UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DETECCIÓN Y SEGUIMIENTO A FALLAS EN RED DE COMUNICACIONES CELULARES DESDE EL CENTRO DE OPERACIONES (NOC)

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero Eléctrico Electrónico

P R E S E N T A

Alfonso de Jesús Enríquez Jiménez

ASESOR DE INFORME

M.C. Edgar Baldemar Aguado Cruz

Ciudad Universitaria, Cd. Mx., 2016

Dedicatoria

A mis padres y todas las personas que me han brindado su apoyo incondicional a lo largo de mi formación profesional

Índice

Capítulo 1

Introducción

Actualmente las empresas de telecomunicaciones utilizan un centro de monitoreo para la detección y solución de fallas en los elementos de su red, este se conoce como Centro de Operaciones de la Red (*NOC*, por sus siglas en inglés).

Un *NOC* se encarga de la detección oportuna de fallas, así como del proceso de seguimiento hasta obtener solución al problema. La duración de una falla repercute en los servicios que se entregan a los clientes y para la compañía se refleja en pérdidas monetarias y en desconfianza por parte del usuario de la red.

La función primordial es la detección de fallas en la red, particularmente en los elementos que la conforman, equipos de transporte de datos, *routers*, *switches*, fibras ópticas, antenas, etc. Ésta se realiza por medio del monitoreo constante de alarmas en *softwares* especializados que gestionan los distintos elementos.

El monitoreo lo realiza personal de primer nivel o "*Front Office*" y su tarea es detectar fallas y asignarlas al siguiente nivel o "*Back Office*", este se encarga de realizar un análisis profundo de la falla mediante la revisión de las alarmas, registro de eventos (conocidos como *logs*), conexión remota a equipos, revisión de parámetros (energía, potencias, configuración, temperatura, etc.)

El *back office* tiene la responsabilidad de analizar la falla para determinar cuál es su solución y en caso de depender de terceras áreas lo canaliza para su atención. La falla

puede ser atendida por ingenieros de campo, soporte especializado, ingenieros de centrales y proveedores de servicios.

1.1 Objetivo

Describiré los procesos que se siguen en un *NOC* para el seguimiento a fallas, así como los distintos tipos de análisis y pruebas para determinar la solución al problema. También describiré la relación que existe entre el *NOC* y las distintas áreas de ingeniería que forman parte de la empresa.

Al formar parte del personal de segundo nivel es fundamental aplicar toda la experiencia y conocimientos que he adquirido en la empresa por tres años. Las áreas de conocimientos son diversas, desde la instalación de *software* hasta el análisis de fallas en elementos eléctricos, ópticos, de configuración en *routers* y *switches*, hasta fallas que no son imputables a la empresa (lluvias, temblores, apagones, vandalismo, etc.)

Capítulo 2

Descripción de la empresa

La empresa en la que laboro forma parte de la industria de las comunicaciones celulares, tiene presencia internacional, y se enfoca en la venta de servicios de telefonía móvil. En México cuenta con red propia para brindar comunicación a lo largo del país y la infraestructura va creciendo cada día.

Se tiene como propósito brindar servicios de calidad y gran disponibilidad a los usuarios finales. El trabajo de la empresa es mantener una red estable a través de diversos procesos de ingeniería, como la implementación y diseño para un crecimiento óptimo, el mantenimiento correctivo y preventivo, el soporte a equipos para corrección de fallas y por último el monitoreo constante de la red en busca de fallas y debilidades.

Al ser una empresa de grandes proporciones, además de ofrecer servicios de telefonía móvil, también renta parte de su infraestructura a empresas más pequeñas para tener comunicación con redes que se encuentran a largas distancias o bien para lograr la conexión a la nube de Internet.

Es fundamental el trabajo de la ingeniería para la empresa, y a pesar de que se tiene una red tan robusta, siempre se busca el crecimiento y desarrollo de nuevas tecnologías. En México se tiene planeado un gran crecimiento en los próximos años, lo que se reflejaría en la creación de gran cantidad de empleos para profesionistas.

2.1 Visión de la empresa

En México no se tienen permitidos los monopolios, sin embargo existen empresas que abarcan la mayoría del mercado, y a las empresas más pequeñas o emergentes les es imposible hacerles competencia, por lo que el usuario final no tiene opciones para elegir entre un proveedor u otro, esto los lleva a aceptar los precios impuestos por las compañías aun cuando sean excesivos y el servicio sea de mala calidad.

En años recientes se han incorporado más empresas a este ramo de las comunicaciones, se ha logrado una competencia más pareja entre las empresas que ofrecen estos servicios. El usuario ha obtenido más beneficios, ya que los precios bajan mientras que el servicio celular es más rápido y de mayor calidad.

La empresa planea elevar aún más la competencia y brindar a los usuarios una mejor experiencia, otorgando servicios de las tecnologías celulares más avanzadas como el servicio de LTE ($4G$) así como una mayor cobertura cubriendo todo el territorio mexicano. Además, se tiene una mayor disponibilidad en sus servicios, es decir que una falla en la red es lo más transparente posible para los usuarios, esto se logra creciendo la red y a su vez implementado redundancias (respaldo) en los servicios.

La inversión es una de las más grandes en México. Apostando a ser uno de los proveedores de servicios celulares más grandes del país.

2.2 Organización del *NOC*

La organización de las áreas puede variar de acuerdo a las necesidades de la empresa. En México existen empresas que cuentan con uno o varios *NOC´*s. Otras rentan este servicio a terceras compañías, todas ellas venden sus equipos, y a su vez ofrecen servicios de diseño, instalación, operación, mantenimiento y monitoreo.

Dependiendo de la cantidad o el tipo de servicios que la empresa ofrece a sus usuarios, se forman las distintas áreas. Por ejemplo una empresa que ofrece el servicio de telefonía, Internet y televisión por cable, probablemente tenga un área encargada de monitorear cada uno de los servicios por separado.

Nuestro *NOC* se encarga del monitoreo y atención a las fallas de la red, también compra servicios de monitoreo a otras empresas, y en ocasiones toma el papel de proveedor. Al tener el rol de cliente y proveedor mis funciones como *NOC* se expanden a solucionar no solo fallas internas sino de terceros.

Las diversas áreas y puestos de un *NOC* se crean a partir de jerarquías y/o niveles, con tareas específicas asignadas a cada uno de ellos. A continuación se listan estos niveles de menor a mayor rango.

2.2.1 Nivel 1. Front Office (Monitoreo)

El nivel 1 llamado *front office* o mesa de monitoreo, está pendiente de las alarmas y desempeño de los equipos de la red, ya que son indicadores de una anomalía en los equipos. Entre sus tareas se encuentran:

- Monitorear

- Crear folios de atención
- Reunir información del impacto de la falla
- Catalogar la falla, como menor, mayor, crítico o emergencia
- Asignar los folios de falla al Nivel 2
- Reportes

2.2.2 Nivel 2. Back Office (Análisis y seguimiento a fallas)

En este nivel me encuentro actualmente laborando y mis actividades son las descritas en el apartado de "Funciones desempeñadas". A continuación se resumen en forma de lista:

- Análisis de las alarmas descritas en los folios asignados
- Revisión de los equipos de manera remota
- Discernir el tipo de falla y aplicar solución de ser posible
- Asignar folio al área de atención en caso de no poder ser resuelta internamente
- Tener comunicación constante con el área asignada a la solución
- Brindar soporte remoto a los ingenieros implicados
- Validación de la solución y término de la falla

2.2.3 Nivel 3. Coordinación del área (Supervisión)

- Los coordinadores de área o Supervisores, asignan tareas a los ingenieros a su cargo y vigilan que todo se realice de manera correcta y en tiempo. Agiliza el manejo y pronta solución de las fallas.

2.2.4 Nivel 4. Gerencia

Encargado de gestionar a las diversas áreas y administrar los recursos dentro del *NOC* (personal, equipo, mobiliario, instalaciones, etc.). También agiliza el manejo y pronta solución de las fallas, generalmente a fallas mayores y críticas.

2.2.5 Nivel 5. Dirección

Es la cara del *NOC*. Se encarga del ámbito administrativo, como la contratación de nuevos recursos, adquisición de nuevas herramientas y equipo, etc. Es el nivel más alto del esquema jerárquico del *NOC (Figura 1)*.

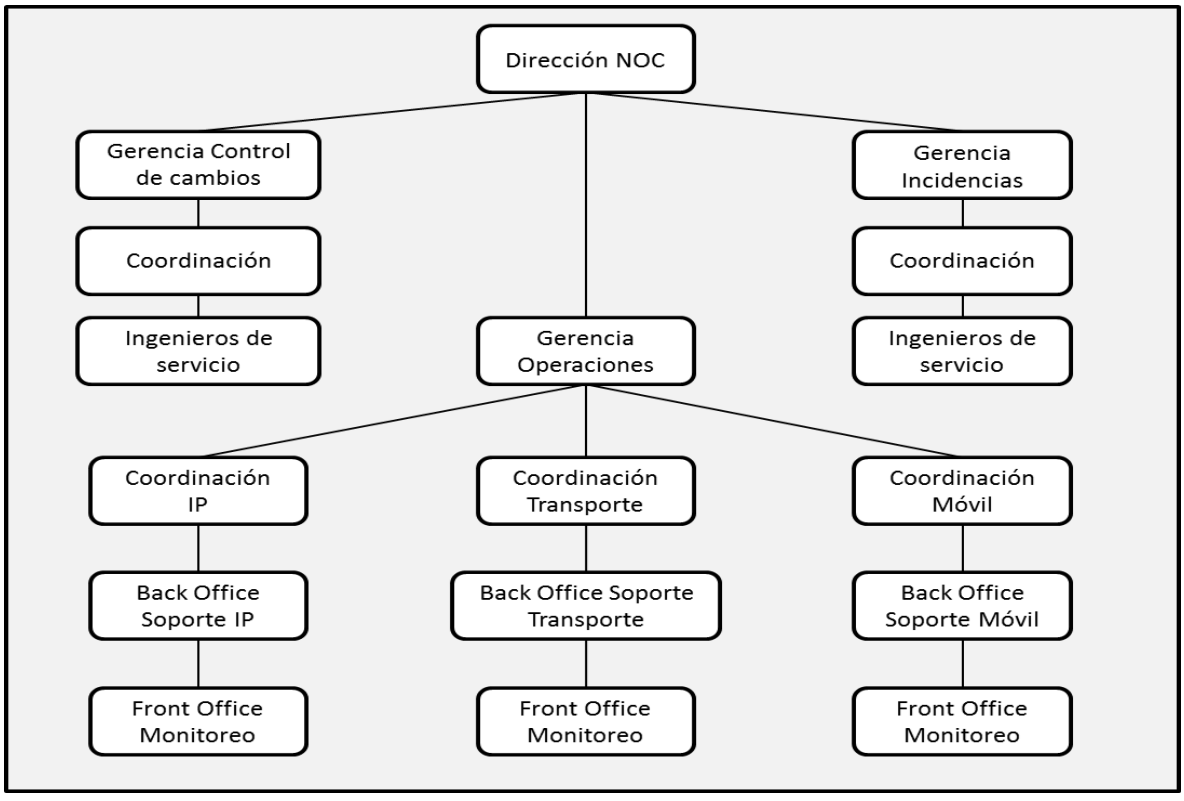

Figura 1. Esquema jerárquico. Se muestra un ejemplo básico de la estructura jerárquica de un NOC

Capítulo 3

Puesto desempeñado

En el mes de enero del 2013 ingresé al *NOC* con el puesto de Ingeniero de Monitoreo (Nivel 1) con la función de monitorear y detectar fallas a través de alarmas en equipos de transporte *DWDM* y equipos de redes *IP* como *routers* y *switches*.

En el año 2014 obtuve el ascenso al "*Back Office*". Actualmente se me asignó el puesto de "*Senior Back Office*" como especialista en fallas de la red *IP* y de transporte (*IP CORE*), es decir se me asignan las fallas relacionadas con los equipos de transmisión e *IP* que comentaré más adelante. Actualmente estos equipos se encuentran a lo largo del país y son el núcleo (conocido como *CORE*) de la red, por lo que son de vital importancia para la correcta operación de la operación a nivel nacional.

3.1 Instalación y configuración de software de monitoreo

Se asegura un correcto y eficaz monitoreo por parte de los ingenieros de primer nivel, que deben ser precisos y veloces al momento de detectar una falla, ya que se busca el menor intervalo de tiempo desde que se originó la falla hasta que se da solución.

Para el monitoreo se utilizan herramientas como PRTG y ORION, también es común que cada elemento de la red como un *router* tenga un gestor de monitoreo propio del fabricante. Estos gestores se basan en el protocolo SNMP para establecer comunicación

entre un servidor central y los distintos equipos de la red *(figura 2).* A su vez un operador se conecta al servidor central por *http* desde un buscador web.

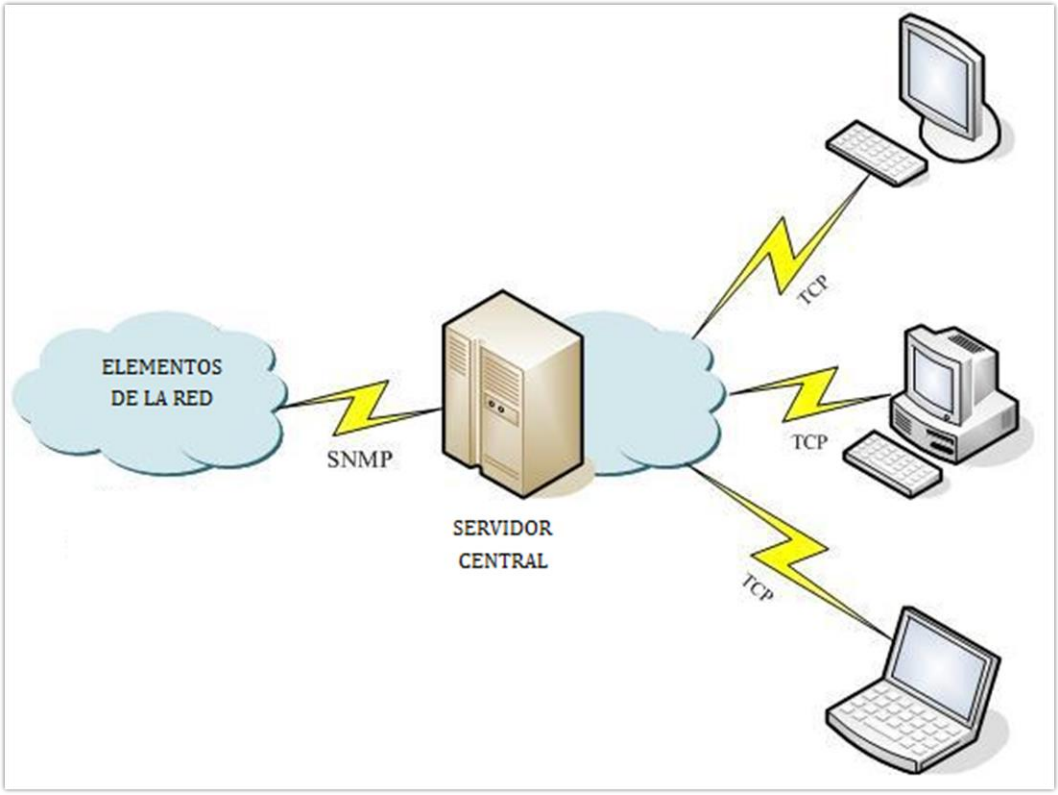

Figura 2. Diagrama de conexiones para el monitoreo de la red

El protocolo *SNMP* se establece por el puerto lógico 161 (en algunos casos el 162) en los *routers* se habilita el protocolo *SNMPv2c* con la IP del servidor al que enviará datos y una comunidad que establece que tipo de comunicación se tendrá con el equipo (lectura o escritura). En el servidor central se instala el *software* (PRTG, ORION, etc.) y se dan de alta las direcciones IP que quiere monitorear, se establece la comunidad (tiene que ser la misma que en el *router)* y por último se da de alta el tipo de información que deseamos obtener del equipo, esto se realiza por medio de sensores configurados con una Base de Información de Administración (*MIB,* por sus siglas en inglés)

La *MIB* es una colección de información ordenada jerárquicamente en forma de árbol (*figura 3)* se puede consultar información específica de una rama por medio de un identificador *OID (Object ID).* Contiene estados de CPU, memoria RAM, capacidad de disco duro, temperatura, estado de los puertos, etc.

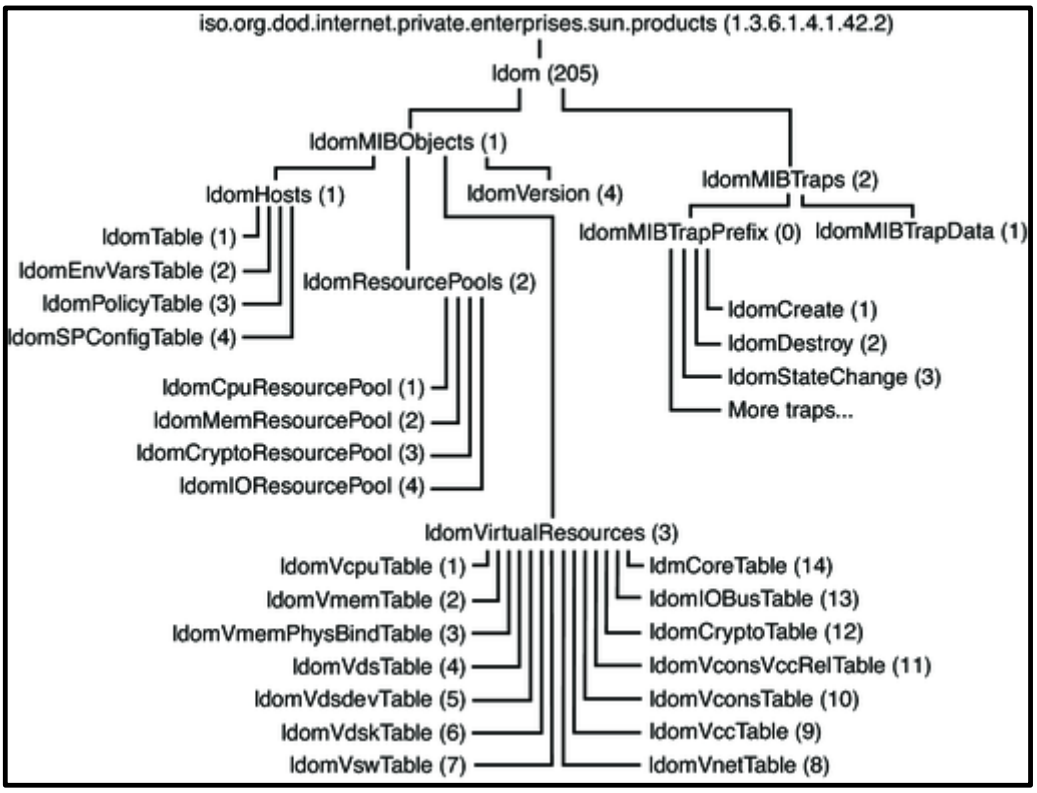

Figura 3. Ejemplo de la estructura de una MIB. Al final se obtiene un OID compuesto por números separados de puntos, que indican la jerarquía y el objeto a ser consultado.

3.2 Recepción y análisis de las fallas

Por medio de un sistema de folios se asigna la falla detectada a las diversas áreas para su revisión. Los folios asignados a mi área (IP CORE) son analizados y catalogados por el tipo de falla, el elemento con la anomalía, el servicio y la ciudad o región que se ve impactado, la criticidad del problema, y lo más importante la solución que se aplicará,

Más adelante se detallaran los tipos de falla más comunes y el análisis o *troubleshooting* que se aplica para determinar la causa raíz del problema y el método para su solución.

3.3 Asignación de fallas a otras áreas

Si la solución no puede realizarse desde el *NOC*, se designa a otra área, por ejemplo una falla en elementos eléctricos solo puede solucionarse con personal en sitio, por lo tanto se asigna la solución a un ingeniero de campo.

3.4 Seguimiento a fallas

Una vez asignado el caso a otra área, mi responsabilidad es comunicarme con el ingeniero implicado para determinar el tiempo de solución y en caso de ser necesario orientarlo de manera remota sobre las acciones a seguir, también es mi deber proporcionarle todas las facilidades que requiera (llamadas, accesos a las radio bases, información sobre equipos, material de repuesto, etc.) Todas las áreas tienen un tiempo de respuesta para realizar las acciones que crean pertinentes y así encontrar una solución, una vez que se excede este tiempo, realizo la asignación del caso a los siguientes niveles del área asignada (supervisores, gerentes y directores).

3.5 Validación de la solución

Una vez que nos reportan la solución de la falla necesito revisar de manera remota que efectivamente los equipos se encuentren operando correctamente, reviso que los

servicios reestablecieron, y la última validación es que las alarmas que dispararon el folio hayan desaparecido en su totalidad. En caso de que alguna validación no haya sido satisfactoria se repite el proceso.

3.6 Control de ventanas de mantenimiento

La ventana de mantenimiento es un periodo de tiempo en el que se acuerda trabajar en cierto equipo, región, servicio, etc. con el fin de incrementar la red, aplicar mejoras o dar mantenimiento, generalmente son en horarios nocturnos en los que el impacto a los servicios es mínimo. Mi función en este rol es llevar un control de las actividades, autorizar a los ingenieros sus trabajos o bien rechazarlos dependiendo de si cumplen o no con las normas establecidas por la empresa.

3.7 Reportes

Es necesario que realice reportes de las fallas críticas y de aquellas que se requieran por parte de directivos. También realizo reportes semanales de la tendencia de la red en cuanto a fallas detectadas. Realizo un reporte de utilización de tráfico de los enlaces de alta capacidad, esto con el fin de determinar si es necesario un crecimiento en la red, como la instalación de nuevos equipo o crear nuevas rutas de fibra óptica.

Capítulo 4

Tipos de fallas y análisis para su solución

En la empresa se manejan varias marcas de equipos *routers* y *switches*, la teoría en cuanto a su configuración y funcionamiento es la misma, sin embargo el análisis y revisión de los equipos cambia de un equipo a otro por los comandos que se utilizan y que son propios de las marcas o del Sistema Operativo que utilizan.

La revisión se hace de manera remota. Para el monitoreo utilizamos los protocolos *SNMP* e *ICMP*, en cuanto a la revisión se utiliza el *SSH* y *Telnet* con herramientas como el Putty y SecureCRT.

En este informe no incluiré los comandos ejecutados ya que es una lista muy extensa y como mencioné antes, cambian de una marca a otra. Sin embargo los protocolos de ruteo son estandarizados, y permiten la comunicación entre equipos aun cuando se trate de fabricantes distintos.

4.1 Corte de fibra óptica

Es la falla más común en la red. Las fibras son la conexión física entre dos equipos y forman los enlaces de toda la red. Un equipo *router* o *switch* de la red central (*CORE)* tienen tarjetas con puertos de capacidades que van desde 100Mbps hasta 100Gbps y aquellos destinados a la comunicación con fibra óptica se equipan con módulos ópticos (SFP o GBIC) que convierten la señal eléctrica proveniente del router a una señal óptica.

Una vez que la señal es convertida a óptica se conecta una fibra corta (alrededor de 10 a 30 metros) llamada *jumper* que conecta a un Distribuidor de Fibra Óptica (DFO) y es de aquí donde se saca para su transporte. Existen enlaces de fibras ópticas de 1km hasta 40km dentro de la red. La fibra se instala en postes (fibra aérea) o dentro de conductos bajo tierra (fibra canalizada o subterránea)

Hay muchos factores que provocan el corte de una fibra:

- Caída de postes
- Excavaciones
- Accidentes con camiones de gran tamaño
- Vandalismo
- Incendios
- Degradación natural de la fibra, por dobleces, manipulación o desgaste.

La forma en que diagnóstico una falla por corte es la siguiente: Se revisan los niveles de potencias en los puertos de los equipos afectados, si la potencia o niveles de luz en los equipos es igual a cero, se determina que el enlace está abierto en algún punto y es necesario realizar la revisión física, en este caso se envía a personal de planta externa, que es un grupo de ingenieros con equipo especial *(figura 4)* para realizar mediciones y detectar en qué punto está la falla.

Para las pruebas se utiliza un equipo llamado *OTDR (Optical Time Domain Reflectometer)* para obtener una representación visual de las características de atenuación de una fibra óptica a lo largo de toda su longitud. El ensayo mediante el *OTDR* es el único método disponible para determinar la localización exacta de las

roturas de la fibra óptica en una instalación de cable óptico ya instalado y cuyo recubrimiento externo no presenta anomalías visibles.

Cuando está operando el *OTDR* envía un corto impulso de luz a través de la fibra y mide el tiempo requerido para que los impulsos reflejados retornen de nuevo al *OTDR*. Conociendo el índice de refracción y el tiempo requerido para que lleguen las reflexiones, el *OTDR* calcula la distancia recorrida del impulso de la luz reflejada. De esta manera se conoce a que distancia del punto de medición se encuentra la falla.

Figura 4. Equipo OTDR para medición de potencias y estimación de distancias donde se pierde la señal.

Una vez localizado el corte de la fibra, se procede al empalme de la misma, existen dos tipos de empalme, por fusión y mecánico. El empalme por fusión como su nombre lo indica suelda las fibras fundiéndolas con ayuda de una máquina empalmadora. El empalme mecánico consiste en alinear las fibras y utilizar un adhesivo especial, este es provisional y no es muy conveniente. Siempre que se realiza un empalme se provoca una atenuación de potencia (aproximadamente entre 0.3 y 0.5 dB´s), al tener una fibra con varios empalmes, se recomienda remplazar el tramo en vez de empalmarlo.

4.2 Falla en algún elemento del equipo

Los equipos routers son modulares y escalables. Es un chasis que se compone de diversos elementos como tarjetas, fuentes de poder, ventiladores, módulos ópticos, etc. Esto permite realizar el cambio de algún elemento sin afectar en su totalidad al equipo, así mismo permite el incremento de sus capacidades remplazando alguno de estos módulos por nuevos elementos.

Los principales elementos que integran los equipos son los siguientes:

- Tarjetas Ethernet
- Tarjetas procesadoras
- Fuentes de poder
- Ventiladores
- Tarjetas de almacenamiento de información

La falla en alguno de los elementos es detectado por medio de alarmas que indican una anomalía en el *hardware*. El primer paso es conectarse de manera remota por *SSH* o *Telnet* a la IP configurada en el equipo *(figura 5)*.

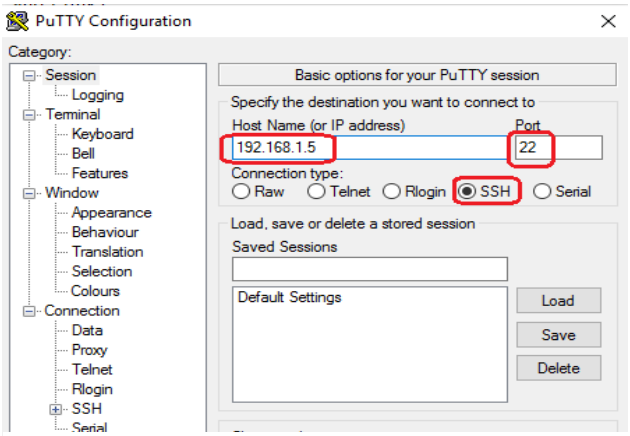

Figura 5. Conexión al equipo, se utiliza el host name o la IP que identifica al equipo dentro de la red, y se elige el tipo de conexión, SSH o Telnet

Una vez dentro del equipo lo primero que hago es comprobar las alarmas, una vez confirmada la falla a través de algunos comandos se analiza si es posible la solución remota con la aplicación de ciertos comandos como un *reset* del dispositivo, o bien si es necesario la revisión física.

Para la revisión física se envían a ingenieros de campo a los equipos para que revisen todas las conexiones, una de las principales fallas son falsos contactos entre las fibras y los puertos, las tarjetas con el chasis, las fuentes de poder con el cableado eléctrico, etc.

Si en la revisión no se encontraron fallas, los elementos tienen que ser reemplazados y es necesario hacer la solicitud a los almacenes para su reemplazo. Si las tarjetas o equipos cuentan con garantía del proveedor me encargo del envío a estas empresas para su reparación.

Algunos elementos son críticos para el funcionamiento de los equipos, como las fuentes de poder y las tarjetas procesadoras, así como las tarjetas que tengan enlaces importantes. La mayor parte de la red tiene redundancia o respaldo de todos sus elementos, por ejemplo un equipo tiene dos o más fuentes de poder, dos tarjetas controladoras y uno o más enlaces que permiten la comunicación con la red. Sin embargo algunos elementos no lo tienen y las fallas son críticas ya que afectan a los servicios que cuelgan de estos equipos. La solución es la misma sin embargo se toman en cuenta como vulnerabilidades de la red y para tener en un futuro algún crecimiento y mejora.

4.3 Fallas de energía

Estas fallas son muy comunes en cortes de energía por parte de CFE o por fallas en los elementos eléctricos, para mí como *NOC* simplemente se genera una alarma de energía y la revisión se hace por parte de ingenieros de campo, de mi parte no realizo más que la asignación de la falla y la validación una vez que se reporte el fin de actividades, ya que perdemos la comunicación con el equipo y es imposible acceder de manera remota.

4.4 Fallas de ruteo

Las redes actuales utilizan la comunicación por protocolos de ruteo en donde se identifican a los equipos por su dirección IP. Básicamente se construyen caminos lógicos conocidos como rutas entre los dispositivos que permiten el direccionamiento de paquetes de datos entre una fuente y un destino.

Cuando se pierde la comunicación con un dispositivo se puede imputar a las fallas mencionadas anteriormente, si no aplica ninguna de ellas entonces se procede a revisar las rutas lógicas.

Existen varias topologías físicas para las redes IP las más comunes se listan en la figura 6, en ellas se observa cómo se conectan uno con otro creando una red. La conexión física es importante, pero el punto fundamental de los *routers* son las redes lógicas que crea, cada elemento genera una tabla de ruteo donde se listan las direcciones IP, la forma (protocolo) y el camino que toma para lograr la comunicación. Estas conexiones lógicas permiten que *routers* que se ubican en distintos puntos de la red se comuniquen sin ser necesaria una conexión directa.

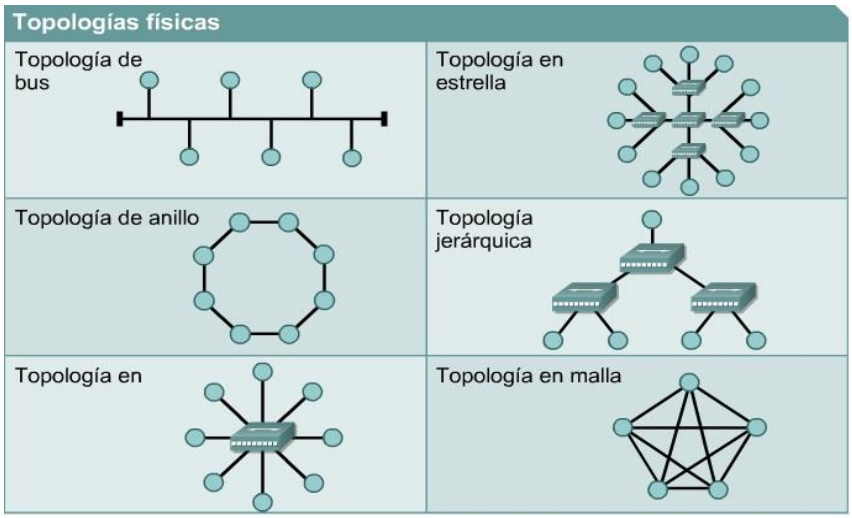

Figura 6. Topologías físicas.

Los protocolos utilizados se dividen en dos grupos importantes *IGP (Internal Gateway Protocol)* y *EGP (Exterior Gateway Protocol).* El *IGP* se utiliza en redes que están bajo la misma administración es decir en el mismo sistema autónomo, por lo general redes corporativas de pequeño y mediano tamaño. Y el *EGP* que se utiliza para comunicar redes de diferente sistema autónomo, por ejemplo en redes de gran tamaño o redes de distintas empresas. Estos grupos contienen a su vez varios protocolos:

- *IGP*:
    - *OSPF*
    - *RIP*
    - *IS-IS*
    - *IGRP*
- *EGP*
    - *BGP*

Una falla de este tipo se deriva de la mala configuración de los equipos y ruteo por parte de las áreas de implementación y soporte. Actualmente se están llevando a cabo una gran cantidad de implementaciones y configuraciones en la red debido al plan de crecimiento, sin embargo esto puede traer fallas a la red, ya que se pueden configurar equipos de forma errónea y provocar fallas por utilizar direcciones IP que ya están en uso (en esta red se utilizan miles de direcciones IP por lo que la administración de las mismas es complicada), también se puede borrar configuraciones por equivocación.

Estas fallas son las más complicadas de detectar según mi experiencia, ya que no tenemos alarmas precisas de donde se originan, y es necesario que revise todos los elementos y configuraciones de los equipos donde se reporta falla en servicio.

El análisis se hace en conjunto con ingenieros de soporte de los equipos y en ocasiones con el proveedor, se revisa que el ruteo de los equipos se encuentre bien configurado, así como los servicios y revisar que no falte nada esencial para su buen funcionamiento.

Los equipos tienen una configuración de hasta mil o más líneas de programación, y los logs de fallas son de hasta 500 o más por minuto. La gran cantidad de información generada dificulta y atrasa la solución. En este punto la experiencia previa es fundamental para realizar el *troubleshooting*.

4.5 Fallas por ventanas de mantenimiento

Las ventana de mantenimiento son un lapso de tiempo para hacer modificaciones en la red, implementar nuevos servicios, o llevar a cabo mantenimiento de equipos. Una

falla derivada de una ventana de mantenimiento es muy probable por el hecho de que se tocan elementos críticos de la red.

Una vez que un Ingeniero me reporta que trabajará con un equipo es esencial que yo los mantenga en observación para evitar que cometan errores y deriven en problemas. También mantengo a los ingenieros dentro del lapso de tiempo destinado para las actividades. Una vez que se acaba el tiempo y no finalizaron sus actividades o si tuvieron alguna falla, les solicitó que realicen un *rollback* (regresen todo al estado inicial) que significa regresar conexiones, quitar configuración realizada, desinstalar software, etc.

Capítulo 5

Participación profesional en la empresa

Mi posición dentro de la empresa es de Ingeniero del *NOC* nivel 2 o *Back Office*, de acuerdo a las funciones que desempeño y que anteriormente mencioné las llevo a cabo de manera exitosa gracias a la experiencia adquirida y los conocimientos durante mi preparación en la carrera de Ingeniería.

Todos los servicios brindados por la empresa tienen una red en común, conocida como la red *CORE* o red Central y es la columna vertebral o del inglés conocido como el *backbone*. Específicamente esta red es de la que yo me encargo a nivel *NOC* asegurando la disponibilidad y la solución a las fallas. Esta red transporta y procesa toda la información generada a nivel nacional, los equipos que se utilizan son los más robustos y de mayor capacidad en toda la red. Generalmente estos equipos se instalan en puntos estratégicos del país; en México es conocido que las ciudades más importantes son el D.F., Monterrey y Guadalajara, por lo que es común que las compañías tengan presencia en estos lugares.

Los equipos en la red Central son generalmente *routers* y *switches* de gran capacidad y equipos de transporte como *DWDM*, ellos se comunican por medio de enlaces de fibra óptica. De acuerdo a lo anterior mi área de trabajo se enfoca en los conocimientos de redes IP y de transporte por medios ópticos, además de los elementos eléctricos que se encuentran en los sitios donde se instalan estos equipos. Debido a que es la red más

importante de la compañía, es necesario no solo contar con los conocimientos antes descritos, sino con las tecnologías y las redes finales de los clientes y usuarios.

Los equipos de la red se encuentran distribuidos a través de todo el país, sin embargo al ser parte del *NOC*, no dispongo de contacto físico con los dispositivos, pero sí de conexión remota a ellos. Esta comunicación remota se realiza por medio de protocolos IP.

Tengo comunicación constante con los ingenieros de campo, para la revisión física de los equipos. Pero no todas las fallas son directamente en los equipos, la mayoría puede ser solucionada de manera remota y damos solución al 70% de las fallas de acuerdo a los conteos de folios que atendemos.

Mi desarrollo en la empresa a lo largo de tres años de labor ha sido positivo y lleno de éxitos en el ámbito profesional, iniciando con los ascensos y el puesto fijo dentro de la empresa, así como el enriquecimiento de conocimientos a través de los cursos que la compañía nos proporciona.

Resultados

La estancia en esta empresa me ha aportado una gran cantidad de conocimientos, así mismo me tengo la oportunidad de aplicar los conocimientos que adquirí durante mi preparación profesional, en las asignaturas de comunicaciones electrónicas, electrónica digital, sistemas eléctricos de potencia y las materias donde es vital realizar algún tipo de programación, como microprocesadores y microcontroladores, computación y programación para ingenieros, etc.

Otra fuente de conocimientos importante es la experiencia de trabajos anteriores. Laboré durante 8 meses en el área de radiofrecuencia y microondas, con cursos y entrenamiento en tecnologías celulares como 2G, 3G y 4G (GSM, UMTS y LTE), también en equipos de microondas y antenas.

Considero que mi papel dentro de la empresa es importante en la solución de las fallas de la red, debido a la relevancia de los equipos que manejo y de los cuales como se mencionó son la columna de la red nacional. En la empresa he sido reconocido por mi desempeño, otorgándome puestos más importantes. Inicie como Ingeniero de nivel 1 o de monitoreo, después de un año fui ascendido a nivel 2, y este año obtuve el reconocimiento como especialista con el puesto de “Senior Back Office”.

Conclusiones

Por mi experiencia personal puedo decir que este trabajo requiere conocimientos adquiridos en la preparación profesional (Universidad), básicamente en temas relacionados a las comunicaciones electrónicas. Cabe resaltar que el plan de la carrera Ingeniería Eléctrica Electrónica es muy amplio y un estudiante de esta carrera está capacitado para laborar en diversos campos, desde el enfoque eléctrico, electrónico, control, área biomédica, telecomunicaciones, sistemas energéticos, etc. En este empleo me he enfocado en desarrollar y ejercer lo aprendido en asignaturas como son comunicaciones electrónicas, análisis de sistemas y señales, programación, amplificadores, microcontroladores, por contar las más importantes.

Siguiendo en importancia la experiencia laboral y por último los cursos y la certificación CCNA que actualmente tengo. La conclusión a la que he llegado es que un ingeniero es fácilmente adaptable a cualquier área de la Ingeniería, ya que más que el conocimiento adquirido han desarrollado una habilidad para enfrentar y resolver problemas de cualquier tipo.

Glosario

2G. Tecnología para la comunicación celular enfocada en la conmutación de paquetes de voz, conocida también como GSM.

3G. Tecnología celular conocida como UMTS y evolución de GSM, enfocada a la transmisión de datos.

4G. Evolución y última tecnología en el mercado celular conocida como LTE y con mayor capacidad de transmisión y recepción de datos móviles.

AT&T. Empresa de Telecomunicaciones con presencia Internacional. Del inglés American Telephone and Telegraph.

Call Center. Centro de atención a los usuarios sobre el servicio proporcionado.

DWDM. Del Inglés Dense Wavelength Division Multiplexing. Equipo cuya función consiste en multiplexar una gran cantidad de señales por un solo enlace y asi se reduce la cantidad de enlaces de fibra a instalar.

DFO. Distribuidor de Fibra Óptica. Es un equipo al que llegan todas las fibras de una instalación y las saca por una sola fibra de varios hilos.

Ethernet. Es un estándar para la transmisión de datos en una red

GBIC. Gigabit Interface Converter. Convertidor de señales de eléctricas a ópticas y visceversa.

IP. Internet Protocol. Estándar de comunicación de redes de datos, utilizado en el modelo OSI de Telecomunicaciones

ICMP. Internet Control Message Protocol. Protocolo para la detección de errores en la comunicación IP.

LAN. Local Area Network. Cualquier red local

NOC. Network Operation Center. Centro de monitoreo, detección y seguimiento a fallas en la red.

OLT. Optical Line Terminal. Equipos utilizados para distribuir servicios que se transmiten por fibra óptica.

ONT. Optical Network Terminal. Equipos que conectan de OLT´s y llevan el servicio al usuario final, por ejemplo un módem puede tomar el papel de ONT.

SFP. Small form-factor pluggable transceptor. Realiza la misma función que un GBIC

SNMP. Simple Network Management Protocol. Permite la comunicación e intercambio de información entre dos equipos, utlizado principalmente en los gestores de monitoreo.

SSH. Secure Shell. Es un protocolo que permite la comunicación remota con un equipo por medio de una dirección IP, hostname, usuario y contraseña.

Telnet. Realiza la misma función que el SSH, sin embargo es menos utilizado por tener más vulnerabilidades en la red.

UTP. Unshielded Twisted Pair. Cable de red conocido por ser el más utilizado en las instalaciones de red caseras o redes locales entre computadoras.

Bibliografía:

Hundley, Kent.. (2009). Alcatel-Lucent Scalable IP Network Self-Study Guide. Indianapolis, USA: Wiley Publishing, Inc..

Cevallos, D., Paredes, M., & Pilicita, A.. (2015). ¿QUÉ ES LA TECNOLOGIA NOC?. Noviembre 25, 2015, de wordpress Sitio web: https://comunicaciondedatos.wordpress.com/noc-networks-on-chip-parte2/

AT&T México. (2015). ¿Quiénes somos?. Noviembre 25, 2015, de AT&T Sitio web: https://www.att.com.mx/quienes-somos.html

RF Wireless World. (-). GSM Tutorial. Noviembre 27, 2015, de RF Wireless World Sitio web: http://www.rfwireless-world.com/Tutorials/gsm-tutorial.html

Menco, D., & Valencia, J.. (2011). Tecnologías CWDM - DWDM.. Noviembre 30, 2015, de Optica Conocimientos Sitio web: http://optica.conocimientos.com.ve/2011/09/tecnologias-dwdm-cwdm.html

Rouse, M.. (2015). Ethernet. Noviembre 27, 2015, de Search Networking Sitio web: http://searchnetworking.techtarget.com/definition/Ethernet