Traffic Flow Measurements within IP Networks: Requirements, Technologies, and Standardization

Jürgen Quittek
Network Laboratories, NEC Europe Ltd.
Adenauerplatz 6
69115 Heidelberg, Germany
quittek@ccrle.nec.de

Tanja Zseby, Georg Carle, Sebastian Zander
FhI FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
{zseby,carle,zander}@fokus.gmd.de

Abstract

This contribution gives an overview of applications requiring detailed flow-based traffic measurements within IP routers or probes. From the applications, requirements for these measurements are derived and compared to the capabilities of existing technologies. Finally, current activities at the IETF on standardizing the export of flow information out of routers to data collectors are summarized.

1. Introduction

With the steady growth of the Internet and with voice over IP services, the need to conduct detailed measurements of IP traffic flows increases for several reasons including charging and traffic engineering issues. But so far there is no commonly accepted standard technology matching the requirements for traffic flow measurements. A standardized MIB module by the IETF called Meter MIB [1] lacks acceptance in industry. Currently, the dominating technology is NetFlow [4] from Cisco. However, several manufacturers recently developed competing technologies [2, 5, 7], and the IETF has started again working in this area [6].

2. Applications requiring flow measurements

Four application areas requiring traffic flow measurements are discussed below. Out of these we consider usage-based accounting to be the main driver for current technology developments. Further application areas not discussed here include traffic profiling and network surveillance.

Usage-based accounting serves as input to charging and billing for IP services. Several new business models for selling IP service and IP-based services are currently under investigation. Accounting for these models can be based on time or volume, and it can be performed per user group, per user, individually per high-level service, or even per content type delivered. For advanced future services, accounting may also be performed per class of service, per applications, per time of day, per used (label switched) path, etc. Consequently, flexible and fine-grained traffic flow measurement systems are required to satisfy the upcoming needs.

Traffic engineering (TE) aims at optimization of network resource utilization and traffic performance. Traffic measurements serve as input to TE. Required measurements include link utilization, load between particular network nodes, and number, size and entry/exit points of current active flows. On congested links, detailed information on which traffic contributes to the congestion is required.

QoS monitoring is the non-intrusive (passive) measurement of quality parameters for single flows or traffic aggregates, e.g. for validating of QoS parameters negotiated in a service level agreement (SLA). QoS monitoring often needs the correlation of data from multiple measurement instances, e.g. for measuring one-way metrics. This requires proper clock synchronization of the involved measuring devices.

Attack/intrusion detection. Capturing of flow information plays an important role in network security, both for detection of security violation and for subsequent defence. Flow analysis is used for gathering information about the attacking flows or acts of intrusion. Consequently, attack/intrusion detection requires means for detailed flow measurement and analysis.

3. Requirements

From the applications listed above we derived a set of requirements concerning distinguishing flows, the metering

process, and the data transfer from measuring devices to data collectors. A detailed description of these requirements is given in [6]. For distinguishing flows we use the following definition of the term *flow*:

> A flow is a set of packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties derived from the data contained in the packet and from the packet treatment at the observation point.

The observation point may be a network interface of a device, a probe, or an entire router. Properties derived from packet treatment include for example the interface at which the flow arrived.

The definition covers the range from a flow containing all packets observed at a network interface to a flow consisting of just a single packet with a specific sequence number. Please note that the definition does not match a general application-level end-to-end stream, because it is only based on observing a single point in the network.

As properties for distinguishing flows, we consider the five-tuple of source and destination IP and tranport addresses and the transport type to be essential as well as the incoming or outgoing interface where the flow was observed. In presence of MPLS or Differentiated Services, also the MPLS label (see RFC 3031) and the DiffServ code point (see RFC 2474) are essential.

Requirements for the metering process concern reliability of measurements, timestamps and timeouts. Timestamps are required for correlating measurements at different points in a network and for time-based accounting. Finally, timeouts should help to close accounts, when a connection was terminated or is unused for some time.

Requirements for the data transfer from measuring devices to data collectors include reliability again, but also security issues including confidentiality, integrity and authenticity. As basic reporting mode, push mode (initiated by the measuring device) is to be preferred to pull mode (initiated by the data collector). A requirement to the the data model used for the transfer is openness to future extensions.

4. Technologies

The following technologies are currently competing in the area of IP traffic flow measurements:

The Meter MIB [1] standardized by the IETF is a MIB module intergrated into the Internet SNMP management framework. It meets almost all requirements except that it operates in pull mode. Its further drawbacks are high complexity and performance limitations, because of that its acceptance at hardware manufacturers is very limited.

Cisco NetFlow [4] is a feature available on almost all Cisco routers which almost makes it the de-facto standard. It conducts per-flow measurements and meets most of the listed requirements. However, it lacks scalability and extensibility. Therefore, Cisco has started to develop a new version that matches the requirements much better.

Diameter [3] is a protocol under standardidzation by the IETF for purposes of authentication, authorization and accounting. It is reliable and very flexible concerning the data format. However, the implementation is rather complex and it generates a large communication overhead.

LFAP [2] and the CRANE protocol [7] can be seen as compromizes between NetFlow and Diameter. They are sufficiently reliable and flexible, but their overhead is much smaller than Diameter's one.

sFlow [5] differs from the other mentioned technologies by focussing traffic measurement based on packet sampling. Therefore its accuracy is much lower and the range of applications is more restricted.

5. Standardization

In October 2001 the IETF chartered a new working group on Internet Protocol Flow Information eXport (IPFIX). The tasks of the working group include developing a requirements specification of a protocol for exporting measured traffic flow data from a measuring device to a data collector [6], designing an architecture for traffic flow measurements, defining a data model for this purpose, and selecting (or defining) a suited transport protocol.

References

[1] N. Brownlee. *Traffic Flow Measurement: Meter MIB.* IETF, RFC 2720, October 1999.

[2] P. Calato and M. MacFaden. *Light-weight Flow Accounting Protocol Specification Version 5.0.* Internet draft draft-riverstone-lfap-00.txt, work in progress, June 2001.

[3] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, and G. Zorn. *Diameter Base Protocol*. Internet draft draft-ietf-aaa-diameter-07.txt, work in progress, July 2001.

[4] Cisco Systems. Netflow services solutions guide. *white paper, http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.pdf*, July 2001.

[5] P. Phaal, S. Panchen, and N. McKee. *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks.* IETF, RFC 3176, September 2001.

[6] J. Quittek, T. Zseby, G. Carle, S. Zander, and B. Claise. *Requirements for IP Flow Export*. Internet draft draft-ietf-ipfix-reqs-00.txt, work in progress, October 2001.

[7] K. Zhang and E. Elkin. *Common Reliable Accounting for Network Element (CRANE)*. Internet draft draft-kzhang-crane-protocol-00.txt, work in progress, June 2001.