UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

GESTIÓN Y SOPORTE EN EL CENTRO DE OPERACIÓN DE LA RED DE DATOS (COR) DE UNA OPERADORA TELEFÓNICA.

INFORME DE TRABAJO

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A :

DANIELA LÓPEZ LÓPEZ

DIRECTOR:

DR. MIGUEL MOCTEZUMA FLORES

CD. UNIVERSITARIA, MAYO 2008

Reconocimientos

A la Universidad Nacional Autónoma de México, especialmente a la Facultad de Ingeniería, por abrirme sus puertas y haberme permitido realizar mi carrera profesional, formando parte de esta gran Univerisadad, de la cual siempre me sentiré orgullosa.

A todos los profesores que me brindaron sus conocimientos y que con sus consejos y enseñanzazas, me permitieron concluir esta etapa profesional.

A la empresa para la cual laboro, ya que gracias a ella he adquirido el conocimiento necesario para la realización de este trabajo, y por la oportunidad que me ha dado para poderme realizar como profesionista en el área que me interesa. Y al Dr. Moctezuma por su apoyo durante la realización de este trabajo.

A todos mis compañeros y amigos con quienes conviví en el transcurso de mi carrera, y a las diferentes personas que se van conociendo a lo largo de este camino, a quienes les agradezco su apoyo, consejos y enseñanzas.

A todos ellos mi mas profundo y sincero reconocimiento.

Agradecimientos

En primer lugar agradezco a Dios por todas las cosas buenas que me ha dado, por mi vida y las grandes que bendiciones que he recibido a lo largo de ella, por mis padres y mis hermanos, y por esta etapa profesional que me ha permitido concluir, gracias por que me haz brindado la Fe y la Esperanza necesaria en mi vida.

A mis padres Luis e Isabel, es el más profundo agradecimiento, por que gracias a su esfuerzo nos han brindado a mis hermanos y a mí el apoyo y los medios necesarios para poder realizarnos profesionalmente, por todo su amor y consejos les agradezco profundamente y saben que los amo. A mis 4 hermanos a quienes quiero mucho: Ángeles, Lety, Elisa y Fernando; a Jonh y mis sobrinos por que me han brindado grandes momentos gracias por todo su apoyo, saben que los quiero.

Agradezco a todos mis amigos y amigas a quienes siempre me han dado buenos consejos, la lista sería muy grande pero saben que los llevo en mi corazón de una manera muy especial, sólo quiero agradecer especialmente a Mariana, ya que con ella conviví toda la carrera y compartimos muchas cosas y situaciones similares gracias niña por tu amistad y buenos consejos, en general a agradezco a mis amigos de la carrera, del Instituto, de Telcel y a la bandaly.

INDÍCE

1. Objetivo

Las actividades profesionales realizadas en el área de Operación y Mantenimiento contribuyen a la detección y la solución de problemas que pueden afectar la disponibilidad de la Red de Datos de una empresa de Telecomunicaciones que brinda Servicios de Telefonía Celular tanto a nivel Nacional como Internacional.

Es por ello, que se considera de suma importancia indicar cuales son las plataformas de gestión y soporte, así como las actividades profesionales que realiza el área de Ingeniería de Soporte, en el Centro de Operación de la Red de Datos, para mantener los servicios, gestión y operación de la Red de Datos en un 99.99%.

2. Introducción

Esta empresa, Operadora de Telefonía Celular dedicada a la comercialización de telefonía móvil y datos inalámbricos. Tiene presencia en todo México. Es subsidiaria de la empresa mexicana América Móvil, una filial de CARSO Holding Telecom. A la fecha es la empresa número uno y la de mejor calidad de servicio de telefonía móvil en México.

En 1984 la empresa obtiene el nombre de Radiomovil Dipsa bajo su marca comercial Telcel, convirtiéndose en una empresa proveedor líder de servicios de comunicación inalámbrica, en México mantiene concesiones para operar en las nueve regiones de México, usando dos bandas del espectro radioeléctrico (banda “B” – 800 MHz y banda “D” 1900MHz).

Los comienzos de esta Operadora en la telefonía celular fueron en 1987, cuando la SCT autoriza la instalación del sistema celular en la ciudad de Tijuana. Dos años más tarde en esta misma Ciudad comienza a brindar el servicio a usuarios mexicanos como estadounidenses. En febrero de 1990 se inicia la comercialización de la telefonía celular en el Distrito Federal y área metropolitana; cinco meses después cubre las ciudades de Cuernavaca y Toluca, así como Valle de Bravo. De esta forma, logra rebasar los pronósticos más ambiciosos en número de usuarios, que siguen incrementándose mes con mes. Sobre todo en la ciudad de México y zona conurbana, en un caso extraordinario en el mundo.

Actualmente esta Operadora, es un sistema telefónico móvil con infraestructura propia que opera en todo México, ofreciendo servicio de gran tecnología móvil, gracias a la concesión nacional con la que contaba en 1990 el número de usuarios o líneas celulares ha ido incrementando de tal manera que el crecimiento ha sido explosivo llevando a cerrar el año 2000 con 10 millones 500 mil usuarios.

Para el 2002 la Operadora Telefónica lanza la red GSM en nuestro país, marcando la pauta hacia lo que serán los servicios de tercera generación, siendo la primera compañía en México que lanzó esta tecnología, utilizada ya en los países más desarrollados del mundo.

En el año 2003 la Empresa lanza innovadores servicios de valor agregado bajo el concepto Ideas Telcel, con lo que al cierre de ese año sobrepasa los 23 millones de usuarios.

En el 2008 cuenta con más de 50 millones de usuarios y con el 75% de participación a nivel nacional.

Al día de hoy, la Empresa mantiene concesiones para operar en las nueve regiones de México, cubriendo más de 100 mil poblaciones del país, a través de sus redes de comunicaciones para tecnología GSM en 850 MHz y en 1900 MHz. La banda TDMA en 800 MHz será paulatinamente desactivada, ya que es el mínimo de usuarios que se tienen en esa banda actualmente.

La tecnología 3G/UMTS de Telcel ofrece enlaces de banda ancha móviles de hasta 1.5 Mbps por segundo, servicio de video llamada, Televisión en vivo y video en streaming, siendo labor de las distintas áreas del Centro de Operación de la Red (COR) brindar servicios los 365 días del año las 24 horas, para mantener y operar la Red de Comunicaciones a nivel Nacional. La cobertura de 3G hasta el mes de febrero de este año abarca 5 ciudades del país: Mérida, Hermosillo, Guadalajara, León y Cd. de México. A finales de año se espera tener cobertura total en las principales ciudades de México y carreteras.

3. Antecedentes

3.1 Principales actividades del área de Ingeniería de Soporte

En esta sección, se darán a conocer las principales funciones y actividades que se realizan en el **Centro de Operación de la Red de Datos** COR de una operadora telefónica, que brinda servicios a nivel Nacional dividiendo el País en 9 regiones de acuerdo a la **SCT**[1] y a nivel Internacional, donde se interactúa con distintos operadores.

Parte de las actividades profesionales que se llevan a cabo en el área de Ingeniería de Soporte en el COR de Datos son las siguientes:

- **Atención a reportes de usuarios**.

Es una de las actividades más frecuentes, la atención al servicio de Red de Datos, se atiende a los usuarios a través de un reporte en el cual se indica el problema, el cual puede ser: servicios de Tomas de Datos, solucionar conflictos con direcciones **IP**[2] duplicadas, configuración o cambio de **VLANs**[3], se requiere recolectar los datos de usuario, tales

[1] SCT. Secretaria De Comunicaciones y Transportes: En 1977 este Órgano brinda una concesión a la empresa para instalar, operar y explotar un sistema de radiotelefonía móvil.
[2] Dirección IP. Una dirección de 32 bits asignada a un host, usando el protocolo TCP/IP.
[3] VLAN. Virtual LAN. un grupo de dispositivos, conectados a uno o más switches, con los dispositivos agrupados dentro de un único dominio de broadcast configurado a través del switch.las VLANs permiten a los administradores de redes separar los dispositivos que están conectados a los switches en redes virtuales, sin separar físicamente a los switches, con esto se obtienen ventajas de diseño al separar el tráfico sin tener que adquirir hardware adicional.

como dirección **MAC**[4] y dirección IP, con estos datos podemos determinar a que capa del modelo **OSI**[5] el usuario tiene el problema y poder dar la correcta solución a este.

Con respecto a la atención a usuarios, se requiere que en horarios fuera de oficina el usuario tenga acceso a los servicios de red desde la comodidad de su hogar, es por ello, que se realizan configuraciones de acceso a la Red vía **VPN**[6] en los Firewalls o **Dial-up**[7] en el servidor que provee el acceso a Internet.

- **Atención a fallas en los equipos de la red de datos**

Gracias a las herramientas de monitoreo, se pueden detectar problemas con equipos o enlaces que provoquen fallas en la Red, se determina el o los equipos involucrados, los cuales son analizados en tiempo real para solucionar la falla en el menor tiempo posible, principalmente las fallas son a nivel de capa 2 y capa 3 del modelo OSI.

Se accesa a los equipos vía **Telnet**[8], se realizan pruebas de interfaces Ethernet / FastEthernet, pruebas de Interfaces Seriales para enlaces Point to Point y para seriales de tarjetas controladoras de enlaces E1, se determina el estado de dichas interfaces y si es posible desde nuestra administracion corregir el problema a traves de los protocolos básicos para la determinición del problema son el **ICMP**[9] Ping y Trace, cuando no es posible corregir el problema desde nuestra administracion se solicita apoyo de los Ingenieros en Sitio, y en conjunto con ellos se determina y corrige el problema.

O bien, se pueden presentar problemas en la convergencia de los protocolos de redundancia o ruteo utilizados en la red, dependiendo del problema el Ingeniero debe de ser capaz de dar un correcto **troubleshooting**[10] a la red de datos.

Cuando se determina que el problema es causado por el Hardware de los equipos se procede a levantar reportes con proveedores.

---

[4] MAC. Media Access Control. Término utilizado en la capa de enlace de Datos por el IEEE.
[5] OSI. Open System Interconnection. Un modelo de la arquitectura de red desarrollado por el ISO. El modelo consiste de 7 capas, cada una de las cuales especifica funciones particulares de la red, definidas en el capitulo 5.
[6] VPN. Virtual Private Network. Es el proceso de comunicación segura entre dos dispositivos, donde los paquetes pasan sobre alguna red pública que no es segura, típicamente Internet. VPN encripta paquetes así que la comunicación es privada y autentica la identidad de los puntos finales, endpoints
[7] Dial Up. Conexión a red a través de un MODEM y un Proveedor de Servicios de Internet ISP.
[8] Telnet. Protocolo de la capa de Aplicación. Telnet es usado para la conexión remota, permitiendo a los usuarios autenticarse en el sistema remoto, haciendo uso de los recursos como si ellos estuvieran conectados localmente en el sistema.
[9] ICMP. Internet Control Message Protocol. Un protocolo de capa de Red que reporta errores y provee otra información relevante a el proceso de paquetes IP
[10] Troubleshooting. Termino utilizado en Redes de Datos para la solución a distintitos problemas que puedan presentarse en la operación de esta, ya sea a nivel de capa 1, 2 y 3.

Todo este análisis se lleva a cabo en cado uno de los elementos que integran la red de datos y en el trasporte de datos de la red **GPRS**[11]; los cuales serán presentados en las distintas secciones que conforman este informe.

- **Atención a reportes de la red GPRS**

Principalmente se atienden reportes de **APNs**[12]. En general, se realiza cualquier cambio de configuración de APNs, lo que involucra el manejo de equipos de la red GPRS el cual será detallado en la siguiente sección, se analizan y se solucionan fallas de los distintos APNs, se realizan capturas de tráfico de un segmento de red o un móvil en especifico, y capturas para los servicios de Roaming Internacional así como la configuración necesaria para que se pueda brindar este el servicio de navegación a través de GPRS.

En resumen, se deben tener en cuenta las siguientes metas: solucionar los problemas que afecten el servicio de la red de Datos en el menor tiempo posible, es decir, mantener el soporte y operación a la Red LAN a nivel Nacional, documentando en bitácora las posibles fallas y la solución de estas. Y segundo atender repotes de los usuarios de región R1-R9 en un tiempo menor a 24hrs. La ejecución de Órdenes de Trabajo y Solicitudes de Cambio en el menor tiempo posible.

3.2 Herramienta utilizada para la administración de la red de datos

Dentro de la administración y gestión de una red de datos de gran tamaño, como es el caso de esta Operadora Telefónica, es de suma importancia llevar un orden en los cambios que pudiesen afectar el servicio a la red y en caso de que esto ocurra tener una fecha y hora exacta en la cual se puedan realizar intervenciones a la red de datos, para ello es indispensable contar con alguna herramienta que nos ayude a llevar los registros y estadísticas que a su vez miden el trabajo realizado por cada uno de los integrantes del área.

A partir de las actividades básicas de gestión, soporte, almacenamiento de eventos, procesamiento y entrega de reportes estadísticos es como se puede conocer el estado de la infraestructura técnica que esta en operación en la Red Celular.

[11] GPRS. General Packet Radio Services. Detallado en la sección 4.2

[12] APN. Access Point Name. Se puede definir como una red IP a la cual un móvil puede ser conectado, o bien, los parámetros utilizados para la conexión del móvil y una opción en particular parecida a una URL de Internet en el teléfono móvil.

Para poder documentar y tener un orden en los cambios y procedimientos en la red de datos utilizamos la herramienta llamada Remedy.

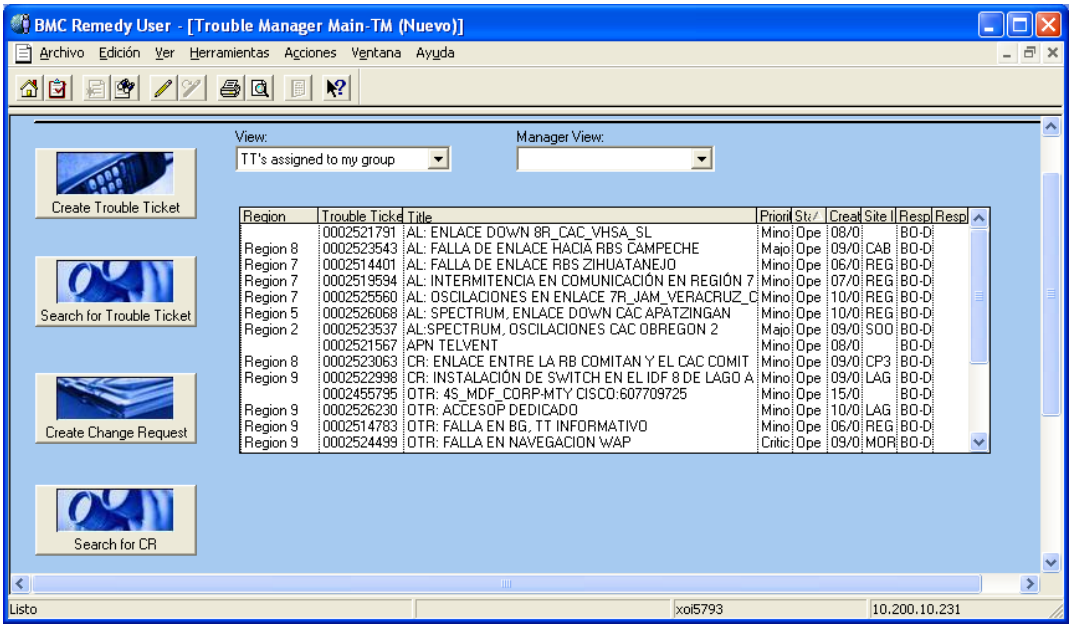


Figura 1. Herramienta de Administración Remedy

La plataforma Remedy es utilizada para llevar el control del flujo de trabajo de las actividades que permitirán atender un incidente que afecta el desempeño y disponibilidad de los diferentes elementos que integran una Red Celular o de Telecomunicaciones.

A través de Remedy se llevan a cabo la ejecución de:

- **Trouble Tickets** (TT). Reporte en el cual se da seguimiento a un problema específico de cualquier elemento de la Red
- **Solicitudes de Cambio** (CR). Reporte en el cual se requiere realizar algún cambio de configuración a cualquier elemento de la Red
- **Ordenes de Trabajo** (WO). Reporte en el cual se pide apoyo de Ingenieros en Sitio
- **Rutinas de Mantenimiento** (RM). Reporte en el cual se piden realizar tareas a ciertos equipos para dar mantenimiento como su nombre lo indica
- **Reportes de Incidentes de Clientes** (CPD). Reporte en el cual se brinda atención a algún usuario o cliente de la Operadora Telefónica
- **Solicitudes de usuarios de a Acceso a Plataformas**. Reporte en el cual se pide realizar las altas o bajas para ingresar a las Plataformas de la Red

Gracias a estos reportes generados por Remedy se pueden clasificar las actividades que se tienen que realizar por cada uno de los diferentes departamentos que integran el Centro de Operación de la Red.

4. Participación Profesional en la Gestión y Operación de la Red de Datos

4.1 Plataformas utilizadas para la gestión y soporte a la red de datos

Las plataformas de gestión y soporte de la red de telecomunicaciones (voz, datos, transmisión, GPRS) de esta Operadora Telefónica son un conjunto de sistemas que interactúan entre si con el fin de apoyar a las diferentes Áreas de la Dirección de Operación y Mantenimiento en las actividades de atención a incidentes que afectan la disponibilidad de los diferentes elementos que integran la Red Celular.

La información generada por las plataformas de gestión y monitoreo de la red (alarmas, estadísticas, mediciones) es almacenada en algún equipo que dependiendo de la capacidad y requerimientos del área usuaria, esta información puede ser guardada por varios meses.

Este capítulo, tiene como objetivo dar a conocer la secuencia y operación de las plataformas utilizadas para monitorear las alarmas operativas de los equipos (routers, firewalls, switches, servidores de acceso remoto, equipos que integran la Red de GPRS) y enlaces de la red de datos a nivel nacional. Para su pronta solución a fallas afectando

en lo menos posible las aplicaciones y servicios que hacen uso de esta Red de Datos, además de garantizar la disponibilidad de la Red Celular en un 99.99%

La pronta atención de las alarmas ayuda a tener una mejor administración de la red, así como la prevención de fallas críticas que afecten la operación del flujo de la información de las aplicaciones de la red. El orden de la atención de las alarmas es de acuerdo a alarmas críticas, mayores y menores realizando solamente el borrado de esta última.

4.1.1 Operación y soporte con la plataforma SPECTRUM

Spectrum, es una aplicación avanzada de software para la administración de redes, que permite monitorear de forma confiable el estado de los diferentes dispositivos existentes en la red. Brindando al administrador la facilidad de localizar un problema y sus posibles fallas y disminuir el tiempo de respuesta para la solución de cualquier problema relacionado con la red de datos.

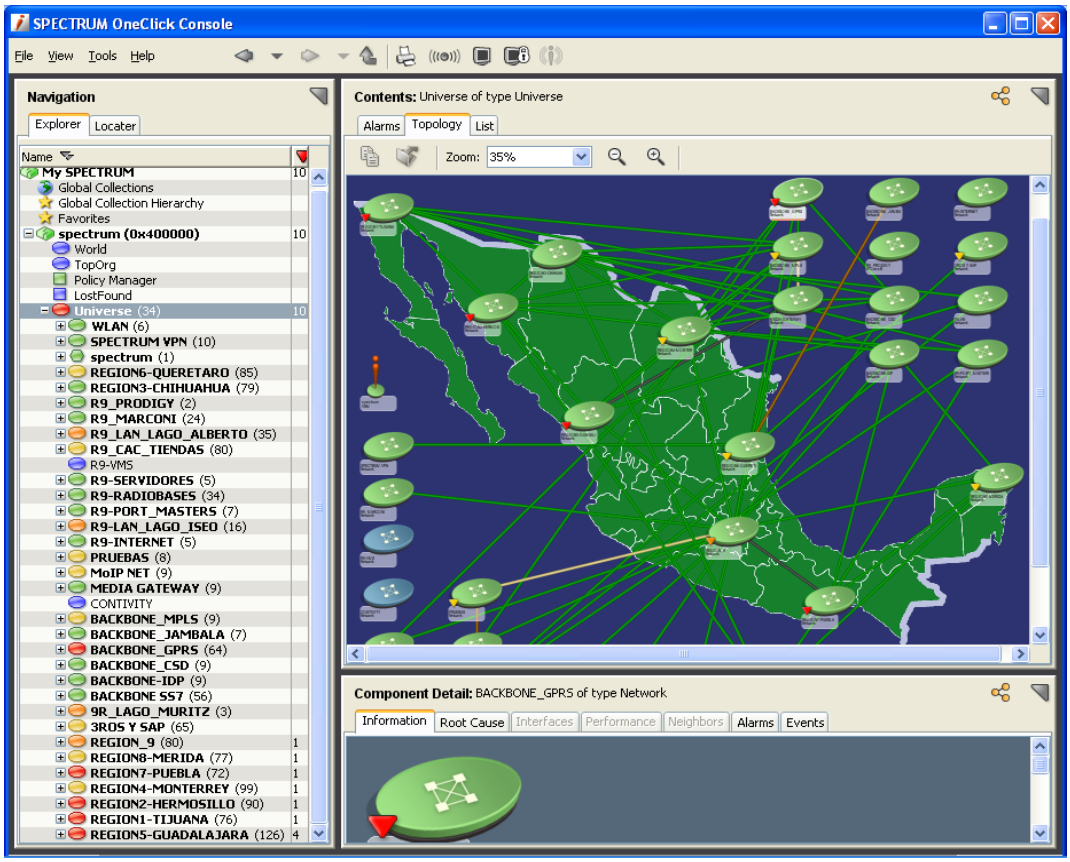


Figura 2. Modelado de la Red de Datos a Nivel Nacional con Spectrum

Spectrum, trabaja bajo una arquitectura Cliente–Servidor, donde el *Server* es el encargado de almacenar y actualizar los modelos de red y dispositivos, y el cliente, representado a través de la **Interfaz Gráfica del Usuario** GUI despliega la información contenida en la base de datos del Server, presentando un listado de las alarmas en cada uno de los equipos.

La vista de localización representa a la red en términos de localidad física, y en términos de la estructura corporativa, figura 2. En esta empresa, para el diseño de la red de datos se sigue el modelo de Red Jerárquico, compuesto por 3 capas Acceso, Distribución y Core (Backbone).

Esta arquitectura es manejada y modelada en Spectrum en las 9 regiones del país, teniendo en el Centro de Operación de la Red la visibilidad de todos los equipos a nivel nacional.

Spectrum genera mensajes de algún tipo de dispositivo modelado, a través de protocolo SNMP[13]. De esta forma podemos obtener del equipo alertas, eventos y alarmas.

Por último, cabe señalar que en Spectrum se encuentran modelados únicamente Routers y Switches, donde para cada uno de ellos se modelan todas las interfaces que tiene el dispositivo, tenemos la interfaces Ethernet, FastEthernet, seriales, en su caso, si están configuradas y modeladas, también nos muestra las interfaces Multilink.

4.1.2 Operación y soporte con la plataforma CONCORD

Concord, es una herramienta de Software administrativa y de análisis end to end, en el desempeño y disponibilidad de la Red de Datos mediante reportes, la cual ofrece soluciones que maximizan y optimizan la disponibilidad de recursos de Red, Aplicaciones y Sistemas (servidores), a través de la detección de fallas, degradaciones de servicio, análisis de tráfico, disponibilidad de servicio, en cada una de las áreas respectivas.

Con esta herramienta es posible: analizar y generar reportes sobre el desempeño y disponibilidad de tecnologías de Red como por ejemplo: Switches, Routers, **RAS**[14], **Frame Relay**[15], **ATM**[16], entre otros. Además de monitorear el desempeño de servidores mediante notificación de fallas de procesos.

[13] SNMP. En la sección 5 se explica el funcionamiento del Protocolo
[14] RAS. Remote Access Services. Se refiere a cualquier combinación de Hardware y Software que habilita el acceso remoto a herramientas de información que típicamente residen sobre una Red
[15] Frame Relay. Un estándar internacional a nivel de la capa de datos, que define la capacidad para crear un servicio de frame-switched (paquetes conmutados), permitiendo a los dispositivos DTE (típicamente Routers) enviar datos a muchos otros dispositivos usando solo una conexión física para el servicio de Frame Relay.

La herramienta provee información sobre que tipos de aplicaciones consumen mayor tiempo de procesamiento en el Central Processing Unit CPU. Permite monitorear y administrar la disponibilidad, desempeño, tiempo de respuesta de las aplicaciones, que genere tráfico **TCP / IP**[17]. Midiendo el tiempo total de la transacción y separándolo en el tiempo de red, usuario y servidor.

Todos los servicios que se brindan con esta herramienta se realizan a través del protocolo SNMP.

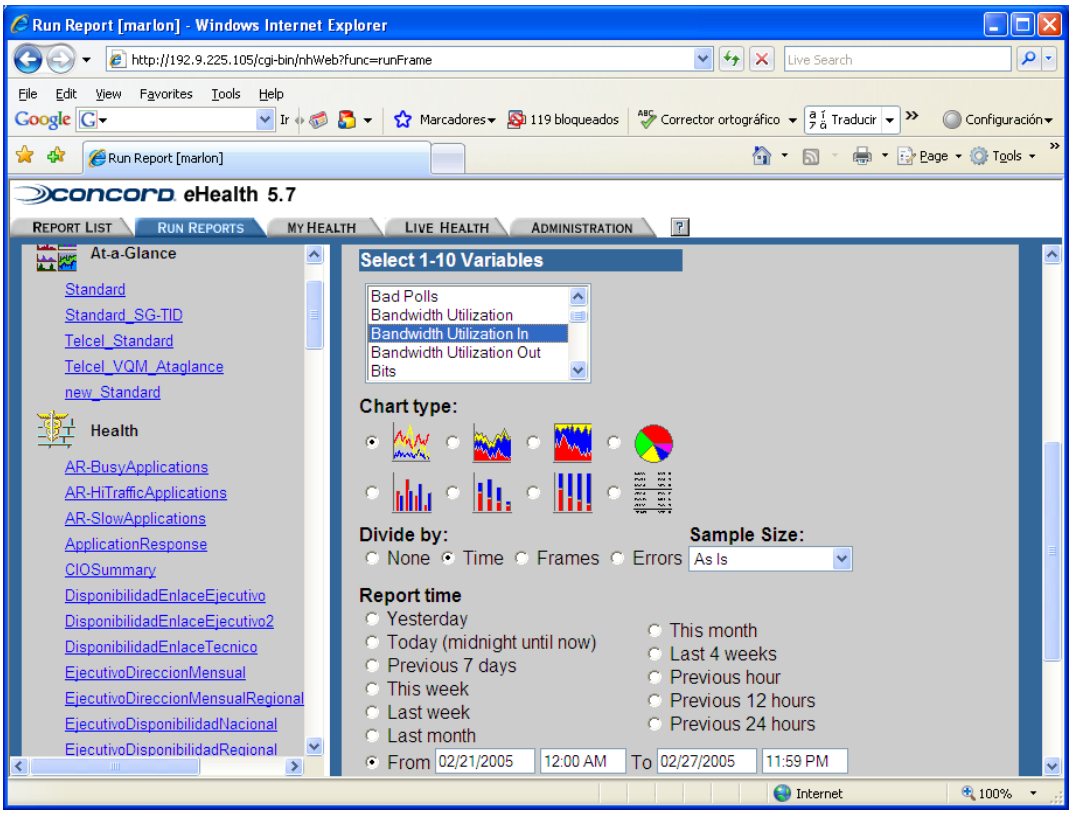


Figura 3. Generación de Reportes a través de CONCORD

Por el momento, el COR utiliza más la herramienta para verificar el estado de los enlaces hacia las distintas regiones del país, generando reportes de utilización de ancho de banda en cada uno de ellos, con la finalidad de mantener un registro de la capacidad de los enlaces y evitar la saturación de estos. Generalmente, este es el soporte que se brinda con esta herramienta, obteniendo graficas y estadísticos de la ocupación de enlaces puede ser en tiempo real, o bien, se guarda en memoria la actividad de las últimas 4 semanas por cada uno de los

[16] ATM. Asynchronous Transfer Mode. El estándar internacional para retransmitir células en las cuales múltiples tipos de servicios (tales como voz, video y datos) están convergiendo en una longitud de célula fija. esto permite que el procesamiento ocurra a nivel de Hardware.
[17] TCP/IP. Transmission Control Protocol/Internet Protocol. un nombre común para la pila de protocolos desarrollada por el departamento de defensa de US en 1970 para soportar la construcción de redes a nivel mundial.

equipos que se tienen dados de alta en esta plataforma. Actualmente se tienen configurados todos los enlaces desde R1 hasta R9. Cuando un usuario de cualquier región reporta lentitud en sus aplicaciones, algunas veces este problema se presenta con más frecuencia en los **Centros de Atención a Clientes** CACs; esta es la principal herramienta usada, aunada al troubleshooting que brinda el ingeniero para determinar el problema. Cuando se descubre que hay saturación debido a que los enlaces tienen anchos de banda muy bajos, se realiza un requerimiento con el área corporativa para que genere las Ordenes de Trabajo necesarias y se brinde el apoyo necesario para que los Ingenieros de Campo levanten nuevos enlaces o es su caso se realice el incremento, realizando desde el COR de Datos las configuraciones necesarias en las controladoras y seriales de los Routers para que se complementen los enlaces.

4.1.3 Operación y soporte con la plataforma Cisco Works

Cisco Works, es una plataforma para la administración de equipos Cisco a través de forma gráfica, figura 4. Trabaja a través del protocolo SNMP.

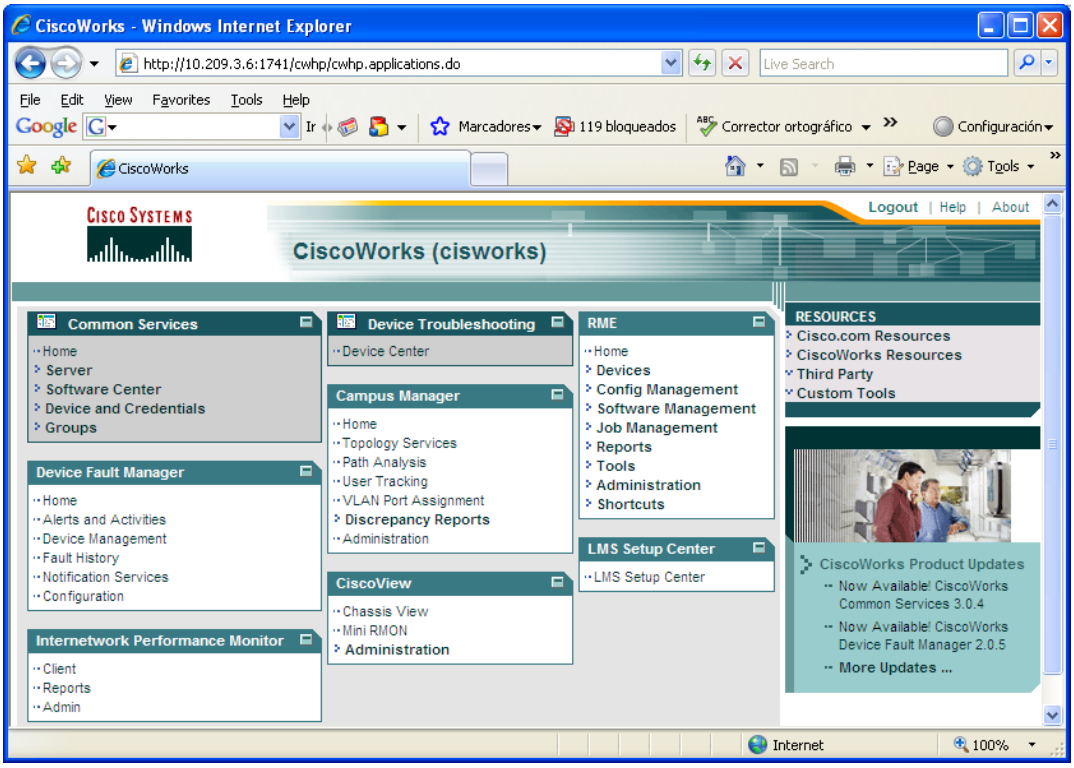


Figura 4. Vista de la plataforma de administración Cisco Works

Se determinan los equipos que serán dados de alta en la plataforma, se realiza el modelado de estos dispositivos, es decir se configuran en el software de esta plataforma. Para la red de datos de esta Operadora Telefónica, se dieron de alta Switches y Routers de Región 1 a Región 9.

A través de las opciones con las que cuenta esta plataforma, en el Centro de Operación de la Red, se realizan las siguientes tareas: generación de mapas de la topología de la red, programación tareas de configuración a uno o varios dispositivos, siempre y cuando la configuración sea la misma para todos ellos, estas tareas pueden ser ejecutadas inmediatamente o bien programando el día y hora indicada en que se requiere realizar la configuración. Una vez ejecutada la tarea, se muestra un reporte detallado indicando el resultado de esta misma.

A través de la interface gráfica de la plataforma se puede observar el estado de la caja de un dispositivo modelado, en tiempo real, en este caso de Switches y Routers, de esta forma podemos ver el estado de los LEDs de las tarjetas y determinar que tipo de problemas puede tener algún equipo.

Se pueden ejecutar búsquedas de un dispositivo vía IP, hostname, dirección MAC de una PC, o por modelo. Se pueden obtener reportes de tareas ejecutadas o programadas, la vista en tiempo real de las interfaces y tarjetas que contiene el dispositivo.

4.1.4 Operación y soporte con la plataforma NetAct

NetAct es la herramienta utilizada para la gestión y soporte de los elementos que integran la red de GPRS, que esta a cargo del departamento de Datos, en este caso el encargado del modelado de los equipos y de verificar el buen funcionamiento de esta plataforma es el proveedor Nokia. El COR tiene acceso a la herramienta vía GUI para el monitoreo, figura 5.

Gracias a esta herramienta se lleva a cabo el monitoreo de la Red GPRS en tiempo real.

Generalmente se envían alarmas que son mayores y menores, se da prioridad a alarmas críticas ya que son las que nos indican el estado físico del dispositivo, o bien si existe algún problemas de configuración dentro del equipo que pueda afectar el servicio.

Generalmente los problemas que ocurren con estos equipos son atendidos por el proveedor. El uso de esta herramienta se limita únicamente al monitoreo, generación de reportes del estado de la Red, o bien obtención de históricos de cada uno de los elementos.

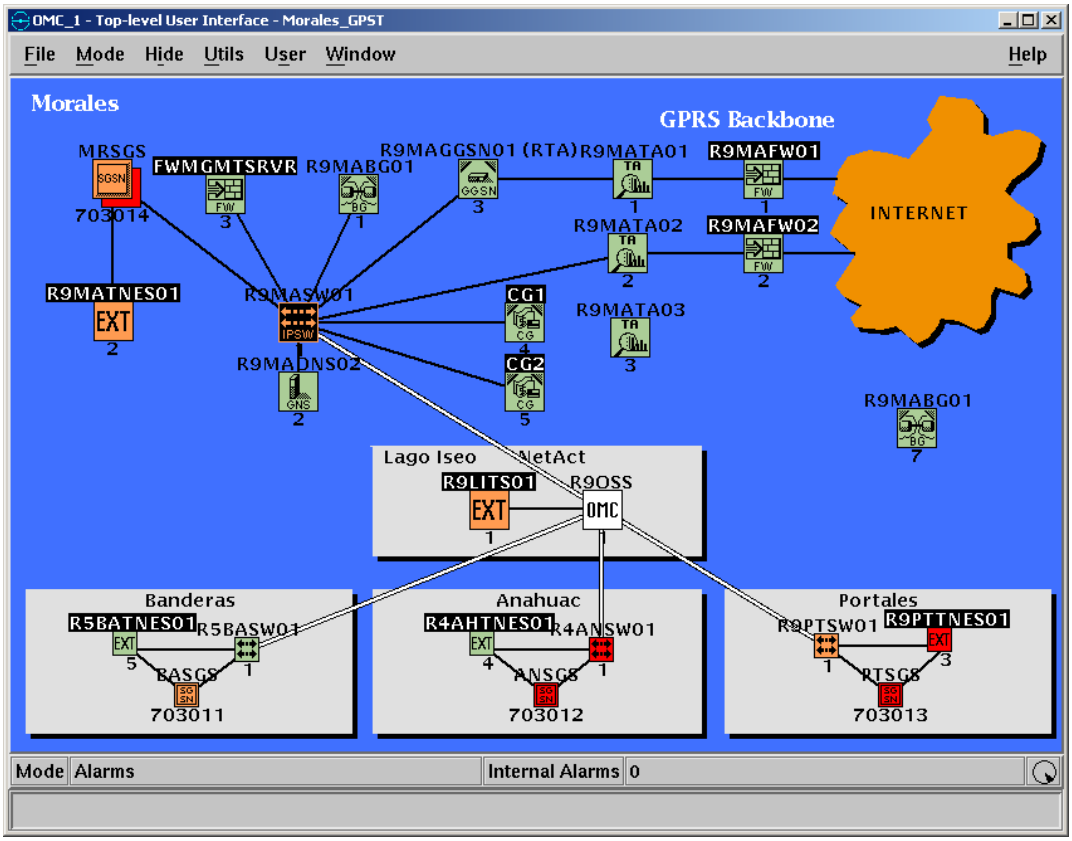


Figura 5. Monitoreo de la Red GPRS a través de NetAct

Cabe señalar que esta plataforma funciona gracias al envió de mensajes SNMP. En la sección 4.2, se detalla la participación profesional que se tiene además del monitoreo en la Red de GPRS.

4.2 Gestión y soporte a la Red de GPRS.

Las comunicaciones móviles y los datos están convergiendo rápidamente entre ellas, para ofrecer nuevos servicios que cumplan con las expectativas de los usuarios, en donde el uso de Internet, Intranet o del correo electrónico es más común hoy en día.

Dada la gran demanda que existe por comunicaciones más rápidas y con mayor ancho de banda, el **European Telecommunications Standards Institute** ETSI ha estandarizado varias tecnologías para permitir a **GSM**[18] integrarse a los sistemas de comunicación de tercera

[18] GSM. Sistema Global para comunicaciones Móviles, es un sistema estándar para comunicación utilizando teléfonos móviles que incorporan tecnología digital. Definido originalmente como estándar Europeo abierto para que una red digital de teléfono móvil soporte voz, datos, mensajes de texto y roaming en varios países. El GSM es ahora uno de los estándares digitales inalámbricos 2G más importantes del mundo.

generación 3G conocidos como **UMTS**[19], para el caso que nos ocupa enfocaremos nuestra atención en la tecnología de GPRS, debido a que en los meses de febrero y marzo del presente año no ha sido liberado al 100% el servicio de la tecnología 3G en todas las regiones.

General Packet Radio Services o GPRS es una tecnología digital de telefonía móvil.

GPRS es considerada la generación 2.5, entre la segunda generación GSM y la tercera UMTS. Proporciona velocidades de transferencia de datos de 110 kbps máximos teóricos, superiores a las proporcionadas por la tecnología GSM 9,6 kbps máximos teóricos, especialmente es útil para conectar a Internet

GPRS es una modificación de la forma de transmitir datos en una red GSM, pasando de la conmutación de circuitos en GSM (donde el circuito está permanentemente reservado mientras dure la comunicación aunque no se envíe información en un momento dado) a la conmutación de paquetes.

GPRS es un servicio de conmutación de datos por medio de paquetes que incrementa la utilización de canales de radio GSM para la transmisión de datos a través del protocolo TCP/IP para aplicaciones como Web Browsing y transferencia de archivos. Esto significa que si no se envía ningún dato por el usuario, las frecuencias quedan libres para ser utilizadas por otros usuarios.

4.2.1 Arquitectura de la Red GPRS

Cuando se hace una petición de celular a la Red Internet, GSM. El proceso se inicia en el teléfono celular, que al originar la solicitud (llamada) es identificada por la estación base más cercana y esta a su vez, por la **Controladora de Estaciones Base** BSC. A través de la controladora, la solicitud se vincula al **Serving GPRS Support Node** SGSN nodo encargado de soportar el servicio de GPRS, que finalmente la direcciona a la compuerta **Gateway GPRS Support Node** GGSN para permitir la conexión a Internet.

[19] UMTS. Servicios Universales de Telecomunicaciones Móviles, es una de las tecnologías usadas por los móviles de tercera generación 3G. Sucesor de GSM, también llamado W-CDMA. Utilizada para teléfonos móviles y otros dispositivos; sus tres grandes características son las capacidades multimedia, una velocidad de acceso a Internet elevada, la cual además permite transmitir audio y video a tiempo real; y una transmisión de voz con calidad equiparable a la de las redes fijas.

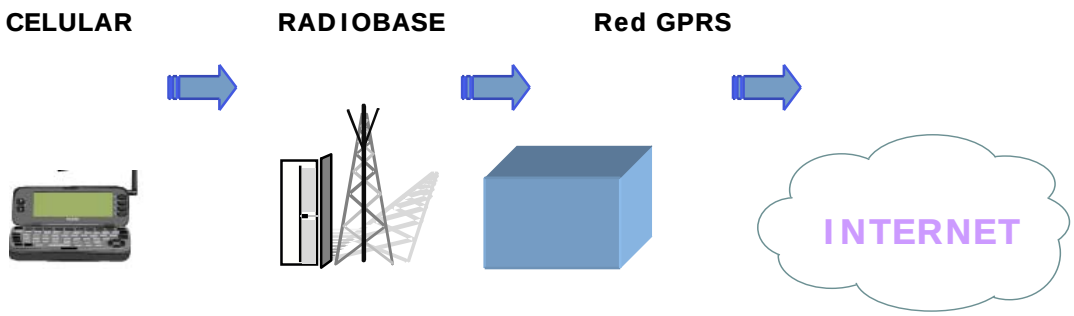


Figura 6. Petición de Celular a Red Internet a través de GSM

La figura 6 muestra de forma muy general como un móvil ingresa a la red GPRS. Para los fines de este trabajo nos enfocaremos más en la arquitectura de la Red GPRS, que es donde se lleva a cabo en intercambio de datos a través de Internet y donde realizamos labores de Ingeniería para mantener la disponibilidad de esta Red.

El sistema GPRS trae consigo nuevos elementos a la red GSM. El nodo **SGSN** y el nodo **GGSN**. Existen otros elementos como el **Border Gateway** BG el cual se necesita para comunicar las redes GPRS a nivel local o mundial y la creación de una red IP para intercomunicar los SGSNs con los GGSNs o con el BG. Además de los elementos de cobro como el **Charging Gateway** CG. La arquitectura de los elementos que integran la Red GPRS, tiene un esquema similar al de la figura 7.

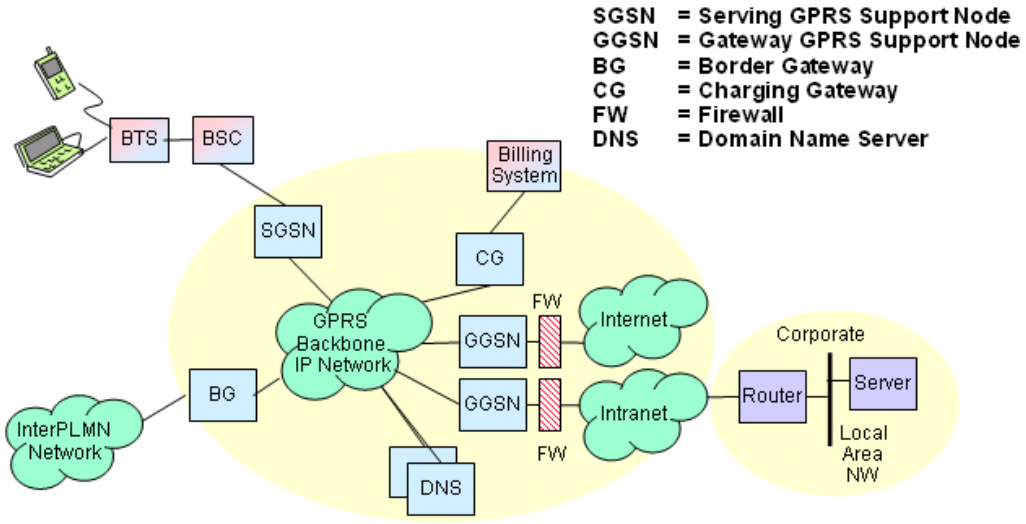


Figura 7. Core GPRS. Elementos que conforman la Red GPRS

En la arquitectura real de esta Operadora Telefónica, se cuenta con 10 cajas de SGSNs, cada una ubicada a nivel nacional desde Región 1 hasta Región 9, 1 Border Gateway, 1 Traffic Analyzer elemento que remplaza al Charging Gateway, utilizado para cobro, 2 DNSs, 2 GGSNs,

2 Firewalls; estos últimos ubicados en Región 9, brindando servicios a nivel nacional con un diagrama similar al mostrado en la figura 8.

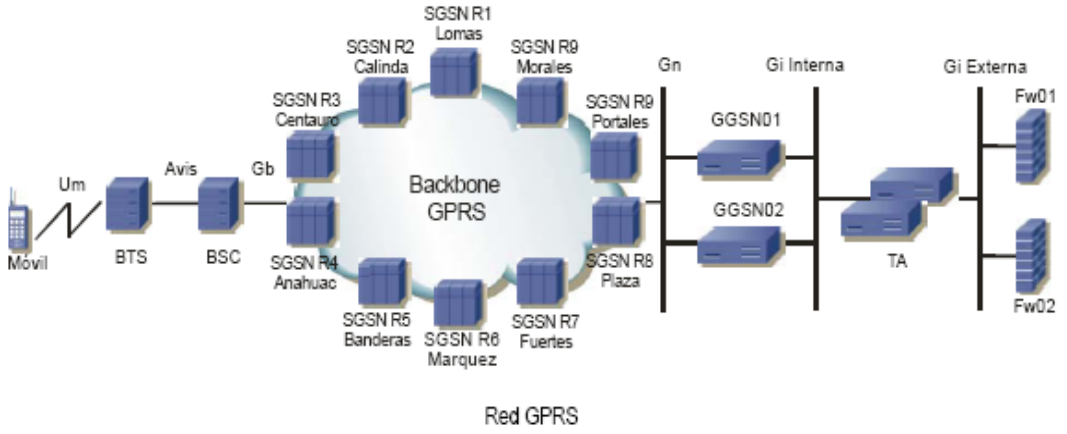


Figura 8. Topología actual de la red GPRS de la operadora telefónica

En la sección 4.2.3 se detalla la participación profesional que se realiza sobre cada uno de estos elementos, cabe señalar que todos estos elementos se integran al Backbone de IP a través de la interface llamada ***Gi***[20] .

En el apartado siguiente se presenta una breve explicación del funcionamiento de la Red GPRS sobre la red de datos**.**

4.2.2 Transporte de datos en la Red de GPRS

Para intercomunicar todos los dispositivos de la red GPRS, es necesario contar con una red de transporte IP, para el caso de esta Operadora Telefónica se cuenta con una red de datos bastante amplia que cubre las 9 regiones del País, permitiendo el transporte de datos sobre la red GPRS.

El transporte y la conexión a la red GPRS se puede resumir de la siguiente manera:

- ***Administración de la sesión y movilidad***

Dentro de todos los procesos que existen en la administración de una llamada en las redes GPRS, podemos encontrar los dos más importantes para acceder a una aplicación determinada utilizando la

[20] Gi. Interface GPRS que permite la comunicación entre GGSN y Redes IP.

Red de GPRS como tecnología de acceso, estos son el *registro* **"attach"** y la *activación de un contexto de datos* **PDP[21] context**.

a) Registro a la red

Antes de utilizar los servicios de GPRS, el equipo debe registrarse en un SGSN de la red, lo cual es conocido como attach GPRS. El nodo SGSN confirma en el **HLR**[22] que el móvil tenga permiso para utilizar la red GPRS. Una vez que se completa el attach, el equipo esta físicamente conectado a la red GPRS.

b) Contexto de datos

Es una asociación lógica que permite enlazar al móvil con la Red de Datos externa a través de los nodos GPRS. Se genera una vez que el usuario hace la petición a algún servicio, por ejemplo una conexión a Internet. La activación de un PDP context se puede entender como el proceso de conexión hacia una aplicación externa (Internet, corporativos). Este proceso de conexión es autorizado por el SGSN dependiendo de las categorías habilitada en el HLR para un determinado usuario.

- ***Proceso de activación de un contexto de datos***

1. El móvil envía la solicitud para activar un contexto de datos. El móvil invoca un APN y esta es enviado al SGSN

2. El SGSN realiza una búsqueda en el DNS para saber cual es la dirección IP que le corresponde a ese APN. El DNS le envía la respuesta al SGNS

3. EL SGSN direcciona la solicitud del móvil a la IP enviada por el DNS, la cual corresponde al GGSN

4. El GGSN accede a la creación del contexto de datos (PDP context) y le contesta al SGSN

5. El SGSN le confirma su petición al móvil y e completa la activación del contexto solicitado mediante el APN

[21] PDP context. Packet Data Protocol. es una estructura de datos presente entre el SGSN y el GGSN, el cual contiene la información de sesión del subscritor cuando tiene una sesión activa. cuando u móvil quiere usar la red GPRS primero debe realizar el attach y luego activar un PDP context.
[22] HLR: Home Location Register. Registro local de abonados, es una base de datos que contiene la información del usuario, tales como planes de pago y APNs a los cuales tiene acceso.

Cabe hacer mención que este proceso esta dentro de la administración de la movilidad para la Terminal. Un PDP context no se puede llevara cabo si no registra primero el móvil a red GPRS. Cuando el móvil envía la solicitud para la activación de un servicio o aplicación hacia la red de GPRS, lo realiza utilizando un APN o Access Point Name.

El APN, tiene el mismo formato que un URL de Internet por ejemplo **apn.operador.com.mcc[23].mnc[24].gprs** el operador al recibir la petición del móvil revisa en su HLR si el usuario tiene dado de alta en su perfil la categoría de GPRS y si esta tiene aprovisionado el APN solicitado.

Esta es la sintaxis del APN

- El APN Identificador de la Red
  (Ejemplo: apn1.operador.com)

- El APN Identificador del Operador
  (Ejemplo: mnc009.mcc262.gprs)

Dentro de la arquitectura de la red de GPRS la interconexión a los distintos elementos de la red esta clasificada a través de interfaces que corresponden a distintos protocolos, para el caso que nos ocupa analizaremos la interfaz Gi. La cual realiza la conexión de la siguiente manera:

Gi. GGSN a Redes externas. Utilizando el protocolo TCP/IP o GRE[25].

La interface Gi conecta al GGSN y la red de datos externa permitiendo a los suscriptores de GPRS el intercambio de paquetes IP con Internet.

En esta operadora se utilizan Firewalls entre el GGSN y la red externa como método de seguridad y establecimiento de túneles para garantizar el servicio y proteger la red de cualquier ente malicioso.

El diseño de los APNs (Access Point Name) es enviado por el área de diseño y en el Centro de Operación de la Red de Datos nos encargamos de realizar las configuraciones correspondientes en las interfaces Ethernet Gi en los GGSN y diversos equipos por los cuales pasara el APN.

Para la creación de los distintos APNs La asignación de direcciones IP puede ser de manera dinámica o estática en los nodos GGSN. Para la interconexión del APN se utiliza ruteo o encripción mediante túneles GRE como la forma de acceso a Internet.

[23] MCC = Mobile Country Code. Código del País
[24] MNC = Mobile Network Code. Código de la Red
[25] GRE. Generic Routing Encapsulation. Se explica en la sección 5

Durante la creación de un APN es necesario asignar un segmento de direcciones IPs a los móviles que formaran parte de este APN. El móvil con tarjeta GPRS que requiera conectarse al servidor tendrá configurado el APN correspondiente, la asignación de IP a los móviles corresponden a la red del APN y las asigna el GGSN.

Cabe mencionar que el APN puede configurarse en diferentes GGSN pero la asignación del APN desde un móvil se asigna a un sólo GGSN debido a que así lo requiere la aplicación. Dependiendo del direccionamiento asignado el GGSN ofrecerá el servicio después de consultar al servidor de dominios de APN's en la red (DNS de GPRS).

El SGSN y el GGSN elegido establecen una comunicación mediante el protocolo GTP **GPRS Tunneling Protocol** para enviar información que el suscriptor móvil y la red externa que deseen establecer.

De acuerdo a la Arquitectura de Solución de GPRS de la Operadora Telefónica, la interface Gi conecta a los nodos GGSN con el sitio del corporativo. Para separar el tráfico cursado por la interface Gi se manejan por medio de interfaces, cada una de ellas dedicadas a un servicio.

En el caso de que el cliente lo requiera se maneja el uso de túneles IPSec como método de ruteo entre una red de datos IP conectados a la interface Gi, además el uso de IPSec ofrece seguridad y previene de anunciar los segmentos de red utilizadas por los usuarios móviles.

Los GGSN se encargan de la creación del Access Point Name y contienen los segmentos de direcciones de red que serán asignados a los móviles del servicio masivo. Para el caso de los APN con direcciones dinámicas estos dividirán la carga de tráfico, mientras que para el caso de que sean estáticos funcionan en alta disponibilidad con la condicionante de cambiar la dirección del DNS al GGSN que se encuentre disponible en caso de existir alguna falla.

Una vez creado el contexto el tráfico pasa a un equipo llamado **Traffic Analyzer** TA el cual en capa 3 y 4 se encarga de filtrar tanto protocolos como puertos, haciendo más selectivo el tráfico que puede tener acceso al corporativo.

El TA también se encarga de proporcionar los **Call Detail Records** CDR necesarios para tarificar todo el tráfico del APN. Estos equipos trabajan como Cluster lo que permite proporcionar una alta disponibilidad del equipo en caso de falla.

Posteriormente pasa por los Firewall, los cuales trabajan también con Alta Disponibilidad, llegando finalmente a la red de Datos Corporativa.

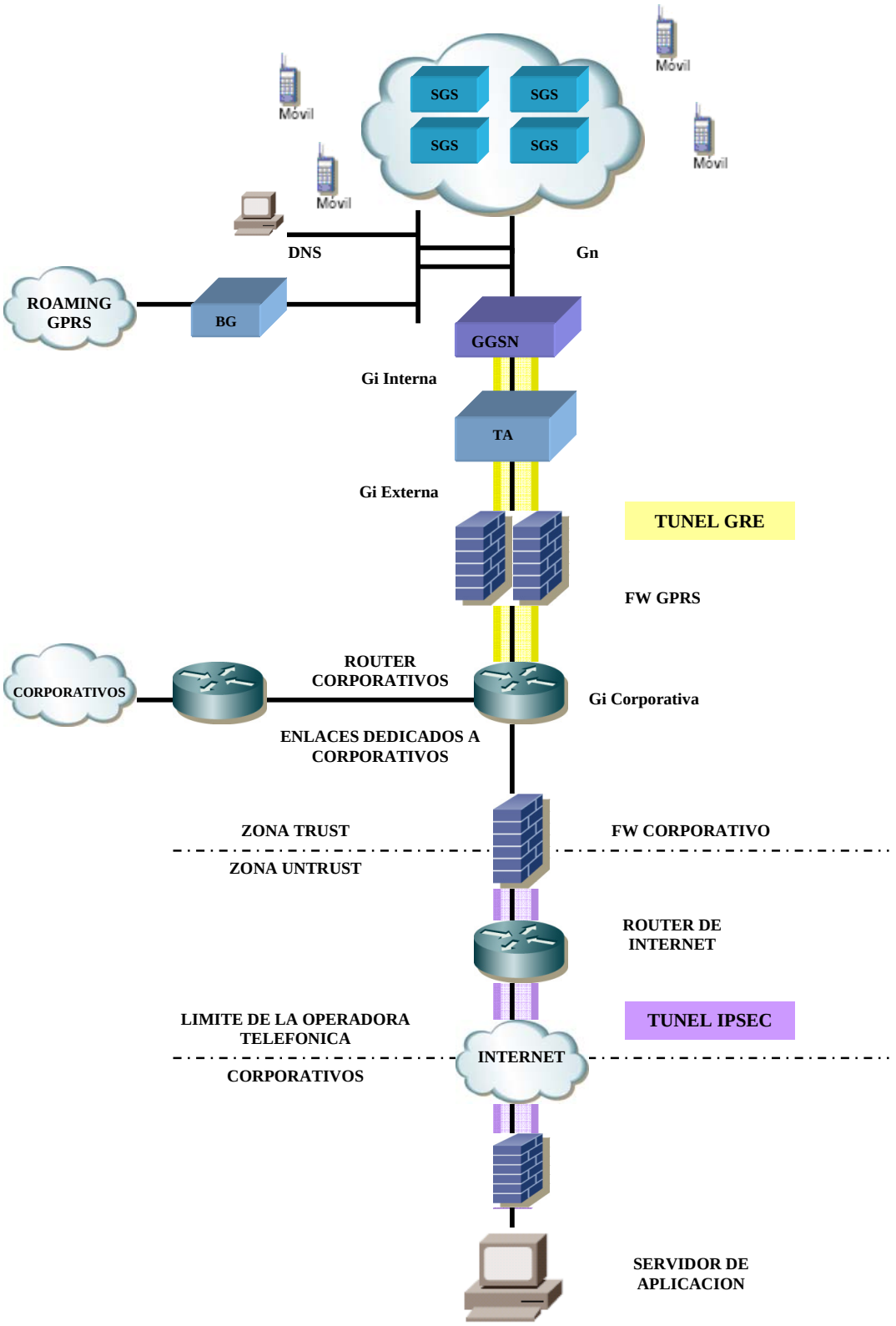


Figura 9. Elementos de redes de datos que forman parte de la integración de un APN en la Red GPRS

4.2.3 Soporte y Participación Profesional a la Red de GPRS

EL soporte que el Centro de Operación de la Red de Datos brinda a la red de GPRS es principalmente en la interface Gi la cual ya se ha descrito anteriormente.

Es necesario que el Ingeniero de Soporte, quien trabaja directamente con los equipos tenga claros los conceptos y el funcionamiento de la Red GPRS para así poder dar una correcta solución a los problemas o fallas que se presenten en los equipos, o bien poder atacar problemas de configuración que se puedan presentar en algún APN y que tenga afectación a los servicios que la operadora brinda a los clientes.

Por lo anterior, a continuación se detallan los equipos que son administrados por el área de Soporte de datos y una breve descripción de las principales actividades que se llevan a cabo sobre estos.

*El nodo **SGSN** tiene las siguientes funciones:*

- Conversión de protocolos entre la red IP y los protocolos utilizados en la Radiobase y la central
- Conexión hacia BSC, HLR, GGSN. DNS y BG.
- Compresión y cifrado de información
- Autenticación y manejo de la movilidad del usuario
- Ruteo de datos hacia el GGSN
- Recolección de datos de tarificación CDRs
- Estadísticas

Este es el único equipo del Backbone de GPRS que no esta bajo la administración del área de Datos, sin embargo es necesario interactuar con el área que tiene a su cargo la administración de este equipo para obtener informes acerca de los móviles, principalmente si verificar el attach a la red GPRS de estos.

*El nodo del **GGSN** tiene las siguientes funciones:*

- Envía paquetes de datos hacia los móviles a través del SGSN.
- Rutea paquetes originados por el móvil hacia la red destino correcta (APNs que contiene la operadora).
- Asigna direcciones IP estáticas o dinámicas a los móviles.
- Creación del inicio de túneles GRE para distintos APNs.
- Generación de estadísticas, principalmente PDPs activos en un APN.

La participación profesional en este equipo es:

Cargar la configuración para nuevos APNs, esto implica: indicar el tipo de APN a ser utilizado es decir si es normal por IPv4 o bien si utilizara Túnel GRE si es el caso se crear el inicio en el GGSN, se indica el tipo de direccionamiento de los móviles indicando el número máximo de PDP context que se pueden tener en el APN, en caso de que ya exista el APN se realizan modificaciones a este, se genera ruteo de los móviles a la interfaz Gi

Se podría decir que desde el punto de vista externo del GGSN es visto como un router.

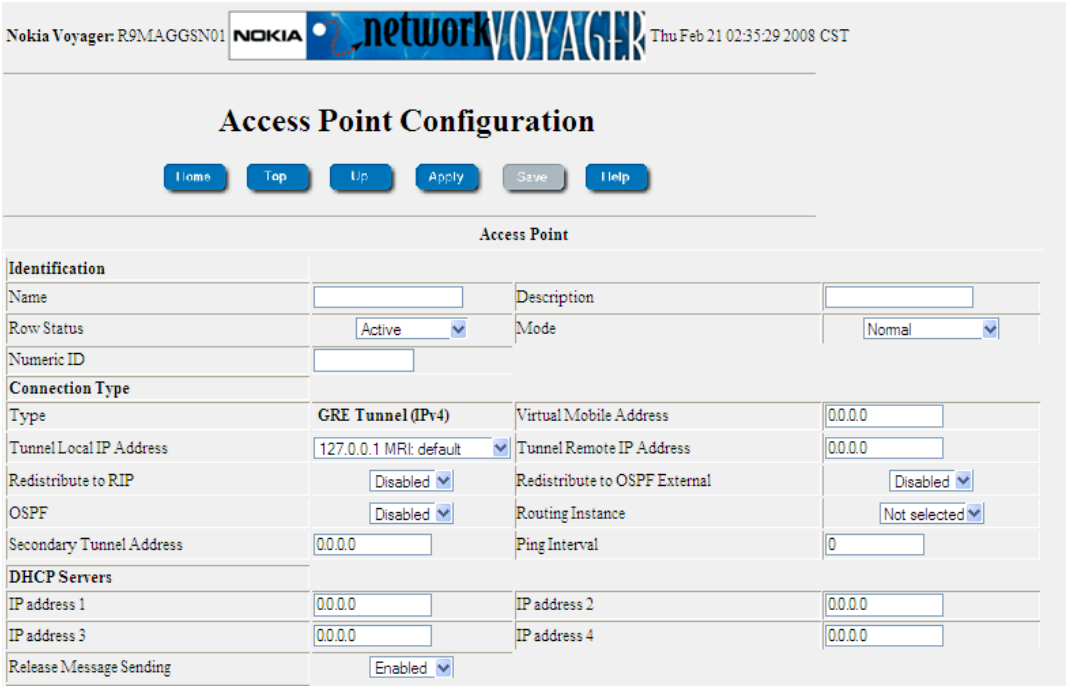


Figura 10. Acceso a Web vía Voyager para configuraciones en los GGSNs

*El elemento **DNS** tiene las siguientes funciones:*

- Este dispositivo estándar IP convierte nombres a direcciones IP, por ejemplo nombreapn.operdor.com =>192.9.198.4

Nombre	bimsa.itelcel.com.mnc020.mcc334.gprs
IP Address	200.79.17.11
IP Address	200.79.17.61

Generalmente el acceso a este equipo es a través de la Interface Gráfica del Usuario, donde las configuraciones más comunes es agregar el mapeo entre el nombre y la dirección IP.

Para la parte de Roaming, a través de Command Line Interface se carga la configuración de distintos operadores, gracias al uso del editor Vi en los DNS.

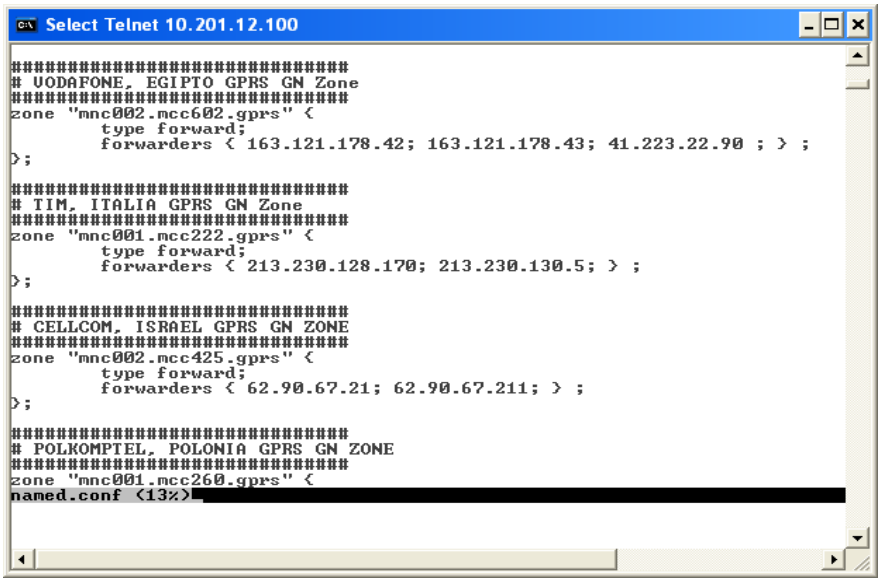


Figura 11. Configuración a través de CLI en el DNS

El elemento ***Border Gateway BG****:*

- Este dispositivo tiene la funcionalidad de interconectar la red GPRS con distintas operadoras que brinden servicios GPRS. Para proporcionar servicios de Roaming de datos. Generalmente la actividad más realizada vía Web es la carga de rutas hacia nuevos operadores.

Figura 12. Configuración de ruteo en el Border Gateway hacia distintos operadores

*El elemento **Traffic Analyzer TA**:*

- Este dispositivo tiene la funcionalidad de recolectar CDRs que son generados por elementos de red, principalmente por los APNs en los cuales se tiene costo al navegar en ellos.

Este equipo presenta varias características, en el se tiene la posibilidad de colocar un bypass para que la navegación no tenga costos, esto únicamente se realiza cuando hay fuertes intervenciones en la Red GPRS. Generalmente se crean las reglas de cobro a las URLs por las que navega el usuario. Por CLI se pueden obtener la generación de los archivos CDRs que son enviados al departamento de prepago para tarificar la navegación o bien obtener a través del numero telefónico, la IP y el APN al cual se esta conectando dicho móvil.

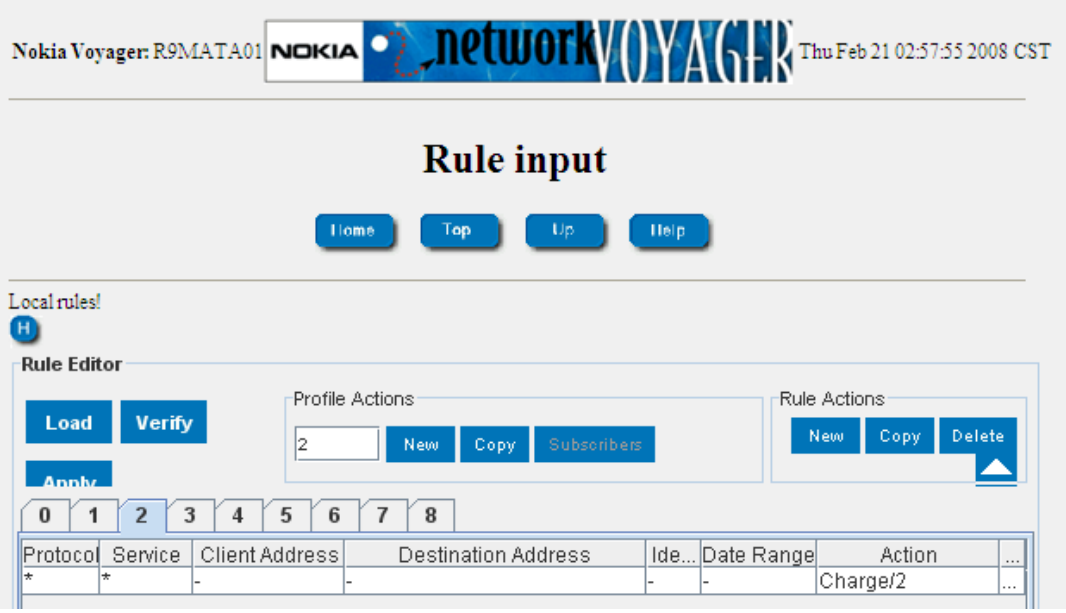


Figura 13. Configuración de reglas en el Traffic Analyzer

*El elemento **Firewall** de GPRS*

- Este dispositivo permite que el tráfico sea filtrado a través de reglas configuradas en el cluster del Firewall por lo que solo tendrá paso el tráfico válido en las reglas descartando el resto. Permitiendo la comunicación bidireccional.

Además del método de filtro en este equipo se direcciona el tráfico de los móviles hacia la red corporativa. Generalmente se crea ruteo estático vía Web, además se pueden obtener capturas de tráfico para analizar los paquetes y protocolos utilizados sobre cualquier APN.

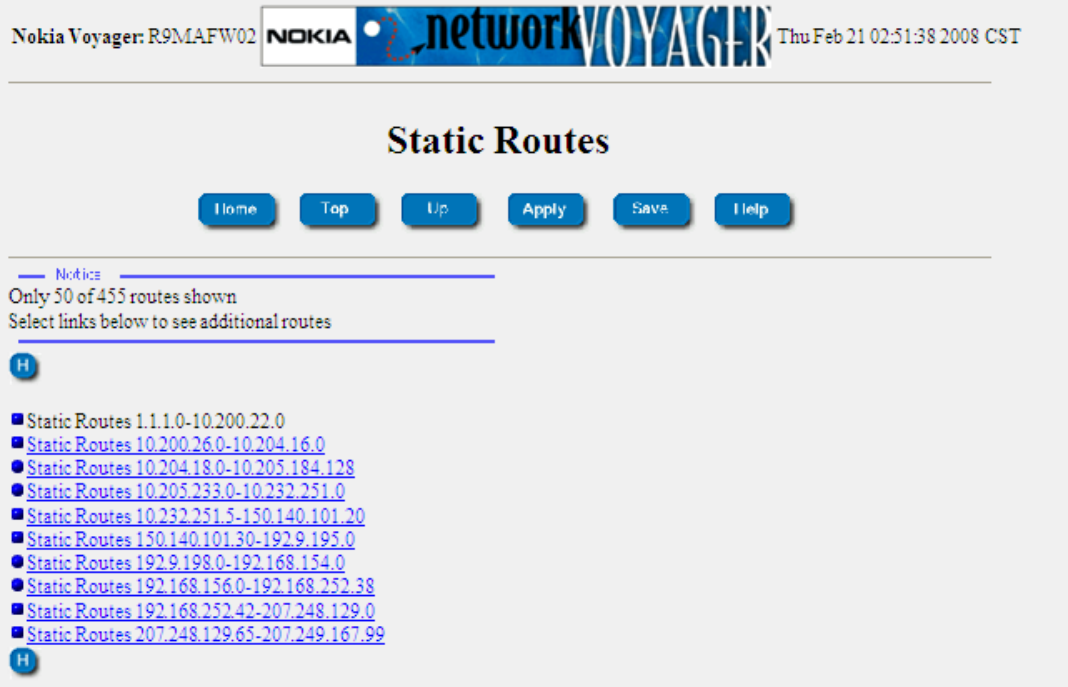


Figura 14. Configuración de ruteo estático para los diferentes APNs en el Firewall de GPRS

Los elementos descritos son parte del trabajo diario que se lleva a cabo en el COR de Datos además de que con todos ellos se tienen en común las siguientes tareas:

- El monitoreo de los equipos a través de la plataforma NetAct.
- El análisis de tráfico que pasa por cada uno de los equipos en sus respectivas interfaces, ya sea vía IP o a través del número telefónico, por medio del análisis de paquetes de datos.

4.2.4 Servicios de datos a través de la Red GPRS

Hoy en día el operador que cuenta con GPRS puede ofrecer dos tipos de servicios, el primero fungir como ISP y el segundo proporcionar Servicios de Valor Agregado. Esto significa nuevas fuentes de ingresos para los servicios ofrecidos:

Funciones básicas del **Internet Service Provider** ISP, tales como acceso a Internet, intranet o Correo Electrónico.

Servicios de valor agregado, tales como WAP **Wireless Application Protocol**, MMS **Multimedia Messaging Service**, **PoC**[26].

En esta operadora se manejan los siguientes servicios masivos:

Servicios de información y entretenimiento
Servicios de suscripción (mejor conocido como Hotnews)
Tonos
Imágenes fijas y animadas
Juegos y aplicaciones Java
Videos
Servicios de interactividad: trivial, votaciones, promociones, etc.

A través del servicio de WAP. Se permite a los usuarios acceder a información de una red (Internet) por medio de dispositivos inalámbricos tales como, celulares, palms, pagers. Etc. En el caso especial de esta operadora se cuenta con una gran variedad de contenidos y su propio Portal.

Gracias al servicio de MMS de mensajera como telefonía celular muy similar al servicio de mensajes cortos. Proporciona el envió y recepción de mensajes multimedia de un teléfono a otro. Los mensajes multimedia pueden contener imágenes, graficas, voz o archivos de audio.

También se brindan servicios de AVL **Automatic Vehicle Location.** Servicio de localización vehicular empleado para el rastreo de unidades móviles.

Y servicios de PoC. Estas llamadas son half duplex; mientras una persona habla la otra escucha.

Los servicios descritos anteriormente son clasificados por APNs en la red de GPRS. Siendo responsabilidad del COR de Datos verificar el buen funcionamiento de estos servicios en conjunto con otras áreas de la Operadora Telefónica.

[26] PoC. Push to Talk over Celular. Sistema de comunicación celular que utiliza la red GPRS para transmitir voz en modo Half Duplex.

5. Análisis y Metodología Empleada

5.1 Conocimientos de Protocolos de Redes de Datos

En esta sección, se darán a conocer los protocolos más utilizados en el troubleshooting de Redes de Datos, los cuales el Ingeniero de Soporte de un Centro de Operación de Red, utiliza como método de análisis ante algún problema que afecte la disponibilidad de la Red de Datos. En general todo el ambiente de trabajo relacionado con equipos de redes de datos se le llama “networking”.

Modelo OSI y Modelo jerárquico de redes de datos

Generalmente utilizamos estos dos modelos como la base para comenzar a analizar un problema, primero se explica de forma muy general el Modelo OSI y señalando las capas en las que sobre las que más trabaja el Ingeniero de Soporte.

Después se explica el Modelo Jerárquico de Redes y el por que es importante tener un orden al integrar los equipos en la Red de Datos.

Modelo OSI

Este modelo es una de las herramientas más importantes para diseñar y resolver problemas de comunicación. También conocido como modelo de red, o arquitectura de red, se refiere a una organización de documentos. Individualmente, estos documentos describen una pequeña función requerida para una red, los cuales pueden definir un protocolo, el cual es una regla que los dispositivos deben seguir para comunicarse. Otros documentos pueden definir algunos requerimientos físicos para redes, por ejemplo, se puede definir el voltaje y niveles de corriente usados en el cableado.

Para crear una red de trabajo, los dispositivos en la red necesitan seguir los detalles referenciados por un modelo de red particular. Cuando múltiples computadoras y otros dispositivos de red implementan estos protocolos, especificaciones físicas, reglas y los dispositivos están conectados correctamente, los dispositivos de la red pueden comunicarse exitosamente, gracias al modelo creado por la Organización Internacional de Estandarización ISO, la cual se da a la tarea de crear un estándar abierto del modelo de red para que sea soportado a nivel mundial, a este modelo de red se le llama Open System Interconnection conocido como modelo OSI. Con la meta fundamental de: estandarizar los protocolos de redes de datos para permitir la comunicación entre todas las computadoras del planeta entero.

1. **FÍSICA**. En esta capa define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante la definición de: conexiones físicas entre computadoras, técnicas de transmisión, tipo de transmisión, codificación de la línea, velocidad de transmisión y describir el aspecto mecánico, eléctrico y funcional de la interface física.

2. **ENLACE**. La capa de enlace de datos define las reglas (protocolos) que determinan cuando un dispositivo puede enviar datos sobre un medio en particular. Los protocolos de la capa de enlace también definen el encapsulamiento de datos además de definir un campo de Frame Check Sequence FCS, el cual permite al dispositivo que recibe detectar errores de transmisión, estableciendo un esquema de detección de errores para las retransmisiones o re-configuraciones de la red.

Es en esta capa donde se detectan errores en el nivel físico. Se establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes. Realizar la transferencia de datos a través del enlace físico, enviar bloques de datos con el control necesario para la sincronía. En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

3. **RED**. Esta capa define tres características principales: direccionamiento lógico, enrutamiento y determinación del camino. Los conceptos de enrutamiento definen como los dispositivos (típicamente routers) reenvían paquetes a su destino final.

El direccionamiento lógico define como cada dispositivo puede tener una dirección que pueda ser usada por el proceso de enrutamiento o mejor dicho protocolo empleado. La determinación del camino se refiere al trabajo hecho por los protocolos de enrutamiento por el cual todas las posibles rutas son aprendidas pero la mejor ruta es elegida para ser utilizada. En resumen esta capa define el enrutamiento y el envío de paquetes entre redes; es responsabilidad de esta capa establecer, mantener y terminar las conexiones.

4. **TRANSPORTE**. Esta capa actúa como un puente entre las tres capas inferiores del modelo OSI, totalmente orientadas a las comunicaciones y a los tres niveles superiores de las capas del modelo, totalmente orientados al procesamiento. Además, garantiza una entrega confiable de la información, asegura la llegada de datos del nivel de red, encuentra las características de transmisión y calidad de servicio requerido por la capa de sesión, esta capa define como direccionar la localidad física de los dispositivos de la red. Asigna una dirección única de transporte a cada usuario, define una posible multicanalización. Esto es, puede soportar múltiples conexiones.

Define la manera de habilitar y deshabilitar las conexiones entre los nodos. Determina el protocolo que garantiza el envío del mensaje, puede ser TCP o UDP.

Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

5. **SESIÓN**. La capa de sesión define como comenzar, controlar, y terminar conversaciones (llamadas sesiones). Esto incluye el control y administración de múltiples mensajes bidireccionales. Es decir, administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión.

6. **PRESENTACIÓN**. El propósito principal de esta capa es definir y negociar el formato de los datos, es decir, dar el formato mediante el cual se logra la comunicación de dispositivos. En esta capa, la encripción también es definida por OSI como un servicio de la capa de presentación.

7. **APLICACIÓN**. Provee una interface entre la comunicación del software y cualquier aplicación que necesite comunicarse a la salida de

la computadora sobre la cual reside la aplicación también define procesos para autenticación.

Una vez que el Ingeniero de Soporte conoce este modelo de forma detallada en cada una de sus capas es capaz de determinar las posibles fallas en la red de datos, generalmente utilizamos las primeras cuatro capas, analizando el cableado, método de acceso, protocolo de enrutamiento y tipo de conexión.

Un ejemplo de identificar las capas en un equipo se muestra en la siguiente figura:

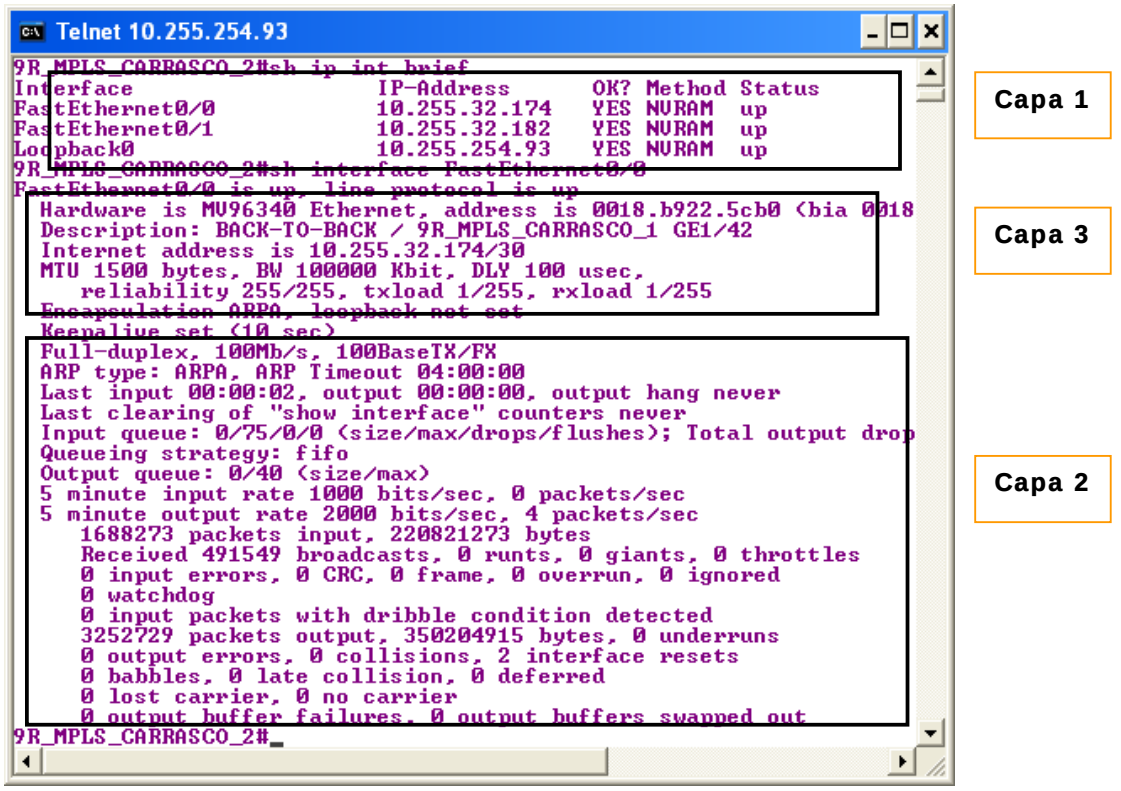


Figura 15. Capas del Modelo OSI dentro de un Router

MODELO JERARQUICO

Las 3 capas que componen este modelo se dividen de la siguiente forma:

- **Capa de acceso**

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Esta capa de acceso se denomina capa de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales esta confinado entre los recursos, switches y usuarios

finales. En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos.

En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

- **Capa de distribución**

La capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.
En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, como:

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquete pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo (Core o Backbone). La capa de core podrá entonces transportar la petición al servicio apropiado.

- **Capa de Core**

La capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia. Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

Este es en general, un diagrama de la topología que debe tener una red que utiliza el Modelo Jerárquico. Es indispensable conocer este modelo ya que se puede con la ayuda del modelo OSI es posible determinar en que capa ocurren los problemas, además este modelo es de gran ayuda para el diseño de Redes de Datos que son robustas, como es el caso de la Red de Datos de la Operadora Telefónica.

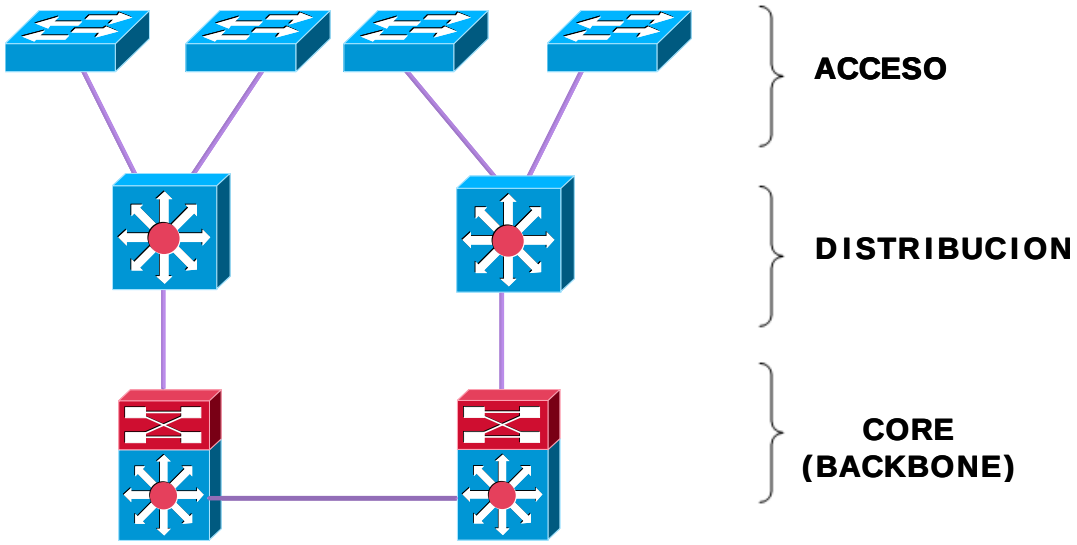


Figura 16. Modelo Jerárquico de una Red de Datos

5.1.2 Funcionamiento de equipos a nivel Capa 2 y Capa 3

Capa 2

A continuación se detallan los conceptos básicos que se deben conocer de un Switch, el cual trabaja a nivel de capa 2 y es el equipo que da acceso a los usuarios en la red, el trabajo realizado sobre este equipo en términos de networking es conocido como Switching.

La comunicación inicia a través del transporte de las tramas de Ethernet, las cuáles contienen direcciones MAC origen y destino, que se encuentran en las tarjetas de red de las PC o dispositivos que requerían acceso a Red de Datos, se componen por 48 bits, la MAC es impresa en la tarjeta de red del fabricante, y es única.

Un switch es un equipo que implementa algoritmos en ASICS (Application Specific Integrated Circuit Application), no es encargado de inspeccionar el paquete IP, no modifica la trama, pero es encargado de realizar parte del transporte de esta, brinda velocidades de transporte

de hasta 100Mbps, este equipo es capaz de reducir el dominio de colisión esto implica que cada puerto es un dominio de colisión, las tramas se envían sólo a través del puerto correspondiente permitiendo un aumento del ancho de banda disponible a cada usuario brindando seguridad y no permite ver el tráfico de otros usuarios.

Este equipo puede ser susceptible a loops (bucles en la Red), los cuales se resuelven con el protocolo Spanning Tree Protocol (STP) pero pueden llegar a aumentar la complejidad del manejo del equipo y llegar a tener convergencia lenta.

Otras de las funciones básicas que realiza el equipo son: aprendizaje de direcciones MAC a través de una tablado direccionamiento la cual se va creando agregando las dirección MAC origen y el puerto en el cual se recibió la trama, este equipo permite realizar reenvío (Forwarding) inspeccionando la dirección destino en cada trama, si la dirección se encuentra en la tabla, la trama se reenvía solamente a través del puerto correspondiente en caso contrario, la trama se reenvía a través de todos los puertos del equipo excepto en el puerto donde se recibió, cuando el destinatario responde, su dirección origen se agrega a la tabla.

Los loops que se crean en el equipo mencionados anteriormente se pueden presentar o generar en soluciones que proveen redundancia, sí no existe un mecanismo de control para estos lazos se puede causar: tormentas de Broadcast e imposibilidad aprendizaje de direcciones en la tabla de MAC. Para evitar que se presenten este tipo de problemas se utiliza STP.

Spanning Tree Protocol STP es estandarizado por el IEEE bajo el estándar 802.1d, Su función es la de gestionar la presencia de lazos en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). Permitiendo a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de lazos. Su operación se compone a través de generar una topología lógica de la red en forma de árbol estableciendo distinto estados en los puertos que conectan los enlaces, dar la explicación de este protocolo no es un objetivo de esta sección simplemente se menciona ya que el Ingeniero de Soporte debe conocer bien su funcionamiento para atacar problemas que se presenten causados por este protocolo.

El switch también permite la segmentación del dominio de broadcast, dividiendo la red LAN en segmentos independientes entre si, brindando un mejor aprovechamiento del ancho de banda disponible dentro de la Red a través de la creación de VLANs.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados la definimos como una subred virtual y es considerada como un dominio de Broadcast, el cual puede estar en el mismo medio físico o bien parte de sus integrantes se puede ubicar en distintos edificios que conformen la Red de Datos. De esta forma se tiene un control más inteligente del tráfico de la red.

La comunicación que se hace entre switches para interconectar VLANs utiliza un proceso llamado Trunking. El protocolo VLAN Trunk Protocol VTP es el que se utiliza para esta conexión, puede ser utilizado en todas las líneas de conexión incluyendo ISL o IEEE 810.1Q.

La figura 17 muestra el switch configurado con parámetros de capa 2.

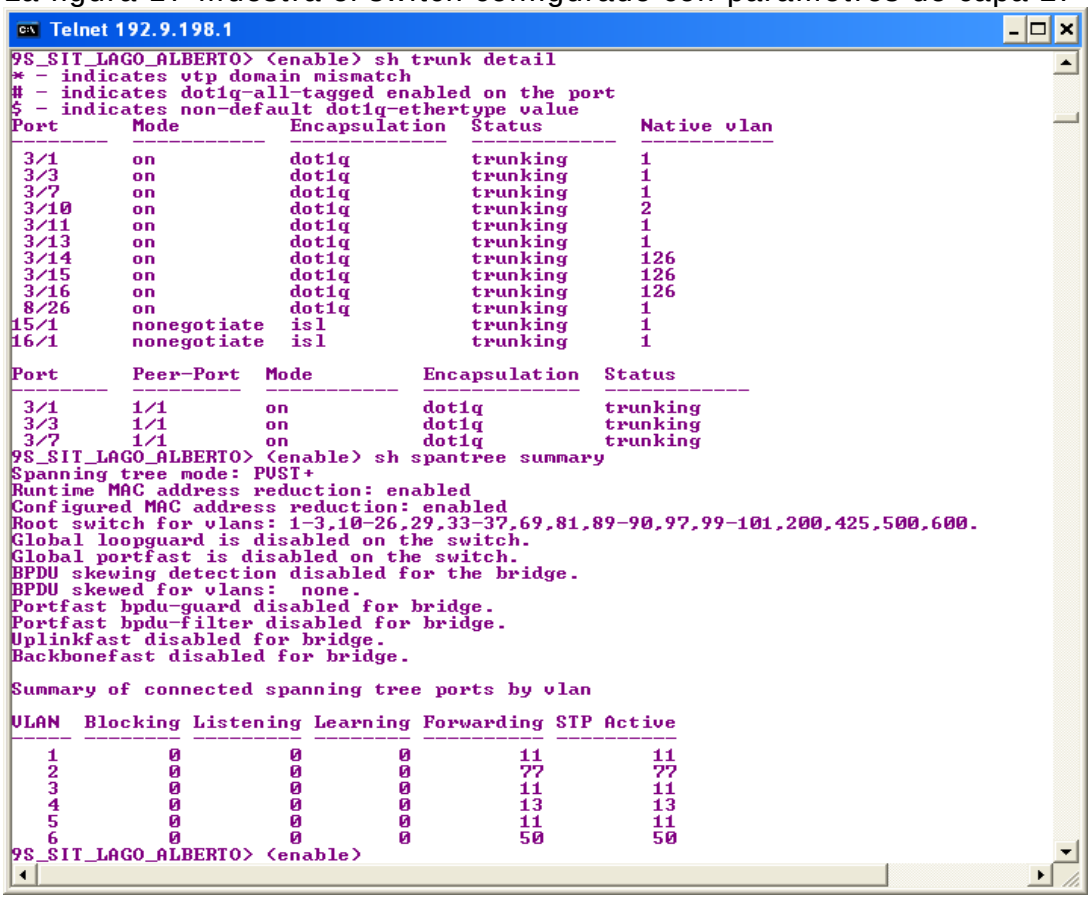


Figura 17. Switch configurado en capa 2

Capa 3

A nivel de capa 3 la comunicación de los equipos ocurre a través de paquetes IP por medio de Routers y el análisis, funcionamiento de esta capa es llamado Routing o Ruteo.

Ruteo es básicamente informar y decidir cual es la ruta más eficiente para enviar información. Ruteo es el acto de intercambiar información a través de la Red de datos desde un origen a un destino. A lo largo del camino al menos un nodo puede estar presente, dicho acto ocurre a nivel de capa 3 del modelo OSI. El ruteo involucra dos actividades básicas: determina una trayectoria óptima y transporta grupos de información llamados paquetes a través de direcciones IP de una Red.

La determinación de la trayectoria suele ser compleja, para ello existen ciertos protocolos que utilizan métricas y una gran variedad de mensajes para evaluar que trayectoria será la mejor para que pueda viajar el paquete IP. Una métrica es una medida estándar de los algoritmos de ruteo, entre ellas se utilizan cálculos de: longitud de la trayectoria, confiabilidad, retardo, ancho de banda, carga y costo. La métricas y mensajes permiten inicializar y mantener tablas que contienen la información de todas las posibles rutas, estas varían dependiendo del protocolo utilizado también llamados Protocolos de Ruteo "Routing Protocols" así agilizan y facilitan la transferencia de Información de paquetes IP, estos algoritmos pueden ser implementados en varios Sistemas Operativos y su selección depende del tipo de conectividad que se emplee.

Dentro de los protocolos más utilizados y manejados en el Centro de Operación de la Red de datos se encuentran:

- **RIP** Routing Information Protocol
- **OSPF** Open Shortest Path First
- **EIGRP** Enhanced Internet Gateway Routing Protocol
- **BGP** Border Gateway Protocol

Todos ellos se implementan en los routers y permiten la comunicación entre las 9 regiones del país, explicar su funcionamiento es una tarea muy detallada y hasta cierto punto compleja, y no es un objetivo de este trabajo, pero es necesario señalar que un ingeniero de Redes debe conocer al menos el funcionamiento básico de estos protocolos, para poder atacar diversos problemas que se puedan presentar en la convergencia de estos protocolos y que puedan afectar la Red de Datos.

El ruteo también incrementa el nivel de seguridad en la Red LAN, para permitir y negar acceso a usuarios, aplicaciones o acceso a

Internet a través de la creación de Listas de de Acceso que el administrador de la red ingresa al equipo de acuerdo a sus requerimientos, a través de **Command Line Interface** CLI.

Como parte de la seguridad también se utiliza NAT **Network Address Translation**. NAT es el método por el cual se traduce la dirección IP de un usuario o equipo a otra dirección, se usa principalmente cuando

existen varios nodos IP en una LAN que requieran comunicarse al exterior (Internet) pero solo existe un solo nodo para ingresar, en otras palabras, NAT coordina varias direcciones a través de una sola dirección IP, de igual forma que las Listas de Acceso es configurado en el equipo de acuerdo a los requerimientos del administrador de la Red

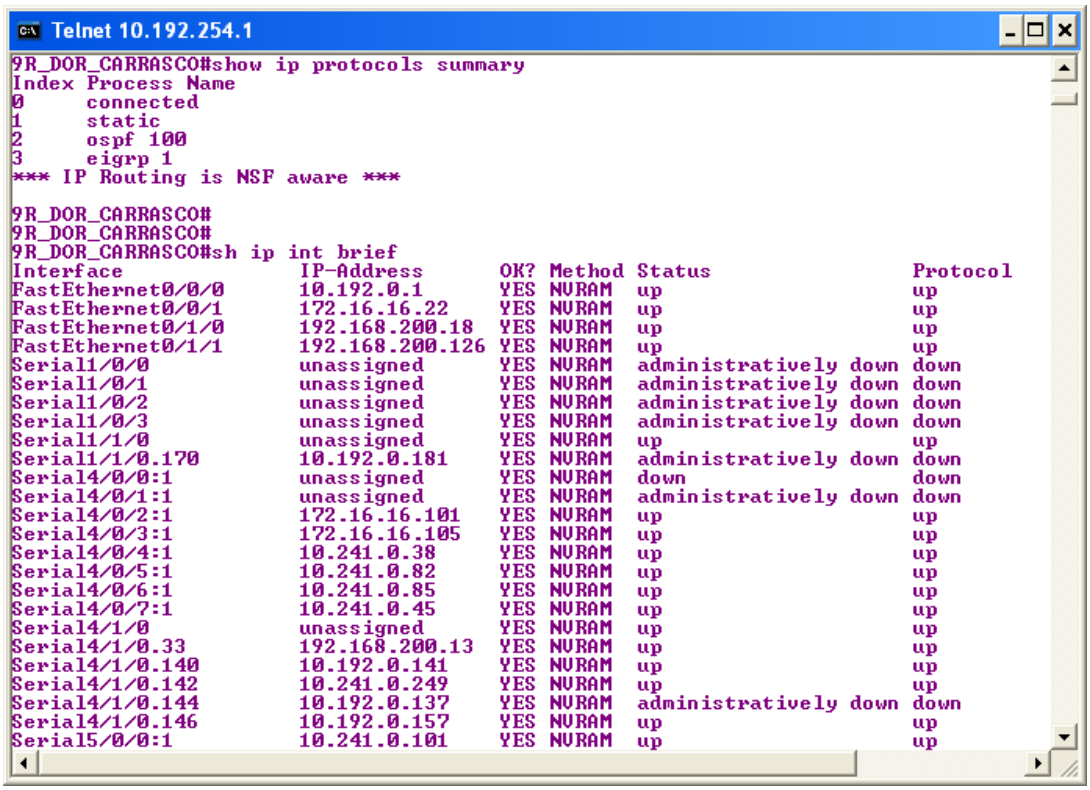


Figura 18. Router configurado en capa 3

En ambas capas 2 y 3, el Ingeniero de Soporte realiza: el monitoreo de los equipos, cambios de configuración que se requieran, análisis de problemas, es decir Troubleshooting. Pero es importante señalar que existen cursos de certificación los cuales se especializan tanto en Switching como Routing, donde dichos cursos se complementan con el aprendizaje contacto diario a los equipos que integran la Red de Datos.

5.1.3 Funcionamiento de túneles GRE y IPSec VPNs

En esta sección se dan a conocer algunos de los protocolos más utilizados para configurar y analizar problemas de VPNs, el análisis que se utiliza para resolver un problema que se presente con estas conexiones es a través de conocer el funcionamiento de los protocolos que a continuación se presentan, la configuración realizada por el Ingeniero de Soporte se dará a conocer en el apartado 6.

VPN

Una **Virtual Private Network** VPN, es una tecnología de red que permite extender la red local sobre una red pública o no controlada, como por ejemplo Internet. La conexión se realiza de forma segura ya que se proporcionan los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación. La VPN en si provee las siguientes características de seguridad:

- **Privacidad.** Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).
- **Autenticación**. Verifica que quien envía el paquete VPN es un dispositivo legitimo y no uno utilizado por un agente invasivo, se valida Usuario/equipo y qué nivel de acceso debe tener. Se realiza a través del intercambio de llaves.
- **Integridad de Datos**. La garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de Hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- **No repudio (Antireplay)**. Previene que alguna persona copie paquetes enviados por un usuario legítimo, y luego más tarde reenvié el paquete para que aparezca como un usuario legitimo.

Básicamente existen tres tipos de VPNs que se implementan en una empresa, estos tipos se encuentran implementados en la Operadora Telefónica, y es tarea del Ingeniero de Soporte levantar VPNs y realizar un análisis detallado cuando se presenten problemas en alguna de estas configuraciones.

- **Acceso.** Consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la Red Local de la empresa
- **Intranet.** Este esquema se utiliza para conectar oficinas remotas con la sede central de la empresa. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet,

típicamente mediante conexiones de banda ancha. En este punto a la VPN también se le conoce como VPN tunneling. En término tunneling generalmente se refiere a cualquier paquete de protocolos que es enviado por la encapsulación del paquete dentro de otro paquete. El termino VPN tunneling implica que el paquete encapsulado ha sido encriptado, mientras que el termino túnel no implica que necesariamente haya sido encriptado.

- **Extranet.** Este tipo de VPN es muy parecida a la VPN de Intranet, pero en este caso el túnel se realiza entre dos redes diferentes es decir, entre la Red Local y una Red Externa a la empresa, muchas veces también es llamada VPN WAN, ya que el túnel es creado a través de enlaces **Wide Area Network** WAN.

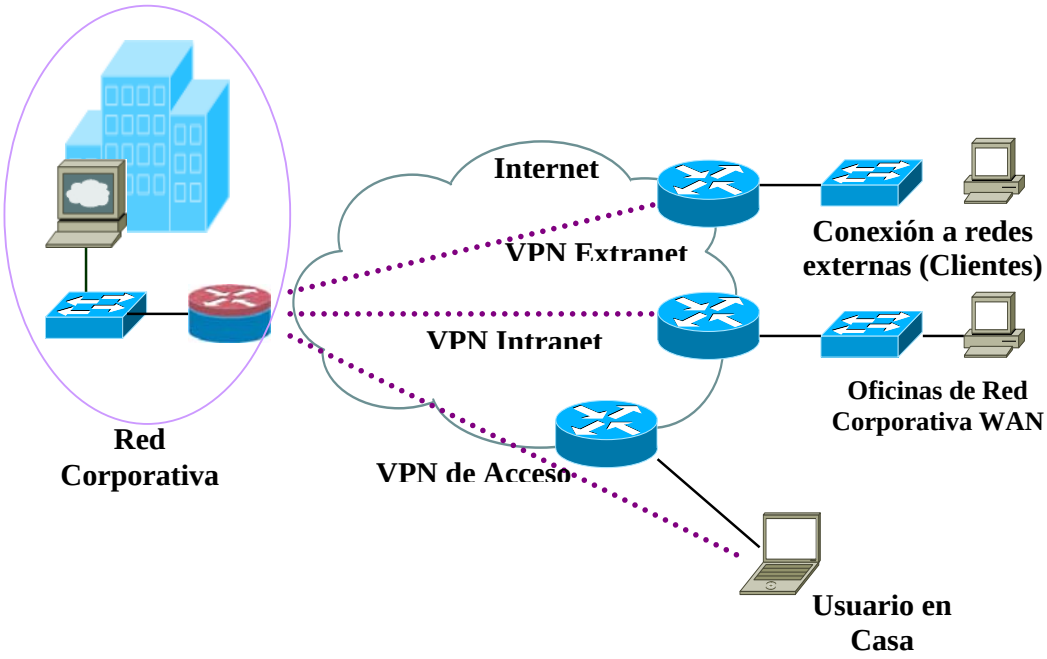


Figura 19. Tipos de acceso a una VPN

Para construir una VPN, los dispositivos que se necesitan en los sitios requieren hardware o software que comprenda y elija protocolos y estándares de seguridad de VPNs, algunos dispositivos que se manejan en el COR son:

- Routers
- Firewalls
- Concentradores de VPNs
- Clientes de VPNs

Cuando se aborda el análisis o creación de VPNs nacen dos conceptos: Primero, la red virtual, también llamada túnel, que emula una conexión punto a punto entre 2 nodos conectados a Internet. Y segundo, la encripción de los datos que circulan sobre ese túnel para darle seguridad al intercambio privado de información sobre una red pública. Como se ha visto anteriormente, hay protocolos involucrados en ambos aspectos. Protocolos para la creación y funcionamiento del túnel y protocolos de encripción de datos. De estos protocolos que manejamos en el COR y son GRE y IPSec, a continuación se presenta una breve explicación de estos.

Túnel GRE

Para el túnel uno de los protocolos más utilizados es el Point-to-Point Tunneling Protocol. Este protocolo utiliza **Genereric Routing Encapsulation** GRE para generar los túneles, GRE es un protocolo originalmente desarrollado por Cisco Systems que se ha convertido en un estándar de la industria. Es un protocolo de túnel, es decir, que permite transportar paquetes de una red a través de otra red diferente, generalmente es más implementado en estos casos. Para implementarlo es necesario revisar los comandos que se deben considerar en ambos extremos del enlace a través del cual debe operar el túnel, esto generalmente se lleva a cabo sobre las interfaces de los Routers, cada una de estas interfaces utiliza su propia red, comportándose como un enlace punto a punto. Así el tráfico de este túnel será físicamente enviado a través de las interfaces seriales, o fastEthernet del Router.

En algunas ocasiones puede ocurrir que el túnel se configure sobre un enlace privado de algún cliente o bien puede realizarse sobre Internet; en este caso se puede utilizar algún protocolo de encripción como IPSec para brindar privacidad y seguridad. Ya que GRE no provee encripción de la información.

Las redes se diseñan normalmente para impedir el acceso no autorizado a datos confidenciales desde fuera de la intranet de la empresa mediante el cifrado de la información que viaja a través de redes públicas, sin embargo, la mayor parte de las redes manejan las comunicaciones entre los hosts de la red interna como texto sin formato. Con acceso físico a la red y un analizador de protocolos, un usuario no autorizado puede obtener fácilmente datos privados.

Túnel IPSec

IPSec el **Protocolo Seguro de Internet**, autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP. IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

IPSec aumenta la seguridad de los datos de la red mediante: La autenticación mutua de los equipos antes del intercambio de datos. El establecimiento de una asociación de seguridad entre los dos equipos. IPSec se puede implementar para proteger las comunicaciones entre usuarios remotos y redes, entre redes e incluso, entre equipos cliente dentro de una red de área local LAN.

IPSec usa formatos de paquete IP estándar en la autenticación o el cifrado de los datos. Por tanto, los dispositivos de red intermedios, como los routers, no pueden distinguir los paquetes de IPSec de los paquetes IP normales.

IPSec también proporciona las siguientes ventajas:

Transparencia de IPSec para los usuarios y las aplicaciones. Como IPSec opera al nivel de red, los usuarios y las aplicaciones no interactúan con IPSec.

IPSec puede implementarse a través de dos protocolos ESP **Encapsulating Security Payload**, o AH **Authentication Heade**r. Ambos cumplen con los propósitos de seguridad y se usan dependiendo de los requerimientos del cliente. Presentar una definición y funcionamiento de estos protocolos es un trabajo muy extenso, pero como se ha mencionado anteriormente el Ingeniero de Soporte debe conocer las funciones básicas de los protocolos para poder determinar cuando hay problemas en que fases de la VPN se presentan problemas. Las configuraciones principales se realizan en los Firewalls y concentradores de VPN que se tienen en la Red de Datos, a continuación se muestra un ejemplo del requerimiento y configuración necearía para el levantamiento de servicios de una VPN.

Equipos de seguridad

Es de suma importancia la parte de seguridad en cualquier red de datos, en este caso, por ser una red bastante amplia se manejan

además de la seguridad que brindan los Rotures, Firewalls de distintos proveedores y concentradores de VPNs con el fin de dar servicios a clientes y a usuarios de la empresa.

En los Firewalls principalmente se generan los túneles GRE y IPSec para la creación de VPNs. La configuración es cargada en los distintos equipos como, Netscreen, Junnipers y Contivity.

El ingeniero de soporte debe conocer e identificar los métodos que permiten el funcionamiento de estos túneles, para poder brindar un mejor servicio cuando se levantan VPNs con los distintos clientes.

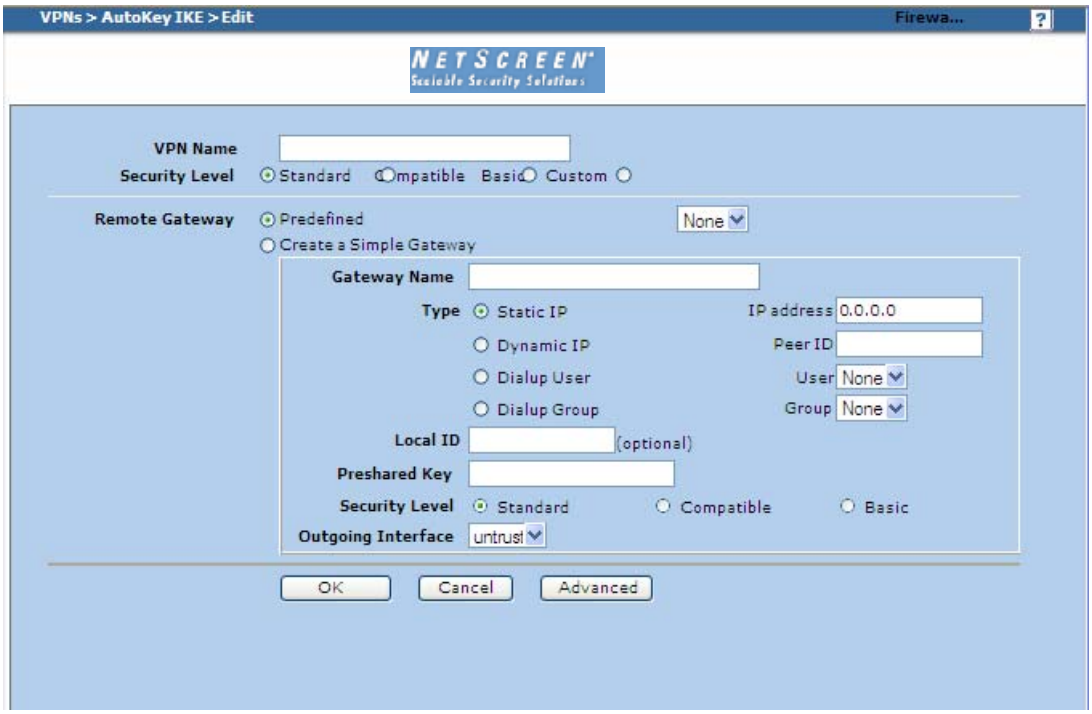


Figura 20. Imagen de un Firewall acceso vía GUI

Como se observa en la figura anterior vía GUI o CLI se pude configurar el equipo de acuerdo a los requerimientos del cliente, en este punto es el área de diseño la encargada se enviarnos los datos que han recolectado del cliente para poder levantar las VPNs. En este caso nos envían: tipo de dispositivo manejado por el cliente, dirección IP de la VPN, las redes locales y remotas que serán dadas de alta, el Pre-shared Key, protocolo de seguridad a utilizar ESP o AH, protocolos de encripción y autenticacion que se utilizaran en fase 1 y fase 2. Así como las políticas, NAT si se requiere y servicios de puertos que necesarios para poder levantar nuevas VPNs hacia distintos clientes o bien solucionar algún problema que se pueda presentar en VPNs que estén en servicio.

En la siguiente figura se muestra un ejemplo de los requerimientos de un cliente para la creación de una VPN.

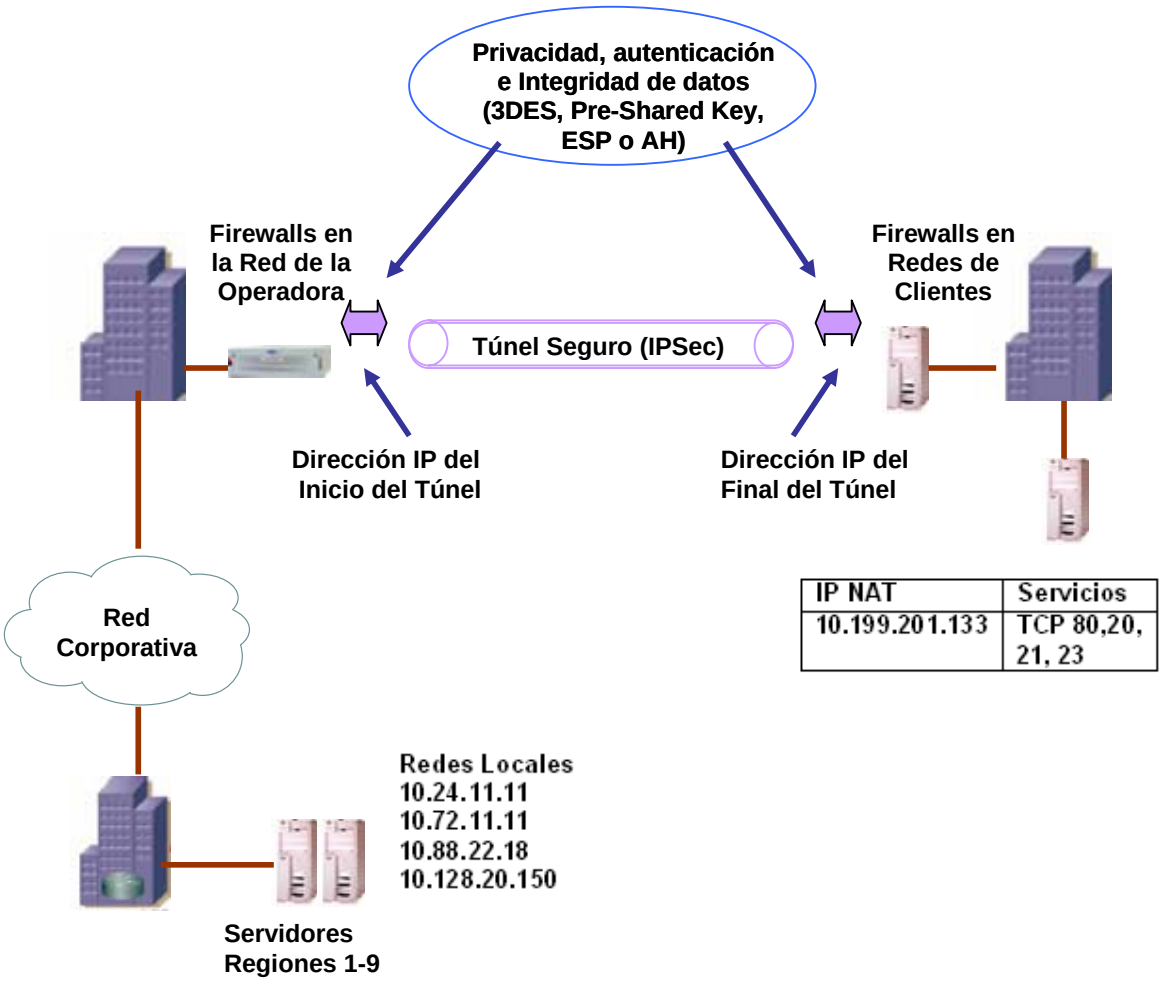


Figura 21. Requerimientos para levantar VPNs con distintos Clientes

Los requerimientos de la figura anterior, son trasladados a configuración en los Firewalls que forman parte de la seguridad de la Red de datos. Cabe señalar que el Ingeniero de Soporte aporta sus conocimientos en la atención a problemas que puedan presentarse al levantar una VPN. A manera de ejemplo a continuación se muestran los equipos con los que determinamos el estado de las VPNs, sobre estos es donde se realizan las configuraciones.

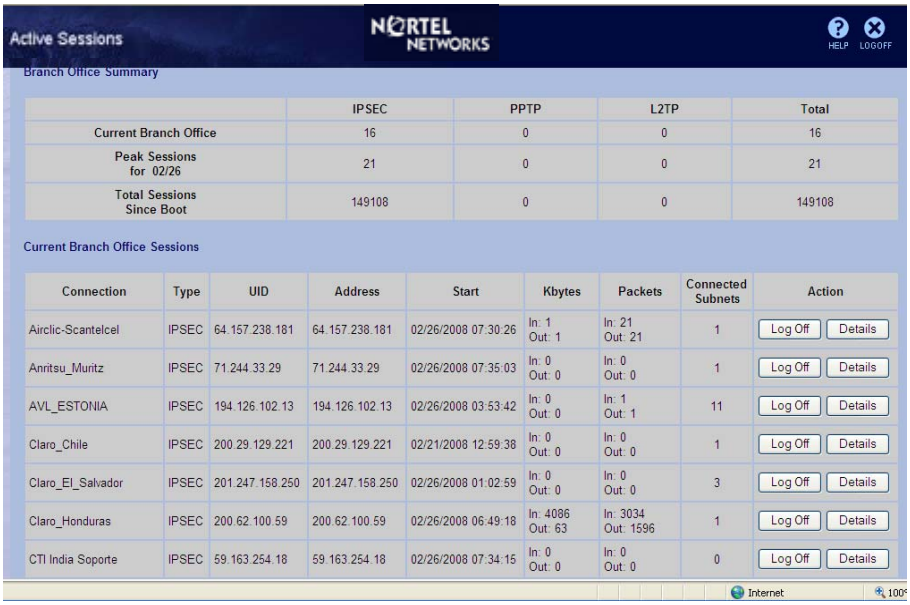


Figura 22. VPNs creadas a distintos clientes a nivel Internacional

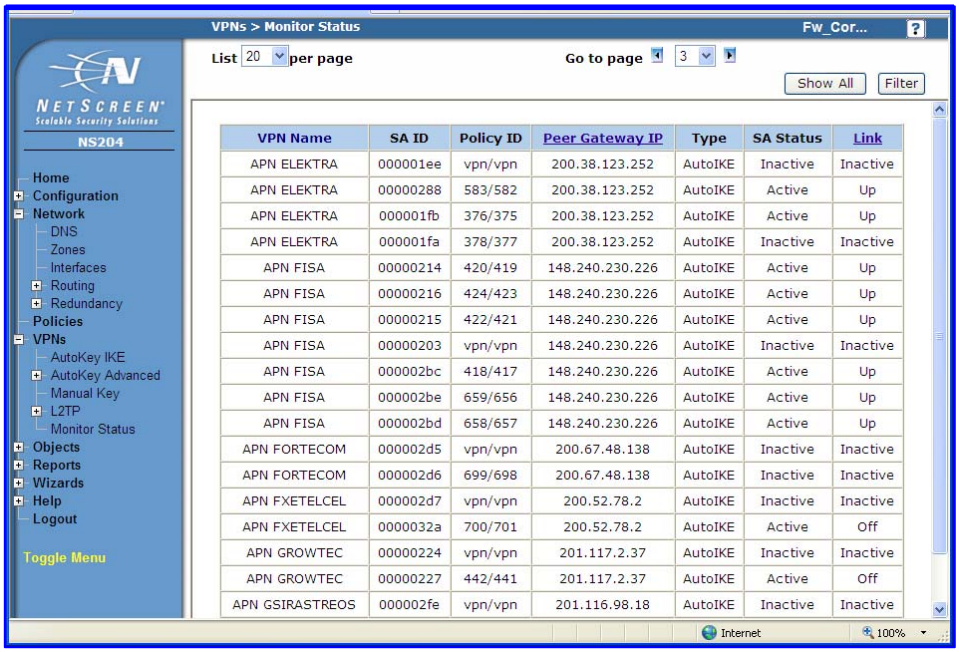


Figura 23. VPNs creadas a distintos clientes a nivel de APNs que utilizan Túnel IPSec

5.1.4 Funcionamiento del protocolo SNMP

El **Protocolo Simple de Administración de Red** o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

Los componentes de una red administrada a través de SNMP consisten de tres componentes claves:

- *Entidad gestora*. Es una aplicación con control humano que se ejecuta en una estación centralizada NOC. Aplicación que controla la recolección, procesamiento, análisis y visualización de la información de gestión. Se encarga de controlar la recolección, procesamiento, análisis y visualización de la información de gestión; es donde se inician las acciones que controlan el comportamiento de la red, y donde el administrador de la red interactúa con los dispositivos de la red. Esta entidad gestora también es llamada **NMS**[27].

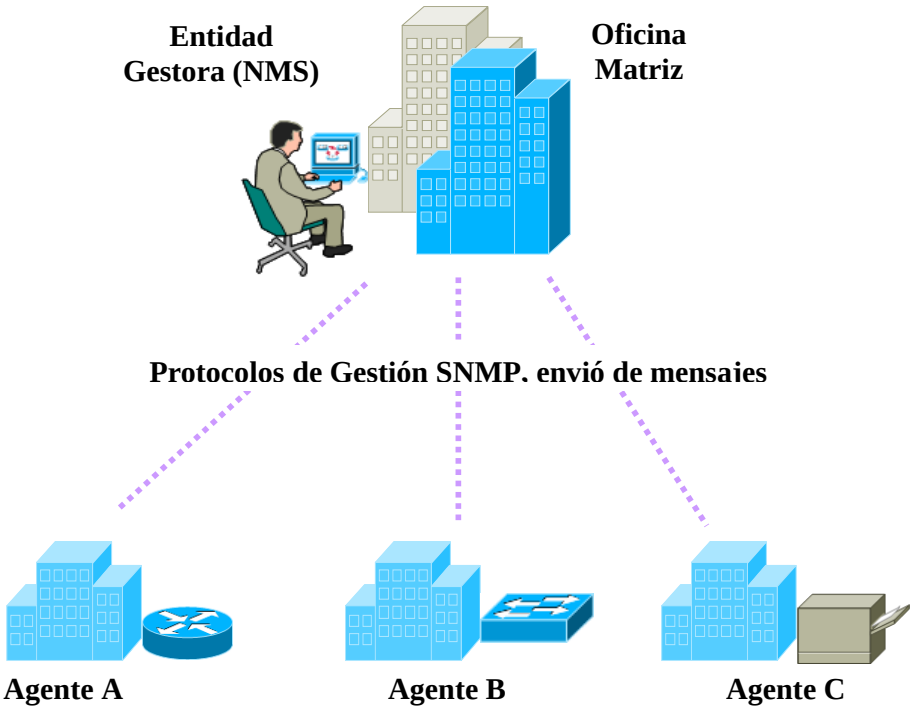
- *Dispositivos gestionados*. Es una componente de la red, incluye al equipo de comunicaciones y al software.

En el equipo hay diversos objetos gestionados, por ejemplo una tarjeta, un protocolo de enrutamiento, etc. y contiene lo siguiente: Un agente es un proceso que se ejecuta en cada dispositivo residente y se encarga de comunicar con la entidad gestora y actualizar la **MIB**[28]. Una base de datos de gestión MIB. El agente también esta capacitado para informar de acontecimientos inusuales en su entorno por medio de mensajes "Traps", los eventos que origina un trap pueden ser un reinicio, que haya demasiado tráfico en la red, un router que deja de responder. Los traps los envía el agente sin haberlos solicitado previamente la entidad gestora. Un SNMP TRAP es un mensaje que es iniciado por el elemento de red y enviados a la red de gestión del sistema. Un trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración.

- *Protocolos de Gestión*. Permite a la entidad gestora comunicarse con los agentes. Permite al gestor comunicarse con el agente para conocer el estado de los dispositivos (consultar la MIB). Los agentes pueden informar al gestor de situaciones "anómalas" en los dispositivos. El protocolo no controla por si mismo, sino que

[27] NMS Sistema de Gestión de Red
[28] MIB. Base de Información de Administración

proporciona una herramienta con la que el administrador de red puede gestionar la red (supervisar, comprobar, sondear, configurar, analizar, evaluar, controlar, etc.).



Dispositivos Administrados contienen Agente y MIB

Figura 24. Diagrama del protocolo SNMP

La figura anterior muestra de manera muy general el funcionamiento del protocolo SNMP.

Otros tipos de mensajes utilizados por el SNMP:

Los mensajes SNMP pueden ser presentados por cualquiera de los sistemas de gestión de red NMS, o por los elementos de red.

Un SNMP GET es un mensaje que se inicia por el sistema de gestión de red cuando quiere recuperar algunos datos de un elemento de red. Por ejemplo, el sistema de gestión de la red podría consultar un router para la utilización de un vinculo WAN cada 5 minutos. Podría entonces crear los cuadros gráficos de los datos, o puede advertir al operador cuando el vinculo se sobre utiliza.

Un SNMP SET es un mensaje que es iniciado por los nuevos estados miembros cuando se desea cambiar los datos en un elemento de red.

Para realizar las operaciones básicas de administración, el protocolo SNMP utiliza un servicio no orientado a la conexión **User Datagram Protocol UDP**[29] para enviar un pequeño grupo de mensajes **Packet Dta Units** PDUs entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP. Los puertos comúnmente utilizados para SNMP son los siguientes: UDP 161 SNMP Y UDP 162 SNMP-trap.

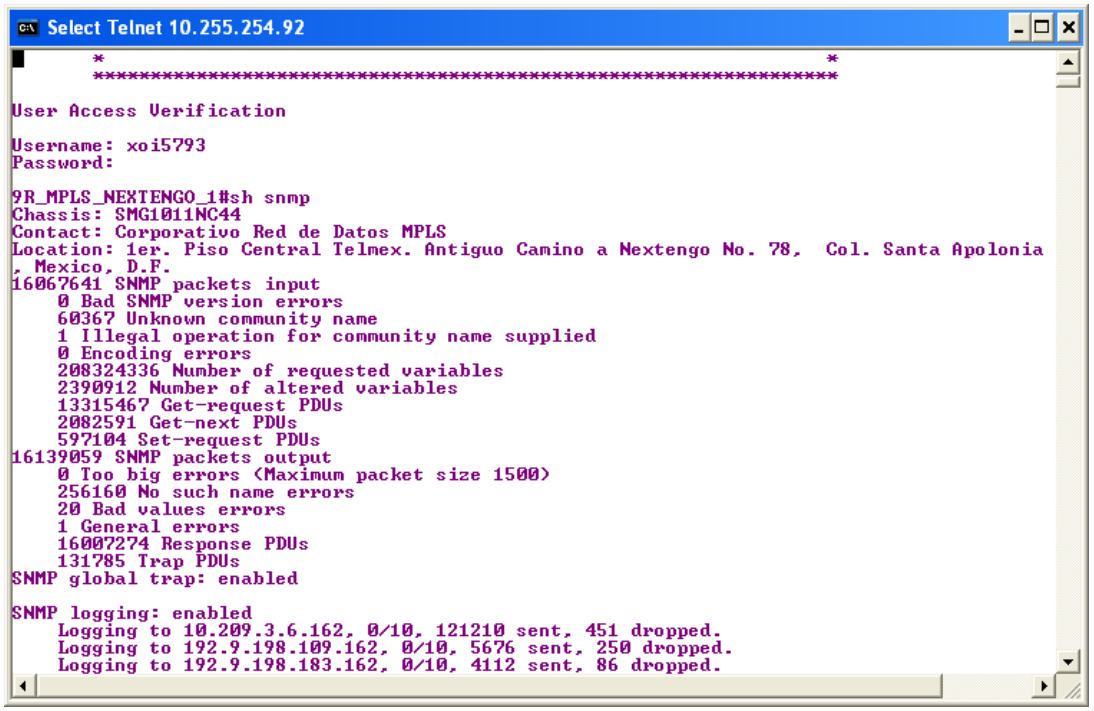


Figura 25. Ejemplo de un envió de mensajes SNMP a través de un Router

Para el Centro de Operación de la Red, este protocolo es de suma importancia ya que a través del protocolo SNMP funcionan varias de las herramientas de gestión, como las mencionadas en el apartado 3.

[29] UDP. Protocolo no orientado a conexión en el Stack TCP/IP.

6. Participación Profesional

La participación profesional en esta Operadora Telefónica, se lleva a cabo a través de aportar nuestro conocimiento y experiencia adquiridos en el ámbito del Networking, dando la solución a problemas de Red de Datos, además de contribuir con las áreas Corporativas a presentar los requerimientos necesarios para mantener la disponibilidad de la Red al 99.99%.

Las actividades realizadas diariamente son muy variadas en el Centro de Operación de la Red de Datos, algunas de ellas, las principales y más cotidianas han sido descritas en las diferentes secciones de este Informe, las cuales van desde la atención a reportes de usuarios, pasando por las diversas configuraciones que día con día son requeridas para levantar nuevos servicios a distintos clientes, hasta la resolución de problemas que puedan afectar el servicio de la red en alguna de la 9 regiones o a nivel nacional.

El análisis que se lleva a cabo en los equipos que integran la Red de Datos y de GPRS de esta Operadora, es siempre basado en Protocolos y Estándares establecidos por diversos fabricantes y Organizaciones de Estandarización, además de la actualización y estudio continuo de los Ingenieros que integran estas áreas de Operación y Mantenimiento.

En este ámbito laboral, mucha de la practica en la resolución de problemas (troubleshooting) se adquiere diariamente, y de forma muy general nuestro trabajo se puede resumir en el manejo de la Red de

Datos, llamado Networking, siguiendo básicamente el análisis de un problema a través de las 7 capas del modelo OSI, principalmente en capa 2 y 3 a un nivel avanzado, el modelo jerárquico de una red LAN, y la parte de seguridad de Redes de Datos; parte de este análisis ya fue descrito en las secciones 4 y 5.

7. Aportaciones

El trabajo realizado por Ingenieros que laboramos en áreas de Mantenimiento y de Operación de un Network Operation Center NOC. Es de suma importancia, ya que hoy en día las redes ya no sólo son consideras sistemas de transporte de datos, ni sólo una manera ágil de compartir información, sino son un componente crítico al éxito de las empresas, para el caso de esta empresa al ser una de las mejores Operadoras de Telefonía Celular, a la medida en que clientes, usuarios y proveedores utilizar la red para realizar diversas funciones que ofrece la Operadora, el desempeño de la red de datos y las aplicaciones que en ella corran es fundamental para mantenerse en el mercado como una empresa líder en su ramo, es por ello que el trabajo profesional que desarrollamos en el NOC es fundamental para mantener la disponibilidad de la red al 99%.

Con las actividades descritas a lo largo de este Informe de Trabajo apoyamos a la Operadora Telefónica a cumplir con los niveles de eficiencia, y productividad necesarios que requiere la Red de Datos, a través del manejo de diversos equipos y herramientas con los que realizamos la Gestión y Soporte a Servicios y Aplicaciones de la Red de Datos, siendo parte integral del éxito de esta empresa.

Al brindar servicios de Gestión y Soporte aseguramos: la eficiencia en el uso de ancho de banda, eliminando o minimizando el uso inapropiado de los recursos, la disponibilidad y alto desempeño de la red, reduciendo o eliminando perdidas de tiempo ocasionados por fallas en el servicio, la prioridad de transporte para usuarios o servicios mas

importantes además de asegurar la disponibilidad y alto desempeño de aplicaciones críticas, eliminando perdidas de transacciones realizadas a través de Internet.

El NOC de la Operadora Telefónica, se conforma por un gran equipo de Ingenieros, quienes tenemos la responsabilidad prevenir problemas ocasionados por mal desempeño de la red y aplicaciones; controlar el uso de los recursos; y predecir las necesidades de la infraestructura para agilizar el crecimiento de la empresa; así como mantenernos actualizados ante las nuevas tecnologías que se integran día a día en esta amplia Red de Datos.

8. Conclusiones

La creación de este Informe de Trabajo, cumplió con el objetivo principal dar a conocer las actividades profesionales que realiza un Ingeniero de Red en el Centro de Operación de la Red de Datos de una Operadora Telefónica.

La información que se presentó a lo largo de este Informe, se adquirió a través del trabajo que se realiza día con día sobre cado uno de los elementos que integran la Red de Datos, fuentes de información de distintos fabricantes como son principalmente Cisco, Nortel, Nokia y Junipers, además de complementarse con mi desarrollo profesional y el aprendizaje continuo que he adquirido en esta empresa.

Generalmente las áreas de soporte en una Red de Datos son de las más importantes, ya que es aquí donde se tiene el contacto real con la implementación de nuevas tecnologías, vigilancia en el desempeño de la Red Datos y sobre todo la resolución a los distintos problemas, logrando con ello adquirir una amplia experiencia en el manejo de Redes.

9. Bibliografía

Páginas Consultadas:

www.cisco.com
www.juniper.net

Libros Consultados:

Tisal, Joachim, *La Red GSM*, Parafino Thomson Lerning, España, 2000, PP 157-170.

Reyders Deon y Wright Edwin, P*ractical TCP/IP and Ethernet Networking*, El Servier, EUA, 2003, PP 150-154

Manuales:

GPRS
Performance Management
Roaming Basics
Troubleshooting Nokia GGSN

ISNDO0040.00
Nokia GGSN Release 4.0 Product
Documentation
Troubleshooting Nokia GGSN