FlowMon PROBE

FlowMon probe is a passive network monitoring device based on the COMBO hardware platform. It is able to generate and collect statistics about network traffic (IP flows) and export them in real-time to external collectors. Currently supported export formats are versions 5 and 9 of Cisco NetFlow.

Introduction

Most modern communication services (world wide web, streaming, databases, e-mail, on-line shops etc.) now use the Internet infrastructure. Its reliable operation also depends on large-scale monitoring capable of providing accurate data about traffic patterns, applications used, hostile activities etc. Such monitoring systems can help network operators to manage their current networks or plan new network topologies. Other management techniques such as bandwidth provisioning, detecting DoS attacks, billing and accounting also require detailed monitoring. Currently available monitoring devices have their limitations in terms of performance and flexibility. In particular, for security-related applications it is not acceptable to get information about only a random portion of the network traffic when the monitoring device becomes overloaded, for example during a DoS attack.

NetFlow as a general method for flow monitoring, first implemented in Cisco routers, is the most widely used measurement solution today. Statistics on IP traffic flows provide information about who communicates with whom, how long, how often, using what protocol and service and also how much data was transfered.

So far, NetFlow data are usually acquired and exported by IP routers. Such a setup has several drawbacks, namely

- Routers are by definition visible Layer 3 systems that can easily be discovered by simple tools such as *traceroute*. Consequently, they can become targets for all types of attacks.
- The main task of routers is to forward datagrams and exchange routing information with their neighbours. The processing power available is thus rather limited and so operations on NetFlow data do not usually go much beyond simple export of raw flow records.
- As a special case of the previous item, some routers impose sampling on the incoming traffic. Even if sampling is not strictly required, in some cases it is the only way for keeping the router operational, especially when high-speed interfaces are monitored.

In contrast, standalone monitoring probe is essentially a stealth device - invisible at both Layer 3 and 2 - dedicating all its resources to the tasks of flow record acquisition and processing.

FlowMon probe capabilities

HW parameters of FlowMon probe:

- monitoring of two 1 Gbps ports at full speed
- precise timestamps, active and inactive timeouts
- standard sampling, sample and hold
- repeater and splitter ports

SW parameters of FlowMon probe:

- export in NetFlow v5, v9
- anonymization and per collector filtering

FlowMon probe deployment

The probe is typically deployed on the LAN side of the WAN router and is totally invisible on the network. The probe can be connected in two modes to your network:

- probe is inserted in line, all incoming and outgoing traffic pass by the probe. You will be able to do 1 Gbps full-duplex measurement.
- probe is connected to mirror port of WAN router or T-splitter is used. You will be able to do measurement on two 1 Gbps half-duplex ports.

Each measurement port is mirrored to dedicated port (see fig. 4). You can easily chain several cards e.g. flow monitoring system with IDS system without any time or performance penalties.

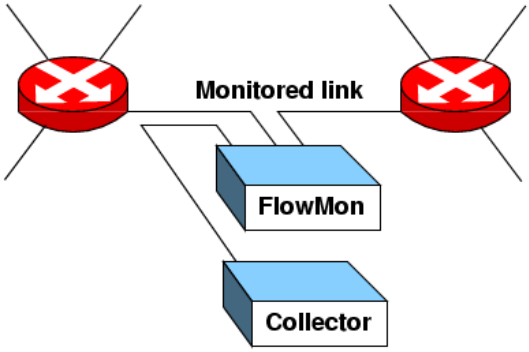

Fig. 1 - Probe inserted in line

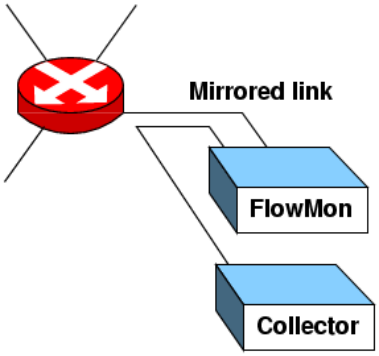

Fig. 2 - Probe connected to mirror port

FlowMon probe hardware

The FlowMon hardware has been designed to work on any PC-AT compatible computer running Linux or other Unix-like operating system. It has been successfully tested on computers that use the x86 family of processors. The hardware requirements necessary to run FlowMon probe are:

- Intel Pentium or equivalent x86 based PC
- 1 GB RAM, 50 MB disk space for tools installation
- PCI-X bus - 64-bit/66 MHz

The probe hardware consist of COMBO6X and an interface card COMBO-4SFPRO. Both cards together fit into one PCI-X slot.

The software requirements necessary to run FlowMon probe are:

- Linux kernel version 2.4.x or 2.6.x
- Red Hat Enterprise Linux, Ubuntu or Debian distribution

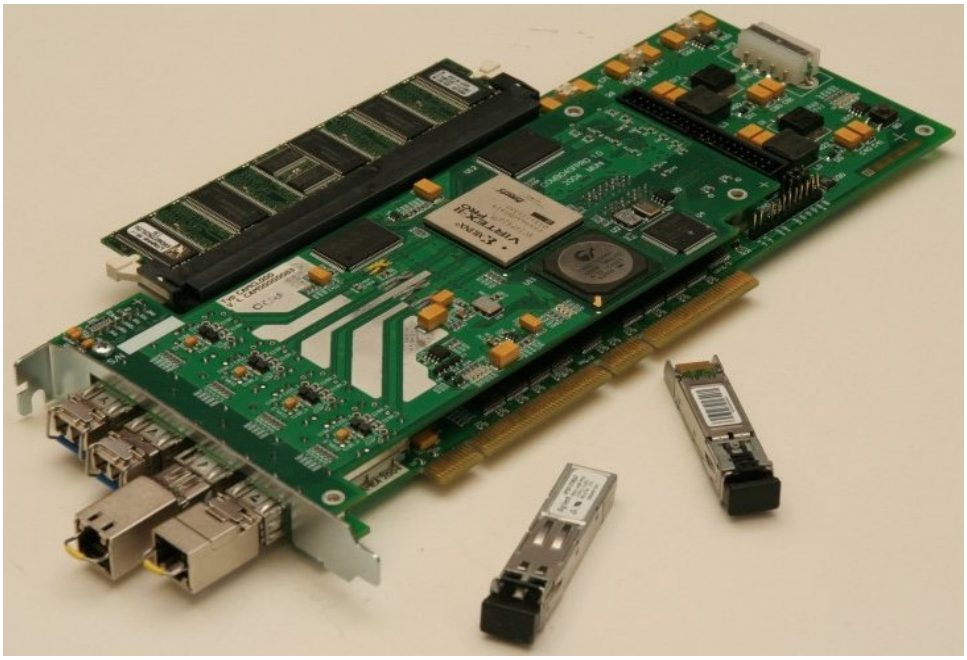

Fig. 3 - COMBO6X - PCI-X 64/66MHz hardware accelerated card

The FlowMon probe consists of two parts: hardware and software. The hardware part processes incoming packets at high speed (wire speed) while the software together with an ordinary network card handle the task of transmitting flow records to a remote collector.

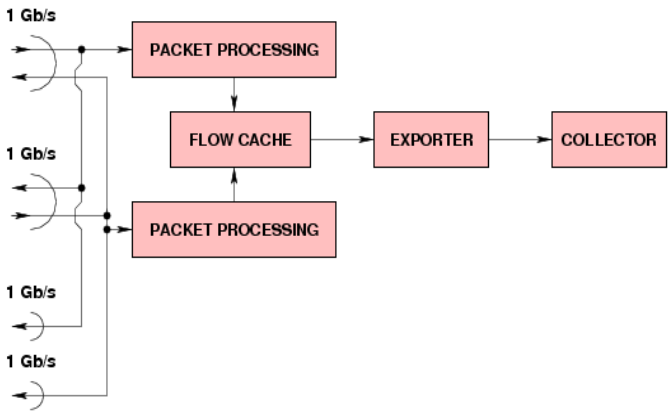

Fig. 4 – FlowMon probe block structure

Nowadays, the Internet traffic has no lack of malicious traffic such as DoS attacks, smurfs and port scans. Such traffic often generates a large number of flows. Consequently, NetFlow monitoring systems may become overwhelmed and thus unable to give vital information about those attacks. To protect the monitoring system several techniques are implemented in FlowMon probe.

Input sampling

Input sampling of incoming packets is the easiest way how to decrease the traffic volume to be processed, and also decrease the number of new flows during attacks where every

incoming packet belongs to a new flow. On the other hand, sampling makes it difficult to estimate precise flow statistics.

Output Sampling

Rate of exported flow records is strongly dependent on the actual traffic mix. Output sampling can keep it in a specified range and prevent collector from being overwhelmed by aggressive export rate during traffic peaks or attacks.

Sample and Hold

This method is quite similar to input sampling but with the following twist. As with ordinary sampling, each packet is sampled with certain probability. However, for every new entry in the flow memory, all subsequent packets belonging to that flow are protected from sampling the flow memory, a new item is created. This way we obtain precise data about large flows.

Adaptive Input Sampling

A static sampling rate is either suboptimal at low traffic volumes or can exhaust resources (memory, bandwidth) or cause other difficulties at high traffic volumes. Adaptive Input Sampling keeps the device load within reasonable limits while using the optimal sampling rate for all traffic mixes.

FlowMon probe software

The fig. 5 shows typical FlowMon probe installation. Probe is inserted in line, incoming data are processed by COMBO card and stored in flow cache. Software reads data from cache and send them to the collector. Several export applications can be used to read data from hardware and send to collector. The the CPU usage is very low and the probe doesn't require a lot of resources.

The FlowMon probe configuration is very easy. You can use command line (terminal) interface or web interface to setup the probe. Once the probe is configured the system works completely autonomously.

Export application communicates with a collector via IPv4 or IPv6 protocol using UDP connection. NetFlow version 5 and 9 are supported. NetFlow v9 implementation includes full support for IPv6 traffic.

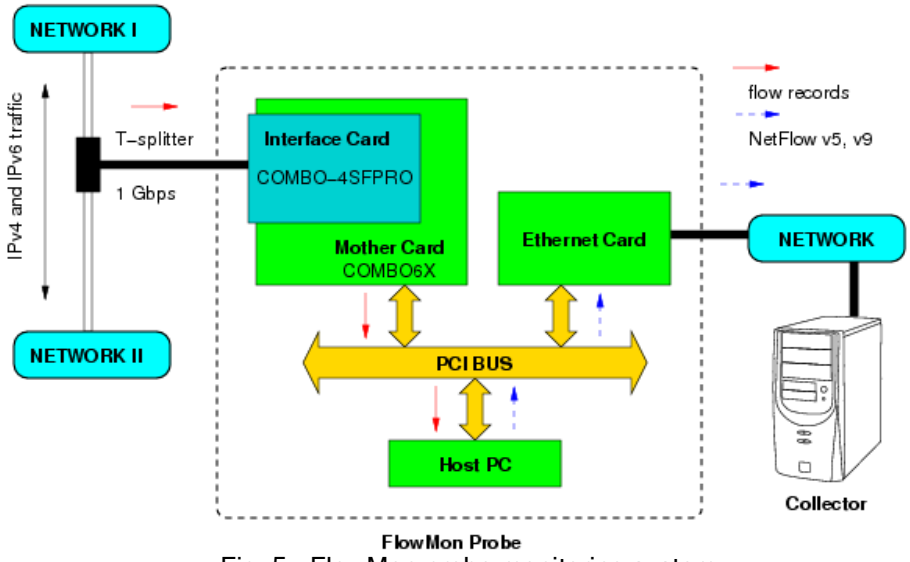

Fig. 5 - FlowMon probe monitoring system

To keep users privacy traffic anonymization can be applied. The anonymization module is designed to hide original data source information, like IP addresses and port numbers. The anonymization process is IP version independent and the probe is able to anonymize IPv4 as well as IPv6 traffic.

To split original traffic between several collectors the filter module can be applied. The backbone traffic can be distributed between several ISPs depending on the traffic origin. Filter module supports IPv4 as well as IPv6 traffic.

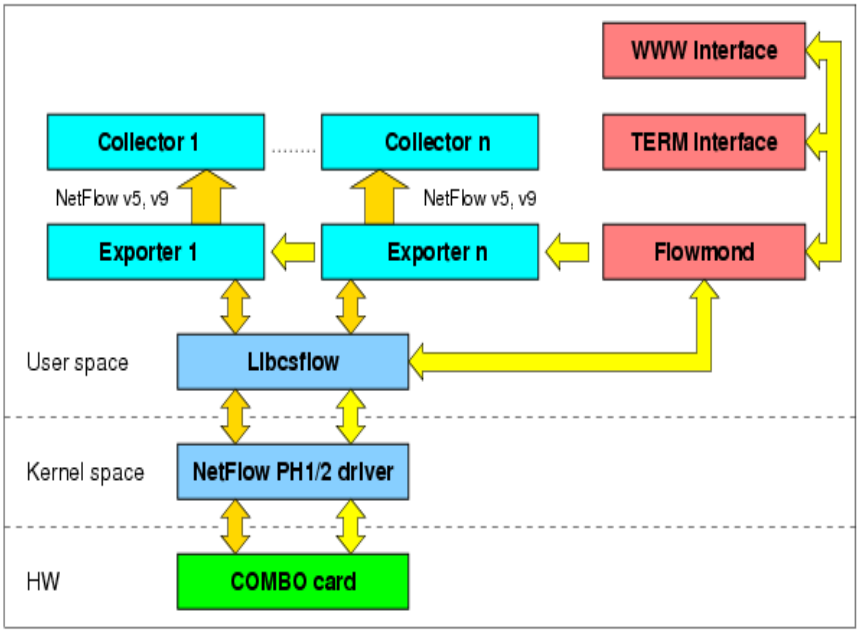

Fig. 6 - FlowMon probe software structure

NetFlow collectors

The NetFlow collector is independent part of FlowMon probe. Several third party collectors can be used to collect, view and analyze network traffic. Statistics can be viewed from different angles and with different granularity. The system is perfectly scalable using sampling at different stages of monitoring (input sampling, export sampling, collector sampling).

Fig. 7 – NfSen collector output

The collector output can be used for

- network traffic monitoring (traffic time series)
- security analysis
- backbone management and planning
- QoS (bandwidth provisioning)
- billing and accounting

Summary of FlowMon probe features

SW Features		HW Features	
NetFlow protocol	V5, v9 with Ipv6 support	Performance	2 x 1 Gbps half-duplex or
Connections	YES		1 x 1 Gbps full-duplex processing
Data Filtering	YES	Connections	2 x 1 Gbps Ethernet ports (cooper or fiber) – input (repeater) ports
OS	Linux 2.4.x/2.6.x		2 x 1 Gbps Ethernet ports (cooper or fiber) – mirror (splitter) ports
		Input sampling	static, random or adaptive sampling, sample and hold
		Dimension	27 x 13,5 cm