DEEP PACKET INSPECTION

SD-WAN AND DPI

A POWERFUL COMBINATION FOR APPLICATION-DRIVEN NETWORKING

ROHDE&SCHWARZ

Make ideas real

CONTENT

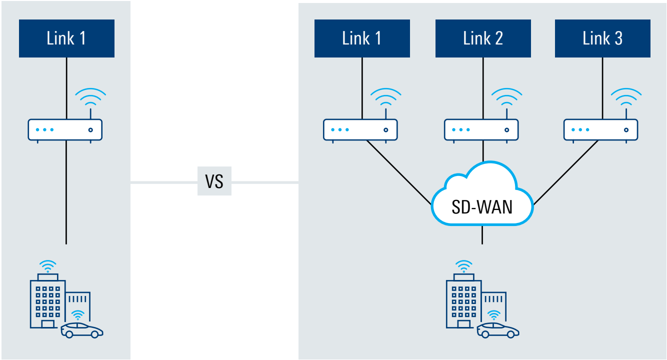
1. DEFINING SD-WAN

The software-defined wide area network (SD-WAN) is a specific application of software-defined networking (SDN) technology applied to WAN connections that are used to connect enterprise networks, including branch offices and data centers, over large geographic distances.[1]

SD-WANs are gaining traction with enterprises looking for more flexible and cost-effective WANs that support multiple transport modes suitable for every site: internet, DSL, Ethernet or MPLS. A separate control and data plane offers companies a programmable network with more flexible traffic management, independent of the chosen transport mode. Network and IT departments have long wanted direct control over policy and routing of applications to assure apt performance. This becomes even more critical in times when companies increasingly rely on cloud applications hosted by private data centers or public cloud providers such as Amazon Web Services.

For managed service providers such as AT&T, Orange, Deutsche Telekom etc., an SD-WAN presents an opportunity to add network as a service to their portfolio, but also to attract commercial customers with valuable network management, application analytics and security tools.

TRADITIONAL WAN VERSUS SD-WAN



Up-and-coming SD-WAN vendors such as Versa Networks or Nuage Networks are introducing new solutions to the market while vendors from related business fields such as Riverbed or Infovista are also entering the SD-WAN field. Even established routing vendors like Cisco are redefining their portfolio to react to market demands by acquiring startup SD-WAN vendors such as Viptela. As with any new market, there are multiple facets of an SD-WAN: It is a single virtual network function (VNF) and can be delivered as part of virtual customer premises equipment (vCPE) or universal CPE (uCPE). It can also be delivered alone on a lightweight appliance and may or may not replace legacy CPE.

In combination with vCPE, an SD-WAN is already one of the leading use cases of network functions virtualization (NFV). NFV is an architecture where VNFs are run on standard equipment (x86 servers). uCPE is a platform on which multiple VNFs can be delivered. This architecture allows companies to rapidly deploy functionalities to branch offices. uCPE supports VNFs such as SD-WANs, WAN optimization, firewalls, SIP trunking or routing. Being able to provide multi-vendor VNFs is very useful for managed service providers. For example, an SD-WAN could be combined with next generation firewalls, intrusion detection or prevention, unified communications etc. and delivered to a branch office in a single grey box. An SD-WAN as a strategic NFV application can be a massive opportunity for managed service providers, but only if they are able to add value beyond their services. For SD-WAN vendors, the market is heating up. This is why it is of critical importance to be able to offer advanced features such as application analytics for policy and security so that service providers can build features to match them.

This paper explores the market trends, challenges and opportunities for vendors in the SD-WAN field. Then it highlights the key value of deep packet inspection (DPI), which is in providing application visibility as the driving factor for dynamic path selection, application performance management and advanced security.

WHAT IS AN SD-WAN?

Gartner says SD-WANs have four characteristics:

Must support multiple connection types
MPLS, internet, LTE etc.

Can do dynamic path selection
Allow for load sharing across WAN connections

Provide a simple interface for managing WAN
Must support zero-touch provisioning at a branch site and should be as easy to set up as a home Wi-Fi

Must support VPNs
And other third-party services such as WAN optimization controllers, firewalls, web gateways etc.

[1] https://www.sdxcentral.com/sd-wan/definitions/software-defined-sdn-wan

2. SD-WAN MARKET TRENDS AND OPPORTUNITIES

The SD-WAN market is growing fast with increasing commercial interest and adoption plans. Growing competition among SD-WAN vendors means that SD-WAN solutions need features and capabilities that differentiate them from competitors. With startup vendors competing against traditional CPE and network vendors as well as others from related industries that are entering the SD-WAN field, it will be critical to offer more than just path selection and improved WAN management.

Companies now provision Network on Demand solutions that support dynamic application service level agreements (SLAs). This poses new challenges to service providers and SD-WAN vendors, as they will need to supply tools such as customer management portals that offer full visibility into network and application performance on a real-time basis. These can be a key point of difference. For example, companies might want to take advantage of video conferencing without over-provisioning bandwidth. With an SD-WAN, they can increase their bandwidth temporarily and then turn it down again.

Another trend is uCPE, which accelerates branch office deployment by bringing offices online quickly. uCPE also simplifies the IT infrastructure without requiring different CPE and equipment for SD-WANs, firewalls, intrusion detection or prevention, WAN optimization etc. Instead, these can be provisioned as software-based VNFs. SD-WANs, next generation firewalls and WAN optimization may still be required in the branch office, but companies want more flexibility in deploying and consuming network functions as needed rather than having them all on a single platform.

Market opportunities

The opportunity to provide enterprises with additional services such as security, application monitoring and application optimization beyond basic connectivity is a compelling value proposition of an SD-WAN. More service providers will offer an SD-WAN as a managed service, as well as resellers, system integrators and IT service companies that are looking to expand their service range by giving companies more choices. The digital transformation will require network infrastructures to seamlessly connect any user to any application. This will require an SD-WAN to work across the branch sites, campus, data center and the cloud with open and programmable architectures for vendor interoperability. Unified application delivery across the company will require centralized management, application visibility and monitoring to ensure greater agility, uniform security and an improved overall quality of experience for all users.

We also expect to see managed service providers increasing the value of SD-WAN services through real-time application visibility, advanced performance analytics and reporting. This could happen in the form of reports to companies' IT departments on the performance of applications on the WAN, suggestions etc.

For example, U.S. provider Windstream's SD-WAN service Concierge intends to "flip the service provider model on its head" by proactively offering IT departments an assessment of application performance over the network and, in many cases, helping identify unknown or rogue applications in the process. How networks consume bandwidth and how users perceive the applications' quality of experience (QoE) will have greater significance. Another SD-WAN service provider is offering a dedicated technical service manager that helps monitor, analyze and prioritize companies' real-time business communication services and optimize application performance.

SD-WAN also represents the first major SDN-based product offered by cable providers. It is poised to become a leading-edge product in cable providers' portfolios tailored to attract large companies and multi-site enterprises, helping them to increase their market share. SD-WANs provide a platform to layer VNFs that cable providers are exploring.

Besides cost and performance benefits, advanced SD-WAN security and analytics are important USPs, helping providers to differentiate themselves from competitors. Most SD-WAN vendors offer encryption for branch-to-branch corporate traffic using IP Sec, which protects data in transit. However, in order to ensure holistic security, securing the edge is critical. Providers are increasingly offering firewall VNFs at branch sites, intrusion detection and prevention systems (IDS/IPS), quarantine or other deflection of detected malware, and web filtering. All of this protects against break-ins, man-in-the-middle attacks and malware that can cause denial of service or data theft.

3. HOW DPI ENABLES APPLICATION-DRIVEN SD-WAN FEATURES

SD-WAN vendor solutions rely on an integrated DPI library of applications and protocols to identify and analyze the traffic running on their networks in real time.

DPI enables an SD-WAN to identify the application and application family types. The number of bytes of incoming and outgoing traffic is recorded for every application. This data can be viewed in a centralized management portal or customer dashboard at the defined polling interval. It can also be displayed as reports.

Application statistics enable companies to view detailed information on incoming and outgoing traffic as well as the top applications, sites, and application families as reports. This provides a holistic view of network bandwidth usage, a feature that IT departments have a strong demand for. Besides the real-time discovery and classification of applications, SD-WAN solution vendors and service providers can opt to enable DPI at particular sites or across all sites.

This application visibility and control can be useful to secure and segment traffic. For example, regional internet exit points can break out specific applications rather than backhauling all traffic to a data center. This can be particularly useful in case of security breaches. In addition, once a packet is classified, the application identifier can be used in a firewall filter as a match criterion to identify this type of traffic.

3.1. Application-driven policy

A further selling point of an SD-WAN is intelligent path control, which means that even if a network link is down, mission-critical enterprise applications can be rerouted without loss of performance. This is increasingly attractive to enterprises that are using third-party cloud application providers, e.g. Microsoft, Salesforce, Amazon Web Services etc., companies with a high number of mobile workers and distributed companies such as banks or retailers with many small sites and branch offices.

A DPI-enabled SD-WAN with application visibility and real-time data is required to support:

- Fine-grained policies on a per-application basis
- Dynamic, application-aware and performance-based routing
- QoE and performance of applications, particularly cloud applications that businesses are increasingly dependent on (e.g. Office 365)
- Application SLA enforcement — SLA management of an application or service type based on latency, jitter, packet loss and voice mean opinion score (MOS)

3.2. Application visibility and performance control

Business customers want to be in control of their application and performance management (APM). DPI can help collect and closely monitor metrics that are relevant to application performance monitoring:

The first set of performance metrics defines the performance experienced by end users of the application. One example metric of performance is the average response times under peak load. The components of the set include load and response times. The second set of performance metrics measures the computational resources used by the application for the load. This metric set indicates whether enough resources are available to cope with the load and if there are possible performance bottlenecks. Measuring these variables establishes an empirical performance baseline for the application.

A customized dashboard UI can provide easy access to these metrics as well as other application and traffic routing data (SLA-based, application policies, routes, sites).

Highly granular application identification allows for strong traffic engineering policies. For example, a specific website such as Facebook could automatically trigger the use of URL filtering policies and the assignment of broadband connectivity only.

> “SD-WAN vendor solutions rely on an integrated deep packet inspection (DPI) library of applications and protocols to identify and analyze the traffic running on their networks in real time.”

3.3. Overview: DPI-enabled SD-WAN features

Feature	Benefit
Application visibility by site, app or app family	Identify over 3000 applications and be able to manage quality of service (QoS) and application security.
Application performance — per app, per session, per site	Gain insight into application delivery in order to proactively manage user experience with computed statistics in real time (e.g. MOS for VoIP).
Traffic management — inbound and outbound	Gain insight into application traffic and bandwidth usage and support secure cloud migration at branch offices.
Per-app policy control	Prioritize mission-critical apps — in case of bandwidth limitations, these apps can be dynamically routed with the fastest available transit time. Closed-loop automation maintains high performance for mission-critical enterprise apps, even if a link fails. High-bandwidth apps can be balanced across multiple links to provide steady performance for large file transfers.
Application-level security	Identify potentially malicious traffic and anomalies, prevent data leakage and receive actionable security information in real time (e.g. forged or corrupted files are automatically identified). Enhance security and enable direct connections from branch offices to cloud internet and software as a service (SaaS) applications. Secure data with application-level visibility, security policies and data segmentation.
Application WAN optimization	A range of techniques such as TCP flow control, data compression, deduplication and protocol optimization improve end-user experience and optimize bandwidth.
Management and visibility	Report application delivery to users in the branch office for monitoring and managing portals. Export data to third-party applications that offer insight into networks and applications.
Hybrid WANs (MPLS and internet)	Based on the underlying network infrastructure — MPLS or internet site — map each application to the best path through the network and ensure high quality and a secure user experience.

4. HOW DPI ENABLES ADVANCED SD-WAN SECURITY

DPI adds an additional layer of protection to SD-WANs. This is required because many organizations are connecting their branch offices directly to the internet, which risks exposing them to more security threats even though the SD-WAN features a secure overlay. DPI provides full application visibility and control to segment branch offices from the WAN to prevent attacks on any branch from spreading across the entire company.

When paired with DPI, service chaining provides an effective way of securing SD-WAN networks. By means of DPI, traffic is collected from the edges of a network. Service chaining supports this by merging multiple security functions into a single, centralized hub that analyzes the traffic and identifies threats.

Deploying an SD-WAN in combination with proprietary or third-party software-based security VNFs further secures the WAN and internet perimeters without the need for additional hardware. DPI grants application visibility, supporting software-based VNFs for unified threat management such as stateful and next-generation firewalls, virus and malware protection, URL and content filtering, DDoS mitigation and IPS. DPI application visibility also prevents firewalls from accepting malicious traffic and any attempts to sneak malware through the gates unseen.

> “DPI provides application-level visibility for traffic leaving the branch perimeter, and this capability can accelerate the response to attacks by enabling the definition of dynamic policies for branch traffic based on L7 traffic analytics.”

Overview: enhanced SD-WAN security enabled by DPI

Feature	Benefit
Application visibility for next-generation firewalls	Policy rules based on application identity, IP blacklisting, whitelisting, geo-IP and customer app ID signatures; protection based on firewall SSL certificates, expired certificates, untrusted CAs, unsupported cyphers and key lengths.
Application visibility and control to segment traffic	Segment branch traffic and apply individual security policies to each segment. Create multiple virtual private networks (VPNs) on top of a single fabric to functionally segregate different types of traffic between private and public cloud environments. Steer traffic from a remote hub to a regional hub for inspection. Supports various treatments of client applications using encryption, e.g. surveillance, PCI and load balancing between circuits.
Multi-layered security at the application level	Supports predictive network analytics and unified threat management such as threat profile reports: URL filtering and captive portal actions, IDS/IPS, antivirus, SSL certificate anomalies, packet capture for known or unknown applications and detected vulnerabilities etc.

5. ENCRYPTED TRAFFIC ANALYTICS

An increasing number of protocols and applications is encrypted, such as Skype, WhatsApp, BitTorrent, Facebook, Twitter, Dropbox, Gmail, Office 365 and Instagram. Additionally, some protocols such as Tor, Freenet and other P2P apps such as Ultrasurf and Your Freedom can adapt to circumvent firewalls and DPI detection, for example, when traffic generated by a specific protocol is limited or blocked.

Most encrypted connections on the internet are using transport layer security (TLS) or secure socket layer (SSL) for encryption. Both technologies are established with a handshake. All information that is necessary to classify a protocol application is transferred with this handshake.

While it is still possible to classify an encrypted application, end-to-end encryption entirely prevents metadata extraction. This means that there can be no insight into the content of a message.

The OEM DPI software R&S®PACE 2 delivers reliable classification results with a very low false negative rate and virtually no false positives, regardless of end-to-end encryption. This is achieved through a variety of detection techniques:

Pattern matching: scanning for strings or generic bit and byte patterns anywhere 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, the number of flows and the new flow rate per application.

Statistical analysis: calculating statistical indicators that can be used to identify transmission types (e.g. real-time audio and video, chat or file transfer), including mean, median and variation of values collected as part of the behavioral analysis, and the entropy of a flow.

Statistical and behavioral analytics provide the foundation for metrics and heuristics such as packet sizes, packet timing, latency, throughput, entropy and jitter. Network performance metrics are especially important in security applications, as many sophisticated applications such as VPNs can only be detected by combining various metrics with specific session behavior. For example, packet sizes and packet timing are used to distinguish between messaging and file transfers in encrypted messaging apps such as Skype.

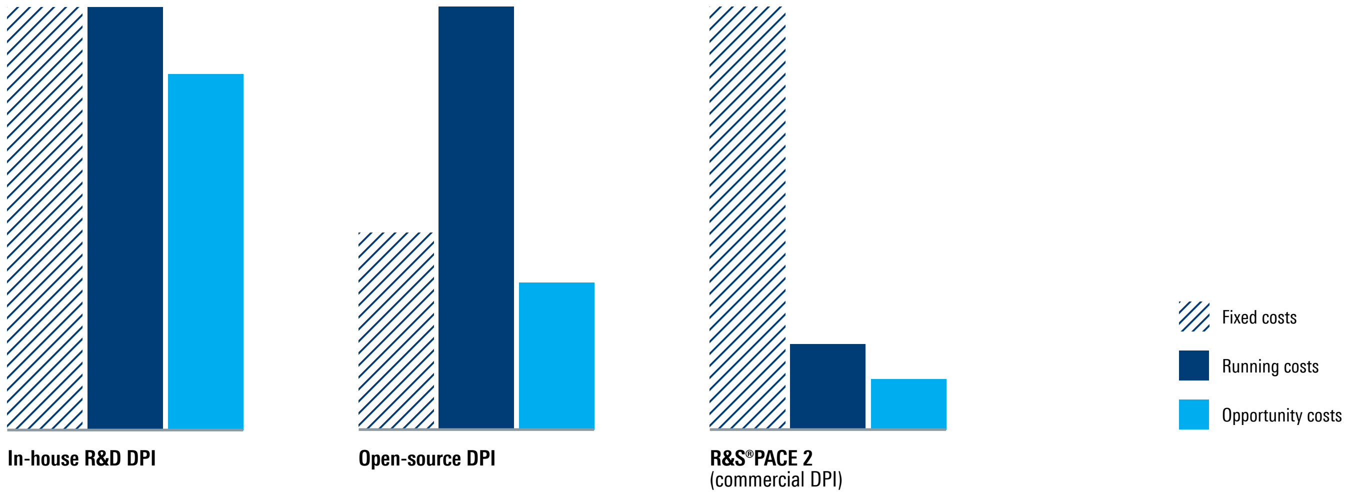
> “DPI can gather information about encrypted or obfuscated applications and protocols by using heuristic methods.”

DPI-extracted metadata from encrypted and unencrypted traffic

Metadata category	Example metadata
Traffic volume	Per user, per protocol, per application, per flow, per direction
Service detection	Differentiation between e.g. Skype audio and video calls
Quality of service	Jitter, throughput, latency, round-trip time, ramp-up time, packet loss, retransmissions
Security and data leakage	File up- and downloads, entropy-based DNS tunneling detection, prevention
Client information	HTTP/QUIC user agents, operating system

6. BUILD OR BUY DPI?

COMMERCIAL DPI REDUCES DEVELOPMENT COSTS



SD-WAN vendors rely on DPI application awareness as a key feature for policy control, critical traffic steering and application security. Consequently, they have to make a strategic choice between building in-house DPI libraries and licensing software from a DPI specialist.

A major challenge for SD-WAN vendors trying to build in-house DPI is the need to continually update their software with the latest applications and protocols so the SD-WAN can offer up-to-date network traffic visibility. A DPI engine is only as effective as its creators design it. The evolution of network traffic with new applications and protocols emerging nonstop means that DPI software is never complete.

DPI software companies have dedicated DPI experts that add new application signatures on a weekly basis. This ensures that a high percentage of network traffic can be reliably classified, which is critical for SD-WAN solutions that need to make policy and routing decisions on the basis of reliably classified traffic. As a result of continuous performance and reliability testing, regular improvements can be made to the software to ensure that all applications are detected.

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

Most SD-WAN vendors simply do not have the in-house resources to track and classify the latest apps and protocols. Ready-to-use DPI software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally. Instead, SD-WAN vendors can spend their valuable time and resources on their core products in what is proving to be a highly competitive market.

> “Ready-to-use DPI software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally.”

7. DPI ENGINE BY ROHDE & SCHWARZ

SD-WAN vendors need to integrate behavioral, heuristic and statistical analytics to detect network protocols and applications reliably and extract metadata in real time. The DPI solution from Rohde & Schwarz for SD-WANs is the easiest to integrate, whether on an SD-WAN appliance or an SD-WAN vCPE platform. The R&S®PACE 2 protocol and application classification software offers the industry's most efficient memory and CPU utilization, featuring the smallest processing footprint. R&S®PACE 2 only requires approx. 400 bytes per flow while using very little processing power (CPU load) and no memory allocation during runtime.

The R&S®PACE 2 OEM DPI software can be implemented in the user space or the kernel space of the processor, reducing the impact on processing performance. The backwards-compatible R&S®PACE 2 engine has 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.

R&S®PACE 2 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)
- MIPS (Linux, BSD)

R&S®PACE 2 identifies applications up to Layer 7 of the OSI model accurately and makes it possible to manage network and application performance in real time. By integrating R&S®PACE 2, SD-WAN vendors can keep up with dynamic changes in protocols and applications, ensuring a high detection rate in traffic management.

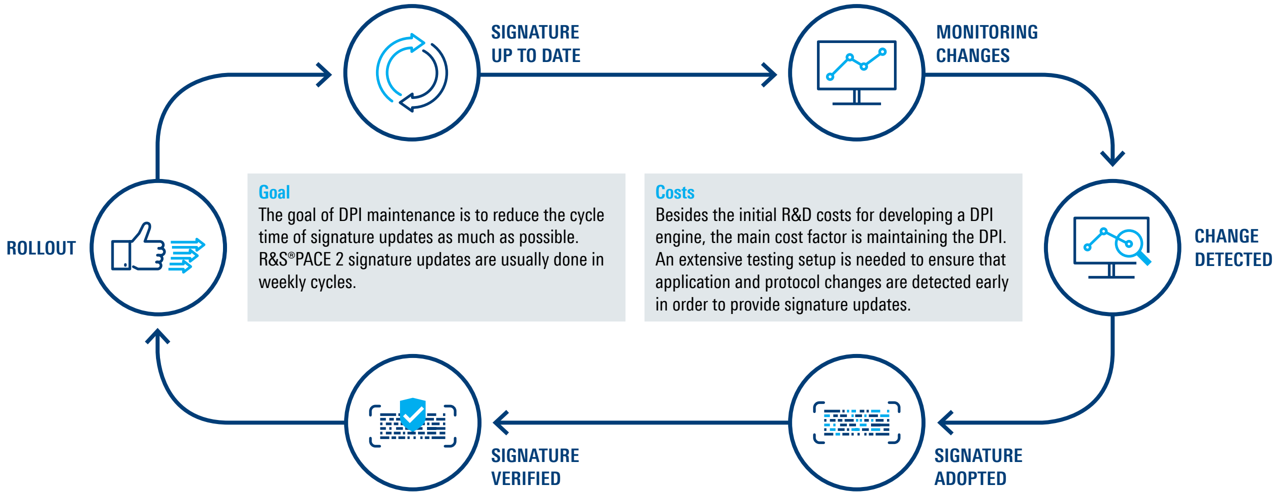
The R&S®PACE 2 software makes it easy to extract metadata and to report and handle information in real time. The modular DPI engine can be tailored to meet customer SD-WAN requirements including configurable event reporting to improve performance and customizable analysis that saves time and effort.

Customers also find many benefits from sourcing the DPI engine R&S®PACE 2:

- Weekly protocol and application signature updates
- Highest classification accuracy in the DPI market
- Focus on core competencies to become more efficient and profitable
- Faster time to market through optimized development schedule
- Reduced and optimized development costs by outsourcing DPI
- Maximized return on investment (ROI)

Rohde & Schwarz is recognized globally as a leading developer of DPI software. They have more than 10 years of expertise in optimizing the performance of network equipment and software vendors around the world.

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.

8. SUMMARY

The SD-WAN market is growing fast, and so is the competition. SD-WAN vendors need DPI to support critical features such as real-time application visibility and enhanced security features and analytics. This also caters to commercial customers' use cases. One example is the visualization of and reporting on application performance and security diagnostics at key customer sites and cloud data centers. With the help of DPI technology, SD-WAN vendors can now deliver intelligent routing, traffic steering and enterprise application performance with advanced reporting capability. However, cost and performance benefits are meaningless without strong end-to-end security. DPI offers an exponentially growing amount of information on the network and plays a key role in providing critical information on the health and performance of the network. The accuracy of the data and the frequency of data collection will also drive automation and efficiency in network management and enable more predictive application and security policies.

The SD-WAN market is highly competitive. Vendors cannot compete if they do not lower their development costs. Lowering costs is especially important when competing with service providers that want a piece of the fast-growing market and rapidly gain access to enterprise customers. Sourcing DPI can enable both: reduction of development costs and market differentiation by partnering with a dedicated DPI expert who has more than ten years of experience in the traffic analytics business.

The flexible and customizable R&S®PACE 2 software simplifies integration with on-premise and cloud-based SD-WAN products. The DPI software allows SD-WAN providers to further enhance real-time monitoring capabilities and intelligent routing based on dynamic network conditions and to strengthen application performance SLAs and 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.

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, Germany
Info: + 49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 5216.1170.52 | Version 02.00 | July 2020
White paper | DPI and 5G
Data without tolerance limits is not binding | Subject to change

5216117052
5216.1170.52 02.00 PDP 1 en