DPI for vEPC vendors: Real-time analytics, QoE and security

ROHDE&SCHWARZ

White Paper | Version 01.00

Table of contents

Acronyms and abbreviations

CSP	Communication service provider
EPC	Evolved packet core
NFV	Network function virtualization
vEPC	Virtual evolved packet core
VNF	Virtual network function
PCRF	Policy and charging rules function
DPI	Deep packet inspection
QoE	Quality of experience
QoS	Quality of service
MEC	Mobile edge computing
MME	Mobility management entity
P-GW	Packet gateway
S-GW	Serving gateway
VM	Virtual machine
COTS	Commercial off-the-shelf
RAN	Radio access network
MVNO	Mobile virtual network operator
IoT	Internet of things
APN	Access point name
M2M	Machine-to-machine
AI	Artificial intelligence
OTT	Over-the-top
TCP	Transmission control protocol
KPI	Key performance indicator
TLS	Transport layer security
SSL	Secure socket layer

1. Introduction

Virtualized Evolved Packet Core (vEPC) is a major breakthrough in network function virtualization (NFV). When asked where they have deployed NFV in production networks, communication service providers (CSPs) consistently name vEPC as one of the top answers. Why is that? In order to maximize their processing capacity, CSPs virtualize a subset of their network applications, including mobile edge computing (MEC), base stations (small/macro cells) and the mobile core, because these systems use a large bandwidth.

The mobile packet core builds the foundation of the core network on which mobile CSPs offer IP-based services to their customers. Implementing vEPC solutions can help CSPs obtain the scale necessary to accommodate growing numbers of subscribers and large amounts of traffic or connections while controlling costs and improving on quality of experience (QoE). In the past, evolved packet core (EPC) solutions were deployed on purpose-built hardware. NFV enables operators to deploy EPC components as virtual network function (VNF) software on standard servers that they can scale up cost-effectively to accommodate projected mobile data demand. Besides reducing the total cost of ownership and operating expenses, vEPC drives the creation of new, more flexible services for an improved time to market and increased revenue.

Many of the world's leading CSPs, including NTT Docomo, Vodafone, Telus, Swisscom, Telstra, VEON, SK Telecom, Tele2, Orange and Ooredoo, have deployed vEPC solutions. Key vendors in the vEPC market include traditional networking vendors Ericsson, Nokia, Huawei and Cisco, Ciena as well as leading challengers, including Affirmed Networks and Mavenir.

Positioned at the intersection of the mobile access network and the wireline backbone transport network, the mobile core is where data handoffs from the access network to the backbone network are processed, policies are enforced and billing information is collected.

Policy and charging rules functions (PCRF) and deep packet inspection (DPI) functions therefore play a critical role for vEPC solutions. vEPC vendors typically license DPI software from a specialist vendor. A high-quality DPI software engine provides the basis for identifying applications in the mobile policy, driving policy and traffic steering and assuring high-quality customer experience.

This paper provides insights on the importance of DPI in creating added value and competitive differentiation for vEPC solutions. It explores what vendors need to consider when evaluating high-quality DPI classification and application analytics. These are, in turn, necessary to ensure high-quality user experience for mobile applications services and to identify new revenue-generating opportunities.

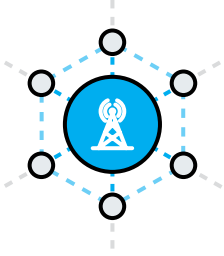
2. Defining vEPC

EPC is the core network of the LTE System. It was introduced by 3GPP in release 8 as a "flat architecture" with the goal of handling data traffic more efficiently from a performance and cost perspective. Recently, it has become available as a virtualized solution (vEPC). vEPC based mobile core network services are built with components such as the mobility management entity (MME), packet gateway (P-GW) or serving gateway (S-GW). These software components are run in virtual machines (VMs) on commercial off-the-shelf (COTS) servers. The number of VMs deployed on a server and the bandwidth delivered have a direct impact on service levels and the number of concurrent mobile user connections that can be supported. Operators typically deploy vEPC when building a new mobile packet core or upgrading an existing one without needing to invest in purpose-built hardware

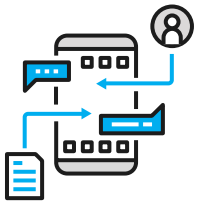
Benefits of vEPC

The benefits of vEPC are widely acknowledged among CSPs that face growing traffic and bandwidth demands as well as pressure to improve the QoE of their mobile applications and services. CSPs are constantly looking out for ways to become more innovative, scale up their networks to satisfy growing demand and deploy more personalized services faster – all without significantly ramping up costs. Moving to a vEPC allows CSPs to react to market changes quickly. Simplified deployment, interoperability and optimization reduce backhaul costs and time to market for new services. Content optimization and intelligent routing in vEPCs can reduce radio access network (RAN) bandwidths by 15-25%.

vEPCs are very useful for mobile virtual network operator (MVNO) and Internet of things (IoT) use cases. By providing IoT devices with a unique access point name (APN), CSPs can steer traffic to a specific packet core isolated from those currently providing consumer and enterprise services. With 5G networks on the horizon, CSPs are preparing for 5G-ready vEPC solutions with an integrated 4G/5G core to ensure network investments are future-proof.



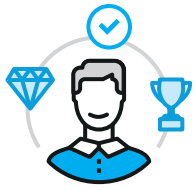
Scale up mobile networks, on-demand and cost-effective



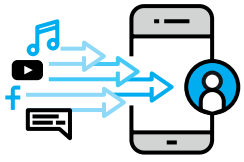
Satisfy an increasing demand for mobile data/Internet services

vEPC business benefits for CSPs

Deliver Network as a Service and new IoT/machine-to-machine (M2M) services to enterprises with network slicing



Improve mobile customers' quality of experience (QoE)



Deliver faster and more personalized services to mobile customers

3. vEPC challenges and the value of DPI

3.1 Network efficiency and optimization

As mobile traffic reaches new heights, the ability to scale up networks cost-effectively becomes a crucial advantage. The arrival of 5G comes along with new bandwidth demands for applications and services that CSPs must satisfy in order to stay competitive. This includes supporting low-latency services and network slicing to suit different mission-critical IoT applications such as healthcare monitoring and enterprise customer requirements.

Value of DPI:
vEPC solutions optimize bandwidth through content optimization and intelligent routing. This requires DPI to classify mobile applications and services and to provide intelligence on subscriber traffic, application usage and patterns. With as much as 80% of mobile traffic consisting of video streaming, an integrated DPI software helps quickly identify types of mobile traffic, such as video streaming, to implement dedicated handling for such traffic, e.g. video optimization, steering or local breakout. High-quality DPI software can also identify encrypted applications and services by means of advanced heuristic analysis. Machine learning and artificial intelligence (AI) algorithms are also employed to identify and recognize traffic flow patterns and large traffic files that cause network congestion. All in all, DPI helps significantly increase customer satisfaction.

„vEPC solutions require DPI to classify mobile applications and services and to provide intelligence on subscriber traffic, application usage and patterns."

3.2 Customer experience and QoE

CSPs are interested in delivering excellent customer experience and reducing customer churn while also developing new services and revenue sources. To do so, they need insight into their network performance (quality of service – QoS) and quality of experience (QoE). These indicate how customers actually experience applications and services. Leading CSPs are transforming their IT and network architecture to be able to manage their actual customer experience or QoE on services proactively and in real time.

Network quality issues are a leading cause of customer churn. Service providers are looking for vendors that can provide them with better network visibility and real-time analytics to identify application and service congestion and to take pro-active action before customers notice any impact.

Value of DPI:
By embedding DPI, vEPC vendors can identify which applications and services are currently active on their networks, helping them drive automated policy and traffic steering to assure QoE. Real-time analytics that identify which mobile applications are in use help classify traffic, for example as low-latency (voice), guaranteed-latency (web traffic), guaranteed-delivery (application traffic) and best-effort-delivery applications (file sharing).

3.3 Real-time subscriber analytics and NFV service chaining

With operators virtualizing the mobile network core, services become more dynamic and personalized. This allows for new functions such as on-demand services powered by chains of VNFs. Real-time analytics are crucial in understanding subscriber behavior, identifying active applications and network problems and taking the appropriate actions based on the gained insights.

A DPI VNF embedded in a service chain can feed application information and metadata to other integrated components. For example, embedded DPI in dedicated service chains can improve QoE on over-the-top (OTT) video applications. DPI extracts performance metadata such as transmission control protocol (TCP) optimization key performance indicators (KPIs) and dynamic bitrate adaptation to maximize video QoE and improve customer experience.

Value of DPI:
DPI identifies and extracts information transmitted over networks in real time, providing accurate insight into traffic by identifying protocols, types of application and extracting additional information in the form of metadata. Streaming these data records to an analytics engine in real time facilitates business decisions and process automation. Subscriber analytics can also be critical in driving new services and creating revenue. Next-best-offer/action or micro-segmenting subscribers for marketing campaigns are examples of how understanding subscriber behavior and application usage can enable targeted action, such as sending top-ups for mobile data or offering discounts in case of customer complaints.

3.4 Security threats and fraud protection

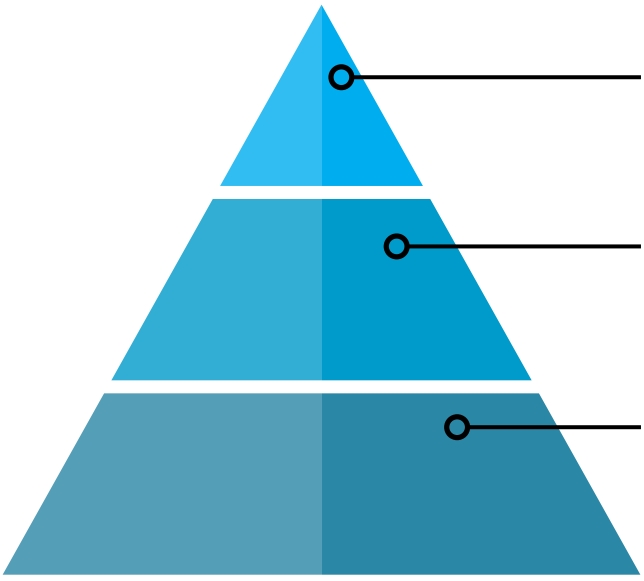
Malware embedded in mobile applications and attempts to defraud mobile operators pose serious threats. Application visibility helps security teams discern patterns in the data. With in-depth traffic inspection features, they can spot unusual activity more easily. For example, a detection functionality for Discord, a chat app that is popular with online gamers, enables network security solutions to distinguish legitimate use of the chat app from malicious activity. Machine learning and AI algorithms can also help catch DDoS attacks or other unusual malicious and suspicious activity. Suspicious traffic can then be steered for inspection.

DPI provides application visibility, which is useful to support software-based VNFs for unified threat management, including state-of-the-art and next-gen firewalls, malware protection, URL and content filtering, IPS, antivirus software and DDoS protection. DPI application visibility prevents firewalls from accepting malicious traffic and malware from passing through the gates unseen.

Value of DPI:
DPI content and metadata extraction is key to advanced threat and fraud analytics and can not only strengthen network security, but also enables enhanced security services such as NAT, subscriber firewalls, content filtering, parental control etc.

„DPI identifies and extracts information transmitted over networks in real time, providing accurate insight into traffic by identifying protocols, types of application and extracting additional information in the form of metadata."

Key functionalities of the DPI engine R&S®PACE 2



Encrypted Traffic Intelligence (ETI)
- Classify applications regardless of encryption and obfuscation
- Classify encrypted audio and video streams
- Classify devices behind NAT and tethering

Content & Metadata Extraction
- Performance KPIs, e.g. for VoIP, VoLTE and video streaming
- Full content and metadeta extraction for SIP, RTP and many other communication protocols

Protocol & Application Classification
- Classify over 2800 applications and protocols such as Netflix, Snapchat, Skype and Youtube
- Classify full protocol stack from layer 3 to 7+

4. DPI use cases for vEPC

By integrating DPI into a vEPC as a virtual network function (VNF), vEPC vendors can offer virtual probe analytics and additional functionalities enabled by DPI from a single source. Co-locating DPI with the vEPC reduces hardware cost, network complexity and performance issues typically associated with legacy probe solutions.

Analytics

- Real-time application visibility
- Most used applications and web sites
- Usage profiles
- Quality of experience metrics
- Dynamic and personalized marketing (next best offer/action), Customer Experience Management (CEM), telecom fraud and threat detection
- Selective reports on session control, subscriber events and subscriber data by user-defined filtering

Policy enforcement

- Traffic shaping and management
- Prioritization of key business traffic
- Enhanced VoIP performance
- Enforcing QoS based on dynamic network conditions
- Time of day policies

Tiered pricing

- Individual charging based on application level
- Zero-rate charging per application, service or unlimited mobile data packages
- Policies per user or user group enforced by DPI

Web and video optimization

- Measuring mobile application performance and user QoE
- Support of voice over IP (VoIP), audio & video KPIs such as throughput, latency, jitter
- Attribution of application usage types, such as Skype audio and video calls, to determine application performance and QoS for VoIP and video and to protect against network security threats
- Policy-based optimization, video pacing/caching/optimization, QoE-based optimization

Content filtering and parental control

- Application visibility and advanced signature analysis allowing insight into the traffic flow to filter content

Fraud detection, e.g. tethering abuse

- Tethering and fraud detection powered by network address translation (NAT), including the identification of:
  - Internet access points shared by several devices
  - The number of devices behind a tethered IP
  - The traffic share per device

Security services

- Application identity-based policy rules, Application and Service blacklisting, whitelisting, geo-IP, customer app ID-signatures, firewall SSL certificate-based protection, expired certificates, untrusted CAs, unsupported cyphers and key lengths
- Subscriber firewall, NAT/CG-NAT, Operator blacklists, Static/dynamic categorization, fraud detection, malware/phishing detection, content filtering, Operator whitelists, IWF

NFV service chaining

- Embedding of DPI into service chains allows operators to easily segment and steer traffic (using application detection, classification and policy controls) to network slices optimized for the services delivered, e.g. video streaming traffic
- Traffic steering based on a variety of criteria, such as device type, location, loading, time of day or external policy
- Automated network slicing in 5G networks
- Traffic selection and steering based on highly granular criteria
- Slice performance monitoring in real time
- Overall: delivering high QoE with the right level of security

5. DPI in vEPC solutions

5.1 Service classification for dynamic function chaining

Challenge for service providers
CSPs require full control of video traffic in order to improve customer QoE. A dedicated, DPI-enabled service chain in a vEPC that includes TCP optimization and dynamic bitrate adaption maximizes QoE and reduces RAN congestion. DPI software detects and classifies traffic and forwards it to the respective service chain.

DPI benefits
- Identifying OTT video streaming, including encrypted video
- Extracting TCP performance KPIs
- Enabling TCP optimization

5.2 Zero-rated fraud using DNS tunneling

Challenge for service providers
Various freeware tools are able to hide web surfing traffic by means of DNS tunneling to avoid mobile charges. With DPI integrated into the firewall, vEPC vendors can detect potential policy bypasses and zero-rating fraud. Anomaly detection and heuristic analysis enable vEPC vendors to not only detect, but also block this kind of traffic.

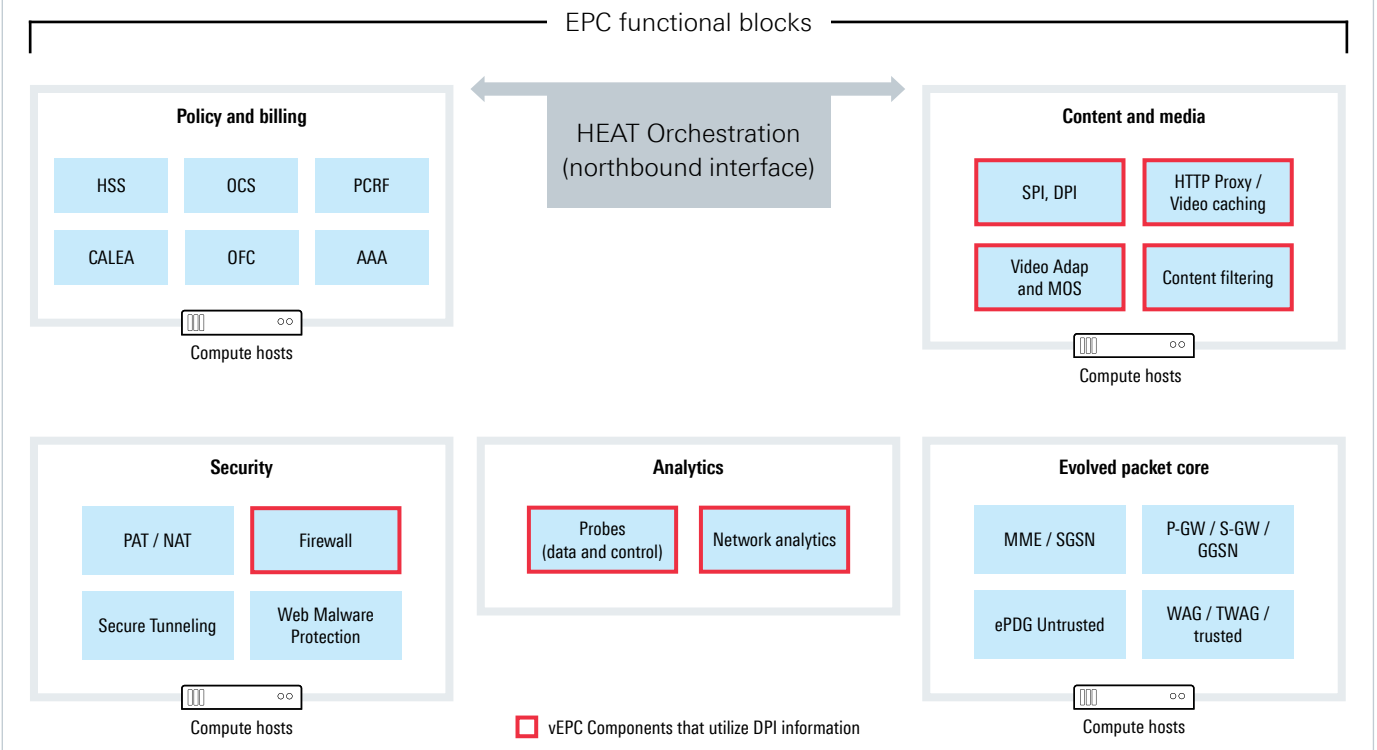
DPI benefits
- DPI content and metadata extraction as key to advanced threat and fraud analytics
- Detecting DNS tunnelling
- Identifying anomalies in DNS transactions

5.3 Advanced subscriber analytics

Challenge for service providers
AI-based subscriber analytics and correlation techniques enabled by DPI revealed that 75% of online gamers use the chat app Discord. A CSP used this insight to provide a dedicated zero-rating plan that includes popular games and Discord.

DPI benefits
- Identifying mobile apps used by subscribers
- Enabling the creation of subscriber profiles and trend analytics
- Supporting new service revenue and marketing opportunities

The core components of vEPC in combination with DPI



6. Encrypted Traffic Intelligence (ETI)

While advanced DPI techniques cannot extract content from encrypted applications, they still provide valuable classifications, such as into Facebook, WhatsApp, Skype etc.

An increasing number of protocols and applications, including Skype, WhatsApp, BitTorrent, Facebook, Twitter, Dropbox, Gmail, Office365, Instagram etc., are encrypted. In addition, some protocols, such as eDonkey, Freenet and other P2P apps, Ultrasurf or YourFreedom, can adapt to circumvent firewalls and DPI detection, for example when traffic is limited or blocked for a specific protocol.

Most encrypted internet connections encrypt with transport layer security (TLS) or secure sockets layer (SSL). Both technologies establish connections by means of a handshake. All information that is necessary to classify a protocol application is transferred with this handshake.

While it is still possible to classify an encrypted application, extracting metadata or content data is not possible for end-to-end encrypted applications.

However, DPI engines can still detect application categories, such as voice call or chat, using advanced heuristic and statistical approaches.

R&S®PACE 2, the DPI engine by Rohde&Schwarz, is able to provide reliable classification results with a very low false negative rate and virtually no false positives. A variety of detection techniques make this possible:

1. Pattern Matching – Simply checking for recurring strings and numbers in IP packets.

2. Behavioral Analysis - Checking for packet sizes and the order of different packet sizes within the IP flow while tracking information about the subscriber and host.

3. Statistical/Heuristic Analysis on common attributes such as recurring byte-orders or metadata analysis within the IP flow.

„DPI can gather information about encrypted or obfuscated applications and protocols by using heuristic methods."

DPI extracted metadata from encrypted and unencrypted traffic

Metadata category	Example metadata
Traffic volume	Per user, per protocol, per application, per flow, per direction
Service detection	Differentiation between e.g. Skype audio and video calls
Quality of Service	Jitter, throughput, latency, roundtrip time, ramp up time, packet loss, retransmissions
Security and data leakage	File up- and downloads, entropy-based DNS tunneling detection, prevention
Client information	HTTP/QUIC user agents, operating system

7. Build or buy DPI?

vEPC solutions rely on DPI application awareness as a key enabling feature for policy control, critical traffic steering, content optimization and security. Vendors have to make a strategic choice between building in-house DPI libraries and licensing software from a DPI specialist.

A DPI engine is only as effective as its creators make it. In-house DPI engines face the major challenge of needing to continually update their software with the latest applications and protocols in order to offer up-to-date visibility of network traffic. Because of the constant evolution of network traffic with new applications and protocols appearing non-stop, DPI software is never complete.

DPI software companies have dedicated DPI experts that add new application signatures on a weekly basis. This ensures that a high percentage of network traffic can be reliably classified, which is critical in the case of vEPC solutions that need to make policy and intelligent routing decisions on the basis of reliably classified traffic. As a result of continuous performance and reliability testing, regular improvements can be made to the software to ensure all applications are detected.

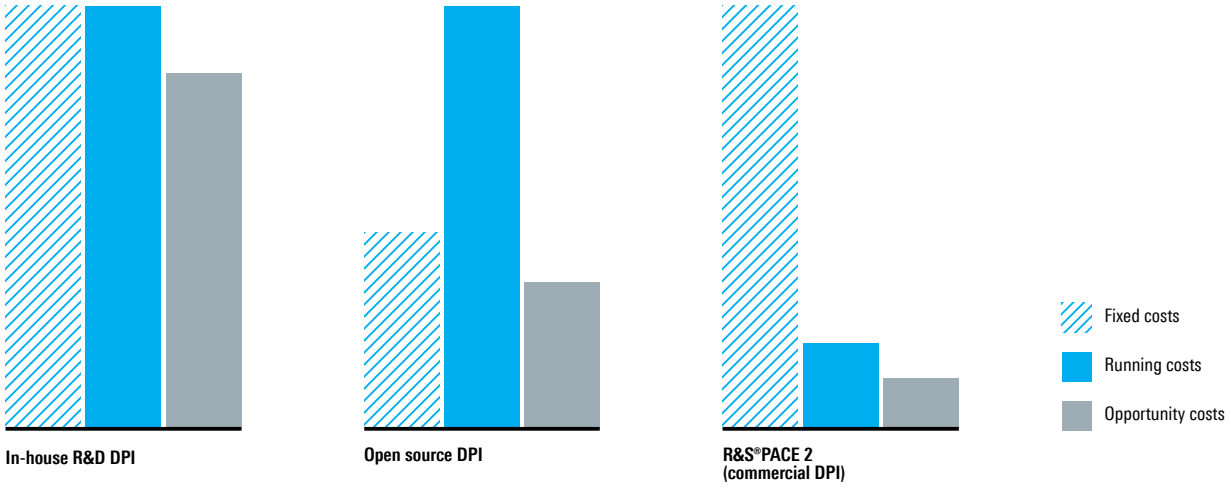
Vendors may consider open source DPI with the idea that it is free to use. However, there are some important considerations – both pros and cons – to adopting an open source DPI library. Open source software often ends up not being free, because it still requires in-house developers to learn about the software and, more importantly, to customize it. Frequently, this requires working with a third-party vendor to manage and add new features.

Most vEPC vendors simply do not have the in-house resources to track and classify the latest apps and protocols. Ready-to-use DPI software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally. Instead, vEPC vendors can focus valuable time and resources on their core products in what is proving to be a highly competitive market.

> „Ready-to-use DPI software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally."

The DPI solution by Rohde&Schwarz is extremely easy to integrate and enables vEPC vendors to obtain DPI for their vEPC solutions from a single source, eliminating the need for standalone probes. The protocol and application classification engine R&S®PACE 2 offers the industry's most efficient memory and CPU utilization, featuring the smallest processing footprint. R&S®PACE 2 only requires ~ 400 bytes per flow while using very little processing power (CPU load) and no memory allocation during run time. This is crucial for CSPs looking for efficient solutions that reduce operating expenses and can support 5G and NFV-enabled network slicing. By integrating R&S®PACE 2, vEPC vendors can keep up with the dynamic changes in protocols and applications, which ensures a high rate of detection for traffic management.

Commercial DPI reduces development costs



8. Conclusion

The vEPC market is developing fast with vEPC becoming a critical prerequisite for mobile operator networks. In 5G and NFV telco cloud networks, real-time application visibility and enhanced security features and analytics are highly valued and key to driving QoE for on-demand and personalized services. DPI embedded in service chains and network slices supports real-time analytics and QoE, including visualization and reports on application performance and security diagnostics for real-time network and service operations. With the help of DPI technology, vEPC vendors can now deliver powerful intelligent routing, traffic steering and enterprise application performance solutions with advanced reporting capability. The software detects and classifies applications reliably and accurately, is easy to implement and requires no in-house resources to track and classify the latest apps and protocols, simplifying the extraction of valuable metadata. Analytics, policy enforcement, tiered pricing, web and video optimization, content filtering, parental control or security services – DPI is a crucial enabling technology to implement value-adding services in vEPC solutions.

„DPI is the essential key for vEPC vendors in order to truly maximize competitive service differentiation and to transform markets focused on network agility, intelligence and automation."

Service that adds value

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

ipoque

ipoque, a Rohde&Schwarz company, is a leading vendor of deep packet inspection software that adds protocol and application classification capabilities to network analytics, traffic management and cybersecurity solutions. Rohde&Schwarz also provides a holistic network traffic analytics system for communication service providers that allows deep insights into network behavior, network performance and trends to optimize both quality of experience and quality of service.

Rohde&Schwarz

The Rohde&Schwarz technology group develops, produces and markets innovative information and communications technology products for professional users. Rohde&Schwarz focuses on test and measurement, broadcast and media, cybersecurity, secure communications and monitoring and network testing, areas that address many different industry and government-sector market segments. Founded more than 80 years ago, the independent company has an extensive sales and service network in more than 70 countries.

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

ipoque GmbH
Augustusplatz 9 | 04109 Leipzig
Info: + 49 (0)341 59403 0
E-Mail: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 5216.4310.52 | Version 01.00 | November 2018 (mh)
White paper | DPI for vEPC vendors:
Data without tolerance limits is not binding | Subject to change

5216431052