RADCOMize your NETWORK

ENABLING A SMOOTH TRANSITION TO 5G

RADCOM Network Intelligence

© 2018 RADCOM Ltd. ALL RIGHTS RESERVED.

This document and any and all content or material contained herein, including text, graphics, images and logos, are either exclusively owned by RADCOM Ltd., its subsidiaries and/or affiliates ("RADCOM") or are subject to rights of use granted to RADCOM, are protected by national and/or international copyright laws and may be used by the recipient solely for its own internal review. Any other use, including the reproduction, incorporation, modifcation, distribution, transmission, republication, creation of a derivative work or display of this document and/or the content or material contained herein, is strictly prohibited without the express prior written authorization of RADCOM.

The information, content or material herein is provided "AS IS", is designated confdential and is subject to all restrictions in any law regarding such matters, and the relevant confidentiality and non-disclosure clauses or agreements issued prior to and/or after the disclosure. All the information in this document is to be safeguarded and all steps must be taken to prevent it from being disclosed to any person or entity other than the direct entity that received it directly from RADCOM.

The text and drawings herein are for the purpose of illustration and reference only.

RADCOM reserves the right to periodically change information that is contained in this document; however, RADCOM makes no commitment to provide any such changes, updates, enhancements or other additions to this document to you in a timely manner or at all.

Publication Date: August 2018

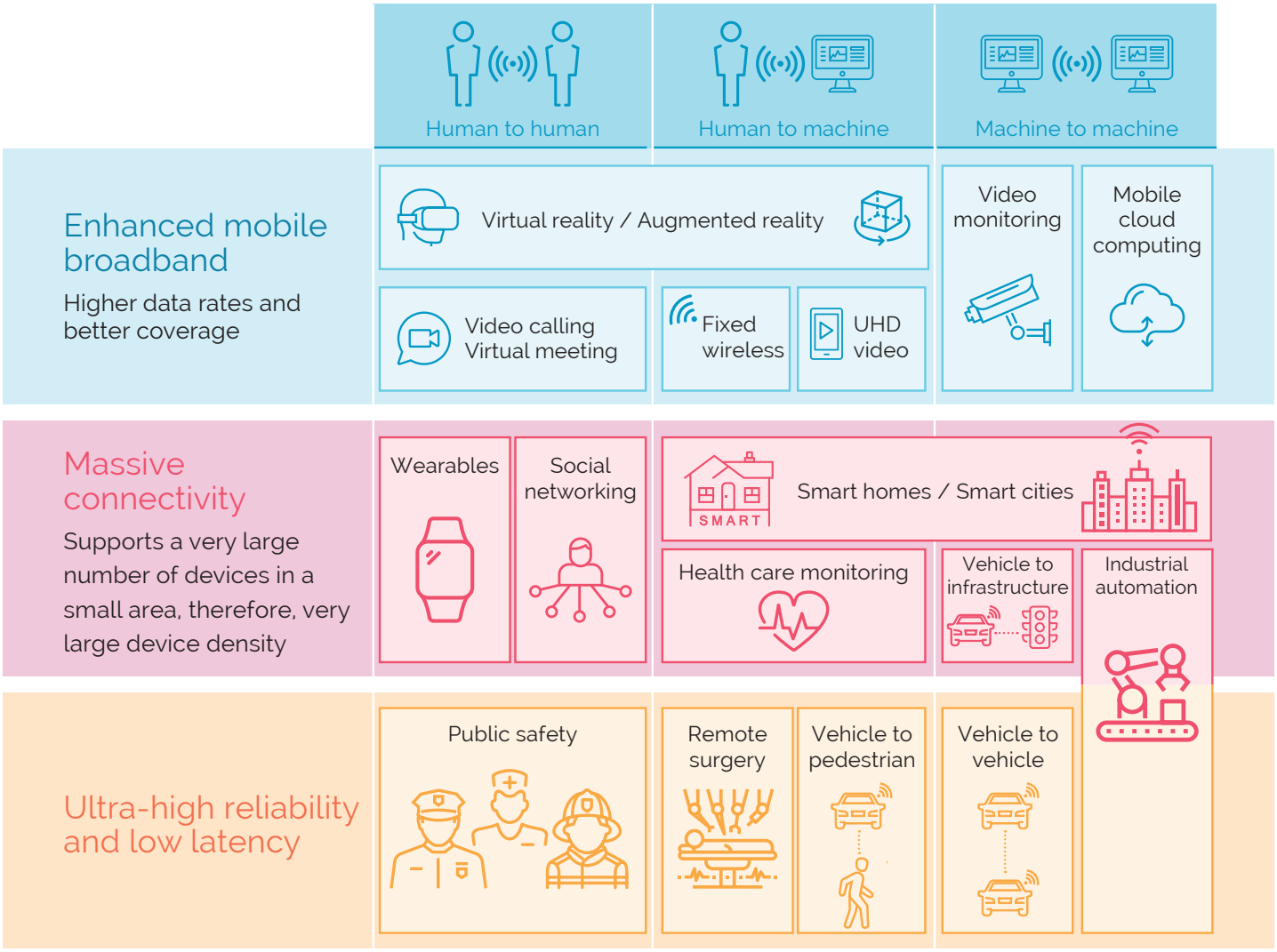
Web Site:
http://www.radcom.com

Table of Contents

Introduction

Previous generations of mobile networks were purpose-built for delivering communications services such as voice and messaging (e.g., 2G) or mobile broadband (e.g., 4G), 5G is much more than just the next iteration of mobile networks. In the initial stages, 5G will deliver enhanced mobile broadband (eMBB) with higher data speeds (20x that of 4G) and better coverage. However, over time, 5G will open the door to new use cases such as autonomous cars, telehealth services and remote operation of machinery that will depend on an ultra-high reliable and low latency (10x that of 4G) network that will revolutionize our lives and how we communicate. Think of Neo and the Matrix. As well as an always-connected world 5G will also support large-scale connectivity, with Massive IoT (MIoT) connecting tens of billions of devices, objects, and machines even in the most remote locations to the network. By 2023, the number of connected devices is forecast to grow from 17.5 billion to 31.4 billion.

Up until recently, 5G remained a vision and a technology that was being vigorously tested by operators and vendors alike even though the specifications were not finalized.



That was until June 2018[1] when the Standalone 5G NR radio specifications (known as option #2 in the 3GPP 5G deployment models) for a new network that will operate in tandem with an LTE network were ratified by 3GPP which represents a significant milestone on the road to 5G. This follows the release of the 5G NR specifications for non-standalone (NSA) operation in December 2017 (that will use the LTE radio access and the core network; known as option #3). Now, standards are endorsed the telecom industry is taking the final sprint towards commercializing 5G. Elisa just claimed the launch of the first 5G network[2] with services available in Tallinn city center in Estonia while some Middle East countries (Kuwait, Qatar, Saudi Arabia and the United Arab Emirates) have also turned on limited 5G services. By the end of 2018, ten 5G launches are expected[3] including AT&T Mobility and Verizon Wireless as well as some operators in Bahrain, Estonia, Finland, Italy, Qatar, San Marino, Sweden, and Switzerland. The rest of the operators will follow in 2019 (at least seventeen are expected) and beyond.

However, while 3GPP is defining both a new 5G core network (5GC) as well as a new radio access technology (NR), it is possible to integrate elements of different generations in a different configuration with 5G: SA (standalone) and NSA (non-standalone). An SA scenario uses only one radio access technology (5G NR or the evolved LTE (Long Term Evolution) radio cells), and the core networks are operated alone. NSA scenario combines NR radio cells and LTE radio cells using dual-connectivity to provide radio access and the core network may be either EPC (Evolved Packet Core) or 5GC.

In the end each operator will decide on their own migration paths from LTE (option #1) to 5G depending on their own needs, whether they have the required spectrum to provide widespread coverage of NR in standalone mode and whether they are interested in upgrading their current LTE RAN infrastructure to connect to the next generation core. Some of the likely paths that operators will take in their journey to 5G are:

1. EPS (Evolved Packet System) to SA Option #2
2. EPS to NSA Option #3
3. NSA Option #3 to NSA Option #7 and SA Option #5
4. NSA Option #3 to NSA Option #3 and SA Option #2
5. NSA Option #3 to NSA Option #4 and SA Option #2

As in every technology transition operators will be maintaining the balance between moving forward to the next generation network will also utilization their significant investments in their previous network infrastructures. So, in an ideal world, the pathway to 5G would be to choose scenario one (from the list above) in which the operator moves from option #1 to option #2. This scenario would provide full 5G use cases but would mean the operator needs to make sure there is interworking between 4G and 5G networks. Scenario two means limited support for full 5G use cases, but a quick time to market and the ability to leverage the LTE network. RADCOM Network Intelligence already supports option #3, and platform coverage will extend to option #4 and option #7 in the next release.

[1] 3GPP TSG #80 Plenary Meeting has approved the completion of the standalone (SA) Release 15, 5G specifications

[2] Elisa first in the world to launch commercial 5G

[3] Global Progress to 5G - Trials, Deployments and Launches

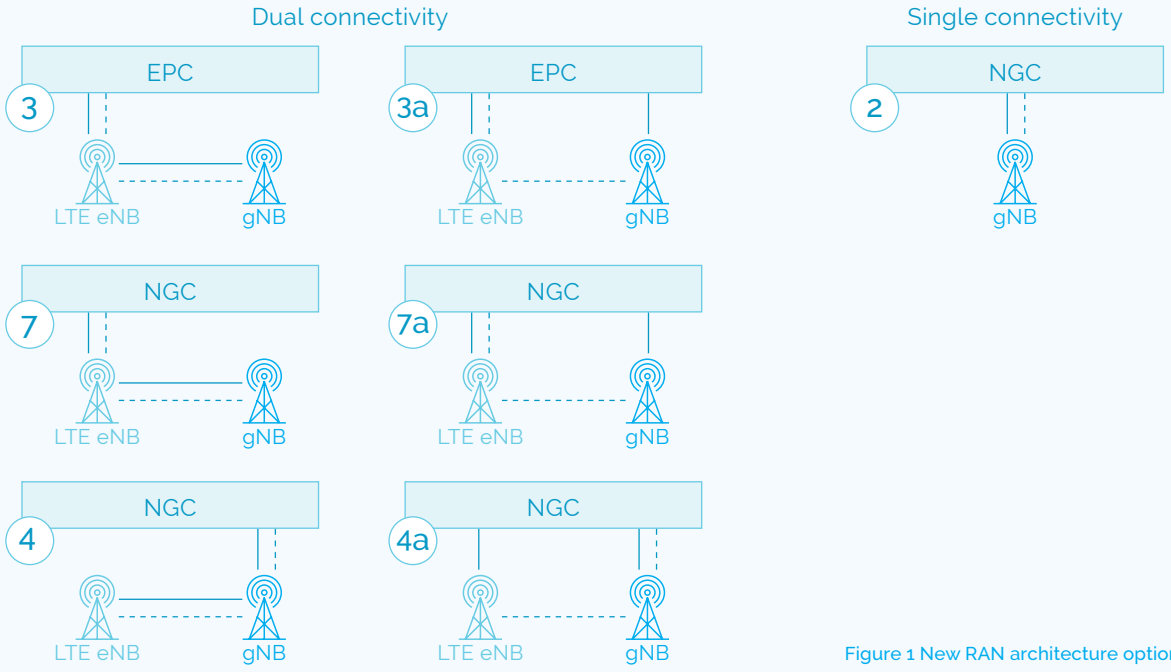


Figure 1 New RAN architecture options by 3GPP

Each 5G deployment scenario has its advantages and disadvantages for the operator. Some of which are covered in the following table:

		Advantages	Disadvantages
Radio Access Network	SA	• Easy to manage • Inter-generation handover between 4G-5G	• Not able to leverage current LTE deployments if NR is used in SA
	NSA	• Leverage current LTE deployments	• Tight interworking between LTE and NR required • May impact end-user experience
Core Network	EPC	• Leverage current EPC deployment	• Cloud support is optional
	5GC	• Cloud-native • Easier to support multiple access	• New deployment required

Table 1 Comparison of 5G radio access and core networks

In initial 5G deployments operators will be focused on utilizing their LTE core, and then transitioning to a new 5G core in the future. However, the new 5G core is required for advanced 5G features, such as end-to-end network slicing in which operators will be able to sell customized slices of their networks and provide different Service Level Agreements (SLAs) for various industrial applications. For example, autonomous vehicles will need a high bandwidth slice for infotainment, and an ultra-reliable slice for telemetry assisted smart driving.

The new 5G core architecture as specified in Release 15 is designed to be cloud-native and use service-based interactions between control-plane functions - known as a Service-Based Architecture (SBA) - and will be deployed on a shared, orchestrated cloud infrastructure.

Enabling 5G with the cloud

The majority of operators are redesigning their network architectures and core functions using cloud-native design principles and IT web-based development and methodologies to gain the necessary platform agility to deliver 5G services. However, to succeed in this journey to the cloud, operators will need to effectively manage the transition from LTE while launching their initial 5G offerings and continuing their network virtualization journey to NFV and then expanding their 5G offerings to deliver full 5G use cases.

Only by implementing a cloud-native service assurance solution will operators be able to manage this journey successfully. With service assurance deployed across their entire network operators will have eyes and ears into their end-to-end network services to ensure the transition is transparent to customers and provide tools to pinpoint and troubleshoot issues as quickly as possible.

Legacy service assurance solutions were designed to monitor physical networks and do not meet the requirements to assure cloud-based networks that will provide the foundation for full 5G use cases. For operators to successfully transform their networks to NFV and 5G, service assurance must be reimagined to:

- Support the levels of operational automation required in these dynamic networks
- The sheer scale and dynamism of 5G means existing hardware-based service assurance are just not practical. In cloud environments, virtual network functions (VNFs) can be created, moved or terminated based on service demands, and so service assurance needs to adapt in real-time to network changes
- Enable feedback loops for NFV Management and Orchestration (MANO)
- Service assurance empowers the management layer with end-to-end service monitoring and feedback functions from across the network. Policy rules fed by the assurance feedback then enables closed-loop automation at each management layer to rectify issues automatically and assure service quality
- Monitor the virtual traffic that travels between the VNFs (East-West traffic)

Physical network probes are incompatible with virtual networks, and so with more and more service functions moving to the cloud, virtual probes need to be deployed to expose the virtual blind spots. Monitoring the virtual network functions (VNFs) will need to be combined with the monitoring of traditional, physical network functions (PNFs) and most critically the transition between them

For 5G to succeed, operators must put in place an integrated nervous system that lives within the network and provides the real-time feedback needed to maintain end-to-end service quality for customers. A cloud-native service assurance solution will be critical in helping operators negotiate this technology transformation successfully and assuring 5G services that will delight customers and revolutionize our lives and how we communicate.

MAXIMize your 5G services with RADCOM Network Intelligence

Service assurance is used to monitor and analyze network data to ensure service levels are achieved and maintained, which is critical for operators to deliver high customer experience. In 5G, there will be many new changes and challenges that will need to be addressed by service assurance to assure service quality. 5G introduces new;

- Interfaces and protocols that means 5G specific N-type reference points
- Network architecture such as Control Plane and User Plane Separation (CUPS) - initiated in 4G - and a Services-based Architecture (SBA)
- New network functions such as those related to network slicing (i.e., NSSF that supports handling multiple slices) and SBA that includes NEF & NRF functions to support services subscription, exposure, and access

All these will drive new service assurance requirements while assuring multiple network slices on different core networks will introduce new correlation changes. RADCOM Network Intelligence is based on an entirely cloud-native architecture and is 5G-ready with the inherent design that provides operators with end-to-end service visibility for the continued transition to NFV, the initial rollout to 5G and for assuring services on the new 5G core.

RADCOM Network Intelligence encapsulates both RADCOM's deep network expertise from over 25 years in the telecom industry while at the same time reimagining service assurance and network visibility for a 5G-ready cloud network. This reimagined offering enables operators a dynamic approach to capturing, processing and analyzing network traffic on scale and on-demand in line with the needs of optimizing and troubleshooting networks in an NFV and 5G era. With an on-demand approach, operators gather statistics from across the network while zooming in and analyzing focused datasets (by specific applications, network elements or subscriber group) to assure the customer experience efficiently.

Integration with NFV MANO

Managing dynamic 5G networks will require closed-loop automation controlled by the management and orchestration (MANO) layer and enabled by the service assurance solution that collects, analyzes, and steams events from across the network to the orchestrator. These events are then streamed to the policy and control loop engine that processes the events and correlates them into specific policies that are then executed by the NFV MANO; making service assurance essential for the real-time management and operation of the 5G network.

Tight integration with NFV MANO requires service assurance and network visibility deployed as a Virtual Network Function (VNF) for full lifecycle management of the solution (instantiation, healing, upgrades, modification, and scaling) because it enables the network to be dynamic and respond to continual changes. RADCOM Network Intelligence is fully integrated with ETSI-compliant NFV Management and Orchestration (NFV MANO). These include Amdocs Network Cloud Service, HPE, Open NFV Partner Program, Huwaei Fusionsphere, Intel Network Builders Program, ONAP, OpenSource Mano, Nokia Cloudband

Ecosystem, and Telefonica UNICA. These partnerships allow RADCOM Network Intelligence to integrate into the NFV environment seamlessly and provide the feedback loop to NFV MANO.

The entire solution from RADCOM Network Visibility, RADCOM Service Assurance, and RADCOM Network Insights is deployed as a VNF with multiple VNFCs (VNF Components) which allows the full RADCOM Network Intelligence portfolio to be instantiated, modified, and scaled up and down in minutes. Being fully cloud-native also enables on-demand probing and troubleshooting close to the tapping point that will be crucial in assuring 5G services.

Built on a microservices architecture

The robust and agile system is created using a microservices architecture allowing for scaling, updating or even the complete replacement of each part and offers increased efficiency, real-time performance with less hardware, reliability for failure resilience and continuous monitoring as well as elastic scalability with dynamic, automated in/out scalability. All these capabilities are critical in today's high capacity networks and even more essential as operators move to 5G.

Some operators are already adopting the next iteration of virtual software design – containerization and Kubernetes – that enables multiple execution environments to exist on a single operating system instance so that numerous application components can coexist in a single VM environment. By implementing containerization operators gain more application processing from any given hardware to maximize utilization levels for all a server's resources, rather than just loading it up with multiple processor-hogging applications that leave some network capacity unused. As we move forward more and more operators will start implementing containerization, and RADCOM Network Intelligence will adopt this system design to enhance solution scalability and performance.

A distributed cloud deployment

With solution components being divided into microservices operators gain the benefits of a distributed cloud assurance and visibility solution (for both nationwide and CoOp deployments) that can be implemented across the entire network at multiple sites on small VMs for resource efficiency while enabling central management and access to admin functionality and access to aggregated data for all regional deployments.

Monitoring large geographically dispersed networks poses a significant challenge for operators. On the one hand, these top-tier operators want to have a centralized view of the end-to-end services across their entire network, while on the other hand having a single backend to store all the monitored data from all regions isn't efficient.

RADCOM's distributed cloud solution concept enabled by its cloud-native design provides the solution for both these challenges. A cloud-native architecture simplifies the splitting of the solution into multiple microservices, and so the backend is split into central and regional deployments. The central operations center has access to aggregated data for all their nationwide services and enables the administrators to manage all regional solutions centrally. The detailed data is stored in each region and can be queried by central operations.

As a distributed cloud solution, RADCOM's solution only stores what is needed with lots of flexibility on what data to save, while utilizing local storage and not sending everything to a centralized site.

Enabling regional deployments provides the operators with a distributed, stand-alone solution that allows new regions to scale out their systems. RADCOM Network Intelligence also provides operators with a distributed database while RADCOM Network Insights makes this distributed solution transparent to the solution users. RADCOM Network Intelligence is also deployed on different "availability zones" of the cloud to provide integral geo-redundancy.

By delivering a cloud-based operational model that combines flexible central management and distributed regional deployments these operators can efficiently

improve services across their entire nationwide network while being resource efficient. Central administration provides a complete end-to-end service understanding, call tracing down to a local deployment level, fault management, and centralized services instantiation while the regional deployments have local customer experience insights, troubleshooting, and local services instantiation.

Delivering an agile, distributed solution will be critical for operators in their 5G cloud deployments that include network slicing, CUPS, edge placements (essential for lots of 5G use cases) and management of the entire network according to unified service level policies.

Short term architectural changes

5G networks will be deployed, initially, in non-standalone mode (NSA) on a host LTE network using an enhanced 4G core and will migrate over time to a new 5G core, operating in standalone (SA) mode. Optimizing and assuring network services on both NSA and SA 5G networks will be critical if operators are to transition to 5G successfully. Operators are moving to a 5G core that is composed of microservices, deployed on cloud infrastructure, distributed to the edge, and supporting granular, dynamic network slices. To optimize and assure network services and the customer experience operators will need to implement cloud-native network visibility, service assurance, and network insights to monitor the quality of the individual network slides, ensure compliance with SLAs as well as deploy monitoring probes at the edge of the network.

Initial 5G roll-outs

In the initial phase of 5G (based on 3GPP Release 15) operators will use it to provide their customers with Enhanced mobile broadband (eMBB). With one of the first use cases being to capitalize on 5G as a fixed wireless alternative to deliver last-mile connectivity. Fixed Wireless Access (FWA) will be utilized by fixed operators (such as cable operators) to speed up broadband roll-outs, and provide mobile operators an opportunity to tap into the multi-play sector including a new route into the home broadband and video market.

FWA will by commercially launched at the end of 2018 by Verizon Communications and AT&T in the United States. SNS Research estimates that 5G-based FWA subscriptions are expected to account for $1 Billion in service revenue by the end of 2019 alone[4]. The majority of 5G-based FWA is expected to be implemented in densely populated urban areas. However, some rural carriers (including C Spire and U.S. Cellular) are examining 5G as a means to deliver last-mile broadband connectivity to rural communities as well.

[4] 5G for FWA (Fixed Wireless Access): 2017 – 2030 – Opportunities, Challenges, Strategies, and Forecasts report by SNS Telecom

Multi-Access Edge Computing (MEC)

Multi-access Edge Computing (MEC), formerly known as Mobile Edge Computing, is a network architecture concept that 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 will see the convergence of IT and telecommunications networking, 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 by further congestion and can efficiently serve customers.

Some MEC use cases include:

- Video services
- Location services
- Internet-of-Things (IoT)
- Augmented reality
- Optimized local content distribution

RADCOM is already working with customers on monitoring MEC services. To deploy traditional, hardware-based assurance at the edge would be prohibitively expensive and would severely restrict operational flexibility. Also, MEC will be implemented with minimal network resources, so RADCOM's approach matches this strategy by assuring services at the edge with lightweight micro-probes deployed on small VMs. RADCOM's assurance on the edge provides a flexible solution that can be rapidly scaled via integration with NFV MANO and is cost-effective. As the edge data center will support multiple services types (and associated VNFs) and may allocate resources dynamically, it is vital that network visibility and service assurance be automated via NFV MANO. Similarly, if a new service is deployed, or a new customer-type is on-boarded, the monitoring and visibility capabilities will be required.

RADCOM already provides operators today a cloud-distributed deployment model that delivers central management while having light deployments across the network. This deployment model will be utilized by our customers as they expand their services to the edge and need to assure them.

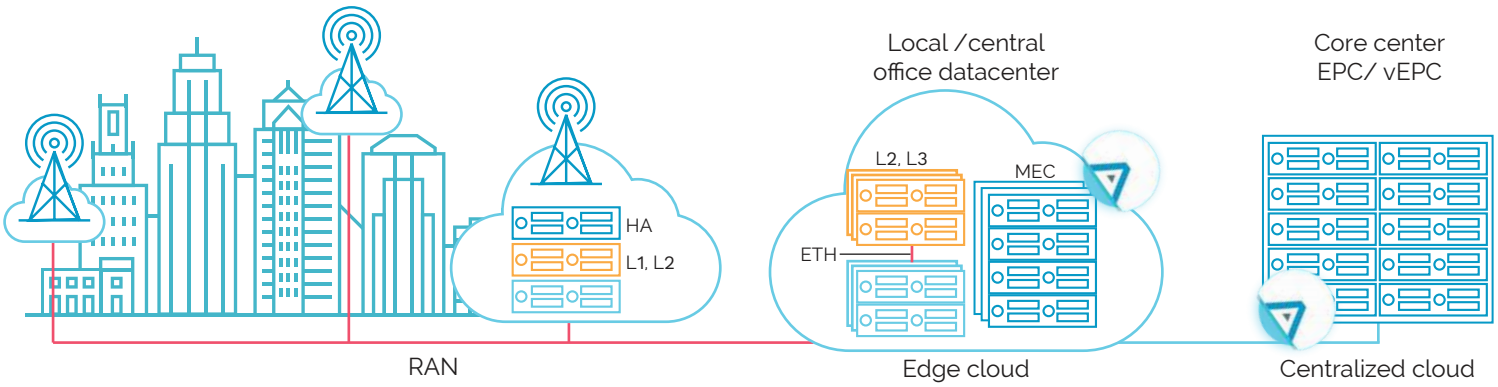


Figure 2 – RADCOM's lightweight micro-probes deployed to monitor edge services

Control & User Plane Separation (CUPS)

Introduced in Release 14 and developed in 3GPP Release 15 Control & User Plane Separation (CUPS) is native to the 5G system and core network and will support a flexible and agile network, with centralized and edge deployments. CUPS involves extracting the control plane functions from the gateway to leave a simpler user-plane node. The gateway is split into S/PGW-U and S/PGW-C components that can scale independently. The main benefit of CUPS is that the control plane and all the associated complex interactions can be centralized, while the user plane is distributed across the IP services platform and scaled as required by the traffic load. This means S/PGW-U functions can be deployed at the edge and as VNFs rather than hardware functions so they can be easily placed at the optimal location.

CUPS represent a notable change to the mobile network architecture and have major implications for service assurance. RADCOM is already working with customers on ensuring full control plane, and user plane correlation as well as new CUPS protocol decoding, Packet Forwarding Control Protocol (PFCP), new aggregations, dimensioning, and network insights to provide operators with a solution that can deliver end-to-end service assurance for 5G.

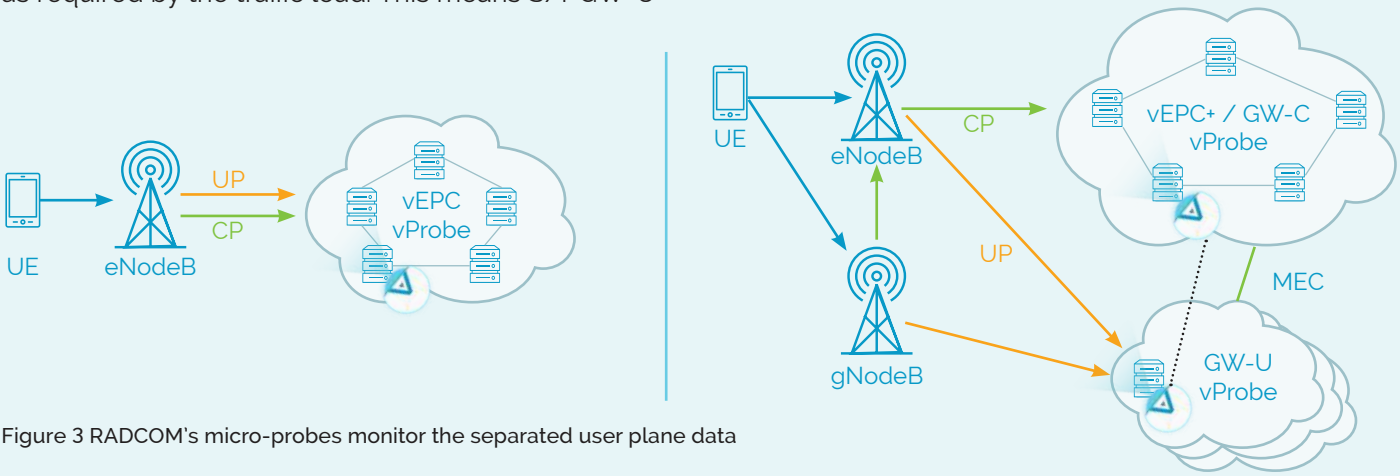


Figure 3 RADCOM's micro-probes monitor the separated user plane data

A peek into the 5G crystal ball

The next stage of 5G, founded on 3GPP Release 16 (based on small cell deployments), will bring further enhancements to mobile data, and full 5G use cases including massive IoT (MIoT) and critical communication services.

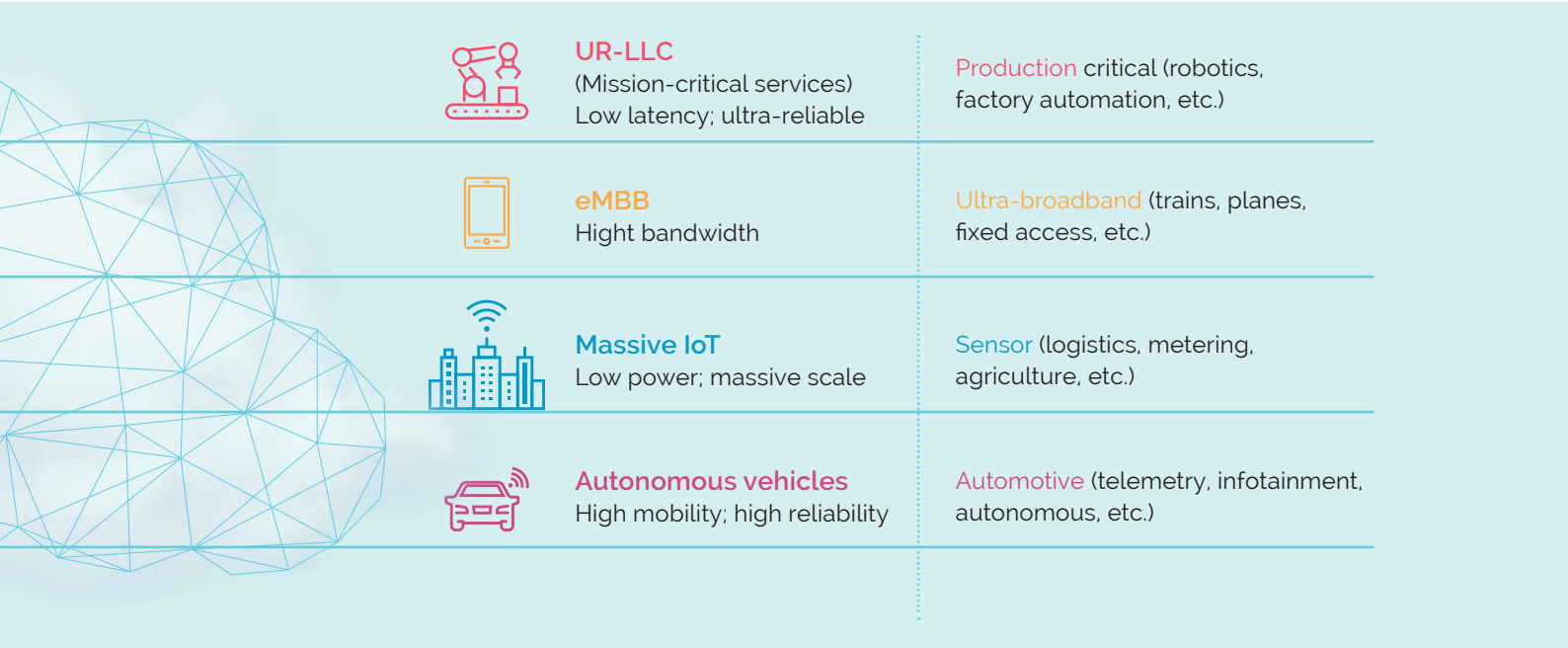
Network Slicing

Network slicing is an essential bridge from a 4G core to a new 5G core. The idea is to create virtual network instances (or slices) dedicated to different services. Each slice is optimized for the relevant traffic profile and the commercial perspective of the associated service. For example, IoT, public safety, healthcare, autonomous vehicles and enterprise services, supporting multiple customer and service types, each with individual performance requirements and can be fine-tuned, at the per-user or per-service level, or at a company or industry level. Network slicing is perhaps the most critical commercial driver for 5G and can be thought of as the network adapting itself to the needs of the customer application.

With network slicing set to be a critical component of an operator's investment strategy service assurance will be used to enable closed-loop automation, policy-based service orchestration and deliver real-time slice monitoring to correlate multiple slices and automatically scale in and out.

To meet performance demands each network slice will run end-to-end from the radio to the core and up to the application layer. This requires service and resource orchestration across the primary functional domains. For zero-touch network management, each of these domains must be assured, so service assurance will need to monitor each of these domains and continually provide feedback to the NFV MANO to maintain service levels as each slice must meet SLA thresholds determined by the operator and customer. As each slice is designed and tailored for specific requirements, service assurance will be vital to measure KPIs for each network slice, especially when it comes to critical service requirements such as end-to-end latency.

The tight integration between assurance and NFV MANO will also be critical in order to provide full lifecycle management so that the assurance solution can onboard, scale out/scale in and adjust itself in real-time as some slices will have a relatively short lifespan or will require constant adjustments (for example in a live sporting or music event). Service assurance will be vital in ensuring the different services deliver on the relevant threshold. For example, with a low-latency service like autonomous cars or ultra-reliable services like public safety, the slice will have rigid service performance thresholds, whereas non-essential IoT services may have more flexible thresholds.



Service-Based Architecture

The new 5G core network is specified in Release 15 and uses what is known as the Service-Based Architecture (SBA) that is fundamental to the commercial success of 5G.

In 2G, 3G, 4G a point-to-point (P2P) architecture has been used. In this model, network functions are connected over standardized interfaces that allow for multi-vendor networks. The challenge with the P2P architecture is that contains a large number of unique interfaces between functional elements, each connected to multiple adjacent elements. This "tangle" of connections creates dependencies between functions and makes it difficult to change.

The SBA architecture decouples the end-user service from the underlying network and platform infrastructure enabling both functional and service agility. By virtue of SBA being designed to operate using the cloud model, in which different functions can be composed into an end-to-end service over standardized application programming interfaces (APIs), it is 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).

The SBA supports services not available in the 4G core – notably related to network slicing and multi-access – and is intended to be "cloud native" by design. 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), respectively; and the move to service-based interfaces.

Massive IoT (MIoT)

When 4G networks were introduced in 2008, there were close to 700M mobile subscribers worldwide. Today, there are more than 7b mobile subscribers worldwide. By 2020, there will be approximately 20b Internet of Things (IoT) devices, in addition to the 9 billion mobile subscribers that are expected worldwide.

As mentioned 5G networks are not only delivering eMBB they are also designed to provide massive scale supporting. In the long-term 5G networks are expected to support as many as a trillion connected devices, including mission-critical and potentially lifesaving applications and scenarios. Unlike smartphones and other cellular devices, IoT device communications can be sporadic. Many of these devices "sleep" (to extend battery life for ten or more years in some cases) for long periods of time — hours, days, or weeks — before transmitting a few bytes of data, and thus needn't always be connected to the network. 5G networks must be designed to handle infrequent, but important communications from these types of IoT devices. Although the amount of data these devices send may be significantly lower, they may still be of a time-critical nature. For example, a sensor that detects a hazardous condition may instruct an Evolved Node B (eNodeB) element to shut down equipment in an industrial plant or building. These types of communication, though infrequent, must be handled with the utmost responsiveness and reliability.

In LTE (Release 13) the 3GPP defined a new standard called NarrowBand IoT (NB-IoT) for handling low volumes of data (similar to 2G) from tens of thousands of devices in a single cell tower. The standard optimized for low data rate, latency-tolerant IoT applications, enabled multiyear battery life and provided more in-depth coverage to reach sensors in challenging locations, such as remote rural areas or inside buildings.

5G NR will use resource spread multiple access (RSMA) on the uplink to enable grant-free transmission of data. A device does not need an enhanced Node B (eNodeB) to give it a grant (or slot) in the pipe to transmit data. This capability eliminates the need for signaling and allows devices to send small packets asynchronously. 5G NR will also address distance and location challenges in low-power IoT devices, using a technique called multi-hop mesh to relay uplink data via nearby devices.

NB-IoT data is transferred via the control plane in three different paths to the application server:

1. Through the MME via the SCEF in CP mode for non-IP data
2. Through the MME via the SGW in CP mode for IP data
3. From the UTRAN via the SGW in UP mode

RADCOM Network Intelligence enables end-to-end NB-IoT service monitoring and continues to evolve

its solution according to the developing network standards and architecture. Today, RADCOM's solution defines baseline performance thresholds for machine groups (devices of the same type) and sends alerts for individual machines which cross these thresholds. Operators can utilize RADCOM's group tracing feature to create full control plane and user plane traces for new machine types or drive tests for extended periods of time. This shows the operator how a network issue can impact IoT performance and drill down to a list of affected devices and extract PCAP traces to troubleshoot issues or send to the network vendor (if the IoT service vendor is not the network operator).

Today RADCOM provides operators with:

1. Connectivity assurance
2. Anomaly detection
3. Location intelligence
4. Troubleshooting per device/connection
5. Service Level Agreement monitoring

As we move forward to MIoT, RADCOM will be deploying machine learning to set these performance thresholds dynamically, detect significant anomalies as well as delivering real-time feeds to IoT security solutions.

Conclusions

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 cloud-native services.

However, the sheer amount of events and traffic in a 5G network will overwhelm human understanding and their ability to make optimal network policy decisions manually. Automation, rather than human intervention is required to take the 5G service vision into reality, which is dependent on a cloud-native approach to service assurance. The ability to assure these diverse service types on a cloud-native 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.

5G rollouts will be determined by many factors (including whether operators can attain the required spectrum which mainly depends on the region the operator is located), but what is certain is that the initial phase of 5G will begin rolling out at the end of 2018.

RADCOM is working closely with its customer to ensure a smooth transition to a 5G-ready cloud 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. For more information on how to RADCOMize your network, today, please visit www.radcom.com.

RADCOMize

your NETWORK

Visit our website: www.radcom.com

Copyright © 2018 RADCOM Ltd. All rights reserved. This documentation contains proprietary information of RADCOM Ltd. Without the express prior written permission of RADCOM Ltd., no part of the contents hereof may be used for any other purpose, disclosed to persons or firms outside the recipient company, or reproduced by any means. RADCOM Ltd reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, and services.

www.radcom.com | ©2018 RADCOM. All rights reserved.