DEEP PACKET INSPECTION

BUILD OR BUY DPI?

Why you should consider investing in OEM software from a deep packet inspection specialist

ROHDE&SCHWARZ

Make ideas real

MAKING THE RIGHT DECISION— BUILD OR BUY DPI?

When your solution needs deep packet inspection (DPI) application awareness as a key enabling feature, highly reliable and accurate identification of network traffic and applications—in real time—is an expected requirement. Whether it's for software-defined networks to enable policy control and critical traffic steering or to protect corporate networks, IoT devices and cloud platforms from malicious attacks, it's crucial to choose the right DPI solution.

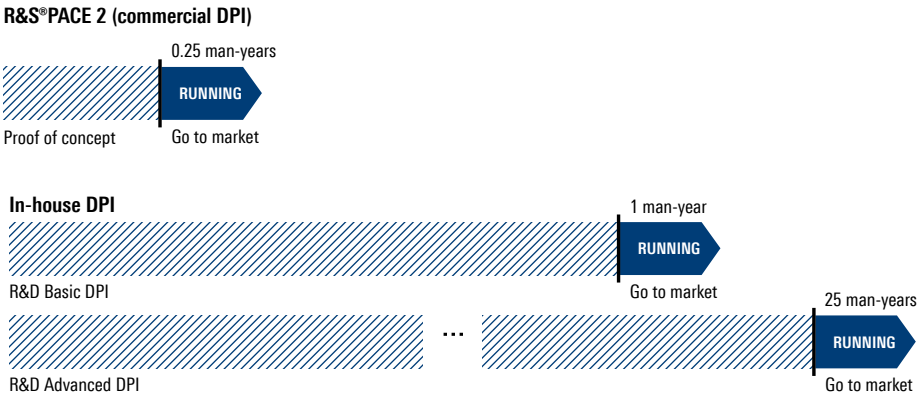
Vendors looking at the business case can decide to build in-house DPI libraries or to license software from a DPI specialist. Developing an IP classification in-house constantly requires resources to both maintain and regularly update the protocol and application signatures. Achieving this target is both challenging and crucial, especially when you consider the level of performance, accuracy and reliability expected from network and security solutions, today and even more in the future when billions of "things" will connect to the internet.

THE VALUE OF LICENSING DPI SOFTWARE

ACCELERATE TIME TO MARKET

Sourcing DPI software from an OEM solution provider gives immediate access to an up-to-date library with over 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 and not be distracted by the labor-intensive practice of building an in-house DPI. As a guide, it can take an in-house DPI team about one man-year to build a basic DPI solution. It takes significantly longer to reach such a number of signatures, while there is always the potential risk of leaving a higher percentage of network traffic unclassified. An advanced DPI engine which is built in-house may require more than 25 man-years. Furthermore, licensed OEM DPI software is easy and fast to integrate and comes with on-site integration assistance by a technical consultant. Considering that technical consultants bring years of professional experience, they have an understanding of potential errors and risks, integration short cuts and the knowledge of multiple differing integrations, too.

COMMERCIAL DPI ENSURES OPTIMAL TIME TO MARKET



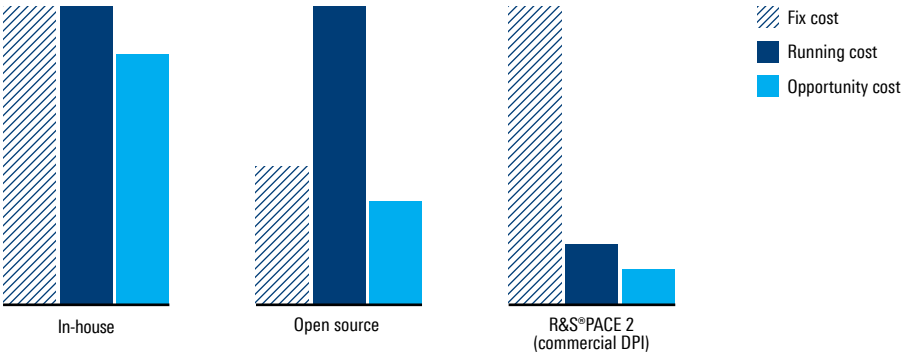
GET PREDICTABLE COSTS

Building DPI software in-house may appear more profitable, but vendors also have to consider 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 (e.g. new versions and new obfuscation techniques). In addition to the costs for regular signature updates that are needed to constantly check for potential changes, there are further costs in setting up various required tests to simulate real network scenarios along with the 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 requires ongoing internal experts and development resources for implementation, testing and validation to keep signatures up to date. Besides the obvious costs for implementing and maintaining a DPI, 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 a 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



ENSURE RELIABILITY AND ACCURACY

A DPI engine is only as good as its creators design it to be. In particular, DPI software needs to be constantly updated, as new applications appear all the time. 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 who need to make accurate decisions on reliably classified traffic.

Signature updates should be provided in 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 infrastructure initializes proper actions. As a result of ongoing performance and reliability testing, regular improvements can be made to the software to ensure that all applications are detected.

Moreover, a solid DPI software engine should be able to update hot signatures without interrupting or stopping the system. Commercial OEM DPI software such as R&S®PACE 2 ensures a continuously running signature update system that saves time by not losing track of any flows that were already classified.

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.

> "We decided to license from Rohde&Schwarz as we recognized their technical leadership in deep packet inspection and behavioral analysis. We are pleased that Rohde&Schwarz was able to provide a specific decoding functionality allowing us to deliver a better service for the customers we protect."
>
> Sharon Uziel, VP Product and Business Development, CELARE

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.

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. That way, 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. In addition, the SLA and performance reporting assure a defined amount of stability, reliability and the desired performance level for the licensed software.

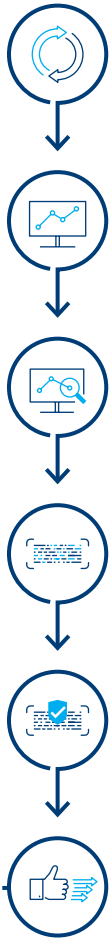
ROHDE&SCHWARZ ENSURES UP-TO-DATE SIGNATURES

GOAL

The goal of DPI maintenance is to reduce the cycle time of signature updates as much as possible. R&S®PACE 2 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—
BENEFITS VS. BARRIERS

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 the software. 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

"We are extremely satisfied with the support and response we have received from the Rohde&Schwarz team. Their strong understanding of our needs and prompt, expert service delivery exceeded our expectations. Licensing DPI by Rohde&Schwarz definitely helped us to concentrate on our core business."

Josef Waclaw, CEO, Infotecs

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: Growing number of new and updated protocols and applications gets daily introduced into the network. 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.

MAKE OR BUY DPI

CHALLENGES OF MAKING

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

Rohde&Schwarz 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.

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 3607.7286.62 | Version 02.00 | May 2020

3607.7286.62
3607.7286.62.02.00.PDP 1.en