Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING
WHITE PAPER

A Probe-Based Approach to Service Visibility

A Heavy Reading white paper produced for RADCOM

RADCOM

AUTHOR: JAMES CRAWSHAW, SENIOR ANALYST, HEAVY READING

EXECUTIVE SUMMARY

In Heavy Reading's view, service assurance systems should measure and detect problems in real time and provide feedback to orchestration systems to enable closed-loop automation. The application of advanced methods of predictive analytics and machine learning is now making it possible to anticipate network and service quality degradations, enabling operators to take proactive action or even automate preemptive action.

Legacy service assurance solutions that many operators still use are expensive to operate and hard to adapt to changing network technologies and services. They provide no single-pane-of-glass view or correlation across subsystems. Operators lack a network-wide context when evaluating problems. Legacy systems suffer from an excessive number of events, noise, and duplication, leading to many non-useful trouble tickets. They lack support for collaboration, which means that domain-specific teams are left to do troubleshooting in silos. They also suffer from reactive workflow – too much time is spent on customer-reported faults, which does not leave enough time for proactively preventing problems.

The fundamental problem with legacy service assurance tools, as used in a network operating center (NOC), is that they lack service-level awareness. What is needed instead is a service operating center (SOC) capability that can answer the question of what is the service experience through the eyes of customers. For example, is the user trying to watch streaming video on a device that recently had its firmware updated and is now suffering from repeated buffering? In this case, only monitoring the resource and network layer is not enough. To understand why the video is not streaming adequately, we need to see the service layer.

By monitoring key performance indicators (KPIs) and key quality indicators (KQIs) that are calculated based on probe-based data enriched with additional data sources (e.g., from operations support systems [OSSs] and business support systems [BSSs]), operators can gain an end-to-end view of the service on a per-subscriber basis. The SOC can provide real-time visibility to the customer care team and engineering about network events and their service impact. Through automated root cause analysis, the SOC can suggest fixes that reduce the time to resolve complaints. The probes themselves are a key tool in troubleshooting problems. The comprehensive insights delivered by correlating probe-based data and OSS/BSS data mean that operators can truly understand the end-to-end service and customer experience on a per-application basis.

The SOC can prioritize network issues that affect high value VIP customers or customers that may be at risk of churn. The customer experience management aspect of the SOC generates benchmarks on the quality of experience and tracks the impact of network changes on the net promoter score. The SOC acts as a linchpin between the business-facing side of an operator (customer care, sales, and marketing) and the operational side (network planning, optimization, and engineering).

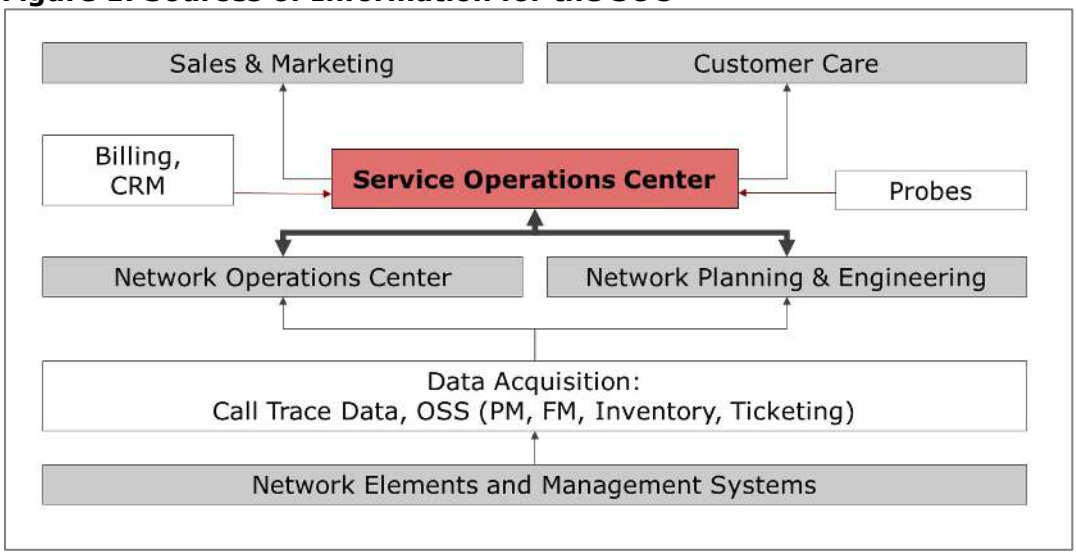
FROM NETWORK TO SERVICE VISIBILITY

The SOC concept has evolved from the traditional NOC to reflect a service-centric approach to management as opposed to the traditional network element-based approach. Monitoring a service requires end-to-end visibility, rather than focusing on isolated, domain-specific silos.

The SOC tracks KQIs (e.g., video service quality) and key business indicators (e.g., churn) whereas the NOC is more focused on traditional KPIs (e.g., dropped calls, packet loss, latency). By taking a more business-oriented approach, the SOC is able to prioritize specific services, such as streaming video, or customer groups, such as VIPs. The SOC also has a strong focus on predicting service impact, unlike the NOC, which is more reactive.

The SOC is supplied with multiple sources of information, as **Figure 1** indicates. At the bottom are the traditional OSS feeds (performance monitoring, fault management, alarm management, trouble ticketing) already used by the NOC and network engineering functions. The SOC complements these with additional information from probes and BSSs, such as billing and customer relationship management (CRM). These additional sources help with problem troubleshooting while also enabling the operator to identify which individual subscribers are affected. If these are high value customers, a problem can be escalated accordingly. Note that the SOC can also provide feedback to the NOC and network planning functions (as indicated by the bidirectional arrows below). The SOC can provide them with additional insights (e.g., where network capacity should be added to benefit VIP customers) or instructions (e.g., requesting the NOC to resolve a network issue that is affecting service quality but has not yet generated any network alarms).

Figure 1: Sources of Information for the SOC



Source: Heavy Reading

How Service Quality Management and Customer Experience Management Relate to the SOC

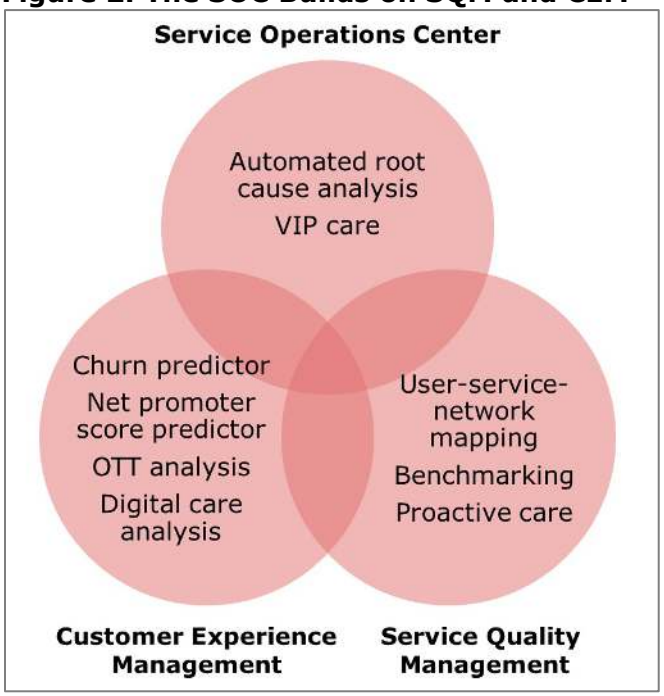
As **Figure 2** below indicates, the capabilities of the SOC include customer experience management (CEM) and service quality management (SQM). These may be deployed as separate systems or as one holistic system, depending on the architecture a particular operator chooses.

SQM takes network KPIs and other data (e.g., device type, location) to create quality of service (QoS)-oriented KQIs. These KQIs can be used to identify service quality degradations (e.g., call handover failures for voice over long-term evolution [VoLTE]) before there is any impact on customer experience. SQM can drill down to pinpoint the network resources that are causing the problem.

CEM is a broad set of capabilities, based on the analysis of service-oriented KQIs, designed to manage customer satisfaction, loyalty, and advocacy. The CEM generates a customer experience index through its monitoring and analysis of its multiple data feeds. This index can be based on factors such as the following:

- Product experience (e.g., network quality, VoLTE, roaming)
- Customer service (e.g., proactive customer care)
- Billing experience (e.g., accuracy, understandability)
- Complaint handling (e.g., reactive customer care, first-time resolution)

Figure 2: The SOC Builds on SQM and CEM



Source: Heavy Reading

SOC AS THE ORGANIZATIONAL LINCHPIN

The SOC plays a key role in supporting customer-facing departments, such as customer care, sales, and marketing. The SOC can act as a liaison between these business-oriented teams and infrastructure teams, such as network operations and engineering. By using the same data and analytics in customized views, the teams are better able to collaborate and solve problems collectively.

How the SOC Supports Customer Care

The visibility and analysis that the SOC provides can enable a higher rate of first-call resolution by the customer care team and reduce the average call handling time. This enables both higher customer satisfaction and lower opex. The SOC is fed with customer complaint data from the customer care team and is able to pinpoint whether the problem is related to the network, their device, or some external factor. It is also able to act proactively, warning the customer care team when a network problem has occurred so that they can be prepared for inbound complaints. The team can even begin outbound proactive communications with customers, advising them that a problem has been encountered and is being addressed.

How the SOC Supports Marketing

The insights the SOC generates about customer usage could enable the marketing department to devise new offers that help the operator stand out in the market. Examples include free data allowances for certain applications (e.g., WhatsApp, Spotify, etc.). Such offers could be made independently or in collaboration with over-the-top (OTT) application providers. Another marketing use case is the identification of customers who are using the latest generation handset (e.g., 5G) but have not yet been permissioned for this (i.e., still on 3G since an old SIM card has been used). By proactively contacting these customers and making them aware of their eligibility for a superior radio technology, the operator could increase its revenue potential and avoid a possible customer defection.

How the SOC Helps Network Planning and Optimization

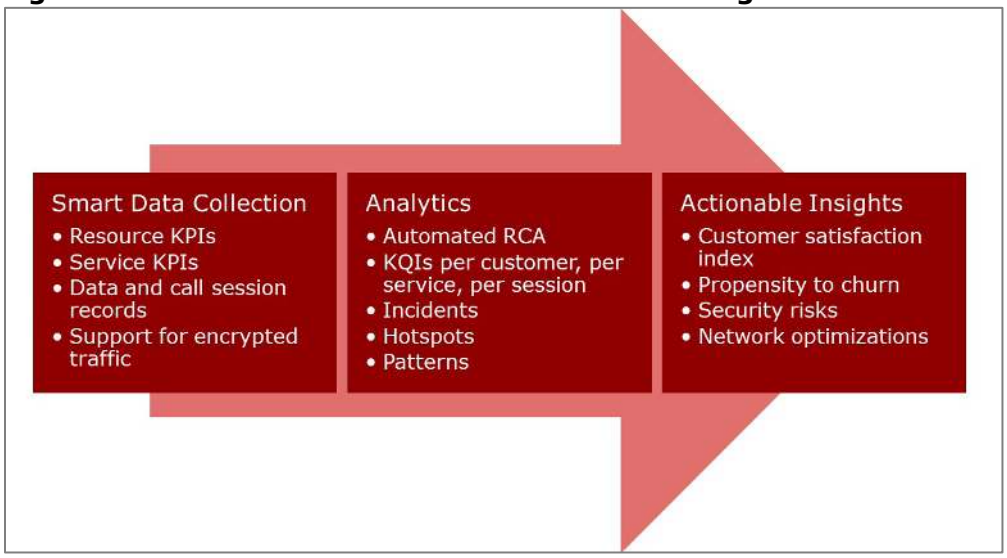
While the network planning team already has a plethora of performance monitoring tools, what it lacks is an appreciation of the impact on service quality of the changes that they make to the network. The SOC can provide inputs for capacity planning and optimization based on service and subscriber analytics. Rather than optimizing network capacity utilization, the focus becomes service quality optimization. Instead of planning networks based on broad measures of traffic, operators can plan their coverage requirements based on application usage, bearing in mind that different applications have different sensitivities to latency and packet loss.

How the SOC Can Help the NOC

While the NOC can be a useful source of information for the SOC, the flow of information is increasingly from SOC to NOC. By harnessing insights into customer impact, the SOC is able to help the NOC prioritize trouble tickets based on service and customer impact. In particular, network improvements to support VIP customers (large value or influential) can be prioritized over general users.

Figure 3 summarizes how the SOC applies various analytics techniques to the data it collects and produces actionable insights that are useful to multiple parties within the service provider.

Figure 3: How the SOC Generates Actionable Insights



Source: Heavy Reading

KEY DATA SOURCES FOR THE SOC

As discussed above, the SOC collects data from a number of sources, including traditional performance and fault management systems. While these provide detailed information on nodes/elements throughout the network, they do not offer any service- or subscriber-specific data and are, therefore, of little use for subscriber problem troubleshooting or CEM (see **Figure 4** below).

More useful is cell trace record (CTR) information, which can be collected from the radio access network (RAN). CTRs contain user information (identifiers), traffic type and destination information, radio network quality parameters, and bearer type, indicating the type of service being used (streaming video, conversational, etc.). However, CTR information is only available in the RAN, so in order to achieve end-to-end visibility, it must be complemented with additional information coming from probes.

Figure 4: Usefulness to the SOC of Different Data Sources

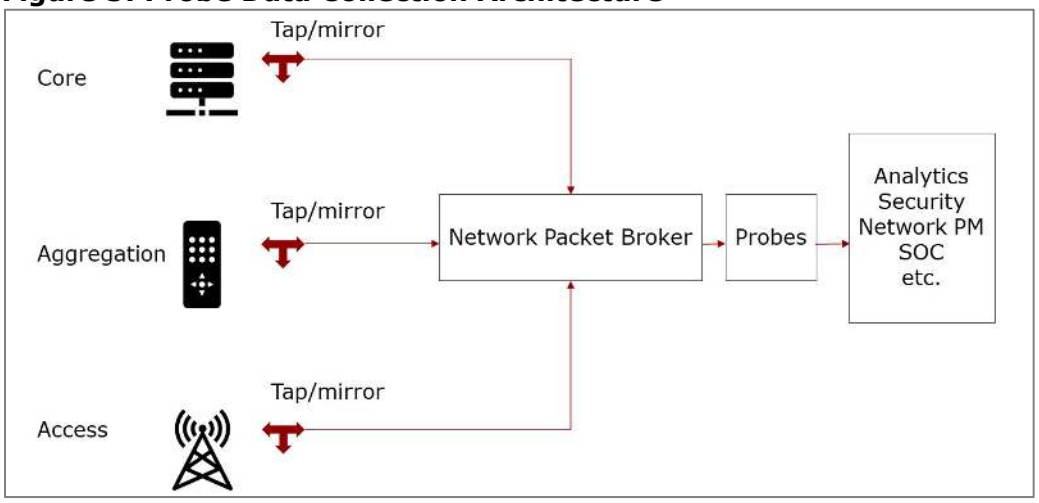
Metrics	Probes	Cell Trace Records	Performance Management	Fault Management
Coverage	Anywhere (virtual probes for control and user planes can be on-demand)	RAN	Full network	Full network
Granularity	Per node, service, subscriber, session	Per RAN	Per node	Per node
Network Troubleshooting	Yes, wherever deployed	In RAN only	No subscriber-level view	No subscriber-level view
Importance to CEM	High	High	Low/none	Low/none
Importance to SOC	High	Medium	Medium	Medium

Source: Heavy Reading

Probe Data Collection

The process of probe data collection has a number of steps, as shown in **Figure 5**. Each device or network function to be monitored must have a tap connected, which feeds one or more network packet brokers and, in turn, feeds the probes and other systems.

Figure 5: Probe Data Collection Architecture



Source: Heavy Reading

The tap requires the use of a spare port on a network device, which is used to send a copy of the network traffic (control and user plane) via a separate optical network that is dedicated to monitoring. With the move to network function virtualization (NFV), operators now use virtual taps (vTaps). The vTap is co-resident with the service virtual network function (VNF) of interest and uses packet mirroring at the shared virtual switch. Alternatively, it may use port mirroring at the network interface card (single root input/output (I/O) virtualization) or top-of-rack switch port mirroring.

Passive vTaps deployed on a VNF interface measure the following:

- Detailed VNF transaction records (flow records, session records, transaction records, etc.)
- Control-plane message stream processed by the VNF
- User-plane stream (IP addresses, time interval, etc.)

Replicated data from taps is then passed to the network packet broker (NPB). The NPB aggregates the data, manipulates it (e.g., packet deduplication, header-stripping, time-stamping), and relays it to probes and other clients for network operations, security, and other uses.

Note that the NPB filters the data, only sending traffic that is relevant to the issue being investigated. It provides load balancing so that if one probe is overloaded or fails, the data can be rerouted elsewhere for analysis. The NPB can also carry out secure sockets layer (SSL) decryption (to gain more visibility into the network traffic) and generate NetFlow records, along with additional context-aware extensions like uniform resource locators (URLs) from traffic fed to the visibility platform. The NPB should be able to correlate between data interfaces in order to take actions based on the subscriber ID (international mobile subscriber identity [IMSI], international mobile equipment identity [IEMI], etc.).

Probes On-Demand for Troubleshooting

While probes can provide granular information (per node, service, subscriber, session) and be deployed anywhere in the network, in practice, it is not cost effective to deploy them everywhere all of the time. Many parts of the transport network (e.g., IP/multiprotocol label switching [MPLS] routers) are so reliable that there is little need for probes to analyze them. A great deal of information in the RAN can be collected from CTRs. However, in aggregation and for the many core network elements that make up a mobile network, probe analysis can be invaluable. Typically, an operator would look to collect 100% of the control-plane data from such elements, but only monitor a small sample of user-plane traffic (e.g., 10%). If problems are detected, then additional virtual probes can be spun up and deployed to increase the size or frequency of samples. Once the issue is resolved, the probes can be wound down and the associated computing resources released back to the network.

Operators should take an on-demand approach to service assurance and network visibility, using smart sampling and filtering on specific datasets. They can then decide, on the fly, on which areas of the network they want to perform in-depth analysis, zooming in on high priority issues or selected customer groups.

BENEFITS OF PROBE-LEVEL VISIBILITY

The probe-fed SOC/CEM provides an end-to-end view that enables the prioritization of network issues according to their service and customer impact. By understanding the impact on the subscriber, operators can troubleshoot issues faster and improve the customer experience. Customer care representatives can gain access to customer-level diagnostics that guide them through a series of recommended steps, leading to higher first-call resolutions rates. Marketing can execute promotions based on known customer value and measured service quality deviations in order to optimize churn (reducing it for high value customers). Engineering can better prioritize capacity expansion and problem resolution based on the impact on customer service.

Benefits for Customer Care

- Reduce mean time to resolve (MTTR) for customer complaints; greater first-call resolution
- Notify customers of problems that have been identified (e.g., phone OS update leading to performance degradation) before they complain
- Improve customer satisfaction and loyalty; avoid potential revenue loss

Benefits for Marketing

- Segment customers based on application usage (e.g., streaming video)
- Optimize churn; focus promotions on high value customers
- Understand bandwidth consumption by application for better campaign management

Benefits for Engineering

- Prioritize problems in the network based on high value customer impact
- Understand the impact of OTT usage; better capacity planning
- Improve capacity management based on high value subscriber location; prioritize opex and capex

ABOUT RADCOM

RADCOM (NASDAQ: RDCM) is the leading expert in cloud-native Network Intelligence for telecom operators transitioning to software-defined networking (SDN)/NFV. Providing a critical first step in an operator's NFV transformation, RADCOM's Network Intelligence delivers end-to-end network visibility from virtual tapping point to network insights. Consisting of RADCOM Service Assurance, RADCOM Network Visibility, and RADCOM Network Insights, RADCOM's Network Intelligence portfolio provides operators with complete visibility across their virtual and hybrid networks. RADCOM Network Intelligence is automated, cost-efficient, provides on-demand functionality, and is specifically designed for the needs of telecom operators. RADCOM specializes in assuring next-generation, high capacity networks, including LTE, Advanced-LTE, 5G, IP multimedia subsystem (IMS), SDN/NFV, and others.

Further reading:
RADCOM SOC and CEM Solution