Network Digital Experience Management Service Technical White Paper

Product Solution V4.0

NETDEM Technology

Table Of Contents

1. Background Overview

1.1. Research and Development Background

With the rapid development of informatization, enterprise network structures are becoming more and more complex and extensive. Information integration is a new mindset that accompanies the application of information technology in enterprises. It is an effective means to improve efficiency, reduce costs, and enhance competitiveness. In recent years, with the continuous expansion of business scope in various enterprises, the continuous improvement of network infrastructure, and the leasing of a large number of operators dedicated lines, the difficulty of network management has become increasingly significant. Network operations and maintenance personnel lack suitable tools to pinpoint the root causes of the current decline in business quality, primarily manifested in:

1. The reasons affecting business quality and user experience have evolved from the original path interruptions to gradual deterioration in network performance, specifically characterized by severe degradation in latency or packet loss, leading to a noticeable reduction in efficiency;
2. Inadequate equipment performance and the presence of degradation make it difficult to automatically discover issues and quickly locate problems. Fault localization often requires a significant amount of time and lacks electronic evidence to trace issues. This situation can lead to suppliers easily deflecting responsibility and engaging in disputes;
3. Different telecom operator lines have the characteristics of wide distribution and high management complexity. There is a lack of effective assessment methods and ledger information, often

resulting in the phenomenon of service interruption without fee reduction;

4. Currently deployed network management products can only detect and alert major faults such as device crashes and line interruptions. However, there is a lack of comprehensive, visualized management tools that can provide real-time feedback on network quality metrics such as latency, jitter, packet loss, etc. This leads to high time and cost investment in network maintenance and low efficiency in daily operational analysis.

In order to address the challenges of difficult discovery and localization of network performance degradation, there is a need for professional service tools to conduct in-depth monitoring and analysis of leased dedicated network and internal communication paths. This is essential for identifying and resolving the aforementioned issues. To meet this need, our company has designed and developed a professional-grade enterprise-level proactive network performance insight product.

2. Introduction to Product Solution Features

2.1. Product Features

Establish an 'end-to-end, connectivity-oriented' network intelligent operation and maintenance system, achieving full coverage, automation, intelligence, visualization, and digitization to enhance users' digital experience.

- Full Coverage: Fusion of multiple detection technologies, covering Layer 2, Layer 3, standby links, WIFI, 5G networks, the industry's first to achieve end-to-end monitoring without dead angle
- Automation: realising fully automated closed-loop management such as auto-discovery→auto-identification→auto-nano-pipeline→auto-monitoring→auto-topology→auto-sensing→auto-warning→auto-warning→auto-positioning→auto-reporting etc.
- Intelligent: establish a learning analysis model, through multi-dimensional intelligent algorithms, to achieve intelligent detection, intelligent perception, intelligent positioning, intelligent analysis, and directly arrive at the conclusion of the analysis of the problem, without manual intervention and judgement, significantly improve the efficiency of operation and maintenance
- Visualization: Provides powerful spatial and temporal visualization capabilities, offering customized dashboards, multi-dimensional topology views, end-to-end positioning views, multi-indicator correlation views and other intuitive displays, to achieve three-dimensional visual monitoring and help O&M personnel to fully perceive the network operation situation
- Quantifiable: Through leading AI modelling and machine learning

algorithms, it provides a multi-dimensional view of network quality and establishes a scientific and quantitative network quality assessment mechanism to help users improve their digital experience

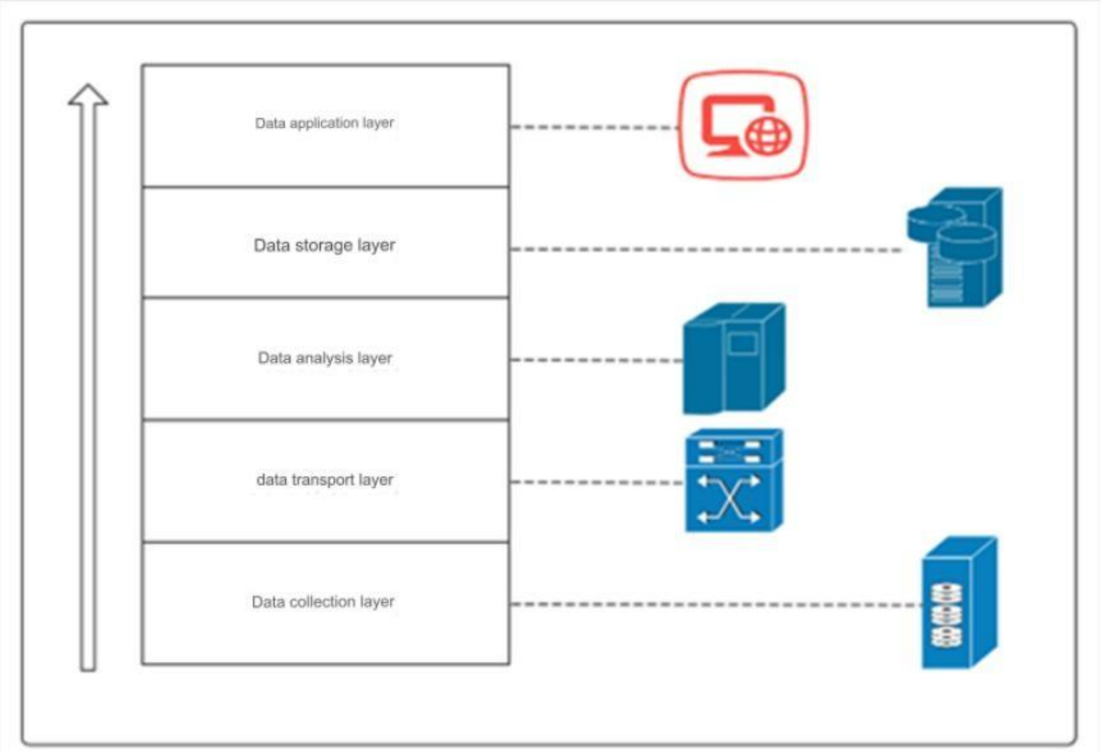
2.2. System Architecture Description

2.2.1. Hardware Architecture

Hardware Architecture with Five Layers:

1. Data acquisition layer: currently supports two acquisition modes: hard probe and relay acquisition.
2. Data transmission layer (gateway): in order to address the complex network environment of various enterprises, to achieve unified network access security management and unified business data management.
3. Data analysis layer: responsible for providing computing and storage resources for quality situational awareness, path analysis, relay analysis, network fault location function modelling and analysis.
4. Data storage layer: according to the needs of customers in different industries and the order of magnitude, select the corresponding data storage mode, while supporting the mainstream relational database and non-relational database.
5. Data application layer (data display): according to the results of business modelling and analysis, as well as business-related static

configurations, to provide data query services presented by the UI interface; WEB server to provide user-facing UI interactive interface capabilities.



Hardware Architecture Diagram

2.2.2. Software Architecture

2.2.3.1. Design Principles

In the design of application systems, the overall design principle is based on 'consider maintenance during design, consider the future during design,' and strictly adheres to the principles of advancement, practicality, openness, stability, security, and compliance with international standards.

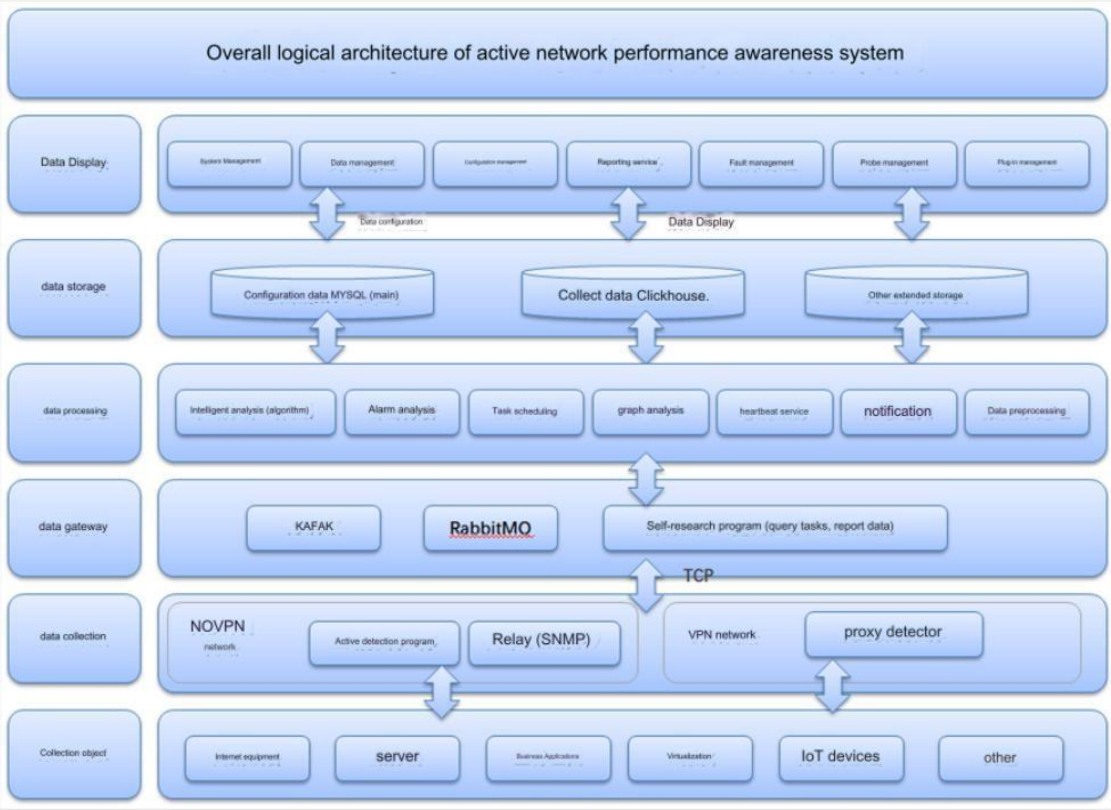
In software design, it is crucial to fully consider the diversity and complexity of the business, as well as the potential for future evolution. During the development phase, it is important to assess in advance the potential impact on the production environment posed by new devices and newly introduced applications. This assessment includes evaluating the effects on system performance, system architecture, fault localization, customer perception, and other factors. This proactive evaluation aims to lay the groundwork and prepare processes for subsequent stable operation.

2.2.3.2. Overall Architecture

Active network performance perspective system, the overall architecture of the software uses a fully distributed architecture, each layer of the technical architecture has a good contraction and scalability, while supporting load balancing and high availability. The reliability of the data to support multiple copies, can be very smooth to ensure data integrity and security.

The overall technical architecture has strong flexibility, good contraction of hardware resources, suitable for different industry customers and industry needs, while it is very convenient to support the expansion of customised business R & D, support for 20,000 and more link analysis, and can support the PB level and more data volume.

This technical architecture is suitable for more complex network architecture design, can be very practical in the financial, electric power, airports, carriers and other application scenarios. The architecture incorporates artificial intelligence analysis algorithms, machine learning related technologies and science, which can quickly analyse and locate problems and predict potential problems in real time.



2.2.3.3. Other Designs

2.2.3.3.1. Interface Responsiveness

The responsiveness of the user interface is less than or equal to 5 seconds to open the page.

2.2.3.3.2. Responsiveness in Massive Data Queries

Queries should yield results within 15 seconds or less.

2.2.3.3.3. Average Response Time

The time elapsed from the system receiving a business request to providing the response. This includes page response time, transaction processing response time, database processing time, network transmission time, etc. For query-type business operations, the page response time should be kept within 3 seconds, and for business processing operations, the page response time should be kept within 5 seconds.

2.2.3.3.4. Security

The system should have robust security measures in place to ensure that data is not unlawfully accessed or modified, and to guarantee data consistency. Various checks and mechanisms should be employed to address issues such as unauthorized logins or system failures. The implementation of fault detection, alarms, and handling mechanisms is essential to ensure data integrity and prevent loss or damage due to unforeseen circumstances.

2.2.3.3.5. Reliability

The system is equipped with the capability to operate continuously 24 hours a day, 7 days a week.

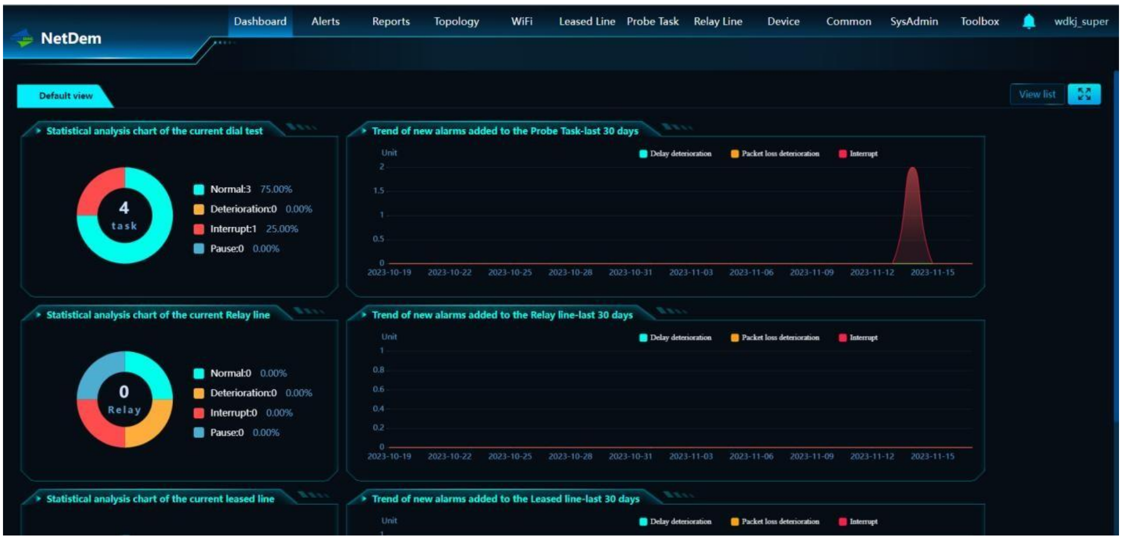
2.3. Functional Design - Management Back-Office

2.3.1. Dashboard

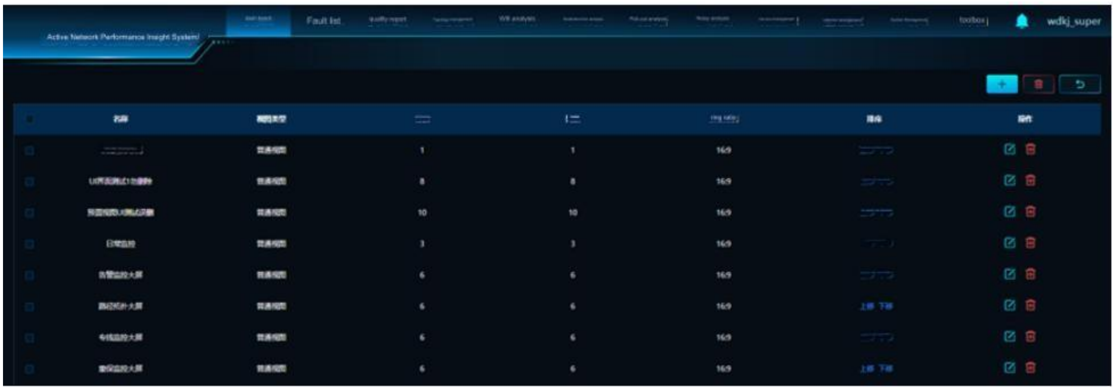
Support for personalized custom dashboards, dashboards can be added, modified, deleted, and the dashboard display components can be customized, so that users can present the information they care about on a single dashboard, which greatly facilitates operation and maintenance monitoring.

- Built-in Default Dashboard: Supports counting the number and percentage of normal, interruption and degradation of the monitored tasks, leased lines and relays on the same day in the form of concentric circles; Supports counting the trend of new alarms generated by the tasks, leased lines and relays in the recent month (based on 30 days), divided into interruption, delay degradation and packet loss degradation;

- Supports user creation and maintenance of customized dashboards;
- Support for switching to view existing dashboards

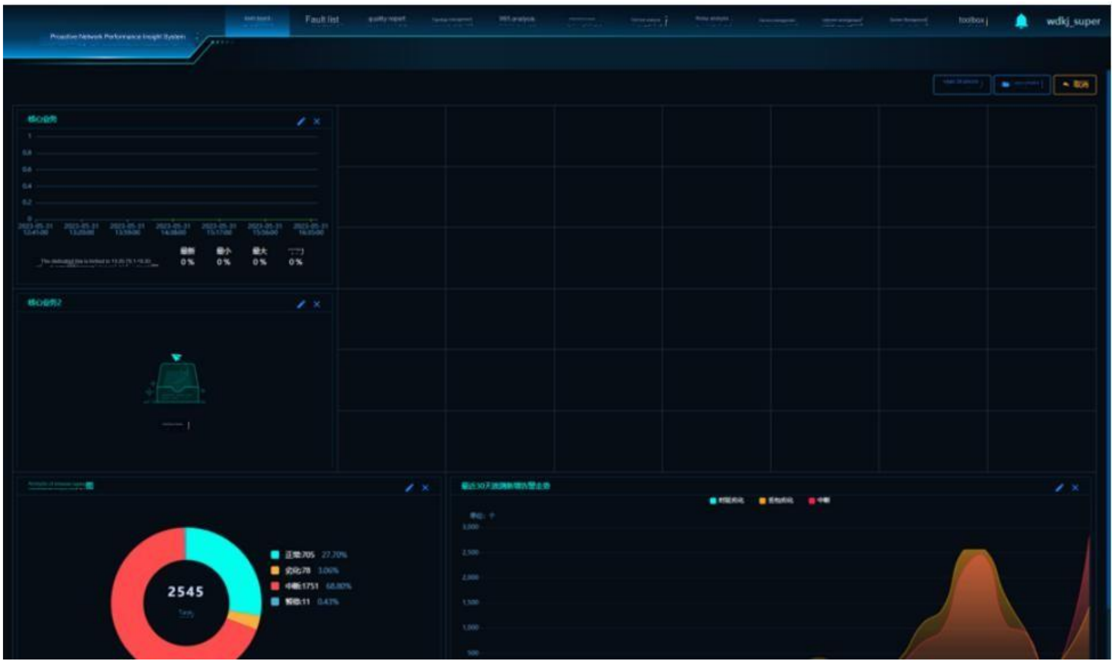


- Supports comprehensive management of dashboard additions, deletions, changes and checks

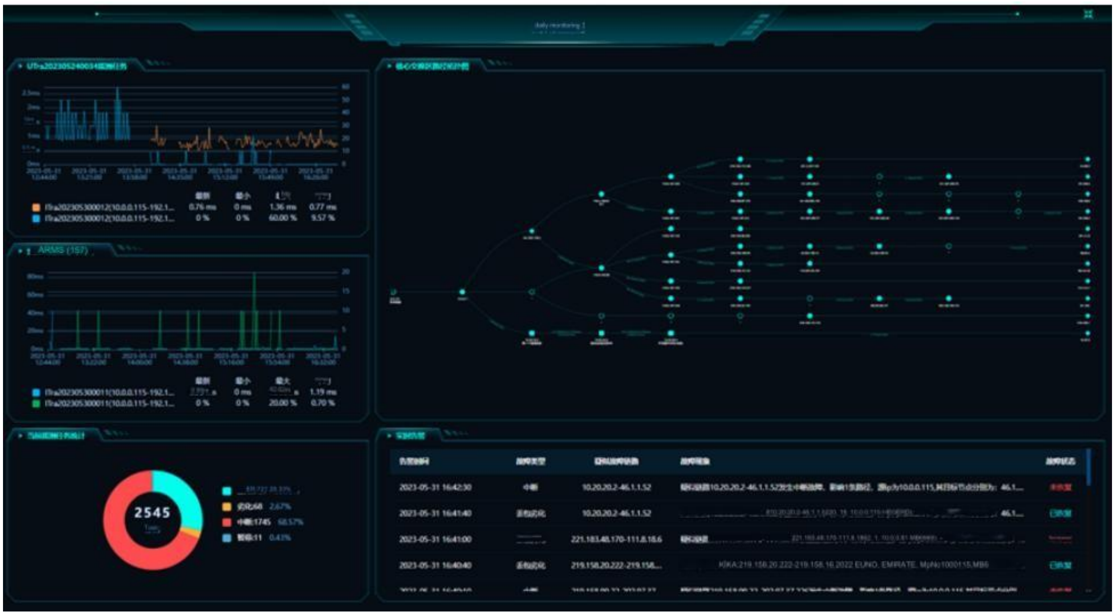


□	名称	视图类型	[illegible]	[illegible]	[illegible]	排序	操作
□	[illegible]	普通视图	1	1	16:9	[illegible]	
□	UI界面测试1勿删除	普通视图	8	8	16:9	[illegible]	
□	[illegible]	普通视图	10	10	16:9	[illegible]	
□	日常监控	普通视图	3	3	16:9	[illegible]	
□	告警监控大屏	普通视图	6	6	16:9	[illegible]	
□	[illegible]大屏	普通视图	6	6	16:9	上移 下移	
□	专线监控大屏	普通视图	6	6	16:9	[illegible]	
□	[illegible]监控大屏	普通视图	6	6	16:9	上移 下移	

- Supports the editing of dashboards, including the management of adding, deleting, changing and checking the components displayed on the dashboards



- Dashboards that support full-screen display options



- Provides a variety of building blocks: path topology, leased line operational overview, real-time alarms, physical topology, operational statistics (dial-up, leased line, trunk), 30-day alarm trends (dial-up, leased line, trunk), aggregated graphs .

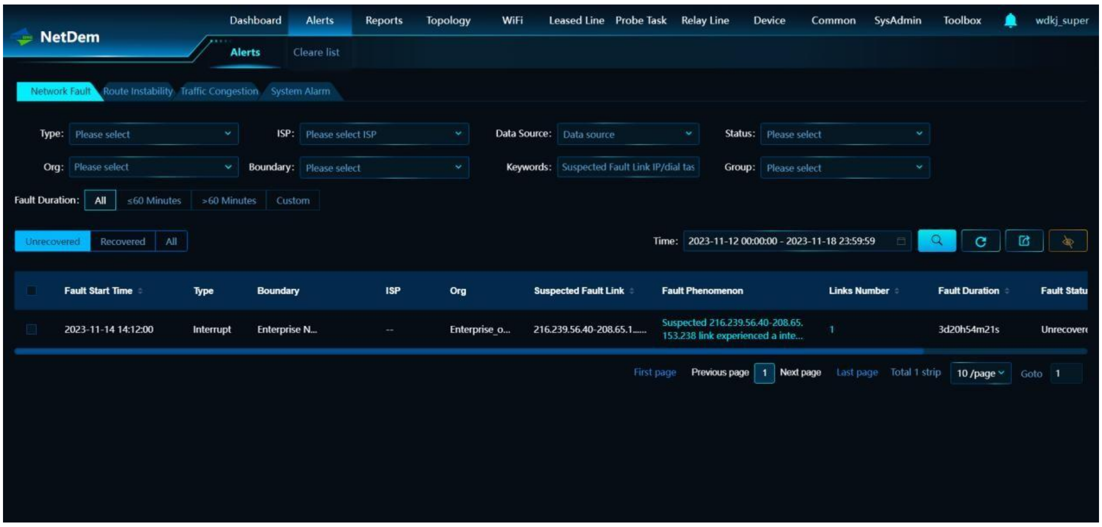
2.3.2. Fault List

After completing the probe dialling task or relay monitoring task creation, the system will automatically monitor the status of the path/relay, proactively sense interruptions, delay degradation, packet loss, route fluctuations and other issues, and automatically generate alerts (faults), with different faults displayed in different Tab pages (network failure, route fluctuations, leased line congestion), as follows:

- Generate fault work orders based on "fault type + suspected fault node IP", network faults include: interruption, delay degradation, packet loss degradation;
- Support multi-dimensional query fault list and export, data dynamic refresh;
- Provide detailed information on fault start time, fault classification, operator, organization, suspected fault link, fault phenomenon, fault cause, number of paths affected, fault duration, fault status, work order status and operation;
- Support for fault definition and accountability (leased line and enterprise network, where enterprise network = non-leased line) ;
- Supports retrospective view and additional processing records of fault history, including operator, operation time, operator's affiliation, processing, and processing results;
- Provides viewing of the suspected fault node association impact path, including: impact path number, alarm trigger time, alarm recovery time, source IP, target IP, target name;
- Not only provides end-to-end topology maps of Layer 3 paths, but also shows Layer 2 devices that can be managed in the end-to-end topology map of paths and allows for more accurate fault location, where degraded link segments are highlighted in yellow and interrupted

link segments are highlighted in red with a cross X;

- ➢ Provides indicator trend graph positioning display, with a red small triangle △ marking the fault generation time point, with a green small triangle △ marking the fault recovery time point, support in the time range of 3 hours before the occurrence of the fault to 3 hours after the recovery of the fault (if not recovered to the current system time) dragging to view the trend of the original indicators, the original indicators, including latency, packet loss, inbound flow rate, outbound flow, which outbound/inbound flow rate to support the display of the unit of adaptive between the K/M/G/T;



Type: Please select ISP: Please select ISP Data Source: Data source Status: Please select

Org: Please select Boundary: Please select Keywords: Suspected Fault Link IP/dial tas Group: Please select

Fault Duration: All ≤60 Minutes >60 Minutes Custom

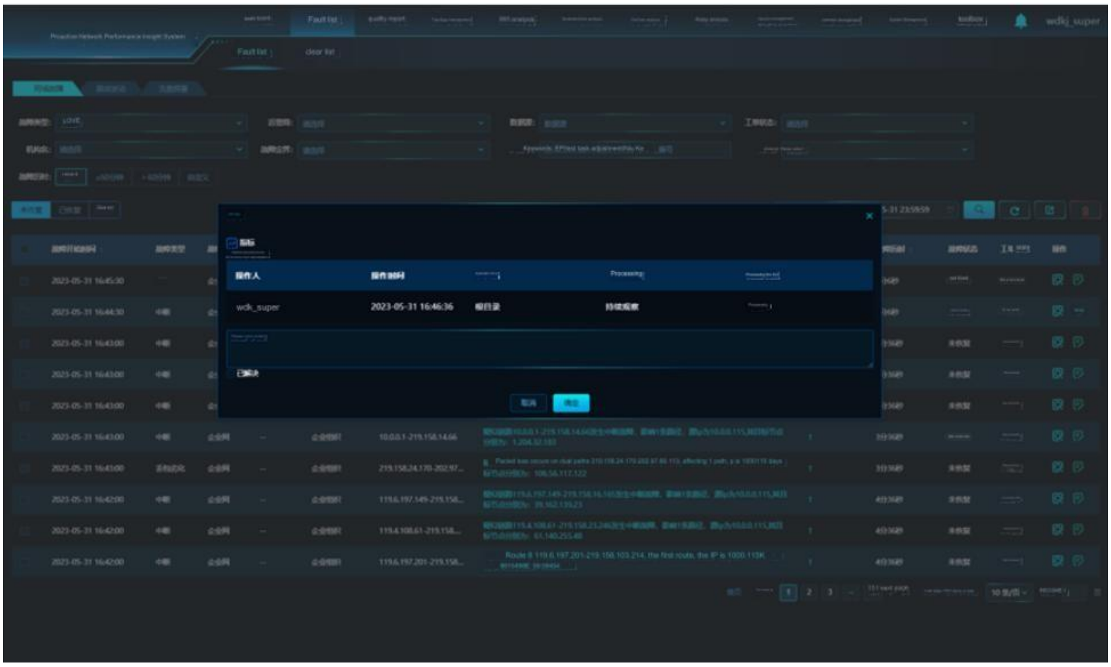
Unrecovered Recovered All

Time: 2023-11-12 00:00:00 - 2023-11-18 23:59:59

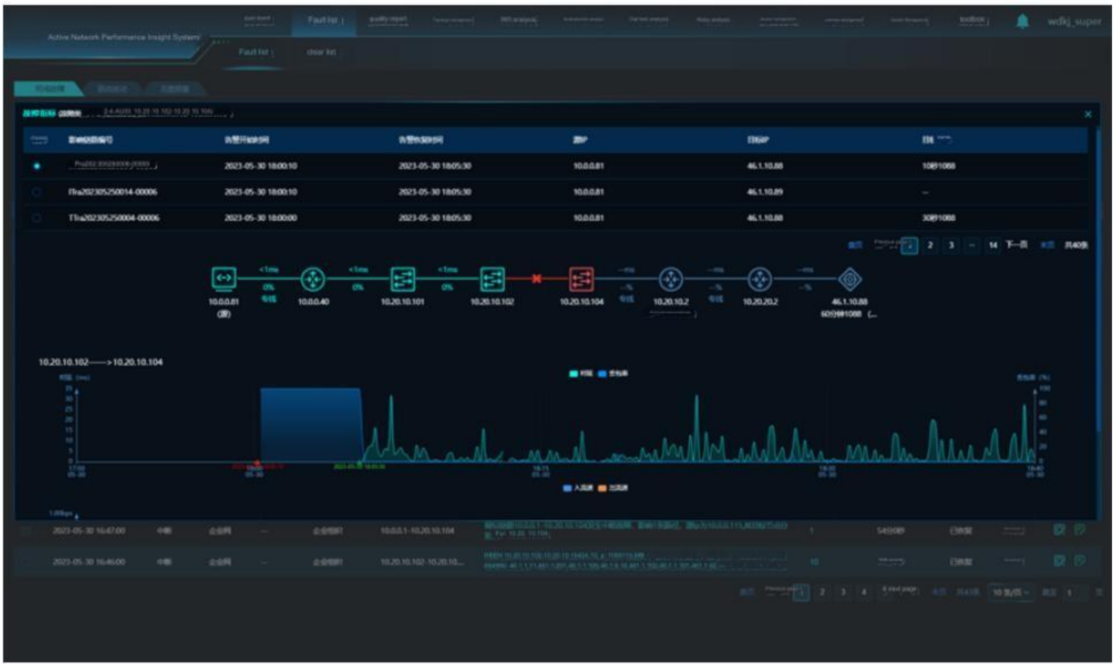
□	Fault Start Time	Type	Boundary	ISP	Org	Suspected Fault Link	Fault Phenomenon	Links Number	Fault Duration	Fault Statu
□	2023-11-14 14:12:00	Interrupt	Enterprise N...	--	Enterprise_o...	216.239.56.40-208.65.1......	Suspected 216.239.56.40-208.65.153.238 link experienced a inte...	1	3d20h54m21s	Unrecovere

First page Previous page 1 Next page Last page Total 1 strip 10 /page Goto 1

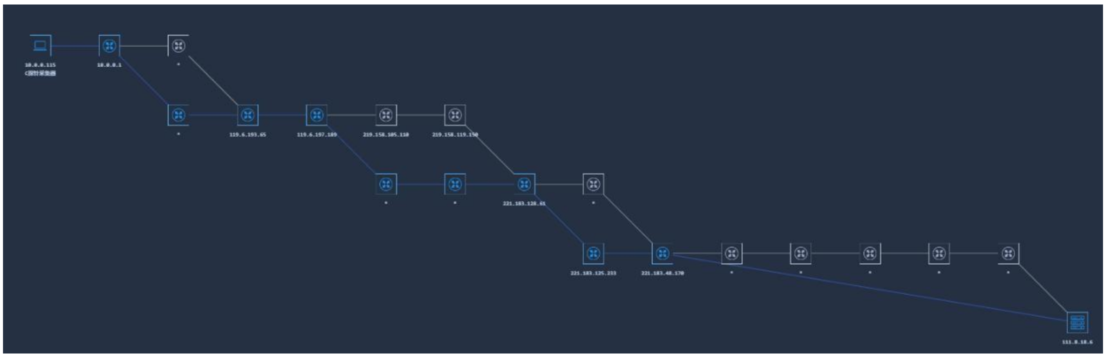
Fault List



Historical processing log (supports processing and appending operations)



Metric Details

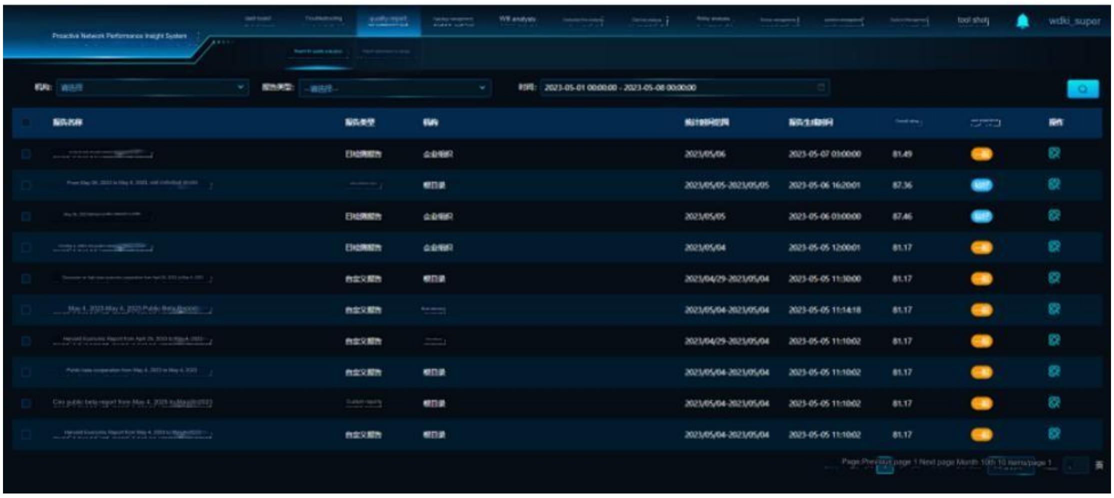


Routing Fluctuation

2.3.3. Quality Reports

2.3.3.1. Quality Test Reports

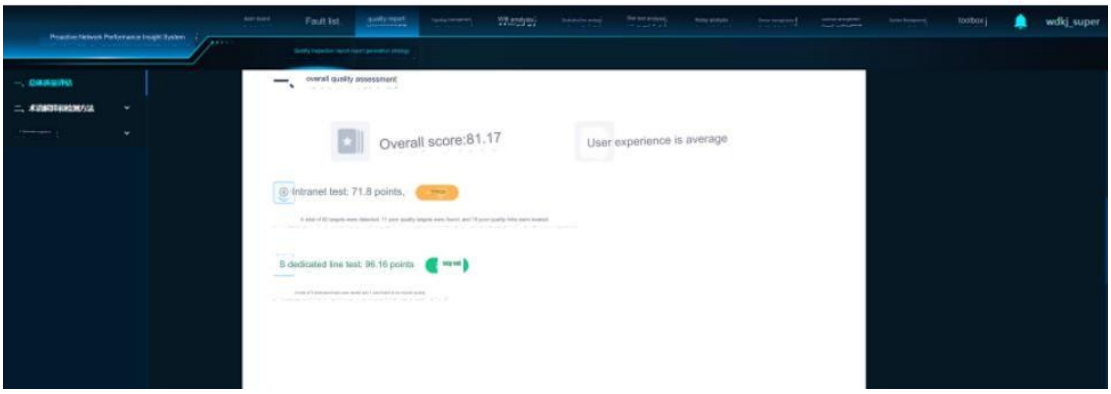
- ✓ Support to view the list of different types of reports (daily, weekly, monthly, custom reports); support to evaluate the ratings, user experience within the statistical time period of the report；
- ✓ Support for Report Printing；
- ✓ Support for viewing report details；
- ✓ Supports network full-coverage active detection technology to achieve 360-degree dead-angle-free detection of WIFI + intranet + leased lines. Through leading AI modelling and machine learning algorithms, it transforms invisible network quality into intuitive digital scores and provides targeted rectification recommendations for problems found in the detection content respectively, helping users to enhance their digital experience；



[illegible]: 2023-05-01 00:00:00 - 2023-05-08 00:00:00

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	2023/05/06	2023-05-07 03:00:00	81.49	[illegible]
[illegible]	[illegible]	根目录	2023/05/05-2023/05/05	2023-05-06 16:20:01	87.36	[illegible]
[illegible]	[illegible]	[illegible]	2023/05/05	2023-05-06 03:00:00	87.46	[illegible]
[illegible]	[illegible]	[illegible]	2023/05/04	2023-05-05 12:00:01	81.17	[illegible]
[illegible]	自定义报告	根目录	2023/04/29-2023/05/04	2023-05-05 11:30:00	81.17	[illegible]
May 4, 2023-May 4, 2023 Public Beta Report	自定义报告	[illegible]	2023/05/04-2023/05/04	2023-05-05 11:14:18	81.17	[illegible]
[illegible]	自定义报告	[illegible]	2023/04/29-2023/05/04	2023-05-05 11:10:02	81.17	[illegible]
[illegible]	自定义报告	根目录	2023/05/04-2023/05/04	2023-05-05 11:10:02	81.17	[illegible]
City public beta report from May 4, 2023 to [illegible]	[illegible]	根目录	2023/05/04-2023/05/04	2023-05-05 11:10:02	81.17	[illegible]
[illegible]	自定义报告	根目录	2023/05/04-2023/05/04	2023-05-05 11:10:02	81.17	[illegible]

Page Previous page 1 Next page Month 10th 10 items/page 1



overall quality assessment

Overall score:81.17

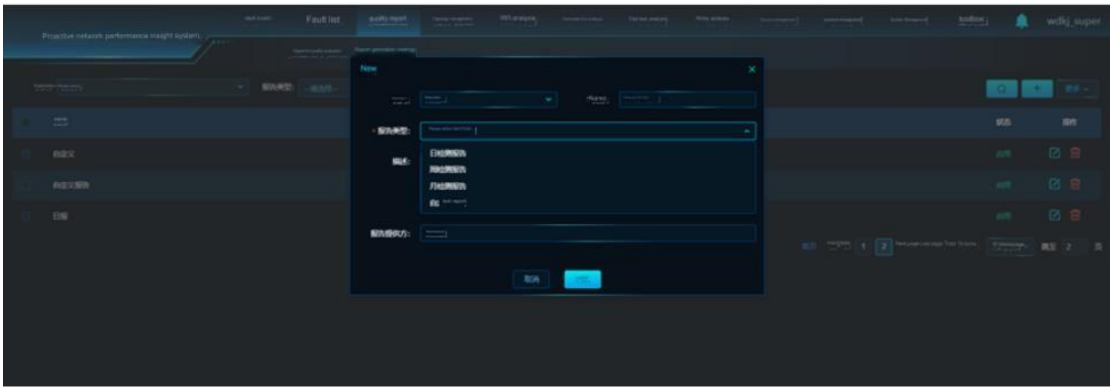
User experience is average

Intranet test: 71.8 points,

B dedicated line test: 96.16 points

2.3.3.2. Report Generation Strategy

- ✓ Supports user-configurable report generation policies for different types of reports (daily, weekly, monthly, custom reports) ;
- ✓ Supports automatic generation of network quality inspection reports according to the generation policy;



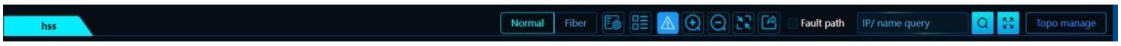
2.3.4. Topology Map Management

Topology management includes path topology and physical topology. Path topology refers to the topology of the network service path, i.e., end-to-end presentation of the service flow through the network elements; physical topology refers to the physical network structure, i.e., the layout of the line connection between the devices is presented. A major feature of this system is that the system can automatically generate various types of topology, adaptive to network changes, without manual maintenance.

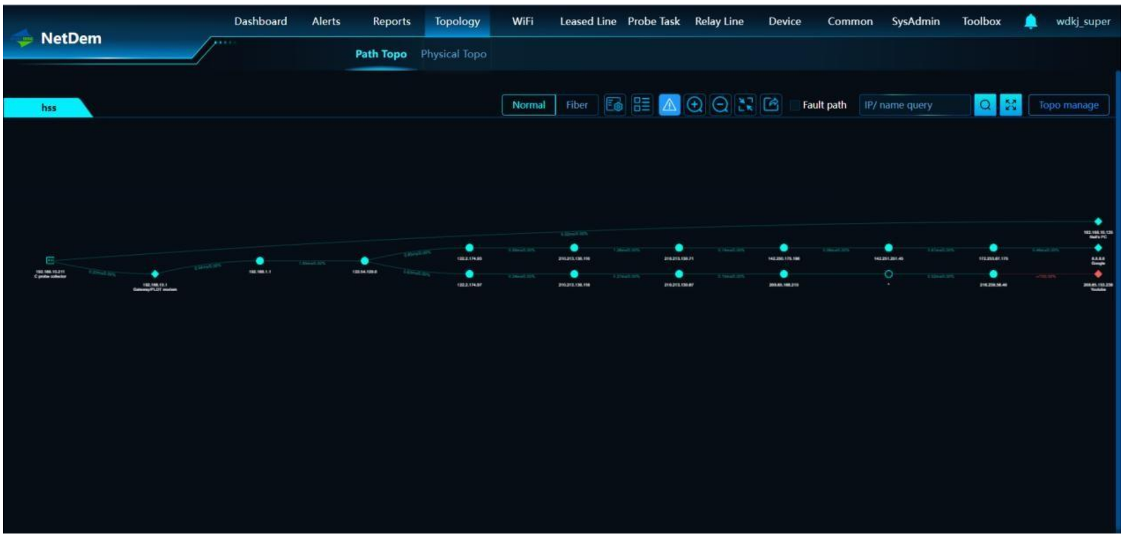
2.3.4.1. Path topology

Path topology is the topology of the network service path, i.e., the end-to-end presentation of the service flow through network elements.

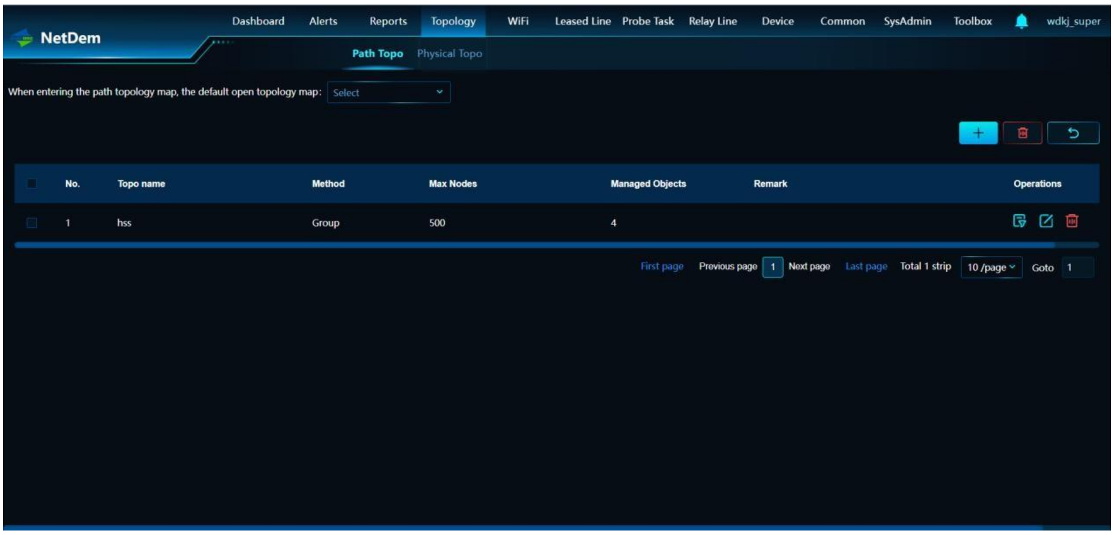
- ✓ Automatic generation of path topology, statistical analysis of data collected from dial-a-test tasks (ordinary dial-a-test, high-frequency monitoring), automatic learning and generation of paths, and automatic generation of path topology through self-developed algorithms.
- ✓ Convenient tool operations: topology selection, zoom in, zoom out, page restore, tree layout, star layout, alarm display configuration, export, information display settings, legend, etc.



- ✓ Probe IP, Probe Name, Node IP, Node Name Search Locate
- ✓ Enables topology viewing: supports auto-refresh;
- ✓ Support alarm message display (color marking), alarm message viewing;
- ✓ Supports integrated display of line performance metrics (latency, packet loss, outages, flow rate, etc.)



- ✓ Support for Automatic Thumbnail Generation
- ✓ Supports manual creation of thumbnails, expanding thumbnails
- ✓ Supports integrated management of topology map addition, modification, deletion, etc.

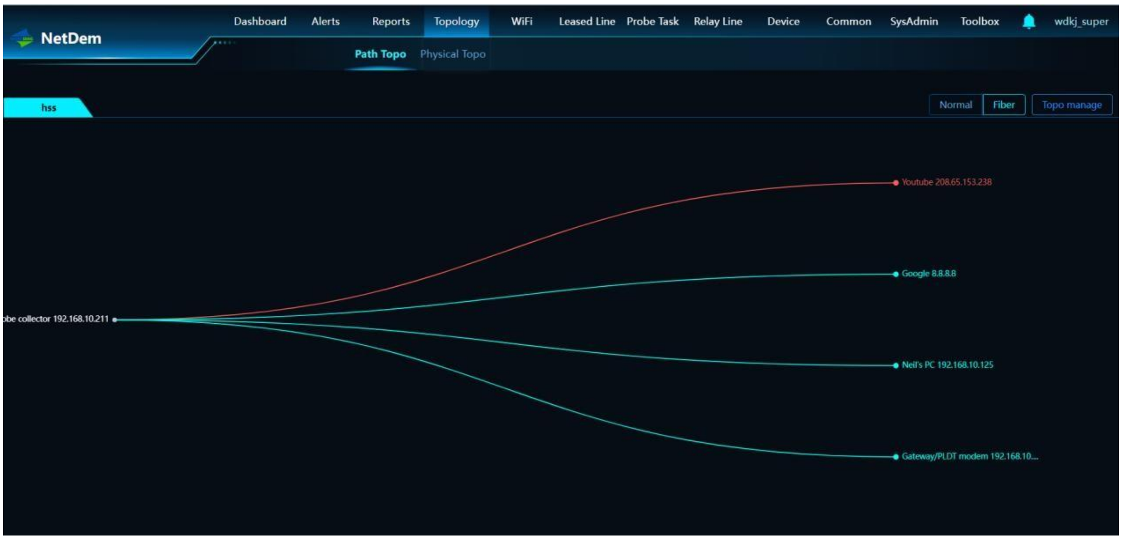


When entering the path topology map, the default open topology map: Select

No.	Topo name	Method	Max Nodes	Managed Objects	Remark	Operations
1	hss	Group	500	4		

First page Previous page 1 Next page Last page Total 1 strip 10 /page Goto 1

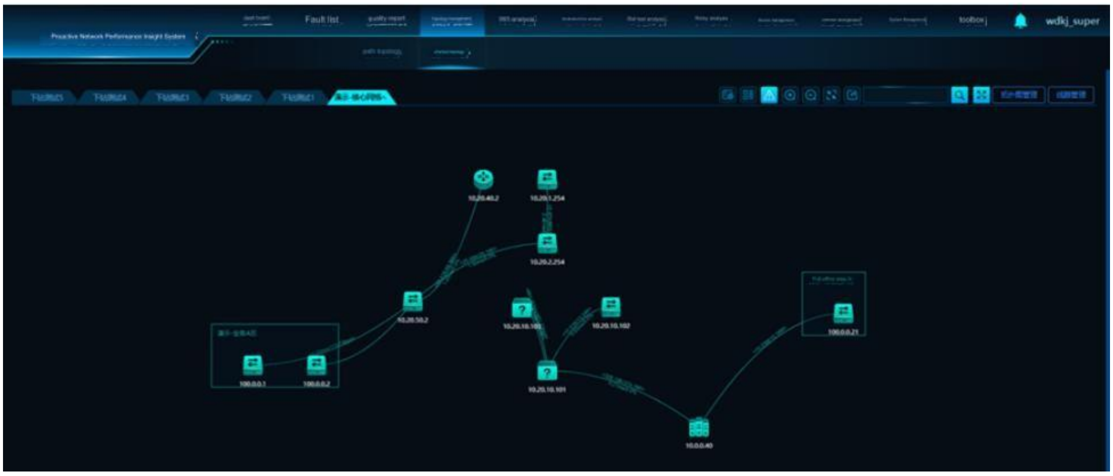
- ✓ Supports viewing as a fibre map;



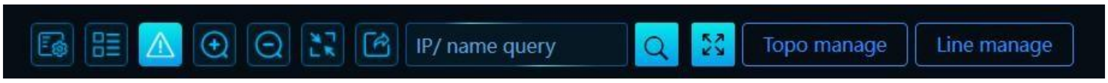
- ✓ Support for presenting Layer 2 devices on a path topology map;

2.3.4.2. Physical Topology

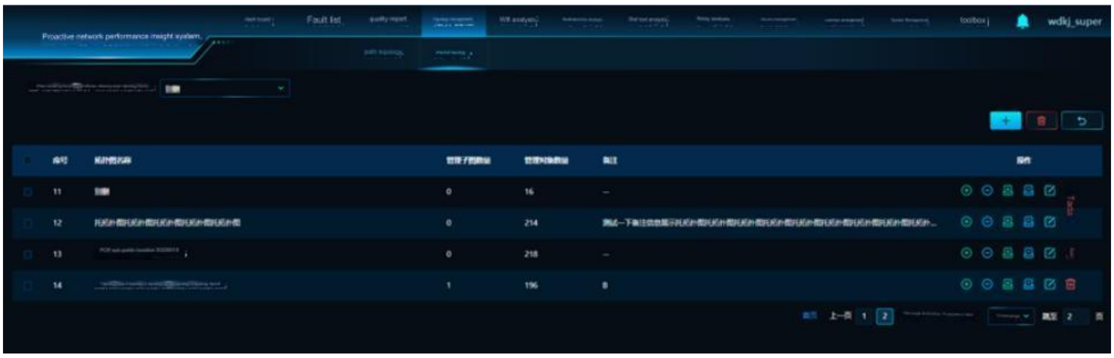
Physical topology refers to the physical networking structure of the network, i.e., the layout of the line connections between devices presents.



- ✓ Enables automatic generation of physical topology based on auto-discovered network neighbours.
- ✓ Enables easy-to-use tools: topology selection, zoom in, zoom out, page restore, alarm display configuration, export, information display settings, legend, etc.



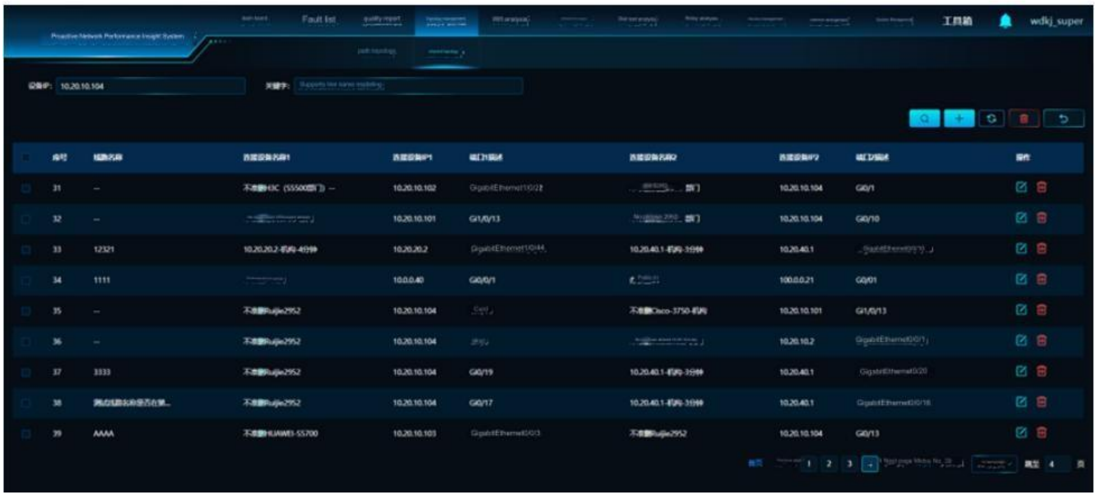
- ✓ Support device IP, device name search and location
- ✓ Enables topology viewing: supports automatic refresh; alarm message display (color coding); supports integrated display of line performance metrics (latency, packet loss, interruptions, flow rate, etc.)
- ✓ Supports integrated management of topology diagrams such as adding, modifying, deleting, etc., supports multi-layer topology diagrams, supports adding/removing objects to/from topology diagrams, and supports adding/removing sub-diagrams to/from topology diagrams;



序号	拓扑图名称	管理子图数量	管理对象数量	备注	操作
11	[illegible]	0	16	–	
12	拓扑图拓扑图拓扑图拓扑图拓扑图	0	214	测试一下备注信息显示拓扑图拓扑图拓扑图拓扑图拓扑图拓扑图拓扑图拓扑图拓扑…	
13	[illegible]	0	218	–	
14	[illegible]	1	196	8	

上一页 1 2 跳至 2 页

- ✓ Supports comprehensive management of line additions, deletions, changes and checks



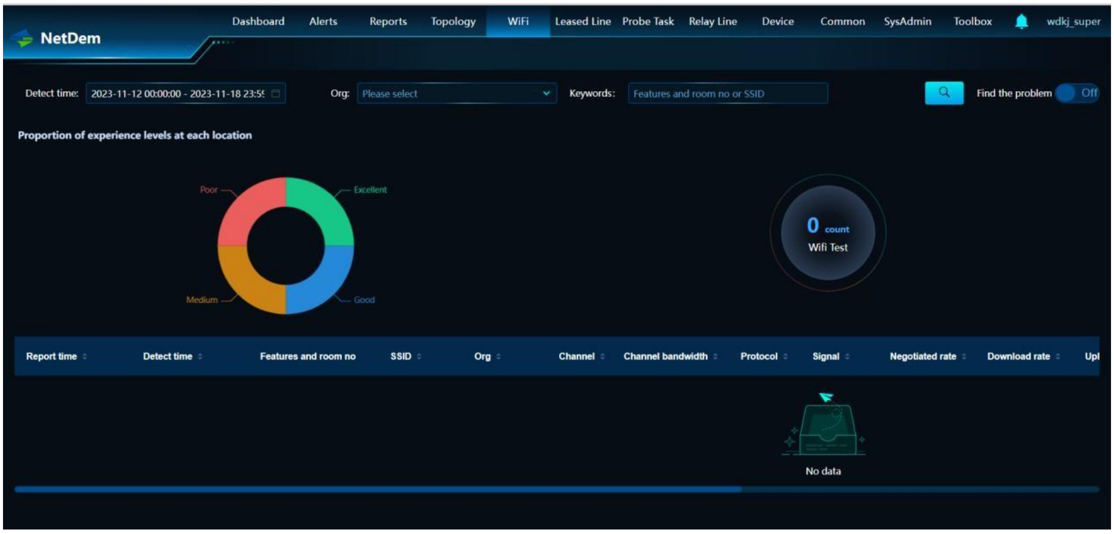
设备IP: 10.20.10.104 关键字: Supports line name matching

序号	线路名称	首端设备名称1	首端设备IP1	端口1描述	首端设备名称2	首端设备IP2	端口2描述	操作
31	–	不准删H3C（S5500部门）–	10.20.10.102	GigabitEthernet1/0/22	[illegible]部门	10.20.10.104	Gi0/1	
32	–	[illegible]	10.20.10.101	Gi1/0/13	[illegible]部门	10.20.10.104	Gi0/10	
33	12321	10.20.20.2-机构-4599	10.20.20.2	GigabitEthernet1/0/44	10.20.40.1-机构-3599	10.20.40.1	[illegible]	
34	1111	[illegible]	10.0.0.40	Gi0/0/1	[illegible]	100.0.0.21	Gi0/01	
35	–	不准删Ruijie2952	10.20.10.104	[illegible]	不准删Cisco-3750-机构	10.20.10.101	Gi1/0/13	
36	–	不准删Ruijie2952	10.20.10.104	[illegible]	[illegible]	10.20.10.2	GigabitEthernet0/0/1	
37	3333	不准删Ruijie2952	10.20.10.104	Gi0/19	10.20.40.1-机构-3599	10.20.40.1	GigabitEthernet0/20	
38	测点线路名称是否在…	不准删Ruijie2952	10.20.10.104	Gi0/17	10.20.40.1-机构-3599	10.20.40.1	GigabitEthernet0/0/16	
39	AAAA	不准删HUAWEI-S5700	10.20.10.103	GigabitEthernet0/0/3	不准删Ruijie2952	10.20.10.104	Gi0/13	

1 2 3 4 跳至 4 页

2.3.5. WiFi Analysis

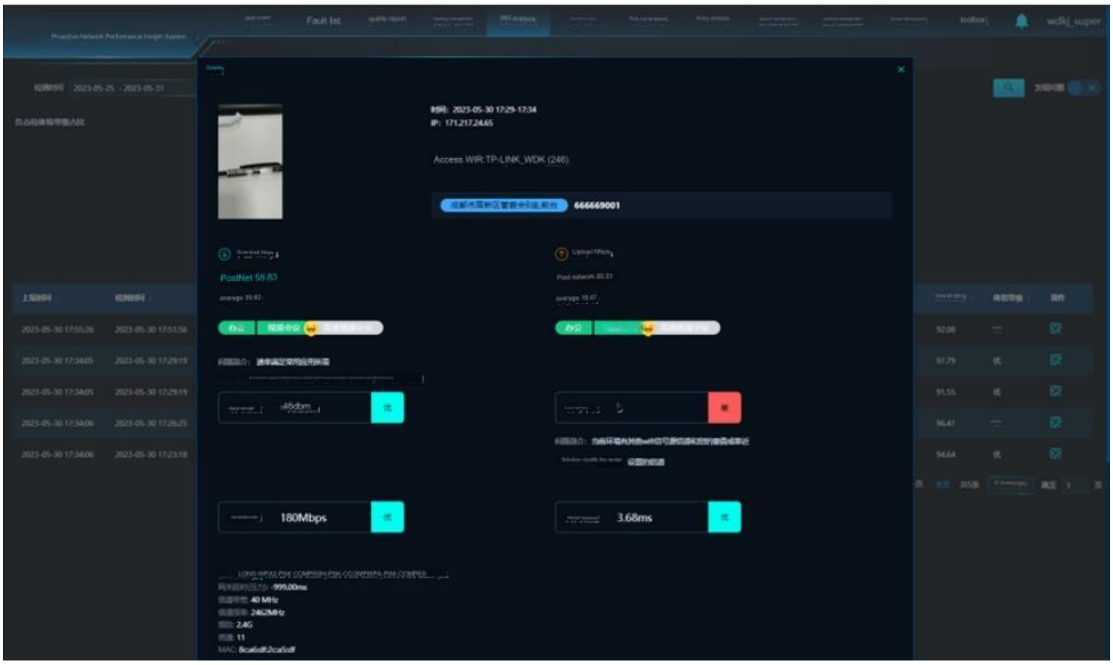
- Supports list view of key indicators of WiFi detection records such as band, bandwidth, protocol, signal strength, negotiated connection rate, download rate, uplink rate, gateway response, problem items, etc., and at the same time, it supports drill down to view details;



Detect time: 2023-11-12 00:00:00 - 2023-11-18 23:5
Org: Please select
Keywords: Features and room no or SSID
Find the problem: Off

Proportion of experience levels at each location

Report time	Detect time	Features and room no	SSID	Org	Channel	Channel bandwidth	Protocol	Signal	Negotiated rate	Download rate	Upl

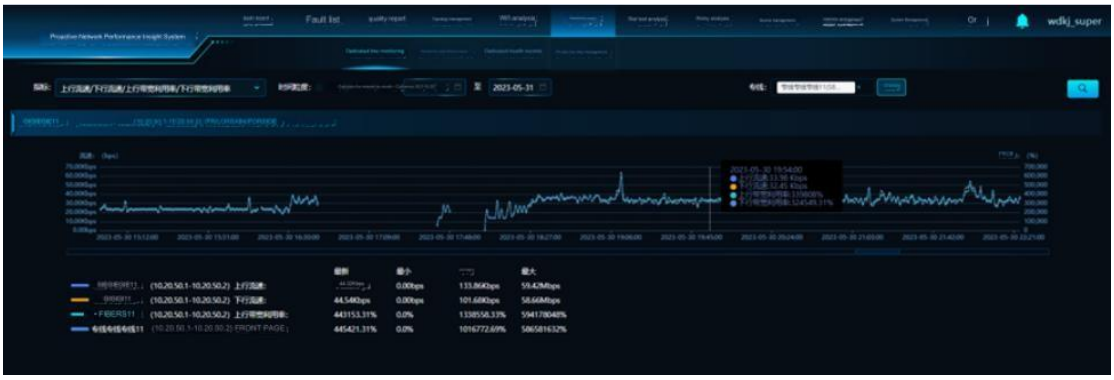


时间: 2023-05-30 17:29-17:34
IP: 171.217.24.65
Access WiFi:TP-LINK_WDK (246)
666669001
频道带宽: 40 MHz
信道频率: 2462MHz
频段: 2.4G
信道: 11
MAC: 8cadd82ca5df

2.3.6. Leased line Management

2.3.6.1. Leased Line Monitoring

This feature shows the current performance of leased lines and is suitable for maintenance personnel to monitor leased line performance in bulk. For leased lines that need to be focused on, you can specify a time period to view specific metrics, including latency/packet loss, inbound flow rate/outbound flow rate/inbound utilization rate/outbound utilization rate, availability/goodness rate/availability (exempt)/goodness rate (exempt):



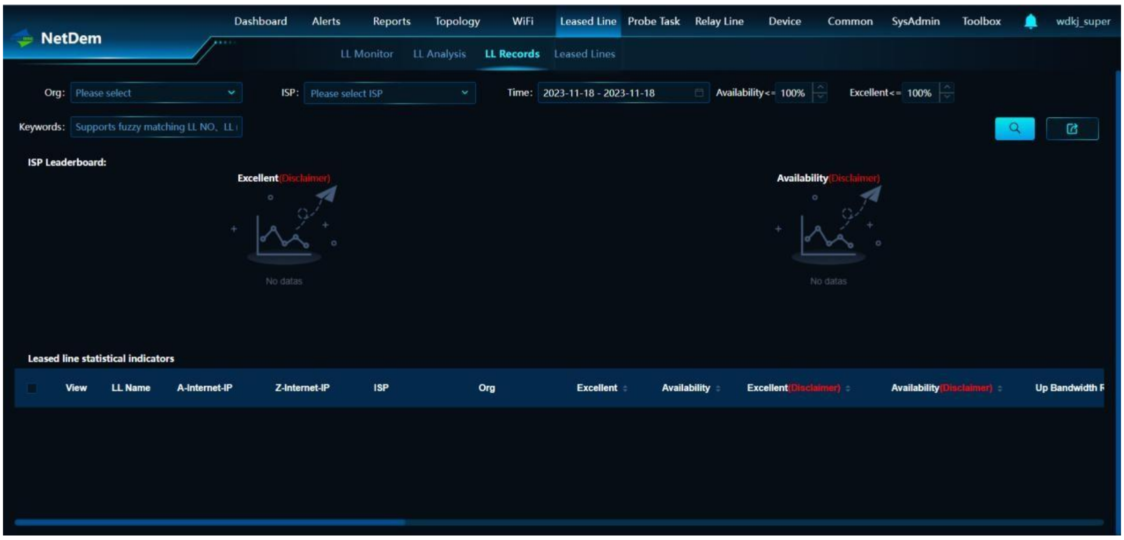
	最新	最小	[illegible]	最大
[illegible] (10.20.50.1-10.20.50.2) 上行流速:	[illegible]	0.00bps	133.86Kbps	59.42Mbps
[illegible] (10.20.50.1-10.20.50.2) 下行流速:	44.54Kbps	0.00bps	101.68Kbps	58.66Mbps
FIBERS11 (10.20.50.1-10.20.50.2) 上行带宽利用率:	443153.31%	0.0%	1338558.33%	594178048%
[illegible] (10.20.50.1-10.20.50.2) FRONT PAGE	445421.31%	0.0%	1016772.69%	506581632%

2.3.6.2. Leased-line Health Records

The system creates health records for dedicated lines leased by enterprises, tracking the operational status of the leased lines. It automatically identifies nodes within the path of the dedicated lines and calculates their operational quality. This enables the system to promptly identify dedicated lines with potential quality issues, ensuring that operators take corrective actions as required. Once dedicated line information and corresponding test tasks or relay collection tasks are established, the system automatically calculates operational indicators based on relay priority principles in the dedicated line health records.

This includes viewing original collection indicators. The specific manifestations are as follows:

- Supports multi-dimensional enquiry on the operation quality indicators of leased lines by operator, branch, etc.;
- Supports statistics on the key indicators of leased lines, including: excellence rate, availability rate, excellence rate (exempted), availability rate (exempted), outgoing utilization rate, incoming utilization rate, maximum delay, average delay, maximum packet loss rate, average packet loss rate, maximum outgoing flow rate, average outgoing flow rate, maximum incoming flow rate, average incoming flow rate, cumulative degradation, delay degradation, packet loss degradation and outage cumulative duration;
- Supports the presentation of key metrics of leased lines by means of trend graphs, whose key metrics include: latency, packet loss rate, outbound flow rate, inbound flow rate, outbound utilization rate, inbound utilization rate, excellence rate, availability rate, excellence rate (exempted), and availability rate (exempted);
- Indicator trend charts are presented at an adaptive granularity based on the time range selected from the TAB page, supporting synchronous switching between granularities by scrolling the mouse wheel to view the details of the associated indicators;
- Supports interfacing with external systems to obtain cutover information through the Extended Interface API;
- Supports the ranking of the quality of leased lines of various carriers (in terms of the excellence rate of exemption or the availability rate of exemption;



Org: Please select

ISP: Please select ISP

Time: 2023-11-18 - 2023-11-18

Availability<= 100%

Excellent<= 100%

Keywords: Supports fuzzy matching LL NO、LL

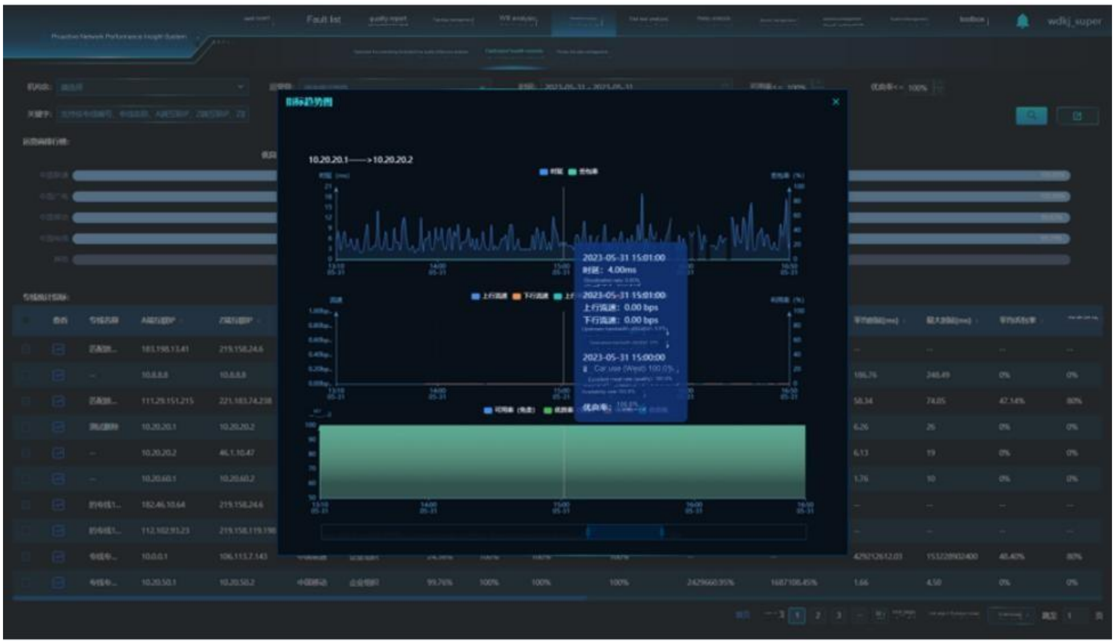
ISP Leaderboard:

Excellent(Disclaimer)

Availability(Disclaimer)

Leased line statistical indicators

View	LL Name	A-Internet-IP	Z-Internet-IP	ISP	Org	Excellent	Availability	Excellent(Disclaimer)	Availability(Disclaimer)	Up Bandwidth F



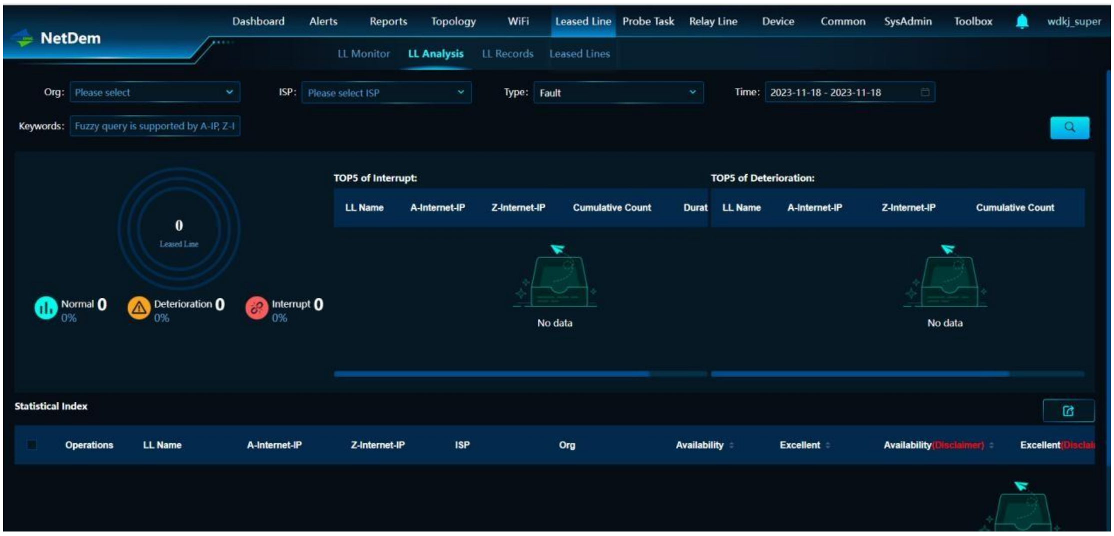
Note:

Excellence rate (exemption) = [Effective operating hours - (interruption hours - power outage hours - cutover hours) - (degradation hours - congestion hours)]/Effective operating hours*100 %;

Availability (exemption) = [active operating hours - (interruption hours - power outage hours - cutover hours)]/active operating hours*100%;

2.3.6.3. Leased Line Quality Analysis

The system automatically collects data for dedicated lines, performs statistical analysis on the quality issues of relays, and defaults to analyzing the data for all dedicated lines on the current day. It supports selecting organizations, operators, statistical perspectives, time periods, and keywords to specify the data range for statistical analysis. The system provides a summary of quality analysis information:



Org: Please select

ISP: Please select ISP

Type: Fault

Time: 2023-11-18 - 2023-11-18

Keywords: Fuzzy query is supported by A-IP, Z-I

TOP5 of Interrupt:

LL Name	A-Internet-IP	Z-Internet-IP	Cumulative Count	Durat

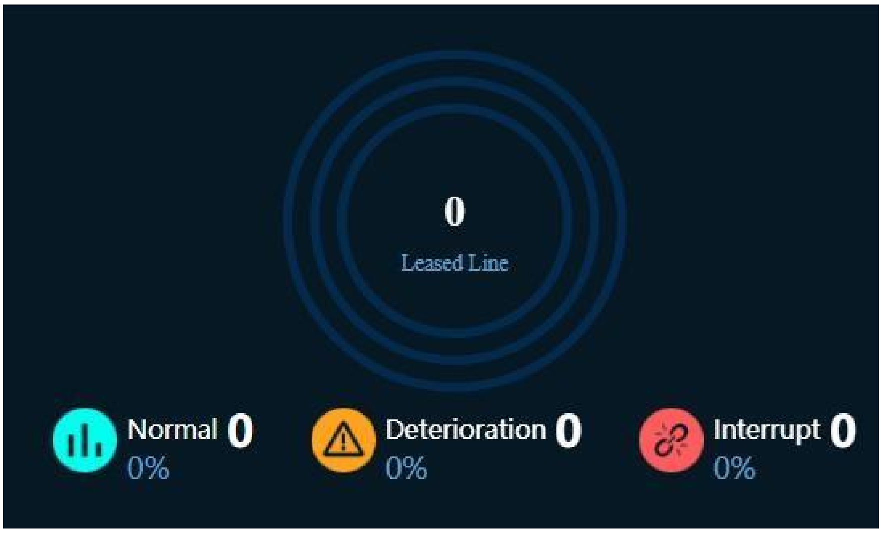
TOP5 of Deterioration:

LL Name	A-Internet-IP	Z-Internet-IP	Cumulative Count

Statistical Index

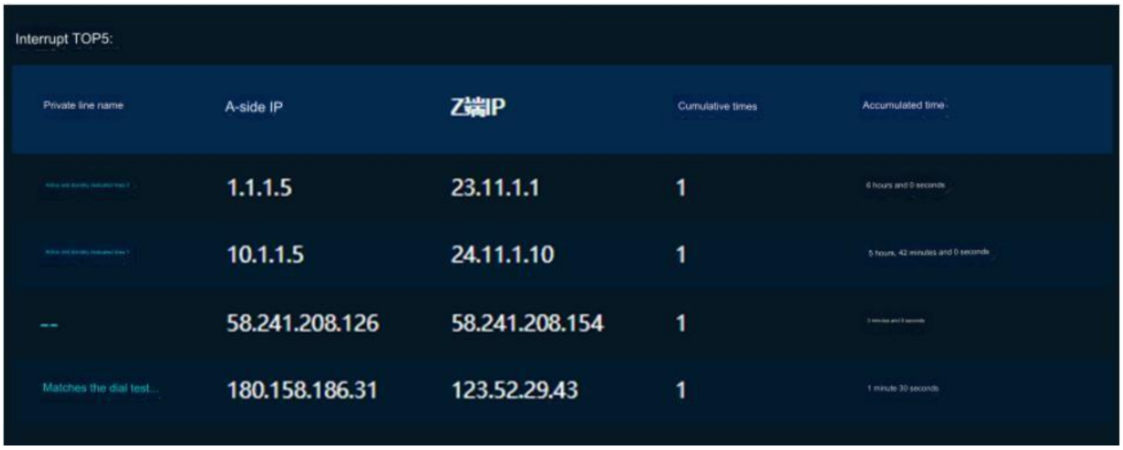
	Operations	LL Name	A-Internet-IP	Z-Internet-IP	ISP	Org	Availability	Excellent	Availability(Disclaimer)	Excellent(Disclai

- ➢ Graphical presentation of leased line statistics: ring graphs presenting total, outage, degraded, normal numbers and percentages;



- ➢ Based on leased line event/event statistical analysis, provide

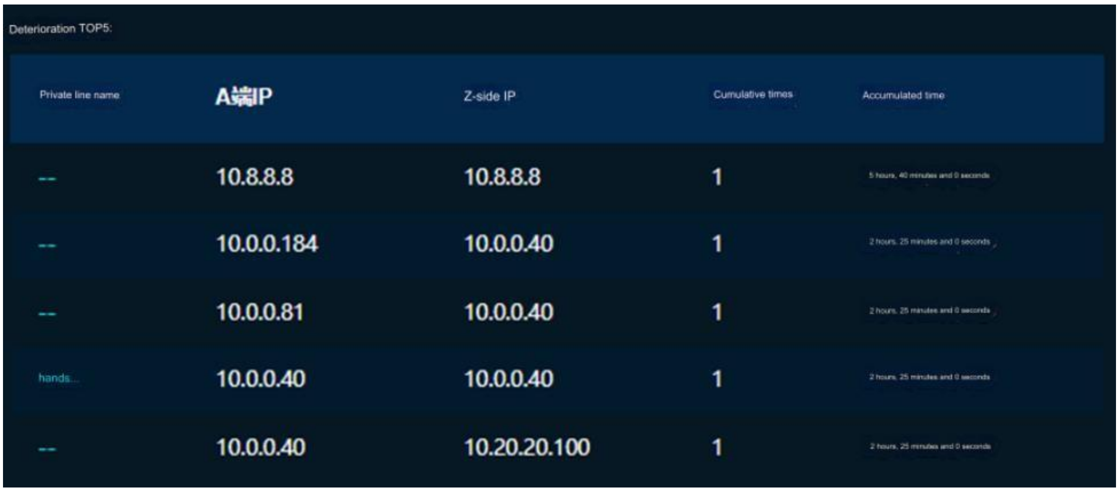
TOP5 ranking of leased line outages, list display: leased line name, A-side IP, Z-side IP, cumulative number of times, cumulative length of time;



Interrupt TOP5:

Private line name	A-side IP	Z端IP	Cumulative times	Accumulated time
[illegible]	1.1.1.5	23.11.1.1	1	6 hours and 0 seconds
[illegible]	10.1.1.5	24.11.1.10	1	5 hours, 42 minutes and 0 seconds
--	58.241.208.126	58.241.208.154	1	[illegible]
Matches the dial test...	180.158.186.31	123.52.29.43	1	1 minute 30 seconds

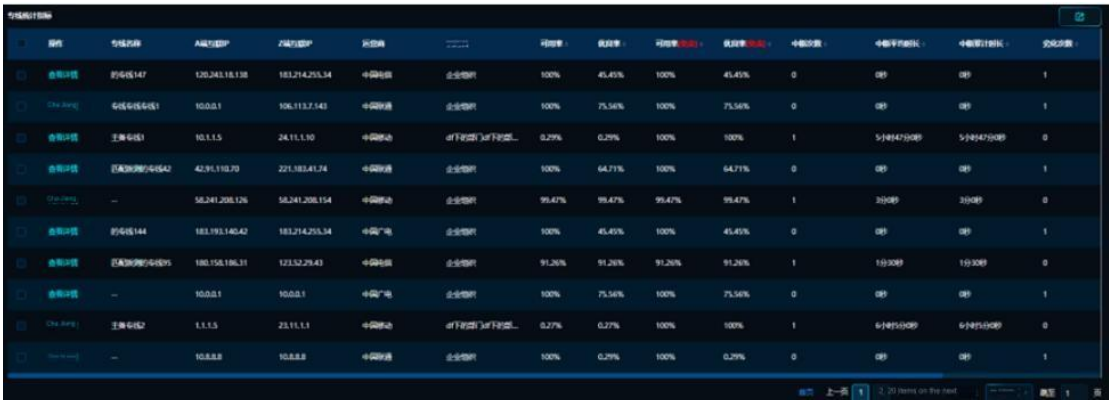
- ➢ Based on degradation event/fault statistical analysis, provide TOP5 rankings of leased line degradation times, list display: leased line name, A-side IP, Z-side IP, cumulative number of times, cumulative length of time;



Deterioration TOP5:

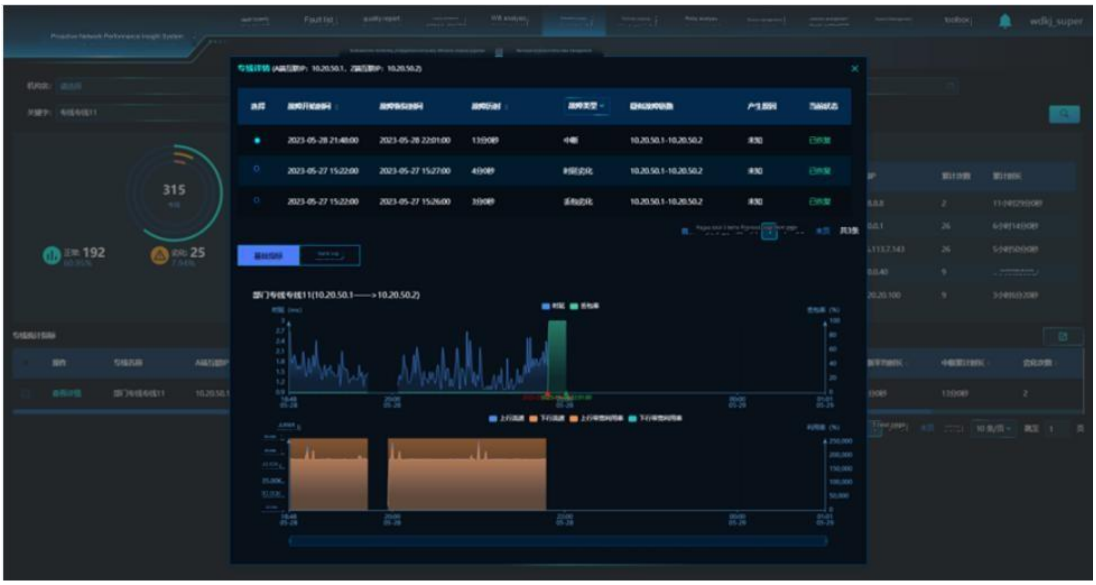
Private line name	A端IP	Z-side IP	Cumulative times	Accumulated time
--	10.8.8.8	10.8.8.8	1	5 hours, 40 minutes and 0 seconds
--	10.0.0.184	10.0.0.40	1	2 hours, 25 minutes and 0 seconds
--	10.0.0.81	10.0.0.40	1	2 hours, 25 minutes and 0 seconds
hands...	10.0.0.40	10.0.0.40	1	2 hours, 25 minutes and 0 seconds
--	10.0.0.40	10.20.20.100	1	2 hours, 25 minutes and 0 seconds

- ➢ Provides analysis of relay statistical indicators, including leased line information, outage information, delay degradation information, packet loss degradation information, availability rate, good rate, etc.;

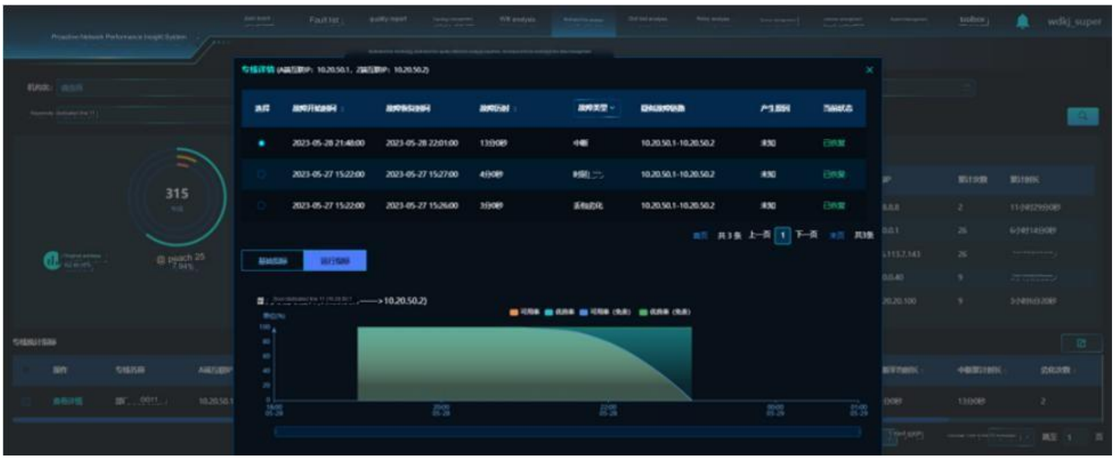


[illegible]	[illegible]	A[illegible]IP	Z[illegible]IP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]147	120.243.18.138	183.214.255.34	[illegible]	[illegible]	100%	45.45%	100%	45.45%	0	0秒	0秒	1
[illegible]	[illegible]1	10.0.0.1	106.113.7.143	[illegible]	[illegible]	100%	75.56%	100%	75.56%	0	0秒	0秒	1
[illegible]	[illegible]1	10.1.1.5	24.11.1.10	[illegible]	[illegible]	0.29%	0.29%	100%	100%	1	[illegible]	[illegible]	0
[illegible]	[illegible]42	42.91.110.70	221.183.41.74	[illegible]	[illegible]	100%	64.71%	100%	64.71%	0	0秒	0秒	1
[illegible]	--	58.241.208.126	58.241.208.154	[illegible]	[illegible]	99.47%	99.47%	99.47%	99.47%	1	[illegible]	[illegible]	0
[illegible]	[illegible]144	183.193.140.42	183.214.255.34	[illegible]	[illegible]	100%	45.45%	100%	45.45%	0	0秒	0秒	1
[illegible]	[illegible]95	180.158.186.31	123.52.29.43	[illegible]	[illegible]	91.26%	91.26%	91.26%	91.26%	1	[illegible]	[illegible]	0
[illegible]	--	10.0.0.1	10.0.0.1	[illegible]	[illegible]	100%	75.56%	100%	75.56%	0	0秒	0秒	1
[illegible]	[illegible]2	1.1.1.5	23.11.1.1	[illegible]	[illegible]	0.27%	0.27%	100%	100%	1	[illegible]	[illegible]	0
[illegible]	--	10.8.8.8	10.8.8.8	[illegible]	[illegible]	100%	0.29%	100%	0.29%	0	0秒	0秒	1

- ➢ Supports drill-down to view the details of poor-quality leased line information, displays a list of leased line-related events/failures, and supports switching between events/failures to view the trend graph of the raw indicators; clearly identifies the point in time when the event/failure started on the trend graph; and evaluates the overall operation of the leased line based on the event/failure.



[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
●	2023-05-28 21:40:00	2023-05-28 22:01:00	[illegible]	[illegible]	10.20.50.1-10.20.50.2	[illegible]	[illegible]
○	2023-05-27 15:22:00	2023-05-27 15:27:00	[illegible]	[illegible]	10.20.50.1-10.20.50.2	[illegible]	[illegible]
○	2023-05-27 15:22:00	2023-05-27 15:26:00	[illegible]	[illegible]	10.20.50.1-10.20.50.2	[illegible]	[illegible]



(A端互联IP：10.20.50.1，Z端互联IP：10.20.50.2)

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
●	2023-05-28 21:48:00	2023-05-28 22:01:00	[illegible]	[illegible]	10.20.50.1-10.20.50.2	[illegible]	[illegible]
○	2023-05-27 15:22:00	2023-05-27 15:27:00	[illegible]	[illegible]	10.20.50.1-10.20.50.2	[illegible]	[illegible]
○	2023-05-27 15:22:00	2023-05-27 15:26:00	[illegible]	[illegible]	10.20.50.1-10.20.50.2	[illegible]	[illegible]

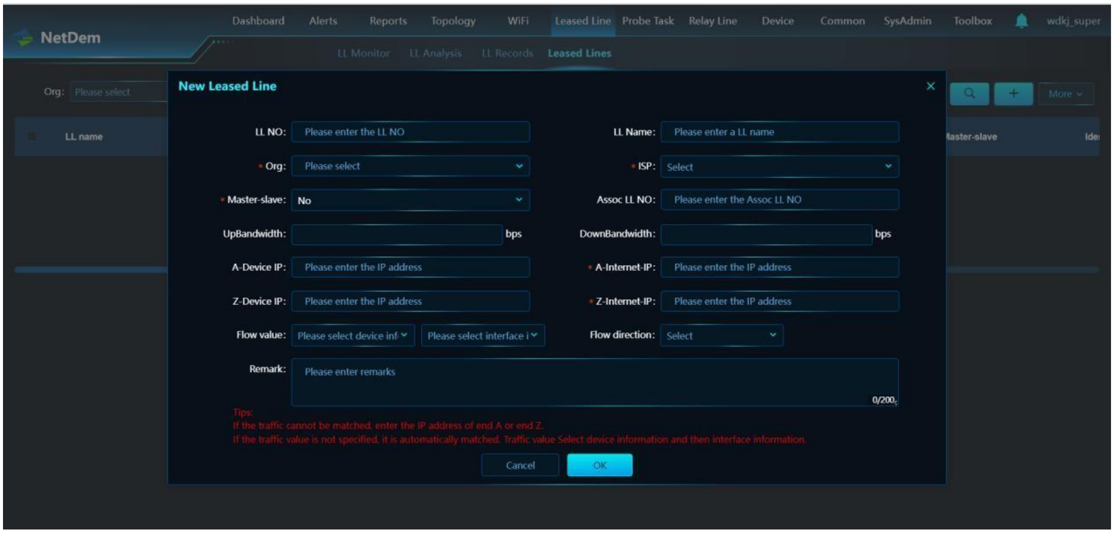
- Supports fault point location display;

2.3.6.4. Leased line Information Management

The system provides for the establishment of ledger information on leased lines of enterprises, centralized and unified management, as follows:

- Support the operation of adding, deleting, changing and checking the information of the leased line;
- Supports batch import and export of leased line data;
- Record leased line information data including: leased line number, leased line name, affiliation, operator, A-side device IP, A-side interconnection IP, Z-side device IP, Z-side interconnection IP, master-standby relationship, associated leased line number, upstream bandwidth, downstream bandwidth, identification tasks and notes, in which the identification tasks are used to automatically identify leased line nodes in the path and associated tasks for statistics on the quality of leased lines;
- If any field of A-side interconnection IP and Z-side interconnection IP is empty, it supports automatic supplementation by the rule of "Odd + Even -", and supports modification;

- Uplink bandwidth, downlink bandwidth is not all empty, each other automatically complement each other, support input K, M, G, T automatic identification;
- Use system templates or custom templates to map matches during batch imports;



New Leased Line

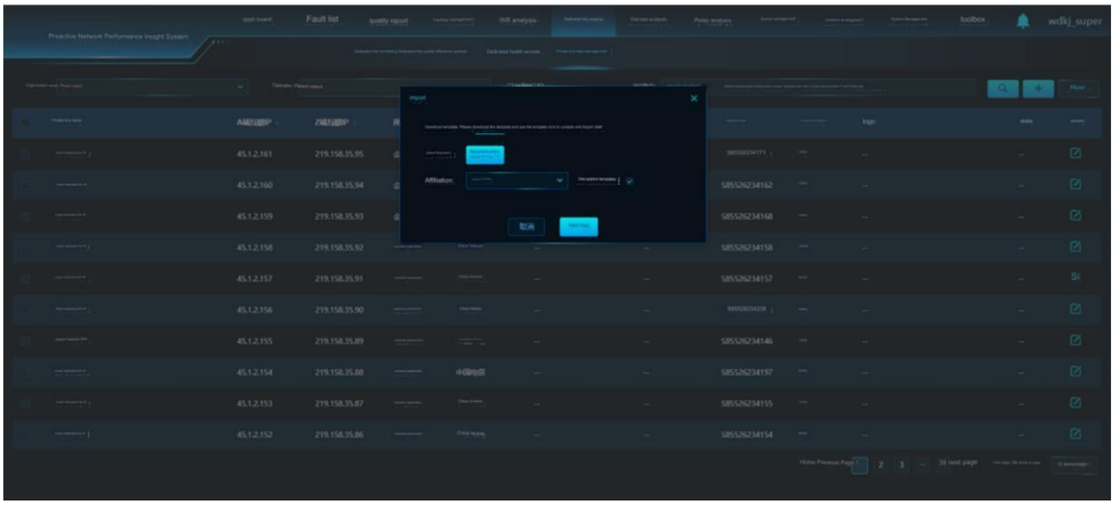
LL NO: Please enter the LL NO
LL Name: Please enter a LL name
* Org: Please select
* ISP: Select
* Master-slave: No
Assoc LL NO: Please enter the Assoc LL NO
UpBandwidth: bps
DownBandwidth: bps
A-Device IP: Please enter the IP address
* A-Internet-IP: Please enter the IP address
Z-Device IP: Please enter the IP address
* Z-Internet-IP: Please enter the IP address
Flow value: Please select device inf Please select interface i
Flow direction: Select
Remark: Please enter remarks 0/200

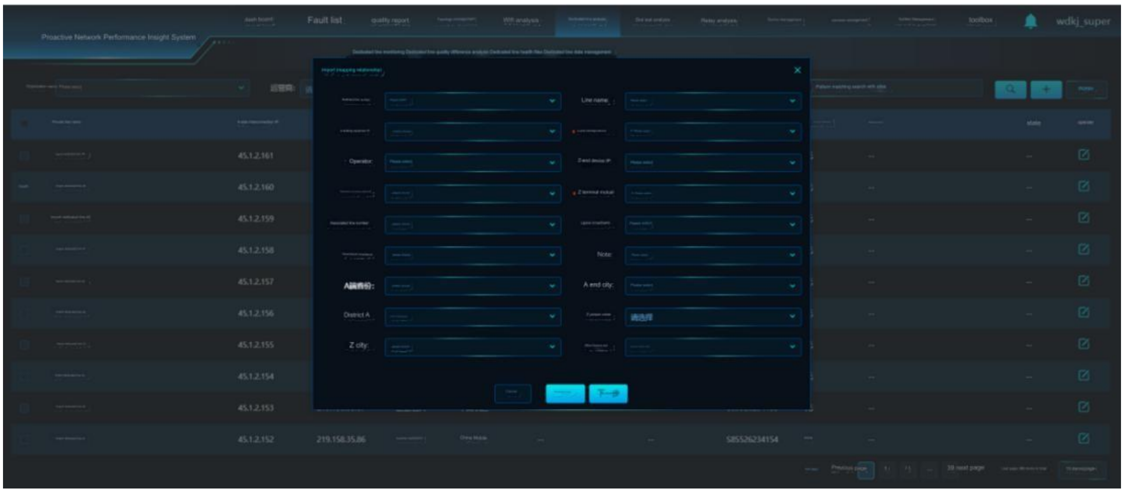
Tips:
If the traffic cannot be matched, enter the IP address of end A or end Z.
If the traffic value is not specified, it is automatically matched. Traffic value Select device information and then interface information.

Cancel OK

New Creation Interface

<span style="color:red">Note:</span> When master-standby relationship = none, the associated leased line number is automatically populated to match the leased line number;





Import Interface

2.3.7. Probe Test Analysis

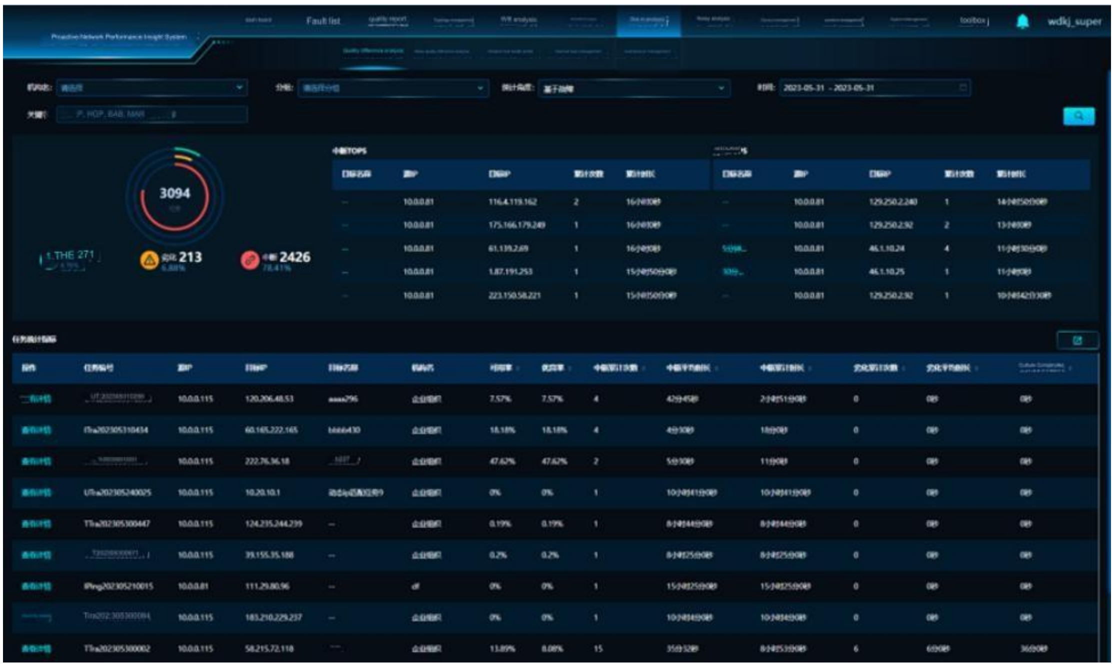
The system establishes probe test tasks for each primary business path of the enterprise's network, and creates quality health records for these probe test tasks. It can promptly identify paths in a suboptimal health state, pinpoint areas of quality degradation, allowing customers to proactively take maintenance measures for suboptimal networks and carry out timely rectifications. Specific functionalities include: Probe Test quality analysis, Probe Test quality reports, Probe Test health records, and Probe Test task management.

2.3.7.1. Probe Test Quality Analysis

- Provide an Overview of Poor-Quality Probe test tasks;
- Provide Top N Information for Interrupted Probe test tasks;
- Provides TOPN for degradation dialing tasks, where TOPN information includes: task name, source IP, target IP, cumulative number of times, cumulative length of time.;
- Provides a detailed list of poor quality tasks, including task number, source IP, target IP, target name, organization name, recent event

type, availability rate, good rate, recent event time, status, cumulative length of outage, cumulative length of deterioration;

- Detailed lists can be further drilled down to show details of each event/fault (including: start time, elapsed time, type, suspected faulty node, cause, current status), end-to-end topology location analysis and raw metrics trending graphs, with degraded link segments highlighted in yellow and interrupted link segments highlighted in red with a forked X. In the trending graphs, the point in time at which the fault was generated is identified by a small red triangle △, and the point in time at which the interruption was restored is identified by a small green triangle △;
- The trend graph supports dragging to view the original metric trends within the time range from 3 hours before the fault occurrence to 3 hours after the interruption recovery (or until the current system time if not recovered). Original metrics include latency, packet loss rate, inbound flow rate, and outbound flow rate. Adaptive display for units (K/M/G/T) is provided for inbound and outbound flow rates;

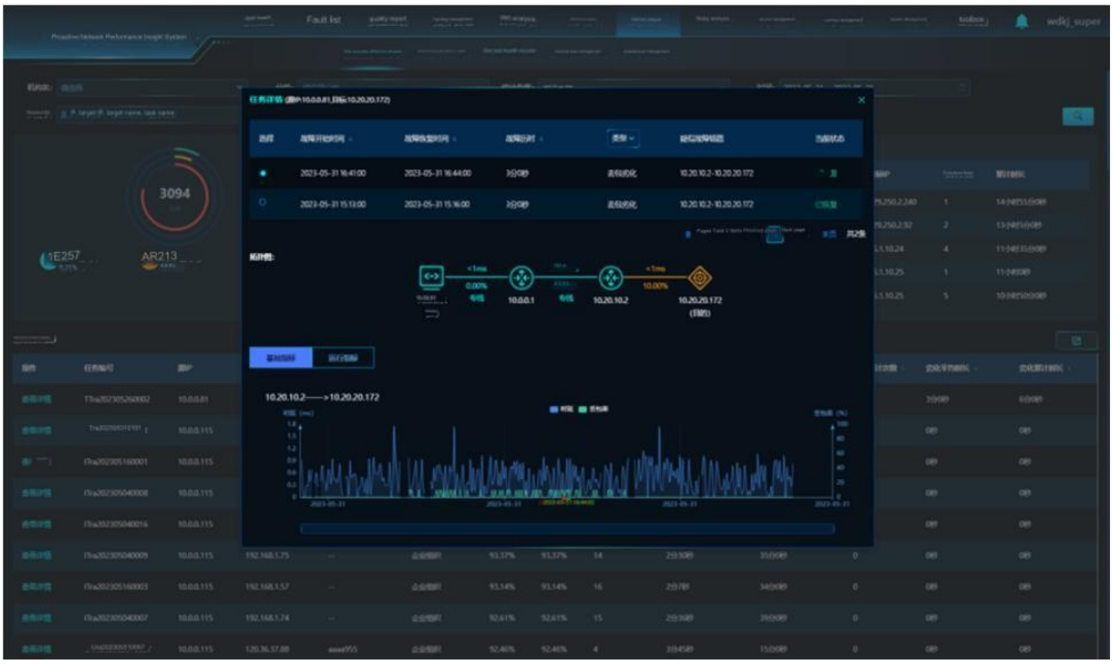


2023-05-31 - 2023-05-31

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
—	10.0.0.81	116.4.119.162	2	[illegible]
—	10.0.0.81	175.166.179.249	1	[illegible]
—	10.0.0.81	61.139.2.69	1	[illegible]
—	10.0.0.81	1.87.191.253	1	[illegible]
—	10.0.0.81	223.150.58.221	1	[illegible]

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
—	10.0.0.81	129.250.2.240	1	[illegible]
—	10.0.0.81	129.250.2.92	2	[illegible]
[illegible]	10.0.0.81	46.1.10.24	4	[illegible]
[illegible]	10.0.0.81	46.1.10.25	1	[illegible]
—	10.0.0.81	129.250.2.92	1	[illegible]

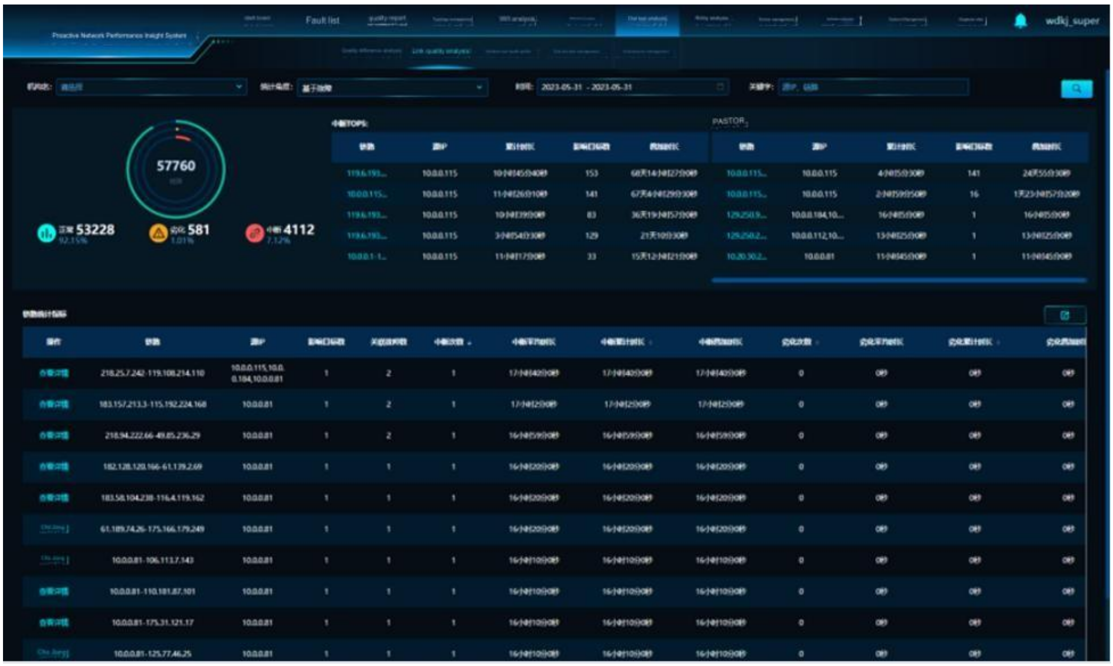
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	10.0.0.115	120.206.48.53	aaaa296	[illegible]	7.57%	7.57%	4	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	ITa202305310434	10.0.0.115	60.165.222.165	bbbb430	[illegible]	18.18%	18.18%	4	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	[illegible]	10.0.0.115	222.76.36.18	[illegible]	[illegible]	47.62%	47.62%	2	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	UTra202305240025	10.0.0.115	10.20.10.1	[illegible]	[illegible]	0%	0%	1	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	TTra202305300447	10.0.0.115	124.235.244.239	—	[illegible]	0.19%	0.19%	1	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	[illegible]	10.0.0.115	39.155.35.188	—	[illegible]	0.2%	0.2%	1	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	IPing202305210015	10.0.0.81	111.29.80.96	—	df	0%	0%	1	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	[illegible]	10.0.0.115	183.210.229.237	—	[illegible]	0%	0%	1	[illegible]	[illegible]	0	[illegible]	[illegible]
[illegible]	TTra202305300002	10.0.0.115	58.215.72.118	—	[illegible]	13.89%	8.08%	15	[illegible]	[illegible]	6	[illegible]	[illegible]

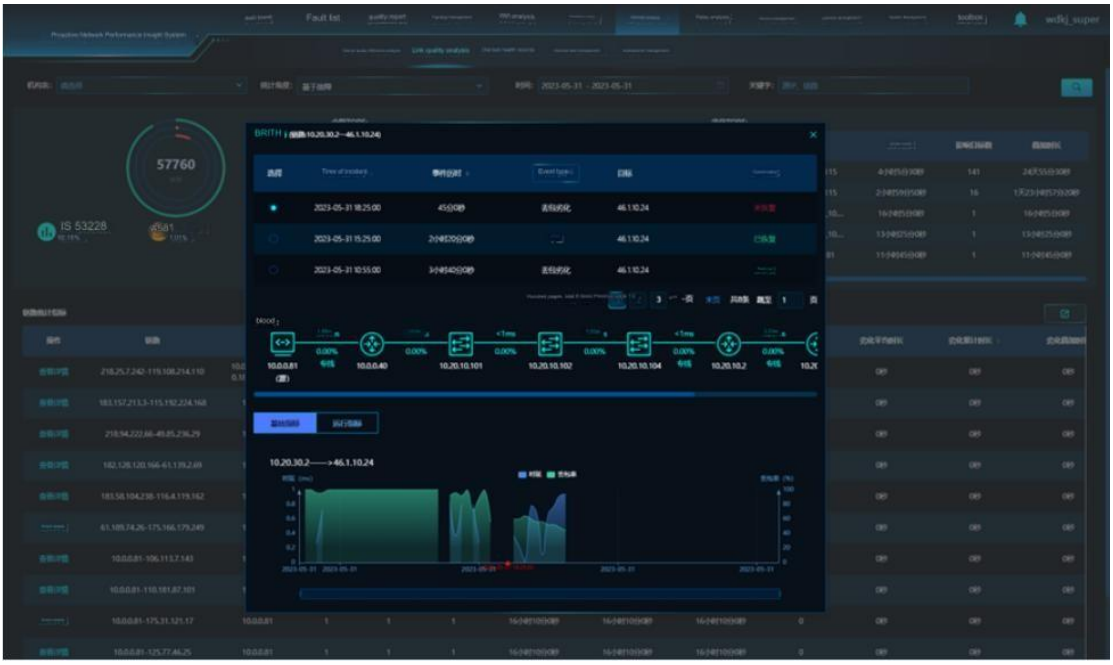


2.3.7.2. Link Quality Analysis

- Provides an overall view of the quality difference link;
- Provides broken link TOPN, degraded link TOPN;
- Provides a detailed list of poor-quality links, which can be further drilled down to show details of each event/fault (including: start time, elapsed time, type, suspected faulty node, cause, and current status), end-to-end topology positioning analysis, and raw metrics trending graphs, with degraded link segments highlighted in yellow, and interrupted link segments highlighted in red with a cross-hair mark, and small red triangles △ marking the point in time when the fault was generated, and small green triangles △ marking the point in time when the interruption was restored, in the trending graphs;
- The trend graph supports dragging to view the original metric trends within the time range from 3 hours before the fault occurrence to 3 hours after the interruption recovery (or until the current system time if not recovered). Original metrics include latency, packet loss rate, inbound flow rate, and outbound flow rate. Adaptive

display for units (K/M/G/T) is provided for inbound and outbound flow rates;



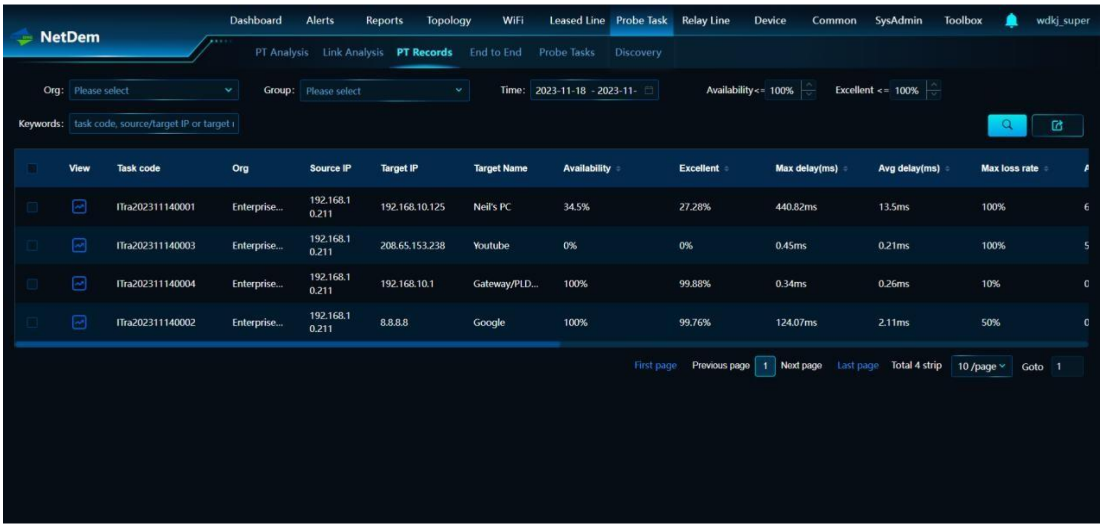


2.3.7.3. Probe Test Health Records

- Supports combined queries by organization name, time period, availability, excellence and keywords;
- Keyword support fuzzy matching query by task number, source/target

IP and target name;

- Supports selecting export and exporting all the result records retrieved by query conditions;
- The result records include: task number, organization name, source IP, target IP, target name, availability rate, good rate, delay maximum, delay average, packet loss maximum, packet loss average, outage cumulative duration, degradation cumulative duration;
- Provides metrics trend charts with adaptive granularity according to the time range selected from the TAB page, and supports synchronous switching between the granularity by scrolling the mouse wheel to view the details of the associated metrics, which include latency, packet loss, inbound flow rate and outbound flow rate, and the outbound/inbound flow rate supports the adaptive display between K/M/G/T units;



Org: Please select
Group: Please select
Time: 2023-11-18 - 2023-11-
Availability<= 100%
Excellent <= 100%
Keywords: task code, source/target IP or target i

□	View	Task code	Org	Source IP	Target IP	Target Name	Availability	Excellent	Max delay(ms)	Avg delay(ms)	Max loss rate	A
□		ITra202311140001	Enterprise...	192.168.10.211	192.168.10.125	Neil's PC	34.5%	27.28%	440.82ms	13.5ms	100%	6
□		ITra202311140003	Enterprise...	192.168.10.211	208.65.153.238	Youtube	0%	0%	0.45ms	0.21ms	100%	5
□		ITra202311140004	Enterprise...	192.168.10.211	192.168.10.1	Gateway/PLD...	100%	99.88%	0.34ms	0.26ms	10%	0
□		ITra202311140002	Enterprise...	192.168.10.211	8.8.8.8	Google	100%	99.76%	124.07ms	2.11ms	50%	0

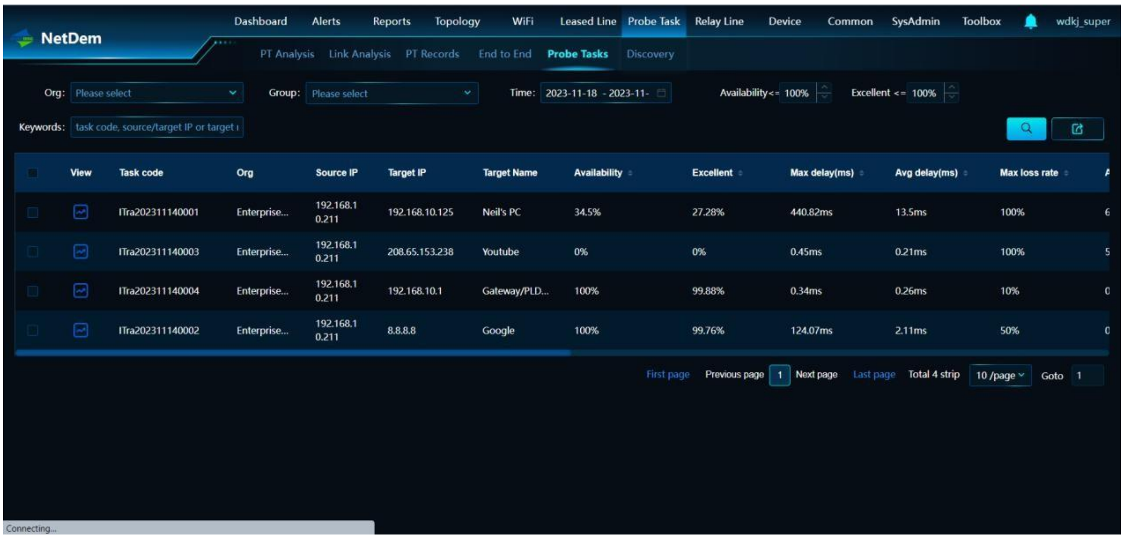
First page Previous page 1 Next page Last page Total 4 strip 10 /page Goto 1

2.3.7.4. Probe Test Task Management

The probing task supports a variety of dialing protocols, supports the configuration of dialing frequency, number of packets, packet size, which can be selected according to the actual needs, after configuration, the probe sends probe packets to the target IP, and sends the returned probe results to the management platform, which conducts statistics and analysis of the probing behavior, and the network events that can be detected include: interruptions, delay deterioration, packet loss deterioration, and route fluctuation, as follows:

- Supports UDP trace, ICMP trace, TCP trace and ICMP ping;
- Supports adding, deleting, changing and checking of dialing tasks, and automatically performs fixed dialing according to the rules and generates the dialing path after the task is created, in which the current online path is marked in green;
- Supports the creation of dynamic IP dialing tasks, correlating the data collected by SNMP to achieve the tracking and monitoring of dynamic IP;
- The task creation interface mainly includes information: dialing type, probe IP and port, target IP and port, target name, affiliation, alarm parameter settings and dialing parameter settings, of which the dialing parameters are the starting TTL and the number of TTL-limited hops;
- Alarm parameters are: interrupt generation threshold, delay degradation generation threshold, packet loss degradation generation threshold, route fluctuation alarm switch control;
- Supports batch operation, including: import, suspend, start, alarm setting, delete and export;
- Supports viewing the raw metrics chart of tasks and associated paths, including latency, packet loss rate, inbound flow rate, outbound flow rate, of which the outbound/inbound flow rate supports adaptive display between K/M/G/T units;
- Trend charts are presented at an adaptive granularity based on the selected timeframe, with support for switching between granularities by scrolling the mouse wheel to view the details of

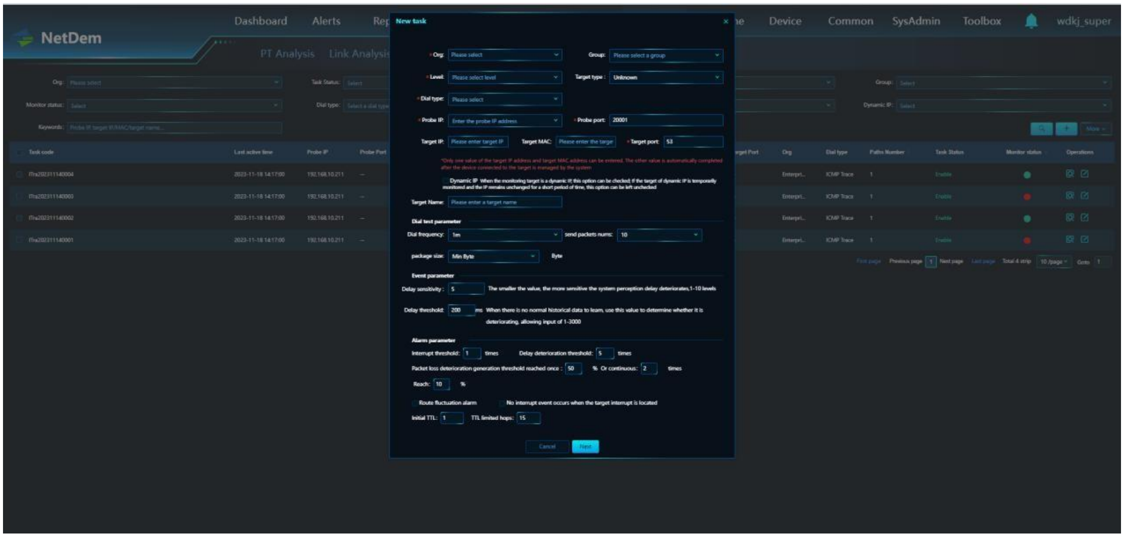
the metrics;



Org: Please select
Group: Please select
Time: 2023-11-18 - 2023-11-
Availability<= 100%
Excellent <= 100%
Keywords: task code, source/target IP or target

□	View	Task code	Org	Source IP	Target IP	Target Name	Availability	Excellent	Max delay(ms)	Avg delay(ms)	Max loss rate	A
□		ITra202311140001	Enterprise...	192.168.1 0.211	192.168.10.125	Neil's PC	34.5%	27.28%	440.82ms	13.5ms	100%	6
□		ITra202311140003	Enterprise...	192.168.1 0.211	208.65.153.238	Youtube	0%	0%	0.45ms	0.21ms	100%	5
□		ITra202311140004	Enterprise...	192.168.1 0.211	192.168.10.1	Gateway/PLD...	100%	99.88%	0.34ms	0.26ms	10%	0
□		ITra202311140002	Enterprise...	192.168.1 0.211	8.8.8.8	Google	100%	99.76%	124.07ms	2.11ms	50%	0

First page Previous page 1 Next page Last page Total 4 strip 10 /page Goto 1



New task

* Org: Please select
Group: Please select a group
* Level: Please select level
Target type : Unknown
* Dial type: Please select
* Probe IP: Enter the probe IP address
* Probe port: 20001
Target IP: Please enter target IP
Target MAC: Please enter the targe
* Target port: 53

*Only one value of the target IP address and target MAC address can be entered. The other value is automatically completed after the device connected to the target is managed by the system

□ Dynamic IP When the monitoring target is a dynamic IP, this option can be checked; If the target of dynamic IP is temporarily monitored and the IP remains unchanged for a short period of time, this option can be left unchecked

Target Name: Please enter a target name

Dial test parameter

Dial frequency: 1m
send packets nums: 10
package size: Min Byte Byte

Event parameter

Delay sensitivity : 5 The smaller the value, the more sensitive the system perception delay deteriorates,1-10 levels

Delay threshold: 200 ms When there is no normal historical data to learn, use this value to determine whether it is deteriorating, allowing input of 1-3000

Alarm parameter

Interrupt threshold: 1 times
Delay deterioration threshold: 5 times
Packet loss deterioration generation threshold reached once : 50 % Or continuous: 2 times
Reach: 10 %

□ Route fluctuation alarm
□ No interrupt event occurs when the target interrupt is located

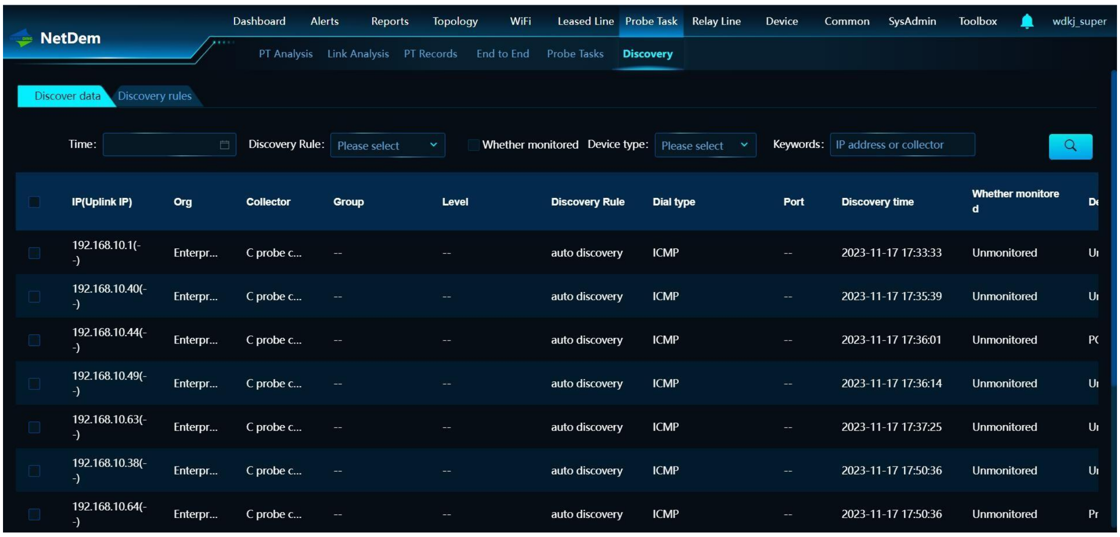
Initial TTL: 1
TTL limited hops: 15

Cancel Next

2.3.7.5. Automatic Discovery

2.3.7.5.1. Discovery Data

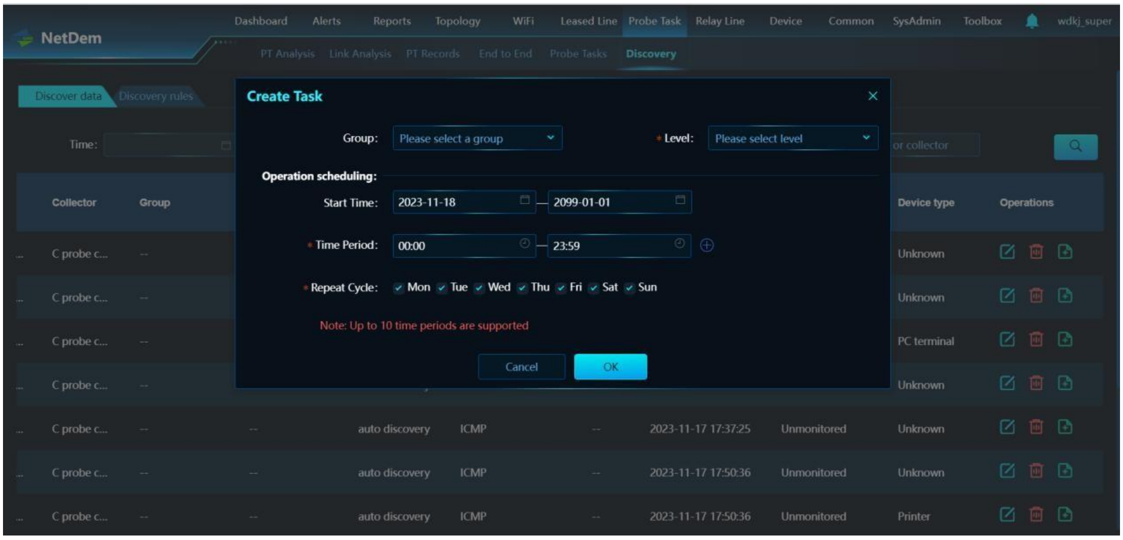
Supports list view and management of discovered data;



Time: Discovery Rule: Please select ☐ Whether monitored Device type: Please select Keywords: IP address or collector

☐	IP(Uplink IP)	Org	Collector	Group	Level	Discovery Rule	Dial type	Port	Discovery time	Whether monitored	De
☐	192.168.10.1(--)	Enterpr...	C probe c...	--	--	auto discovery	ICMP	--	2023-11-17 17:33:33	Unmonitored	Ur
☐	192.168.10.40(--)	Enterpr...	C probe c...	--	--	auto discovery	ICMP	--	2023-11-17 17:35:39	Unmonitored	Ur
☐	192.168.10.44(--)	Enterpr...	C probe c...	--	--	auto discovery	ICMP	--	2023-11-17 17:36:01	Unmonitored	PC
☐	192.168.10.49(--)	Enterpr...	C probe c...	--	--	auto discovery	ICMP	--	2023-11-17 17:36:14	Unmonitored	Ur
☐	192.168.10.63(--)	Enterpr...	C probe c...	--	--	auto discovery	ICMP	--	2023-11-17 17:37:25	Unmonitored	Ur
☐	192.168.10.38(--)	Enterpr...	C probe c...	--	--	auto discovery	ICMP	--	2023-11-17 17:50:36	Unmonitored	Ur
☐	192.168.10.64(--)	Enterpr...	C probe c...	--	--	auto discovery	ICMP	--	2023-11-17 17:50:36	Unmonitored	Pr

Supports rapid creation of discovery data from uncreated tasks as dial-a-test tasks;



Create Task

Group: Please select a group

* Level: Please select level

Operation scheduling:

Start Time: 2023-11-18 — 2099-01-01

* Time Period: 00:00 — 23:59

* Repeat Cycle: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

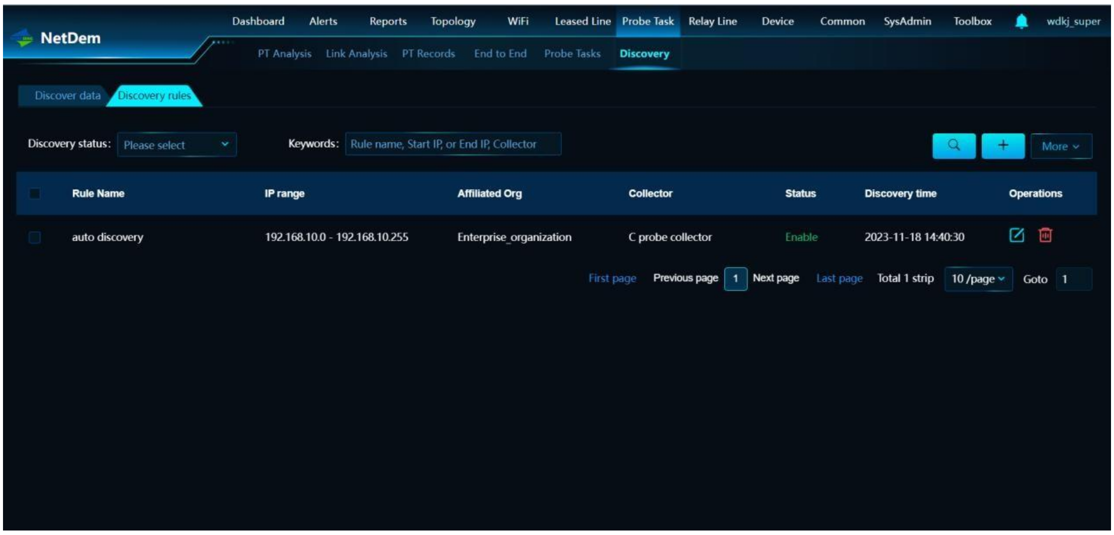
Note: Up to 10 time periods are supported

2.3.7.5.2. Discovery Rules

- ➢ Support for Automatic Discovery Rule Configuration Based on IP Range;
- ➢ Support for Sequentially Scanning IP for Online Status and

Automatically Identifying Device Types;

- Support for Automatically Creating Probe test tasks for Discovered IPs;
- Automatic Discovery and Monitoring for Any Valid IP Address.
- Support for Multiple Device Types.
- Comes with inbuilt device categories such as servers, routers, switches, firewalls, wireless, etc. which are classified into different categories.

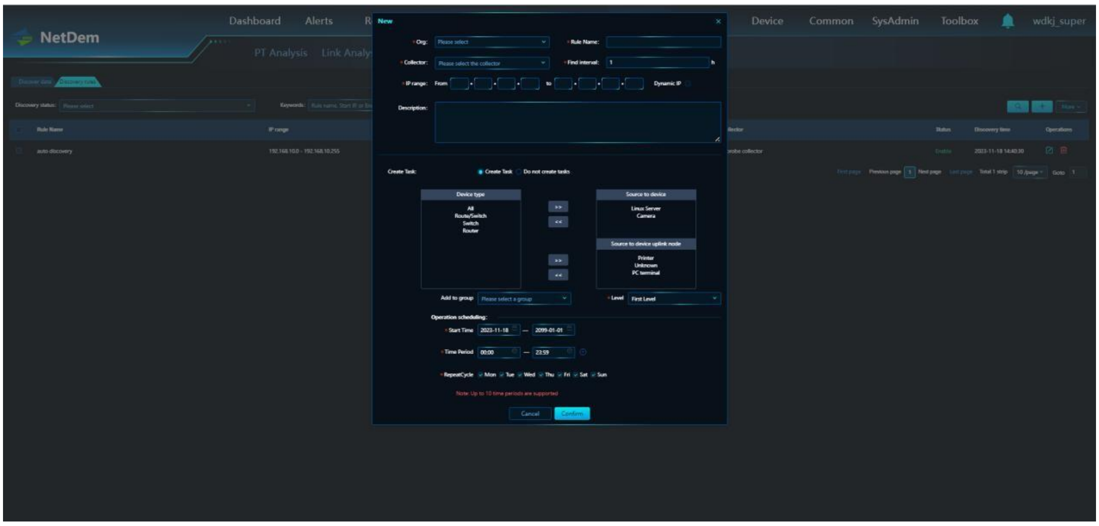


Discovery status: Please select

Keywords: Rule name, Start IP, or End IP, Collector

Rule Name	IP range	Affiliated Org	Collector	Status	Discovery time	Operations
auto discovery	192.168.10.0 - 192.168.10.255	Enterprise_organization	C probe collector	Enable	2023-11-18 14:40:30	

First page Previous page 1 Next page Last page Total 1 strip 10 /page Goto 1



* Org: Please select

* Rule Name:

* Collector: Please select the collector

* Find interval: 1 h

* IP range: From . . . to . . . Dynamic IP

Description:

Create Task: ● Create Task ○ Do not create tasks

Device type	Source to device
All Route/Switch Switch Router	Linux Server Camera
	Source to device uplink node
	Printer Unknown PC terminal

Add to group: Please select a group

* Level: First Level

Operation scheduling:

* Start Time 2023-11-18 — 2099-01-01

* Time Period 00:00 — 23:59

* RepeatCycle ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

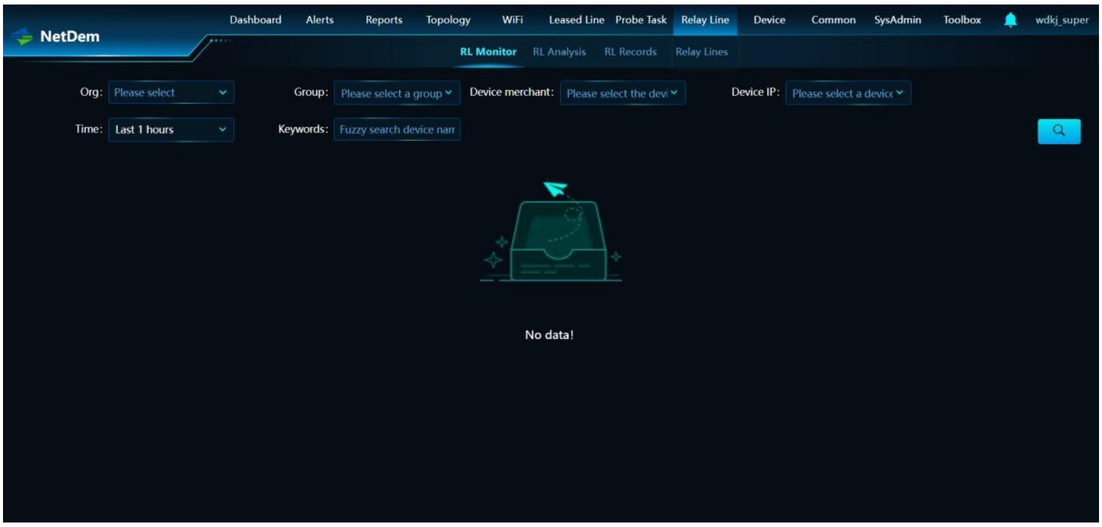
Note: Up to 10 time periods are supported

2.3.8. Relay Analysis

Based on SNMP protocol to achieve automatic discovery of relay, through the configuration of the relevant collection tasks to achieve the collection of relay monitoring indicators, relay delay, packet loss, interrupt monitoring, and through the graphical real-time presentation of the relay state, performance, and at the same time, the analysis of historical performance data, the overall quality of the poor relay focus on the analysis of the overall health of the relay file generation. On the one hand, let the user understand the relay real-time monitoring status, on the other hand, let the user know the current relay overall health status.

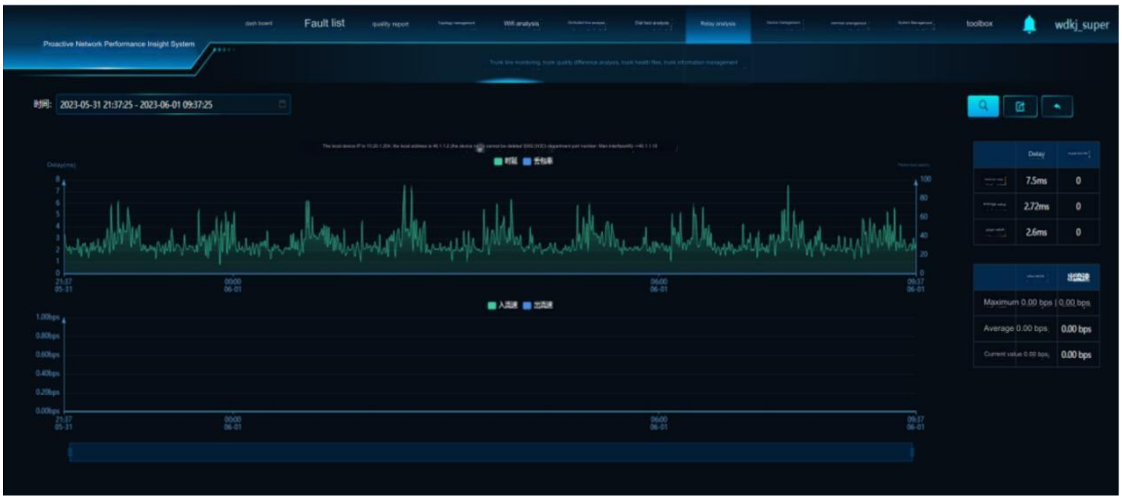
2.3.8.1. Relay Line Monitoring

Thumbnail real-time presentation of relay delay, packet loss rate trend graph, inbound flow rate, outbound flow rate trend graph; at the same time, you can drill down to view the details of relay data, including: delay/packet loss rate trend graph, inbound flow rate/outbound flow rate trend graph, as well as delay/packet loss rate, inbound flow rate/outbound flow rate, the maximum, minimum, current value.



Org: Please select
Group: Please select a group
Device merchant: Please select the devi
Device IP: Please select a device
Time: Last 1 hours
Keywords: Fuzzy search device nan

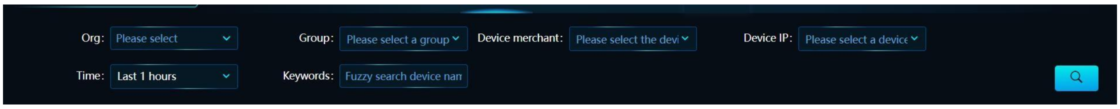
No data!



时间: 2023-05-31 21:37:25 - 2023-06-01 09:37:25

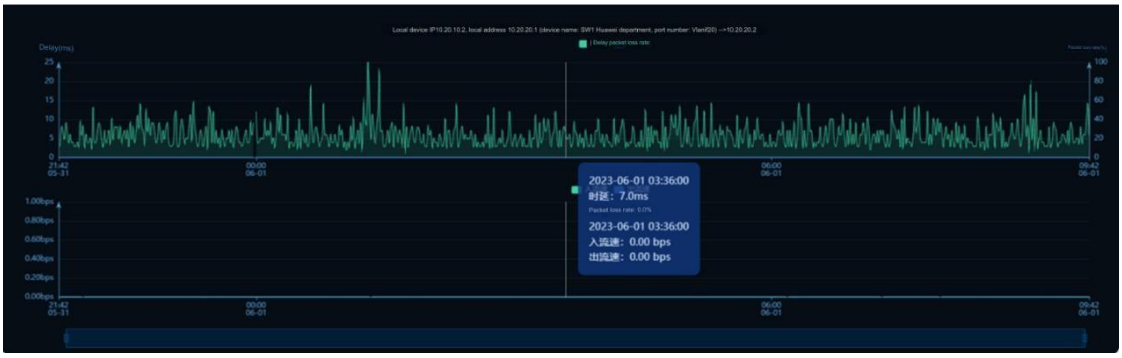
To make it easier to find and view data, the following functions are also provided:

- ➢ Thumbnail interface supports combined query retrieval display by organization name, equipment vendor, equipment IP, time window, keywords (fuzzy matching query by relay name, local/counter address, local/terminal alias is supported)



Org: Please select
Group: Please select a group
Device merchant: Please select the devi
Device IP: Please select a device
Time: Last 1 hours
Keywords: Fuzzy search device nan

- ➢ Supports mouse positioning to view data corresponding to a point in time, including (date + time, delay value, packet loss rate value) or (date + time, inbound traffic value, outbound traffic value) ;

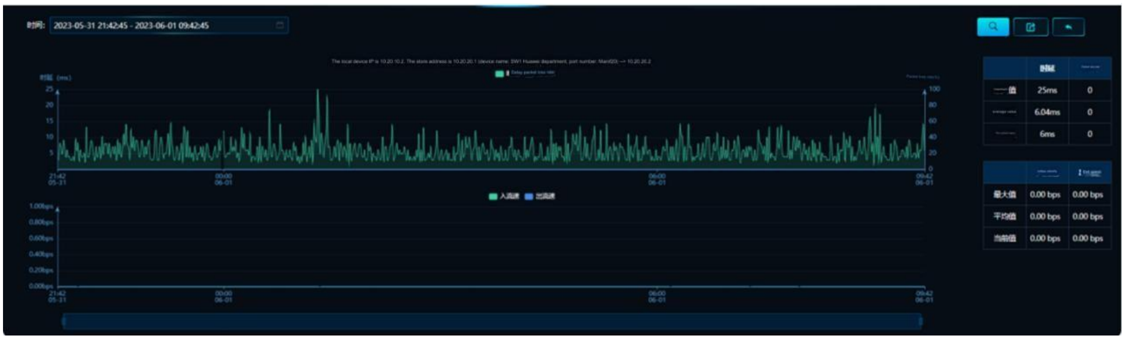


Local device IP10.20.10.2, local address 10.20.20.1 (device name: SW1 Huawei department, port number: Vlanif20) -->10.20.20.2

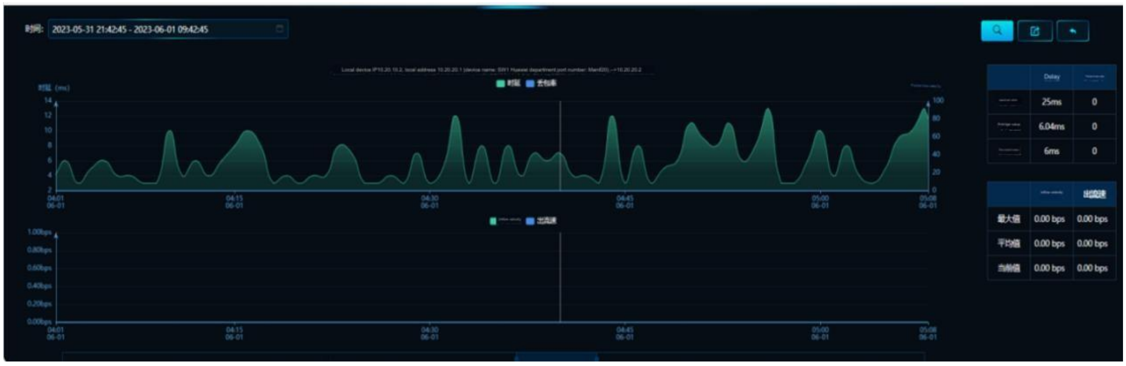
2023-06-01 03:36:00
时延：7.0ms
Packet loss rate: 0.0%
2023-06-01 03:36:00
入流速：0.00 bps
出流速：0.00 bps

- ➢ Supports automatic refreshing of data display at regular intervals when the page is open;

- The detail page loads 12 hours of data by default, and supports the display of data in the selected time period;



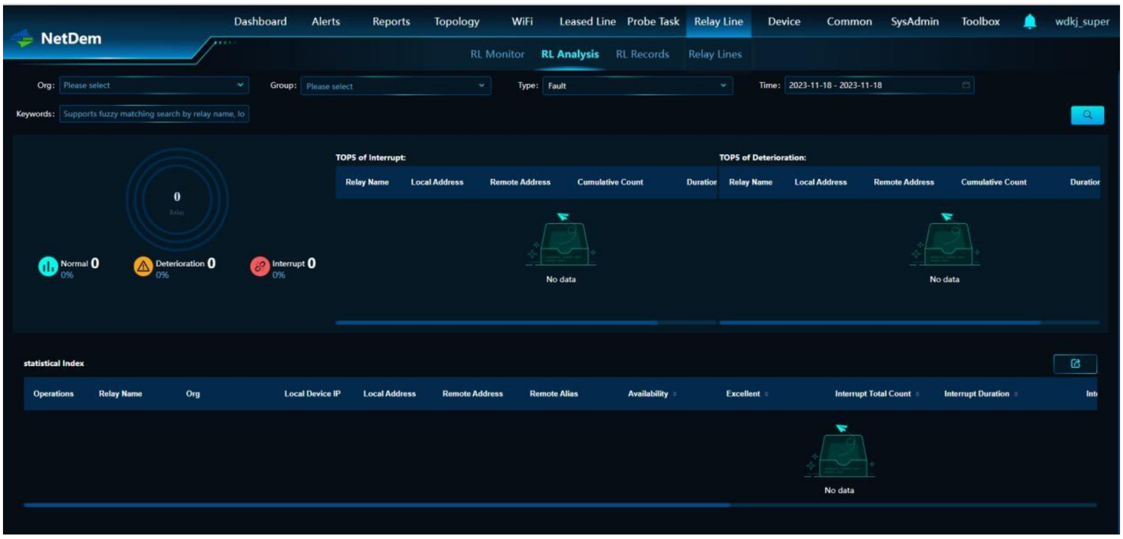
- ➢ The graphical window of the detail page supports drag-and-drop and scrolling to adjust the range of data displayed;



- ➢ Support for Data Export;

2.3.8.2. Relay Quality Analysis

The system automatically collects data for relays and performs statistical analysis on the quality issues of relays. By default, it analyzes the data for all relays on the current day. It also supports the selection of organizations, operators, time periods, and keywords to specify the data range for statistical analysis. The system provides a summary of quality analysis information:



Org: Please select

Group: Please select

Type: Fault

Time: 2023-11-18 - 2023-11-18

Keywords: Supports fuzzy matching search by relay name, lo

TOP5 of Interrupt:

Relay Name	Local Address	Remote Address	Cumulative Count	Duratior

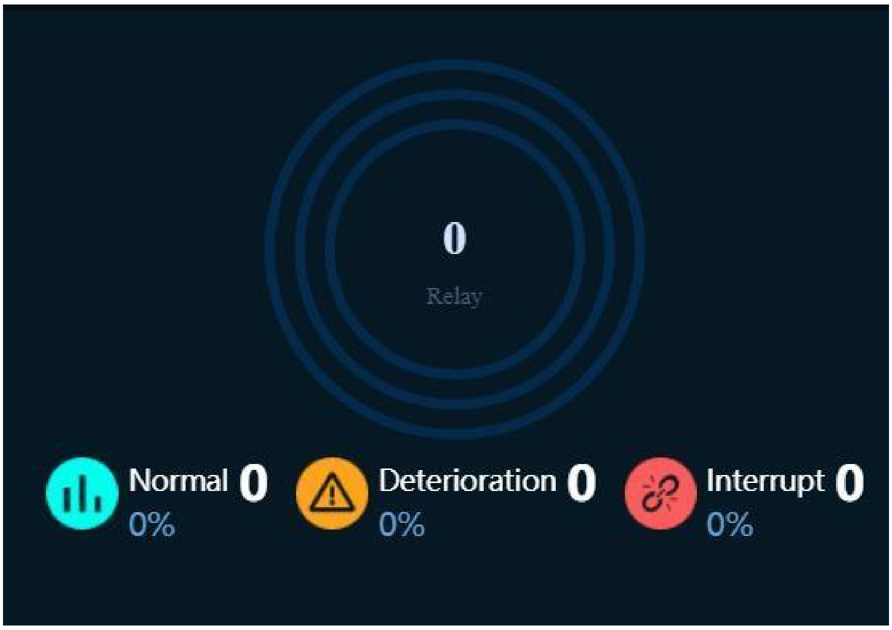
TOP5 of Deterioration:

Relay Name	Local Address	Remote Address	Cumulative Count	Duratior

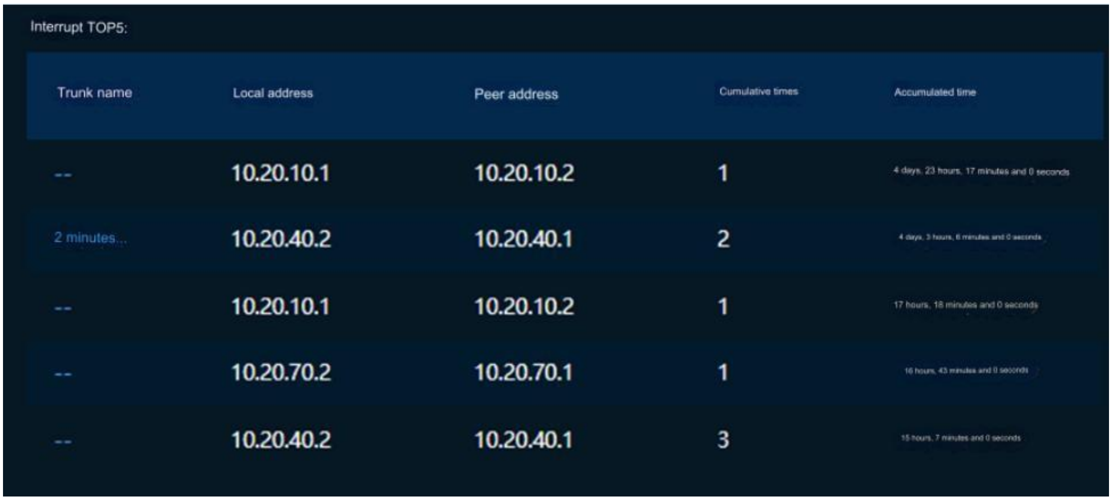
statistical Index

Operations	Relay Name	Org	Local Device IP	Local Address	Remote Address	Remote Alias	Availability	Excellent	Interrupt Total Count	Interrupt Duration	Int

- Graphical presentation of relay view statistics: ring graph presenting the total number, number and percentage of outages, degradations, and normalities;



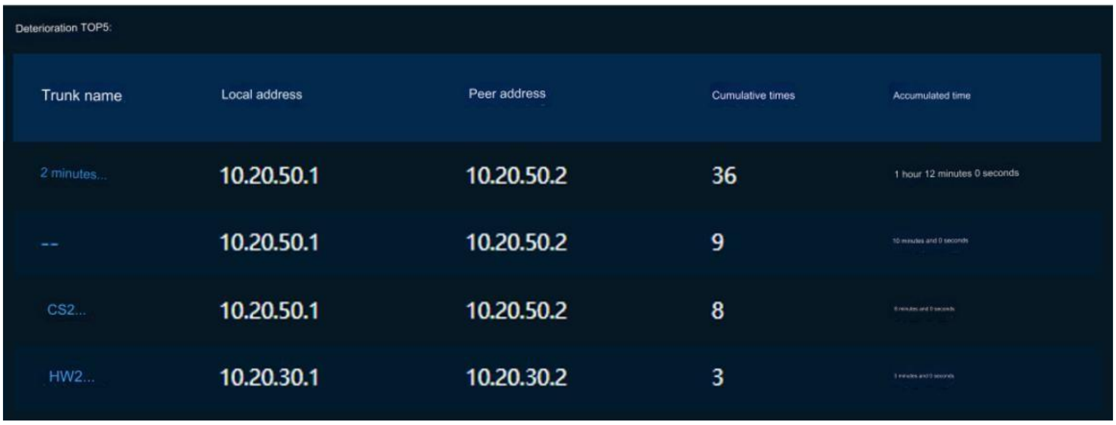
- Based on the statistical analysis of interruption events/faults, provide TOP5 ranking of relay interruption times, with the list displaying: relay name, local address, peer address, cumulative number of times and cumulative duration;



Interrupt TOP5:

Trunk name	Local address	Peer address	Cumulative times	Accumulated time
--	10.20.10.1	10.20.10.2	1	4 days, 23 hours, 17 minutes and 0 seconds
2 minutes...	10.20.40.2	10.20.40.1	2	4 days, 3 hours, 6 minutes and 0 seconds
--	10.20.10.1	10.20.10.2	1	17 hours, 18 minutes and 0 seconds
--	10.20.70.2	10.20.70.1	1	16 hours, 43 minutes and 0 seconds
--	10.20.40.2	10.20.40.1	3	15 hours, 7 minutes and 0 seconds

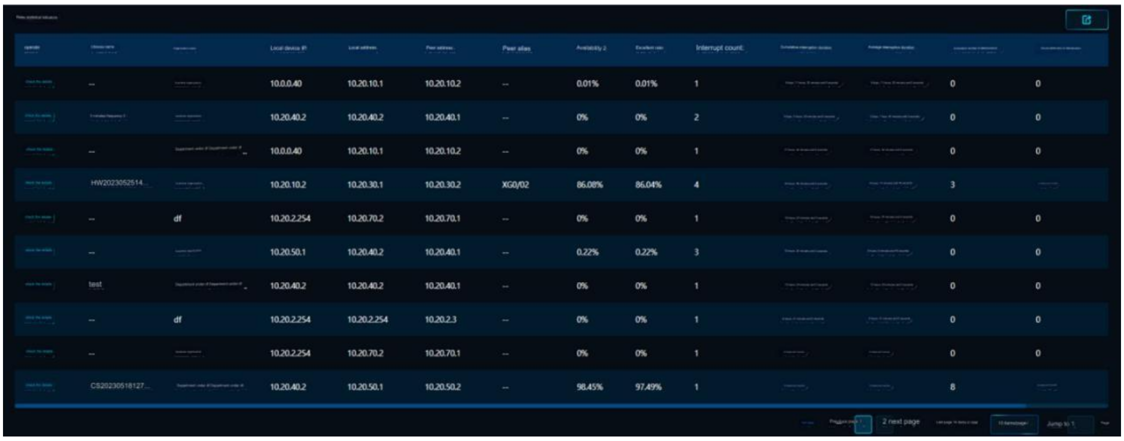
- ➢ Based on the statistical analysis of interrupt events/faults, provide TOP5 ranking of relay deterioration times, list display: relay name, local address, peer address, cumulative number of times, cumulative time duration;



Deterioration TOP5:

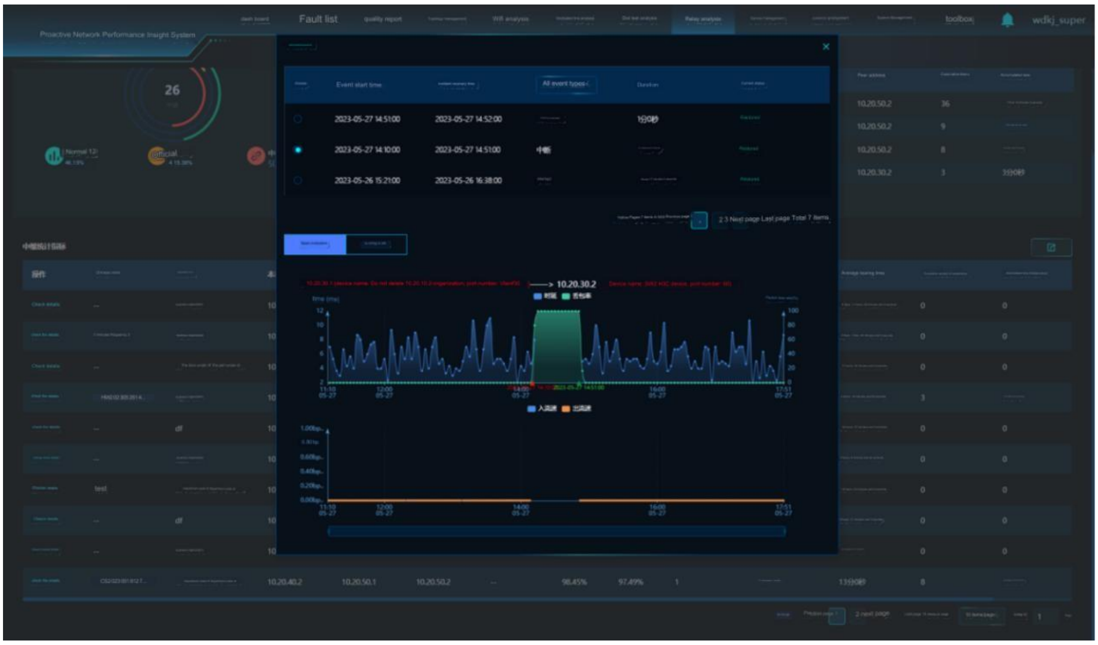
Trunk name	Local address	Peer address	Cumulative times	Accumulated time
2 minutes...	10.20.50.1	10.20.50.2	36	1 hour 12 minutes 0 seconds
--	10.20.50.1	10.20.50.2	9	10 minutes and 0 seconds
CS2...	10.20.50.1	10.20.50.2	8	6 minutes and 0 seconds
HW2...	10.20.30.1	10.20.30.2	3	3 minutes and 0 seconds

- ➢ Provides relay statistical metrics analysis, including relay information, outage information, delay degradation information, packet loss degradation information, availability rate, good rate;

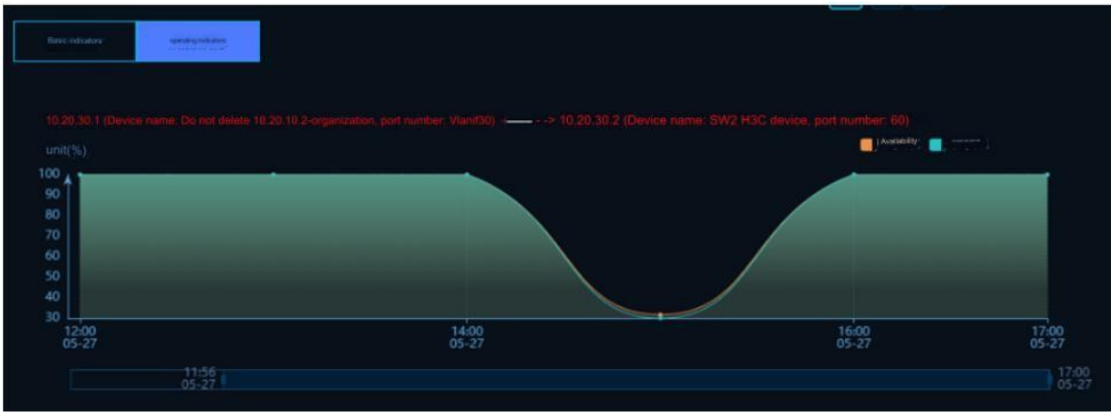


[illegible]	[illegible]	[illegible]	Local device IP	Local address	Peer address	Peer alias	Availability	Excellent rate	Interrupt count	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	--	[illegible]	10.0.0.40	10.20.10.1	10.20.10.2	--	0.01%	0.01%	1	[illegible]	[illegible]	0	0
[illegible]	[illegible]	[illegible]	10.20.40.2	10.20.40.2	10.20.40.1	--	0%	0%	2	[illegible]	[illegible]	0	0
[illegible]	--	[illegible]	10.0.0.40	10.20.10.1	10.20.10.2	--	0%	0%	1	[illegible]	[illegible]	0	0
[illegible]	HW2023052514...	[illegible]	10.20.10.2	10.20.30.1	10.20.30.2	XG0/02	86.08%	86.04%	4	[illegible]	[illegible]	3	[illegible]
[illegible]	--	df	10.20.2.254	10.20.70.2	10.20.70.1	--	0%	0%	1	[illegible]	[illegible]	0	0
[illegible]	--	[illegible]	10.20.50.1	10.20.40.2	10.20.40.1	--	0.22%	0.22%	3	[illegible]	[illegible]	0	0
[illegible]	test	[illegible]	10.20.40.2	10.20.40.2	10.20.40.1	--	0%	0%	1	[illegible]	[illegible]	0	0
[illegible]	--	df	10.20.2.254	10.20.2.254	10.20.2.3	--	0%	0%	1	[illegible]	[illegible]	0	0
[illegible]	--	[illegible]	10.20.2.254	10.20.70.2	10.20.70.1	--	0%	0%	1	[illegible]	[illegible]	0	0
[illegible]	CS20230518127...	[illegible]	10.20.40.2	10.20.50.1	10.20.50.2	--	98.45%	97.49%	1	[illegible]	[illegible]	8	[illegible]

- Support drill down to view the details of poor quality relay information, display the list of relay-related events/faults, and support switching events/faults to view the raw indicator trend graph; the start time point will be clearly identified on the trend graph; and based on the events/faults to assess the overall operating condition of the relay.



[illegible]	Event start time	[illegible]	All event types	Duration	[illegible]
○	2023-05-27 14:51:00	2023-05-27 14:52:00	[illegible]	1分0秒	[illegible]
●	2023-05-27 14:10:00	2023-05-27 14:51:00	中断	[illegible]	[illegible]
○	2023-05-26 15:21:00	2023-05-26 16:38:00	[illegible]	[illegible]	[illegible]

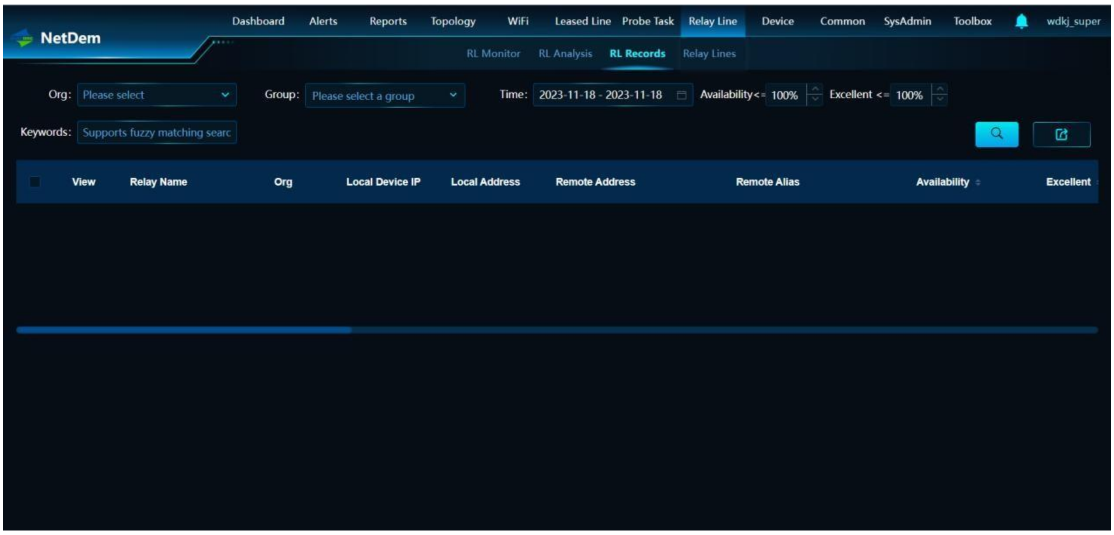


- ➢ Supports fault point location display;

2.3.8.3. Relay Health Records

Create a profile for each relay, automatically collect data, and integrate and analyze the data to form a relay health profile.

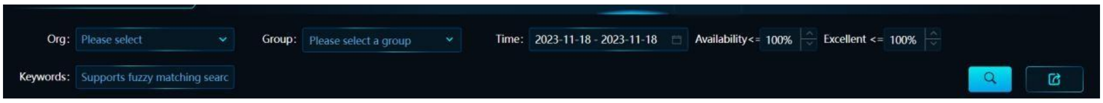
- ➢ Provides a relay health profile list, displaying details of each relay's operating metrics, including relay information, delay degradation information, packet loss degradation information, flow rate information, availability rate, and good rate;



Org: Please select
Group: Please select a group
Time: 2023-11-18 - 2023-11-18
Availability<= 100%
Excellent <= 100%
Keywords: Supports fuzzy matching searc

□	View	Relay Name	Org	Local Device IP	Local Address	Remote Address	Remote Alias	Availability	Excellent

- ➢ Supports querying by organization name, time period, keywords (fuzzy match search by trunk name, local device IP, local/opposite address, opposite alias is supported) as required;



Org: Please select

Group: Please select a group

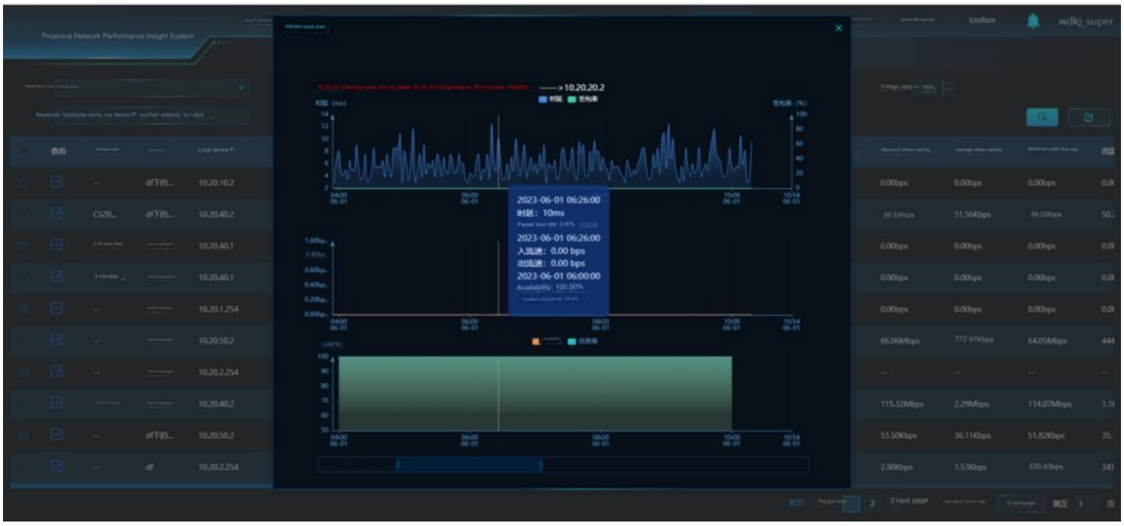
Time: 2023-11-18 - 2023-11-18

Availability<= 100%

Excellent <= 100%

Keywords: Supports fuzzy matching searc

- Supports selecting data export or all export;
- Support drill down to view trunking metrics trend graphs, including latency/packet loss, inbound/outbound flow rate, availability/goodness rate trend graphs;



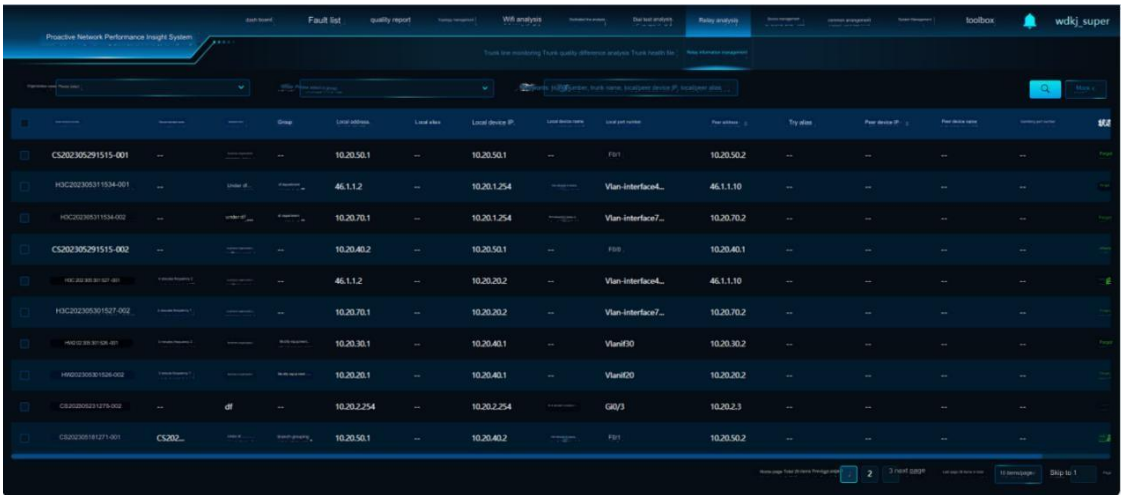
2023-06-01 06:26:00
时延: 10ms

2023-06-01 06:26:00
入流速: 0.00 bps
出流速: 0.00 bps

2023-06-01 06:00:00
Availability: 100.00%

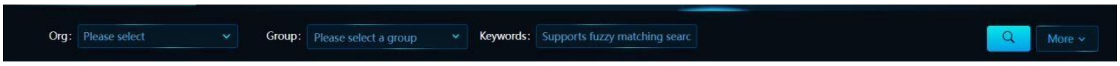
2.3.8.4. Relay Information Management

Relay information management is the comprehensive management of relay, through the configuration of the collection task using the snmp protocol to automatically discover the relay information, and list presentation. On the basis of automatic discovery of the upper relay, it carries out comprehensive management of relay information such as updating, modifying, exporting, exporting all, deleting and so on.

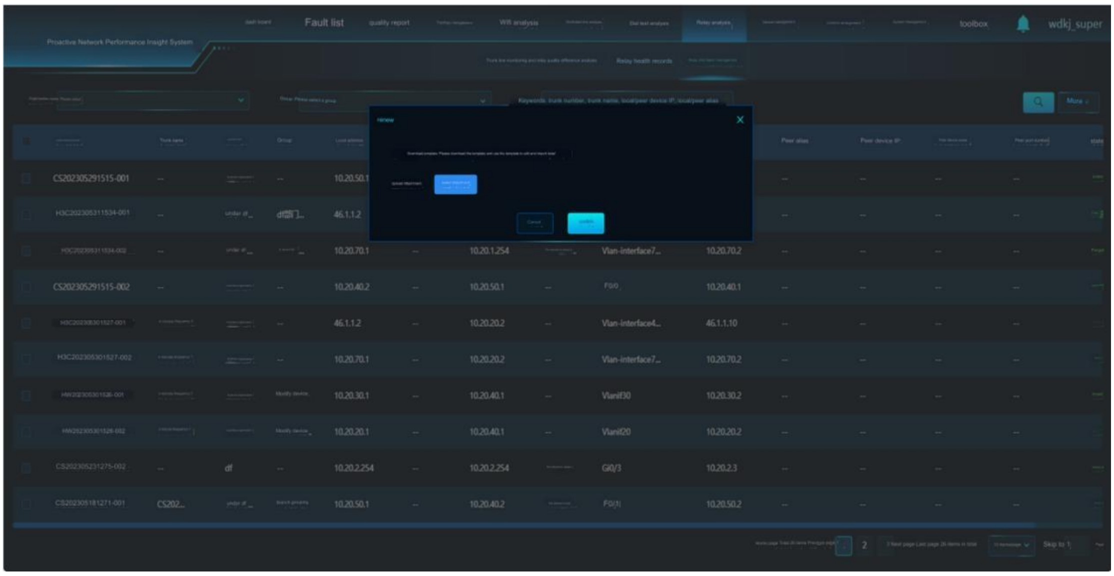


[illegible]	[illegible]	[illegible]	Group	Local address	Local alias	Local device IP	Local device name	Local port number	Peer address	Try alias	Peer device IP	Peer device name	[illegible]	[illegible]
CS202305291515-001	--	[illegible]	--	10.20.50.1	--	10.20.50.1	--	F0/1	10.20.50.2	--	--	--	--	[illegible]
H3C202305311534-001	--	Under df...	[illegible]	46.1.1.2	--	10.20.1.254	[illegible]	Vlan-interface4...	46.1.1.10	--	--	--	--	[illegible]
H3C202305311534-002	--	under df...	[illegible]	10.20.70.1	--	10.20.1.254	[illegible]	Vlan-interface7...	10.20.70.2	--	--	--	--	[illegible]
CS202305291515-002	--	[illegible]	--	10.20.40.2	--	10.20.50.1	--	F0/0	10.20.40.1	--	--	--	--	[illegible]
H3C202305301527-001	[illegible]	[illegible]	--	46.1.1.2	--	10.20.20.2	--	Vlan-interface4...	46.1.1.10	--	--	--	--	[illegible]
H3C202305301527-002	[illegible]	[illegible]	--	10.20.70.1	--	10.20.20.2	--	Vlan-interface7...	10.20.70.2	--	--	--	--	[illegible]
HW202305301526-001	[illegible]	[illegible]	[illegible]	10.20.30.1	--	10.20.40.1	--	Vlanif30	10.20.30.2	--	--	--	--	[illegible]
HW202305301526-002	[illegible]	[illegible]	[illegible]	10.20.20.1	--	10.20.40.1	--	Vlanif20	10.20.20.2	--	--	--	--	[illegible]
CS202305231275-002	--	df	--	10.20.2.254	--	10.20.2.254	[illegible]	Gi0/3	10.20.2.3	--	--	--	--	[illegible]
CS202305181271-001	CS202...	[illegible]	[illegible]	10.20.50.1	--	10.20.40.2	[illegible]	F0/1	10.20.50.2	--	--	--	--	[illegible]

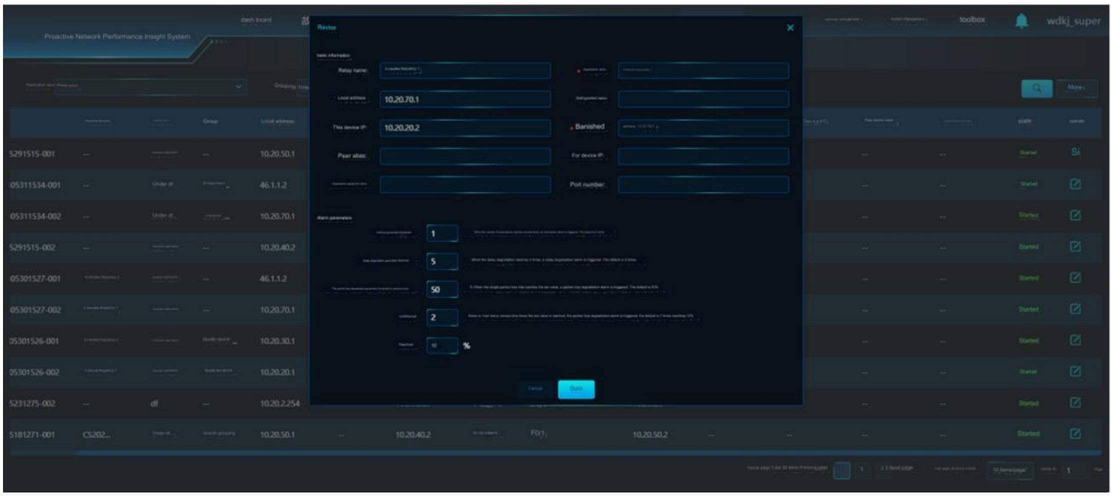
- ➢ Supports combined query by organization name, operator, keyword (supports query by trunk name, local/opposite equipment IP, local/opposite address, local/opposite alias, etc.) ;



- ➢ Supports batch updating of relay information by importing, downloading templates, uploading templates after filling them with data, the system automatically parses the template data, prompts for duplicates of templates and abnormalities of template data matching the system data, and supports the export of abnormal items.



- ➢ Supports modification of relay records in the system, including relay name, organization name, local alias, peer alias, peer device IP, peer device name, peer port number, alarm parameters, etc.



Revise

Relay name:

Local address: 10.20.70.1

This device IP: 10.20.20.2

Banished

Peer alias:

For device IP:

Port number:

1

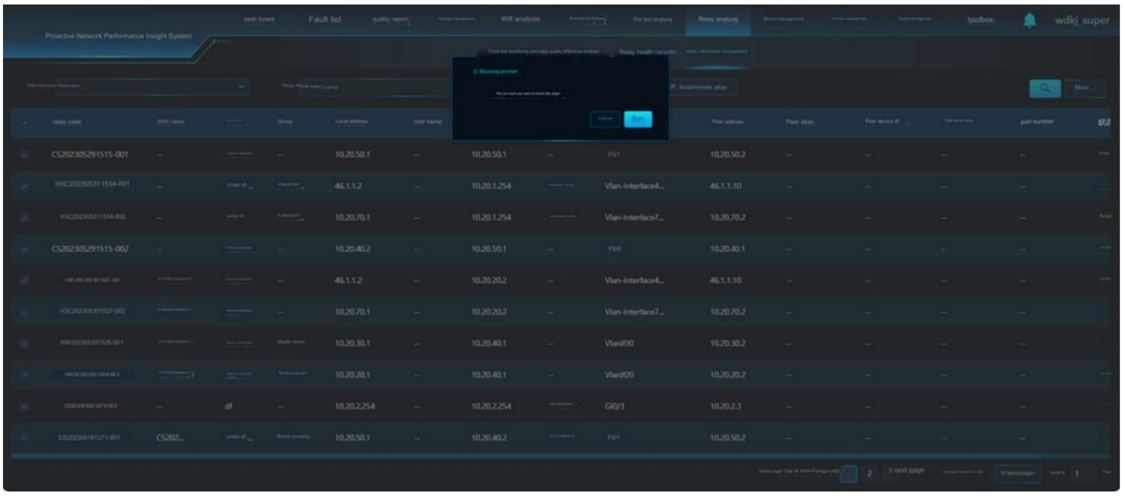
5

50

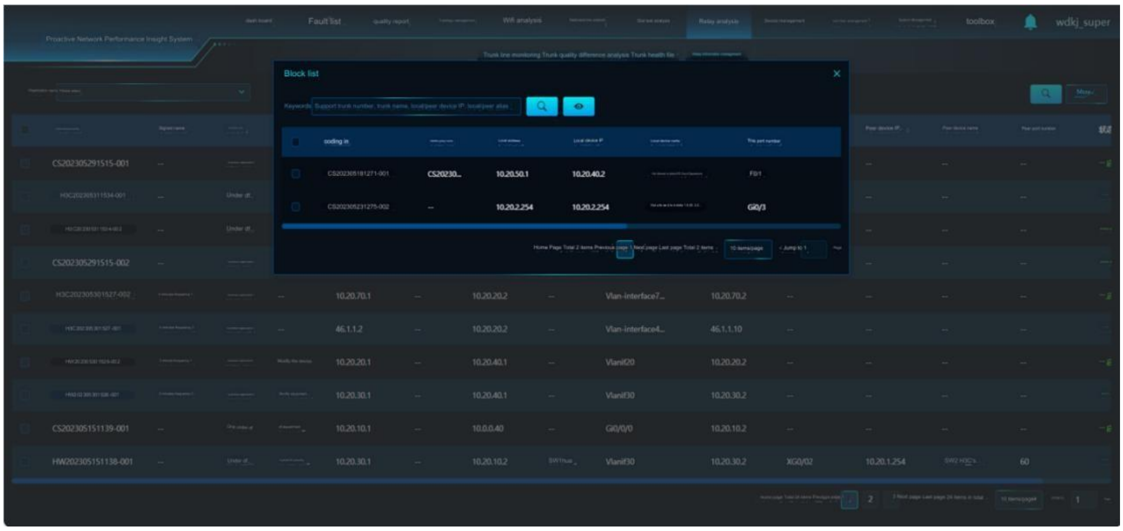
2

%

- ➢ Supports shielding/un-shielding of relay information that does not need to be monitored, select the data to be shielded in the list, click the [Shield] button, a tip window will pop up for prompting, confirm and then perform shielding, and at the same time, update the list record (shielded relay information is not displayed in the list of relay information, it can be viewed in the shielding list, and no longer shielded relays for (the blocked relay information is not displayed in the relay information list and can be viewed in the blocked list, and no more data acquisition is performed on the blocked relay). For the blocked relay information, it supports to view the list, and at the same time, it supports to release the blocking;

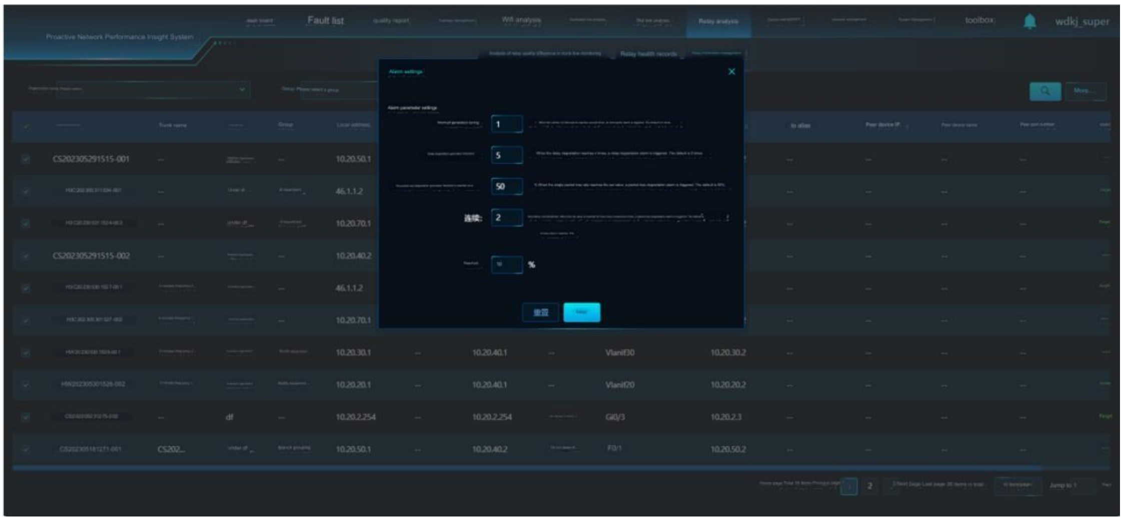


relay code	AVC name	Group	Local address	real name				Peer address	Peer alias	Peer device IP		port number
CS202305291515-001	--	--	10.20.50.1	--	10.20.50.1	--	F0/1	10.20.50.2	--	--	--	--
H3C202305311534-001	--	[illegible]	46.1.1.2	--	10.20.1.254	[illegible]	Vlan-interface4...	46.1.1.10	--	--	--	--
H3C202305311534-002	--	[illegible]	10.20.70.1	--	10.20.1.254	[illegible]	Vlan-interface7...	10.20.70.2	--	--	--	--
CS202305291515-002	--	--	10.20.40.2	--	10.20.50.1	--	F0/0	10.20.40.1	--	--	--	--
[illegible]	[illegible]	--	46.1.1.2	--	10.20.20.2	--	Vlan-interface4...	46.1.1.10	--	--	--	--
H3C202305301527-002	[illegible]	--	10.20.70.1	--	10.20.20.2	--	Vlan-interface7...	10.20.70.2	--	--	--	--
HW202305301526-001	[illegible]	[illegible]	10.20.30.1	--	10.20.40.1	--	Vlanif30	10.20.30.2	--	--	--	--
[illegible]	[illegible]	[illegible]	10.20.20.1	--	10.20.40.1	--	Vlanif20	10.20.20.2	--	--	--	--
[illegible]	--	--	10.20.2.254	--	10.20.2.254	[illegible]	Gi0/3	10.20.2.3	--	--	--	--
CS202305181271-001	CS202...	[illegible]	10.20.50.1	--	10.20.40.2	[illegible]	F0/1	10.20.50.2	--	--	--	--


Proactive Network Performance Insight System
Fault list
Wifi analysis
Relay analysis
toolbox
wdkj_super
Trunk line monitoring Trunk quality difference analysis Trunk health file
Block list
Keywords
Support trunk number, trunk name, local/peer device IP, local/peer alias

	coding in			Local device IP		The port number
□	CS202305181271-001	CS20230...	10.20.50.1	10.20.40.2	[illegible]	F0/1
□	CS202305231275-002	--	10.20.2.254	10.20.2.254	[illegible]	Gi0/3

- ➢ Support the setting of relay information alarm parameters, select the data list to update the alarm parameters, click the [Alarm Settings] button, the tip window will pop up to set the alarm, support editing the alarm parameters or restoring them to the default value and then save them to complete the update of the alarm settings.

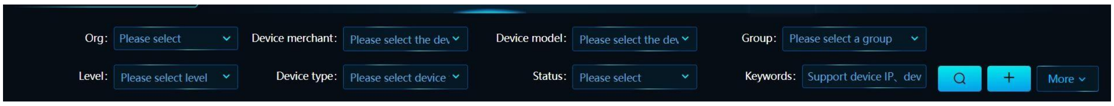


2.3.9. Device Management

2.3.9.1. Collection Tasks

Acquisition task management refers to the management of SNMP acquisition tasks. Users can configure the acquisition tasks in the acquisition task management to achieve the acquisition of parameters of relay devices through the snmp protocol (supporting snmp_v1, snmp_v2, snmp_v3), to achieve the auto-discovery of relay, and to automatically generate relay acquisition tasks according to the configuration, to achieve the acquisition of relay-related monitoring indicators, supporting device information, delay/packet loss rate, and in/out flow rate indicators. The system provides the following main functions:

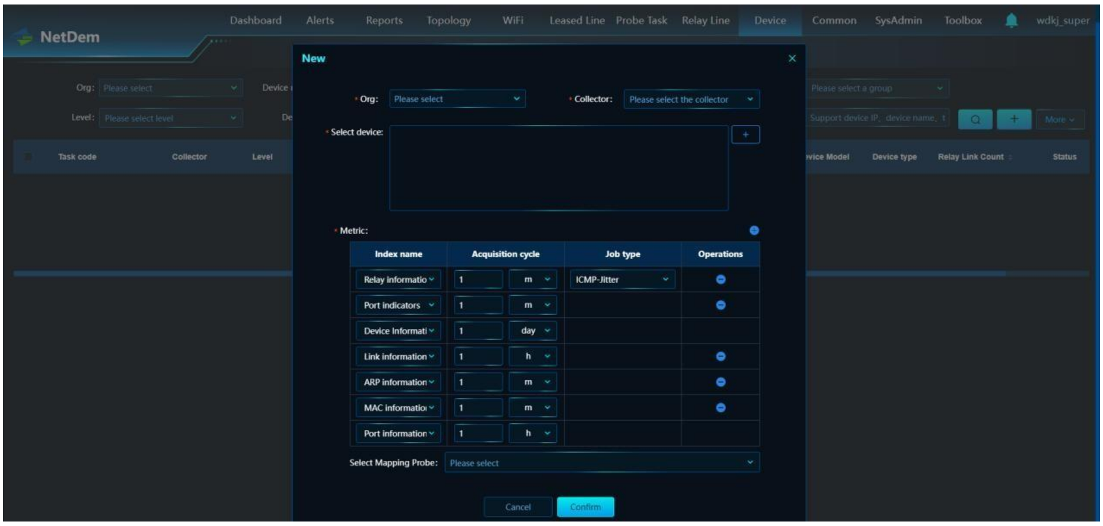
- Supports combined query by organisation name, device manufacturer, device model, status, keywords (supports fuzzy matching query by device IP, device name)



Org: Please select
Device merchant: Please select the dev
Device model: Please select the dev
Group: Please select a group
Level: Please select level
Device type: Please select device
Status: Please select
Keywords: Support device IP、dev

- Alarm parameters use default values (interrupt generation threshold, delay degradation generation threshold, packet loss degradation generation threshold), support for modification of alarm thresholds in relay information management;

- ➢ Supports new collection tasks, you can configure the collection indicators, etc.;



New

* Org: Please select * Collector: Please select the collector

* Select device:

* Metric:

Index name	Acquisition cycle		Job type	Operations
Relay informatio	1	m	ICMP-Jitter	⊖
Port indicators	1	m		⊖
Device Informati	1	day		
Link information	1	h		⊖
ARP information	1	m		⊖
MAC informatio	1	m		⊖
Port information	1	h		

Select Mapping Probe: Please select

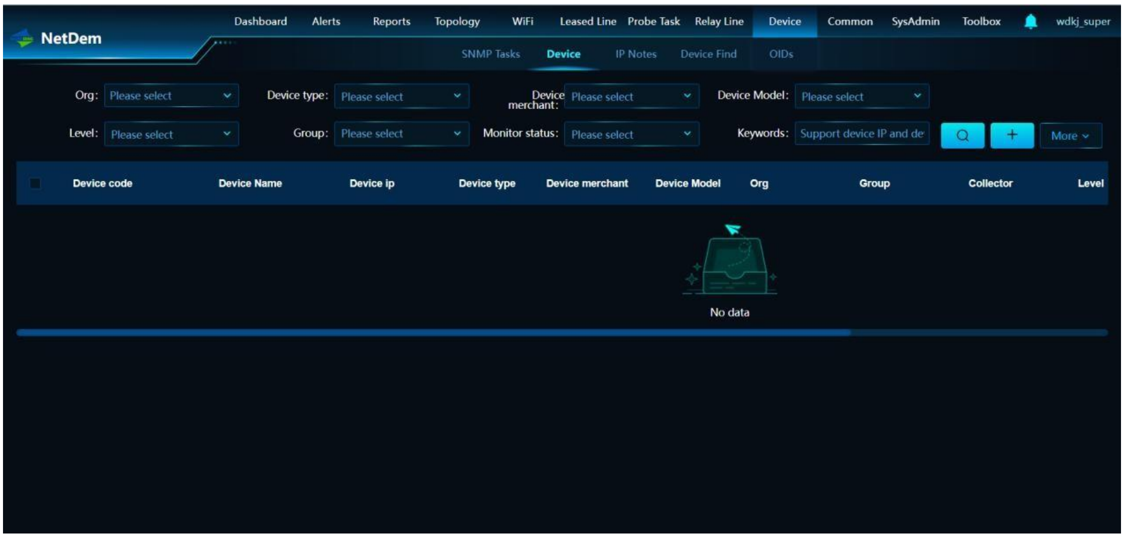
- ➢ Supports quick import of collection tasks by editing the collection task template;
- ➢ Holds selective data or export all collection tasks;
- ➢ Supports pause/start tasks to achieve task pause and start; the paused task and the relay information found through the acquisition task will stop data acquisition, and the related events and alarms will be cancelled at the same time;
- ➢ Supports the collection of basic indexes, and supports the collection of basic indexes for statistical analysis to evaluate the operation status of the relay;

2.3.9.2. Device Management

Device management is the comprehensive management of each node's network management unit, such as adding, deleting, changing and checking.

- ➢ Support for adding, modifying, deleting, and querying devices;
- ➢ Support for viewing interface information for devices;

- Support for viewing Network Neighborhood;
- Support to view port metrics trends, including inbound and outbound flow rate, inbound and outbound utilization, receive packet loss, transmit packet loss, receive error, transmit error;
- Support for viewing ARP information on ports;
- Support for viewing MAC information on ports;



Org: Please select
Device type: Please select
Device merchant: Please select
Device Model: Please select
Level: Please select
Group: Please select
Monitor status: Please select
Keywords: Support device IP and de

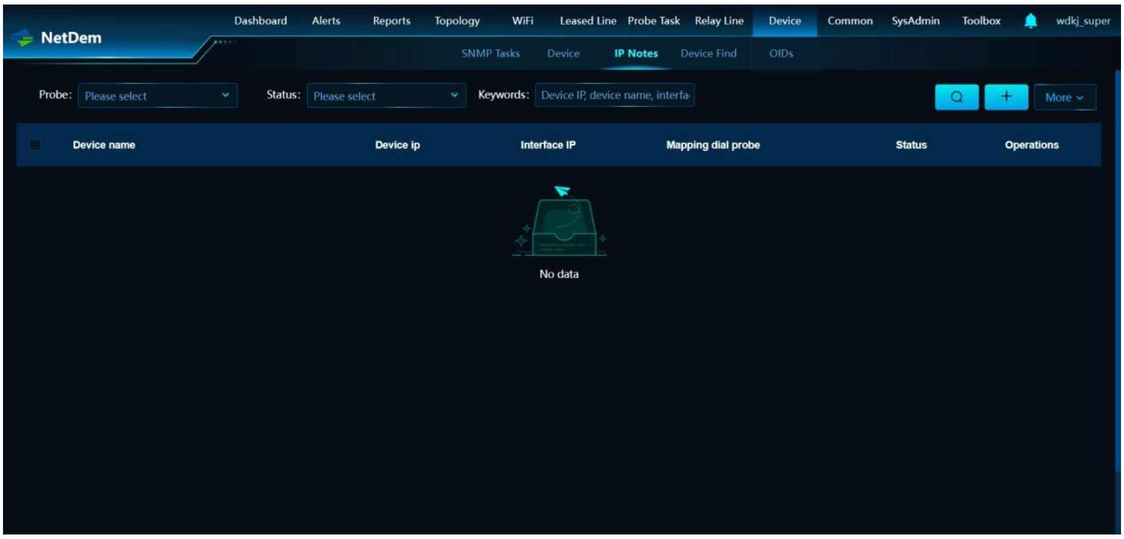
□	Device code	Device Name	Device ip	Device type	Device merchant	Device Model	Org	Group	Collector	Level

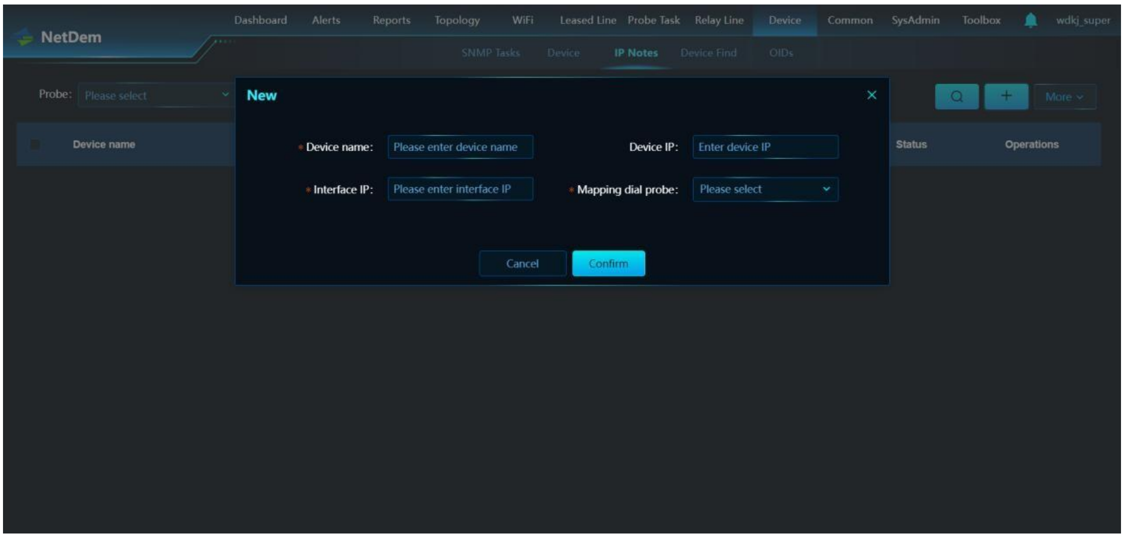
No data

2.3.9.3. Associated Display

Supports manual entry or automatic collection of the association relationship between the interface IP and the device through SNMP, when the path detected in the dialing test task contains the IP that has been entered, the device name mapped to the IP will be displayed at the same time.

- Supports the addition, modification and query of interface information;
- Supports manual entry or automatic collection of the association relationship between the interface IP and the device via SNMP;
- When the path detected in the Probe Test task contains an IP that has been recorded, the mapped device name of the IP is also displayed;



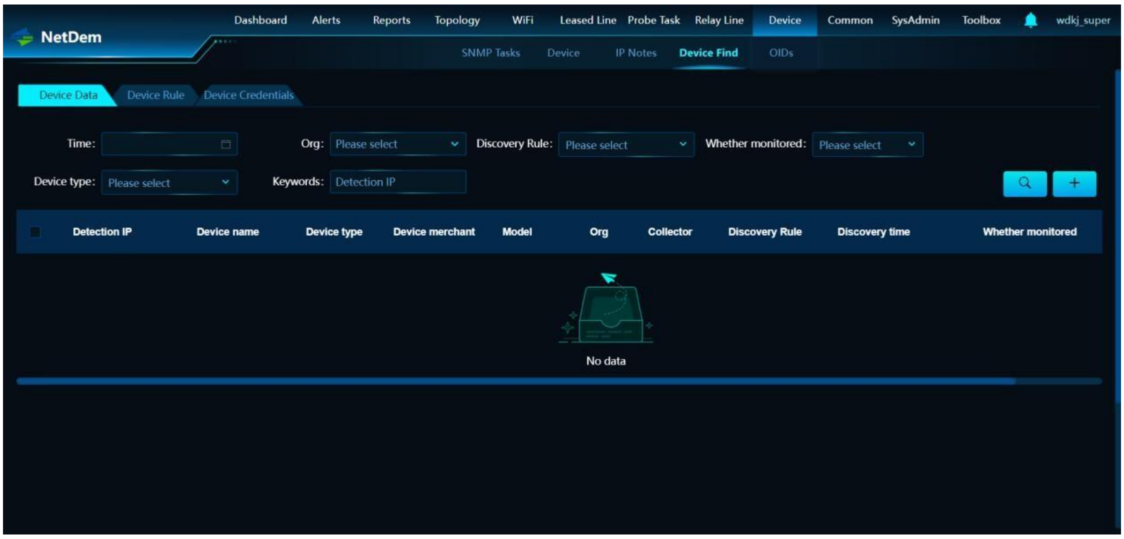


2.3.9.4. Device Discovery

2.3.9.4.1. Device Discovery Data

Device discovery data is the management of data discovered based on device discovery rules.

- Support for viewing and deleting discovery data;
- Supports the creation of tasks for discovery data;



Time:

Org: Please select

Discovery Rule: Please select

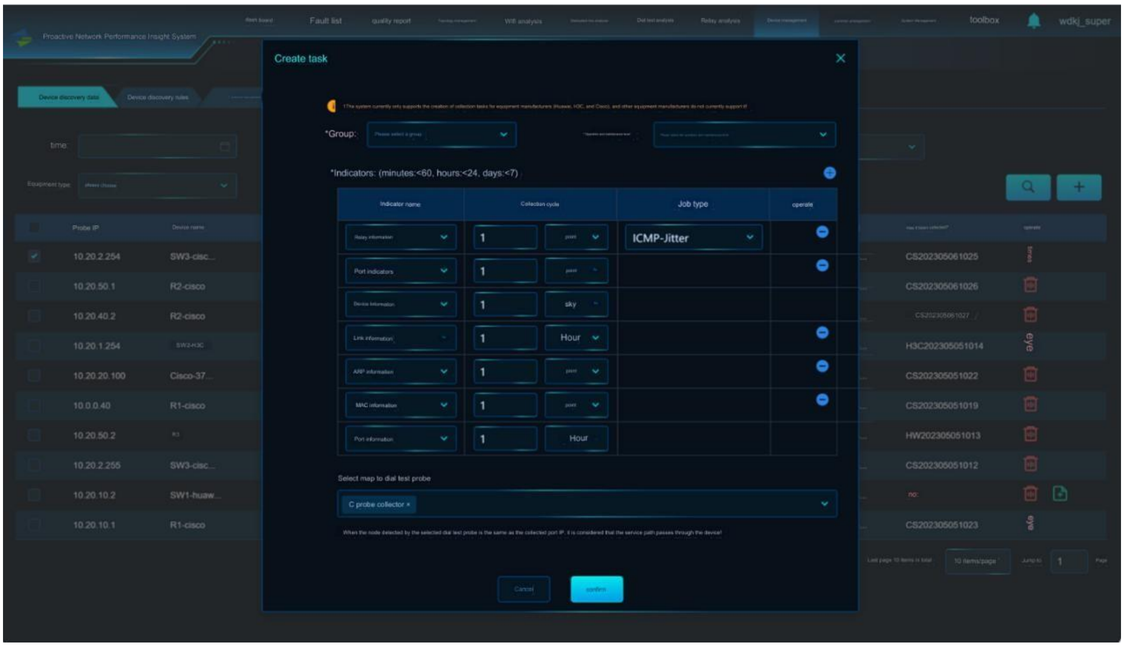
Whether monitored: Please select

Device type: Please select

Keywords: Detection IP

Detection IP	Device name	Device type	Device merchant	Model	Org	Collector	Discovery Rule	Discovery time	Whether monitored

No data



Create task

!The system currently only supports the creation of collection tasks for equipment manufacturers (Huawei, H3C, and Cisco), and other equipment manufacturers do not currently support it!

*Group: Please select a group

*Indicators: (minutes:<60, hours:<24, days:<7)

Indicator name	Collection cycle		Job type	operate
Relay information	1	point	ICMP-Jitter	⊖
Port indicators	1	point		⊖
Device Information	1	sky		
Link information	1	Hour		⊖
ARP information	1	point		⊖
MAC information	1	point		⊖
Port information	1	Hour		

Select map to dial test probe

C probe collector ×

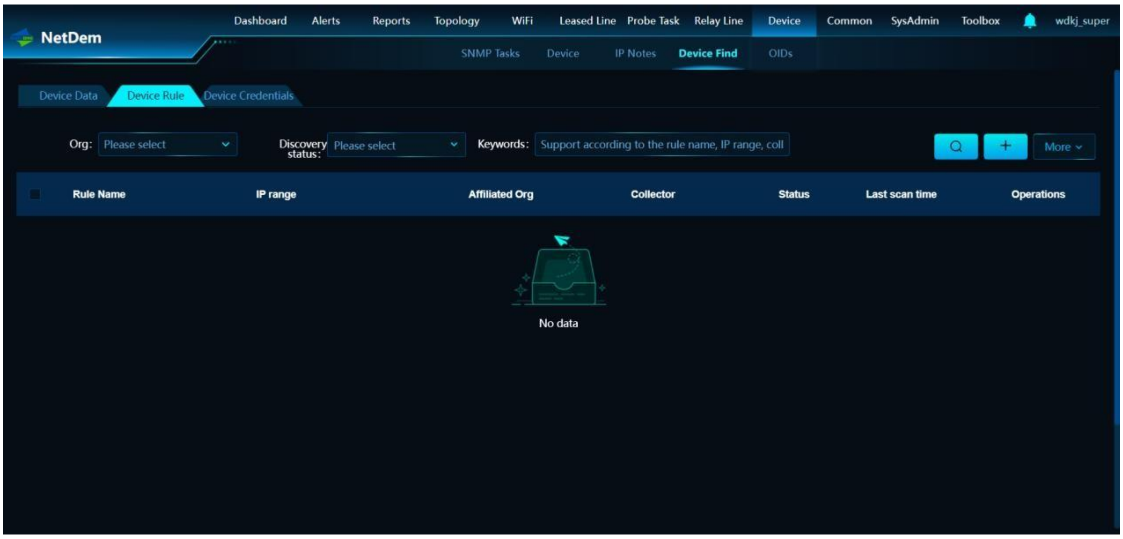
When the node detected by the selected dial test probe is the same as the collected port IP, it is considered that the service path passes through the device!

Cancel confirm

2.3.9.4.2. Device Discovery Rules

- ➢ Supports auto discovery rule configuration for IP ranges based on SNMP protocols;
- ➢ Supports scanning IPs one by one and automatically identifies whether they are authenticated or not;
- ➢ Supports automatic creation of discovered IPs as collection tasks;
- ➢ Any device with open SNMP authorization can be automatically discovered and monitored.

- ➢ Supports auto-discovery-auto-nano-monitoring of devices.



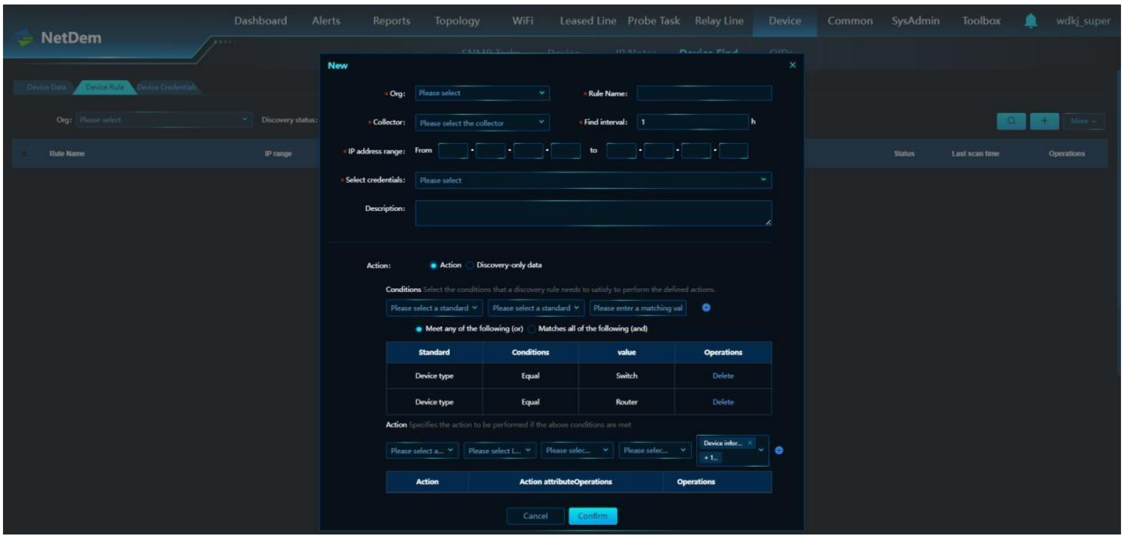
Org: Please select

Discovery status: Please select

Keywords: Support according to the rule name, IP range, coll

Rule Name	IP range	Affiliated Org	Collector	Status	Last scan time	Operations

No data



New

* Org: Please select
* Rule Name:
* Collector: Please select the collector
* Find interval: 1 h
* IP address range: From . . . to . . .
* Select credentials: Please select
Description:

Action: ● Action ○ Discovery-only data

Conditions Select the conditions that a discovery rule needs to satisfy to perform the defined actions.

Please select a standard | Please select a standard | Please enter a matching val

● Meet any of the following (or) ○ Matches all of the following (and)

Standard	Conditions	value	Operations
Device type	Equal	Switch	Delete
Device type	Equal	Router	Delete

Action Specifies the action to be performed if the above conditions are met

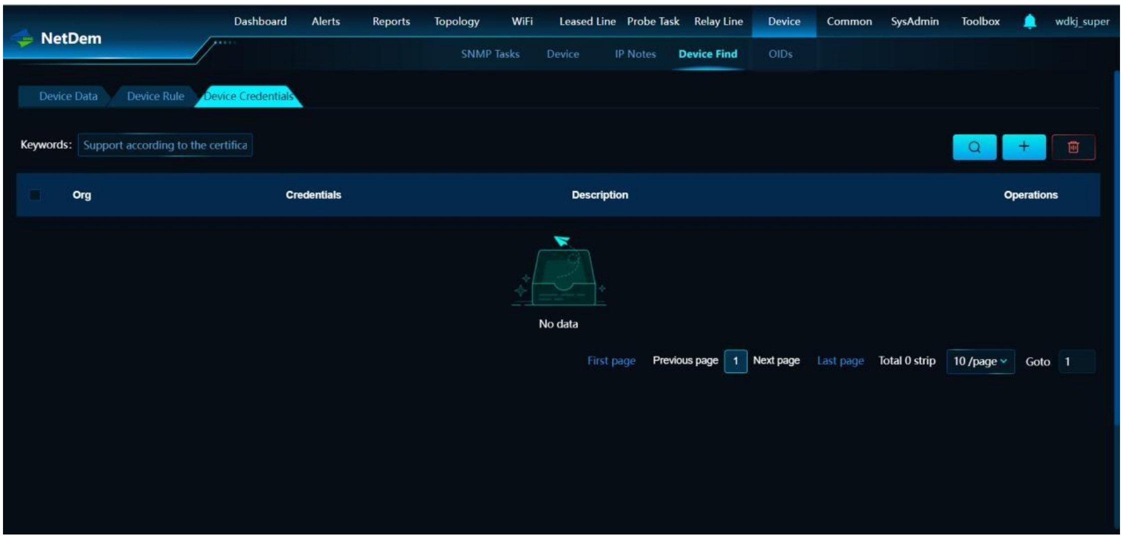
Please select a... | Please select I... | Please selec... | Please selec... | Device infor... +1...

Action	Action attributeOperations	Operations

2.3.9.4.3. Credential Management

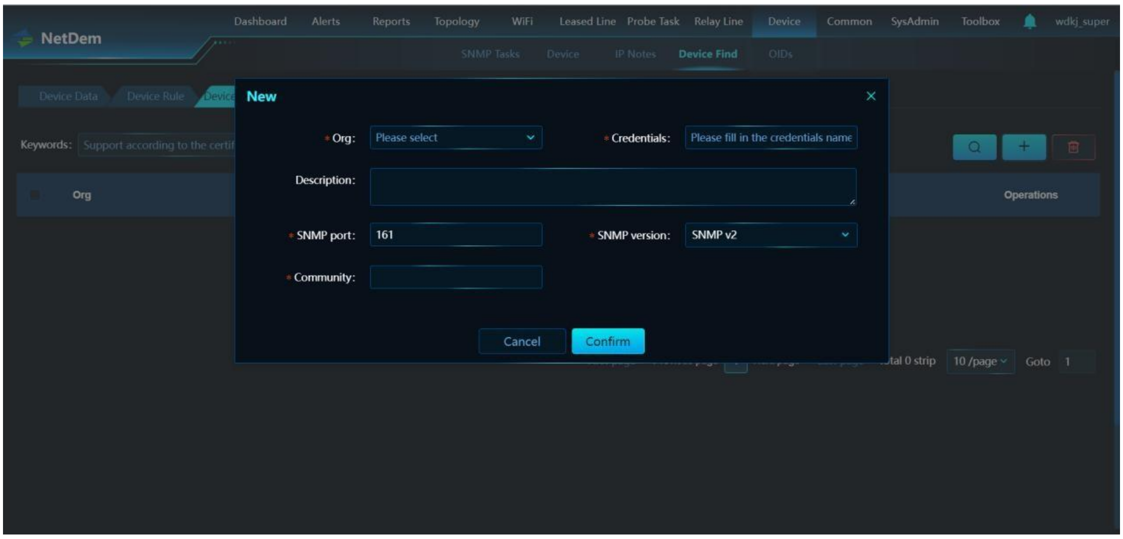
The system uses the SNMP protocol to access remote devices, SNMP group names may vary from device to device, a pre-configured set of credentials in the system helps to apply them to multiple devices at once, thus saving a lot of manual work.

- ➢ Supports integrated management of vouchers such as adding, deleting, changing and checking;



Keywords: Support according to the certifica

Org	Credentials	Description	Operations



* Org: Please select

* Credentials: Please fill in the credentials name

Description:

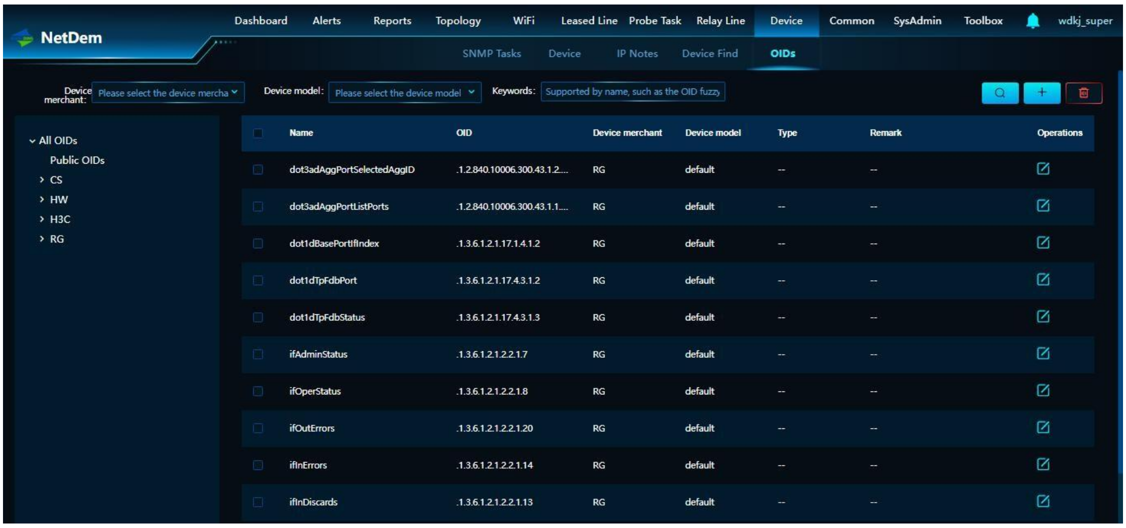
* SNMP port: 161

* SNMP version: SNMP v2

* Community:

2.3.9.5. OID management

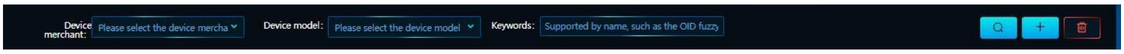
OID management is the unified storage and management of OIDs used for network data collection of relay devices based on the SNMP protocol. Manage OIDs of different equipment manufacturers and equipment models, and automatically match OIDs according to the equipment manufacturers and models configured in the collection task for data collection.



Device merchant: Please select the device mercha
Device model: Please select the device model
Keywords: Supported by name, such as the OID fuzzy

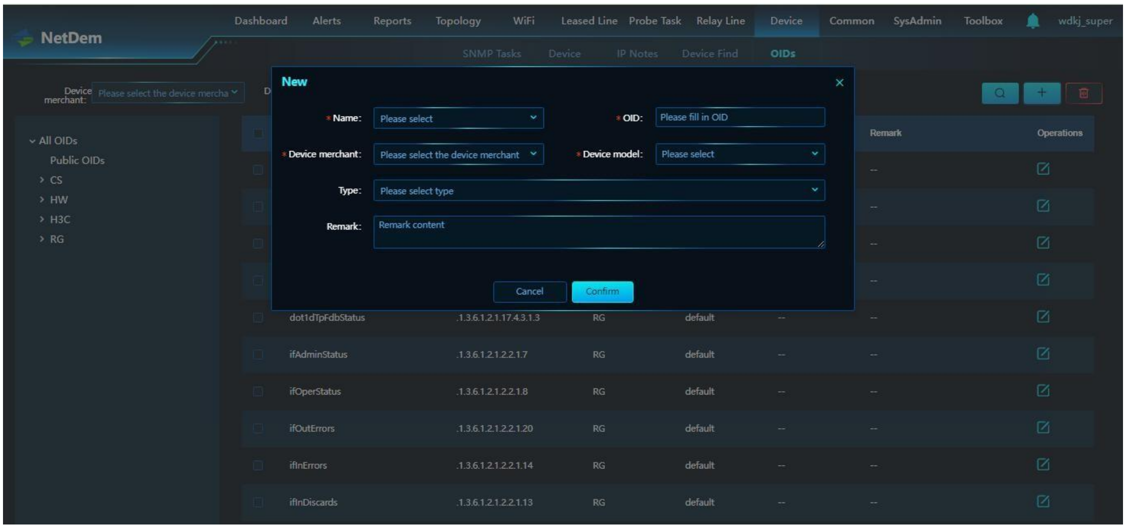
□	Name	OID	Device merchant	Device model	Type	Remark	Operations
□	dot3adAggPortSelectedAggID	.1.2.840.10006.300.43.1.2....	RG	default	--	--	
□	dot3adAggPortListPorts	.1.2.840.10006.300.43.1.1....	RG	default	--	--	
□	dot1dBasePortIfIndex	.1.3.6.1.2.1.17.1.4.1.2	RG	default	--	--	
□	dot1dTpFdbPort	.1.3.6.1.2.1.17.4.3.1.2	RG	default	--	--	
□	dot1dTpFdbStatus	.1.3.6.1.2.1.17.4.3.1.3	RG	default	--	--	
□	ifAdminStatus	.1.3.6.1.2.1.2.2.1.7	RG	default	--	--	
□	ifOperStatus	.1.3.6.1.2.1.2.2.1.8	RG	default	--	--	
□	ifOutErrors	.1.3.6.1.2.1.2.2.1.20	RG	default	--	--	
□	ifInErrors	.1.3.6.1.2.1.2.2.1.14	RG	default	--	--	
□	ifInDiscards	.1.3.6.1.2.1.2.2.1.13	RG	default	--	--	

- Supports querying by equipment manufacturer, equipment model (equipment manufacturer cascade), keywords (supports fuzzy matching by name, OID, etc.);



Device merchant: Please select the device mercha
Device model: Please select the device model
Keywords: Supported by name, such as the OID fuzzy

- Supports the addition of OIDs required for collecting indicators to facilitate expansion of non-common requirements of different equipment manufacturers and equipment models;



New

* Name: Please select
* OID: Please fill in OID
* Device merchant: Please select the device merchant
* Device model: Please select
Type: Please select type
Remark: Remark content

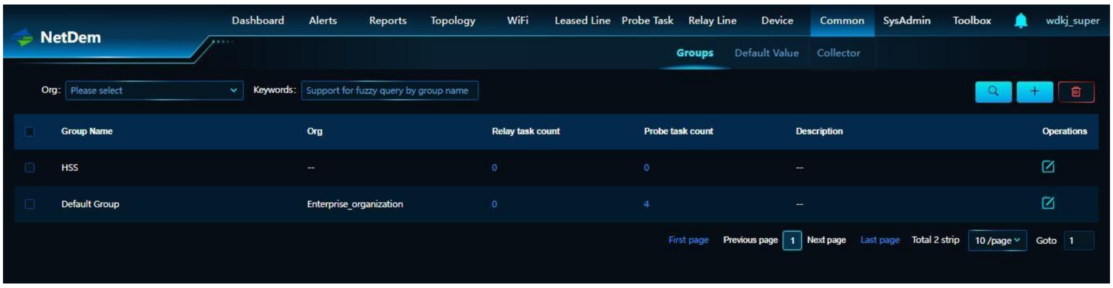
□	Name	OID	Device merchant	Device model	Type	Remark	Operations
□	dot1dTpFdbStatus	.1.3.6.1.2.1.17.4.3.1.3	RG	default	--	--	
□	ifAdminStatus	.1.3.6.1.2.1.2.2.1.7	RG	default	--	--	
□	ifOperStatus	.1.3.6.1.2.1.2.2.1.8	RG	default	--	--	
□	ifOutErrors	.1.3.6.1.2.1.2.2.1.20	RG	default	--	--	
□	ifInErrors	.1.3.6.1.2.1.2.2.1.14	RG	default	--	--	
□	ifInDiscards	.1.3.6.1.2.1.2.2.1.13	RG	default	--	--	

- Support modification of OID;
- Supports deletion of OID;

2.3.10. Common configuration management

2.3.10.1. Group Management

Grouping is to group tasks into categories according to business scenarios, making it easier for users to maintain and manage monitoring content.

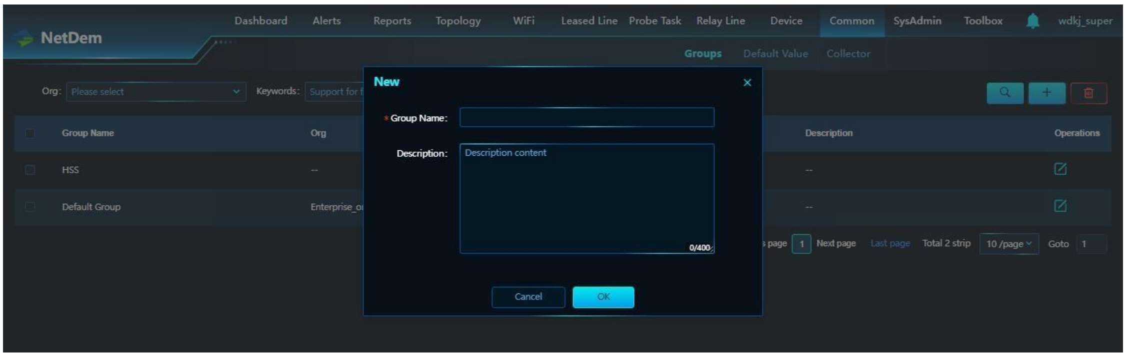


Org: Please select Keywords: Support for fuzzy query by group name

□	Group Name	Org	Relay task count	Probe task count	Description	Operations
□	HSS	--	0	0	--	✎
□	Default Group	Enterprise_organization	0	4	--	✎

First page Previous page 1 Next page Last page Total 2 strip 10 /page Goto 1

- ➢ Supports paging display of group list: group name, number of relay tasks, number of detection tasks, description, operation
- ➢ Supports combined query based on keywords (supports fuzzy matching query by group name)



New

* Group Name:

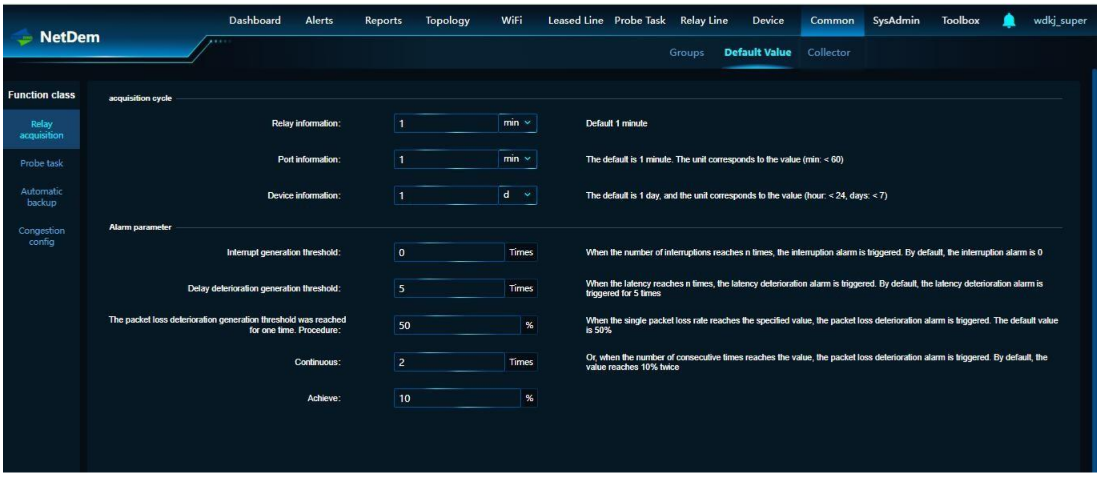
Description: Description content

0/400

- ➢ Support new grouping: group name, description
- ➢ Supports single and batch deletion of groups. When associated with path topology, prompts to delete the topology first.
- ➢ Support modification: group name, description
- ➢ Support adding and deleting probe test tasks within the group
- ➢ Support adding and deleting relay tasks within the group

2.3.10.2. Default value management

Default value management is used to manage specific parameter default values, including: probe monitoring, emergency notification, ordinary Probe Test, high-frequency monitoring, and relay collection. The system will use this default value when performing related actions.



acquisition cycle

Relay information: 1 min — Default 1 minute

Port information: 1 min — The default is 1 minute. The unit corresponds to the value (min: < 60)

Device information: 1 d — The default is 1 day, and the unit corresponds to the value (hour: < 24, days: < 7)

Alarm parameter

Interrupt generation threshold: 0 Times — When the number of interruptions reaches n times, the interruption alarm is triggered. By default, the interruption alarm is 0

Delay deterioration generation threshold: 5 Times — When the latency reaches n times, the latency deterioration alarm is triggered. By default, the latency deterioration alarm is triggered for 5 times

The packet loss deterioration generation threshold was reached for one time. Procedure: 50 % — When the single packet loss rate reaches the specified value, the packet loss deterioration alarm is triggered. The default value is 50%

Continuous: 2 Times — Or, when the number of consecutive times reaches the value, the packet loss deterioration alarm is triggered. By default, the value reaches 10% twice

Achieve: 10 %

- ➢ Support modifying and updating default values;
- ➢ Supports resetting the default value to the initial value;

Specific management parameters include:

- Network Probe Test

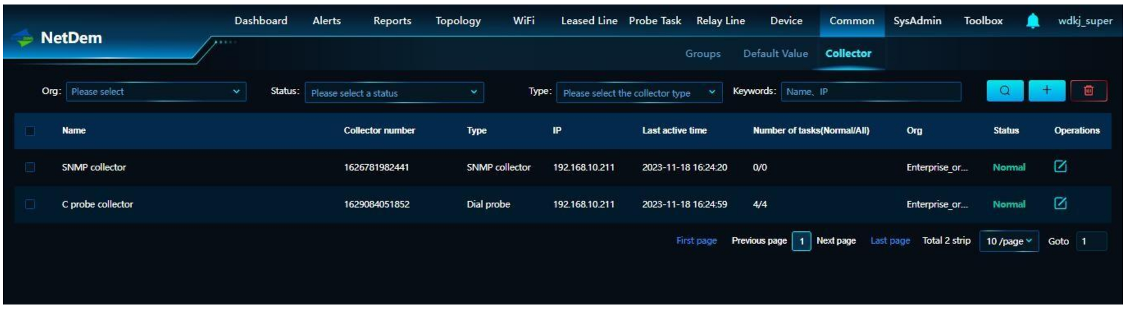
Probe port, UDP target port, TCP target port, Probe Test frequency, number of packets sent, packet size, starting TTL, Trace limited hop count, event generation cycle, event recovery cycle, interrupt generation threshold, delay degradation generation threshold , packet loss degradation generation threshold, route fluctuation alarm switch, and device type that does not generate interruption events when the target interruption is located.

- Relay collection

Delay/packet loss rate, flow rate, device information, interruption generation threshold, delay degradation generation threshold, packet loss degradation generation threshold, congestion threshold

2.3.10.3. Collector management

The collector manages Probe Test probes and SNMP collector servers, and supports comprehensive management such as adding, modifying, deleting, and status monitoring of collectors.



Org: Please select

Status: Please select a status

Type: Please select the collector type

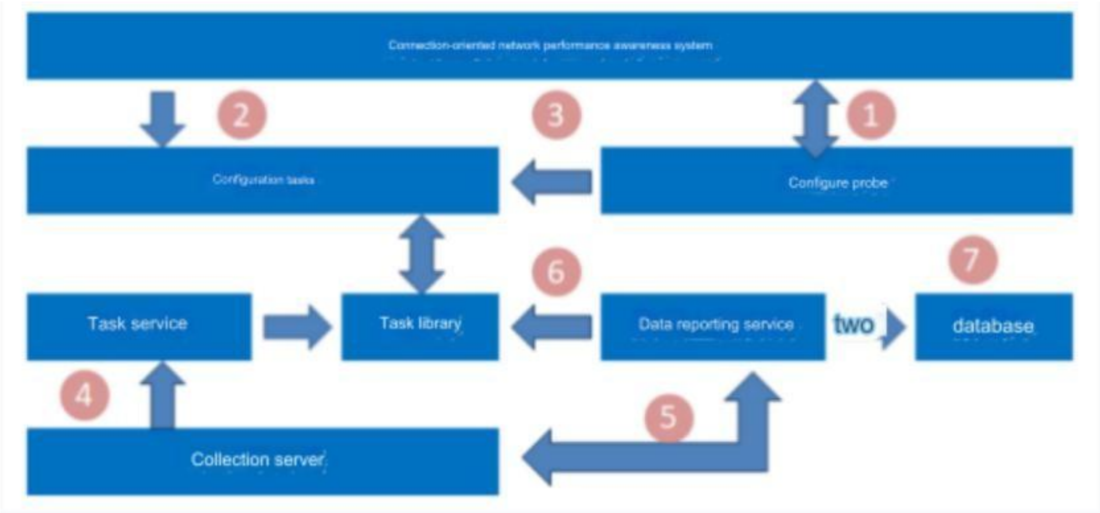
Keywords: Name、IP

□	Name	Collector number	Type	IP	Last active time	Number of tasks(Normal/All)	Org	Status	Operations
□	SNMP collector	1626781982441	SNMP collector	192.168.10.211	2023-11-18 16:24:20	0/0	Enterprise_or...	Normal	
□	C probe collector	1629084051852	Dial probe	192.168.10.211	2023-11-18 16:24:59	4/4	Enterprise_or...	Normal	

First page Previous page 1 Next page Last page Total 2 strip 10 /page Goto 1

The Probe Test probe receives the probe test tasks configured by the management platform, executes the tasks, and reports the Probe Test results to the data service. The system collects, analyzes and stores the data into the database.

The SNMP collection server receives the relay collection task, executes the task, and reports the collection task to the data service.



The system collects, analyzes and stores the data into the database.

- Supports the creation, modification and deletion of monitoring probe servers.

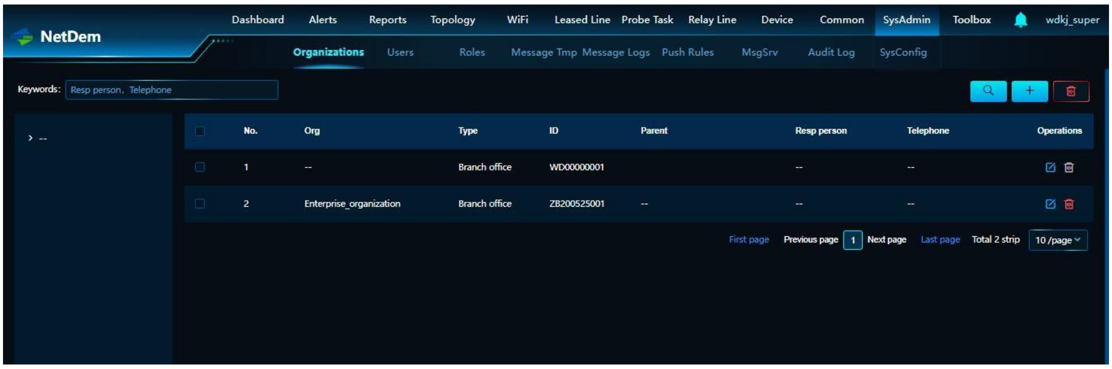
- Supports the collection server to report heartbeats in real time.

When the heartbeat cannot be detected three times, the collection server status changes to "offline". When the heartbeat is detected again, the recovery status is "normal".

2.3.11. System Management

2.3.11.1. Organizational Management

Organizational management is the hierarchical management of organizations to achieve the management of subordinate relationships between superiors and subordinates.

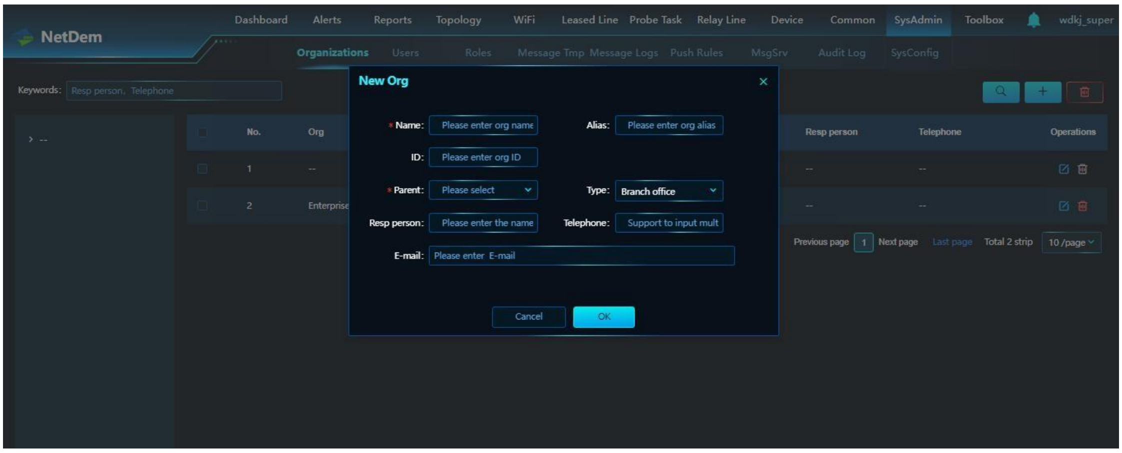


Keywords: Resp person, Telephone

□	No.	Org	Type	ID	Parent	Resp person	Telephone	Operations
□	1	--	Branch office	WD00000001		--	--	
□	2	Enterprise_organization	Branch office	ZB200525001	--	--	--	

First page Previous page 1 Next page Last page Total 2 strip 10 /page

- ➢ Support the addition, modification, inquiry, etc. of institutions;
- ➢ Support province, city, and keyword query data;
- ➢ Input information includes: organization ID, organization name, organization alias, province and city information, parent organization, organization type, sort number, contact name, contact information, and E-mail;



Keywords: Resp person, Telephone

New Org

* Name: Please enter org name   Alias: Please enter org alias

ID: Please enter org ID

* Parent: Please select   Type: Branch office

Resp person: Please enter the name   Telephone: Support to input mult

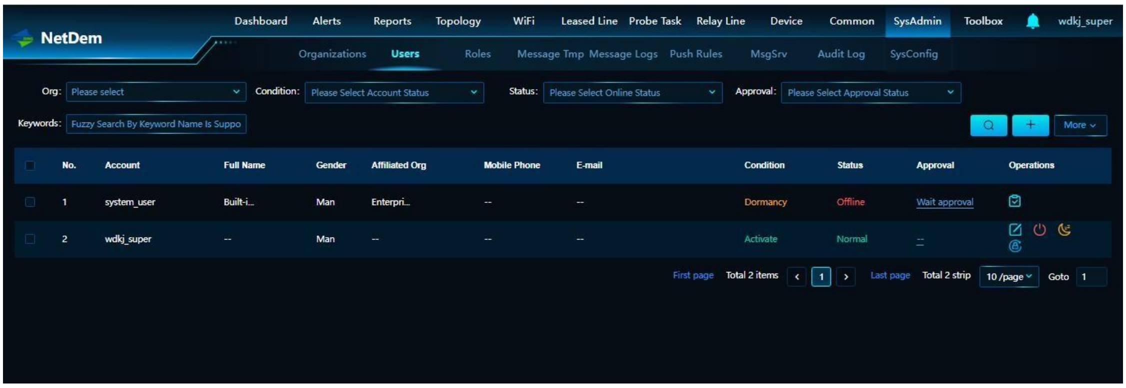
E-mail: Please enter E-mail

No.	Org	Resp person	Telephone
1	--	--	--
2	Enterprise	--	--

Previous page 1 Next page Last page Total 2 strip 10 /page

2.3.11.2. User Management

User management is the management of user accounts using the system.



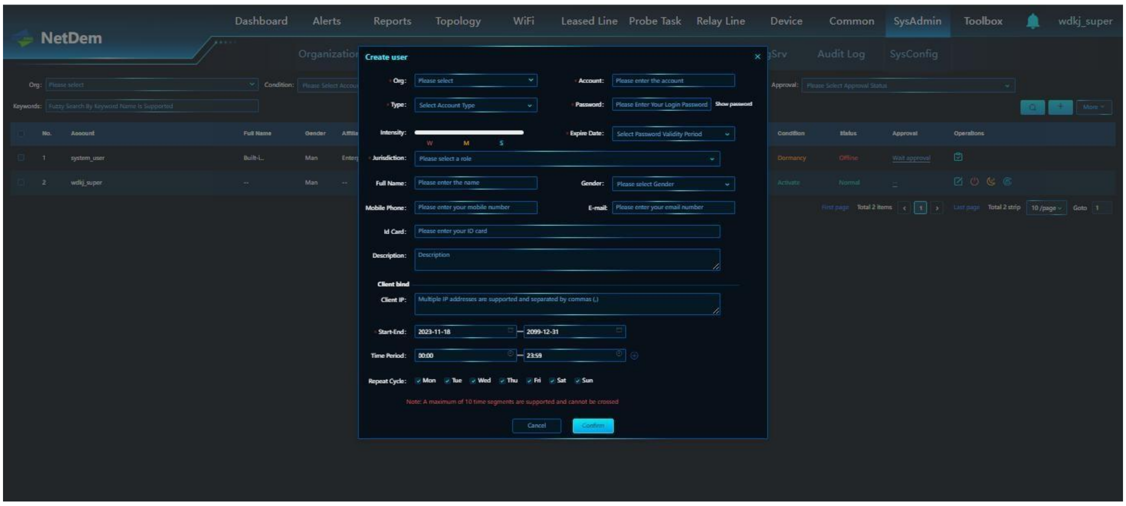
Org: Please select   Condition: Please Select Account Status   Status: Please Select Online Status   Approval: Please Select Approval Status

Keywords: Fuzzy Search By Keyword Name Is Suppo

No.	Account	Full Name	Gender	Affiliated Org	Mobile Phone	E-mail	Condition	Status	Approval	Operations
1	system_user	Built-i...	Man	Enterpri...	--	--	Dormancy	Offline	Wait approval	
2	wdkj_super	--	Man	--	--	--	Activate	Normal	--	

First page Total 2 items ‹ 1 › Last page Total 2 strip 10 /page Goto 1

- Support multi-user account management, including adding, deleting, modifying, checking, freezing, activating, and password reset;
- Supports control of user function permissions and data scope based on organization + role;
- Input information includes: account number, password, password validity period, affiliation, account status, role name, gender, mobile phone number, email, and personnel name;
- Supports the provision of rich authentication security control mechanisms, such as password complexity and automatic locking for abnormal logins.

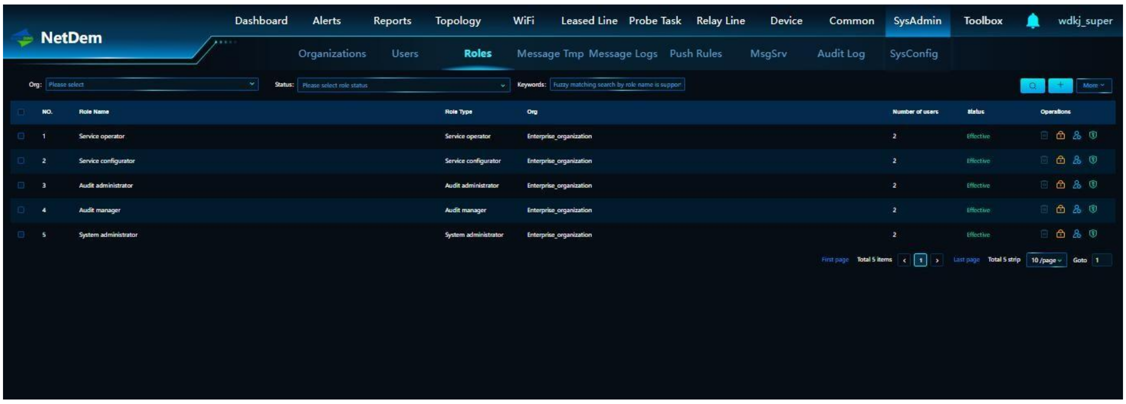


Org: Please select
Account: Please enter the account
Type: Select Account Type
Password: Please Enter Your Login Password
Intensity:
Expire Date: Select Password Validity Period
Jurisdiction: Please select a role
Full Name: Please enter the name
Gender: Please select Gender
Mobile Phone: Please enter your mobile number
E-mail: Please enter your email number
Id Card: Please enter your ID card
Description: Description
Client IP: Multiple IP addresses are supported and separated by commas (,)
Start-End: 2023-11-18 — 2099-12-31
Time Period: 00:00 — 23:59
Repeat Cycle: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Note: A maximum of 10 time segments are supported and cannot be crossed

2.3.11.3. Role management

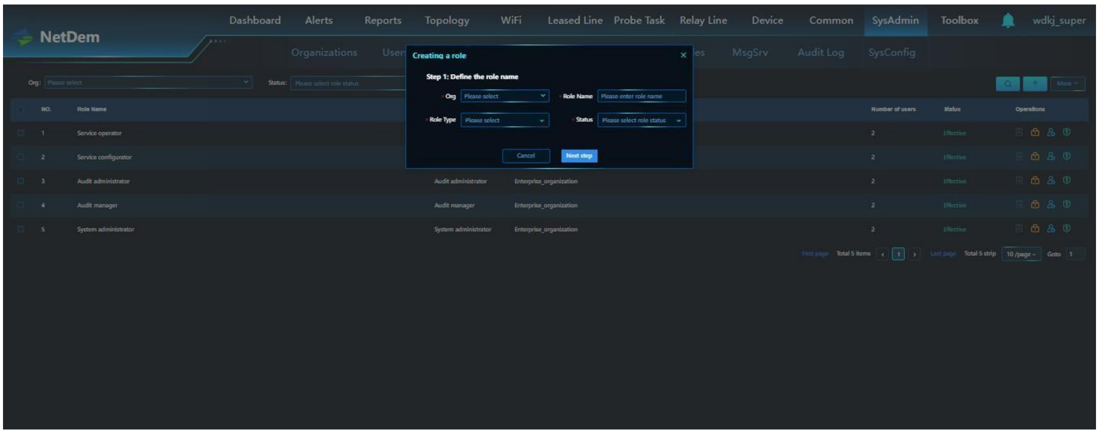
Role management is the management of user roles. It supports configuring function permissions and data ranges for roles. When a user is associated with a role, the role permissions are given to the user. Supports adding, deleting, checking, freezing, activating, adding



Org: Please select
Status: Please select role status
Keywords: Fuzzy matching search by role name is suppor

NO.	Role Name	Role Type	Org	Number of users	Status	Operations
1	Service operator	Service operator	Enterprise_organization	2	Effective	
2	Service configurator	Service configurator	Enterprise_organization	2	Effective	
3	Audit administrator	Audit administrator	Enterprise_organization	2	Effective	
4	Audit manager	Audit manager	Enterprise_organization	2	Effective	
5	System administrator	System administrator	Enterprise_organization	2	Effective	

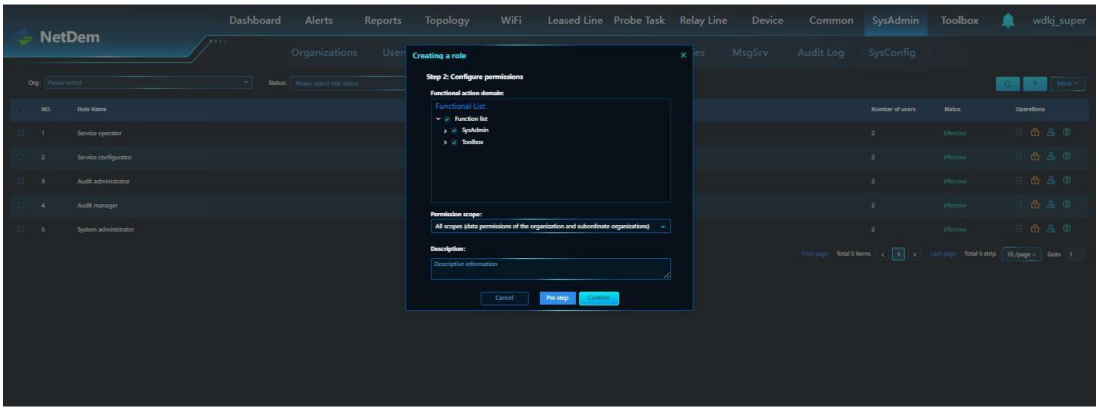
First page Total 5 items ‹ 1 › Last page Total 5 strip 10 /page Goto 1



Step 1: Define the role name

Org: Please select
Role Name: Please enter role name
Role Type: Please select
Status: Please select role status

personnel and permission management of roles.



Org: Please select Status: Please select role status

NO.	Role Name	Number of users	Status
1	Service operator	2	Effective
2	Service configurator	2	Effective
3	Audit administrator	2	Effective
4	Audit manager	2	Effective
5	System administrator	2	Effective

First page Total 5 items ‹ 1 › Last page Total 5 strip 10 /page Goto 1

Creating a role ×

Step 2: Configure permissions

Functional action domain:

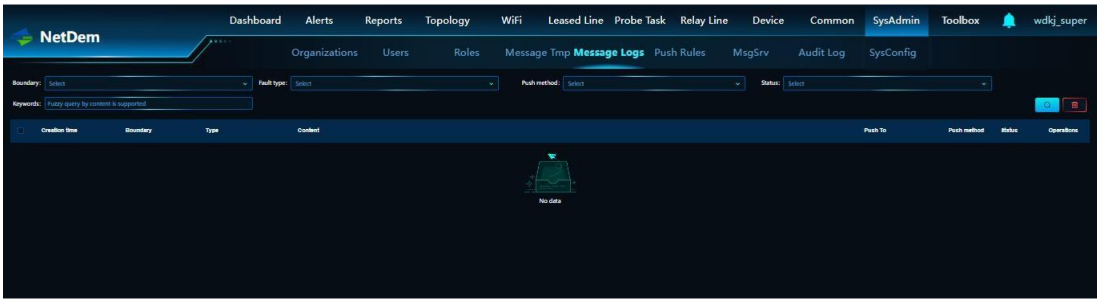
Functional List:
- ☑ Function list
  - ☑ SysAdmin
  - ☑ Toolbox

Permission scope: All scopes (data permissions of the organization and subordinate organizations)

Description: Descriptive information

2.3.11.4. Message record

Message record is the management of message push records, including SMS and email push records. It supports viewing of push status, query of message records, and deletion of message records.



Boundary: Select Fault type: Select Push method: Select Status: Select

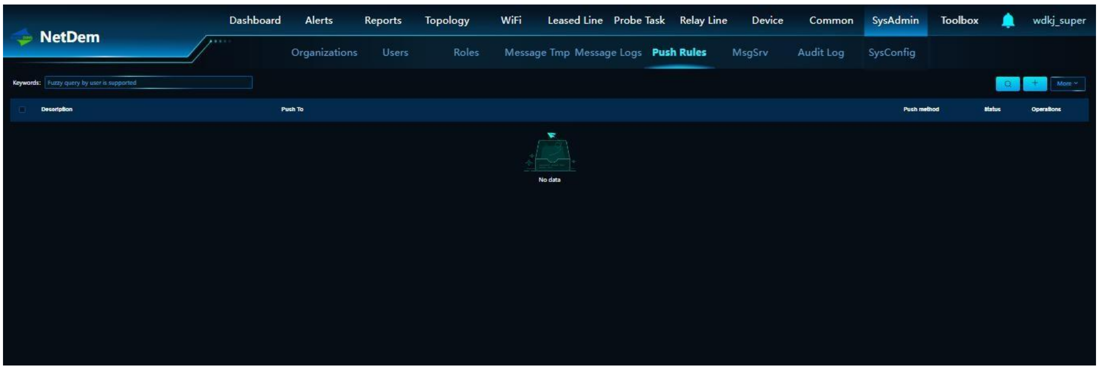
Keywords: Fuzzy query by content is supported

Creation time	Boundary	Type	Content	Push To	Push method	Status	Operations

No data

2.3.11.5. Push rules

Push rules are the management of message push strategies. When an alarm is triggered, messages are pushed to users according to the message push rules, including defining the alarm types that need to be pushed, the push method, etc. Support query, add, modify, delete, freeze and activate push rules;



Keywords: Fuzzy query by user is supported

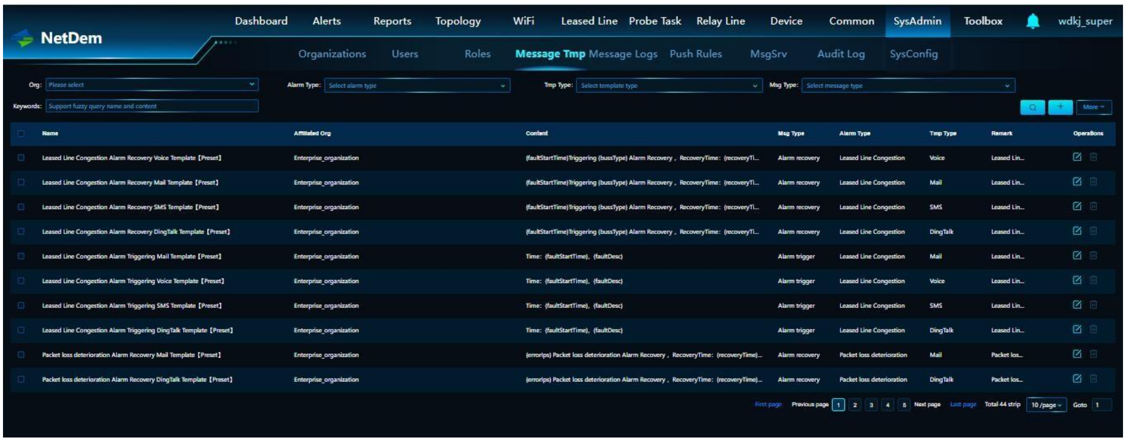
□	Description	Push To	Push method	Status	Operations

No data

- ➢ Supports query rules based on conditions and users.
- ➢ Supports adding new push rules, supports simple settings (all alarm information is pushed by default) and can also be switched to advanced settings (specify conditions for alarm push)
- ➢ Supports deletion of push rules;
- ➢ Supports freezing of push rules, updated from "valid" to "invalid";
- ➢ Select the data with the status "Invalid" in the list, click the [Activate] button above the list, the activation prompt will pop up, after confirmation, activate the data, and update the status of the data in the list, from "Invalid" updated to "valid";

2.3.11.6. Message template

Message templates support user-defined templates. When an alarm is triggered, messages are pushed based on the content of the defined message template. Main functions: adding, modifying, deleting templates, etc.



Org: Please select
Alarm Type: Select alarm type
Tmp Type: Select template type
Msg Type: Select message type
Keywords: Support fuzzy query name and content

Name	Affiliated Org	Content	Msg Type	Alarm Type	Tmp Type	Remark	Operations
Leased Line Congestion Alarm Recovery Voice Template【Preset】	Enterprise_organization	{faultStartTime}Triggering {bussType} Alarm Recovery，RecoveryTime：{recoveryTi...	Alarm recovery	Leased Line Congestion	Voice	Leased Lin...	
Leased Line Congestion Alarm Recovery Mail Template【Preset】	Enterprise_organization	{faultStartTime}Triggering {bussType} Alarm Recovery，RecoveryTime：{recoveryTi...	Alarm recovery	Leased Line Congestion	Mail	Leased Lin...	
Leased Line Congestion Alarm Recovery SMS Template【Preset】	Enterprise_organization	{faultStartTime}Triggering {bussType} Alarm Recovery，RecoveryTime：{recoveryTi...	Alarm recovery	Leased Line Congestion	SMS	Leased Lin...	
Leased Line Congestion Alarm Recovery DingTalk Template【Preset】	Enterprise_organization	{faultStartTime}Triggering {bussType} Alarm Recovery，RecoveryTime：{recoveryTi...	Alarm recovery	Leased Line Congestion	DingTalk	Leased Lin...	
Leased Line Congestion Alarm Triggering Mail Template【Preset】	Enterprise_organization	Time：{faultStartTime}，{faultDesc}	Alarm trigger	Leased Line Congestion	Mail	Leased Lin...	
Leased Line Congestion Alarm Triggering Voice Template【Preset】	Enterprise_organization	Time：{faultStartTime}，{faultDesc}	Alarm trigger	Leased Line Congestion	Voice	Leased Lin...	
Leased Line Congestion Alarm Triggering SMS Template【Preset】	Enterprise_organization	Time：{faultStartTime}，{faultDesc}	Alarm trigger	Leased Line Congestion	SMS	Leased Lin...	
Leased Line Congestion Alarm Triggering DingTalk Template【Preset】	Enterprise_organization	Time：{faultStartTime}，{faultDesc}	Alarm trigger	Leased Line Congestion	DingTalk	Leased Lin...	
Packet loss deterioration Alarm Recovery Mail Template【Preset】	Enterprise_organization	{errorIps} Packet loss deterioration Alarm Recovery，RecoveryTime：{recoveryTime}...	Alarm recovery	Packet loss deterioration	Mail	Packet los...	
Packet loss deterioration Alarm Recovery DingTalk Template【Preset】	Enterprise_organization	{errorIps} Packet loss deterioration Alarm Recovery，RecoveryTime：{recoveryTime}...	Alarm recovery	Packet loss deterioration	DingTalk	Packet los...	

First page Previous page 1 2 3 4 5 Next page Last page Total 44 strip 10 /page Goto 1

Supports configuring alarm triggering/alarm recovery templates;

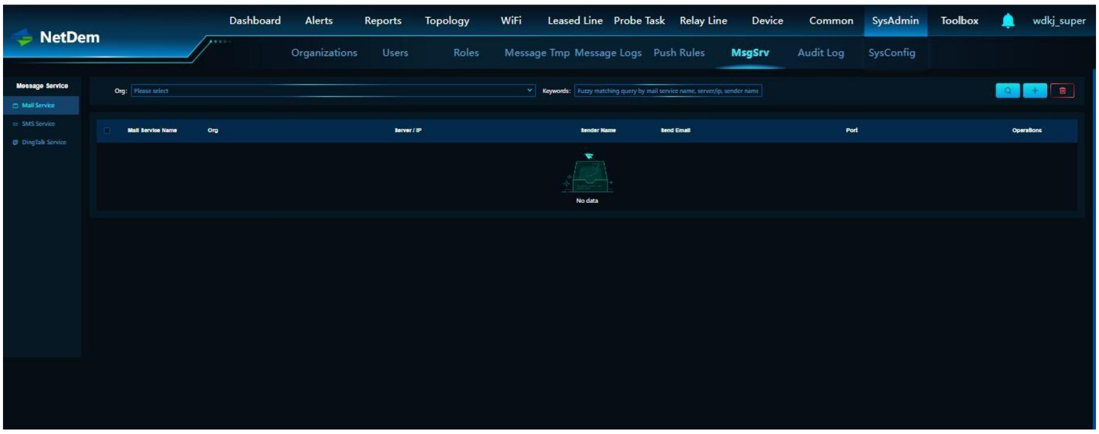
Supports configuring SMS/email templates;

Supports template query, addition, modification, deletion and other operations;

Support inserting variables to combine message content;

2.3.11.7. Messaging service

Message service is the configuration of user message services, including email service and SMS service. When an alarm is triggered, you can use the configured service to push messages. Supports comprehensive management of message services such as query, addition, modification, and deletion.



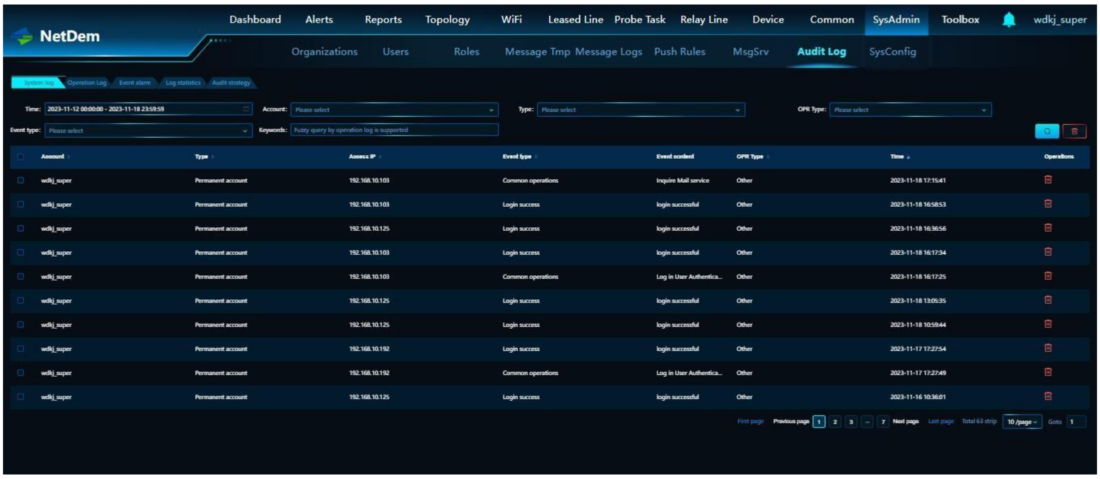
Org: Please select
Keywords: Fuzzy matching query by mail service name, server/ip, sender name

Mail Service Name	Org	Server / IP	Sender Name	Send Email	Port	Operations

No data

2.3.11.8. Security audit

Supports recording system logs such as successful login, failed login, exit, unauthorized access, etc.;

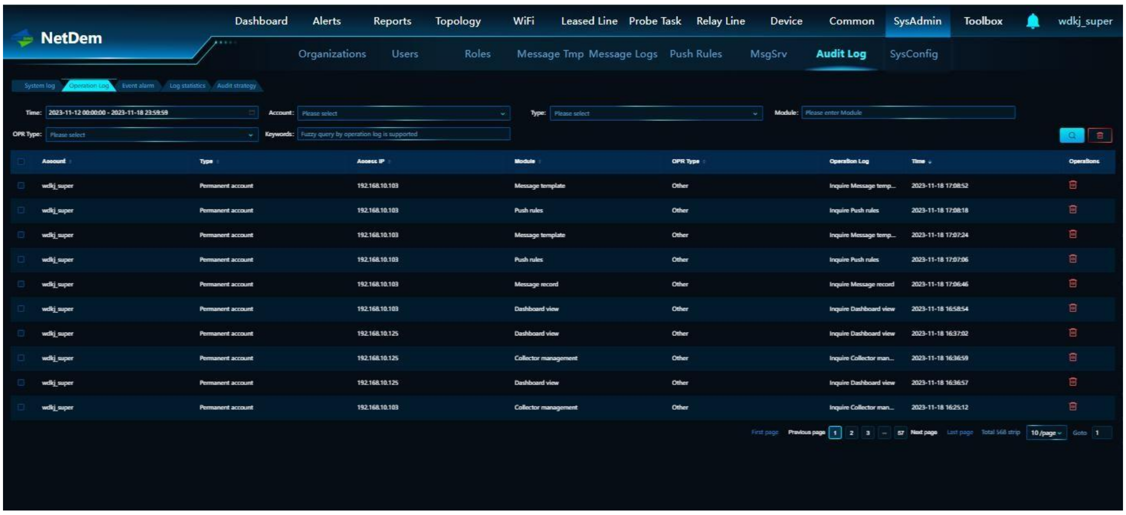


Time: 2023-11-12 00:00:00 - 2023-11-18 23:59:59
Account: Please select
Type: Please select
OPR Type: Please select
Event type: Please select
Keywords: Fuzzy query by operation log is supported

□	Account	Type	Access IP	Event type	Event content	OPR Type	Time	Operations
□	wdkj_super	Permanent account	192.168.10.103	Common operations	Inquire Mail service	Other	2023-11-18 17:15:41	🗑
□	wdkj_super	Permanent account	192.168.10.103	Login success	login successful	Other	2023-11-18 16:58:53	🗑
□	wdkj_super	Permanent account	192.168.10.125	Login success	login successful	Other	2023-11-18 16:36:56	🗑
□	wdkj_super	Permanent account	192.168.10.103	Login success	login successful	Other	2023-11-18 16:17:34	🗑
□	wdkj_super	Permanent account	192.168.10.103	Common operations	Log in User Authentica...	Other	2023-11-18 16:17:25	🗑
□	wdkj_super	Permanent account	192.168.10.125	Login success	login successful	Other	2023-11-18 13:05:35	🗑
□	wdkj_super	Permanent account	192.168.10.125	Login success	login successful	Other	2023-11-18 10:59:44	🗑
□	wdkj_super	Permanent account	192.168.10.192	Login success	login successful	Other	2023-11-17 17:27:54	🗑
□	wdkj_super	Permanent account	192.168.10.192	Common operations	Log in User Authentica...	Other	2023-11-17 17:27:49	🗑
□	wdkj_super	Permanent account	192.168.10.125	Login success	login successful	Other	2023-11-16 10:36:01	🗑

First page Previous page 1 2 3 ... 7 Next page Last page Total 63 strip 10 /page Goto 1

Supports recording business-level operation logs such as additions, deletions, modifications and checks of business data;

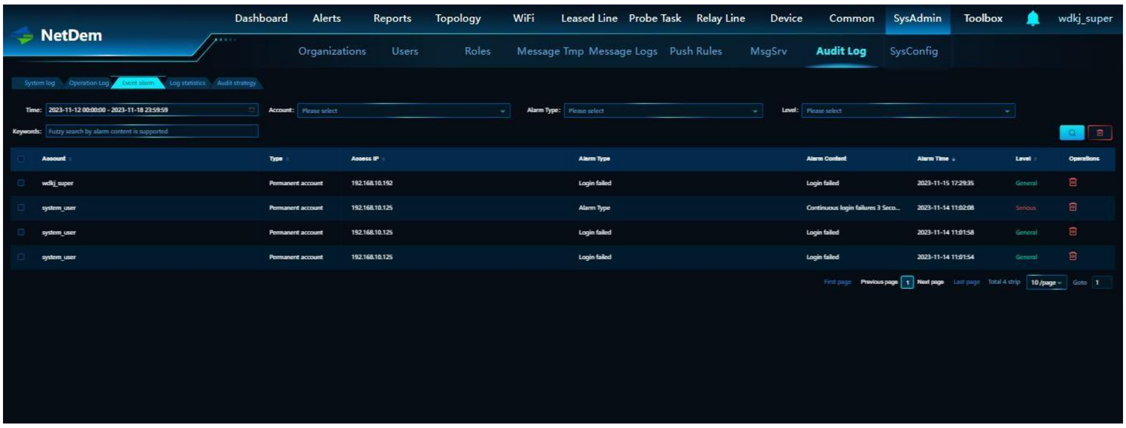


Time: 2023-11-12 00:00:00 - 2023-11-18 23:59:59
Account: Please select
Type: Please select
Module: Please enter Module
OPR Type: Please select
Keywords: Fuzzy query by operation log is supported

□	Account	Type	Access IP	Module	OPR Type	Operation Log	Time	Operations
□	wdkj_super	Permanent account	192.168.10.103	Message template	Other	Inquire Message temp...	2023-11-18 17:08:52	🗑
□	wdkj_super	Permanent account	192.168.10.103	Push rules	Other	Inquire Push rules	2023-11-18 17:08:18	🗑
□	wdkj_super	Permanent account	192.168.10.103	Message template	Other	Inquire Message temp...	2023-11-18 17:07:24	🗑
□	wdkj_super	Permanent account	192.168.10.103	Push rules	Other	Inquire Push rules	2023-11-18 17:07:06	🗑
□	wdkj_super	Permanent account	192.168.10.103	Message record	Other	Inquire Message record	2023-11-18 17:06:46	🗑
□	wdkj_super	Permanent account	192.168.10.103	Dashboard view	Other	Inquire Dashboard view	2023-11-18 16:58:54	🗑
□	wdkj_super	Permanent account	192.168.10.125	Dashboard view	Other	Inquire Dashboard view	2023-11-18 16:37:02	🗑
□	wdkj_super	Permanent account	192.168.10.125	Collector management	Other	Inquire Collector man...	2023-11-18 16:36:59	🗑
□	wdkj_super	Permanent account	192.168.10.125	Dashboard view	Other	Inquire Dashboard view	2023-11-18 16:36:57	🗑
□	wdkj_super	Permanent account	192.168.10.103	Collector management	Other	Inquire Collector man...	2023-11-18 16:25:12	🗑

First page Previous page 1 2 3 ... 57 Next page Last page Total 568 strip 10 /page Goto 1

Supports alarming for abnormal events such as continuous login failures, unauthorized access, abnormal IP addresses, etc.;



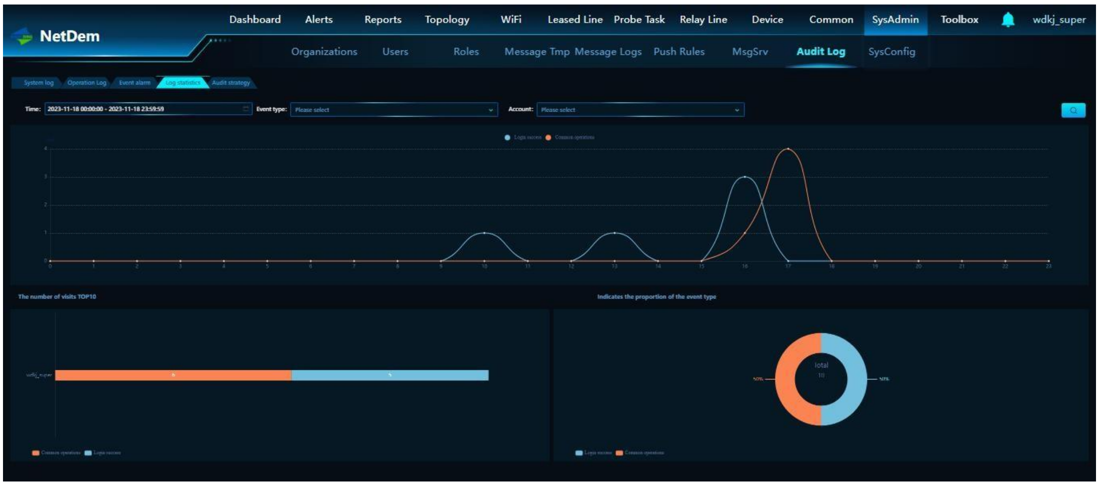
Time: 2023-11-12 00:00:00 - 2023-11-18 23:59:59 Account: Please select Alarm Type: Please select Level: Please select

Keywords: Fuzzy search by alarm content is supported

□	Account	Type	Access IP	Alarm Type	Alarm Content	Alarm Time	Level	Operations
□	wdkj_super	Permanent account	192.168.10.192	Login failed	Login failed	2023-11-15 17:29:35	General	🗑
□	system_user	Permanent account	192.168.10.125	Alarm Type	Continuous login failures 3 Seco...	2023-11-14 11:02:08	Serious	🗑
□	system_user	Permanent account	192.168.10.125	Login failed	Login failed	2023-11-14 11:01:58	General	🗑
□	system_user	Permanent account	192.168.10.125	Login failed	Login failed	2023-11-14 11:01:54	General	🗑

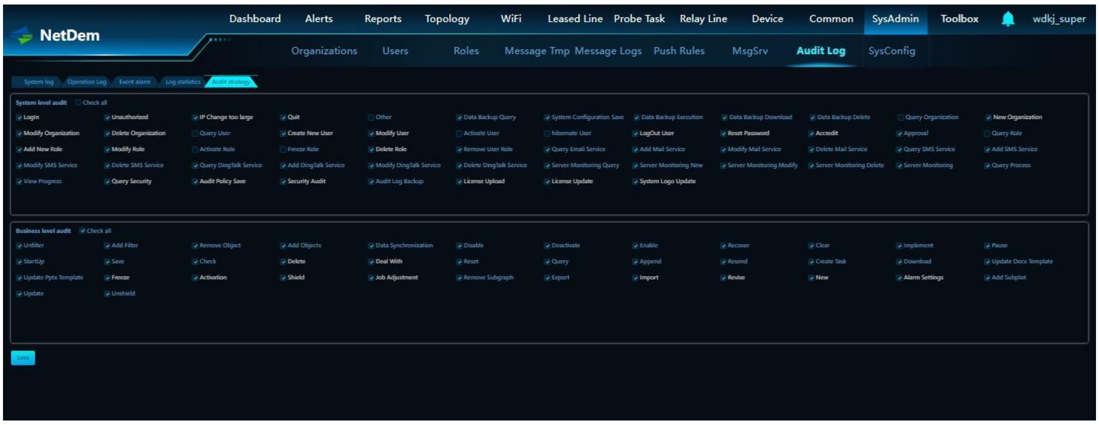
First page Previous page 1 Next page Last page Total 4 strip 10 /page Goto 1

Supports statistical analysis of system logs according to time period, account number, event type, etc.;



Time: 2023-11-18 00:00:00 - 2023-11-18 23:59:59 Event type: Please select Account: Please select

Support the configuration of audit policies;



System level audit ☐ Check all

☑ Login ☑ Unauthorized ☑ IP Change too large ☑ Quit ☐ Other ☑ Data Backup Query ☑ System Configuration Save ☑ Data Backup Execution ☑ Data Backup Download ☑ Data Backup Delete ☐ Query Organization ☑ New Organization

☑ Modify Organization ☑ Delete Organization ☐ Query User ☑ Create New User ☑ Modify User ☐ Activate User ☐ hibernate User ☑ LogOut User ☑ Reset Password ☑ Accredit ☑ Approval ☐ Query Role

☑ Add New Role ☑ Modify Role ☐ Activate Role ☐ Freeze Role ☑ Delete Role ☑ Remove User Role ☑ Query Email Service ☑ Add Mail Service ☑ Modify Mail Service ☑ Delete Mail Service ☑ Query SMS Service ☑ Add SMS Service

☑ Modify SMS Service ☑ Delete SMS Service ☑ Query DingTalk Service ☑ Add DingTalk Service ☑ Modify DingTalk Service ☑ Delete DingTalk Service ☑ Server Monitoring Query ☑ Server Monitoring New ☑ Server Monitoring Modify ☑ Server Monitoring Delete ☑ Server Monitoring ☑ Query Process

☑ View Progress ☑ Query Security ☑ Audit Policy Save ☑ Security Audit ☑ Audit Log Backup ☑ License Upload ☑ License Update ☑ System Logo Update

Business level audit ☑ Check all

☑ Unfilter ☑ Add Filter ☑ Remove Object ☑ Add Objects ☑ Data Synchronization ☑ Disable ☑ Deactivate ☑ Enable ☑ Recover ☑ Clear ☑ Implement ☑ Pause

☑ StartUp ☑ Save ☑ Check ☑ Delete ☑ Deal With ☑ Reset ☑ Query ☑ Append ☑ Resend ☑ Create Task ☑ Download ☑ Update Docx Template

☑ Update Pptx Template ☑ Freeze ☑ Activation ☑ Shield ☑ Job Adjustment ☑ Remove Subgraph ☑ Export ☑ Import ☑ Revise ☑ New ☑ Alarm Settings ☑ Add Subplot

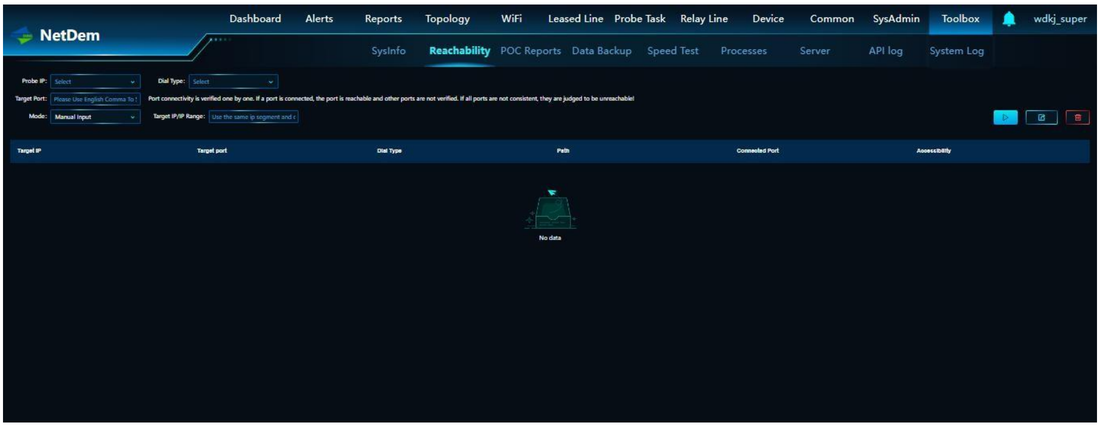
☑ Update ☑ Unshield

2.3.12. Toolbox

2.3.12.1. Reachability verification

Supports selecting probe IP + dialing test method, detecting port, uploading attachments, dialing and testing the target in the attachment, and generating execution results after the execution is completed. The execution results support downloading and viewing;

It supports selecting the probe IP + Probe Test method, detecting the port, inputting the IP or IP segment, and dialing the input target IP/IP segment. After the execution is completed, the execution result is generated, and the execution result supports downloading and viewing;



Probe IP: Select
Dial Type: Select
Target Port: Please Use English Comma To !
Port connectivity is verified one by one. If a port is connected, the port is reachable and other ports are not verified. If all ports are not consistent, they are judged to be unreachable!
Mode: Manual Input
Target IP/IP Range: Use the same ip segment and c

Target IP	Target port	Dial Type	Path	Connected Port	Accessibility

Manual Entry

Supports selecting probe IP + Probe Test method, detecting port, input IP or IP segment, click the [Execute] button to automatically execute. When the input is an IP segment, each IP will be listed in the list below. After the execution is completed, the execution result will be generated. Execute The results can be downloaded and viewed.

When there are multiple input ports, the port connectivity is verified one by one. If one port is connected, it is determined to be reachable and other ports are not verified; if all ports are unreachable, it is determined to be unreachable;

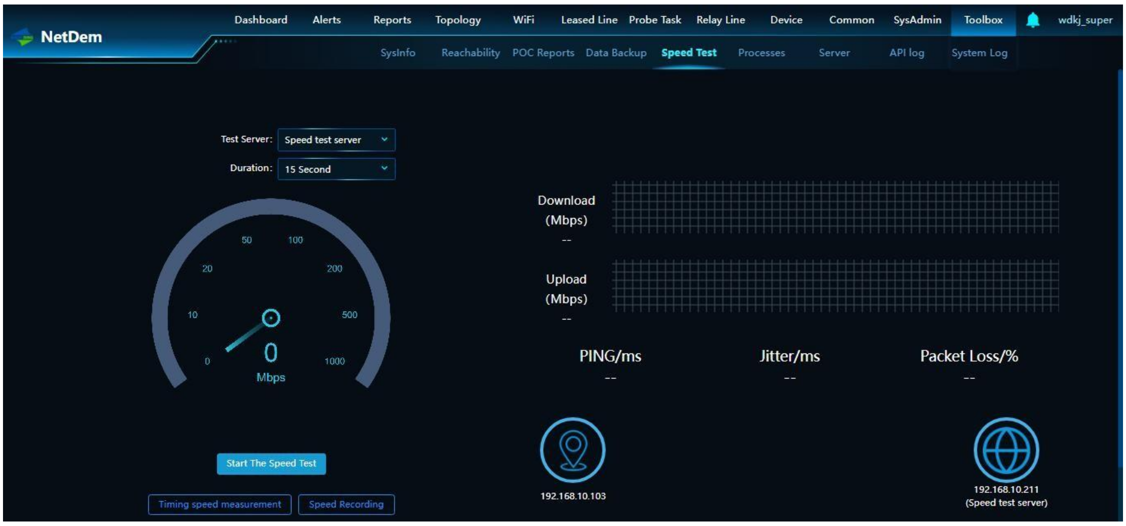
Batch Import

Select the probe IP + Probe Test method, detection port, and upload attachments. The attachment fields include: target IP/target address segment + target port. After the upload is completed, click the [Execute] button to automatically execute. After the execution is completed, the execution results are generated. The execution results support Download to view.

When there are multiple input ports, in addition to dialing and testing the imported ports, the connectivity of the input ports is verified one by one. If a port is connected, it will be determined to be reachable and other ports will not be verified; if all ports are unreachable, it will be determined to be unreachable!

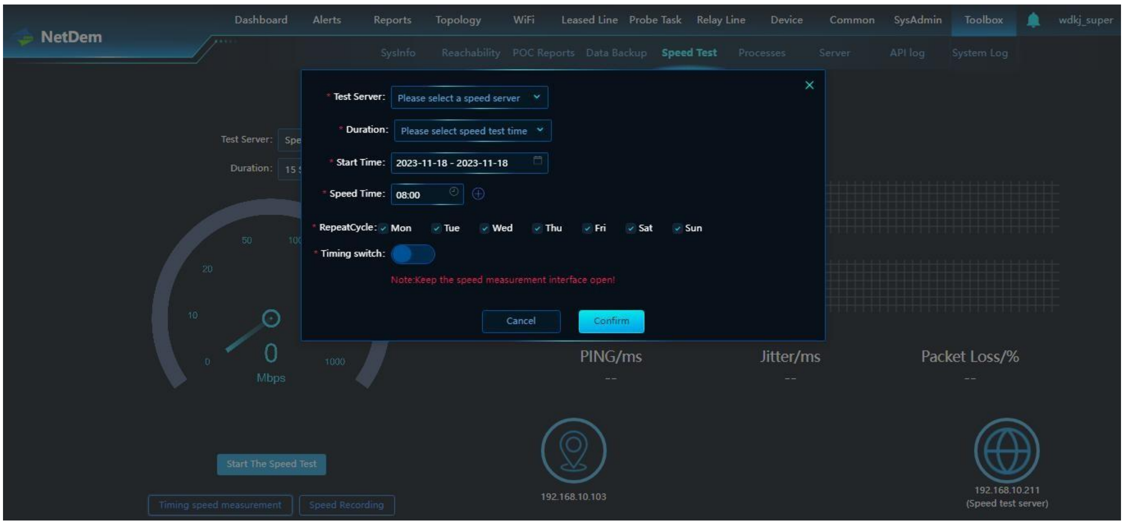
2.3.12.2. Online speed test

- Deploy a speed measurement server at the headquarters to support each branch's web terminal to detect the network speed from the branch to the headquarters;
- When a branch passes a dedicated line to the headquarters, it automatically locates which dedicated line it passes through;
- Support timing speed measurement;
- Support online speed measurement;
- Supports viewing of speed measurement records;



Test Server: Speed test server

Duration: 15 Second



* Test Server: Please select a speed server

* Duration: Please select speed test time

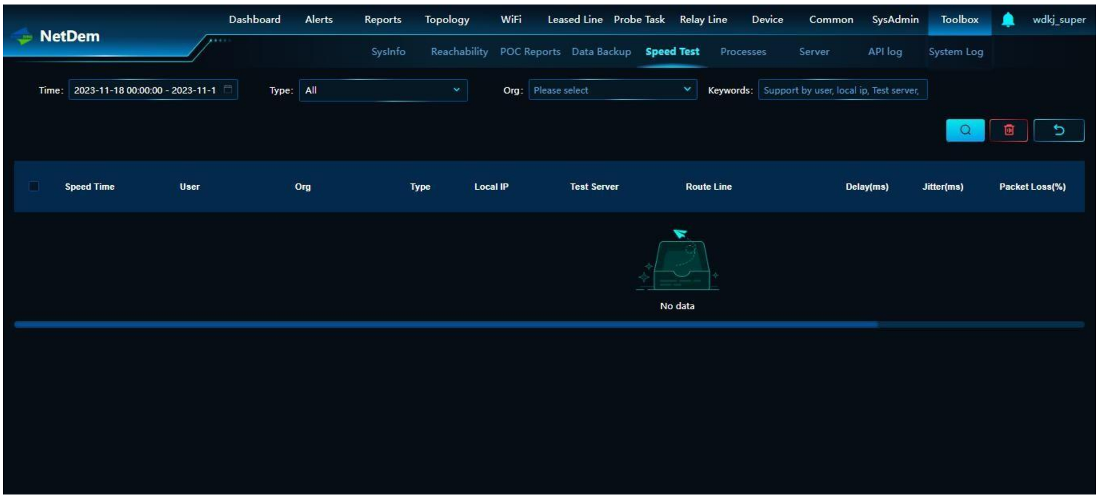
* Start Time: 2023-11-18 - 2023-11-18

* Speed Time: 08:00

* RepeatCycle: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

* Timing switch:

Note:Keep the speed measurement interface open!



Time: 2023-11-18 00:00:00 - 2023-11-1

Type: All

Org: Please select

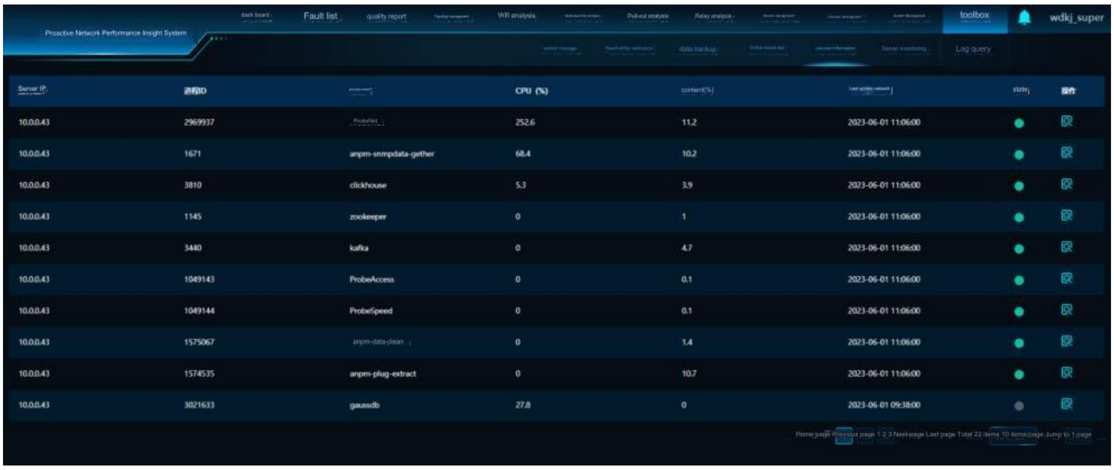
Keywords: Support by user, local ip, Test server,

□	Speed Time	User	Org	Type	Local IP	Test Server	Route Line	Delay(ms)	Jitter(ms)	Packet Loss(%)

No data

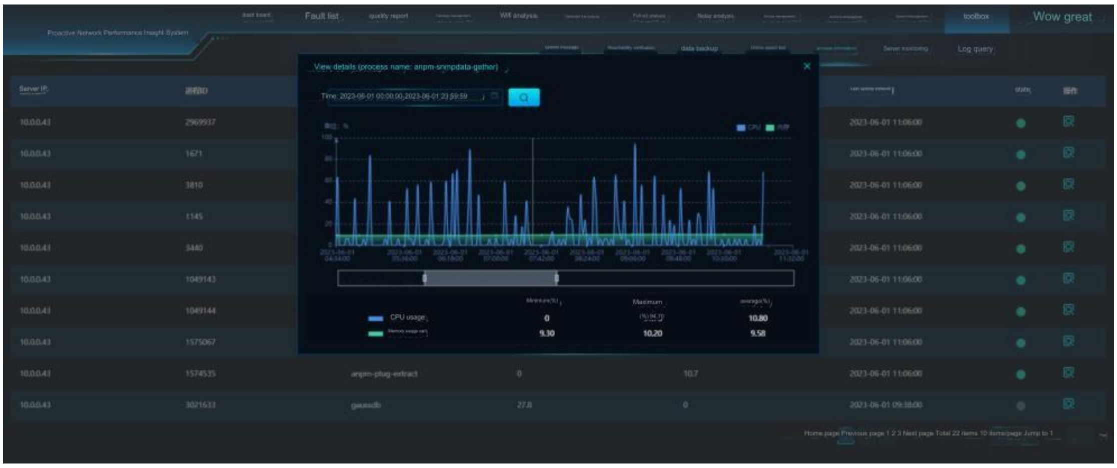
2.3.12.3. Process information

Monitor the status of the service processes required by the system; the list displays the latest status and latest monitoring data; supports detailed viewing of trend charts of memory and CPU occupied by the process.



Server IP	进程ID	[illegible]	CPU (%)	content(%)	[illegible]	state	操作
10.0.0.43	2969937	ProbeNet	252.6	11.2	2023-06-01 11:06:00	●	
10.0.0.43	1671	anpm-snmpdata-gether	68.4	10.2	2023-06-01 11:06:00	●	
10.0.0.43	3810	clickhouse	5.3	3.9	2023-06-01 11:06:00	●	
10.0.0.43	1145	zookeeper	0	1	2023-06-01 11:06:00	●	
10.0.0.43	3440	kafka	0	4.7	2023-06-01 11:06:00	●	
10.0.0.43	1049143	ProbeAccess	0	0.1	2023-06-01 11:06:00	●	
10.0.0.43	1049144	ProbeSpeed	0	0.1	2023-06-01 11:06:00	●	
10.0.0.43	1575067	anpm-data-clean	0	1.4	2023-06-01 11:06:00	●	
10.0.0.43	1574535	anpm-plug-extract	0	10.7	2023-06-01 11:06:00	●	
10.0.0.43	3021633	gaussdb	27.8	0	2023-06-01 09:38:00	●	

Home page Previous page 1 2 3 Next page Last page Total 22 items 10 items/page Jump to 1 page



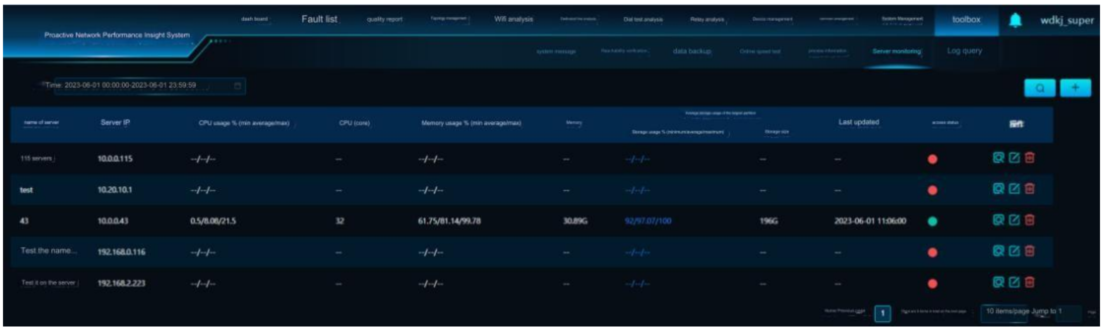
View details (process name: anpm-snmpdata-gether)

Time: 2023-06-01 00:00:00,2023-06-01 23:59:59

	Minimum(%)	Maximum	average(%)
CPU usage	0	(%) 94.70	10.80
Memory usage rate	9.30	10.20	9.58

2.3.12.4. Server monitoring

Supports monitoring of server resource usage, including CPU, memory, and disk. Supports adding multiple servers for monitoring.



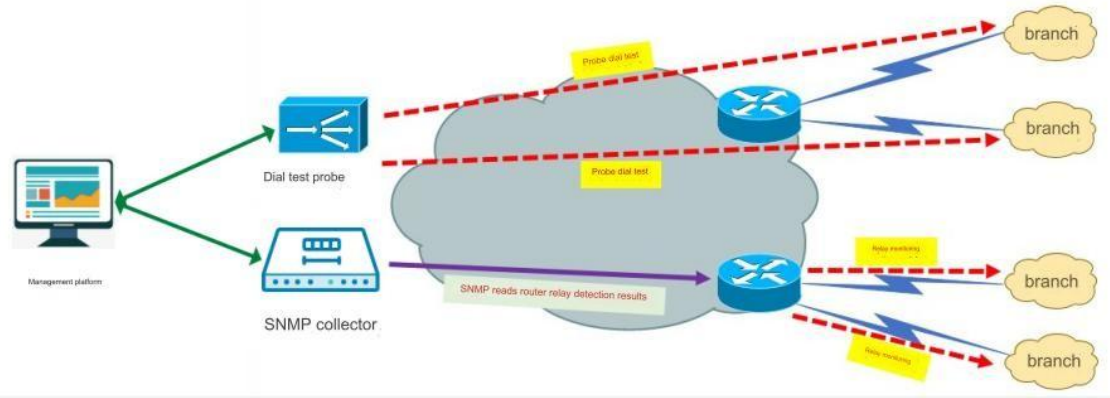
Time: 2023-06-01 00:00:00-2023-06-01 23:59:59

						Average storage usage of the largest partition				
name of server	Server IP	CPU usage % (min average/max)	CPU (core)	Memory usage % (min average/max)	Memory	Storage usage % (minimum/average/maximum)	Storage size	Last updated	access status	[illegible]
115 servers	10.0.0.115	--/--/--	--	--/--/--	--	--/--/--	--	--	●	
test	10.20.10.1	--/--/--	--	--/--/--	--	--/--/--	--	--	●	
43	10.0.0.43	0.5/8.08/21.5	32	61.75/81.14/99.78	30.89G	92/97.07/100	196G	2023-06-01 11:06:00	●	
Test the name...	192.168.0.116	--/--/--	--	--/--/--	--	--/--/--	--	--	●	
Test it on the server	192.168.2.223	--/--/--	--	--/--/--	--	--/--/--	--	--	●	

1 10 items/page Jump to 1

2.3.13. Collector

The collector refers to the data collection agent program, which is divided into Probe Test probe and SNMP collector. The probe probe sends detection data packets to the target IP, and the returned detection results are sent to the management platform, which performs statistics and analysis; the SNMP collector is used by network equipment (usually routers, switches) to send data to the target IP. IP sends detection data packets and records the detection results, and then collects the detection results through the SNMP collector and sends them to the management platform, which performs statistics and analysis.



2.3.13.1. Probe Test probe

The network events that the Probe Test probe can detect include three categories: interruption, delay degradation, and packet loss degradation.

The dial-test probe has no restrictions on the type of detection targets. For example, it can detect servers, videos, routers, switches, LAN links, dedicated line links, external websites, etc., as long as the detection packets between the probe and the target IP can be detected normally. Just reach it. The Probe Test probe supports multiple Probe Test protocols: ICMP Ping, ICMP Trace, UDP Trace, and TCP Trace.

- The probe receives the collection instructions from the basic management platform and performs the testing tasks according to the instructions.
- Through the Probe Test function, network performance data is collected in real time, and corresponding operating indicators are generated after real-time analysis for the platform to analyze and monitor the end-to-end quality of the dedicated line.
- The probe uploads the collected network operation indicators to the basic management platform.

2.3.13.2. SNMP collector

The network events that can be detected by relay monitoring include three categories: interruption, delay degradation, and packet loss degradation. Relay monitoring is suitable for the following scenarios: lines with unreachable routes, such as backup lines with no traffic, or lines with no route published on the Internet address; lines with changing routes.

- The collector receives the collection instructions from the basic management platform and performs collection tasks according to the instructions;
- Through the collection function, network equipment indicator data is collected in real time, and corresponding operating indicators are generated after real-time analysis for the platform to analyze

and monitor network operation quality;

- The collector uploads the collected network operation indicators to the basic management platform;

2.3.13.3. License management

License management is controlled by time and the number of monitoring objects, which refers to test targets and relays.

1. 1 License in the test task = 1 destination IP address = full link from probe to 1 destination IP address.

2. The test target with the same IP is regarded as a License.

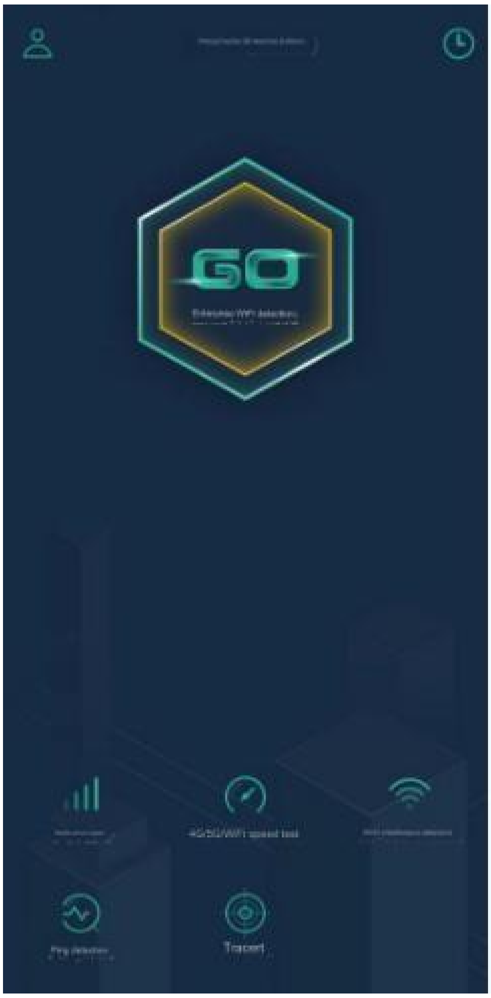
3. The same trunk is considered to occupy a License.

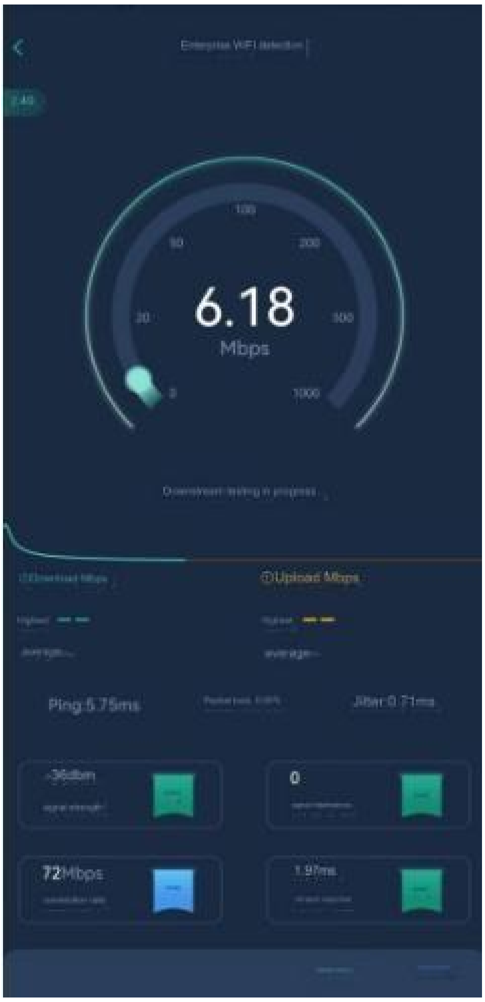
4. After the expiration of License, the system will automatically suspend data collection and analysis.

2.4. Wangchacha APP

2.4.1. Enterprise WiFi detection

- Provide mobile phones to connect to WIFI for signal coverage and signal quality testing in the service area, and support taking photos and note tags at the testing locations;
- Supports external network speed measurement and internal network speed measurement;
- Supports viewing of test results, including signal quality, signal interference, negotiation rate, encryption method, and router gateway performance;
- Supports pushing test results to the management platform to generate quality reports;

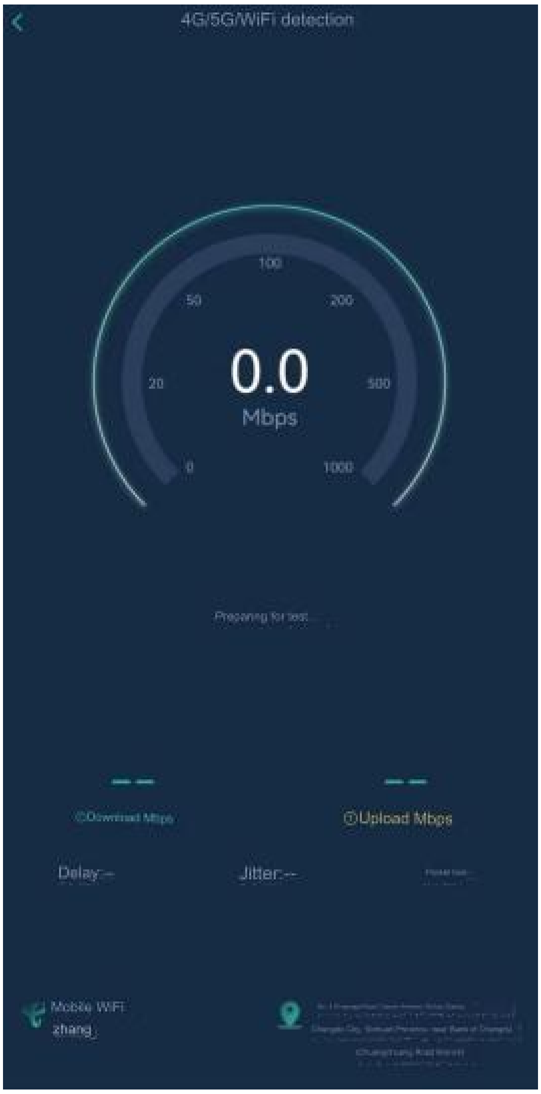


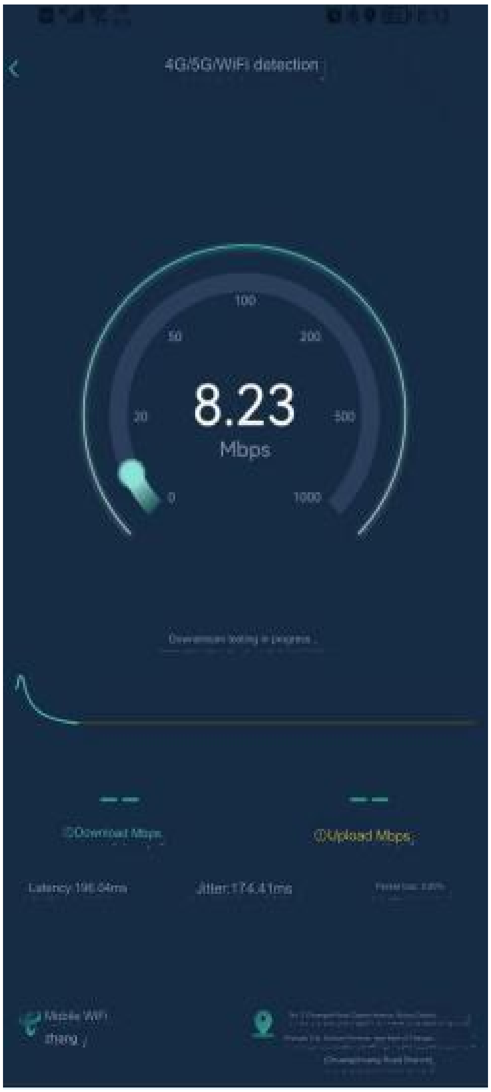


2.4.2.4 G5GWiFiSpeed Test

- Provides 4G, 5G, and WiFi network bandwidth speed testing, with indicators including device test location information, maximum upload rate, minimum upload rate, average upload rate, maximum download rate, minimum download rate, average download rate, network delay, packet loss, etc. index;
- When the mobile device is connected to the enterprise WiFi, the speed measurement process increases. The mobile phone is applied to the box to measure the speed results (internal network speed); if the external network speed exceeds 100Mbps, the internal network speed measurement is not performed. When it is not in the same network segment, it will be skipped if it cannot be executed;

- Provide 4G, 5G, and WiFi network test reports. The test reports include basic information on WiFi/mobile network signal strength, bandwidth speed test results, network performance, and user experience evaluation;

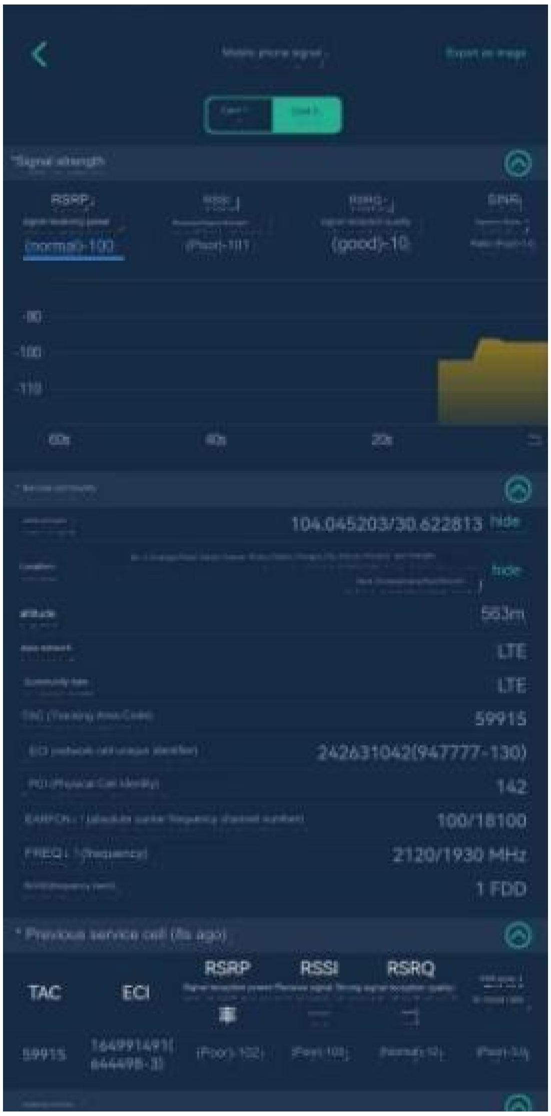




2.4.3. Mobile phone signal

- Provide multiple SIM signal quality collection functions, switch different cards to view signal quality, including signal strength, serving cell, neighboring cells, mobile phone information and network operator information;

- Provide mobile phone wireless signal quality trend charts, which report RSRP, RSSI, RSRLQ, and SINR evaluation indicator tracking;
- Supports collection of mobile phone base station location and detailed information analysis data, including data network, cell type, TAC (area tracking code), ECI (network cell unique identifier), PCI (physical cell identifier), BAND WIDTH (signal broadband), EARFCN (absolute carrier frequency channel number), FREQ (frequency) and BAND (frequency band) indicators;
- Provide signal quality analysis of mobile phone connection base stations and cells, which reports TAC, ECI, RSRP, RSSI, RSRQ, and PCI indicators;
- Provide basic information about mobile phone terminals, including terminal device system version number, device model, and SIM operator information;
- Provide the current SIM network operator information, including operator name, MCC and MNC information;
- Supports exporting detailed base station analysis data and all detailed data of the day collected by the current SIM in text format, and supports automatic sharing to WeChat, DingTalk, SMS, and Bluetooth using the mobile terminal system;
- Supports the function of exporting the collection results to share pictures on WeChat and save them to the photo album;



Signal strength

RSRP	RSSI	RSRQ	SINR
(normal)-100	(Poor)-111	(good)-10	[illegible]

Location: 104.045203/30.622813 hide

altitude 563m

LTE

LTE

TAC (Tracking Area Code) 59915

ECI (network cell unique identifier) 242631042(947777-130)

PCI (Physical Cell Identity) 142

EARFCN (absolute carrier frequency channel number) 100/18100

FREQ (frequency) 2120/1930 MHz

1 FDD

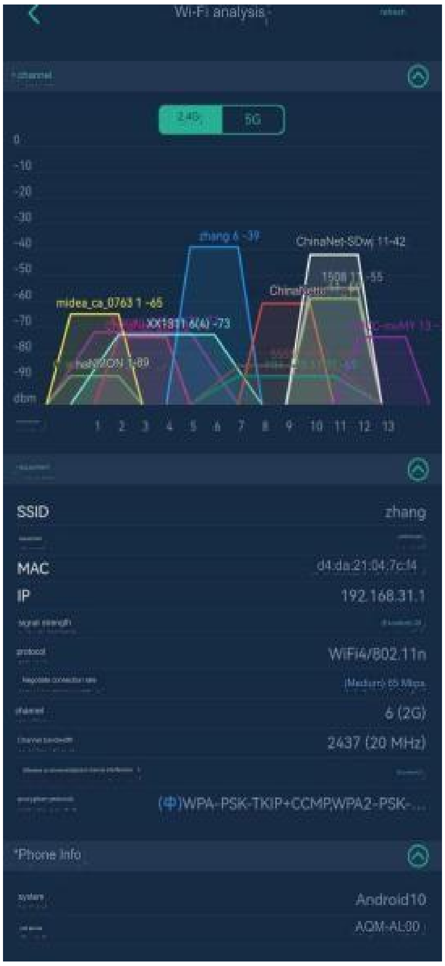
* Previous service cell (8s ago)

TAC	ECI	RSRP	RSSI	RSRQ	
59915	1649914911 644498-3)	(Poor)-102)	(Poor)-103)	(Normal)-10)	(Poor)-3)

2.4.4. WiFi interference detection

- Provide 2.4G band/5.8G band wifi channel diagram analysis chart;
- Provide WiFi information of the current access point of the device (SSID, signal strength, negotiated connection rate, channel, channel bandwidth, effective co-channel/adjacent channel interference, encryption protocol indicators);
- Supports viewing information of nearby access points (SSID, device, MAC, signal strength, channel, channel bandwidth);
- Supports viewing 2.4G frequency band/5.8G frequency band channel rating;

- Supports viewing LAN devices (IP, device, MAC);
- Supports exporting text data for sharing to WeChat, DingTalk, SMS, and Bluetooth; supports exporting pictures for sharing to WeChat and saving to photo albums;



SSID zhang

MAC d4:da:21:04:7c:f4

IP 192.168.31.1

protocol WiFi4/802.11n

(Medium) 65 Mbps

channel 6 (2G)

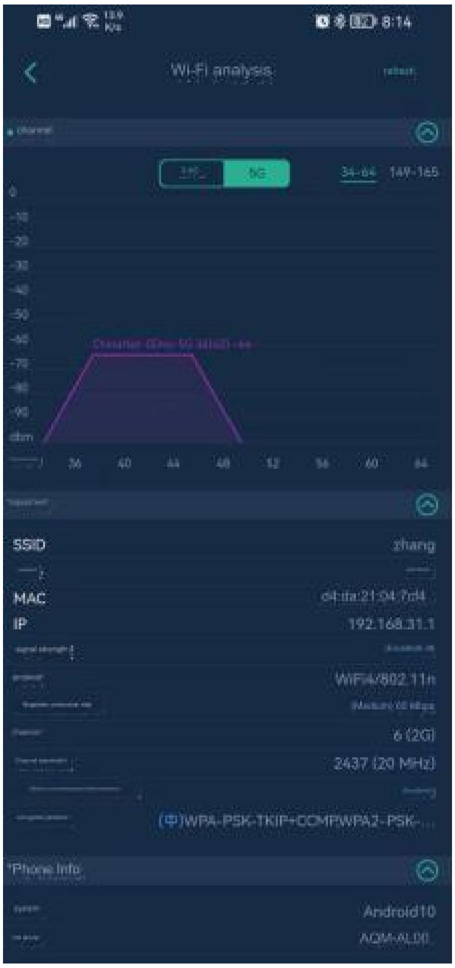
2437 (20 MHz)

(中)WPA-PSK-TKIP+CCMP,WPA2-PSK-...

*Phone Info

system Android10

AQM-AL00



SSID zhang

MAC d4:da:21:04:7c:f4

IP 192.168.31.1

protocol WiFi4/802.11n

(Medium) 65 Mbps

6 (2G)

2437 (20 MHz)

(中)WPA-PSK-TKIP+CCMP,WPA2-PSK-...

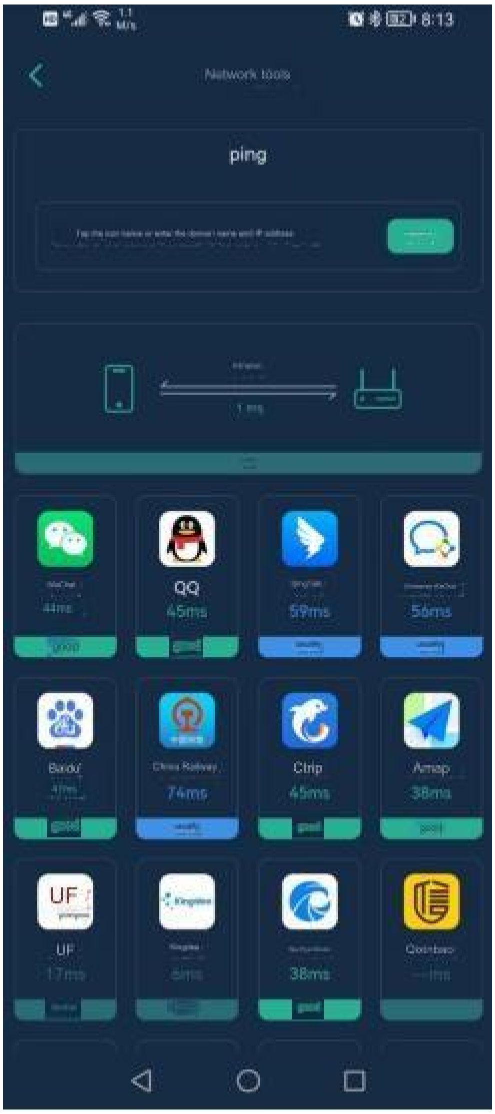
*Phone Info

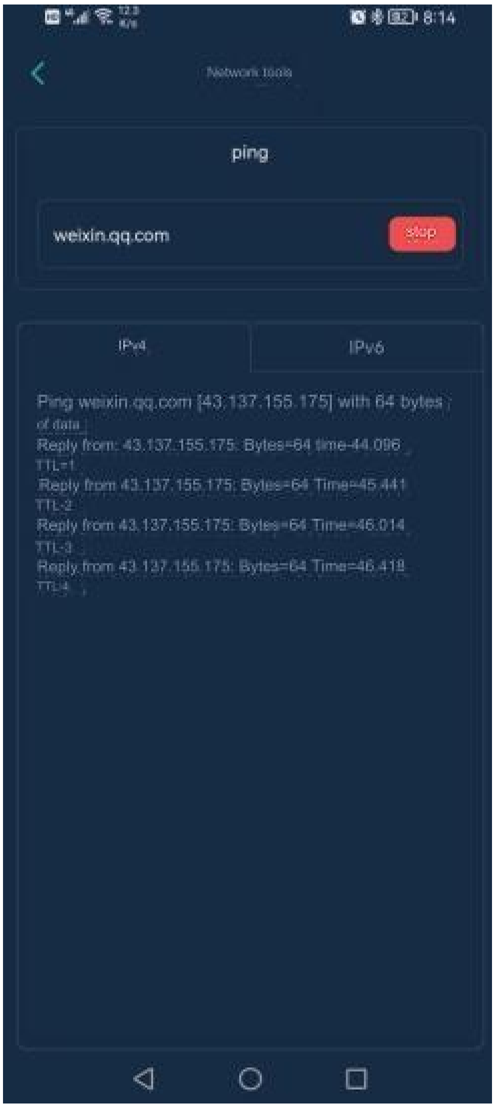
system Android10

AQM-AL00

2.4.5. PING Detection

- Provide operation and maintenance PING command testing capabilities, initiate network performance detection from mobile phone devices to test targets, and test target addresses support IPv4 IP, IPv6 IP and domain name methods;

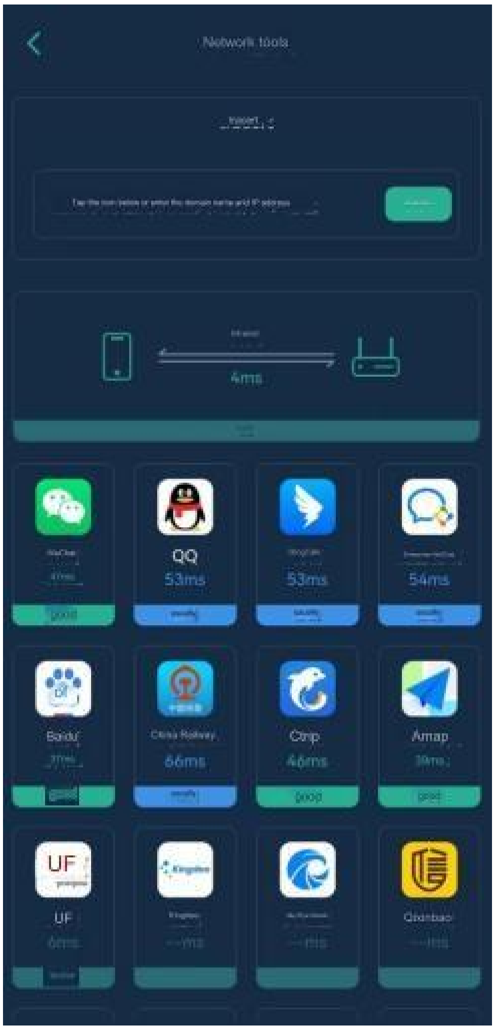


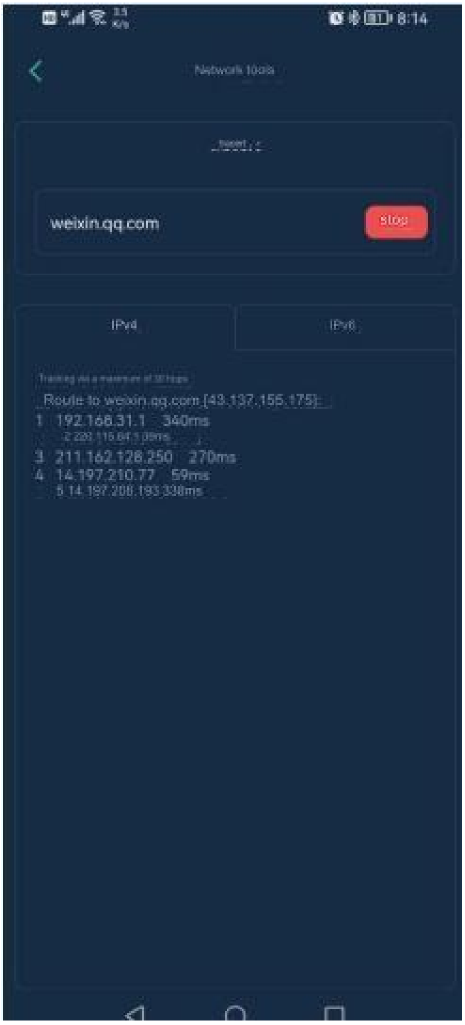


```
Ping weixin.qq.com [43.137.155.175] with 64 bytes
of data
Reply from: 43.137.155.175: Bytes=64 time=44.096
TTL=1
Reply from 43.137.155.175: Bytes=64 Time=45.441
TTL=2
Reply from 43.137.155.175: Bytes=64 Time=46.014
TTL=3
Reply from 43.137.155.175: Bytes=64 Time=46.418
TTL=4
```

2.4.6. Traceroute（Tracert）

- Provide operation and maintenance Tracert command testing capabilities, initiate network route tracing from mobile devices to test targets, and test target addresses support IPv4 IP, IPv6 IP and domain name methods;





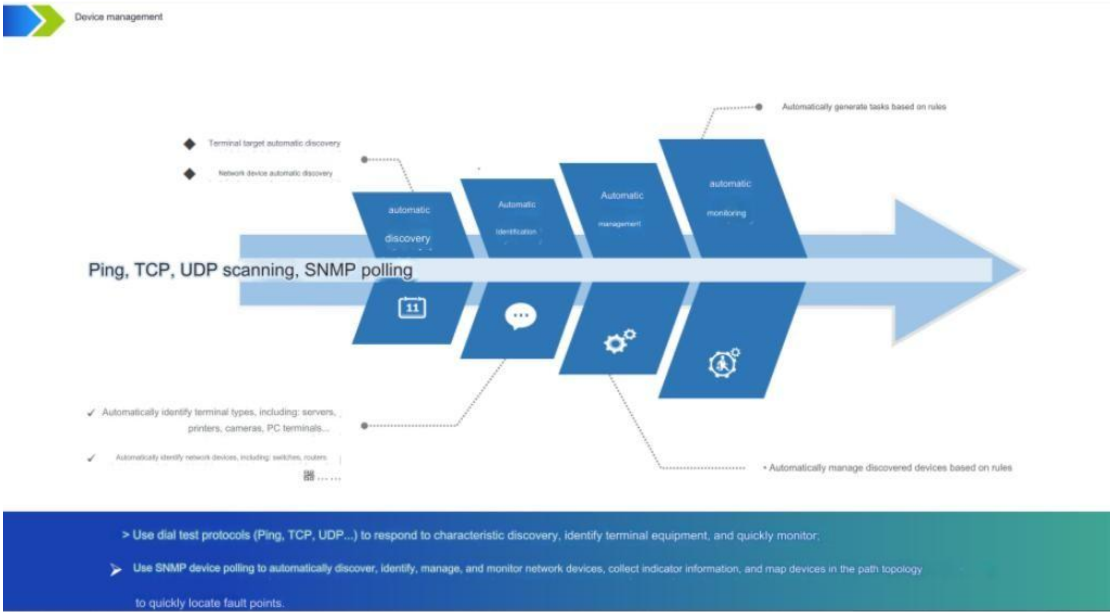
```
Route to weixin.qq.com [43.137.155.175]:
1  192.168.31.1    340ms
   2 220.115.64.1 39ms
3  211.162.128.250    270ms
4  14.197.210.77    59ms
   5 14.197.208.193 338ms
```

3. Product solution application introduction

3.1. Application mode

3.1.1. Device management

Achieve automatic discovery, automatic identification, automatic management, and automatic monitoring of terminal targets and network equipment. Use Probe Test protocols (Ping, TCP, UDP...) to respond to feature discovery, identify terminal equipment, and quickly monitor; use SNMP device polling Automatically discover, identify, manage, and monitor network equipment, collect indicator information, and map equipment in the path topology to quickly locate fault points.



Device management

- Terminal target automatic discovery
- Network device automatic discovery

Automatically generate tasks based on rules

automatic discovery

Automatic identification

Automatic management

automatic monitoring

Ping, TCP, UDP scanning, SNMP polling

✓ Automatically identify terminal types, including: servers, printers, cameras, PC terminals...

✓ Automatically identify network devices, including: switches, routers ......

• Automatically manage discovered devices based on rules

> Use dial test protocols (Ping, TCP, UDP...) to respond to characteristic discovery, identify terminal equipment, and quickly monitor;

➤ Use SNMP device polling to automatically discover, identify, manage, and monitor network devices, collect indicator information, and map devices in the path topology to quickly locate fault points.

3.1.2. Whole network monitoring

Integrate active Probe Testing, relay monitoring, layer 2 network monitoring, dynamic address monitoring, WIFI/mobile network monitoring and other monitoring technologies to realize enterprise layer 3/layer 2 networks, various access terminals, backup links, and WIFI networks , 5G network monitoring without blind spots.

➢ Active Probe Test

Adopting the industry's leading active intelligent detection technology, it provides detection capabilities for large concurrency, multi-protocols, customized cycles, number of packets sent, and customized packet sizes to achieve end-to-end network path detection. Applicable scenarios are as follows:

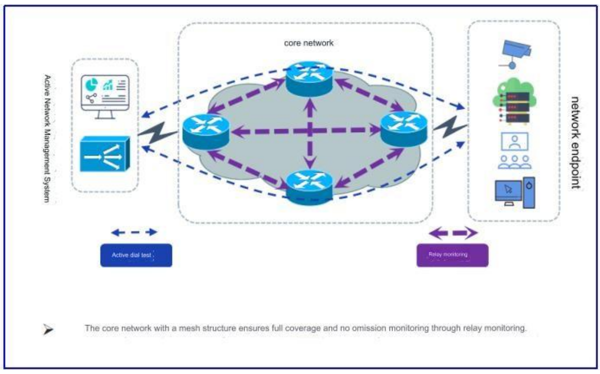
◆ Detection of a large number of fixed network access nodes uses moderate frequency small packet detection

- IoT nodes are sensitive to traffic and use low-frequency small packet detection
- Second-level high-frequency detection is used for important protection targets
- Use ultra-large packet dialing test to verify the network large packet passing performance and locate problems. For example, in video services, the data packet size often reaches 1500 or even 3000 bytes. The large packet passing performance of the network is directly related to the video transmission quality.
- Use SIP protocol for simulation detection of voice and video services

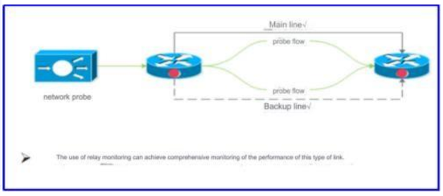
- Relay monitoring

By linking with network equipment, it can automatically monitor the relay lines between equipment 24/7. Like the probe dialing method, it can effectively detect problems such as interruptions, delay degradation, and packet loss degradation.

- For the core network with a mesh structure, full coverage and no omission monitoring can be ensured through relay monitoring.
- For routes that are unreachable, such as backup links and links whose interface addresses have not published routes, traditional network management systems can see the link port status, but cannot perceive performance degradation, and there are false positives in the port status. This causes unreachable links to become monitoring blind spots, and availability cannot be guaranteed. The use of relay monitoring can achieve comprehensive monitoring of the performance of this type of link.



➢ The core network with a mesh structure ensures full coverage and no omission monitoring through relay monitoring.

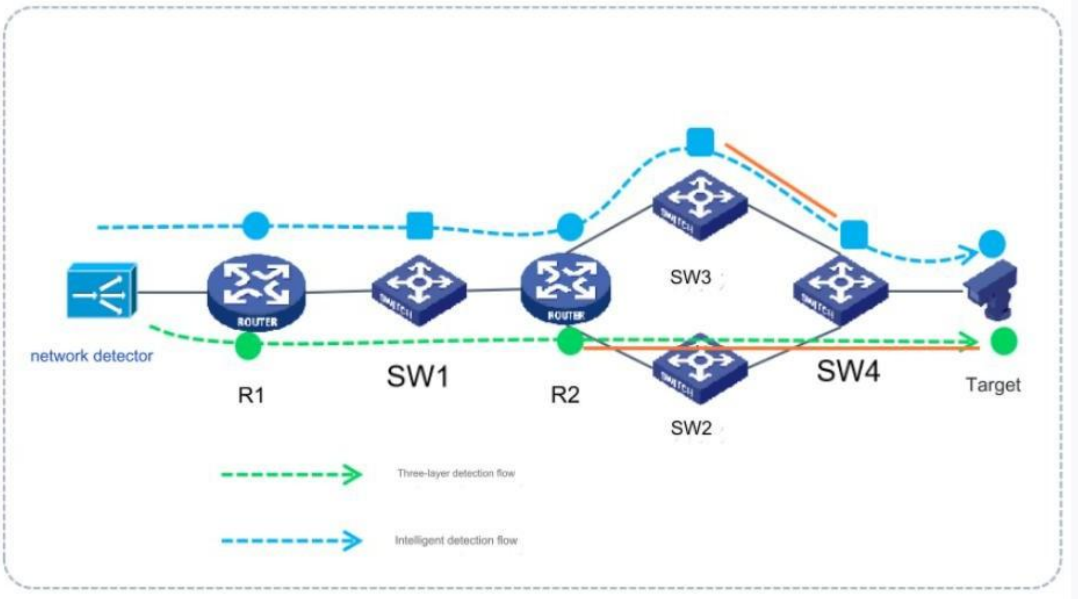


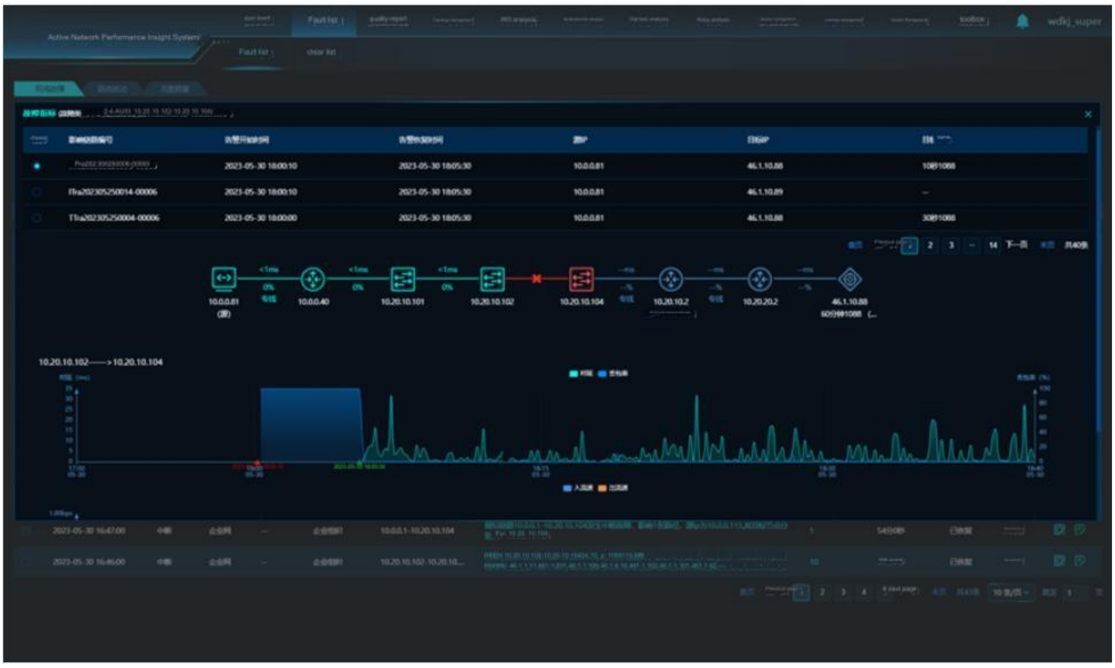
➢ The use of relay monitoring can achieve comprehensive monitoring of the performance of this type of link.

- ➢ Layer 2 network monitoring

For the first time in the industry, it implements Layer 2 network path detection and complete end-to-end performance monitoring of Layer 2/3 networks, effectively solving the problem of blind spots in Layer 2 network performance monitoring.

- ◆ Layer 2 equipment that intelligently identifies business flow paths;
- ◆ Intelligently completes the three-layer service path to achieve full-link detection;
- ◆ Further improves the accurate analysis of data and fault locatio





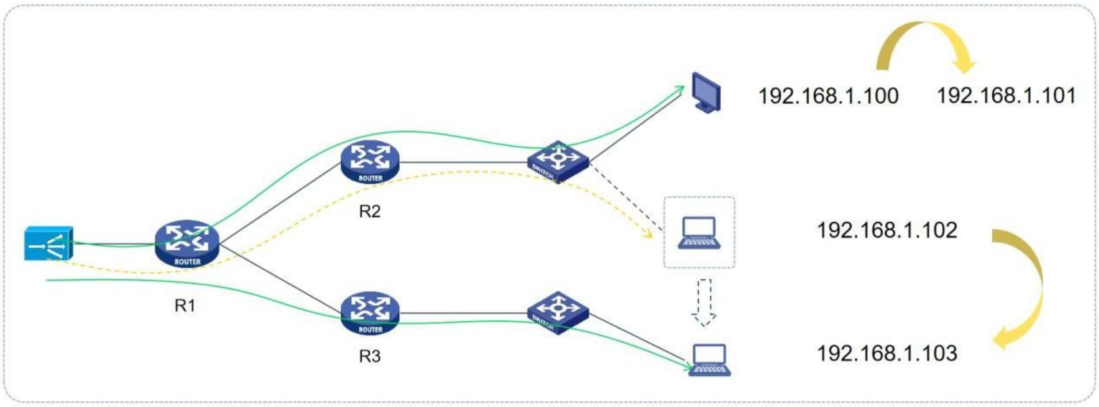
Active Network Performance Insight System

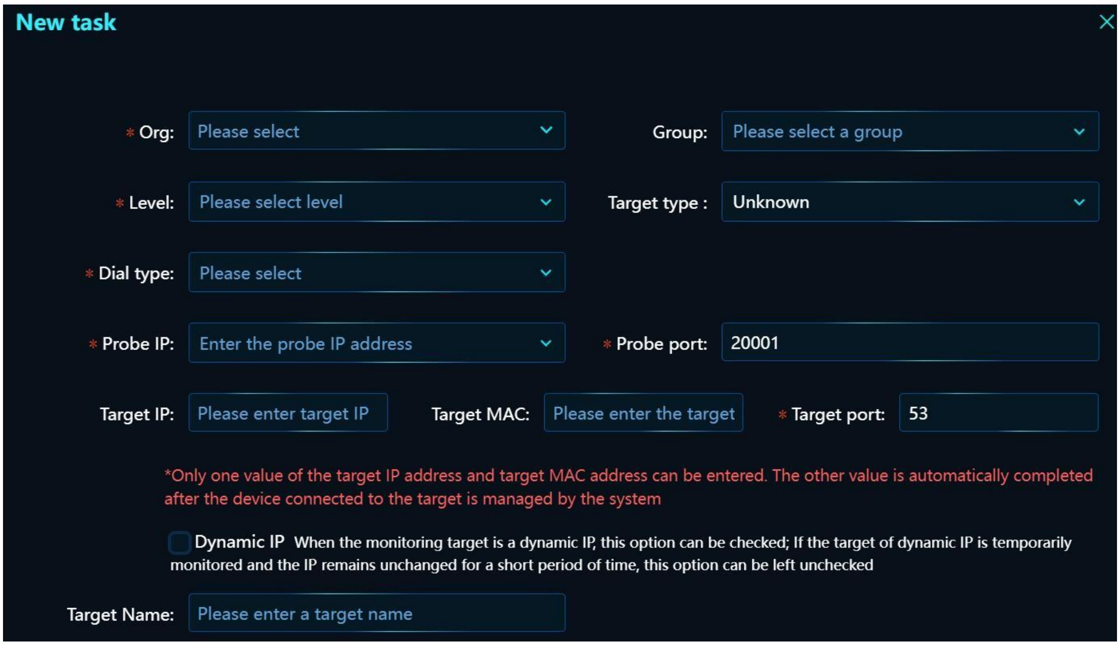
Fault list | clear list

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
●	[illegible]	2023-05-30 18:00:10	2023-05-30 18:05:30	10.0.0.81	46.1.10.88
○	fTra202305250014-00006	2023-05-30 18:00:10	2023-05-30 18:05:30	10.0.0.81	46.1.10.89
○	TTra202305250004-00006	2023-05-30 18:00:00	2023-05-30 18:05:30	10.0.0.81	46.1.10.88

➢ Dynamic address monitoring

For the first time in the industry, remote monitoring of dynamic address terminals is realized. When the terminal's DHCP assigned address changes, or the terminal is connected to another place, the system can still continue to monitor.





New task

* Org:	Please select	Group:	Please select a group
* Level:	Please select level	Target type :	Unknown
* Dial type:	Please select		
* Probe IP:	Enter the probe IP address	* Probe port:	20001

Target IP: Please enter target IP Target MAC: Please enter the target * Target port: 53

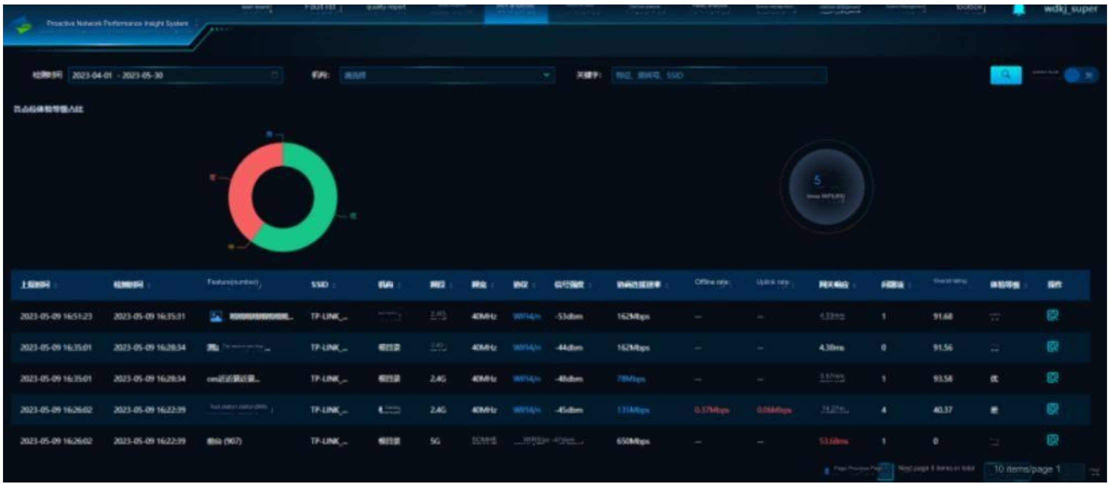
*Only one value of the target IP address and target MAC address can be entered. The other value is automatically completed after the device connected to the target is managed by the system

□ Dynamic IP When the monitoring target is a dynamic IP, this option can be checked; If the target of dynamic IP is temporarily monitored and the IP remains unchanged for a short period of time, this option can be left unchecked

Target Name: Please enter a target name

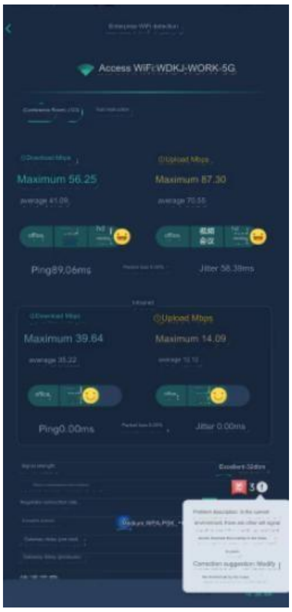
➢ Wireless network monitoring

After extensive proofreading, the professional version of Wangchacha realizes instrument-level WIFI and mobile network monitoring on mobile terminals; for enterprise WiFi, it can use tag + photo method to accurately conduct testing; for diagnosed problems, it directly provides more than a dozen professional Process opinions and guide users to optimize the network; the monitoring results of the APP are summarized in the background to achieve a comprehensive analysis from point to area.



[illegible]	[illegible]	Feature(number)	SSID	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Offline rate	Uplink rate	[illegible]	[illegible]	Overall rating	[illegible]	[illegible]
2023-05-09 16:51:23	2023-05-09 16:35:31	[illegible]	TP-LINK_...	[illegible]	[illegible]	40MHz	WiFi4/n	-53dbm	162Mbps	--	--	[illegible]	1	91.68	[illegible]	
2023-05-09 16:35:01	2023-05-09 16:28:34	[illegible]	TP-LINK_...	[illegible]	[illegible]	40MHz	WiFi4/n	-44dbm	162Mbps	--	--	4.38ms	0	91.56	[illegible]	
2023-05-09 16:35:01	2023-05-09 16:28:34	[illegible]	TP-LINK_...	[illegible]	2.4G	40MHz	WiFi4/n	-48dbm	78Mbps	--	--	[illegible]	1	93.58	[illegible]	
2023-05-09 16:26:02	2023-05-09 16:22:39	[illegible]	TP-LINK_...	[illegible]	2.4G	40MHz	WiFi4/n	-45dbm	135Mbps	0.37Mbps	0.06Mbps	[illegible]	4	40.37	[illegible]	
2023-05-09 16:26:02	2023-05-09 16:22:39	[illegible] (907)	TP-LINK_...	[illegible]	5G	[illegible]	[illegible]	[illegible]	650Mbps	--	--	53.68ms	1	0	[illegible]	

10 items/page 1



Access WiFi:WDKJ-WORK-5G

Maximum 56.25

Maximum 87.30

Ping89.06ms

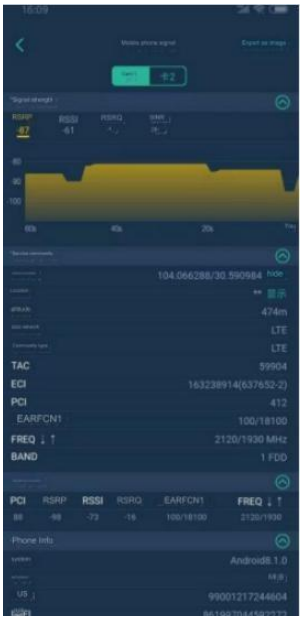
Jitter 58.39ms

Maximum 39.64

Maximum 14.09

Ping0.00ms

Jitter 0.00ms



RSRP -67

RSSI -61

104.066288/30.590984

474m

LTE

LTE

TAC 59904

ECI 163238914(637652-2)

PCI 412

EARFCN1 100/18100

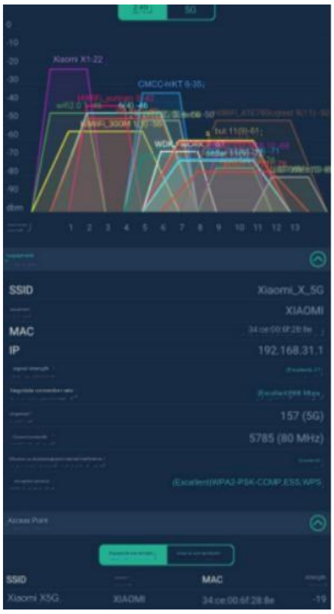
FREQ 2120/1930 MHz

BAND 1 FDD

Phone Info

Android8.1.0

99001217244604



SSID Xiaomi_X_5G

XIAOMI

MAC

IP 192.168.31.1

157 (5G)

5785 (80 MHz)

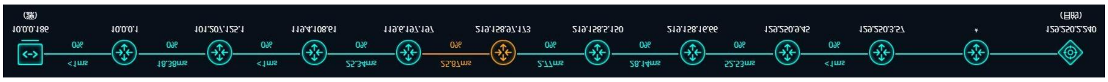
Excellent(WPA2-PSK-CCMP,ESS,WPS)

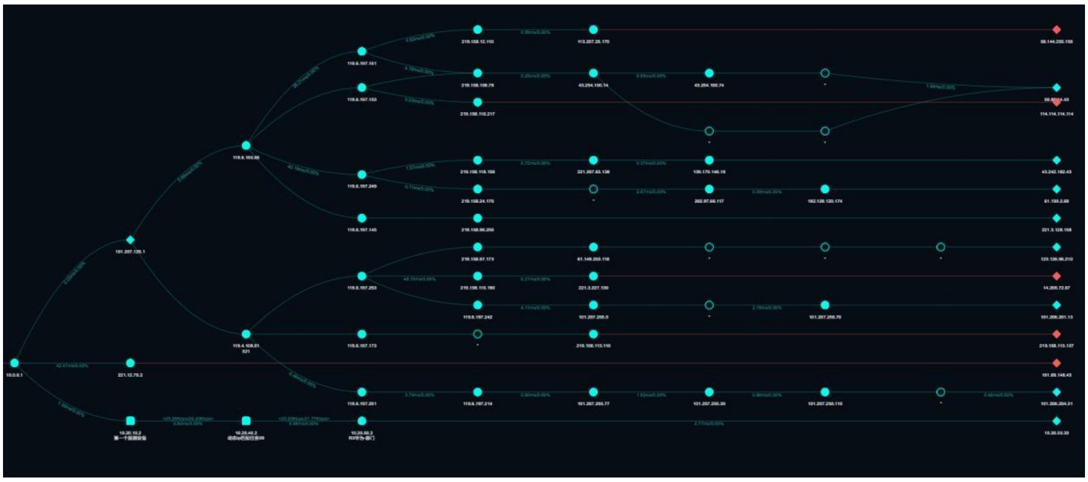
Access Point

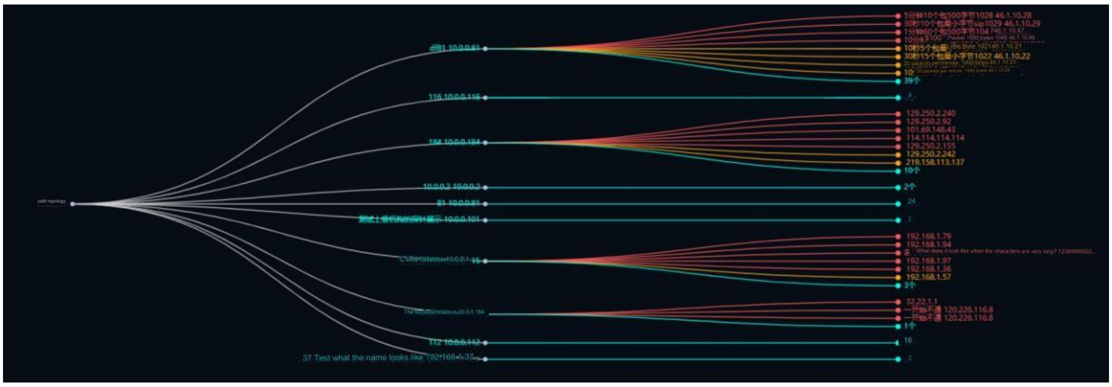
SSID Xiaomi X5G XIAOMI MAC -19

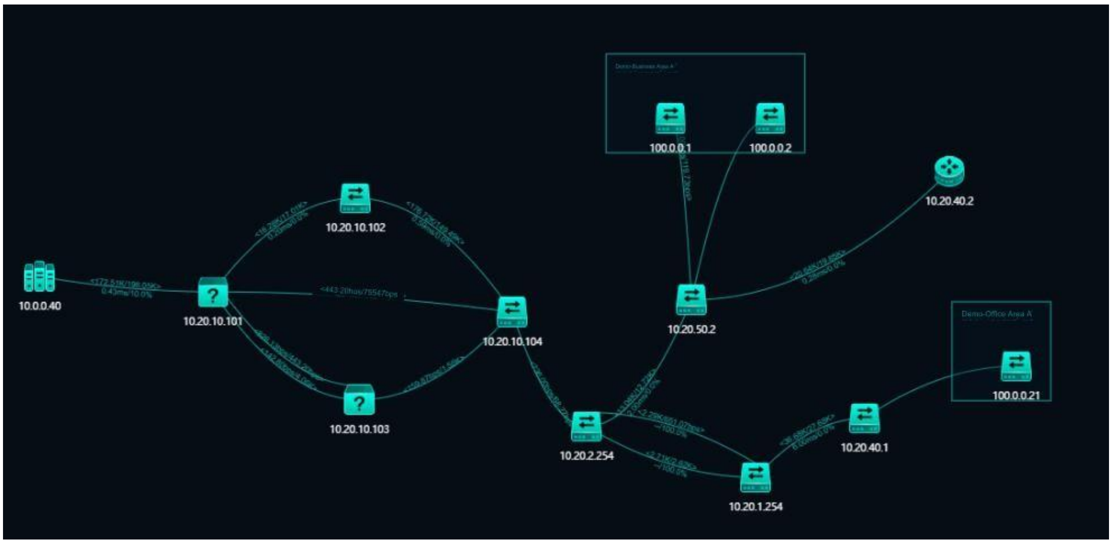
3.1.3. Internet browsing

It provides powerful spatio-temporal visualization capabilities, provides customized dashboards, multi-dimensional topology views, end-to-end positioning views, multi-index correlation views and other intuitive displays to achieve three-dimensional visual monitoring and help operation and maintenance personnel fully perceive the network operating situation.



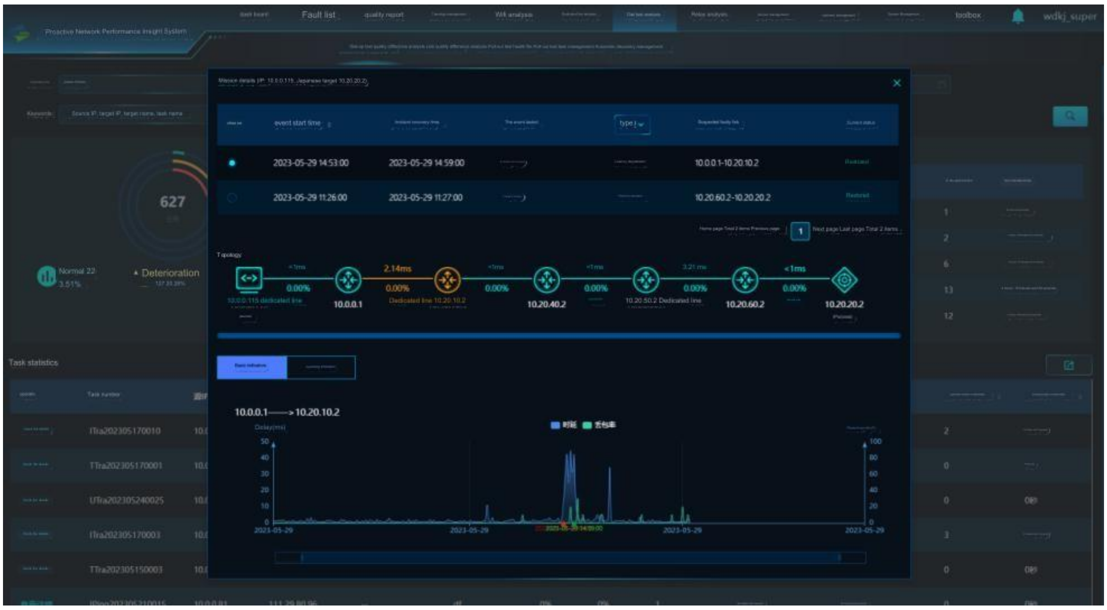






3.1.4. Network warning

In the original operation and maintenance model, network maintenance personnel could only intervene after performance degradation occurred. This system can proactively sense subtle problems such as interruptions, delay degradation, packet loss, route fluctuations, etc., and automatically generate events. Each event can locate the specific link and trace back the original indicators, so that it can warn users as early as possible and take proactive maintenance measures. Rectify sub-health links to nip failures in the bud.

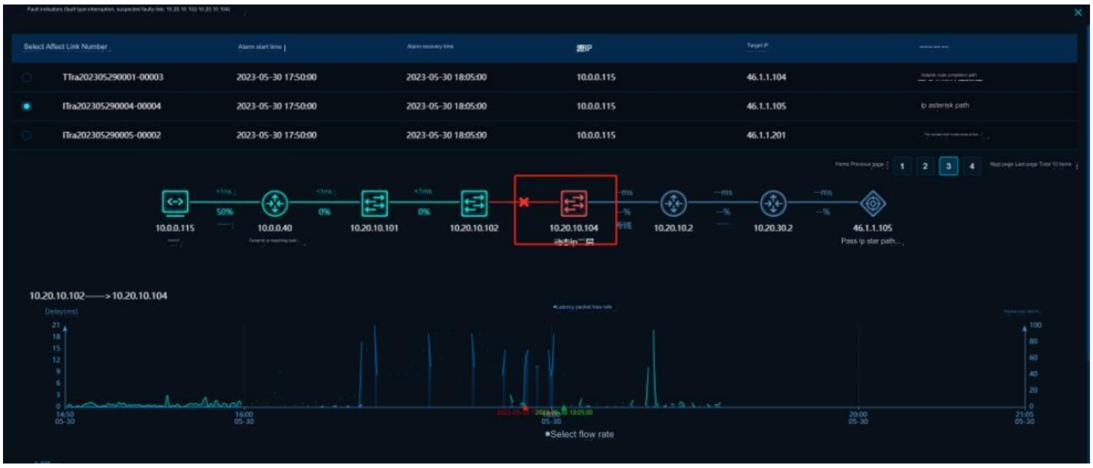


[illegible]	event start time	[illegible]	[illegible]	type	[illegible]	[illegible]
●	2023-05-29 14:53:00	2023-05-29 14:59:00	[illegible]	[illegible]	10.0.0.1-10.20.10.2	[illegible]
○	2023-05-29 11:26:00	2023-05-29 11:27:00	[illegible]	[illegible]	10.20.60.2-10.20.20.2	[illegible]

Illustration of network quality difference analysis

3.1.5. Fault management

Alarm rules can be flexibly customized according to the severity of degradation, and support SMS and email notifications, and can be expanded to DingTalk, WeChat, voice and other notification methods. Through highly visual path topology display, it helps customers quickly locate fault points and can accurately locate specific IPs and network elements, allowing maintenance personnel to quickly repair faults. Change the original way that network maintenance can only be based on experience after a fault occurs.



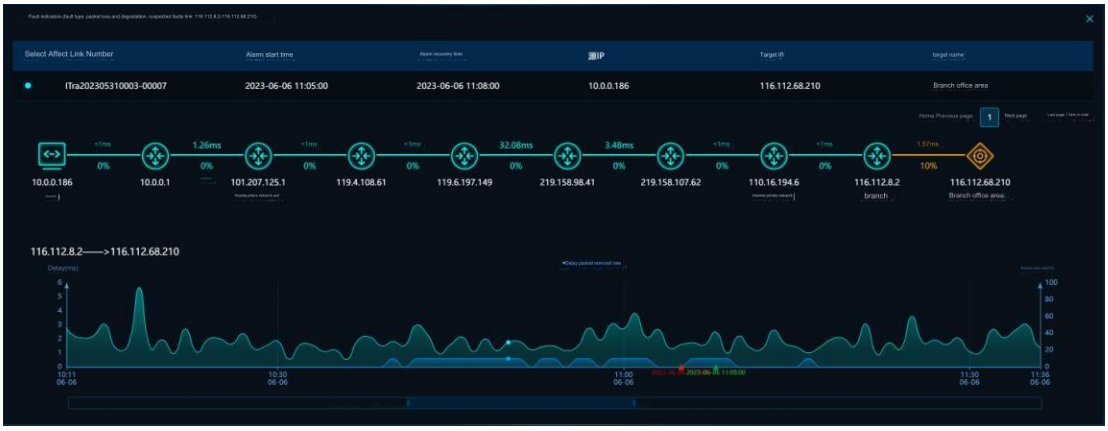
Select Affect Link Number	Alarm start time	Alarm recovery time	源IP	Target IP	[illegible]
○ TTra202305290001-00003	2023-05-30 17:50:00	2023-05-30 18:05:00	10.0.0.115	46.1.1.104	[illegible]
● ITra202305290004-00004	2023-05-30 17:50:00	2023-05-30 18:05:00	10.0.0.115	46.1.1.105	ip asterisk path
○ ITra202305290005-00002	2023-05-30 17:50:00	2023-05-30 18:05:00	10.0.0.115	46.1.1.201	[illegible]

Illustration of quick fault location

3.1.6. Define responsibilities

For cross-region, cross-network, and cross-department networking, clearly locate fault points, map and display the identification of key points, and clarify the responsible

party.

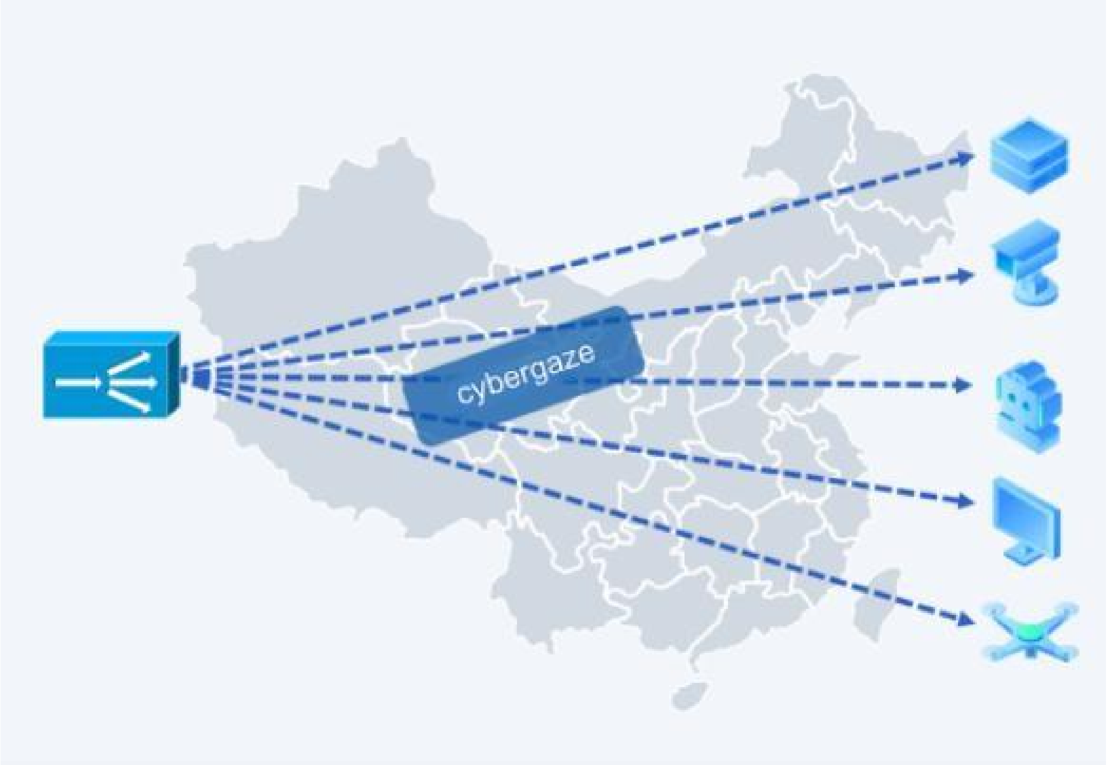


Fault indications (fault type: packet loss and degradation, suspected faulty link: 116.112.8.2-116.112.68.210)

Select Affect Link Number	Alarm start time	Alarm recovery time	源IP	Target IP	target name
ITra202305310003-00007	2023-06-06 11:05:00	2023-06-06 11:08:00	10.0.0.186	116.112.68.210	Branch office area

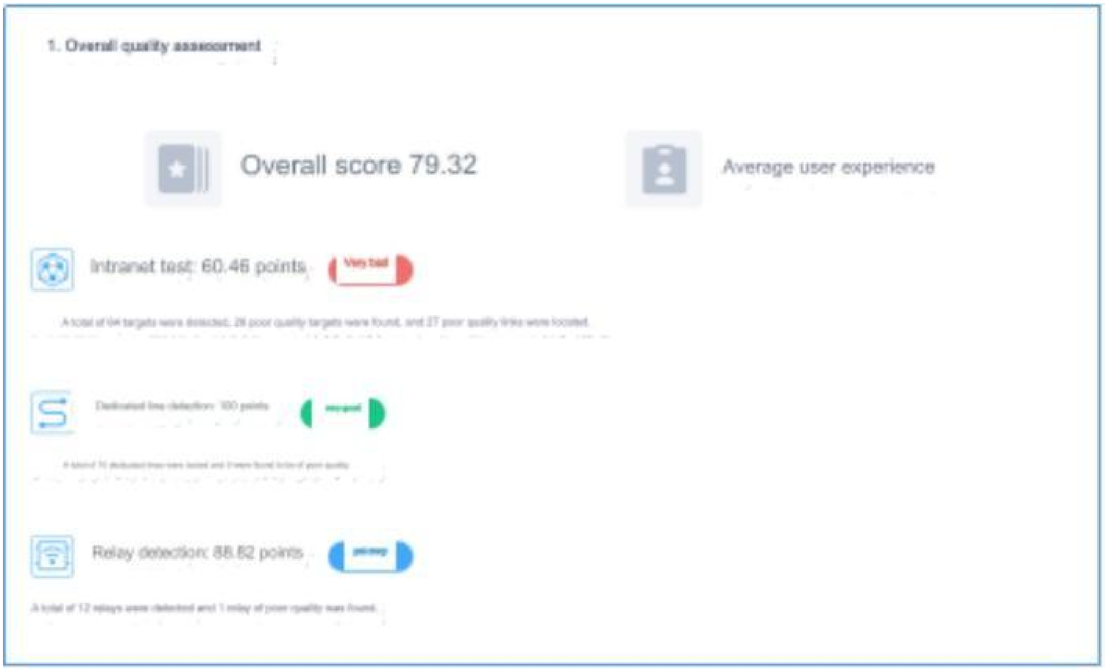
3.1.7. Important guarantees

For important communication support scenarios such as emergency rescue, core business, and video conferencing support, line quality requirements are very high, and faults must be discovered and repaired as soon as possible. This system can provide second-level dial-up testing, realize line "staring" monitoring, and can complete the discovery and location of network interruptions and degradation faults within 30 seconds, helping operation and maintenance personnel quickly repair faults and achieve the best guarantee effect.



3.1.8. Run analysis

Automatically generate operation analysis reports, and use leading AI modeling and machine learning algorithms to convert invisible network quality into intuitive digital scores, helping operation and maintenance personnel quickly grasp the overall network operation quality, focus on poor quality links, and guide rectification measures.



1. Overall quality assessment

Overall score 79.32

Average user experience

Intranet test: 60.46 points Very bad

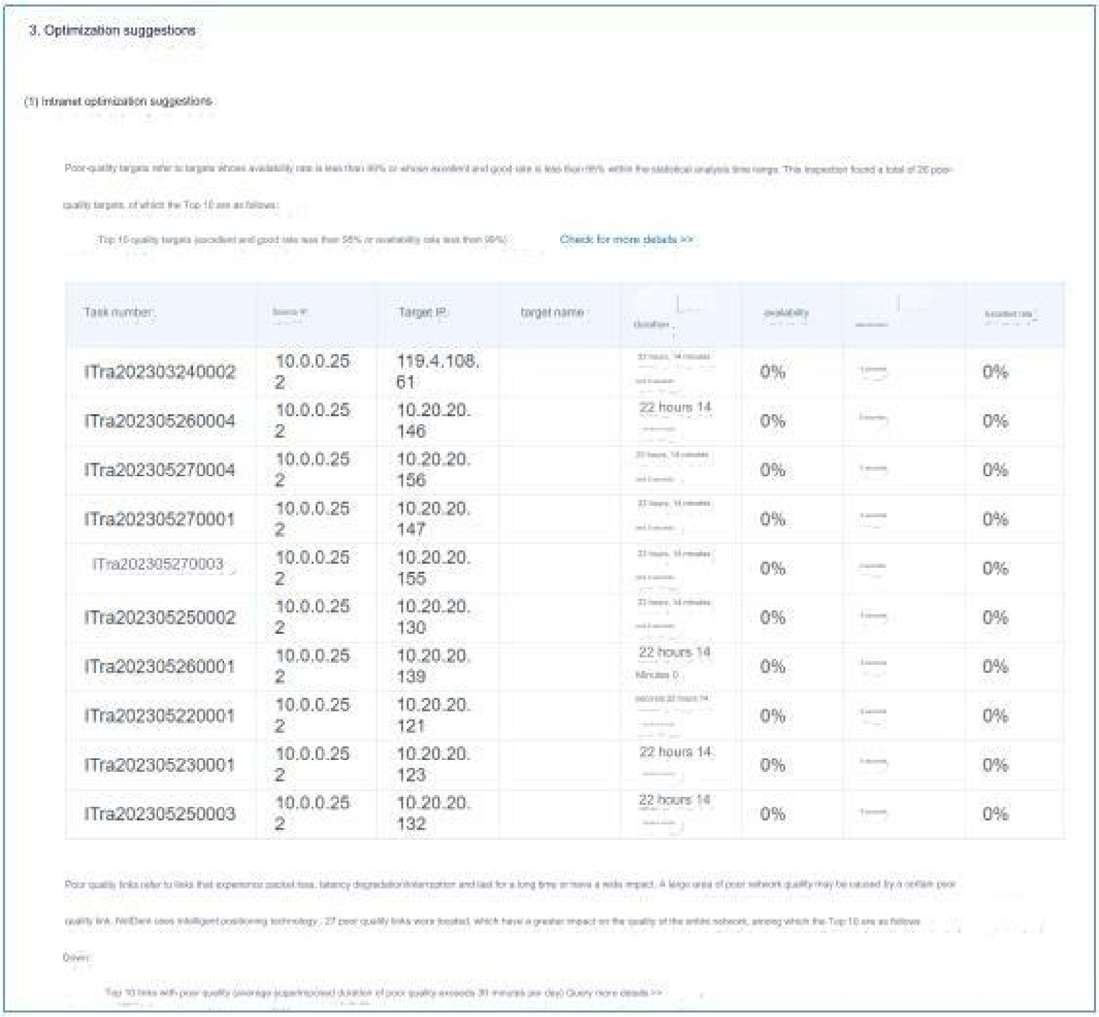
A total of 64 targets were detected, 28 poor quality targets were found, and 27 poor quality links were located.

Dedicated line detection: 100 points Very good

A total of 15 dedicated lines were tested and 0 were found to be of poor quality.

Relay detection: 88.82 points Average

A total of 12 relays were detected and 1 relay of poor quality was found.



3. Optimization suggestions

(1) Intranet optimization suggestions

Poor-quality targets refer to targets whose availability rate is less than 99% or whose excellent and good rate is less than 95% within the statistical analysis time range. This inspection found a total of 28 poor-quality targets, of which the Top 10 are as follows:

Top 10 quality targets (excellent and good rate less than 95% or availability rate less than 99%) Check for more details >>

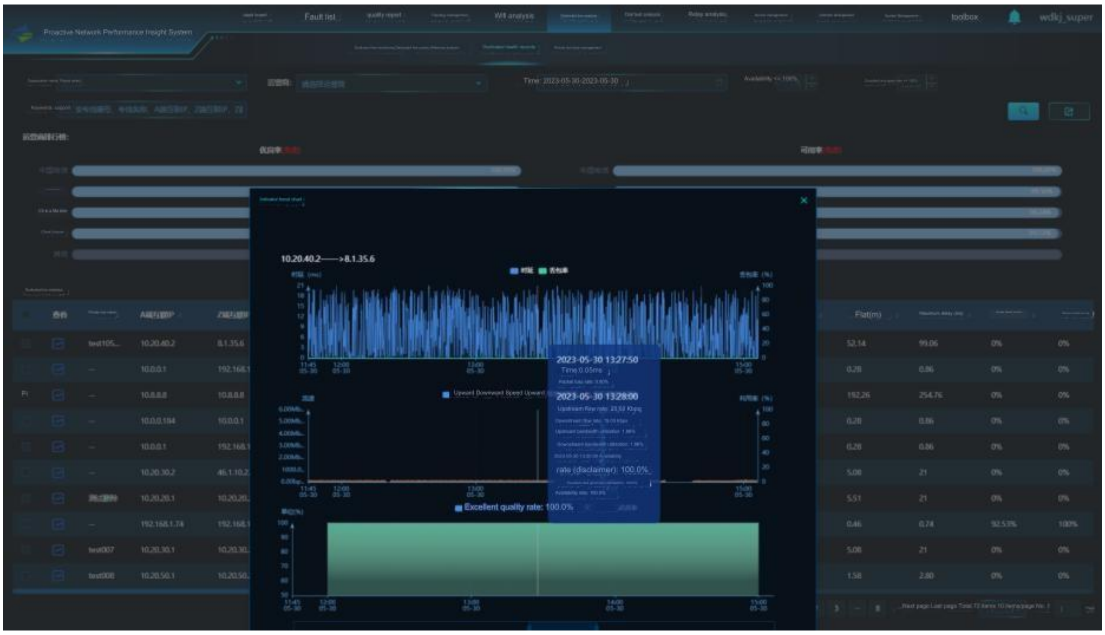
Task number	Source IP	Target IP	target name	duration	availability	[illegible]	Excellent rate
ITra202303240002	10.0.0.25 2	119.4.108. 61		22 hours, 14 minutes and 0 seconds	0%	[illegible]	0%
ITra202305260004	10.0.0.25 2	10.20.20. 146		22 hours 14 [illegible]	0%	[illegible]	0%
ITra202305270004	10.0.0.25 2	10.20.20. 156		22 hours, 14 minutes and 0 seconds	0%	[illegible]	0%
ITra202305270001	10.0.0.25 2	10.20.20. 147		22 hours, 14 minutes and 0 seconds	0%	[illegible]	0%
ITra202305270003	10.0.0.25 2	10.20.20. 155		22 hours, 14 minutes and 0 seconds	0%	[illegible]	0%
ITra202305250002	10.0.0.25 2	10.20.20. 130		22 hours, 14 minutes and 0 seconds	0%	[illegible]	0%
ITra202305260001	10.0.0.25 2	10.20.20. 139		22 hours 14 Minutes 0	0%	[illegible]	0%
ITra202305220001	10.0.0.25 2	10.20.20. 121		seconds 22 hours 14 [illegible]	0%	[illegible]	0%
ITra202305230001	10.0.0.25 2	10.20.20. 123		22 hours 14 [illegible]	0%	[illegible]	0%
ITra202305250003	10.0.0.25 2	10.20.20. 132		22 hours 14 [illegible]	0%	[illegible]	0%

Poor quality links refer to links that experience packet loss, latency degradation/interruption and last for a long time or have a wide impact. A large area of poor network quality may be caused by a certain poor quality link. NetDem uses intelligent positioning technology , 27 poor quality links were located, which have a greater impact on the quality of the entire network, among which the Top 10 are as follows Down:

Top 10 links with poor quality (average superimposed duration of poor quality exceeds 30 minutes per day) Query more details >>

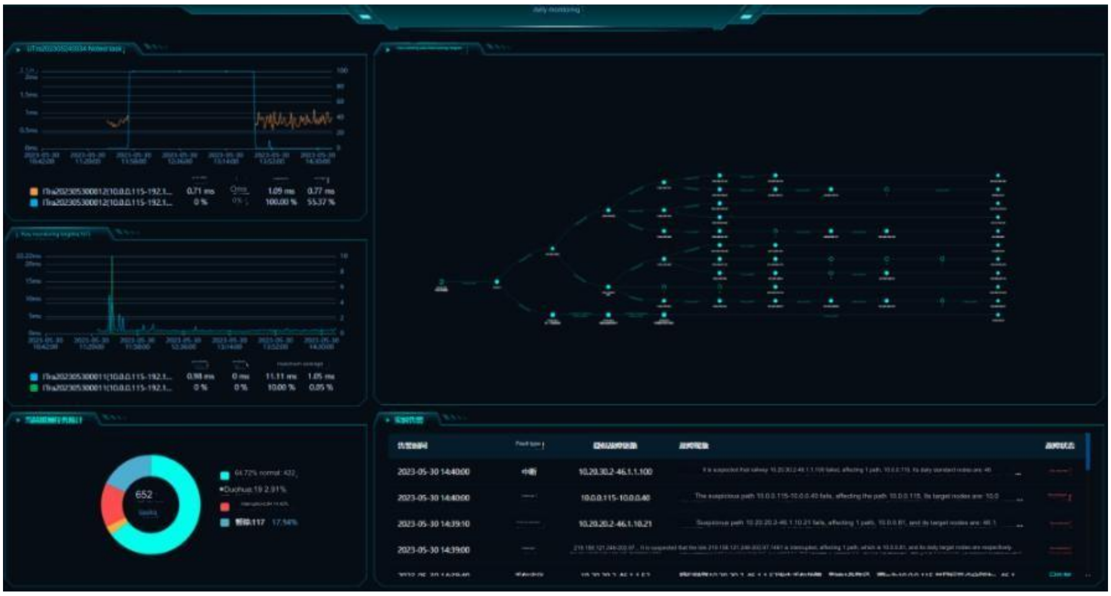
3.1.9. Quality assessment

For a large number of dedicated lines rented or built by customers, a 360-degree dedicated line evaluation model is established to scientifically evaluate the quality and cost-effectiveness of the dedicated lines to help customers reasonably evaluate operators and line assurance units; provide dedicated line quality query analysis and graphical presentation of original indicator trends; adopt Intelligent algorithms automatically eliminate dedicated line quality problems caused by traffic congestion, power outages, and network cutovers; automatically discover "zombie dedicated lines" with no traffic and long-term interruptions, promptly investigate and deal with them, and reasonably optimize costs.

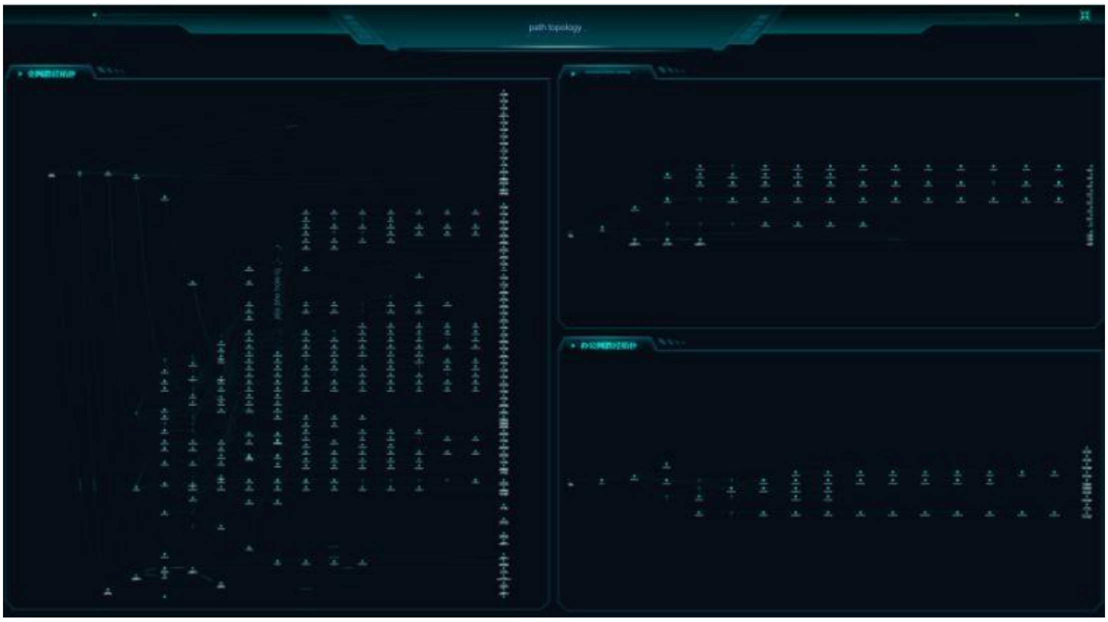

Proactive Network Performance Insight System
Fault list
WR analysis
toolbox
wdkj_super
Time: 2023-05-30-2023-05-30
10.20.40.2——>8.1.35.6
2023-05-30 13:27:50
Time:0.05ms
2023-05-30 13:28:00
Upstream flow rate: 23.53 Kbps
rate (disclaimer): 100.0%
Upward Download Speed Upward
Excellent quality rate: 100.0%
11:45 05-30
12:00 05-30
13:00 05-30
14:00 05-30
15:00 05-30

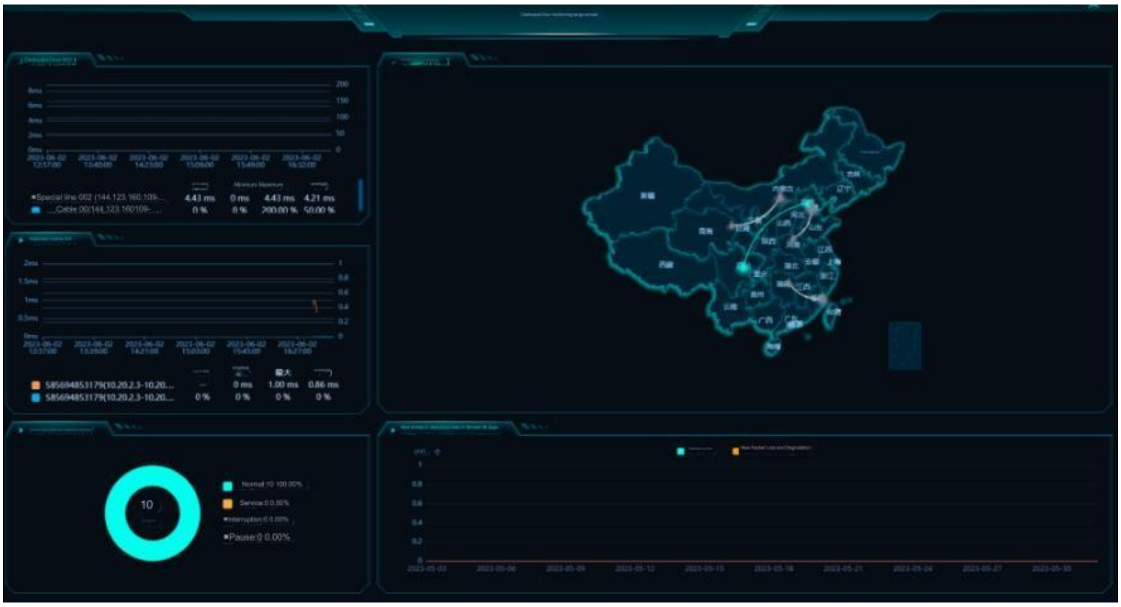
3.1.10. Situational awareness

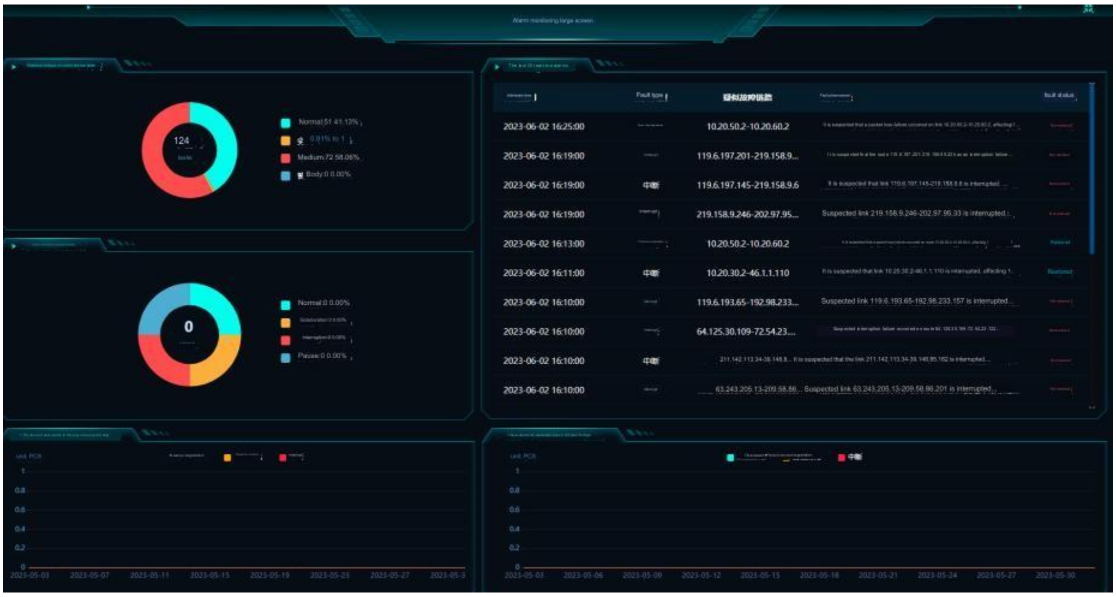
It supports customizing multiple dashboards according to different dimensions and business scenarios to meet a variety of monitoring scenarios, allowing operation and maintenance to fully grasp the network operating status. It supports the free combination layout of different components and provides a wealth of components: path topology, dedicated line overview (GIS map), real-time alarms, physical topology, operation statistics, 30-day alarm trend...



[illegible]	Fault type	[illegible]	[illegible]	[illegible]
2023-05-30 14:40:00	中断	10.20.30.2-46.1.1.100	[illegible]	[illegible]
2023-05-30 14:40:00	[illegible]	10.0.0.115-10.0.0.40	The suspicious path 10.0.0.115-10.0.0.40 fails, affecting the path 10.0.0.115. Its target nodes are: 10.0	[illegible]
2023-05-30 14:39:10	[illegible]	10.20.20.2-46.1.10.21	Suspicious path 10.20.20.2-46.1.10.21 fails, affecting 1 path, 10.0.0.81, and its target nodes are: 46.1	[illegible]
2023-05-30 14:39:00	[illegible]	[illegible]	[illegible]	[illegible]





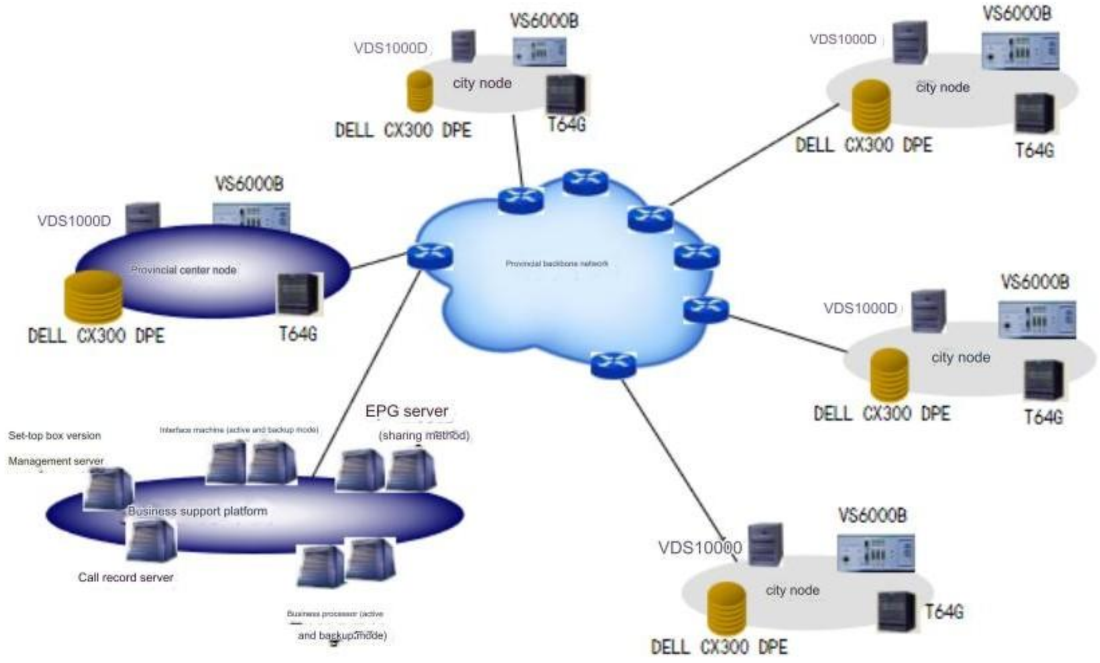


[illegible]	Fault type	链路故障信息	[illegible]	fault status
2023-06-02 16:25:00	[illegible]	10.20.50.2-10.20.60.2	It is suspected that a packet loss failure occurred on link 10.20.50.2-10.20.60.2, affecting t...	[illegible]
2023-06-02 16:19:00	[illegible]	119.6.197.201-219.158.9...	[illegible]	[illegible]
2023-06-02 16:19:00	中断	119.6.197.145-219.158.9.6	It is suspected that link 119.6.197.145-219.158.9.6 is interrupted.	[illegible]
2023-06-02 16:19:00	[illegible]	219.158.9.246-202.97.95...	Suspected link 219.158.9.246-202.97.95.33 is interrupted.	[illegible]
2023-06-02 16:13:00	[illegible]	10.20.50.2-10.20.60.2	[illegible]	[illegible]
2023-06-02 16:11:00	中断	10.20.30.2-46.1.1.110	It is suspected that link 10.20.30.2-46.1.1.110 is interrupted, affecting t...	Restored
2023-06-02 16:10:00	[illegible]	119.6.193.65-192.98.233...	Suspected link 119.6.193.65-192.98.233.157 is interrupted...	[illegible]
2023-06-02 16:10:00	[illegible]	64.125.30.109-72.54.23...	[illegible]	[illegible]
2023-06-02 16:10:00	中断	211.142.113.34-38.148.8...	It is suspected that the link 211.142.113.34-38.148.85.182 is interrupted...	[illegible]
2023-06-02 16:10:00	[illegible]	63.243.205.13-209.58.86...	Suspected link 63.243.205.13-209.58.86.201 is interrupted...	[illegible]

3.2. Application environment

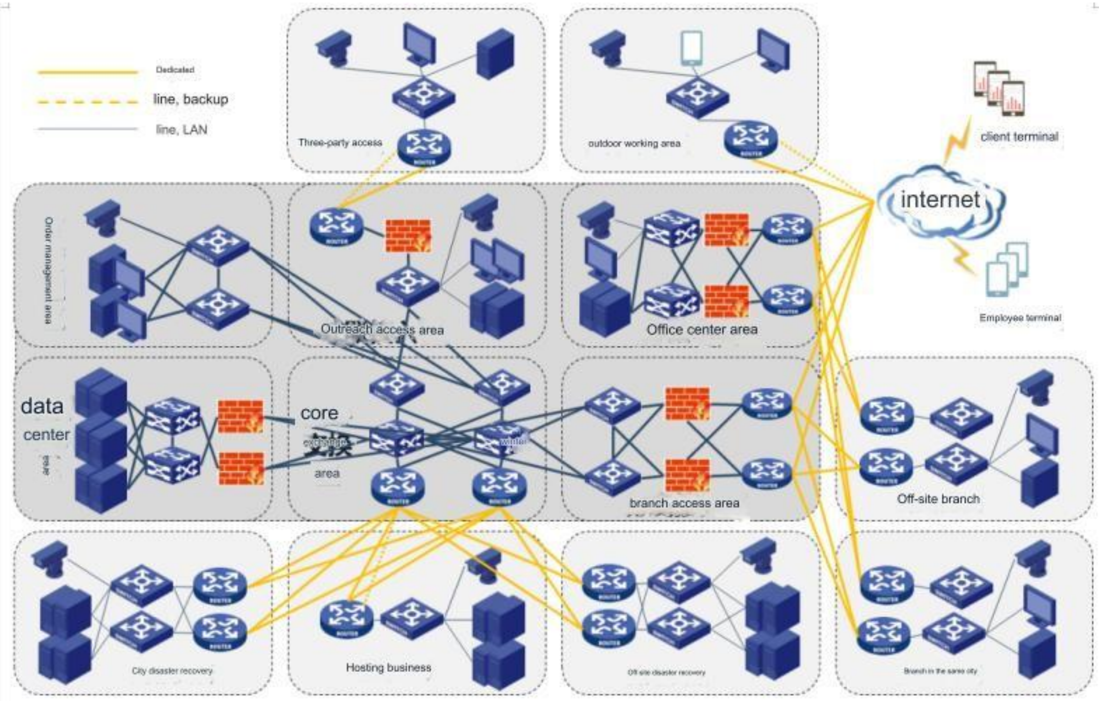
3.2.1. Data backbone network

The data backbone network has the characteristics of large capacity and long transmission distance. Once a failure occurs, the impact will be huge. Active network performance insight products are very suitable for performance monitoring of data backbone networks. Through low-consumption, high-frequency active dialing and testing tasks, intelligent algorithms that combine time domain and spatial domain fault diagnosis can accurately locate network faults and provide real-time early warning of network performance. Deterioration, prevent it before it happens, and reduce the losses caused by network interruption.



3.2.2. Enterprise production network

Deploying active network performance insight products in the enterprise's production network can monitor the data transmission performance of the enterprise's production network in real time and detect network path performance fluctuations in a timely manner. By observing early warnings of performance degradation, network management and maintenance personnel can locate suspected fault points in advance to reduce or even avoid interruptions. They can effectively improve production efficiency by getting rid of the situation of passively handling network faults after production business interruptions.



4. Introduction to product solution features

4.1. Product advantages introduction

- Connection-oriented real-time performance monitoring

This product uses a variety of advanced active detection technologies to achieve end-to-end real-time monitoring of complex networks, solving the blind spots of performance monitoring of traditional network management and overcoming the inability of packet capture and monitoring methods to monitor network performance when there is no traffic. question. The connection-oriented network monitoring system provides operation and maintenance personnel with a new network path view, allowing operation and maintenance personnel to truly manage the network from a business-aware perspective.

- Highly intelligent

In aspects such as probe detection, degradation identification, fault location, and network early warning, AI technology is widely used. Through machine learning algorithms, the network status is completely autonomously learned without manual intervention. Monitoring and analysis results are directly presented for operation and maintenance, and operation and maintenance personnel are It is liberated from the ocean of data and greatly improves the efficiency of network performance monitoring.

- Low deployment cost, safe and reliable

The probe uses a general X86 server, an open source operating system, and a centralized deployment method with low deployment cost and high compatibility. No mirroring or network structure adjustment is required, and it is seamlessly integrated into the existing network, making it safe and reliable.

- High ease of use

The active network performance insight product adopts a highly intuitive graphical interface and the operation process is humanized. Network maintenance managers can get started after simple training. When defining each functional module, the production process of network maintenance is fully considered to help operators integrate into operation and maintenance production as soon as possible.

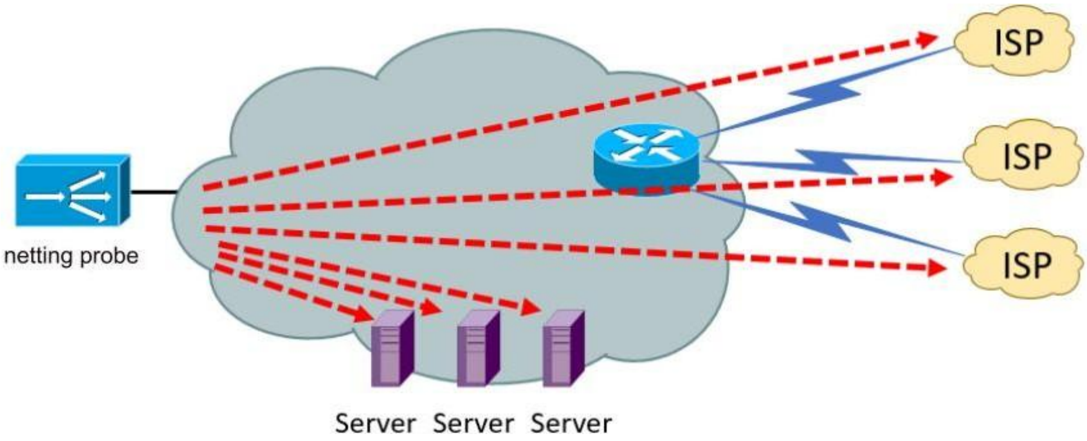
4.2. Introduction to product features and technologies

4.1.1. Full network coverage monitoring technology

This product adopts advanced network full coverage monitoring technology. Through probe dialing technology, relay monitoring technology and intelligent detection message sending strategy, it can realize 360-degree monitoring of large-scale complex networks without blind spots.

4.1.1.1. Probe Probe Testing Technology

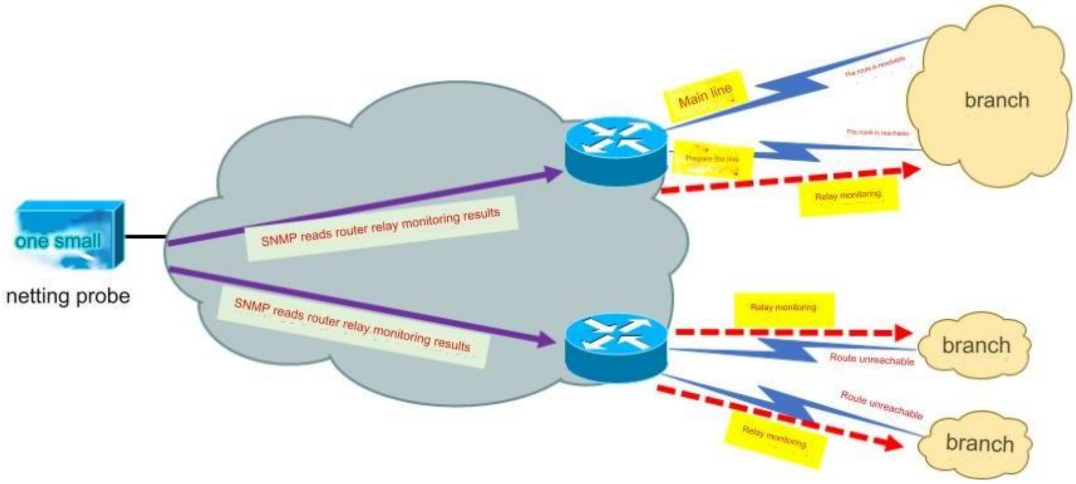
The probe constructs layer 3 and 4 detection packets based on the Probe Test type and sends similar traceroute detection packets to the target IP, as shown in the following figure:



Probe Probe Testing has no restrictions on the type of detection targets. For example, it can detect servers, videos, routers, switches, LAN links, dedicated line links, external websites, etc., as long as the route between the probe and the target IP is reachable. . The system supports multiple detection methods such as ICMP, UDP and TCP to adapt to different network environments and achieve the best detection results. Active dial-testing technology is fast to deploy, can create dial-test tasks in batches, and is suitable for performance monitoring of a large number of access network points. Probe supports deployment of Linux and Windows systems.

4.1.1.2. Relay monitoring technology

Relay monitoring technology can be understood as turning a network device into a probe that can monitor the performance of the relay directly connected to the device. The basic principle is to configure a connection-oriented network connectivity detection task on the device interface to obtain performance indicators such as delay and packet loss of relay connections. The system reports the collected data to the platform through the SNMP protocol to implement relay network performance indicator monitoring. The specific schematic diagram is shown below:



Relay monitoring technology is mainly suitable for monitoring unreachable routes, such as backup lines, cross-connect links between devices, or interconnection addresses of devices that are unreachable by routes. In particular, the monitoring of backup lines is often a headache for users. It is difficult to detect interruptions of backup lines using conventional monitoring methods, and it is even impossible to detect degradation. For example, in an MSTP-type backup leased line, when the intermediate link is interrupted, the status of the device ports at both ends is still UP, which will cause the system to misjudge that the backup line is normal. If the active-standby switchover occurs at this time, it will cause serious business interruption. as a result of. The relay monitoring technology can quickly sense the interruption and deterioration status of the backup line, relieving users from worries.

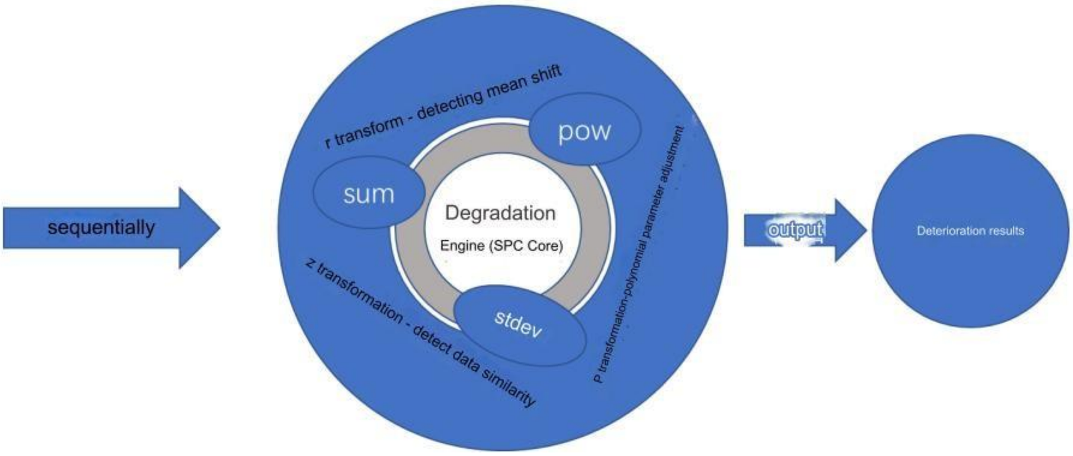
Relay monitoring technology is also suitable for complex mesh network monitoring. For mesh networks or load sharing lines, there are multiple end-to-end routes, and there may be inconsistent round-trip routing. It is difficult to fully cover the network using the probe Probe Testing method. Path, through relay monitoring technology, each relay section is monitored, which can perfectly realize the monitoring coverage of complex mesh networks.

4.1.2. Intelligent diagnostic technology

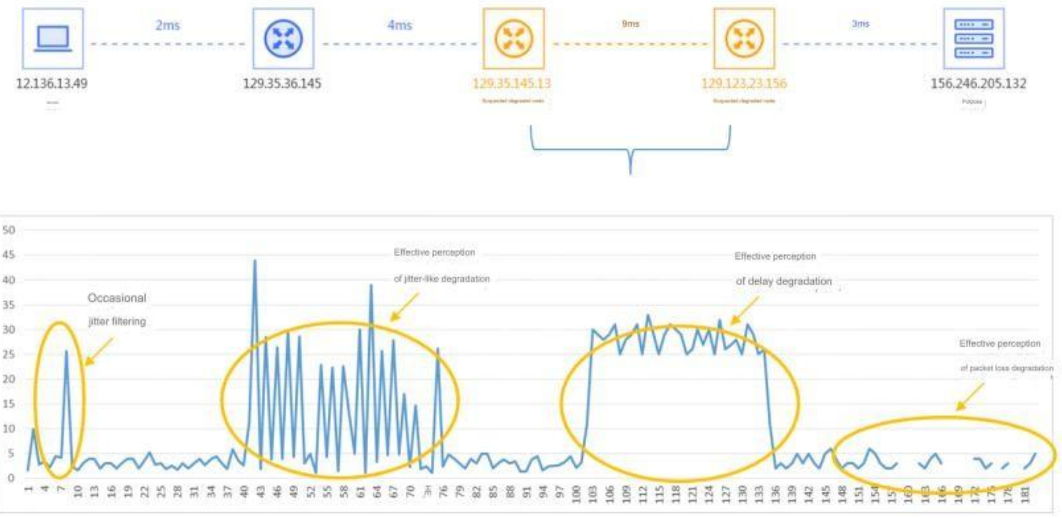
The system uses a large number of intelligent algorithms to realize automatic perception, quantitative analysis and precise positioning of network performance degradation.

4.1.2.1. Time domain intelligent diagnosis technology

The system uses advanced machine learning algorithms and uses an unsupervised degradation identification model to learn the network status completely autonomously and scientifically output the degradation results. The specific principle is shown in the figure below. Traditional monitoring methods use fixed threshold methods to judge degradation, which has great limitations. For example, the delay of both lines is 50ms. It is difficult to judge subjectively which one is degraded. However, in actual situation, line A is a long-distance line, and the delay of 50ms is a normal value. Line B is a local line, and the usual delay is only 5ms. Suddenly increased to 50ms, obvious degradation occurred. The unsupervised degradation identification model can automatically identify various types of network performance degradation without manual intervention, and the results will be directly quantified and output as degradation duration, which is simple and intuitive.


sequentially
r transform - detecting mean shift
pow
sum
Degradation
Engine (SPC Core)
stdev
z transformation - detect data similarity
P transformation-polynomial parameter adjustment
output
Deterioration results

The system uses time-domain intelligent diagnosis technology, which can effectively sense interruptions, large delays, jitter, packet loss and other situations and scientifically quantify them to accurately locate network fault points. Adaptive filtering technology is used to effectively filter out the influence of accidental factors. The details are shown in the figure below:



4.1.2.2. Spatial domain intelligent diagnosis technology

The system uses spatial domain intelligent diagnosis technology to efficiently merge faulty business flows according to public paths. Based on the weight of the bearer services, it can accurately locate network group faults at the minute level, helping maintenance personnel get to the core of the problem and troubleshoot efficiently.

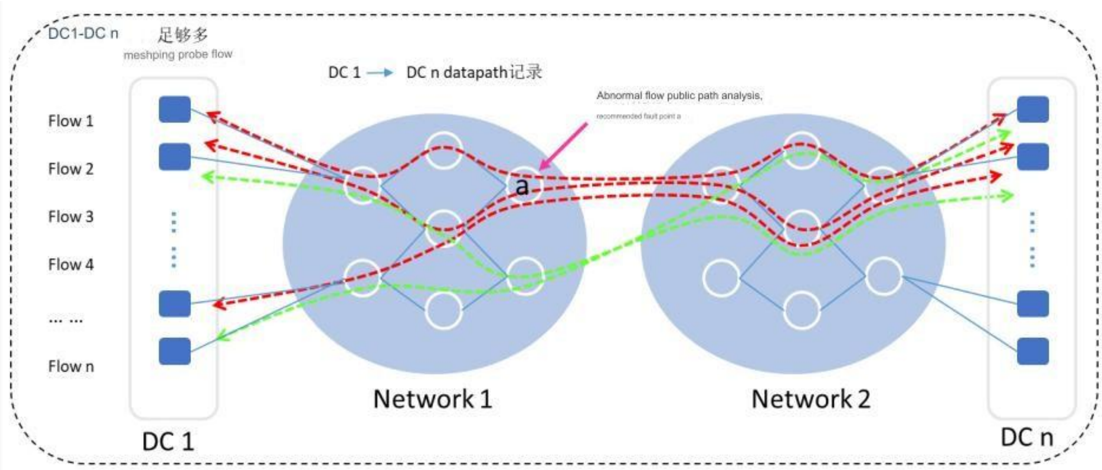


Illustration of spatial domain intelligent diagnosis technology

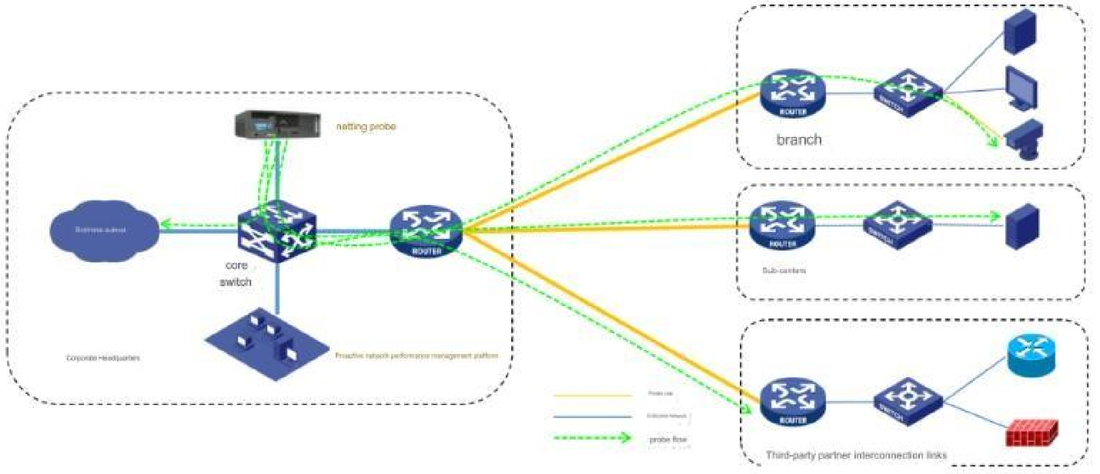
5. Product deployment plan

5.1. Network deployment plan

5.1.1. All-access network deployment solution

For enterprise networks that do not use VPN isolation, by deploying an active network performance monitoring and management platform in the core network of the enterprise headquarters, end-to-end monitoring services can be provided for the entire enterprise network, including the headquarters' business subnets, branch networks, and third-party networks. Partner interconnection links, leased lines, node equipment, etc.

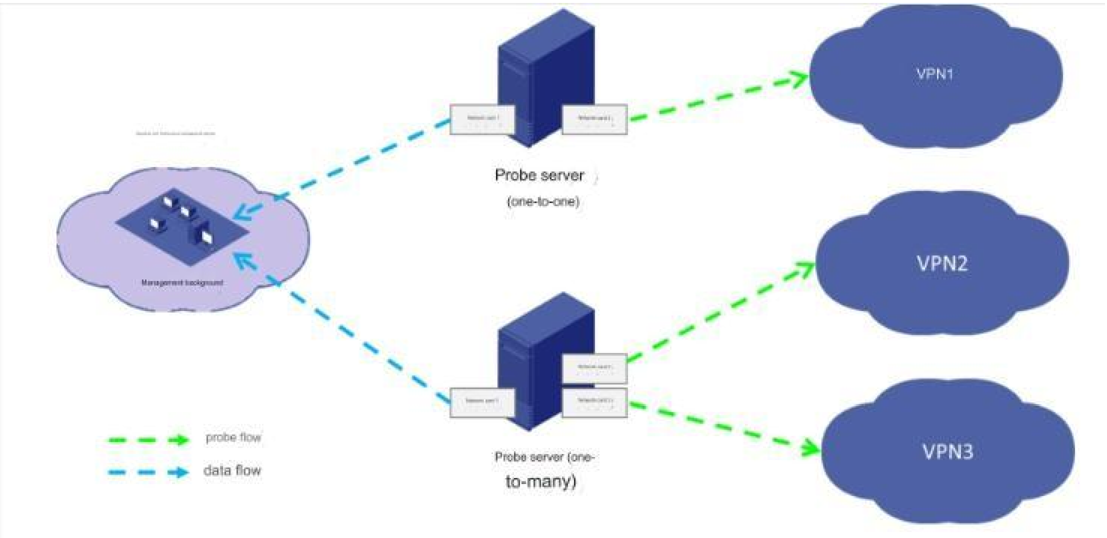
It is recommended that the network probe be directly or indirectly connected to the core network switch. The management backend can be deployed in the same area as the network probe, or in the data center or operation and maintenance management area, as shown in the following figure:



5.1.2. VPN network deployment solution

—Some large enterprise networks adopt VPN isolation (such as MPLS VPN). Generally speaking, in such enterprise networks, a separate operation and maintenance management domain is set up to directly connect each network node. Therefore, in order to ensure comprehensive monitoring coverage of each VPN network, it is recommended that the management backend be placed in the operation and maintenance management domain of the enterprise network, and the probe server be placed at the entrance of each VPN, using a dual network card configuration, and one network port is connected to the VPN for detecting the VPN. network, and another network port is connected to the operation and maintenance management domain for reporting data to the management background. The details are shown in the figure below.

The network probe supports multi-network card detection, so in actual deployment, a one-to-many solution can also be adopted, that is, multiple network cards are configured and each network port detects a VPN.

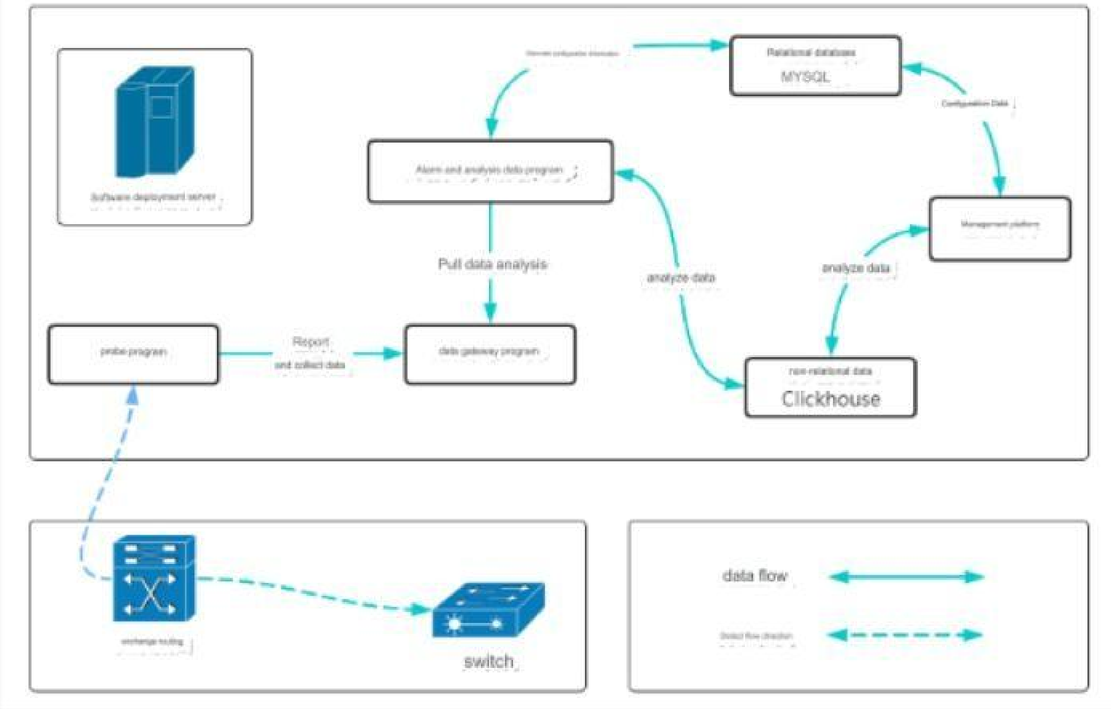


5.2. Server configuration plan

The server configuration scheme is divided into two types: single-machine centralized configuration and cluster distributed configuration scheme.

5.2.1. Single-machine centralized configuration solution

Single-machine centralized deployment is mainly suitable for demonstration pilots, application scenarios with low reliability requirements and small volume. In this scenario, the probe and management background can be deployed on one server.



Schematic diagram of stand-alone deployment plan

System architecture description and deployment requirements: 1) Deploy a set of software packages, including collection programs, alarms, analysis programs, application management programs, databases, and data gateway programs.

2) The network between the probe and the collection object is reachable.

3) Data storage period, default is 3 months.

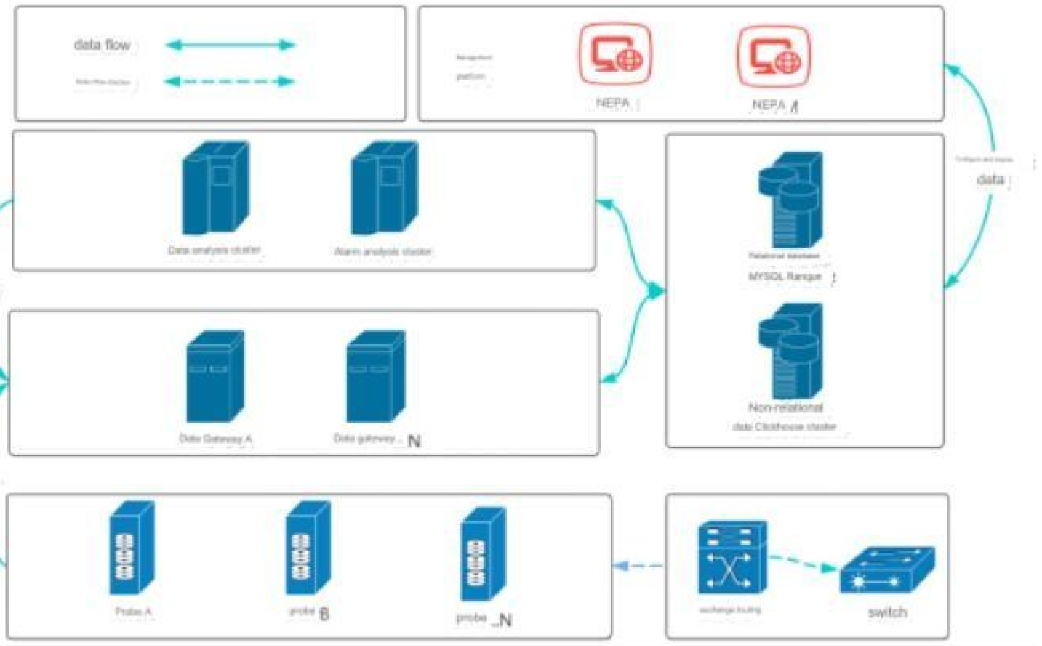
The specific configuration scheme recommends monitoring less than 3,000 links and the following server configuration is provided. Please evaluate and select based on specific business needs.

serial number	project	unit	quantity	Configuration specifications	Remark
1	server	tower	1	The configuration requirements are as	1. Support physical

				follows: CPU: no less than 32 cores; Memory: no less than 32G; Hard drive: no less than 512G, read and write speed 1000MB/s and above; Network card: 1 Gigabit adaptive electrical port; Ride0: active and backup (optional) Operating system: openEuler	machines 2. Disk read and write speed is high 3. It is recommended to support data primary and backup
2	Deployment package	set	1	Collection program, analysis program, application management program, database, data gateway program, JDK	

5.2.2. Cluster distributed deployment

Cluster distributed deployment is mainly suitable for commercial use, application scenarios with high reliability requirements and large amounts of data.



Schematic diagram of cluster deployment scheme

System architecture description and deployment requirements: 1) Software package deployment is based on the actual number of links, and mainly includes collection programs, alarms, analysis programs, application management programs, databases, and data gateway programs.

2) Data analysis, alarm analysis, data gateway, database, and management platform networks are reachable to each other.

3) The probe and data gateway network are reachable.

4) The network between the probe and the collection object is reachable.

5) The data retention period defaults to 3 months and is recommended to be determined based on the actual project.

For specific configuration options, it is recommended to add a set of the following server configurations for every 1,000 additional links. Please evaluate and select based on specific business needs.

serial number	project	unit	quantity	Configuration specifications	Remark

1	probe server	tower	1	CPU: no less than 16 cores;
				Memory: no less than 8G;
				Hard drive: no less than 512G;
				Network card: 1 Gigabit adaptive electrical port;
				Operating system: centos7.6
					Support physical machine

2	analysis server	tower	1	CPU: no less than 16 cores;
				Memory: no less than 16G;
				Hard drive: no less than 512G;
				Network card: 1 Gigabit adaptive electrical port;
				Operating system: openEuler
					Support virtual machines and physical machines

3	application server	tower	1	CPU: no less than 4 cores;	Support virtual machines and

				Memory: no less than 8G;
				Hard drive: no less than 512G;
				Network card: 1 Gigabit adaptive electrical port;
				Operating system: openEuler
					physical machines

4	Database service	tower	1	CPU: no less than 8 cores;
				Memory: no less than 16G;
				Hard drive: no less than 512G;
				Network card: 1 Gigabit adaptive electrical port;
				Operating system: openEuler
					Support virtual machines and physical machines

5	software package	set	1	Collection program, analysis program, application management program, database, data gateway program, JDK	