Whitepaper

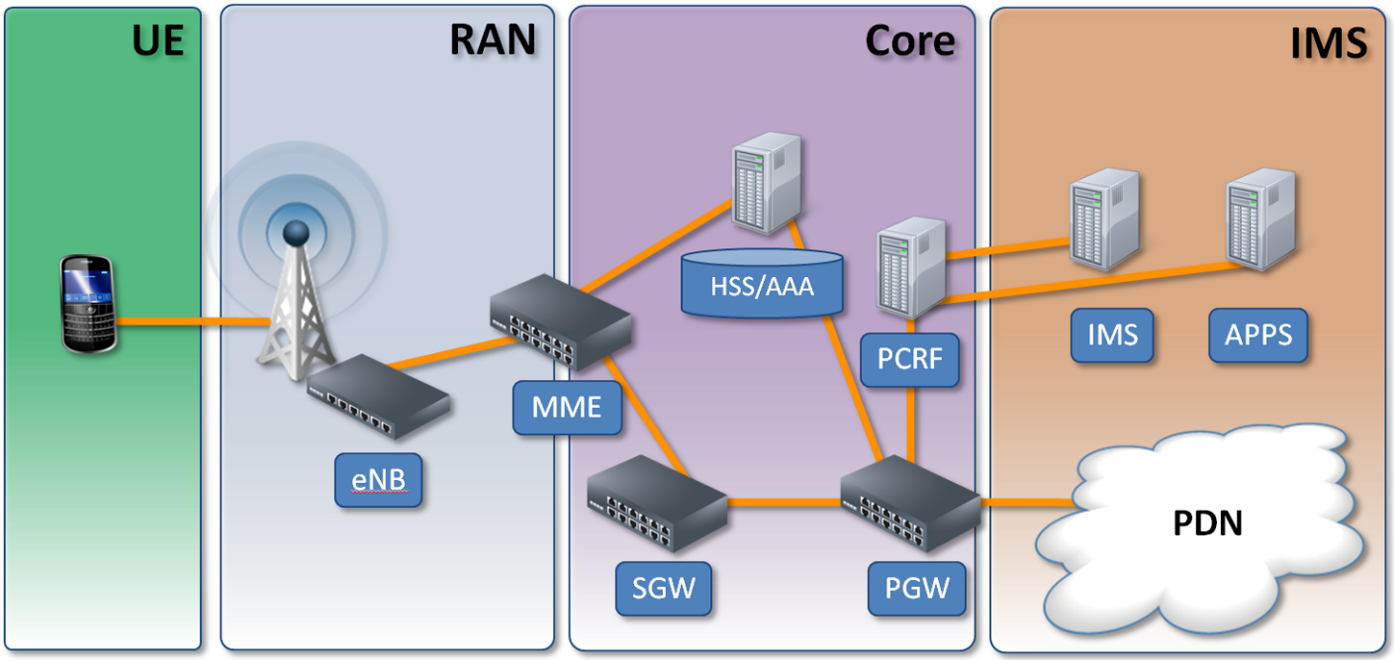
10 Metrics to Monitor in the LTE Network

The deployment of LTE increases dependency on the underlying network, which must be closely monitored in order to avert service-impacting events. In addition, the rise of vendor-specific performance management platforms establishes barriers to end-to-end network visibility and hinders operational troubleshooting. The following whitepaper highlights ten critical metrics for successful monitoring of an LTE network and recommends solutions to LTE monitoring challenges.

LTE was designed to increase the capacity and speed of wireless data networks by moving away from dedicated circuit networks to a more simple IP-based architecture with significantly reduced transfer latency. The migration to an all-IP infrastructure of converged voice, video, and data places additional emphasis on the underlying network and associated mechanisms, all of which must be closely monitored in order to avert service-impacting events.

In order to ensure efficient delivery of services and Quality of Experience (QoE) for the customer, the following performance metrics must be monitored and collected in the LTE environment:

1. Authentication Response (AAA)
2. Firewalls and Load Balancers (Connections, Sessions)
3. CPG/PGW/SGW Gateways (Web Connect, IP Pools, Current Session, QoS, Traffic)
4. MME (Successful Bearer Established)
5. eNb (Upload, Radio Resource Management)
6. Transport: Switches (Queues, Load)
7. Physical Servers (CPU, Memory, Interfaces)
8. Synthetic Testing (Y.1731, RTP, SIP Connect - Call Setup)
9. Application Flow (Capacity)
10. Signaling (S1, X2)



Monitoring performance metrics across each layer of the LTE and IMS architecture provides a complete and immediate view of infrastructure performance and user impact.

1. **Authentication**
   The load caused by authentication creates many issues for carriers. In addition to collecting baselines for internal user metrics, synthetic tests should be used to check the availability of the authentication process (AAA, HLR/HSS) and provide a user experience metric that ensures the UE can be authenticated on the network. Employing a multi-layered testing strategy requires a simple ping on the DNS name (to test the lookup), a port lookup test to query if the port is accessible, as well as a more thorough test of the authentication process itself. This multi-layered approach indicates if there is an issue with the server, the process, or the backend application itself.

2. **Firewalls and Load Balancers**
   The core is front-ended with load balancers and firewalls. Monitoring the number of connections and sessions prevents overload that might indicate Distributed Denial of Service (DDoS) attacks and ensures the performance of these devices as they protect the core. New load balancers can use performance information from other parts of the infrastructure to perform on-demand updates to the routes, provide in-line insight, and manage user function.

3. **PDN Gateway and Serving Gateway: CPG**
   In the IP environment, it is important that the PGW has sufficient IP addresses in the pool for the requesting User Equipment (UE). Alerting on abnormal allocation – as well as capacity prior to exhaustion – is critical to maintaining user connectivity. Collecting session and connection history provides an understanding of baseline usage patterns and allows for alerting of abnormal behavior. Understanding the connectivity to the Internet (HTTP requests) allows for more efficient routing and – combined with the SGW QoS metrics and traffic behavior – provides offloading assistance in peering decisions. As the SGW is the connect point for traffic, making sure that it has sufficient memory and processing power is critical to its serving functions.

4. **MME**
   An important metric for service connectivity is bearer success history of the end user equipment (and its associated ratio of success to failure). Monitoring the S6a interface for effective success ratio of subscriber information reveals if the UE is successfully entering the network. This data also provides usage information for capacity planning and capital expenditures. In addition, understanding the performance of the transport (router/switch) in time context with the MME provides insight as to the impact of the infrastructure on the service.

5. **eNodeB**
   While the eNB does not provide direct communication with the UE, it does motivate and manage the complex radio initiatives. It is specifically important to monitor the radio bearer, radio admission, and connection mobility control, as well as the uplink/downlink scheduling. Combining metrics around radio resource provides a Radio Quality indicator to allow for 'hot spot' determination. As the eNB provides the forwarding/routing function to traffic transiting the tower, it is important to make sure that the data utilization to SGW stays within quality limits.

6. **Transport**
   All service to and from the UE depends on the devices that transport the packets. Performance monitoring and the creation of thresholds for metrics such as CPU and memory on Layer 1, 2, and 3 devices, as well as the performance metrics (Utilization, IN/OUT, Discards, etc.) of individual interfaces across multiple technologies (Ethernet, MPLS, Microwave, etc.) are critical to the delivery of end-to-end service and each individual service component.

7. **IMS/Applications: Physical Servers**
   At the core of the network is a sophisticated data center, with applications and the hosting servers constantly under stress from the demands of the network. The control mechanisms are not purpose-built hardware, but servers loaded with sophisticated software (EMS, Authentication, Control Plane functionality, and the IMS core applications). Traditional monitoring of these servers' critical components becomes extremely important, as well as monitoring the processes necessary to keep user sessions active. CPU, memory, processes, and interface statistics provide insight into the health of the devices.

8. **Bearer Path Testing**
   While performance of devices is important in transit, end-to-end performance – latency, loss, jitter at L3, and frame delay, frame loss, and FDV at L2 – is critical to end user experience and customer satisfaction. The performance of voice and real-time streaming data are highly dependent upon low latency and loss metrics. Network Operations must be alerted in real-time of any degradation to performance or increase in latency, jitter, or number of lost packets. While the ITU specifies parameters for synthetic testing (such as jitter < 30ms), all parameters are changeable and most are likely to be more stringent than the "norm." Ethernet backhaul emulates the Classes of Service (CoS) inherent within circuit-switched technologies such as ATM and frame relay in order to meet commitments on bandwidth and QoS. Network Engineering and Operations must also be able to understand the performance of their backhaul links and backhaul service providers, easily segment the network and isolate troublesome spots, optimize performance, and increase customer quality of experience.

9. **Application Flow**
   Traffic flows from many different parts of the network can be analyzed for application behavior along with UE analysis for troubleshooting configuration changes and capacity/traffic engineering. The volume of data from flow sources is typically too large to be analyzed in real time, but a drill down into atypical behavior allows for detailed forensic analysis.

10. **Signaling**
    There are a variety of 3GPP signaling interfaces that should be monitored, including S1 for MME to eNB communication and X2 for handoff. While it is possible to obtain internal metrics around how many, how fast, and how long, an external metric will provide an additional layer of service for the signaling path. While it was previously mentioned that the bearer path should be tested, it is also good practice to test the signaling path. While it may not be possible to test and measure delay device to device, it may be possible to test from access-device to access-device. Monitoring the performance of latency along the signaling path and alerting on threshold violations provides a 'first alert' to signaling delays and potential failures. There are a variety of 3GPP signaling interfaces that should be monitored, including S1 for MME to eNB communication and X2 for handoff.

The LTE Monitoring Challenge

An increase in the number of new technologies offered by major vendors in the LTE market – such as Alcatel-Lucent, Cisco, and Ericsson – has driven a similar increase in the number of stand-alone management systems that rely on difficult-to-access performance data for the specific portion of the network they monitor. SNMP is not always available to the individuals responsible for monitoring the health of specific devices.

Having multiple, disparate performance monitoring and reporting tools for the LTE network presents a number of challenges:

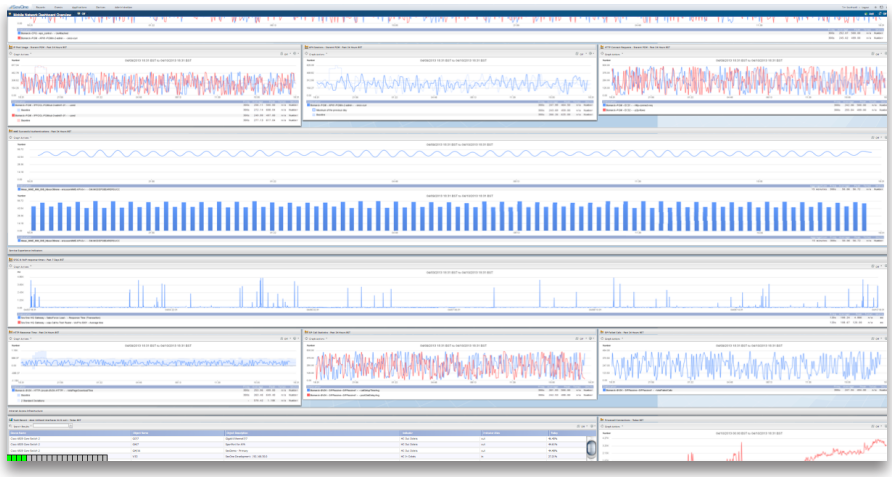
- End-to-end visibility is difficult to achieve from a single pane of glass
- Correlation of events is problematic
- Gaps in network visibility increases service risk
- Management silos hinder communication among internal groups
- Troubleshooting becomes more difficult, increasing MTTR

In addition, these fragmented management tools often do not store historical data for more than four to six weeks, or they do not baseline performance – a pre-requisite for an intelligent alerting system.

The Solution: SevOne

SevOne provides the world's fastest, most scalable network management and reporting platform, delivered as an all-in-one solution, to help network engineering and operation teams detect and avoid performance events before they impact service delivery.

SevOne provides the ability to alert – in real-time – on increased latency, jitter, number of lost packets, and other metrics that impact QoE and foreshadow a degradation of LTE network performance. With complete visibility of the infrastructure, any single event can be correlated with its impact on other service components, allowing for better understanding of the end-to-end network.



SevOne provides a real-time view all critical LTE metrics from a single dashboard

SevOne's xStats™ adapters provide the fastest, most flexible way to collect metrics from multiple data sources – including network probes, proprietary business applications, and element management systems from network equipment vendors that provide management functions for LTE, IMS, and Ethernet backhaul components – and present them in side-by-side dashboards, even when SNMP is not available.

SevOne automatically baselines these statistics, allowing alerts to be triggered based on deviations from "normal" performance. This eliminates false positive alerts, allowing for prioritization of service-impacting events and reducing the amount of time to troubleshoot. In addition, SevOne maintains this data in its raw, non-aggregated form for a year, allowing for historical analysis and improved capacity planning.

To see SevOne live, sign up for a Demo at www.sevone.com/demo.