

TM Forum

ANLAV Report

Vodafone Türkiye

GB1523E – IP Network Fault Management

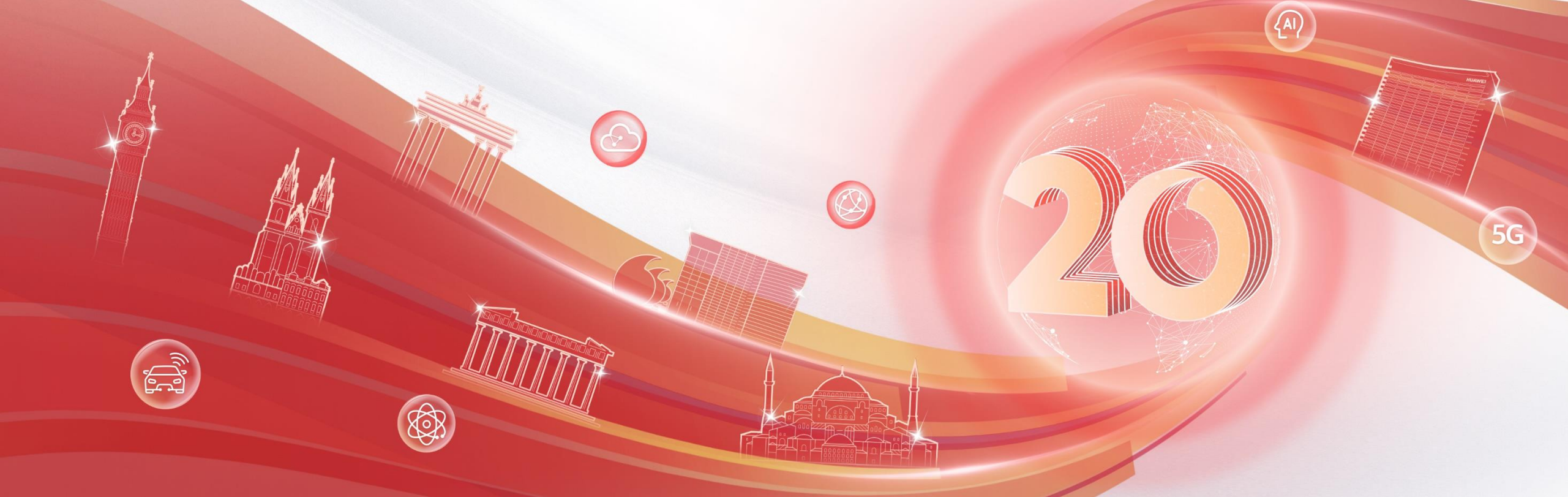
Version: 2.0.0

Score: 3.4

Vodafone Türkiye IP Network Fault Management

ANL Assessment

GB1523E_IP_Network_Fault_Management_Questionnaire_v2.0.0



IP Fault Management ANL Assessment Overall Score

Cognitive Activities (IAADE)	Service capability	Weight	Question	Answer			Final Score
				Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal (should include but not limit to IGP and BGP peer state abnormal, BFD session abnormal)	
				16%	64%	4%	
Intent	Intent Translation & Fulfillment	10%	How does the System translate and process intents & ensure intent fulfilment ? Note: 1) Intent could be fault management requirements such as MTTR (mean time to repair) , troubleshooting priority (e.g., emergency restoration in highest priority) , customized troubleshooting preference based on fault impact scope and severity, etc. 2) Fault management target include alarm severity, alarm threshold, alarm aggregation rules, fault notification rules, etc.	A	A	A	3.4
Awareness	Data Collection& Alarm filtering	10%	How does the System support data collection, alarms correlation and fileting? Note: All types and fault-related indicators mentioned in options should be covered when choosing a related option	A	B	A	
Analysis	Fault Identification ,Risk identification, impact analysis	15%	How does the System support fault identification, risk identification and subsequent impact analysis? Note: These four sub-scenarios are required to consider potential risk: Optical Module Failure or Optical Power Abnormal, High Error Rate, Protocol State Abnormal, VPN Degradation.	B	B	B	
	Fault Demarcation	15%	How does the system support fault demarcation? Note: 1) Examples of demarcation involve pinpointing the exact roles of malfunctioning routers, like identifying whether they are access routers, aggregation routers, or Autonomous System Boundary Router (ASBR).	A	A	A	
	Fault Locating and Root Cause Analysis	15%	How does the system support root cause analysis? Note: 1) Examples of detailed causes of identified faults, including the smallest replaceable unit, software modules, and ports.	A	A	A	
	Solution Generation	10%	How does the System support generation of fault recovery solutions?	B	B	B	
Decision	Solution Evaluation & Decision Making	15%	How does the System support evaluation & decision of fault recovery solutions?	A	A	A	
Execution	Solution Implementation	10%	How does the system support automatic solution implementation and on-site instructions?	B	B	A	

IP Fault Management Sub-scenario Evidence

Alarm Name	Counting	proportion	Fault Category
ETH_LOS	334	56.13%	Port Failure
Optical Invalid	92	15.46%	Optical Module Failure
Link Down	44	7.39%	Port Failure
Output rate alarm notification	30	5.04%	
IS-IS Adjacency Changed	25	4.20%	Protocol State Abnormal
Input rate alarm notification	22	3.70%	
MPLS LDP Session Down	21	3.53%	
PW VC Down	17	2.86%	
BGP Status Changed	2	0.34%	
Time synchronization failed	2	0.34%	
Clock Source Check Fail	2	0.34%	
Crc error alarm notification	2	0.34%	
CCC VC Status Changed to Down	1	0.17%	
The state of clock source is failed	1	0.17%	
Total	595	100%	



Sub-scenario	Weight
Optical Module Failure	16%
Port Failure	64%
Protocol State Abnormal	4%
Total	84%

Based on trouble ticket statistics for one month.



Intent Translation & Fulfillment-1

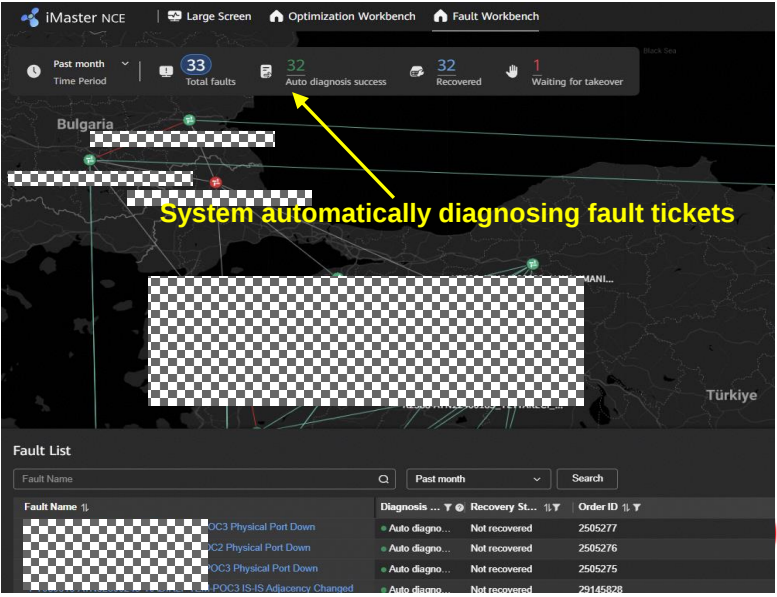
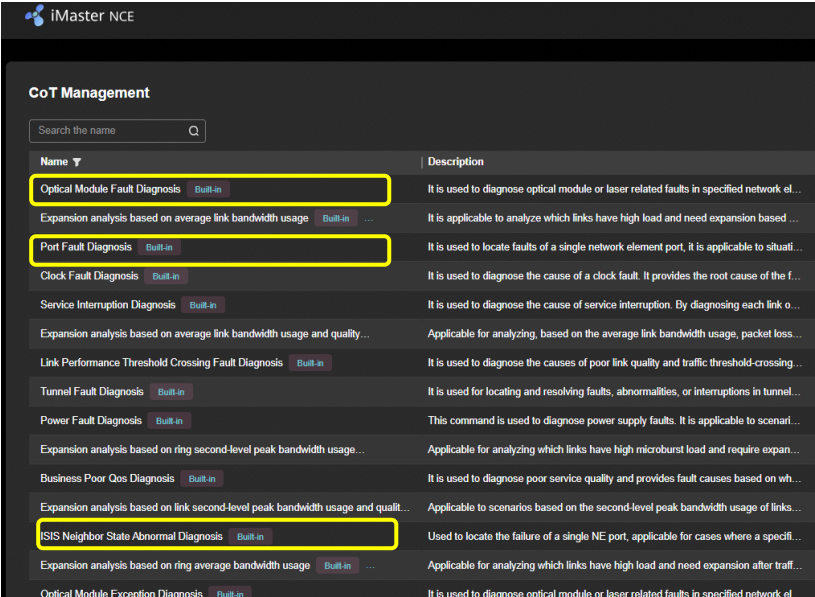
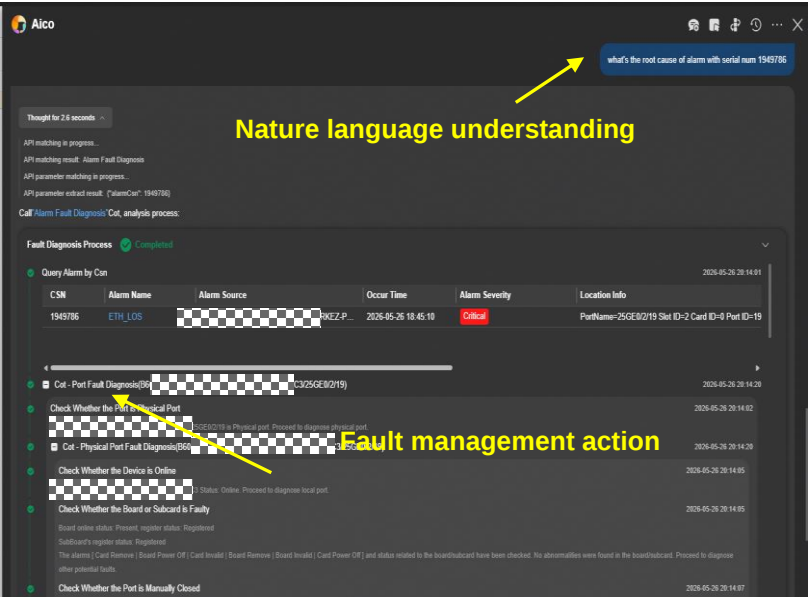
		Optical Module Failure or Optical Power Abnormal		Port Failure	Protocol State Abnormal	
		A		A	A	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Intent Translation & Fulfillment	10%	How does the System translate and process intents & ensure intent fulfilment ? Note: 1) Intent could be fault management requirements such as MTTR (mean time to repair) , troubleshooting priority (e.g., emergency restoration in highest priority), customized troubleshooting preference based on fault impact scope and severity, etc. 2) Fault management target include alarm severity, alarm threshold, alarm aggregation rules, fault notification rules, etc.	The system supports the input of fault management intent by simplified human-system interaction (e.g., nature language user interface provided by system), system automatically translates the intent into fault management targets . The System evaluates intent fulfillment based on the implementation effect, providing overview of fault management results, including automatically fault-handling results and the suggestions for faults that required manually handling, etc.	The System processes Intent through the execution of predefined Rules and Policies. Intent fulfillment is manually evaluated	Fault management task targets and policies are manually defined based on expertise. Manually evaluate the effect after the intention is implemented.	Manually set fault management targets based on expertise(such as setting alarm severity and classification) .

Example evidence for option A:

1、The system support nature language based fault management, the system automatically translates the intent into fault management target and take action.

2、The system supports fault management and provides diagnostic CoT for various types of faults. The supported fault CoT includes Port Failure, Optical Module Failure, Optical Power Abnormal, Protocol Abnormal etc.

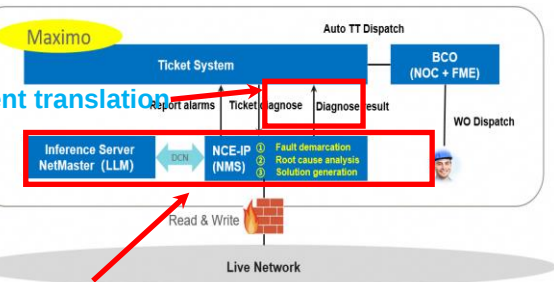
3、When a fault occurs, the system automatically takes over the fault ticket, understands the intent of the ticket, automatically loads the corresponding fault diagnosis CoT , performs fault demarcation and localization, and generates a repair solution, thereby realizing the automated disposal of the fault process.



Intent Translation & Fulfillment-2

Intent Translation & Fulfillment-2			Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal	
			A	A	A	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Intent Translation & Fulfillment	10%	How does the System translate and process intents & ensure intent fulfilment ? Note: 1) Intent could be fault management requirements such as MTTR (mean time to repair) , troubleshooting priority (e.g., emergency restoration in highest priority), customized troubleshooting preference based on fault impact scope and severity, etc. 2) Fault management target include alarm severity, alarm threshold, alarm aggregation rules, fault notification rules, etc.	The system supports the input of fault management intent by simplified human-system interaction (e.g., nature language user interface provided by system), system automatically translates the intent into fault management targets . The System evaluates intent fulfillment based on the implementation effect, providing overview of fault management results, including automatically fault-handling results and the suggestions for faults that required manually handling, etc.	The System processes Intent through the execution of predefined Rules and Policies. Intent fulfillment is manually evaluated	Fault management task targets and policies are manually defined based on expertise. Manually evaluate the effect after the intention is implemented.	Manually set fault management targets based on expertise(such as setting alarm severity and classification) .

Example evidence for option A:



Fault diagnose task has been done automatically by NMS with AI, no need human confirmation.

Scenario 1: Diagnose task invoked by human intent input

Natural Language Input of Expert Troubleshooting Experience

Fault service keep-alive backoff strategy: allow sacrificing SLA performance to ensure service connectivity

The large model parses the troubleshooting intent, orchestrates network capability APIs, and generates a troubleshooting chain of thought

Intent input text

Parsed intent and generate the fault diagnose target then take diagnose action

Fault occur time and diagnose time



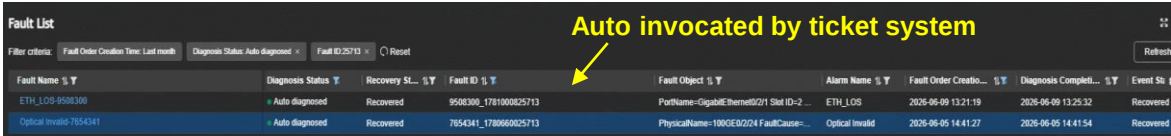
Intent Translation & Fulfillment-3

Intent Translation & Fulfillment-3			Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal	
			A	A	A	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Intent Translation & Fulfillment	10%	How does the System translate and process intents & ensure intent fulfilment ? Note: 1) Intent could be fault management requirements such as MTTR (mean time to repair) , troubleshooting priority (e.g., emergency restoration in highest priority), customized troubleshooting preference based on fault impact scope and severity, etc. 2) Fault management target include alarm severity, alarm threshold, alarm aggregation rules, fault notification rules, etc.	The system supports the input of fault management intent by simplified human-system interaction (e.g., nature language user interface provided by system), system automatically translates the intent into fault management targets . The System evaluates intent fulfillment based on the implementation effect, providing overview of fault management results, including automatically fault-handling results and the suggestions for faults that required manually handling, etc.	The System processes Intent through the execution of predefined Rules and Policies. Intent fulfillment is manually evaluated	Fault management task targets and policies are manually defined based on expertise. Manually evaluate the effect after the intention is implemented.	Manually set fault management targets based on expertise(such as setting alarm severity and classification) .

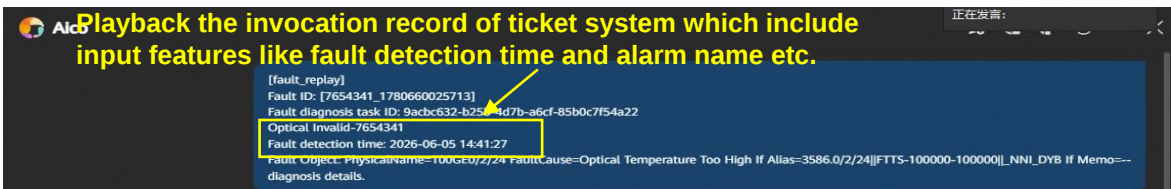
Example evidence for option A:

Scenario 2: Diagnose task invoked by ticket system

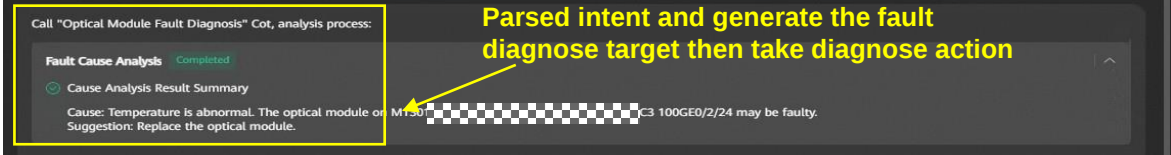
Auto invoked by ticket system



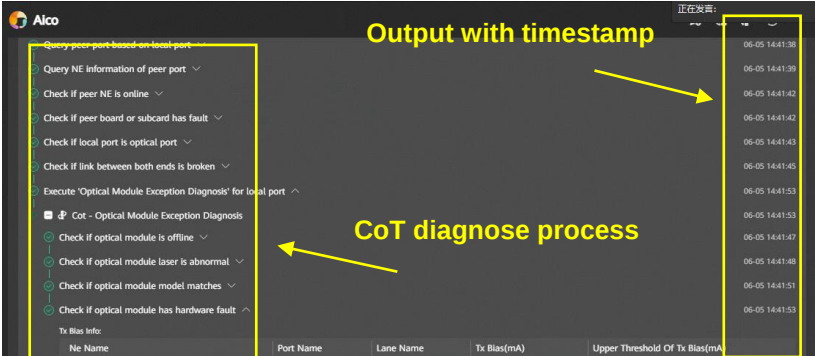
Playback the invocation record of ticket system which include input features like fault detection time and alarm name etc.



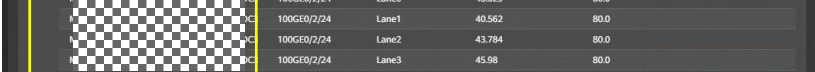
Parsed intent and generate the fault diagnose target then take diagnose action



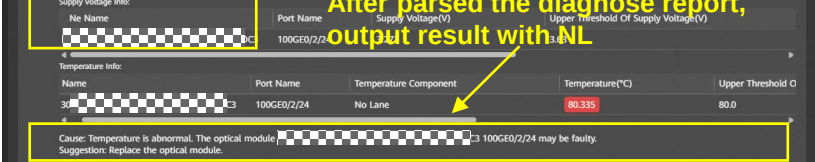
Output with timestamp



CoT diagnose process



After parsed the diagnose report, output result with NL





Data Collection& Alarm filtering-1

		Optical Module Failure or Optical Power Abnormal		Port Failure	Protocol State Abnormal	
		A		B	A	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Data Collection& Alarm filtering	10%	How does the System support data collection, alarms correlation and fileting? Note: All types and fault-related indicators mentioned in options should be covered when choosing a related option	The system automatically collects fault-related indicators including alarms, logs, performance, and OAM data, detecting service and network status in minutes, and automatically associates alarms, filters & correlates alarms. For specific sub-scenarios, data awareness at higher precision is needed for accurate root cause analysis: 1) For sub-scenario "device offline", millisecond-level optical power data is needed. 2)For sub-scenario "Port Failure", data collection of OTDR is needed.	The system automatically collects fault-related indicators including alarms, logs, performance, detecting service and network status within 15 minutes or 24 hours, associates alarms, filters & correlates alarms based on manually defined rules.	Manually select and use the System to collect data and filter out invalid/redundant alarms	Data collection and alarm filtering of invalid / redundant alarms are manually done.

Example evidence for option A:

Real-time Fault & Performance Alarm Management

iMaster NCE									
Current Alarms Alarm Logs Historical Alarms Masked Alarms Event Logs Alarm Log Statistics Event Log Statistics Alarm Settings									
Template Management Filter									
Auto Refresh Quick Filter									
Control Sorting Export Comment Clear									
Acknowledge									
Severity Alarm ID Name Location Info Other Information Occurrences First Occurred									
Major 260906 BFD For TE LSP Down Ala... MED... MPLS Tunnel Id=147 Ingress LSR Id... MPLS Tunnel Name=Tunnel1421 633 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... MED... MPLS Tunnel Id=163 Ingress LSR Id... MPLS Tunnel Name=Tunnel1422 633 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-172-b63e LocalDiscriminator=2078 Diagnosis... 729 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-183-8a60 LocalDiscriminator=2197 Diagnosis... 729 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... MED... MPLS Tunnel Id=172 Ingress LSR Id... MPLS Tunnel Name=Tunnel1348 661 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... MED... MPLS Tunnel Id=183 Ingress LSR Id... MPLS Tunnel Name=Tunnel1349 671 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... MED... MPLS Tunnel Id=194 Ingress LSR Id... MPLS Tunnel Name=Tunnel1350 682 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... JANE... MPLs Tunnel Id=1 Ingress LSR Id=10... MPLS Tunnel Name=Tunnel1 665 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... JANE... MPLs Tunnel Id=2 Ingress LSR Id=10... MPLS Tunnel Name=Tunnel2 641 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... JANE... MPLs Tunnel Id=6 Ingress LSR Id=10... MPLS Tunnel Name=Tunnel5 672 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... JANE... MPLs Tunnel Id=8 Ingress LSR Id=10... MPLS Tunnel Name=Tunnel6 636 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... JANE... MPLs Tunnel Id=8 Ingress LSR Id=10... MPLS Tunnel Name=Tunnel6 683 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... JANE... MPLs Tunnel Id=10 Ingress LSR Id=1... MPLS Tunnel Name=Tunnel10 636 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... JANE... MPLs Tunnel Id=3101 Ingress LSR Id... MPLS Tunnel Name=Tunnel03101 629 2026-05-25 23:12...									
Major 260906 BFD session down JANE... SessName=hsb-4-168a LocalDiscriminator=15 Diagnosis... 716 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... MED... MPLs Tunnel Id=176 Ingress LSR Id... MPLS Tunnel Name=Tunnel1423 636 2026-05-25 23:12...									
Major 260906 BFD For TE LSP Down Ala... MED... MPLs Tunnel Id=3279 Ingress LSR Id... MPLS Tunnel Name=Tunnel03279 631 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-184-6a93 LocalDiscriminator=2190 Diagnosis... 741 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-116d LocalDiscriminator=1299 Diagnosis... 695 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-3279-433a LocalDiscriminator=5661 Diagnosis... 698 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-176-266f LocalDiscriminator=2184 Diagnosis... 687 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-147-39a2 LocalDiscriminator=2121 Diagnosis... 699 2026-05-25 23:12...									
Major 260906 BFD session down MED... SessName=hsb-4-981a LocalDiscriminator=71 Diagnosis... 734 2026-05-25 23:12...									

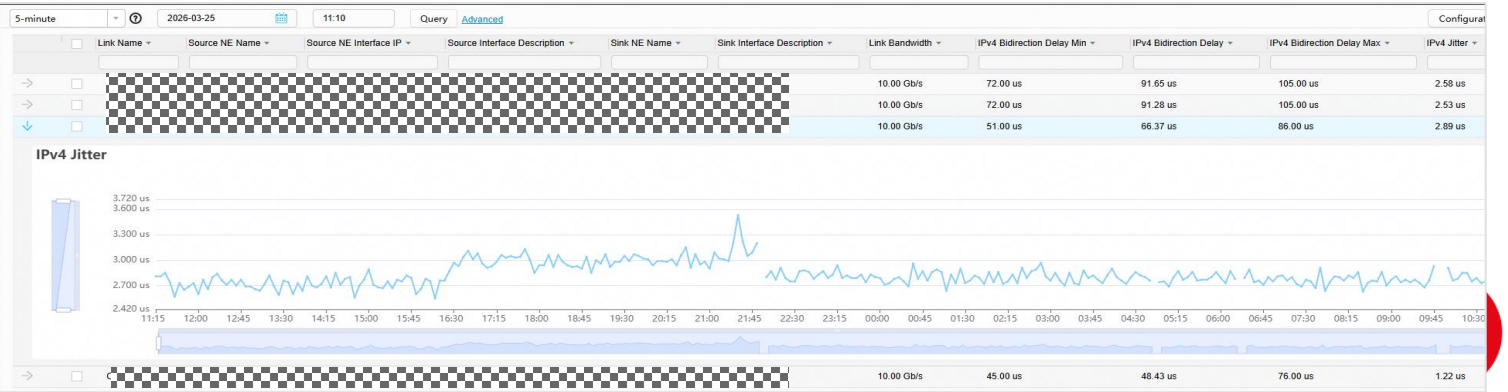
Log Management

Log Manage...		Operation Logs	
Security Logs		Filter Criteria From 26-05-2026 01:29:16 to 26-05-2026 01:29:16	
System Logs		Total records: 287	
Operation Logs		Operation Log Details	
Disable an interface		Details	
Query logs		Previous Next	
Query online map business			
Save request clauses conf.			
Save request clauses conf.			
Save request clauses conf.			
Save request clauses conf.			
Save request clauses conf.			
Save request clauses conf.			
Unicast BFD			

Minute-level OAM data (Packet Loss, Delay, Jitter, etc.)

1-minute		2026-05-27		00:45		Query Advanced Group Configuration	
Subnet Name		NE Name		NE Type		Avg. CPU Usage(%)	
Adana		NetEngine 8...		40.00		36.00	
Adana		ATN 980C		37.00		37.00	
Adana		ATN 980C		36.00		36.00	
ANKARA		ATN950D		22.00		22.00	
Adana		NE40E-X3A...		12.00		37.00	
Adana		NE40E-X3A...		9.00		21.00	

Minute-level performance data (CPU/Memory Usage, etc.)



Data Collection& Alarm filtering-2

		Optical Module Failure or Optical Power Abnormal		Port Failure	Protocol State Abnormal	
		A		B	A	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Data Collection& Alarm filtering	10%	How does the System support data collection, alarms correlation and fileting? Note: All types and fault-related indicators mentioned in options should be covered when choosing a related option	The system automatically collects fault-related indicators including alarms, logs, performance, and OAM data, detecting service and network status in minutes, and automatically associates alarms, filters & correlates alarms. For specific sub-scenarios, data awareness at higher precision is needed for accurate root cause analysis: 1) For sub-scenario "device offline", millisecond-level optical power data is needed. 2)For sub-scenario "Port Failure", data collection of OTDR is needed.	The system automatically collects fault-related indicators including alarms, logs, performance, detecting service and network status within 15 minutes or 24 hours, associates alarms, filters & correlates alarms based on manually defined rules.	Manually select and use the System to collect data and filter out invalid/redundant alarms	Data collection and alarm filtering of invalid / redundant alarms are manually done.

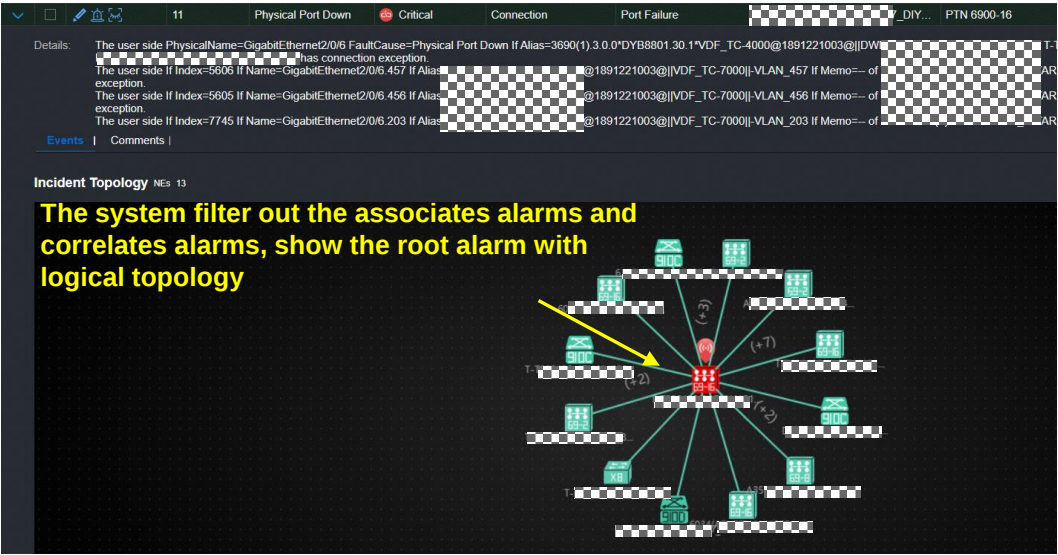
Example evidence for option A:

The system support automatically associates alarms, filters & correlates alarms.

Alarms You can click an NE in the topology to view its alarms.

Event Serial...	Event ID	Name	Severity	Description	Source Ob
2083885	2505274	Physical Port Down	Critical	PhysicalName=GigabitEthernet2/0/6 FaultC...	T-T090400
2083886	3	Link Down	Critical	If Index=4784 If Name=GigabitEthernet2/0/6...	T-T090400
2083887	3	Link Down	Critical	If Index=7744 If Name=GigabitEthernet2/0/6...	T-T090400
2083888	3	Link Down	Critical	If Index=7745 If Name=GigabitEthernet2/0/6...	T-T090400
2083889	3	Link Down	Critical	If Index=5605 If Name=GigabitEthernet2/0/6...	T-T090400
2083890	3	Link Down	Critical	If Index=5606 If Name=GigabitEthernet2/0/6...	T-T090400
2083895	2601239	Local Fault Alarm	Critical	PortName=GigabitEthernet2/0/6 If Alias=36...	T-T090400
2083891	1101056	PW VC Down	Major	PWVclIndex=44775 PWVcType=Ethernet Pe...	T-T090400
2083892	1101056	PW VC Down	Major	PWVclIndex=44776 PWVcType=Ethernet Pe...	T-T090400
2083893	1101056	PW VC Down	Major	PWVclIndex=37185 PWVcType=Ethernet Pe...	T-T090400

Total records: 11



Note: VF Turkey can not collect the fiber cut distance with OTDR tool automatically on port failure scenario, option B for port failure.



Fault Identification ,Risk identification-1

Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal
B	B	B

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Fault Identification ,Risk identification, impact analysis	15%	How does the System support fault identification, risk identification and subsequent impact analysis? Note: These four sub-scenarios are required to consider petential risk: Optical Module Failure or Optical Power Abnormal, High Error Rate, Protocol State Abnormal, VPN Degradation.	The system identifies faults, potential risk and subsequent impact with severity based on AL modes without need for Human intervention. Note: The AI models should conduct analysis based on multi-dimensional data including service topology (e.g., consists of L2VPN, L3VPN, L2EVPN, L3EVPN, SRv6-Policy, etc.), physical topology, performance data, alarm correlations, etc.	The System identifies faults, potential risk and subsequent impact based on Dynamic programable rules (configurable or ML), but may needs human confirmation	The System identifies faults, potential risk and subsequent impact based on manually defined rules	Faults,potential risk and impact need to be manually identified based on human expertise or through the execution of manual written procedures.

Example evidence for option B:

Settings

Network Map Settings

Path Restoration Policy Settings

Network Traffic Settings

Intelligent Analysis Settings

Configuration Simulation Settings

Planning Simulation Setting

Diagnosis

Digital Radar: Configuration

Collection Item

Analysis Item

NE Level

Collection Item Settings

Collection Item Templates

Physical Entity Statistics

Master/Slave Engine Status

ISIS Neighbor Status

Default Template

OSPF Neighbor Status

OSPFv3 Neighbor Status

IP Routing Table Information

VPN Instance Route Exceeds The Limit

Board Temperature Abnormal

NE CPU Usage

NE Memory Usage

Disk Usage

Abnormal Port Bit Errors

MPLS TE Tunnel status

LSP Tunnel status

Clock Synchronization Status

SR Policy Tunnel Statistics

SRv6 Policy Tunnel Statistics

LLDP Neighbor Information

Port Optical Power Information

Interface Bandwidth Usage

FTP Service Status

Telnet Service Status

BGP Neighbor Statistics

Template Configurations

Template name

Default Template-1780045751541

Normal value of ISIS neighbor status

Up

ISIS anomalous neighbor burst range

0

-

5

%

Health degree

100

5

-

10

%

Health degree

80

10

-

100

%

Health degree

0

Mutation range of the total number of I...

0

-

5

%

Health degree

100

5

-

10

%

Health degree

80

10

-

100

%

Health degree

0

Dynamic programable rules

Network Health Details

Weight Configurations

Analysis Item Name

Weight

Statistics On NE Information

1

Physical Entity Statistics

5

Master/Slave Engine Status

1

Physical Topology Information

5

Long Chain

5

Ring Information

1

ISIS Neighbor Status

10

OSPF Neighbor Status

10

OSPFv3 Neighbor Status

10

IP Routing Table Information

10

VPN Instance Route Exceeds The Limit

1

Bgp Neighbor Status

1

LSP tunnel information

1

MPLS TE Tunnel status

1

SR Policy Status

1

SRv6 Policy Status

1

Layer 3 Topology Information

1

Board Temperature Abnormal

1

NE CPU usage

5

NE Memory Usage

5

Abnormal Port Bit Errors

5

LLDP neighbor information

5

Disk Usage

5

Clock Synchronization Status

10

Port Optical Power Information

5

Interface Bandwidth Usage

5

Self-define healthy weight for different checklist

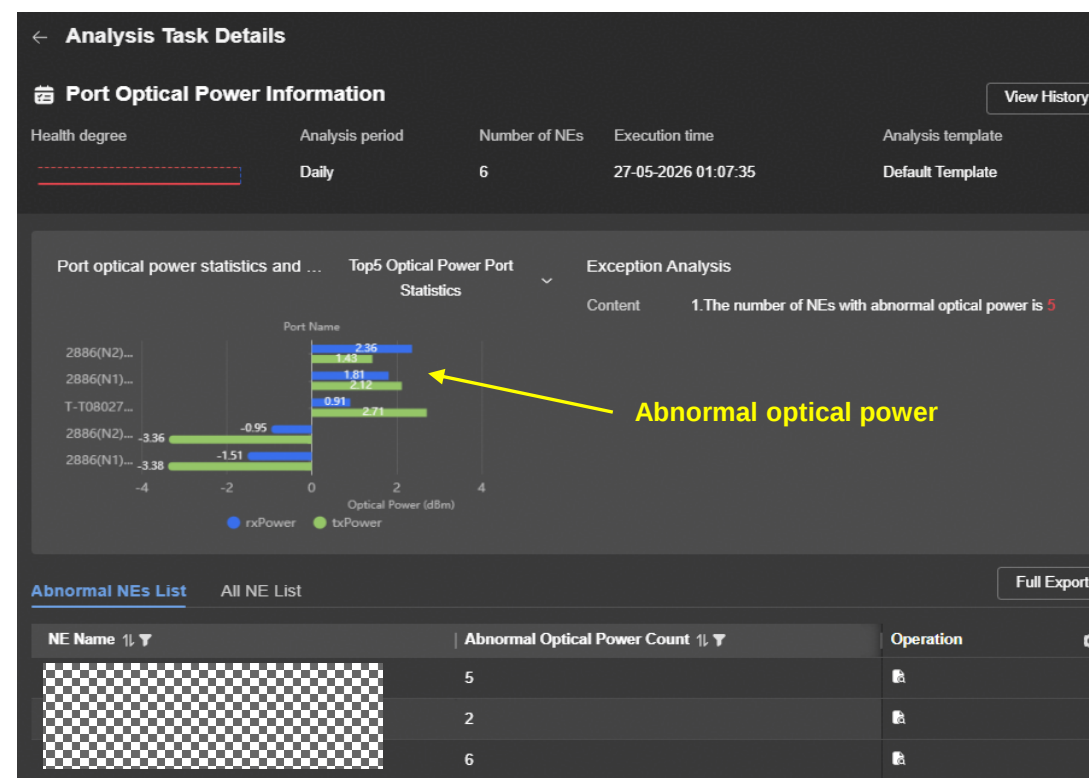
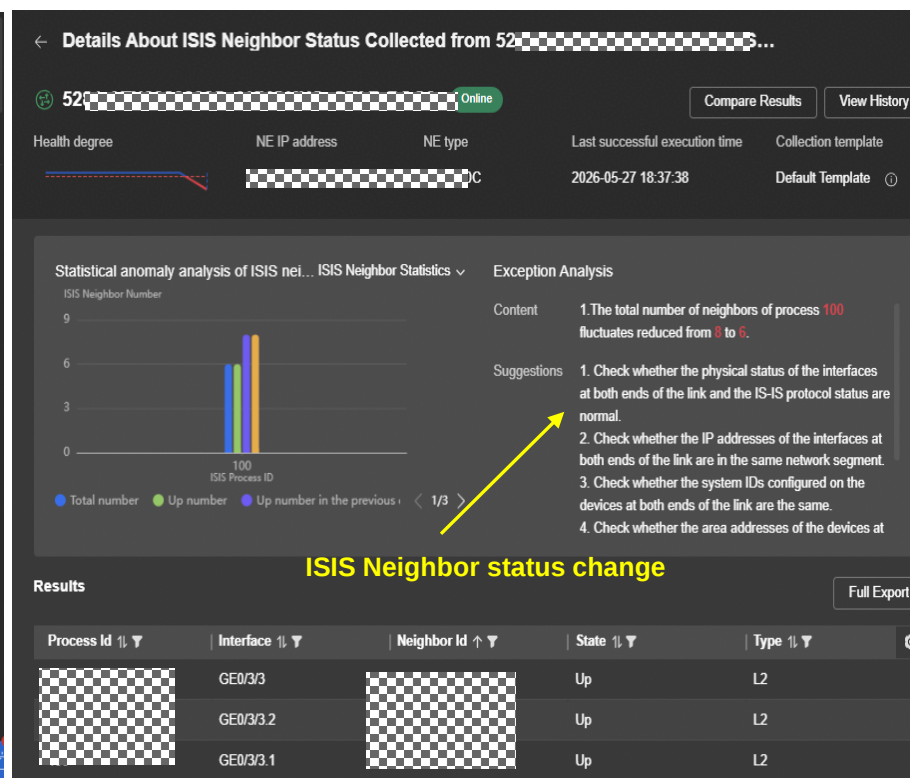
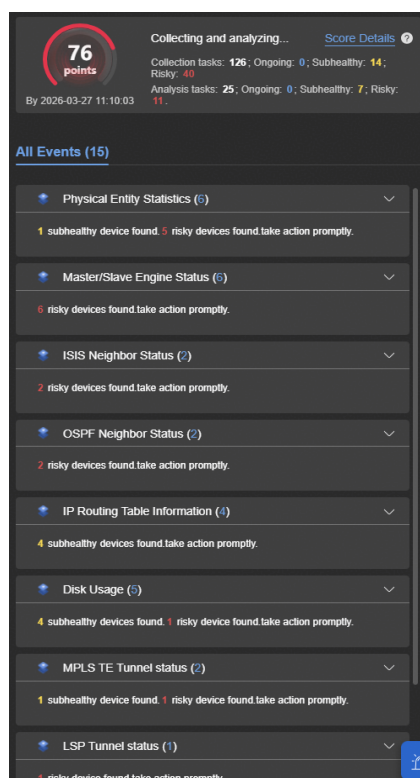


Fault Identification ,Risk identification-2

Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal
B	B	B

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Fault Identification ,Risk identification, impact analysis	15%	How does the System support fault identification, risk identification and subsequent impact analysis? Note: These four sub-scenarios are required to consider petential risk: Optical Module Failure or Optical Power Abnormal, High Error Rate, Protocol State Abnormal, VPN Degradation.	The system identifies faults, potential risk and subsequent impact with severity based on AL modes without need for Human intervention. Note: The AI models should conduct analysis based on multi-dimensional data including service topology (e.g., consists of L2VPN, L3VPN, L2EVPN, L3EVPN, SRv6-Policy, etc.), physical topology, performance data, alarm correlations, etc.	The System identifies faults, potential risk and subsequent impact based on Dynamic programmable rules (configurable or ML), but may needs human confirmation	The System identifies faults, potential risk and subsequent impact based on manually defined rules	Fault, potential risk and impact need to be manually identified based on human expertise or through the execution of manual written procedures.

Example evidence for option B:



Fault Demarcation-1

		Optical Module Failure or Optical Power Abnormal		Port Failure	Protocol State Abnormal	
		A		A	A	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Fault Demarcation	15%	How does the system support fault demarcation? Note: 1) Examples of demarcation involve pinpointing the exact roles of malfunctioning routers, like identifying whether they are access routers, aggregation routers, or Autonomous System Boundary Router (ASBR).	The system automatically demarcates the faults based on AI models without manual intervention.	The system demarcates the faults based on Dynamic programable rules (configurable or ML), results may need manually confirmation.	The system demarcates the faults based on manually defined rules, results need manually confirmation.	Manually demarcates the fault based on data such as operation logs and captured packets.

Example evidence for option A: The system intelligently demarcate for the exact device that cause the fault by invoking dynamic generated COT by LLM

Sub-scenario: Optical Module Failure

[fault_replay]

Fault ID: [fault-516711918]

Fault diagnosis task ID: 4b91ed20-57ae-4d71-8760-c650c616e271

Fault detection time: 2026-05-28 18:23:13 +08:00

Fault Object: ISIS Sys Instance=100 ISIS Sys Level Index=Level2IS ISIS Circ If Index=8 ISIS Pdu Lsp Id=0070.0700.400

diagnosis details.

Call 'Optical Module Fault Diagnosis' Cot, analysis process:

Fault Cause Analysis Completed

Cause Analysis Result Summary

Cause: [redacted] 10/6: The input optical power was too low.

Suggestion: 1. Run the display interface command in the user view to check whether the current transmit optical power (Tx power) of the local interface is in the normal range. If no, go to step 4.

- If the peer interface is not down and no alarm is generated, go to step 4.

- Rectify the fault that causes the peer interface to go down and triggers an alarm.

2. Check whether the optical fiber is faulty by replacing the optical fiber.

3. Check whether an alarm is generated on the local interface. If the optical module is pluggable, replace the optical module. If the optical module is not pluggable or the alarm persists after the optical module is replaced, go to step 4.

4. Collect alarm, log, and configuration information, and contact technical support engineers.

5. End.

Fault Diagnosis Process Completed

Check Whether the Device is Online

Proceed to diagnose other faults.

Give the exact device, port name and related performance data

Fault Diagnosis Process Completed

Check Whether the Port is Optical Port

Check Whether the Link between Ports is Disconnected

The RxTx and optical power have been detected. No line faults were found. Proceed to diagnose other potential faults.

Query NE Optical Power Info:

Ne Name	Port Name	Transmit Optical Power(dBm)	Receive Optical Power(dBm)
[redacted]	25GE3/0/6	-1.96	-11.35

Peer NE Optical Power Info:

Ne Name	Port Name	Transmit Optical Power(dBm)	Receive Optical Power(dBm)
[redacted]	GigabitEthernet2/0/6	-2.18	-16.53

Cot - Optical Module Exception Diagnosis

Sub-scenario: Port Failure

[fault_replay]

Fault ID: [fault-516711918]

Fault diagnosis task ID: 4b91ed20-57ae-4d71-8760-c650c616e271

Fault detection time: 2026-05-28 18:23:13 +08:00

Fault Object: ISIS Sys Instance=100 ISIS Sys Level Index=Level2IS ISIS Circ If Index=8 ISIS Pdu Lsp Id=0070.0700.400

diagnosis details.

Call 'Port Fault Diagnosis' Cot, analysis process:

Fault Cause Analysis Completed

Cause Analysis Result Summary

Cause: The NE is unreachable due to device power failure or optical cable fault. The following network elements are out of management: [redacted] 10/6: The input optical power was too low.

Suggestion: Please check the power supply and optical cable connectivity of NEs.

Fault Diagnosis Process Completed

Check Whether the Port is Physical Port

Check Whether the Link between Ports is Disconnected

The RxTx and optical power have been detected. No line faults were found. Proceed to diagnose other potential faults.

Find out the fault location and give the logical topology

Fault Diagnosis Process Completed

Query current uncleared IS-IS alarms on NE

Unknown step

Cot - Port Fault Diagnosis

No abnormalities were detected in the above diagnostics. If any faults persist, please escalate the issue to technical support for manual resolution.

Query the Peer Port

Peer port found, Peer port: [redacted] 0/0. Proceed to diagnose other peer port potential faults.

Check IS-IS Port Configuration at Both Local End and Peer End

Ne Name	Port Name	MTU	IP Address	Circuit Type	Auth Mode
[redacted]	25GE1/0/1	9600	[redacted]	p2p	simple
[redacted]	25GE1/0/0	9600	[redacted]	p2p	-

Cause: NE [redacted] port 25GE1/0/1 and NE [redacted] C3 port 25GE1/0/0 have inconsistent ISIS configurations.

1. The authentication mode does not match

Suggestion: Modify the configuration to ensure that the configuration is consistent on both ends.

Sub-scenario: IS-IS Adjacency Changed

[fault_replay]

Fault ID: [fault-516711918]

Fault diagnosis task ID: 4b91ed20-57ae-4d71-8760-c650c616e271

Fault detection time: 2026-05-28 18:23:13 +08:00

Fault Object: ISIS Sys Instance=100 ISIS Sys Level Index=Level2IS ISIS Circ If Index=8 ISIS Pdu Lsp Id=0070.0700.400

diagnosis details.

Call 'ISIS Neighbor State Abnormal Diagnosis' Cot, analysis process:

Fault Cause Analysis Completed

Cause Analysis Result Summary

Cause: NE [redacted] 2 port 25GE1/0/1 and NE [redacted] C3 port 25GE1/0/0 have inconsistent ISIS configurations.

1. The authentication mode does not match

Suggestion: Modify the configuration to ensure that the configuration is consistent on both ends.

Fault Diagnosis Process Completed

Query current uncleared IS-IS alarms on NE

Unknown step

Cot - Port Fault Diagnosis

No abnormalities were detected in the above diagnostics. If any faults persist, please escalate the issue to technical support for manual resolution.

Query the Peer Port

Peer port found, Peer port: [redacted] 0/0. Proceed to diagnose other peer port potential faults.

Check IS-IS Port Configuration at Both Local End and Peer End

Ne Name	Port Name	MTU	IP Address	Circuit Type	Auth Mode
[redacted]	25GE1/0/1	9600	[redacted]	p2p	simple
[redacted]	25GE1/0/0	9600	[redacted]	p2p	-

Cause: NE [redacted] port 25GE1/0/1 and NE [redacted] C3 port 25GE1/0/0 have inconsistent ISIS configurations.

1. The authentication mode does not match

Suggestion: Modify the configuration to ensure that the configuration is consistent on both ends.

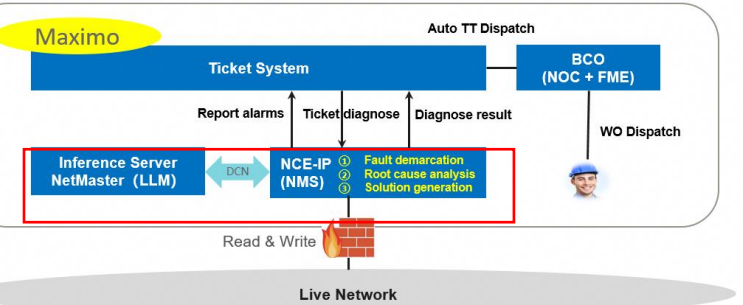
Demarcate the fault caused by configuration

Fault Demarcation-2

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Fault Demarcation	15%	How does the system support fault demarcation? Note: 1) Examples of demarcation involve pinpointing the exact roles of malfunctioning routers, like identifying whether they are access routers, aggregation routers, or Autonomous System Boundary Router (ASBR).	The system automatically demarcates the faults based on AI models without manual intervention.	The system demarcates the faults based on Dynamic programmable rules (configurable or ML), results may need manually confirmation.	The system demarcates the faults based on manually defined rules, results need manually confirmation.	Manually demarcates the fault based on data such as operation logs and captured packets.

Example evidence for option A: The system intelligently demarcate for the exact device that cause the fault by invoking dynamic generated COT by LLM

Scenario: IS-IS Adjacency Changed



Locate the root cause and fix the following fault:
Alarm Source: T-T030276(M1) -POC2
IP Address: 182.169
Name: IS-IS Adjacency Changed
Other Information: T-T030276(M1) -POC2: ISIS Circ Index=5 ISIS Adj State=down If Name=GigabitEthernet0/2/1 Reason=isNbrHoldTimeExpired

Fault Demarcation task has been done automatically by NMS with AI, no user action history.

The other scenarios are the same way to invoke the AI model

AI Model preliminary analysis the issue by knowledge

The IS-IS adjacency on interface GigabitEthernet0/2/1 went down because the Hold Timer expired (180s/180s). This means the local device stopped receiving IS-IS Hello packets (III - IS-IS Hello Packets) from its neighbor within the configured hold time interval. Common causes for this specific error include:

- Physical Layer Issues: Cable faults, SFP/module failures, or link flapping on GigabitEthernet0/2/1.
- MTU Mismatch: If the MTU on the local interface or the neighbor is smaller than the IS-IS packet size, Hellos may be dropped.
- IS-IS Timer Mismatch: The Hello Interval or Hold Time configured on the local interface does not match the neighbor's configuration, causing premature timeout.
- CPU/Resource Constraints: High CPU usage on either the local or neighbor device causing delayed processing of IS-IS Hellos.
- ACL/Filtering: An ACL or firewall rule blocking IS-IS protocol traffic (IP Protocol 124 or Ethernet Type 0x8137/0x8138).

Recommended Fix Steps

- Check Physical Link Status
- Verify IS-IS Neighbor Status
- Confirm the if the neighbor is listed and its state.
- Check the Hello Interval and Hold Timer values.

AI model CoT diagnosis guiding principles

• Ensure the Interface is UP and UP.

• Check for errors (CRC, input/output errors) or flapping.

• If errors are present, replace the cable or SFP module.

AI model CoT diagnose steps show RCA process

The root cause is IS-IS authentication mismatch between the two endpoints on GE0/2/1. Now let me check the peer device's authentication configuration. The neighbor system ID is 3205.2895.4026. Let me check the third neighbor of the affected device: This is likely the peer - System ID 3205.2895.4026 maps to device 182.169.182.169. Let me check its IS-IS config on the interface connected to 182.169. The peer on GE0/2/1 is in the same state as the local device. This confirms the authentication issue is preventing the adjacency from establishing. Let me check the peer device's interface config:

No authentication line returned - confirmed removed.

AI model demarcate the fault position by CoT

Root cause identified. Here's the comparison:

Item	182.169 (GE0/2/1)	182.26 (GE0/2/8)
IP Address	11.2/30	11.1/30
IS-IS Enable	isis enable 200	isis enable 200
Circuit Type	p2p	p2p
Authentication	isis authentication-mode simple cipher %^%#...	Not configured

The root cause is clear: Device 182.169 has IS-IS authentication configured on GE0/2/1, but the peer device 182.26 does not have any authentication configured on GE0/2/8. This authentication mismatch causes Hello packets to be rejected with 'Bad Authentication' errors (47 counted), preventing the IS-IS adjacency from establishing. Now let me fix this. I need to either:

- Add matching authentication on the peer device (182.26), or
- Remove authentication from 182.169.

Since the peer is stuck in 'Init' state and the auth failure is the blocker, the safest fix is to remove the authentication from 182.169 (Since the peer never had it configured, suggesting it was added unilaterally on 182.169). However, removing security config could be a policy concern. Let me remove authentication from 182.169 have auth: GE0/2/3 (which is the only other IS-IS interface configured). This confirms that authentication was added only on GE0/2/1 without configuring the peer side. The fix is to remove the authentication from GE0/2/1 to match the peer. Let me apply the fix: Configuration change applied (pending commit). Let me commit it: Configuration committed. Now let me verify the fix by checking if the IS-IS adjacency comes back. Now let me check the IS-IS peer status: The IS-IS adjacency on GE0/2/1 is now UP. The peer 182.26 (System ID 3205.2895.4026) is showing state up with Hold time 23s. Let me also verify from the peer side: Peer device also shows the adjacency as up. Let me do a final verification of the interface config: No authentication line returned - confirmed removed.

Summary

Root Cause

- IS-IS authentication mismatch between the two endpoints of the link.
- 182.169 (GE0/2/1) had isis authentication-mode simple cipher configured
- 182.26 (GE0/2/8) had no IS-IS authentication configured

This caused all IS-IS Hello packets from 182.26 to be rejected by 182.169 with authentication failure. Evidence:

- display isis 200 peer-change showed Details: Auth Failed at 2026-06-14 14:04:09
- display isis error interface GigabitEthernet 0/2/1 showed Bad Authentication: 47 error packets

Fix Applied

Removed the unilateral IS-IS authentication configuration from interface GE0/2/1 on device 182.169:

```
undo isis authentication-mode commit
```

Verification

- 182.169: display isis 200 peer: now shows 182.26* GE0/2/1 Up 23s 1s
- 182.26: display isis 200 peer: now shows 18.169* GE0/2/8 Up 27s 1s
- IS-IS adjacency is fully restored on both sides

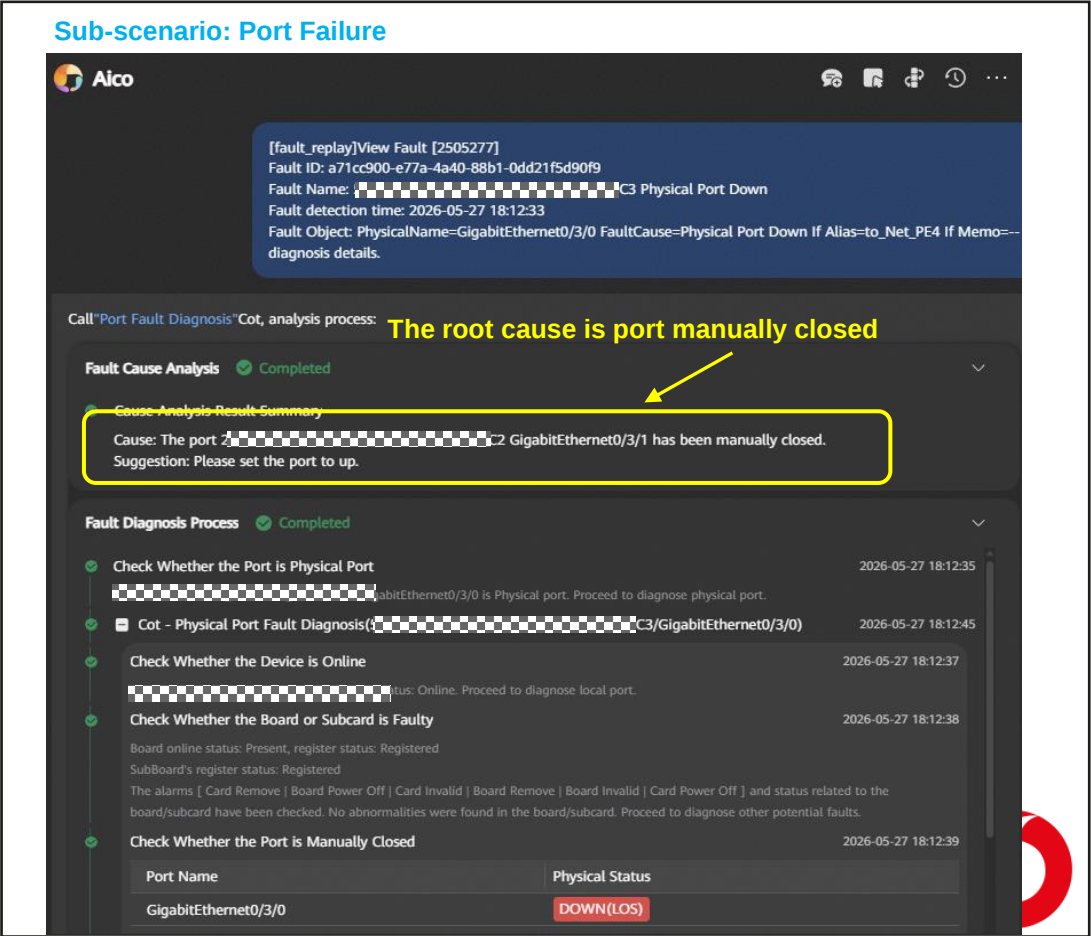
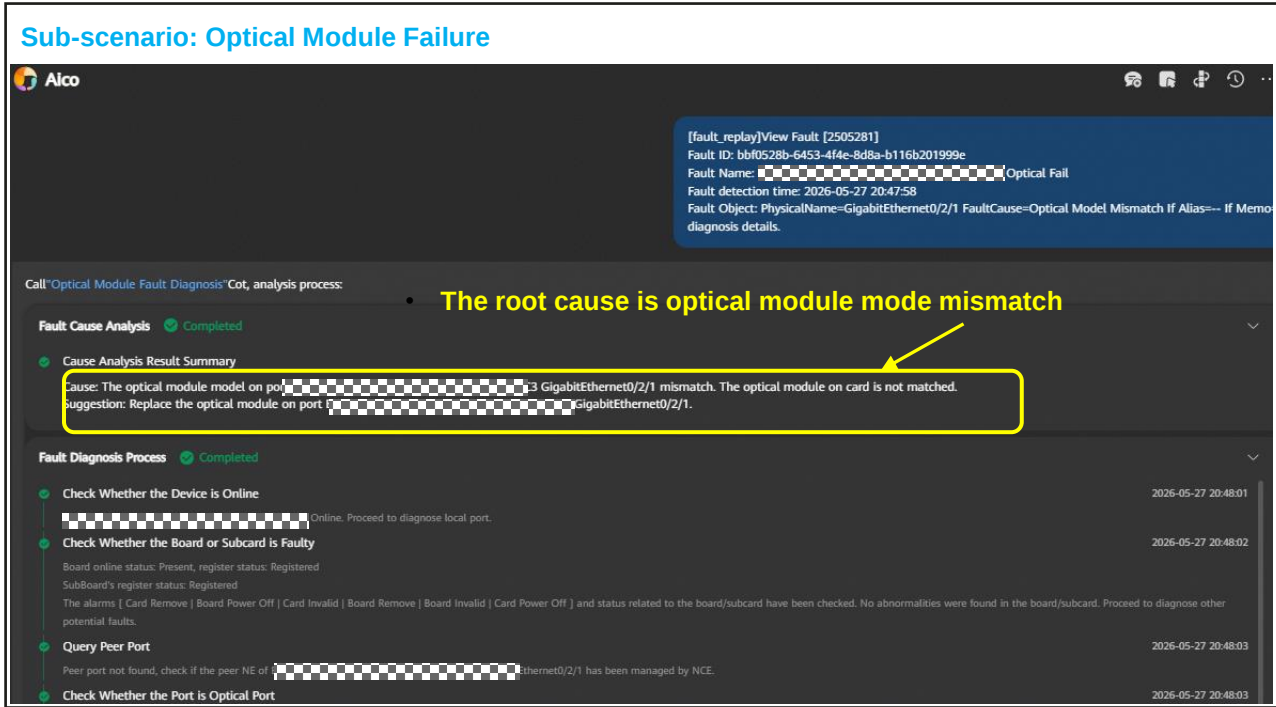
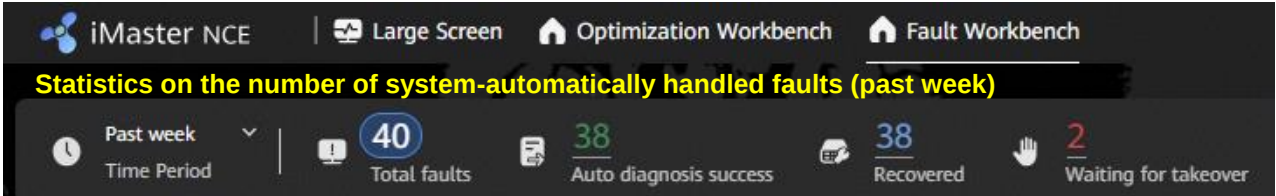


Fault Locating and Root Cause Analysis-1

Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal
A	A	A

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Fault Locating and Root Cause Analysis	15%	How does the system support root cause analysis? Note: 1) Examples of detailed causes of identified faults, including the smallest replaceable unit, software modules, and ports.	The system automatically analyzes root cause based on AI models without manual intervention.	The system provides one or more suspected causes based on Dynamic programable rules (configurable or ML), results may need human confirmation.	The system provides cause analysis based on manually defined rules, manually analyze and confirm the root cause.	Manually analyze root cause based on expertise.

Example evidence for option A: Base on the diagnosis COT, further analyze for the root cause



Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal
A	A	A

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Fault Locating and Root Cause Analysis	15%	How does the system support root cause analysis? Note: 1) Examples of detailed causes of identified faults, including the smallest replaceable unit, software modules, and ports.	The system automatically analyzes root cause based on AI models without manual intervention.	The system provides one or more suspected causes based on Dynamic programmable rules (configurable or ML), results may need human confirmation.	The system provides cause analysis based on manually defined rules, manually analyze and confirm the root cause.	Manually analyze root cause based on expertise.

Sub-scenario: Protocol State Abnormal

[illegible][illegible]

Fault: Diagnosis Process

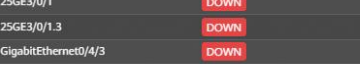
Completed

Provide the analysis process, all of the links connect to this NE are broken

Check Ports

Status of links at the border of an disconnection scope

Network Element	Port	Physical Status	Protocol Status
	FlexE-50G0/5/1	DOWN	DOWN
	GigabitEthernet0/3/0	DOWN	DOWN
	GigabitEthernet0/3/0.1	DOWN	DOWN
	25GE3/0/1	DOWN	DOWN
	25GE3/0/1.3	DOWN	DOWN
	GigabitEthernet0/4/3	DOWN	DOWN



Cause: The NE is unreachable due to device power failure or optical cable fault. The following network elements are out of management:

as follows:

3. The interrupted links are as follows:

Alco

[fault_replay]

Fault ID: [fault-516711918]

Fault diagnosis task ID: 4b91ed20-57ae-4d71-8760-c650c616e271

IS-IS Adjacency Changed

Fault detection time: 2026-05-28 18:23:13 +08:00

Fault Object: ISIS Sys Instance=100 ISIS Sys Level Index=level2ISIS ISIS Circ If Index=8 ISIS Pdu Lsp Id=0070.0700.4000

diagnosis details.

The root cause is authentication mode does not match

Call ISIS Neighbor State Abnormal Diagnosis Cot, analysis process:

Fault Cause Analysis

Completed

Cause Analysis Result Summary

Cause: NE C2 port 25GE1/0/1 and NE C3 port 25GE1/0/0 have inconsistent ISIS configurations.

1. The authentication mode does not match

Suggestion: Modify the configuration to ensure that the configuration is consistent on both ends.

Fault Diagnosis Process

Completed

Query current uncleared IS-IS alarms on NE

Unknown step

Cot - Port Fault Diagnosis

No abnormalities were detected in the above diagnostics. If any faults persist, please escalate the issue to technical support for manual resolution.

Query the Peer Port

Peer port found, Peer port C3 port 25GE1/0/0. Proceed to diagnose other peer port potential faults.

Check IS-IS Port Configuration at Both Local End and Peer End

Expand all

05-28 18:23:17

05-28 18:24:08

05-28 18:24:08

05-28 18:24:09

05-28 18:24:09

Check the IS-IS configuration on both side find out Auth Mode is inconsistent

Ne Name	Port Name	MTU	IP Address	Circuit Type	Auth Mode
C2	25GE1/0/1	9600	C2	p2p	simple
C3	25GE1/0/0	9600	C3	p2p	-

Cause: C2 POC port 25GE1/0/1 and NE C3 port 25GE1/0/0 have inconsistent ISIS configurations.

1. The authentication mode does not match

Suggestion: Modify the configuration to ensure that the configuration is consistent on both ends.

Call ISIS Neighbor State Abnormal Diagnosis: Col, analysis process:

Fault Cause Analysis Completed

Cause Analysis Result Summary

Cause: NE # [redacted] port 25GE1/0/1 and NE # [redacted] port 25GE1/0/0 have inconsistent ISIS configurations.
1. The authentication mode does not match
Suggestion: Modify the configuration to ensure that the configuration is consistent on both ends.

Fault Diagnosis Process Completed

- Query current uncleared IS-IS alarms on NE ▾
- Unknown step ^

Cot - Port Fault Diagnosis

No abnormalities were detected in the above diagnostics. If any faults persist, please escalate the issue to technical support for manual resolution.

Query the Peer Port

Peer port found, Peer port [redacted] E1/0/0. Proceed to diagnose other peer port potential faults.

Check IS-IS Port Configuration at Both Local End and Peer End

Ne Name	Port Name	MTU	IP Address	Circuit Type	Auth Mode
[redacted]	25GE1/0/1	9600	[redacted]	p2p	simple
	25GE1/0/0	9600	[redacted]	p2p	-

Cause: [redacted] POC2 port 25GE1/0/1 and NE [redacted] OC3 port 25GE1/0/0 have inconsistent ISIS configurations.
 1. The authentication mode does not match
 Suggestion: Modify the configuration to ensure that the configuration is consistent on both ends.

Fault Locating and Root Cause Analysis-3

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Fault Locating and Root Cause Analysis	15%	How does the system support root cause analysis? Note: 1) Examples of detailed causes of identified faults, including the smallest replaceable unit, software modules, and ports.	The system automatically analyzes root cause based on AI models without manual intervention.	The system provides one or more suspected causes based on Dynamic programable rules (configurable or ML), results may need human confirmation.	The system provides cause analysis based on manually defined rules, manually analyze and confirm the root cause.	Manually analyze root cause based on expertise.

Example evidence for option A: Base on the diagnosis COT, further analyze for the root cause

Scenario: IS-IS Adjacency Changed

Locate the root cause and fix the following fault:
Alarm Source: T-1030276(M1) - POC2
IP Address: 182.169
Name: IS-IS Adjacency Changed
Other Information: T-1030276(M1) - POC2: ISIS Circ Index=5 ISIS
Adj State=down If Name=GigabitEthernet0/2/1 Reason=isNbrHoldTimeExpired

Diagnose task invoke AI Model

AI Model preliminary analysis

Based on the alarm information and knowledge base search, here is the root cause analysis and fix:

Root Cause: The IS-IS adjacency on interface GigabitEthernet0/2/1 went down because the Hold Time expired (180 seconds).

Analysis: This means the local device stopped receiving IS-IS Hello packets (HELLO IS-IS Hello Packets) from its neighbor within the configured hold time interval. Common causes for this specific error include:

1. **Physical Layer Issues:** Cable faults, SFP/module failures, or link flapping on GigabitEthernet0/2/1.
2. **MTU Mismatch:** If the MTU on the local interface or the neighbor is smaller than the IS-IS packet size, Hellos may be dropped.
3. **IS-IS Timer Mismatch:** The Hello Interval or Hold Timer configured on the local interface does not match the neighbor's configuration, causing premature timeout.
4. **CPU/Resource Constraints:** High CPU usage on either the local or neighbor device causing delayed processing of IS-IS Hellos.
5. **ACL/Filtering:** An ACL or firewall rule blocking IS-IS protocol traffic (IP Protocol 124 or EtherType 0x00000000).

Recommended Fix Steps:

1. **Check Physical Link Status:**
 - Ensure the interface is UP and UP.
 - Check for errors (CRC input/output errors) or flapping.
 - Check if errors are present, replace the cable or SFP module.
2. **Verify IS-IS Neighbor Status:**
 - Confirm if the neighbor is listed and its state.
 - Check the **Hold Interval** and **Hold Timer** values.

AI model CoT diagnose guiding principles

Root Cause Identified: The root cause is authentication failure. The adjacency went down due to authentication failure. The error statistics clearly show: 47 Hello packets were rejected due to authentication failure.

Analysis: The peer device (182.169) has IS-IS authentication configured on GE0/2/1, but the peer device (182.26) does not have any authentication configured on GE0/2/1. This authentication mismatch causes Hello packets to be rejected with Bad Authentication errors (47 counted), preventing the IS-IS adjacency from establishing.

Now let me fix this. I need to either:

1. Add multilink authentication on the peer device (182.26).
2. Check IS-IS interface and process configuration.

Find out the root cause

Item	182.169 (GE0/2/1)	182.26 (GE0/2/1)
IP Address	11.2/30	11.1/30
IS-IS Enable	isis enable 200	isis enable 200
Circuit Type	p2p	p2p
Authentication	isis authentication-mode simple cipher %^%#...	Not configured

The root cause is clear: Device 182.169 has IS-IS authentication configured on GE0/2/1, but the peer device 182.26 does not have any authentication configured on GE0/2/1. This authentication mismatch causes Hello packets to be rejected with Bad Authentication errors (47 counted), preventing the IS-IS adjacency from establishing.

Now let me fix this. I need to either:

1. Add multilink authentication on the peer device (182.26).
2. Check IS-IS interface and process configuration.

Ticket start and end time

Remote repair confirmation

The other scenarios are the same way to invoke the AI model

Log for the AI model root cause analysis



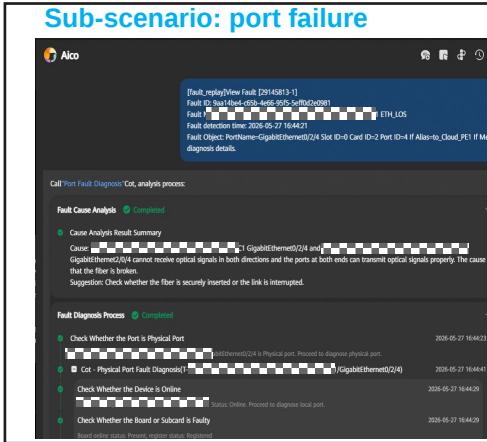
Solution Generation-1

Solution Generation-1

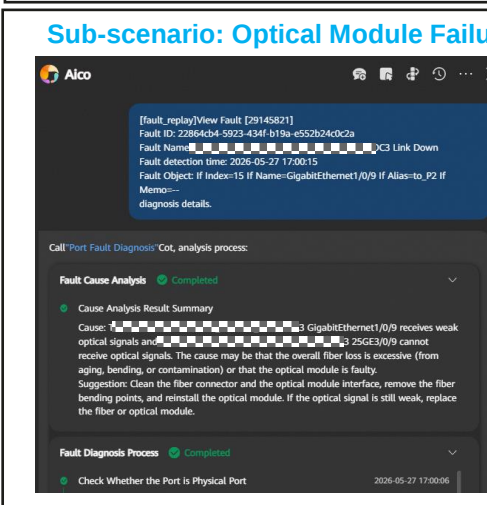
			Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal	
			B	B	B	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Solution Generation	10%	How does the System support generation of fault recovery solutions?	The System generates the optimal recovery or fault rectification solution based on AI models without the need for Human confirmation	The System generates multiple possible recovery or rectification solutions, but may need human confirmation.	The System generates the optimal recovery or fault rectification solution through predefined rules and needs Human confirmation	The recovery solution needs to be manually generated based on human expertise

Example evidence for option B: The system automatically generate the close-loop recovery solution or rectification suggestion

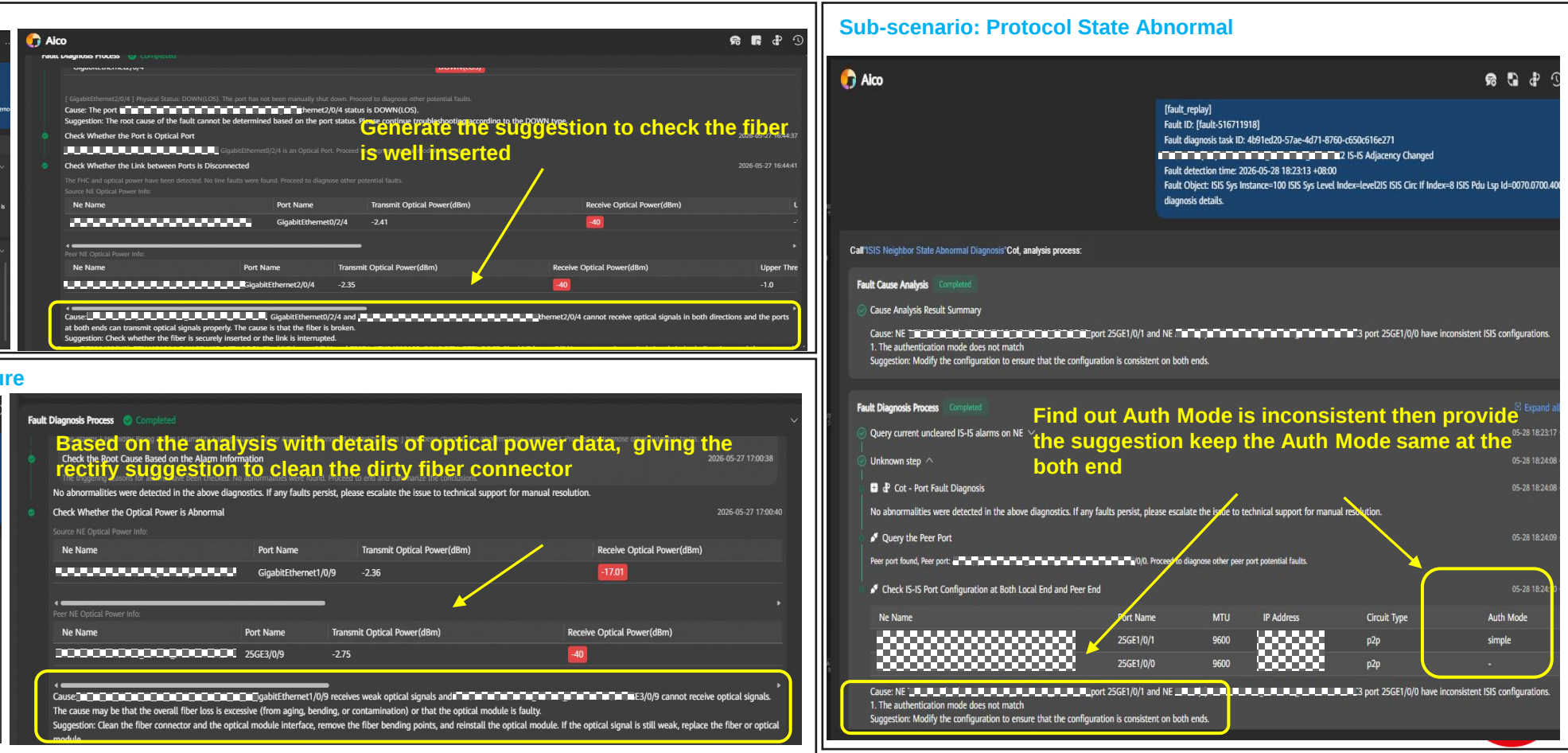
Sub-scenario: port failure



Sub-scenario: Optical Module Failure



Sub-scenario: Protocol State Abnormal



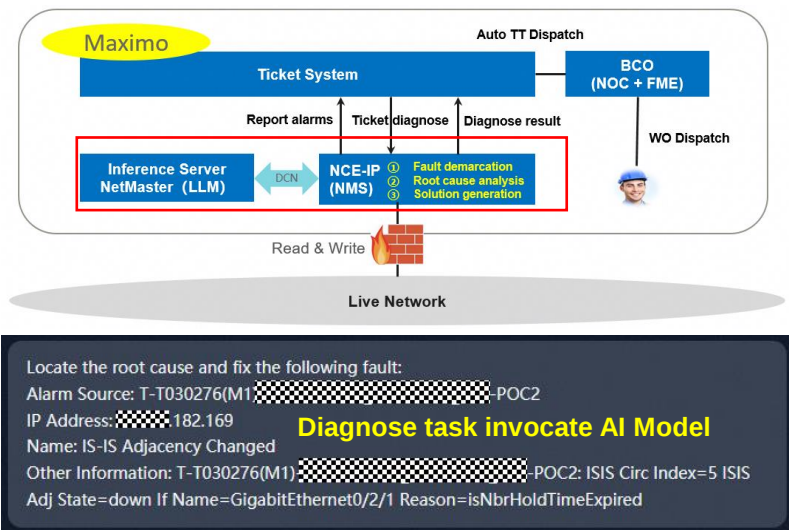
Solution Generation-2

Solution Generation-2

		Optical Module Failure or Optical Power Abnormal		Port Failure	Protocol State Abnormal	
		B		B	B	
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Solution Generation	10%	How does the System support generation of fault recovery solutions?	The System generates the optimal recovery or fault rectification solution based on AI models without the need for Human confirmation	The System generates multiple possible recovery or rectification solutions, but may need human confirmation.	The System generates the optimal recovery or fault rectification solution through predefined rules and needs Human confirmation	The recovery solution needs to be manually generated based on human expertise

Example evidence for option B: The system automatically generate the close-loop recovery solution or rectification suggestion

Scenario: IS-IS Adjacency Changed



Diagnose task invoke AI Model

The other scenarios are the same way to invoke the AI model

(Note: Use debugging cautiously in production environments.) I'll analyze this IS-IS adjacency failure and work through the diagnostic steps systematically.

Let me find the device and its neighbor first.

Good. The affected device is 182.169 (resId: 8256a335-2a02-4a23-866a-a920d04895) and it has a neighbor at 182.26 (resId: a28866b0-062a-4a87-8286-5886a9a0a835). The alarm indicates IS-IS adjacency down on interface GigabitEthernet0/2/1, with reason (timersNotSynced). (Hold timer expired).

Let me start the diagnostic steps.

Step 1: Check the interface status on the affected device.

Interface is UP, line protocol is UP. Multicast packets are being received (153M) and sent (2.3M), so multicast connectivity appears fine. Let me check the IS-IS configuration.

Step 2: Check IS-IS interface and process configuration.

Now let me check the IS-IS peer status and last peer change info.

Interesting — the IS-IS peer on GE0/2/1 is not showing in the peer list. Only two peers are up: one on GE0/2/3 and one on Flex0/79/207. The adjacency on GE0/2/1 is indeed down.

Let me check the last peer change and error info.

Key finding! The most recent peer change on GE0/2/1 shows:

```
Time : 2024-06-14 14:04:09.031000
System Id : 0250.2500.4026
Interface : GE0/2/1 (T)
State : Up -> Down
Details : Auth Failed
```

The root cause is authentication failure. The adjacency went down due to Auth Failed, not hold timer expired. The alarm reason (timersNotSynced) was from an earlier event, but the latest failure is authentication mismatch.

Let me also check the IS-IS error statistics to confirm.

Confirmed. The error statistics clearly show:

- * Bad Authentication: 47 — 47 Hello packets were rejected due to authentication failure
- * Bad Circuit type: 2 — Minor, 2 packets with bad circuit type

The root cause is IS-IS authentication mismatch between the two endpoints on GE0/2/1. Now let me check the peer device's authentication configuration. The neighbor System ID is 0250.2500.4026. Let me find which device that is:

Let me check the other neighbor 182.26 to see if it's connected on the same link.

This device (182.26) has peer 0250.2500.4026 (which is our affected device 182.169) but on Flex0/79/207, not on the GE0/2/1 link. The neighbor with System ID 0250.2500.4026 is a different device. Let me find it.

Let me check the third neighbor of the affected device:

This is likely the peer — System ID 0250.2500.4026 maps to device 151515.182.26. Let me check its IS-IS config on the interface connected to 182.169:

The peer on GE0/2/8 is in state: state — stuck, not reaching up. This confirms the authentication issue is preventing the adjacency from establishing. Let me check the peer's authentication config.

AI model CoT diagnose process

Root cause identified. Here's the comparison:

Item	182.169 (GE0/2/1)	182.26 (GE0/2/8)
IP Address	11.2/30	11.1/30
IS-IS Enable	isis enable 200	isis enable 200
Circuit Type	p2p	p2p
Authentication	isis authentication-mode simple cipher %^%#...	Not configured

The root cause is clear: Device 182.169 has IS-IS authentication configured on GE0/2/1, but the peer device 182.26 does not have any authentication configured on GE0/2/8. This authentication mismatch causes Hello packets to be rejected with Bad Authentication errors (47 counted), preventing the IS-IS adjacency from establishing.

Now let me fix this. I need to either:

- Add matching authentication on the peer device (182.26), or
- Remove authentication from 182.169

Since the peer is stuck in state: state and the auth failure is the blocker, the safest fix is to remove the authentication from 182.169 (since the peer never had it configured, suggesting it was added unilaterally on 182.169). However, removing security config could be a policy concern. Let me check if there's a pattern — let me see if other interfaces on 182.169 have auth:

GE0/2/3 (which has a working IS-IS peer) does not have authentication configured. This confirms that authentication was added only on GE0/2/1 without configuring the peer side. The fix is to remove the authentication from GE0/2/1 to match the peer.

Let me apply the fix:

Configuration change applied (pending commit). Let me commit it:

Configuration committed. Now let me verify the fix by checking if the IS-IS adjacency comes up:

Now let me check the IS-IS peer status:

The IS-IS adjacency on GE0/2/1 is now UP. The peer 182.26 (System ID 0250.2500.4026) is showing state up, with HoldTime 23s.

Let me also verify from the peer side:

Peer device also shows the adjacency as up. Let me do a final verification of the interface config:

No authentication line returned — confirmed removed.

AI model generated candidate solutions

Root cause identified. Here's the comparison:

Item	182.169 (GE0/2/1)	182.26 (GE0/2/8)
IP Address	11.2/30	11.1/30
IS-IS Enable	isis enable 200	isis enable 200
Circuit Type	p2p	p2p
Authentication	isis authentication-mode simple cipher %^%#...	Not configured

The root cause is clear: Device 182.169 has IS-IS authentication configured on GE0/2/1, but the peer device 182.26 does not have any authentication configured on GE0/2/8. This authentication mismatch causes Hello packets to be rejected with Bad Authentication errors (47 counted), preventing the IS-IS adjacency from establishing.

Now let me fix this. I need to either:

- Add matching authentication on the peer device (182.26), or
- Remove authentication from 182.169

Since the peer is stuck in state: state and the auth failure is the blocker, the safest fix is to remove the authentication from 182.169 (since the peer never had it configured, suggesting it was added unilaterally on 182.169). However, removing security config could be a policy concern. Let me check if there's a pattern — let me see if other interfaces on 182.169 have auth:

GE0/2/3 (which has a working IS-IS peer) does not have authentication configured. This confirms that authentication was added only on GE0/2/1 without configuring the peer side. The fix is to remove the authentication from GE0/2/1 to match the peer.

Let me apply the fix:

Configuration change applied (pending commit). Let me commit it:

Configuration committed. Now let me verify the fix by checking if the IS-IS adjacency comes up:

Now let me check the IS-IS peer status:

The IS-IS adjacency on GE0/2/1 is now UP. The peer 182.26 (System ID 0250.2500.4026) is showing state up, with HoldTime 23s.

Let me also verify from the peer side:

Peer device also shows the adjacency as up. Let me do a final verification of the interface config:

No authentication line returned — confirmed removed.

```
141788 2026-06-14 14:11:25.477 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141789 2026-06-14 14:11:25.527 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141790 2026-06-14 14:11:25.577 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141791 2026-06-14 14:11:25.627 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141792 2026-06-14 14:11:25.676 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141793 2026-06-14 14:11:25.727 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141794 2026-06-14 14:11:25.776 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141795 2026-06-14 14:11:25.827 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141796 2026-06-14 14:11:25.877 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141797 2026-06-14 14:11:25.927 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141798 2026-06-14 14:11:25.977 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141799 2026-06-14 14:11:26.027 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141800 2026-06-14 14:11:26.077 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141801 2026-06-14 14:11:26.126 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141802 2026-06-14 14:11:26.177 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141803 2026-06-14 14:11:26.227 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141804 2026-06-14 14:11:26.276 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141805 2026-06-14 14:11:26.326 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
141806 2026-06-14 14:11:26.377 [trace-mqddui8a-8y00verki] [ForJoinPool.commonPool-worker-1] INFO com.huawei.lingxi.agent.AgentLoop
```

Log for the AI model generate candidate solution



Solution Evaluation & Decision Making-1

Solution Evaluation & Decision Making-1				Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal
				A	A	A
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Solution Evaluation & Decision Making	15%	How does the System support evaluation & decision of fault recovery solutions?	The System evaluates and determines the optimal recovery or fault rectification solution to be executed based on AI models, without the need for Human confirmation	The System evaluates multiple possible recovery or fault rectification solutions and determines the optimal solution to be executed based on Dynamic programmable rules (configurable or ML) , but may need Human confirmation	The recovery of fault rectification solution is manually evaluated and determined	

Example evidence for option A: After receiving the fault ticket, the system automatically generates emergency restoration and solutions.

The system automatically generates an emergency repair solution based on information such as the fault cause and location. The repair solution includes capabilities for two phases:

Phase 1: The system can automatically calculates alternative paths to restore the service which was interrupted by Link or port fault.

Phase 2: The physical faults requiring on-site manual handling, the system provides a detailed repair suggestion to guide maintenance personnel in conducting accurate on-site operations, thereby improving on site work efficiency.

Sub-scenario 1: Link Down fault cause the protect service switch

Major	2620021	Sr Policy Candi Path Down	2886(A2)-PTN3221...	Destination Address=2023:23:3 Color=2241 Protocol Source=BGP(20) N...	1	2026-05-27 03:59:10	2026-05-27 03:59:10
Major	2616033	SR Policy Down	2886(A2)-PTN3221...	Destination Address=2023:23:3 Color=1003 Protocol Source=BGP(20) N...	1	2026-05-27 03:59:10	2026-05-27 03:59:10
Major	2620021	Sr Policy Candi Path Down	2886(A2)-PTN3221...	Endpoint=2023:23:3 Color=1003	1	2026-05-27 03:59:10	2026-05-27 03:59:10
Major	2616033	SR Policy Down	2886(A2)-PTN3221...	PhysicalName=GigabitEthernet2/0/4 If Alias=to_P1 If Memo=...	1	2026-05-27 03:59:10	2026-05-27 03:59:10
Critical	3074752	Physical Port Down	2886(A2)-PTN3221...	Destination Address=2.1.23.3 Colors=100 Protocol Source=BGP(20) Node ...	1	2026-05-27 03:59:11	2026-05-27 03:59:11
Major	2620021	Sr Policy Candi Path Down	2886(A2)-PTN3221...	Endpoint=2.1.23.3 Color=100	1	2026-05-27 03:59:09	2026-05-27 03:59:09
Major	2616033	SR Policy Down	2886(A2)-PTN3221...	If Index=3764 If Name=GigabitEthernet2/0/4.4000 If Alias=to_P1 If Memo=...	1	2026-05-27 03:59:09	2026-05-27 03:59:09
Critical	3	Link Down	2886(A2)-PTN3221...	If Index=4218 If Name=GigabitEthernet2/0/4.3 If Alias=-- If Memo=...	1	2026-05-27 03:59:09	2026-05-27 03:59:09
Critical	3	Link Down	2886(A2)-PTN3221...	If Index=3902 If Name=GigabitEthernet2/0/4.164 If Alias=-- If Memo=...	1	2026-05-27 03:59:09	2026-05-27 03:59:09
Critical	3	Link Down	2886(A2)-PTN3221...	If Index=44 If Name=GigabitEthernet2/0/4 If Alias=to_P1 If Memo=...	1	2026-05-27 03:59:09	2026-05-27 03:59:09
Critical	3	Link Down	2886(A2)-PTN3221...	If Index=4183 If Name=GigabitEthernet2/0/4.2 If Alias=-- If Memo=...	1	2026-05-27 03:59:09	2026-05-27 03:59:09
Critical	3	Link Down	2886(A2)-PTN3221...	If Index=4180 If Name=GigabitEthernet2/0/4.1 If Alias=-- If Memo=...	1	2026-05-27 03:59:09	2026-05-27 03:59:09
Major	1100882	IS-IS Adjacency Changed	2886(A2)-PTN3221...	ISIS Sys Instance=100 ISIS Sys Level Index=level2ISIS Circ If Index=44 IS...	1	2026-05-27 03:59:10	2026-05-27 03:59:10
Major	1100882	IS-IS Adjacency Changed	2886(A2)-PTN3221...	ISIS Sys Instance=100 ISIS Sys Level Index=level2ISIS Circ If Index=4180...	1	2026-05-27 03:59:10	2026-05-27 03:59:10

Path before switchover

Automatically generated fault route switching solution

Path after automatic switching

Alco

[fault_replay]View Fault [29145894-2]
Fault ID: ccb0a085-261d-40bb-9ea4-60413e23e8f8
Fault Name: Link Down
Fault detection time: 2026-05-27 04:05:15
Fault Object: If Index=44 If Name=GigabitEthernet2/0/4 If Alias=to_P1 If Memo=...
diagnosis details.

Further identify the root cause of the fault and provide a repair solution.

Call "Port Fault Diagnosis" Cot analysis process

Fault Cause Analysis Completed

Cause Analysis Result Summary

Cause: The port GigabitEthernet2/0/4 has been manually closed.
Suggestion: Please set the port to up.

Fault Diagnosis Process Completed

Check Whether the Port is Physical Port 2026-05-27 04:05:18
GigabitEthernet2/0/4 is Physical port. Proceed to diagnose physical port.

Port - Physical Port Fault Diagnosis 2026-05-27 04:05:24
1/Gigabit...

Check Whether the Device is Online 2026-05-27 04:05:22
Status: Online. Proceed to diagnose local port.

Check Whether the Board or Subcard is Faulty 2026-05-27 04:05:23

Solution Evaluation & Decision Making-2

Solution Evaluation & Decision Making-2			Optical Module Failure or Optical Power Abnormal		Port Failure	Protocol State Abnormal
			A		A	A
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Solution Evaluation & Decision Making	15%	How does the System support evaluation & decision of fault recovery solutions?	The System evaluates and determines the optimal recovery or fault rectification solution to be executed based on AI models, without the need for Human confirmation	The System evaluates multiple possible recovery or fault rectification solutions and determines the optimal solution to be executed based on Dynamic programmable rules (configurable or ML) , but may need Human confirmation	The recovery of fault rectification solution is manually evaluated and determined	

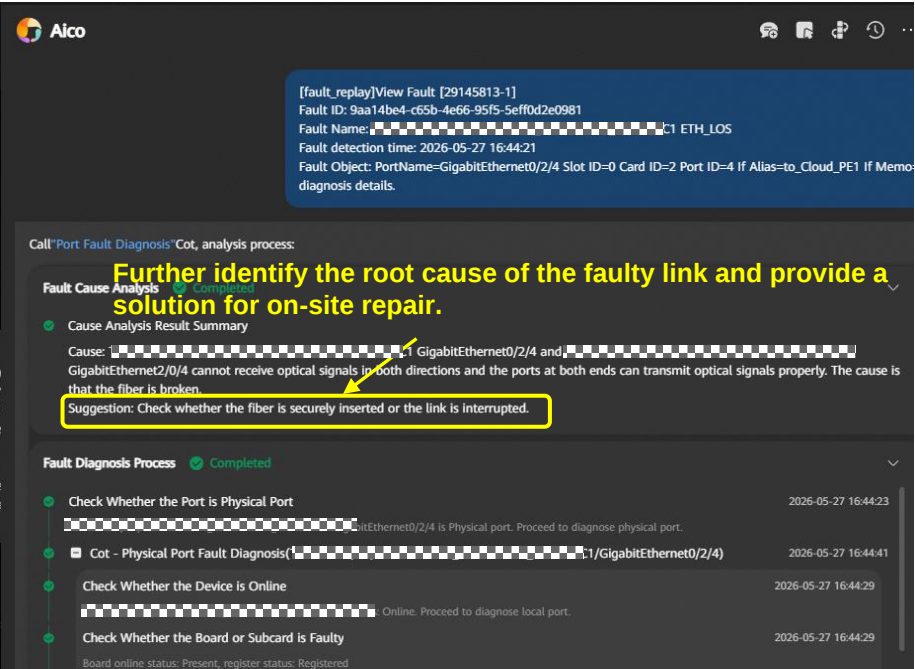
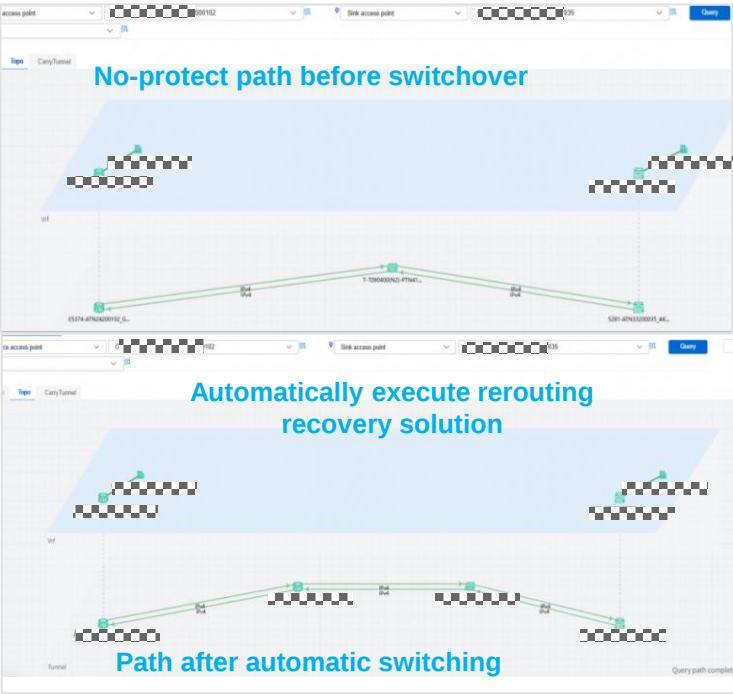
Example evidence for option A: After receiving the fault ticket, the system automatically generates emergency restoration and solutions.

The system automatically generates an emergency repair solution based on information such as the fault cause and location. The repair solution includes capabilities for two phases:

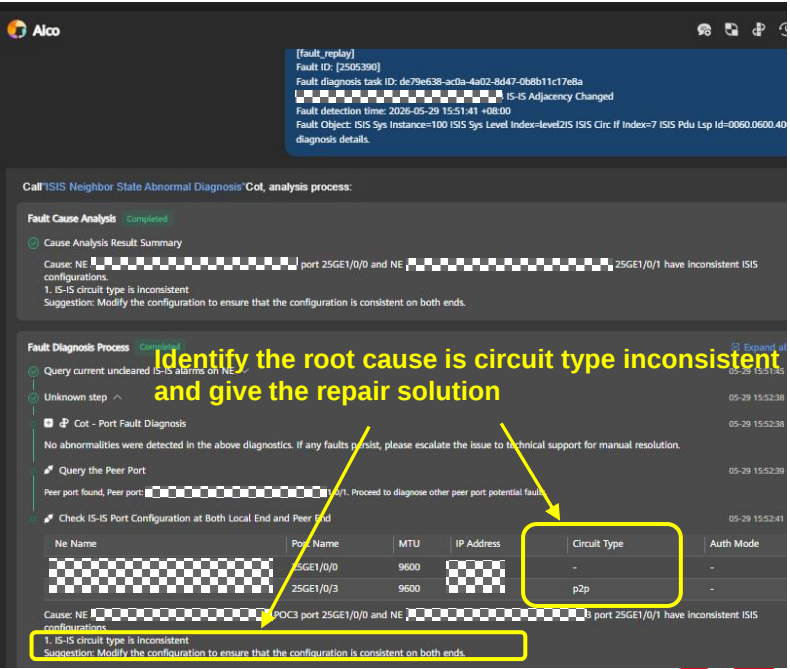
Phase 1: The system can automatically calculates alternative paths to restore the service which was interrupted by Link or port fault.

Phase 2: The physical faults requiring on-site manual handling, the system provides a detailed repair suggestion to guide maintenance personnel in conducting accurate on-site operations, thereby improving on site work efficiency.

Sub-scenario 2: ETH_LOS fault cause the no-protect service reroute



Sub-scenario 3: Protocol State Abnormal

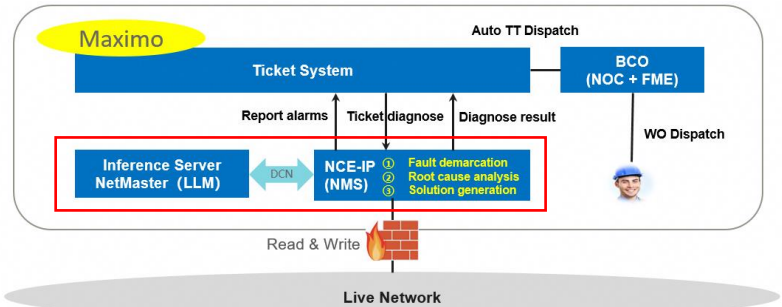


Solution Evaluation & Decision Making-3

	Optical Module Failure or Optical Power Abnormal				Port Failure	Protocol State Abnormal
	A				A	A
Service capability	Weight	Question	Option A	Option B	Option C	Option D
Solution Evaluation & Decision Making	15%	How does the System support evaluation & decision of fault recovery solutions?	The System evaluates and determines the optimal recovery or fault rectification solution to be executed based on AI models, without the need for Human confirmation	The System evaluates multiple possible recovery or fault rectification solutions and determines the optimal solution to be executed based on Dynamic programmable rules (configurable or ML) , but may need Human confirmation	The recovery of fault rectification solution is manually evaluated and determined	

Example evidence for option A: After receiving the fault ticket, the system automatically generates emergency restoration and solutions.

Scenario: IS-IS Adjacency Changed



Locate the root cause and fix the following fault:
Alarm Source: T-T030276(M1) POC2
IP Address: 182.169
Name: IS-IS Adjacency Changed
Other Information: T-T030276(M1) POC2: ISIS Circ Index=5 ISIS
Adj State=down If Name=GigabitEthernet0/2/1 Reason=IsNbrHoldTimeExpired

Diagnose task invoke AI Model

The other scenarios are the same way to invoke the AI model

AI model CoT diagnose process

Root cause is authentication failure. The adjacency went down due to authentication failure. The peer device 182.169 has peer authentication configured on GE0/2/1, but the peer device 182.26 does not have any authentication configured on GE0/2/1. This authentication mismatch causes Hello packets to be rejected with Bad Authentication errors (47 counted), preventing the IS-IS adjacency from establishing.

Now let me fix this. I need to either:

- Add matching authentication on the peer device (182.26), or
- Remove authentication from 182.169

Since the peer is stuck in `DOWN` state and the auth failure is the blocker, the safest fix is to remove the authentication from 182.169 (since the peer never had it configured, suggesting it was added unilaterally on 182.169). However, removing security config could be a policy concern. Let me check if there's a pattern — let me see if other interfaces on 182.169 have auth:

GE0/2/3 (which has a working IS-IS peer) does not have authentication configured. This confirms that authentication was added only on GE0/2/1 without configuring the peer side. The fix is to remove the authentication from GE0/2/1 to match the peer.

Let me apply the fix:

Configuration change applied (pending commit). Let me commit it: Configuration committed. Now let me verify the fix by checking if the IS-IS adjacency comes up:

Now let me check the IS-IS peer status:

The IS-IS adjacency on GE0/2/1 is now UP. The peer 182.26 (System ID 0250.2550.4026) is showing state `Up` with HoldTime 23s.

Let me also verify from the peer side:

Peer device also shows the adjacency as `Up`. Let me do a final verification of the interface config:

No authentication line returned — confirmed removed.

AI model generated candidate solutions

Item	182.169 (GE0/2/1)	182.26 (GE0/2/8)
IP Address	11.1.2.30	11.1.30
IS-IS Enable	isis enable 200	isis enable 200
Circuit Type	p2p	p2p
Authentication	isis authentication-mode simple cipher %*#...	Not configured

The root cause is clear: Device 182.169 has IS-IS authentication configured on GE0/2/1, but the peer device 182.26 does not have any authentication configured on GE0/2/8. This authentication mismatch causes Hello packets to be rejected with Bad Authentication errors (47 counted), preventing the IS-IS adjacency from establishing.

Now let me fix this. I need to either:

- Add matching authentication on the peer device (182.26), or
- Remove authentication from 182.169

Since the peer is stuck in `DOWN` state and the auth failure is the blocker, the safest fix is to remove the authentication from 182.169 (since the peer never had it configured, suggesting it was added unilaterally on 182.169). However, removing security config could be a policy concern. Let me check if there's a pattern — let me see if other interfaces on 182.169 have auth:

GE0/2/3 (which has a working IS-IS peer) does not have authentication configured. This confirms that authentication was added only on GE0/2/1 without configuring the peer side. The fix is to remove the authentication from GE0/2/1 to match the peer.

Let me apply the fix:

Configuration change applied (pending commit). Let me commit it: Configuration committed. Now let me verify the fix by checking if the IS-IS adjacency comes up:

Now let me check the IS-IS peer status:

The IS-IS adjacency on GE0/2/1 is now UP. The peer 182.26 (System ID 0250.2550.4026) is showing state `Up` with HoldTime 23s.

Let me also verify from the peer side:

Peer device also shows the adjacency as `Up`. Let me do a final verification of the interface config:

No authentication line returned — confirmed removed.

AI model make the decision

The root cause is clear: Device 182.169 has IS-IS authentication configured on GE0/2/1, but the peer device 182.26 does not have any authentication configured on GE0/2/8. This authentication mismatch causes Hello packets to be rejected with Bad Authentication errors (47 counted), preventing the IS-IS adjacency from establishing.

Now let me fix this. I need to either:

- Add matching authentication on the peer device (182.26), or
- Remove authentication from 182.169

Since the peer is stuck in `DOWN` state and the auth failure is the blocker, the safest fix is to remove the authentication from 182.169 (since the peer never had it configured, suggesting it was added unilaterally on 182.169). However, removing security config could be a policy concern. Let me check if there's a pattern — let me see if other interfaces on 182.169 have auth:

GE0/2/3 (which has a working IS-IS peer) does not have authentication configured. This confirms that authentication was added only on GE0/2/1 without configuring the peer side. The fix is to remove the authentication from GE0/2/1 to match the peer.

Let me apply the fix:

Configuration change applied (pending commit). Let me commit it: Configuration committed. Now let me verify the fix by checking if the IS-IS adjacency comes up:

Now let me check the IS-IS peer status:

The IS-IS adjacency on GE0/2/1 is now UP. The peer 182.26 (System ID 0250.2550.4026) is showing state `Up` with HoldTime 23s.

Let me also verify from the peer side:

Peer device also shows the adjacency as `Up`. Let me do a final verification of the interface config:

No authentication line returned — confirmed removed.

Log for the AI model make decision



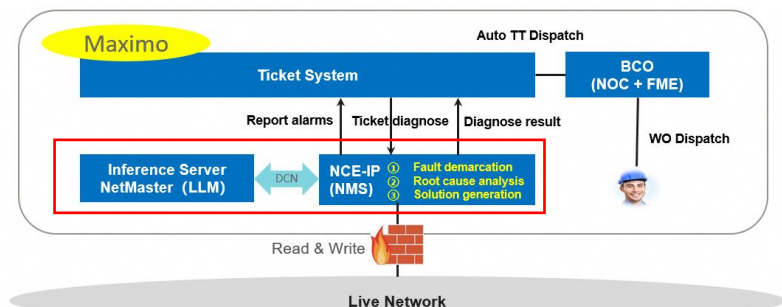
Solution Implementation-1

Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal
B	B	A

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Solution Implementation	10%	How does the system support automatic solution implementation and on-site instructions?	1) The system automatically executes the recovery or rectification solution(Automatic repair excludes the faults that on-site handling is necessary, such as power supply failure, board fault, fiber cut). 2) The system support intelligent on-site instruction and efficient information query based on simplified human-system interaction, independent from NOC assistance.	1)The system executes the recovery solution with human confirmation/instruction. 2)The on-site handling are assisted by tool,but still requires assistance from NOC.	1) The recovery solution need to be manually implemented. 2) On-site handling is guided by NOC.	

Example evidence for option A: Scenario 1: For the configuration type error, the system executes the recovery solution without human confirmation/instruction.

Scenario: IS-IS Adjacency Changed



Locate the root cause and fix the following fault:

Alarm Source: T-T030276(M1 -POC2

IP Address: [REDACTED] 182.169

Name: IS-IS Adjacency Changed

Other Information: T-T030276(M1) [REDACTED] -POC2: ISIS Circ Index=5 ISIS

Adj State=down If Name=GigabitEthernet0/2/1 Reason=isNbrHoldTimeExpired

```
2026-06-14 14:12:02.862 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:02.862 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:02.862 [trace-mgddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:03.255 [trace-mgddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:03.255 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:03.255 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:03.255 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:11.981 [trace-mgddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:12.021 [trace-mgddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:12.071 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:12.121 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:12.121 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:12.171 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:12.222 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:12.273 [trace-mqddui8a-8y00verki] [ForkJoinPool.com
```

```
2026-06-14 14:12:12.423 [trace-mgddui8a-8y00verki] [ForkJoinPool.com
2026-06-14 14:12:12.473 [trace-mgddui8a-8y00verki] [ForkJoinPool.com
```

□ $\frac{1}{2} \leq \frac{1}{2} \leq \frac{1}{2}$ (because $\frac{1}{2} \leq \frac{1}{2} \leq \frac{1}{2}$), $\frac{1}{2} \leq \frac{1}{2} \leq \frac{1}{2}$

***Note:** Use debugging carefully in production environments, *YJB* analyze this IS-95 adjacency failure and work through the diagnostic steps systematically.

Let me find the device and its neighbor first.

Good. The affected device is `10.20.20.1` (red). `show ip adj` (red) `10.20.20.1` shows that it has a neighbor `10.20.20.2` (green) in the `adj` table.

The alarm indicates IS-95 adjacency down on interface `10.20.20.1` with reason `linkdown(keepalive)` (hold timer expired).

Let me start the diagnostic steps.

Step 1: Check the interface status on the affected device.

Interface is UP but keepalive on IP Multicast packets are being received (10.20.20.2) so multicast connection appears fine. Let me check the IS-95 configuration.

Step 2: Check IS-95 interface and process configuration.

Now let me check the IS-95 peer status and last peer change info.

Interesting – the IS-95 peer is not in the peer list. Not showing in the peer list. Only two peers are up: one on GEO/2/1 and one on Fxo/G7/20/207. The adjacency on GEO/2/1 is indeed down.

Let me check the last peer change and error info.

Key Finding: The most recent peer change on GEO/2/1 shows:

```

Time: 1 2024-06-14 14:14:03.000
System: 14 0250.25000000
Interface: GEO/2/1 (7)
State: 1 Up -> Down
Details: 1 Auth failure
    
```

Al model CoT diagnose process

The root cause is authentication failure. The adjacency went down due to `auth failure`, not hold timer expiration. The alarm reason `linkdown(keepalive)` was from an earlier event, but the latest failure is authentication failure.

Let me also check the IS-95 error statistics to confirm.

Confirmed. The error statistics clearly show:

- Auth Authentication: 4 of 47 Hello packets were rejected due to authentication failure.
- Link Circuit Type: 2 – Minor, 2 packets with bad circuit type

The root cause is IS-95 authentication mismatch between the two endpoints on GEO/2/1. Now let me check the peer device's authentication configuration. The neighbor System ID is 10.20.20.2.

Let me check the other neighbor `10.20.20.2` (green) to see if it's connected on the same link:

This device (182.78.1) has peer `10.20.20.2` (green) (which is our affected device 182.169) but on RcvGEO/2/207, not on the GEO/2/1 link. The neighbor with System ID `0250.25000.4298` is a different device, let me find it.

Let me check the third neighbor of the affected device:

This is likely the peer – System ID `0250.25000.4298` maps to device `10.111.183.26`. Let me check its IS-95 config on the interface connected to 182.169:

The peer on GEO/2/18 is in `wait` state – stuck, not reaching UP. This confirms the authentication issue is preventing the adjacency from establishing. Let me check the peer device's interface config.

Log for the AI model execution

```
com.huawei.lingxi.agent.AgentLoop - chunk is: { "choices": [{"delta": {"content": "me commit it", "index": 0}, "created": 1781417517, "tool_calls": [{"function": {"arguments": "", "name": "ne ci"}]}], "index": 0}, {"delta": {"content": "\n\n", "index": 0}, "created": 1781417517, "id": "c1"}], "created": 1781417517, "id": "c1"}]
```

Root cause identified.
Here's the comparison:

Item	182.169 (GE0/2/1)	182.26 (GE0/2/8)
IP Address	11.2/30	11.1/30
IS-IS Enable	isis enable 200	isis enable 200
Circuit Type	p2p	p2p
Authentication	isis authentication-mode simple cipher %*%*%...	Not configured

The **root cause is clear**: Server **182.169** has IS-IS authentication configured on GE0/2/1, but the peer device **182.26** does **not** have any authentication configured on GE0/2/8. This authentication mismatch causes Hello packets to be rejected with **Bad Authentication** errors (47 counted, 48 discarded). Now let me fix this. I need to either:

1. Add matching authentication on the peer device (182.26), or
2. Remove authentication from 182.169

Since the peer is stuck in **Init** state and the auth failure is the blocker, the **safest fix is to remove the authentication from 182.169** (since the peer never had it configured, suggesting it was added unilaterally on 182.169). However, removing security config could be a policy concern. Let me check if there's a pattern — let me see if other interfaces on 182.169 have auth:

GE0/2/3 (which has a working IS-IS adjacency) does **not** have authentication configured. This confirms that authentication was added only on GE0/2/1 without configuring the peer side. **The fix is to remove the authentication from GE0/2/1 to match the peer.**

Let me apply the fix:

Configuration change applied (pending commit). Let me commit it: Configuration committed. Now let me verify the fix by checking if the IS-IS adjacency comes up:

Now let me check the IS-IS peer status:

The **IS-IS adjacency on GE0/2/1 is now UP**. The peer **182.26** (System ID 0250.0000.0026) is showing state **Up** (Hello received).

Let me also verify from the peer side:

Peer device also shows the adjacency is up.

config:

No authentication is configured on the peer device.

AI model Implement solution and verify the result without human confirmation

Solution

The solution is to change the authentication mode from IS-IS to simple cipher.

```
IS-IS authentication mismatch between the two endpoints of the link:  
• 182.169 (GE0/2/0) had 'isis authentication-mode simple cipher' configured  
• 182.26 (GE0/2/0) had no IS-IS authentication configured
```

The configuration error was found by running the command `show ip isis neighbors` at 2026-06-14 17:04:05:

```
182.169#show ip isis neighbors  
Neighbor Capability Information  
+-----+-----+-----+-----+-----+-----+  
error packets
```

Fix Applied

Removed the unilateral IS-IS authentication configuration from interface GE0/2/1 on device 182.169:

```
undo isis authentication-mode  
commit
```

Verification

```
182.169> display isis peer now shows 182.26* GE0/2/1 up 2w 1d  
182.26> display isis peer now shows 18:169@ GE0/2/8 up 2w 1d
```

This discrepancy is truly resolved on both sides.

[illegible]

- Ticket start and end time

Remote repair confirmation



Solution Implementation-2

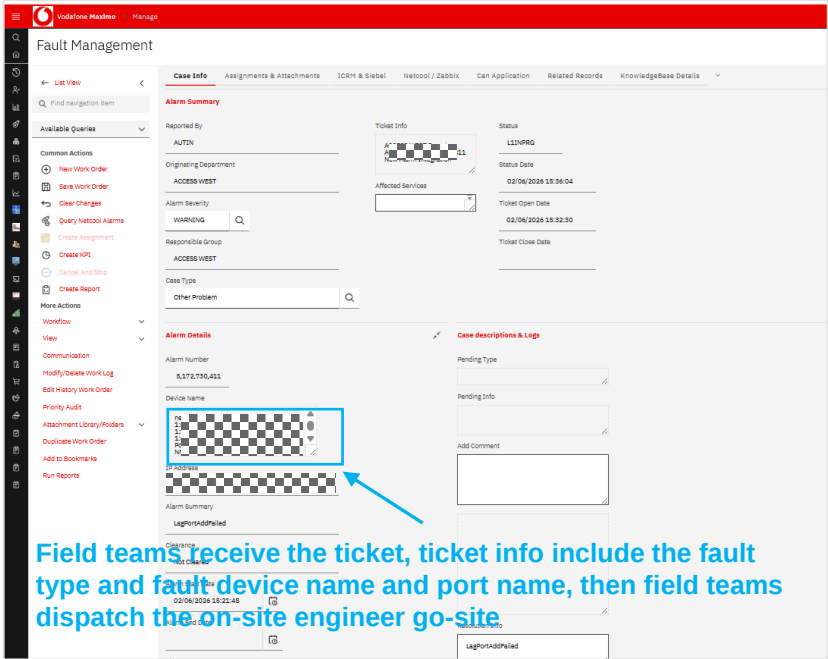
Optical Module Failure or Optical Power Abnormal	Port Failure	Protocol State Abnormal
B	B	A

Service capability	Weight	Question	Option A	Option B	Option C	Option D
Solution Implementation	10%	How does the system support automatic solution implementation and on-site instructions?	1) The system automatically executes the recovery or rectification solution(Automatic repair excludes the faults that on-site handling is necessary, such as power supply failure, board fault, fiber cut). 2) The system support intelligent on-site instruction and efficient information query based on simplified human-system interaction, independent from NOC assistance.	1)The system executes the recovery solution with human confirmation/instruction. 2)The on-site handling are assisted by tool,but still requires assistance from NOC.	1) The recovery solution need to be manually implemented. 2) On-site handling is guided by NOC.	

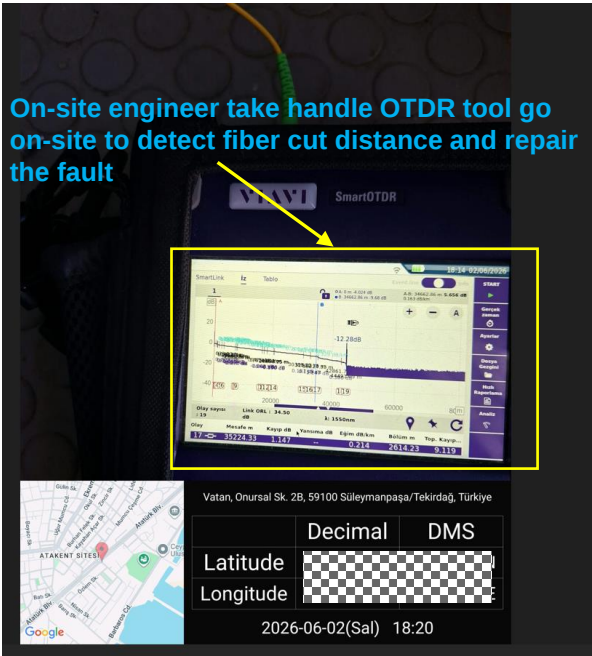
Example evidence for option B:

Scenario 2: For faults requiring on-site manual intervention, frontline engineer handling are assisted by tools like OTDR measuring instrument, but still requires assistance from NOC.

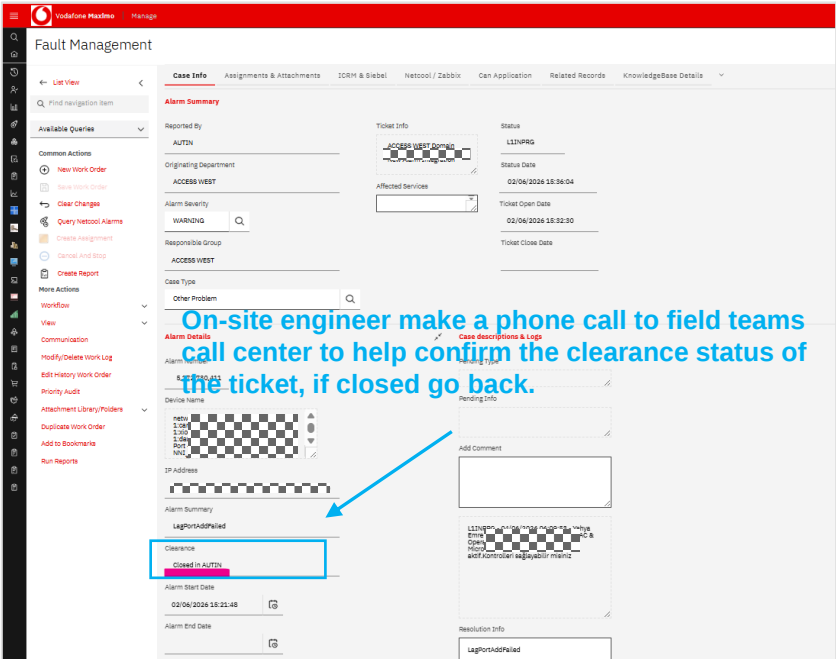
Scenario 2: Hardware fault on-site repair



Field teams receive the ticket, ticket info include the fault type and fault device name and port name, then field teams dispatch the on-site engineer go-site



On-site engineer take handle OTDR tool go on-site to detect fiber cut distance and repair the fault



On-site engineer make a phone call to field teams call center to help confirm the clearance status of the ticket, if closed go back.



Thank you.

