Cubro Hybrid Packetmaster EX5-3 and EX6-3

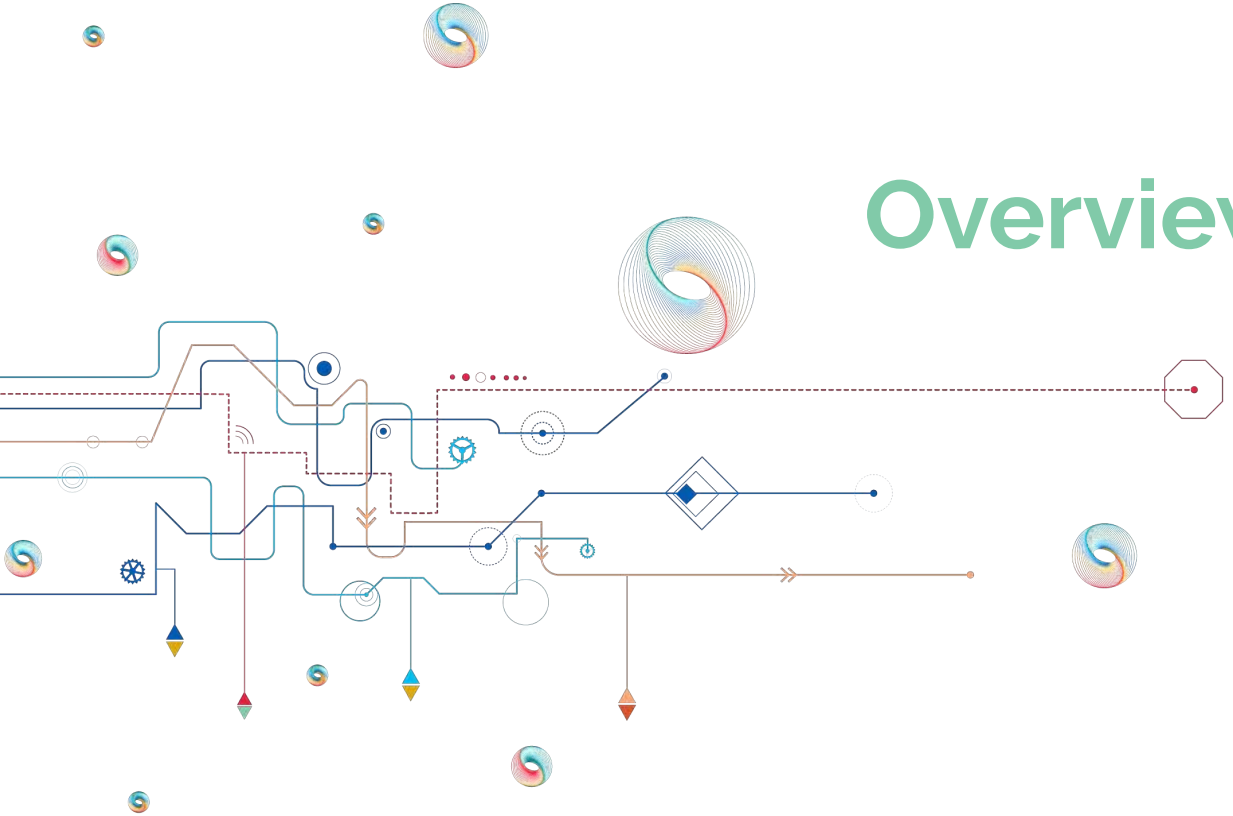
APPLICATION NOTE

June 2019

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

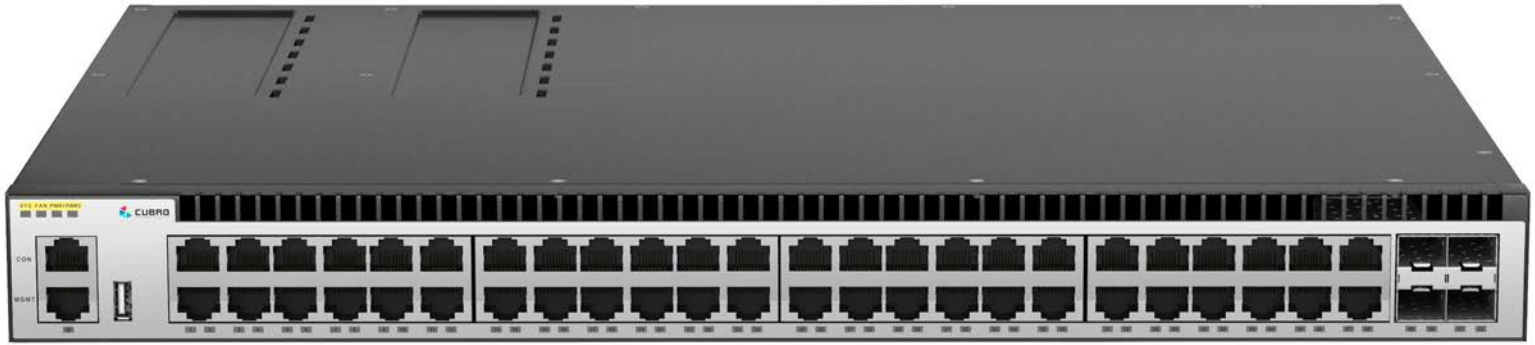
Table of Content

Overview



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Packetmaster EX5-3



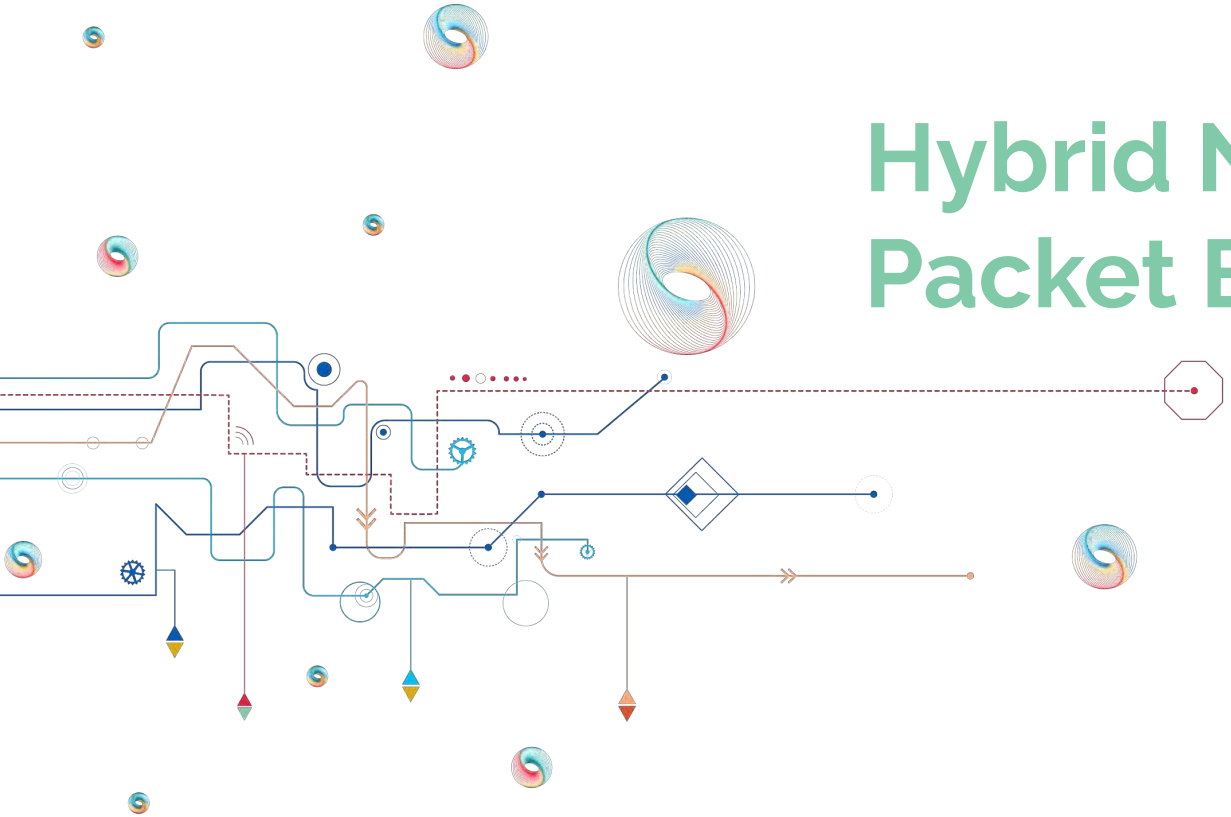
- 48 x 10/100/1000 Base-T Copper ports (RJ45)
- 4 x SFP/SFP+ for 1G/10G
- Each port can be used simultaneously as input and output and is totally independent from other ports
- Non-blocking architecture
- All ports are open – no software licence to enable ports

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Packetmaster EX6-3

- 48 x SFP ports for 10/100/1000M
- 4 x SFP/SFP+ ports for 1G/10G
- Each port can be used simultaneously as input and output and is totally independent from other ports
- Non-blocking architecture
- All ports are open – no software licence to enable ports

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE



Hybrid Network Packet Broker

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

What is a Hybrid Network Packet Broker?

A hybrid network packet broker (NPB) combines the features of a common L2 network switch and a NPB. As a result, it offers better inline monitoring applications like traffic blocking (a feature similar to that of a Firewall). Since the switch and the NPB are in one unit, it saves cost and space. Additionally, there is no need of physical TAP which also reduces the cost.

Cubro offers **Packetmaster EX5-3 and EX6-3** as the first known hybrid NPBs on the market.

How does it work?

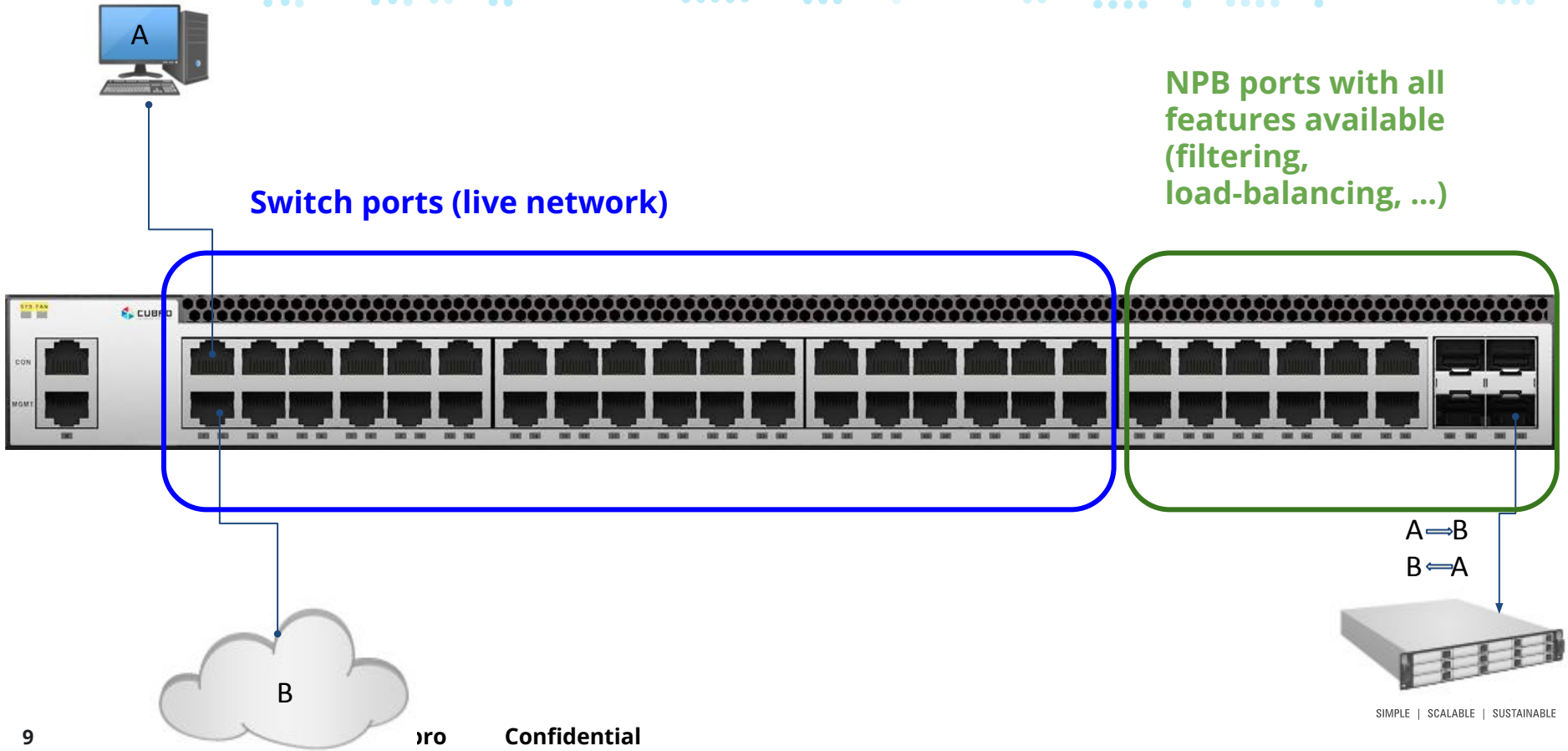
There are two entities in the unit, namely, the switch engine and the NPB engine.

The key point to know is that the NPB overrules the switch, if requested.

The NPB can “steal” the traffic from the switch engine, copy the traffic and give it back to the switch. This gives us two main functions:

- Extract traffic from the switch to the NPB on any level in the stack from physical port to IP address
- Block any traffic in the switch

Example

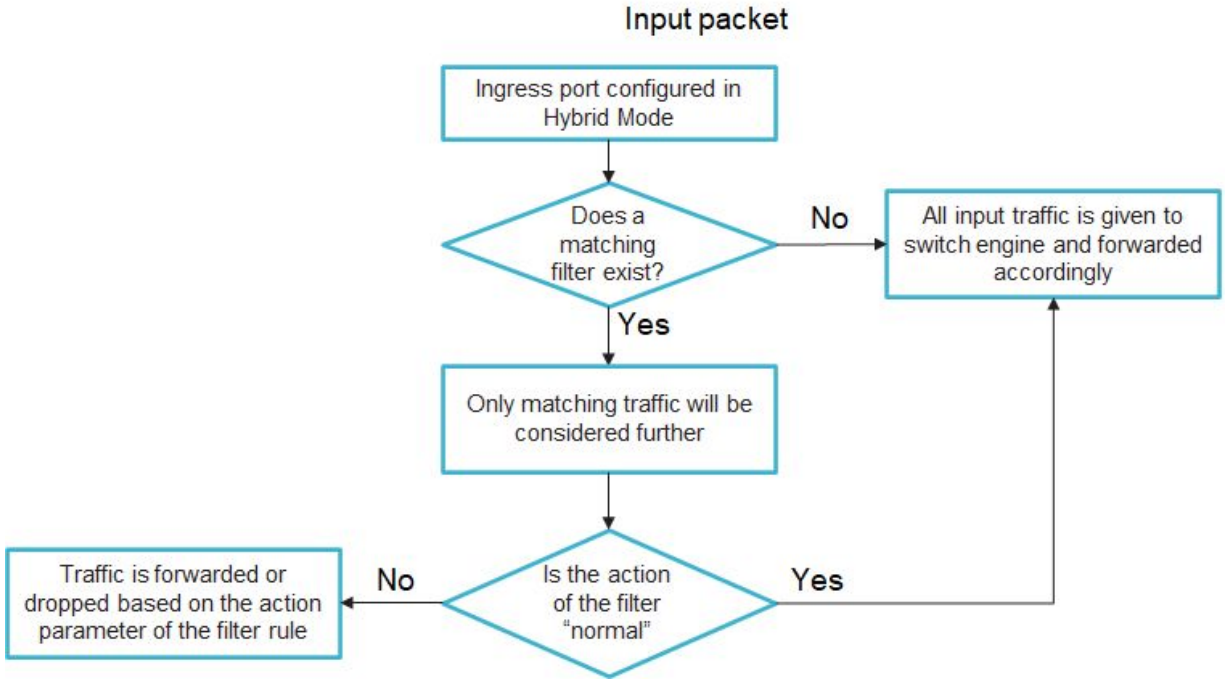


Traffic Forwarding Logic

How does the Hybrid Packetmaster handle incoming traffic?

1. When a packet is sent to one ingress port, the Packetmaster will check whether the port is a Hybrid port or not;
   - If yes, it will continue with step 2
   - If no, the packet will be handled by the Filter configuration (Rule Table)
     The packet will be dropped if no matching filter exists
2. Check the packet is matching the “protected-vlan” config of the port
   - If yes, the packet will be forward to the switch
   - if no, it will continue with step 3
3. Check the packet is matching a filter of the Rule Table
   - If yes, it will continue with step 4
   - if no, the packet will be forward to the switch
4. If the action of the matching filter is “normal”, the packet will be forwarded to the switch

Traffic Forwarding Logic



General feature Set

Aggregation
- One to Many
- Many to One
- Many to Many
- Load balancing
- Inner IP load-balancing

Filtering
- Layer 2 to Layer 4
- MPLS Label
- VXLAN tunnel ID (VNI)

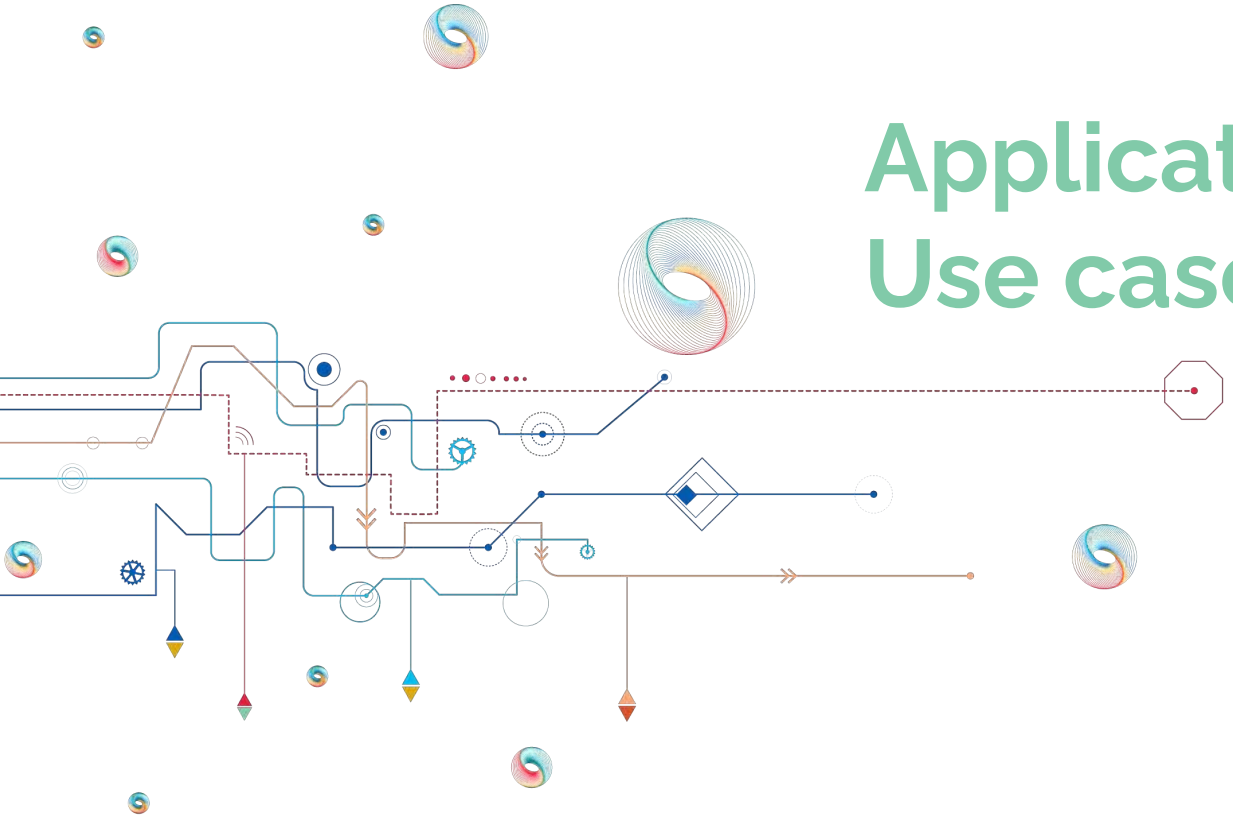
Tunnel De- & Encapsulation
- L2GRE
- NvGRE
- VXLAN
- MPLS

General Management
- Easy to use WebUI, CLI and Rest API
- SNMPv2
- NTP synchronisation
- Syslog to remote host

User management
- Role based access
- RADIUS authentication
- TACACS+

Key features that makes Cubro Hybrid NPB different

- VXLAN tunnel ID filtering (similar to Cubro G5 series)
- Inner tunnel load-balancing (similar to Cubro G5 series)
  - Advanced hashing based on VXLAN VNI or MPLS Label possible
- Inline tunnel termination
- Combination of L2/L3 Network Switch and L5 NPB functions
- Up to 4500 parallel filters



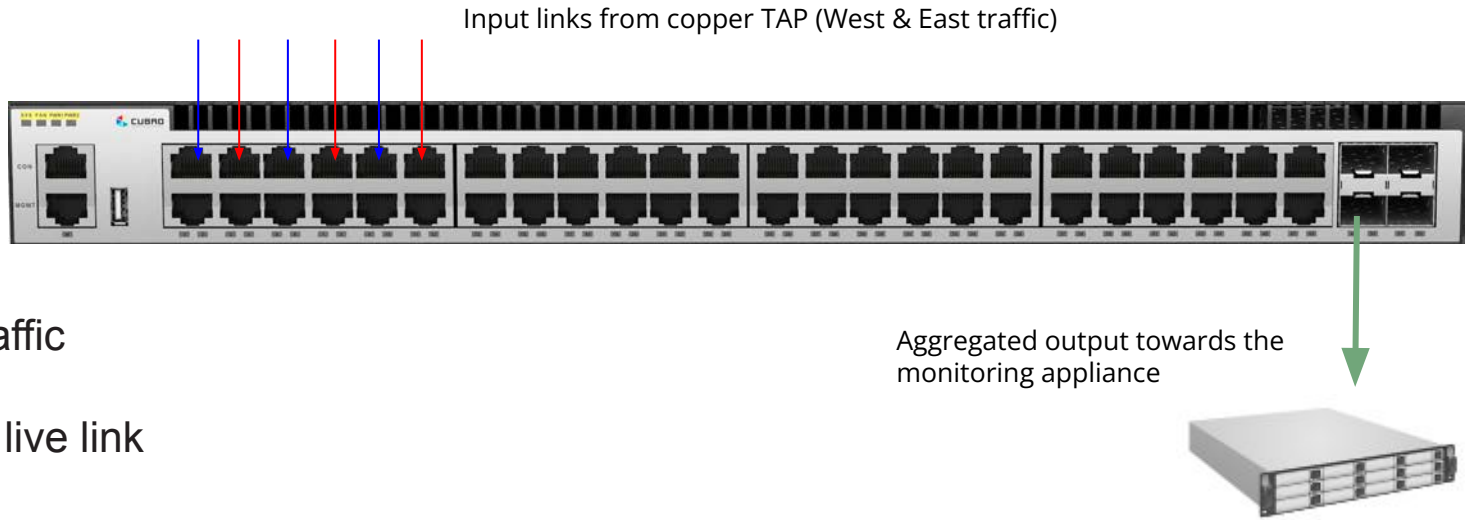
Applications / Use cases

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Aggregation

Traffic aggregation, multiplication and filtering to send only the relevant traffic to the monitoring tools.

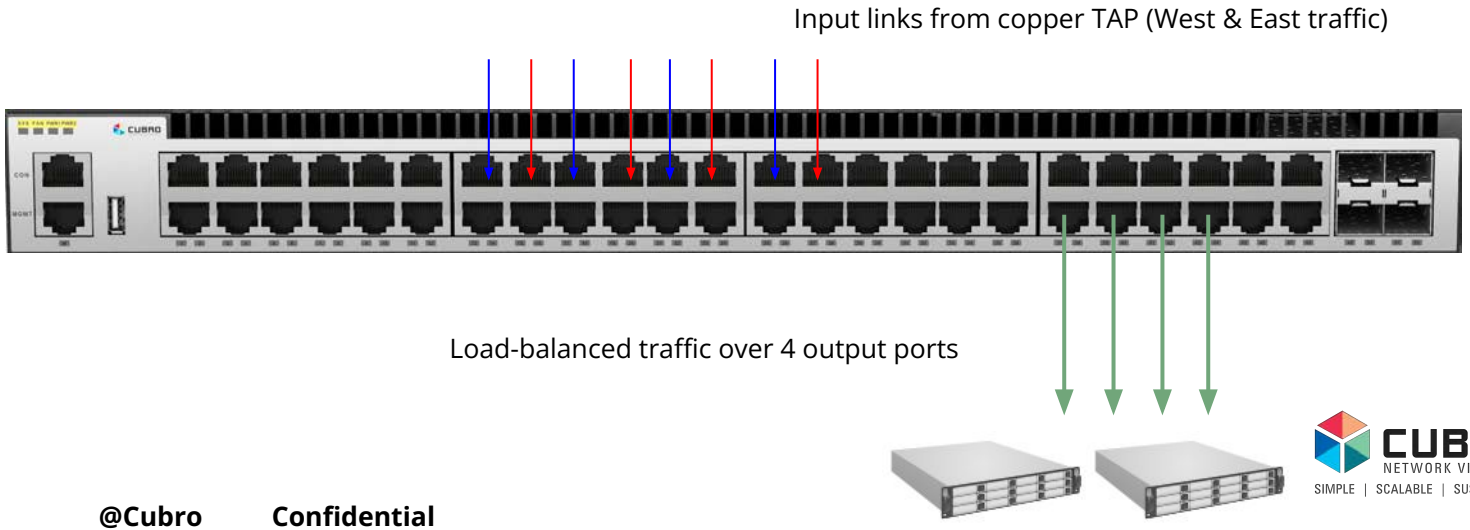
- no reorder
- no loss
- no jitter
- passively tap traffic
- no influence on live link



CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Load-balancing

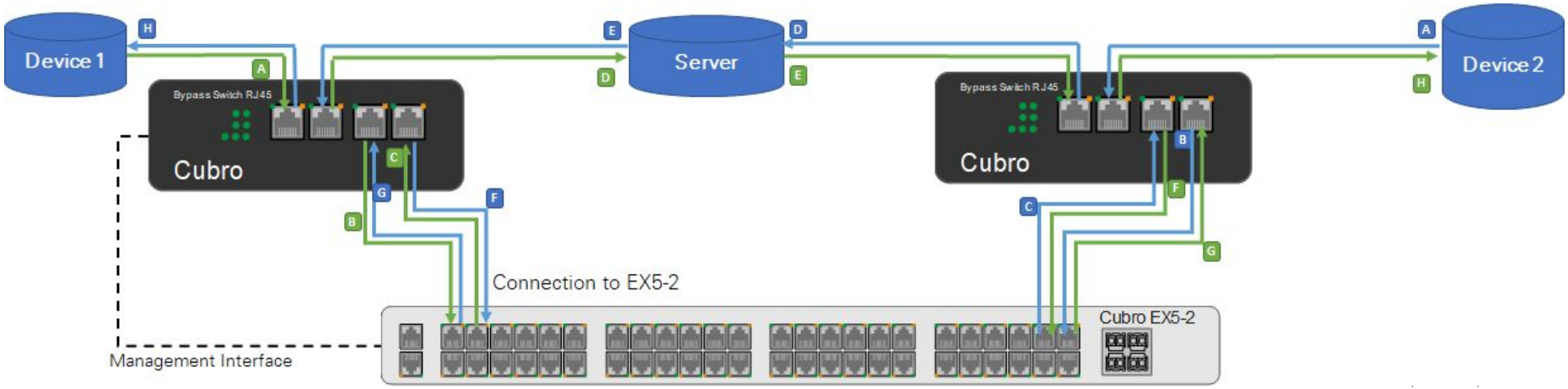
Cubro Packetmasters can filter the network traffic before performing session aware load balancing for the targeted traffic into 4 output ports. This functionality of the Cubro Packetmasters ensures the efficiency, reliability and effectiveness of each of the monitoring tools.



Bypass application

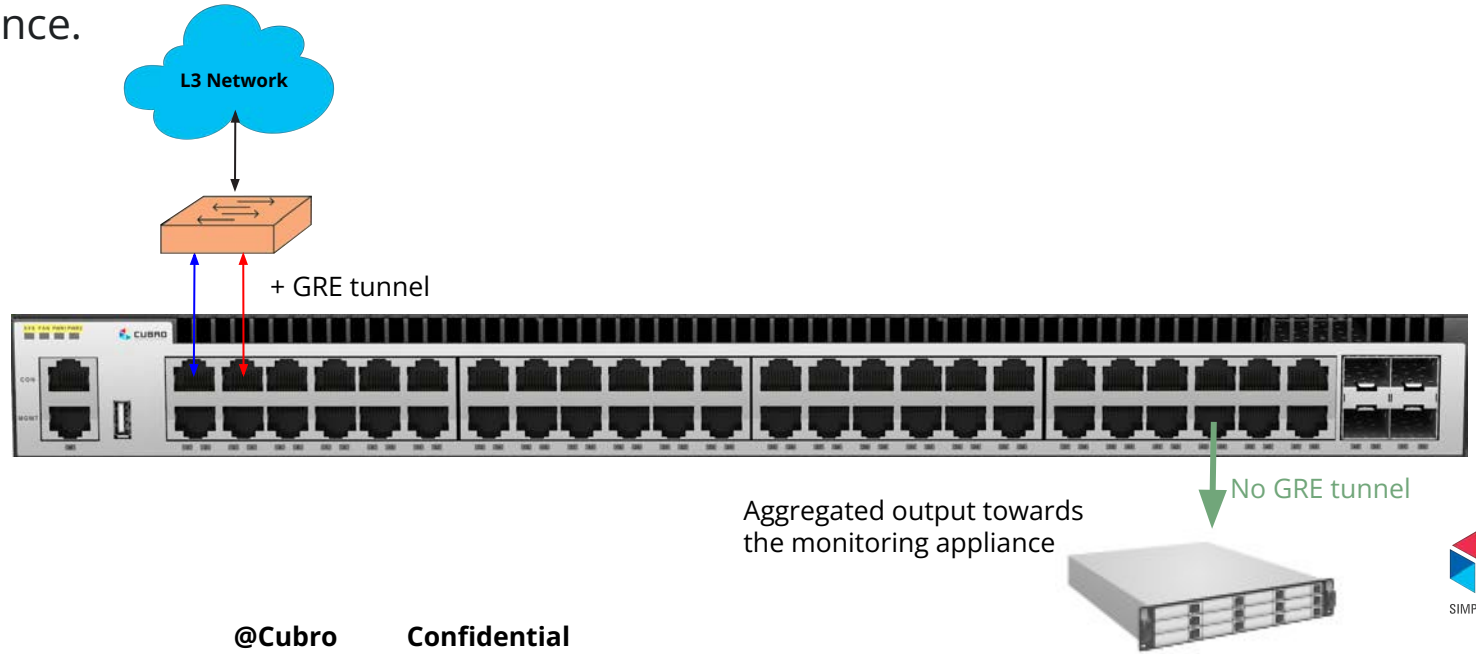
Cubro Packetmasters can be used as an inline tool for bypassing sensitive devices and to create an alternative route for the traffic flow, keeping the system alive.

To avoid a SPOF (Single Point of Failure), additional Cubro Bypass Switches are required to ensure a 100% fail-save environment.



Tunnel termination (VXLAN/GRE/NVGRE)

In virtual environments it may be required to forward relevant traffic through a L3 network to the monitoring system. Cubro Packetmasters allow to terminate VXLAN/GRE/NVGRE tunnels and forward the de-encapsulated traffic to the monitoring appliance.

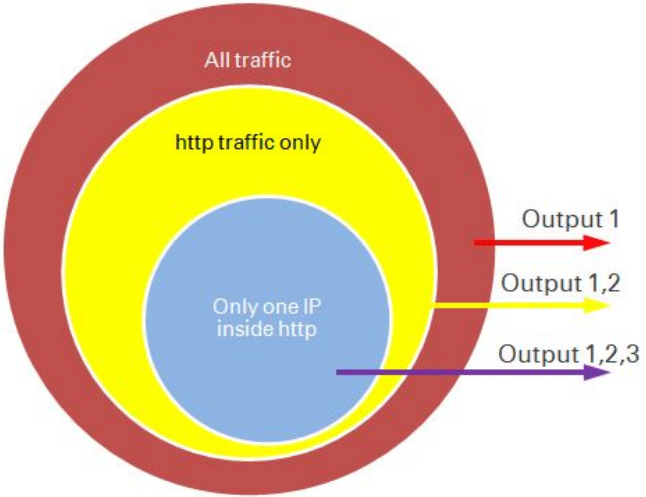


Overlapping Filters

Sometimes the same traffic should be available at multiple egress ports

- Assign highest priority to smallest traffic portion (most detailed filter criteria)
- Send traffic to all other ports where needed
- Continue with setup for other filters

Highest priority: ***65535***
Lowest priority: ***0***

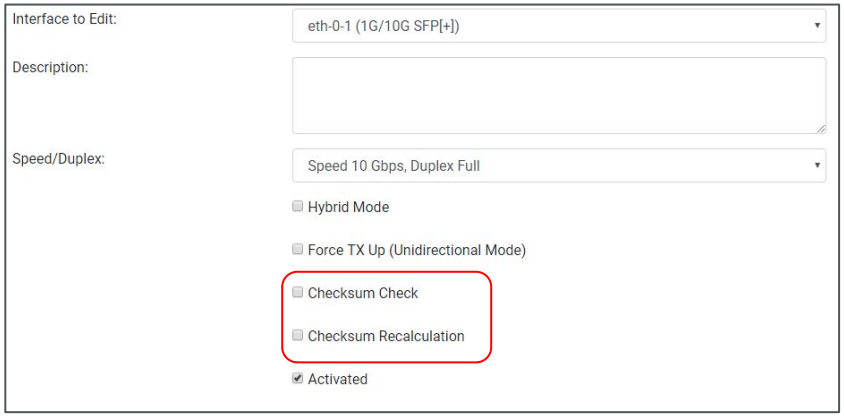


60000	input=6, IP, TCP Port 80	Output=1,2,3
50000	input=6, TCP Port 80	Output=1,2
40000	input=6	Output=1

CRC transparency

Hybrid Packetmaster platform not only allows 100% transparency to L2 protocols but also to CRC errors.

- Per default, the device will drop incoming CRC packets
- Via a simple configuration option, the ingress and egress interfaces can be allowed to receive and forward incoming CRC errors transparent.
- This option makes it possible that the monitoring appliance provides statistics about CRC errors of the live network



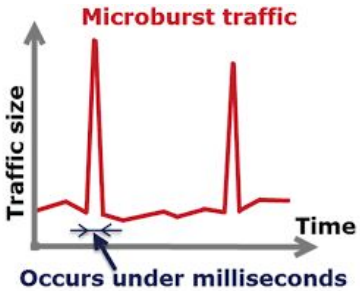
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Microburst detection

What are microbursts?

In Ethernet/IP networking, micro-bursting is a behavior seen on fast packet-switched networks, where rapid bursts of data packets are sent in quick succession, leading to periods of full line-rate transmission that can overflow packet buffers of the network stack, both in network endpoints and routers and switches inside the network. It can be mitigated by the network scheduler. In particular, micro-bursting is often caused by the use of the TCP protocol on such a network.

In an aggregation application where the aggregated output combines the traffic of several inputs it can happen that the egress port gets overloaded because of bursty input traffic – see following picture.



How to overcome this problem?

If the input traffic can not be smoothed or shaped the Aggregator needs to have a buffer that holds the data until there is again free bandwidth available to send the data. Basically two different concepts are available for buffering. The first one is to use a dedicated buffer per port while the second concept uses a centralized buffer that is available for any port that requires it. The Packetmaster EX G4 family supports both concepts.

In the centralized buffer mode the Cubro Packetmaster supports 9 MB of buffer. In order to avoid that a single ports uses up all the buffer size of 9 MB a single port can use a maximum of 8 MB.

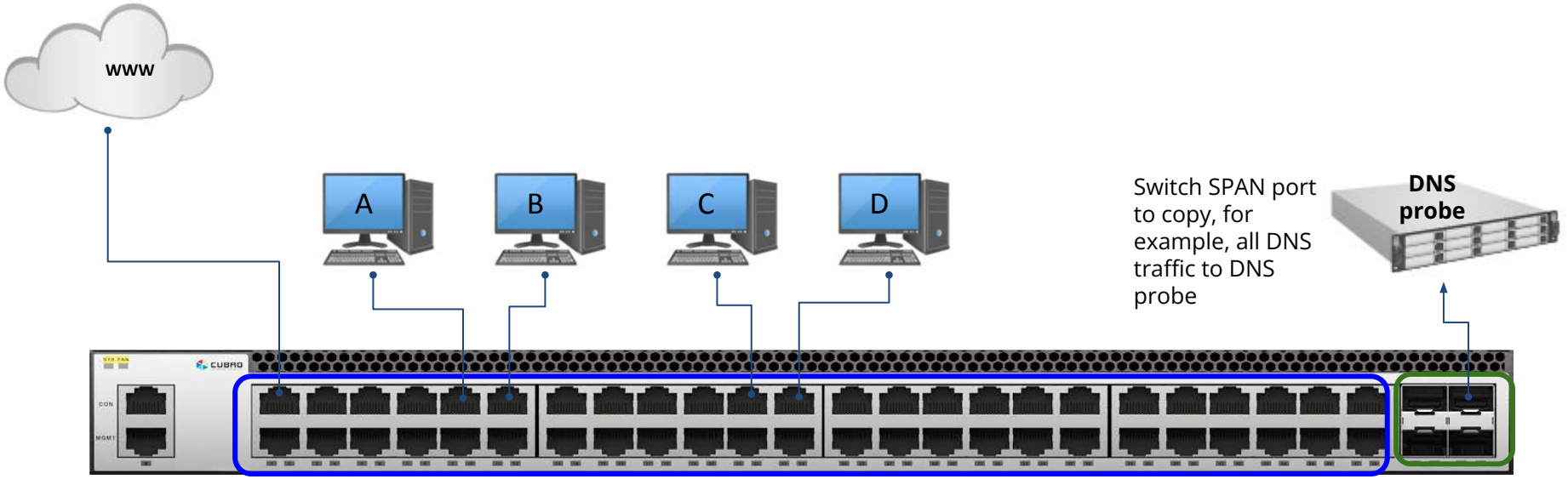
Visibility via Port statistics

In the case of packet drop due to oversubscription, the port statistics of the dedicated ports will show a counter for the number of dropped packets. This is a useful indicator for the user, it signals that either the filtering needs to be extended or it is required to add more output ports for the forwarded traffic.

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Switch SPAN port

The architecture allows to copy relevant traffic over a designated output port towards a monitoring appliance. The below example explains how an external DNS monitoring can be fed with relevant traffic. **No additional TAPs, NPB or other switches are required.**




THANK YOU