IPmiser[1] : Herramienta de medida y análisis de redes de alta velocidad

Javier Aracil, Daniel Morató y Mikel Izal

Grupo de Redes, Sistemas y Servicios Telemáticos
Departamento de Automática y Computación
Universidad Pública de Navarra
Campus de Arrosadía s/n
31006 PAMPLONA
email: {javier.aracil,daniel.morató,mikel.izal}@unavarra.es
WWW: http://www.tlm.unavarra.es

RESUMEN

Las redes de área extensa IP generan en la actualidad un tráfico difícil de predecir y caracterizar. Así, se hace necesario disponer de herramientas que proporcionen monitorización en tiempo real de los enlaces, sin interrupción y con la máxima fiabilidad y precisión de reloj. La herramienta IPmiser consigue este objetivo mediante un hardware dedicado y una estación de trabajo para el proceso de datos, que es además servidor seguro de información de monitorización.

En este artículo se presenta la arquitectura de IPmiser, junto con los resultados más destacables de diversas mediciones en el enlace IP sobre ATM de la Universidad Publica de Navarra.

`Palabras clave`: medidas de red, sistemas de monitorización, IP sobre ATM, servicios Internet.

1. INTRODUCCIÓN

Las redes de alta velocidad que actualmente constituyen el núcleo de la Internet transportan un tráfico muy poco predecible, por lo que el análisis y dimensionamiento de estas redes se complica. Así, el gestor de red realiza una primera aproximación de diseño asignando un ancho de banda determinado a los enlaces que pone en servicio. Una vez se acomete este primer dimensionamiento es preciso disponer de un equipo que mida las prestaciones reales del enlace, mediante el análisis del tráfico que circula.

En la actualidad se utilizan sistemas basados en sondas de monitorización (*sniffer*) que en mayor o menor medida son capaces de recoger estadísticas de tráfico de la red durante un tiempo limitado. Estos sistemas se construyen con un hardware dedicado que permite la captura de paquetes con una resolución muy alta. Sin embargo, una de sus principales limitaciones es la imposibilidad de captura continua, en el rango de varias horas, dias o incluso semanas. Este aspecto es especialmente importante en redes IP, donde el tráfico es claramente no homogéneo. Precisamente, el tráfico de la Internet presenta características autosimilares. Si consideramos el proceso de llegadas de paquetes por intervalo de duración constante nos encontramos con que el dicho proceso estocástico es invariante en varias escalas de tiempo. Esto es, la varianza o intermitencia del proceso se mantiene independientemente de la escala de tiempo que consideremos, de manera que podemos encontrar ráfagas muy grandes en intervalos de tiempo considerables, que provocarán la sobrecarga de las colas de los routers. La explicación más plausible para este fenómeno se encuentra en un teorema límite que dice que la multiplexación de varias fuentes que producen ráfagas con distribución de Pareto y llegadas exponenciales converge a un Ruido Browniano Fraccional (Fractional Brownian Motion o FBM), que es un proceso autosimilar [4].

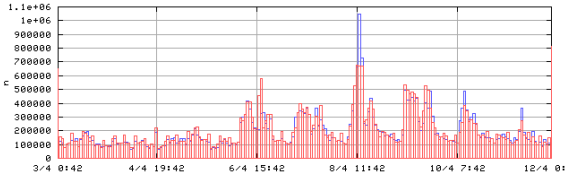

Figura 1 – Tráfico del enlace la Universidad Pública de Navarra con RedIris en una semana

La figura 1 muestra el tráfico del enlace de la Universidad Pública de Navarra (UPNA) durante una semana, donde se observa claramente la existencia de ráfagas en escalas de tiempo muy grandes, con un pico a mitad de semana. A la hora de monitorizar este enlace es necesaria la monitorización continua y no limitada en el tiempo, ya que de otra manera perderíamos el pico de tráfico, que es precisamente lo más interesante a efectos de dimensionamiento de red.

1.1 Monitorización distribuída

Por otro lado, la creciente complejidad de las redes de

[1] La herramienta *IPmiser* se encuentra en proceso de patente. Todos los derechos reservados.

comunicaciones impulsa la idea de monitorización distribuída en contraposición con el carácter centralizado de los equipos de medida actualmente existentes. De esta manera es posible tener un número de supervisores de red que se responsabilizan del correcto funcionamiento de cada una de las subredes. Para hacer esto posible, el sistema de monitorización debe permitir la obtención de *vistas de tráfico*, al igual que una base de datos permite la obtención de vistas de los datos que almacena. La idea consiste en que cada gestor de red tenga acceso únicamente al tráfico que genera su subred pero no al de las otras subredes. En el entorno de RedIris, por ejemplo, se podría asignar a cada gestor de subred (esto es, los responsables de los centros de cálculo de cada una de las universidades conectadas) la vista del tráfico que genera su universidad, para que así tome las medidas oportunas si detecta generación excesiva de tráfico o servidores no deseados, intrusos, etc.

Finalmente, los parámetros de monitorización que los gestores de red exigen conocer son cada vez más variados. No solo bastan los típicos parámetros de número de bytes por protocolo y servicio, numero de conexiones, etc. Hoy en dia debemos estar preparados para calcular en tiempo real parámetros como el jitter de los paquetes de una determinada conexión de Voz sobre IP, realizando además las funciones de tarificación y llevando cuenta de miles de conexiones concurrentemente. En un entorno de alta velocidad esto complica en gran manera el diseño de estas herramientas de monitorización, verdaderos sistemas operativos en tiempo real para propósito especifico de monitorización.

En resumen, tres factores impulsan el diseño de un nuevo equipo de monitorización, el sistema IPmiser:

· La falta de *capacidad de almacenamiento* en los actuales sistemas de monitorización.

· La falta de *flexibilidad* a la hora de permitir que distintos gestores tengan acceso de forma segura y fiable a la información de monitorización, por ejemplo, distintos proveedores de Internet pueden querer información del tráfico que generan, pero sin que sus competidores accedan a esta información.

· La falta de *programabilidad* de las herramienta de monitorización, para las que añadir nuevos parámetros resulta imposible, quedándose obsoletas en muy breve plazo.

El sistema *IPmiser* responde a esta triple necesidad: mayor capacidad de proceso y almacenamiento, distribución de la información de monitorización de forma fiable y segura entre varios gestores y capacidades de reconfiguración de parámetros sin límites. La innovación tecnológica del IPmiser se centra en dos aspectos:

· Arquitectura optimizada para la monitorización de un enlace ATM de alta velocidad (155.5 megabits por segundo): La invención consiste en un hardware dedicado conectado a una estación de trabajo con software de captura de datos y unidad de almacenamiento masivo. Esta unidad de almacenamiento masivo permite el almacenamiento de todas las cabeceras de protocolo IP, TCP, UDP e ICMP aparte de las marcas de tiempo de cada una de las celdas ATM que circulan por el enlace. Así, es posible realizar una auditoria perfecta del enlace a monitorizar, aparte de los estadísticos que, en tiempo real o en diferido, sirve el sistema IPmiser.

· Servidor de información de monitorización basado en tecnología de navegadores de Internet: El propio sistema IPmiser se convierte en servidor de información de monitorización en tiempo real y de días pasados. El sistema permite una jerarquía de supervisores de subredes en lugar de un supervisor centralizado como hasta la fecha. Por otro lado, la información de monitorización se distribuye de forma segura, utilizando mecanismos de autentificación y confidencialidad de datos que se describirán mas adelante. Además, la consola de monitorización no esta ligada a una maquina en concreto sino que esta distribuida en la Internet en forma de navegador estándar de Internet.

En este articulo describimos de forma breve la arquitectura del sistema, junto con un ejemplo de análisis del enlace de la Universidad Pública de Navarra con RedIris. El artículo se estructura como sigue: en el apartado 2 se detalla la arquitectura del sistema y en el apartado 3 se presenta el análisis del enlace de la UPNA, seguido de las conclusiones.

2. ARQUITECTURA DEL SISTEMA IPMISER

El diagrama de bloques del sistema IPmiser se muestra en la figura 2.

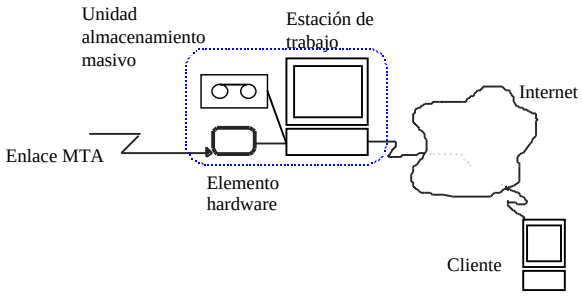

Figura 2 – Diagrama de bloques de *IPmiser*

Un elemento hardware se encarga de la extracción de las celdas del enlace ATM sin perdidas, de manera que las cabeceras de los distintos protocolos se envían a la estación de proceso, que es el núcleo del sistema. Esta estación no solo procesa los datos del enlace sino que sirve la información en tiempo real a traves de la Internet, utilizando encriptación y autentificación.

La estación de trabajo implementa un sistema de clasificación de paquetes que hace que no se pierda información de monitorización.

Precisamente, este algoritmo de clasificación es uno de los principales méritos del sistema. En una red de alta velocidad puede ser necesario calcular miles de parámetros en tiempo real. Por ejemplo puede interesar conocer en detalle el tráfico generado por cada uno de los usuarios, que pueden ser muchos. También puede ser necesario conocer el estado de cada una de las conexiones TCP que circulan por el enlace, para saber exactamente el numero de bytes o duración, o para realizar funciones de tarificación y control de la calidad de servicio.

El lector interesado en una descripción más exhaustiva de este tipo de algoritmos, que han sido desarrollados e implantados en herramientas reales por el Grupo de Redes, Sistemas y Servicios Telemáticos de la UPNA puede acudir a las referencias [3,4,5]. En lo que sigue, vamos a centrarnos en mostrar las funcionalidades de IPmiser a través de un ejemplo de monitorización de un enlace.

3. MONITORIZACIÓN DEL ENLACE DE LA UNIVERSIDAD PÚBLICA DE NAVARRA

El enlace IP sobre ATM a analizar une la UPNA a Rediris, dando servicio a un número aproximado de 1500 usuarios. Los detalles de la medida se resumen en la siguiente tabla:

Fecha de comienzo	Mon 14/12/98 0:00 GMT
Fecha de finalización	Sun 20/12/98 24:00 GMT
Conexiones TCP analizadas	1.700.000
Paquetes IP analizados	9.000.000

Tabla 1 – Datos de la medida

En la tabla se observa que se han analizado 1.700.000 conexiones TCP y unos 9.000.000 de paquetes IP en una semana, sin interrupción. Esto ha sido posible gracias a que IPmiser es capaz de analizar en tiempo real el tráfico del enlace, sin necesidad de guardar en cinta y realizar paradas de análisis.

Protocolo	Bytes (%)	Paquetes (%)
TCP	88.78	79.8
UDP	1.38	5.93
ICMP	0.11	0.37
Otros	9.73	13.9

Tabla 2 – Porcentaje de protocolos

La tabla 2 muestra el porcentaje de tráfico por protocolos en el enlace. Basicamente la mayoría del tráfico son paquetes TCP, lo que es de esperar puesto que es el protocolo que soporta los servicios de WWW, los más populares. Mas en detalle, la tabla 3 muestra los servicios TCP que se han detectado, distinguiendo por el número de puerto.

Servicio (puerto)	Conexiones	%
WWW (80)	1601815	91.71
SMTP (25)	83225	4.76
ProxyWWW (8080)	11957	0.68
FTP-data (20)	9627	0.55
AUTH (113)	5901	0.34
FTP-control (21)	4771	0.27
LOGIN (49)	4080	0.23
HTTPS (443)	3742	0.21
DNS (53)	3532	0.20
POP3 (110)	3265	0.19

Servicio (puerto)	KBytes	%
WWW (80)	12223548	72.91
FTP-data (20)	2134731	12.73
Hotline-data (5501)	445047	2.65
ProxyWWW (8080)	141606	0.84
POP3 (110)	67982	0.41
(50070)	54713	0.33
SMTP (25)	39415	0.24
(65445)	23876	0.14
(33910)	22058	0.13
(1078)	21988	0.13

Table 3 – Servicios analizados

Observemos que hay un número significativo de servicios que generan mucho tráfico con pocas conexiones como por ejemplo AUTH(113), LOGIN(49) y DNS over TCP(53).
El servicios AUTH se usa normalmente con FTP o con otros servicios de transferencia de ficheros para permitir la autentificación del cliente varias veces durante la misma sesión. Por otro lado, otros servicios como Hotline(5501) consumen un porcentaje significativo de recursos de la red (número cuatro en generación de bytes) con muy pocas conexiones (181 en una semana!). Hotline[2] integra una gran variedad de servicios como chat, transferencia de ficheros y news en la misma sesión. Así, las transferencias de ficheros ocasionan un fuerte incremento del número de bytes que produce Hotline. Es importante destacar que estas conexiones no se hubieran detectado de no ser por la monitorización continua del enlace, ya que son muy pocas. Finalmente, observamos bastantes puertos "deconocidos" como el 50070, 65445, 33910 y 1078. Para verificar estos puertos realizamos distintas conexiones a los servidores en cuestión y nos damos cuenta de que pertenecen a servicios FTP. De hecho, algunos servidores FTP no usan el puerto 20 para la conexión de datos iniciada por el servidor en respuesta al comando GET desde el cliente.

Observamos que el tráfico está dominado por el WWW con casi el 75% de ocupación del enlace en bytes y el 90% de conexiones. Como se muestra en la tabla 3, el WWW usa el puerto 80 para conexiones TCP directas y el puerto 8080 para conexiones a través de un proxy. Al WWW le sigue a distancia el FTP (puerto 20 para datos y puerto 21 para control) y Hotline, que es muy similar al FTP debido a las transferencias de ficheros.

Un pequeño porcentaje del tráfico se debe a descarga de email por el servidor POP3 (puerto 110), envio de emails mediante SMTP (puerto 25) y transacciones seguras con HTTPS (puerto 443). Por otro lado, observamos transferencias que se deben el protocolo de las news (NNTP), pero estas se generan periódicamente por el servidor de news de la Universidad y no por los usuarios.

[2] http://www.hotlinesw.com

Un análisis más detallado de las conexiones TCP se muestra en la tabla 4. Observamos que las conexiones WWW son de poco tamaño, con la media en 6.5 Kbytes y el 99% de la distribución por debajo de 70 KB. También observamos una fuerte asimetría de las conexiones hacia el lado del servidor, excepto con SMTP, que es asimétrico en el otro sentido.

	Bytes por conexión		Duración
Servicio	cli -> ser	ser -> cli	(s)
WWW	0.5 KB	6.5 KB	16.5
SMTP	23.4 KB	0.4 KB	43
POP3	0.06 KB	18.6 KB	19.4
FTPdata	5.2 KB	212.5 KB	13
Telnet	0.2 KB	8.9 KB	110

Tabla 4 – Características de conexiones TCP

Por ultimo, la figura 3 muestra el número de conexiones TCP simultáneas en el enlace. La gráfica es interesante porque muestra el numero de operaciones de conmutación de flujos que un hipotético router con IP switching debería realizar, si se pretendieran conmutar las conexiones TCP por separado con distintas calidades de servicio. También es interesante porque muestra el número de conexiones que en un momento dado han estado siendo analizadas por el kernel del IPmiser. Para cada una de estas conexiones se mantuvo en cada momento un registro de su estado, atendiendo a la maquina de estados TCP. Así, la complejidad de llevar la cuenta del estado de cada una de las conexiones exige la puesta en marcha de algoritmos de filtrado y análisis de tráfico, como se ha comentado anteriormente.

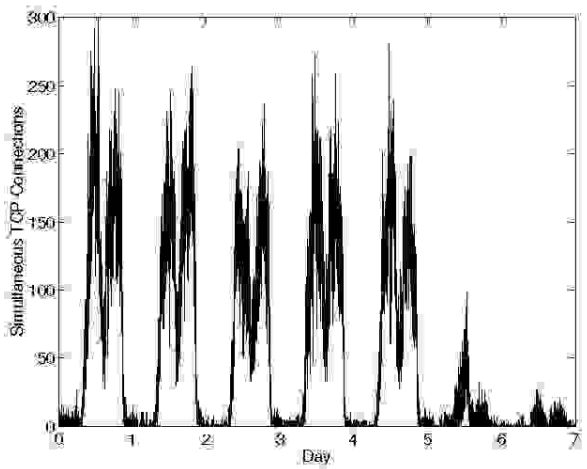

Figura 3 – Número de conexiones TCP simultaneas

4 . CONCLUSIONES

En este artículo se ha presentado de forma muy breve el sistema IPmiser, junto con un ejemplo de las medidas que se han realizado en el enlace IP sobre ATM de la UPNA-Rediris. La flexibilidad del sistema es practicamente total en cuanto a mediciones de parámetros, puesto que solo es necesaria la modificación del kernel de filtrado, escrito en C sobre Solaris. Así, se realizan medidas de traffic shaping emulado para redes IP sobre WDM, modelización estocástica de conexiones TCP para IP swicthing, etc. Un ejemplo de estos calculos puede encontrarse en [1].

5. AGRADECIMIENTOS

Los autores agradecen a Telefónica I+D por su patrocinio en el diseño de la herramienta y por la realización diseño hardware.

6. REFERENCIAS

[1] J. Aracil, D. Morató, M. Izal, “Analysis of Internet Services for IP over ATM”, *IEEE Communications Magazine*, aceptado para publicación en el número de Diciembre 1999.

[2] M. E. Crovella and A. Bestavros, ``Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes,'' in IEEE/ACM Transactions on Networking, 5(6):835--846, December 1997.

[3] E. Magaña, J. Aracil, J. Villadangos, “PROMIS: A reliable tool for real-time network monitoring “, *IEEE Euromicro 1998*, Vaasteras, Suecia, Agosto 1998.

[4] E. Magaña, J. Villadangos, J. Aracil, J. R. González de Mendivil, “Reliable Network Management Tool through Internet”, *Proceedings of Seventeenth IASTED Inernational Conference on Applied Informatics*, Innsbruck, Austria, Febrero 1999.

[5] J. Ruiz, E. Magaña, J. Aracil y J. Villadangos, “Tecnicas de filtrado y analisis de paquetes para análisis de tráfico”. *Procedings JITEL 99*, Madrid, Septiembre 1999.