ETSI GR ENI 049 V4.1.1 (2025-05)

Experiential Networked Intelligence (ENI); Definition of Data Centre Networks autonomic 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-0049v411_def_DCNAL

Keywords
6G, closed control loop, data centres, GenAI, LLM, native AI

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

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 defines network autonomous features and levels for Data centre networks, including the intelligent characteristics at each layer (from Level 1 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.3] and ETSI GR ENI 010 [i.4]:
  - Data centre 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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] TM Forum IG1230: "Autonomous Network Technical Architecture".

[i.2] ETSI GR ENI 004: "Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI".

[i.3] ETSI GR ENI 007: "Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks".

[i.4] ETSI GR ENI 010: "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 given in ETSI GR ENI 004 [i.2] and the following apply:

application fault management: alarm monitoring, correlation, and troubleshooting for connectivity related to data centre applications

autonomous networks: set of self-governing programmable and explainable systems that seamlessly deliver secure, context-aware, business-driven services

NOTE: These services are created and maintained using model-driven engineering and administered by using policies.

Availability Zone (AZ): set of one or more physical data centres

NOTE: Multiple AZs with independent geographical locations, power, and networks are created in a region. AZs are connected through low-latency networks. Each AZ is not affected by faults in other AZs.

deployment unit Point Of Delivery (POD): minimum equipment unit connected to the data centre network

NOTE: It consists of switches, routers, firewalls, load balancers, and servers, etc. to provide network services and applications. A POD refers to a physical area connected to a service distribution network.

evaluation dimension: viewpoint that can be divided into five dimensions such as ManMachine Interface, Decision Making Participation, Data Collection and Analysis, Degree of Intelligence and Environmental Adaptability

NOTE: As defined in ETSI GR ENI 007 [i.3].

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

network digital map: basic function of the network digital twin and physical network in operation

NOTE: Topology Models and associates resource model data to provide data centre applications and network topology association for the network digital twin, supporting network intent management and display.

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

region: collection of resources divided by the geographical location of a data centre

NOTE: Users can be authorized by region. AZs in the same region can communicate with each other over the intranet, but not between different regions. A country can be geographically divided into different regions and regions can be selected based on the service proximity principle.

subsystem: network element, management system, network platform

technical expert: person in charge of defining or supporting Operational Procedures within a CSP Network

NOTE: This person is in charge of Capacity Planning, Engineering, Designing, and Troubleshooting.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR ENI 004 [i.2], ETSI GR ENI 007 [i.3] and the following apply:

AI	Artificial Intelligence
DC	Data Centre
DC-GW	Data Centre Gateway
DCN	Data Centre Network
KPI	Key Performance Indicator
RMA	Return Material Authorization
SLA	Service Level Agreement
VPC	Virtual Private Cloud

4 Concept and Method for Autonomicity Classification targeting Data centre Network Operation and Management

Referring to ETSI GR ENI 010 [i.4], and the TMF autonomous network technical architecture [i.1], the Data Centre Network (DCN) 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 and system).

The goal of the DCN autonomous mode of operation is to reduce and eliminate manual operations on the network gradually. Customers can gradually evolve into a fully automated and autonomous data centre network by defining autonomous capabilities. Network automation and intelligent technologies are key enabling technologies of the autonomous network.

DCN lifecycle management service, generally includes planning and construction, network operations, monitoring and O&M, and optimization. Table 1 describes the DCN autonomous classification Levels.

Table 1: Overview of DCN Autonomous Classification Levels

L1-L5 Level	Level Definition Description
L1 Phase - Manual Management	• All network operation management processes are completed manually and rely heavily on human experience. The efficiency is closely related to human capabilities and experience. • Network management and O&M knowledge accumulation rely on document sharing and human communication, which is low in efficiency and high in learning costs.
L2 Phase - Tool Management	• Some network operations introduce specific tools to improve productivity in the field. Typical tools include the configuration automation tool and the traffic collection and analysis tool. The efficiency is improved. • Network planning and design requires personnel to participate in network design and configuration audit, resulting in low efficiency.
L3 Phase - Automatic Network Management	• Network management systems have network automation capabilities throughout the lifecycle management of network operation. • These systems generally deliver automation.
L4 Phase - Intelligent Network Management	• In some network operation scenarios, network management systems can provide autonomous capabilities. • The autonomous systems provide user-friendly intent-based interface, more reliable due to pre-test, post-checks, and validation.
L5 Phase - Intelligent Network Management	• The autonomous system is fully independent in all service scenarios and people are normally outside of the process. No details will be present in the following Classification Requirement tables.

5 Autonomous Workflow for Data centre Network Operation and Management

The DCN of a large organization generally includes multiple data centres across multiple geographic regions. To support modular management of each data centre, Point of Delivery (POD) as a specific point of delivery or service point, is designed to group devices to support specific workloads or services. From a functional point of view, these PODs can be further classified into service PODs, access PODs (Internet access PODs, external access PODs, wide area access PODs), and transit PODs. These intra-POD and inter-POD interconnection networks are large-scale and complex. Therefore, autonomous network capabilities are needed to improve automatic management.

When an application encounters problems of poor network quality, joint analysis and diagnosis by the application and network departments are often required. Since the application department's operation and maintenance system usually cannot see the network information, the network management software cannot see the application information either. The two systems operate independently, and data is isolated, resulting in a lack of global perspective and low efficiency in application network monitoring and insurance. Thus application quality assurance is also a key requirement for DCN autonomous networks.

General network lifecycle management includes network planning, network construction, network maintenance, network optimization, and network operation. In the case of DCNs, the typical network design scenario is POD planning and construction. For O&M, the DCN requires not only network management automation, and also fast application deployment and application quality assurance.

Regarding network management processes, each process can be further divided into five general network service task phases, including intent, perception, analysis, decision-making, and execution.

Data Centre Autonomous Networks perform five tasks of common network services at each managed service stage throughout its lifecycle, as described in Figure 1:

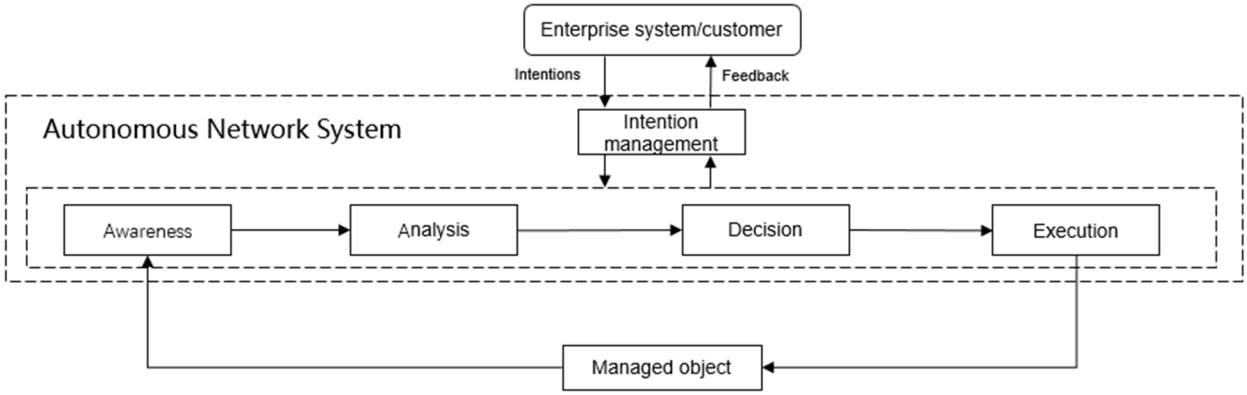

Figure 1: 5 Common Task Phases for Network Services

- **Intent management:** Understands customers' service and management intents and translates them into specific network configurations and policies. Intent management supports low-level traditional functions, such as coordinating any required orchestration of configuration operations on the network. It also supports higher-level abstraction and open modifiable capabilities, allowing customers to adjust solutions based on actual networking. Intent management also includes the full record of the business intent operation process, which can be traced and queried.

- **Awareness:** Monitors data centre network in real-time to detect network service exceptions or SLA problems, and triggers network analysis and location. Collects original network data and preprocesses the data (such as data cleaning, enhancement, and statistics collection) to monitor and perceive network information (including network performance, network exceptions, and network events) and the purpose of visual presentation.

- **Analysis:** Analyses the current data centre network status and network analysis based on historical data and customer intents, and generates operation actions, execution policy options, and suggestions that can meet customer intents.

- **Decision-making:** Reviews the operation options or suggestions provided by the process to determine the executable network operations and policies that meet the customer's intent requirements.

- **Execution:** Generates executable network operations and policies based on the customer intents that have been decided, automatically implements the network operations and policies deployed on the production network of the data centre, and verifies the network intents after the network implementation.

6 Network Service Scenarios and Autonomous Network Classification Recommendations

6.1 Overview

The present document defines the scenarios and requirements for data centre network autonomous in terms of network design and provisioning, network service automation, network troubleshooting, and optimization. According to network deployment practices, these scenarios need to be defined first.

6.2 Network Design and Provisioning - DC POD Planning and Deployment

6.2.1 Function Requirement Overview

Racks are deployed in the POD to install servers, storage, network devices (such as switches, routers, and load balancers), and power supplies, etc.

POD involves many types of devices. Manual design and deployment of PODs are inefficient and error-prone. Automatic POD deployment improves the overall efficiency by supporting the E2E automation of design, rollout, and configuration.

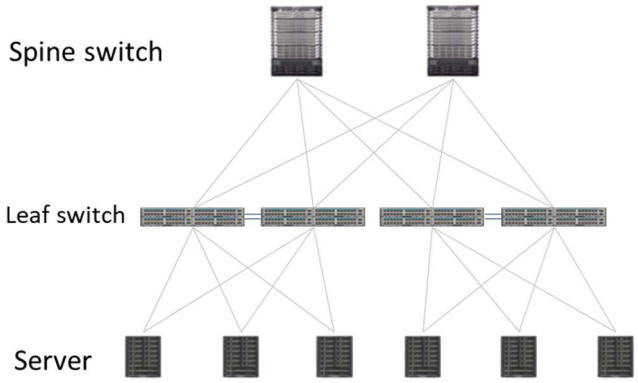

Figure 2: POD network example

6.2.2 Workflow Process and Task Definition

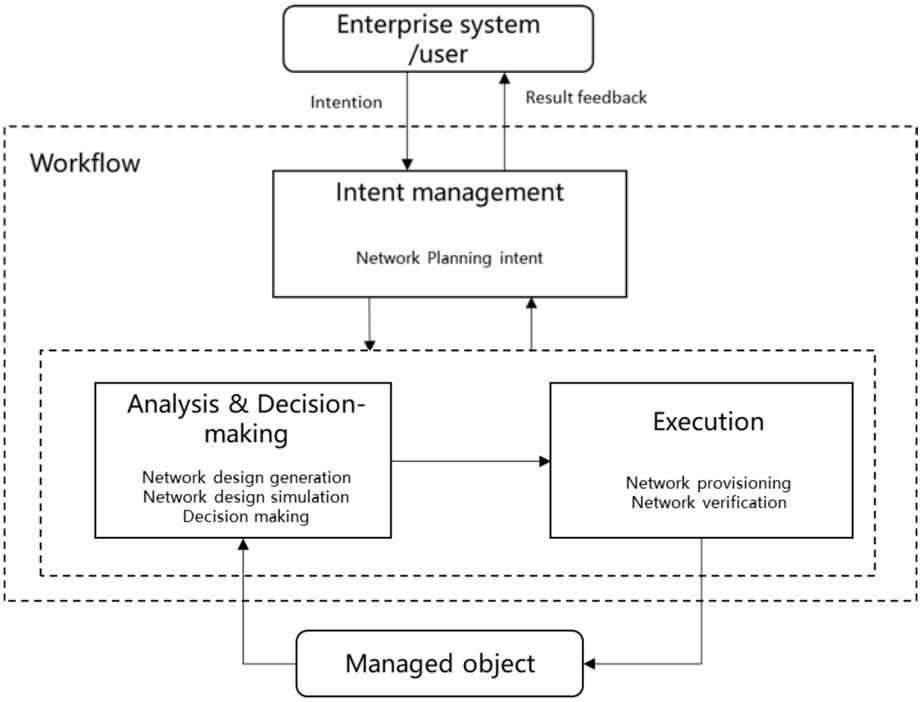

Figure 3: POD network design and provisioning process

The DC POD design, and provisioning process is shown in Figure 3, including intent, analysis, decision-making, and execution. The detailed management tasks are as follows:

a) **Intent management tasks:**

POD design intent: the system supports the following design input:

1) Network capacity: number of spine and leaf switches, etc.
2) IP address space management.
3) Network security requirements, including the firewall.

b) **Analysis/decision-making task:**

Network design and configuration generation for the planned network, the system supports the following capabilities:

1) Networking topology design: including the network interconnection topology, NE types, NE roles, and link connections.
2) Network address resources allocation: including IP networks and addresses, VRFs, and VLANs ranges.
3) Network routing protocol configuration: including BGP, OSPF, and ISIS configuration.
4) Interface configuration, such as IP address configuration and VLAN configuration.
5) Service access configuration, such as Layer 2 broadcast domain configuration and Layer 3 gateway configuration.
6) Reliability configuration.

Network simulation and decision-making: The system supports simulation and verifies the planned network connectivity, including IP reachability, route conflict, route black hole, route loop, and protocol configuration.

c) **Execution tasks:**

Network Provision: After the hardware installation engineers complete the infrastructure installation according to the planned network, the system starts the network provisioning automatically.

Network verification: The system supports automatically observing the network health status for the new PODs and creates reports, verifies the IP reachability and routing protocol consistency of the entire network and output the verification results in a visualized manner.

6.2.3 Classification requirements

Table 2: Requirements for DC POD planning and provisioning

General Process	Capability	L1	L2	L3	L4
Intent management	POD Requirement analysis	Manually analyse planning requirements.	Manually analyse planning requirements.	The system supports preconfigured template to input the network design scheme. (e.g. device model, board type, topology connection, and protocols).	The system supports the POD design intent input, including the network capacity, IP addresses space, and security requirements.
Analysis/ Decision-making	Network design generation	Manually generating a network design scheme.	Manually generating a network design scheme.	Based on the templates, the system automatically generates the network topology scheme and recommended network configurations. The configuration parameters can be manually adjusted.	Based on the POD design intent, the system automatically recommends the POD network design and generates the recommended network configuration.
	Network simulation & decision-making	Manually verify the network design and configuration solution.	Manually verify the network design and configuration based on expert experience.	Manually verify system design and configuration problems based on tools and make solution decisions.	The system supports near real time within minutes in one-click simulation verification to avoid network exceptions, such as routing loops and IP address conflicts. The system supports the digital twin function, which facilitates manual decision-making and allows manual modification of network configuration solutions.

General Process	Capability	L1	L2	L3	L4
Execution	Configuration / provisioning	Manual configuration implementation.	Manually use tools such as Ansible and Python scripts to deliver configurations.	The system automatically fulfils the configuration. And the configuration can be customized.	The system supports automatic device configuration with zero-touch deployment, and plug-and-play.
	Verification	Manual test and verification.	Manual test and verification.	The system automatically verifies that the data plane is reachable and generates a network-wide reachability acceptance report.	The system supports automatic verification, including network health verification, data plane reachability and protocol connectivity, scheduled and periodic automatic acceptance (verifying connectivity between any device), and network security risk verification. The system supports digital twin verification.

6.3 Network Service Automation - Application Rollout and Provisioning

6.3.1 Function Requirement Overview

The number of enterprise applications increases as the enterprise needs to grow and the application release cycle is shortened from weeks to days. However traditional network O&M management is more network-centric and focuses on network IP management, routing protocols, policy configuration, and fault monitoring instead of application-centric. To prioritize applications across networks, automatic application rollout and provisioning is a process of automatically configuring, and optimizing networks and devices based on the application requirements to provide new services.

6.3.2 Workflow Process and Task Definition

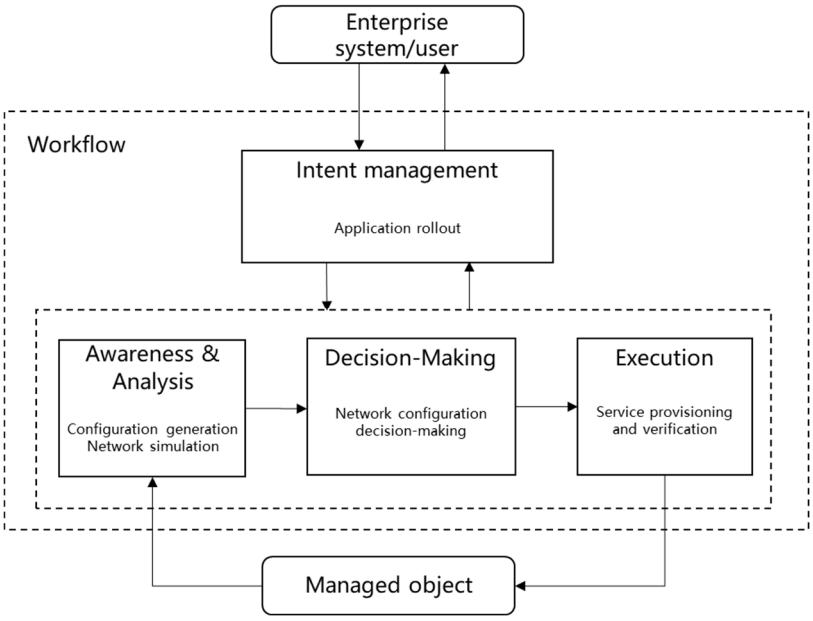

Figure 4: Application rollout and provisioning process

The general workflow of application rollout and provisioning consists of four tasks: intent, awareness and analysis, decision-making, and execution. The detailed management tasks are as follows:

a) **Intent management tasks:**

Intent management has two types of processes, aimed to create the template of the network configuration for each application and to install it in live network respectively:

1) **Network configuration requirements for application deployment:** This type of intent represents a low-level configuration template. After the application deployment requirements are manually translated into network requirements, the system supports Virtual Private Cloud (VPC) network configuration templates, including logical/virtual router, logical/virtual switch, logical/virtual firewall, external zone, and peering configuration, as shown in Figure 5.

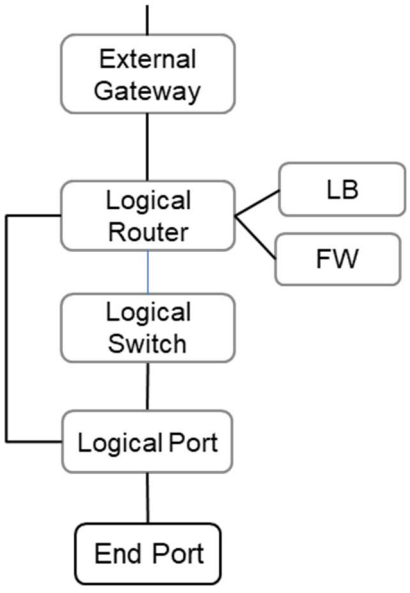

Figure 5: VPC creation example

2) **Application rollout and provisioning intent:** This type of intent represents a high-level declarative goal. Since data centres need to support a large number of application instances, and application instance rollout is a common network operation. The system supports application instance's rollout intent requirements which include the services information, service dependencies, and security zone requirements of the application. The security zone requirements have to meet the security compliance requirements when an application is brought online, so that the application can communicate with public services and other applications. For application rollout, some applications need to create new VPC instance. On the other side, an analysis can determine that an existing VPC instance can be reused. In any case, there will be additional requirements for routing and security policies.

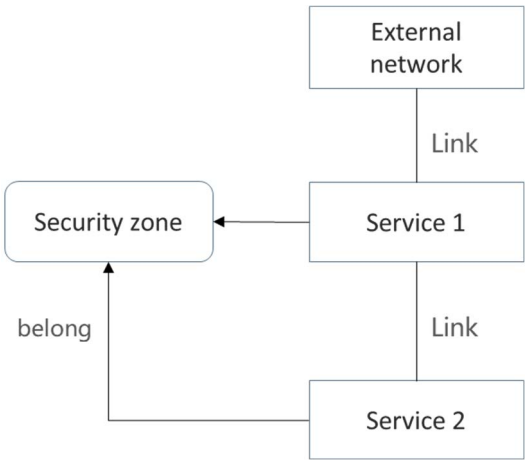

Figure 6: Application instance Rollout Example

b) **Awareness/analysis/decision-making tasks:**

Network configuration generation: Based on the two types of intents, and logical resource information (e.g. IP addresses, VLANs) and configuration information (e.g. VPN configuration, VXLAN configuration) collected from the network, the system supports generating device configurations that meet network requirements, including:

1) VPN Configuration, including VRF RT/RD (Route Target / Route Distinguisher)

2) VXLAN Configuration

3) Layer 2 broadcast domain configuration (including VLAN and VXLAN)

4) Inter-VPN routing configuration

5) Reliability configuration

6) Security policies configuration

Network configuration pre-verification: The system supports verifying the impact of network configurations on the network.

Decision-making: The system supports decision-making with the assistance of a network digital twin. Any possible conflicts will be solved according to the priority of the request. In case of show stopper the process will be interrupted. The user will get notified of the compromise and eventually will be asked for confirmation or for more information to be able to continue the deployment

c) **Execution tasks:**

Solution implementation, validation, and visibility:

1) The system supports the network configurations that can be provisioned on the network.

2) The system supports verifying and displaying the network updates after service provisioning.

6.3.3 Classification requirements

Table 3: Requirements for Application Rollout and Provisioning

General Process	Capability	L1	L2	L3	L4
Intent management	Application launch intent management	Manually process the service provisioning requirements and convert the requirements into network requirements.	Manually process the service provisioning requirements and convert the requirements into network requirements by using tools.	The system supports the network creation template required for service deployment and allows users to enter the network configuration requirements (e.g. VPC configuration) for application deployment.	The system supports the input of the application provisioning intent and translates the service provisioning intent into detailed network requirements.
Perception/ Analysis/ Decision-making	The solution Generated	Manually analyse live network resources, generate network task solutions, evaluate impact, and make decisions.	Manually analyse live network resources, generate network task solutions, evaluate impact, and make decisions.	The system supports automatic recommendation of network provisioning, such as VPC network interconnection. The system supports automatic analysis of the impact of the existing network connectivity and automatic simulation verification of the newly configured network connectivity. Manual decision-making.	The system supports automatic recommendation of network configuration for application provisioning, for example, VPC configuration and VPC interconnection. The system supports the one-click simulation of application rollout intents in seconds to verify the impact of application deployment, including routing loops and IP address conflicts. The system supports the preceding functions with a digital twin interactive interface to assist decision-making.

General Process	Capability	L1	L2	L3	L4
Execution	The solution Implementation	Manual configuration implementation.	Manually configure the implementation tool (such as Ansible) and script (such as Python).	The system supports automatic delivery of network configurations in the generated solution.	The system supports automatic delivery of network configurations in the application intent generation solution. The system supports multi-level configuration rollback, including tenant-, network-, and service-level configuration rollback. The system supports the one-click rollback of customer decision-making.
Verification	Verification	Manually verify the data.	Manual verification using tools.	The system supports automatic network health verification (including the network, device, and protocol). The system supports automatic snapshots before and after the service configuration network, and the comparison and visualization acceptance.	On the L3 basis, The system supports security risk verification. The system supports the monitoring of service protection, including the end-to-end service path, application interaction, and application quality. The system supports the preceding verification with digital twin verification.

6.4 Network Monitoring and Troubleshooting

6.4.1 Function Requirement Overview

To quickly detect data centre network and application faults, improve root cause diagnosis efficiency, eliminate invalid dispatching, and implement service self-healing, the network IP manager has to detect all the faults, to timely warning of potential network risks, to perform automate and intelligent fault diagnosis, and to handle service fault automatically.

6.4.2 Workflow Process and Task Definition

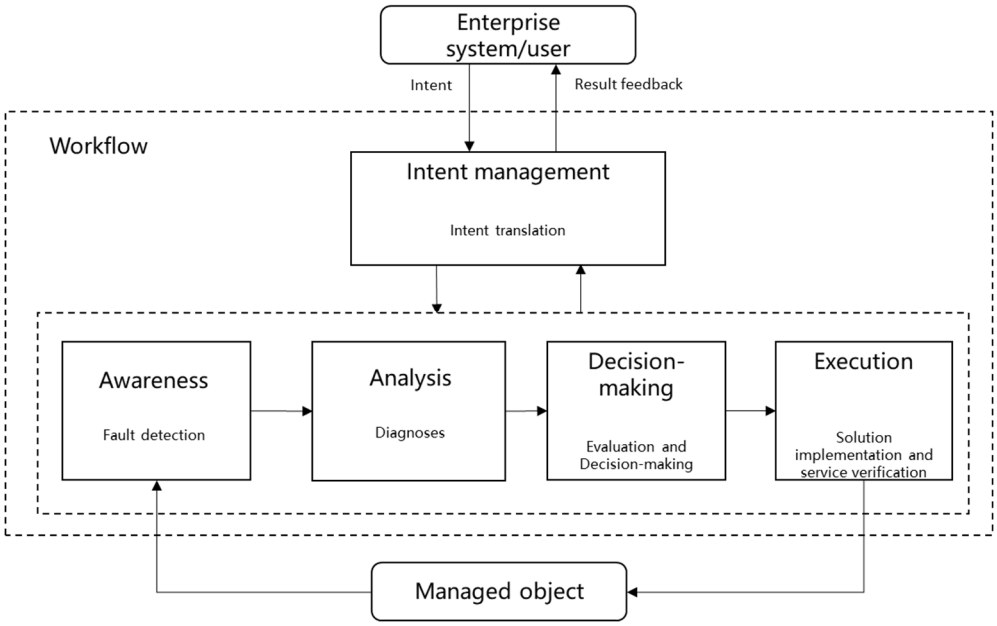

Figure 7: Network and Application Monitoring and Troubleshooting Tasks Process

The network monitoring and troubleshooting process consists of five general tasks: intent management, awareness, analysis, decision-making, and execution. The detailed management tasks are as follows:

a) **Intent management tasks:**

Network and application fault monitoring: The system supports automatic fault detection of networks and applications.

b) **Awareness tasks:**

The system supports network fault detection and potential risk monitoring in real-time and periodically:

1) Network status monitoring: Network Element (NE), link, port, card, NE role, and NE configuration.

2) Network alarm monitoring: network alarms, network protocol status, CPU/memory performance indicators, and logs.

3) Network quality monitoring: network port traffic statistics, packet loss, delay, bandwidth, and throughput.

4) Network logical resource monitoring: such as IP addresses, ACLs, VRFs, VLANs and VXLANs.

5) Network traffic monitoring: network traffic between IP pairs, packet loss rate based on IP pairs, and delay.

6) Network health monitoring: including NEs (including the CPU, memory, forwarding entries, interfaces, and links) and protocols (including BGP and VPN).

7) Network risk monitoring: NE reliability, performance load, capacity, risks, and protocol consistency risks.

8) Application Monitoring: Application flow performance (latency, packet loss rate, throughput, retransmission rate, connection setup duration), application workload (session numbers, number of connections, and packet rate), and application exceptions (connection failure, timeout, packet loss, etc.).

c) **Analysis tasks:**

Fault identification and potential risk prediction: the system monitors network and application traffic, and identifies faults and potential risks. Then, the system analyses and diagnoses the fault and impact to locate the software and hardware causes. There are two types of fault diagnosis:

1) The network fault analysis includes:

- Cross-domain fault identification: Analyse and locate network-level faults on a domain or inter-domain link, for example, the service area and external interconnection area may need to communicate with each other.
- Single domain of multiple PODs fault identification: Analyse and locate network-level faults on network devices.
- Single-NE fault identification: Analyse and locate component-level faults, e.g. boards, CPUs, memory, and optical modules.

2) Application analysis: perform service troubleshooting by analysing each connection and each application involved in the service path, correlating all the connection faults and SLA breaches.

Solution generation: The system supports multiple recommended solutions based on the fault diagnosis result. The solution may be to move or quarantine traffic, take ports and devices offline, change rollback, etc.

d) **Decision-making tasks:**

Solution evaluation and decision-making: Based on the recommended solutions and assistance of the network digital twin, the system supports evaluation criteria and decision-making. For example, whether the solution can solve the problem and the additional impact on the system.

e) **Execution tasks:**

The system supports solution implementation and verification:

1) Supports fault rectification and service verification, and implements fault rectification and risk elimination based on the optimal solution determined by the evaluation, such as isolating traffic, isolating ports, or devices, and change rollback.

2) Verify the troubleshooting results after the solution is implemented, including whether the service connectivity and application quality meet requirements to make sure it has been repaired.

6.4.3 Classification requirements

Table 4: Requirements for Network Monitoring and Troubleshooting

General Process	Capability	L1	L2	L3	L4
Intent management	Scenario-based monitoring	Manually manage the monitoring area and scope.	Use tools to manually configure monitoring tasks (such as Ansible and Python scripts).	The system supports the configuration of a monitoring task template. After a task is manually configured, the system automatically monitors the task.	The system supports input of monitoring intents such as applications SLA. The system automatically converts intents into monitoring tasks.

General Process	Capability	L1	L2	L3	L4
Perceived Analysis and Decision-making	Fault and risk detection	Manually collect device data.	Use the tool to collect device data, such as alarm and performance data.	The system supports automatically collect network inventory, topology, alarm, resource, traffic, and health data in minutes.	The system supports collect network device performance data in seconds, for example, microburst traffic fault detection. The system can detect application faults in seconds, including E2E service flow SLA paths, application connectivity, and application experience quality. The system supports network risk detection. The system supports the preceding functions through the network digital twin.
	Fault diagnosis, solution generation, and decision-making	A fault triggers manual fault identification.	The system automatically identifies faults. Manually determine the impact on services, manually generate network task solutions, and manually make decisions.	The system supports the automatic identification of network faults. The system supports preconfigured fault rectification solutions. Manually decide the optimal solution.	The system supports the automatic identification of network and application faults and generates rectification solutions. The system supports the generation of rectification solutions for potential network risks. The system supports simulation verification of the repair solution in seconds, including loop, address conflict, and security policy conflict. The system supports the preceding functions and uses the digital twin interactive interface to assist manual decision-making.

General Process	Capability	L1	L2	L3	L4
Execution	Solution implementation	Manual configuration implementation.	Manually use tools, such as Ansible and Python scripts.	The system supports automatic delivery of the recovery solution.	The system supports automatic delivery of the recovery solution. The system supports one-click rollback of the solution.
	Implementation verification	Manually complete the repair operation. Manually verify services.	Use tools, such as Ansible and Python scripts, to manually rectify the fault. Use the tool to verify the service.	The system supports automatic network health verification and network health visualization. The system supports data plane reachability verification and network protocol connectivity. The system supports scheduled and periodic automatic dialling tests to verify the connectivity between any device.	Based on the implementation of the rectification solution, the system supports network health check and network risk check. The system supports real-time verification of rewarranty services and service recovery status. The system supports automatic snapshots of the network before and after service configuration, and the comparison and acceptance are visible. The system supports the preceding functions with network digital twin verification.

6.5 Network Change - Application Policy Change

6.5.1 Function Requirement Overview

After a customer's application is brought online, some changes are also frequently made during daily routine maintenance. For example, the access relationship and policy between applications are adjusted, or the customer's partner organization needs to access the customer's data centre application, so the access policy is changed. These changes account for a high proportion of customers' routine changes. However, the current automation rate is insufficient. Security assurance depends on manual implementation and protection.

6.5.2 Workflow Process and Task Definition

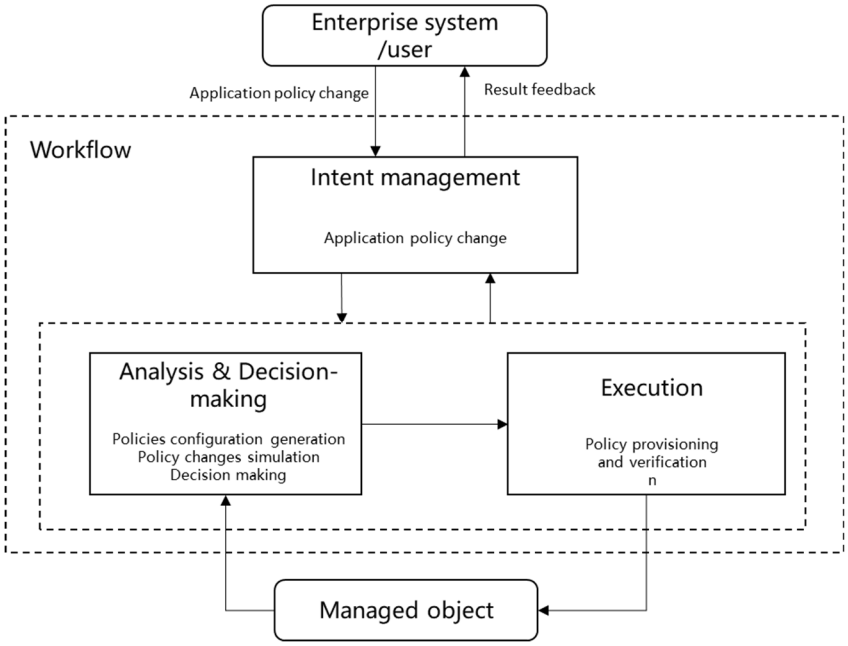

Figure 8: Application Policy Change Tasks Process

The application policy change process is shown in Figure 4, including intent, analysis, decision-making, and execution. The detailed management tasks are as follows:

a) **Intent management tasks:**

Application policy change intent: the system supports the following input:

1) Source and destination IP Address of the applications: Can be IPv4 or IPv6
2) Source port and destination port
3) Application names, including local application name, remote application name
4) Access policy: permit or deny

b) **Analysis/decision-making tasks:**

The system analyses the change intent, verifies whether the security compliance requirements are met, and allows users to check the compliance requirements. When compliance requirements are met, the system can generate a recommendation scheme. The recommended solution includes path provisioning and security policy configuration on each firewall along the path. The system displays paths and configurations in a visualized manner. The system supports the following capabilities:

1) Policy intent translation
2) Generate network change configuration solution, including NAT and security policy configuration
3) Visualized network changes
4) Online simulation and verification, and provide impact analysis

c) **Execution tasks:**

Network Provision: The system supports automatic deployment of solution configurations to the customer network. The system supports configuration rollback.

Application and network verification: the system supports automatically observing the applications and network health status for the new configuration, and verifying the applications and underlay network reachability of the entire network and output the verification results in a visualized manner.

Security policy verification: The system supports the verification of the changed secure path, which can be observed and verified in a visualized manner. And can also support security compliance analysis after changes.

6.5.3 Classification requirements

Table 5: Requirements for Application Policy Change

General Process	Capability	L1	L2	L3	L4
Intent management	Intent management	Manual conversion to network configuration.	Manually converted to a network configuration.	Intent management: network policy provisioning intent, input source and destination IP address information, policies, and ports.	Intent for application policy of source and destination application names, policies, etc.
Analysis/ Decision-making	Solution generation	Manually generate the network configuration, manually evaluate the impact, and manually make decisions.	Manually generate the network task solution, manually evaluate the impact, and manually make decisions.	The network policy configuration is automatically recommended, and also security policy configurations of the firewalls are generated, and manual decision-making is performed.	Application-centric policy intents are automatically translated to network configuration and security policies of the firewalls on the network paths, The system verifies the connectivity and provides impact analysis of existing services.
Execution	The policy Implementation	Manual configuration.	Manual configuration with collaborative tools (ansible...) and scripts (python...).	The generated configuration is automatically delivered.	Automatically deliver the intent and support rollback.
Verification	Verification	Manual tool test (e.g. ping).	Manual test with collaborative tools (ansible...) and scripts (python...).	The system supports automatic network health verification. The system can also automatically compare the policy configuration before and after the change and verifies visually.	The system supports the automatic verification the network connection and the impact of the policy changes on existing services. The system automatically verifies and visualizes the E2E service paths, applications, and application access quality.

7 Conclusions

Based on the general framework of network management and operation autonomous level classification in ETSI GR ENI 007 [i.3], the present document breaks down the management and operation workflow into common tasks and then evaluates the intelligence of each task to evaluate the intelligence of each phase in the entire lifecycle of DC network O&M.

Clause 5 describes the evolution direction of management autonomy in the lifecycle of typical DC networks, including POD planning and construction, and the evolution direction from network-oriented management and assurance to application-centric network management and assurance. Clause 6 describes in detail the autonomous classification requirements for both data centre infrastructure and service lifecycle, emphasizing the requirements for level-3 automation and level-4 autonomy.

Defining the level of intelligence in network management and operations helps the industry to reach a consensus on the path and goals for the future. This will drive the entire industry, especially enterprises, operators, and equipment providers, to invest more actively in technology introduction, helping to fully achieve Level 4 autonomy in most of the described scenarios, using the assumptions made in the present document.

History

Document history		
V4.1.1	May 2025	Publication