ZTE

MEC Intelligent O&M White Paper

MEC Intelligent O&M White Paper

Version	Date	Author	Reviewer	Notes
V1.0	2021/02/25	ZTE		Not open to the third party

TABLE OF CONTENTS

1 Overview 5

2 MEC Development Trend 5

3 Features of MEC O&M Management 7

4 Development of MEC O&M Management 8

5 ZTE MEC O&M Management Solution 10
5.1 ZTE MEC O&M Management System 10
5.2 Unpacking and Use of MEC Equipment 12
5.3 Agile Onboarding of MEC Applications 13
5.3.1 Automatic Orchestration of Application Resource 13
5.3.2 Agile Configuration of Application Policies 15
5.3.3 On-Demand Invoking of Application Capabilities 16
5.4 Intelligent Maintenance of MEC 17
5.4.1 All-Round Monitoring of MEC 17
5.4.2 Automatic Locating of MEC Fault 19
5.4.3 MEC Service Quality Assurance 23
5.4.4 Intelligent Self-Healing of MEC Policies 23
5.5 Self-Maintenance Portal of MEC 24

6 Discussion of MEC O&M Modes 26
6.1 MEC O&M Scenarios 26
6.2 O&M Division Interface 27
6.3 O&M System 27
6.4 O&M Organization 28

7 Conclusion 30

8 Appendix 31
8.1 Abbreviations 31

1 Overview **5**

2 MEC Development Trend **5**

3 Features of MEC O&M Management **7**

4 Development of MEC O&M Management **8**

5 ZTE MEC O&M Management Solution **10**
5.1 ZTE MEC O&M Management System 10
5.2 Unpacking and Use of MEC Equipment 12
5.3 Agile Onboarding of MEC Applications 13
5.3.1 Automatic Orchestration of Application Resource 13
5.3.2 Agile Configuration of Application Policies 15
5.3.3 On-Demand Invoking of Application Capabilities 16
5.4 Intelligent Maintenance of MEC 17
5.4.1 All-Round Monitoring of MEC 17
5.4.2 Automatic Locating of MEC Fault 19
5.4.3 MEC Service Quality Assurance 23
5.4.4 Intelligent Self-Healing of MEC Policies 23
5.5 Self-Maintenance Portal of MEC 24

6 Discussion of MEC O&M Modes **26**
6.1 MEC O&M Scenarios 26
6.2 O&M Division Interface 27
6.3 O&M System 27
6.4 O&M Organization 28

7 Conclusion **30**

8 Appendix **31**
8.1 Abbreviations 31

FIGURES

Figure 2-1 MEC System Architecture..... 5
Figure 3-1 MEC Full-Lifecycle O&M Management 7
Figure 4-1 MEC Management Domain System Architecture 9
Figure 4-2 CCSA Management Domain System Architecture 10
Figure 5-1 ZTE MEC O&M Management Domain Architecture.....11
Figure 5-2 Out-of-the-Box Deployment Process of MEC 12
Figure 5-3 Automatic Onboarding of MEC Applications 13
Figure 5-4 Agile Configuration of Application Policies.....15
Figure 5-5 On-Demand Invoking of Capabilities 16
Figure 5-6 Alarm Root Cause Analysis Procedure.....17
Figure 5-7 Hierarchical Visual Monitoring of MEC 18
Figure 5-8 Alarm Root Cause Analysis Process.....20
Figure 5-9 Automatic Network Fault Diagnosis.....21
Figure 5-10 Log Exception Inspection.....22
Figure 5-11 MEC Service Log Analysis.....23
Figure 5-12 Self-Maintenance Portal of MEC.....25
Figure 6-1 MEC O&M Scenarios and Modes.....26

TABLES

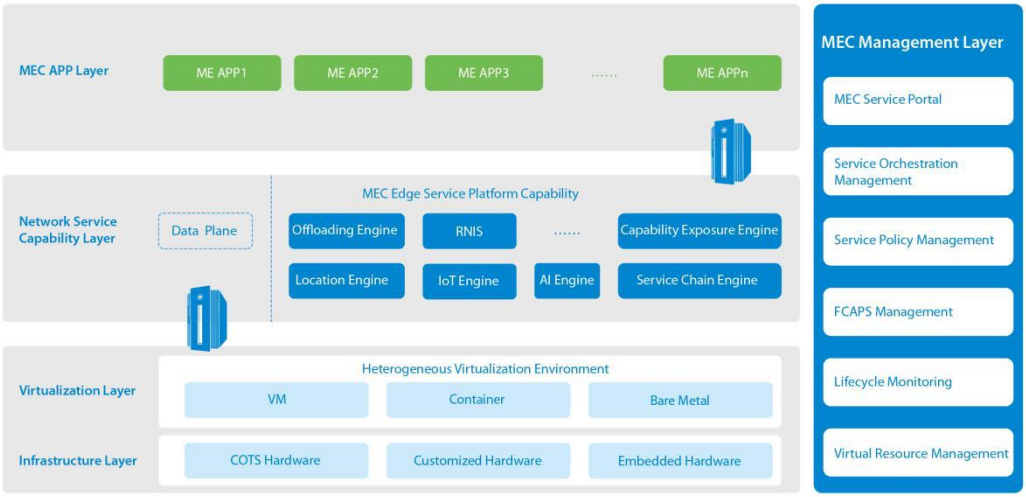
Table 6-1 O&M Organization.....28
Table 8-1 Abbreviations 31

1 Overview

With the large-scale deployment of 5G, more and more telcos take MEC as the key strategy. MEC, the extension of 5G networks, moves network capability to the edge. It can not only meet differentiated service requirements of vertical industries such as high bandwidth, low latency and massive connections, but also build a service ecosystem with integrated cloud and network by opening network capabilities and resource capabilities, bringing brand-new service experience and digital services to thousands of industries.

2 MEC Development Trend

Figure 2-1 MEC System Architecture



The MEC system includes cloud infrastructure, virtualization layer, network service layer, application layer, and MEC management layer. It is an end-to-end system of "network + cloud + capability" and adopts the deployment architecture based on edge network and computing, forming the aggregation point of edge computing and network. Based on the service capability layer, it opens hierarchical service capabilities such as network, resource, and platform. The trend of MEC commercial deployment and service development is as follows:

- Mass distributed deployments

Currently, industry application requirements are relatively clear and fixed, and MEC is usually deployed in cities or campuses. In the future, thousands of industries will raise differentiated and uncertain requirements for network applications, and MEC deployment will evolve from relatively fixed areas to national mass distribution. Take the Internet of Vehicles (IoV) and other industries for example, the site radius of MEC is usually smaller than 30 KM to meet the requirements of low latency and service continuity. However, the requirements of Internet services such as CDN and cloud games for MEC are usually relatively uncertain, and telcos need to provide nation-wide MEC computing resources on demand according to the dynamically changing service traffic.

- Multiple heterogeneous resource forms

The MEC resource layer bears CT NFs and IT applications of different industries. Therefore, the MEC infrastructure should not only meet the requirement of CT NFs for high forwarding, but also support the requirements of AI and video applications for GPU/FPGA acceleration and heterogeneous computing processing.

- Hierarchical service mode

The MEC platform has rich capabilities to implement rapid iteration and development of industry applications, enabling rapid launch of industry services. The MEC of integrated cloud and network not only provides the basic offloading service, but also provides edge cloud capabilities with more core value, including resource IaaS, network capability and platform PaaS. It leads telcos to transform from the traditional pipeline service to the hierarchical service mode.

- Asset ownership in multiple scenarios

Different from the traditional ToC network, MEC, as a part of the 5G ToB network, has such networking modes as sharing and dedicated. MEC assets can be divided into the following three scenarios:

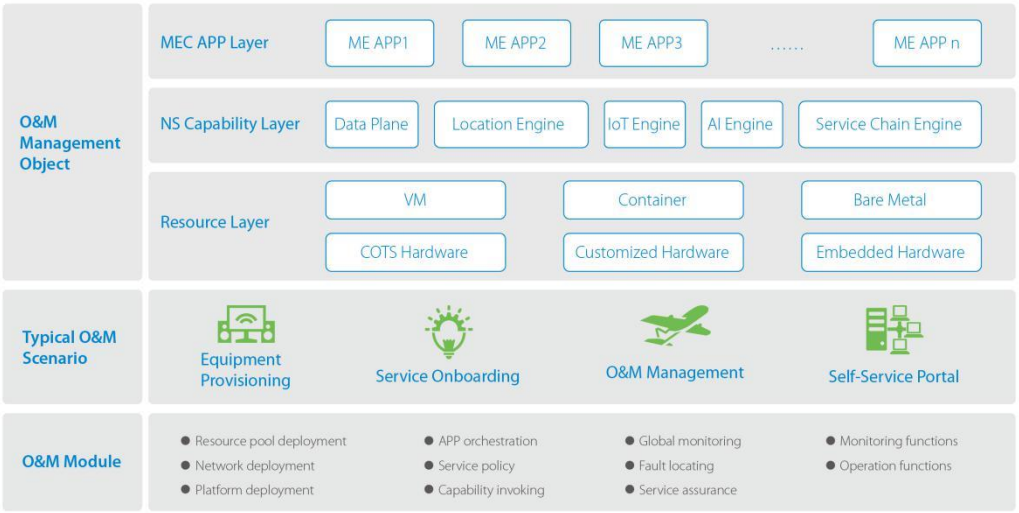
  - MEC equipment is deployed in the telco's equipment room, and the assets belong to the telco. It only provides integrated cloud and network capabilities for customers.
  - MEC equipment is deployed in the enterprise equipment room, and the assets belong to the telco, ensuring data security and reliability.
  - MEC equipment is deployed in the enterprise equipment room and the assets

belong to the enterprise.

The above three asset ownership scenarios bring new problems to management system construction and O&M modes.

3 Features of MEC O&M Management

Figure 3-1 MEC Full-Lifecycle O&M Management



MEC O&M management focuses on MEC resources, network platform capabilities, and applications, covering site commissioning, service launch, O&M management, self-maintenance, and other full-lifecycle management. Based on distributed deployment, heterogeneous resources and other MEC characteristics, how to introduce automatic and intelligent means in each O&M stage to support MEC to provide agile application deployment and reliable service guarantee for the ToB market, and finally achieve edge self-management is a common concern of telcos and industries.

- Automatic deployment of MEC devices

The rapid deployment of massive MEC devices at the edge will be the first problem for the large-scale MEC commercial use. MEC deployment involves computing, storage, network infrastructure, VM/container and other virtualized resources, and multiple layers such as UPF/MEP, requiring multi-domain coordination. The traditional mode with manual data design

and engineer on-site deployment usually takes about one week, which cannot meet the digital service development of thousands of industries.

- Agile onboarding of MEC applications

Building an open and agile edge ecosystem for industry applications is the key for MEC to provide digital services for industries. Firstly, MEC needs to provide agile deployment modes for differentiated applications to reduce the cloud access threshold of different applications. Secondly, the MEC ecosystem needs to provide flexible service policy configurations to quickly match different application requirements and provide rich edge capabilities for various applications on demand.

- Automatic MEC maintenance

Industrial control, IoV, and other industries impose strict requirements upon the reliability and maintenance SLA of the MEC system. In addition, MEC maintenance is faced with problems of decentralized nodes and remote locations. Automatic and intelligent methods need to be introduced to implement self-perception and self-management of MEC, preventing frequent O&M personnel visiting and reducing O&M costs.

- MEC self-maintenance portal

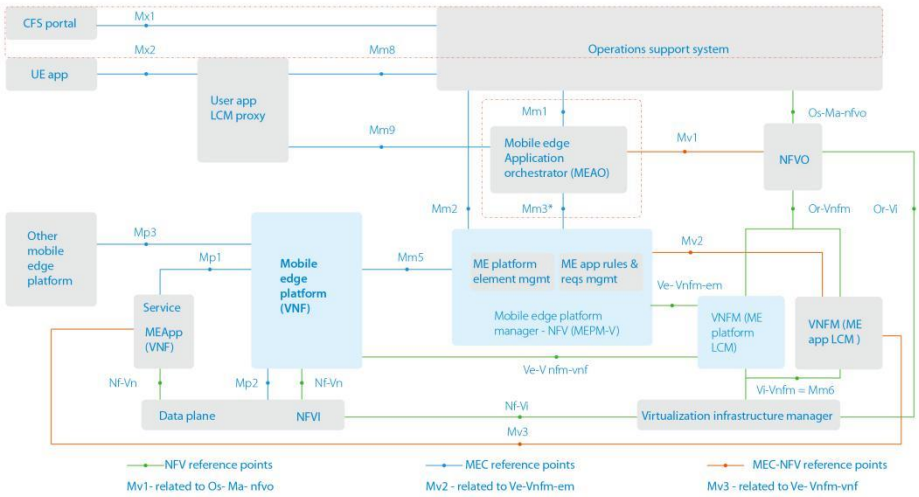
For industries with strong ICT technology capabilities, MEC is required to support self-maintenance and resource management. As the industry participates in application deployment, monitoring, and O&M, on the one hand, the maintenance efficiency can be improved, and on the other hand, end-to-end digital service perception can be guaranteed. In this O&M management mode, the corresponding O&M management interface must be opened in the MEC management domain to provide simple and easy-to-operate maintenance portals for industry customers.

4 Development of MEC O&M Management

MEC O&M management mainly complies with the 3GPP and ETSI specifications, which have defined the management system architecture and MEC application lifecycle management process.

- ETSI

Figure 4-1 MEC Management Domain System Architecture

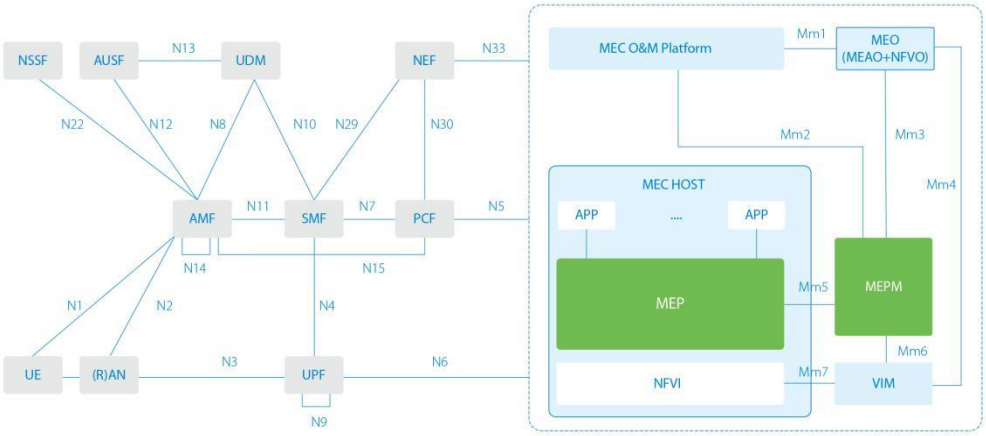


ETSI released the technical specifications of the MEC management system in 2016, focusing on MEC platform, network capability exposure, and MEC application operation and deployment. As shown in the above figure, on the basis of the original architecture of MANO, modules such as MEAO and CFS portal are introduced. The CFS portal is the entrance of telcos for industry subscription and monitoring edge applications. Together with the NFVO and MEPM, MEAO implements flexible configuration of MEC application resource orchestration and capability exposure.

- CCSA

Based on the progress of standards and the requirements of domestic industries, the China Communications Standards Association (CCSA) proposes the edge computing operation management platform, which is interconnected with the MEC management layer MEO and MEPM to implement MEC-oriented unified service, operation and O&M management functions, supporting the unified O&M of the MEC system.

Figure 4-2 CCSA Management Domain System Architecture

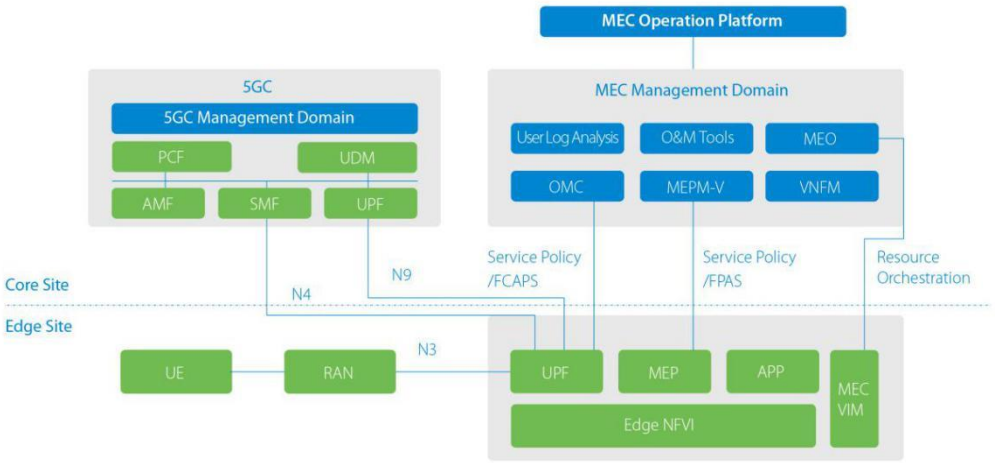


5 ZTE MEC O&M Management Solution

5.1 ZTE MEC O&M Management System

The 5GC in the core area focuses on the full lifecycle management of telecom NFs, while the MEC network on the edge node focuses on exposing network, service and O&M capabilities to industry applications. The two management systems are usually built separately.

Figure 5-1 ZTE MEC O&M Management Domain Architecture



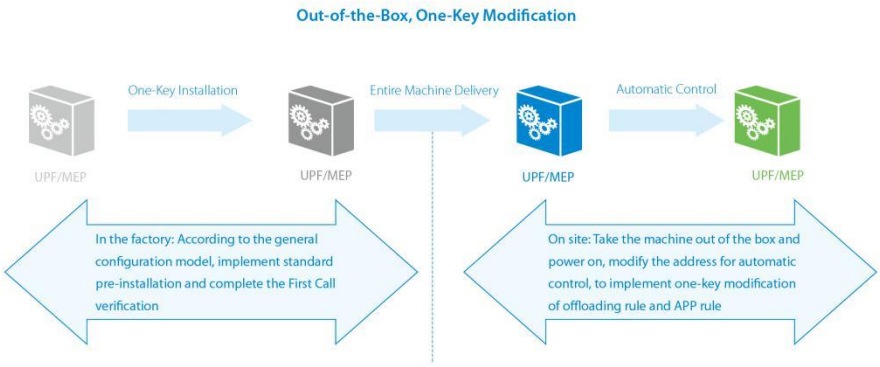
The edge management layer includes such systems as MEO, VNFM, OMC, MEPM, user log analysis and O&M tools. The MEC-oriented management provides the following functions.

- Unpacking and Use: The edge management domain MEO collaborates with the OMC and MEPM to provide automatic management and one-point configuration of the edge cloud, so as to implement the Unpacking and Use deployment mode of MEC and shorten the deployment period of MEC sites.
- Agile Onboarding: The MEO collaborates with the edge cloud to provide the model-driven orchestration and deployment mode, align with the application onboarding process of the public cloud, and provide deployment modes such as on-demand resource distribution, thus simplifying IT application deployment. In addition, as MEC is an integrated cloud and network ecosystem, the MEPM/OMC provides atomic capabilities such as network offloading and service strategy according to typical scenarios, to implement on-demand and one-click release of service strategies and to support the fast end-to-end onboarding of industry applications.
- Autonomous Management: In the face of MEC distribution, virtualization, and industry SLA differentiation, sophisticated automation and AI technologies of CT are introduced to provide global monitoring, active maintenance, and timely prevention, achieving edge autonomous management, thus effectively improving the maintenance efficiency of MEC and the end-to-end service quality of industry applications.
- Self-maintenance Portal: The industry and telcos are jointly responsible for the

maintenance of the MEC system based on the maintenance portal. The industry can monitor industrial applications and the service quality of associated resources, networks, and capabilities in real time, flexibly deliver resources, QoS, and other adjustment policies, achieving edge application self-maintenance and improving the O&M efficiency of MEC.

5.2 Unpacking and Use of MEC Equipment

Figure 5-2 Out-of-the-Box Deployment Process of MEC



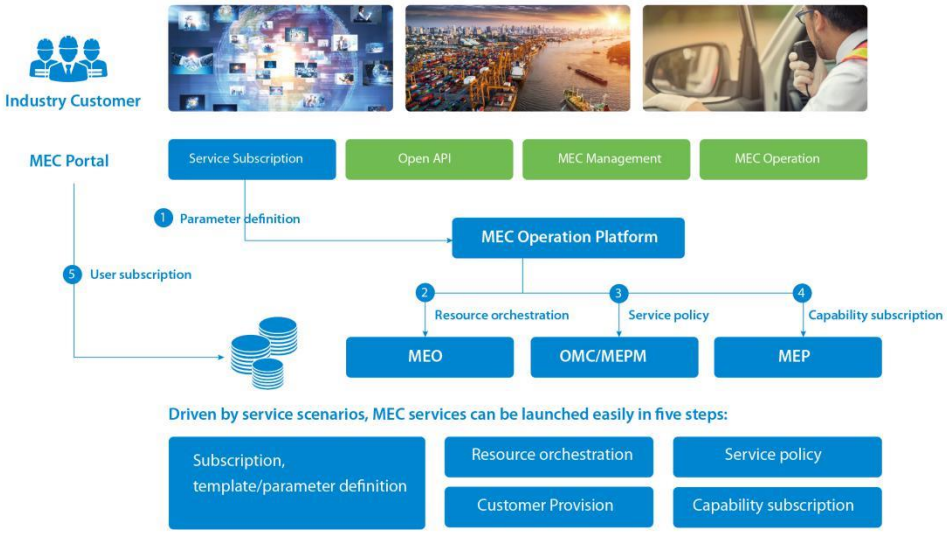
The MEC site commissioning procedure complies with standardized pre-configuration for general data and remote one-click configuration for personalized data, and supports plug-and-play and fast deployment of MEC equipment, shortening the onboarding period of MEC sites.

1. Standardized pre-installation: Before delivery, MEC equipment automatically completes the automatic installation of the standardized MEC operating environment and software and the standardized pre-configuration of general data.
2. One-click configuration: The pre-installed MEC equipment supports automatically accessing to the O&M management domain at the edge node. The edge O&M domain automatically designs the configuration script of MEC equipment according to the specific on-site environment, and configures the personalized office data through OMC and MEPM.
3. Automatic test: The edge management domain provides automatic test tools to encapsulate MEC test cases and tools. The O&M personnel select test cases in accordance

with different scenarios, and the system automatically implements end-to-end MEC service tests.

5.3 Agile Onboarding of MEC Applications

Figure 5-3 Automatic Onboarding of MEC Applications



The MEC management system links MEO, MEPM, and OMC systems. It provides resource orchestration, service policy activation and capability subscription functions for industry applications. For various edge application scenarios, MEC services can be onboarded easily in five steps.

5.3.1 Automatic Orchestration of Application Resource

The orchestration function of MEC management domain provides three deployment modes for different scenarios:

1. Model-driven automatic deployment, complying with the standard NFV architecture.
2. Simplified deployment to distribute resources directly, aligning with the public cloud.
3. Intelligent orchestration and deployment for the Internet services with uncertain requirements.

- Standard deployment mode

Following NFV's mature experience in cloud access, applications in different industries can abstract the resource model of application virtualization and container through the standard TOSCA/Helm chart model. The orchestration function of management domain has a built-in rich standard component library, and provides a wizard GUI to quickly design standard templates. Based on the model-driven orchestration concept, it can rapidly deploy industry applications in accordance with specified processes and interfaces.

- Simplified deployment mode

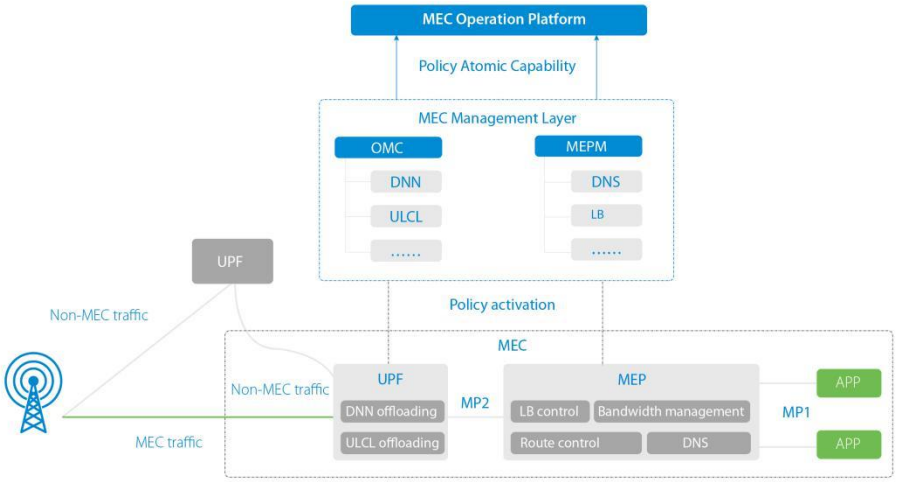
To enable flexible APP deployment for various industries, the orchestration function of management domain provides deployment modes like that of public cloud, which are more suitable for IT application deployment habits. Industry customers can select or customize resources, systems, and environments of edge applications through portals to enjoy secure and reliable infrastructure services.

- Intelligent deployment mode

The services of Internet companies, such as CDN and games, cover the whole country. MEC service traffic and node locations will change continuously according to the specific services. MEO provides intelligent deployment mode, which collects such data as MEC resources and service usage, comprehensively analyzes and deeply mines service changes for dynamic modeling. Among massive edge nodes, the best edge nodes are selected to deploy MEC services and applications, helping telcos implement efficient application orchestration, improving the service utilization of MEC and ensuring business profit.

5.3.2 Agile Configuration of Application Policies

Figure 5-4 Agile Configuration of Application Policies

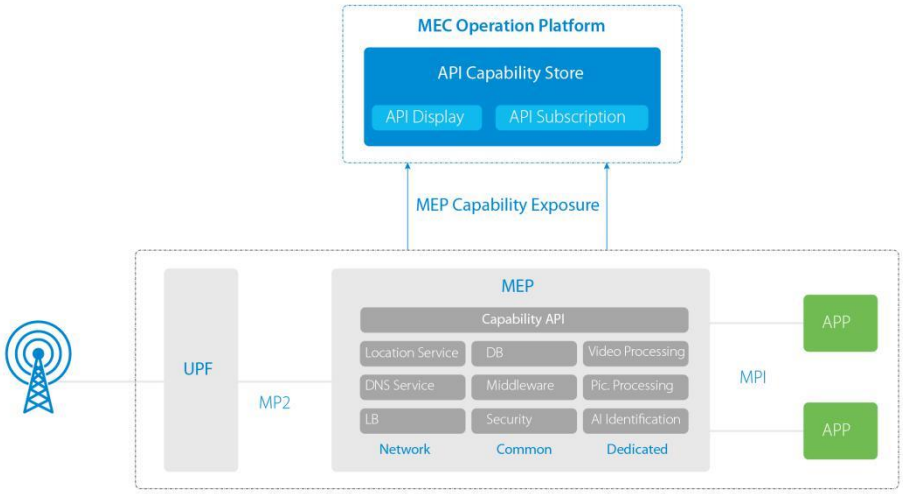


As the aggregation platform of 5G networks and services, MEC provides industry applications with network offloading, bandwidth management, DNS and more capabilities, and solves problems caused by the synergy of cloud and network such as network delay, congestion, and security. The edge UPF network triggers different policies such as DNN and ULCL based on DNN, service area and service flow to provide local offloading function for applications. In addition, the MEC platform provides applications with network capabilities such as DNS, load balancing, bandwidth adjustment, and TCP acceleration, to accelerate uplink and downlink data transmission and ensure reliability.

The MEC management domain provides a rich atomic edge capability library, including the above network policy configurations. The upper-level edge operation system can flexibly invoke these atomic capabilities, and combine them with commercial products to provide applications for various industries, to support the rapid onboarding of digital industry services, and to ensure excellent service experience for applications.

5.3.3 On-Demand Invoking of Application Capabilities

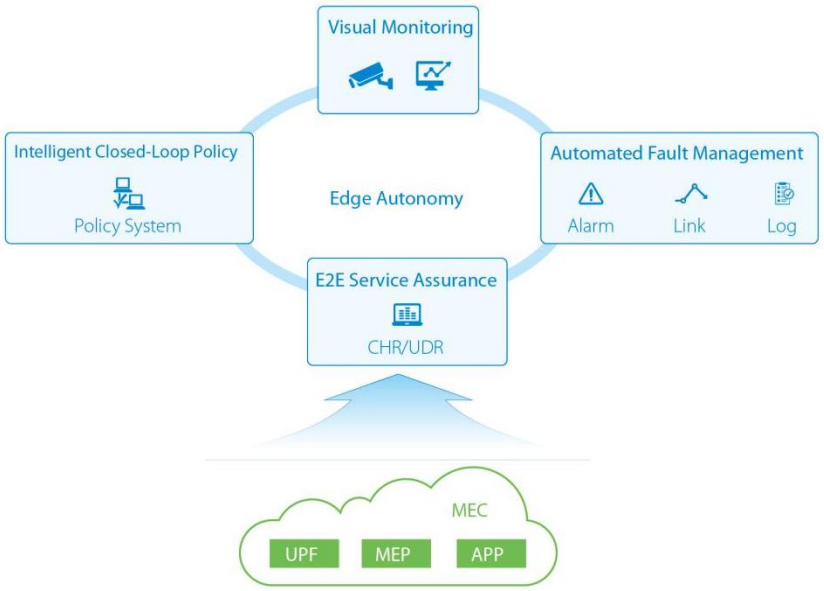
Figure 5-5 On-Demand Invoking of Capabilities



Based on the MEP platform, MEC provides industry customers with network, general or dedicated PaaS platform capabilities. The management domain, based on the capability exposure principle of "front-end store and back-end factory", provides on-demand capability and provides industry applications with greater edge core value. On the back end, after registering for various capabilities, the MEP provides simple and real-time API invoking interfaces based on capability APIs, and provides capability invoking authentication, statistics, and traffic control functions. At the front end, the MEC capability store presents open services and configuration descriptions in the MEC system to industry customers based on open back-end APIs, and provides a one-stop capability subscription entrance.

5.4 Intelligent Maintenance of MEC

Figure 5-6 Alarm Root Cause Analysis Procedure

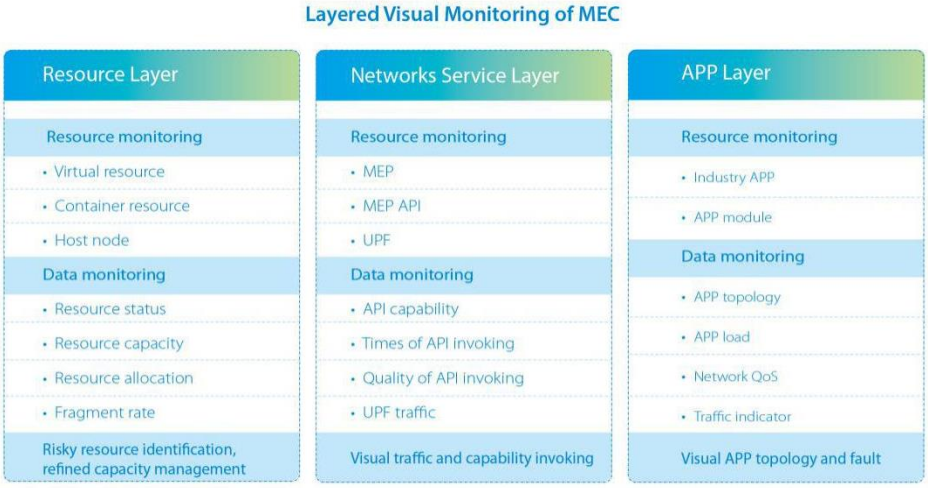


The MEC management domain introduces automatic and intelligent methods in four phases: MEC monitoring, troubleshooting, service assurance, and fault recovery. It implements edge autonomous maintenance, improves the maintenance efficiency of massive MEC nodes, and guarantees the service experience of MEC applications.

5.4.1 All-Round Monitoring of MEC

The MEC management domain implements hierarchical monitoring on three layers: resource layer, network service layer, and application layer. It provides multidimensional visual monitoring views of all MEC sites, helping O&M personnel of different maintenance teams understand the health status of global resources.

Figure 5-7 Hierarchical Visual Monitoring of MEC



- Resource layer monitoring

For massive and heterogeneous MEC nodes, the management domain system provides such monitoring methods as centralized monitoring of heterogeneous resources, streamline capacity management and risk resource identification:

- Based on the standard or enterprise standard, MEO is pre-matched with mainstream cloud resources, and compatible with heterogeneous computing frameworks such as CPU/GPU/FPGA, achieving unified management and centralized monitoring of distributed and ICT-integrated edge nodes.
- MEO collects baseline data such as global capacity, resource allocation and resource load, and makes a better and wiser decision on how to handle application scaling through peak value analysis and prediction analysis to ensure the balance between application performance and resource consumption.
- MEO monitors resources on TOP N load list, analyzes their running status and logs, and identifies resources at risk timely.

- Network service layer monitoring

The operation of the network service layer directly affects the service perception of MEC applications. The MEC management domain provides all-round monitoring for network pipes and capability exposure, thus improving the efficiency of APP fault delimiting. In terms of network pipelines, DPI data is used to monitor the traffic, rate and other indicators of

multidimensional applications such as terminal, location, NF and service. In addition, comprehensive history data analysis is used to identify abnormal indicators timely, so as to directly show which dimensions are the main factors affecting abnormal indicators. In terms of capability exposure, the system collects statistics on the number of API invocations, number of successful invocations, number of failures, and number of delays based on API types of the MEP, to better understand usage load and service quality of capability exposure and ensure better service experience.

- Application layer monitoring

To cope with dynamic changes such as virtualized resource elasticity and migration, the edge cloud provides visual application topology view. It supports top-down to drill and present the topology of applications, virtual resources and physical resources, and visually display physical locations of applications. In addition, it renders alarms and key performance data of resources on the topology, and presents the running health of applications in real time, helping the O&M personnel visualize and efficiently maintain various industry applications.

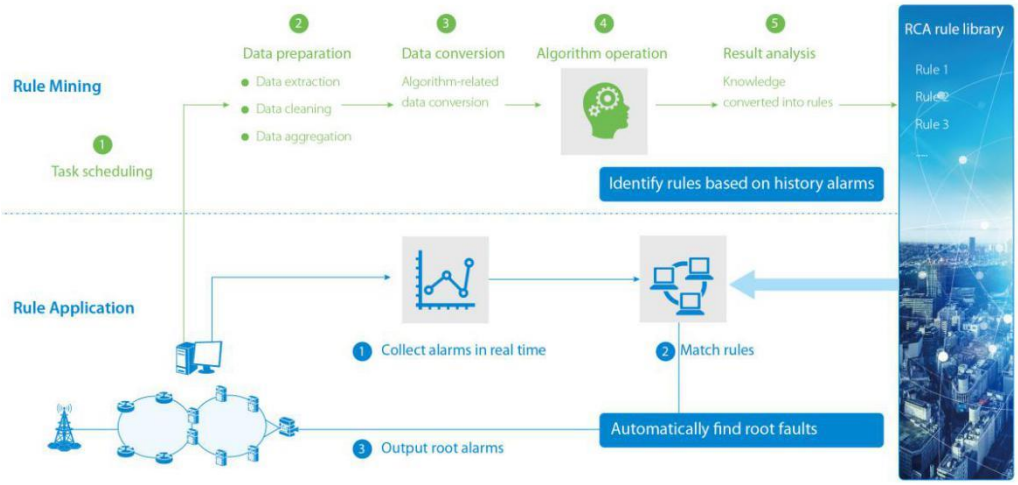
5.4.2 Automatic Locating of MEC Fault

For maintenance difficulties of MEC such as scattered locations and weak maintenance capabilities, the MEC management domain provides automatic methods such as alarm root cause analysis, network diagnosis, and log analysis to implement self-sensing and self-management of MEC faults, to maximally improve MEC maintenance efficiency.

- Automatic alarm root cause locating

The MEC system uses a virtualized and hierarchical network architecture. Troubleshooting involves lots of cross-domain and cross-layer alarm association analysis, making it difficult to manually locate alarm root causes. The alarm RCA function analyzes the logical relationship of massive NF alarms in real time, and automatically traces root causes. The RCA alarm function includes RCA rule mining and RCA rule application.

Figure 5-8 Alarm Root Cause Analysis Process



1) RCA rule establishment

Training-based RCA rule mining includes the following steps:

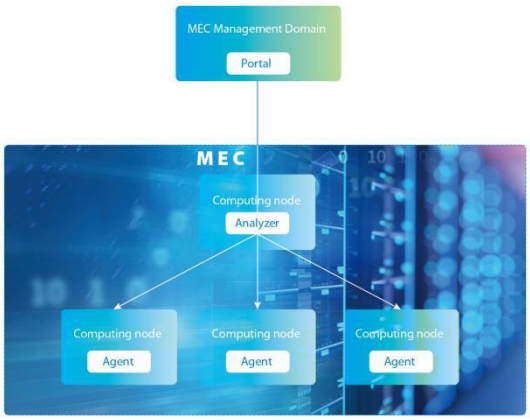
- Data extraction, involving alarm, statistics, and configuration data collection.
- Data cleaning, to remove invalid data.
- Format normalization and data fragmentation, to split alarms into different transactions based on time and resource bearer relationships, forming transaction data sets for associated mining.
- Algorithm operation: Association analysis is used to find all frequent item sets that meet the minimum support level, and then strong association rules are generated based on the frequent item sets and confidence level. After a association rule is generated, it is converted into a rule and released to the rule library, and then deployed to the production system. If a bottom-layer hardware component is removed, services on the VM layer are unavailable and connections are interrupted, resulting in VM failure and affecting services on the upper layer. Based on the resource relationship, alarm code, and time window, the system can comprehensively determine and establish the primary-secondary alarm relationship through the AI algorithm.
- Result analysis: In accordance with a certain internal rule and the obtained knowledge, create an RCA rule and store it in the RCA rule library.

2) RCA rule application

The MEC management domain monitors MEC resource data and configuration data in real time, and uses RCA rules to comprehensively judge alarm data, resource data, service bearer relationship, and time sequence of the existing network, to find out the real root cause in the network, and automatically repair or present the data to the O&M personnel for repair.

- Automatic network fault diagnosis

Figure 5-9 Automatic Network Fault Diagnosis



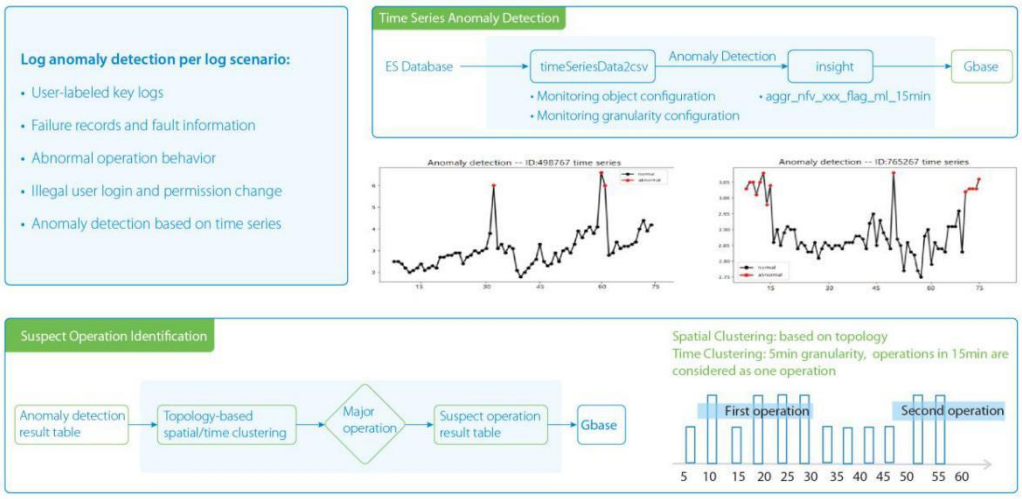
After virtualization and containerization technologies are introduced, the MEC network faces many difficulties such as complicated topology, dynamic changes, and long forwarding paths. The MEC management domain introduces automatic network analysis tools to collect the topology and operational status of each compute node in real time based on the Agent, and aggregates the data to the analysis node to provide network topology, automatic troubleshooting, and remote packet capture functions.

- Visual topology: Provides inner-host, inter-VM, and physical topology views inside the MEC site, and renders the information of faulty nodes, achieving visual network and visual fault.
- Automatic troubleshooting: Automatically delimits fault areas and causes through path analysis, operational status, and flow table statistics.
- Remote packet capturing: Captures packets remotely through the agent of host, and

analyzes traffic to automatically locate the fault cause.

- Log analysis for fault prevention

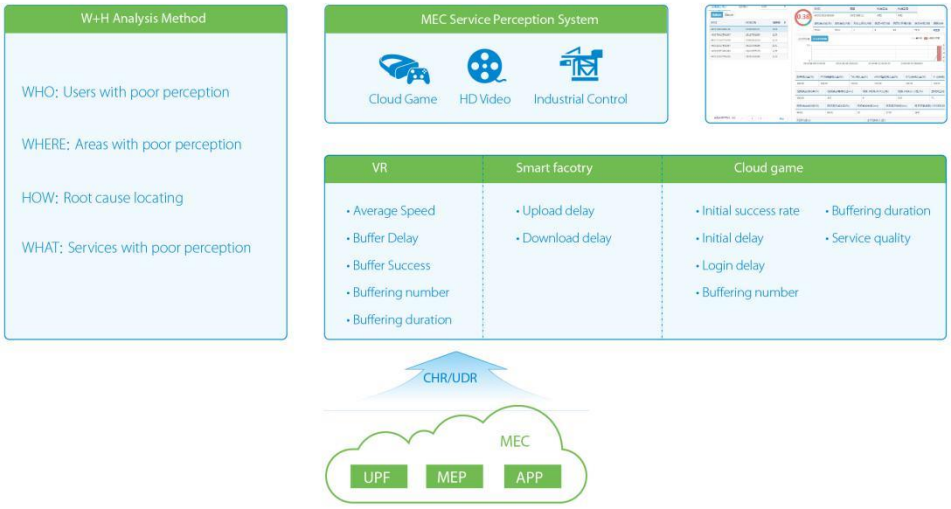
Figure 5-10 Log Exception Inspection



The contents of device logs are more detailed and comprehensive than alarms. The log system triggers log exceptions through the built-in expert library or rules discovered through intelligent means. In accordance with actual scenarios, the system provides methods such as suspected operation identification and time sequence error detection to detect system exceptions in advance and prevent risks from occurring.

5.4.3 MEC Service Quality Assurance

Figure 5-11 MEC Service Log Analysis



MEC service experience is vital to telcos and is the basis of industry innovation and collaboration. The service analysis system of MEC management domain establishes the key indicator system according service scenarios, and establishes the intelligent service quality assurance solution according to the "W+H" process. First, a key indicator system including latency, packet loss rate, and speed is established for typical MEC scenarios such as cloud games, HD videos, and industrial control. It collects signaling and forwarded data through software collection and hardware collection. The system flexibly mines and analyzes massive data based on OLAP and other technologies, collects statistics of cells, terminals, and service types, and analyzes service exceptions to locate problems that affect service indicators. During the locating process, the system can drill down each result to automatically identify the root cause of service indicator degradation.

5.4.4 Intelligent Self-Healing of MEC Policies

MEC sites are usually located in a remote equipment room and has a relatively weak maintenance capability. The O&M management domain recovers faults at the resource layer and application layer hierarchically through the policy system to ensure optimal service experience. The MEC network policy architecture includes the following functional modules:

- AI + data engine: It introduces model training and application of big data analysis and

machine learning, and provides intelligent analysis and policy decision capabilities for the MEC network. Its main functions include collecting network data and service data, performing AI analysis, and pushing AI data analysis results to the policy decision module and service platform.

- Policy decision module: It receives AI data analysis results from the AI engine, generates execution policies based on such results, and sends them to the policy execution module and service platform.
- Policy execution module: It is divided as resource-layer operation management system and network-service-layer EMS support. As the source of network data, it provides mass data to the AI engine for data analysis. As the strategy executor, it also obtains policy information from the policy decision module and executes it locally.

The MEC policy system implements intelligent closed-loop fault processing, including automatic bandwidth adjustment and elastic expansion scenarios.

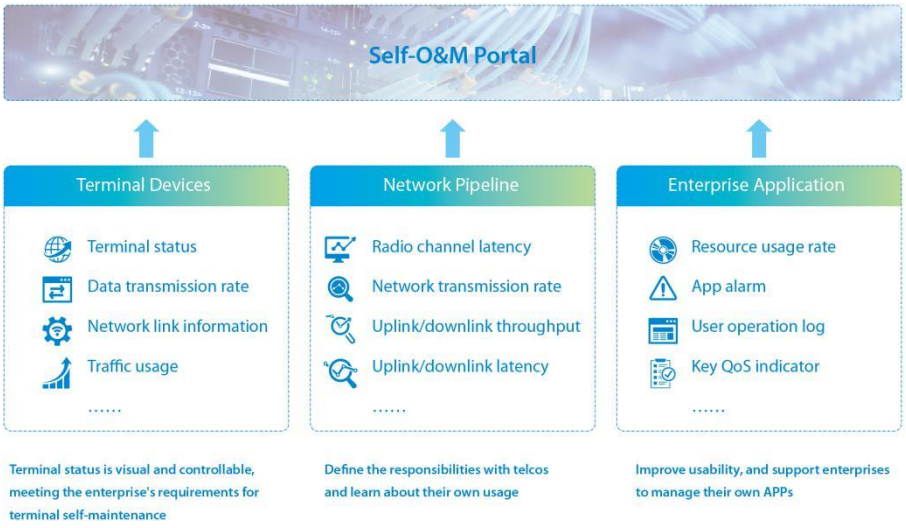
- Automatic bandwidth update: In a video monitoring scenario, when the policy center detects that the video service bandwidth reaches the upper threshold limit, and it instructs the MEP platform to update the service bandwidth threshold to adjust the application bandwidth capability.
- Elastic expansion: When the policy center detects that the overall performance indicator of the edge UPF reaches the upper threshold limit and needs to expand the processing capability of the media-plane NF, it delivers an NF update operation request to perform capacity expansion by increasing the number of VMs on the NF.

5.5 Self-Maintenance Portal of MEC

In addition to telcos, enterprises also need to participate in MEC network management to implement better network O&M through coordination. Telcos focus on deployment, in-depth maintenance, and other operations with high technical requirements. Enterprises focus on managing their own applications and terminals, and monitoring network conditions, with low requirements for O&M personnel skills. As an enterprise O&M system, the self-maintenance portal can support efficient enterprise O&M, manage enterprise terminals and APPs, and assist in network O&M.

The self-maintenance portal provides multi-layer O&M for terminals, network channels, and enterprise applications, and provides comprehensive network monitoring and intelligent location analysis, helping users accurately understand network service quality, rapidly troubleshoot network faults, and ensure stable service operation.

Figure 5-12 Self-Maintenance Portal of MEC



- Monitors the operational status, device traffic, and link quality of terminals.
- Monitors the resource and status of network channels, such as wireless channel delay, transmission rate, and API invocation.
- Monitors various indicators of enterprise applications, such as application network performance, user security logs, QoS indicators, and threshold alarms.

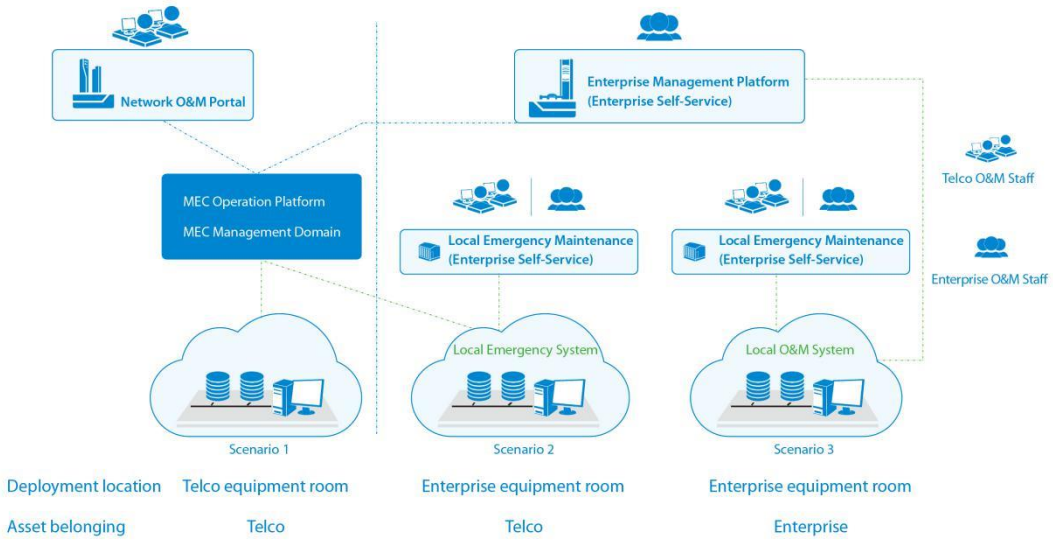
Different from telcos' O&M systems, the enterprise self-maintenance portal has more simplified functions and more flexible display, greatly reducing enterprises' O&M pressure.

- Simplified functions: Only basic functions such as network performance, resource monitoring, and alarm processing are provided, and complex network operations such as NF instantiation and service configuration are not included, thus reducing enterprises' O&M pressure
- Simplified interface: The system supports user-defined large screen metrics, such as displaying only TOP N metrics or only displaying the service SLA concerned by the enterprise.

6 Discussion of MEC O&M Modes

6.1 MEC O&M Scenarios

Figure 6-1 MEC O&M Scenarios and Modes



In accordance with different requirements of vertical industries for network and data security, MEC can be deployed at different locations. Depending on device deployment location and asset classification, there are multiple O&M scenarios:

- Scenario 1: Deployed in a telco's equipment room and the assets belong to the telco.
- Scenario 2: Deployed in an enterprise's equipment room and the assets belong to the telco.
- Scenario 3: Deployed in an enterprise's equipment room and the assets belong to the enterprise.

For the above O&M scenarios, they require different corresponding O&M division interface, O&M system architecture, and O&M organization.

6.2 O&M Division Interface

The O&M division interface is based on different industry features. In different O&M scenarios, the O&M responsibilities of telcos and enterprises are divided as follows:

- Scenario 1: Industries such as HD video and media playing have service features of many nodes and high bandwidth. Because the system is provided by the telco, the telco is responsible for the maintenance of the MEC resource layer and network service layer. Industry customers are mainly responsible for the maintenance of MEC applications. The telco can also provide application maintenance hosting services. In addition, the telco can provide enterprise monitoring portals to monitor the edge resources subscribed by enterprises, thus ensuring the normal operation of enterprise applications.
- Scenario 2: Industries such as ports and mines have the characteristics of low latency and local service data remaining. Because edge assets belong to telcos, the O&M division interface is basically the same as that in scenario 1. However, because devices are deployed in the enterprise's equipment room, local emergency O&M personnel should be available in the enterprise, so that O&M operations can be completed as soon as possible in case of disasters.
- Scenario 3: Industries such as electricity have the characteristics of complete network isolation. In this case, enterprises usually purchase MEC devices by themselves, and O&M must be completed locally. The industry has abundant ICT maintenance capabilities. In this scenario, enterprises can perform end-to-end integrated maintenance of the resource layer, network service layer, and application layer, and professional equipment vendors or telcos can assist to solve difficult problems and operations.

6.3 O&M System

Following the principle of "reliable system and efficient maintenance" and facing different O&M scenarios, the MEC O&M system can adopt the following architecture:

- Scenario 1: An edge management domain system is built for the telco's network to implement centralized management on distributed MEC sites. In addition, a

maintenance portal is provided for industry customers, including application indicator monitoring, application policy changes, and resource scheduling, to facilitate independent maintenance and application in the industry.

- Scenario 2: In addition to the centralized edge management domain system of the telco, a local lightweight emergency maintenance system can be configured at the enterprise due to the remote location of MEC site. When the link between the MEC and the telco's NM system is broken, emergency local maintenance functions can be provided, including system restart, reset, and re-deployment, so that emergency faults on the MEC can be handled locally to recover services quickly.
- Scenario 3: In line with the security principle that enterprise data is not delivered out of the campus, MEC devices in the enterprise are not connected to the telco's centralized management systems. A separate local maintenance system in the enterprise is required for daily O&M, providing integrated full lifecycle management functions such as MEC deployment, policy configuration, monitoring and maintenance. In addition, a simple and easy-to-use self-service O&M portal is provided to implement simple and efficient maintenance of the MEC system.

6.4 O&M Organization

According to the current development of telcos, O&M organizations usually take responsibilities in different fields. The division of organizations and departments is clear, and the process is clear. However, O&M organizations of different enterprises in different industries do not have clear division of work. Therefore, they can use the maintenance process of telcos for reference, and reuse their organization and personnel. The above scenarios 1 and 2 are operator-leading O&M modes. Combining with MEC project practices, the following sector is going to discuss the general MEC O&M organization modes in the two scenarios based on the telco’s O&M system.

Table 6-1 O&M Organization

O&M Stage	O&M Content	O&M Organization
Service Provision	Service product design, service provision	MEC operation team

Equipment Deployment	Solution design, resource layer / network service layer deployment	VNF/APP team NFVI team
APP Onboarding	APP deployment, APP policy deployment	APP team
Monitoring & Troubleshooting	Resource layer / network service layer maintenance	APP team NFVI team
	APP maintenance	APP team

- Service provisioning: Different from the service provisioning of the traditional ToC network, MEC service provisioning parameters involve network requirements of key features such as the number of users, latency, reliability and security. The MEC operation team plans and designs replicable service products and parameters according to the requirements of different industry customers, so that industry customers can flexibly subscribe related services through the enterprise portal.
- Equipment deployment: As the telecom network evolves into the virtualization network, the telco's virtualized core network O&M organization evolves into horizontally layered teams including VNF/APP team and NFVI team, exploiting the advantages of agility and openness of the NFV network. The deployment of MEC equipment involves core network, private cloud, public cloud and other O&M specialties, and can copy the layered NFV architecture, to meet the requirements for rapid MEC service growth.
- APP onboarding: IT APP onboarding includes APP orchestration and policy configuration. Compared with the traditional CT APP onboarding, it faces many difficulties, such as multiple vendors, lack of specifications and insufficient maintenance experience. An MEC APP team is needed to work with industry partners, to lead the full lifecycle process of APP onboarding, such as requirement communication, pre-integration, deployment and policy activation, and formulate the process of APP onboarding, so as to better promote MEC construction and operation.
- Monitoring and troubleshooting: Complying with the rule of layered NFV O&M, the NFVI team and VNF/APP team are respectively responsible for the monitoring, troubleshooting and maintenance of MEC infrastructure, edge network and service platform. The MEC APP team provides the VNF/APP monitoring and fault closed-loop services, while the equipment vendor, telco and integrator can provide consulting,

technical support and other professional services. Based on the integrated maintenance system of the telco, an efficient O&M mode with one-point response and full-process support is established for digital industry services.

7 Conclusion

As an extension of the 5G network, MEC brings brand-new service experience and digital services to all industries. In terms of MEC O&M management, telcos need to comprehensively consider cloud, mobile networks, and vertical industries to build a coordinated O&M system, so as to provide industry customers with rich edge service capabilities and efficient maintenance assurance methods. At the same time, enterprises can establish simple and easy O&M systems to meet the requirements of industry service development.

The MEC management domain provides such means as "automatic resource orchestration, one-click policy configuration and on-demand capability invocation" to build the MEC into an agile cloud network service ecosystem, quickly empowering different industry applications, leading the new 5GC business models with new experience and new services. In addition, due to scattered MEC nodes and differentiated scenarios, automatic and Intelligent maintenance means are introduced to the MEC management domain, reducing the O&M complexity and achieving efficient edge autonomous management.

MEC O&M mode is upgraded from traditional telco maintenance to collaborative maintenance by telcos and industries. Industry customers can implement automatic APP deployment, policy adjustment, and flexible capability invocation through the maintenance portal, further improving the MEC O&M efficiency and activating the 5G upstream and downstream collaboration efficiency.

ZTE works with telcos and industry partners to build an easy-to-maintain, manageable, intelligent and simplified MECO&M system to drive the MEC to become a more intelligent and agile ICT platform, to embrace the real burst of various industry services with large bandwidth, low latency, and massive connections. ZTE is going to make greater contributions to building a communication-centric ecosystem.

8 Appendix

8.1 Abbreviations

Table 8-1 Abbreviations

Abbreviation	Description
3GPP	3rd Generation Partnership Project
API	Application Programming interface
CFS	Customer Facing Service
CDN	Content Delivery Network
DNN	Content Network Name
DPI	Deep Packet Inspection
ETSI	European Telecommunications Standards Institute
FPGA	Field Programmable Gate Array
GPU	Graphic Processing Unit
MEC	Multi-access Edge Computing
MEO	MEC Orchestrator
MEP	MEC Platform
MEPM	MEC Platform Manager
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
OSS	Operations Support System
OMC	Operation and Maintenance Center
SLA	Service-Level Agreement
RCA	Root Cause Analysis
VNF	Virtualized Network Function
VNFM	Virtualized Network Function Manager
UPF	User Plane Function
ULCL	Uplink Classifier