ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRONICA, REDES Y COMUNICACIÓN DE DATOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA

AUTOR: LORENA MOSERRATTE PÁEZ MARTÍNEZ

TEMA: ANÁLISIS DEL TRÁFICO DE LA RED PARA LA OPTIMIZACIÓN Y MEJORA DEL SISTEMA VSAT DE CNT EP.

DIRECTOR: ING.SÁENZ, FABIAN

CODIRECTOR: ING. ROMERO, CARLOS

SANGOLQUÍ, FEBRERO 2014

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: ANÁLISIS DEL TRÁFICO DE LA RED PARA LA OPTIMIZACIÓN Y MEJORA DEL SISTEMA VSAT DE CNT EP., ha sido desarrollado en su totalidad por la señorita LORENA MONSERRATTE PÁEZ MARTÍNEZ, bajo nuestra dirección.

Atentamente

Ing. Fabián Sáenz E. **DIRECTOR**	Ing. Carlos Romero G. **CODIRECTOR**

DECLARACIÓN DE RESPONSABILIDAD

LORENA MOSERRATTE PÁEZ MARTÍNEZ

DECLARO QUE:

El proyecto denominado "**ANÁLISIS DEL TRÁFICO DE LA RED PARA LA OPTIMIZACIÓN Y MEJORA DEL SISTEMA VSAT DE CNT EP**", ha sido desarrollado en base a una investigación exhaustiva, respetando los derechos intelectuales de terceros, conforme a las fuentes que se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 14 de Febrero de 2014.

Lorena Monserratte Páez Martínez

AUTORIZACIÓN

LORENA MONSERRATTE PÁEZ MARTÍNEZ

Autorizo a la Universidad de las Fuerzas Armadas “ESPE” la publicación, en la biblioteca virtual de la Institución del trabajo “ANÁLISIS DEL TRÁFICO DE LA RED PARA LA OPTIMIZACIÓN Y MEJORA DEL SISTEMA VSAT DE CNT EP”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 14 de febrero de 2014.

Lorena Monserratte Páez Martínez

DEDICATORIA

A ti mami, por enseñarme siempre, a ser constante y perseverante. Por todos tus consejos, mimos y abrazos. Por todo tu esfuerzo por formar y mantener la familia tan unida que ahora somos; y por enseñarme a valorar que el regalo más importante que uno tiene en la vida es la familia.

A ti papi, por enseñarme a no escoger el camino más fácil en la vida y demostrar que con perseverancia y constancia se logra aun el reto más difícil.

A ti hermana por día a día soportar mi mal humor y saberme apoyar de cualquier manera; por haberte eximido de ciertos privilegios que yo tuve durante esta etapa.

A ti Andrés por ser mi impulso y mi motor, gracias estar siempre pendiente de mí y enseñarme a ser perseverante; gracias por darme ánimos para culminar esta etapa que es uno de mis logros más anhelados.

Lorena Páez M.

AGRADECIMIENTOS

A DIOS por haber sido mi motor, mi guía y por llenarme con su inmensa sabiduría todos estos años de carrera universitaria. Gracias a ti mi Divino Niño por escuchar siempre mis peticiones y ser tan bueno y bondadoso conmigo.

A quienes siempre han sido mi apoyo, mi fuerza; quienes siempre confiaron y creyeron en mí. Gracias Padre por haberme brindado la posibilidad de desarrollarme profesionalmente, y por ser mi ejemplo a seguir.

Como no agradecerte Madre por todas las palabras de aliento, cariño y motivación; por estar siempre junto a mí y enseñarme a valorar las pequeñas cosas que da la vida, porque siempre me enseñaste que más allá de crecer profesionalmente, es más importante crecer como persona.

A mi hermana que desde niña fue un complemento en mi vida; gracias por tu compañía, y por formar parte de mi vida y porque a pesar de las peleas de hermanos, siempre estuviste ahí.

A ti amor mío, Andrés, como no agradecerte que formes parte de mi vida y que hayas sido mi impulso para hoy obtener este logro tan grande. Gracias por ser esa persona tan especial, y por día a día ayudarme a crecer y a ser mejor.

A todas y cada una de las personas que ocupan un lugar en mi corazón y que hacen de cada momento vivido en la universidad, un bonito recuerdo que lo llevaré por siempre en mi memoria. Gracias amigos por estos cinco años de esfuerzo, sacrificio, malas noches y buenos momentos compartidos.

A mis queridos Ingenieros Fabián Sáenz y Carlos Romero por todo su apoyo y cariño durante mi carrera universitaria, por que más que profesores y orientadores fueron mis amigos quienes me supieron brindar palabras de aliento y consejos en duros momentos. Para ustedes mi aprecio incondicional

RESUMEN

La red satelital VSAT banda Ku de CNT fue creada para brindar servicio a 1500 usuarios en los lugares más lejanos del territorio ecuatoriano. Actualmente los usuarios finales han percibido que su navegación en Internet se ha vuelto lenta, y en ciertas ocasiones no pueden ingresar a ninguna página. Es necesario entonces buscar analizar el tráfico cursante de la red y buscar las causas y posibles soluciones que permitan un mejor desempeño de la red y por ende un servicio mejor al usuario final; para lo cual se hará uso de la herramienta PRTG, y el equipo ALLOT. El presente proyecto se ha desarrollado específicamente para buscar la solución óptima ante el problema actual que presenta la red VSAT de CNT EP, para lo cual se procede a realizar pruebas de la red en diferentes días y horas para poder verificar la velocidad de navegación de internet, y de esta manera encontrar las causas del problema; posteriormente se realiza el análisis del tráfico y se encuentran las posibles soluciones.

PALABRAS CLAVES:

- VSAT
- CNT
- TRÁFICO
- ALLOT
- PRTG

ABSTRACT

The Ku band VSAT satellite network of CNT was created to service 1500 users in the far reaches of Ecuador. Currently end users have received your Internet surfing has become slow, and at times can not enter any page. It is then necessary to analyze traffic trainee search the net and look for possible causes and solutions to better network performance and hence a better service to the end user , for which PRTG will use the tool , and device ALLOT . This project is specifically developed to find the optimal solution to the current problem with the network VSAT of CNT EP, for which we proceed to perform network testing on different days and hours to verify Internet browsing speed , and thus find the causes of the problem, then traffic analysis is performed and the possible solutions are .

ANÁLISIS DEL TRÁFICO DE LA RED PARA LA OPTIMIZACIÓN Y MEJORA DEL SISTEMA VSAT DE CNT EP.

CNT EP. Implementó la red VSAT banda KU, con el propósito de brindar servicio de internet a los sitios más lejanos del territorio ecuatoriano. En los últimos meses los usuarios finales de la red presentan quejas acerca de la lentitud del internet, y en casos la falta del mismo. Por lo cual CNT EP. Solicita asistencia en cuanto al problema, buscando las posibles causas de la lentitud de la red.

En base a la necesidad de tener un buen servicio, y cumplir con los requerimientos de la empresa, se realiza un exhaustivo análisis de la red VSAT, buscando las f la simultaneidad de la red y comprobar si la red está en saturación; para lo cual se revisa previamente el dimensionamiento actual y contractual de la red.

En el **Capítulo 4**, se plantean soluciones ante el problema de saturación que presenta la red; previo a esto se realiza un análisis de resultados prácticos y teóricos, para poder presentar una solución óptima y aporte con la mejora del desempeño de la red.

Finalmente, en el **Capítulo 5**, se presentan las conclusiones y recomendaciones obtenidas de todo el proceso de análisis, presentando de esta manera las soluciones óptimas para la mejora del sistema.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

Spam: Correo basura, mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, enviados en grandes cantidades (masivas) que perjudican de alguna o varias maneras al receptor.

ICMP: Es el Protocolo de Mensajes de Control de Internet, el cual da control y notificación de errores del Protocolo de Internet (IP). Es decir, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

DNS: Sistema de nombres de dominio.

Malware: También llamado badware, o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

SSL, TLS: Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

SSH: Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

UDP: Es un protocolo del nivel de transporte basado en el intercambio de datagramas

HTTP : Protocolo de transferencia de hipertexto. El propósito del protocolo es permitir la transferencia de archivos entre un navegador y un servidor web.

HTTPS: Protocolo de transferencia de hipertexto de forma segura. A diferencia de HTTP utiliza un cifrado basado en SSL (**Secure Socket**

Layers)**,** creando un canal de transferencia cifrado para aumentar la seguridad en la transferencia de datos.

IP: Protocolo de Transferencia de Archivos entre sistemas conectados a una red TCP, funciona en la capa de red del modelo OSI.

SMTP : Protocolo para la transferencia simple de correo electrónico entre ordenadores o dispositivos, que funciona en la capa de aplicación.

POP: Protocolo de Oficina de Correo, en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de la capa de aplicación del modelo OSI.

IMAP: Internet Message Access Protocol, es un protocolo de la capa de aplicación, que permite el acceso a mensajes electrónicos almacenados en un servidor.

POP3s: Post Office Protocol versión 3, dirigido a través de la capa SSL que permite la obtención de correo electrónico de manera segura.

IMAPs: Internet Message Access Protocol dirigido a través de la capa SSL.

ACM: Codificación y Modulación Adaptativa que permite al sistema variar dinámicamente la modulación y códigos en el canal de Outroute para cada transmisión.

CAC: Control de acceso condicional, generan los key necesarios para la n y des-encriptación de los paquetes IP.

CDS: Sistemas Demoduladores Configurables.

DHCP: (*Dynamic Host Configuration Protocol*, permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata

de un protocolo de tipo cliente en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

DNCC : (Direcway Network Control Cluster). Controlador o procesador de las informaciones enviadas a través de los Inroutes.

DNS: (Domain Name System), en español: sistema de nombres de dominio es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes.

DSCP: Hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan.

DVB-S: (Digital Video Broadcasting by Satellite) Es un sistema que permite incrementar la capacidad de transmisión de datos y televisión digital a través de un satélite UH11 usando el formato MPEG2. La estructura permite mezclar en una misma trama un gran número de servicios de video, audio y datos.

DVB-S2: (Digital Video Broadcasting by Satellite - Second Generation) es un estándar de transmisión de televisión digital considerado el sucesor del sistema DVB-S, ratificado durante 2005por el organismo regulador ETSI.

HPA: (High Power Amplifier) proporciona una sensibilidad de entrada adecuada para propagar la señal al transponder del satélite.

HTTP: (Hypertex Transfer Protocol) Protocolo de transferencia de hipertexto es el método más común de intercambio de información en la world wide web, el método mediante el cual se transfieren las páginas web a un ordenador.

TRANSPONDER: Un Transponder (transmisor-receptor) es una cadena completa de dispositivos montados sobre un satélite artificial de telecomunicaciones, que permite recibir señales de radiocomunicación emitidas desde cierta región de la Tierra en una frecuencia, las convierte a otra frecuencia, las amplifica y retransmite a una cierta zona ubicada en un punto de la tierra.

IGMP: (Internet Group Managment Protocol) El protocolo de red se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.

MPLS: (*Multiprotocol Label Switching*) es un mecanismo de transporte de datos estándar creado por la IETF. Opera entre la capa de enlace de datos y lacapa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MSPS: (Mega Símbolos por Segundo). En la modulación digital, a la relación de cambio a la entrada del modulador se le llama *bit-rate* y tiene como unidad el bit por segundo (bps). A la relación de cambio a la salida del modulador se le llama *baud-rate*. En esencia el *baud-rate* es la velocidad o cantidad de símbolos por segundo.

TDMA: (*Time Division Multiple Access*) La *multiplexación por división de tiempo* es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del

SNMP : (*Simple Network Management Protocol*), El Protocolo Simple de Administración de Red o es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

STREAMING: Es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto al mismo tiempo que se descarga. La palabra *streaming* se refiere a que se trata de una corriente continua (sin interrupción). Este tipo de tecnología funciona mediante un búfer de datos que va almacenando lo que se va descargando para luego mostrarse al usuario. Esto se contrapone al mecanismo de descarga de archivos, que requiere que el usuario descargue los archivos por completo para poder acceder a ellos.

THROUGHPUT: Se llama *throughput* al volumen de trabajo o de información que fluye a través de un sistema. Así también se le llama al volumen de información que fluye en las redes de datos.

UEM: Administrador Unificado de Elementos, sistema que permite el comisionamiento de los remotos, proporciona las claves de acceso condicional a los remotos, gestión y descarga de software.

UNICAST: Es el envío de información desde un único emisor a un único receptor.

ENDPOINTS: Son puntos de destino y origen de los mensajes que transportan los datos desde un punto hasta otro punto.

CAPÍTULO I: INTRODUCCIÓN

1.1. ANTECEDENTES

CNT empresa pública dedicada al sector de las telecomunicaciones a nivel nacional, especializada en brindar soluciones para las comunicaciones a largas distancias, tiene por finalidad brindar el servicio de telecomunicaciones como un servicio social, contribuyendo de esta forma al desarrollo del país.

La Corporación Nacional de Telecomunicaciones CNT, actualmente posee una red satelital en banda KU, la misma que brinda un servicio social de internet a sitios alejados o de difícil acceso del Ecuador. Esta red contiene un Hub satelital que maneja el consumo de ancho de banda, a través de equipos compresores de imágenes y aceleradores del servicio de internet.

El sistema VSAT está conformado por 1500 terminales distribuidos a nivel de todo el país, con velocidades asignadas según su prioridad; 938 Centros Educativos 256x128 kbps, 291 Eurosolares 512 x128 kbps, 362 Centros de Salud y Cooperativas 28x64 kbps, 200 Infocentros 1024x512 kbps Debido a la necesidad del correcto funcionamiento del servicio de internet en los terminales, se requiere un monitoreo periódico del sistema. (HUGHES, 2012)

1.2. JUSTIFICACIÓN E IMPORTANCIA

Actualmente el consumo total de los terminales VSAT sobrepasa el consumo de ancho de banda previsto, presentando de esta manera retardo en la red, debido a que el ancho de banda total de la red es 40Mbps. Es necesario analizar el funcionamiento de los equipos compresores que se

encuentran en el Hub, ya que estos manejan el consumo de ancho de banda, y controlan la simultaneidad de cada terminal

Debido al bajo rendimiento que presenta la red VSAT de CNT EP, se requiere realizar un estudio sobre el causal del retardo para mejorar el rendimiento de dicha red y brindar un mejor servicio a los usuarios. Es muy importante encontrar una pronta solución al problema que existe en la red a través de la implantación de equipos de monitoreo de tráfico, gestionar las velocidades de cada uno de los terminales para que sean aceptables y de esta manera poder encontrar soluciones para que no exista saturación en la red. En virtud que este servicio es dedicado a los sitios más lejanos y necesitados del país, es indispensable el funcionamiento adecuado de la red.

El monitoreo de redes es esencial para sistemas de cualquier tamaño, es por eso que es necesario escoger la herramienta de monitoreo apropiada, ya que esta no sólo asegura la notificación cuando ocurren averías, sino que también nos ayudará a rastrear el consumo de recursos y de ancho de banda

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Analizar el tráfico cursado por la red a través del equipo ALLOT, para mejorar y optimizar la misma.

1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar la situación actual de la red, para determinar la saturación.

- Revisar el funcionamiento de la red, así como también realizar el diagrama actual de la misma.
- Analizar los equipos inmersos en la red para comprobar la simultaneidad de la red.
- Implantar el gestor PRTG para monitorear periódicamente la red.
- Analizar el tráfico de la red VSAT de CNT EP para encontrar los problemas usando el gestor de red.
- Sugerir soluciones para optimizar la red y evitar la saturación en la misma.
- Realizar una evaluación económica para determinar la mejor solución de la red.

1.4. MARCO TEÓRICO

1.4.1. SISTEMA SATELITAL

Un sistema Satelital tiene el propósito de enlazar múltiples sitios de comunicaciones, con el propósito de obtener una comunicación eficiente; dicho sistema está compuesto por los siguientes segmentos:

1.4.2. SEGMENTO ESPACIAL

Este segmento se refiere a la ubicación de satélites artificiales de comunicaciones, ya que es un medio muy útil para emitir señales de radio en zonas amplias o poco desarrolladas y alejadas; pueden utilizarse como un repetidor de radio (transpoder), el cual recibe las señales de microondas a una cierta frecuencia denominada uplink, y la retransmite en otra frecuencia diferente denominada downlink.

1.4.3. SEGMENTO TERRESTRE

a) Estación Terrestre: Se encarga de transmitir la información del usuario en Tierra hacia el Satélite ubicado en el espacio. En el Satélite, el transponder recibe la señal, la amplifica, cambia su frecuencia y la retransmite.

FIGURA 1: Estación terrestre

b) Estación Remota: Se refiere a la estación ubicada en el usuario final y se encarga de proveer internet al usuario.

1.4.4. BANDAS DE FRECUENCIAS SATELITALES

Los satélites comerciales generalmente operan en dos bandas de frecuencias, llamadas C y Ku.

TABLA 1: Frecuencias C y KU

Banda	Frecuencia ascendente (GHz) Uplink	Frecuencia descendente (GHz) Downlink	Problemas
C	5,925 - 6,425	3,7 - 4,2	Interferencia Terrestre
Ku	14,0 - 14,5	11,7 - 12,2	Lluvia

1.4.4.1. BANDA C

Para evitar posibles interferencias entre satélites que trabajan en la misma frecuencia, lo que se recomienda, en la banda C es separarlos a una distancia mínima de 2 grados entre sí, por lo que en la práctica esto limita el número total de satélites puestos en órbita a 180 en total.

Una de las ventajas de esta banda es que presenta un mínimo de atenuación, por otra parte, su principal problema son las interferencias terrestres por lo que se debe encontrar un sitio adecuado, libre de interferencias, para colocar una estación remota dentro de la ciudad. (Ftapinamar, 2010)

1.4.4.2. BANDA KU

La banda Ku está destinada para servicios de comunicación satelital, siendo la televisión uno de sus principales usos, ya que las interferencias terrestres no son obstáculos para ella. Los satélites deben estar ubicados a una distancia mínima entre ellos para evitar posibles interferencias, en este caso la distancia será de un grado, lo que en la práctica limita a tener 360 satélites en órbita. Por otra parte, el tamaño de las antenas en banda Ku es menor comparado con la banda C. (ZatInforme, 2007)

1.4.5. EQUIPOS DE LA RED

Cada Estación Remota posee una banda garantizada y una banda máxima, tanto en Inroute (portadora generada desde las estaciones remotas), como Outroute (portadora generada desde el sistema central) La red está conformada por dos secciones, la Estación satelital Remota y el Sistema Central (denominado HUB). La topología de la red es en estrella, al igual que las redes VSAT tradicionales.

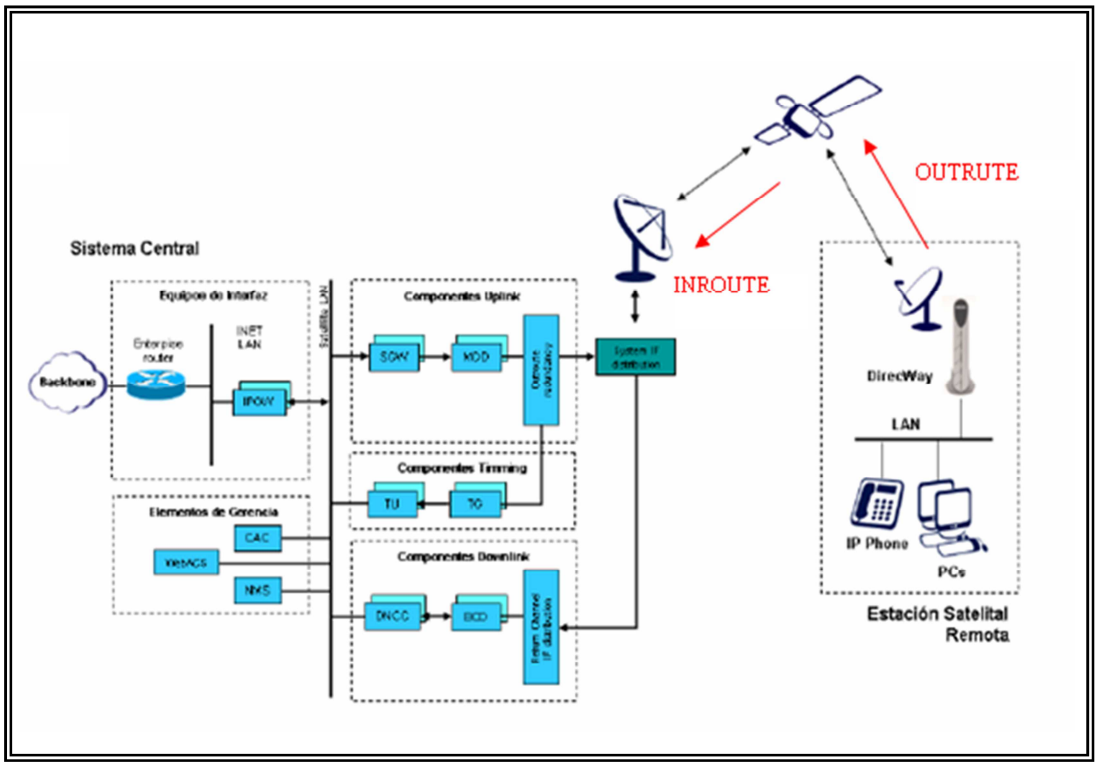

FIGURA 2: Esquema sistema satelital

1.4.5.1. ESTACIÓN REMOTA

Conformada por:

- Unidad Interna (IDU)
- Antena parabólica

- Unidad Externa (ODU)

1.4.5.1.1. Unidad Interna (IDU)

Realiza el procesamiento de la señal digital recibida a través del Outroute y las puertas para datos de usuario. Igualmente, realiza el procesamiento de la señal de los datos de usuario desde las puertas preparándolas para su transmisión a través del Inroute. (HUGHES, 2010)

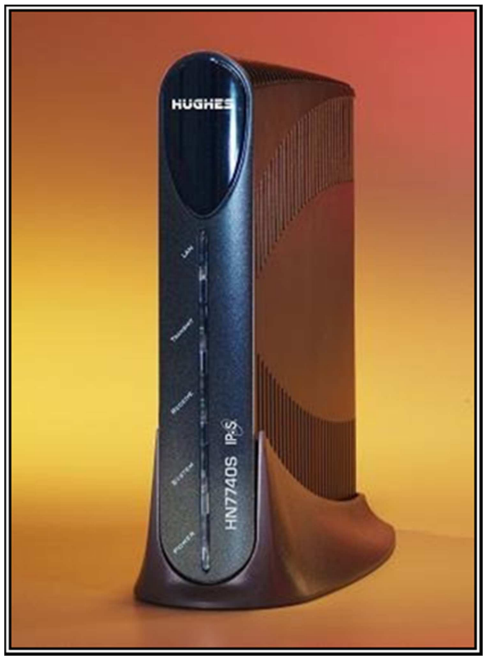

FIGURA 3: Unidad interna IDU

1.4.5.1.2. Antena Parabólica

Generalmente varían desde 1,2 Mts hasta 2.4 Mts. Estas antenas de fibra de vidrio reforzadas con un tipo especial de poliéster; poseen la propiedad de un material impermeable al agua minimizando las atenuaciones.

Su función es la de concentrar toda la potencia generada por la RF en un haz muy fino que está apuntando al satélite al igual que concentrar toda la

señal recibida por su superficie hacia la entrada del amplificador de recepción, LNA. (HUGHES, 2010)

FIGURA 4: Antena Parabólica

1.4.5.1.3. Unidad Externa (ODU).

Es un equipo que integra la electrónica de radiofrecuencia (RF), el amplificador de potencia de estado sólido (SSPA), el amplificador de recepción (LNB), los conversores de frecuencia (up/downconverters), la bocina cónica corrugada (feedhorn) y el acoplador ortomodo (OMT).

Su función es convertir la frecuencia desde Banda L a la banda de trabajo del Satélite y viceversa. Igualmente, amplifica la señal que proviene de la IDU a los niveles que requiere el sistema central en la transmisión y amplifica la señal total del satélite (señal y ruido) a niveles óptimos para ser demodulados en la recepción. (HUGHES, 2010)

FIGURA 5 Unidad externa ODU

1.4.5.2. ESTACIÓN CENTRAL

Conocido como NOC (Network Operation Center), es el encargado del monitoreo en tiempo real, control y administración de la red, capacidad de generación de reportes incluyendo estudio de horas pico, uso del canal y de los puertos. CNT EP. Dispone de una Estación Central en el puente 7(estación terrena), además de toda la infraestructura de periféricos necesarios para el monitoreo permanente de la red.

1.4.5.3. SISTEMA SATELITAL HUGHES

El sistema HN de HUGHES consta de un modem satelital y un router IP con características optimizadas para comunicaciones vía satélite, incluye también un avanzado sistema de manejo de ancho de banda y priorización de tráfico que permite configurar múltiples definiciones de QoS.

Todos los sistemas satelitales IP de banda ancha de HUGHES usan el estándar DVB para el canal de transmisión OUTROUTE, proveyendo ventajas significativas al operador.

Posee una eficiente escalabilidad en los canales DVB para soportar portadores desde 1 Msps hasta 45 Msps en el canal de Outroute, esto no obliga al operador a trabajar con canales de Outroute menores de manera artificial (10 Msps como la mayoría de sistemas). (HUGHES)

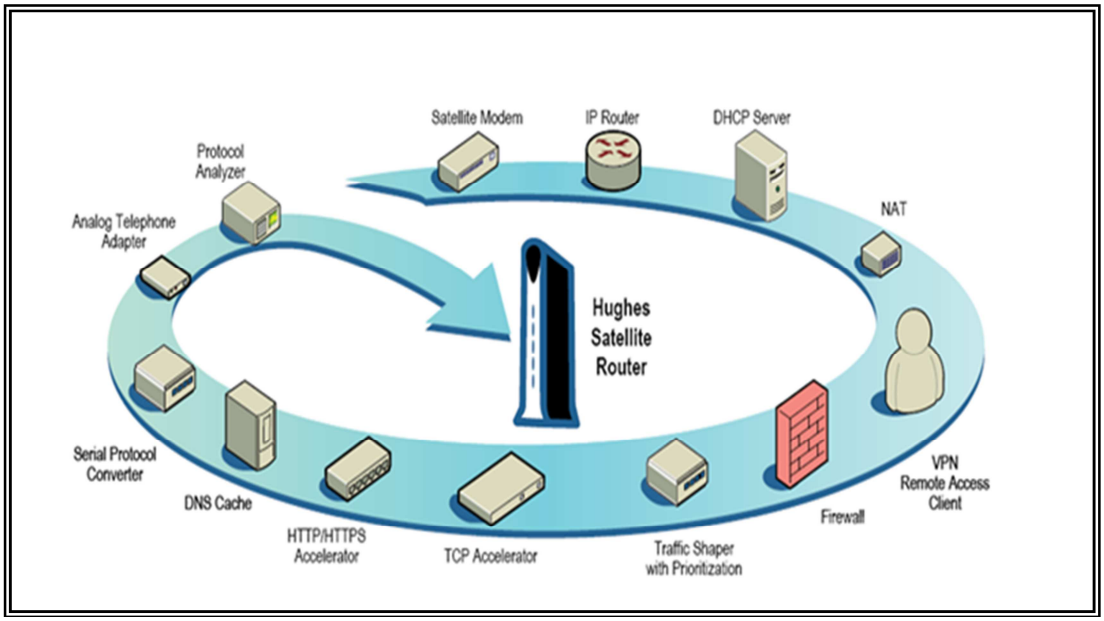

FIGURA 6: Características HN

1.4.5.3.1. Eficiencia Inroute

El sistema HN presenta un avanzado sistema de asignación dinámica de ancho de banda con una variedad de planes de QoS para múltiples perfiles de trabajo. Adicionalmente, se emplean tramas de transmisión de longitud variable para el Inroute, optimizando su uso por la demanda existente en tiempo real.

Entre las funcionalidades claves del Inroute están:

- Eficiencia del Ancho de Banda en el Inroute.
- Asignación dinámica de ancho de banda.
- Escalabilidad.
- Alta calidad en el servicio.

1.4.5.3.2. Seguridad de Red

El sistema HN incluye un mecanismo de Acceso Condicional que es usado para prevenir espionaje de terminales remotas sobre el tráfico de Outroute. Adicionalmente, el sistema maneja encriptación de llaves propias para cada terminal. Dado que las funciones de encriptación están integrados en el sistema; la aceleración y priorización de tráfico se mantienen.

1.4.5.4. DIMENSIONAMIENTO ACTUAL DE LA RED

Se presenta la solución de HUGHES para soportar 1,500 sitios con los siguientes planes de servicio:

SERVICIO DE INTERNET

TABLA 2: Número de Estaciones

N0. De Sitios	Outroute (Kbps)	Inroute (Kbps)
5	1,024	256
310	512	128
406	256	128
779	128	64

Se puede observar en la tabla el número de estaciones y planes de servicio, el porcentaje de simultaneidad realizado en el dimensionamiento es

12% para el Outroute y 7% para el Inroute. Además una compresión de tráfico de 15% para el Outroute y 20% para el Inroute.

Idu

A través del router HN7740S con 2 puertos de voz integrados al chasis, así como 2 puertos RJ45 Ethernet 10/100 Base T que soporta diferentes funcionalidades.

Outroute

Una portadora Outroute DVB-S2 con ACM, que permite modulación dinámica 16PSK y 8PSK, 11.5 Msps que da una velocidad aproximada de 30.7 Mbps en 13.8 MHz**.**

De manera general los valores anteriores se calcularon en base a un estudio de Ingeniería de HUGHES basado en la modulación y codificación adaptativa que soporta el Outroute, se basó también en un estimado del porcentaje de uso de las codificaciones por remota, además se tomó en cuenta el tráfico de usuario, así como también el tráfico que se requiere para el sistema de monitoreo y gestión de la red y el tráfico que se usará para las diferentes aplicaciones.

Inroute:

Al igual que el dimensionamiento del Outroute, en el Inroute se realizó un estudio minucioso del tráfico necesario para cada aplicación requerida por el usuario, así como también el tráfico de administración y control, la transacción diaria de bits por sitio, un promedio de tamaño de paquetes enviados por las Inroutes, el uso de bits para los mecanismos de sincronismo entre otros.

En definitiva el dimensionamiento del Inroute es más complejo que el dimensionamiento del Outroute por lo que solo se considera los valores proporcionados por HUGHES sin necesidad de cálculos.

21 portadoras Inroute de 256 Ksps con la funcionalidad de AIS (Adaptive Inroute Selection), que permite hasta 8.15 Mbps de velocidad en 7.52 MHz, con un 80% de sitios configurados en 256 Ksps y FEC 4/5 y 20% de sitios configurados con 256 Ksps con FEC 2/3.

1.5. DIAGRAMA DE LA RED

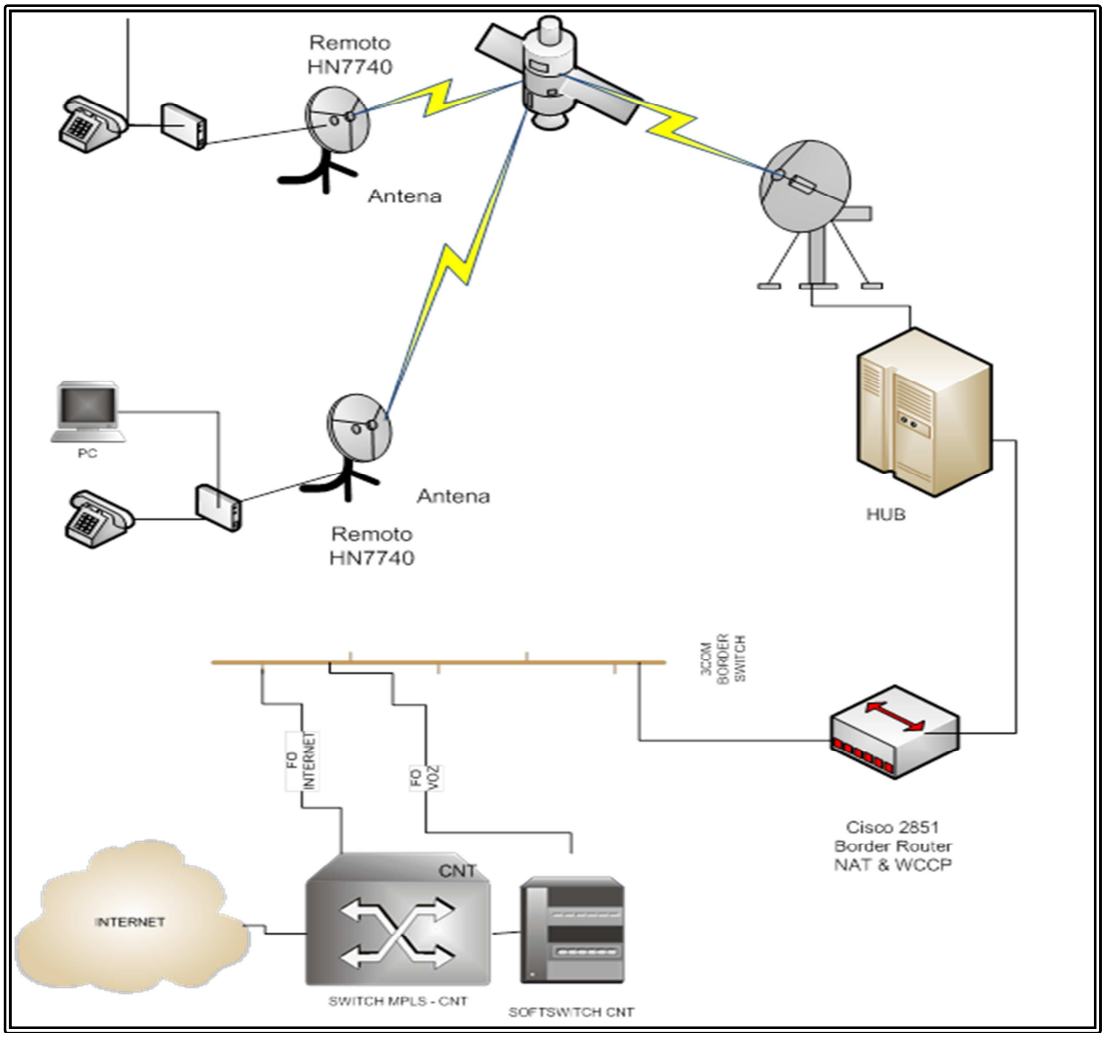

FIGURA 7: Diagrama del sistema VSAT

CAPÍTULO II: ANÁLISIS DE LOS EQUIPOS INMERSOS EN LA RED

2.1. DIAGRAMA ESQUEMÁTICO DEL HUB

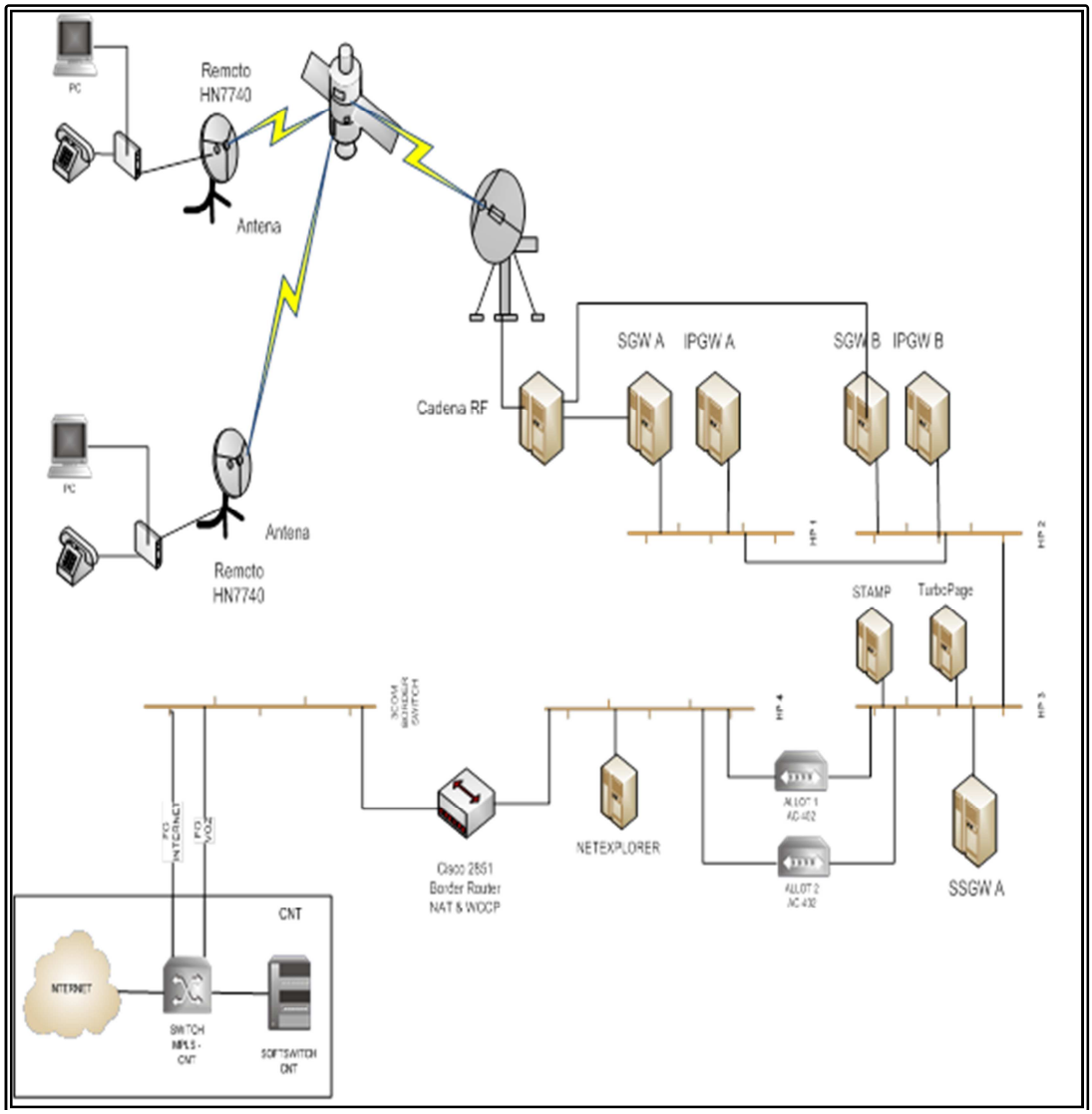

FIGURA 8: Diagrama esquemático del HUB

2.2. DESCRIPCIÓN DE LOS COMPONENTES

A continuación se describirán los equipos que conforman el HUB. El Centro de Operaciones de la Red es el punto central o eje del Sistema HN de HUGHES. Se ofrece una alta velocidad de transmisión de paquetes IP hacia y desde los terminales remotos. El HUB posee equipos de

procesamiento de banda base, subsistema IF, subsistemas de control y el sistema de gestión de red.

El HUB soporta TDM/TDMA Acceso múltiple del segmento espacial de satélite para el acceso eficiente de la red de satélites. El equipo de banda base del NOC HN se compone de un subsistema de enlace ascendente de satélite, un subsistema de temporización y un subsistema Inroute con todos los componentes críticos configurados con la suficiente redundancia para soportar la máxima disponibilidad de la red.

2.2.1. SUBSITEMA DEL ENLACE SATELITAL ASCENDENTE

El subsistema del enlace satelital ascendente soporta transmisión IF con Outroutes mayores 30 Msps de capacidad y 36MHz del transponder satelital. El HUB cuenta con un equipo denominado Satélite Gateway (SGW). El SGW es el elemento clave dentro del subsistema de enlace ascendente. Este recibe el tráfico satelital desde los otros componentes del NOC HN sobre el segmento llamado LAN, les da formato en paquetes individuales, y los reenvía al modulador DVB-S2 para la transmisión sobre el satélite. El SGW también recibe el tráfico satelital de los distintos subsistemas, incluyendo las puertas de enlace IP (IP GATEWAYS), DNCC (configuran las inroutes las frecuencias) y elementos de gestión de red en un segmento de LAN. Los SGWs pueden recibir tráfico usando direcciones unicast y/o multicast. (HUGHES, 2010)

2.2.2. SUBSITEMA DE INROUTE

El subsistema de Inroute está configurado con cuatro Sistemas Demoduladores Configurables (CDS). Cada módulo de CDS puede

demodular la capacidad total de la Inroute de 2,5 Msps. El subsistema satelital ascendente y el subsistema de Inroute son escalables para soportar a futuro un Outroute y 36 Inroutes de 256 Ksps. El grupo de control de la red HN (DNCC) es responsable de la multiplexación eficiente del canal de retorno del tráfico TDMA. El DNCC puede ser considerado como el gestor de ancho de banda del sistema HN.

2.2.3. SUBSISTEMA DE TEMPORIZACIÓN

El subsistema de temporización HN incluye un generador de temporización (TG2) y dos unidades de temporización (DTU), que proporciona la sincronización maestra para todo el sistema. Además, mantiene la sincronización de tiempo entre los componentes del NOC HN y los terminales remotos. La puerta de enlace IP (IPGW) proporciona la interfaz entre el NOC y las conexiones de datos terrestres. Los IPGWs realizar la asignación de dirección IP, la transmisión de paquetes, compresión y otras funciones necesarias para comunicarse con los terminales remotos HN de HUGHES. La interfaz entre los IPGWs y el mundo "exterior" es a través del protocolo IP estándar. Los IPGWs están diseñados con redundancia de tal forma de que si falla el primario entra a funcionar el secundario. Hay 4 servidores IPGW en la configuración de NOC.

2.2.4. SISTEMA DE GESTIÓN DE LA RED

El sistema HN utiliza el Administrador Unificado de Elementos (UEM), sistema que permite el comisionamiento de los remotos, proporciona las claves de acceso condicional a los remotos, gestión y descarga de software. El NMS permite la configuración, administración, gestión y control de los

componentes del NOC HN y las IDUs remotos. El NMS además permite al operador realizar dos operaciones de red (como la supervisión del estado de la red y las estadísticas) y las actividades generales de gestión de red (como la configuración y el control). El sistema de gestión además permite que varios usuarios clientes accedan a la vez al sistema de monitoreo del estado de la Red.

La UEM consiste de los siguientes componentes:

VISION: Ofrece una configuración y una interfaz de control para muchos de los componentes del NOC

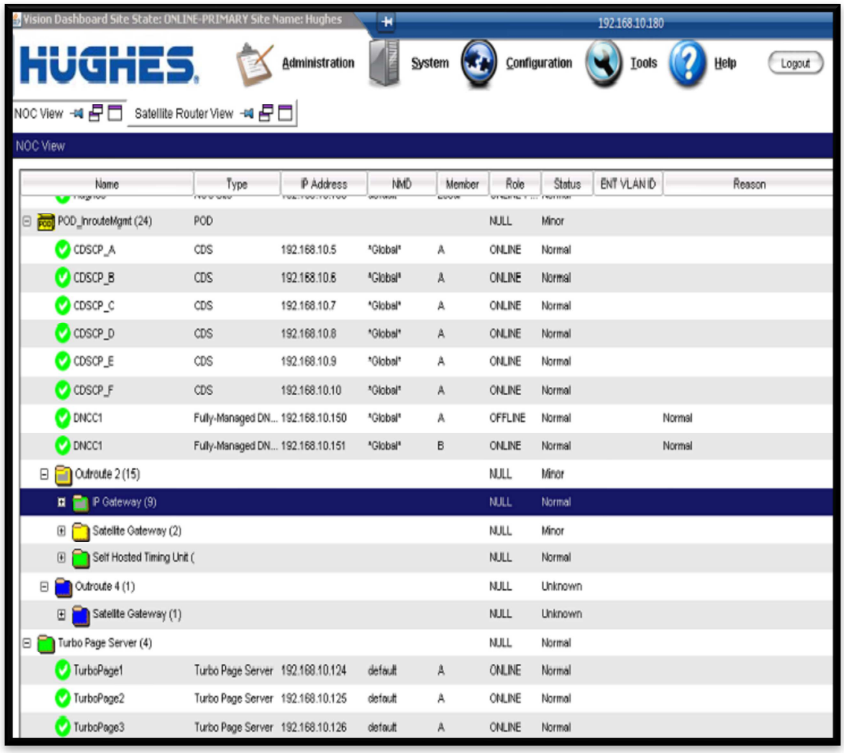

FIGURA 9: Componente Vision

CAC: Proporciona el control de acceso para la información transmitida a través del servicio de HUGHES Net.

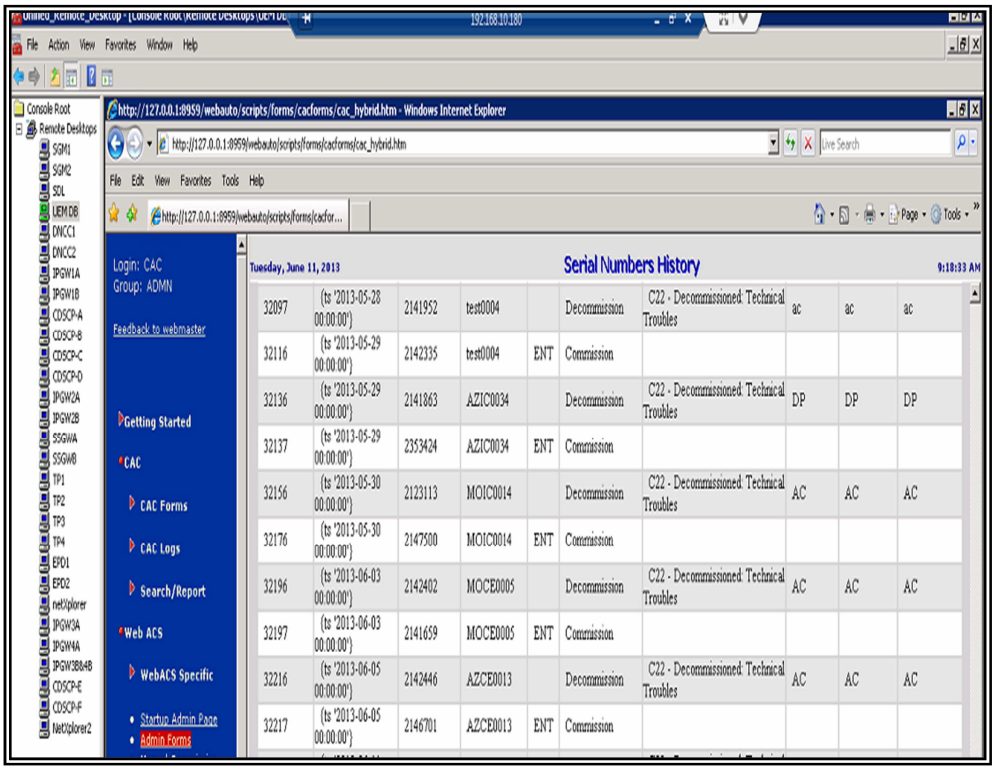

FIGURA 10: Componente CAC

WebACS: Ofrece servicios de puesta en servicio de módems satelitales.

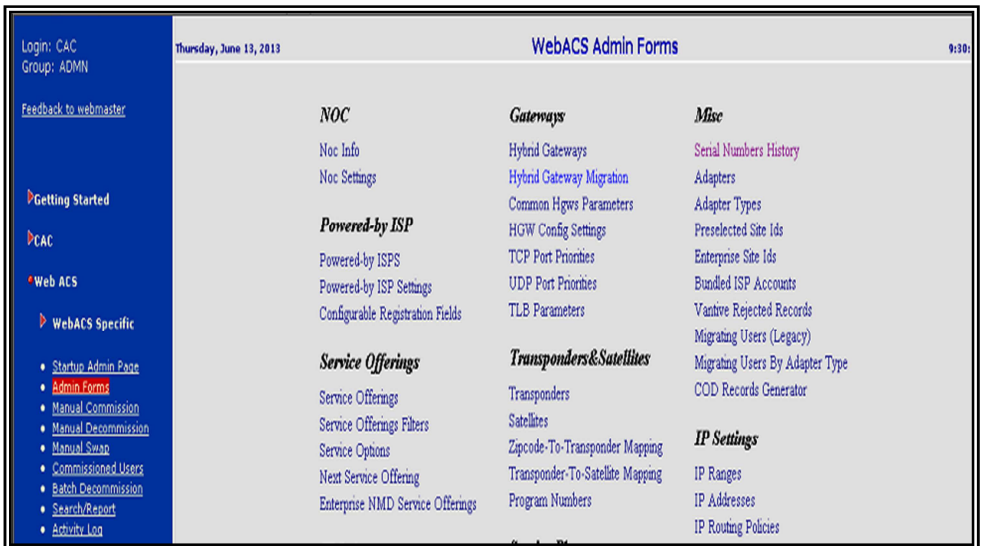

FIGURA 11: Componente WebACS

Base de datos de la UEM: Almacena todos los datos de configuración de red.

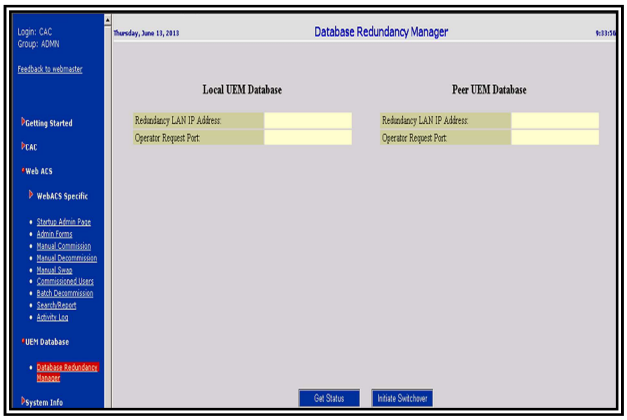

FIGURA 12: Base de datos de la UEM

Puerta de servicios Especiales (Special services Gateway SSGW): Actúa como una puerta de enlace IP de los módems satelitales antes de que estos estén comisionados, son una especie de corredores de ancho de banda para el enlace descendente.

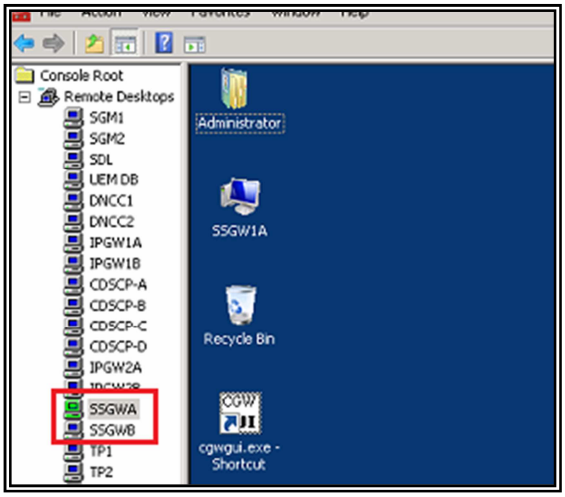

FIGURA 13: SSGW

TurboPage: La configuración consta de servidores TurboPage. Estos servidores son usados para mejorar el rendimiento del acceso a Internet, hacen la función de memoria cache. De tal forma que aceleran el trafico de la red en un 10%.

Son considerados servidores Cache para el uso del tráfico de Internet aseguran la entrega de aplicaciones web con la optimización y aceleración

del tráfico de Internet y datos. Los servidores además ayudan a la optimización de la red WAN y a la entrega de aplicaciones a las remotas, todo esto en una misma plataforma. (HUGHES)

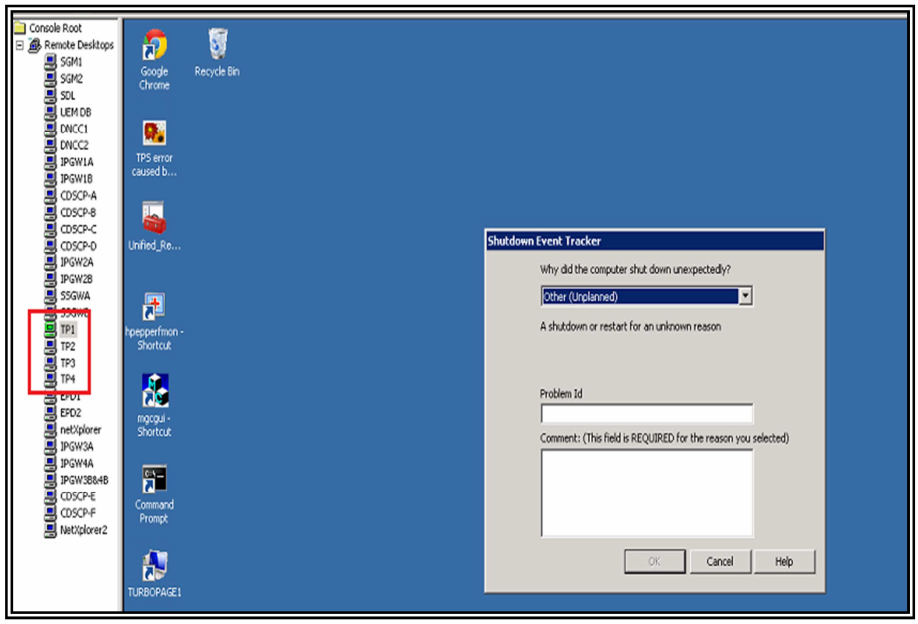

FIGURA 14: Turbo Page

Servidores EPD: (*Enterprise Package Delivery*). El servidor EPD permite al operador enviar archivos específicos a las remotas al mismo tiempo. El EPD es el servidor que se encarga de entregar todos los paquetes de datos necesarios que la remota requiere para sus diferentes aplicaciones.

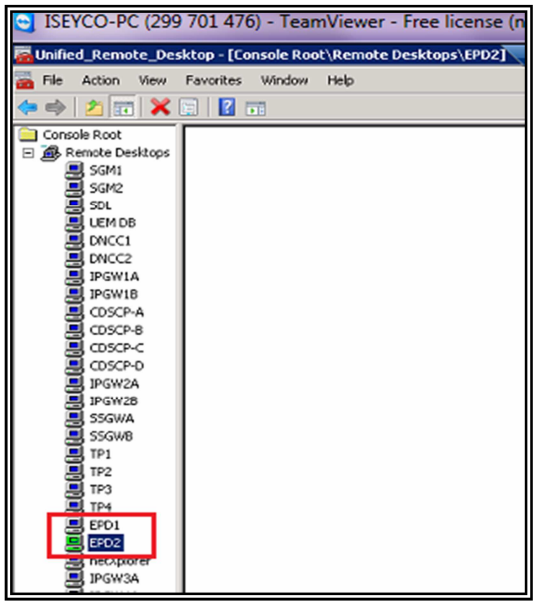

FIGURA 15: Servidor EPD

2.3. ANÁLISIS DEL EQUIPO ALLOT Y STAMPEDE

Para el análisis del tráfico en la red, es necesario conocer los equipos que van a ayudar a monitorear la misma, para lo cual se analizará el funcionamiento del equipo allot y stampede los cuales permiten observar el tráfico que pasa por la red, y a su vez controlarlo a través de compresores y aceleradores para tener un mejor rendimiento.

2.3.1. EQUIPO ALLOT NETENFORCER MODELO

Allot netenforcer es un dispositivo que permite recolectar estadísticas del tráfico que cursa por la red. Dichas estadísticas son tomadas para procesar datos en tiempo real o en un período establecido de tiempo, del flujo que cursa por la red.

La monitorización en tiempo real permite al usuario conocer exactamente lo que ocurre en la red, o a su vez observar el tráfico de la red en alguna fecha específica.

Este equipo monitorea todo el tráfico que pasa a través del independientemente del número de enlaces que este posea, en este caso el modelo 402 cuenta con un enlace de administración para controlar el tráfico.

FIGURA 16: Equipo ALLOT

2.3.1.1. CONFIGURACIÓN

De manera general existen cuatro formas de configurar este equipo:

- Menú de administración vía consola
- Menú de administración vía telnet
- Lcd
- Interfaz gráfica de usuario Net Explorer.

2.3.1.2. PARÁMETROS CONFIGURABLES

- Dirección ip del dispositivo
- Mascara de subred
- Nombre del dispositivo
- Nombre del domino
- Dirección ip default Gateway
- DNS
- Vlan
- Velocidad de las interfaces Ethernet

2.3.2. NETEXPLORER

Netexplorer es un sistema de administración central para Allot netenforcer. Permite la configuración de los equipos netenforcer y a su vez establecer las políticas del tráfico para el mismo.

Adicionalmente desempeña tareas de monitoreo en tiempo real para solucionar los problemas existentes en la red, y al mismo tiempo permite obtener un reporte periódico en un determinado tiempo para observar el uso y evolución de tráfico. (Allot comunications, 2011)

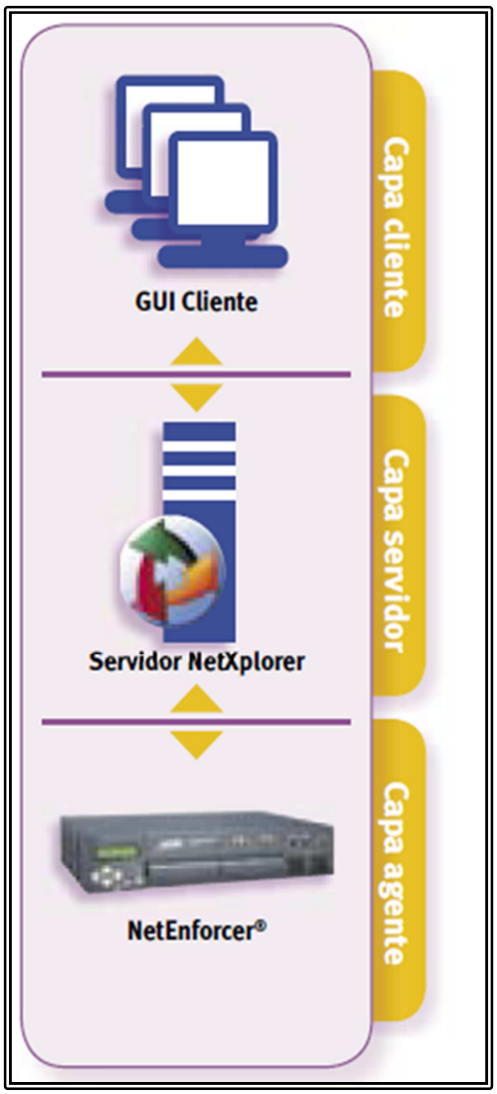

FIGURA 17: Arquitectura

2.3.2.1 Arquitectura

Netexplorer se basa en una arquitectura altamente escalable, su paquete de instalación es sencillo para servidores Windows XP y Windows 2003. La arquitectura está formada por tres capas

CAPA CLIENTE: Es la aplicación GUI Netexplorer, que comprende los clientes que se conectaran al servidor Netexplorer.

CAPA SERVIDOR: En esta capa se encuentra la base de datos y el servidor netexplorer, el cual permite al administrador comunicarse con los clientes que acceden al sistema, además se realizan las configuraciones del netenforcer y cada una de las políticas y alarmas para el monitoreo, para luego generar los reportes o informes respectivos.

CAPA DE AGENTE: En esta capa se encuentra el equipo netenforcer que va a ser administrado por el servidor.

2.3.2.1.1. Secciones de interface

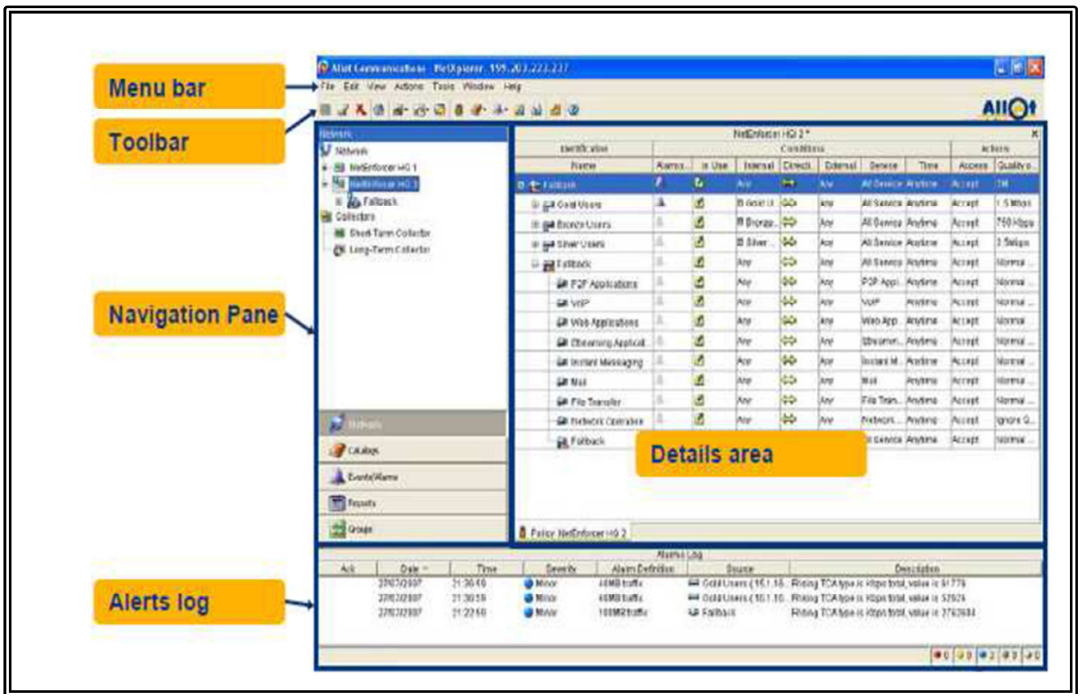

FIGURA 18: Secciones de interface de Netexplorer

La interface de usuario está compuesta por varias secciones:

BARRA DE MENU: Provee el acceso funcional a las aplicaciones.

BARRA DE HERRAMIENTAS: Son los botones de acceso directo a las funcionalidades.

PANEL DE NAVEGACIÓN: Contiene a la zona inferior, y es la que permite seleccionar las distintas aplicaciones, y la zona superior que es la que contiene listas tipo árbol de acuerdo a la aplicación seleccionada.

PANEL DE DETALLES DE APLICACIÓN: despliega datos con respecto a las aplicaciones y operaciones activas.

ALERTAS: Contiene la lista de alarmas configurados, estas son actualizadas cada 30s.

2.3.2.1.2. Monitoreo y reportes

Netexplorer puede llevar a cabo el monitoreo en tiempo real y en un período de tiempo, y analiza cada tipo de gráfico y características especiales de cada uno de ellos.

Existen varios tipos de gráficos:

ESTADÍSTICOS: Muestra e l ancho de banda consumido por un periodo de tiempo.

DE UTILIZACIÓN: Despliega el ancho de banda consumido de un terminal en base a un porcentaje.

DE OBJETO: Por cada objeto listado presentan dos tipos de reportes

Objetos más activos: Se definen como los objetos activos al ancho de banda consumido, número de conexiones, número de paquetes entrantes.

Distribución de objetos: distribución de los objetos seleccionados en un periodo de tiempo.

PROMEDIO DE PROTOCOLOS: Despliega reporte de estadísticas de los protocolos utilizados durante un período de tiempo.

2.3.3. STAMPEDE

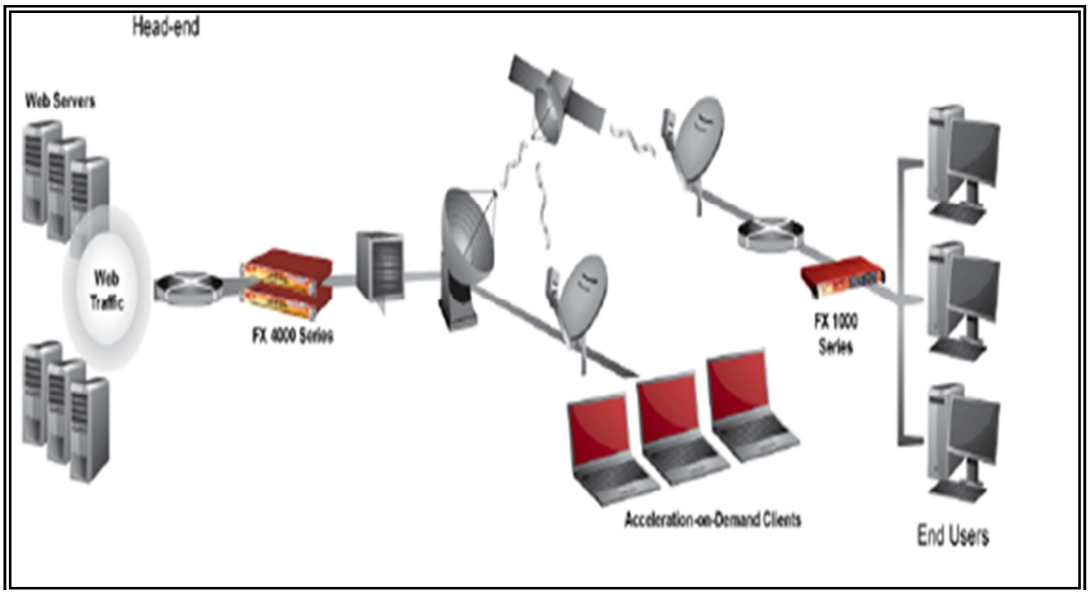

FIGURA 19: Equipo Stampede

Stampede es un equipo que se coloca en el HUB para comprimir el tráfico de salida a sus clientes, en este caso a cada uno de los terminales VSATS. Esta optimización es equivalente a la reducción dinámica del tráfico de la red en un 25% o más, adicionalmente el administrador puede realizar la compresión y aceleración en cada sitio remoto, mediante el almacenamiento caché y así eliminar la congestión de la misma. (COMTECH, 2012)

CAPÍTULO III: ANÁLISIS DEL TRÁFICO EN LA RED

3.1. DESCRIPCIÓN DE LA HERRAMIENTA PRTG

PRTG Network Monitor es un software utilizado para el monitoreo de redes empresariales, utiliza el protocolo SNMP, sniffing de paquetes WMI, IP SLA Y NETFLOW, para obtener de esta manera los datos necesarios para estadísticas y sensores. Existen versiones de uso comercial sin límites, y la versión libre la cual brinda la posibilidad de añadir hasta diez sensores como máximo.

Esta herramienta de monitoreo permite mantener al usuario formado de cualquier alarma a través de informes vía correo electrónico, además permite encontrar cuellos de botella, y evitar la caída de la red.

3.1.1. ARQUITECTURA DE PRTG

Es importante conocer como está estructurado el prtg para poder hacer uso correcto de la misma, y poder cambiar las configuraciones de monitorización.

PRTG está conformado por un árbol de aparatos distribuido de la siguiente manera: (PRTG, 2012)

FIGURA 20: Árbol de elementos de PRTG

3.1.1.1. GRUPO ROOT

Es la instancia sobre ordinada de la herramienta prtg, y contiene todos los objetos de configuración de la misma, normalmente todos los objetos heredan la configuración de este grupo, es por eso que es necesaria la correcta configuración.

3.1.1.2. SONDA

Todos los grupos a excepción del grupo root pertenecen a una sonda, la cual es la encargada de monitorear cada uno de dichos grupos. Prtg automáticamente crea una sonda local, si se requieren más sondas, se deberá hacer manualmente

3.1.1.3. GRUPOS

Cada sonda contiene varios grupos, los cuales tienen funciones estructurales, aquí se organizan objetos similares para facilitar la herencia de configuración de los mismos. Se puede organizar los aparatos en varios grupos para reflejar la estructura de la red, se puede observar a continuación la estructura de un árbol de aparatos con una sonda local, grupos, aparatos y sus sensores.

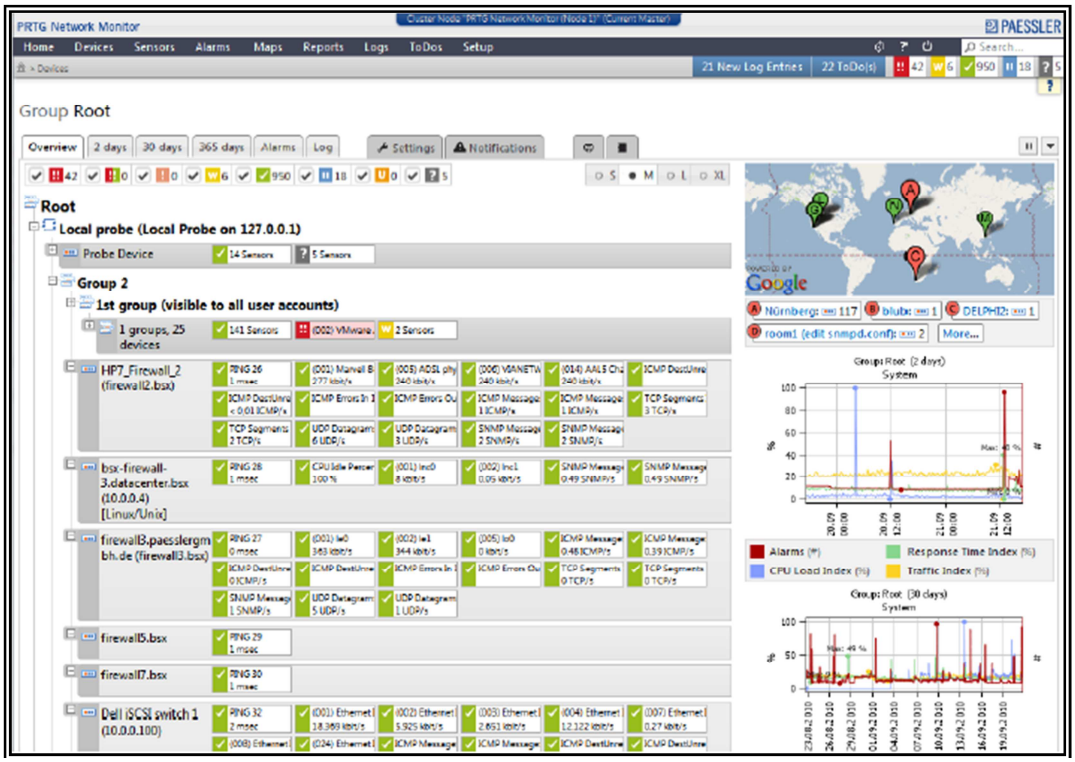

FIGURA 21: Grupos en PRTG

3.1.1.4. EQUIPOS

El aparato se añade para monitorear cada grupo o sonda. Cada aparato en su grupo representa un equipo real en la red como ejemplo: servidores web, ordenadores, enrutadores o switches, o cualquier aparato que tenga una ip individual.

3.1.1.5. SENSORES

Cada aparato puede contener un número de sensores, los cuales monitorizan un aspecto del equipo por ejemplo:

- Un servicio de red, FTP, SMTP, HTTP, ect.
- El tráfico que fluye por un puerto del switch.
- La carga de procesador de un aparato.
- El tráfico que fluye por la tarjeta de red.

3.1.1.6. CANAL

Cada sensor está compuesto por un número de canales a través de los cuales procesa y visualiza los tramos de datos, estos canales dependen de cada tipo de sensor, entre los principales canales se tiene:

- Tiempo de falla de un aparato de ancho de banda.
- Tráfico in de un aparato de ancho de banda.
- Trafico out de un aparato de ancho de banda.
- Trafico suma de un aparato de ancho de banda.
- Trafico de correo de un aparato de ancho de banda.

3.2. IMPLANTACIÓN DE LA HERRAMIENTA PRTG

3.2.1. DESCARGA E INSTALACIÓN DE LA HERRAMIENTA

Como primer paso se ingresa a la página oficial del gestor de red www.paessler.com/prtg/download y se selecciona la versión que vamos a instalar, en este caso se procede a escoger la versión comercial la cual tiene la opción de instalar indeterminado número de sondas para el monitoreo de la red. (PAESSLER, 2013)

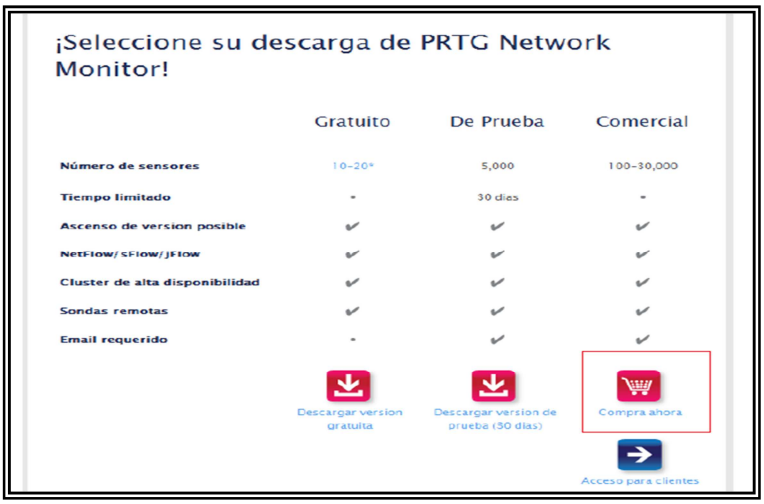

FIGURA 22: Descarga de la herramienta PRTG

Una vez descargado el archivo, se descomprime y se procede a la instalación:

- Se selecciona el idioma de instalación:

FIGURA 23 Selección del idioma

- Aparecerá la siguiente pantalla. Simplemente se selecciona la opción siguiente:

FIGURA 24: Instalación de la herramienta PRTG

- A continuación se mostrará los términos de licencia, en los cuales se debe poner aceptar luego de haberlos leído.

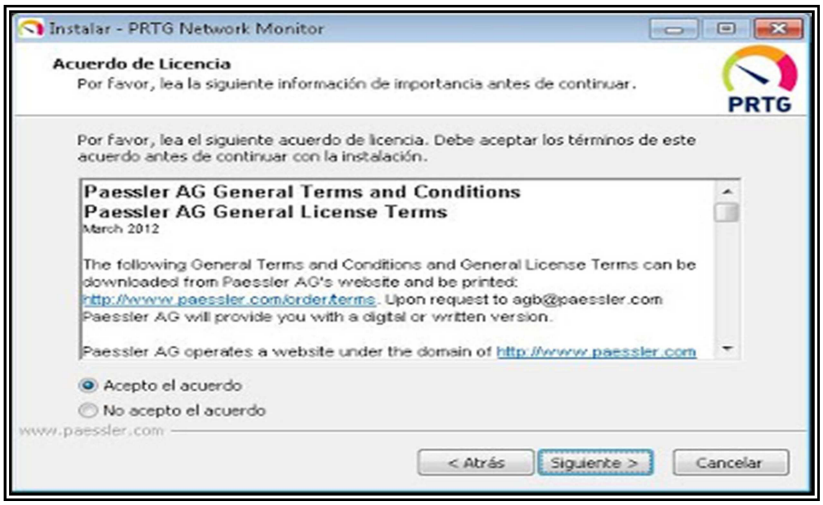

FIGURA 25: Acuerdo de licencia

- El siguiente requerimiento es ingresar la dirección de correo a la cual llegarán las notificaciones de alarmas de monitoreo de la red.

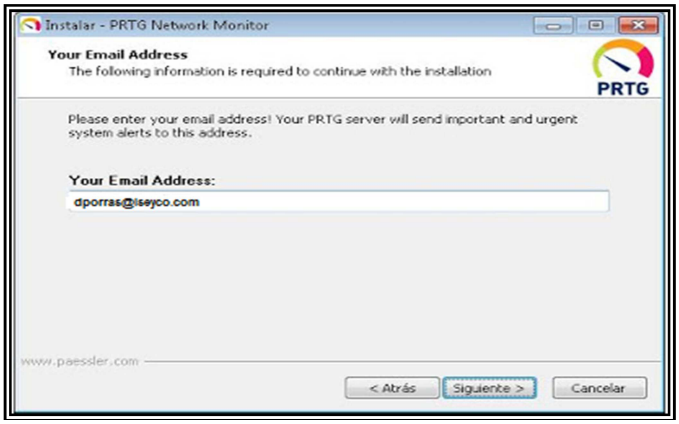

FIGURA 26: Configuración de correo

- Ahora se introducen las claves proporcionadas al momento de la compra de la herramienta

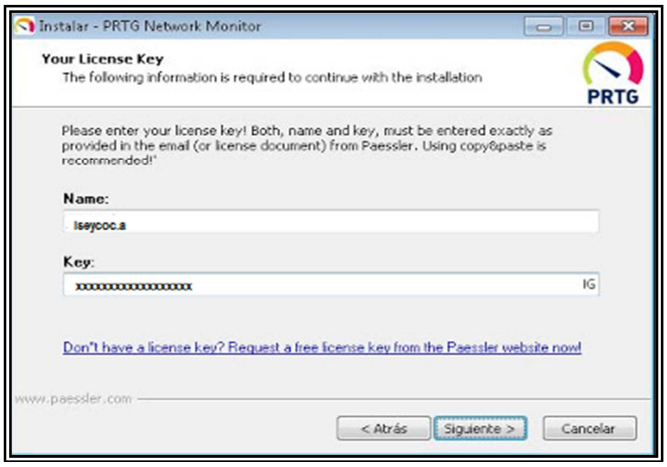

FIGURA 27: Activación de licencias

- Se selecciona la carpeta de instalación:

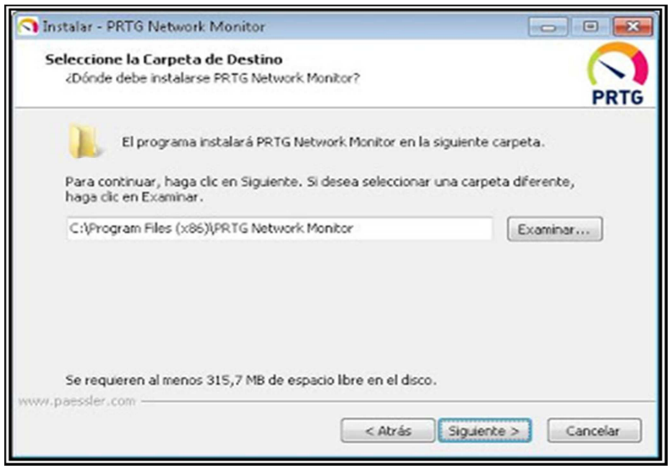

FIGURA 28: Carpeta de instalación

- Y finalmente aparecerá un acceso directo en el escritorio:

FIGURA 29: Ícono de acceso

3.2.2. IMPLANTACIÓN DEL ÁRBOL PRTG PARA EL MONITOREO DE LA RED VSAT CNT EP.

3.2.2.1. IMPLANTACIÓN DE GRUPOS

- Primero se selecciona la opción añadir grupo:

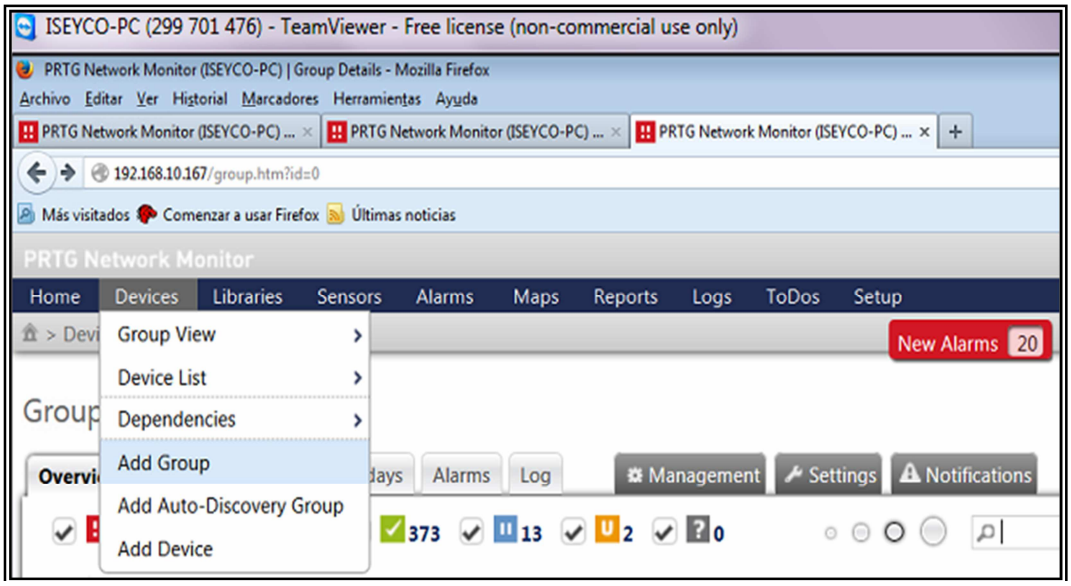

FIGURA 30: Añadir grupo

- La sonda que va a contener todos los grupos se llama en este caso CNT VSAT, entonces se selecciona dicha sonda y se procede a crear el grupo.

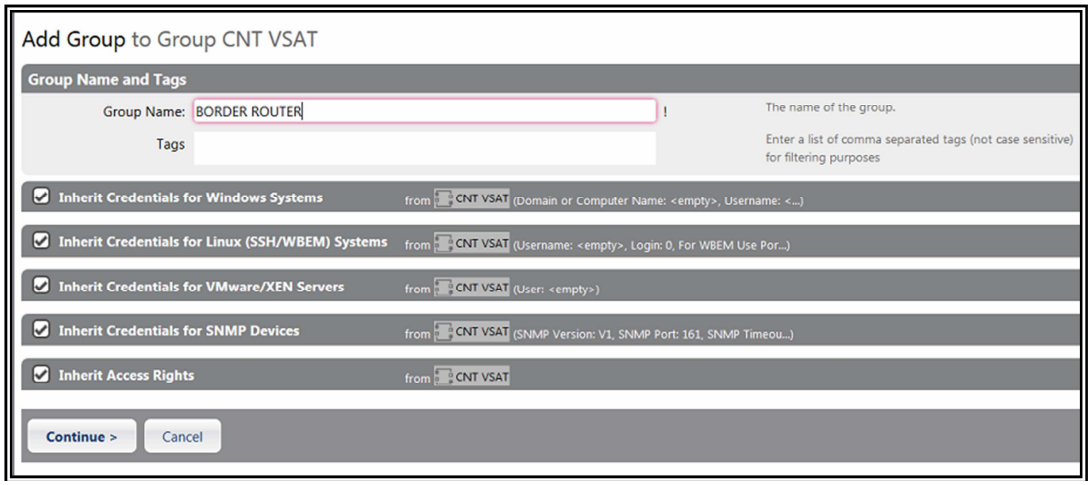

FIGURA 31: Selección de Sonda

- Se selecciona continuar y está creado el grupo, cada sonta puede contener varios grupos, en este caso se crearon varios como se muestra a continuación:

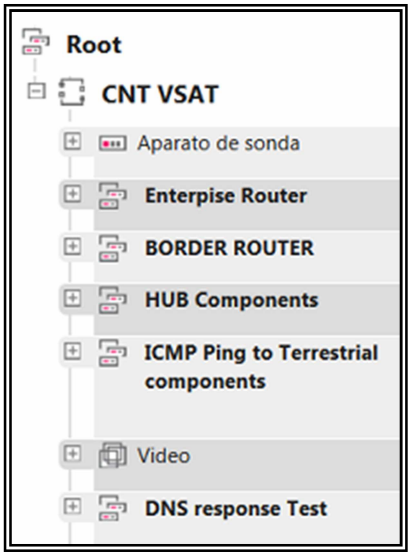

FIGURA 32: Grupos creados

3.2.2.2. CREACIÓN DE EQUIPOS

Dentro de cada grupo se crean equipos, se crea en este caso dentro del grupo ¨HUB COMPONENTS¨, donde se encontrarán los equipos más importantes que nos permitirán el monitoreo de la red.

- Primero se selecciona agregar equipo.

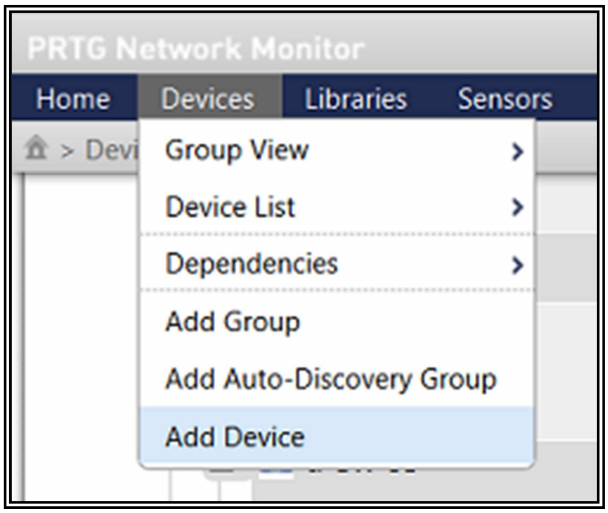

FIGURA 33: Añadir aparato

- Se selecciona el grupo dentro del cual se crea el equipo.

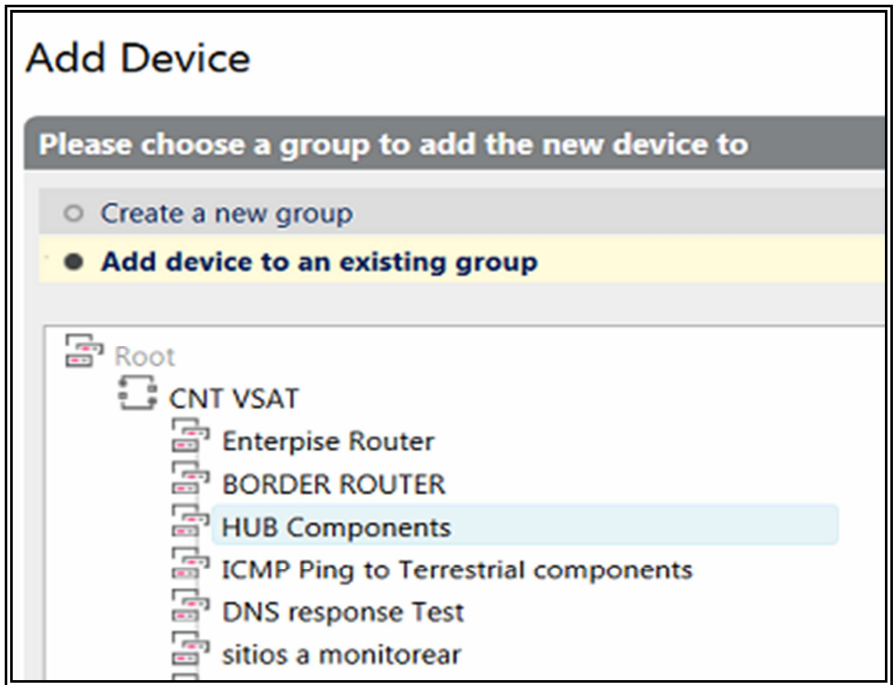

FIGURA 34: Selección del grupo

- Se pone el nombre el aparato y la dirección ip que pertenece al equipo.

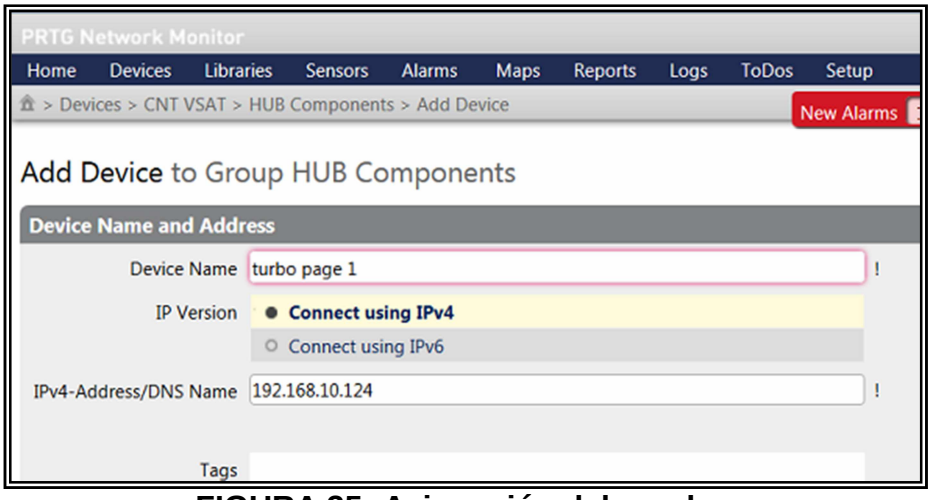

FIGURA 35: Asignación del nombre

- Los equipos que conforman el HUB de la red VSAT CNT EP son:

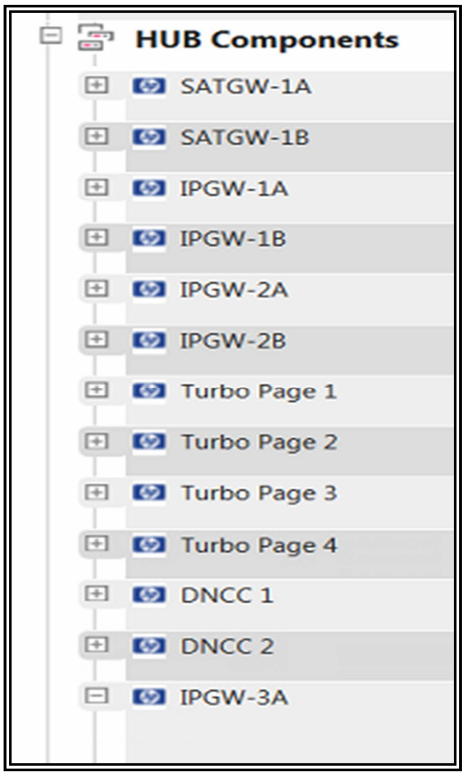

FIGURA 36: Aparatos creados en el HUB

3.2.2.3. IMPLANTACIÓN DE SENSORES

Dentro de cada aparato se puede agregar los sensores, que se representan lo que se desea monitorear, pueden ser uno o varios

- Primero se selecciona la opción añadir sensor en este caso dentro del aparato turbo page.

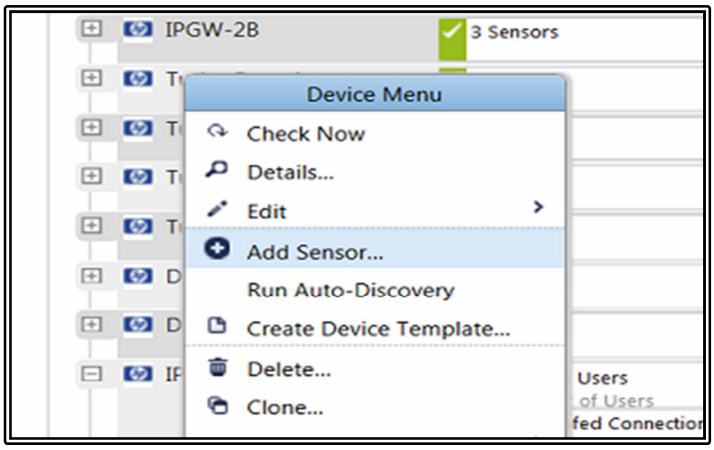

FIGURA 37: Añadir sensor

- En este caso se va a monitorear los clientes que están haciendo consumo de trafico vamos a utilizar el protocolo snmp y seleccionamos el siguiente sensor:

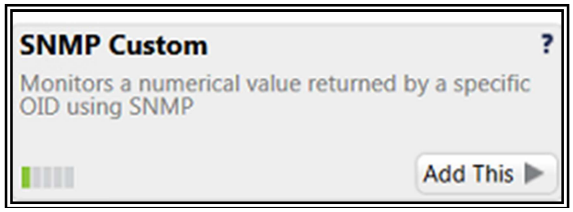

FIGURA 38: Selección del sensor

- Se pone el nombre del sensor

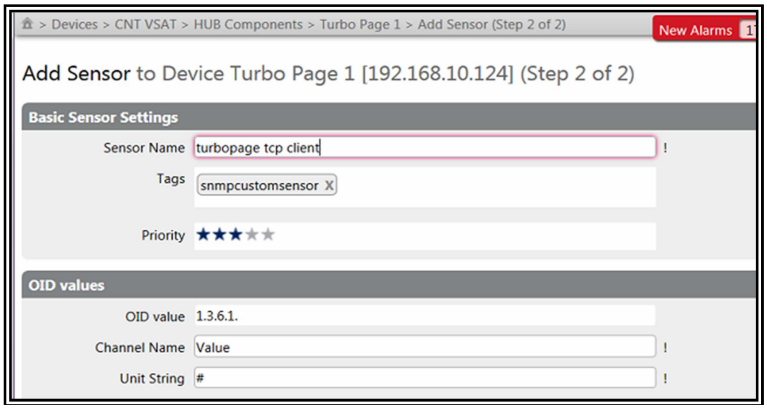

FIGURA 39: Asignación de nombre del sensor

- Dentro de cada equipo se pueden agregar varios sensores por ejemplo dentro del turbopage se tiene 5 sensores.

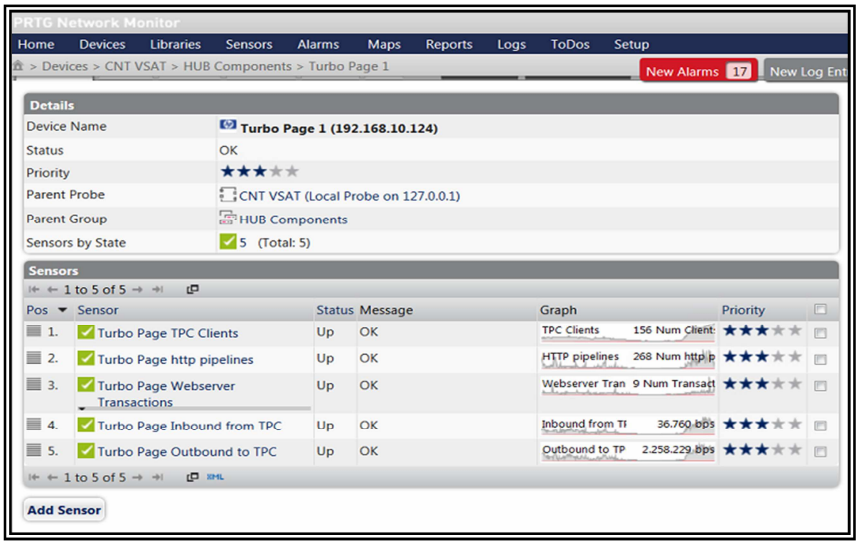

FIGURA 40: Sensores creados dentro del aparato turbopage

3.2.2.4. ÁRBOL CREADO PARA EL MONITOREO

El árbol de la red VSAT CNT creado en la herramienta prtg queda de la manera siguiente:

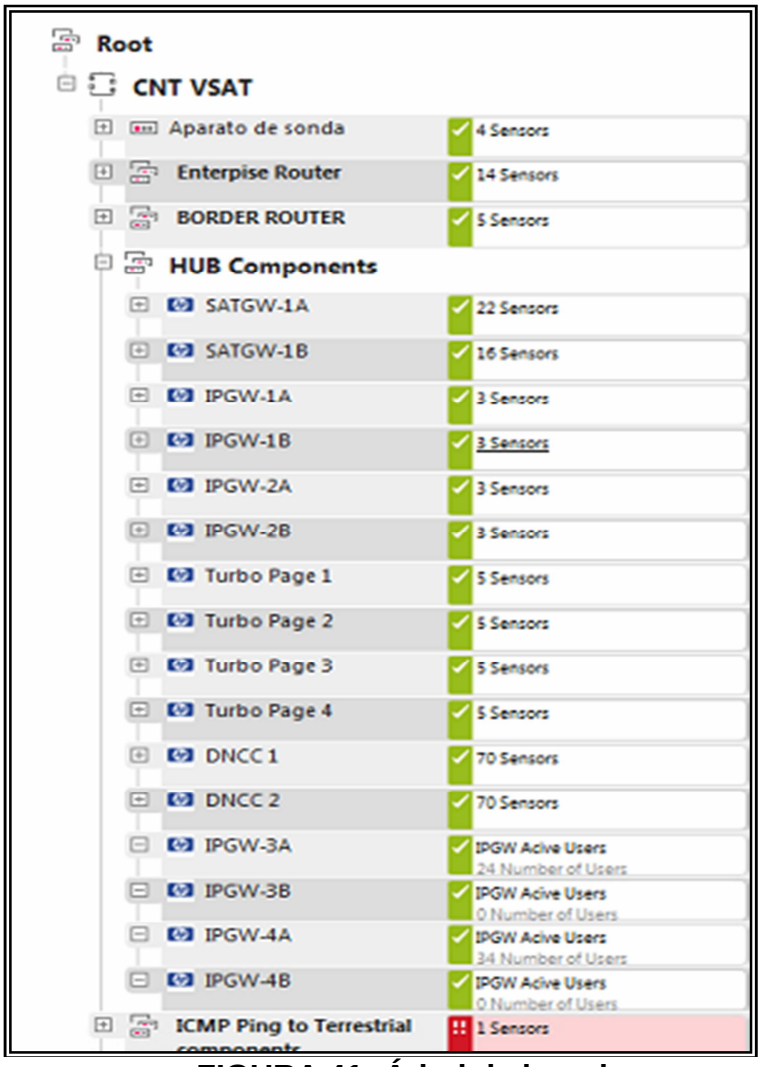

FIGURA 41: Árbol de la red

3.3. ANÁLISIS DEL TRÁFICO EN LAS HORAS PICO

Debido a los cambios de listados realizados por CNT y al aumento de terminales requeridos, la cantidad de sitios contractuales y la asignación de perfiles que se cambiaron ocasionaron mayor necesidad de ancho de banda satelital.

La demanda 12% en el outbound y 7% en Inbound asumida por CNT en el proyecto resultó ser muy baja, lo que ocasiona actualmente saturación en la red satelital y la necesidad de buscar las posibles para evitar saturación y mal funcionamiento de la red diseñada para una demanda del 12% en el outbound.

El contrato prevé la instalación de 1500 sitios de acuerdo al siguiente plan de velocidad

TABLA 3: Tabla de velocidades y sitios propuestos inicialmente

Plan de Velocidad	Número de sitios
1024 x 256	5
512 x 128	310
256 x 128	406
128 x 64	779
TOTAL:	1.500

Debido a la adición de sitios extras instalados, de acuerdo con a la solicitud de CNT de la inclusión de nuevos sitios la situación actual de acuerdo al plan de velocidad es el siguiente:

TABLA 4: Tabla de velocidades y sitios propuestos actualmente

Plan de Velocidad	Número de sitios actuales
1024 x 256	29
512x128	267
256 x 128	940
128 x 64	365
TOTAL:	**1601***

Debido a la modificación del número de remotos con distintos perfiles la capacidad requerida por la red incrementó, además se observó que la

simultaneidad de usuarios no fue la considerada en el proceso contractual del 12% para outbound. Considerando una simultaneidad para el outbound del 25% y con la nueva distribución de usuarios se obtienen las siguientes tablas de tráfico para el contrato como para la situación actual:

TABLA 5: Tráfico considerado en sizing contractual

Velocidad		Simultaneidad		Velocidad considerando la simultaneidad		PREVISTO EN EL CONTRATO		
Download (Kbps)	Upload (Kbps)	Simult Download %	Simult Upload %	Datos Usuario D/L (Kbps)	Datos Usuario U/L (Kbps)	Cantidad de sitios	Outbound hub -> rem	Inbound rem -> hub
1024	256	12,00%	7,00%	122,88	17,92	5	614	90
512	128	12,00%	7,00%	61,44	8,96	310	19.046	2.778
256	128	12,00%	7,00%	30,72	8,96	406	12.472	3.638
128	64	12,00%	7,00%	15,36	4,48	779	11.965	3.490
Total Sites						1.500		
Total END USER Traffic – kbps							44.099	9.995

TABLA 6: **Tabla de velocidades y sitios propuestos actualmente**

Velocidad		Simultaneidad		Velocidad considerando la simultaneidad		SITUACION ACTUAL		
Download (Kbps)	Upload (Kbps)	Simult Download %	Simult Upload %	Datos Usuario D/L (Kbps)	Datos Usuario U/L (Kbps)	Cantidad de Sitios	Outbound hub -> rem	Inbound rem -> hub
1024	256	25,00%	7,00%	256	17,92	29	7424	520
512	128	25,00%	7,00%	128	8,96	269	34432	2410
256	128	25,00%	7,00%	64	8,96	940	60160	8422
128	64	25,00%	7,00%	32	4,48	365	11680	1635
Total Sites						1.603		
Total END USER Traffic – kbps							113.696	12.988

Se observa que para el outbound el valor considerado previsto inicialmente es de 44,099 Mbps y en la configuración actual de la red llega a 113,696 Mbps que corresponde a un incremento de 2,57 veces más que el tráfico considerado, mientras que para el inbound la diferencia es de 9,995 Mbps a 12,988 Mbps que corresponde a un incremento de 1,3 veces más

La demanda de tráfico de internet se observa en la siguiente gráfica que corresponde a la interconexión con la red MPLS de CNT, esta demanda está afectada por la restricción de tráfico del equipo Allot.

FIGURA 42: Tráfico hacia y desde la red MPLS

TABLA 7: Canal Satelital requerido considerando una compresión del 35%

Internet Traffic:	Download (Kbps)	Upload (Kbps)	Online Simult Download %	Online Simult Upload %	raw user D/L data (Kbps)	raw user U/L data (Kbps)	QTY Site	Outbound hub -> rem	Inbound rem -> hub
Service Plans	1024	256	25,00%	7,00%	256,00	17,92	29	7.424	520
	512	128	25,00%	7,00%	128,00	8,96	269	34.432	2.410
	256	128	25,00%	7,00%	64,00	8,96	940	60.160	8.422
	128	64	25,00%	7,00%	32,00	4,48	365	11.680	1.635
Total Sites							1.603		
Total END USER Traffic - kbps								113.696	12.988
Outbound & Inbound Standard Compression :								35%	30%
Outbound/ Inbound capacity after Standard Compression – kbps								73.902	9.091
Outbound channel OH (Timing and Supervisory Traffic) / Inbound channel OH (Aloha traffic) – kbps								200	455
Outbound & Inbound Efficiency:								94%	89%
Outbound/ Inbound capacity after efficiency – kbps								78.832	10.726

El incremento de usuarios no considerado en el diseño (sizing contractual) y el incremento del uso como indica el cálculo de simultaneidad de usuarios está ocasionando que la red utilice en exceso la capacidad total (deficitaria con relación a lo requerido por el sizing contractual) entregada en el satélite 40 Mbps y observando que el canal satelital está permanentemente saturado.

3.3.1. DESCRIPCIÓN DEL TURBOPAGE

El turbopage en un acelerador de internet, nos permite acelerar o aumentar la velocidad de entrega del contenido web de la red, aumentando el rendimiento de la misma en un 80% o más.

3.3.2. CÓMO FUNCIONA TURBOPAGE

TurboPage actúa reduciendo las solicitudes o involucrados en ir a buscar los objetos que forman parte de una página Web. Los TurboPage cliente intercepta las solicitudes web en el router y se comunica con un servidor TurboPage en el centro de datos remoto.

El proceso normal implicaría la espera de un PC remoto para analizar la página HTML inicial, el envío de una petición DNS (servidor de nombres de dominio) para cada servidor que tiene un objeto tal como un archivo de imagen o flash y , a continuación, la apertura de otra conexión TCP a cada uno de los otros servidores para solicitar los objetos. En su lugar, el servidor TurboPage busca con anticipación o recopila los artículos y temporalmente los almacena en una memoria caché, asegurando el contenido más actualizado desde el servidor Web , que ofrece un rendimiento extraordinariamente rápido . (HUGHES, 2011)

3.3.2.1. PASOS QUE REALIZA EL TURBOPAGE

1. El PC remoto navegador Web solicita una página Web, lo que genera una petición HTTP desde el navegador Web en el servidor Web, como se muestra en la Figura.

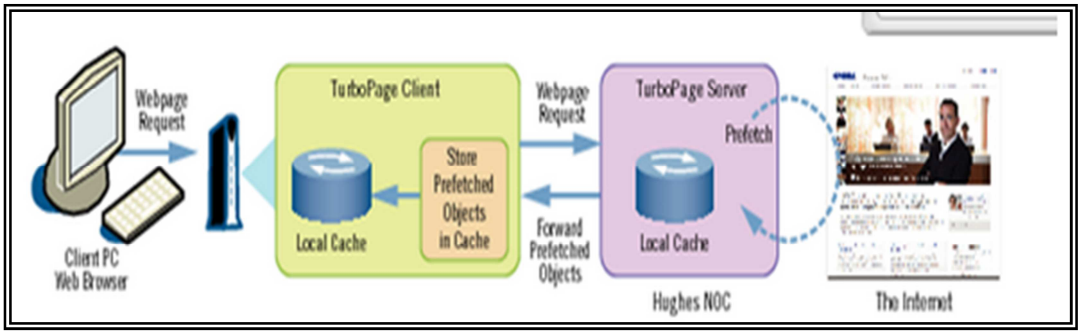

FIGURA 43: Diagrama del proceso que realiza turbopage

2. Esta solicitud es interceptado por el cliente TurboPage y reenvía al servidor TurboPage. El servidor tiene una conexión con el servidor Web y envía la solicitud.
3. Cuando el servidor Web devuelve una respuesta con el código HTML inicial de la página Web, el servidor TurboPage reenvía la respuesta de vuelta al cliente TurboPage, que a su vez la envía al navegador Web de

PC. Al mismo tiempo, el servidor TurboPage analiza el HTML y perfecciona cualquier objeto que se ha identificado, generando al mismo tiempo una lista de objetos, que se envía al cliente TurboPage.

4. Mientras esto sucede, y mientras el servidor TurboPage está a la espera de los objetos que se entregarán, el navegador Web PC remoto analiza el HTML y comienza solicitando estos objetos, así como el inicio de peticiones DNS si varios servidores son referenciados por el código HTML.
5. Las intercepciones cliente TurboPage estas solicitudes y los compara con la lista del servidor TurboPage. Si hay una coincidencia, el cliente TurboPage espera a que el objeto que se entrega desde el servidor TurboPage que ha sido el reenvío de los objetos a medida que llegan. Si el objeto ya ha sido entregado, el cliente envía el objeto sobre la LAN local al navegador Web PC.
6. Si el objeto no está en la lista, reenvía la solicitud al servidor Web de destino y espera la respuesta.
7. El cliente TurboPage responde a las peticiones de la PC remota DNS inmediatamente con la información almacenada en caché y luego se anticipa al TCP de tres vías cuando el PC remoto intenta ponerse en contacto con cada uno de los servidores web. Emite un mensaje solicitando los objetos pre buscados del servidor TurboPage y entrega éstos a la PC remota.
8. En última instancia, el navegador Web PC representa la página después de haber recibido la mayor parte de los objetos del cliente TurboPage

localmente a través de LAN rápido en lugar de esperar a que todos los objetos que vienen a través de la WAN más lento.

TurboPage reduce el número de transacciones interactivas a través de la WAN. Debido a que el proceso de la obtención previa recoge localmente objetos para la entrega a velocidad de LAN para el PC remoto, TurboPage antepone a la latencia WAN normal de interés en cada objeto en serie. Por otra parte, TurboPage acelera las páginas web tanto seguras y no seguras. (HUGHES, 2010)

3.3.2.2. ANÁLISIS DE NÚMERO DE USUARIOS.

Turbopage se encuentra en el gestor de monitoreo PRTG, este equipo contiene un sensor el cual nos permite adicionalmente observar el número de usuarios que se encuentran haciendo uso de la web en este caso.

3.3.2.3. DETERMINACIÓN DE HORAS PICO

- **Turbopage 1**

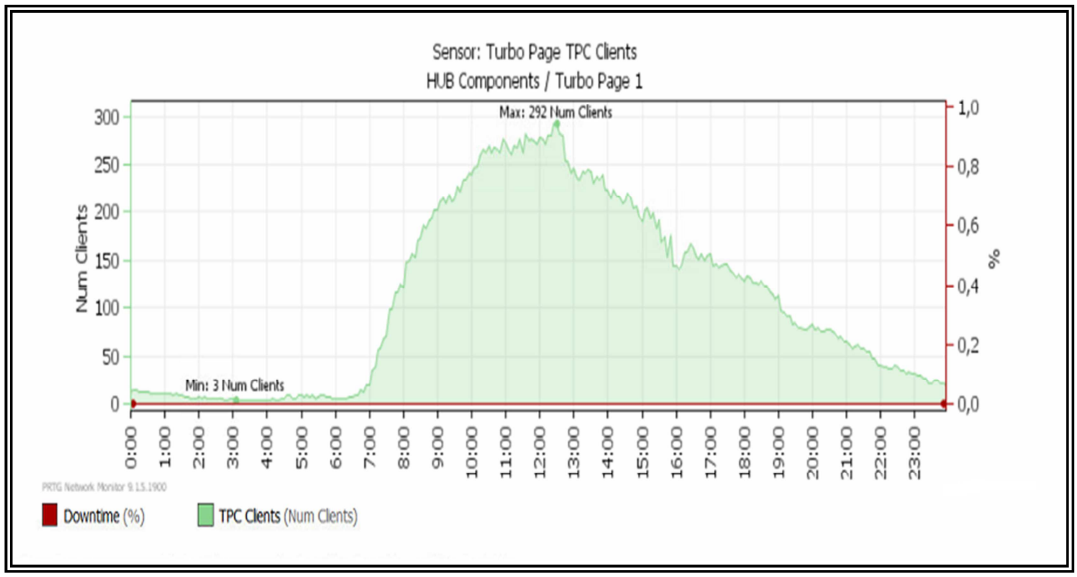

FIGURA 44: Tráfico en el turbopage1

Se puede observar que el tráfico se incrementa entre las 9:00 y las 18:00 horas

- **Turbopage 2**

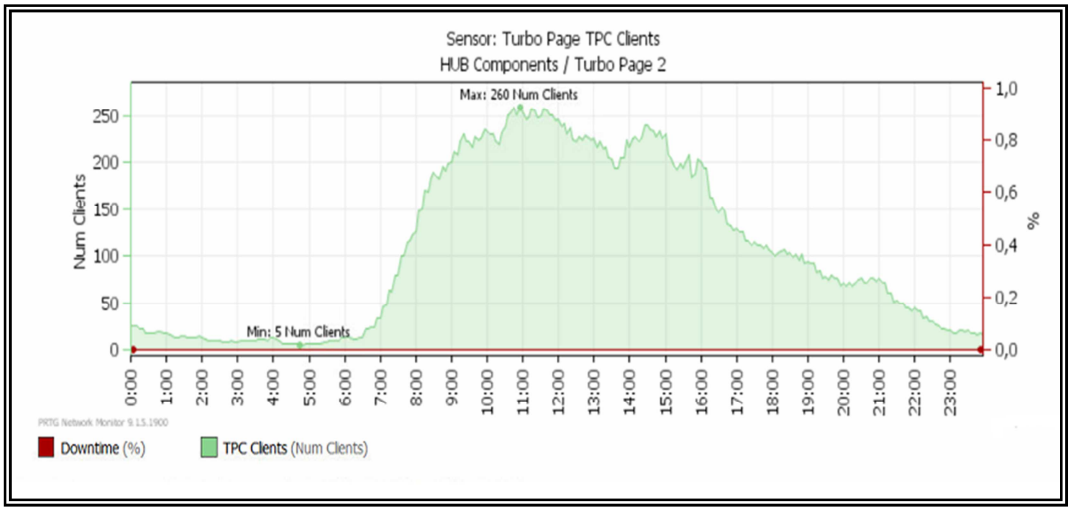

FIGURA 45: Tráfico en el turpopage 2

Se ha considerado los horarios en que la red se encuentra en saturación y cuando la red no se encuentra en saturación, adicionalmente se realizan estas pruebas en las horas pico las cuales según los horarios en que la red se encuentra en saturación se encuentra entre las 9:00 y las 18:00.

3.3.2.3.1. Pruebas Con Red Saturada

Se realizó las pruebas entre las 14H00 y 16H30 del día 15 de Julio de 2013, en este horario la red de encontraba saturada, verificándose esto en las pérdidas de paquetes obtenidos en el siguiente gráfico:

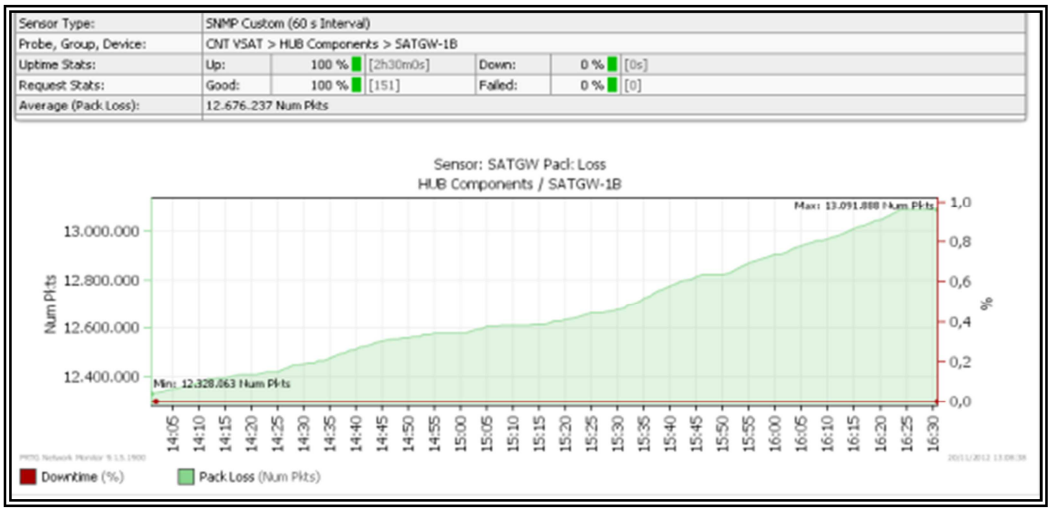

FIGURA 46: Pérdida de paquetes

3.3.2.3.2. Número de usuarios en horas pico

- **Turbopage 1**

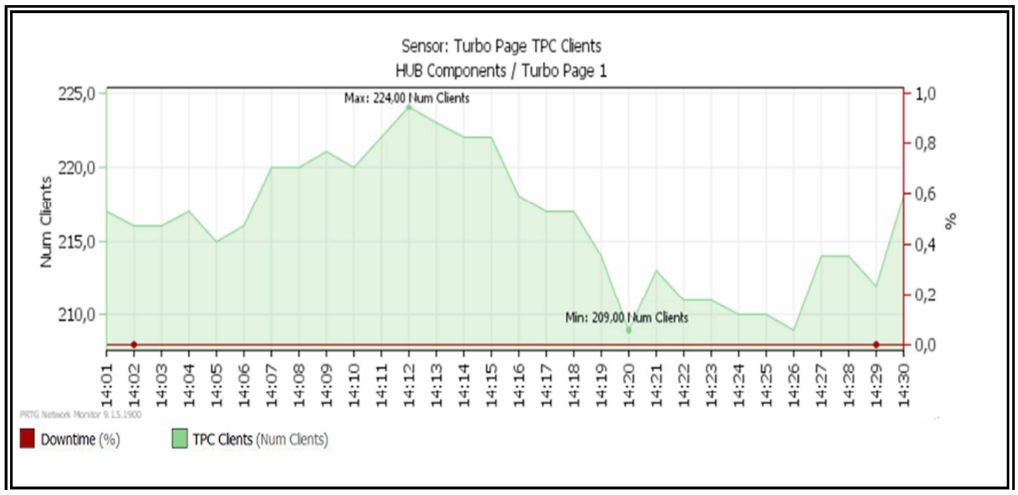

FIGURA 47: Usuarios 14:00:14:30

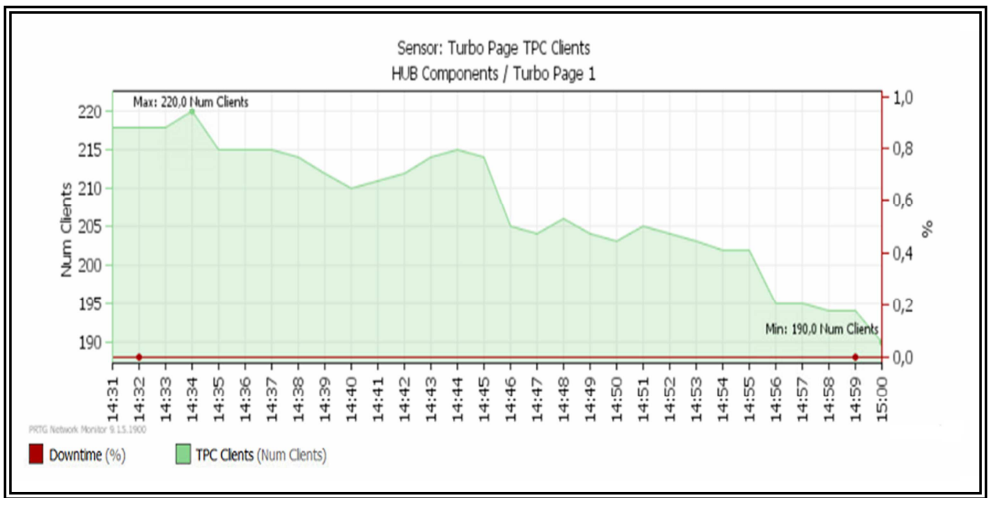

FIGURA 48: Usuarios 14:30:15:00

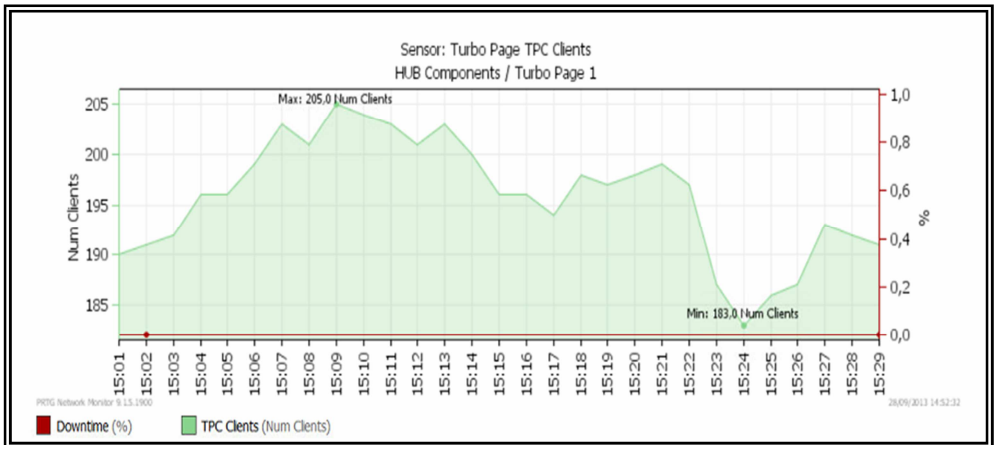

FIGURA 49: Usuarios 15:00-15:30

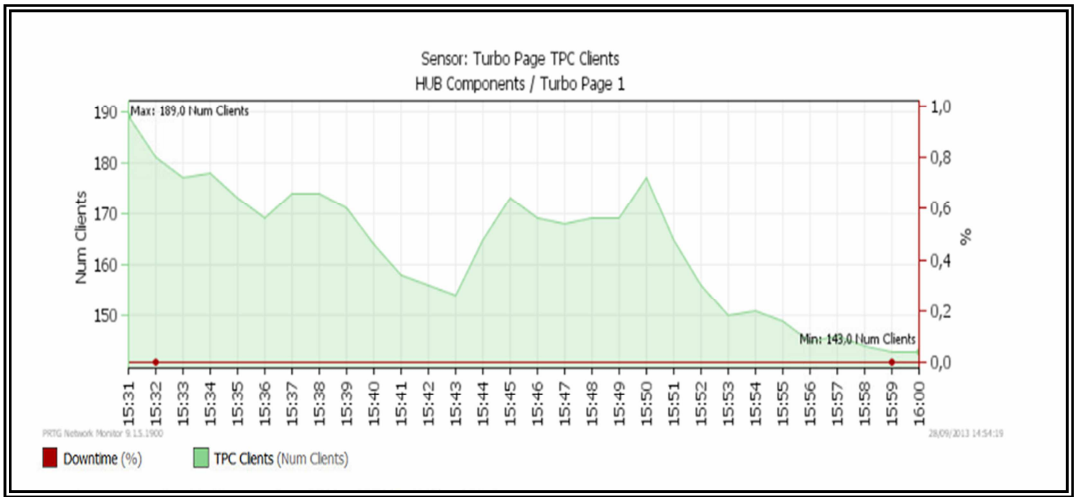

FIGURA 50: Usuarios 15:30-16:00

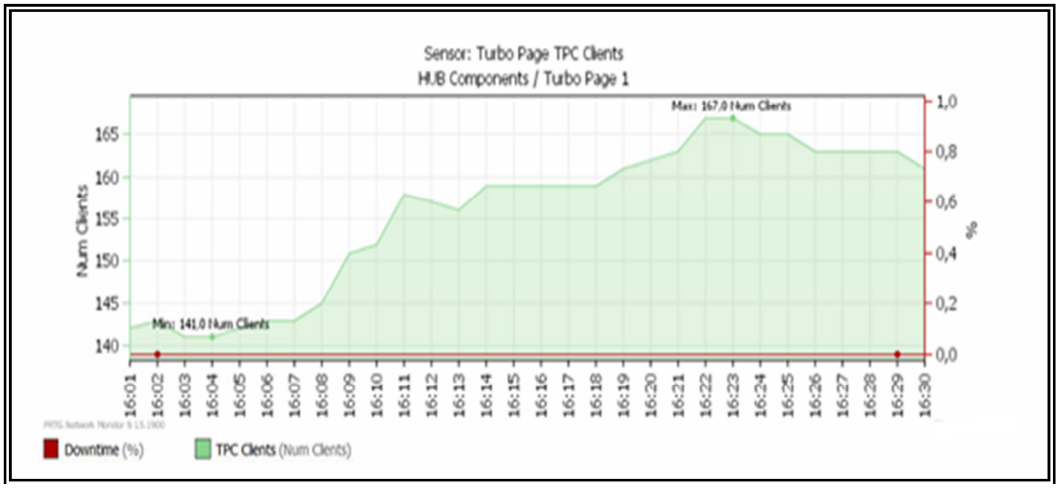

FIGURA 51: Usuarios 16:00-16:30

- **Turbopage 2**

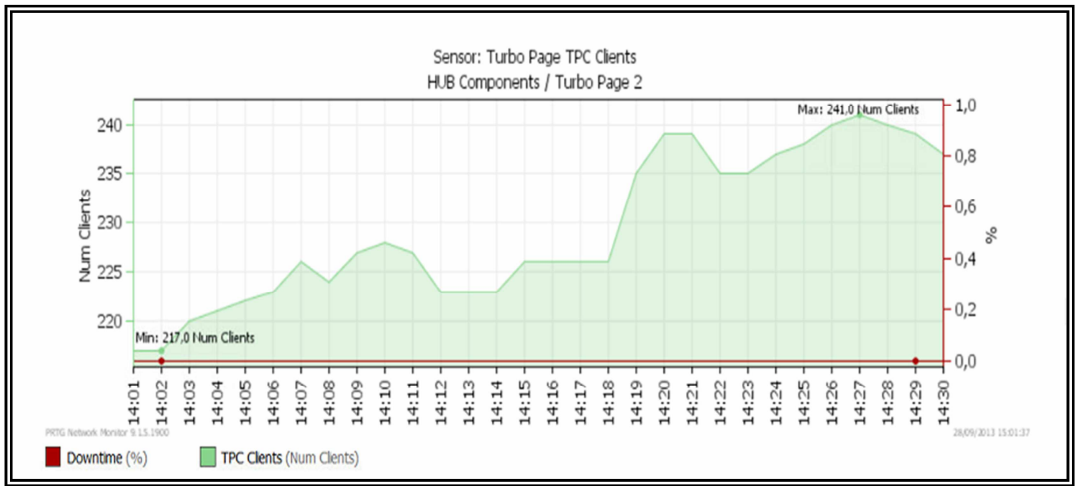

FIGURA 52: Usuarios 14:00-14:30

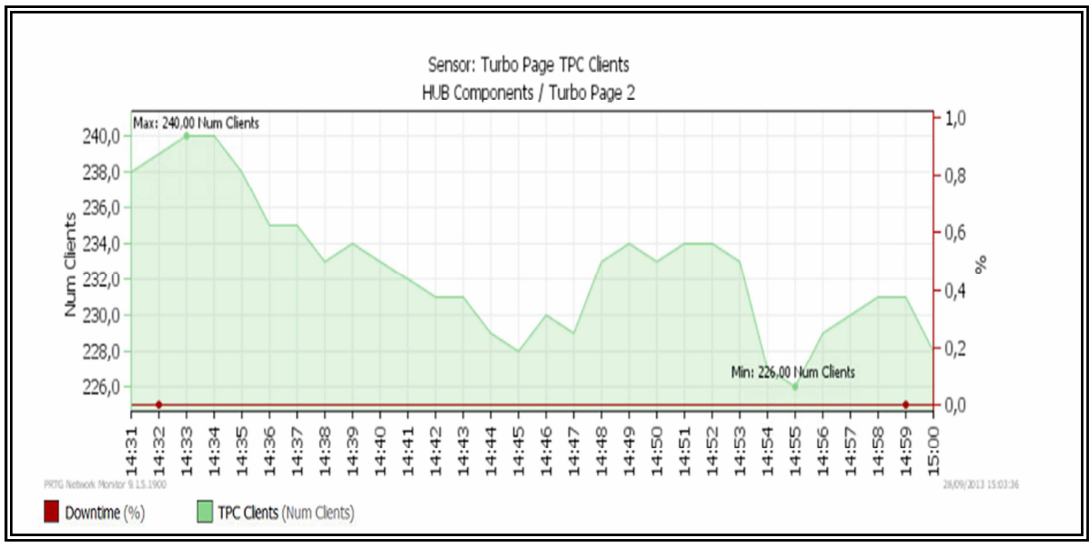

FIGURA 53: Usuarios 14:30-15:00

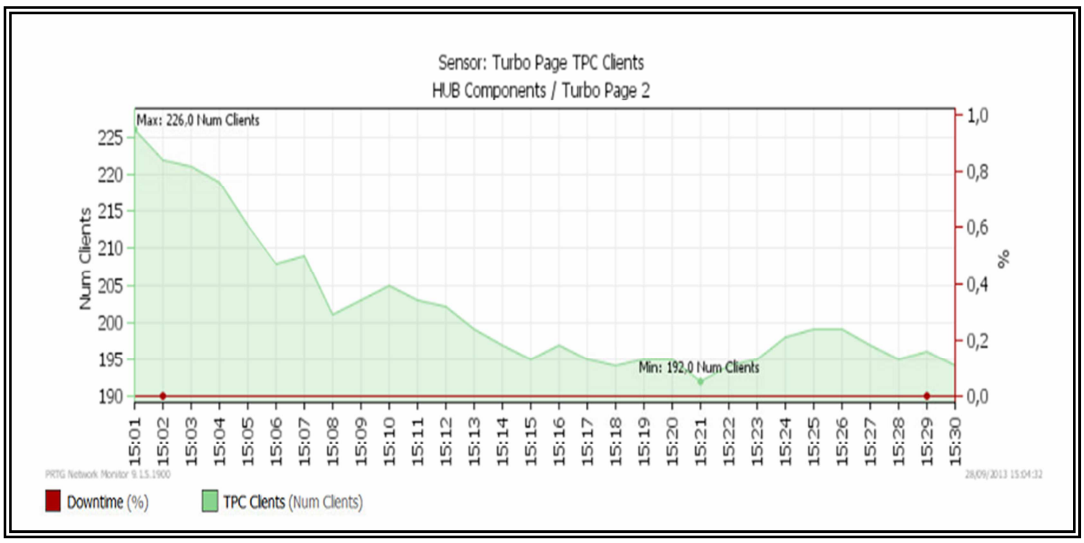

FIGURA 54: Usuarios 15:00-15:30

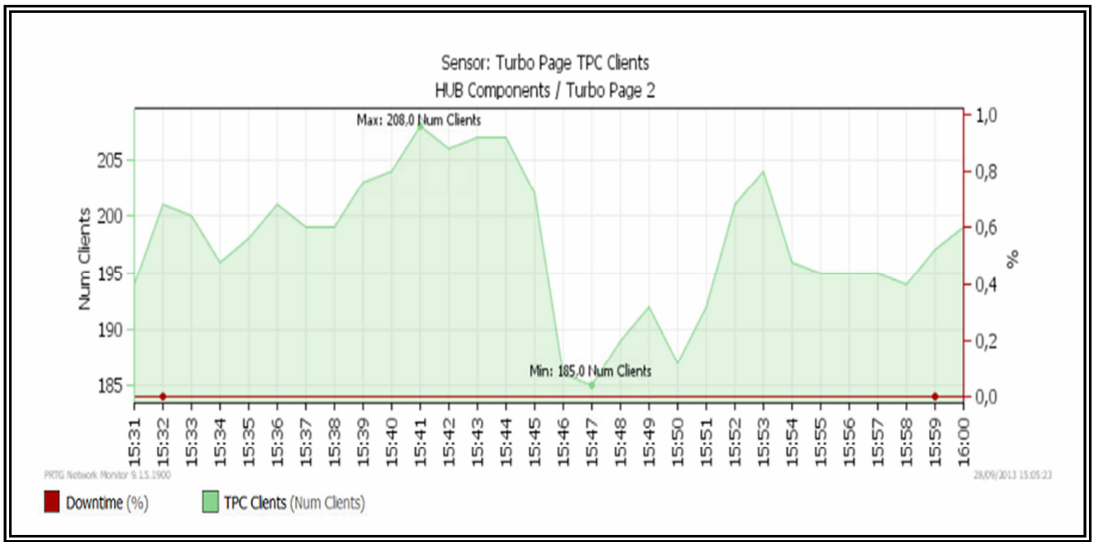

FIGURA 55: Usuarios 15:30-16:00

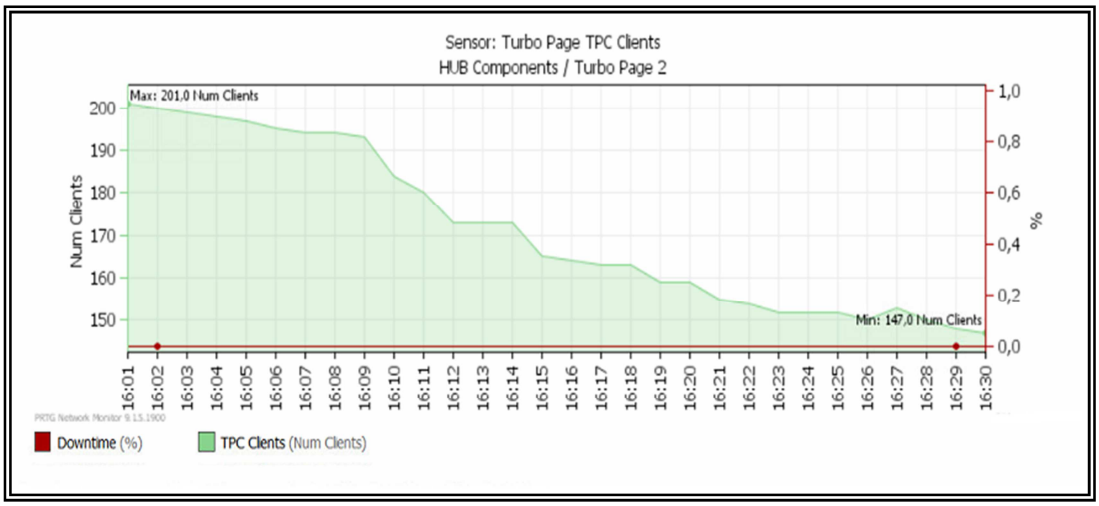

FIGURA 56: Usuarios 16:00-16:30

Luego de determinar la hora pico, que, comprende las 9:00 AM hasta las 18:00 PM; se realizó la captura en los turbopage del número de usuarios activos en la red. A continuación se presenta la tabla de simultaneidad total en diferentes horas, de acuerdo al número de usuarios.

TABLA 8: Simultaneidad instantánea de Usuarios

Date	Hora Inicial	Hora final	Numero Clientes Turbo Page 1	Numero Clientes Turbo Page 2	Total Clientes	Simultaneidad
15/07/2013	14:00:00	14:01:00	217	217	434	27,87%
15/07/2013	14:01:00	14:02:00	217	216	433	27,81%
15/07/2013	14:02:00	14:03:00	220	216	436	28,00%
15/07/2013	14:03:00	14:04:00	221	217	438	28,13%
15/07/2013	14:04:00	14:05:00	222	215	437	28,07%
15/07/2013	14:05:00	14:06:00	223	216	439	28,20%
15/07/2013	14:06:00	14:07:00	226	220	446	28,64%
15/07/2013	14:07:00	14:08:00	224	220	444	28,52%
15/07/2013	14:08:00	14:09:00	227	221	448	28,77%
15/07/2013	14:09:00	14:10:00	228	220	448	28,77%
15/07/2013	14:10:00	14:11:00	227	222	449	28,84%
15/07/2013	14:11:00	14:12:00	223	224	447	28,71%
15/07/2013	14:12:00	14:13:00	223	223	446	28,64%
15/07/2013	14:13:00	14:14:00	223	222	445	28,58%
15/07/2013	14:14:00	14:15:00	226	222	448	28,77%
15/07/2013	14:15:00	14:16:00	226	218	444	28,52%
15/07/2013	14:16:00	14:17:00	226	217	443	28,45%
15/07/2013	14:17:00	14:18:00	226	217	443	28,45%
15/07/2013	14:18:00	14:19:00	235	214	449	28,84%
15/07/2013	14:19:00	14:20:00	239	209	448	28,77%
15/07/2013	14:20:00	14:21:00	239	213	452	29,03%
15/07/2013	14:21:00	14:22:00	235	211	446	28,64%
15/07/2013	14:22:00	14:23:00	235	211	446	28,64%
15/07/2013	14:23:00	14:24:00	237	210	447	28,71%
15/07/2013	14:24:00	14:25:00	238	210	448	28,77%
15/07/2013	14:25:00	14:26:00	240	209	449	28,84%
15/07/2013	14:26:00	14:27:00	241	214	455	29,22%
15/07/2013	14:27:00	14:28:00	240	214	454	29,16%
15/07/2013	14:28:00	14:29:00	239	212	451	28,97%
15/07/2013	14:29:00	14:30:00	237	218	455	29,22%

Continúa….

15/07/2013	14:30:00	14:31:00	238	218	456	29,29%
15/07/2013	14:31:00	14:32:00	239	218	457	29,35%
15/07/2013	14:32:00	14:33:00	240	218	458	29,42%
15/07/2013	14:33:00	14:34:00	240	220	460	29,54%
15/07/2013	14:34:00	14:35:00	238	215	453	29,09%
15/07/2013	14:35:00	14:36:00	235	215	450	28,90%
15/07/2013	14:36:00	14:37:00	235	215	450	28,90%
15/07/2013	14:37:00	14:38:00	233	214	447	28,71%
15/07/2013	14:38:00	14:39:00	234	212	446	28,64%
15/07/2013	14:39:00	14:40:00	233	210	443	28,45%
15/07/2013	14:40:00	14:41:00	232	211	443	28,45%
15/07/2013	14:41:00	14:42:00	231	212	443	28,45%
15/07/2013	14:42:00	14:43:00	231	214	445	28,58%
15/07/2013	14:43:00	14:44:00	229	215	444	28,52%
15/07/2013	14:44:00	14:45:00	228	214	442	28,39%
15/07/2013	14:45:00	14:46:00	230	205	435	27,94%
15/07/2013	14:46:00	14:47:00	229	204	433	27,81%
15/07/2013	14:47:00	14:48:00	233	206	439	28,20%
15/07/2013	14:48:00	14:49:00	234	204	438	28,13%
15/07/2013	14:49:00	14:50:00	233	203	436	28,00%
15/07/2013	14:50:00	14:51:00	234	205	439	28,20%
15/07/2013	14:51:00	14:52:00	234	204	438	28,13%
15/07/2013	14:52:00	14:53:00	233	203	436	28,00%
15/07/2013	14:53:00	14:54:00	227	202	429	27,55%
15/07/2013	14:54:00	14:55:00	226	202	428	27,49%
15/07/2013	14:55:00	14:56:00	229	195	424	27,23%
15/07/2013	14:56:00	14:57:00	230	195	425	27,30%
15/07/2013	14:57:00	14:58:00	231	194	425	27,30%
15/07/2013	14:58:00	14:59:00	231	194	425	27,30%
15/07/2013	14:59:00	15:00:00	228	190	418	26,85%
15/07/2013	15:00:00	15:01:00	226	190	416	26,72%
15/07/2013	15:01:00	15:02:00	222	191	413	26,53%
15/07/2013	15:02:00	15:03:00	221	192	413	26,53%
15/07/2013	15:03:00	15:04:00	219	196	415	26,65%
15/07/2013	15:04:00	15:05:00	213	196	409	26,27%
15/07/2013	15:05:00	15:06:00	208	199	407	26,14%
15/07/2013	15:06:00	15:07:00	209	203	412	26,46%
15/07/2013	15:07:00	15:08:00	201	201	402	25,82%
15/07/2013	15:08:00	15:09:00	203	205	408	26,20%
15/07/2013	15:09:00	15:10:00	205	204	409	26,27%

Continúa….

15/07/2013	15:09:00	15:10:00	205	204	409	26,27%
15/07/2013	15:10:00	15:11:00	203	203	406	26,08%
15/07/2013	15:11:00	15:12:00	202	201	403	25,88%
15/07/2013	15:12:00	15:13:00	199	203	402	25,82%
15/07/2013	15:13:00	15:14:00	197	200	397	25,50%
15/07/2013	15:14:00	15:15:00	195	196	391	25,11%
15/07/2013	15:15:00	15:16:00	197	196	393	25,24%
15/07/2013	15:16:00	15:17:00	195	194	389	24,98%
15/07/2013	15:17:00	15:18:00	194	198	392	25,18%
15/07/2013	15:18:00	15:19:00	195	197	392	25,18%
15/07/2013	15:19:00	15:20:00	195	198	393	25,24%
15/07/2013	15:20:00	15:21:00	192	199	391	25,11%
15/07/2013	15:21:00	15:22:00	194	197	391	25,11%
15/07/2013	15:22:00	15:23:00	195	187	382	24,53%
15/07/2013	15:23:00	15:24:00	198	183	381	24,47%
15/07/2013	15:24:00	15:25:00	199	186	385	24,73%
15/07/2013	15:25:00	15:26:00	199	187	386	24,79%
15/07/2013	15:26:00	15:27:00	197	193	390	25,05%
15/07/2013	15:27:00	15:28:00	195	192	387	24,86%
15/07/2013	15:28:00	15:29:00	196	191	387	24,86%
15/07/2013	15:29:00	15:30:00	194	191	385	24,73%
15/07/2013	15:30:00	15:31:00	194	189	383	24,60%
15/07/2013	15:31:00	15:32:00	201	181	382	24,53%
15/07/2013	15:32:00	15:33:00	200	177	377	24,21%
15/07/2013	15:33:00	15:34:00	196	178	374	24,02%
15/07/2013	15:34:00	15:35:00	198	173	371	23,83%
15/07/2013	15:35:00	15:36:00	201	169	370	23,76%
15/07/2013	15:36:00	15:37:00	199	174	373	23,96%
15/07/2013	15:37:00	15:38:00	199	174	373	23,96%
15/07/2013	15:38:00	15:39:00	203	171	374	24,02%
15/07/2013	15:39:00	15:40:00	204	164	368	23,64%
15/07/2013	15:40:00	15:41:00	208	158	366	23,51%
15/07/2013	15:41:00	15:42:00	206	156	362	23,25%
15/07/2013	15:42:00	15:43:00	207	154	361	23,19%
15/07/2013	15:43:00	15:44:00	207	165	372	23,89%
15/07/2013	15:44:00	15:45:00	202	173	375	24,08%
15/07/2013	15:45:00	15:46:00	186	169	355	22,80%
15/07/2013	15:46:00	15:47:00	185	168	353	22,67%
15/07/2013	15:47:00	15:48:00	189	169	358	22,99%
15/07/2013	15:48:00	15:49:00	192	169	361	23,19%

Continúa….

15/07/2013	15:49:00	15:50:00	187	177	364	23,38%
15/07/2013	15:50:00	15:51:00	192	165	357	22,93%
15/07/2013	15:51:00	15:52:00	201	156	357	22,93%
15/07/2013	15:52:00	15:53:00	204	150	354	22,74%
15/07/2013	15:53:00	15:54:00	196	151	347	22,29%
15/07/2013	15:54:00	15:55:00	195	149	344	22,09%
15/07/2013	15:55:00	15:56:00	195	145	340	21,84%
15/07/2013	15:56:00	15:57:00	195	146	341	21,90%
15/07/2013	15:57:00	15:58:00	194	144	338	21,71%
15/07/2013	15:58:00	15:59:00	197	143	340	21,84%
15/07/2013	15:59:00	16:00:00	199	143	342	21,97%
15/07/2013	16:00:00	16:01:00	201	142	343	22,03%
15/07/2013	16:01:00	16:02:00	200	143	343	22,03%
15/07/2013	16:02:00	16:03:00	199	141	340	21,84%
15/07/2013	16:03:00	16:04:00	198	141	339	21,77%
15/07/2013	16:04:00	16:05:00	197	142	339	21,77%
15/07/2013	16:05:00	16:06:00	195	143	338	21,71%
15/07/2013	16:06:00	16:07:00	194	143	337	21,64%
15/07/2013	16:07:00	16:08:00	194	145	339	21,77%
15/07/2013	16:08:00	16:09:00	193	151	344	22,09%
15/07/2013	16:09:00	16:10:00	184	152	336	21,58%
15/07/2013	16:10:00	16:11:00	180	158	338	21,71%
15/07/2013	16:11:00	16:12:00	173	157	330	21,19%
15/07/2013	16:12:00	16:13:00	173	156	329	21,13%
15/07/2013	16:13:00	16:14:00	173	159	332	21,32%
15/07/2013	16:14:00	16:15:00	165	159	324	20,81%
15/07/2013	16:15:00	16:16:00	164	159	323	20,75%
15/07/2013	16:16:00	16:17:00	163	159	322	20,68%
15/07/2013	16:17:00	16:18:00	163	159	322	20,68%
15/07/2013	16:18:00	16:19:00	159	161	320	20,55%
15/07/2013	16:19:00	16:20:00	159	162	321	20,62%
15/07/2013	16:20:00	16:21:00	155	163	318	20,42%
15/07/2013	16:21:00	16:22:00	154	167	321	20,62%
15/07/2013	16:22:00	16:23:00	152	167	319	20,49%
15/07/2013	16:23:00	16:24:00	152	165	317	20,36%
15/07/2013	16:24:00	16:25:00	152	165	317	20,36%
15/07/2013	16:25:00	16:26:00	150	163	313	20,10%
15/07/2013	16:26:00	16:27:00	153	163	316	20,30%
15/07/2013	16:27:00	16:28:00	150	163	313	20,10%
15/07/2013	16:28:00	16:29:00	148	163	311	19,97%
15/07/2013	16:29:00	16:30:00	147	161	308	19,78%
15/07/2013	16:30:00	16:31:00	146	161	307	19,72%

Al realizar el cálculo de la simultaneidad, se hace referencia al número total de usuarios en la red sobre el número de usuarios totales en determinada hora. Entre las 14:00 y las 16:30 se puede observar que la simultaneidad de la red sobrepasa el nivel pre determinado que fue del 12%, por lo tanto la red se encuentra saturada.

CAPÍTULO IV: ANÁLISIS PARA OPTIMIZACIÓN Y MEJORA DEL SISTEMA VSAT

4.1. ANÁLISIS DEL EQUIPO STAMPEDE

Para analizar el tráfico de la red y determinar las posibles soluciones ante la saturación, se debe realizar previamente un análisis del funcionamiento de los equipos inmersos en la red y controlan el tráfico de la misma. Se realizan entonces pruebas con el equipo COMTECH modelo Stampede activado y desactivado, que permite la compresión de datos para alcanzar un 35% de compresión, estas pruebas se realizan en los diferentes perfiles del contrato (128x64, 256x128, 512x128) mediante el uso de los medidores de velocidad de CNT, TV CABLE, Speedtest – TELCONET. Para tener una percepción del servicio además se realiza pruebas de descarga de video de la página de YouTube.

4.1.1. PRUEBAS CON RED SATURADA

Se realizó las pruebas entre las 14H00 y 16H30 del día 15 de noviembre de 2013, en este horario la red se encontraba saturada, verificándose esto las pérdidas de paquetes obtenidos en el siguiente gráfico:

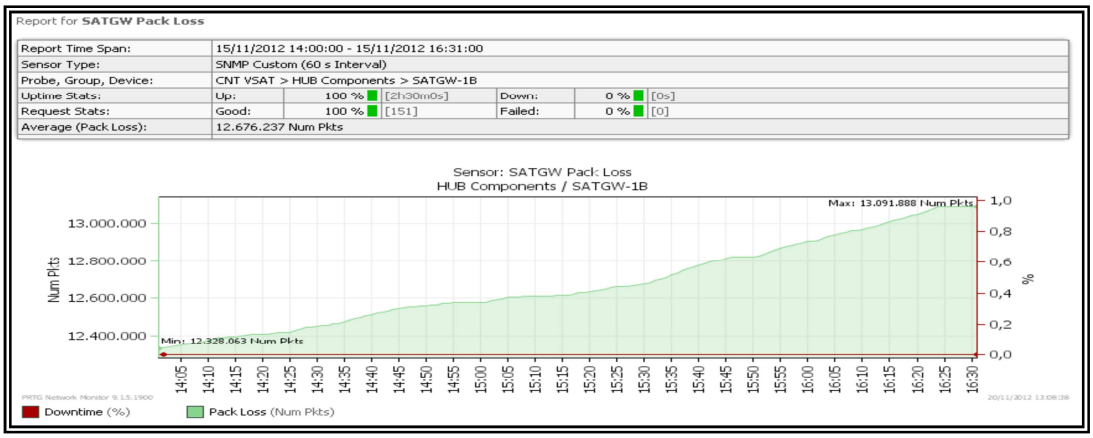

FIGURA 57: Pérdida de paquetes con stampede activo

Se realizan las pruebas de velocidad con los equipos Stampede activos.

TABLA 9: Red Saturada – Stampede habilitado

MEDIDOR DE VELOCIDAD	PERFILES					
	128X64		256X128		512X128	
	Resultado Medidor	Simultaneidad de Usuarios	Resultado Medidor	Simultaneidad de Usuarios	Resultado Medidor	Simultaneidad de Usuarios
CNT	76x85	28,45 %	168x64	28,13 %	182x82	26,53 %
TV CABLE	79x135	28,52 %	186x140	28,00 %	261x169	26,14%
Speedtest – TELCONET	70x60	28,58 %	130x70	27,30 %	190x40	26,46%
Speedtest - LIME (Internacional)	70x50	28,52 %	120x60	26,85 %	140x70	25,82%
Jperf	129x318	28,50 %	247x282	26,82 %	506x247	25,78 %
Descarga de video YouTube: Tiempo 43 Segundos	2:58	28,40 %	1:22	27,30 %	0:54	26,15 %

Se observa que cada uno de los perfiles con sus respectivas pruebas de velocidad y de descarga realizadas en horas pico, debido a la presencia del equipo allot las velocidades no son las esperadas ya que el equipo se encuentra haciendo compresión del tráfico.

Se deshabilita el interfaz Ethernet del Stampede, verificando que si existe navegación y que la salida al internet la VSAT ya no la realiza a través de este equipo. Los resultados de las mediciones de velocidad son los siguientes:

TABLA 10: Red Saturada – Stampede deshabilitado

MEDIDOR DE VELOCIDAD	PERFILES					
	128X64		256X128		512X128	
	Resultado Medidor	Simultaneidad de Usuarios	Resultado Medidor	Simultaneidad de Usuarios	Resultado Medidor	Simultaneidad de Usuarios
CNT	126x192	20,62 %	226x172	21,19 %	500x80	25,11 %
TV CABLE	137x229	20,49 %	255x293	21,13 %	519x250	24,98 %
SpeedTest – TELCONET	110x160	20,36 %	250x190	21,32 %	250x40	25,18 %
Speedtest - LIME (Internacional)	100x140	20,10 %	230x170	20,81 %	240x60	25,24 %
Jperf	129x118	20,10 %	247x118	20,81 %	506x118	25,24 %
Descarga de video You Tube: Tiempo 43 Segundos	3:45	20,49 %	2:55	21,15 %	1:02	25,10%

Para este caso se observa que los medidores tienen mediciones mayores y se acercan a los perfiles configurados, pero en esta caso la saturación de la red es mayor ya que no existe compresión del equipo Stampede lo que ocasiona que el tiempo de descarga sea mayor que cuando estaba habilitado el compresor.

De esta manera se comprueba que el equipo stampede está realizando su trabajo de compresión, no obstante esto no resuelve el problema actual en la red, ya que se sigue percibiendo saturación en la misma.

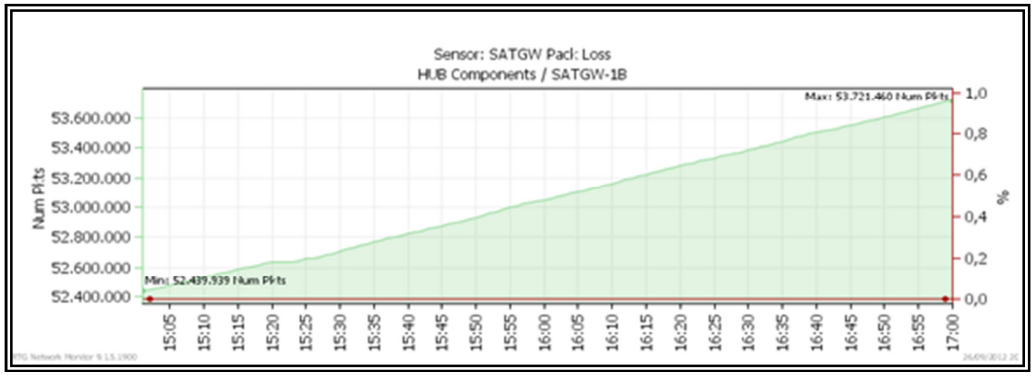

FIGURA 58: Pérdida de paquetes con stampede inactivo

4.2. PRUEBAS CON EL EQUIPO ALLOT

Allot es un dispositivo que permite recolectar estadísticas de tráfico cursante, dichas estadísticas son tomadas para poder verificar el estado de la red, es necesario realizar pruebas en horas pico para poder establecer el tipo de tráfico que está contribuyendo con la saturación de la red, y de esta manera poder buscar las posibles soluciones.

4.2.1. USO DE APLICACIONES WEB

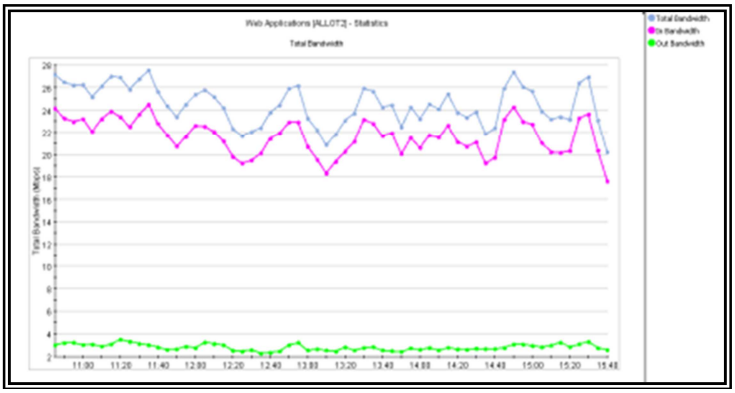

FIGURA 59: Uso de aplicaciones straming

En la gráfica se puede observar el uso de aplicaciones web se han considerado para la medición aplicaciones como: http, https, facebook, Metacafe, Http-proxy, Http_Browsing, Twitter, etc. El pico máximo alcanza 28 Mbps.

4.2.2. APLICACIONES STREAMING

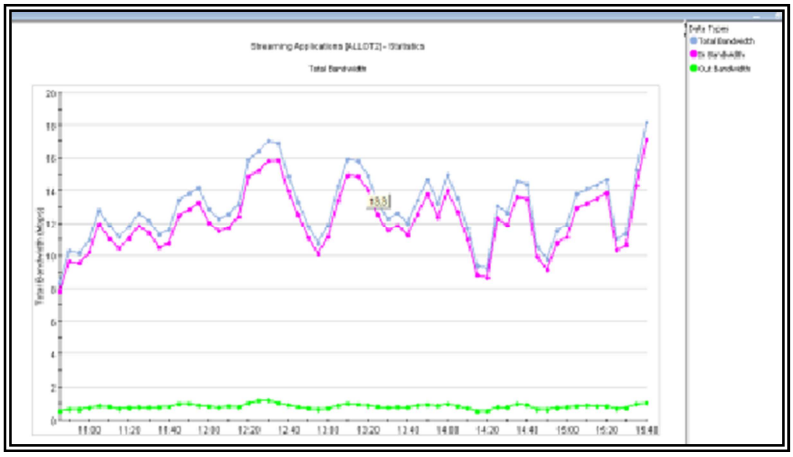

FIGURA 60: Uso de aplicaciones de Streaming

El uso de aplicaciones streaming es muy común en una red puesto que los usuarios acceden a diario a cada una de estas aplicaciones como son Yputube, facebook, entre otras.el pico máximo es 18 Mbps.

4.2.3. MENSAJERÍA INSTANTÁNEA

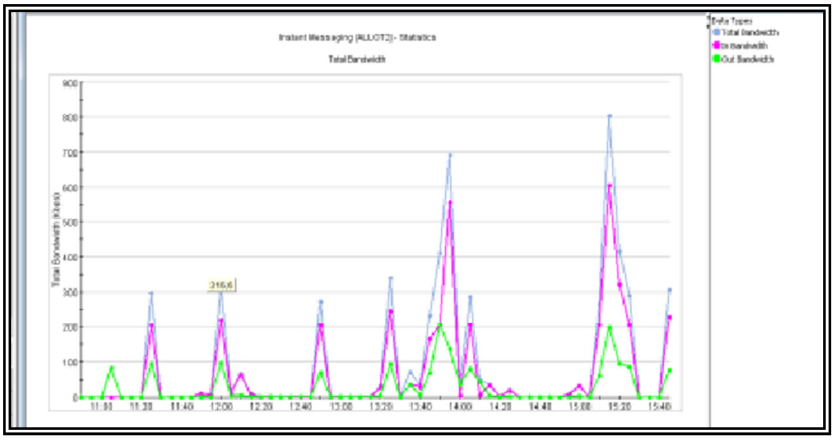

FIGURA 61: Uso de Mensajería Instantánea

El uso de mensajería instantánea hace referencia a aquellas aplicaciones utilizadas para la comunicación como es el mesenger, ebuddy, Yahoo Chat, etc. Ocupa un máximo de 0.9 Mbps

4.2.4. APLICACIONES TCP

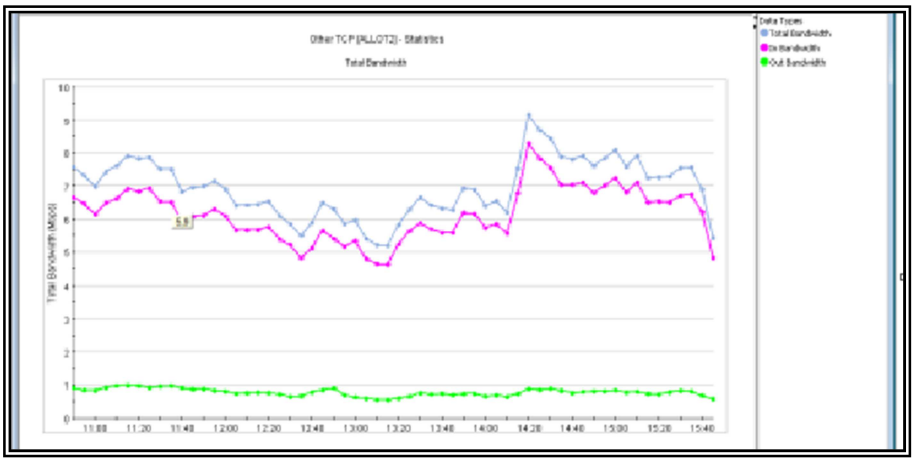

FIGURA 62: Uso de Aplicaciones TCP

Se observa el pico máximo de consumo del protocolo TCP de 9Mbps.

4.2.5. MAIL

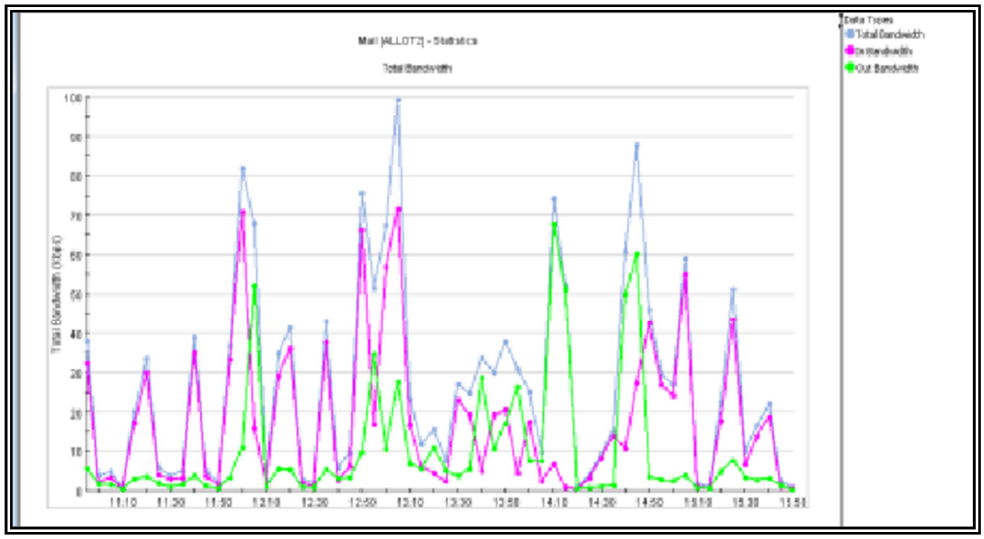

FIGURA 63: Uso de Mail

Para esta medición se tomó en cuenta protocolos como imap, imap2, pop3, entre otros; alcanzando un pico máximo de 0.1 Mbps.

4.2.6. TRANSFERENCIA DE ARCHIVOS

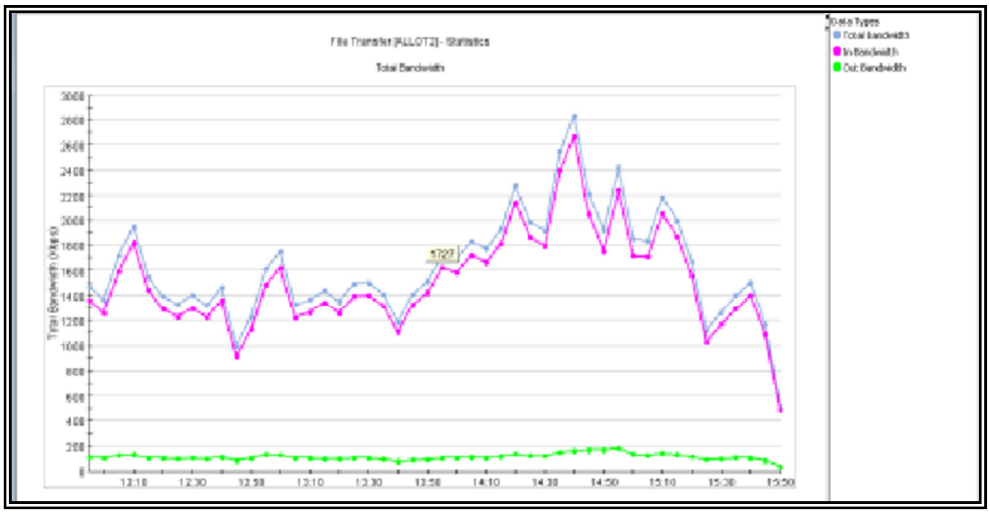

FIGURA 64: Uso de Transferencia de archivos

En la transferencia de archivo se tiene protocolos utilizados como FTP,FTTP, el uso de estos protocolos consumen 2,8 Mbps.

4.2.7. PROTOCOLOS DE OPERACIONES DE RED

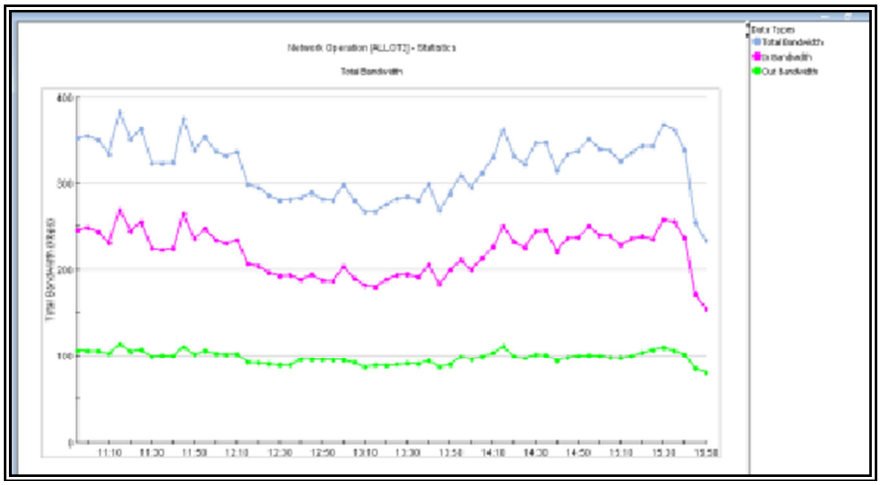

FIGURA 65: Uso de operaciones de red

La operación de la red genera consumo de protocolos los cuales consumen 0,4 Mbps dentro de la red.

4.2.8. PROTOCOLOS DE SEGURIDAD

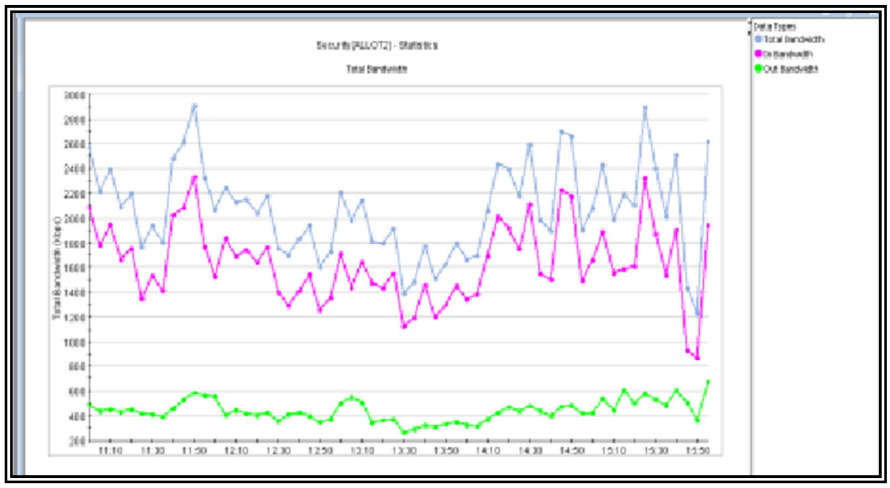

FIGURA 66: Uso de protocolo de Seguridad

Los protocolos que intervienen en la seguridad de la red consumen 2,9 Mbsps de ancho de banda de la red.

4.2.9. USO DE BASE DE DATOS

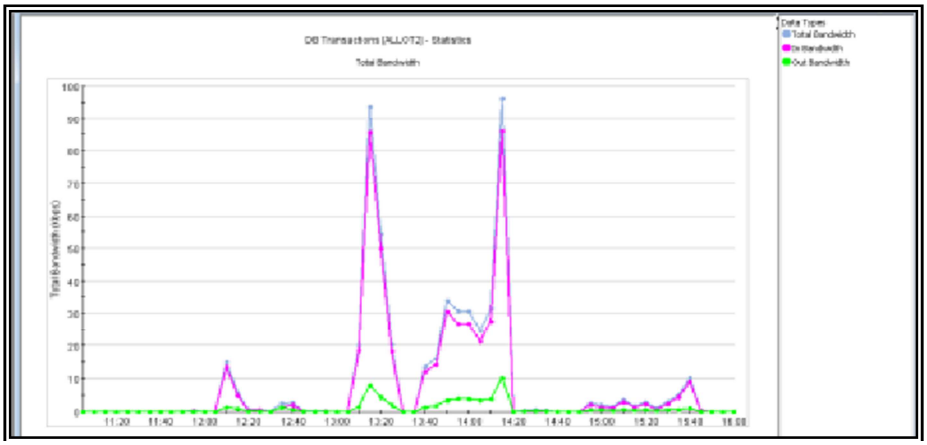

FIGURA 67: Uso de transacciones de Bases de Datos

El uso de transacciones de base de datos también consumen el ancho de banda de la red, para este caso consume 0.1 Mbps.

Se obtiene el siguiente resumen de los diferentes tipos de tráfico de la red:

TABLA 11: Tabla de consumo de protocolos

Aplicaciones (Canal Virtual)	Protocolos Utilizados	Pico Máximo (Mbps)
Web	http, https, facebook, Metacafe, Http-proxy, Http_Browsing, HttpTunnel, Socks, TOR, Twitter, etc.	28
Streaming	Abacast, AOL Radio, CNN Streaming, DivX Web Player, FAcebook Video, Flash Media, Google Earth, iPhone Live Streaming, iPlayer, IPTV, YouTube, YouTube HD, WinAmp, My Space, etc.	18
Mensagería Instantanea	AOL Client, Yahoo Chat, eBuddy, ICQ, MSN, QQ Chat, etc.	0,8
Otras aplicaciones TCP	Gopher, LDAP, Myth, NetwareIP, Philips-VC, etc.	9
Mail	Gmail, IMAP, IMAP2, POP3, SMTP, MS-exchange, etc.	0,1
Transferencia Archivos	BITS, FTP, TFTP, Windows Update, Aspera, etc.	2,8
Operaciones de Red	ARP, BGP, Cisco CDP, ECHO, IGMP, IS-IS, ICMP, NTP, OSPF, PPPoE, RADIUS, NTP, etc.	0,4
Seguridad	GRE, IKE, IPSEC, SSL, SUGP	2,9
Transacciones de Base de Datos	CORBA, CVS, Oracle, SAP, SQL, LDAPS, etc.	0,1
Otras Aplicaciones UDP	Chat, Finger, LDAP, NetwareIP, Philips-VC	0,65

4.2.10. PROTOCOLOS MÁS UTILIZADOS

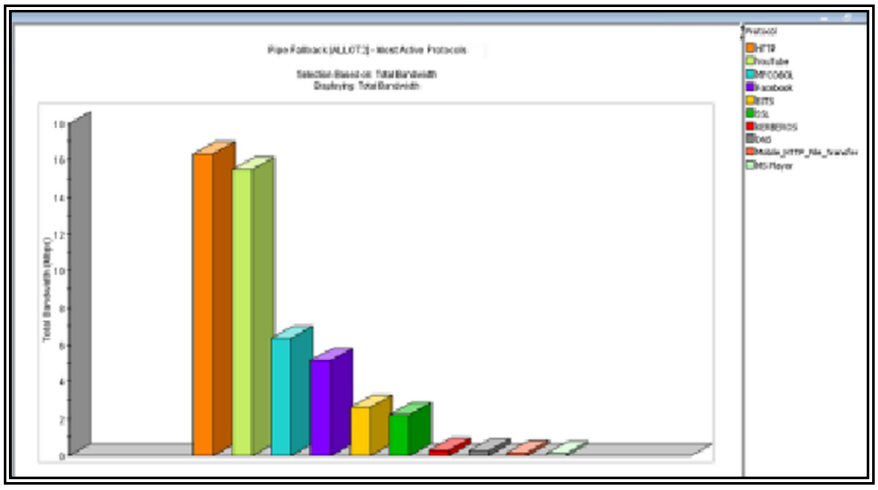

FIGURA 68: Protocolos más utilizados

Se hace un resumen del protocolo más usado en general, obteniendo como resultado el protocolo HTTP.

El equipo Allot no permite detectar todas las firmas de tráfico P2P, por lo que se realiza la captura sobre el equipo que permite el control de ataques IPS:

A continuación se detallan las principales amenazas obtenidas en el monitoreo del tráfico desde el 14 al 21 de junio:

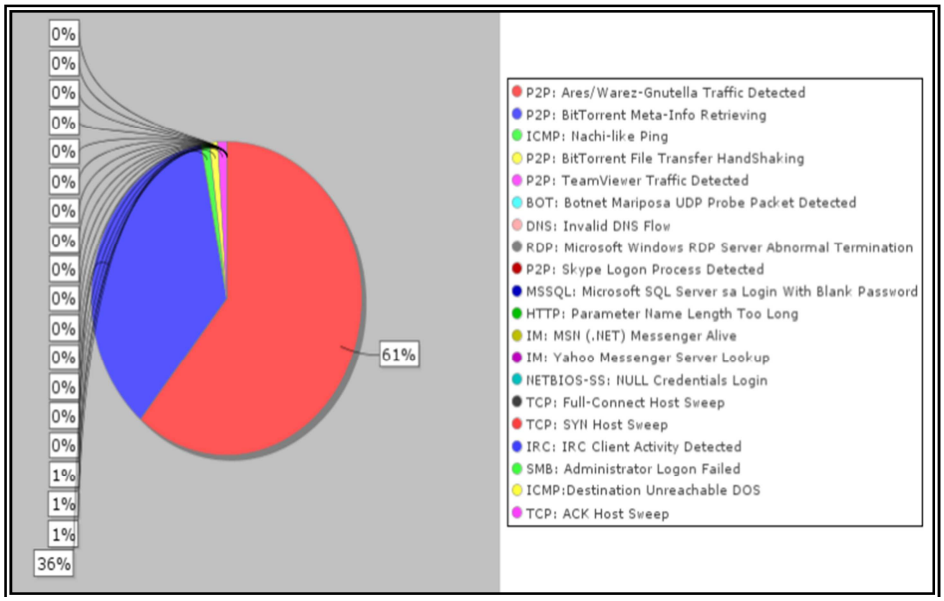

FIGURA 69: Top Amenazas

En la gráfica se representan las principales amenazas obtenidas en la red satelital, cuyo mayor cantidad de tráfico se lo observa en tráfico P2P, colores rojo y azul.

En la siguiente tabla se presentan la cantidad de ataques según el tipo de tráfico.

TABLA 12: Top Amenazas – Cantidad Ataques

#	Attack Name	Attack Count
1.	P2P: Ares/Warez-Gnutella Traffic Detected	2343608
2.	P2P: BitTorrent Meta-Info Retrieving	1495846
3.	ICMP: Nachi-like Ping	59933
4.	P2P: BitTorrent File Transfer HandShaking	59867
5.	P2P: TeamViewer Traffic Detected	40206
6.	BOT: Botnet Mariposa UDP Probe Packet Detected	14547
7.	DNS: Invalid DNS Flow	9391
8.	RDP: Microsoft Windows RDP Server Abnormal Termination	8698
9.	P2P: Skype Logon Process Detected	8504
10.	MSSQL: Microsoft SQL Server sa Login With Blank Password	7567
11.	HTTP: Parameter Name Length Too Long	6491
12.	IM: MSN (.NET) Messenger Alive	6397
13.	IM: Yahoo Messenger Server Lookup	6074
14.	NETBIOS-SS: NULL Credentials Login	3969
15.	TCP: Full-Connect Host Sweep	3697
16.	TCP: SYN Host Sweep	3538

Continúa….

17.	**IRC: IRC Client Activity Detected**	**3125**
18.	SMB: Administrator Logon Failed	2693
19.	ICMP: Destination Unreachable DOS	2652
20.	TCP: ACK Host Sweep	2072
21.	SMTP: Invalid SMTP Flow	2041
22.	IM: Web Based Instant Messenger Services	1788
23.	IM: MSN Messenger Server Lookup	1774
24.	IM: Meebo Access Detected	1636
25.	HTTP: Mozilla Products IDN Spoofing Vulnerability aka Homograph Attacks	1523
26.	HTTP: ZmEu Exploit Scanner	1428
27.	BOT: Spam Bot Activity - Multiple Blacklist Responses from SMTP server	1335
28.	UDP: Host Sweep	1030
29.	BOT: Potential Bot Activity - Multiple Resets from SMTP receiver	974
30.	SIP: SIP Bruteforce Attack Detected-I	764

En la tabla se observan las principales 30 amenazas encontradas con la cantidad de ataques de cada una, se observa que existe un considerable uso de aplicaciones P2P así como ataques de Spam, exploits, Flujos SMTP no válidos, Ataques de denegación de servicio BOT, entre otros.

TABLA 13: Top Amenazas – Cantidad Ataques

Amenaza	IP Origen
P2P: Ares/Warez-Gnutella Traffic Detected	172.3.179.2 172.3.179.3 172.3.11.5 172.6.180.3 172.4.254.2 172.4.191.3 172.1.172.3 172.2.12.2 172.4.155.2
P2P: BitTorrent Meta-Info Retrieving y P2P: BitTorrent File Transfer HandShaking	172.2.116.3 172.2.228.4
ICMP: Nachi-like Ping	172.4.231.4 172.6.121.5 172.2.70.16 172.6.178.10 172.4.228.2 172.16.28.5 172.5.13.2 172.5.119.8 172.2.113.10 172.4.184.3 172.7.71.6 172.4.170.2 172.1.34.3
BOT: Botnet Mariposa UDP Probe Packet Detected	172.6.141.1 172.6.141.4 172.6.64.3 172.4.173.3

En la tabla se observa las principales IPs origen de ataques, corresponden a PCs instalados en infocentros, centros de salud y cooperativas, estás máquinas son las que principalmente generan tráfico malicioso dentro de la red satelital.

El mayor porcentaje de alertas corresponde a trafico P2P 97% de amenazas corresponden a este tráfico, lo que indica que la red está siendo inundada con tráfico utilizado para compartición de archivos, música, videos, piratería. La mayor cantidad de trafico P2P es correspondiente a Ares, un programa de uso masivo que fomenta la piratería y la utilización de programas warez, debido a que por medio del mismo se puede compartir gran cantidad de información, la cual en su gran mayoría es ilícita, ya sea a través de compartición de música, videos, software, pornografía, etc. Otra particularidad de este tipo de aplicaciones es que a más de permitir la descarga ilegal de productos violando así los derechos de propiedad intelectual, es un gran contenedor de todo tipo de malware como pueden ser spyware, gusanos, etc.

En el análisis se identificó otro tipo de amenazas como son infecciones tipo malware, el mismo que se produce por la infección de máquinas de los clientes finales, las cuales al acceder a internet, ya sea a sitios infectados o utilizar programas P2P, provocan que sus computadores se infecten, y sean utilizados posteriormente como zombies (maquinas empleadas por criminales para realizar ataques de denegación de servicio, propagación de virus, realizar tareas de procesamiento, etc.).

Todo el tráfico detectado en el análisis mediante el ALLOT y el ips colocados en el HUB permiten observar que la red tiene un alto consumo en cuanto a aplicaciones web y que está siendo afectada en su mayoría por el tráfico p2p, contribuyendo con esto a la saturación de la red y la percepción de lentitud en el servicio de internet brindado a cada uno de los sitios remotos.

4.3. POSIBLES SOLUCIONES

4.3.1. RESTRICCIÓN DE TRÁFICO MEDIANTE EL EQUIPO ALLOT

Se sugiere como primera instancia que se restringa el tráfico P2P, existen aplicaciones de esta categoría de tráfico que no resultan beneficiosas e inclusive pueden llegar a infringir principios y derechos de propiedad intelectual. Aplicaciones del tipo Ares, BitTorrent deben ser bloqueadas ya que a más de infringir las leyes anteriormente expuestas, causan que la aplicación se apodere del ancho de banda que se tenga en el enlace, sin importar que tan grande pueda llegar a ser el enlace, este tipo de aplicaciones tan solo se apoderan del mismo, causando de esta forma latencia a las aplicaciones válidas y de esta forma malestar para los demás usuarios.

Por otro lado sería conveniente que los EndPoints de los clientes cuenten con un sistema antivirus, además de contar con el mismo, se debe verificar que este se encuentre actualizado y se hagan análisis periódicos de los sistemas, para eliminar el Malware que los equipos puedan tener y afecten con estos a la red. Debido a que es posible que al encontrarse maquinas infectadas produzcan ataques, spam, etc, a servidores locales y

remotos, lo cual puede ocasionar que tanto los servidores DNS como IPs públicas con las que cuenta CNT puedan llegar a caer en listas negras, lo cual puede causar que no se puedan comunicar los usuarios de la red CNT con el resto del mundo que tengan sistemas que hagan filtrado por reputación IP y/o DNS.

Mediante el equipo ALLOT también se puede configurar políticas principalmente destinadas a limitar el tráfico Streaming, CNT debe evaluar el tipo de tráfico que desea limitar en estar red para lograr un buen desempeño. Las políticas creadas en el equipo Allot tienden a limitar el uso del tráfico de streaming en la red.

La captura del tráfico WEB con reportes de contenido de páginas WEB, mediante un equipo Zyxel, se observó que el contenido más visto en la red es Facebook.

Tabla 14: Aplicaciones Web

#	Web Site	Hits
1	static.ak.fbcdn.net (Facebook)	110594
2	profile.ak.fbcdn.net (Facebook)	109318
3	au.download.windowsupdate.com	32960
4	www.facebook.com	19750
5	s.ytimg.com	15884
6	l.yimg.com	14086
7	www.google.com.ec	12982
8	www.google.com	10396
9	sphotos.xx.fbcdn.net (Facebook)	9027
10	www.educacion.gob.ec	8370
11	col.stc.s-msn.com	8257
12	safebrowsing-cache.google.com	7856

Continúa….

13	t2.gstatic.com	7658
14	t1.gstatic.com	7593
15	t0.gstatic.com	7586
16	t3.gstatic.com	7502
17	i2.ytimg.com	6756
18	pagead2.googlesyndication.com	6692
19	i3.ytimg.com	6074
20	i4.ytimg.com	6023

La instalación y operación de una red Satelital demanda ajustes permanentes en los servidores que conforman el HUB, para el HUB de CNT se debe realizar estos ajustes en la medida de la demanda de tráfico de los clientes de la red y el crecimiento de terminales, para un uso eficiente del segmento satelital. En la red se observa que existe tráfico principalmente de contenido social como es el Facebook y tráfico de streaming como es You Tube, se sugiere que el ISP de CNT evalúe el uso del internet de este proyecto ya que el objeto de esta red tiene un interés social. El trafico de streaming causa el consumo excesivo de tráfico de la red satelital los que ocasiona, lentitud en la red , mediante el equipo ALLOT se puede restringir el tráfico, creando políticas configurables. Realizar este proceso no tendría un costo económico ya que las modificaciones se deben realizar únicamente en equipos existentes en la red.

Considerando las horas pico y cantidad de usuarios se recomienda la restricción de la siguiente manera:

TABLA 15: Restricción protocolos

PROTOCOLO	12:00 – 13:00	13:00 -14:30	14:30 – 18:00	RESTO DEL DÍA
FTP	1Mbps	Abierto	1Mbps	Abierto
Seguridad	1.5Mbps	Abierto	1.5Mbps	Abierto
P2P	Abierto	Abierto	500Kbps	Abierto

Al tráfico streaming se lo dividió en dos partes: youtube, y el resto de streaming(protocolos utilizados por streaming sin considerar youtube , según la Tabla)

TABLA 16: Restricción tráfico streaming

PROTOCOLO	11:30 – 12:30	12:30 – 18:00	RESTO DEL DÍA
YOUTUBE	Reducir el consumo al 95%	Reducir el consumo al 92%	Abierto
Resto de streaming(tabla)	Reducir el consumo al 90%	Reducir el consumo al 92%	Abierto
Aplicaciones TCP	Reducir el consumo al 95%	Reducir el consumo al 92%	Abierto

4.3.2. AMPLIACION DEL HUB

Para que CNT no tenga la necesidad de restringir ningún tipo de aplicaciones como yotube, faceboock, entre otras se plantea un asegunda opción; la ampliación del HUB para lo cual es necesario que exista un aumento en el espectro satelital. El transponder actual es de 36MHZ lo cual nos proporciona un total de ancho de banda para la red de 40Mbps. En la red se realizó incremento de usuarios de tal manera que para la ampliación es necesario analizar la arquitectura actual de la red, para posteriormente determinar los equipos necesarios a aumentar.

4.3.2.1. ARQUITECTURA ACTUAL DE LA RED

4.3.2.1.1. Ip gateways

Son las interfaces entre el Estación Central y el cliente, que normalmente se encuentra conectado a través de un backbone terrestre. Básicamente, son servidores que realizan el manejo de las direcciones IP, la transmisión de los paquetes, compresión y encriptación entre otras. Su capacidad de procesamiento y por ello, cantidad de clientes y aplicaciones soportadas puede variar según el modelo y recursos de IPGW utilizado.

Actualmente la red VSAT CNT EP está constituida por 4 ipgateways marca hp modelo DL36G7:

- 4 IPGATEWAYS ACTIVOS
- 1IPGATEWAY SPARE

4.3.2.1.2. Características DL360 G7

- QuadCore Xeon E5630 2.53 GHz
- 6 GB RAM
- Raid 0,1,5
- DVD-ROM
- Rack
- Red: 2 HP NC382i Dual Port Multifunction Gigabit Server Adapter (4 x 1Gb Ports)

Especificaciones Técnicas	
Procesador	• Intel Xeon E5606 (2.13GHz, 8MB, 4 núcleos, 80 Watts)
Numero de Procesadores	• 1
Memoria RAM	• 4 GB
Ranuras para Memoria RAM	• 18 DIMM
Unidad Óptica	• 1 x HP Slim 12.7mm SATA DVD
Controlador de Red	• 2 x NC382i , 1 GbE de 2 puertos
Controlador de Almacenamiento	• Smart Array P410i/Zero Memory
Ranuras de Expansión	• 2 x PCI-E / 1 x PCI-X
Bahías	• 4 x SFF SAS/SATA/SDD, expandible a 8 discos necesario drive cage
Fuente de Poder	• 460 Watts, Hot Plug

FIGURA 70: Ipgateway

La topología actual de la red está basada en una arquitectura tipo estrella donde múltiples VSATs se comunican hacia un HUB Central. La red provista permite entregar al usuario una capacidad de outbound de banda ancha y una alta velocidad de del canal inbound. La red VSAT implementada permite el soporte de varios tipos de terminales fabricados por Hughes para la red HNS, entre ellos el modelo HN740S que es el instalado en la red actual. El canal de retorno de la red permite el soporte de aplicaciones multimedia y calidad de servicio. La arquitectura del HUB es escalable lo que permite la expansión de la red como el crecimiento que se sugiere implementar.

EL NOC HN Hughes se encuentra localizado en la Estación Terrena de Quito perteneciente a CNT sector la Armenia en el Valle de los Chillos. La arquitectura del NOC consiste en un doble rack, el principal y su expansión, la configuración del NOC es redundante. Todos los servidores son configurados con el sistema operativo Windows 2008 y Windows 2003 server. El uso de un cliente “Remote Desktop” basado en IP elimina la necesidad del uso de un switch KVM.

El subsistema de Inroute está configurado con cuatro Sistemas Demoduladores Configurables (CDS). Cada módulo de CDS puede demodular la capacidad total de la Inroute de 2,5 Msps.

4.3.3. EQUIPOS NECESARIOS PARA LA AMPLIACIÓN

Es muy importante luego de tener el aumento de espectro satelital en este caso a 72MHZ, adquirir equipos que permitan el flujo de tráfico de manera correcta en la red para esto se ha considerado el incremento de los siguientes equipos: (Hughes, 2014)

TABLA 17: Equipos necesarios para la ampliación

BIEN O SERVICIO		CANT
HN SYSTEM UPGRADE		
HN-IPGW_HC	HIGH CAPACITY HN IPGATEW SERVER	3
HN-CDS	Configurable Demulator Subsystem – 2.5 Msps.	2
HNNOC-EXP-RACK	Expansion Rack with PDUs, LAN Switch and RPS.	1
NETENFORCER-200M	NET ENFORCER with 200 MBPS Bandwidth support, redundancy power supply.	1
CISCO	Router CISCO de Frontera, para conexión a red de CNT EP.	2
PM-INST-ENG	PM Engineering and installation, HNS Engineering Support.	
HUB Spares :		
HN-IPGW_HC	HIGH CAPACITY HN IPGATEW SERVER	1

4.4. VALORACIÓN ECONÓMICA

Los equipos a instalarse, con la descripción y cantidad, se enumeran a continuación: (SETANEL, 2014)

TABLA 18: Valoración económica

EQUIPO	VALOR UNITARIO	CANTIDAD	VALOR TOTAL
HN-IPGW_HC	$26.400,00	3	79.200,00
HN-CDS	30.601,00	2	79.200,00
CABLE-KIT	2.960,00	1	2.960,00
HNNOC-EXP-RACK	37.500,00	1	37.500,00
NETENFORCER-200M	62.604,00	1	62.604,00
CISCO	7.500,00	2	15.000,00
SERVICIOS DE HUGHES			
PM-INST-ENG	32.741,00		32.741,00
SOPORTE HUGHES ANUAL	45.500,00		45.500,00
HUB Spares :			
HN-IPGW_HC	26.400,00	1	26.400,00
TOTAL SIN IVA			363.107,00

La cotización de los equipos necesarios para la ampliación del HUB tienen un estimado de trescientos sesenta y tres mil ciento siete dólares 00/100 Dólares de los Estados Unidos de América(USD 363.107.00). También a la valoración presentada se debe agregar el valor del arriendo del segmento satelital que CNT deberá cancelar para el aumento del mismo; actualmente la capacidad transponder es de 36 MHz, para lo cual los precios varían entre US$ 2.500 a US$ 3.000 por MHz-mes. Se sugiere cambiar el transponder de capacidad de 72MHz, lo que implica un estimado de $216.000,00 mensuales por el arriendo del segmento satelital.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Al realizar el análisis de tráfico cursado por la red VSAT de CNT EP, se determinó que la red se encontraba saturada, presentando una simultaneidad de usuarios (36%) superior a la prevista en el dimensionamiento inicial del proyecto; causando lentitud en el servicio brindado a los usuarios finales.
- Los equipos inmersos en la red que contribuyen al manejo de tráfico de la red; como es el quipo STAMPEDE, el cual realiza compresión de datos y el equipo TURBOPAGE que actúa como acelerador; se encuentran realizando su trabajo sin ninguna anomalía, por lo cual se descartó la posibilidad de que la saturación se deba a su mal desempeño.
- Mediante el equipo ALLOT se determinó que los usuarios hacen uso de una gran cantidad de tráfico streaming; haciendo referencia a “youtube” y a “facebook” como las aplicaciones más utilizadas por parte de infocentros y centros educativos; siendo este una de las principales causas por la cual la red se encuentra en saturación
- Mediante el análisis del ips, se identificó tipo de amenazas como son infecciones tipo malware, el mismo que se produce por la infección de máquinas de los clientes finales, las cuales al acceder a internet, ya sea a sitios infectados o utilizar programas P2P, provocan que sus computadores se infecten, y sean utilizados posteriormente como zombies (maquinas empleadas por criminales para realizar ataques de

denegación de servicio, propagación de virus, realizar tareas de procesamiento, etc.).

- Cabe anotar también que las velocidades configuradas para los estándares de demanda de las aplicaciones actuales en internet de influyen en la generación de una mala percepción del usuario por causa de una velocidad configurada muy baja configurada y prestada por el sistema para estos estándares.
- La red VSAT de CNT EP, brinda servicio de internet a sitios de zonas rurales; por lo cual se debe tomar medidas ante la saturación lo más pronto posible, para que de esta manera centros educativos infocentros y centros de salud sigan contando con el servicio de internet que hoy en día se ha convertido en una de las herramientas más importantes de trabajo.
- Luego de realizar la valoración económica que implica brindar soluciones para la mejora de la red; la solución que brindaría mayor eficacia y eficiencia para la red es la ampliación del HUB conjuntamente con el aumento del espectro Satelital. No obstante esto implica una gran cantidad de inversión, por lo cual se sugiere que primero se implante políticas de seguridad en el equipo ALLOT ya que e4sto no tendría ningún costo económico, posterior a esto si la red permanece saturada, entonces se tomara la opción de la ampliación.

5.2. RECOMENDACIONES

- Se recomienda que se restringa el tráfico P2P, existen aplicaciones de esta categoría de tráfico que no resultan beneficiosas e inclusive pueden llegar a infringir principios y derechos de propiedad intelectual. Aplicaciones del tipo Ares, BitTorrent deben ser bloqueadas ya que a más de infringir las leyes anteriormente expuestas, causan que la aplicación se apodere del ancho de banda que se tenga en el enlace, sin importar que tan grande pueda llegar a ser el enlace, este tipo de aplicaciones tan solo se apoderan del mismo, causando de esta forma latencia a las aplicaciones válidas y de esta forma malestar para los demás usuarios.
- Se recomienda que los “EndPoints” de los clientes cuenten con un sistema antivirus, además de contar con el mismo, se debe verificar que este se encuentre actualizado y se hagan análisis periódicos de los sistemas, para eliminar el Malware que los equipos puedan tener y afecten con estos a la red. Debido a que es posible que al encontrarse maquinas infectadas produzcan ataques, spam, etc, a servidores locales y remotos, lo cual puede ocasionar que tanto los servidores DNS como IPs públicas con las que cuenta CNT puedan llegar a caer en listas negras, lo cual puede causar que no se puedan comunicar los usuarios de la red CNT con el resto del mundo que tengan sistemas que hagan filtrado por reputación IP y/o DNS.
- Se recomienda implementar un sistema de prevención de Intrusos (IPS) para que se pueda mitigar todo tipo de amenazas.

- Se recomienda la instalación de servidores WEB Cache en cada uno de los sitios, con esto permita optimizar la utilización del servicio de Internet manteniendo las páginas, gráficos, documentos, etc. más utilizadas localmente, así disminuir la utilización del segmento satelital con una consecuente mejora de la percepción del servicio.
- Se recomienda que Mediante el equipo ALLOT se configure políticas principalmente destinadas a limitar el tráfico Streaming, CNT debe evaluar el tipo de tráfico que desea limitar en estar red para lograr un buen desempeño.
- Se recomienda también la ampliación del HUB, luego de realizar un incremento en el espectro satelital, ya que el actual no abastece al ancho de banda que requiere actualmente la red.

REFERENCIAS BIBLIOGRÁFICAS

HUGHES. (2012). Dimensionamiento de la red. 2012. *HN Systems Remote Installations and Opertions*, 315.

Allot comunications. (2011). NETENFORCER.

COMTECH. (2012). STAMPEDE GUIDE.

Ftapinamar. (1 de Diciembre de 2010). *Blogspot.* Recuperado el 29 de junio de 2013, de http://ftapinamar.blogspot.com/2010/12/lnbf-dual-para-banda-c-y-banda-ku.html

HUGHES. (2010). HN 0650 System installation and operation. Washintong.

HUGHES. (2010). HN 0650 System introduccion. Washintong.

HUGHES. (2010). HN System installation and operation. Washintong.

HUGHES. (2010). HN0610 Systems Remote Instalations. Washintong.

HUGHES. (2010). *Turbopage Solutions.* Washintong.

HUGHES. (2011). *TURBOPAGE.*

Hughes. (ENERO de 2014). COSTO DE EQUIPOS Y MANTENIMIENTO.

HUGHES. (s.f.). HN0620 Configurations and operations.

PAESSLER. (JULIO de 2013).Obtenido de www.paessler.com/prtg/download

PRTG. (2012). *PRTG GUIDE.* Recuperado el Agosto de 2013, de http://www.es.paessler.com/bandwidth_monitoring

SETANEL. (ENERO de 2014). ARRIENDO DEL ESPECTRO.

ZatInforme. (diciembre de 2007). *Blogspot.* Recuperado el 2013 de junio 27, de http://zatinforme.blogspot.com/2007/12/la-diferencia-entre-las-antenas-de.html