nFlow: Monitoring Flows on IPv4/v6 Networks

Luca Deri
NETikos S.p.A.
c/o Telecom Italia, Via del Brennero Km 4
56123 Pisa, Italy
Email: luca.deri@netikos.com

Abstract

Cisco NetFlow V5 is a popular flow format used for network monitoring. Unfortunately its format is not open and it has been designed only for IPv4 network monitoring. Other limitations include lack of payload access and insecure flow transmission.
nFlow is an open flow format defined by the author, which overcomes the above limitations. This paper describes the design and implementation of an nFlow probe, and positions this work with respect to similar efforts of both Cisco and the IETF IPFIX working group.

Keywords
Network monitoring, Cisco NetFlow.

1. Introduction

Cisco NetFlow is a popular protocol used for monitoring network traffic. Mid-high level network routers usually include a NetFlow probe that, based on the routed traffic, sends flows to one or more collectors that compute traffic statistics. The most popular NetFlow versions are v5 and v8. These two main NetFlow limitations are:

- The flow format is fixed and defined by Cisco.
- Only IPv4 is supported (i.e. no IPv6 support).

Recently Cisco has decided to define a new flow version named v9 [1] that overcomes the above limitations and finally allows third party to extend the flow format including non-standard information. The IETF IPFIX (Internet Protocol Flow Information export) [2] working group is also working at a new format that is basically NetFlow v9 with very limited changes.

Although there are several ongoing activities in the NetFlow arena, the author has decided to define a new flow format named *nFlow* that introduces several new features with respect to both NetFlow v9 and IPFIX. This format has been submitted to IETF IPFIX for consideration during the 57th IETF meeting, and it has been implemented in *nProbe* and *ntop*, two open source applications developed by the author and freely available on the Internet.

2. The nFlow Format

From the experience learnt running the ntop project for more than six years, the author has realized that:

- Modern protocols use dynamic IP ports hence it is necessary to have a limited access to the initial payload information in order to characterize the traffic.
- The ICMP protocol is very important for knowing the health of a network hence it should be monitored very precisely
- A probe can calculate simple network performance figures (e.g. network latency) with very little effort; hence performance data should be exported into the flow.

The idea behind nFlow is to exploit some of the principles on which NetFlow v9 is based and enhance it with new features just listed. nFlow is a new flow format characterized by the following properties:

- Superset of Cisco NetFlow v9 in order to ease the migration towards it.
- Support of both IPv4 and IPv6.
- Compressed (RFC 1950, 1952) flow format for reducing network traffic and obfuscating the data being transmitted.
- Flow authentication, protection against forging, and non-repudiation (RFC 1321).

- Flow payload information.
- Accurate ICMP access.
- Support of packet sampling for easing probe scalability.
- Provides performance (network and application) information.
- MPLS and VLAN tag info.

The nFlow header is basically an extension of NetFlow v9 with information concerning the sampling rate and the flow digest in MD5 format. The digest is calculated as follows:

- The probe generates a buffer containing the uncompressed flow.
- The md5Sum field is replaced with a shared password.
- The MD5 summary is computed on the buffer and stored on the md5Sum field.
- The flow is emitted.

This algorithm guarantees that flows cannot be forged or modified on transit without knowing the shared password whose concept is similar to the community used in SNMP. Contrary to NetFlow v9 that has introduced the concept of template for periodically informing the collector with the flow format definition, nFlow embeds the flow format into the emitted flow. In fact each flow item contains the field type (subset of the NetFlow v9 format), length and data. Using this solution, each field is slightly larger than the equivalent v9 flow (in v9 the field type and length are sent into the flow template) but thanks to the flow compression the total flow length is significantly smaller (at least 50%) than the equivalent v9 flow. In addition, the collector implementation is significantly simpler than a v9 collector that has to store the flow template and that is unable to decode the flow until the flow template is received.

In order to validate this work, nFlow and v9 support has been added to ntop/nProbe [3] two open source network monitoring tools. ntop can now handle both nFlow and v9 flows emitted by nProbe. During the tests, nFlow format has demonstrated to be superior to v9 with respect to flow size and security, and very similar to v9 from the point of view of flow richness as nProbe extended the v9 format with the additional nFlow fields. An advantage of nProbe with respect to Cisco v9 implementation is that the flow format can be defined at runtime, whereas Cisco's implementation provides a static v9 format very similar to the previous v5 format.

3. Final Remarks

The nFlow format is a superset of the NetFlow v9/IPFIX format currently being defined. Presented to the IPFIX working group, it extends v9 with new features such as flow compression and authentication, in addition to new flow fields. An open source nFlow probe/collector has been implemented in order to evaluate and compare it to v9/IPFIX.

4. Availability

The nFlow home page is http://www.nflow.org/. Both ntop and nProbe are distributed under the GPL2 license and can be downloaded from the ntop home page (http://www.ntop.org/) and other mirrors on the Internet.

5. References

[1] B. Claise, *Cisco Systems NetFlow Services Export Version 9*, Internet Draft, August 2002.

[2] G. Sadasivan and N. Brownlee, *Architecture Model for IP Flow Information Export*, Internet Draft, October 2003.

[3] L. Deri, *nProbe: an Open Source NetFlow Probe for Gigabit Networks*, Proceedings of Terena TNC 2003, Zagreb, May 2003.

6. Vitae

Luca Deri <luca.deri@netikos.com> is currently sharing his time between NETikos S.p.A. and the University of Pisa where he has been appointed as lecturer at the CS department. He received his Ph.D. in Computer Science with a thesis on Software Components from the University of Berne in 1997. He previously worked as research scientist at the IBM Zurich Research Laboratory and as research fellow at the University College of London. His professional interests include network management and monitoring, software components and object-oriented technology. His home page is http://luca.ntop.org/.