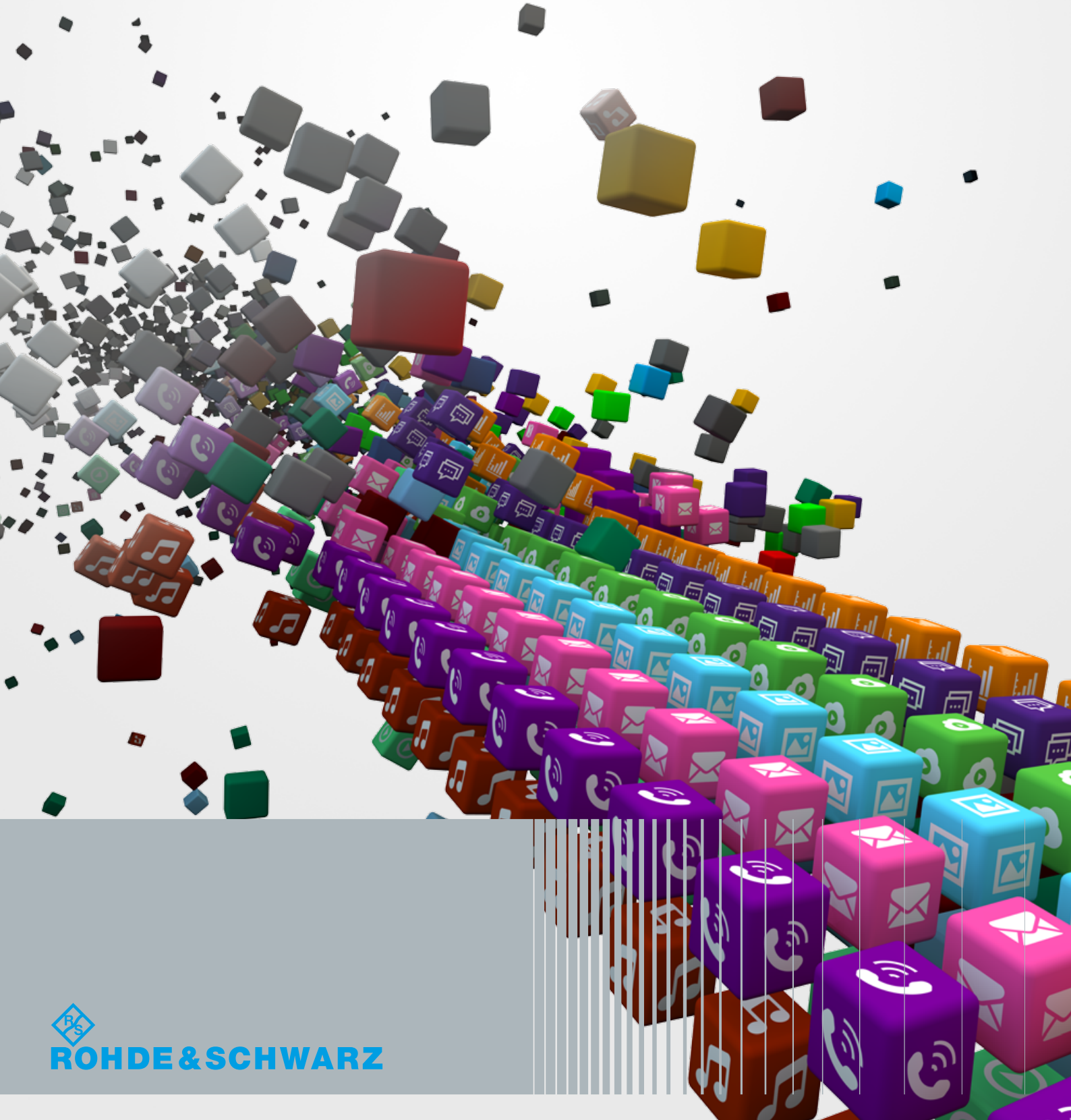
# R&S®PACE 2
# Solution Guide



ROHDE&SCHWARZ

# Contents


**1. Introduction** ..... 3
Key Benefits of R&S®PACE 2 ..... 3

**2. R&S®PACE 2 as an OEM solution** ..... 4
2.1 Integration ..... 4
2.2 Performance ..... 4

**3. Architecture overview** ..... 5
3.1 Packet Preparation ..... 5
3.2 Packet Reordering ..... 6
3.3 Packet Classification ..... 6
3.4 Packet Decoding ..... 6
3.5 Timeout Handling ..... 6

**4. Protocol and application classification** ..... 7

**5. Ensuring classification accuracy** ..... 9

**6. Handling encryption** ..... 10

**7. Metadata extraction** ..... 11
7.1 Performance Metadata ..... 11
7.2 Protocol and Application Metadata ..... 12

**8. Content decoding** ..... 13

**9. Additional features** ..... 14
9.1 Dynamic Upgrade ..... 14
9.2 OS Detection ..... 14
9.3 NAT/Tethering Detection ..... 14
9.4 Client Server Indication ..... 14
9.5 Unidirectional Traffic Support ..... 14
9.6 Customization ..... 14
9.7 Fastpath ..... 14

**10. Performance testing** ..... 15
10.1 Test Data ..... 15
10.2 Single Thread Tests ..... 15

**11. Service and support** ..... 16
11.1 Product Evaluation ..... 16
11.2 Maintenance ..... 16
11.3 Customer Portal ..... 16
11.4 Training ..... 16

**12. Use cases** ..... 17
12.1 Network and Traffic Management (QoS/QoE) ..... 17
12.2 Policy Control and Charging ..... 17
12.3 Network Security (Firewalls, IPS/IDS, SIEM, UTM) ..... 18
12.4 Network and Subscriber Analytics ..... 18
12.5 Mobile Data Offload ..... 18
12.6 WAN Optimization ..... 19
12.7 SDN/NFV Environments ..... 19

# 1. Introduction

Network infrastructure and security vendors increasingly need a deeper understanding of applications and IP network traffic. This network visibility is important with the move to LTE mobile networks, combined with the high growth in mobile apps, cloud computing and video traffic. Vendors are embedding realtime application awareness in their solutions to enable their customers to better manage performance, improve the end user experience as well as secure applications end-to-end.

**R&S®PACE 2 solution is integrated by vendors to enhance their products with state-of-the-art protocol and application awareness capabilities.**

R&S®PACE 2, is a software library using different technologies - deep packet inspection, behavioral, heuristic and statistical analysis - to reliably detect network protocols and applications and extract metadata in realtime. R&S®PACE 2 can accurately detect network protocols and applications, even if they use advanced obfuscation and encryption techniques. R&S®PACE 2 is integrated by network equipment and security vendors to enhance their products with state-of-the-art protocol and application awareness capabilities. Designed by developers with years of experience in Layer 7 protocol and application awareness, R&S®PACE 2 can be deployed in a variety of use cases including Network Security (IDS/IPS, Next Generation Firewalls, SIEM, UTM), Network Monitoring and Traffic Management, Policy and Charging, Application Delivery and Optimization, Analytics, and Mobile Data Offload.

## Key Benefits of R&S®PACE 2

- Time to Market and Save Costs - reduce development time and CapEx and OpEx by licensing R&S®PACE software including updates and maintenance
- Easy and Fast Integration - highly flexible API for integration, platform-agnostic, no external dependencies
- Fast Performance - throughput average of 4Gbps per core
- Highly Efficient - most efficient memory consumption on the market
- Accuracy and Reliability – classifies over 95% of network traffic (no false positives)
- Coverage - support for thousands of protocols and applications across diverse operating systems, application versions and service types.
- Metadata extraction - deeper insight on application attributes e.g., QoS/QoE KPIs on network performance and applications such as VoIP and video, etc.
- Stay Current – frequent signature updates, including new additions to classification library
- Deployed Globally as OEM – deployed in global mobile networks which provides better visibility and detection rate of applications

# 2. R&S®PACE 2 as an OEM solution

## 2.1 Integration

R&S®PACE 2 software is platform-agnostic (hardware/software) and runs in any Linux, Mac, Solaris and Windows environment, accessible via C interface. The software is developed in-house by ipoque engineers and fully documented APIs including code samples are provided. The software kit includes ipoque's powerful network traffic test tool, which double-checks the validity of an integration and provides a deeper understanding for further use-cases.

## 2.2 Performance

R&S®PACE 2 is developed entirely in C to deliver high performance including optimized code for high-end multicore technology. Multi-threading provides almost linear scalability on multi-core systems. Also integrated is highly-optimized flow tracking to support millions of concurrent connections.

**Integration is easy with fully documented APIs including code samples.**

| PACE fast facts | |
|---|---|
| **CPU Architecture** | Basically no restrictions, optimized for Intel x86 |
| **Operating System** | Basically no restrictions, optimized for Linux |
| **Performance** | 4 Gbps per core on average |
| **Meta Data Extraction** | yes |
| **Full Content Decoding** | yes |
| **Service** | Professional services, Design, Build and Run |
| **Protocol/Application Coverage** | 2,000 + , around 95% recognition |
| **Protocol/Application Updates** | Frequent dynamic signature updates, at minimum on monthly basis |
| **Memory Footprint** | Library: no memory for initialization, per subscriber: <900 B, per flow: <400 B; |
| **APIs** | C |

# 3. Architecture overview

R&S®PACE 2 combines detection, decoding and the related packet processing components into a single unified library. A polling API is used for packet processing and meta data extraction. This allows for easier integration without the need for callbacks. Flow and subscriber tracking may also be handled internally by the library or externally. Each stage can be configured so that it is possible to enable or disable features such as packet reordering or defragmentation without the need for code changes. After the "Packet Classification", "Packet Decoding" and "Timeout Handling"stages, a list of metadata events is provided for processing. The "Packet Decoding" stage is completely optional and does not need to be called if the advanced metadata option is not required. The R&S®PACE 2 flow is divided into different stages which are called one after another.
The stages are used in the following order:

1. Packet Preparation
2. Packet Reordering
3. Packet Classification
4. Packet Decoding
5. Timeout Handling

## 3.1 Packet Preparation

The packet preparation is a per-packet based operation and involves building up the frame stack, protocol decapsulation and IP defragmentation. The output is a single packet, which can be processed by the following stages.

### Protocol Decapsulation

R&S®PACE 2 needs access to the IP packet.
The required components are:

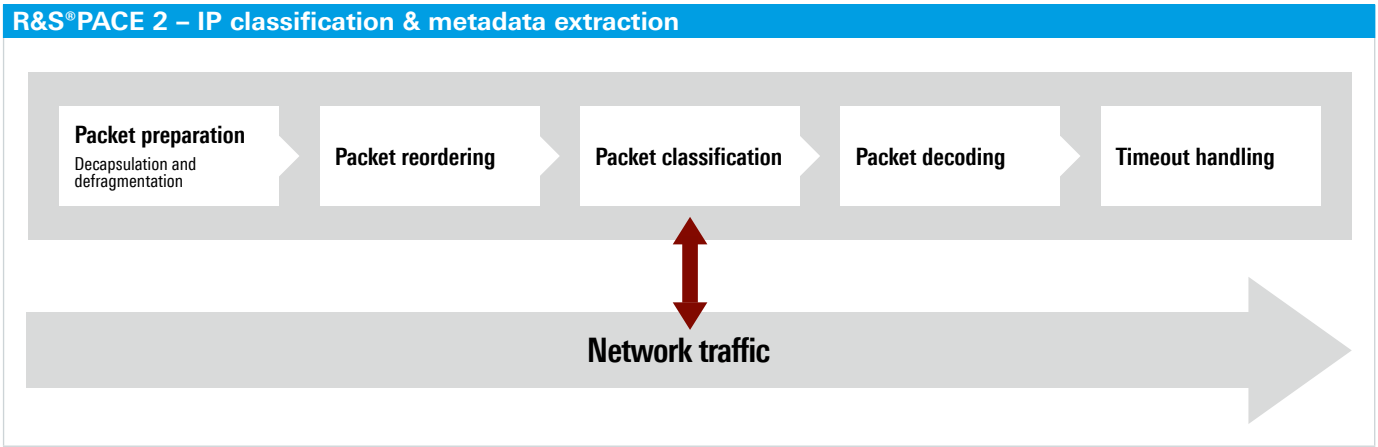
- Pointer to IP header
- Accessible length of the packet starting from the IP header
- Packet time stamp

### IP Defragmentation

The IP Defragmentation engine is used to reassemble fragmented IP packets from Layer 3 to Layer 7. The packet classification expects no fragmented IP packets in order to reliably classify all the protocols and applications from the IP traffic. The IP defragmentation engine helps to transform the IP flow which is key for better detection results.

**R&S®PACE 2 restructures IP packets, if required, which is key for better detection results**

**R&S®PACE 2 – IP classification & metadata extraction**



# 3. Architecture overview

## 3.2 Packet Reordering

TCP Packets can be optionally reordered by the packet reordering engine. The engine will buffer out-of-order packets until the missing packets arrive or a specific timeout occurs. With the help of packet reordering, the detection classification rate will be improved.

**Flow/Subscriber Tracking**

For the reordering to work it is required to do flow tracking before calling this stage. The state of every TCP and UDP flow is maintained along with internal values. The process to get the flow information can be split into three phases:

1. In the first phase, the unique 5 tuple must be created.
2. The second phase inserts this into a connection tracking table.
3. When the insert has created a new entry, it has to be set to zero in phase 3.

A similar state buffer is maintained for every subscriber. In most situations, a subscriber is identified by an internal IP address.

## 3.3 Packet Classification

The packet classification stage provides the protocol and application detection results, as well as network performance metadata. The packet classification is the core intelligence of the library and includes a high number of different protocol and application detections.

## 3.4 Packet Decoding

Packet decoding provides advanced metadata as well as content decoding. If the R&S®PACE 2 decoding stage is used, it is possible to extract more detailed metadata in real time, for example, entire email messages or compressed HTTP payload contents. It is also possible to decode social network content such as ICQ buddy names, group activities or sent messages.

## 3.5 Timeout Handling

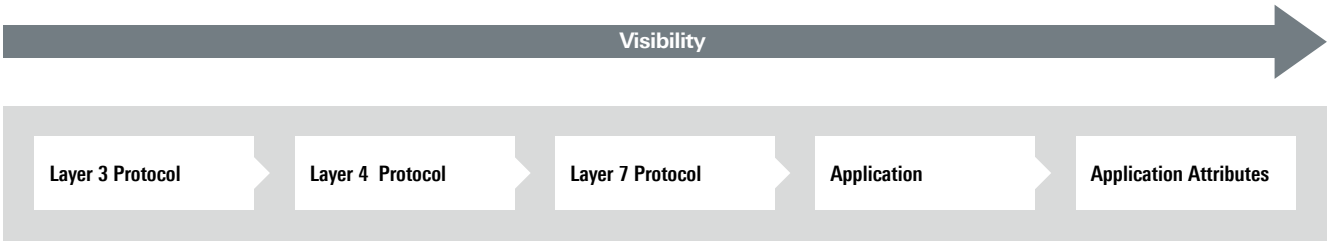
This stage primarily provides timeout events from the decoder and should be called even if the current packet was buffered in the Packet Reordering stage. If internal flow or subscriber tracking is used these timeout events will be returned by this stage as well.

**R&S®PACE 2 analyzes network data in realtime, providing accurate detection of today's most popular applications.**

# 4. Protocol and application classification

R&S®PACE 2 software engine inspects and analyzes network data in realtime, providing accurate detection of today's most popular applications with the ability to extract metadata and application attributes from the network traffic. Different technologies such as deep packet inspection (DPI), behavioral, heuristic and statistical analysis are used to analyze the IP packet in order to determine the protocol and application and other application based attributes of the traffic.

## From Layer 3 to Layer 7 and above




Delivered as a software developer kit (SDK), R&S®PACE 2 provides advanced protocol and application classification designed for quick integration into network infrastructure and security platforms.

**R&S®PACE 2 is flexible in terms of how classification results are presented to support different use cases.**

R&S®PACE 2 accurately detects applications based on Layer 7 protocols (e.g. Skype, Facebook, Twitter, Dropbox), as well as detection of application client service functionality such as audio, video or file transfer for deeper insight. R&S®PACE 2 provides support for thousands of network protocols and applications. Frequent updates of protocol and application versions ensure ongoing reliable detection.

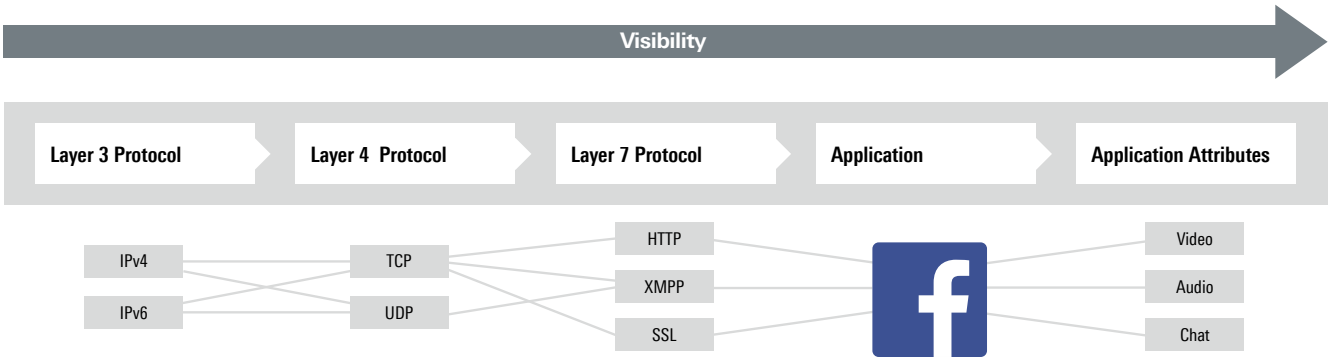
## Detecting the right things right

| | |
|---|---|
| **Layer 7 Protocols** | A Layer 7 Protocol is a network protocol located on the OSI layer 7 (application layer) which interact directly with the application. Layer 7 network protocols can be standardized, encrypted, or proprietary which can mean little or no network protocol information is available.<br>▪ Standard (e.g. HTTP, FTP, SIP, IAX, IMAP)<br>▪ Encrypted (e.g. SSL, SSH, IPsec, OpenVPN)<br>▪ Proprietary (e.g. MSN, OSCAR (Icq), Skype, UltraSurf, eDonkey) |
| **Application** | An Application is a specific software that causes a computer or mobile device to perform useful tasks for a wide range of application types. "Application detection" identifies computer programs that use Layer 7 protocols, e.g. Facebook, Twitter, Dropbox, Skype, etc. |
| **Application Attributes** | Application Attributes are used to classify the application in more detail, e.g. audio and video flows for VoIP applications such as Skype; chat and file transfer for instant messaging protocols e.g. ICQ. |

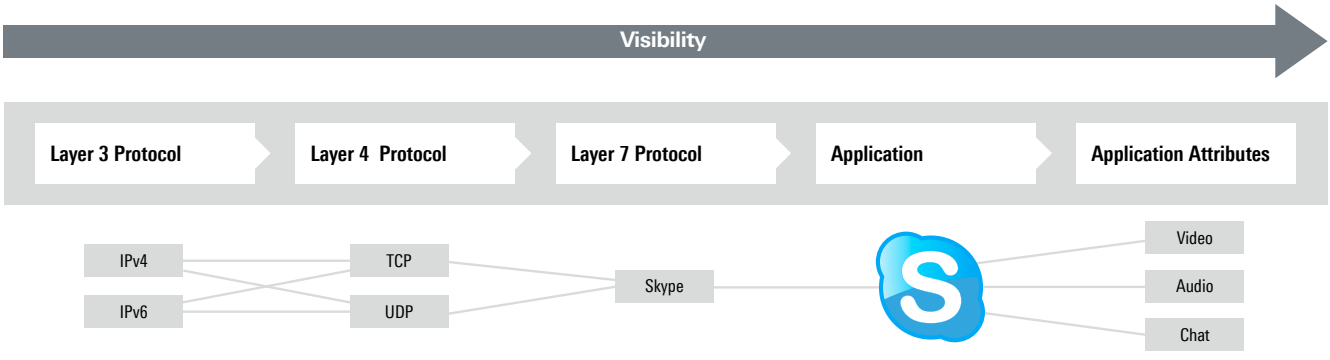
# 4. Protocol and application classification

Applications can be grouped into service types e.g. Video, Peer-2-Peer, VoIP, Instant Messaging, making it easier to analyze and enable intelligent traffic decisions. R&S®PACE 2 is flexible in terms of how classification results are presented to support different use cases.

## Example 1: Facebook




## Example 2: Skype



# 5. Ensuring classification accuracy

R&S®PACE 2 uses diverse industry-leading classification techniques to recognize network traffic including pattern matching and behavioral, heuristic and statistical analysis. This enables R&S®PACE 2 to reliably detect network protocols, even if they use advanced obfuscation and encryption techniques. R&S®PACE 2 is designed to minimize the false positive detection rate i.e. incorrectly identifying an application. In the area of billing, for example, it is critical to avoid false positives as that can have a real negative revenue impact and potentially damage the brand image of an operator. R&S®PACE 2 is also designed for traffic management, which requires a very low false negative rate i.e. low classification rate of applications. Based on performance tests on real traffic data, R&S®PACE 2 can accurately identify around 95% of network traffic.

**Using industry-leading classification techniques, R&S®PACE 2 can accurately identify around 95% of network traffic.**

ipoque issues signature updates on a frequent basis to ensure a high level of accurate application identification. Even small changes to protocols and applications can lead to problems with classification and since details for most application changes are not publicly announced, this requires constant attention. ipoque has a team of experts who live and breathe application protocols and are dedicated to monitoring and analyzing their patterns and behaviors 24/7. As a result of ongoing performance and reliability testing, regular improvements can be made to the software to ensure all applications are detected.

ipoque's database contains thousand of different traces for all supported protocols and applications. The database contains traces from ipoque since 2005 as well as anonymized test data from different customers, markets and regions. ipoque checks for changes to well-known applications on a weekly basis, especially frequent changing mobile applications.

# 6. Handling encryption

Increasingly many protocols and applications are encrypted e.g. Skype, WhatsApp, BitTorrent, Facebook, Twitter, Dropbox, Gmail, Office365, Instagram etc. In addition, some protocols such as eDonkey, Freenet and other P2P apps, Ultrasurf, YourFreedom can adapt to circumvent firewalls and DPI detection when for example traffic for a specific protocol is limited or blocked. R&S®PACE 2 can deal with this challenge because a variety of detection techniques are used including flow tracking, byte pattern matching and behavioral analysis.

1. Pattern Matching
   - Simple check for recurring string and numbers inside IP packets
2. Behavioral Analysis
   - Checks for packet sizes, order of different packet sizes within IP flow while tracking information of the subscriber and host
3. Statistical/Heuristic Analysis
   - Common appearances like recurring byte-order or metadata analysis within IP flow
   - In the most cases there are many different checks to ensure a reliable classification result
4. Finite State Machine
   - Set of specific requirements must be fulfilled for a classification result

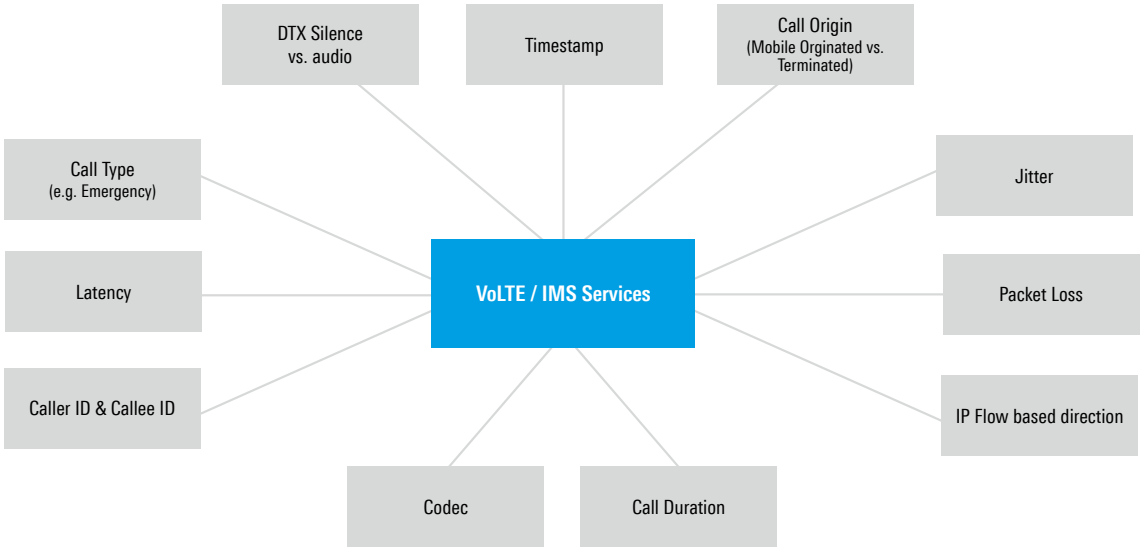
By combining all of these techniques, R&S®PACE 2 is able to reliably detect encrypted protocols with a very low false negative rate and virtually no false positives.

# 7. Metadata extraction

## 7.1 Performance Metadata

R&S®PACE 2 includes functions to measure the TCP performance, for example, the round- trip time between SYN-SYN/ACK and SYN/ ACK-ACK packets which could be useful for network troubleshooting as application performance indicators such as latency and jitter. Furthermore, R&S®PACE 2 includes the functionality to get information about the quality of Voice over IP and video applications. These performance measurements are key for TCP/IP based QoS/QoE use cases.

**Metadata extraction including key performance indicators**



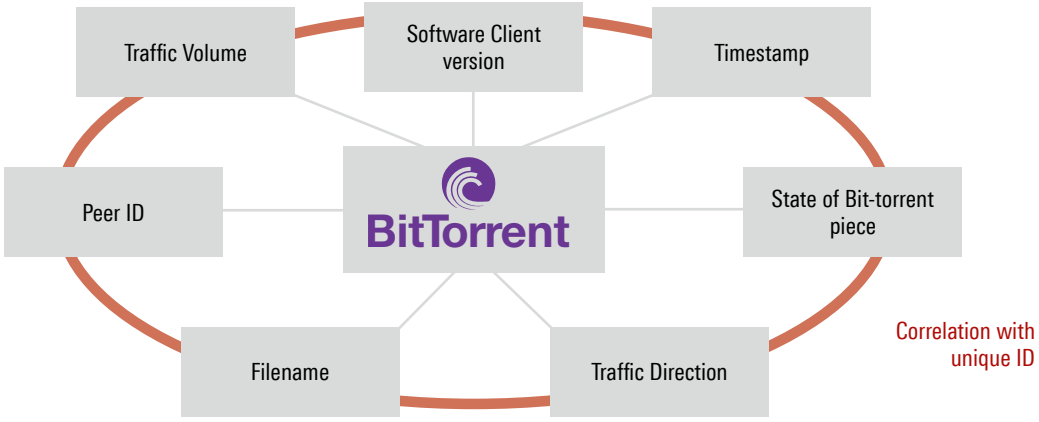
# 7. Metadata extraction

## 7.2 Protocol and Application Metadata

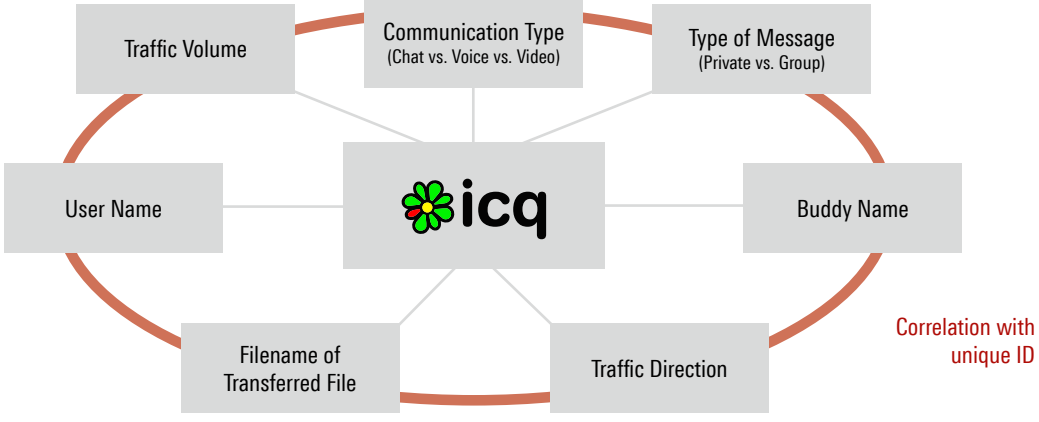
R&S®PACE 2 includes the possibility to extract protocol (Layer 3 to Layer 7) and application based metadata from IP traffic. The extraction of the metadata can be done in real time, providing insight into user behavior and application usage. The ability of R&S®PACE 2 to go further to extract protocol and application metadata, enables detailed understanding of network transactions and behavior. This insight can be used for a wide array of applications such as customer experience management, network planning, policy management, network security and many others. Examples of metadata that can be extracted from IP traffic include:

- Volume: e.g. the volume of traffic per application and per user and per protocol.
- Identifiers: e.g. email sender / receiver addresses or any other ID that can be used to implement strong security rules.
- Files: e.g. used codec from Video on Demand application can be used for security applications, QoS/QoE applications and others.
- Usage: e.g. HTTP URL or used client software can be used for intelligent traffic decisions as well as for customer experience management.

**Example 1: BitTorrent**




**Example 2: ICQ**



# 8. Content decoding

The decoding results of R&S®PACE 2 provides the deepest information about the current connection. R&S®PACE 2 extracts all important and relevant metadata from a number of network classification results with a configurable level of detail to suit different use cases. For example, it is possible to decompress HTTP payload and reconstruct all images or videos from internet sites. The depth of information required can be flexibly adjusted to provide just the actual data needed. Internal aggregators gather decoding information from certain decoders and bundle them into classes. For example, even if an email connection takes a long time the full session decoding information still provides all of the data in one single place.

The decoding feature of R&S®PACE 2 is especially useful in network security applications, e.g, the playback of VoIP calls, websites and chat sessions or gathering upload and download statistics of various documents. Next-generation firewalls can enable data leakage prevention, deep security scans and network access control based on the R&S®PACE 2 decoding results. Traffic management and policy control solutions also rely on detailed insight on application content to enable the best available decisions about bandwidth management and quality of service (QoS)/quality of experience (QoE) rules. Individual charging based on the application level is also possible.

# 9. Additional features

## 9.1 Dynamic Upgrade

R&S®PACE 2 can be updated during runtime without interruptions so detection improvements can be used in a live system. This update includes signature updates for known protocols, updated detection logic and may also seamlessly add new detections for newly supported protocols. Updates of detection logic are designed to improve performance and detection results.

## 9.2 OS Detection

OS detection analyzes specific attributes of flows to detect the corresponding operating system. Similar to protocol detections, the OS detection will return a result for each flow stating whether the OS has been found or not.

## 9.3 NAT/Tethering Detection

R&S®PACE 2 includes subscriber based NAT and Tethering detection. It uses the OS detection to determine if multiple operating systems are in use for a single subscriber and sets a flag for the subscriber accordingly. For each subscriber the detected main OS and the detected NAT state are available.

## 9.4 Client Server Indication

R&S®PACE 2 can identify those hosts which are mainly used as a client or as a server. This can be used to detect servers in internal networks or to decide which side of a network is actually the internal network if this information is not inherently known. The feature will identify whether each flow is a client to a server flow, server to a client, or even client to client in the case of P2P networks. Server to server is also possible in pure server communication.

## 9.5 Unidirectional Traffic Support

Depending on the network setup, a specific network link can carry packets traveling in both directions (i.e., the bidirectional case) or only one direction (i.e., the unidirectional case). This unidirectional routing can apply to all packets on that link, or a subset of the packets (e.g. only a specific subscriber group). A typical example of a highly unidirectional configuration is an Internet connection with a cable downlink and a satellite uplink. R&S®PACE 2 is able to detect both bidirectional and unidirectional traffic.

## 9.6 Customization

R&S®PACE 2 allows for the addition of custom-defined protocols (CDP) to extend the detection without the need for a new library. Those CDPs can be added by a customer. The features are the following:

- Rule based approach (HTTP host matches, port matches etc) and/or C code for greatest possible flexibility
- Virtually any number of protocols are supported
- Configurable during library initialization

## 9.7 Fastpath

The fastpath mechanism is used to speed up the handling of flows which are already identified and for which additional processing is not necessary. R&S®PACE 2 includes a API function to query the status of this fastpath so it can be used to completely skip those flows which do not need additional processing.

# 10. Performance testing

ipoque has conducted testing to assess the performance of R&S®PACE 2 using IP capture files from different customer products where R&S®PACE 2 was successfully deployed.

All tests are done with enabled:

- Flow tracking
- Subscriber tracking
- IP defragmentation
- Detection

**The idea behind the test data is to provide a performance indication based on a wide selection of customer use cases.**

The detection requires a valid pointer to the internal flow data structure for TCP and UDP connections. The built-in hash table can be used to store this information. For flow tracking, the hash table uses the 5 tuple (IP addresses, TCP/UDP ports and IP protocol) as connection information. The subscriber tracking is very similar to the connection tracking. IP defragmentation is used to reassemble fragmented IP packets before passing them to R&S®PACE 2. The basic idea of the R&S®PACE 2 defragmentation engine is to store all fragments until the whole packet can be reassembled. The detection itself is the main purpose of R&S®PACE 2, a software library which detects nearly all applications in a network packet stream. R&S®PACE 2 uses a wide range of IP classification technologies, including pattern matching, heuristic and behavioral analysis. Based on this combination, R&S®PACE 2 is able to reliably detect encrypted protocols with a very low false negative rate and virtually no false positives.

## 10.1 Test Data

All listed use cases are different IP capture files from different customer products where R&S®PACE 2 was successfully deployed. Each file represents a spezialised usecase and represents a selection from a range of application scenarios. The idea behind the table is to provide a performance indication according to a wide selection of customer use cases.

## 10.2 Single Thread Tests

The tests are focussed on CPU cycles per packet. All measurements are performed on a commercially available system:

| Test environment specification | |
|---|---|
| **Chassis** | Dell PowerEdge R210 II |
| **CPU type** | Intel Core i3-2100 CPU @ 3.10GHz |
| **Internal memory** | 8GB DDR3-1333 SDRAM |
| **Ethernet interface** | Broadcom NetXtreme II BCM5716 Gigabit Ethernet |
| **Storage** | 2x Seagate ST31000340NS (1TB), RAID0 |
| **Operating system** | Ubuntu 10.04 LTS |

For performance measurement a live-link traffic capture file has been used which was recorded on an ISP link. This capture file contains $80 \cdot 10^6$ packets with a total amount of 47 GB of data resulting in an average packet size of 471 bytes. The maximal number of concurrently active connections is $1.5 \cdot 10^6$ while the maximum number of concurrently active IP addresses is $0.3 \cdot 10^6$ . Furthermore the rate of fragmented packets is 21.94% and the average number of packets per flow is 33. The average number of new flows per second is 2360 and the average number of packets per flow before it gets detected is 3.7. The following table shows the average throughput in GBit/s of the different customer use cases by using one thread only to process the data through R&S®PACE 2.

| Use case | General info | General info |
|---|---|---|
| 1 Network Operator | number of packets: 33.1M<br>Average packet size: 569<br>Max. concurrent connections: 418720<br>Average throughput: 3.4 Gbit/s | HTTP, FLASH, BITTORRENT, MPEG, SKYPE, DIRECT DOWNLOAD LINK, PPSTREAM, SSL, GNUTELLA, QUICK- TIME, MSN, SHOUTCAST, MMS, DNS, RTP, YAHOO, POP, RTSP, OGG, WINDOWS MEDIA, SSH, H323 |
| 2. Next Generation Firewall Vendor | number of packets: 6.1M<br>Average packet size: 523<br>Max. concurrent connections: 71191<br>Average throughput: 5.6 Gbit/s | HTTP, SSL, RTP, FLASH, OPENVPN, IPSEC, BITTORRENT, RTP, H323, QUICKTIME |
| 3. Enterprise (Medium Deployment) | number of packets: 203.5M<br>Average packet size: 396<br>Max. concurrent connections: 18128<br>Average throughput: 9.9 Gbit/s | HTTP, FLASH, QUICKTIME, RTP, SIP, SSL, BITTORRENT, EDONKEY, YAHOO, DIRECT DOWNLOAD LINK, SKYPE, H323, TEAM VIEWER, OPENVPN, IPSEC |
| 4. Enterprise (Small Deployment) | number of packets: 1M<br>Average packet size: 786<br>Max. concurrent connections: 5702<br>Average throughput: 20.2 Gbit/s | BITTORRENT, HTTP, SSL |

# 11. Service and support

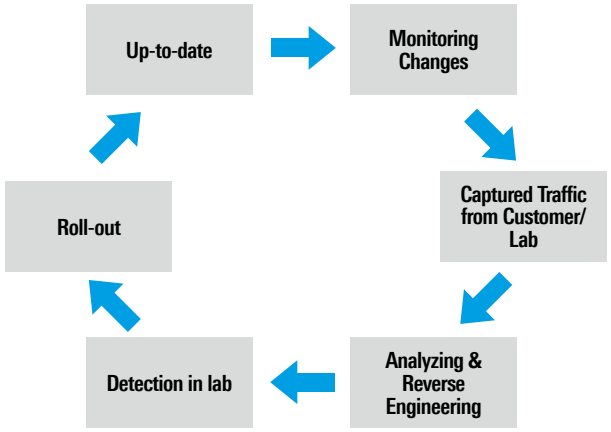
## 11.1 Product Evaluation

A demo version of the R&S®PACE 2 software can be provided to a qualified customer in order to evaluate the library. In this phase, ipoque provides remote or on-site support in order to ease the integration process and help customers to effectively evaluate and customize the solution.

## 11.2 Maintenance

Regular firmware updates are essential for high performance IP classification and decoding software. ipoque constantly monitors the effectiveness of protocol and application detection by developing classification algorithms for new protocol signatures. All supported signatures are constantly tested and refreshed in order to keep up with the evolution of network applications. Signature updates are available to customers on a frequent basis (at minimum on a monthly basis). When there is an update, customers receive a notification email and can access the update via ipoque's customer portal.

**Always up-to-date**




## 11.3 Customer Portal

For R&S®PACE 2 customers, ipoque maintains a Web-based Portal which can be used by a customer's technical staff to:

- Open/manage troubleshooting issues
- Handle priority levels of tickets
- Share documents and attachments in a bidirectional way (PCAPs, Patches, etc)
- Receive information about available firmware releases

Customers are given dedicated access logins for the customer portal. Multiple access logins can be provided, in order to have personal accounts on the system.

## 11.4 Training

ipoque provides high quality training for our customers and partners. Our comprehensive offer is designed to meet all of your product-related educational needs. Our training team has unrivalled knowledge of the ipoque products and can transfer the level of understanding needed to enable a proper implementation and integration of the PACE software into a customer's solution. Training can be organized at ipoque's premises or at a customer site. The product training is an optional service offered by ipoque. There are different training modules available starting from technical traning for developers up to high-level product capability training for executives and product managers.

# 12. Use cases

R&S®PACE 2 can be deployed in a variety of networking solutions including Network Security (IDS/IPS, firewalls, SIEM, UTM), Network Monitoring (QoS/ QoE), Policy and Charging, OSS/BSS, WAN Optimization and Application Delivery, Mobile Data Offloading, and Network and Subscriber Analytics.

**By integrating R&S®PACE 2, vendors can introduce application detection to their products and keep up with the dynamic changes in protocls and applications.**

## 12.1 Network and Traffic Management (QoS/QoE)

Traffic management vendors need to provide their end customers e.g., mobile network operators, with accurate realtime insight into subscribers' application usage and performance, Key Performance Indicator (KPI) monitoring and trend analysis and quality of service and experience of subscribers. These solutions need detailed and reliable information on protocols and applications usage e.g., 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. R&S®PACE 2 accurately identifies applications to Layer 7 and provides the ability to manage network and application performance in real- time. By integrating R&S®PACE 2, vendors can keep up with the dynamic changes in protocols and applications, which ensures a high rate of detection for traffic management.

## 12.2 Policy Control and Charging

Network operators have to balance the demand for network bandwidth with the need to drive revenue for new services and applications. Policy control and charging is a key component of LTE networks as operators look to define bandwidth guarantees, priorities and limits, offer QoS for an additional fee and importantly be able to offer realtime charging and billing support. Policy control and charging vendors need to provide support for fine- grained QoS and enable application servers to dynamically control the QoS and charging requirements of the services they deliver. R&S®PACE 2 software can identify over 95% of network traffic and frequent signature updates ensures a high detection rate and accurate application identification for policy and billing purposes.

# 12. Use cases

## 12.3 Network Security (Firewalls, IPS/IDS, SIEM, UTM)

With the huge growth in IP network traffic using Web protocols, security vendors need to be able to identify the application to distinguish between traffic. Next Generation Firewalls (NGFW) are application-aware and, instead of allowing all traffic coming in via typical Web ports, a NGFW can distinguish between specific applications (for instance, Hulu vs. Salesforce.com) and then apply policies based on business rules. By integrating ipoque R&S®PACE 2, security vendors quickly gain accurate application visibility and control and can better manage security threats and prevent network attacks. R&S®PACE 2's ready to use software libraries and signature database reduce costs and risks associated with developing and maintaining a highly complex technology internally. A big challenge for a security vendor doing this in-house would be continually updating the software with the latest applications and protocols so the security product is effective in managing threats and malware.

**R&S®PACE 2's ready to use software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally.**

## 12.4 Network and Subscriber Analytics

Gaining business intelligence from network and subscriber data is a fast growing area as operators recognize they can unlock value by better understanding subscriber application usage and behavior. This in turn is being used by the marketing department to enhance data packages as well as by network planning and optimization to plan investment and improve QoE per application. R&S®PACE 2 offers analytics vendors high performance, accurate identification of the applications subscribers are using as well as richer data around usage time, type of content e.g. who are the power users and what are the top applications used by subscriber segment or geography. This provides enhanced reporting features and fast time to market for vendors and since application recognition is a core expertise in itself, vendors do not have to use in-house resources to track and classify the latest apps and protocols. In a typical integration, this application usage data is linked directly to third party analytics systems that delivers reports and dashboards about subscribers mobile data consumption.

## 12.5 Mobile Data Offload

Network operators are using mobile data offload solutions to offload lower priority (low revenue) traffic that is clogging up the network and improve the overall quality of service. Mobile data offload solutions typically treat all traffic flows equally without distinguishing the application involved or the device used. However, in LTE deployments, operators prefer to selectively steer traffic flows based on the application used. R&S®PACE 2 software enables

# 12. Use cases

vendors to reliably detect applications and to implement smarter offload strategies based on total flow visibility. Intel has integrated R&S®PACE 2 technology into their "Smart Pipe" server used in small cells as a mobile Internet access gateway. The solution enables network operators to classify Internet traffic at the application level to ensure improved QoE for mobile Voice over IP (VoIP) calls and video streaming.

**R&S®PACE software enables vendors to implement smarter offload strategies based on total flow visibility.**

## 12.6 WAN Optimization

With the combined growth in cloud computing and mobile working, guaranteeing the performance of business critical applications on wide area networks and ensuring bandwidth efficiency has become more difficult. Vendors need to embed realtime application awareness and gain a deep understanding of the applications running over the wide area network in order to prioritise key business traffic far more efficiently and also ensure that bandwidth does not become congested. R&S®PACE 2 can identify thousands of applications for every IP flow in realtime. WAN optimization vendors can then get an accurate picture of applications running on the network and user behavior and avoid the upfront costs, time-to-market delays, and associated business risks of in-house development. With the emergence of complex applications aggregating several multimedia content types (video, images, VoIP etc.) from different servers, WAN optimization solutions require complete protocol and application visibility.

## 12.7 SDN/NFV Environments

The move by telecom operators from hardware to a software based virtualized network environment based on commercial off the shelf hardware is progressing at a steady pace. Operators are commited to reducing proprietary hardware, driving down network costs and providing more flexibility to manage applications on scalable IP-based networks. With SDN and NFV, IP application classification software such as R&S®PACE 2 can migrate from being embedded in many network appliances to becoming a shared function hosted on standard servers. R&S®PACE 2 has no external dependency, works on standard servers and OS and can be used in all environments regardless of whether it is a physical or virtualized environment or even a SDN architecture

**About ipoque**

ipoque GmbH, a Rohde & Schwarz company, is a leading supplier of network traffic analytics and IP classification solutions to network operators and infrastructure vendors. Over 200 customers in more than 60 countries across the globe rely on ipoque to maximize network efficiency, improve the quality of experience for their subscribers and develop the intelligent communications networks of the future.

**About Rohde&Schwarz**

The Rohde&Schwarz electronics group is a leading supplier of solutions in the fields of test and measurement, broadcast and media, secure communications, cybersecurity, and radiomonitoring and radiolocation. Founded more than 80 years ago, this independent global company has an extensive sales network and is present in more than 70 countries. The company is headquartered in Munich, Germany.

Certified Quality Management
ISO 9001

**ipoque GmbH**
www.ipoque.com

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


PD 3607.2332.32 | Version 01.00 | June 2015
R&S®PACE 2 Solution Guide


3606000000

3607.2332.32 01.00 PDP 1 en