# FAQ (NFA)

On this page:

- What is an IP flow?
- What is IP flow accounting?
- What is NetFlow?
- What is the network traffic overhead generated by the NetFlow data export?
- Why is traffic presented in 5-min data points (grains)?
- Why is traffic shown sometimes in 5-min and sometimes in 30-min, or even in 3-hour grains?

## 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 provides information about the source and destination IP address, source and destination port, protocol, DSCP field, etc. 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.

## 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.

## Why is traffic presented in 5-min data points (grains)?

Constant NetFlow data stream consumes vast amount of processing and storage resources, it is necessary to aggregate historical values and show them as 5-min averages. Based on our experience, 5-min aggregation (instead of 1-min aggregation, as an example) provides practical application performance and space saving on one side, as well as sufficient details for analysis and trend on the other.
This enables you to keep aggregated data/charts for a longer period (eg. 1 year) for monitoring trends, comparison and planning, whereas raw data/archive is kept for a shorter period (eg. 1 month) for instant event analysis, inspection and troubleshooting.

## Why is traffic shown sometimes in 5-min and sometimes in 30-min, or even in 3-hour grains?

To provide even more HDD saving while storing data for a longer period, our aggregation works in a way that shorter history is shown in smaller grains (more details and space consumption), whereas longer history is presented in larger grains (less details and space consumption).
For the best use of monitoring and comparison, you can see the following grains:

| Grain Name | Grain Period | Grain Size |
|---|---|---|
| G1 | Previous 3 weeks | 5 min |
| G2 | Previous 3 months | 30 min |
| G3 | Maximum history | 3 hour |

ⓘ Maximum history period is defined in Settings (⚙ > Settings > NetFlow Settings > Configuration > Database size in weeks)