ANL Assessment and evidences of China Mobile on GB1059B

April 2025

Evaluation Result Analysis

				Evaluation
High-Value Scenario	**Cognitive Activity (IAADE)**	**Service Capability**	**Weight**	**Guangdong**
Core Network - Fault Management	**Awareness**	Data collection Alarm correlation	10%	A
	Analysis	Fault identification	10%	A
		Risk prediction	10%	A
		Demarcation	15%	A
		Locating	15%	A
	Decision	Failure recovery solution generation	10%	A
		Solution pre-verification	10%	**B**
	Executions	Solution implementation	10%	**B**
		Service verification	10%	A
				3.6

				Evaluation
High-Value Scenario	**Cognitive Activity**	**Service Capability**	**Weight**	**Guangdong**
Core Network - Stability	**Basic stability**	Stable deployment architecture	10%	**B**
		Control plane disaster recovery	15%	A
		User-plane disaster recovery	15%	A
		Infrastructure disaster recovery	15%	**B**
		Anti-signaling surge capability	15%	A
	Intelligent stability	Risk prediction	15%	A
		Service degradation recovery	15%	**B**
				3.6

- The score in fault management is 3.6, which is attributed to the signaling storm prevention and control capability of MAE-MDAF, the intrinsic intelligence capability of VNFs on the live network, and the automation capability of O&M devices on the live network.
- The score in stability is 3.6, which is attributed to the stable architecture and good DR capability of VNFs on the live network.
- Currently, the shortcoming is that solution confirmation and implementation must be performed manually. The improvement point is that intelligent O&M needs to continuously evolve to achieve E2E automation without manual intervention.
- It is planned to reach AN L4 in 2027 to achieve E2E automation.

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 1 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Data collection Alarm correlation	10%	Does your system automatically collect data? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. The system can automatically collect data (alarms, configuration data, and performance data etc.) and sort alarms. The data should be at the module level, including NF modules, cloud OS (VMs or pods), hardware (hosts and ports), detected KPIs indicating slight service damage (e.g., service KPI deterioration < 5%) and infrastructure-layer hardware data (servers, storage devices, EOR/TOR devices and IP core).	The system can automatically collect data (alarms, configuration data, and performance data), associate alarms, and sort alarms. The data should be at the VNF level and cloud OS (VMs or pods).	No. The system supports manual data collection.	

This question evaluates whether the core network fault management system can automatically collect network data and the detailed level of the collected data.

Guangdong uses the fault center and eSight to automatically collect data (such as alarms, configuration data, and performance data) and correlate and sort alarms. The collected data is module-level data, including NF data, cloud OS (VM or pod) data, hardware (host and port) data, KPIs indicating slight service loss (for example, service KPI deterioration < 5%), and infrastructure-layer hardware data (server, storage, EOR/TOR, and IP core data).

Example evidence for option A:

Figure 1

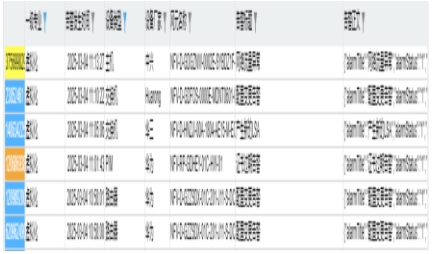


Figure 2

Figure 3

Figure 4

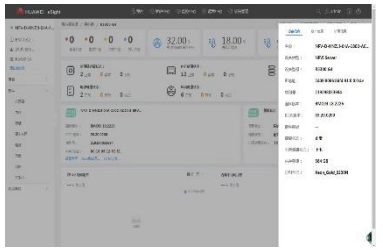


Figure 5

Figure 6

- As shown in Figure 1 and Figure 2, the fault center can automatically collect device alarms and monitor the device running status in real time. The alarm system monitors the device status in real time, associates and sorts alarms, and preferentially handles alarms of key devices to ensure that core services are not affected.
- As shown in Figure 3, the performance alarm page displays detailed performance data and alarms. The system continuously monitors performance counters. When the value of a performance counter is close to or exceeds the preset threshold, the system automatically triggers an alarm, reminding O&M personnel to promptly take measures to prevent performance deterioration.
- Figure 4 shows the alarms of infrastructure-layer devices. You can view the infrastructure-layer hardware data (server, storage, EOR/TOR, and IP core data).
- Figure 5 shows eSight for the infrastructure layer, which can display the infrastructure-layer data in real time.
- Figure 6 shows the KPIs indicating slight service loss.

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 2-1 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C
Fault identification	10%	Does your system support fault identification and visualization related to the core network status? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs) NOTE 1: "Degraded" is an intermediate state indicating that the network functions are abnormal, but not completely faulty. The example causes of NF degradations include the following: Packet loss occurs on host NICs; packet loss occurs on TOR/EOR switches; faults occur on CPU and memory resources. NOTE 2: Fault identification is used to provide detected exception information related to the network and services based on multiple data sources.	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on multiple data sources (alarms, KPIs, heartbeat messages, and identified issues etc.). The system can compress the number of alarm notifications and provide the aggregated alarms. Fault management supports visualization of the following management capabilities in one view of VNFs/NFs and the telecom cloud. 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud 4. Information of telecom cloud infrastructure, including server (CPU, memory, NIC) information, storage information, storage controller/storage port information, vNIC information and rack information	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on alarms or KPIs. The system can identify and filter out redundant alarm notifications and related tickets based on pre-defined rules. Fault management supports visualization of the following management capabilities: 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud	No. The system supports manual fault detection based on the alarm notification and KPIs.

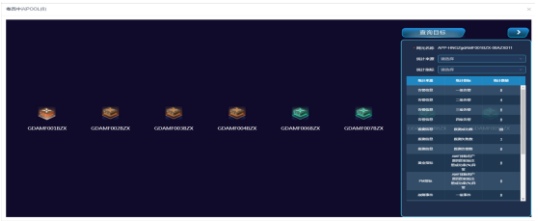
This question evaluates whether the core network fault management system can identify faults and visualize device health status.

The core networks in Guangdong use the fault center to support automatic fault detection and identification based on multiple data sources (alarms, KPIs, heartbeats, and identified issues), as well as alarm aggregation and compression in fault scenarios. In addition, the core network workbench and network cloud management system (eSight/FusionStage) are used to support unified, visualized fault management for VNFs/NFs and the telecom cloud, including VNF status/health visualization, network cloud VM/pod/server/storage/port/rack information visualization, and fault visualization.

Example evidence for option A:

Monitoring: The fault center automatically identifies root alarms, compresses and filters alarms, and automatically identifies correlative alarms and generates alarm correlation rules.
The fault center analyzes the mode and frequency of correlative alarms to predict potential fault risks and take measures in advance.—Support 0

MAE-MDAF: The health status of VNFs is visualized based on multi-source data.—Support 1



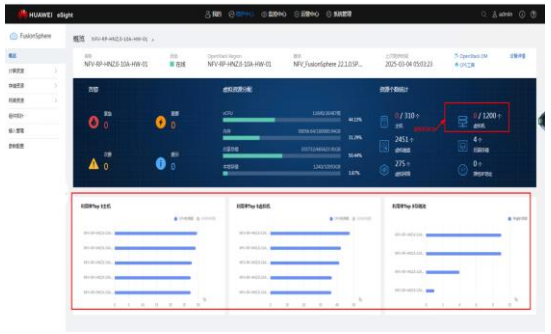
Core network workbench: Faults are automatically detected and identified based on multiple data sources (alarms, KPIs, fault events, logs, and dialing tests), alarms are aggregated, and topology views are provided to visually manage VNF object status and VNF health status.—Support 1 and Support 2

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 2-2 A)

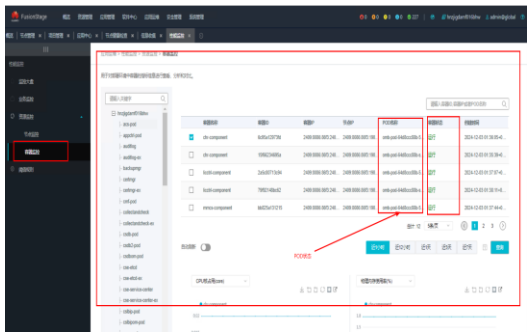
Capability or Task	Weight	Questions	Option A	Option B	Option C
Fault identification	10%	Does your system support fault identification and visualization related to the core network status? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs) NOTE 1: "Degraded" is an intermediate state indicating that the network functions are abnormal, but not completely faulty. The example causes of NF degradations include the following: Packet loss occurs on host NICs; packet loss occurs on TOR/EOR switches; faults occur on CPU and memory resources. NOTE 2: Fault identification is used to provide detected exception information related to the network and services based on multiple data sources.	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on multiple data sources (alarms, KPIs, heartbeat messages, and identified issues etc.). The system can compress the number of alarm notifications and provide the aggregated alarms. Fault management supports visualization of the following management capabilities in one view of VNFs/NFs and the telecom cloud. 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud 4. Information of telecom cloud infrastructure, including server (CPU, memory, NIC) information, storage information, storage controller/storage port information, vNIC information and rack information	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on alarms or KPIs. The system can identify and filter out redundant alarm notifications and related tickets based on pre-defined rules. Fault management supports visualization of the following management capabilities: 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud	No. The system supports manual fault detection based on the alarm notification and KPIs.

This question evaluates whether the core network fault management system can identify faults and visualize device health status.

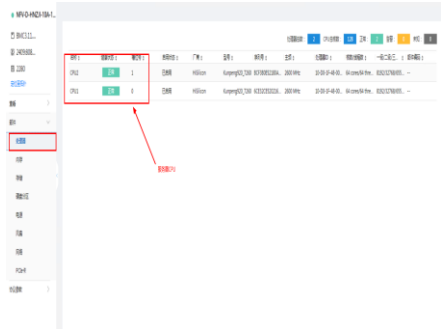
Example evidence for option A:



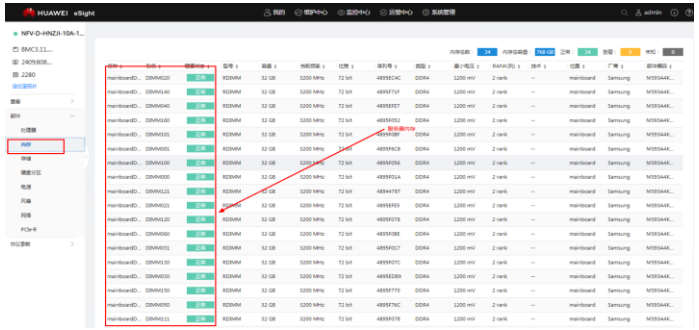
The status of VMs in a resource pool can be viewed.—Support 3



The pod status of VMs in a resource pool can be viewed.—Support 3



The CPU status of servers in a resource pool can be viewed.—Support 3



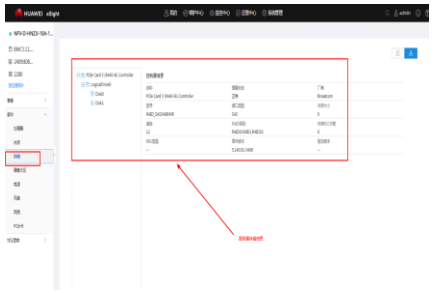
The memory status of servers in a resource pool can be viewed.—Support 4

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 2-3 A)

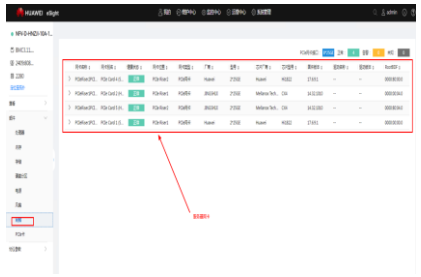
Capability or Task	Weight	Questions	Option A	Option B	Option C
Fault identification	10%	Does your system support fault identification and visualization related to the core network status? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs) NOTE 1: "Degraded" is an intermediate state indicating that the network functions are abnormal, but not completely faulty. The example causes of NF degradations include the following: Packet loss occurs on host NICs; packet loss occurs on TOR/EOR switches; faults occur on CPU and memory resources. NOTE 2: Fault identification is used to provide detected exception information related to the network and services based on multiple data sources.	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on multiple data sources (alarms, KPIs, heartbeat messages, and identified issues etc.). The system can compress the number of alarm notifications and provide the aggregated alarms. Fault management supports visualization of the following management capabilities in one view of VNFs/NFs and the telecom cloud. 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud 4. Information of telecom cloud infrastructure, including server (CPU, memory, NIC) information, storage information, storage controller/storage port information, vNIC information and rack information	The system supports automatic fault detection and identification and alarm aggregation in fault scenarios based on alarms or KPIs. The system can identify and filter out redundant alarm notifications and related tickets based on pre-defined rules. Fault management supports visualization of the following management capabilities: 1. VNF object (5GC NFs and EPC VNFs) status (faulty or normal) visualization 2. VNF health status (degraded and overloaded) visualization 3. Visualized status (faulty or normal) of VMs and pods in the telecom cloud	No. The system supports manual fault detection based on the alarm notification and KPIs.

This question evaluates whether the core network fault management system can identify faults and visualize device health status.

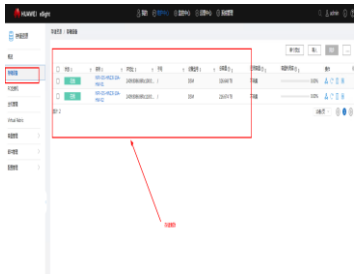
Example evidence for option A:



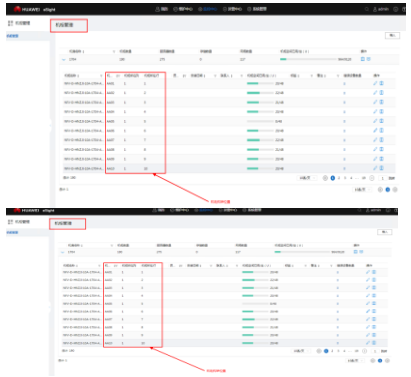
The storage status of servers in a resource pool can be viewed.
—Support 4



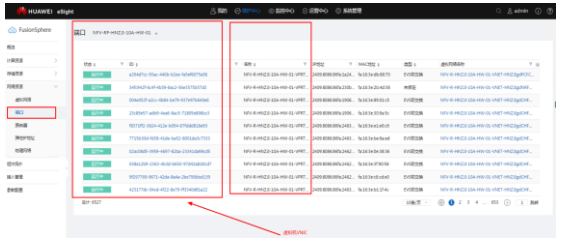
The NIC status of servers in a resource pool can be viewed.
—Support 4



The port status of storage servers in a resource pool can be viewed.
—Support 4



The locations of cabinets and racks in a resource pool can be viewed.
—Support 4



The vNIC status of VMs in a resource pool can be viewed.
—Support 4

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 3 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Risk prediction	10%	Does your system automatically detect and prevent risks of VNF faults? Assessment object: management entities Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. The system can use intelligent risk identification to recognize potential faults and automatically prevent faults. It can: 1. Prevent potential risks and analyze the risks involving capacity, links, signaling storms, DR, and hardware. 2. Analyze the cause of risks and provide recommended actions automatically.	The system can use automatic risk identification, which requires manual confirmation, to recognize potential faults and prevent faults. It can: 1. Prevent potential risks and analyze the risks involving capacity and links.	The system can use risk identification to recognize potential faults and prevent faults by providing an automatic checklist which requires engineers to periodically confirm the potential risks in this checklist. It can: 1. Prevent potential risks and analyze the risks involving capacity.	No. The system does not support risk prediction.

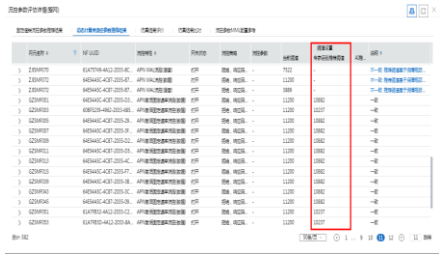
This question evaluates whether the core network fault management system can identify potential faults and prevent faults.

The core networks in Guangdong use Huawei OWS (including the MDAF module) to implement intelligent risk identification, potential fault identification, and automatic fault prevention. Specifically, Huawei OWS is used to check potential risks, analyze the causes of capacity, link, signaling storm, DR, and hardware risks, and provide recommended measures.

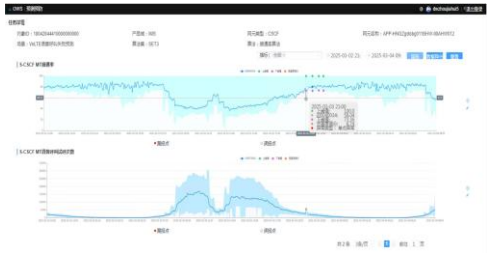
Example evidence for option A:

MAE-MDAF: Impact simulation in typical fault, emergency drill, holiday assurance, and signaling storm scenarios is supported to intelligently identify potential network risks in advance.—Support 1

MAE-MDAF: Network bottlenecks in switchover scenarios, as well as bottleneck VNFs and flow-controlled VNFs are identified in advance, and signaling storms and DR risks are prevented.—Support 1



MAE-MDAF: Optimal flow control parameters are recommended based on China Mobile's flow control specifications and AI algorithms to prevent signaling storms.
—Support 1



OWS: A KPI dynamic threshold detection model is built based on multi-source data and AI algorithms to monitor VNF KPI deterioration in real time and report risks.
—Support 2

OWS: Automatic risk cause analysis is carried out, and handling measures are provided.
—Support 2

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 4-1 A)

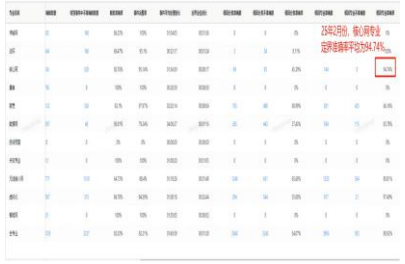
Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Demarcation	15%	Does your system support automatic demarcation of core network faults? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs and IMS VNFs)	Yes. The intelligent system supports automatic fault demarcation without manual intervention (e.g., core network VNFs and managed objects in telecom cloud) covering 95% or higher of live network faults. The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for VNFs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation covering 80% or higher of faults (only for the alarms after aggregation and alarms generated based on KPI monitoring). The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for VNFs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation and provides one or multiple analysis results to assist fault demarcation.	No. The system does not support automatic fault demarcation.

This question evaluates whether the automatic core network fault demarcation and locating capabilities are developed.

The core networks in Guangdong use the fault center and core network workbench to implement horizontal demarcation in the core network domain and vertical demarcation on the network cloud without manual intervention. Over 95% of live network faults are covered. The average monthly accuracy exceeds 90%.

Example evidence for option A:

The network-wide events cover more than 99% of live-network faults.—Support 0



The average monthly fault demarcation accuracy is higher than 90%. (China Mobile defines the root cause demarcation accuracy as the fault demarcation accuracy.)—Support 0

The system supports automatic demarcation of fault events in the core network domain.—Support 1

The fault demarcation process can be quickly orchestrated and hot deployed.—Support 1

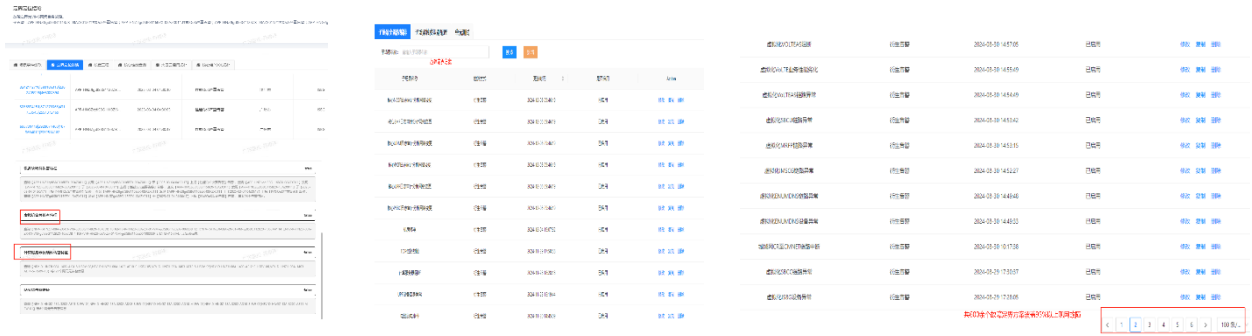
MAE-MDAF: Faults are automatically analyzed based on multi-source data, and VNF-level demarcation results are provided after a signaling storm occurs.—Support 1

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 4-2 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Demarcation	15%	Does your system support automatic demarcation of core network faults? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs and IMS VNFs)	Yes. The intelligent system supports automatic fault demarcation without manual intervention (e.g., core network VNFs and managed objects in telecom cloud) covering 95% or higher of live network faults. The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for VNFs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation covering 80% or higher of faults (only for the alarms after aggregation and alarms generated based on KPI monitoring). The average accuracy per month is above 90%. The system supports demarcation of following scenarios: 1. Horizontal demarcation for VNFs in the core network domain 2. Demarcation between VNFs and vertical demarcation for the telecom cloud	The system supports automatic fault demarcation and provides one or multiple analysis results to assist fault demarcation.	No. The system does not support automatic fault demarcation.

This question evaluates whether the automatic core network fault demarcation and locating capabilities are developed.

Example evidence for option A:



Inter-VNF demarcation and vertical demarcation on the telecom cloud are supported.—Support 2

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 5 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Locating	15%	Does your system support automatic locating related to core network fault management? Assessment object: the core network management function and network function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. Intelligent fault diagnosis is capable of automatically providing precise locating (e.g., detailed causes of identified faults, including minimum units, software modules, and ports) of faults, covering 95% or higher of live network faults without human intervention. The average accuracy per month is above 90%.	Automatic fault diagnosis is capable of providing root causes of faults, and providing precise fault locating, covering 80% or higher faults (only for the alarms after aggregation and alarms generated based on KPI monitoring). The average accuracy per month is above 90%.	The system supports automatic fault locating and provides one or multiple analysis results to assist fault locating.	No. The system does not support automatic fault locating.

This question evaluates whether the automatic core network fault location and demarcation capabilities are developed.

The core networks in Guangdong implement intelligent fault diagnosis through the core network workbench (connected to Huawei fault intelligent twins) without manual intervention. The workbench can automatically locate faults (identify detailed fault causes, involving the minimum unit, software module, and port). Currently, more than 95% of live-network faults can be covered monthly, and the average accuracy exceeds 90%.

Example evidence for option A:

Intelligent fault diagnosis can automatically provide information about accurate fault locations (for example, detailed causes of identified faults, involving the minimum unit, software module, and port). More than 95% of live-network faults can be covered from December 1 to December 31 without manual intervention. The average monthly accuracy exceeds 90%.

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 6 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Fault rectification solution generation	10%	Does your system automatically generate the fault rectification solution? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. The system can generate the optimal rectification solution (minimum impact scope and time). Fault rectification can cover but not be limited to the following scenarios: 1. Generating an NF fault rectification solution automatically 2. Generating a solution to recover slight service losses 3. Providing a DR solution in case of accidents or natural disasters 4. System can generate optimization to network for failure (e.g., signaling storm, service outage etc.) automatically.	The system can generate a fault rectification solution (e.g., fault rectification scripts including operation objects and operation sequences). Fault rectification can cover the following scenarios: 1. Providing a DR solution in case of accidents or natural disasters. 2. System can generate optimization to network for failure (e.g., signaling storm, service outage etc.) automatically.	The system can generate fault rectification recommendations based on specialized checklist, to determine the rectification operations and operation objects based on rectification decision rules (configuration). Fault rectification can cover the following scenarios: 1. Providing a DR solution in case of accidents or natural disasters	No. The system supports fault rectification based on manual decisions.

This question evaluates whether the core network fault management system can automatically generate fault rectification solutions.

The core networks in Guangdong generate the optimal fault rectification solutions (with the minimum impact scope and duration) through the core network workbench. Fault rectification is applicable to the following scenarios: (1) VNF fault scenario; (2) Slight service loss scenario; (3) Accident and natural disaster scenario; (4) Signaling storm or service interruption scenario.

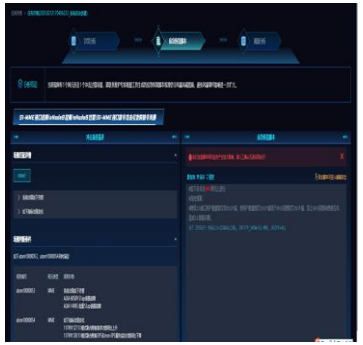
Example evidence for option A:

Core network workbench: The system supports automatic generation of NF fault rectification methods.—Support 1

Core network workbench: The system generates solutions to handle slight service loss.—Support 2

Fault rectification solutions are automatically generated.—Support 3

MAE-MDAF: DR switchover scripts are automatically generated.—Support 3



MAE-MDAF: Emergency rectification scripts are automatically generated after signaling storm exception analysis.—Support 4

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 7 B)

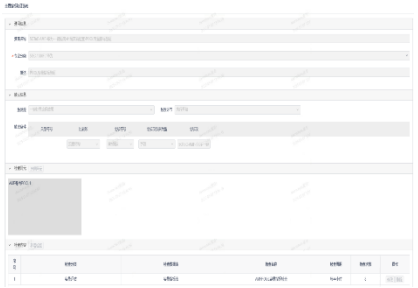
Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Solution pre-verification	10%	Does your system support rectification solution evaluation and verification to support decisions in core network? NOTE: Fault rectification solution can be evaluated before implementation by being verified in a simulation or sandbox environment. Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. The system supports intelligent rectification solution evaluation for the core network to verify the feasibility of rectification solution and provides the visualization results of accuracy effect before implementation. The evaluation tasks can cover but not be limited to the following scenarios: 1. Solution feasibility check and configuration verification 2. Emulation or simulation of rectification solution based on network digital twin The system supports the decision.	The system supports automatic rectification solution evaluation for core network, to verify the feasibility of rectification solution before implementation. The evaluation tasks can cover the following scenarios: 1. Solution feasibility check and configuration verification 2. DR rectification solution evaluation and verification The system supports the simulation results for manual decisions made for rectification solution.	The system provides a checklist for manual evaluation to verify the feasibility of rectification solution before implementation. The checklist includes but is not limited to: 1. NF healthy status check 2. Influence of rectification solution	No. The system verifies the rectification solution based on manual decisions.

This question evaluates whether the core network fault management system supports automatic evaluation and verification on the feasibility of fault rectification solutions. **The core networks in Guangdong support automatic evaluation on solution execution criteria before the core network fault rectification solutions are executed through the core network workbench and Huawei MAE-MDAF system. For example, evaluation can be carried out on whether the DR criteria are met, whether the health check on the standby VNF for active/standby switchover is performed, and whether the digital simulation of network impact is conducted.**

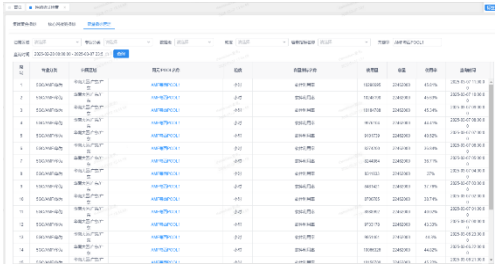
Example evidence for option B:

Core network workbench: Feasibility command check and configuration verification before rectification implementation are supported.—Support 1

Core network workbench: Counter check and verification before DR rectification implementation are supported.—Support 1



Core network workbench: Pool capacity check is supported.—Support 1



MAE-MDAF: The construction of network impact models is supported to digitally simulate the actual impact scenarios on the live network, generate simulation results, and optimize the result comparison in a visualized manner based on various flow control parameters.—Support 2

Reason why criteria in option A are not met: Manual decision-making is required for the fault rectification solutions. The simulation system does not support the decision-making.

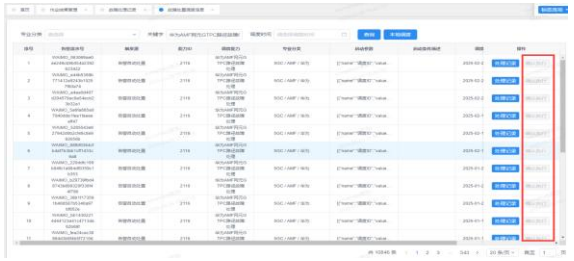
Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 8 B)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Solution implementation	10%	Does your system support automatic fault rectification? Assessment object: the core network management function and network element Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs).	Yes. The system can support automatic fault rectification in all fault rectification scenarios.	The system supports fault rectification after manual confirmation.		

This question evaluates whether the core network fault management system supports automatic fault rectification in various scenarios.

The core networks in Guangdong support automatic fault rectification in all scenarios (28 scenarios in total) through the core network workbench. The system can automatically determine the trigger condition and check the criteria before automatic execution. However, manual confirmation on the criteria is required for fault rectification execution in one-click mode.

Example evidence for option B:



Core network workbench: Both automatic fault rectification and manual fault rectification after confirmation are supported. If automatic execution is configured, rectification is automatically triggered by faults. If manual intervention is configured, fault rectification is completed after confirmation.

Reason why criteria in option A are not met: Emergency fault rectification can be triggered only after manual confirmation. Therefore, certain criteria are not met.

Core Network Fault Scenario Evaluation Criteria—Fault Management (Question 9 A)

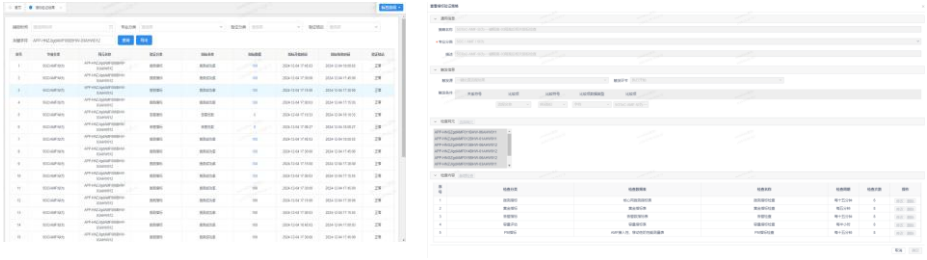
Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Service verification	10%	Does your system support automatic service verification after faults on core networks are rectified? Assessment object: the core network management function Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. The system automatically verifies whether network services are recovered and faults are rectified successfully.	The system automatically verifies that the alarms are cleared and KPI data is successfully recovered.	No. The system does not support automatic service verification.	

This question evaluates whether the core network fault management system supports automatic service verification after fault rectification.

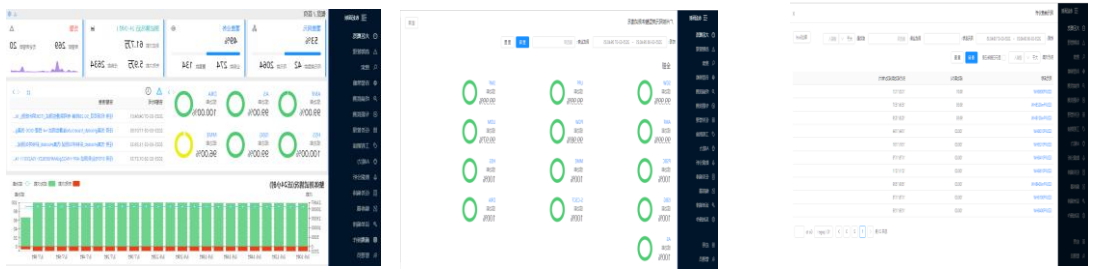
The core networks in Guangdong automatically detect data such as the alarm, KPI, and dialing test data through the core network workbench to automatically check whether network services are restored and whether the fault is rectified successfully.

Example evidence for option A:

MAE-MDAF: DR attendance in switchover scenarios is supported to display VNF KPI changes in a visualized manner to ensure that services are restored properly.



Core network workbench: Checks on whether the dialing test counters are normal, whether alarms are cleared, and whether KPIs are automatically restored after fault rectification are carried out.



Dialing test system: Automatic dialing tests on each service type (voice, data, SMS, and MMS) of each core network VNF are carried out to verify service restoration.

Core Network Fault Scenario Evaluation Criteria—Stability (Question 1 B)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Stable deployment architecture	10%	Does the core network deployment architecture have a capability for redundancy modules to take over the services carried by faulty modules? NOTE 1: There are service processing modules, LB load sharing modules, and service data modules. Core network VNFs for assessment: core network VNFs (e.g., 5GC VNFs, EPC VNFs, IMS VNFs)	Yes. The system can deal with multiple-module faults within a VNF, which uses multiple types of module resources within this VNF. If M module experiences an abnormal situation, N backup module can take over all service loads, preventing a decrease in the VNF overall processing capacity. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service connection context remains uninterrupted. 2. Service access can recover within minutes.	The system can deal with multiple-module faults within a VNF, which uses multiple types of module resources within this VNF. If M module experiences an abnormal situation, N backup module can take over all service loads, preventing a decrease in the overall processing capacity. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service access can recover within minutes.	The system can deal with a single module fault and restore service loads. The communication service experiences minimal impacts during the service takeover of redundancy modules: 1. Service access can recover within minutes.	Not supported

This question evaluates the architecture reliability of core network VNFs and module-level redundancy capabilities.

Core network VNFs in Guangdong China can automatically handle internal faults in multiple modules. If *M* modules become abnormal, *N* backup modules can take over all services to prevent the overall processing capability of the VNF from deteriorating. In addition, service connection contexts are not interrupted during the service takeover, and service access can be restored within minutes.

Example evidence for option B:

Stable Product Architecture

1. Service modules of VNFs on the live network are deployed in N-way mode (N+M deployment mode, where *M* is greater than 1). In this mode, if *M* modules become abnormal, *N* backup modules can take over all services to prevent the overall processing capability of the VNF from deteriorating.
2. The LB and DB on the live network are deployed in distributed mode, which minimizes the impacts of redundancy takeover on communication services.
3. The AMF hot backup function for the live network has entered the pilot phase but has not been deployed on a large scale. Therefore, service connection contexts cannot be kept uninterrupted, but service access can be restored within minutes.

The example VNFs on the live network include the UNC, UDG, UDM, ATS, CSC, PCF, and others.

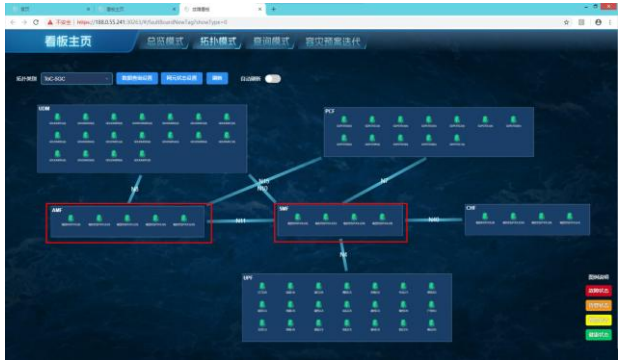
Core Network Fault Scenario Evaluation Criteria—Stability (Question 2 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Control-plane disaster recovery (DR)	15%	Does your system support automatic control-plane DR for DR VNFs to take over communication services without service interruption? Core network VNFs for assessment: core network VNFs, e.g., 5GC control-plane VNFs (AMF, SMF, PCF, UDM, NRF, SCP etc.), EPC VNFs (S-GW, MME, etc.), IMS VNFs	Yes. The control-plane DR VNFs and DR DCs can take over all services based on the following DR scenarios in minutes and UEs remain connected. 1. When an accident or natural disaster occurs, core network VNFs can switch over services across DCs and the backup VNFs can take over all services successfully. 2. When control-plane VNFs are faulty, backup VNFs can take over the services carried by faulty VNFs and UEs remain connected. 3. In the case of control-plane VNF (UDM/HSS, PCF/PCRF, OCS/CHF, NRF, ENUM etc.) faults, control-plane VNFs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above). 4. In the case of a management entity fault, control-plane VNFs can maintain subscribers' communication active for a period of time (hours or above). During control-plane DR, control-plane VNFs are required to maintain data connections.	The control-plane DR VNFs and DR DCs can take over all services based on the following DR scenarios in minutes. 1. When an accident or natural disaster occurs, core network VNFs can switch over services across DCs and the backup VNFs can take over all services successfully. 2. When control-plane VNFs are faulty, backup VNFs can take over the services carried by faulty VNFs. 3. In the case of critical control-plane VNF (UDM/HSS and PCF/PCRF and OCS/CHF) faults, control-plane VNFs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above). 4. In the case of a management entity fault, control-plane VNFs can maintain subscribers' communication active for a period of time (hours or above).	The control-plane DR VNFs and DR DCs can take over all services based on the following DR scenarios: 1. When an accident or natural disaster occurs, backup DCs can restore all service data and subscribers' data. 2. When control-plane VNFs are faulty, backup VNFs can take over the services carried by faulty VNFs. During control-plane DR, the control-plane VNFs can restore subscribers' data.	No. The service switchover can be triggered manually.

This question evaluates the control-plane DR capability of the core network.

Control-plane VNFs on the core network in Guangdong, China support automatic DR. Services are not interrupted during DR.

Example evidence for option A:



DR for ontrol-plane VNF

Bypass for ontrol-plane VNF

Bypass for agement-plane V

1. Control-plane VNFs on the live network are pooled for DR, and DC DR is implemented physically. If an accident occurs, core network VNFs can switch over services across DCs, and the backup VNFs can take over all services successfully.—Support 1 and Support 2
2. Control-plane VNFs on the live network support bypass-based DR. If critical control-plane VNFs (UDM, PCF/PCRF, or OCS/CHF) are faulty, control-plane VNFs, with data stored locally, can maintain subscribers' communication active for a period of time (hours or above).—Support 3
3. Management-plane VNFs on the live network support bypass-based DR. If a management entity is faulty, control-plane VNFs can maintain subscribers' communication active for a period of time (hours or above).—Support 4

Core Network Fault Scenario Evaluation Criteria—Stability (Question 3 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
User-plane disaster recovery	15%	Does your system support automatic user-plane DR to take over all services without service interruption? NOTE 1: The user-plane DR scenario indicates that the backup UP VNF (UPF) can take over the services in the fault scenario. Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs (UPF), EPC VNFs (PGW), IMS VNFs (SBC))	Yes. The user-plane DR VNFs and DR DCs can take over all services without service interruption: 1. When an accident or natural disaster occurs, user-plane VNF's pool-based deployment supports the switching of traffic among user-plane VNFs in minutes. 2. In the case of a management entity fault, user-plane VNFs can maintain communication services for a period of time (hours or above). 3. The data connection remains active.	The user-plane DR VNFs and DR DCs can take over all services in a short period of time: 1. User-plane VNFs can take over all traffic in minutes. 2. The data connection can recover in minutes.	The user-plane DR VNFs and DR DCs can take over traffic of faulty user-plane VNFs. 1. User-plane VNFs can take over all traffic.	Not supported

This question evaluates whether user-plane DR capabilities are supported on the core networks.

The core networks in Guangdong support automatic DR on the user plane without interrupting services.

Example evidence for option A:

Figure 1: DR in the VNF group pool on the user plane

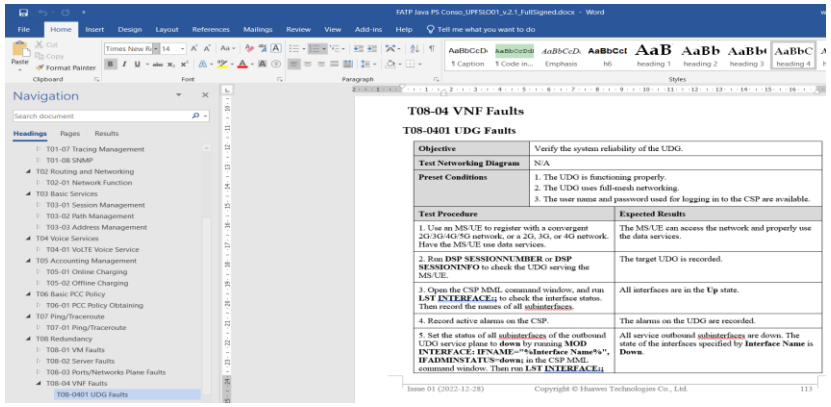


Figure 2: Full-mesh networking for the UDG DR on the user plane

1. DR in the UPF group pool on the user plane is supported on the live network. If an accident or natural disaster occurs, traffic can be switched within a few minutes.—Support 1
2. Full-mesh networking for the UDG DR on the user plane is supported on the live network. The DR VNFs and DR DCs on the user plane can take over all services without any service interruption.—Support 2 and Support 3
3. Bypass DR for the VNFs on the user plane is supported on the live network. The DR VNFs and DR DCs on the user plane can take over all services without any service interruption.—Support 2 and Support 3

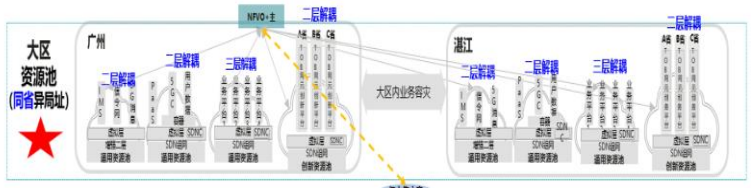
Core Network Fault Scenario Evaluation Criteria—Stability (Question 4 B)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Infrastructure disaster recovery	15%	Does your system support automatic disaster recovery on telecom cloud infrastructure to ensure uninterrupted communication services? NOTE: Telecom cloud infrastructure is considered to include the following elements: Cloud OS and hardware (server, storage, and IP Core). The faults may result from the IP backbone router, transmission faults, or the overall telecom cloud faults. Core network VNFs for assessment: core network VNFs (e.g., 5GC VNFs, EPC VNFs, and IMS VNFs)	Yes. The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When DC transmission is faulty, the core network can provide local area (e.g., within a region) communication normally. 2. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the VNFs in running status for a period of time, or trigger DR switchover to maintain the communication without interruption. 3. In case of whole core network outage, at least VIP calls and emergency calls can proceed through the backup core network. 4. Distributed user-plane VNF deployment can reduce the impacts of user-plane VNFs faults, and user-plane VNF switchover can minimize the affected region. 5. When the core network subdomain or subsystem experiences faults, network can fallback without affecting other communication services (e.g., IMS fallback should not affect data connection). 6. When the core network subdomain becomes faulty, network in the subdomain can fall back, keeping normal UE connection. (e.g., 5GC data connectivity can fall back to EPC network and EPC data connectivity can fall back to 3G PS services.) 7. When a natural disaster occurs and affects two active DCs, additional third DC can take over service loads from the two active DCs and remain data connection alive.	The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When DC transmission is faulty, the core network can provide local area (e.g., within a region) communication for a period of time. 2. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the VNFs in running status for a period of time. 3. Distributed user-plane VNF deployment can reduce the impacts of user-plane VNFs faults, and user-plane VNF switchover can minimize the affected region. 4. When the core network subdomain experiences faults, network in the subdomain can fall back, keeping normal UE connection. (e.g., 5GC data connectivity can fall back to EPC network and EPC data connectivity can fall back to 3G PS services.)	The system can support service continuity in any possible disaster scenario related to telecom cloud infrastructure: 1. When telecom cloud infrastructure experiences an abnormal situation (e.g., storage fault), the core network is capable to keep the VNFs in running status for a period of time.	Not supported

This question evaluates the DR and reliability capabilities of core network infrastructure in various exception scenarios.

Core networks and network clouds in China Mobile Guangdong support service continuity in infrastructure DR scenarios, including all scenarios of option B.

Example evidence for option B:



Bypass-based
R for Infrastructu

1. The figure shows the DR for the central DC of China Mobile Guangdong. When the DC transmission is faulty, the core network can still offer communications in certain areas (for example, in one area) within a period of time.— Support 1
2. With the bypass function enabled for core network infrastructure, core network VNFs can run for a period of time even if Telco Cloud infrastructure encounters a fault (for example, a storage fault).— Support 2
3. Huawei user-plane devices of China Mobile Guangdong adopt CUPS. When a user-plane VNF is faulty, CUPS can mitigate the impacts of the VNF fault, and the user-plane VNF switchover can reduce the affected areas.— Support 3
4. Huawei 5G Core devices of China Mobile Guangdong are capable of EPS Fallback. When a 5G core network subdomain is faulty, UEs in this network can fall back, maintaining normal network connectivity for the UEs.— Support 4

Reason for not meeting option A: The devices on the live network cannot meet functions 3, 5, and 7 in option A.

Core Network Fault Scenario Evaluation Criteria—Stability (Question 5 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Anti-signaling surge capability	15%	Does your system support automatic signaling overload control to avoid core network service outage? NOTE: The terminal behaviors are affected by the software logic or server design. Since the terminal behaviors are highly consistent, wide-range signaling impact can occur. Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. The system can control signaling storm and maintain the end to end services: 1. When signaling storm occurs, VNFs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end VNFs can evaluate and adaptively adjust subscribers' service requests delivered to back-end network elements, so the back-end elements can remain at the optimized workload without service congestion. 3. When signaling storm occurs, core network VNFs are capable to evaluate and adjust traffic to avoid impact to other domains when services fall back. The system can converge signaling storm in minutes.	The system can control signaling storm and maintain the end to end services: 1. When signaling storm occurs, VNFs are capable to protect its processing capability without service outage. 2. In the signaling surge scenario, the front-end VNFs can reduce the service requests delivered to back-end network elements, so the back-end VNF faults can be avoided. The system can converge signaling storm within 1 hour.	VNFs are capable to protect its processing capability.	Not supported

This question evaluates whether the capabilities for withstanding the signaling surge impact are supported on the core networks.

Automatic signaling overload control is supported on the core networks in Guangdong, ensuring uninterrupted core network services, which is a criterion for option A.

Example evidence for option A:

Peripheral VNFs are protected, HTR flow control configurations are queried or licenses are obtained in surge scenarios.

NE Flow Control Function

The flow control functions are supported for the VNFs on the live network.—Support 1 and Support 2

MAE-MDAF: The construction of network impact models is supported to digitally simulate the actual impact scenarios on the live network, generate simulation results, and optimize the result comparison in a visualized manner based on various flow control parameters.—Support 3

Core Network Fault Scenario Evaluation Criteria—Stability (Question 6 A)

Capability or Task	Weight	Questions	Option A	Option B	Option C	Option D
Risk prediction	10%	Does your system automatically detect and prevent the risks of network VNF faults to ensure the service continuity? Core network VNFs or NFs for assessment: core network VNFs (e.g., 5GC NFs, EPC VNFs, and IMS VNFs)	Yes. The system can use intelligent risk identification to recognize the potential faults and automatically prevent faults, and it can do the following: 1. Prevent potential risks and analyze the specification-related risks including capacity, links, signaling storm, and DR. 2. Analyze the cause of risk and provide the recommended measures automatically.	The system can perform automatic risk identification, which requires manual confirmation, to recognize the potential faults and prevent faults, and it can do the following: 1. Prevent potential risk and analyze the specification-related risks, including capacity and links.	The system can use risk identification, which provides an automatic check list and requires periodically manual confirmation about the potential risks in this check list, to recognize the potential faults and prevent faults, and it can do the following: 1. Prevent potential risk and analyze the specification-related risks including capacity.	Not supported

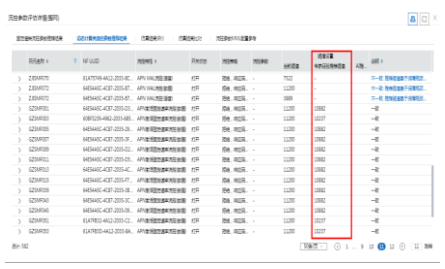
This question evaluates whether the VNF fault risk prediction capabilities of the core networks are developed.

The core networks in Guangdong automatically detect and prevent VNF fault risks, check potential risks, and analyze risks in terms of capacity, links, signaling storms, DR, and hardware through the OWS system. Automatic risk cause analysis is carried out, and suggestions regarding the requirements of each scenario in option A are provided.

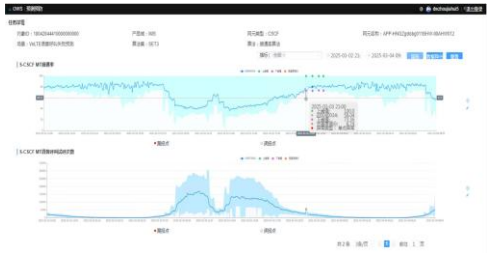
Example evidence for option A:

MAE-MDAF: Impact simulation is supported in typical fault, emergency drill, holiday assurance, and signaling storm scenarios to intelligently identify potential network risks in advance.—Support 1

MAE-MDAF: Network bottlenecks are identified in switchover scenarios in advance, bottleneck VNFs and flow-controlled VNFs are identified, and signaling storms and DR risks are prevented.—Support 1



MAE-MDAF: Optimal flow control parameters are recommended based on China Mobile's flow control specifications and AI algorithms to prevent signaling storms.
—Support 1



OWS: A KPI dynamic threshold detection model is built based on multi-source data and AI algorithms to monitor VNF KPI deterioration in real time and report risks.
—Support 2

OWS: Automatic risk cause analysis is carried out, and handling measures are provided.
—Support 2

Thank you