



How to use header modification in monitoring

APPLICATION NOTE

Jan 2021

Contents

1. What is header modification?
2. Header modification feature on Cubro EX Series
3. Use-case for header modification
4. Summary

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 1-54

<input type="checkbox"/> Push VLAN 1-4094, pushes a new VLAN ID.	<input type="checkbox"/> Modify VLAN ID 1-4094
<input type="checkbox"/> Strip VLAN	<input type="checkbox"/> Pop Layer 2 Remove Layer 2 from the packet
<input type="checkbox"/> Pop all MPLS Removes all MPLS Labels. In most cases you should also Push Layer 2	<input type="checkbox"/> Push Layer 2 Add Layer 2 to the packet, needs to Modify MAC Dest.
<input type="checkbox"/> Modify IP Source	<input type="checkbox"/> Modify MAC Source e.g. FE:ED:FE:ED:FE:ED or 0.0.1
<input type="checkbox"/> Modify MAC Dest.	<input type="checkbox"/> Modify IP Dest.
<input type="checkbox"/> Modify UDP Dest.	<input type="checkbox"/> Modify UDP Source
<input type="checkbox"/> Modify TCP Dest.	<input type="checkbox"/> 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.**

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

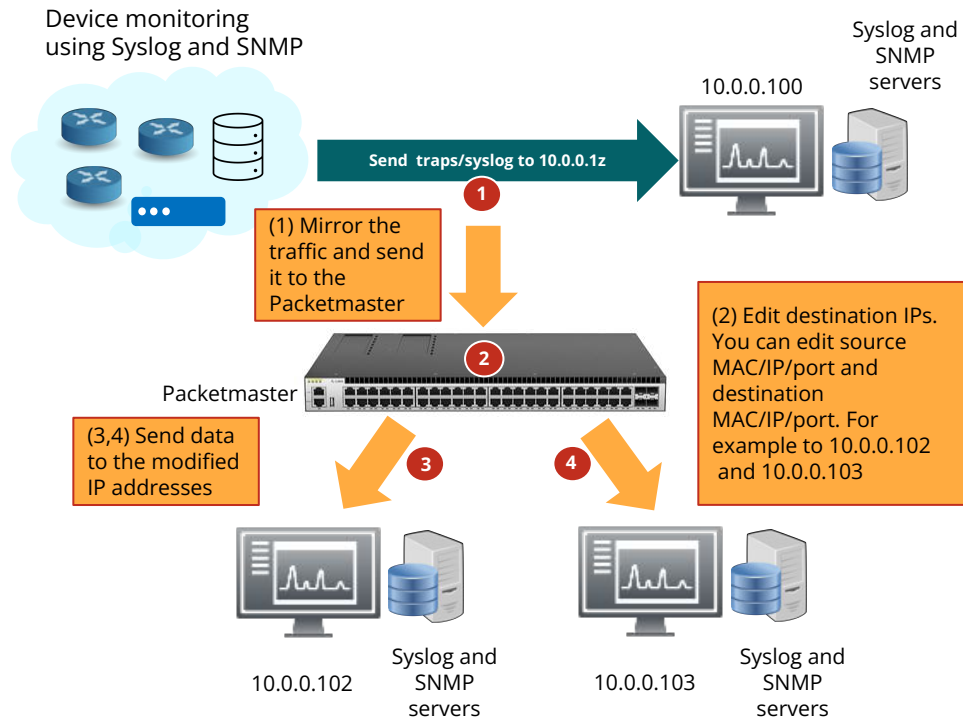
Instead of defining multiple addresses per device, use just one. Mirror the traffic from the devices, which you already are most likely doing, modify destination IP addresses and send the packets to the destination monitoring systems.

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

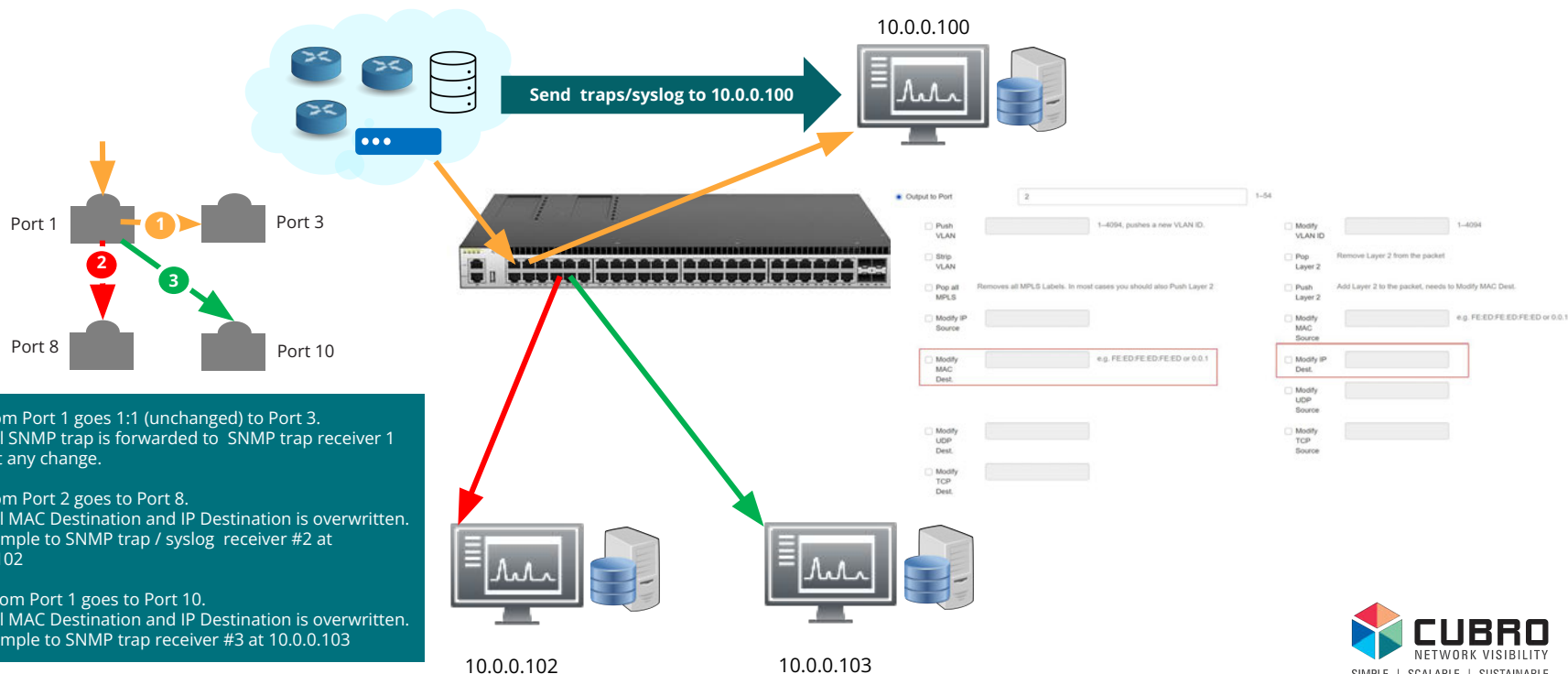
EX2 / EX5 / EX6 / EX12 / EX32 / EX484-3 / EX48400 / EX20400



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)



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/>

