www.pipelinepub.com
Volume 19, Issue 1

Reimagining How We Monitor and Assure Network Services

By: Charles Thompson

The telecom industry is buzzing with anticipation for the amazing new services that 5G Standalone (5G SA) networks will enable: mass-scale industrial automation, remote surgery, ubiquitous augmented reality experiences, and much more. But before communication service providers (CSPs) start tallying up revenue projections for new 5G offerings, they'll need to nail down a few small details. Things like verifying that their networks are actually delivering the low latency and reliability that these services demand. Or that they're actually complying with the service-level agreements (SLAs) on which new revenue models depend.

It sounds straightforward, but for CSPs adopting 5G SA architectures, fundamental tasks—like monitoring, troubleshooting, change management, and more—are proving much harder than anticipated. More and more, the industry is discovering that getting where we want to go with 5G will require top-to-bottom rethinking of the way we monitor and assure network services.

Bumping up against limitations of legacy tools

Previous mobile evolutions—from 2G to 3G, 3G to 4G—brought faster speeds and higher-quality services, but the underlying network technology remained basically the same. The transition to 5G SA, however, represents a fundamental break from the past. No more does "telecom infrastructure" imply a set of chassis, line cards, physical radio units, and other (mostly hardware)

appliances, typically from one or two vendors. In a 5G SA world, network functions are composed of thousands of Kubernetes-orchestrated microservices, often from multiple vendors, implemented as a dynamic service mesh.

It's a radically different network—one that's always on, changing constantly as containers spin up and down and vendor software gets continually updated. Yet somehow, CSP operations teams still need to manage, monitor, and troubleshoot 5G services, often under more stringent SLAs. There's no way to do that using assurance tools designed for yesterday's networks. Existing assurance approaches can't meet some of the challenges, including:

Scale with 5G networks

Traditionally, assurance has involved collecting and analyzing network data via fixed infrastructures of passive probes. This type of monitoring can still play a role in 5G environments, but it's no longer sufficient. There is no way to keep up with dynamic microservices-based architectures, where service paths can change minute to minute, using static monitoring that assumes data always traverses the same links.

Provide proactive visibility

Existing passive monitoring tools collect real user data as it traverses the wire. By definition then, any problem they identify has already affected customers—and potentially, already violated an SLA. If CSPs want to offer more stringent (and profitable) SLAs by guaranteeing ultra-low latency, nonstop connectivity, or other attributes, they need real-time, end-to-end visibility to spot emerging issues *before* they become critical. They also need to be able to map out how network changes will affect live services, even as the scope of network functions and performance requirements to measure grows.

Synthesize network- and service-level visibility

CSPs have long employed network- and service-level monitoring, but in the past, these tools existed in largely separate worlds. That won't work if CSPs want to maintain stringent network performance requirements to meet SLA targets. Monitoring at the level of individual devices and network layers is still important for segmenting issues, but CSPs need to more quickly connect the dots between underlying problems and application-layer degradations. At the same time, operations teams need to be able to spot signs of unresolved problems in the underlying infrastructure—even if they present as sporadic, seemingly minor issues that modern self-healing networks can quickly adapt around.

Taking a more active approach

To address these blind spots, CSPs around the globe are adopting active assurance to complement passive monitoring. With active assurance, they can proactively test end-to-end networks and services by injecting synthetic traffic into the network. It's like placing a CSP-controlled end-user device anywhere in the network to act as a probe.

By emulating real users—including mimicking the full set of user behaviors, even under load, from anywhere users might access a service—CSPs can proactively identify issues. They can maintain real-time visibility into both the network- and service-level experience to validate and police SLAs. And they can run active testing continually—prior to activating new services, automatically when something in the environment changes, or on demand to troubleshoot an issue. With active assurance, CSPs can:

Keep up with dynamic 5G networks

Unlike passive monitoring, active assurance can react to continually changing infrastructure. It uses the same authentication, runs the same applications, and traverses the same network paths as real subscriber traffic, allowing CSPs to measure services exactly as users experience them. That's a huge benefit, as CSPs don't have to rearchitect their visibility strategy every time the infrastructure changes, as they would relying on passive probes.

Gain continuous visibility

As paths change, as the network dynamically updates, active assurance can proactively test 24/7/365. Operations teams don't have to wait until real users are impacted to find out about a degradation or an outage. In many instances, they can identify, isolate, troubleshoot, and resolve problems before subscribers even notice them.

Accelerate root cause analysis

Assurance platforms can now use artificial intelligence and machine learning (AI/ML) to accelerate issue identification. In 5G SA networks, these capabilities become absolutely essential. With ML-based active assurance intelligence, CSPs can follow the end-to-end service path in complex 5G networks and sub-segment service components to quickly diagnose issues. This is especially useful for troubleshooting sporadic issues and ensuring that seemingly minor problems don't turn into large-scale outages.

Proactively "stress-test" networks

With the ability to emulate user behavior and generate synthetic traffic anywhere in the network, CSPs can continually and proactively test all links. They can measure from multiple points in the network—for example, one agent simulating an end device connected over the Radio Access Network (RAN) and backhaul, another testing through the mobile core. And they can quickly detect emerging issues, often before they impact real users and SLAs.

Bring lab validation testing to the live network

CSPs have long relied on lab tools to precertify new infrastructure, providing a "birth certificate" to verify that a component is ready for live traffic. With active assurance, they can bring this same testing to the live network, recertifying infrastructure for any new service or network change. They can even integrate active testing into continuousintegration/continuous delivery (CI/CD) frameworks, and automatically add active testing profiles for every new service as part of the service catalog.

Test against standby

Using active testing across both primary and standby network paths, operations teams can perform A/B-type testing of planned changes and analyze their effects. Operations teams (and automated network orchestrators) can also use this capability to respond to real-time degradations and outages. They can immediately see if a problem affects just the primary or the standby as well, and quickly determine when to migrate services to the standby system.

Building a virtuous circle

By embracing active assurance, CSPs can implement monitoring that is much better suited to always-on, dynamic 5G SA networks. But active assurance can also play a central role in network lifecycle management for a 5G world. Consider the following example of a CSP deploying a new network slice:

Service activation

The CSP needs to turn up a new ultra-low-latency network slice for a customer and wants to create a birth certificate—a final check before connecting the new service path to live customer traffic. The operations team uses assurance tools to perform an activation test, injecting synthetic traffic into the path to test latency, throughput, and other attributes before activating the slice. (Note that if the CSP has integrated activation testing into the Method of Procedures for new services, this testing happens automatically.)

Proactive monitoring

Next, the CSP Network Operations Center (NOC) continually monitors the state of the network for deviations in behavior—ideally, before they evolve into more significant problems. It's a task that's tailor-made for ML-based statistical analysis, and the active assurance platform uses this intelligence to monitor across multiple domains to identify emergent issues. More than just monitoring, however, the NOC also uses ML-based assurance tools to continually learn about services and identify the right KPIs to configure for a given SLA.

Root cause analysis

When assurance systems detect an anomaly, they immediately trigger active testing workflows to analyze it. Because active testing follows the end-to-end path of the service, the NOC can quickly identify the network domain where the issue originates, all the way down to the specific network function or interface causing the problem.

Continuous validation

After isolating a problem, the operations team applies the fix—and then returns to Step 1, activation testing, to revalidate that everything is working as it should. The process repeats in a continuous cycle.

Looking ahead

The buzz around 5G isn't hype. 5G SA networks can deliver amazing new capabilities, and transformative new service experiences really do become possible. But that doesn't mean CSPs are ready to deliver them. As an industry, we need to make sure we've mastered the basics of day-to-day operations in a 5G SA world. By bringing active testing out of the lab and into the NOC, we can build an assurance framework agile enough to keep up with highly complex, dynamic 5G networks. And we can finally start making the vision of new 5G service experiences reality.