www.pipelinepub.com
Volume 18, Issue 4

Unified Service Assurance in the 5G Era

By: Sergio Pessoa

5G technology is expected to enable significant new revenue opportunities from mission-critical applications like smart cities, autonomous vehicles, industrial automation, and smart healthcare, among others.

To enable these new services, 5G is being built on an entirely new architecture. The 3rd Generation Partnership Project (3GPP) has provided 5G network architecture specifications that are much more service-oriented than previous generations—and go well beyond offering voice, video, and web browsing to network users. At its foundation are the concepts of virtualization, disaggregation, geographical distribution of functions, and open APIs supported by many vendors.

The architecture enables service customization through network slices. Network slicing leverages network function virtualization (NFV) and software-defined network (SDN) capabilities to allow operators to partition the network on demand, creating end-to-end virtual networks that can be used for different types of services.

These dynamic services will come and go, demanding and releasing resources based on real-time needs. Operations and the network must not only react in real-time but also take a customer-facing view to meet service quality expectations and service level agreements (SLAs).

To deliver these services on 5G, fundamental changes must be made to service assurance solutions. Entirely different approaches are required—not just upgrades.

Legacy service assurance for an older era

Historically, network operations center (NOC) teams have focused on managing infrastructure rather than the services that run on the networks.NOCs process a very high number of events daily, usually leveraging siloed, domain-specific fault, performance, topology, and service management tools.

To identify and resolve problems, NOC experts use “swivel chair” management, manually plowing through reams of data to identify a problem’s root cause. They swivel between element management system screens, inventory system screens, and customer databases, all with different user interfaces.

Problem identification, isolation, and resolution may take hours, if not days, causing SLA violations or widespread network outages in the interim. And the manual effort is not effective, scalable, or economical.

Legacy applications are built on old architectures that are not dynamic. They cannot scale to meet the demands of today’s networks, and to overcome this, they filter out and discard data. But trends and anomalies can’t be spotted when part of the information has been deleted, leaving an incomplete view of the data.

The solutions lack flexibility for enhancements, and integration with other systems usually requires long and costly professional services.

Traditional service assurance and operations methodologies are not feasible in a 5G world.

Why 5G is a whole new ballgame

Service assurance is so heavily impacted by 5G because of the new services it enables, as well as its technical innovations.

Operator revenue opportunities that feature high bandwidth, low latency, and real-time service creation have been the stimulus for 5G’s innovative architecture. Customer expectations are high and degraded service quality is not tolerated. Because of this, network and customer quality of service (QoS) KPIs must be actively monitored in real-time to ensure that contracted SLAs are met. Problem identification and resolution can’t wait to be triggered by customer complaints but must be addressed proactively to maintain customer loyalty. Downtime is not an option.

The 5G network is effectively a new network. Its infrastructure is becoming virtualized and cloud-native, essentially integrating the telecom and IT worlds. There is not only a new distributed and disaggregated radio access network (RAN) with distinct control and user (data) planes that can be separated geographically, but the 5G core has also been completely reinvented.

To provide the agility needed to support innovative and differentiated offers, the core network is migrating from proprietary physical network elements to hybrid networks with virtual network functions (VNFs) to cloud-native functions (CNFs), containers, and microservices. The end goal is to virtualize everything, including creating virtual versions of physical devices.

Standards plus open architectures and APIs mean that the market is accessible to a wide variety of vendors instead of a few major players, so interoperability challenges will rise to a new level.

5G opens the door to many new capabilities and revenue streams, but the complexity of its networks and operations are raising the industry bar for ensuring reliability, performance, and security.

Of course, for the foreseeable future there will be both 4G and 5G networks, as well as older vintages. That means a hybrid mix of physical, logical, and virtual entities need to be managed and assured, across physical and cloud network domains, from edge to RAN to core.

How service assurance must change

Traditional service assurance approaches must be completely rethought to enable the business opportunities created by 5G technologies.

Fundamental changes are needed to marry the customer-facing business with network-facing operations to identify proactively how network issues impact the service and the customer. Operators must predict, prevent, and act quickly to remediate service-impacting issues that cause downtime or performance degradation—which ultimately impact the customer experience.

5G assurance must be unified and holistic. The ability to ingest data from multiple domains—ignoring nothing—and to normalize the data into a common format can bring visibility to areas that may previously have been lost because of disconnected siloes. Unification and normalization of the different data sources enable the data to be processed holistically based on a single source of truth. This is critical for achieving greatest insights. Machine learning (ML) can be applied for advanced correlation, root cause analysis, and automation across domains—in real-time and at scale.

With 5G, service assurance needs to provide end-to-end visibility across physical, logical, and virtual network entities, across all network domains and vendors. There must also be vertical visibility from the network infrastructure all the way up the stack layers to the services. Both perspectives must be analyzed together automatically to provide accurate insights into network issues and their correlation to services and customers.

The 5G assurance scope goes well beyond 4G and includes traditional physical networks, virtual RAN nodes, transport network interfaces, containers-as-a-service, controllers, network functions such as AMFs and CNFs, resource management VIMs, Kubernetes clusters, and many more.

Topology views must be updated in real-time—becoming a real-time inventory. This live view of the end-to-end and top-down network must be presented on a single pane of glass. The views should be enabled by multiple data overlays and visualized as a map, a hierarchy, or similar, with drilldowns as desired. Issues should be prioritized based on customer impact and indicated in the topology views.

This task is made even more complicated with 5G because of the large number of vendors involved, each with their own agile schedules for frequent solution updates that are driven by continuous integration/continuous delivery (CI/CD) software processes. The network and operations are continually changing in 5G.

As well, 5G brings an exponential increase in the number of devices and the way they are connected within increasingly complex environments. Operators know that these changes are only going to accelerate and become harder to manage.

The need for proactive, real-time service assurance that is driven by actionable insights and event "noise-reduction-through-correlation" requires automation of fault identification, performance monitoring, and root cause analysis. Closed-loop automated assurance is ultimately what will make it all work at scale.

Once an issue's root cause has been determined, automated workflows should be triggered for quick remediation. Open APIs are essential to enable seamless integration with orchestrators to close the loop by taking remediation action in the network—for example, remediations like increasing container capacity or off-loading traffic from a failing element.

A 5G service assurance solution should provide insights that can drive smart fulfillment, self-scaling, and self-healing actions. Such end-to-end closed-loop assurance will eventually lead to zero-touch and self-service operations that enable scalability and reduce error, time and effort, and operational costs.

Zero-touch can only happen through extensive use of automation, sophisticated analytics and contextual decision-making driven by AIOps, unsupervised machine learning, supervised event correlation, and topological root cause analysis. These are the essential capabilities of 5G service assurance.

A hyperscale architecture enabled by microservices is critical to address 5G's assurance challenges. By replacing operating system virtual machines with containers, microservice applications can support extremely high levels of scale with far less dedicated hardware. And microservice components and integrations can be developed and deployed quickly.

Machine learning and microservices capabilities are designed to handle and automate 5G and IoT's explosion of data and real-time response time requirements, both of which surpass human processing ability.

These are just some of the fundamental impacts of 5G on operations and service assurance. It all comes down to proactive and automated assurance in real-time that focuses on actionable insights to enable contextual decision-making at speed and at scale.

Moving forward with 5G service assurance

Operators are becoming increasingly dependent on their networks to provide services anytime, anywhere. They want to capitalize on the business opportunities created by cloud, 5G, SDN and NFV, IoT, and artificial intelligence (AI) and ML technologies to deliver new services—but they have been challenged by the increased complexity of integrating these new technologies into their existing networks, as well as by higher customer expectations.

To address these challenges while modernizing and future-proofing the business, operators are moving toward assurance solutions that provide data-driven actionable insights and automate the way the network identifies and resolves service-impacting incidents in real-time.

Operators can move forward by deploying a unified 5G assurance solution that can act as a manager of managers to consolidate NOCs as well as legacy tools that can't meet the business needs and scale of today's networks. This solution should be built on a scalable platform that provides the capabilities highlighted above.

The 5G assurance solution can be deployed in a phased approach, acting in a way that is comparable to a city planning strategy, where valuable legacy assets can be preserved while new assets are being added, but all coherently linked based on an overall plan and architecture—and with lower overall impact and risk.

This approach can also bring benefits to operators at every step as it migrates from 4G LTE to 4G LTE with 5G RAN, and then to 5G standalone.

Service assurance provides critical capabilities for 5G

A next-generation unified and holistic service assurance platform that puts service quality—what the customer wants—first is essential for 5G. It should support 5G's need for real-time operations and scalability, while at the same time enabling new revenues and providing cost efficiencies.

5G services must be monitored and managed to perform well all the time, no matter the complexity of the environment. If failures occur, services must be brought back to an operational state with speed and accuracy through closed loop automation, thus reducing downtime.

Critical capabilities include a hyperscale architecture for scalability and AI and ML to automatically manage 5G's wealth of data in real time and to provide closed-loop assurance automation.

Such a next-generation service assurance solution is essential for the 5G era.