Mobile Networks QoE

White paper
Commissioned by:

{Core Analysis}
Patrick Lopez
Mobile Networks QoE

Contents

About this report ............................................................................................................................................ 2

New consumer behaviours force changes .................................................................................................. 3

New Networks ............................................................................................................................................. 5

  1. Network Slices ........................................................................................................................................ 5
  2. Complexity increases .............................................................................................................................. 6
  3. Security, visibility, topology management key concerns .................................................................... 8

How do other service providers solve these problems? ........................................................................... 9

  1. Google ................................................................................................................................................ 9
  2. Netflix ................................................................................................................................................ 11

Instrumentation layer as a key success factor for next generations networks ........................................... 13

Accedian’s Virtualized Instrumentation ...................................................................................................... 14

About Accedian .......................................................................................................................................... 15

About {Core Analysis} ................................................................................................................................. 15

About this report

This report has been prepared by {Core Analysis} for public distribution. All rights of distribution and license of this report as well as the content and intellectual property herein are reserved by {Core Analysis}. This report can be distributed freely but its content cannot be reproduced neither partially nor completely without attribution to {Core Analysis}. 
2016 is an interesting year in mobile networks. Maybe for the first time, we are seeing tangible signs of evolution from digital services to mobile-first. As it was the case for the transition from traditional services to digital, this evolution causes disruptions and new behaviour patterns in the ecosystem, from users to networks, to service providers.

Take for example social networks. 47% of Facebook users access the service exclusively through mobile and generate 78% of the company’s ad revenue. In video streaming services, YouTube sees 50% of its views on mobile devices and 49% Netflix’ 18 to 34 years old demographics watch it on mobile.

This extraordinary change in behaviour causes unabated traffic growth on mobile networks as well as changes in the traffic mix. Video becomes the dominant use that pervades every other aspect of the network. Indeed, all involved in the mobile value chain have identified video services as the most promising revenue opportunity for next generation networks. Video services are rapidly becoming the new gold rush.

Video is essentially a very different animal from voice or even other data services. While voice, messaging and data traffic can essentially be predicted fairly accurately as a function of number and density of subscribers, time of day and busy hour patterns, video follows a less predictable growth. There is a wide disparity in consumption from one user to the other, and this is not only due to their viewing habits. It is also function of their device screen size and resolution, the network that they are using and the video services they access. The same video, viewed on a social sharing site on a small screen or on full HD or at 4K on a large screen can have a 10-20x impact on the network, for essentially the same service.

“Video services are the new gold rush”
Mobile Networks QoE

Video requires specialized equipment to manage and guarantee its quality in the network, otherwise, when congestion occurs, there is a risk that it consumes resources effectively denying voice, browsing, email and other services fair (and necessary) access to the network.

This unpredictable traffic growth results in exponential costs for networks to serve the demand.

As mobile becomes the preferred medium to consume digital content and services, Mobile Network Operators (MNOs), whose revenue was traditionally derived from selling “transport,” see their share squeezed as subscribers increasingly value content and have more and more options in accessing it. The double effect of the MNOs’ decreasing margins and increasing costs forces them to rethink their network architecture.

New services, on the horizon such as Voice and Video over LTE (VoLTE & ViLTE), augmented and virtual reality, wearable and IoT, automotive and M2M will not be achievable technologically or economically with the current networks.

Any architecture shift must not simply increase capacity; it must also improve the user experience. It must give the MNO granular control over how services are created, delivered, monitored, and optimized. It must make best use of capacity in each situation, to put the network at the service of the subscriber. It must make QoE — the single biggest differentiator within their control — the foundation for network control, revenue growth and subscriber loyalty.

By offering exceptional user experience, MNOs can become the access provider of choice, part of their users continuously connected lives as their trusted curator of apps, real-time communications, and video.

As a result, the mobile industry has embarked on a journey to design tomorrow’s networks, borrowing heavily from the changes that have revolutionized enterprise IT departments with SDN (Software Defined Networking) and innovating with 5G and NFV (Networks Functions Virtualization) for instance. The target is to emulate some of the essential attributes of innovative service providers such as Facebook, Google and Netflix who have had to innovate and solve some of the very same problems.

“How to build massively scalable networks while guaranteeing Quality of Experience?”

QoE is rapidly becoming the major battlefield upon which network operators and content providers will differentiate and win consumers’ trust. Quality of Experience requires a richly instrumented network, with feedback telemetry woven through its fabric to anticipate, detect, measure any potential failure.
New Networks

1. Network Slices

Until recently, mobile networks were centered around voice services (calls, voice mails), then came messaging (texts, picture messages, IM) then data services (browsing, email, streaming...). Essentially, in the past, MNOs built specialized networks for each service:

- circuit switched for voice and transactional data (USSD, SMS)
- Packet switched for multimedia (MMS, wap),
- IP for streaming, VoLTE...

This strategy is not sustainable from a cost perspective, and we have, with 3G started to transition all services to an IP network architecture. Future networks must be designed to accommodate a lot of different services with different constraints (speed, latency, bandwidth, upstream, downstream, transactional, streams...).

This is one of the founding assumption of SDN and NFV. But running different services with different needs on the same set of homogenized resources require higher and finer grained control mechanisms.

Whereas in the past, control was embedded in the data/service flow, SDN and NFV allow to separate data from control, providing a single point of management of all network attributes.
Mobile Networks QoE

As hardware is separated from (virtualized) functions, control can now be centralized. Current plans show that networks will evolve towards network slices which will be used to allocate sets of resources that are specific for each use cases. Network slices will essentially be specialized virtual networks that will draw from the common resource pool to deliver specific services with unique attributes.

As next generation networks start to emerge, some key technologies are being investigated. A key tenet of these new architectures is the transition from specialized to generic Commercial Off The Shelf (COTS) hardware. This migration reduces substantially the cost of acquisition, deployment and maintenance of the physical network infrastructure. The apportioning of the network resources is now essentially managed by a software layer, that acts as a network operating system. Software Defined Networking (SDN) allows the abstraction of basic network capabilities (such as networking, storage, computing...) and provides a single point of management for these resources, irrespective of the number of processors, servers, data centers or clouds.

As COTS are increasingly deployed, traditional network elements and functions are transitioning to pure software and are being virtualized. This trend, known as Network Functions Virtualization (NFV), leads also to new network topologies, where control of network functions and their access to physical resources is being abstracted and centralized. In parallel, the integration of these new networks with traditional OSS / BSS functions is embryonic with many questions still unanswered as to how to create a service from the order taking, to its fulfilment, delivery and subscriber integration in this new paradigm. All these layers do not necessarily have a coherent integration model to link how a “service” uses functions that necessitate virtual resource assignment and physical resource corresponding budget allocation.

2. Complexity increases

The separation of the control from the data plane, common in SDN and NFV has great benefits, allowing to essentially invoke services from network functions without manually configuring each physical network element. As functions become virtualized their instances are no longer linked to physical constraints, which enables some key attributes:

- Flexibility (functions can be moved from one part of the network to another).
- Elasticity (functions can be invoked or killed on demand based on traffic increase).
Automation (functions can automatically be invoked, positioned chained without human intervention beyond initial conditions programming).

On the other hand, flexibility and elasticity will not effectively be achieved without automation, which requires meaningful control. At this point in time, there are still multiple control layers that are poorly integrated between SDN and NFV, with too little in term of visibility and integrated mapping of physical and virtualized functions.

The virtualization of key network elements such as the Evolved Packet Core (EPC) and the Radio Access Network (RAN) provide an exciting opportunity for MNOs but also a great series of challenges as network functions become simultaneously more layered and more distributed (physically in the core and the RAN and logically in network slices). Each of these slices, each of the functions, each of the services today have separate control layers. This fabric, woven from vertical service logic and horizontal infrastructure control multiplies control layers for each aspect of a service, from its physical location (which region, cloud, data center, cabinet, rack, server, processor…) to its configuration (scaling thresholds…) to its allocation (slice, subscriber, service chain…).

This level of complexity can only be manageable in an automated environment with an equally automated fabric of sensors that observe, detect, map, measure infrastructure, functions and services in real time.
3. **Security, visibility, topology management key concerns**

Virtualized functions, when automated provide great performance elasticity benefits. A challenge associated with automated scale out / scale in is that virtual machines being spun out dynamically can be difficult to track. Mapping static physical topology to virtual, dynamic resource anchors can become quite problematic. It is necessary to have correlated physical and virtual sensors that can provide as close to real time a faithful representation of the network and its usage by service and function.

Another corollary of the multiplication of virtualized elements and layers is the increase in possible points of vulnerability.

In past networks, security was enforced by tightly integrated proprietary systems that offered little or no access to external entities without physical manual intervention — they were centralized, and they saw everything from the vantage point of the EPC. In virtualized and software-defined network, the automation and centralization of infrastructure, functions and services control is a double edged weapon, which can immensely facilitate deployments and reduce costs but also become an ideal point of vulnerability for possible attacks. As functions, traffic and control distribute, core visibility becomes inadequate to gain a complete picture of network state, behavior and user experience.

Even without ill-intent, networks are growing so fast in size and complexity, that it would be irresponsible to deploy fully automated virtualized functions without means of monitoring, measurement and control.
How do other service providers solve these problems?

1. Google

Google is certainly a reference in innovative network designs. Early on, the company had decided that its services necessitated dedicated data centers with pretty unique attributes. The data center had to be able to provide massive multi-pathing, with plentiful, uniformly distributed bandwidth. As latency became as important as bandwidth, the teams started looking for means to shorten round-trip times and reduce buffering across data centers.

One conclusion was for Google to deploy uniform hardware throughout the data center, with specialization of purpose operated exclusively at the software level. Most of the technology necessary to achieve these objectives was to be invented, which led the company to design its own datacentres, from silicon to cabinet, from cabling to cooling systems.

As Google embarked on this journey, it designed and deployed 6 generations of data center fabrics to date and is still researching and innovating in this field. Between 2004 (Four Post) and 2012 (Jupiter generation datacenters), the company has increased traffic capacity per server by 50x and moved from 1G to 10G/40G host speed.

Today, Google manages 5 different fabric architectures with respectively over 10,000 nodes and a ¼ million links. Each fabric routinely features over 10 million rules and policies...

"A Google data center features over 10k nodes, 250k links and 10 million rules"

That level of scale and complexity represents some challenges that are familiar to anyone building networks, although at an extreme scale:

- How do you verify that your physical and virtual network corresponds to your plans?
- How do you assure that each link is consistently providing a high level of performance at the control and data level?
- How do you measure and represent traffic at the macro, micro and service level in an accurate manner?
Mobile Networks QoE

The company started defining a model for data center fabric service assurance and QoE. Google’s finding should guide many network operator seeking to build software defined, virtualized networks:

1. Design the data center with a telemetry instrument layer fed from every physical and virtual network element. The sensors should push / stream data to collectors.
2. Measure host and service level reachability across all host pairs and all traffic classes with varying SLAs.
3. Utilize a publish/subscribe API to select desired data so that collectors can selectively monitor certain slices or aspects of the service, infrastructure or functions.
4. Must implement a hierarchical, logically centralized control mechanism. This falls squarely into the integrated infrastructure, functions and services framework described before.

Although Google’s networks are probably amongst the most advanced commercial data networks, they are not without limit. Continuously monitoring 10k nodes and 250k links in real-time has proven problematic. To date, the company has opted to perform sample based audits, where host pairs and end-to-end services are tested in a round-robin fashion. When a fault is detected, it is triangulated through intersecting measurements and quarantined. Traffic and sessions are rerouted and the quarantines section is then passed on to a more active auditing level. The results of the investigation are feedback through the machine-learning layer responsible for (optimizing) network control.

The conclusions of Google are clear.

1. Next generation networks, to be highly scalable, elastic and provide homogeneous performance must be fully instrumented.
2. Telemetry must be part of the design phase and evolve together with the fabric.
3. The complexity, scale and speed of transactions and streams prevents human intervention for fault detection and route cause analysis. Those network instrumentation layers must rely on fully automated telemetry sensors permanently streaming data to collectors that must organize, map and represent finely grained network elements and rules, and abstract hierarchical alerts, thresholds and alarms.
2. Netflix

Another interesting example is the case of Netflix. The company has had to innovate tremendously because of its unique mission. Delivering digital video over the internet is an interesting challenge. This unique model has forced the company to continuously innovate and use some of the most advanced cloud and software defined technology to benefit from elasticity, agility and performance beyond legacy data centers technology. Netflix has its technology deployed in hybrid clouds, drawing performance and capacity from commercial offerings such as Amazon’s Elastic Transcoder where it creates hundreds of versions of each title in its catalogue to fit any screen and any network condition. Netflix also operates its own private cloud infrastructure, for the production, packaging and delivery of its video service.

In its private cloud, Netflix has implemented a number of testing and instrumentation initiatives to monitor and control its service. More interestingly, the company has created a framework to proactively attack its network from different angles—a Netflix-centric active monitoring and optimization method.

The operating assumption is that the delivery of digital services across a large number of networks and devices will always exhibit paths and host client combinations that will be less than optimal, and in some cases faulty. In other words, failure is to be expected. Networks are complex, and the tendency is to test only when a change occurs, with new elements, path, technology appliance, etc. The problem with that approach is that the testing results become mostly predicated on what one thinks will happen and circumscribed to only the new device, occurrence, element and its immediate surrounding. Netflix already had monitoring capabilities, as well as the ability to arbitrarily inject faults in specific paths for testing purposes. Relying on academic research from UC Berkeley’s Peter Alvaro and internal work, Netflix created a generalized fault injection framework. For this to work, Netflix had to map all possible interactions between all its systems resulting from a simple Netflix request (register, login, scroll content, play title...).

Rather than wait for a failure to be detected, analysed, worked around and fixed, the company is continuously inserting faults in its network and monitoring the effect of these faults on systems and services, so that when unscheduled faults occurs, they can be rapidly compared to the template of cause-effect that has been accumulated by the machine learning instrumentation layer.
Mobile Networks QoE

More importantly, the company was able to define and quantify more precisely what criteria enter into the definition of success or failure of a Netflix request. Specifically, the company’s number one criterion is members’ QoE. All failures are then graded based on their impact on QoE. That framework became the directing template not only for analysing faults, but also for the testing strategy. Impacting QoE significantly for a large number of members is unacceptable, so proactive, non-intrusive testing is necessary to detect, explore and circumvent potential failures. In many cases. Though, testing a live service on a live network will have an impact on QoE. Netflix has created a framework to measure and control the QoE impact of its tests on live service. To mitigate this impact, the company runs about 500 micro tests per day, designed to last 20 to 30 seconds and affecting less than 10 members each.

This framework has proven effective in not only detecting proactively potential faults, but also in delivering an automated fault triangulation apparatus. Netflix estimates that to test only the “app boot” request which launches the application, \(2^{100} \approx 10^{30}\) test iterations would have been necessary due to the complexity of the hundreds of internal processes involved. The micro testing delivered good failure exposition in only 200 experiments.

Netflix’ example provides valuable insight:

- Testing must rely on good knowledge of network topology and paths.
- Simple user actions must be traced throughout the network and its components to understand sequence of events.
- Quality of Experience impact can be the guiding criteria to judge failure severity
- Testing strategy should be proactive, with voluntary, directed fault insertion and impact analysis.
- Micro testing can be more effective and less time and resource consuming than brute force testing

“Netflix runs about 500 micro tests per day, designed to last 20 to 30s and affecting less than 10 members each"
Mobile Networks QoE

Instrumentation layer as a key success factor for next generations networks

In light of these examples from some of the most innovative service providers, it becomes obvious that networks must be designed and architected with instrumentation in mind from the get-go. SDN and NFV are at a stage where they have not yet been massively commercially deployed in mobile networks. It is the right time to think about creating a network that is aware of itself before deploying it.

Virtualization and control layer abstractions bring increased operational complexity that can’t be effectively dealt with without massive automation. Automation can be extremely efficient or destructive, depending on the level of control one can exert over it. As a result, it is crucial network operators embed smart sensor capabilities woven into the infrastructure, functions and service fabric. That “sensors mesh” ideally is vendor independent, able to correlate physical and virtual state to provide an accurate mapping of network topology, resiliency, performance and QoE.

Once deployed, that ever-changing sensor swarm does not only monitor and report, but is ideally continuously testing, validating end-to-end host-guest and service paths. Testing is not only reactive — for troubleshooting upon discovery of a failure or performance loss — but more importantly, proactive, inserting “golden” reference probe packets as well as micro failures as that have well-understood network, service and customer impacts. This serves as consistent input to detect any new issue rapidly, so it can be quarantined, analyzed, and compared to the growing, learned inventory of known failures and effects.

When Quality of Experience becomes the frame of reference for understanding, categorizing and treating network and service failure, a hierarchized tree of defects and resolutions starts to emerge, which in turn feedbacks to networks and service configuration and design.

This is not easy. There are many obstacles to overcome. Many service providers have not been able to find what they needed in commercially available solutions, so they had to design it themselves. Fortunately, markets evolve and MNOs can rely on few vendors to help them tackle this challenge... but if you are thinking about 5G, IoT, Video Services, SDN and NFV, it is time to roll up your sleeves. You cannot achieve service domination without overwhelming QoE... and that is not going to happen if you can't measure it and control it.
Mobile Networks QoE

Accedian’s Virtualized Instrumentation

In an app-centric era, user experience is key to communication service providers’ (CSPs) success. To deliver the user experience customers expect, operators must be able to analyze how well applications are performing, in addition to monitoring network quality of service (QoS)—they need visibility at all layers to effectively monitor, troubleshoot and optimize quality of experience (QoE).

Put another way, QoE assurance requires ‘illuminated troubleshooting,’ involving:

- All-layer visibility for rapid root cause isolation of issues affecting customers.
- A combination of active test injection and distributed, passive traffic “tapping”
- Multi-layer, multi-metric insight into the relationship between QoS and QoE.
- Focusing optimization efforts where subscribers will notice—and benefit.

Solutions to achieve this type of 20/20 vision with actionable insights must be cost and bandwidth efficient (measuring QoE shouldn’t impact it), and provide metrics from all layers, all locations, at all times and seasons. It also must be simple to deploy: almost immediate, or on-demand. It needs to be programmable, and open to control by analytics platforms, analyzers, SDN controllers and NFV orchestrators.

Virtualized instrumentation can address these requirements by applying the principles of SDN and NFV to the creation, collection and analysis of test, control and user traffic. Centralized performance assurance orchestration with virtualized controllers can be combined with distributed data plane modules, test agents and standards-based reflectors to provide localized test access that can fully cover the entire network and service topology.

Accedian’s SkyLIGHT Performance Platform embodies and exemplifies these principles, with active QoS test and monitoring capabilities that currently cover over 70% of global Tier-1 MNOs’ infrastructures, providing real-time network performance visibility from EPC to eNodeB.

Accedian recently introduced FlowBROKER™—the industry’s first NFV-powered, distributed packet broker solution—into the SkyLIGHT platform. FlowBROKER’s unique ability to efficiently tap the entire network, and bring any flow of interest to centralized and virtualized analyzers, security collectors, policy enforcement and DPI platforms extends SkyLIGHT’s monitoring capabilities to include all aspects of the user experience. It creates, for the first time, an integrated, standards-based, network and cloud scale QoS and QoE performance assurance platform.
Mobile Networks QoE

About Accedian

Accedian delivers exceptional end-to-end network performance visibility, for control over the best possible user experience.

Providing the most complete, current view of network health, Accedian dramatically improves visibility with actionable insights that providers use to reach peak reliability and significantly boost quality of service (QoS). Accedian enables control over increasingly complex, multi-vendor networks to increase agility and reduce cost—without constraint. With unrivalled performance assurance, providers extract the most from their network, and can fully embrace the migration to Software Defined Networking (SDN) and Network Functions Virtualization (NFV) with confidence.

By delivering a fully optimized and performance assured network, Accedian proactively ensures networks meet increasingly stringent performance requirements to deliver exceptional quality of experience (QoE) to every end-user. Since 2005, Accedian has delivered platforms assuring hundreds of thousands of networks and services globally, turning performance into a key competitive differentiator.

About {Core Analysis}

Patrick Lopez
Founder & CEO
{Core Analysis}
www.coreanalysis.ca
Blog (http://coreanalysis1.blogspot.com/)
Twitter: @coreanalysis

Patrick Lopez has nearly 20 years of international progressive experience in product and technology introduction in the United States, Canada, Switzerland, Ireland and France. Founder and CEO of {Core Analysis}, he provides advisory services to technology vendors, board of directors, carriers and venture capital firms on OTT video. As an analyst, he presents at influential industry forums and conferences and publish an acclaimed blog, industry articles and reports. In 2016, he is chairman / speaker at 5G World Summit, NFV World Congress, and SDN / NFV Summit .... Recent achievements:

- {Core Analysis} was exclusive advisor to Opera Software in its acquisition of Skyfire for $155 millions.
- Presented at NAB (National Association of Broadcasters) on PayTV vs OTT strategies and business models.
- Presented at United Nations’ ITU Telecom on convergence of broadband and broadcast.

Patrick has collaborated to various industry reports including Deutsche Bank, JP Morgan, Morgan Stanley Credit Suisse First Boston, IDC, Frost & Sullivan, Yankee group, Ovum, Informa... and has written several articles in collaboration with The Wall Street Journal, TMCNet, Wireless Week, RCR Wireless News, CNN and CNBC Europe.

Patrick holds a MBA in Corporate Management and Bachelor Degree in Marketing Strategy.

---

iGoogle Networking - Data Center Networks & Telemetry” Conference Carrier Networks Virtualization 2015
ii“Jupiter Rising: A Decade of Clos Topologies and Centralized Control in Google’s Datacenter Network,” SIGCOMM 2015
iii “Lineage-driven Fault Injection” – Peter Alavaro, Joshua Rosen, Joseph M Hellerstein – UC Berkeley
“Automated Failure Testing” – Kolton Andrus, Ben Schmaus - Netflix Blog