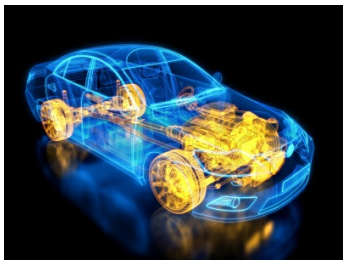
Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 7, Issue 15

2019: The Year 5G Gets Real

By: Heather Broughton



It seems the hype surrounding 5G has been with us for a few years now, but 2019 figures to be the year when actual deployments begin and things “get real.” This article takes a look at four critical areas of the new network environment that will come with 5G networks and how things may develop as the year goes along.

5G will drive virtualization in 2019

Momentum is building behind 5G. The US and South Korea are leading the charge with the rollout of the first commercial networks; trials are taking place in every major market worldwide; and Verizon and Samsung have just announced plans to launch a 5G handset in early 2019. Expectations for 5G are high: the next-generation mobile standard will underpin mission-critical processes and innovations, including telemedicine, remote surgery and even driverless cars. However, vast sums of money will need to be spent on network infrastructure before any of this can be realized, and it’s the mobile and fixed carriers who will be expected to foot the bill. This complexity is compounded by the fact that many of the aforementioned 5G use cases have yet to be defined, so carriers are being asked to gamble on an uncertain future.

So, what will the 5G future look like and what will it take to get us there?

One thing is for certain amid uncertainty: 5G will drive network virtualization. In 2019, we will see an increasing number of carriers committing to deploying virtualized network infrastructure to support 5G applications and services. Without virtualization, it will be ‘virtually’ impossible to deliver 5G. This is because 5G requires virtualization both at the network core and, critically, at the network edge. Puns aside, the days of building networks to support a single use case—such as mobile voice and data or home broadband—are behind us. If 5G is to become a reality, then the networks of the future will need to be smart and automated, with the ability to switch between different functions to support a range of use cases. Hence the application of network slicing to provide network instances that are tuned to the particular attributes of a given (e.g. IoT) service.

Moving from the physical world to the virtual, however, is no mean feat. Carriers are now discovering that their already complex networks are becoming even more so, as they replicate

existing functions and create new ones in a virtualized environment. Wholesale migrations aren't possible either, so carriers are having to get to grips with managing their new virtual networks alongside earlier generations of mobile and fixed technologies. Despite these challenges, 5G will undoubtedly accelerate the virtualization process. Subsequently, no one will want to be left behind, and we will see greater competition emerge between carriers as they commit funds and resources to building out their virtualized network infrastructures.

To justify this spend and to tackle the challenges that lie ahead, carriers will require smart visibility into their constantly evolving network architectures. Virtual probes that produce smart data, supported by intelligent tools, offer much needed visibility into the performance of these new networks and the services they support. The invaluable knowledge they provide will be absolutely critical for carriers as they accelerate their use of virtualized infrastructure to successfully deploy 5G.

In 2019, as virtualized network architectures are rapidly adopted to support 5G, we expect to see containers emerge as the de-facto platform to run new applications and workloads.

The excitement around 5G is building as we hear more news about network deployments, trials and handsets. However, one 5G-related issue that hasn't yet been crystallized is what form 5G software and innovations will take, and how these new services and applications will be deployed into the network. Unlike 4G/LTE network infrastructure, the architectures that support 5G are virtualized and cloud-based, so the smart money is on application developers, mobile operators and equipment vendors using microservices—and, in particular, containers—to drive 5G evolution.

It makes sense to use containers to support 5G, as they will provide operators with a flexible and easier-to-use platform to build, test and deploy applications, one that is now also becoming more secure. This is vital for the development of 5G services at a time when the use cases for 5G are still being defined. Operators will need to be in a position to spin up services as and when needed to support different use cases; by using containers, it will be possible to serve customers quickly and efficiently.

Another key aspect is the need to deliver services and applications closer to the end user by utilizing mobile edge computing. This is integral to ensuring the low latency and high-bandwidth associated with 5G and will support use cases across a wide range of verticals including transportation, manufacturing and healthcare. However, flexible architectures will be required to support this type of infrastructure throughout hybrid cloud and virtualized environments. As operators move network infrastructure to the edge, the use of containers will become pivotal to supporting 5G applications.

The use of microservices and containers will increase during 2019 as operators ramp up their 5G propositions. Despite offering clear advantages, they will also add a new layer of complexity, and carriers will need to have clear visibility across their service delivery network if they are going to make a success of 5G.

Operators will 'scale or fail' to meet the 5G demand in 2019

5G will be faster, smarter and more efficient than 4G, but in order to meet demand and to support new architectures, networks will have to scale. While most of the scale in the core network will be cloud and software-based, there will still be a need for hardware and equipment at the network edge—and in a 5G environment there will be a lot more equipment. In fact, the number of cell sites will increase dramatically to support and propagate the higher-frequency bands that will transmit 5G data traffic over the air. This is when network management tools will come into their own. In 2019 we will see the deployment of automated networks driven by software and controlled by virtual machines and artificial intelligence.

Network automation and orchestration are by-products of virtualization and will add another layer of complexity. However, they are also integral to the rollout and sustainability of 5G networks,

particularly as network topologies will change to accommodate a combination of small cell and macro cell sites. Small cells in particular will form the bulk of the new RAN (radio area network), and they are expected to increase cellular networks threefold. If network engineers think they already have enough issues to deal with today in maintaining 4G/LTE networks, then they may be in for a shock as 5G networks are gradually rolled out. In fact, without having total visibility of these more complex and expansive networks, 5G in the RAN is going to become extremely difficult to manage.

If the number of cells were to double or triple, not only would network engineering teams need to have the full confidence in their network management tools to make sure the network is running optimally, but they would also be faced with one heck of a job troubleshooting hundreds, and potentially even thousands, of cells if an issue arose.

In 2019, carriers will be scrutinizing costs per cell site as they look to invest in new infrastructure. They will look to offset any costs by implementing intelligent and automated systems that can support 5G networks. However, carriers need assurances that these systems are providing them with the right information about the uptime and performance of their new networks. Having a window into this multi-layered and virtualized environment—and being able to extract smart data in near real-time—will be essential for the ongoing management of new 5G networks. Indeed, the only way to achieve the requisite level of automation will be to have complete visibility of these complex new architectures with real-time smart data that can inform policy engines in a closed feedback loop.

Carriers come to grips with 5G security

The benefits of 5G are clear: the new communications standard will offer carriers and their enterprise customers faster network speeds and performance, ultra-low latency and greater efficiencies. General discussion around carrier trials and deployments tends to focus on increased speeds and the new innovations that 5G will enable, but security rarely comes up. That's all about to change, with 5G security set to become a big issue for the industry and a major talking point in 2019.

To date, it appears that 5G security has almost been treated as an afterthought rather than as a critical aspect of network development. Behind the scenes, however, 5G security is an issue that the carriers take very seriously. The situation for carriers has altered dramatically because, in a 5G domain, the attack surface becomes much greater. Consequently, the number of opportunities for malicious players to exploit vulnerabilities increases.

This is partly due to the adoption of virtualized network infrastructures that will allow carriers to scale and meet the demands of 5G, but also because 5G networks will be configured to support a wide variety of industrial and business use cases. This means that, going forward, carriers will be responsible for managing mission-critical systems and devices, in addition to handling high volumes of sensitive data. In a 5G environment, there will be a strong emphasis on securing smart factories, automated production lines and fleets of driverless cars. The network security stakes have suddenly got a lot higher.

As new 5G network architectures are based on virtualization and distributed cloud models and a containerized environment to support workloads and applications, it's apparent that carriers have to deal with a whole new set of complexities. Existing security protocols will need to be scrapped and replaced with robust systems and procedures that account for this newly complex environment and the burgeoning 5G value chain. That chain includes application developers, device manufacturers, cloud service providers and the carriers themselves. A new built-in resilience is required to limit the attack landscape and to reduce the risk of malicious attacks and perimeter breaches.

A pervasive security model that offers comprehensive insight on both service performance management and security offers the best solution to address 5G security. It enables service providers to extract 'smart data' that is collected and processed at the source from legacy, virtual and hybrid cloud environments. It's the closest carriers and their customers will ever get to implementing 'holistic security' across their entire IT estate.

Delivering a Future Smarter Network with 5G

As illustrated by these four examples, 5G will differ quite a bit from 4G LTE. Unlike previous generations of mobile network technologies, 5G is an overlay to 4G, and not a rip-out-and-replace scenario. The need for visibility into this 4G/5G interworking and new virtual infrastructures and automation is clear. For service providers that are rolling out 5G and planning to realize all of the promised benefits, having fast and accurate smart data tools can deliver critical visibility into the performance characteristics and security of any given service is essential to success.