NetFlow FAQ

What is an IP flow?

IP flow is an unidirectional stream of IP packets of a certain network protocol, traveling between two network points. IP flow is identified by the source and destination IP address, source and destination port, protocol and DSCP field, within a certain period of time. Within an IP flow all IP packets have identical:

- Source and destination IP addresses
- IP header protocol number
- IP header ToS field (DSCP)
- Source and destination ports if the TCP or UDP protocols are used

What is IP flow accounting?

IP flow accounting is a feature of a router enabling it to create IP flows collection, count IP flows passing through it and to export the traffic via NetFlow® protocol. The collection itself consists of the following data:

- Number of packets in IP flow
- Number of bytes in IP flow
- Timestamps

What is NetFlow?

NetFlow is a network protocol, developed by Cisco Systems, used for exporting collected IP flow traffic. This data is exported to a server, where it is collected, processed, aggregated and archived. It can then be reviewed in a more user-friendly form. NetFlow Analyzer performs all of these functions. There are numerous NetFlow protocol versions, most important of which are versions 5 and 9. Version 5 is commonly used on most Cisco NetFlow enabled devices. NetFlow version 9 is the latest version, created to support advanced technologies such as MPLS, IPv6, Multicast, VLANs, etc.

Which devices support NetFlow?

NetFlow® technology was developed by Cisco Systems, so all of the Cisco IOS routing platforms can export NetFlow data. From Cisco Catalyst switching platforms, only Catalyst 6500 series multilayer switches support NetFlow data export. Other vendors are also offering NetFlow-like capabilities on their network devices. These similar technologies are named differently by different vendors, for example J-Flow® by Juniper, NetStream® by Huawei, IPFIX® by Nortel etc.

Which versions of NetFlow protocols are supported by NetFlow Analyzer?

NetFlow Analyzer is based on Cisco NetFlow protocol versions 5 and 9. NetFlow Analyzer also supports IPFIX. The system is capable of recognizing protocol formats from other vendors, which are compatible with NetFlow protocol versions 5 and 9 such as Juniper J-Flow, Huawei NetStream.

However, NetFlow Analyzer has been tested to support NetFlow enabled Cisco devices and IPFIX from Juniper devices only.

NetFlow Analyzer utilizes Traffic Patterns which are based on IP addresses and not on physical interfaces, this allows NetFlow Analyzer to support netflow probes - software generated NetFlow-like protocol. One such (free) software is Softflowd, available at http://code.google.com/p/softflowd/ .

Indirectly, sFlow is supported if you convert it to NetFlow, using free tool such as sFlow Toolkit, available at http://www.inmon.com/technology/sflowTools.php .

What is the network traffic overhead generated by the NetFlow data export?

NetFlow data overhead is expected to be less than 0.5% of the total network traffic included in the charts. This means, for instance, that 1 Mbps user traffic will produce approximately 50 kbps of additional traffic exported from routers to NetFlow Server.