



Solution Guide

R&S® PROBE OBSERVER

Ready-to-use network analytics suite for
high-performance network monitoring

ROHDE & SCHWARZ

Make ideas real



CONTENT

- Content**.....2
- 1 Introduction**.....3
 - 1.1 Key benefits3
 - 1.2 Key features3
- 2 Solution Architecture**.....4
 - 2.1 Components.....4
 - 2.2 Deployment scenarios5
 - 2.3 Connecting to Big Data solutions6
- 3 Business Cases**7
 - 3.1 Large-scale CSP increases business profitability through sampling approach.....7
 - 3.2 Reducing cyber risk through enhanced SOC and CDC capabilities8
 - 3.3 Mobile CSP optimizes network quality with edge and core data9
 - 3.4 Solving Open RAN observability for mobile network operators (MNO)11
- 4 Technical Features**13
 - 4.1 Traffic input and processing by R&S®Probe.....14
 - 4.2 R&S®Probe Observer front-end.....14
 - 4.3 Visual presentation15

1 INTRODUCTION

Communication service providers (CSPs) are struggling to remain competitive in today's fast-changing environment. To successfully face future challenges such as Big Data, 5G and IoT, CSPs need to:

- ▶ Be able to handle increasingly large data volumes and a growing number of connected endpoints.
- ▶ Keep a lid on costs by avoiding classical price-per-throughput models, which are too costly to optimize and plan networks effectively.
- ▶ Be able to connect their existing analytics tools to multiple systems without being limited to only one type of analytics solution.
- ▶ Reduce cost pressure by reducing operational expenditure (OpEx) and capital expenditure (CapEx) as well as generating new revenue streams and finding ways to keep customers satisfied.

The following factors are essential for choosing the right traffic analytics solution:

- ▶ Flexibility and scalability: Accelerate performance and be prepared for changing conditions without having to replace existing systems.
- ▶ Real-time IP network monitoring and subscriber analytics: Increase customer satisfaction and decrease customer churn.
- ▶ Holistic analytics approach for maximum business efficiency: Avoid silo mentality and drive business with cross-departmental data usage.

1.1 Key benefits

Revenue generation

Connecting R&S®Probe Observer to Big Data analytics systems creates new opportunities for CSPs to monetize additional services based on objective data from the network, for example subscriber segmentation and NB-IoT analytics.

OpEx savings

R&S®Probe Observer enables real-time monitoring of the core network reducing monitoring efforts at the edge and optimizing RAN network troubleshooting.

CapEx savings

Reduce capital expenditure (CapEx) through inherent modularity and scalability. Easily integrate, fully virtualize, and scale on demand, optimizing your infrastructure investment.

Future-proof solution

The various deployment scenarios of R&S®Probe Observer and the use of open standards such as Apache Kafka and IPFIX as a connector to any type of analytics solution make the whole system future-proof. R&S®Probe Observer allows decoding of control plane data providing new insights into RAN, such as RSRP, RSRQ, SINR measurements, cell congestion, re-selection events etc., and NB-IoT patterns, such as PSM and eDRX activities, coverage enhancement, device communication intervals etc., enabling deeper network optimization and dynamic slicing.

Customer retention

Real-time traffic analytics deliver advanced and efficient troubleshooting capabilities, directly improving quality of experience (QoE) and quality of service (QoS).

1.2 Key features

- ▶ Highly scalable virtualized system, with the option for deployment on dedicated hardware to reach the Tbps mark
- ▶ Deepest insights based on real network usage, application performance and subscriber experience
- ▶ High statistics resolution with a configurable reporting rate down to 1 second
- ▶ Easy-to-use drill-down dashboards to get insights about overall network, subnetwork, individual subscriber
- ▶ Data export for Big Data systems makes it a holistic analytics platform

R&S®Probe Observer excels in modularity and processing speed, offering optimal support to CSPs facing future challenges and technologies.

2 SOLUTION ARCHITECTURE

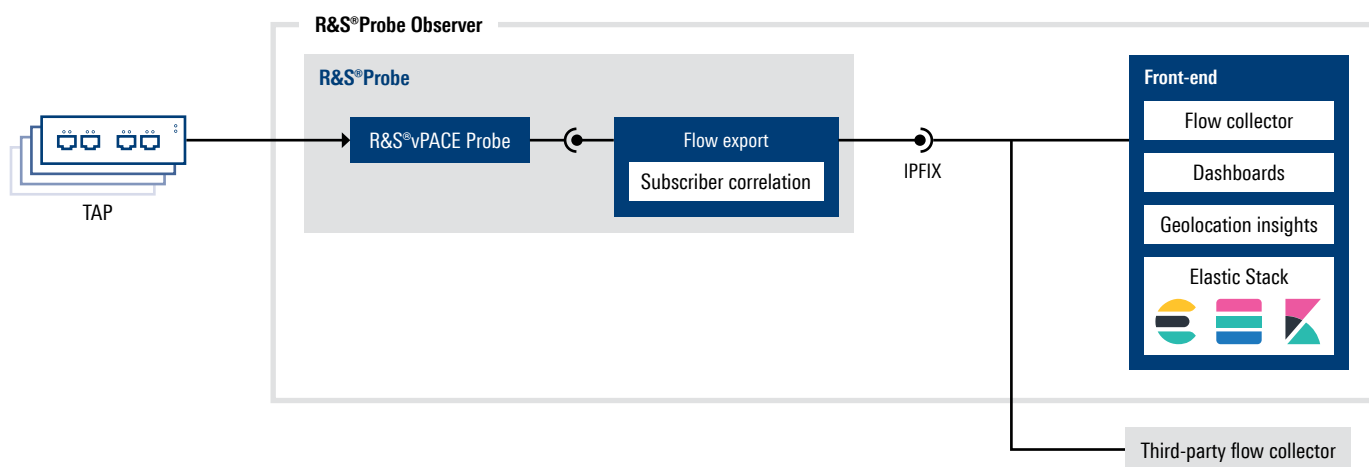
R&S[®]Probe Observer is a traffic analytics solution that extracts data from a passive copy of the production traffic, in real time. Its flexibility and adaptability to different deployment situations and customer requirements make it easy for CSPs to extract all the insights they need, even when dealing with highly specific implementations.

Featuring the technologically leading deep packet inspection (DPI) engine R&S[®]vPACE and advanced real-time packet processing, R&S[®]Probe Observer offers high-quality real-time information about network traffic, subscriber sessions and network metadata.

2.1 Components

R&S[®]Probe Observer can handle several Tbps of real-time traffic. It consists of an analytics platform and multiple instances of R&S[®]Probe, which are powered by the DPI engine R&S[®]vPACE.

- ▶ **R&S[®]Probe:** A technically advanced, intelligent IP probe that allows CSPs to extract meaningful network traffic and subscriber behavior data. It identifies statistical trends in mobile and fixed networks leveraging R&S[®]vPACE Probe, powered by our DPI engine R&S[®]vPACE.
- ▶ **R&S[®]vPACE:** A powerful DPI engine for highly reliable real-time classification of IP traffic, covering thousands of protocols and applications. It extracts rich data such as usage time, type of content, identification of different types of services, and the top applications. R&S[®]vPACE is deployed worldwide and known for its fast performance and efficient memory usage.
- ▶ **Front-end:** A data analysis and high-performance network monitoring front-end that automatically aggregates and stores all relevant information extracted from IP packets and flows. Open REST APIs of the Elastic Stack provide direct access to the underlying analytics database. An easy-to-use, intuitive and customizable user interface provides a wide variety of views, displaying detailed insights into all kind of network traffic flows.



R&S[®]Probe Observer component overview: Processing, front-end

2.2 Deployment scenarios

R&S®Probe Observer offers a variety of deployment scenarios, depending on the specific use cases and customer needs.

2.2.1 All-in-one analytics system

R&S®Probe Observer can be deployed as a stand-alone main traffic analytics system. This scenario is especially suitable for CSPs that need an end-to-end analytics system to process traffic and present relevant reports for strategic decision-making, network planning, and subscriber analytics.

- ▶ Reads real-time data records from a pool of R&S®Probe instances
- ▶ Connects to external systems to enrich its database with additional information, including CRM, TAC, etc.
- ▶ Performs subscriber correlation and data correlation, and generates reports
- ▶ Provides customizable dashboards via its graphical web interface

2.2.2 Supplement to Big Data systems

The front-end of R&S®Probe Observer provides an aggregation function for traffic and subscriber information to correlate data with additional sources, creating a Big Data pool.

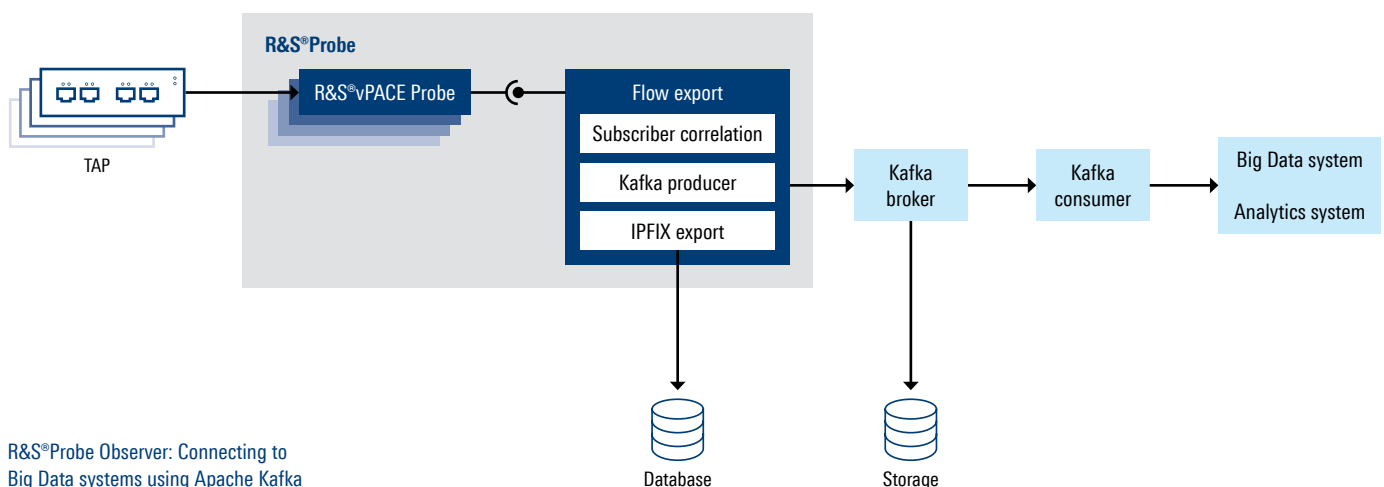
- ▶ Reads real-time data records from a pool of R&S®Probe instances
- ▶ Provides aggregated information on network traffic, subscribers, services and applications to Big Data systems
- ▶ Integrates the analytics capabilities of Elastic Stack
- ▶ Ready to integrate into analytics system landscapes via Apache Kafka and IPFIX

2.2.3 Combined set-up

R&S®Probe Observer can be deployed as both an independent traffic analytics system that provides insights and dashboards, and as an aggregator for Big Data and third-party analytics.

Benefits

- ▶ Developing a Big Data system containing knowledge based on aggregated data from multiple sources offering a solution which provides valuable data for several internal departments with differing demands
- ▶ Avoiding proprietary data extraction systems with vendor lock-in as well as specific analytics for narrow and inflexible use cases
- ▶ Very short time-to-market through use of existing systems
- ▶ Future-proof analytics architecture that supports further extensions, virtualization and an agile approach to changing requirements



2.3 Connecting to Big Data solutions

The true value of collected data emerges when data is extracted from all the CSP's business units and then analyzed as a whole. To connect an analytics system effortlessly to any Big Data system, flexible interfaces are crucial.

R&S®Probe Observer can be easily deployed in any network to enrich existing Big Data systems, as well as external analytics tools, with real-time data from the network. The Apache Kafka interface ensures optimized and reliable real-time data delivery between R&S®Probe Observer and third-party data analytics systems. This synergy of multiple analytics systems ensures an optimal use of data and brings value to several use cases and departments.

For example, the data rates of each individual application (e.g. Netflix on mobile) regarding radio sector and radio technology can be coupled with network layout maps to extrapolate potential optimization approaches, ensuring a consistent QoE for Netflix users across access technologies and locations. The same data can be analyzed in parallel and combined with subscriber analytics and CRM systems to identify potential strategies for monetizing over-the-top (OTT) services, such as flat rates, premium packages, partnering with OTT providers, etc.

Apache Kafka is an open-source streaming platform used for building real-time data pipelines. Systems and applications can publish (producers) or subscribe (consumers) to a stream of data (records). In the example below, R&S®Probe Observer is acting as a Kafka producer, while the customer's Big Data system is the Kafka consumer. Information about communication flows as well as subscriber sessions are reported in real-time by R&S®Probe Observer and are temporarily stored in the Kafka broker. Depending on the use case and implementation, customer Big Data systems can subscribe to specific data on demand and read data at their own tempo.

R&S®Probe Observer leverages Elastic Stack with industry-grade data analytics capabilities to efficiently index, filter, and visualize the insights that are required for the task.

With data exchange grounded in the widely adopted industry standard IPFIX and enhanced with our year-long experience in the domain, we ensure interoperability, stability and tailored insights for every use case.

Other real-time data feed platforms are available if required.



3 BUSINESS CASES

The following business cases are a selection of scenarios and do not intend to cover all potential use cases.

3.1 Large-scale CSP increases business profitability through sampling approach

3.1.1 Initial customer situation

A large-scale fixed-line CSP is facing huge volumes of daily and peak traffic. Their amount of traffic, especially for landline connections, is constantly increasing and even light users' internet consumption is steadily growing. Forecasting the evolution of customer needs and increasing the efficiency of marketing and product management requires objective insights into the network. Installing a fully-fledged analytics system that covers the whole network traffic as well as all subscribers would be a considerable financial and organizational burden. This is why they are opting for a sampling approach to analytics.

Customer's requirements:

- ▶ Very high traffic volumes and multi-million subscriber base
- ▶ Network planning, finance and marketing departments need detailed information about traffic volumes, peak traffic, application and protocol distribution, acceptance and usage of offered products and services of the provider

3.1.2 Solution: deployment scenario

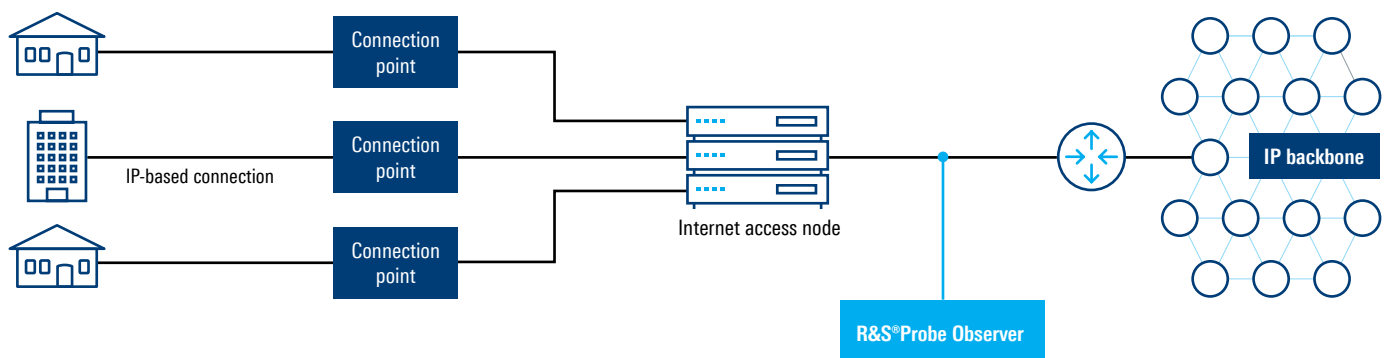
For this implementation, a representative sample of 3% of all subscriber lines has been selected based on a balanced distribution in terms of geographical location and line rate (used data packages).

- ▶ Several locations country-wide to monitor landline traffic and extrapolate the acquired data
- ▶ Flexible connectivity to accommodate different BNG lines (10 GbE, 40 GbE, 100GbE)
- ▶ Customized subscriber correlation in the context of GTP or L2TP tunnel tracking, for example via RADIUS or Diameter
- ▶ Advanced decapsulation and tracking for asymmetric network stack structure (several layers of VLAN, MPLS)
- ▶ Data export from R&S®Probe Observer to feed into customer's specific analytics system
- ▶ Anonymization of attributes that would identify specific customers, GDPR compliance

3.1.3 Main business results

Capital investment savings

- ▶ Dramatic savings in hardware, licenses and power thanks to a representative sampling approach
- ▶ Excellent network planning and forecasting based on extrapolated data and averages
- ▶ Computing optimal investment for the next years based on network data and available technologies



Visibility into real network usage by extracting network metadata samples

Higher business profitability

- ▶ Optimize agreements with virtual network operators (VNO) by leveraging detailed insights into subscriber usage, peak times, and overall network demand
- ▶ Create, monitor, and evaluate new offerings based on representative data analysis across products and subscriber types
- ▶ Manage products effectively and gain early feedback on the usage of products and packages
- ▶ Better strategic decisions and agility to answer traffic- and subscriber-related questions at any time when they appear

Cost reduction

- ▶ Improve efficiency with a sampling approach that requires less hardware, power, and cooling
- ▶ Pay-as-you-grow model, no large upfront investment
- ▶ Runs on COTS hardware (no vendor lock-in)

3.2 Reducing cyber risk through enhanced SOC and CDC capabilities

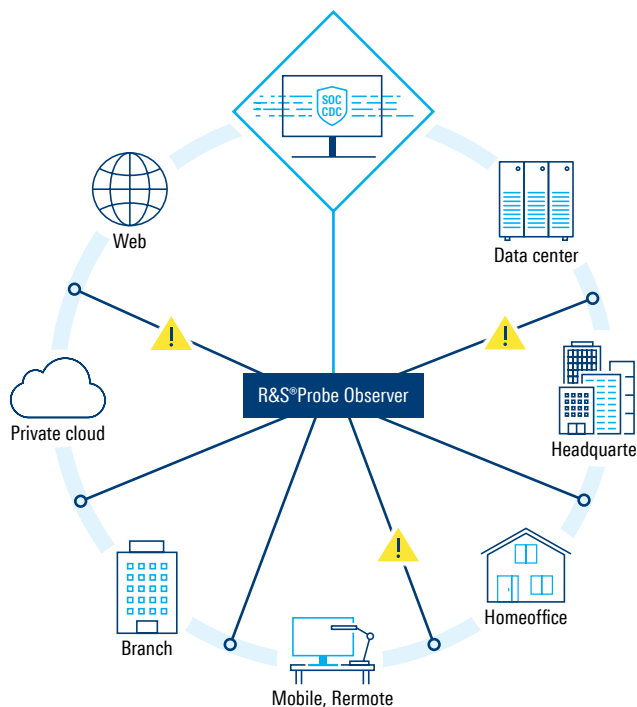
3.2.1 Initial situation

In modern enterprise architectures, fragmented network environments often limit visibility for security operations centers (SOC) and cyber defense centers (CDC), the operational functions responsible for managing and mitigating cyber threats. This fragmentation creates critical deficiencies in security monitoring, leaving telemetry insufficient for a full operational picture. With excessive alert volumes and blind spots in encrypted traffic, detecting lateral movement becomes a challenge, leading to the risk of long attacker dwell times, time-consuming investigation cycles, or threats remaining entirely undetected. Continuous, passive network telemetry is essential to identify unknown assets in real time and detect critical behaviors, including east-west traffic, unusual internal connections, and remote management protocols. Without this data, there is no insight into the scan and anomaly patterns required to reconstruct accurate attack timelines. This lack of visibility elevates vulnerability to undetected threats and overall cyber risk.

3.2.2 Solution: Establishing a network intelligence layer for cyber defense

R&S®Probe Observer serves as a network intelligence and security visibility layer for SOC and CDC operations, providing the evidence, context, and telemetry required to detect, investigate, and understand cyber threats.

- ▶ **Continuous network visibility with enriched metadata:** Use passive traffic observation to continuously watch network communications without impacting production systems. Generate enriched network metadata that identifies unknown assets and maps relationships between users, services, and applications, providing critical insight into east-west traffic, irregular internal connections, and the unusual usage of remote management protocols.
- ▶ **Advanced behavioral analytics and detection:** Establish behavioral baselines and leverage encrypted traffic analytics to reveal suspicious communication patterns and lateral movement, providing the network-based threat detection necessary to identify activities that bypass existing security telemetry.
- ▶ **Accelerated threat hunting and incident response:** Provide historical visibility and build communication graphs to enable proactive threat hunting for indicators of compromise. Rapidly reconstruct attack timelines for digital forensics and incident response.
- ▶ **Strategic security integration:** Deliver the essential telemetry required to move from reactive security operations to continuous cyber defense, serving as a critical foundation for implementing zero trust, exposure management and negative trust strategies.



3.2.3 Main business results

Increased cyber resilience

- ▶ Faster threat detection and significantly reduced attacker dwell time
- ▶ Improved detection coverage across diverse network environments
- ▶ Enhanced ability to prevent, identify and mitigate the impact of potential threats

Operational efficiency

- ▶ Reduced analyst workload through higher-quality, context-rich telemetry metadata
- ▶ Accelerated incident response and investigation cycles
- ▶ Improved validation of detection engineering and security analytics

Risk and compliance optimization

- ▶ Strengthened support for governance, risk, and compliance (GRC) initiatives
- ▶ Reduction of organizational risk through the elimination of network blind spots
- ▶ Improved alignment with modern cyber defense standards

3.3 Mobile CSP optimizes network quality with edge and core data

3.3.1 Initial customer situation

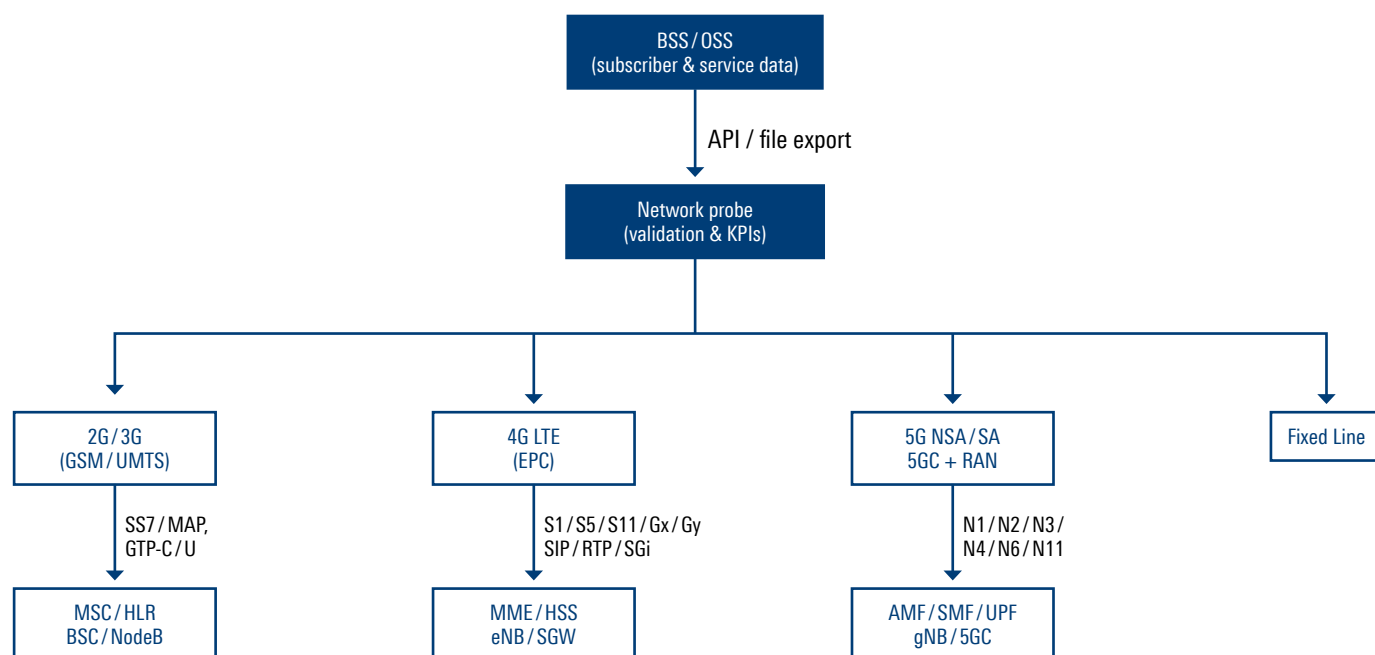
A European tier 1 mobile service provider wants to reduce customer churn and improve monitoring of network quality and subscriber QoE.

Customer's requirements:

- ▶ CSP requires a 360-degree view of their subscriber base and network
- ▶ CSP wants to use their own Big Data system to bring together data from various sources
- ▶ CSP wants to create an infrastructure which will ultimately help them move towards a self-organizing network (SON)
- ▶ The network optimization and planning team wants to dynamically tailor the extracted data based on their project needs

3.3.2 Deployment scenario adapted to the customer's challenges

In response to the challenges faced by modern CSPs, Rohde&Schwarz provides a series of products from within the mobile network testing (MNT) division. Orchestrating



360 degree view of the network: from RAN to core

these products provides the required streams of analytical data for building a complete 360-degree view of the network, ranging from the core and the radio access network (RAN) all the way to end user devices.

This visibility into their networks, optionally integrated with Big Data solutions, assists CSPs with network optimization projects and moving towards self-organizing networks (SON).

Together with Rohde & Schwarz, the CSP set up a holistic analytics system to gather and analyze data from both edge and core. This solution provides the statistics needed to optimize QoE and create innovative solutions for 5G networks, which helps the CSP optimize their networks, improve customer experience, and generate new revenue streams.

For the CSP's major network optimization project, R&S®Probe Observer was deployed to serve as the main data source for the planning department. The solution provides the team with the critical information they need to review the impact of IP data on existing networks: IP statistics, TCP KPIs and RAN statistics in combination with layer 7 awareness. This will help them improve performance and save costs.

For this customer's project, the extracted data was tailored with the following goals:

- ▶ Combine the data from RAN testing with information about subscriber connections and communication KPIs to gain complete awareness of the network state from the end device to the CSP core and all the way to the used service
- ▶ Report RAN parameters and attributes directly from the control plane of the traffic, ensuring an additional perspective about the access network state and performance
- ▶ Be aware of daily network peaks and troughs to assure maximum performance and efficiency of delivered services
- ▶ Correlate subscriber information to get full visibility of communications in the context of multiple default bearers, roaming traffic, LTE-2G/3G handover, etc.
- ▶ Ensure high system scalability and sustainability by using modular architecture and intelligent, subscriber-aware load balancing
- ▶ Control and validate new technologies and services introduced by the CSP by using the application visibility capabilities
- ▶ Comprehend data from fixed-line to 5G networks to increase network performance and optimize network planning

The solution combines IP traffic insights from the core with detailed RAN analytics provided by Rohde&Schwarz solutions: ROMES drive test software, QualiPoc Android (smartphone-based tool for voice and data service quality troubleshooting), the postprocessing and reporting software platform SmartAnalytics, and several diversity optimizer tools. The RF and IP data are integrated into the CSP's global Big Data solution.

For the CSP, this combination of technologies and data ensures faster root cause analysis and situation awareness, along with a better understanding of what is truly happening in the network, pinpointing the network's strengths and, even more important, the areas that need further optimization.

Moreover, this comprehensive visibility into networks facilitates managing both CapEx and OpEx and assists operational teams in planning external optimization tasks with near real-time user data.

3.3.3 Main business results

Higher business profitability

- ▶ Advanced network optimization capabilities thanks to better subscriber-based planning with data from the core and the edge
- ▶ Improved QoE/QoS through more efficient troubleshooting thanks to real-time traffic analytics
- ▶ Minimized churn rate by improving network performance and enhancing customer loyalty
- ▶ Monetization of new services by identifying and evaluating frequently-used applications, top-tier subscribers and OTT



Capital investment savings

- ▶ Better network planning and optimization by evaluating network performance and coverage as perceived by the subscriber
- ▶ Better forecasting of future demand for network capacity based on real network usage and application performance

Cost reduction

- ▶ Reduced edge network monitoring costs (e.g. for extensive drive tests) by complementing core network monitoring with edge network monitoring
- ▶ Reduced need for traditional field testing such as drive tests and handheld measurements, so that more engineering and expert resources can focus on solving significant problems
- ▶ Re-usage of collected data for various insights and even for future use cases thanks to the standard and vendor-independent Big Data export

3.4 Solving Open RAN observability for mobile network operators (MNO)

3.2.1 Initial situation

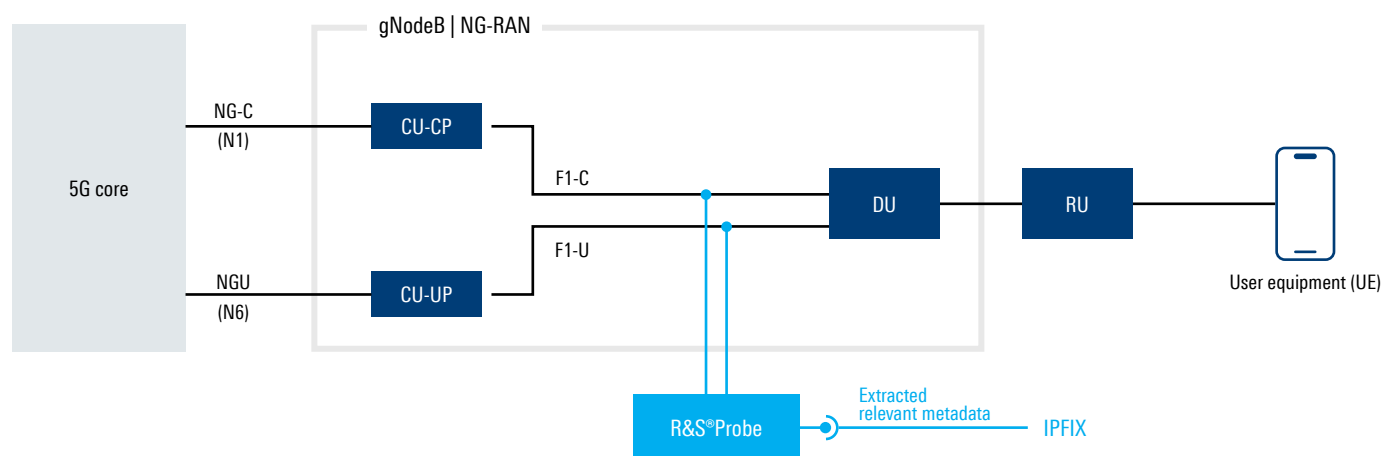
Next-gen wireless technologies such as 5G, 5.5G, and 6G, combined with emerging data applications such as AR/VR gaming and V2X communications, are driving mobile network operators (MNO) toward Open RAN. This approach leverages virtualization, disaggregation, and multi-vendor interoperability to enhance network agility and innovation. Successful Open RAN implementation relies on advanced analytics and deep packet inspection (DPI) to provide the granular visibility needed for intelligent decision-making and improved customer experiences.

To manage this complexity, the industry is adopting cloud-native observability, analyzing metrics, events, logs, and traces (MELT). While standard tools work within application boundaries, multi-vendor interfaces require deeper network insights. This requires analyzing transport-layer behavior (TCP/TLS handshakes, retransmissions, etc.) or inspecting traffic directly to understand the relationship between protocols, applications, and overall performance.

3.4.2 Solution: Bridging the inter-module observability gap

Powered by DPI, R&S®Probe Observer enhances Open RAN observability, particularly for inter-module interactions.

- ▶ **Application & service context:** Accurately identify applications (e.g. distinguishing VoNR calls from Teams video calls or IoT data) traversing interfaces such as F1 or flowing into the UPF. This context is vital for RIC-based optimization (via xApps/rApps) needing to apply policies based on application type or slice requirements. xApps managing slice QoE, for instance, can use DPI data to differentiate high-priority URLLC traffic from best-effort flows sharing the same logical slice resources.
- ▶ **True network performance:** By analyzing application-layer transactions within the traffic crossing interfaces, DPI can derive granular performance indicators (e.g. application-specific latency, video/voice quality metrics such as jitter affecting MOS, retransmission rates impacting throughput) that reflect actual user experience more accurately than infrastructure counters alone. This helps pinpoint whether latency issues originate in the transport network, the radio interface, or within a specific RAN function.



Using R&S®Probe on F1-U between CU-UP and DU to extract deeper insights and metadata that can be streamed to IPFIX collectors for comprehensive analysis

- ▶ **Rich metadata for correlation:** Extract metadata (subscriber identifiers, device types, application transaction details, etc.) and export it (e.g. via IPFIX) to enrich logs and traces from other systems. Correlate network-level events (e.g. a latency spike on the F1 interface) with specific application flows or subscriber groups, drastically speeding up root cause analysis.
- ▶ **Security context & encrypted traffic insights:** Identify protocols and application behavior, aiding security tools in detecting anomalies or policy violations crossing inter-module boundaries. Crucially, advanced DPI techniques incorporating machine learning can classify and analyze encrypted traffic patterns (e.g. using TLS 1.3 or QUIC), providing vital security and performance context even when payload visibility is limited – essential for ZTNA and threat detection across distributed architectures.

3.4.3 Main business results

Cost reduction

- ▶ Reduce development costs by outsourcing DPI and IP probing
- ▶ Streamline operations with our ready-to-use solution
- ▶ Save resources by deploying a small-footprint DPI in multiple network locations to achieve comprehensive, end-to-end visibility in disaggregated architectures
- ▶ Minimize costly downtime and security breaches with observability, accelerating threat detection and response
- ▶ Runs on COTS hardware (no vendor lock-in)
- ▶ Minimize field testing such as test drives and handheld measurements, freeing engineering and expert resources to solve critical problems

Competitive advantages

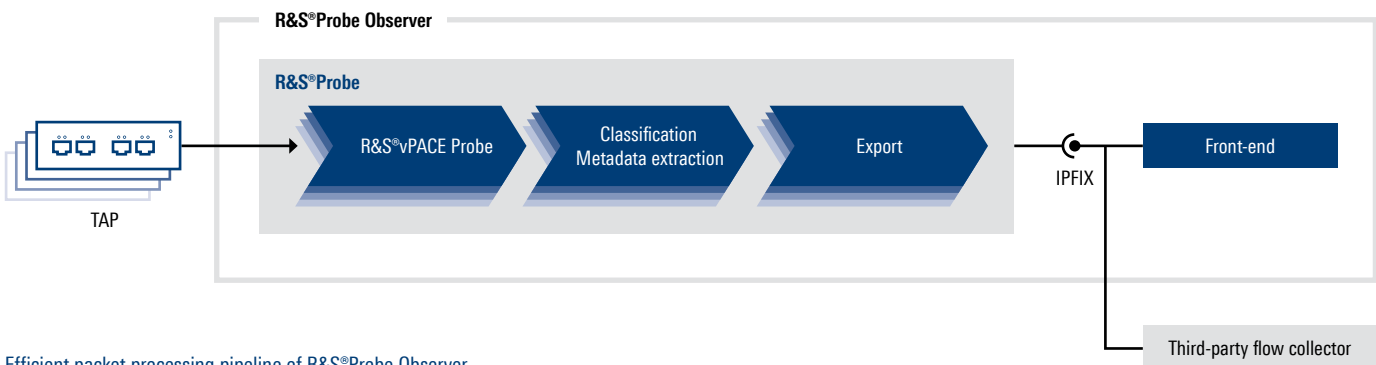
- ▶ Fastest software probe on the market
- ▶ Understand complex Open RAN setups in real time
- ▶ Bridge the visibility gap across disaggregated components, assuring performance and enhancing security
- ▶ Supports zero-trust network access (ZTNA)
- ▶ Get a handle on virtualized network functions (CNF, VNF)

Capital investment savings

- ▶ Savings in hardware and resource demands through low-footprint software components
- ▶ Improved network planning and forecasting from deeper insights into complex networks and enhanced observability
- ▶ Higher flexibility thanks to hardware-agnostic and platform-agnostic solutions

Higher business profitability

- ▶ Make informed strategic decisions and respond quickly to evolving traffic and subscriber trends
- ▶ Optimize networks with subscriber-aware data from the core to the edge
- ▶ Resolve network issues faster and improve QoE/QoS with real-time traffic analytics and AI-driven automated responses
- ▶ Minimized churn rate by improving network performance and enhancing customer loyalty



Efficient packet processing pipeline of R&S®Probe Observer

4 TECHNICAL FEATURES

R&S®Probe Observer is a robust and flexible system that ensures optimal data input and processing, traffic analytics and reporting:

Traffic input

- ▶ High performance: real-time line speed data, up to 800 G connectivity, and subscriber-aware load balancing and scalability up to several Tbps
- ▶ Passive analytics on a copy of traffic
- ▶ Content processing for IPv4, IPv6, dual stack (e.g. Teredo), L2TP, GRE, GTPv1, GTPv2, etc.
- ▶ User plane and control plane traffic
- ▶ Support for asymmetric traffic, processing uplink and downlink traffic
- ▶ Traffic pre-filtering based on address range, MPLS, VLAN

Traffic processing

- ▶ In-house DPI engine R&S®vPACE with 2,900+ classification signatures and 95% classification coverage with virtually no false positives
- ▶ Subscriber correlation and tracking over multiple IPs and default bearers
- ▶ GTP subscriber correlation: linking subscribers to user traffic by processing both GTP control (GTP-C) and user (GTP-U) traffic
- ▶ Subscriber analytics: radio access technology, cell ID, etc.
- ▶ Geolocation insights: mapping network traffic to geographic locations
- ▶ Extracting selected control plane data for analytics: DNS, DHCP, RADIUS, GTPv1/2, etc.

Reporting

- ▶ Intuitive, configurable graphical web interface support-ing various data rate values, with flexible granularity (total, per application and protocol, per subscriber, per flow)
- ▶ Customizable data and reporting granularity (down to 1 second) to match any use case with minimal foot-print and cost
- ▶ Consistent reporting for services, applications, proto-cols and configurable application groups, incl. insights into content delivery networks (CDN), etc.
- ▶ Subscriber insights: data consumption rates, radio attributes, distribution of used services, applications and protocols
- ▶ Network information (statistics aggregated per radio access technology, location, cell, etc.) and KPIs (TCP retransmission counter, TCP round trip time)

System architecture, integration & adaptability

- ▶ Connect to third-party analytics platforms or Big Data systems using open standards (CSV, IPFIX), via REST API, Apache Kafka, the Elastic Stack, etc.
- ▶ Optimal vertical and horizontal scalability thanks to a decoupled multi-stage architecture with highly efficient load balancing between stages and packet-processing pipelines
- ▶ Separate stages for traffic preprocessing (incl. decapsulation), and classification and metadata extraction (incl. flow tracking, control plane data extraction)
- ▶ Up to 10 decapsulation levels allow analytics of traffic within tunnels or with labeling, even when using multiple headers or labels
- ▶ 5-tuple flow tracking plus optional tunnel tracking ensure precise traffic classification as well as flexible subscriber correlation and statistics
- ▶ Support for containerization
- ▶ Privacy & compliance: built-in data privacy (e.g. IP anonymization) and full alignment with regulatory standards such as GDPR

4.1 Traffic input and processing by R&S®Probe

R&S®Probe is a passive network probe that analyzes traffic in real time and extracts network KPIs, statistics (e.g. number of packets and bytes transferred upstream or downstream) and classification details (e.g. protocols, services, applications).

4.1.1 Traffic classification by R&S®vPACE

The DPI engine R&S®vPACE constitutes the core of R&S®Probe. The engine inspects and analyzes network data in real time to reliably classify the most popular applications and extract relevant metadata. To do so, it employs advanced DPI techniques, as well as behavioral, heuristic and statistical analyses.

Benefits of using an in-house DPI solution:

- ▶ Seamless, full integration into R&S®Probe
- ▶ Short time to market for new features
- ▶ Control over product roadmap
- ▶ Faster and more efficient support

4.1.2 Handling encryption

As encrypted traffic constitutes approximately 70% of all communications data and is steadily growing, CSPs need to be able to identify which of their services and resources are being accessed.

Today, encryption is just another transport layer that is used to access streaming, browsing, messaging and corporate applications. R&S®vPACE features a variety of classification techniques such as network flow tracking, byte pattern matching and behavioral analysis. Using this technology, R&S®Probe can correctly identify a large number of services and applications that use encryption, for example:

- ▶ IPv4-TCP-TLS-Youtube
- ▶ IPv4-TCP-TLS-Facebook
- ▶ IPv4-TCP-TLS-WhatsApp

4.2 R&S®Probe Observer front-end

The front-end of R&S®Probe Observer features extensive analytics capabilities to extract insights and create reports. Data sources include information on network flows and corresponding statistics, details on classifications and network protocol stacks, and further metadata, such as control plane information indicating traffic forwarding.

4.2.1 Faster subscriber correlation

To optimize customer care and QoS, R&S®Probe Observer delivers fine-grained data to associate data rates and communication KPIs with individual endpoints.

R&S®Probe Observer helps resolve service issues quickly and identify problems faster by connecting subscriber activity with detailed network data, using protocols such as RADIUS and GTP. RADIUS provides information on subscriber network access (e.g. line ID, IP address), and GTP helps link traffic data to subscribers.

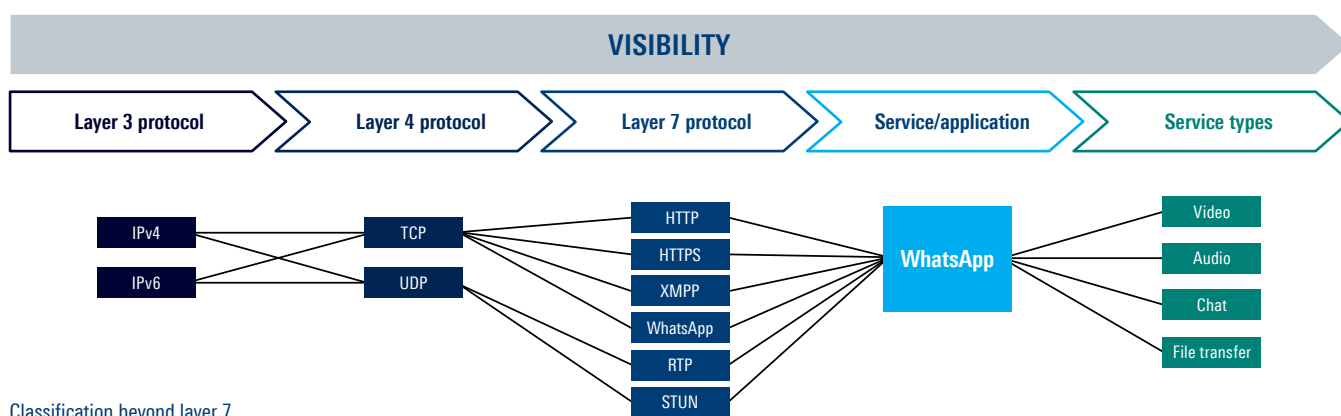
The solution can export flow and subscriber information via IPFIX, protecting personal data with subscriber anonymization.

4.2.2 DNS lookup

DNS reverse lookup aggregates flows with domain names, allowing for analysis based on hostnames rather than IP addresses. This provides enhanced visibility into the endpoints of monitored traffic.

4.2.3 Geolocation insights

By using geolocation data to map network traffic to geographic locations, R&S®Probe Observer supports critical fault detection, enables GeoIP-based security measures, and provides valuable insights for performance monitoring.



4.2.4 Standard reports and insights

R&S®Probe Observer includes the following reports by default:

Standard reports	Insights for specific use cases
▶ Network ▶ Subscribers ▶ Attributes (related to subscribers) ▶ Applications ▶ Protocols ▶ DNS servers ▶ Domains	▶ Content delivery networks (CDN) ▶ Media streaming ▶ Domain details ▶ Domain relations

Beyond the default reports, R&S®Probe Observer offers more customizable widgets for creating tailored views for specific operational needs.

4.2.5 Reporting & measurement interval

Providing good customer care and real-time monitoring for network services depends on fine-grained data to quickly identify network issues and poor user experiences. In contrast, marketing use cases prioritize powerful application recognition over granularity.

R&S®Probe Observer is highly adaptable and offers flexible reporting and aggregation intervals. The solution continuously analyzes every communication stream with an aggregated value interval down to 1 second, periodically sending this data to the front-end.

4.3 Visual presentation

The intuitive, customizable web interface of the R&S®Probe Observer front-end includes multiple reports.

4.3.1 Overview of general traffic data

Application consumption insights

Gain valuable insights into subscriber behavior by analyzing the data volume of specific applications, their usage patterns over time, and their popularity within the subscriber base. Aggregated views of the data reveal weekly and monthly trends, as well as fine-grained activity at a 5-minute granularity, e.g. empowering CSPs to offer targeted marketing plans and generate additional revenue. Use the comprehensive view of the network traffic to spot weekly or daily fluctuations in downstream and upstream usage, and zoom in to proactively plan network capacity based on data usage patterns.

Access detailed insights into media streaming usage: For example, with an overview of the volume used per streaming type (audio/video), CSPs can compare paid with free content and gain a deeper understanding of subscriber preferences for paid subscriptions. Using these insights, they can refine marketing strategies and make informed strategic decisions regarding partnerships with entertainment and streaming platforms.

4.3.2 Insights on specific issues

Traffic mix of specific subscribers

Analyze one-day snapshots of an individual subscriber's traffic, and get detailed visibility into application, protocol, transport, and network layer characteristics. Understand upload and download volumes, identify data peaks, and troubleshoot network performance issues. The data resolution is configurable, offering granularity down to 5-minute intervals.

Detection of encrypted traffic

Identify encrypted communication patterns efficiently by using detailed analyses of encrypted traffic volumes within the network.

Overview of roaming subscribers

Discover roaming subscriber activity with detailed statistics, including aggregated data consumption rates per country of origin (mobile country code, MCC) and a breakdown of application usage. These insights empower operators to develop optimized roaming packages tailored to data rates and subscriber behavior, maximizing revenue opportunities.

Overview of mobile access technology

The solution provides detailed insights into data rates and subscriber statistics segmented by mobile access technology (UTRAN, EUTRAN, GERAN), along with correlated application distribution. This visibility allows operators to understand how applications use network resources and verify that protocols requiring higher data rates are using appropriate technologies.

Insights on content delivery networks (CDN)

Detailed analysis reveals which CDNs are most used, based on data volume, number of subscribers that access them, and domain usage. Detailed visibility into server locations by country/geolocation and throughput peaks allows operators to optimize peering arrangements and enhance connectivity to frequently accessed CDNs.

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 is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test & measurement, technology systems and networks & cybersecurity. Founded more than 90 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

ipoque GmbH

A Rohde & Schwarz Company

Augustusplatz 9, 04109 Leipzig

Info: +49 (0)341 59403 0

Email: info.ipoque@rohde-schwarz.com

www.ipoque.com

Rohde & Schwarz GmbH & Co. KG

www.rohde-schwarz.com

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG

Trade names are trademarks of the owners

PD 3610.3365.62 | Version 04.00 | September 2026

Solution Guide | R&S®Probe Observer

Data without tolerance limits is not binding | Subject to change

© 2026 Rohde & Schwarz GmbH & Co. KG | 81671 Munich, Germany

© 2026 ipoque GmbH | 04109 Leipzig, Germany