SUBSCRIBER AWARENESS

R&S®GSRM FOR GREATER VISIBILITY IN THE MOBILE CORE

Using GTP correlation to power mobile network analytics with real-time subscriber and session awareness

ROHDE&SCHWARZ

Make ideas real

INTRODUCTION

Billions of data packets navigate the Evolved Packet Core (EPC). This node processes and manages all the traffic that traverses today's 4G and 5G Non-Standalone Networks. The EPC, or the mobile core, hosts hundreds of network functionalities that shape these traffic flows, ensuring that the network is performing optimally at all times.

Central to all the processing that takes place in the core is network analytics. Network analytics delivers the intelligence required to fuel network operations and decision-making, not only within the core, but also across all other nodes between the access network and the network gateways, where control and user flows are processed and delivered for onward transmission. A large number of network functionalities such as routing, network address translation and security screening hinge on network analytics to support dynamic traffic policies and to automate the management of networks.

IP Probes

Network analytics is supported by a number of tools, namely IP probes. Deployed as a software that is embedded into an existing hardware or deployed as a proprietary hardware, IP probes work both actively, by logging each data packet that passes through a link, and passively, by sending queries to devices in the environment to collect data on network events, as IP packets are transported from one node to another. An IP probe collects and analyses a wide range of traffic data including bandwidth and speeds, protocols and ports, applications and services, hosts, IP addresses and session timings. Analytics from an IP probe is used to monitor traffic flows in the core and to feed various network subsystems that are dependent on its inputs. IP probes are also programmed to trigger alerts in the network when the logged parameters surpass their allowed thresholds.

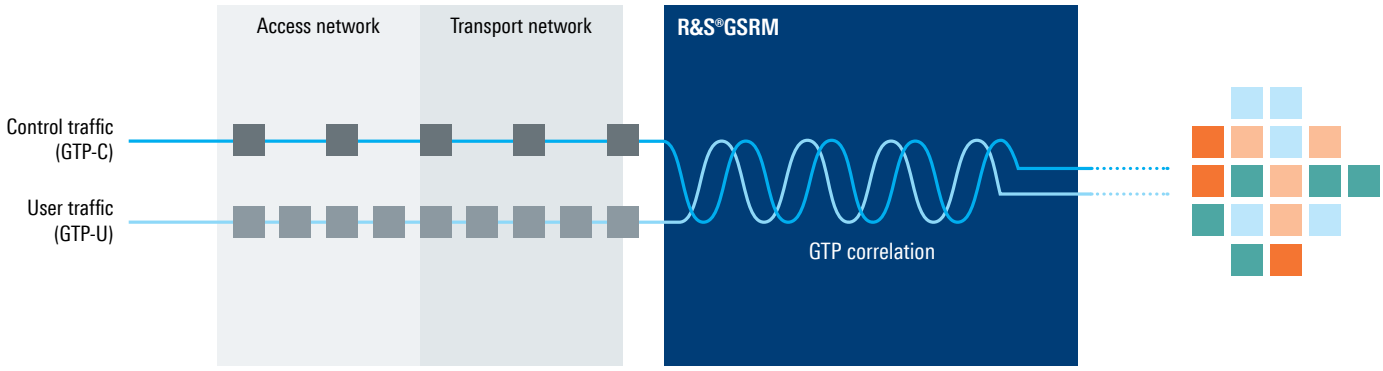
HOW TRADITIONAL LOAD BALANCING AFFECTS TRAFFIC VISIBILITY

With the rapid growth in traffic, a mobile core may feature multiple IP probes that operate as a subsystem. However, when two or more IP probes process packets simultaneously, packets from a single session or a single user are split into multiple flows and processed separately. This happens when networks deploy load balancing, where a network packet broker distributes incoming packets to multiple devices in a subsystem to reduce the processing load on any single device. Load balancing speeds up operations in the core and improves network performance.

Forwarding by a network packet broker typically uses rules such as packet rate, total traffic, bandwidth, number of connections or logical sequences such as round-robin or stateless hashing. While these rules provide a systematic method for distributing traffic, they lead to major visibility gaps in the core, especially as the number of devices in a subsystem multiply. Across an analytics subsystem for example, traditional load balancing leaves each IP probe with partial information on any given session. This leads to the impairment of an IP probe's functionality as the identification of sessions, subscribers, applications and anomalies and the timely communication of network events to other subsystems becomes difficult and time consuming.

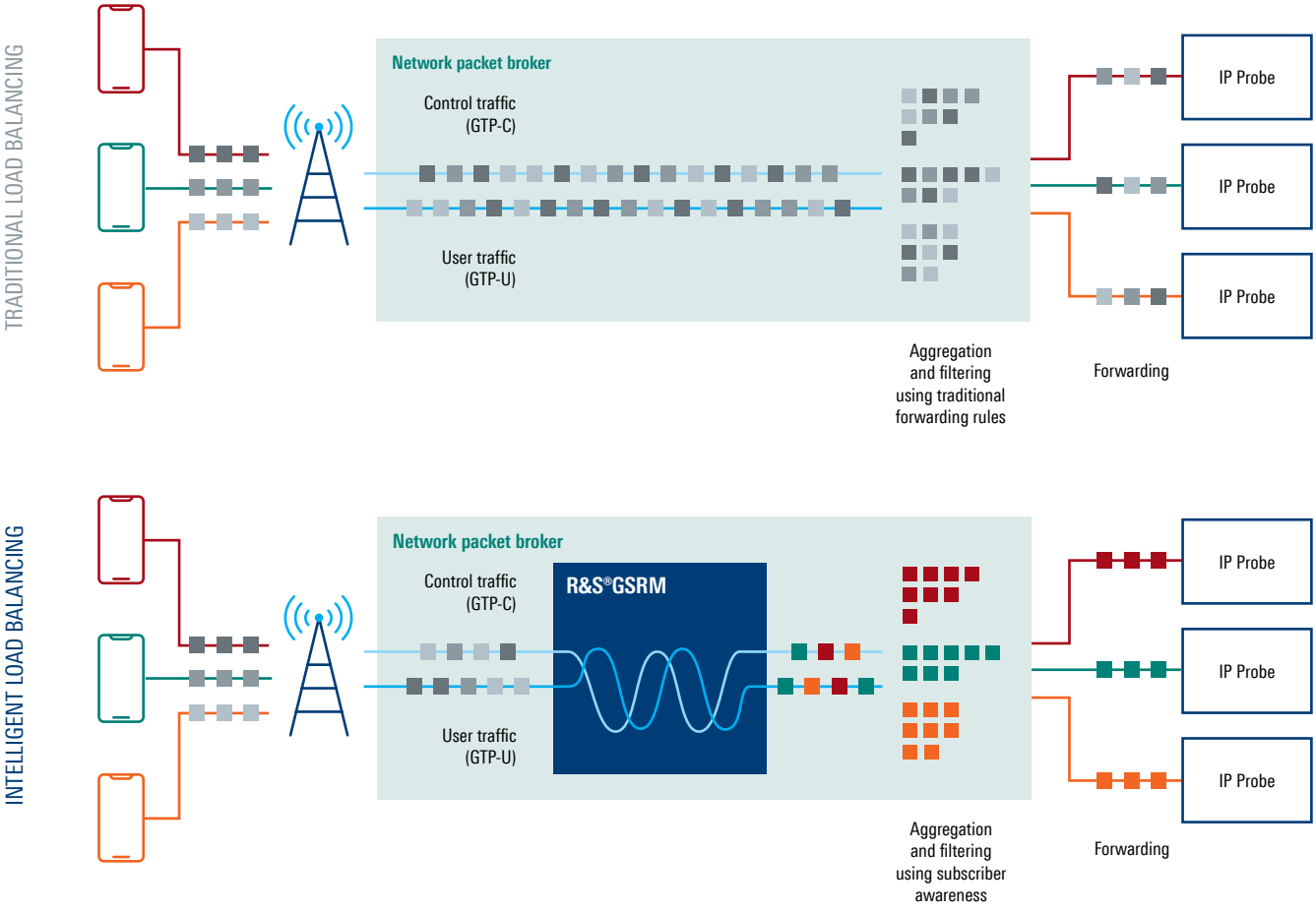
R&S®GSRM

To circumvent the limitations of traditional load balancing, network packet brokers can deploy the GTP Subscriber Resolving Module (R&S® GSRM). R&S®GSRM is developed by Rohde&Schwarz to deliver subscriber and session awareness for the mobile core network. R&S®GSRM uses the correlation of GTP user plane (GTP-u) and GTP control plane (GTP-c) to identify each packet by the subscriber. It correlates a wide range of GTP-c attributes with GTP-u's Tunnel Endpoint Identifiers (TEIDs). These attributes include the International Mobile Subscriber Identity (IMSI), the Mobile Station International Subscriber Directory Number (MS-ISDN) and the International Mobile Equipment Identity (IMEI). R&S®GSRM correlates traffic at both the GTPv1-C and GTPv2-C layers, with support for network interfaces such as Gn, S1-U, S11 and S5.



GTP correlation by R&S®GSRM

Using identification information provided by R&S®GSRM, a network packet broker is able to aggregate all packets of a session, and filter them by each subscriber. Packets from the same session are forwarded to a single device such as an IP probe, providing complete visibility for any end device, across any user session. With GTP correlation, operators do not have to rely on bandwidth-intensive, traditional session analysis, which is limited due to its inability to scale up to rapidly increasing traffic volumes in the core.

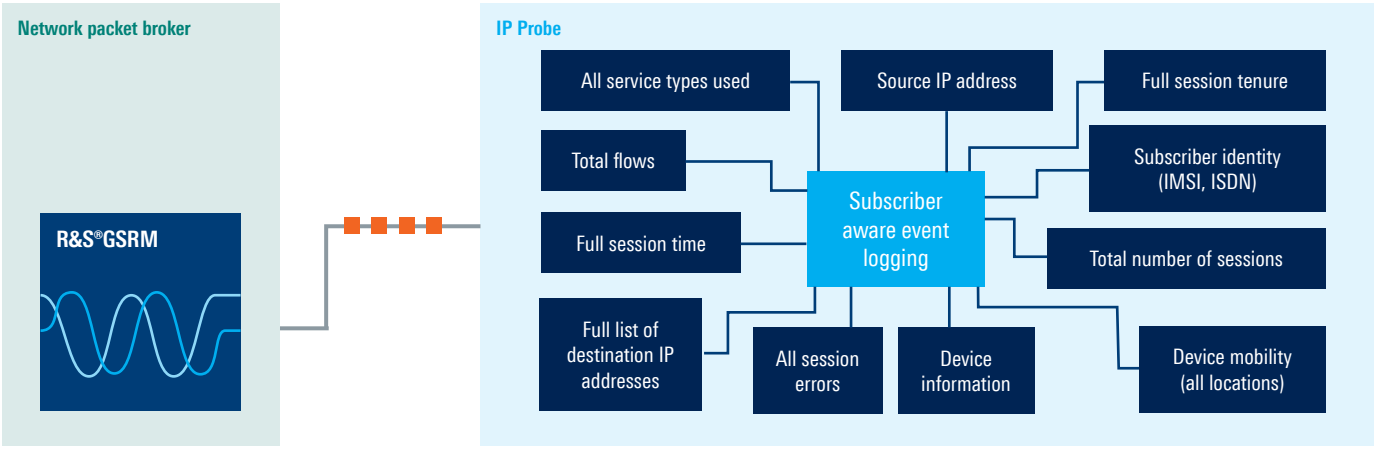


Traditional load balancing vs intelligent load balancing

Intelligent load balancing powered by GTP correlation also avoids onward processing tools in the core from being inundated with multiple, sometimes conflicting information about the same session, as devices processing different parts of a flow report different parameters. It also reduces redundant communication between network functions, which leads to improved network efficiencies.

In more advanced cases, subscriber awareness provided by GTP correlation enables session-specific manipulation of packets by network packet brokers. This includes replication and deduplication of packets as well as the creation of new metadata for a more detailed tagging.

SUBSCRIBER AWARENESS FOR NETWORK INTELLIGENCE



Processing of subscriber-filtered traffic by an IP probe

IP probes decipher network traffic by reading and logging data that is readily available in the header of a packet. This includes information such as source and destination IPs, packet size, device identity, device type and location.
IP probes also calculate and report wider traffic attributes such as speeds and latency. While the analysis of this data provides basic information on network performance and its usage, subscriber awareness provided by R&S®GSRM powers IP probes to deliver deeper and more accurate insights on traffic flows navigating the mobile core for a number of important use cases. These can be divided into the following categories:

Monitoring subscribers

By processing all the packets of a session in a single sequence, an IP probe is able to compute various metrics relating to a subscribers' mobile usage in real-time. This includes the total duration of a subscriber session, the average duration of a subscriber session for a given time, the average duration of a session for a given subscriber and the frequency with which a subscriber accesses the network. By aggregating data from a subscriber class, mobile operators are able to compute similar metrics for various subscriber classes for a meaningful comparison on how plan types influence subscriber network usage and behavior, in real-time, without lengthy post-processing of separate sets of data logs. This information can be used to deliver customer-specific deals/plans, for example, high-worth customers who exhibit high consumption of data can be offered a special rate/add-on quota.

Monitoring network performance

Having complete visibility into a session also translates to superior network performance analytics. Mobile operators are able to determine a session's attributes such as speeds, bandwidth usage, packet loss, latency and jitter by logging all packets from a session in a single IP probe. Session performance data is critical in determining if an active session is being handled according to its SLA and also in identifying past sessions that may not have met the required SLAs. This can be used by IP probes to trigger alerts in the system and to provide first-level indicators that can be used in issue diagnosis. In a traditional load balancing scenario, performance issues are detected only upon the completion of post-processing analysis which involves collection, aggregation and reconciliation of data from all active probes at various intervals.

With intelligent load balancing, IP probes can also be configured to extend session performance analysis to various access points, enabling operators to establish performance attributes for a single cell site, a region, an edge network and the entire network. This allows operators to monitor and identify issues that are specific to a node.

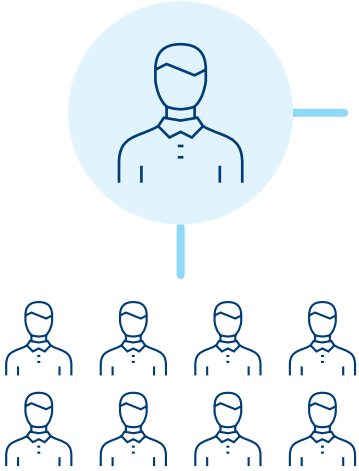
In combination with subscriber information, session performance data also allows mobile operators to determine subscriber experience for a given time, day, week or month. Intelligent load balancing enabled by R&S®GSRM allows mobile operators to identify, in real-time, the effect of network performance on subscriber usage, and vice versa. It also enlightens operators on how different subscribers are reacting to different network events. More importantly, it enables operators to pinpoint subscribers who can be the source of network issues such as congestion or DDoS attacks.

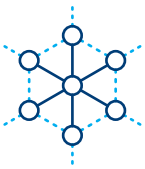
Designing policies and rules for traffic management

With subscriber and session awareness, traffic analysis becomes more accurate, as the risks for data loss and data duplication are minimized. This analysis is valuable in setting new policies and rules for network management as content and subscriber trends can be used to decide on how traffic should be routed, managed, charged and secured. Accurate identification of subscribers and sessions via intelligent load balancing also enables IP probes to support network automation powered by AI-based techniques such as deep learning (DL) and machine learning (ML). It allows network functions to automate network responses using dynamic rules built on past subscriber and session data.

Sampling for analytics subsystem

Session/subscriber awareness is particularly important for traffic forwarding that involves an analytics subsystem because it allows the use of sampling, where representative flows are used to analyze the overall traffic. Sampling significantly reduces the resources spent on traffic analysis and accelerates traffic processing. For example, the number of IP probes and the processing cycles within a probe can be highly optimized with the use of sampling. Sampling also allows customized forwarding. Operators can, for example, forward traffic from high ARPU subscribers in full while using sampling for traffic from low ARPU subscribers. Using data pools, operators can select unique samples to be forwarded, matching them to the analytics subsystems to which the packets are forwarded.





Supporting network functions to implement session- and subscriber-based policies

Apart from helping operators develop dynamic policies and rules, intelligent load balancing enables IP probes to support network functions relating to IP traffic management, policy control and security, in implementing these policies and rules. For example, video traffic from high-priority customers is automatically optimized to the content quality and screen size to deliver the best viewing experience for this user group. Where policies are based on session parameters and thresholds, for example maximum session tenure or total memory used, or subscriber attributes such as bandwidth consumed and number of concurrent requests at any single time, analysis provided by an IP probe allows for these policies to be executed effectively for each distinct user classes.

Enabling application-specific traffic management

In a data-driven age, identification of applications enables operators to apply differentiated routing, caching, compression and security filtering rules to different application classes. Identification of applications also allows custom rating and charging. To deliver application awareness, IP probes are often embedded with traffic inspection technologies such as deep packet inspection (DPI). DPI enables an IP probe to log data beyond the generally available information extracted from a packet header, which leads to deeper and more granular insights relating to each packet payload.

With R&S®GSRM, DPI delivers this not only in real-time as the first packets hit the network, but also does so with high accuracy given that all session packets are pre-aggregated and delivered to each probe in succession. Quick identification of applications allows IP probes to communicate the information to policy control and AAA engines as well as security tools in the mobile core such as intrusion prevention systems or next-generation firewalls. This allows real-time invocation of application-specific rules. For example, applications susceptible to malware will see the associated packets routed through additional malware screening. Other examples include scenarios where a charging engine zero-rates the use of educational websites and where a policy control engine delivers contextual content offers such as discounted time-based Facebook passes.

Delivering location-based services

In a heterogeneous network setting, session metadata provided by R&S®GSRM covering cell location and bearer fields allows for an IP probe to map a subscriber's mobility pattern in real-time, and use this information to offload data to another available connection, for example, from LTE to 5G or from 3G to an operator WiFi hotspot. This helps operators maximize network capacity and improve service quality. Subscriber mobility patterns can also be used to trigger location-based offers. This is particularly beneficial when an IP probe is tasked to send relevant inputs to a policy control engine in charge of creating and sending timely offers that can range from merchant deals to operator WiFi hotspot access.

Optimizing network resources

Analytics is key for monetization. With session awareness, IP probes enable network management tools to compute resources consumed by specific sessions and subscribers, allowing revenue metrics such as ARPU to be computed in real-time. Session awareness also helps operators curtail overages, as well as network abuses such as illegal tethering because all concurrent sessions from the same SIM are delivered to the same probe.

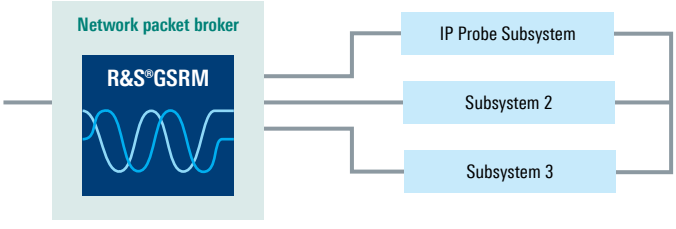
WHY R&S®GSRM

Network intelligence hinges on the ability of operators to record, monitor and analyze data in real-time, regardless of the number of sessions and subscribers. R&S®GSRM delivers exactly this, supporting the ecosystem of devices involved in providing timely traffic insights across 3G, 4G and 5G networks. It enables network monitoring tools such as IP probes and traffic forwarding devices such as network packet brokers to benefit from a rich set of capabilities such as:

- An OEM software module that can be implemented in any network environment and integrated into any end solution without vendor lock-in
- A multi-core architecture with linear scalability to satisfy high bandwidth demands
- Easy-to-use REST APIs for seamless and fast integration
- Efficient total cost of ownership (TCO) from predictable costs and flexible SLAs
- Ready pairing with the renowned, high-performant DPI engine, R&S PACE 2 for a highly reliable classification of applications and protocols. R&S PACE 2 boasts a comprehensive traffic signature library and the use of ML and DL for real-time traffic identification, even for traffic that is encrypted or obfuscated.

Deployment options

Analytics tools such as IP probes can enrich their functionalities with R&S®GSRM-powered subscriber awareness using the model of deployment that best suits the environment they operate in. For example, when R&S®GSRM is readily embedded in the network packet broker used in the core network, IP probes benefit from the consistency in traffic analysis across all core subsystems using the same session data sets. This allows its analytical outputs to be congruent with any packet information extracted by these subsystems (refer Model 1).



Model 1

Where intelligent load balancing is unavailable within the core, IP probe vendors can provide their own network packet brokers that are embedded with R&S®GSRM. This model is suitable for larger deployments where volumes and budgets justify such investments. It also enables more targeted deployment for R&S®GSRM (refer Model 2).

Model 2

For IP probes and analytics tools requiring a more customized analysis of sessions and subscribers, R&S®GSRM can be built directly into the processing device and configured to meet their specific requirements (refer Model 3). As an OEM software, R&S®GSRM offers seamless integration into any GTP traffic processing tool.

Model 3

CONCLUSION

Network analytics will continue to play a pivotal role in the management of mobile networks. For operators seeking a cost-effective and scalable means to delivering richer traffic insights built on subscriber and session awareness, R&S®GSRM provides a lean and highly efficient solution capable of supporting a wide range of network subsystems. Network packet brokers in particular, benefit tremendously by being able to forward packets that are session-aggregated and session-filtered, fuelling smart distribution of traffic within the core network. IP probes, tasked with monitoring network events and delivering real-time deep insights into the network, benefit from complete visibility into subscriber sessions. These insights in turn enable operators to capture and maximize the value of each subscriber and each session, enhancing network performance and its monetization.

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 3683.7125.32 | Version 01.00 | March 2022
Use case | R&S®GSRM for greater visibility in the mobile core
Data without tolerance limits is not binding | Subject to change

3683712532
3683.7125.32 01.00 PDP 1 en