CUBRO
NETWORK VISIBILITY

NETWORK TAPPING OF 2G THROUGH 5G STANDALONE TELECOM NETWORKS

WHITE PAPER

JUNE 2022

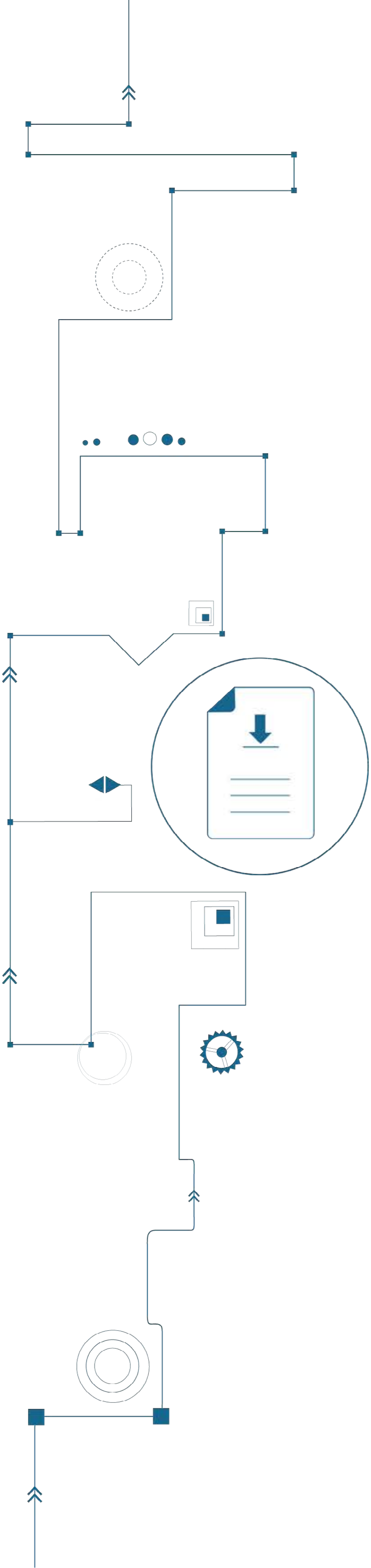


TABLE OF CONTENTS

Tapping and packet brokering in 2G, 3G, 4G and 5G

The purpose of this document is to provide an overview of Physical and Virtual tapping and network packet brokers, their role in telecom networks and how they have evolved from 2G through to 5G Stand Alone network environments.

1. Introduction

Ten years ago tapping the network was simple. Getting a copy of packets to the monitoring systems required only port spanning or an electrical or optical tap between network elements.

Today this is no longer the reality. The links can carry several interfaces and they are not located point to point between physical network elements. Virtualization has made it possible to have a hardware pool being utilized by virtual network functions on a per needed basis, and dedicating certain servers for a specific function is bygone. Furthermore, container based native clouds have changed the landscape. This has all created new challenges for retrieving packet data and providing correct traffic feeds for monitoring systems.

The principle of physical tapping and network packet brokers (NPB) still remains the same. Tapping and NPBs consist of optical splitters mirroring the signal on the link towards the network packet broker that aggregates, filters and distributes the packets to recipients:

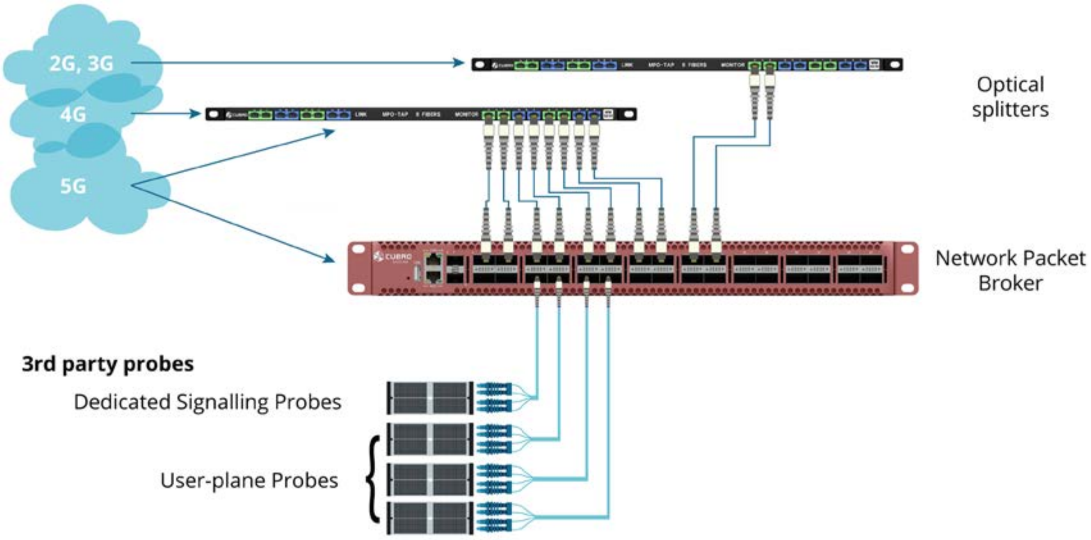


Figure 1: Physical Tapping and network packet broker

Optical splitters are passive components that require no power and the NPB receives the packets passively without interacting with the network. Later chapters will describe the solution for virtualized and native clouds.

The role of tapping and NPB is to passively copy packets from the network and to send them to the probing and monitoring systems which will ingest the packets, open the protocols, decrypt data and create analytics of the received data.

2. Tapping in virtualized networks

When virtualized networks started to evolve, we were often asked whether we provide virtual tapping 'because the network is virtualized'. Cubro still receives this requirement, and a brief answer is: 'We can but a virtualized network doesn't necessarily need virtual tapping and, in most cases, physical tapping is lower cost, easier to maintain, doesn't impact the network and has superior capacity compared to the virtual solution.'

Real life experience shows that networking with OvS is limited to a few Gbps per OvS instance. The performance is better in the VMWare environment, but still limited to 10-15 Gbit/s. This severely limits the usability of virtual tapping.

Regardless of what virtual switch is used, the data is sent from the servers' NIC card towards the Top of the Rack (ToR) switch. ToR switches allow rack-to-rack communication and typically an architecture of leaf and spine switches is used.

Fabric Spine and Border Leaf tapping will capture all of the traffic and allows tapping of multi-Terabit/s traffic.

In some virtualized networks another communication method used is called SR-IOV. SR-IOV allows vNIC to be connected directly to the physical NIC thus bypassing the hypervisor and OvS and enabling a high data capture rate.

Taking into account these factors, in nearly all cases the most efficient solution is to tap the links between leaf and spine switches and access the remaining traffic from NIC cards that are using SR-IOV. This kind of solution is not limited in bandwidth and can scale up significantly to Tbps traffic.

Sometimes east-west traffic between VMs is needed and in that case a virtual tap is required. Many network equipment vendors provide their own SDN/virtual tapping solution that can extract the east-west traffic, which is then routed using GRE.

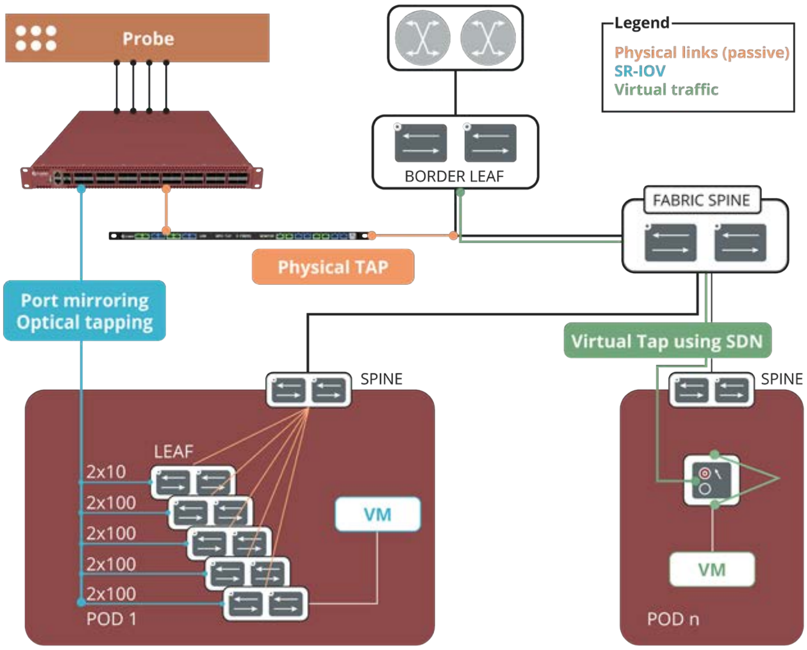
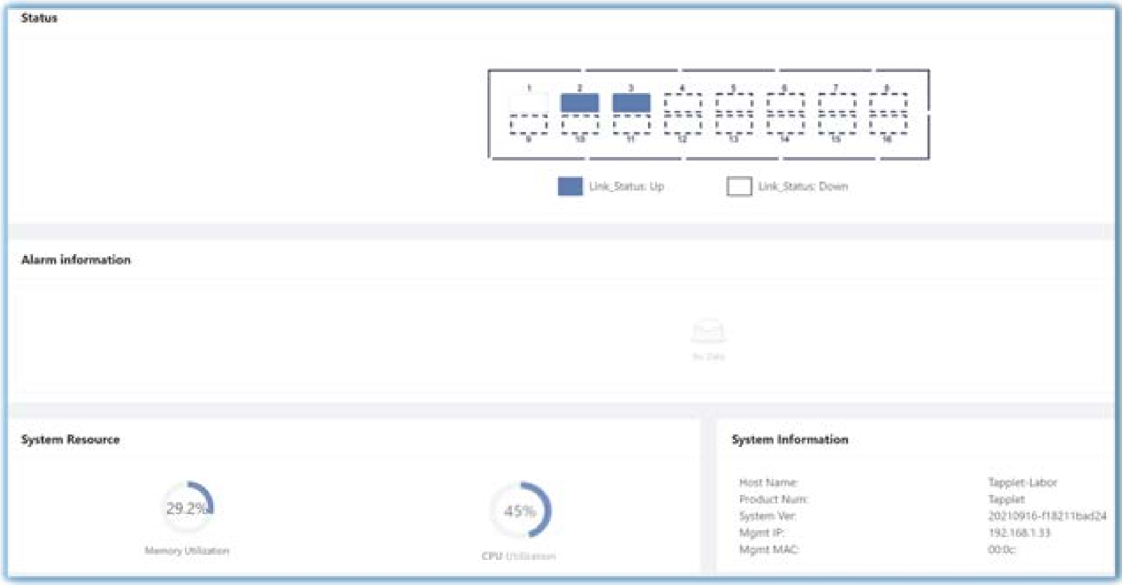


Figure 2: Physical Tapping and network packet broker

Cubro recognizes that virtual tapping can be a viable option when data volumes are from Gbps to tens of Gbps . Under the VMWare environment Cubro provides a virtual TAP and virtual network packet broker as a single VM (Cubro Tapplet). The installation of the VM is done by using ESXi. Once the installation has been done the Tapplet automatically maps its virtual NIC to the physical NICs of the host and mirrors the relevant traffic to the physical NIC.

The Tapplet can filter the traffic based on 5 tuples and send the traffic to a defined IP address or using GRE encapsulation (under Egress configuration).

Below are examples of the Tapplet GUI.



Status

🟦 Link_Status: Up □ Link_Status: Down

Alarm information

System Resource

29.2%

45%

System Information

Host Name: Tapplet-Labor
Product Num: Tapplet
System Ver: 20210916-f18211bad24
Mgmt IP: 192.168.1.33
Mgmt MAC: 00:0c:

Figure 3: Cubro virtual TAP and vNPB (Tapplet) – Main view

In addition to physical tapping and virtual tapping, in some cases a Smart NIC can be a feasible solution to offload the traffic when the architecture and the use case supports it.

3. Tapping in 5G networks

5G networks can be either 5G Non-Stand Alone (5G NSA) or 5G Stand-alone (5G SA). 5G NSA still uses 4G EPC or vEPC. The solution for EPC and vEPC is described in chapters ‘Introduction’ and ‘Tapping in virtualized networks’. 5G SA using 5G Core (5GC) is architecturally very different and requires a new, different tapping approach.

5GC with SBI and cloud native is a major step towards a software based architecture. Cloud elasticity and microservices make it impossible to set fixed rules like before. HTTP2 and more advanced ciphering, such as TLS1.3, challenge the use of any offline tapping methods. In this kind of environment packets need to be fetched within the SBI and data extraction is required to provide the packets to systems outside the SBI.

There are some solutions in the market with 3rd party CNFs, and all of the major network equipment vendors have their own data extraction in clear text.

Cubro is working with major network vendors' data extraction solutions as shown below.

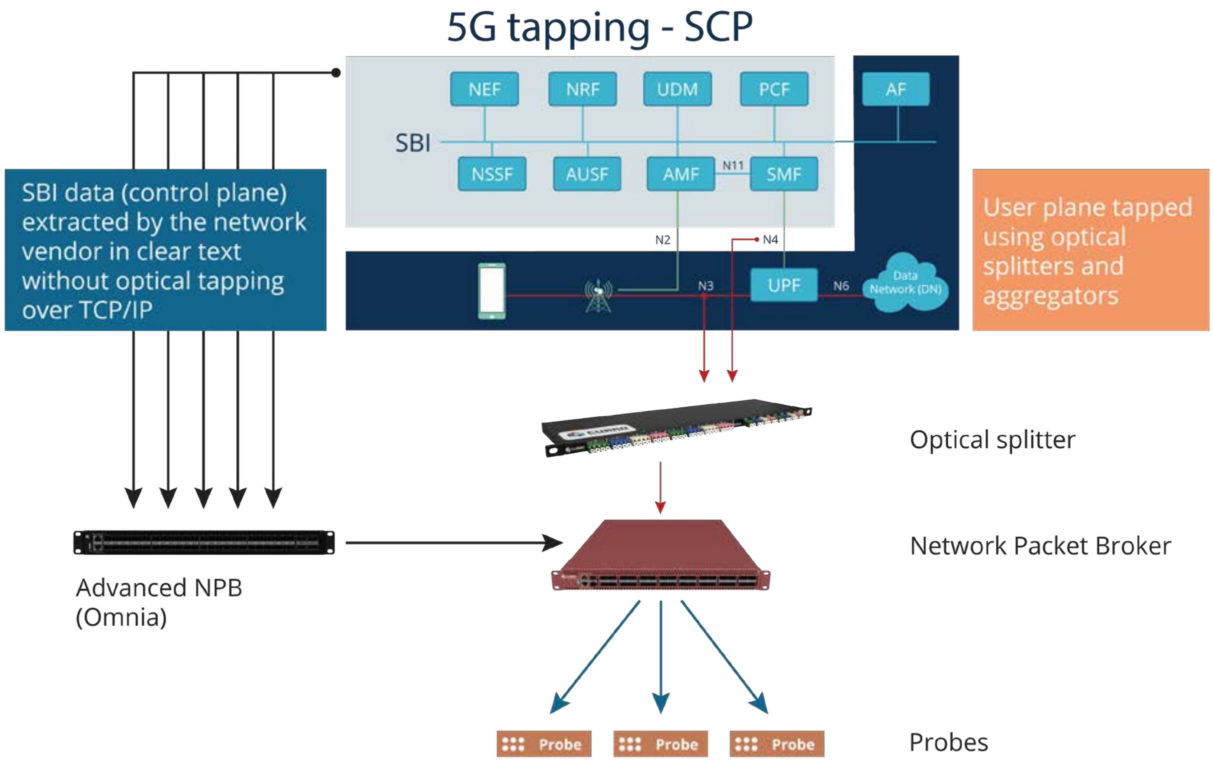

5G tapping - SCP
NEF
NRF
UDM
PCF
AF
SBI
NSSF
AUSF
AMF
N11
SMF
N2
N4
N3
UPF
N6
Data Network (DN)
SBI data (control plane) extracted by the network vendor in clear text without optical tapping over TCP/IP
User plane tapped using optical splitters and aggregators
Optical splitter
Advanced NPB (Omnia)
Network Packet Broker
Probe
Probe
Probe
Probes

Figure 4: Cubro virtual TAP and vNPB (Tapplet) – Main view

Probe and monitoring equipment vendors need to receive both control and user plane traffic. In the example, the vendor extracts the Control plane data and it is received in the Omnia advanced network packet broker. Omnia has the TCP/IP stack to receive the HTTP2 packets and sends the data without any changes to the NPB.

User plane data interfaces are physically tapped and the data is aggregated, filtered and delivered to probes and monitoring systems by the NPB. NPB also sends the control plane data towards the recipients. NPB or advanced NPB can also correlate the user and control plane providing user plane with subscriber identity information towards the monitoring systems.

4. Summary

CSPs have built and are building their own clouds in their Data Centers. The purpose is to use one common cloud stack for all application deliveries. Vendors are expected to deliver their solutions using the cloud software stack that the CSP offers. Often CSPs choose one vendor to deliver NFV Infrastructure that allows them to deploy virtual Network Functions (VNFs) or cloud native functions (CNFs) from multiple vendors. It is also possible to see several 'sub-clouds' which each have slightly different cloud stacks.

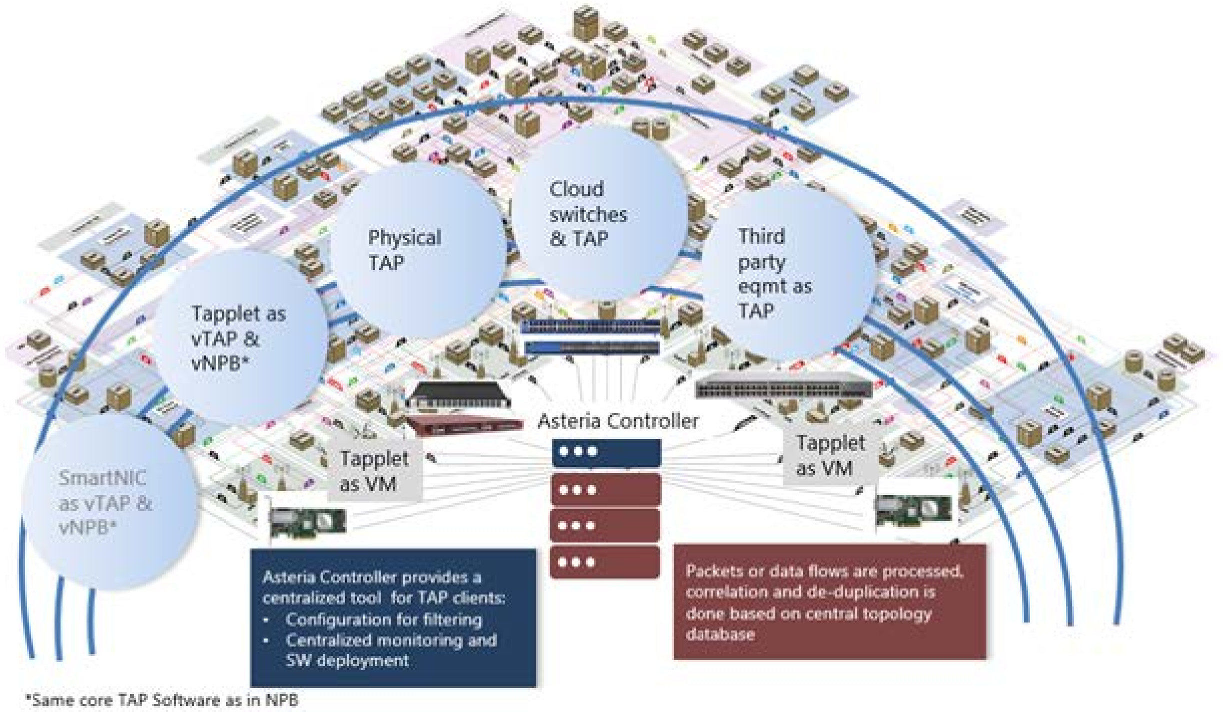
Currently the trend is towards diverse environments where it is possible to see cloud, cloud native and different variants of cloud stack in one network. It is possible that one vendor can provide all NFV / CNF or that there are several vendors providing the functions. This, along with the increasing number of base stations and the high bandwidth needed requires more network flexibility and capacity than ever.

The challenge with bigger networks with extensive technological diversity is:

- Lots of 100G links and very soon 400G links
- Many virtual endpoints
- Cloud native tapping, especially 5GC tapping when encryption is turned on
- Many data centers all over the country
- Network slice monitoring

Despite the increasingly complex environment the monitoring requirements are the same as before – to provide full visibility of the network for various monitoring, security and analytics systems. Cubro believes that visibility needs to be an integral part of the network and not something that is implemented afterwards as an add-on.

Cubro's solution provides customers a number of different options depending on what kind of network is deployed, which vary from physical taps to virtual taps and which can also include Smart NICs and 3rd party embedded solutions.



Asteria Controller provides a centralized tool for TAP clients:

- Configuration for filtering
- Centralized monitoring and SW deployment

Packets or data flows are processed, correlation and de-duplication is done based on central topology database

*Same core TAP Software as in NPB

Figure 5: Cubro solution for diverse cloud solutions

This is to guarantee that no matter what the network comprises, there is a Cubro component that can be used to catch the traffic. Cubro solutions also allow scalability from 1U sized units to 13U appliances that make it possible to use packet broker functionality as well as DPI and probe functions, if needed, with very high capacity.

In many cases the solution includes physical tapping for the reasons explained in previous chapters.

Glossary of terms:

OvS	Open Virtual Switch
NIC	Network Interface Card
ToR	Top of Rack Switch
SR-IOV	Single Root I/O Virtualization
ESXi	VMware Hypervisor
5G NSA	5G Non Stand Alone mobile core network
5G SA	5G Stand Alone mobile core network
EPC	Evolved Packet Core
5GC	5G Core mobile network
SBI	Service Based Interface
HTTP2	Revised Hypertext Transfer Protocol
CNF	Cloud Native Function
NFV	Network Functions Virtualization
Probe	Software or hardware based system that receives network traffic either in packet or xDR format, opens used protocols, correlates user and control plane and creates analytical information from the received data.