Deep Packet Inspection for Wireless Access Points:

Analyze. Control. Secure.

ROHDE&SCHWARZ
Cybersecurity

White Paper | 01.01

Table of Contents

Introduction

According to many market research analysts, the global wireless access point (WAP) market is anticipated to continue its upward trajectory and to grow at an impressive compound annual growth rate (CAGR) of approximately 8% through 2020. Many enterprises are utilizing cloud-computing technology for cost-cutting purposes, eliminating investments required for storage hardware and other physical infrastructures. With significant growth expected in Internet usage, particularly bandwidth consuming video traffic, WAP vendors need to enable their customers to monitor and improve device performance, improve end user experience, and enhance security. These customers include general enterprises that offer Internet access to patrons like airports, hotels, retail/shopping centers and so on. These external Internet access providers can differentiate themselves by offering optimum service through advanced network analytics, traffic shaping, application control, security capabilities and more.

Wireless access points are now used for in-depth network traffic and user analytics that allow enterprises to better understand Internet communication, such as web traffic or instant messenger. In addition, protocol and application classification with metadata extraction is becoming a fundamental tool to deliver the desired network traffic visibility and management.

All of this is achieved via deep packet inspection technology (DPI) embedded into the WAP platform. Implementing DPI software into WAPs creates an intelligent network infrastructure that can offer an opportunity to monetize new data services, improve quality of experience (QoE), strengthen network security measures and more. With exponential increases in both data rates and bandwidth demands, WAP vendors are unable to meet the requirements of QoS, QoE and performance without proper IP traffic analytics capabilities provided by DPI technology. In short, DPI is a crucial prerequisite for the success of next generation wireless access points.

WAP Utilization & Challenges

Wireless access points (WAPs) are special-purpose communication devices on wireless local area networks (WLANs). Serving as a central transmitter and receiver of wireless radio signals, the network hardware allows a WiFi compliant device to connect to a wired network. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. WAPs also enable WiFi hotspots. These hotspots commonly deploy one or more WAPs to support the WiFi coverage area and traffic. Business networks also typically install WAPs throughout the office areas. While most homes only require one wireless router (access point) to cover the physical space, businesses may use many of them. Determining the optimal locations for where to install a set of WAPs can be a challenging task, even for network professionals, due to the need to cover areas with a reliable signal.

The growing number of enterprises that offer WiFi service has led to significantly increased competition in the marketplace. Revenue is lagging, traffic is growing, and users are increasingly demanding consistent, high-quality service regardless of where they are or what device they are using. The need to stand out from competitors through quality of service (QoS) is critical. Enhancing a user's shopping, banking or leisure experience can attract customers and increase business and market share. Optimizing the performance of the WAP network through traffic management capabilities can save colleges/schools, hospitals, malls and other enterprises significant costs. These savings can be realized when IT managers can avoid purchasing a larger (and more expensive) fixed broadband line through optimal management of existing capacity.

Enterprises and other WiFi service providers around the world are recognizing the need for in-building cellular/Internet solutions that are easy to deploy and provide an attractive total cost of ownership (TCO) while improving coverage and performance. There is a growing desire to optimize WiFi service and maximize customer/employee coverage through the implementing of WAPs that enable the improved resource utilization and planning via full visibility and tracking of Internet traffic.

WAPs now have been enhanced, as they can now monitor WiFi usage in real time and increase QoS based on dynamic network conditions. In addition, WAPs improve security by enforcing usage rules for personal devices once they are on the network. All of this is achieved by embedding DPI technology onto the WAP platform.

Embedding DPI technology onto WAP platforms has been difficult in the past. WAP devices typically do not have the memory or computing processing power to support DPI technology. Previous technology needed a significant amount of processing power (CPU-load) and memory. But with the development of new, more advanced DPI software with a low memory footprint, this is no longer an area of concern or difficulty.

DPI Defined

As services and applications become more integrated and customized, the knowledge of the Internet Protocol (IP) layer is desirable. Enabling accurate network monitoring and analytics requires technology with the intelligence to do more than just a high level view of the data packets traversing the network. As such, deep packet inspection goes beyond the IP header. Deep packet inspection, also known as complete packet inspection, provides that visibility by analyzing up to Layer 7 of the packet. This provides a finer control and more granular application identification than header-based classification. This requires maintaining a software library of thousands of protocols and applications and understanding patterns and behaviors for every new app and version. Otherwise, a packet can easily be incorrectly classified. A classified packet may be redirected, marked/tagged, blocked, rate limited, and, of course, reported to a reporting agent in the network.

Many DPI software solutions can identify packet flows, allowing control actions based on accumulated flow information. DPI enables the extraction of WAP content and metadata as well as the reporting and handling of the extracted information from IP-based traffic. This extracted data can be used for a wide range of use cases including:

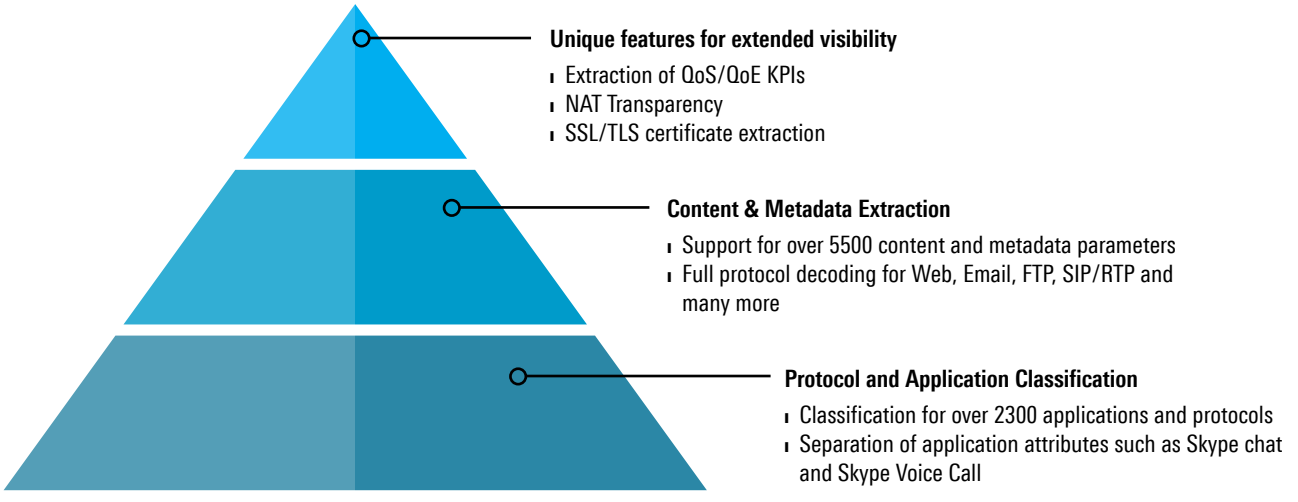
- Strengthen network security
  - Fine-grain application and access control
  - Enforce usage rules for personal devices on the network
  - Facilitate parental control
- Network optimization & planning
  - Measure WAP performance and user QoE
  - Enable traffic shaping and management
  - Prioritize key business traffic
  - Enhance VoIP performance
  - Enforce QoS based on dynamic network conditions
  - Reduce maintenance costs
- Enhance marketing and grow revenue
  - Increase revenue through tiered WiFi packages and real-time or post-event upsell
  - Rate based access control down to application layer

In addition, some DPI engines deliver modular functionality that can be tailored to meet customer WAP system requirements. Customized functionality can include:

- Configurable event reporting to improve performance
- Signature updates on runtime with no service interruption
- Support for VoIP, audio & video KPIs such as throughput, latency, jitter
- Application attributes separate different application usage types (e.g. Skype audio & Skype video calls) to determine application performance and QoS for VoIP and video as well as to protect against network security threats.

As external Internet access providers seek to improve the QoE by making their networks application-aware and adaptive, there is a corresponding opportunity for network equipment and solution suppliers to provide offerings that enable more intelligent networks. This, in turn, is driving demand for embedded deep packet inspection.

DPI capability categories – Examples



DPI Benefits

Traffic monitoring through implemented DPI technology plays an important role in network management, network optimization and planning. Internet access providers are typically only aware of general characteristics of the web traffic. When embedded into new and existing wireless access point systems, DPI can help network professionals to dive deeper into the user activity data. DPI provides intelligence about user traffic, application usage, content communicated and anomalous patterns. As a result, they can prevent WiFi network congestion and ensure WiFi service availability to all customers by monitoring traffic patterns and bandwidth needs, thus increasing customer satisfaction.

Gaining business intelligence from WAP network and user data is a fast growing area, as external Internet access providers recognize they cannot only increase the efficiency of their network, but also generate additional revenue through tiered WiFi packages as well as real-time and post-event upsell.

With the huge growth in IP network traffic using web protocols, Internet access providers need to be able to identify the application to distinguish between traffic. DPI can be used to 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, Internet access providers can better optimize resources for mission-critical traffic and police the use of noncritical traffic.

DPI empowered WAPs can distinguish between specific applications for instance Hulu versus Salesforce and then apply policies based on business rules. Enabling a WAP to enforce usage rules for business and personal devices once they are on the network is increasingly valuable. Not only does this strengthen network security by limiting potential threats/attacks, it also prioritizes key business traffic.

DPI technology goes beyond security protocols to offer a suite of capabilities that includes analyzing the payload of the packet and extracting content-level information such as malware, specific data and application types that are otherwise unavailable. This enables enterprises and corporations to better manage their network in case they are increasingly dependent on the efficiency of their networks and the applications that run on these.

Top DPI Benefits

- Reduce total cost of ownership for WAP operators
- Increase revenue
- Increase network security
- Reduce time-to market by sourcing DPI
- Improve QoS and QoE
- Monetize new business services

Improving Airport Public WiFi QoE/QoS

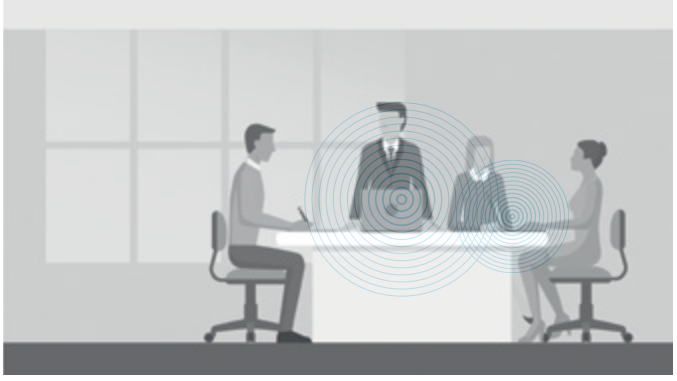
Traffic shaping, or packet shaping, is the practice of regulating network data transfer to ensure a high QoS or return on investment (ROI). The practice involves delaying the flow of packets designated as less important or less desired than those of prioritized traffic streams. Regulating the flow of packets within a network is called bandwidth throttling. Traffic shaping is vital for WiFi hotspots in airports to lower the WAP operators TCO by improving link utilization. Reasons for traffic shaping include:

- Time-sensitive data or airport/flight specific data that is given priority over traffic that can be delayed briefly. This data can include real-time flight updates and concession recommendations.
- Frequent flyer airport lounges that can be given priority over other traffic.
- An ISP that may limit bandwidth consumption for certain applications to reduce costs and to create the capacity to take on additional subscribers.

The era of big data has brought about an entirely new way of understanding customers. Airport WAPs with DPI technology can deliver advanced network analytics that uncover passenger behavior and preferences. This permits data-driven decision making critical to business operations and key for uncovering new opportunities. The data can be used as marketing input, including:

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

As such, airports are likely to see Netflix, Hulu or Spotify used significantly and can specify peak Mbit/s for each application, ensuring optimum connectivity to accommodate these applications. For example, Netflix, Hulu and Spotify all currently recommend different bandwidth requirements to maximize HD quality. Additional WiFi operational insights address how much data is consumed, the length of user connects and the network load by defined locations like a terminal, gate or restaurant/bar. Geo-plotting multi-dimensional attributes allows the enterprise to pinpoint where users are congregating, whether it's a popular concession stand, busy gate or check-in kiosk. This level of knowledge can be crucial for operation teams, as it helps your network planning team ensure the airport has a dense wireless infrastructure that can handle high passenger traffic with the right coverage.



Increasing Enterprises' WiFi Security and Control

Protecting networks requires flexible network architectures,constant observation, and active handling of identified issues. Threats can be brought in unknowingly through BYOD (bring your own device), IoT, file download permissions and automatic software upgrades, which all contribute to network congestion or malware infection. WAPs with embedded DPI provide high-grade security policies via layer 7-aware classification and metadata extraction. The WAP analytics allow enterprises to recognize irregular behavior from a network security breach and identify the issue.

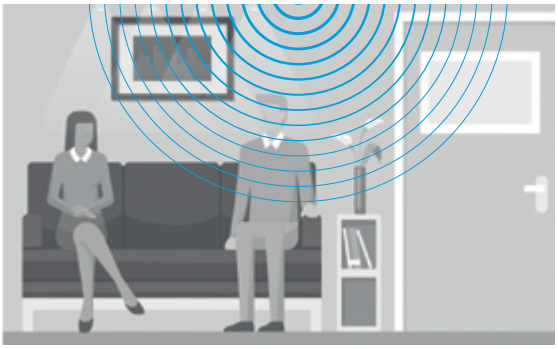
The increasing number of devices connecting to a network with BYOD and the propensity of some devices to be easily infected makes policy enforcement challenging, particularly considering the widespread use of encryption and obfuscation techniques. Any first-level approach to network protection usually involves website/application blacklisting and role-based access management. WAPs with DPI technology simplify this task.

DPI technology provides fine-grained application control that delivers efficiency and high level security. It enables precise policy implementation, including access to specific websites, applications or servers/files. Managers can quickly and easily restrict users based on specific attributes, such as identity, role, location, action request, and time of request. Unlike current authorization and control tools, WAPs with fine-grained application control offer greater flexibility, accuracy, and security.

Besides increasing security and control, DPI-enhanced WAPs enable a holistic approach to traffic management when combined with existing SD-WAN solutions. By implementing traffic management on multiple points within the network, enterprises can optimize traffic flow and bandwidth usage over the whole corporate network instead of focusing just on WAN optimization.

By facilitating advanced fine-grained application control and metadata extraction, DPI technology creates leading-edge products that:

- Blacklist file sharing services like BitTorrent or other types of applications often abused
- Filter possible threats such as e-mail attachments, URLs, filenames and other types of suspicious payload
- Classify security-critical applications that actively hide and obfuscate traffic such as anonymizers, VPNs, Tor and peer-to-peer clients
- Investigate encryption quality and parameters by providing detailed metrics such as TLS/SSL ciphers, sessions, and certificates used



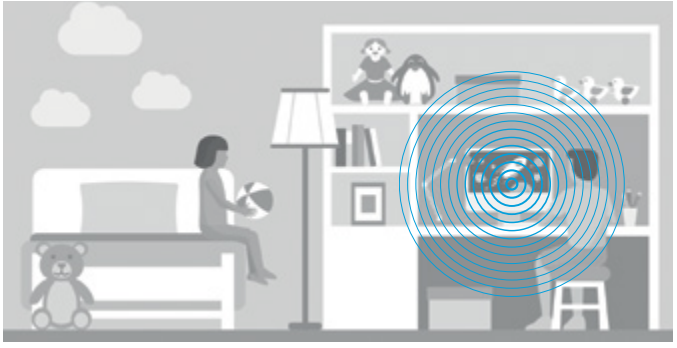
IoT-Ready Application-Aware Residential CPEs

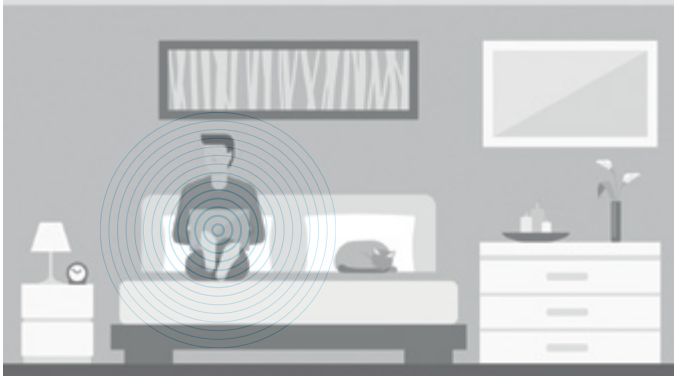
Customer-premises equipment (CPE) providers have limited solution offerings, because traffic visibility is restricted to Layers 1 to 4. The value of security protocols, QoS, service chaining, and reporting are greatly enhanced by leveraging the complete data spectrum of Layers 1 to 7. DPI technology is easily embedded into WAPs to provide IP classification up to Layer 7, delivering real-time application and user information that permit advanced control of application access.

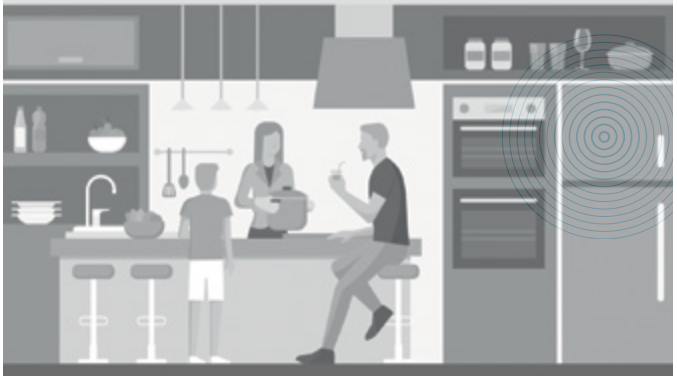
For example, WAPs with DPI technology can control access to certain services based on the time of day or frequency of visits. Parents can control when children are allowed to use certain applications, such as restricting Netflix after 10:00 pm. DPI technology can also limit access to online gaming platforms based on the frequency of visits. Therefore enabling a limiting in the number of times per day or week that a child can join the World of Warcraft gaming community for example. In addition, WAPs with DPI technology can be set to prioritize video streaming over other web traffic to ensure a higher QoE.

DPI technology creates an opportunity for WAP vendors to offer customers new value-added services like smarter homes. With the vast amount of new connected IoT devices and services, it becomes mandatory for WAPs to manage the available bandwidth efficiently while optimizing the quality of experience (QoE) for users. It has to be ensured that important signals and messages like those needed for controlling alarm systems and home automation have priority over entertainment-related or web surfing traffic.

Embedded DPI technology enables WAP vendors to classify a variety of IoT protocols, applications and services in order to create fine-granular traffic management and security policies. DPI-enabled residential CPEs help users reduce costs, maximize link utilization and enable superior quality of experience.







Build or Buy DPI

When a device needs deep packet inspection application awareness as a key enabling feature, the choice between building in-house DPI libraries and licensing software from a DPI specialist can be difficult. Whether an application requires software-defined networks to support policy control and critical traffic steering, protect corporate networks from malicious attacks or deliver metadata on network traffic and subscriber analytics, selecting the right DPI solution is becoming a more strategic and challenging decision.

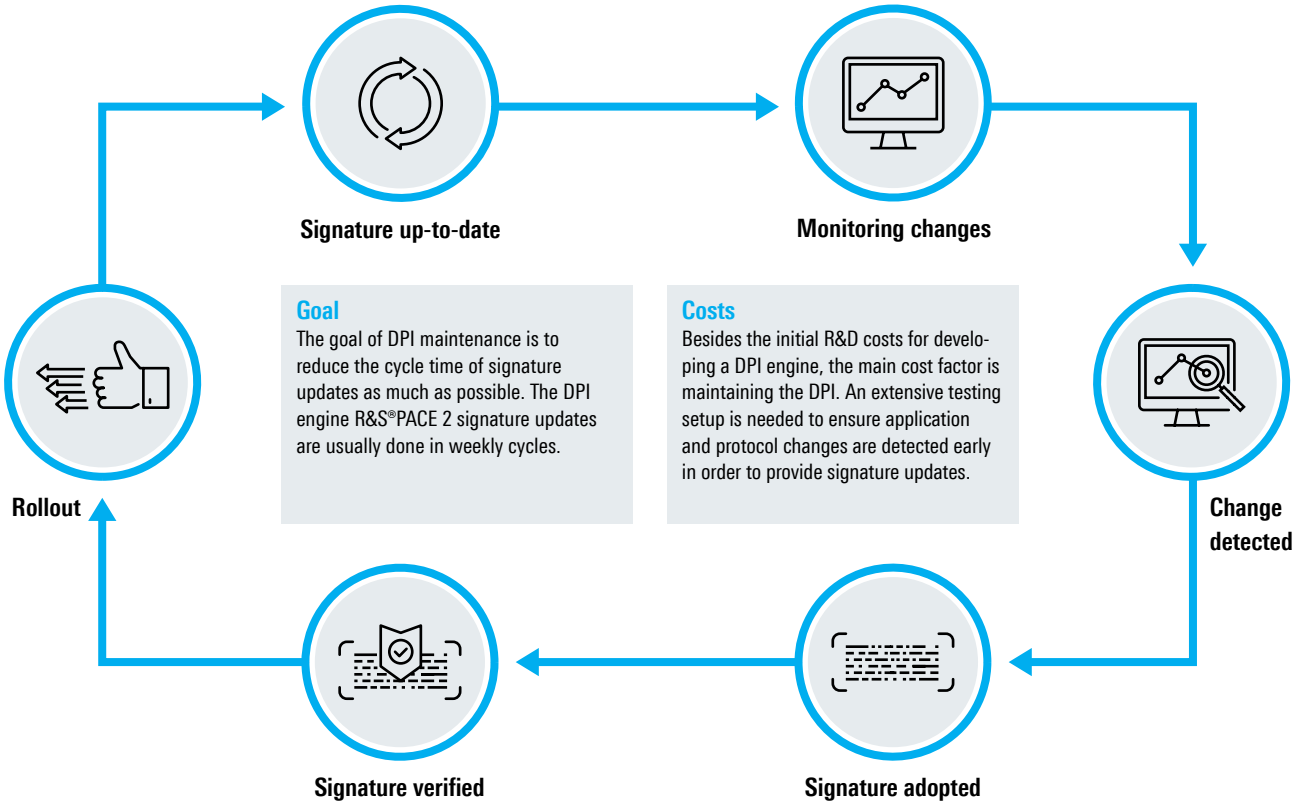
A big challenge for WAP vendors and Internet access providers trying to build in-house DPI would be the need to continually update the software with the latest applications and protocols so the security product is effective in managing threats and malware. A DPI engine is only as effective as its creators make it. The evolution of network traffic means that DPI software is never complete, with new applications and protocols continually appearing.

DPI software companies have dedicated DPI experts adding new application signatures on a weekly basis. This ensures that a high percentage of network traffic can be reliably classified, which is critical in the case of security and network management vendors that need to make accurate decisions on reliably classified traffic. As a result of ongoing performance and reliability testing, regular improvements can be made to the software to ensure all applications are detected.

Vendors may consider open source DPI with the idea that it is free to use. However, there are some important considerations – both pro and con – to adopting an open source DPI library. Open source software often ends up not being free, because it still requires in-house developers to learn about the software and, more importantly, to customize it. Frequently, this requires working with a third-party vendor to manage and add new features.

Most WAP vendors simply do not have the in-house resources to track and classify the latest apps and protocols. In a typical integration, the WAP application usage data is linked directly to third-party analytics systems that deliver reports and dashboards about data consumption. Ready-to-use software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally.

Rohde&Schwarz Cybersecurity ensures up-to-date signatures



DPI Done Better

WAP vendors need to deliver behavioral, heuristic and statistical analysis to reliably detect network protocols and applications and extract metadata in real time. Rohde&Schwarz Cybersecurity's DPI solution for WAP applications is the easiest to integrate with both new and legacy products. The protocol and application classification engine R&S®PACE 2 offers the industry's most efficient memory and CPU utilization. Featuring the smallest processing footprint, this engine is ideal for low-power equipment including next-generation and legacy WAPs. R&S®PACE 2 only requires 410 bytes per flow, while using very little processing power (CPU-load) and no memory allocation during run time.

The R&S®PACE 2 software can be implemented in the user space or in the kernel space of the processor, reducing the impact on processing performance. This is of particular importance in legacy WAPs. The backwards-compatible R&S®PACE 2 software is an intuitive, highly flexible and platform-agnostic application programming interface (API) that speeds up integration and has no external dependencies. R&S®PACE 2 also simplifies upgrades by enabling automatic weekly signature updates without rebooting.

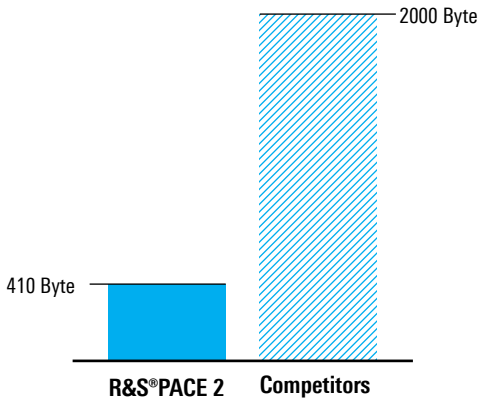
The R&S®PACE 2 software supports a wide range of operating systems and hardware architectures:

- Intel x86 (Linux, Solaris, FreeBSD, Windows)
- ARM (Linux, Android, BSD)
- Cavium Octeon (SE, BSD, Linux, HFA)
- PowerPC (Linux, BSD)

R&S®PACE 2 accurately identifies applications up to Layer 7 and provides the ability to manage network and application performance in real time. By integrating R&S®PACE 2, WAP vendors can keep up with the dynamic changes in protocols and applications, which ensures a high rate of detection for traffic management.

The R&S®PACE 2 software makes WAP metadata extraction, reporting and handling of information in real time easy. The modular DPI engine can be tailored to meet customer WAP system requirements including configurable event reporting to improve performance and customizable analysis that saves time and effort.

R&S®PACE 2 requires only 410 Bytes per flow



By embedding R&S®PACE 2 software into WAP devices, R&S®PACE 2 delivers a new revenue stream for Internet access providers. WAP vendors can offer enterprises and Internet access providers accurate, real-time insight into patrons' application usage and performance, key performance indicator (KPI) monitoring and trend analysis and quality of service and experience of users – all by segment and geography. These solutions need detailed and reliable information on protocols and applications – for example carrier VoIP and video as well as YouTube, Netflix etc. – and the ability to extract application metadata such as delay, packet latency, jitter, call completion on VoLTE or video.

Conclusion

Today's WAPs must offer high-performance wireless connectivity tailored to fit customer needs. Through DPI technology, WAP vendors can now deliver enterprise-class WiFi with the highest levels of performance and enhanced reporting capability. The flexible and customizable R&S®PACE 2 software simplifies integration of both new and legacy products. The DPI software allows WAP providers to monetize Wi-Fi networks via enhanced real-time monitoring capabilities that enforce QoS based on dynamic network conditions to prevent Wi-Fi congestion, enforce usage rules for personal devices once they are on the network and strengthen network security measures. The software is easy to implement and requires no in-house resources to track and classify the latest apps and protocols, simplifying the extraction of valuable metadata.

Service that adds value

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

Rohde&Schwarz Cybersecurity
Rohde&Schwarz Cybersecurity is an IT security company that protects companies and public institutions around the world against espionage and cyberattacks. With around 500 employees, the company develops and produces technologically leading solutions for information and network security. Development of the trusted IT solutions is based on the security-by-design approach for proactively preventing cyberattacks.

Rohde&Schwarz
The Rohde&Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-223
Email: cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

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

PD 5215.3985.62 | Version 01.01 | November 2017 (sch)
Deep Packet Inspection for Wireless Access Points: Analyze. Control. Secure.
Data without tolerance limits is not binding | Subject to change

5215398562

5215.3985.62 01.01 PDP 1 en