BUILD OR BUY DPI?

Why you benefit substantially from OEM deep packet
inspection software by ipoque, a Rohde & Schwarz company

ROHDE & SCHWARZ

Make ideas real

TABLE OF CONTENT

DPI IS NOT A
ONE-TIME PROJECT

Whether it's critical traffic steering in software-defined networks, policy control at wireless access points or protecting IoT devices from cyberattacks – many solutions require application awareness in IP traffic. Deep packet inspection (DPI) is widely known as a key technology for application and protocol classification. DPI technology is of little use though if not reliable and accurate at any time. A sustainable solution must master frequent traffic signature changes, growing encryption and obfuscation rates. That's why it's so important to choose the right DPI solution.

In this situation, you have basically two options: either build in-house DPI libraries or license software from a DPI specialist. Developing an IP classification in-house is not a one-time project but constantly requires resources to maintain and update the traffic signatures. Achieving this target is challenging, especially when you consider the level of performance, accuracy and reliability expected from network and security solutions. Even more in the near future when billions of "things" will connect to the internet.

Licensing next-generation DPI software from ipoque, vendors gain a reliable partner to master the challenges of encryption, growing traffic rates and disruptive technologies.
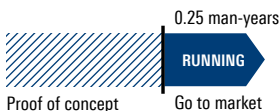
THE VALUE OF LICENSING DPI SOFTWARE

Accelerate time to market

Sourcing DPI software from an OEM solution provider grants immediate access to an up-to-date signature library with thousands of applications and protocols, out of the box. This enables you to meet aggressive product cycles whilst your software developers can maintain the required focus upon your core technology. As a guide, it can take an in-house DPI team about one man-year to build a basic DPI solution, with the ever-present risk of leaving a higher percentage of network traffic unclassified. To reach a number of signatures, as in commercial 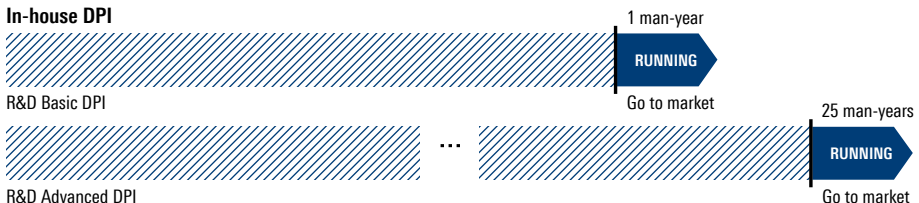DPI solutions, takes far longer. An advanced DPI engine can easily require more than 25 man-years. Licensed OEM DPI software, on the other hand, is easy and fast to integrate. Ideally, it comes with on-site integration assistance by technical consultants, who contribute years of professional experience. With a profound understanding of potential errors, integration short cuts and optimization counseling, they minimize the risk of developing a highly complex technology in-house. So keep focus – and don't let your developers get distracted by the significant challenge of building their own DPI from scratch.

COMMERCIAL DPI ENSURES OPTIMAL TIME TO MARKET

R&S®PACE 2 (commercial DPI)

0.25 man-years

RUNNING

Proof of concept   Go to market

In-house DPI

1 man-year

RUNNING

R&D Basic DPI   Go to market

25 man-years

RUNNING

...

R&D Advanced DPI   Go to market

Get predictable costs

Building DPI software in-house may appear more profitable, but vendors are facing hidden operational costs, especially with the growing complexity of classifying applications. In-house DPI software libraries face the costly challenge of constantly updating signatures for protocols because these change regularly and without prior notice (for example new versions and new obfuscation techniques). In addition to the costs that derive from the need to constantly check for potential changes, there are further costs in setting up various required tests to simulate real network scenarios along with frequent QA testing. While some basic protocols are relatively stable and, therefore, easy to manage, a growing number of proprietary and fast-evolving protocols such as social networking, video streaming and virtual private network (VPN) applications are adding further complexity. Maintaining a DPI engine constantly requires development resources for implementation, testing and validation. Besides the obvious costs for implementing and maintaining a DPI library, opportunity costs should also be considered.

Is a DPI software the most lucrative option to invest your R&D resources in? What is the return on investment (ROI) when compared to acquiring an OEM DPI solution? To answer these questions, vendors should consider whether DPI technology forms the core of their business model, where the expected returns may justify a "make" decision, or if the costs of in-house development and the supplier efficiency of a professional solution are in favor of a "buy" decision.

COMMERCIAL DPI REDUCES DEVELOPMENT COSTS

Legend:
- Fix cost
- Running cost
- Opportunity cost

Categories: In-house, Open source, R&S®PACE 2 (commercial DPI)
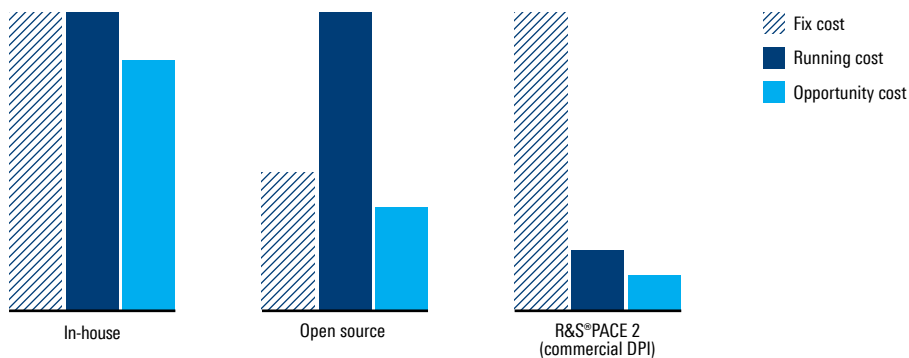
Ensure reliability and accuracy

A DPI engine is only as accurate as its update policy allows it to be. DPI software companies have experts living and breathing DPI with a dedicated team adding new application signatures on a weekly basis, ensuring that a high percentage of network traffic can be reliably classified. This is crucial for vendors of security and network management solutions who need to make accurate decisions on reliably classified traffic.

Signature updates should be provided on a timely and frequent basis to ensure a high level of accurate application identification. Even small changes to protocols and applications can lead to problems with classification. Since the details for most protocols and application changes are not publicly announced, this update process requires a sophisticated automated testing infrastructure that continuously checks the accuracy of all classification signatures. When detecting changes in the behavior of protocols and applications that influence classification accuracy, the testing infrastructure initializes proper actions. As a result of ongoing testing, regular updates and improvements ensure that all applications are detected at any time. 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.

Moreover, a solid DPI software engine should be able to update hot signatures without interrupting or stopping the system. Commercial OEM DPI software provides smooth signature updates during runtime. This way, the system saves time and gains reliability by not losing track of any flow.

Another key factor in choosing to source DPI is that the software is often deployed globally and regularly enhanced with the newest applications based on continuous feedback from multiple customers and regions. In particular, commercial DPI vendors are able to receive feedback on localized versions of major applications and protocols through their global presence. This makes for a much better detection rate than in-house DPI.

Next-generation DPI engines such as the flexible all-around solution R&S®PACE 2 or the cloud-native vector packet processing (VPP) DPI engine R&S®vPACE by Rohde & Schwarz combine these requirements and boost your solution with market-leading DPI technology that is always up to date.

Outsource complexity

As most of the internet traffic is now encrypted, a reliable DPI software engine needs a tool kit of advanced techniques to classify traffic and, for example, determine if an encrypted WhatsApp session is a voice call, a text message, a sent video or the like, with a very high accuracy.

This requires traditional DPI techniques such as pattern matching to be supplemented by heuristic and statistical approaches as well as machine learning and complex algorithms developed by a team of engineers. These techniques can analyze many flow dimensions as well as the flow duration, the transfer size, group attributes to parse types of traffic, and identify protocols. It's also possible to indicate the quality of experience (QoE) of videos using buffer counts, buffer stalls, pauses, bitrate changes and so on. A key question is whether your in-house DPI tools and analytics are intelligent enough to handle future encrypted networks.

With a team of more than 160 in-house developers and extensive partnerships with leading universities, Rohde & Schwarz pushes the boundaries of research in big data, AI and machine learning.

Access professional expertise

When buying commercial OEM DPI software, it includes a service level agreement (SLA), performance reporting, a trouble ticketing system, an engineer on site, phone support and other benefits tailored to your needs. In addition, the SLA and performance reporting assure a defined amount of stability, reliability and the desired performance level for the licensed software.

With Rohde & Schwarz, DPI engineers are directly working on site with your technical staff on the integration of the DPI software into your product or application. This two-way communication provides access to experts with years of DPI experience, valuable consulting to optimize system utilization and performance, up-to-date information on the latest software enhancements and the ability to request new features.

"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

ROHDE & SCHWARZ ENSURES UP-TO-DATE SIGNATURES

GOAL

The goal of DPI maintenance is to reduce the cycle time of signature updates as much as possible. R&S®PACE 2 and R&S®vPACE signature updates are usually done in weekly cycles.

COSTS

Besides the initial R&D costs for developing a DPI engine, the main cost factor is maintaining the DPI. An extensive testing setup is needed to ensure that application and protocol changes are detected early in order to provide signature updates.

UP-TO-DATE SIGNATURE
After the signature update has been released, customers can benefit from the improved signatures within their applications.

MONITORING CHANGES
Rohde & Schwarz uses highly automated testing frameworks and testing setups to ensure that any application change is detected as early as possible.

CHANGE DETECTED
If a change in an application or protocol behavior is detected, traces are recorded and provided to R&D in order to extend R&S®PACE 2 signatures.

SIGNATURE ADOPTED
The affected signature is complemented by additional detection patterns in order to cover the new behavior or application functionality.

SIGNATURE VERIFIED
Before the signature update is released, its accuracy is validated against live traffic and our extensive offline traffic database.

ROLLOUT
After quality assurance has been done, the signature update is provided to customers as part of one of our weekly releases.

OPEN SOURCE DPI— A FREE ALTERNATIVE?

Vendors may consider open source DPI with the idea that it's free to use. However, there are other important considerations when looking at the pros and cons of using open source DPI. Open source software does not end up being "free" because it still requires in-house developers to learn about the software and, more importantly, to customize it. In addition, it frequently requires working with a third-party vendor to manage and add new features.

Open source DPI comes with the following benefits and barriers:

Benefits
- ▶ Free software to save on license fees
- ▶ Customized software to contribute to code
- ▶ Easy to integrate with other platforms and systems
- ▶ Improved time to market vs. in-house DPI
- ▶ No vendor lock-in
- ▶ For free, but you're on your own!

Barriers
- ▶ Newness of open source DPI technology and ongoing staff costs to maintain, operate and update
- ▶ Requires ongoing in-house expertise and skills to manage open source software and develop new protocol or application classifications
- ▶ Commercial DPI software also comes with flexible APIs for easy integration
- ▶ Reliability and performance risks: lower levels of detection, lower performance/throughput
- ▶ Limited additional features besides pure classification
- ▶ Reduced number of application signatures/coverage: typically, open source DPI has 250 signatures, whereas there are over 3000 signatures in commercial DPI software
- ▶ No vendor support or professional services, no SLAs or performance guarantees
- ▶ There is always a risk of the open source software or project to disappear in the future due to a lack of support

"With the 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 well known across our industry for high quality and professionalism, are the most reliable DPI partner to fulfill our requirements."

Matt Donnelly, CSMO, Keenetic

NEXT-GENERATION DPI

ipoque, a Rohde&Schwarz company, is a leading vendor of OEM DPI software. Our next-generation DPI portfolio contains R&S®PACE 2, a flexible all-around solution, and R&S®vPACE, a slim and fast vector packet processing (VPP) based DPI engine for virtual and cloud-native network functions. Our DPI engines classify thousand of protocols, applications and even application attributes (such as audio/video). With weekly signature updates that can be updated smoothly during runtime our DPI libraries are always up to date.

Leveraging research partnerships with leading universities, our DPI technology is the only one on the market mastering encryption and obfuscation with machine learning and deep learning capabilities.

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 boost 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.

Additional options, add-ons and features extend the capabilities of our DPI technology, such as first packet classification, tethering detection and many more. In close cooperation with our customers and partners who are industry-leading manufacturers of networking, telco and cybersecurity solutions, we continuously add new features to our roadmap.

Key benefits of licensing ipoque DPI technology
- ▶ The only DPI engine on the market mastering encryption and obfuscation methods such as TLS 1.3, eSNI, D-o-x, etc.
- ▶ Most flexible DPI partner: well-defined APIs and extensive support
- ▶ Always up to date: weekly signature updates
- ▶ High traffic detection accuracy and reliability with virtually no false positives
- ▶ On-site application engineering and performance optimization consulting
- ▶ High perfromance with a super small memory footprint
- ▶ First packet classification, tethering detection, IPFIX flow data export and many other additional features

COMPARISON OF TECHNICAL FEATURES AND SUPPORT

Criteria	R&S®PACE 2 (commercial DPI)	Open source DPI engine	Wireshark Protocol Analyzer (non-DPI)	In-house developed DPI
Classification coverage	● ● ●	● ●	● ●	●
Performance	● ● ●	●	●	●
Additional features (e.g. decoders, dissectors)	● ● ●	●	● ●	●
Frequency of signature updates	● ● ●	● ●	●	● ●
Memory footprint	● ● ●	●	●	●
Accuracy	● ● ●	● ●	●	● ●
Technical support & available SLAs	● ● ●	●	●	● ● ●

Functional and non-functional requirements are essential for a determination of the return on investment (ROI) and the actual product value.

Classification coverage: This refers to the absolute number of supported application and protocol signatures. This number directly influences the share of the analyzed traffic that can actually get classified.

Performance: This refers to the amount of needed computing resources (e.g. processing power, memory accesses) needed to perform the DPI tasks of classification and metadata extraction.

Additional features: This refers to the availability of functionality besides classical DPI features of classification and metadata extraction. Examples are protocol decoders, dissectors, operating system detection, extraction of voice over IP (VoIP) performance KPIs and many more.

Signature updates: A growing number of new and updated protocols and applications gets introduced into the network daily. DPI vendors must continuously invest in redeveloping their software to handle the latest protocol versions.

Memory footprint: This refers to the amount of memory needed to perform the DPI tasks of classification and metadata extraction.

Accuracy: There are two requirements:
1. A DPI result must be correct (e.g. if the DPI indicates that an IP connection is Facebook, but actually it's Twitter).
2. A DPI result must not miss some IP connections or parts thereof (e.g. some connections that should be classified as Facebook).

Technical support & SLAs: This refers to the availability of dedicated product support and service with guaranteed service level agreements.

BUILD OR BUY DPI

CHALLENGES OF BUILDING

Development of a software DPI
engine is difficult and costly

Besides initial R&D, DPI software
needs ongoing investment in
signature plug-ins and maintenance

Ensuring accuracy and
dealing with encrypted apps
require extra resources

BENEFITS OF BUYING

Licensing OEM DPI software from
Rohde & Schwarz
is simple and cost-effective

Licensing fees are a small fraction
of necessary R&D

Rohde & Schwarz has an in-house
team of experts dedicated to quality
assurance and ongoing monitoring of
the latest apps

WHY ROHDE & SCHWARZ DPI

ipoque, a Rohde & Schwarz company, is recognized globally as a leading developer of DPI software. We have more than 10 years of expertise in optimizing the performance of network equipment and IT security solutions with embedded DPI. With customers in over 60 countries worldwide in the areas of network analytics, traffic management and network security, our objective is customer satisfaction throughout the entire product lifecycle.

Value to our customers
► We understand the needs of vendors that are integrating DPI as a key enabling feature of core solutions.
► We have years of expertise in optimizing the performance of systems with embedded DPI software.
► Solution vendors need a reliable embedded DPI software for enabling features and the ability to reliably detect thousands of applications. A trusted and stable DPI software partner is key for vendors that are launching new products and developing new business and customer relationships.
► Complement your own signatures with Rohde & Schwarz signatures, so your developers can focus on their core product while we handle the complexity of constantly evolving applications and protocols.

Benefits
► We focus exclusively on embedded DPI for network equipment and software products.
► We are a reliable long-term partner for DPI software — our own security products rely on our DPI.
► We make our application signature library available to customers for use and customization.

"As an early adopter of the technology by Rohde & Schwarz, we managed to release one of the first next-generation firewalls almost 10 years ago. Beyond award-winning products, we are committed to providing excellent support to our customers and partners. This is only possible if our technology partners, also, live up to the same high expectations. Throughout the past 10 years we have always felt very well looked after by Rohde & Schwarz who have always been highly committed to providing a timely solution to any problems."

Dr. Klaus M. Gheri, VP & GM Network Security, Barracuda Networks

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.

3607.7286.62

3607.7286.62 03.01 PDP 1 en