WHITEPAPER

ABot as MEC Validation tool for Operators and End Customers

Rebaca

ENSURING QUALITY ON SCHEDULE

Background:

A new era of applications demanding millisecond latency and very high compute has brought about the concept of edge network, which is also referred to as "intelligent edge network" or "5G edge" or "multi-access edge computing" (MEC). 5G deployments and the trend toward open RAN technology in the wireless market are helping to drive the edge computing opportunity. MEC is designed to push resources closer to the radio access networks in 4G and 5G. It brings cloud-computing capabilities and an IT service environment at the edge of the mobile network. This provides ultra-low latency and high bandwidth as well as real-time access to radio network information that can be leveraged by applications. These applications are enabling new enterprise solutions, IoT, and consumer services such as video, robotics, and gaming, etc.

MEC functional layers are end devices, access networks, edge networks, and core infrastructure. Telcom operates would leverage virtualized core networks operating across a mix of macro cell towers, small cells, fiber networks, data centers, and edge. Edge provides compute, storage, and network resources to address the needs of various new-age application use cases. Edge devices use different access technologies including 3G, 4G, 5G, Wi-Fi, Wi-Max, etc. Hence heterogeneity needs to be catered for the smooth functioning of MEC operations. MEC architectural components are ME host and network, MEC platform, MEC orchestrator, and Operation support system.

Challenges of MEC Management for Operators and End Customers:

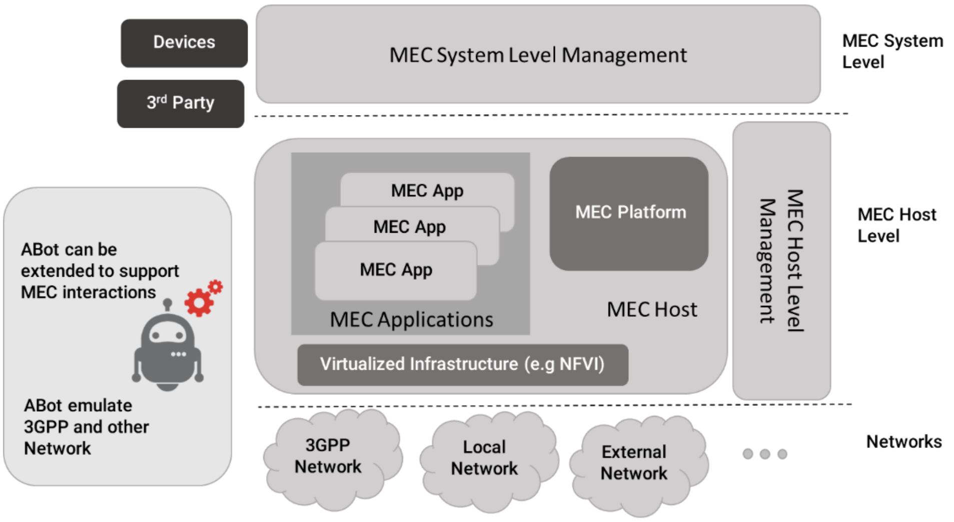
The diversity of the network technologies and the application use cases of MEC necessitates an environment that may have dozens, hundreds, or thousands of locations to configure, deploy, turn up, monitor, and maintain. Manual processes that might have worked before will now require automation for all these processes and mechanisms to create an autonomous process that allows their integration and interoperability. Operating and maintaining such a diverse network is quite challenging as well. The support team needs to aware of a variety of network technologies and use cases to be able to detect and rectify.

Edge has two business models – public and private. The public model enables developers to build latency-sensitive apps and use cases such as delivering high-resolution video or virtual reality. Private edge is for customers that want dedicated edge compute infrastructure with ultra-low latency and high levels of security and customization.
Edge computing will open a floodgate of new devices in the network. Service assurance and performance monitoring need to be in place that will monitor every issue faced by remote applications and microservices. After the roll-out, billions of devices will be communicating machine-to-machine, and there would be addition or subtraction of connected devices at an unprecedented scale. Without a validation, monitoring, and analyzing platform for the edge, the reliability of edge will always remain questionable and, hence, dissuade adoption.

Before the IT managers deploy edge computing and open a floodgate of new devices in their network, they need assurance that there will be a smart performance monitoring platform in place that will monitor every issue faced. Creating and validating various use cases that can be easily authored and automated by different stakeholder is extremely important.

ABot for MEC Deployment Validation and Operational SLA monitoring:

ABot from Rebaca Technologies is a Tester and Analytics solution for End-to-End (E2E) Call Flow validation. It is Cloud native and its extensive REST API support enables it to work with other Orchestrators, Configuration & Provisioning tools. ABot architecture enables rapid implementation of new network protocol messages associated with any use case scenario. Its emulated protocol stacks are very lightweight and versatile to fit various architectures of the MEC solution for the different verticals. ABot currently supports 4G, 5G, and hybrid test cases. Hence it can facilitate the integration of multi-vendor solutions within the RAN and the Mobile Core. ABot can support any TCP/IP traffic and we can be extended to support other IP-based protocols. The MEC components and the http-based communication between them can easily be supported by the ABot framework. ABot test cases, its Analytics engine, and the extensive REST support for integration with any Orchestrator and CI/CT/CD pipeline make it an effective tool for MEC solution.


Devices
3rd Party
MEC System Level Management
MEC System Level
ABot can be extended to support MEC interactions
ABot emulate 3GPP and other Network
MEC App
MEC App
MEC App
MEC Applications
MEC Platform
MEC Host
Virtualized Infrastructure (e.g NFVI)
MEC Host Level Management
MEC Host Level
3GPP Network
Local Network
External Network
Networks

MEC platform comprises of Edge and Cloud infrastructure of various configuration and capability, which can scale up and down in real-time. Hence it is important to validate a use case and the performance of the associated NFs on various infrastructure configurations. ABot cloud native stacks are lightweight and can easily be deployed on any network configuration.

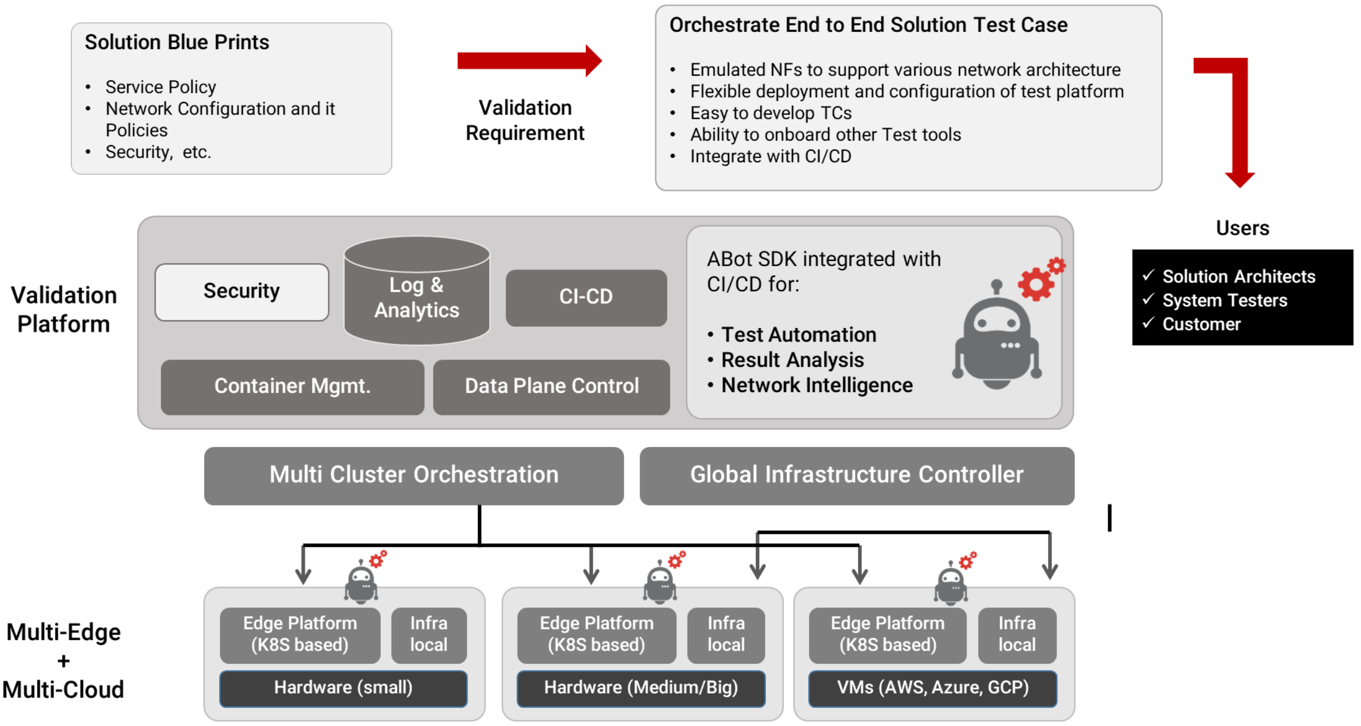
In addition, the services or service clusters that each node will support are often new and can vary quite a bit in traffic characteristics and volume. Operators want to provide the quality-of-service needed for each area. Ensuring and maintaining the service is a big challenge. There are a lot of unknowns in the number of subscribers, traffic type, and demand on a per-site or per-node basis. ABot English like e2e test scripts are easy to modify and can be executed by the operations team to deploy, verify, debug, and maintain a network.

Security in MEC environments, especially DDoS protection, is a growing challenge and it is much more difficult to ensure because of the number of locations and the evolving nature of DDoS attacks. It is essential not only to secure the building blocks but also to orchestrate diverse security mechanisms to create an autonomous view that allows better policy implementation. Hence there is a need to have network behavior models against which real time production network traffic patterns can be compared and verified. ABot behavior driven test cases and their Analytics enables one to capture various KPIs for different e2e uses cases and create models of expected behavior needed for anomaly detection.

Successful MEC deployments will hinge on three operational pieces: edge asset management; change management (deploying and removing on demand) and capacity (space, power, etc.). ABot solution can facilitate asset management and change management.

ABot integration with Operator and End User Tool kits or frameworks:

ABot can be integrated with any CI engine targeted for the MEC Platform to validate and analyze the call flows of a solution. These test cases are written in English like domain language; hence they are easy to understand for the operation & support team and can even be provided to customers as a canned test case repository.

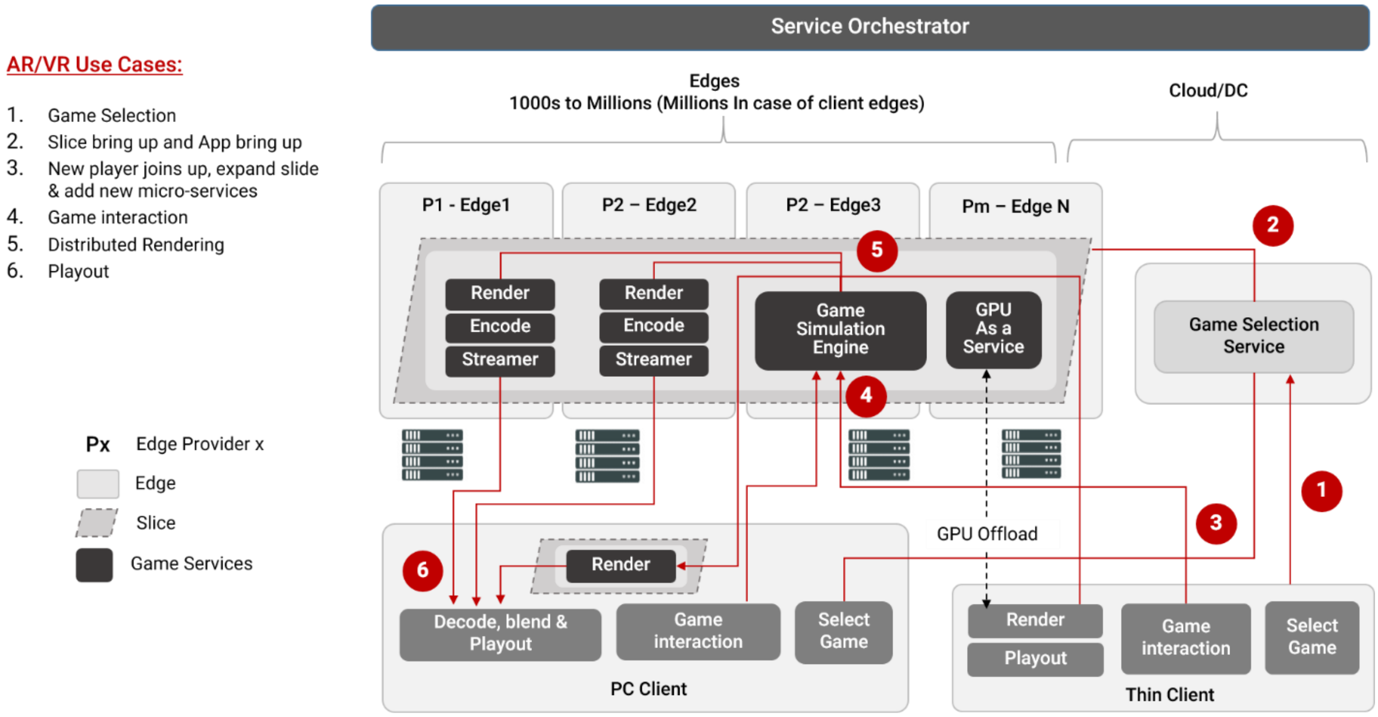


ABot can be used to validate the various MEC exemplary reference architecture deployment models by running use case specific scenarios. It can also emulate any NF required for validating the use case. ABot NF can coexist with actual nodes and can be managed through an orchestrator. ABot framework enables rapid development of new protocols and interfaces required to support different NF needed to support MEC application use cases. New scenarios can very easily be developed using application specific domain knowledge only; hence ABot generate scenarios are understandable across a larger user group. ABot can be integrated with the CI engine and can be part of the CI-CT-CD solution.

ABoT provides the ability to select a particular 5G slice and generate traffic required to test the application use case on a MEC Platform. ABot test cases can be used to validate both functional and performance scenarios to help understand the scalability of a solution on any platform. The Analytics module of ABot based e2e test case can be used to validate various aspects of solution deployment. ABot can help establish a correlation between Network Function performance and its infrastructure KPIs (NFVI, Container, etc.). Various network related KPIs are also derived from the executed test cases, like connection time, bearer vs dedicated connection, etc. Quality parameters of different types of network activities/procedures are also derived from the pass/fail analysis. This capability will enable Operators in doing Root Cause Analysis (RCA) expeditiously. Intelligent correlations of KPIs will enable optimization of the MEC platform resources. The network and infrastructure KPIs captured by ABot and the associated analytics generated, can be used to understand the behavior of the MEC platform against different use case executed. This information can be used to generate traffic characteristics models which can be used for modeling and understanding network and infrastructure behavior against different use cases. Such behavioral models can be used for maintenance, network planning, and detecting security threats.

AR/VR Solution Use Case Example:

If we consider an AR/VR use case, there could be a bunch of e2e scenarios that would need to be validated. For an AR/VR use case, one would be writing test cases using video domain language while drone related test cases would be using a different one; however, they both will follow similar English like domain specific syntax of ABot. Such a canned test case repository can be used by Operator and End Users for network modeling, RCA, and network maintenance.



AR/VR Use Cases:

1. Game Selection
2. Slice bring up and App bring up
3. New player joins up, expand slide & add new micro-services
4. Game interaction
5. Distributed Rendering
6. Playout

Sample test case for Game Selection:

Given the end points of Network Configuration X are active
When I send <GameCatalogRq> message to Game Selection Service
{parameters: values}
Then I receive <GameCatalogRsp> message from Game Seletcion Service
{parameters: values}
When I send <GameChoiceRq> message to Game Selection Service
{GameID: value}
{Parameters: value}
When I send <SliceSelection> message to Node A
{SliceId: value}
{Parameters: value}

etc.....