuando se tenga este tipo de afectación no necesariamente se pierde gestión de la tarjeta.

En la Figura 45 se observa un ejemplo de un sitio 3G que tiene afectación producto del medio de transmisión, en este caso se puede observar que no hay gestión de la tarjeta, que las celdas configuradas están en condición Disable (fuera de

servicio) y se tiene activa la alarma Failed to resolve Notification IRP (Heartbeat Failure).

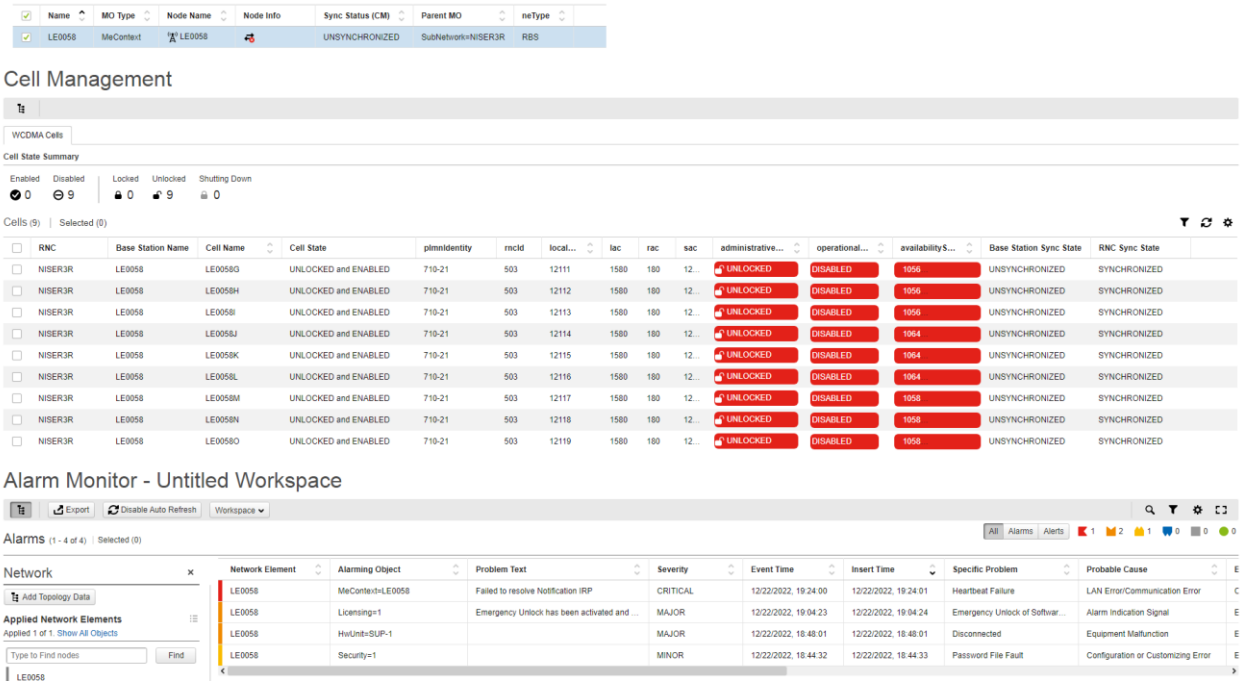


Figura 45. Nodo B afectado por falla en red Tx

Desde el criterio del Ingeniero NOC encargado de la validación del servicio Movil, se tiene una falla en el transporte o la tarjeta DU. Antes de enviar a campo para revisión de tarjeta es recomendable evaluar toda la ruta de transmisión con las áreas correspondientes en busca de eventos que se puedan correlacionar con la afectación que se tiene en la RBS, y de este modo se evitan movilizaciones innecesarias de Ingenieros de campo RBS.

El NOC ejecuta el rol más importante sobre la supervisión de red ya que es el lugar en donde se toman las decisiones sobre las atenciones de campo y al mismo tiempo recae la responsabilidad de tratar de minimizar las afectaciones, con diagnósticos acertados, movilizaciones oportunas y escalaciones a instancias superiores cuando las fallas lo ameriten.

VII. RESULTADOS – ATENCIÓN DE FALLAS RBS

Como se ha explicado en la investigación documental, existen 2 tipos de alarmas que pueden ser monitoreadas desde una radio base: Alarmas Internas y alarmas externas, el uso de cada una, depende del tipo de Hardware y las capacidades de alarmas que tenga el mismo en dependencia de los factores que puedan condicionar el tipo de sitio celda, como lo son adecuaciones de infraestructuras, impacto comercial (la necesidad de conectividad de llamadas y/o datos del sector donde se instaló la celda según la experiencia previa de los usuarios), accesibilidad al sitio, entre otros factores que contribuyan a definir el tipo de tecnología que se instala al momento de la planificación del proyecto, definen si instalan macro, micro, pico o femtoceldas y el tipo de gabinete.

Las alarmas Interna son las generadas y monitoreadas desde la misma radio base, son alarmas que traen de fábrica según el proveedor. Se tiene por ejemplo alarmas como Battery Missing, corriendo en baterías, comercial Power Failure, Alarmas de PSU y alarmas de cualquier elemento que esté monitoreado desde el módulo SHU de una RBS, algunas de ellas pueden ser configuradas y otras vienen con textos de fábrica que el Operador no puede modificar, por lo que tiene que adecuar su sistema para que reconozca este tipo de alarmas y se procesen de acuerdo a sus intereses.

Las alarmas Externas son generadas desde elementos externos a la radio base, como los sensores y/o relés y traducidas a las DU mediante un módulo OVP, SUP, SAU o SHU. El tipo de alarmas y la conexión de las mismas depende del interés del Operador respecto a la variable física que desea censar, para habilitar el monitoreo según los propósitos operacionales que tenga en su red. Se tienen alarmas externas del Motor Generador como Baja Presión de Aceite, Bajo Nivel de Combustible, Alta Temperatura, Motor Operando y Falla de red comercial.

En un estudio realizado a los indicadores de indisponibilidad de red a uno de los Operadores más importantes del país durante el 1er semestre del año 2019, se logró identificar que la mayor cantidad de incidencias que impactan los KPI en las tecnologías 3G y LTE son las fallas energía en los sitios de Motor Generador y en un menor porcentaje, pero impactando más que otros causales están los sitios sin Motor Generador, por lo que tener conocimiento de la infraestructura del sitio, modo de operación y análisis de las alarmas que reflejan en el gestor nativo son de gran relevancia. Además, se debe tener en cuenta la escalabilidad de la red y si los nuevos sitios que se piensan implementar tendrán iguales o diferentes condiciones en su infraestructura en comparación con la red en producción.

A continuación, se presentará un TOP 5 de alarmas que generan impacto en la red celular del operador y con ello la forma de tratar con cada una.

7.1. Fallas más recurrentes en RBS

El estudio de las fallas que se presenta en la red ayuda a tener una matriz de posibles soluciones cuando se presenta determinada alarma, debido a que normalmente estas fallas son repetitivas la experiencia de Ingenieros NOC y campo son de vital importancia y en base dicha experiencia se hará una explicación del tipo de alarmas, troubleshooting, gestión de movilización, revisión y resolución en campo para un TOP 5 de alarmas de alta recurrencia.

Basado en el estudio estadístico para el año 2019 tenemos las principales fuentes de indisponibilidad móvil provienen de las siguientes alarmas:

1. Fallas de energía AC
2. Fallas de energía DC
3. Fallas de sectores.
4. Fallas de diversidad.
5. Fallas de Hardware/Software DU/BB.

La presente guía abordará 4 puntos esenciales: Cableado de las alarmas o conexión del hardware que interviene en la etapa que se plantea, configuración lógica de las alarmas cuando aplique, Monitoreo/gestión de alarma y acciones correctivas en campo. Se brindará un panorama completo de sobre las alarmas citadas con el objetivo de acotar los tiempos de atención en dependencia del área de interés, bien sea Ingeniero NOC o Ingeniero campo.

7.2. Escenarios de restablecimiento.

7.2.1. Fallas de energía AC

7.2.1.1. Cableado de alarmas externas

En las RBS, como se ha indicado las fallas de energía están configuradas en dos tipos, las alarmas internas y alarmas externas, siendo las externas las de mayor concurrencia ante eventos programados o inesperados por energía eléctrica, en este caso las alarmas externas declaradas son corte de AC comercial y Baterías en descargas. Las alarmas externas al igual que las alarmas internas están configuradas en categorías según su importancia.

En la Tabla 1, se muestra como están configuradas e interconectadas las alarmas en una RBS 6150.

Tabla 1. ALARMAS EXTERNAS SITIOS CON MG

ESTANDAR PARA SITIOS CON MG					
NORMAS PARA INSTALACION DE ALARMAS EXTERNAS					
OVP	POSICION	CODIGO DE COLOR	TEXTO ALARMA	SEVERIDAD	PROVIENE
1	1	BLANCO-NARANJA / NARANJA	CORTE DE AC COMERCIAL	MAYOR	MG
1	2	BLANCO-VERDE / VERDE	MG OPERANDO	MAYOR	MG
1	3	BLANCO-AZUL / AZUL	FALLA DE MG	CRITICA	MG
1	4	BLANCO-CAFÉ / CAFÉ	BAJO NIVEL DE COMBUSTIBLE	CRITICA	MG
2	1	BLANCO-NARANJA / NARANJA	BATERIAS EN DESCARGA	CRITICA	RBS
2	2	BLANCO-VERDE / VERDE	FALLA DE RECTIFICADOR	MAYOR	RBS
2	3	BLANCO-AZUL / AZUL	ALTA TEMPERATURA	MAYOR	RBS
2	4	BLANCO-CAFÉ / CAFE	PUERTA ABIERTA DE RBS	MENOR	RBS

En la figura 46, se brinda detalle de conexión y etiquetado de alarmas externas de MG y gabinete 6150 en OVP-ALM8. Como puede visualizar las alarmas externas consiste en un conjunto de cambios externos que se requieren censar para tener información del entorno que rodea a la RBS, Algunos eventos son tomados desde elementos con infraestructura diferente al de una radio base como es el caso de los Motor Generadores (MG), lo cuales son elementos de respaldo energético que cuenta de 2 fases, la parte de Motor de Combustión y la parte de Generador eléctrico, es por ello que este elemento necesita un módulo de control eléctrico que gobierne todas sus funciones, cense los eventos que suceden en su estructura para luego exportar pulsos eléctricos con señales que son interpretadas en la OVP, es por ello que en la Figura 63, una de las entradas del sistema son Alarmas provenientes desde el MG: CORTE DE AC COMERCIAL, MG OPERANDO, FALLA DE MG, BAJO NIVEL DE COMBUSTIBLE.

La otra entrada son Alarmas que se toman desde borneras de la misma radio base: BATERIAS EN DESCARGA, FALLA DE RECTIFICADOR, ALTA TEMPERATURA, PUERTA ABIERTA RBS. Cada una de la alarma entra al OVP por lo general siguiendo las recomendaciones de códigos de colores del cableado UTP, y en la salida del OVP la conexión hacia las DU en donde se configuran los textos de las alarmas, según la posición física que llegan a los puertos.

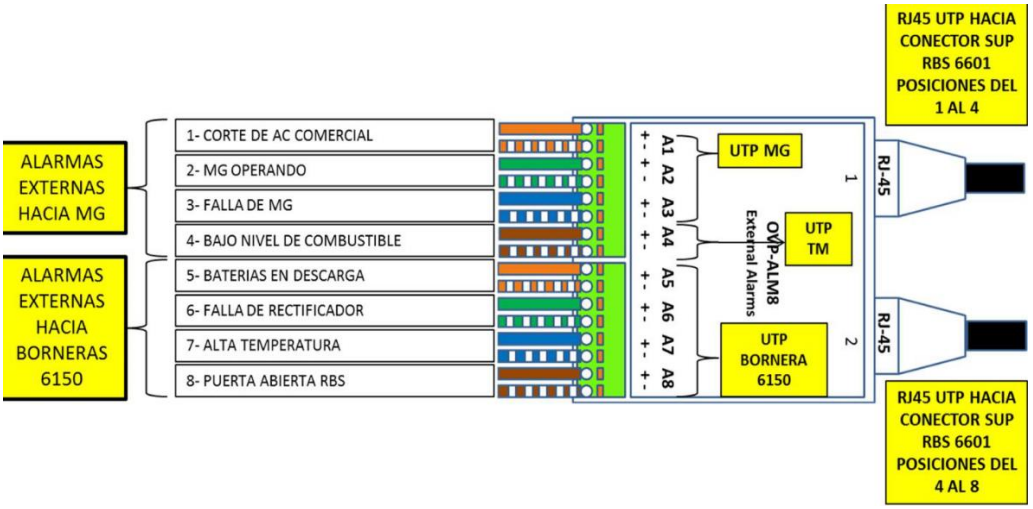


Figura 46. Alarmas Externas - Conexiones OVP

En la figura 47, puede visualizar a detalle la conexión de alarmas externas desde las borneras en un gabinete 6150.

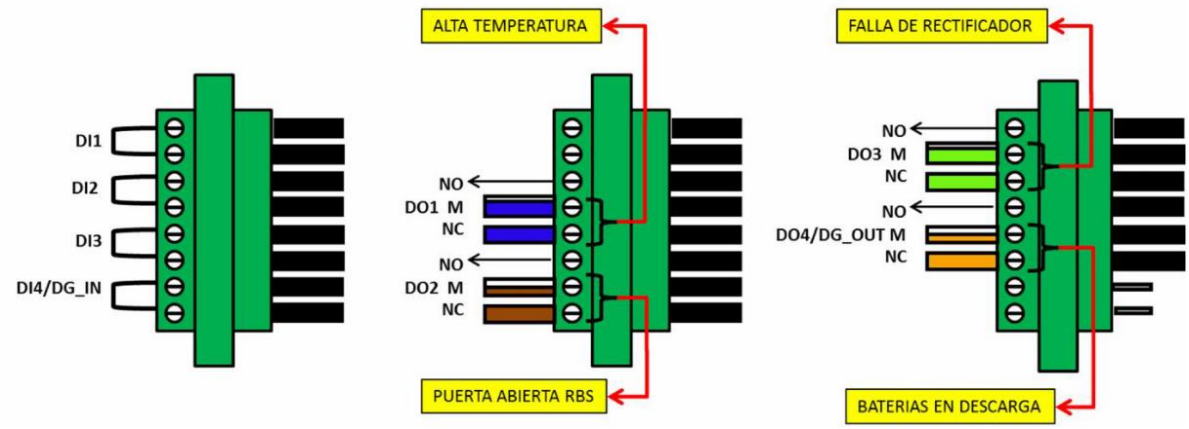


Figura 47. Conexión de alarmas externas - Borneras

En la figura 48, se visualiza la conexión entre una bornera SUP RBS 6601 HACIA OVP- ALM8 con detalle de código de colores en RJ45.

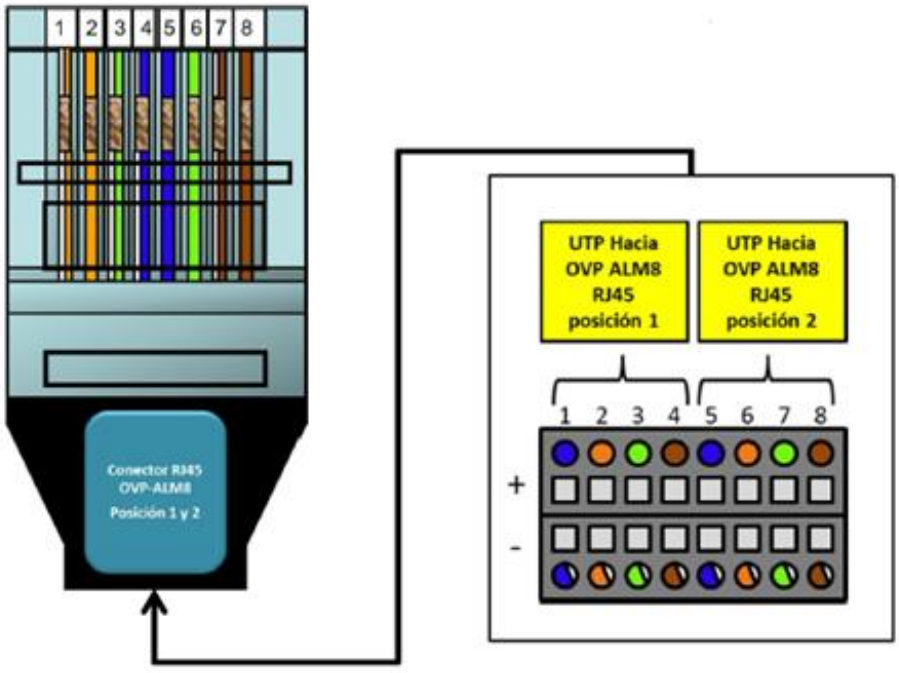


Figura 48. Conexión Bornera SUP hacia OVP

Cuando el sitio no cuenta con MG la designación de pines no cambia, únicamente se simplifican las conexiones ya que son variables menos que se cesan. Observa la tabla 2.

Tabla 2. ALARMAS EXTERNAS SITIOS SIN MG

ESTANDAR PARA SITIOS SIN MG					
NORMAS PARA INSTALACION DE ALARMAS EXTERNAS					
2	1	BLANCO-NARANJA/NARANJA	BATERIAS EN DESCARGA	CRITICA	RBS
2	2	BLANCO-VERDE/VERDE	FALLA DE RECTIFICADOR	MAYOR	RBS
2	3	BLANCO-AZUL/AZUL	ALTA TEMPERATURA	MAYOR	RBS
2	4	BLANCO-CAFÉ/CAFE	PUERTA ABIERTA DE RBS	MENOR	RBS
1	4	BLANCO-NARANJA/NARANJA	CORTE DE AC COMERCIAL	MAYOR	RBS

En la figura 49 se tienen entradas providentes del gabinete de la RBS, pasan por el OVP y se dirigen a las unidades DU.

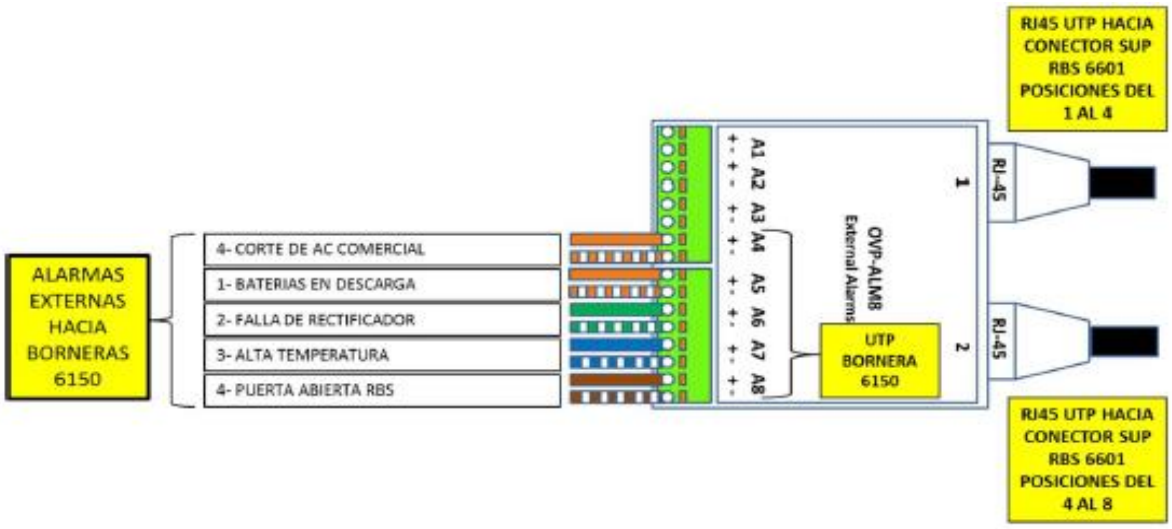


Figura 49. Alarmas Externas sitio sin MG

En dependencia de la tarjeta de la Unidad Digital y del tipo de gabinete de RBS, existen diversos escenarios de conexiones físicas desde las generaciones de alarmas bien sea provenientes del módulo de control del Motor Generador o del mismo gabinete RBS hasta llegar a la DU. En la Figura 50, se muestran los escenarios de conexión más probables para alarmas externas.

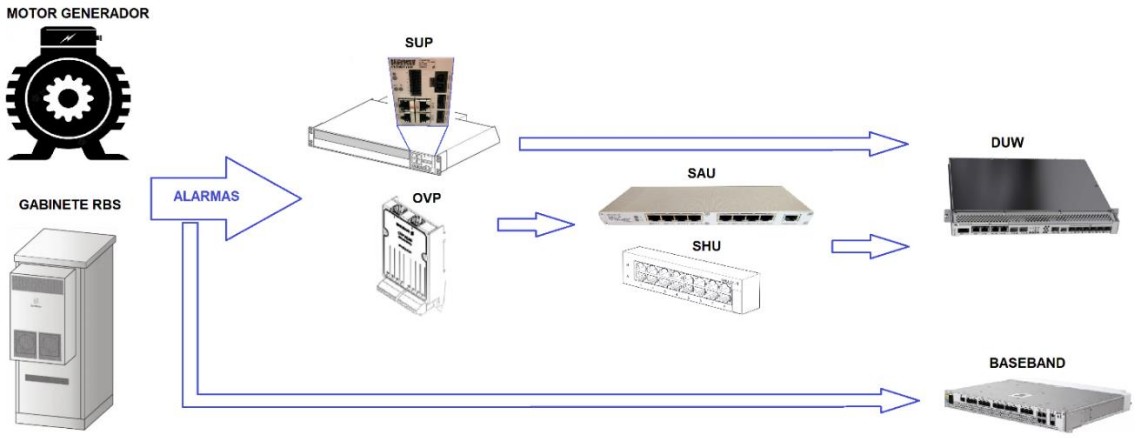


Figura 50. Conexiones alarmas externas hacia las DU

En la gráfica se plantean 3 escenario que se explican a continuación:

1. Cuando la Unidad de control de la RBS es una DUW y el gabinete es un 6601, las alarmas externas se reciben la tarjeta SUP, la cual se encarga de administrar los recursos de clima (fanes) y las alarmas eternas, luego se conectan a las DU mediante el puerto EC. Existe la posibilidad que se instale antes de la SUP un OVP como protector de voltaje para que no se dañen los puertos de la SUP, sin embargo, no es necesario para el funcionamiento de las alarmas.
2. Cuando la Unidad de control de la RBS es una DUW, pero los gabinetes no necesitan SUP para su funcionamiento porque el sistema de clima es independiente como las 6101, 6102, para el reconocimiento de las alarmas externas se requiere de una tarjeta OVP que se encargara de enviar los pulsos de alarmas hacia un equipo intermediario que se administraran todas las alarmas tanto externas como internas, a las tarjetas SAU y/o SHU, los cuales son elementos de multiplicación para alarmas, tienen varios puertos para recibirlas y las transmiten a la DU mediante un solo medio hacia el puerto EC.
3. Cuando la Unidad de control de la RBS es una baseband no se necesita ningún elemento intermedio, las alarmas entran directamente hacia el puerto de alarmas de la BB. Es posible que en algunos gabinetes le instalen OVP como una medida de protección para los puertos de alarmas de la Baseband

ya que si se dañan se tendría que cambiar toda la BB o quedar sin supervisión de alarmas, pero no es un elemento necesario para el funcionamiento de las alarmas.

Es importarte conocer los escenarios de conexión de alarmas ya que cada elemento que interviene en el procesamiento de la alarma es punto potencial de falla y debe ser revisado por el Ingeniero de campo cuando se atiendan eventos en donde se estén generando falsos positivos.

7.2.1.2. Configuración lógica de alarmas externas

Las alarmas externas se reciben en los puertos EC de las tarjetas de control de las RBS (DUG, DUW, DUS, BaseBand). La configuración del texto de la alarma se puede efectuar tanto de manera local por el Ingeniero de campo como de forma remota por el Ingeniero NOC, sin embargo, al realizarlo de forma remota no se tiene la certeza de que las conexiones físicas de las alarmas se correspondan con el puerto lógico en donde se hará la configuración, es por ello que la configuración inicial se realiza de forma local durante el proceso de integración del sitio, luego si se hará algún cambio en el texto de la alarma se debe valorar si es conveniente realizar localmente o remotamente.

Pasos para configuración lógicas de alarmas:

1. Se deben identificar las interfaces lógicas de alarmas y el MO asignado con el comando ***get alarmport***. Al ejecutar el comando se brinda información de puertos de alarmas y los puertos de fanes (SCU) en caso de tener el gabinete. Se debe buscar los puertos que hagan referencia a las tarjetas que manejan las alarmas: SUP, SAU o BB, dependiendo del tipo de Hardware instalado.

   En la figura 51, se muestra un ejemplo para 2 sitios con distinto Hardware:

   El primero tiene una tarjeta de control DUW4101, las alarmas son recibidas desde una tarjeta SAU, en la primera línea seccionada se puede observar el texto: Equipment=1,HwUnit=SAU-1,AlarmPort=1, nos indica que la información en el tramo seccionado que se presentara es la configuración para el Puerto 1 de la SAU, Adicional del dado izquierdo del texto, está el numero: 861, el cual es la referencia lógica MO/Proxy asignado a ese puerto.

Por cada tramo/puerto se brinda información de la configuración actual, para el puerto 1, Se etiquetó a nivel lógico como CORTE DE AC COMERCIAL y su estado es UNLOCKED (ACTIVO). Para editar el texto los campos de interés son: administrativeState, alarmSlogan.

El segundo ejemplo de la figura 51, se tiene una tarjeta de control BASEBAND: Equipment=1,FieldReplaceableUnit=BB-1,AlarmPort=1. Las alarmas entran directamente a la Baseband, pero los campos a evaluar son iguales. Se debe tener en cuenta el número de MO/Proxy para la posterior configuración.

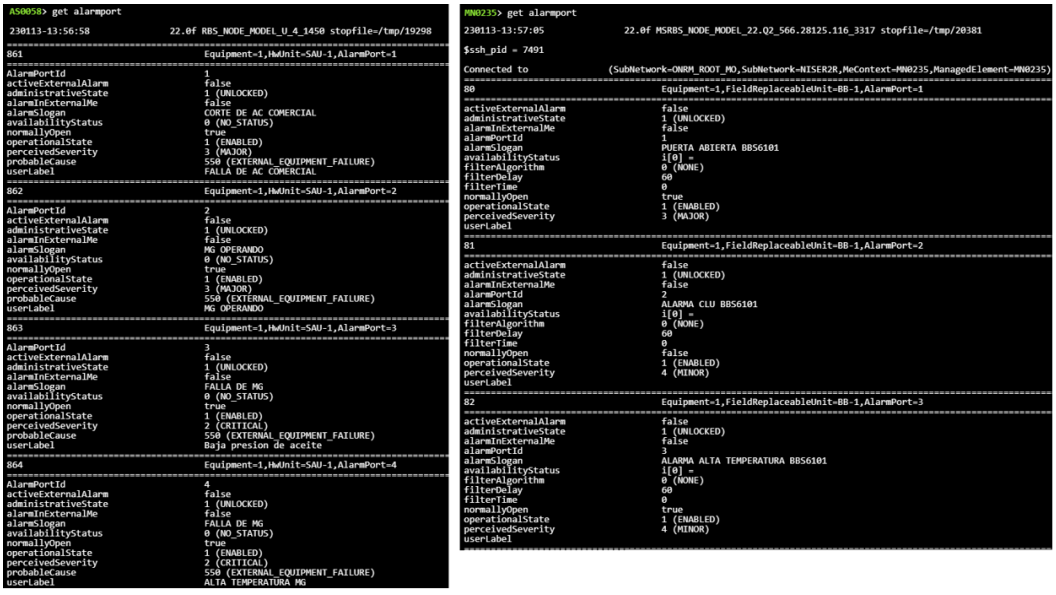


Figura 51. Verificación lógica de puertos de alarmas

2. Una vez se tenga identificado el puerto lógico sobre el cual se hará la configuración e identificado el MO/Proxy asociado al puerto, se procede a bloquear la alarma con la instrucción: ***bl (#proxy)***.

   Observe en la figura 52, con el comando get (#proxy) se visualiza puntualmente el puerto de interés, el campo administrativeState tiene como estado UNLOCKED, luego de aplicar la instrucción ***bl 861***, se verifica nuevamente y dicho campo cambio a estado LOCKED.

   Es necesario bloquear la alarma antes de aplicar un cambio ya que si se ejecuta un cambio sin previo bloqueo la instrucción nueva no tiene efecto.

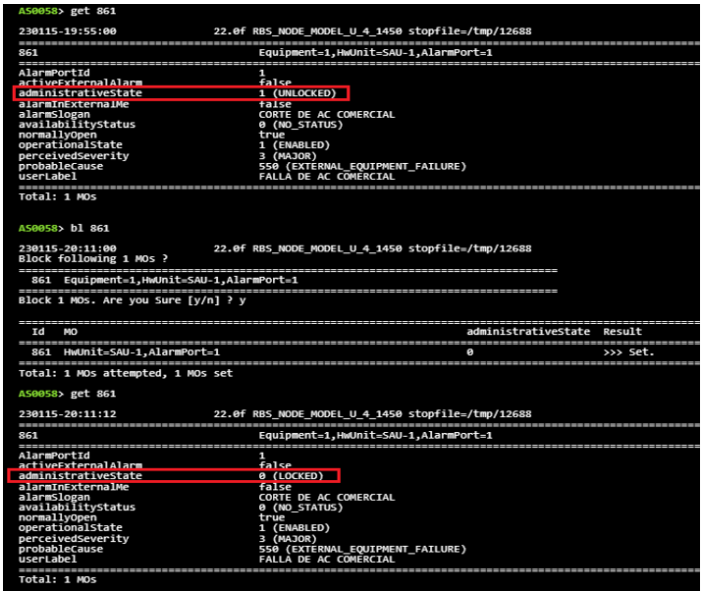


Figura 52. Bloqueo de alarmas externas

3. Una vez se bloquee el proxy, se procede a ejecutar la instrucción de configuración de la alarma la cual lleva la siguiente sentencia, observan el ejemplo:

   set (#proxy) alarmSlogan (Texto a configurar)
   set 861 alarmSlogan FALLA DE RED COMERCIAL

   Observa en la figura 53, inicialmente con el comando ***get*** observamos que en el campo ***alarmSlogan*** tiene el texto CORTE DE AC COMERCIAL, luego ejecutamos la instrucción set con los parámetros de configuración indicados y cambiamos el texto a FALLA DE RED COMERCIAL.

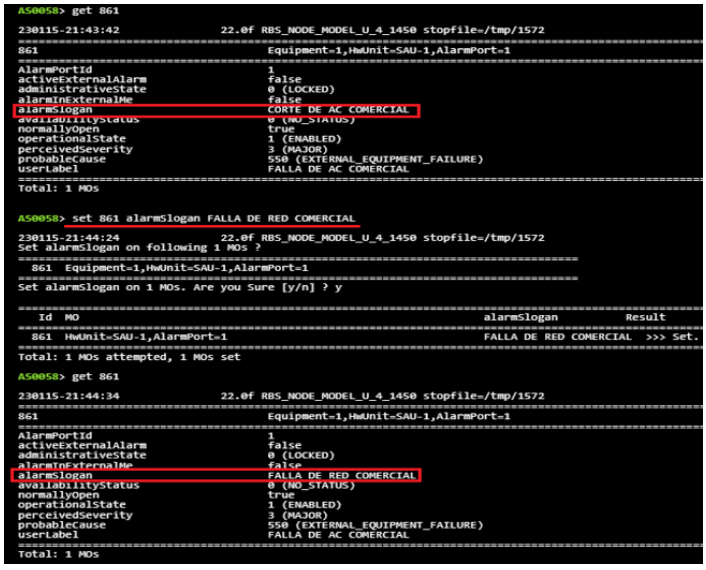


Figura 53. Configuración de Slogan Alarmas Externas

4. Luego de realizar la configuración del nuevo Slogan (texto) de la alarma es necesario activarla nuevamente, es decir, el campo alarmSlogan debe quedar en condición UNLOCKED. Si no queda activa la alarma, cuando suceda un evento de corte de energía, en cual se debería visualizar la alarma, no será visible porque está bloqueada, es por ello, que debe quedar activada. Para efectuar este paso ejecutamos el comando ***bl (#Proxy);*** para este ejemplo seria ***bl 861***.

   Observa la figura 54, inicialmente la condición del campo alarmSlogan era LOCKED, luego de ejecutar la instrucción ***deb 861***, cambio a condición UNLOCKED. En esta condición si hubiese un evento de energía se mostraría la alarma FALLA DE RED COMERCIAL según el texto que configuramos. Si la tarjeta de control de Nodo B fuese una Baseband, los comandos a ejecutar para efectuar las configuraciones de las alarmas serian exactamente los mismos, siempre teniendo en cuenta el puerto que se hará la configuración y su proxy asociado. El mismo procedimiento es aplicado para las demás alarmas: BATERIAS EN DESCARGA, MG OPERANDO, FALLA DE MG, etc.

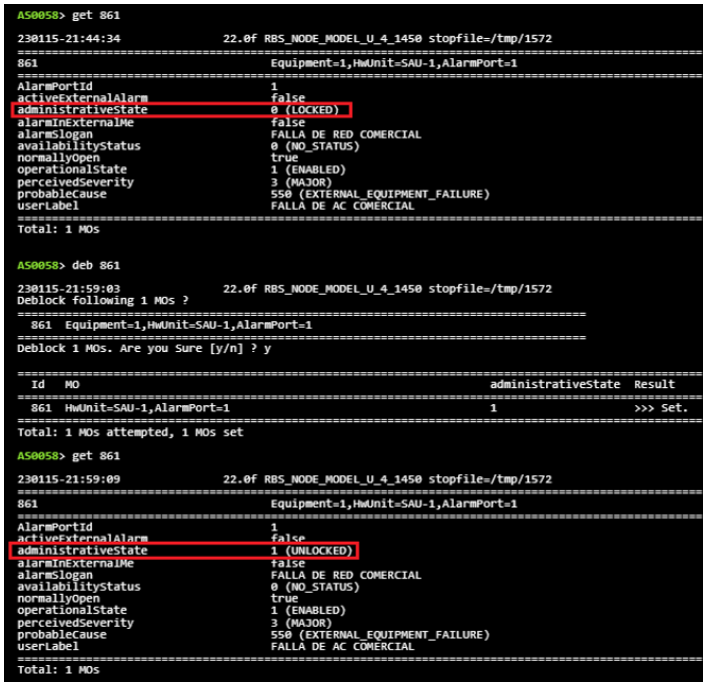


Figura 54. Activación de alarmas externas

5. Por último, luego de hacer todos los cambios debemos crear un CV nuevo que guarde las configuraciones ejecutadas y dejarlo como start table; con ello logramos en casos de reinicios de la tarjeta de control, se recargue la última configuración ejecutada y nuestras alarmas continúen trabajando correctamente. El modo de crear un CV varía entre una DUW y una BaseBand. Para crear un CV utiliza los siguientes comandos:

   Crear CV: ***cvms (Nombre_del_CV)***
   Configurar CV como Startable: ***cvset (Nombre_del_CV)*** En DUW/DUS
   Configurar CV como Startable: ***cvre (Nombre_del_CV)*** En Baseband

   Para verificar listado de CV del Nodo use el comando: ***cvls***

7.2.1.3. Monitoreo Remoto de la red

El monitoreo remoto de la red respecto a la alarma de energía, se puede atender desde dos tipos de entradas a como fue explicado en el capítulo 3. Idealmente cuando suceden eventos de energía en la red, la alarma que se genera en el gestor nativo es capturada por el TeMIP, ésta plataforma de acuerdo a las reglas que tenga configuradas, enviara a aperturar un ticket con los detalles de la alarma de energía en la plataforma de apertura de Incidentes. Luego el Ingeniero NOC deberá ingresar al sistema, asignarse el Incidente, verificar la información que muestra, corroborar en el gestor nativo puntualmente el sitio alarmado y por ultimo enviar al Ingeniero de campo a atender la falla.

El segundo escenario, es que el Ingeniero NOC aplique un filtro de alarmas sobre el gestor nativo con la alarma que le interesa visualizar. Y en base a su criterio decida movilizar al Ingeniero de campo. Ambos casos son válidos la preferencia de uno sobre otro depende de la situación.

Es importante también manejar una base de datos que le indique al ingeniero NOC el tipo de infraestructura del sitio, principalmente si cuenta con respaldo de Motor Generador y baterías o sino tiene respaldo de MG y únicamente su fuente de autonomía ante eventos energético es su banco de baterías.

Sitios con respaldo de MG

Cuando un sitio tiene Motor Generador y suceden un evento de energía el criterio a tener encuentra es si el MG entró a Operar y Asumió la carga del sitio o si el MG Falló y el sitio está corriendo en baterías. Para ello el Ingeniero NOC hace una

revisión de alarmas desde el gestor nativo móvil para el sitio de interés y se evalúan las siguientes combinaciones de alarmas:

- **CORTE DE AC COMERCIAL + MG OPERANDO:** Cuando esta combinación de alarmas está activa nos indica que en el sitio hay un evento de energía, los más probable desde la red comercial, aunque puede haber sus excepciones y la falla sea interna a nivel de breakers en panel principal o cableados hasta la trasferencia del Motor Generador y dicho MG está asumiendo la carga del sitio.

  En la figura 55 se muestra la visualización de las alarmas externas en evaluación mediante la vista de interfaz GUI (grafico) y CLI (comando).

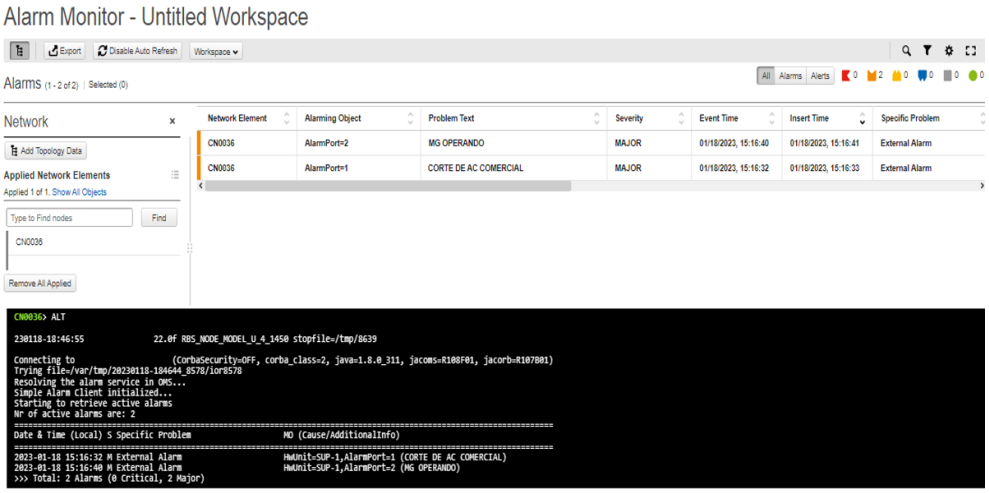


Figura 55. Alarmas Externas Corte AC + MG Operando. GUI - CLI

Bajo este escenario de alarmas durante un periodo prudencial no es necesario enviar al Ingeniero de campo RBS o la contrata encargada de atender los eventos de energía porque no existe un riesgo de caída potencial del servicio. Hay un MG que está energizando a la RBS y con ello garantizando la disponibilidad. La gestión del Ingeniero NOC bajo esta condición, es hacer un reporte al distribuidor eléctrico para que corrijan la averías a nivel de su red eléctrica. En Nicaragua el principal proveedor de energía en Unión Fenosa, para efectuar un reporte con ellos, se digita la marcación corte 125 desde cualquier Operador fijo o móvil y un call center atenderá para tomar los datos, generan un reporte y posteriormente movilizar a una cuadrilla que haga revisión en su red eléctrica.

Cuando el MG cumple un tiempo de operación continuo prolongado que no hay retorno de energía, es prudente efectuar una movilización con el personal de energía (interno o contrata) para haga una revisión eléctrica y determine si efectivamente el problema es derivado de una falla con el distribuidor y en dicho caso el Ingeniero NOC puede hacer insistencia con la seguridad que es un evento externo al sitio o que determine si hay problema interno que deban atender y de este modo cesar las alarmas.

Existe la posibilidad que las alarmas sean falsas y que exista una falla en los elementos de alarmas, este escenario únicamente será identificado después de una revisión de campo con el personal de energía, para resolver el problema será necesaria una movilización del Ingeniero de campo especialista en RBS.

- **CORTE DE AC COMERCIAL + BATERIAS EN DESCARGA:** Ésta combinación de alarmas que se visualiza en la figura 56, indica que en el sitio hay un evento de energía, al igual que el caso anterior puede ser un evento de externo al sitio o una falla interna. Sin embargo, la condición de BATERIAS EN DESCARGA es un indicativo que el MG falló, no está asumiendo la carga y es una alerta de una caída potencial del servicio. La RBS estará operando hasta que se agote la carga de las baterías. Es por ello que a diferencia del escenario anterior acá es urgente una movilización para Revisión de MG no Operativo. El Ingeniero NOC hará las gestiones correspondientes con el personal de campo encargado de la revisión del Motor Generador que por lo general es una contrata especializada en ello. El Objetivo de esta gestión es poner en Operación el respaldo de MG y evitar la afectación del servicio, y caso que se afecte, procurar que el tiempo de indisponibilidad sea el menor posible.

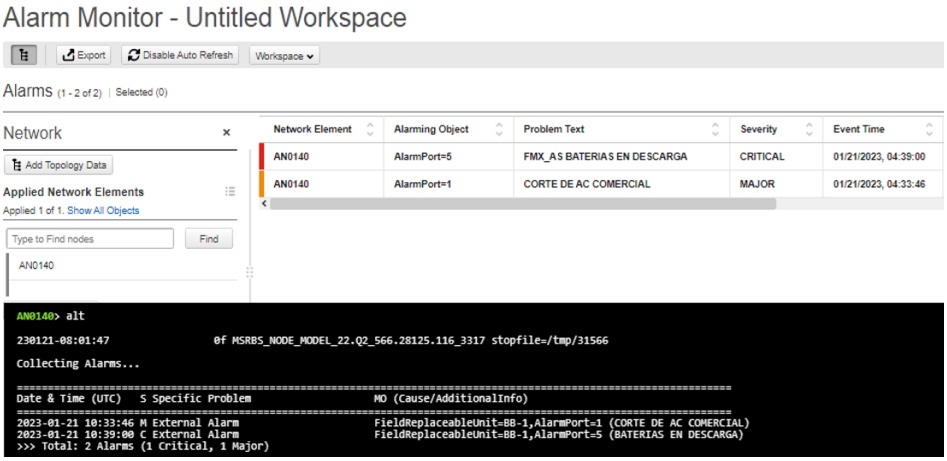


Figura 56. Alarmas Externas Corte AC + Baterías en descarga. GUI - CLI

En paralelo a la movilización de la cuadrilla que atenderá la revisión del MG es prudente realizar un reporte con el proveedor eléctrico para garantizar el restablecimiento de la red comercial.

Luego que el personal de campo resuelva el problema del MG y éste entre en operación, el Ingeniero NOC debe hacer nuevamente validación de alarmas del sitio que estuvo afectado, garantizar que quede sin alarmas de Baterías en descarga, que aparezca la de MG Operando y en caso de el servicio se hubiera tendido afectado, debe garantizar que todas las tecnologías del sitio queden en operación y con tráfico. Una vez llegado este punto de la atención, vuelve al primer escenario planteado y los pasos a seguir son cuando se tienen alarmas Corte de AC Comercial + MG Operando.

En este segundo escenario también existe la posibilidad que las alarmas sean falsas y que exista una falla en los elementos de alarmas, o elementos de energía internos de la RBS como PSU, BFU, PDU, lo cual será identificado después de una revisión de campo con el personal de energía, para resolver el problema será necesaria una movilización del Ingeniero de campo especialista en RBS para que realice revisión, identifique y cambie el elemento dañado.

- **SITEMAS SOLARES Y RESPALDOS ALTERNOS:** Adicional a los dos escenarios explicados, existe una tercera posibilidad de combinación de alarmas; existen sitios en los que los operadores opten por instalar sistemas solares como la fuente de energía principal del sitio y un Motor Generador como una fuente de respaldo. También puede darse la posibilidad que operador tengo como fuente de energía principal un banco de baterías de gran capacidad y que se esté recargando mediante un Motor Generador, estas posibles combinaciones de sistemas energético surgen como una necesidad para mantener en operación los sitios que están ubicados en zonas muy alejadas y en donde aún no existe una red de distribución eléctrica por parte de ningún proveedor de energía en el país. El ingeniero NOC debe tener claro el tipo de infraestructura energética que tiene el sitio que presente alarmas y cuál es su modo de trabajar para decidir si realiza una movilización de personal o, aunque estén las alarmas no es necesario enviar personal a campo.

  Cuando se tiene un sitio cuya principal fuente de energía son los paneles solares, probablemente siempre se observarán alarmas de Baterías en

descarga (externas) o Running on Battery Supply (internas), ya que el sistema solar estará cargando el banco de baterías y estas a su vez energizando a la radio base. Si el sistema solar no está trabajando por la condición climática, entonces el Motor Generador tomara la tarea de entrar en operación y suministrar energía a la radio base.

Sucede algo similar cuando la fuente de energía principal son las baterías, la mayor parte de tiempo se tendrá presente la alarma de BATERIAS EN DESCARGA, cuando las baterías agoten carga, el Motor Generador se encargará de suministrar energía a la radio base y cargar las baterías para un nuevo ciclo de trabajo. Es decir que no es necesario movilizar personal al sitio en ninguno de los dos escenarios planteados ya que es parte de la operación normal del mismo.

Es por ello que la movilización del personal, dependerá cuando se reciba alarma que indique que el MG no entró a trabajar cuando correspondía su turno de operación. Dicha alarma se configura como externa en las radios bases con el texto: FALLA DE MG a como se visualiza en la figura 57.

Figura 57. Alarma Externa Falla de MG. GUI.

Sitios sin respaldo de MG

Cuando un sitio no cuenta con respaldo de Motor Generador, bien sea porque es un poste, una valla, un hotel, centro comercial, hospital, complejos de oficinas o simplemente de difícil acceso y sin mucho espacio de maniobra para implementar un Motor Generador, cuando se tengan eventos de energía, las únicas alarmas que recibirán serán las de Corte de AC Comercial y Baterías en descarga, en algunos casos que el tipo de radio base no permita configurar este tipo de alarmas, se recibirán como alarmas internas: Loss of mains (Comercial Power Failure) y Running on Batery Supply en el campo Specific Problem del ENM a como se observa en la figura 58.

Algunos gabinetes micro incluso no generan alarmas por caídas de energía. Pero en los sitios que es posible monitorear las alarmas, el Ingeniero NOC debe

gestionar movilización de personal acorde al criterio consensuado en su organización, para evitar caídas del servicio.

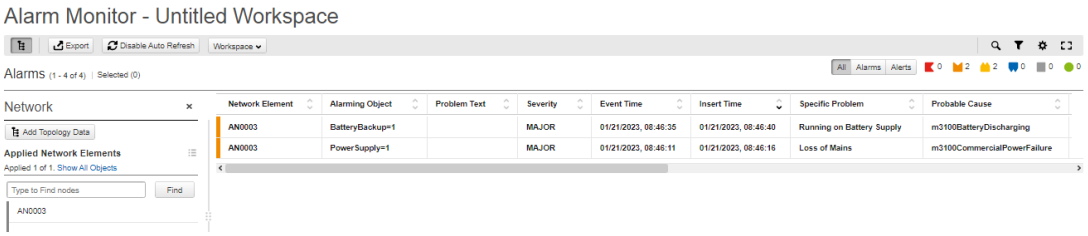


Figura 58. Alarmas Internas Comercial Power Failure . Running on Battery. GUI.

Las posibles gestiones que el Ingeniero NOC debe realizar cuando un sitio sin MG está con alarmas por caídas potenciales de energía son las siguientes:

- Aperturar reporte con el distribuidor eléctrico, se debe realizar la consulta si hay un trabajo programado, hora de normalización, y en caso de no haber, solicitar que generen un numero de aviso para movilización de cuadrillas.
- Validar el tiempo de autonomía del sitio, es decir debe verificar cuanto tiempo tienen de respaldo de baterías el sitio, esto lo pueden realizar desde una base de datos que facilite el área de campo según las instalaciones previas, si no se cuenta con una base de datos o se cree que pueda estar desactualizada, se puede hacer la consulta directamente al equipo encargado de instalar baterías si existe un tiempo aproximado que se maneje sobre la autonomía del sitio.
- Verificar si los sitios tienen dependencias, con ayuda del equipo de Ingenieros NOC de transporte se debe consultar la topología a nivel de medio de transmisión en la que se encuentra el sitio, éste es un criterio muy importante, ya que puede ser último elemento, puede estar en un anillo sobre el cual sea posible habilitar redundancia y al hacerlo en caso de afectación el sitio sería el único caído, o pueden estar una topología línea con una o más dependencias.
- Consolidar la información, contrastar los tiempos de retorno y respaldo con las dependencias y en base a criterios de su organización movilizar personal o solicitar autorización para movilizar recursos para instalación de una fuente de energía provisional mientras retorna la red comercial (planta portátil).
- Validar que cesen las alarma.

7.2.1.4. Trabajo de campo

La función del personal de campo para alarmas de energía es habilitar la fuente de energía alterna mientras retorna la red comercial para sitios que cuentan con una red de distribución eléctrica, y habilitar la fuente de energía principal en los sitios que no. Según fue explicado en el inciso de monitoreo remoto existen sitio que cuentan con Motor Generador y otros que operan Sin Motor Generador. En Nicaragua los Operadores de telecomunicaciones subcontratan empresas para atención de eventos relacionados con fallas de energía en los sitios celulares.

Atención de sitios con Motor Generador

Cuando un sitio tiene MG y se reporta como una falla, el personal de campo debe garantizar las siguientes revisiones en sitio:

- Revisión general del sitio: Desde el medidor para ver si hay red comercial, panel eléctrico y si los equipos están encendidos, Niveles de combustible, niveles de aceite, nivel de refrigerante, conexiones eléctricas para descartar flojedad, revisión de módulo de control, horas trabajadas, perímetro, descartar vandalismos y robos con datos de bitácora contrastado con horas de operación y el nivel de combustible medido.
- Revisión de alarma en el módulo de control del MG, se revisa que alarma hay presente y realizar las pruebas correspondientes para cada escenario posible.
- Si la alarma en módulo de control es BAJA PRESION DE ACEITE. Se debe efectuar una revisión visual de conexiones en busca de posibles fugas, ver si en el suelo hay manchas de aceite que pueden ser provocadas por filtros en mal estado, tapones zafados o con flojedad por la vibración del motor o daños en empaques de la culata, si hay indicios alguno de estas posibilidades, se debe limpiar el área del motor con aceite, lavar de ser posible, se enciende el Motor y se verifica por donde se fuga el aceite. Si no hay manchas que indiquen probable fuga, aplicar reset al módulo de control y mandar arrancar en manual el MG, luego validar en el módulo de control la presión censada, la cual debe mantenerse dentro los umbrales: 4.5 a 5.5 BAR o en otro sistema de medición entre 65 a 75 PSI. Si existe un nivel menor al umbral establecido probablemente el sensor este en mal estado, se revisará el cableado y las conexiones en busca de flojedad o sulfatación, harán limpieza de las terminales, si la falla persiste debe cambiar el sensor de presión de aceite y repetir las pruebas. Cuando la medición en módulo de control es superior al umbral pueden ser síntomas de descompresión, si esto pasa el motor tira aceite por los respiraderos y

se requiere un trabajo mayor en el motor de combustión, deberán realizar un Over houl.

- Si la alarma del MG es ALTA TEMPERATURA, se realiza una revisión visual de manchas de refrigerante en el suelo en busca de posibles fugas y flojedad en mangueras, luego se debe completar el nivel de refrigerante, aplicar reset al módulo de control y encender el MG para realizar una nueva revisión visual en busca de fugas en sistema de enfriamiento, radiador y precalentador. Deben revisar los valores de temperatura cesados en el módulo de control de MG, el rango de operación depende del tamaño del MG (10, 15, 25 KVA) pero oscila entre los 55 – 85 grados celsius. Se debe monitorear si la temperatura se mantiene estable o si va elevándose sobre el umbral de operación hasta generar la alarma, si se eleva, hay que revisar el sistema de circulación de refrigerante, bomba de agua y realizar limpieza de la bomba en busca de obstrucciones. Si todo lo anterior está bien puede ser un problema en el sensor de temperatura, se debe revisar el cableado y terminales en busca de flojedad en conexiones eléctricas o sulfatación, hacer limpieza y por último cambio del sensor. Otra posible causa es una banda reventada o floja que se verifica visualmente.
- La alarma BAJA FRECUENCIA DE GENERACION, aparece cuando varia la frecuencia del generador que es de 60 Hz con un rango de trabajo del 3%, cuando se recibe ésta alarma en el módulo de control, puede ser provocada por Bajo nivel de combustible, deben revisar niveles y abastecer el tanque. También puede haber aire en el sistema, se debe verificar filtros, mangueras y realizar una purga, es decir, extraer el aire al sistema de combustible, aplicar reset al módulo de control y arrancar el MG, monitorear que trabaje estable.
- Si la alarma en módulo de control es ALTO VOLTAJE. Puede ser provocado por AVR dañado por alto o bajo voltaje, se reinicia el modulo control, se arranca el Motor Generador, se revisan los valores de cesado de la red comercial, deben oscilar entre los 200V y 250V. Para corregir la falla se regula el potenciómetro del AVR, se verifica si cambia el valor de censado, sino lo hace, se debe cambiar el AVR. Si se cambia el AVR y continua la falla, posiblemente se tenga problemas en borneras del generador (corto circuito), hay que validar posibles cortocircuitos en borneras. Se valida puentes de diodos del generador, si están quemados y si tienen continuidad, en última instancia si se diagnostica generador dañado, se desinstala y se le hacen pruebas mayores.
- Si la alarma del módulo de control es ARRANQUE FALLIDO, puede ser por baterías dañada (cortocircuitadas), se debe realizar pruebas en la batería de arranque o cambio de la misma, también puede ser provocado por aire

en las tuberías, para lo cual es viable realizar purga del sistema de alimentación de combustible.

- Si el módulo de control se encuentra apagado. Pueden ser flojedad en borneras de batería, o conexiones eléctricas en la entrada del motor de arranque, Se debe ajustar terminales, revisar cableado, realizar limpieza y cambiar batería, realizar pruebas en chicharra o auxiliar de arranque y verificar si el cargador de baterías está en mal estado y amerita cambio.
- Cuando todas las pruebas anteriores están bien y el módulo de control está sin alarmas, el Motor arranca correctamente. Puede existir un problema en módulo de Transferencia de carga eléctrica (ATS), que básicamente realiza la función de conmutar el suministro eléctrico hacia la radio base entre la energía de la red comercial y la energía producida por el Motor Generador, si falla la transferencia, aunque el MG entre en operación, la radio base continuara en baterías, para validar el ATS, se verifican si hay algún breaker disparado o relevadores de señal de bobina de transferencia visualmente si esta quemados, bobina o cables con flojedad hacia bobina. Se debe reemplazar la ATS y verificar si realizar correctamente la transferencia y re transferencia de carga.

Atención de falla sitio sin Motor Generador.

Cuando un sitio no tiene MG y se reporta con alarmas de energía, el personal de campo debe garantizar las siguientes revisiones en sitio:

- Medición del Voltaje de entrada y salida del medidor, que lleguen y salgan correctamente los 220 VAC desde la red de distribución eléctrica y que no se tenga problemas en las fases.
- Si llega a conclusión que no hay red comercial, se debe instalar una fuente de energía provisional, es decir, una planta generadora eléctrica portable y garantizar que los equipos enciendan nuevamente y el servicio entre en operación.
- Si hay red comercial en el suministro eléctrico, se debe continuar con una visión eléctrica del sitio.
- Revisión de panel eléctrico de energía, igualmente se miden los voltajes de salida en los breaker que están en producción.
- Revisión de breaker en RBS, se debe garantizar por medio una revisión visual que todos los breaker de la radio base estén operacionales y no se encuentra disparados o semi disparados.
- Medición de voltajes en elementos de energía de la RBS, se debe garantizar que le lleguen 54VDC a los equipos.

7.2.2. Fallas de energía DC

7.2.2.1. Conexión de alarmas internas de energía DC

En una radio base se ha explicado que existen alarmas provenientes de elementos externos a la radio base y alarmas provenientes de elementos internos; las alarmas externas ya fueron abordadas en la primer etapa de esta guía, respecto a las alarmas internas, podemos entenderlas como la que se cesan eventos dentro del gabinete de la radio base, algunas se pueden configurar como es el caso de: ALTA TEMPERATURA, PUERTA ABIERTA, FALLA DE RECTIFICADOR y otras no son editables ya que los scrip vienen cargados por default en las tarjetas DU de la RBS, únicamente se garantiza que el cableado interno y las conexiones a nivel de tarjetas estén correctas.

En esta segunda etapa de alarmas de mayor incidencia sobre la disponibilidad de la red se abordará las alarmas de energía DC, es decir, alarmas sobre los elementos que se encargan de proveer y distribuir la energía rectificada en DC hacia los demás elementos de la radio base, los cuales son: RECTIFICADORES, BATERIAS, PSU, PDU, BFU.

Las alarmas sobre los RECTIFICADORES es la única que se puede editar el texto de alarma, en el inciso de Configuración de alarmas externas 9.2.1.2 está la forma de efectuar una revisión de los puertos asignados en las DU y la edición del campo alarmSlogan para cambiar el texto de la alarma, es por ello que para las alarmas internas de energía DC no habrá un inciso de configuración, únicamente se explicará la conexión de los elementos para un entendimiento del funcionamiento de cada uno.

En la Figura 59 se puede observar dos tipos de escenarios para conexión de alarmas internas, cada uno depende del tipo de gabinete que tienen la radio base, la primera parte (remarcado con señalización azul) es referente a gabinetes que poseen una controladora de gabinete como las RBS6150 o PBC05, mientras que la segunda parte (remarcado con señalización naranja) refiere a gabinetes que no poseen una controladora de gabinete como es caso de las RBS 6101 y 6102.

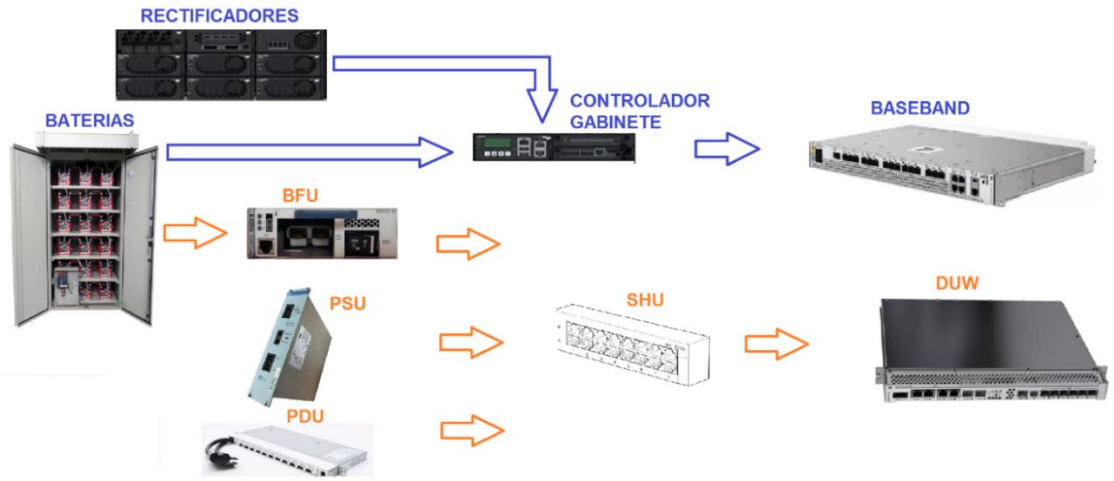


Figura 59. Conexión de alarmas internas hacia las DU

Cuando se tiene un controlador de gabinete, todas las variables internas de la RBS son censadas en primera instancia por el controlador, es decir que éste elemento multiplexa las señales para luego enviarlas a la tarjeta DU, en el ejemplo una BASEBAND. Los 2 elementos relacionados a energía DC del gabinete son las baterías y los rectificadores, ambos se conectan directamente al controladora de gabinete, aunque se tenga un banco con muchas baterías y un sistemas de rectificación de corriente con muchos módulos rectificadores, al salir del controlador se generara un único pulso de alarma, lo que significa que además de multiplexar la señales, se debe entender que cuando falle cualquiera de los elementos de entrada, por ejemplo uno de ocho módulos rectificadores, se generara una alarma de falla de FALLA DE RECTIFICADOR, igualmente si fallan dos o tres módulos, continuara generándose la misma alarma; la cantidad de módulos rectificadores del gabinete depende de la carga que se conectara, es posible se tenga falla en alguno de los módulos, pero el consumo de los equipos sea más bajo que la corriente que generan los módulos restantes y por ello no se tengan fallas de servicio, o puede suceder el escenario inverso que la carga este conforme a la cantidad de módulos rectificares instalados y cuando un módulo se dañe inicie a afectar el servicio por reinicio constantes de equipos.

Para el caso de las baterías, el controlador de gabinete quien manda a cargarlas y se encarga de controlar la conmutación de carga cuando suceden eventos de fallas en la red comercial, de igual modo recibe la señal de alarma y la envía a la Baseband, si el banco de baterías falla, se generan alarmas como Battery Missing o Battery Disconneted (textos no editables).

Luego del controlador de gabinete existe una conexión directa hacia la BaseBand en los puertos de alarmas, pero la configuración de los mismos ya viene por

establecida por el proveedor en el scrip inicial de la radio base, no es editable para los ingenieros NOC y Campo. Aunque la conexión entre el controlador de gabinete y la baseband sea directa, también existe el escenario donde se coloque un elemento intermedio como protección a los puertos de la BaseBand, pueden tener instalado un OVP, pero no es necesario para el funcionamiento de las alarmas, estaría únicamente con medio de protección a sobre voltajes.
Cuando un gabinete no posee un controlador, el banco de baterías necesita un elemento que controle la carga de las mismas, esta función es efectuada por la BFU que además se encarga de enviar el pulso de alarma hacia la SHU. Para la rectificación de la corriente en DC, no existe un módulo rectificador como el escenario anterior, se tienen instaladas elementos modulares que efectúan esta tarea llamados PSU; una radio base puede tener varias PSU y todas ellas ocupan un puerto distinto en la SHU, así que, a diferencia de los rectificadores, cuando se daña una PSU podemos saber de forma remota cual es el HW que está fault, ya que se genera una alarma por cada elemento.

Existe otro elemento de energía que es monitoreado desde la DUW, son las PDU cuya función es distribuir la energía DC en los elementos internos de la RBS, al igual que las PSU, cada PDU ocupa un puerto de alarmas en la SHU por lo que se puede saber de forma remota que PDU está fallando. Luego de recibir todas las señales entrantes, la SHU las multiplexa y saca una única conexión hacia la DUW.

7.2.2.2. Monitoreo Remoto

El monitoreo de estas alarmas consiste en poder identificar cuando un elemento de energía está fallando. Se pueden dar varios escenarios para detectar la falla, por ejemplo, bien sea las PSU, PDU o BFU generen alarma de Hw Fault y el Ingeniero NOC lo visualice desde una alerta por un ticket de falla o por un filtro de monitoreo contextualizado en las alarmas mencionadas, o bien se tenga intermitencia a nivel de servicios, no existan alarmas presentes al momento de la revisión y se tenga que valorar un log de alarmas para ver si alguno de los elementos está fallando.

Las alarmas que comúnmente se generan son:

- Battery Missing
- Battery disconneted
- FALLA DE RECTIFICADOR
- HwUnit=PDU Disconnected
- HwUnit=BFU Disconnected
- General HW Error BFU
- Loss of Mains HwUnit=PSU-2
- PSU Output Power Failure

Una vez se verifique se tienen una falla en alguno de los elementos DC, se debe ubicar y verificar el elemento afectado a nivel remoto. En la figura 60, se muestra como validar los elementos de energía que generan un valor de entrada o salida en voltaje o corriente DC, con el comando ***lpr energy***, visualizamos los elementos y su MO/Proxy, es importarte identificar el MO del elemento que tenemos alarmado para luego buscar las mediciones energéticas sobre dicho elemento.

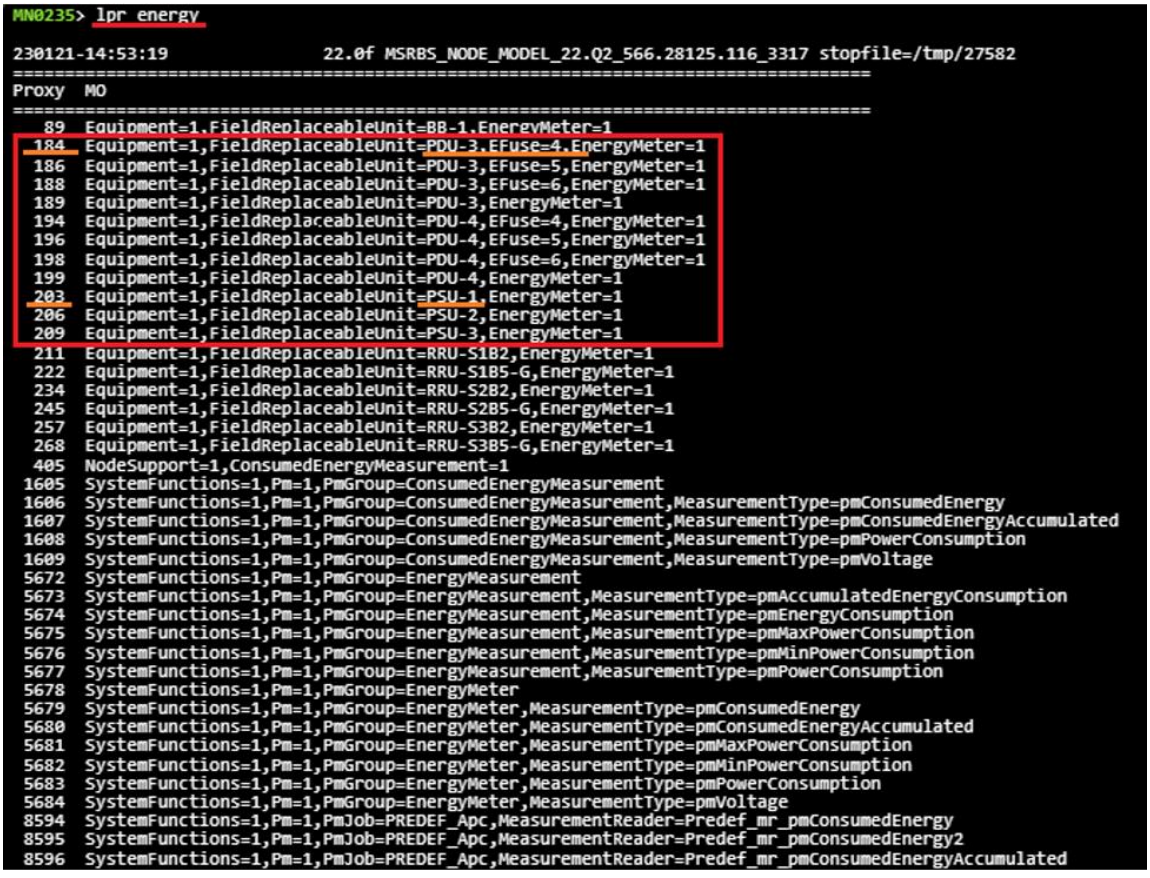


Figura 60. Verificación de elementos energía DC. ENM CLI

En la Figura 61, se observa que mediante el comando ***get***, se obtienen el valor de la medición de energía de los elementos cuando usamos en la sentencia el número del Proxy; por ejemplo, ***get 184*** muestra información de la PDU-3, su estado es ENBABLE, y su voltaje de salida 53.9V, sin embargo, si usamos get pero en la sentencia utilizamos el nombre del MO, obtenemos información del Hardware instalado, por ejemplo get BFU-1 nos dio información del HW de la BFU,

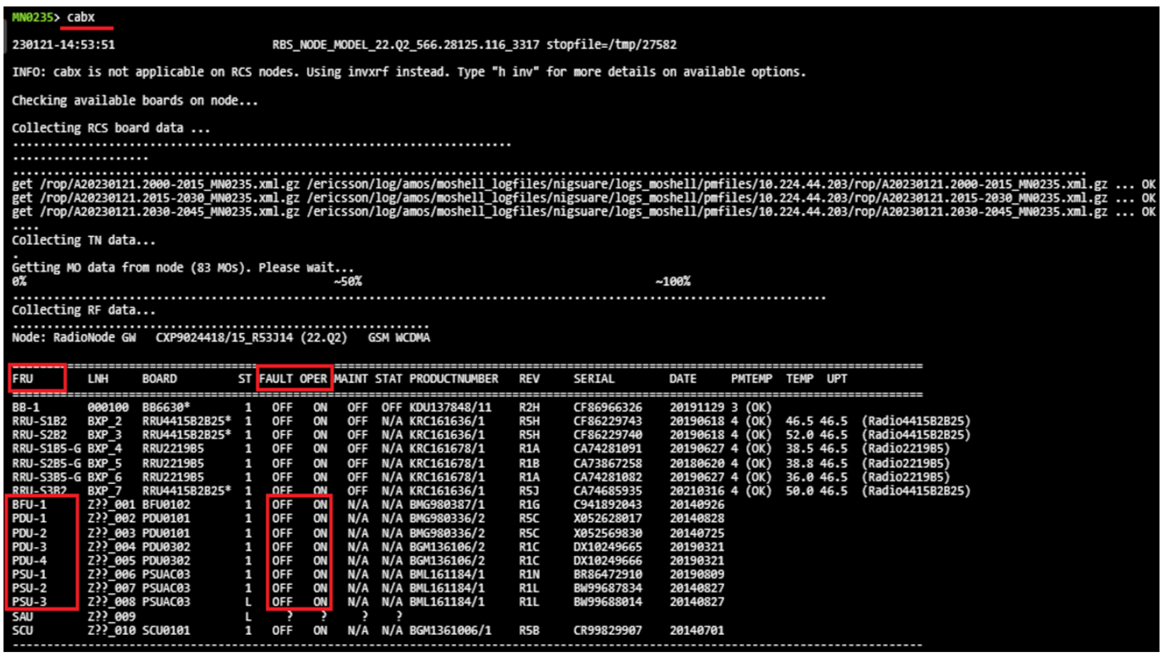
```
MN0235> get 184

230122-14:19:42              22.0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/15533

$ssh_pid = 20694

Connected to 10.224.44.203 (SubNetwork=ONRM_ROOT_MO,SubNetwork=NISER2R,MeContext=MN0235,ManagedElement=MN0235)
================================================================================================================
184                                  Equipment=1,FieldReplaceableUnit=PDU-3,EFuse=4,EnergyMeter=1
================================================================================================================
availabilityStatus                   i[0] =
consumedEnergyMeasurementRef
energyMeterEnabled                   1 (ENABLED)
energyMeterId                        1
inputCurrent
inputVoltage
operationalState                     1 (ENABLED)
outputCurrent                        4
outputPower                          217
outputVoltage                        -539
powerLoad
unitInformation                      N/A
================================================================================================================
Total: 1 MOs

MN0235> get 203

230122-14:19:50              22.0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/15533
================================================================================================================
203                                  Equipment=1,FieldReplaceableUnit=PSU-1,EnergyMeter=1
================================================================================================================
availabilityStatus                   i[0] =
consumedEnergyMeasurementRef
energyMeterEnabled                   1 (ENABLED)
energyMeterId                        1
inputCurrent                         5
inputVoltage                         2445
operationalState                     1 (ENABLED)
outputCurrent                        23
outputPower                          1220
outputVoltage                        -537
powerLoad                            67
unitInformation                      8 A
================================================================================================================
Total: 1 MOs
MN0235> get BFU-1

230122-14:14:47              22.0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/15533
================================================================================================
144                                  Equipment=1,FieldReplaceableUnit=BFU-1
================================================================================================
administrativeState                  1 (UNLOCKED)
availabilityStatus                   i[0] =
deepSleepStatus                      0 (NOT_SUPPORTED)
faultIndicator                       2 (OFF)
fieldReplaceableUnitId               BFU-1
floorInformation                     Struct{2}
  >>> 1.floorNumber = -101
  >>> 2.heightOfDot = -1
hwTestResult                         Struct{0}
isSharedWithExternalMe
maintenanceIndicator                 0 (NOT_APPLICABLE)
operationalIndicator                 3 (STEADY_ON)
operationalState                     1 (ENABLED)
positionCoordinates                  Struct{0}
positionInformation                  s[0] =
positionRef                          Cabinet=1
productData                          Struct{5}
  >>> 1.productionDate = 20140926
  >>> 2.productName = BFU 01 02
  >>> 3.productNumber = BMG 980 387/1
  >>> 4.productRevision = R1G
  >>> 5.serialNumber = C941892043
reservedBy                           [0] =
specialIndicator                     t[1] =
  >>> Struct[0]  has 2 members:
  >>> 1.indicatorName = Battery Fault Indicator
  >>> 2.indicatorStatus = 2 (OFF)
statusIndicator                      0 (NOT_APPLICABLE)
supportUnitRef                       [0] =
userLabel
================================================================================================
Total: 1 MOs
```

Figura 61. Mediciones energéticas elementos DC RBS - ENM CLI

El ingeniero NOC también puede verificar el estado de los elementos de forma general, es decir es posible que algún elemento aun no esté generando alarmas,

pero que esta no operacional y se tenga una afectación a futuro sobre con el comando ***cabx*** obtenemos información de varios elementos de la RBS, entre ellos los de energía.

En la figura 62, se muestra en el campo FRU, los elementos de la RBS, su tarjeta DU en este caso una Baseband 6630, los RRU con su número de producto, la BFU, PDU y PSU, Nótese que esta radio base posee 4 PDU y 3 PSU, en el campo FAULT, todos los elementos están en OFF, es decir no está fallidos, mientras en que el campo OPER, todos los elementos están ON, es decir, todos operacionales. Si alguno cambia su estado es un indicativo de falla en el Hardware y tendrá que ser reemplazado, para superar las alarmas o para cesar la intermitencia en el servicio en caso que hubiese.



```
MN0235> cabx

230121-14:53:51                    RBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/27582

INFO: cabx is not applicable on RCS nodes. Using invxrf instead. Type "h inv" for more details on available options.

Checking available boards on node...

Collecting RCS board data ...
.........................................................................
....................
..................................................................................................................................................
get /rop/A20230121.2000-2015_MN0235.xml.gz /ericsson/log/amos/moshell_logfiles/nigsuare/logs_moshell/pmfiles/10.224.44.203/rop/A20230121.2000-2015_MN0235.xml.gz ... OK
get /rop/A20230121.2015-2030_MN0235.xml.gz /ericsson/log/amos/moshell_logfiles/nigsuare/logs_moshell/pmfiles/10.224.44.203/rop/A20230121.2015-2030_MN0235.xml.gz ... OK
get /rop/A20230121.2030-2045_MN0235.xml.gz /ericsson/log/amos/moshell_logfiles/nigsuare/logs_moshell/pmfiles/10.224.44.203/rop/A20230121.2030-2045_MN0235.xml.gz ... OK
....
Collecting TN data...
.
Getting MO data from node (83 MOs). Please wait...
0%                                            ~50%                                              ~100%
.......................................................................................................................
Collecting RF data...
...............................................................
Node: RadioNode GW   CXP9024418/15_R53J14 (22.Q2)   GSM WCDMA

==========================================================================================================================
FRU        LNH      BOARD         ST FAULT OPER MAINT STAT PRODUCTNUMBER   REV    SERIAL       DATE      PMTEMP  TEMP  UPT
==========================================================================================================================
BB-1       000100   BB6630*       1   OFF   ON   OFF   OFF KDU137848/11    R2H    CF86966326   20191129 3 (OK)
RRU-S1B2   BXP_2    RRU4415B2B25* 1   OFF   ON   OFF   N/A KRC161636/1     R5H    CF86229743   20190618 4 (OK)  46.5 46.5  (Radio4415B2B25)
RRU-S2B2   BXP_3    RRU4415B2B25* 1   OFF   ON   OFF   N/A KRC161636/1     R5H    CF86229740   20190618 4 (OK)  52.0 46.5  (Radio4415B2B25)
RRU-S1B5-G BXP_4    RRU2219B5     1   OFF   ON   OFF   N/A KRC161678/1     R1A    CA74281091   20190627 4 (OK)  38.5 46.5  (Radio2219B5)
RRU-S2B5-G BXP_5    RRU2219B5     1   OFF   ON   OFF   N/A KRC161678/1     R1B    CA73867258   20180620 4 (OK)  38.8 46.5  (Radio2219B5)
RRU-S3B5-G BXP_6    RRU2219B5     1   OFF   ON   OFF   N/A KRC161678/1     R1A    CA74281082   20190627 4 (OK)  36.0 46.5  (Radio2219B5)
RRU-S3B2   BXP_7    RRU4415B2B25* 1   OFF   ON   OFF   N/A KRC161636/1     R5J    CA74685935   20210316 4 (OK)  50.0 46.5  (Radio4415B2B25)
BFU-1      Z??_001  BFU0102       1   OFF   ON   N/A   N/A BMG980387/1     R1G    C941892043   20140926
PDU-1      Z??_002  PDU0101       1   OFF   ON   N/A   N/A BMG980336/2     R5C    X052628017   20140828
PDU-2      Z??_003  PDU0101       1   OFF   ON   N/A   N/A BMG980336/2     R5C    X052569830   20140725
PDU-3      Z??_004  PDU0302       1   OFF   ON   N/A   N/A BGM136106/2     R1C    DX10249665   20190321
PDU-4      Z??_005  PDU0302       1   OFF   ON   N/A   N/A BGM136106/2     R1C    DX10249666   20190321
PSU-1      Z??_006  PSUAC03       1   OFF   ON   N/A   N/A BML161184/1     R1N    BR86472910   20190809
PSU-2      Z??_007  PSUAC03       1   OFF   ON   N/A   N/A BML161184/1     R1L    BW99687834   20140827
PSU-3      Z??_008  PSUAC03       L   OFF   ON   N/A   N/A BML161184/1     R1L    BW99688014   20140827
SAU        Z??_009                L    ?     ?    ?     ?
SCU        Z??_010  SCU0101       1   OFF   ON   N/A   N/A BGM1361006/1    R5B    CR99829907   20140701
--------------------------------------------------------------------------------------------------------------------------
```

Figura 62. Validación de Operatividad de los elementos de energía DC. ENM CLI

Para el caso de la FALLA DE RECTIFICADOR, esta no se puede hacer una medición o saber cuál es el elemento afectado pues como se ha explicado a la DU le llega un único pulso de alarmas, por tanto, en caso de estar presente ésta alarma, el Ingiero de campo de realizar una validación en y verificar si los módulos rectificadores están en buen estado o su falla algún elemento de los que intervienen el procesamiento de las alarmas.

Toda la informa recopilada de la alarma y el comportamiento de la radio base ante esta alarma debe ser transmitida del Ingeniero NOC al Ingeniero RBS para una dar una solución rápida a la problemática planteada.

7.2.2.3. Trabajo de campo

El ingeiero de campo RBS tiene la mision de restablecer el servicio o cesar las alarmas lo mas rapido posible; en la mayor parte de las situaciones de fallas la accion mas conveniente en campo en el reemplazo del Hardware dañado, es por ello que debe de mantener un stock de repuestos de difentes modelos de radio bases según el operador tenga instaladas en su zona de operación, disponer de un transporte eficaz y toda la logistica necesaria para su movilizacion y llegada a sitio, estando en el lugar del reporte de falla hara las siguientes pruebas:

Para los elementos de rectificación de corriente como las PSU o modulos rectificadores, se deben garantizar las siguientes acciones:

- Deben hacer una revision visual del estado del elmento, si no se observa o presenta olor a quemado.
- Luego hacer mediciones de voltaje a cada elemento, los cuales deben generar aproximadamente 54VDC.
- Si se detenta un problema en el elemtno rectificador, proceder con el cambio inmediato.
- Si aun persisten las alarmas se debera revisar los elementos que intervienen en el procesamiento de las alarmas como conexiones de entrada y salida del Controlador de gabinete o SHU, deben descartar flojedad en los puertos, conectores dañados, cables con moderduras de roedores, etc. Si la falla se detecta a nivel de estos componentes proceder en la medida de lo posible a reemplazar el cableado, conectores o puerto en elemento multiplexor.

Cuando los elementos alarmados con las Baterias, asegurar las siguientes acciones:

- Realizar una Medicion de voltaje en las beterias cuando estas son de plomo deben medir 12v sin carga conectada, si hay un valor inferiror es un indicativo de daño en las baterias.
- Si las baterias son de litio, tienen una tarjeta de control eletronica integrada, validar si el Led de bateria presenta algun tipo de alarma visual, en caso de hacerlo, aplicar un reinicio y efectuar una medicion de voltaje, si muestra valores esta buen estado y la alarma tuvo que cesar, si no hay valor de voltaje, se volvera a alarmar y se debe reemplazar la baterias.
- Puede haber falla en Fusible o sulfatacion de borneras de BFU y baterias por humedad, se debe hacer limpieza de conectores y pruebas de respaldo.

- Verificar que no se tengan Breaker disparado en baterias de litio, normalmente sucede cuando se tiene sobre voltaje en la controladora.
- Revision de la temperatura de gabinete, algunas baterias de litio se alarman cuando alcanzan un umbral de temperatura y se protejen, de estar afectada por temperatura se debe corregir el defecto en el sistema de clima y luego hacerle pruebas a la baterias para verificar si no tuvo daños al exponerse a altas temperaturas.
- Alguas baterias de litio se bloquean por demanda carga, cuando el sistema requiere mas de la capacidad del banco actual, para solvenar este problema se debe ampliar respaldo, reiniciar las baterias alarmadas y repetir las pruebas.
- Si las baterias estan en buen estado, se debe hacer pruebas con la BFU, que ésta mande a cargar las baterias y luego pruebas de descarga y validar que se haga la conmutacion o tranferencia de carga de la fuente principal al respaldo de baterias.

Una vez se supera el problema encontrado se debe validar con el NOC que cesen las alarmas.

7.2.3. Fallas de sectores

7.2.3.1. Conexiones físicas de RRU

Los operadores telefónicos van modernizando su infraestructura de red tanto a nivel de transporte, Core y Acceso, las radio bases van evolucionando, los primeros modelos de RBS tenían los radios (RRU) en el gabinete y existía una conexión RF por líneas feeder de cobre de gran distancia entre el radio y la antena, en virtud de reducir la cantidad de fallas y optimizar espacio en gabinetes los proveedores cambiaron esa infraestructura por un modelo dónde los RRU son aéreos, es decir, están instalados en la torre y la conexión entre la antena y el RRU son distancias cortas, reduciendo de este modo la atenuación inducida por líneas feeder de cobre de grandes distancias, y la cantidad de fallas, debido que cuando la conexión entre el RRU y la antena se realizaba desde el gabinete hasta la torre se presentaban fallas por infiltraciones de agua en feeder que bloqueaban los RRU, eran más propensos a vandalismos, ya que esa cantidad de cobre era atractiva para los infractores, adicional existía una mayor dificultad para atender fallas debido a que si se necesita cambiar una línea de feeder, requería de más de un torrero (personal que atiende en altura), se requería un equipo de torreros que sostuvieran el cable a instalar en los distintos tramos de la torre, en el nuevo esquema con RRU en la torre hay una mayor facilidad de atención respecto al número de torreros, con una sola persona por lo general es suficiente para atender eventos de fallas en las conexiones del RRU, se necesita más de un torrero solo en aquellos casos que se tenga que cambiar el RRU y éste sea de gran tamaño.

En el nuevo esquema con RRU Aéreo la conexión entre el RRU y las tarjetas DU, se efectúa mediante fibra óptica, la cual es más fácil de manipular e instalar en la torre, sin embargo, al efectuar este cambio existen muchos puntos potenciales de falla ya que intervienen más elementos, por ejemplo, las fibras se acoplan hacia el RRU y la DU mediante transiver de altas velocidades (SFP) lo cuales deben ser iguales ambos extremo y son propensos a daños por temperatura o humedad, además el RRU necesita una fuente de alimentación DC para Operar por lo que debe existir un cableado eléctrico desde la parte de distribución DC del gabinete hasta el RRU, lo cual también supone un posible evento de vandalismo en busca de cobre.

En la Figura 63, se muestra la conexión entre el RRU y las tarjetas DU, el RRU está instalado en la torre y la DU en el gabinete de la RBS, una DU puede ser una baseband, DUS, DUW, DUG, existe una conexión de fibra óptica entre el RRU2212 y la BB6630 del ejemplo. Adicional existe una conexión eléctrica en el puerto DC del RRU hacia el sistema de distribución DC del gabinete que puede

ser breakers o PDU dependiendo del tipo de radio base. Por cada RRU instalada se tendrán 2 líneas bajantes al gabinete fibra y energía, ambos son puntos potenciales de fallas y se debe identificar que conexión está fallando.

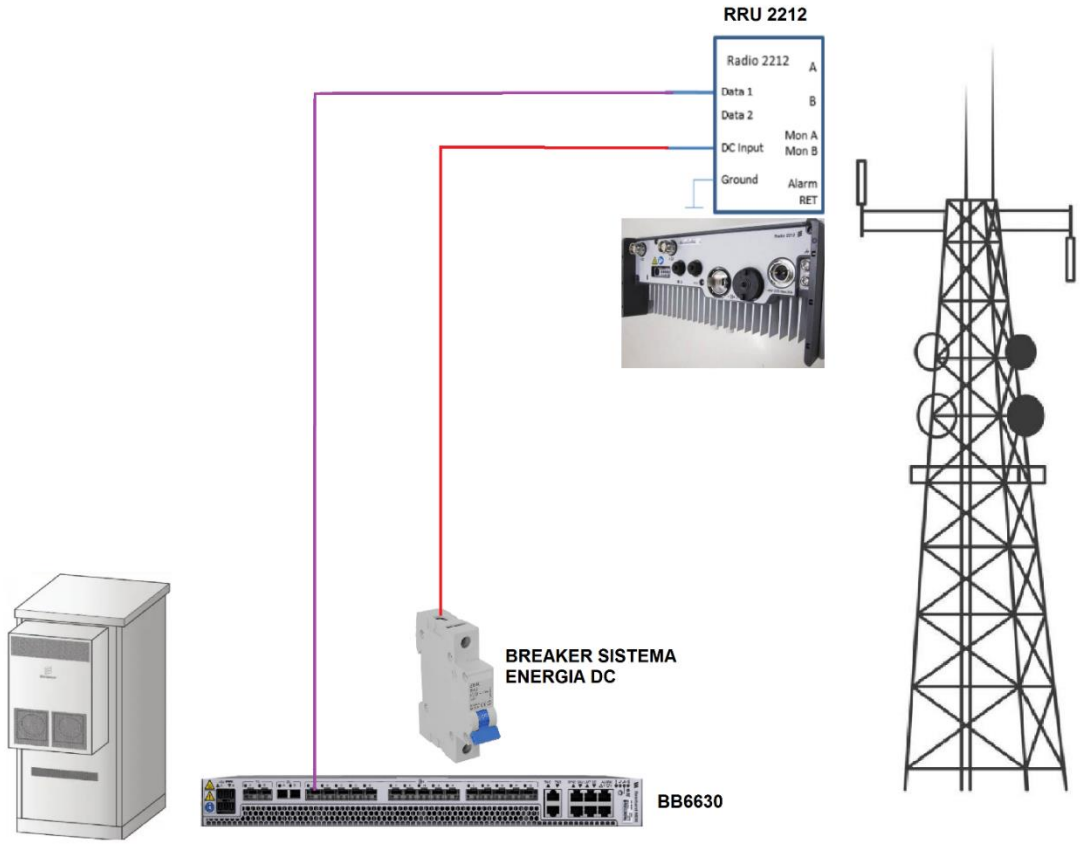


Figura 63. Conexión RRU Aéreo hacia Gabinete RBS

Este RRU posee dos puertos de datos, es decir, puede ser utilizado en configuración Mixed Mode, un puerto de datos hacia la baseband LTE y otro hacia la Baseband 3G, los puetos A y B del RRU son utilizados para la conexión RF hacia la antena, del lado de baseband o cualquier tarjeta DU se utilizan los puertos ópticos para las conexiones de RRU, que utilizan como nomenclatura letras del abecedario, para éste ejemplo la BB6630 posee tres bloques de puertos ópticos, cada uno con cinco puertos, es decir se podrían conectar hasta 15 RRU.

Existe una conexión alternativa para la alimentación de los RRU, ya que el bajante de cobre es propenso a robos, se pueden instalar líneas de aluminio, pero requieren 2 cambios en la conexión, primero el breker de la RBS debe soportar la carga, de ser posible se debe instalar un breaker de mayor capacidad y en la parte de la torre se debe instalar un panel eléctrico con breaker de protección con el objetivo de distribuir la carga DC que va desde el gabinete hacia los RRU, lo que

significa que anexamos un punto de falla adicional al sistema ya que esos brekers de protección son propensos a dispararse y se necesitaría un torrero para restablecer el servicio de los sectores alarmados.

7.2.3.2. Monitoreo y Troubleshooting remoto

Cuando se tengan eventos en la red por alarmas en sectores es importarte que el Ingiero NOC identifique el tipo de afectación, verifique alarmas, realice un troubleshooting sobre el elemento alarmado y movilice a personal en caso de ser necesario.

Al igual que en los demás escenarios de alarmas, la fuente de alerta sobre una falla en la red puede ser un Incidente aperturado en la herramienta de gestión de incidentes o detectado mediante el monitoreo de alarmas, sin embargo, existe otras dos posibilidades que no habían sido abordados previamente y son un reporte por parte del área responsable de calidad de red o una queda de los clientes por una experiencia mala como usuario de la red. Para cualquiera que fuese la fuente de alerta de la falla existen varios escenarios posibles, por ejemplo:

- Sectores fuera de servicio (celdas Disable), afectando la disponibilidad de la red con alarmas que atribuya dicha afectación a eventos en los RRU.
- Sectores o celdas en servicio, pero sin tomar tráfico. Lo que significa que no hay usuarios atachandose por falla en el Hardware.
- Sectores o celdas en servicio, con tráfico, pero con alarmas atribuya dicha afectación a eventos en los RRU, lo que degrada el servicio y eventualmente iniciará a afectar la disponibilidad.

Durante la validación de fallas, se pueden encontrar alarmas en sectores como el siguiente listado:

- Hw Partial fault (FieldReplaceableUnit=RRU-X): Cuando se tiene esta alarma en el gestor la causa probable sea una falla en hardware del RRU y deba ser reemplazado.
- Link failure: Es una probable falla en la fibra o conectores SFP bien sea del lado del RRU o de la DU.
- Power Disturbance: Esta alarma cuando apunta aun RRU, significa que hay una falla a nivel del sistema de alimentación DC del RRU. Puedo ser causado por algún breaker disparado o falsos contactos en el puerto DC del RRU, en Nicaragua esta alarma es un indicio probable de vandalismo ya que muy seguramente el cable de alimentación DC del RRU fue cortado por robo en sitio.

- SW Error (FieldReplaceableUnit=RRU-X): Es un indicativo que el RRU pueda estar en mal estado y requiera cambio del mismo o simplemente esté inhibido y requiera un roset físico.
- Link Degraded (RiLink=X): Es una falla en fibra o SFP.
- Fiber loss UL/DL: Es una degradación en los niveles ópticos la fibra del RRU, el rango de operación está entre -2 y 2 dbm por ello cuando supera el umbral envía alarma de fiber loss, se debe hacer un reemplazo de la línea de fibra para superar las atenuaciones.
- Linearization Disturbance Performance Degraded (FieldReplaceableUnit=RRU-X): Normalmente se genera en combinación con alguna de las anteriores alarmas, puede ser un daño en alguna de las SFP, fibra o RRU.
- Emergency Unlock Reset Key Required: Cuando esta alarma está presente no hay un problema físico que atender, simplemente los sectores afectados no están incluidos en la configuración de la licencia que corre sobre el Software actual en el Nodo, se necesita que el proveedor le recargue una nueva licencia que incluya a los sectores afectados. En este caso Ericsson da opción de habilitar una licencia provisional (LKF Emergency) mientras se genera una la licencia definitiva, al realizar esta activación, se tendrá un periodo de 7 días habilitados sin afectación de las celdas, al pasar éste tiempo se podrá habilitar un segundo periodo de otros 7 días para cargar la licencia definitiva.
- DigitalCable_CableFailure: Es una alarma general que puede ser provocada por daño en la fibra, SFP o energía en el RRU.
- SFP Config: Cuando esta alarma se genera normalmente es por un conflicto de Hardware, es decir se tiene un SFP instalado en la DU y un tipo diferente de SFP instalado en el RRU, ambos deben tener la misma capacidad, ambos de 1 GB o ambos de 10 GB. Cuando se tiene identificado que el RRU está en configuración Mixed Mode, las SFP deben ser de 10GB porque demanda más tráfico, si tienen un valor inferior dará problemas para tomar tráfico.

En la Figura 64, se realiza una verificación de falla para un eNodeB que tiene una celda fuera de servicio mediante el comando ***st cell***, el estado **Disable** del sector B indica que están fuera de servicio, el estado **Enable** en los demás sectores indica que ellos están en servicio. Luego se validan alarmas presentes con el comando ***alt***, la información que brida en este caso fue alarmas de: *Link Failure RiLink=2 (No signal detected (link start time-out)* indicando que el link 2 de fibra tiene una falla, luego se observa una segunda alarma: *Resource Activation Timeout EUtranCellFDD=LCH0049B (Unable to allocate radio resources.)* indicando que el sector B del LTE no tiene perdida de conexión a la BB. También

es conveniente evaluar si el sector está tomando tráfico, cuando el valor es diferente a cero, significa que toma tráfico, cada unidad significa un usuario atachado a la celda que se identifica con la columna cellid, para el ejemplo era lógico que no estuviese generando trafico porque la celda B esta Disable, sin embargo se puede dar el escenario que la celda este Enable y que igualmente siga sin tomar tráfico, es decir, aunque la celda esté operativa a nivel del hardware, no hay usuario que estan conectados, buscan otra más cercana en la red porque la celda sin tráfico no está disponible. Puede suceder para el ejemplo que cuando la celda restablezca, queda sin tomar tráfico y aunque este en servicio y no genere indisponibilidad en la red, la experiencia del usuario no va a cambiar, sencillamente porque no tiene una celda que le dé cobertura y su dispositivo se atachará a otra celda en la red con menos calidad del servicio por la lejanía y la posible saturación de usuarios, por ello el Ingeniero NOC debe realizar las mismas validaciones cuando se diagnostica la falla y cuando se ha realizado un cambio en campo.

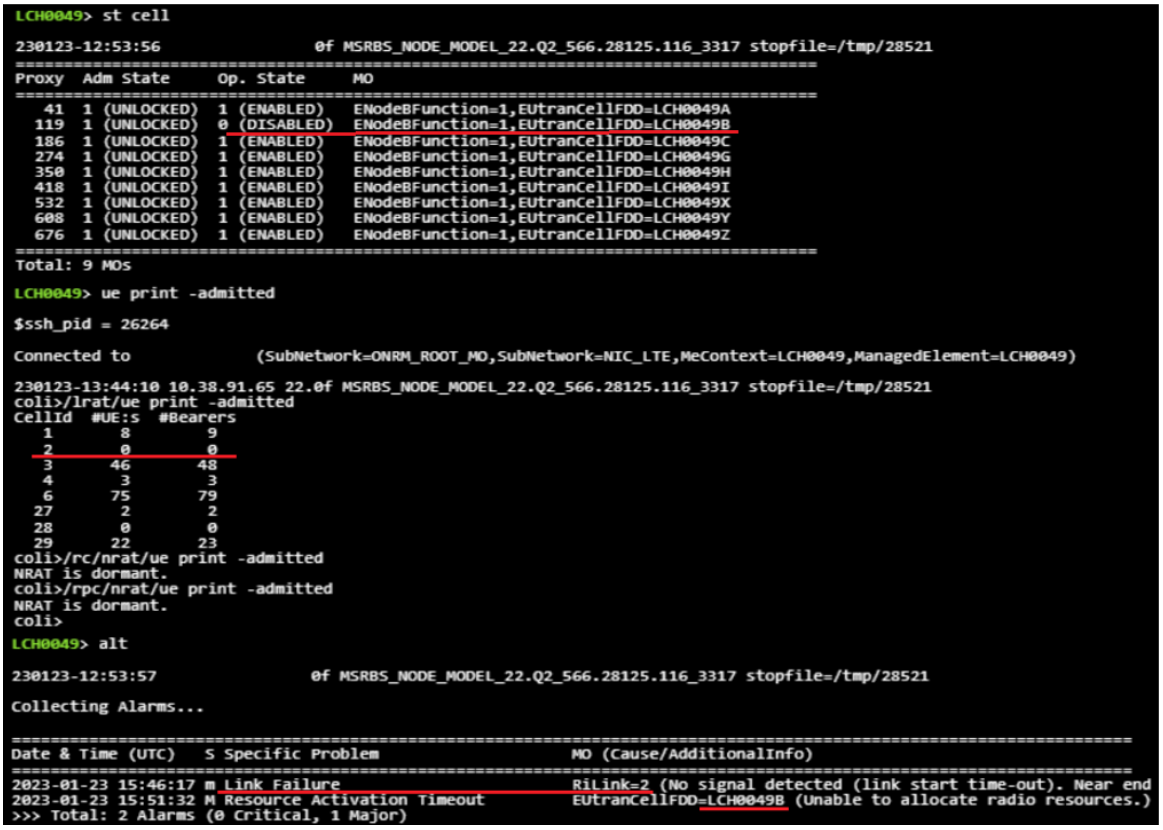


Figura 64. Validación de alarmas de sectores. ENM CLI

Dentro de las validaciones remotas que se puede hacer en las radio bases, se tiene la ejecución del comando ***sdic***, el cual muestra gran cantidad de información

del inventario del hardware y el estado de dichos elementos. En la Figura 65 se muestra la primer parte del comando sdic, genera un diagrama de bloques de conexiones entre la baseband y los RRU instalados, en la parte superior hay una leyenda de la lectura del estado de los CPRI links, muestra que tiene 5 CPRI Links OK y 1 CPRI Link NOK, es decir con falla, luego en el diagrama de bloques marca en rojo el link afectado, se muestra información de la distancias físicas de los link (52 metros), para que esta información sea ocupada por el Ingeniero de campo para llevar la cantidad adecuada de repuesto de cable de fibra óptica para RRU; del lado de radio indica el modelo de RRU, el numero asignado, y da información de las celdas lógicas que tiene configurada, por ejemplo el RRU-2 que está afectado, únicamente tiene configurado el sector B, si lo comparamos con el RRU-4 se aprecia que tiene configurados los sectores G, X.

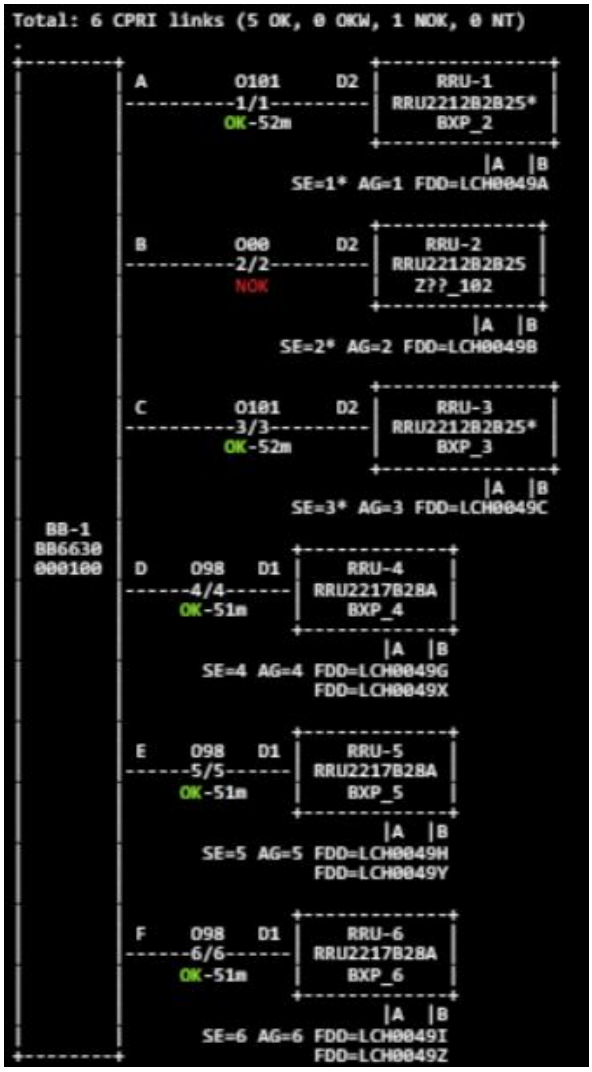


Figura 65. Diagrama de bloques BB - RRU. ENM CLI

La figura 66, muestra la siguiente parte de la ejecución del comando, hay información de la alarma presente que es Link Failure, y sugiere una serie de procedimientos a realizar para superarla, además se puede observar que en la información del RRU no muestra datos en los campos FAULT y OPER, significa que la información del estado de RRU no está disponible, debido que se tiene un problema de comunicación entre la BB y el radio por una posible falla en la fibra, no significa necesariamente que el radio esté en mal estado, puede ser la fibra o la SFP.

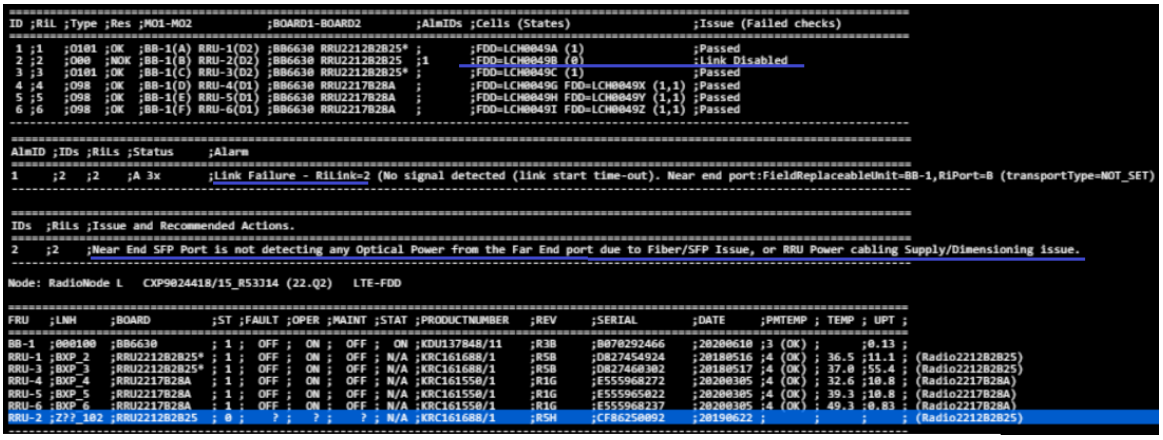


Figura 66. Información de la Alarmas SDIC. ENM - CLI

En algunos casos se puede realizar un troubleshooting para superar las falla de sectores, el Ingeniero NOC puede reinicar el RRU o la Baseband y cuando con son tarjetas DU puede reiniciar unicamente la DU, no asi el RRU y se le puede recagar el CV. En caso que estas pruebas no tengan efecto se debe enviar a personal de campo para revision del hardware. Existe la posibilidad que se recupre la disponibilidad y el trafico, pero quede con alarmas de degradación, en este caso tambien es necesario enviar a personal de campo a realizar el reemplazo del hardeware pero la urgencia de la atencion de la falla baja considerablemente.

Para reinicar un RRU se deben seguir los siguentes pasos:

- Identificar el numero del RRU alarmado, si se muestra la letra de la celda, hay que buscar cual es el RRUque esta asociado. Con los comandos ***cabx, invxhf, invgx, sdic***, es posible ver la asociacion de la celda con el RRU.
- Buscar el Proxy asociado al RRU de interes. Con el comando ***st RRU*** observamos el proxy.
- Ejecutamos el comando ***acc (proxy) restartunit*** en el caso de las baseband, ejemplo: ***acc 1253 restartunit***, y aceptamos todas las consultas que genera el comando. Tambien es posible reiniciar desde el numero del RRU, por ejemplo: ***acc RRU-2 restartunit***, y el resultado será el mismo.

- Se espera un tiempo produncial luego de reinicio del RRU y se verifica si cambio el estado del sector y si hubo cese de alarmas.

Para reiniciar una Baseband se debe unicamente identificar el numero del proxy, que se puede hacer con el comando ***st field***, y se ejecuta el renicio acc con el proxy con el numero de la baseband. Ejemplo: ***acc BB-1 restartunit***. En el caso que la tarjeta de control sea una DU, se debe ejecuar el comando ***acc 0 manualrestart***.

Tambien es posible verificar un log de manipulaciones del Nodo mediante el comando ***lgn***, mostrará si algun otro usuario ya aplicó un procedimiento de troubleshooting y de este modo evitamos repetir un procedimiento infructuoso. El siguiente paso es enviar toda la información recopilada al área de campo para que se movilice a sitio y resulva la falla.

7.2.3.3. Trabajo de campo

El ingeniero de campo de llevar el equipamente necesario para atender los eventos de sectores, es decir, stock de repuestos de SFP, RUU, Fibra y cable bajante de alimentacion DC, adicional es escencia que se movilice como equipo con un personal de altura ya el 100% de la infraestructura actual es bajo el esquema de BB/DU en gabinete y RRU en torre.

Una vez en sitio debe garantizar las siguientes revisiones:

- Reemplazo de transceiver (SFP), recordemos que cada sector o RRU de la torre tiene asignado un puerto en la tarjeta en el gabinete y utiliza un SFP para conversion optica a electrica en puertos de las tarjetas o RRU. En el gabinete suelen dañarse por altas temperaturas, si se da el caso no solo se debe reemplazar el SFP, sino que hay que garantizar las condiciones de clima de la radio base, tambien puede sufrir dañados por humedad debido a mal clima o por el tipo de zona donde se encuentra la RBS, la humedad genera condensacion y luego se introduce agua por medio de la fibra hasta dañar el SFP o incluso el puerto de la BB, si hay daño en muchos puertos de la BB se debe cambiar la tarjeta completamente.
- Reemplazo de cable de fibra óptico con personal de altura (torrero). Una vez descartado falla de los transiver debe proceder a cambiar la línea de fibra y con ello descartar que la perdida de conexión entre la tarjeta y el RRU sea por falla en la fibra.
- Es necesario verificar las conexiones eléctricas de alimentación DC del RRU, medir si le está llegando el voltaje adecuado, si no lo está, pueden

ser varias razones, breaker disparado en gabinete por RRU en mal estado o cortocircuitado, vandalismo cuando cortan el cableado. El ingeniero de campo procede a reemplazar RRU dañado, verificación del funcionamiento del breaker, si es necesario de debe reemplazar por uno de mayor capacidad; cuando suceden vandalismos se realiza conexión provisional y se activan los breaker normalmente, luego se cambian las líneas de cobre por aluminio para evitar reincidencias de robos y se le instala un sistema de breaker de protección y distribución de carga en la torre, con ello surge una nueva potencial falla que consiste en que disparen los breakers de los RRU en la torre, lo cual también debe ser verificado con el torrero.

- Cuando el RRU esta en mal estado, por lo general se observa un led rojo que se enciende por la parte inferior del RRU, con ellos se se esta seguro del daño y se procede a reemplazar con personal de altura.

Luego de efectuar todos cambios posibles a nivel de hardware en el sitio el Ingeniero de campo debe llamar al Ingeniro NOC y pedir validacion del servicio y consultar si los parametros observables se encuentran dentro del rango como la medicion del fiber loss, cero alarmas, celda y trafico OK, incluso si la SFP no generan conflictos y las que se instalaron son las adecuadas, esto lo debe hacer para corroborar que el torrero efectuase el cambio correcto y deje cruzados conectores, sobre todo cuando los radio tienen varias tecnologias integradas (Mixed Mode).

7.2.4. Fallas de diversidad

7.2.4.1. Conexión física de RRU

Siguiendo el esquema actual de RRU aéreo, adicional a la conexión hacia el gabinete de radio base, debe existir una conexión del RRU hacia la antena, esta conexión se realiza mediante un feeder que es un cable de cobre con conectores estándar para las antenas y RRU a como se muestra en la figura 67.

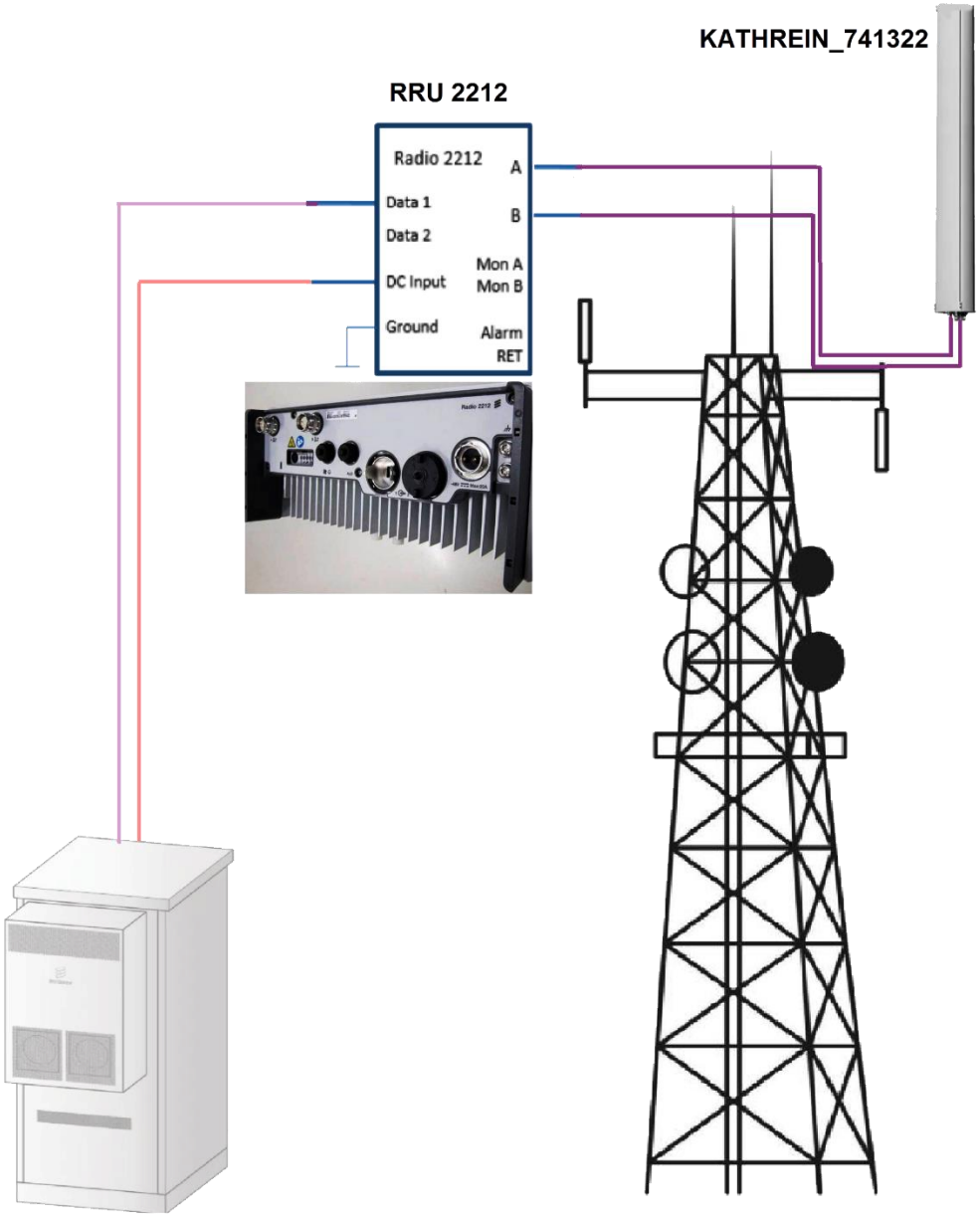


Figura 67. Conexión RRU hacia antena

En la figura 67, podemos observar las conexiones posibles del RRU, en la entrada van dos líneas bajantes hacia el gabinete de la radio base, una para datos y otra para energía, luego en la salida del RRU son 2 líneas RF puerto A y B ambos se conectan hacia la antena. No existen muchos elementos de internexión en esta etapa es por ello que el punto de falla es únicamente el feeder.

Las Antenas básicas poseen 2 puertos de entrada RF, igualmente los RRU, también existen Atenas más complejas que tienen 4, 6, u 8 puertos para conexión de mas RRU, es decir que soportan configuraciones Mixed Mode o configuración de varias portadoras para un mismo sector, en estos casos usan un bus de feedder ya que son más líneas entre el radio y la antena, la configuración de las portadoras se realiza a nivel lógico en la radio base y viene hecha por el proveedor, según los requerimientos del cliente.

Este tipo de fallas referentes a diversidad no afectan la disponibilidad de la red ya el RRU seguirá pasando tráfico, no se afectarán los sectores, sin embargo, se tendrá degradación en el servicio, los indicadores de calidad de red (KPI) estarán afectados al igual que la experiencia del cliente.

7.2.4.2. Monitoreo Remoto

El monitoreo respecto a alarmas de diversidad consiste en verificación generales de alarmas presentes en el Nodo y revisión de valores de VSWR, RSSI e imbalances entre los puertos de un mismo RRU.

Las alarmas más frecuentes que se encuentran son las siguientes:

- Rx Diversity lost
- Carrier_RxDiversityLost
- VSWR limit Exceed
- RX Branch Imbalance Fault
- Feeder Cable Incorrectly Connected
- Carrier_TxBranchFailure
- AntennaBranch_AntennaSystemProblemInBranchB

El **VSWR** es uno de los parámetros que se evalúa en las fallas de diversidad, significa relación de onda estacionaria de voltaje. Este error indica si hay un cortocircuito o un circuito abierto en la antena utilizada, Este problema generalmente ocurre cuando hay un cable o conector de antena defectuoso.

VSWR es una forma de medir las imperfecciones de la línea de transmisión que generalmente es causada por la falta de coincidencia de impedancia, en este caso

entre el puerto del RRU y la antena conectada a él. VSWR también indica cuanta energía se refleja desde el puerto de antena cuando la BTS está transmitiendo. Si el valor de VSWR es igual a 1, entonces no hay reflexión y toda la potencia se transmite a través de la antena. Cuando el valor de VSWR es igual a infinito, toda la potencia se refleja, en este caso no se transmite potencia. Entonces, el valor de VSWR oscila entre 1 e infinito, siendo 1 el valor ideal. Es un valor asimétrico no tiene unidad de medición y se calcula utilizando la siguiente formula.

$$VSWR = \frac{1 + 10^{\frac{-RL}{20}}}{1 - 10^{\frac{-RL}{20}}}$$

Donde,

RL = Pérdida de retorno en dB

VSWR = Relación de onda estacionaria de tensión

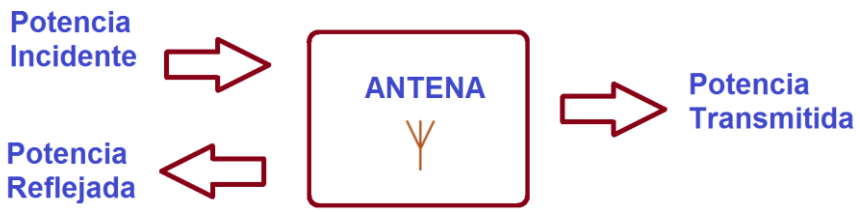


Figura 68. Pérdida de retorno RL (VSWR)

La figura 68 describe el concepto de VSWR. La pérdida de retorno de un sistema se define como la relación entre la potencia incidente y la potencia reflejada y se mide en dB. La pérdida de retorno alta da como resultado una potencia reflejada baja, por lo que es deseable una pérdida de retorno alta para un sistema.

El ingeniero NOC debe evaluar el nivel de VSWR cuando reporta Incidentes por fallas de éste tipo. Se hace validación mediante el comando ***lh ru fui get vswr***.

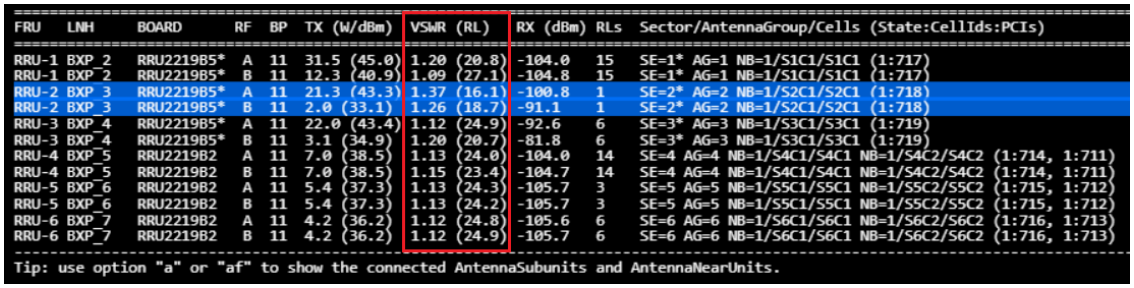
En la Figura 69, se muestra un ejemplo de la ejecución de uno de los comandos para revisión del VSWR, en éste caso en valor que se muestra no es si asimétrico por ello no es el VSWR, sin el valor RL que representa la pérdida del retorno, el cual se mide en db y entre mayor el valor mejor nivel de VSWR se tendrá, es por

ello que medir el valor RL es una opción válida para diagnosticar una falla, el valor que recomendado desde la experiencia del equipo de ingeniería RF y Operaciones O&M de un operador de telefonía en Nicaragua es 17.0 db en RL, traducido a VSWR sería un valor asimétrico de 1.32, por tanto el valor de 16.3 db que muestra el BXP_3 es una falla que debe atenderse en campo, adicional si se valora ese nivel RL en comparación el resto de los BXP, hay una amplia diferencia de caso 10 db.

Figura 69. Medición del nivel de Perdida de retorno (RL) VSWR

Existe la posibilidad que algunos BXP (grupo de puertos del RRU) no muestren valores RL, si esto se dá significa que en scrip del Nodo no viene declarada la fórmula de cálculo del VSWR. Adicional la medición presentada en la Figura 88 no es completa ya que muestra únicamente el valor del puerto A del RRU, un radio tiene un mínimo de 2 puertos RF, por tanto, falta información. El comando que brinda la medición RL para cada puerto de cada RRU de la radio base es ***cabx***.

En la Figurar 70 se muestra la medición del RL y su conversión a VSWR mediante la ejecución del comando ***cabx***, tomando el mismo ejemplo de la Figura 89, el BXP_3 mostró un valor de 16 db, se corresponde con el BXP_3 (RRU-2) Puerto A, mientras que en el mismo RRU pero en su puerto B hay una medición RL de 18 db, es decir que solamente una de las líneas en esas conexión entre el RRU-2 y la antena tiene perdidas que rompen el umbral. Este evento debe ser atendido con el personal de campo.



FRU	LNH	BOARD	RF	BP	TX (W/dBm)	VSWR (RL)	RX (dBm)	RLs	Sector/AntennaGroup/Cells (State:CellIds:PCIs)
RRU-1	BXP_2	RRU2219B5*	A	11	31.5 (45.0)	1.20 (20.8)	-104.0	15	SE=1* AG=1 NB=1/S1C1/S1C1 (1:717)
RRU-1	BXP_2	RRU2219B5*	B	11	12.3 (40.9)	1.09 (27.1)	-104.8	15	SE=1* AG=1 NB=1/S1C1/S1C1 (1:717)
RRU-2	BXP_3	RRU2219B5*	A	11	21.3 (43.3)	1.37 (16.1)	-100.8	1	SE=2* AG=2 NB=1/S2C1/S2C1 (1:718)
RRU-2	BXP_3	RRU2219B5*	B	11	2.0 (33.1)	1.26 (18.7)	-91.1	1	SE=2* AG=2 NB=1/S2C1/S2C1 (1:718)
RRU-3	BXP_4	RRU2219B5*	A	11	22.0 (43.4)	1.12 (24.9)	-92.6	6	SE=3* AG=3 NB=1/S3C1/S3C1 (1:719)
RRU-3	BXP_4	RRU2219B5*	B	11	3.1 (34.9)	1.20 (20.7)	-81.8	6	SE=3* AG=3 NB=1/S3C1/S3C1 (1:719)
RRU-4	BXP_5	RRU2219B2	A	11	7.0 (38.5)	1.13 (24.0)	-104.0	14	SE=4 AG=4 NB=1/S4C1/S4C1 NB=1/S4C2/S4C2 (1:714, 1:711)
RRU-4	BXP_5	RRU2219B2	B	11	7.0 (38.5)	1.15 (23.4)	-104.7	14	SE=4 AG=4 NB=1/S4C1/S4C1 NB=1/S4C2/S4C2 (1:714, 1:711)
RRU-5	BXP_6	RRU2219B2	A	11	5.4 (37.3)	1.13 (24.3)	-105.7	3	SE=5 AG=5 NB=1/S5C1/S5C1 NB=1/S5C2/S5C2 (1:715, 1:712)
RRU-5	BXP_6	RRU2219B2	B	11	5.4 (37.3)	1.13 (24.2)	-105.7	3	SE=5 AG=5 NB=1/S5C1/S5C1 NB=1/S5C2/S5C2 (1:715, 1:712)
RRU-6	BXP_7	RRU2219B2	A	11	4.2 (36.2)	1.12 (24.8)	-105.6	6	SE=6 AG=6 NB=1/S6C1/S6C1 NB=1/S6C2/S6C2 (1:716, 1:713)
RRU-6	BXP_7	RRU2219B2	B	11	4.2 (36.2)	1.12 (24.9)	-105.7	6	SE=6 AG=6 NB=1/S6C1/S6C1 NB=1/S6C2/S6C2 (1:716, 1:713)

Tip: use option "a" or "af" to show the connected AntennaSubunits and AntennaNearUnits.

Figura 70. Medición VSWR (RL) comando cabx

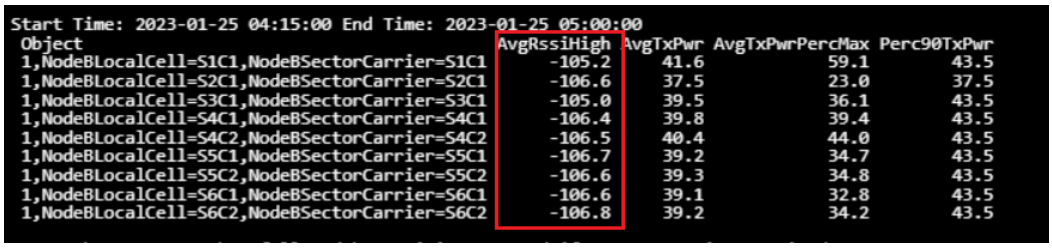
Las fallas de VSWR siempre son un problema a nivel físico, no de configuración o interferencia, por tanto, siempre que se tenga un valor de VSWR fuera del umbral de operación deberá ser reportado para corrección en campo.

El siguiente parámetro a medir son los niveles **RSSI** en cada puerto del RRU. EL nivel de RSSI es el indicador de fuerza de la señal recibida, es una escala de referencia para medir el nivel de potencia de las señales recibidas por un dispositivo en las redes inalámbricas, se mide en dBm. En un dispositivo móvil receptor indica el nivel de señal de recepción, se mide en rangos negativos porque los niveles de potencia recibido son rango bajos respecto a la referencia y el cálculo logarítmico del valor arroja un número negativo, los niveles por convención para la red celular LTE se maneja un valor excelente de RSSI mayores o iguales a -80 dBm, un valor bueno de recepción entre -80 dBm y -90 dBm, valor medio entre -90 dBm y -100 dBm y un mal valor con recepción nula a partir de los valores menores o igual a -100 dBm, por tanto desde el UE un nivel de RSSI que tiende a un valor positivo es un buen nivel de recepción de señal; sin embargo esa lógica no se aplica en el mismo sentido cuando medimos los niveles de RSSI en una antena. Cuando analizamos los valores de RSSI en la red del operador, lo realizamos en el espectro de frecuencia UL, es decir de subida de tráfico, ya que nos interesa ver el nivel de interferencia que tenemos cuando transmitimos, es deseable que las interferencias sean pocas o nulas para así poder enviar sin problemas el tráfico de voz o datos, es decir, al medir el espectro UL lo deseable es que los niveles de RSSI tiendan hacia valores muy negativos, en niveles casi nulos, ya que un mejor valor de recepción RSSI en este canal significaría estamos recibiendo potencia desde una fuente externa, lo que va interferir con nuestra transmisión.

Bajo el esquema de medición planteado definimos un umbral en -95 dBm, a partir de ese punto de referencia los valores con tendencia a cero (hacia lo positivo) generaran una falla de diversidad, por ejemplo -80 dBm es un nivel que desde el punto de vista del Operador debe corregirse porque hay una fuente externa de

interferencia, mientras que si tenemos un nivel de -110 dBm es un valor excelente de señal, y que las interferencias son casi nulas.

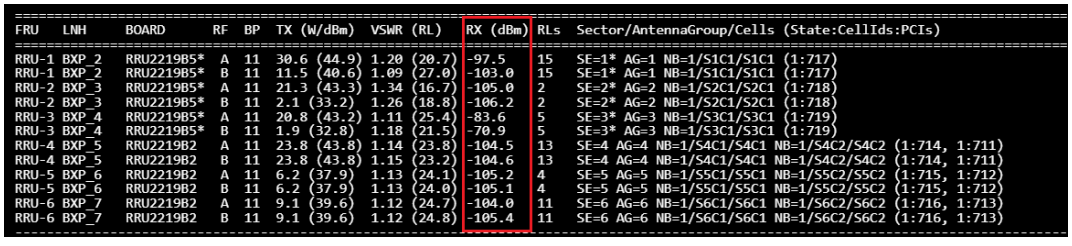
Al igual que con los valores de VSWR, para observar los RSSI existe más de una forma de revisión. El comando ***pmr***, muestra las mediciones de RSSI del Nodo. En la figura 71, se muestra una captura de una medición RSSI para un Nodo 3G, se observa que el sitio en revisión tiene configurados 9 celdas, todas con RSSI dentro de rango, mediante este mismo comando, hay otras opciones de verificación, por ejemplo, se puede seleccionar una de las opciones que muestra un log de 1 hora seccionado en tramos de 30 minutos o 15 minutos para evaluar el comportamiento del RSSI del sitio en ese periodo de tiempo. Si se desea ver el comportamiento en un periodo más prolongado, por ejemplo un día, una semana o meses no será posible desde la información que se va almacenando en el nodo, ya que se va borrando, únicamente guarda valores de una hora, pero los datos son enviados sistemas de calidad de red, por tanto el Ingeniero NOC se deberá apoyar de herramientas estadísticas que guarden la información y muestren o grafiquen los datos para realizar un análisis de la falla, en función de los valores afectados.



```
Start Time: 2023-01-25 04:15:00 End Time: 2023-01-25 05:00:00
 Object                                                  AvgRssiHigh AvgTxPwr AvgTxPwrPercMax Perc90TxPwr
 1,NodeBLocalCell=S1C1,NodeBSectorCarrier=S1C1               -105.2      41.6           59.1        43.5
 1,NodeBLocalCell=S2C1,NodeBSectorCarrier=S2C1               -106.6      37.5           23.0        37.5
 1,NodeBLocalCell=S3C1,NodeBSectorCarrier=S3C1               -105.0      39.5           36.1        43.5
 1,NodeBLocalCell=S4C1,NodeBSectorCarrier=S4C1               -106.4      39.8           39.4        43.5
 1,NodeBLocalCell=S4C2,NodeBSectorCarrier=S4C2               -106.5      40.4           44.0        43.5
 1,NodeBLocalCell=S5C1,NodeBSectorCarrier=S5C1               -106.7      39.2           34.7        43.5
 1,NodeBLocalCell=S5C2,NodeBSectorCarrier=S5C2               -106.6      39.3           34.8        43.5
 1,NodeBLocalCell=S6C1,NodeBSectorCarrier=S6C1               -106.6      39.1           32.8        43.5
 1,NodeBLocalCell=S6C2,NodeBSectorCarrier=S6C2               -106.8      39.2           34.2        43.5
```

Figura 71. Medición RSSI pmr

Con el comando ***cabx***, también es posible evaluar los niveles RSSI, en este caso nos da información del nivel RX en cada puerto del RRU. En la figura 72, se muestra información de los niveles actuales de RSSI para cada puerto de cada radio, por ejemplo, el RRU-1 tiene niveles dentro del rango permitido en el puerto A: -97.5 dBm, en el puerto B: -103.0 dBm, sin embargo en el RRU-3 ambos puertos muestran niveles RSSI fuera de rango, Puerto A: -83.6 dBm y Puerto B: -70.9 dBm.



```
FRU    LNH     BOARD       RF  BP  TX (W/dBm)  VSWR (RL)    RX (dBm) RLs  Sector/AntennaGroup/Cells (State:CellIds:PCIs)
RRU-1 BXP_2   RRU2219B5*  A   11  30.6 (44.9) 1.20 (20.7) -97.5    15   SE=1* AG=1 NB=1/S1C1/S1C1 (1:717)
RRU-1 BXP_2   RRU2219B5*  B   11  11.5 (40.6) 1.09 (27.0) -103.0   15   SE=1* AG=1 NB=1/S1C1/S1C1 (1:717)
RRU-2 BXP_3   RRU2219B5*  A   11  21.3 (43.3) 1.34 (16.7) -105.0   2    SE=2* AG=2 NB=1/S2C1/S2C1 (1:718)
RRU-2 BXP_3   RRU2219B5*  B   11  2.1 (33.2)  1.26 (18.8) -106.2   2    SE=2* AG=2 NB=1/S2C1/S2C1 (1:718)
RRU-3 BXP_4   RRU2219B5*  A   11  20.8 (43.2) 1.11 (25.4) -83.6    5    SE=3* AG=3 NB=1/S3C1/S3C1 (1:719)
RRU-3 BXP_4   RRU2219B5*  B   11  1.9 (32.8)  1.18 (21.5) -70.9    5    SE=3* AG=3 NB=1/S3C1/S3C1 (1:719)
RRU-4 BXP_5   RRU2219B2   A   11  23.8 (43.8) 1.14 (23.8) -104.5   13   SE=4 AG=4 NB=1/S4C1/S4C1 NB=1/S4C2/S4C2 (1:714, 1:711)
RRU-4 BXP_5   RRU2219B2   B   11  23.8 (43.8) 1.15 (23.2) -104.6   13   SE=4 AG=4 NB=1/S4C1/S4C1 NB=1/S4C2/S4C2 (1:714, 1:711)
RRU-5 BXP_6   RRU2219B2   A   11  6.2 (37.9)  1.13 (24.1) -105.2   4    SE=5 AG=5 NB=1/S5C1/S5C1 NB=1/S5C2/S5C2 (1:715, 1:712)
RRU-5 BXP_6   RRU2219B2   B   11  6.2 (37.9)  1.13 (24.0) -105.1   4    SE=5 AG=5 NB=1/S5C1/S5C1 NB=1/S5C2/S5C2 (1:715, 1:712)
RRU-6 BXP_7   RRU2219B2   A   11  9.1 (39.6)  1.12 (24.7) -104.0   11   SE=6 AG=6 NB=1/S6C1/S6C1 NB=1/S6C2/S6C2 (1:716, 1:713)
RRU-6 BXP_7   RRU2219B2   B   11  9.1 (39.6)  1.12 (24.8) -105.4   11   SE=6 AG=6 NB=1/S6C1/S6C1 NB=1/S6C2/S6C2 (1:716, 1:713)
```

Figura 72. Medición RSSI cabx

El otro factor a valorar durante una revision de niveles de RSSI, consiste en imblancia en niveles entre puertos del mismo RRU, cara RRU debería tener aproximadamente el mismo nivel de RSSI (interferencia) en cada uno de sus puertos ya que usan el mismo hardward (Radio y antena), un imbalance significa que en la línea que tiene un valor peor del RSSI existe una inducción de interferencia que puede ser producto de un defecto en el cableado (feeder – jumper).

Tomando como referencia la figura 91, se observa un imbalance en el nivel Rx para el RRU-1 de 5.5 dbm que sería la diferencia entre los -103 dbm del puerto B respecto a los -97.5 dbm del puerto A. También existe otro imbalance para el RRU-3, La diferencia entre el Puerto A y B es de aproximadamente 13 dbm, aunque ambos RRU presente este imbalance el nivel de RSSI para el RRU-1 está dentro rango Rx (mejor que -95 dmb), pero para el RRU-3 está fuera del rango permitido, además el imbalance Rx es muy grande. Se maneja en la practica un umbral de diferencia de 10 dbm, ya es un valor significativo, en base a ello, para el RRU-1 no es necesario efectuar un cambio, pero para el RRU-3 si se necesita una revisión de campo, puede existir algún cortocircuito, atenuación o mal acople en el jumper de ese puerto.

Los factores que normalmente afectan el RSSI son:

- Corrosión
- Polvo
- Humedad
- Flojedad en conectores
- Antena en mal estado

Sin embargo, no todas las fallas por malos valores de RSSI deben atenderse en campo, algunas veces pueden ser inducidas por interferencias de señales por operar en una misma banda de frecuencia con otra entidad de telecomunicaciones, también puede ser producto del tráfico (cantidad de usuarios) de la zona y/o orientación y distancia de las antenas respecto a los poblados. Para ese tipo de revisión, es necesaria la valoración de un especialista en radio frecuencia (RF) ya que deben evaluar factores topográficos ubicación de la torre (georreferencia), Tild de la antena y otras series de pruebas que no son del alcance de un Ingeniero NOC, ya que propósito del NOC no es el de optimizar los recursos de los sitios celulares, sino monitorear y gestionar fallas sobre la red que afecten o degraden el servicio por fallas en hardware o software en algunos escenarios y el área de O&M RBS atiende las fallas que se le reportan desde el monitoreo de la red.

A nivel del Ingeniero NOC, se realiza una valoración los parámetros de VSWR en primera instancia, ya el VSWR puede degradar influir en la medición del RSSI; también valorar las imbalancias en los puertos de los RRU, además de las degradaciones de Hardware o evento de temperatura ya que son indicativos de fallas físicas y se deberán atender con el personal de campo.

7.2.4.3. Trabajo de campo

El trabajo de campo para fallas de diversidad dependerá del tipo de radio base que se tiene instalada en sitios, actualmente como se ha indicado existían radios bases con DTRU en el gabinete y la antena en la torre, para ese esquema existían muchos más puntos de falla y se realizaban más revisiones:

- Estado del DTRU
- Revision de acoples en los jumpers
- Posible agua en la línea de feeder
- Estado en la CDU
- Estado del TMA
- Estado general del feeder

Sin embargo, con el esquema actual en el cual tanto el radio y antena estan en la torre, hay menos puntos de falla, el Ingeniero de campo debe revisar:

- Estado del puerto del RRU
- Descartar flojedad en conector
- Descartar daño de conector por corrosión
- Validar posible infiltración de agua en el feeder
- Verificar estado general de la línea feeder de conexión entre el RRU y la atena por posible quebradura (circuito abierto) o cortocircuito.

Las acciones posibles para superar la falla son:

- Resocar terminales en el RRU (puerto) y en la antena (dipolo)
- Cambio de jumper.
- Revisión de la impermeabilización de las juntas (envulcado de protección contra cambios climáticos)
- Reset físico al RRU.

7.2.5. Fallas de Hardware/Software DU/BB

7.2.5.1. Conexiones Física de la Transmisión hacia la RBS

Una tarjeta DU o BB puede quedar completamente fuera de servicio y gestión remota por 2 razones principales: una falla a nivel de transporte o una falla en propia en la tarjeta de radio base. Existe una conexión física entre el medio de transmisión y la RBS, puede ser una conexión eléctrica o una conexión Optica, el medio de Tx puede tener más opciones de ultimas millas hacia la red de transporte, puede haber una conexión óptica, una conexión por radiofrecuencia o incluso una conexión satelital, sin embargo, de forma local en un sitio celular la conexión entre los equipos es por medio de cableados.

Un cableado es un punto potencial de falla en 3 partes físicas: puerto/conector del equipo de transmisión, cable óptico/eléctrico, puerto/conector de la tarjeta de control móvil, se pueden dar fallas a nivel de configuración lógica como problemas de negociación, o se pueden presentar problemas físicos como daño en el equipo de transporte, daño en los equipos de la radio base, daño en los conectores, daños en los puertos, equipos inhibidos, etc. También pueden presentase fallas en las conexiones entre las tarjetas de la RBS.

En la figura 73, se muestra dos escenarios diferentes de conexiones entre equipos de transmisión y equipos RBS, no son los únicos posibles, pero son los más representativos y otros escenarios serian una combinación de ambos casos. Se observan 2 bloques claramente definidos: el primer bloque corresponde a la transmisión, es decir equipos de transporte (router, switch, radios, vsat), el ultimo equipo de la red de transporte que tiene una conexión directa hacia la radio base, y el segundo bloque corresponde a los equipos de la radio base, posibles combinaciones de tarjetas DU/BB interconectados para lograr conectividad entre el Core Movil o Equipos de control RAN (BSC/RNC) y esos equipos RBS.

El primer ejemplo: Sitio A, se muestra una conexión entre un equipos de transporte, un Router Cisco ASR920 mediante una conexión por cable de fibra óptica hacia una tarjeta Baseband BB6630, internamente en la radio base (bloque RBS) existe una segunda conexión, ésta vez entre las dos tarjetas baseband, este tipo de conexión a nivel de radio base se conoce como Cascadeo, ya que la primer baseband le da la transmisión a la segunda, es útil para optimizar los puertos en los equipos de transmisión por que se requiere de un solo puerto Tx para dar transporte a dos o más baseband, es posible, realizar una conexión de cada baseband hacia el ASR, sin embargo se perdería el propósito de la optimización de puertos y en dependencia de la ubicación del ASR en el sitio A puede requerir

de un mayor cableado, ya que los equipos de transporte pueden estar ubicados físicamente en el mismo gabinete de la radio base o pueden estar ubicados en una caseta/datacenter independiente al gabinete. Cuando se hace cascadeo de baseband por lo general en la primera BB se configuran los sectores para la tecnología LTE, y en la segunda basedand se configura los sectores para las tecnologías WCDMA y GSM, es decir se tendrá una BB para el 4G y una BB para 2G/3G. Bajo este escenario pueden fallar los transiver (SFP) de conexión en los puertos ópticos, o los conectores RJ45 en caso que fueran eléctricos en todos los puertos de ambos bloques, puede fallar la negociación, por general se deja configurada en 1GB full dúplex y pueden fallar el ASR o cualquiera de las Baseband, en cuyo caso se debe efectuar un restoring y/o cambio de la tarjeta y puede fallar la fibra óptica o el cable eléctrico

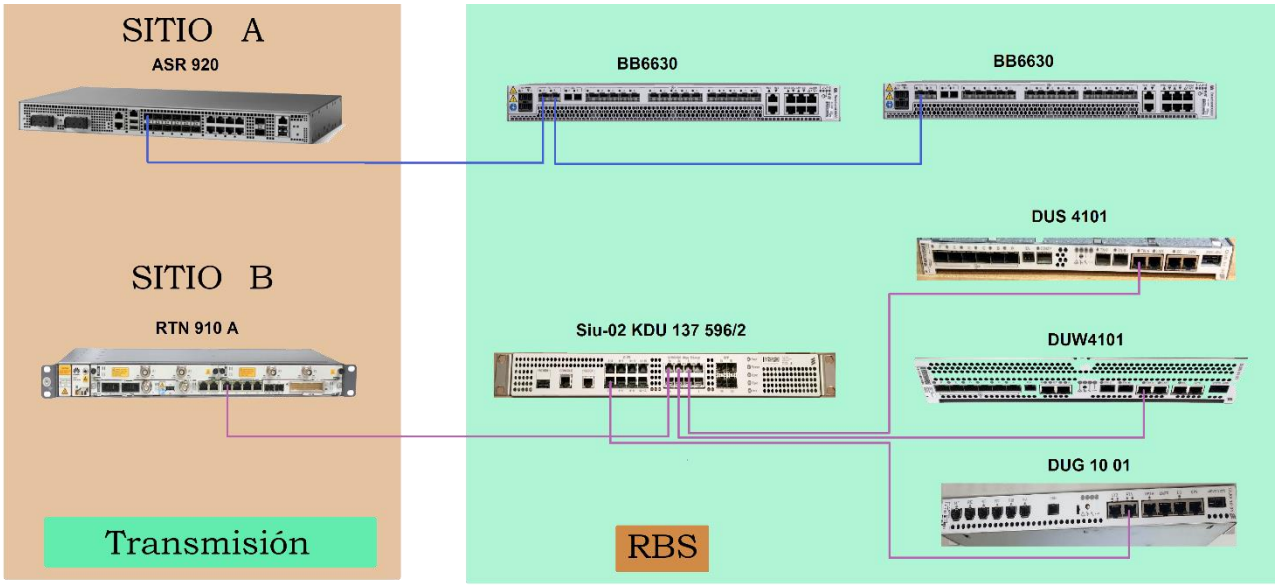


Figura 73. Conexiones equipos Transmisión y RBS

En el segundo ejemplo: Sitio B, el equipo de transporte es un radio Huawei RTN910A, la conexión hacia la RBS se realiza mediante el puerto eléctrico del radio, de lado de la RBS también se conecta en un puerto eléctrico en un equipo de distribución de trafico llamado SIU, esta conexión también es posible realizarla mediante los puertos óptico, dependerá de las condiciones y la planificación del sitio; en el bloque correspondiente a la RBS, tenemos además de la SIU, 3 tarjetas de control de tráfico móvil: DUG para control del sectores 2G, DUW para 3G y DUS para 4G, la SIU se encarga de recibir en un único puerto la trasmisión y luego distribuirla hacia las otras tarjetas, separando y distribuyendo el tráfico que viene filtrado por VLAN y realizando además de la conectividad IP, una conectividad hacia la BSC en el caso de las GSM, para el caso de los Nodos B y los eNodeB

es transparente únicamente sirve como túnel físico para pasar el trafico filtrado. Al igual que con el ejemplo del sitio A, en el sitio B se tienen los mismos puntos de falla, todo el cableado, conectores, transiver (SFP) y puertos ópticos o eléctricos.

La conexión desde la SIU hacia la DUG se realiza mediante los puertos E1/T1 del lado de la SIU y en los puertos ETA o ETB del lado de la DUG, utilizan un cable ethernet con una distribución de pines especial, este cable lo facilita el proveedor, el personal de campo si atiende una falla y encuentra daño en cable, no lo construiría, lo reemplazaría por una que brinde el proveedor.

Desde la SIU hasta la DUW o DUS se puede establecer una conexión por medio de puertos óptico o eléctricos, normalmente se usan los puertos eléctricos, igualmente es un cable eterneth con conectores RJ45 y las posibles fallas son las mismas en cableado o conectores. Adicional existe la posibilidad que se dañe el Software de la tarjeta y o la tarjeta como tal y se deben efectuar procedimientos de campo para el restablecimiento del servicio en estos escenarios como recarga de Software en las tarjetas existentes o en tarjetas nuevas para el cambio de hardware.

Se pueden realizar otras combinaciones como por ejemplo conectar una baseband a un puerto de una SIU, o conectar una DUW/DUS directamente a un puerto del equipo de transporte, todo dependerá de las necesidades que se tengan en sitio por ejemplo hay que equipos de transporte que aunque tengan puertos disponibles, no se tenga la licencia para ponerlos en operación y prácticamente no se pueden utilizar, pasa bastante en los radios, entonces desde la RBS únicamente se tendrá un puerto disponible para el transporte, habrá que adaptar el Hardware mediante una SIU o mediante cascadeo de Baseband. Bajo el mismo ejemplo que el radio tiene un solo puerto de transporte con licencia, se puede dar una solución a nivel de transporte de integrar un Switch o un router que sirva para tener más disponibilidad de puertos para la RBS e incluso integrar otros servicios distintos a la móvil, volviendo a tener disponibilidad de puertos en el medio de transmisión.

Por lo general se necesitan usar puertos adicionales en los equipos de transmisión cuando se tiene degradación en la medición del IUB que es la interfaz de conexión entre la RNC y un Nodo B, para ello se separa el tráfico que se pasa a través de una SIU y se utilizan los puertos del equipo de transmisión directamente para conectar las tarjetas DUW o DUS.

7.2.5.2. Monitoreo remoto

Cuando se tiene fallas de hardware en DU/BB normalmente lo que se observa desde el monitoreo es que no se tiene gestión remota del sitio, se pierde conectividad al servicio y presenta alarma como:

- Gigabit Ethernet Link Fault
- Heartbeat Failure (Failed to resolve Notification IRP)
- RaxDeviceGrupe_GeneralSwError

Estas alarmas nos indican que no tenemos conexión hacia el Nodo, sin gestión remota el Ingeniero NOC no podrá realizar un TroubleShooting para intentar restablecer el servicio desde el equipo caído, pero si se pueden efectuar una serie de pruebas en conjunto con el equipo NOC que administra la red de transporte. Por ejemplo, en la figura 92, para el sitio A, donde la primer baseband es el LTE y la segunda baseband es el Nodo B/GSM, si están caídas ambas baseband, se debe consultar por el estado el puerto en el ASR, a nivel de transporte podrán hacer una revisión por ejemplo si hubo falla en la negociación (que se encuentre en half dúplex en vez de full dúplex), si hay acumulación de errores CRC, realizar una limpieza de errores, en caso que el puerto este Down probar un reset remoto de la interfaz para descartar que esté inhibida; en cambio si la baseband que está afectada es únicamente la que tiene configurada las celdas 3G, significa que la falla no está en el transporte sino en la conexión local entre ambas baseband, en esa circunstancia se tendrá gestión de la BB LTE y se validara únicamente que el puerto TN asignado para el cascadeo esté Disable, pero no se efectúa un troubleshooting para intentar restablecer el servicio como un reset. Se debe movilizar inmediatamente al personal de campo para que haga una revisión física de la conexión indicada y de la tarjeta BB. Para revisar los puertos configurados en una Baseband se utiliza el comando ***lst***.

Si el servicio no estuviera caído por completo y presentara intermitencia se puede verificar desde la baseband la negociación de los puertos, para ello se efectúa el siguiente procedimiento:

- Revisión de puertos TN con el comando ***lst***. En la figura 74 se muestra como revisar la cantidad de puerto TN configurados y cuáles son, éste ejemplo se aplica para el Sitio A cuando la BB LTE debe tener dos puertos TN en operación, un puerto para hacia el equipo de transporte y otro puerto hacia la BB 3G.

```
LMN0019> lst

230125-23:00:30                    MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/20114
================================================================================
Proxy  Adm State      Op. State     MO
================================================================================
   41  1 (UNLOCKED)  1 (ENABLED)   ENodeBFunction=1,EUtranCellFDD=LMN0019A
  133  1 (UNLOCKED)  1 (ENABLED)   ENodeBFunction=1,EUtranCellFDD=LMN0019B
  246  1 (UNLOCKED)  1 (ENABLED)   ENodeBFunction=1,EUtranCellFDD=LMN0019C
  359  1 (UNLOCKED)  1 (ENABLED)   ENodeBFunction=1,EUtranCellFDD=LMN0019U
  458  1 (UNLOCKED)  1 (ENABLED)   ENodeBFunction=1,EUtranCellFDD=LMN0019V
  575  1 (UNLOCKED)  1 (ENABLED)   ENodeBFunction=1,EUtranCellFDD=LMN0019W
15106                1 (ENABLED)   Transport=1,Bridge=GSM
15107                1 (ENABLED)   Transport=1,Bridge=IUB
15108                1 (ENABLED)   Transport=1,Bridge=MUB
15109  1 (UNLOCKED)  1 (ENABLED)   Transport=1,EthernetPort=TN_C
15110  1 (UNLOCKED)  1 (ENABLED)   Transport=1,EthernetPort=TN_D
15112                1 (ENABLED)   Transport=1,Ntp=1,NtpFrequencySync=1
15113                1 (ENABLED)   Transport=1,Ntp=1,NtpFrequencySync=2
15116                1 (ENABLED)   Transport=1,Router=LTE,InterfaceIPv4=1
15121  1 (UNLOCKED)                Transport=1,Router=LTE,TwampInitiator=1
15122  1 (UNLOCKED)  1 (ENABLED)   Transport=1,Router=LTE,TwampInitiator=1,TwampTestSession=1
15125                1 (ENABLED)   Transport=1,Router=OAM,InterfaceIPv4=1
15131                1 (ENABLED)   Transport=1,SctpEndpoint=1
15189  1 (UNLOCKED)                Transport=1,Synchronization=1,RadioEquipmentClock=1,NodeGroupSyncMember=2
15190  1 (UNLOCKED)  1 (ENABLED)   Transport=1,Synchronization=1,RadioEquipmentClock=1,RadioEquipmentClockReference=1
15191  1 (UNLOCKED)  1 (ENABLED)   Transport=1,Synchronization=1,RadioEquipmentClock=1,RadioEquipmentClockReference=2
================================================================================
Total: 251 MOs
```

Figura 74. Revisión de puerto TN configurados

- Verificación de la velocidad de negociación de los puertos TN mediante comando ***get*** con la sentencia del MO asignado a dicho puerto. En el siguiente ejemplo, ***get Transport=1,EthernetPort=TN_C***, se utiliza para verificación de la negociación del puerto TN_C, observa en la figura 75, que ambos puertos TN están configurados para negociar a 1 GB Full, y que tienen habilitada la auto negociación (TRUE), si ese valor estuviera el FALSE, sería un puerto con negociación forzada.

```
LMN0019> get Transport=1,EthernetPort=TN_C

230125-23:00:55                0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/20114
================================================================================
15109                          Transport=1,EthernetPort=TN_C
================================================================================
admOperatingMode               6 (1G FULL)
administrativeState            1 (UNLOCKED)
autoNegEnable                  true
availabilityStatus             i[0] =
egressQosClassification
egressQosMarking
egressQosQueueMap
encapsulation                  FieldReplaceableUnit=BB-1,TnPort=TN_C
ethernetPortId                 TN_C
holdDownTimer
ingressQosMarking              [0] =
lldpTransmit                   0 (DISABLED)
macAddress                     78:D3:47:A3:E9:3A
mtu                            9000
operOperatingMode              7 (1G_FULL_SLAVE)
operationalState               1 (ENABLED)
reservedBy                     [5] =
 >>> reservedBy = Transport=1,VlanPort=LTE
 >>> reservedBy = Transport=1,VlanPort=MUB_D
 >>> reservedBy = Transport=1,VlanPort=IUB_D
 >>> reservedBy = Transport=1,VlanPort=GSM_D
 >>> reservedBy = Transport=1,VlanPort=OAM
supplicant
userLabel
================================================================================
Total: 1 MOs
```

```
LMN0019> get Transport=1,EthernetPort=TN_D

230125-23:01:10                0f MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/20114
================================================================================
15110                          Transport=1,EthernetPort=TN_D
================================================================================
admOperatingMode               6 (1G FULL)
administrativeState            1 (UNLOCKED)
autoNegEnable                  true
availabilityStatus             i[0] =
egressQosClassification
egressQosMarking
egressQosQueueMap
encapsulation                  FieldReplaceableUnit=BB-1,TnPort=TN_D
ethernetPortId                 TN_D
holdDownTimer
ingressQosMarking              [0] =
lldpTransmit                   0 (DISABLED)
macAddress                     78:D3:47:A3:E9:3B
mtu                            9000
operOperatingMode              7 (1G_FULL_SLAVE)
operationalState               1 (ENABLED)
reservedBy                     [3] =
 >>> reservedBy = Transport=1,VlanPort=MUB_C
 >>> reservedBy = Transport=1,VlanPort=IUB_C
 >>> reservedBy = Transport=1,VlanPort=GSM_C
supplicant
userLabel
================================================================================
Total: 1 MOs
```

Figura 75. Revisión de negociación en Puertos TN

- Revisión del tipo de SFP instalada en los puertos TN, este valor es importante saberlo por si la capacidad del SFP instalado en el puerto TN excede a la del puerto Tx y este ocasionando valores de alta potencia en el Rx del ASR para el ejemplo del sitio A, condición que podría generar errores y posterior caída del puerto e intermitencias en la baseband. Se valida con el comando sdic y se visualiza como se muestra en la figura 95. Se puede visualizar el tipo de SFP en el puerto TN, únicamente cuando se utilice un puerto óptico en la baseband, si el puerto Tx es uno de los puertos eléctrico no será posible ver un inventario de SFP ya que no tiene instalada, es un conector RJ-45.

  Se podrá revisar el inventario de las SFP y tarjetas únicamente si hay gestión remota de la Baseband, pero es importante saber que si hay un daño o se cree que existe indicios de falla producto de la SFP si el técnico de campo no cuenta con repuestos, puede hacer pruebas con las SFP de los RRU ya que con conexiones ópticas y las SFP son las mismas que se utilizan para el puerto Tx, observa que en la figura 76, los SFP para los 6 puertos en la BB que van hacia los RRU utilizan del modelo RDH10265/2 (10GB / 10Km), el mismo que está instalado para el puerto TN, es por ello que, el intercambio de transiver puede ser una solución provisional en caso de falta de repuesto, ya que es prioritario recuperar la gestión y el servicio de toda la baseband y que quede un RRU alarmado momentáneamente mientras trasladan el SFP de repuesto.

```
==========================================================================================================================================================
ID ;RiL ;BOARD                    ;SFPLNH  ;PORT ;VENDOR          ;VENDORPROD       ;REV  ;SERIAL          ;DATE     ;ERICSSONPROD   ;WL       ;TEMP  ;TXbs  ;TXdBm  ;RXdBm  ; BER
==========================================================================================================================================================
 1 ;  1 ;BB6630                   ;000100  ;   1 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000122841 ;20201211 ;RDH10265/2 R1A ;1310.00 ;47C   ;49%   ;-2.21  ;-2.13  ;    0
 2 ;  2 ;BB6630                   ;000100  ;   2 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121119 ;20201210 ;RDH10265/2 R1A ;1310.00 ;48C   ;47%   ;-1.41  ;-4.44  ;    0
 3 ;  3 ;BB6630                   ;000100  ;   3 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121100 ;20201210 ;RDH10265/2 R1A ;1310.00 ;48C   ;47%   ;-1.92  ;-2.33  ;    0
 4 ;  7 ;BB6630                   ;000100  ;   7 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121120 ;20201210 ;RDH10265/2 R1A ;1310.00 ;50C   ;54%   ;-1.97  ;-3.49  ;    0
 5 ;  8 ;BB6630                   ;000100  ;   8 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000122861 ;20201211 ;RDH10265/2 R1A ;1310.00 ;50C   ;53%   ;-2.88  ;-2.04  ;    0
 6 ;  9 ;BB6630                   ;000100  ;   9 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121117 ;20201210 ;RDH10265/2 R1A ;1310.00 ;49C   ;51%   ;-3.00  ;-3.81  ;    0
 2 ;  2 ;RRU449944B2/B2544B66AC*  ;BXP_2   ;   1 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121107 ;20201210 ;RDH10265/2 R1A ;1310.00 ;49C   ;50%   ;-1.82  ;-1.97  ;    0
 4 ;  7 ;RRU449944B544B28C*       ;BXP_3   ;   1 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121108 ;20201210 ;RDH10265/2 R1A ;1310.00 ;43C   ;48%   ;-2.00  ;-1.91  ;    0
 5 ;  8 ;RRU449944B544B28C*       ;BXP_4   ;   1 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121106 ;20201210 ;RDH10265/2 R1A ;1310.00 ;41C   ;46%   ;-1.91  ;-3.16  ;    0
 6 ;  9 ;RRU449944B544B28C*       ;BXP_5   ;   1 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121105 ;20201210 ;RDH10265/2 R1A ;1310.00 ;44C   ;46%   ;-2.93  ;-2.18  ;    0
 1 ;  1 ;RRU449944B2/B2544B66AC*  ;BXP_6   ;   1 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121082 ;20201210 ;RDH10265/2 R1A ;1310.00 ;56C   ;56%   ;-2.20  ;-1.98  ;    0
 3 ;  3 ;RRU449944B2/B2544B66AC*  ;BXP_7   ;   1 ;WTD             ;RTXM228-702-C27 ;1.0  ;HA205000121109 ;20201210 ;RDH10265/2 R1A ;1310.00 ;50C   ;54%   ;-2.08  ;-3.09  ;    0
----------------------------------------------------------------------------------------------------------------------------------------------------------
TN ;    ;BB6630                   ;000100  ;   A ;SOURCEPHOTONICS ;SPP10ELRIDFREN  ;10   ;I5E2014496     ;20180413 ;RDH10265/2 R1A ;1310    ;42C   ;40%   ;-2.32  ;-7.54  ; 0/0
----------------------------------------------------------------------------------------------------------------------------------------------------------

==========================================================================================================
BOARD  ;LNH    ;PORT ;T ;S ;OpMode         ;AutoNeg ;MacAddress        ;VlanIds             ;LOS ;BER
==========================================================================================================
BB6630 ;000100 ;TN_A ;O ;1 ;1G_FULL        ;true    ;F0:B1:07:74:A6:B8 ;2400,2402,2500,2502 ;6   ;0/0
BB6630 ;000100 ;TN_C ;E ;1 ;1G_FULL_MASTER ;true    ;F0:B1:07:74:A6:BA ;2500,2502           ;0   ;0/0
----------------------------------------------------------------------------------------------------------
```

Figura 76. Revisión de modelo de SFP, comando sdic.

El otro escenario posible cuando estamos en una radio base que tiene una topología de red como se muestra en el Sitio B de la Figura 73, antes de las tarjetas DU existe un equipo intermedio que distribuye el trafico llamado SIU, el cual es administrado de forma remota por el Ingeniero NOC móvil, así que cuando afectan las tecnologías móviles, parte del diagnóstico del NOC es revisar la se tiene conexión hacia la SIU y en caso de haberlo, se debe revisar que alarmas hay en éste equipo.

Se debe analizar la lógica de las conexiones del sitio, por ejemplo: para el sitio B, si durante el monitoreo se detecta que esta fuera de servicio una de las tecnologías móviles, no hay un problema en la transmisión ya que los demás elementos que usan el mismo canal Tx esta Operativos, puede ser un problema en la tarjeta afectada o en la conexión entre la SIU y esa tarjeta DU, puede darse el caso que se dañe el puerto en la SIU y se tenga que cambiar todo el equipo por ello. Si están fuera todas las tecnologías, es decir, no hay conectividad hacia la DUG, DUW, DUS puede existir un daño en la SIU y se debe evaluar si hay conexión hacia la SIU, además de realizar todas las pruebas con el equipo de transporte que se indicaron cuando era una BB porque se está evaluando la conexión principal entre el Equipo Tx y el primer equipo de distribución de la móvil.

Para revisar si tenemos conectividad hacia una SIU se utiliza la herramienta de aprovisionamiento del ENM llamada Shell Terminal, es una interfaz CLI que ayuda a realizar pruebas con la SIU. Se debe manejar la IP de la SIU de cada sitio en la red en una base de datos para agilizar las revisiones.

- Primero se ingresa al Shell Termina y se ejecuta el comando ***ping***, para verificar que exista conectividad hacia la SIU. Se puede utilizar con una sentencia que permita analizar la cantidad de paquetes descartados, lo que resulta muy útil cuando el equipo de transmisión es una VSAT (enlace satelital) que es propenso a pérdidas de datos por cambios climáticos.

  En la Figura 77, se muestra un ejemplo de ping con 10 paquetes trasmitidos. El comando ejecutado para este propósito fue: ***Ping (dirección IP de la SIU) -c (cantidad de muestras).*** Sin embargo, también es posible hacer un ping sin determinar el número de muestras.

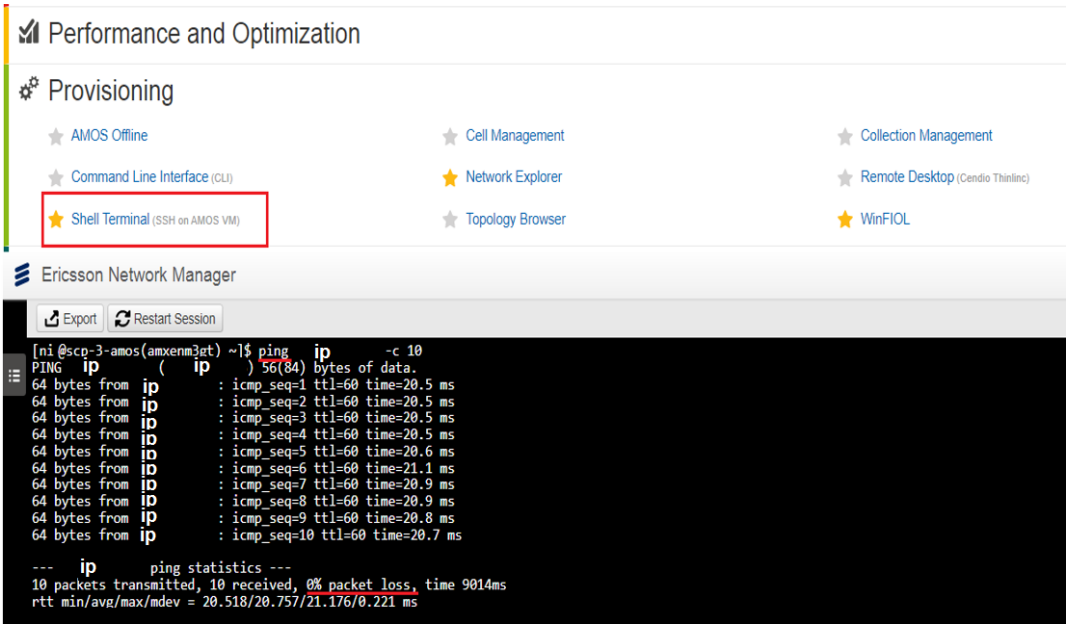


Figura 77. Prueba de ping hacia la SIU

- Lo siguiente es establecer una conexión ssh con la SIU para poder hacer revisiones de ella. En la figura 78, se muestra la ejecución del comando para la conexión, ***ssh admin@(dirección IP de la SIU)***, aceptamos la conexión con ***yes***, y luego ingresamos el ***password*** de acceso al equipo que el operador configura genéricamente en cada SIU.

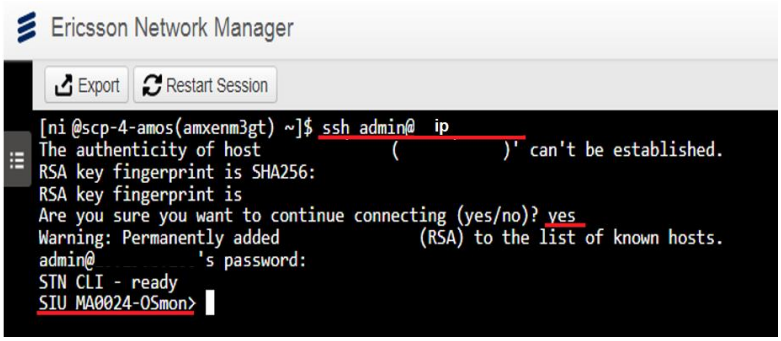


Figura 78. Conexión SSH con una SIU

- Luego se verifican alarmas presentes en la SIU con el comando ***getalarmlist*** como se muestra en la figura 79.

```
STN CLI - ready
SIU_MA0024-OSmon> getalarmlist
STN=0,Synchronization=0;
alarmId=            9;
eventTime=          2022-08-09 T14:57:55;
eventType=          "communicationsAlarm(2)";
perceivedSeverity=  "warning(4)";
probableCause=      "x733LossOfSignal(329)";
specificProblem=    "No Calibration from Time Server";
additionalText=     "Timing quality too bad or missing time server.";

STN=0,Synchronization=0;
alarmId=            10;
eventTime=          2022-08-09 T14:57:55;
eventType=          "communicationsAlarm(2)";
perceivedSeverity=  "major(2)";
probableCause=      "x733LossOfSignal(329)";
specificProblem=    "Calibration Date Expired";
additionalText=     "";

STN=0,EthernetInterface=SITE_LAN_1;
alarmId=            1328;
eventTime=          2022-12-20 T21:34:17;
eventType=          "communicationsAlarm(2)";
perceivedSeverity=  "major(2)";
probableCause=      "x733LossOfSignal(329)";
specificProblem=    "Ethernet Interface Down";
additionalText=     "Ethernet Interface Link Down - physical port 1";


OperationSucceeded

SIU_MA0024-OSmon>
```

Figura 79. Revisión de alarmas de una SIU

- De forma remota también podemos hacer una revisión de los puertos configurados sus velocidades de Negociación con el comando ***getmoattribute:***

```
STN=0,E1T1Interface=0; instanceId= 0;
STN=0,E1T1Interface=0; operationalState= enabled;
STN=0,E1T1Interface=0; type= E1;
STN=0,E1T1Interface=0; transmitClockSource= localTiming;
STN=0,E1T1Interface=0; receiveClockSource= notUsed;
STN=0,E1T1Interface=0; loopbackMode= off;
STN=0,E1T1Interface=0; loopbackStatus= off;
STN=0,E1T1Interface=0; loopbackRemainingTime= 0;
STN=0,E1T1Interface=0; fdlPerformanceReports= disabled;
STN=0,E1T1Interface=1; instanceId= 1;
STN=0,E1T1Interface=1; operationalState= enabled;
STN=0,E1T1Interface=1; type= E1;
STN=0,E1T1Interface=1; transmitClockSource= localTiming;
STN=0,E1T1Interface=1; receiveClockSource= notUsed;
STN=0,E1T1Interface=1; loopbackMode= off;
STN=0,E1T1Interface=1; loopbackStatus= off;
STN=0,E1T1Interface=1; loopbackRemainingTime= 0;
STN=0,E1T1Interface=1; fdlPerformanceReports= disabled;
STN=0,Equipment=0; instanceId= 0;
STN=0,Equipment=0; serialNumber= TU8XCE9073;
STN=0,Equipment=0; productRevision= R2F;
STN=0,Equipment=0; productNumber= KDU 137 596/2;
STN=0,Equipment=0; manufacturingDate= 20171106;
STN=0,Equipment=0; productName= SIU02;
STN=0,EthernetInterface=SITE_LAN_0; instanceId= SITE_LAN_0;
STN=0,EthernetInterface=SITE_LAN_0; operationalState= enabled;
STN=0,EthernetInterface=SITE_LAN_0; MAC_Address= 34:6E:9D:B5:76:DD;
STN=0,EthernetInterface=SITE_LAN_0; port= Gigabit;
STN=0,EthernetInterface=SITE_LAN_0; mode= AUTO;
STN=0,EthernetInterface=SITE_LAN_0; currentMode= gigabit;
STN=0,EthernetInterface=SITE_LAN_0; currentState= master;
STN=0,EthernetInterface=SITE_LAN_0; portNumber= 0;
STN=0,EthernetInterface=SITE_LAN_0; ethMaxFrameSize= 1522;
STN=0,EthernetInterface=SITE_LAN_0; flowControl= off;
STN=0,EthernetInterface=SITE_LAN_0; sendLinkAlarmAllowed= true;
STN=0,EthernetInterface=SITE_LAN_0; depTrafficManager= STN=0,TrafficManager=0;
STN=0,EthernetInterface=SITE_LAN_0; ptpInterfaceGroup= none;
STN=0,EthernetInterface=SITE_LAN_1; instanceId= SITE_LAN_1;
STN=0,EthernetInterface=SITE_LAN_1; operationalState= disabled;
STN=0,EthernetInterface=SITE_LAN_1; MAC_Address= 34:6E:9D:B5:76:DE;
STN=0,EthernetInterface=SITE_LAN_1; port= Gigabit;
STN=0,EthernetInterface=SITE_LAN_1; mode= 100MBitfullduplex;
STN=0,EthernetInterface=SITE_LAN_1; currentMode= noMode;
STN=0,EthernetInterface=SITE_LAN_1; currentState= master;
STN=0,EthernetInterface=SITE_LAN_1; portNumber= 1;
STN=0,EthernetInterface=SITE_LAN_1; ethMaxFrameSize= 1522;
STN=0,EthernetInterface=SITE_LAN_1; flowControl= off;
STN=0,EthernetInterface=SITE_LAN_1; sendLinkAlarmAllowed= true;
STN=0,EthernetInterface=SITE_LAN_1; depTrafficManager= STN=0,TrafficManager=1;
STN=0,EthernetInterface=SITE_LAN_1; ptpInterfaceGroup= none;
```

Figura 80. Revisión de Puertos de una SIU

En la Figura 80, se ejecutó el comando ***Getmoattribute***, muestra toda configuración de la SIU, se debe buscar las interfaces físicas para revisar que puerto se usa y que negociación tiene, se puede acotar la búsqueda dándole más información al comando como el SRN y la interfaz, pero si no hay una idea de la configuración de esta SIU, es recomendable ejecutar el comando sin ninguna sentencia adicional y buscar la información que necesitamos para el diagnóstico. En este caso podemos ver que la conexión E1/T1 utiliza el puerto 0 (***E1T1Interface=0***), esta interfaz conecta hacia una DUG para tráfico 2G, además hay 2 conexiones eléctricas LAN, es decir que una ira hacia el equipo de transporte y la otra hacia una DUW o DUS. La primera conexión LAN_0 (***EthernetInterface=SITE_LAN_0***) es un puerto de 1GB y está autonegociando a 1 GB, la segunda conexión LAN_1 (***EthernetInterface=SITE_LAN_1***) es un puerto de 1GB, negociando a 100MB full dúplex, entonces LAN_0 es la conexión hacia el equipo de transporte y LAN_1 es la conexión hacia una DUW.

Cuando tenemos afectación de una de las tecnologías móviles y hay gestión de una SIU, es recomendable efectuar un reset a una SIU. Se realiza un reset con el comando ***restart***.

Cuando se descartado falla a nivel de las conexiones hacia los medios de transmisión, y fallas en lo equipos intermedios, la última opción es una avería en el equipo final DU/BB, si no hay gestión se debe movilizar al personal de campo de forma inmediata, pero si logra gestión de la DU en un escenario donde hay intermitencia en el servicio, o celdas sin tráfico es conveniente revisar el estado de la tarjeta DU y brindar esta información al Ingeniero de campo que atenderá el evento.

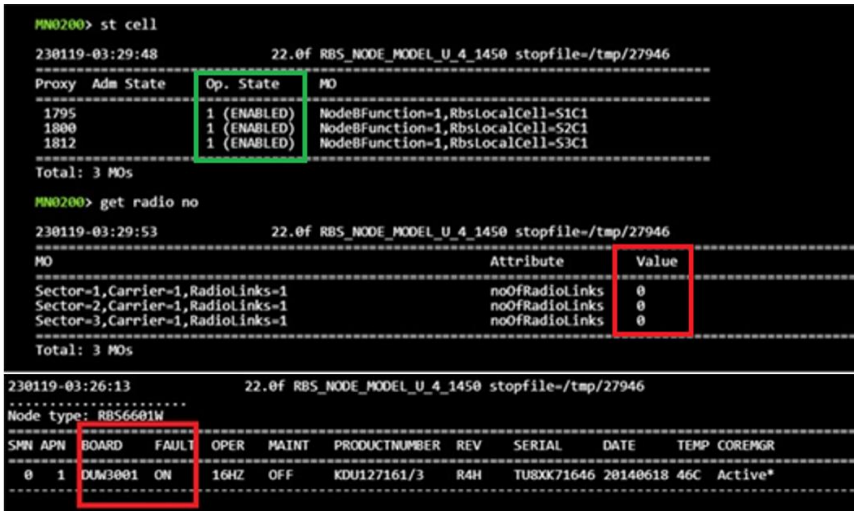


Figura 81. Revisión de tráfico y estado tarjeta DUW

En la figura 81, se muestra un ejemplo de una tarjeta DUW que está afectando la disponibilidad en el rubro 3G, al revisar las celdas se observa ENABLE (en servicio), pero al revisar el tráfico, no se generan valores, lo que significa que no hay tráfico 3G, con ***cabx*** o ***sdic***, revisamos que la tarjeta DUW3001 está en el campo FAULT mostrando el valor ON, con ellos nos damos cuenta que la DUW debe ser cambiada.

Como en todas las alarmas explicadas, entre más información se tenga de la falla y sea transmitida a los Ingenieros de campo, existen mayores posibilidades de resolver las averías más rápido y mantener en meta los KPI.

7.2.5.3. Trabajo de campo

El trabajo de campo para las fallas de Hardware/Software de una DU/BB consiste en efectuar una revisión física de todos los elementos de la radio base desde la etapa de transporte hasta la tarjeta DU/BB. El ingeniero de campo deberá:

- Revisar puerto estado del puerto en el equipo Tx, debe hacer una revision visual del código de colores que muestra el puerto en la transmisión y fi hay elemento que se observe quemado. Se pueden hacer pruebas de cambio de puerto con apoyo del NOC de transporte.
- Revisión del cableado de interconexión entre todos los elementos: Tx, BB, SIU, DUG, DUW, DUS.
- Revisión de la SFP en las BB, cuando utilizan puertos ópticos en la baseband si la interfaz no muestra color, es posible que la SFP esté en mal estado, se puede probar cambio con un repuesto se porte y no se tiene mano, se pueden utilizar los mismos SFP de las interfaces ópticas hacia los RRU.
- Pruebas de conexiones directa, establecer conexiones provisionales de pruebas entre algunos elementos para descartar Hardware. Por ejemplo, para sitio A de la figura 92, si están caídas ambas tecnologías, se puede quitar el cable Tx de la primer BB y conectarlos directamente el segunda BB, si levanta la BB 3G, se descarta falla de Transmisión y se descarta falla en la BB 3G, se tendrá un posible daño en la únicamente en la BB 4G.
- Si hubiese una SIU como el ejemplo del Sitio B de la figura 92, cuando todas las tecnologías están afectadas, también se puede conectar la DUS o DUW directamente en el equipo de transporte, si levanta el servicio, hay un daño en la SIU y debe cambiarse.

- Si hay afectación GSM en un sitio con SIU – DUG y se diagnostica que la SIU está en buen estado, en la DUG se puede probar recargar IDB a la flascard antes de cambiar la DUG.

Cuando se requiere hacer el cambio del Hardware, no solamente es cambiar tarjetas, por lo general vienen sin ningún tipo de configuración, se les debe cargar el Software y la configuración de la radio base para trabaje en condiciones óptimas, a este proceso se le conoce como restoring. Un restoring se puede hacer sobre una tarjeta DU/BB que este instalada y perdiera la configuración o sobre una tarjeta nueva que será instalada en sitio.

A continuación, se presentarán unos ejemplos de restoring en atención de campo.

Restoring DUW (Nodo B) / DUS (LTE)

Figura 82. Alarma local DUW

Figura 82, muestra alarmas de SW Error en la conexión local hacia la CDU/DUW, lo que indica un posible daño en la tarjeta, adicional el equipo muestra una alarma local de colores en led que indican daño en la tarjeta, por ello, será necesario recargar el Software a la tarjeta instalada o realizar cambio con una tarjeta nueva, en cuyo caso también es necesario cargarle el Software por lo que éste procedimiento es válido para ambos casos.

Pasos para restoring:

1. Ubicar el cable Emily en el puerto TEST de la CBU1 y/o puerto LMT de la tarjeta DUW y hacer la conexión HIPERTERMINAL de WINDOWS como se muestra en la figura 83.

Figura 83, Conexión hiperterminal

2. Ingresar el comando:
$ reload –
3. El sistema entra en modo basic setup listo para formatear las unidades.
4. Ingresar el comando:
$ mount_c2
$ formathd /c2
5. Preguntara si deseamos formatear y le digitamos y (yes).
6. Ingresar el comando:
$ reload --
7. Ingresar el comando:
$ formathd /d
8. Preguntara si desea formatear y le digitamos y (yes).
9. Ingresar el comando:
$ reload --
10. Ponerle IP de fábrica al nodo con el siguiente comando:
$ ifconfig le0 (dirección IP del nodo) netmask (mascara de red)
11. Ingresar el comando:
$ reload
12. Comprobar la nueva IP digitando el comando:

$ ifconfig

13. Luego de configurar la IP, se realiza una conexión ethernet:
    - Ubicar cable de Red en puerto ETH DE LA CBU1, en caso que la tarjeta dañada fuese una DUW, permanecería conectado en el puerto LMT.
    - Configurarle IP a la PC: (dirección IP) Máscara: (mascara de red)
    - Probar el segmento de la red: esto se hace en INICIO-EJECUTAR: ping (direccionip) –t (se comprueba conexión hacia la tarjeta que se aplicara el procedimiento)
    - En disco C de la PC debe haber 2 carpetas: llamadas CV y la otra UP. Dentro de CV se ubica el cv que vamos usar para restaurar el nodo y en UP se ubica el SOFTWARE con nombre CXP9014346_R6AC02 para el ejemplo, pero los tipos de Software van cambiando, actualizándose para las tarjetas, se debe saber con seguridad cual es el Sofware que tenía la tarjeta dañada para recargar el mismo y no generar conflictos a nivel de hardware y software por ejemplo problemas de licencia. Estos dos archivos (CV y SW) previamente se deben solicitar al Ingeniero NOC que tenga acceso al servidor utilizado como repositorio de datos de SW para los equipos de la red móvil. El Ingeniero de campo también puede tener guardados estos archivos de acuerdo a los equipos que tiene en su zona de operación para agilizar tiempos de atención ya que la descargar de los archivos puede tardar un poco ya que por seguridad se deben compartir mediante las plataformas internas de los operadores (intranet).

- Ingresar en el CMD y ubicarse en la ruta C:\ a como se muestra en la figura 84.

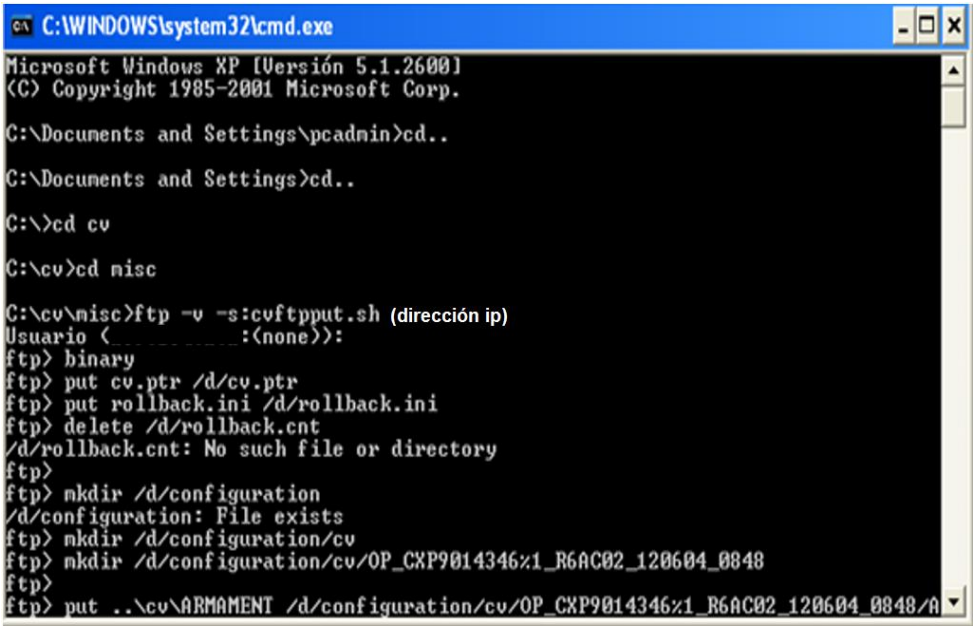


Figura 84. Búsqueda del archivo del Software a cargar en la tarjeta

- C:\cv\misc>ftp -v -s:cvftpput.sh (dirección ip) (Al ejecutar este comando, se hace una conexión la carpeta que contiene la información para instalarse en la tarjeta)
- Luego de ejecutar el comando hay que ir a la carpeta UP Y LUEGO al software mediante el comando cd, como se visualiza en la figura 85.

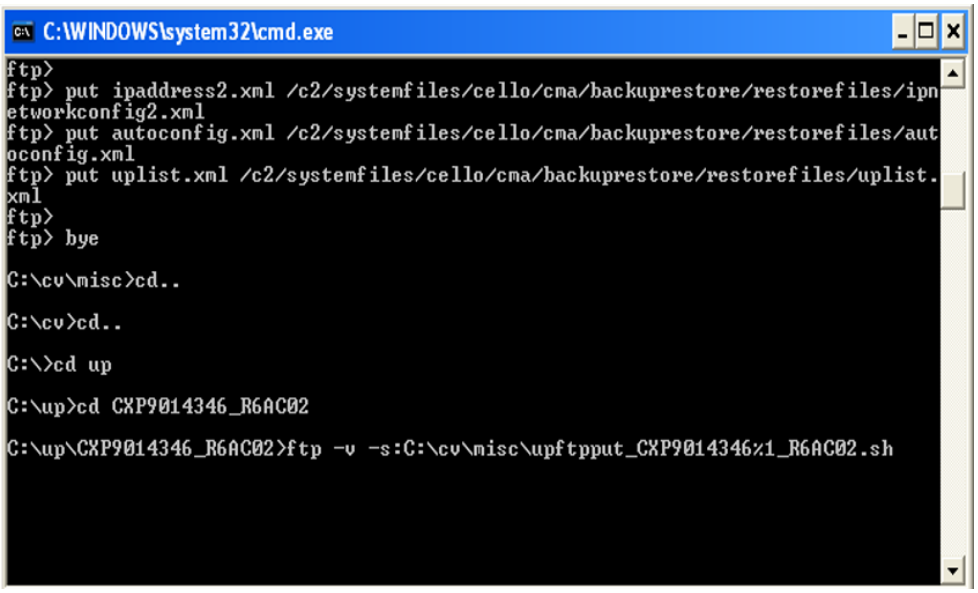


Figura 85. Búsqueda del archivo del CV a cargar en la tarjeta

- C:\up\CXP9014346_R6AC02>ftp -v -s:C:\cv\misc\upftpput_CXP9014346%1_R6AC02.sh (dirección ip) (Al ejecutar este comando, se hace una conexión la carpeta que contiene la información para instalarse en la tarjeta)

En este momento iniciará el proceso de carga del Software. Al finalizar la carga, se deberá efectuar nuevamente una conexión hiperterminal y ejecutar el comando:

- $ reload

Una vez a finalizado el restoring del Nodo, se procede a conectar el cable de Tx para que sincronice y levanten los servicios.

Restoring BB

Una vez se identifica que la Baseband debe cambiarse, o recargar el software se procede con el restoring. A continuación, se muestran los pasos a seguir.

1. Configuramos el puerto de red de nuestro Ordenador con las direcciones mostradas en la figura 86. Las cuales son genéricas cualquier tarjeta baseband, es decir creamos una ruta estática hacia la BB.

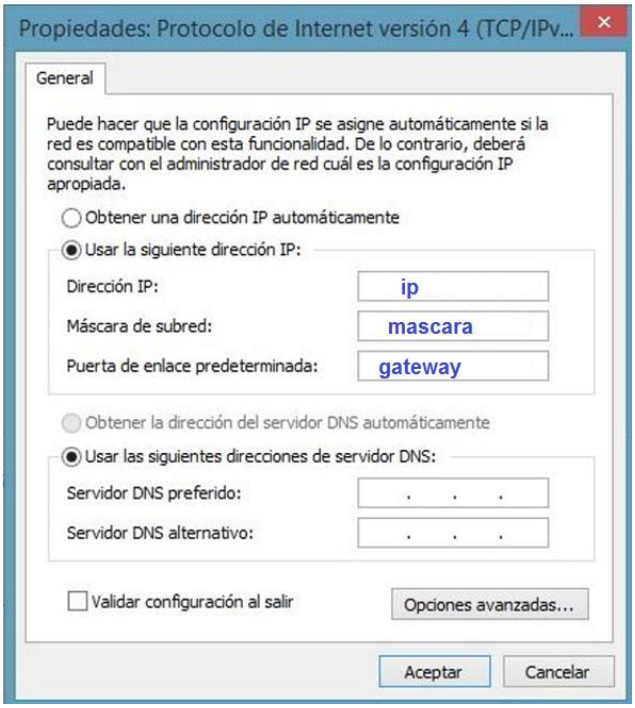


Figura 86. Configurar ruta estática en PC hacia BB

2. Nos aseguramos que los firewall y antivirus de nuestro Ordenador estén bloqueados para que nos permitan trabajar. Es recomendable trabajar con Internet Explorer para realizar los procesos en la BASEBAND

3. Poseer el Element Management Launcher ya instalado para hacer Troubleshooting luego del Restore.

4. Iniciamos el proceso conectándonos a la BASEBAND, en modo Baseband Emergency Access Windows mediante el navegador web en la dirección url destinada para ello, en la figura 87, se observa la vista del modo Emergency Access.

5. Verificamos estado en la tarjeta
   - NODE STATUS
   - NODE HANDLING

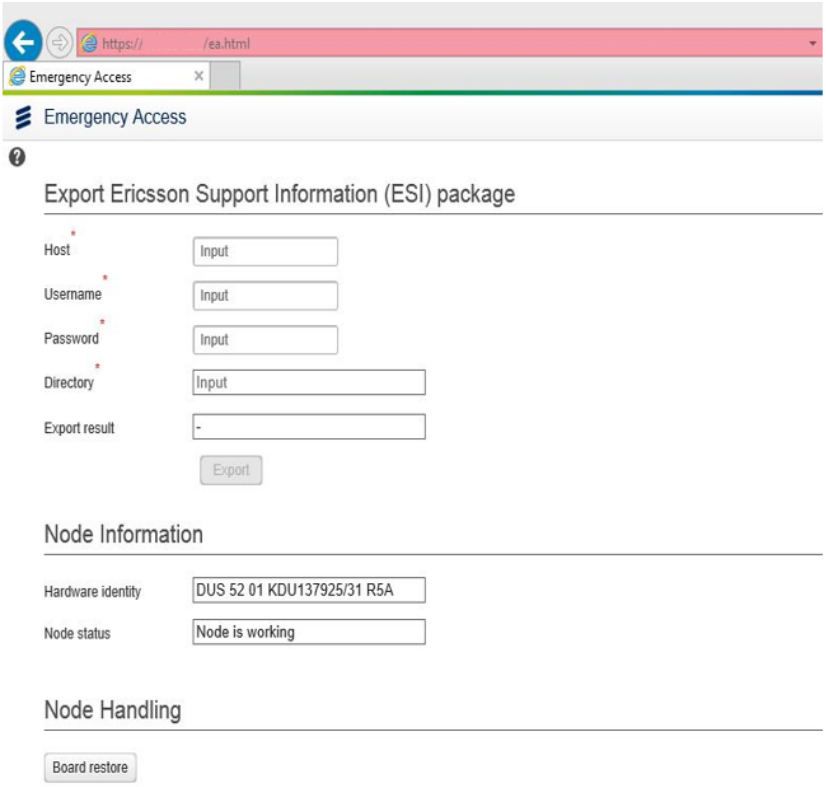


Figura 87. Baseband Emergency Access

6. Restauramos la BASEBAND, a su configuración Original. Accionamos el Botón de Restore Board y luego aguardamos que reinicie la BASEBAND a como se observa en la figura 88.

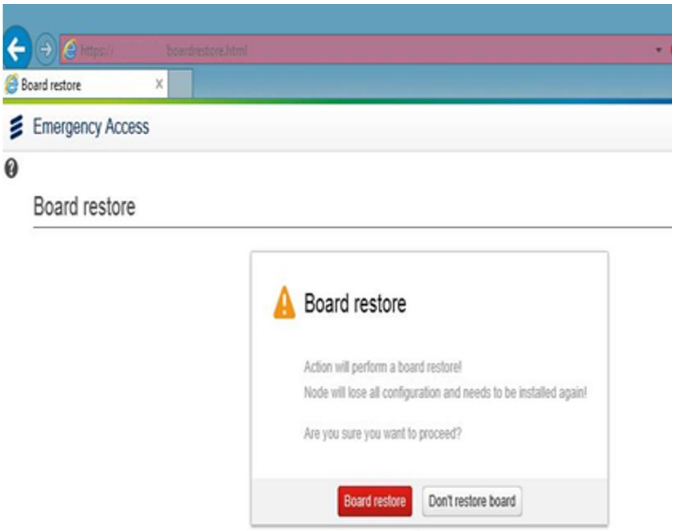


Figura 88. Ejecución de Board Restore

7. Exploramos nuestro Ordenador en Disco C; en esa ubicación a como se muestra en figura 89 Creamos una carpeta que contenga lo siguiente:
   - MiniCore SFP
   - Script de restore
   - CV_Backup el cual será con el que se hará el restore
   - SW en la versión que está el CV_Backup

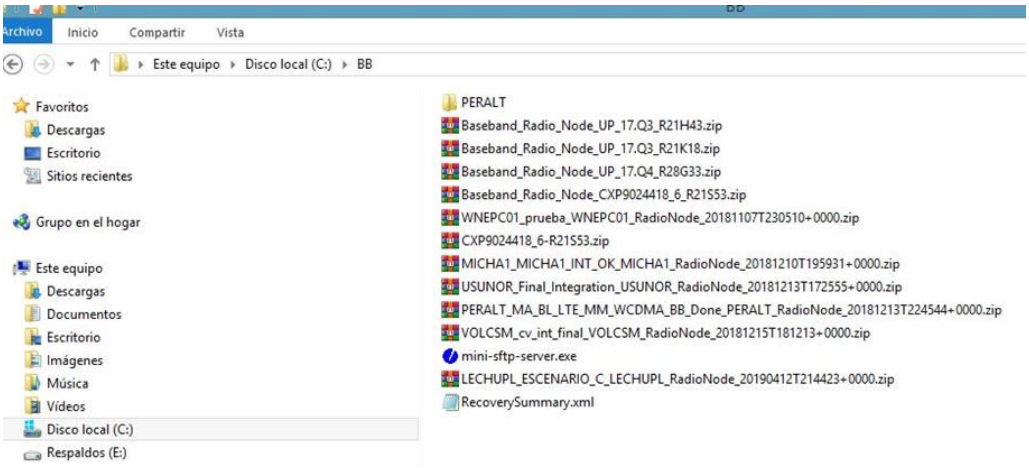


Figura 89. Carpeta en Disco C con archivos para restoring

8. Aperturamos el MiniCore SFP (mini-sfp-server) dentro de la carpeta y lo configuramos de tal manera que la dirección de donde se extraerá el CV con el que restauraremos la BASEBAND, será la misma de donde se encuentra nuestro Script de Restore y SW en la versión que está el CV Backup, descargado Previamente.

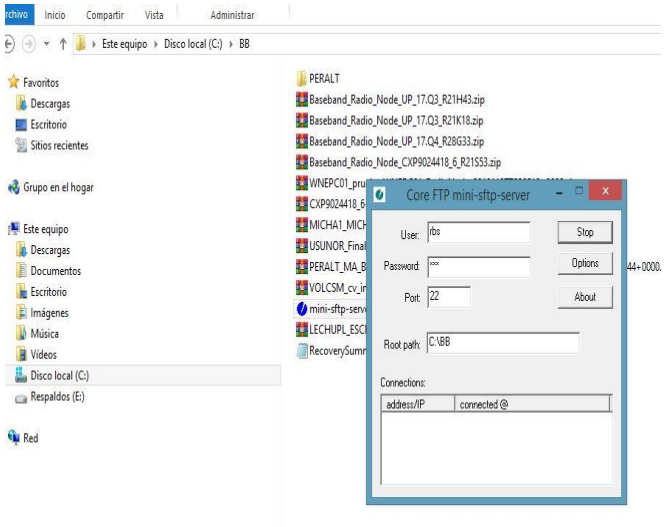


Figura 90. Configuración de ruta mini-sfp-core

9. Luego aperturamos el archivo RecoverySummary. Como se muestra en la figura 91, se realizará el Cambio del Script de Restauración, se colocarán en las líneas detalladas, el Nombre del CVBackup y el SW con la versión que se rescató, se deben declarar exactamente igual que el nombre que tiene dentro de la carpeta.

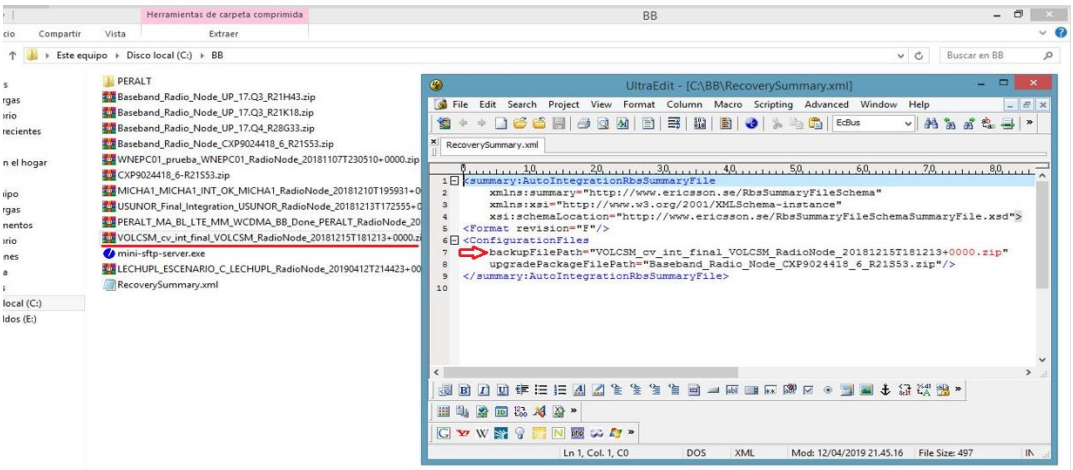


Figura 91. Configuración ruta CV en Recovery Summary

En la Figura 110, se observa cómo se declara en el campo ***backupfilepath*** y entre comillas dobles, el nombre del archivo del CV que contiene la última configuración del nodo. En la figura 111, se observa en el campo ***upgradePackegeFilePath*** igualmente entre comilla el nombre del Software a como está en la carpeta que usaremos para el restoring. Guardamos la configuración y cerramos el archivo.

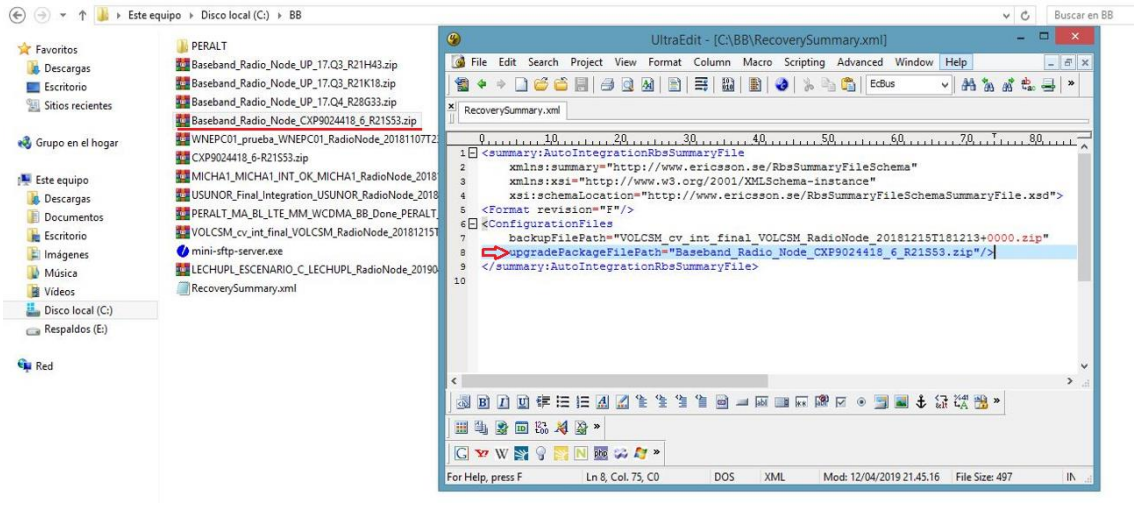


Figura 92. Configuración ruta SW en Recovery Summary

10. Aperturamos la ventana de configuración de la BASEBAND en el navegador web del ordenador con la URL: https://169.254.2.2, para que logre abrir la aplicación web debemos asegurándonos de poseer las direcciones en nuestro puerto de red ya configuradas previamente (Pestaña de LMT Integration activa), ese procedimiento se realizó en el primer paso.

11. Procedemos a colocar en la casilla de Host del menú Autointegration la dirección IP que configuramos previamente en el ordenador como se observa en la figura 112, dirección IP: 169.254.2.1.
    En los campos USUARIO Y PASS colocamos los mismos datos que fueron configuramos en el MiniCore SFP.
    En el campo SITE INSTALATION FILE, colocamos el nombre del script de restauración con su extensión, para que pueda ser llamado, es decir el archivo Recovery Sumary, como se aprecia en la figura 112 se declara el nombre RecoverySummary.xml.

12. Se procede a activa el botón Download Files como se muestra en la figura 93, asegurándose previamente que el mini core SFP continue abierto para que se ejecuten la descarga de archivos correctamente.

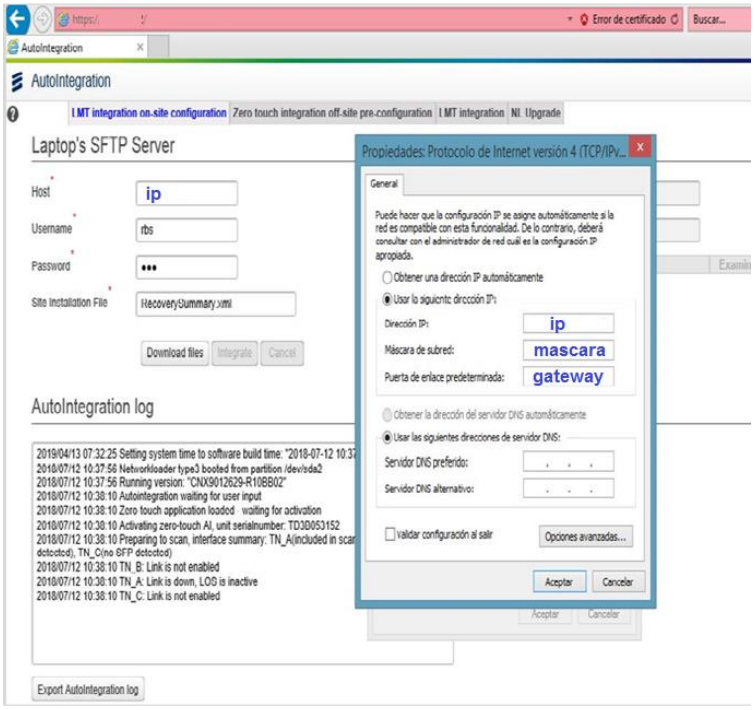


Figura 93. Configuración menú Autointegration BB

13. Se observa el avance en % para el proceso de restauración como se muestra en la figura 94.

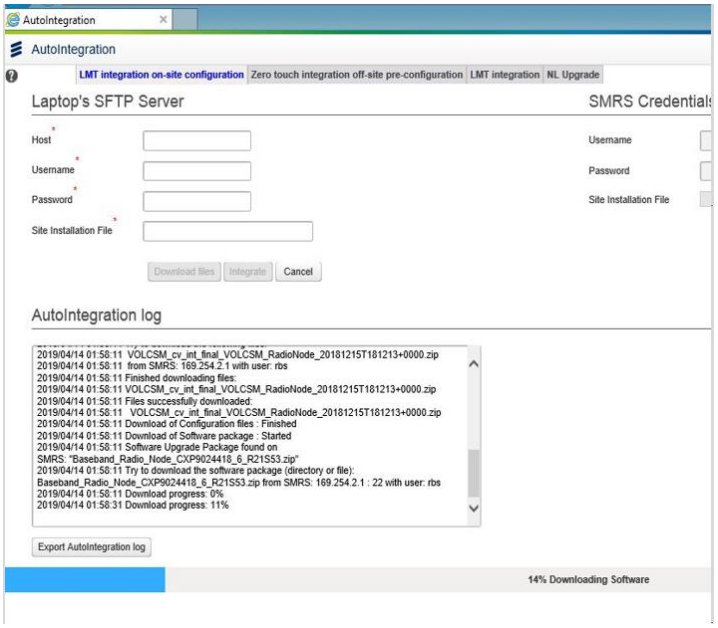


Figura 94. Porcentaje de descarga de archivos en la BB

14. Al avanzar el proceso de descarga de archivos se habilita la opción: ***Integrate***, la activamos y esperamos que finalice el proceso como lo muestra la figura 95.

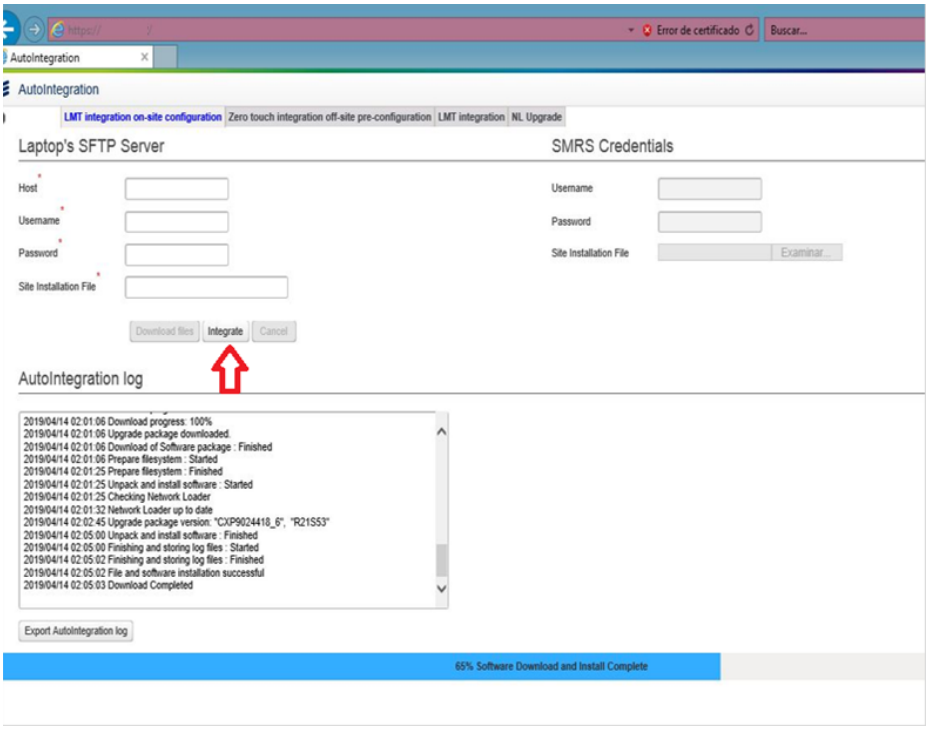


Figura 95. Activación de la opción Integrate - proceso de instalación SW - CV

15. Al finalizar la instalación, se conecta el cable de transmisión en la Baseband y se verifica localmente si lo servicios restablecieron. Luego se validan servicios con el NOC. La validación consiste en verificar:
    - Estados de las celdas, con el comando ***st cell***.
    - Alarmas activas, con el comanto ***alt***.
    - Trafico, con el comando ***get radio no*** (3G), ***ue print –admitted*** (4G).
    - Listado de cv, con el comando ***cvls***

Configuración SIU

Cuando el ingeniero de campo identifica que la SIU está generando la falla que ocasiona la caída del servicio una o más tecnologías se realiza el siguiente de procediendo:

1. Se realiza una revisión visual de la SIU, que esté encendida, que los leds muestren alarmas, y posible flojedad en conectores de alimentación DC, cable de alimentación dañado o breaker disparado.
2. Si el LED está en rojo, la SIU esta fault y se debe realizar el cambio del Hardware
3. Actualizar la SIU (Primary y Backup)

- Configurar en el ordenador la dirección IP: (ip de conexión a SiU); SUBNETMASK: *(mascara)*
- Conectar la PC al puerto de consola de la SIU (CONSOLE)
- Habilitar una sesión DOS (CMD) y efectuar un Ping infinito hacia el puerto de consola de SIU-02: *ping (ip Gateway SIU) –t* con el objetivo de verificar la conectividad entre la PC y la SIU.
- Habilitar la sesión Telnet en Putty o Winfiol para la SIU-02.
- Descargar el archivo de software T11B_MAINT2 de la carpeta C:\tn_ftp_home; y nombrarlo: siu02_sw.tar

PROCESOS DE COMISIONAMIENTO DE SIU-02

Conectarse a SIU por medio de software WINFIOL:

- OSmon> admin (Usuario para Inicio de Sesión)
- OSmon> hidden (Password para Inicio de Sesión)

Se Resetea la SIU:

- OSmon> resettofactorysetting
- OSmon> deleteAiMo

Luego del reinicio debemos establecer nuevamente una conexión a la siu desde el Winfiol con el admin y password por default y escribimos los siguientes comandos para iniciar la carga del nuevo software:

- OSmon> *startSWSession s1* (Iniciar sesión de carga de sw)
- OSmon> *uselocalsftp on* (Encender SFTP para transferencia de SW)
- OSmon> *downloadSW s1 sftp://anonymous:anonymous@(IP servidor data)/siu02_sw.tar*
  (descarga del sofrware para ser usado en SIU)

- OSmon> *getSWSessionstatus s1* (Revisión de estado de upgrade y esperas que aparezca el downlaodcomplete)
- OSmon> *activateSW s1* (Activas el upgrade cargado)
- OSmon> *endSWSession s1* (Finalizas la sesión de carga)
- OSmon> rev (Revisas el sw cargado y solo te aparece el primarybakcup)
- OSmon> startSWSession s1 (Inicias sesión para activar el backup de sw)
- OSmon> approveSW s1 (Activas el backup del sw y te muestra esta barra de progreso luego finalizas la session)
  [==========] OperationSucceeded
- OSmon> endSWSession s1 (finalizas la sesion)
- OSmon> rev (te muestra tanto el primary como el backup cargados)

Actualización del Backup Bank:

- OSmon> startSWSession S2
  OperationSucceeded
- OSmon> uselocalsftp on
- OSmon> downloadSW S2 sftp://anonymous:anonymous@(ip server data)/siu02_sw.tar
  OperationSucceeded
- OSmon> getSWSessionstatus S2
  DownloadInProgress
  OperationSucceeded
- OSmon> getSWSessionstatus S2
  DownloadCompleted
  OperationSucceeded
- OSmon> endSWSession S2
  OperationSucceeded
- OSmon> rev

Carga de SCRIPTS:

- OSmon> startSession bcm1
- OSmon> uselocalsftp on
- OSmon> download bcm1 sftp://anonymous:anonymous@(ip server data)/SIU_2VEL_ETH_RevD.xml (Nombre con extensión xml es único por sitio). ¡MUY ESPECIFICO EN EL NOMBRE !
- OSmon> getSessionstatus bcm1

- OSmon> activate bcm1
- OSmon> endSession bcm1

Antes de reemplazar una siu-02 en algunos casos se logra recuperar backup o scripts, los cuales facilitan la carga de la información en la nueva siu-02. En tal caso utilizamos los siguientes comandos generales para extraer dicha información y volver a cargar a la nueva tarjeta siu-02:

Descarga de Backup de SIU:

- OSmon> startSession bcm1
- OSmon> uselocalsftp on
- OSmon> backup bcm1 sftp://anonymous:anonymous@(ip server data)/backup_GBCNMXC0059.xml admin
- OSmon> getSessionstatus bcm1
- OSmon> endSession bcm1

Con ello finaliza el proceso de cargar de SW a una nueva SIU. El siguiente paso es rehabilitar las conexiones de la SIU y proceder a realizar validaciones de servicio con el NOC.

Existen situaciones en las que puede ser necesario realizar verificaciones de la configuración de la SIU de manera local como parte de un Troubleshooting, A continuación, se muestra un listado de comandos para distintas validaciones de la SIU:

i. Revisión de Tx por VLAN en Orden. proyecto ATT

- getmoattribute STN=0, VLANGroup=SIU_WAN
- getmoattribute STN=0, VLANGroup=SIU_WAN,VLAN=ABIS
- getmoattribute STN=0, VLANGroup=SIU_WAN,VLAN=IuB_WAN
- getmoattribute STN=0, VLANGroup=SIU_WAN,VLAN=MuB_WAN
- getmoattribute STN=0, VLANGroup=SIU_WAN,VLAN=S1X2_WAN
- getmoattribute STN=0, VLANGroup=SIU_WAN,VLAN=MuL_WAN
- getmoattribute STN=0, VLANGroup=SIU_WAN,VLAN=OAM
- getmoattribute STN=0,TGTransport=all
- getmoattribute STN=0,EthernetInterface=SIU_WAN
- showtable interface STN=0,EthernetInterface=SIU_WAN
- showtable interface STN=0,EthernetInterface=SIU_3G
- showtable interface STN=0,EthernetInterface=SIU_4G

ii. Revisión general y estado de puertos e IP´s (ENABLE/DISABLE)

- OSmon> getMOAttribute STN=0, ethernetinterface=all (Estado de puertos)
- OSmon> rev (REVISAR SW DE SIU)
- OSmon> getalarmlist (REVISAR ALARMAS)
- OSmon> getmoattribute stn=0, ipinterface=all (Interfaces IP en SIU)
- getmoattribute STN=0,TGTransport=all (Revision TG y IP de la BSC)

iii. Setear GATEWAY de OAM (gestión remota de la SIU)

- BCNMXC0077-OSmon> starttransaction asdf
- BCNMXC0077-OSmon> setmoattribute asdf STN=0, IPInterface=TCU_OAM defaultgateway (dirección ip de gestion)
- BCNMXC0077-OSmon> commit asdf
- BCNMXC0077-OSmon> endtransaction asdf

iv. Cambio de asignación en puertos eléctrico/óptico e IP OAM:

Estos comandos se utilizarán normalmente cuando un puerto ethernet (WCDMA o LTE), se daña; se tiene la opción de poder utilizar y configurar los demás puertos disponibles sin necesidad de cambiar todo el modulo o tarjeta(siu-02), para que siga operando. Por lo general estos puertos se dañan por corrientes parasitas como lo son las descargas atmosféricas. Utilizaremos los siguientes comandos dentro del programa winfiol y activando el sftp server:

- OSmon> starttransaction bcm1
- OSmon> setmoattribute STN=0,IPInterface=INT_OAM primaryIP_Address (dirección IP) (La IP puede variar según asignación)
- OSmon> checkconsistency bcm1
- OSmon> commit bcm1 forcedCommit
- OSmon> endtransaction bcm1
- OSmon> starttransaction bcm1
- OSmon> setmoattribute STN=0,wakeUpRegistration (dirección IP) (La IP puede variar según asignación)
- OSmon> checkconsistency bcm1
- OSmon> commit bcm1 forcedCommit
- OSmon> endtransaction bcm1

v. Cambiar puerto eléctrico

En este caso se utiliza para cambiar un puerto eléctrico o E1 que es utilizado solo para la GSM (2G).

- OSmon> starttransaction 1
- OSmon> setmoattribute 1 STN=0,Ethernetinterface=SITE_LAN_0 port Gigabit
- OSmon> setmoattribute 1 STN=0,EthernetInterface= SITE_LAN_0 mode 1000MBitfullduplex o AUTO
- OSmon> checkconsistency 1
- OSmon> commit 1 forcedcommit
- OSmon> endtransaction 1

vi. Cambiar puerto óptico:

También al igual que el caso anterior, se tiene la opción de poder realizar cambios de puertos ópticos por daños, para ello utilizamos los siguientes comandos:

- OSmon> starttransaction 1
- OSmon> setmoattribute 1 stn=0,Ethernetinterface=SITE_LAN_0 port SFP
- OSmon> setmoattribute 1 STN=0,EthernetInterface= SITE_LAN_0 mode Gigabitfullduplex
- OSmon> checkconsistency 1
- OSmon> commit 1 forcedcommit
- OSmon> endtransaction 1

vii. Restaurar una SIU:

Este paso se realiza cuando en una visita de campo o supervisión logramos extraer la información de la siu-02 y posteriormente cuando se presenta una falla en donde se halla perdido la información del backup de la siu-02 del sitio especifico, se procede a cargar la información en la nueva tarjeta a partir de los siguientes comandos:

- Login:admin
- Password:hidden
- OSmon> resettofactorysetting
- OSmon> deleteAiMo
- OSmon> startSession s1
- OSmon> uselocalsftp on

- OSmon> download s1 sftp://anonymous:anonymous@(ip server data)/SIU_BCKUP_GUALOSO.xml 15
- OSmon> getsessionstatus s1
- OSmon> restore s1 admin
- OSmon> endsession s1
- OSmon> getMOAttribute STN=0, Equipment=0 serialNumber

viii. Revisar temperatura:

Para monitorear la temperatura de la tarjeta y así saber el buen funcionamiento del sistema de clima o fanes que tiene la misma se ejecuta el siguiente comando.

- getmoattribute STN=0,TempSensor=0; currentTemp
- gettemperature

ix. Comandos de verificación:

- getmoattribute stn=0,ethernetinterface=all (revisar la interfaces ethernet)
- getmoattribute stn=0,ethernetinterface=all Mode (velocidad de puerto configurado)
- getmoattribute stn=0,ethernetinterface=all currentMode (muestra velocidad del puerto actualmente)
- getmoattribute stn=0,ethernetinterface=all operationalState (para verificar si esta enable o disable)
- getmoattribute stn=0,ethernetinterface=all portId (se utiliza para leer cuál puerto está asociado con la interface)
- timeservertest start (Revisar Sincronía)
- ping -c 1000 -s 1400 (dirección ip de la SIU)
- traceroute -s (ip origen) (ip destino)
- getneighbors (Status network)
- showMACFwTable all (Mac de transito de la red)
- getmoattribute STN=0,RoutingTable=0,IpRoute=all (tabla de ruta)
- getlinkoam interfacestatus STN=0,EthernetInterface=SITE_LAN_0,LinkOAM=0
- getTransactionStatus (confirma que está trabajando el performance)
- GetIRPVersion (Verificar Versión de SW)
- GetTemperature (verificar temperatura)
- Gettim (verificar fecha y hora de SIU)

- Restart (Reiniciar la siu sin borrar datos)
- getlinkoam interfacestatus STN=0,EthernetInterface=0,LinkOAM=0
- getlinkoam interfacestatus STN=0,EthernetInterface=SITE_LAN_0,LinkOAM=0
- startsw <tab>
- getsessionst <tab>
- getmo <tab>
- getcontai <tab>
- gettime
- gettemperature
- repeat <cerrarlo con control+c>
- show arp (muestra el protocolo de internet)
- show ip route (muestra la ruta)
- show ip interface brief (muestra las intrface)
- showInterfaceMapping (muestra el mapa de interface y puertos)
- showtable route (muestra tabla de rutas asignadas)
- showtable route ipv4 static (muestra tabla de rutas asignadas)
- tracepath <ip-address>
- traceroute_ethernet AC:60:B6:20:4D:1E level 0 vlan 847 < ping a macaddress por vlan>
- getMOAttribute STN=0,IPInterface=all MTU
- getMOAttribute STN=0,VLANGroup=all depLinkLayer
- getMOAttribute STN=0,EthernetInterface=all -c
- getMOAttribute -c
- getcounters STN=0,EthernetInterface=TCU_3G - 4G - WAN
- gettransactionid
- getTransactionStatus <id>
- getsessionids
- getSWSessionIds

IX. CONCLUSIONES

En el presente documento hemos dejado una guía procedimental para la atención de las fallas recurrentes a nivel de acceso sobre la red móvil (RAN), por cada alarma seleccionada se incluye el cableado o interconexión de elementos involucrados, configuraciones remotas, monitoreo, toma decisiones y el procedimiento de campo a efectuar para restablecer el servicio afectado.

Para que las guías realizadas tengan un aporte significativo dentro de la formación de la Universidad Nacional de Ingenieria es importante que los estudiantes conozcan el modelo NOC – Campo, en este trabajo se planta el desarrollo de las guías procedimentales desde un ámbito del modelo NOC – Campo propio de las empresas operadores de telecomunicaciones el cual consiste en la coordinación de actividades desde una estación remota de monitoreo con el apoyo de herramientas específicas que ayudan a la toman las decisiones para atender eventos en la red junto con el personal de campo que se encargará de efectuar los procedimientos correctivos en hardware en cada sitio celular que presente falla.

Se realizó una investigación documental sobre los estándares de las tecnologías móviles y se dio a conocer la arquitectura física de los dispositivos que conforman una estación base en tecnologías WCDMA y LTE para facilitar la comprensión de su funcionamiento, además de dejar claro que el enfoque fue sobre la red de acceso.

Existen una gran cantidad de fallas posibles que afectan la disponibilidad y calidad del servicio de red móvil, sin embargo nos enfocamos en los cinco grupos de alarmas que se presentan con mayor frecuencia las cuales determinamos mediante datos recabados por un operador de telefonía en Nicaragua durante el primer cuatrimestre del año 2019, siendo los grupos seleccionados: fallas de energía AC, fallas de energía DC, falla en sectores, fallas de diversidad y fallas de Hardware o Software en tarjetas de control de las estaciones base.

El trabajo en general fue diseñado para que los estudiantes de Ingenieria electrónica, telecomunicaciones o carreras a fines que estén interesado en laborar en empresas que ofrecen servicios de telefonía celular tengan una visión amplia del tipo de trabajo que se realiza, desde la perspectiva del NOC y de campo, de modo que puedan elegir de acuerdo a sus intereses profesionales el área donde pretenden desempeñarse. Para las personas que recién inician a laborar en un campo similar al expuesto, le ayudará a enfocarse y entender mejor los procesos técnicos que se atienden por los Ingenieros de monitoreo y campo, mejorando la curva de aprendizaje, es decir, que la capacitación del personal nuevo en las áreas sea más rápida, lo que implicará un beneficio a las empresas de telecomunicaciones.

X. RECOMENDACIONES

El trabajo realizado les servirá a los estudiantes para tener claro el escenario encontrado en la práctica profesional en las empresas que brindan servicio de telefonía celular, sin embargo, una interesante mejora seria el poder establecer convenios con los operadores de telecomunicaciones del país para facilitar Hardware que no esté en producción y montar maquetas para que el estudiante pueda ver de mi primera mano lo explicado en el contenido de este trabajo monográfico o en su defecto brindar accesos con privilegio de bajo nivel y con las restricciones pertinentes al Hardware en operación instalado dentro de la universidad, de modo que, bajo un uso controlado, los estudiantes puedan practicar ciertas fases del monitoreo y detección de posibles fallas en las estaciones base.

Una posible continuidad a este trabajo, puede ser un enfoque en una tecnología móvil que está en etapa de implementación y dando sus primeros pasos en Nicaragua como lo es 5G. Se podría abordar la estructura de la red 5G desde el acceso o incluso profundizar en el Core. También se podrían abordar etapas de la red mencionadas en este trabajo, en las cuales no se profundizo como los son la red Core en sus distintos subsistemas: Core para la conmutación de Datos, Core para la conmutación de circuitos, servicios como Roaming, de modo que el estudiante tenga un conocimiento más amplio de una red celular y pueda decidir acertadamente desde el entendimiento de la red en que área de interés se pueda desempeñar a futuro.

Un posible enfoque para complementar este trabajo seria el desarrollo de herramientas digitales que intenten competir con las herramientas profesionales utilizadas actualmente para el monitoreo de estos elementos basados en direccionamientos IP, para la asignación, control y documentación de fallas de modo que se puedan generar soluciones de bajo costo de posible interés no solo para los operadores de telecomunicaciones, sino también para empresas relacionadas con este rubro.

XI. BIBLIOGRAFÍA

[1] Centeno Zeledón Fátima Hitzzel. "Manual Técnico para la Gestión y Mantenimiento Preventivo de Equipos de RBS". Universidad Nacional de Ingeniería. Nicaragua. Junio 2017. Disponible en:
http://ribuni.uni.edu.ni/1571/

[2] Vanegas Brenes, Juan Carlos y Ramírez García, Ariel Albert (2018) "Sistema de monitoreo de variables externas e internas en gabinetes de macros y micros celdas celulares". Universidad Nacional de Ingeniería. Nicaragua. Noviembre 2018. Disponible en:
http://ribuni.uni.edu.ni/2417/

[3] Telefonía Móvil 2G. Disponible en:
https://www.ecured.cu/Telefon%C3%ADa_m%C3%B3vil_2G

[4] Tecnologías GSM, CDMA, TDMA, GPRS, EDGE, UMTS. Disponible en:
https://www.monografias.com/trabajos75/tecnologias-gsm-cdma-tdma-gprs/tecnologias-gsm-cdma-tdma-gprs2.shtml

[5] Garrido Rodrigo. ¿Qué es la tecnología LTE? Disponible:
https://www.xataka.com.mx/celulares-y-smartphones/que-es-la-tecnologia-lte

[6] MODELO PORTER Y ESTRATEGIAS DE NEGOCIOS DE TELECOMUNICACIONES.
https://core.ac.uk/download/pdf/41798455.pdf

[7] ERICSSON. Disponible en:
https://es.wikipedia.org/wiki/Ericsson

[8] HUAWEI. Disponible en:
https://es.wikipedia.org/wiki/Huawei#Redes_de_telecomunicaciones

[9] Arquitectura de Red Movil 2G. Disponible en:
https://es.slideshare.net/andysarangoveliz/captulo-iv-arquitectura-de-la-red-mvil-2g-gsm

[10] NOKIA. Disponible en:
https://es.wikipedia.org/wiki/Nokia#:~:text=Nokia%20Corporation%20es%20una%20empresa,de%20telecomunicaciones)%20y%20Nokia%20Technologies.

[11] Ficha de Mercado Telefonía Celular. Disponible en:
https://unctadcompal.org/wp-content/uploads/2017/03/NICARAGUA-Ficha-mercado-telefonia-movil-NUEVO.pdf

[12] Panorama de mercado en Nicaragua. Disponible en:
https://www.telesemana.com/panorama-de-mercado/nicaragua/

[13] SISTEMAS DE ESTACIONES BASE. Disponible en:
https://www.researchgate.net/figure/Figura-5-Arquitectura-GSM-21-Sistema-de-Estaciones-Base-BSS-El-sistema-de_fig5_308879041

[14] ARQUITECTURA Y CIFRADO DE SEGUIRDAD EN REDES 3G. Disponible en:
https://empresas.blogthinkbig.com/arquitectura-y-cifrado-de-seguridad-en/

[15] ANALISIS DE LA IMPLEMENTACION DE IUB FULL IP. Disponible en:
https://rdu.iua.edu.ar/bitstream/123456789/402/1/ANALISIS%20DE%20LA%20IMPLEMENTACION%20DE%20IUB%20FULL%20IP.pdf

[16] UMTS TERRESTRIAL RADIO ACCESS NETWORK. Disponible en:
https://es.wikipedia.org/wiki/UMTS_Terrestrial_Radio_Access_Network

[17] SISTEMAS DE TELEFONIA Y COMUNICACIONES MOVILES. Disponible en:
https://mastermoviles.gitbook.io/tecnologias2/sistemas-de-telefonia-y-comunicaciones-moviles

[18] PS CORE NETWORK. Disponible en:
https://telecomstudy18.blogspot.com/2015/04/ps-core-network.html

[19] ARQUITECTURA 4G. Disponible en:
http://rubensm.com/arquitectura-4g/

[20] E-UTRA. Disponible en:
https://en.wikipedia.org/wiki/E-UTRA

[21] PCRF. Disponible en:
https://es.wikipedia.org/wiki/Policy_and_charging_rules_function

[22] Radio Base Station. Disponible en:
https://en.wikipedia.org/wiki/Radio_Base_Station

[23] Radio Base Station RBS. Disponible en:
http://tel3pedia.blogspot.com/2011/11/radio-base-station-rbs.html

[24] Familia de productos RBS3000 Disponible en:
https://silo.tips/download/la-familia-de-productos-rbs-3000-para-sistemas-wcdma

[25] RBS6000 Disponible en:
https://lafibre.info/images/4g/201004_ericsson_rbs6201_lte1800.pdf

[26] Funciones del NOC. Disponible en:
https://telecominfraproject.com/naas-playbook-oandm/

[27] Operation Support System. Disponible en:
https://es.wikipedia.org/wiki/Operations_Support_Systems

[28] Critix App. Disponible en:
https://en.wikipedia.org/wiki/Citrix_Virtual_Apps

[29] Critix Metaframe. Disponible en:
https://www.ciset.es/glosario/420-citrix

[30] NOC Eficiente. Disponible en:
https://qualitynoc.es/cuenta-con-un-noc-eficiente-que-acompane-su-crecimiento/

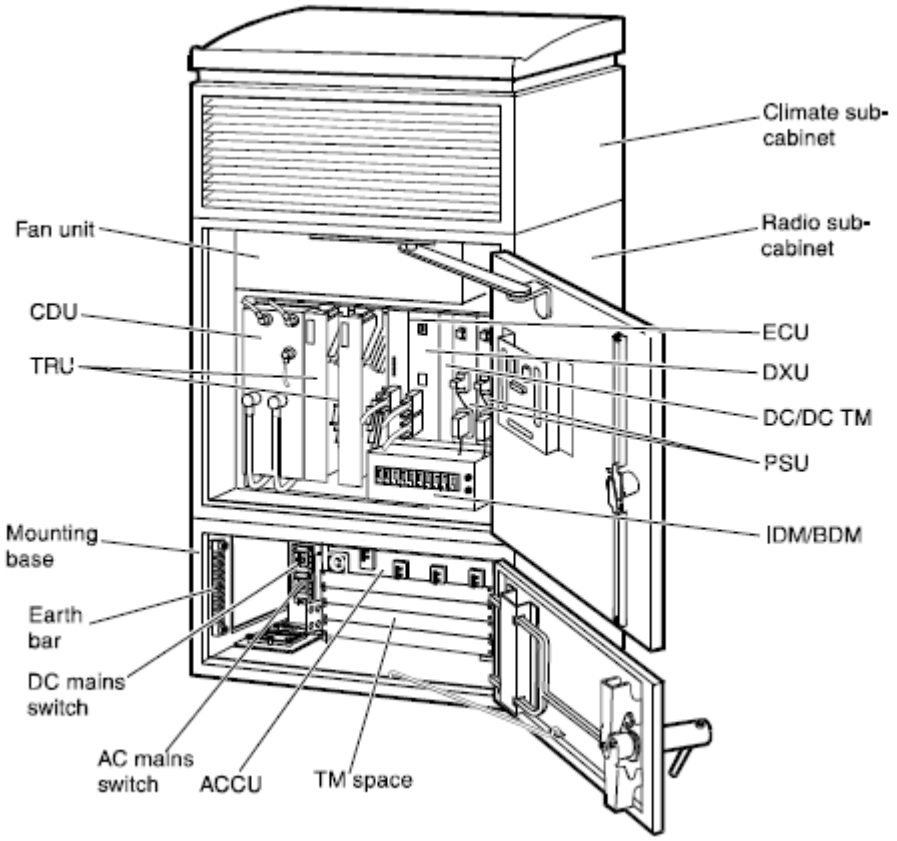
[31] Diseño e implementación de una estación base GSM/UMTS. Disponible en:
https://riunet.upv.es/bitstream/handle/10251/8972/memoria.pdf

XII. ANEXOS

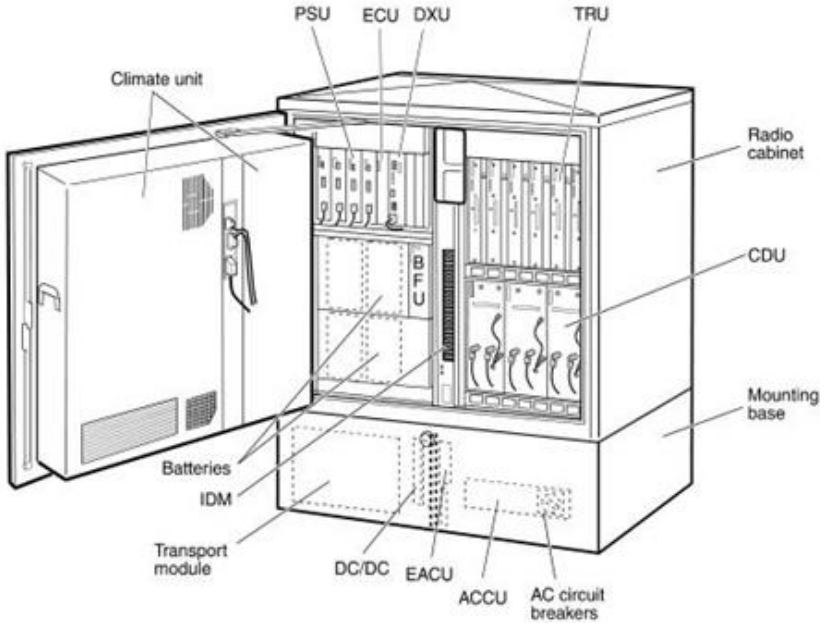
DESCRIPCIONES DE LA SERIE RBS 2000

RBS Type	Location	Max. TRU	Cells	Coverage Type	Dimensions (h-w-d) (mm)	Temperature Range (°C)
RBS 2101	Outdoor	2	1	Macro	1285-705-450	-33...+55
RBS 2102	Outdoor	6	1-3	Macro	1605-1300-760	-33...+45
RBS 2103	Outdoor (GSM 900 only)	6	1-3	Macro	2300-900-795	-33...+35
RBS 2202	Indoor	6	1-3	Macro	1775-600-400	+5...+40
RBS 2301	Indoor/Outdoor	2	1	Micro	535-408-160	-33...+45
RBS 2302	Indoor/Outdoor	2	1	Micro	535-408-170	-33...+45
Maxite	Indoor/Outdoor (GSM 900 only)	2	1	Macro	535-408-160	-33...+45
RBS 2401	Indoor	2	1	Pico	387-510-126	+5…+40

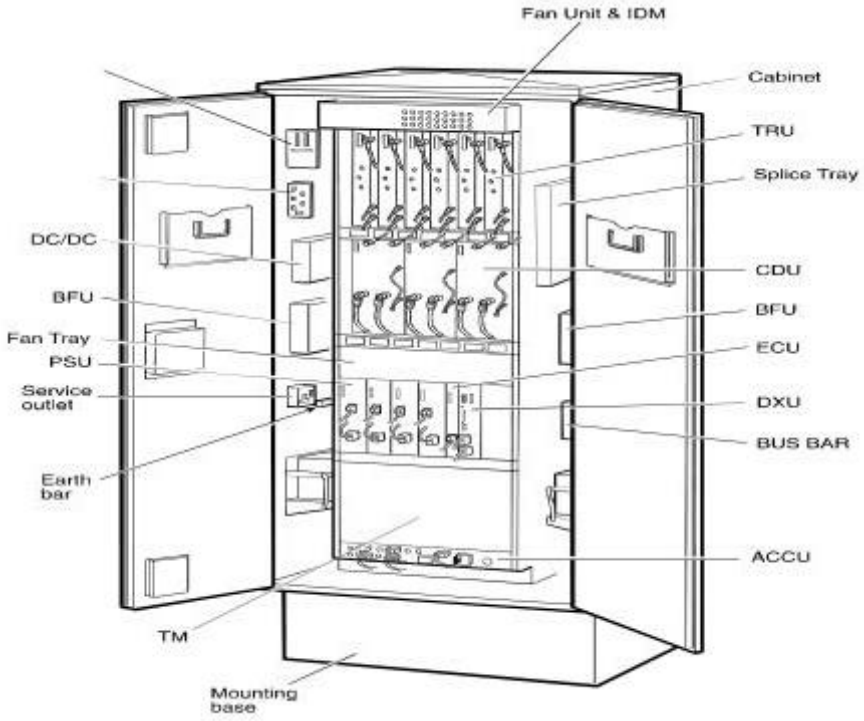
RBS 2101



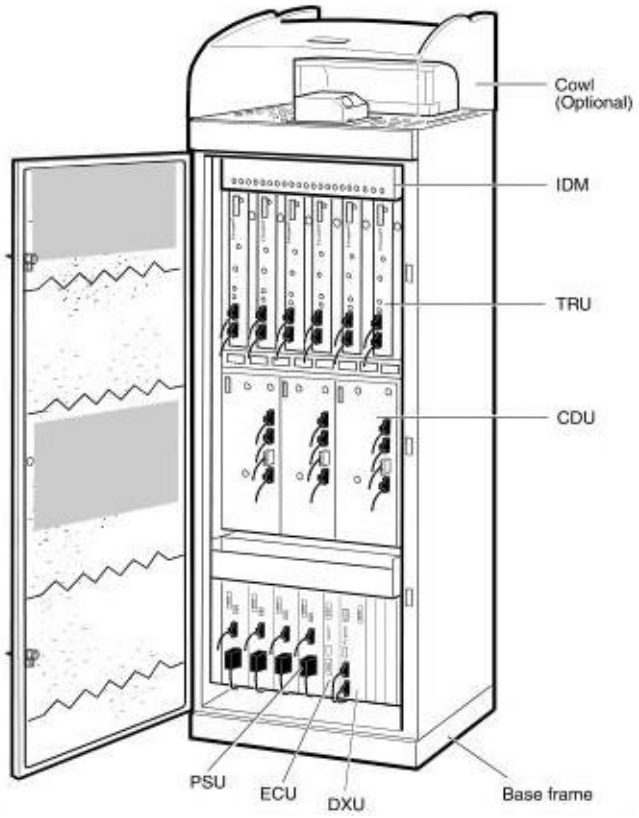
RBS 2102



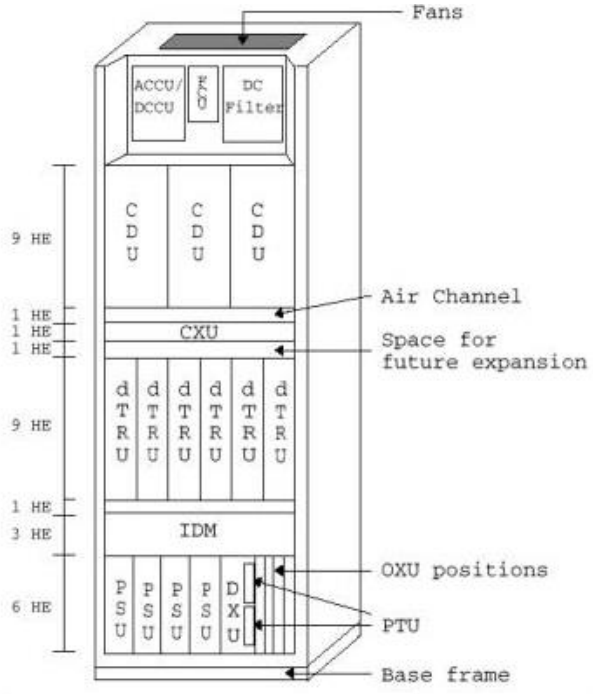
RBS 2103



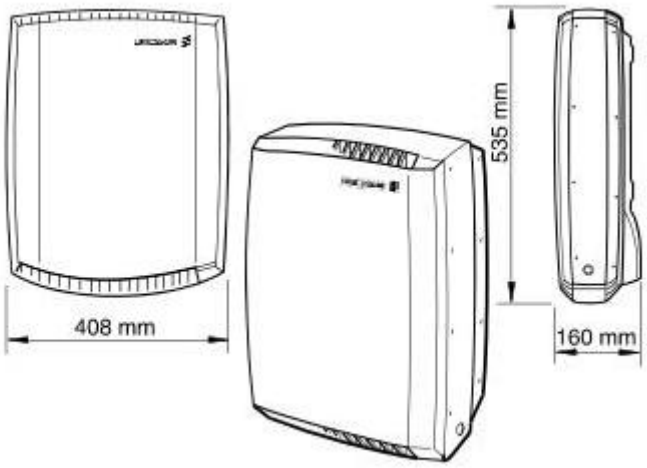
RBS 2202



RBS 2206


Fans
ACCU/ DCCU
FCU
DC Filter
CDU
CDU
CDU
9 HE
1 HE
1 HE
1 HE
Air Channel
CXU
Space for future expansion
dTRU
dTRU
dTRU
dTRU
dTRU
dTRU
9 HE
1 HE
3 HE
IDM
PSU
PSU
PSU
PSU
DXU
OXU positions
PTU
6 HE
Base frame

RBS2302



RBS 3000