Sistema de Monitoreo de Tráfico WAN

Ing. Juan E. Caillava[1], Ing. Miguel A. Canal Martínez[1]

[1] Universidad Nacional de Tucumán, Facultad de Ciencias Exactas y Tecnología,
Carrera de Ingeniería en Computación,
Trabajo Final de Carrera.

Abstracto. En la actualidad, el costo afrontado por las empresas para mantener enlaces dedicados de área extendida, ubica a los mismos como recursos escasos y valiosos dentro de toda organización. La criticidad de estos enlaces juega un rol vital si se tiene en cuenta que generalmente dan soporte a diferentes procesos de negocios, principalmente en aquellas organizaciones distribuidas geográficamente. El siguiente proyecto aborda la problemática que a menudo enfrentan los administradores de red de conocer en todo momento el tráfico por estos enlaces, a los efectos de controlar su uso y monitorear su rendimiento. Para ello, se diseña un sistema de software que lleva a cabo diferentes análisis de tráfico, ofreciendo sus resultados en forma comprensible, permitiendo de ese modo tomar acciones apropiadas, basadas en hechos reales y no en supuestos. El sistema fue implementado en una empresa real y cuenta con la generalidad suficiente para ser adaptado e instalado en cualquier empresa o institución que utilice redes de datos.

1 Introducción

El objetivo de este proyecto es lograr una herramienta que sirva a los administradores de red para conocer la naturaleza del tráfico en los enlaces WAN, permitiéndoles de este modo controlar su uso y monitorear su rendimiento con el fin de planificar su capacidad y detectar posibles irregularidades en la prestación del servicio. Este tipo de enlace corresponde generalmente a una conexión a Internet o a una conexión entre sucursales de la misma empresa.

El proyecto presentado a continuación trata sobre un sistema analizador de tráfico de red, compuesto por dos aplicaciones que conforman un sistema distribuido tipo cliente/servidor, cuya meta es realizar tal monitoreo de enlaces WAN.

La aplicación servidora analiza todo el tráfico de entrada y salida del enlace indicado, generando información disponible en una arquitectura orientada a servicios la cual puede ser accedida sólo por usuarios con credenciales.

La aplicación cliente brinda al usuario una interfaz gráfica que le permite, a través de una red de datos, tener acceso a la información generada por el servidor y que sirve para conocer el estado actual del enlace. Además, la aplicación cliente permite al usuario configurar el análisis de tráfico que se desea realizar.

2 Redes de Datos

2.1 Redes de Datos Empresariales

En la actualidad, la infraestructura de comunicaciones de datos que poseen la mayoría de las empresas e instituciones, está conformada por redes LAN, de alta velocidad, interconectadas entre sí por enlaces WAN. Este conjunto de redes está conectado a Internet por uno o más puntos de accesos. La figura 1, muestra en forma esquemática dicha infraestructura.

Las velocidades de los enlaces WAN, contratados a TELCO's para comunicaciones privadas o para el acceso a Internet, son muy inferiores a las utilizadas en las redes LAN (decenas e incluso centenas de veces inferiores). Por otra parte, el costo de dichos enlaces es bastante oneroso, en particular cuando cubren grandes distancias. Por este motivo, las empresas encuentran en sus enlaces WAN recursos muy valiosos que deben aprovecharse al máximo, evitando todo tipo de tráfico espurio que no esté alineado con el perfil del negocio de la compañía.

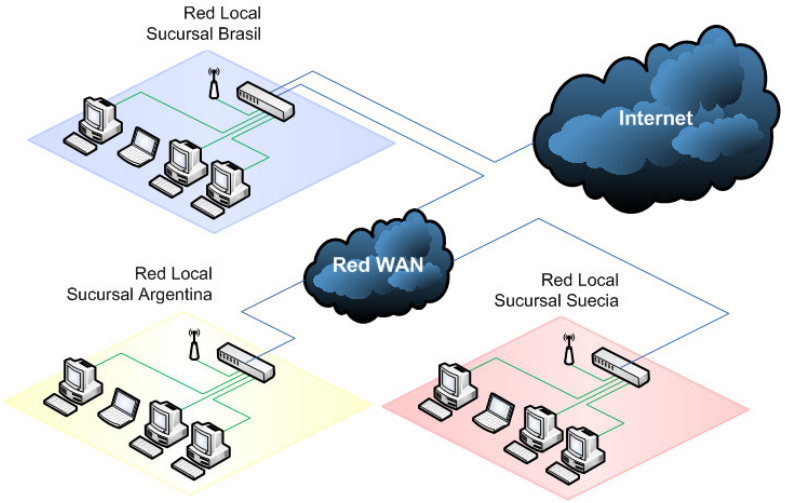

Fig. 1. Redes LAN interconectadas por una red WAN.

2.2 Objetivos del Análisis del Tipo de Tráfico WAN

Al ser los enlaces WAN recursos costosos y escasos dentro de la estructura de comunicaciones de una empresa, analizar el tipo de tráfico brinda a los administradores de la red las siguientes posibilidades:

Mejorar las políticas internas de seguridad informática. Un análisis del tráfico de red permite conocer las aplicaciones y protocolos de red que están utilizando los usuarios en un determinado momento. Incluso es posible detectar el tráfico de *streaming* de audio o video.

En base a este análisis, los administradores de red pueden mejorar la implementación de políticas de seguridad y filtrar el tráfico no deseado mediante el uso de sistemas especializados, como por ejemplo con el uso de servidores *proxy*.

Detectar computadoras y dispositivos con comportamiento errático. Es posible que una computadora u otro dispositivo conectado a la red de la organización sufra algún tipo de desperfecto físico o lógico que provoque un mal-comportamiento del mismo. Estas fallas, bastante difíciles de detectar, pueden ocasionar la generación de tráfico sostenido sobre los enlaces WAN. Ejemplos típicos incluyen virus informáticos, configuración inapropiada o *bugs* en *drivers* de dispositivo de comunicación, o fallas en la configuración de sistemas y protocolos de comunicación.

Si se analiza constantemente un enlace de comunicación, es posible detectar patrones de tráfico y tomar acciones inmediatas que contrarresten estos fenómenos de alto consumo de ancho de banda.

Evaluar la capacidad del enlace de comunicación. Una tarea usual para los administradores de red es determinar si la capacidad del enlace de comunicación es adecuada. Conocer en todo momento el consumo global de ancho de banda permite saber a-priori si es necesario contratar un mayor ancho de banda con la prestataria de servicio. También puede resultar de gran utilidad saber el consumo promedio por computadora, permitiendo detectar usuarios que se encuentren haciendo un uso abusivo del enlace.

Mediante este mismo análisis, es posible detectar irregularidades en el servicio ofrecido por el prestador y así evaluar si el proveedor del enlace cumple o no con los términos del contrato.

Discriminar tráfico por usuarios y unidades departamentales. Si la organización mantiene una base de datos sobre los responsables de los dispositivos conectados a la red, con el análisis discrecional del tráfico es posible identificar en tiempo real los usuarios que están haciendo uso del enlace. También es deseable almacenar un histórico de consumos de ancho de banda y conocer los patrones de utilización del mismo. En consecuencia, surge la posibilidad de discriminar la utilización del enlace según unidades departamentales, lo cual resulta útil si la empresa decide implementar un sistema de facturación interna o de centros de costos.

Discriminar tráfico de Internet e intranet. Si el enlace de comunicaciones es compartido entre *Internet* e *Intranet*, examinando la información transferida es posible distinguir entre estos dos tipos de tráfico, pudiendo evaluar en qué medida se emplea el enlace para traficar datos dentro de la misma empresa, lo cual podría significar información relevante a la hora de tomar una decisión estratégica. Por ejemplo, si una empresa detecta que el uso del enlace es principalmente para Internet, una posible decisión sería contratar un proveedor local para cada sucursal para acceder a Internet y utilizar los enlaces WAN solamente para tráfico privado de datos de la red.

Determinar patrones de utilización del enlace. Mediante un análisis de tráfico sostenido en el tiempo, se puede construir una línea base (*baseline*) y así detectar intervalos del día donde la utilización del enlace alcanza valores mayores pudiendo inferir si la capacidad del mismo se encuentra cerca de la saturación y hacer las provisiones del caso.

Así mismo, otro análisis útil, puede incluir las aplicaciones, sitios webs y datos transferidos por cada dispositivo conectado a la red LAN y evaluar consumos (en kbps) por usuarios o servidores durante el transcurso de un rango de tiempo establecido (día, semana, mes, etc.). De este modo, se obtiene una idea cabal de la forma en que los usuarios utilizan el enlace alineados con los objetivos de la empresa o con fines personales (ocio, recreación, sociales, etc.).

El trabajo realizado cumple todos estos objetivos y además posee las siguientes características:

- Emisión automática de alarmas ante la presencia de anomalías en el enlace.
- Elaboración de un ranking de dispositivos con mayor consumo de ancho de banda, tanto en tiempo real como en intervalos de tiempo especificados por el usuario.
- Elaboración de un ranking de los sitios de *Internet* más visitados por los usuarios de la organización.
- Integración con la base de datos de empleados de la organización, a los efectos de conocer los responsables por cada dispositivo y/o unidad departamental.
- Búsqueda de dispositivos en base a diversos tipos de entradas, como ser dirección IP, nombre de *host*, nombre y apellido de la persona responsable, etc.

3 Monitoreo de Tráfico

El trabajo desarrollado hace uso de técnicas de monitoreo de tráfico de modo tal de poder acceder a todos los paquetes de datos que atraviesan un enlace WAN. En la actualidad, las herramientas más utilizadas para lograr este objetivo son *gateways*, servidores *proxy* y los *sniffers* de red. La técnica de *sniffing* presenta una serie de ventajas que se darán a conocer a lo largo de este trabajo, razón por la cual fue adoptada para la implementación del proyecto.

3.1 Sniffing

Las comunicaciones en las redes de datos se realizan intercambiando pequeñas porciones de información denominados paquetes. La información de control contenida en dichos paquetes (direccionamiento, control de errores y de flujo, etc.) es particular de cada tipo de protocolo utilizado en las distintas capas de abstracción en las que se divide una arquitectura de comunicación de computadoras. Esta información de control, adicionada a los datos reales a transmitir, constituye una sobrecarga u *overhead* en la comunicación.

Un analizador de tráfico de red es un *software* que captura todos los paquetes que circulan por un segmento de red y analiza diferentes aspectos de las comunicaciones, según criterios especificados por el usuario de estas aplicaciones. Este tipo de programas está basado en lo que se conoce como un *sniffer*, o más precisamente un *sniffer* de paquetes, que se define como una pieza de *software* o *hardware* que se conecta a una red de computadoras y es capaz de acceder a todo el tráfico que pasa por la misma.

El concepto del *sniffer* de paquetes puede ser comparado, en términos cotidianos, con los dispositivos que se utilizan para intervenir llamadas telefónicas, teóricamente sin afectar la comunicación en curso. Para continuar con esta analogía, estos dispositivos de intervención telefónica no tienen utilidad si no existe una persona o computadora capaz de analizar lo que por ellos fluye. De igual manera, un *sniffer* de paquetes de red por sí mismo no tiene utilidad si no existe un *software* adicional que sea capaz de analizar el contenido de los paquetes de información que viajan por la red a la que están conectados.

Generalmente los productos de *software* están conformados por ambas piezas, un *sniffer* de paquetes y un analizador de tráfico o protocolos.

En la actualidad, las redes LAN están basadas en tecnología conmutada (*Switched Ethernet*), en la cual no es posible utilizar un *sniffer* de paquetes de manera tan sencilla como se lo hace en las de medio compartido (*Shared Ethernet*), puesto que cada computadora conectada a la red sólo recibe aquellos paquetes que realmente estén destinados a ella, es decir, aquellos cuya dirección física destino (MAC *Address*) coincida con la de su interfaz de red.

En el mercado pueden encontrarse diversos paquetes de *software* que poseen las características de un *sniffer*, como ser: Wireshark, TCPDump, Cain and Abel, Ettercap, etc.

Puerto Espejo. Aunque en las redes LAN conmutadas no es posible utilizar un *sniffer* de manera directa, existen soluciones que nos permiten analizar el tráfico de distintas porciones de la misma cuando así se lo requiera.

El puerto espejo, conocido comúnmente como *Port Mirroring*, es una característica que poseen los *switches* administrables de media y alta gama de la mayoría de los fabricantes actuales. Esta característica permite designar uno o más puertos de un *switch* como destinatarios (puerto destino) de todos los paquetes originados o destinados a otro puerto (puerto origen) del mismo *switch*. En términos generales, estos dispositivos replican el tráfico de los puertos seleccionados como origen en aquellos puertos seleccionados como destino. La figura 2 muestra el uso de un puerto espejo en un *switch* Ethernet con la correspondiente captura de paquetes de dos puertos de acceso.

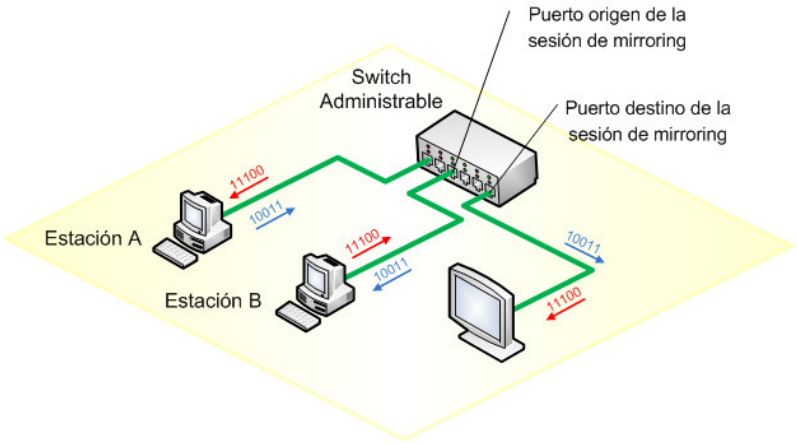

Fig. 2. Esquema de utilización de un *switch* con soporte para puerto espejo.

Para analizar el tráfico de una red mediante la utilización de esta característica, es importante conocer en detalle la topología de la red y de esta manera, planificar la captura de paquetes mediante estos puertos para obtener los resultados esperados.

Como ejemplo de *switches* que soportan esta característica, podemos mencionar los siguientes productos: D-Link DES-3852, Cisco Catalyst 3750 Series.

4 Captura de Paquetes

La captura de paquetes es la acción de recolectar esos paquetes a medida que viajan a través de la red. Los sniffers, explicados anteriormente, son los mejores ejemplos de estos sistemas de captura.

Un esquema general del proceso de captura y análisis de paquetes llevado a cabo en una aplicación, se ilustra en la figura 3 y puede resumirse de la siguiente manera:

1. Se inicializa la interfaz de red elegida para la captura, especificando la utilización del modo **promiscuo**, es decir, que se desea recibir no sólo aquellos paquetes dirigidos a la propia estación, sino todos los visibles.
2. Se aplican los filtros deseados, de tal manera de recibir sólo los paquetes de importancia para el proceso.

3. Se ingresa en un bucle indefinido, en el cual la librería de captura llama a una función bloqueante denominada generalmente *callback*, enviándole cada paquete capturado. Dicha función realiza las tareas de procesamiento o análisis consideradas de importancia por el usuario del sistema sobre cada paquete que se recibe y sólo puede tener una instancia por vez, de ahí que es bloqueante.
4. Finalmente, cuando se interrumpe el bucle mediante una función de la librería de captura desde un hilo de ejecución diferente, la interfaz de red seleccionada debe ser debidamente cerrada.

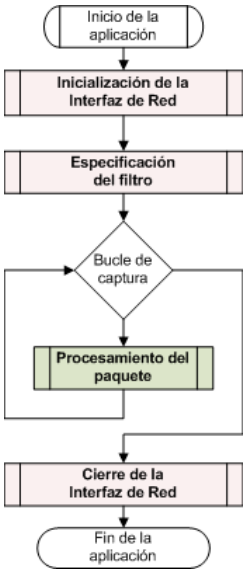

Fig. 3. Diagrama de flujo de un proceso de captura y análisis general.

5 Requerimientos de Software

Luego de analizar los objetivos planteados en la segunda sección de este documento, acerca de la importancia de monitorear el tráfico WAN en redes de datos empresariales, salen a la luz las principales necesidades de monitoreo de enlaces WAN. Cabe destacar que el proyecto se enfoca en el monitoreo de un único enlace WAN, previamente identificado, aunque los mismos principios rigen el monitoreo simultáneo de múltiples enlaces. Los requerimientos de monitoreo que se tienen en cuenta son brevemente enunciados a continuación:

5.1 Requisitos de Tiempo Real

- Determinación del ancho de banda global, tanto de subida como de bajada.
- Determinación del ancho banda consumido por cada computadora de la organización.
- Determinación del ancho de banda promedio consumido por cada computadora de la red LAN.
- Determinación del ancho banda consumido por cada unidad departamental de la organización.
- Discriminación del tráfico correspondiente a *Internet* del tráfico *intranet*.
- Determinación de los protocolos/aplicaciones que hacen uso del enlace y su correspondiente consumo de ancho de banda. Este requisito se aplica tanto a nivel global como a nivel de usuario y a nivel de unidad departamental.
- Emisión automática de alarmas (*e-mails*) ante la presencia de cierto tipo de anomalías en el enlace.
- Detección de tráfico de Internet correspondiente a *streaming* sobre proxy, ya que es la forma más común en que los usuarios pueden acceder a este tipo de servicio (por ejemplo: YouTube, radios on-line, etc).

5.2 Requisitos de funcionalidades bajo demanda

- Integración con la base de datos del personal a los efectos de poder distinguir, en todo momento, el ancho de banda consumido por usuario y por unidad departamental.

- Búsqueda de dispositivos de red en base a diversos tipos de criterios, a saber: nombre de *host*, usuario, departamento organizacional al que perteneces, etc.
- Medición automática de la capacidad del enlace.
- Mantenimiento de un histórico de consumo de datos por cada computadora de la organización.
- Mantenimiento de un histórico de sitios web visitados.
- Posibilidad de acceso remoto al sistema analizador de tráfico.

En la tercera sección de este documento se enuncian los tipos de técnicas que podrían emplearse para conocer los datos que circulan a través de un enlace WAN y así obtener la información necesaria que permite satisfacer los requerimientos definidos.

Si bien existen diversas herramientas de software y/o hardware que utilizan como principio de funcionamiento un *gateway*, permitiendo naturalmente discriminar el tráfico, medir las velocidades utilizadas por cada estación de trabajo de la red LAN y hasta administrar el ancho de banda utilizado por ellas, se trata de una solución activa e intrusiva. Esta característica significa que la herramienta puede influir de manera directa en el comportamiento del enlace WAN y presenta una serie de desventajas que la descartan como posible solución:

Punto único de falla. En caso de algún desperfecto físico (*hardware*) o de configuración (*software*), podría dejarse a la red LAN sin comunicación externa.

Administración y mantenimiento. La instalación de un sistema de este tipo implica un elemento adicional de administración y mantenimiento, que exige en cualquier caso que el personal de infraestructura sea adecuadamente capacitado y disponga del tiempo necesario para ocuparse de la nueva herramienta.

Costo de licencias. Si bien existen en el mercado herramientas de uso libre, las empresas deben seguir lineamientos generales y utilizar herramientas previamente analizadas y certificadas por su organización a nivel mundial. Además, es de importancia contar con una herramienta cuyo soporte esté garantizado por el fabricante.

Hardware adicional. Al ser una solución activa, requiere que el hardware empleado para su funcionamiento posea características de alto rendimiento y que además posean elementos que brinden tolerancias a fallas en todos los aspectos posibles, (alimentación eléctrica, memoria, procesadores, almacenamiento, interfaces de comunicación, etc.) con el objeto de no interrumpir las comunicaciones. Todo esto determina una importante inversión en *hardware*, que impacta en el presupuesto de las empresas.

5.3 Técnica de Monitoreo Seleccionada.

Luego de exponer las desventajas que presentan las herramientas, cuyo funcionamiento se basan en puertas de enlaces, se decide buscar una solución pasiva cuyo funcionamiento no interfiera con la utilización normal del enlace WAN, de manera que las desventajas mencionadas no se presenten o estén atenuadas. Es importante destacar que una solución pasiva no puede limitar el ancho de banda consumido por las estaciones de trabajo de la red LAN, pero puede servir para tomar decisiones de control y tomar acciones activas sobre el tráfico mediante otros medios, en los casos en que se requieran.

Cualquier solución pasiva, basada en analizadores de tráficos aplicados dentro de una red LAN de nivel empresarial con topología de red conmutada, requiere la utilización de la característica especial de **puerto espejo**, detallada en la sección 3 de este informe, la cual es una característica soportada por la mayoría de los *switches* administrables de media y alta gama.

5.4 Análisis de Mercado.

Como la solución propuesta es emplear un analizador de tráfico conectado a un puerto monitor del *switch* principal de la organización, de manera tal que refleje toda la información transmitida por el enlace WAN, se realiza un análisis de las herramientas disponibles en el mercado a los efectos de determinar cuál es la mejor alternativa para cubrir los requisitos planteados.

Si bien en el mercado existen numerosas aplicaciones que hacen análisis de tráfico, es prácticamente evidente la necesidad de construir un *software* a medida, por la particularidad de los siguientes requerimientos:

Integración con la base de datos del personal. Este requisito no es cubierto por ninguna herramienta evaluada debido a la necesidad de realizar consultas particulares a dicha base de datos, todo esto en tiempo real.

Discriminación del tráfico correspondiente a Internet del tráfico intranet. Para cubrir esta necesidad, se requiere definir el rango de direcciones IP públicas que forman parte de la *intranet* de la empresa, lo cual no es admisible por ninguna de las herramientas tenidas en cuenta.

Mantener un histórico del consumo de datos de cada computadora de la organización y de los sitios web visitados. Para ello es necesario realizar un análisis de tráfico particular y trabajar en conjunto con una base de datos, lo cual no realiza ninguna de las herramientas evaluadas.

Emisión automática de alarmas (*e-mails*) ante la presencia de cierto tipo de anomalías en el enlace. Cada organización es única y sus indicadores de performance no son necesariamente generales. Toda empresa debe definir los indicadores que desea monitorear y los rangos de valores dentro de los cuales estos indicadores denotan anomalías, con el propósito de emitir alertas.

La evaluación realizada de los analizadores de tráfico más populares dentro del mercado, no hace más que confirmar la hipótesis de construir un software a medida.

Como se menciona en la introducción de este informe, el producto de *software* realizado consta de dos aplicaciones que conforman un sistema distribuido tipo cliente/servidor, en donde el servidor captura y analiza el tráfico, mientras que el cliente, entre otras cosas, presenta los resultados del análisis al usuario.

Los analizadores de paquetes considerados en el análisis son:

Wireshark: http://www.wireshark.org/
Ntop: http://www.ntop.org/
Solarwinds: http://www.solarwinds.com/

6 Diseño del Servidor

A continuación se exponen las bases del diseño de la aplicación servidora. Los puntos más importantes son analizados en profundidad, mostrando gráficamente el comportamiento de ciertas partes del software.

6.1 Filtrado de Paquetes de Datos

Una vez llevada a cabo la conexión de componentes del sistema tal como muestra la figura 4, la aplicación servidora captura todo el tráfico entrante y saliente de la organización.

Debido a las características de los diferentes análisis de tráfico que se requieren realizar, surge la necesidad de capturar sólo aquellos paquetes que entran o salen de la red LAN y que además posean cabecera IP.

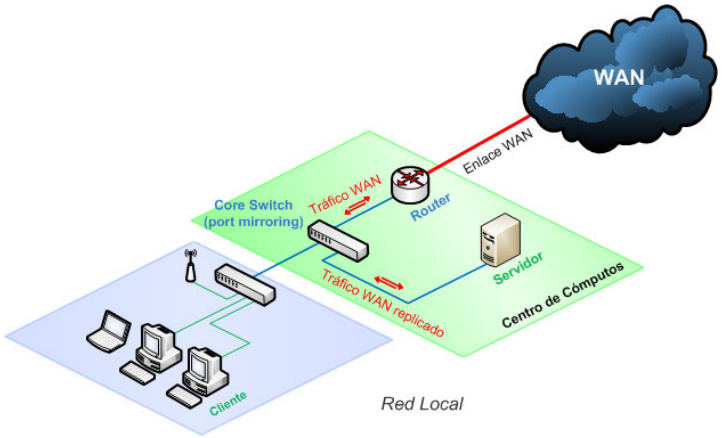

Fig. 4. Diagrama de conexión. *Port mirroring*.

En función de esto, la aplicación servidora establece dos filtros para la captura de paquetes:

- Se capturan sólo aquellos paquetes cuya dirección MAC origen o destino coincida con la dirección MAC de la interfaz de red del *router* que da acceso a la red WAN.
- Se capturan sólo aquellos paquetes que posean cabecera IP.

Con estos dos filtros, se descartan por ejemplo los paquetes de *broadcast*[1] (porque la dirección MAC destino de este tipo de paquetes no coincide con la dirección MAC de la interfaz del *router*) y los paquetes ARP[2] (porque este tipo de paquetes no tiene cabecera IP).

6.2 Almacenamiento Temporal

Estructura *Packet*. Cada paquete provisto por las funciones de las diferentes librerías que pueden utilizarse para la captura de tráfico de red está representado por estructuras de datos que varían según la librería. Al mismo tiempo, sea cual fuere la estructura representativa de un paquete, ésta tiene información completa acerca de todas las cabeceras de protocolos[3] que encapsulan los datos de nivel de aplicación, mientras que los análisis realizados por la aplicación servidora sólo requieren una parte de cada una de ellas.

Por las razones expuestas, es necesario que la aplicación servidora defina una estructura *Packet* particular que represente los datos de importancia para los análisis que realiza y que permita independizar el diseño de la librería de captura utilizada.

Cada vez que se obtiene un paquete provisto por la librería de captura, se extrae la información correspondiente y se crea un nuevo paquete de estructura propia.

Estructura FIFO. Los diferentes análisis que realiza la aplicación servidora bajo demanda, necesitan contar con un conjunto de paquetes capturados que representen el estado de la red en un intervalo temporal, determinado por la diferencia de tiempo de llegada del primero y el último de la muestra. Mantener el orden de llegada de los paquetes es necesario con el objeto de conocer de manera rápida el intervalo temporal que el conjunto representa.

La estructura de datos que posee estas características es conocida como cola del tipo FIFO (*First In First Out*). Este tipo de estructura mantiene el orden de sus elementos según vayan ingresando, permitiendo eliminar aquellos que lo hagan en primer lugar (elementos más viejos).

Como la mayoría de los análisis requieren diferenciar aquellos paquetes que pertenecen al tráfico que se dirige hacia afuera de la red LAN (denominado tráfico de subida), de aquellos que pertenecen al tráfico que se dirige hacia adentro de la misma (denominado tráfico de bajada), es necesario mantener dos

[1] *Broadcast* es la transmisión de un paquete que será recibido por todos los dispositivos en una red.
[2] ARP (*Address Resolution Protocol*) es un protocolo que permite traducir direcciones lógicas (por ejemplo IP) en direcciones físicas (por ejemplo MAC).
[3] Las cabeceras corresponden a los protocolos Ethernet, IP, TCP/UDP, HTTP, FTP, DNS, etc.

estructuras de características similares que permitan almacenar los paquetes correspondientes a cada caso. Denominamos a dichas estructuras: cola de subida y cola de bajada respectivamente.

Estructura *PacketQueue*. Para dar soporte a la funcionalidad de proveer un histórico del consumo de tráfico WAN por parte de cada computadora que forma parte de la red LAN, es necesario acumular el tamaño de cada paquete que proviene desde o se dirige hacia cada computadora de la red. El tamaño almacenado será la cantidad de bytes que posea el paquete en el medio de transmisión físico, es decir, incluyendo no sólo los datos de capa de aplicación, sino también los pertenecientes a todas las cabeceras que encapsulan el mismo (*overhead*).

Para llevar a cabo esta tarea, las colas utilizadas para almacenar los paquetes constituyen una estructura de datos especial que posee en su interior una tabla *hash*[4]. Dicha tabla se utiliza para acumular los tamaños de los paquetes correspondientes a cada computadora. Como clave de acceso a la tabla se utiliza la dirección IP de la computadora, información que puede obtener del paquete a almacenar. Si el paquete es de subida, entonces la dirección IP de la computadora local corresponde con la dirección IP origen del paquete, en cambio si el mismo es de bajada, la dirección IP destino es la utilizada.

El valor a almacenar en la tabla hash, accediendo a la misma con una dirección IP dada, es un acumulador que se incrementa cada vez que llega un paquete correspondiente a dicha IP.

Los valores acumulados de la tabla hash sólo son reiniciados (puestos a cero) cada vez que la información acumulada es transferida a una base de datos con tablas diseñadas para tal fin.

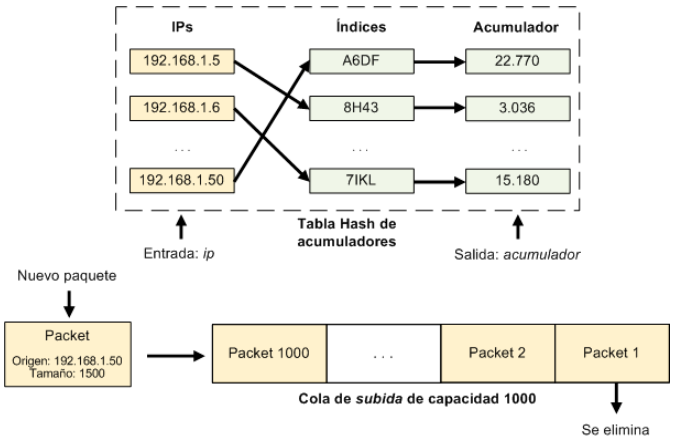

Fig. 5. Esquema de la estructura de datos especial PacketQueue.

La figura 5 proporciona un esquema de la estructura especial basada en una cola que se utiliza para el almacenamiento de los paquetes del tráfico de red de subida y de bajada.

Cada vez que llega un nuevo paquete a la cola de subida, se toma su dirección IP de origen, se accede a una tabla hash con dicho valor como clave y se incrementa el acumulador de datos almacenado en ella, utilizando como valor de suma el tamaño del nuevo paquete.

Antes de almacenar el paquete en la cola se procede a verificar si la misma tiene espacio disponible para un elemento más, eliminando el primero de la fila si la evaluación es negativa.

6.2.1 Proceso de Captura y Despacho.

El proceso de captura completo está constituido por cuatro etapas fundamentales: apertura de la interfaz, aplicación de filtros, despacho y almacenamiento de paquetes, y por último cierre de la interfaz.

Al iniciar la aplicación servidora, se debe realizar la inicialización de la interfaz de red mediante la cual se realiza la captura de paquetes, habilitando el modo promiscuo de la misma de tal manera que se puedan recibir no sólo paquetes dirigidos a la estación local, sino también aquellos que tienen como destino otras estaciones.

[4] Una tabla o mapa *hash* es una estructura de datos que asocia claves (*keys*) con valores (*values*). Su característica principal es que soporta de manera muy eficiente la recuperación de valores, a partir de sus claves asociadas.

Una vez que la interfaz de red se encuentra seleccionada y lista para iniciar el proceso, se establecen los filtros necesarios para evitar que el hilo de ejecución de captura de la aplicación reciba paquetes indeseados que no cumplan con los parámetros establecidos y que sólo constituyan un desperdicio de ciclos de procesador.

Luego, se inicia lo que se denomina **bucle de captura**, en el cual una función definida en la aplicación servidora, comúnmente denominada *callback*, es llamada por la librería de captura cada vez que llegue un paquete nuevo a la interfaz, enviándole el mismo como parámetro. Es importante destacar que la función *callback* no se ejecuta más de una vez al mismo tiempo, lo que significa que ante la llegada de un nuevo paquete, la librería de captura no la llama si no ha finalizado la ejecución correspondiente a la llamada previa.

La misión de la función *callback* definida en el servidor es la de llamar a un procedimiento despachador, encargado de convertir un paquete del tipo específico de la librería de captura en uno del tipo *Packet* como se detalló en la sección de almacenamiento temporal. Paso siguiente, la comparación de la dirección MAC del router que encamina hacia la WAN con las direcciones MAC destino y origen del paquete, determina si el mismo es de subida o de bajada. Cuando un paquete es de subida se lo agrega en la cola especial de subida, caso contrario, se lo agrega en la cola de bajada.

Este proceso se repite de manera indefinida en un hilo de ejecución independiente y de alta prioridad dentro de la aplicación servidora, que sólo se detiene si es interrumpido mediante la utilización de una función especial de la librería de captura, que debe ser llamada desde un hilo de ejecución diferente.

Es importante destacar la existencia de un *buffer* de bajo nivel, que permite acumular aquellos paquetes que ingresan por la interfaz de red y que no pueden ser enviados a la función *callback* por estar procesando un paquete anterior. Una vez liberada la función *callback*, los paquetes contenidos en el buffer son enviados de a uno a la función. En aquellos casos en los cuales la velocidad del tráfico de red es suficientemente elevada como para impedirle a la función *callback* procesar todos los paquetes del *buffer*, los nuevos paquetes son descartados y en consecuencia no son analizados.

Cabe destacar que la pérdida de paquetes aumenta con la velocidad del tráfico que se desea medir, y disminuye con la capacidad de procesamiento disponible en el *host* en donde se realice el análisis de paquetes. También en importante mencionar que el sistema presentado permite medir velocidades de tráfico de varias decenas de Mbps sin detectarse pérdida de paquetes en una computadora de gama media.

6.3 Análisis de Paquetes Previo al Despacho.

Algunos análisis que realiza la aplicación servidora deben efectuarse sobre todos y cada uno de los paquetes que se capturan, puesto que la información que los análisis determinan debe ser sobre el total del tráfico que fluye y no sobre muestras parciales de tráfico, como las representadas por las colas de subida y de bajada.

De esta manera, los procedimientos de análisis deben ser realizados previos al despacho real de los paquetes a la cola correspondiente y en consecuencia en el interior del hilo de ejecución de la función *callback*, llamada por la librería cada vez que captura un paquete.

El procedimiento de despacho realiza de manera secuencial los diferentes análisis llevados a cabo sobre un paquete, previo al despacho real del mismo a la cola de subida o de bajada, según corresponda.

Es importante destacar que el tiempo total empleado en los análisis secuenciales repercute de manera directa en la máxima velocidad de tráfico que la aplicación servidora es capaz de analizar, sin que haya pérdida de paquetes. En este caso, un análisis secuencial permite superar ampliamente (decenas de veces) la velocidad de tráfico esperada (10 mbps), con lo cual se descartan las implementaciones de ejecución de tareas en paralelo.

En la figura 6 se puede apreciar el diagrama de flujo del proceso de despacho y su conjunto secuencial de análisis previos.

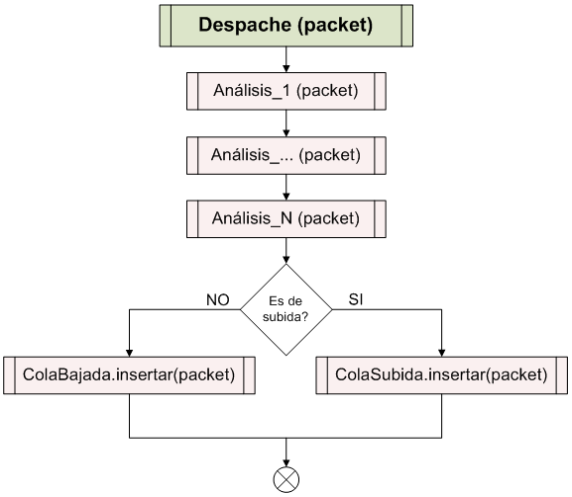

Fig. 6. Proceso de despacho.

Análisis de sitios visitados. Para poder detectar los sitios web visitados por las estaciones de trabajo de la red LAN, es necesario inspeccionar todos los paquetes que conforman el tráfico de subida en busca de aquellos cuyo protocolo de capa de aplicación sea HTTP y que a su vez posean una petición por un recurso remoto ubicado en un servidor web.

Cada vez que un paquete de estas características sea detectado, la aplicación verifica que el recurso solicitado corresponda con una página web. Esto se logra indicando a la aplicación servidora, mediante un archivo de configuraciones, qué tipo de recursos se deben tratar como tales (por ejemplo archivos con extensión .html, .htm, .asp, .jsp, .php, etc.). Además, un pedido HTTP a la raíz de un sitio web también es considerado un acceso a dicho sitio.

El paso siguiente es buscar, dentro de la cabecera HTTP del paquete observado, el *host* remoto al cual se está realizando la solicitud. La cabecera HTTP del paquete debería contener, además, un encabezado con la información del *host*, como por ejemplo: www.w3.org

La aplicación servidora mantiene una tabla hash con la información de los sitios visitados, la cual es almacenada en una base de datos de manera periódica y automática con el objeto de mantener un histórico de los sitios visitados para que los usuarios del sistema puedan acceder a esta información haciendo consultas a la base de datos, seleccionando para ello un intervalo de tiempo deseado. Además, esta operación de limpieza asegura que la tabla no crece indefinidamente, lo cual puede ocasionar problemas de ocupación de memoria principal en el servidor donde reside la aplicación analizadora de tráfico.

Análisis de streaming sobre HTTP. Para poder detectar la transferencia y utilización de *streaming* por parte de una estación de trabajo de la red LAN, es necesario inspeccionar todos y cada uno de los paquetes que conforman el tráfico de bajada, en busca de aquellos cuyo protocolo de capa de aplicación sea HTTP y que a su vez posean un tipo de contenido (*Type-Content*) que especifique que la descarga se trata de *streaming*.

Cuando se detecta un paquete de bajada con dichas características, es necesario mantener un registro de la dirección IP y el puerto TCP origen de la estación de trabajo cliente del *streaming*, con el objeto de identificar dicha conexión a lo largo de su tiempo de vida.

Es importante mencionar que los registros almacenados deben eliminarse cuando el *streaming* deje de formar parte del tráfico, es decir, cuando la conexión TCP sobre la cual fluye deje de existir entre los extremos.

La función que verifica este tipo de tráfico debe, en primer lugar, identificar si un paquete de bajada contiene un mensaje de respuesta HTTP, es decir que su primera línea posea las cadenas de texto “HTTP”, “200” (u otro código de operación exitosa) y “OK”. Luego, determina si la línea de cabecera de tipo de contenido (*Content-Type*) tiene un valor que coincide con los tipos conocidos de *streaming*, comparando dicho valor con una lista obtenida desde un archivo de configuración y que puede ser ampliada editándolo cada vez que se requiera.

Si las comprobaciones dan un resultado positivo, entonces se almacena en un arreglo (como el ilustrado en la figura 7) un nuevo elemento del tipo [IP:Puerto] formado por la dirección IP de la estación

cliente de *streaming*, dada por la dirección IP destino del paquete, y el puerto TCP origen de dicha estación.

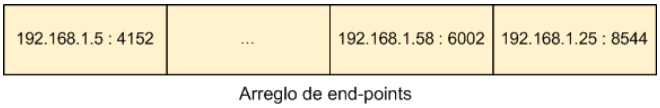

Fig. 7. Arreglo de *end-points* de *streaming*.

Este arreglo que registra parte de las conexiones que pertenecen a *streaming*, permite al método de análisis bajo demanda de velocidades por puerto de una estación de trabajo, revelar información correspondiente a la utilización de ancho de banda en *streaming* por parte de una estación de trabajo en particular.

6.4 *Análisis Bajo Demanda*

Algunos análisis que realiza la aplicación servidora sólo se efectúan bajo demanda, es decir, cada vez que un cliente solicita información acerca del estado actual de la red.

Todos estos análisis se realizan sobre una imagen o copia de las colas de paquetes en el momento en que se solicita el servicio, puesto que las mismas cambian constantemente con el ingreso de nuevos paquetes y la posible eliminación del más viejo de ellos. La única excepción es la medición del ancho de banda global, en cuyo caso no se analizan copias de las colas de paquetes sino que se consulta directamente a cada una de ellas (cola de subida o bajada).

Es importante destacar que todos los análisis bajo demanda se realizan en hilos de ejecución diferentes e independientes de aquel encargado de la obtención, análisis y almacenamiento de los paquetes, puesto que el proceso de captura no puede detenerse por un tiempo prolongado ante la solicitud de cada servicio sin provocar la pérdida de paquetes por parte de la librería de captura subyacente.

Medición del ancho de banda global. La medición del ancho de banda global se realiza mediante consultas directas a las colas de subida y de bajada que mantiene la aplicación. Cada vez que un cliente solicita este servicio, el servidor realiza una consulta a cada una de las colas, las cuales mantienen la siguiente información acerca de la muestra de tráfico que ellas mismas representan:

- **Acumulador de datos:** es la suma en bytes de todos los paquetes de datos alojados en la cola en un instante de tiempo. Cada vez que ingresa un paquete nuevo a la cola, el acumulador es incrementado con la cantidad de bytes que posee dicho paquete y a su vez se le resta la cantidad de bytes que posee el paquete que tuvo que descartarse para dar cabida al paquete que ingresó, en caso de que la cola se encuentre llena.
- **Tiempo de llegada del paquete más reciente:** corresponde con la marca de tiempo que posee el paquete más reciente de la cola. Dicha marca de tiempo es provista por la librería de captura al momento de capturar el paquete.

El ancho de banda actual, tanto de subida como de bajada, es determinado según el cociente entre el acumulador de datos y la diferencia de tiempo que existe entre el primer y último paquete de la cola. Al tratarse de una estructura FIFO, se tiene acceso directo al primer paquete que ingresa a la cola y por lo tanto es posible obtener la diferencia de tiempo entre dicho paquete y el más reciente de la cola. En la figura 8 se puede apreciar la información asociada a la cola de subida en un momento determinado. Es de importancia mencionar que el cálculo del ancho de banda se realiza independientemente de la cantidad de paquetes que se encuentren en la cola en un momento dado.

Cabe destacar que esta medición del ancho de banda corresponde con una muestra de tráfico mantenida por la aplicación, como lo son las colas de paquetes. Una vez obtenida la velocidad de subida y de bajada, se retorna a la aplicación cliente los resultados del proceso de medición, enviando una única respuesta que contiene ambas velocidades.

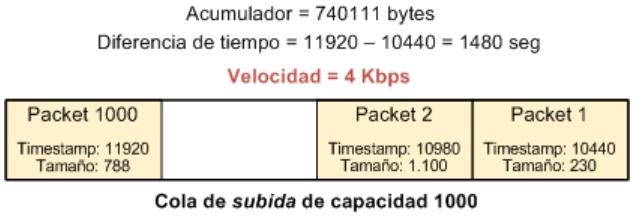

Fig. 8. Obtención de la velocidad global.

Medición de ancho de banda por estación de trabajo. La medición del ancho de banda utilizado por cada estación de trabajo se efectúa en dos hilos de ejecución independientes, cada uno de los cuales se encarga de analizar una imagen de las respectivas colas de subida y de bajada.

El procedimiento efectuado en cada hilo de ejecución es el de recorrer la imagen de la cola asignada, acumulando los tamaños de los paquetes que corresponden a las diferentes direcciones IP de las estaciones de trabajo de la red LAN que en ella se encuentran.

Dado que el primero y el último paquete de cada cola determinan el intervalo temporal que ellas representan, la utilización del ancho de banda o velocidad del tráfico de cada una de las estaciones encontradas en las colas, se obtiene dividiendo sus respectivos acumuladores en dicho intervalo.

En resumen, cada uno de estos hilos obtiene las direcciones IP de la estaciones de trabajo consultando la dirección IP destino de cada paquete si la cola es de bajada, y consultando la dirección IP origen de cada paquete si la cola es de subida.

Cada nueva dirección IP encontrada, crea un registro en una tabla, en donde se establece como valor correspondiente el tamaño del paquete que le da origen, y se acumulan los tamaños de los próximos paquetes que correspondan a dicha dirección IP, como muestra la figura 9.

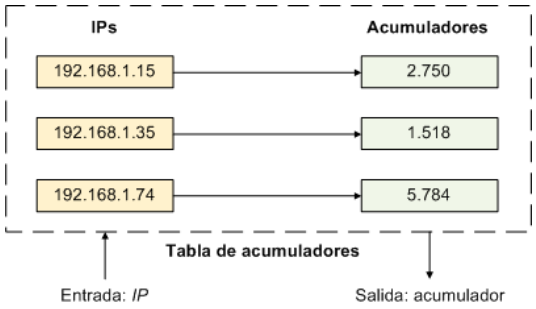

Fig. 9. Tabla de acumuladores por IP.

Al recorrer la cola completa, se procede al cálculo de los anchos de bandas, empleando el método descripto en los párrafos anteriores.

Una vez que se obtienen los anchos de bandas utilizados por cada estación de trabajo de cada cola, se procede a realizar una conjunción de los mismos, conformando una única respuesta con los valores de subida y de bajada para cada dirección IP encontrada.

Existen dos variantes más al análisis recién explicado. Uno de ellos constituye la medición del ancho de banda utilizado por un grupo de direcciones IP entregadas como parámetro por el cliente que solicita el servicio, y el restante es la medición para una única dirección IP también entregada como parámetro.

Ambos análisis se efectúan de la misma manera que el análisis para el total de las direcciones IP encontradas en la cola, pero en vez de considerarlas a todas ellas, sólo se registran los tamaños de los paquetes de las direcciones especificadas, dejando de lado o ignorando aquellas estaciones de trabajo que no se solicitan de manera explícita.

Medición de ancho de banda por protocolos/aplicaciones. La aplicación servidora debe determinar el ancho de banda consumido por cada protocolo de capa de aplicación, tanto a nivel global como a nivel de usuario (una única dirección IP) y a nivel de unidad departamental (un conjunto de direcciones IP). Dicha medición tiene en cuenta el tipo de puerto (TCP o UDP) y el número de puerto (origen o destino según corresponda) de todos los paquetes que atraviesan el enlace WAN de la empresa.

La medición del ancho de banda por protocolos se efectúa en dos hilos de ejecución independientes, cada uno de los cuales se encarga de analizar una imagen de las respectivas colas de subida y de bajada. El proceso de medición involucra cuatro tablas hash que permiten alojar los paquetes TCP de subida, TCP de bajada, UDP de subida y UDP de bajada. El procedimiento que efectúa cada hilo de ejecución es el de recorrer la imagen de la cola asignada (subida o bajada) acumulando los tamaños de los paquetes en la tabla correspondiente, según el paquete tenga cabecera TCP o UDP. Finalmente la velocidad de cada protocolo está determinada por los acumuladores obtenidos y la diferencia de tiempo entre el primer y el último paquete de cada cola. Si la medición solicitada por el cliente involucra una o más direcciones IP particulares, no se tienen en cuenta aquellos paquetes cuya dirección IP no corresponde a las indicadas.

Durante la medición también se verifica si un paquete corresponde a tráfico de *streaming* sobre proxy, con el propósito que los usuarios del sistema puedan identificar este tipo de tráfico y diferenciarlo del tráfico HTTP común.

Medición de ancho de banda por tipo de red. El tráfico de red que atraviesa el enlace WAN puede ser considerado como la suma o el aporte de dos tráficos pertenecientes a redes claramente diferentes. Una de ellas es *Intranet*, cuyo tráfico está compuesto por paquetes dirigidos a o provenientes de direcciones IP públicas o privadas que pertenecen a la compañía en términos globales, es decir, considerando todas las sucursales que conforman la misma en las diferentes áreas geográficas que puedan ocupar. La otra es *Internet*, cuyo tráfico está compuesto por paquetes dirigidos a/o provenientes de direcciones IP sólo públicas y que no pertenecen a la compañía.

La medición del ancho de banda empleado en cada uno de estos tráficos se efectúa en dos hilos de ejecución independientes, cada uno de los cuales se encarga de analizar una imagen de las respectivas colas de subida y de bajada.

El procedimiento que se efectúa en cada hilo de ejecución es el de recorrer la imagen de la cola asignada, acumulando los tamaños de los paquetes que corresponden a la red a la que pertenece cada uno de los paquetes analizados.

Dado que el primero y el último paquete de cada cola determinan el intervalo temporal que ellas representan, la utilización del ancho de banda o velocidad del tráfico de cada red se obtiene dividiendo sus respectivos acumuladores en dicho intervalo.

En resumen, un paquete es de *Internet* cuando la cola es de subida y la dirección destino del paquete no pertenecen a las redes de la compañía o cuando la cola es de bajada y la dirección origen del paquete no es de las redes de la compañía. En cualquier otro caso, el paquete es considerado de *Intranet*.

Es importante destacar que la utilización de un servidor *proxy* que emplee una dirección IP perteneciente a la compañía, requiere que todos los paquetes dirigidos a/o provenientes del mismo, sean considerados como parte del tráfico de *Internet*.

Una vez recorrida la cola completa, se puede proceder al cálculo de los anchos de banda empleando el método descripto.

Una vez que se obtienen los anchos de bandas utilizados por cada red en cada cola, se procede a realizar una conjunción de los mismos, conformando una única respuesta con los valores de subida y de bajada para cada red.

6.5 Monitoreo de KPI's.

Un KPI (*Key Performance Indicator*) es un indicador empleado para cuantificar el rendimiento de un proceso que es clave para la organización. Una de las características fundamentales de todo KPI es que debe ser medible.

La aplicación servidora posee una lista de indicadores de performance que debe monitorear con frecuencia. Cada uno de estos KPI posee una tolerancia (cantidad de mediciones anormales que se toleran antes de disparar una alarma) y una acción de alarma específica.

La tarea de monitoreo de KPI's se trata de un hilo que se ejecuta frecuentemente con un periodo definido por los administradores del sistema, el cual es por defecto de 1 minuto.

Ante la presencia, sostenida en el tiempo, de valores anormales en alguno de estos indicadores, el sistema alerta a los administradores de red mediante la emisión de un *email* de alarma, con el objeto de que los administradores puedan tomar acciones tempranas que consideren pertinentes, según cada caso. Cada indicador posee su propio mensaje de alarma para poder ser diferenciado de otros. Los indicadores que monitorea el servidor se detallan a continuación:

- Nivel de congestión del ancho de banda de subida.

- Nivel de congestión del ancho de banda de bajada.
- Consumo de ancho de banda por *host*.

Nivel de congestión del ancho de banda de subida. Este indicador combina dos valores: *Ancho de banda global de subida* y *ancho de banda de subida promedio por host*. Ambos valores poseen límites configurados por los administradores del sistema. Para el *ancho de banda global* se debe definir un límite superior mientras que para el *ancho de banda promedio* se debe definir un límite inferior. Cuando el ancho de banda global supere el límite superior establecido y el ancho de banda promedio esté por debajo del límite inferior también establecido, el indicador nota una condición de anomalía. Si esta condición se mantiene al cabo de cierta cantidad consecutiva de mediciones, el servidor envía un email de alarma hacia el destinatario configurado por los administradores, indicando que el enlace se encuentra congestionado en cuanto a la subida de datos respecta, junto con un informe de la medición realizada.

Nivel de congestión del ancho de banda de bajada. Este indicador es análogo al anterior, realizando el servidor las mismas acciones que las descriptas anteriormente, sólo que esta vez teniendo en cuenta la capacidad de bajada de datos, en lugar de la de subida.

Consumo de ancho de banda por *host*. Este indicador analiza la velocidad actual de cada uno de los *hosts* que se encuentran haciendo uso del enlace WAN. Si un *host* excede el umbral especificado por los administradores del sistema, ya sea para subida o para bajada de datos, el indicador nota una condición anómala. Si dicho *host* continúa excedido al cabo de cierta cantidad consecutiva de mediciones, el servidor envía un *email* alarma hacia el destinatario configurado por los administradores indicando la presencia de un *host* excedido, junto con un informe de la medición realizada.

7 Caso de Ejemplo

El trabajo descripto, junto con los productos de software resultantes de la ejecución de este proyecto final de carrera, fueron implementados en la empresa *Scania Argentina S.A.*, en su unidad de producción ubicada en la provincia de Tucumán y actualmente se encuentran en pleno funcionamiento, conformando una valiosa herramienta de diagnóstico cotidiano para los administradores de red, desde principios del año 2010.

7.1 Scania

Scania Argentina S.A. forma parte de una empresa internacional con presencia en más de 100 países. Una de sus plantas productoras de autopartes se encuentra en la provincia de Tucumán. Dicha planta posee una red LAN de más de 300 nodos y se encuentra interconectada mediante enlaces WAN a sitios ubicados en Buenos Aires, San Pablo (Brasil) y el resto de la red global de Scania.

Todos los objetivos planteados en el apartado 2.2 fueron aplicados a esta empresa, poniendo particular énfasis en el monitoreo del enlace WAN con la sede de San Pablo. Dicho enlace WAN, de tecnología MPLS[5], fue contratado con un ancho de banda de 2 Mbps simétrico (igual ancho de banda de subida que de bajada) lo que permite mantener una comunicación directa con su par en Brasil y desde allí al resto de la red global de Scania. Es importante mencionar que, a su vez, la planta de Tucumán tiene acceso a *Internet* a través de un servidor *proxy* ubicado en Brasil, por consiguiente también utiliza este enlace dedicado para acceder a *Internet*. El diagrama general de esta porción de la red es el mostrado en la figura 10.

[5] Multiprotocol Label Switching (MPLS) es una tecnología de conmutación creada para proporcionar circuitos virtuales en las redes IP. Para más información, visitar: http://es.wikipedia.org/wiki/MPLS

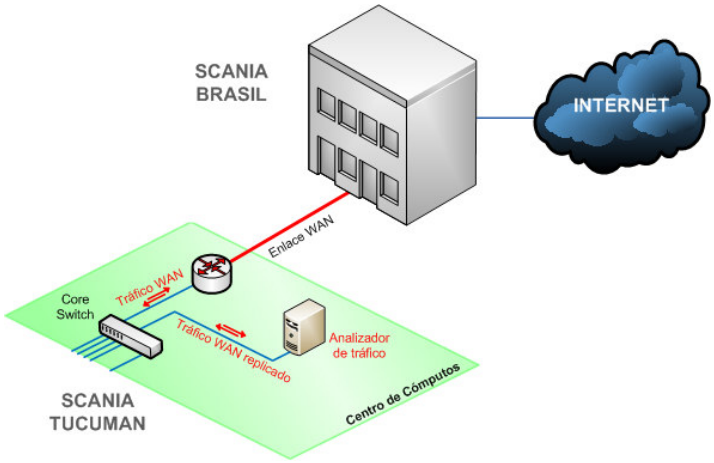

Fig. 10. Esquema detallado de la conexión del analizador de tráfico.

Conclusiones

La construcción del sistema de monitoreo de enlaces WAN fue realizada con éxito, cumpliendo con todos los objetivos estipulados al inicio del proyecto. Su arquitectura está basada en una aplicación cliente/servidor desarrollada completamente en el lenguaje de programación Java. A su vez, para dar soporte a la comunicación entre la aplicación cliente que sirve al usuario final como interfaz gráfica y la aplicación servidora que constituye el motor de análisis de tráfico, se utilizó el middleware ZeroC ICE.

Este sistema permite tomar medidas proactivas de acuerdo a los resultados obtenidos para lograr un uso eficiente del enlace, descubrir posibles limitaciones o sobrecapacidad del ancho de banda y reconocer irregularidades en la prestación del servicio.

Cabe destacar que se encuentra en funcionamiento desde Febrero de 2010, siendo empleado diariamente por los administradores de red del departamento de sistemas de la unidad de producción que Scania posee en la provincia de Tucumán.

Si bien el sistema trabaja en conjunto con una base de datos que mantiene información sobre los dispositivos conectados a la red LAN y sus responsables, no se trata de un requisito indispensable para su funcionamiento, ya que el análisis de tráfico realizado por el servidor no depende de dicha información.

Los criterios de diseño seguidos durante el proceso de construcción hacen del sistema una herramienta flexible, posibilitando su utilización en diferentes dominios de implementación y permitiendo la adición de nuevos módulos de análisis que se adapten a requisitos particulares de otras organizaciones.

El apéndice mostrado al final de este documento exhibe de manera gráfica los principales escenarios del sistema implementado, explicando su comportamiento y la información que cada uno presenta.

Agradecimientos

Al Ing. Sergio Saade por su constante dedicación a la excelencia en la enseñanza de ciencias de la computación.
Al Lic. Miguel Bazzano por la confianza depositada en nosotros y por su permanente apoyo.
A la Facultad de Ciencias Exactas y Tecnología por formar excelentes profesionales y seres humanos.
A nuestras familias, profesores, compañeros y amigos.

Bibliografía

1. William Stallings, Comunicaciones y Redes de Computadores, Prentice Hall, 2004
2. Andrew S. Tanenbaum, Redes de Computadoras, Prentice Hall, 2003
3. Harvey Deitel and Paul Deitel, Cómo Programar en Java, Prentice Hall, 2003
4. Michi Henning and Mark Spruiell, Distributed Programming with Ice, ZeroC, 2009
5. Loris Defioanni, Development of an Architecture for Packet Capture and Network Traffic Analysis, Graduation Thesis, Politecnico Di Torino, 2000

Apéndice: Principales escenarios del sistema.

1 Información del enlace

Esta pantalla muestra información sobre el ancho de banda total del enlace WAN utilizado por todas las estaciones de trabajo de la red LAN.

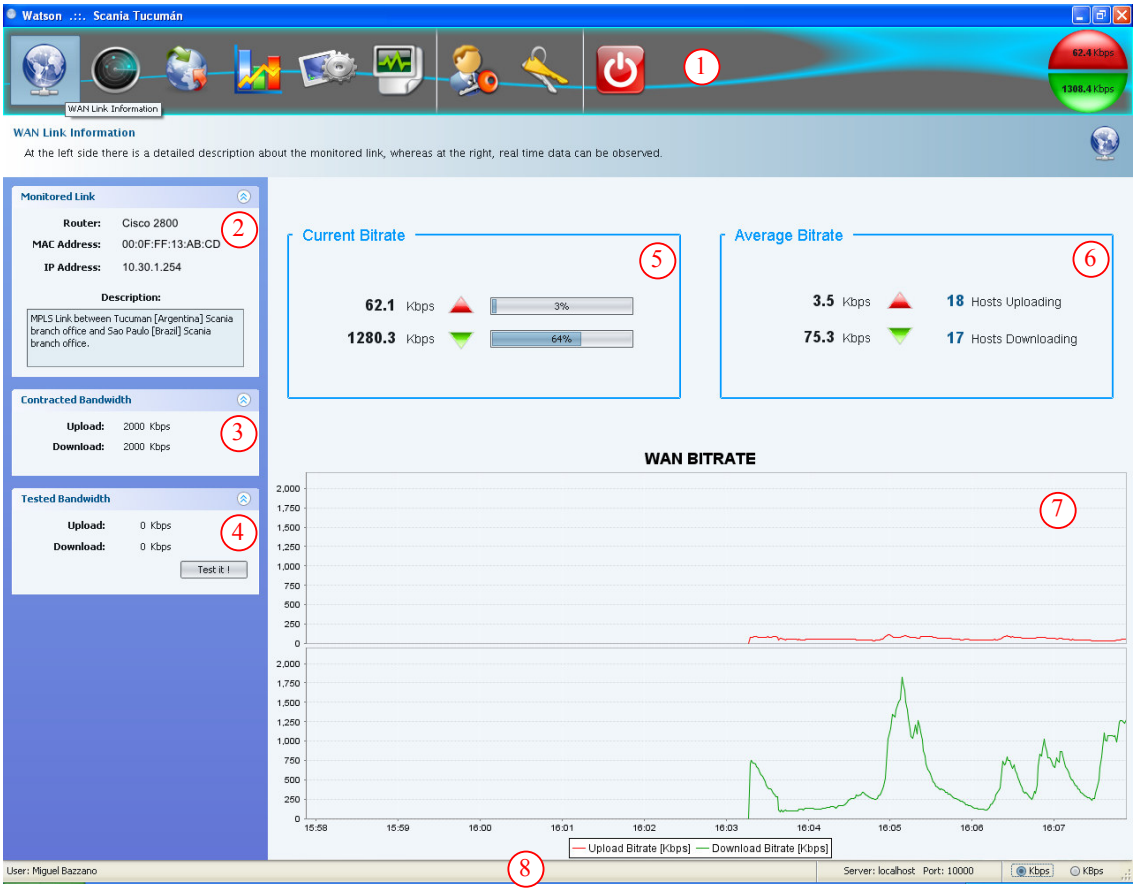

Fig. 1. Pantalla de visualización del tráfico global.

La información brindada en este escenario se detalla a continuación:

1. Barra principal. Brinda acceso a los diversos escenarios del sistema y permanece visible en todo momento.
2. Información del enlace. Provee una breve descripción del router utilizado, junto con sus direcciones MAC e IP.
3. Ancho de banda total contratado. Sirve como referencia, tanto para los administradores de red como para los porcentajes de las barras de medición.
4. El botón *Test it!* solicita al servidor que realice una medición del ancho de banda real que es capaz de soportar el enlace. Los valores especificados son actualizados al finalizar la medición.
5. Ancho de banda en tiempo real, medido en Kbps (Kilo bits por segundo) o KBps (Kilo bytes por segundo), según las preferencias del usuario.
6. Ancho de banda promedio, calculado en base al número de estaciones de trabajo de la red LAN que se encuentran haciendo uso del enlace.
7. Gráfica de ancho de banda de subida y de bajada que permite visualizar el patrón de tráfico actual. El tiempo inicial de la gráfica corresponde al inicio de sesión en la aplicación cliente.
8. Barra de estado que permite visualizar el nombre del usuario actualmente autenticado en el sistema, nombre de host y número de puerto TCP que escucha la aplicación servidora. También posee un botón que permite seleccionar la unidad de medición empleada en los valores de ancho de banda mostrados en todos los escenarios, ya sea Kbps o KBps.

2 Barra de acceso principal

Esta barra se encuentra en la parte superior de la ventana de la aplicación cliente y determina el punto de acceso a los diferentes escenarios mediante los íconos que posee en su interior. Estos íconos sólo se habilitan para el usuario que haya podido validar correctamente sus credenciales al inicio de sesión.

Fig. 2. Barra de acceso principal.

Los escenarios a los cuales se puede acceder mediante esta barra son:

1. Visualización del ancho de banda global.
2. Visualización del ancho de banda por estación de trabajo y departamento.
3. Visualización del ancho de banda por tipo de red y protocolo de aplicación.
4. Estadísticas de tráfico.
5. Configuración del sistema.
6. *Logs* de la aplicación cliente y servidora.
7. Nuevo inicio de sesión.
8. Cambio de contraseña.
9. Salida de la aplicación.

En la esquina derecha se puede observar un medidor de velocidad que expresa, sobre un semicírculo rojo, el ancho de banda global de subida, y sobre un semicírculo verde, el ancho de banda global de bajada. Este medidor se encuentra visible en todo momento, independientemente del escenario en donde se encuentre el usuario.

Ancho de banda por estación de trabajo

La figura 3 muestra información sobre el ancho de banda del enlace, discriminando su utilización por estación de trabajo y por departamento. También provee información acerca de aquellas estaciones de trabajo que hacen mayor utilización del mismo enlace.

Los puntos de acceso e información del escenario se detallan a continuación:

1. Esta pestaña permite acceder al árbol conformado por todas las estaciones de trabajo de la red LAN que están haciendo uso del enlace. Al seleccionar la raíz de dicho árbol (*ALL*) se activa la pestaña mostrada en 3.
2. Esta pestaña permite acceder al árbol conformado por departamentos, mostrando a su vez las estaciones de trabajo pertenecientes a cada departamento de la lista.
3. Detalle de las estaciones de trabajo que aparecen en el árbol del hosts. La información que se muestra abarca: dirección IP, nombre de host, velocidad de subida, velocidad de bajada, responsable de la estación (si aplica), perfil de usuario global, sector y departamento al que pertenece el usuario responsable.
4. Ranking de hosts con mayor consumo de ancho de banda.
5. Seleccionando una estación en particular se accede a información más detallada sobre dicha estación, como se podrá apreciar en la siguiente sección de este apéndice.
6. El botón *Hostnames* permite visualizar las estaciones de trabajo del árbol de hosts por sus nombres de hosts, mientras que el botón *IP Addresses* muestra sus direcciones IP.
7. Barra de búsquedas que permite localizar una determinada estación de trabajo según una expresión que esté contenida en cualquiera de los campos que conforman la tabla, ya sea, nombre de host, dirección IP, o información del propietario.

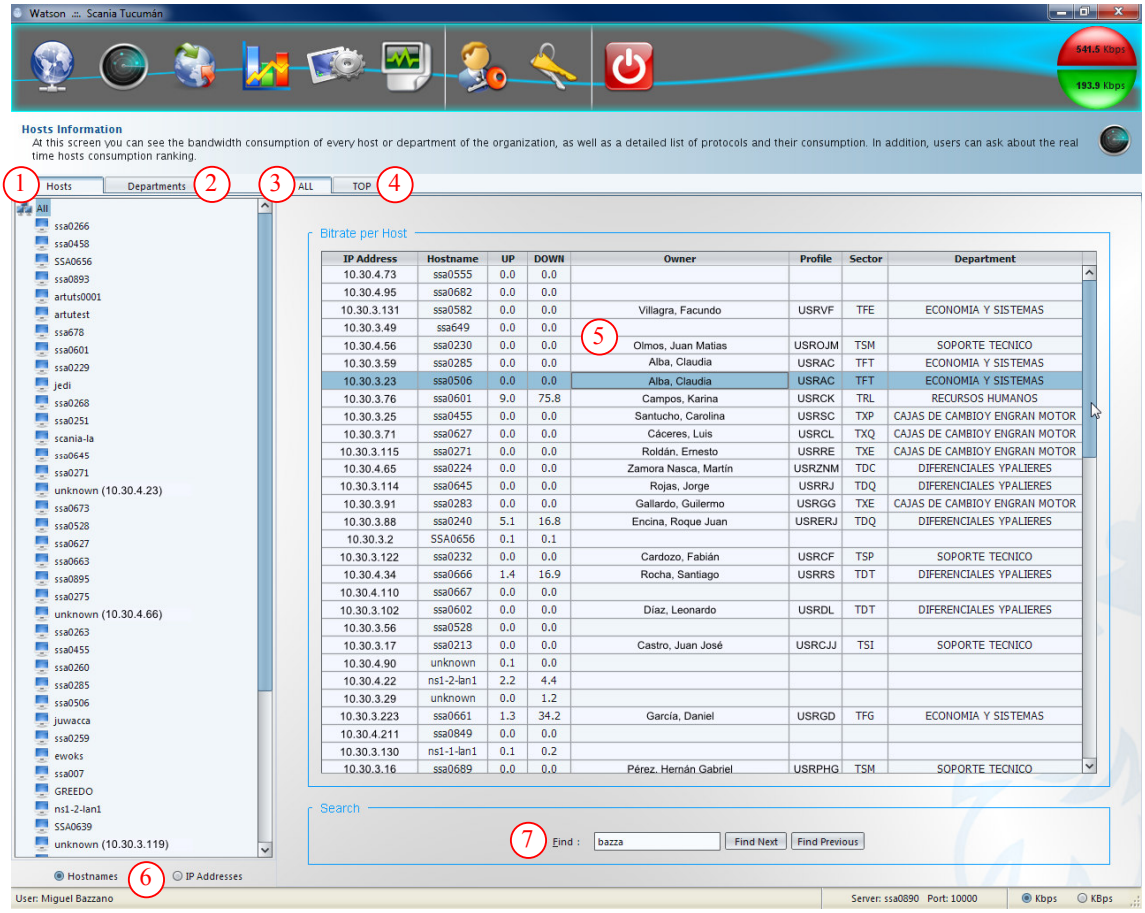

Fig. 3. Tráfico de hosts y departamentos

3 Información de host

La pantalla mostrada en la figura 4 denota información detallada sobre un host en particular. Se puede acceder a ella de dos maneras:

- Seleccionando el host deseado en el árbol de hosts.
- Haciendo doble clic o presionando la tecla *ENTER* sobre el host deseado, en las tablas mostradas en los paneles *ALL* y *TOP* de la figura 3.

La información mostrada al usuario en esta pantalla es la siguiente:

- **Información corporativa:** dirección IP, nombre de host, responsable, nombre de usuario, sector, departamento, número de teléfono interno.
- **Ancho de banda:** consumo de ancho de banda de subida y de bajada, en tiempo real.
- **Información de aplicaciones:** protocolos de capa de aplicación que están siendo empleados por la estación y que a su vez trafican datos por el enlace WAN, junto con su respectiva velocidad de subida y de bajada.

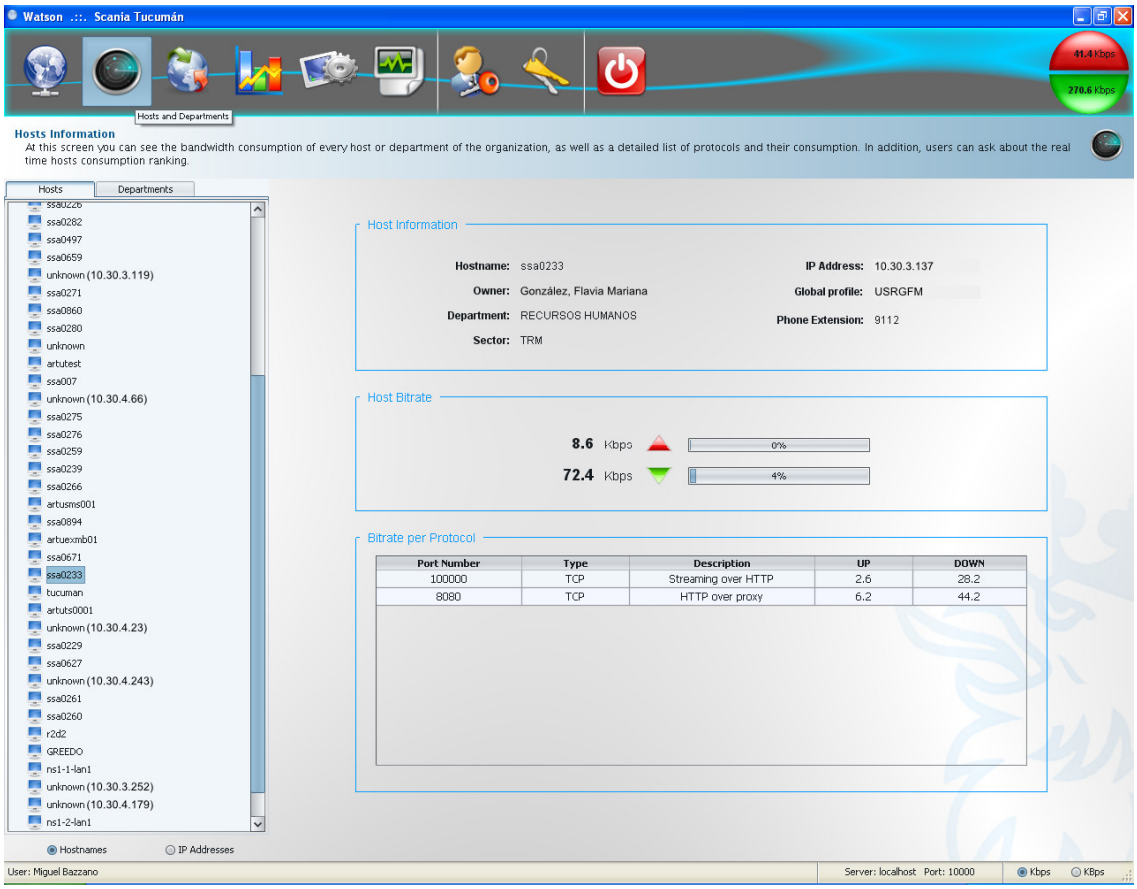

Fig. 4. Información detallada de host.

4 Ancho de banda por departamento

Este escenario, expuesto en la figura 5, muestra una tabla con los distintos departamentos que conforman la estructura organizacional de Scania, junto con el ancho de banda consumido por cada uno de ellos, medido en tiempo real. En la parte inferior de la pantalla se observa una barra para buscar departamentos en particular, de manera rápida.

La tabla de departamentos permite ordenamiento según sus tres columnas, es decir que si el usuario presiona la columna *DOWN*, los departamentos se ordenarán según el consumo de ancho de banda de bajada. Cabe destacar que dicho ordenamiento se mantendrá a lo largo de las sucesivas actualizaciones automáticas de la tabla.

Al hacer clic sobre un departamento del árbol, se mostrará información detallada sobre el departamento en cuestión, al igual que al hacer doble clic en la tabla o al presionar la tecla *ENTER* luego de seleccionar un departamento de la tabla.

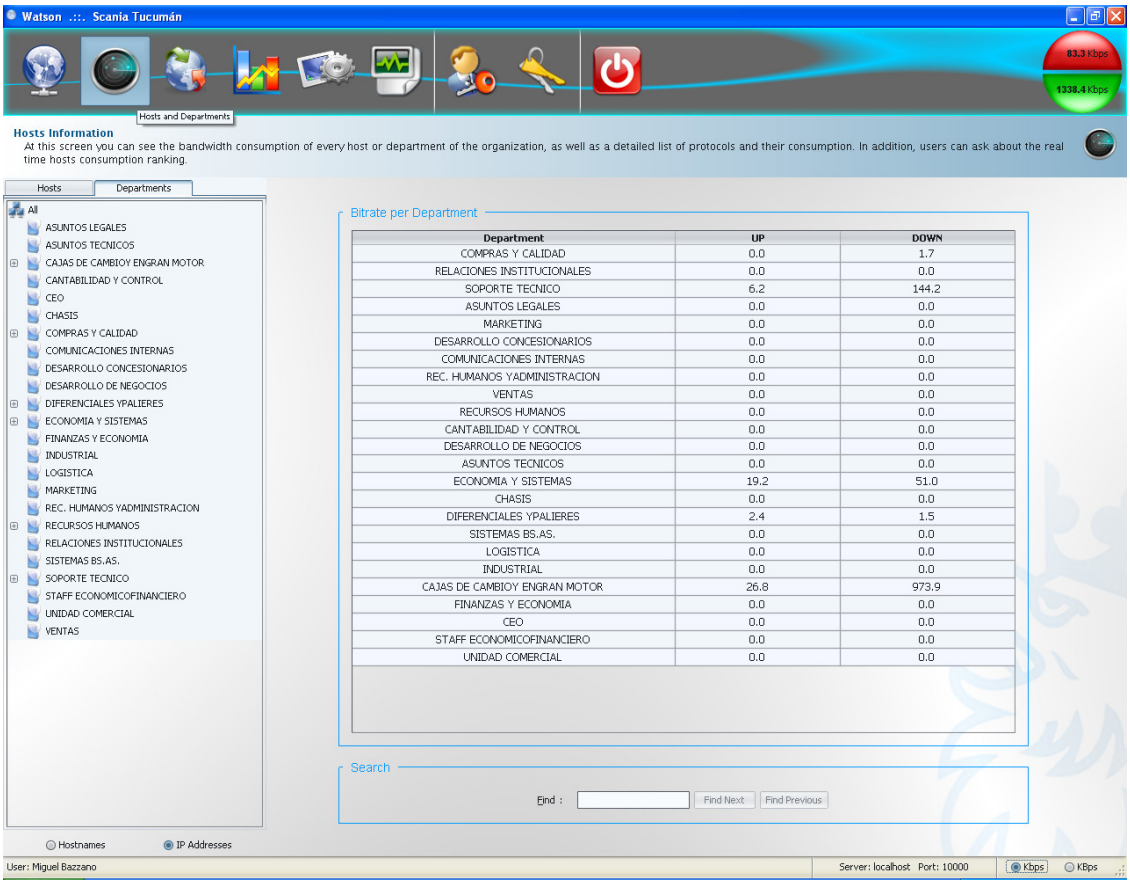

Fig. 5. Consumo de ancho de banda por departamento.

5 Información de redes

La pantalla mostrada en la figura 6 expone información sobre el consumo de ancho de banda, separando el tráfico de Internet del tráfico correspondiente a Intranet. Se considera tráfico de Internet a todo aquel que se dirija o que provenga de direcciones IP públicas que no pertenezcan a la compañía, así como también al que se dirige o que proviene de los servidores *proxies* de la empresa.

Esta pantalla muestra también el detalle de protocolos de capa de aplicación que se encuentran haciendo uso del enlace, independientemente si pertenecen a Internet o Intranet.

La información presente en este escenario es la siguiente:

1. Ancho de banda total correspondiente a Internet, medido en Kbps (Kilo bits por segundo) o KBps (Kilo bytes por segundo) según la opción seleccionada en la barra de estado. También es posible observar el porcentaje que dicho valor representa frente al ancho de banda teórico o contratado del enlace.
2. Ancho de banda total correspondiente a Intranet.
3. Protocolos o aplicaciones que conforman el total del tráfico de ambas redes, junto con sus respectivos anchos de banda de subida y de bajada. En esta tabla se especifican los números de puerto y sus tipos (TCP o UDP), junto con una descripción que permite identificar los puertos reconocidos. La descripción *not available* significa que el puerto es desconocido para la aplicación servidora, ya que la misma dispone de un archivo de configuraciones en donde se especifican cada una de las aplicaciones y protocolos conocidos.

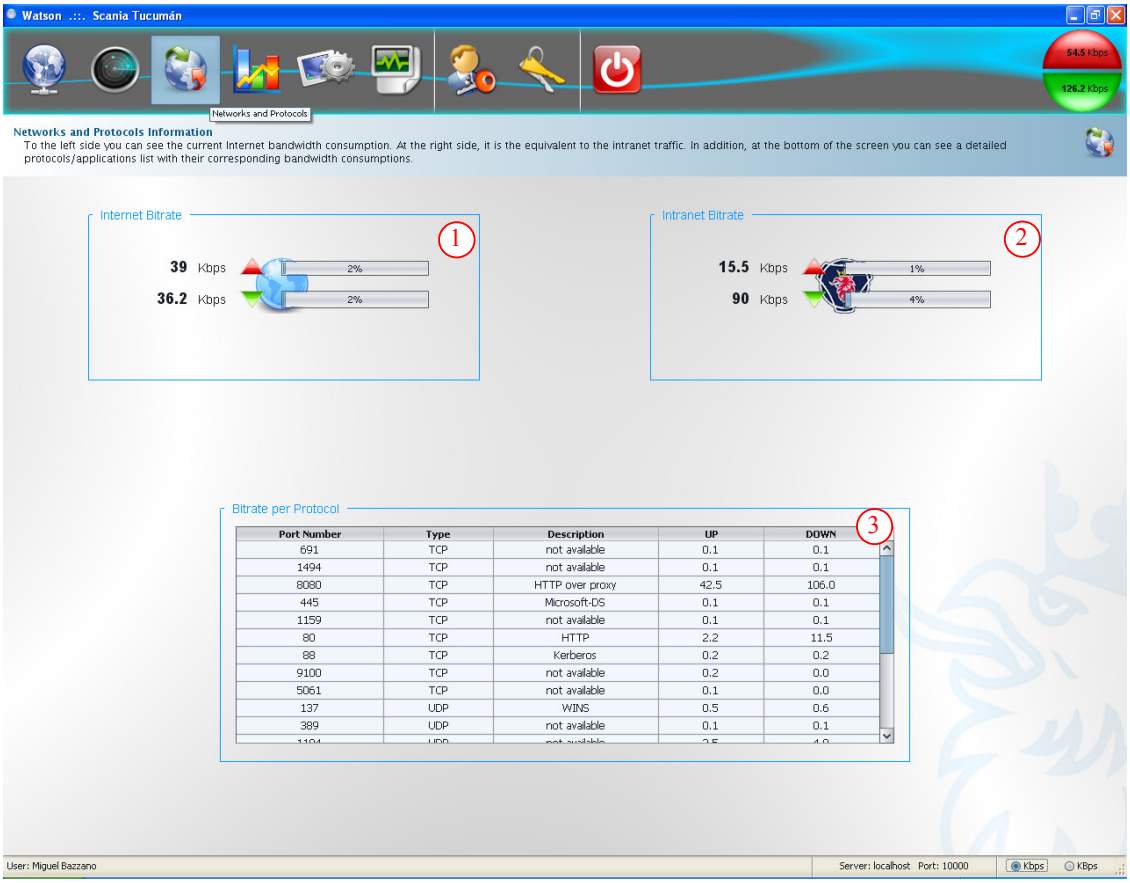

Fig. 6. Tráfico Internet/Intranet y protocolos de capa de aplicación.

6 Estadísticas

La sección de estadísticas brinda al usuario información que no se obtiene directamente desde la aplicación servidora, sino por medio de consultas a una base de datos mantenida por el sistema. Por consiguiente, la información mostrada en pantalla, si bien es precisa, no es en tiempo real y podría tardar en actualizarse dependiendo del periodo de almacenamiento de datos configurado en el servidor, el cual se encuentra establecido en 10 minutos por defecto.

En esta sección es posible acceder al consumo acumulado de datos por host y a los sitios web accedidos por los usuarios de la red LAN. El panel mostrado a la izquierda permite la búsqueda dentro de un rango de fechas, tanto para el consumo de datos como para los sitios visitados. Por defecto, el lapso de tiempo seleccionado en cada caso corresponde al día en curso.

En la parte inferior de la pantalla de consumos y de sitios visitados se encuentra una barra de búsqueda rápida, la cual permite la búsqueda de datos en base a cualquier valor de la tabla.

6.1 Tráfico acumulado por host

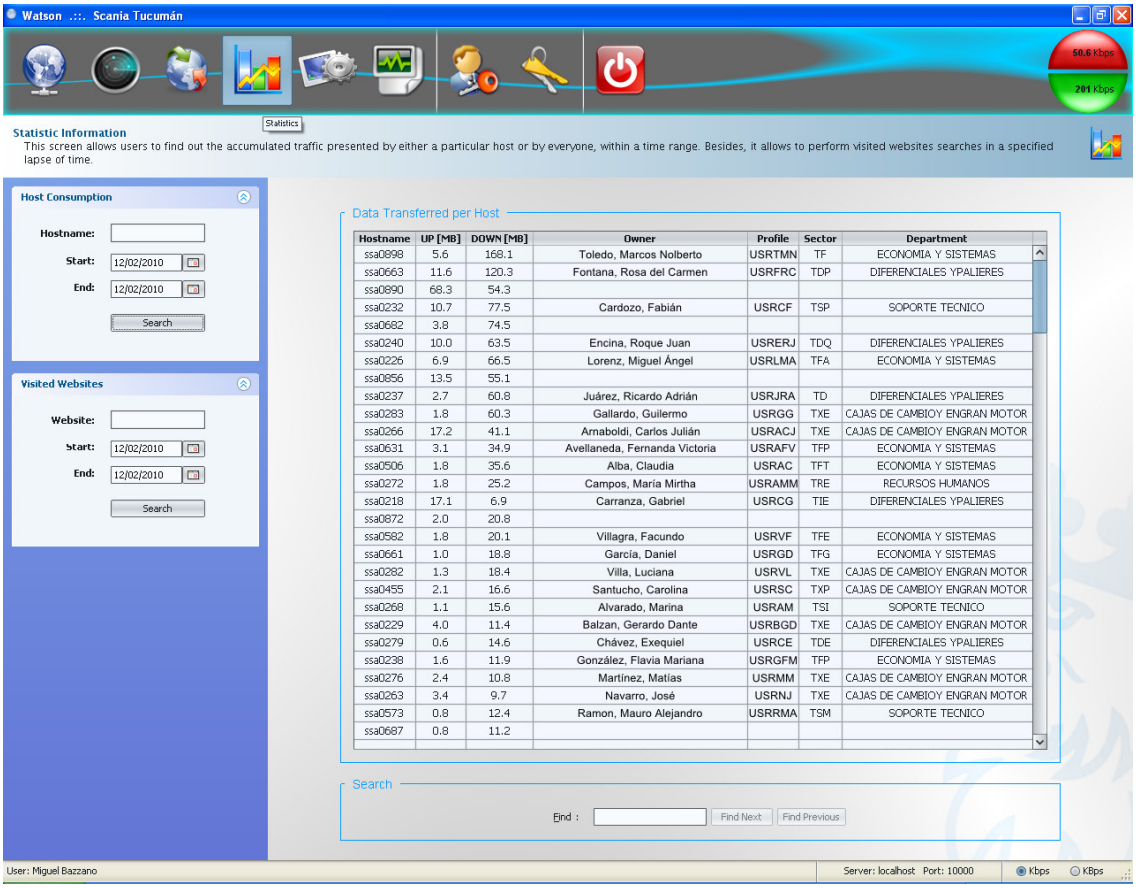

Fig. 7. Consumo de datos acumulado por host.

Al realizar una nueva búsqueda por rango de tiempo, es posible especificar el nombre de un host en particular (o parte del nombre) o directamente dejar en blanco el campo *Hostname*, en cuyo caso el sistema traerá la información de todos los hosts que hicieron uso del enlace en el periodo indicado, como se puede observar en la figura 7. La información mostrada en la tabla consta de los siguientes campos: nombre de host, tráfico acumulado de subida en MBytes, tráfico acumulado de bajada en MBytes, persona responsable por el dispositivo, nombre de usuario corporativo, sector y departamento al que pertenece el responsable.

6.2 Sitios web visitados

La búsqueda de sitios visitados por los usuarios de la red LAN se realiza de manera análoga a la del consumo por host. Es posible especificar parte del nombre de un sitio web o dejar en blanco el campo *Website*, en cuyo caso el sistema mostrará una lista con todos los sitios visitados y la cantidad de accesos contabilizados para el rango de tiempo indicado, como se puede observar en la siguiente figura:

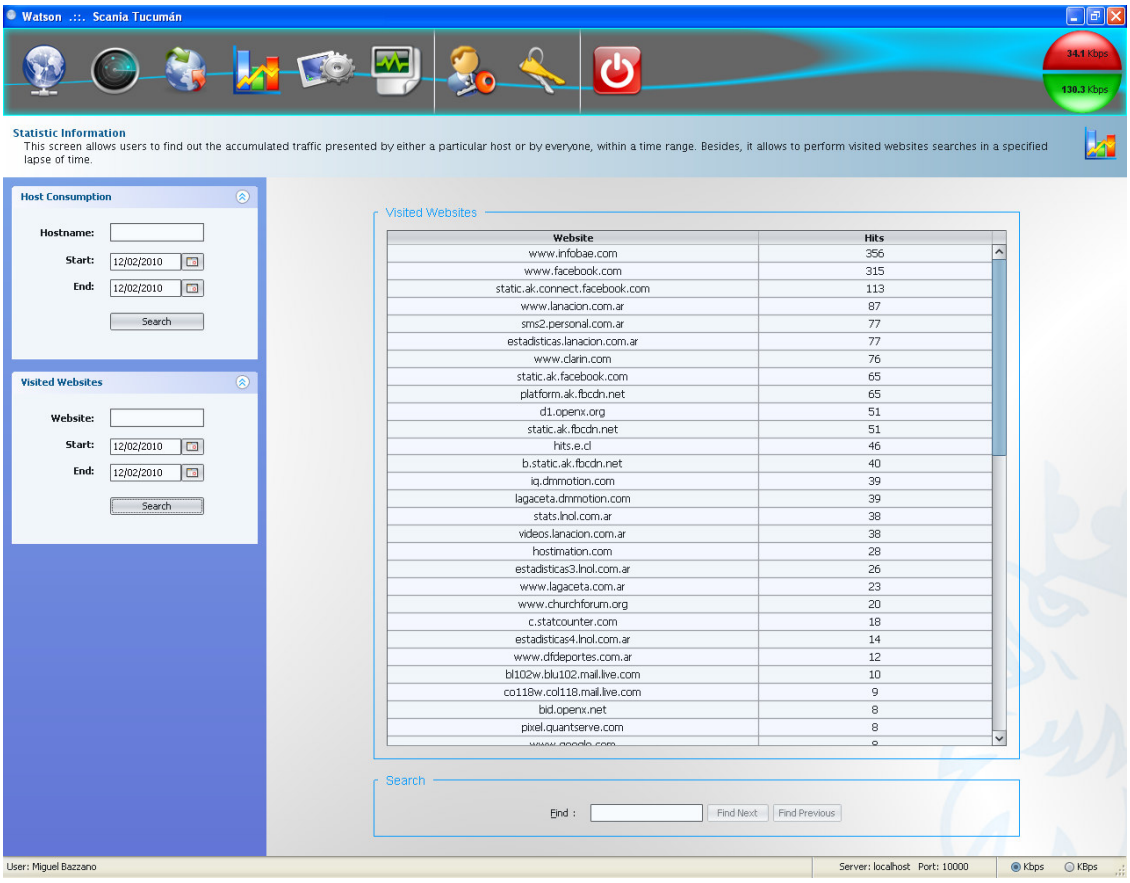

Fig. 8. Sitios web visitados.

El número de accesos contabilizados corresponde a la cantidad de veces que un usuario ingresa a una página perteneciente al sitio web en cuestión. Por ejemplo, si un usuario ingresa a tres páginas que pertenecen al sitio www.infobae.com, los accesos contabilizados serán tres.

7 Configuración de Alarmas

Esta pantalla permite a los usuarios con rol de administrador, configurar dos tipos de alarmas que serán enviadas por la aplicación servidora cuando se detecten anomalías en el tráfico, así como también las cuentas de correo electrónico que se usarán como remitente y destinatario de los mensajes de alarma.

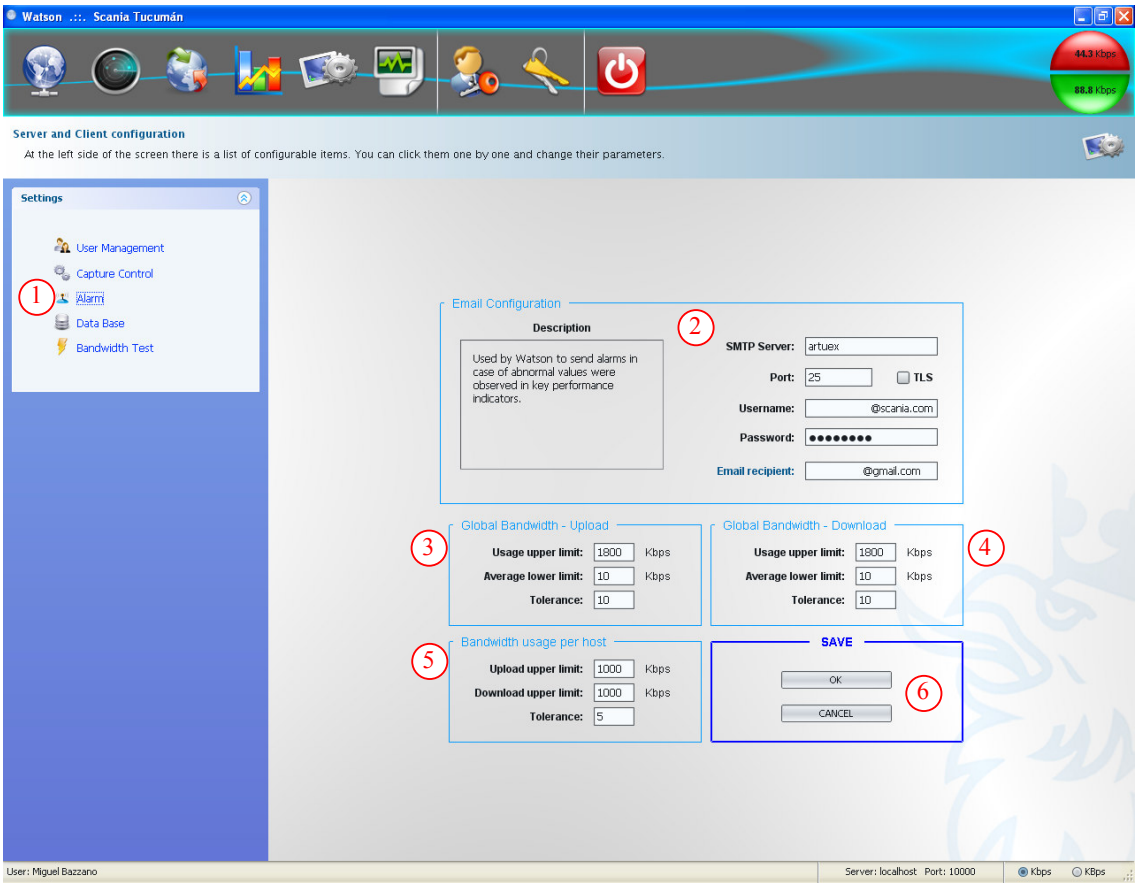

Fig. 9. Configuración de alarmas.

La información que presenta este escenario es la siguiente:

1. Al acceder al enlace *Alarm* del panel ubicado a la izquierda de la pantalla, se habilita la pantalla mostrada en la figura 9.
2. Permite establecer parámetros del servidor de correo electrónico utilizado para enviar los mensajes de reporte de anomalías, especificando servidor y puerto. También es posible especificar información de la cuenta de correo que se utilizará para enviar los mensajes y el destinatario de la misma.
3. Permite configurar los parámetros que utilizará el servicio de detección de anomalías de insuficiencia en el ancho de banda de subida. Cuando el servicio detecta que el tráfico de subida es superior a *Usage upper limit*, y que el tráfico promedio de subida, considerando todas las estaciones que influyen en dicho cálculo, es inferior a *Average lower limit,* y si además esta condición persiste durante la cantidad de mediciones consecutivas definida como *Tolerance*, se enviará un email reportando esta situación.
4. Permite configurar los parámetros que utilizará el servicio de detección de anomalías de insuficiencia en el ancho de banda de bajada. Cuando el servicio detecta que el tráfico de bajada es superior a *Usage upper limit*, y que el tráfico promedio de bajada, considerando todas las estaciones que influyen en dicho cáculo, es inferior a *Average lower limit,* y si además esta condición persiste durante la cantidad de mediciones consecutivas definida como *Tolerance*, se enviará entonces un email reportando la situación.
5. Permite configurar parámetros que utilizará el servicio de detección de anomalías para determinar si existen excesos en la utilización de ancho de banda por parte de ciertas estaciones de trabajo, durante la cantidad de mediciones consecutivas definida como *Tolerance*, tomando como referencia los valores *Upload upper limit* y *Download upper limit* como máximos de ancho de banda de subida y de bajada respectivamente.

6. Permite guardar los cambios realizados en los parámetros de configuración de esta pantalla, o bien cancelar si se desea descartar los cambios. Es importante tener en cuenta que el servidor utilizará los nuevos parámetros luego de reiniciar manualmente el proceso de captura.

7.1 Mensajes de anomalías en el tráfico del enlace

A continuación se muestran los mensajes de alerta enviados por el servidor de captura cuando el servicio de detección de anomalías reconoce situaciones potencialmente problemáticas.

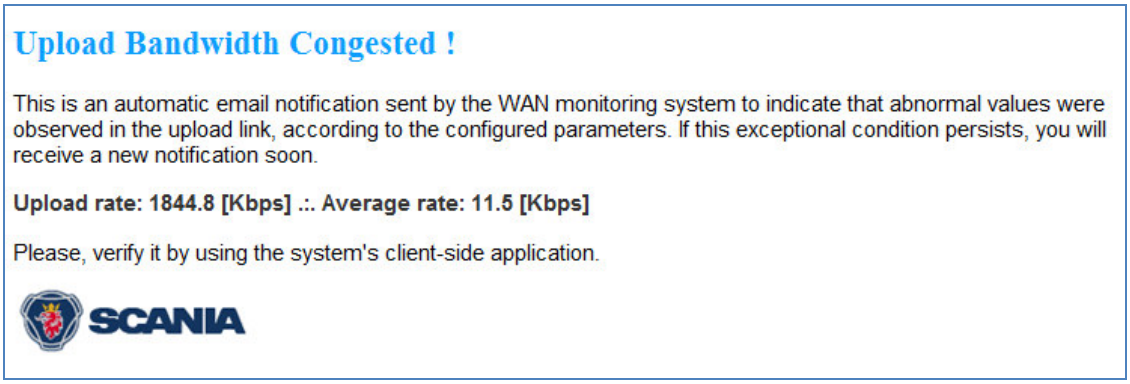

Fig. 10. Notificación de ancho de banda de subida congestionado.

En la notificación es posible observar que la tasa de transferencia total de subida alcanzó un valor de 1844,8 [Kbps] mientras que la velocidad promedio es de apenas 11,5 [Kbps]. Esto sugiere que un gran número de estaciones de trabajo de la red LAN están haciendo uso del enlace, experimentando una baja velocidad al momento de la medición, denotando de este modo una posible insuficiencia de ancho de banda de subida.

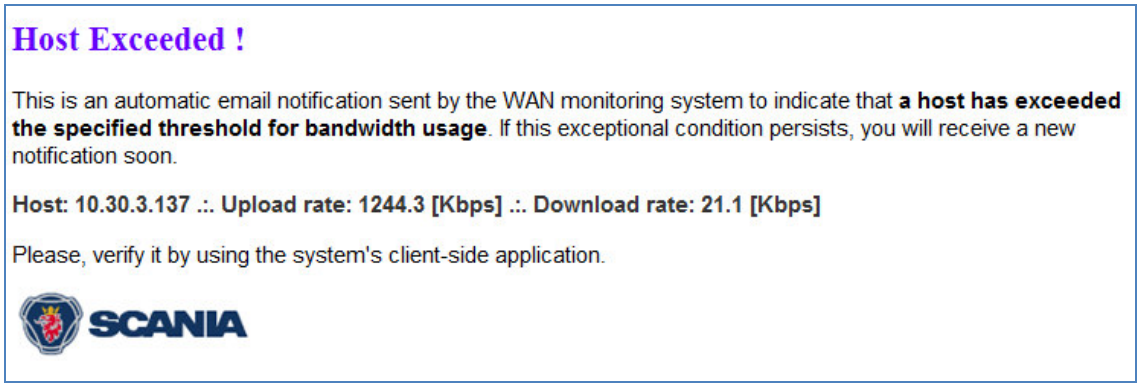

Fig. 11. Notificación de consumo excesivo por parte de un host.

En la notificación de la figura 11 es posible observar que el ancho de banda de subida de la estación de trabajo de dirección IP 10.30.3.137 alcanzó una tasa de 1244,3 [Kbps]. Esto sugiere que el usuario de la estación podría estar haciendo un uso indebido del enlace, si el ancho de banda contratado es de 2000 [Kbps].