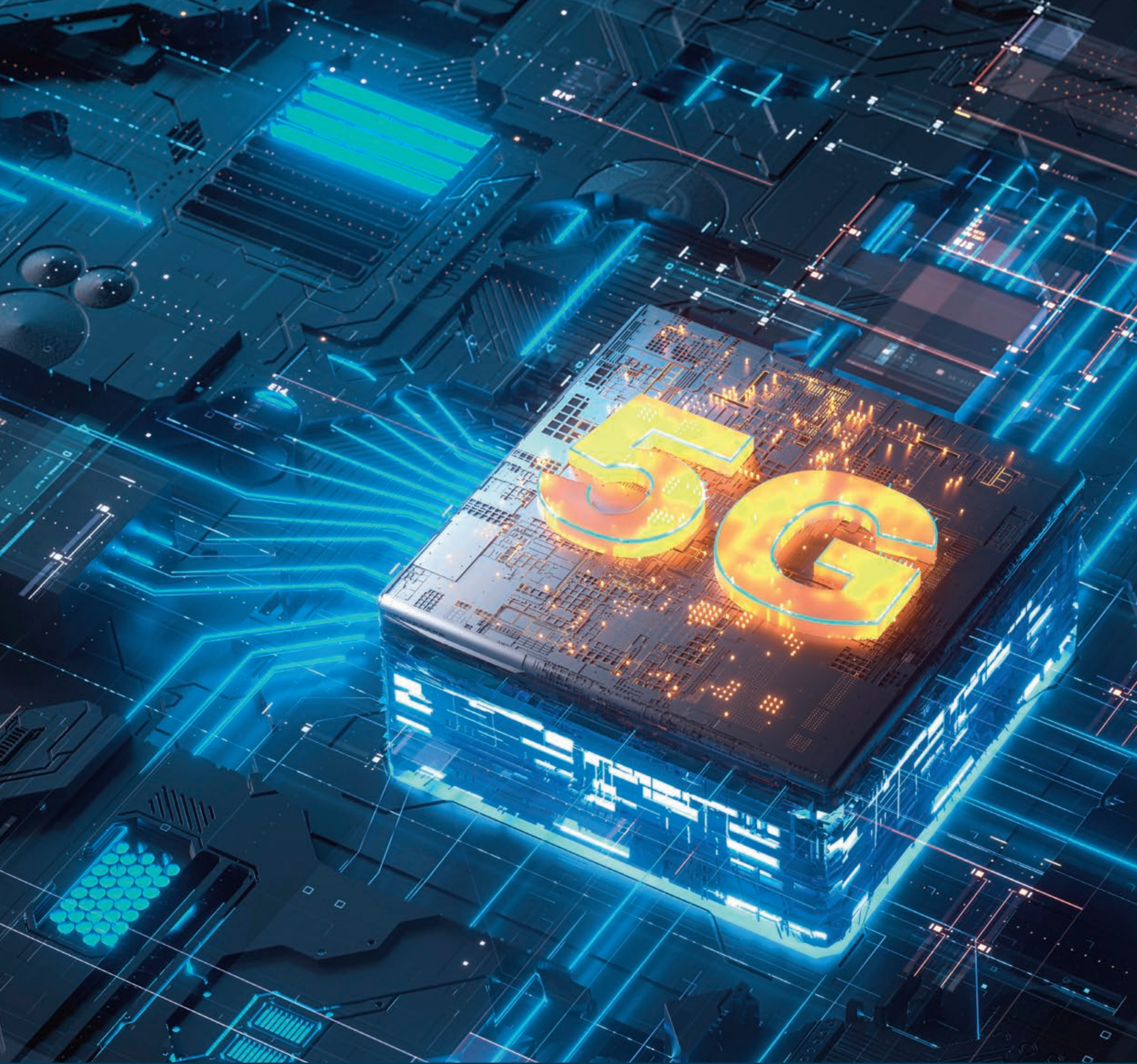


How to build the best 5G core

Future-proofing policy, signaling and testing in a dynamic new network environment

Published by

MOBILE WORLD LIVE

Sponsored by

ORACLE Communications

Executive summary

Almost two-thirds of mobile operators around the world plan to launch standalone 5G networks during 2022 and 2023, according to GSMA Intelligence. With a standalone 5G network, operators will be able to employ a service-based architecture that can support web scale technologies, open source software and high levels of automation.

Experts say a cloud-native 5G core network will make operators agile, cost-effective and customer-oriented. Standalone 5G operators should, for example, find it easier and quicker to use big data analytics, artificial intelligence and machine learning to optimise network resources, understand customer behaviour and offer personalised and tailored services. This paper explores the implications of this new architecture for the policy, signaling and routing, and testing systems that operators use to manage their networks.

The case for a converged 5G policy solution

A 5G core policy solution needs to support network slicing, integration with network data analytics functions, differentiated services and edge computing. It must be agile and secure enough to flexibly manage different domain-specific policies for more differentiated and personalised customer offerings and granular enough to manage individual services across network slices. It also needs to be a converged solution that uses common resources and micro-services to simultaneously support 4G and 5G. In the lengthy migration period from 4G to 5G, the solution needs to allocate resources efficiently in line with the specific network traffic demands.

How a service communication proxy can support 5G signaling

As 5G networks will handle much greater traffic levels and diversity than their predecessors, operators need a robust signaling solution that can manage this complexity and allow for elastic growth, while supporting interoperability with 3G and 4G. Oracle has developed a service communication proxy (SCP) to address these challenges, while optimising signaling controls, reducing congestion, and improving routing and load balancing. It is also designed to give the operator better visibility into the core network: collecting metrics related to message processing can provide a view of network health. Furthermore, the SCP can expose a new release to a fraction of the user base for testing purposes.

An automated framework can speed up 5G testing

With the deployment of a new cloud-native core network, new network functions and an array of new use cases for mobile connectivity, testing 5G systems could be a lengthy and error-prone process. To allow for the rapid rollout of new platforms and configuration changes, operators need a robust and flexible automated testing suite that can verify new versions of software efficiently and quickly. In particular, fully automating the DevOps pipeline (including verification and testing) should remove much of the potential for human error. Developed originally for in-house use, Oracle has expanded its automated framework to run 900 test cases out-of-the-box, enabling operators to automate the whole 5G core testing process. It says operators can use the framework to test either a single network function or multiple network functions independently in the same environment.

In summary, the service-based architecture that underpins a 5G core network needs to be reinforced and enhanced to handle the demanding challenges faced by public telecoms networks, particularly in environments where 4G and 5G are working alongside each other. In particular, operators need flexible, yet robust and highly automated policy, signaling and testing solutions that are both versatile and efficient.

Introduction

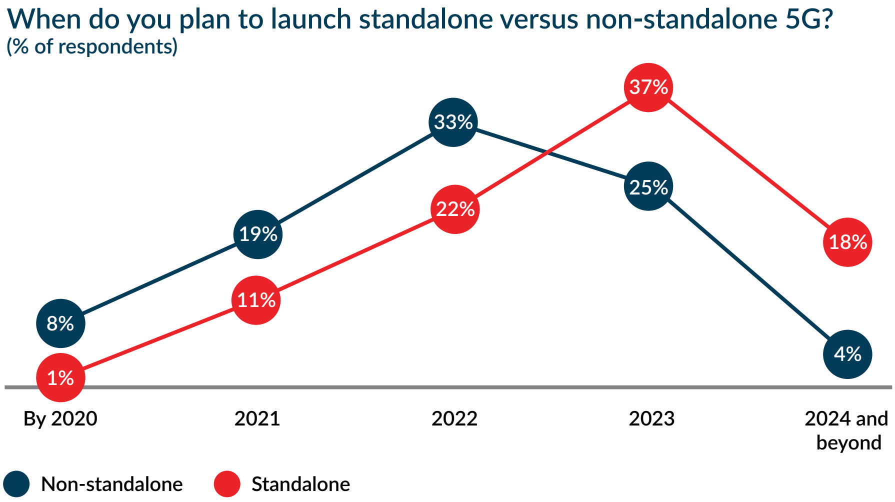
The road to full 5G

The latest mobile technology - 5G - is spreading across the globe. By June 2020, 87 mobile operators in 39 markets had launched 5G, according to GSMA Intelligence. The research firm estimates there will be 1.7 billion 5G connections in use worldwide by 2025.

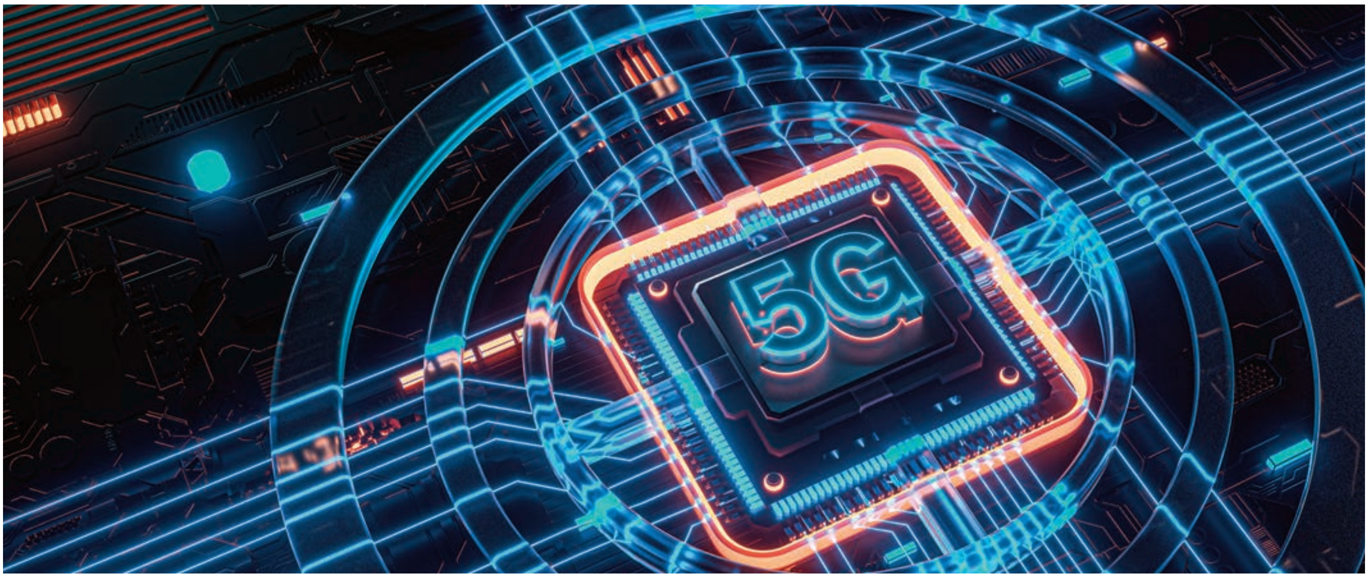
To date, most of the commercial 5G networks are connected to a 4G core. Referred to as non-standalone (NSA) networks, they take advantage of the new 5G radio interface, but have yet to benefit from other key 5G features, such as a flexible core architecture and network slicing. In practice, NSA networks can support enhanced mobile broadband (faster speeds), but not ultra-low latency connectivity, which requires a standalone 5G network with a dedicated 5G core.

A survey by GSMA Intelligence found that about 60% of mobile operators intend to launch standalone (SA) networks with a 5G core in 2022 or 2023 (see Figure 1). The researchers note this represents a two-year lag on NSA, which partly reflects the higher costs associated with SA and the fact that new standards from 3GPP will not be available until 2021. Still, "we expect some operators to fast-track their SA deployments or to launch micro deployments on custom specifications before international standards are agreed," wrote Tim Hatt, head of research at GSMA Intelligence, in a June 2020 report.

Figure 1: The mobile industry is on the cusp of rolling out standalone 5G networks



Source: GSMA Intelligence



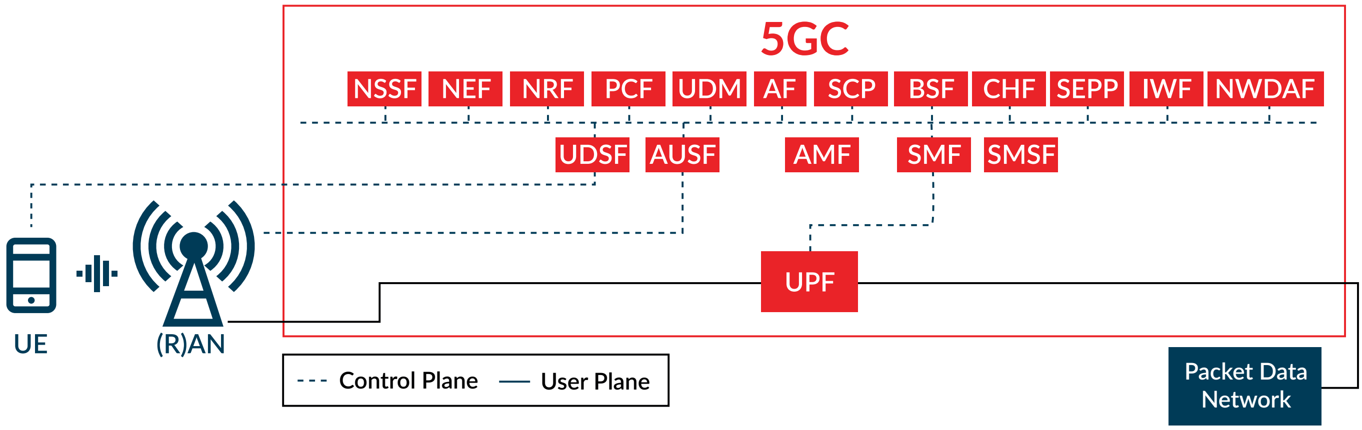
The characteristics of a 5G core

Drawing on the architecture that underpins modern IT systems, components in a 5G core network communicate with each other in a completely different way to the components in a 4G core network. A 5G core employs a service-based architecture (SBA) where network elements advertise and provide services that can be consumed by other elements using application programming interfaces (APIs). This allows for telecoms networks to adopt web scale technologies and open source software, enabling a step change in automation.

Mobile operators can leverage the existing SBA tools used in IT architectures. For example, a cloud-native service mesh is an emerging technology for handling congestion control, traffic prioritisation, overload control and optimized routing within a microservices architecture. It is designed to make inter-service communication safe, fast, secure, and reliable.

However, experts caution an off-the shelf service mesh solution is not 5G aware, meaning it will lack critical capabilities required to meet the needs of a 5G core SBA. Modifications may be required to support traffic routing, prioritisation, overload control, load balancing, and interworking.

Figure 2: The network functions that compose a 5G core service-based architecture



AF: Application Function • AMF: Access and Mobility Management Function • AUSF: Authentication Server Function • BSF: Binding Support Function • CHF: Charging Function • IWF: Interworking & Mediation Function • NEF: Network Exposure Function • NRF: Network Repository Function • NSSF: Network Slice Selection Function • NWDAF: Network Data Analytics Function • PCF: Policy Control Function • SEPP: Security Edge Protection Proxy • SCP: Service Communication Proxy • SMF: Session Management Function • SMSF: SMS (Short Message Service) Function • UDM: User Data Management • UDSF: Unstructured Data Storage Function • UPF: User Plane Function

Source: GSMA

The importance and implications of a cloud-native approach

By adopting cloud-native technology, a telecoms network should be able to tap the advantages of IT web-scale models that have proven to be agile, cost-effective and customer-oriented. Such solutions could be deployed in either a public cloud or a private cloud, but experts caution only a truly cloud-native architecture will allow for the flexibility and scalability associated with the leading Internet platforms.

"The term cloud-native is sometimes stretched to refer to existing solutions that have been transplanted into a cloud environment, rather than being architected from scratch as a cloud-based solution," cautions Shirin Esfandiari, product marketing director at Oracle Communications. "As they develop their 5G core networks, telecoms operators need to ensure they really can harness all the benefits that the cloud has brought to IT." Oracle has developed a cloud native 5G core solution, which uses microservices and a distributed architecture to provide resiliency, scalability and security.

Proponents of a cloud-native approach see a wide range of benefits. For example, it should be easier for operators to leverage IT cloud-based technologies, such as big data analytics, artificial intelligence and machine learning, to optimise the network resources, understand customer behaviour and offer personalised and tailored services more efficiently and rapidly.

At the same time, the adoption of IT-style agile processes should enable mobile operators to benefit from increased automation and more efficiency gains. These processes include the continuous delivery and deployment of software, enabled by automated testing, as well as enabling canary releases[1] and blue/green deployments[2] to validate new concepts. An automated agile approach could also allow for end-to-end service orchestration, dynamic slice management and, eventually, one-click procurement of network slices deployed as-a-service for specific use cases and market segments.

[1] A canary release involves rolling out new software to a small subset of users before making it widely available
[2] Blue/green deployments involve running two production environments side by side, allowing for testing to occur in one, while the other is live

The importance of policy, signaling/routing and automated testing systems

This paper looks at how the deployment of 5G core networks will impact the policy, signaling and routing, and testing systems that telecoms operators depend upon. Policy systems manage and govern network behaviour and drive quality-of-service control. They support traffic steering, subscriber spending, usage monitoring, interworking with IMS and roaming, among other capabilities (see Figure 3).

Signaling and routing systems control communications across networks – the transmitting end of the network uses a signal to inform the receiving end it is sending data to the recipient. To enable 5G networks to interwork with 4G, there will be at least three signaling protocols to manage in parallel: SS7, Diameter and HTTP/2.

Testing systems are, of course, essential to ensure that telecoms networks and the services they deliver work in the way they are intended to. In a fast moving and competitive marketplace, testing needs to be rigorous, efficient and rapid.

Figure 3:
Policy systems are responsible for managing an array of key capabilities

Source: GSMA

[3] Internet Protocol multimedia subsystem

5G network policy

New network policy challenges

With 5G, policy systems need to have a much broader set of capabilities than their predecessors. They need to support next-generation functionality, such as network slicing, integration with network data analytics functions, and the enablement of differentiated services. They also need to support edge computing – the deployment of computing resources at the edge of the network to deliver more responsive services and applications.

At the same time, the policy system needs to be agile enough to flexibly manage different domain-specific policies for more differentiated and personalised customer offerings, while also remaining secure. It must also be granular enough to manage individual services across network slices.

To complicate matters further, the policy system will need to simultaneously support 4G/NSA 5G and SA 5G, as traffic migrates from 4G networks to 5G networks. "In the lengthy migration period, resource utilisation could be erratic and inefficient," says Shirin Esfandiari, Oracle Communications. "Distributed network functions will add to the complexity of dimensioning resources when subscriber traffic patterns are changing rapidly."

Potential policy solutions

One way to address these challenges is to deploy a converged policy solution that uses common resources and microservices across 4G and 5G networks, based on the specific network traffic demands. This approach could make efficient use of resources and keep costs in check. It will also enable the interworking between 4G and 5G required to support existing 4G services, as operators roll out the 5G network and new business models. Operators will also want to migrate their 4G-enabled policy use cases over to 5G platforms.

"For operators that start with NSA 5G, a cloud native converged policy solution is a future proof option – they can continue to use the same converged policy solution as they transition to SA 5G," says Tarek Assali, Director of Software at Oracle Communications. "At the same time, a converged cloud-native solution makes it easier to perform the modifications/software upgrades required to support the smooth migration from 4G LTE/5G NSA to 5G SA architecture."

Oracle says a cloud-native policy framework for 4G and 5G interworking will allow operators to migrate and design current use cases in a consistent way for both 4G and 5G subscribers. "This is critical for operators to provide a reliable and unified customer experience during 5G migration, which is essential to ensuring uptake of 5G services," adds Tarek Assali.

One advanced operator in Asia, for example, has deployed a converged cloud native policy solution from Oracle to control its 5G network. The operator is using the solution to implement complex policies decisions based on network, subscriber and service information. It employs Oracle's Communications Policy Control Function (PCF), which is designed to generate and test operator policies from scratch and deploy them into a production environment in matter of minutes. Oracle says PCF empowers operators to develop tailored offerings for a wide range of use cases ranging from enhanced mobile broadband, ultra-reliable and low latency communication, and massive IoT.

The leading telco in the Nordics market and one of the largest American operators have also deployed Oracle's policy solutions. These forward-looking operators view cloud native architecture as a must for their 5G migration, according to Oracle, which says they also value Oracle's security-by-design and rigorous regulatory compliancy, spanning infrastructure, platform and applications.

5G network signaling

New network signaling challenges

For mobile operators, 5G networks promise to bring about a step change in traffic levels and traffic diversity. The challenge of managing this traffic will be compounded by the introduction of a new signaling protocol, which has implications for routing and optimisation, and traffic management scalability, visibility and security. Operators will need to support the HTTP/2 protocol, as well as the existing Diameter and SS7 protocols that are used in legacy telecoms networks, presenting interworking, network visibility and interoperability challenges.

Oracle says the lack of 5G awareness in the standard IT-based service mesh employed by a service-based architecture can result in other important gaps, such as:

- No integration with the network repository function (the NRF) that maps the 5G core topology.
- No support for routing based on user identities or other 5G criteria, since this information is conveyed in a JSON payload.
- Message prioritisation requires 5G service awareness.
- Overload control requires 5G service awareness.
- Mediation capabilities require modifications to the JSON payload.
- No 5G built-in service metrics.

Potential signaling solutions

Ideally, a signaling solution will curb the cost and complexity of 5G signaling and allow for elastic growth, while supporting interoperability with 4G and 3G traffic. Oracle advocates the use of a service communication proxy (SCP) to resolve the challenges introduced by the 5G service-based architecture, while optimising signaling controls, reducing congestion, and improving routing and load balancing.

Designed to support HTTP routing services in 5G networks, an SCP can use the network function notifications sent by the NRF to create routing rules and provide enhanced routing control. The SCP is intended to boost the resilience of the 5G network by supporting alternate routing, outlier detection and circuit breaking. It can make re-routing decisions based on load conditions and the health status of network functions. With a SCP in place, consumer network functions will no longer need to remember and interpret complex routing rules associated with next hop selection.

"As it has a complete view of all the messages arriving for each network function, the service communication proxy enables the operator to get better visibility into the core network," explains Sameh Naguib, Head of Americas Sales Consulting at Oracle Communications. "It can be used to reprioritize traffic, as well as protecting the network from flooding by malicious or rogue consumer network functions, and prevent provider network functions from being overloaded." In the event of an overload, the SCP is designed to identify and prioritise the important messages and provide a proxy for the overloaded provider network function.

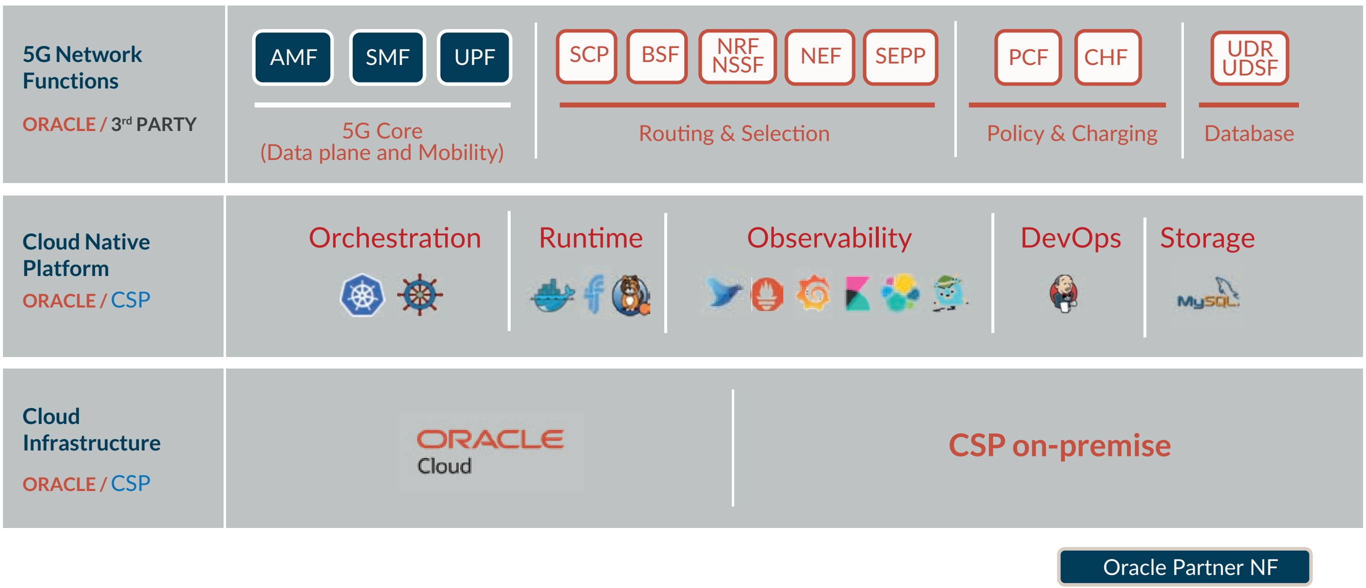
Oracle says the network can be architected in a way that ensures each instance of a network function maintains a set of redundant connections to the SCP and uses those connections for all outbound requests. That eliminates the need for the network functions to establish direct connections with each other. It also enables the SCP to collect metrics related to message processing, thereby providing a view of network health.

As the SCP gives operator granular control, it could, for example, be used to expose a new release to a fraction of the user base or friendly users for testing purposes.

Oracle signaling solutions, which are used by some of the world's largest telcos, are part of a much broader cloud offering (see Figure 4).

"Our extensive experience of building and operating in cloud native environments, and delivering signaling, routing, and policy solutions, has allowed us to add 5G awareness to the service mesh foundation," says Sameh Naguib, Oracle Communications. "In addition to the SCP, Oracle's 5G core solutions support the routing of IMS-related policy signaling traffic, the secure exposure of the 5G core to application functions, slice selection and interworking between 4G and 5G cores." They also allow for the dynamic discovery and selection of network functions, and the secure interconnect between operators and roaming hubs for roaming use cases, he adds.

Figure 4: Oracle provides software and solutions across the cloud technology stack



Source: Oracle

5G network testing

Network testing challenges

Implementing standalone 5G involves the deployment of a new cloud-native core and new network functions. For incumbent operators, this approach marks a radical departure from what they had before, so testing this new architecture is potentially a lengthy and error-prone process. Furthermore, the highly dynamic service-based architecture of 5G enables operators to support a very wide range of use cases for connectivity, which all need to be tested.

To quickly roll out new services, forward thinking operators have started following the DevOps model of software delivery. “In our case, the number of software releases delivered per year has risen from two to six, making manual testing a serious challenge,” says Shirin Esfandiari, Oracle Communications. “You cannot have continuous delivery without continuous testing.”

Potential testing solutions

To deliver a seamless experience for 5G consumer and business customers, telcos will need a robust and flexible automated testing suite. Such a suite should enable operators to verify new versions of software efficiently, roll out new platforms quickly, change configurations easily, expand their networks, ensure resiliency and perform accurate benchmarking and capacity planning.

"By fully automating the DevOps pipeline, including verification and testing, you can really reduce the potential for human error and increase agility,” notes Shirin Esfandiari, Oracle Communications. “Working with a leading operator we have developed an automated testing suite for 5G core NFs, where in some cases they were able to reduce a typical 4 weeks testing cycle down to 10 hours. With more than 900 test cases out-of-the-box, this enables operators to automate the 5G core testing process and test either a single network function or multiple network functions independently in the same environment."

Conclusion

The best 5G core networks will combine the flexibility of modern IT architectures with the reliability and security of traditional telecoms solutions. In particular, the underlying service-based architecture needs to be adapted to enable the smooth running of complex public telecoms networks, particularly in demanding environments where 4G and 5G are working alongside each other.

To ensure they provide customers with a compelling 5G proposition, telcos need to pay particular attention to how to implement policy controls, signaling and automated testing. Operators need flexible, yet robust and highly automated solutions that are both versatile and efficient.

"To build the perfect 5G core, operators will need partners with a deep understanding of both IT and telecoms networks with a security first mindset," concludes Shirin Esfandiari, Oracle Communications. "Oracle's best-in-class 5G core solutions are based on Oracle's IT and cloud heritage, combined with over 40 years of expertise in core network technologies in areas that are most critical for operators, such as security, signaling and policy. Oracle can help operators to really light up 5G with networks built from the ground up for cloud technology and applications."

ORACLE Communications

Oracle Communications provides integrated communications and cloud solutions for Service Providers and Enterprises to accelerate their digital transformation journey in a communications-driven world from network evolution to digital business to customer experience.

Find out more at www.oracle.com/industries/communications

MOBILE WORLD LIVE

Produced by the mobile industry for the mobile industry, Mobile World Live is the leading multimedia resource that keeps mobile professionals on top of the news and issues shaping the market. It offers daily breaking news from around the globe. Exclusive video interviews with business leaders and event reports provide comprehensive insight into the latest developments and key issues. All enhanced by incisive analysis from our team of expert commentators. Our responsive website design ensures the best reading experience on any device so readers can keep up-to-date wherever they are.

We also publish five regular eNewsletters to keep the mobile industry up-to-speed: The Mobile World Live Daily, plus weekly newsletters on Mobile Apps, Asia, Mobile Devices and Mobile Money.

What's more, Mobile World Live produces webinars, the Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and exclusive home to all GSMA event keynote presentations.

Find out more at www.mobileworldlive.com