DEEP PACKET INSPECTION

A CRUCIAL ENABLER FOR NETWORK AWARENESS

ROHDE&SCHWARZ

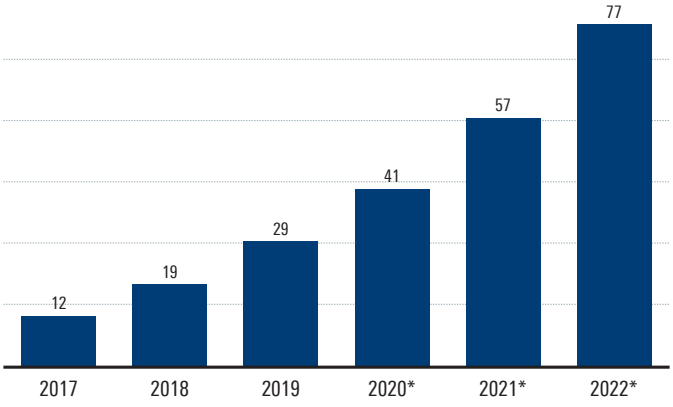
TABLE OF CONTENT

1. INTRODUCTION

Deep packet inspection (DPI) technology has been an essential component of information technology (IT) networks for well over two decades. The volume of Internet traffic and – more importantly – the rate of encrypted traffic has exponentially increased over the years. At the same time, DPI software has evolved into a powerful tool to meet new network challenges and plays a vital role in today's Internet and network infrastructure. With expanding technologies such as cloud computing, 5G or the Internet of things (IoT), DPI is becoming even more important for networks. This white paper aims to provide a better understanding of this powerful technology, focusing on current challenges in the fields of network analytics, traffic management and network security.

Analysts estimate the current number of mobile Internet users to be around 3.3 billion globally, with an expected steady growth to around 5 billion by 2025[1]. The growth of cell phone users alone will not challenge the industry – the amount of data used on these smartphones will. During the past five years, big data requirements have increased with the use of bandwidth-demanding applications and activities (see graphic below). These originate from general consumer and commercial business applications, including video and web conferencing, cloud storage, virtual desktops, video chat, video streaming, music streaming, gaming and social media. Increased data requirements will challenge IT professionals significantly.

Global mobile data traffic from 2017 to 2022 (in exabytes per month)



* Forecast
Source: Cisco VNI mobile 2019

Many enterprises use cloud computing technology to cut costs and reduce investments in physical infrastructure like storage hardware. Guaranteeing the performance of business-critical applications on wide area networks (WAN) and ensuring bandwidth efficiency is becoming more and more difficult. Software defined WAN (SD-WAN) solutions need to prioritize key business traffic while avoiding network congestions. DPI empowers SD-WAN vendors to add application awareness to their solutions in order to block, prioritize or throttle IP traffic caused by certain apps. As a consequence of the IoT revolution, a myriad of additional non-cellphone connected devices, among them smart cars, smart homes and smart cities, will challenge the bandwidth of networks. These IoT devices will introduce new requirements for operators, placing new demands on how to maintain security and integrity of their networks. Thus, networks will need to be managed more efficiently. Smart traffic management with strong security policies can be built on a solid data foundation with application metadata provided by DPI.

5G networks will soon support big data and IoT applications. The move to 5G speeds is placing a high priority on the most efficient network routing. Managing bandwidth efficiently while optimizing the quality of experience (QoE) for users will be a challenge. DPI-powered traffic management with real-time dynamic routing decisions reduces congestions while optimizing QoE.

Today, many apps are encrypting content and user data, raising questions about the future of DPI. With as many as one out of four protocols and applications now being encrypted, it has become increasingly difficult to identify them. As we will see later on, with the evolution of encryption techniques, DPI techniques keep advancing as well.

According to Global Industry Analysts Inc.[2], the global market for deep packet inspection is projected to reach USD 3.4 billion by 2024. This growth is fueled by increasing wireless bandwidth demand, the need for load balancing and network monitoring tools as well as the ever-growing sophistication of cyberattacks. To meet future data service demands, governments, enterprises and carriers are not only enhancing their network infrastructure for greater speed and quality of service (QoS), but also looking for ways to manage their data flows more intelligently. The key to maintaining integrity, ensuring security and optimizing efficiency of a multi-Gbps network is deep packet inspection.

1) https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/05/The-Mobile-Economy-2018.pdf
2) https://www.strategyr.com/MarketResearch/ViewInfoGraphNew.asp?code=MCP-7015

2. WHAT IS DEEP PACKET INSPECTION?

Internet traffic is made up of data packets with information about origin and destination, referred to as header and footer, as well as the message itself, referred to as payload. Deep packet inspection is a filtering technology that examines these data packets.

A key issue is that Internet packets are composed of more than a single header plus payload. A communication system can be divided into seven layers, with layers 1 to 3 referred to as media layers and layers 4 to 7 as host layers (OSI model). Accordingly, each packet consists of 7 layers, each with a header and payload. Layer 7, for example, is called application layer, supporting end-user processes and applications. Each layer implements a subset of functions necessary for end-to-end data transmission, which is ensured by defined interfaces between these layers. In a sending system, for example, each layer receives data via these interfaces from the layer above. This data constitutes the payload for the current layer.

Previously, stateful packet-filtering technologies (stateful packet inspection, SPI) utilized the header and footer information of the packet. This is comparable to only reading the sender and recipient address on a parcel, as it does not provide any information on the content of the packet and whether it is part of a larger transmission. If the packet appears to be legitimate according to its basic transportation information, SPI will allow that packet to travel through the network, even if it contains malicious code or other damaging data. Embedded DPI classifies the protocol and application the packets belong to (layer 7).
This information provides a better understanding of network traffic and facilitates informed decisions. By analogy, DPI is like X-raying a parcel and detecting explosives.

2.1 Functionalities

Generally speaking, DPI functionalities cover three key categories:

- Protocol and application classification
- Content and metadata extraction
- Statistical and behavioral analysis

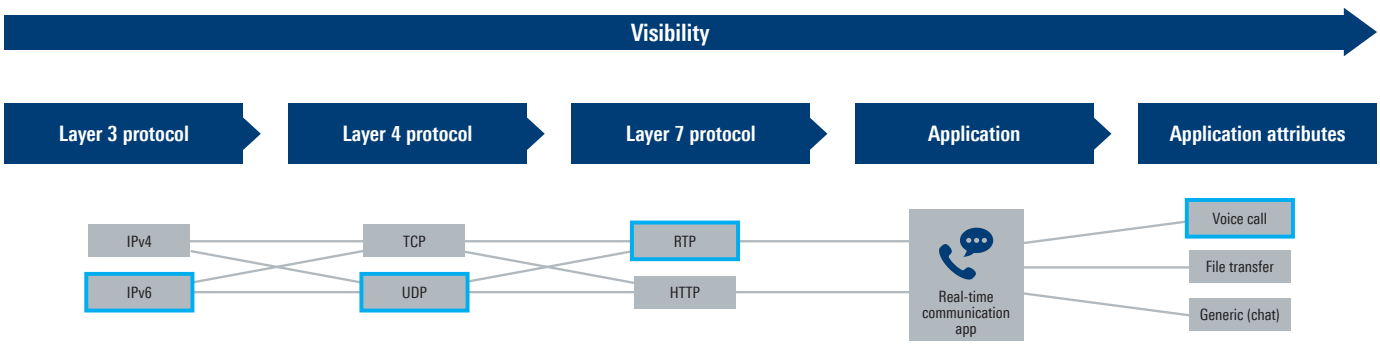
2.1.1 Protocol and application classification

Protocol and application classification examines the layer 3 to layer 7 protocols in a communication system. Beyond determining the specific application, for example a real-time communication app, DPI can identify the application attributes revealing whether the communication is a voice call, a file transfer or a generic chat (see figure below). This allows fine-grained application visibility and control. Frequent updates are necessary as some applications' signatures may change regularly and new signatures need to be added to face emerging threats.

2.1.2 Content and metadata extraction

DPI can also extract content and metadata, providing structured data insights, depending on the communication protocol. Full content and metadata extraction of communication protocols such as server initiation protocol (SIP) and real-time transport protocol (RTP) provides key performance indicators (KPI) on network traffic performance including jitter, packet loss, bit rate, throughput, re-transmissions, voice over IP (VoIP), etc. This is an essential tool to deliver the desired network traffic visibility and optimize QoE and QoS.

Classification vector results and application attributes for a real-time communication app voice call



2.1.3 Statistical and behavioral analysis

A third DPI functionality is statistical and behavioral analysis. These techniques provide the basis for metrics and heuristics, even in encrypted traffic. Checking packet sizes, packet timing, latency, throughput, entropy and jitter provides information on applications and protocols, even in an encrypted flow. Video streams, for example, show a characteristic buffering behavior that is reflected in a sawtooth-like throughput pattern as opposed to the stable throughput pattern of file downloads. Combining various metrics while focusing on specific session behavior is a suitable method to classify applications and even extract metadata in encrypted traffic. These metrics are important in security applications, because many sophisticated applications, such as VPNs, can only be detected this way. For example, an employee is using a corporate Internet connection to illegally share content using BitTorrent, a peer-to-peer file transfer protocol. BitTorrent actively obfuscates behavior at protocol level to circumvent firewalls. DPI can help in this situation by identifying the obfuscated connection and denying file sharing.

Techniques:

- Pattern matching: scanning for strings or generic bit and byte patterns everywhere in the packet, including the payload portion, usually at fixed locations.
- 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.

2.2 Advantages and importance

In a general sense, DPI makes network trends visible, helps communication service providers (CSP) optimize bandwidth and throughput, and reveals user behavior. Over the years, DPI has evolved from a basic signature-based security mechanism used for identifying threats through pattern matching to an advanced behavioral and statistical analysis tool delivering full insight into IP-based network traffic. Today, DPI enables network infrastructure and security vendors to develop products with efficient bandwidth control, prioritized QoS delivery and robust network security empowering intelligent networks for the future. DPI is a key technology to master new challenges like cloud computing, the Internet of things, the move to 5G and increased encryption. For example, the drive for more intelligent decision-making in networks can be addressed with embedded DPI functionality in IoT gateways or wireless access points. It is smarter to take some networking decisions as close to the user as possible to maximize QoE and optimize bandwidth utilization. A connected car, for instance, will need to be constantly connected, and any downtime might compromise safety or even put lives at risk. A connected fridge, on the other hand, needs to sync with the user's phone very infrequently. Intelligent connectivity can be established with DPI-enabled real-time data management.

> DPI has evolved from a basic signature-based security mechanism to an advanced behavioral and statistical analysis tool.

With heuristic detection techniques, DPI technology can be adapted to the growing amount of encrypted data traffic. Although encryption may prevent a look into the data packet itself, other information can be gleaned from the origin and destination of the packet, its size and associated packets. This inferred information can provide almost as much traffic visibility as findings from unencrypted traffic. As a result, heuristic detection techniques can be applied for anomaly detection: Instead of looking for matches, the system looks for behaviors that are unusual, unexpected or atypical. This way, it is possible to determine where malware is active and prevent phising attacks even when they are hidden in encrypted traffic. Along with rising automation and machine learning, DPI is a lean and powerful tool to fight future network security threats.

3. DEPLOYMENT SCENARIOS

With advances in network technology, DPI is also evolving. Today, DPI is deployed in many areas. By embedding DPI, software vendors can introduce new features like application detection to their products and keep up with the dynamic changes in protocols and applications. DPI technology is primarily used in IP networks in the following three areas:

- Network analytics solutions
- Traffic management solutions
- Network security solutions

3.1 Network analytics solutions

DPI software is typically used by CSPs as a network analytics tool for two main tasks: subscriber analytics and network statistics. DPI-enabled in-depth network traffic and subscriber analytics allow IT professionals to better understand networks and their traffic. With the enormous growth in IP network traffic, application identification is critical to distinguish between different types of traffic. The traffic management chapter will provide information about that in more detail.

Furthermore, DPI technology helps uncover subscriber behavior and preferences. This allows for decisionmaking based on solid data, which is critical to business operations and key to unlocking new opportunities. Subscriber data can be used as marketing input, answering crucial questions like:

- Which applications are customers using?
- Which manufacturer's devices are connected, using which operating system and browser?
- Which are the customer's preferences, including language settings, demographics and interests?

> Accurate network monitoring requires more intelligence than just a high-level view of data packets travelling through the network.

Delivering metadata on network traffic and subscriber behavior can be monetized as an additional revenue stream. Media companies commonly use data mining and in-line content injection with DPI-enabled applications for targeted advertising. Accurate network monitoring requires more intelligence than just a high-level view of data packets travelling through the network. Traffic analytics using DPI technology plays an important role in network management, optimization and planning. DPI can help network professionals to dive deeper into user activity data and provide intelligence about user traffic, application usage, communicated content and abnormal patterns. As a result, monitoring traffic patterns and bandwidth needs prevents network congestions and ensures service availability. The most important result is an increased customer satisfaction and QoS/QoE delivery.

Use case: Mobile network planning and optimization solutions in a 5G world

5G networks are built to lower latency, energy requirements and costs while increasing capacity, bandwidth, flexibility, security and reliability. The major network traffic increase driven by 5G speeds will make efficient network routing a top priority. DPI enables intelligent networking close to the subscribers and their individual demands. With application layer information, traffic optimization decisions can be made with concise input. This way, a more efficient network and a higher QoE are established and maintained. Additionally, DPI empowers network security taking advantage of application usage information. All in all, accurate network planning and optimization can contribute to jumpstart the multi-layer, intelligent, secure network of tomorrow.

3.2 Traffic management solutions

Mainly focused on maximizing QoS/QoE and avoiding downtimes, traffic management solutions aim at optimizing limited network bandwidth. In their solutions, vendors need to provide accurate real-time insights into QoS/QoE as well as application usage, KPI monitoring and even trend analysis. Accordingly, their solutions need detailed and reliable protocol and application classification to disclose, for example, carrier VoIP or video streaming in IP traffic. Additionally, it is essential for vendors to extract application metadata such as delay, packet latency, jitter or call completion on voice over LTE (VoLTE). With DPI, application layer information enables fact-based traffic optimization, resulting in a more efficient network.Potential benefits for DPI-based bandwidth management include:

- Prioritizing interactive real-time applications such as VoIP, live online gaming and remote access
- Rate-limiting bandwidth-intensive applications such as large downloads from peer-to-peer (P2P) networks and web-based file hosting services during traffic peaks
- Blocking access to undesired applications such as P2P file sharing in an enterprise environment

Use case: SD-WAN

SD-WAN is a specific application of software-defined networking (SDN) technology applied to WAN connections, which are commonly used in enterprise networks. SD-WAN vendor solutions rely on an embedded DPI library. The benefits of DPI in SD-WAN are paramount as application visibility allows for agile and intelligent networking in many areas.

Application visibility and performance control in general are key DPI enhancements in SD-WAN. This includes application performance for end users as well as the computational resources per application to indicate whether sufficient resources are available. Highly granular application identification allows for strong traffic engineering policies.
For example, even if a network link is down, mission-critical enterprise applications can be re-routed without loss of performance. This has become increasingly attractive to enterprises that are using third-party cloud application providers, for instance Microsoft, Salesforce or Amazon Web Services, as well as companies with a high number of mobile workers or distributed companies, such as banks or retailers with many small sites and branch offices.

Application statistics provide a holistic view of network bandwidth usage, a feature for which IT departments have a great demand. This application visibility and control can be useful to secure and segment traffic. For example, regional Internet exit points can re-rout specific applications rather than backhaul all traffic to a data center. When paired with DPI, service chaining provides an effective way to secure SD-WANs. DPI grants application visibility, supporting software-based virtual network functions (VNF) for unified threat management such as stateful and next-generation firewalls, malware protection, URL and content filtering, intrusion prevention systems (IPS), anti-virus or distributed denial of service (DDoS). DPI application visibility also prevents firewalls from accepting malicious traffic and attempts to sneak malware through the gates unseen.

3.3 Network security solutions

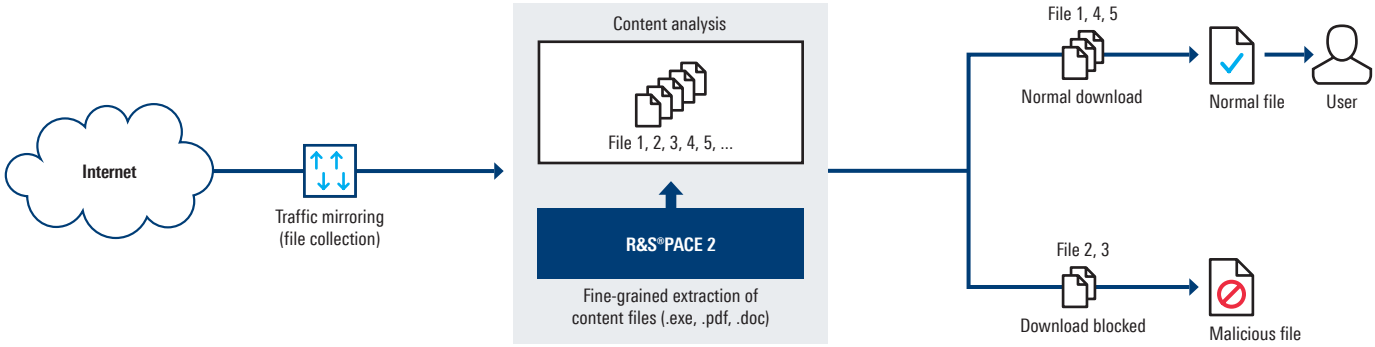
In today's networking ecosystem, network security vendors have to address multiple challenges such as data growth, growing encryption and obfuscation rates, growing protocol complexity and app/service growth. For instance, with the huge growth in IP traffic using web protocols, network security vendors need to be able to identify applications in order to distinguish between malicious and regular traffic. DPI empowers network security applications, such as spam and virus filters, email filtering software, intrusion detection systems (IDS), IPS, malware protection and firewalls to respond to these challenges.

Use case: Advanced threat protection

Advanced persistent threats (APT) are more covert and malicious than ever. Sophisticated techniques are used to quietly breach organizations and to deploy customized malware, which potentially goes undetected for months. Such attacks are caused by cybercriminals who target individual users with highly invasive tools. Legacy security approaches are bypassed to steal sensitive data, such as credit card details, intellectual property or government secrets. Traditional cybersecurity solutions, for example email spam filters, anti-virus software or firewalls, are ineffective against APTs as they can bypass such solutions and gain hold within a network to make organizations vulnerable to data breaches.

With DPI, network-based threat detection software can intercept possible APTs at any point in a network. DPI identifies and blocks various types of malware that existing security solutions cannot detect – even if they have never been reported before or belong to a new family of malware. To fingerprint malicious activity and deeply understand the observed network traffic, the full potential of traffic analytics has to be unlocked. As shown above, APT detection software needs real-time extraction of file content to identify potentially dangerous executables.

DPI-enabled advanced persistent threat protection



DPI software extracts file content and metadata such as files attached to emails (for example .pdf, .exe or .doc) or files sent through file transfers within the traffic in real time. For example, an advanced ransomware uses a vulnerability in the windows file sharing service SMB to gain access to a system. The vulnerability is triggered by malformed protocol requests. After infection, the malware tries to utilize the Tor network. DPI identifies the SMB connection, extracts the SMB request content and enables the security solution to block the Tor connection. Hence, by using metadata and content extraction techniques, an embedded DPI engine significantly enhances advanced malware response and threat detection software.

3.4 DPI and the impact of machine learning and artificial intelligence on future networks

As in many other areas, artificial intelligence (AI) is driving fundamental changes in IP networking and telecommunications. AI, mostly based on (deep) machine learning (ML), is complex, and has to be built on a solid foundation. Harrison/O'Neill[1] assert that a critical mass of automated processes is required to successfully use ML. A cross-functional and cross-departmental approach to network analytics is another important point (not only) for CSPs, according to a McKinsey report.[2] The most important prerequisite for a successful implementation of ML technology is the data foundation[3], as ML can only provide results as good as the data they are based on. If, one day, AI is to be the brain of a given network, it needs to have, so to speak, eyes and ears. This is where DPI comes into play.

DPI enables the most accurate user and network profiles for network analytics (see graphic below). With more and more accurate data to build upon, ML can prove its worth, for example, in predicting which customers might be about to churn. With this business intelligence, CSPs can proactively solve issues and keep their customers. As Harrison/O'Neill claim, CSPs are 75 times more accurate at predicting whether their customers are about to churn, when applying ML.

DPI is a critical enabler for meaningful machine learning and artificial intelligence.

In traffic management, ML can help to better understand traffic streams. Automated detection of DSCP values (indicating transmission requirements in the packet header, for example „low latency") facilitate proactive measures before an overload occurs. DPI helps to differentiate between mission-critical and best-effort data streams, this way, again, building the right data foundation. With this data, AI can, for example, decide which traffic actually needs expensive multiprotocol label switching (MPLS), a fast routing technique connecting two nodes, and which can be sent through the Internet. In another example, predictive AI in an SD-WAN deployment can reconfigure QoS settings and reduce bandwidth for a given best-effort app to free capacity for a prioritized business-critical app. Also, the impact of an additional real-time application on the network can be predicted. As a result, video streaming bandwidth might be blocked in order to maintain sufficient bandwidth for audio applications. Again, DPI, delivering fine-grained application and metadata information in real time, serves as a critical enabler for meaningful ML and AI.

DPI-enabled user, system and network profiles can serve as machine learning input

User

User activity*
User communication*
Downloads, uploads, file transfers

System

Device activity*
Device communication

Network

Devices
Device activity*
Communication patterns*
Network service activity

* DPI increases network-based visibility on activities and communications

1) Nick Harrison/Deborah O'Neill: If your company is not good at analytics, it´s not ready for AI, https://hbr.org/2017/06/if-your-company-isnt-good-at-analytics-its-not-ready-for-ai
2) https://www.mckinsey.com/industries/telecommunications/our-insights/reducing-churn-in-telecom-through-advanced-analytics
3) Monica Rogati: The AI Hierarchy of Needs, https://hackernoon.com/the-ai-hierarchy-of-needs-18f111fcc007

4. DPI AS A SERVICE

When a device or solution needs DPI application awareness as a key enabling feature, the choice between building in-house DPI libraries and licensing software from a DPI expert may seem difficult. Whatever the use case may be, selecting the right DPI solution has become a critical strategic decision.

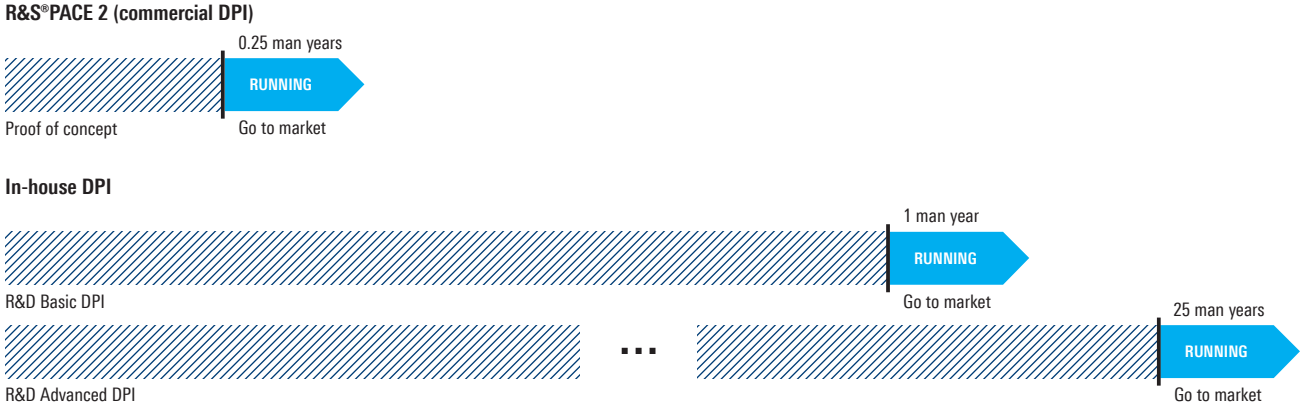
While developing a DPI solution in house saves the licensing costs of a commercial solution, vendors often forget to factor in maintenance costs. Building their own DPI, they are hardly able to estimate maintenance costs in advance. With a commercial solution, the licensing costs are predictable fixed costs. Additionaly, developing a thorough solution takes time. Commercial DPI solutions can provide the desired services almost instantaneously.

A DPI engine is only as effective as its creators make it. The ongoing evolution of network traffic with its steady increase in the numbers and complexity of applications and protocols means that DPI software is never complete. Any DPI requires continuous software updates with the latest application and protocol signatures. As a result, DPI developed in house causes ongoing and unpredictable maintenance costs. DPI software companies, on the other hand, have dedicated experts adding new signatures to the library on a weekly basis. This ensures that at any time, a very high rate of network traffic can be reliably classified, which is vital for network equipment and software vendors. With ongoing performance and reliability testing, licensed DPI software is continually being improved to ensure a high detection rate. For advanced analytics use cases, DPI vendors also offer DPI-powered IP probes as OEM software such as R&S®Net Sensor OEM. Such flexible probing software allows analytics vendors to include a customizable, ready-to-use DPI-powered software probe in their solutions without much development effort.

Vendors may consider open-source DPI because they are under the illusion that it is free to use. Open-source software is free but still requires in-house developers to learn about the software and, more importantly, to customize it. Frequently, this requires collaboration with a third-party vendor to manage and add new features. Again, unpredictable costs accrue.

A licensed DPI software, customized and deployed on site by leading experts, reduces costs and risks associated with developing and maintaining a highly complex technology internally. For example, in a typical network analytics setup, usage data is directly linked to third-party analytics systems that deliver reports and dashboards about data consumption. For seamless integration into such a third-party analytics system, the DPI software has to be heavily customized. Likewise, with more and more IP traffic being encrypted or obfuscated, open-source or in-house developed DPI software reaches its limits. Licensed DPI engines offer advanced techniques such as behavioral and statistical analysis to classify a high rate of encrypted applications. Altogether, licensing DPI software or DPI-powered software probes offers software vendors predictable costs, a short time to market and expert knowledge. As a result, they can focus on their core competencies.

Commercial DPI ensures short time to market



5. SPEED AND EFFICIENCY MATTER

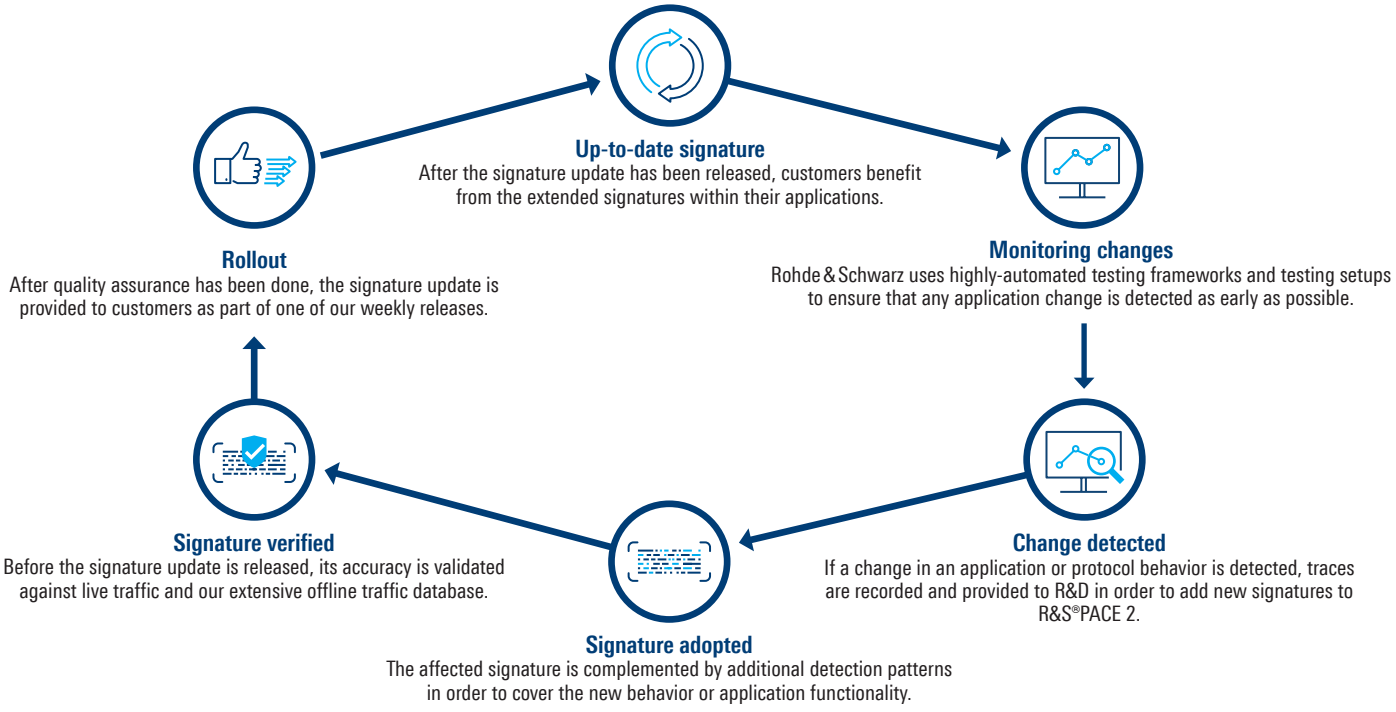
The Rohde&Schwarz DPI engine R&S®PACE 2 is a software library that reliably detects network protocols and applications, and extracts metadata and content in real time. Using different technologies including deep packet inspection as well as behavioral and statistical analysis, R&S®PACE 2 classifies IP traffic reliably, even if advanced obfuscation and encryption techniques are used. R&S®PACE 2 is embedded by network equipment and software vendors worldwide to enhance their products with state-of-the-art protocol and application awareness capabilities. Designed by developers with many years of experience in layer 7 protocol and application awareness, R&S®PACE 2 can be deployed in a variety of use cases as described in chapter 3.

R&S®PACE 2 is designed to inspect packets at high wire speeds with outstanding performance. Yet, the critical factor is maintaining the throughput while keeping the resources required to integrate DPI and application classification technology low. The fewer cores (on a multi-core processor) and the less on-board memory an engine needs, the better. R&S®PACE 2 is known for the smallest processing footprint on the market. Multi-threading provides almost linear scalability on multi-core systems. In addition, highly-optimized flow tracking facilitates handling millions of concurrent subscribers.

Key benefits of R&S®PACE 2

- Time to market and cost savings – reduced development time, capex and opex by licensing R&S®PACE 2
- Easy and fast integration – highly flexible APIs, platform-agnostic, no external dependencies
- Fast performance – up to 10 Gbps per core
- Most efficient memory and CPU utilization – smallest processing footprint on the market
- Accuracy and reliability – classifies over 95 % of network traffic (no false positives)
- Coverage – support for more than 2800 protocols and applications across diverse operating systems, application versions and service types
- Metadata extraction – deeper insight into application attributes, such as QoS/QoE, KPIs for network performance
- Up-to-date – weekly signature updates, including additions to the classification library (see below)
- Deployed globally by OEMs – global feedback ensures better visibility and detection rate of applications

Rohde&Schwarz ensures up-to-date signatures



6. CONCLUSION AND FORECAST

Currently, there are quite a few challenges for IT professionals in the fields of network analytics, traffic management and network security. Mobile data traffic is growing with bandwidth-demanding applications such as video streaming. Enterprise networks opt for SDN, cloud computing and software as a service (SaaS), facing new challenges in the areas of traffic steering and network security. The IoT and IIoT revolution is about to increase the number of connected devices. 5G networks will soon support big data applications, placing a high priority on efficient network routing. At the same time, rising encryption and obfuscation rates are posing a new challenge to traffic analytics. Network equipment and software vendors continuously need a deep understanding of IP network traffic to keep future networks safe, agile and reliable. Managing network performance, improving end user experience and securing applications end-to-end requires application visibility.

DPI is a key enabling technology to respond to current and future network challenges. In the field of network analytics, DPI helps to develop products that unlock value and increase revenue by better understanding subscriber application usage and behavior. Traffic management use cases powered by DPI benefit from a holistic view of networks to shape them accordingly. Regarding network security, DPI allows vendors to stay ahead of threats with detection techniques as sophisticated as the cyberattacks themselves. In all the applications and use cases discussed, DPI is a powerful tool to build a solid data foundation for ML and AI.

Only advanced DPI techniques, which continuously co-evolve with the advances in encryption technologies, can meet the challenges of an increasing use of encryption and obfuscation. Accordingly, licensing DPI is a prerequisite to keep up with the dynamic changes in protocols and applications and meet high customer expectations with state-of-the-art technology. Of course, the future development of network trends cannot be predicted. Still, as application visibility will remain a prerequisite of intelligent network decisions, a future without the use of a high-performance, easy-to-use DPI engine like R&S®PACE 2 by Rohde&Schwarz appears quite unlikely.

SUMMARY

DPI is a filtering technique used to inspect data packets in IP networks. With traffic visibility up to layer 7 (application layer in the OSI model), DPI reveals a clear picture of protocols, applications and application attributes. Embedding DPI enables software vendors to track down, identify, categorize, measure, reroute or stop packets.

Advanced DPI features

- Protocol and application classification
- Content and metadata extraction
- Statistical and behavioral analysis to classify encrypted traffic

Main DPI use cases

- Traffic analytics and management
- Policy enforcement
- Application-level security
- Next-generation firewalls
- Tiered pricing
- QoS and QoE optimization
- Dynamic routing decisions in real time
- Machine learning input for network automation
- Enabling network function virtualization (NFV)

Benefits of DPI as a service

- Staying ahead of threats with advanced detection techniques and weekly signature updates
- Concentrating on core competencies by licensing leading-edge technology
- Fast time to market and customization with APIs, integration examples, thorough documentation and dedicated service and support teams
- Deployed globally by OEMs – global feedback ensures better visibility and detection rates of applications

ipoque

ipoque, a Rohde & Schwarz company, is a global leader of network analytics software for the communications industry. We leverage our deep domain expertise to create software solutions that empower customers to transform data into intelligence.

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 3608.1575.52 | Version 01.01 | October 2019
White paper | Deep Packet Inspection

3608157552