ETSI GR ENI 035 V4.1.1 (2023-12)

GROUP REPORT

Experiential Networked Intelligence (ENI); Definition of IP networks autonomicity level

Disclaimer

The present document has been produced and approved by the Experiential Networked Intelligence (ENI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/ENI-0035v411_Def_IPNAL

Keywords
control, IP-Network, levels

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.
All rights reserved.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Experiential Networked Intelligence (ENI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document define network autonomicity features and levels for IP networks, including the intelligent characteristics at each layer (from Level 0 to Level 5) and closed-loop management process, including:

- The concept, scope, dimension and overall method of IP network operation and management autonomous level classification, evolving from ETSI GR ENI 007 [i.2] and ETSI GR ENI 010 [i.3].
- IP network operation and management processes and classification method, including service and resource management.
- Technical requirements for autonomous level classification, and its key technical processes.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR ENI 004 (V3.1.1): "Experiential Networked Intelligence (ENI); Terminology".

[i.2] ETSI GR ENI 007 (V1.1.1): "Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks".

[i.3] ETSI GR ENI 010 (V1.1.1): "Experiential Networked Intelligence (ENI); Evaluation of categories for AI application to Networks".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms defined in ETSI GR ENI 004 [i.1] and the following apply:

autonomous networks: set of self-governing programmable and explainable systems that seamlessly deliver secure, context-aware, business-driven services that are created and maintained using model-driven engineering and administered by using policies

evaluation dimension: one of the five dimensions defined as ManMachine Interface, Decision Making Participation, Data Collection and Analysis, Degree of Intelligence and Environment Adaptability

NOTE: As defined in ETSI GR ENI 004 [i.1].

evaluation object: AI application or a part of Network Lifecycle, defined from two dimensions: the subsystems and the network lifecycle

network lifecycle: work-flow of activities including network planning, network deployment, network service provisioning, network changes, network maintenance, network optimization in real-time

subsystem: network element, management system, network platform

technical expert: person in charge of defining or supporting Operational Procedures within a CSP Network (e.g. in charge of Capacity Planning, Engineering and Designing, Troubleshooting)

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR ENI 004 [i.1] and ETSI GR ENI 007 [i.2] apply.

4 Overall Framework for Autonomicity Classification targeting IP Network lifecycle

The IP network operation and management autonomous level classification framework describes the categorization dimensions (Intent management, Perception, Analysis, Decision making, Execution) of evaluating the autonomous level of specific network operation and management functional characteristics, and the categorization principle (human participation in the whole process) and qualitative descriptions (operator, system, operator + system).

Referring to ETSI GR ENI 010 [i.3], the TMF autonomous network closed-loop framework in the reference, the research on the intelligent hierarchical capability of network operation management mainly involves the service operation layer and the resource operation layer. From the end-to-end network service operation perspective, the IP network operation management process is mapped to the management and operation of one or more IP networks.

The main scope of IP network operation management in the present document involves the resource operation layer and the business operation layer, which are decomposed into life cycle operation phases (network planning, network deployment, network service provisioning, network changes, network maintenance, network optimization); each operation phase can be further split into operation sub-phases. The specific content is shown in table 1.

Table 1: Overall Framework of Network Operation Management

Operation management process	Operation Management Task
01 Network Planning, Design and Deployment	Requirements analysis and forecast
	Resource survey
	Resource analysis
	Solution design and decision-making
	Integrated configuration
	Onsite acceptance
02 Service provisioning	Service provisioning process
	Resource survey
	Solution design
	Solution implementation and service verification
03 Monitoring and Troubleshooting	Scenario-based monitoring
	Fault awareness
	Demarcation and location of faults
	Evaluation and Decision-making
	Solution implementation and service verification
04 Network Change	Intent translation
	Resource survey
	Change analysis and design
	Evaluation and Decision-making
	Change implementation and service verification
05 Network Optimization	Intent translation
	Quality monitoring
	Optimization identification
	Optimization solution
	Solution implementation and service verification

The present document will focus on the closed-loop workflows of each sub-phase in the entire life cycle of IP network operation and management, and describe the operation management tasks that each process should have at different levels. The present document will serve as the basis for the evaluation of intelligent and hierarchical categorization of IP network operation and management.

In clause 5 a deep analysis of each of the operation management process and task identified in table 1 will be analysed for each autonomous level (from 0 to 5), as defined in ETSI GR ENI 007 [i.2].

Clause 6 gives the general procedures and detailed capabilities of typical scenarios, respectively, and specifies each typical scenario. Autonomic Classification for different autonomous levels of the more relevant scenarios involving IP network.

5 Autonomous Workflow for IP Network Operation and Management

5.1 Network Planning, Design and Deployment of IP Network

5.1.1 Workflow and Task Definition

Although the network planning and design and deployment of the IP network are two phases of intelligent network operation and management, they together form a closed loop of operation and management activities.

Network planning refers to the process of surveying key information such as network coverage and high-value user distribution based on network KPI requirements, providing network planning requirements, and evaluating whether the planned solution meets network KPI requirements. The core objective of network planning is to improve the utilization of network resources.

Network deployment refers to the design of network topology, choosing appropriate hardware and software devices, estimating network capacity, IP/MPLS network design, and routing selection based on network planning. Network deployment also includes installing and deploying devices on site according to the network plan, configuration, and network test. The core objective of network deployment is to accurately construct the network according to the planning and to shorten the deployment duration as much as possible.

According to the closed-loop processing process, the IP network planning and deployment process can be divided into seven sub-tasks: network planning requirements, resource collection, resource analysis, solution design, simulation decision-making, integration configuration, and on-site acceptance. The seven subtasks can be mapped to the general workflow of network management, control, and operation, and used to further analyse the intelligent Classification of each task against the overall method of the intelligent classification framework.

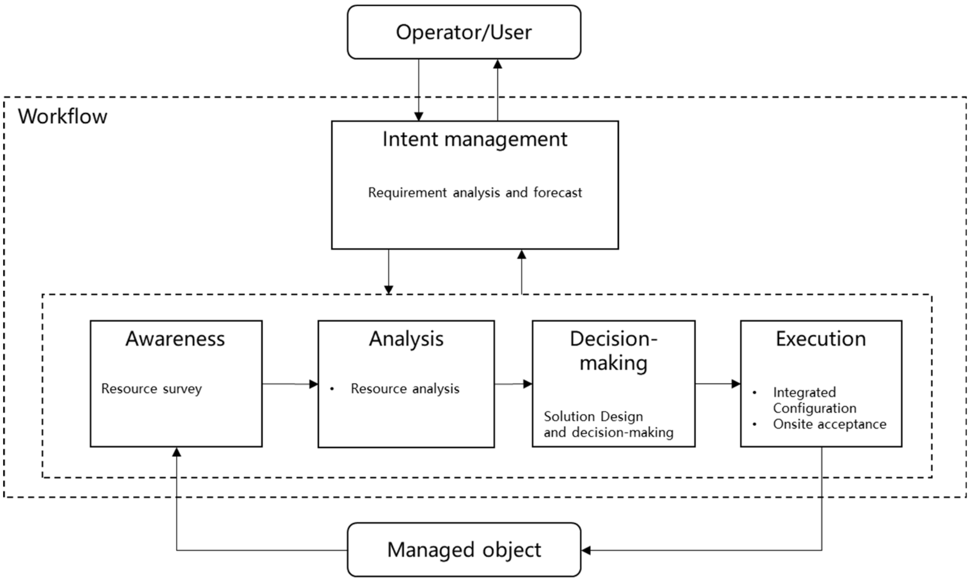

Figure 1: Mapping between network planning and design deployment tasks and operation management activities

Definition of the operation management tasks for IP network planning, design and deployment:

- **Intent management tasks:**
  - Requirement analysis and forecast: Output the network planning requirements based on the customer's business intention, service development objective, and network deployment plan (including Network topologies, IGP/BGP routings, IP addresses/VLANs space allocation, network resource bandwidth requirements, and service quality requirements).
- **Awareness tasks:**
  - Resource survey: Based on the network planning objectives and requirements, survey the resource usage (such as traffic performance, and resource usage) of the whole existing network or some areas, and collect O&M data of the existing network. (Requirements related to monitoring and troubleshooting, network optimization, service provisioning, and network complaints) Conduct a survey.
- **Analysis tasks:**
  - Resource analysis: Based on the network planning requirements and resource survey results, analyse the gap between the planning requirements and the current network resource status, obtain the resource bottleneck, and output the High-Level Design (HLD), including the IP network topology architecture (for example, multi-level AS and IP network topology). Network scale, service model (such as VPN network design), network security solution, and deployment solution.

- **Decision-making tasks:**
  - Solution design and decision-making: Output the Low-Level Design (LLD) based on the HLD, existing network survey results, device procurement, and networking technical requirements. (such as network topology, board resources and interconnection relationships, IP addresses/VLANs space planning, IGP/BGP route selection and policy configuration, QoS policy formulation, security policy design, and network monitoring and optimization policies, etc.). Evaluate the correctness and rationality of network planning requirements and perform simulation verification based on the solution planning or design results.

- **Execution tasks:**
  - Integrated configuration: Complete hardware installation and software deployment (NE initialization and NE software installation) based on the network simulation decision, and open O&M channels to ensure that NEs are managed. In addition, the NE data is delivered to the network to ensure correct software and hardware configurations.
  - Onsite acceptance: Verify the service connectivity, SLA, and reliability, generate a verification report, and pass the acceptance criteria to meet the transfer-to-maintenance requirements.

5.1.2 Classification Requirements

Table 2: Network Planning, Design and Deployment Capability Classification Requirements

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Intent management.	Requirement analysis and forecast.	Manually analyse planning requirements.	Manually analyse planning requirements.	Collect network resource data based on the system and manually analyse planning requirements.	The system automatically collects and analyses the data. (e.g. network resource usage data, network traffic growth data, etc.), manually analyse and plan requirements.	The system automatically predicts network and service requirements based on collected data and AI models. (e.g. network traffic growth trend, network connection scalability, and service quality level).	In all scenarios, the system automatically identifies planning requirements and completes the entire process of planning and design, including requirement mapping, resource survey, planning, design, simulation, data production, data delivery, commissioning and optimization, and service verification. When AI models need to be iterated, Supports automatic optimization of online learning.
Awareness.	Resource survey.	Manual resource survey.	Manual resource survey.	Manually survey resources in limited scenarios based on auxiliary tools.	The system supports the automatic online collection of online IP resources and their status, including network device resources, L2/L3 topology, and L2/L3 network connections.	The system supports the automatic collection of online IP resources, operation and SLA status, including network device resources, L2/L3 topologies, L2/L3 network connections, traffic, and applications status.	
Analysis.	Resource analysis.	Manual resource analysis.	Manual resource analysis.	The system displays resource statistics based on fixed rules, facilitating manual analysis.	The system supports device resource bottleneck analysis, such as board, port usage, and traffic analysis, and automatically identifies board resource bottlenecks.	The system can predict the growth trend of network traffic and IP connections based on AI models or digital twins and automatically identify network bottlenecks, such as network devices, boards, ports, link bandwidth, and connection reliability.	

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Decision-making.	Solution design and Decision-making.	Manually perform network simulation and decision-making.	Manually perform network simulation and decision-making with tools.	Manually perform network simulation and decision-making using tools.	The system provides templates, and the planning design is performed manually based on the templates (such as the historical project cases).	The system uses the intelligent model or digital twin to make network simulation decisions. The system automatically generates the network design scheme (such as network topology, device types, IGP/BGP route planning, and tunnel and VPN services). Perform network design, and the system automatically outputs the network design result.	
Execution.	Integrated configuration.	Prepare NE parameters and assurance policy data by using the tool and manually deliver the configuration.	Use the tool to prepare NE parameters and assurance policy data, and use the tool to deliver configurations onsite.	Use the system to prepare NE parameters and assurance policy data, and use the tool to remotely deliver configurations.	The system automatically creates NEs settings based on the design scheme, When physical network resources are ready, the system can automatically deliver configurations.	The system automatically creates NEs configuration based on the design scheme. When physical network resources go online, the system automatically manages devices and activates predefined configurations.	
	Onsite acceptance.	Manually perform onsite acceptance.	Manual on-site acceptance (such as dialling test by meter, tool, and service verification).	Use the system to verify services remotely and generate reports automatically. The system supports automatic validation of device configurations and software versions based on the manually entered acceptance data.	Based on the manually entered acceptance data, the system validates the software version, configuration, device status, and network service quality.	The system supports the flexible definition of the service validation process. After the service goes online, the system automatically validates the service and generates the validation report.	

5.2 Service provisioning in the IP network operation phase

5.2.1 Workflow and Task Definition

In the IP network operation management, carriers expect the service provisioning process to be e-commerce-based, one-click, and visible. In addition, the service provisioning process can be continuously ensured for services with differentiated SLAs, improving network serviceability. The present document divides the service provisioning sub-phase in the IP network operation phase into four tasks: service provisioning process, resource survey, solution design, solution implementation and service verification. The four tasks can be mapped to IP network operation management activities.

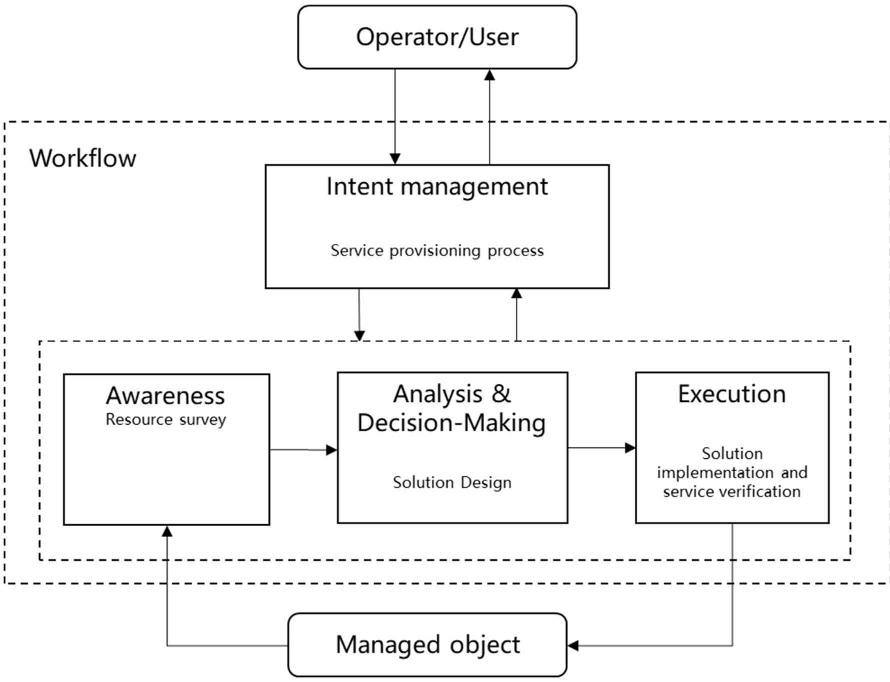

Figure 2: Mapping between service provisioning tasks and operation management activities

The following tasks can be obtained by dividing the service provisioning process based on the IP network operation management activities:

- **Intent management activities:**
  - Service provisioning process: based on user service requirements (such as the number of sites, site location, service volume, and security requirements), convert to specific network requirements (such as bearer technologies, protection requirements, security policies, and SLA assurance policies).
- **Awareness-like activities:**
  - Resource survey: Based on user service requirements and real-time network status, the resource operational status is collected.
- **Analysis and decision-making activities:**
  - Solution design: Assessment , design, and allocate network resources based on the network requirements. (for example, the device types, fibre/cable connection, port/interface numbers, and IP/VLAN space. If resources are insufficient, add new devices.) and comprehensively evaluate the design scheme (e.g. whether the customer's requirements are met and whether the existing services are affected) and provide the evaluation result.

- **Execution activities:**
  - Solution implementation and service verification: Deliver network configurations (including SLA assurance policies) to network devices based on the final solution. After the solution is implemented, verify and confirm the service implementation result, for example, whether the service is connected and whether the service SLA meets the requirements.

5.2.2 Classification requirements

Table 3: Requirements for service provisioning task levels

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Intent management.	Service provisioning process.	Manually translate the network configuration parameters from the service intent to the service.	Manually completes the network configuration parameters from the service intent to the service. (such as bearer technology, protection requirements, NE list, tunnel policy, and SLA monitoring instance).	Manually completes the network configuration parameters from the service intent to the service. (such as bearer technology, protection requirements, NE list, tunnel policy, and SLA monitoring instance).	The system has built-in service configuration templates. Service requirements (including VPN Service type, Service topology,QoS profile, etc.) can be manually selected. The system automatically maps the service parameters into network configuration parameters. (such as VPN configuration, interface configuration, etc.).	The system provides customized defined system model interface. The system automatically matches and completes network configuration for services. (e.g. VPN configuration, interface configuration, protection schemes, Tunnel policy, etc.).	In all scenarios, the system completes the intelligent closed-loop management of the entire process, including requirement mapping, data sensing, analysis, decision-making, and execution, achieving full intelligence in all scenarios.
Awareness.	Resource survey.	Manually view and collect network status information, including resource status, available ports, link bandwidth, and service resource usage.	Use tools to detect network status, including resource status, available ports, link bandwidth, and service resource usage.	The system can provide the network status, including the device resource status, available ports, link bandwidth, and service resource usage.	The system automatically detects the network operation status in non-real-time (e.g. 15 minutes), including the network topology, available ports, link bandwidth, VPN service resource usage, etc.	The system automatically detects network service status (including operation status, SLA, etc.) in real-time， e.g. seconds, and the network status in near real time, e.g. minutes, including the network topology, available ports, link bandwidth, and service resource usage.	

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Analysis & Decision-making.	Solution design.	Manually allocate network resource parameters and manually formulate service solutions.	Manually allocate network resource parameters and manually formulate service solutions.	Manually uses the system to allocate network resource parameters and manually formulates a service plan.	The system provides the resource setting templates (such as the IP addresses, VLAN IDs, bandwidth resource, and tunnel policy name). The system calculates network resources and automatically checks resource conflicts.	Based on the intention interface, the system automatically allocates network resource parameters such as the IP addresses, VLAN IDs, bandwidth resource, tunnels, etc. and calculates and recommends optimal network paths and network configuration.	
Execution.	Solution implementation and service verification.	Manually deliver service configurations and start service SLA monitoring. Manually verify the configuration.	Use the tool to deliver service configurations and start service SLA monitoring. Manual verification is performed using tools.	Operators trigger service configuration delivery through the system and manually start service SLA monitoring and service verification via the system.	The system automatically delivers the service configuration. If the service configuration fails, the system automatically rolls back and retries the configuration.	The system automatically delivers the service configuration. If the service configuration fails, the system automatically rolls back. The system support automatically retry the configuration and starts SLA monitoring.	

5.3 IP Network Maintenance

5.3.1 Overview

Network maintenance starts after network deployment and service provisioning. The objective is to accurately detect and rectify faults in a timely manner. The technical aspects focus on improving the complaint coverage rate, reducing the fault duration, fault occurrence rate, personnel investment, and test automation, improving user experience, and reducing O&M costs.

Network maintenance scenarios include monitoring, troubleshooting, and network change.

5.3.2 Monitoring and Troubleshooting

5.3.2.1 Workflow and Task Definition

According to the closed-loop processing process, the IP network monitoring and troubleshooting process consists of seven subtasks: scenario-based monitoring, fault awareness (availability and monitoring status of network resources), risk discovery, fault demarcation and locating, potential risk handling solution, solution implementation, and service verification. The seven subtasks can be mapped to the general workflow of network management, control, and operation, and are used to further analyse the intelligent Classification of each task based on the overall method of the intelligent classification framework, as shown in figure 3.

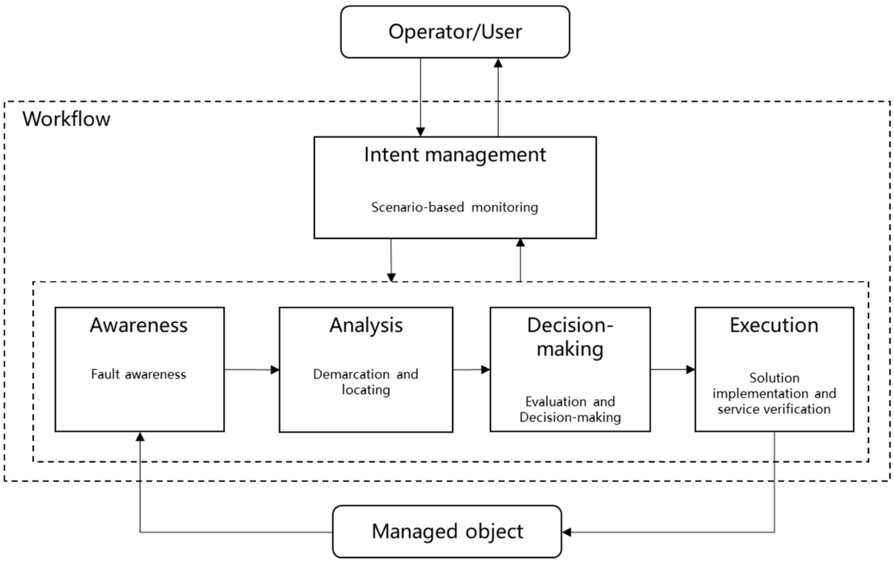

Figure 3: Mapping between monitoring and troubleshooting tasks and operation management activity

The IP network monitoring and troubleshooting process is broken down by IP network operation management activities. The following tasks can be obtained:

- **Intent management tasks:**
  - Scenario-based monitoring: Network monitoring assurance targets are defined as specific monitoring requirements, such as monitoring areas, monitoring objects, reliability requirements, and service SLA requirements. For example, SLA assurance policies for important festivals and service provisioning processes are used.
- **Awareness tasks:**
  - Fault awareness: Monitors and analyses network operation data and external spatiotemporal data to detect unexpected service interruptions or service quality deterioration on the network promptly.

- **Analysis tasks:**
  - Demarcation and locating: Demarcate faults based on identified faults and potential risks. For the cross-domain scenario, demarcate the fault to a specific technical domain. For the single-domain scenario, demarcate the fault to a specific NE. Based on the fault demarcation result, locate the specific software and hardware causes (such as configuration, board, and optical module) of the problem, and generate a solution to rectify the service as soon as possible. Analyse the impact of the fault/potential risk on services and notify the impact.
- **Decision-making tasks:**
  - Evaluation and decision-making: Generate several alternative solutions (including recovery) based on the problem demarcation and locating results (e.g. modifying configurations, restarting NEs, replacing boards, and isolating NEs).
- **Execution tasks:**
  - Solution implementation and service verification: Rectify faults and eliminate potential risks based on the optimal solution. For faults or risks that can be remotely rectified, configurations are delivered to the network through the CLI or NETCONF interface, or hardware faults are isolated from NEs or links. For faults or potential risks that cannot be rectified remotely, replace boards or optical modules on site manually, or remove and insert boards or optical modules manually. After the fault rectification and potential risk elimination actions are performed, verify and confirm the execution results, for example, whether the service interruption is recovered, whether the quality deterioration is recovered, and whether alarms and KPI exceptions are cleared.

5.3.2.2 Classification Requirements

Table 4: Monitoring and Troubleshooting Classification Requirements

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Intent management.	Scenario-based monitoring.	Manually monitor the system.	Manually define monitoring rules (such as alarm severity and category) based on alarm dimensions.	Manually developed and supervised control rule template. The system converts the template into monitoring rules (such as service paths) based on the templates.	Monitoring templates and assurance policies are preconfigured in the system. Users can select templates and assurance policies based on the scenario and confirm the templates and assurance policies.	Based on scenario-specific monitoring intentions, the system automatically monitors scenarios and areas and generates monitoring rules and automatically applies rules.	In all scenarios, the system automatically completes the whole process of intent mapping, fault detection, risk prediction, demarcation and location, repair evaluation, and implementation verification, achieving full-scenario and full-process intelligence.
Awareness.	Fault awareness.	Fault locating triggered manually by user complaints.	Use the tool to periodically check the network to detect faults. Manually identify affected services and determine the service status.	The system automatically collect the status of network resources, such as alarms and events.	The system automatically performs NE-level root cause analysis based on configured rules and identifies affected network services.	The system automatically collects and processes network operation data, automatically identifies affected services, automatically determines the service status (interrupted, degraded, or interrupted outside the network), and automatically aggregates alarms, e.g. using the AI algorithm.	
Analysis.	Demarcation and locating.	Manually use ping and trace methods to demarcate the fault, and locate the fault by querying logs, device status information, and routing information.	Use a tool to export current or historical alarms, performance data, and logs for correlation analysis, and manually demarcate and locate faults.	The system provides auxiliary functions. (e.g. visible alarms and logs associated with trails). Manually demarcate and locate the fault.	The system provides configured rules (such as alarm correlation rules), automatically perform correlation analysis and provide possible root cause recommendations, facilitating manual demarcation and locating.	The system performs intelligent fault diagnosis based on the AI model and/or digital twin of the network and automatically demarcates and locates faults.	

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Decision-making.	Evaluation and Decision-making.	Manually design problem rectification solutions based on problem demarcation and locating results.	Manually use the system to collect related information, analyse the cause, and complete the solution.	The system provides the tools (such as resource collection, script command lines, etc.) to complete the rectification solution.	Based on the demarcation and locating results, the system automatically matches the configured rectification process and generates a rectification solution.	The system supports a flexible definition of fault rectification solutions and can automatically generate a rectification solution based on the demarcation and locating results.	
Execution.	Solution implementation and service verification.	The network engineer manually completes the repair operation according to the approved final solution. Perform service acceptance through on-demand tests.	Use the tool/system to perform the repair solution in a single step. The tool provides tasks such as service on-demand test, alarm observation, and service KPI observation. With the help of the tool, the personnel can complete service acceptance.	Complete the execution of all steps in the solution at a single site level. Users can view object information in batches to assist users in service acceptance.	The system remotely and automatically executes the solution. The system provides a network-level service verification tool to automatically verify service recovery solutions and output acceptance reports.	The system supports automatic delivery and execution the solution. The system support automatically verifies the service and output acceptance reports.	

5.3.3 Network change

5.3.3.1 Workflow and Task Definition

When the network deployment is complete and basic network changes are involved, the operator expects the changes to be simple and efficient and to minimize the impact on services, or even have no impact on services. According to the closed-loop processing process, the IP network change workflow can be divided into six tasks: intent translation, resource survey, change analysis and design, evaluation and decision-making, change implementation, and service verification. The five tasks can be mapped to the general workflow of IP network operation management.

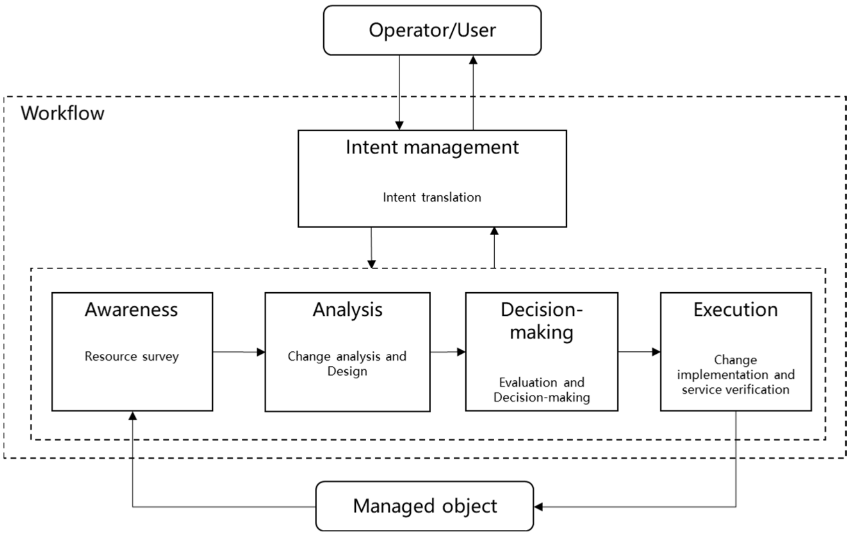

Figure 4: Mapping between network change tasks and operation management activities

The IP network change process is broken down by IP network operation management activities. The following tasks can be obtained:

- **Intent management activities:**
  - Intention translation: Based on the network change request (change type, area scope, involved NEs, etc.), evaluate the affected user scope, and output the change constraint conditions based on factors such as the user service SLA and the allowed change period (such as the change time window and service interruption time).
- **Awareness-like activities:**
  - Resource survey: Collect information about the network and services affected by the change, including the network topology, recent network traffic and quality data, network routing information, and service information carried by the change object, such as service paths, traffic, and quality. Design the alternative change solution based on the network change request and change constraints.
- **Analysis activities:**
  - Change analysis and design: Design the change solution based on the network change request and change constraints.
- **Decision-making activities:**
  - Evaluation and decision-making: Perform simulation on the change solution, compare the network topology, route, and service changes before and after the change, evaluate the impact of the solution on service quality, and determine the final solution to be implemented.

- **Execution activities:**
    - Change implementation and service verification: Implement the network change solution, including the delivery of software configuration changes and synchronization with hardware changes. Perform changes to the network infrastructure based on the optimal solution (e.g. hardware installation/replacement, software upgrade, patching, etc.). After the network change is implemented, verify and confirm the execution result (for example, whether the service SLA meets the expected target), observe the change, and handle the problem in time.

5.3.3.2 Classification requirements

Table 5: Requirements for hierarchical network change tasks

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Intent management.	Intent translation.	Manually decide the network change scenarios, restrictions, and configuration requirements, and guide the corresponding operations.	Manually decide the network change scenarios, restrictions, and configuration requirements, and guide the corresponding operations.	Manually decide the network change scenarios, restrictions, and configuration requirements, and guide corresponding operations.	The system support preset common scenario patterns, configuration templates, and change constraints. Operators can select multiple scenarios and enter the change scope to complete the intention translation.	The system automatically associates the template and changes constraint information in the scenario mode based on the policy. The intention translation is completed by selecting the template and entering the changing scope at one time.	In all scenarios, the system completes the intelligent closed-loop management of the entire process of network change, including requirement mapping, data collection, solution design, decision-making, and execution, achieving all-scenario and all-process intelligence.
Awareness.	Resource survey.	Manually collect network topology, network traffic, service traffic, and quality information.	Manually collect data on a large scale and in batches by using tools, improving the collection efficiency.	The system provides 15-minute and 24-hour collection tasks for service resources, such as ports and bandwidths and displays data in graphics.	After the network change mode and scope are determined, the system automatically starts data collection for related resources and services in 15 minutes or 24 hours.	After the network change mode and scope are determined, the system automatically starts to collect data of related resources and services in seconds or minutes.	
Analysis.	Change analysis and design.	Manually design the operation object change process, service migration process, and configuration information.	Manually design the operation object change process, service migration process, and configuration information.	The tool consolidates common change modes, and the change process and configuration information help simplify the design process.	The system provides a configuration template. The system automatically generates a change solution.	The system automatically matches the template based on the change scope and change mode and generates a change solution with one click.	
Decision-making.	Evaluation and decision-making.	Review the change solution by experts, identify problems, and correct the problems.	Review the change solution by experts, identify problems, and correct the problems.	Use tools to simplify resource allocation and consistency check, assist experts in reviewing change solutions, identify problems, and correct problems.	The system supports configuration verification and outputs the verification result to assist decision-making.	The system automatically completes configuration simulation, verifies the changed network topology, routes, alarms, and service status, and makes decisions automatically.	

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Execution.	Change implementation and service verification.	Manually perform the involved configuration changes on site. Manually verify the operation result by running commands on site.	Use tools to remotely complete software changes. Manually verify the operation result by running commands.	Based on the solution design result, the personnel deliver the configuration through the system. The system collects the network topology, alarms, traffic, and service quality information after the change and verifies the implementation effect.	The system automatically detects hardware changes and delivers configurations to the network-level solution based on the solution design result. After the solution is implemented successfully, the system collects network-level data, such as the network topology, alarm, traffic, and service quality information, and verifies the effect.	The system automatically detects hardware changes and automatically delivers network-level configurations based on the solution design result. Hardware installation personnel do not need to trigger or communicate with each other. After the solution is implemented, the system automatically collects the changed network-level data, such as the network topology, alarm, traffic, and service quality information, and compares the data with the data before the solution implementation to generate an acceptance report.	

5.4 Network optimization in the IP network optimization phase

5.4.1 Workflow and Task Definition

Network optimization mainly includes quality optimization. By collecting network data, creating different data models, and analysing the data based on AI technologies, network optimization improves resource utilization, service quality, and energy efficiency. The present document divides the network optimization sub-phase of IP network optimization into tasks: intent translation, quality monitoring, optimization identification, optimization solution, solution implementation and effect verification. The tasks can be mapped to IP network operation management activities.

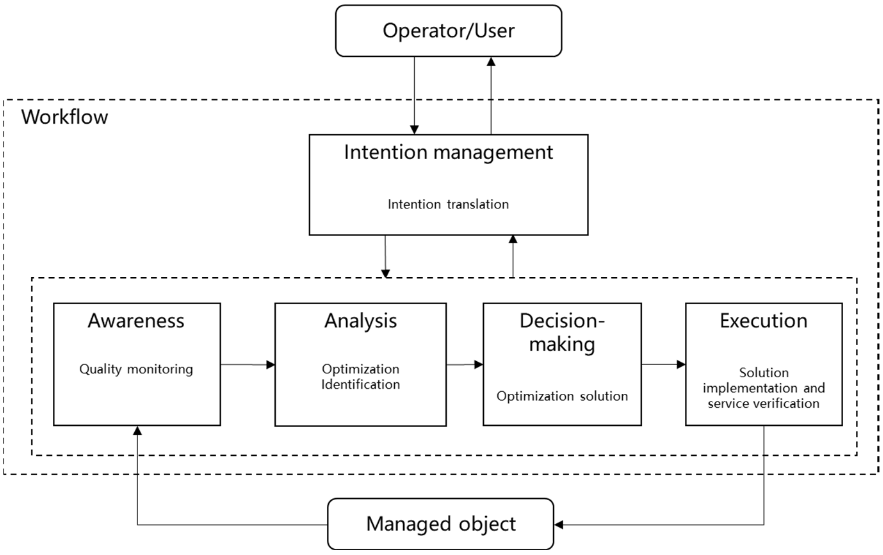

Figure 5: Mapping between network optimization tasks and operation management activities

The network optimization process is broken down by IP network operation management activities. The following tasks can be obtained:

- **Intent management activities:**
  - Intention translation: Network quality and service SLA monitoring and assurance targets are defined as specific monitoring requirements, such as monitoring areas, monitored objects, and monitored contents.
- **Awareness-like activities:**
  - Quality monitoring: Monitors and associates network running data and external spatiotemporal data, such as service traffic, interruption, and latency.
- **Analysis activities:**
  - Optimization identification: Performs periodic trigger analysis on the network running data and external spatiotemporal data. Detects and analyses poor network connection quality (such as packet loss) and service SLA problems (e.g. protection degradation, latency, availability, intermittent disconnection, etc.), perceive and predict user experience and satisfaction issues. Based on the identified performance anomaly or deterioration prediction information and the environment monitoring the situation, support the generation of optimization solutions.
- **Decision-making activities:**
  - Optimization solution: Formulate an optimization solution based on the problem demarcation and locating results. Review the solution to improve the automation capability of the whole process.

- **Execution activities:**
  - Solution implementation and service verification: Optimize the network based on the optimal solution and deliver the optimized parameter settings to the network through the CLI and NETCONF interfaces. After the optimization is performed, verify and confirm the execution result, such as the customer experience, energy saving requirements, and resource usage.

5.4.2 Classification requirements

Table 6: Requirements for network optimization task classification

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Intent management.	Intent translation.	Manually perform the network parameter adjustment requirements to specific network parameter adjustment operations.	Manually completes the network parameter adjustment requirement to the specific operation of the network parameter adjustment.	Manually completes the network parameter adjustment requirement to the specific operation of the network parameter adjustment.	The system support predefines templates for common parameter adjustment intentions, such as bandwidth, reliability, and latency, and completes intention translation.	The system supports predefining common adjustment intentions. The system automatically selects parameter adjustment templates and assurance policies based on industry and network conditions and completes intention translation.	In all scenarios, the system completes intention mapping, network health identification, and risk prediction, achieving all-scenario intelligence.
Awareness.	Quality monitoring.	Manually view and collect network and service status and identify services to be adjusted.	Operators can use tools to detect the network and service status and identify services to be adjusted.	The system provides network topology and service status data and identify services to be adjusted.	The system monitors the quality data periodically (e.g. in 15 minutes or 24 hours). The system can automatically detect the service running status, priority, and network situation.	The system monitors the network topology, service status, and service quality in real-time (e.g. in seconds).	
Analysis.	Optimization identification.	Manual check and identification.	Manual identification based on the information provided by the tool.	The system provides trend fitting and manual identification of network data.	Based on the detected data, the system provides possible causes and suggestions to assist personnel in designing and evaluating optimization solutions.	The system automatically identifies network and service deterioration such as link congestion and service SLA deterioration based on the AI model or digital twin model.	

Operation management activities	Task	L0	L1	L2	L3	L4	L5
Decision-making.	Optimization solution.	Manually design the parameter adjustment solution based on the demarcation and locating results.	Manually design the parameter adjustment scheme using the auxiliary function of the system.	The system supports preset alternative parameter adjustment schemes, manual selection of alternative schemes, and manual adjustment to generate the final parameter adjustment scheme.	The system provides possible causes and suggestions based on the optimization identification results, helping engineers design and evaluate optimization solutions.	The system is capable of analysing the impact of it decisions and it autonomously identified an appropriate optimization solution based on quality demarcation and location results and evaluates the solution (for example, link bandwidth change information, tunnel path change information, and delay change information before and after optimization).	
Execution	Solution implementation and service verification.	Manually adjust and verify the parameters based on the final solution.	Use the tool to adjust parameters. Use tools to complete the verification.	Manually use the system and execute the optimization solution at a single site level according to the embedded fixed instructions. Manually determine the optimization effect.	Based on the determined optimization solution, the system provides the network-level solution execution capability and automatically verifies the optimization effect.	Based on the determined optimization solution, the system automatically executes the network-level solution and verifies the optimization effect.	

6 Network Service Scenarios and Autonomous Network Classification Recommendations

6.1 Overview

Based on the general procedures and classification methods for IP network planning, deployment, maintenance, optimization, and operation of five scenarios specified in clause 5, this clause gives the general procedures and detailed capabilities of typical scenarios, respectively, and specifies each typical scenario. Autonomic Classification for different autonomous levels of the more relevant scenarios involving IP network.

6.2 Service Provisioning in the Operation Phase - 5G Bearer Service Provisioning

6.2.1 Function Requirement Overview

The fast rollout of new 5G base stations requires that IP bearer networks be opened up before wireless base stations go online. To meet the requirements for rapid provisioning of a large number of base stations, the bearer network needs to provide simplified service requirement input interfaces, automatically convert network parameters, and automatically deploy and verify services to ensure quick provisioning of bearer services.

6.2.2 Process Task Definition

Figure 6 shows the general process task mapping for 5G bearer service provisioning. The details are as follows.

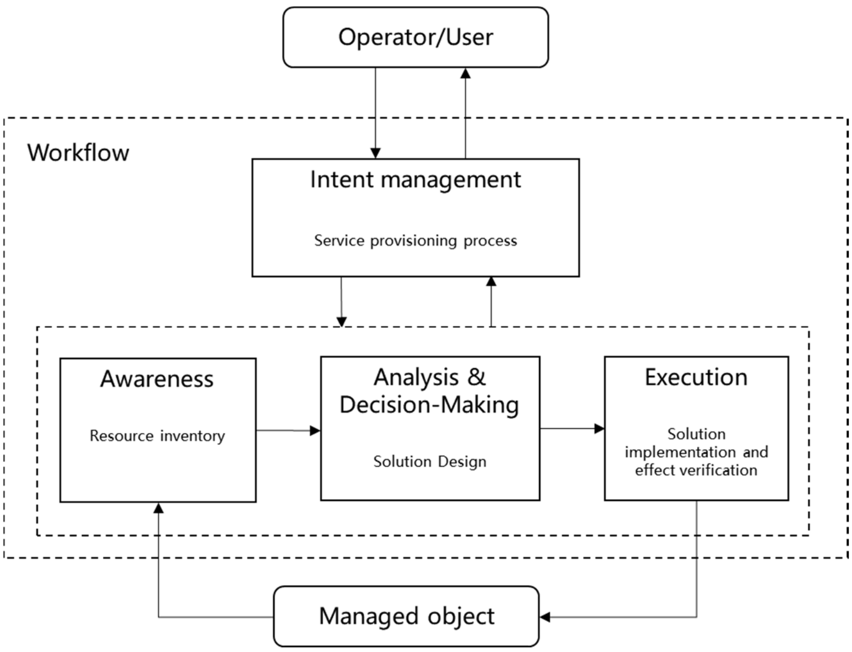

Figure 6: 5G bearer service provisioning capability and task mapping

- **Intent management tasks:**
  - Bearer service provisioning intention: Bearer network planning personnel and wireless network planning personnel work together to prepare bearer service planning data, including base station location and bearer service SLA requirements, and import the data into the management and control system through the simplified intention interface. The network parameter configuration template of the built-in service in the management and control system automatically converts the service requirements imported through the simplified intent interface into the bearer technology at the network layers (e.g. L3VPN, HOVPN, L2+L3 solution), protection requirements (HSB, VPN FRR, VRRP and E-Trunk protection), NE list and tunnel policy (LDP LSP, RSVP-TE, SR-TE, and SRv6 Policy) and SLA assurance.

- **Perception tasks:**
  - Resource survey: Dynamically obtains network device resources, idle ports, and link bandwidth, and dynamically detects network resource changes. Obtains network SLA monitoring data in real time, including latency, bandwidth, and traffic, and dynamically detects network changes.

- **Analysis and decision-making tasks:**
  - Solution design: After confirming the service network requirements, the system automatically allocates resources, including the VRF RD/RT, L2VPN VCID, and LSP label, and automatically generates a service configuration solution. At the same time, the service assurance solution is automatically generated.

- **Perform the following tasks:**
  - Solution implementation and effect verification: Hardware installation engineers connect fibre connections from base stations to the bearer network. NEs on the bearer network automatically detect the online bearer service and notify the management and control system of new service access. The management and control system automatically delivers configurations and service SLA assurance based on the service solution.

6.2.3 Classification requirements

Table 7 lists the technical requirements for 5G bearer service provisioning level classification.

Table 7: Requirements for 5G bearer service provisioning capabilities

General Process	Ability	L0	L1	L2	L3	L4	L5
Intent management.	Translation of bearer service provisioning intention.	Manually transfer the service intention. (e.g. base station type, access address, access rate, and quality requirements) Convert to network configuration parameters. (such as access devices, VPN types, bearer tunnels, and QoS requirements).	Operators use tools to integrate business intentions. (e.g. base station type, access address, access rate, and quality requirements) Convert to network configuration parameters. (such as access devices, VPN types, bearer tunnels, and QoS requirements).	Operators use the system to transfer business intentions. (e.g. base station type, access address, access rate, and quality requirements) Convert to network configuration parameters. (such as access devices, VPN types, bearer tunnels, and QoS requirements).	The system uses the preset service template to add the service intention. (e.g. base station type, access address, access rate, and quality requirements) Convert to network configuration parameters. (such as access devices, VPN types, bearer tunnels, and QoS requirements).	The system supports a flexible online service model definition. The system uses the service template to export the service intention. (e.g. base station type, access address, access rate, quality requirements, etc.) Automatically convert to network configuration parameters. (such as access devices, VPN types, bearer tunnels, and QoS requirements).	In all scenarios, the system completes the intelligent closed-loop of the entire process, including requirement mapping, data sensing, analysis, decision-making, and execution, achieving complete intelligence in all scenarios.
Awareness.	Resource survey.	Manually view and collect network status information, including resource status, available ports, and link bandwidth.	Users can use tools to detect the network status, including the resource status, available ports, and link bandwidth.	The system detects the network status, including the resource status, available ports, and link bandwidth usage.	The system can detect network resource and status changes within 15 minutes and automatically generate a network topology, including resource status, available ports, and link bandwidth usage.	The system supports minute-level network resource awareness. The system can detect the network status in seconds. Automatically generates the network topology, including the resource status, available ports, and link bandwidth usage.	

General Process	Ability	L0	L1	L2	L3	L4	L5
Analysis & Decision-Making.	Design the solution.	Manually allocate network resource parameters and manually formulate service solutions. Manually evaluate the design scheme. (e.g. whether user requirements are met, whether existing services are affected, and whether resources are met), provide the evaluation result, and confirm the final business solution.	Manually allocate network resource parameters and manually formulate service solutions. Manually evaluate the design scheme. (e.g. whether user requirements are met, whether existing services are affected, and whether resources are met) and provide the evaluation result and confirm the final business solution.	Network resource parameters are allocated by the system and service solutions are manually formulated. Manually evaluate the design scheme. (e.g. whether user requirements are met, whether existing services are affected and whether resources are met) Provide the evaluation result and confirm the final business solution.	When network resources (such as RDs, and RTs) are specified, the system automatically checks resource conflicts, precomputes paths for services, and evaluates the configuration. (for example, whether user requirements are met and whether resources are met).	The system automatically allocates network resources (such as RDs, and RTs) based on user intentions. The system automatically calculates and recommends optimal network paths based on user intentions, and automatically generates network device configurations. The solution is fully defined and tested in Digital Twin before the Execution.	
Execution.	Solution implementation and effect verification.	Manually deliver service configurations. Manually verify and confirm the service delivery result, including whether the service status meets the requirements.	Use the tool to deliver service configurations. Use the tool to verify and confirm the service delivery result, including whether the service status meets the requirements.	A operator triggers service configuration delivery through the system. The human-driven system verifies and confirms the service delivery result, including whether the service status meets requirements.	The system automatically delivers service configurations. After the service provisioning is complete, the system creates a detection instance and verifies and confirms the service delivery result, including whether the service status meets the requirements.	The system automatically delivers the service configuration. If the service configuration fails to be delivered, the system rolls back the service configuration. After the service provisioning is complete, the system automatically creates a detection instance and verifies and confirms the service delivery result, including whether the service status meets the requirements.	

6.3 Service provisioning in the operation phase: private line service provisioning

6.3.1 Function Requirement Overview

At present, under the tide of digital transformation, the cloud development of thousands of industries is in full swing. On an IP network, the controller will provide SRv6 technical capabilities, including SRv6 Policy and EVPN L3VPN. In converged construction, the IP network will provide simplified service input interfaces for a large number of services, automatically convert network parameters, and automatically deploy and verify services, achieving quick and intelligent service provisioning.

6.3.2 Process Task Definition

Figure 7 shows the general process task mapping for private line service provisioning. The details are as follows.

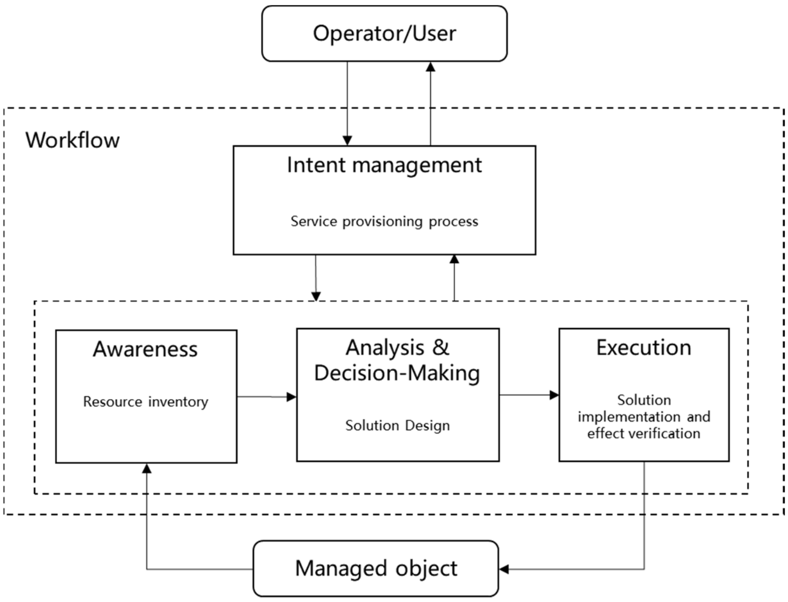

Figure 7: Private line service provisioning capability and task mapping

- **Intent management tasks:**
    - Planning personnel prepare service planning data, including PE planning, RD/RT planning, and network parameter configuration templates for built-in services in the management and control system, and automatically convert the data into network-layer bearer technologies (such as L3VPN) and protection requirements (HSB). VPN FRR, NE list, tunnel SRv6 policy, and SLA assurance parameters; In addition, the system automatically selects service assurance policies based on service intents (such as tunnel switchover, active/standby service switchover, and tunnel re-optimization).
- **Awareness tasks:**
    - Resource survey: Obtains network SLA monitoring data in real time, including latency, bandwidth, and traffic, and dynamically detects network changes. Dynamically obtains network device resources, idle ports, and link bandwidth, and dynamically detects network resource changes.
- **Analysis and decision-making tasks:**
    - Solution design: The management and control system automatically allocates resources, including VRF RD/RT, NE interface, and VLAN resources, and automatically generates service configurations and service assurance solutions.

- **Perform the following tasks:**

  - Solution implementation and effect verification: The system automatically delivers configurations based on the service solution. The management and control system automatically accepts services, tests whether the service status is normal, and verifies whether the service meets the requirements.

6.3.3 Classification requirements

Table 8 lists the technical requirements for the provisioning of intelligent-level classification for private line services.

Table 8: Requirements for the intelligent capability of provisioning private line services

General Process	Ability	L0	L1	L2	L3	L4	L5
Intention management.	Provisioning Intention Translation.	Translate the network configuration parameters of the service intent to the service.	Users completes the network configuration parameters from the service intent to the service. Translation of (such as bearer technology, protection requirements, NE list, and tunnel policy).	Users completes the network configuration parameters from the service intent to the service. (e.g. bearer technology, protection requirements, NE list, tunnel policy, etc.).	VPN service templates are preconfigured in the system. The system automatically converts the manually selected templates to network service configurations.	The system supports online and flexible service model definition. The system automatically converts user intentions into network configurations. (e.g. VPN configuration, interface configuration, protection configuration, tunnel policy, etc.).	In all scenarios, the system completes the intelligent closed-loop of the entire process, including requirement mapping, data sensing, analysis, decision-making, and execution, achieving full intelligence in all scenarios.
Awareness.	Resource survey.	Manually view and collect network status information, including resource status, available ports, link bandwidth, and service resource usage.	Operators can use tools to detect the network status, including the resource status, available ports, link bandwidth, and service resource usage.	The system detects the network status, including the resource status, available ports, link bandwidth, and service resource usage.	The system can detect network resource, service, and status changes within 15 minutes and automatically generate a network topology, including resource status, available ports, link bandwidth, and service resource usage.	The system supports minute-level network resource awareness utilizing Digital Twin. The system can detect the network resource status, network service status, and quality in seconds. Automatically generates the network topology, including the resource status, available ports, link bandwidth, and service resource usage.	

General Process	Ability	L0	L1	L2	L3	L4	L5
Analysis & Decision-Making.	Solution decision-making.	Manually allocate network resource parameters and manually formulate service solutions. Manually evaluate the design scheme. (e.g. whether user requirements are met, whether existing services are affected, and whether resources are met) and provide the evaluation result and confirm the final business solution.	Manually allocate network resource parameters and manually formulate service solutions. Manually evaluate the design scheme. (e.g. whether user requirements are met, whether existing services are affected, and whether resources are met) and provide the evaluation result and confirm the final business solution.	Network resource parameters are allocated by the system and service solutions are manually formulated. Manually evaluate the design scheme. (e.g. whether user requirements are met, whether existing services are affected, and whether resources are met), provide the evaluation result, and confirm the final business solution	When network resources, such as, RDs, and RTs are specified, the system automatically checks resource conflicts. The system automatically precomputes service paths and evaluates service configurations. (for example, whether user requirements are met and whether resources are met).	The system automatically allocates network resources (such as RDs, and RTs) based on user intentions. The system automatically calculates and recommends optimal network paths based on user intentions, and automatically generates network device configurations. The solution is fully defined and tested in Digital Twin before the Execution.	
Execution.	Solution implementation and effect verification.	Manually deliver service configurations. Manually verify and confirm the service delivery result, including whether the service status meets the requirements.	Use the tool to deliver service configurations. Use the tool to verify and confirm the service delivery result, including whether the service status meets the requirements.	A operator triggers service configuration delivery through the system. The human-driven system verifies and confirms the service delivery result, including whether the service status meets requirements.	The system automatically delivers the service configuration. After the service delivery is complete, the system automatically verifies and confirms the service delivery result, including whether the service status meets the requirements.	The system automatically delivers the service configuration. If the service configuration fails to be delivered, the system rolls back the service configuration. After the service delivery is complete, the system automatically verifies and confirms the service delivery result, including whether the service status meets the requirements.	

6.4 Monitoring and Troubleshooting in the Maintenance Process - Network Fault Analysis

6.4.1 Function Requirement Overview

To quickly detect service faults, improve root cause diagnosis efficiency, eliminate invalid dispatching, and implement service self-healing, service fault management should cover all fault detection, timely warning of potential network faults, automatic and intelligent fault diagnosis, and automatic service path recalculation.

6.4.2 Process Task Definition

Figure 8 shows the general process task mapping of the service fault analysis capability. The details are as follows.

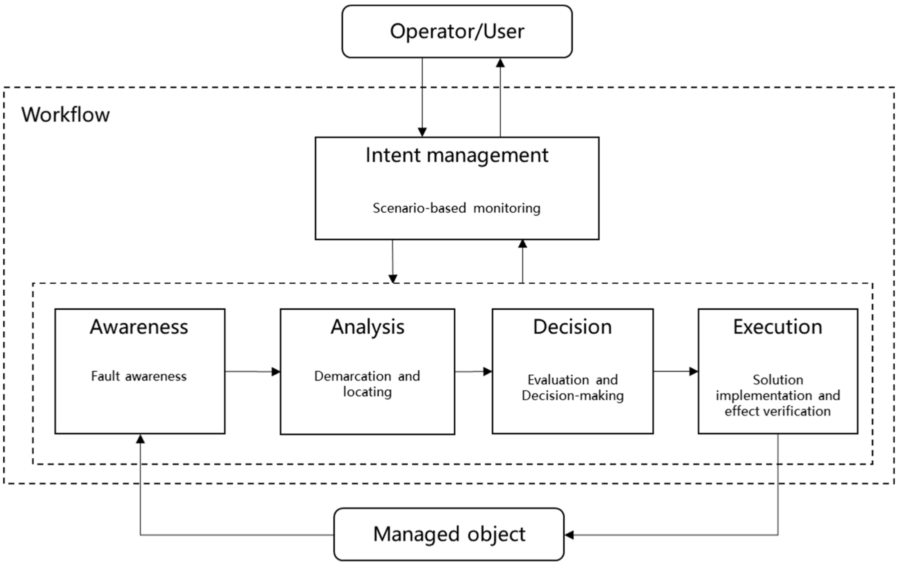

Figure 8: Service fault analysis capability and task mapping

- **Intent management tasks:**
  - Scenario-based monitoring: The system needs to understand the service monitoring and assurance intention and implement the fault analysis intention through the system processing logic.
- **Awareness tasks:**
  - Fault detection: Service monitoring is visible. After services are provisioned, the system automatically creates E2E SLA monitoring, service traffic monitoring, and status and traffic monitoring of network nodes and links on service paths. Service fault identification: The system automatically identifies network exceptions based on AI. Alarms are compressed and aggregated based on flow detection and AI, implementing automatic identification of massive service faults.
- **Analysis tasks:**
  - Demarcation and locating: The system automatically performs hop-by-hop diagnosis based on flow detection to quickly demarcate service faults, perform correlation analysis on service- and network-level problems, and automatically match fault modes to locate the smallest replaceable unit.
- **Decision-making tasks:**
  - Evaluation and decision-making: After detecting a service fault, the system automatically computes alternative paths online based on the path computation policy and service SLA requirements.

- **Perform the following tasks:**

    - Solution implementation and effect verification: The system supports one-click automatic service path adjustment. The system automatically completes service acceptance and checks whether the damaged services are recovered, including whether the service connectivity and SLA meet the requirements.

6.4.3 Classification requirements

Table 9 lists the technical requirements for service fault analysis capabilities.

Table 9: Requirements for service fault analysis capabilities

General Process	Ability	L0	L1	L2	L3	L4	L5
Intention management.	Fault analysis intention translation.	Translate the service fault analysis intention.	Translate the service fault analysis intention.	Translate the service fault analysis intention.	The system has built-in fault analysis correlation rules, which can be manually selected to match service fault analysis requirements.	The system displays the simplified intent externally. People only need to enter the service endpoint and SLA requirements, and the system automatically selects rules to match the service fault analysis requirements.	In all scenarios, the system completes the intelligent closed-loop management of the entire process, including requirement mapping, data sensing, analysis, decision-making, and execution, achieving full intelligence in all scenarios.
Awareness.	Fault awareness.	Manually create E2E SLA monitoring and service traffic monitoring for services. Manually view and collect network exceptions and alarms.	Operators use tools to create E2E SLA monitoring and service traffic monitoring. Manually view and collect network exceptions and alarms.	Operators can create E2E SLA monitoring and service traffic monitoring for services through the system. Users can use the system to identify network exceptions and alarm-based identification.	The system can detect the status and traffic of network nodes and links on service paths within 15 minutes or 24 hours. The system automatically identifies associated alarms.	The system can detect the service status in seconds and the status and traffic of network nodes and links on the service path in minutes. The system automatically identifies network exceptions. Compresses and aggregates alarms based on flow-based detection and AI to identify root faults.	
Analysis.	Service demarcation and locating.	Manually locate the minimum replaceable unit layer by layer hop by hop.	Manually locate the minimum replaceable unit layer by layer hop by hop.	The system is used to locate the fault layer by layer and manually locate the minimum replaceable unit.	Based on alarm information, the system can demarcate and locate faults in an end-to-end manner.	The system automatically performs hop-by-hop diagnosis based on flow detection, quickly demarcates service faults, matches fault modes based on rules, and automatically locates the smallest replaceable unit.	

General Process	Ability	L0	L1	L2	L3	L4	L5
Decision-making.	Evaluation Decision.	Manually allocate network resource parameters and manually formulate service solutions.	Manually allocate network resource parameters and manually formulate service solutions.	Based on the path computation policy and service SLA requirements, the system computes alternative paths.	After detecting a service fault, the system automatically computes alternative paths online based on the fault mode based on the path computation policy and service SLA requirements, and manually makes decisions on the alternative solutions.	After detecting a service fault, the system automatically computes alternative paths online based on the path computation policy and service SLA requirements based on the demarcation and locating results. The system automatically makes a decision based on the evaluation solution. The solution is fully defined and tested in Digital Twin before the Execution.	
Execution.	Solution implementation and service verification.	Manually deliver service configurations. Manually verify and confirm the service delivery result.	Use the tool to deliver services. Use the tool to verify and confirm the service delivery execution result.	A Operators triggers service path delivery through the system. Use the system to verify and confirm the service delivery execution result.	The system supports one-click automatic service path adjustment. Use the system to verify and confirm the service delivery execution result.	The system supports automatic service path adjustment. After the service provisioning is complete, the system automatically verifies and confirms the service delivery result, including the service connectivity and whether the SLA meets the requirements.	

6.5 Network Optimization - Real-Time Scheduling of IP Traffic

6.5.1 Function Requirement Overview

The IP network carries multiple services. The service quality should be continuously guaranteed. High-bandwidth services are not congested and delay-sensitive services are not degraded. Bandwidth monitoring should be implemented in real-time to predict potential risks. To improve service quality, IP flows are collected in real time, and optimization solutions should be customized for network bottlenecks. Traffic is diverted to tunnels for traffic optimization, implementing IP flow-based service assurance and improving user experience.

6.5.2 Process Task Definition

Figure 9 shows the general process task mapping of the real-time IP traffic scheduling capability.

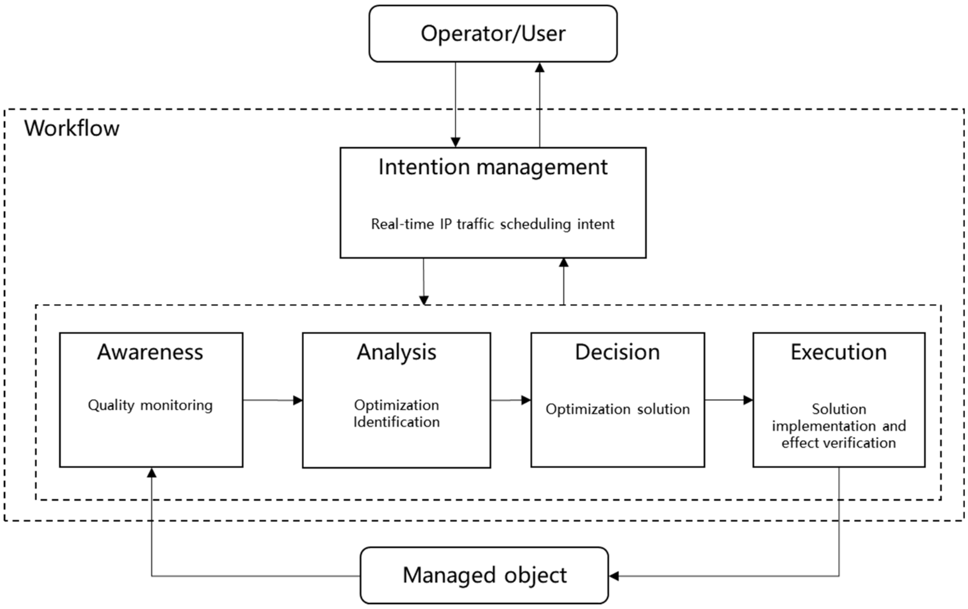

Figure 9: Mapping between the real-time IP traffic scheduling capability and tasks

- **Intent management tasks:**
  - Real-time IP traffic scheduling intention translation: Users need to understand the assurance intention of services carried by links. Users need to set thresholds, select prediction algorithm models, and set path computation constraints and traffic adjustment policies to complete the translation of the intention.
- **Awareness tasks:**
  - Quality monitoring: The system automatically collects network information such as IP traffic and status periodically to identify IP traffic performance.
- **Analysis tasks:**
  - Optimization identification: The system analyses the network traffic distribution based on the warning information or performance threshold-crossing information.
  - Demarcation and locating: Determine the links to be optimized based on the network popularity information, such as the traffic load on the egress links.
- **Decision-making tasks:**
  - Optimization solution: The system automatically computes paths based on path computation constraints, such as affinity attributes, cost values, and explicit paths, and provides a traffic optimization solution based on the traffic adjustment policy.

- **Perform the following tasks:**
  - Solution implementation and result verification: The system supports one-click traffic optimization and automatic rollback in case of exceptions. The system automatically verifies the link load after optimization, the traffic load status of the egress link after adjustment, and the SLA information of the service carried by the link.

6.5.3 Classification requirements

Table 10 lists the technical requirements for real-time IP traffic scheduling and intelligent-level classification.

Table 10: Requirements for the intelligent capability of real-time IP traffic scheduling

General Process	Ability	L0	L1	L2	L3	L4	L5
Intent management.	Traffic Optimization Intention Translation.	Translate the traffic optimization intention.	Translate the traffic optimization intention.	Translate the traffic optimization intention.	Traffic optimization correlation rules are preconfigured in the system. Rules can be manually selected to match traffic optimization requirements.	The system displays the simplified intent and automatically selects rules to match traffic optimization requirements.	In all scenarios, the system completes the intelligent closed-loop management of the entire process, including requirement mapping, data sensing, analysis, decision-making, and execution, achieving complete intelligence in all scenarios.
Awareness.	Quality monitoring.	Manually collect network information, such as the egress link bandwidth and port status.	Use the tool to collect network information such as egress link bandwidth and port status.	Operators collect network information such as egress link bandwidth and port status through the system.	The system can collect network information such as egress link traffic, bandwidth, and link status within 15 minutes.	The system can process network information such as egress link traffic, bandwidth, and link status in minutes.	
Analysis.	Optimization Identification.	Manually try repeatedly to find the link to be optimized.	Manually try repeatedly to find the link to be optimized.	Operators can analyse the egress link traffic load and manually identify the links to be optimized.	The system analyses the performance threshold-crossing information, network traffic distribution, and egress link load based on rules in 15 minutes, and automatically identifies links to be optimized.	The system automatically analyses the performance threshold-crossing information, network traffic distribution, and egress link load in minutes, and automatically identifies links to be optimized.	
Decision-making.	Optimization solution.	Manually evaluate the solution and confirm the final optimization solution.	Manually evaluate the optimization solution and confirm the final optimization solution.	Based on the path computation policy and service SLA requirements, the system planning department optimizes the solution.	The system evaluates the solution online based on the collected data, provides the evaluation result, and manually determines the optimization solution.	Based on real-time data, the system evaluates the solution online, provides the evaluation result, and automatically determines the optimization solution. The solution is fully defined and tested in Digital Twin before the Execution.	

General Process	Ability	L0	L1	L2	L3	L4	L5
Execution.	Solution implementation.	Manually deliver and verify the optimization configuration.	Use the tool to deliver and verify the optimization configuration.	The system triggers optimization configuration delivery and verification.	The system uses the management protocol to deliver configurations to complete traffic optimization. Rollback upon failure is supported. Use the system to verify and confirm the optimization results, for example, whether the traffic load on the egress link meets the requirements.	The system can use the control protocol to deliver routing policies to complete traffic optimization. After the egress link optimization is complete, the system automatically verifies and confirms the optimization result, for example, whether the traffic load on the egress link meets the requirements.	

6.6 Optimization Phase Network Optimization - IP Network Path Optimization

6.6.1 Function Requirement Overview

The IP network carries different services, and the SLA for each service is different. To ensure the quality of services carried on IP networks, ensure that the delay, bandwidth, and packet loss rate do not deteriorate. Therefore, the bandwidth should be monitored in real time to predict potential risks. When IP network services are sensitive to delay, bandwidth, and packet loss rate, the IP network needs to be optimized accordingly. SR-TE/SRv6 Policy TE tunnel optimization is triggered to ensure service optimization and improve user experience.

6.6.2 Process Task Definition

Figure 10 shows the task mapping in the general process of optimizing the TE tunnel capability on an IP network. The details are as follows.

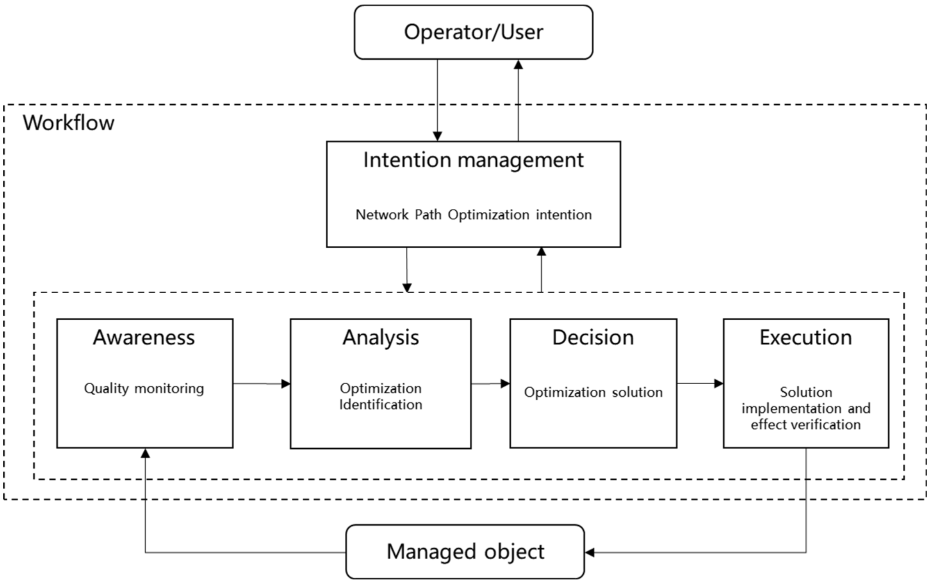

Figure 10: Mapping between IP network path optimization capabilities and tasks

- **Intent management tasks:**
  - Network path optimization intention translation: To understand the assurance intention for services carried by the IP network, a person need to set thresholds, select prediction algorithm models, and set path computation constraints and traffic adjustment policies to complete the translation of the intention.
- **Awareness tasks:**
  - Quality monitoring: The system automatically collects network information such as TE tunnel bandwidth, delay, and port status.
- **Analysis tasks:**
  - Optimization identification: The system analyses the network traffic distribution based on the warning information or the delay, bandwidth, and packet loss rate threshold-crossing information, analyses the delay, bandwidth, and packet loss rate requirements of service traffic, and determines the TE tunnels to be optimized.

- **Decision-making tasks:**
  - Optimization solution: The system automatically computes paths based on path computation constraints, such as affinity attributes, cost values, and explicit paths, and provides a TE tunnel optimization solution based on the delay, bandwidth, and packet loss rate requirements. There should not be any manual intervention.

- **Perform the following tasks:**
  - Solution implementation and effect verification: The system supports one-click optimization of latency, bandwidth, and packet loss rate, and automatic rollback in case of exceptions. The system automatically verifies the delay of the traffic after optimization. After adjustment, the traffic is transmitted over the TE tunnel that meets the delay, bandwidth, and packet loss ratio requirements and meets the SLA information of the service.

6.6.3 Classification requirements

Table 11 lists the technical requirements for network path optimization.

Table 11: Requirements for network path optimization capabilities

General Process	Ability	L0	L1	L2	L3	L4	L5
Intent management.	Network Path Optimization Intention.	Translate the delay, bandwidth, and packet loss rate optimization intentions.	Translate the delay, bandwidth, and packet loss rate optimization intentions.	Translate the delay, bandwidth, and packet loss rate optimization intentions.	The system has built-in optimization correlation rules. Rules can be manually selected to match optimization requirements (latency, bandwidth, and packet loss rate).	The system displays the simplified intention externally and automatically selects rules to match the optimization intention (latency, bandwidth, and packet loss rate).	In all scenarios, the system completes the intelligent closed-loop of the entire process, including requirement mapping, data sensing, analysis, decision-making, and execution, achieving full intelligence in all scenarios.
Awareness.	Quality monitoring.	Manually collect network information such as TE tunnel bandwidth, delay, and port status.	Use a tool to collect network information such as TE tunnel bandwidth, delay, and port status.	The system collects network information such as TE tunnel bandwidth, delay, and port status.	The system automatically detects the delay, packet loss rate, port status changes, and link and tunnel traffic changes in minutes.	The system automatically detects the delay, packet loss rate, and port status changes in seconds, and detects the link and tunnel traffic changes in minutes.	
Analysis.	Optimization Identification.	Manually analyse the TE tunnels to be optimized.	Manually analyse the TE tunnels to be optimized.	Use the system to analyse the TE tunnels to be optimized.	The system analyses indicators such as delay and bandwidth threshold-crossing information and network traffic distribution based on rules, and automatically identifies TE tunnels to be optimized in hours.	The system analyses parameters from multiple dimensions, including the delay, bandwidth, and packet loss rate threshold-crossing information and network traffic distribution, and automatically identifies TE tunnels to be optimized in minutes.	
Decision-making.	Optimization Scheme.	Manually evaluate the optimization solution and confirm the final optimization solution.	Manually evaluate the optimization solution and confirm the final optimization solution.	Use the system to evaluate the optimization solution and confirm the final optimization solution.	The system evaluates the optimization solution online based on the collected data and manually provides the evaluation result and final optimization solution.	Based on real-time data, the system automatically provides the evaluation result and optimization solution. The solution is fully defined and tested in Digital Twin before the Execution.	

General Process	Ability	L0	L1	L2	L3	L4	L5
Execution.	Solution implementation and effect verification.	Manually deliver optimization configurations. Manually verify and confirm the optimization results.	Use the tool to deliver the optimization configuration. Use the tool to verify and confirm the optimization results.	Operators uses the system to trigger the delivery of optimization configurations. Use the system to verify and confirm the optimization results.	The system supports automatic traffic adjustment. Use the system to verify and confirm the optimization results.	The system automatically adjusts paths in seconds. Traffic is not interrupted and no packet loss occurs during the optimization. After the optimization is complete, the system automatically verifies and confirms the optimization results, including the traffic volume of the TE tunnel and whether the SLA meets the requirements.	

6.7 Optimization: Network Optimization - Network Energy Saving Optimization

6.7.1 Function Requirement Overview

The IP network carries multiple types of services, which are carried by devices such as routers. Traditional network management systems mainly monitor alarms and performance and are weak in monitoring and managing network device power consumption. They lack the analysis of power consumption effectiveness and cannot effectively schedule network power consumption. Device managers cannot effectively monitor the energy consumption of devices on the entire network in real-time and analyse data in depth. It is difficult to formulate and implement network energy-saving optimization policies. Provides visualized, manageable, and optimized power consumption of IP networks, continuously improving network energy conservation and emission reduction, and achieving energy conservation and emission reduction goals.

6.7.2 Process Task Definition

Figure 11 shows the task mapping in the general process of the energy saving capability of the IP network. The details are as follows.

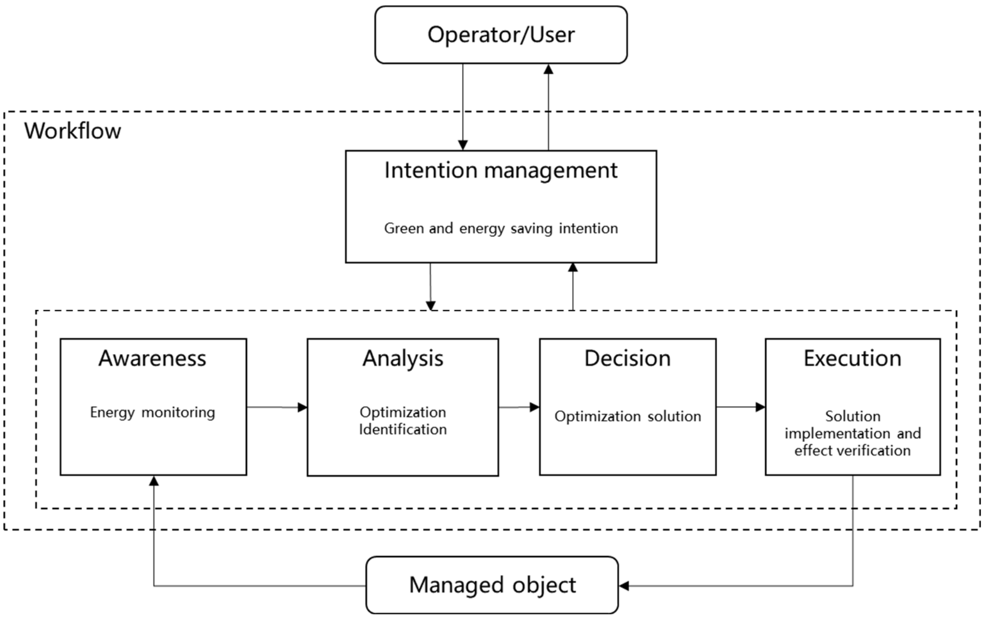

Figure 11: Energy-saving process of the IP network

- **Intent management tasks:**
  - Green energy saving intention: Operators need to understand the green energy saving intention on the IP network and translate the intention by setting energy saving policies.
- **Awareness tasks:**
  - Energy monitoring: The system collects the energy consumption of devices and networks by detecting the energy consumption of devices.
- **Analysis tasks:**
  - Optimization identification: Collect the actual energy consumption saved by network devices and draw the energy-saving benefit curve. Ensure that the energy-saving benefits of equipment can be evaluated and the energy saving effect can be quantified.

- **Decision-making tasks:**
  - Optimization solution: The system can discover the most profitable energy-saving resources, improving the efficiency of policy formulation. The utilization of Digital Twin simulation is essential in this phase.
- **Perform the following tasks:**
  - Solution implementation: Network-level energy-saving policies are deployed based on the NETCONF/Yang technology. One-click energy-saving policies can be applied to multiple devices, providing convenient and smooth energy-saving policy delivery experience. In addition, the system updates the energy-saving status of devices in real-time, automatically saves energy, and provides analysis reports.

6.7.3 Classification requirements

Table 12 lists the technical requirements for green and energy-saving intelligent horizontal classification.

Table 12: Requirements for green and energy-saving intelligent capabilities

General Process	Ability	L0	L1	L2	L3	L4	L5
Intention management.	Green and energy-saving intention.	Operators complete the translation of green energy saving intentions.	Operators complete the translation of green energy saving intentions.	Operators complete the translation of green energy saving intentions.	The system has built-in associated rules for energy saving, and the rules can be manually selected to match the energy-saving requirements.	The system displays the simplified intent and automatically matches the green and energy-saving policy.	In all scenarios, the system completes the intelligent closed-loop management of the entire process, including requirement mapping, data sensing, analysis, decision-making, and execution, achieving complete intelligence in all scenarios.
Awareness.	Quality monitoring.	None.	None.	Operators collect information such as equipment energy consumption through the system.	The system supports hour-level power consumption monitoring instances and automatically collects device power consumption information by hour.	The system supports minute-level power consumption monitoring instances and collects device and board power consumption information in real-time.	
Analysis.	Optimization Identification.	Manually identify high energy consumption devices.	Manually identify high energy consumption devices.	Operators analyse energy consumption and demarcate high energy consumption devices through the system.	The system analyses the energy consumption based on the rules and automatically demarcates the devices with high energy consumption.	The system analyses the energy consumption based on the rules and automatically demarcates the devices with high energy consumption.	
Decision-making.	Decision-making on energy saving solutions.	Manually evaluate the solution and confirm the final energy saving solution.	Manually evaluate the solution and confirm the final energy saving solution.	Manually evaluate the solution and confirm the final energy saving solution.	Based on the collected data, the system automatically evaluates the green energy saving solution online, providing a basis for formulating optimization solutions.	Based on the collected data, the system automatically evaluates the green energy saving solution online and generates energy-saving policies based on the evaluation results. The solution is fully defined and tested in Digital Twin before the Execution.	

General Process	Ability	L0	L1	L2	L3	L4	L5
Execution.	Solution implementation and result verification.	Manually deliver energy-saving configurations. Verify and confirm the manual energy saving results.	Use the tool to deliver energy-saving configurations. Use tools to verify and confirm the energy-saving results.	The system triggers the delivery of energy-saving configurations. Operators use the system to verify and confirm the energy saving results.	The system can automatically deliver energy-saving policies. Operators use the system to verify and confirm the energy saving results.	The system can automatically deliver the green energy-saving policy. The system automatically verifies and confirms the energy-saving result after the energy-saving is complete.	

7 Conclusions

Based on the general framework of network management and operation autonomous level classification in ETSI GR ENI 007 [i.2], the intelligent level of each phase of the entire life cycle of IP network O&M can be evaluated by breaking down the workflow into tasks and then evaluating the intelligent level of each tasks.

Clause 5 provides the autonomous level of IP network throughout the network lifecycle, which gives the evolution direction of autonomy, while clause 6 defines the specific autonomous level of some typical IP network services and network operation scenarios, such as 5G bearer, private line services, fault analysis, IP traffic optimization, and energy saving scenarios, highlighting the requirements to reach Level 3 and Level 4 autonomicity.

Based on the analysis and evaluation of identified typical use cases, the autonomous level of some IP network management and operation functions is close to or already reached Level 3. Defining the level of intelligence in network management and operation help the industry to reach a consensus on the way forward and objectives. It will lead to promote more active investment in technology introduction by the whole industry, especially by operators and equipment providers, helping to fully reach Level 4 autonomicity.

History

Document history		
V4.1.1	December 2023	Publication