



OMNIA

高级网络数据包代理

Oct. 2020

目录



1. Omnia概览

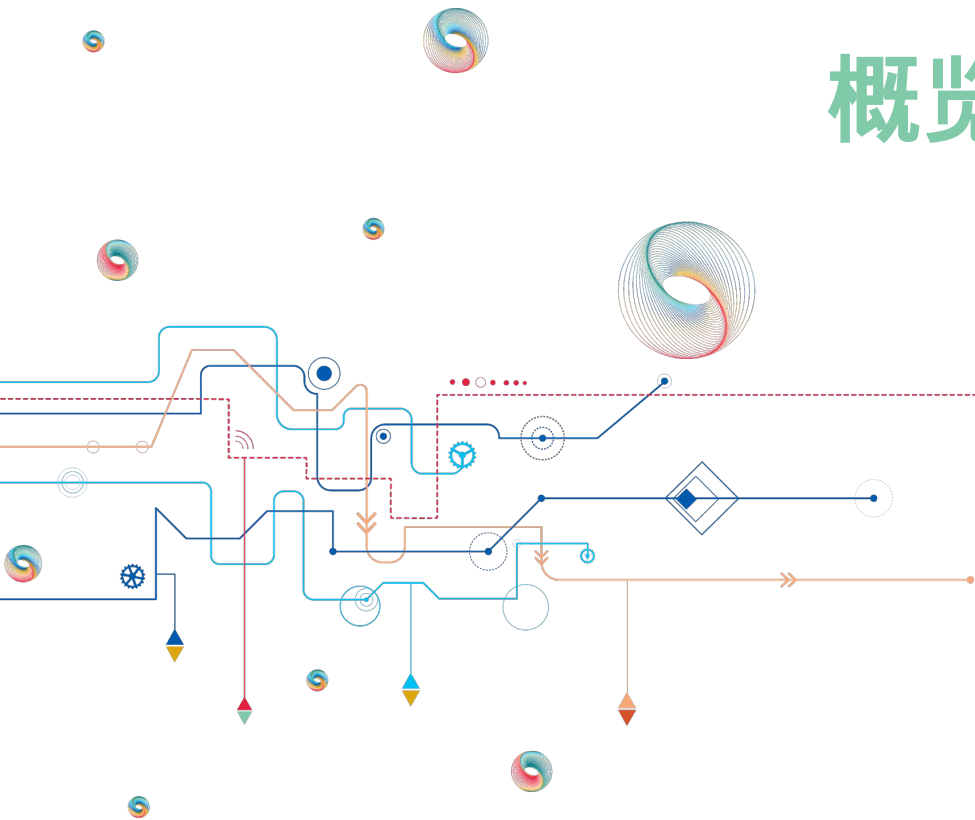
- a. Omnia 10
- b. Omnia 20
- c. Omnia 120
- d. PacketMaster功能
- e. SessionMaster功能

2. 网络数据包代理功能

- a. Web GUI
- b. 内联ACL过滤
- c. ACL Regex过滤
- d. 负载均衡
- e. GRE解封装
- f. ERSPAN解封装
- g. VLAN和VXLAN封装
- h. 时间戳
- i. 数据包切片
- j. 隧道报头移除
- k. MAC修改
- l. 偏移剥离
- m. 数据脱敏（数据屏蔽）
- n. GRE和VXLAN端点
- o. TCP重排序和数据包片段重组
- p. 内联或SPAN端口的重复数据删除
- q. 在光TAP之后被动执行重复数据删除
- r. V5和V9 NetFlow探针
- s. 元数据导出器：NetFlow / NetFlow - DPI / DPI
- t. SSL / TLS解密

概览

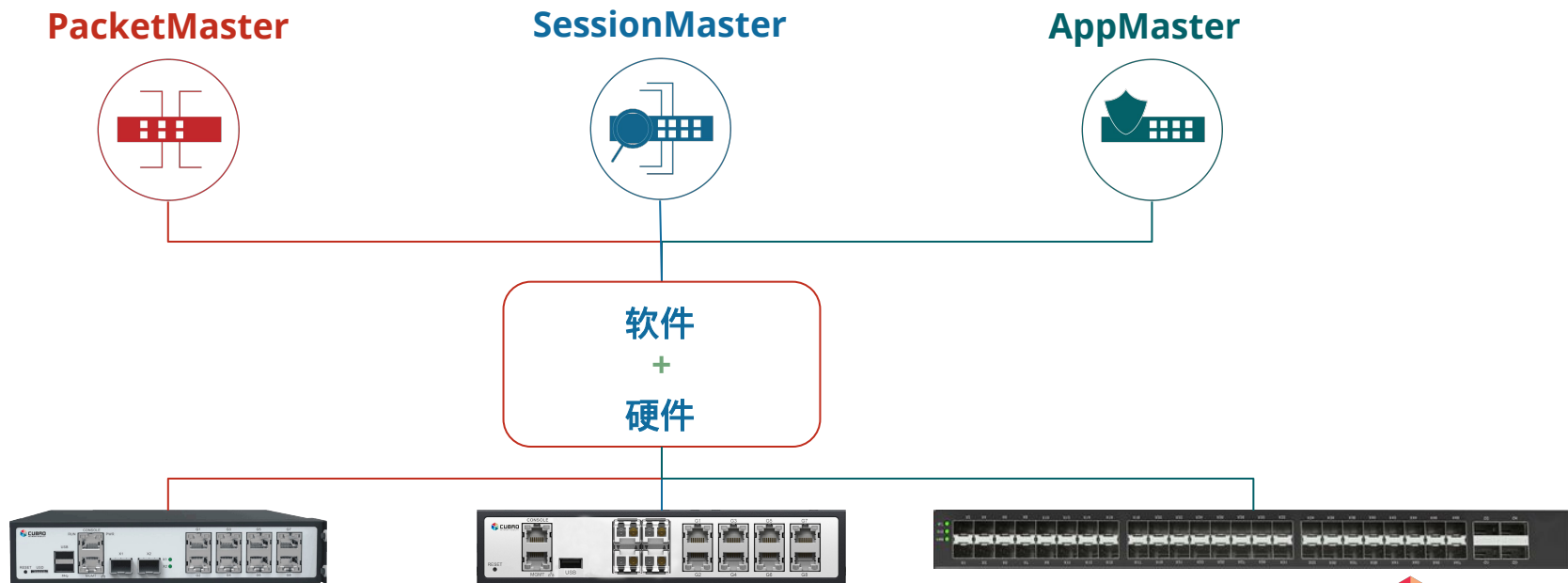
OMNIA



强大&多功能，适用于任何企业



Omnia 将 Cubro 在网络可视性和监控方面的经验与 EXA8 平台的设计相结合。其结果是一个由目的驱动的软件与经过多年经验和工程开发的功能堆栈相搭配的产品系列。这种方法为客户提供了更多的选择和更多的功能。



Omnia 10: 跨越多种部署的多功能性



CPU	四核 ARMv8
Switch	88E6190X Marvell
Memory	DDR4 ECC UDIMM 16GB
eMMC	16 GB
MGMT	10/100/1000 Base-T RJ45
Console	1 * RS232 (RJ45)
I/O	2 * USB3.0 (Type A) MicroSD Card slot
Bypass	支持4 组铜缆端口
Port	2 * 10GbE 8*GbE(RJ45)
Internal extended I/O	1* mini PCIe1 Gen 3 2* M.2(PCIex4 Gen3,2280) 1* M.2(Sata Gen3, 2242 & 2280 compatible) 1* SATA (Gen3, support 2,5 inch HDD or SSD)
Power Supply	AC 100 - 264 or DC 48V
Size (W x H X D) mm	335 x 220 x 44.4
Power consumption	30 W

Omnia 10, 原名EXA8, 是一款多功能网络设备, 非常适合中小企业、分支机构办公室和远程部署。它具有内置的无源分接能力、10G接口、板载存储以及多样化的软件选择, 是一款能够解决多种网络和安全挑战的设备。



Omnia 20: 针对要求苛刻的工作负载的性能



CPU	四核ARMv8
Switch	88E6190X Marvell
Memory	DDR4 ECC UDIMM 16 GB
eMMC	16 GB
MGMT	10/100/1000 Base-T RJ45
Console	1 * RS232 (RJ45)
USB	1 * USB3.0 (Type A)
Bypass	Support 4 group Copper Ports
Port	2 * 10GbE 2 * 1 GbE (SFP) 8*GbE(RJ45)
Internal extended I/O	1* mini PCIe1 Gen 3 2* M.2(PCIex4 Gen3,2280) 1* M.2(Sata Gen3, 2242 & 2280 compatible) 1* SATA (Gen3, support 2,5 inch HDD or SSD)
Power Supply	AC 100 - 264 or DC 48V
Size (W x H X D) mm	335 x 220 x 44.4
Power consumption	30 W

Omnia 20在Omnia 10的基础上增加了额外的1G SFP接口，并将处理能力提高了一倍。它保留了Omnia 10的多功能性，同时也是执行特别苛刻任务的首选。



Omnia 120: 大型企业的强大设备



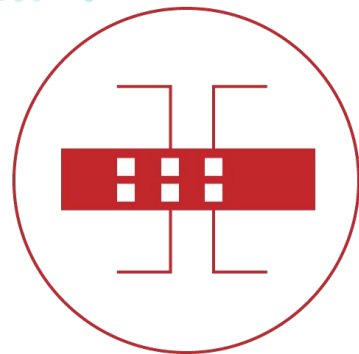
CPU	2 x Multi-Core ARM CPU
Switch	Cavium Xplicant
Memory	DDR4 ECC UDIMM
MGMT	10/100/1000 Base-T RJ45
Console	1 * RS232 (RJ45)
Port	48 * 1/10GbE SFP+ 4 * 40/100GbE QSFP28
Power Supply	AC 100 - 264 or DC 48V
Size (W x H x D) mm	440 x 660 x 44.4
Power consumption	400W



PacketMaster功能：L2-L4可见性



PacketMaster的功能堆栈包含了传统的网络数据包代理功能，如任意到多或多到任意的流量转发、过滤和拦截、报头修改和剥离、负载均衡、隧道终止等。

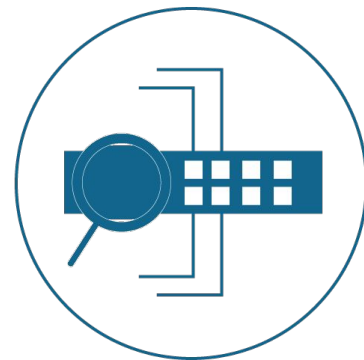


- 内联ACL过滤
 - 通过OSI L4标准过滤OSI L2的流量
 - 将特定流量转发到一个或多个接口
 - 丢弃指定流量
- 负载均衡
 - 从多种对称或非对称负载均衡算法中选择
- GRE终止
- ERSPAN终止
- VXLAN终止
- 时间戳
- 数据包切片
- 隧道报头移除
- VLAN添加/修改/剥离
- MAC修改
- 偏移剥离
 - 为特定的应用创建自定义的报头剥离偏移
- GRE和VXLAN活动隧道端点

SessionMaster功能：深度过滤&分析



The SessionMaster功能堆栈借鉴了Cubro先进的高级网络数据包代理。功能包括流量重复数据删除、正则表达式搜索、数据屏蔽（数据脱敏）、SSL/TLS解密等。在当今的网络中，在许多情况下，仅仅过滤L2-L4层的流量已经不够了。SessionMaster的功能为尖端部署提供了必要的深度可见性。



-
-
-
-
-
-
-
-
-
-
-

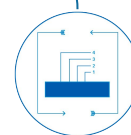
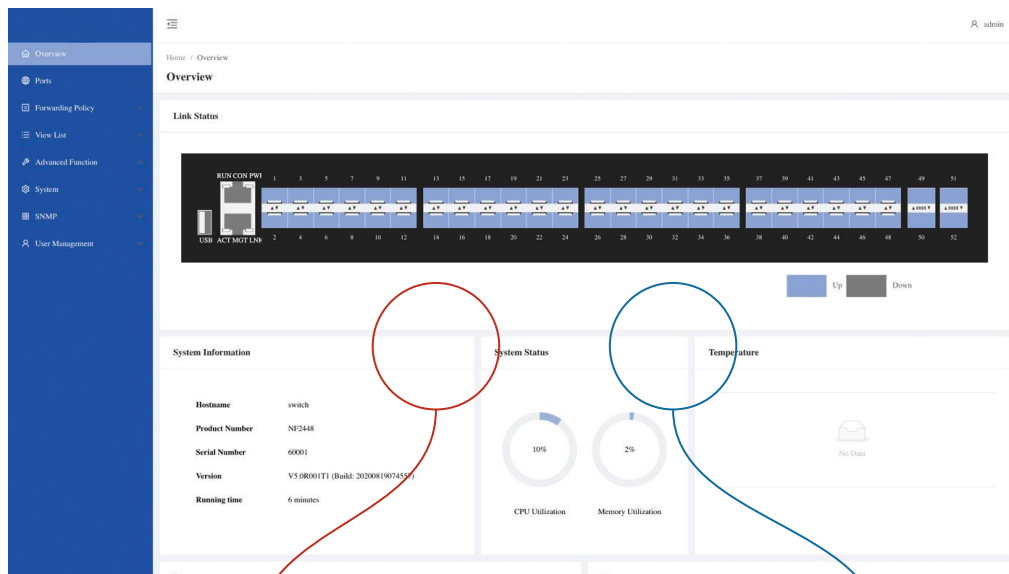
An abstract network diagram featuring a complex web of blue, orange, and red lines. The lines connect various nodes, including gears, circles, and diamond shapes. A prominent red dashed line extends from the center towards the right, ending at a red octagonal node. Several colorful, multi-layered circular icons are scattered throughout the scene. The overall aesthetic is clean and modern, representing network connectivity and data flow.

网络数据包代理功能

集成的Web UI



PacketMaster和SessionMaster功能集成到单个直观的GUI中，以简化可用性和简化配置。



Omnia网络数据包代理WebGUI



Omnia系列提供了一个简单易用的Web UI来实现快速配置。此外，还可以看到内存和CPU利用率等系统资源。

通过左侧菜单上的选项卡，用户可以在UI中导航。

The screenshot displays the Omnia Web GUI interface. On the left is a blue navigation menu with the following items: Home, Forwarding Policy, Interface Statistics, Advanced Setting, System Configuration, System Upgrade, User Management, and Log Management. The main content area is divided into several sections:

- Status:** Features a network topology diagram with nodes labeled 'Host', 'vSO', 'S1', 'S2', 'S3', 'S4', 'S5', 'S6', 'S7', 'S8', 'S9', 'S10', 'S11', 'S12', 'S13', 'S14', 'S15', 'S16', 'S17', 'S18', 'S19', 'S20'. Below the diagram are two checkboxes: 'Link_Status: Up' (checked) and 'Link_Status: Down' (unchecked).
- Alarm information:** Shows 'No Data' with a warning icon.
- System Resource:** Contains two circular progress indicators: 'Memory Utilization' at 93.9% and 'CPU Utilization' at 24.2%.
- System Information:** Lists the following details:

Host Name:	EXA8_SM
System Ver:	20191227-78dea1a17f6
Mgmt IP:	192.168.1.210
Mgmt MAC:	d8:20:9f:00:07:13
License:	

ACL Filtering Inline



该设备支持IP+MASK和5元组内/外过滤。如果要使用内五元组，需要开启内五元组过滤。

ACL配置有7种过滤器类型：

1. Tuple
2. Tuple V6
3. Ipset
4. Ipset V6
5. L2
6. Packet Type
7. Regex

设备支持多组ACL。

每个ACL组是相互独立的。

Add Filter ✕

Filter Type:

Action: Permit

Src IP:

Src Port: -

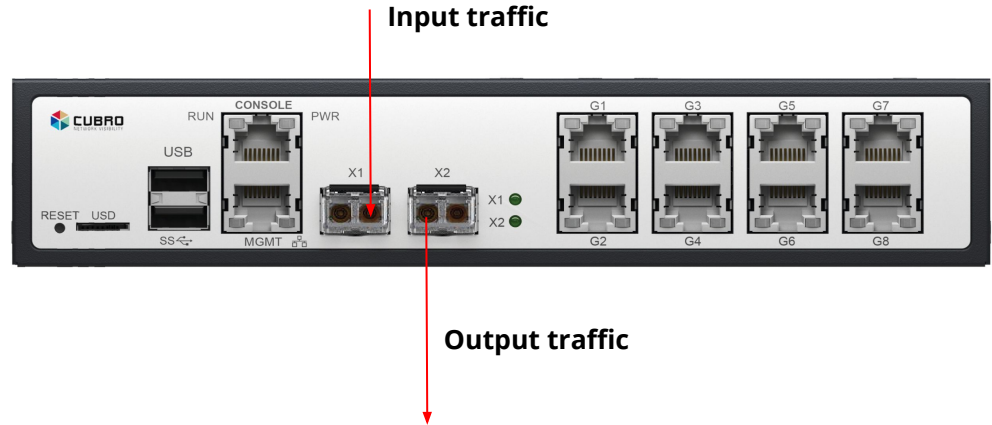
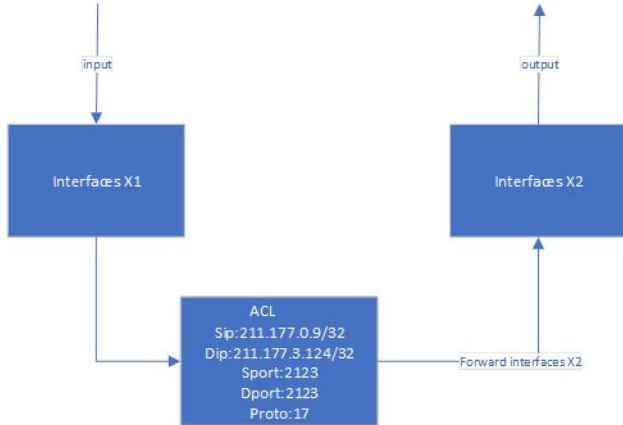
Dst IP:

Dst Port: -

Protocol: -

VLAN: -

ACL Filtering Inline



ACL Regex Filtering



在选择 “Regex Filter Type” 时，有不同的搜索类型：

- **Full Packet** - 扫描完整的数据包寻找关键字。一旦找到，就会过滤掉数据包。

。

- **Fixed Window** - 它只扫描数据包前256个字节。当发现关键字时，数据包将被过滤掉。

- **Float Window** - 设置特定搜索区域搜索关键字。一旦在范围内找到，就会过滤掉数据包。

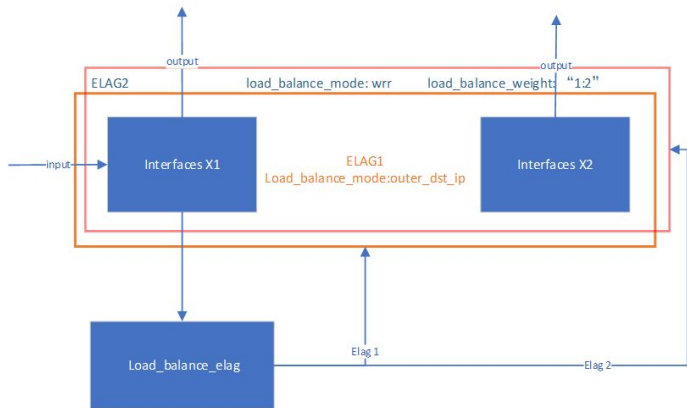
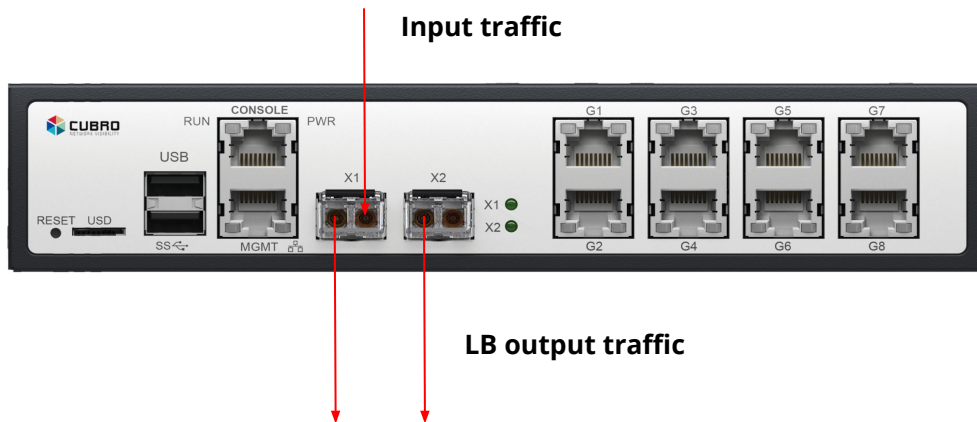
The screenshot shows a dialog box titled "Add Filter" with a close button (X) in the top right corner. The "Filter Type" dropdown menu is set to "Regex". Below it, the "Action" is set to "Permit" with a radio button. The "* Search Type" dropdown menu is open, showing three options: "full_packet", "fixed_window", and "float_window". At the bottom right of the dialog, there are two buttons: "Add" and "Ok".

负载均衡

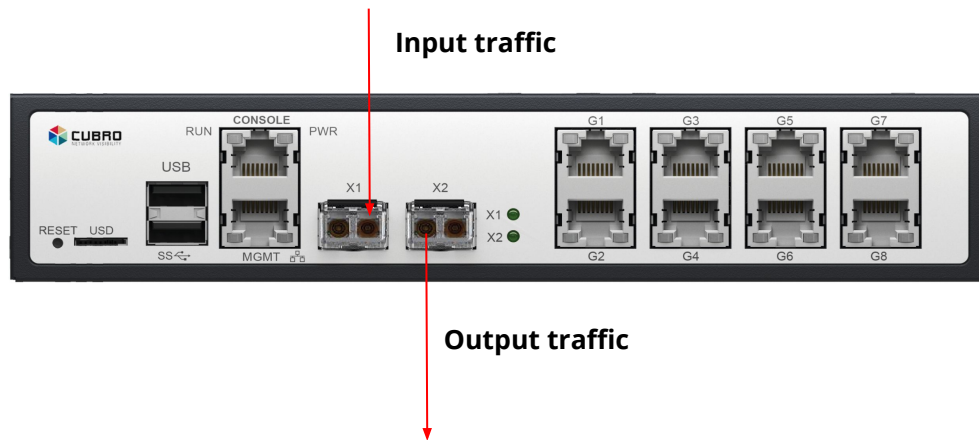
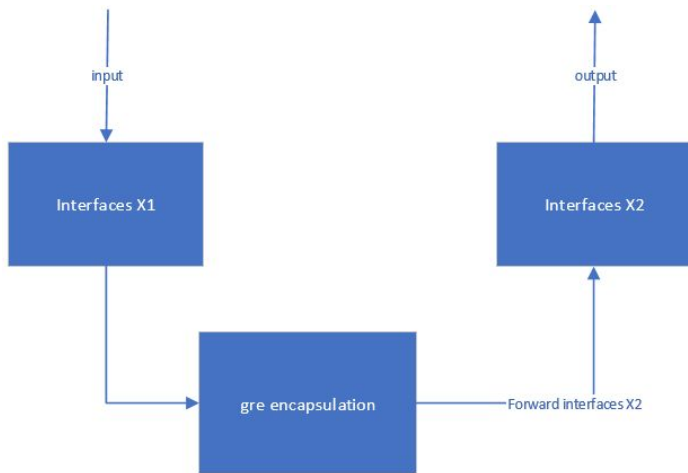


负载均衡可以基于多种哈希方法在多个端口上进行，包括：5元组、源IP地址和目的IP地址和轮询。以及隧道内层负载均衡模式。

基于5元组哈希的负载均衡可以保证两台设备之间的同步，保证数据的完整性。



通过这个功能，我们可以将流量封装在GRE隧道中。



GRE封装示例



Encapsulation

Encapsulation Type: GRE

Gre Enable: On

* DMAC: 00:00:00:00:00:01

* DIP: 10.10.10.1

* DSCP: 0

```
> Frame 2: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits) on interface \Device
> Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
> User Datagram Protocol, Src Port: 57977, Dst Port: 5004
> Data (1328 bytes)
```

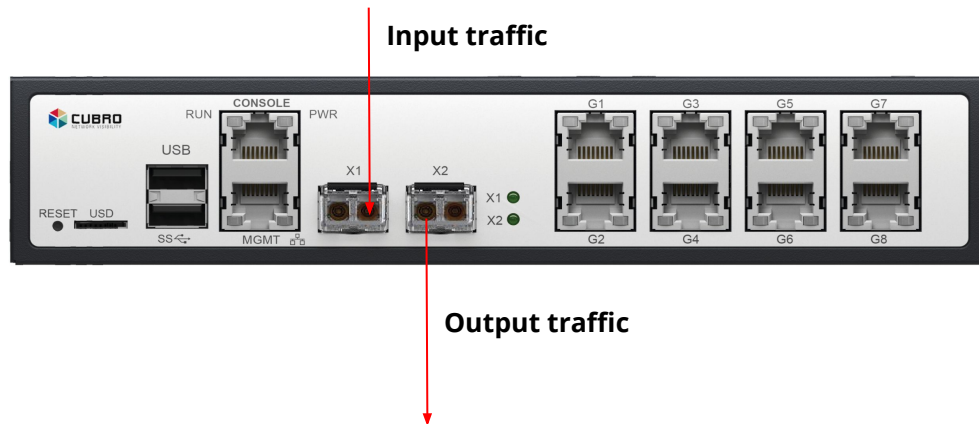
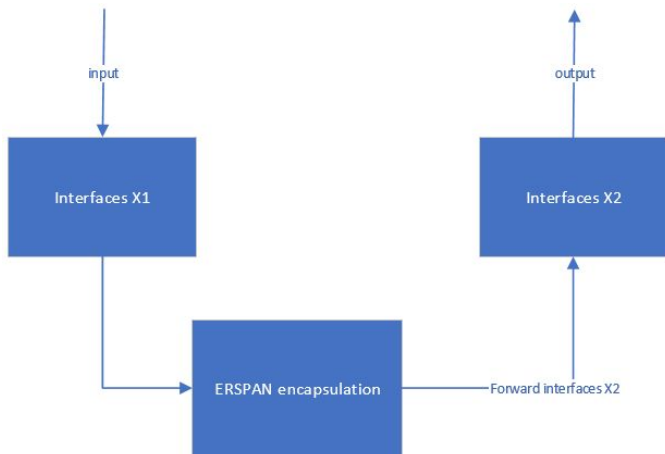


```
> Frame 1: 1408 bytes on wire (11264 bits), 1408 bytes captured (11264 bits) on interface \Device\NPF
> Ethernet II, Src: CubroAcr_00:07:15 (d8:20:9f:00:07:15), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
> Internet Protocol Version 4, Src: 192.168.255.254, Dst: 10.10.10.1
> Generic Routing Encapsulation (Transparent Ethernet bridging)
> Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
> User Datagram Protocol, Src Port: 57977, Dst Port: 5004
> Data (1328 bytes)
```

ERSPAN封装



通过这个功能，我们可以将流量封装在 ERSPAN v1、v2或v3报头中。



ERSPAN v2封装示例



Encapsulation

Encapsulation Type:

Erspan Enable:

* DMAC:

* DIP:

* SessionID:

* Type:

* DSCP:

```
> Frame 2: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits) on interface \Device
> Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
> User Datagram Protocol, Src Port: 57977, Dst Port: 5004
> Data (1328 bytes)
```

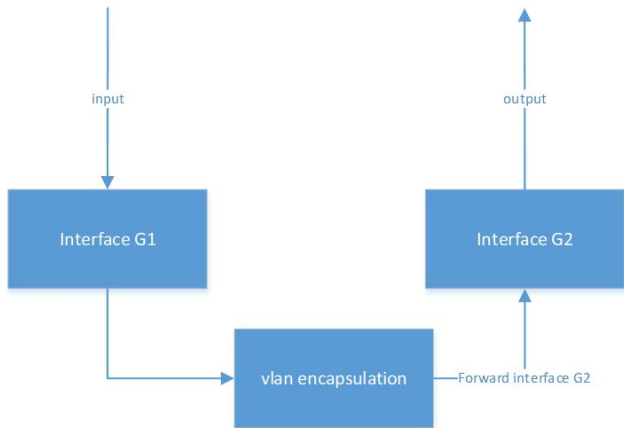


```
> Frame 1: 1420 bytes on wire (11360 bits), 1420 bytes captured (11360 bits) on interface \Device\NPF
> Ethernet II, Src: CubroAcr_00:07:15 (d8:20:9f:00:07:15), Dst: 00:00:00_00:00:02 (00:00:00:00:00:02)
> Internet Protocol Version 4, Src: 192.168.255.254, Dst: 10.10.10.2
< Generic Routing Encapsulation (ERSPAN)
  > Flags and Version: 0x1000
    Protocol Type: ERSpan (0x88be)
    Sequence Number: 1
< Encapsulated Remote Switch Packet Analysis Type II
  0001 .... .. = Version: Type II (1)
  .... 0000 0000 0000 = Vlan: 0
  000. .... .. = COS: 0
  ...1 1... .. = Encap: VLAN tag preserved in frame (3)
  .... .0.. .. = Truncated: Not truncated (0)
  .... .00 0110 0100 = SpanID: 100
  0000 0000 0000 .... .. = Reserved: 0
  .... .... 0000 0000 0000 0000 = Index: 0
> Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
> User Datagram Protocol, Src Port: 57977, Dst Port: 5004
> Data (1328 bytes)
```

VLAN封装



通过这个功能，我们可以在输出的数据包中添加一个VLAN标签。



Input traffic

Output traffic

VLAN 封装示例



Add VLAN

Add VLAN:

* Vlan ID:

No.	Time	Source	Destination	Protocol	Length	Type	Info
10	0.000000	192.168.0.36	192.168.1.235	TCP	66	IPv4	55002 → 22 [ACK...
20	0.000000	192.168.0.36	192.168.1.235	TCP	66	IPv4	[TCP Dup ACK 18...
30	0.000000	192.168.0.36	192.168.1.235	TCP	66	IPv4	[TCP Dup ACK 16...

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Tp-LinkT_37:89:df (0c:4b:54:37:89:df), Dst: IntelCor_08:89:38 (00:1e:67:08:89:38)
Internet Protocol Version 4, Src: 192.168.0.36, Dst: 192.168.1.235
Transmission Control Protocol, Src Port: 55002, Dst Port: 22, Seq: 1, Ack: 1, Len: 0



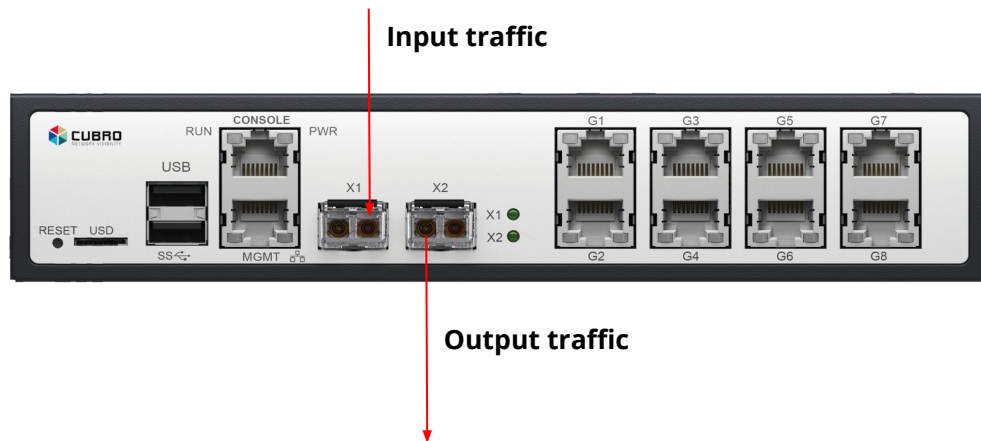
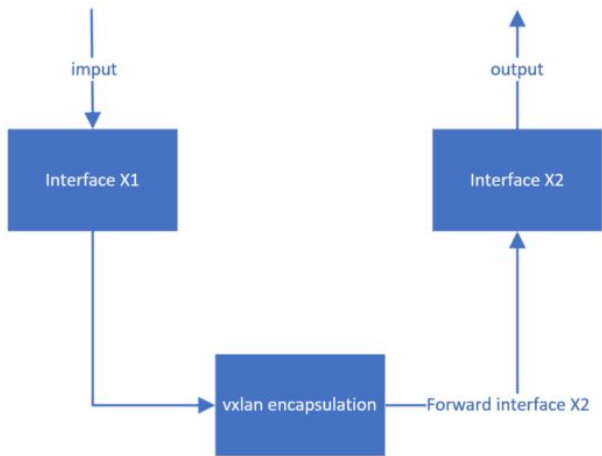
No.	Time	Source	Destination	Protocol	Length	Type	Info
10	0.000000	192.168.0.36	192.168.1.235	TCP	70	802...	55002 → 22 [ACK...
20	0.000003	192.168.0.36	192.168.1.235	TCP	70	802...	[TCP Dup ACK 18...
30	0.000009	192.168.0.36	192.168.1.235	TCP	70	802...	[TCP Dup ACK 16...

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: Tp-LinkT_37:89:df (0c:4b:54:37:89:df), Dst: IntelCor_08:89:38 (00:1e:67:08:89:38)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 513
Internet Protocol Version 4, Src: 192.168.0.36, Dst: 192.168.1.235
Transmission Control Protocol, Src Port: 55002, Dst Port: 22, Seq: 1, Ack: 1, Len: 0

VXLAN封装



通过这个功能，我们可以将流量封装在一个VxLAN报头中。



VXLAN封装示例



Encapsulation

Encapsulation Type:

Vxlan Enable:

* DMAC:

* DIP:

* DPort:

* VNI:

* DSCP:

```
> Frame 2: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits) on interface \Device
> Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
> User Datagram Protocol, Src Port: 57977, Dst Port: 5004
> Data (1328 bytes)
```

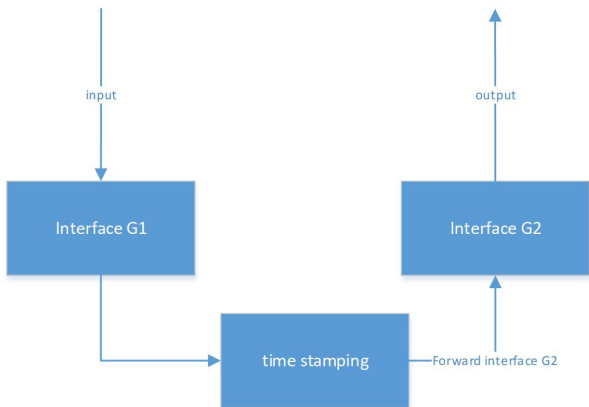


```
> Frame 1: 1420 bytes on wire (11360 bits), 1420 bytes captured (11360 bits) on interface \Device\NPF
> Ethernet II, Src: CubroAcr_00:07:15 (d8:20:9f:00:07:15), Dst: 00:00:00_00:00:04 (00:00:00:00:00:04)
> Internet Protocol Version 4, Src: 192.168.255.254, Dst: 10.10.10.4
> User Datagram Protocol, Src Port: 4789, Dst Port: 777
✓ Virtual eXtensible Local Area Network
  > Flags: 0x0800, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 250
    Reserved: 0
  > Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
  > Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
  > User Datagram Protocol, Src Port: 57977, Dst Port: 5004
  > Data (1328 bytes)
```

时间戳



启用该功能后，输出数据包的时间戳分辨率在20-200ns之间。



时间戳示例



Tagging

Time-Stamping:

No.	Time	Source	Destination	Protocol	Length	Type	Data
	10.000000	10.27.229.244	10.0.0.172	GTP...	6...	802...	GET http://i.if...

Frame 1: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits)
Ethernet II, Src: Ericsson_14:58:e9 (00:30:88:14:58:e9), Dst: JuniperN_e0:d3:fc (00:24:dc:e0:d3:fc)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 60
Internet Protocol Version 4, Src: 221.177.79.2, Dst: 221.177.83.35
User Datagram Protocol, Src Port: 2152, Dst Port: 2152
GPRS Tunneling Protocol
Internet Protocol Version 4, Src: 10.27.229.244, Dst: 10.0.0.172
Transmission Control Protocol, Src Port: 34282, Dst Port: 80, Seq: 1, Ack: 1, Len: 520
Hypertext Transfer Protocol



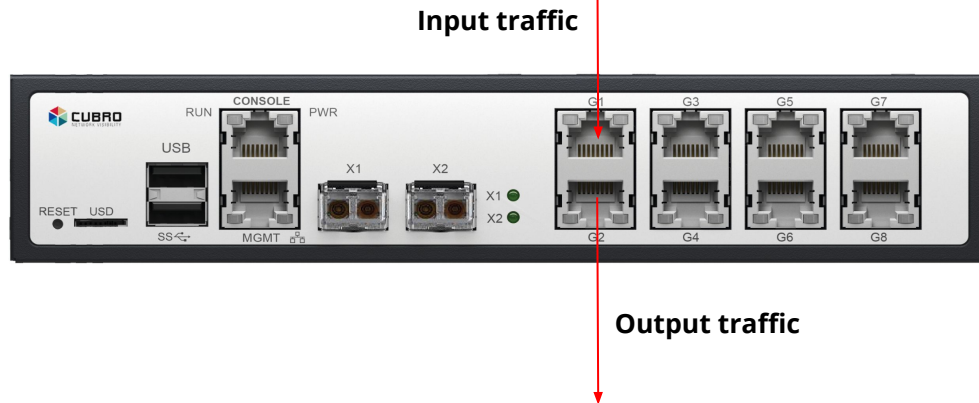
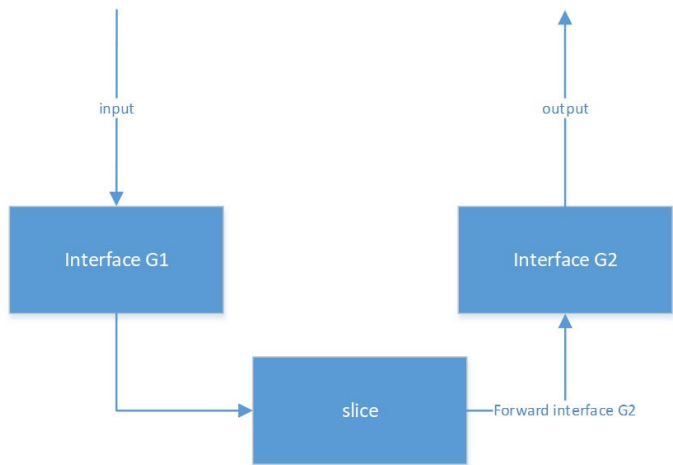
No.	Time	Source	Destination	Protocol	Length	Type	Data
	10.000000	10.27.229.244	10.0.0.172	GTP...	6...	802...	GET http://i.if...

Frame 1: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits)
Ethernet II, Src: Ericsson_14:58:e9 (00:30:88:14:58:e9), Dst: JuniperN_e0:d3:fc (00:24:dc:e0:d3:fc)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 60
Internet Protocol Version 4, Src: 221.177.79.2, Dst: 221.177.83.35
User Datagram Protocol, Src Port: 2152, Dst Port: 2152
GPRS Tunneling Protocol
Internet Protocol Version 4, Src: 10.27.229.244, Dst: 10.0.0.172
Transmission Control Protocol, Src Port: 34282, Dst Port: 80, Seq: 1, Ack: 1, Len: 520
Hypertext Transfer Protocol
VSS-Monitoring ethernet trailer, Timestamp: 15:10:58.116865081

数据包切片



通过这个功能，我们可以对数据包帧的有效载荷进行切片，切片范围在40到1550字节之间。CRC可以重新计算。



数据包切片示例



Slicing

Slicing:

* Slice Bytes:

CRC:

```
> Frame 2: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits) on interface \Device
> Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
> User Datagram Protocol, Src Port: 57977, Dst Port: 5004
> Data (1328 bytes)
```



```
> Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF_
> Ethernet II, Src: Microsof_c5:2a:12 (f0:6e:0b:c5:2a:12), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 239.0.0.1
> User Datagram Protocol, Src Port: 57977, Dst Port: 5004
> Data (58 bytes)
```

隧道报头移除



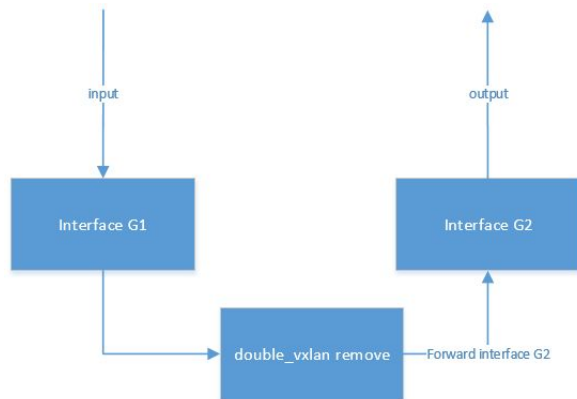
通过这个功能，我们可以删除下面列出的隧道报头：

- 剥离VLAN隧道
- 剥离MPLS隧道
- 剥离VXLAN隧道(剥离两层VXLAN)
- 剥离GRE隧道



Input traffic

Output traffic



Remove Tunnel Header

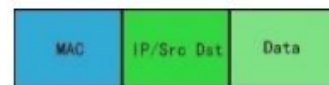
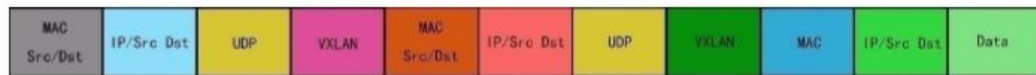
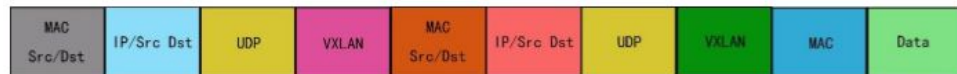
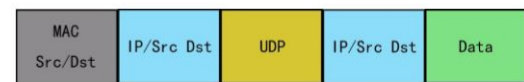
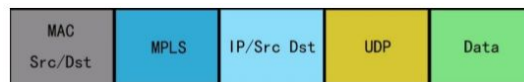
Remove Header: On

Header:	Protocol	Layers
<input type="checkbox"/>	VLAN	1-15
<input type="checkbox"/>	MPLS	1-15
<input type="checkbox"/>	VXLAN	1,2
<input type="checkbox"/>	GRE	

隧道报头移除



报头删除并不局限于单个报头，可以同时删除多个报头。



隧道报头移除示例



VXLAN报头

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	65:64:6f:72:61:20	Cisco_00:1a:66	0x5b66	293	Ethernet II

```
> Frame 1: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
> Ethernet II, Src: Netgear_c0:3f:0e:44:86:3b, Dst: IPv4mcast_01:01:01 (01:00:5e:01:01:01)
> Internet Protocol Version 4, Src: 192.168.1.79, Dst: 239.1.1.1
> User Datagram Protocol, Src Port: 53678, Dst Port: 8472
> Virtual eXtensible Local Area Network
> Ethernet II, Src: fe:1b:3b:4b:60:f2 (fe:1b:3b:4b:60:f2), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Virtual eXtensible Local Area Network
> Ethernet II, Src: 65:64:6f:72:61:20 (65:64:6f:72:61:20), Dst: Cisco_00:1a:66 (00:05:00:00:1a:66)
> Data (179 bytes)
```

1st VXLAN报头移除

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	65:64:6f:72:61:20	Cisco_00:1a:66	0x5b66	243	Ethernet II

```
> Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
> Ethernet II, Src: fe:1b:3b:4b:60:f2 (fe:1b:3b:4b:60:f2), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Virtual eXtensible Local Area Network
> Ethernet II, Src: 65:64:6f:72:61:20 (65:64:6f:72:61:20), Dst: Cisco_00:1a:66 (00:05:00:00:1a:66)
> Data (179 bytes)
```

多个MPLS层

No.	Time	Source	Destination	Protocol	Length	Type	Info
1	0.000000	110.16.222.192	10.64.13.154	GTP...	1...	MPLS...	Fragmented IP p...
2	28.000000	110.16.222.192	10.64.13.154	GTP...	1...	MPLS...	13445 + 12711 L...

```
> Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
> Ethernet II, Src: JuniperN_cd:01:fe (3c:94:d5:cd:01:fe), Dst: HuaweiTe_fa:f1:35 (e4:68:a3:fa:f1:35)
> MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 0, TTL: 254
> MultiProtocol Label Switching Header, Label: 22, Exp: 0, S: 0, TTL: 255
> MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 0, TTL: 254
> MultiProtocol Label Switching Header, Label: 22, Exp: 0, S: 0, TTL: 255
> MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 0, TTL: 254
> MultiProtocol Label Switching Header, Label: 22, Exp: 0, S: 1, TTL: 255
> Internet Protocol Version 4, Src: 100.65.248.1, Dst: 100.64.25.113
> User Datagram Protocol, Src Port: 2152, Dst Port: 2152
> GPRS Tunneling Protocol
> Internet Protocol Version 4, Src: 110.16.222.192, Dst: 10.64.13.154
> Data (1400 bytes)
```

MPLS层移除

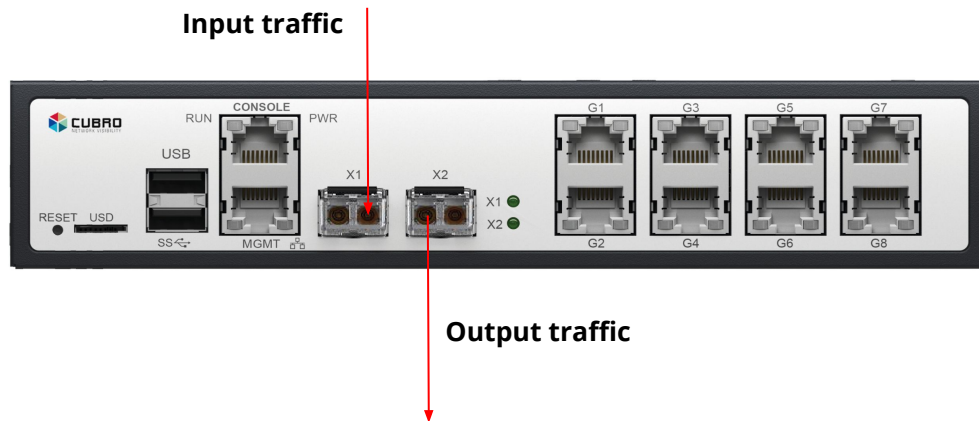
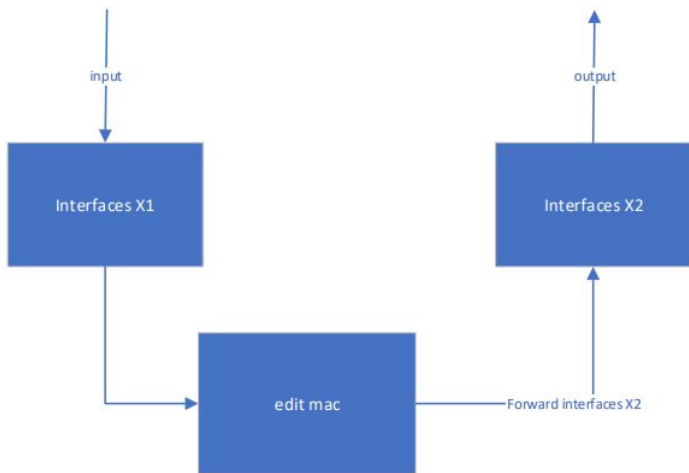
No.	Time	Source	Destination	Protocol	Length	Type	Info
1	0.000000	110.16.222.192	10.64.13.154	GTP...	1...	IPv4	Fragmented IP p...
2	28.000000	110.16.222.192	10.64.13.154	GTP...	1...	IPv4	13445 + 12711 L...

```
> Frame 1: 1470 bytes on wire (11760 bits), 1470 bytes captured (11760 bits) on interface 0
> Ethernet II, Src: JuniperN_cd:01:fe (3c:94:d5:cd:01:fe), Dst: HuaweiTe_fa:f1:35 (e4:68:a3:fa:f1:35)
> Internet Protocol Version 4, Src: 100.65.248.1, Dst: 100.64.25.113
> User Datagram Protocol, Src Port: 2152, Dst Port: 2152
> GPRS Tunneling Protocol
> Internet Protocol Version 4, Src: 110.16.222.192, Dst: 10.64.13.154
> Data (1400 bytes)
```

MAC修改



通过这个功能，我们可以修改数据包帧的源和目的MAC地址。



MAC修改示例



Modify MAC

Modify MAC:

SMAC:

DMAC:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	1.1.1.1	2.2.2.200	UDP	354	100 → 210 Len=254

<

- > Frame 1: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface \Device\NPF_{66A...}
- > Ethernet II, Src: CubroAcr_0b:86 (70:b3:d5:01:ab:86), Dst: 00:00:00_00:00:02 (00:00:00:00:00:02)
- > Internet Protocol Version 4, Src: 10.10.10.1, Dst: 20.20.20.2
- > User Datagram Protocol, Src Port: 49152, Dst Port: 4789
- > Virtual eXtensible Local Area Network
- > Ethernet II, Src: Veritech_01:6e:8c (00:18:63:01:6e:8c), Dst: cc:bb:aa:dd:ff:aa (cc:bb:aa:dd:ff:aa)
- > IEEE 802.1ad, ID: 200
- > 802.1Q Virtual LAN, PRI: 3, DEI: 0, ID: 100
- > Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.200
- > User Datagram Protocol, Src Port: 100, Dst Port: 210
- > Data (254 bytes)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	1.1.1.1	2.2.2.200	UDP	354	100 → 210 Len=254

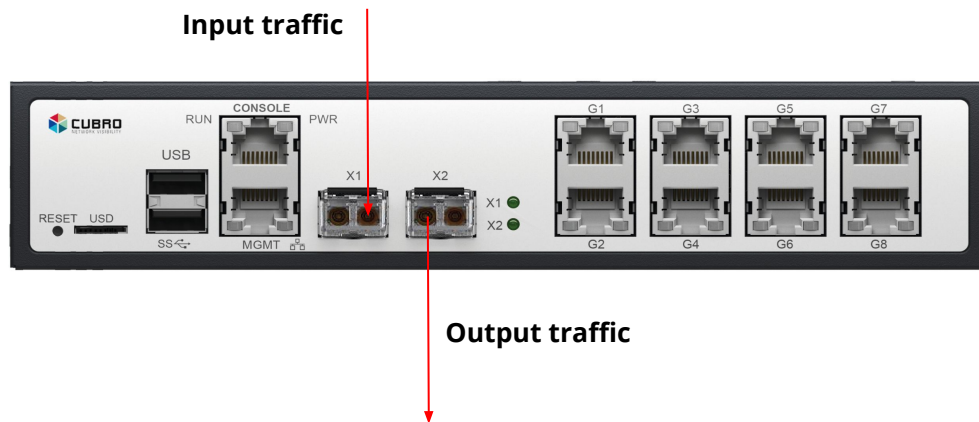
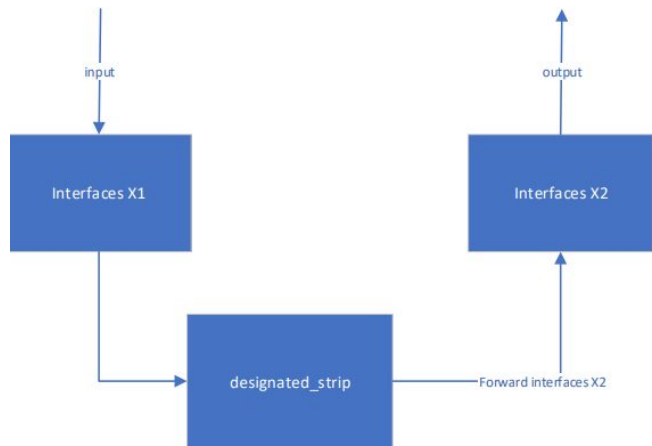
<

- > Frame 1: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface \Device\NPF_{66A...}
- > Ethernet II, Src: 00:00:00_00:00:01 (00:00:00:00:00:01), Dst: 00:00:00_00:00:02 (00:00:00:00:00:02)
- > Internet Protocol Version 4, Src: 10.10.10.1, Dst: 20.20.20.2
- > User Datagram Protocol, Src Port: 49152, Dst Port: 4789
- > Virtual eXtensible Local Area Network
- > Ethernet II, Src: Veritech_01:6e:8c (00:18:63:01:6e:8c), Dst: cc:bb:aa:dd:ff:aa (cc:bb:aa:dd:ff:aa)
- > IEEE 802.1ad, ID: 200
- > 802.1Q Virtual LAN, PRI: 3, DEI: 0, ID: 100
- > Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.200
- > User Datagram Protocol, Src Port: 100, Dst Port: 210
- > Data (254 bytes)

偏移移除



通过这个功能，我们可以删除数据包帧中的一些范围的字节。



偏移移除示例



本示例展示了在4G会话中通过“ offset Stripping (偏移移除)”进行GTP报头剥离。从补货中可以看楚，GTP报头(外网IP地址+外网L4协议+GTP)的长度为40字节，数据包帧中的offset起始值为14“45”。通过设置这些值，我们可以看到，在第二次捕获中，GTP报头被删除了。

```
5 1.197520_ 192.168.1.161 8.8.8.8 GTP <DNS> Standard query 0x643e A eventlog.beacon.qq.com
<
> Frame 5: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)
> Ethernet II, Src: CombaTel_31:3b:8b (00:27:1d:31:3b:8b), Dst: 00:00:00:00:00:01 (00:00:00:00:00:01)
> Internet Protocol Version 4, Src: 192.168.10.40, Dst: 192.168.10.28
> User Datagram Protocol, Src Port: 2152, Dst Port: 2152
> GPRS Tunneling Protocol
> Internet Protocol Version 4, Src: 192.168.1.161, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 43436, Dst Port: 53
> Domain Name System (query)

0000 00 00 00 00 01 00 27 1d 31 3b 8b 08 00 45 02 .....:1;...E-
0010 00 6d 00 01 00 00 80 11 a4 e8 c0 a8 0a 28 c0 a8 ...m.....(
0020 0a 1c 08 68 08 68 00 59 73 8b 32 ff 00 49 00 1e ...h-h-Y s-2-I-
0030 84 80 00 01 00 04 45 00 00 45 39 9e 40 00 40 11 .....E-E9@_@-
0040 2e b1 c0 a8 01 a1 08 08 08 a9 ac 00 35 00 31 .....-5-1 B-d-
0050 42 81 64 3e 01 00 00 01 00 00 00 00 00 09 61 .....a eventlog
0060 65 76 65 6e 74 6c 6f 67 06 62 65 61 63 6f 6e 02 .....-beacon-
0070 71 71 03 63 6f 6d 00 00 01 00 01 .....qq com-....
```



```
5 0.000647 192.168.1.161 8.8.8.8 DNS 83 Standard query 0x643e A eventlog.beacon.qq.com
<
> Frame 5: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{66A4CD0E-AC1E-4567-8160-676618B}
> Ethernet II, Src: CombaTel_31:3b:8b (00:27:1d:31:3b:8b), Dst: 00:00:00:00:00:01 (00:00:00:00:00:01)
> Internet Protocol Version 4, Src: 192.168.1.161, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 43436, Dst Port: 53
> Domain Name System (query)

0000 00 00 00 00 01 00 27 1d 31 3b 8b 08 00 45 00 .....:1;...E-
0010 00 45 39 9e 40 00 40 11 ff ff c0 a8 01 a1 08 08 ...E9@_@-.....
0020 08 08 a9 ac 00 35 00 31 42 81 64 3e 01 00 00 01 .....-5-1 B-d-
0030 00 00 00 00 00 09 61 65 76 65 6e 74 6c 6f 67 .....-a eventlog
0040 06 62 65 61 63 6f 6e 02 71 71 03 63 6f 6d 00 00 .....-beacon-qq com-
0050 01 00 01 .....
```

Stripping by Offset

Strip:

* Offset Type:

* Offset Length:

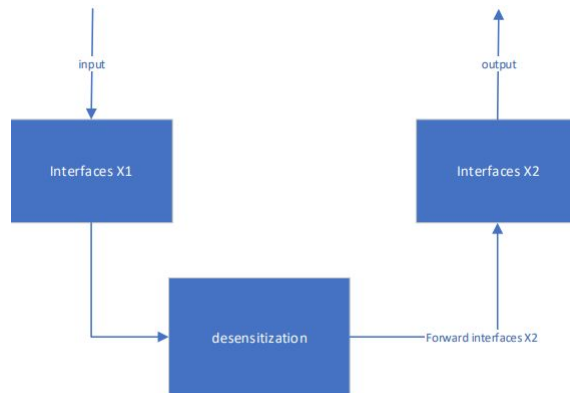
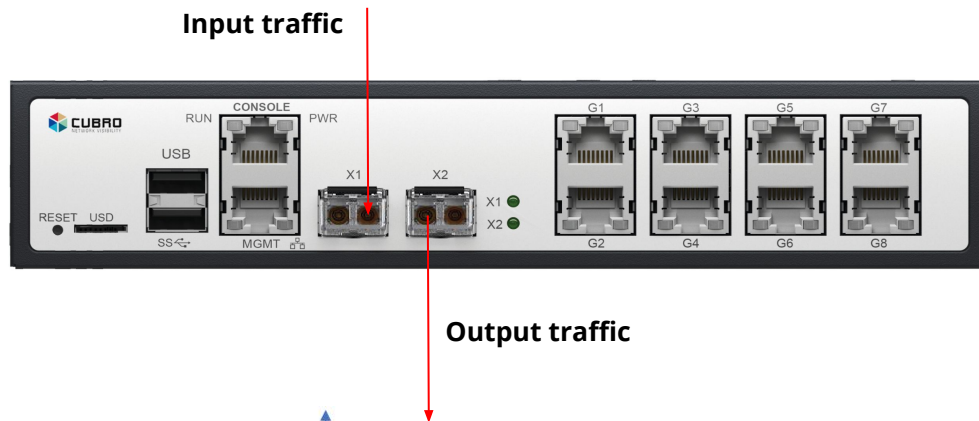
* Strip Length:

Update Headers:

通过这个功能，我们可以修改内容来隐藏原始数据。数据屏蔽有2个选项：

1- **Keyword:** 在指定的范围内，通过设置的十六进制值来搜索和修改关键字。

2- **Customized:** 选择一个随意的字节范围进行修改。



2- Customized

示例：如下图所示，我们定义的 "L4_Hdr_Start" 参数之后的8个字节，已经被十六进制值 "01" 修改了。

Desensitization

Desensitization:

* Select Mode:

* Offset Type:

* Offset Length:

* Process Length:

* Mode:

* Value:

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 00:00:00_00:00:01 (00:00:00:00:00:01), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
> Internet Protocol Version 4, Src: 0.0.18.7, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 1, Dst Port: 1
> Data (8 bytes)
```

0000	00 00 00 00 00 01 00 00	00 00 00 01 08 00 45 00E-
0010	00 24 de ad 00 00 80 11	89 6b 00 00 12 07 c0 a8	-\$.....-k.....
0020	00 01 00 01 00 01 00 10	f1 e0 de ad be ef de ad-.....
0030	be ef 00 00 00 00 00 00	00 00 00 00



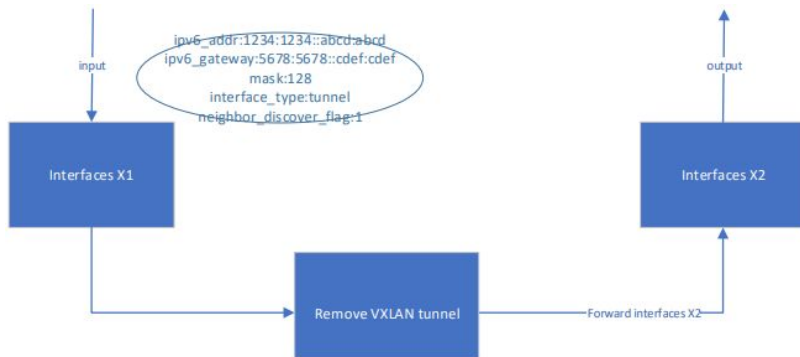
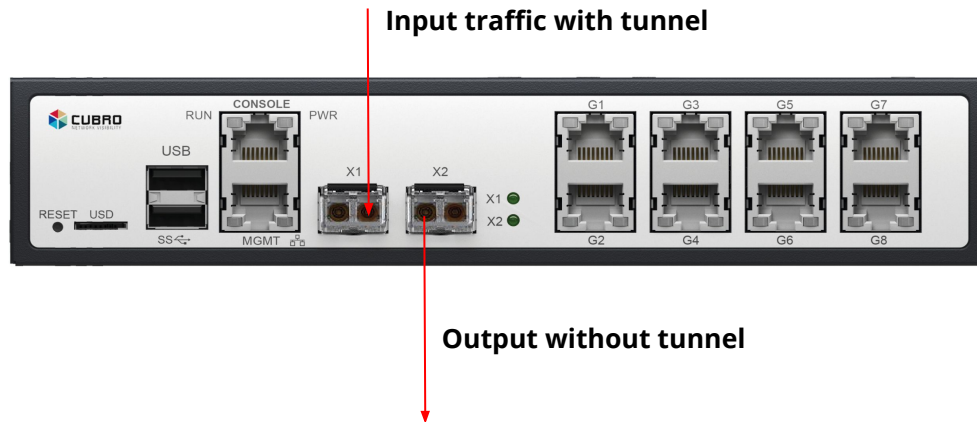
```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{66A4CD...}
Ethernet II, Src: 00:00:00_00:00:01 (00:00:00:00:00:01), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
Internet Protocol Version 4, Src: 0.0.18.7, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 1, Dst Port: 1
Data (8 bytes)
```

000	00 00 00 00 00 01 00 00	00 00 00 01 08 00 45 00E-
010	00 24 de ad 00 00 80 11	89 6b 00 00 12 07 c0 a8	-\$.....-k.....
020	00 01 00 01 00 01 00 10	f1 e0 01 01 01 01 01 01-.....
030	01 01 00 00 00 00 00 00	00 00 00 00

GRE and VXLAN Endpoint



通过在输入接口上配置IP和必要的协议（如IPv4的ARP或IPv6的NDP），Omnia设备可以被配置为主动端点，以便发送器找到网络上的端点。主动接收隧道，然后将其解封装（终止）。



GRE and VXLAN Endpoint



通过G1接口将Omnia设备配置为主动端点。

Properties of Port G1

Basic Advanced

Speed: 1G

Type: Normal

MAC Address: db:20:9f:00:07:18

Ipv4: 0.0.0.0

Arp: Off

Gateway: 0.0.0.0

Ipv6: ::

Ndp: Off

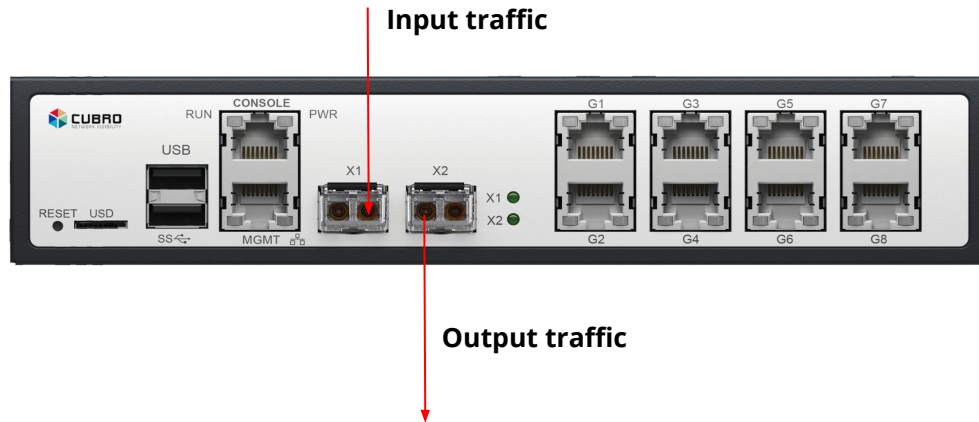
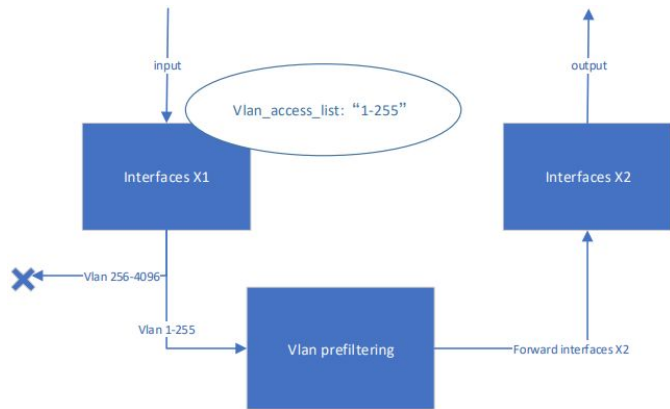
Gateway: ::

Cancel Ok

VLAN过滤



根据端口限制，含有VLAN标签的数据进入系统，实现过滤数据的功能。



不需要将ACL配置为通过VLAN ID进行过滤。

TCP Reordering and Packet Fragment Reassembling

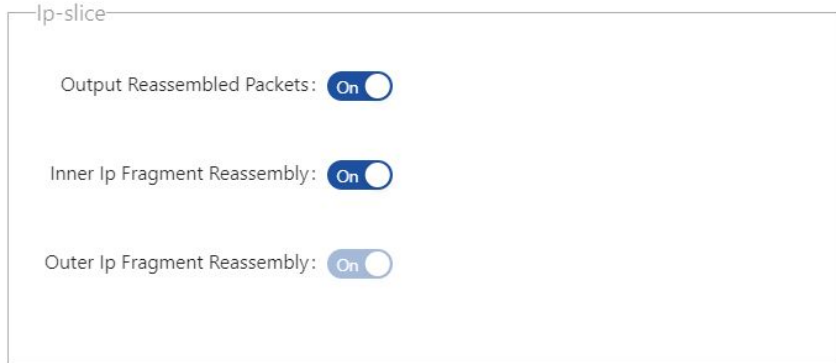
TCP重排序与数据包片段重构



TCP Reordering: 通过这个功能，就可以对已经到达的失序的会话包进行重新排序。



Packet Fragment Reassembling: 通过这个功能，碎片化的IP数据包会被重新组合，并发送到输出端口。

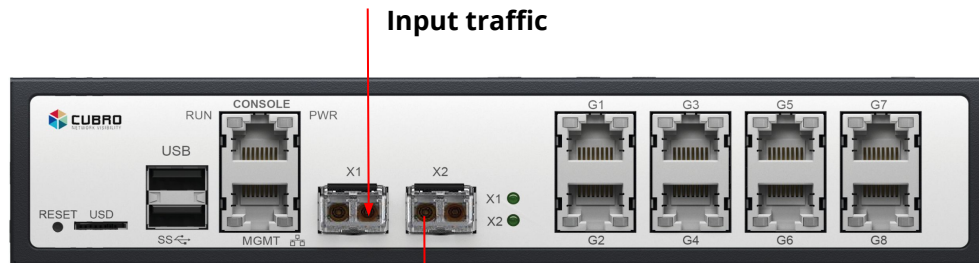


内联或在SPAN端口上进行重复数据删除

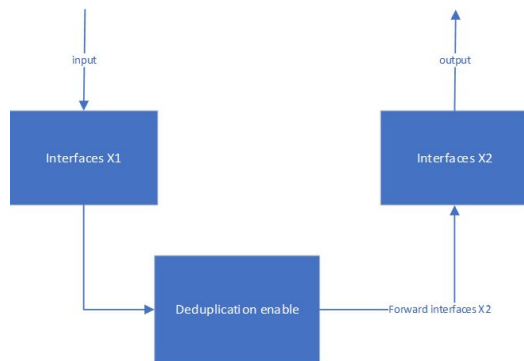


由于在链路上的多个点进行分流，链路上会传输重复的数据包。此功能可在1s内检索出链路上的重复信息，并删除重复信息。

重复报文的基础是从报文的IP层开始，并比较报文末尾的所有数据。用户可以确定数据包的起始深度（Compare - offset）和匹配长度（Compare - depth）。



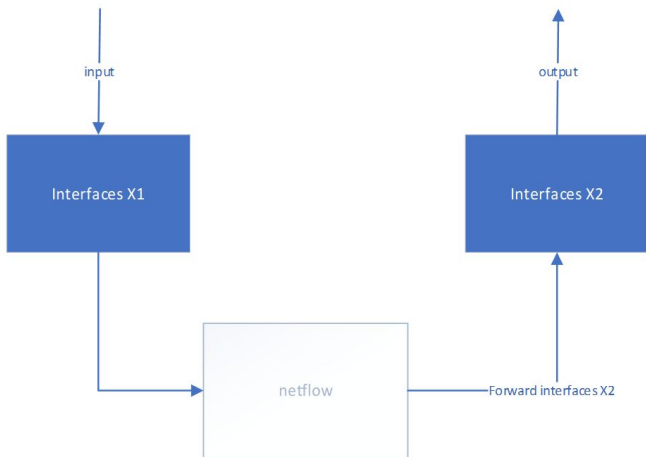
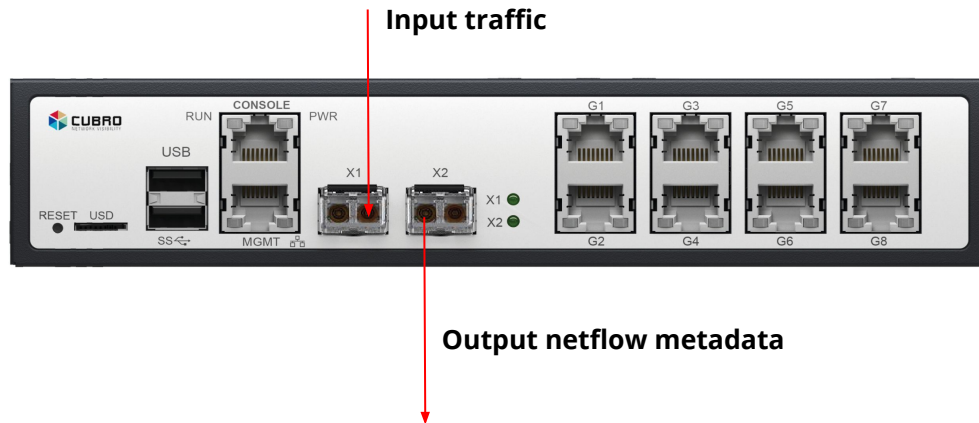
Output traffic



V5 and V9 Netflow Probe



有了这个特性，Omnia就可以作为NetFlow探针，为网络监控生成元数据。我们支持NetFlow V5和V9。



V5 and V9 Netflow Probe



Netflow v9 配置

NetFlow Enable: On

* NetFlow Version:

* IP Type: IPv4 IPv6

* SMAC:

* SIP:

* SPort:

* DMAC1:

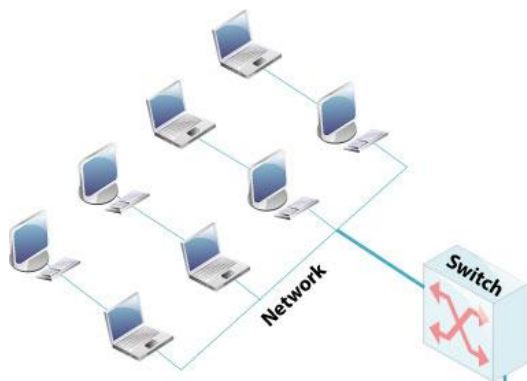
* DIP1:

* DPort:

* Time Out:

* Forwarding Port:

Metadata Exporter Netflow / Netflow - DPI / DPI

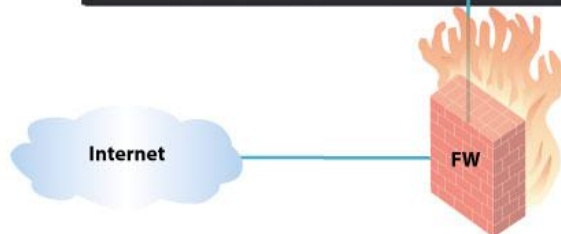


Cubro EXA8

- + 4 x TAP (bypass)
- + Aggregator
- + Metadata extractor



Metadata export
Netflow v9 or IPFIX
Netflow v9 or IPFIX DPI enriched
DPI XDR



SSL/TLS Decryption



SSL / TLS 解密功能配置

SSL Setting

Decrypt Ports: Decrypt Forwarding Port:

[Setting](#)

Flow Session Setting

TCP Flow Session:

[Setting](#)

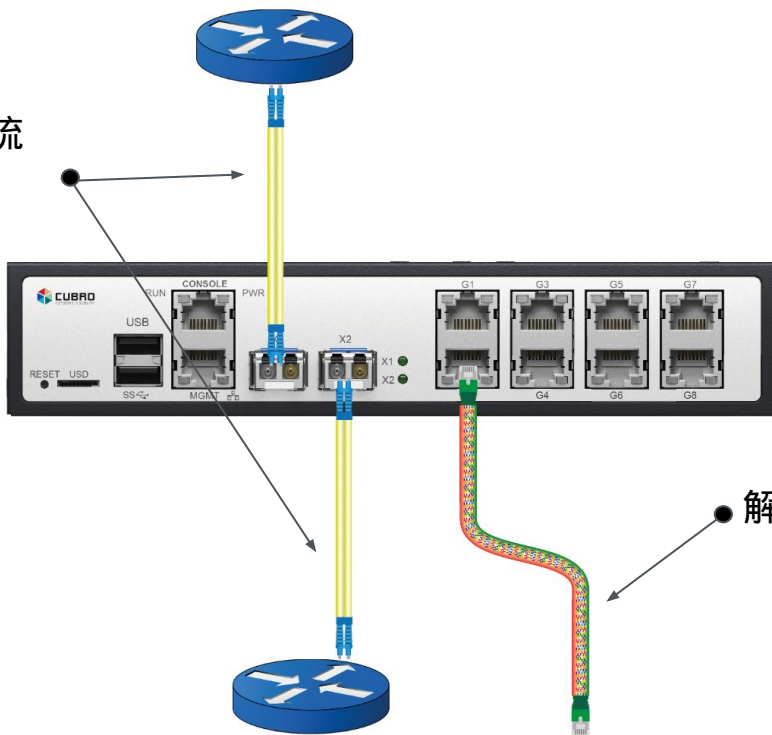
Pkey File Setting

Pkey File List

SSL/TLS Decryption 应用



实时链路加密流量



解密的流量



CERTIFICATE

Management system as per
DIN EN ISO 9001 : 2015

In accordance with TÜV NORD CERT procedures, it is hereby certified that

Cubro Acronet GesmbH
Ghegastraße 3
1030 Wien
Austria



applies a management system in line with the above standard for the following scope

**Sales and development of network monitoring and network
visibility solutions**

Certificate Registration No. 44 100 18600030
Audit Report No. ZCE18/034

Valid from 2019-06-12
Valid until 2022-06-11
Initial certification 2019

Certification Body
at TÜV NORD CERT GmbH

TÜV Nord Austria GmbH
Dietrichshausgasse 35
1150 Vienna, Austria
Vienna, 2019-06-12

This certification was conducted in accordance with the TÜV NORD CERT auditing and certification procedures and is subject to regular surveillance audits.

TÜV NORD CERT GmbH Langenmarkstraße 20 45141 Essen www.tuv-nord-cert.com



CERTIFICATE

Management system as per
DIN EN ISO 14001 : 2015

In accordance with TÜV NORD CERT procedures, it is hereby certified that

Cubro Acronet GesmbH
Ghegastraße 3
1030 Wien
Austria



applies a management system in line with the above standard for the following scope

**Sales and development of network monitoring and network
visibility solutions**

Certificate Registration No. 44 104 18600030
Audit Report No. ZCE18/034

Valid from 2019-06-12
Valid until 2022-06-11
Initial certification 2019

Certification Body
at TÜV NORD CERT GmbH

TÜV Nord Austria GmbH
Dietrichshausgasse 35
1150 Vienna, Austria
Vienna, 2019-06-12

This certification was conducted in accordance with the TÜV NORD CERT auditing and certification procedures and is subject to regular surveillance audits.

TÜV NORD CERT GmbH Langenmarkstraße 20 45141 Essen www.tuv-nord-cert.com



Cubro按照国际标准通过了ISO 9001
质量管理认证。

Cubro公司已获得ISO 14001认证，以
管理我们的环境保护工作。



谢谢

HongKe
虹科

广州虹科电子科技有限公司

需要详细信息？请通过sales@hkaco.com

联系我们 | 电话: 400-999-3848 办事处: 广州 | 北京 | 上海 | 深圳 | 西安 | 武汉 | 成都 | 沈阳 | 香港 | 台湾 | 美国



关注我们



hongwangle