APPLICATION AWARENESS

Solution Guide

NEXT-GENERATION DEEP PACKET INSPECTION

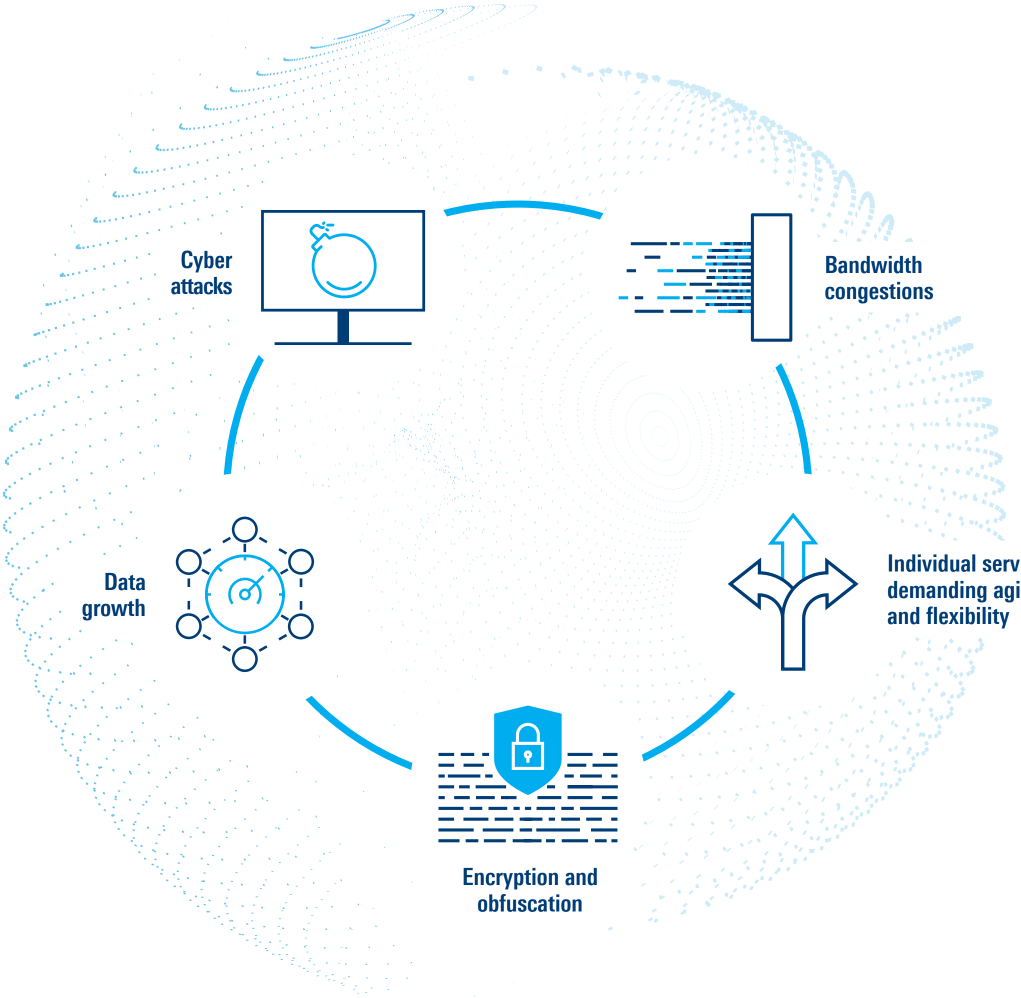
ROHDE&SCHWARZ

Make ideas real

CONTENT

1. INTRODUCTION

Over the past years, the evolution of networks has accelerated in many areas. Expanding technologies such as cloud computing, 5G and widespread encryption are introducing new risks and opportunities that significantly challenge IT professionals. If you are a provider of (mobile) networking or cybersecurity solutions, you are navigating your business in challenging and yet promising times. And you are well aware that in order to thrive, you must find cogent ways to deal with:



Cyber attacks
Bandwidth congestions
Individual services demanding agility and flexibility
Encryption and obfuscation
Data growth

Tackling these challenges demands granular visibility into IP traffic data at any time. Accordingly, a solution has to:

- Provide real-time insights into IP traffic
- Cover a broad portfolio of network protocols and applications across diverse operating systems, versions and service types
- Be up to date with recent changes in applications and protocols at any time
- Find ways to analyze encrypted and obfuscated traffic

By embedding the ipoque deep packet inspection (DPI) technology into your networking, telco or cybersecurity solution, you gain granular and reliable IP network traffic visibility, even into encrypted or obfuscated traffic.

2 FAST FACTS

Enhance your networking, telco or cybersecurity solution with powerful application awareness! The next-generation DPI engine R&S®PACE 2 or the cloud-native vector packet processing (VPP) DPI engine R&S®vPACE boost your solution with market-leading DPI technology superior in performance, reliability and ease of use.

The ipoque DPI fast facts	R&S®PACE 2	R&S®vPACE
CPU architectures	Any hardware with a C compiler: 32-bit and 64-bit x86, MIPS, ARM v7 and v8, Power PC, Cavium, etc.	64-bit x86
Operating systems	Unix-based operating systems	Unix-based operating systems
Performance	14 Gbps throughput per core, on average	High-performance optimized for vectoring/VPP, up to 3x higher than with scalar packet processing. Reduced clocks-per-packet count.
Metadata extraction	Yes incl. full decoding (incl. TCP reassembly)	Yes, support for TLS, HTTP, SIP, QUIC, OS (user agent), DNS extraction
Service and support	Individual SLAs Dedicated consulting engineers	Individual SLAs Dedicated consulting engineers
Memory footprint	458 bytes per flow (5-tuple connection) 681 bytes per subscriber (endpoint address)	384 bytes per flow (5-tuple connection) 672 bytes per subscriber (endpoint address)
Written in	C	C
APIs	C public headers (events) Supports JSON serialization	C public headers

Key Features

- Market-leading performance values and linear scalability
- Encrypted traffic intelligence: reliable application classification despite encryption and obfuscation powered by machine learning and deep learning algorithms
- Most efficient memory usage on the market
- Classifies almost 100 % of network traffic (virtually no false positives) with a time resolution down to nanoseconds
- Real-time classification of protocols and applications for all verticals and regions across diverse operating systems, application versions and service types
- Detailed insights into application-centric statistics for QoS/QoE, for example KPIs on network performance for applications such as VoIP and video streaming
- Weekly signature updates, including new and updated applications and protocols
- No downtimes thanks to dynamic upgrades
- Tethering detection: Detect devices behind routers or smartphones using mobile tethering
- First packet classification through service caching and DNS caching
- Flow data exporter compatible with any IPFIX network, supporting export to Netflow v10, and input of sFlow samples
- Custom service classifier: Define your own signatures

3 NEXT-GENERATION DPI

3.1 What is DPI?

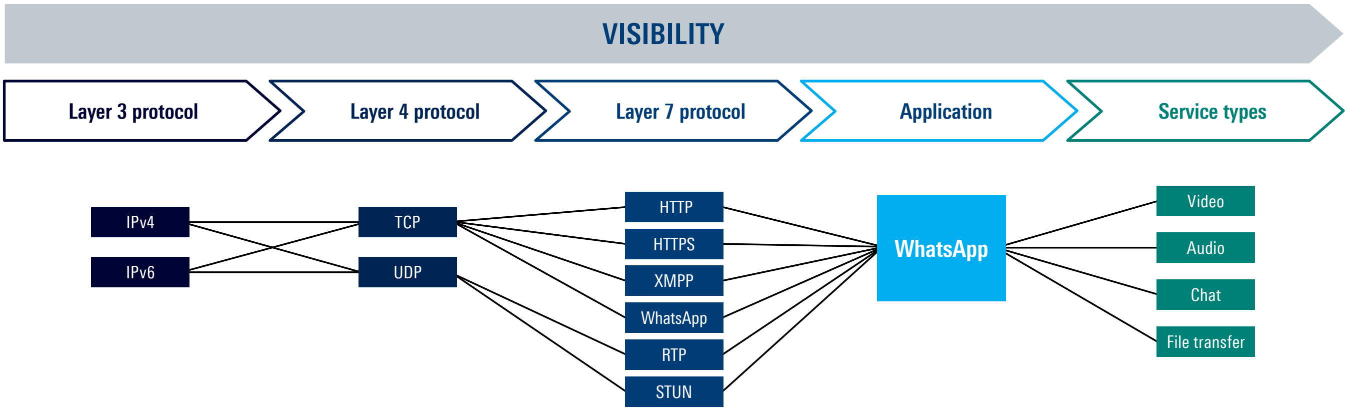
Deep packet inspection (DPI) is a filtering technology, essential for examining IP data packets from layer 3 to 7, classifying IP traffic and extracting metadata. Our next-generation DPI technology provides granular insights into IP traffic by detecting protocols, applications and even application attributes and services (for example video, audio, chat or file transfers in a messaging client). Metadata extraction reveals specific information on speed, latency, user locations, jitter, bandwidth consumption, type of devices, etc. With a wide range of traffic classification methods, including port-based matching, pattern matching, behavioral analysis and statistical/heuristic analysis, the ipoque DPI technology provides more than standard DPI and delivers modern networks with what they need most – intelligence. Machine learning (ML) and deep learning (DL) capabilities enhance classification accuracy and enable encrypted traffic awareness. Deployed as a software or purpose-built hardware, our DPI engines can perform large-scale traffic filtering, inline or out-of-bound, in any part of an IP network.

3.2 Next-generation DPI technology for multiple networking use cases

We offer two DPI engines, specifically designed to meet the needs of today's and future networks. R&S®PACE 2 is a powerful, all-around DPI engine, optimized to provide a rich set of metadata. Slim and fast, R&S®vPACE is vector packet processing (VPP) based and designed for frameworks such as FD.io or DPDK Graph to empower virtual and cloud-native network functions with high performance. DPI-based packet classification is the core of both libraries that are updated on a weekly basis. Leveraging the OEM DPI software from ipoque, vendors of networking, traffic management and cybersecurity solutions can readily deploy DPI without having to develop the capabilities in-house or resort to open-source DPI tools.

Additional options, add-ons and features extend the capabilities of our DPI technology, making it adaptable to any individual solution. For example, in analytics use cases, R&S®PACE 2 can use optional output buffers to serialize events to JSON for visualization. Options to group results per service type (for example "video", "audio", "chat") or protocol and application (for example "messaging", "web", "streaming") facilitate data flow analysis and intelligent decisions for traffic management and policy enforcement solutions. Flexible SLAs allow vendors to adapt the DPI engine to their customer's demands, while our dedicated consulting engineers are happy to offer integration and optimization consulting.

CLASSIFICATION BEYOND LAYER 7



4 LICENSING OEM DPI

With more than 15 years of experience in network intelligence, ipoque has established itself as a market-leading OEM DPI software vendor. Our DPI software is being deployed globally by developers of networking and cybersecurity solutions to accelerate time to market, reduce R&D cost and stay ahead of the competition.

4.1 DPI as a service

Developing a simple IP traffic signature is no rocket science. So why don't you build up your own DPI library? Developing a DPI solution in-house is doable, yet it takes many working hours by domain experts. Advanced DPI engines such as R&S®PACE 2 and R&S®vPACE instantly provide a market-leading classification portfolio, grown and developed with years of feedback and requirements by customers from all over the world. And while the costs of developing and maintaining a complex technology in-house are hard to estimate in advance, licensing costs are predictable and fixed.

Open-source software, on the other hand, is free at first glance, but your developers still need to learn about the software and how to customize it. Oftentimes, this customization requires collaboration with third-party vendors to manage and add new features. Our dedicated experts maintain licensed DPI software by adding new signatures every week through seamless updates during runtime. This way, you make sure that your DPI solution works reliably at any time. This reliability enables you to make informed and vital decisions based on granular traffic classification. DPI technology by ipoque, customized and deployed on-site by leading experts, reduces your costs and risks associated with internally developing and maintaining a highly complex technology.

With well-defined APIs, integration examples, superior service and support, the ipoque DPI engines can be easily embedded in any solution – developed in-house or by third parties – and enhance it with real-time traffic visibility. The ipoque DPI technology is platform-agnostic (supporting x86, ARM, Cavium Octeon, Power PC, etc.) and runs on Unix operating systems, such as Linux, Mac, FreeBSD, using a C interface.

Tap into our DPI expertise

Leverage decades of experience
Over 15 years of experience in OEM DPI software and IP network analytics

Minimize R&D
A team of more than 160 in-house developers and extensive partnerships with leading universities, pushing the boundaries of research in big data, AI and machine learning

Deploy industry leading software
Market leading commercial OEM DPI solutions with one of the highest traffic detection rates and lowest memory footprint in the industry

Stay ahead of the market
Continuously improved, weekly-updated DPI signature library with thousands of signatures

4.2 Key benefits of licensing OEM DPI from ipoque

- Reduce development costs and maximize return on investment (ROI)
- Tailor our OEM DPI software to suit your exact use case or application
- Take advantage of flexible SLAs
- Benefit from deployment support and consulting, including on-site integration and application engineering assistance
- Receive support from a dedicated account manager
- Instantly report any issue with 24/7 support
- Stay up to date with high-level product trainings down to low-level feature and integration trainings
- Optimize your DPI performance with in-house code reviews and troubleshooting assistance
- Influence our product roadmap by requesting new features and support for new protocols and applications

5 TECHNICAL CAPABILITIES AND FEATURES

5.1 Signature core

Classification accuracy

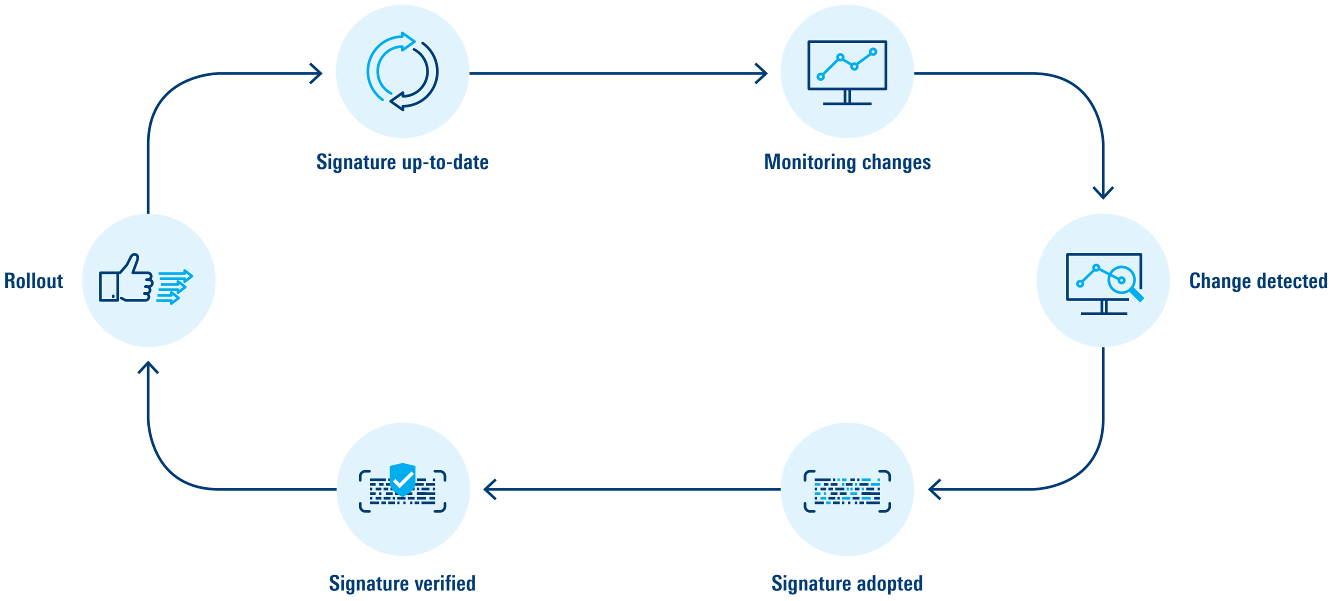
The ipoque DPI engines use a wide variety of leading-edge techniques to classify network traffic. Thanks to this approach, they can reliably detect network protocols and applications despite advanced obfuscation and encryption techniques (see below). In many use cases, false positives in the classification results are not acceptable. For example, operators have to rule out false positives in the area of billing as this can have a negative revenue impact and potentially damage the brand image. In cybersecurity use cases, false positives can make a huge difference and enable attacks and data breaches. With sophisticated classification algorithms ruling out false positives, the ipoque DPI library proves its worth.

> Using leading-edge classification techniques, the ipoque DPI engines can accurately classify almost 100% of network traffic with virtually no false positives.

Thanks to the feedback and requirements from customers from different areas and verticals worldwide, DPI technology by ipoque has a very low rate of undetected applications (false negative rate). The application portfolio covers the IT, OT and IoT range and includes numerous business and mobile applications.

New releases of an application, such as new clients or new features, can change its behavior and cause classification problems. This requires constant attention since details for most application changes are not announced publicly. In addition, applications behave differently on different devices, on different operating systems and in different networks. As a result, reliable and accurate application classification does not only require a signature library, but ongoing maintenance and testing, particularly for frequently changing mobile applications. Automated traffic monitoring and testing as well as our dedicated team of experts that continuously tests traffic captures for each new version of an application, ensure that the classification library is always up to date. With our expertise in network testing at Rohde&Schwarz, we even emulate radio cells to reveal patterns in application behavior, as applications may cause distinct patterns depending on the network characteristics. Consequently, when licensing DPI from ipoque, you adopt a traffic classification solution that is always reliable.

UP-TO-DATE SIGNATURE UPDATES ON A WEEKLY BASIS



Classification techniques

So how is the ipoque DPI library able to detect all sorts of applications, protocols and even service types in the vast streams of IP traffic? By using diverse and sophisticated classification techniques that cover the whole range of IP traffic, even if encrypted or obfuscated. These techniques include:

Behavioral analysis: Scanning for patterns in the communication behavior of an application, including absolute and relative packet sizes, per-flow data and packet rates, number of flows and new flow rate per application.

Statistical analysis: Calculating statistical indicators, including mean, median and variation of values collected as part of the behavioral analysis, and the entropy of a flow.

Deep learning (DL) algorithms: Our algorithms include convolutional neural networks (CNN), recurrent neural networks (RNN) and long short-term memory (LSTM). DL leverages huge data sets available from the network to identify features automatically in encrypted traffic, such as statistical, time-series and packet-level features. These features serve as input for machine learning algorithms.

Machine learning (ML) algorithms: Learning extremely complex patterns in encrypted traffic using k-nearest neighbors (k-NN) and decision tree learning, machines learn from a given set of examples to produce 'intelligent' outputs.

Tackling future-proof mobile security and connectivity with ML-powered DPI and encrypted traffic intelligence

With novel technologies, increased complexities and a significantly expanded threat surface that now spans space, air and ground networks, 6G calls for new levels of IP network traffic visibility and intelligence. Networking and cybersecurity vendors and network operators taking on the challenge of managing and securing 6G networks can leverage the ipoque next-generation deep packet inspection (DPI) technology to not only address the increasingly evasive network threats, but also gain real-time traffic awareness that can greatly augment their network capabilities. With our encrypted traffic intelligence which uses advanced machine learning and deep learning techniques, operators and vendors benefit from granular, real-time visibility across new and emerging 6G applications and services, even for traffic that's encrypted, obfuscated and anonymized.

Encrypted traffic intelligence (ETI)

Encryption has deep implications for the delivery of applications and network management. It protects critical applications, applications handling sensitive information and applications that are susceptible to interception via techniques such as sniffing. In addition, encryption provides companies and individuals with highly secure means of communication. While encryption keeps packets obscure and safe, it poses various visibility and monitoring challenges for network operators. They can no longer identify cyberattacks, or implement traffic management policies such as SLA-based routing, application-specific content caching and content-specific optimization, as the underlying protocols, applications and application attributes remain concealed.

The ipoque encrypted traffic intelligence (ETI) technology combines multiple ML algorithms, including k-nearest neighbors (k-NN) and decision tree learning, as well as multiple DL algorithms, including convolutional neural networks (CNN), recurrent neural networks (RNN) and long short-term memory (LSTM) networks (see above). These algorithms maximize the accuracy of traffic identification and classification results. With over 1000 features, including statistical, time-series and packet-level features, ipoque's ML/DL capabilities boast the ability and the capacity to learn extremely complex patterns and DL automatically identifies the features to be used in such algorithms.

ML and DL techniques combined with behavioral, statistical and heuristic analysis deliver fine-grained traffic analysis into not only encrypted traffic but also traffic delivered via VPNs and proxies as well as traffic obfuscated by randomization, tunneling, domain fronting and mimicry. Insights delivered by ETI enable the ipoque DPI product suite to support a wide range of networking solutions such as routers, network packet brokers, policy control engines, IP probes and security tools, including next-gen firewalls, DDoS prevention systems and cloud access security brokers. These features are unique to our DPI engine and guarantee a future-proof solution that no other DPI on the market can offer.

5.2 Selected add-ons, features and complementary products

Deploy additional modules and plug-ins, such as the tethering detection plug-in, the flow data exporter plug-in, or a complementary product to gain subscriber awareness in mobile networks such as our GTP correlation module R&S®GSRM, to suit your application or network needs.

Tethering detection

With tethering or custom hotspots, multiple network devices with distinct private IP addresses masquerade as a single public IP address. This technique can lead to misusing network resources. By combining multiple heuristic methods, for example leveraging the Google QUIC user agent, TTL and TCP timestamp, the tethering detection feature reliably detects devices behind network address translation (NAT). Gathered data appears in a well-defined data structure, including a NAT detection state, information on main devices, the number of detected devices and device groups. With this data, enterprise IT departments can prevent cyberattacks and operators can uncover tethering fraud or charge optional tethering plans.

Custom service classifier

The Custom Service Classifier (CSC) provides the possibility to define custom signatures for flow-based service classifications based on IPv4 (address and range), IPv6 (address and range), HTTP (host line), server name indication (SNI, for QUIC and SSL/TLS), User agent (UAID), DNS (common name) and HTTP2 (authority). Supported protocols include: DNS, HTTP, HTTP2, QUIC and SSL/TLS. With DNS correlation, IP addresses and ranges or QUIC client hello messages, CSC actually classifies flows with the very first packet. In other cases, CSC classifies flows at the first payload packet. Using CSC, admins and security officers can swiftly add new signatures, for example after a new threat has been uncovered. In enterprise networks, custom business applications can be defined for allowlisting.

Flow data exporter

The flow data exporter plug-in is an extension of the R&S®PACE 2 library to export flow-data records using the Internet Protocol Flow Information Export protocol (IPFIX). Throughout the lifetime of a flow, the plug-in collects all information elements (IE fields) in an internal flow-user-data structure. The plug-in forwards the flow information entry as an IPFIX flow record with configurable options such as Netflow v10 export or sFlow sample input and augments IPFIX flow records with market-leading DPI technology. For each flow entry, the flow data exporter adds only minimal overhead to the default amount of flow data used by R&S®PACE 2.

As IPFIX-enabled devices are deployed at significant positions in the network, it enables broad-based monitoring of hosts and network infrastructure devices with the resulting flow record data presenting an extensive set of connection summaries. IPFIX flow data can also be optimally utilized for threat detection use cases. As a result, IPFIX flow reporting is used to identify and remediate network attacks, such as denial of service (DoS), viruses and worms. Network administrators can utilize IPFIX-based flow reporting to deal with network performance problems with foresight and distinguish between challenges instigated by the underlying network and those triggered by higher-level applications and services.

First packet classification

The ipoque DPI engines can classify traffic from the first incoming packet in relation to corresponding DNS traffic. If the DNS cacher engine (DECA) successfully parses a DNS response, the referencing IP address is used to classify the following flows. DECA aims to improve the classification performance of R&S®vPACE and R&S®PACE 2. The DECA engine uses a single internal hash table to store and retrieve related data. By default, DECA parses responses from all DNS servers. Whitelisting allows admins to limit the responses to certain IPs or IP ranges. First packet classification enables for example security measures and realtime IP traffic management policies.

User and control plane correlation with R&S®GSRM and R&S®5GSRM

R&S®GSRM and R&S®5GSRM are standalone software modules to correlate control and user plane traffic within the core of mobile networks resolving data traffic per subscriber. This subscriber-level traffic visibility empowers network packet brokers and IP probe vendors to enhance their solutions with session-aware traffic aggregation, filtering and load balancing capabilities. Policy control, cybersecurity and IP traffic management solutions also benefit highly from mobile subscriber awareness, easily integrated as OEM software. R&S®GSRM and R&S®5GSRM are combinable with our DPI engines to enrich subscriber awareness with application awareness in mobile networking solutions.

5.3 The all-around solution: R&S®PACE 2

Architecture

R&S®PACE 2 combines classification and metadata extraction of IP traffic and the related scalar packet processing (SPP) components in a unified library. A single, C-based API and a command-line interface facilitate integration and require, in a basic version, only a few hundred lines of code.

Flexibility

R&S®PACE 2 can be embedded in any networking equipment and on any hardware. This applies also to solutions with hardware acceleration products (such as Napatech, Nvidia and Cavium) and packet frameworks such as DPDK and VPP. Also, our DPI engines boosts the functionality of open-source software (such as Suricata) and support open standards (such as IPFIX and JSON). Well-defined APIs with C public headers and integration examples and, above all, extensive support make ipoque the most flexible DPI partner on the market. Leading-edge performance and the many ways to optimize make R&S®PACE 2 compatible with setups that require ambitious traffic throughput. Through its configurable event system, R&S®PACE 2 outputs information such as classification and metadata extraction results, processing states and errors. For example, reducing the number of thrown events or defining groups of events helps to optimize the performance and to adapt results to specific use cases. External applications can process the event queue output by R&S®PACE 2 without other dependencies, allowing for high flexibility downstream.

> Growing protocol complexity is mastered with weekly signature updates that lay the foundation for the unrivalled reliability of R&S®PACE 2.

Scalability

R&S®PACE 2 is designed for high performance and scalability through multithreading and supports uniform (UMA) and non-uniform memory access (NUMA). Implementing processing units as threads or single processes with individual flow and endpoint tracking allows for almost linear scalability with the number of used CPUs. This approach scales even better with NUMA architectures because all flow and endpoint tracking tables can be stored in the local memory node. Distinct components, such as inter--process correlation (for setups with multiflow decoders) and an inherent symmetric multiprocessing capability, empower leading-edge classification and decoding results and almost linear scalability in multithreading setups.

Stages

The scalar pipeline architecture of R&S®PACE 2 divides processing of a single frame into subsequent stages. Each stage can be configured to adapt easily to different setups and requirements. Depending on the setup, the activation of a stage can increase the classification results. Our support team gladly helps to find the best, individual solution for each given setup. Throwing events in an early stage, packets can be dropped to enhance performance. Some stage components, such as packet reordering or defragmentation, can be enabled or disabled without code changes to optimize performance and classification results.

Stage 1: Decapsulation and defragmentation

Stage 1 is the packet preparation stage. This stage includes optional decapsulation and defragmentation functionalities. R&S®PACE 2 supports all commonly used tunnel protocol formats and all their possible combinations. Decapsulation covers all GTP versions and scenarios with multiple tunnels, such as IP in IP. IP defragmentation reassembles IP packets from layer 3 to layer 7. Transforming the IP flow is key for better classification results.

Stage 2: Packet reordering

Stage 2 buffers out-of-order packets until the missing packets arrive or up to a specific timeout. Optional packet reordering eliminates out-of-order sequences in a flow and can improve classification results.

Stage 3: Classification and basic metadata extraction

In stage 3, R&S®PACE 2 classifies protocols and applications, and extracts basic metadata for certain protocols using dissectors (for example HTTP, IP, TCP, H.264, SIP). Additionally, statistical metadata allow to determine key performance indicators (KPI) for network traffic. KPIs include jitter, packet loss, round-trip time, server response time, etc. For RTP traffic, statistical metadata help to measure performance in order to determine quality of service (QoS) and quality of experience (QoE) metrics in multiple use cases.

Stage 4: Advanced metadata extraction (optional)

In stage 4, R&S®PACE 2 decodes network traffic to provide advanced metadata in real time. This intelligence enables a wide array of use cases, such as application performance management (APM), network performance management (NPM), policy enforcement, network security and many others. Advanced metadata from IP traffic extraction includes but is not limited to:

- Identifiers: email sender/receiver addresses or any other ID that can be used to implement strong security rules
- Usage: HTTP, URL or client software information for intelligent traffic decisions and customer experience management
- DNS: Detecting tunneling and identifying anomalies in DNS transactions for security and policy enforcement use cases

Advanced decoding options suit the requirements of different use cases and help to optimize the performance with regard to the decoding results. Decoding options include:

- Decoding interrupted flows in lower-quality networks
- A frame buffer interface for subsequent UDP decoding of complete flows if the required classification and correlation results are delayed
- Reassembling missing TCP payload segments of not yet processed packets with configurable timeouts

Stage 5: Timeout handling

The timeout handling stage creates timeout events from decoders and frees unused resources, which helps to optimize memory usage. This stage can also support buffered packets from stage 2.

In addition, the configurable level of detail for the event output allows to adapt to individual requirements: For example, this can help to restrict decoding to HTTP payload and reconstruct all images or videos from internet sites.

5.4 Slim and fast: R&S®vPACE for VPP

Architecture

With the shift to cloud-based networking, new computing methods driven by the performance and scalability needs of such environments are rapidly being adopted. Vectoring-based frameworks such as FD.io's or DPDK Graph's VPP significantly improve speeds and latency by using a cloud-optimized methodology based on batch processing of IP packets and a locally stored vertex memory cache. A significantly improved average clocks-per-packet ratio results in up to three times the speed compared to scalar packet processing (SPP) DPI engines.

> By offering a native VPP implementation that delivers superior performance while ensuring computing efficiencies, R&S®vPACE delivers a differentiation that puts it above all other DPI solutions in the market.
>
> **Ali Shaikh, Chief Product Officer at Graphiant**

R&S®vPACE is a software library for classifying protocols and applications in a network packet stream and builds on the signature base of R&S®PACE 2. While R&S®PACE 2 is a scalar processor that processes each network packet separately, R&S®vPACE is a vector processor that can process entire vectors of network packets at once. R&S®vPACE supports any packet processing framework that processes vectors of network packets. In addition, the engine is optimized for the Vector Packet Processing (VPP) platform. By using VPP, R&S®vPACE combines the advancements in cloud computing with the reliability and accuracy of its market-leading DPI techniques to deliver unparalleled, real-time traffic insights for virtualized and cloud-native functions (VNF/CNF), as well as 5G user plane functions (UPF) hosted and managed in the cloud.

5.5 Feature synopsis

The ipoque DPI fast facts	R&S®PACE 2	R&S®vPACE
Layer 3 to 7 protocol detection	Yes	Yes
Application detection	Yes	Yes
Service type detection	Yes, audio, chat, file transfer etc.	Yes, audio, chat, file transfer etc.
Metadata extraction per packet (basic decoding)	Yes, TLS, HTTP, SIP, QUIC, OS (user agent), DNS packets	Yes, TLS, HTTP, SIP, QUIC, OS (user agent), DNS packets
Expandability	Add-ons through a plugin interface	Continuous feature additions
Custom service classifier	Yes	Yes
Flow data exporter	Yes, via plugin	Feature is on roadmap
Tethering detection	Yes, via plugin	Yes, inherent feature (without TCP timestamp)
High-performance optimized for vectoring/VPP	No	Up to 3x higher than SPP
Dynamic upgrades during runtime	Yes	Yes
First packet detection	Yes	Yes
Supports KVM, VMware, Hyper-V and Xen	Yes	Yes
Fastpath	Yes, bypasses all upcoming packets of a flow after the flow has been classified	Yes, bypasses all upcoming packets of a flow after the flow has been classified
Flow and subscriber tables (external tracking)	Yes, high-performance time-ordered hash table implementation	Yes, high-performance time-ordered hash table implementation
Memory management	Yes, with individual optimization options. Memory usage of latest release: 458 bytes per flow 681 bytes per subscriber	Yes, with individual optimization options. Memory usage of latest release: 384 bytes per flow 672 bytes per subscriber
Metadata dissectors	IP, TCP, RTP, AMR, H.263/4, RTCP, HTTP, MP3, MP4, ID3 dissectors	No
Metadata extraction across multiple TCP segments (full decoding)	Yes, including TCP reassembly	No
Tunnel decapsulation/ TCP reordering	Optional processing stages	Already available in VPP framework
Multiprocessing	Designed for symmetric multiprocessing systems and supports uniform (UMA) and non-uniform memory access (NUMA)	Designed for symmetric multiprocessing systems and supports uniform (UMA) and non-uniform memory access (NUMA)
SSL session ID tracker: Improve SSL classification results	Yes	Yes

6 SELECTED USE CASES POWERED BY DPI

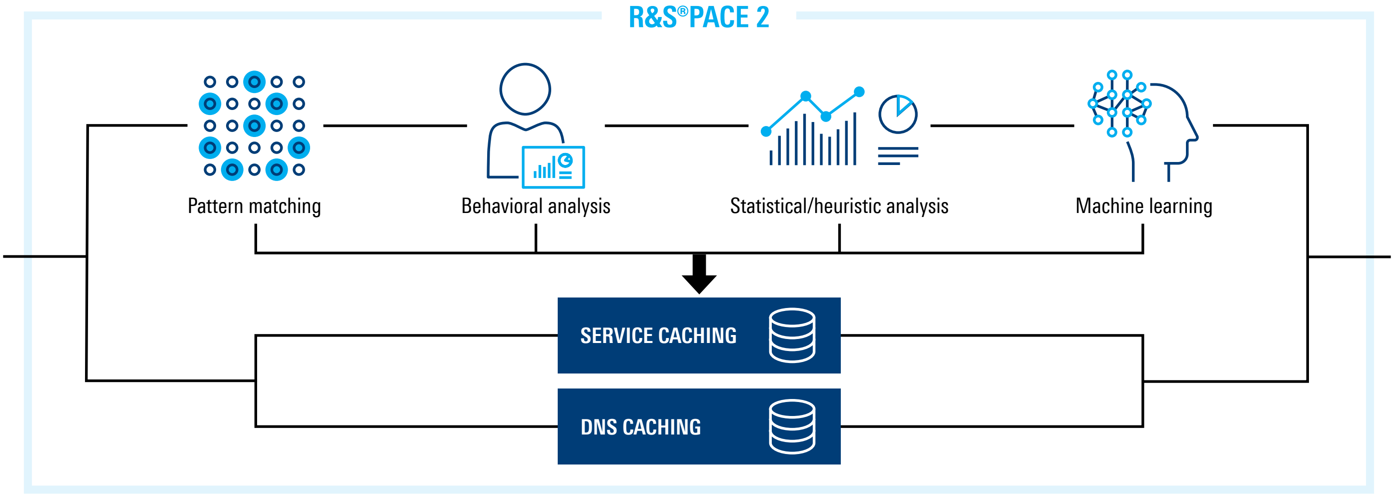
The ipoque DPI engines are critical for a more secure and connected world. They can be deployed in a variety of networking and cybersecurity solutions such as SD-WAN, SASE, firewalls, vEPC, IDS/IPS or wireless access points. The multitude of use cases and deployments reflects the adaptability, flexibility and scalability of the ipoque DPI portfolio. DPI-powered application awareness offers you the flexibility you need to handle many functionalities that require a focused analysis of specific applications and protocols, such as:

- Traffic analytics and management
- Application performance monitoring and control
- Application-aware routing
- Policy enforcement
- Application-level security
- Threat detection and malware protection
- Tiered pricing
- QoS and QoE optimization
- Content filtering and parental control
- … and many more

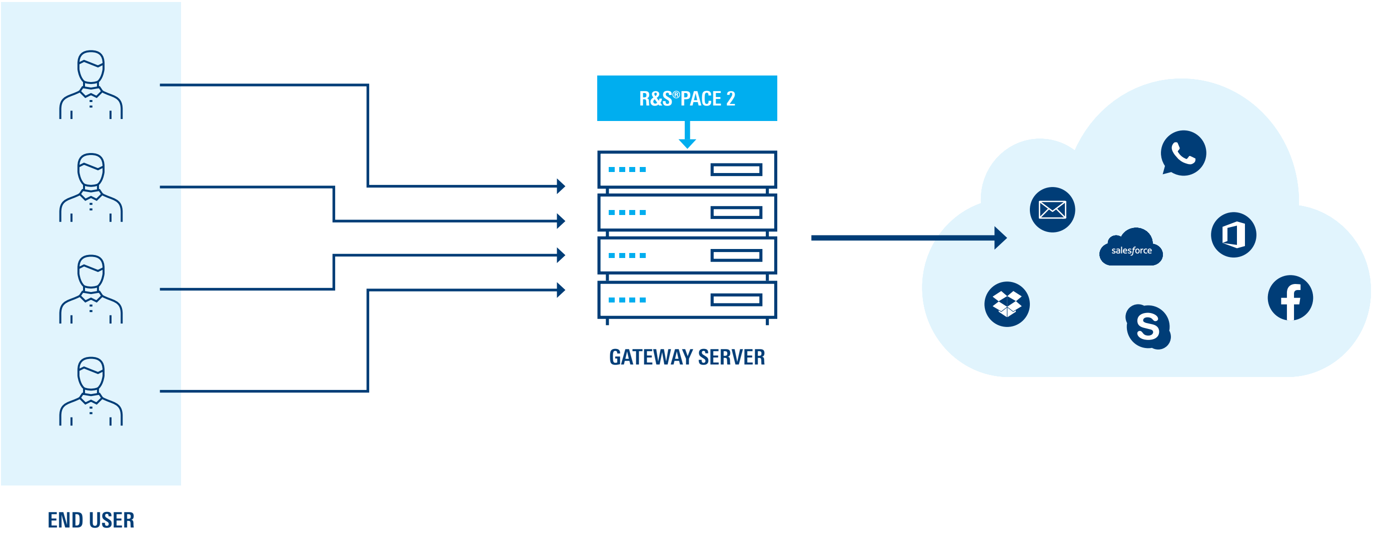
6.1 Software-defined wide area networks (SD-WAN)

As the new digital habits require enterprise networks to connect any user seamlessly to any application, enterprise SD-WANs are seeing an increasingly critical need to develop real-time application monitoring and network management capabilities. Without packet-level analytics, there will be delays in diagnosing application performance issues and bottlenecks in the network. To offer high-quality services, enterprises must rely on a comprehensive library of business applications and network protocols to identify and analyze the traffic running in their networks. The ipoque DPI engines enable application-specific performance metrics such as bandwidth consumption, TCP round-trip time (RTT), out-of-order and retransmission counters, etc. Their vast signature portfolio contains business applications (such as Microsoft Teams) and even differentiates between application service types (such as video calls within Microsoft Teams). First packet classification based on DNS caching and service caching enables instantaneous classification of applications and protocols. Vendors who perform real-time traffic steering and policy enforcement, rely on first packet classification to ensure that routing decisions and traffic policies are applied across all the packets of a flow in real time. Additionally, they can classify encrypted protocols and applications that are used increasingly in enterprise networks. This way, DPI advances SD-WAN solutions with deep traffic visibility right from the first packet on.

R&S®PACE 2 CACHING AND ENCRYPTED TRAFFIC INTELLIGENCE



DPI IN A FORWARD PROXY CASB



6.2 Cloud access security broker (CASB)

The cloud era has done away with the perimeter that used to set a clear boundary between a network and the outside world. Cloud deployment, encryption and obfuscation in addition to the increasing mobile workforce that remotely accesses corporate software are just some of the challenges that IT departments are facing. The "bring your own device" (BYOD) trend represents an attack surface with countless new attack vectors that cybercriminals can exploit to gain access to corporate networks. Also, there is an increase in cloud usage by shadow IT activities, spurred by employees' inherent need to leverage more effective means of processing their IT workload outside the limits set by their IT departments. In order to secure their IT perimeters, enterprises are deploying the cloud access security broker (CASB) software to secure the traffic flows between the cloud applications and the plethora of users including employees on site, data centers and remote workers. Advanced DPI offers a wide range of capabilities to enhance CASB's defenses. An advanced DPI engine like R&S®PACE 2 or R&S®vPACE masters distinguishing network traffic by application, protocol or service type plus metadata, revealing details about the traffic information, such as bandwidth consumption, speed, jitter and latency. Thus, CASB expands its reporting capacity. It can provide information not just about the applications and clouds being accessed, but also who is accessing them and how frequently they are being accessed. These insights, in turn, improve CASB's ability to detect threats and enforce security policies, for example to identify data loss or theft. Similarly, shadow IT activity can be managed by whitelisting/ blacklisting certain applications and cloud services, and data transfers can be authorized only when specific conditions are met.

Finally, the CASB/DPI combo can enable companies to maintain compliance in the industry they operate in, for example the Payment Card Industry Data Security Standard (PCI DSS) in the US and the General Data Protection Regulation (GDPR) in the EU. By combining the capabilities of both CASB and DPI, enterprises are sure to be safe as they move their work to the cloud.

> With advanced DPI, CASB expands its reporting capacity, providing information not just about the applications and clouds being accessed, but also who is accessing them and how frequently they are being accessed.

6.3 Security service edge (SSE)

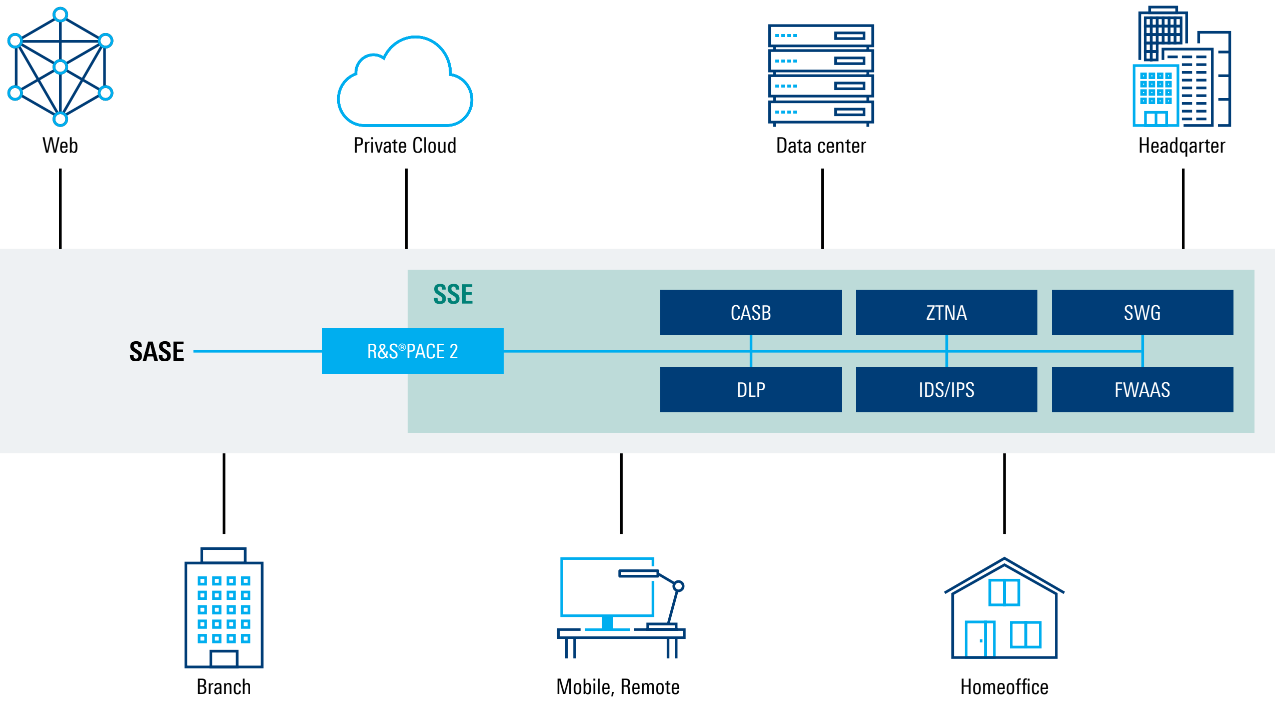
The pandemic gave rise to two major shifts across enterprise networks – the growth of the remote workforce and the increasing dependence on Cloud/SaaS. New models for managing dispersed users, devices and resources from a security point of view gave rise to security service edge (SSE). SSE comprises a suite of security services delivered from the cloud. Its essential components are the CASB (see above), the secure web gateway (SWG) and the zero-trust network access (ZTNA). Other services include firewall-as-a-service (FWaaS), DNS security, data loss protection (DLP) and web application and API protection-as-a-service (WAAPaaS). DPI equips SWGs with insights on the use of on-premises applications and resources. These insights assure that access controls are met based on application and service types. For ZTNA, real-time identification of applications goes a step further to enable the matching of access privileges with networks, clouds, servers, applications and files across any number of internal and external users. Advanced DPI technology also brings additional layers of traffic intelligence to support more granular, customized access control policies within the SSE. For example, provided metadata can be used to validate device IDs and source URLs for applications that only allow access from enterprise-managed devices and authorized network addresses. DPI-powered traffic analysis also supports access rules based on specific traffic attributes such as concurrent user sessions, multiple log-ins, number of requests per minute, type of services/content that is being engaged, file transfer sizes, time of day and location. Advanced DPI can help identify flows that are suspicious, anomalous or malicious in real time. This makes irregularities in application access and usage patterns immediately visible within the SSE ecosystem and helps alert CASBs and SWGs of potential hazards. Vendors can leverage ipoque advanced DPI technology to boost their value proposition by combining next-generation cloud-based security solutions with advanced application intelligence.

> DPI-powered traffic analysis supports access rules based on specific traffic attributes such as concurrent user sessions, multiple log-ins, number of requests per minute, type of services/content that is being engaged.

6.4 Secure access service edge (SASE)

Most enterprises have already transitioned to SD-WANs (see above) to do away with unnecessary backhauling of cloud and SaaS traffic to the data center. With ever more remote employees and IoT endpoints, such as smart meters or vehicle fleets, new challenges arise: an expanding number of corporate edge points on various mobile, IoT, WAN and edge computing clusters. Each of these edge points generates hundreds of authentication requests and

DPI IN SASE/SSE DEPLOYMENTS



thousands of user sessions while accessing corporate resources to complete tasks such as placing a purchase order, collaborating on a project file, entering a new customer record or, in an IoT context, delivering sensor log data. Secure access service edge (SASE) addresses both these requirements, merging network performance management (mostly SD-WAN solutions, see above) and network security (SSE, see above). The biggest selling point of SASE is the context awareness that it adds to network management. This is where DPI comes into play. The real-time network intelligence provided by DPI builds the context for the underlying traffic at any point of presence (PoP), enabling SASE to apply the relevant policy rules for both network performance and network security. This means that DPI provides the SASE platform with the input it requires to invoke the right mix of security functions from an array of available options. It also means that the SASE platform is able to enforce the right traffic management policies such as prioritization of low-latency applications, implementation of CDN, NAT and WAN optimization.

6.5 Virtualized evolved packet core (vEPC)

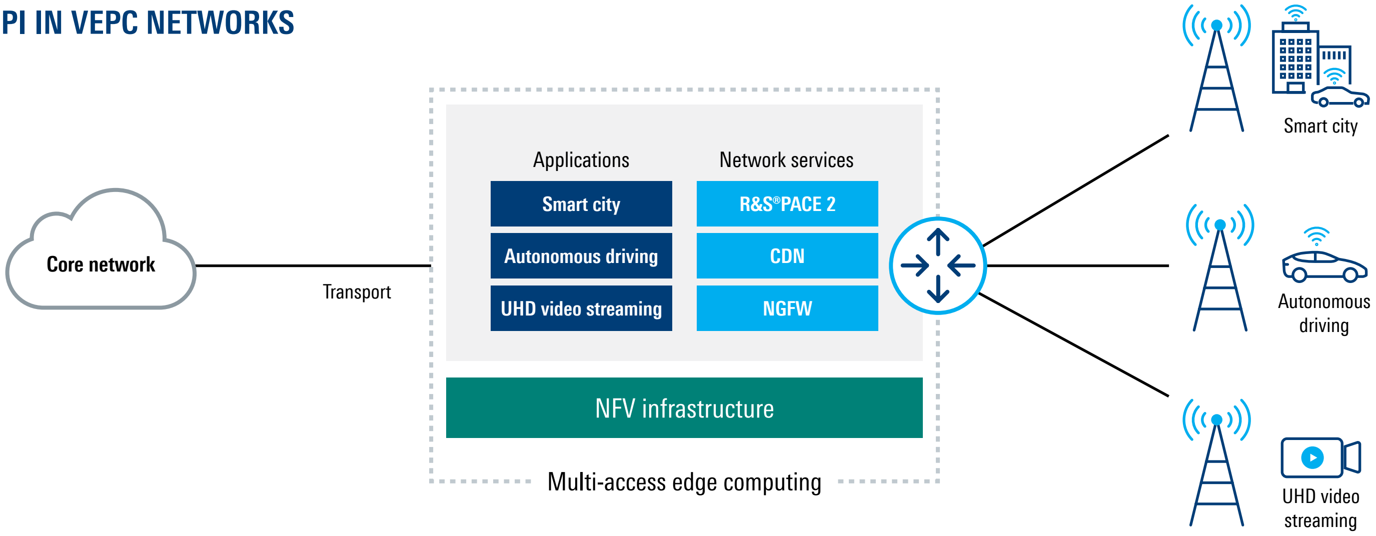
In 5G, the vEPC in mobile networks is a major breakthrough in network function virtualization (NFV). The development of multi-access edge computing (MEC) creates a powerful new network edge with user plane functions (UPF) involving packet routing and forwarding. UPF and MEC require real-time traffic visibility for the network as well as user analytics and application-specific information (for example, latency and type of content delivered), including packet inspection and QoS handling. By embedding the ipoque DPI technology in their solutions, vEPC vendors can empower their customers with traffic visibility in real time, even in cases of encryption, obfuscation or tethering. For MNOs, this visibility can unlock special benefits in countless business cases. Extensive coverage of VPNs and anonymizer signatures and detection of DNS tunneling allows vEPC vendors to prevent policy bypassing and zero-rating fraud. The broad signature portfolio, including machine-to-machine (M2M) and IoT protocols, allows fine-grained traffic management rules for each service class. Most importantly, despite ever-growing IP traffic rates, the ipoque DPI technology offers future-proof analytics capabilities in 5G architectures with high performance, linear scalability, and optimized support for DPDK and VPP.

> Despite ever-growing IP traffic rates, the ipoque DPI technology offers future-proof analytics capabilities in 5G architectures with high performance, linear scalability and optimized support for DPDK and VPP.

6.6 Wireless networking solutions (routers/access points/small cells)

With significant growth, particularly in bandwidth-consuming video traffic, vendors of wireless networking solutions such as wireless access points (WAP), wireless routers and small cells are unable to meet the requirements of QoS, QoE and performance without proper IP traffic analytics capabilities. When embedded into new and existing

DPI IN VEPC NETWORKS



wireless systems, DPI can help network professionals to dive deeper into the user activity data with intelligence about user-generated traffic, application usage, content communicated and anomalous patterns. With its broad application portfolio, the ipoque DPI library enables vendors to distinguish between specific applications (for example Hulu versus Salesforce) and then apply policies based on business or custom rules. This visibility is key to meet customer needs by improving device or network performance, end-user experience and enhancing network security measures. By classifying traffic down to service types (for example voice versus chat), the ipoque DPI engines can separate traffic into classes such as low-latency (voice), guaranteed-latency (web traffic), guaranteed-delivery (application traffic) and best-effort delivery applications (file sharing). Using these classifications, vendors can create application policies for thousands of applications by identifying bandwidth-heavy apps and analyzing usage trends over time. These insights enable their customers to prioritize, block or throttle applications or application groups and to define policies by device, user type or globally across the network. The low memory footprint and the platform-agnostic design of the ipoque DPI product suite allow integrations into legacy products and saving costs on hardware.

> With the ever-growing number of applications and constant application updates, it is a necessity to always have up-to-date traffic classification technology in order to provide fast and secure wireless connectivity. We are convinced that Rohde&Schwarz, who are very well known across our industry for high quality and professionalism, are the most reliable OEM DPI partner to fulfill our requirements.
>
> **Matt Donnelly, CSMO at Keenetic**

6.7 Service assurance and analytics

Gaining business intelligence from network and subscriber data is a fast-growing area as operators recognize they can unlock value by better understanding application usage and subscriber behavior. Marketing departments can use this information for targeted advertising and context marketing. Furthermore, with granular information about network bottlenecks and bandwidth demands, network planning and optimization departments can plan investments better and improve QoE per application. The ipoque DPI engines offer analytics vendors high performance and scalability for real-time analytics: for example an accurate identification of used applications, combined with a rich set of data such as mobile cell identification, traffic patterns or service types of OTT applications (chat vs. audio vs. video). These metrics reveal who the power users are and what the top applications are per subscriber segment or geographic location. In a typical integration, this application usage data is linked directly to third-party analytics or big-data systems with the data serialization option. Also, licensing DPI from ipoque supports analytics vendors with enhanced reporting features and fast time to market, harnessing weekly signature updates and a broad signature portfolio covering different regions, verticals and metrics.

ETI Use cases

ETI is pivotal to many use cases involving encrypted traffic, e.g. OTT video apps such as Netflix or Amazon Prime. Traffic from these platforms is encrypted which limits the visibility of traditional DPI methods to ascertain whether a user is downloading a video or streaming a movie on demand. With ETI, operators can identify the underlying service, allowing them to apply the right policy control and traffic steering rules. They can prioritize video streaming over download packets by delivering the former via priority routes. They can also implement compression for an on-demand stream to avoid content buffering, especially during congestion where speeds are compromised.

This is similar in the case of services from Apple, Google or Meta. Applications by Meta, such as Facebook, Facebook Messenger or Facebook Video, are encrypted over TLS 1.3, making it virtually impossible for network operators to tell these services apart. With ETI, operators can classify each of these applications and their services in real time, allowing the implementation of differentiated policies. For example, video content from Facebook Video that is accessed multiple times may be cached, while packets from a Messenger application can be run through additional filtering to identify security threats hidden in file attachments.

7 EMBEDDING DPI IN YOUR SOLUTION

7.1 Requirements

With its flexible and platform-agnostic design, R&S®PACE 2 can be integrated in solutions from small routers (ARM CPU) up to large carrier networks (multicore x86). Classification works in a source-agnostic way, requiring nothing but a data area in the memory with a valid IP packet (valid layer 2 header). This allows for any format (PCAP, text, network interface card memory, etc.) from any source (IP, Ethernet, etc.). R&S®vPACE requires a VPP framework.

7.2 Integration process

The elaborated integration process includes a proof-of-concept (PoC) phase that enables customers to test our DPI technology and validate its benefits for a given solution, even remotely. To facilitate PoCs, we offer a framework for demo tools apt for analyzing or health monitoring and logging. Integration examples and an internal tracking component allow testing the integration without much effort. Later on, integration examples can be used as a basis for customized solutions.

Qualification

In a first call, optionally with technical consultants on the line, we figure out whether our DPI engines can be installed on the customer's equipment and whether they can fulfill the expectations for the given business case.

Proof of Concept

After qualification, an individual account is created to download the demo version. Demo software packages include a variety of integration examples that help to quickly test a selection of features and options on PCAP files. At this stage, customers can create help tickets and ask questions in a dedicated PoC portal. These will be taken care of by highly specialized support engineers. Help options include on-site support, remote help and phone consulting. Optionally, we support customers with integrating a demo version in their solution or a comparable system. With a single, C-based API and a command-line interface, all R&S®PACE 2 stages can be configured. In simple setups, our DPI engines can be integrated remotely in a couple of hours, with only a few hundred lines of code.

After signing a licensing contract, the full version of our DPI engines can be downloaded swiftly from the customer portal. From this moment on, weekly signature releases keep the licensed software up to date.

Custom implementations

In case of special setups or requirements, our support engineers can help customize our DPI engines with custom implementations.

8. SERVICE AND SUPPORT

Sustainable technical support and service go far beyond basic troubleshooting. With continuous optimization and maintenance, licensing our DPI technology ensures a smooth operation with calculable operating costs through the entire product lifecycle. Adaptable service level agreements (SLAs) with adjustable response times provide technical expertise tailored to customer's requirements.

Online ticket tracking

Customers receive dedicated access credentials to an online ticket tracking service to:

- Open and manage an unlimited number of troubleshooting requests
- Handle priority levels
- Keep up to date with the status of tickets
- Share documents and attachments

Monthly support performance report

With an overview of all pending requests, this report helps customers identify bottlenecks and understand the fulfillment rate of the agreed service level.

Customer portal: Releases and maintenance

Maintenance engineers work continuously on the weekly updates that include classification algorithms for new protocols and applications and updates for existing signatures. We roll out software updates with new features several times a year. In addition, we distribute maintenance releases that solve reported issues whenever necessary. Customers can download the weekly releases swiftly from the customer portal.

Support channels

Depending on the SLA, we provide different support channels:

- Web: Customer Portal and ticket tracking system
- Email: Customer Support email address
- Phone: Customer Support hotline

Remote consulting and assistance

Consulting engineers can coordinate and support integration into customer solutions remotely. Remote assistance sessions are an option to solve reported problems. Remote technical consulting can support product planning and evaluation.

Proactive communication and alerts

As soon as we become aware of issues that affect customers’ solutions, our customer support team gets in touch right away before things get critical.

Dedicated support account manager

Customers are assigned a dedicated support account manager who is responsible for their service requests and is the central point of contact for any request.

On-site support

Support engineers visit customers for

- System performance optimization
- Hands-on trainings to test the functionality under supervision, for example with new features
- Integration support

Individual consulting and feature request

Our consulting engineers offer additional DPI know-how for our customers to meet technology challenges. Customers can influence our product roadmap, for example by requesting new application and protocol classifications for the library. In regular meetings, the account managers present product roadmap updates, assess further requirements for customers' solutions and keep up with their business strategy.

ipoque

ipoque, a Rohde & Schwarz company, is a global leader in the world of network analytics software. We leverage our deep domain expertise to create customized software solutions that empower our customers to transform data into intelligence. As a subsidiary of Rohde & Schwarz, we take advantage of potential synergies.

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, Germany
Info: + 49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 3608.7309.62 | Version 02.01 | August 2024
Solution Guide | Next-generation deep packet inspection
Data without tolerance limits is not binding | Subject to change