

Advanced Cubro Bypass TAP & Universal Optical Bypass

APPLICATION NOTE

Content



1. Hardware specs Copper Bypass TAP
2. Cubro Concept
3. Drill down of the Web UI
4. Use cases
5. Universal Optical Bypass (after page 32)

Hardware Specs

Advanced Copper Bypass TAP



- 10/100/1000 **Copper bypass switch**, with several trigger options
- 10/100/1000 **Copper TAP** with “no link drop” feature
- 4 x 10/100/1000 Copper port **patch panel**

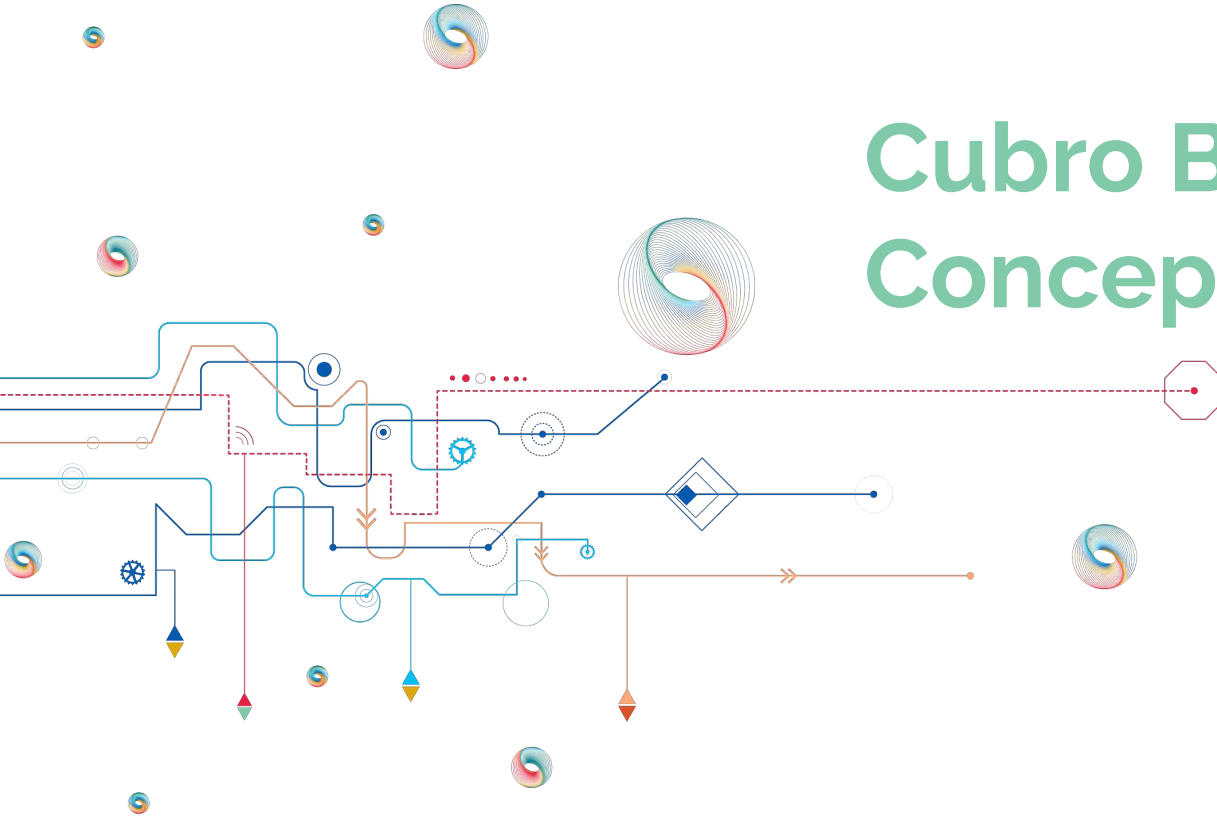


Features of the Cubro Bypass TAP



- Available as electrical or optical design
- Can be used as passive TAP or Bypass Switch
- Trigger options:
 - Ping (ICMP)
 - Rest API
 - GPIO pins
 - Front panel button
 - Power loss
- Graphical throughput statistics
- Intuitive Web UI for management
- SNMPv2 support
- Dual power supply

Cubro Bypass Concept



Standalone Bypass or with Packetmaster



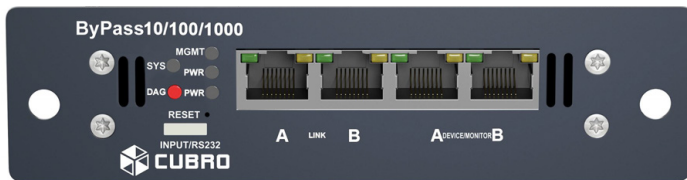
The Cubro Bypass TAP can work standalone, but also in combination with a Cubro Packetmaster.

Cubro Packetmasters have the ability to work as a bypass device with heartbeat functionality, on any port at any port speed.

The advantage of combining the Bypass TAP and a Packetmaster is to bypass multiple links that are connected to one sensitive device, for example a firewall.

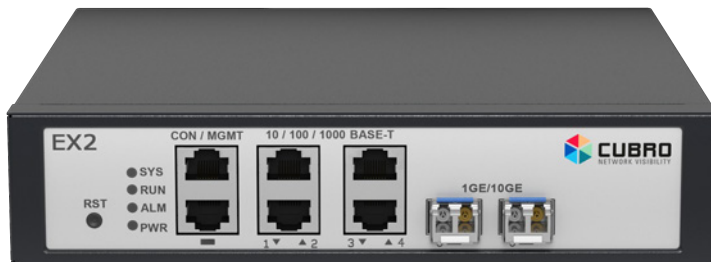
This modular concept reduces cost and offers a lot of flexibility.

Cubro Bypass Concept



Physical Bypass

&



Logical Bypass service chaining and heartbeat

Management
Connection

Cubro Copper Bypass Concept standalone

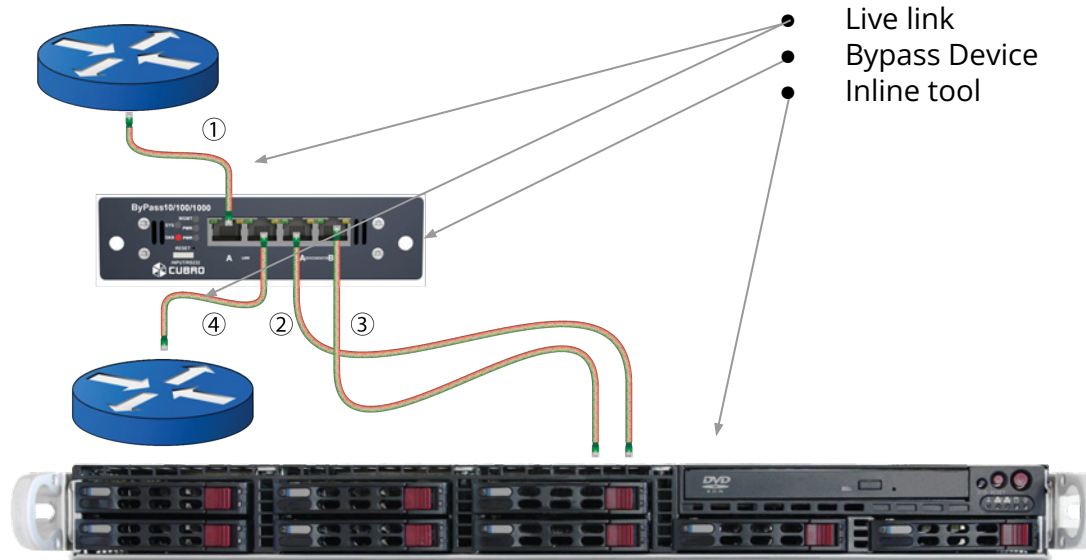


This is the simplest solution to use the Cubro Copper Bypass.

The inline tool is protected by Bypass tap **(without heartbeat)**

The Bypass link activation works with

- Ping (ICMP)
- Rest API
- GPIO pins
- Front panel button
- Power loss
- Bandwidth change

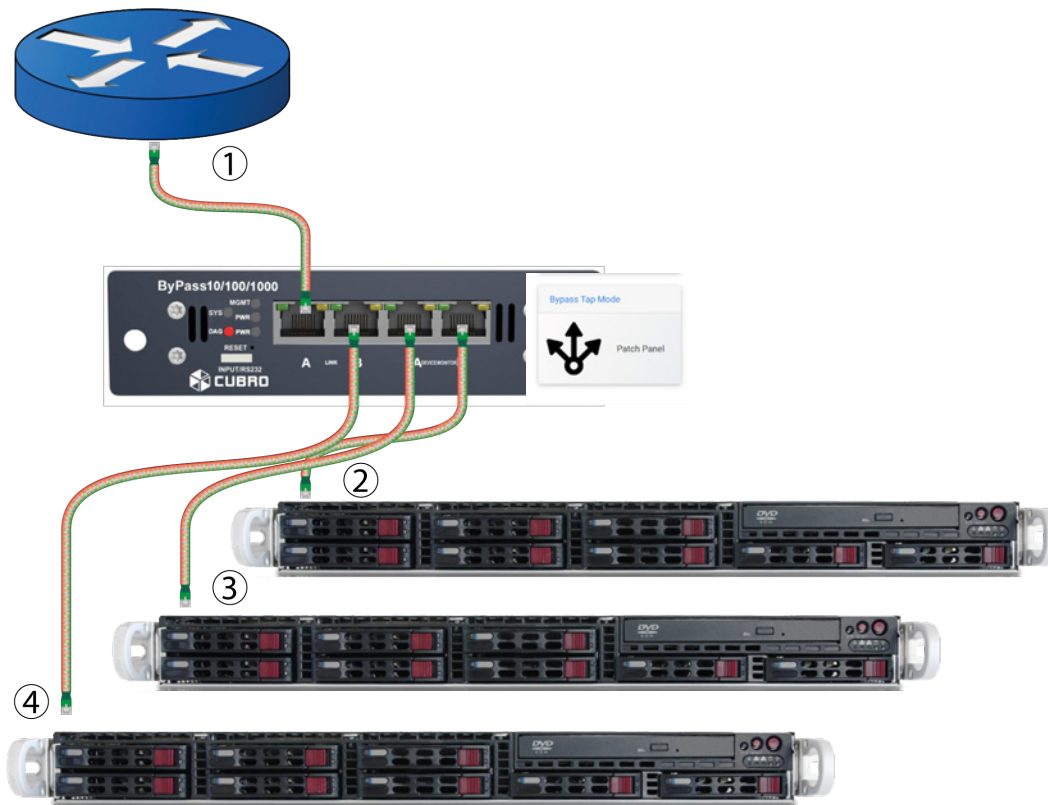


Patch panel mode



In this mode, the device works as a remote full duplex 4 port patch panels. (10/100/1000 Mbit/s)

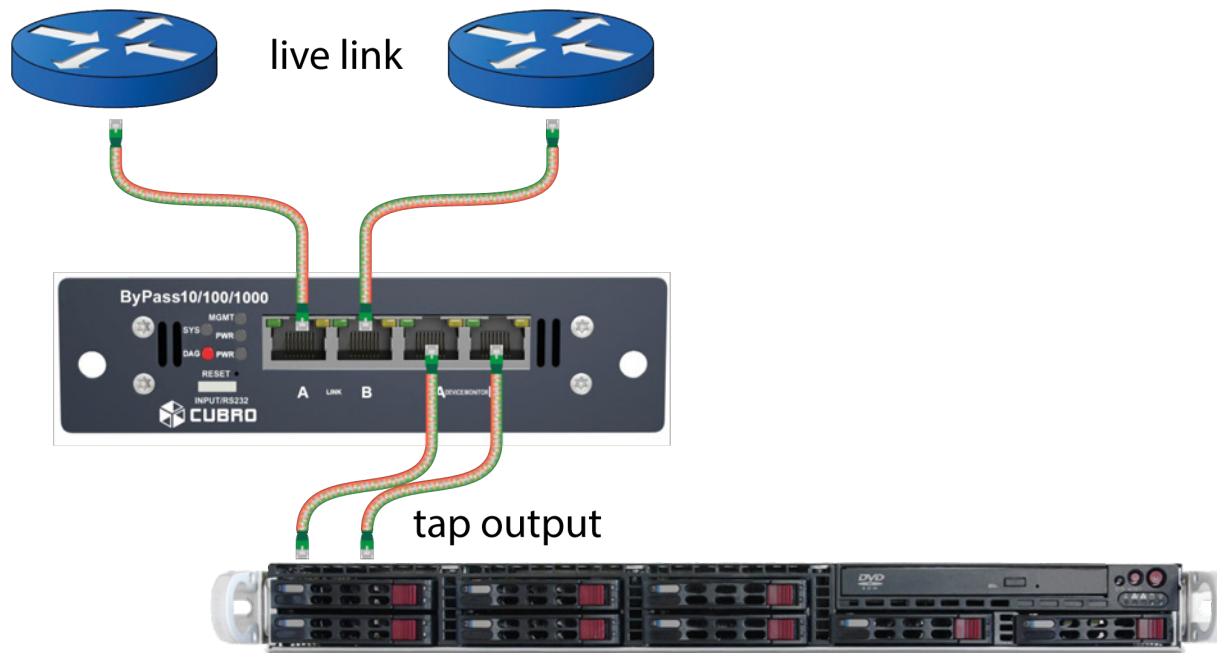
This is a nice add-on which could help in lab and test environments.



Tap mode



In this mode, the device works as a full duplex. (10/100/1000 Mbit/s) classical tap device.



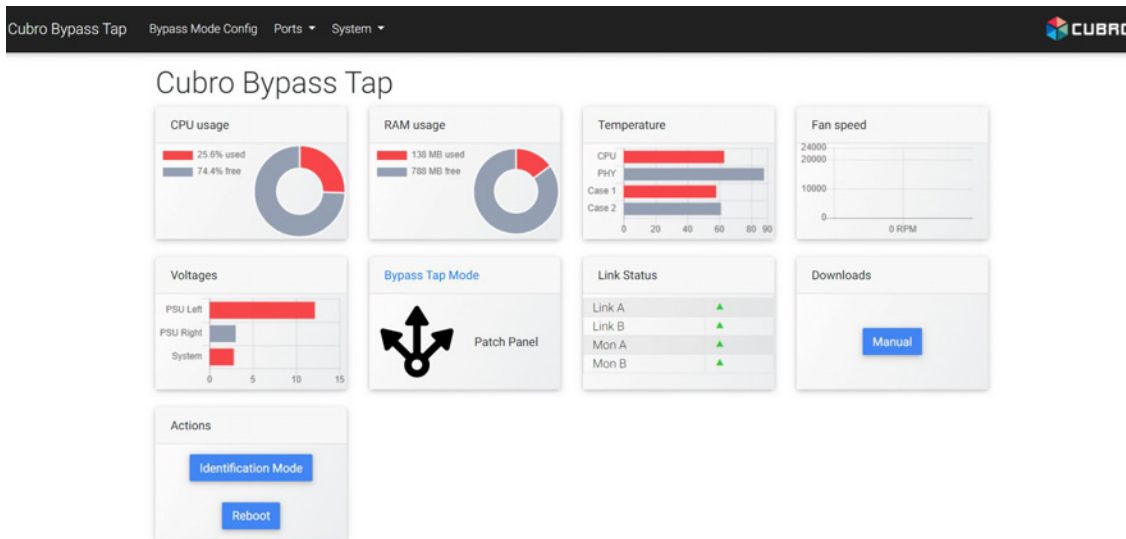
The Web UI

WEB UI Bypass Switch



After connecting to the Cubro Bypass TAP, the Web UI shows the current status of the Bypass TAP. This includes CPU / RAM usage, temperature, fan speed and the current mode of the Bypass TAP.

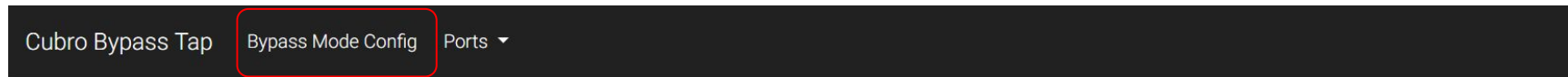
These values refresh every 5 seconds automatically.



Bypass Mode Config



Navigate to “Bypass Mode Config” via the top menu to access the configuration panel for the Bypass Mode. The Bypass supports up to 3 different modes which are explained in the next few slides.



Mode Config

Mode selection

Mode

Tap

Bypass

Tap

Patch Panel

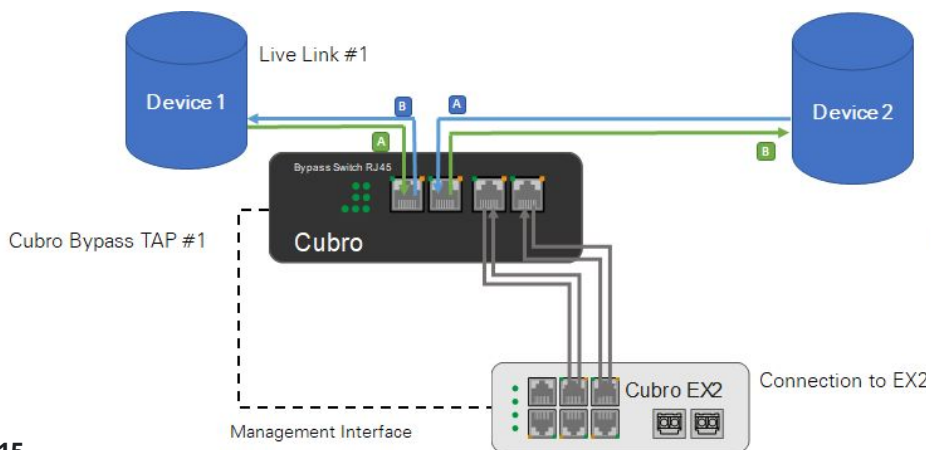
Usage in Bypass mode



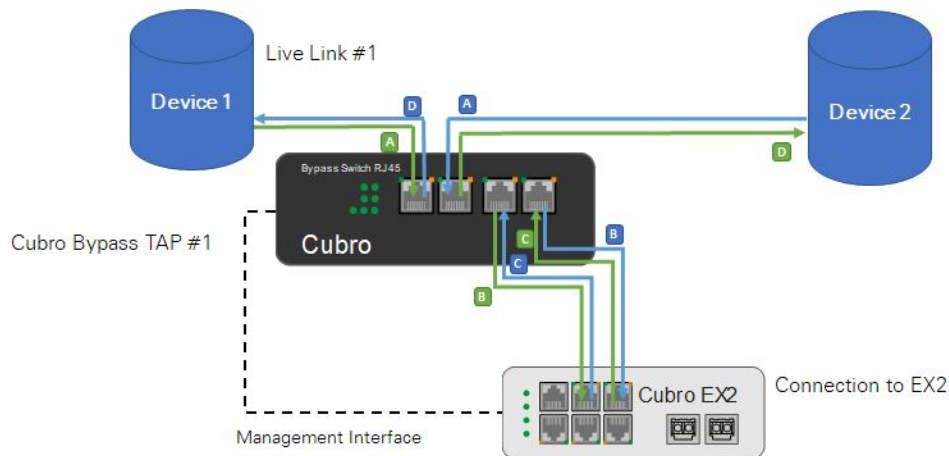
The Bypass TAP works as a 1 link Bypass switch.

When power is lost, the Bypass TAP will always switch to Bypass mode.

Bypass mode



Throughput mode



Bypass Mode - PING



The Bypass TAP can be controlled via ICMP protocol (ping).

Concept:

The Bypass TAP sends continuous ping requests to an external device.

As long as the external device responds to those pings the Bypass TAP will stay in Throughput mode. When the ping fails the Bypass TAP switches to Bypass mode as long as the external device does not answer the ping requests.

- Ping target: The IP address of the external device

Bypass Settings

Trigger

Ping

Ping target

192.168.0.144

Submit

Bypass Mode - REST



The Bypass TAP can be controlled via the REST API of the Bypass TAP and Cubro Packetmaster.

Concept:

A Cubro Packetmaster of Generation 2 to 4 can control the Bypass TAP via the installed Bypass App. To allow this application, the trigger needs to be set to "REST".

- Timeout: After x seconds the Bypass TAP engages the bypass mode when the Cubro Packetmaster is not reachable.

Bypass Settings

Trigger

REST

Timeout

0.1 seconds

Submit

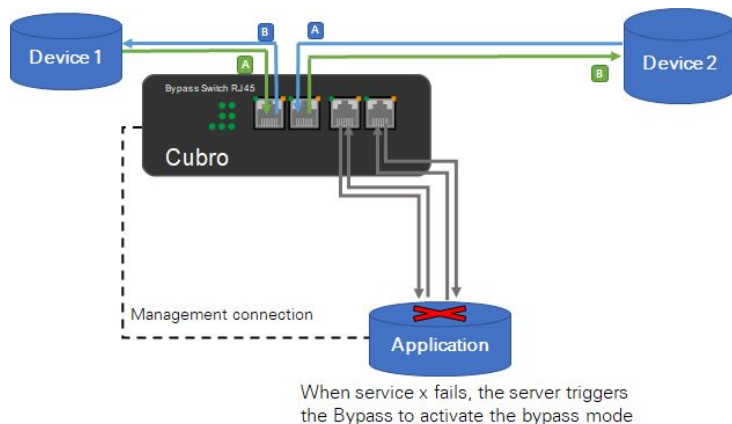
Bypass Mode - REST - 3rd party



The REST API of the Bypass TAP can also be used by any 3rd party device to trigger the bypass mode whenever it is required.

Concept:

An application which is bypassed using the Cubro Bypass TAP is connected to the same IP network like the before named Bypass. The application can use the REST API to take control over the Bypass and switch into Bypass mode when service x fails or crashes.



When service x fails, the server triggers the Bypass to activate the bypass mode

Bypass Mode - GPIO



The Bypass TAP can be controlled via the GPIO pins on the front panel.

Concept:

Using the four GPIO pins on the front panel also allows triggering of the bypass mode when the specific selected requirements are met.

Bypass Settings

Trigger

GPIO

Bypass device if

Pin 1 and 2 are shorted

AND

Pin 3 and 4 are shorted

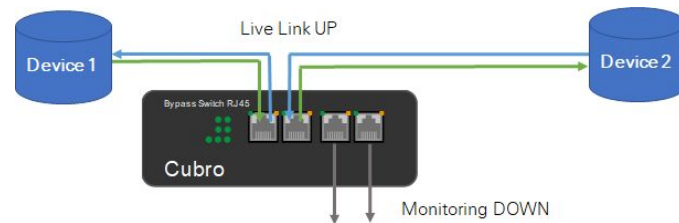
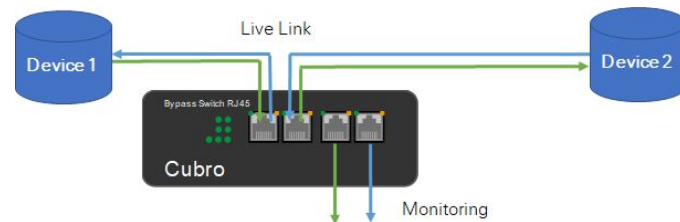
Submit

Usage in TAP mode



The Bypass TAP works as a common 1 link passive TAP.

- POWER ON:
 - The link connected via the “link ports” is UP
 - The ingress traffic is mirrored to the “device ports”.
- POWER OFF:
 - The link connected via the “link ports” is UP
 - No traffic mirroring during power off.
 - The monitoring ports connected to “device ports” are DOWN



Usage in patch panel mode



The Bypass TAP works as a 4 port patch panel with many combinations.

Each network port can work as an egress interface for one ingress interface.

This means that the patch panel mode allows aggregation (many to one) but no traffic duplication (one to many / many to many).

The patch panel mode always requires power.

When losing power the Bypass TAP will always switch to Bypass mode (Port 1 ↔ Port 2).

Mode Config

Mode selection

Mode

Patch Panel

Patch Panel Settings

Port

2

→ Port 1

Port

1

→ Port 2

Port

1

→ Port 3

Port

2

→ Port 4

Submit

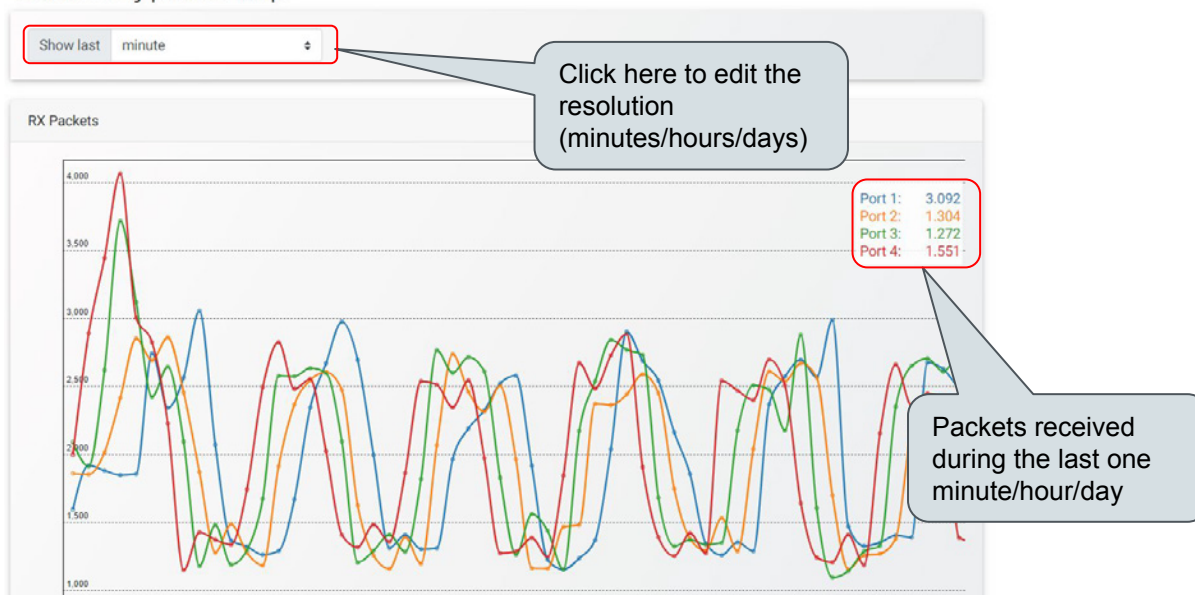
Ports - Counters



Navigate to “Ports” → “Counters” to access the port counter overview.

The values for RX packets and CRC errors are displayed graphically.

Cubro Bypass Tap



Ports - Configuration



Navigate to “Ports” → “Configurations” to access the port settings of the Bypass TAP.
The port settings are valid device-wide for all ports of the Bypass TAP.

Port Config

Device-wide Settings

Speed/Duplex

Autoneg

⌵

Master-Slave

Automatic

⌵

Jumbo Frames

Off

⌵

MDI/MDI-X

Port 1

Automatic

⌵

Port 2

Automatic

⌵

Port 3

Automatic

⌵

Port 4

Automatic

⌵

Submit

SNMP settings



The Bypass TAP support SNMPv2 per default.

This allows sending SNMP traps to a target host and to pull system information via SNMP GET or WALK.

A trap is sent to the defined host when

- Any physical port changes to status “down”
- Any physical port changes to status “up”
- Bypass mode is engaged
- Bypass mode is disengaged

SNMP Settings

SNMP Settings	
<input checked="" type="checkbox"/> Enable SNMP	
<input checked="" type="checkbox"/> Enable Trap	
Trap target	192.168.0.158
SNMP community	public
System description	Cubro BypassTap
System location	Sitting on the Dock of the Bay
System contact	Cubro Support <support@cubro.com>
<button>Submit</button>	



Bypass Application Use Cases

1 Link Bypass TAP - standalone



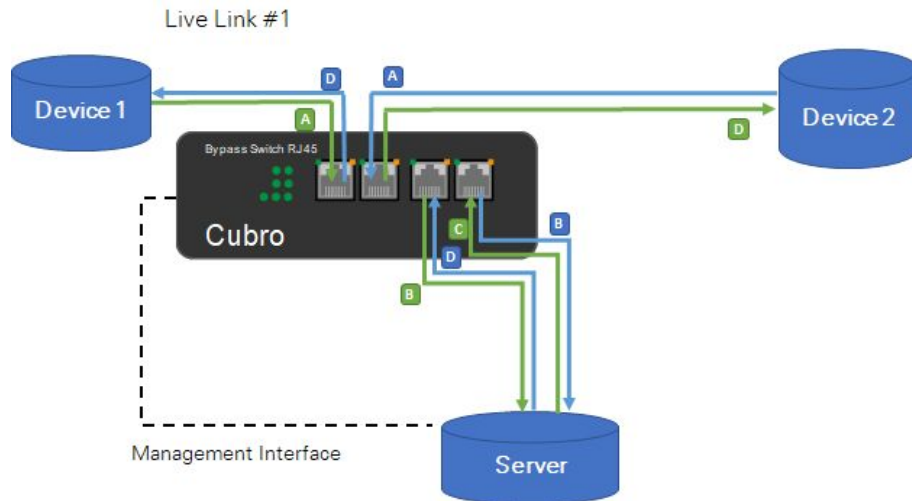
The application:

The Bypass TAP is connected to 2 network devices via the Link ports and to a 3rd party server via the device ports.

The trigger of the Bypass TAP is set to PING and it sends continuous ping requests to the server.

As soon as the server stops responding the pings the Bypass TAP will engage the bypass mode. When the server starts responding again the Bypass TAP switches back to the throughput mode.

This application works only via ICMP (ping). No heartbeat packets are used to monitor the connectivity between the server and the Bypass TAP.



EX2 + Bypass TAP - Normal status



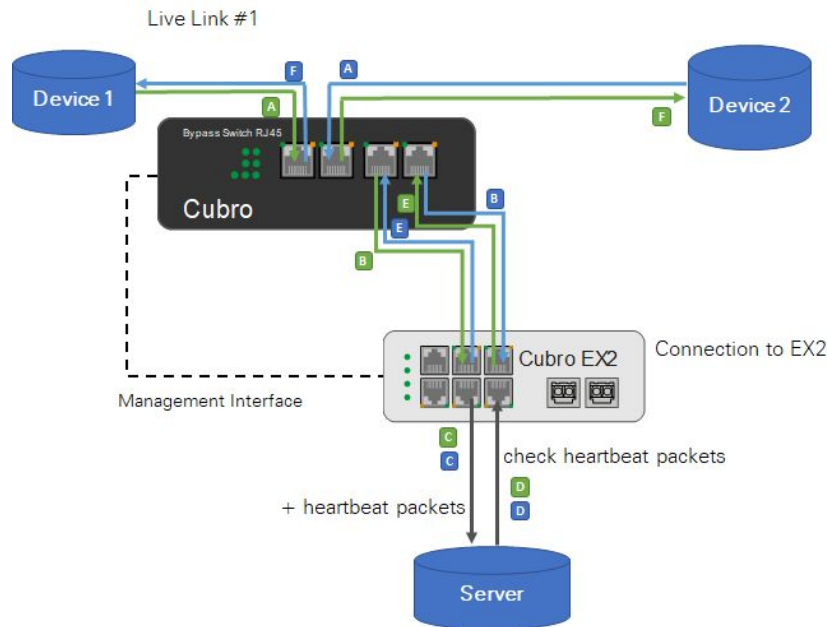
The application:

The Bypass TAP is connected to 2 network devices via the Link ports and to a Cubro Packetmaster EX2 via the device ports. A 3rd party server is connected to the EX2 via 2 x 1G copper. The Packetmaster EX2 sends heartbeat packets to the server via port #1 and expects to receive them again on port #2.

The trigger of the Bypass TAP is set to REST and the EX2 runs the Bypass App.

Traffic flow in throughput mode:

Device 1 ↔ Bypass TAP ↔ EX2 ↔ Server ↔ EX2 ↔ Bypass TAP ↔ Device 2



EX2 + Bypass TAP - Software Bypass



Software Bypass explained:

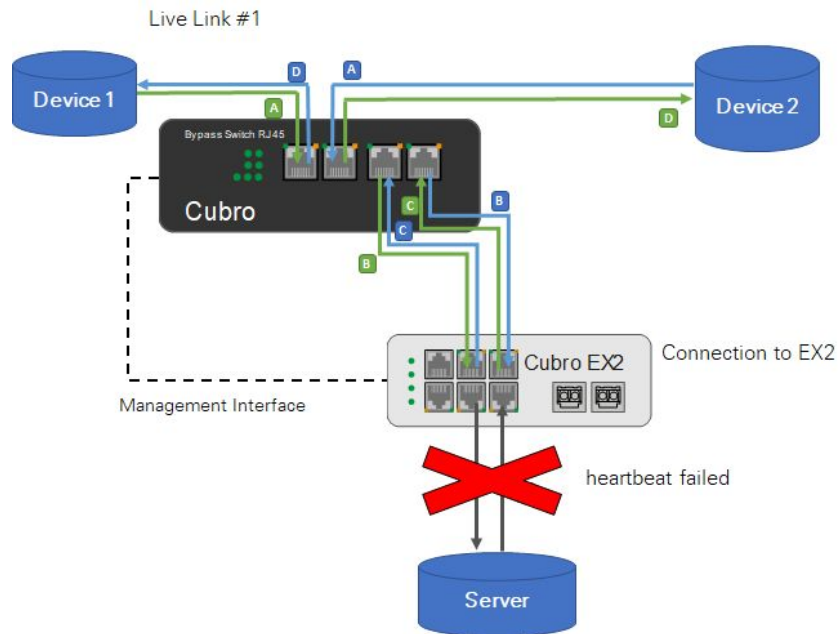
In the case the heartbeat packets are not detected by the EX2, it will engage the software bypass.

The configuration of the EX2 automatically changes to send the incoming traffic back to bypass TAP which reinserts the traffic back into the live link with minimal packet loss.

The Bypass TAP does not need to react at all because all bypassing is done by the EX2.

Traffic flow during software bypass:

Device 1 ↔ Bypass TAP ↔ EX2 ↔ Bypass TAP ↔ Device 2



EX2 + Bypass TAP - Hardware Bypass



Hardware Bypass explained:

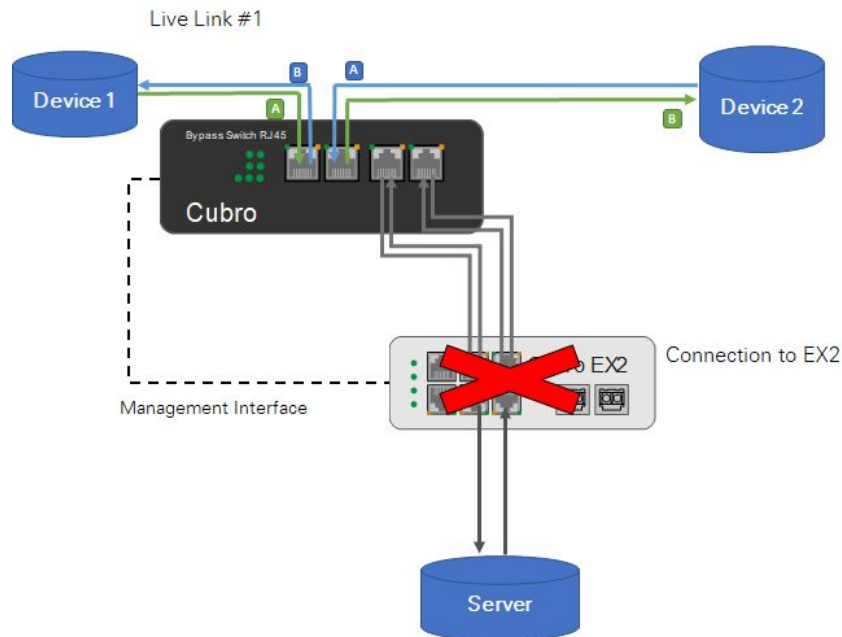
In the case that the EX2 fails or a connection between the Bypass TAP and the EX2 goes down, the Bypass TAP will switch to bypass mode to keep the live link up.

When the Bypass TAP engages the bypass mode, the EX2 and the external server will be bypassed and do not receive any traffic until the Bypass TAP switches back to throughput mode.

Bypass mode is also triggered when the Bypass TAP no longer receives power.

Traffic flow during hardware bypass:

Device 1 ↔ Bypass TAP ↔ Device 2

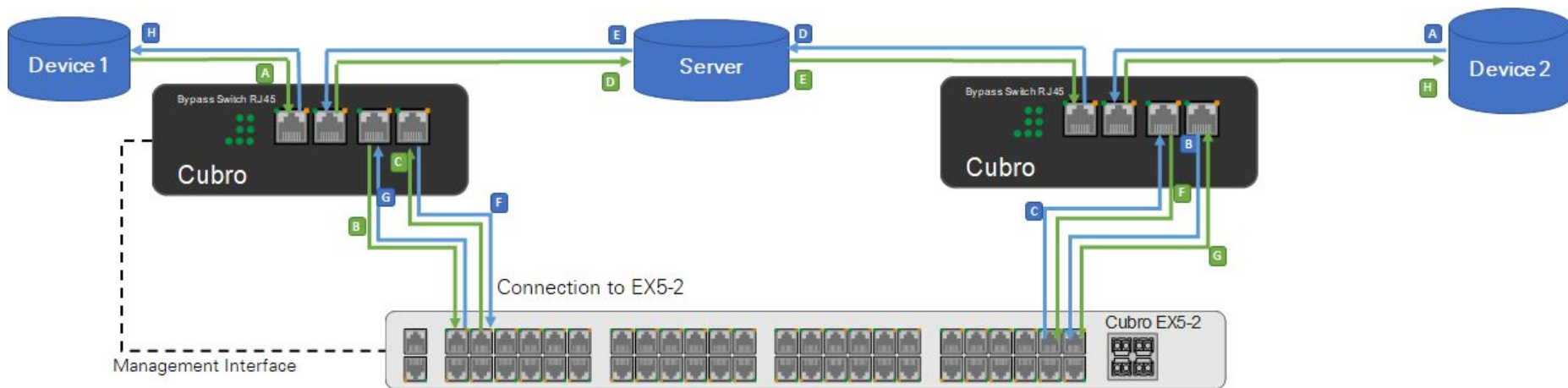


2 x Bypass TAP per Link



Setup explained:

In this setup, one copper link of 2 devices connected to a certain server is bypassed via 2 x Cubro Copper Bypass TAP. The advantages compared to the 1 Bypass solution is, that when the connection to the Packetmaster is disturbed the server is still part of the live link.



2 x Bypass TAP per Link - Software Bypass

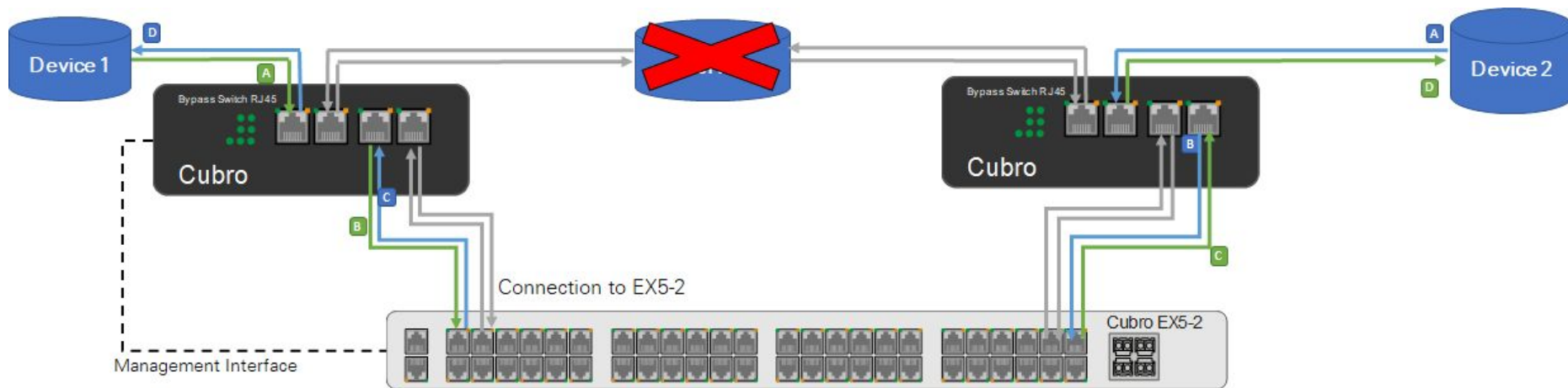


Software Bypass explained:

In the case the heartbeat packets are not detected by the EX5-2, it will engage the software bypass.
The Bypass TAPs do not need to react at all because all bypassing is done by the EX5-2.

Traffic flow during software bypass:

Device 1 ↔ Bypass TAP1 ↔ EX5-2 ↔ Bypass TAP2 ↔ Device 2



2 x Bypass TAP per Link - Hardware Bypass



Hardware Bypass explained:

In the case that the EX5-2 fails or a connection between the Bypass TAPs and the EX5-2 goes down, both Bypass TAPs will switch to bypass mode to keep the live link up. Compared to the “1 Bypass per Link” setup, the Server is still included to the live link.

Device 1 ↔ Bypass TAP1 ↔ Server ↔ Bypass TAP2 ↔ Device 2

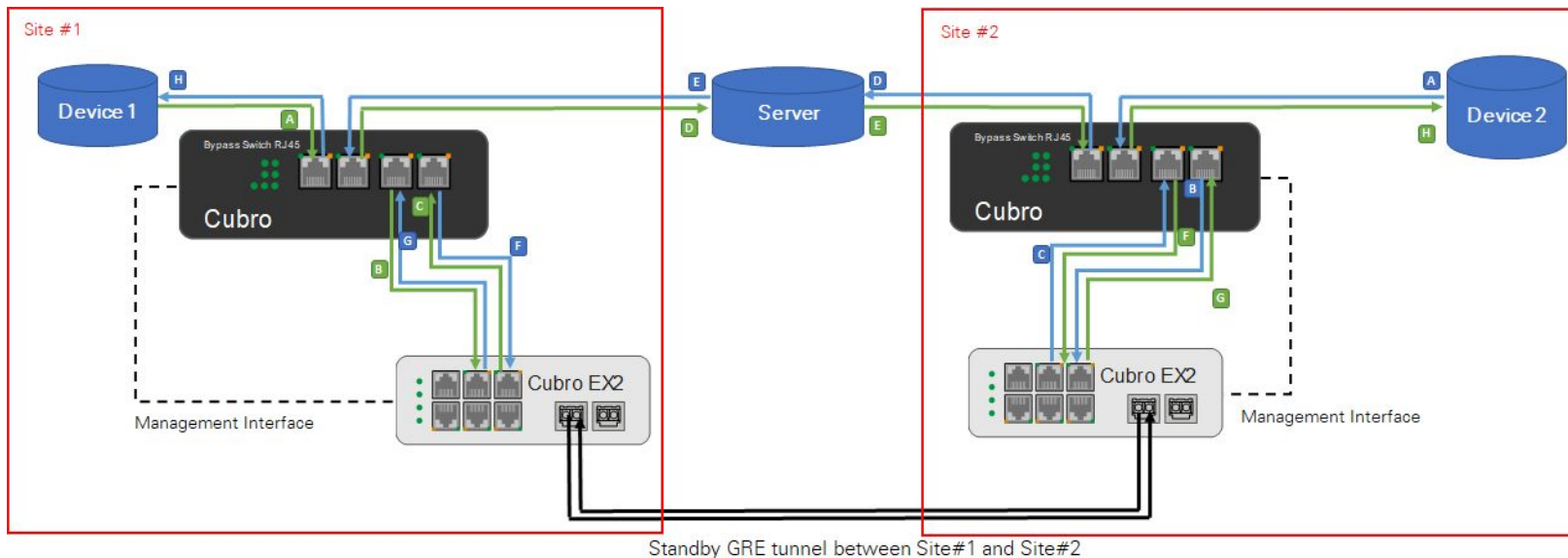


2 x Bypass TAP per Link over 2 sites

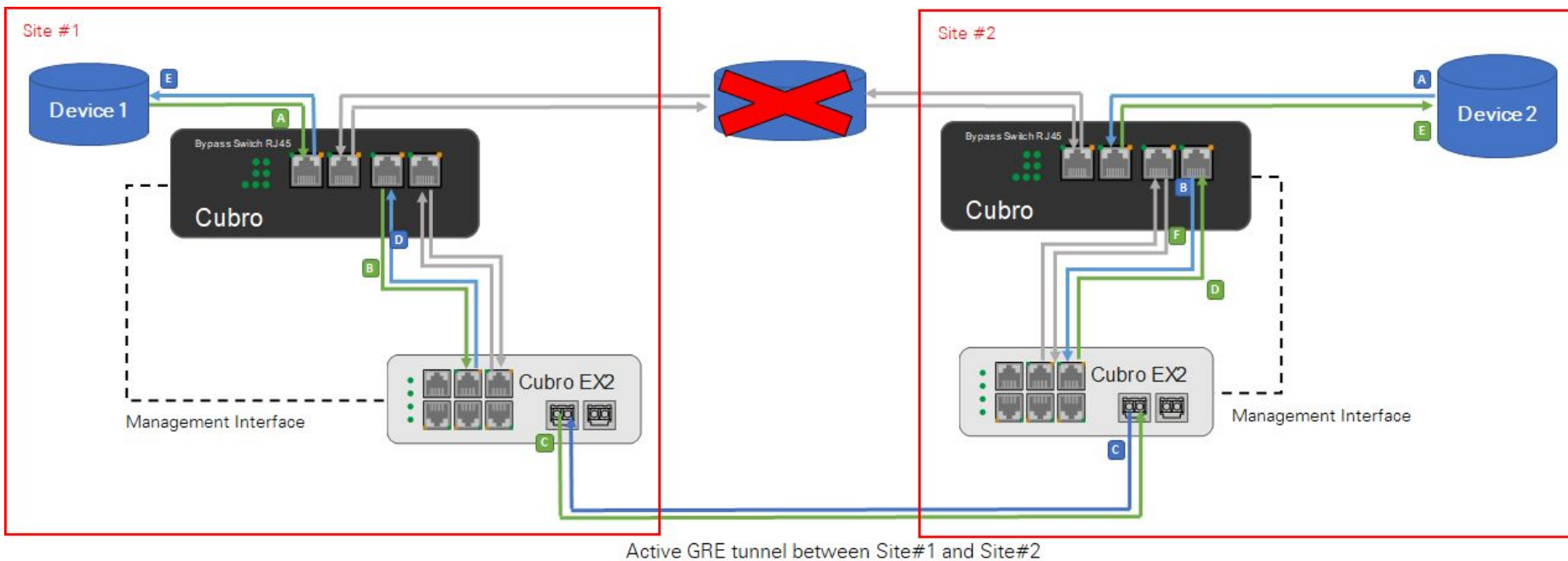


Setup explained:

Optional: Instead of one Packetmaster EX5-2, two Packetmaster EX2 can be used for interconnecting two different sites via a GRE tunnel. In the case that the server connecting both sites fails, the Cubro solution will bypass the server and the traffic can be distributed via the GRE tunnel of the Packetmaster EX2. (shown in next slide)



2 x Bypass TAP per Link over 2 sites (Bypassed)



Hardware Specs Optical Bypass

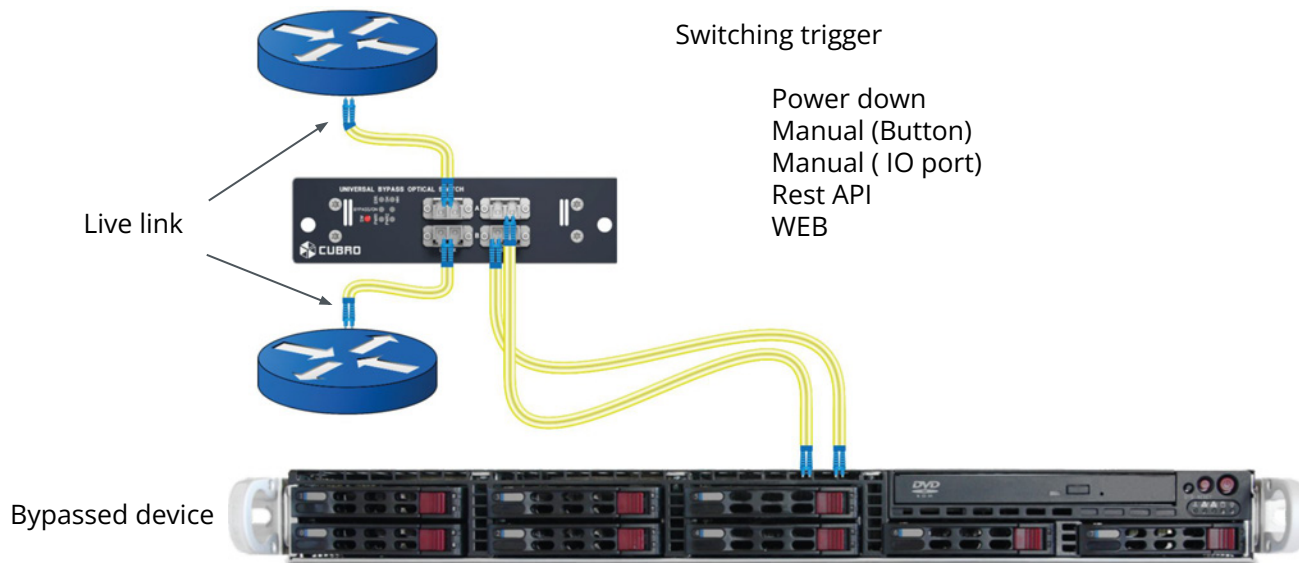
Universal Optical Bypass TAP



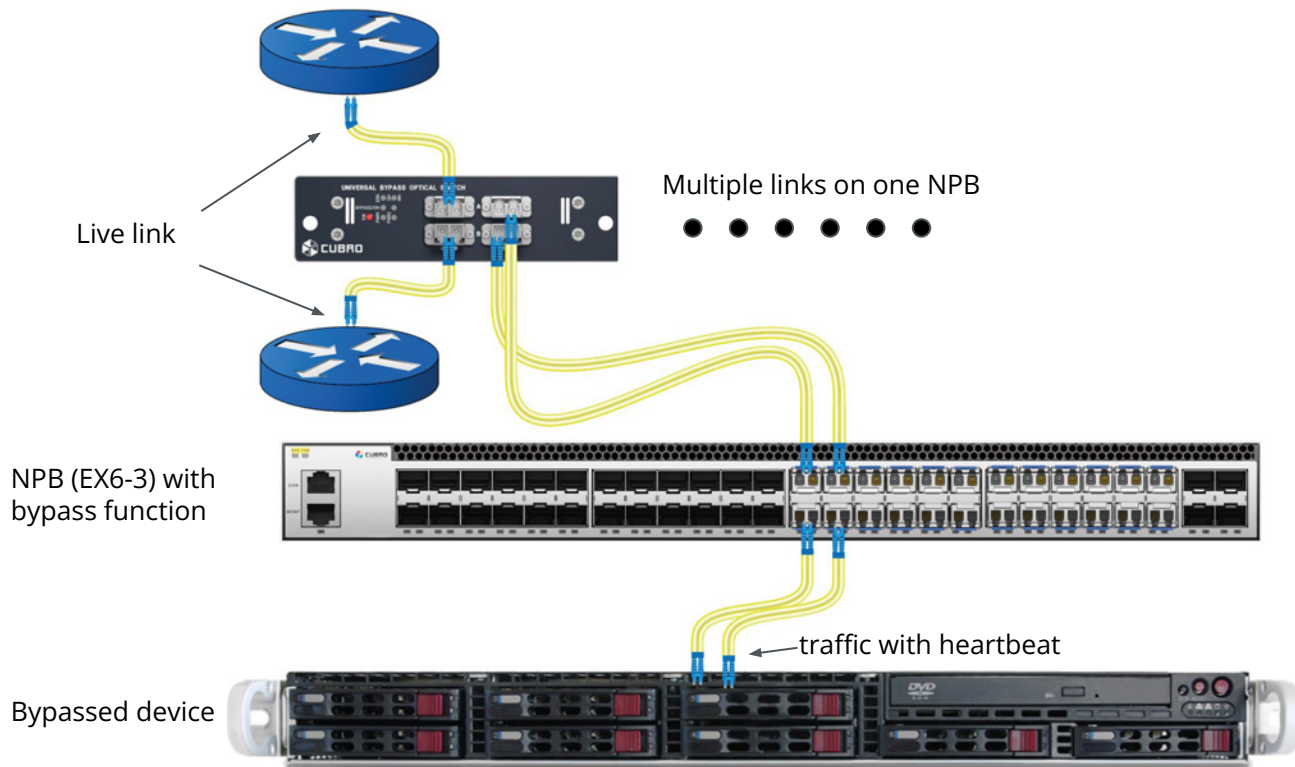
- Available Versions
 - 1/10/40/100 GBit/s SM
 - 1/10 GBit/s MM



Universal Optical bypass schema



Universal Optical bypass schema (heartbeat)



Universal Optical bypass schema (heartbeat multi-link)



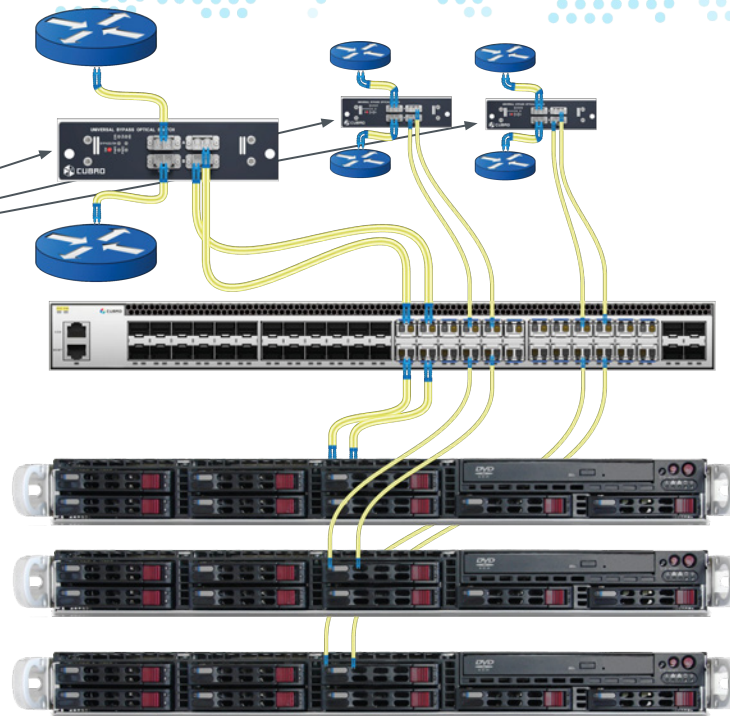
This example shows how the bypass can work on a multi-link environment!

In this drawing

Multiple links &

Multiple inline tools

In this case
each link is forwarded
to a designated tool.



Universal Optical bypass schema (heartbeat multi-link)



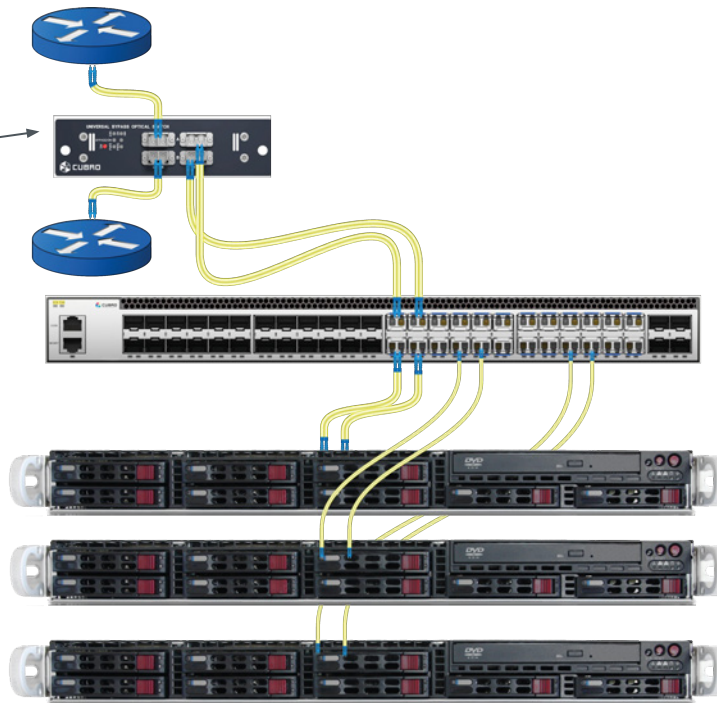
This example shows how the bypass and the NPB Supports link bypass and and service chaining in one Application

Live link &

Multiple inline tools

In this case
The NPB acts also as
the service chaining device
to forward the traffic to the tools
in a chain.

Follow the numbers to see the flow of the traffic
(because of simplicity we show only one direction but the application supports full duplex)



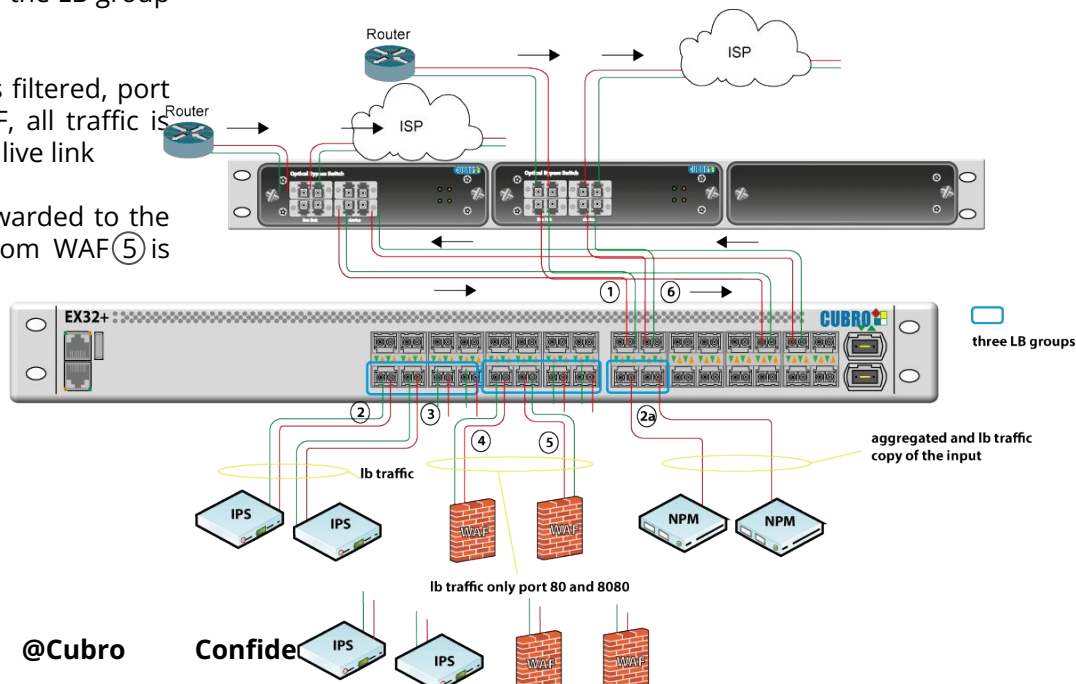
Multi-link multi-device application with EX32

① traffic from protecting optical bypass switch

② traffic is sent from input to the LB group 1 and 3 ②a

③ received traffic from IPS is filtered, port 80 and 8080 is sent to WAF, all traffic is sent to ⑥ and inserted in the live link

④ all http/https traffic is forwarded to the WAF, the received traffic from WAF ⑤ is reinserted to the live link ⑥



App Manager on Cubro NPB



It is possible to run the APP multiple times on different ports, in this case 4 times, to realize a multilink bypass

Available Apps

Actions	Name	Description
	SNMP Server	Runs an SNMP Server
	ArpResponder	Responds to an arbitrary packet with an ARP response
	HeartbeatBypass	This app is used to controll a Cubro Bypass Switch device.

Running Apps

Actions	PID	Name	Description	User Description	Status
	0	HeartbeatBypass	This app is used to controll a Cubro Bypass Switch device.	Bypass at 192.168.0.100	• IN_PORT on Port:3 LINK_DOWN • OUT_PORT on Port:4 LINK_DOWN
	1	HeartbeatBypass	This app is used to controll a Cubro Bypass Switch device.	Bypass at 192.168.0.101	• OUT_PORT on Port:5 LINK_DOWN
	2	HeartbeatBypass	This app is used to controll a Cubro Bypass Switch device.	Bypass at 192.168.0.102	• BYPASS_PORT_1 on Port:9 LINK_DOWN • BYPASS_PORT_2 on Port:10 LINK_DOWN • IN_PORT on Port:11 LINK_DOWN • OUT_PORT on Port:12 LINK_DOWN
	3	HeartbeatBypass	This app is used to controll a Cubro Bypass Switch device.	Bypass at 192.168.0.103	• BYPASS_PORT_1 on Port:13 LINK_DOWN • BYPASS_PORT_2 on Port:14 LINK_DOWN • IN_PORT on Port:15 LINK_DOWN • OUT_PORT on Port:16 LINK_DOWN

☒ Refresh Automatically

Bypass APP configuration screenshot



Main Properties

PID	2
Name	HeartbeatBypass
Description	This app is used to control a Cubro Bypass Switch device.

App Settings

User Description	Bypass at 192.168.0.102	
Check Interval	2000	Check interval in milliseconds
Connection Type	IP	Type of connection between EX32plus and Bypass
Bypass IP	192.168.0.102	IP address of the bypass device
Bypass Port 1	9	First port connected to the Cubro Bypass Switch. Optional. If given, flows connecting Bypass Port 1 and Heartbeat In-port will be created.
Bypass Port 2	10	Second port connected to the Cubro Bypass Switch. Optional. If given, flows connecting Bypass Port 2 and Heartbeat Out-port will be created.
Heartbeat In-port	11	Port on which the app expects the heartbeats to arrive
Heartbeat Out-port	12	Port on which the app sends the heartbeats
Protocol	UDP	Protocol of the heartbeat packets
Source MAC	00:00:00:00:00:01	Source MAC address of the heartbeat packets
Destination Mac	00:00:00:00:00:02	Destination MAC address of the heartbeat packets
Source IP	0.0.0.1	Source IP address of the heartbeat packets
Destination IP	0.0.0.2	Destination IP address of the heartbeat packets
Source Port	5555	Source UDP port of the heartbeat packets
Destination Port	5556	Destination UDP port of the heartbeat packets

✓ Modify App

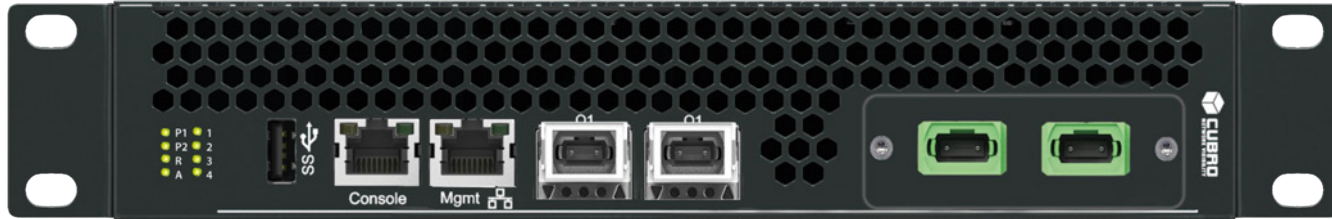
40 & 100 Gbit bypass

100/40/4 x 25 /4 x 10 Gbit Bypass



device link

active link



With programmable heartbeat
½ 19" in size / 2 links in 19" possible



Cubro is launching the new Bypass solution to meet the increasing demand. The new Bypass is a better solution based on its NPB technology at an affordable price.

Quality & Environment Management



Cubro is certified with ISO 9001 for Quality Management to ensure to deliver best product and services



Cubro is certified with ISO 14001 for Managing the efforts to protect our environment.

