RADCOM

DELIVERING A SUPERIOR CUSTOMER EXPERIENCE FOR 5G

Table of Contents

1. Introduction ... 3
   1.1. A new dynamic, open and modular network ... 3
   1.2. Web-based APIs not legacy protocols ... 4
2. Challenges ... 4
   2.1. Transitioning to a 5G core ... 5
   2.2. Deploying a cloud-based RAN ... 7
   2.3. Navigating the right migration path ... 8
   2.4. NSA option 3, 3a and 3x ... 9
   2.5. Long-term migration ... 11
   2.6. Increased network complexity ... 11
3. Redefining the customer experience ... 12
   3.1. Enabling complete 5G network and service visibility ... 13
   3.2. Efficient correlation of multiple data feeds ... 15
4. Ensuring 5G services with RADCOM Network Intelligence ... 16
   4.1. Intelligent ... 18
   4.2. Container-based ... 19
   4.3. On-demand ... 19
   4.4. Network Analysis ... 19
   4.5. RADCOM's NWDAF solution ... 20
   4.6. From next-generation packet analysis and call tracing to end-to-end SOC ... 24
5. Initial 5G services ... 25
   5.1. Enhanced Mobile Broadband (eMBB) ... 25
   5.2. Fixed Wireless Access (FWA) ... 25
   5.3. Multi-access Edge Computing (MEC) ... 25
6. Summary ... 26
7. Abbreviations ... 28
8. References ... 30

1. Introduction

With the recent introduction of 5G into a broad range of markets worldwide, the Fourth Industrial Revolution has begun. 5G promises a future in which people are always connected, and technology is deeply embedded in society; providing high speed and instant connectivity for any device and any person anywhere on earth, without restrictions.

Previous generations of mobile networks were purpose-built for delivering communications services such as voice (2G), mobile data services like messaging (3G), and then true mobile broadband (4G) for multimedia on the move with services such as video chat and video streaming. 5G is much more than just the next iteration of mobile networks. In the initial stages, 5G will deliver enhanced mobile broadband with higher data speeds (up to twenty times that of 4G), and better coverage for use cases such as Fixed Wireless Access (FWA). However, over time, 5G will transform the role that telecommunications play in society. True 5G will enable new use cases such as autonomous cars, remote control of critical infrastructure/machinery, smart-grid control, industrial automation, robotics, drone control, and remote telehealth services which will be empowered by an ultra-reliable, low latency network (up to ten times that of 4G) that will revolutionize our lives.

With the new 5G network being cloud-native, network functions will run as stateless, container-based, virtual network functions (VNFs). Being cloud-native will make operators more agile, and faster to innovate, delivering new, exciting services like cloud service providers such as Amazon and Google. Containerization means individual services are updated with minimal impact on other services. This cloud-native design built on white boxes or Commercial-Off-The-Shelf (COTS) hardware enables operators to reduce costs, accelerate the introduction of new services, and deliver faster iterations to their network and services. Upon this cloud-native infrastructure, operators are redesigning their network architectures, and core network using web-based standards to create a dynamic, open, scalable, and modular platform to deliver upon the promise of 5G.

1.1 A new dynamic, open and modular network

5G provides a modular, Lego-like framework in which services/applications can be deployed using components from multiple sources and vendors. The 5G network allows control plane Network Functions (NFs) to expose Service-based Interfaces (SBIs) that act as service consumers or producers. The NFs register their services in the network repository function, and services can then be discovered by other NFs. This new architecture enables modular deployments, where every NF allows the other authorized NFs to access the services, which provides incredible flexibility to consume and expose services and capabilities for both internal and external parties. Network functions are self-contained (without affecting each other. e.g., healing and scaling) and interchangeable while also being able to take the role of either a service producer or consumer. This new network design provides the following benefits:

- Modularity - The network is composed of modularized services - also known as Microservices - that can be reused among different network functions.
- Extensibility - The network can be easily extended without introducing new reference points. So, traffic can be easily balanced or offloaded by the deployment of new NF service instances.
- Interoperability - Network functions can be easily exposed to external users - such as 3rd-party application developers, thus making the platform interoperable, and open while extending the cloud platform beyond the operator.

1.2 Web-based APIs not legacy protocols

The 5G core moves away from traditional telecom-style protocol interfaces to allow functions to communicate with one another and share data using a distributed web services model and not specific network protocols. Each function exposes its functionality and communicates through an SBI using RESTful based APIs via HTTP/2. With JavaScript Object Notation (JSON) being the application layer serialization protocol, and for security at the transport layer, all 3GPP NFs will support Transport Layer Security (TLS).

An API enables the exposure of an organization's digital services and assets in a controlled way and is a universal concept used by modern software design, especially for web-services and encompasses a wide range of use cases which is why 3GPP decided that 5G service exposure should be based on RESTful APIs. Using a modern, open, web-based design like Amazon, Google, and Facebook to expose their cloud platform in a controlled way, using already widely adopted RESTful paradigms will enable operators to break down traditional network silos and empowering vertical markets to build upon the operators' infrastructure with modular services that will seamlessly slot into place, turning the telco cloud into a service platform for other vendors. This approach will also make it simpler for an operator to add, remove, or modify network functions from a network processing path (functional agility) and create new service-specific service paths on-demand (service agility). This major re-architecture of the network will provide operators with the necessary platform agility needed to deliver the new generation of exciting mobile services and provide a hub in which other companies can also be part of the Fourth Industrial Revolution.

In total, about 45 operators in 30 countries[1] have already activated 5G within their live network. Currently, 5G handsets are limited, however, over 3M 5G subscriptions are projected worldwide by the end of 2019. Overall, the forecast is that by the end of 2025, there will be 1.9 billion 2.6 subscriptions and that 45% of mobile data traffic will be carried by 5G networks[2].

2. Challenges

5G will be delivered using a new core network (5GC) that is cloud-native, as well as a new radio access technology called 5G New Radio (NR). Unlike earlier mobile networks that required both access and core of the same generation to be deployed, with 5G, it is possible to mix elements of different generations in different configurations. Initially, 5G networks will be deployed in non-standalone mode (NSA) that combines multiple radio access technologies. So, a host LTE network using an enhanced 4G core will deliver 5G services via a 5G NR.

Over time operators will migrate to a cloud-native 5G core and deliver 5G services in a standalone (SA) mode that no longer depends upon the 4G core, which will enable operators to execute network slicing, dynamically control the network, deliver intelligence at the edge, and offer multiple radio networks and connections.

However, the cloudification of the network is a challenging task and adds a lot of complexity that will take numerous years to implement fully. Operators will need to support 5G and legacy networks while also managing traffic growth. So, optimizing and assuring the network services that run across both legacy and cloud-native environments will be critical if operators are to transition successfully and ensure that the technology migration is seamless to their subscribers.

With customer expectations and the ease in which subscribers can churn, it will be essential for operators to deploy Service Operations Center (SOC) and Customer Experience Management (CEM) solutions. SOC and CEM will enable operators to monitor the end-to-end service quality smartly, prioritize customer affecting service degradations, and understand the overall customer experience to optimize churn. Both SOC and CEM solutions correlate multiple data sources (such as OSS and BSS data) to provide operators complete end-to-end service visibility. When enhanced with probe-based service assurance data, SOC and CEM provide root-cause analysis and troubleshooting at both a high level and granular level, with drill-down capabilities to the packet or subscriber level.

Furthermore, with so much of the underlying network changing in 5G, operators will also need to ensure they deploy next-generation, low-level tools like protocol and session analyzers to troubleshoot the network performance and optimize their services. Laying down the foundations to assuring services in a cloud-native platform now will also enable operators to embed the fundamentals needed for future closed-loop functionality.

2.1 Transitioning to a 5G core

The introduction of Control and User Plane Separation (CUPS) in the 4G EPC was the first step towards the 5G core architecture. The Serving Gateway (SGW) resides in the user plane and forwards and routes packets to and from the radio to the Packet Data Network Gateway (PGW). CUPS split the SGW and PGW functions into a control and data plane component. So, the SGW becomes the SGW-C and SGW-U, and the PGW becomes the PGW-C and PGW-U. First introduced in Release 14 and developed in 3GPP Release 15 Control & User Plane Separation (CUPS) was added to support a more flexible, distributed architecture, with both centralized and edge deployments that will be essential for 5G.

The control plane and all the associated complex interactions are centralized, while the user plane is distributed at the edge closer to the user and as virtual functions rather than hardware functions, placed at the optimal location on-demand. This separation of control and user plane will be critical as new 5G use cases are rolled out like autonomous cars, so the user plane can be run in a data center in a city closer to the end-user, thus reducing latency. Furthermore, this will also enhance high-bandwidth services that are offered today like video streaming, where the data will be closer to the end-user, at the network edge, improving service performance and saving on valuable network resources in the core.

CUPS represents a notable change to the mobile network architecture. It has significant implications for service assurance vendors who need to correlate the control plane and user plane as well as perform new CUPS protocol decoding to provide operators with complete network visibility.

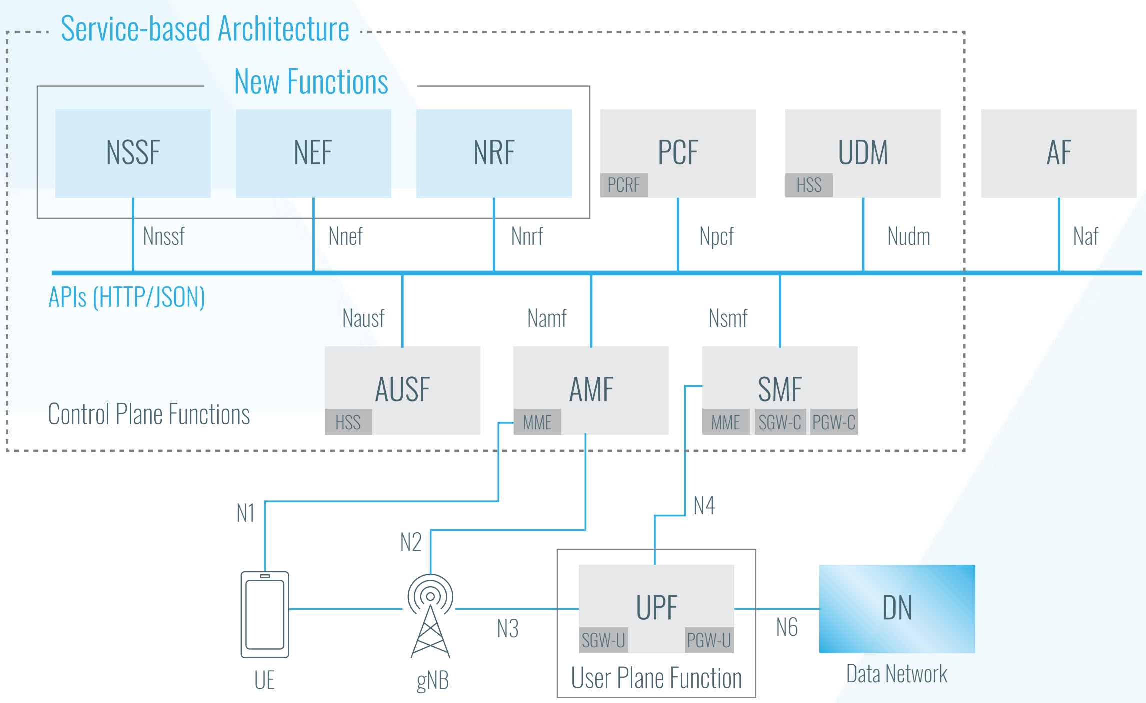


Figure 1 – The new 5G core architecture with 4G functions mapped to their 5G equivalent

The second step towards the 5G core architecture is the move to Service-Based Architecture (SBA). In the 2G, 3G, 4G network core, a point-to-point (P2P) architecture was deployed. The challenge with a P2P architecture is that it contains many unique interfaces between functional elements, each connected to multiple adjacent elements. This “tangle” of connections creates dependencies between functions and makes it difficult to iterate fast and deliver agile services. SBA introduces a new software architecture based on IT principles that enable faster service creation and provides a critical foundation for the evolution of all future mobile innovations.

Moving away from the point-to-point approach and providing a more flexible, plug, and play type framework in which services can be easily switched in and out will address the diverse service types and highly demanding performance requirements in a highly efficient way. The new architecture also supports additional services not available in the 4G core – notably related to network slicing and multi-access. Some of the key features are a formal separation of control and user plane, split of session and mobility management into the session management function (SMF), and the access and mobility management function (AMF).

Secure and encrypted

5G is about enabling a diverse new set of services and use cases affecting nearly every aspect of our lives and will open the network up to allow 3rd parties access to add their services. So, 5G must be delivered securely even while exposing functionality to other operators and 3rd parties. Also, in the long-term, 5G will enable Massive Internet of Things (MIoT) applications such as traffic sensors and Vehicle-to-Infrastructure (V2I) services that are the foundation for smart cities. Therefore, it’s critical to prevent hackers from accessing that data, hijack IoT devices, or disrupt services.

Security has been a top priority for 5G, with multiple organizations working together to create a more secure network. 3GPP, ETSI, and IETF have each focused on specific parts. The 5G core network functions support security protocols such as TLS 1.3 (defined by the IEFT in RFC 84464[3]) to protect the network communication at the transport layer. 3GPP’s Release 15 makes TLS 1.3 mandatory for networks in the service-based interfaces, and Release 16 (5G phase 2) extends this to make it mandatory for mobile devices as well. Although, adoption of TLS 1.3 for the network core depends on the operator – it is expected that some operators will adopt this protocol – one of the challenges that TLS 1.3 will introduce is how to gain network visibility for security and monitoring purposes as passive mode decryption will no longer be possible (see Packet-based monitoring for more details). Also defined by the IETF is the OAuth 2.0 framework (defined in RFC 6749[4]) at the application layer to ensure that only authorized network functions are granted access to a service offered by another function.

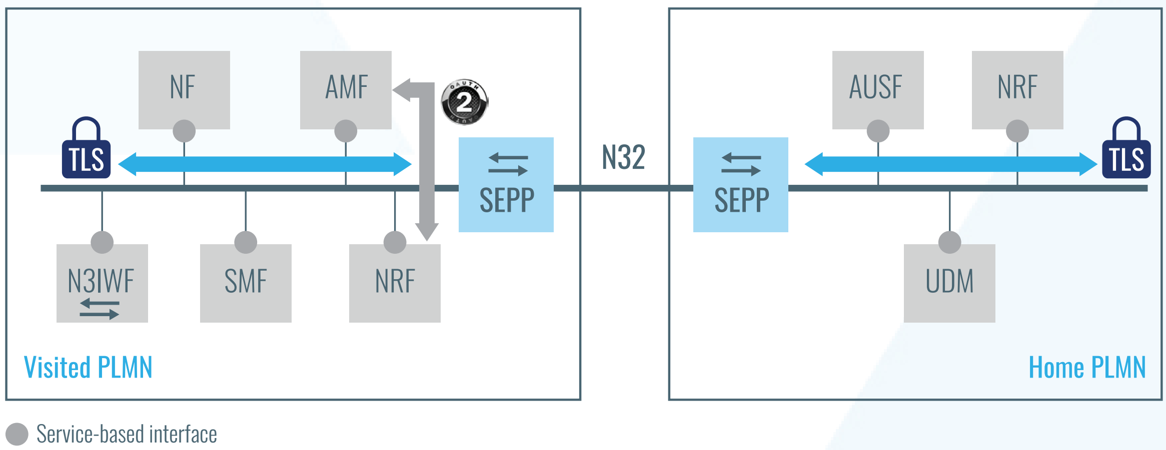


Figure 2 - SEPP function provides end-to-end security protection for inter-operator control plane traffic

To further enhance security in the SBA, 3GPP has defined a new function called the Security Edge Protection Proxy (SEPP) to implement end-to-end security protection for inter-operator control plane traffic. The SEPP function securely transports signaling between the Home and Visited Public Land Mobile Network (PLMN). SEPP will significantly improve security in interconnect situations and make it impossible to read or manipulate message content without prior agreement with the operator as it traverses to other networks. However, SEPP terminates TLS connections between the 5G core and another network's SEPP. So, the SEPP function could conceivably provide service assurance vendors an unencrypted copy of the network traffic for the N12, N16, N8, N24, N31, N32 interfaces.

In addition to the new functionality, authentication between SEPPs is required, and a new application-layer security solution on the N32 interface (between the SEPPs) has been created to protect sensitive data while still allowing mediation services. So, the main components of SBA security are authentication, and transport protection between network functions using TLS, the authorization framework using OAuth2, and improved interconnect security using the new SEPP protocol designed by 3GPP. With the new core being designed to allow plug and play functions and services from other vendors, these added layers of security are essential to providing a secure cloud for delivering the next stage of mobile innovation.

2.2 Deploying a cloud-based RAN

A critical element in any mobile network (as well as one of the costliest and most restrictive) is the RAN that provides wireless connectivity between the end-user devices such as a smartphone, laptop, or IoT device and the core of a wireless network. In a typical 4G network, the radio head unit (RRH) and baseband unit (BBU) is connected through fiber across a short distance and sit together at the edge of the network and are supplied by the same vendor. This vendor lock-in is required because of the Common Public Radio Interface (CPRI) that transmits digitized RF data over optical fiber between the RRH at the top of the cell tower and the base station below is proprietary, which basically means that an operator needs to buy the baseband equipment and radios that work on the same system from the same vendor.

Although the CPRI continues to evolve, it is not a standard but complements 3GPP frameworks and is designed by four companies; Ericsson, Huawei, NEC, and Nokia. With the latest iteration released in May 2019, it enhances the support for the 5G front-haul. However, in designing their new 5G RANs, operators want to break out from this vendor dependency and move to a multi-vendor RAN. Also, when it comes to 5G, CPRI could become a bottleneck and not scale to deliver on 5G demands. Operators want to make this critical part of the network more cost-effective, more straightforward to upgrade, and dynamic to manage.

The next-generation RAN architecture is defined with a functional split between the baseband and the radio. Virtualization will help operators make this transition more cost-effective and allow them to manage their services more dynamically. These changes in the RAN will come in several forms:

Cloud-RAN or Centralized-RAN (cRAN)

cRAN moves the baseband unit (that is the brains of the RAN) to a central location rather than sitting at the base of a tower, which decouples the radio elements from the processing servers. These cRAN baseband units are virtualized units running on standard servers and centrally located, reducing the number of sites needed, cutting costs, and easily managed as a pool of baseband units that operate multiple radios. cRAN means that the radio head units generally have a smaller footprint as the base station with on-site processing is decoupled from the radio unit. However, the cRAN architecture itself contributes latency between the RRH and the BBU due to the distances between the centralized BBU and RRH that can be up to 25 km.

Virtualized RAN (vRAN)

vRAN replaces the proprietary baseband unit hardware that would sit below the antenna and the radio in traditional network architecture and replaces it with virtual functions running on generic servers at a central location. By decoupling the RAN functions from proprietary hardware, operators can manage their network more efficiently and scale their network resources dynamically that will be essential for deploying high bandwidth, on-demand, 5G services. A virtualized base station will also improve spectral efficiency by utilizing a pool of BBUs that share signaling among different cells.

Although virtualizing the RAN has many advantages, a high-speed connection is required between the radio (RRU) and compute elements (BBU) as the centralization of RAN functions demands high-bandwidth and low-latency between the base station and data center, so these deployments favor fiber-rich regions.

However, in the long-term, virtualization is critical for operators on the road to 5G. As operators begin to implement dynamic network slices for such use cases as IoT and mission-critical services, it will be necessary to smartly control network resources on a service-by-service basis using multiple access technologies. Only by decoupling functions and virtualizing the RAN will operators gain this dynamic, smart control of their end-to-end resources.

Both cRAN and vRAN deployments have/are being implemented. In North America, both AT&T and Verizon have adopted cRAN. Verizon, for example, has utilized cRAN[5] to implement Self Optimizing Network (SON) technology that can adjust the power of individual cell sites depending on real-time demand. In Asia, China Unicom and Nokia[6] have partnered on cRAN in the newly created "megacity" of Xiongan, China. With the network, being dubbed the "world's largest field trial," to more rapidly deploy 5G.

As for vRAN, in June 2019, Rakuten Mobile announced[7] that they would be building a 5G open vRAN architecture in Japan. As well as partnering with NEC, Rakuten is investing in Altiostar that provides a 5G-ready vRAN software solution. Whereas, in North America, Nokia publicized a blog post[8] that they had deployed a cloud-based vRAN with Verizon. As more and more operators start adopting both cRAN and vRAN, multiple vendors are expected to enter the fray as the RAN market opens up to new startups as well as the established vendors transitioning to cloud-native solutions.

2.3 Navigating the right migration path

3GPP released the 5G NR specifications for non-standalone (NSA) operation in December 2017[9] (known as option 3) that was phase one of the 5G standard. That was followed in June 2018 with phase two when the Standalone 5G NR radio specifications (known as option 2) were finalized. NSA options consist of two generations of radio access technologies (both 4G and 5G) using dual-connectivity, and the core network being either EPC (Evolved Packet Core) or 5GC. NSA means that the 5G NR network cannot stand alone and relies on the 4G EPC for control-related functions. The SA options include only one generation of radio access technology, and the core networks operate separately. SA means that the 5G RAN can be run independently of a 4G network.

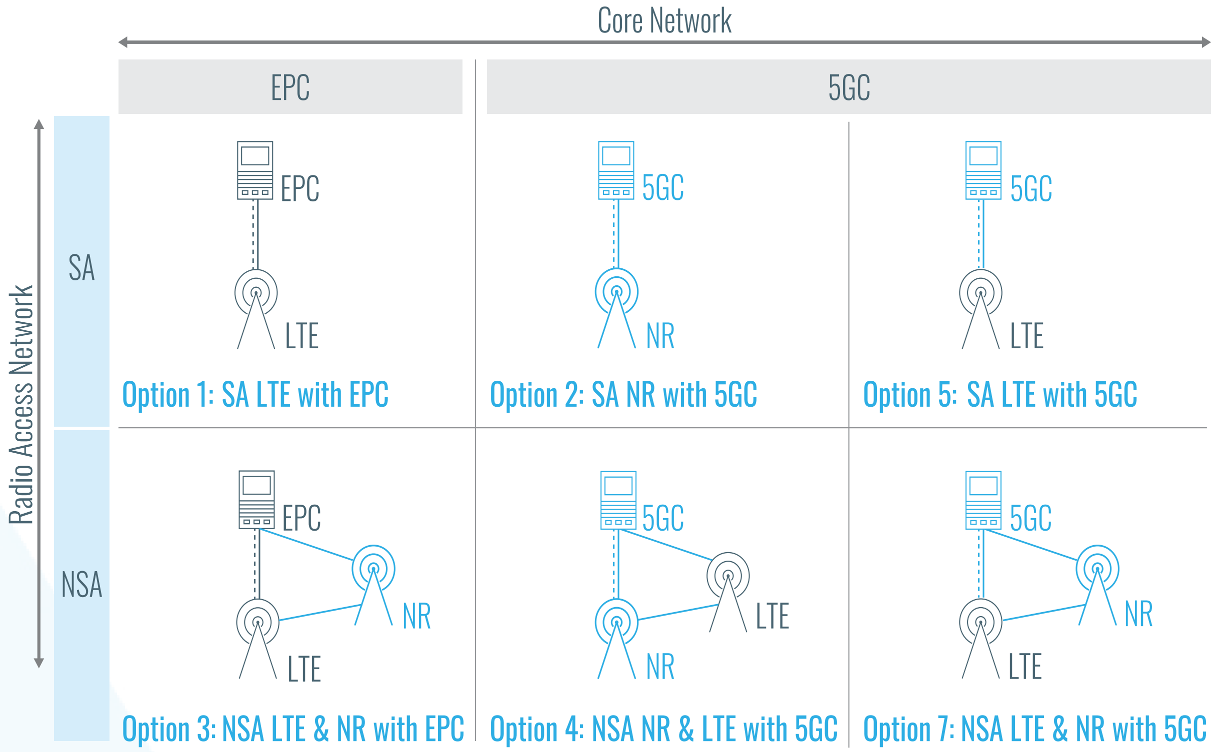
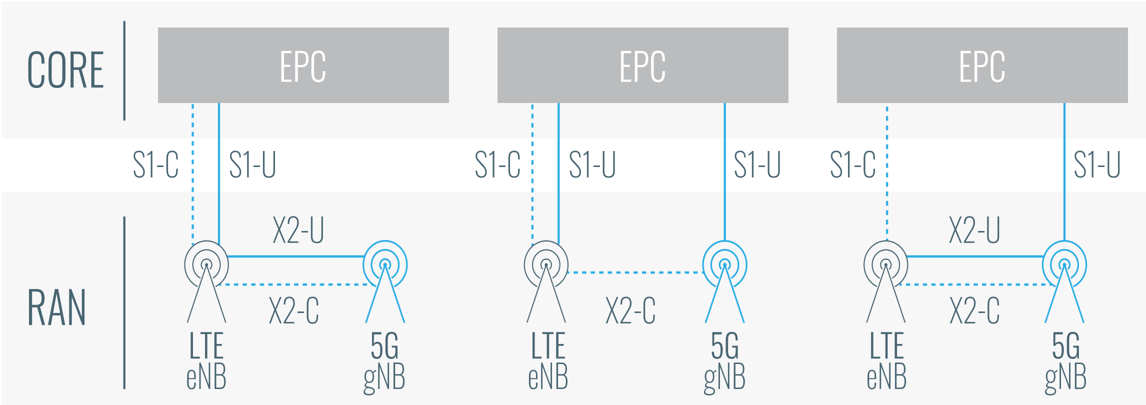


Figure 3 – Deployment scenarios for 5G

2.4 NSA option 3, 3a and 3x

Most operators that have started rolling out 5G have adopted some form of NSA option 3 (see the diagram below) as it leverages existing 4G deployments, and can be brought to market swiftly with only minor alterations to the operators' 4G network. The dual connectivity used for a Master eNodeB to connect to Secondary eNodeB has been standardized in the 4G network, and NSA Option 3/3a/3x has adopted this standard. The end-user device is connected to both 4G and 5G radios at the same time; 4G for signaling and 5G NR for the delivery of data (streaming video, audio, etc.). To support NSA, the operators need to do a minor software upgrade, and there is no need to make any modifications to the hardware. The overall process, including handover, is no different from that of a 4G network. This deployment option also supports legacy 4G devices, and voice services will remain unchanged. That means 5G devices will only need to support the new radio protocols so new devices can be developed quickly.



In Option 3, there is no connection between the gNB and the 4G network. All 5G user plane traffic is routed through the 4G eNB to the 4G network. Operators will need to increase the bandwidth of the S1-U interface to meet 5G requirements and upgrade their eNB hardware.

In this scenario the X2 interface traffic between the eNB and gNB has 5G user plane traffic which means the amount of traffic could be significant.

Option 3a provides for dynamic switching of the 5G user plane traffic between the 4G and 5G network. The gNB has an S1-U interface to the 4G network, but no X2 interface.

So, the 4G eNB and the 5G gNB directly talk to the 4G core but do not directly talk with each other over the X2 interface. This means that there can be no load sharing of data over a single bearer over 4G and 5G.

In this scenario, only control plane traffic transverses the X2 interface. So X2 traffic is significantly lower than in Option 3.

Option 3x is a combination of option 3 and 3a with both the S1-U and X2 interfaces being available from the gNB.

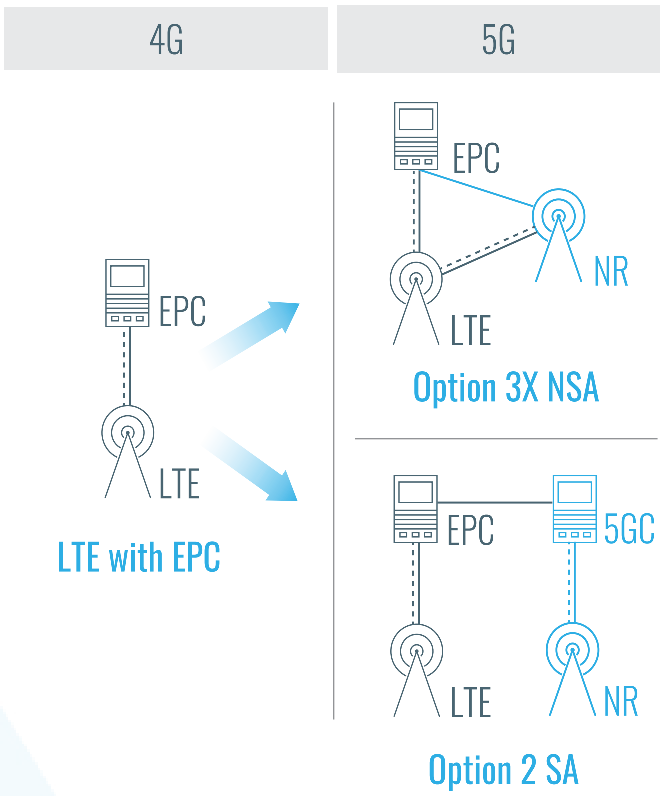
In this scenario, all the 5G user plane traffic travels via the gNB, and the control plane travels via the eNB.

Control plane - - - - - -
User plane ———

Figure 4 - NSA option 3, 3a and 3x

One approach that can be adopted by operators is to deploy new core network elements that can support both the EPC user plane (SGW and PGW) along with next-generation 5GC User Plane Function (UPF) and Session Management Function (SMF). RAN will use the existing 4G base stations with upgrades to support the NSA features as well as the deployment of new 5G NR cells to provide dual-connectivity, with interconnectivity using 3GPP defined extensions of the X2 interface. One of the variants to option 3 (known as 3X), provides for high bandwidth flows to be first routed to the 5G NR to avoid extreme user plane overload on the existing 4G radio.

The downside to deploying the option 3 scenario is that it does not introduce the new 5G core so, beyond enhanced mobile broadband, the network will not serve advanced 5G use cases that utilize new capabilities such as network slicing, advanced QoS, etc. that run on the new service-based cloud network. A different approach some operators are taking is to roll out 5G using option 2 SA. Deployment of option 2 means operators are introducing the new 5G Core network functions and 5G NR base stations and will circumvent the need to rebuild EPC core networks and minimize changes to 4G radio stations. This scenario is only expected to be adopted by operators that don't have an existing 4G network.



Transitioning to option 3x allows for high bandwidth flows to be first routed to the 5G radio to avoid extreme user plane overload on the existing 4G radio.

By adopting option 2 SA operators introduce the new 5G core network and 5G radio without the need to rebuild their EPC core and minimize changes to their 4G radio.

2.5 Long-term migration

After operators roll out their first 5G services, they will need to select longer-term migration paths with options 2, 4, 5, and 7. Options 7, 4, and 5 all require an upgrade to the 4G radio to support 5GC interfaces (N2/N3 to 5GC and Xn to gNB and ng-eNB). Options 5 and 7 would maintain the 4G radio as the master node. In simple terms, option 7 means that the 5GC completely replaces the 4G EPC so that it handles all traffic from both the 4G and 5G radios. Option 4, however, would act as an extension of option 2 SA and would result in the 4G radio taking a secondary node role with the 5G NR as the master node. As in every technology transition, operators will be maintaining the balance between moving forward to the next generation network while also utilization their significant investments in their previous network infrastructures. Only time will tell which specific path each operator will take.

2.6 Increased network complexity

The shift to a 5G network is a seismic transformation of the network architecture and its management, bringing many benefits to the operator in terms of operational flexibility and scalability while also laying down the foundations for the next generation of exciting, dynamic customer and business services. However, this technology change also presents many more complexities and challenges that the operator will need to overcome to make this transformation a success.

Operators are virtualizing hundreds of network functions from the RAN to the network core. Up until recently, these functions were proprietary hardware solutions supported by Network Equipment Providers (NEPs) and known and deployed by network engineers for years. Now each function is virtual, dynamic, and can be launched on-demand with certain functions running alongside other functions on the same commodity hardware so east-west and north-south traffic need to be monitored.

Operators are also integrating new management layers to streamline and automate their service deployments and to manage services using a unified service level policy that down the road will lead to a closed-loop network. Of course, although the industry is moving to virtualization, there remains a legacy network, and so operators will need to understand the end-to-end service quality running across both network domains. Add to this the significant increase in data traffic and millions of more devices connecting to the cloud operators have significant challenges in understanding the end-to-end customer experience and troubleshooting the network performance.

3. Redefining the customer experience

5G offers innumerable opportunities for operators to redefine the services that they deliver to their customers and change what it means to be a telecom operator.

As they transition from providing only communication services to delivering content and offering a cloud platform for other companies to provide additional services, operators are shifting from being Communication Service Providers (CSPs) to becoming Digital Service Providers (DSPs). This transition has the potential of giving operators new revenue streams, and increasing their brand loyalty, but only if they can compete with other digital content providers and deliver a superior user experience.

Just like in previous mobile generations, the foundation for success is focusing on the customer experience. Service assurance needs to be the cornerstone and at the heart of CSPs' customer experience strategy amid the increasing network complexity as operators rebuild their network functions on a cloud platform. Only then will operators have full network and service visibility. Only with full, end-to-end visibility will operators understand the customer experience and have the tools and smart insights to troubleshoot the network performance effectively and ensure the network transformation to 5G is seamless to customers.

As in past mobile technology iterations operators that fail to understand the real customer experience and don't smartly monitor and rectify customer-affecting service issues will suffer churn. Continually ensuring a high quality of experience (QoE) and quality of service (QoS) has never been easy, and 5G will make this even more of a challenge.

With a cloud-native architecture being essential for 5G, operators will need to master network virtualization with its new architecture and dynamic nature to lay down the foundations for their next-generation of services. Imagine a network full of virtual functions that can change on the fly. Multiply this by hundreds 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) within the same server and can also change on the fly. All of this complexity needs to be monitored for operators to understand the QoE and QoS.

Add the fact that physical networks are not going away. Therefore, for the foreseeable future, services will transverse both virtual and physical domains, which further increases the challenge for operators to understand the customer experience and service quality and know what customer-affecting issues are critical. Despite this, all these underlaying changes will need to be transparent to the operators' customers, and so the operator needs to ensure the QoE and QoS, however, intricate the situation. Furthermore, as the 5G rollout continues, operators will need to support the new use cases around ultra-low latency, edge clouds, and network slicing all while the number of devices and amount of traffic that needs monitoring continues to rise dramatically.

If operators are to transition to becoming DSPs successfully, they understand the need to change customer perceptions and reach the same level of customer experience and brand loyalty that web-first companies like Amazon, Netflix, and Google offer their customers. In a 2018 consumer survey[10] , it showed that operators in Europe and North America had Net Promoter Scores (NPS) between –5 and 40 compared to companies like Amazon and Netflix, typically scoring 50 or above.

> CSPs must recalibrate their customer experience strategies to tackle the increasing network complexity as they embark on various network transformation initiatives such as network function virtualization (NFV), software-defined networking (SDN) and 5G."

Anil Rao, Principal Analyst, Analysys Mason

In such a highly competitive market, operators must increase their focus on delivering superior customer experiences to differentiate themselves, boost brand loyalty, and gain new customers. Excellent customer experience will be essential for the success of 5G and could open a window of opportunity in which operators can redefine their relationship with their customers.

3.1 Enabling complete 5G network and service visibility

In recent years JSON has become the primary format for data exchange on the cloud and even though it generates human-readable statements and is being adopted for telco networks, not all the data needed by operators for network troubleshooting will be exposed, and the data that will be revealed only covers partial interfaces, for some users, for selected periods. Incomplete information and statistics will leave gaps in the operators' understanding of the customer experience and will not provide the smart, network, and service insights needed for comprehensive end-to-end troubleshooting. These capabilities are only enabled by an assurance solution that provides end-to-end tracing so that the operator can see the whole data flow.

Traditionally, operators have deployed probe-based service assurance solutions as an independent auditor of their networks. These solutions provide end-to-end tracing and full end-to-end visibility of the network services while empowering the operator with comprehensive root cause analysis and troubleshooting tools at both a high level and granular level; with drill-down capabilities to the packet or subscriber level. With so many new technologies, functions, and network architectural changes, both high-level and low-level tools in a container-based solution will be critical for operators transitioning to the cloud for NFV and 5G.

Packet-based monitoring

TLS 1.3 brings many changes to the cryptographic protocol to improve performance and security, while also eliminating complexities and simplifying the stack. The main security change that affects passive probing is that the use of static RSA (Rivest–Shamir–Adleman) and Diffie-Hellman key exchange has been removed, and so passive mode decryption will no longer be possible — replaced with ephemeral mode Diffie-Hellman which provides forward secrecy. Forward secrecy ensures that access to a key in the future cannot compromise the confidentiality of all past sessions. To do that, ephemeral mode Diffie-Hellman creates a unique one-time key for each separate conversation between a client and a server.

The adoption of TLS 1.3 depends entirely on the operator. Some may decide to deploy the TLS 1.2 protocol on their SBI or deploy an unencrypted SBI, which would mean that packet-based monitoring still has visibility into the core. However, if the operator decides to implement TLS 1.3 encryption, it would mean packet-based monitoring could not be used, as passive probes would be blind to the traffic that runs through the SBI. (Non-SBI interfaces such as the N1, N2, N3, N4, N6, N9 will not use TLS 1.3). If visibility into the SBI is limited, assurance vendors can acquire data from other sources. Some sources are new to 5G and others not. What is critical is the need for an independent auditor of the network to take all the different data feeds, correlate them into smart insights to provide operators with an understanding of the customer experience and enable end-to-end network troubleshooting. Some of the additional data sources in 5G are:

Network Data Analytics Function (NWDAF)

Part of the 5GC standard is the Network Data Analytics Function (NWDAF), as defined in TS 23.503[11] . It's a network analytics capability built into the general framework of the network architecture and is an evolution of the RAN Congestion Awareness Function (RCAF) from previous 3GPP releases. Its purpose is for centralized data collection/analytics, and although this function is still in the "early stages" of standardization, it could become a more critical function for analytics in future iterations of the 5GC.

Currently, 3GPP has standardized northbound interfaces. In the future, 3GPP may standardize the NWDAF format and the types of raw information that the function will examine. In theory, the NWDAF should be able to make use of any data in the core network, and upon request from other network functions, provide analytics information.

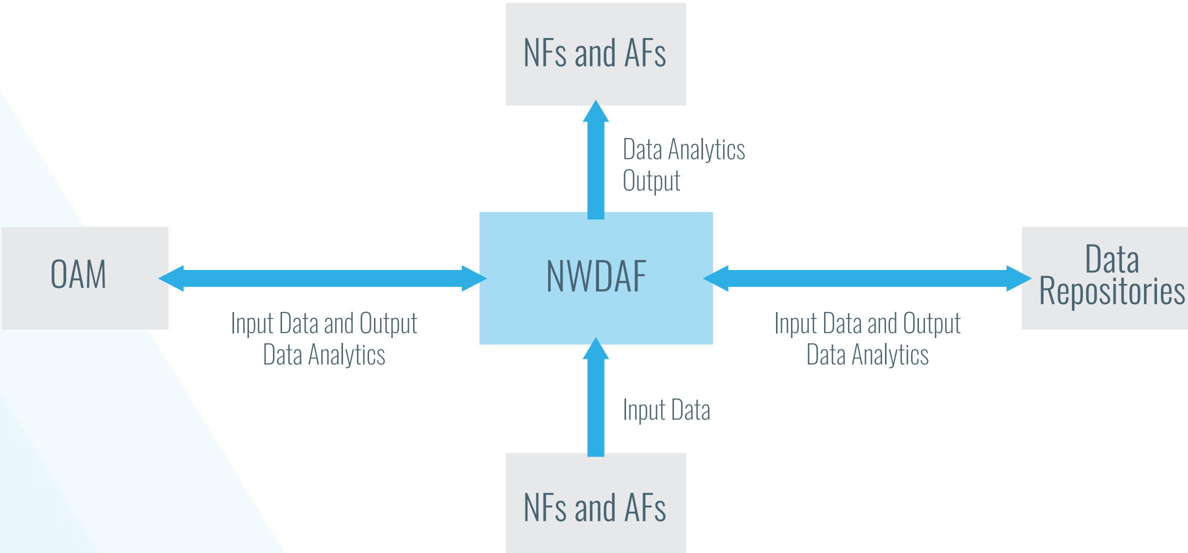


Figure 5 - Network Data Analytics Function as defined in TS 23.503

As defined in Release 15, the NWDAF description and capabilities are very elementary and provide load level information for a network slice. Release 15 defines the NWDAF as providing the 5GC with the ability to collect and analyze aggregated data per slice and to aid network optimization. Currently, some interfaces are defined between the NWDAF and the NSFF, (mainly the northbound ones), but the southbound interfaces and the way KPIs are calculated is not defined at all. So, time will tell if NWDAF expands to become more of an all-encompassing analytics function for 5GC than just for monitoring network slices.

OpenTracing

OpenTracing is an open-source project governed by the Cloud Native Computing Foundation (CNCF) that has defined a standardized API for distributed tracing. As OpenTracing is an API, a backend tracing system is required (for example, Jaeger) to collect the data and provide a feed (for example, using Kafka). As this is a framework, the actual trace content is not defined and will vary between network vendors. The NEPs primary concern is to provide the hardware functionality and not to burden their hardware by sending out trace data. So, NEPs that implement OpenTracing will limit the trace traffic coverage to about 10% of the overall traffic that flows through their hardware. Furthermore, OpenTracing does not have any correlation functionality, so it is just showing one side of the communication, which is useful for debugging, but not for network troubleshooting and understanding the customer experience.

So, assurance vendors will need to collect and correlate additional data to provide operators with an end-to-end view of the network for detailed network troubleshooting. For operators who want to use OpenTracing, each network function in 5GC would need to send OpenTracing events to an assurance solution, and each network event will need to be detailed and provide the following:

- The end-to-end flow of transactions related to each subscriber across all 5GC NFs, logical and physical interfaces
- A full, complete trace of every transaction in the 5GC, including all messages and attributes included in the transaction
- A clear indication of failed transactions, including the NF that signaled the failure and failure cause

Operators interested in utilizing OpenTracing can contact RADCOM's product team via our website for detailed specification requirements and recommendations.

Network event subscriptions

Network event subscriptions are a standard 3GPP service that allows an application to subscribe to network events and receive notifications. Most network service functions have this ability. These event subscriptions provide many different APIs that the assurance vendor can subscribe to, that give very detailed information on what's happening in the network. However, this does depend on the network equipment vendor, and so far, this service hasn't been implemented. In the future, this may be something that changes, and this service could be a good source of information that operators can use to understand what's happening in the network and could compliment the data received via OpenTracing.

3.2 Efficient correlation of multiple data feeds

So, considering the new network architecture and added network functions (which depends on each operator's implementation), service assurance vendors will need to collect different types of data from many various sources efficiently. The main challenge is the correlation and visualization of this data into the form of smart insights so that operators can understand the customer experience as well as troubleshoot and optimize the service quality. All this without burdening the operator with the need to store significant amounts of network data that is both unnecessary and a waste of valuable CAPEX and OPEX.

This streamlined assurance solution also needs to come with automated, on-demand capabilities that are tightly integrated with operators' NFV orchestration so that a fully automated assurance solution can be deployed on the fly to investigate any service degradations, provide root-cause analysis and then scale down and release cloud resources.

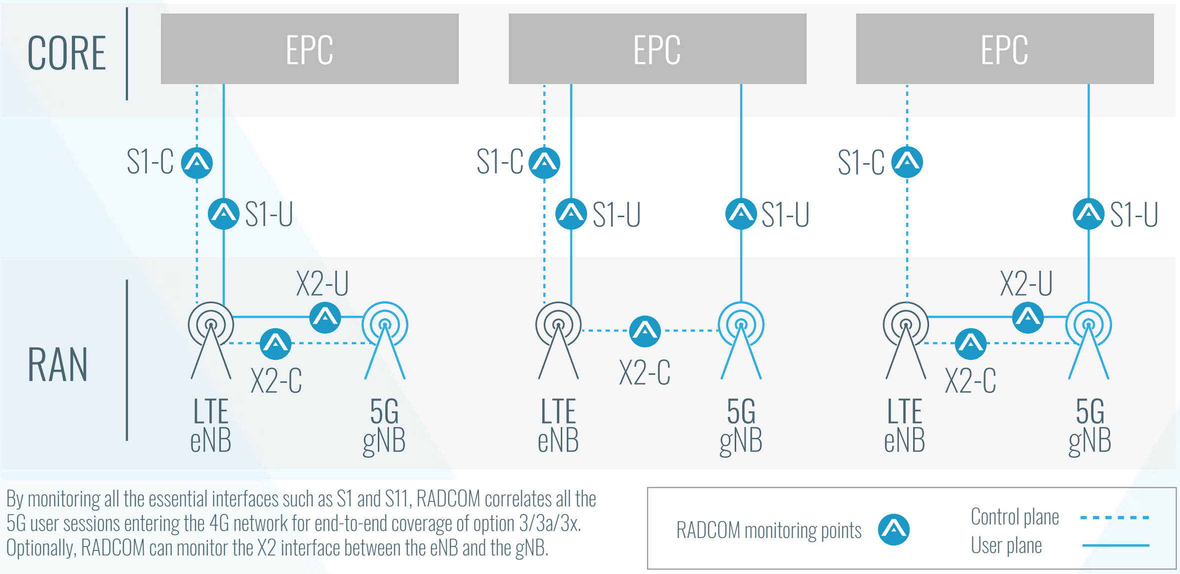
Furthermore, as data encryption becomes an integral part of the telco network, assurance vendors will need to utilize Machine Learning (ML) and Artificial Intelligence (AI) to smartly provide insights that automatically detect anomalies (for IoT) and understand the customer experience for encrypted traffic (such as for video streaming and gaming).

By reducing data collection to the minimal, enabling on-demand capabilities and utilizing AI, service assurance vendors can provide operators an efficient and cost-effective assurance solution. Delivering a tremendous customer experience that matches subscriber expectations in the age of a continually changing network and personalized services.

4. Ensuring 5G services with RADCOM Network Intelligence

RADCOM Network Intelligence delivers next-generation customer and service insights for 5G. RADCOM Network Intelligence is an automated, dynamic, and multi-functional solution, with smart minimal data collection and on-demand troubleshooting. Breaking away from the limitations of a virtualized probe-based service assurance solution, RADCOM Network Intelligence delivers a fully cloud-native, container-based approach that acquires data close to the source and uses a stateless architecture that seamlessly integrates within an operators' cloud environment. Kubernetes (K8s) control the containerized components lifecycle starting from the initial day-0 instantiation and throughout the overall platform lifecycle. Being dynamic and fully integrated enables operators to take an on-demand, closed-loop approach to assure the customer experience for first 5G use cases (such as enhanced mobile broadband, fixed wireless access, and edge deployments) and more advanced use cases along their 5G journey.

RADCOM Network Intelligence already supports NSA option 3/3a/3x and provides operators with end-to-end service visibility into the network performance and customer experience for the hybrid 4G/5G world. Option 3 routes 5G user plane traffic through the eNodeB. Option 3a is dynamic and allows 5G user plane traffic to switch between the 4G and 5G radios. In option 3x, all 5G user plane travels via the 5G radio, whereas 5G control plane traffic goes via the eNodeB.



By monitoring all the essential interfaces such as S1 and S11, RADCOM correlates all the 5G user sessions entering the 4G network for end-to-end coverage of option 3/3a/3x. Optionally, RADCOM can monitor the X2 interface between the eNB and the gNB.

RADCOM's solution ensures that the current 2G, 3G, and 4G networks are performing, services delivered over the new 5G radio are functioning, and with support for the new SBA, that the 5G network itself is working correctly and fully optimized as operators roll out their 5G services. RADCOM Network Intelligence has the operator covered from the RAN to the network core.

Operators that deploy NSA dual connectivity to deliver enhanced mobile broadband have to support both radios as well as the interactions between them. In NSA, scheduling and handovers are steered using the 4G control channel, so for handoffs between RATs, operators must monitor the control plane. 4G devices already have reliable handoff mechanisms, but switching a session from one RAT to another can still have significant latency that might cause sessions to drop during handoff. So, it is critical operators monitor these handoffs to ensure they do not impact the customer experience. RADCOM's solution for 5G covers network and service performance, RAN optimizations, as well as marketing and business intelligence (for example, if users own a 5G handset and are not utilizing 5G services).

RADCOM's solution benefits for operators:

- Offers SBA readiness (supporting complex CUPS correlation)
- Enables end-to-end service and network visibility from the RAN to Core
- Integrates into NFV orchestration with a container-based architecture that has a low footprint, consumes minimal resources, is easy to deploy on-demand, scalable and offers high performance
- Delivers a unified, multi-functional, cloud-native portfolio of network visibility, service assurance, and network insights
- Combines virtual probe functionality and complex back-end processing into one containerized node for improved cloud efficiency, easy capture, and correlation of multiple data feeds, as well as efficient indexing and minimum data storage
- Provides the Network Data Analytics Function (NWDAF) capabilities
- Automates solution deployment for on-demand instantiation, scaling, healing, and updating for a closed-loop approach to assurance with Kubernetes controlling the containerized components lifecycle
- Samples and filters traffic to smartly and efficiently manage and load balance massive traffic volumes across multiple clouds
- Correlates data from numerous sources. Including, network packets, generic network events, JSON, Protobufs, Counters, PM/FM/Infrastructure/Alarms/VNF Inputs/Events, CDRs from legacy probes (normally packet-based), and OpenTracing

RADCOM Network Intelligence's multi-functional solution includes RADCOM Network Visibility, a virtual network packet broker that collects, processes, distributes, and load-balances traffic across multiple clouds and domains (virtual and physical). RADCOM Network Visibility helps operators smartly sample and filter traffic to manage vast traffic volumes in 4G and 5G.

RADCOM Service Assurance extracts and intelligently correlates the raw data from multiple sources across the network and converts into rich, actionable network intelligence presented as RADCOM Network Insights. RADCOM Service Assurance also utilizes advanced cutting-edge technology such as AI and Machine Learning to provide operators with smart, proactive monitoring for automatic anomaly detection in IoT and insights into encrypted traffic.

RADCOM's next-generation solution

Delivering a next-generation customer experience that optimizes customer interactions to provide a best in class, personalized experience means understanding the customer in real-time and gathering a broad range of streaming data to make decisions in real-time. To do this, an operator needs the ability to analyze streaming data at a massive scale while utilizing built-in machine learning to detect anomalies automatically. Enhancing the customer experience and optimizing network performance in real-time for high-quality 5G services.

RADCOM's next-generation service assurance solution is designed to provide operators with real-time insights for the transition to 5G. Evolving from a virtual probe-based service assurance solution where all the Virtual Network Function Components (VNFCs) are hosted in Virtual Machines (VMs), RADCOM's next-generation solution unifies all its VM hosted functions (backend and frontend) into a single node, hosted in a container and deployed as close as possible to the source of the monitored traffic.

RADCOM Service Assurance is built to process large volumes of streaming data at lightning speed with very low-latency and perform batch analytics, all using RADCOM's dynamic, modular, stream-based microservices architecture. RADCOM's solution can analyze billions of network events per day from multiple types of data feeds highly efficiently and converts the data into smart, actionable network intelligence presented in RADCOM Network Insights.

RADCOM Service Assurance is empowered by patented technology – I.C.O.N – to deliver **I**ntelligent, **C**ontainer-based, **O**n-demand, **N**etwork Analysis from the RAN to the Core.

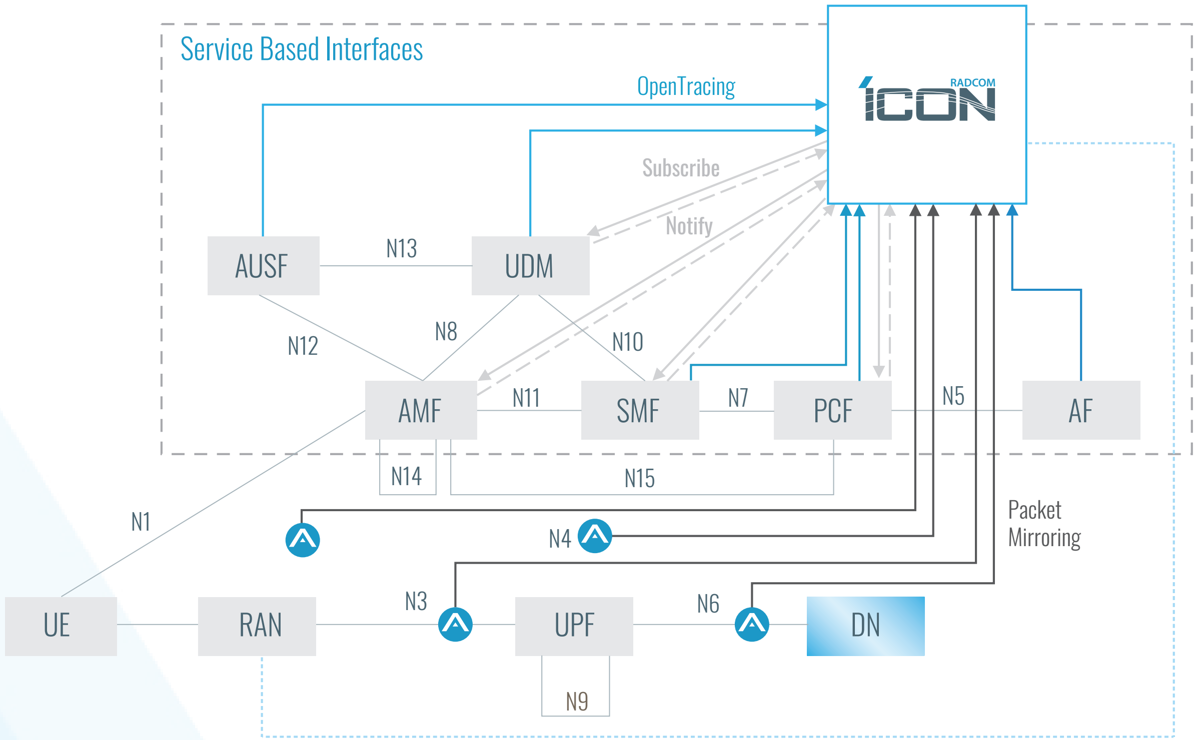


Figure 6 - RADCOM I.C.O.N correlates multiple data sources for end-to-end 5G assurance from the RAN to the core

4.1 Intelligent

Designed to provide complete network and service visibility for 5G covering the RAN to the core, RADCOM's I.C.O.N technology intelligently consolidates the capture, processing, indexing, correlation, and storage of multiple data feeds such as OpenTracing, generic Events, Protobuf, Performance Management, Fault Management, Radio Events, Alarms, CSV, JSON, PCAP, Counters, and legacy probes (typically packet-based) all on the same containerized node. Significantly decreasing the amount of network data that operators need to collect, process and store RADCOM's I.C.O.N technology enables operators to understand the 360° customer experience and troubleshoot network performance from a high to granular level (individual subscriber or packet) while reducing storage costs and cloud resource utilization to the minimum.

Once data is captured, RADCOM's I.C.O.N technology streams the data through various interchangeable modules that process (convert the data to a different structure or convert unformatted data to a formatted output), filter, run calculations (such as correlation or machine learning) and output the data. Stored data is in a searchable format, using patented indexing that creates primary indexes with pointers to the raw packets. Data can also be sent out to data streaming solutions (like Kafka) in mid-stream, and then the enriched data sent back to RADCOM's solution and subsequently processed and transmitted to RADCOM Network Insights. RADCOM's solution correlates user sessions by maintaining user identifiers (such as IMSI, MSISDN, IMEI, and more) in a stateless database.

With indexes including pointers to the raw network packets, RADCOM's I.C.O.N technology enables operators to run on-demand queries at blistering speed and work on streamed data while making calculations on the fly or run in batch mode to produce historical reports. Operators can execute session and protocol analysis, and if the query extends beyond the data included in the primary indexes, RADCOM's I.C.O.N technology intelligently combines indexed data with information extracted from the raw packet data to provide PCAP traces on the fly. Operators can also run advanced analytics by defining several types of "correlation" or "session" types for different users and different use cases. For example, a network element can have a session compiled from different protocols describing a specific network activity.

4.2 Container-based

Being fully containerized, RADCOM's solution is stateless, has a low footprint and consumes minimal resources, is easy to deploy on-demand, scalable, and offers high performance. Placing the data acquisition and processing right next to the VNF and designed to work side-by-side and spun up with the VNF. RADCOM's I.C.O.N technology comes with an input API (to capture the data), streaming, storage, querying capabilities – all in one containerized solution. Deployed on the same host as the monitored network element, RADCOM's solution receives the raw data (packets) and metadata directly from the VNF. A sidecar deployment provides optimal load balancing, and the data integrity is agnostic to any network changes, as RADCOM's solution is an "organic" part of the operator's network.

Benefiting from store state functionality, RADCOM's solution delivers high availability and reliability, recovering state in midstream so that data analysis is constant and network issues detected in real-time. RADCOM's solution also uses a distributed architecture so an operator can set-up a RADCOM Service Assurance cluster that handles traffic filtering, another that controls traffic aggregation. Each cluster being small, highly cloud efficient, and providing end-to-end coverage. RADCOM's solution offers high reliability, high availability, and ease of use for streaming and batch data analysis, all critical for 5G.

4.3 On-demand

Due to its stateless nature, self-contained operation, as well as integration into the operators' NFV orchestration, RADCOM's I.C.O.N technology enables the solution to be launched on-demand to investigate network issues on the fly. If service degradation is detected, the operator can spin up to perform in-depth, on-demand analysis, root-cause problems that affect the customer experience, and enable the operator to optimize network performance. Once service quality is restored, the operator can spin down the solution to free up valuable cloud resources and continue performing smart sampling on a percentage of the traffic.

> "Operators should take an on-demand approach to service assurance and network visibility, using smart sampling and filtering on specific datasets. They can then decide, on the fly, on which areas of the network they want to perform in-depth analysis, zooming in on high priority issues or selected customer groups."

James Crawshaw, Senior Analyst, Heavy Reading

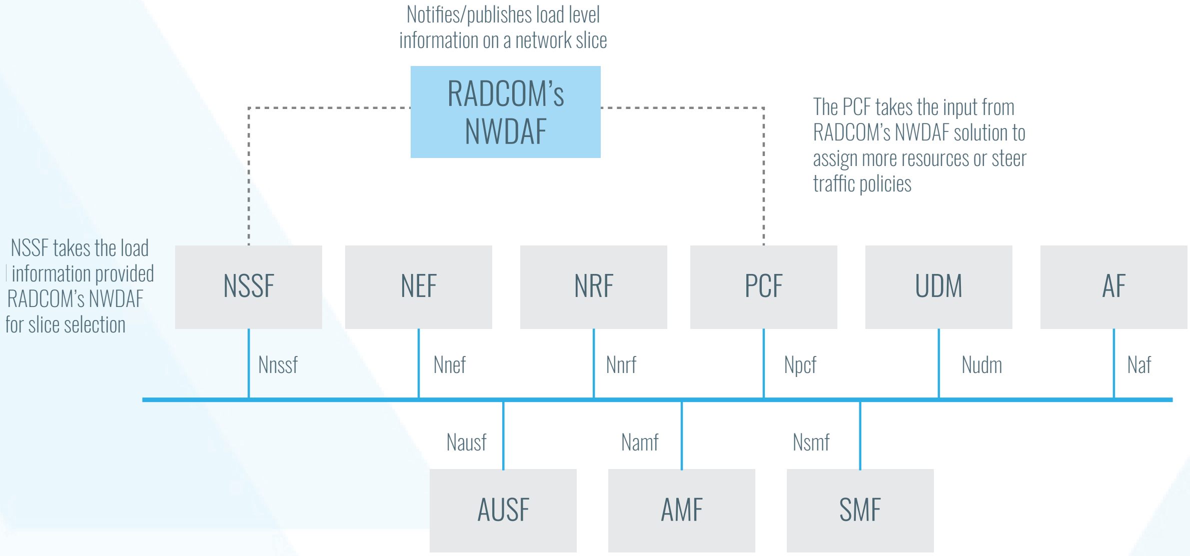
4.4 Network Analysis

From the RAN to the network core, RADCOM's I.C.O.N technology smartly correlates multiple data feeds to provide operators network analysis to improve the customer experience and optimize the network performance. For blind spots in the operator's network visibility, RADCOM leverages AI and Machine Learning to enable automatic anomaly detection and insights into encrypted traffic. The combination of intelligent correlation of multiple data feeds, and AI provides smart insights for comprehensive network intelligence and closed-loop service assurance.

Processed data can be used for operators to understand the customer experience, troubleshoot network performance, and stream processing can be used to transform and enrich this data. The enriched stream data is then pushed back to the message transport system to make the data available for analytics by multiple consumers within the operators' organization, such as network engineers and data scientists. Stream data can also be part of a real-time dashboard used for SOC and CEM. RADCOM's I.C.O.N technology is comprised of interchangeable microservices that can be easily updated or swapped out. This architecture is machine learning-friendly and enables new and updated ML models to be added to the solution seamlessly. So, for example, RADCOM's solution can create a self-learning mechanism that optimizes smart traffic sampling so that data capture and storage are reduced to the minimum while ensuring the sampled traffic represents the complete customer experience, including subscriber trends and behavior. RADCOM's solution provides operators with a more intelligent, more efficient, and much more flexible way of processing and analyzing all the data feeds needed to understand service quality and assure the customer experience in 5G.

4.5 RADCOM's NWDAF solution

At the heart of RADCOM's NWDAF solution is RADCOM's next-generation technology for 5G assurance - RADCOM I.C.O.N - which captures the data and events from the 5G core network functions and creates the load KPI's that are provided to the PCF and NSSF. Enhancing the 5G core with the ability to collect and analyze aggregated data per slice and to aid network optimization via interaction with the PCF and NSSF. The PCF can take the input from RADCOM's NWDAF solution to assign more resources or steer traffic policies, which will help operators run their network slices more dynamically. While the NSSF can take the load level information provided by RADCOM's NWDAF for slice selection.



RADCOM NWDAF supported services:

- N23 interface: a reference point between PCF (Policy Control Function) and the NWDAF
- N24 interface: a reference point between NSSF (Network Slice Selection Function) and the NWDAF
- Nnwdaf_EventsSubscription which enables the NF service consumers to subscribe/unsubscribe for network slice specific congestion events notification from the NWDAF
- Nnwdaf_AnalyticsInfo which allows the NF to service consumers to request and acquire analytics from the NWDAF

As the NWDAF continues to be defined by the 3GPP and evolves, it is expected that additional information will be provided from the NWDAF to network control functions responsible for handling the mobility of active and idle UEs. Moreover, it is expected that the output of NWDAF will also feed new network functions related to Access Traffic Steering, Switching, and Splitting schemes (ATSSS). This framework is currently under investigation by the 3GPP as traffic steering of user sessions through multiple RATs is of paramount importance for 5G networks.

The three primary operations supported by the ATSSS are:

- Access Traffic Steering: The procedure that selects an access network for new data flow and transfers the traffic of this data flow over the selected access network. For example, traffic steering of user sessions through multiple Radio Access Technologies (RATs) for dynamic RAT selection to better satisfy the service and subscriber needs. This function can be provided based on location analytics, congestion analytics, etc.
- Access Traffic Switching: The procedure that moves all traffic of ongoing data flows from one access network to another in a way that maintains the continuity of the data flow.
- Access Traffic Splitting: The procedure that splits the traffic of data flow across multiple access networks. When traffic splitting, to a data flow, some traffic of the data flow is transferred via one access, and some other traffic of the same data flow is transferred via another access system.

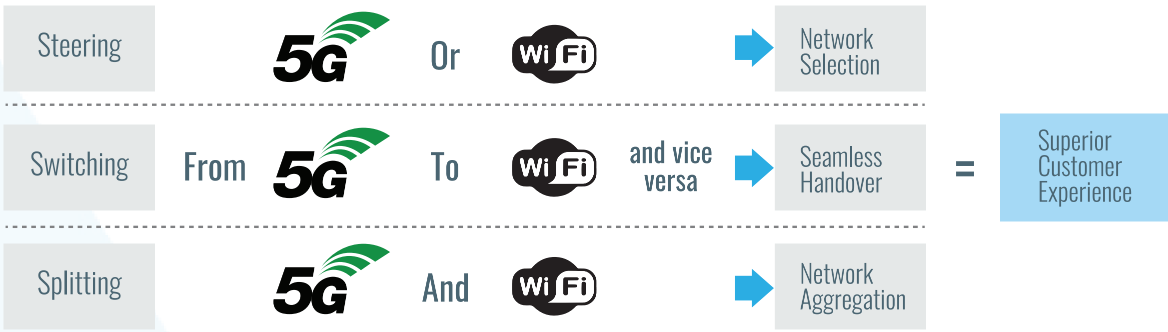


Figure 7 - ATSSS capabilities and the benefits to subscribers

RADCOM's solution for NWDAF is highly agile and customizable, fitting both the operators' needs as their 5G core functions are implemented and as the NWDAF function evolves. Powered by RADCOM's next-generation technology - RADCOM I.C.O.N - RADCOM's NWDAF takes data from multiple sources in the network (such as JSON, AVRO, Protobuf, raw packets, PCAP) and outputs the analytics in numerous formats (such as Kafka, TCP, REST, file, email) and is flexible in exposing its services to other network functions and which functions should benefit from them.

RADCOM's NWDAF provides operators with the ability to capture data from both non-SBI interfaces (N1, N2, N3, N4, N6, N9) and SBI interfaces (N5, N7, N8, N10, N11, N12, N13, N14, N15) so that as 5G services roll out, RADCOM's NWDAF ensures a smooth transition to the new core architecture; delivering a central point for network analytics.

Other use cases for the NWDAF that have been studied by 3GPP are:

- 5G edge computing whereby the NWDAF can be used to influence SMF routing decisions
- Determining areas with fluctuating network conditions

  By correlating and analyzing information coming from the network functions with data from the application functions (like MOS), RADCOM's NWDAF can provide statistical information that enables operators to change network deployment and configuration to improve E2E QoS. Examples of improvements that can be triggered are:

- RADCOM's NWDAF will correlate service data with data provided by the NFs to find out why the service experience is low.
- The AF can be informed when a UE is approaching a potentially overloaded area so that the AF can know that there is a higher chance of service fluctuation in these network conditions.

In 5G services like URLLC and Vehicle to Everything (V2X) will require network-wide analysis to both validate and improve NF deployment and configuration. Operators will also be able to monitor network slices (for example, performance requirements for groups of UEs associated with a type of service). The NWDAF will help operators determine areas of fluctuations in the network conditions and ensure service levels match expectations.

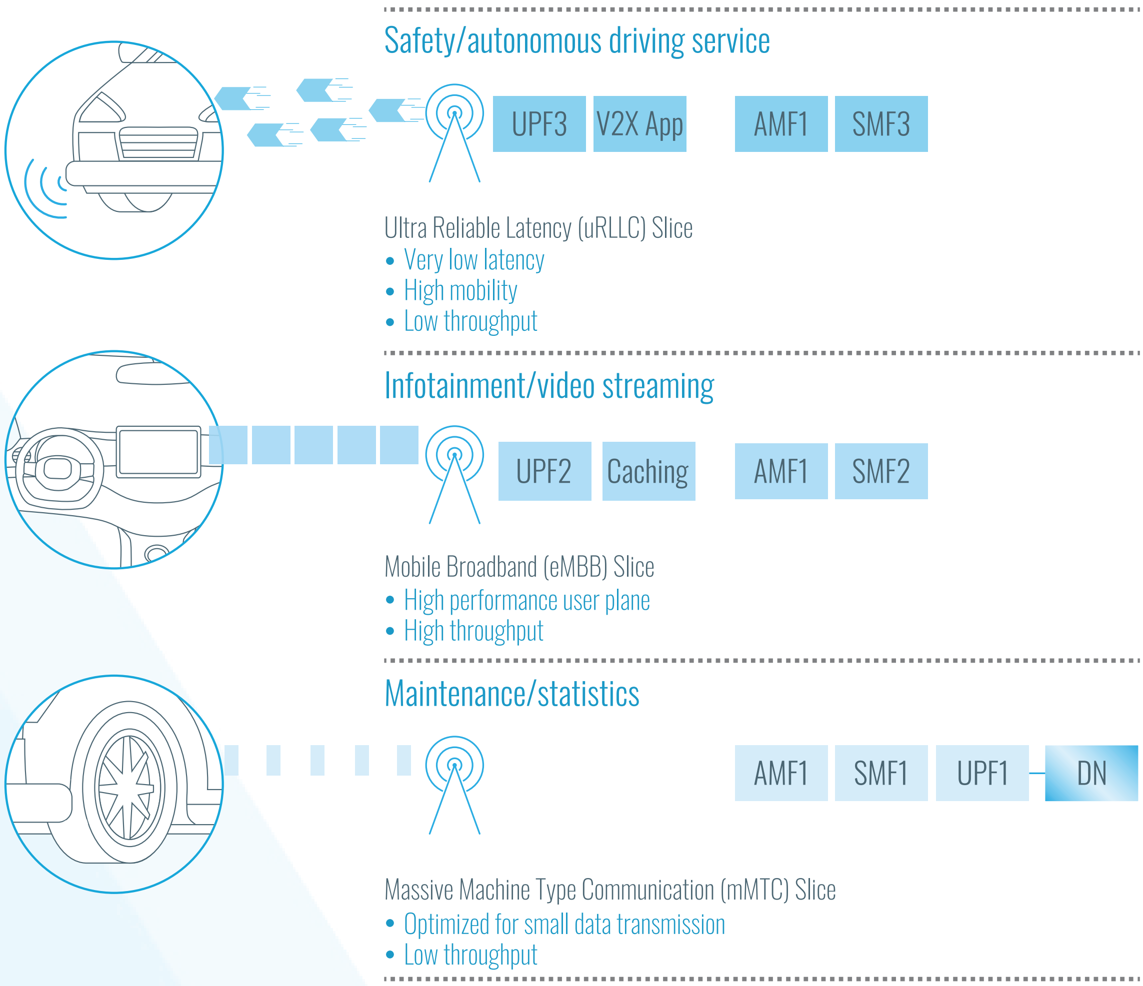


Figure 8 - Ensuring network slice performance for V2X

- Load (re-)balancing of NFs
- Management of Massive IoT (MIoT) infrastructure by utilizing both the NWDAF and NSSF. The NWDAF can provide the expected UE behavioral information to the UDM to help supervise MIoT terminals.
- Policy determination
- Prevention of security attacks/anti-fraud
- QoS adjustment and provisioning

  QoS control in 4G only covers the RAN and core network, and the data related to QoS is compartmentalized inside each network domain, which limits the ability to analyze the data together. For 5G, the goal is for E2E QoS (e.g., RAN, backhaul, core network, network to interconnect) to achieve the necessary 5G user experience. The NWDAF is used to collect and analyze information from different sources (UE, AN, CN, etc.) and provide the E2E QoS hub. QoS parameters can include standard 5G QoS indicators (5QI) and on-standardized 5QI, such as packet error rate, default priority level, and packet delay budget (defined in milliseconds).
- Slice SLA assurance or predictable network performance

3GPP defines basic network slice types such as eMBB, mMTC, and URLLC, where each network slice is designed for a group of services sharing comparable service requirements. However, some applications and services will require multiple service flows. These service flows can be implemented by using QoS flows (defined in 3GPP TS 23.501[12]), different PDU sessions, or even different network slices. For instance, in remote driving use cases, HD video requires high throughput, which is supported via the eMBB slice. However, the in-vehicle sensor data and vehicle control signaling require low latency and high reliability, which is supported by the URLLC slice. When a subscriber requests a service, the 5G network automatically assigns an identifier: 5QI (5G QoS Identifier) for each service with the required QoS (Quality of Service) and changes the technical parameters of the network to fulfill the requirements of each assigned 5QI. Monitoring these QoS flows will be an essential part of SLA assurance for network slices.

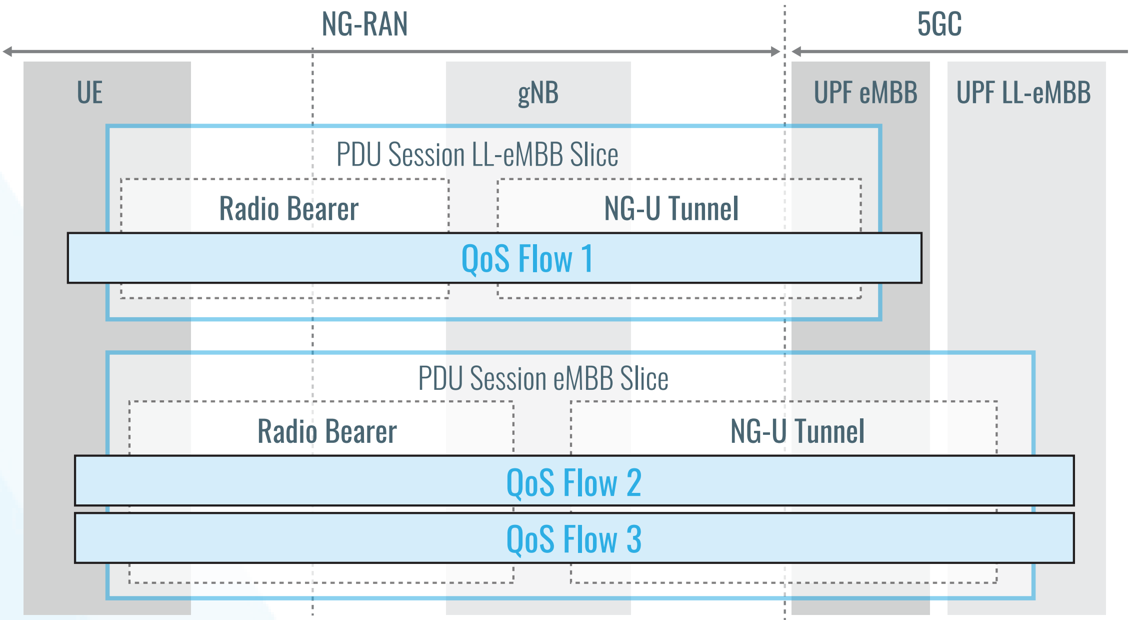


Figure 9 - QoS flows in different network slices

- UE driven analytics

  UE-driven analytics is a relatively new proposal for enhancing the data collected by the NWDAF and other NFs. UEs are useful data collection points to gather more localized analytics within the network. For example, positioning information (from the vast array of device sensors) or user profiling info (for example, when a subscriber moves from different environments such as outdoors to indoors or from a car to walking). Such information could assist the NWDAF in making more intelligent decisions on slice selection (for example, switching from a slice with more flexible resources to a resilient one, etc.).

  Long-term, UE driven analytics could include the prediction of the UE context/behavior to enable the network to better provision resources. For example, the mobility of a group of users can be used for handover management, or the prediction of interference that the UE will suffer from/cause in a particular area.

Utilizing RADCOM's NWDAF solution requires RADCOM to understand from the operator more about their 5G core, their custom use cases, which NEPs are partnering with the operator, and requires integration between RADCOM's NWDAF and the operators' network. As RADCOM's NWDAF reuses similar service exposure mechanisms as other 5G NFs for data collection and analytics exposure (including the subscription model and request/response model), these data structures will need to be maintained as the operator rolls out their 5G core. RADCOM's next-generation solution inherent flexibility enables operators to decide what data sources they want to incorporate into their NWDAF. RADCOM's experts will provide guidance to operators, but from whatever sources the operators choose, RADCOM will take the data, use it to calculate KPIs and KQIs, and provide the analytics to ensure a smooth transition to 5G.

4.6 From next-generation packet analysis and call tracing to end-to-end SOC

Even more so now than ever before, ensuring a high-quality customer experience will require an independent auditor to correlate all the data, extract smart insights, pinpoint where there are customer-affecting service degradations, and troubleshoot the network performance. Operators need next-generation, container-based solutions that provide them with both low-level tools such as call tracing and packet analysis to perform network troubleshooting for the new underlying network architectures. Also, operators need to understand the overall customer experience and end-to-end service performance with the ability to drill down to the lower level to perform root cause analysis.

SOC and CEM solutions are crucial to helping operators deliver a high-quality customer experience in 5G and move from being reactive to proactive when handling service degradations. Bringing the customer experience into the center of focus and enabling the operator to make customer-led decisions on top of engineering-led choices. As 5G continues rolling out, this will be even more critical when operators offer network slices per segment or use case. Without a single, end-to-end solution that spans both the network and service layer to monitor activity on a "per slice" basis, operators will find themselves blind to what is happening across their network.

> "SOC acts as a linchpin between the business-facing side of an operator (customer care, sales, and marketing) and the operational side (network planning, optimization, and engineering)."

James Crawshaw, Senior Analyst, Heavy Reading

For a comprehensive SOC solution, RADCOM Network Insights is correlated with BSS and OSS data that enables operators to monitor the overall service quality intelligently and rectify service degradations and service outages that impact subscribers. For an end-to-end CEM solution, RADCOM Network Insights is correlated with BSS and OSS data to generate a Customer Experience Index (CEI), so operators can smartly monitor the entire customer experience journey with easy access to end-to-end troubleshooting, trend analysis as well as churn and Net Promoter Score (NPS) prediction.

Service assurance must work in conjunction with orchestration systems to dynamically monitor the 5G network and leverage machine learning and artificial intelligence (ML/AI)-based predictive assurance to guarantee the SLAs and QoS delivered. Utilizing ML and AI will be critical to performing closed-loop automation based on the insights generated from monitoring 5G services.

With virtualization opening the network to even more complexity, it will be down to an independent auditor to ensure continuous and consistent network performance. RADCOM is already working closely with its customers to ensure a smooth transition to 5G with RADCOM Network Intelligence assuring that the technology transformations under the surface are transparent to the customer, and whatever migration path the operator chooses and whatever use cases are deployed the end-to-end services are optimized, and the customer experience remains high throughout the transition.

From the first use cases up to the most advanced, RADCOM Network Intelligence is designed to efficiently correlate the network data so that operators can understand the customer experience and troubleshoot network performance from the RAN to the core while using a stateless architecture that seamlessly integrates within an operators' cloud environment.

5. Ensuring initial 5G service quality

5.1 Enhanced Mobile Broadband (eMBB)

In the initial phase of 5G, operators will use the technology to provide their customers with Enhanced Mobile Broadband (eMBB). As a proven business case, it is the priority use case for 5G deployments offering early 5G adopters enhanced data speeds and higher quality user experience with its superior radio. It provides tangible revenue streams and will enable the operator to differentiate themselves from competitors.

These faster data rates and the improved connectivity will also enable telecom operators to offer mobile services to provide last-mile connectivity. By using 5G, these services can potentially eclipse the quality and speed customers currently experience from fixed broadband technologies, which are why one of the first use cases that operators are rolling out is Fixed Wireless Access (FWA) as an alternative to fixed wireless connectivity. Both speed and costs are in play with some estimates stating that 5G-based FWA can reduce the initial cost of establishing last-mile connectivity by 40% (vs. FTTP).

5.2 Fixed Wireless Access (FWA)

Fixed Wireless Access (FWA) will be deployed by both fixed operators (such as cable operators) to speed up broadband rollouts and mobile operators as an opportunity to tap into the multi-play market segment, including a new route into the home broadband and video market. FWA has already been launched by multiple operators across the globe. In the UK, both Vodafone[13] and Three[14] have launched FWA services. While in the US, Verizon[15] (using proprietary standards rather than 3GPP specs) began rolling out services in 2018, and other US operators have followed. While in February 2019, Optus and Nokia claimed the world's first live 5G fixed-wireless access network based on 3GPP standards, and in June 2019, Globe Telecom launched services in the Philippines.

5G opens new opportunities for operators as they move into new market segments. FWA enables operators to provide broadband services to both consumers and businesses households in locations where there is no fixed telecom infrastructure and where it would be too costly or take too much time to deploy. According to the GSMA, FWA[16] reduces the cost to connect households to broadband (per bit) by 74% compared to wireline connections. With FWA, residential gateways connect to the mobile operators' network to provide reliable broadband connectivity into the home. As 5G advances, FWA will enable operators to deliver more data-intensive services at the fiber-like speeds for both business and consumer use cases, such as immersive gaming, telepresence, and AR/VR applications.

FWA started in 4G with around 100 mobile operators worldwide offering this service. However, 5G will significantly boost the service and even overtake fixed broadband speed and performance. For example, Optus said that their 5G Home Broadband would include unlimited data at superfast speeds with a 50Mbps Satisfaction Guarantee[17].

5.3 Multi-access Edge Computing (MEC)

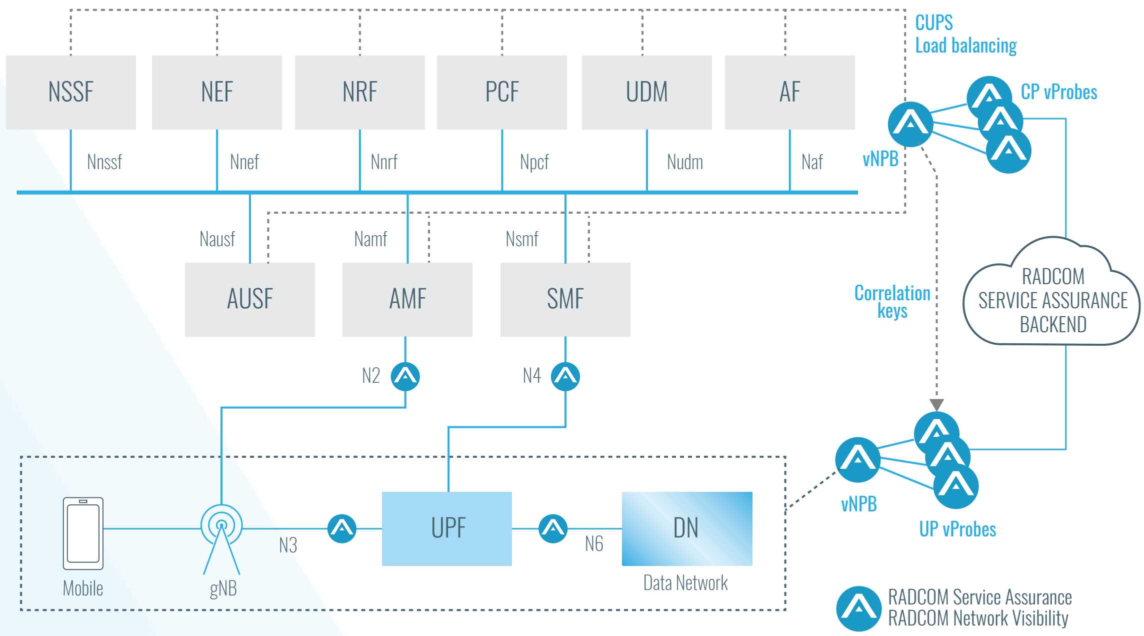
Multi-access Edge Computing (MEC), formerly known as Mobile Edge Computing, enables cloud computing capabilities and an IT service environment at the edge of the cellular network. The premise behind MEC is that by running applications and performing high-intensity processing tasks closer to the device (and end-user), network congestion is reduced, and applications perform better.

The technology is designed to be implemented at the cellular base stations and is already enabling flexible and rapid deployment of new applications and services for customers. By deploying services and content at the network edge, mobile core networks are alleviated from further congestion and can efficiently serve customers.

Some MEC use cases that operators are already deploying:

- High-speed video services
- Location-based services
- Internet-of-Things (IoT)
- AR/VR
- Optimized local content distribution

RADCOM is working with customers on monitoring MEC services and already offers SBA readiness that supports the complex CUPS correlation needed to monitor edge traffic efficiently. RADCOM's solution assures services at the edge using RADCOM's I.C.O.N technology, which is container-based and lightweight, maximizing insights while being resource-efficient.



Both RADCOM Network Visibility (with ingress load balancing) and RADCOM Service Assurance combine on the edge to provide a flexible solution that can be rapidly scaled via integration with NFV MANO and is cost-effective. As the network edge will support multiple service types (and associated VNFs), resources will be dynamically managed, this integration into the operators' NFV MANO is critical. Similarly, if a new service is deployed, monitoring and visibility can be launched automatically.

6. Summary

The wide range of 5G services is vital to the long-term economic health of the telecommunications industry and will boost many other vertical industries. With the service-based architecture offering additional capabilities that enable operators to accelerate the deployment of flexible, dynamic services.

However, the sheer scale of traffic in a 5G world will overwhelm human understanding and the ability of operators to make optimal network policy decisions manually. A combination of automation and human intervention is required to take the 5G service vision into reality, which is dependent on a containerized approach to service assurance that fully integrates into a telecom operators' cloud. The ability to assure these diverse service types on a cloud-based, containerized platform is fundamental to the success of these services. 5G introduces many new interfaces, protocols, and technologies into the cloud core and dynamic, cloud-native service assurance will be used to support automated, closed-loop service optimization that will enable operators to meet SLAs across these multiple service types as well as deliver end-to-end services that meet a unified network policy.

RADCOM's solution brings service assurance into the 5G era by combining the functionality of a virtual probe (with all the sophisticated back-end processing capabilities) into one containerized, self-contained component/framework. Together these significantly improve the utilization of NFVI resources, taking inputs from many different sources, storing data in an open (non-proprietary) way, for easy integration into BSS/OSS systems. This will encourage collaboration between teams while providing on-demand analysis that can be spun up on the fly to troubleshoot, and then spun down to release valuable cloud resources. All this while significantly reducing the amount of data they store, and enabling, rapid, in-depth troubleshooting of high priority, customer-affecting service degradations.

RADCOM is designed to ensure a smooth transition to 5G. With RADCOM Network Intelligence, operators can assure that the technology transformations under the surface are transparent to the customer, and whatever use cases deployed, the end-to-end services are optimized efficiently, and the customer experience remains high throughout the transition.

For more information on how to MAXIMize your 5G services today, visit www.radcom.com.

7. Abbreviations

Term	Description
5G NR	5G New Radio
5GC	5G core network
5QI	5G QoS Identifier
AF	Application Function
AMF	Access and Mobility Management Function
AN	Application Network
API	Application Programming Interface
ATSSS	Access Traffic Steering, Switching and Splitting schemes
AUSF	Authentication Server Function
BBU	Baseband unit
BSS	Business Support Systems
CEI	Customer Experience Index
CEM	Customer Experience Management
CN	Core Network
CPRI	Common Public Radio Interface
cRAN	Cloud-RAN or Centralized-RAN
CU	Centralized Unit
CUPS	Control and User Plane Separation
DC	Dual connectivity
DU	Distributed Unit
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core (4G)
FWA	Fixed Wireless Access
HPLMN	Home Public Land Mobile Network
MEC	Multi-access Edge Computing
MIoT	Massive Internet of Things
NEF	Network Exposure Function
NEP	Network Equipment Providers
NRF	Network Repository Function
NPS	Net Promoter Score

NSA	Non-standalone
NSSF	Network Slice Selection Function
NWDAF	Network Data Analytics Function
OSS	Operations Support Systems
PCF	Policy Control Function
PDU	Protocol Data Unit
RAN	Radio Access Network
RAT	Radio Access Technology (Bluetooth, Wi-Fi, as well as 2G, 3G, 4G or 5G NR)
RCAF	RAN Congestion Awareness Function
RRH	Radio head unit
SA	Standalone
SBA	Service-based Architecture
SBI	Service-based Interface
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
SOC	Service Operations Center
TLS	Transport Layer Security
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
uRLLC	Ultra Reliable Low Latency Communications
V2X	Vehicle to everything
vRAN	Virtualized RAN

8. References

1 GSA Report | May 2019 | Evolution from LTE to 5G - Global Market Status

2 Ericsson Mobility Report | November 2019

3 The Transport Layer Security (TLS) Protocol Version 1.3 -
https://tools.ietf.org/html/rfc8446

4 The OAuth 2.0 Authorization Framework -
https://tools.ietf.org/html/rfc6749

5 FierceWireless - This is why the wireless industry is running from cRAN to vRAN
https://www.fiercewireless.com/tech/editor-s-corner-why-wireless-industry-running-from-cran-to-vran-to-oran

6 China 'Mega City' Hosts 4G/5G cRAN Test Network
https://www.sdxcentral.com/articles/news/china-mega-city-hosts-4g-5g-cran-test-network/2019/03/

7 Rakuten Mobile and NEC to Build Open vRAN Architecture in Japan
https://global.rakuten.com/corp/news/press/2019/0605_01.html

8 A giant leap for 5G Cloud RAN
https://www.nokia.com/blog/giant-leap-5g-cloud-ran/

9 3GPP TSG #80 Plenary Meeting has approved the completion of the standalone (SA) Release 15, 5G specifications
http://www.3gpp.org/news-events/3gpp-news/1965-rel-15_news

10 Connected Consumer Survey 2018: mobile customer satisfaction in Europe and the USA
https://www.analysysmason.com/Research/Content/Reports/Mobile-satisfaction-Europe-USA-RDMMO

11 Policy and Charging Control Framework for the 5G System; Stage 2
https://www.etsi.org/deliver/etsi_ts/123500_123599/123503/15.02.00_60/ts_123503v150200p.pdf

12 System architecture for the 5G System (5GS)
https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf

13 Vodafone Unlimited and Vodafone Together
https://mediacentre.vodafone.co.uk/news/5g-unlimited-and-vodafone-together/

14 Three enters the 5G fracas with FWA offering
http://telecoms.com/497826/three-enters-the-5g-fracas-with-fwa-offering/

15 5G becomes real as Verizon launches FWA offering in four cities
http://telecoms.com/492549/5g-becomes-real-as-verizon-launches-fwa-offering-in-four-cities/

16 GSMA, "Fixed Wireless Access: Economic Potential and Best Practices," 2018
https://www.gsma.com/futurenetworks/5g/fixed-wireless-access-economic-potential-and-best-practices/

17 Optus announces plans for 1,200 5G sites in the first wave, $70 per month unlimited 5G broadband plans
https://www.optus.com.au/about/media-centre/media-releases/2019/01/Optus-5G-Whiz