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

Javier Aracil, Daniel Morat y Mikel Izal

Grupo de Redes, Sistemas y Servicios Telem ticos
Departamento de Autom tica y Computaci n
Universidad P blica de Navarra
Campus de Arrosad a s/n
31006 PAMPLONA
email: {javier.aracil,daniel.morat ,mikel.izal}@unavarra.es
WWW: http://www.tlm.unavarra.es

RESUMEN

Las redes de rea extensa IP generan en la actualidad un tr fico dif cil de predecir y caracterizar. As , se hace necesario disponer de herramientas que proporcionen monitorizaci n en tiempo real de los enlaces, sin interrupci n y con la m xima fiabilidad y precisi n de reloj. La herramienta IPmiser consigue este objetivo mediante un hardware dedicado y una estaci n de trabajo para el proceso de datos, que es adem s servidor seguro de informaci n de monitorizaci n.

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

Palabras clave: medidas de red, sistemas de monitorizaci n, IP sobre ATM, servicios Internet.

1. INTRODUCCI N

Las redes de alta velocidad que actualmente constituyen el n cleo de la Internet transportan un tr fico muy poco predecible, por lo que el an lisis y dimensionamiento de estas redes se complica. As , el gestor de red realiza una primera aproximaci n de dise o 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 an lisis del tr fico que circula.

En la actualidad se utilizan sistemas basados en sondas de monitorizaci n (*sniffer*) que en mayor o menor medida son capaces de recoger estad sticas de tr fico de la red durante un tiempo limitado. Estos sistemas se construyen con un hardware dedicado que permite la captura de paquetes con una resoluci n 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 tr fico es claramente no homog neo. Precisamente, el tr fico de la Internet presenta caracter sticas autosimilares. Si consideramos el proceso de llegadas de paquetes por intervalo de duraci n constante nos encontramos con que el dicho proceso estoc stico 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 r fagas muy grandes en intervalos de tiempo considerables, que provocar n la sobrecarga de las colas de los routers. La explicaci n m s plausible para este fen meno se encuentra en un teorema l mite que dice que la multiplexaci n de varias fuentes que producen r fagas con distribuci n de Pareto y llegadas exponenciales converge a un Ruido Browniano Fraccional (Fractional Brownian Motion o FBM), que es un proceso autosimilar [4].

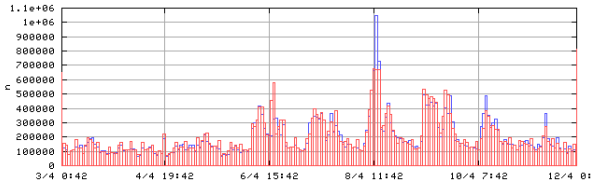

Figura 1 — Tr fico del enlace la Universidad P blica de Navarra con RedIris en una semana

La figura 1 muestra el tr fico del enlace de la Universidad P blica de Navarra (UPNA) durante una semana, donde se observa claramente la existencia de r fagas en escalas de tiempo muy grandes, con un pico a mitad de semana. A la hora de monitorizar este enlace es necesaria la monitorizaci n continua y no limitada en el tiempo, ya que de otra manera perder amos el pico de tr fico, que es precisamente lo m s interesante a efectos de dimensionamiento de red.

1.1 Monitorizaci n distribu da

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 monitorizaci n distribu da en contraposici n con el car cter centralizado de los equipos de medida actualmente existentes. De esta manera es posible tener un n mero de supervisores de red que se responsabilizan del correcto funcionamiento de cada una de las subredes. Para hacer esto posible, el sistema de monitorizaci n debe permitir la obtenci n de *vistas de tr fico,* al igual que una base de datos permite la obtenci n de vistas de los datos que almacena. La idea consiste en que cada gestor de red tenga acceso nicamente al tr fico que genera su subred pero no al de las otras subredes. En el entorno de RedIris, por ejemplo, se podr a asignar a cada gestor de subred (esto es, los responsables de los centros de c lculo de cada una de las universidades conectadas) la vista del tr fico que genera su universidad, para que as tome las medidas oportunas si detecta generaci n excesiva de tr fico o servidores no deseados, intrusos, etc.

Finalmente, los par metros de monitorizaci n que los gestores de red exigen conocer son cada vez m s variados. No solo bastan los t picos par metros de n mero de bytes por protocolo y servicio, numero de conexiones, etc. Hoy en dia debemos estar preparados para calcular en tiempo real par metros como el jitter de los paquetes de una determinada conexi n de Voz sobre IP, realizando adem s las funciones de tarificaci n y llevando cuenta de miles de conexiones concurrentemente. En un entorno de alta velocidad esto complica en gran manera el dise o de estas herramientas de monitorizaci n, verdaderos sistemas operativos en tiempo real para prop sito especifico de monitorizaci n.

En resumen, tres factores impulsan el dise o de un nuevo equipo de monitorizaci n, el sistema IPmiser:

- La falta de *capacidad de almacenamiento* en los actuales sistemas de monitorizaci n.

- La falta de *flexibilidad* a la hora de permitir que distintos gestores tengan acceso de forma segura y fiable a la informaci n de monitorizaci n, por ejemplo, distintos proveedores de Internet pueden querer informaci n del tr fico que generan, pero sin que sus competidores accedan a esta informaci n.

- La falta de *programabilidad* de las herramienta de monitorizaci n, para las que a adir nuevos par metros resulta imposible, qued ndose obsoletas en muy breve plazo.

El sistema *IPmiser* responde a esta triple necesidad: mayor capacidad de proceso y almacenamiento, distribuci n de la informaci n de monitorizaci n de forma fiable y segura entre varios gestores y capacidades de reconfiguraci n de par metros sin l mites. La innovaci n tecnol gica del IPmiser se centra en dos aspectos:

- Arquitectura optimizada para la monitorizaci n de un enlace ATM de alta velocidad (155.5 megabits por segundo): La invenci n consiste en un hardware dedicado conectado a una estaci n 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. As , es posible realizar una auditoria perfecta del enlace a monitorizar, aparte de los estad sticos que, en tiempo real o en diferido, sirve el sistema IPmiser.

- Servidor de informaci n de monitorizaci n basado en tecnolog a de navegadores de Internet: El propio sistema IPmiser se convierte en servidor de informaci n de monitorizaci n en tiempo real y de d as pasados. El sistema permite una jerarqu a de supervisores de subredes en lugar de un supervisor centralizado como hasta la fecha. Por otro lado, la informaci n de monitorizaci n se distribuye de forma segura, utilizando mecanismos de autentificaci n y confidencialidad de datos que se describir n mas adelante. Adem s, la consola de monitorizaci n no esta ligada a una maquina en concreto sino que esta distribuida en la Internet en forma de navegador est ndar de Internet.

En este articulo describimos de forma breve la arquitectura del sistema, junto con un ejemplo de an lisis del enlace de la Universidad P blica de Navarra con RedIris. El art culo se estructura como sigue: en el apartado 2 se detalla la arquitectura del sistema y en el apartado 3 se presenta el an lisis 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.

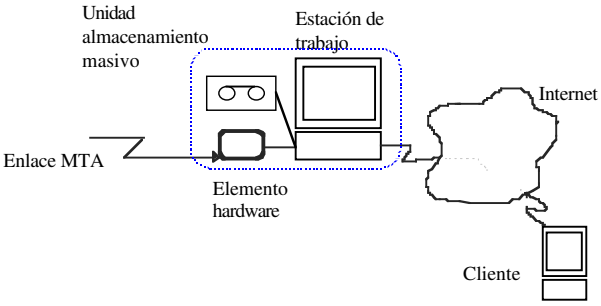

Figura 2 — Diagrama de bloques de *IPmiser*

Un elemento hardware se encarga de la extracci n de las celdas del enlace ATM sin perdidas, de manera que las cabeceras de los distintos protocolos se env an a la estaci n de proceso, que es el n cleo del sistema. Esta estaci n no solo procesa los datos del enlace sino que sirve la informaci n en tiempo real a traves de la Internet, utilizando encriptaci n y autentificaci n.

La estaci n de trabajo implementa un sistema de clasificaci n de paquetes que hace que no se pierda informaci n de monitorizaci n.

Precisamente, este algoritmo de clasificaci n es uno de los principales m ritos del sistema. En una red de alta velocidad puede ser necesario calcular miles de par metros en tiempo real. Por ejemplo puede interesar conocer en detalle el tr fico generado por cada uno de los usuarios, que pueden ser muchos. Tambi n 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 duraci n, o para realizar funciones de tarificaci n y control de la calidad de servicio.

El lector interesado en una descripci n m s exhaustiva de este tipo de algoritmos, que han sido desarrollados e implantados en herramientas reales por el Grupo de Redes, Sistemas y Servicios Telem ticos 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 trav s de un ejemplo de monitorizaci n de un enlace.

3. MONITORIZACI N DEL ENLACE DE LA UNIVERSIDAD P BLICA DE NAVARRA

El enlace IP sobre ATM a analizar une la UPNA a Rediris, dando servicio a un n mero 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 finalizaci n	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 interrupci n. Esto ha sido posible gracias a que IPmiser es capaz de analizar en tiempo real el tr fico del enlace, sin necesidad de guardar en cinta y realizar paradas de an lisis.

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 tr fico por protocolos en el enlace. Basicamente la mayor a del tr fico son paquetes TCP, lo que es de esperar puesto que es el protocolo que soporta los servicios de WWW, los m s populares. Mas en detalle, la tabla 3 muestra los servicios TCP que se han detectado, distinguiendo por el n mero 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 n mero significativo de servicios que generan mucho tr fico 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 autentificaci n del cliente varias veces durante la misma sesi n. Por otro lado, otros servicios como Hotline(5501) consumen un porcentaje significativo de recursos de la red (n mero cuatro en generaci n 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 sesi n. As , las transferencias de ficheros ocasionan un fuerte incremento del n mero de bytes que produce Hotline. Es importante destacar que estas conexiones no se hubieran detectado de no ser por la monitorizaci n 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 cuesti n y nos damos cuenta de que pertenecen a servicios FTP. De hecho, algunos servidores FTP no usan el puerto 20 para la conexi n de datos iniciada por el servidor en respuesta al comando GET desde el cliente.

Observamos que el tr fico est dominado por el WWW con casi el 75% de ocupaci n 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 trav s 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 peque o porcentaje del tr fico 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 peri dicamente por el servidor de news de la Universidad y no por los usuarios.

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

Un an lisis m s detallado de las conexiones TCP se muestra en la tabla 4. Observamos que las conexiones WWW son de poco tama o, con la media en 6.5 Kbytes y el 99% de la distribuci n por debajo de 70 KB. Tambi n observamos una fuerte asimetr a de las conexiones hacia el lado del servidor, excepto con SMTP, que es asim trico en el otro sentido.

Servicio	Bytes por conexi n		Duraci n
	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 — Caracter sticas de conexiones TCP

Por ultimo, la figura 3 muestra el n mero de conexiones TCP simult neas en el enlace. La gr fica es interesante porque muestra el numero de operaciones de conmutaci n de flujos que un hipot tico router con IP switching deber a realizar, si se pretendieran conmutar las conexiones TCP por separado con distintas calidades de servicio. Tambi n es interesante porque muestra el n mero 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. As , la complejidad de llevar la cuenta del estado de cada una de las conexiones exige la puesta en marcha de algoritmos de filtrado y an lisis de tr fico, como se ha comentado anteriormente.

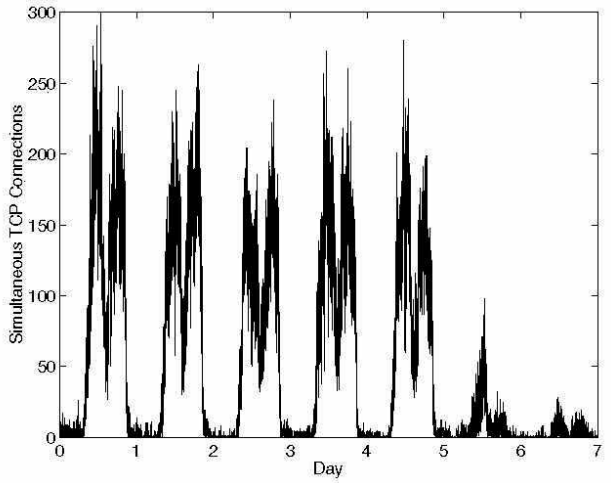

Figura 3 — N mero de conexiones TCP simultaneas

4 . CONCLUSIONES

En este art culo 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 par metros, puesto que solo es necesaria la modificaci n del kernel de filtrado, escrito en C sobre Solaris. As , se realizan medidas de traffic shaping emulado para redes IP sobre WDM, modelizaci n estoc stica de conexiones TCP para IP swicthing, etc. Un ejemplo de estos calculos puede encontrarse en [1].

5. AGRADECIMIENTOS

Los autores agradecen a Telef nica I+D por su patrocinio en el dise o de la herramienta y por la realizaci n dise o hardware.

6. REFERENCIAS

[1] J. Aracil, D. Morat , M. Izal, Analysis of Internet Services for IP over ATM , *IEEE Communications Magazine,* aceptado para publicaci n en el n mero 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. Maga a, J. Aracil, J. Villadangos, PROMIS: A reliable tool for real-time network monitoring , *IEEE Euromicro 1998*, Vaasteras, Suecia, Agosto 1998.

[4] E. Maga a, J. Villadangos, J. Aracil, J. R. Gonz lez 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. Maga a, J. Aracil y J. Villadangos, Tecnicas de filtrado y analisis de paquetes para an lisis de tr fico . *Procedings JITEL 99,* Madrid, Septiembre 1999.