How to use header modification in monitoring

APPLICATION NOTE

Jan 2021

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Contents

1. What is header modification?

2. Header modification feature on Cubro EX Series

3. Use-case for header modification

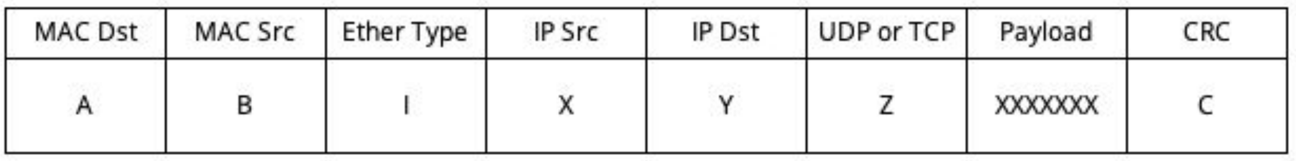
4. Summary

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

What is header modification?

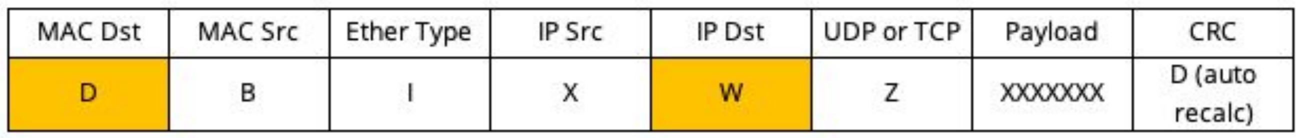
Header modification allows overwriting original packet header fields such as MAC Destination or IP Destination.

Original Packet



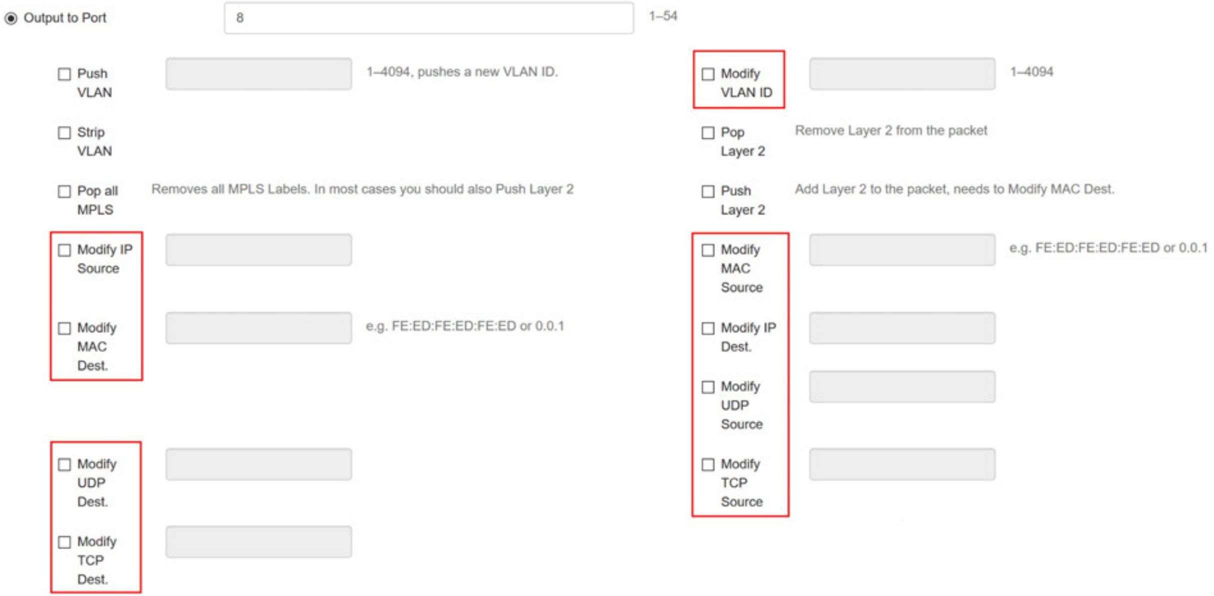
MAC Dst	MAC Src	Ether Type	IP Src	IP Dst	UDP or TCP	Payload	CRC
A	B	I	X	Y	Z	XXXXXXX	C

Modified Packet



MAC Dst	MAC Src	Ether Type	IP Src	IP Dst	UDP or TCP	Payload	CRC
D	B	I	X	W	Z	XXXXXXX	D (auto recalc)

Header Modification Feature on Cubro Packetmaster EX series



● Output to Port 8 1–54

□ Push VLAN 1–4094, pushes a new VLAN ID.

□ Strip VLAN

□ Pop all MPLS Removes all MPLS Labels. In most cases you should also Push Layer 2

□ Modify IP Source

□ Modify MAC Dest. e.g. FE:ED:FE:ED:FE:ED or 0.0.1

□ Modify UDP Dest.

□ Modify TCP Dest.

□ Modify VLAN ID 1–4094

□ Pop Layer 2 Remove Layer 2 from the packet

□ Push Layer 2 Add Layer 2 to the packet, needs to Modify MAC Dest.

□ Modify MAC Source e.g. FE:ED:FE:ED:FE:ED or 0.0.1

□ Modify IP Dest.

□ Modify UDP Source

□ Modify TCP Source

Cubro EX Packetmaster family allows modifying following header fields via easy- to-use WebGUI (see screenshot on the left).

The fundamental characteristic of the Cubro Packetmaster EX family is that every output port can have different values.

Use-case for header modification

Syslog is commonly used for system management, security auditing and other analysis. Network monitoring uses SNMP traps to get alerts from the network elements. Configuring IP addresses for Syslog and SNMP traps recipients is not difficult, but it can create a lot of work if there are lots of network elements and many monitoring systems are receiving data. New monitoring systems or changes in IP address plan add to the workload.

There is an easier way – create just one default IP address for Syslog and SNMP manager. And for additional recipients use a **Cubro Packetmaster EX to multiply traffic**.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Use-case for header modification

Challenge

Several monitoring systems expect to get traps and syslog from various devices. Currently for certain equipment you can specify up to 5 SNMP trap IP addresses and you can set several IP addresses for syslog as well (conf t … logging host x.x.x.x). However maintenance is going to be a challenge as you need to modify the settings per device.

Solution

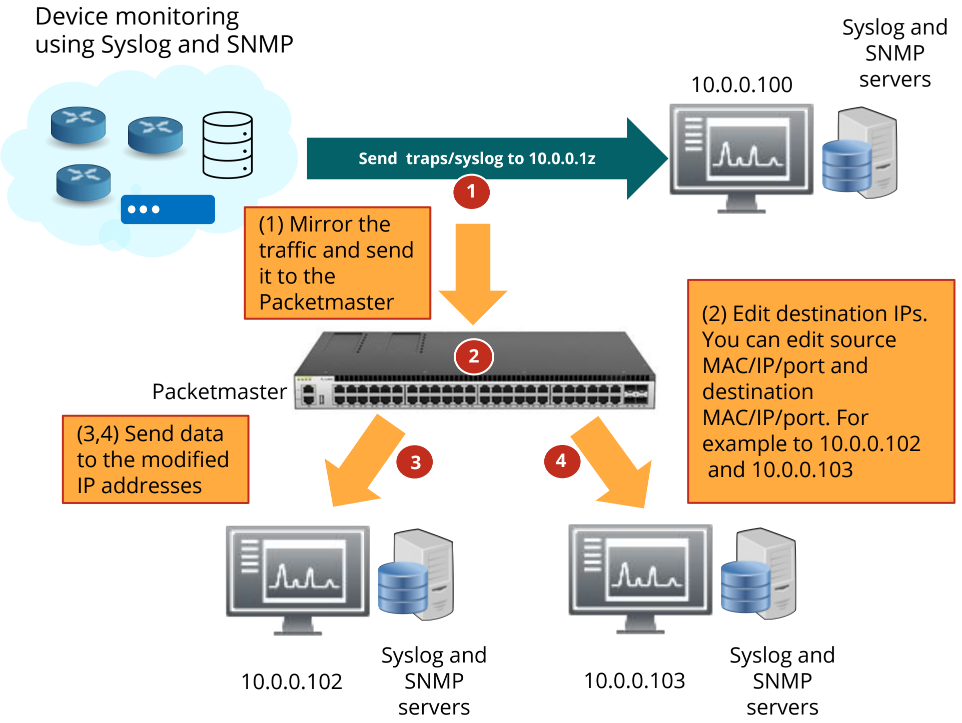
Instead of defining multiple addresses per device, use just one. Mirror the traffic from the devices, which you already are most likely doing, modify destination IP addresses and send the packets to the destination monitoring systems.

Benefits

One centralized place for maintaining monitoring system addresses. Easy to add and modify new syslog and SNMP servers. Cubro solution allows the modifications per output thus allowing several destinations to be configured conveniently.

Cubro device support

EX2 /EX5 /EX6 /EX12 /EX32/EX484-3 /EX48400 /EX20400



(1) Mirror the traffic and send it to the Packetmaster

(2) Edit destination IPs. You can edit source MAC/IP/port and destination MAC/IP/port. For example to 10.0.0.102 and 10.0.0.103

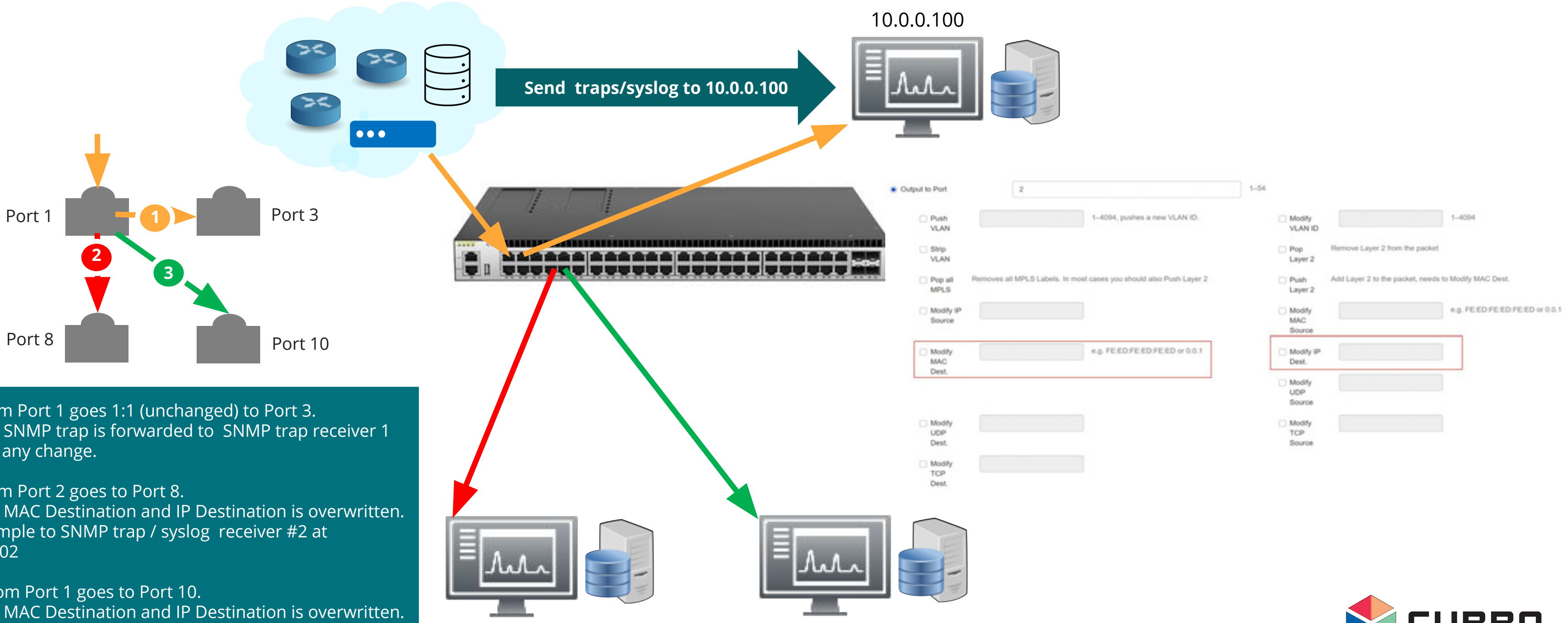
(3,4) Send data to the modified IP addresses

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Use-case/Details of header modification

MAC Source : 00:00:00:00:00:01 (MAC Address of the SNMP trap sender)
IP Source : 10.0.0.1 (IP Address of the SNMP trap sender)

MAC Destination : 00:00:00:00:00:AA (MAC Address of normal/default SNMP trap receiver)
IP Destination : 10.0.0.100 (IP Address of normal/default SNMP trap receiver)



● Output to Port 2 1–54

□ Push VLAN		1–4094, pushes a new VLAN ID.	□ Modify VLAN ID		1–4094
□ Strip VLAN			□ Pop Layer 2	Remove Layer 2 from the packet	
□ Pop all MPLS	Removes all MPLS Labels. In most cases you should also Push Layer 2		□ Push Layer 2	Add Layer 2 to the packet, needs to Modify MAC Dest.	
□ Modify IP Source			□ Modify MAC Source		e.g. FE:ED:FE:ED:FE:ED or 0.0.1
□ Modify MAC Dest.		e.g. FE:ED:FE:ED:FE:ED or 0.0.1	□ Modify IP Dest.		
			□ Modify UDP Source		
□ Modify UDP Dest.			□ Modify TCP Source		
□ Modify TCP Dest.					

1. Traffic from Port 1 goes 1:1 (unchanged) to Port 3.
   - Original SNMP trap is forwarded to SNMP trap receiver 1 without any change.
2. Traffic from Port 2 goes to Port 8.
   - Original MAC Destination and IP Destination is overwritten.
   - For example to SNMP trap / syslog receiver #2 at 10.0.0.102
3. Traffic from Port 1 goes to Port 10.
   - Original MAC Destination and IP Destination is overwritten.
   - For example to SNMP trap receiver #3 at 10.0.0.103

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Summary

The header modification feature of the Packetmaster EX is an excellent way to multiply traffic to different receivers without changing any configuration on live equipment. It can be used to distribute traffic to parallel running Syslog or SNMP receivers. Moreover, it can be used in testing applications when packets from a test generator need to be multiplied to generate more load.

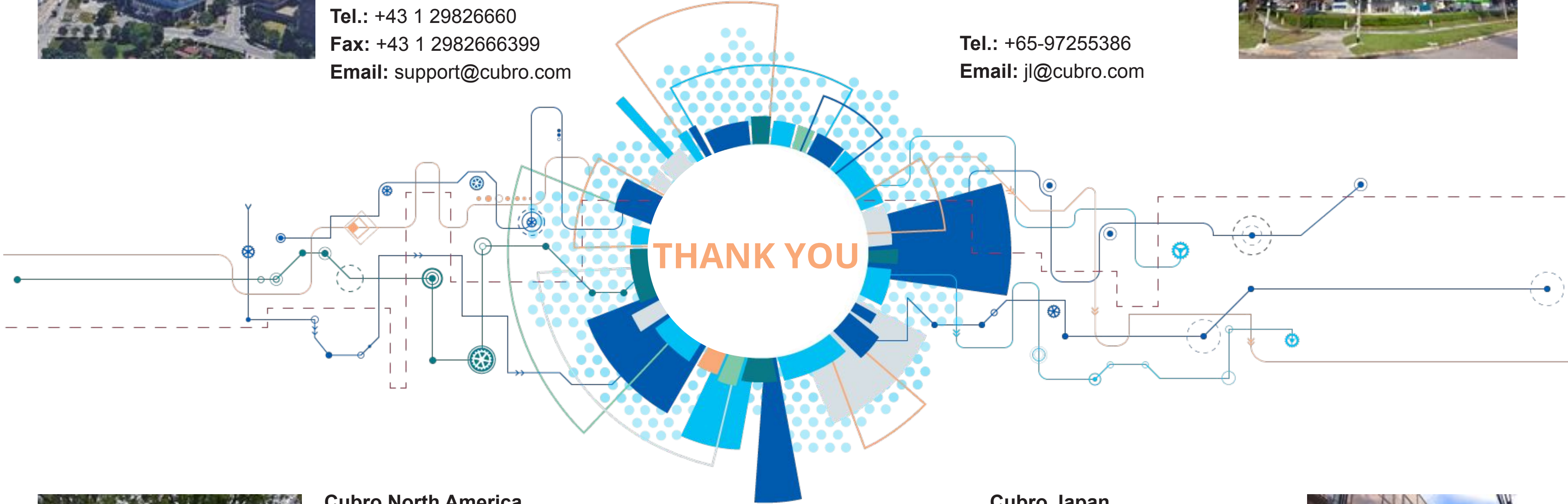
Learn more about the Cubro Packetmaster EX family at: https://www.cubro.com/en/products/network-packet-brokers/

Cubro Network Visibility
Ghegastraße 3
1030 Vienna, Austria

Tel.: +43 1 29826660
Fax: +43 1 2982666399
Email: support@cubro.com

Cubro Asia Pacific
8, Ubi Road 2 #04-12 Zervex
Singapore 408538

Tel.: +65-97255386
Email: jl@cubro.com



Cubro North America
Cubro Network Visibility Inc.
225 Peachtree Street NE,
Suite 1100, Atlanta, GA, 30303, USA

Email: americas@cubro.com

Cubro Japan
6-7-22, Shinjuku, Shinjuku,
Tokyo, 160-0022 Japan

Tel: +81(0)50-3708-5839
Email: japan@cubro.com