UNIVERSIDAD AUTONOMA METROPOLITANA

"CASA ABIERTA AL TIEMPO"

UNIDAD AZCAPOTZALCO

CIENCIAS BASICAS EN INGENIERIA

INGENIERIA ELECTRONICA

UEA - 112007

ESTANCIA INDUSTRIAL DE INGENIERIA ELECTRONICA

"REPORTE DE ACTIVIDADES"

EMPRESA Y LUGAR:
ERICSSON - GSC MEXICO - TECNOPARQUE

PROFESOR: ROBERTO ALCANTARA RAMIREZ
ASESOR INTERNO: JOSE LUIS ZAMORANO FLORES
RESPONSABLE DENTRO DE LA EMPRESA: MAURICIO HERNANDEZ
ALUMNO: HECTOR HUGO ZARZA MENDEZ
MATRICULA: 201307075

FECHA DE ENTREGA: 04 DE ENERO DE 2013

INDICE

I. CONCLUSIONES GENERALES

Me ha resultado muy grato y satisfactorio haber tomado la opción de Estancia Industrial y haberla realizado en Ericsson. En distintos aspectos de mi crecimiento profesional ha sido estimulante y provechosa. A continuación los expongo de manera general.

Trabajo en grupo

Algo en lo que como ingenieros me parece nos cuesta un poco de trabajo es el trabajo en equipo, coordinando actividades para lograr un resultado común. En las primeras semanas de mis actividades fue difícil tratar con distintas personas de distintos caracteres. La forma de trabajar de cada quien era muy distinta. Poco a poco mu fui acoplando con mis compañeros de IP CORE. Aprendí que uno debe ser muy tolerante con cada uno de nuestros compañeros, de eso depende también que ellos lo sean con uno. También comprendí que existen personas de distintos caracteres y con algunas no tendremos conflicto en nuestro trabajo pero con otras será mas difícil tener un acoplamiento de trabajo común pero sin duda si lo buscamos, lo obtenemos.

De esta manera entendí que no se busca complacer a nadie ni que las cosas se hagan como una persona las dice, sino mas bien lo único que se busca es realizar nuestras actividades lo mejor posible, brindarle a la empresa nuestro mejor esfuerzo con resultados, y aprender de los demás para ser mejores en lo que hacemos.

Conocimientos técnicos

Este es el rubro en el que me encuentro más satisfecho y motivado. Tanto el grupo en el que fui asignado, la empresa a la que le brinde servicio técnico (Sprint) y la dinámica de trabajo diaria me permitieron conocer, aprender y utilizar conocimiento de tecnologías modernas de telecomunicaciones y su aplicación en el mundo real.

Uno de las cosas que sin duda me agrado mucho fue la utilización de tecnología y equipos de Cisco. Siendo la empresa líder actualmente en equipos y tecnologías de red, me ha permitido entender porque lo es y como pisar firme en sus certificaciones. Ha sido motivante el saber como puedes crecer con sus certificaciones y con ello ser competitivo en el mundo de las redes.

Hubo también una correlación entre el conocimiento que aprendí en mi carrera junto con las tecnologías que se manejaban en el grupo IP CORE. Mi especialización en la carrera fue Sistemas Digitales. En ella, entendí mucho de computadoras, algoritmos, procesos, sistemas como microcontroladores, microprocesadores, etc.; esto lo pude relacionar directamente con routers y switches que son exactamente computadoras digitales que realizan muchas tareas en pocos segundos pero que lo hacen a través de algoritmos y programas que son implementados en cada uno de ellos. También en el grupo IP CORE manejé hardware de routers, piezas y componentes de muy alta tecnología. Aprendí que todos ellos trabajan sobre las mismas bases de la electrónica digital básica; su lógica y operación depende de que cada pequeño componente haga bien su tarea y que todos se coordinen en la forma correcta. Es decir; su operación es modular y síncrona.

Podría entrar en varios temas comentando como mi conocimiento de la carrera lo vincule con la información que recibí, sin embargo no es la idea en esta sección.

Una vez que veo la aplicación del conocimiento que aprendí en la carrera, entiendo la importancia de la ingeniería para nuestra sociedad, y a su vez, el papel que juega la electrónica en el mundo actual.

Valores profesionales

Los valores que la empresa estimula en su misión son; perseverancia, profesionalismo y respeto. Estos valores los descubrí en su aplicación cabal en cada espacio de las oficinas. Me han servido para mi crecimiento profesional y personal. El trato entre compañeros de trabajo, el ambiente de respeto diario, el respecto que la empresa te da como profesionista, los proyectos que te ofrece para crecer profesionalmente, etc.; son definitivamente cosas que me dejan muy agradecido.

El valor hacia tu trabajo es algo que se cultiva poco a poco y lo vas desarrollando conforme pasa el tiempo. Observe que existen dos formas de hacer las cosas; sea por cumplir y realizar el trabajo o porque realmente te comprometes con el grupo y esto se ve reflejado en el día a día. Si tenemos compromiso con nuestra labor entonces siempre buscamos salir adelante e ir más allá de nuestra labor diaria.

II. AGRADECIMIENTOS

Son muchas las personas que han contribuido para que haya realizado las actividades aquí descritas. He tenido la oportunidad de tener las condiciones favorables para obtener un gran aprendizaje en distintos aspectos como profesionista.

Mis más sinceros agradecimientos a;

Primeramente, a mi padre Daniel Zarza quien me ha apoyado incondicionalmente en todo momento a lo largo de mi carrera.

A la Universidad Autónoma Metropolitana; ha sido mi casa de estudios en la cual he podido obtener mi licenciatura que me permitirá ser un profesionista competitivo y que contribuya al desarrollo de mi país.

A mi asesor Jose Luis Zamorano el apoyo y la disponibilidad que me brindo en mis actividades de Estancia Industrial. Su apoyo en la creación de este reporte, así como en la orientación del proceso de mi Estancia han sido muy valiosos.

A mi coordinador de carrera Ing. Roberto Alcántara Ramírez. Fue muy atento y abierto a todas mis inquietudes.

A el Ing. Cecilio Ivan Estrada y el Ing. Mauricio Hernandez de Ericsson. Su apoyo y atención fueron de muy importantes para mí.

III. BIBLIOGRAFIA

- Documentación interna de Ericsson para la creación de tickets
- Documentación de Sprint “Sprint Job Aids“
- Documentación de Sprint para uso de las aplicaciones del grupo IP CORE

1.- INTRODUCCION GENERAL

Mi elección de Estancia Industrial

Como estudiante de la carrera de Ingeniería en Electrónica, una de las áreas en las que he tenido gran interés es el ramo de las telecomunicaciones. Me parecía un campo muy amplio y fascinante.

Durante una plática que se llevo a cabo en la universidad por parte de la empresa Ericsson supe que podía colaborar en alguno de los proyectos que planeaban abrir, para cubrir mi Estancia Industrial. Realice los trámites pertinentes e inicie mis actividades en Tecnoparque.

Ericsson

Ericsson es una empresa que se desarrolla en el campo de las telecomunicaciones. Dentro de este ramo tiene una amplia variedad de servicios y productos; sea bien en el desarrollo de productos tales como celulares y de equipos de telecomunicaciones, así como brindar servicios administrativos de operaciones de red a empresas proveedoras de servicios.

Tecnoparque

En las instalaciones de Tecnoparque se encuentran ubicadas las oficinas del GSC (Global Service Center) México de Ericsson. El **GSC** es un centro global de operaciones de red que cumple con diversas tareas tanto de soporte técnico como administrativas. Distintos grupos de trabajo convergen en este lugar con funciones específicas cada uno.

Podemos ver que cada uno cubre una tecnología específica de la amplia gama de las telecomunicaciones modernas; por ejemplo, existe un grupo denominado GNOC 3 (Global Network Operativos Center 3) el cual se avoca específicamente a tecnología de radiofrecuencia de la empresa Sprint Nextel. Con las herramientas de oficina adecuadas el grupo GNOC3 provee soluciones y apoyo técnico a cualquier evento que surja en la operación de los equipos.

De igual manera se encuentran otros grupos desempeñando la misma misión pero utilizando tecnologías especificas de la empresa a la que Ericsson brinda el servicio. Por mencionar otro caso; tenemos al grupo de Clearwire que da soporte técnico a la red de la empresa Clearwire. De manera similar al primero mencionado son denominados Primer Nivel de Operaciones (First Level Operations).

Se denomina **First Level Operations** por que los procesos de solución de problemas tienen jerarquización en grupos de trabajo. Con ello la asignación de las tareas se vuelve mucho más sencilla, dinámica y eficiente. En First Level Operations se realizan tareas como generación de reportes (tickets) de eventos en la red, asistencia telefónica a otros equipos de trabajo o también a clientes que usen los servicios, entre otras. Podemos decir que es el nivel 1 en la jerarquía, el cual realiza las tareas elementales de solución de problemas.

Un **Second Level Operations** se encarga de resolver los problemas que requieren un conocimiento técnico y tecnológico mas profundo y que también requieren un trabajo multi-grupal con técnicos de sitio y personal que asista en el sitio físico donde el problema ocurre.

2.- PRESENTACION E INTRODUCCION AL ENTORNO

En los primeros días me fue presentado las oficinas donde se encuentran las estaciones de trabajo al grupo que iba a ser asignado. El ingeniero Mauricio Hernández fungió como responsable de mis las actividades en mi Estancia. De igual manera el encargado del grupo IP CORE; el Ingeniero Cecilio Iván Estrada.

Posteriormente junto con otros compañeros recibimos un curso de capacitación de las herramientas. Una vez terminado el curso inicie actividades en el grupo NOC5. NOC5 se enfoca en las operaciones IP de la red Sprint Nextel. El grupo a su vez se encuentra subdividido en tres denominados de la siguiente forma; IP CORE, NGVN y WDI.

Grupos de trabajo

El subgrupo de IP CORE maneja directamente equipos de red como routers y switches así como los enlaces locales e internacionales de la red de Sprint.

NGVN trabaja específicamente con el tráfico de voz, así como con los equipos de red que manejan éste tráfico. Finalmente el equipo

WDI trabaja con equipos inalámbricos y la infraestructura de estos.

Cada subgrupo maneja distintas aplicaciones informáticas pero pertenecen a la misma plataforma de software patentada por Sprint y Ericsson.

Específicamente fui asignado en el primero; IP CORE

La Operación

Ahora bien, uno de los términos que debo explicar es la operación de la red. La **operación** es la ejecución en tiempo real de un conjunto de herramientas informáticas que trabajan bajo una misma plataforma de desarrollo. Esta plataforma esta bajo la licencia de Sprint Nextel y Ericsson. Dado el código de privacidad de información que Ericsson me dejo saber al inicio de mi capacitación, utilizare términos coloquiales para designar a las herramientas y equipo propio de Ericsson ó Sprint. Básicamente puedo mencionar las siguientes aplicaciones

- ***Pantalla de alarmas.*** Aplicación grafica que despliega las alarmas en el momento de haber ocurrido algún problema en la red.
- ***Pantalla de línea de comandos***: Aplicación estilo Unix en la cual se trabaja con línea de comandos en un entorno modo texto.
- ***Pantalla de Tickets***: Aplicación grafica para la creación de tickets
- ***Pantalla de tickets de mantenimiento***
- **Pantalla de alarmas de Calidad de Servicio (Quality of Service)**
- **Pantalla de Peticiones de Servicio de Cisco**
- **Pantalla Grafica de la Red**

Grupo IP CORE

En el **grupo IP CORE** el trabajo se centra justamente en los equipos que manejan información en formato de direcciones IP, es decir dispositivos digitales de telecomunicaciones que "entienden" las capas 1, 2 y 3 del modelo OSI de redes. En particular son routers y switches.

Los routers y switches son equipos de red que están diseñados para trabajar con información utilizando sus datos IP. Es decir, se trata de computadoras especializadas en el manejo de grandes cantidades de información que circula a través de cada uno de ellos y que en base a datos denominados direcciones IP puede administrarlos de la mejor manera en un corto espacio de tiempo.

No necesitamos profundizar mucho en ellos para entender mis distintas actividades. Sólo saber que su misión es recibir el tráfico que circula por las líneas de comunicación de sus puertos, leer su dirección IP y en base a programas que tienen almacenados, envían el paquete por otro puerto con información IP indicándole al siguiente router/switch que debe hacer con el paquete.

La infraestructura de red

La **infraestructura de red** que trabaja el equipo IP CORE son routers, switches y enlaces de comunicación. La mayor parte de los routers y switches que conforman la red Sprint son equipos Cisco. Los routers y switches Cisco forman una familia de equipos en los que Cisco define varias arquitecturas. La **red de Sprint** se denomina *Sprintlink* la cual opera mayormente con las familias denominadas *GSR* de *Gigabit Switch Router* y *CRS* que es el acrónimo de *Carrier Router System* del proveedor Cisco.

Al igual que la red se conforma de otros modelos de Cisco, igualmente hay equipos de los proveedores Juniper y Ciena en menor proporción. A través de la descripción de las distintas actividades iré mencionando estos equipos y conoceremos un poquito de cada uno de estos.

Sprintlink es una red muy grande. Posee comunicaciones transoceánicas entre Europa, América y Asia. Su casa es Estados Unidos, allí se encuentra la mayor cantidad de infraestructura que la compone. En México cuenta con algunos routers en la Ciudad de México y en Monterrey.

Otro término que utilizaremos es el de alarma. Una **alarma** es una alerta informática que aparece en la Pantalla de alarmas con motivo de un evento ocurrido en la red. Se trata de información técnica desplegada en forma de campos. Los campos en conjunto forman una fila. Así, se puede decir que cada fila es una alarma distinta. Cada campo es un parámetro técnico particular de la alarma. Por ejemplo, el equipo y/o línea de transmisión afectado, el error o mensaje que el equipo reporta, la hora exacta que ocurrió, entre otros.

3.- ACTIVIDADES REALIZADAS

En esta sección voy a describir las distintas actividades que desempeñe. Hare hincapié en los puntos mas destacados de las tareas realizadas.

Los objetivos de las distintas actividades eran comunes; dar solución a los distintos eventos que se presentaban en la red. En un determinado evento ocurrido, cada actividad estaba intrínsecamente relacionada con la anterior y con la siguiente. Sin embargo esto no quiere decir que existía un mismo procedimiento para todos los eventos que debían ser resueltos. En cambio, cada evento era un hecho como tal que debía ser atendido con su propio contexto. Así mismo, los equipos y componentes involucrados en cada problema variaban.

Por otro lado, los objetivos de las actividades podían cumplirse en los minutos en que tardase en resolver un problema técnicamente sencillo. En cambio, problemas de mayor dificultad podían llevar varias semanas en quedar completamente resueltos.

A continuación enlisto de manera general las actividades desarrolladas

3.1 MONITOREO DE ALARMAS

3.2 CREACION DE TICKET Y TRATAMIENTO DEL PROBLEMA

Alta utilización de una interface

Interface abajo

Tarjeta dañada

Equipo abajo

3.3 SEGUIMIENTO/ACTUALIZACION DE TICKETS

Cisco Service Request

Orden de mantenimiento

3.4 SOLUCION DE PROBLEMAS / CIERRE DE TICKETS

Problemas de alta utilización

Problemas de inestabilidad en una interface

Problemas de inestabilidad en una interface

Problemas de fallo de hardware/software

Comencemos con la primera actividad listada; monitoreo de alarmas.

3.1 MONITOREO DE ALARMAS

Diariamente cada ingeniero llegaba a su hora indicada para ocupar una estación de trabajo. En la estación era ejecutada la plataforma de software de las aplicaciones de Sprint Nextel. Una vez lanzada quedaba enlazada con los servidores de información los cuales proveían tanto las alarmas en tiempo real como la información de red que se solicitaba a través comandos.

Una vez que se iniciaba la sesión del ambiente de operación, el ingeniero tenía la responsabilidad de asistir en forma inmediata a las alarmas que durante su jornada se presentaban en la Pantalla de Alarmas.

Bien, una alarma se conformaba de distintos campos de información técnica. Ordenados en forma de filas, y divididos por columnas teníamos el nombre del router/switch afectado, la interface en cuestión, el evento ocurrido, el numero de veces ocurrido, el tiempo exacto en que ocurrió por primera vez y por ultima vez, la descripción de la línea de transmisión y su otro extremo; entre los mas importantes

Para la operación, en todo momento al menos un ingeniero debía encontrarse conectado a la operación y en plena disponibilidad de trabajar cada una de las alarmas. La operación funcionaba 24 horas por 7 días. Se tenían tres turnos: matutino, vespertino y nocturno. Regularmente por cada turno de trabajo había al menos dos ingenieros que operaban cada línea. Se denomina línea al grupo IP CORE. Otra línea era el grupo WDI.

Cuando iniciaba el turno, remplazaba a un compañero del turno previo. Mi turno fue el turno vespertino. Los compañeros del turno previo, el turno matutino nos explicaban que eventos habían ocurrido en su turno. Nos decían que tickets había que darles seguimiento, cuales se habían cerrado y los problemas pendientes por resolver.

Lo primero que hacíamos antes de cualquier otra cosa era revisar la pantalla de alarmas. Usualmente debía estar vacía, sin ninguna alarma en ella. Muchas veces aparecían varias alarmas que estaban completamente relacionadas con un solo evento. Se trataba de mantenimientos que hacían a la red con previa planeación. Mas adelante explicare esto con detalle.

Una alarma podía aparecer en pantalla en cualquier momento. La alarma podía permanecer por algunos minutos desplegada pero también podía durar solo unos cuantos segundos visible. Esto dependía del evento o problema que se estuviese presentando.

Aquí también cabe mencionar que las alarmas aparecen de distintos colores. Las alarmas que aparecen en color rojo indican que afectación o impacto a la red. Para estas alarmas puede necesitarse crear tickets de severidad 1 o 2. Estas son las severidades más importantes que podíamos tener. La severidad es sinónimo de prioridad de atención y solución al problema e

involucra un determinado impacto a la red y a los clientes. Estas dos severidades requieren la mayor rapidez y eficacia en su solución.

Otro color que se utilizaba en las alarmas era el verde que indicaba que la alarma estaba “limpia”; es decir, el problema había terminado. Aunque estuviese apareciendo en verde y el evento ya había terminado, para nosotros el hecho de haber ocurrido una sola vez y en un muy breve tiempo, era suficiente para investigar. Entonces en este caso la alarma en cualquier momento se borraba automáticamente de la pantalla. Por eso debíamos hacerle caso en el menor tiempo posible.

Una vez aparecida la alarma, lo que teníamos que hacer inmediatamente era crear un ticket correspondiente. En este debíamos poner prácticamente toda la información que la alarma nos reportaba.

Inicialmente trabajábamos de manera casi automática observando alarmas y creando tickets para cada una. Creábamos muchos tickets que enviábamos al Segundo Nivel. Sin embargo, no teníamos idea de la mayoría de las alarmas que observamos y mucho menos de su solución. Al principio las alarmas se presentaban de forma muy peculiar que no sabíamos a que se debía.

Por ejemplo, un escenario muy común era la ocurrencia de un evento que duraba solo unos segundos. Sucedía que, tan rápido como llegaba la alarma, así se borraba de manera inmediata. No sabíamos por que ocurría así, e inclusive no alcanzábamos a percatarnos de los suficientes datos que necesitábamos con el fin de crear el ticket. Tiempo después entendimos que era porque así había ocurrido el problema; esto es, en un espacio de tiempo muy breve.

Uno de los casos que se presentaban constantemente era la alarma reportaba una alta utilización de una línea de comunicación entre dos equipos.

Usualmente las líneas de trasmisión son diseñadas con un ancho de banda de mayor magnitud al trafico que se espera se presente. En general, hasta un 70% de utilización de la línea podía ocurrir sin que una alarma se presentara. Pero cuando superaba ese límite la alarma aparecía. La alarma indicaba “*ALTA UTILIZACION DETECTADA*” como problema. Nos indicaba el nodo de red donde se detectaba, es decir, un router ó switch. También presentaba el tipo de enlace, su otro nodo de conexión y el tiempo exacto en que se detecto la alta utilización.

El tráfico de datos por una línea de comunicación entre dos routers puede tener cualquier comportamiento en un periodo de solo algunos segundos. El caso era que la utilización de pronto pasaba de un 50 % a un 90 % casi instantáneamente. Resultaba algo inquietante para nosotros esto al principio, pero posteriormente entendimos que la utilización de las líneas era aleatoria.

Bueno, finalmente también observábamos que la utilización después de unos segundos caía dramáticamente volviendo a su porcentaje de utilización habitual. Igualmente nos sorprendíamos que sucediera casi de forma inmediata (en solo unos milisegundos). Igualmente, la alarma aparecía momentáneamente y unos segundos después desaparecía.

Lo que con el tiempo entendimos fue que la curva de utilización de una línea de comunicación puede tener espigas muy breves y eso es, en general, normal. En cambio también aprendimos que si la espiga permanece por varios minutos con un valor de 90% o mayor, entonces allí había que investigar algo, ya que esa sobreutilización podría saturar la línea y provocar perdida de información y algunos errores en la línea. Mas adelante explicare como se daba seguimiento a problemas de este tipo.

Respecto a cada una de las alarmas desde un principio nos dimos cuenta que era muy importante tener el conocimiento básico tanto de los fundamentos de la teoría de redes de computadoras como de los equipos tecnologías que maneja la red de Sprint; por ejemplo, la arquitectura interna de los routers y switches, los tipos de enlaces que conforman su infraestructura, etc., ya que esto permitía hacer un razonamiento correcto de la acción a tomar en el momento de la aparición de la alarma.

Básicamente el proceso era crear un ticket para cada alarma que el sistema reporta. En el quipo IP CORE también contábamos con una documentación puntal y organizada de muchas de las alarmas que ya eran muy conocidas. Inicialmente seguíamos los procesos tal cual se indicaba textualmente y posteriormente nos dimos cuenta de que no solo era el hecho de seguir el proceso como tal sino de entender lo que estábamos haciendo y en base a ello decidir ciertas acciones.

Otro escenario muy común era cuando teníamos algo que se denomina *falsa alarma*. Bajo nuestro proceso documentado teníamos que una vez que aparecía la alarma creábamos de inmediato el ticket correspondiente usando los datos técnicos que la alarma nos reportaba. No obstante las alarmas no eran correctas; el evento nunca había ocurrido en realidad. ¿Qué sucedía entonces? Resulta que los servidores de alarmas por alguna razón arrojaban alarmas que no eran ciertas ya que el evento nunca había sucedido. Es decir, era algún error o problema en los servidores.

Lo que entendimos que era correcto hacer era que por medio de la Pantalla de línea de comandos verificásemos el estado del equipo, sea router o switch o línea de comunicación. De esta manera con la información obtenida directamente de el equipo en cuestión constatábamos si el hecho reportado era correcto o no. Hablare un poquito mas adelante acerca de esto.

En general, esto es respecto a lo que concierne a las alarmas. En los siguientes párrafos profundizare en el trabajo completo que llevábamos a cabo con el fin de resolver justamente el problema que cada alarma nos reportaba.

3.2. CREACION DE TICKET Y ANALISIS DEL PROBLEMA

La creación de tickets era nuestra principal tarea como Primer Nivel de Operaciones en el NOC. La creación de ticket es el primer paso en cualquier evento de la red para posteriormente resolverlo. El objetivo de la creación de un ticket es para constatar la existencia de una alarma que hace referencia a un problema de la red. También el ticket tendrá vigencia mientras se siga trabajando para solucionar el problema. Un ticket no debe ser cerrado a menos que el problema haya sido completamente resuelto. Es así como un ticket viene a tener sentido en nuestro trabajo diario; actualizándolo cada vez que se de un avance en la solución de su problema.

Un ticket estaba compuesto de un titulo. El titulo del ticket explicaba muchas cosas. El formato era el siguiente,

Nombre del grupo – [Equipo afectado] Problema reportado [Extremo lejano] [Numero de circuito]

Los corchetes indican que el parámetro no es obligatorio sino es acorde al problema reportado. Por ejemplo:

CORE – router1-mia pos10/0/1 *Interface inestable* hacia router8-chic, pos5/7/2 – circuito 21765428

En este caso en particular estamos reportando un problema de INTERFACE INESTABLE; es decir, que la interface del router se encuentra cambiando de estado activo a inactivo y viceversa.

El nombre “router1-mia” indica que es el router numero 1 del sitio de Sprint en Miami. La interface reportada es la POS10/0/1 del equipo router1-mia. POS es el acrónimo de Packet Over SONET ó paquetes sobre SONET. Se trata de un tipo de tecnología de trasmisión de información por una línea de transmisión de fibra óptica. La información es dividida en paquetes con un formato de protocolo IP de enrutamiento. Y la numeración que le sigue es Numero-de-ranura/Numero-de-sub-ranura/Numero-de-puerto. Todo esto es la designación de la interface.

Posteriormente aparece “hacia” que indica a donde iba conectado; es decir, el otro extremo de la línea. En nuestro ejemplo es el router numero 8 del sitio de Chicago con interface pos5/7/2. Finalmente el número de enlace, que es la línea que comunica a router1-mia con router8-chic.

A continuación revisare los campos que conformaban la plantilla de cualquier ticket a crear.

Fecha y hora. – Indicar la fecha y hora exacta en que ocurrió el problema

Tipo de red.- El tipo de red al que pertenece el equipo o equipos afectados

Tipo de equipo.- Que modelo de equipo es el involucrado. Ej. GSR 12000, CRS1, Ciena, Juniper, etc.

Tipo de problema.- Existían problemas que pertenecían a una categoría especia. Por ejemplo Alta Utilización en la línea, Interface inestable, etc.

Severidad.- El grado de severidad que corresponde al problema en cuestión. Por ejemplo severidad 2

Equipo.- Nombre del equipo afectado. Por ejemplo el router10-mia.

Ranura.- Ranura dañada o afectada en el equipo. Por ejemplo ranura1

Sub-ranura.- La ranura contiene sub-ranuras que se diferencian numéricamente. Por ejemplo subranura1 ó subranura2 de la ranura1.

Puerto.- Cada subranura cuenta con cierta cantidad de puertos. La forma de definir un punto de enlace de router específico es Ranura/Subranura/Puerto. Los tres términos son enumerados para su distinción. Por ejemplo, ranura3/subranura2/puerto1.

Numero de facilidad/Numero de circuito.- Es una codificación numérica que contiene cada enlace entre equipos que permite identificar a cada uno.

Como vimos en la descripción de una alarma, la mayoría de los parámetros que llenamos en el ticket los podemos encontrar en esta. Otra información requerida, nos apoyábamos en la Pantalla de línea de comandos y desplegamos información acerca del router o la línea de comunicación. Básicamente así es como llenábamos la platilla de ticket para crearlo. Una vez introducidos todos los datos mencionados, dábamos clic en un botón que indicaba la creación del ticket y, era creado.

A continuación, revisare los problemas representativos en la creación de tickets.

Alta utilización de una interface

Uno de los problemas que se nos presentaba con gran frecuencia era la alta carga de tráfico en una determinada línea de transmisión.

Una vez creado el ticket, a continuación poníamos la nota del estado actual de la interface. Para ello, desde la Pantalla de línea de comandos nos apoyamos del comando "*show interfaces <interface>*", la cual nos desplegaba la información que necesitábamos. Datos como la taza de utilización tanto de trafico de entrada como de salida en los últimos minutos, la carga de la cola de entrada y salida, el tiempo en que llego el ultimo dato de entrada y salida; nos daban un perfecto diagnostico y resumen de nuestra carga de trafico en la línea. Veamos el siguiente ejemplo:

c4500-1# **show interfaces fastethernet 0**
FastEthernet0 is up, line protocol is up
Hardware is DEC21140, address is 0000.0c0c.1111 (bia 0002.eaa3.5a60)
Internet address is 11.0.0.1 255.0.0.0
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255**, load 1/255**
Encapsulation ARPA, loopback not set, keepalive not set, hdx, 100BaseTX
ARP type: ARPA, ARP Timeout 4:00:00
Last input never, output 0:00:16, output hang 0:28:01
Last clearing of "show interface" counters 0:20:05
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 1786161921 ignored, 0 abort
0 watchdog, 0 multicast
0 input packets with dribble condition detected
67 packets output, 8151 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets, 0 restarts
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

A continuación copiábamos y pegábamos esta información en el ticket y describíamos lo que sucedía. En esta descripción vemos que la interface esta "up"; es decir, se encuentra habilitada o "arriba". Vemos en la segunda línea que indica *FasEthernet0 is up, and protocol us up*. Se refiere a que la interface física; una línea tipo *DEC21140*, esta activa y también el protocolo de operación de la línea esta activo o "up". Después vemos en las líneas 11 y 12 que su taza de entrada es 0 y de salida también es 0. Entonces teníamos un problema en la línea. La interface y el protocolo están habilitados pero no hay tráfico en la línea. Debía investigarse más a fondo. Enseguida enviábamos el ticket al Segundo Nivel de Operaciones. Por "enviar el ticket" me refiero a que en la Pantalla de Creación de tickets teníamos distintas opciones para procesar un ticket. Una de ellas era enviar el ticket a otra *cola de trabajo*.

Una cola de trabajo es un elemento de la aplicación de creación de tickets que es como una caja en donde podemos acumular tickets.

A través de un chat interno con el Segundo Nivel de Operaciones, les hacíamos saber de que cierto número de ticket había sido enviado a su *cola de trabajo* para investigar el problema; en este caso, una línea sin tráfico de información.

En particular el comando **show interface <interface>** resultaba muy útil. Como observamos, nos despliega muchos parámetros importantes de la interface. Algunos de ellos se utilizaban en otros problemas que ocurrían.

Pantalla grafica de la red

Otra herramienta muy valiosa era la Pantalla grafica de la red. Entre otras cosas, podíamos observar en forma grafica la curva de utilización de la línea de transmisión. Nos mostraba su comportamiento en los últimos dos días en un eje de coordenadas cartesianas siendo el eje horizontal el tiempo y el vertical el porcentaje utilización de la línea de transmisión. También podíamos obtener la curva de utilización de las últimas dos semanas. Y si deseábamos indagar mas la del ultimo mes. Nos resultaba útil esta información y poder realizar comparaciones del comportamiento de la curva de tráfico de la línea. De esta forma acorde a nuestras conclusiones poníamos las notas correspondientes en el ticket. Una vez colocada esta información en el ticket, dejábamos el ticket en observación por cierto tiempo y tener conclusiones finales.

De esta manera en Primer Nivel de Operaciones le dábamos un completo seguimiento y solución a los tickets de ALTA UTILIZACION DE LA LINEA. El ticket era cerrado cuando de acuerdo a nuestros análisis veíamos que era lo correcto. En otro caso podría ser investigado más a fondo por el Segundo Nivel de Operaciones.

Interface abajo

Una interface caída o “abajo” significa que no se encuentra activa y no hay flujo de información a través de ella. Un escenario de interface caída se nos presentaba a menudo. Veamos con un ejemplo en las acciones que llevábamos a cabo con el análisis y decisiones de cada detalle investigado.

La alarma que utilizaremos es la siguiente,

Primera ocurrencia	Ultima ocurrencia	Contador	Nodo	componente	Resumen	Descripción de interface
11/16/2012 8:27:04 PM	11/16/2012 8:27:04 PM	1	router2-mia	POS0/9/5/6	INTERFACE ESTA ABAJO	Hacia router10-rio, POS0/9/5/6 – FAC 10231234

Me resulta muy adecuado mostrarla en forma de tabla ya que precisamente así era como era desplegada en la Pantalla de alarmas.

Para una alarma de INTERFACE ESTA ABAJO, inicialmente nos íbamos a la Pantalla de línea de comandos, ejecutábamos el comando **info router2-mia**. Con ello obteníamos los tickets que router2-mia tenia asociados tanto cerrados como abiertos en los últimos 15 días. Entonces observábamos con detalle si existía un ticket abierto para router2-mia po0/9/5/6. Debíamos tener cuidado de no confundir las interfaces porque podría haber tickets de router2-mia pero que se referían a otras interfaces.

En caso de que previamente ya se hubiese creado un ticket para este evento, simplemente dentro de la Pantalla de alarmas teníamos una opción para “Asignar ticket a alarma”. Con eso la alarma pasaba al estado de “alarma en trabajo”. La alarma se “borrara” cuando deje de estar abajo la línea. Así mismo el ticket será cerrado hasta que la línea se encuentre de nuevo en operación.

En algunas ocasiones aunque ya estuviese un ticket abierto para la alarma INTERFACE ESTA ABAJO y en su momento se asignara el ticket a la alarma, podía suceder que tiempo después la alarma volviera aparecer en la Pantalla de alarmas. Entonces nuevamente debíamos asignar el ticket a la nueva alarma.

Ahora bien, si la alarma no tuviese ticket abierto en el momento que aparecía, nos íbamos la Pantalla de creación de tickets y lo creábamos con los parámetros correspondientes. El título quedaba:

CORE - ROUTER2-MIA POS0/9/5/6 *IINTERFACE ESTA ABAJO* HACIA ROUTER10-RIO, POS0/9/5/6 – FAC.10231234

El titulo del ticket decía grupo al que pertenecía, el problema, donde ocurría, y los datos la línea. FAC es acrónimo del termino "facility" y es un identificador de la línea. FAC se utilizaba en una investigación mas detallada de la línea.

Una vez que llenábamos los campos de la plantilla de creación de ticket, creábamos el ticket. Enseguida nos íbamos a la Pantalla de línea de comandos, ingresábamos al router y ejecutábamos el comando **show log | include 9/5/6**. “show log” nos desplegaba todos los mensajes (denominados logs) que el router hubiese registrado en los últimos días. Dado que nos desplegaba bastante información que no necesitábamos, utilizábamos un filtro en el comando. Con “| include 9/5/6” le decíamos al sistema operativo del router que nos desplegara todos los mensajes que incluyeran la cadena “9/5/6”. Con ello veíamos los logs de la interface po0/975/6. En el ejemplo, serian como las siguientes;

POS0/9/5/6, changed state to **down**
Nov 16 08:27:23: %LINK-5-CHANGED: Interface POS0/9/5/6, changed state to administratively down
Nov 16 08:27:23: %LINEPROTO-5-UPDOWN: Line protocol on Interface POS0/9/5/6, changed state to down

Observando estas líneas dentro del router autentificábamos el problema, corroborábamos el tiempo exacto de ocurrencia y si la línea aun seguía “caída”. Como observamos los mensajes nos dicen que interface cambio a “down” y a que hora. La segunda línea se refiere a que la interface física se “abajo” y la tercera que el protocolo de la línea esta “abajo”. Distinguíamos estos dos datos por que son nos aclaran que tanto el protocolo que se encarga del envió de paquetes y el trabajo de la información en la línea así como también la línea física por alguna razón física no funcionaba.
Por otro lado, con el comando ejecutado nos desplegaba todos los mensajes relacionados con la interface 9/5/6. Si aparte de los tres ya comentados no nos mostraba otros que indicaran que la interface estaba “arriba”, entonces la línea aun seguía abajo.

Una vez que estos mensajes los copiábamos y pegábamos en el ticket, poníamos los comentarios que la línea seguía abajo. Inmediatamente nos íbamos a la Pantalla de creación de tickets mantenimiento y buscábamos los mantenimientos programados del día. Nos aparecían listados por filas y columnas con su periodo de implementación, su impacto y los equipos y/o líneas involucradas. El impacto de un mantenimiento podría ser “de red” o “de red y de clientes”. Un impacto “de red” es cuando el trabajo de mantenimiento solo impacta a equipos y enlaces que no afectan a clientes de Sprint. Se entiende así por que muchos equipos no conectan directamente a los clientes con la red sino que lo pueden hacer indirectamente proporcionando redundancia a los enlaces. El impacto “de red y clientes” afecta tanto a equipos y enlaces como a clientes directamente.

En caso de encontrar algún trabajo de mantenimiento que afectara a router2-mia pos0/9/5/6, o bien a la línea 10231243, entonces no había ningún problema en el estado de la línea. En el ticket poníamos el numero de ticket del mantenimiento correspondiente en indicábamos detalles como el periodo de duración del mantenimiento. El ticket lo podíamos continuar actualizando en las siguientes horas con los comentarios que en el ticket de mantenimiento fueran escritos.

Ahora bien, en caso que no encontrásemos el problema debía seguirse investigando. Poníamos en una nueva nota algo como “No se encontró trabajo de mantenimiento en la línea”. Enseguida les enviábamos el ticket al Segundo nivel de operaciones. El Segundo nivel de operaciones podía ver con el grupo de trabajo “Equipo de transporte”; quienes podían investigar directamente en el sitio físico del problema, mandar técnicos a revisar los equipos, etc.

De nuestra parte nos seguía correspondiendo seguir observando las notas que en el ticket se escribieran en razón de saber el avance de la solución. Aunque el ticket estuviese en otra cola de trabajo podíamos seguir observando sus actualizaciones e incluso podíamos poner notas de igual manera.

Tarjeta de línea dañada

Los routers tienen una arquitectura modular basada en tarjetas de línea. Cada tarjeta de línea realiza tareas específicas que contribuyen a la funcionalidad del router. Se trata de tarjetas de alta tecnología que Cisco ha venido mejorando a través de los años y que son diseñadas con propósitos bien definidos y con el fin común de administrar el tráfico de información de manera eficiente y segura.

En el grupo de Primer nivel de operaciones uno de los eventos más delicados que manejábamos era el de una alarma de TARJETA DAÑADA. Casi siempre era un problema de afectación a clientes. Veamos como iniciábamos nuestras tareas para el problema.

Una vez que veíamos en la Pantalla de alarmas la alarma TARJETA DAÑADA, inmediatamente comenzábamos a crear el ticket correspondiente. Antes de terminar de crear el ticket debíamos ejecutar un comando en la Pantalla de línea de comandos. El comando nos daba la cantidad de clientes dañados. Es decir, el comando llevaba como argumentos el nombre del equipo y la ranura y sub-ranuras afectadas. Había comentado que una ranura es en donde se insertan las tarjetas de línea que componen al router. Por tanto una tarjeta de línea tiene asignado un número de ranura. En las sub-ranuras se encuentran los puertos de la tarjeta de línea.

Era posible que para una tarjeta dañada no hubiese clientes afectados, sin embargo no era algo común. En ese caso el ticket era de severidad 5. Una vez obtenidos los clientes afectados, en el ticket existía un campo en cual indicábamos la cantidad. Éste campo no se utilizaba en otro tipo de problemas ya que no existían clientes afectados. Si el número de clientes era mayor a 100, el ticket tenía una severidad 2. En cambio si el problema había impactado a más de 100 clientes en ticket se creaba como severidad 1.

Un ticket severidad 2 tenía gran prioridad de trabajo y solución. Un ticket severidad 1 tenía la máxima prioridad posible. Algo esencial en nuestro proceso de investigación de datos era dos cosas; una era si el problema seguía. Es decir, si aun continuaba dañada la tarjeta y con ello todos los puertos de las sub-ranuras seguían abajo. Y por consiguiente los clientes conectados a esos puertos habían perdido todo tipo de servicios y comunicación. El otro punto crucial era si el problema era real o una posible “falsa alarma”. Debo comentar que para estos problemas era muy raro que la alarma fuese falsa. Pero si llegaba a suceder.

Por ejemplo, con el siguiente trabajo en la Pantalla de línea de comandos corroborábamos la existencia del problema

Router#**show context summary**
CRASH INFO SUMMARY
S**lot 1 : 1** c**ra**s**hes**
1 - crash at 10:36:20 UTC Wed Dec 19 2001
Slot 2 : 0 crashes
Slot 3 : 0 crashes
Slot 4 : 0 crashes
Slot 5 : 0 crashes
Slot 6 : 0 crashes
Slot 7 : 0 crashes
Slot 8 : 0 crashes
Slot 9 : 0 crashes
Slot 10: 0 crashes
Slot 11: 0 crashes
Slot 12: 0 crashes
Slot 13: 0 crashes
Slot 14: 0 crashes
Slot 15: 0 crashes

Como observamos, la ranura 1 (slot, en idioma ingles) tuvo un “crash” que quiere decir daño o destrozo. Nos indica el tiempo exacto en que ocurrió. En el ticket se pega esta información que autentifica el hecho. Aun no hemos comentado como nos aparece la alarma, cual es el error que se observa y como sabemos que es una tarjeta dañada.

En las líneas de abajo observamos los mensajes que nos arroja el router cuando ejecutamos show log | i “Mar 2”. La alarma era **%RP-4-RSTSLOT: Resetting the card in the slot: 7**, el cual es un mensaje de Cisco indicando un problema serio en el slot 7 del router.

En las siguientes líneas confirmábamos el verdadero problema con %LCINFO-3-CRASH: Line card in slot 7 crashed. La tarjeta se había dañado y por tanto había dejado de operar llevando al estado de caído a todas sus interfaces, en este caso, a las 7/1 7/2, 7/3 7/4 y 7/5; todas ellas del tipo Fast Ethernet.

Aquí lo podemos observar con cada mensaje tanto para el protocolo (software de operación) como para la interface física en cada una.

Mar 2 17:44:22: **%RP-4-RSTSLOT: Resetting the card in the slot: 7**,Event: linecard error report
Mar 2 17:44:22: %LINK-5-CHANGED**: Interface FastEthernet7/1,** changed state to administratively **down**
Mar 2 17:44:23: **%LCINFO-3-CRASH: Line card in slot 7 crashed**
Mar 2 17:44:23: %LINEPROTO-5-UPDOWN: Line protocol on Interface **FastEthernet7/1**, changed state to **down**
Mar 2 17:44:23: %LINK-5-CHANGED**: Interface FastEthernet7/2,** changed state to administratively **down**
Mar 2 17:44:23: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7/2**, changed state to **down**
Mar 2 17:44:23: %LINK-5-CHANGED**: Interface FastEthernet7/3,** changed state to administratively **down**
Mar 2 17:44:23: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7/3,** changed state to **down**
Mar 2 17:44:24: %LINK-5-CHANGED: **Interface FastEthernet7/4,** changed state to administratively down
Mar 2 17:44:24: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7/4**, changed state to **down**
Mar 2 17:44:24: %LINK-5-CHANGED: **Interface FastEthernet7/5**, changed state to administratively **down**
Mar 2 17:44:24: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7/5**, changed state to **down**

Bueno, como comente anteriormente, era esencial ver si seguían las interfaces abajo. Con el mismo comando ejecutado nos debía dar razón de ello. Podríamos observar los mensajes siguientes

SLOT 7:*Mar 1 00:00:20: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GLC1-LC-M), Version 12.0(32)S5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Wed 18-Oct-06 15:24 by leccese
Mar 2 17:46:03: %LINK-3-UPDOWN**: Interface FastEthernet7/1**, changed state to **up**
Mar 2 17:46:03: %LINK-3-UPDOWN**: Interface FastEthernet7/2**, changed state to **up**
Mar 2 17:46:03: %LINK-3-UPDOWN**: Interface FastEthernet7/3**, changed state to **up**
Mar 2 17:46:03: %LINK-3-UPDOWN**: Interface FastEthernet7/4**, changed state to **up**
Mar 2 17:46:03: %LINK-3-UPDOWN**: Interface FastEthernet7/5**, changed state to **up**
Mar 2 17:46:04: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7**/**1,** changed state to **up**
Mar 2 17:46:04: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7/2**, changed state to **up**
Mar 2 17:46:04: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7/3**, changed state to **up**
Mar 2 17:46:04: %LINEPROTO-5-UPDOWN**: Line protocol** on Interface **FastEthernet7/4**, changed state to **up**
Mar 2 17:46:04: %LINEPROTO-5-UPDOWN: **Line protocol** on Interface **FastEthernet7/5,** changed state to **up**

Como observamos, los mensajes indican que las interfaces están “up” o arriba desde las 17:46:03 de marzo 2. Entonces el problema ya no seguía sino que la tarjeta se había reiniciado y vuelto a operar habilitando sus componentes.

Con todo esto, el ticket estaba listo para ser enviado al Segundo nivel de operaciones. El ticket debía ser considerado por otros equipos y ver que había sucedido con la tarjeta, tal vez ir al sitio físico donde se encuentra el equipo y revisar que sucedió y el estado. Acuerdo a sus consideraciones y conclusiones el ticket continuaba actualizándose.

En ocasiones la tarjeta debía ser remplazada, ya sea porque estaba dañada o por que el evento ya había sucedió en otra ocasión y entonces se le denominaba “crónico”. Entonces por ser un “problema crónico” la tarjeta debía ser cambiada.

Cuando alguna pieza de hardware necesitaba remplazarse requeríamos saber con detalle dentro del router que pieza era la que se había dañado.

Router#show diag

SLOT 1 (RP/LC 1): 1 Port Packet Over SONET OC-12c/STM-4c Single Mode
MAIN: type 34, 800-2529-02 rev C0 dev 16777215
HW config: 0x00 SW key: FF-FF-FF
PCA: 73-2184-04 rev D0 ver 3
HW version 1.1 S/N CAB0242ADZM
MBUS: MBUS Agent (1) 73-2146-07 rev B0 dev 0
HW version 1.2 S/N CAB0236A4LE
Test hist: 0xFF RMA#: FF-FF-FF RMA hist: 0xFF
DIAG: Test count: 0xFFFFFFFF Test results: 0xFFFFFFFF
L3 Engine: 0 - OC12 (622 Mbps)

Estos datos eran proporcionados a Cisco en una petición de servicio ó Service Request. Cisco brindaba un gran servicio en tiempo y envió del hardware. Cuando el hardware llega al sitio correspondiente, la siguiente acción era crear una orden de mantenimiento a través de un ticket de mantenimiento. Finalmente se remplazaba la pieza.

Equipo abajo

Uno de los problemas que se presentaban con cierta regularidad eran alarmas de “EQUIPO ABAJO”. Una alarma EQUIPO ABAJO indicaba que el router o switch se había caído; es decir, había quedado inoperable completamente. Primero debíamos asegurarnos de que se tratase de una alarma correcta.

El siguiente comando lo utilizábamos frecuentemente. Nos proporcionaba información muy valiosa acerca del equipo. En el caso de una alarma “EQUIPO ABAJO” nos permitía confirmar si era correcta la alarma. Es decir, en este ejemplo, el equipo Thunder nos muestra que el equipo se cayó el día jueves 3 de Julio de 2001 a las 00:01:30. Desde entonces el equipo se ha mantenido en operación continua.

Thunder#**show version**
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR−P−M), Experimental Version 12.0(20010505:112551)
[tmcclure−15S2plus−FT 118]
Copyright (c) 1986−2001 by cisco Systems, Inc.
Compiled Mon 14−May−01 19:25 by tmcclure
Image text−base: 0x60010950, data−base: 0x61BE6000
ROM: System Bootstrap, Version 11.2(17)GS2, [htseng 180] EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
BOOTFLASH: GS Software (GSR−BOOT−M), Version 12.0(15.6)S, EARLY DEPLOYMENT
MAINTENANCE INTERIM SOFTWARE
Thunder uptime is 17 hours, 53 minutes
System returned to ROM by reload at 23:59:40 MET Mon Jul 2 2001
System restarted at 00:01:30 MET Tue Jul 3 2001
System image file is "tftp://172.17.247.195/gsr−p−mz.15S2plus−FT−14−May−2001"
cisco 12012/GRP (R5000) processor (revision 0x01) with 262144K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power−on
2 Route Processor Cards
1 Clock Scheduler Card
3 Switch Fabric Cards
1 8−port OC3 POS controller (8 POs).
1 OC12 POs controller (1 POs).
1 OC48 POs E.D. controller (1 POs).
7 OC48 POs controllers (7 POs).
1 Ethernet/IEEE 802.3 interface(s)
17 Packet over SONET network interface(s)
507K bytes of non−volatile configuration memory.
20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).

En base a esta información podemos decir si la alarma que indica “”EQUIPO” abajo es realmente cierta. Resultaba que en muchas ocasiones encontramos que no era correcta y con ello limpiábamos la alarma y no se requería mayor acción de investigación o solución.

Este comando también nos da información acerca de los componentes que integran el equipo. Aparecen listados en las últimas líneas. El equipo Thunder tiene 2 procesadores, 1 tarjeta de reloj; para la sincronización de los procesos, 3 tarjetas POS; 1 de OC12, 1 de OC48 y 1 de 8 puertos OC3, entre otros. Esta información de los componentes es muy general, en realidad si deseábamos saber acerca de una tarjeta en particular ejecutábamos otros comandos, algunos los he comentado.

En caso que no coincidiera la ultima fecha de “uptime” o tiempo arriba de la información del router con el tiempo que la alarma reportaba, entonces no se le hacia caso a la alarma; se consideraba “falsa alarma”.

3.3 SEGUIMIENTO/ACTUALIZACION DE TICKETS

Diariamente una de las tareas que teníamos asignadas era darle continuo seguimiento a los tickets abiertos. Esta podía ser una tarea breve de unos minutos de dedicación a cada ticket o bien podría ser mucho más compleja. Podría suceder que un solo ticket nos llevara cerca de una hora de trabajo en su actualización y seguimiento al proceso de su solución.

Un ejemplo de una actualización muy breve era el continuo monitoreo de una ALTA UTILIZACION DE INTERFACE. Aquí únicamente revisábamos que la carga de tráfico se encontrase dentro del rango normal de la línea o bien no mayor a su 70% de capacidad. En el ticket poníamos una nota indicando el estado actual. Específicamente poníamos la información que nos daba la Pantalla de la línea de comandos.

Algo similar realizábamos con las INTERFACES INESTABLES. En este caso lo importante era que la interface se mantuviera estable después de haber ocurrió un “bouncing” (haber caído y vuelto a subir). Al monitorear una interface que cayo y volvió a subir nuestra principal intención era saber que ese “bounceo” solo se había generado en forma aislada y lo podíamos atribuir a algún error momentáneo detectado, algún reacomodo de los cables tal vez por la condiciones físicas del lugar o, algo por el estilo. Por tanto ingresábamos al equipo, desplegábamos los mensajes (logs) registrados referentes a la interface y debíamos notar que no hubiese mas mensajes de interface abajo/arriba que el ocurrido en el ticket registrado. Esto nos decía que ningún otro evento se había registrado en esa interface y nos daba la total seguridad de la estabilidad de la misma. Esto lo agregábamos como una nota en el ticket. Con ello decíamos que la interface continuaba estable. Un ticket de interface inestable continuaba abierto según consideramos era necesario para confirmar la estabilidad del enlace. Había enlaces que tenían gran inestabilidad que de forma recurrente. Por tanto, debían ser monitoreados por un periodo de algunas horas.

También se le daba seguimiento a otra clase de problemas. Cuando un problema de TARJETA DAÑADA requería el remplazo de una pieza de hardware, el ticket requerida un proceso mas complejo que los dos mencionados anteriormente.

El que una pieza de hardware se hubiese dañado y se necesitara remplazar requería que se solicitara una orden de petición de servicio a la compañía Cisco para solicitar la pieza a reponer. Esto se realizaba a través del sitio Web de Cisco. Con una cuenta previamente creada y con un contrato de servicios dispuesto entre la empresa Ericsson y Cisco, podíamos hacer la petición requerida. Llenando los datos necesarios en la plantilla electrónica del sitio ya estábamos diciendo a Cisco lo que necesitábamos. Esto se denomina Cisco Service Request

Cisco Service Request

Entonces para los tickets que llevaban este proceso necesitábamos estar constantemente monitoreando el Service Request en la página de Cisco. Esto es, con el número de Service Request que se creaba al momento de hacer la petición de la pieza podíamos ver estatus de nuestra petición. En forma de documento se despliegan los detalles del Service Request. Entonces en nuestro ticket podíamos poner los últimos detalles que encontraremos allí acorde a lo que necesitábamos.

Orden de mantenimiento

Otra etapa del ticket en este caso de problemas era la creación de un ticket de actividad de mantenimiento. Esto es, dado que se debe remplazar la pieza, no lo podíamos hacer en cualquier momento del día. Al contrario, debía llevarse a cabo en un periodo de tiempo que fuese lo menos perturbador para la red en lo posible. A esto se le denominaba “ventana de mantenimiento”; es decir, el periodo de tiempo en el cual se realizan actividades de mantenimiento a la red. Entonces para realizar una actividad de mantenimiento requería algunas tareas previas. Primero se debía crear un ticket de mantenimiento. Este tipo de tickets era completamente distinto a los tickets de solución de problemas. Se realizaban con otra aplicación y su objetivo era completamente distinto. Un ticket de mantenimiento se creaba justamente para pedir que la actividad de mantenimiento o servicio fuese aceptada por un grupo de trabajo especializado en aprobar estas actividades. Ellos evaluaban los riesgos, el impacto, el periodo de afectación, los componentes implicados, etc., de la actividad. Además de este propósito, en el ticket de mantenimiento se especifica todos los detalles de la actividad; quien la iba a desempeñar, cuando y a que hora, que equipos serian afectados, cuantos clientes serian impactados y por cuanto tiempo, cual es el objetivo y descripción de la actividad. Además también un Manager o Supervisor debía hacerse responsable de esto, aquí se detallaba también. Entonces un ticket de mantenimiento tenia mucha importancia no solo para remplazar una pieza de hardware en un router sino para cualquier actividad sea de servicio o mantenimiento a la red, por pequeña y breve que fuese necesitaba un ticket mantenimiento.

Volviendo a nuestros tickets de solución de problemas que debían ser monitoreados, si el ticket tenia un ticket de mantenimiento asociado entonces debíamos observar que ese ticket fuese aprobado en un tiempo breve, que la actividad planeada se indicara correctamente en el ticket de mantenimiento y que los por menores de la actividad estuvieran al día. Lo mas importante era ver el día de implementación de el remplazo de hardware y que todo estuviese listo antes de esa fecha. Para que el ticket de mantenimiento fuese aprobado, debíamos enviar un correo de petición de aprobación al grupo correspondiente. Mientras se aprobaba el ticket de mantenimiento, poníamos los detalles de la orden de mantenimiento en el ticket de solución del problema.

Podría suceder que el trabajo de mantenimiento no fuese aceptado ya sea porque en el horario planeado ya había otros programados, por que se debía justificar una posible afectación a clientes o por que el horario no estaba en la ventana de mantenimiento del tiempo local. En cualquiera de los casos se hacia las correcciones pertinentes y el proceso seguía adelante.

Una vez que el ticket de mantenimiento era aprobado nos llegaba un correo indicando la aprobación. Entonces indicábamos en el ticket de solución de problemas que el ticket de mantenimiento estaba aprobado. A continuación el ticket de solución de problemas era enviado al Segundo nivel de operaciones en donde el grupo se encargaba de continuar con el proceso.

3.4 SOLUCION DE PROBLEMAS/CIERRE DE TICKETS

Una vez que se había resuelto por completo el problema de un ticket; entonces al ticket se le realizaban dos acciones:

Limpiar el ticket.- Esta acción era muy importante por distintas razones. Primero, un ticket “limpiado” era una indicación de que el problema se había resuelto y los equipos o refacciones afectados funcionaban correctamente. Segundo, el tiempo exacto en que se puso la nota de “limpiado” era exactamente el momento en que había quedado resuelto el problema. Era muy importante este tiempo ya Ericsson tenia acuerdo de tiempos de resolución con sus clientes.

El tiempo de duración en resolver el problema contemplaba desde que el ticket se creo hasta que se “limpio”. De ahí la importancia tanto del tiempo de creación del ticket como del tiempo de “limpiarlo”.

Una vez que un ticket era “limpiado” en Primer Nivel de Operaciones confirmábamos que todo funcionara correctamente entrando al equipo a través de la Pantalla de línea de comandos y desplegábamos el estado del equipo o componente con ayuda de algún comando.

Un ticket “limpiado” aun estaba activo para ponerle alguna nota acerca del estado del equipo. También se acostumbraba ponerle algunos comentarios acerca de si el problema era crónico (ocurría repetidamente), acerca de tickets previos creados por el mismo evento, conclusiones del problema

ocurrido y el proceso de solución, etc., consideraciones que se considerara adecuadas incluir en el ticket tal vez para futuras consultas del ticket.

También un ticket “limpiado” podía seguir siendo considerado para poner en observación el equipo reparado por un periodo de tiempo. Es decir, una vez reparado el hardware afectado ó software modificado y limpiado el ticket, se podían continuar realización actividades de monitoreo y revisión del estado. Esto dependía específicamente del problema y solución. En caso de que se requiérase, se hacia por un periodo bien definido; algunas horas regularmente. En caso de encontrarse algún error el ticket entonces se le ponía una nota de lo observado y según se requiérase se habría otro ticket o se continuaba monitoreando.

Cierre del ticket. Para que un ticket pueda ser “cerrado” debe estar “limpiado”. Un ticket cerrado ya no podía ser utilizado. Es decir, al cerrarlo se asumía que ya no se requería en lo absoluto. En este caso, el tiempo de cierre no era tan importante como el tiempo de “limpiado”.

Algo curioso que nos sucedía en ocasiones era que en un problema de interface inestable que el ticket ya sea había “limpiado” y cerrado con conclusiones favorables acerca de la estabilidad de la línea, entonces, unos minutos después de cerrar el ticket, el evento volvía ocurrir apareciendo la alarma. Entonces volvíamos a crear el ticket poniendo una nota acerca del trabajo que se había hecho en el ticket previo. A continuación se le daba el seguimiento que requería en particular el problema.

A continuación mencionare algunos casos muy frecuentes en mis actividades y como se actuaba en el cierre de tickets

Problemas de Alta utilización

Como los problemas de alta utilización en las líneas de transmisión los solucionábamos en Primer nivel de operaciones, entonces aquí se “limpiaban” y cerraban. Cuando la curva de utilización se había mantenido en su habitual rango por un periodo de tiempo que consideráramos adecuado, entonces “limpiábamos” el ticket poniendo los comentarios respectivos. También cerrábamos el ticket a continuación.

Regularmente lo que encontrábamos en este tipo de eventos eran espigas en la utilización de la línea. Esto es, por un corto periodo de tiempo la carga se incrementaba notablemente, sin embargo regresaba a su rango habitual en el cual se mantenía.

Con la Pantalla grafica de la red veíamos como se había comportado en las últimas horas y estos valores los podíamos comparar con días o semanas previos y sacar conclusiones.

Si el ticket había requerido una investigación mas profunda y se había enviado al Segundo nivel de operaciones, entonces éste grupo lo “limpiaba” con las anotaciones respectivas, el tiempo adecuado y era devuelto a nosotros para su cierre. Únicamente confirmábamos que su rango de carga estuviese bien y lo cerrábamos.

Una vez que se había encontrado que el tráfico de información que circulaba por la línea de transmisión se había mantenido en su porcentaje de operación habitual por un determinado periodo, se concluía que no había ningún problema en la línea. Por tanto, se limpiaba y cerraba el ticket con una nota indicando que la utilización había permanecido en sus valores normales por el periodo de monitoreo.

Problemas de inestabilidad en una interface

Para los problemas de INESTABILIDAD EN INTERFACE, el ticket era “limpiado” con el tiempo en que la interface había “subido” por ultima vez y desde entonces se mantenía operable. Con esto esclarecíamos a que hora el problema había dejado de ocurrir y se había resuelto. En otro caso, seguramente el ticket se había enviado al Segundo nivel de operaciones por que la línea se había encontrado abajo cuando el ticket se creo y se reviso la línea en el router. En este caso, el Segundo nivel de operaciones le habría dado seguimiento y solución. Entonces pondrían el tiempo de “limpiado” y el ticket era regresado a Primer nivel de operaciones. La tarea final era confirmar que la interface estaba “arriba” y no tenía “bounceos”. Lo hacíamos a través de la Pantalla de comandos, viendo los últimos logs (mensajes) de “caída” y “subía”, así como con el status de la interface con show interface <interface>. Cuando confirmábamos que todo estaba bien, cerrábamos el ticket poniendo algo como “interface esta arriba y estable. Problema resuelto.”.

Problemas de fallo de hardware/software

Cuando se había hecho algún remplazo de una pieza de hardware ó algún trabajo de configuración o actualización de software, el ticket lo “limpiaba” el Segundo nivel de operaciones con el tiempo correcto en que el hardware o software volvió a operar. En Primer nivel de operaciones únicamente revisábamos que el equipo y las interfaces trabajaran con trafico “en vivo” y no observáramos nada extraño. A continuación cerrábamos el ticket con algún comentario como “tarjeta de la ranura 2 fue remplazada satisfactoriamente. Interfaces operan correctamente.”. En problemas de configuración o actualización de software el cierre del ticket era similar; verificábamos que los componentes y enlaces operaran bien, poníamos los comentarios en el ticket y, lo cerrábamos.