Table of Content

1. Introduction
2. Cubro DPI Approach
3. DPI Applications Overview
4. Analytics Applications
5. Filtering Applications
6. Blocking Applications
7. Full Picture Inline Applications
8. Advantages of Cubro DPI
Deep Packet Inspection (DPI) is a technology that enables the network owner to analyse internet traffic, through the network, in real-time and to differentiate them according to their payload.

DPI is often used for understanding the performance or behavior of subscribers, which applications they use, how often etc. This helps operators to focus on improving service for the important applications. For instance, video streaming services like Netflix, YouTube, etc consume a lot of bandwidth. DPI can be used to limit this.
Overview of DPI Applications

DPI facilitates analyzing and managing IP traffic and securing IP networks in real time by providing network visibility and real-time application awareness. Besides influencing bandwidth and traffic management decisions, DPI can provide insights into:

- Network Security
- Network Management
- Network and Subscriber Analysis
- Content Regulation
- Targeted Advertisement
- Application Distribution and Load Balancing
Deep Packet Inspection (DPI) is detecting traffic type by Signature; beyond port and protocol

```json
{ "hash":"7461864e", "service": "whatsapp", "ip_1":"213.143.110.250", "ip_2":"31.13.84.49" }
{ "hash":"7461864e", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"213.143.110.250" }
{ "hash":"ce931c02", "service": "whatsapp", "ip_1":"192.168.3.83", "ip_2":"31.13.84.51" }
{ "hash":"ce931c02", "service": "whatsapp", "ip_1":"31.13.84.51", "ip_2":"192.168.3.83" }
{ "hash":"70d46209", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"192.168.3.30" }
{ "hash":"b6cd9e62", "service": "whatsapp", "ip_1":"80.110.82.15", "ip_2":"192.168.3.130" }
{ "hash":"6fc2f8ce", "service": "whatsapp", "ip_1":"192.168.3.130", "ip_2":"80.110.82.15" }
{ "hash":"55e8f416", "service": "whatsapp", "ip_1":"192.168.3.44", "ip_2":"192.168.43.12" }
{ "hash":"113d5e32", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"192.168.3.44" }
{ "hash":"a597661a", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"192.168.3.72" }
```

This is the output from our DPI engine so we can find WhatsApp even when it is ciphered!
We can find up to 4000 different applications.
DPI applications

There are generally two different main applications for DPI

1. Analytics

In this application the DPI engine can decode the full traffic and produce results in DB format for analytics purpose. This is only possible on CPU based units like (EXA8 / EXA24160 / EXA40 and so on). Since every packet has to be handled, it is a big effort in terms of CPU load and data output.

2. Tagging/filtering/blocking

This application resonates with Cubro approach - remove an unwanted application type from the monitoring. Most common is to remove all video streaming services because it is not relevant for monitoring.

The same application is for blocking certain applications, or sending certain traffic to a special monitoring device. In this case it is not needed to do a full decode because sampling gives a similar result but with much less effort.
DPI Signatures (Applications & Protocols)

We support up to 4000 signatures. These signatures are divided into two parts:

- 1400 see [DPI Services](#) - these are the top signatures which are maintained manually.

- The other signatures are maintained by deep learning and AI.

(The update cycle is between 7 and 10 Days)
Analytics Applications up to multiple TB

Live traffic from TAP/NPB

Available Metadata:
- Timestamp
- User
- User IP
- Service IP
- Application (4000+)
- Packetcount
- Bytes per APP

Possible units EXA8 and EXA1008 (from 8 Gbit/sec to up to 400 Gbit per unit)

Metadata from DPI application

Kafka / Hadoop Cluster

{ "hash":"7461864e", "service": "whatsapp", "ip_1":"213.143.110.250", "ip_2":"31.13.84.45" }
{ "hash":"7461864e", "service": "whatsapp", "ip_1":"31.13.84.45", "ip_2":"213.143.110.250" }
{ "hash":"ce931c02", "service": "whatsapp", "ip_1":"192.168.3.83", "ip_2":"31.13.84.51" }
{ "hash":"ce931c02", "service": "whatsapp", "ip_1":"31.13.84.51", "ip_2":"192.168.3.83" }
Filtering application

Traffic out without video stream traffic to reduce load on monitoring or capture device

and some more
The EXA8 in combination with the EX2 can also be used to block applications like WhatsApp, Skype, Youtube, etc.

We currently support up to 4000 signatures and applications.

The traffic passes EX2 which performs a special sampling method to feed the EXA8 with traffic.

The DPI engine on EXA8 decodes the traffic and configures the drop rules on EX2.
Blocking applications

traffic is passing the unit “inline”

Remove these applications

traffic is passing the unit “inline”
DPI Analysis implemented on EXA8
Blocking applications with G5

traffic is passing the unit “inline”

1% special Cubro sampled traffic

detect these applications

dynamic server IP table to block services

The detector can be any CPU based unit, also a server.

It is also possible to do this on the G5 units host controller (under investigation)
Blocking applications with G5

1) input traffic
2) special Cubro sampling traffic to EXA8
3) generate filter table
4) add filter on EXA32100

WhatsApp is gone :-)

drop ip 31.13.84.49 / 31.13.84.51 and all IP which are in the dynamit table

WhatsApp is gone :-)

@Cubro Confidential
The full picture inline application

1 Live link
2 Bypass output
3 Cubro sampling (pat pending) to DPI unit
4 Management from DPI to Cubro NPB
5 (Load balanced) output to downstream gear

The Cubro bypass protects the live link in a power outage situation.

The Cubro G5 NPB handles the traffic separation, the load balancing and the traffic reinserting of the traffic.

DPI engine based on the resources which are needed. Different models can be used from EXA8 - up to 400 Gbit units.
Up to 2 TB and 8 x 100 Gbit link inline
Advantages of Cubro DPI

Cubro DPI introduces intelligence into the internet network. Unlike most other vendors, Cubro’s DPI approach includes **bypass** and **application blocking** which can enable Internet Service Providers to effectively monitor, speed up, filter, block and make any other useful decision about the traffic of the users.

- Gain the business intelligence to tackle the 5G challenge
- Ensure a lower TCO for the network
- Maintain high levels of network performance
- Enhance the overall QoS
Cubro is certified with ISO 9001 for Quality management according to international standards.

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