RADCOM

Cloud-native service assurance

The cornerstone of a successful NFV transformation

Table of Contents

Introduction

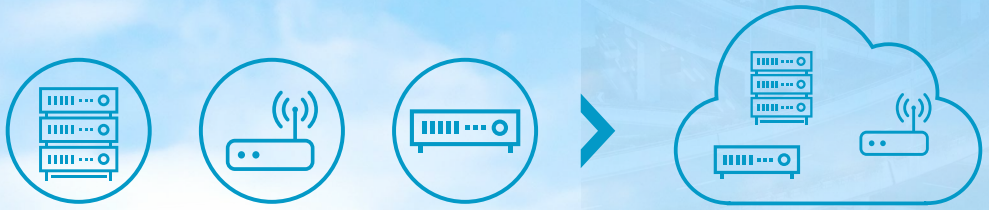
Communications service providers' (CSPs) profits, business efficiency and brand reputation all depend on the service quality and on the overall experience they provide their customers. So, it's critical for a CSP to have complete visibility into the network; always understanding what's happening, knowing how services are performing and being aware of real-life customer experiences.

To gain network visibility, CSPs deploy service assurance solutions that monitor the network traffic and provide actionable, contextual insights into network performance, and the customers' quality of experience. Service assurance solutions also provide the ability to proactively and reactively troubleshoot issues, allowing CSPs to constantly maintain top-level service quality and by that, keep customer experience levels up.

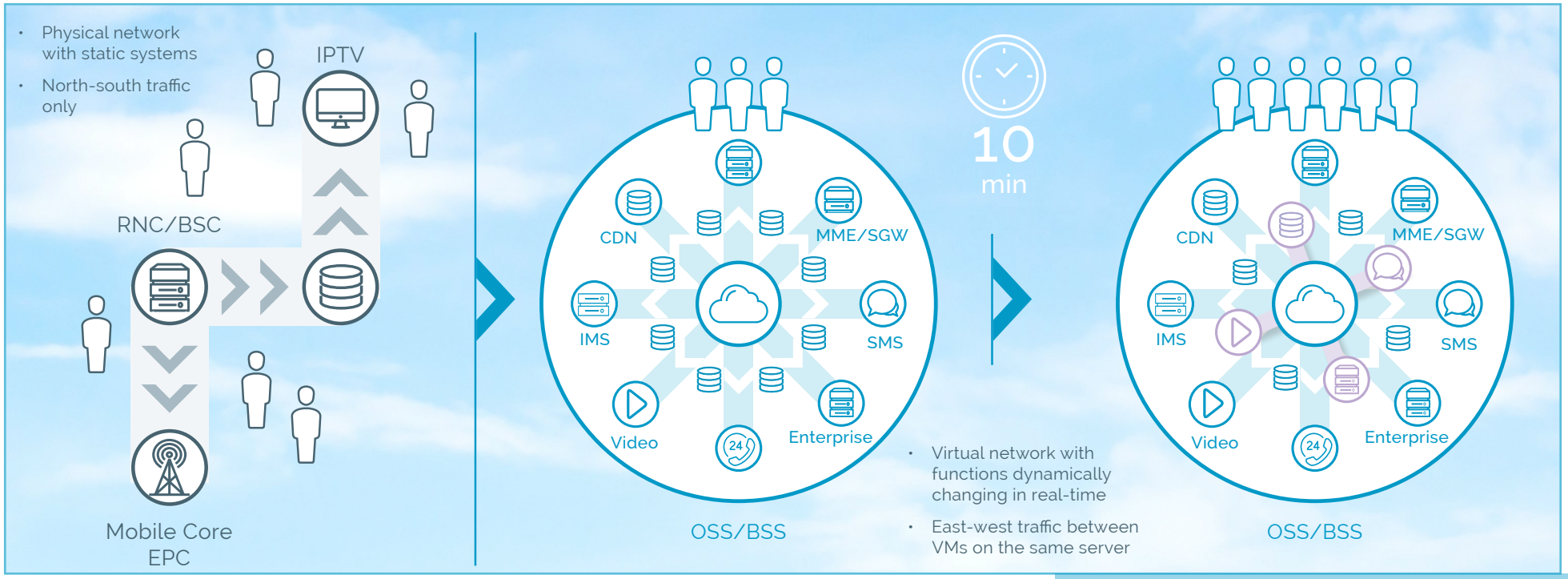
Traditionally, service assurance solutions - like the networks they are monitoring - are comprised of expensive, static, proprietary-owned hardware and deployed as add-ons to the network. Every time the network changes, for example, when capacity grows, engineers need to manually add additional hardware and reconfigure the service assurance solution.

Now, as the transition to NFV picks up pace, control of the network is being decoupled from proprietary hardware to software; with the goal of creating a more agile, cost-effective and automated network. However, the dynamic nature of such network topologies generates challenges for the CSP in managing the network, and a fragmented approach to service assurance through an "add-on" solution will not work, as legacy assurance will not be able to adapt in real-time to the agile, constantly changing network. To fully gain the benefits of NFV, service assurance needs to be fully virtualized and embedded as part of the virtual or hybrid network, to assure customer experience is not affected in the transition, and to assure that the new network infrastructure works as intended.

However, the transition to NFV will not take place overnight, so hybrid networks comprised of virtual network functions (VNFs) and physical network functions (PNFs) will need to be assured by service assurance solutions for many years to come. Yet, increasingly, CSPs are looking for assurance vendors



Virtualization brings more complexity



with expertise in virtualization, while also being able to provide cost-effective software-based solutions to handle their physical networks. By providing CSPs the same service assurance solution that can be deployed in a software only version on Commercial-off-the-Shelf (COTS) hardware, and then deployed in a virtual environment as a fully virtualized version assurance vendors can help CSPs make this transition as seamless as possible, while leveraging their assurance investments to the maximum.

While bringing many advantages, virtualization also brings complexity, and if the transition is not carefully executed it could lead to customer churn. If service assurance for a static, hardware based network was complicated, then imagine a network full of virtual elements installed as virtual machines on commercial-off-the-shelf hardware that can change on the fly from being one function (a router) to being another (a firewall). Multiple this by millions of instances and then consider that each hardware element can have multiple instances of a virtual function and each of those functions communicate with each other (East-west traffic) and can also change on the fly. All these modifications in the network services need to be monitored in real-time by the assurance solution.

In the past, service assurance was about monitoring whether the network was running. Today, the real-life customer experience is key and if a CSP wants to maintain competitiveness a transformational shift in a CSPs' approach to service assurance. With this transition to virtualization, both CSPs and vendors have a chance to reset their approach to service assurance and embed assurance to be part of the network to assure the delivery of dynamic, on-demand services that meet customers demand for quality, and streamline their operational efficiency. This can only happen with assurance solutions that are built as cloud native solutions.

The shift from carrier grade hardware to carrier grade virtual software is a must for CSPs to maintain competitiveness.

Cloudifying the network

With the industry shift to a software-centric network, CSPs are transforming the way they operate and manage their networks, by using standard IT hardware resources on a cloud platform. This move to virtualization has meant a mind and- skill set change as the CSP transitions from hardware expertise and working with vendor solutions, to the need for software and virtualization skills, for creating their cloud infrastructures.

The "IT-ification" of CSPs means that traditional IT functions are merging into network operations and engineering functions, silos are coming down and the network infrastructure and management are converging, no matter the service delivered.

By creating a single management interface to define, manage, provision and troubleshoot the network. CSPs are going through the same processes that cloud providers such as Google and Facebook went through a decade ago. Unlike cloud providers though, CSPs are an established market, with millions of active customers, and so their transition to the cloud needs to be transparent and deliver a carrier-grade service, right out of the box.

A sizeable number of CSPs are already transitioning to virtualized networks and creating their cloud-based platforms- essentially the "brains" of the network - utilizing a mix of NFV and SDN technologies. AT&T created ECOMP (Enhanced Control, Orchestration, Management & Policy). This initiative was committed to open source and merged with another cloud management platform - Open-O - to create ONAP (Open Network Automation Platform). Orange are evaluating the platform. Telefonica established their UNICA platform after they started by virtualizing their data center capacity in 2011, whereas Vodafone have their Ocean platform and Verizon are also

CSP goals for their cloud platforms are to:

- Reduce OPEX and CAPEX by transitioning to a software-controlled network
- Significantly decrease time from service concept to market, using dynamic and elastic scalable services
- Deliver a seamless customer experience by integrating service level policies into network management
- Create a single view of all network (physical and virtual) resources and services
- Automate service configuration & management

building their private cloud infrastructure. Recently, SK Telecom announced their NFV MANO platform named 'T-MANO.' All these cloud based platforms constitute the very fabric of the communication networks and are responsible for controlling, and delivering telecommunications services.

While creating these new platforms, CSPs are rethinking how a network should be managed and operated; focusing on providing a new level of customer experience, delivering business agility while lowering capital and operational costs, facilitating rapid service chaining and adding automation to network operations and management.

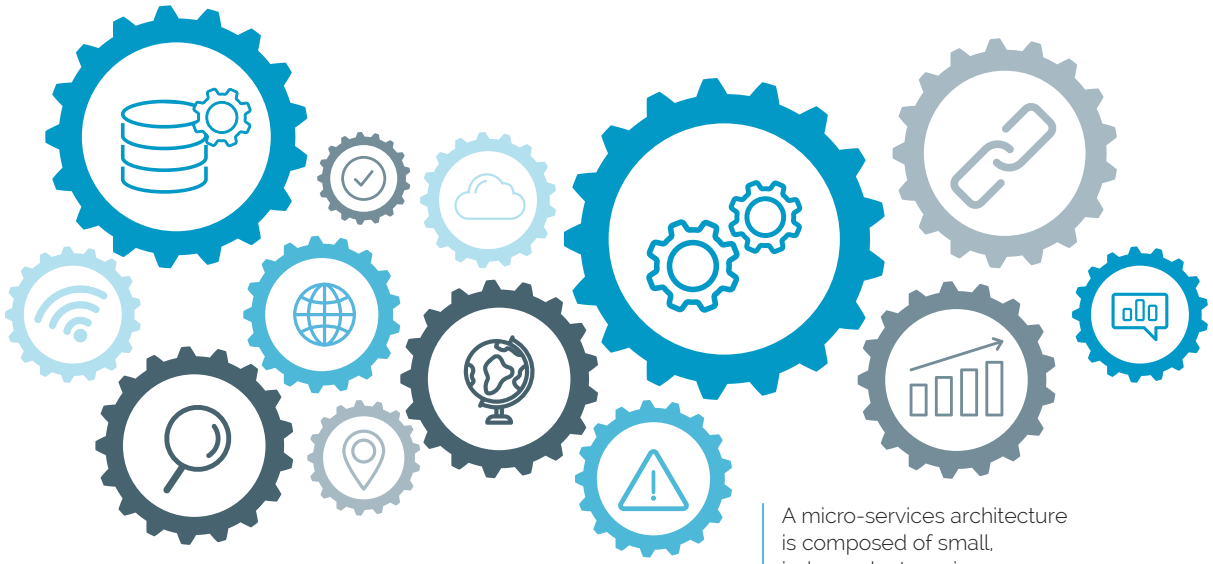
Cost savings, service agility, and centralized policies and management are delivered via the NFV environment that consists of bare-metal storage, network, and computing resources (comprised of commercial-off-the-shelf hardware) managed in a unified, and more automated way using virtualized functions and software control. In NFV terminology, NFV MANO (NFV Management and Orchestration) manages the network, while the orchestrator is responsible for assuring the provisioned services, as well as remediation and optimization tasks.

With the cloud-based orchestration platform being the brain of the network, it needs senses and a nervous system that is native to the body, communicates with the rest of the body, recognizes pain points, and then sends feedback to the brain so it can react to, and resolve issues. In these newly emerging networks, the sensory systems are the service assurance capabilities.

For a service assurance solution to provide the required functionality and value, being native to that environment is essential. That means CSPs need a cloud-native service assurance solution (something designed and built specifically for a cloud environment), not a legacy solution, copied and pasted into the new network environment as software.

Only by deploying a fully virtualized solution, built especially for the cloud, will CSPs be able to deliver a low-touch, cost-effective, end-to-end service assurance solution that delivers a closed loop solution, to automatically correct issues and adjust the network to maintain services and deliver a continuously high level of customer experience.

Cloudifying assurance



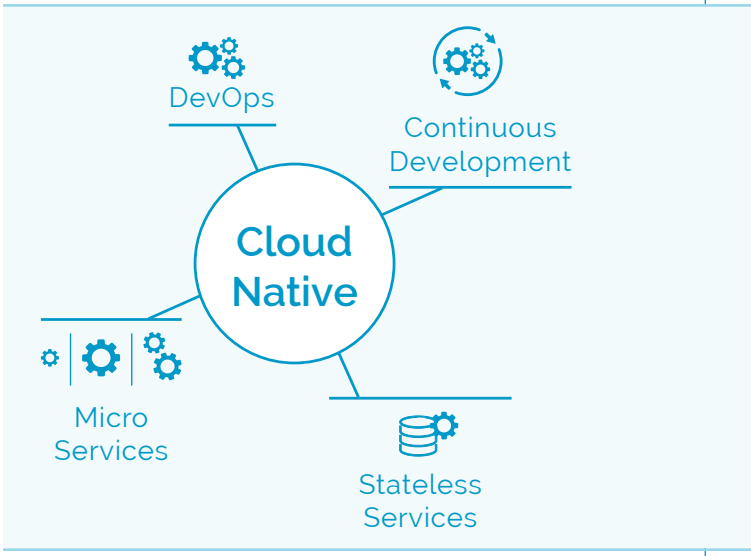
A micro-services architecture is composed of small, independent services

A mature cloud-native service assurance is built with a micro-services architecture composed of small, independent services that allow scaling, updating, or even complete replacement of each part. This architecture enables the embedding of the solution into the network for:

- Increased efficiency - real-time performance, using less hardware
- Reliability - failure resilience for continuous monitoring
- Elastic scalability - dynamic, automated in/out scalability

All of these features are critical in today's high capacity networks and even more essential as CSPs move closer to 5G and to increased IoT traffic.

Cloud-native assurance is easy to deploy, agile, and integrated into the network and built for dynamic NFV networks. With fault tolerance, seamless upgrades, stateless services (control state and data states are separate) so whatever the traffic load, service assurance is running 24*7*365. With elastic scalability that allows individual solution elements (probing, database, etc.) to horizontally and vertically scale independently, cloud-native assurance constantly adjusts itself to remain vigilant to monitor network performance and service quality.



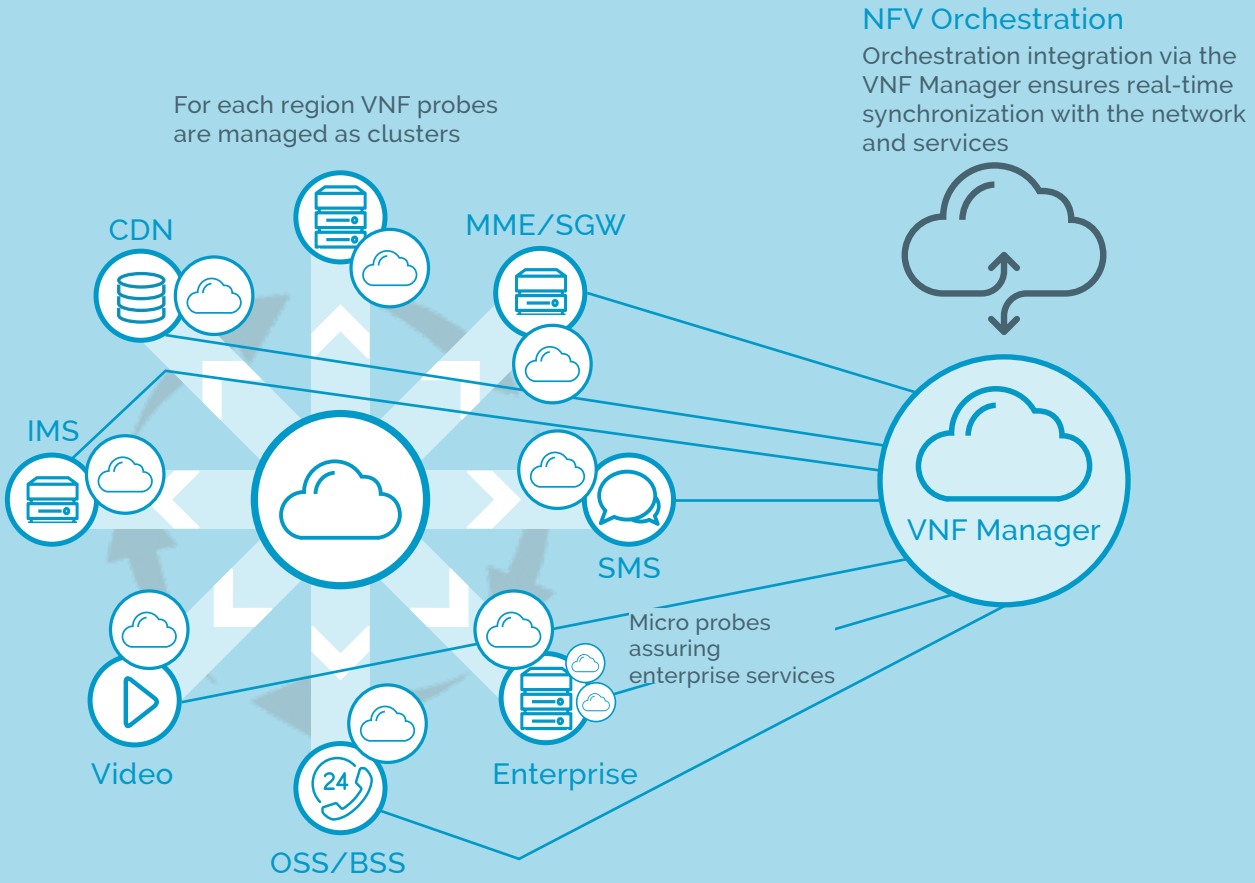
By cloudifying the service assurance solution, CSPs gain significant benefits:

Tight integration with NFV Orchestration

Cloud-native service assurance constantly syncs with the orchestration, to utilize hardware resources efficiently and keep up to date in real-time with what network services are running. This delivers a solution that resets what is possible for service assurance. It is highly cost-efficient and assures the seamless migration of a CSPs' customers to NFV, while helping assure a new level of customer experience. Moreover, KPIs shared with the network "brains" can now be available to other service VNFs to enrich the data available for additional service analytics applications.

In NFV networks, the service assurance solution acts as the sensory and nervous system of the network by synchronizing with the orchestrator, ensuring real-time service quality across the entire service delivery network; thus, evolving into one of the most advanced VNFs in the network. Through constant maturing with DevOps design and modeling for continuous integration and delivery (CI/CD) cloud-native solutions push forward their development; making changes quickly without compromising on quality.

Service Assurance
The most advanced VNF in the service delivery network



Rapid, agile development

Legacy service assurance hardware release cycles take months or years, but by virtualizing service-assurance, component upgrade cycles take minutes or days.

To keep up with changes in the NFV environment, service assurance vendors need to move to an agile and DevOps development so that as the virtual network advances so too does the virtual service assurance that supports it.

Significantly reduced CAPEX and OPEX

With cloud-native service assurance the solution cost is decoupled from the network capacity and embraces new software pricing models;

Pricing is now based on functionality which allows the CSP to deploy service assurance across the whole network effectively, and to be able to scale as the network grows. Traditionally huge costs are involved in capacity upgrades that up until now have remained part and parcel of a CSPs soaring CAPEX and OPEX.

Some vendors aren't adopting this approach, but pricing is an issue which vendors and CSPs are currently grappling with, and certainly for CSPs to enjoy the full benefits of NFV pricing models will need to be resolved to fit the transformation to a software controlled network.

Rethinking pricing structures also applies to commercial-off-the-shelf (COTS) hardware and white boxes.

The transition to NFV won't have solved anything if the underlying hardware pricing is not as cost-efficient as the controlling software layer.

Laying the foundations for a successful NFV transformation

CSPs have stated a key cornerstone for NFV transformation is a cloud-native service assurance solution.

Without a mature and production-ready solution, CSPs lack network visibility and the ability to assure that the NFV transition is transparent to customers and the required quality of service is in place to prevent churn.

Furthermore, by laying down this critical cornerstone early, CSPs will have a solid foundation in which to embrace NFV, and deliver a closed loop network that provides a centralized service level agreement policy across the entire network and creates a new type of experience for their customers. Key elements of a cloud-native service assurance solution are:

- Interoperability
- Automation
- Unified business analytics
- Elastic scalability
- Real-time performance
- Cost effective

Interoperability

Network and service agility are the foundations of dynamic NFV networks. These networks optimize, modify and re-configure the network and services on demand, in real-time and require centralized orchestration and management. Today's service assurance solutions are static and not optimized to handle these types of networks. So, for CSPs, it means a rethink of their current service assurance solutions that move from traditional reactive monitoring to proactive, real-time intelligence with tight integration into the NFV orchestration so that service quality is monitored continually and issues rectified automatically.

For CSPs, the quality of experience (QoE) will be the critical factor in making SDN and NFV initiatives successful and realizing the vision of an automated network.

By following the ETSI NFV architecture model, cloud-native service assurance interfaces at multiple levels across the MANO hierarchy (cloud inventory, collection, mediation, reporting and alarming). Tight integration allows CSPs to seamlessly consolidate assurance components into other areas of the network, for example, to provide centralized, network-wide alarming functionality throughout the organization or to maintain an inventory of the virtualized network elements' health.

A cloud-native service assurance solution slots into an NFV network as a Virtual Network Function (VNF) with multiple VNFC (VNF Components). Each system component is a virtual machine and built to work seamlessly in the cloud; integrated into standard ETSI-compliant NFV Management and Orchestration (MANO). Working with OpenStack and VMware the assurance solution can be deployment and configured at the click of a mouse.

By assimilating MANO and assurance, CSPs maintain a unified service-level policy across all network domains and service types to deliver a consistently high customer experience and assure that service levels between CSPs for network sharing and roaming are consistent.

The service assurance solution acquires traffic data from multiple sources, such as virtual port mirroring, vTAP, physical port mirroring and directly from VNFs and TAPs over GRE Tunnels and others.

While CSPs are building out their cloud platforms and strategies, it's important for cloud-native service assurance to offer CSPs the option to integrate service assurance into a generic Virtual Network Functions Manager (VNFM) or a branded vendor version. This decision comes down to the CSPs' preference. As a key component of the NFV MANO architectural framework, the VNFM is responsible for the lifecycle management of VNFs under the control of the NFV Orchestration (NFVO) and is the operations, administration and management component of the assurance solution that synchronizes and installs the system via the onboarding procedure. Once the Manager has installed and verified the system is up and healthy, it runs scripts to automatically configure the system so that the system is fully operational and ready to monitor the network. While running, it constantly communicates with all the solution elements and the cloud orchestration to assure system health is maintained and network services and customer experience monitored.

Embedding service assurance as an integral part of the network is also essential to creating the automation layer through its continual synchronization with the NFVO.

This provides cross-domain (physical, virtual and hybrid) and cross-service (voice and data) analytics, breaking down traditional silos and optimizing network capacity and resources.

Automation

Automation is key to agile service creation, delivery, and scaling. With this dynamic, real-time, automation, CSPs aim to provide their customers a new type of experience in which the user receives a constantly high level of customer experience and offers a more personal and accessible network. With features such as a self-service portal in which the users have direct access to, and can request new services on-demand.

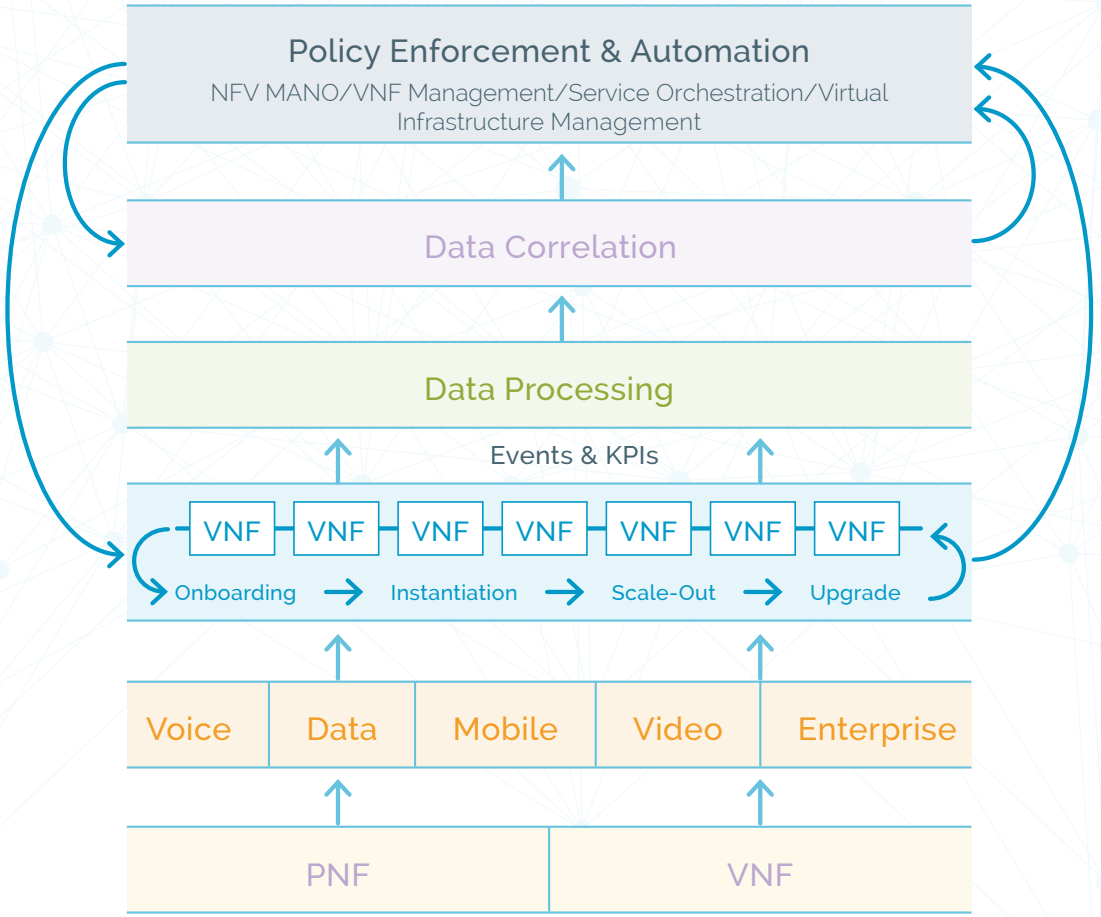
For this type of service delivery and orchestration model to work, orchestration and service assurance need to work in harmony to deliver and assure these services with minimal manual intervention.

Cloud-native service assurance needs to constantly synchronize with the NFV MANO so that advanced orchestration scenarios automatically deploy for rapid onboarding in minutes, and to facilitate the delivery of on-demand probing. These automated scenarios are triggered to provide assurance with the launch of new services - without manual intervention - to constantly monitor network performance to assure the delivery of high-quality services 24*7. NFV MANO manages the cloud-native service assurance hardware resources in unison with the rest of the network scaling up and down as and when needed to make capacity and resource management much more cost-efficient and effective.

In legacy assurance solutions data is collected and analyzed, problems pinpointed, and then the process requires manual intervention by an engineer who needs to take that insight and act on it manually.

In a closed loop solution, the service assurance solution collects, analyzes, and pinpoints problems, and then makes recommendations to the NFV orchestration.

With assurance and MANO constantly synchronizing and able to automate some processes, time to resolution is reduced, preventing service level degradation and maintaining high-quality customer experience. This automation layer enables the CSP to implement a self-healing network, that is only possible by deploying cloud-native solutions and deeply embedding assurance into the network.



Due to the amount of traffic crossing through the network, it won't be possible to manage future networks efficiently without moving to a more automated network.

In the next few years, more and more Internet of Things (IoT) devices will be connecting to the network. Today, approximately 400 million IoT devices connect to the network. Between 2017 and 2022, this number is expected to increase at a CAGR of 21 percent, so approximately 18 billion devices will be connected by 2022. This increase in devices and traffic as well as the introduction of 5G services; with reduced latency, extremely high bandwidth and network slicing will make the necessity of more and more network automation even more critical.

Unified business analytics

During the CSPs, transition to NFV, a mix of physical and virtual network elements (hybrid networks) will be used to deliver communication services to consumers, consequently service assurance solutions need unified business analytics that run across all network types and all services (fixed and mobile) to provide CSPs complete network visibility.

Cloud-native service assurance provides real-time, contextual actionable intelligence giving customer, service, network and device insights in real-time for engineering, operations, marketing and customer care, so that CSPs can optimize network performance, maintain service quality and deliver a high customer experience.

Unified business analytics plays a crucial role in assuring that the transition to NFV is transparent to customers, and maintaining high service quality. The goal of analytics is to convert network intelligence into real-time, actionable insights to maximize revenue streams, assure all the network services, proactively locate and resolve performance issues as well as improve customer retention and network and capital efficiency. With these insights integrated into decisions and processes across the organization, CSPs gain the ability to act faster and in the right areas; taking proactive steps to improve customer loyalty and drive growth.

For the network, unified business analytics ensures optimal service provisioning across the virtual network environment, as well as seamless interoperability in the hybrid network (between physical and virtual resources) which is critical as more and more services, will be delivered across a hybrid network (as the NFV transformation continues).

CSPs at the testing and planning stages of NFV, understand virtualized service assurance is key to their cloud transformation, therefore any service assurance investment will need to be future proof and support this transition as well as the CSPs' current physical network. By providing unified business analytics that covers all network domains (virtual, physical and hybrid) network engineers can continue using the same analytics and workflows tool today and throughout the transition to NFV.

Scalability

Elastic scaling is an essential benefit of adopting a cloud architecture and enabling CSPs to dynamically adjust the network resources to deliver a better customer experience and optimize the network service delivery.

By deploying a cloud-native service assurance solution, elastic scalability is performed automatically via the NFVO under NFV MANO.

Scaling can be triggered by the NFVO resulting from monitoring the VNF components health KPIs or triggered by the VNFM. There are two ways to scale the network in a cloud environment; vertical scaling where more resources are allocated to a Virtual Machine (VM) and horizontal scaling where more VMs are created to support a specific function. Both types of scaling improve solution performance and allow the handling of increased traffic, that is only possible by deploying a cloud-native solution that can accommodate the addition of more cores being made available and splitting traffic between the additional VMs. The cloud-native architecture also allows the system to be managed in VM clusters to simplify scaling and management of the solution.

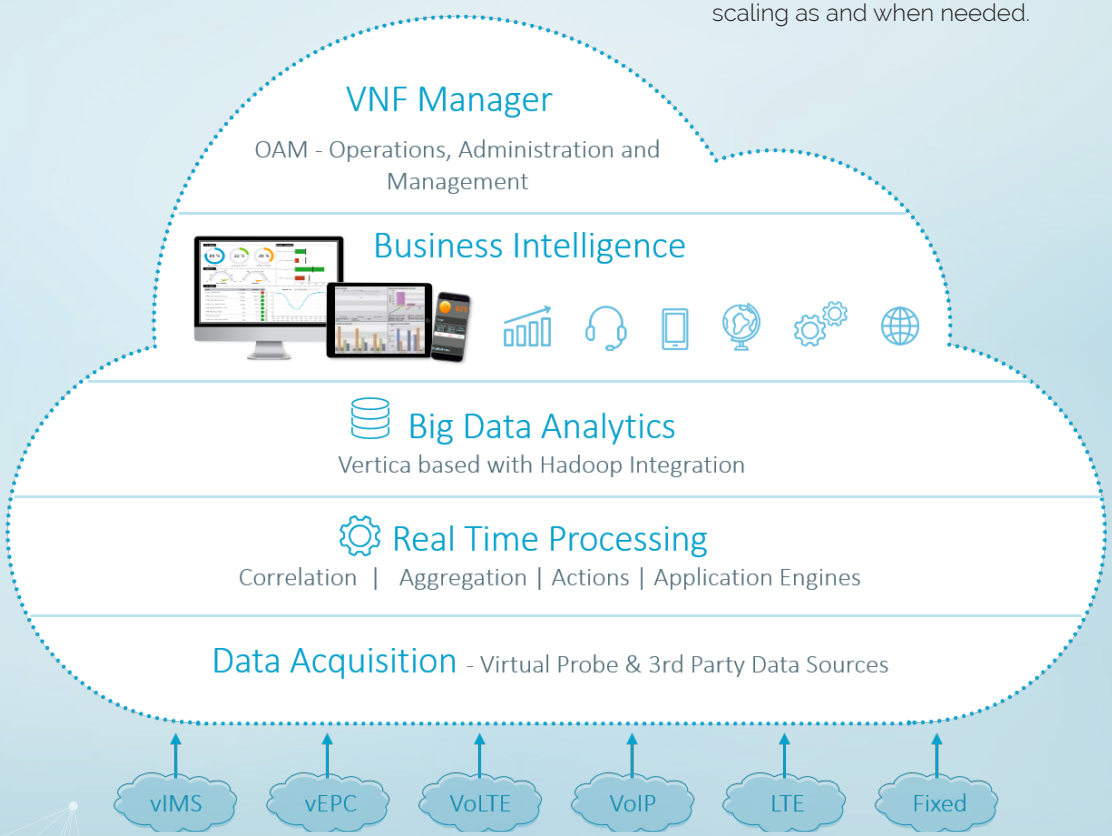
In legacy networks, scaling the assurance solution means throwing more costly hardware and investing time to deploy the new hardware. Legacy assurance solutions often store massive amounts of data (often at the probe layer) for post-processed call tracing and analysis, which simply does not afford cost-effective scalability with today's network traffic growth rate.

A cloud-native service assurance solution splits the system into two main elements; the back-end for the heavy lifting (data processing and big data analytics layer) and the front-end (data acquisition layer – the probes) to be dynamic and agile.

This design is opposed to legacy assurance that throws a lot of hardware at the probe layer but prevents that probe layer being agile and dynamic. Having a lightweight front-end allows the solution to deliver almost unlimited scalability, which will be required as CSPs integrate service assurance into their cloud platforms.

Furthermore, with a cloud-native service assurance solution designed with a micro-services architecture, each element of the system can be scaled independently, according to a built-in elastic scalability rulebook that states system dependencies by components.

Such an architecture allows very efficient capacity and resource management while assuring the solution scaling as and when needed.

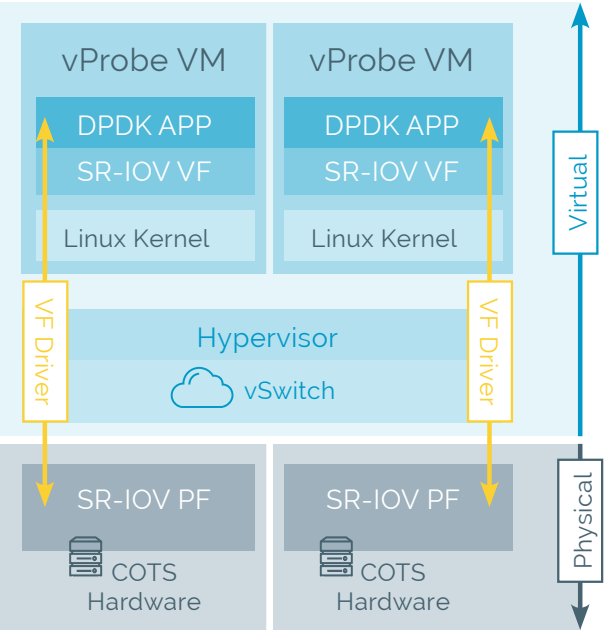


Real-time performance

As networks become increasingly more agile and dynamic, the performance of applications to support those networks will need to match the same pace, so that automation and closed-loop service orchestration can be implemented and assured.

Services on demand necessitate assurance on demand, with real-time software performance that matches wire speed. Cloud-native service assurance needs to utilize software and virtualized technologies such as Data Plane Development Kit (DPDK), Single Root Input/Output Virtualization (SR-IOV) and Massively Parallel Processing (MPP) to achieve real-time performance.

With cloud-native service assurance being the nervous system of the NFV MANO and monitoring all services, the assurance solution needs to be constantly



communicating and providing feedback on the health of the network and the service quality level. When the network changes, for example, a new service or network element is launched, the assurance solution needs to adapt to this change. A probe automatically launches and provides real-time analytics on the service or element performance, to the NFV MANO - a key requirement for self-healing networks - and also provides real-time analytics to network engineering and operations.

By moving the heavy lifting to the backend, a cloud-native service assurance solution can perform aggregation, correlation, and enrichment of the data rapidly to achieve superior performance and making data insights available in real time, as well as being able to provide data feeds to the northbound interfaces.

This backend processing layer enables advanced statistical computations on all multiple KPIs and over multiple dimensions in a matter of seconds with a big data columnar database that provides the ability to perform real-time analytics for large terabit networks. A columnar database stores all information in columns, thus eliminating the need for indexing and allowing for smart queries that process query searches only on the relevant columns, as opposed to the entire row, as per a traditional database.

Cost-efficiency

One of the main challenges that CSPs face in deploying service assurance in physical networks is the lack of cost-efficiency. In a hardware controlled network, hardware rules and so increasing network capacity means adding more expensive hardware. The same applies to expanding the service assurance solution capacity; resulting in more CAPEX outlays and time invested in upgrading the solution.

Fully virtualizing the service assurance functions, makes the solution cost effective and therefore economically viable for CSPs to monitor all their services. By embedding assurance functions into the network, CSPs unify management of the cloud resources and capacity, with upgrades and network changes executed in harmony; saving valuable time and costs, while also allowing automation to reduce costs on corrective measures, that would previously have needed manual intervention.

With network traffic constantly fluctuating, a cloud-native service assurance solution delivers the flexibility to scale vertically and horizontally as and when needed. Once additional resources are no longer needed they are freed up and released back into the network resource pool, making cloud-native assurance much more cost-effective.

Conclusions

The transition to NFV creates a significant opportunity for CSPs; to cost-effectively manage their network, rapidly improve time to market for launching new services, and delivering a new level of quality of experience to their customers.

However, a key enabler to unlocking the benefits of this network transformation is for CSPs to deploy a mature, production proven, cloud-native service assurance solution. Seamless integration into the cloud environment delivers the automation, real-time performance and scalability that is required to bring value to CSPs and cost-effectively assure their network.

Furthermore, CSPs are looking for service assurance vendors that understand the cloud environment to provide their expertise as they integrate assurance into their evolving cloud platforms. In facing such challenges integrating assurance across virtual, physical and hybrid networks (which often means cloud-native assurance needing to tap into legacy probes to provide unified analytics), CSPs need assurance vendors with virtualization experience and knowledge to overcome these challenges.

Lack of industry standards for onboarding different VNFs, dependencies and instantiations mean working with standards organizations such as ONAP and Open Source MANO (OSM), to improve interoperability and push better standardization forward.

Looking to the future, the cloud-native service assurance vendors will continue fine-tuning solution architectures to provide CSPs a lean, agile solution to further increase performance, automation, and scalability. Currently, some CSPs are evaluating containerization - a container being a mechanism that helps build a micro-services architecture and helps save time in building scalability. Once CSPs start adopting containerization, service assurance solutions built on a micro-services architecture will need to adopt containerization to further enhance scalability and performance.

Additionally, as the world of IoT and 5G moves closer, service assurance vendors will need to apply the power of the cloud to become more proactive in analyzing the network traffic, usage and customer trends. 5G will also introduce the concept of network slicing, where a single physical network is partitioned into multiple virtual networks, allowing the CSP to offer distinct levels of services for different customer/usage segmentations (such as IoT, car-to-car communications, higher speed video streaming). For cloud-native service assurance, this will require very high real-time performance and complete integration into the network to monitor different service levels for each service layer.

Despite the significant challenges in transitioning to NFV, ultimately CSPs will succeed in moving to the cloud, which will provide the infrastructure needed to continue pushing innovation in the telecom industry for many years to come. A key prerequisite of this transition is for CSPs to implement cloud-native service assurance to maintain network visibility throughout this transition – whatever the network domain - to assure the delivery of a high-quality customer experience.

www.radcom.com