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

Lorena Monserratte Páez Martínez
Email: lorena2902@hotmail.com

Abstracto - El estado del arte de este proyecto contempla el análisis del tráfico de la red del sistema VSAT perteneciente a la Corporación Nacional de Telecomunicaciones (CNT), la cual brinda servicio de internet a los sitios más alejados y de difícil acceso de todo el país. Actualmente el internet se ha convertido en una de las herramientas indispensable tanto para trabajo como para estudios, es por eso que es importante que la red funcione con eficiencia para que los usuarios finales puedan acceder al internet sin complicaciones; los usuarios beneficiarios son: centros de salud, centros educativos, infocentros y cooperativas

I. INTRODUCCIÓN

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 causas del problema, y mediante análisis de tráfico en horas pico se presentan soluciones óptimas para la mejora del sistema. El presente trabajo se basa en un análisis de la red VSAT de CNT EP, mediante el uso de la herramienta PRTG y el equipo ALLOT, con los cuales se realiza el análisis del tráfico cursante en la red.
Primero se realiza la revisión de conceptos para la comprensión del funcionamiento del sisema, luego se revisa el funcionamiento de equipos de la red; para luego empezar con el análisis del tráfico y poder encontrar las soluciones ante el problema de saturación.

II. CONCEPTOS

2.1 Sistema Satelital:

Un sistema Satelital tiene el propósito de enlazar múltiples sitios, con el propósito de obtener una comunicación eficiente; dicho sistema está compuesto por los siguientes segmentos: Segmento Satelital, Segmento Terrestre. [1]

2.2 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 tráfico 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 [2]

2.3 IP Gateways:

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. [3]

2.4 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. [4]

2.5 Equipo Allot:

Allot netenforcer es un dispositivo que nos 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.[5]

2.6 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.[6]

2.7 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. [7]

III. Red Saturada

Actualmente la red VSAT de CNT EP. Percibe lentitud en la misma, haciendo que los usuarios finales se quejen de no poder hacer uso del servicio. Ante este problema se debe encontrar el motivo de dicha lentitud. La red en un inicio se diseñó para 1500 usuarios, posteriormente CNT aumenta usuarios, es por eso que se requiere mediante la herramienta PRTG analizar el número de usuarios actuales en la red determinar la simultaneidad en horas pico.

3.1 Comparación actual y contractual de la Red

Tabla 1.- Diseño contractual

Simultaneidad		PREVISTO EN EL CONTRATO		
Simult Download %	Simult Upload %	Cantidad de sitios	Outbound hub -> rem	Inbound rem -> hub
12,00%	7,00%	5	614	90
12,00%	7,00%	310	19.046	2.778
12,00%	7,00%	406	12.472	3.638
12,00%	7,00%	779	11.965	3.490
Total Sites		**1.500**		
Total END USER Traffic – kbps			**44.099**	**9.995**

La demanda 12% en el outbound y 7% en Inbound asumida por CNT en el proyecto resultó ser muy baja, la simultaneidad de usuarios medida en hora pico llega alcanzar un 32% para el Outbound, 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.

Tabla 2.- Diseño actual.

Velocidad considerando la simultaneidad		SITUACION ACTUAL		
Simult Download %	Simult Upload %	Cantidad de Sitios	Outbound hub -> rem	Inbound rem -> hub
25,00%	7,00%	29	7424	520
25,00%	7,00%	269	34432	2410
25,00%	7,00%	940	60160	8422
25,00%	7,00%	365	11680	1635
Total Sites		**1.603**		
Total END USER Traffic – kbps			**113.696**	**12.988**

Se puede observar que en la tabla 1 el total de ancho de banda con la compresión y aceleración llega a 40Mbps que fue lo previsto en el contrato en un principio, sin embargo luego de aumentar sitios y modificar velocidades en la tabla dos se observa que la red sobrepasa el ancho de banda límite; de tal manera que la red se encuentra en saturación.

3.2 Análisis de simultaneidad

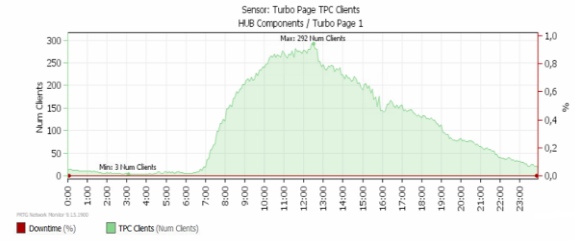

Figura1.-Hora pico

Mediante la herramienta PRTG y el TURBOPAGE, se puede determinar la hora pico, es decir el rango de tiempo en el cual la red se encuentra saturada. En la figura 1 se observa que la red se encuentra saturada desde las 9:00 AM, y vuelve a su curso normal a las 18:00 PM.

Para el análisis de simultaneidad se toma un rango dentro de saturación y mediante el sensor implantado en la herramienta PRTG se contabiliza el número de usuarios que cursan por la red.

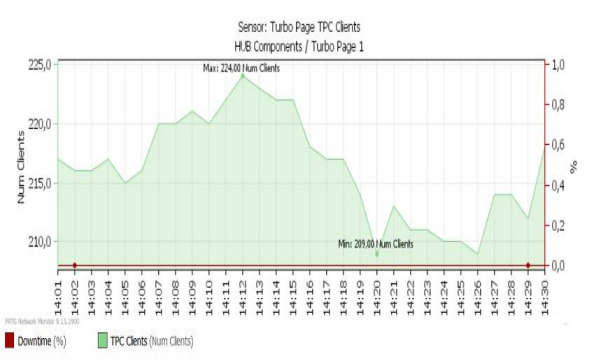

Figura 2.- Número de usuarios

En la figura 2 se observa que entre las 14:00 y 14:30 el número de usuarios cursando la red llega un pico máximo de 224 usuarios por minuto, lo que re4sulta una simultaneidad de 25% de la red superando la prevista en el inicio del proyecto de esta manera se comprueba que la red se encuentra en saturación.

IV. Análisis del Tráfico de la Red

Luego de determinar la saturación de la red, es importante realizar un análisis del tráfico que cursa por la red, para esto se hace uso del equipo allot el cual permite realizar estadísticas de cada tipo de tráfico y aplicaciones que están siendo usadas por los terminales o usuarios finales. El análisis y estadísticas son tomados en determinada hora dentro del horario pico de saturación.

4.1 Estadísticas de tráfico

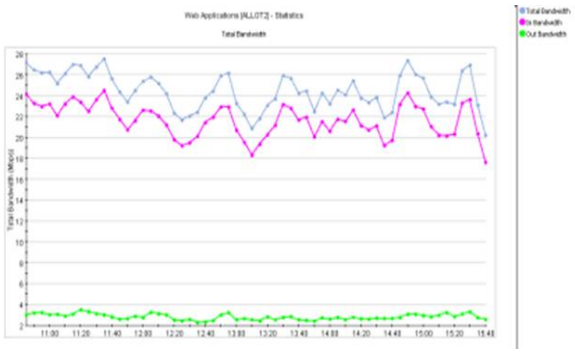

Figura 3.- Aplicaciones Web

Enla figura 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.

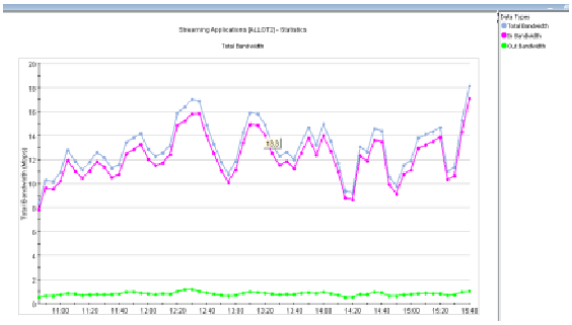

Figura 4.- Tráfico streaming

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 Amenazas

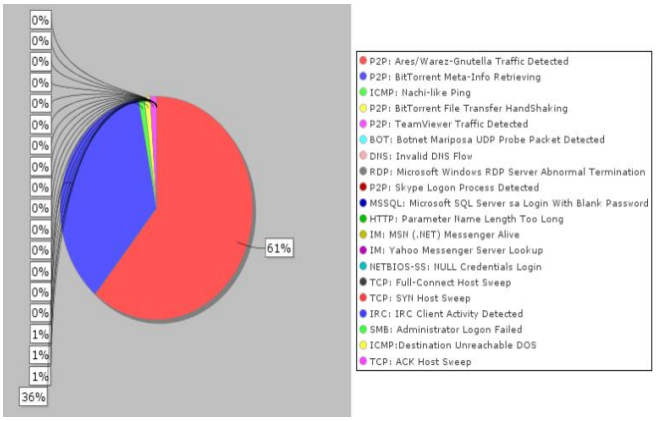

Figura 5.- Amenazas

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.

V. Soluciones

5.1 Restricción del tráfico

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.

Tabla 3.- Restricción del Tráfico

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

5.2 Ampliación del HUB

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:

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 $216.00,00 mensuales por el arriendo del segmento satelital

VI. CONCLUSIONES Y RECOMENDACIONES

6.1 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.

6.2 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

- 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

VII. REFERENCIAS BIBLIOGRÁFICAS

[1] *101 Consulting*. (s.f.). Recuperado el Febrero de 2013, de http://www.101-consulting.com/index.php?option=com_content&view=category&layout=blog&id=51&Itemid=72
[2] HUGHES. (2011). *TURBOPAGE.*
[3] H HUGHES. (2010). HN 0650 System introduccion. Washintong.
UGHES. (2011). *TURBOPAGE.*
[4] HUGHES. (2010). HN0610 Systems Remote Instalations. Washintong.
[5] COMTECH. (2012). STAMPEDE GUIDE.
[6] Allot comunications. (2011). NETENFORCER.
[7] PRTG. (2012). *PRTG GUIDE.* Recuperado el Agosto de 2013, de http://www.es.paessler.com/bandwidth_monitoring

VIII. BIOGRAFÍA

Lorena Monserratte Páez Martínez, nace en la ciudad de Quito el 29 de febrero de 1988, realizó sus estudios secundarios en el colegio Emile Jacquez Dalcroze obteniendo el titúlo de bachiller especialidad físico matemático, actualmente egresada de la carrera ingeniería elect´ronica en redes y comunicación de datos.