UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

ANÁLISIS DE TRÁFICO DE UNA RED LOCAL UNIVERSITARIA

(Traffic Analysis of a University local Network)

Rene Ríos
Universidad Rafael Belloso Chacín
rene.rios@urbe.edu

José R. Fermin
Universidad del Zulia
jfermin@luz.edu.ve

RESUMEN

El propósito del trabajo fue analizar el tráfico de una red local universitaria (ULAN). Mediante un software comercial, Colapsoft Capsa Ver. 6.4, se estudió el flujo de información generado por los sistemas administrativos y académicos de la universidad. El tráfico fue monitoreado a nivel de las capas 2 y 3 del modelo OSI. El desempeño de la red se caracterizó mediante los parámetros Cantidad de Tráfico, Tasa de Transferencia y el Porcentaje de Utilización. Se determinó que la red universitaria, bajo la estructura actual, tiene un comportamiento dentro de los estándares recomendados.

Palabras clave: Tráfico, Red Local, Tasa de transferencia, Cantidad de tráfico, Porcentaje de utilización

ABSTRACT

The main purpose of this work was to analyze the data traffic in a Universitary Local Network (ULAN). Using a commercial software, Colapsoft Capsa Ver. 6.4, we were able to study the traffic generated by the administrative and academic systems of the university. The traffic was monitored at the levels 2 and 3 of the OSI model. The performance of the ULAN was characterized by the parameters Amount of traffic, transfer rate and usage percentage. We have determined that the ULAN under the actual structure, behaves within the recommended standards.

Key words: traffic, Local Network, transference rate, amount of traffic, usage percentage

INTRODUCCION

Hoy día la información llega de varias fuentes y en diferentes formas, esto trae como consecuencia una demanda de mejorar la red o los medios de transmisión final. Las redes de datos han registrado crecimientos muy significativos generados por nuevas formas de hacer llegar la información a los usuarios, en la actualidad las empresas luchan por mejorar sus procesos y su capacidad de poder competir en el

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

mundo de las telecomunicaciones, razón por la cual se deben adoptar soluciones relacionadas con Internet ya que las redes de computo, sufren frecuentemente de cogestión y colapsos importantes. Estos se producen porque en las redes habitualmente no circula tráfico que hasta hace poco era habitual como los videos, audio, mensajería y multimedia.

En vía a solucionar esta problemática, las empresas deben mejorar sus sistemas de comunicación como estructuras organizadas, ya que nadie escapa de los avances tecnológicos.

Las redes locales fueron diseñadas, fundamentalmente, para soportar aplicaciones de procesamiento de datos que, aunque requieren un servicio de transporte fiable, no son muy exigentes en cuanto a otros parámetros de calidad de servicio como retardo, tasa de pérdidas, entre otros aspectos que se pueden mencionar. Sin embargo, el desarrollo de nuevas tecnologías de información y comunicación, ha permitido la evolución de las redes, dotándolas de la capacidad de satisfacer simultáneamente los requisitos de tráficos de muy diversa naturaleza. Situación esta, que favorece la aparición de nuevos servicios y aplicaciones para los cuales las características, anteriormente mencionadas, son esenciales.

Actualmente existen redes locales que poseen conexiones con más de 200 computadores conectados, lo que trae como consecuencia que la red pueda estar más lenta, y es aquí donde existen herramientas capaces de analizar el tráfico de la Red Lan, a través del software Colasoft Capsa 6.4 Professional Edition Demo, el cual permite monitorear la red.

Por otro lado, al hacer referencia al contexto objeto de estudio, se observó que el problema de la lentitud del tráfico en la red que es utilizada, viene de los trabajos que realizan cada uno de los usuarios que por diferentes razones y circunstancias, permanecen conectados a la red de la Universidad; estos usuarios poseen acceso al sistema de Internet y sistemas desarrollados por la institución, situación que hace que en ciertos momentos el sistema se torne lento.

Esta situación llevó a analizar la red, el trafico que se genera a nivel de enlace, identificando toda la información que se transmite, y se visualizaron los paquetes, los bytes que transportan las tramas a nivel de enlace, volumen de trafico, cantidad de colisiones y ancho de banda utilizado, y adicionalmente se pudo contar con la información que permitirá planificar acertadamente la adquisición o sustitución de equipos, en el momento que lo disponga la organización.

En función de lo planteado, el propósito de esta investigación estuvo dirigido a analizar el tráfico de una red local usando el software Capsa Colapsoft el cual permitió evidenciar de manera sistemática la situación que se ha venido presentando en las organizaciones objeto de estudio. A fin de poder contar con una herramienta que permita a los investigadores y administradores de redes utilizar un software apropiado para el análisis del tráfico de redes Lan.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

En este sentido, el estudio se considera relevante desde tres puntos de vista: Metodológico, desde este ámbito el desarrollo del estudio ofrece abordar la problemática de manera sistemática, considerando desde el diagnostico situacional hasta el establecimiento de una propuesta que permita optimizar la red universitaria. Práctico, la determinación de la disposición y adaptabilidad que tienen en la organización objeto de estudio, para asumir los cambios y transformaciones, siempre innovando y dispuestos a incorporar cualquier elemento que contribuya al mejoramiento de la plataforma tecnológica. Teórico, ya que el análisis de las teorías referidas a las redes para establecer procesos, es preactiva al establecimiento de nuevos o reformulados enfoques conceptuales, dentro de los cuales su aporte holístico contribuye a indicar perspectivas hacia una efectiva administración de los aspectos relacionados con la variable analizada.

BASES TEÓRICAS

Redes de Área Local (LAN)

Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña. Estas redes son usadas para la interconexión de computadores personales y estaciones de trabajo.

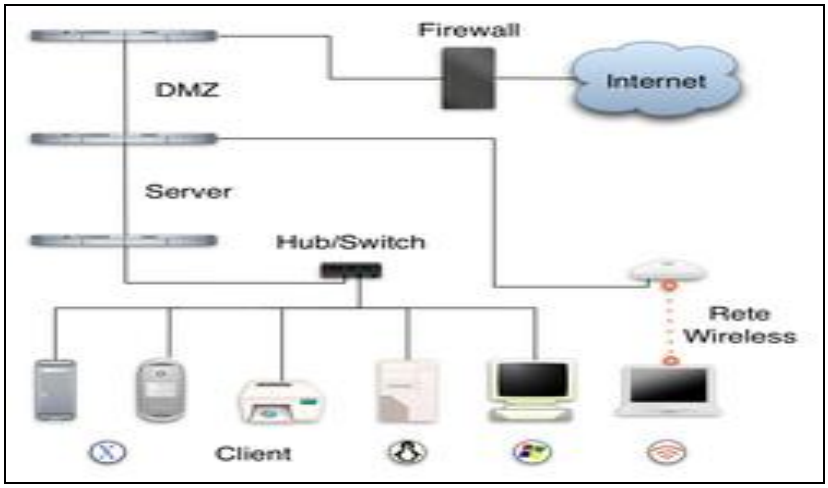

Figura 1. Esquema de una red local típica

Topología de Redes

La configuración de una red, recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se entiende como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando hablamos de la configuración lógica tenemos que pensar en cómo se trata la información dentro de nuestra red, como se dirige de un sitio a otro o como la recoge cada estación.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

Topología en Estrella

Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red, quien se encarga de gestionar las transmisiones de información por toda la estrella. La topología de Estrella es una buena elección siempre que se tenga varias unidades dependientes de un procesador, esta es la situación de una típica mainframe, donde el personal requiere estar accesando frecuentemente esta computadora. En este caso, todos los cables están conectados hacia un solo sitio, esto es, un panel central.

Resulta económica la instalación de un nodo cuando se tiene bien planeado su establecimiento, ya que este requiere de un cable desde el panel central, hasta el lugar donde se desea instalarlo.

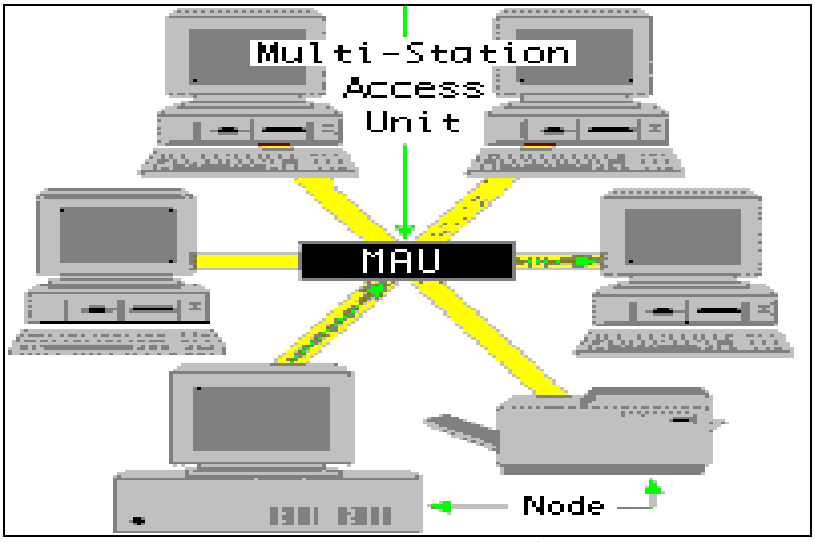

Figura 2. Red Local con topología en estrella

Topología en Bus

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; el bus. Las tramas de información emitidas por un nodo (Terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cuál es la que le corresponde, la destinada a él.

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

Como ejemplo más conocido de esta topología, encontramos la red Ethernet de Xerox. El método de acceso utilizado es el CSMA/CD, método que gestiona el acceso al bus por parte de los terminales y que por medio de un algoritmo resuelve los conflictos causados en las colisiones de información. Cuando un nodo desea iniciar una transmisión, debe en primer lugar escuchar el medio para saber si está ocupado, debiendo esperar en caso afirmativo hasta que quede libre. Si se llega a producir una colisión, las estaciones reiniciarán cada una su transmisión, pero transcurrido un tiempo aleatorio distinto para cada estación.

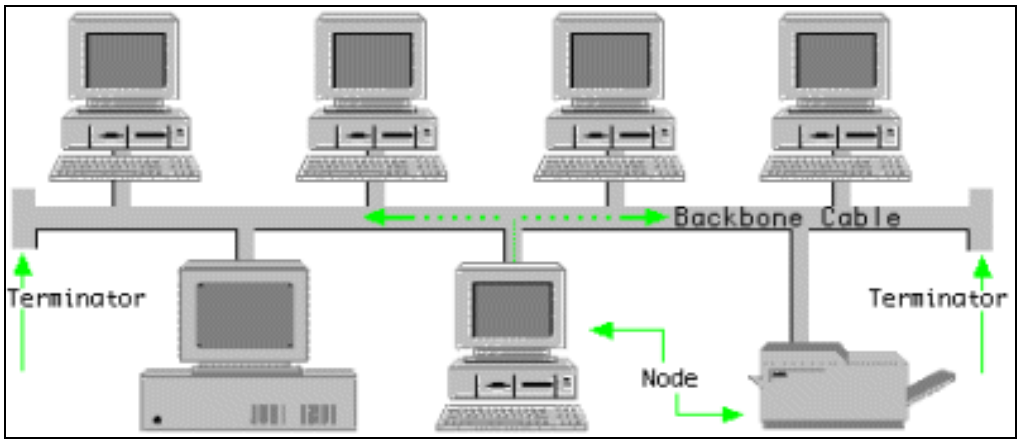

Figura 3. Red Local con topología en BUS

Topología en Anillo

Los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando.

La topología de anillo está diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado. Este esquema de cableado muestra alguna economía respecto al de estrella. El anillo es fácilmente expandido para conectar más nodos, aunque en este proceso interrumpe la operación de la red mientras se instala el nuevo nodo. Así también, el movimiento físico de un nodo requiere de dos pasos separados: desconectar para remover el nodo y otra vez reinstalar el nodo en su nuevo lugar.

Topología de anillo doble

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

Una topología en anillo doble consta de dos anillos concéntricos, donde cada Host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos. La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

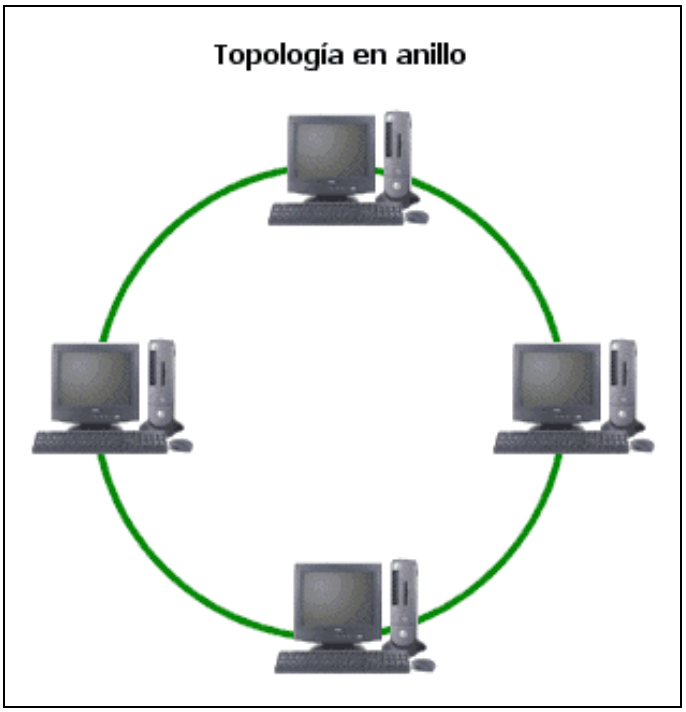

Figura 4. Red Local con topología en anillo

Elementos de una Red Local

Una red local está compuesta básicamente por elementos de hardware y software entre los cuales se pueden destacar:

- **El servidor:** es el elemento principal de procesamiento, contiene el sistema operativo de red y se encarga de administrar todos los procesos dentro de ella, controla también el acceso a los recursos comunes como son las impresoras y las unidades de almacenamiento.

- **Las estaciones de trabajo:** en ocasiones llamadas nodos, pueden ser computadoras personales o cualquier Terminal conectada a la red. De esta manera trabaja con sus propios programas o aprovecha las aplicaciones existentes en el servidor.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

- **El sistema operativo de red:** es el programa (*software)* que permite el control de la red y reside en el servidor. Ejemplos de estos sistemas operativos de red son: NetWare, LAN Manager, OS/2, LANtastic y Appletalk.

- **Los protocolos de comunicación:** son un conjunto de normas que regulan la transmisión y recepción de datos dentro de la red.

- **La tarjeta de interfaces de red**: proporciona la conectividad de la terminal o usuario de la red física, ya que maneja los protocolos de comunicación de cada topología especifica.

Todos estos elementos permiten que una red pueda conectarse para compartir dispositivos de Hardware, los más comunes son impresoras tipo láser, de matriz.

Análisis de Tráfico

El análisis del tráfico de red se basa habitualmente en la utilización de sondas con interfaz Ethernet conectadas al bus. Dichas sondas, con su interfaz Ethernet funcionando en modo promiscuo, capturan el tráfico a analizar y constituyen la plataforma en la que se ejecutaran, de forma continua, aplicaciones propietarias o de dominio público, con las que se podrá determinar el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre la misma

Tráfico de Red

El trafico de redes de área local se mide como la cantidad de información promedio que se transfiere a través del canal de comunicación, y a la velocidad que se transfiere por ello la importancia, del conocimiento sobre la “Teoría de la información” y sus diferentes elementos para poder evaluar en formas más eficiente y eficaz el tráfico en la red.

MATERIALES Y MÉTODOS

El monitoreo del tráfico se realizó durante un período efectivo de 7 días en horario de trabajo, durante 7 días de prueba en horario comprendido desde las 8:00am hasta las 7:00 de la noche.

El flujo de datos de la red administrativa-académica en estudio comprende básicamente: Estudios a Distancia, Contenidos de Información académica, Datos de Contabilidad, de Compras y de Cuentas por pagar. La Figura 5 muestra un diagrama esquemático de la red local bajo estudio. Las pruebas fueron realizadas por medio de un computador dedicado, conectado al enrutador.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

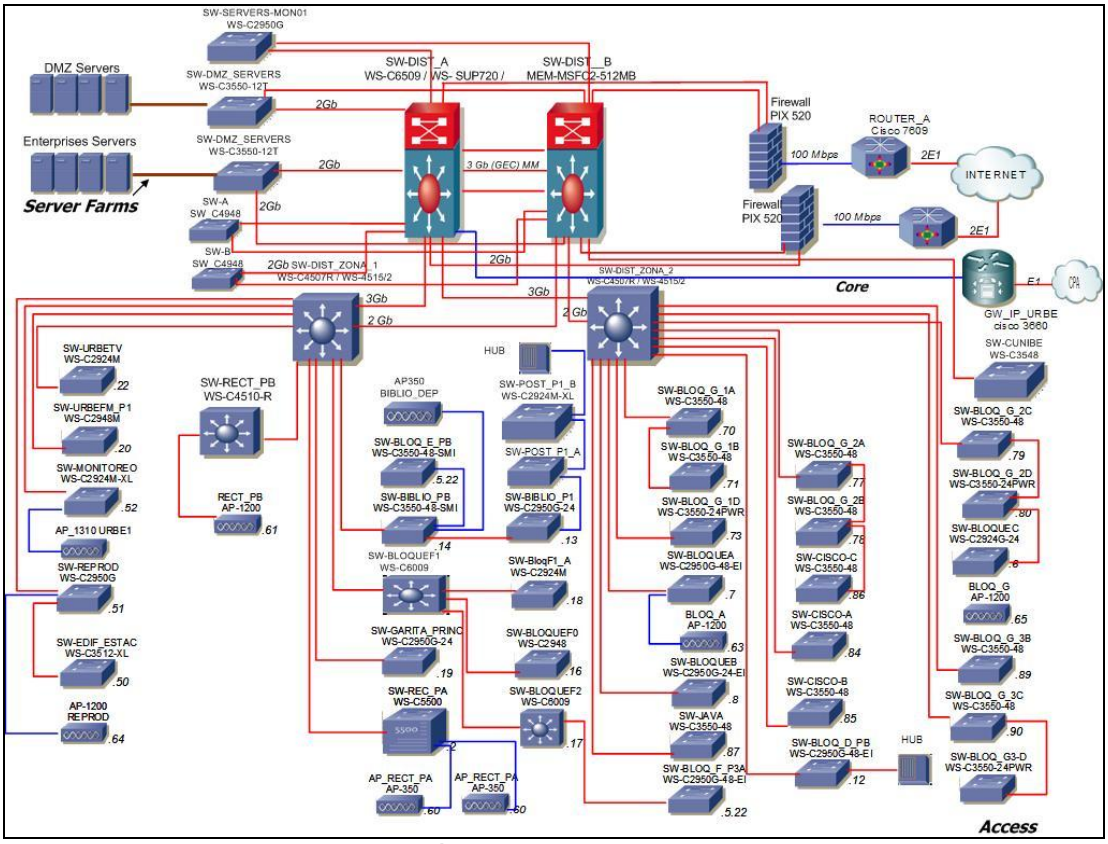

Figura 5. Diagrama esquemático de la red local utilizada para este estudio.

En cuanto al software se utilizó un analizador de tráfico llamado Analyzer Colasoft Capsa 6.4 Professional, la cual es una herramienta que permite realizar un seguimiento y análisis de protocolos, paquetes captura de trafico de un segmento de la red de área local, con la ventaja de capturar paquetes en tiempo real y analizar la data estadísticamente.

El desempeño de la red se caracterizó utilizando los siguientes parámetros:

- Cantidad de Tráfico: cantidad de información promedio que se transfiere a través del canal de comunicación,

- Tasa de Transferencia: velocidad de transmisión que pasa por una línea de telecomunicación.

- Porcentaje de Utilización: relación entre de tráfico medido al tráfico máximo que el puerto puede administrar.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

RESULTADOS Y ANÁLISIS

En la Figura 6 se puede observar la cantidad de bytes o de tráfico que se generó en la red durante los 7 días de mediciones.

Para el segundo día de la prueba la cantidad de información que se transmitió revela que hubo un aumento considerable de la data, ya que un análisis realizado dejar ver que ese día 4 usuarios en diferentes horas realizaron bajadas de archivos en grandes cantidades que requerían para realizar instalaciones; también se pudo evidenciar que el resto de los días de las pruebas el trafico se mantuvo similar en cuanto a la cantidad.

Para los días de las pruebas todos los usuarios de los departamentos involucrados en el estudio estuvieron conectados en sus equipos realizando sus labores diarias en cuanto a conexiones a las diferentes aplicaciones que allí se utilizan, tal como los sistemas administrativos, acceso a Internet, acceso a los servidores donde se imparten clases de Estudios a Distancia y la telefonía IP.

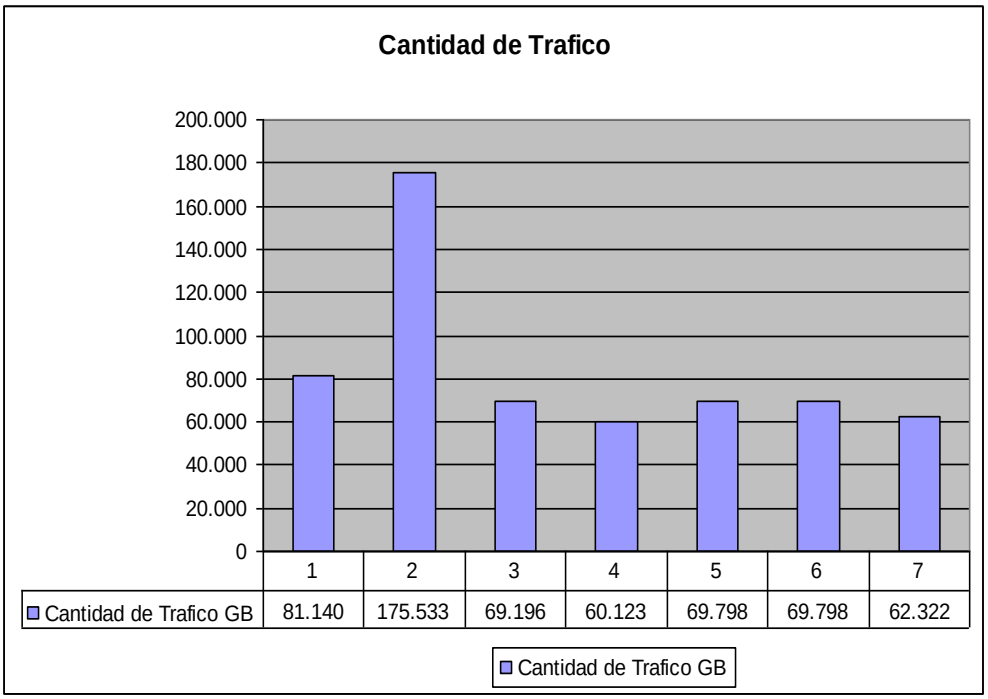

Figura 6. Cantidad de tráfico en GB para un monitoreo efectivo de 7 días

La Figura 7 muestra la tasa de transferencia o velocidad medida en Mbps, en la que se observa que en el segundo día de la prueba el incremento de la velocidad aumentó debido a la cantidad de archivos que fueron bajados por los usuarios, lo que incrementó la transferencia con respecto al resto.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

De igual forma, en los últimos 4 días de las pruebas, la velocidad se mantuvo constante, ya que no hubo alguna variación en cuanto a los accesos a los sistemas, eso se puede interpretar de manera similar a lo analizado en el figura 6, en donde se corroboró que era debido a la cantidad de archivos que bajaron de la Internet y cuyo tamaño era demasiado grande.

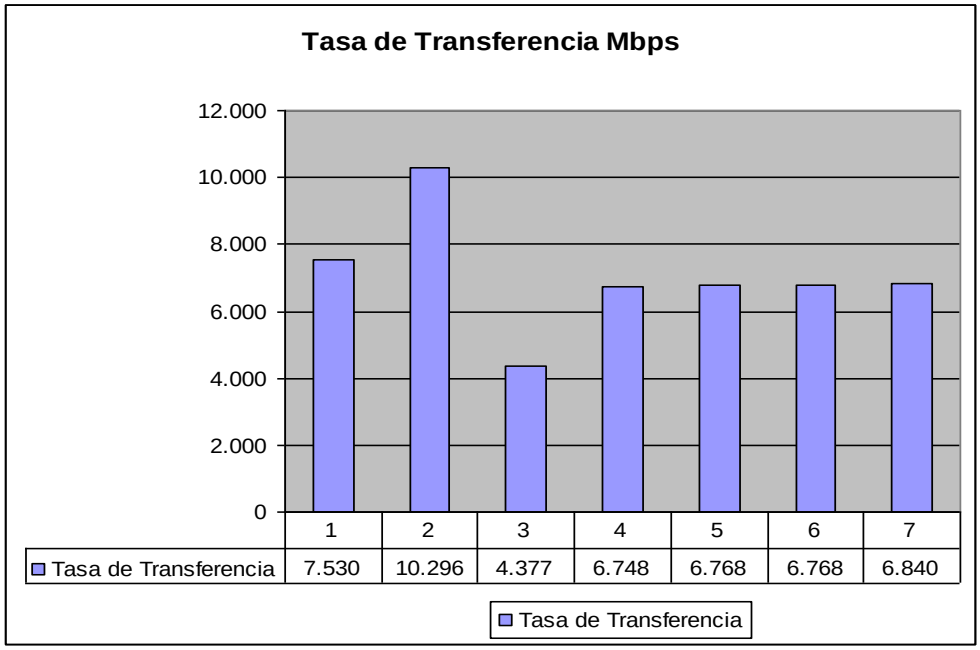

Figura 7. Tasa de transferencia en Mbps para un monitoreo efectivo de 7 días

En la Figura 8, puede observarse el porcentaje de utilización. Este porcentaje muestra como la curva se encuentra por debajo del máximo recomendado de 35% de utilización

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

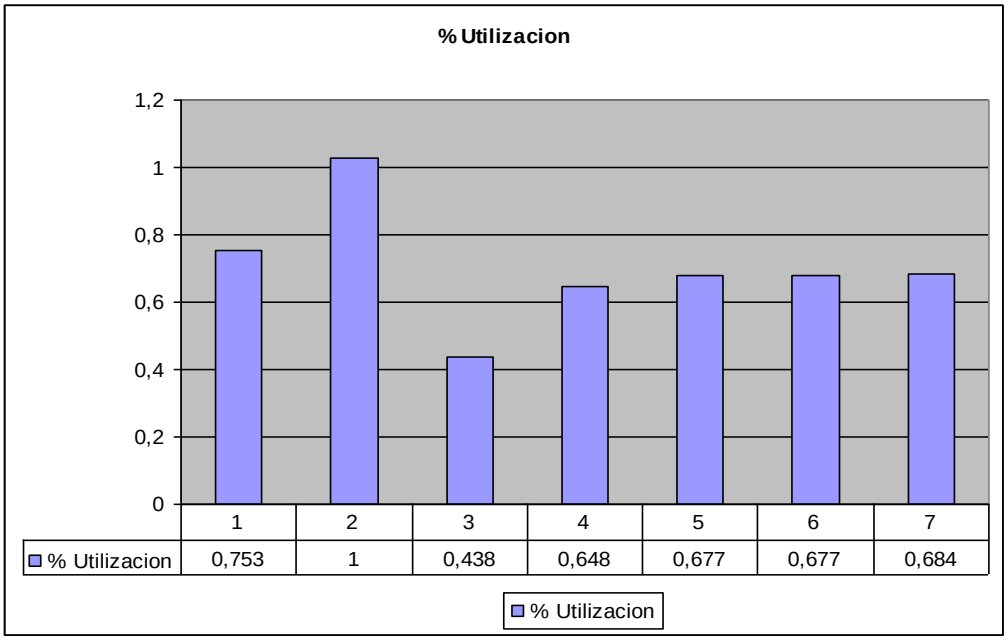

Figura 8. Porcentaje de utilización para 7 días de monitoreo

Esto quiere decir que un porcentaje de utilización que se encuentre por encima del 35% es un indicador de que la red puede comenzar a tener algún tipo de impacto negativo en los tiempos de respuestas para algunos tipos de aplicaciones. Así, el porcentaje de utilización de la Red es la proporción de tráfico de red corriente al tráfico máximo que el puerto pueda manejar. Esto indica el uso del ancho de banda. En este sentido, una tasa de transferencia por encima del 35%, pronostica el inicio de problemas potenciales. También es importante destacar que la utilización del 35% es casi óptima, pero algunas redes experimentan tasas más altas o más bajas debido a factores como el tamaño del paquete y la desviación de los picos de carga.

Es importante observar que el incremento de las colisiones es a menudo el resultado de demasiados usuarios o demasiado tráfico en la red, lo que produce mucha disputa por el ancho de banda de la red. Esto puede disminuir las prestaciones de la red desde el punto de vista de los usuarios. La segmentación, que consiste en la división de la red en segmentos diferentes, unidos lógicamente mediante switch o routers, reduce la congestión en una red saturada.

CONCLUSIONES

Luego de haber realizado el estudio con su respectivo análisis, se identificaron los problemas actuales en la red objeto de estudio. Los datos obtenidos en el instrumento de recolección de datos permitieron llegar a las siguientes conclusiones:

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

Se evidenció que la red es optima debido a que el porcentaje de utilización no supera el 35%, lo que significa que la red no presenta ningún tipo de problema potencial que pudiese afectar el tráfico, por lo tanto es una red estable, es decir se mantiene operativa, independientemente de la cantidad de usuarios conectado a la misma.

De igual forma, el porcentaje de utilización evidenciado, permitió conocer gracias al software colapsoft capsa, la data diaria donde se calculó el uso que los usuarios le daban al ancho de banda cuando accesaban a sus diferentes sistemas y por lo tanto visualizar el comportamiento de la red durante los días que se realizaron las pruebas.

Quedó demostrado que la topología de la red cuenta con un diseño originalmente tomado del modelo de tres capas, dividiendo la infraestructura en núcleo (Equipos principales), distribución (Nodos Principales) y de acceso (switch de usuarios). Físicamente se encuentra estructurada en una estrella extendida donde los core cumplen las funciones de nodos centrales.

Lógicamente, su topología es en bus o Ethernet siendo micro segmentado los dominios de colisión por los conmutadores a una sola máquina en la mayoría de los casos. Esta arquitectura de red permite mantener operativo los sistemas con los que cuenta la organización.

Se concluye que el monitoreo continuo del tráfico de datos permite realizar una evaluación apropiada del comportamiento de la red en tiempo real. Entre los parámetros recomendados para evaluar están la cantidad de tráfico, la tasa de transmisión y el porcentaje de utilización. En particular, la medición del tráfico en una red LAN, por medio de algún software especializado (por ej. Colapsoft Capsa), es una metodología fácil de implementar.

Finalmente, se recomienda realizar un rediseño para convertir la red de comunicación de una capa 2, que es el modelo actual, a una de capa 3 entre distribución y acceso. Esto haría posible que el tráfico de broadcast generado en un área o segmento de la red pueda reducirse, permitiendo que solo la información solicitada sea enrutado hacia el destino.

Igualmente, la aplicación de políticas de calidad de servicio o de clasificación del tráfico, permitirán dar prioridad a la data sensible sobre la que podría soportar pérdidas y retransmisiones.

REFERENCIAS BIBLIOGRÁFICAS

Colasoft Capsa. Technical White Paper. //www.colasoft.com/download/capsa-6.x-whitepaper.pdf

The OSI model: Understanding the Seven Layers of Computers Networks. 2006. //www.rgtechnologies.net/downloads/whitepapers/OSIModel.pdf

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009

Michael Welzl, (2005) **Network Congestion Control**, Wiley & Sons, England

P. Barford and D. Plonka, "Characteristics of network traffic flow anomalies", in *Proceedings of ACM SIGCOMM Internet Measurement Workshop*, San Francisco, CA, Noviembre 2001.

J. Wahle 1, L. Neubert, M. Schreckenberg, Modeling and simulation of traffic flow, Computer Physics Communications, **121-122**, 402, 1999

Martin P. Clark, Networks and Telecommunications, Wiley & Soons, 2nd Edition, New York. 1998.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 2 – Año 2009