EXA8 Applications

June 2019

FRICOM

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

The EXA8

The EXA8 is a compact multi-application device which can be used for aggregation, filtering, and capturing of network traffic in real-time.

- Captures 100% of all data for real-time analysis as well as historical playback – excellent for troubleshooting
- Captures to USB or SSD
- Capable of performing several other advanced applications like a Sessionmaster
- Able to run 3rd party applications
- Rolling Capture “look back in time capture”

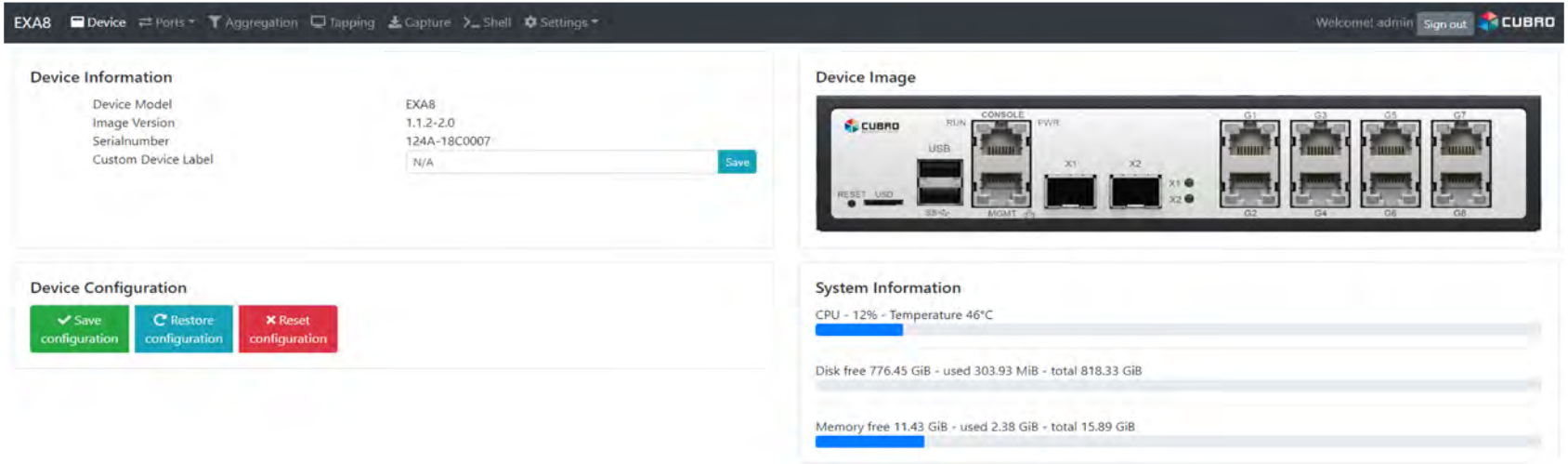
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

EXA8 - “the multi-in-one tool”

- 4 link copper TAP
- 4 link aggregator
- Multi-gbit capture tool with 1TB SSD
- Rolling capture with index
- Web GUI protocol analyzer similar to Wireshark
- Netflow support controller & analyzer

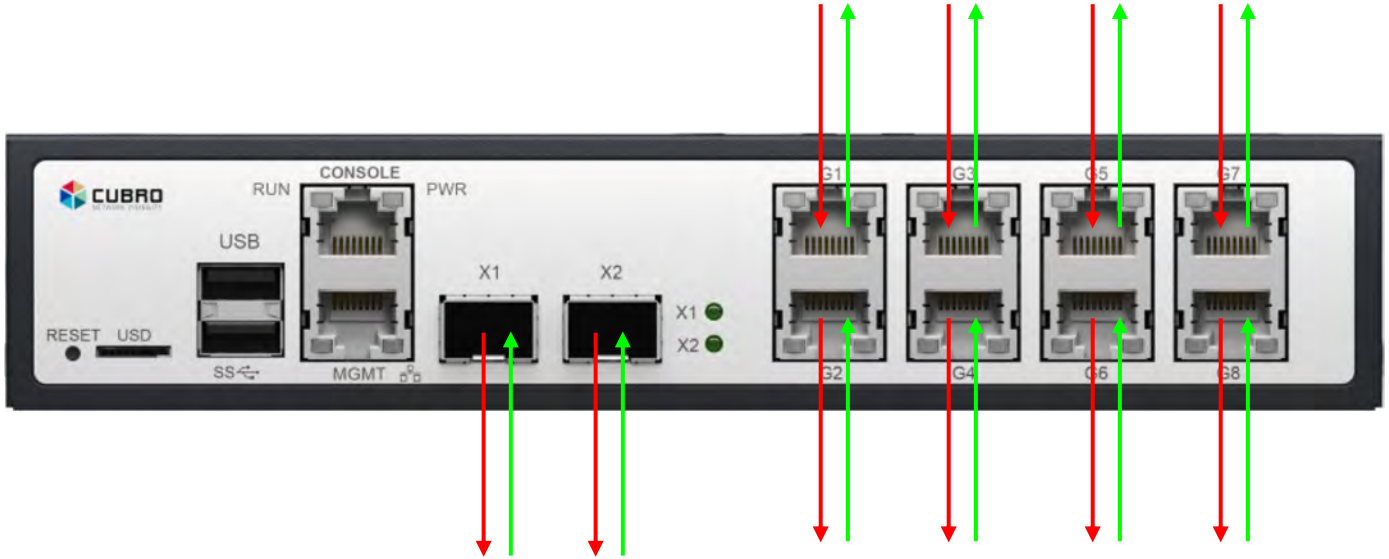
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Intuitive Web GUI



CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

The EXA8



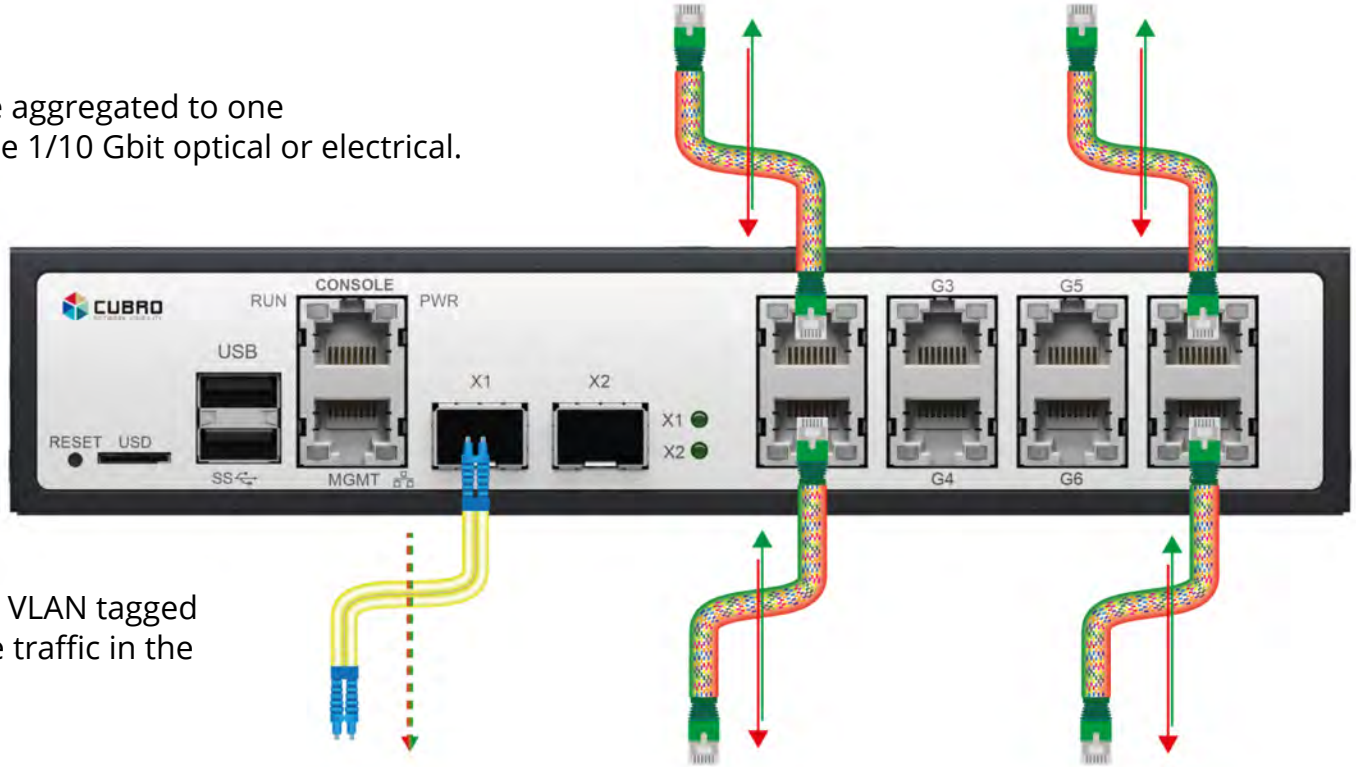
2 x 1/10 Gbit optical/electrical ports usable as input and output (depending on the SFP module)

4 x 1 Gbit links with internal TAP (bypass)

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Aggregation

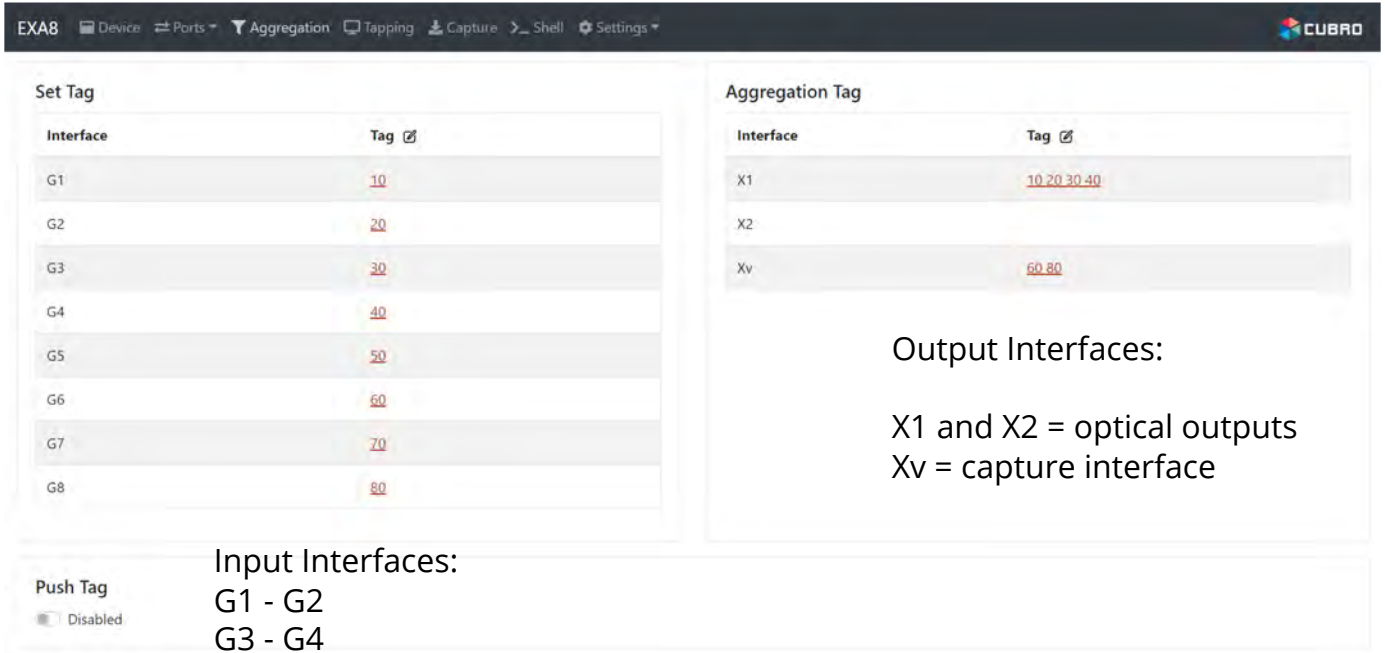
Up to 4 links/8 ports can be aggregated to one output. This output could be 1/10 Gbit optical or electrical.



The output traffic can be VLAN tagged per input to separate the traffic in the monitoring tool.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Aggregation GUI



Output Interfaces:

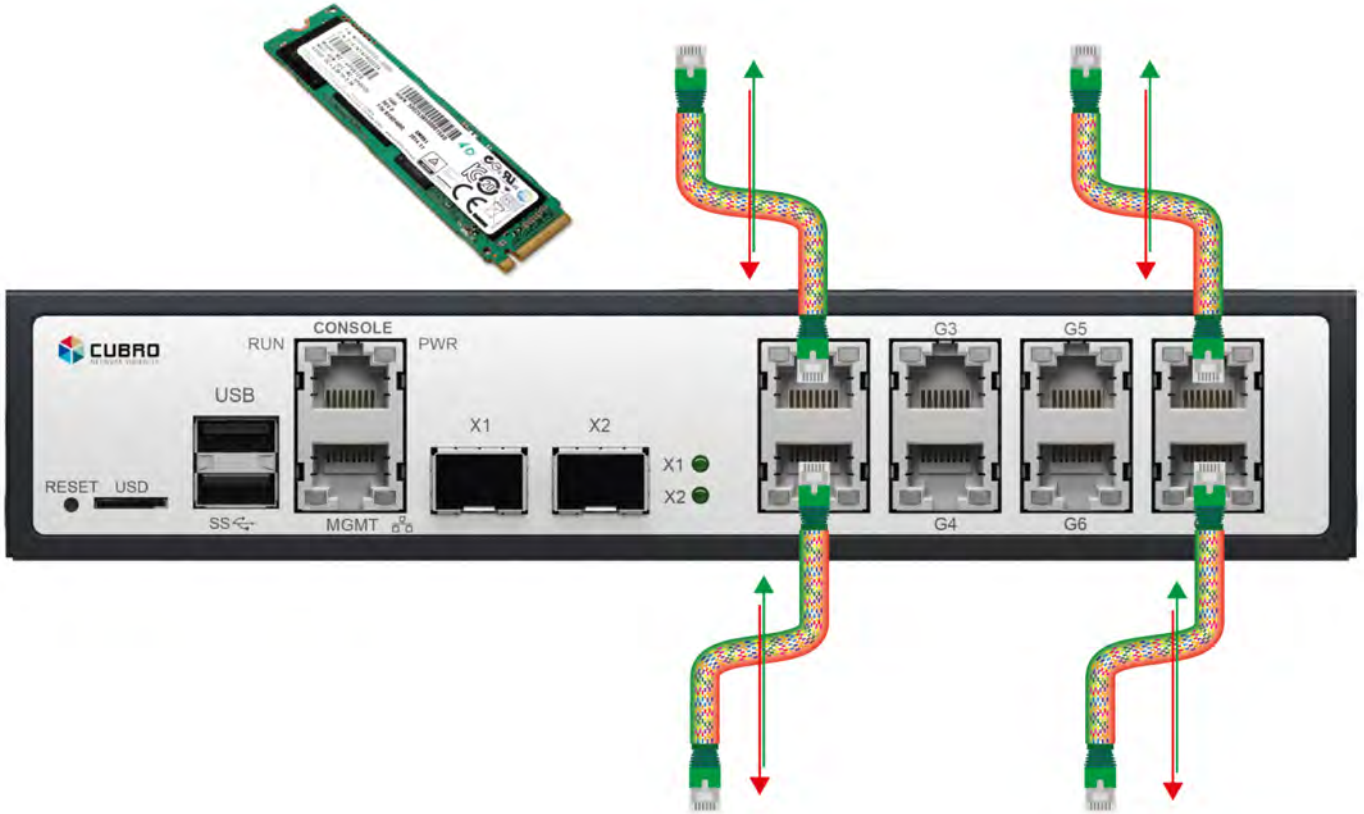
X1 and X2 = optical outputs
Xv = capture interface

Input Interfaces:
G1 - G2
G3 - G4
G5 - G6
G7- G8

4 links

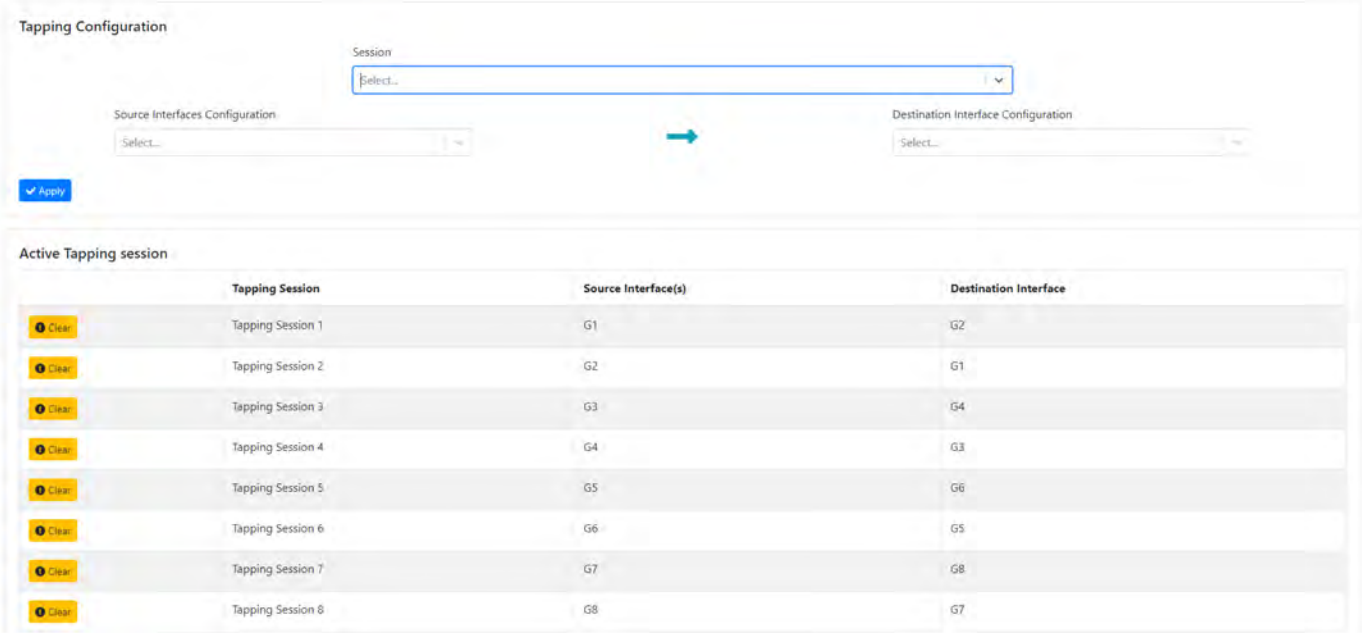
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Aggregation & Capture to SSD



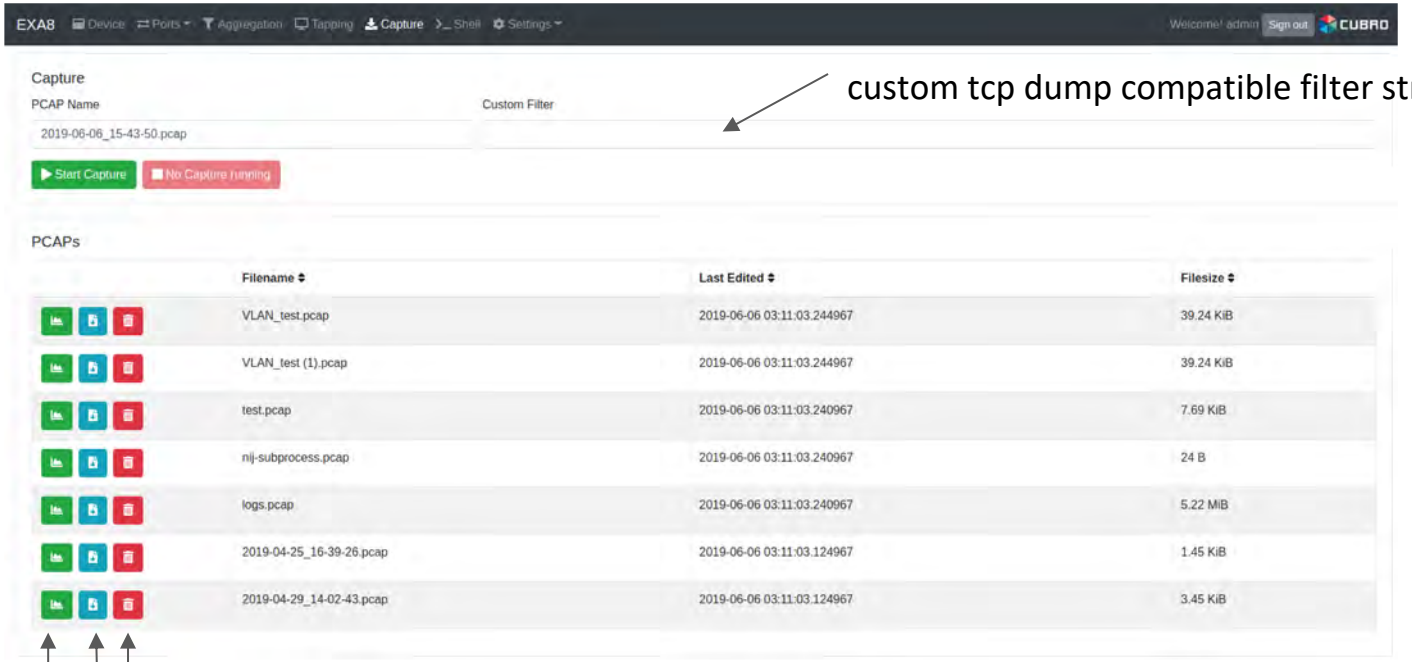
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Tapping Session GUI



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Capture GUI



custom tcp dump compatible filter string

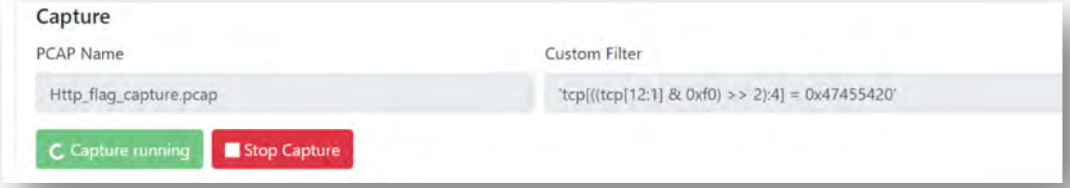
delete capture file

download capture file

start webshark (analyze capture file)

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

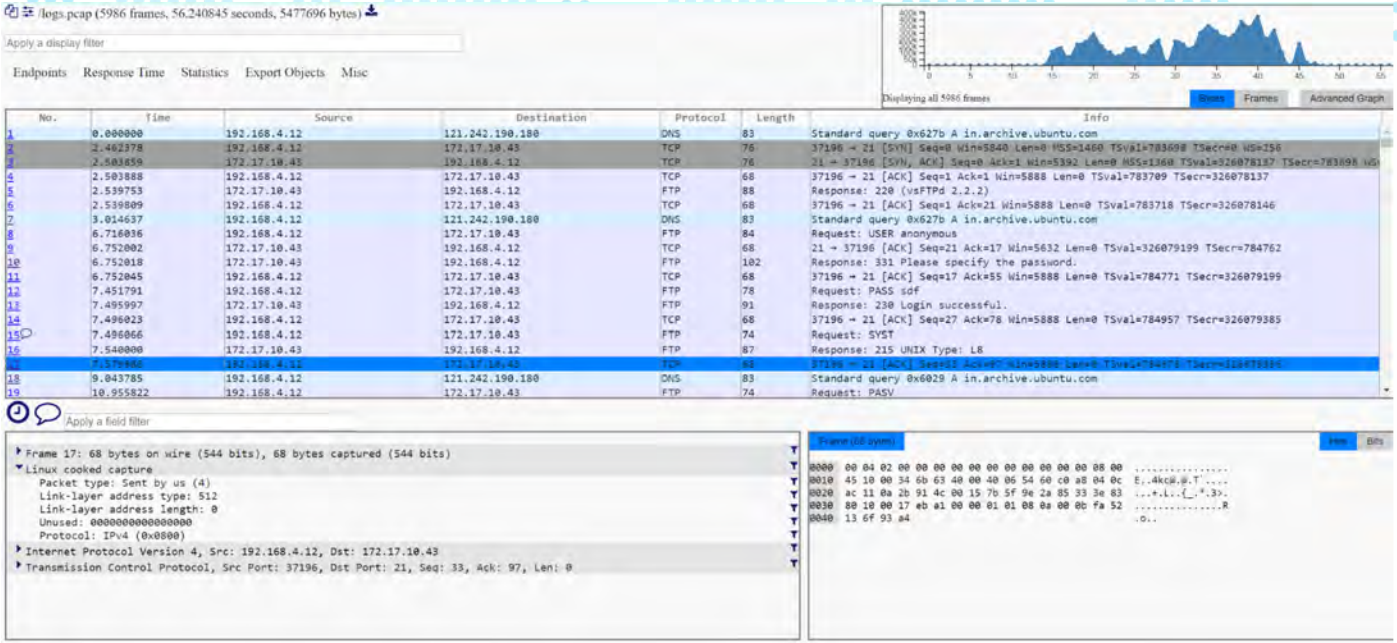
Custom Filter examples



These filters reduce the captured traffic to save disk space.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Webshark GUI

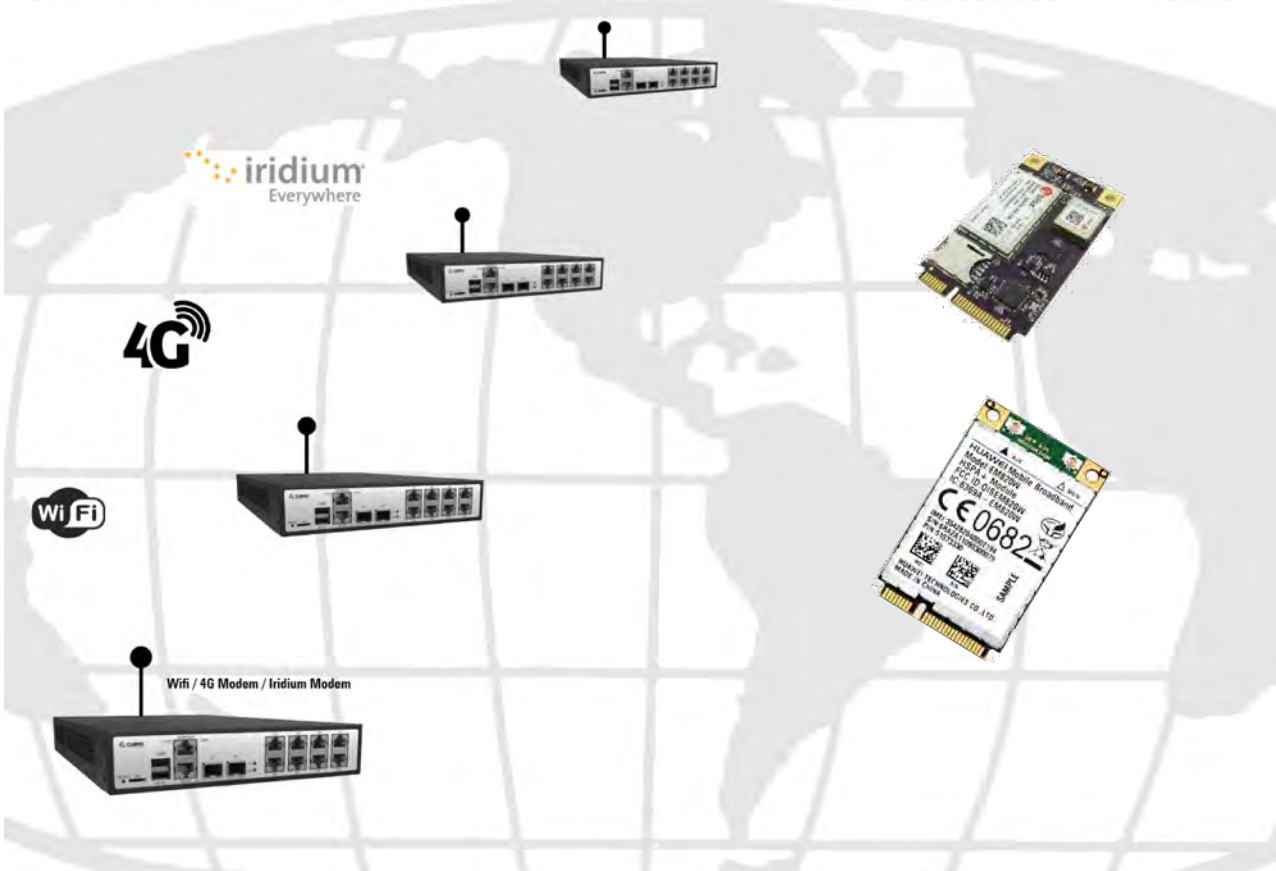


It is possible to open the captured pcap file directly on EXA8 by pressing the green button on the Web GUI without downloading the file. This gives the option of remote troubleshooting using only the EXA8.

The Webshark provides similar feature set as the well known Wireshark.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Remote Capture



With the optional built-in Wifi / 2G/3G/4G modem or Iridium satellite modem, the EXA8 is a versatile monitoring platform, that connects various wireless technologies across every point on Earth.

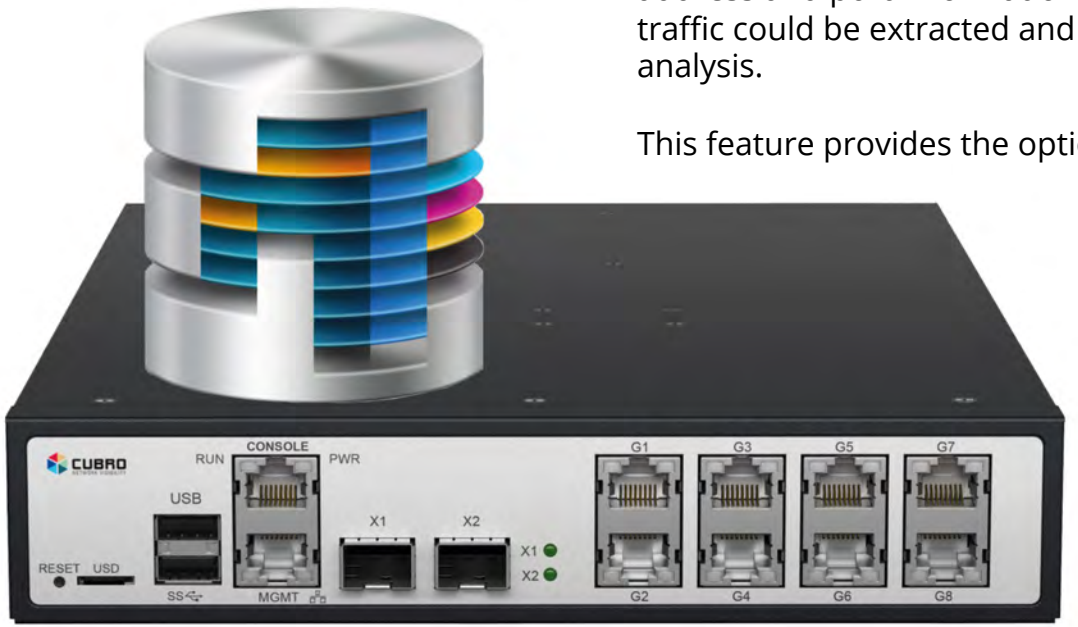
The EXA8 supports a PCIe connector expansion slot as well as holes for an antenna in the enclosure.

One box can do it all - Network connections on multiple interfaces, powerful multi-core CPU, high-performance SSD storage, and the modem support for remote connections.

The powerful CPU gives the user the option to run analysis software at the remote site thus preventing the need to download capture files over a slow connection link.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Rolling Capture & Indexing



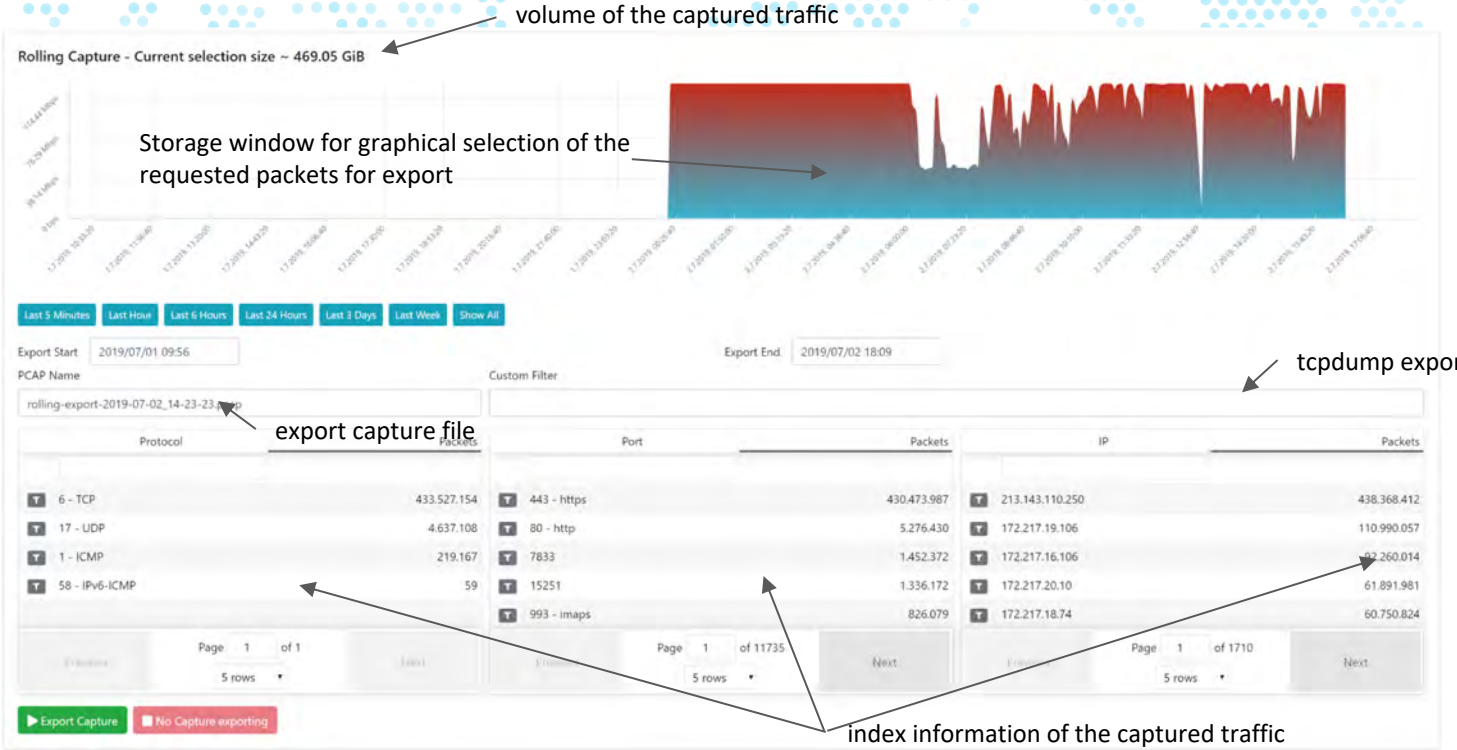
Rolling capture is a feature where the EXA8 is endlessly capturing traffic from the configured ports or links. If the reserved disk space is full, the rolling capture overwrites the older capture automatically.

The rolling capture also produces an Index of the captured traffic (time, IP address and port information). With the help of this index the relevant traffic could be extracted and exported in a PCAP file for the purpose of analysis.

This feature provides the option to look back in time and find past events.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Rolling Capture & Indexing

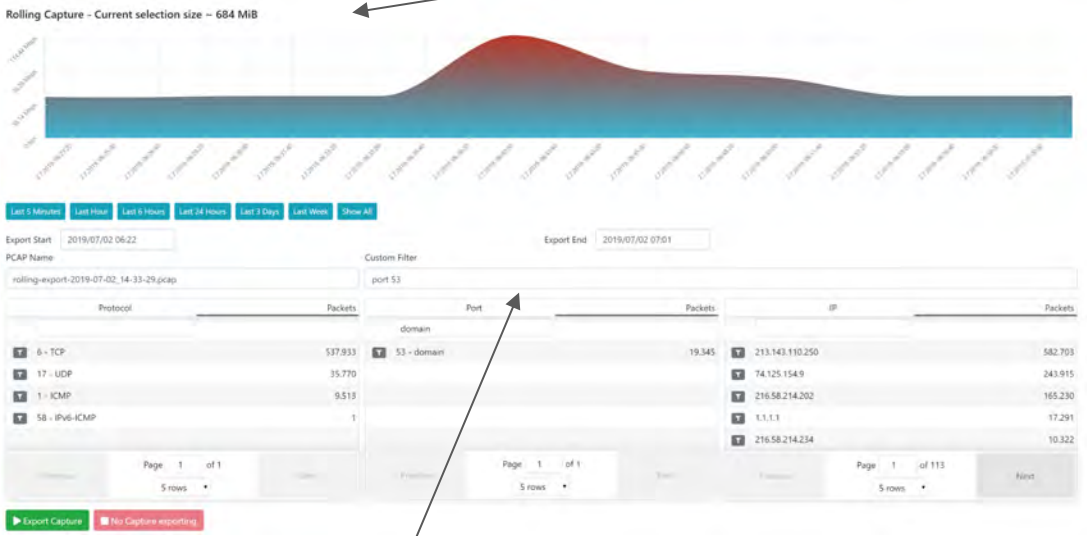


The rolling capture runs 24/7 and the user can extract the capture files by time or IP index and convert it to a PCAP for later analysis. There is also an option for a post filter via tcpdump during the export process.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Rolling Capture & Indexing

volume of the selected time frame



In this example we want to extract only DNS traffic from this time frame

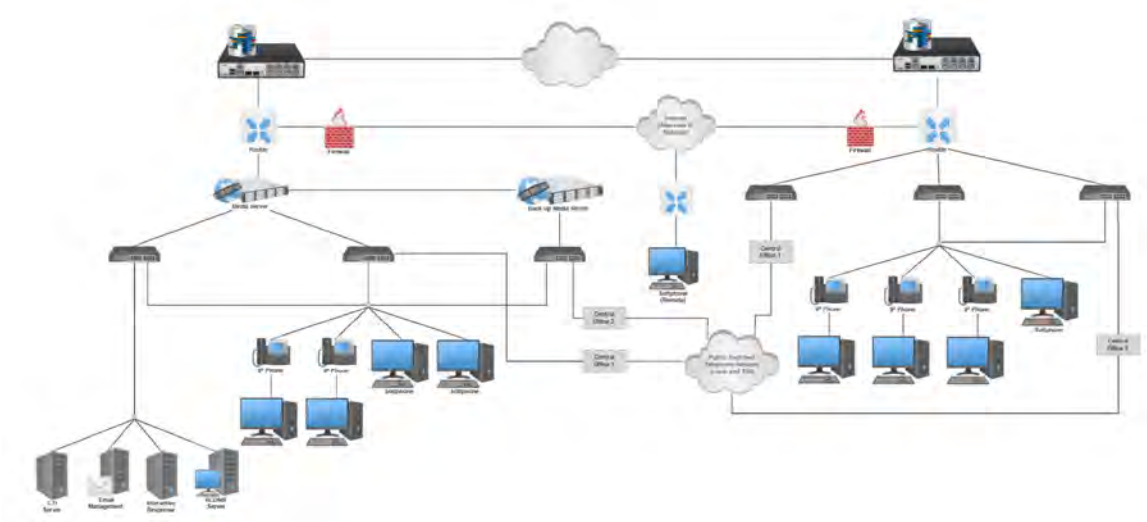
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Rolling Capture & Indexing Use Case

Network troubleshooting is often not that easy because the problem appears only from time to time. In this case a standard capture will not help.

The Cubro Rolling Capture can quickly solve the problem, because the capture is continuously running, and when the error happens, the engineer can look back in time through the capture file. With the help of the query language you can extract the right time frame and the relevant traffic filtered by IP address and port.

In combination with the TAP and remote access, the EXA8 is the perfect remote site troubleshooting tool.



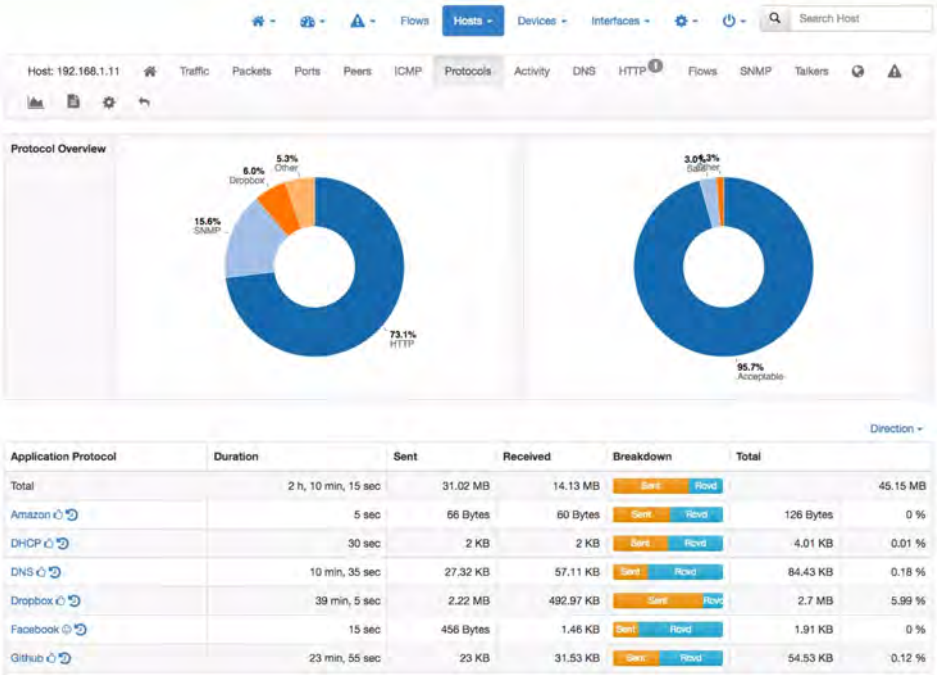
In this example the rolling capture is used on two WAN interfaces to see the behaviour of the WAN at the exact same time when the error event happens.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Netflow on EXA8

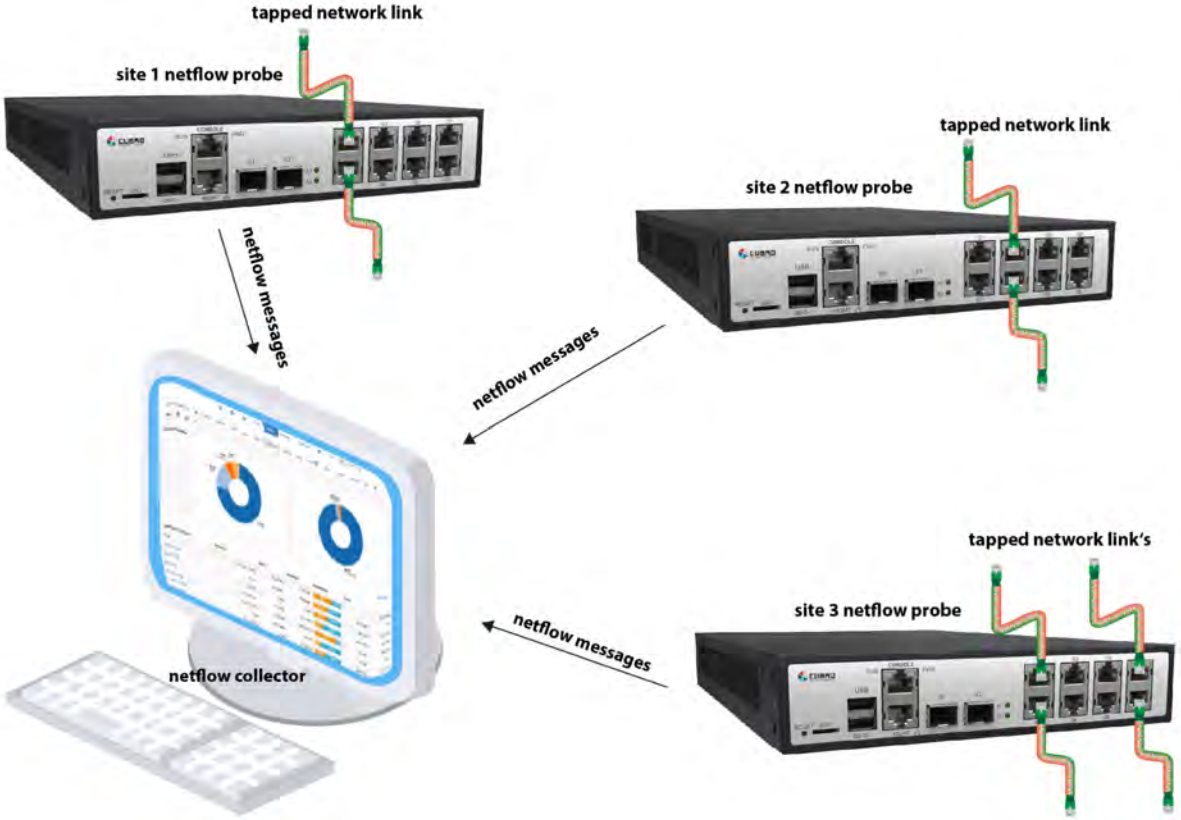
The EXA8 offers a full featured Netflow analyzer.

The user has the option to run the software in two different modes. The first is as only a Netflow generator. In this case the Netflow messages are sent to an external collector for higher performance and to support multiple probes. The second mode is for one EXA8 to serve as both a probe and collector for an out of the box, turnkey solution.



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Multiple Netflow Probes



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Software Roadmap for EXA8

Regex filtering: DPI fingerprint filtering for security applications

[^]*?@[^]*?\.[^]*

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE