SMAЯTxAC: Sistema de monitorización y análisis de tráfico para la *Anella Científica*

SMAЯTxAC: A System for Monitoring and Analysing the traffic of the *Anella Científica*

Resumen

El presente artículo describe un sistema de monitorización y análisis de tráfico en tiempo real, para redes troncales de alta velocidad. Esta herramienta proporciona información detallada sobre el uso de la red, y es de gran valor para su gestión y dimensionado, así como para la optimización de los recursos y la detección de usos irregulares y ataques. El proyecto SMAЯTxAC tiene como objetivo instalar una nueva versión de este sistema para monitorizar de forma permanente el tráfico de la *Anella Científica*, adaptada a las necesidades de sus gestores (CESCA).

Palabras clave: monitorización, captura de tráfico, análisis de tráfico, compartimiento de costes

Summary

Summary…

Keywords: monitoring, traffic accounting, traffic analysis, cost-sharing

1. Antecedentes y motivación

En los últimos años, en la red académica y de investigación española (RedIRIS), se han llevado a cabo diferentes proyectos relacionados con la monitorización y la caracterización del tráfico Internet, como son los proyectos CASTBA, MEHARI [1] y MIRA [2, 3]. Estos proyectos se realizaron de forma conjunta entre la Universidad Politécnica de Madrid, la Universidad Carlos III de Madrid, la Universitat Politècnica de Catalunya (UPC), y con la participación como EPOs de RedIRIS, Telefónica Investigación y Desarrollo, el Centre de Supercomputació de Catalunya (CESCA) y el Institut Català de Tecnologia.

Una vez finalizados estos proyectos y basándose en la experiencia adquirida en la participación en ellos, el Centre de Comunicacions Avançades de Banda Ampla (CCABA) de la UPC, desarrolló un prototipo propio de un sistema completo de monitorización que permite el análisis de tráfico en tiempo real en enlaces de alta velocidad [4, 5]. Este prototipo proporciona información detallada sobre el uso que se hace de la red monitorizada, información que puede ser de gran ayuda para el dimensionado y la optimización de recursos, además de ser útil para detectar usos irregulares y ataques.

El funcionamiento de este prototipo se probó en el troncal de Cataluña de RedIRIS (*Anella Científica*), que constituye la principal vía de salida a Internet de las universidades y centros de investigación catalanes. Los resultados de estas primeras pruebas fueron muy satisfactorios, y animaron a los gestores de la *Anella Científica* (CESCA) a encargar al CCABA-UPC el desarrollo de una versión mejorada de dicho sistema para la monitorización permanente de la *Anella Científica*, que ha dado lugar al proyecto SMAЯTxAC.

2. Descripción del prototipo CCABA-UPC

La funcionalidad principal del prototipo es la monitorización y el análisis de tráfico en tiempo real en enlaces troncales de alta velocidad. Estos enlaces son compartidos por gran cantidad de redes, que a su vez están dando servicio a miles de usuarios. Estos usuarios tienen necesidades y perfiles muy diferentes, y pueden acceder a una gran variedad de servicios. Debido a esta heterogeneidad, no sólo el volumen de tráfico presente en estas redes es muy elevado, sino que también lo es el número de conexiones establecidas simultáneamente. Precisamente la gran cantidad y variedad de datos a capturar y analizar es la principal dificultad a abordar en el desarrollo de un sistema de estas características. El equipo de captura debe ser capaz de capturar todo el tráfico, sin perder ningún paquete, pero la dificultad principal está en el sistema de análisis, que debe ser lo suficientemente ligero y eficiente para poder tratar

toda esta información en tiempo real, y resumirla para que sea viable su almacenamiento de forma permanente.

La Figura 1 muestra que el prototipo de monitorización y análisis de tráfico está dividido en tres sistemas, que por razones de eficiencia se ejecutan en equipos diferentes. Estos tres sistemas son:

- Plataforma de captura
- Sistema de análisis
- Sistema de visualización de resultados

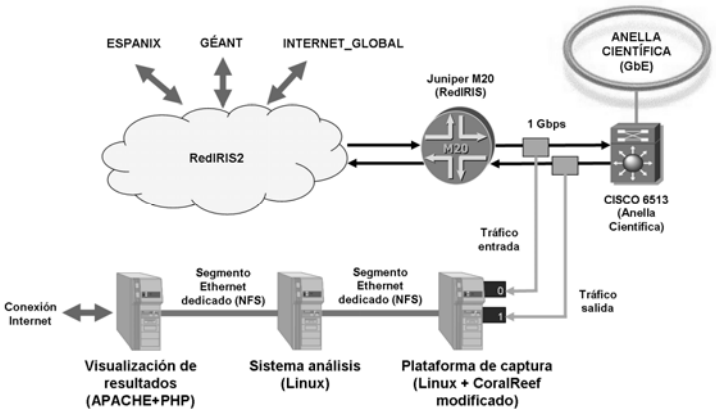

Figura 1: Visión general del sistema

3. Plataforma de captura

Llamamos *plataforma de captura* a la parte hardware y software dedicada a la captura de tráfico. Al igual que en el proyecto MIRA, se realiza una captura pasiva (no intrusiva) del tráfico, utilizado divisores de fibra pasivos (*splitters*), que permiten enviar una copia íntegra del tráfico a un PC, que se encarga de la captura y el procesado de los paquetes. Al contrario de lo que sucede con los métodos de captura activos, como *Cisco NetFlow* [6] o los basados en SNMP, nuestro sistema no afecta en absoluto al rendimiento de la red monitorizada, ya que la captura no se realiza directamente en los equipos dedicados a la interconexión de redes, ni tampoco se genera tráfico adicional.

Se ha desestimado utilizar la plataforma de captura desarrollada en el proyecto MIRA, debido a que los requisitos actuales difieren de forma considerable con los que se plantearon en dicho proyecto. El sistema MIRA realizaba una captura estadística del tráfico (aproximadamente un 10% del tráfico real) debido a que se capturaba el contenido de los paquetes. Actualmente se ha preferido capturar únicamente las cabeceras de los paquetes, y conseguir así una captura completa del tráfico. Esto es debido a que la captura de contenidos presenta varias limitaciones, como la posible infracción de confidencialidad o la imposibilidad de analizar los paquetes cifrados mediante técnicas de encriptación. Además, las cabeceras capturadas pueden agregarse en forma de flujos, y reducir así el volumen de datos a tratar por el sistema de análisis.

En el momento de desarrollo de este prototipo, el escenario de pruebas fue el troncal de Cataluña de RedIRIS (ATM STM-1). La plataforma de captura consistió en un PC estándar equipado con dos tarjetas FORE PCA200 ATM (una para cada sentido del tráfico), utilizando el software de captura de libre distribución *CoralReef* [7].

4. Análisis de tráfico

El sistema de análisis de tráfico se encarga de procesar los flujos IP capturados por la plataforma de captura, y transformarlos en un nuevo tipo de flujos que denominamos *flujos clasificados*. Esta transformación consiste en la traducción de los valores que identifican un flujo IP (direcciones IP, puertos y protocolo) a valores más generales (origen, destino y aplicación) y por tanto más útiles para conocer el uso que se hace de la red. Al reducir el número de posibles valores que identifican un flujo, se consigue una reducción considerable del número de flujos a almacenar, ya que en un mismo flujo clasificado quedan agregados varios flujos IP. La reducción aún es mayor ya que los flujos clasificados son bidireccionales, mientras que los flujos IP son unidireccionales.

Entendemos como *origen*, a los diferentes rangos de direcciones IP definidos en la red monitorizada. Por ejemplo, en nuestro caso serán las instituciones conectadas a la *Anella Científica*, pero podrían ser también sus puntos de acceso (varias instituciones comparten un

mismo punto de acceso) o los departamentos dentro de cada institución, etc. En general el número de orígenes definidos dependerá del nivel de detalle del análisis que considere necesario el gestor de la red.

Análogamente llamamos *destino* a los diferentes rangos de direcciones IP de interés fuera de la red monitorizada. Por ejemplo, en nuestro caso se han definido cinco grupos de destinos, dependiendo de las diferentes conexiones que dispone RedIRIS con el exterior (Géant, Espanix, Internet Global y RedIRIS para el tráfico a otras CC.AA.), más un destino especial para el tráfico *multicast*.

Una vez realizada la transformación de flujos, se acumulan los datos obtenidos en períodos diarios, semanales y mensuales, con lo que se consigue una reducción aún mayor del volumen de datos a almacenar. Adicionalmente, se mantiene un registro de los flujos que no se han podido clasificar, porque contienen direcciones falsas, puertos o protocolos desconocidos, etc. Esta información puede ser de gran valor para la detección de usos irregulares o ataques, y en general para conocer más detalladamente el uso de la red.

Por último, también se desarrolló un modelo de tarificación basado en el uso de la red, que contempla cada uno de los parámetros de clasificación (orígenes, destinos, aplicaciones, sentido y volumen). Esta tarificación podría servir de base para el despliegue de un modelo de compartimiento de los costes derivados del uso y mantenimiento de la red.

5. Visualización de resultados

El prototipo dispone de una interfaz gráfica, basada en un entorno *web*, que permite consultar gráficamente todos los resultados de análisis de tráfico. Estas graficas son generadas dinámicamente por el servidor *web* bajo demanda.

A continuación se enumeran las gráficas de análisis que pueden ser consultadas por los gestores de la red. Cada una de estas gráficas puede representarse para el total de tráfico, o de forma desglosada para cada uno de los orígenes (en este caso para cada institución conectada a la *Anella Científica*), en unidades de bits por segundo, paquetes por segundo, octetos o número de paquetes:

- Evolución temporal del tráfico por aplicaciones (Figura 2)
- Comparativa entre orígenes de la evolución temporal del tráfico por aplicación
- Tráfico cruzado por destinos/aplicaciones (Figura 3) y orígenes/destinos
- Tráfico por orígenes, destinos, aplicación y protocolos de transporte
- Tráfico IP no TCP/UDP
- Tráfico con puertos, direcciones y protocolos de transporte desconocidos
- Gráficas de tarificación y factura

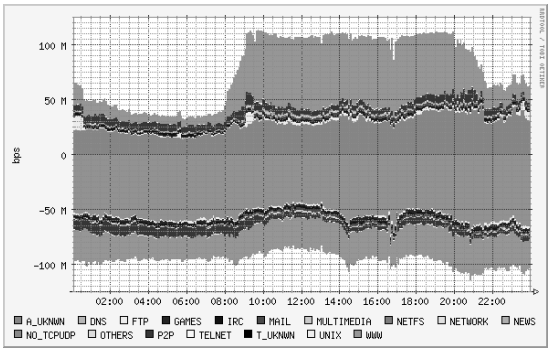

Figura 2: Evolución del tráfico por aplicaciones

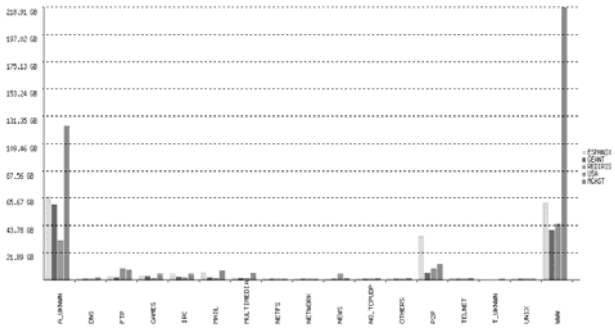

Figura 3: Tráfico por aplicaciones y destinos

6. Proyecto SMAЯTxAC

El proyecto SMAЯTxAC es un acuerdo de colaboración entre el CESCA y la UPC que se inició en Julio de 2003, con el objetivo de instalar una versión mejorada del prototipo presentado para

la monitorización permanente de la *Anella Científica*. Este nuevo sistema debe proporcionar información útil que ayude al CESCA en las tareas diarias de gestión de la red.

El objetivo principal de este proyecto es adaptar el prototipo desarrollado por el CCABA-UPC a la tecnología Gigabit Ethernet, después de que en Mayo de 2003 la *Anella Científica* cambiara de ATM a esta nueva tecnología.

Para conseguir este objetivo es necesario un cambio de la plataforma de captura, ya que el volumen de tráfico puede crecer de los 310 Mbps. de los dos enlaces ATM anteriores, hasta los 2 Gbps. en GbEth. Por este motivo no es posible utilizar tarjetas de red estándar GbEth para la captura, ya que no son capaces de realizar una captura completa con estos volúmenes de tráfico. Actualmente se está utilizando una tarjeta GbEth especializada para la captura (DAG 4.3GE de Endace [10]) que consigue capturar todo el tráfico de dos enlaces GbEth sin perder ningún paquete.

Otro objetivo es la modificación del sistema de análisis según las necesidades que pueda tener el CESCA como gestor de la *Anella Científica*. Éste se concreta en el desarrollo de un módulo de detección automática de situaciones irregulares, como pueden ser cambios repentinos en los patrones habituales de tráfico de alguna de las instituciones conectadas a la red, ataques (DoS, DDoS, *Spoofing*, etc.), uso de aplicaciones *peer-to-peer* o equivalentes, etc.

Actualmente ya se están obteniendo los primeros resultados de análisis de tráfico en la monitorización de enlaces Gigabit Ethernet, y esta previsto que en Febrero de 2004 se ponga en marcha una primera versión del sistema SMAЯTxAC para analizar de forma estable y permanente el tráfico de la *Anella Científica*.

7. Conclusiones

La monitorización y análisis de tráfico en tiempo real en redes de alta velocidad es posible utilizando equipos de bajo coste, sin degradar el rendimiento de la red monitorizada. La combinación de capturar únicamente las cabeceras de los paquetes, junto con la transformación de estos datos a flujos clasificados, consigue un buen equilibrio entre rendimiento, calidad de la información generada, y volumen de datos a almacenar.

El hecho de no capturar el contenido de los paquetes permite realizar una captura completa, y con un buen diseño del sistema análisis es posible también su procesado en tiempo real. Además, permite esquivar los posibles problemas de infracción de la privacidad, o el procesado de paquetes cifrados.

Las pruebas realizadas en la *Anella Científica* han demostrado que la cantidad y calidad de los datos generados por este sistema, permite conocer con detalle el uso que se hace la red. Esto lo convierte en una herramienta de gran valor para la gestión de la red, el dimensionado y la optimización de recursos, así como para la detección de usos irregulares y ataques.

Agradecimientos
Este trabajo ha sido financiado parcialmente por el CESCA (convenio SMAЯTxAC) y por el MCyT (Ministerio de Ciencia y Tecnología) bajo el contrato con ref. TIC2002-04531-C04-02 (SAM). Los autores agradecen también a los participantes de anteriores proyectos (CASTBA, MEHARI y MIRA) que fueron el punto de partida para este trabajo.

8. Referencias

[1] LIZCANO, P.J.; AZCORRA, A.; SOLÉ-PARETA, J.; DOMINGO-PASCUAL, J.; ÁLVAREZ-CAMPANA, M. “MEHARI: A System for Analyzing the Use of the Internet Services”. “Computer Networks”. 31(21):2293-2307.

[2] VECIANA-NOGUÉS, C.; DOMINGO-PASCUAL, J.; SOLÉ-PARETA, J. “Cost-sharing and Billing in the National Research Networks: the MIRA Approach”. Presentada en: Terena Networking Conference. 2002. Limerick (Irlanda).

[3] VECIANA-NOGUÉS, C.; DOMINGO-PASCUAL, J.; SOLÉ-PARETA, J. “Servers Location & Verification Tool for Backbone Access Points”. Presentada en: 13th ITC Specialist Seminar: IP Traffic Measurement, Modeling and Management. 2000. Monterey (USA).

[4] STILLER, B.; BARLET-ROS, P.; CUSHNIE, J.; DOMINGO-PASCUAL, J.; HUTCHISON, D.; LOPES, R.; MAUTHE, A.; POPA, M.; ROBERTS, J.; SOLÉ-PARETA, J.; TRCEK, D.; VECIANA, C. “Pricing and QoS”. Capítulo 6 de: “Quality of future Internet Services”. Springer-Verlag. 2003.

[5] VECIANA, C.; BARLET-ROS, P.; SOLÉ-PARETA, J.; DOMINGO-PASCUAL, J. “Traffic Accounting and Classification for Cost Sharing in National Research Networks”. 2003. UPC-DAC-2003-24. http://www.ac.upc.es/pub/reports/DAC/2003/UPC-DAC-2003-24.ps.Z

[6] CISCO SYSTEMS. “NetFlow Services Solutions Guide”. 2001. http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.pdf

[7] MOORE, D; KEYS, K.; KOGA, R.; LAGACHE, E.; CLAFFY, K. “The CoralReef Software suite as a tool for system and network administrators”. 2001. http://www.caida.org/outreach/papers/2001/CoralApps/CoralApps.pdf

[8] ENDACE MEASUREMENT SYSTEMS. “DAG 4.2GE Dual Gigabit Ethernet”. 2003. http://www.endace.com/dag4.2ge.htm

Pere Barlet Ros
(pbarlet@ac.upc.es)
Josep Solé Pareta
(pareta@ac.upc.es)
Jordi Domingo Pascual
(jordi.domingo@ac.upc.es)
Centre de Comunicacions Avançades de Banda Ampla (CCABA)
(http://www.ccaba.upc.es)
Dept. Arquitectura de Computadors – UPC