Realización de Medidas de Tráfico utilizando NeTraMet

Pablo L.-Matencio, Sergio Almagro, Fernando Cerdan
Departamento de Tecnologías de la Información y las Comunicaciones,
Universidad Politécnica de Cartagena
Campus Muralla del Mar. Edificio Antiguo Hospital de Marina
Telf: 968326585, Fax: 968325973
E-mail: {pablo.lopez, fernando.cerdan}@upct.es

Resumen. *La medición de tráfico basada en flujos proporciona una reducción del volumen de datos recolectados en tiempo real. RTFM es un estándar del IETF que define una arquitectura para la medición de flujos de tráfico y, NeTraMet es una implementación de dicha arquitectura. En este artículo presentamos una introducción de NeTraMet, de sus componentes, y de las distintas formas de configuración para realizar medidas de flujos de tráfico.*

1 Introducción

La realización de medidas de tráfico ha ido ganando interés por parte de los operadores con el fin de conocer mejor el funcionamiento de sus redes. Este conocimiento les permitirá optimizar recursos físicos, tales como routers, switches y líneas alquiladas de comunicación. Además, la información de tráfico es fundamental para realizar soporte (detectando funcionamiento incorrecto de equipos), para obtener datos de uso (usuarios conectados, detección de ataques, facturación) y para la planificación de ampliación de la infraestructura de red.

Una forma de medir tráfico consistiría en realizar copias de paquetes (o sólo sus cabeceras), y guardarlas en un archivo en disco para su análisis posterior, tal y como hace tcpdump [1].

Este método de medir tráfico guardando información de los paquetes en un archivo en disco tiene fundamentalmente dos ventajas. La primera, es que, al tener información de cada paquete, podemos analizarlos desde varios enfoques, aportándonos diversos aspectos relacionados con el comportamiento del tráfico. Lo segundo, es que podemos recopilar la información a alta velocidad, normalmente el límite lo impone la velocidad de escritura del disco. La desventaja de este método es que, al guardar un registro de cada uno de los paquetes, los archivos pueden llegar a ser muy grandes.

Otra forma de medir tráfico consiste en guardar 'flujos' en lugar de paquetes. Podemos ver un flujo de tráfico como una secuencia de paquetes yendo desde una dirección IP a otra, y, por lo tanto, estaría definida sólo por las direcciones IP de la fuente y del destino. A menudo, también identificamos los flujos con mayor detalle, por ejemplo, mediante cinco datos (protocolo, direcciones IP fuente y destino, puertos de la fuente y del destino); en los dos casos, el flujo tendría un carácter unidireccional.

Un 'medidor' de flujos observa los paquetes y construye tablas con información de los flujos, identificando cada flujo mediante los cinco datos que hemos citado, y les asocia, también, contadores de paquetes y de bytes. Los puntos de medición habitualmente son los routers y switches; un ejemplo bastante conocido es Cisco NetFlow [2]. Existen herramientas de libre distribución capaces de recoger y analizar datos de NetFlow, tales como, cflowd [3] y NeTraMet [4].

Los datos obtenidos con NetFlow proporcionan una buena visión del tráfico que cursa un router o un switch, pero los flujos están limitados a los cinco datos antes mencionados. Sin embargo, la arquitectura RTFM (que describimos a continuación) proporciona una forma para que el usuario especifique qué flujos deben medirse. Además, los flujos en RTFM, son bidireccionales, disponiendo contadores de bytes y de paquetes para los dos sentidos del flujo.

RMON es un sistema de supervisión remota de redes del IETF, y es una tercera vía para medir el tráfico de una red. Un agente RMON (normalmente imbuido en el software de un router o switch) implementa una MIB [5]. RMON permite al administrador de la red determinar, entre otros valores, niveles de tráfico en los segmentos de la red, cargas totales de tráfico (entrada y salida) en un ordenador, cargas de tráfico entre pares de computadoras, y todo ello para diferentes protocolos. Sin embargo, RMON no tiene capacidad para medir flujos.

1.1 RTFM y NeTraMet

El Internet Engineering Task Force (IETF) es la organización que produce los estándares de carácter técnico para Internet, publicados como RFC (Request for Comment).

En 1995 se formó el grupo de trabajo que desarrollo la arquitectura de realización de medidas de tráfico

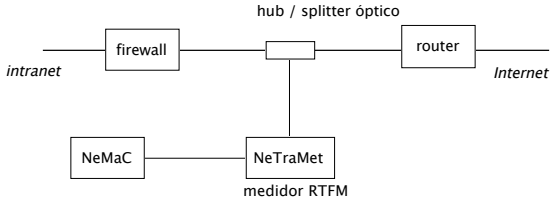

Fig. 1 Medidor de tráfico en un punto de la red

denominada Real Time Flow Meassurement (RTFM). Esta arquitectura define tres entidades de red:

- Medidores: registran datos de los paquetes, y los organizan en forma de datos de flujo. Los flujos son bi-direccionales y están identificados por atributos de los elementos extremos.
- Colectores: recogen datos de los medidores usando SNMP.
- Administradores: coordinan el funcionamiento de los medidores y los colectores.

La arquitectura RTFM queda recogida en las RFCs 2720-2724 publicadas en 1999.

NeTraMet es la primera implementación de la arquitectura RTFM y su código está distribuido como Gnu Public License (GPL). Proporciona un conjunto de herramientas para la medición de flujos de tráfico, incluyendo:

- medidores (NeTraMet, NetFlowMet)
- administrador/colector (NeMac)
- un compilador como ayuda a la generación de archivos de configuración de los medidores (srl)
- programas adicionales (fd_filter, fd_extract)

Hasta ahora, NeTraMet es la única implementación en código abierto de la arquitectura RTFM.

2 Medición de Flujos de Tráfico con NeTraMet

Podemos realizar mediciones de flujos de tráfico en varias ubicaciones de la red. En principio, situaremos los medidores NeTraMet en los puntos de la red que deseemos medir, y, uno o más NeMaC (administrador/colector) en algún punto que sea conveniente para el administrador de la red. NeMaC configura los medidores mediante un conjunto de reglas (en RTFM las reglas describen los flujos que debe medir el medidor), recoge, periódicamente, los datos registrados por los medidores, y los guarda en archivos de datos de flujo.

Seguidamente veremos tres ejemplos sobre cómo situar los medidores en una red.

2.1 Medidor para observar el tráfico entrante/saliente de una intranet

La Fig. 1 muestra un medidor NeTraMet, situado en un ordenador con Unix o Linux, que observa los paquetes que atraviesan el gateway (router) de la red. Los paquetes llegan al gateway desde Internet (a la derecha del esquema). Desde el gateway, los paquetes llegan al firewall, y desde ahí a la intranet. En este ejemplo, todo el tráfico pasa a través de un sólo punto, donde situaremos el medidor del tráfico de entrada/salida desde/hacia Internet.

Existen varias formas de pasar los paquetes por un medidor NeTraMet. Si la red donde está el gateway es una Ethernet, entonces, podemos utilizar un hub que facilitaría una copia de todos los paquetes (entrantes y salientes) a NeTraMet. Si el gateway fuera un ordenador con Unix o Linux con capacidad de encaminar paquetes, entonces, el medidor NeTraMet podría ejecutarse también en este equipo, donde analizaría las cabeceras de los paquetes. Finalmente, si la conexión a Internet fuera con fibra, podríamos utilizar una pareja de splitters ópticos (uno para cada sentido del tráfico), que facilitaría la copia de los paquetes a un par de tarjetas de red ópticas situadas en el equipo donde instalemos NeTraMet.

A la izquierda del medidor tenemos otro ordenador con Unix o Linux y NeMaC instalado, que combina un administrador y un colector RTFM. NeMaC configura las reglas y las descarga en el medidor NeTraMet (indicándole qué flujos debe medir y el nivel de detalle requerido para cada flujo). También lee, en periodos de tiempo seleccionados por el administrador, los datos de flujo que obtiene el medidor, y los escribe en un archivo.

Aunque hemos situado a NeTraMet y NeMaC en equipos distintos, podríamos instalarlos en el mismo ordenador. En nuestro ejemplo, al tener sólo un medidor, lo más sensato sería instalar NeTraMet y NeMaC en la misma plataforma, evitando de este modo posibles retardos en la transferencia de las PDUs SNMP entre el medidor y el colector.

2.2 Varios medidores y un colector

En la Fig. 2 tenemos varios medidores (NeTraMet o NetFlowMet) observando los flujos de tráfico en varios puntos de la red (por ejemplo en varios ISPs). Hay un sólo administrador / colector (NeMaC) en la parte inferior izquierda del esquema, que descarga las reglas RTFM a todos los medidores, y recopila datos de flujo a intervalos periódicos.

Esta configuración requiere una buena conectividad entre NeMaC y los medidores, de forma que los datos lleguen a NeMaC a intervalos de tiempo mucho más

pequeños que los periodos de lectura de los datos de cada medidor.

Podría resultar útil situar dos entidades NeMaC, las dos recopilando datos de flujo de todos los medidores, para así, tener redundancia de los datos recolectados. Igualmente, podríamos tener varios medidores observando el tráfico de un sólo punto de la red.

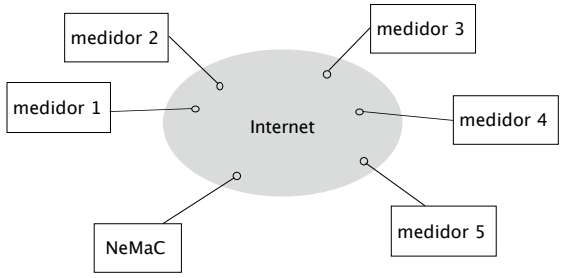

Fig. 2 Medidores en diversos puntos de la red

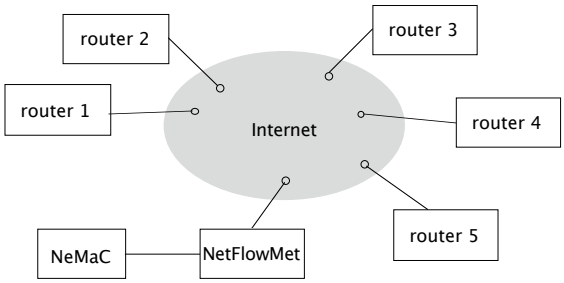

Fig. 3 Un medidor recogiendo datos NetFlow de diversos puntos de la red

2.3 Medidor NetFlowMet recogiendo los datos NetFlow de varios routers Cisco

Este ejemplo es similar al anterior, con la excepción que ahora utilizamos NetFlowMet (medidor RTFM para datos NetFlow) para obtener los datos procedente de los routers Cisco situados en diversos puntos de la red.

Tal y como apreciamos en la Fig. 3, NeMaC es un ordenador con Unix o Linux, encargado de proporcionar a NetFlowMet las reglas que indiquen las características de los flujos a medir, así como de leer los datos de flujo observados por el medidor.

Si utilizamos routers Cisco, NetFlow proporciona una forma sencilla de obtener información de sus interfaces. Al configurar NetFlow en el router debemos tener en cuenta que puede afectar su funcionamiento. Un router con interfaces de red de alta velocidad puede generar gran cantidad de datos NetFlow. Esto nos sugiere emplazar el NetFlowMet en la misma red donde dan servicio los routers que vamos a medir o, al menos, en el mismo Point of Presence o PoP que sirve a los routers observados.

Configurándolo de esta forma, NetFlowMet proporciona una forma adecuada de agregar datos NetFlow de varios routers, resultando una alternativa a otras herramientas existentes, como, por ejemplo, cflowd [3].

3 Conclusiones

RTFM proporciona un entorno general para la realización de medidas de flujos de tráfico de forma distribuida y asíncrona. La definición de flujo RTFM como una entidad bi-direccional determinada sólo por los atributos de los extremos de la comunicación resulta bastante potente, como lo demuestra la posibilidad de definir la información a recolectar mediante reglas expresadas mediante el lenguaje SRL.

NeTraMet es una implementación RTFM de código abierto y libre distribución, que proporciona un conjunto de herramientas para la medición de flujos de tráfico. Poner en funcionamiento los componentes de una plataforma NeTraMet requiere cierto esfuerzo, pero con ello conseguiremos adaptarla a nuestra necesidad de medición de flujos de tráfico. Los componentes de NeTraMet (medidores, colectores, administradores, reglas y lenguaje SRL) permiten al usuario la posibilidad de obtener cualquier informe que necesite.

Referencias

[1] V. Jacobson, C. Leres, and S. McCanne, *tcpdump*, disponible en http://www.tcpdump.org/

[2] *NetFlow Services and Applications (and introduccition and overview)*, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm

[3] *cflowd*, http://www.caida.org/tools/measurement/cflowd/

[4] NeTraMet, http://www.auckland.ac.nz/net/NeTraMet

[5] Waldbusser, *Remote Network Monitoring Management Information Base*, RFC 2819, May 2000.