

Network Visibility for Municipal Utilities and Critical Infrastructure

Securing critical power grid operations and optimizing Network Detection and Response performance.

SECTOR	APPLICATION	PLATFORM	ENGAGEMENT
Municipal utility, energy distribution (Germany)	Network Detection and Response (NDR) enablement	Cubro EXA48800 network packet broker	Direct with Cubro

The Challenge

A German municipal utility came to Cubro while planning a Network Detection and Response rollout across its distribution grid. The challenge was to get clean traffic to the NDR.

- **Detection obligations.** KRITIS (a German regulatory framework designed to protect critical infrastructure) and NIS2 (the Network and Information Security Directive, a European Union law designed to establish a high common level of cybersecurity across EU member states) requirements push operators of critical infrastructure to detect anomalous activity within the network, not only at the perimeter.
- **Tool costs.** Duplicated, unfiltered traffic inflates NDR licence consumption and slows analysis. Duplicated packets can distort the results and will increase the load of the CPU and memory utilization.



The Solution

In the customer's network, mirrored ports send the packets to a single EXA48800. It aggregates mirrored port feeds, deduplicates packets and uses NetFlow for delivering the data to the NDR solution.

NetFlow Generation

The EXA48800 builds flow records on the broker itself and feeds clean telemetry data to the NDR system. Switches focus on their main task instead of spending CPU cycles generating flows.

Packet Deduplication

There are duplicate copies of packets across multiple TAP and SPAN points. Deduplication is needed to ensure NDR gets clean data. This results in fewer false positives, less processing load, and no unnecessary licence spend.

Results and Business Outcomes

- **Clean data into NDR.** One deduplicated NetFlow feed reaches the detection platform
- **Switch tasks minimized.** Telemetry generation moved from the switches to the network packet broker
- **Room to grow.** 4000 Gbps of switching capacity leaves plenty of headroom when the power grid expands and new traffic and monitoring tools are added.



Technical Highlights

High Density

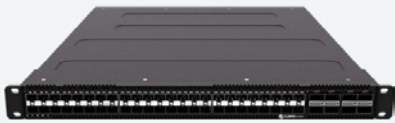
4 x 1G/10G/25G, 44 x 10G/25G and 8 x 40G/100G in a compact 1U form factor.

Dual ARM CPUs

Advanced filtering and telemetry generation that standard packet brokers cannot handle.

Green IT

Visibility and flow generation in one platform: less rack space, cooling and power.



Cubro EXA48800, 1U

4000 Gbps

SWITCHING CAPACITY

0%

PACKET LOSS

Why the Customer Chose Cubro

The utility chose Cubro on the overall package: an architecture built around the NDR use case, design support during the evaluation rather than after the order, and European engineering behind the hardware.

Feature and Value

FEATURE	UTILITY AND NDR BENEFIT
Deduplication	Prevents tool stress, alert fatigue, errors and NDR bottlenecks.
NetFlow Generation	Moves NetFlow generation from switches to the EXA48800. One source of information for the NDR instead of multiple switches.
Design Support	Deployment architecture tailored to utility networks.

For more information, contact us at support@cubro.com.

