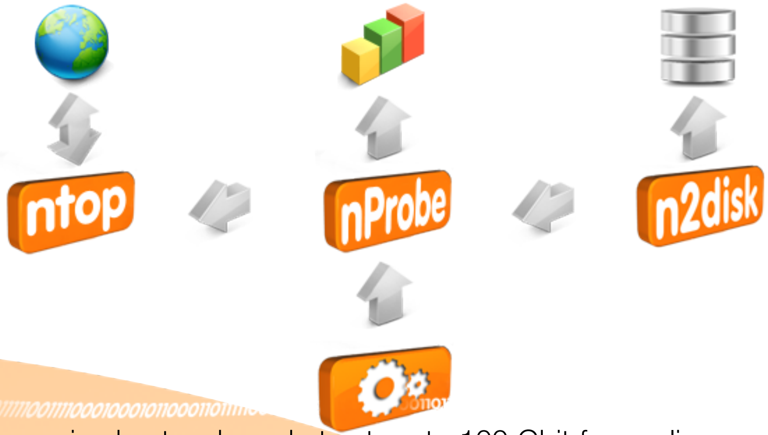
ntop

Network monitoring solutions



About ntop

The **ntop** project was started in 1998 as an open-source network monitoring tool. With more than 25 year spent in R&D in the networking world, the ntop team, still leaded by the project founder, is now a reference in the packet capture and analysis community. ntop has offices in Italy and Switzerland.

nProbe™ and nProbe™ Cento

nProbe is an Extensible NetFlowTM v5/v9/IPFIX/sFlow Probe for IPv4/v6. nProbe has been designed as an engine that processes packets and computes basic statistics, and plugins that extend the core with additional capabilities. Each plugin dissects a specific traffic (e.g. HTTP, GTP, DNS, SMTP, MySQL, Oracle, SIP, etc) to provide enhanced specific statistics. In addition to this nProbe detects hundreds of protocols thanks to the ntop-maintained nDPI library.
nProbe™ Cento is a high-speed NetFlow probe able to keep up with 1/10/100 Gbit. It has been designed as the first component of a modular monitoring system: besides capturing ingress packets and computing flow data, it can be used to classify the traffic via DPI (Deep Packet Inspection) and performs optional actions on selected packets/flows.

ntopng™

High-Speed Web-based Traffic Analysis and Flow Collection.
With the experience of more than 10 years of its previous version, ntopng is the next generation of the original ntop, a network traffic analyser that shows the network usage, similar to what the popular “top” Unix command does. Users can discover and analyse their network traffic just by surfing ntopng web based interface and get a dump of the network status.

n2disk™, disk2n

A multi-Gigabit network traffic recorder with indexing capabilities (n2disk) and replayed sized network packets at up to 100 Gbit from a live network interface, and write them into standard PCAP files without any packet loss with up to nanosecond precision. disk2n has the capability to replay those pcap using original inter frame gap.

nDPI

Open and Extensible LGPLv3 Deep Packet Inspection Library.
nDPI is a ntop-maintained superset of the popular OpenDPI library. Released under the LGPL license, its goal is to extend the original library adding newer and modern protocols available just purchasing commercial DPI library. Today it supports 350+ L7 protocols and it is used by both ntopng and nProbe to add application-layer information for the detected protocols.

PF_RING™, PF_RING™ ZC, PF_RING™ FT

High-speed packet capture, filtering and analysis.
PF_RING is a framework that dramatically improves the packet capture speed. It allows user to achieve 1/10/100G Gbit line-rate packet processing (both RX and TX) at any packet size. It implements Zero-Copy operations including patterns for inter-process and inter-VM (KVM) communications with PF_RING ZC.
PF_RING FT assists any flow processing application in the packet classification activity, implementing a flow table that can be used to keep track of flows and can be easily extended for building any type of application, including probes, IDSs, IPSs, L7 firewalls.

nScrub™

nScrub is a DDoS mitigation engine based on PF_RING ZC able to operate at 10 Gbps line-rate on a low-end machine relying on commodity hardware and Open Source technologies. It can work both as a transparent bridge or as router for on-demand traffic diversion.