R&S®PACE 2 CACHING AND ENCRYPTED TRAFFIC INTELLIGENCE

# FIRST PACKET CLASSIFICATION IN AN ENCRYPTED WORLD

## First packet classification

First packet classification refers to the accurate and reliable classification of the very first packet in a flow instead of waiting for at least 3 to 5 packets before the underlying application is identified. This way, traffic policies can be issued on the first packet and implemented across all following packets for application-wide consistency. Network providers including SD-WAN and SASE 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.

## R&S®PACE 2

R&S®PACE 2 is an advanced OEM deep packet inspection (DPI) software. It classifies protocols and applications up to layer 7 and beyond and performs metadata extraction. By combining the following traditional DPI techniques, R&S®PACE 2 provides state-of-the-art protocol and application awareness:

- **Pattern matching** – With its signature library containing thousands of protocol and application signatures updated weekly, R&S®PACE 2 scans packets for matching string and number patterns to identify protocols, applications and service types.
- **Behavioural analysis** – R&S®PACE 2 analyzes IP packets within a flow for their size, order and frequency in combination with subscriber and host information.
- **Statistical/heuristic analysis** – R&S®PACE 2 computes statistical attributes such as the mean and median across behavioural indicators to identify wider traffic attributes including a flow's entropy.

Combined, these methods deliver real-time, granular visibility into each packet flow. To enable first packet classification, however, R&S®PACE 2 offers advanced caching techniques built on the intelligence developed from traditional DPI methods.

## Caching for first packet classification

Caching means storing thousands of IP addresses and domains across an extensive list of verified web services and applications, which enables R&S®PACE 2 to classify the first packet in a flow in real time. Upon classification, packets are processed further for metadata extraction and service type identification. R&S®PACE 2 uses the following two caching techniques:

- **DNS caching** – This technique reads the hostname from the domain name system (DNS) query and stores the provided IP addresses from the appropriate DNS answer.
- **Service caching** – This technique identifies a service or an application through the DPI engine and caches its IP address. Any packet with the same IP address is immediately recognized and is exempted from being filtered further through other DPI algorithms.

However, as new encryption technologies such as DNS over HTTPS (DoH) become more prevalent, caching-based first packet classification is set to become less effective in the future. Additionally, these methods exhibit weaknesses when it comes to the active use of proxy servers and content delivery networks (CDNs). They may result in false positives as the IP addresses of certain applications are concealed and therefore cannot be reliably matched to the correct applications or services.

### Rise in encrypted, obfuscated and anonymized traffic

There is a steady rise in traffic encryption, obfuscation and anonymization. Encryption, for example, is set to proliferate given the introduction of new encryption methods such as TLS 1.3, TLS 1.3 0-RTT and ESNI as well as DNS over TLS and DNS over HTTPS. There is also a surge in traffic anonymization, which means masking the true identity of the underlying traffic. At the same time, traffic obfuscation techniques such as randomization, tunnelling and mimicry are becoming increasingly common and are typically deployed by threat actors to disguise malicious activity. To address these types of traffic, DPI providers must invest in future-proof first packet classification by deploying newer, more advanced techniques leveraging machine learning (ML) and deep learning (DL).

### ML/DL to drive full application awareness in the future

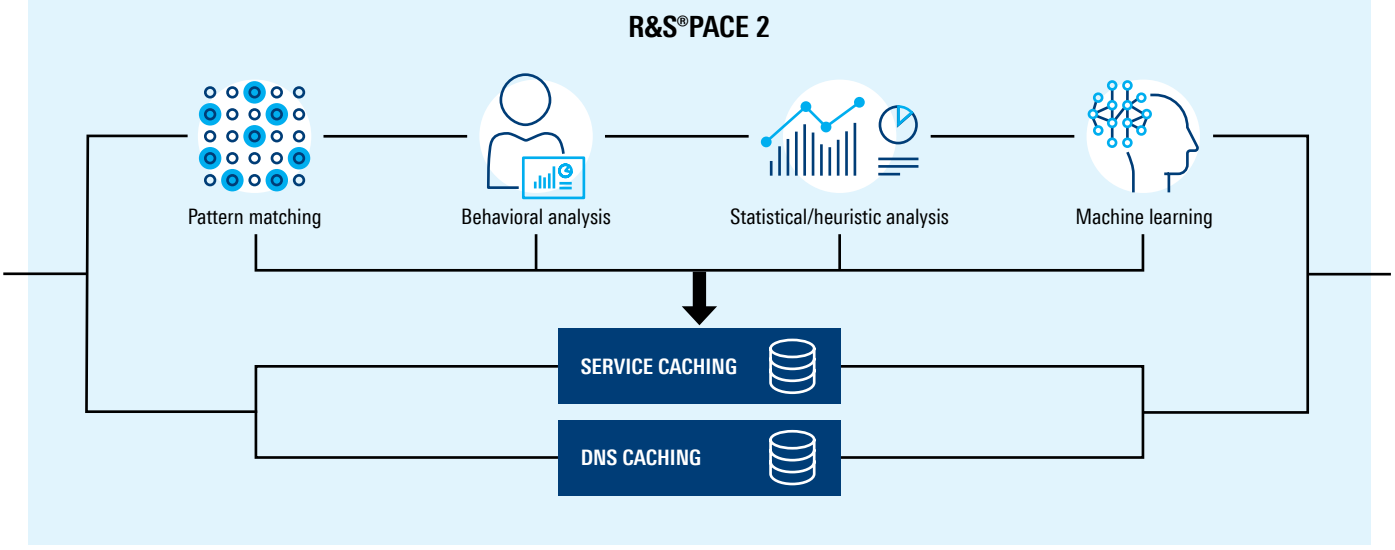
R&S®PACE 2 offers cutting-edge ML and DL capabilities, which, when coupled with its traditional DPI techniques, equip networks with encrypted traffic intelligence (ETI). ETI leverages a mix of advanced ML algorithms combined with different DL layers. To enhance the signature library, for example, ML algorithms automate the detection and verification of new signatures as well as the detection of possibly inaccurate or weak signatures. The ETI functionality of R&S®PACE 2 is enhanced by extensive collaboration with top universities on research into advanced methods to classify traffic encrypted with TLS 1.3, DoH and ESNI as well as traffic obfuscated by domain fronting. This enables Rohde&Schwarz to utilize advanced techniques such as self-learning network management for the classification of obfuscated applications.

With its team of in-house data scientists who deploy advanced statistical as well as classical ML, high-dimensional data analysis and DL, Rohde&Schwarz is able to continuously enhance the ability of R&S®PACE 2 to classify and extract metadata from any encrypted, obfuscated or anonymized traffic accurately.

### R&S®PACE 2: Key functionalities & benefits

- Caching-based first packet classification
- Future-proof technology stack based on disruptive ML/DL methodologies
- Identification of thousands of applications and protocols
- Highest traffic detection rate and accuracy on the market
- Performance of more than 14 Gbps per core
- No vendor lock-in and well defined APIs

## R&S®PACE 2 CACHING AND ENCRYPTED TRAFFIC INTELLIGENCE




**ipoque GmbH**
**A Rohde & Schwarz Company**
Augustusplatz 9, 04109 Leipzig
Info: +49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

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


PD 3609.8880.32 | Version 01.00 | July 2021
First packet classification in an encrypted world
Data without tolerance limits is not binding | Subject to change


3609888032

3609.8880.32 01.00 PDP 1 en