



TM Forum

ANLAV Report

Rakuten Mobile

GB1523E – IP Network Fault Management

Version: 2.0.1

Score: 3.95

Rakuten Mobile TM Forum ANL Evaluation

(IP Fault Management)

Powered By Rakuten Symphony

CONFIDENTIALITY NOTICE

This document contains confidential and proprietary information belonging to **Rakuten Mobile / Rakuten Symphony**, provided solely for the purpose of **TMF ANL Evaluation**. By accessing or reviewing this material, you agree to treat it as strictly confidential, use it only for the stated purpose, and not disclose, copy, or distribute its contents to any third party without our prior written consent. Upon completion, all copies must be returned or securely destroyed.

Autonomous network level evaluation - IP Fault Management(1/3)

Value Scenarios	Cognitive Activities (IAADE)	Service capability	Weight	Question	Option A Rakuten Mobile	Option B	Option C	Option D
IP Network - Fault Management	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.	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) .
	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	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", milisecond-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.

Autonomous network level evaluation - IP Fault Management(2/3)

Value Scenarios	Cognitive Activities (IAADE)	Service capability	Weight	Question	Option A Rakuten Mobile	Option B	Option C	Option D
IP Network - Fault Management	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.	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.
		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.
		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.
		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

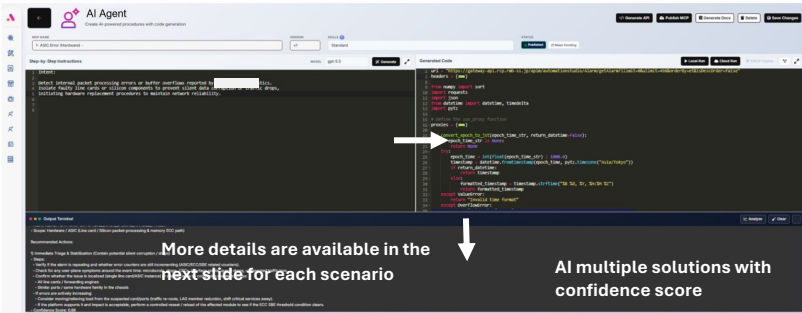
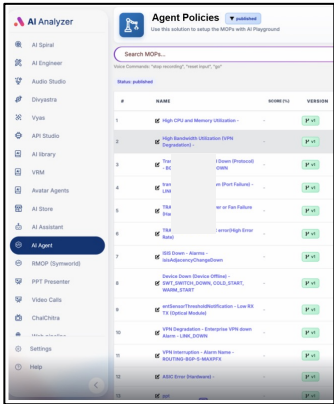
Autonomous network level evaluation - IP Fault Management(3/3)

Value Scenarios	Cognitive Activities (IAADE)	Service capability	Weight	Question	Option A Rakuten Mobile	Option B	Option C	Option D
IP Network - Fault Management	Decision	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 programable rules (configurable or ML) , but may need Human confirmation	The recovery of fault rectification solution is manually evaluated and determined	
	Execution	Solution Implementation	10%	How does the system support automatic solution implementation and on-site intructions?	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.	

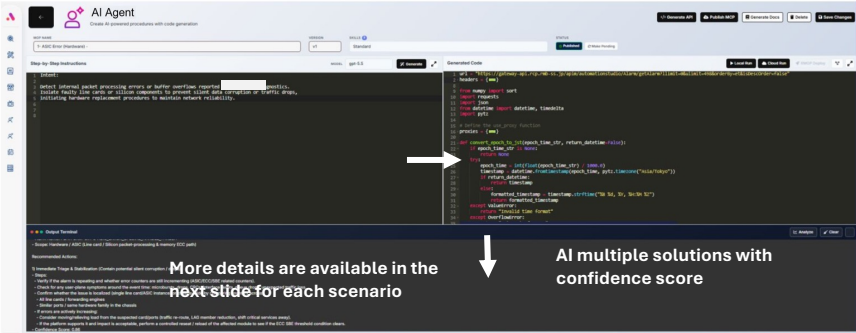
Overall sub-scenario

Sub Scenario's	Ticket Count Distribution Summary	
	Ticket Title	Network Fault %
Hardware Failure	Hardware	2%
Device Offline	Device Down	18%
Optical Module Failure or Optical Power Abnormal	LowRx/HighRx	6%
Port Failure	Link Down	17%
High Error Rate	CRC ERROR	1%
Protocol State Abnormal	ISIS-BGP	46%
VPN Degradation	Bandwidth Traffic utilization / CPU & Memory Utilization	9%
VPN Interruption	ROUTING-BGP-5-MAXPFX	1%
Summary	Grand Total	100%

Intent Translation & Fulfillment

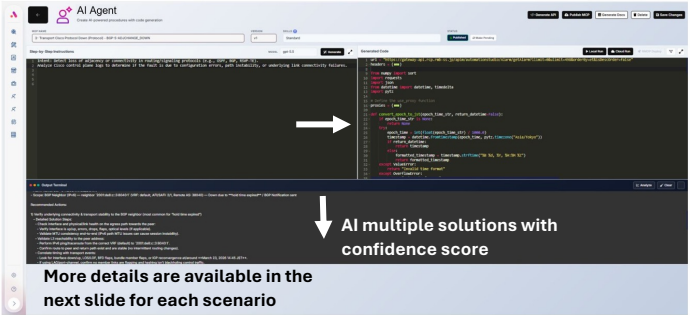


Hardware related intent flow with multiple solution generation

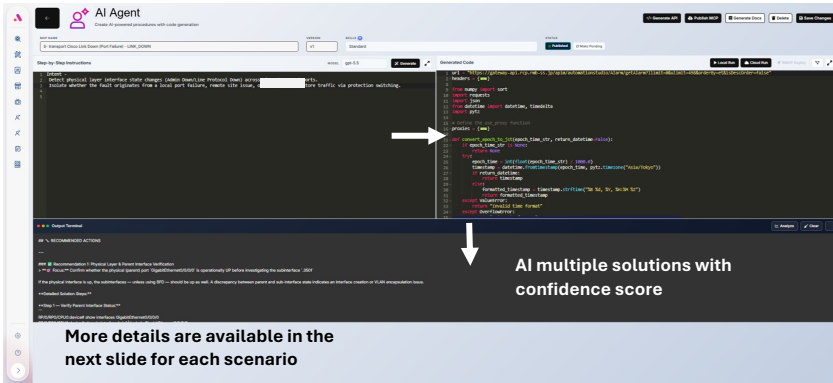


Device offline intent flow with multiple solution generation

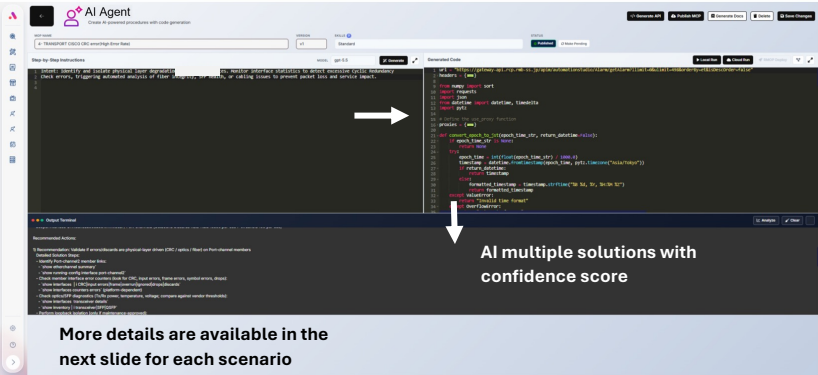
Based on the identified root cause “Scoring Model v1.0 — SolutionRanker” get triggered for policy chain generation



Protocol Down intent flow with multiple solution generation



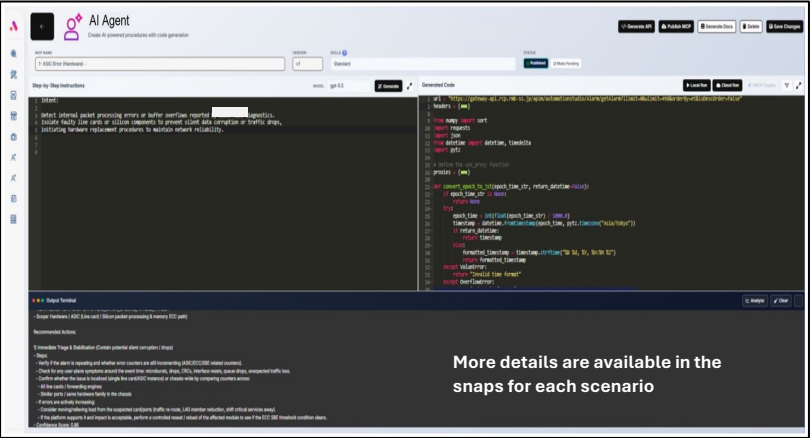
Link Down(Optical) intent flow with multiple solution generation



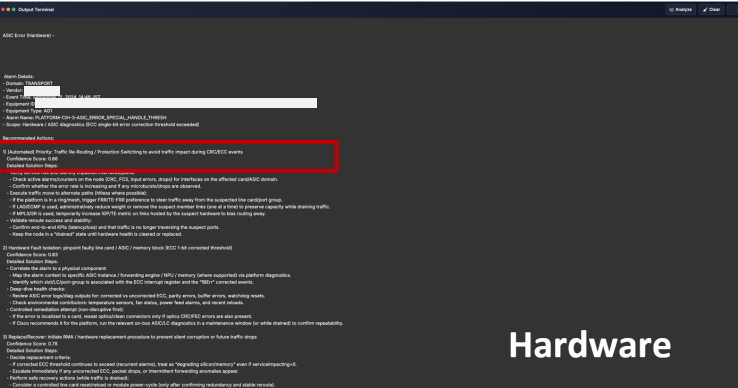
High CRC Error rate intent flow with multiple solution generation

Intent Translation & Fulfillment

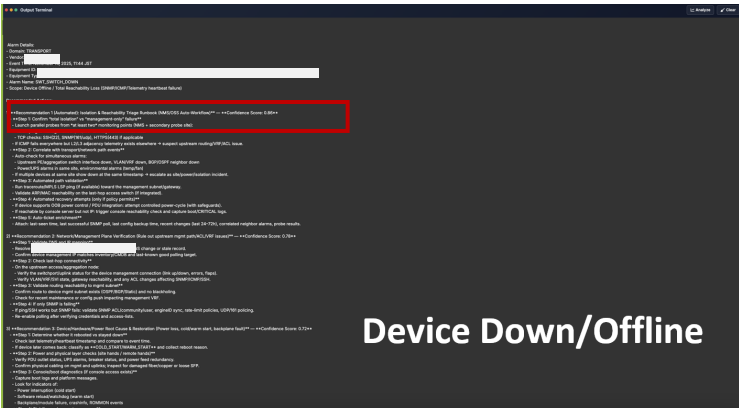
- Detail multiple solution generations for each scenario by the AI system for the evaluation process and implementation are provided below.



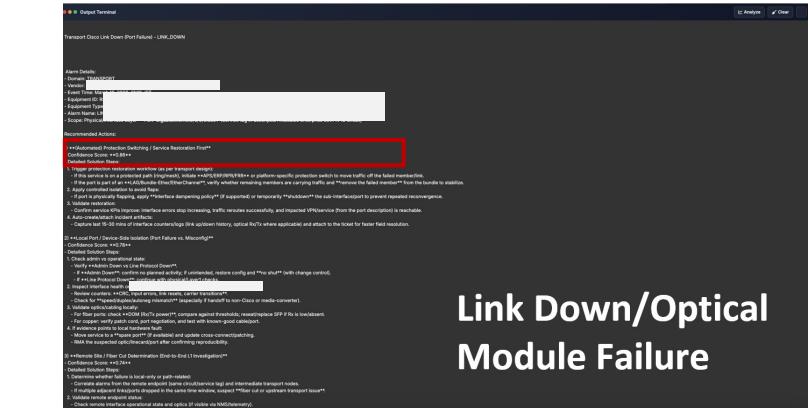
More details are available in the snaps for each scenario



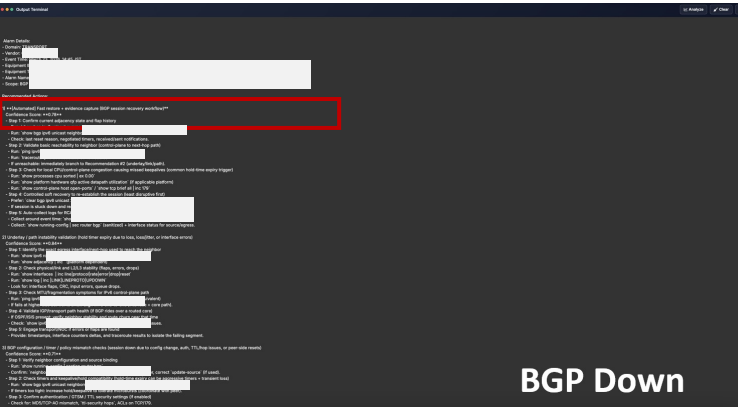
Hardware



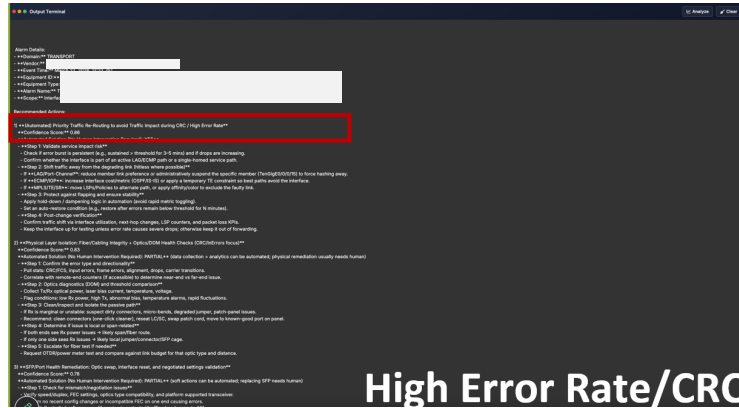
Device Down/Offline



Link Down/Optical Module Failure



BGP Down



High Error Rate/CRC

Awareness - Data Collection & Alarm filtering

Question	Rakuten Mobile Assessment
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	Option A

Capability -

The RMI Fault Management system collects all types of network alarms from multiple sources through interfaces such as SNMP (v3), Webhook, and Kafka. For example, EMS integration is achieved via SNMP v3, while performance-KPI-based threshold breach alerts are received through Kafka and enriched within the FM system. All incoming alarms are filtered using intelligent logic, including:

Intermittent alarm grouping to merge repeated occurrences within a short time window into a single event.

Correlation-based grouping (Topology based, intermittent, parent-child, associated alarms) to identify the unique device, node, or fault responsible for issues across multiple network elements.

The system can raise, clear, discard, filter, and correlate alarms while continuously monitoring health and connectivity with network probes and devices to ensure reliable alarm collection.

Evidence

The screenshot shows the 'Integration Name' dropdown menu in the FortiMonitor configuration page. The menu is open, displaying a list of integration types. The 'Integration User Name' option is highlighted with a red box.

Integration Name	Details	Vendor	EPS	HeartBeat Type	Clear Light Type	Technology	Port Name	Port ID
● Disabled	TRANS-CDMA	TransPort		BTLS-HEARTBEAT	Security Based Check	LTE		TMN
● Disabled	TRANS-NOK-N1-N2	TRANS-PORT		N/A	Security Based Check	LTE		TMN
● Disabled	TRANS-CD-CH2	TRANS-PORT		ALARM-HEARTBEAT	Security Based Check	LTE		TMN
● Disabled	TRANS-NOK-N1-N17	TRANS-PORT		ALARM-HEARTBEAT	Security Based Check	LTE		TMN
● Disabled	TRANS-CD-CAKAS	TRANS-PORT		BTLS-HEARTBEAT	Security Based Check	LTE		TMN
● Disabled	TRANS-CD-CD-19	TRANS-PORT		ALARM-HEARTBEAT	Security Based Check	LTE		TMN
● Disabled	TRANS-NOK-N1-N1P	TRANS-PORT		N/A	Using Based-Code or...	LTE		TMN
● Disabled	TRANS-CD-CH1	TRANS-PORT		N/A	Security Based Check	LTE		TMN
● Disabled	TRANS-CD-CD-CD-CD	TRANS-PORT		N/A	Security Based Check	LTE		TMN
● Disabled	TRANS-CD-CD-CD	TRANS-PORT		N/A	Security Based Check	LTE		TMN
● Disabled	TRANS-NOK-N1-N17-1	TRANS-PORT		ALARM-HEARTBEAT	Security Based Check	LTE		TMN
● Disabled	TRANS-CD-CD-CD-CD-1	TRANS-PORT		N/A	Using Based-Code or...	LTE		TMN

Overview of how the FM system integrates with data sources using SNMP, Kafka, and Webhook interfaces for alarm collection.

[illegible]

Vendor- and technology-specific configuration used to parse raw SNMP trap data into structured alarm information.

[illegible]

The FM System - complete visualization of end-to-end alarm details raised from specific device/node.

Awareness - Data Collection & Alarm filtering

[illegible]

Alarm collection details filtered by network domain and vendor.

[illegible]

Alarm collection view organized by severity level and alarm classification.

[illegible]

Severity-based alarm filtering with additional contextual fields for refined alarm management.

[illegible]

Classification-based alarm filtering with additional fields to support detailed alarm triage.

[illegible]

Probable cause information captured for each alarm along with its occurrence details on the affected device.

[illegible]

Alarm details grouped and displayed based on their correlation relationships.

[illegible]

View showing repeated alarm occurrences on the same device and port to identify recurring fault patterns.

[illegible]

Correlated alarm view showing the linked incident and the auto-generated trouble ticket for each alarm.

[illegible]

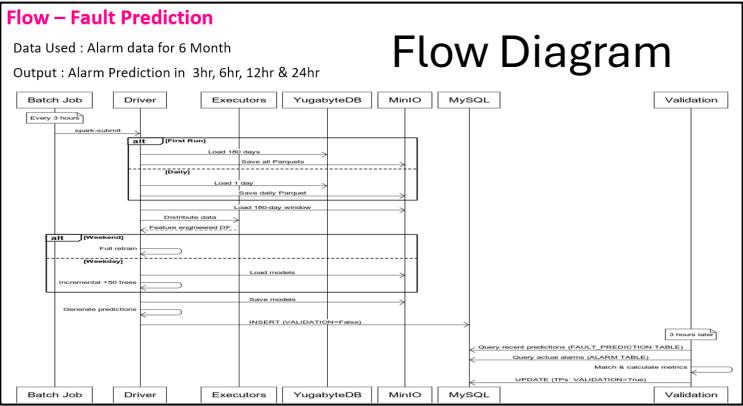
Geographical location details associated with each alarm, indicating where the fault occurred.

Analysis - Fault Identification ,Risk identification, Impact analysis

Fault Identification ,Risk identification, impact analysis

Evidence Submission :

- Model version -
- Input Features – evidence available in slide number – 16
- Live cases – evidence available in slide number 14
- 12 input features:** alarm_class, device_type, device_role, interface_util, error_rate_delta, bfd_status, last_config_change, time_of_day, traffic_loss, peer_count, recent_change_flag, adj_alarm_count
- Output:** fault_type (e.g. BGP_PEER_DOWN), sub_type, severity (CRITICAL/HIGH/MED), false_positive_prob



Prediction Model -

What is XGboost	How it works	Why we are using
- XGBoost (Extreme Gradient Boosting) is an ensemble ML algorithm based on decision trees - Builds multiple trees sequentially to improve prediction accuracy - Each new tree learns from errors of previous trees - Supports both classification and regression problems - Includes built-in regularization to avoid overfitting	- Trained on historical alarm occurrences and device-level features - Learns patterns across alarm codes, equipment IDs, and time windows - Predicts probability of fault occurrence in future horizons (3h / 6h / 12h/24h) - Used as classifier (Fault / No Fault) and regressor (risk or score) - Model is periodically retrained using latest alarm history	- Works well on structured alarm data - Captures non-linear and complex alarm correlations - Handles missing or sparse alarm data efficiently - Scales well for large volumes of network alarms - Gives Maximum accuracy in current data

Equipment ID	Alarm Code	Predicted Time	Actual Time	Variance	Time Tolerance(Hours)	Incident Severity	Classification	Validation	Domain
	TV_PERFORMANCE_CPU	2026-06-18 03:28:10 JST	2026-06-18 03:23:57 JST	Before 5m 13s	0.25	Warning	Normal	Matched	TRANSF
	ROUTING-BGP-5-MAXPFX	2026-06-18 18:31:28 JST	2026-06-18 19:00:38 JST	After 29m 10s	2	Critical	Deterioration	Matched	TRANSF
	LINK_DOWN	2026-06-18 15:50:49 JST	2026-06-18 15:28:21 JST	Before 22m 28s	3	Critical	Deterioration	Matched	TRANSF
	TV_CE_PERFORMANCE_INTERFACE	2026-06-18 14:47:53 JST	2026-06-18 15:10:51 JST	After 22m 58s	2	Major	Normal	Matched	TRANSF
	BGP-5-ADICHANGE_DOWN	2026-06-18 14:56:00 JST	2026-06-18 14:35:54 JST	Before 20m 6s	1	Critical	Outage	Matched	TRANSF
	entSensorThresholdNotification	2026-06-18 16:16:31 JST	2026-06-18 15:49:23 JST	Before 27m 8s	1	Major	Normal	Matched	TRANSF
	SWT_SWITCH_DOWN_COLD_START	2026-06-18 16:38:41 JST	2026-06-18 16:11:44 JST	Before 26m 57s	2	Critical	Outage	Matched	TRANSF
	issAdjacencyChangeDown	2026-06-18 17:39:03 JST	2026-06-18 17:12:44 JST	Before 26m 19s	1	Critical	Outage	Matched	TRANSF
	LINK_DOWN	2026-06-18 17:48:28 JST	2026-06-18 17:34:36 JST	Before 23m 52s	2	Critical	Deterioration	Matched	TRANSF
	ROUTING-BGP-5-MAXPFX	2026-06-18 18:22:34 JST	2026-06-18 18:02:02 JST	Before 20m 32s	2	Critical	Deterioration	Matched	TRANSF
	TV_CE_PERFORMANCE_INTERFACE	2026-06-18 14:20:59 JST	2026-06-18 13:59:22 JST	Before 21m 37s	1.59	Major	Normal	Matched	TRANSF
	BGP-5-ADICHANGE_DOWN	2026-06-18 14:48:30 JST	2026-06-18 14:21:07 JST	Before 27m 23s	1.16	Critical	Outage	Matched	TRANSF
	LINK_DOWN	2026-06-18 15:22:32 JST	2026-06-18 15:44:14 JST	After 21m 42s	2.71	Critical	Deterioration	Matched	TRANSF
	entSensorThresholdNotification	2026-06-18 16:02:09 JST	2026-06-18 16:27:59 JST	After 25m 50s	1.44	Major	Normal	Matched	TRANSF
	SWT_SWITCH_DOWN_COLD_START	2026-06-18 16:58:52 JST	2026-06-18 17:20:10 JST	After 21m 18s	1.76	Critical	Outage	Matched	TRANSF
	issAdjacencyChangeDown	2026-06-18 17:34:37 JST	2026-06-18 18:03:45 JST	After 29m 8s	1.39	Critical	Outage	Matched	TRANSF
	LINK_DOWN	2026-06-18 17:25:53 JST	2026-06-18 17:49:07 JST	After 23m 14s	2.41	Critical	Deterioration	Matched	TRANSF
	ROUTING-BGP-5-MAXPFX	2026-06-18 18:46:51 JST	2026-06-18 18:25:13 JST	Before 21m 38s	2.12	Critical	Deterioration	Matched	TRANSF

High Error Rate

Optical Module/Power

VPN Degradation

Protocol State Abnormal

Analysis - Risk identification, Fault Identification & Impact analysis

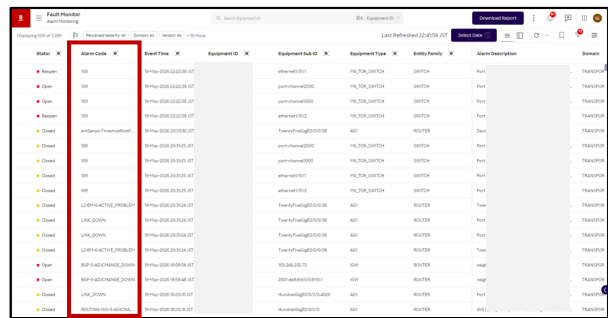
Question	Rakuten Mobile Assessment
How does the System support fault identification, risk identification and subsequent impact analysis? Note: These four sub-scenarios are required to consider potential risk: Optical Module Failure or Optical Power Abnormal, High Error Rate, Protocol State Abnormal, VPN Degradation.	Option A

Capability –

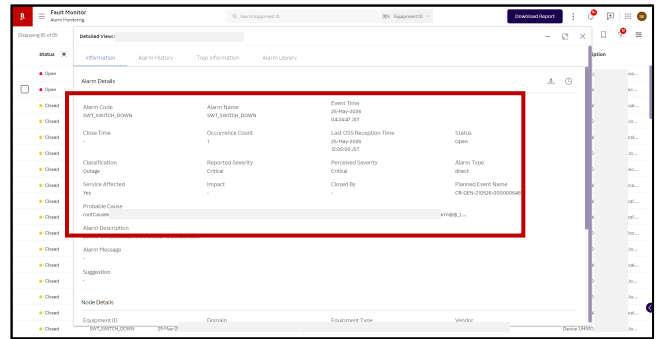
The RMI Fault Management system provides end-to-end monitoring across the network to identify faults and analyze their impact within the underlying TRANSPORT(as well as RAN) topology. Impact Analysis groups related alarms and nodes to show which element is causing the issue and how it affects other connected nodes across IP and cross-domain areas.

It also highlights the impacted region or location resulting from outage conditions.

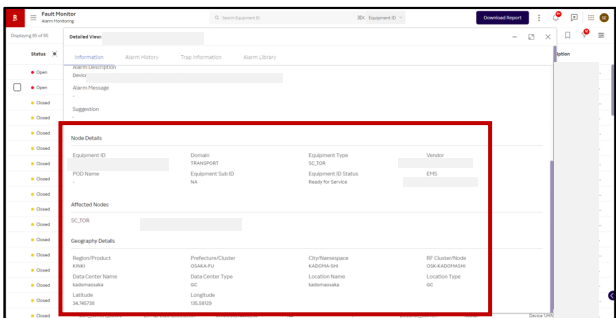
Evidence - Fault Identification



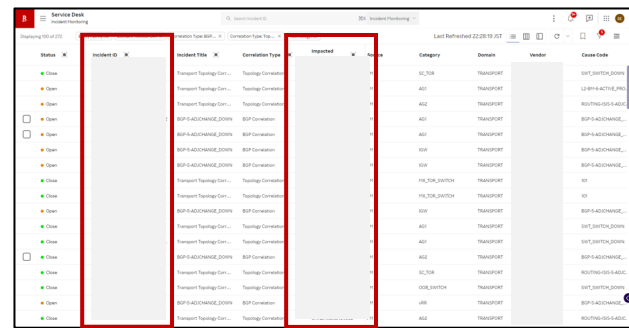
Overview of various alarm types raised across different network nodes, showing fault distribution.



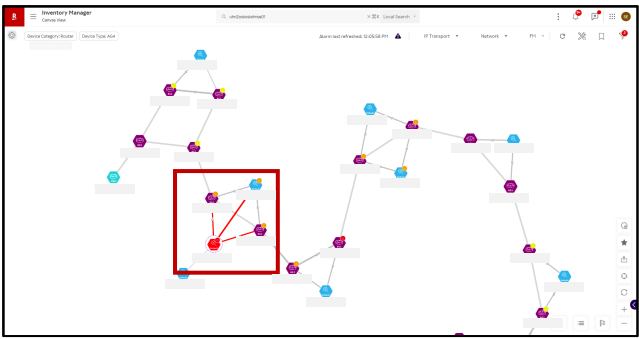
Detailed alarm record for a specific device, including probable cause, description, and event timeline.



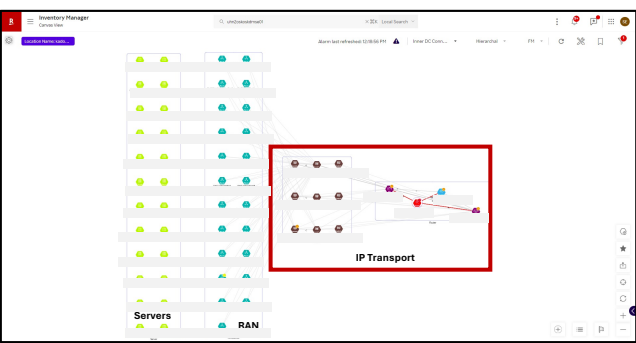
Geographical view showing the physical location of the affected device and the alarm's impact area.



Multiple related alarms consolidated into a single incident to enable unified root-cause and impact analysis.



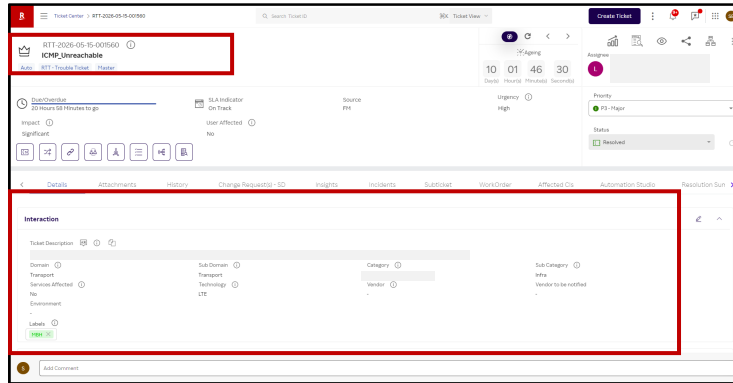
Topology-based impact analysis showing which devices and links are affected due to connectivity to the faulty node.



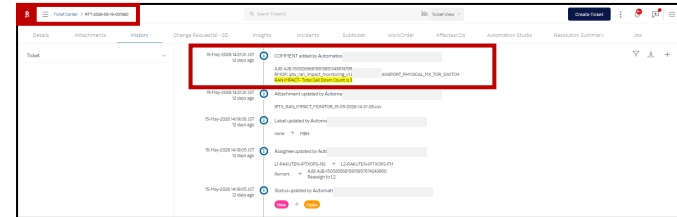
Cross-domain impact view illustrating how a fault on one device propagates across connected network domains via topology.

Analysis - Risk identification, Fault Identification & Impact analysis

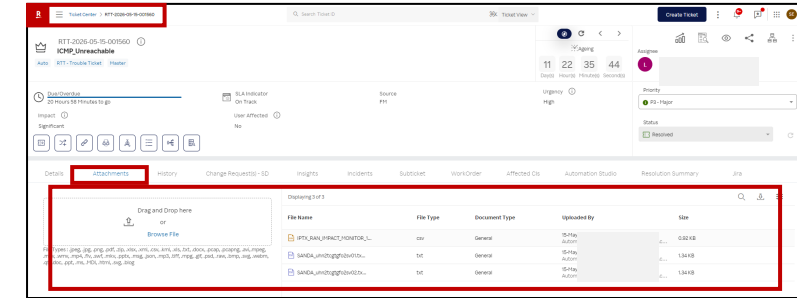
Detailed Impact Analysis across IP-RAN Domain



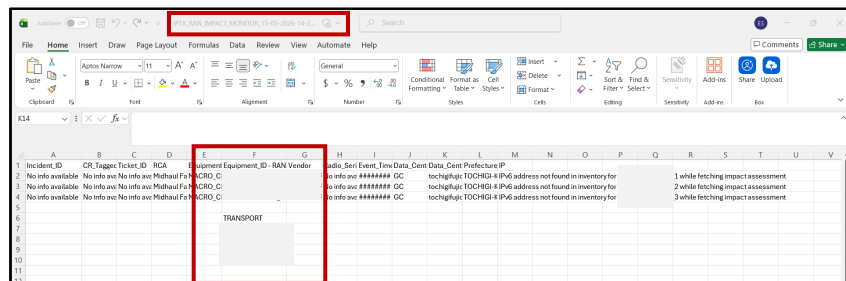
Auto-generated trouble ticket created by the system for the identified fault, capturing all relevant incident details.



Impact analysis result showing that 3 RAN cells are down because of the detected transport fault.



Detailed RAN impact data, included as an attachment within the auto-generated trouble ticket for further analysis.



List of specific RAN cells affected by the transport fault,
with site and cell-level details.



Impact and risk assessment are automatically analyzed by the system across multiple domains (IP-RAN) via topology connectivity information.

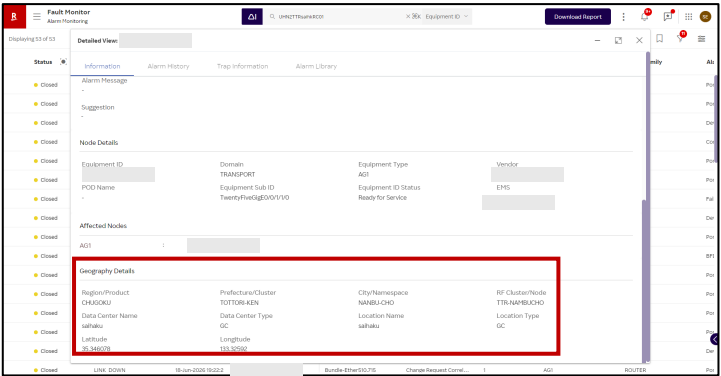
RAN-specific site availability dips during the TRANSPORT impact period.

Analysis - Fault Demarcation , Locating and Root Cause Analysis

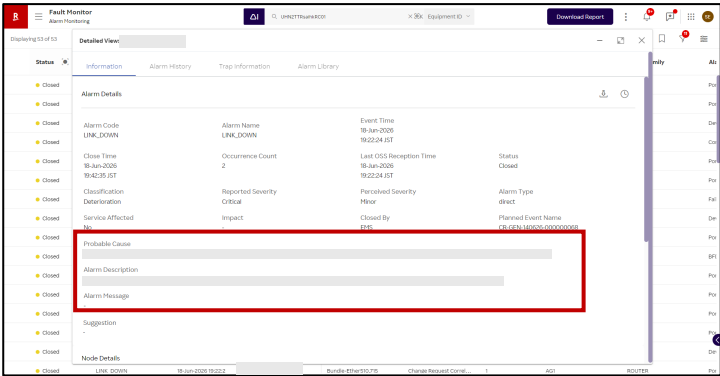
Fault Demarcation , Locating and Root Cause Analysis

Evidence Submission :

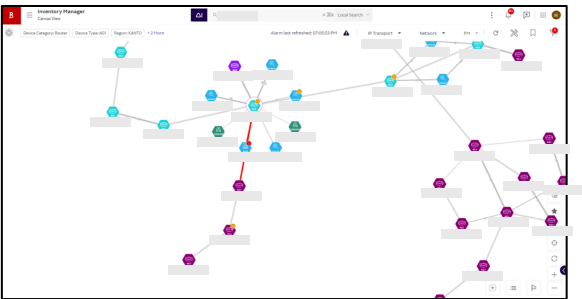
- Triggered via a natural language interface, our system employs a specialized multi-agent architecture for advanced fault management. GNN v1.1 (TopologyFaultLocator) performs granular analysis to pinpoint the smallest affected network component, while Rakuten NLP 3.0 (ImpactAnalyzer) evaluates scope to accurately demarcate the issue's impact.
- These agents integrate directly with LLMs, APIs, and service assurance databases to ingest real-time data.
- By processing information within their specific operational context and executing seamless handovers between stages, the agents orchestrate a highly efficient, automated workflow.
- This synergy ensures precise fault localization and comprehensive impact analysis, significantly accelerating incident diagnosis and resolution.



Demarcating the specific problem



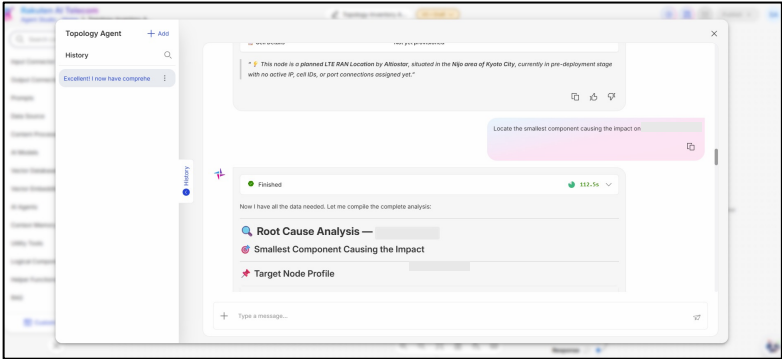
Locating the specific component



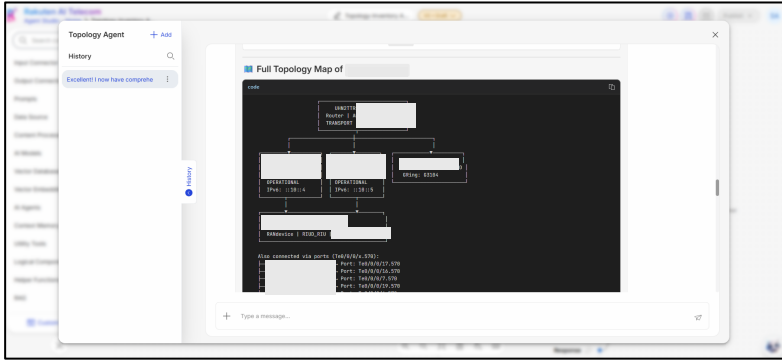
Topology path trace to locate the issue/problem

Analysis - Fault Demarcation

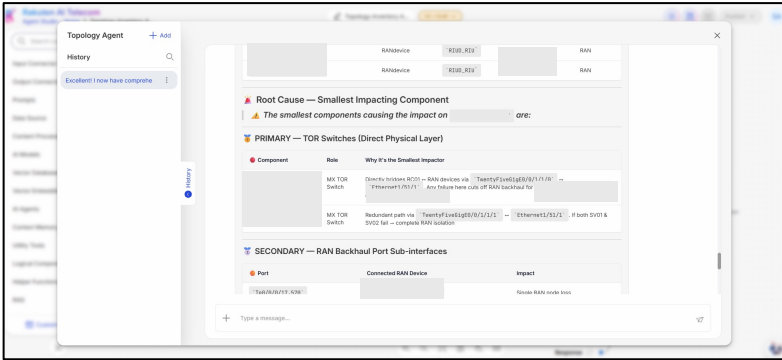
Fault Demarcation



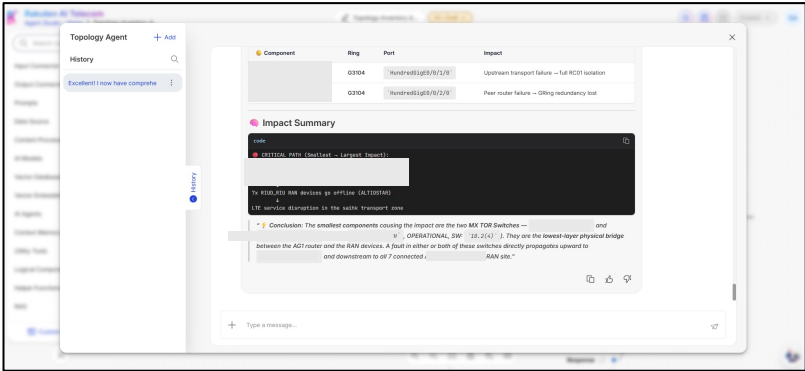
Agent is triggered to identify the smallest component causing the impact.



Based on the connected tools with the agent , it dynamically creates the connected topology chart



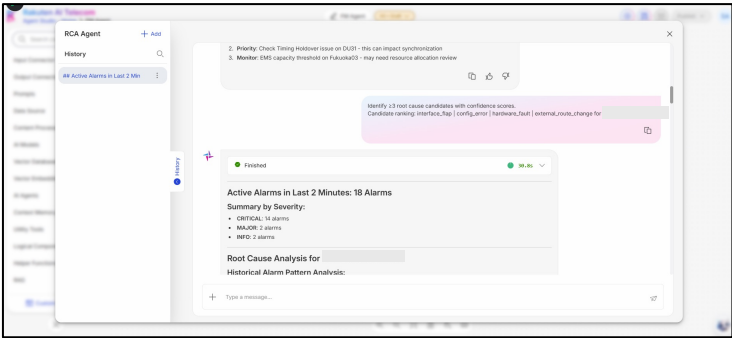
Based on the analysis, the agent identified the all the correlated nodes to identify the smallest component(interface – e.g. ethernet1/51/1)



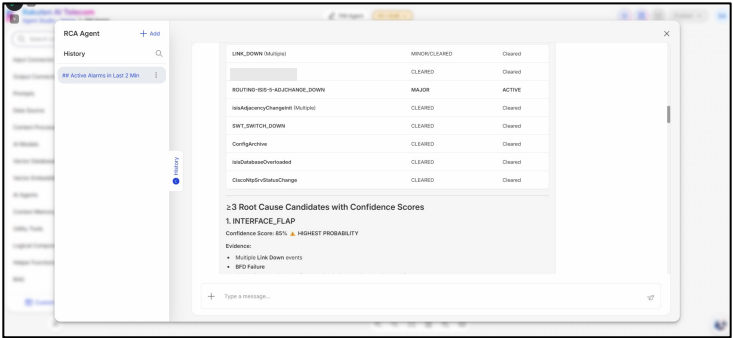
Revalidates its critical path to validate the generated information

Analysis - Fault Locating and Root Cause Analysis

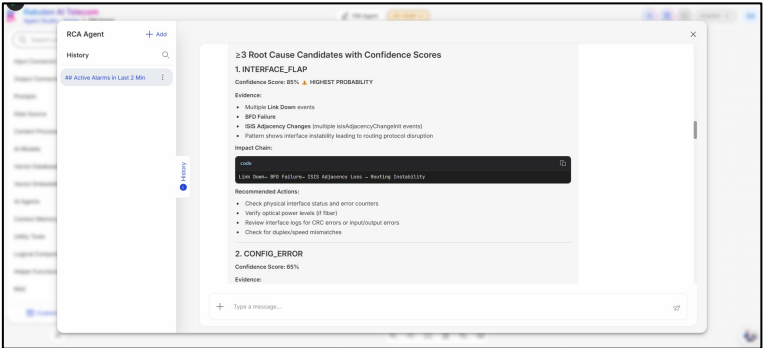
Fault Locating and Root Cause Analysis



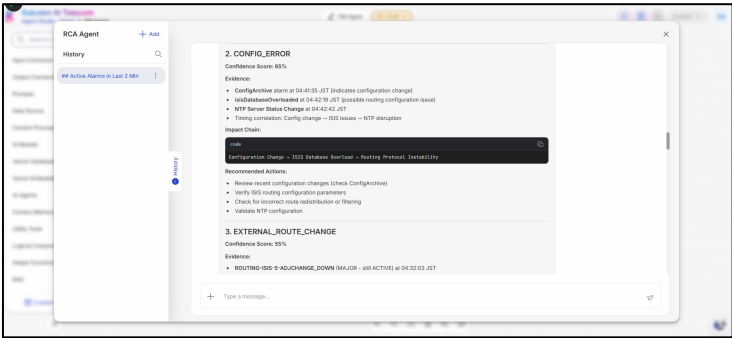
Based on the trigger received from topology agent to the RCA agent to identify the root cause and confidence scoring



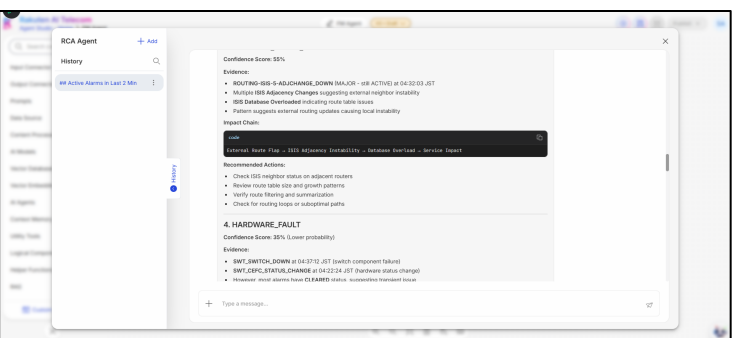
Agent scanned the fault management data on the provided node - to identify the chronology of the cause and potential root cause



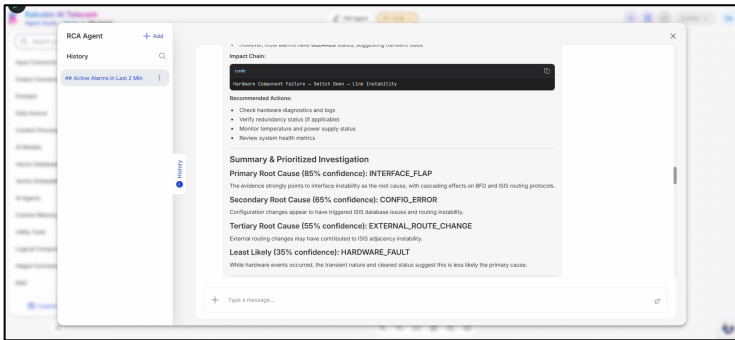
Agent automatically categories the root cause of the impact with confidence score



Agent automatically categories the root cause of the impact with confidence score multiple root cause



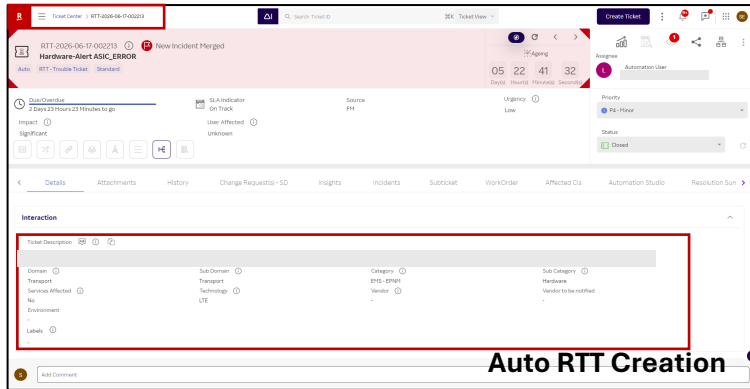
Overall root cause summary with confidence score



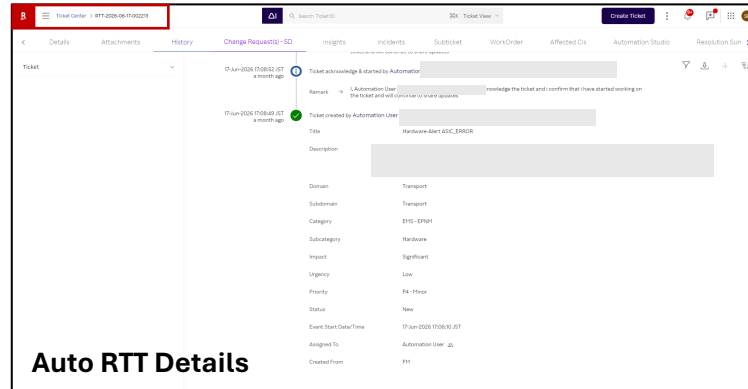
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – Hardware Failure

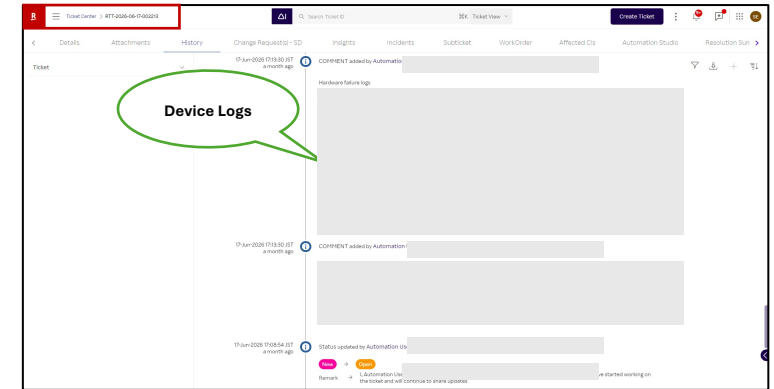
Detection and Ticketing



Trouble ticket created by FM Automation for further analysis, troubleshooting and resolution.

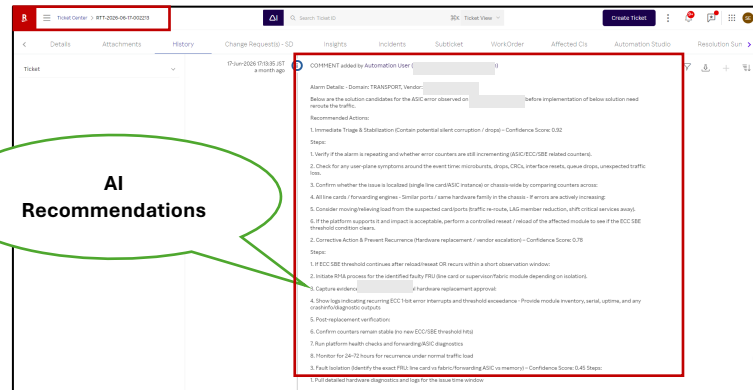


Trouble ticket details with impacted node details and timelines

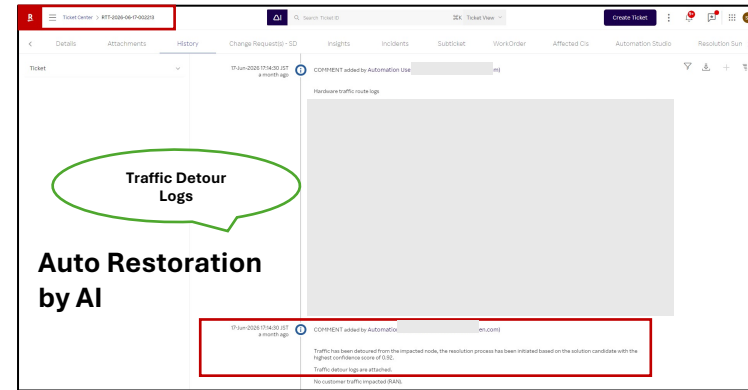


Once the RTT created, the AI agent logs into the device and collects the logs and attached in the ticket comments

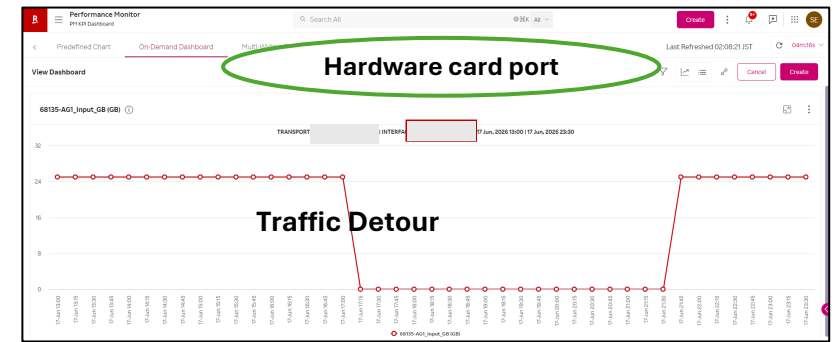
AI Recommendations & Auto Restoration



The AI agent analyses the alarm details and provide the best possible solution candidates for the resolution.



AI agent performs the auto restoration of the services by detouring the traffic from the impacted node.

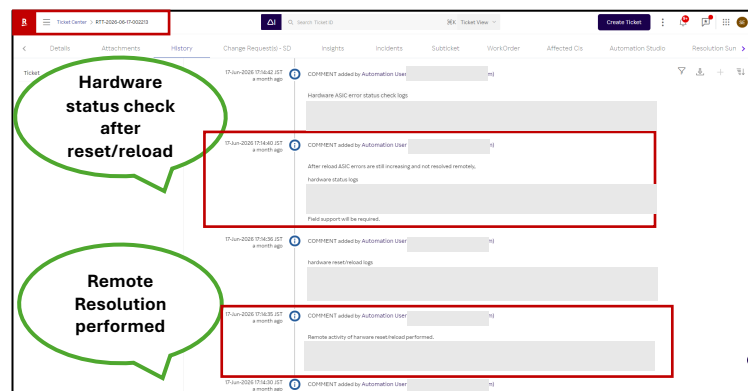


PM performance KPI trend of traffic detouring values.

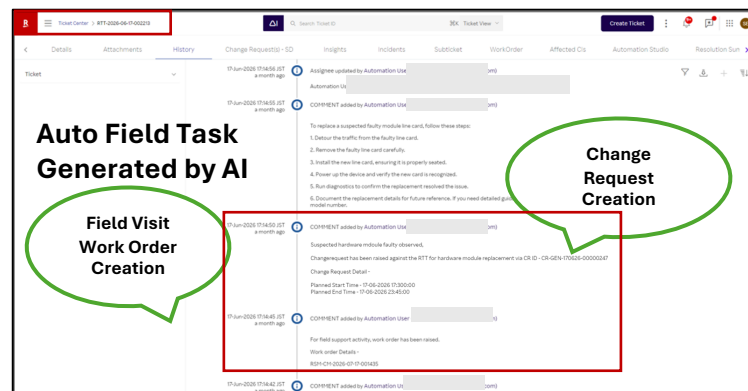
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – Hardware Failure

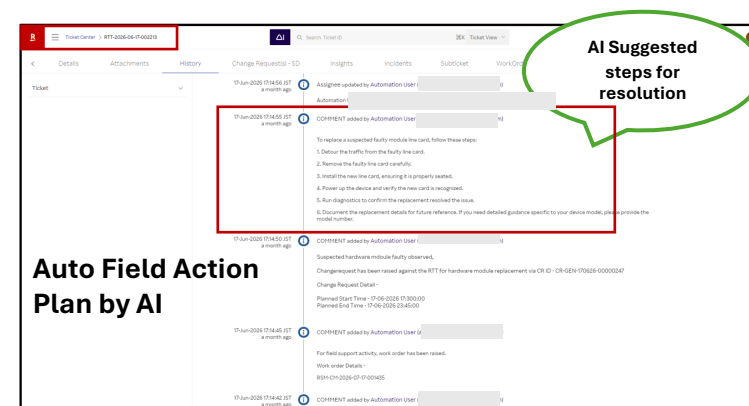
Solution Generation



Once the traffic is detoured, the AI agent performs the auto resolution by trying the hard reset/reload activity to bring the device as per suggested candidate solutions, and if issue is not resolved, plans for field support.

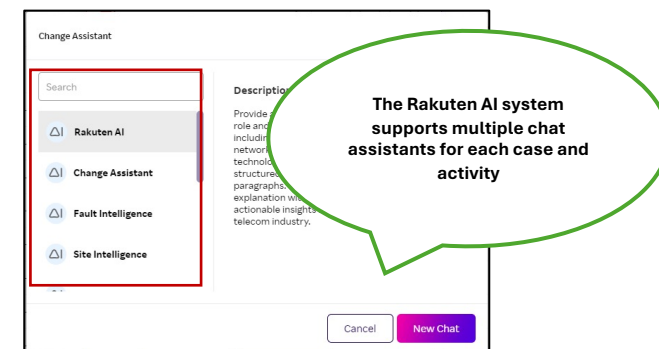
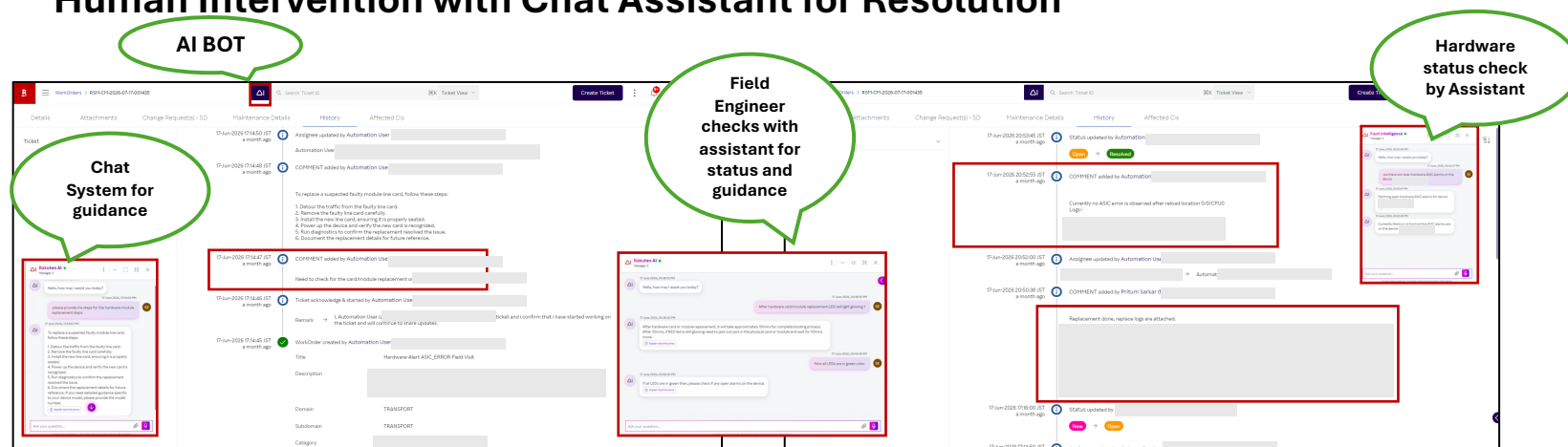


For the field operations, the agent auto creates the work order and change requests and RTT is assigned to field engineer.



For the field operations, the agent auto provides the resolution fix/troubleshooting steps.

Human Intervention with Chat Assistant for Resolution



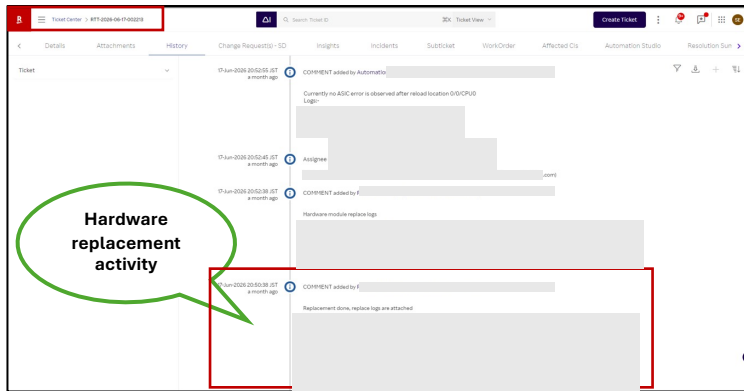
The Rakuten AI system supports multiple chat assistants for each case and activity

Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

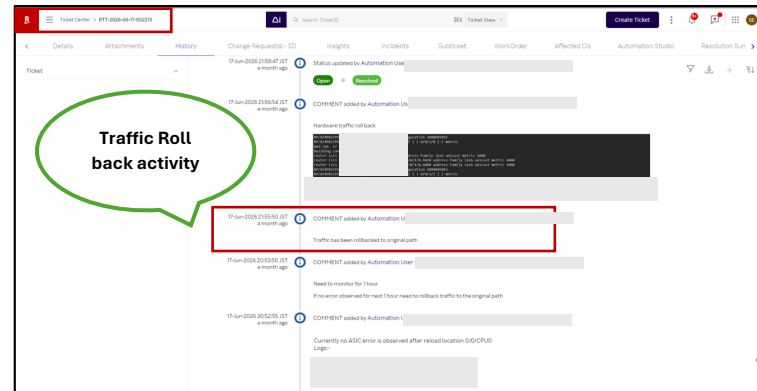
Scenario – Hardware Failure

Solution Implementation

Auto logs updates by AI from field Activity



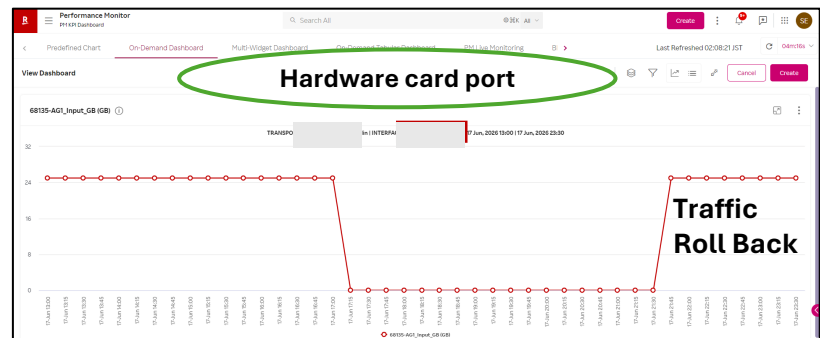
Once the work order side, hardware issue replacement activity is completed, the RTT will be assigned to Automation agent for the logs check of issue resolution and alarm status by agent.



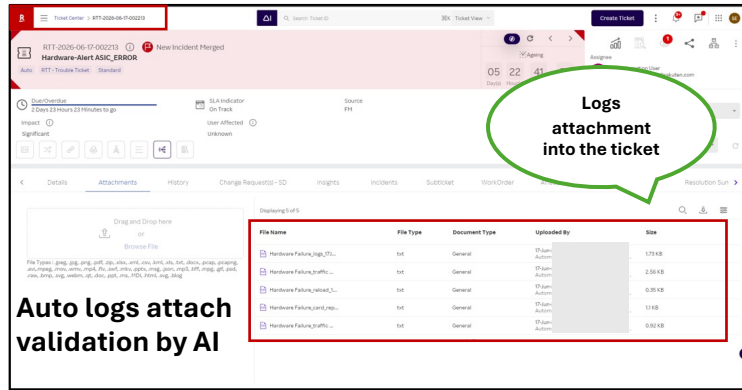
Auto traffic roll back by AI

Once the agent verifies the alarm status , it performs the roll back activity to shift the traffic to the original path.

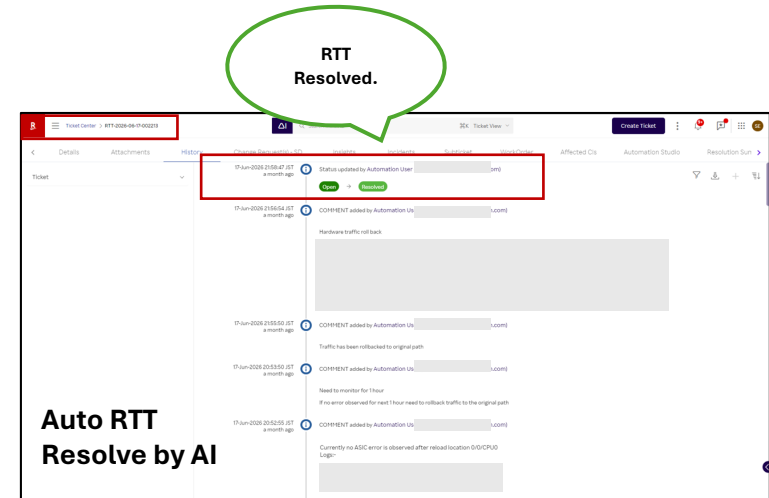
Roll Back and Post Validation



Traffic shift to original path is verified via performance KPI via PM tool



Auto logs attach validation by AI

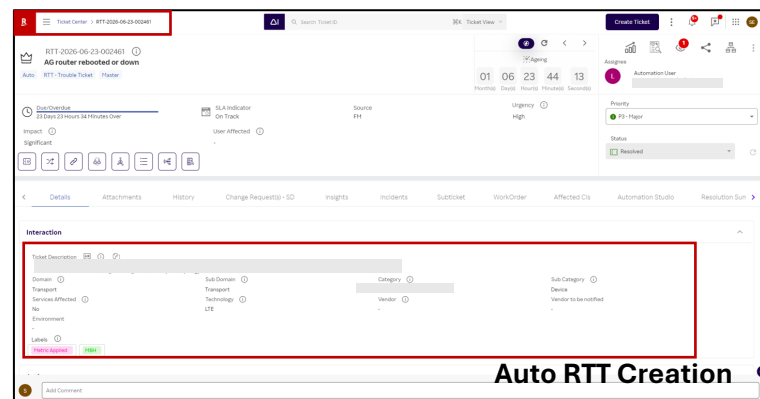


Auto RTT Resolve by AI

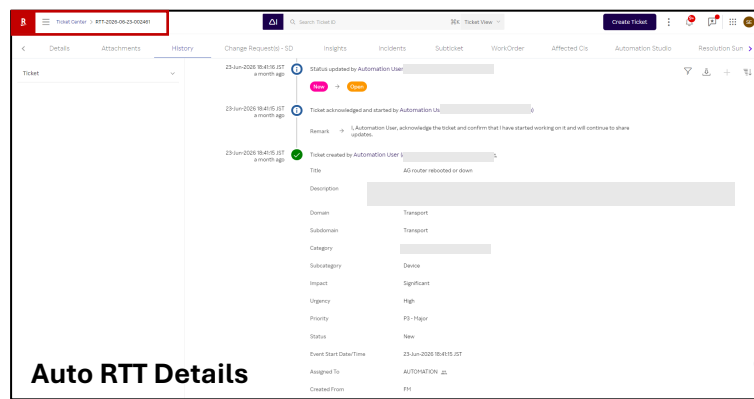
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – Device Offline

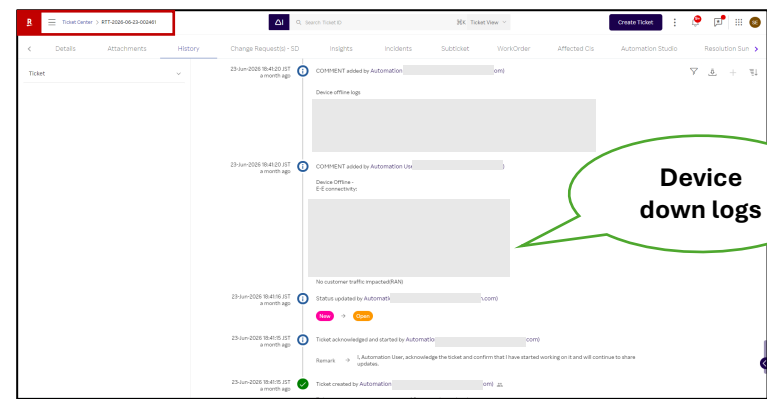
Detection and Ticketing



Trouble ticket created by FM Automation for further analysis, troubleshooting and resolution.

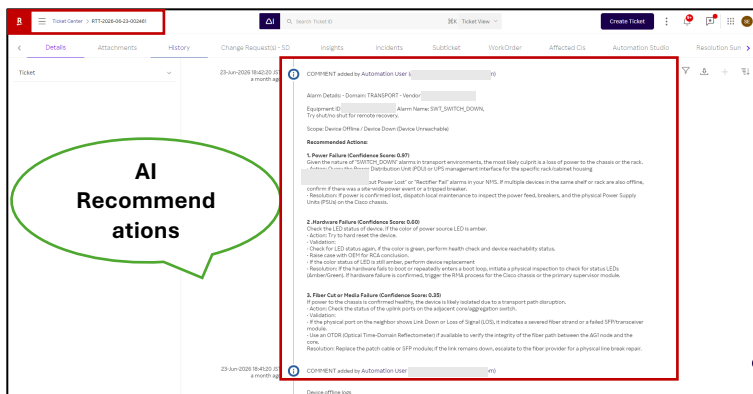


Trouble ticket details with impacted node details and timelines

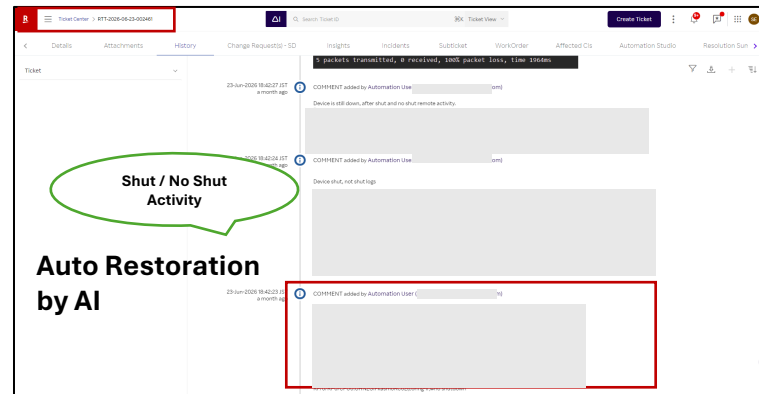


Once the RTT created, the AI agent logs into the device and collects the logs and attached in the ticket comments

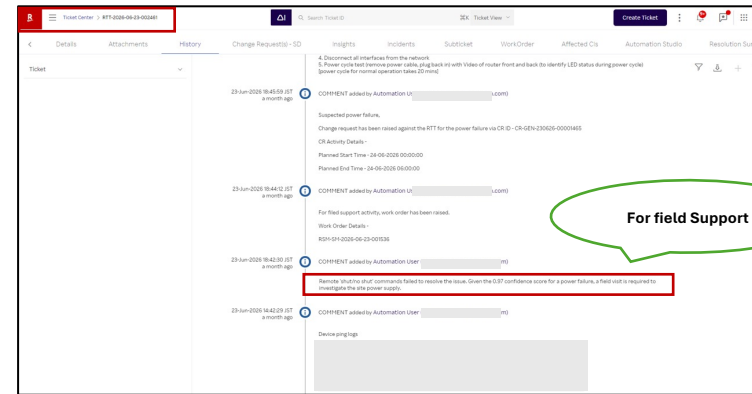
AI Recommendations & Auto Restoration



The AI agent analyses the alarm details and provide the best possible solution candidates for the resolution.



AI agent performs the auto restoration by shut/no shut activity, and checks for the device up status.



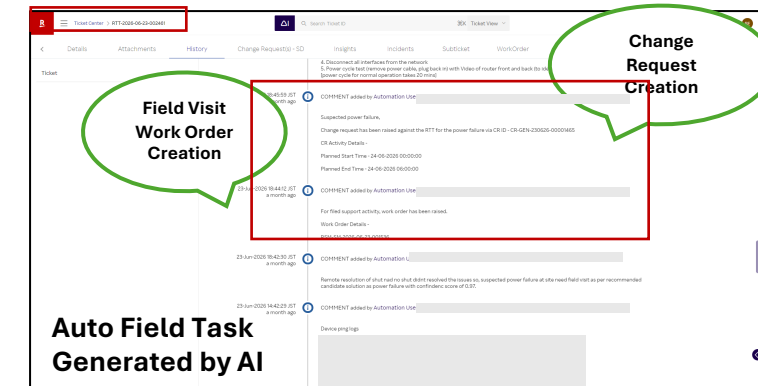
AI agent performs the auto restoration by shut/no shut activity, even of the device is still offline AI agent suggests for the field support activity.

ANLAV Report: Rakuten Mobile GB1523E v2.0.1 IP Network Fault Management

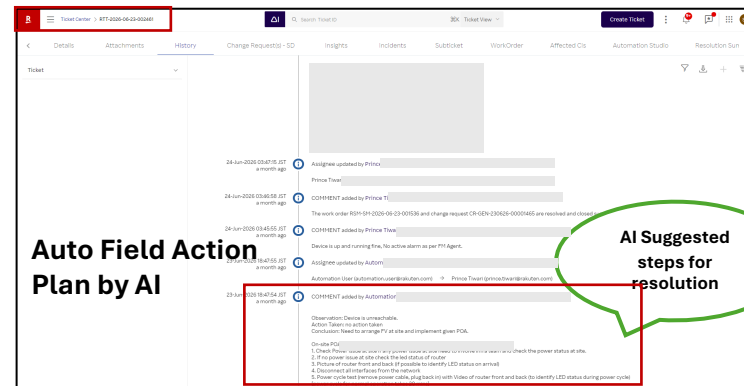
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – Device Offline

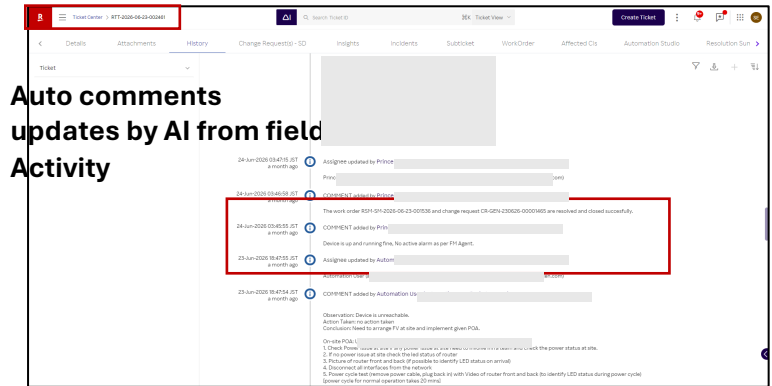
Solution Generation



As suggested by agent, it raises work order and change request for field operations.

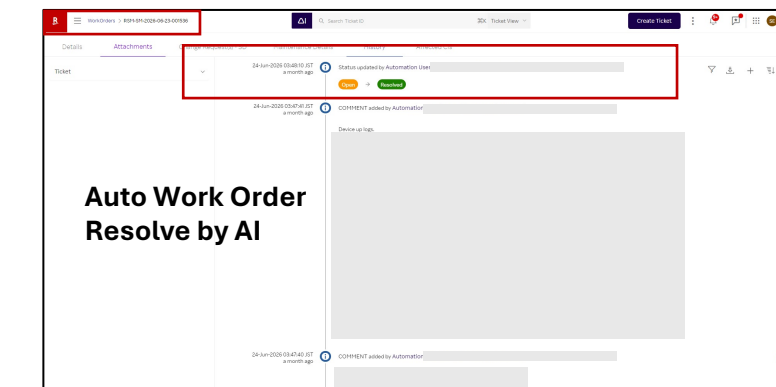


AI agent provides the troubleshooting steps for the engineer which may required during the field activity.

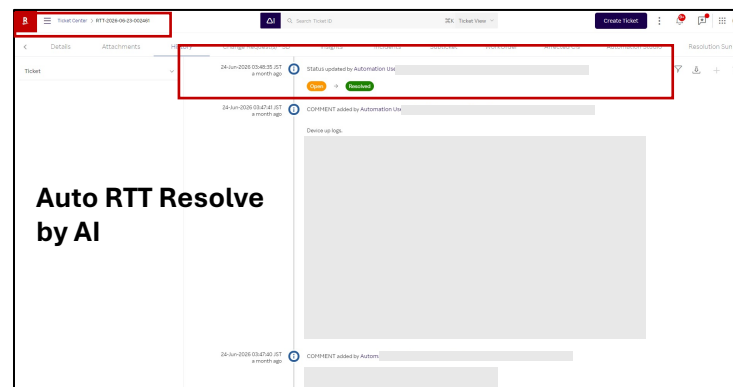


AI agent assigns the RTT to the field engineer for further activity.

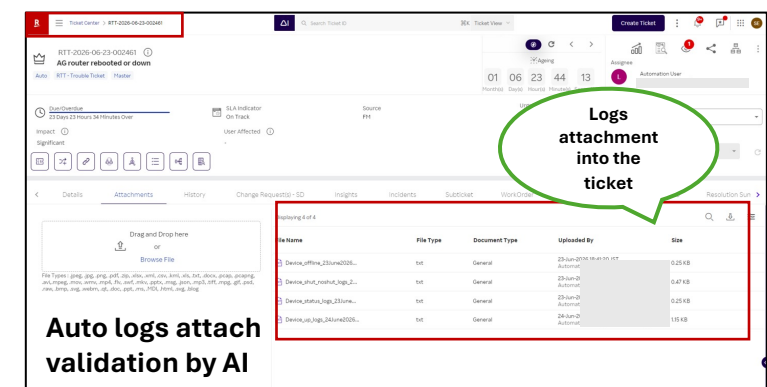
Solution Implementation and Resolution



Once the activity is completed from field side, the work order will be resolved and RTT will be assigned back to automation for further checks



Agent once receives the ticket back it verifies the status of device and if the issue is resolved, agent resolves the ticket as well.

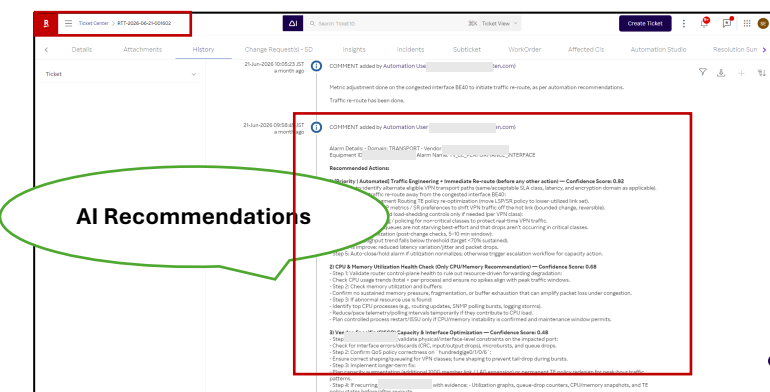


AI agent auto attaches the logs collected during each activity to the RTT attachments.

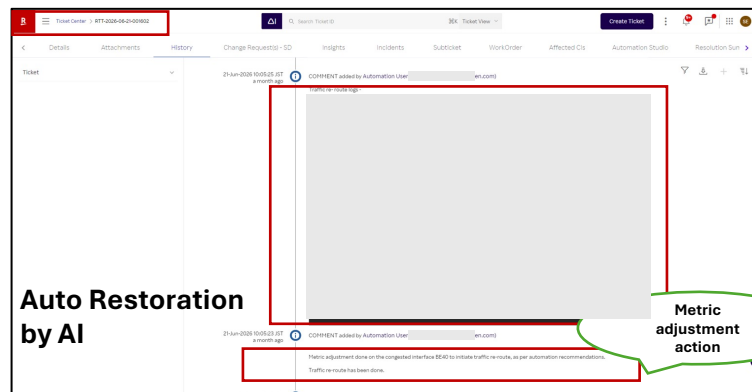
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – VPN Interruption

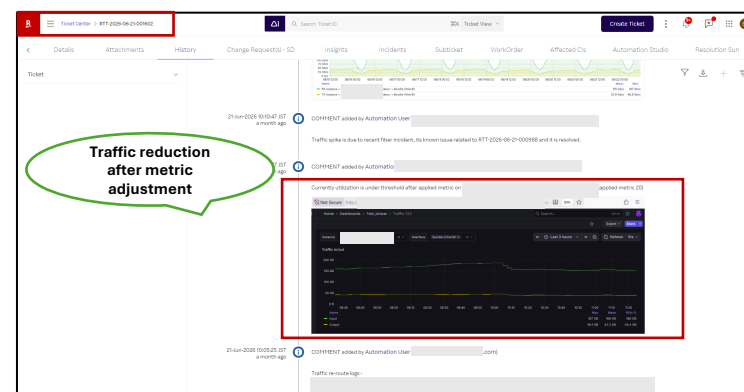
AI Recommendations & Auto Restoration



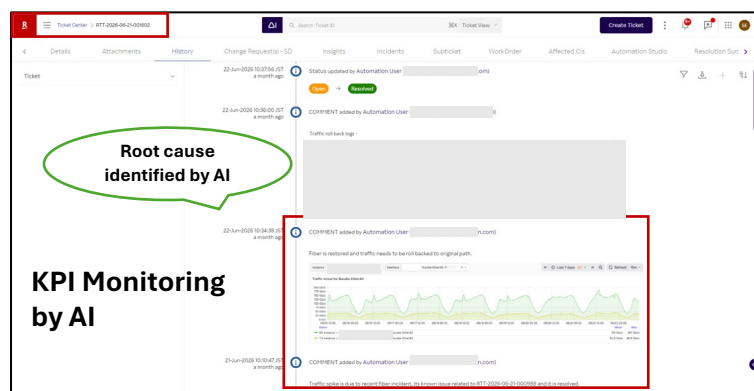
The AI agent analyses the alarm details and provide the best possible solution candidates for the resolution.



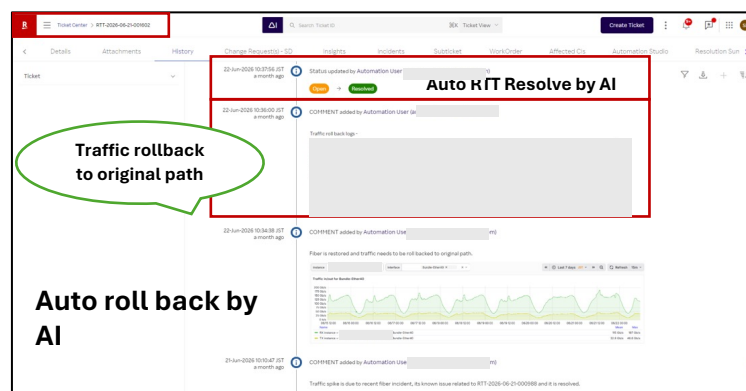
AI agent performs the auto restoration of the service re routing the traffic from impacted to active working vpn.



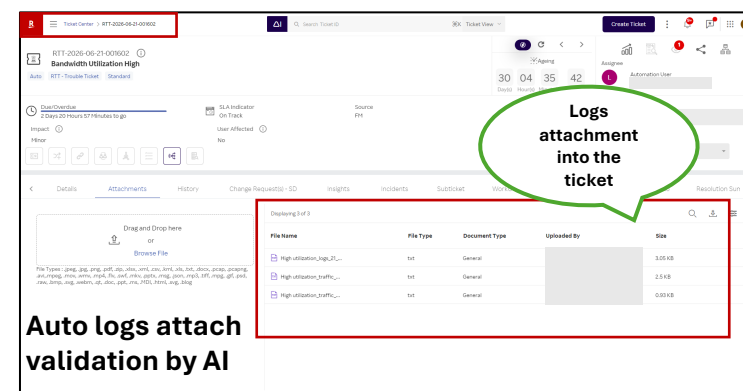
Solution Implementation and Resolution



Once the impact device RTT is fixed , the agent verifies the performance trend of current impact node and attaches status logs.



Once the impact device RTT is fixed , the agent verifies the performance trend of current impact node and attaches status logs and resolves the RTT.

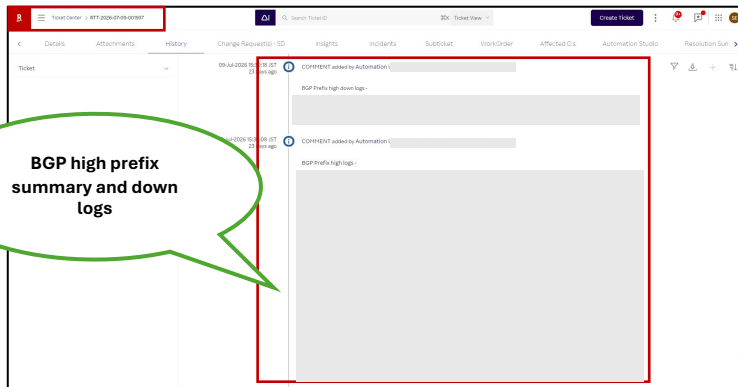


AI agent auto attaches the logs collected during each activity to the RTT attachments.

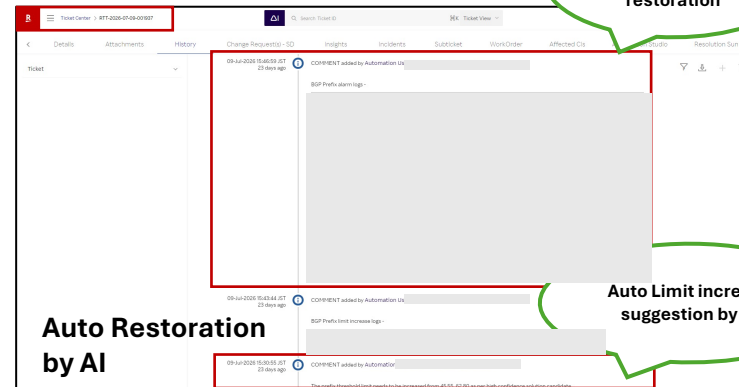
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – VPN Degradation

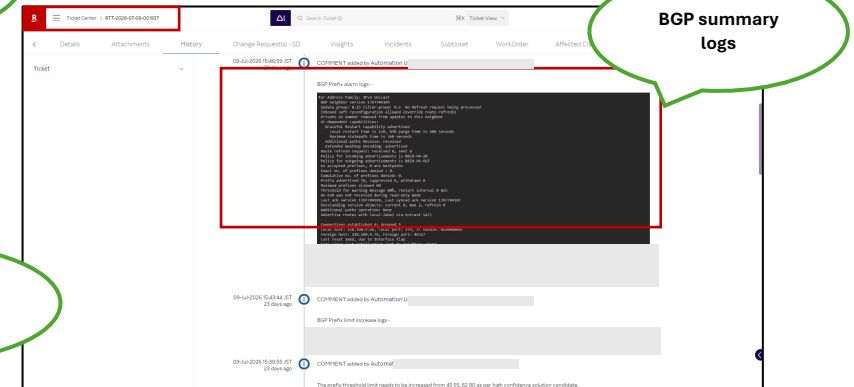
Auto Restoration and Solution Implementation



Once the RTT created, the AI agent logs into the device and collects the logs and comments the same in the ticket.

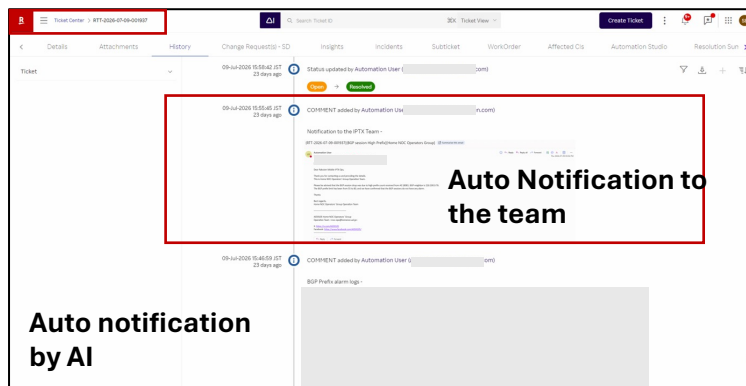


The AI agent plans the auto BGP prefix limit increase for the auto restoration and resolution of the issue.

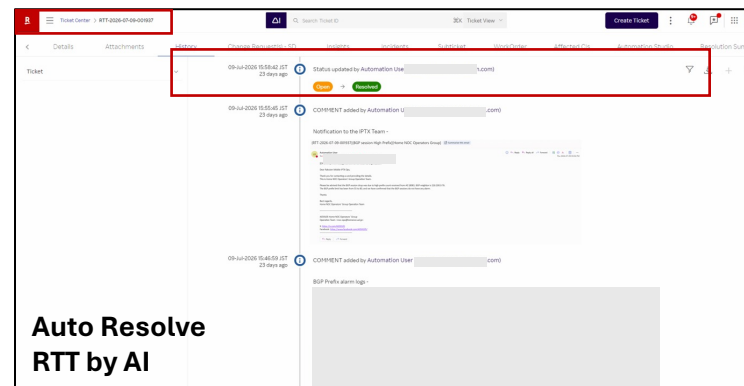


The agent performs the prefix limit increase activity by logging into the device and then verifies the device BGP prefix limit logs.

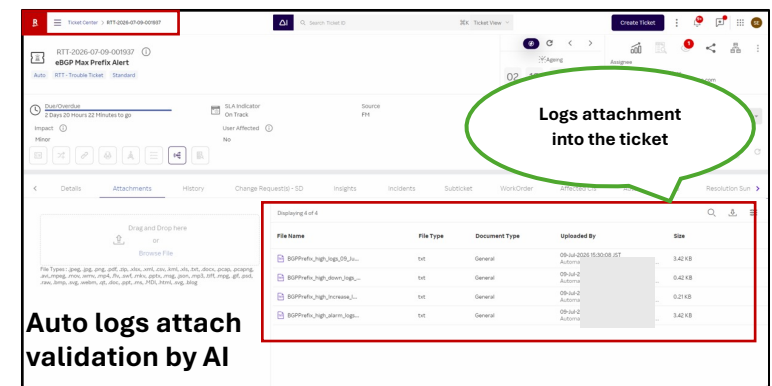
Resolution & Post Validation



The AI agent also notifies and sends an email notification to the NOC/IP Team for the performed activity details.



Agent once receives the ticket back it verifies the status of device and if the issue is resolved, agent resolves the ticket as well.

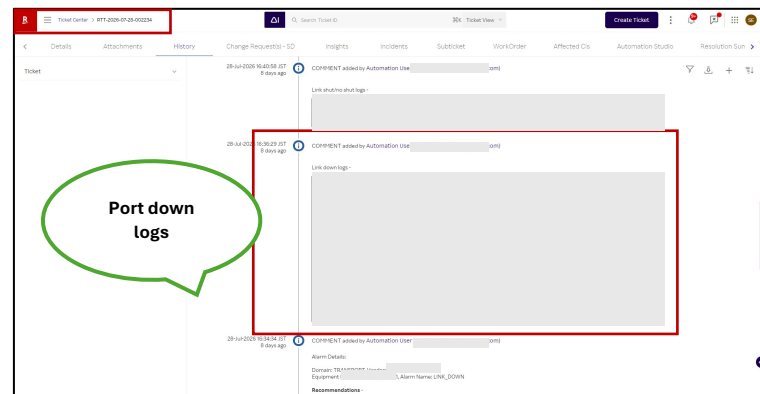


AI agent auto attaches the logs collected during each activity to the RTT attachments.

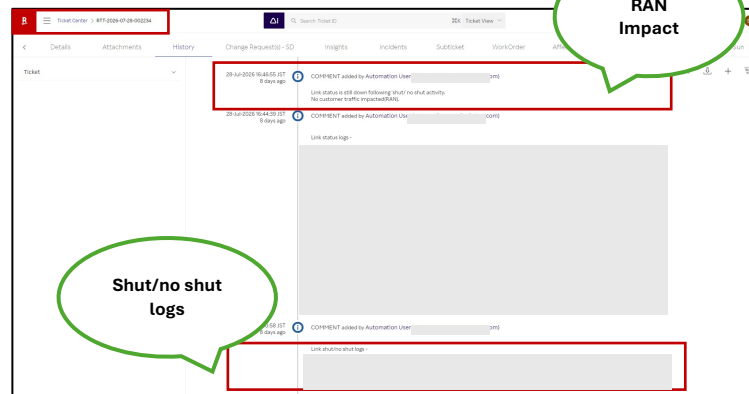
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – Port Failure

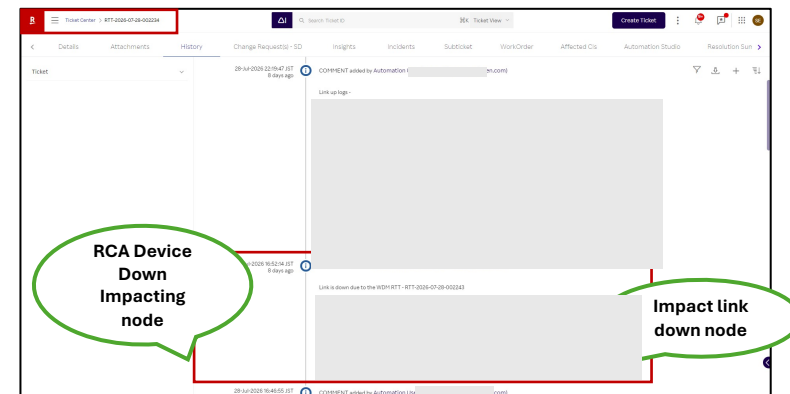
Auto Restoration & Solution Generation (RCA)



Once the RTT created, the AI agent logs into the device and collects the logs and comments the same in the ticket.

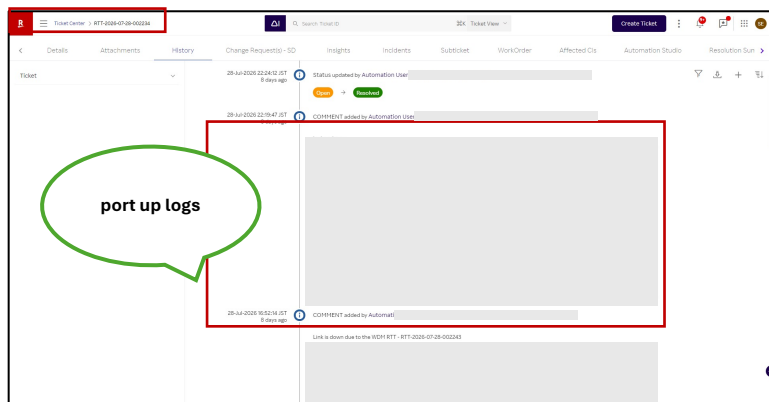


AI agent performs the auto restoration of the services performing the shut / no shut activity and does the impact analysis on the RAN domain.

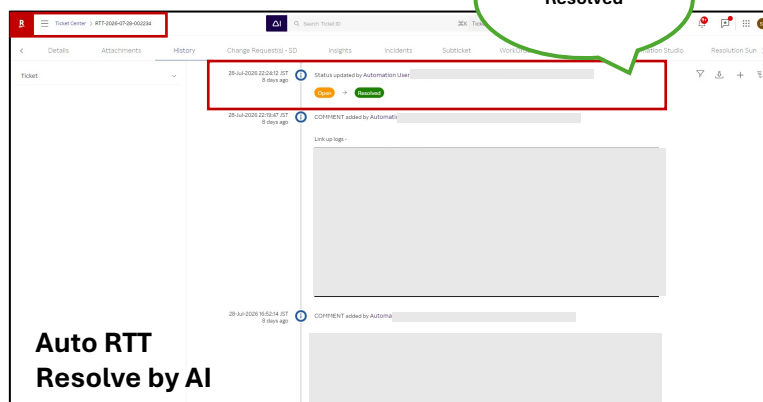


In this case agent identifies that port is due to the impact on another node and provides the details of the same.

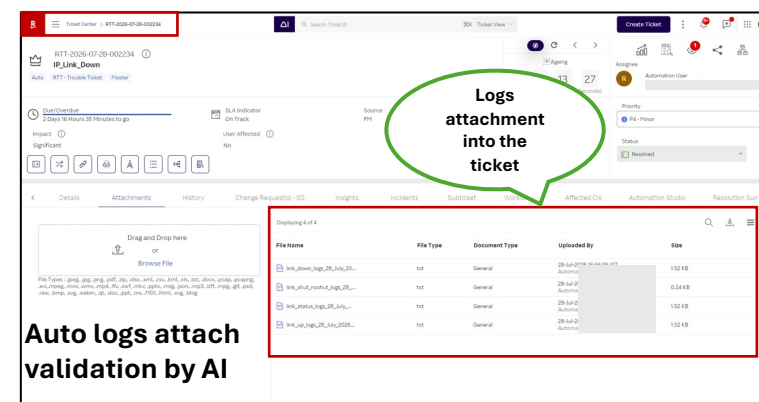
Resolution & Post Validation



Once the impacted node issue resolved as per identified RCA, the agent performs the status check of the port link.



Agent once receives the ticket back it verifies the status of port and if the port is up and issue is resolved, agent resolves the ticket as well.

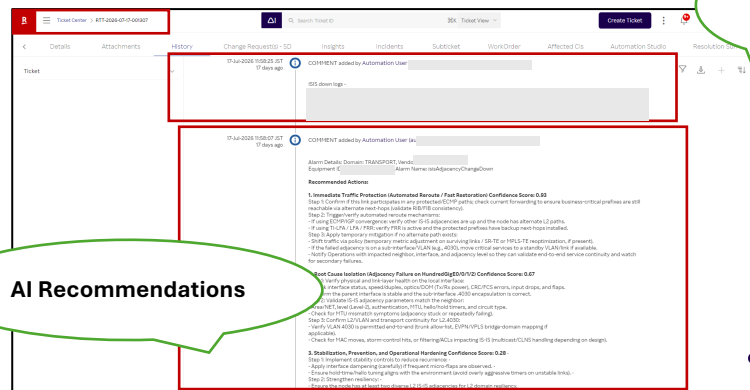


AI agent auto attaches the logs collected during each activity to the RTT attachments.

Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – Protocol State Abnormal

AI Recommendations

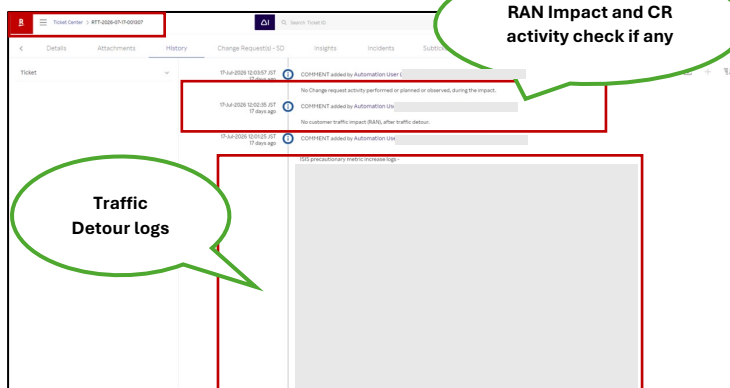


Device
Logs

AI Recommendations

The AI agent analyses the alarm details and provide the best possible solution candidates for the resolution and logs into the device and collects the down logs

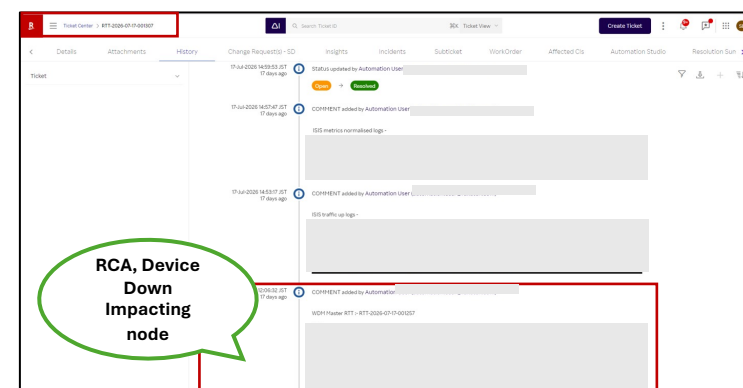
Auto Restoration & Solution Generation (RCA)



Traffic
Detour logs

RAN Impact and CR
activity check if any

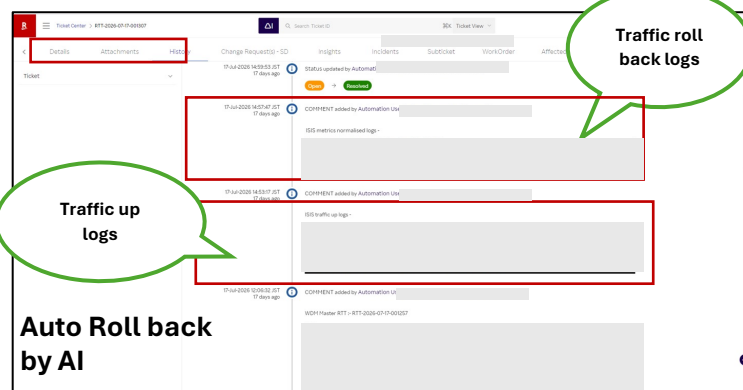
AI agent performs the auto restoration of the services performing by detouring the traffic and does the impact analysis on the RAN domain.



RCA, Device
Down
Impacting
node

In this case agent identifies that ISIS is down due to the impact on another node and provides the details of the same.

Resolution & Post Validation

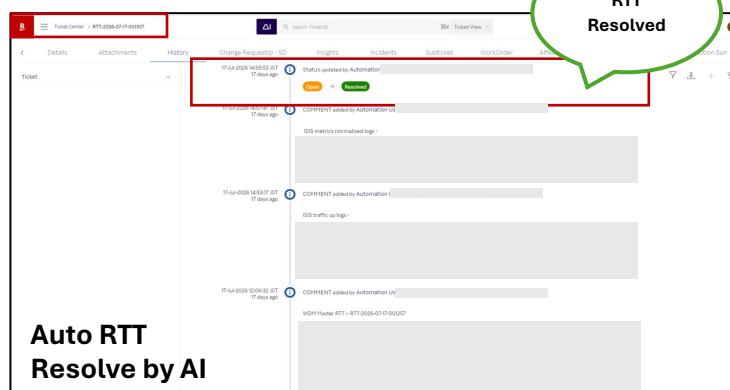


Traffic roll
back logs

Traffic up
logs

Auto Roll back
by AI

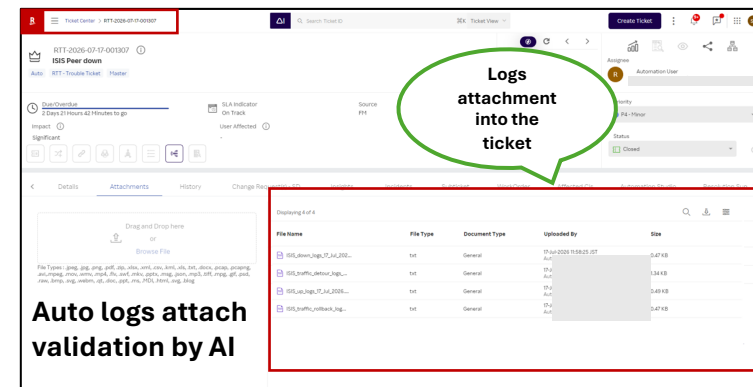
Once the impacted node issue resolved as per identified RCA, the agent performs the status check of the ISIS up log and roll backs the traffic to the original path after monitoring of 1 hour.



RTT
Resolved

Auto RTT
Resolve by AI

Once all the details are verified the AI agent, is automatically resolves the ticket.



Logs
attachment
into the
ticket

Auto logs attach
validation by AI

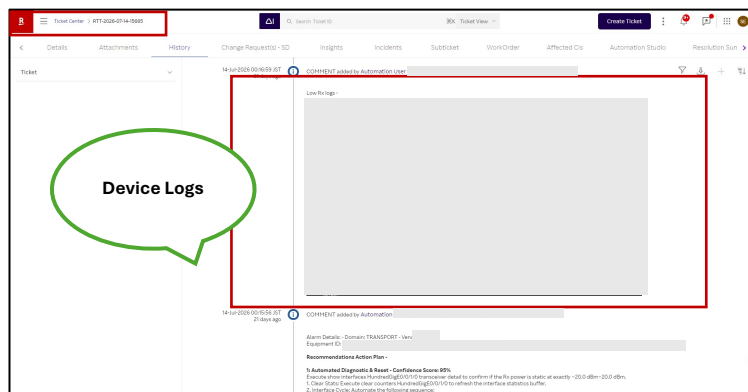
AI agent auto attaches the logs collected during each activity to the RTT attachments.

ANLAV Report: Rakuten Mobile GB1523E v2.0.1 IP Network Fault Management

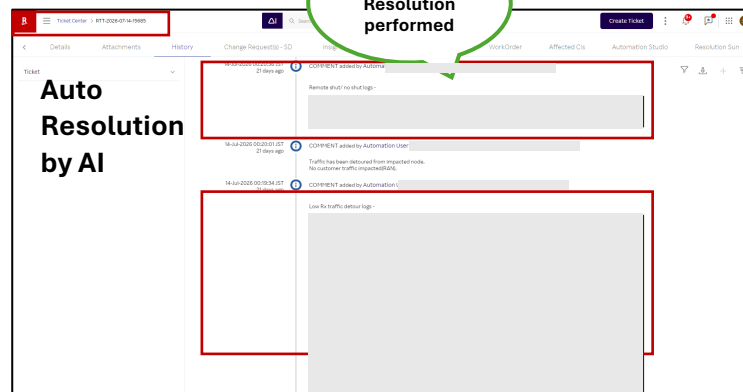
Analysis(Solution Generation) – **Decision**(Solution Evaluation & Decision Making) – **Execution**(Solution Implementation)

Scenario – Optical Module Failure or Optical Power Abnormal (Low RX)

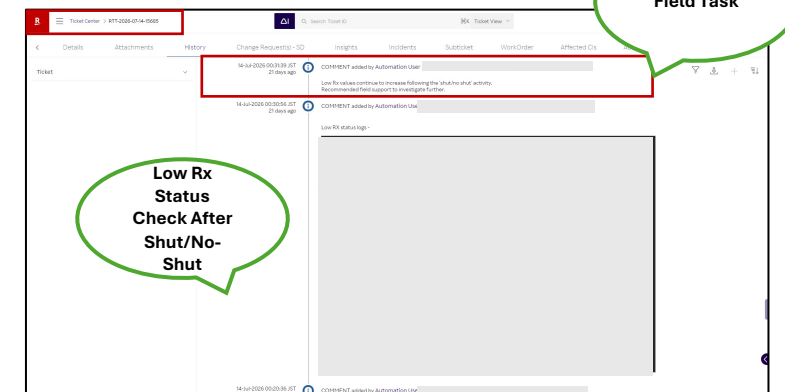
Auto Solution Generation & Auto Restoration



Once the RTT created, the AI agent logs into the device and collects the logs and comments the same in the ticket.

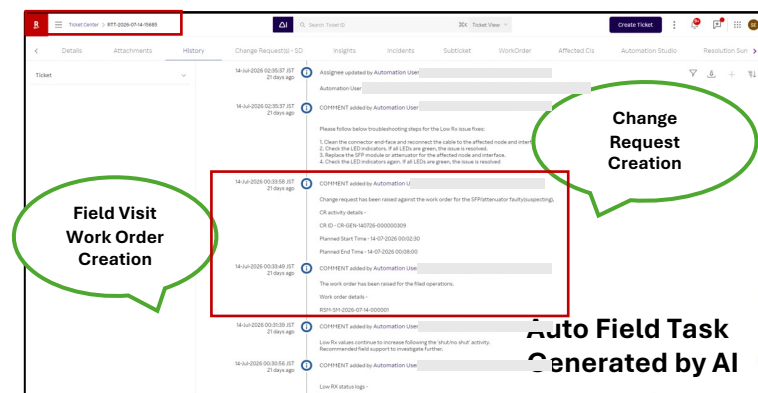


The AI agent performs the auto restoration by shut / no shut activity as suggested.

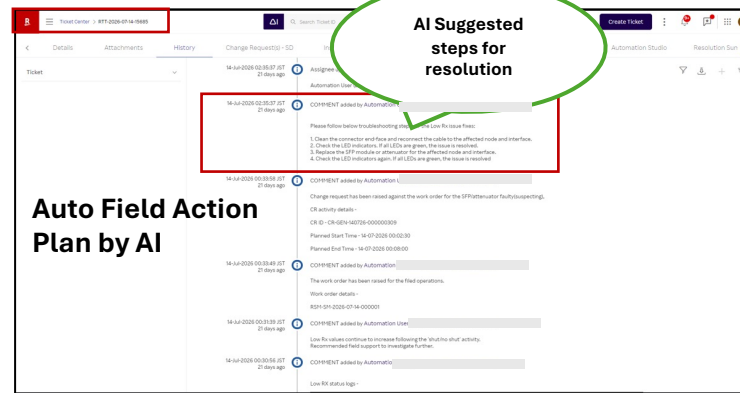


After the shut/no shut activity, the agent verifies the RX logs to verify the status, if issue is not resolved, the agent initiates the field support.

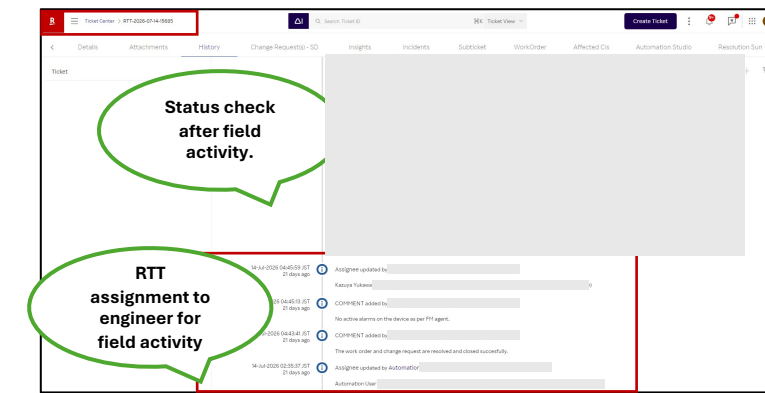
Solution Generation



As suggested by agent, it raises work order and change request for field operations.



AI agent provides the troubleshooting steps for the engineer which may required during the field activity.



AI agent assigns the RTT to the field engineer for further activity.

ANLAV Report: Rakuten Mobile GB1523E v2.0.1 IP Network Fault Management

Analysis(Solution Generation) – **Decision**(Solution Evaluation & Decision Making) – **Execution**(Solution Implementation)

Scenario – Optical Module Failure or Optical Power Abnormal (Low RX)

Human Intervention with Chat Assistant for Resolution

The first screenshot shows a ticket titled 'Low Rx status logs' with a description of the issue. A red box highlights the 'Auto WO creation by AI' section. A green callout bubble labeled 'AI BOT' points to the 'Chat System for guidance' section. A second green callout bubble labeled 'Field Engineer checks with assistant for status and guidance' points to the 'Status updated by Automation User' section. The second screenshot shows the ticket details with a red box highlighting the 'Status updated by Automation User' section. A third green callout bubble labeled 'Low Rx alarm status check' points to the 'Status updated by Automation User' section. The third screenshot shows the ticket details with a red box highlighting the 'Status updated by Automation User' section.

Once the work order is created , with the help of available Rakuten chat assistants the field engineer initiates the connector related clean up activity issue fix for the resolution during the planned change request timelines, and once the issue is fixed, the engineer verifies the status of hardware alarms via FM chat agent and if no alarms resolves the work order.

Roll Back and Post Validation

The first screenshot shows a ticket titled 'Low Rx status logs' with a description of the issue. A red box highlights the 'Status updated by Automation User' section. A green callout bubble labeled 'Traffic Roll back activity' points to the 'Status updated by Automation User' section. The second screenshot shows the ticket details with a red box highlighting the 'Status updated by Automation User' section. A green callout bubble labeled 'Logs attachment into the ticket' points to the 'Status updated by Automation User' section. The third screenshot shows the ticket details with a red box highlighting the 'Status updated by Automation User' section. A green callout bubble labeled 'RTT Resolved.' points to the 'Status updated by Automation User' section. The fourth screenshot shows the ticket details with a red box highlighting the 'Status updated by Automation User' section. A green callout bubble labeled 'Auto traffic roll back by AI' points to the 'Status updated by Automation User' section. The fifth screenshot shows the ticket details with a red box highlighting the 'Status updated by Automation User' section. A green callout bubble labeled 'Auto logs attach validation by AI' points to the 'Status updated by Automation User' section. The sixth screenshot shows the ticket details with a red box highlighting the 'Status updated by Automation User' section. A green callout bubble labeled 'Auto RTT Resolve by AI' points to the 'Status updated by Automation User' section.

Once the agent verifies the alarm status , it performs the roll back activity to shift the traffic to the original path.

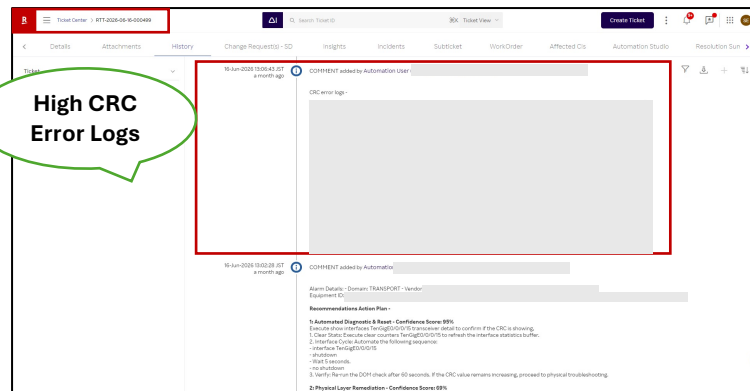
AI agent auto attaches the logs collected during each activity to the RTT attachments.

Agent once receives the ticket back it verifies the status of device and if the issue is resolved, agent resolves the ticket as well.

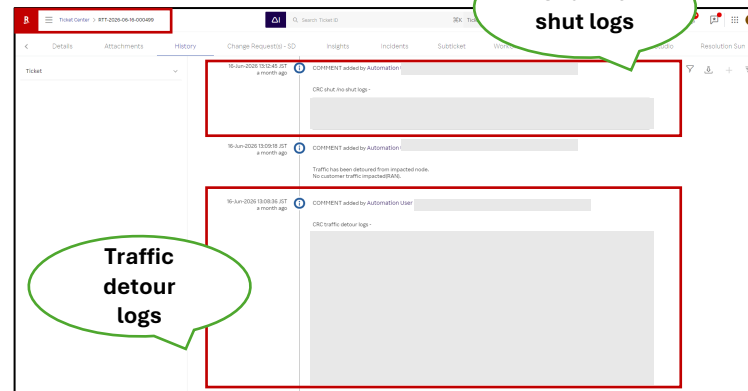
Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – High Error Rate

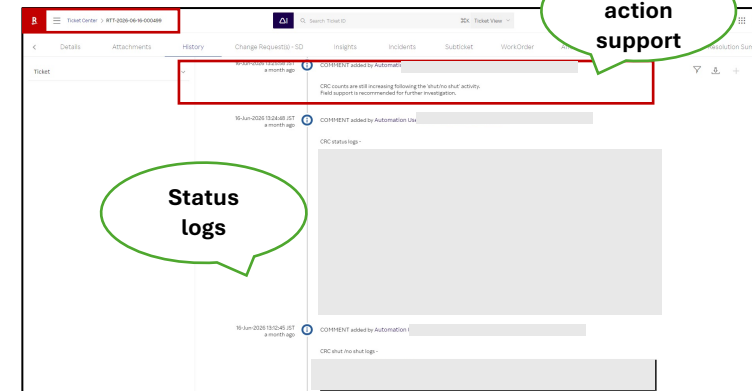
AI Recommendation Actions & Auto Restoration



Once the RTT created, the AI agent logs into the device and collects the logs and comments the same in the ticket.

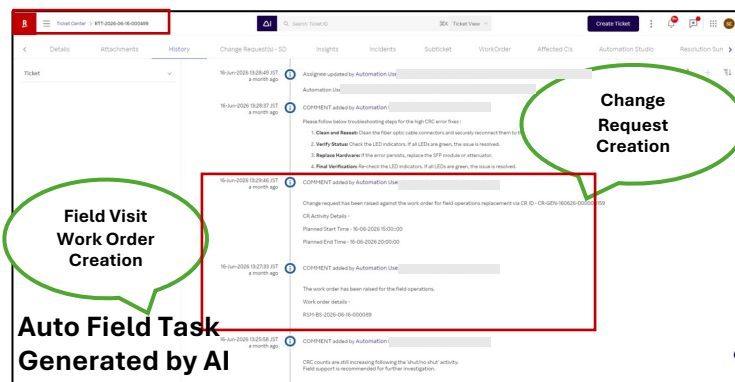


The AI agent performs the auto restoration by detouring the traffic from impacted node and by shut / no shut activity as suggested.



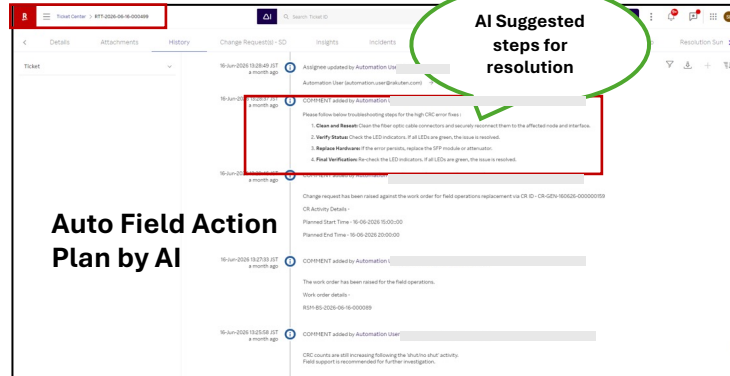
After the shut/no shut activity, the agent verifies the CRC count status to verify the status, if issue is not resolved, the agent initiates the field support.

Solution Generation

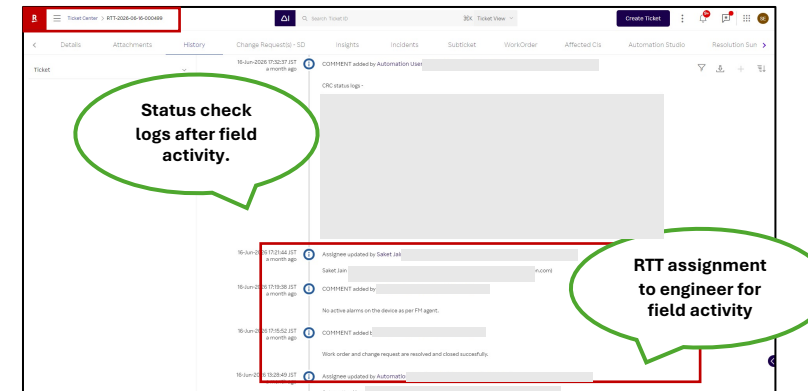


Auto Field Task Generated by AI

As suggested by agent, it raises work order and change request for field operations.



AI agent provides the troubleshooting steps for the engineer which may required during the field activity.



AI agent assigns the RTT to the field engineer for further activity.

Analysis(Solution Generation) – Decision(Solution Evaluation & Decision Making) – Execution(Solution Implementation)

Scenario – High Error Rate

Human Intervention with Chat Assistant for Resolution

Auto WO creation by AI

Field Engineer checks with assistant for status and guidance

AI BOT

The screenshot displays the 'Ticket Center' interface. A ticket titled 'WorkOrder created by Automation' is shown. The chat assistant (AI BOT) provides guidance on the steps to resolve the issue, including checking the cable connector, cleaning it, and reconnecting it. The field engineer follows these steps, and the chat assistant provides real-time status updates and guidance.

Chat System for guidance

CRC Error status check

The screenshot displays the 'Ticket Center' interface. A ticket titled 'CRC Error' is shown. The chat assistant (AI BOT) provides guidance on the steps to resolve the issue, including checking the CRC error status. The field engineer follows these steps, and the chat assistant provides real-time status updates and guidance.

Once the work order is created , with the help of available Rakuten chat assistants the field engineer initiates the connector related clean up activity issue fix for the resolution during the planned change request timelines, and once the issue is fixed, the engineer verifies the status of hardware alarms via FM chat agent and if no alarms resolves the work order.

Roll Back and Post Validation

Resolved

Roll Back logs

Auto Roll back & Resolution by AI

The screenshot displays the 'Ticket Center' interface. A ticket titled 'Roll Back' is shown. The chat assistant (AI BOT) provides guidance on the steps to resolve the issue, including performing a roll back. The field engineer follows these steps, and the chat assistant provides real-time status updates and guidance.

Logs attachment into the ticket

Auto logs attach validation by AI

The screenshot displays the 'Ticket Center' interface. A ticket titled 'Logs' is shown. The chat assistant (AI BOT) provides guidance on the steps to resolve the issue, including attaching logs. The field engineer follows these steps, and the chat assistant provides real-time status updates and guidance.

Once the agent verifies the alarm status , it performs the roll back activity to shift the traffic to the original path.

AI agent auto attaches the logs collected during each activity to the RTT attachments.

Thank You