DPI Use Case

Practical Example

This document discusses practical examples of deep packet inspection use cases that Enea team are involved with in EMEA region.

- **QOE & Traffic Reporting**
- **Enterprise APN / Zero Rating**
- **VOIP Policy Detection & Enforcement**

#1 QOE & Traffic Reporting

The fundamental reporting of connectivity information form the basis of measuring quality of experience. Enea DPI measuring packet loss, jitter and round-trip time for example as key parameters of layer 4 transport protocols for internet traffic for mobile. This is combined with real time application & flow classification. Enea can break down connection, application, and user data for key quality metrics.

Additionally, Enea software can react in real time to moderate flows, but it is critical to metric the key flow parameters and report – for all users to build real time & aggregate reporting of connectivity experience through the protocols actual used to transport the data.

#2 Enterprise APN / Zero Rating

Fundamental to building additional monetization options for Enea customers in region is engaging for B2B functions. Connectivity is provided via specific APN's – for example in this case a popular internet taxi firm. The case in point is to zero-rate & restrict enterprise devices connecting to this service (noting that this are bring your own device to work) to specific data applications; Application detection on mobile as well as domain restrictions to allowed business and connectivity apps like Facebook are a core part of this service enablement.

Users can access via the app but not the browser on their devices [using protocol meta-data the difference between application and browsers can be detected]. This allows the categorization of these services as 'zero rated' but also to restrict to these specific services.

At a more complex level VPNs, advertising and additional extended sources of content that can occur in application access have to be considered.

This service is supplied without special arrangement or negotiation with the application supplier or device manufacturer. This can't be easily configured or detected by physical DPI boxes – an intelligent software solution is essential.

#3 P2P Policy Detection & Enforcement

Acting on the basis of local governmental legislation the Enea DPI capability provides the ability to detect when mobile device applications initiate VOIP calls. The application content remains **encrypted** and messaging / chat can be classified separately from voice calls.

Enea does not comment on purpose of legislation, but it is more common in the MEA region with countries in the Gulf Cooperation Council banning VOIP services.

In enforcing legislation, the Enea DPI detects when a VOIP call is initiated and subsequently take action (block) based on policy. In the Enea case it is focused on mobile device application