SANGFOR

User Manual for Sangfor Application Delivery Controller

Product version AD 7.0.9R1

Issued on March 25, 2021



■ Copyright Statement

Copyright © 2020 Sangfor Technologies Inc. and its licensees. All right reserved.

The copyright is held by Sangfor Technologies Inc. All rights reserved. The pertinent materials include but are not limited to the following: text description, format, illustrations, photos, methods, procedures, and so on, unless otherwise stated. Without prior written permission of Sangfor Technologies Inc., no part of the contents in this document shall be reproduced or excerpted by any individual or institution in any form or by any means.

Content contained in this manual is subject to changes or corrections due to product version update or other reasons. Sangfor reserves the right to update this document as necessary without further notice. This document is for reference only. Best efforts have been made to ensure the accuracy of the content, but this does not rule out possible errors in this document. Statements, information, and recommendations in this manual do not constitute a warranty of any kind, expressed or implied.

Sangfor reserves the right to a final explanation for this document.

Foreword

User Manual for Sangfor Application Delivery Controller (ADC) consists of four parts: The first part gives an overview of the Application Delivery Controller (ADC), including a brief introduction of the Sangfor ADC and its key features. The second part describes the method to install and deploy the ADC. The third part expounds on how to use, manage, and maintain the Sangfor ADC, including application publishing, link load balancing, and global load balancing. The fourth part summarizes common problems encountered during ADC installation and use. The Foreword includes the following information:

1. Intended Readers
2. Product Version
3. Document Conventions
4. Information Acquisition
5. Technical Support
6. Feedback
7. Revisions

Intended Readers

This manual is recommended for the following persons:

1.Network design engineers

2.O&M personnel

3.Onsite technical support personnel

Product Version

The product and version involved in this document are as follows:

Product Name	Version
ADC	7.0.9R1

Document Conventions

1. Acronyms

Acronym	Full Name
ACL	Access Control List
ADC	Application Delivery Controller
BRAS	Broadband Remote Access Server
DNAT	Destination NAT
DNS	Domain Name Service
DR	Direct Route
FTP	File Transfer Protocol
HA	High Availability
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
MAC	Media Access Control
NAT	Network Address Translation
OSPF	Open Shortest Path First
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RTT	Round Trip Time
STP	Spanning Tree Protocol
SNAT	Source NAT
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network

2. Format of graphical interface

Text Description	Symbol	Example
Button	Border + shadow + shading	The "OK" button can be simplified to OK.
Menu item	『 』	The "System Config" menu item may be simplified as 『System Config』.
Continuously select menu items and submenu items	→	Select『System Config』→『Interface Config』.
Drop-down list, radio box, and checkbox options	[ ]	The "Activate User" checkbox option may be simplified as [Activate User].
Window name	【 】	Click to pop up the【New User】window.
Prompt	“”	The prompt box displays "Configuration saved successfully, the configuration has been modified. The service needs to be restarted to take effect. Restart now?"

3. Sign conventions

This manual adopts the following symbols to indicate the parts which require special attention:

Attention: reminds you of the things that need to be noticed during operations. Improper operations may result in invalid settings, data loss, or device damage.

Warning: calls special attention to the comments after this sign. Improper operations may cause injury to the human body.

Notes, Tips, or Tricks: provides necessary additions and explanations to the operation description.

Information Acquisition

To get the latest product information, visit Sangfor's official website (www.sangfor.com):

Installation and configuration:

https://community.sangfor.com/plugin.php?id=sangfor_databases:index#?tags=47

Software version and update:

Please contact Sangfor Technical Support.

Technical Support

Technical support Email: tech.support@sangfor.com

Technical support hotline: +60 12711 7129 (7511)

Sangfor community: https://community.sangfor.com

Sangfor Technologies' service provider and service validity period inquiry:

https://community.sangfor.com/plugin.php?id=service:query

Official website: www.sangfor.com

Feedback

If you find any product information-related problem when using our products, please contact us at the following site:

- https://community.sangfor.com
- Or call the local office to provide feedback.

Contents

Chapter 1 Terms and Definitions 14
Chapter 2 Overview 15
2.1 ADC Introduction 16
2.1.1 Focus of Load Balancing 16
2.1.2 Appearance of the Application Delivery Concept 17
2.2 Fast, Intelligent Application Delivery Network 17
2.3 Key AD Features 17
2.3.1 Multi-Link Load Balancing 17
2.3.2 Server Load Balancing 22
2.3.3 Server Performance Optimization 28
2.3.4 Global Load Balancing 32
2.3.5 Programmable Function iPro 36
2.3.6 Message-based Persistent Connection Load Balancing 37
2.3.7 Deployment and Management 37
2.3.8 High Availability (HA) 39
2.3.9 Full Support for IPv6 42
Chapter 3 Deployment & Installation 44
3.1 Pre-operational Preparation 45
3.1.1 Environment Requirements 45
3.1.2 Power Supply 45
3.1.3 Product Appearance 45
3.1.4 Documentation and Tool Preparation 46
3.2 Device Installation 46
3.2.1 Configuration and Management 46
3.2.2 Wiring Method 46
3.3 Network 47
3.3.1 Interface IP 47
3.3.2 Aggregate Interface 51
3.3.3 Bridge Interface 53

3.3.4 VLAN Interface 55
3.3.5 NAT 56
3.3.6 Static Routing 60
3.3.7 Dynamic Routing 62
3.4 Gateway Deployment for A Single Device 70
3.5 Bypass Deployment for A Single Device 72
3.6 Active-Standby Mode 73
3.6.1 Active Device Configuration 75
3.6.2 Standby Device Configration 80
3.7 Cluster Mode 82
3.7.1 Master 83
3.7.2 Standby Controller or Member 86
3.7.3 Exit A Cluster (Disable A Cluster) 88
3.8 Network Security 88
3.8.1 ACL 88
3.8.2 Anti-DOS(Insider Threat) 90
3.8.3 Anti-DOS(Outside Threat) 92
3.8.4 ARP/ND Protection 94
3.8.5 ARP Proxy 96
Chapter 4 System 97
4.1 General 97
4.1.1 Management Interface 97
4.1.2 Web UI 99
4.1.3 Licensing 101
4.1.4 SMTP 103
4.1.5 Date/Time 104
4.1.6 HOSTS 106
4.1.7 Network 107
4.1.8 WebConsole 108
4.2 Administrators 110

4.2.1 Administrator 110
4.2.2 Roles 111
4.2.3 External Authentication 113
4.3 SNMP 115
4.3.1 SNMP(V1,V2C) 116
4.3.2 SNMP(V3) 117
4.3.3 Traps 119
4.4 Alarm Options 121
4.4.1 Email Alarm 121
4.4.2 SNMP Traps Alarm 124
4.4.3 Syslog Server 126
4.4.4 HTTP Logs 127
4.5 Maintenance 130
4.5.1 Backup/Restore 130
4.5.2 System Upgrade 132
4.5.3 Auto Update 133
4.5.4 Proxy Options 135
4.5.5 Shut Down/Restart 136
4.5.6 Privacy Policy 136
4.5.7 Change Mode 137
4.6 Troubleshooting 138
4.6.1 Session Query 138
4.6.2 Packet Capture 138
4.6.3 Blackbox 140
4.6.4 Cache Retrieval 141
4.6.5 Cache Miss Retrieval 141
4.6.6 Session Persistence 142
Chapter 5 Status Overview 143
5.1 Status 143
5.1.1 App Load Balancing 143

5.1.2 Link Load Balancing 146
5.1.3 Global Load Balancing 147
5.2 Device Status 149
5.3 Network Status 150
5.3.1 Interface 150
5.3.2 Dynamic Routing 151
5.3.3 Link 151
5.3.4 DDoS Attack 151
5.3.5 Policy-based Routing 152
5.4 Logs 152
5.4.1 Service Logs 152
5.4.2 Operation Logs 153
5.4.3 SSL Logs 154
Chapter 6 Objects 155
6.1 Certificates 155
6.1.1 SSL Certificate 155
6.1.2 CA Certificate 158
6.1.3 CRL 158
6.2 Custom Webpage 161
6.2.1 Custom Webpage 161
6.3 Databases 163
6.3.1 IP Database 163
6.3.2 ISP Database 165
6.3.3 Domain Name Database 166
6.3.4 Application Signatures 167
6.3.5 Regional IP Database 168
6.4 Multi-Tenancy 170
Chapter 7 App Load Balancing 176
7.1 Virtual Service 177
7.1.1 Virtual Service Configuration 177
7.1.2 Health Monitor 183

7.1.3 Session Persistence 218
7.1.4 Node Pool 230
7.1.5 IP Anycast 240
7.1.6 SNAT Address Pool 242
7.1.7 SSL Policy 243
7.1.8 SSL Offloading 246
7.1.9 TCP Policy 251
7.1.10 HTTP Optimization Policy 260
7.1.11 HTTP Protection Policy 265
7.1.12 SIP Policy 267
7.1.13 QoS Policy 268
7.1.14 HTTP Rewriting Policy 272
7.1.15 Scheduling Policy 276
7.1.16 Access Control Policy 291
Chapter 8 Link Load Balancing 293
8.1 Policy-based Routing 293
8.1.1 Policy-based Routing 301
8.2 DNS Proxy 304
8.2.1 General 304
8.2.2 Proxy Policy 309
8.2.3 Local DNS Records 311
Chapter 9 Global Load Balancing 315
9.1 Local Intelligent DNS Resolution 315
9.1.1 Configuring DNS server 315
9.1.2 Configuring Domain Name Release 317
9.2 Global Intelligent DNS Resolution 337
9.2.1 Report Center Options 337
9.2.2 Configuring DNS Server 341
9.2.3 Domain Name Release 341
9.2.4 Global Configuration 350

Chapter 10 Report Center 351
10.1 Report Settings 351
10.1.1 Report Options 351
10.1.2 Report Templates 352
10.2 Report Center 359
10.2.1 Enter Report Center 359
10.2.2 Report Center 360
Chapter 11 Routine Inspection for Device 379
11.1 Precautions for Routine Maintenance 380
11.2 Checking the Hardware of the Device 381
11.2.1 Checking the Status Indicator Lights 381
11.2.2 Checking the Indicator Lights of the Interfaces 381
11.2.3 Checking the Running Condition of CPU 381
11.2.4 Checking the Abnormal Status 382
11.3 Checking the Configuration of the Device 382
11.3.1 Device Configuration Backup 382
11.4 Checking the Security of the Device 383
11.4.1 Checking the Security of the Console Account 383
11.4.2 Checking the Remote Maintenance Status of the Console 383
11.5 Checking the Logs of the Device 384
11.6 Description of Log Compliance for the Device 385
11.7 Restoring the Password with a USB Flash Drive 385
Chapter 12 High Risk Operation 386
12.1 Front-end High Risk Operations 386
12.2 Hardware High Risk Operation 388
Chapter 13 Troubleshooting Guidance 388
13.1 Quick Start Guide 388
13.1.1 Troubleshooting Flow 388
13.1.2 Fault Location Method 390
13.2 Use of Auxiliary Tools 390
13.2.1 Web Command Console 390
13.3 Fault Information Collection 391
13.3.1 Collecting Basic Fault Information 391
13.3.2 Collecting Detailed Information On Site 392

13.3.3 Data Reporting Instruction....393
13.4 Troubleshooting....396
13.4.1 Failing to Log In to the ADC Console....396
13.4.2 Failing to Access Virtual Services....396
13.4.3 Slow Access to Virtual Services via ADC....397
13.4.4 Console Reminding Offline Status of Nodes....399
13.4.5 Failing to Connect to ADC's Internet Port....401
13.4.6 Failing to Access the Internet After Switching Between Active and Standby Devices....401
13.4.7 Unbalanced Scheduling of Server Load Balancing Node....403

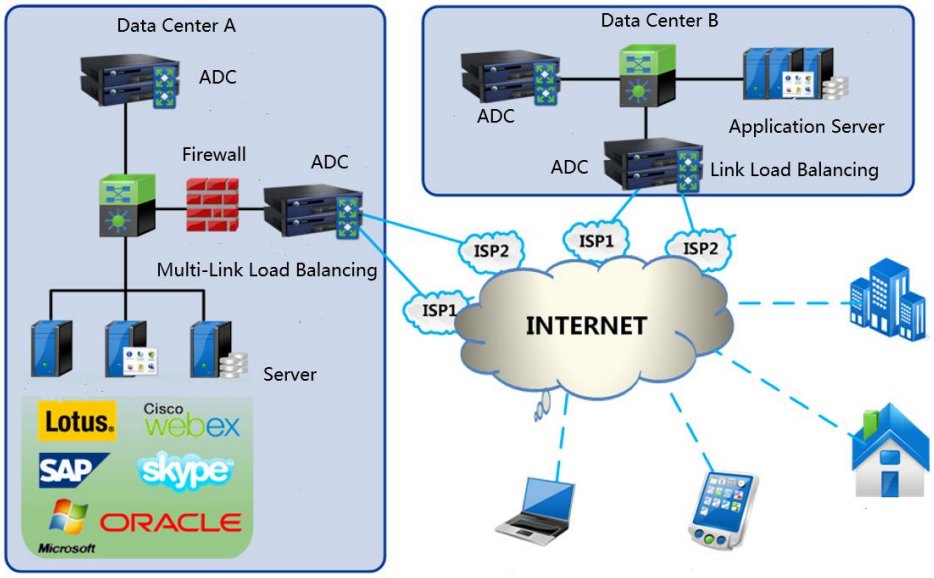
Chapter 1 Terms and Definitions

Term	Definition
ADC	Application Delivery Controller, a load-balancing device.
Cluster	A cluster contains two or more ADCs deployed together to form a large logic device. Each device carries devices and acts as a mutual backup of other devices. This increases the time of continuous stable service operation and resource utilization. An ADC can only join a cluster. After that, all configurations except for network configuration will be synchronized on the cluster controller.
HA	High Available. The purpose of HA is to monitor the condition of the peer device in real time and synchronize its configuration. When a failure is detected on the peer device, a service switch is implemented to ensure service continuity.
Load balancing algorithm	According to a set policy mechanism, the Sangfor ADC dispatches service access traffic to various actual services, such as the server of the corresponding server load balancing, the link of link load balancing, and the site of global load balancing. The dispatch policy mechanism is termed the load balancing algorithm.
Health check	The Sangfor ADC actively detects servers and links using different health check methods and then determines whether a server or link is healthy enough to provide services properly.
Proximity	In the multi-link load balancing scenario, the Sangfor ADC analyzes and compares factors such as the geographical location of the accessing device, the link carrier, and the real-time link health condition detected. Based on the result, the Sangfor ADC selects the best link to ensure that traffic is transmitted via the best link.
Virtual service	Services published by the Sangfor ADC are termed virtual services. They include configuration attributes such as service type (protocol) and node pool (a set of the IP addresses and ports of one or more servers). An access request of a customer arrives at the Sangfor ADC via the Internet. After the request is matched to a virtual service, the ADC dispatches it to an actual server according to the set load

	balancing policy.
Session persistence	The Sangfor ADC provides a mechanism named session persistence to recognize the relevance between a customer and a server. While implementing load balancing, this mechanism ensures that a series of relevant access requests are continuously allocated to the same server. In this particular situation, the ADC will abandon the existing load balancing algorithm.
IP address database	The Sangfor ADC's built-in IP address database records the ISP address ranges owned by various carriers. This enables link load balancing to search the source or destination IP address of a message in the IP address database and find information about the corresponding carrier. The information is then used to select a suitable ISP link for access traffic.

Chapter 2 Overview

A professional application delivery controller, the Sangfor ADC provides a comprehensive solution for users' application publishing, including multi-data center load balancing, multi-link load balancing, and server load balancing. It adopts technologies such as performance optimization, unilateral acceleration, and multiple intelligent management to monitor the status of each data center, link, and server in real time. It allocates access requests to the appropriate data center, link, and server based on preset rules, so as to reasonably distribute the data streams and fully utilize all data centers, links, and servers. This expands the overall processing capacity of the application system, promotes the stability of the application system, effectively improves user access experiences, and reduces the IT costs of an organization. See the figure below:

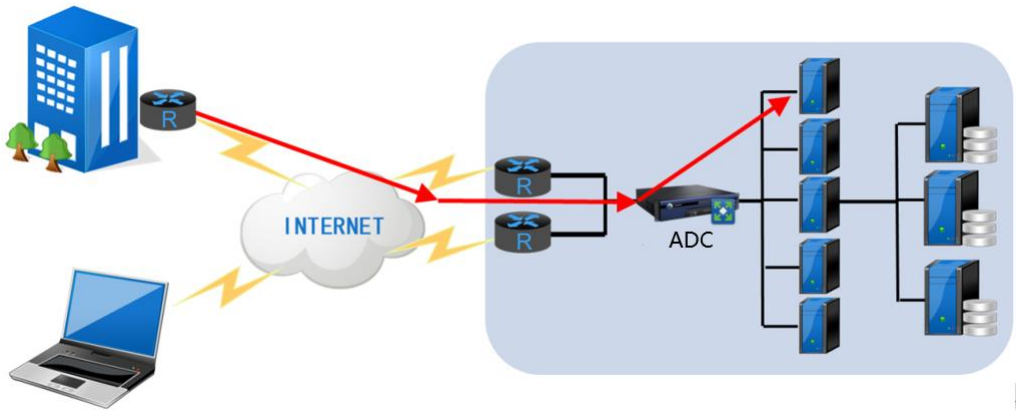


2.1 ADC Introduction

The traditional load balancing technology offers users a cost-effective method to improve the network data processing stability by increasing the bandwidth and throughput of network devices and servers. Compared with load balancing, application delivery adds the functional feature of intelligent optimization on top of the emphasis on stability. This way, it helps users cope with challenges of service deployment and delivery arising in complicated application environments. By reasonably deploying the ADC, users can not only further improve the performance and security of their service applications but also promote the infrastructure efficiency of data centers and even cope with the trend of virtual data center deployment in the future.

2.1.1 Focus of Load Balancing

Server load balancing was originally created to solve network-related problems, such as allocating access requests among a set of servers responsible for certain Web application delivery. It was initially implemented by a simple DNS round robin, which has limitations. As a result, load balancing devices for particular functions emerged on the market. These devices analyze inbound application requests to map them to available servers. See the figure below:



To address the increasingly complicated user access requirements, innovations in load balancing have been continued. In the beginning, innovations centered around problems related to inbound traffic, such as dynamic recognition of server workloads and failures and the session persistence function to prevent the loss of user access operations. However, the market evolved quickly and began to focus on other problems, such as application and server efficiency. The SSL offloading technology is the best example in this aspect.

The attention was finally drawn to outbound traffic. A series of technologies and functions appeared on the market to increase the efficiency of service application delivery over networks. Innovations were also diverted from pure network technologies focusing on infrastructure efficiency to performance optimization and security of service applications. Load balancing began to develop from a simple network product into application delivery, a comprehensive concept covering network, server, service application, and even security.

2.1.2 Appearance of the Application Delivery Concept

The advanced ADC helps users address challenges brought by deployment and delivery in complicated application environments nowadays. The last decade has seen the extensive adoption of service oriented architecture (SOA), Web 2.0, and the current cloud computing models, together with a large-scale migration of enterprise-level applications to the browser-based mode, aiming at service procedures and user productivity.

Built upon the idea of service application environment improvement, the ADC provides a series of functions to cope with complicated network environments. It can be employed to optimize a range of application areas including service persistence, end-user access experience, and data center availability. In addition, it helps reduce the number of servers to be deployed, provides a real-time control mechanism to facilitate data center virtualization, and lowers requirements for power supply and cooling of data centers, allowing user services to continue the trend of compactness, energy conservation, and environmental protection.

2.2 Fast, Intelligent Application Delivery Network

Despite that ADC provides abundant optimization functions for improving users' service application performance and security, most domestic users remain to focus on traditional load balancing in practical use. However, in China and even the whole Asia market, more complicated application delivery requirements are arising in online service and e-commerce, which means more challenges to service providers publishing service applications. China still lags behind European and American developed countries in terms of broadband penetration and line quality, so there is much room for optimization of user access experience. In other words, the performance optimization features of application delivery will become ever clearer, and even been amplified, in such an environment.

The application delivery technology has become full-blown today. Products of all manufacturers are basically similar, with focuses on different aspects. Some products are centralized solutions highlighting integration, while others emphasize security. Sangfor is devoted to a fast, intelligent application delivery solution with many functional details reflecting Sangfor's profound insights into the requirements of various user groups in various regions. The company strives to offer customers a product that outperforms its counterparts on return on investment. In doing so, it improves user access experiences while strengthening its service competitiveness.

2.3 Key AD Features

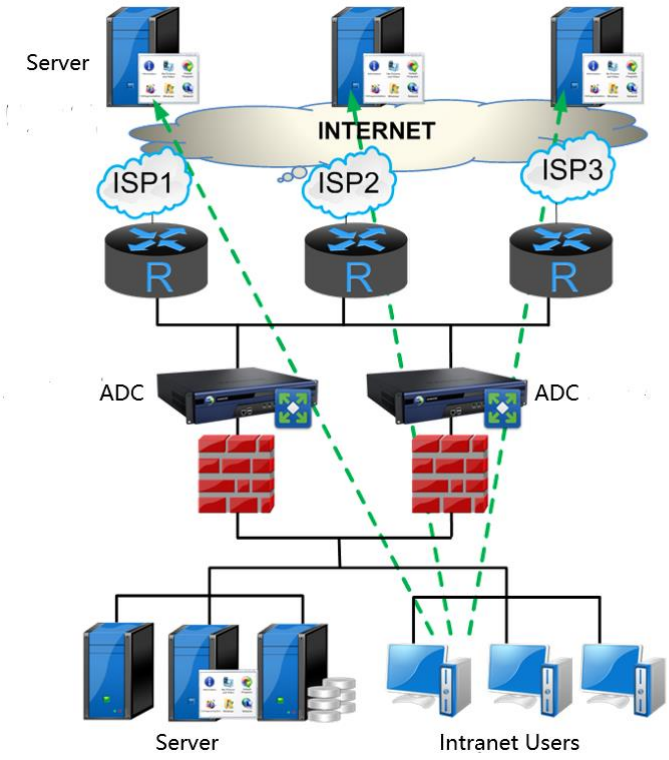
2.3.1 Multi-Link Load Balancing

The Sangfor ADC integrates policy-based routing, DNS transparent proxy, intelligent DNS resolution, and other technologies. Using algorithms such as round robin, weighted round robin, static proximity, and dynamic proximity, it solves traffic load balancing problems in multi-link network environments, thus fully increasing multi-link bandwidth usage and saving investment of enterprises and public institutions in communication links. It also provides users with a superior access experience by allocating optimal communication links. In addition, the Sangfor ADC applies

link health check and session persistence technologies to provide the link access capability even when a link is disconnected. This takes full advantage of the reliability brought by multiple links, providing user access with comprehensive support.

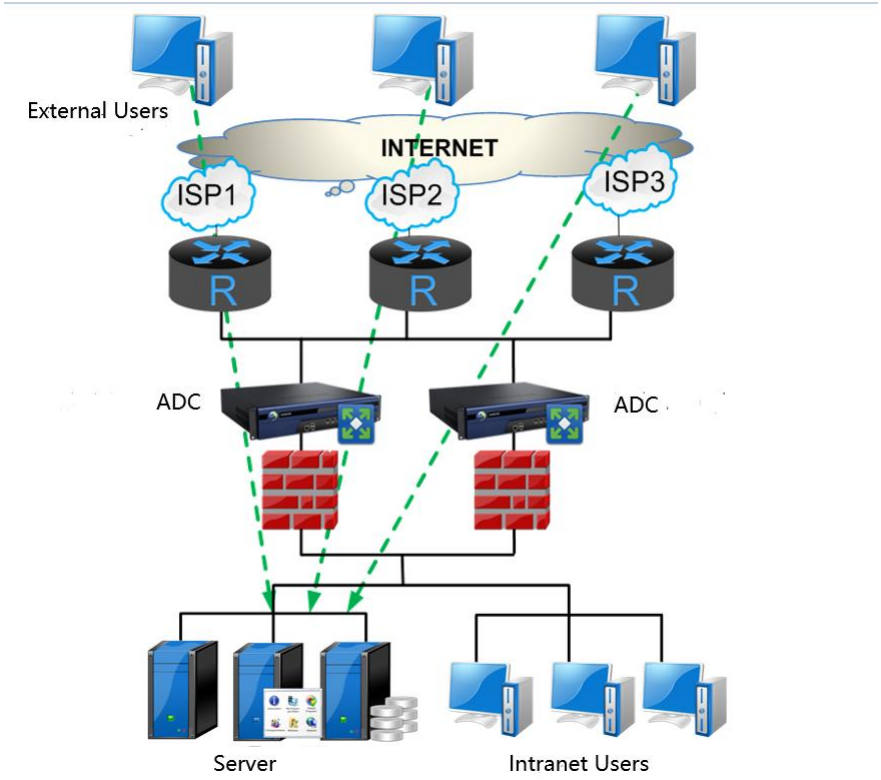
2.3.1.1 Outbound Traffic Load Balancing

When LAN users are accessing Internet access resources, after receiving the access traffic of the users, the Sangfor ADC allocates the traffic to different Internet links based on the preset link load balancing policy for outbound traffic load balancing and enhanced bandwidth usage of Internet links. See the figure below:



2.3.1.2 Inbound Traffic Load Balancing

When external users are accessing internal resources, Sangfor ADC binds a domain name to the external network addresses of multiple carriers using intelligent DNS resolution technology, in order to resolve the domain name resolution requests from users of the carriers. Based on different load balancing policies, Sangfor ADC returns the optimal access addresses to users of different carriers, thus achieving inbound traffic load balancing of users. See the figure below:



2.3.1.3 Link Load Balancing Algorithms

Sangfor ADC supports the following algorithms. Administrators can select the corresponding link allocation policy as required to support more personalized link usage rules.

1. Application Traffic Diversion

Implementation mechanism—Applications corresponding to user Internet access traffic are recognized based on the packet feature, port number, IP address, and other conditions. Data is then diverted according to the application category (for example, video traffic is diverted to line 1 and game traffic to line 2) for reasonable usage of bandwidth resources.

Applicable scenario—There are multiple Internet links differing in bandwidth and quality.

2. Traffic Diversion of Overseas Domain Names

Implementation mechanism—The destination domain name of user access is matched in the built-in overseas domain name database to divert data traffic accessing overseas

domain names to a specified line. This improves the rate and quality of successful access to overseas resources.

Applicable scenario—There are multiple Internet links, one of which is suitable for access to overseas resources.

3. Round Robin

Implementation mechanism— All network links are put in a single queue. The IP address of the next network link in the user queue is returned in sequence.

Applicable scenario—There are multiple Internet links of the same carrier, all with similar bandwidths.

4. Weighted Least Traffic

Implementation mechanism—The real-time traffic of each link is made to be proportionate to its preset weight during new connection scheduling. New connection requests are allocated to the link currently with the least proportion.

Applicable scenario—There are multiple Internet links significantly differing in bandwidth.

5. Static Proximity

Implementation mechanism—The link is selected according to the static optimal route defined in advance for a target. Alternatively, based on the Sangfor ADC's built-in global IP address database, the Internet carrier of a destination IP address is determined to select the corresponding ISP link.

Applicable scenario—There are multiple Internet links of various carriers and the majority of the service traffic is inbound access traffic.

6. Dynamic Proximity

Implementation mechanism—Both the data transmission latency and the real-time link load are taken into account to accurately calculate the optimal route and select the link.

Applicable scenario—There are multiple Internet links of various carriers and the majority of the service traffic is outbound access traffic.

7. Bandwidth Ratio

Implementation mechanism—As Internet links may differ in throughput, the bandwidths of the links are used as the weight (the bandwidth ratio of each link), according to which the data traffic is allocated to each link.

Applicable scenario—There are multiple Internet links of the same carrier that differ significantly in bandwidth.

8. Hash

Implementation mechanism—The Hash Method based on the LOCAL DNS IP address schedules access of different users to different links.

Applicable scenario—There are multiple Internet links and the requests of the same user must be distributed to the same link.

9. Primary/Secondary

Implementation mechanism—Primary and secondary links can be set for a network. User access requests will be scheduled to the secondary link only when the primary link fails.

Applicable scenario—There are multiple Internet links and users require high persistence of service access.

10. First Available

Implementation mechanism—All user requests are scheduled to the first valid fault-free link.

Applicable scenario—There are multiple Internet links and users are sensitive to response latency of service access.

2.3.1.4 Link Health Check

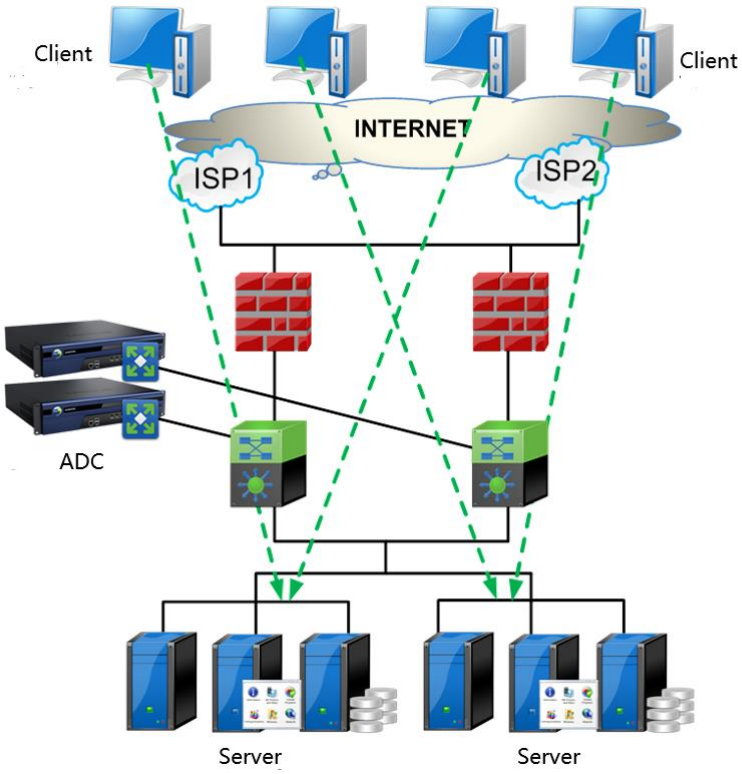
The Sangfor ADC judges the performance of a link based on the availability of multiple Internet sites. For example, inspect TCP port 80 for www.sina.com.cn, www.sohu.com, and www.qq.com through telecommunication lines, and making "or" computation to the inspection result. Therefore, if one site is available, the link status will be good. Using this approach avoids not only the limitations of ICMP inspection but also the single-point error brought about by single-site inspection.

2.3.2 Server Load Balancing

Sangfor ADC uses the mechanism of multiple-server clusters to configure all real server services as virtual services to achieve load balancing and directly publishes one virtual service IP address to the public. When a user request arrives at the ADC, each link can be reasonably and quickly allocated to the corresponding server according to the scheduling strategies preset based on multiple Layer 4 and Layer 7 load balancing algorithms, so as to reasonably utilize the server resources. It not only solves the bottleneck issues that occurred in regard to the performance of a single server while reducing investment in hardware but also facilitates subsequent capacity expansion, providing a performance guarantee for systems with a large number of concurrent users.

Sangfor ADC can detect faulty servers in real-time by comprehensively monitoring server health, and timely forward users' access requests to other servers working in normal conditions, implementing multi-server redundancy. In this way, the stability of key application systems is ensured, and local access to an application system will not be interrupted due to server failure.

In recent years, with the gradual exhaustion of IPv4 addresses and the ongoing improvement of IPv6 in security and reliability, many users gradually upgrade their networks from IPv4 to IPv6. To accommodate this trend, Sangfor ADC can not only implement load balancing in IPv4 application systems but also support the L4/L7 server load balancing based on the IPv6 protocol to implement the IPv6 service publishing by users. See the figure below:



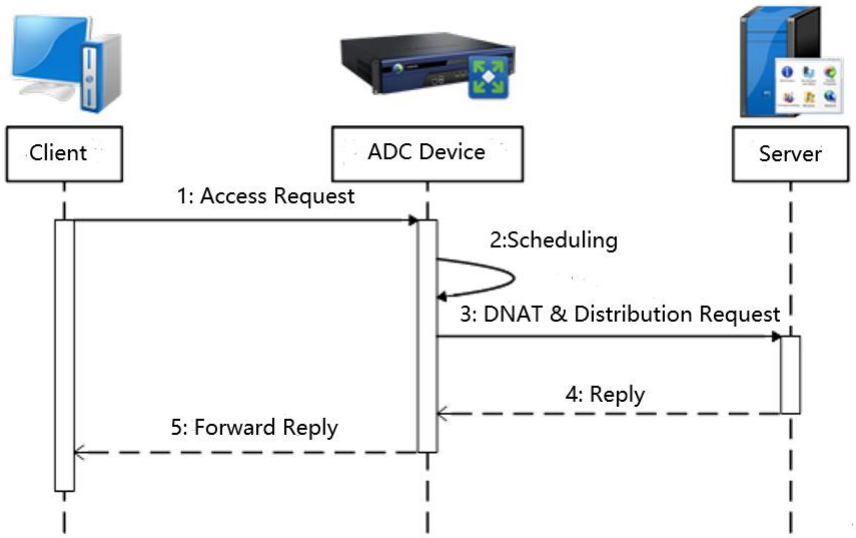
2.3.2.1 L4 Server Load Balancing in NAT Mode

1. Implementation Method

Sangfor ADC supports traffic load balancing based on IP addresses, application types, and content. In this way, the administrator can allocate different server resources for different types of applications. Application type scheduling supports multiple applications based on different protocols, including TCP, UDP, IP, DNS, E-mail, FTP, HTTP, RADIUS, etc. In a scenario of implementing L4 server load balancing, the ADC is responsible for forwarding the client's request to the server, and then a TCP connection is established between the client and the server. At this time, the ADC plays a role similar to that of a router. In NAT mode, when scheduling an access request, the ADC performs a destination IP address translation prior to forwarding the access request to each back-end server.

2. Implementation Process

The implementation process of L4 server load balancing in NAT mode is shown in the following figure:



The process of L4 server load balancing in NAT mode is described as follows:

Step	Description
1	The client sends a request for accessing services. At this very moment, the source IP address is the client IP address and the destination IP address is the IP address for the virtual service
2	After receiving the access request, the Sangfor ADC determines which server the access request should be distributed to according to the predefined load balancing scheduling algorithm
3	Sangfor ADC uses the DNAT technique to distribute access data. At this very moment, the source IP address is the client IP address, and the destination IP address is the server IP address
4	The server processes the received access request and responds with response data.

	At this very moment, the source IP address is the server IP address, and the destination IP address is the client IP address
5	Sangfor ADC receives the response data, converts the source IP address, and then forwards it to the client. At this very moment, the source IP address is the IP address for virtual service, and the destination IP address is the client IP address

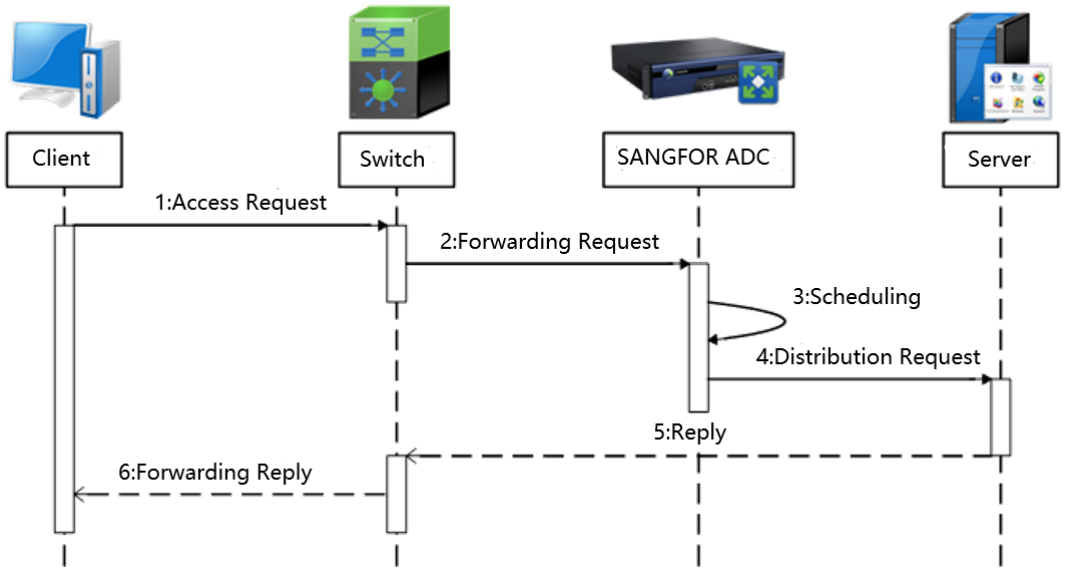
2.3.2.2 L4 Server Load Balancing in DR Mode

1. Implementation Method

The DR (Direct Routing) mode is also called triangle transmission mode. To achieve server load balancing in this mode, the back-end server needs to configure IP address(es) for virtual service on the loopback interface. The ADC does not change the destination IP address when distributing the access request. Instead, it replaces the destination MAC with the server's MAC before forwarding the access request to the back-end server. Responses sent by the server will be directly returned to the user through a switch. Because the server's response does not need to be forwarded by the ADC, the throughput pressure on the ADC is reduced, and performance bottlenecks in the whole service system are effectively avoided.

2. Implementation Process

The implementation process of L4 server load balancing in DR mode is shown in the following figure:



The process of L4 server load balancing in DR mode is described as follows:

Step	Description
1	The client sends a request for accessing services. At this very moment, the source IP address is the client IP address and the destination IP address is the IP address for the virtual service

2	Switch forwards access request to Sangfor ADC
3	After receiving the access request, the Sangfor ADC determines which server the access request should be distributed to according to the predefined load balancing scheduling algorithm
4	Sangfor ADC distributes access data to servers. At this very moment, the source IP address is the client IP address, the destination IP address is the IP address for virtual service, and the destination MAC address is the MAC address of a server
5	The server processes the received access request and responds with response data. At this very moment, the source IP address is the IP address for virtual service, and the destination IP address is the client IP address
6	The switch receives response data and directly forwards it to the client

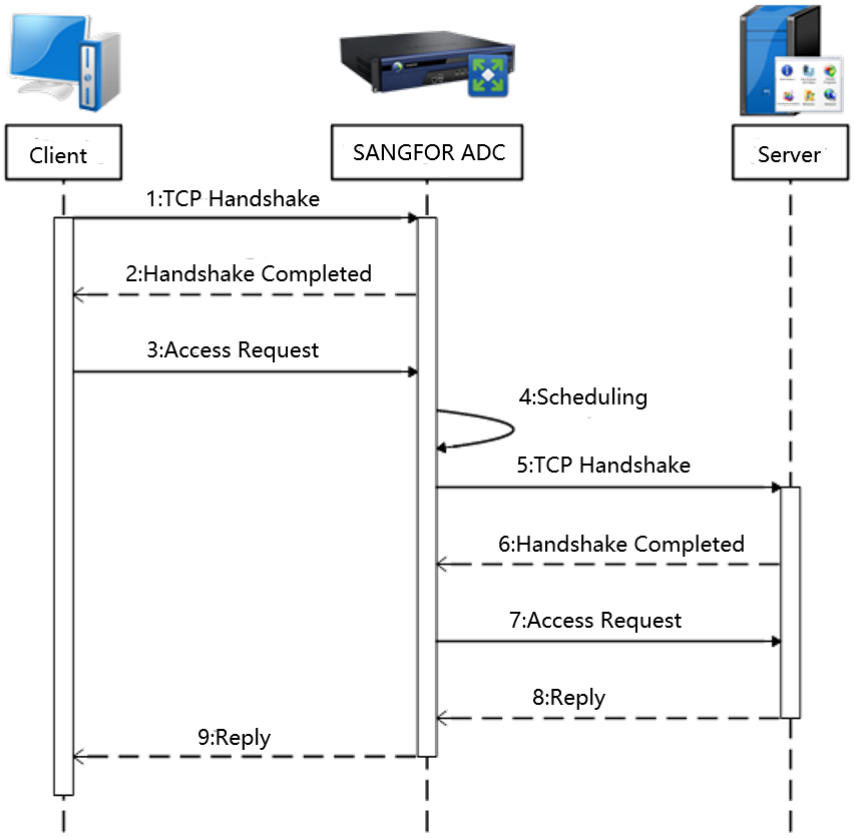
2.3.2.3 L7 Server Load Balancing

1. Implementation Method

The L7 content-based scheduling mechanism enables the administrator to allocate server resources through the content switching in the application layer, so as to realize the diversification and individualization of user request scheduling, and the service application domains can very extensive. For example, select a server based on the matching policy of HTTP header content such as URI, HOST, COOKIE, USER_AGENT, or perform operations such as page jump and discard by rewriting the HTTP headers in requests and responses to realize the interaction and correlation between different service systems. In a scenario of L7 server load balancing, the ADC first establishes a TCP connection with the client, obtains the access request message, and then selects an appropriate server according to the application-layer content in the message and establishes a TCP connection with it. At this time, the ADC plays a role similar to that of a proxy router.

2. Implementation Process

The implementation process of L7 server load balancing is shown in the following figure:



The process of L7 server load balancing is described as follows:

Step	Description
1	The client sends a TCP connection request to the Sangfor ADC. At this very moment, the source IP address is the client IP address, and the destination IP address is the IP address for virtual service
2	Establish a TCP connection between a client and the Sangfor ADC
3	The client sends a request for accessing services. At this very moment, the source IP address is the client IP address and the destination IP address is the IP address for the virtual service
4	After receiving the access request, the Sangfor ADC matches it with the virtual service scheduling policy and uses the load balancing scheduling algorithm to determine which server the access request should be distributed to while caching the data in the access request
5	Sangfor ADC sends a TCP connection request to the server. The SYN sequence number is the SYN sequence number of the client. At this very moment, the source IP address is the client IP address, and the destination IP address is the server IP address
6	Establish a TCP connection between the Sangfor ADC and a server

7	Sangfor ADC modifies the destination IP address and TCP sequence number contained in the cached access request data, and then sends it to the server
8	The server processes the received access request and responds with response data. At this very moment, the source IP address is the server IP address, and the destination IP address is the client IP address
9	Sangfor ADC modifies the source IP address and TCP serial number for the response data, and then forwards it to the client. At this very moment, the source IP address is the IP address for virtual service, and the destination IP address is the client IP address

2.3.2.4 Server Load Algorithm

Sangfor ADC evenly distributes all traffic to each server by using multiple-layer load balancing algorithms, and it not only makes full use of all server resources but also enables each server to undertake traffic processing tasks in a balanced manner, thereby effectively avoiding the occurrence of server task load "imbalance".

2.3.2.5 Session Persistence Mechanism

By using the session persistence technique provided by the Sangfor ADC, a specific server that was connected to can be selected for the visiting user to implement seamless processing of user requests; on the other hand, it can cut down the number of new connections and help to reduce the system overhead of load balancing devices.

2.3.2.6 Server Health Check

Sangfor ADC supports active health checks based on hardware operation status and application categories, passive health checks based on observation modes, and other custom health check mechanisms.

2.3.2.7 Server Smooth Exit

When system maintenance or server upgrade is required, the Sangfor ADC enables the Server Smooth Exit mechanism to ensure that users' access will not be interrupted by server exit. After the administrator selects a certain server that should be out of service from the server group, the Sangfor ADC will not assign any new users to the server. After processing existing user access requests, the server can be managed and maintained accordingly.

2.3.2.8 Bring Online a Warm Standby Server

When adding a newly purchased or maintained server to the server group, the Sangfor ADC can treat this server as a warm standby one and bring it online, so as to avoid system failures of the newly added server caused by a surge in traffic and realize the smooth introduction of the server. After the new server comes online, the ADC will not send any request to the server during its recovery period. During the subsequent warming-up period, the ADC will gradually increase the number of requests allocated to the server, slowly increasing the load on the new server to a stable state, so as to ensure that the server can provide services in an uninterrupted manner during startup and application initialization.

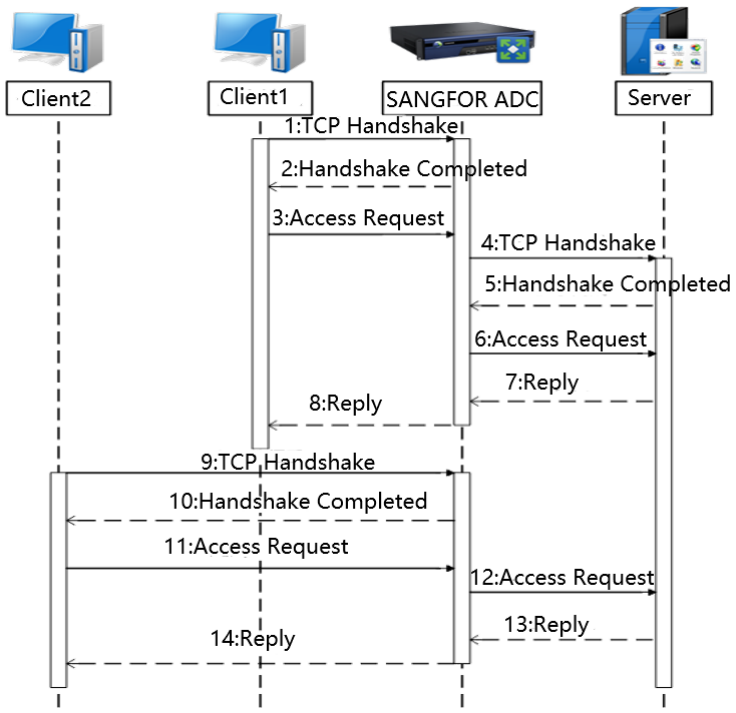
2.3.3 Server Performance Optimization



Informatization construction is a long-term task for each organization. Each IT department has to balance the cost of investment in hardware and achievements related to performance. Different from traditional load-balancing devices, Sangfor ADC can not only implement a server load balancing mechanism to improve server resource utilization, but also support the TCP connection multiplexing, memory caching, HTTP compression, SSL offloading, and many other performance optimization techniques. By reducing hardware resource consumption of servers and shortening the server response time, the ADC saves costs of investment in hardware while effectively ensuring the user access speed and stability, thereby enhancing users' access experience.

2.3.3.1 TCP Connection Multiplexing

For HTTP-based application systems, the Sangfor ADC can bundle numerous client access requests for processing, and forward client requests to servers in turn by multiplexing relatively few server-side TCP connections, instead of forwarding each HTTP request sent from each client to servers via a specially established TCP connection in a one-to-one manner. In this way, the server workload is reduced without performing any change on network structure or increasing costs of investment in hardware, thereby increasing server processing capacity. See the figure below:



The process of TCP connection multiplexing is described as follows:

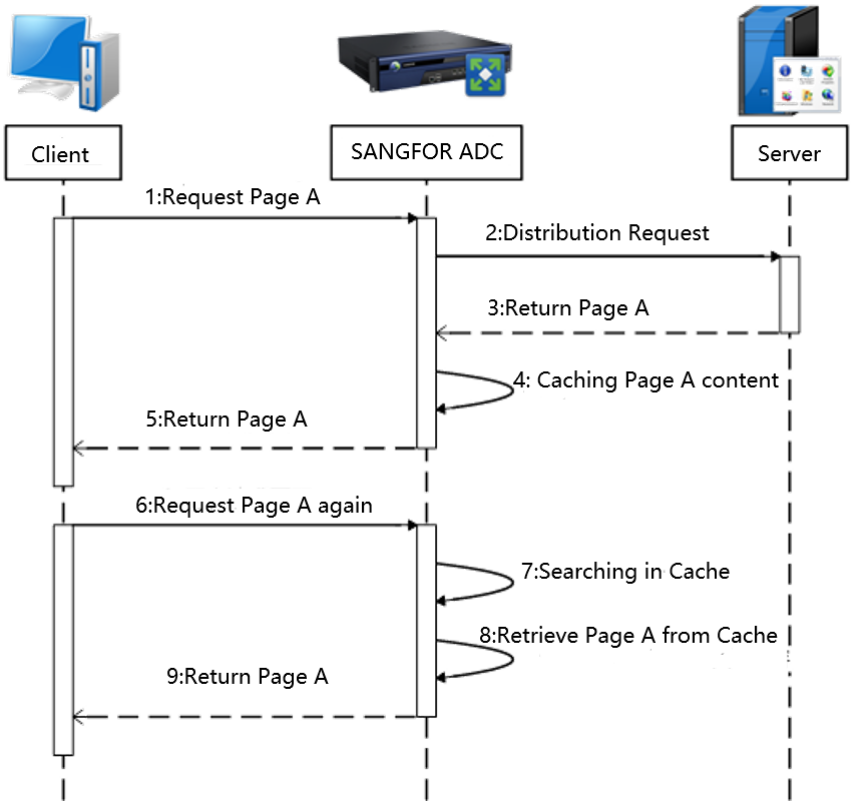
Step	Description
1	The client initiates a TCP handshake request to the ADC
2	The TCP three-way handshake between the client and the ADC is done
3	The client initiates an access request
4	The ADC initiates a TCP handshake request to the server according to the scheduling policy
5	The TCP three-way handshake between the ADC and the server is done
6	The ADC initiates an access request
7	The server responds to the access request from the ADC
8	The ADC responds to the access request from the client
9	The client initiates a TCP handshake request again
10	The TCP three-way handshake between the client and the ADC is done
11	The client initiates an access request
12	The ADC directly initiates access to the service (by reusing the previous TCP connection, without establishing a new connection with the server by using the three-way handshake)

13	The server responds to the access request from the ADC
14	The ADC responds to the access request from the client

Sangfor ADC maintains the TCP connection established between the user side and the back-end server during the previous accessing for subsequent access, significantly reducing the number of user-side connections to be processed by the back-end server (the maximum reduction can reach 90%), accelerating the processing speed for connections between the client and the back-end server, enhancing the processing capacity of the application system, and saving organization's costs of investment in hardware.

2.3.3.2 Memory Caching

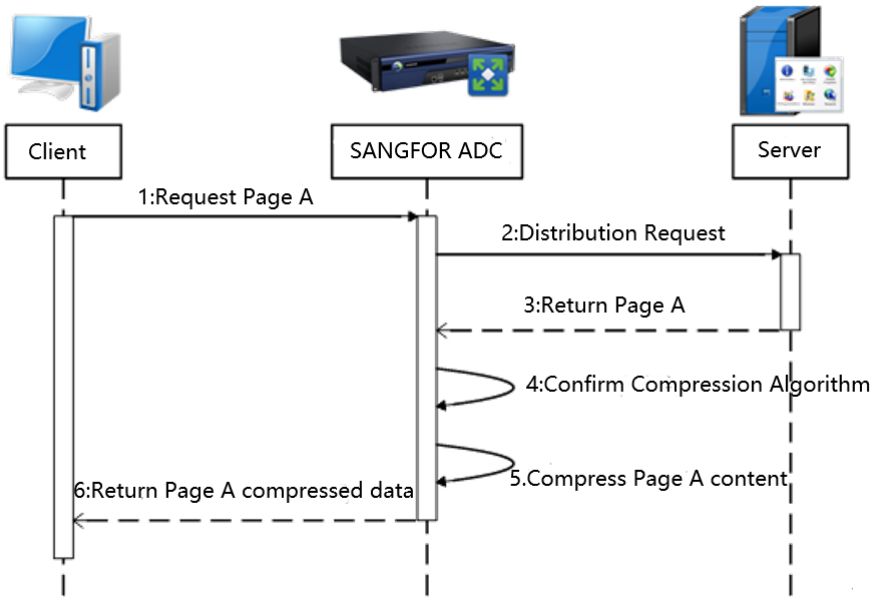
Sangfor ADC adopts the memory-based reverse proxy Cache function to cache the page content of related resources such as websites in the memory. It adopts memory caching and a package storage structure to dynamically adjust the cache size, ensuring a much faster response speed than that of other caching products. See the figure below:



The caching function provided by the Sangfor ADC can reduce the load pressure on the back-end server resulting from users' access. While reducing costs of investment in back-end servers, it also improves the working ability of the system and enhances users' access experience.

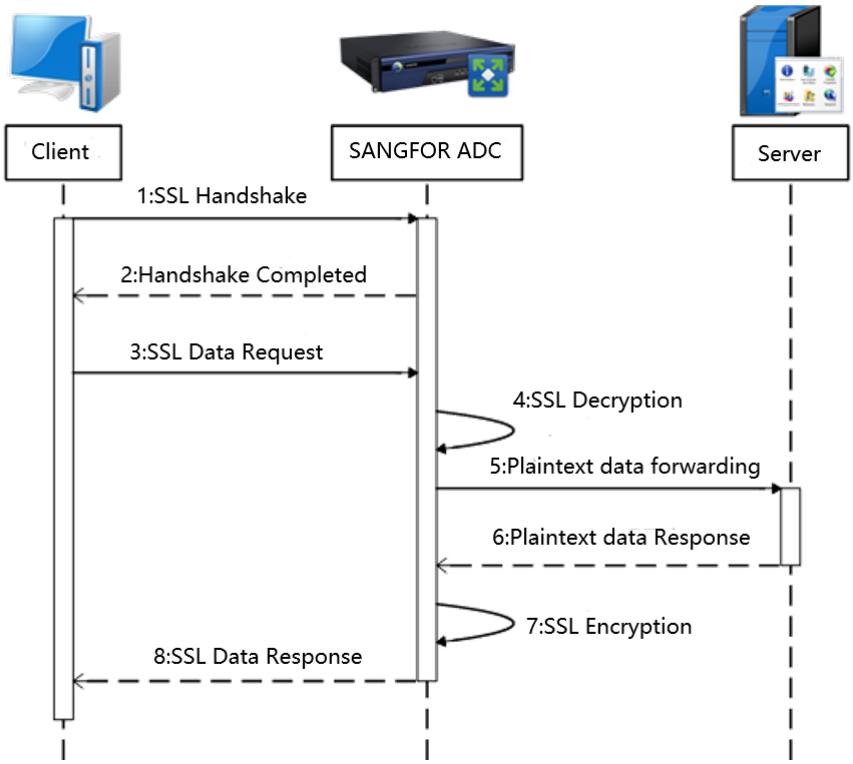
2.3.3.3 HTTP Compression

The HTTP compression function provided by Sangfor ADC. It can be enabled to automatically identify the client's support for gzip or deflate compression algorithm per standard HTTP compression specifications and to implement dynamic data compression.
Enabling the compression function provided by Sangfor ADC can not only save Internet bandwidth to the greatest extent for an organization, shortening the waiting time for users to download content, but also reduce the pressure on Web servers, save costs of investment in hardware, and enhance users' access experience. See the figure below:



2.3.3.4 SSL Offloading

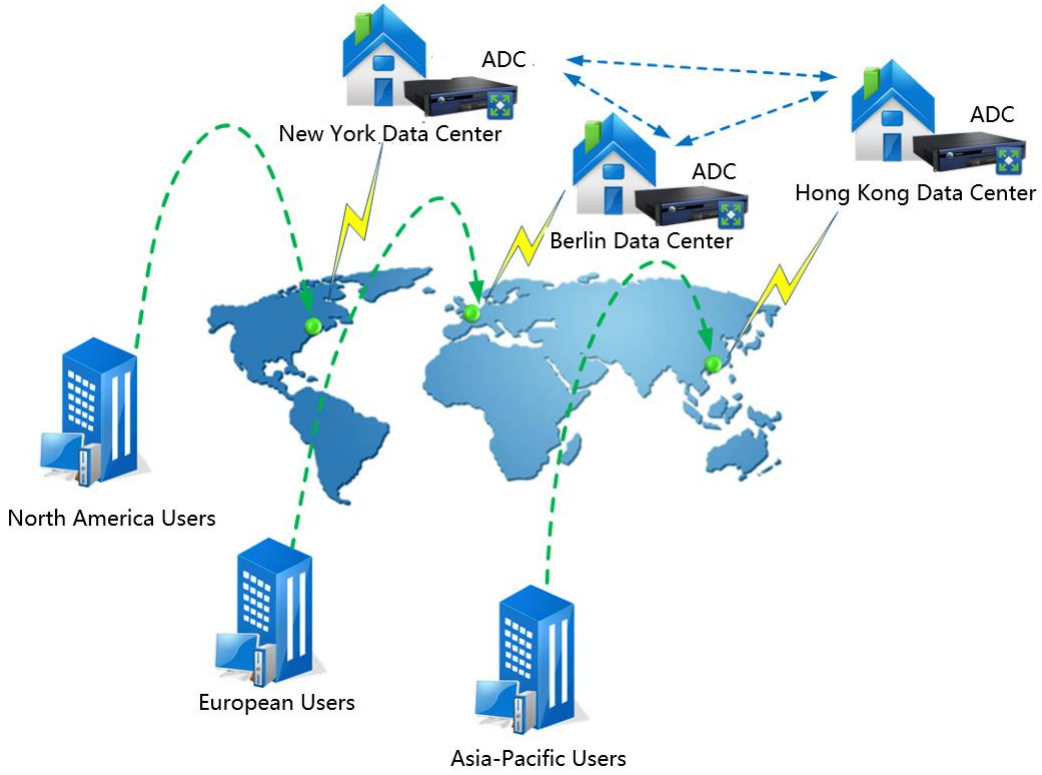
The SSL offloading technology is adopted to transfer the SSL-based encryption and decryption process that occurred during application access to the Sangfor ADC, so as to reduce the pressure on servers' performance and improve the speed to respond to the access requests from a client. Sangfor ADC has the tremendous ability to use the SSL offloading technology to enable end-to-end SSL encryption while supporting comprehensive encryption algorithm configuration and managing server certificates. See the figure below:



Sangfor ADC performs the process of SSL offloading for servers to reduce server performance consumption, saves the number of servers in application systems, reduces investment in the hardware of service systems, and dramatically shortens the response time to respond to user requests, thereby greatly enhancing users' access experience.

2.3.4 Global Load Balancing

Sangfor's global load balancing solution is designed to help organizations deploy the service content of the same application system in different geographic locations, ensuring that multiple data centers bearing the application system can reach a higher level of sustainability, availability as well as a higher rate of speed, ensuring users a faster and more stable access experience no matter where they are in the world. See the figure below:



By implementing a comprehensive health check mechanism, the ADC can monitor the running state of each data center in real-time, and detect any failed data center or any failed server in the data center in a timely manner, so as to ensure that all subsequent access requests sent by users will be allocated to other data centers or servers working in normal condition. It not only makes redundancies across multiple sites to ensure users a stable access experience but also improves the level of resource utilization on each site.

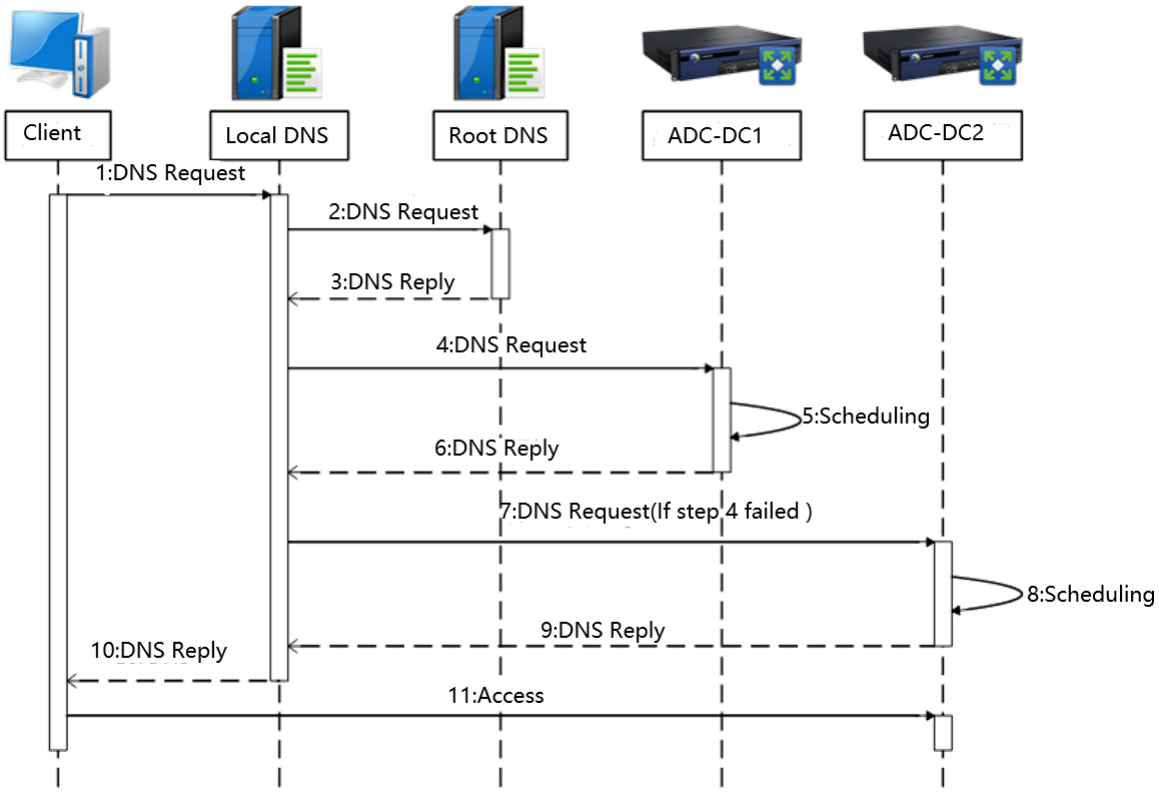
2.3.4.1 Intelligent DNS Multi-site Scheduling

1. Implementation Method

Sangfor ADC uses intelligent DNS resolution technology to provide a unified point of access for all data centers that publish the same service by using a unique domain name, and allocate access requests from users to different data centers according to the load balancing policy preset by the administrator, so as to implement multiple-site load balancing scheduling.
When a user initiates an access request using a domain name, proximity calculations can be carried out according to the location of the local DNS used by the user to parse the IP address of the most appropriate site for the user. The ADC's built-in global IP address database will also be used in combination to further increase the accuracy of the proximity allocation of user requests, so as to completely solve the problem of slow connection speed for users when accessing Internet content from different countries or provided by different carriers.

2. Implementation Process

The implementation process of intelligent DNS multi-site scheduling is shown in the following figure:



The process of intelligent DNS multi-site scheduling is described as follows:

Step	Description
1	The client used by an external user for accessing sends a domain name resolution request to its local DNS server
2	The local DNS server first searches whether there is a corresponding local record, and if not, a query request will be sent to the root DNS server
3	The root DNS server feeds back to the local DNS server, and informs two NS records, pointing to two data centers respectively: DC1 and DC2
4	The local DNS server sends a domain name resolution request to the Sangfor ADC at DC1
5	Sangfor ADC at DC1 first judges the health of the link and then selects an appropriate IP address as the result of domain name resolution according to the predefined load balancing algorithm
6	Sangfor ADC at DC1 feeds back the domain name resolution result to the local DNS server
7	The local DNS server fails to receive the domain name resolution result fed back by the Sangfor ADC at DC1, and sends a domain name resolution request to the Sangfor ADC at DC2
8	Sangfor ADC at DC2 first judges the health of the link and then selects an appropriate IP address as the result of domain name resolution according to the predefined load balancing algorithm

9	Sangfor ADC at DC2 feeds back the domain name resolution result to the local DNS server
10	The local DNS server forwards the obtained domain name resolution result to the client
11	The client initiates a connecting request according to the IP address obtained, and the access request finally reaches DC2

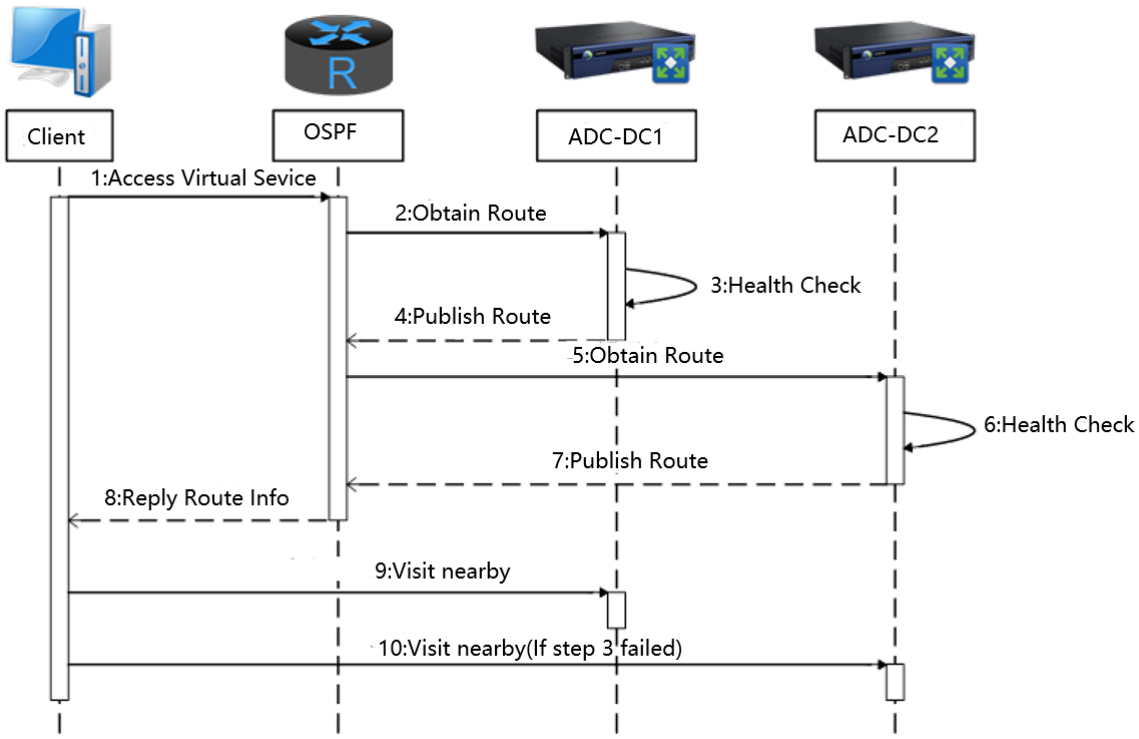
2.3.4.2 IP-Anycast Multi-site Scheduling

1. Implementation Method

Publish the IP address for virtual service on multiple sites through dynamic routing protocols, and use routing information in the network to support users accessing the nearest site and realize site redundancy. In the case that multiple sites provide services online at the same time, the closest site will be selected according to the routing information when a user accesses the virtual service. When a site fails, the OSPF routing will delete routes to the site, so the site will not be selected when a user accessing the virtual service. After the site is restored, the OSPF routing will recover routes to the site. The speed of routing notification depends on the size of networks. Generally, it is within 1 minute.

2. Implementation Process

The implementation process of IP-Anycast multi-site scheduling is shown in the following figure:



The process of IP-Anycast multi-site scheduling is described as follows:

Step	Description

1	The client used by an external user for accessing issues a request for access to the virtual service
2	OSPF routing obtains the dynamic routing information of the DC1 site from the Sangfor ADC at DC1
3	Sangfor ADC at DC1 performs a health check on the virtual service. If the virtual service is available, it will publish the route to the virtual service IP address
4	OSPF routing adds the route published by the Sangfor ADC at DC1
5	OSPF routing obtains the dynamic routing information of the DC2 site from the Sangfor ADC at DC2
6	Sangfor ADC at DC2 performs a health check on the virtual service. If the virtual service is available, it will publish the route to the virtual service IP address
7	OSPF routing adds the route published by the Sangfor ADC at DC2
8	OSPF routing returns the information about dynamic routing to the virtual service IP address to the client
9	The client selects the closest site based on the routing information, and the access request finally reaches DC1
10	When the Sangfor ADC at DC1 detects that the virtual service is unavailable, OSPF routing will remove the route to the DC1's virtual service IP address accordingly. When the client selects the closest site based on the routing information, the access request will finally reach DC2

2.3.4.3 Proximity Judgment Mechanism

To make sure users around the world can be guided to the "optimum" data center when accessing resources, a global load balancer analyzes and judges the distance and time delay between users and sites, current workload of the data center, and many other factors. Sangfor global load balancing supports two proximity methods, static and dynamic, and the two methods can be used together.

2.3.4.4 Health Check Mechanism

The health check mechanism of Sangfor global load balancer can ensure users the best (or optimal) service site.

2.3.5 Programmable Function iPro

Sangfor ADC series products provide the script programming function iPro to realize custom traffic arrangement processing by using Lua language, supporting sub-functions such as traffic scheduling, session persistence, and DNS. iPro is event-driven, inheriting the basic characteristics of the Lua language while being added with certain extensions. Enable the iPro function to write scripts to extract the variable-address and variable-length signatures of application packets, and realize the Layer 7 content switching. It is mainly used for the analysis of unknown protocols and message-based load balancing. iPro can be used to deal with user needs that could not be fulfilled

in the past in many special scenarios.

2.3.6 Message-based Persistent Connection Load Balancing

2.3.6.1 Characteristics of Persistent Connections

At the beginning of a TCP communication, the client will connect with the server, and the message will be transmitted only after the connection is established. After the message is transmitted, the connection between the client and the server will be broke in a short time. The persistent connection means that after the message transmission is completed, the connection between the client and the server will remain unbroken for a long period of time, and subsequent messages can multiplex the connection. Persistent connections are generally used for high-performance processing of large amounts of data. Many important C/S applications use persistent connections. Such applications usually have relatively fixed clients and communicate frequently with servers. However, frequent creation of short connections will lead to a grievous waste of server resources. In contrast, persistent connection effectively reduces the overhead required to create and tear down connections and greatly relieves the pressure on servers' performance.

2.3.6.2 Persistent Connection Load Balancing

Applications that use persistent connections also need to implement load balancing. For many C/S applications, the protocol used is private and not disclosed to the public. Therefore, the content of the protocol cannot be identified in a traditional way, and only connection-based load balancing can be implemented. This method has obvious disadvantages:

1. Scheduling is unreasonable. Load balancing implemented in a traditional way can only be scheduled based on connections, and once a persistent connection is established, it is difficult to be interrupted for reconnection. Different messages in the same connection will be sent to the same server, posing excessive load on the server, while other server nodes may being idle.
2. Failover is too slow. When a server fails, the client keeps waiting for the connection to be timed out rather than immediately re-initiate a new connection. The waiting time is generally so long that the switching speed will be greatly reduced.

The iPro function provided by Sangfor ADC can be used to compile scripts based on the specific characteristics of users' applications, analyze the beginning and end positions of a single message in a connection, and schedule different messages in the same connection to different nodes to implement a message-based persistent connection load balancing, realizing a more reasonable and balanced resource allocation among nodes. In addition, Sangfor ADC will establish a persistent connection with each server node, and detect the health status of each server node in real-time. If an abnormality is detected on any node, messages will be immediately allocated to other normal nodes to avoid any risk of failure, greatly shortening the recovery time after failures and improving service accessing continuity.

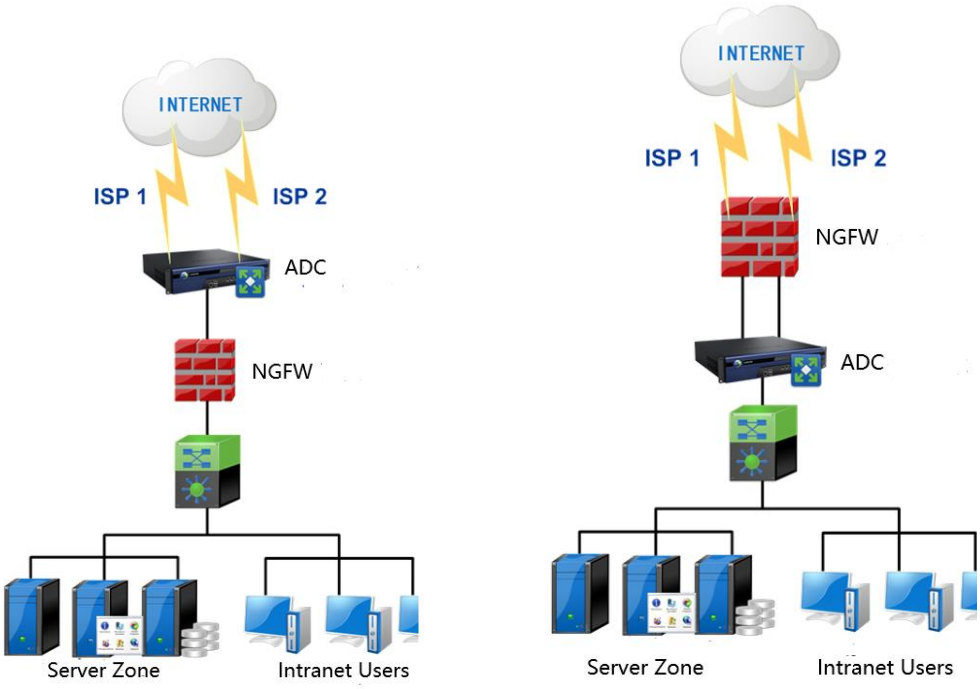
2.3.7 Deployment and Management

Sangfor ADC series products support two deployment modes: routing and bypass. They support LAN protocols such as VLAN and STP and also can be connected with networks that using dynamic routing protocols (e.g. OSPF, RIPv1, and RIPv2) to help users cope with various complex

network environments. ADCs can be employed to optimize a range of application areas including service persistence, end-user access experience, and data center availability.
After starting the simple network management protocol (SNMP) service on an ADC, the user can use the SNMP client software to query the ADC's CPU load, memory usage, new connections, concurrent connections, throughput, and other information to easily monitor the hardware load status of the device. ADC also supports the ACL function, allowing users to precisely control access based on the connected five tuples.

2.3.7.1 Routing Mode

Sangfor ADC is connected in series to a user network link in a gateway mode, and all traffic is processed by the ADC. After receiving an access request from a user, the Sangfor ADC will distribute the user traffic to the most appropriate Internet links according to preset policies, and at the same time, provide the user with the server with the best performance selected from the server group to guarantee a good user experience, thus increasing user satisfaction. This deployment mode is appropriate for implementing link load balancing, server load balancing, and global load balancing. See the figure below:



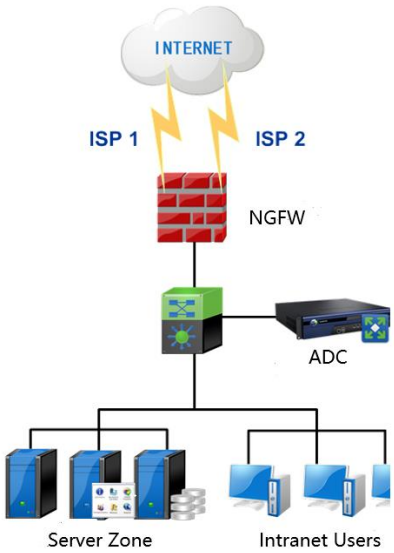
Routing deployment Ⅰ **Routing deployment Ⅱ**

1.**Routing deployment Ⅰ**- the normal ADC deployment mode, which can be used to implement server load balancing and multi-link load balancing at the same time. Enable NAT on the ADC and activate the transparent mode on the firewall.

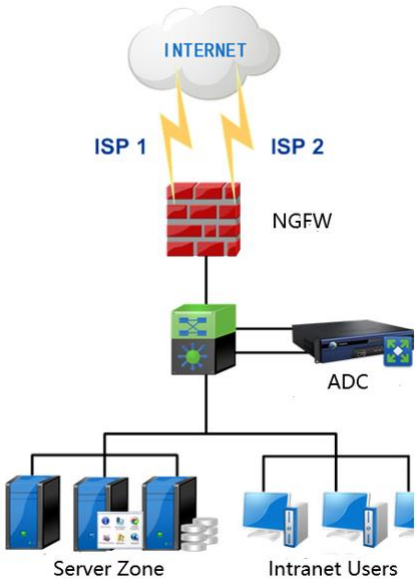
2.**Routing deployment Ⅱ** - enable a NAT firewall (WAN1-LAN1 / WAN2-LAN2) and use the ADC for routing to implement server load balancing and multi-link load balancing at the same time. The firewall needs to be connected to the ADC with two lines at the same time for DNS port mapping.

2.3.7.2 Bypass Mode

Sangfor ADC is deployed in a network in a bypass mode. In such a mode, no change will be made to the customer's network structure and device installation will not cause service interruption, which can implement the rapid and simple deployment of the ADC. After receiving a request from a user, the Sangfor ADC will select the most appropriate server for the user according to a preset load balancing policy, so as to increase server utilization and avoid an uneven allocation of tasks to servers. This mode is appropriate for implementing server load balancing. See the figure below:



Bypass deployment Ⅰ



Bypass deployment Ⅱ

1.**Bypass deployment Ⅰ -** implement port mapping on the firewall or connect to the ADC in a pass-through manner. As long as the DNS request can be received by the device, the link load balancing for inbound traffic as well as server load balancing can be implemented.

2.**Bypass deployment Ⅱ -** a bypass multi-line deployment mode that requires the front-end firewall to support the policy-based routing function, and implements policy-based routing for the ADC's WAN interface IP address, so as to implement link load balancing for outbound and inbound traffic as well as server load balancing.

2.3.8 High Availability (HA)

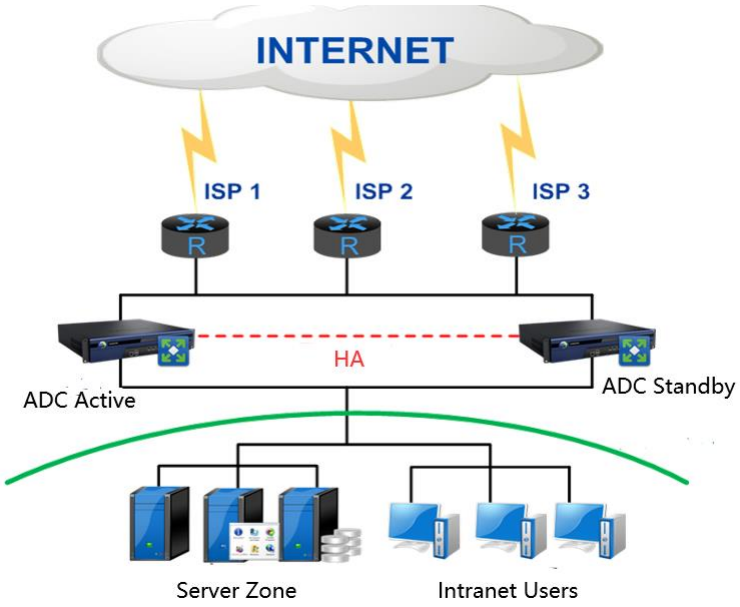
Whether it is used to perform global access scheduling for multi-data centers or to implement load balancing for multiple links and server clusters, the Sangfor ADC is always playing a key role as a control node. Its performance stability and security directly affect the availability of service delivery networks. To eliminate hidden dangers of single-point failures, dual-machine hot standby can be adopted as an effective solution to ensure service continuity, which can largely avoid the interruption of network services.

2.3.8.1 Active-Standby Mode

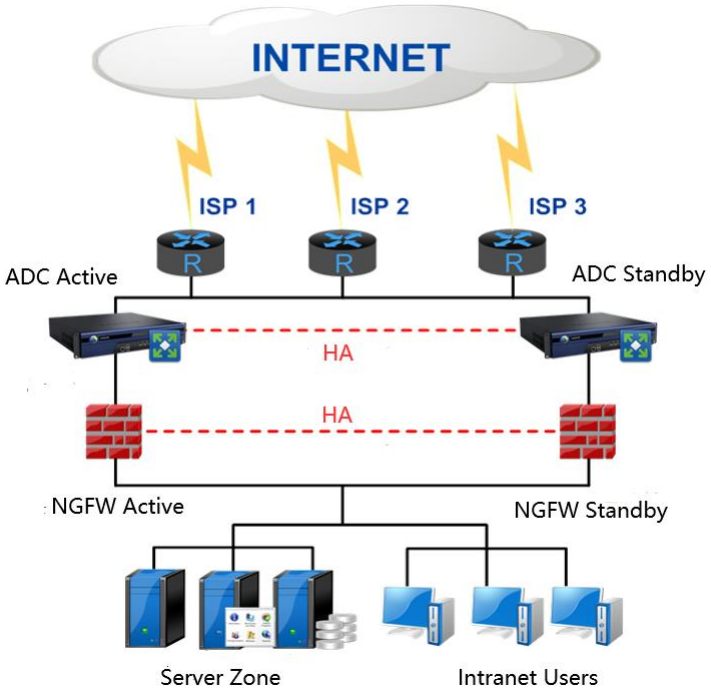
Two Sangfor ADCs are deployed in a network. In this mode, the ADC that is performing load

balancing scheduling is usually called the active device, while the other one that is in a standby state is called the standby device. While the active device is processing services, it will synchronize the session information generated by services to the standby device to ensure that after a dual-device switchover is performed, the newly initiated access to service can still be responded to and processed, and the currently ongoing access will not be interrupted due to switchover. This mode can meet the deployment requirements of avoiding single-point failures in most network environments.

1) **Passive switchover** - When the active device is down and cannot continue working, the standby device detects the active device failure and immediately takes over its job to continue to perform load balancing scheduling. See the figure below:



2) **Active switchover** - When the active device detects a network failure associated with itself (e.g. a WAN interface connection interruption is detected when performing link health check, or an active/standby switchover of firewalls is detected when performing address resolution protocol (ARP) detection), the standby device will actively switch to serve as the active device to ensure the continuity of access to services. See the figure below:



2.3.8.2 Cluster Mode

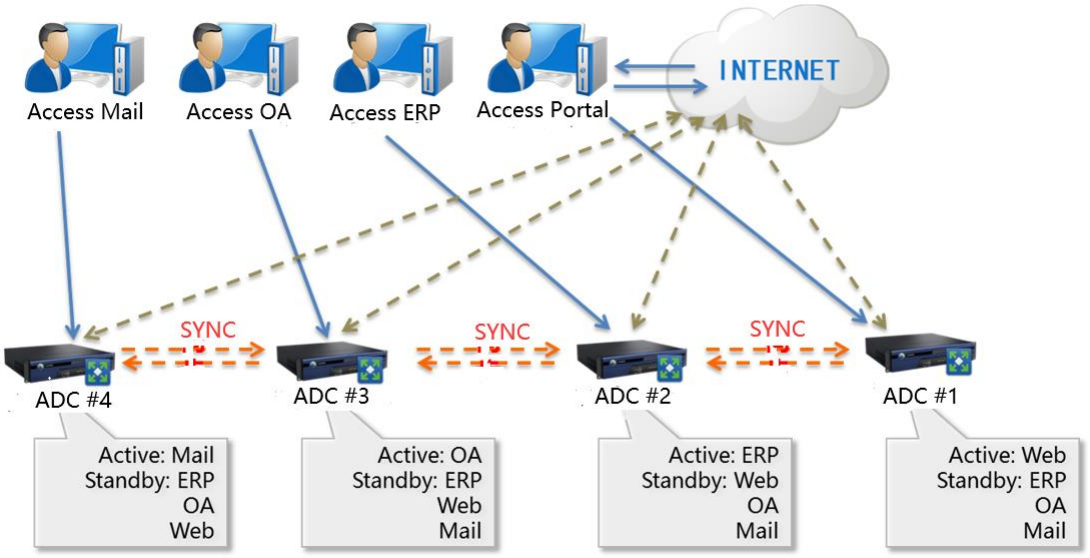
Multiple ADCs form a cluster. In this mode, the processing performance of the entire system can be improved, and each device in the cluster can be fully utilized to publish different services. In addition, devices can serve as backup devices for each other to ensure minimum service interruption when a failure occurs. That is to say, as long as one device is still available in the cluster, no service will be stopped. On this basis, a balanced failover and dynamic switching mechanism is implemented.

(1) Multiple ADCs form a high-availability cluster, supporting various modes such as active-standby, dual-active, multi-active, and M+N.

(2) Compared with the dual-device mode, the cluster mode provides higher redundancy (N+1 vs 1+1) and lower cost control (1+N vs 2×N).

3) ADCs serve as backup devices for each other, and the session mirror is synchronized, Avoiding service interruption during switchover.

See the figure below:

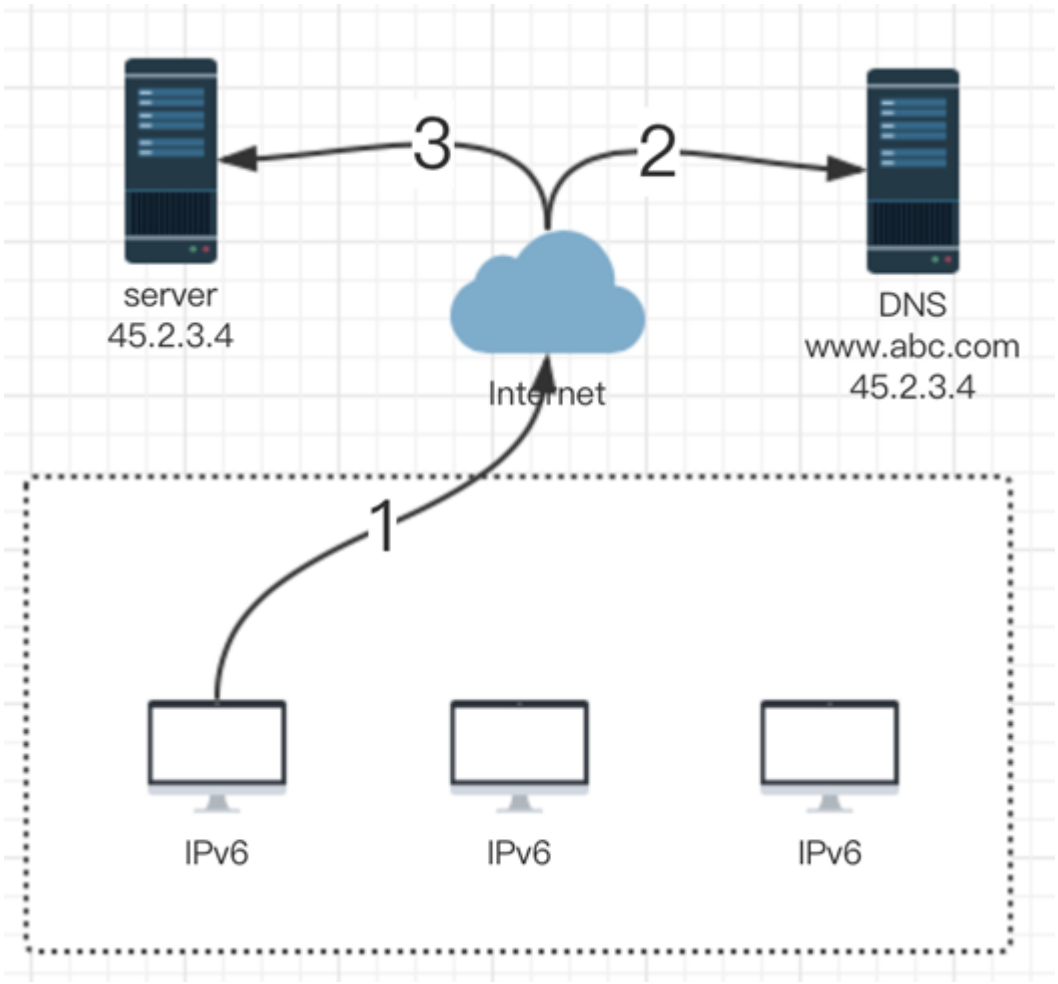


2.3.9 Full Support for IPv6

At present, the ADC product line fully supports IPv6, which can meet the needs of customers to facilitate the transitioning of internal/external networks from the IPv4 infrastructure to IPv6.

2.3.9.1 DNS64

Problem description: After the transition from IPv4 to IPv6 for an enterprise user's network is done, the PCs used by the internal employees of the enterprise are uniformly transformed into IPv6 gateways for outbound access to services. However, when a LAN user queries a portal on the Internet by using an IPv6 network segment, the portal has not yet undergone IPv6 transition and can only respond to requests from IPv4 business addresses, resulting in that the LAN user cannot access portals on the Internet normally by using IPv6 addresses. See the figure below:



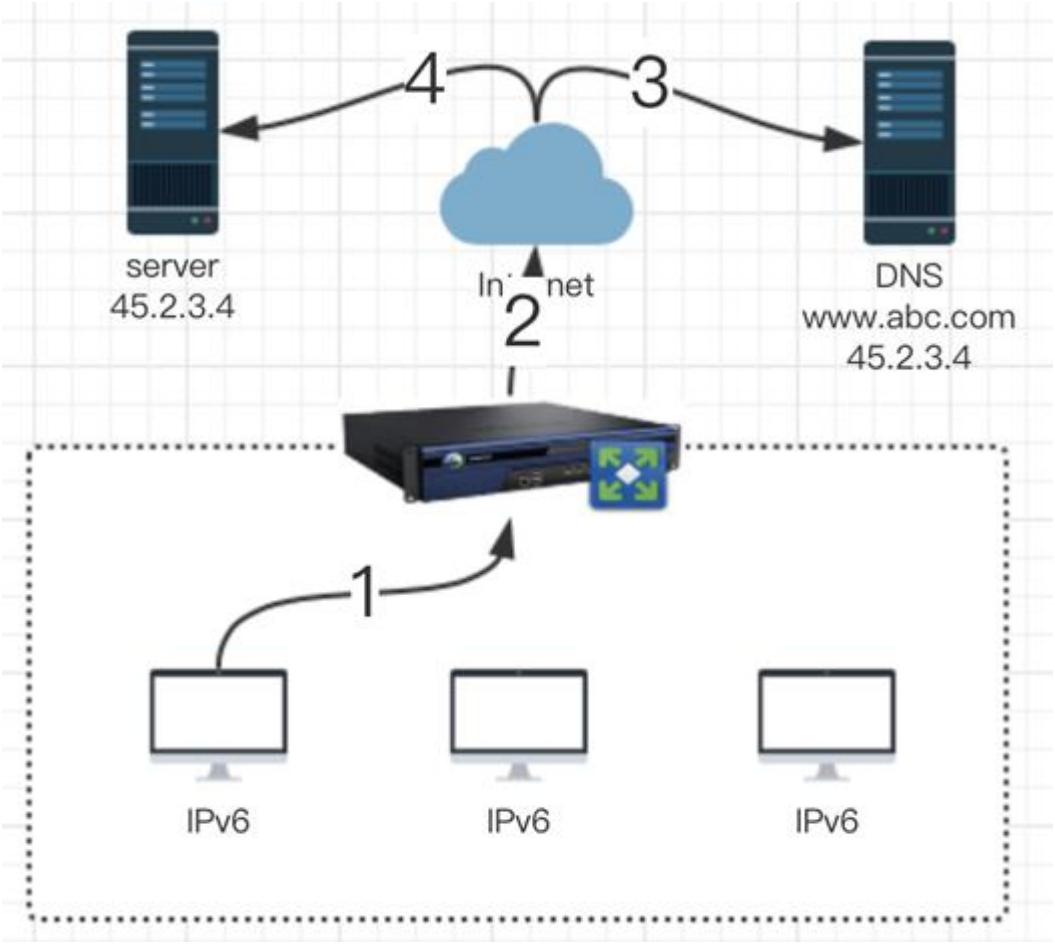
Access steps are as shown in the figure:

1. A LAN user needs to visit the www.abc.com business website on the Internet.

2. The LAN user sends an AAAA record query to the DNS server. However, www.abc.com does not implement IPv4-to-IPv6 transition, resulting in query timeout, or an A record 45.2.3.4 returned from the DNS server.

3. The LAN user cannot use IPv6 addresses to implement access shown as step 3 in the figure, and access to services is interrupted.

Sangfor load balancing solution:



1. A LAN user visits the business website www.abc.com on the Internet and issues an AAAA record query.

2. Sangfor load balancer receives AAAA and sends A & AAAA records to the DNS server.

3. Receive the DNS server response A record, 45.2.3.4. After receiving, Sangfor load balancer fills in an IPv6 address prefix to translate the IPv4 address to an IPv6 address, and then returns it to the client.

4. The LAN user accesses the server address using the IPv6 address. After processing by the Sangfor load balancer, the IPv6 prefix is stripped, and then the original IPv4 address is used for accessing services.

DNS64 is now completed.

Chapter 3 Deployment & Installation

3.1 Pre-operational Preparation

3.1.1 Environment Requirements

The ADC can be used in the following environments.

Input voltage: 110V-230V

Temperature: 0-45℃

Humidity: 5-90%

To ensure long-term and stable running of the system, please make sure that the power supply is well-grounded, dust-proof measures are taken, the working environment is well ventilated and the indoor temperature is stable. This product complies with the design requirements on environment protection. It shall be installed, used, and scrapped in accordance with provisions of relevant laws and regulations enforced by the country where it is applied.

3.1.2 Power Supply

SANGFOR ADC series products are supplied by 110V - 230V AC power. Ensure that the power supply is well-grounded before you turn on the power.

3.1.3 Product Appearance



Figure 1 ADC Gateway Panel (taking AD-1000-A800 as an example)

The indicators from left to right are described respectively as follows:

CONSOLE: connects with a monitor

USB: connects with a USB flash drive for restoring the password

MANAGE LINK: displays the cable connection status of the MANAGE interface

MANAGE ACT: displays the data traffic corresponding to the MANAGE interface

NET1 LINK: displays the cable connection status of the NET1 interface

NET1 ACT: displays the data traffic corresponding to the NET1 interface

NET2 LINK: displays the cable connection status of the NET2 interface

NET2 ACT: displays the data traffic corresponding to the NET2 interface

NET3 LINK: displays the cable connection status of the NET3 interface

NET3 ACT: displays the data traffic corresponding to the NET3 interface

The description of NET4, NET5, NET6, and NET7 interfaces is the same as above.

HA: dual-device deployment indicator

POWER: ADC power indicator

ALARM: ADC alarm indicator (stays on for one minute during device startup)

Notes: The picture is for reference only. The appearance of other products with different model numbers in this series is subject to the actual product.

3.1.4 Documentation and Tool Preparation

- ✓ The latest user manual
- ✓ Several RJ45 network cables
- ✓ Optical module (required if optical ports are used)
- ✓ One local Windows PC or one Apple computer

3.2 Device Installation

3.2.1 Configuration and Management

Before configuring the device, please confirm that the Web browser on the computer can be used normally (supporting IE7-IE11, Firefox, Google, and Safari (browser on Apple devices)), and then connect the computer and the SANGFOR ADC to the same local area network. Configure the device via the network.

3.2.2 Wiring Method

Plug the power cable into the rear panel of the device, and then press the power button. At this time, the Power indicator light (green) and the Alarm indicator light (red) on the front panel will be on. The Alarm indicator light will go out in one or two minutes, indicating the device is working properly.

Please use a standard RJ-45 Ethernet cable to connect the networking interface defined as the LAN interface to the LAN.

Notes:

(1) If no network interface has been defined, connect to the MANAGE interface before entering the WEBUI. After defining a network interface, the SANGFOR ADC console can be accessed through the interface.

(2) The POWER light is staying on during the normal operation of the ADC, and the red ALARM indicator light is only staying on (for about one minute) during device startup due to system booting, **and it is off during normal system operation.** If the red indicator light stays on during installation, please switch off the power supply and reboot the device. If the red light is still staying on after the reboot, please contact Sangfor's technical support engineers as soon as

possible.

3.3 Network

When deploying an ADC in a network, no matter which deployment mode is adopted, it is generally connected to the core. The interface through which the ADC is connected with the core can be an ordinary network interface, aggregate interface (hash, round-robin, 802.3ad, redundant dual network cards), port bridging, or VLAN subinterface. If the internal network supports dynamic routing or static routing, the ADC supports dynamic (OSPF, BGP, RIP) routing or static routing accordingly. These modes are described below:

3.3.1 Interface IP

【Operation Scenarios】

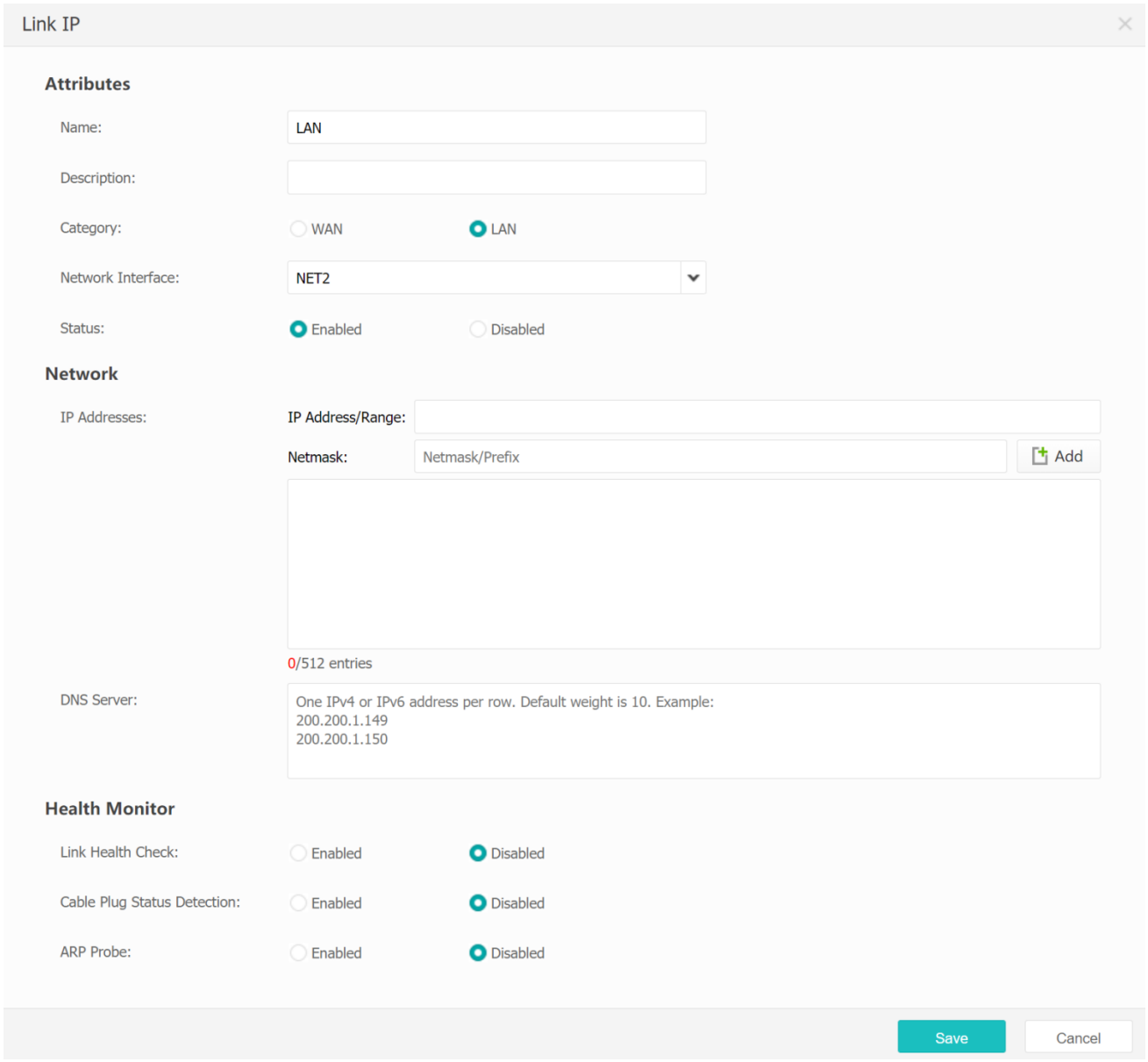
The interface used to connect with the ADC is an ordinary network interface (electrical or optical interface), and the interface used by the ADC is an ordinary network interface (internal or external network interface) as well.

1. Internal network interface: The LAN attribute interface, which is required when deploying a gateway.

2. External network interface: The WAN attribute port. Generally, no matter what deployment mode the ADC adopts, the WAN attribute interface is required for publishing or undertaking services.

【Operation Procedure】

1. Internal network interface: Choose『Network』-『Network Interface』-『Interface IP』and click New. Configure Name, Category, Network Interface, Network, Health Monitor, etc. to complete the configuration of a LAN interface, as shown in the following figure:



『Category』: selects the type of new network interface. Select attribute LAN for internal network interfaces.

『Network Interface』: selects a network interface. Ordinary network interface, aggregate network interface, bridging network interface and VLAN subinterface are available for selection according to specific needs.

『IP Addresses』: defines the IP address bound with the network interface, supporting mixed use of IPv4 and IPv6 addresses.

『Link Health Check』: enables or disables health status monitoring of LAN interface, only supporting IPV4 addresses.

『Monitor』: selects the monitor that needs to be enabled, generally including ping, http, etc. by default. It can be configured under『Network』-『Link Health Check』according to needs. The configuration is similar to that of the Health Monitor under App Load Balancing and Global Load Balancing.

『Monitoring Host』: types in the host to be monitored. Either an IP address or a domain name can be added. Generally fill in the gateway of the link.

『Cable Plug Status Detection』: judges the health status of a LAN interface by detecting whether a network cable is plugged into it.

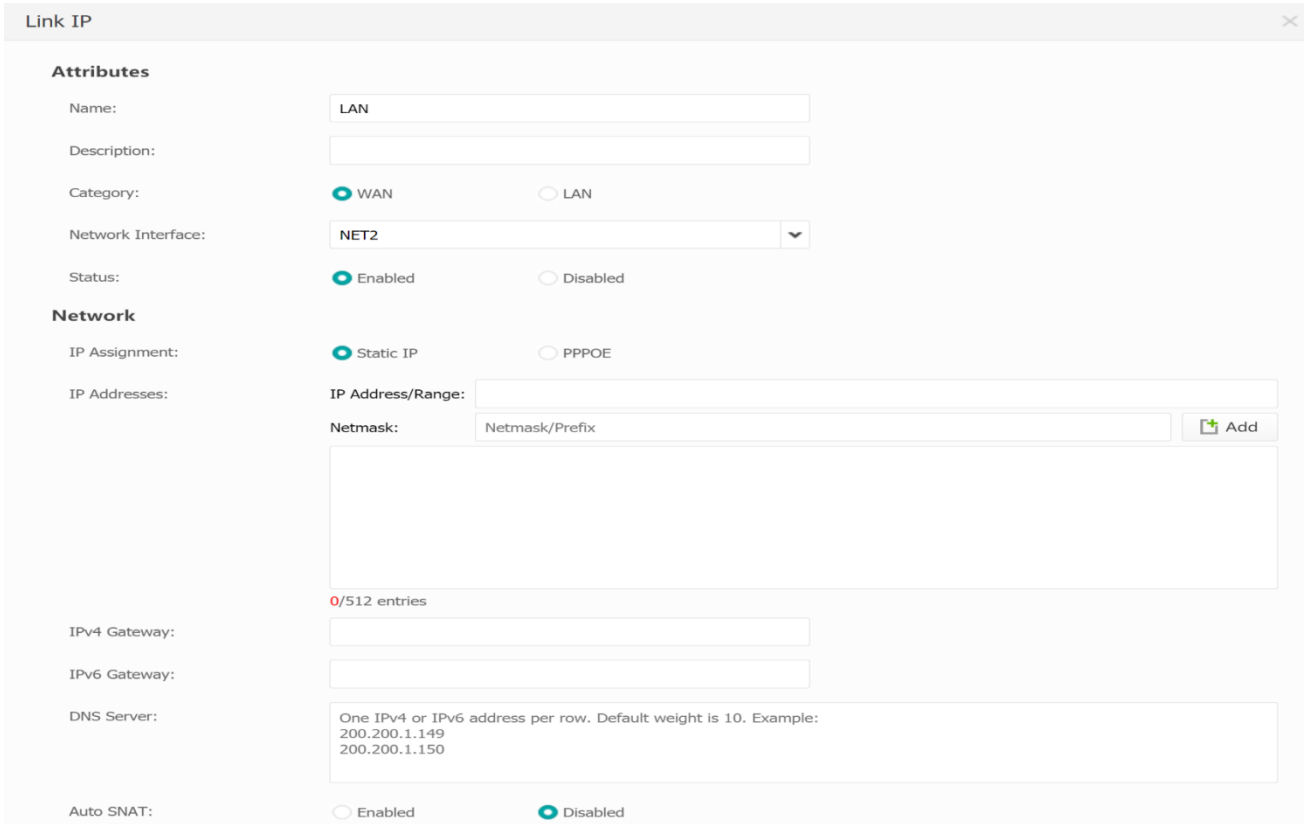
『ARP Probe』: obtains the ARP address of the IP being monitored to judge the health status of a LAN interface.

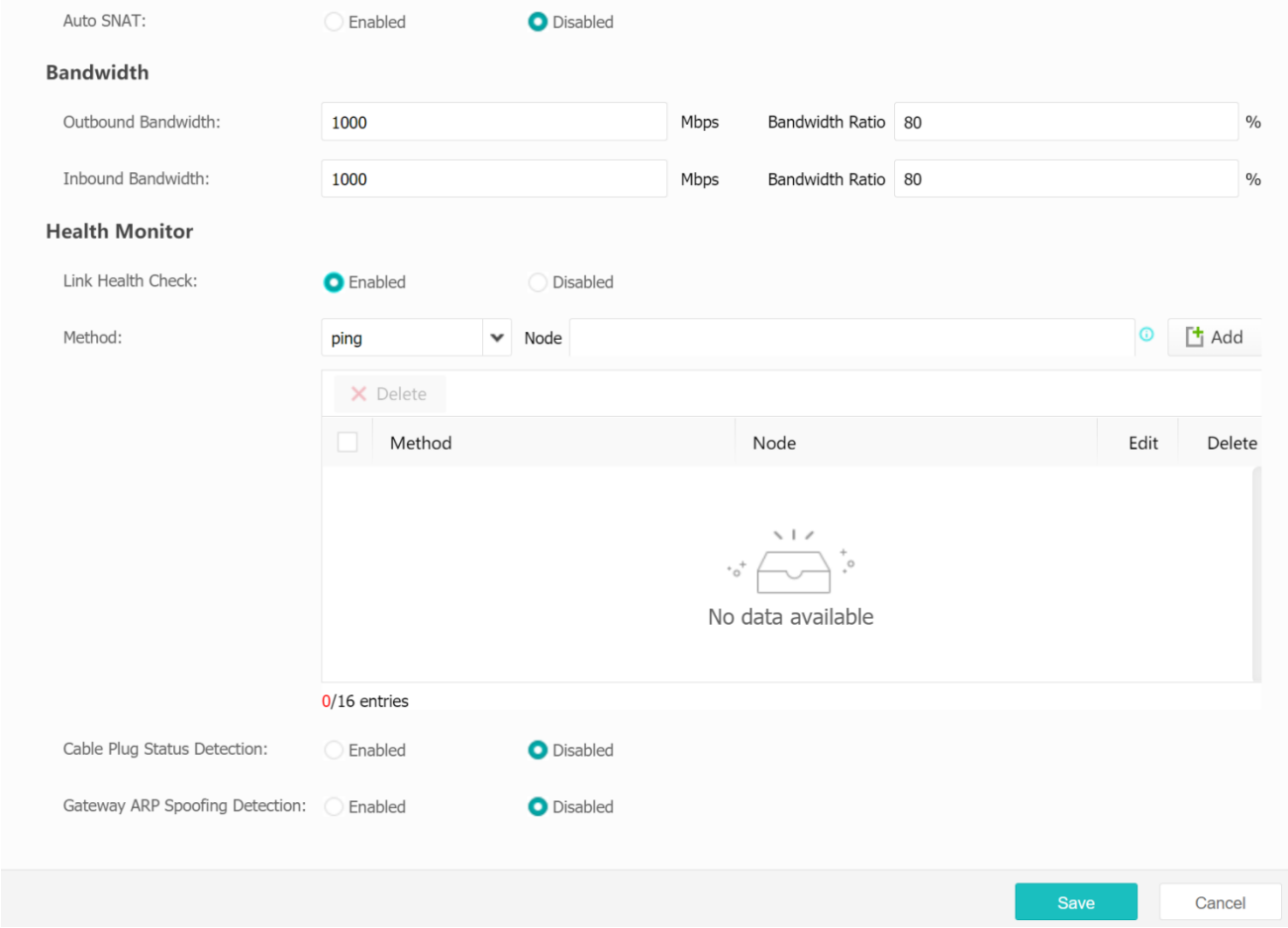
For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『DNS』: configures the DNS server for the interface. The configuration is the same as that under『Link Load Balancing』-『DNS Proxy』-『Global Configuration』-『DNS Server List』. That is to say, a DNS server can be configured when defining the interface, or it can be configured separately under『DNS Server List』.

『Application Group Failover』: switches the application groups of non-common projects in a cluster-multi-tenant mode. When this function is enabled and the link is offline due to PING, ARP, or network interface disconnected, the associated application group will be switched.

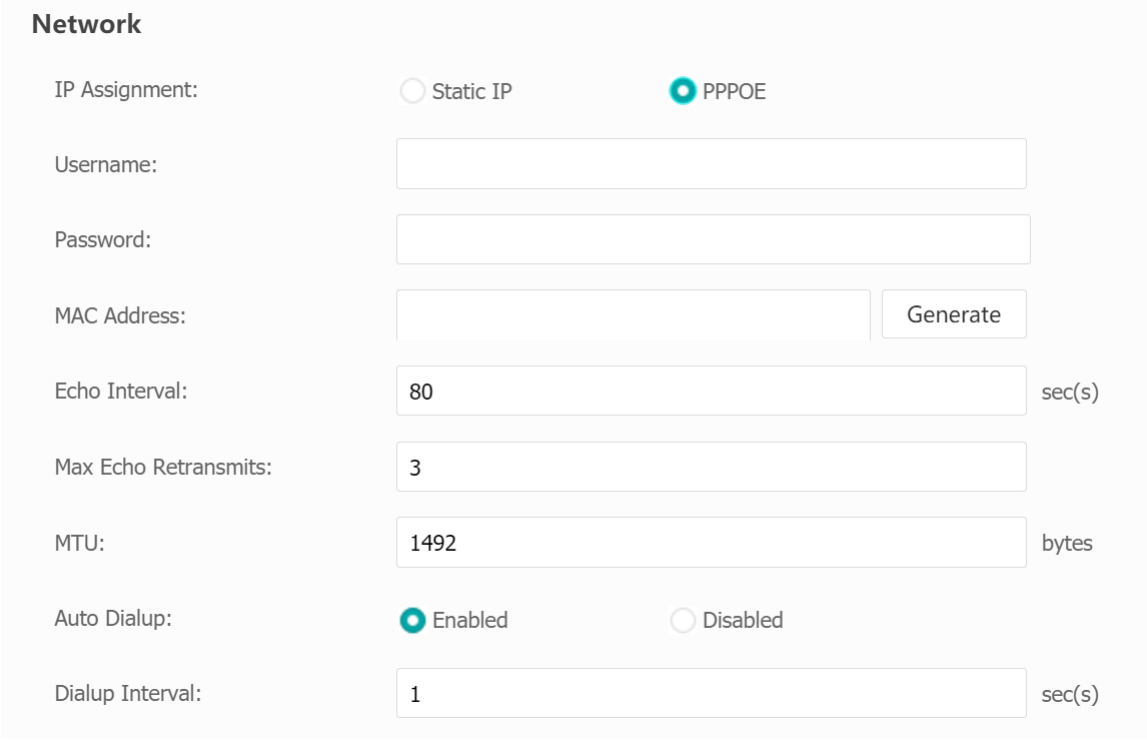
2. External network interface: Choose『Network』-『Network Interface』- 『Link IP』and click New. Configure Name, Category, Network Interface, Network (IP Assignment and IP Addresses), Gateway, Bandwidth, Health Monitor, etc. to complete the configuration of a WAN interface, as shown in the following figure: (Part of the configuration is similar to that of the LAN interface. Differences in configuring WAN and LAN interfaces are explained below)





『IP Assignment』: selects Static IP or PPPOE dial-up for WAN interface.

(1) [Static IP]: directly configures the IP address list and gateway.
(2) For [PPPOE], configure Username, Password, Enabled for Auto Dialup, etc. to complete PPPoE dial-up settings. It is suggested to keep other parameters as default, as shown in the following figure:



『Bandwidth』: sets the bandwidth and heavy load protection ratio of the external line, that is, when the amount of traffic on this line accounts for a certain percentage of the total lines, the heavy load protection will be enabled so that the line will no longer participate in scheduling, so as to prevent this line from being occupied completely.

For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『Auto SNAT』: sets network address translation for the WAN interface. It is the same function as the Source Network Address Translation newly added under【Network Interface】-【SNAT】, but a manually configured SNAT has a higher priority than the automatically generated one.

3.3.2 Aggregate Interface

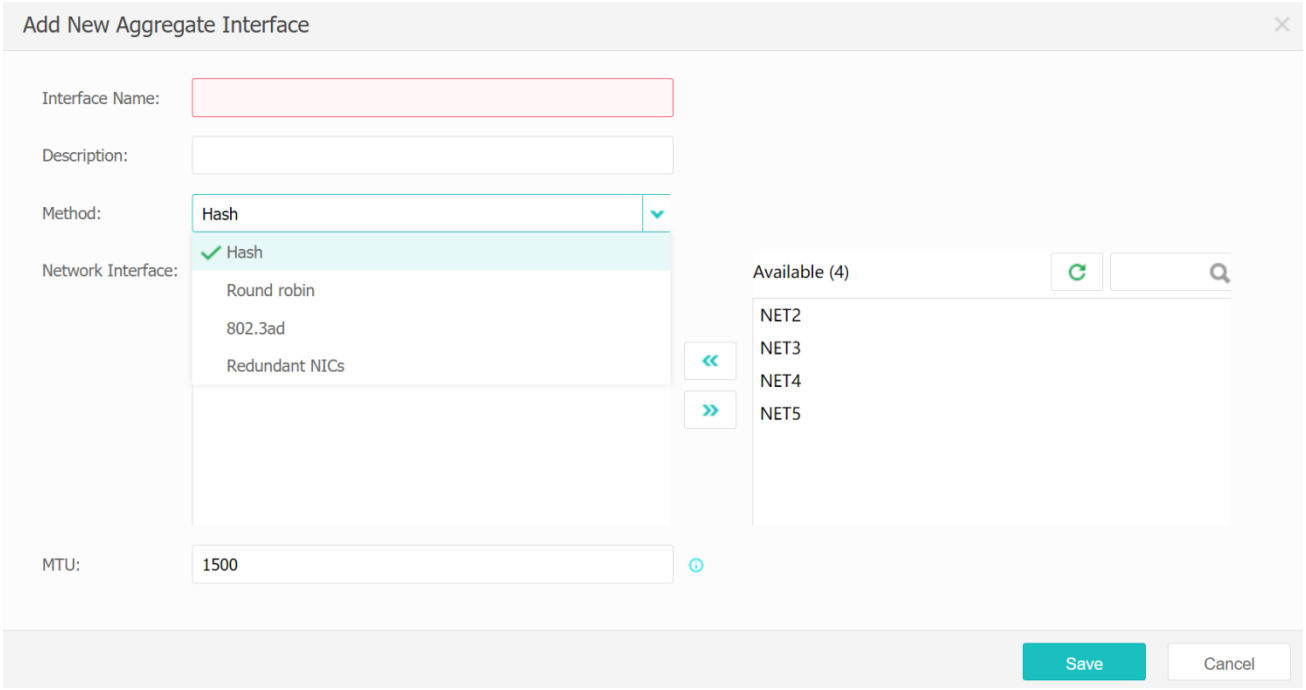
【Operation Scenarios】

Combine multiple physical interfaces on the ADC to form a single logical interface, which allows multiple ports to be connected in parallel to transmit data synchronously, providing higher bandwidth and throughput. Generally, when the interface used by the device for connecting with the ADC is an aggregate interface (electrical interface aggregation or optical interface aggregation), the ADC uses an aggregate interface as well (internal or external network interface). Interface

aggregation methods include Hash, Round robin, 802.3ad, and Redundant NICs. The specific one used should be consistent with the aggregation protocol used by the peer device. Hash and 802.3ad are more commonly used.

【Operational Deployment】

1. Create an aggregate interface. Choose『Network』-『Network Interface』-『Aggregate Interface』 and click New. Configure Interface Name, Method, Network Interface, etc. to complete aggregate interface configuration, as shown in the figure below:



『Method』 sets the working mode of interface aggregation, including Hash, Round robin, 802.3ad, and Redundant NICs.

(1) [Hash] calculates a hash value based on source IP address and destination IP address to select the corresponding interface.

(2) [Round robin] sends packets in a packet-by-packet round robin fashion to corresponding interfaces.

(3) [802.3ad] automatically selects the link with the highest bandwidth as the active link, and the rest are the backup links. If the bandwidth of all links is the same, the Hash method is used to send data.

(4) [Redundant Dual Network Cards] binds multiple physical network interfaces together to create a logical interface, with only one physical network interface in a working state. When the main network interface goes down, the back-up one is switched to serve as the main network interface to continue working.

Notes: Hashes and 802.3ad are most commonly used. If the peer device is in static mode, Hashing is recommended; if the peer device is in dynamic LACP mode, 802.3ad is recommended.

『Network Interface』 selects network interfaces for being bonded together. In general, the number of network interfaces to be selected for bonding on ADC is depending on that of the ones bonded on the peer device.

2. Create LAN or WAN interfaces.

For details, refer to the creation steps for [Ordinary Network Interface].

3.3.3 Bridge Interface

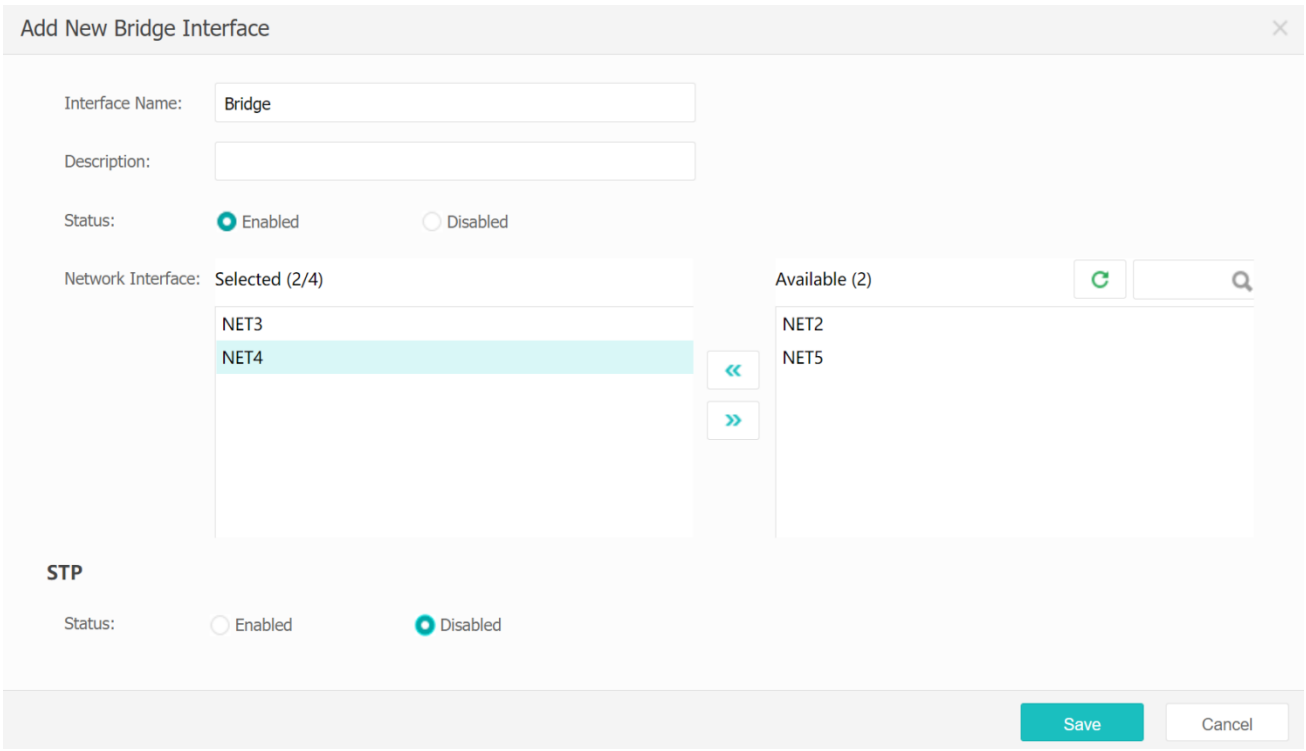
【Operation Scenarios】

It is generally used to logically combine multiple network interfaces of an ADC together into an interface of a Layer 2 switch, where each network interface of the AD can be dealt with as an interface of a Layer 2 switch.

It is mainly used for load balancing through the NGAF device behind ADC when the ADC is deployed under the network egress. The dual-machine hot standby function of firewalls is enabled to ensure the high availability and reliability of the network, that is, two firewalls with the same configuration are used on the same network node. Here, without adding redundant network nodes (such as switches), using the network interface switching function of ADC can solve the problems that occur in dynamic switching between the active and standby firewalls and realize the interconnection of ADC and firewalls as well as that of firewalls.

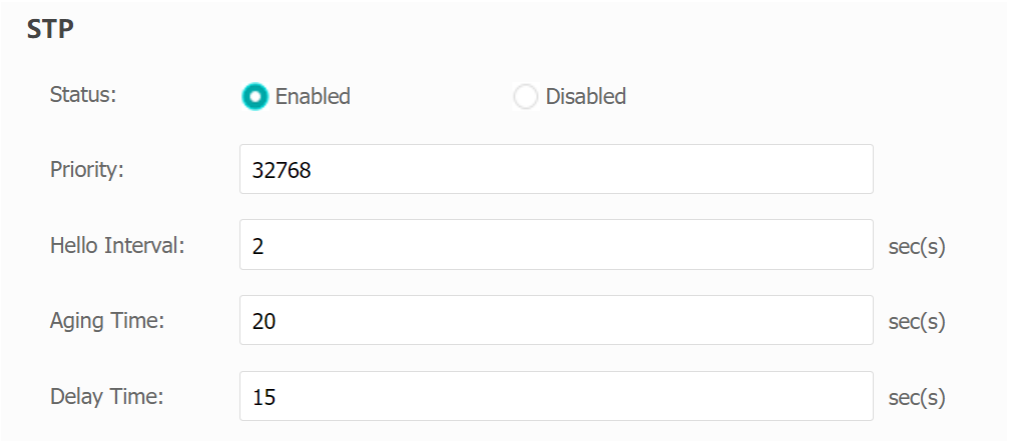
【Operation Procedure】

1. Create a bridge interface. Choose『Network』-『Network Interface』- 『Bridge Interface』and click New. Configure Interface Name, Network Interface, etc. to complete bridge interface configuration, as shown in the figure below:



『Network Interface』 selects the network interfaces for current switching from idle ordinary network interfaces, aggregate interfaces, or VLAN subinterfaces.

『STP』 sets parameters, including but not limited to [Priority], [Hollo Interval], [Aging Time], and [Delay Time]. After clicking Enabled, the default interface is shown as follows:



『Status』 enables or disables the STP protocol for the switch network interface.

『Priority』 sets the protocol priority. The lower the Priority value, the greater the chance of becoming a root bridge.

『Hello Interval』 sets the time interval for the switch network interface to send BPDUs. The BPDUs sent will be forwarded by the receiving switch/bridge.

『Aging Time』 sets the waiting time for the switch network interface to determine topology changes. Usually, the value is a multiple of the Hello Interval.

『Delay Time』 sets the latency for the interface to transit from a blocking state to a forwarding state.

2. Create LAN or WAN interfaces.

For details, refer to the creation steps for [Ordinary Network Interface].

Attention: 4 interfaces can be selected at most for 1 bridge interface.

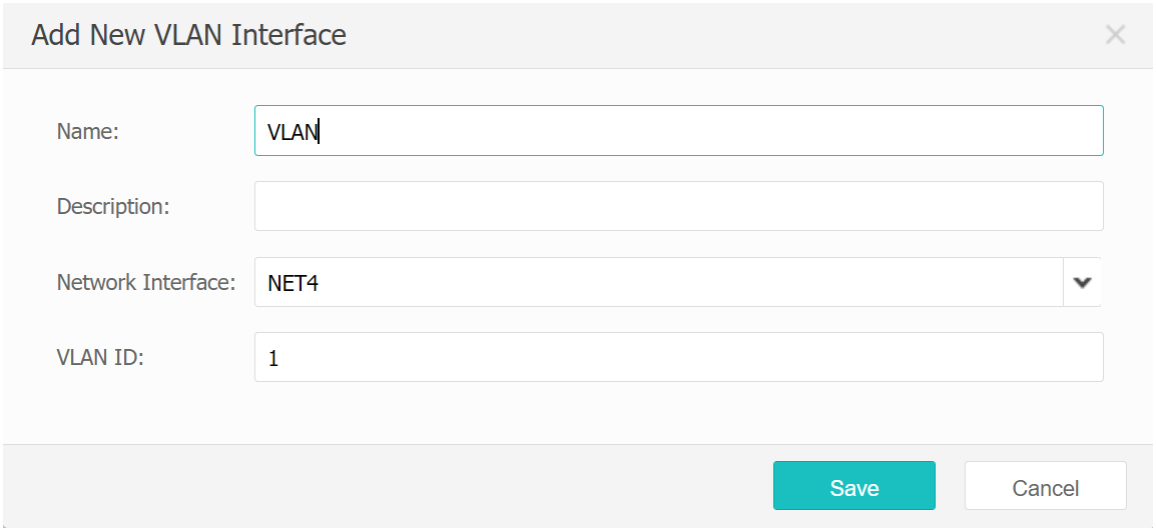
3.3.4 VLAN Interface

【Operation Scenarios】

It is generally used to logically divide a network interface on the ADC into several virtual subinterfaces, so as to realize a virtual workgroup. In general, if VLAN is enabled on the device connected with ADC, it is necessary to enable VLAN on ADC accordingly.

【Operation Procedure】

1. Create a VLAN interface. Choose『Network』-『Network Interface』- 『VLAN Interface』and click New. Configure Interface Name, Network Interface, VLAN ID, etc. to complete VLAN subinterface configuration, as shown in the figure below:



『Network Interface』: selects the physical device interface to be divided from idle ordinary network interfaces and aggregate interfaces.

『Vlan ID』: sets a VLAN ID uniquely identifying the VLAN supported by a designated network interface.

2. Create LAN or WAN interfaces.

For details, refer to the creation steps for [Ordinary Network Interface].

Attention: The sequence of ordinary network interface, aggregate interface, VLAN subinterface, and switch interface, that is, reference relationship: ordinary < aggregate < VLAN < switch.

3.3.5 NAT

【Operation Scenarios】

Network Address Translation is divided into Source Network Address Translation (SNAT) and Destination Network Address Translation (DNAT). In general, this module needs to be configured when a certain IP address (segment) needs to be translated to a different IP address. The introduction to SNAT and DNAT is as follows:

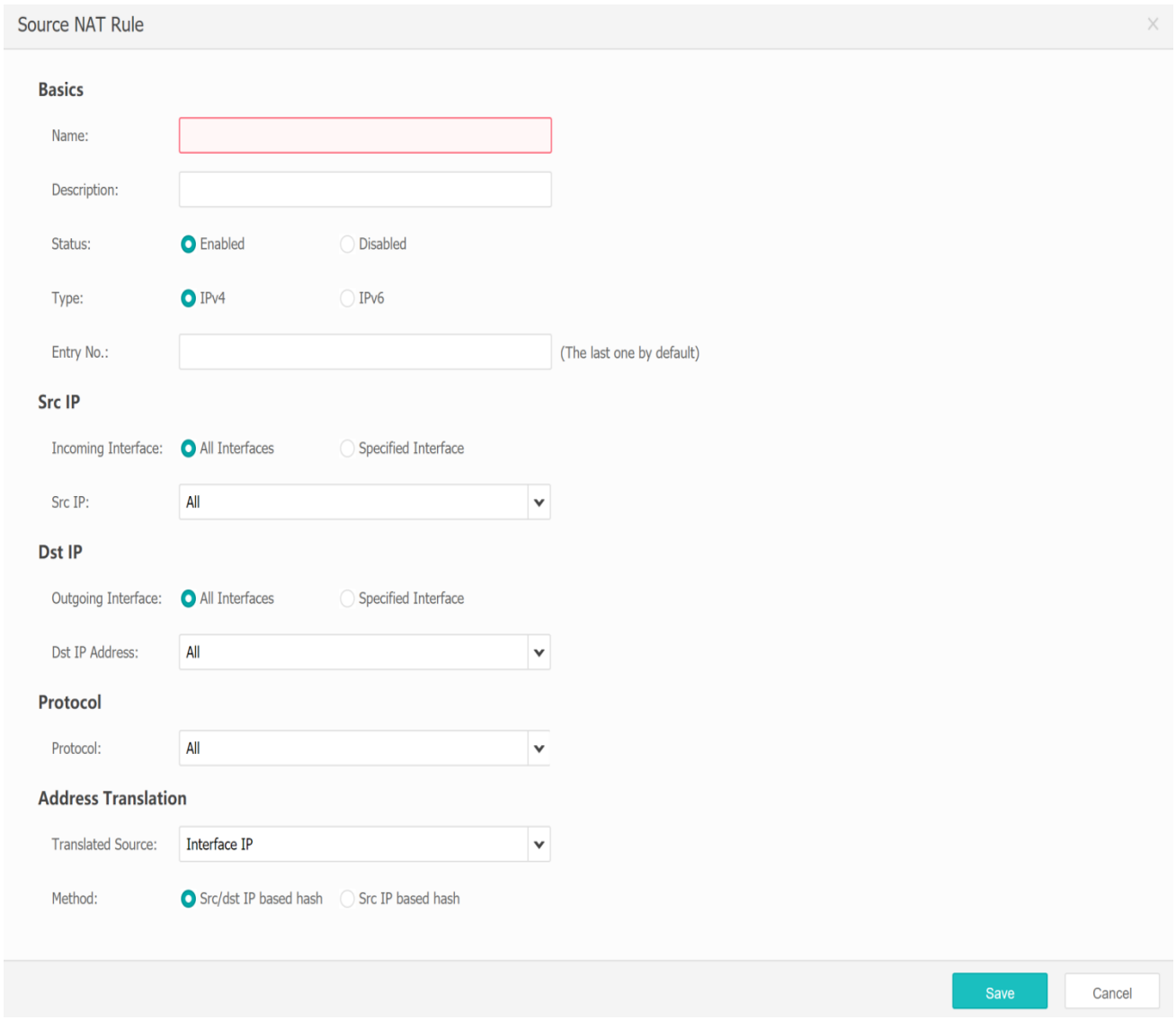
3.3.5.1 Source NAT Rule(SNAT)

【Operation Scenarios】

The source IP address of the data needs to be translated to another IP address by ADC. For example, when deploying a gateway, the LAN IP address needs to be translated to an external network IP address for Internet access. In this case, the SNAT is required.

【Operation Procedure】

1. Create a source NAT rule. Choose『Network』-『NAT』- 『Source NAT Rule』and click New. Configure Name, Type, Src IP, Dst IP, Protocol, Address Translation, etc., as shown in the figure below:



『Type』: selects IPv4 or IPv6 for network address translation as needed. In general, SNAT66 or SNAT44 is implemented. If SNAT64 is required, it needs to be implemented in combination with the DNS proxy called DNS64. For details, please refer to the settings of DNS proxy in Section 8.2.1.

『Src IP』: sets the link for the incoming source IP address and the range of source IP addresses according to the needs of the LAN. If the LAN SNAT is required, only a LAN link needs to be selected. If the IP address translation is required for all sources, all interfaces can be selected. For example, if you want to translate the source of data mapped from a port, the external network link can also be selected.

『Dst IP』: the IP address to be translated from a source IP address. In general, select all links and all IP addresses. If a separate outgoing interface is specified, you can select the specified link, for example, to send the source IP address for a LAN user via a China Telecom link, just select the specified link. Dst IP Address: To implement matching translation when accessing a certain destination IP address (segment), just select according to needs.

『Protocol』: in general, select ALL. If necessary, select an appropriate protocol for translation, for example, indicating to map a certain TCP port.

『Address Translation』: in general, select the IP address of the outgoing interface or the specified IP address. If the source IP address needs to be translated into a dedicated IP address (segment), select it according to needs. Method: Generally, select the Src/Dst IP based hash, and the interpretation is as follows:

[Src/Dst IP based hash]: according to the source IP address and destination IP address for this access, perform a hashing calculation to select the destination IP address for translation. This method works for most cases.

[Src IP based hash]: performs a hashing calculation based on the source IP address for this access to select the destination IP address for translation. This scenario generally occurs when accessing online banking services. The user's access to online banking may involve multiple destination IP addresses. In this case, the source IP-based hashing is used to ensure that the translated IP address remains unchanged.

3.3.5.2 Destination NAT Rule(DNAT)

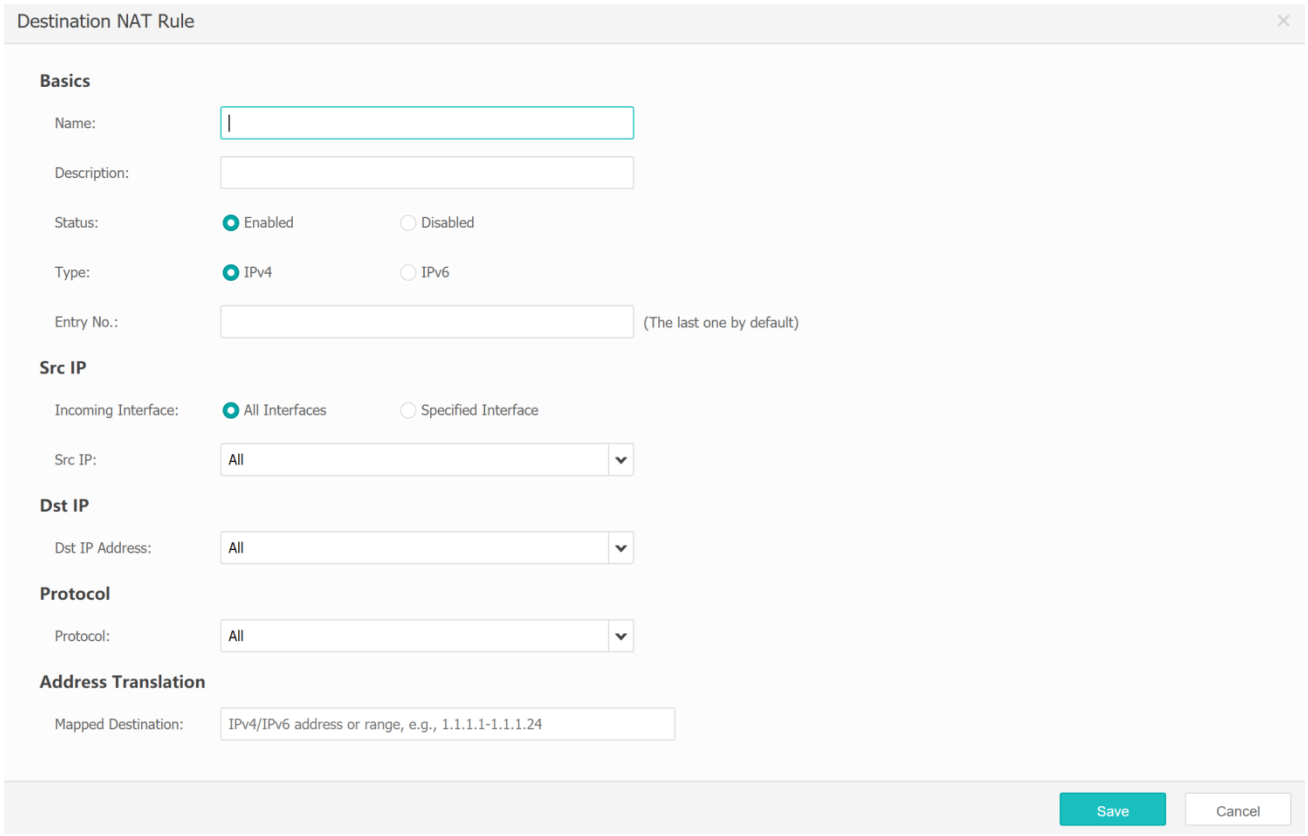
【Operation Scenarios】

This is generally used to make an internal network server (a private IP address) publicly accessible on the Internet (external network IP addresses) so that users on external networks can access service by using external network addresses.

【Operation Procedure】

1. Create a Destination NAT Rule. Choose『Network』-『NAT』-『Destination NAT Rule』

and click New. Configure Name, Type, Src IP, Dst IP, Protocol, Address Translation, etc., as shown in the figure below:

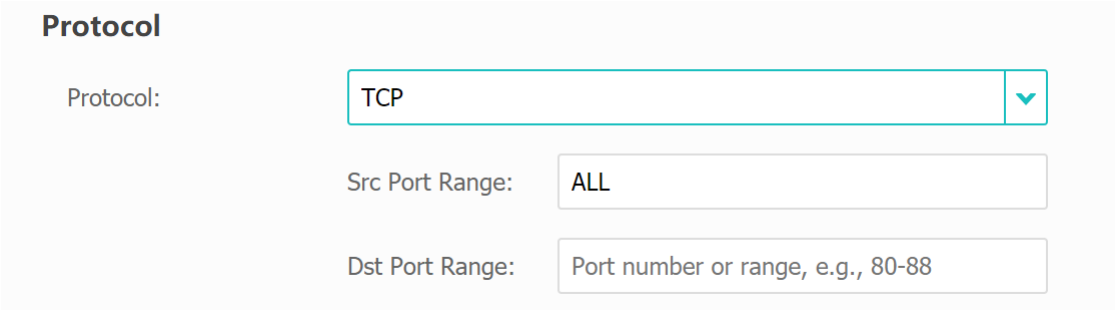


『Type』: selects IPv4 or IPv6 for network address translation as needed. In general, DNAT66 or DNAT44 is implemented. If DNAT64 or DNAT46 is to be implemented, a Layer 4 app load balancing is required. For specific configuration, please refer to Section 7.1.

『Src IP』: sets the link for the incoming source IP address and the range of source IP addresses as needed. In general, select external network links and all IP addresses. For example, to make the external users' access match this rule.

『Dst IP』: sets the destination IP address matching this rule as needed. In general, select the designated external IP address. For example, if an internal IP address needs to be mapped to the external IP address 2.2.2.2, then this field must be filled out with 2.2.2.2. This rule will be matched when users on external networks access 2.2.2.2.

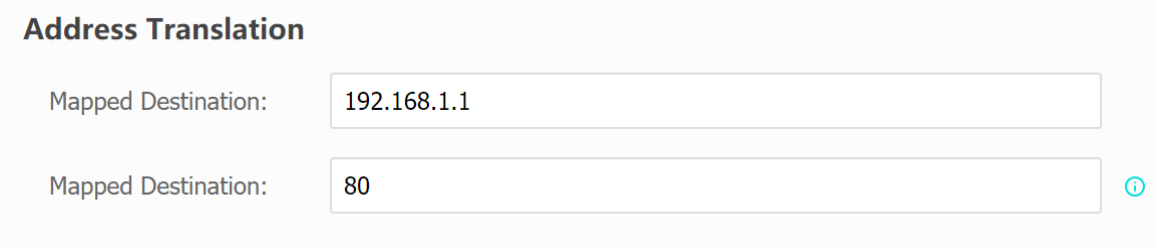
『Protocol』: in general, select a specific port. For example, if an internal IP address needs to be mapped to the external IP address 2.2.2.2, port (TCP) 8080, select the TCP protocol here as shown in the following figure:



Src Port Range: in general, select ALL. It needs to be specified under special circumstances, such as restricting source ports that the user can access.

Dst Port Range: 8080.

『Address Translation』: fill out with the IP address and port to be translated/mapped. For example, if port 80 (192.168.1.1) needs to be mapped to the external network address 2.2.2.2, port 8080, then the 2 fields should be filled out as follows:



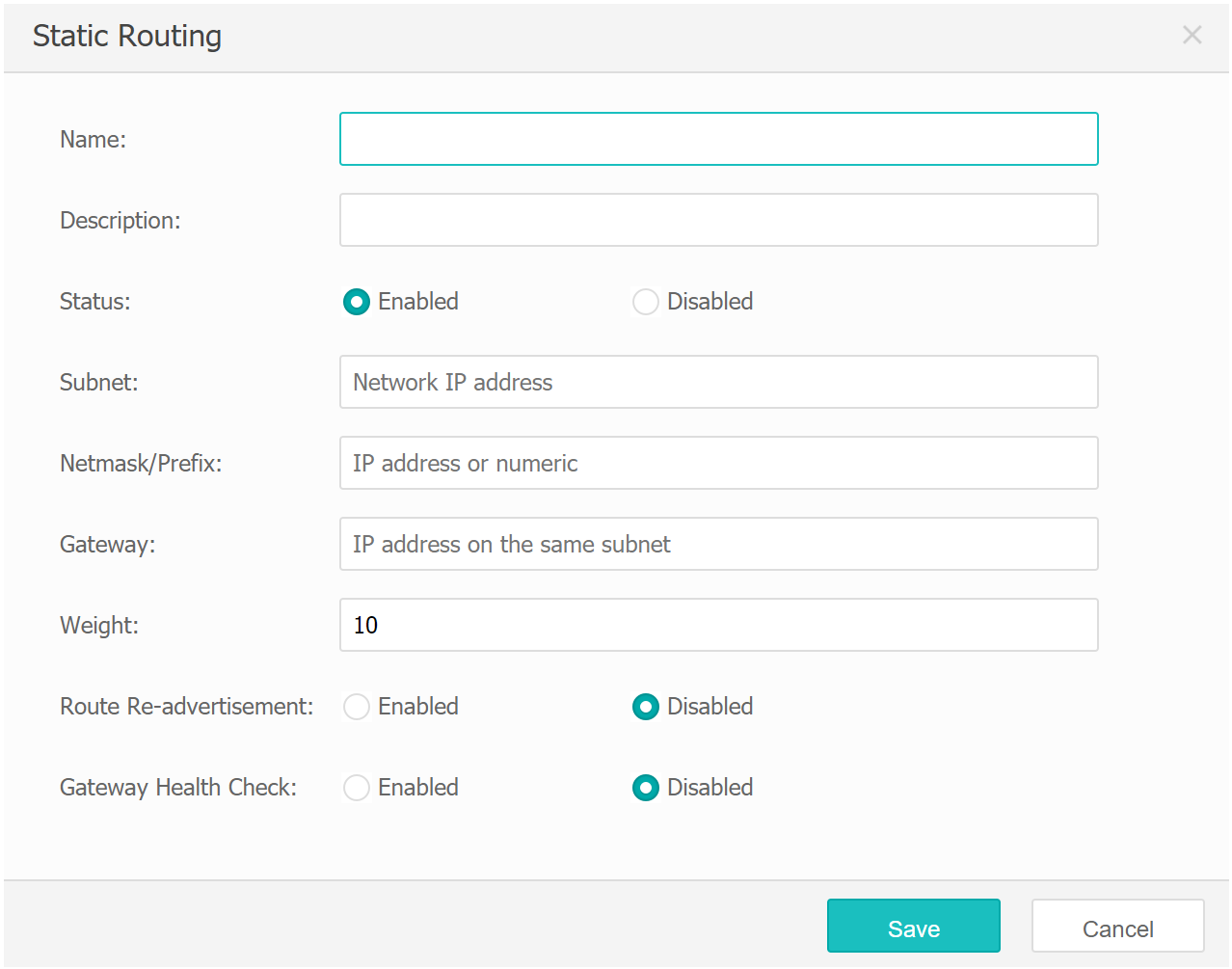
3.3.6 Static Routing

【Operation Scenarios】

Static Routing is generally used to set up routes to network segments that non-directly connected with the ADC. Scenarios supported by internal networks are realizing intercommunication between different network segments through static routing.

【Operation Procedure】

1. Choose『Network』-『Static Routing』and click New. Configure Name, Subnet, Netmask/Prefix, Gateway, Gateway Health Check, etc. to complete static routing configuration, as shown in the figure below:

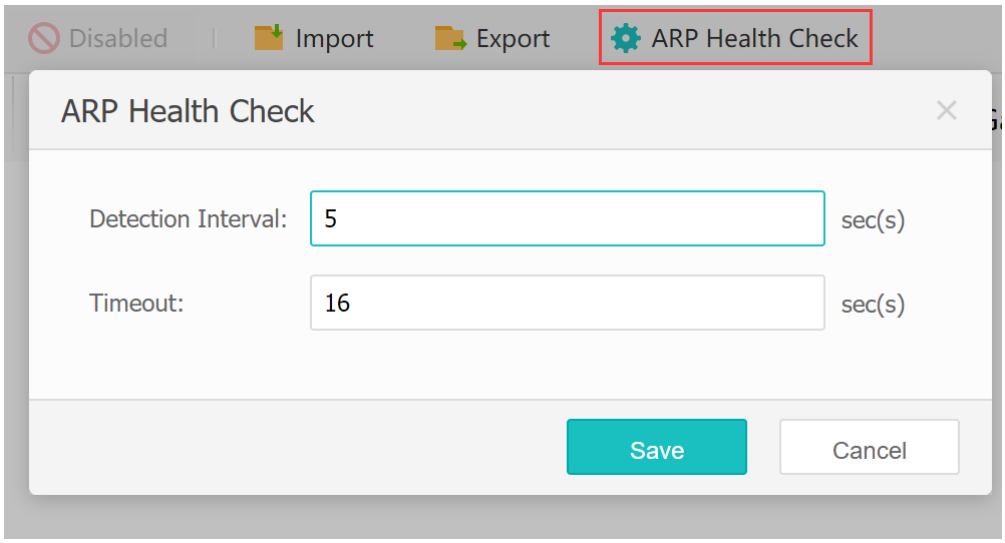


『Subnet』: sets the destination network segment.

『Netmask/Prefix』: sets the subnet mask for the destination network segment.

『Gateway』: sets the next hop's IP address to reach the destination network segment.

『Gateway Health Check』: monitors the gateway by means of ARP to judge the link quality. It is recommended to be enabled. The setting parameters are shown in the following figure:



For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『Weight』 applys to multipath routing (i.e. the destination network segment is the same but there are multiple gateways), where a path with a higher weight is preferred for data forwarding. If the weight of multiple paths is the same, the gateway selection should be performed by using a hashing algorithm to achieve equal-cost load balancing.

『Route Re-advertisement』 sets whether to allow the current static routing entry to be advertised through the dynamic routing protocol. When the destination network segment is an IPv6 address, this item is not configurable.

3.3.7 Dynamic Routing

【Operation Scenarios】

It is generally used in the scenario supported by internal networks to realize intercommunication between different network segments through dynamic routing. ADC supports OSPF, BGP, OSPFV3, and RIP. The specific dynamic routing protocol to be used shall be determined according to the specific dynamic routing protocol running on the internal network. The details are as follows:

3.3.7.1 OSPF

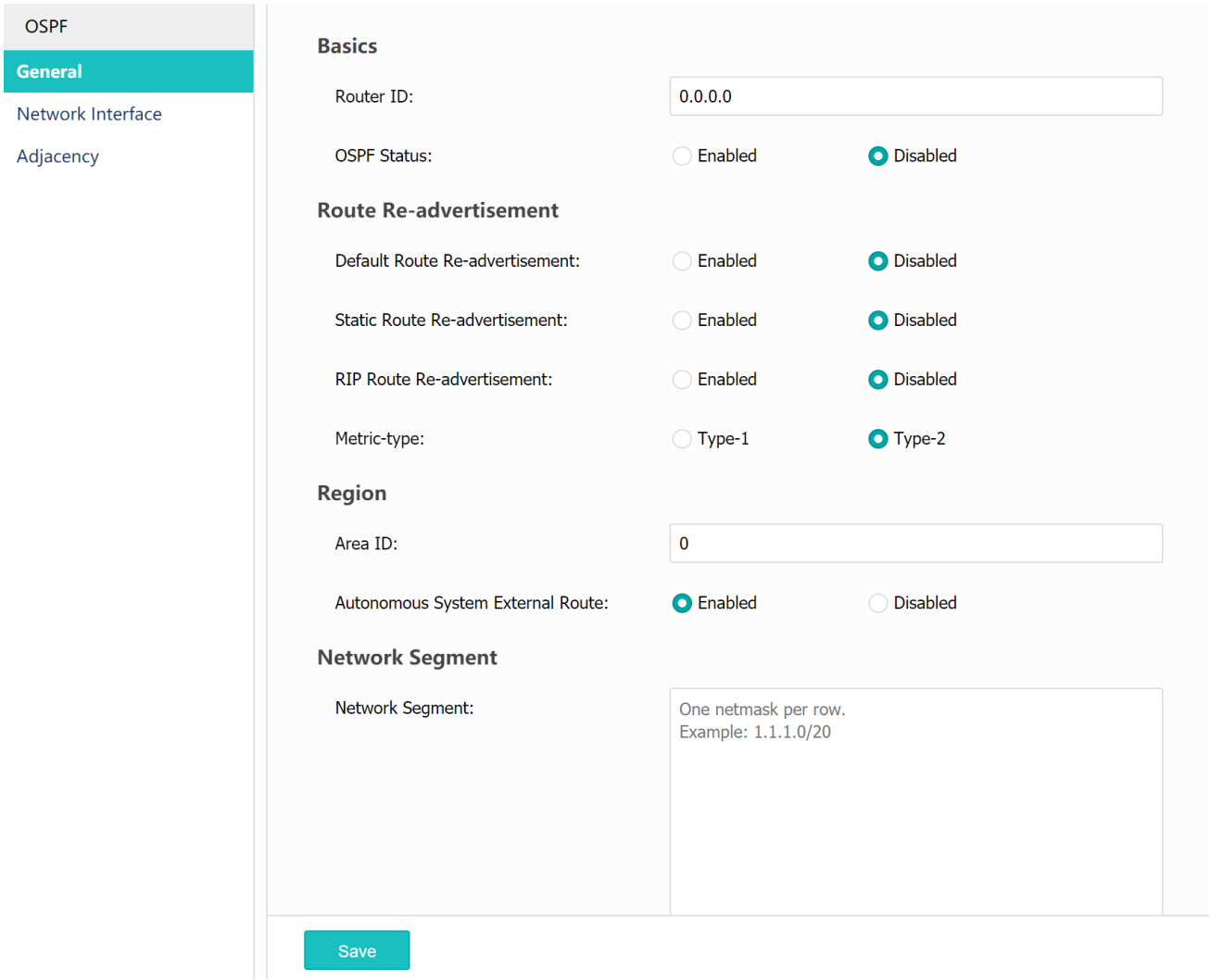
【Operation Scenarios】

Configure the network that the ADC needs to advertise through the OSPF routing protocol. Support the deployment of the ADC in an environment that uses the OSPF routing protocol.

【Operation Procedure】

Navigate through『Network』-『Dynamic Routing』-『OSPF』to complete the configuration of OSPF by configuring [General] and [Network Interface]. [Adjacency] lists routes learned by OSPF. The specific configuration is as follows:

1. General: sets the Router ID, Default Route Re-advertisement, Static Route Re-advertisement, RIP Route Re-advertisement, Metric-type, Autonomous System External Route, Network Segment, etc. to complete the general configuration, as shown in the following figure:



『Router ID』allows you to complete the field with information that is easy to remember to identify the identity of the router. The ID should be represented with numbers （1-4,294,967,295）or using dot-decimal notation.

『Default Route Re-advertisement』sets whether to allow the OSPF to broadcast the default route, making adjacent routers direct default routes to the ADC.

『Static Route Re-advertisement』sets whether to allow the OSPF to broadcast the static route configured on the device.

『RIP Route Re-advertisement』sets whether to allow the OSPF to broadcast the RIP routing information learned by the device.

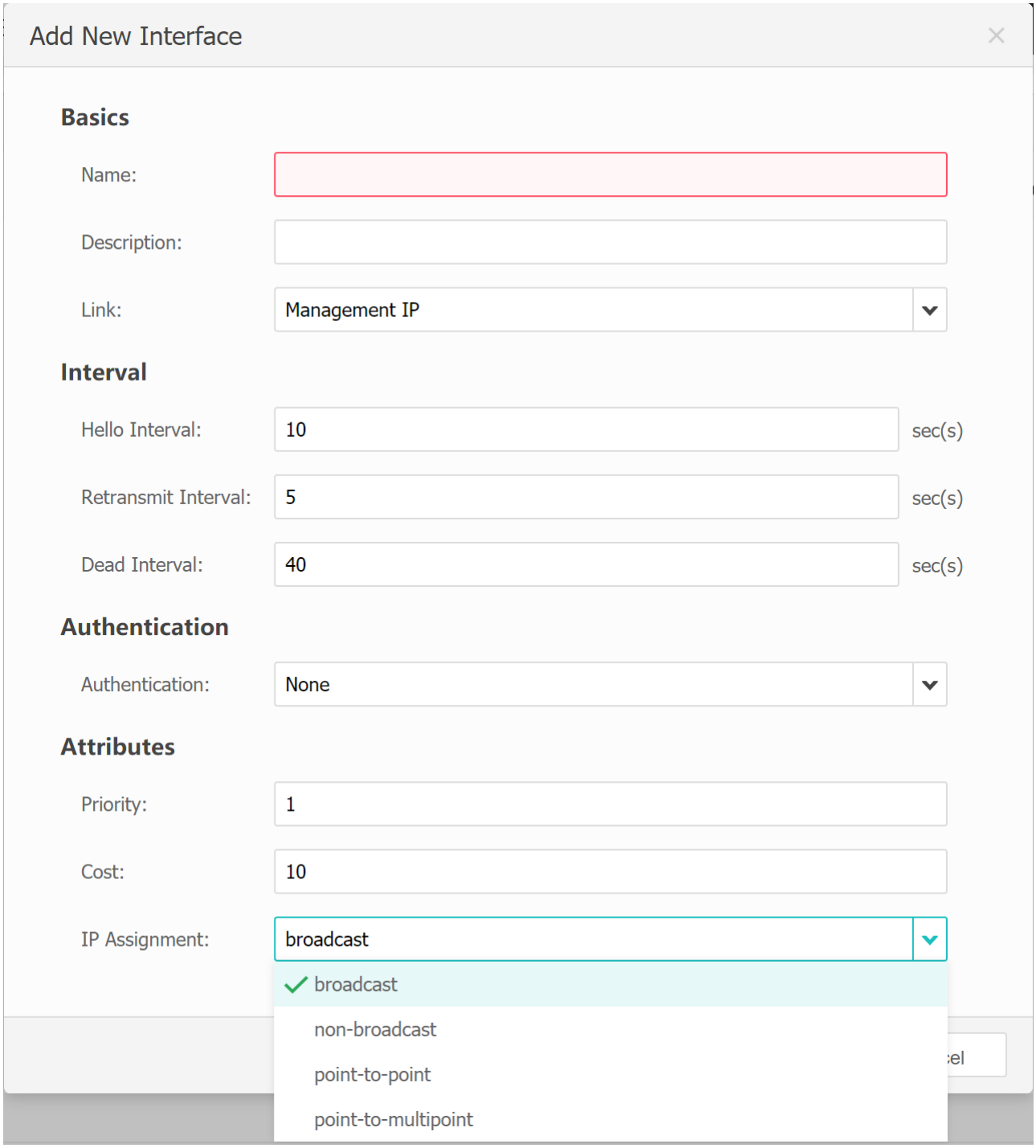
『Metric-type』sets the type used by OSPF to calculate the cost of paths.

『Area ID』sets the identifier of the area where the router is located in.

『Autonomous System External Route』sets whether the device receives the autonomous system external link-state advertisements. If this option is『Enabled』, when the routing entries of a neighboring router change, the router will receive link-state advertisements from the neighboring router. If this option is『Disabled』, the router will not receive any link-state advertisement from the neighboring router.

『Network Segment』configures the network segment that needs to be announced to the peer through OSPF. Enter [IP address] and [Netmask/Prefix].

2. Network Interface: sets the Name, Link, etc. to complete the configuration of the interface, as shown in the following figure:



『Link』: selects the link for which OSPF interface information needs to be set.

For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

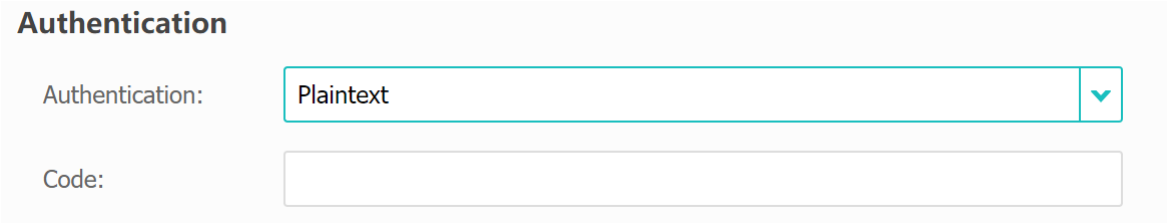
『Hello Interval』: refers to the time interval between two consecutive hello packets sent by the sender router (generally, the default value is used).

『Retransmit Interval』: refers to the time interval set for a sender router to retransmit link-state advertisement packets (generally, the default value is used).

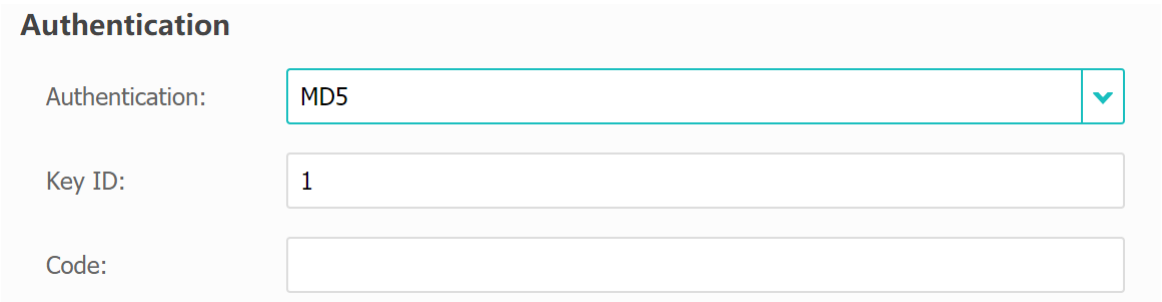
『Dead Interval』: sets how long the sender router should wait for hello packets from the peer before it refuses to form a neighbor relationship with the peer (generally, the default value is used).

『Authentication』: sets the method of OSPF authentication. The type of authentication can be "None", "Plaintext" or "MD5".

If "Plaintext" is to be selected, it is necessary to fill in the authentication Code.



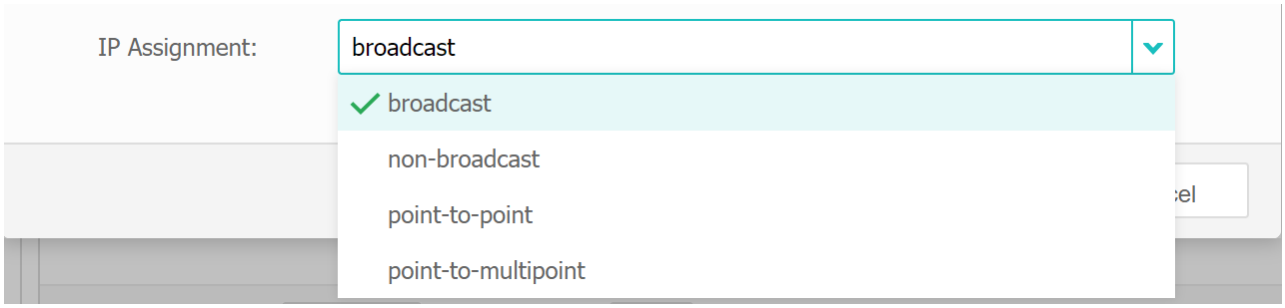
If "MD5" is to be selected, it is necessary to fill in the Key ID along with the Code.



『Priority』: sets the priority of the interfaces which support OSPF. The interface priority is used to elect a DR/BDR. The bigger the number filled in is, the higher the priority of the interface will be.

『Cost』: sets the link cost for the current interface. The bigger the number filled in is, the higher the link cost will be.

『IP Assignment』: sets the network type of the current interface, including broadcast, non-broadcast, point-to-point, and point-to-multipoint.



[point-to-point]: refers to Point-to-point (P2P) networks, indicating the connection between the interface and router is a point-to-point connection. This OSPF network type does not require DR and BDR elections.

When the link layer protocol is PPP or HDLC, OSPF considers the network type as P2P by default. On a P2P network, OSPF sends protocol messages in multicast mode using the multicast address 224.0.0.5.

[broadcast]: refers to Broadcast networks that support broadcasts by default. When the link layer protocol is Ethernet or FDDI, OSPF considers the network type as Broadcast by default. This OSPF network type does require DR and BDR elections. On a Broadcast network, OSPF sends protocol messages in multicast mode using the multicast addresses 224.0.0.5 and 224.0.0.6.

[non-broadcast]: refers to Non-Broadcast Multiple Access (NBMA) networks. Although multiple destination nodes are reachable from one interface, NBMA networks do not allow broadcasts by default. When the link layer protocol is Frame Relay, ATM, or X.25, OSPF considers the network type as NBMA by default. In such cases, OSPF neighbors need to be manually specified by the administrator. On an NBMA network, OSPF sends protocol messages in unicast mode.

[point-to-multipoint]: refers to Point-to-multipoint (P2MP) networks, indicating the connection between the interface and multiple routers is a point-to-multipoint connection.

3.3.7.2 BGP

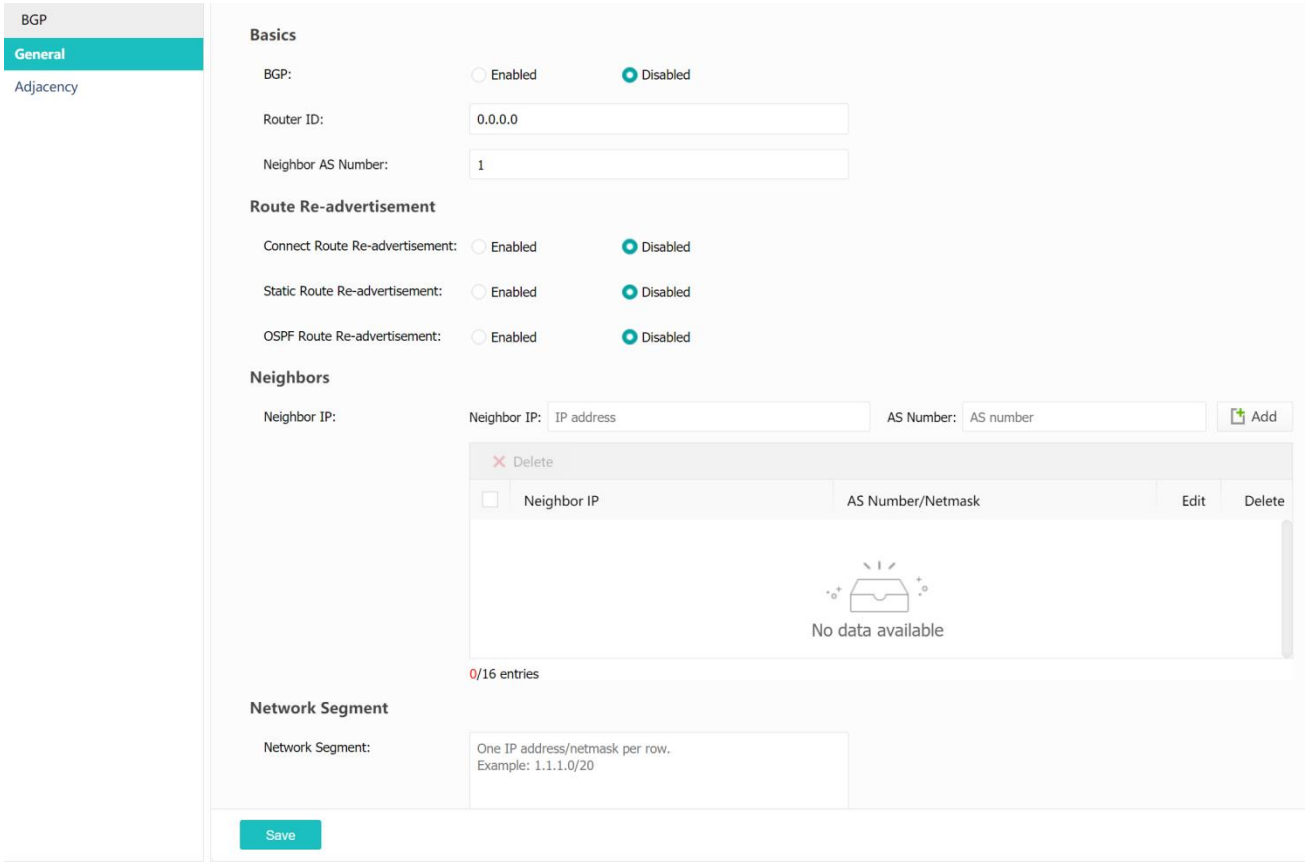
【Operation Scenarios】

It is generally used to set networks that need to be announced through BGP and whether to support broadcasting routing entries learned by other routing protocols using the BGP.

【Operation Procedure】

Navigate through『Network Deployment』-『Dynamic Routing』-『BGP』to complete the configuration of BGP by configuring [General]. [Adjacency] lists routes learned by BGP.

1. General: Set the Router ID, Neighbor AS Number, Route Re-advertisement, Neighbors, Network Segment, etc. to complete the configuration of BGP, as shown in the following figure:



『Router ID』: allows you to complete the field with information that is easy to remember to identify the identity of the router. The ID should be represented with numbers （1-4,294,967,295）or using dot-decimal notation.

『Neighbor AS Number』: sets the AS number of the local device.

『Neighbor IP』: sets BGP neighbors' IP addresses for communication.

『Neighbors』-『AS Number』: sets BGP neighbors' AS numbers.

『Network Segment』: sets local device publishing network segments

Other basic parameters can be left as defaults. Set parameters per requirements according to special needs (if any). Specific interpretations are listed as below:

『Connect Route Re-advertisement』: enables the network segment re-advertisement configured on the local device.

『Static Route Re-advertisement』: enables the static route re-advertisement.

『OSPF Route Re-advertisement』: sets whether to allow the BGP to broadcast the OSPF routing information learned by the device.

3.3.7.3 RIP

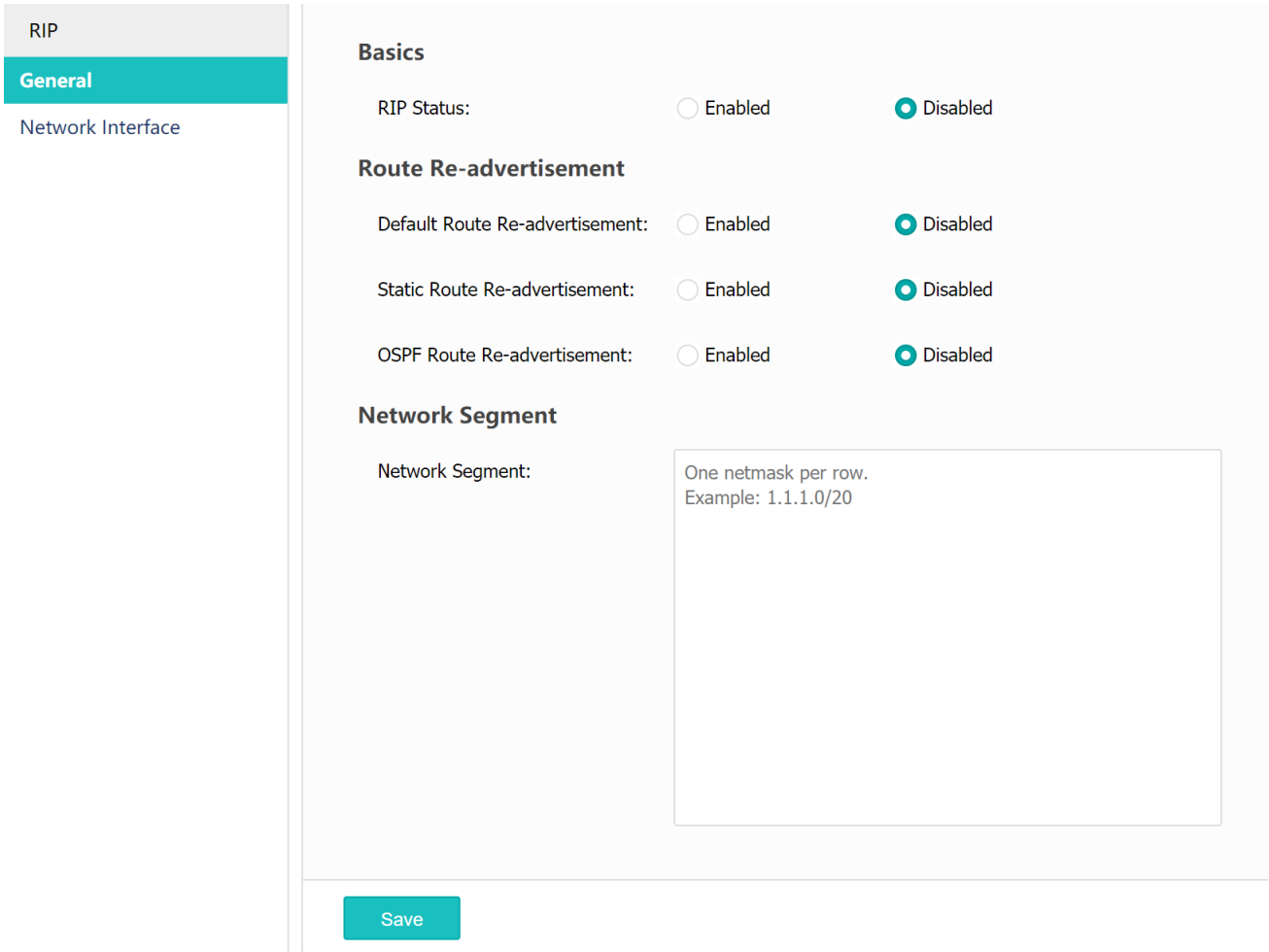
【Operation Scenarios】

It is generally used to configure the network that the ADC needs to advertise through the RIP routing protocol. Support the deployment of the ADC in an environment that uses the RIP routing protocol.

【Operation Procedure】

Navigate through『Network Deployment』-『Dynamic Routing』-『OSPFV3』to complete the configuration of RIP by configuring [General] and [Network Interface]. The specific configuration is as follows:

1. General: Set the Route Re-advertisement, Network Segment, etc. to complete the general configuration, as shown in the following figure:



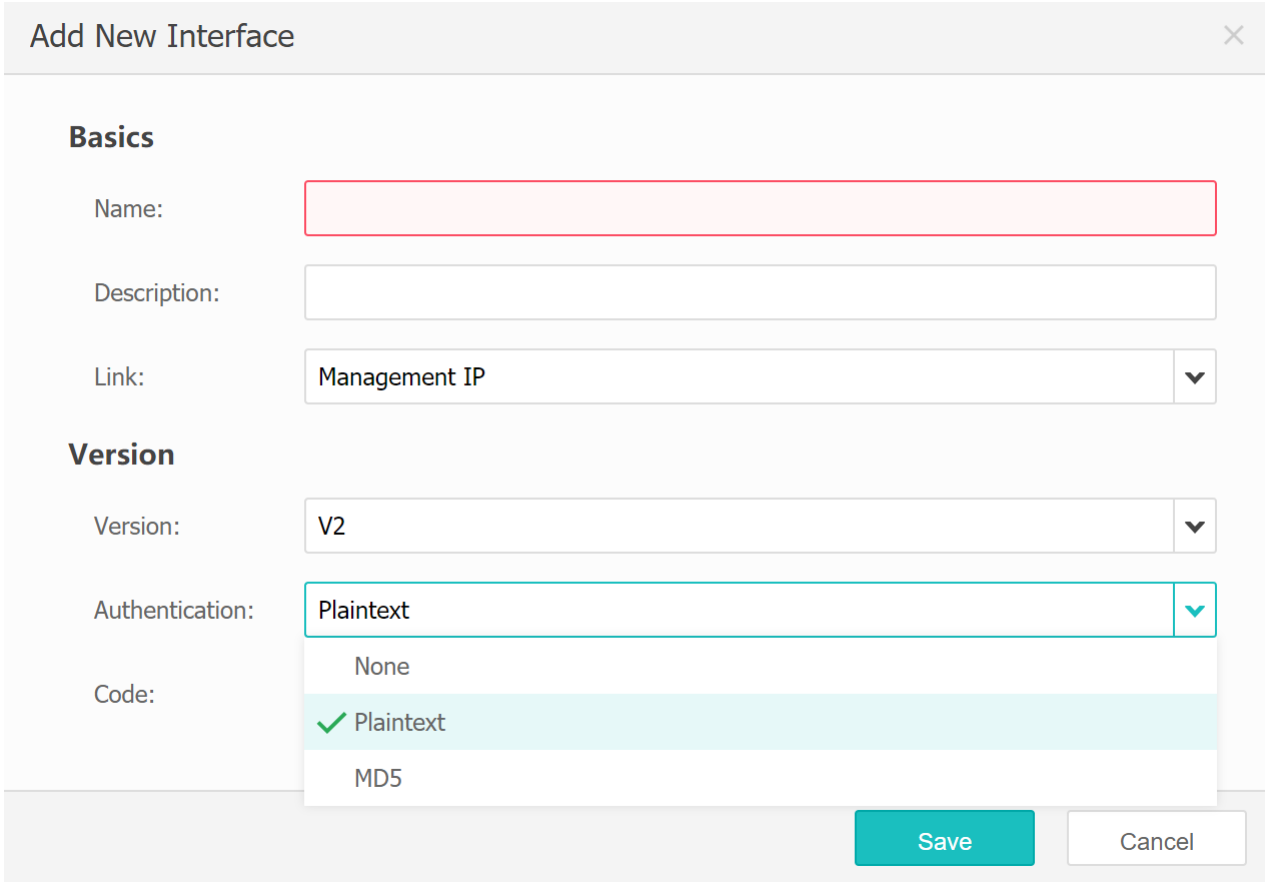
『Default Route Re-advertisement』: sets whether to allow the RIP to broadcast the default route, making adjacent routers direct default routes to the ADC.

『Static Route Re-advertisement』: sets whether to allow the RIP to broadcast the static routes configured on the device.

『OSPF Route Re-advertisement』: sets whether to allow the RIP to broadcast the OSPF routing information learned by the device.

『Network Segment』: configures the network segment that needs to be advertised to the peer through RIP.

2. Network Interface: sets the Name, Link, Version, etc. to complete the configuration of the interface, as shown in the following figure:

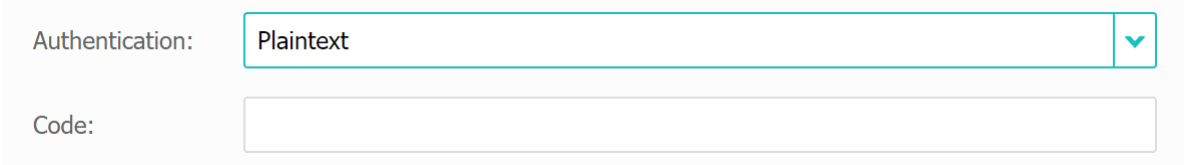


『Link』: selects the link for which RIP interface information needs to be set.

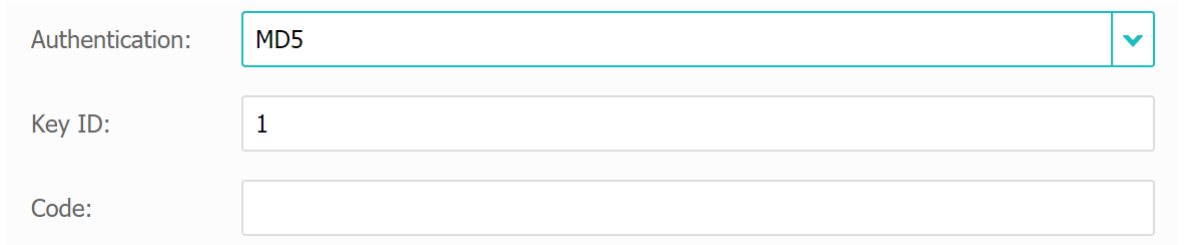
『Version』: selects the version of the RIP supported by the interface. Both V1 and V2 are supported.

『Authentication』: sets the method of RIPv2 Authentication. The type of authentication can be "None", "Plaintext" or "MD5".

If "Plaintext" is to be selected, it is necessary to fill in the authentication Code.



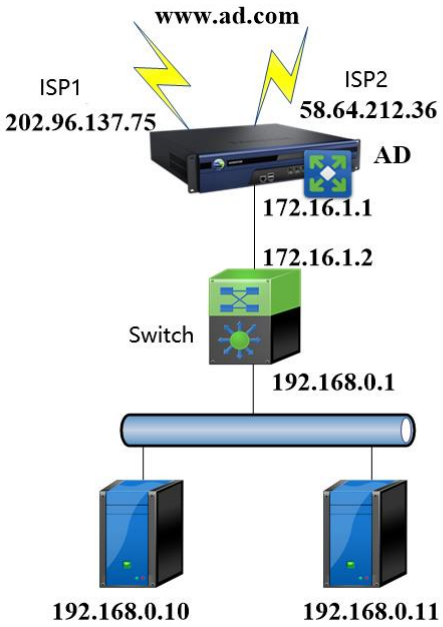
If "MD5" is to be selected, it is necessary to fill in the Key ID along with the Code.



3.4 Gateway Deployment for A Single Device

【Operation Scenarios】

In general, gateway deployment is recommended when a link load balancing or Layer 3 load balancing is required.
Advantages: All the functions of load balancing can be fulfilled (outbound load balancing, global load balancing, app load balancing, etc.).
Disadvantages: This type of deployment changes the network a lot, and it is recommended to perform such deployment when building a new network or the current network is undergoing optimization.
In a gateway deployment: Generally, ADC is connected downward to the core switch and upward to the Carrier. The core switch supports static or dynamic routing. The interface through which the ADC is connected with the core switch can be an ordinary network interface, aggregate interface, port bridging, or VLAN subinterface. This case mainly takes static routing and ordinary network interfaces as examples. For others, please refer to Section 3.3. The customer environment is shown in the following figure:



Network requirements: Use ADC to implement external network link load balancing, and implement app load balancing on two WEB servers.

【Preconditions】

1、 Pre-operational preparations and device installation are done.

2、External lines have been connected and required external IP addresses have been provided by the Carrier.

3、Configuration of the internal network's core and routes have been completed.

4、Complete the planning of internal network interfaces, external network interfaces, IP addresses, etc.

【Operation Procedure】

Overall configuration flow:

1、Configure one internal network interface line and two external network interface IP addresses (China Telecom and China Netcom), both of which are static IP addresses.

2、Configure source network address translation to surf the Internet by using ADC as a proxy for internal network (This can be configured when adding an external network interface).

3、Configure static routing to a LAN segment (192.168.0.0.0) to ensure the intercommunication between ADC and LAN.

4、If the management interface needs to be set separately, a management IP address can be set for the interface. Generally, the interface MANAGE is used.

After completing the above configurations, the overall network configuration has been done.

5、Configure link load balancing. For details, refer to Section 8.

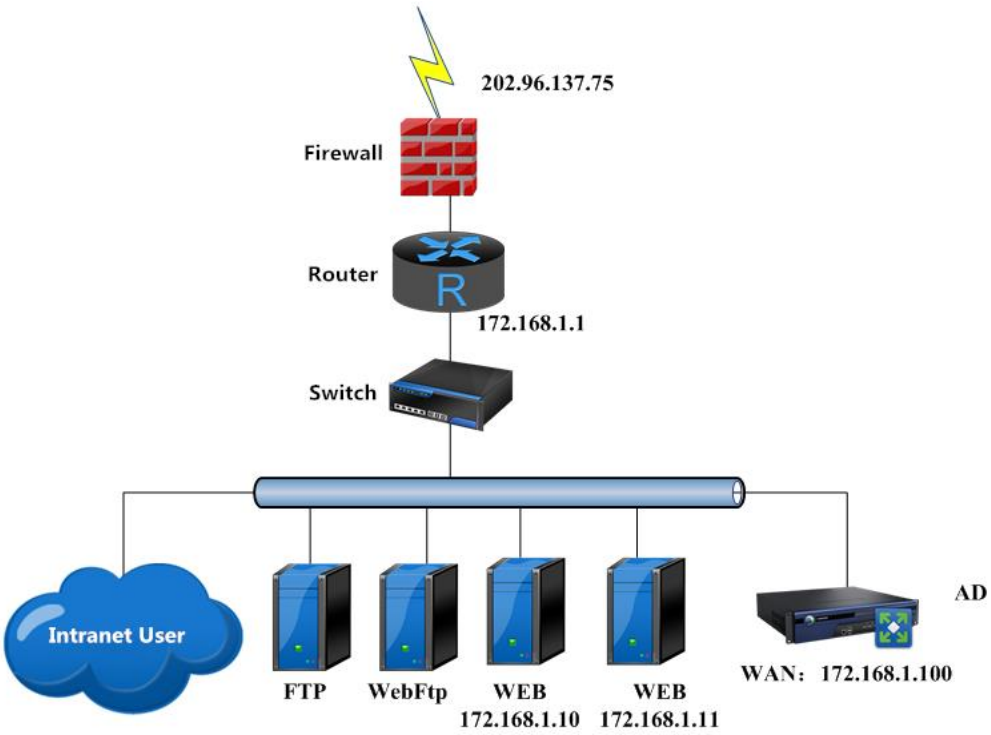
6、Configure app load balancing. For details, refer to Section 7.

**Attention**: For a general gateway deployment, it is not necessary to enable the WAN Port Forwards Outgoing Traffic. However, this option needs to be enabled when external network access to the device is required.

3.5 Bypass Deployment for A Single Device

【Operation Scenarios】

Generally, Bypass deployment is recommended when app load balancing should be implemented.
Advantages: No need to change the original network topology. Only a single connection to the core switch should be established for configuration.
Disadvantages: Link load balancing cannot be implemented, but other functions of load balancing can be fulfilled.
In a Bypass deployment: Generally, ADC's service interface is connected to the core switch. The core switch supports static or dynamic routing. The interface through which the ADC is connected with the core switch can be an ordinary network interface, aggregate interface, port bridging, or VLAN subinterface. This case mainly takes static routing and ordinary network interfaces as examples. For others, please refer to Section 3.3. The customer environment is shown in the following figure:



Network requirements: Use ADC to implement app load balancing on two WEB servers.

【Preconditions】

1、Pre-operational preparations and device installation are done.

2、ADC interface(s) and IP address(es) are already planned.

【Operation Procedure】

Overall configuration flow:

1、Create new WAN attribute interface(s) and configure static IP address(es). If there are IP addresses of multiple network segments, one or more IP addresses can be configured on a WAN interface.

2、Enable the WAN Port Forwards Outgoing Traffic.

3、Configure app load balancing. For details, refer to Section 7.

4、If the management interface needs to be set separately, a management IP address can be set for the interface. Generally, the interface MANAGE is used.

5、When external network access to service is required, it is necessary to map the VIP and service ports on ADC to the external network (port mapping for port devices).

Notes:

1) In the bypass mode deployment, it is only necessary to ensure that the WAN interface can communicate with the LAN server. The WAN interface and the server may not be on the same network segment.

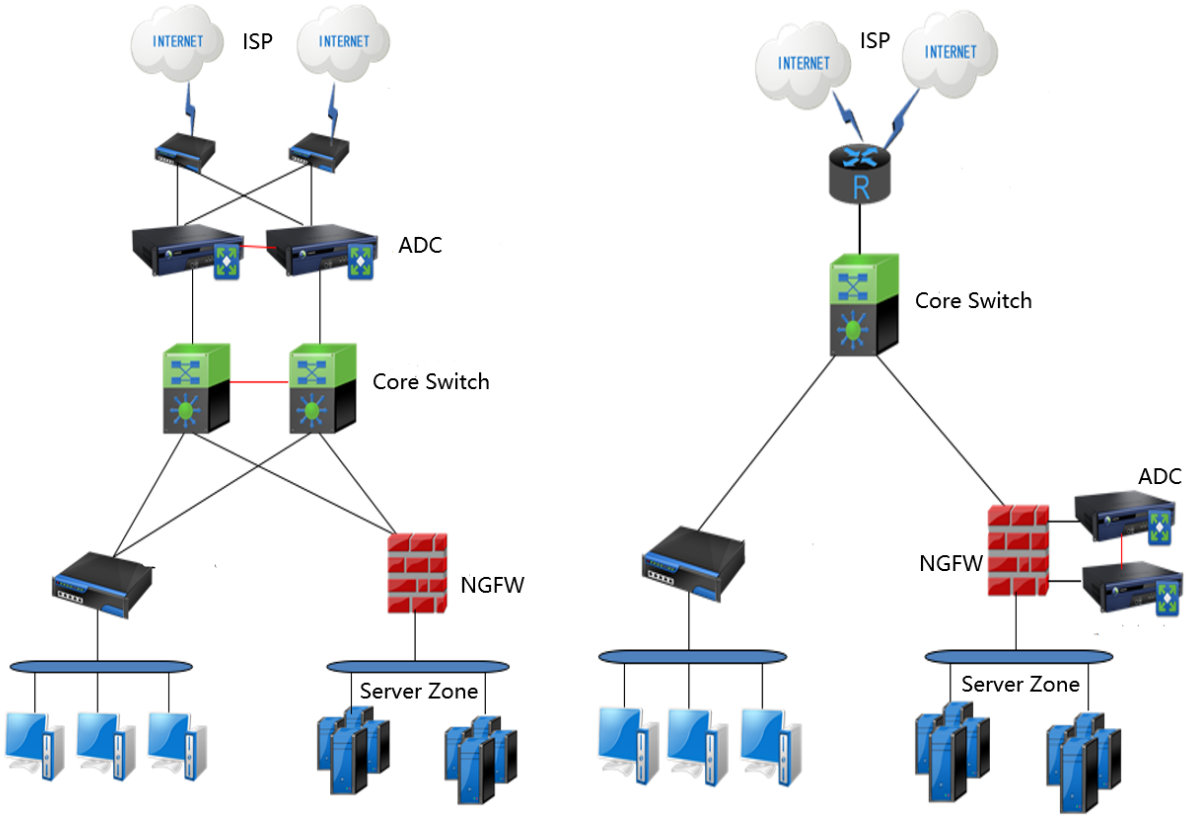
2) If a customer attempts to implement global load balancing - local DNS mapping in a one-arm deployment, port 53 of the DNS server listening address needs to be mapped to the Internet.

3.6 Active-Standby Mode

【Operation Scenarios】

Generally, it is used in network environments that require high network stability. The configuration of the active and standby devices is synchronized, except for different management addresses and HA interface addresses, the others are completely the same. Therefore, in such an active-standby deployment, the active-standby device switchover can be automatically triggered in case of any active device problem, so as to ensure the stable and continuous operation of service.

Active-standby deployment is supported in various deployment modes (Gateway & Bypass). Please see the following two typical deployment modes. In fact, customers can change locations more flexibly according to actual network environments.



The gateway mode & bypass deployment are taken as examples. The configuration of one-arm deployment is the same as that of the gateway. The only difference is whether there are internal and external network interfaces.

【Preconditions】

1、Pre-operational preparations and device installation are done.

2、Hardware platforms must be the same (the number of network interfaces and their arrangement is the same).

3、Authorization must be consistent.

4、Software version information must be consistent.

5、Service ports (internal and external interfaces), HA interfaces (of 2), and IP addresses of the ADC are properly arranged.

【Operation Procedure】

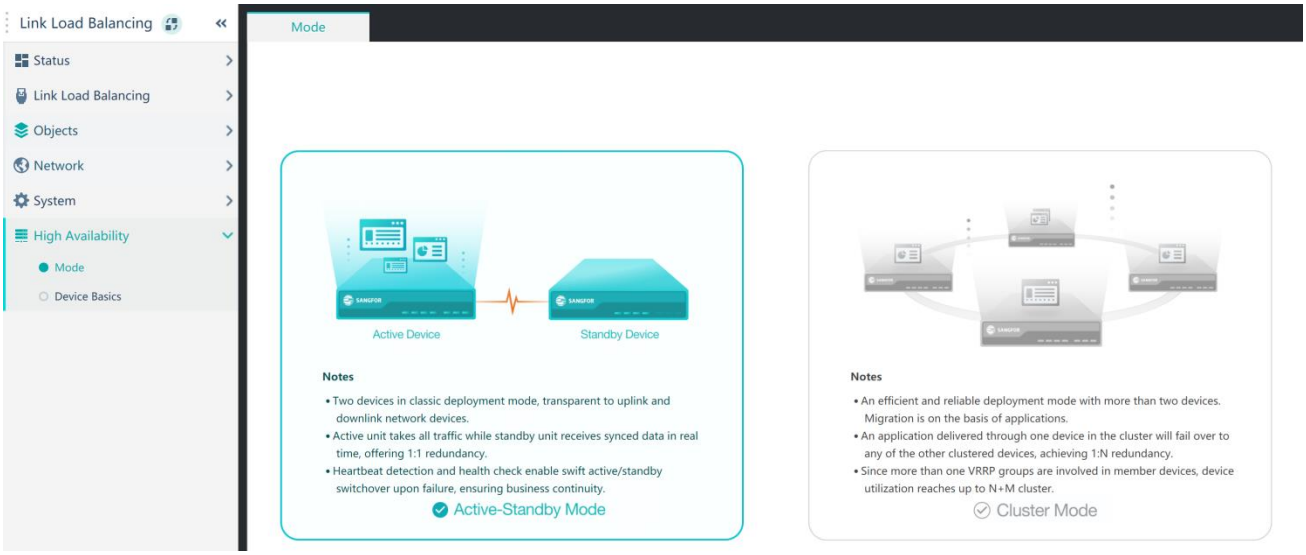
Overall configuration flow:

1. For the Active Device -> All the options of functions displayed on the dual-device interface need to be set up on the active device according to the following instructions. Generally, Device Name, Status, Primary Heartbeat Interface, Secondary Heartbeat Interface, Heartbeat Interface Health Check, Enable failover, etc. need to be configured for the active device.
2. For the Standby Device -> Only Name of Active Device, Status, Action, and Primary & Secondary Heartbeat Interfaces need to be set. Other information will be synchronized from the active device.

Select a mode:

* In the initial state, the Mode under High Availability of devices defaults to the Active-Standby Mode. If it has not been changed before, there is no need to select it again.

1、First, select 【Mode】 under【High Availability】module in the navigation bar on the right, and select【Active-Standby Mode】on the left, as shown in the figure below:

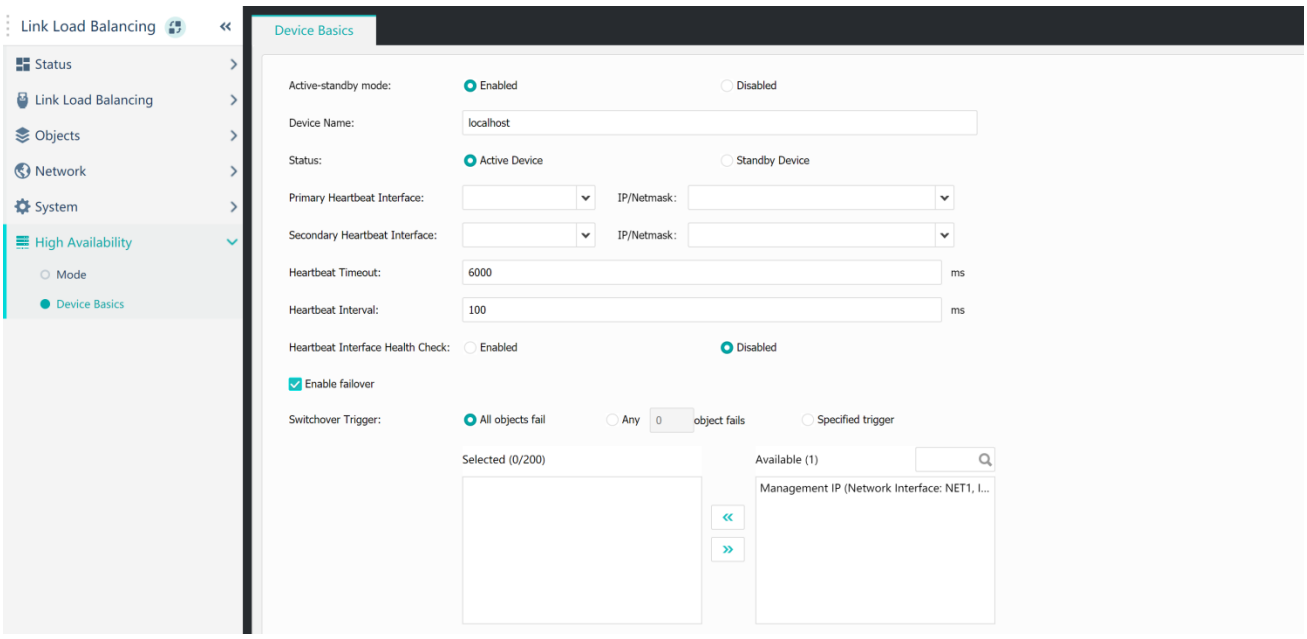


2、Select【Save】to enable the Active-Standby mode for devices, and Device Basics will be selected on the【High Availability】module menu in the left navigation bar.

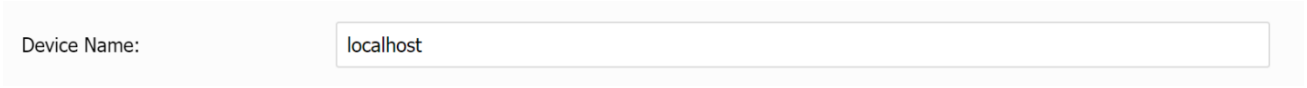
3.6.1 Active Device Configuration

Generally, Device Name, Status, Primary Heartbeat Interface, Secondary Heartbeat Interface,

Heartbeat Interface Health Check, Enable failover, etc. need to be configured for the active device. Details are as follows:



1. Device Name

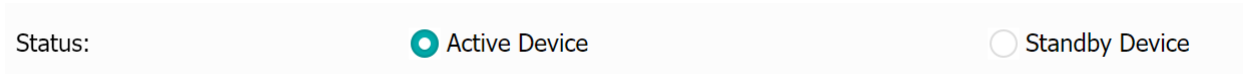


It is recommended to define a device name so as to distinguish logs according to the name of the active device when viewing logs of active & standby devices in the system log.

Function Description:

At present, Device Name is directly represented by the name of a device, which is mainly used to identify which device the current device is in the High Availability log. The dual-device interface supports modification.

2. Status



Select the Active Device.

Function Description:

For initial configuration, the device for which Status selected as Active Device will become the active device, and configuration of all the dual-device rules should be done on this page. The device for which Status selected as Standby Device will become the standby device and directly use the same configuration as the active device.

3. Set Heartbeat Interfaces

1) Primary Heartbeat Interface



It is recommended to select a network interface as the Primary Heartbeat Interface (excluding

the management interface), directly connect HA interfaces of the two devices (without involving a switch), and configure IP addresses on the same network segment (not conflicting with the internal network segment).

Function Description:

The primary heartbeat interface is necessary to be configured. Choose the network interface on the device panel as the HA interface and configure a reasonable network. (Generally, it is recommended that the HA interfaces should be directly connected without involving switches).

2) Secondary Heartbeat Interface



It is recommended to select a management interface as the Secondary Heartbeat Interface, and a reasonable IP address is required (You can directly select an existing IP address on the management interface from the drop-down box).

Function Description:

It serves as a redundancy guarantee mechanism for the primary heartbeat interface, that is, in the case of a primary heartbeat interface failure, the heartbeats and configuration synchronization can still work normally by using the secondary heartbeat interface. Its configurations are the same as those of the primary heartbeat interface. (Generally, it is recommended to use the management interface).

Attention:

1) IP addresses assigned to heartbeat interfaces should be newly added ones, and they cannot be the same as or on the same network segment with any IP address on the interface.

2) The secondary heartbeat interface does not support the session synchronization function, and it must be configured by default.

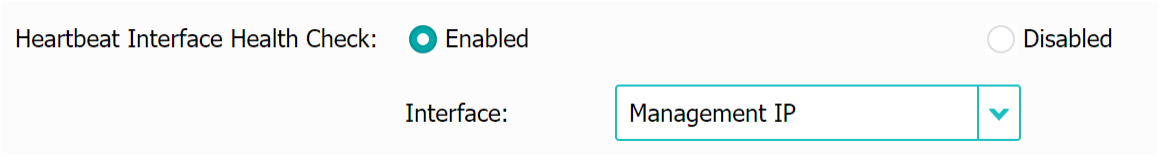
Recommended deployment configuration:

(1) It is recommended to encourage customers whose devices are upgraded smoothly to date to configure a management interface as the secondary heartbeat interface. In this way, the original service topology is not changed, and only the management interface needs to be connected to the same switch.

(2) For new customers, it is recommended to configure a service port as the primary heartbeat interface, and a management interface as the secondary heartbeat interface.

(3) For regular & new users, in case there are not sufficient service network interfaces and the management interface cannot be used for communication due to other reasons, it is recommended that the customer select serial ports to serve as secondary heartbeat interfaces and connect serial ports on the active & standby devices by using a serial cable.

4. Heartbeat Interface Health Check

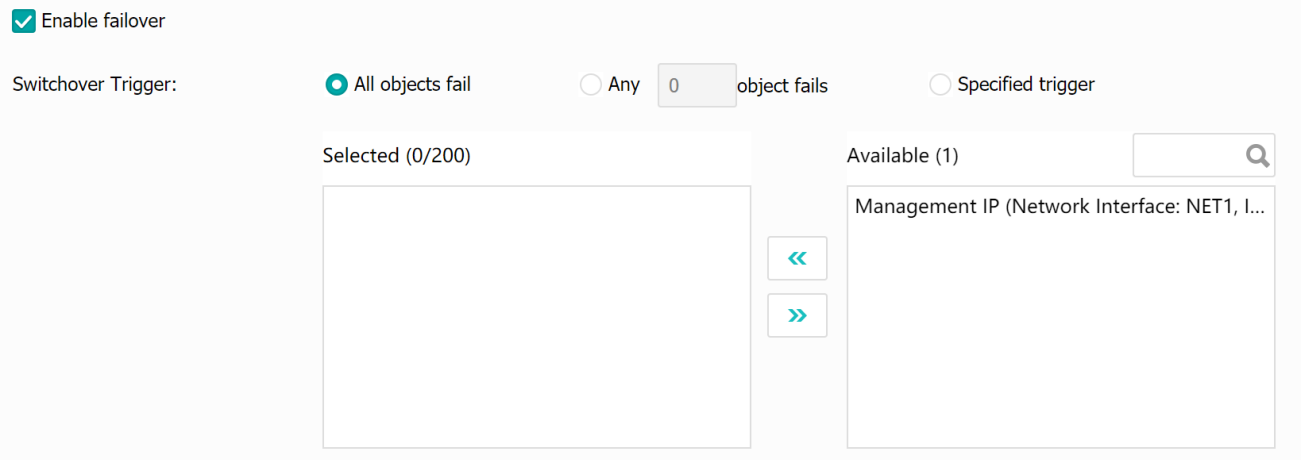


Enable this function and select the Service Port (directly from the drop-down box).

Function Description:

The Heartbeat Interface Health Check function is used to check whether the peer device is online through the network interface selected from the drop-down box when all heartbeat interfaces fail, which is equivalent to making a redundant backup on the secondary heartbeat interface once again.

5. Failover

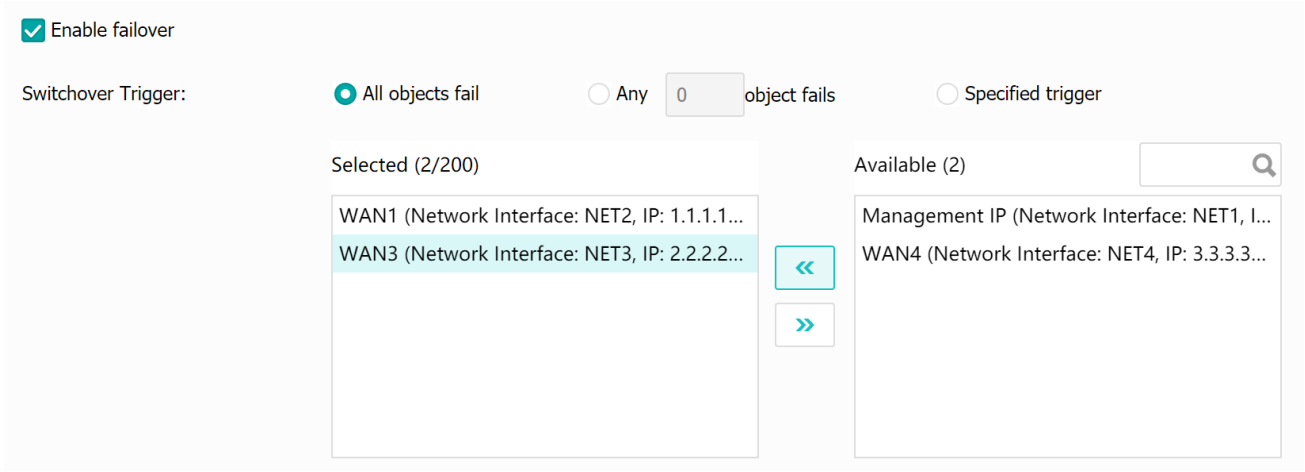


It is recommended to Enable failover, so as to ensure dual-device switchover be triggered in case of link failures.

Function Description:

There are three options for the health check Switchover Trigger, namely: All, Any, and Specified (newly added in AD ver. 7.0.3). The specific configuration meanings and methods are as follows:

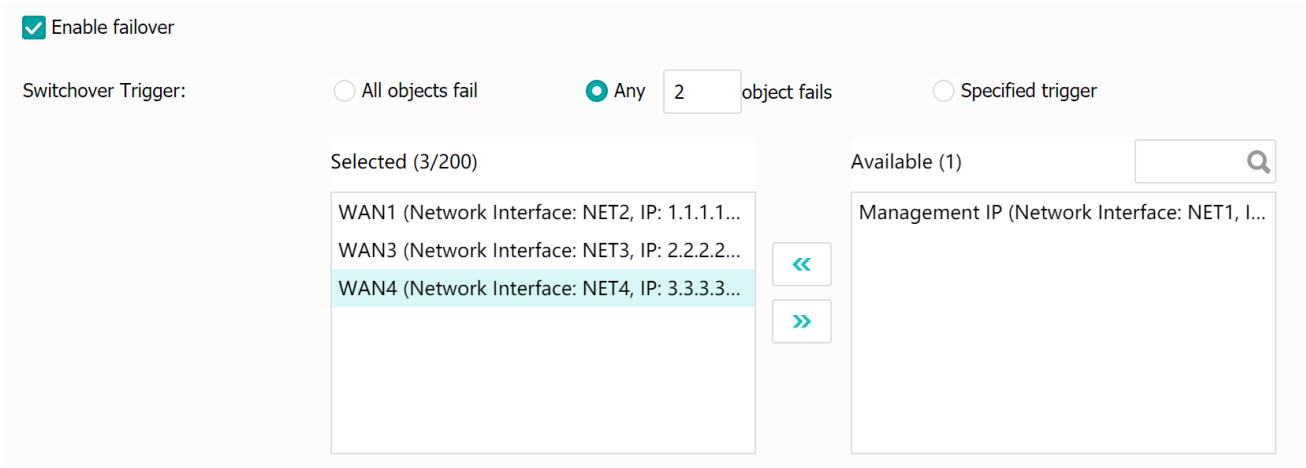
(1) All



After all of the links in the "Selected" box fail, an active-standby device switchover will

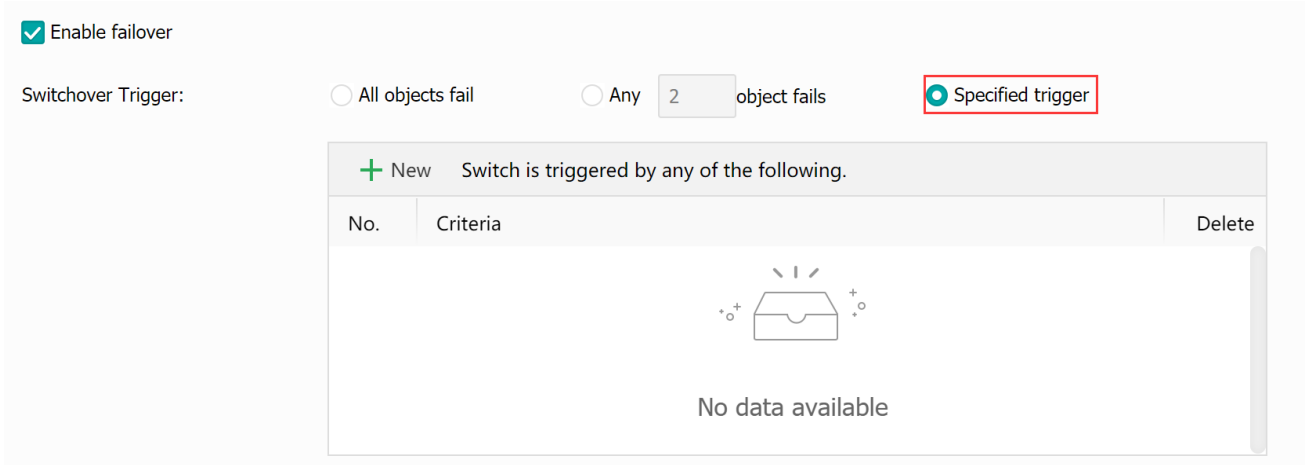
be performed.

(2) Any

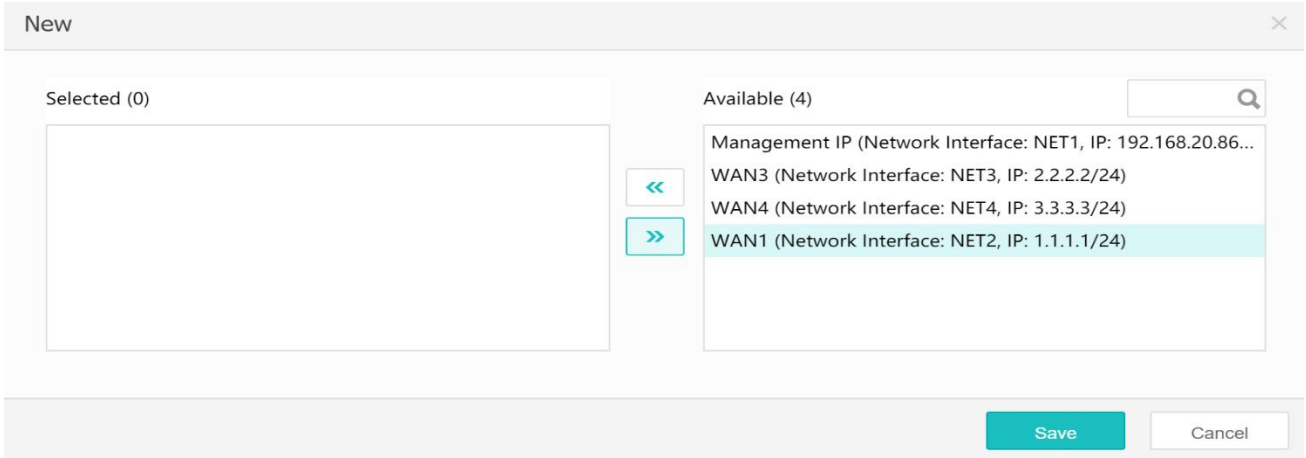


When any 2 of the Selected network interfaces fail, a dual-device switchover will be performed. Assuming that 3 links have been selected and the number of "Any" is 2, then when the number of failed links is greater than or equal to 2, a dual-device switchover will be performed.

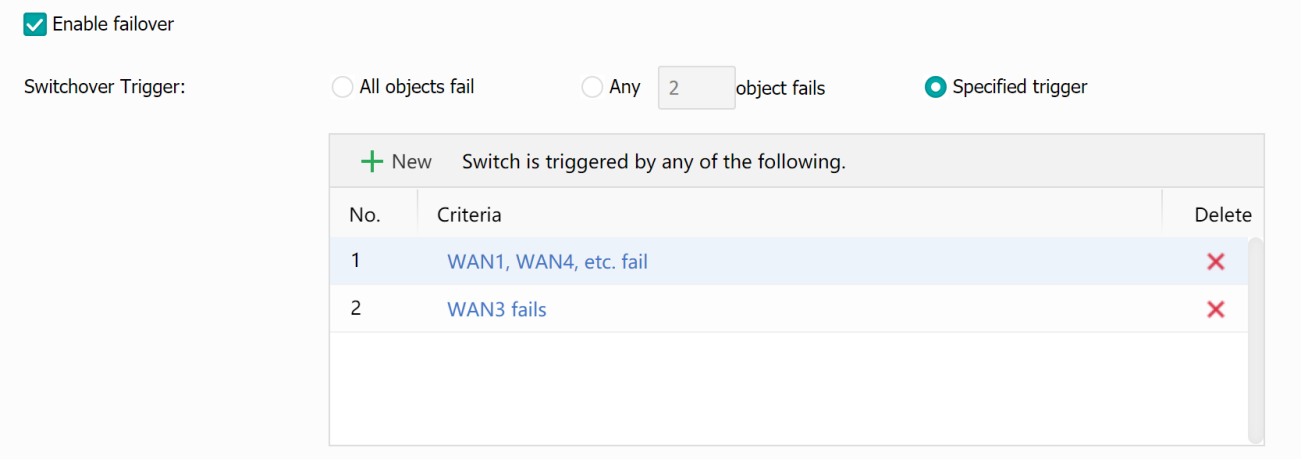
(3) Specified



This is a newly added switching rule. Click the New button to open the pop-up box for selection as shown in the figure below:



Links that available for selection are the ones listing in the health check "Selected" box. By moving the selected links to the list box on the right and clicking OK, these links will be selected as specified switchover triggers and shown in the trigger list.



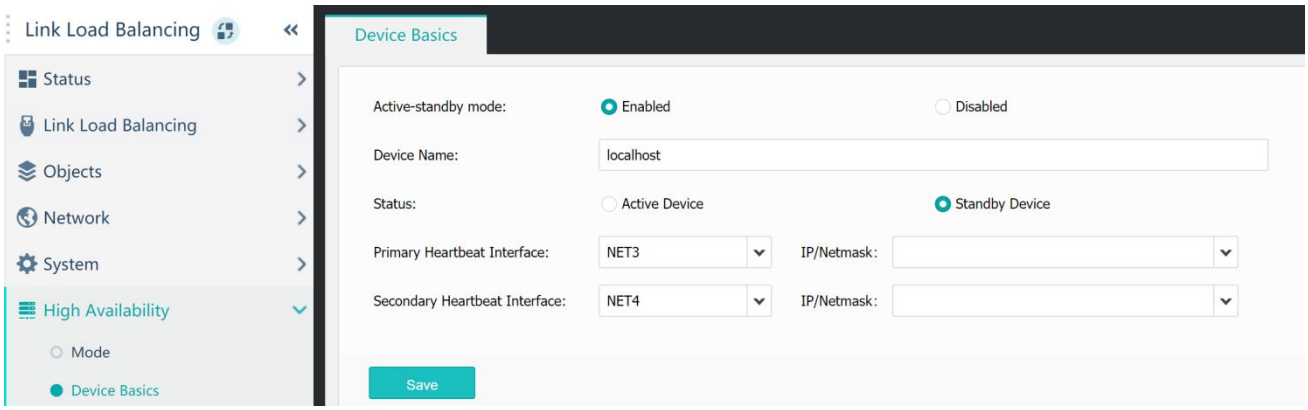
A maximum of 200 rules can be added. The rules shown in each row are independent of each other, and the relationship between any 2 of the rules is "or", that is, as long as one switchover trigger shown in any row is met, a dual-device switchover will be triggered.

After enabling, the active device will calculate the service state of active and standby devices according to the configured link health check triggers and monitor-level detection configuration of the devices. If the service state of the active device is worse than that of the standby device, an active/standby device switchover will be triggered.

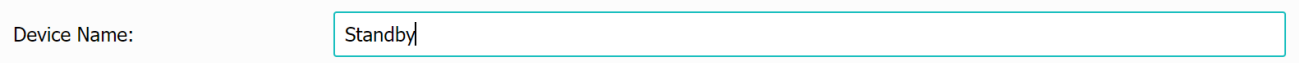
Other basic parameters can be left as defaults. Set parameters per requirements according to your special needs (if any).

3.6.2 Standby Device Configration

Generally, only the (active) Device Name, Status, Action, and Primary & Secondary Heartbeat Interfaces. The details are as follows:



1. Device Name

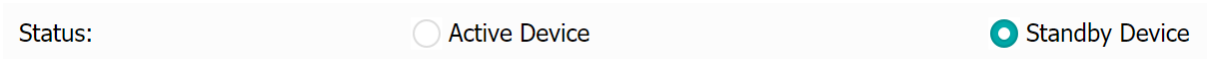


It is recommended to define an active device name so as to distinguish logs according to the name of the active device when viewing logs of active & standby devices in the system log.

Function Description:

At present, Device Name is directly represented by the name of the active device, which is mainly used to identify which device the current device is in the High Availability log. The dual-device interface supports modification.

2. Status



Select the Standby Device.

Function Description:

For initial configuration, the device for which Status selected as Active Device will become the active device, and configuration of all the dual-device rules should be done on this page. The device for which Status selected as Standby Device will become the standby device and directly use the same configuration as the active device.

3. Set Heartbeat Interfaces



It is recommended to select a network interface as the Primary Heartbeat Interface (excluding the management interface), directly connect HA interfaces of the two devices (without involving a switch), and configure IP addresses on the same network segment (not conflicting with the internal network segment). It is recommended to select a management interface as the Secondary Heartbeat Interface, and a reasonable IP address is required (For ver. 707, you can directly select an existing IP address on the interface from the drop-down box).

Function Description:

(1) Primary Heartbeat Interface: it is necessary to be configured. Choose the network interface on the device panel as the HA interface and configure a reasonable network. (Generally, it is recommended that the HA interfaces should be directly connected without involving switches).

(2) Secondary Heartbeat Interface: it is a newly-added function for AD ver. 7.0.3 and serves as a redundancy guarantee mechanism for the primary heartbeat interface, that is, in the case of a primary heartbeat interface failure, the heartbeats and configuration synchronization can still work normally by using the secondary heartbeat interface. Its configurations are the same as those of the primary heartbeat interface. (Generally, it is recommended to use the management interface).

Attention:

1) The IP address assigned to the primary heartbeat interface should be a newly added one, and it is better not to be the same as or on the same network segment with any IP address on the interface.

2) The secondary heartbeat interface does not support the session synchronization

function, and it must be configured by default according to related requirements for the new version.

3.7 Cluster Mode

【Operation Scenarios】

It is recommended to implement cluster deployment in the following scenarios: LAN traffic is high and customers attach great importance to the stability and reliability of service systems. They purchase two or more ADCs for running different services on different devices which can be backed up by each other. At the same time, subsequent expansion transition of the devices should be smoothly implemented. The comparison between Cluster deployment and Active-Standby deployment is as follows:

Cluster: high redundancy, high resource utilization rate, and good scalability.

Dual: simple logic, simple configuration, addresses required to be consistent, easier to maintain.

It is recommended to select the type of deployment depending on the actual conditions of LAN, and each deployment mode has its advantages and applicable scenarios.

【Preconditions】

1. Pre-operational preparations and device installation are done.
2. Hardware platforms must be the same (the number of network interfaces and their arrangement is the same).
3. Authorization must be consistent.
4. Software version information must be consistent.
5. Service ports (internal and external interfaces), HA interfaces (of 2), and (static & dynamic) IP addresses of the ADC are properly arranged.

【Operation Procedure】

Overall configuration flow:

1. Master controller: Select Mode - Create new cluster - Primary & Secondary Heartbeat Interfaces information.

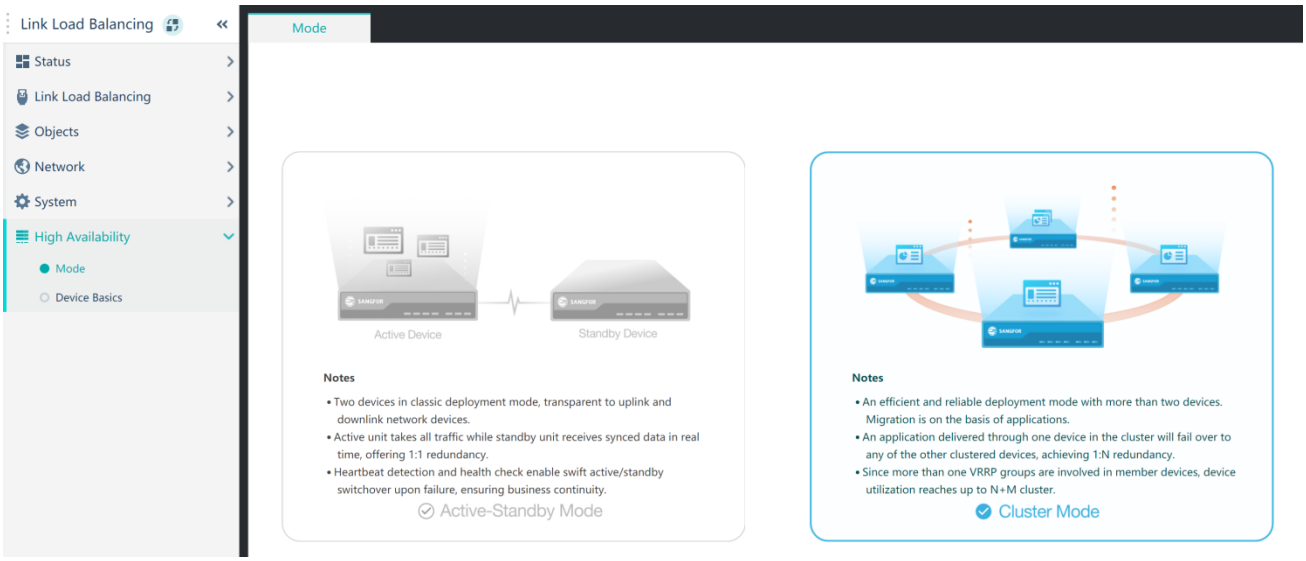
2. Standby controller or member: Select Mode - Join to existing cluster - Primary Heartbeat Interface IP, Login Username & Password for Master controller - Primary &

Secondary Heartbeat Interfaces information for Standby controller.

Select a mode

* In the initial state, the High Availability of the device defaults to Active-Standby Mode. It should be manually switched to Cluster Mode.

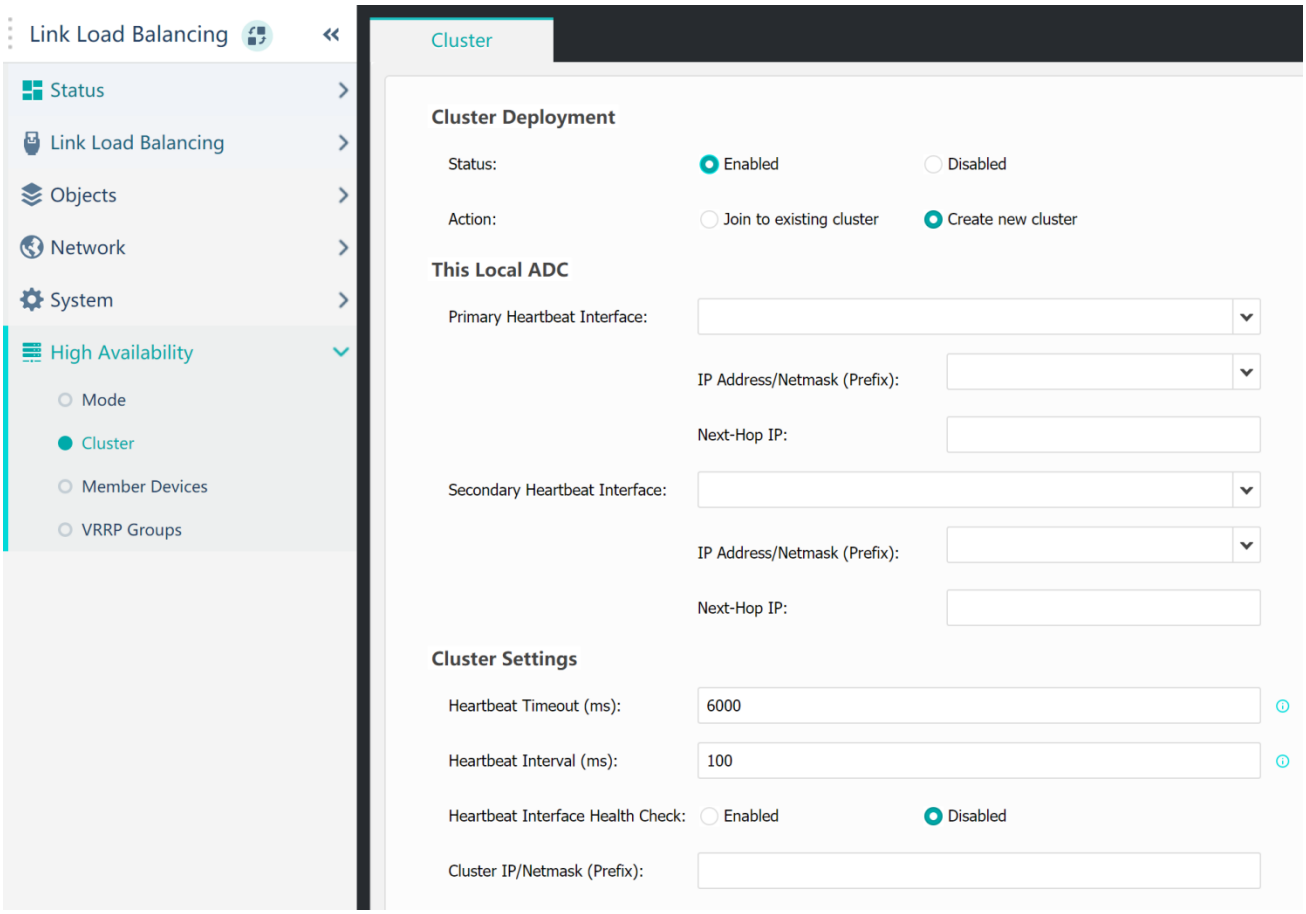
1. First, select 【Mode】 under【High Availability】module in the navigation bar on the right, and select【Cluster Mode】on the right.



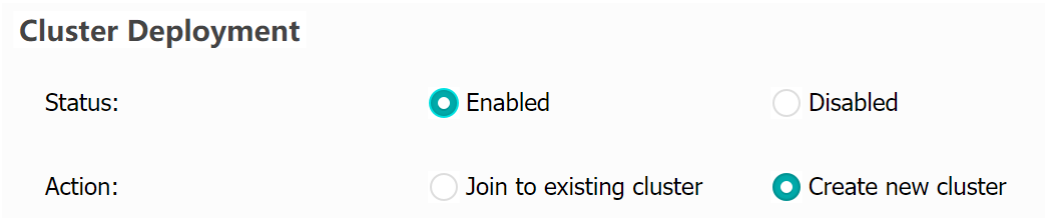
2. Select【Save】to enable the Cluster Mode for devices, and the module menu under【High Availability】in the left navigation bar has been switched to Cluster from Active-Standby.

3.7.1 Master

Generally, the device for which "Create new cluster" is selected will become the Master controller, as shown in the following figure:



1.Create New Cluster



Select "Create new cluster" for the Master controller.

2. This Local ADC

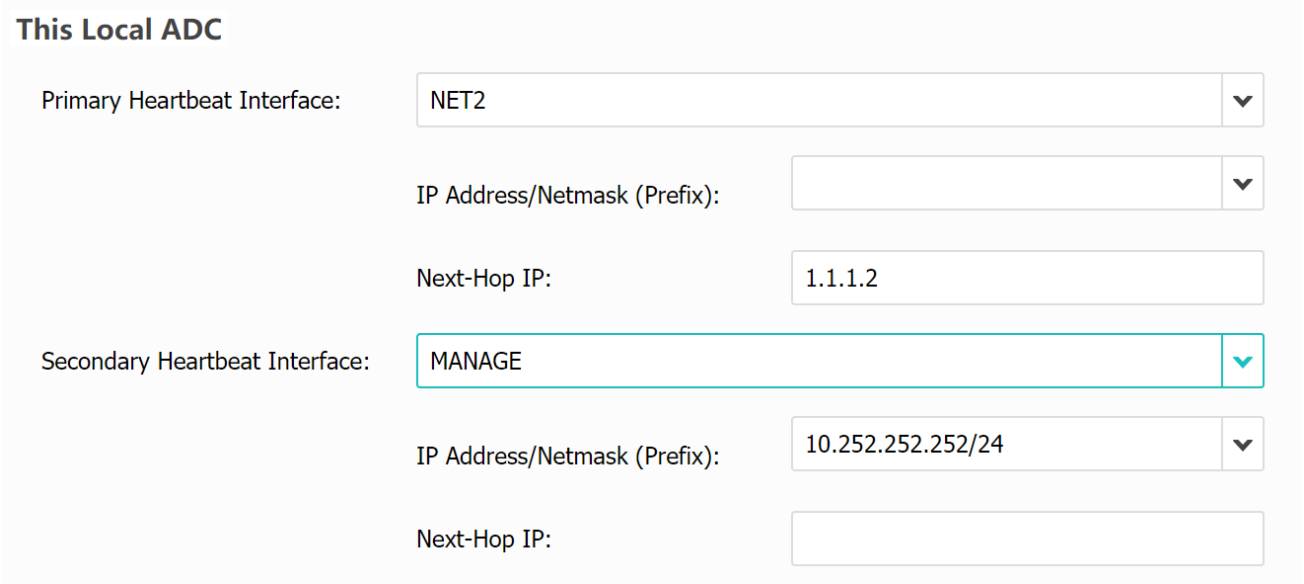
Configuration of Primary & Secondary Heartbeat Interfaces: Implementation of functions such as status maintenance and session synchronization between clustering devices relies on the primary heartbeat interface. Primary & secondary heartbeat interfaces can be selected from various types of network interfaces (physical /VLAN/BOND/BRIDGE/MANAGE interfaces are supported), and all available ports will be listed in the drop-down box for selection.

Attention :

(1) The ports selected as primary & secondary heartbeat interfaces cannot conflict with each other. Service ports can also be used as heartbeat interfaces.

(2) If a management interface is selected as the primary heartbeat interface, session synchronization cannot be performed.

Example: The primary heartbeat interface is a physical interface, and the secondary heartbeat interface is a management interface.



If the connection of heartbeat interface IP addresses of clustering devices is a Layer 2 direct connection on the same network, 【Next-Hop IP】may be left blank.

3. Cluster Deployment

Heartbeat interface health check:

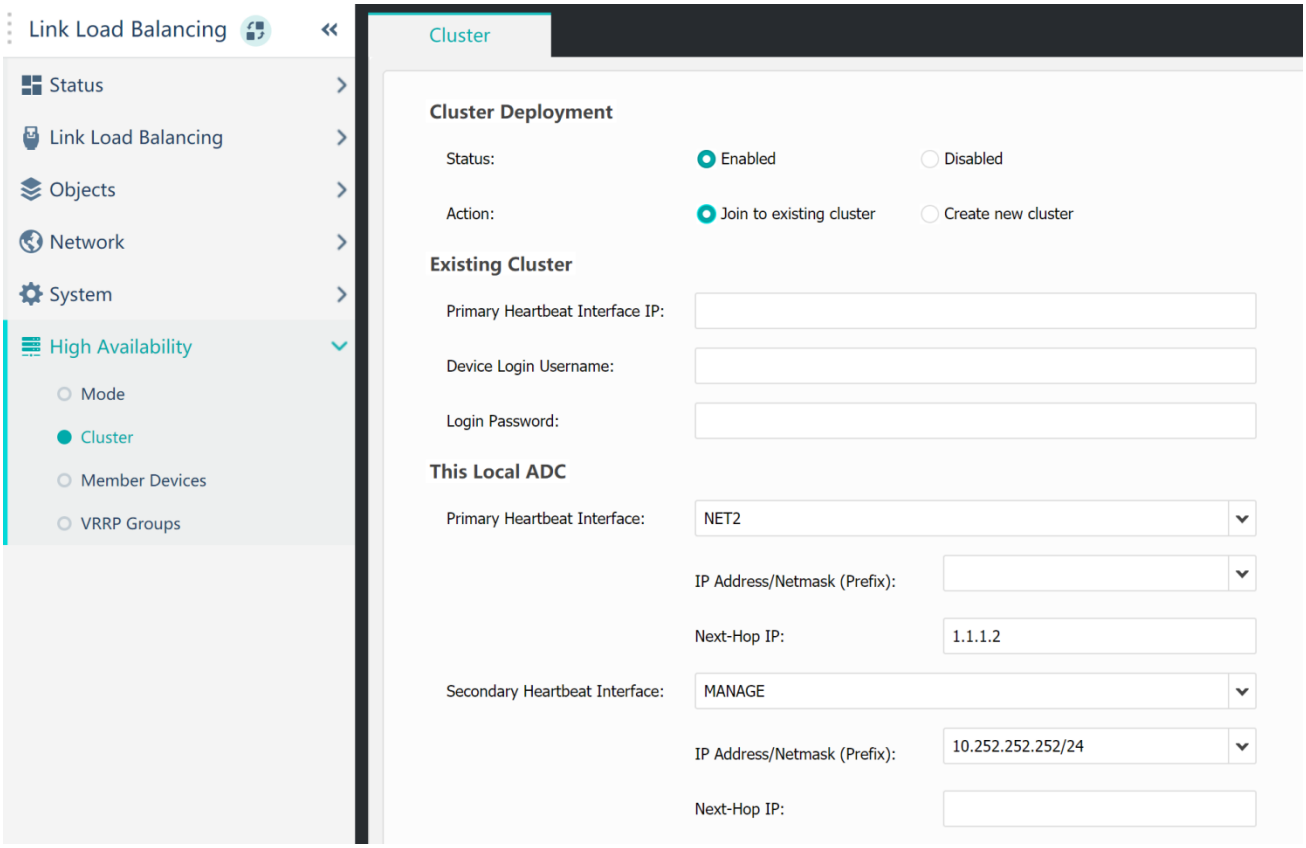
Generally, a service port is selected to serve as the heartbeat failure detection port to prevent split-brain.

This function is also called split-brain detection. Dual-master controlling may be caused by failures of both the primary & secondary heartbeat interfaces, resulting in the disorder of business functions. When both the primary & secondary heartbeat interfaces fail, use another link (both WAN interface and LAN interface are OK) to send the split-brain detection packet. One of the Master control devices will get into a state of split-brain silence after an election, so as to ensure that only one device is left to serve as the Master controller and ensure the normal operation of services.

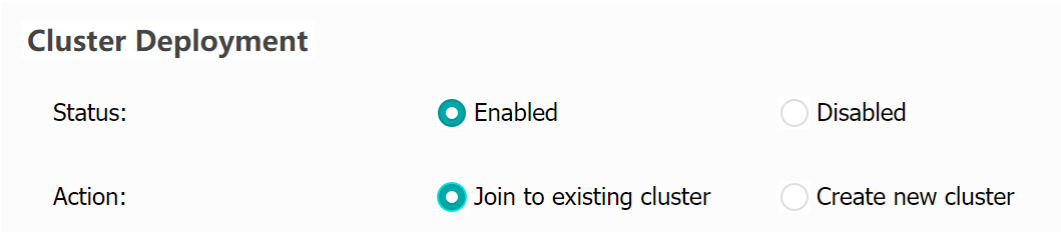
After the above configuration is completed and saved, the device successfully creates a new cluster and becomes the Master controller. Only then can the operation of joining the existing cluster be completed on other devices.

3.7.2 Standby Controller or Member

Generally, the devices for which "Join to existing cluster" is selected will become standby controllers or members, as shown in the following figure:



1. Join to Existing Cluster



Select "**Join to existing cluster**".

2. Existing Cluster

(1) Primary Heartbeat Interface IP

Complete this field with the primary heartbeat interface IP address of the Master controller.

(2) Device Login Username and Login Password

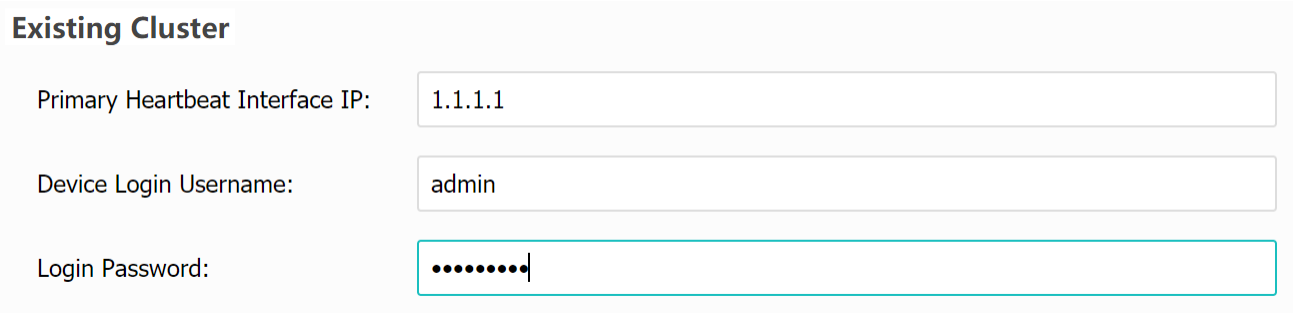
Complete this field with the username and password assigned to the Master controller for logging in to the web front end.

Attention :

(1) The entered account must have been granted API permissions for the High Availability module.

(2) After successfully joining, the username and password assigned to the device will be synchronized with those for the Master controller. The username and password assigned to the Master controller shall be used to log in to the front end, and the command line SSH account will also be synchronized.

Example:



3. This Local ADC

Operation steps that should be followed are the same as those for the Master controller. The HA interface selected should be the same as that for the Master controller, and then fill in the IP address and gateway.

Attention:

1) If the IP addresses of the primary heartbeat interface and Master controller are in the same network segment, the Gateway can be left blank.

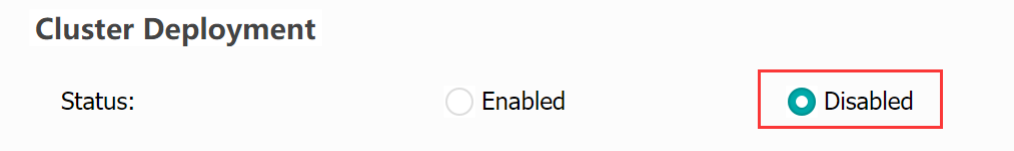
2) Network segments mentioned above are not required to be strictly consistent for the two devices. Instead, they may form a containment relationship. For example, one device is assigned with 192.168.1.1/25, and the other is assigned with 192.168.1.10/24. However, taking management normalization and convenience into account, such settings are usually not recommended.

After completing and saving the above configurations, the device successfully joins the existing cluster and batch synchronization will be started. Joining the existing cluster will restart the front end and trigger a jump prompt which lasts about 1 minute:

During this period of time, the front-end page cannot be displayed because the Aapche server has not finished restarting. When finished, it will automatically jump to the login page. The cluster joining is complete.

3.7.3 Exit A Cluster (Disable A Cluster)

1. Select "**Disabled**" and click "Save".



2. Enter username and password in the pop-up dialog box, and then click "Save".

3. No matter "Exit" or "Join to existing cluster" is selected, you will be redirected to the login page.

Attention:

After exiting the cluster, if relevant configurations of the device are not cleared or restored, resulting in some remaining configurations (such as the network link) are the same as those of the original cluster, IP conflicts will be caused therefrom. In view of this, you need to manually clear relevant configurations.

3.8 Network Security

3.8.1 ACL

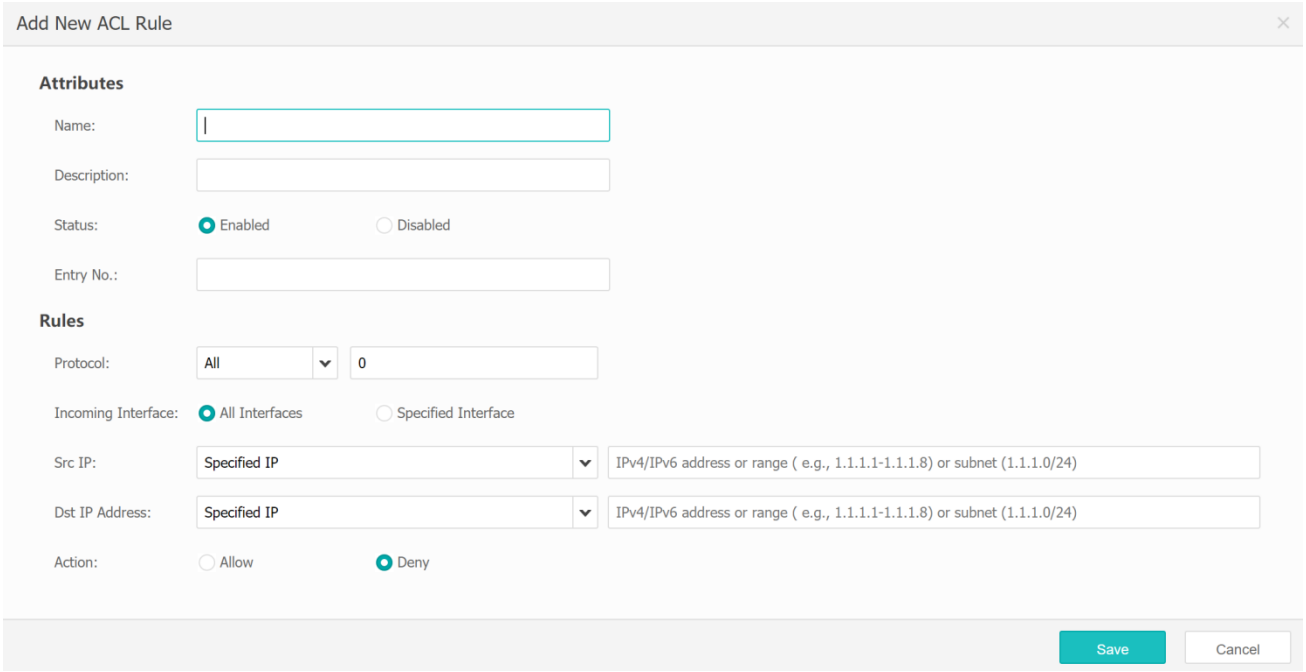
【Operation Scenarios】

ACL is generally used to configure link-level access control, which is similar to the firewall rules of security devices. Access control settings can be performed by using this function based on the link, protocol, source IP, and destination IP addresses. For example, if you want to deny a request sent from a source IP for accessing a certain port of a destination IP, this function can be enabled for all links or a specified link as selected.

【Operation Procedure】

Choose『Network』-『Network Security』- 『ACL』and click New. Configure Name, Priority, Rules, etc. to complete the configuration of an ACL entry, and the ACL configuration items are matched

from top to bottom. See the figure below:



『Protocol』: sets a protocol number. When communication conforms to this protocol number, it matches the current ACL rule. 0 means all protocol numbers.

『Incoming Interface』: selects the effective link.

『Src IP』: configures an IP segment. When the source IP address matches this IP segment, it matches the current ACL rule.

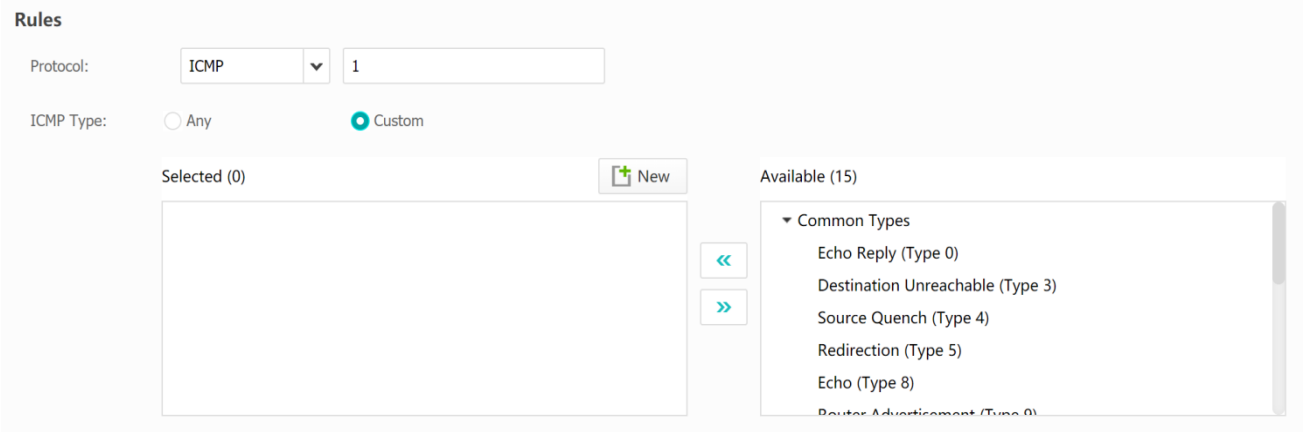
『Dst IP Address』: configures an IP segment. When the destination IP address matches this IP segment, it matches the current ACL rule.

『Action』: configures an action. When all the above conditions are met, the action will be executed.

(1) [Allow] allows the access matching five-tuples.

(2) [Deny] discards the access matching five-tuples.

Notes: Select ICMP Protocol, and select ICMP Type as Custom to perform Common Types selection.



Attention: Carefully configure the Deny action for all links, protocols, source IP addresses, and destination IP addresses. Otherwise, exceptions could be caused to all services, even to device console login.

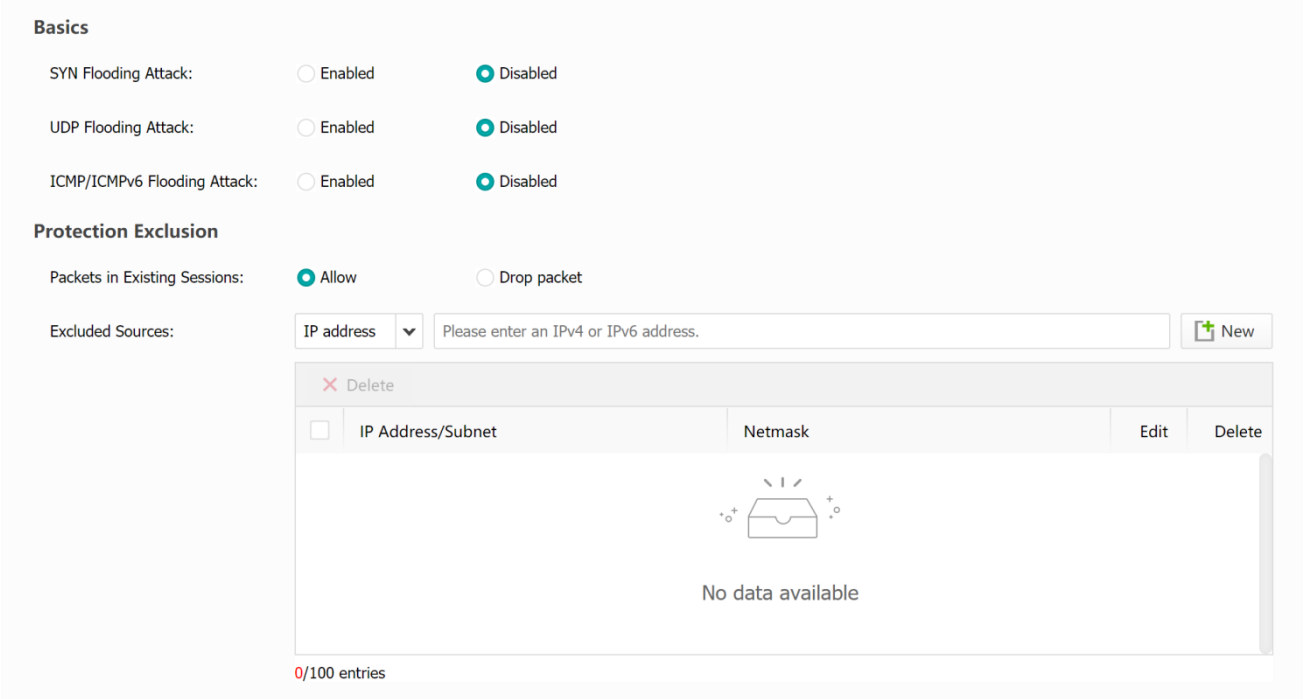
3.8.2 Anti-DOS(Insider Threat)

【Operation Scenarios】

Anti-DOS(Insider Threat) is generally used to protect the device against attacks from an internal network (LAN interface) and prevent service abnormalities caused by virus infections that suffered by one or more computers on the internal network. It is mainly used to prevent DDOS. If a device is specially deployed for securing the internal network, Anti-DOS(Insider Threat) may not be enabled.

【Operation Procedure】

Navigate through『Network』-『Network Security』-『Anti-DOS(Insider Threat)』to set protection parameters as required. Specific parameter values to be set is depending on network traffic volume, as shown in the following figure:



『SYN Flooding Attack』: detects data packets sent from a LAN interface and counts the number of SYN packets accessing the LAN interface address per second to determine if an attack has occurred. If the threshold is exceeded, subsequent TCP handles the proxy 3-way handshake and sends an alarm message to the log center. The 3-way handshake proxy will not stop until the number of SYN packets in a certain second falls below the threshold.

(1) [Threshold per Dst IP]: configures the limit of the number of SYN packets per second as required by the protection module.

『UDP Flooding Attack』: detects data packets sent from a LAN interface and counts the number of UDP packets accessing the LAN interface address per second to determine if an attack has occurred. If the threshold is exceeded, subsequent UDP packets will be dropped within the current second and an alarm message will be sent to the log center.

(1) [Threshold per Dst IP]: configures the limit of the number of UDP packets per second as required by the protection module.

(2) [Drop Empty Packet]: drops empty data packets. Drop all packets with a data length of zero without performing a threshold-dependent evaluation. You can also select and drop packets with a length being out of a specified range, or packets with a specified length. The implementation of these functions is similar to that of the function of dropping packets with a length of zero, that is, dropping packets directly without performing a threshold-dependent evaluation.

『ICMP Flooding Attack』: detects data packets sent from a LAN interface and counts the number of ICMP packets accessing the WAN interface address per second to determine if an attack has occurred. If the threshold is exceeded, subsequent ICMP packets will be dropped within the current second and an alarm message will be sent to the log center.

(1) [Threshold per Dst IP]: configures the limit of the number of ICMP packets per second as required by the protection module.

『Protection Exclusion』 sets a list of source IP addresses that do not need to be prevented.

For『Packets in Existing Sessions』, when "Allow" is selected, packets with which connection has been established will not be prevented. If "Drop packet" is selected, packets of the node monitor using UDP and ICMP will be discarded without any backhaul. Therefore, it is recommended to select "Allow".

For『Excluded Sources』, when the source IP address of a data packet is included in the Excluded Sources list, it can directly PASS without any ICMP Flooding Attack, UDP Flooding Attack, and SYN Flooding Attack processing.



Notes: It is recommended to set a relatively larger value when the specific parameter value can not be determined based on the internal network traffic volume, and then make appropriate adjustments according to the actual service conditions, so as to prevent the value from being too small and affecting normal services.

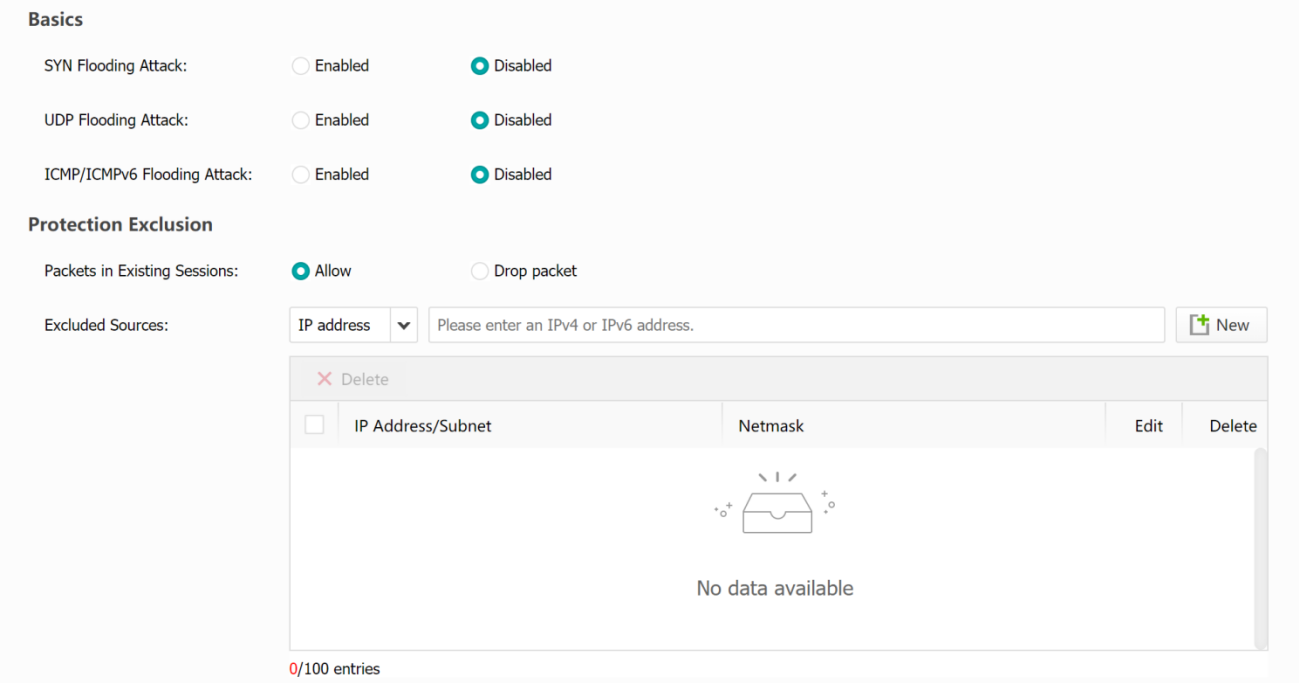
3.8.3 Anti-DOS(Outside Threat)

【Operation Scenarios】

Anti-DOS(Outside Threat) is generally used to protect the device against attacks from an external network (WAN port) and prevent service abnormalities caused by attacks launched by one or more computers on the external network. It is mainly used to prevent DDOS. If a device is specially deployed for securing the internal network, Anti-DOS(Outside Threat) may not be enabled.

【Operation Procedure】

『Network』-『Network Security』-『Anti-DOS(Outside Threat)』Set the protection parameters as required. Specific values of the parameters vary with the traffic volume, as shown in the following figure:



『SYN Flooding Attack』: detects data packets sent from a WAN interface and counts the number of SYN packets accessing the WAN interface address per second to determine if an attack has occurred. If the threshold is exceeded, subsequent TCP handles the proxy 3-way handshake and sends an alarm message to the log center. The 3-way handshake proxy will not stop until the number of SYN packets in a certain second falls below the threshold.

(1) [Threshold per Dst IP]: configures the limit of the number of SYN packets per second as required by the protection module.

『UDP Flooding Attack』: detects data packet sent from a WAN interface and counts the number of UDP packets accessing the WAN interface address per second to determine if an attack has occurred. If the threshold is exceeded, subsequent UDP packets will be dropped within the current second and an alarm message will be sent to the log center.

(1) [Threshold per Dst IP]: configures the limit of the number of UDP packets per second as required by the protection module.

(2) [Drop Empty Packet]: drops empty data packets. Drop all packets with a data length of zero without performing a threshold-dependent evaluation. You can also select and drop packets with a length being out of a specified range, or packets with a specified length. The implementation of these functions is similar to that of the function of dropping packets with a length of zero, that is, dropping packets directly without performing a threshold-dependent evaluation.

『ICMP Flooding Attack』: detects data packet sent from a WAN interface and counts the number of ICMP packets accessing the WAN interface address per second to determine if an attack has occurred. If the threshold is exceeded, subsequent ICMP packets will be dropped within the current second and an alarm message will be sent to the log center.

(1) [Threshold per Dst IP]: configures the limit of the number of ICMP packets per second as required by the protection module.

『Protection Exclusion』sets a list of source IP addresses that do not need to be prevented.

For『Packets in Existing Sessions』, when "Allow" is selected, packets with which connection has been established will not be prevented. If "Drop packet" is selected, packets of the node monitor using UDP and ICMP will be discarded without any backhaul. Therefore, it is recommended to select "Allow".

For『Excluded Sources』, when the source IP address of a data packet is included in the Excluded Sources list, it can directly PASS without any ICMP Flooding Attack, UDP Flooding Attack, and SYN Flooding Attack processing.

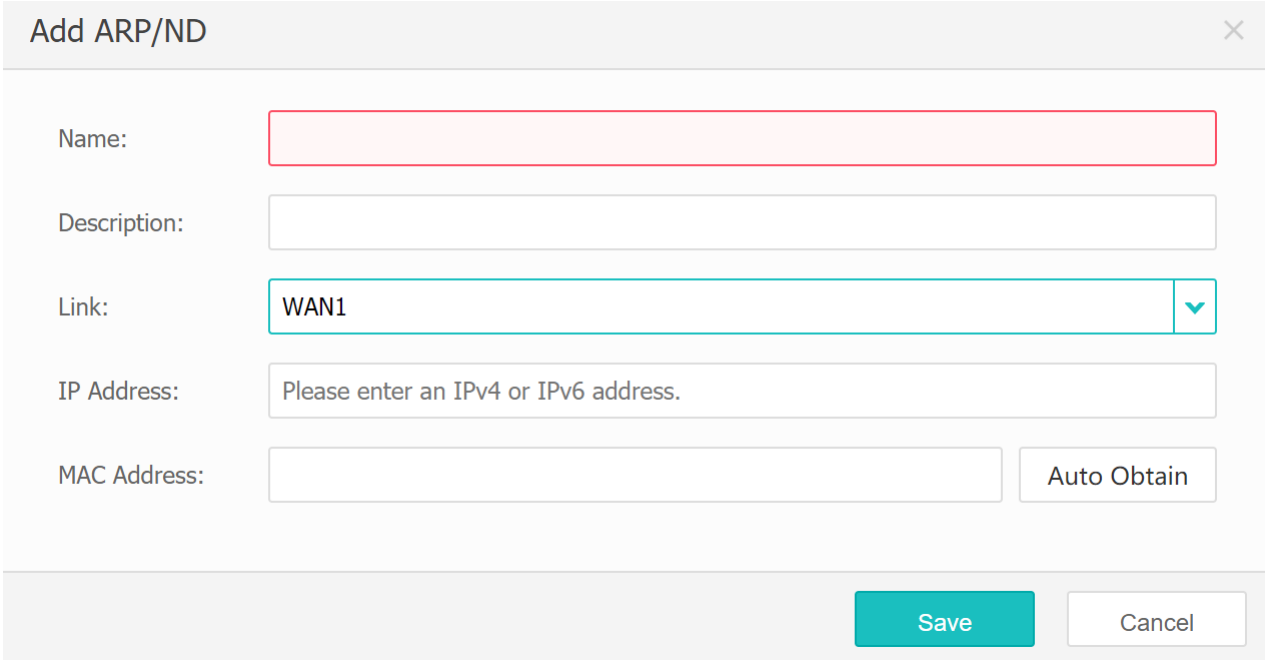
Notes: It is recommended to use the default value when the specific parameter value can not be determined based on the external network traffic volume, and then make appropriate adjustments according to the actual service conditions.

3.8.4 ARP/ND Protection

【Operation Scenarios】

【Operation Procedure】

Choose『Network』-『Network Security』- 『ARP/ND Protection』and click New. Configure Name, Link, IP Address, MAC Address, etc. to complete the configuration of an ARP entry, as shown in the following figure:



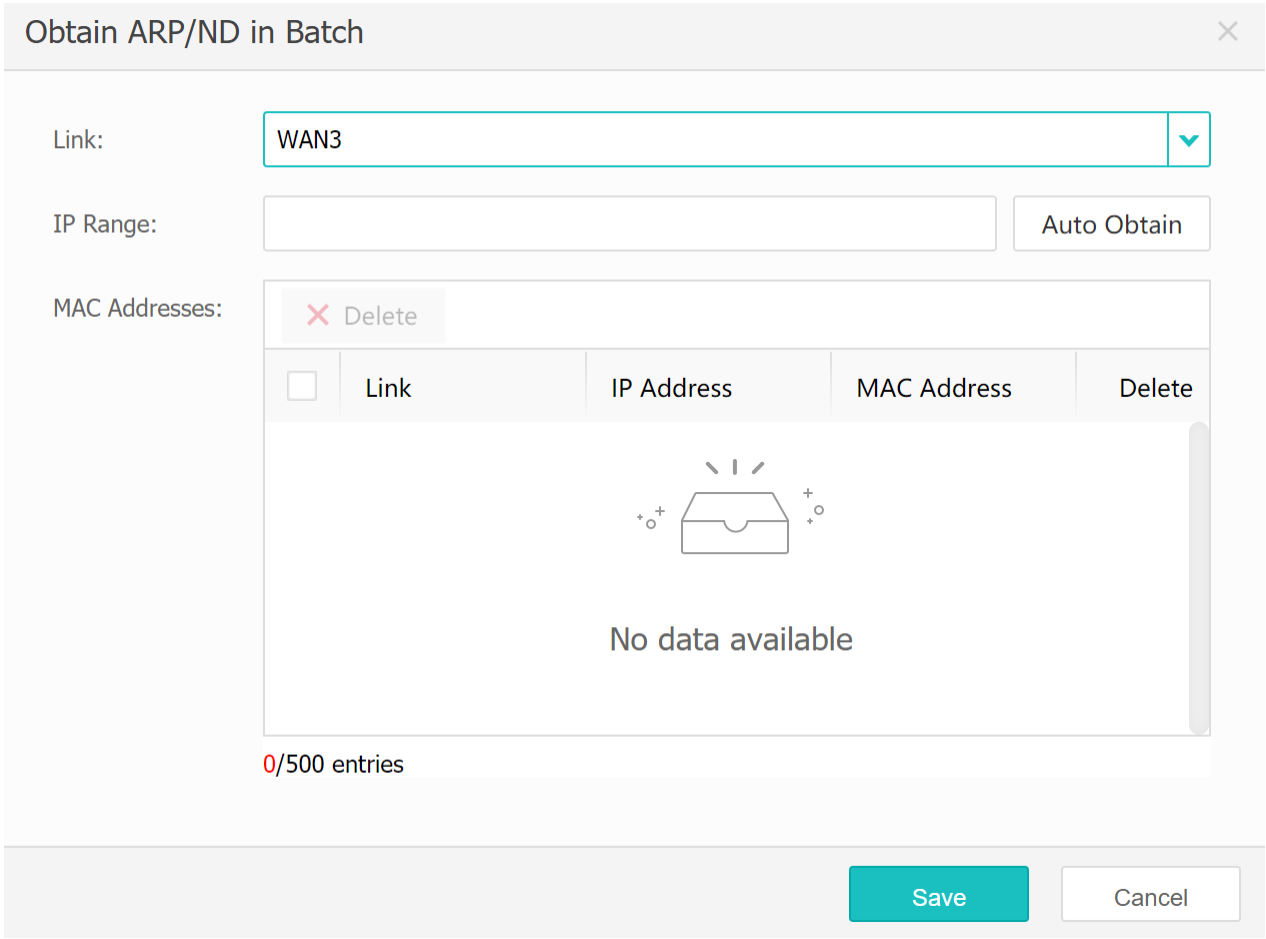
『Link』: sets the network interface for IP/MAC binding.

『IP Address』: sets the corresponding IP address information.

『MAC Address』: sets the MAC address information corresponding to the IP address configured above.

Click Auto Obtain to obtain the MAC address for the specified IP address. If the MAC address cannot be obtained, a prompt will be displayed indicating that the operation has failed.

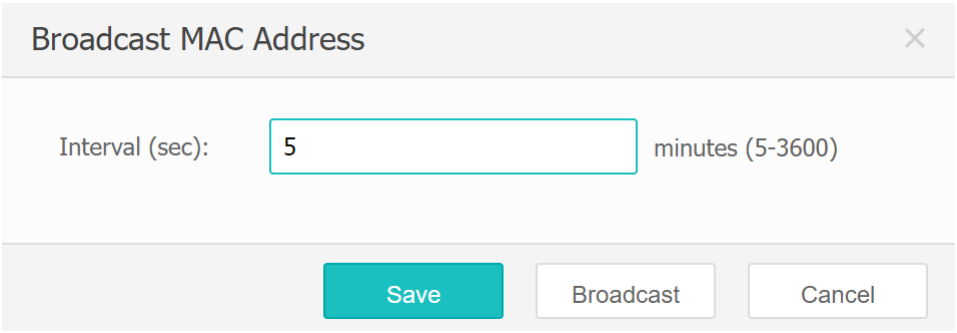
Obtain in Batch: If there are many objects to be bound and it is troublesome to set one by one, you can use the function of automatically obtaining MAC addresses provided by the ADC. Click Obtain in Batch to automatically scan the MAC addresses for a corresponding IP address segment. The configuration interface is shown below:



『IP Range』: Enter the [Initial IP] and [End IP] to be scanned. Click Auto Obtain and the device will obtain the MAC addresses for the corresponding IP address segment by sending ARP broadcasts.

『MAC Addresses』displays the scanned ARP information.

Click Broadcast Options to set the "Broadcast MAC Address".



『Interval (sec)』 configures the interval in minutes for the ADC gateway to send ARP broadcast packets. The value can be left as default without special requirements.

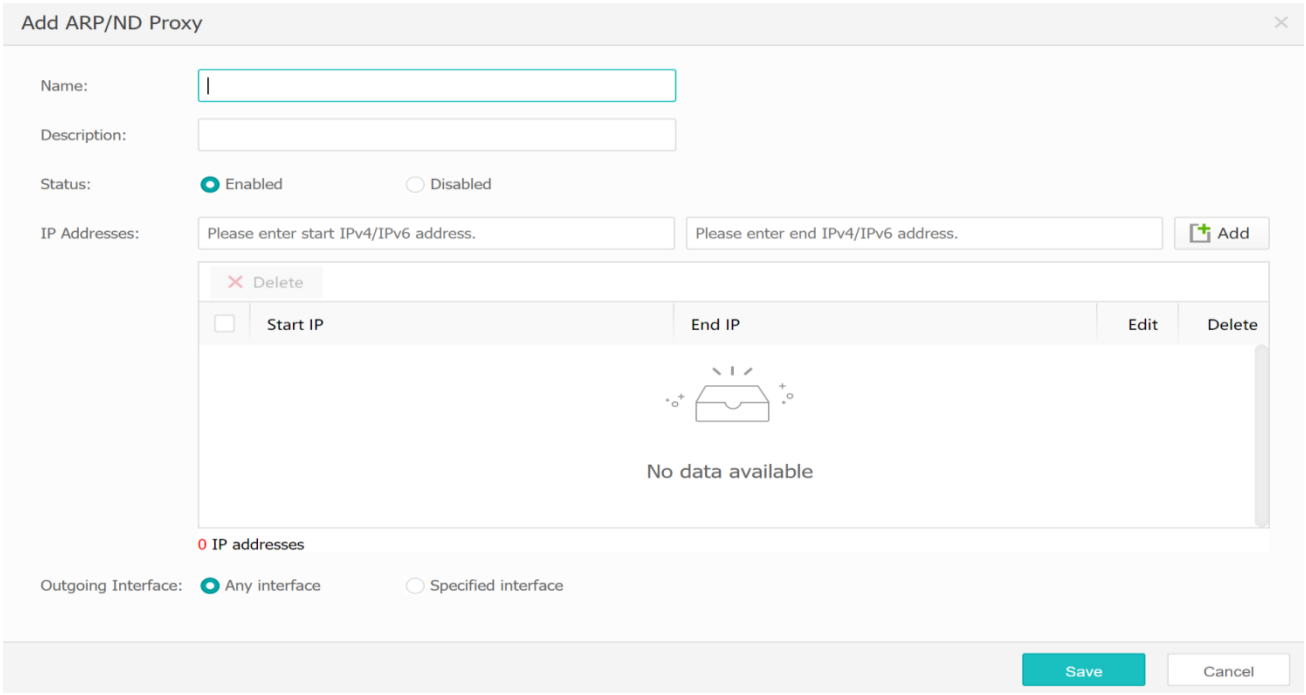
3.8.5 ARP Proxy

【Operation Scenarios】

ARP Proxy is generally used to send ARP requests by ADC as a proxy for intranet devices. For example, if a VIP publishing virtual service is not on the device interface, ADC will not respond to packets from this IP address if the peer device does not have a clear route to ADC, but ADC can respond if ARP proxy is enabled on it.

【Operation Procedure】

『Network』-『Network Security』-『ARP/ND Proxy』and click New. Configure Name, IP Addresses and Outgoing Interface, etc. to complete the configuration of ARP Proxy, as shown in the following figure:



『IP Addresses』 manually adds IP addresses to the address list.

『Outgoing Interface』 matches the outgoing interface of data when this ARP proxy is used. Multiple outgoing interfaces can be selected in one configuration. [Any interface]: selects the destination MAC of ARP response according to the ingoing interface of ARP request; [Specified interface]: specifies the service interface.

Chapter 4 System

【Operation Scenarios】

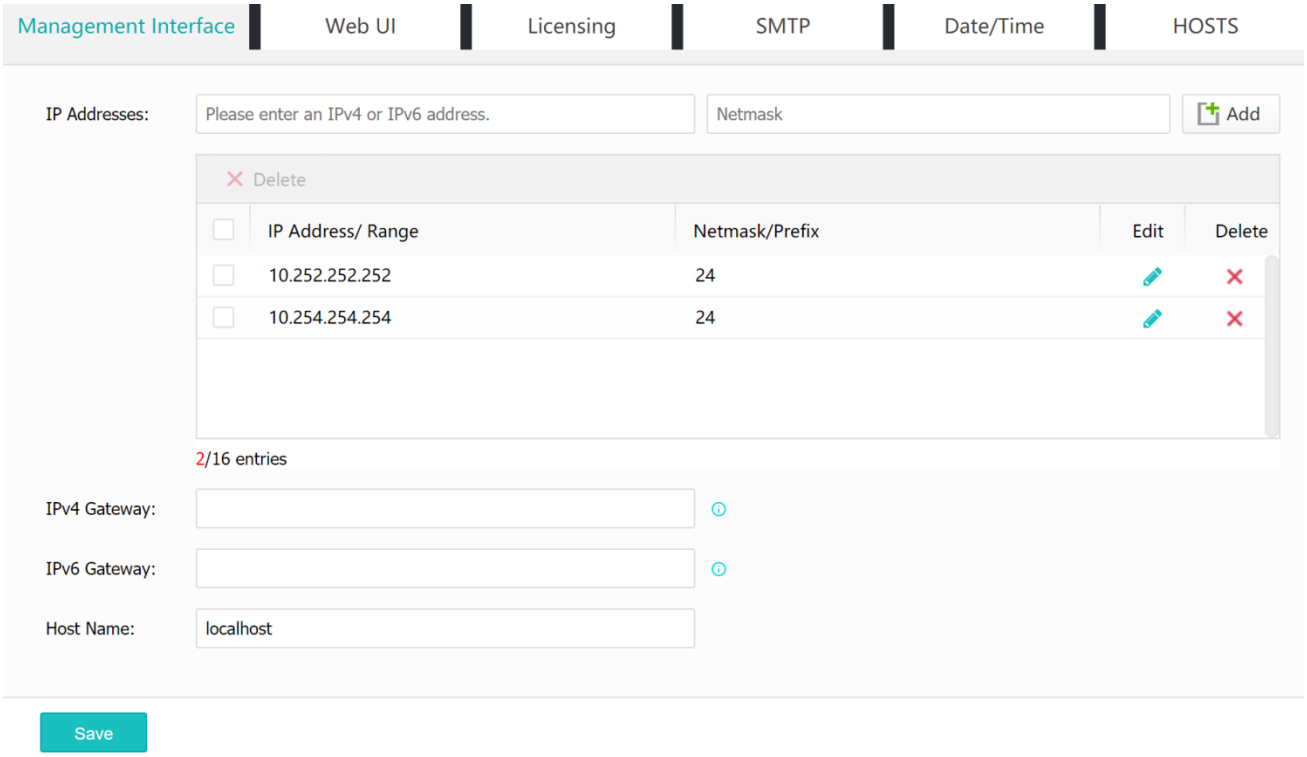
System is used to configure the system information of the device and to manage and maintain the device. Specific modules include 『General』, 『Administrators』, 『SNMP』, 『Alarm Options』, 『Maintenance』, 『Troubleshooting』 and 『Report Options』.

4.1 General

4.1.1 Management Interface

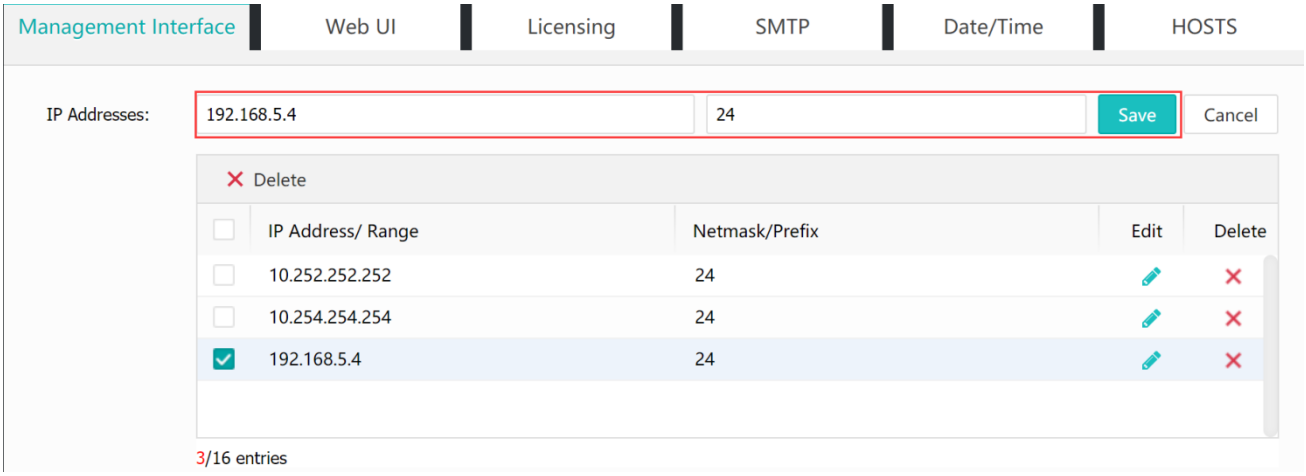
【Operation Scenarios】

Management Interface is used to set the management IP address, gateway, name of the active device, and other information for the ADC management interface. The page is shown in the figure below:



【Operation Procedure】

『System』-『General』-『Management Interface』, enter [IP Address] and [Netmask] in the『IP Addresses』, and click Add to add the IP address to the address list. Click the Edit button corresponding to the IP address in the address list to modify and update the IP information, and click Save after the modification is finished. Click to delete the IP information of the corresponding row.



『IPv4/IPv6 Gateway』is used to set the gateway information of the management interface on the ADC. The management gateway IP address must be in the same network segment as the management interface IP address.

『Host Name』sets the name of the ADC. Note that Chinese characters are not supported.

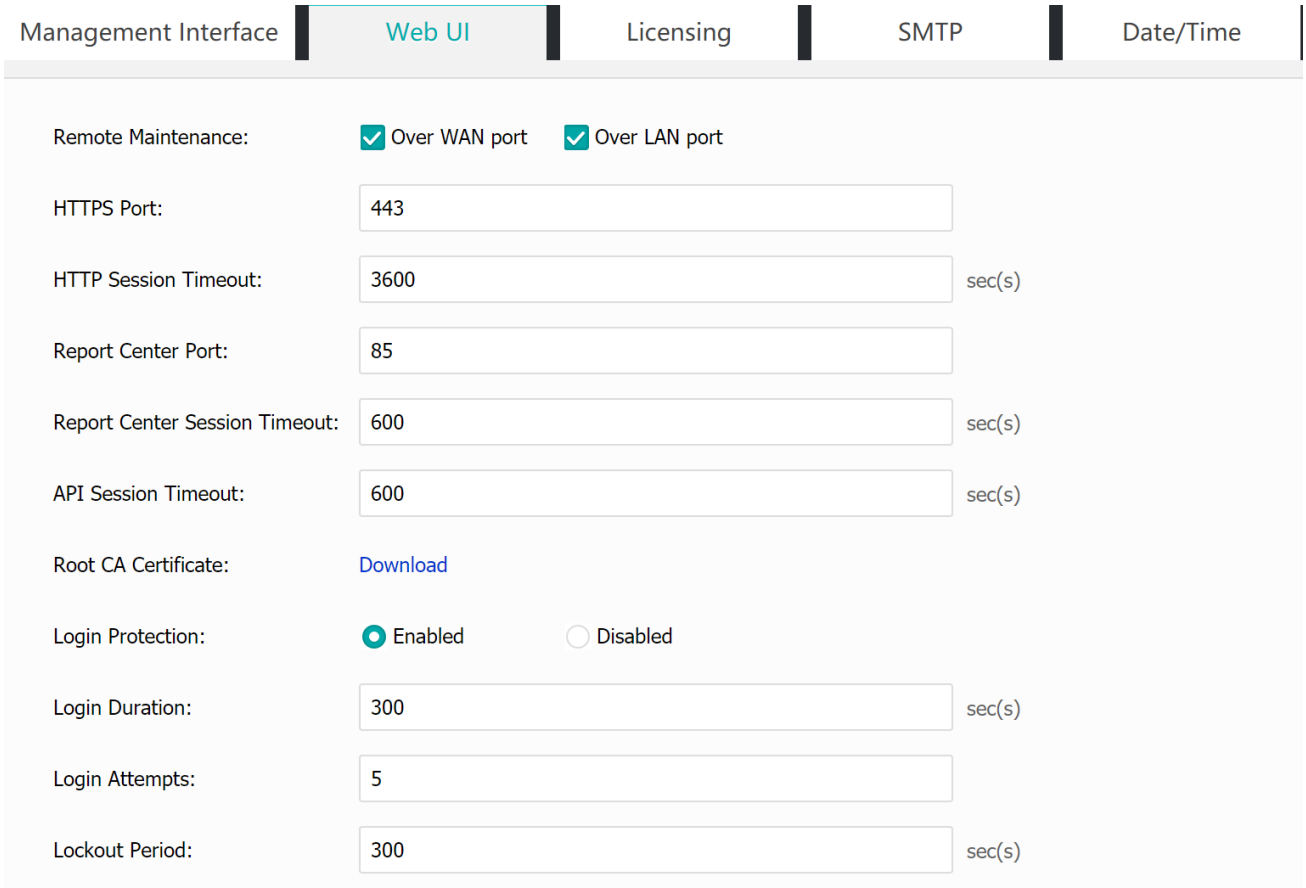
4.1.2 Web UI

【Operation Scenarios】

Web UI is used to set the Web console login port, Remote Maintenance, Session Timeout, Report Center Port, and other Web interface-related configurations.

【Operation Procedure】

Navigate through『System』-『General』-『WebUI』, the interface is shown in the figure below:



『Remote Maintenance』 sets whether to enable remote maintenance of ADC. You can choose to allow access to the device through the WAN/LAN port and manage it.

『HTTPS Port』 sets the login port for logging into the console page of the ADC and the default is port 443; you can change it to other ports if needed.

『HTTP Session Timeout』 sets the controlled timeout for console users. In general, this parameter is left as default.

『Report Center Port』 sets the port used to connect to the report server and the default is port 85. In general, this parameter is left as default.

『Report Center Session Timeout』 configures the session timeout for the login user in the report data center. If you do not perform any operation within this timeout, the session will be cleared and you need to log in again. In general, this parameter is left as default.

『API Session Timeout』 sets the API session timeout. In general, this parameter is left as default.

『Root CA Certificate』 downloads the root certificate for logging in to the console, which can be imported into the browser, and the login console will no longer prompt the certificate error.

『Login Protection』sets the allowable attempts and time limit of wrong input of username and password during user login. When [Enabled] is checked, there are three menu items to set: [Login Duration] sets the time range for accumulating the times of failures after the first login failure. The default value is 300s. [Login Attempts] is the number of allowable login failures. The default value is 5. [Lockout Period] refers to the period during which the login request from the client IP address will be rejected after reaching the threshold of login failures. The default time is 300s. (i.e., if the number of login failures is equal to 5 times within 300s after the first login failure, the client IP will be unable to log in to the console within the lockout time of 300s).

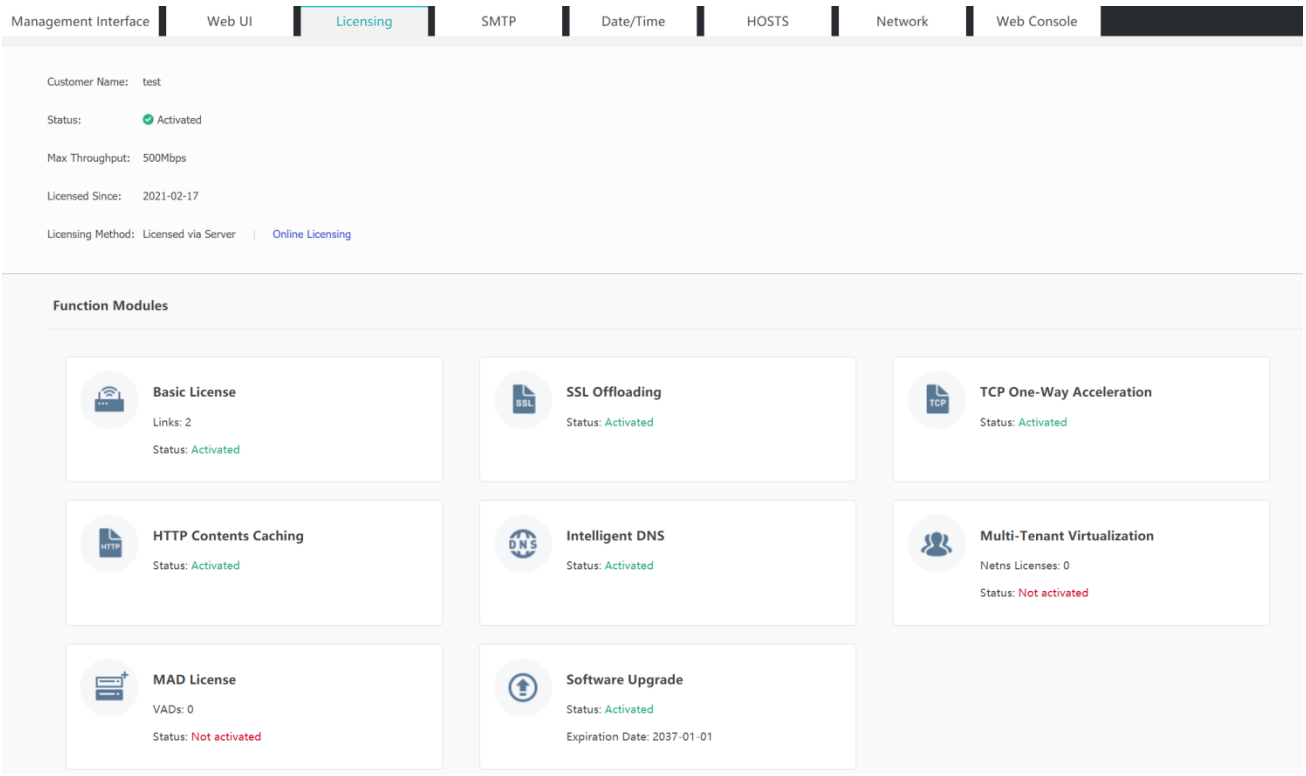
4.1.3 Licensing

【Operation Scenarios】

Licensing is used to authorize the device. The device can only enable certain functional items after acquiring relevant authorizations. Different serial numbers correspond to different functional modules.

【Operation Procedure】

Navigate through『System』-『General』-『Licensing』, the interface is shown in the figure below:



『Customer Name』displays the name of the customer who owns this device.

『Basic License』activates the basic license serial number to use the main functions provided by the ADC (such as app load balancing, link load balancing, etc.). The number of links shows the maximum number of external links, i.e. WAN category interfaces, supported by this ADC.

『SSL Offloading』activates the SSL Offloading serial number to configure SSL-related virtual services.

『TCP One-Way Acceleration』activates the TCP One-Way Acceleration serial number to enable the TCP One-Way Acceleration of virtual services.

『HTTP Contents Caching』activates the HTTP Contents Caching serial number to enable the HTTP caching and HTTP compression of the virtual service optimization policy.

『Intelligent DNS』activates Intelligent DNS serial number to enable global configuration reset, site collection, and other global-related functions.

『Multi-Tenant Virtualization』 shows the serial number limit for the number of OpenAD net-ns.

『MAD License』 shows the number of VADs that can be created under MAD.

『Software Upgrade』 allows you to upgrade the software system. The Software Upgrade serial number is only valid for a certain period of time and you cannot upgrade the system software after the expiration date.

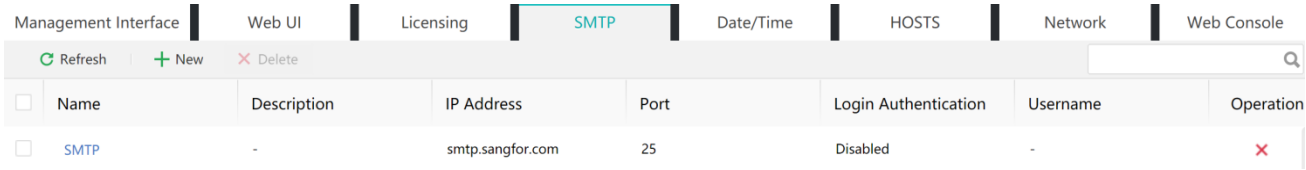
4.1.4 SMTP

【Operation Scenarios】

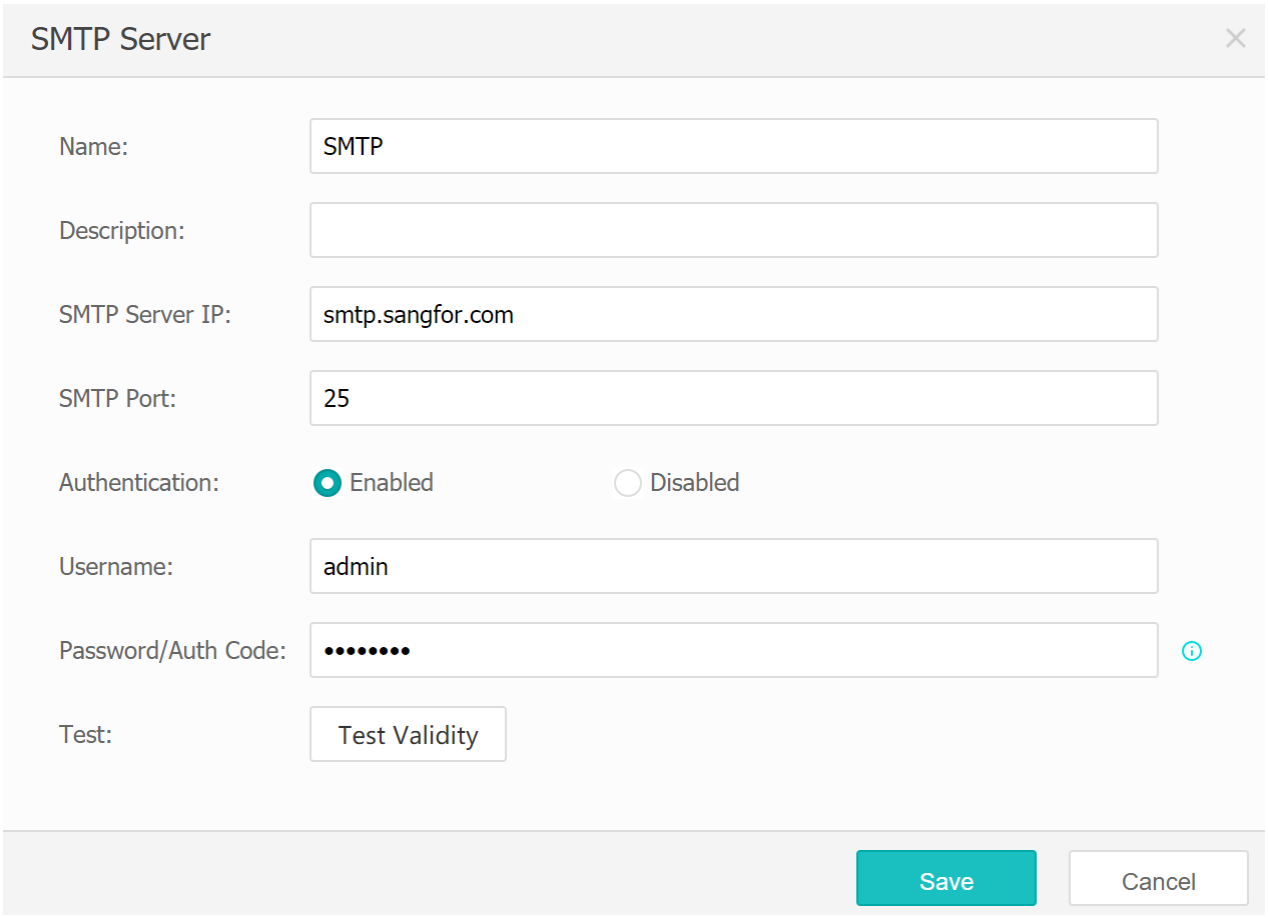
SMTP is used to set SMTP server information, and the SMTP server settings here are mainly used by 『EMAIL Alarm』 and 『Automatic Report Generation』, etc.

【Operation Procedure】

Navigate through 『System』 - 『General』 - 『SMTP』, the interface is shown in the figure below:



Click New to open the [SMTP Server] window and the setting page is as follows: you need to set the Name, SMTP Server IP, SMTP Port and choose whether to authenticate the username and password.



『SMTP Server IP』 sets the SMTP server IP address. You can fill in the IP address or domain name address here.

『SMTP Port』 sets the port used for SMTP and the default is port 25.

If the SMTP server needs to verify the username and password, you need to check [Enabled] to verify the username and password. Just enter [Username] and [Password/Auth Code].

『Test』 can assist in testing whether the configured SMTP server is valid or not, and the accuracy of the test is higher when the network condition is good. Click Test Validity to start the test.

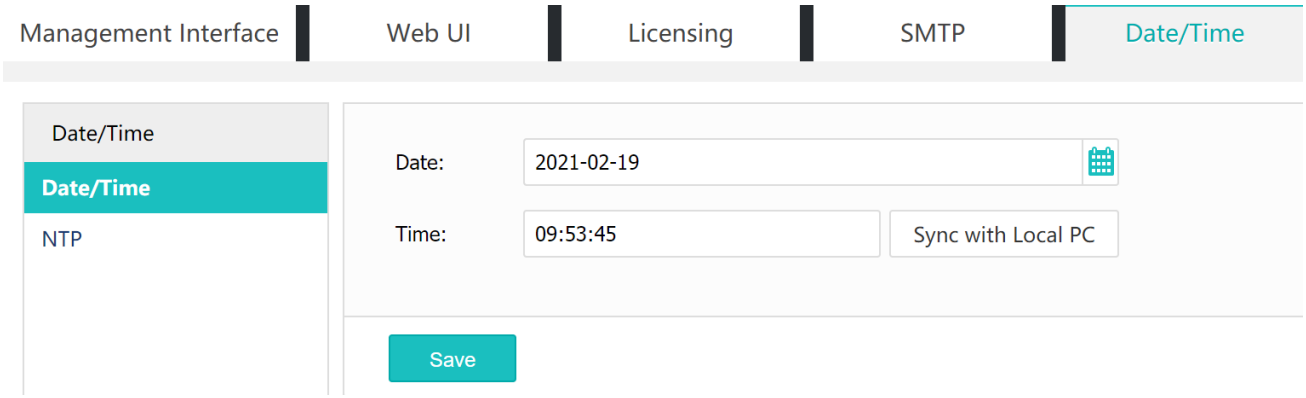
4.1.5 Date/Time

【Operation Scenarios】

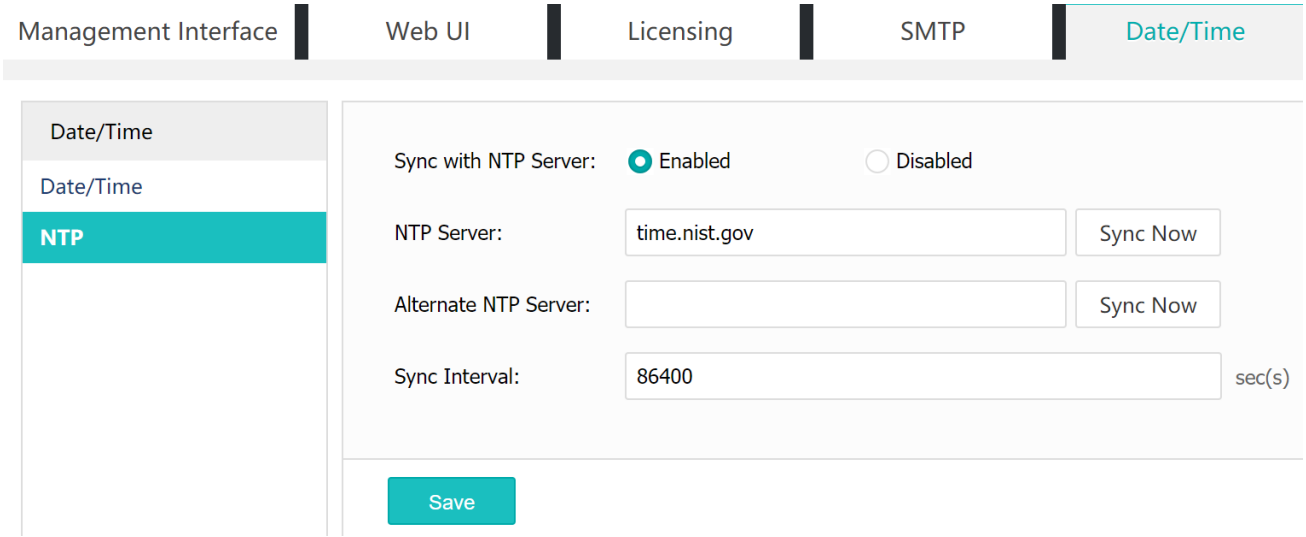
It is used to set the system time of the ADC.

【Operation Procedure】

Navigate through『System』-『General』-『Date/Time』for setting. The interface is shown in the figure below:



Click Sync with Local PC to synchronize the system time of the device with the system time of the computer used for logging in to the console.



Select [Enabled] for『Sync with NTP Server』, and the time will be automatically synchronized with the NTP Server.

Fill in『NTP Server』with the INTERNET NTP server.

Fill in『Alternate NTP Server』with the backup INTERNET NTP server.

Sync Now is used to synchronize the device's system time with the time of the NTP server immediately.

『Sync Interval』is the interval set for the time synchronization between the device and the network.

If the updated time is later than the original time, the data generated within a certain period of time will not be recorded. If the updated time is before the original time, the minute view and hour view in the report are displayed with the latest data, and the day view and month view in the report are displayed with the result of data overlay.

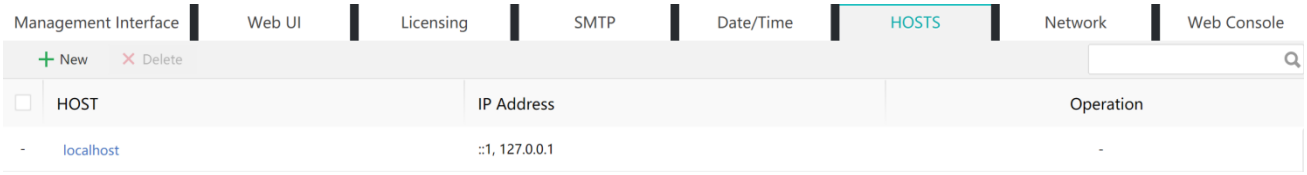
4.1.6 HOSTS

【Operation Scenarios】

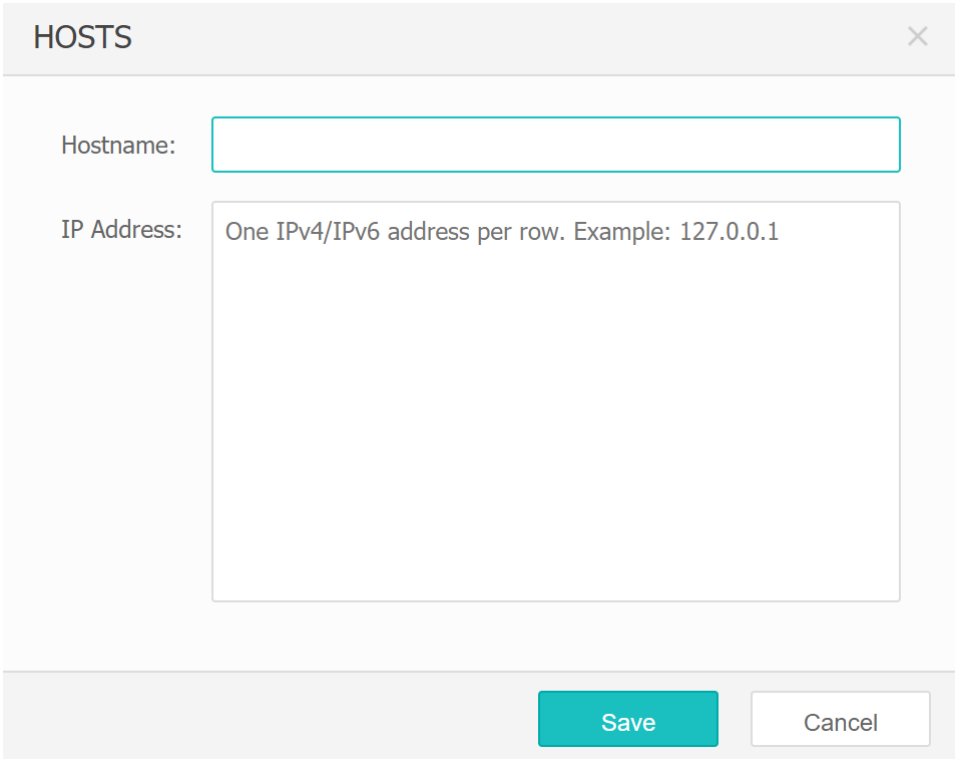
HOSTS is used to set the HOST table of the ADC, which is used for performing domain name resolution when the device itself accesses the domain name.

【Operation Procedure】

Navigate through『System』-『General』-『HOSTS』, the interface is shown in the figure below:



Click New to create a new hosts entry and open the 【HOSTS】window



『Hostname』sets the domain name or hostname.

『IP Address』sets the IP address corresponding to the hostname set above.

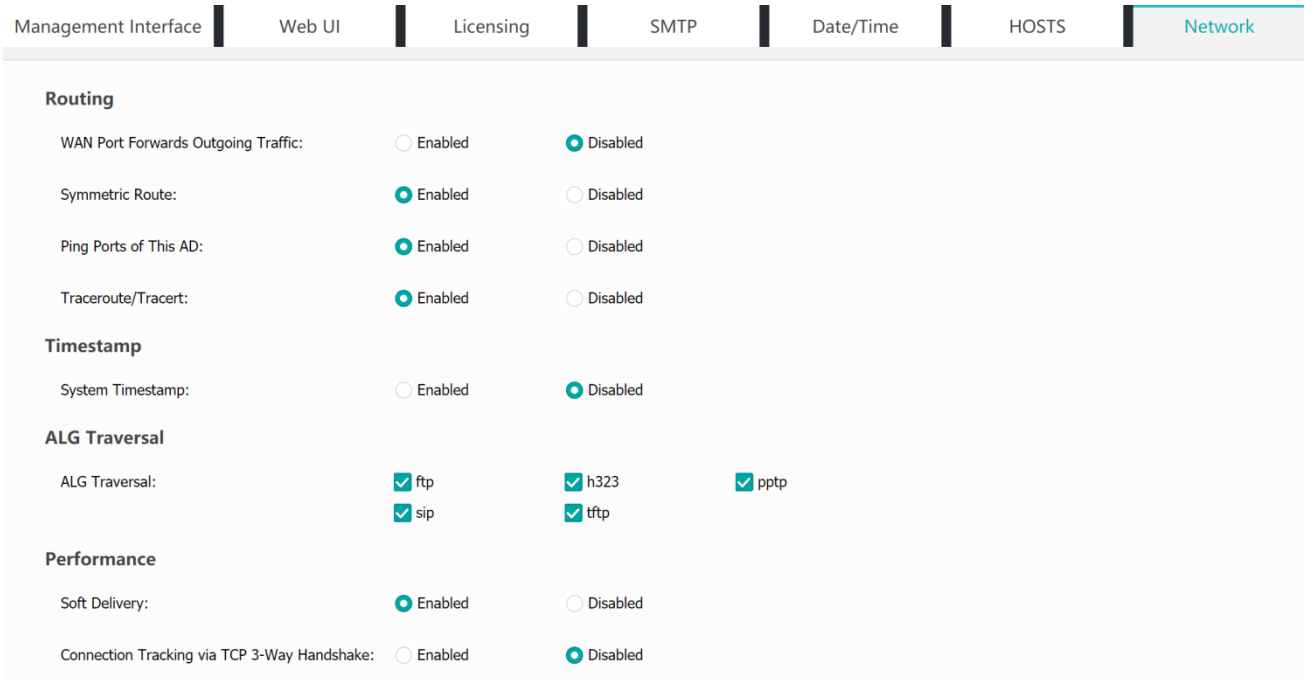
4.1.7 Network

【Operation Scenarios】

Network is used to set the network parameters of the ADC, and the parameters of some network functions of the device, such as device routing and forwarding, number of connections, and other functional settings.

【Operation Procedure】

Navigate through『System』-『General』-『Network』, the interface is shown in the figure below:



For『WAN Port Forwards Outgoing Traffic』, if the WAN Port Forwards Outgoing Traffic is Disabled, the data transfer between WAN and LAN ports is not possible except for virtual services, DNS, SNAT, port mapping, remote login, matching Policy-Based Routing or static routing. Data transmission can only be carried out after WAN Port Forwards Outgoing Traffic is Enabled. Enable this function only if you need to log in to the device console by using a WAN interface address.

Enable『Symmetric Route』to look up routing tables in the original direction only; disable Symmetric Route to look up routes and forward data independently in both directions for the same connection. It is generally recommended to be enabled to ensure the same data path to and from the device.

Enable『Ping Ports of This ADC』to allow responding to a ping request from the WAN port; disabled, not to respond.

『Traceroute/Tracert』is enabled to allow the local device to be exposed to the traceroute path; disabled to hide the device from the traceroute path (traceroute messages can pass through the device). Generally, it is recommended to disable it when there is no special requirement.

『Connection Count Method』shows the connection counting status of the whole system. You can choose [Count All Statuses], or [Count ESTABLISHED Status Connections]. The specific choice of counting method depends on the specific needs.

『Connection Limitation Type』shows the connection limitation types of the whole system. You can choose [Limit for Each Source IP] or [Limit for All IPs under the Rule].

『System Timestamp』sets whether to enable timestamp for ADC active packet sending. Generally, it can be disabled.

『ALG Traversal』supports to enable or disable the traversal of [ftp], [h323], [pptp], [sip] and [tftp] on the interface.

『Soft Delivery』improves CPU usage after being enabled.

If『Connection Tracking via TCP 3-Way Handshake』is disabled, all TCP data is allowed to be connected to the device.

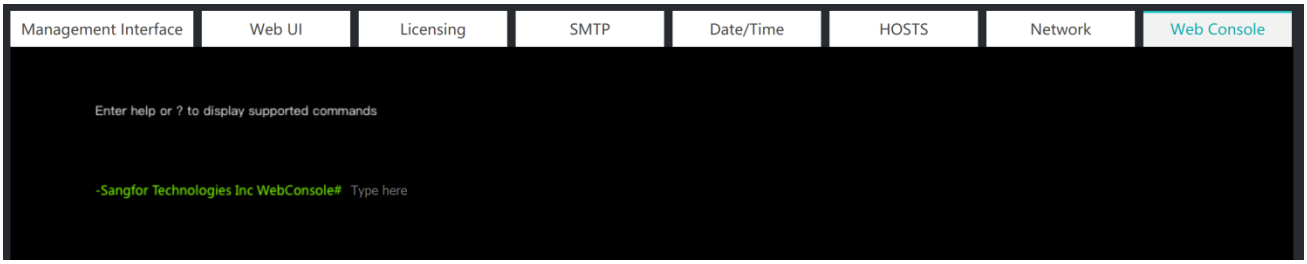
4.1.8 WebConsole

【Operation Scenarios】

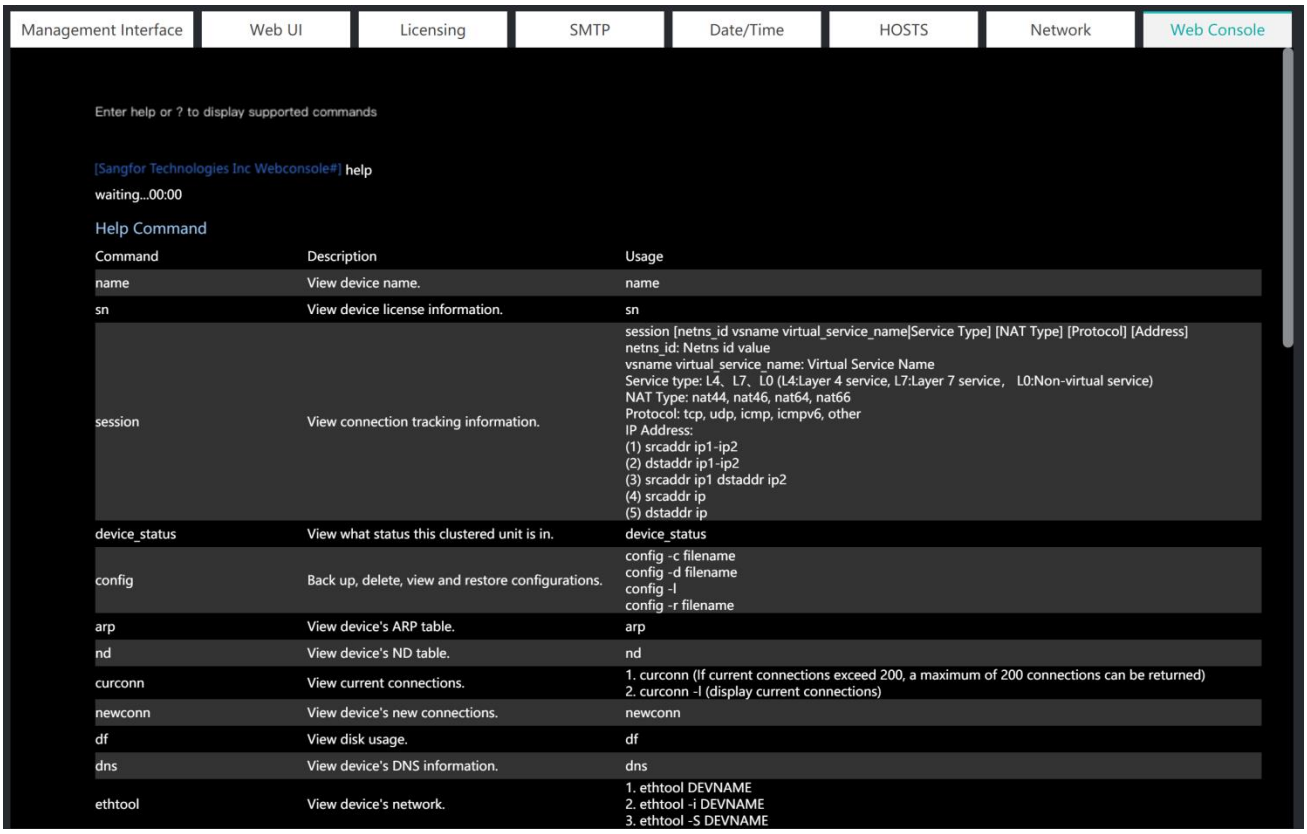
WebConsole is used to allow customers to perform command line operations and view some basic information about the background through the Web page.

【Operation Procedure】

Navigate through『System』-『General』-『Web Console』, the interface is shown in the figure below:



『Help Command』 lists the commands supported by WebConsole and the functions of the commands. Enter a command help or ? after [Sangfor Technologies Inc Webconsole#] at the bottom of the page, and press Enter to view the corresponding information of the system. The page is shown in the figure below:



Command	Description	Usage
name	View device name.	name
sn	View device license information.	sn
session	View connection tracking information.	session [netns_id vsname virtual_service_name|Service Type] [NAT Type] [Protocol] [Address] netns_id: Netns id value vsname virtual_service_name: Virtual Service Name Service type: L4、L7、L0 (L4:Layer 4 service, L7:Layer 7 service， L0:Non-virtual service) NAT Type: nat44, nat46, nat64, nat66 Protocol: tcp, udp, icmp, icmpv6, other IP Address: (1) srcaddr ip1-ip2 (2) dstaddr ip1-ip2 (3) srcaddr ip1 dstaddr ip2 (4) srcaddr ip (5) dstaddr ip
device_status	View what status this clustered unit is in.	device_status
config	Back up, delete, view and restore configurations.	config -c filename config -d filename config -l config -r filename
arp	View device's ARP table.	arp
nd	View device's ND table.	nd
curconn	View current connections.	1. curconn (If current connections exceed 200, a maximum of 200 connections can be returned) 2. curconn -l (display current connections)
newconn	View device's new connections.	newconn
df	View disk usage.	df
dns	View device's DNS information.	dns
ethtool	View device's network.	1. ethtool DEVNAME 2. ethtool -i DEVNAME 3. ethtool -S DEVNAME

4.2 Administrators

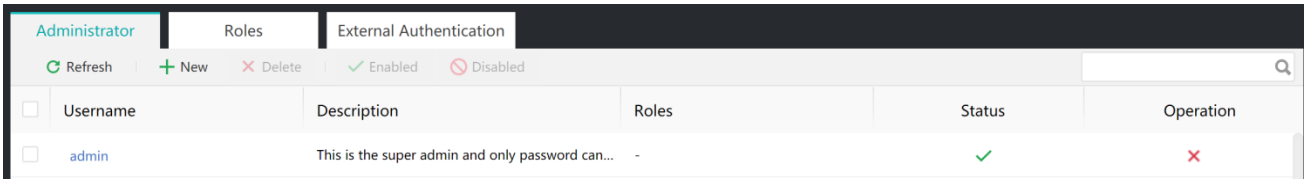
4.2.1 Administrator

【Operation Scenarios】

Administrator is generally used to set the login user who can manage ADC hardware devices by controlling the console.

【Operation Procedure】

Navigate through『System』→『Administrators』→『Administrator』, the interface is shown in the figure below:



『Administrator』displays the console users that have been set up and the roles they belong to.

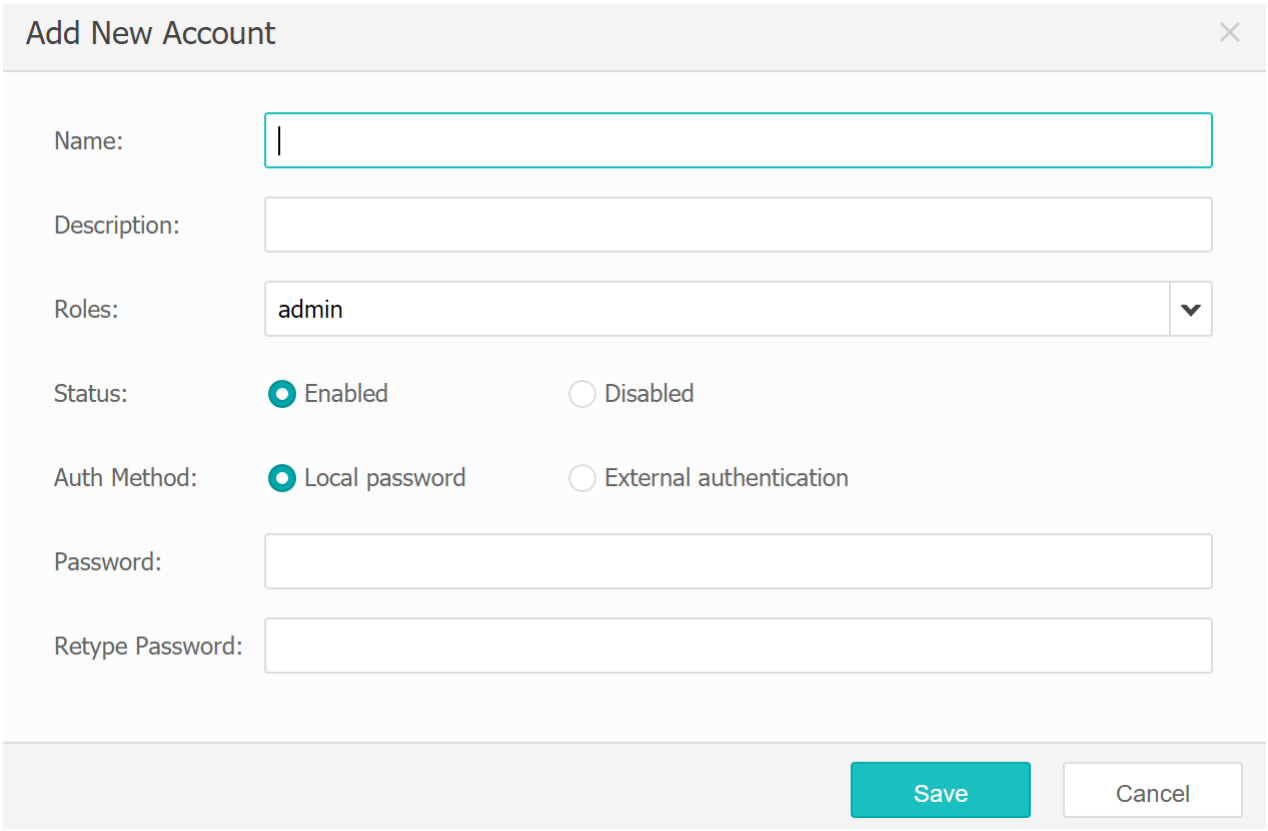
[Enabled]/[Disabled]: enables/disables the selected console user.

[Delete]: deletes the selected console user.

Click a username to modify the corresponding Name, Roles, and Password.

Click New at the top right of『Administrator』to create a new console user.

The configuration interface is shown as follows:



『Roles』 selects the role to which the user belongs.

『Auth Method』 provides two options: [Local Password] and [External Authentication].

『Password』 sets the user's login password.

『Retype Password』 confirms the user's login password, which shall be consistent with the password set in 『Password』 .

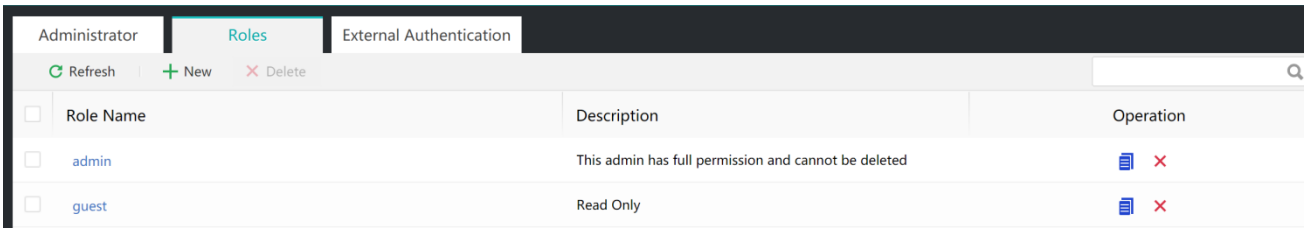
4.2.2 Roles

【Operation Scenarios】

The role used by the console user shall be determined before the console user is created. 『Roles』 sets different control privileges and other related configurations.

【Operation Procedure】

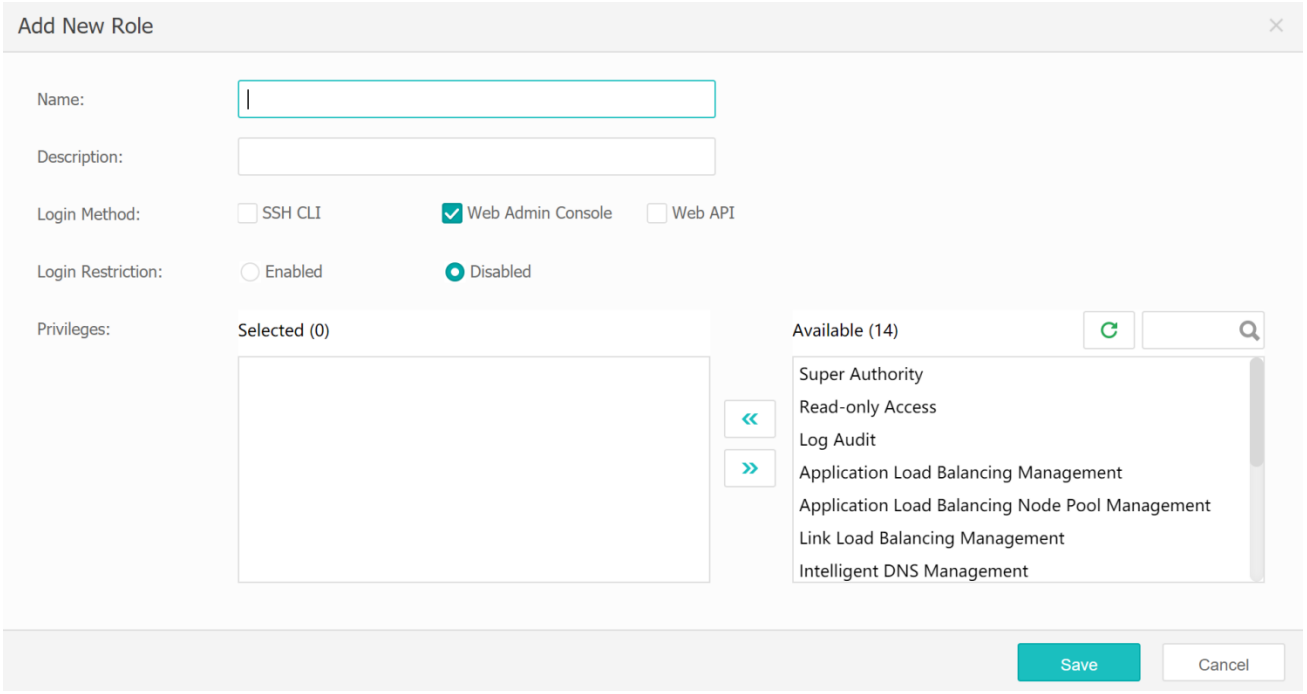
Navigate through『System』→『Administrators』→『Roles』, the interface is shown as the following figure:



『Roles』displays the roles of the console users that have been set.

[Delete]: deletes the selected console user.

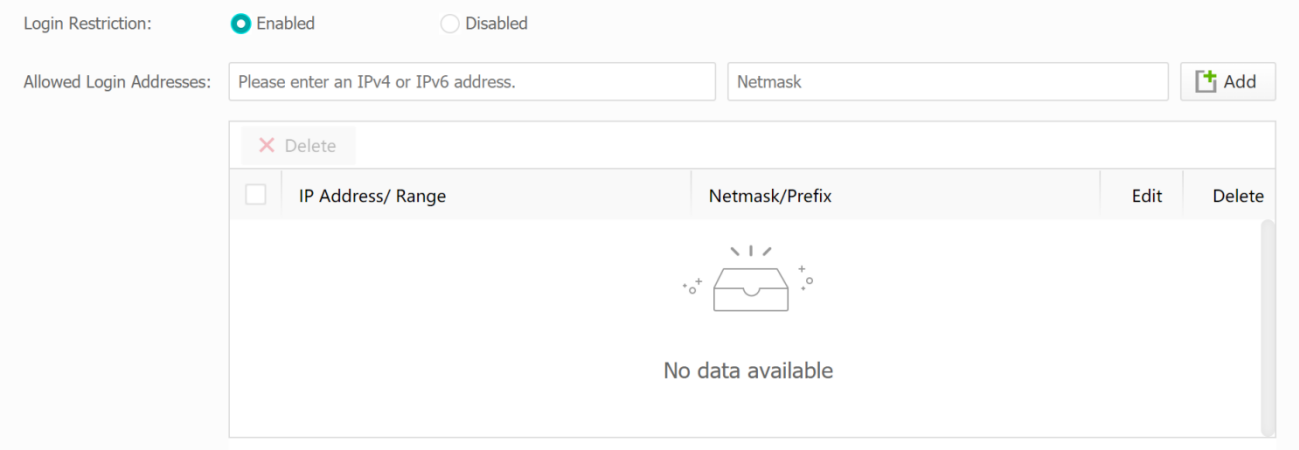
Click New at the top right of『Roles』to create a new console user. 【Add New Role】configuration interface is shown as follows:



『Login Method』sets the login method for a role. [SSH CLI], [Web Admin Console], and [Web API] are available options.

『Login Restriction』sets whether to restrict the IP address for logging in used by console users who log in with this role.

Check [Enabled] to enable the restricted IP address login for this role.



『Allowed Login Addresses』 sets the IP addresses. Fill in the IP address and subnet mask, and click Add to set a login IP address.

『Privileges』 sets the privileges assigned to different console roles. The privileges that can be set include: [Super Authority], [Read-only Access], [Log Audit], [App Load Balancing Management], [App Load Balancing Node Pool Management], [Link Load Balancing Management], [Intelligent DNS Management], [Intelligent DNS Domain Name Management], [Certificate Management], [Rule Resource Library Management], [Network Deployment Management], [High Availability Management], [System], and [Report Center].

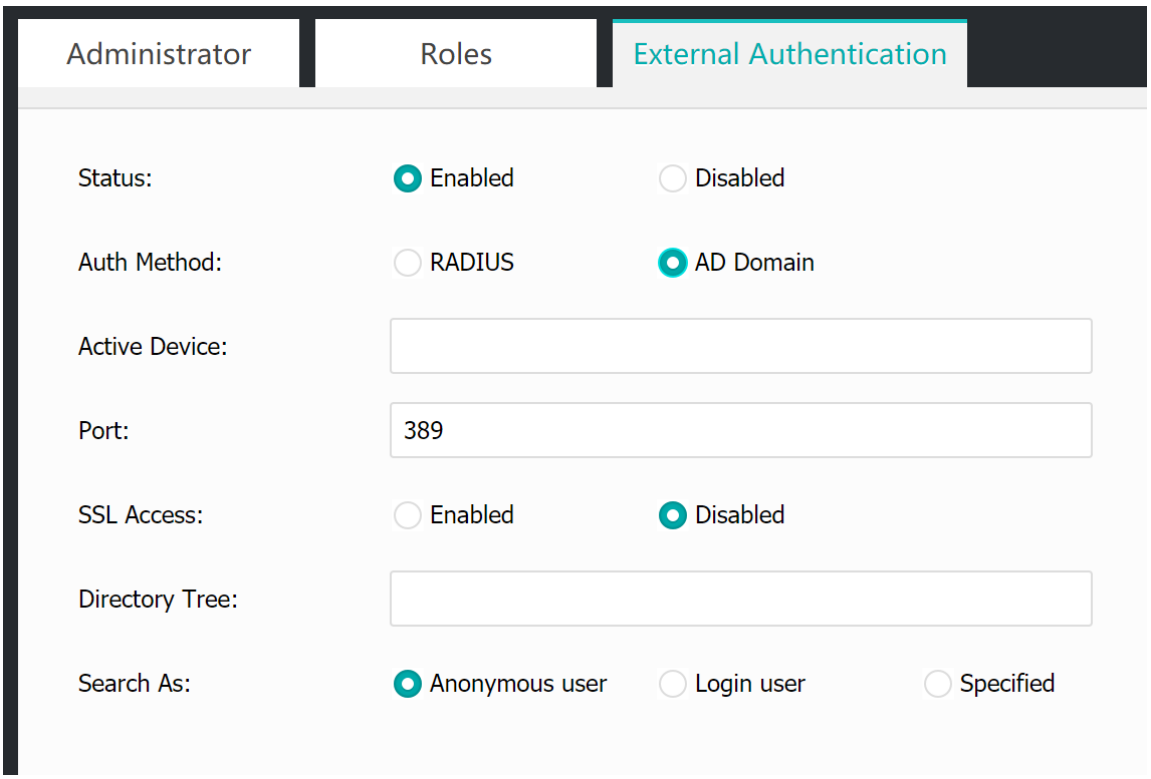
4.2.3 External Authentication

【Operation Scenarios】

External Authentication is generally used to configure the WebConsole to support "External Authentication". RADIUS and AD Domain are optional methods.

【Operation Procedure】

Navigate through 『System』 → 『Administrators』 → 『External Authentication』, the interface is shown in the figure below:



『Enabled/Disabled』: enables/disables external authentication login.

『Auth Method』: selects the type of external authentication server according to the actual situation. RADIUS and AD Domain are optional methods.

『Active Device』: IP address of the server.

『Port』: port of the server.

When [RADIUS] is selected:

『Shared Key』: refers to the "shared key" for communication between the server and the client.

『Authorization Attribute ID』: refers to the identifiers of RADIUS attributes. 56 kinds of attribute identifiers are built-in, and the ID can be customized.

When [AD Domain] is selected:

『SSL Access』: selects whether to enable SSL access, which is disabled by default.

『Directory Tree』: refers to the starting point of a search path. A non-SSL server can select from the list if it gets the directory tree successfully.

『Search As』: configures the way to initiate the first binding to the server, and the default mode is Anonymous user. The available options are [Anonymous user], [Login user] and [Specified].

『Username Extension』needs to be configured when [Login user] is selected for Search As:

『Username Extension』: needs to be configured when "Login user" is selected. For example, if this field is configured as ${user}@sangfor.com, then ${user} will be replaced with the username used to log in.

『DN』and『Password』need to be configured when [Specified] is selected:

『DN』: the system uses the domain user entered here to read the user information on LDAP. The domain user entered here must have sufficient privileges, for example, an LDAP administrator. The username here needs to be filled in with a full DN name. The exception is that when MS Active Directory is used, it can be written as user@domain.

『Password』: enters the password used by the domain user.

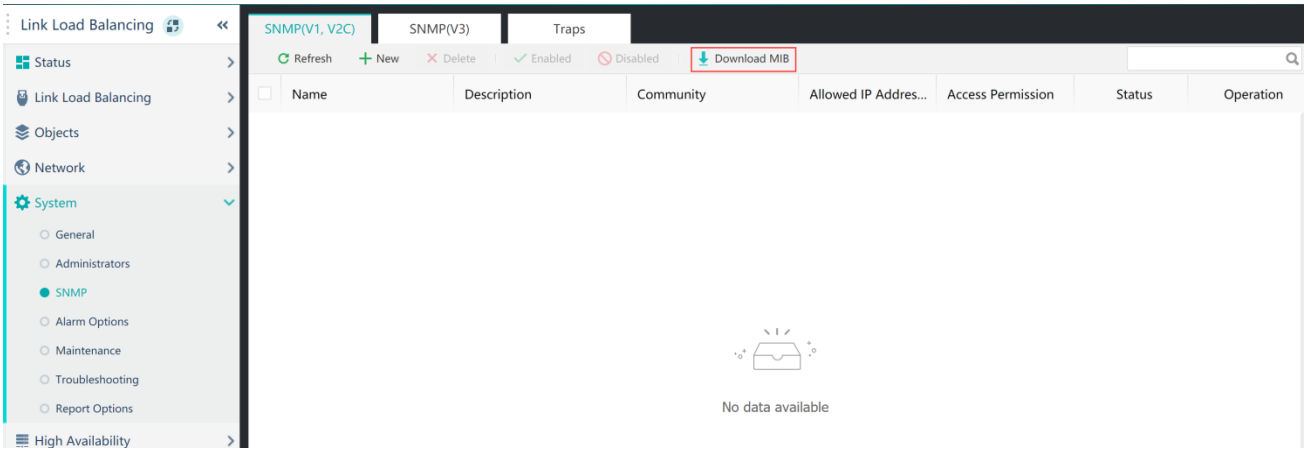
4.3 SNMP

【Operation Scenarios】

SNMP is generally used to set the SNMP information of the ADC, which is mainly used by the network management device to obtain some status information of the ADC through SNMP, such as CPU usage, memory, network card interface status, etc.

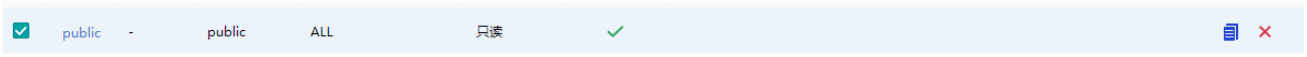
【Operation Procedure】

The configuration page is shown as follows:



Click Download MIB to download the MIB library files used by the device and save them to the local PC.

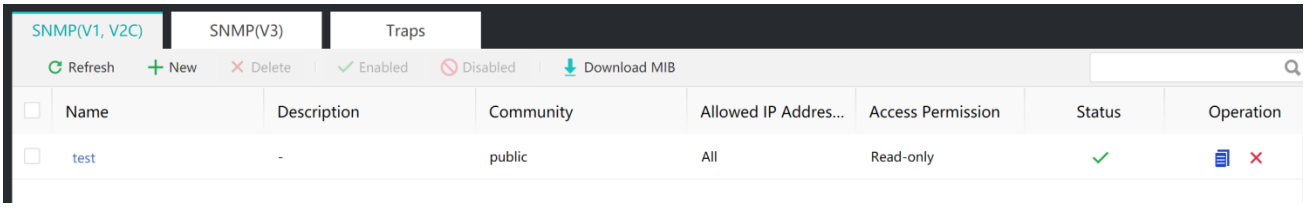
Click  on the right side of the configuration list to copy the selected configuration items.



4.3.1 SNMP(V1,V2C)

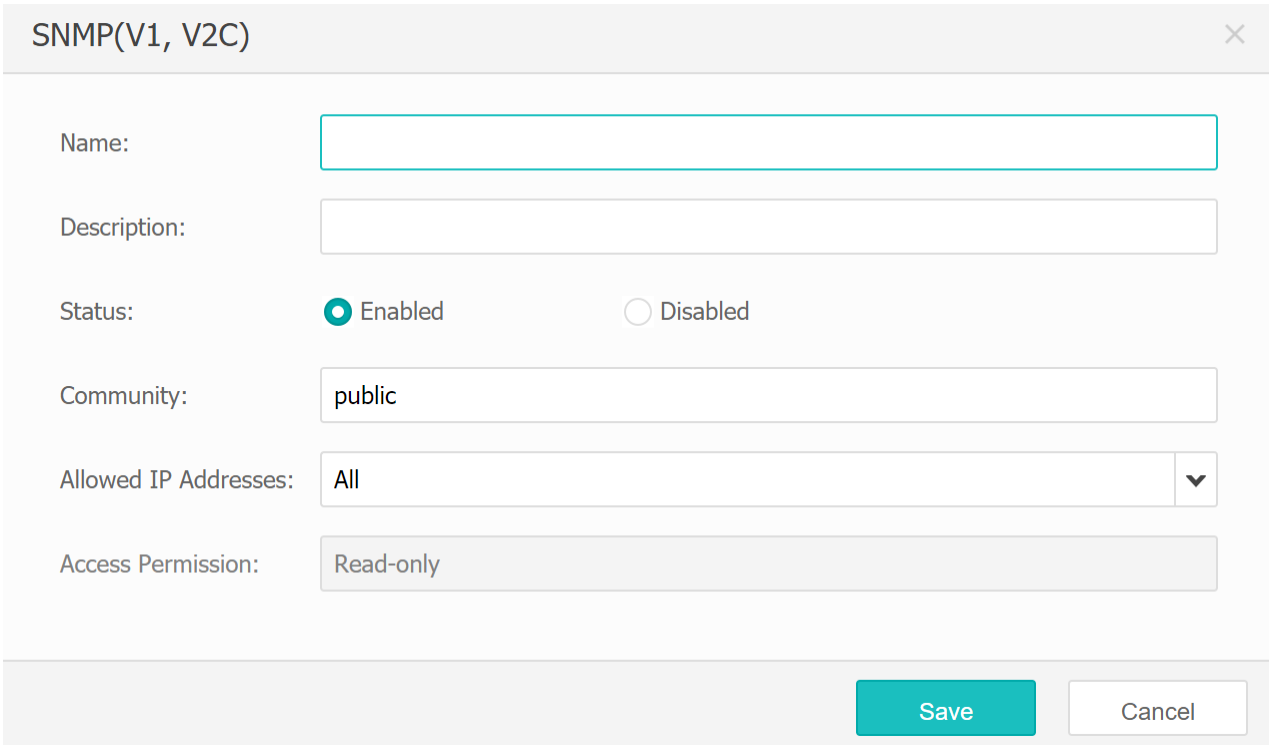
【Operation Scenarios】

SNMP(V1,V2C) is generally used to set the parameters for obtaining device information through SNMP V1 or V2C. The interface is shown as follows:



【Operation Procedure】

Click New to display the following configuration page:



『Community』 sets the same key information as that of the peer device, which is consistent with that set for the peer device.

『Allowed IP Addresses』 sets which IP addresses are allowed to obtain the information of ADC through SNMP. [All] and [Specified] are available options here.

『Access Permission』 sets the permission for the peer device for accessing the ADC through SNMP and [Read-only] is shown here.

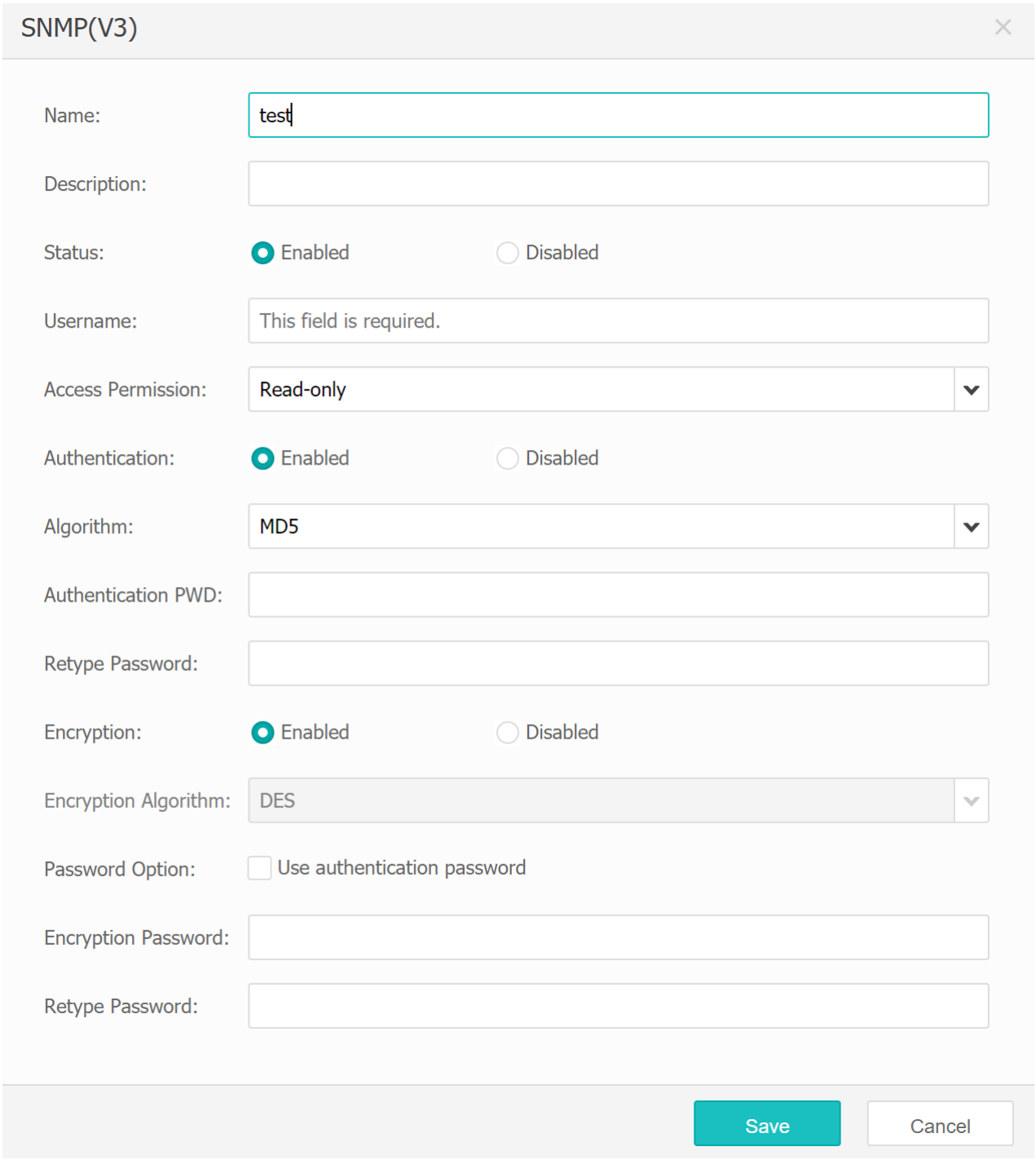
4.3.2 SNMP(V3)

【Operation Scenarios】

SNMP(V3) is generally used to set parameters for other devices to obtain device information through SNMP V3.

【Operation Procedure】

Click New to display the following page:



『Username』 sets the name of the local ADC.

『Access Permission』 sets the permission for the peer device for accessing the ADC through SNMP. [Read-only] and [Read]/[Write] are optional here.

『Authentication』 sets whether to enable authentication.

『Algorithm』 sets the authentication algorithm. [Md5] and [SHA] are optional here, and the setting shall be consistent with that of the peer device.

『Encryption』 sets whether to enable encryption.

『Encryption Algorithm』 sets the encryption algorithm, and the setting shall be consistent with that of the peer device.

If [Use authentication password] is checked for『Password Option』, the『Encryption Password』 below does not need to be filled in, and the 『Authentication PWD』 configured above will be used.

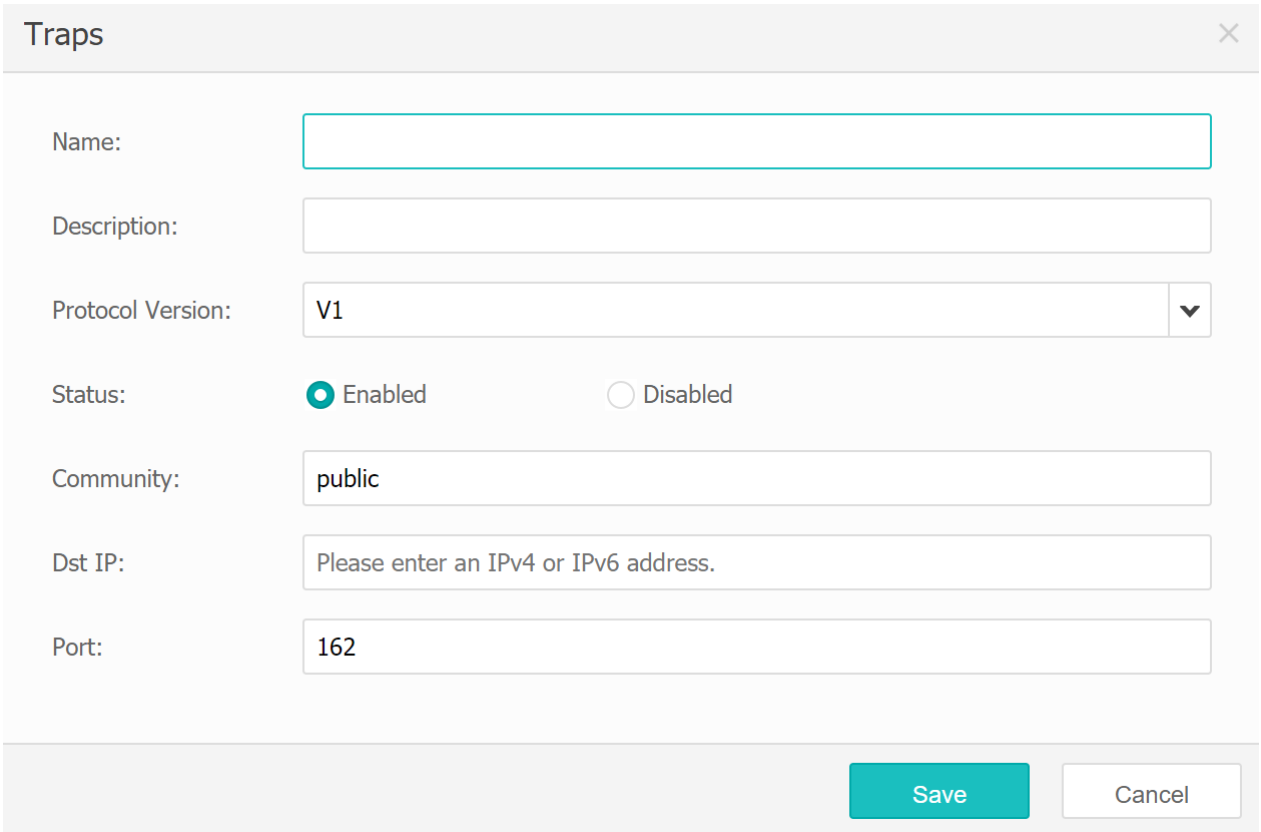
4.3.3 Traps

【Operation Scenarios】

Traps is generally used by ADC to actively send local status information to an IP address.

【Operation Procedure】

Click New to display the following page:



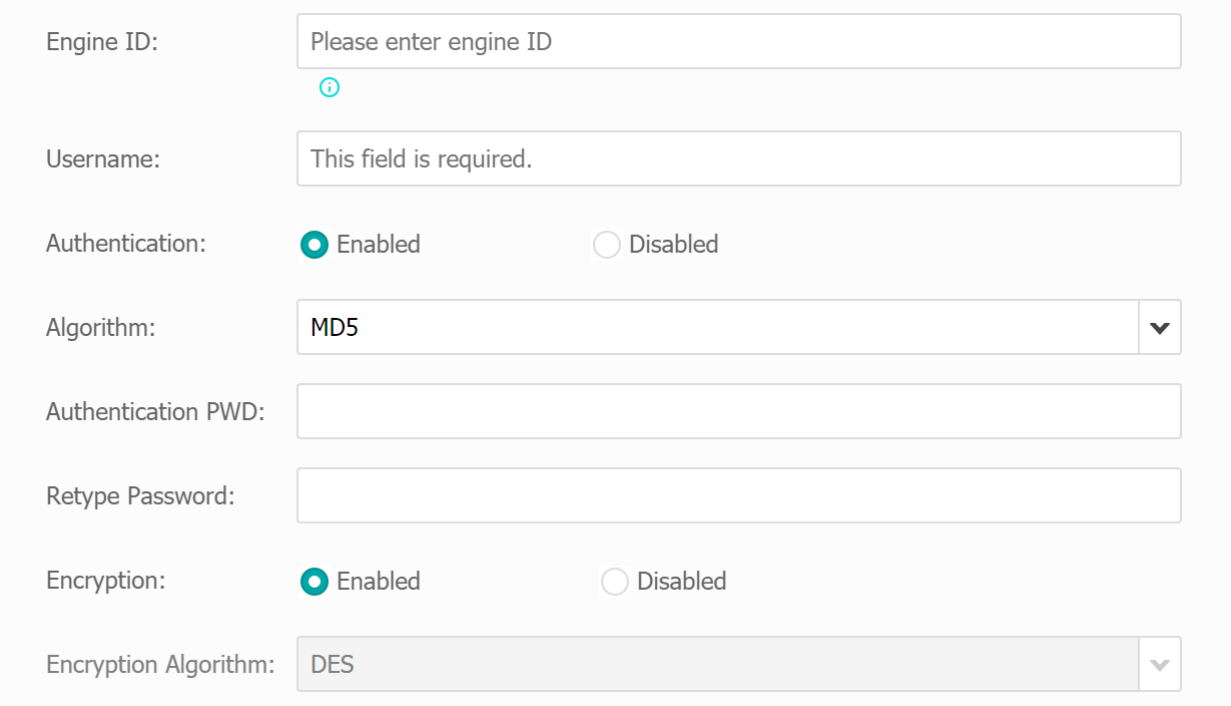
『Protocol Version』 can be selected from [V1], [V2C], and [V3].

『Community』 sets the same key information as that of the peer device, which is consistent with that set for the peer device.

『Dst IP』 sets the IP address to which the ADC actively sends the local status information.

『Port』 sets the listening port of the peer device.

When V3 is selected, the following items need to be configured.



『Engine ID』 is used for SNMP entity identification, authentication, and encryption.

『Username』 sets the name of the local ADC.

『Authentication』 sets whether to enable authentication.

『Algorithm』 sets the authentication algorithm. [Md5] and [SHA] are optional here, and the setting shall be consistent with that of the peer device.

『Encryption』 sets whether to enable encryption.

『Encryption Algorithm』 sets the encryption algorithm, and the setting shall be consistent with that of the peer device.

If [Use authentication password] is checked for『Password Option』, the『Encryption Password』 below does not need to be filled in, and the 『Authentication PWD』 configured above will be used.

4.4 Alarm Options

【Operation Scenarios】

Alarm Options is generally used for ADC to send alarm information by E-MAIL or SNMP Trap. Log-related items include HTTP Logs and Syslog Server.

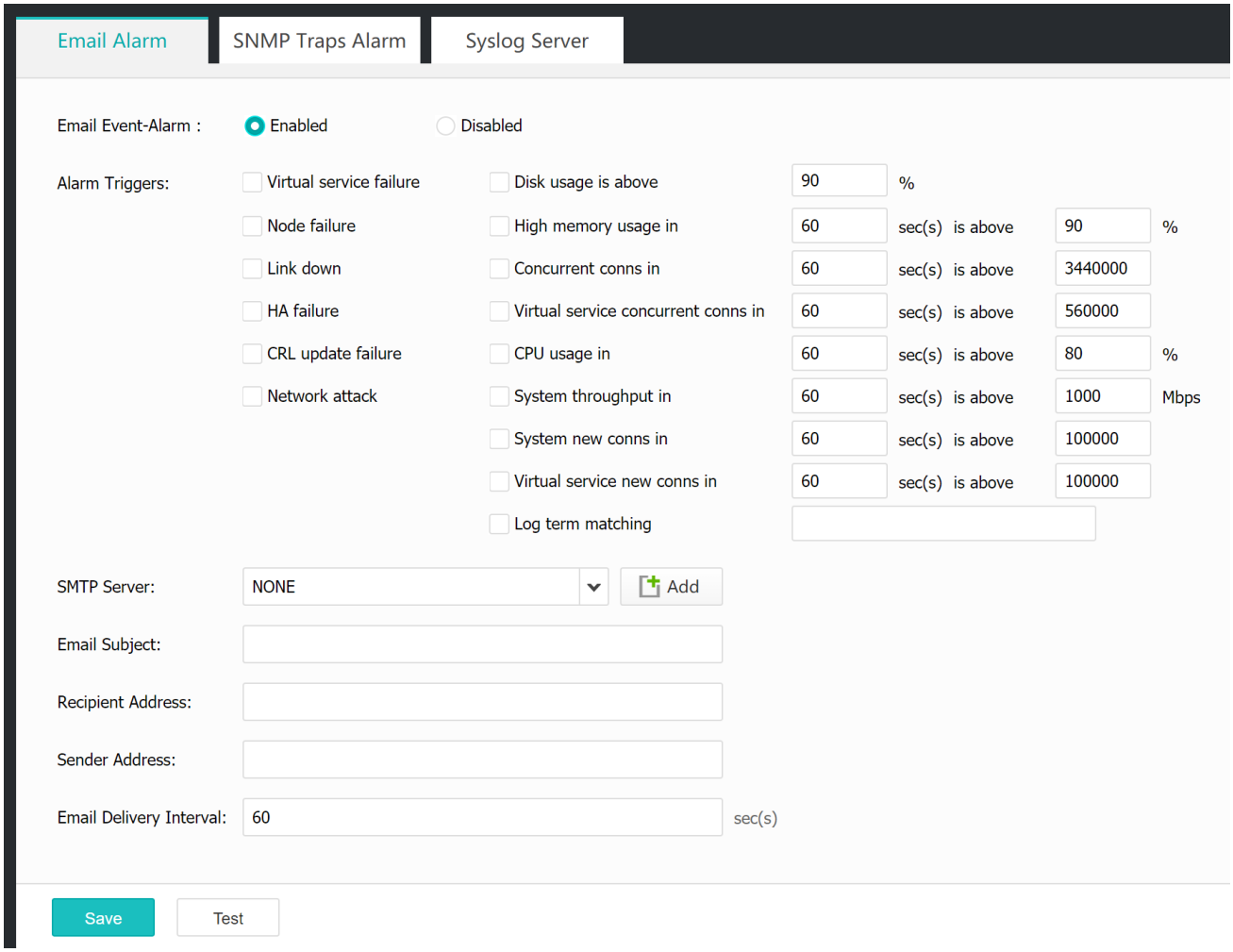
4.4.1 Email Alarm

【Operation Scenarios】

Email Alarm is a function of the ADC to send E-mail alarms automatically.

【Operation Procedure】

Open the configuration interface as follows:



For『E-mail Event-Alarm』, check [Enabled] to enable E-mail Event-Alarm, which will enable the device to send email alarms automatically. Check [Disabled] to disable this email alarm function.

『Alarm Triggers』sets events that will trigger the sending of email alarms:

[Virtual service failure]: an alarm will be sent when all links or all nodes are disconnected or restored.

[Node failure]: an alarm will be sent when a node is disconnected or restored.

[Link down]: an alarm will be sent when any of the links is disconnected/busy/restored.

[HA failure]: if Active-Standby or Cluster mode is enabled, an alarm will be sent when performing a switchover.

[CRL update failure]: an alarm will be sent when a CRL update failure is detected.

[Network attack]: an alarm will be sent when an unauthorized HTTP request is detected or an SYN flood can not be recognized.

[Disk usage]: an alarm will be sent when the disk usage of the ADC exceeds the set percentage.

[High memory usage]: an alarm will be sent when the memory usage of the ADC exceeds the set percentage for a set period of time.

[Concurrent conns]: an alarm will be sent when the number of concurrent connections of the ADC exceeds the set limit for a set period of time.

[Virtual service concurrent conns]: an alarm will be sent when the number of virtual service connections of the ADC exceeds the set limit for a set period of time.

[CPU usage]: an alarm will be sent when the CPU usage of the ADC exceeds the set percentage for a set period of time.

[System throughput]: an email or SNMP alarm will be sent when the system throughput continues to exceed the threshold value for 60 seconds (default).

[System new conns]: an email or SNMP alarm will be sent when newly created system connections continue to exceed the threshold value for 60 seconds (default).

[Virtual service new conns]: an email or SNMP alarm will be sent when newly created virtual service connections continue to exceed the threshold value for 60 seconds (default).

[Log term matching]: an alarm will be triggered when the ADC's log matches the term(s) set.

『SMTP Server』 sets the SMTP server(s) used for sending alarm emails. For the settings of SMTP servers, please refer to the relevant instructions in Section 4.1.4 『SMTP』. The user can select a previously set SMTP server from the drop-down box, or click Add to open the 【SMTP Server】 window to add an SMTP server.

『Email Subject』 sets the email subject of the alarm email to be sent.

『Recipient Address』 sets a mailbox that receives alarm emails.

『Sender Address』 sets a mailbox that sends out alarm emails. Generally, the mailbox corresponding to the selected SMTP server needs to be used.

『Email Delivery Interval』 refers to the interval of sending out alarm emails. Alarm messages generated during this time period will be consolidated into one alarm email for sending.

Click Save to complete the configuration.

Click Test to send an email alarm test email to the Recipient Address mailbox.

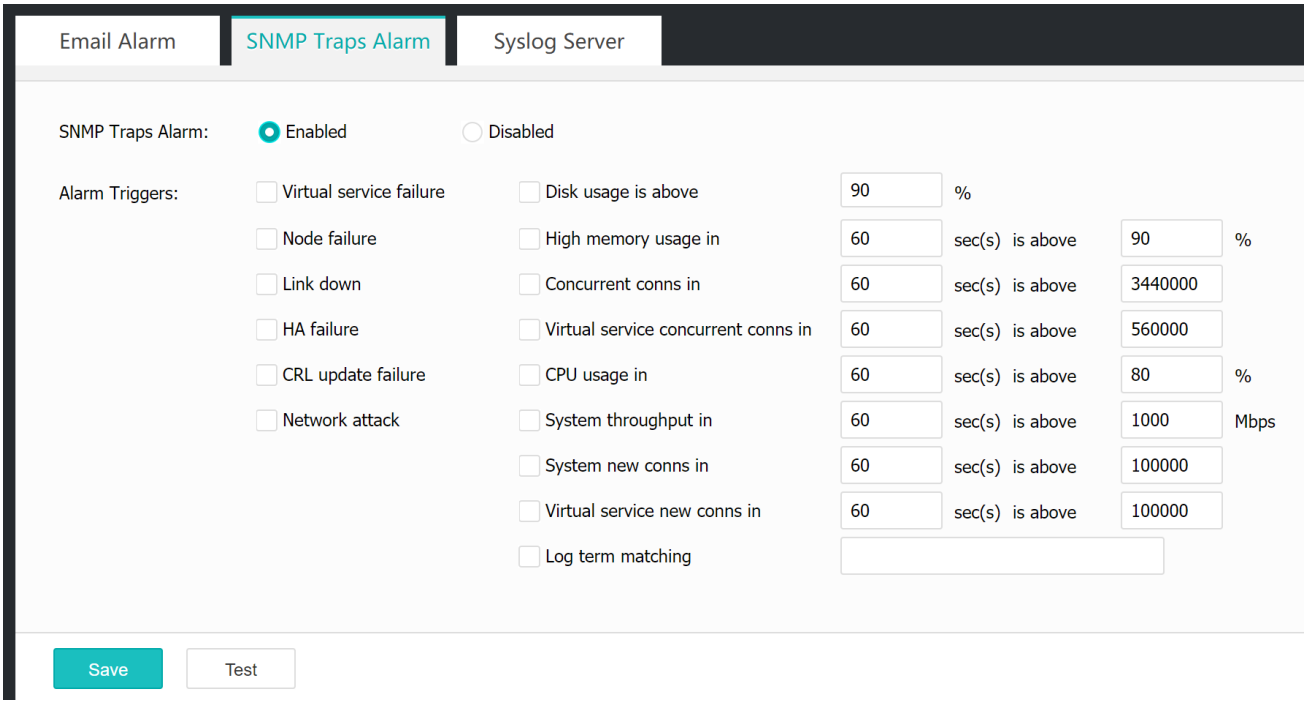
4.4.2 SNMP Traps Alarm

【Operation Scenarios】

It is generally used for ADCs to send warning logs through SNMP Trap.

【Operation Procedure】

The interface is shown as follows:



Check [Enabled] for 『SNMP Traps Alarm』 to enable the device to send alarms through SNMP Trap. Check [Disabled] to disable the device from sending alarms through SNMP Trap.

『Alarm Triggers』 sets events that will trigger the sending of alarms.

[Virtual service failure]: an alarm will be sent when all links or all nodes are disconnected or restored.

[Node failure]: an alarm will be sent when a node is disconnected or restored.

[Link down]: an alarm will be sent when any of the links is disconnected/busy/restored.

[HA failure]: if Active-Standby or Cluster mode is enabled, an alarm will be sent when performing a switchover.

[CRL update failure]: an alarm will be sent when a CRL update failure is detected.

[Network attack]: an alarm will be sent when an unauthorized HTTP request is detected or an SYN flood can not be recognized.

[Disk usage]: an alarm will be sent when the disk usage of the ADC exceeds the set percentage.

[High memory usage]: an alarm will be sent when the memory usage of the ADC exceeds the set percentage for a set period of time.

[Concurrent conns]: an alarm will be sent when the number of concurrent connections of the ADC exceeds the set limit for a set period of time.

[Virtual service concurrent conns]: an alarm will be sent when the number of virtual service connections of the ADC exceeds the set limit for a set period of time.

[CPU usage]: an alarm will be sent when the CPU usage of the ADC exceeds the set percentage for a set period of time.

[System throughput]: an email or SNMP alarm will be sent when the system throughput continues to exceed the threshold value for 60 seconds (default).

[System new conns]: an email or SNMP alarm will be sent when newly created system connections continue to exceed the threshold value for 60 seconds (default).

[Virtual service new conns]: an email or SNMP alarm will be sent when newly created virtual service connections continue to exceed the threshold value for 60 seconds (default).

[Log term matching]: an alarm will be triggered when the ADC's log matches the term(s) set.

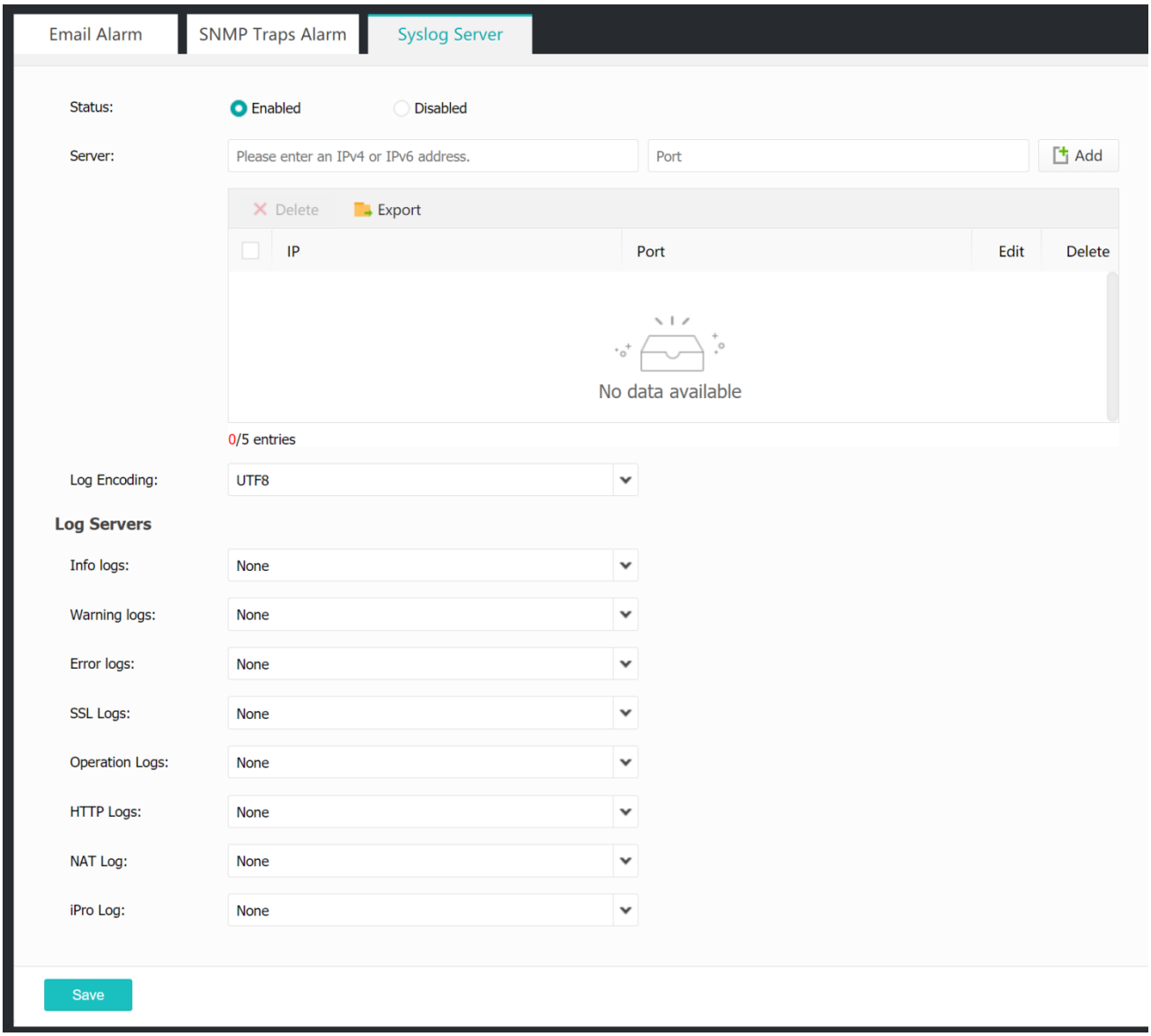
4.4.3 Syslog Server

【Operation Scenarios】

"Syslog Server" is used to set logs of the device to be sent to the Syslog server that has been set.

【Operation Procedure】

The page is shown in the figure below:



『Status』 enables/disables sending logs to the Syslog server.

『Server』 should be filled in with the IP address(es) and service port(s) of the Syslog server. Once finished, click Add to configure the IP address(es) and port(s).

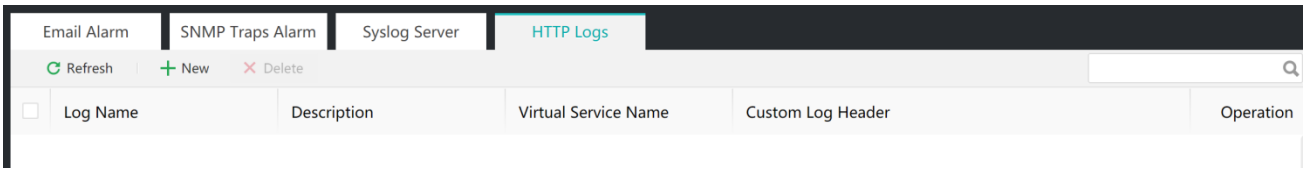
『Log Encoding』 defines log encoding formats. ASCII, UTF8, GBK, and GB2312 are available for selection. Customers can make a decision according to their actual needs to avoid messy code from generation.

『Log Servers』 marks the following Logs with relevant flags before sending them to the Syslog server: Info Logs, Warning Logs, Error Logs, SSL Logs, Operation Logs, HTTP Logs, NAT Log, and iPro Log. This feature is designed to classify the logs on the Syslog server according to different flags. LACAL0 to LOCAL7 represent flags. No matter which one is selected, the corresponding log will be sent to the Syslog server. NONE indicates that no log will be sent to the Syslog server.

4.4.4 HTTP Logs

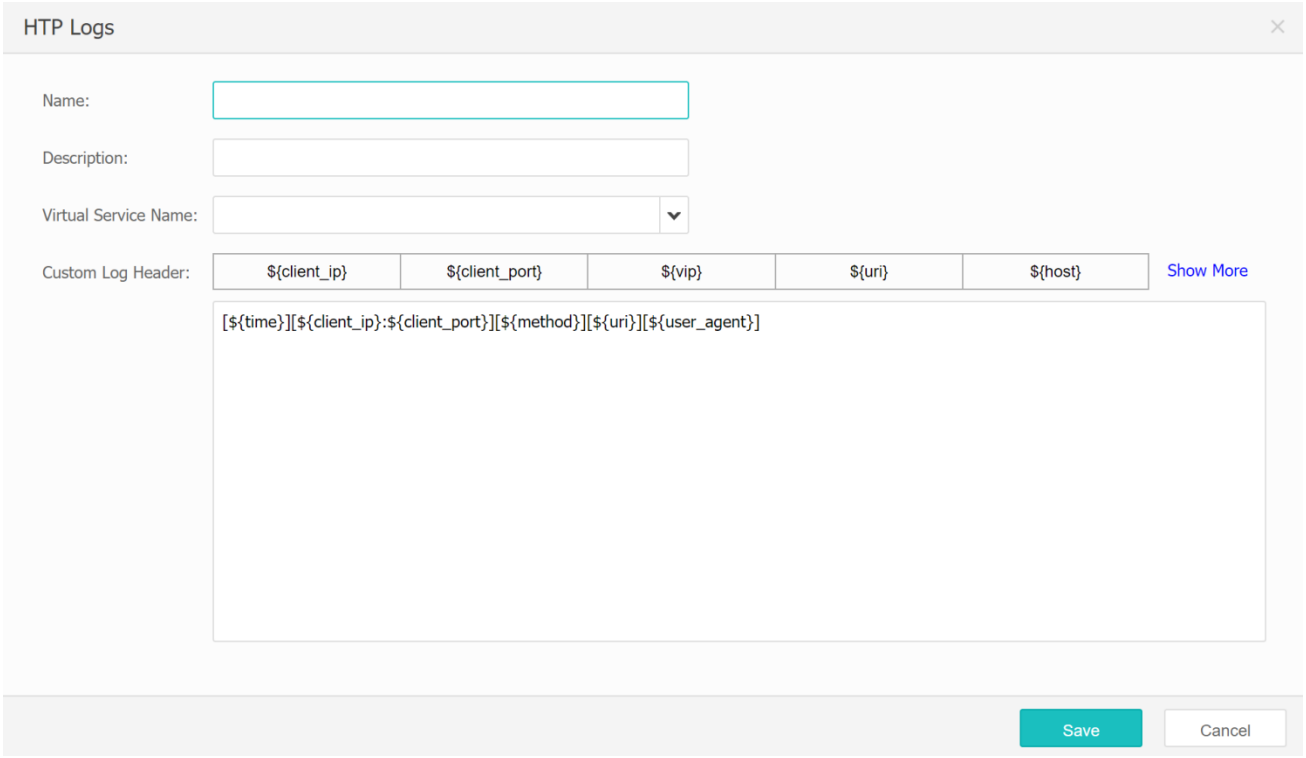
【Operation Scenarios】

『HTTP Logs』can customize the log variables of virtual services and send them through the Syslog server.



【Operation Procedure】

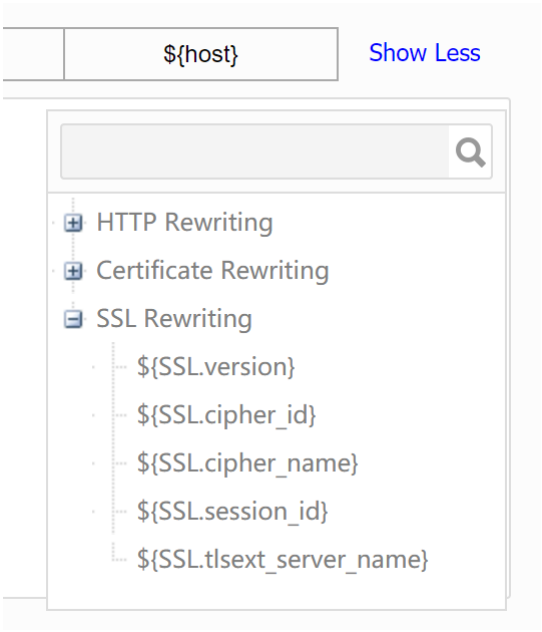
Click New. The following page is displayed:



『Name』 sets the name of the HTTP log.

『Virtual Service Name』 selects a virtual service of HTTP or HTTPS type. A virtual service can only be added once.

『Custom Log Header』 selects the log variables. Click Show More, the following types of variables will be displayed for selection as required:



Description of each field (variables and their corresponding interpretations) is as follows:

HTTP Rewriting

${client_ip} client IP address ${client_port} client port number

${vip} virtual service IP address ${vport} virtual service port number

${uri} request URI ${host} request host

${rs_ip} server IP address ${rs_port} server port number

${rs_val} node correlation variable ${user_agent} browser version information

${method} request method ${time} request time

${cookie.XXX} get XXX cookie (XXX refers to cookie name)

Certificate Rewriting

${X509.version} version of certificate ${X509.serial_num} serial number of certificate

${X509.signature_algorithm} signature algorithm for certificate

${X509.issuer} issuer of certificate

${X509.not_valid_before} certificate entry-into-force time (invalid before this time)

${X509.not_valid_after} certificate expiration time (invalid after this time)

${X509.subject} subject of certificate

${X509.subject_public_key_type} public key type of certificate's subject

${X509.subject_public_key} public key of certificate's subject

${X509.subject_public_key_bits} length of RSA public key of certificate's subject

${X509.hash} MD5 hash (fingerprint) of client certificate

${X509.whole} actual client certificate (.pem) ${X509.DN_CN} issue to ${X509.DN_E} email address

${X509.DN_O} company/organization ${X509.DN_OU} department

${X509.DN_C} country ${X509.DN_S} state/province

${X509.DN_L} city ${X509.errno} certificate authentication error code

SSL Rewriting

${SSL.version} SSL version ${SSL.cipher_id} cipher suite ID

${SSL.cipher_name} cipher suite name ${SSL.session_id} session ID

${SSL.tlsext_server_name} SNI server name

4.5 Maintenance

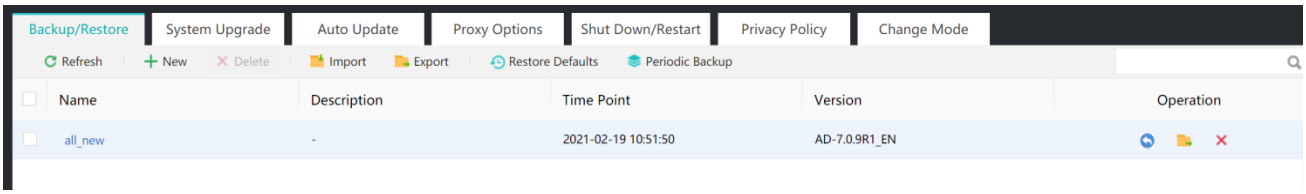
4.5.1 Backup/Restore

【Operation Scenarios】

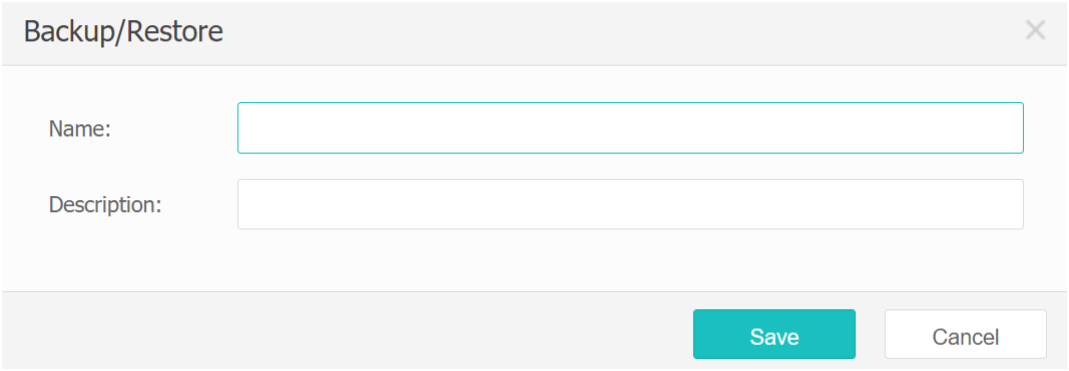
Backup/Restore is provided for executing backup and restore operations on relevant interfaces of the ADC console.

【Operation Procedure】

Navigate through『System』→『Maintenance』→『Backup/Restore』, an interface as shown in the figure below will be presented:

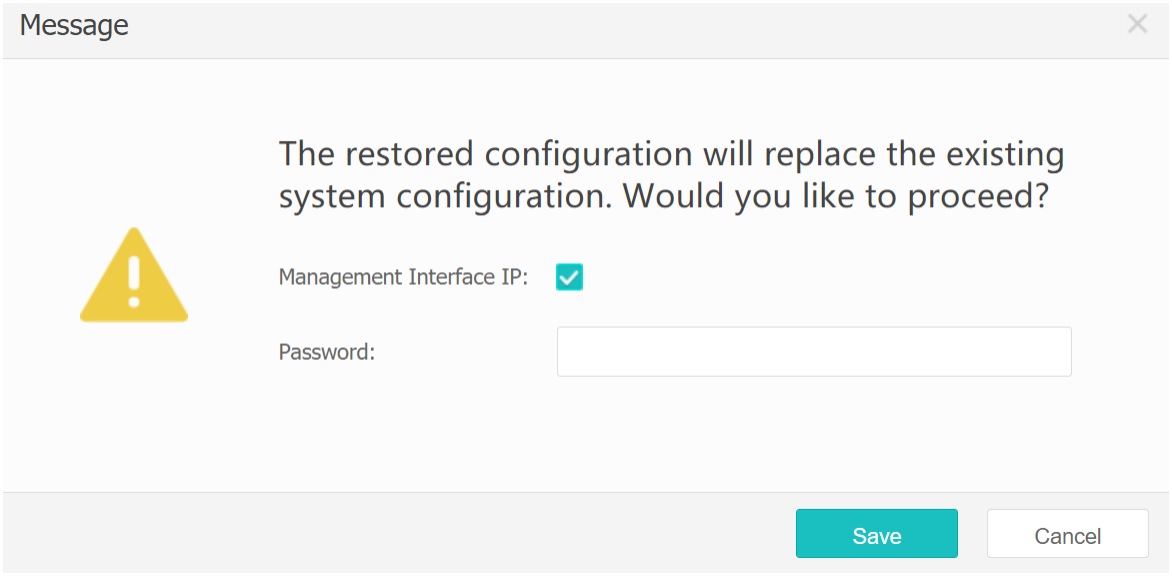


Click New to back up the current configuration. Enter the Name and click Save to complete the backup.

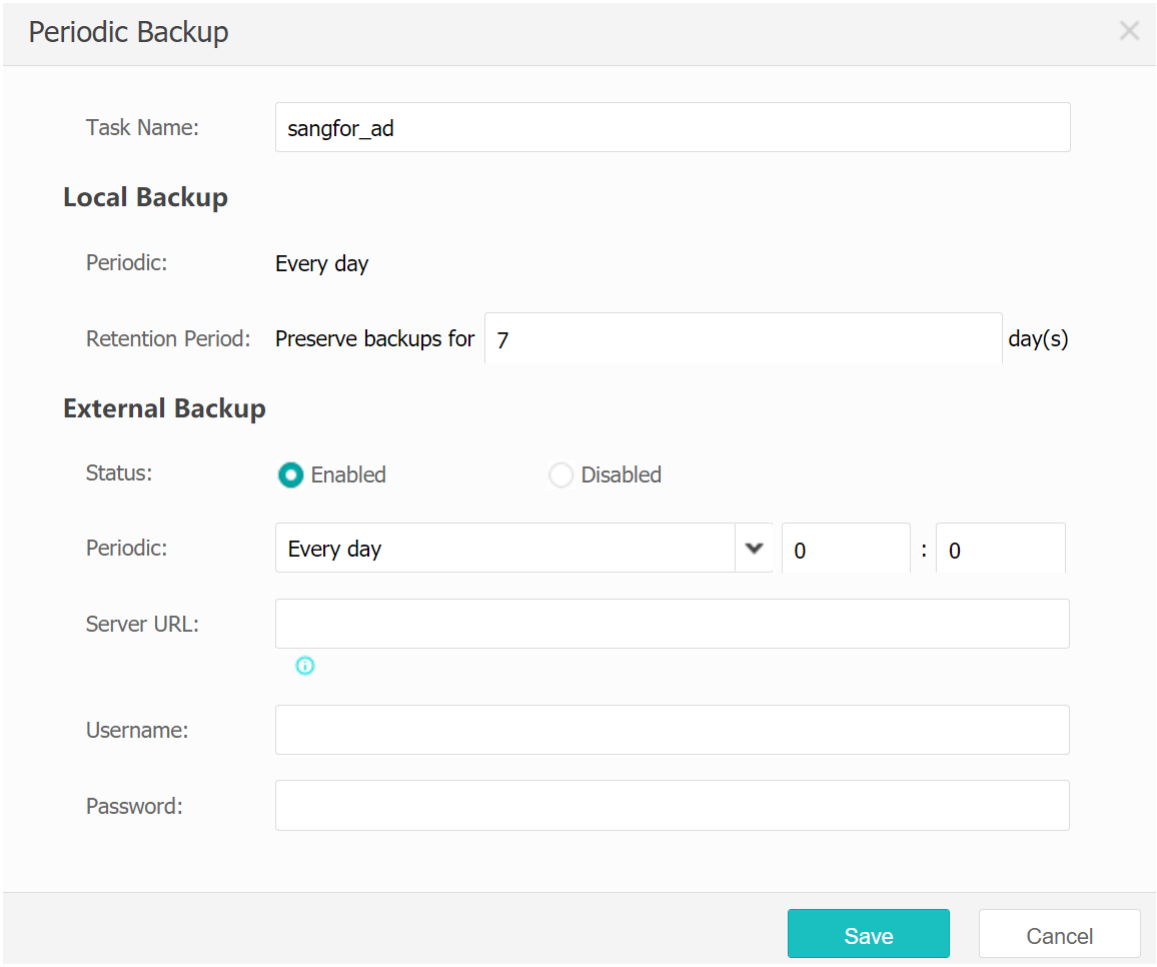


When importing or restoring configuration, the user can choose to retain the management network to avoid being unable to connect to the device after importing the configuration.

『Management Interface IP』 is checked by default. When it is checked, restoring the configuration will also restore the existing management interface IP address.



Click Periodic Backup, and the【Periodic Backup】window will pop up.



『Local Backup』

『Periodic』performs local backup Every day.

『Retention Period』 preserves the local backup records per the number of days set most recently.

『External Backup』

『Status』 enables or disables external backup.

『Periodic』 can be set as [Every day], [Every week], or [Every month]. Set the specific time for performing an external backup.

『Server URL』 specifies the server URL. Only FTP is supported.

In the backup list, select a specific entry of configuration and click  to restore this entry.

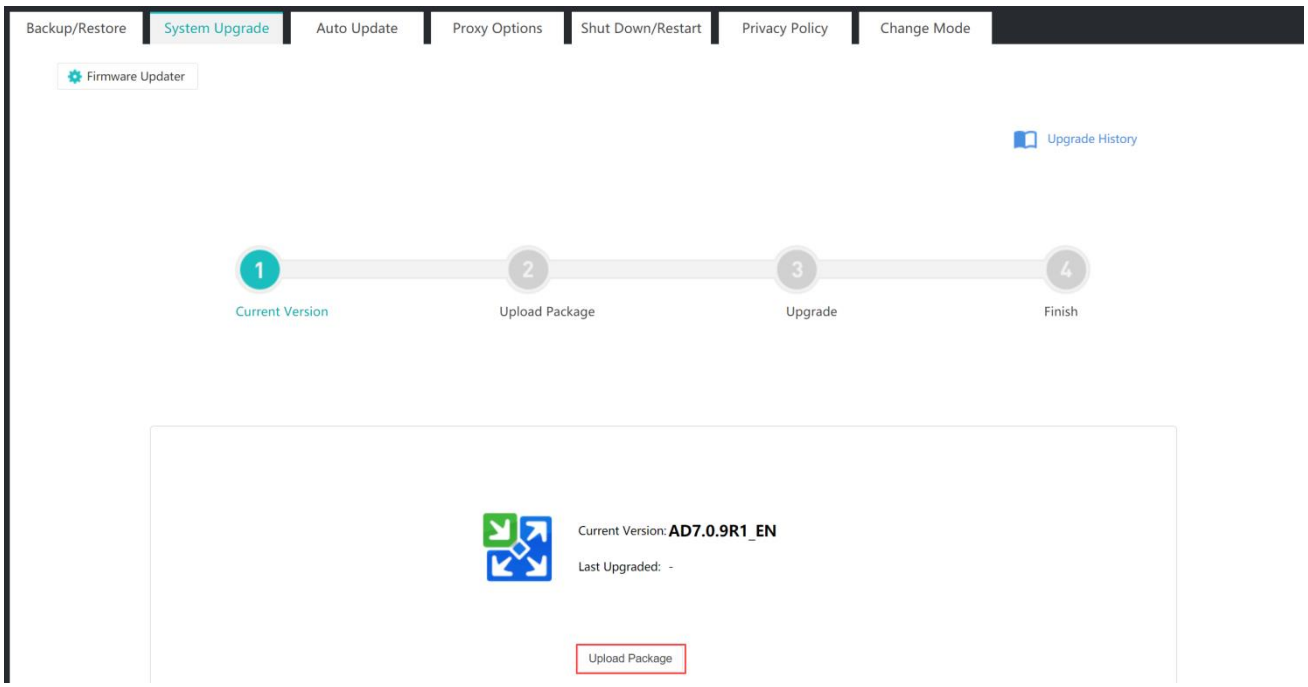
Click  to export a specific entry of configuration.

4.5.2 System Upgrade

【Operation Scenarios】

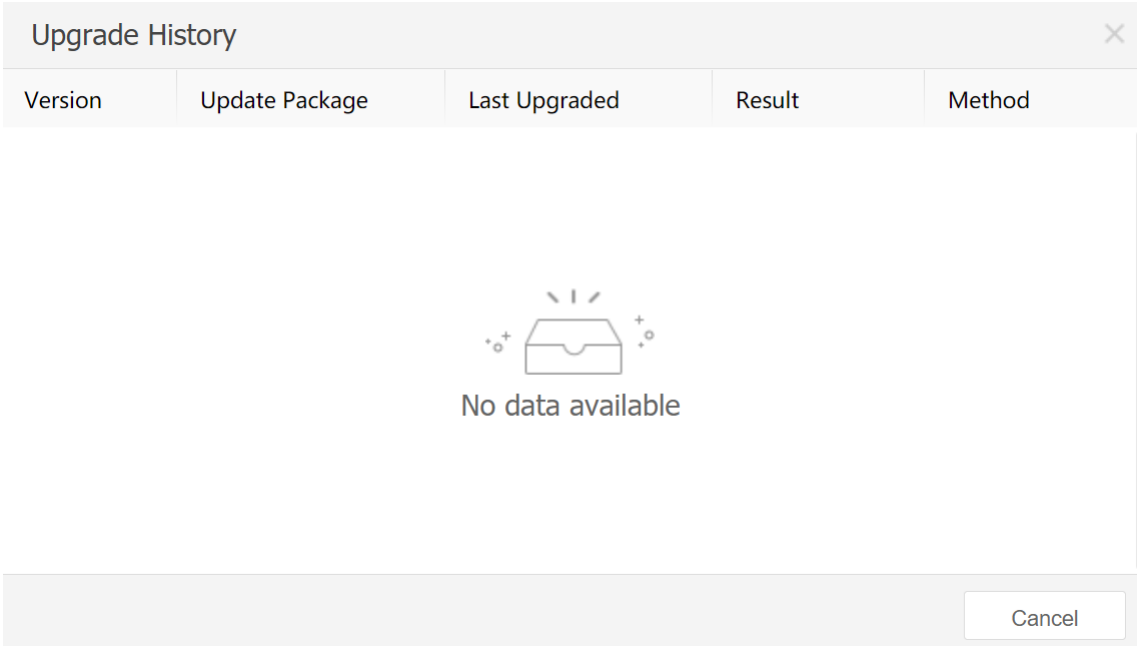
System Upgrade is generally used to upgrade the device by directly performing on the page.

【Operation Procedure】



Click Upload Package, drag or click SSU files for uploading. Follow the prompts and proceed to the next step to complete the upgrade.

Click Upgrade History to view the upgrade history of the device.

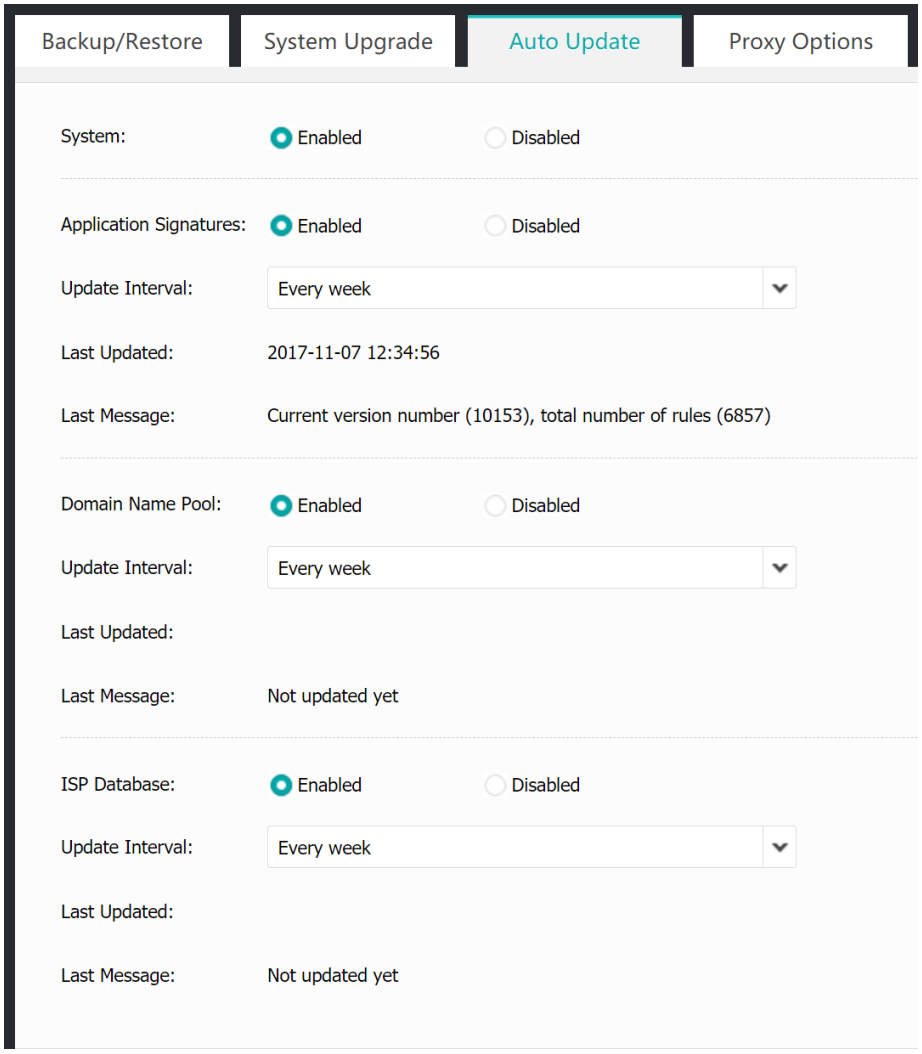


4.5.3 Auto Update

【Operation Scenarios】

Auto Update is generally used to configure automatic system updates and the settings for updating Application Signatures, Domain Name Pool, and ISP Database.

【Operation Procedure】



If the user selects [Enabled] for『System』, the system will automatically download and install the patches released by the SANGFOR website. If [Disabled] is selected, the system will not download patches automatically.

Select [Enabled] or [Disabled] for 『Application Signatures』 to enable/disable Application Signatures updates.

『Update Interval』 can be set as [Every day], [Every week], or [Every month]. Users can also click Update Now.

『Last Updated』 refers to the specific time at which the latest Application Signatures update is done.

『Last Message』 shows information about automatic updates, indicating the current version number of Application Signatures and the total number of signatures.

Select [Enabled] or [Disabled] for 『Domain Name Pool』 to enable/disable Domain Name Pool updates.

『Update Interval』 can be set as [Every day], [Every week], or [Every month]. Users can also click Update Now to download the latest foreign domain name databases.

『Last Updated』 refers to the specific time at which the latest Domain Name Pool update is done.

『Last Message』 shows information about automatic updates.

Select [Enabled] or [Disabled] for 『ISP Database』 to enable/disable ISP Database updates.

『Update Interval』 can be set as [Every day], [Every week], or [Every month]. Users can also click Update Now.

『Last Updated』 refers to the specific time at which the latest ISP Database update is done.

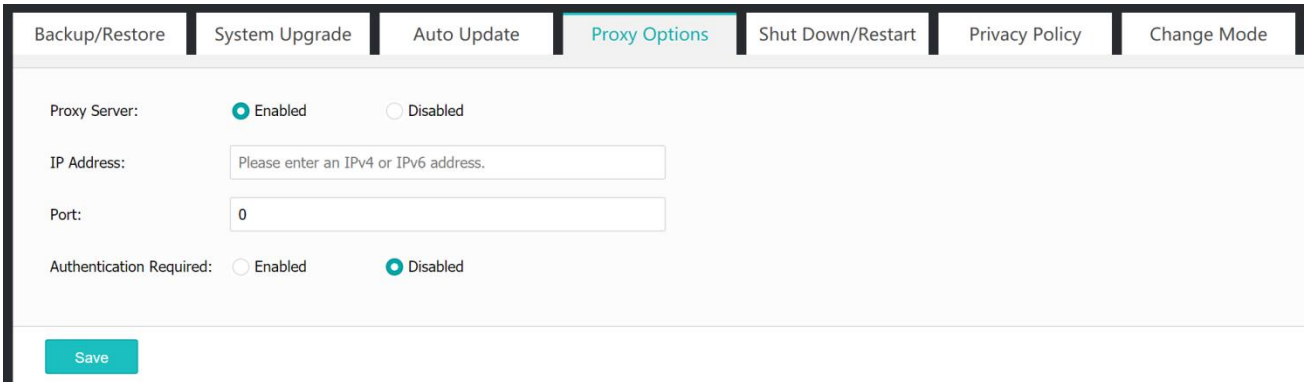
『Last Message』 shows information about automatic updates.

4.5.4 Proxy Options

【Operation Scenarios】

The system obtains configuration updates through the setting of "Proxy Options".

【Operation Procedure】



『Proxy Server』: When using a proxy server, please confirm that it supports HTTP and HTTPS. After [Enabled] is selected, the system obtains updates by using the proxy server.

『IP Address』: the IP address of Proxy Options.

『Port』: the port for Proxy Options (port range: 1 - 65,535).

『Authentication Required』 should be Enabled if authentication is required for the proxy server.

『Username』: a username for the proxy server.

『Password』: a password for the proxy server.

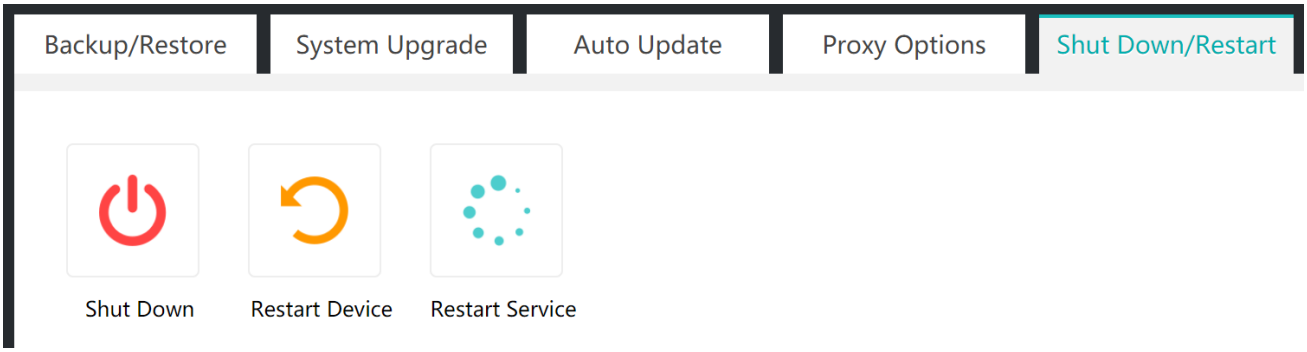
4.5.5 Shut Down/Restart

【Operation Scenarios】

『Shut Down/Restart』interface provides Restart buttons to facilitate the restarting operations.

【Operation Procedure】

The page is shown in the figure below:

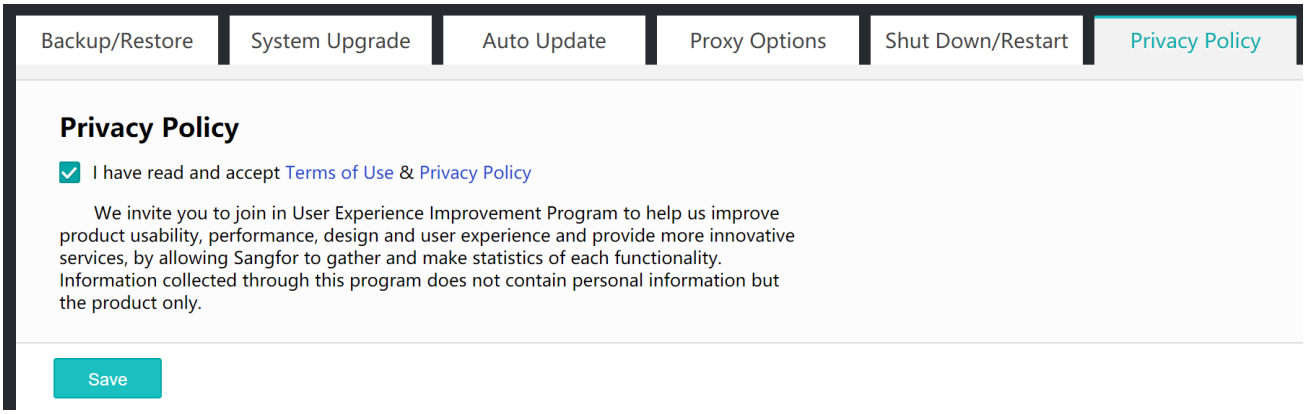


Click Shut Down to shut down the ADC.

Click Restart Device to restart the ADC.

Click Restart Service to restart all services of the ADC, and the hardware will not be restarted.

4.5.6 Privacy Policy



Users can set whether to send the system quality report to Sangfor Technologies Inc. under Privacy Policy.

4.5.7 Change Mode

【Operation Scenarios】

Navigate through『System』→『Maintenance』→『Change Mode』to switch between [Classic Mode] and [Multi-Tenant Mode].

【Operation Procedure】

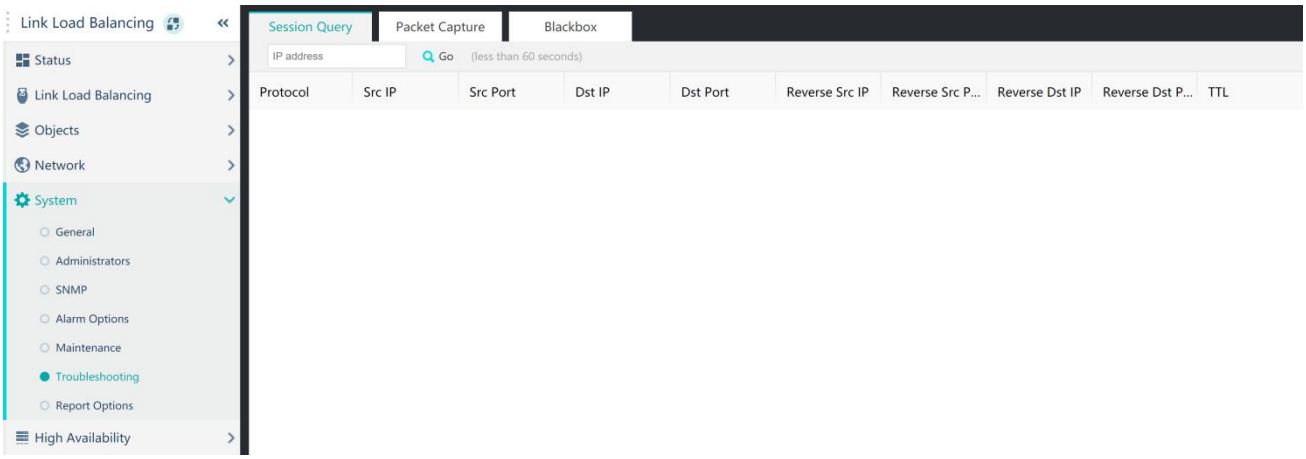
The interface is shown in the figure below. Select a mode as needed. Multi-tenant-related configuration can only be performed after changing to [Multi-Tenant Mode].



4.6 Troubleshooting

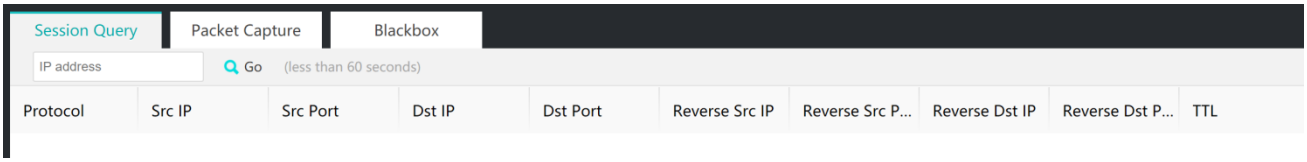
WEBUI path:『System』→『Troubleshooting』.

The interface is shown in the figure below:



4.6.1 Session Query

『Session Query』queries the session persistence for policy-based routing.



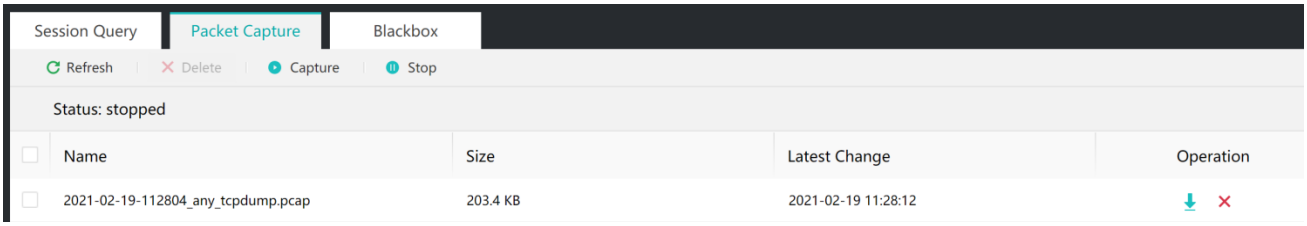
Enter the IP address to be queried and click Go. Matching items will be listed in the list below. Users can then view the relevant session persistence information.

4.6.2 Packet Capture

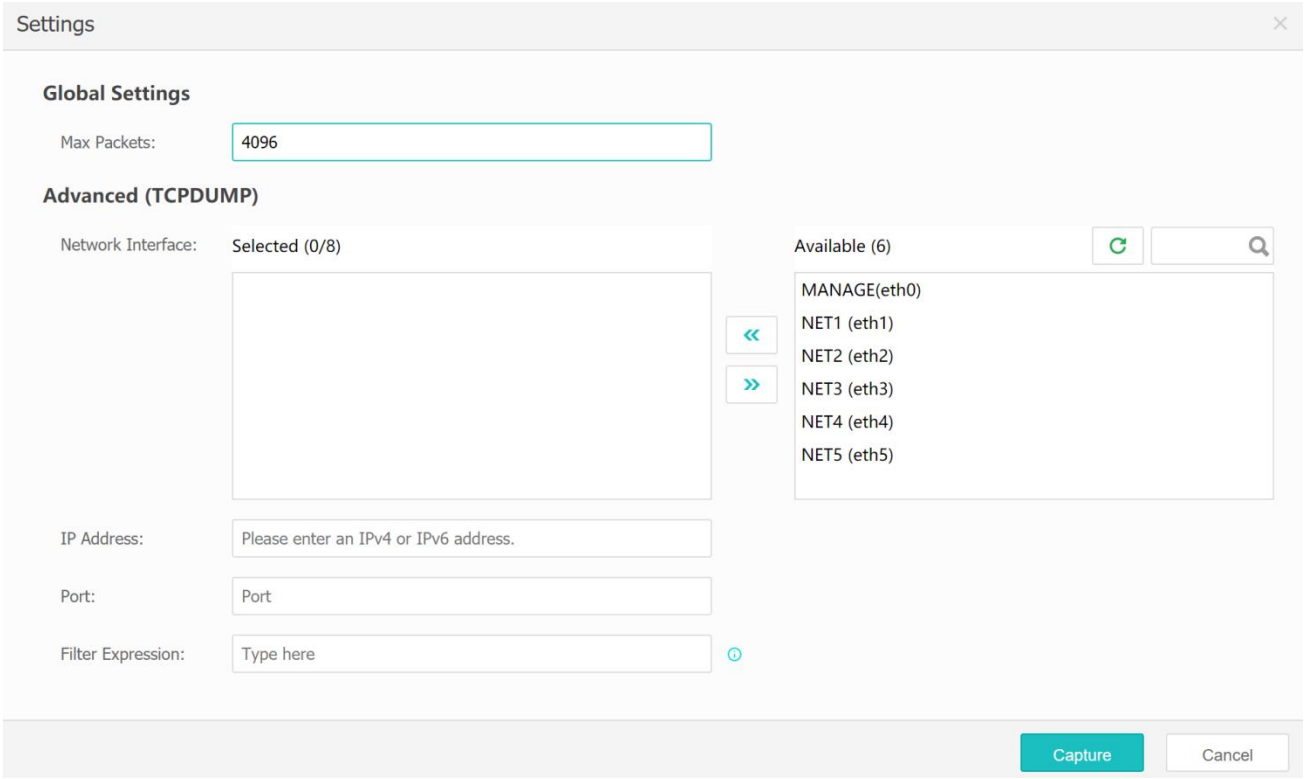
【Operation Scenarios】

Packet Capture interface provides the packet capturing function. In case of issues that need to be troubleshot, directly perform configurations on the interface for capturing packets, view and analyze the data packets captured, so as to facilitate troubleshooting.

【Operation Procedure】



Click Capture to open the【Settings】window.



『Max Packets』 sets the number of packages to be captured.

『Network Interface』 selects the interface for which data packages need to be captured from the Available box. Selected interfaces will be listed in the Selected box on the left.

『IP Address』 refers to the IP rule set for capturing data packets.

『Port』 refers to the port rule set for capturing data packets.

『Filter Expression』 can be customized based on certain parameters and formatted as host 200.200.0.1 and port 50. Data packets on ports 808, 830, and 1360 will not be captured.

Click Capture to capture packets according to the pre-defined conditions. Click Cancel to remove the current packet capturing settings.

Select the packet capturing item that needs to be stopped and click Stop or  on the page to stop the capturing operation.

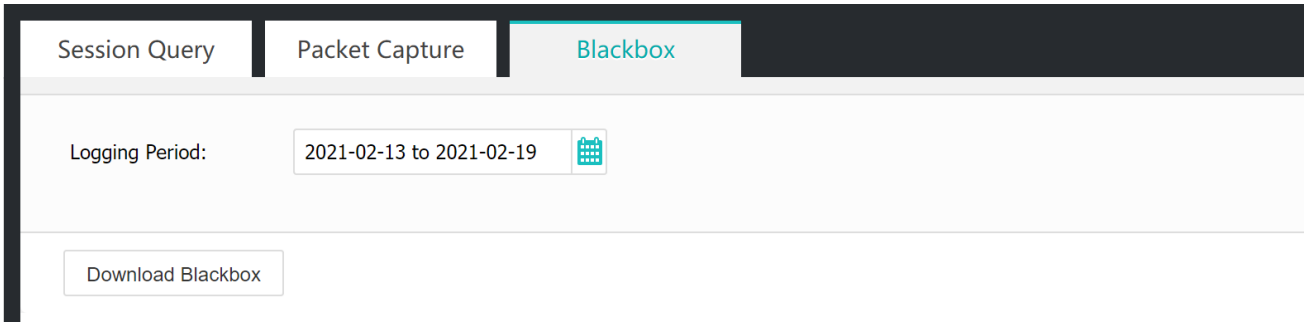
Click  to download captured data packages.

4.6.3 Blackbox

【Operation Scenarios】

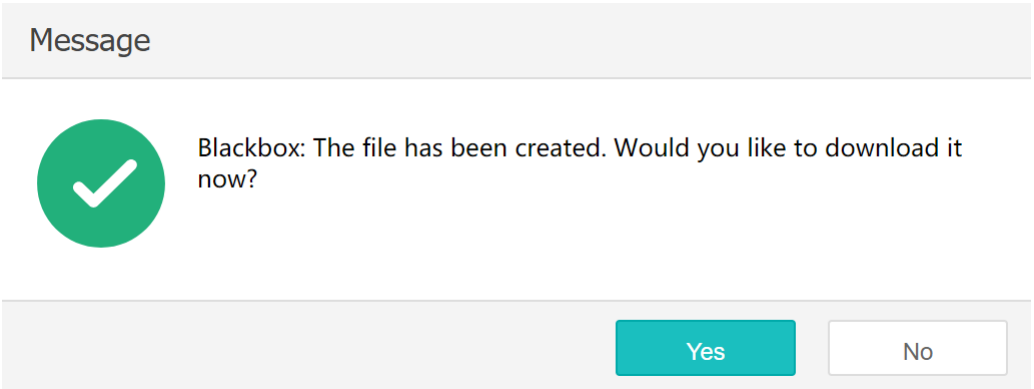
Blackbox interface provides the function of downloading Blackbox logs of the device that can be used as an effective basis for issue troubleshooting when you encounter a complex problem or need to look for causes of a problem that arose previously.

【Operation Procedure】



『Logging Period』requires a date range of fewer than 7 days, not exceeding the last 30 days.

Click Download Blackbox and the【Message】window is displayed. Click Yes to download.

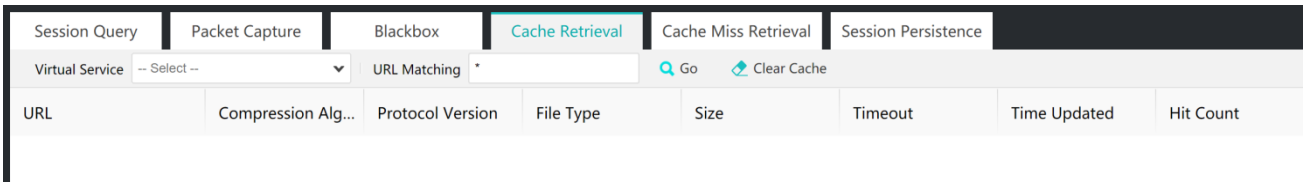


4.6.4 Cache Retrieval

【Operation Scenarios】

Cache Retrieval is used to retrieve whether a URL for a virtual service is cached by the ADC.

【Operation Procedure】



『Virtual Service』 selects the virtual service to be retrieved.

『URL Matching』 should be filled with the URL address to be retrieved. Wildcard characters are supported.

Click Go. The results are displayed.

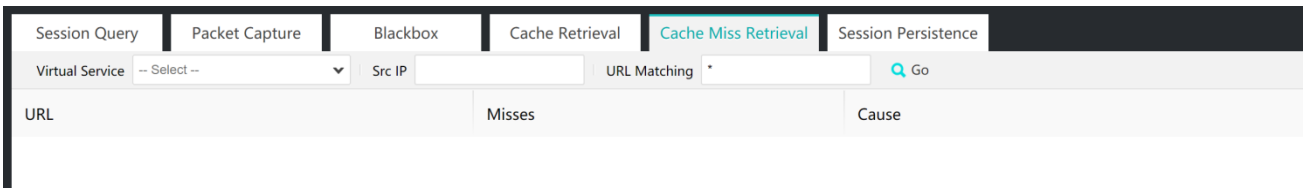
Click Clear Cache to clear all the caches.

4.6.5 Cache Miss Retrieval

【Operation Scenarios】

『Cache Miss Retrieval』 counts the number of times a URL fails to be cached in a period of time and records the reasons why it cannot be cached.

【Operation Procedure】



『Virtual Service』 selects the virtual service to be retrieved.

『Src IP』 refers to the source IP address for accessing the virtual service.

『URL Matching』 should be filled with the URL address to be retrieved. Wildcard characters are supported.

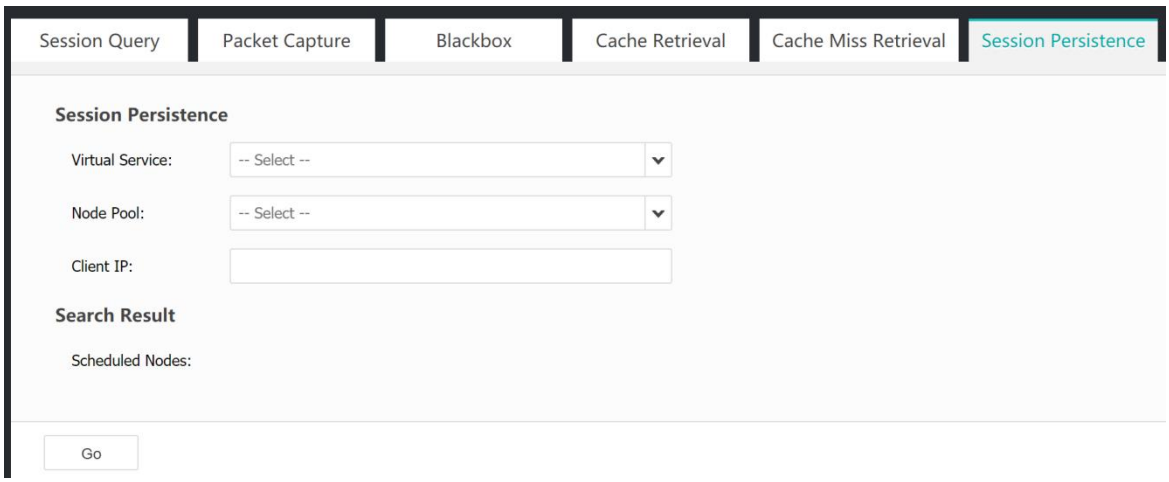
Click Go to start to count the URL access caching failures. After counting completed, click Stop to display the final results.

4.6.6 Session Persistence

【Operation Scenarios】

『Session Persistence』 queries the session (source IP) persistence for virtual service.

【Operation Procedure】



『Virtual Service』 selects the virtual service to be retrieved.

『Node Pool』 selects the node pool to be queried.

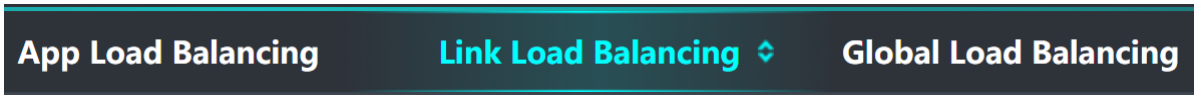
『Client IP』 should be filled with the client IP address to be queried.

『Scheduled Nodes』 maintains search results for virtual service sessions. Click Go to display the nodes for Session Persistence fulfilling the conditions.

Chapter 5 Status Overview

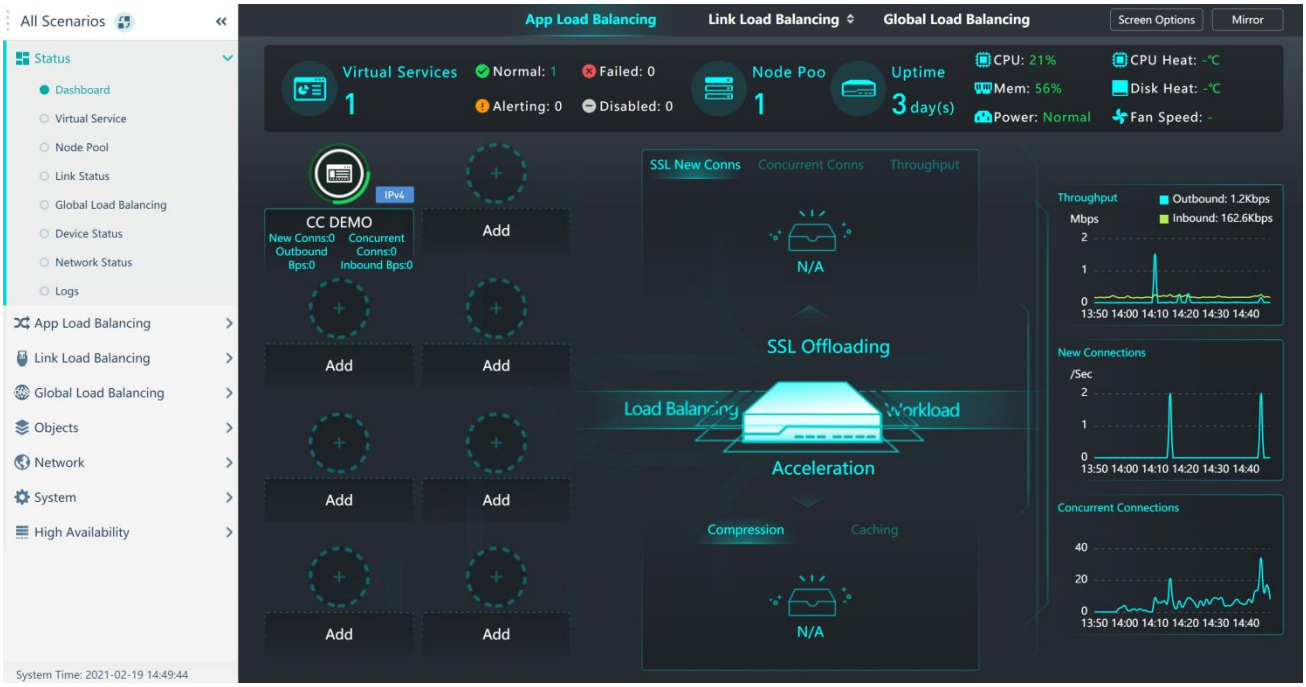
5.1 Status

『Dashboard』displays the overview of ADC App Load Balancing, Link Load Balancing, and Global Load Balancing. Click App Load Balancing, Link Load Balancing, and Global Load Balancing on the interface to switch between pages.



5.1.1 App Load Balancing

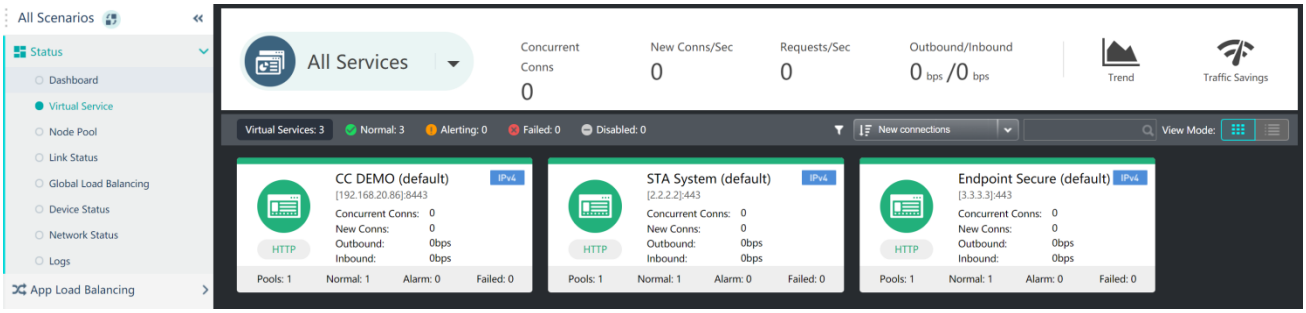
『Dashboard』→『App Load Balancing』page displays the real-time status of virtual services, operating condition of the device, and the total number of existing services and nodes. The page below is divided into four sections: Load Balancing, SSL Offloading, Workload, and Acceleration.



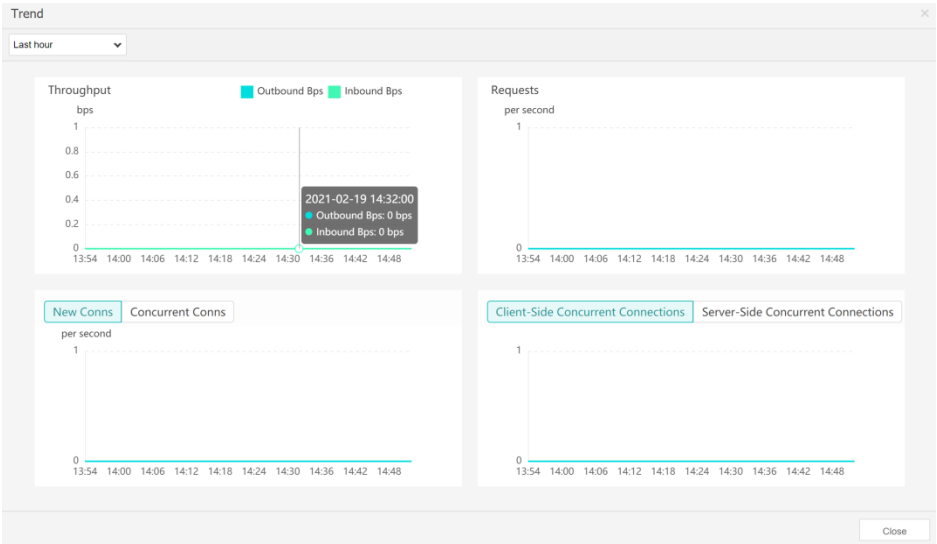
『Virtual Services』indacates the total number of virtual services currently configured. The service status is indicated by different icons and texts on the right, including Normal, Alerting, Failed, and Disabled. Each Status shows the corresponding number of services. By clicking one of

the Statuses (such as Normal), you will be redirected to the virtual service overview page (『Status』 → 『Virtual Service』).

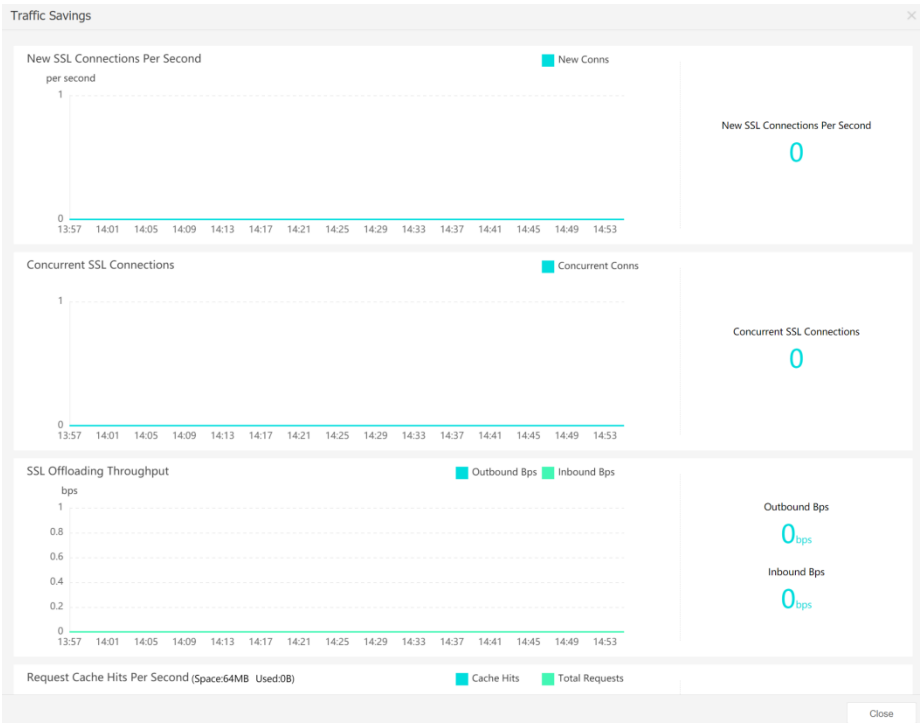
Click 『Status』 → 『Virtual Service』 to display the interface below, which shows the virtual service conditions, including virtual service status, number of Conns (New and Concurrent), Requests/Sec, and traffic information (Outbound/Inbound).



Click Trend in the upper right corner to view the statistical information of virtual services, including network Throughput, request rate, and number of Conns (New, Concurrent, Client-Side Concurrent, Server-Side Concurrent).

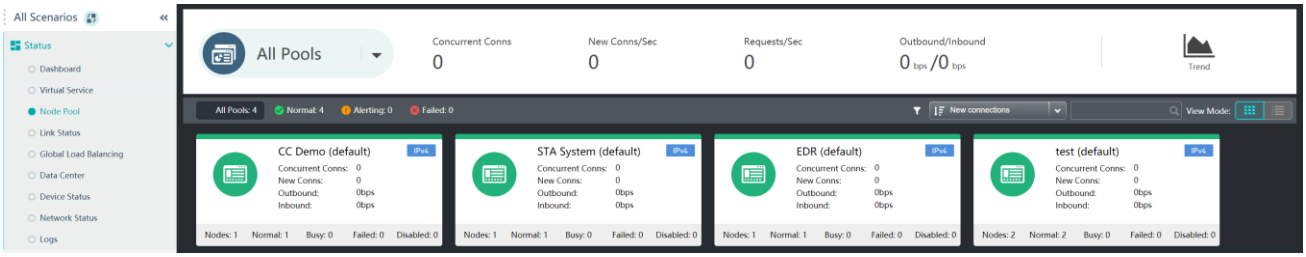


Click Traffic Savings in the upper right corner to display the optimization effect of virtual services. The interface is shown in the figure below.



『Node Pool』 page displays the number and status of virtual service node pools. Relevant information is indicated by different icons and texts on the right, including Normal, Alerting, and Failed. Each Status shows the corresponding number of nodes. By clicking one of the Statuses (such as Normal), you will be redirected to the node pool overview page (『Status』→『Node Pool』).

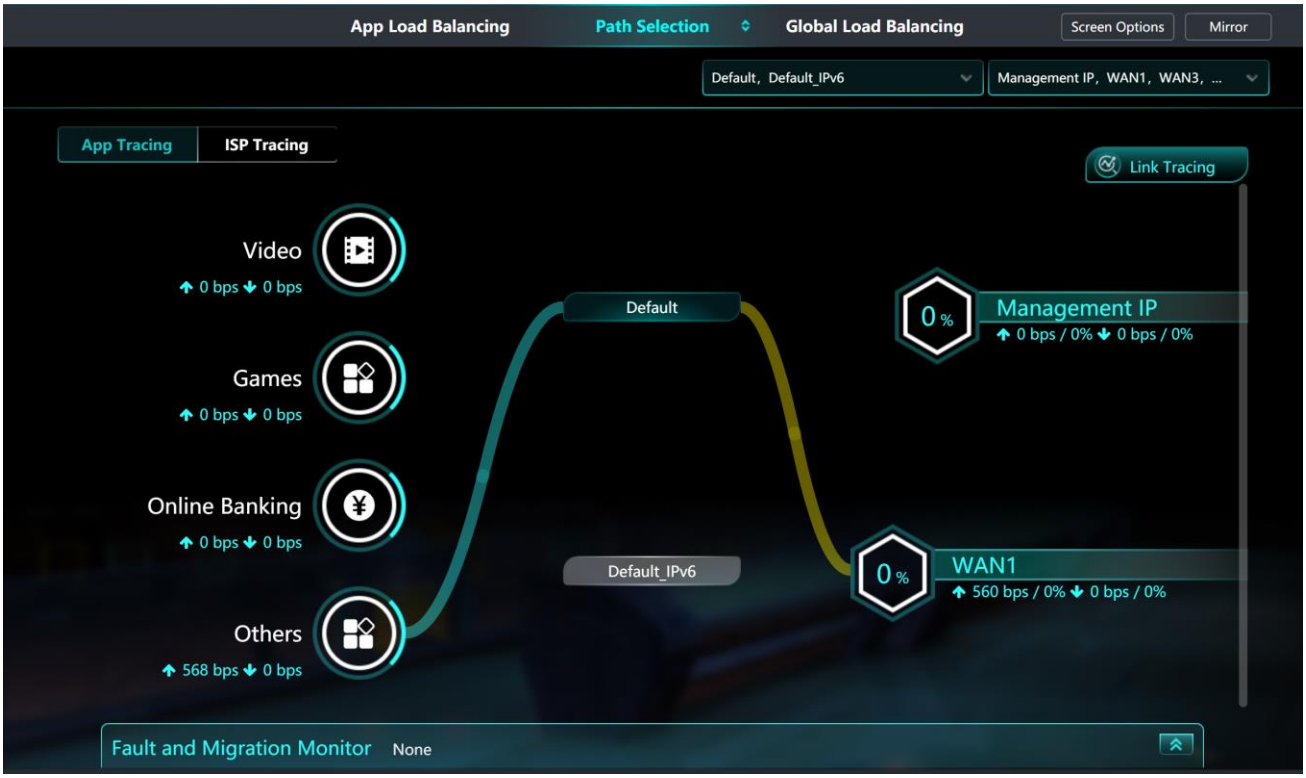
Click『Status』→『Node Pool』to display the interface below, which shows the node condition of node pools, including node status, number of Conns (New and Concurrent), Requests/Sec, and traffic information (Outbound/Inbound).



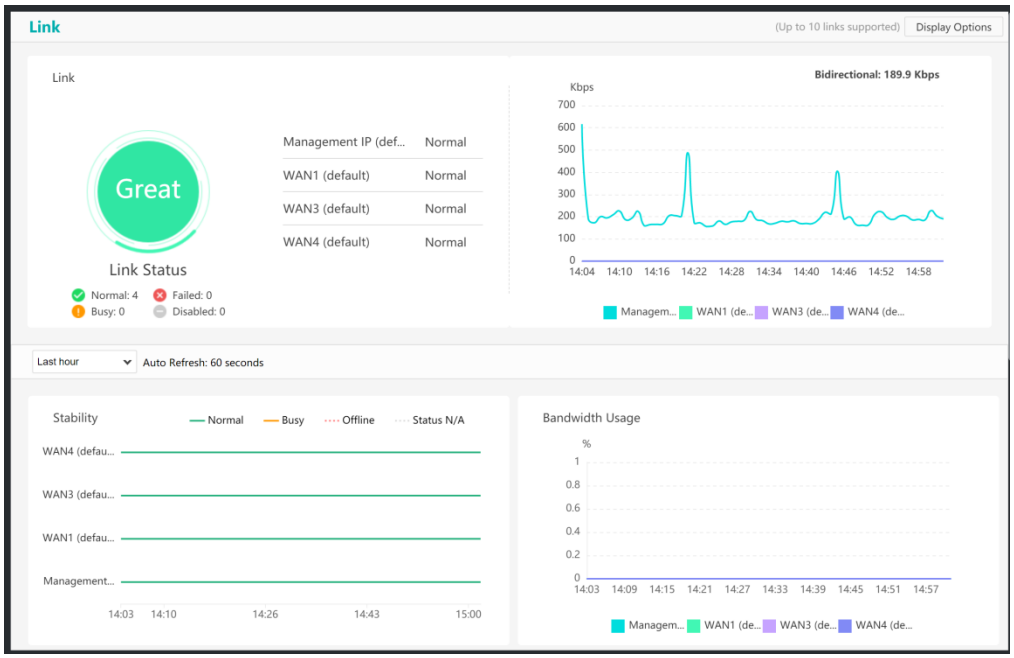
(Above-mentioned information relating to virtual services will be displayed in 『Dashboard』→『App Load Balancing』, so that you can directly view virtual service information on the Dashboard.)

5.1.2 Link Load Balancing

Navigate through『Dashboard』→『Link Load Balancing』→『Path Selection』to view the application route selection analysis. Link tracking analysis and migration event query are also supported.



Click 『Status』→『Link Status』to view the status of each link. This page also shows the real-time status of links and total real-time traffic. A trend chart is provided to indicate the link status within the last hour/the last day/the last week (including link Stability, Bandwidth Usage, traffic statistics, outbound access counts, policy hits statistics, and application route selection statistics).



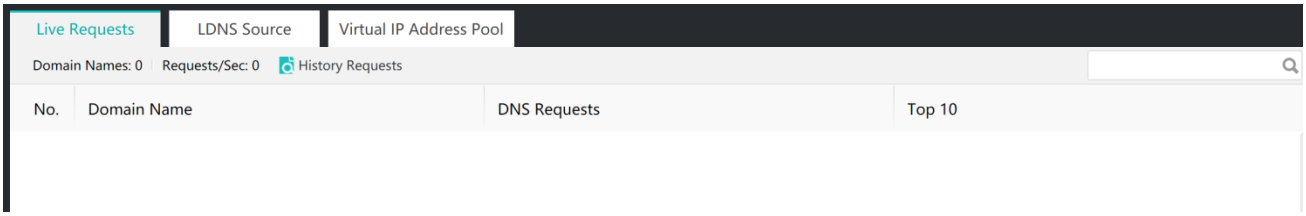
5.1.3 Global Load Balancing

『Dashboard』→『Global Load Balancing』page displays Total Domains, DNS Requests, DNS Requests Per Second, DNS Requests and DNS Record requests.

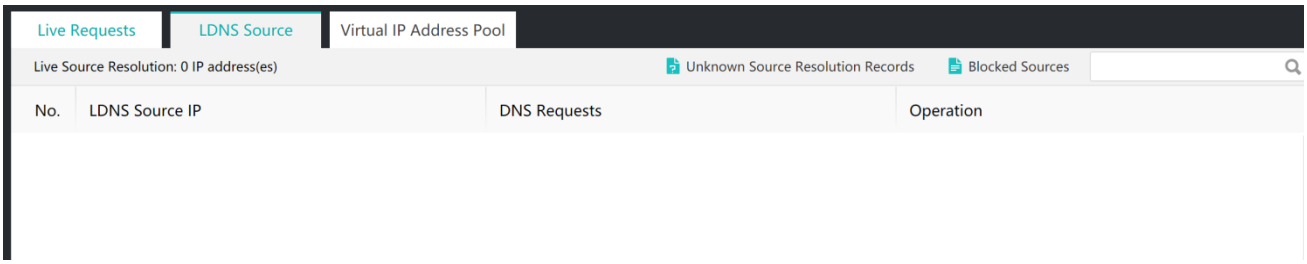


Click『Status』→『Global Load Balancing』to view Live Requests, LDNS Source, and Virtual IP Address Pool.

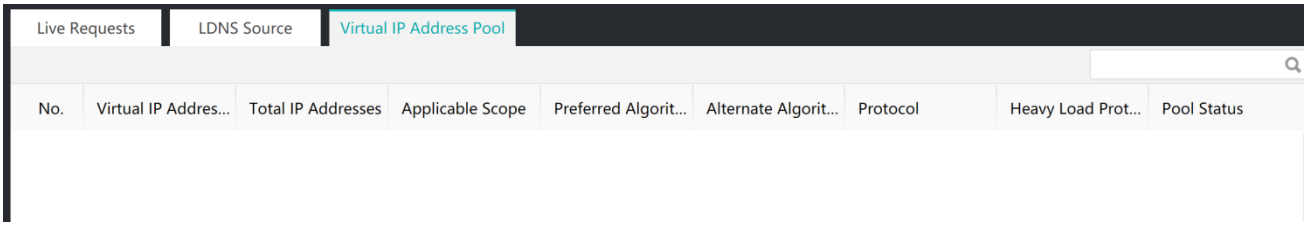
『History Requests』displays the total number of historical requests for each domain name.



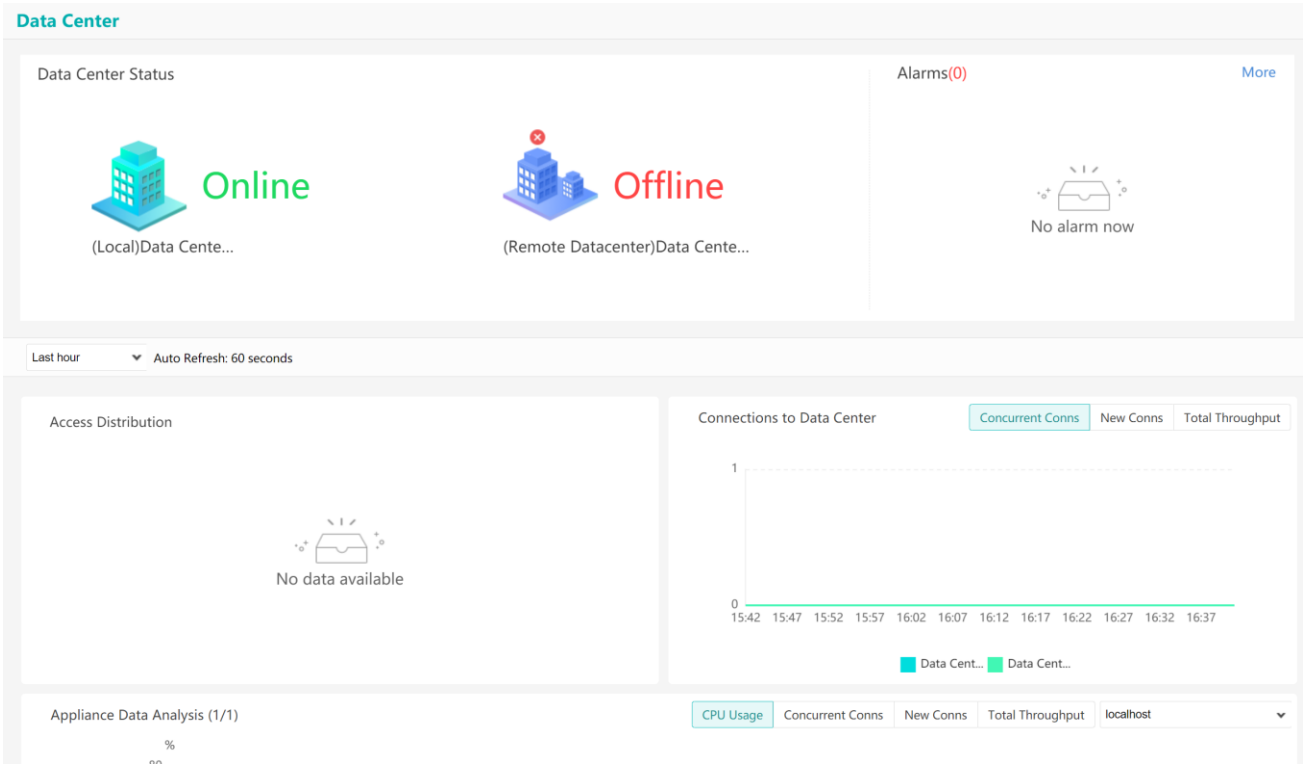
『LDNS Source』displays the LDNS Source IP address(es) and access count(s) for counting DNS requests per second.



Click『Virtual IP Address Pool』to view the policies, protocols, and states of virtual IP address pools.

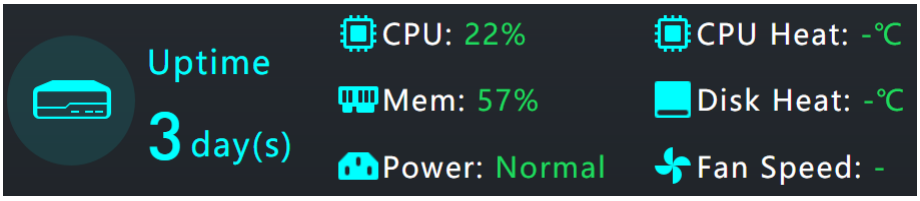


Click『Status』→『Data Center』to display the relevant status of the data center server. You can check the data center's health degree and other relevant states, such as Concurrent Conns, New Conns, Throughput, etc. The interface is shown as follows:



5.2 Device Status

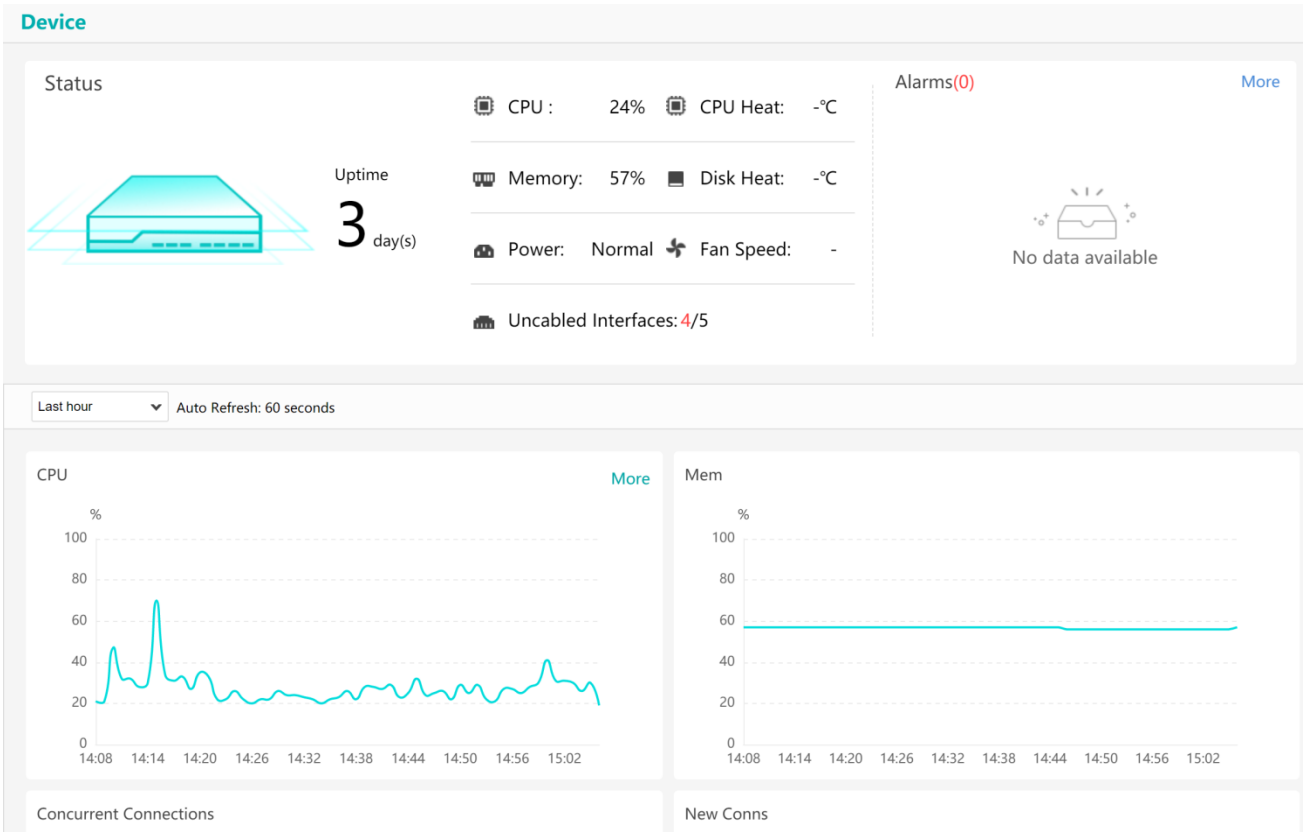
『Uptime』 section displays the following information of the ADC in a real-time manner: CPU utilization, CPU Heat, Mem usage, Disk Heat, Power status, and Fan Speed.



Details are displayed in 『Status』 → 『Device Status』 .

『Status』 → 『Device Status』 page is shown in the figure below. Alarms will be displayed on the right side. Click items to skip to relevant pages.

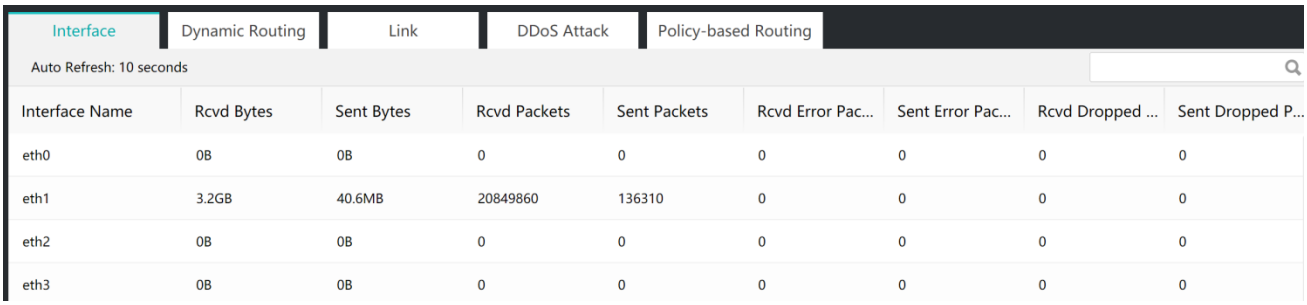
Line charts of system parameters (CPU, Mem, Concurrent Connections, New Conns, and Throughput) are shown below.



5.3 Network Status

5.3.1 Interface

『Interface』 shows the status of network interfaces on the device, including Rcvd & Sent Bytes, Rcvd & Sent Packets, etc.



Interface Name	Rcvd Bytes	Sent Bytes	Rcvd Packets	Sent Packets	Rcvd Error Pac...	Sent Error Pac...	Rcvd Dropped ...	Sent Dropped P...
eth0	0B	0B	0	0	0	0	0	0
eth1	3.2GB	40.6MB	20849860	136310	0	0	0	0
eth2	0B	0B	0	0	0	0	0	0
eth3	0B	0B	0	0	0	0	0	0

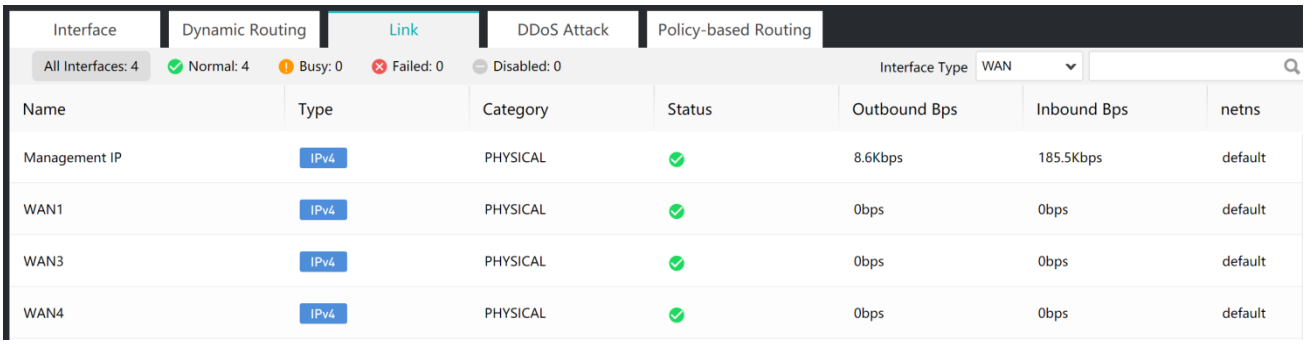
5.3.2 Dynamic Routing

Click『Dynamic Routing』to view routes learned by the device through RIP or OSPF.



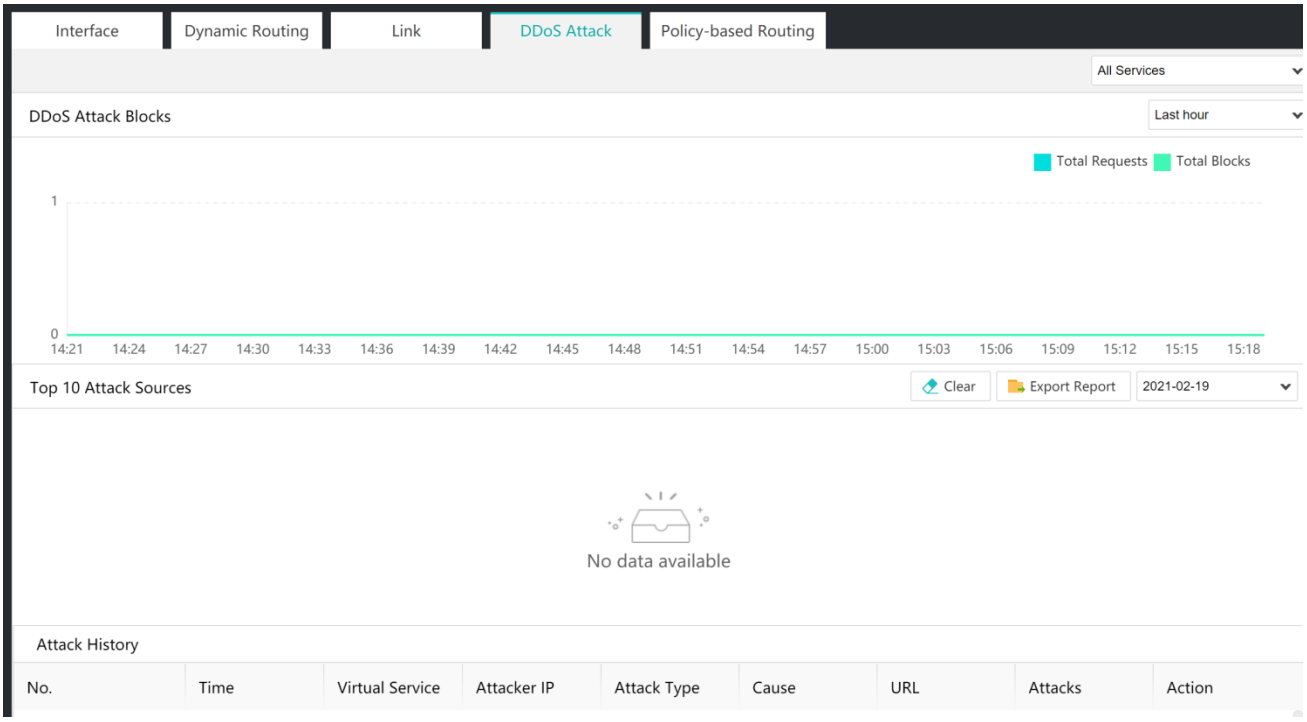
5.3.3 Link

『Link』shows traffic and status of all links.



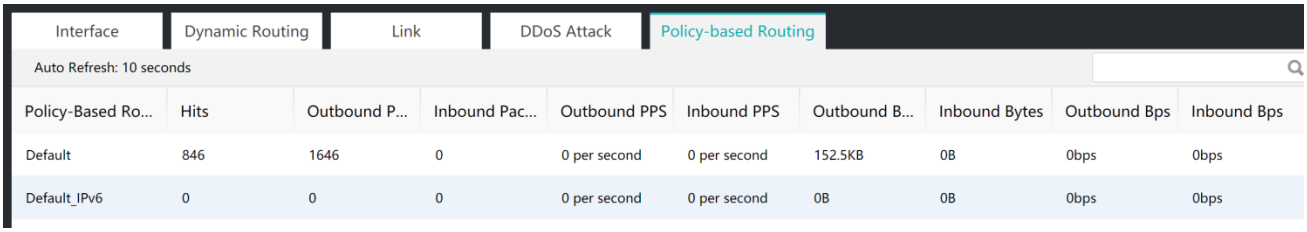
5.3.4 DDoS Attack

『DDoS Attack』analyzes Layer 7 DDoS attacks, including DDoS Attack Blocks, TOP 10 Attack Sources, and Attack History.



5.3.5 Policy-based Routing

『Policy-based Routing』displays the status of policy-based routing service. You can view the policy Hits, Outbound & Inbound Packets, Outbound & Inbound PPS, etc.

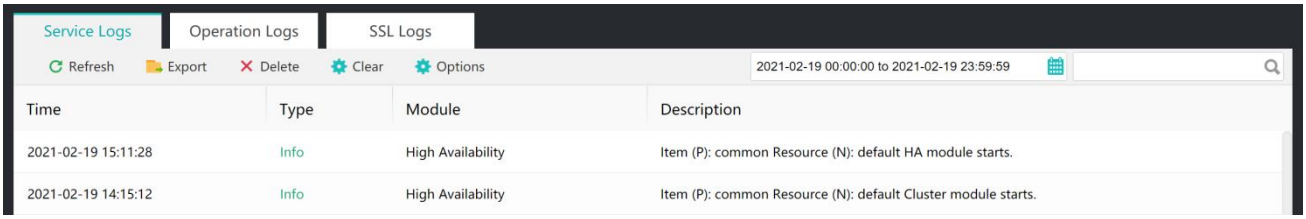


5.4 Logs

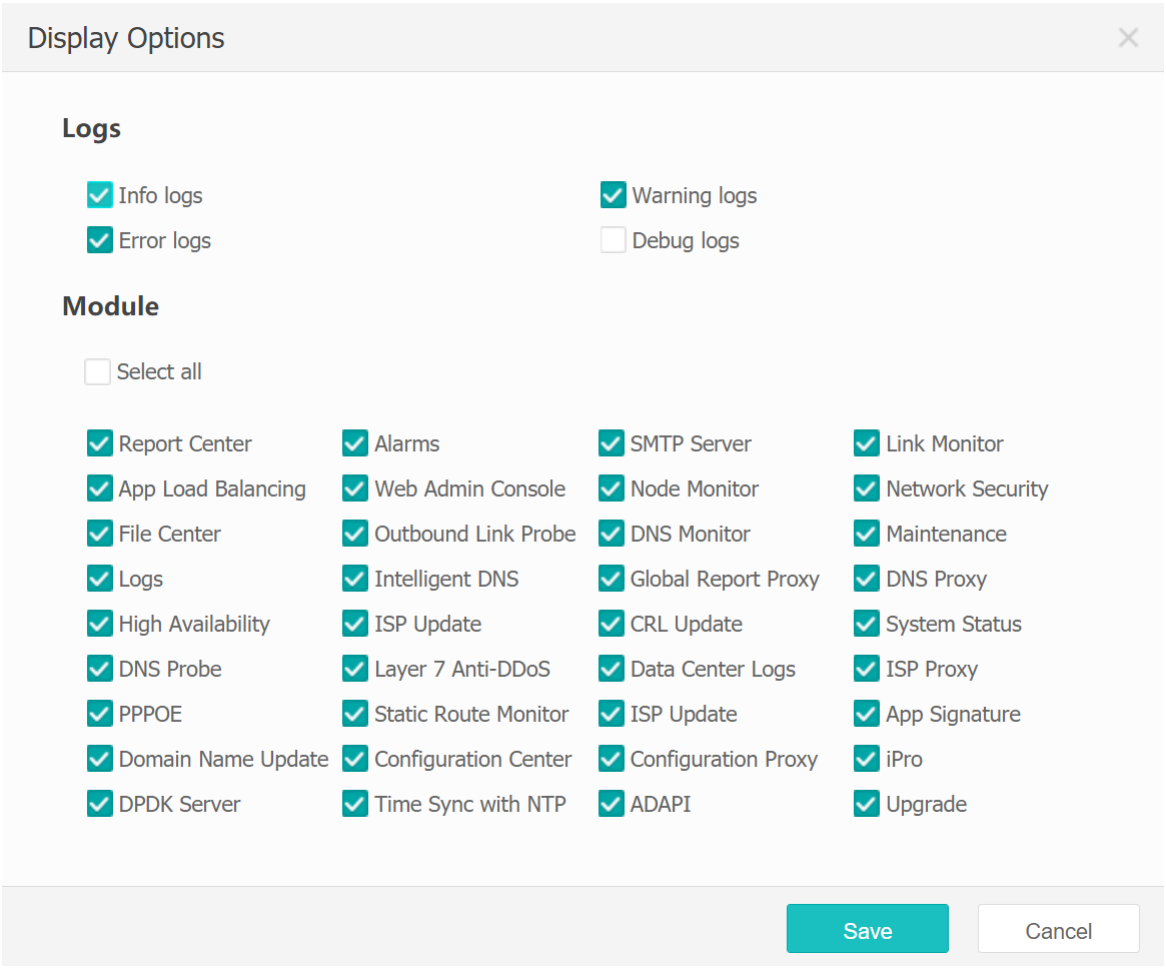
It is used to view running logs and error prompts of the device. Running logs include Service Logs, Operation Logs, and SSL Logs.

5.4.1 Service Logs

Click『Service Logs』to view the system log information of the current device.



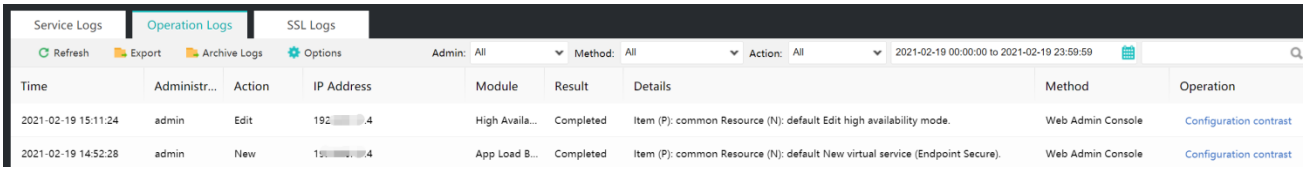
Click Options to configure Service Logs. Check the boxes before the options to set items to be displayed in a service log.



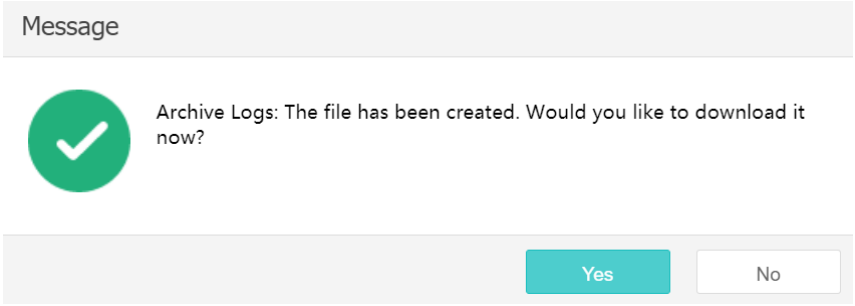
5.4.2 Operation Logs

Click『Operation Logs』to view the log information showing the operations performed by the current device administrator on the device. It can be viewed according to Administrator, Operation,

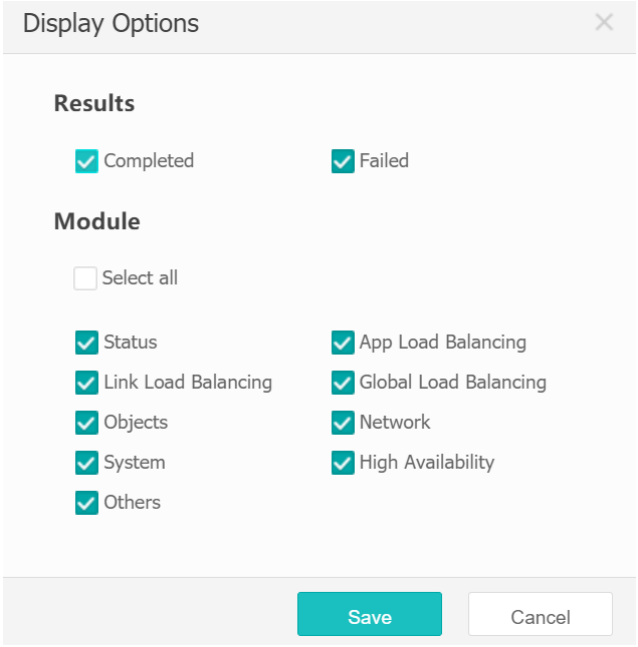
Action, and Time.



Click Archive Logs to archive and download logs. Click Yes to download log files.



Click Options to configure Operation Logs. Check the boxes before the options to set items to be displayed in an operation log.



5.4.3 SSL Logs

『SSL Logs』 displays logs of SSL client authentication failure. Filter and view the log information of a corresponding period according to time.



Chapter 6 Objects

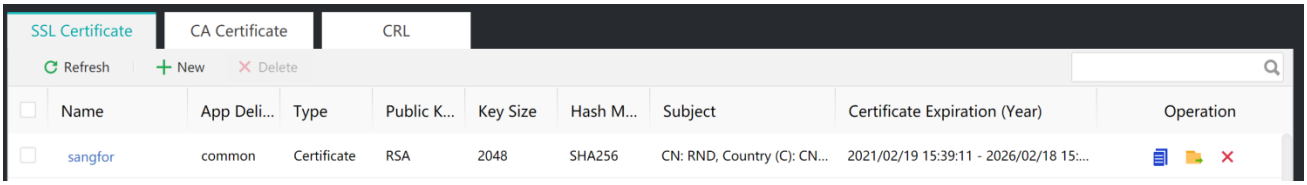
6.1 Certificates

【Operation Scenarios】

SSL is used to establish an encrypted connection between the ADC and the client. If the server publishing the service has a server certificate, the server certificate can also be imported into the ADC for unified management, which can reduce the load on the server to a certain extent. If the server publishing the service does not have a server certificate, you can choose to generate a certificate by operating the ADC or apply for a certificate issued by a third-party CA, ensuring that when the client accessing the service, an encrypted connection will be established between the client and the ADC for implementing data encryption. Certificates in『Objects』can be used for the configuration of『App Load Balancing』→『Virtual Service』.

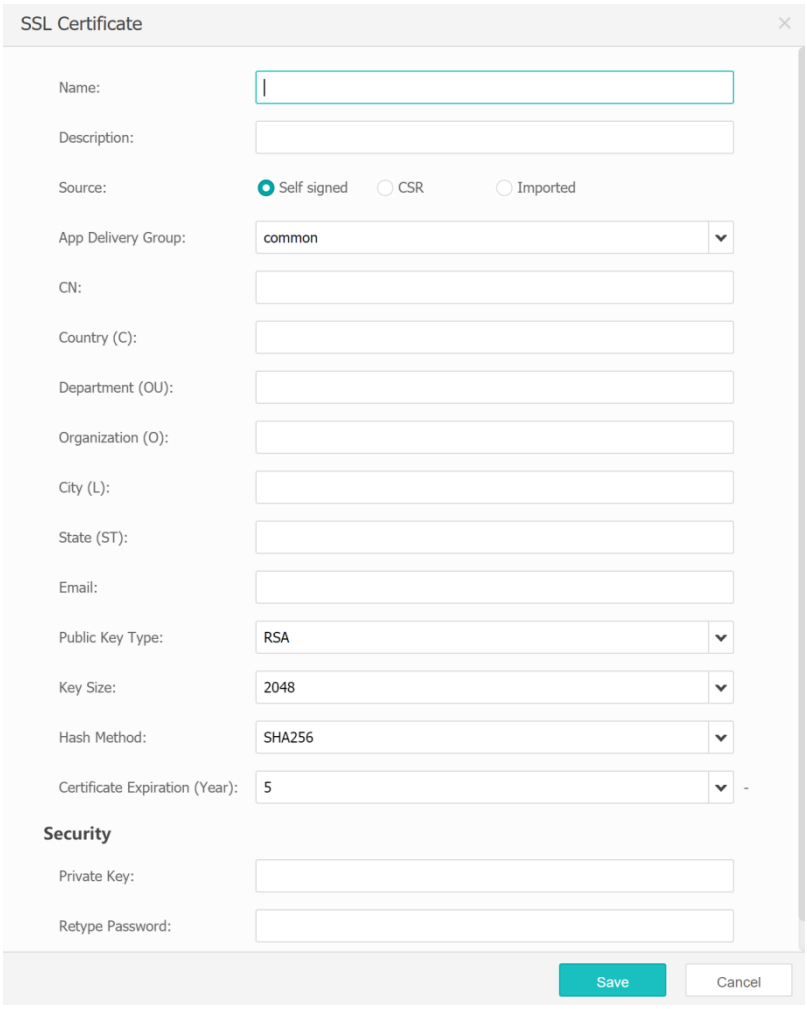
6.1.1 SSL Certificate

【Operation Procedure】



Click Delete button to delete a selected SSL certificate. However, an SSL certificate associated with virtual services cannot be deleted.

Click New to open the【SSL Certificate】configuration window.



『Source』 selects the type of SSL certificates issued. If [Self signed] is selected, a complete certificate will be generated. If [CSR] is selected, a certificate request will be generated and sent to CA for signature. If [Imported] is selected, the certificate will be imported from a file.

『Common Name (CN)』 configures the name of the SSL certificate user.

『Country (C)』 configures the English abbreviation of the country where the SSL certificate user is located.

『Department (OU)』 configures the department to which the SSL certificate user belongs.

『Organization (O)』 configures the company or organization that the SSL certificate user works for.

『City (L)』 configures the city where the SSL certificate user is located.

『State (ST)』 configures the province/state where the SSL certificate user is located.

『Email』 configures the E-MAIL address used by the SSL certificate user.

『Public Key Type』 includes RSA and ECDSA.

『Key Size』 can be selected from [1024], [2048] or [4096].

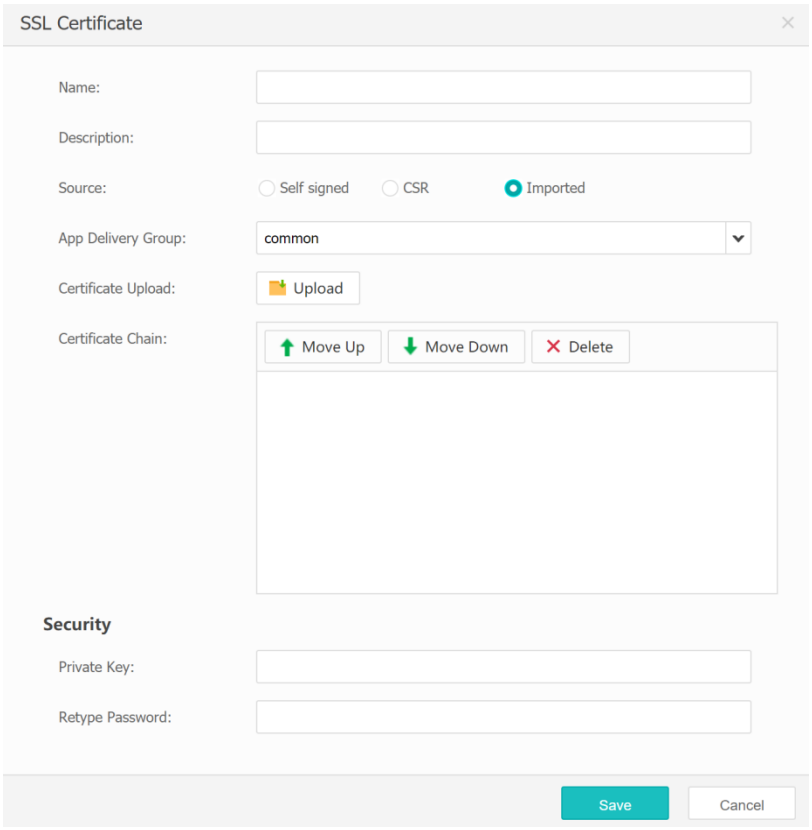
『Hash Method』 includes SHA256 and SHA1.

『Certificate Expiration (Year)』 is the validity period of the self-signed SSL certificate.

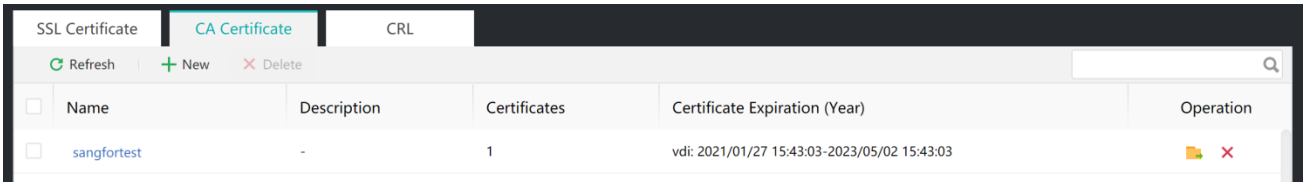
『Private Key』 adds private key password (optional).

『Retype Password』 confirms the private key password.

If [Imported] is selected for Source, the following interface will be displayed. Click Upload, select the file and click Save.

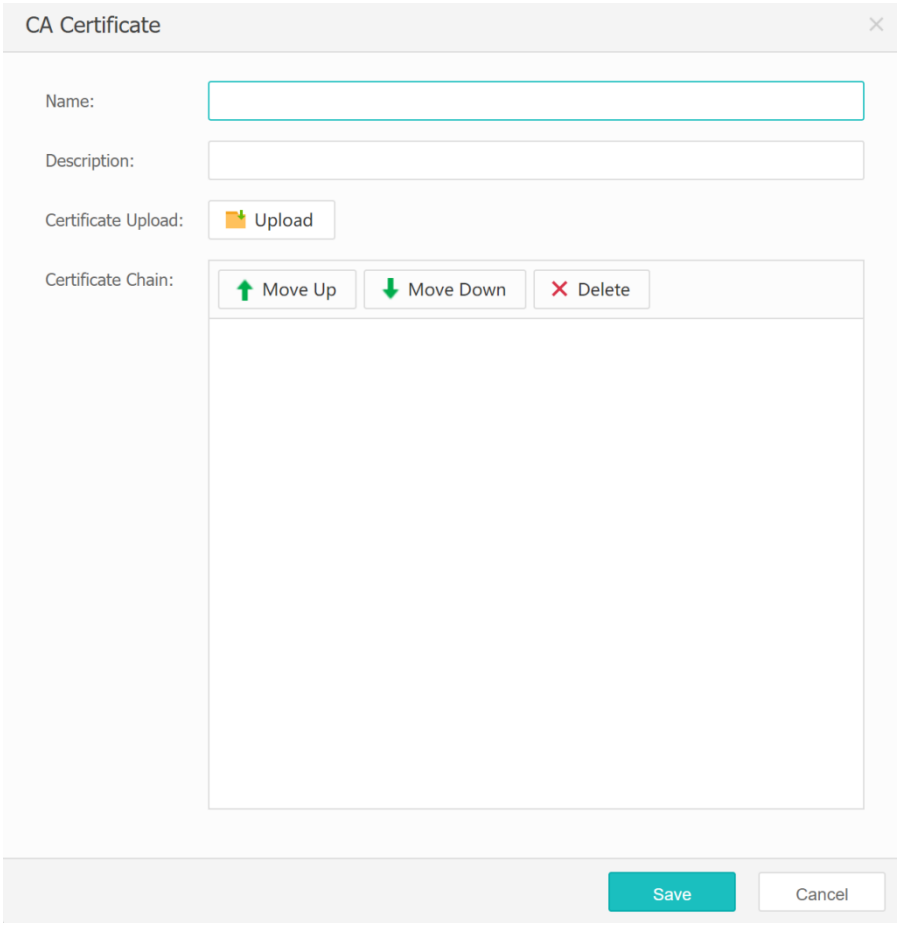


6.1.2 CA Certificate



【Operation Procedure】

Click New to create a CA certificate as shown below.



Enter the『Name』field with a character string that is easy to remember and identify, which is used to identify the name of the new CA certificate.

Click Upload to import a local CA certificate file.

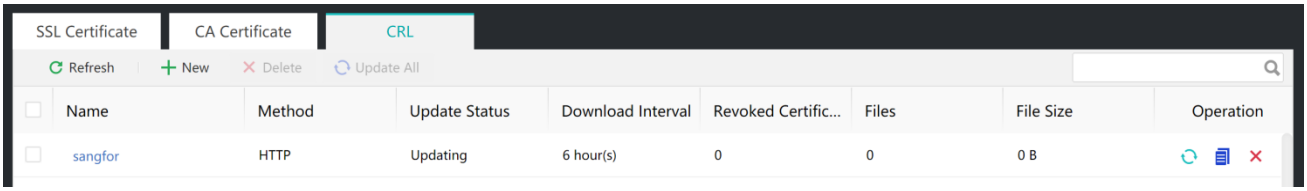
6.1.3 CRL

【Operation Scenarios】

CRL means Certificate Revocation List, which is used to revoke certificates. The Name, Method, Download Interval, Update Status, etc. of the revocation list are displayed in the CRL interface.

【Operation Procedure】

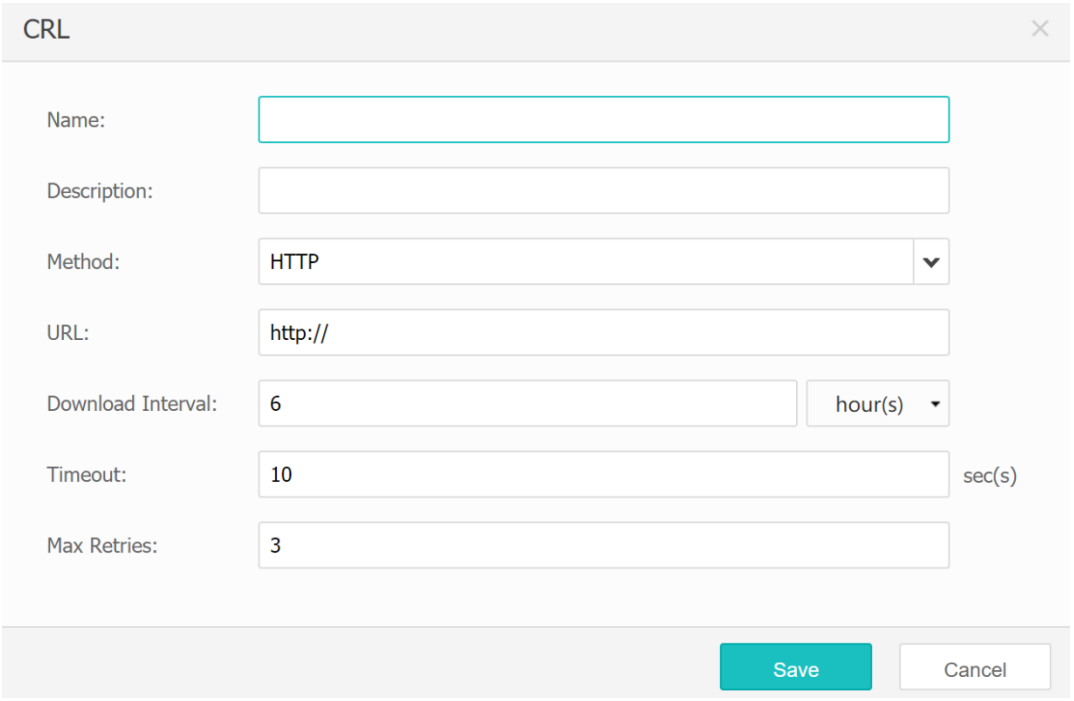
See the figure below:



Click Update All to update the items selected and displayed in the revocation list in batch.

Click  on the right side of a single item to update the item.

Click New to display the following page:



『Method』 can be selected from HTTP, FTP, Uploaded from local PC, and LDAP.

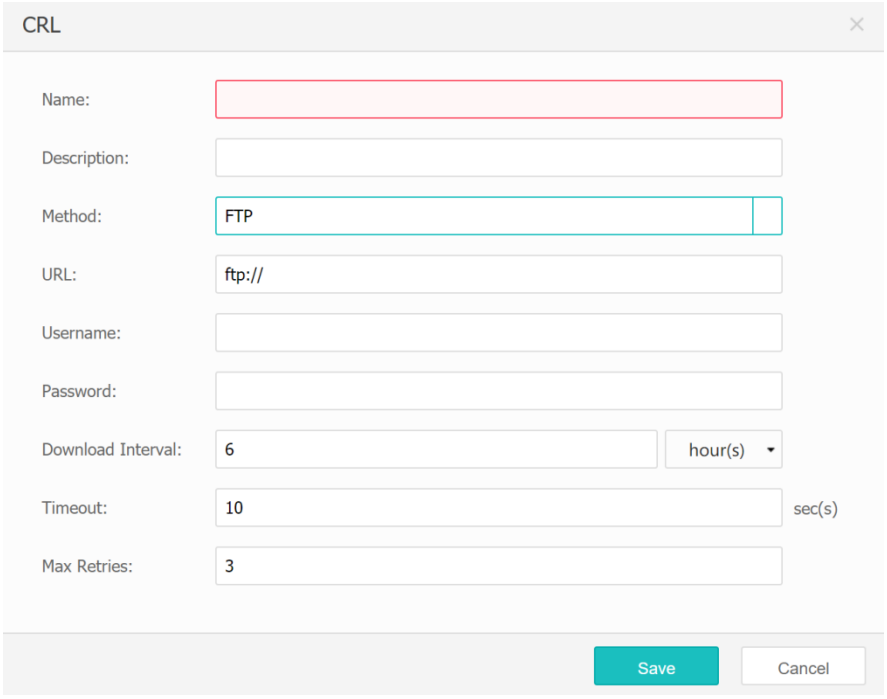
Fill in 『URL』 with the site URL for downloading CRL.

Fill in 『Download Interval』 with the interval of downloading CRLs, and the maximum can be 30 days.

Fill in 『Timeout』 with the timeout duration set for CRL download. If a CRL cannot be downloaded within the timeout duration, the system will try again.

Fill in『Max Retries』with the number of retries.

If FTP is selected for『Method』, the interface is shown below:

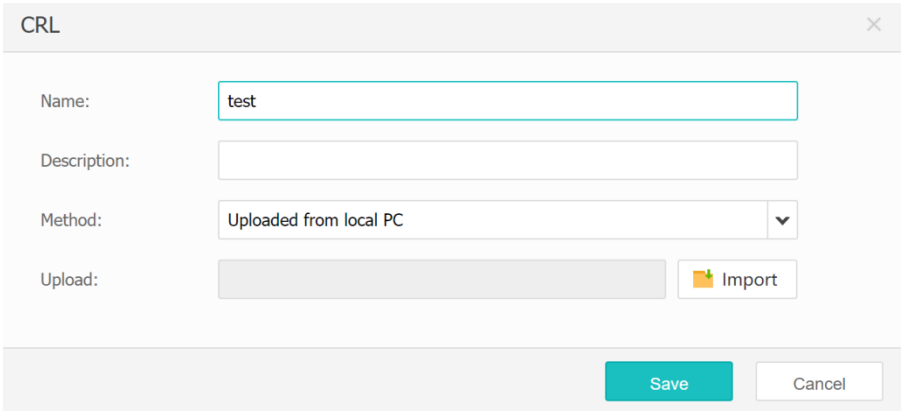


Fill in『URL』with the IP address for downloading CRL.

Fill in『Username』with the username for FTP access.

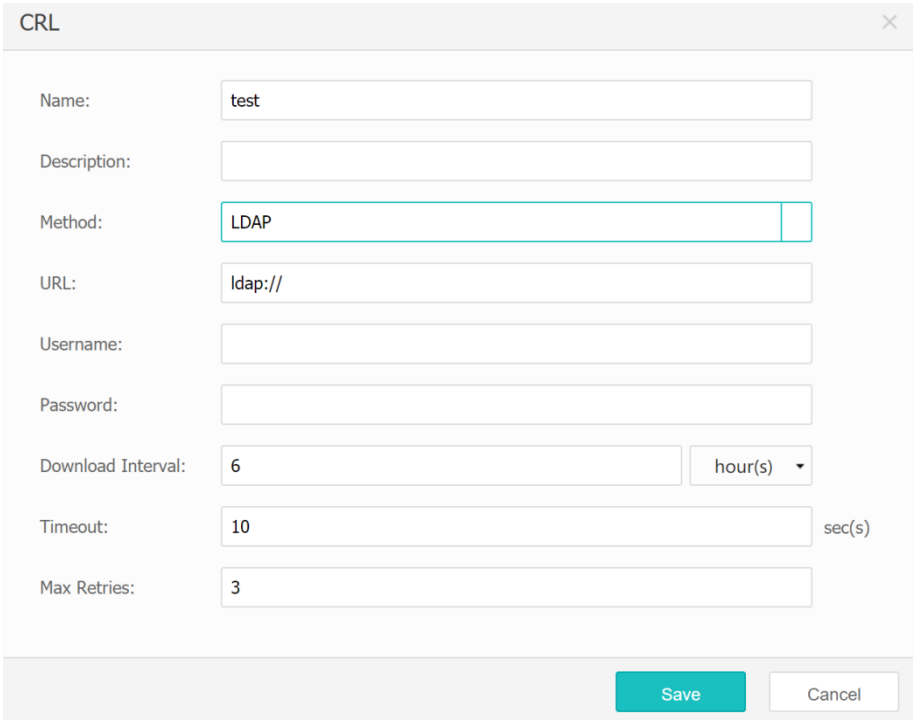
Fill in『Password』with the password for FTP access.

If Uploaded from local PC is selected for『Method』, the interface is shown below:



Click『Import』to upload a local CRL to the device.

If LDAP is selected for『Method』, the interface is shown below:



Fill in『URL』with the IP address for downloading CRL.

Fill in『Username』with the username for LDAP access.

Fill in『Password』with the password for LDAP access.

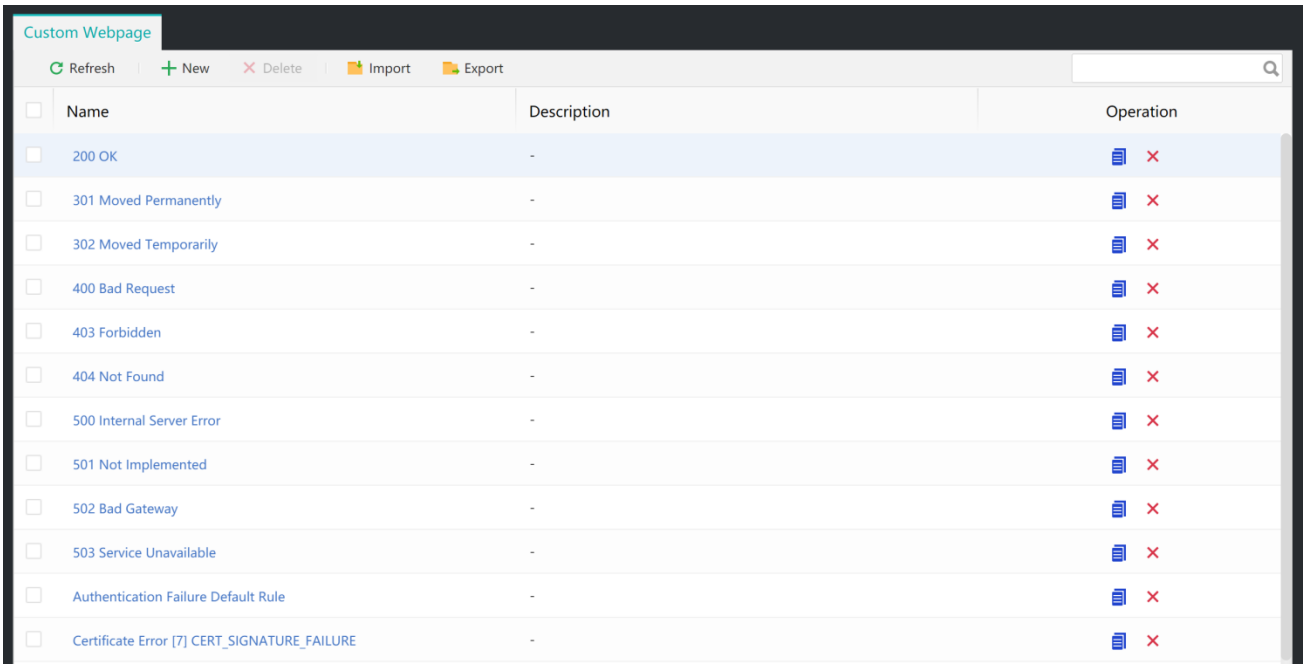
6.2 Custom Webpage

WEBUI path:『Objects』→『Custom Webpage』.

6.2.1 Custom Webpage

【Operation Scenarios】

『Custom Webpage』defines a page to be returned, which is referenced in『App Load Balancing』→『Scheduling Policy』, and the returned custom webpage is set in the scheduling policy.

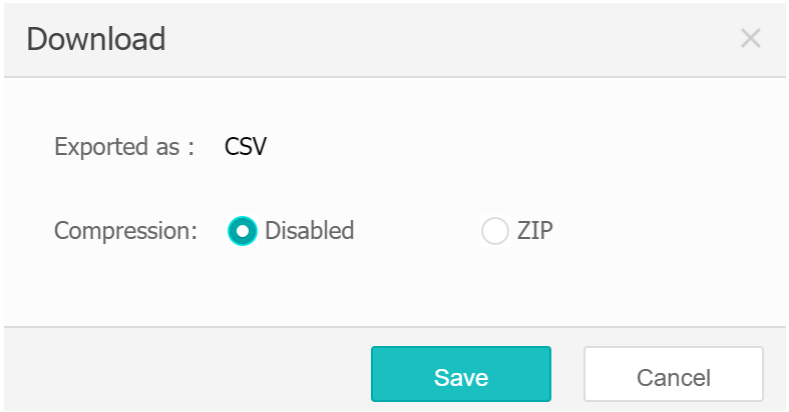


【Operation Procedure】

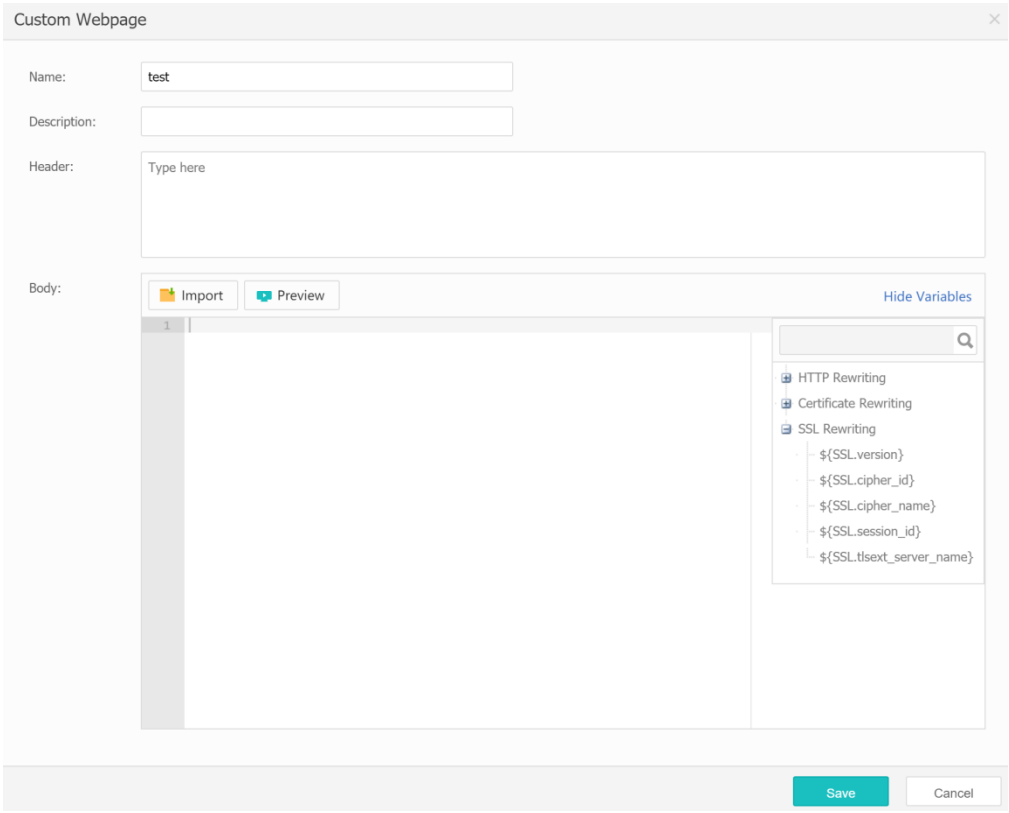
『Custom Webpage』 displays the names and actions of the custom pages. The device defines some templates for pages returned by default, and you can click  to copy the content of a template on the custom page.

Click Import to import local CSV files.

Click Export to export the selected content. Select the desired Compression method and click Save.



Click New to display the following configuration page:



『Header』 and 『Body』 set customized contents. The configuration of Header and Body is completed in two input boxes respectively. The format of Header is automatically converted from Unix to Dos. Click Import for the Body box to import an HTML file and click Preview to preview the configured page. For example, the preview interface of 404 Not Found is shown below:



6.3 Databases

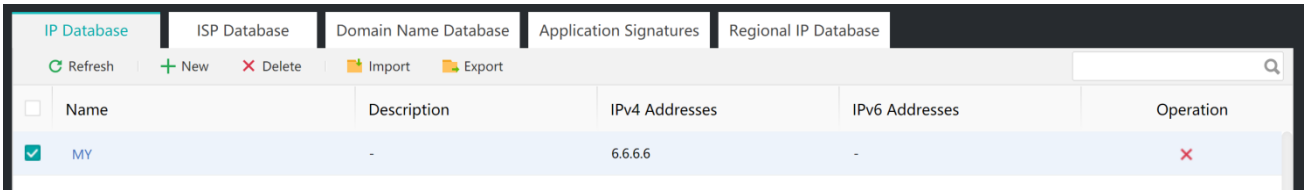
WEBUI path: 『Objects』 → 『Databases』 .

6.3.1 IP Database

【Operation Scenarios】

『IP Database』 defines an internal IP address range. For example, special policies are required for some IP addresses on an internal network. IP Database can be referenced in Policy-Based Routing,

SNAT, Scheduling Policy, and ACL module.

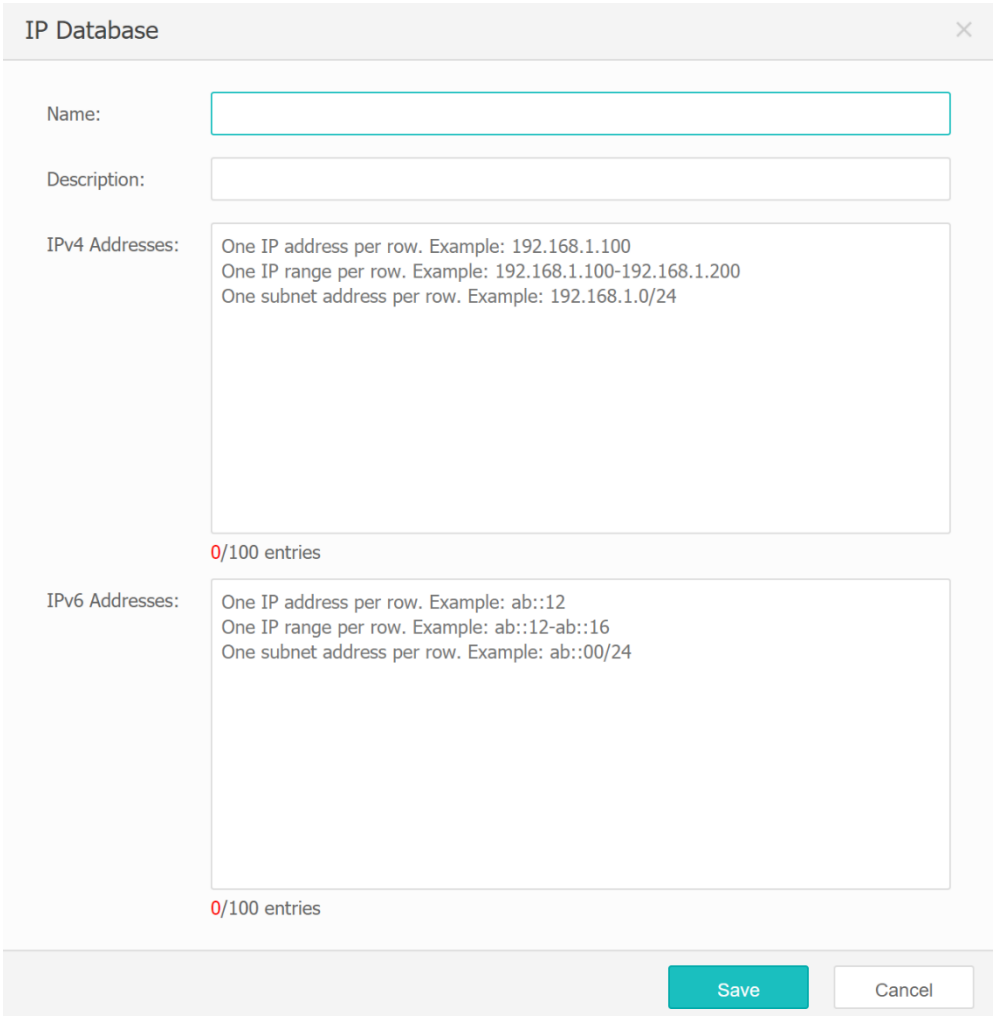


【Operation Procedure】

Click the button Import to import IP addresses into 『IP Database』 from a custom file.

Click the button Export to export IP addresses from 『IP Database』 to a CSV file.

Click New to create a new IP database. The configuration interface is shown below:



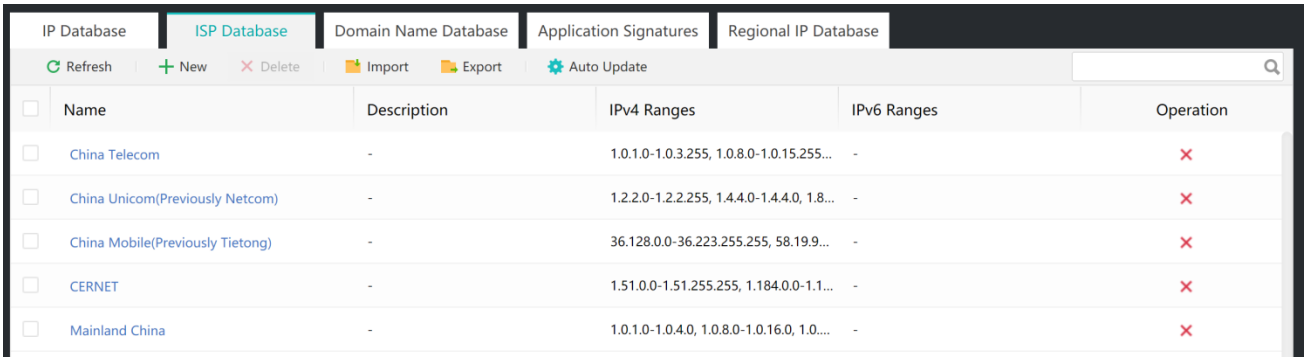
Fill in 『IP Addresses』 with one IP address/IP range/subnet address per row. It is used to customize the IP range of internal IP groups and supports IPv4 or IPv6 addresses.

6.3.2 ISP Database

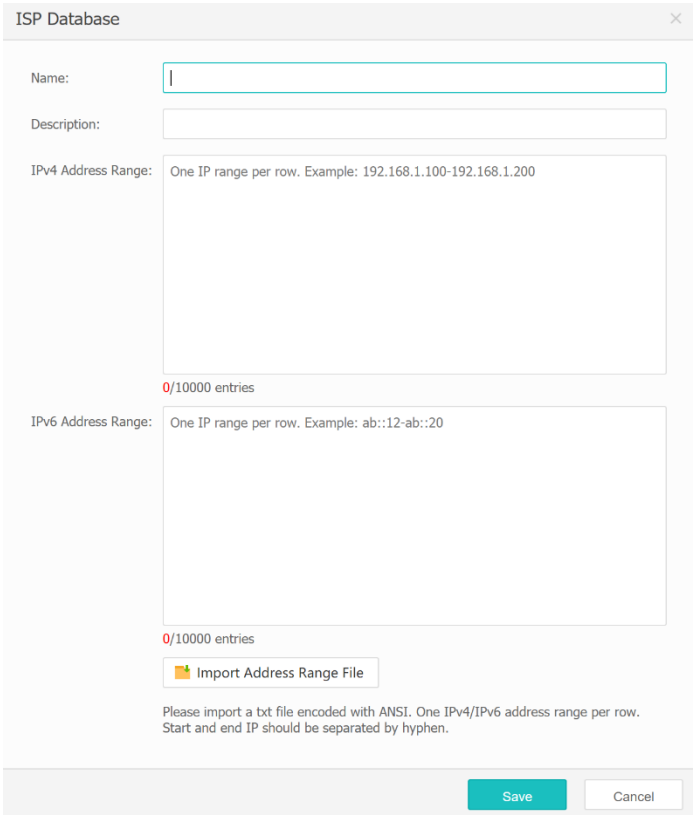
【Operation Scenarios】

『ISP Database』 sets the IP address range for a network carrier. The IP address range is mainly used for configuring Policy-Based Routing. By default, the device has collected IP address ranges owned by China Telecom, China Unicom (formerly China Netcom), China Mobile (formerly Tietong), Education Network, and Mainland China IP database.

【Operation Procedure】



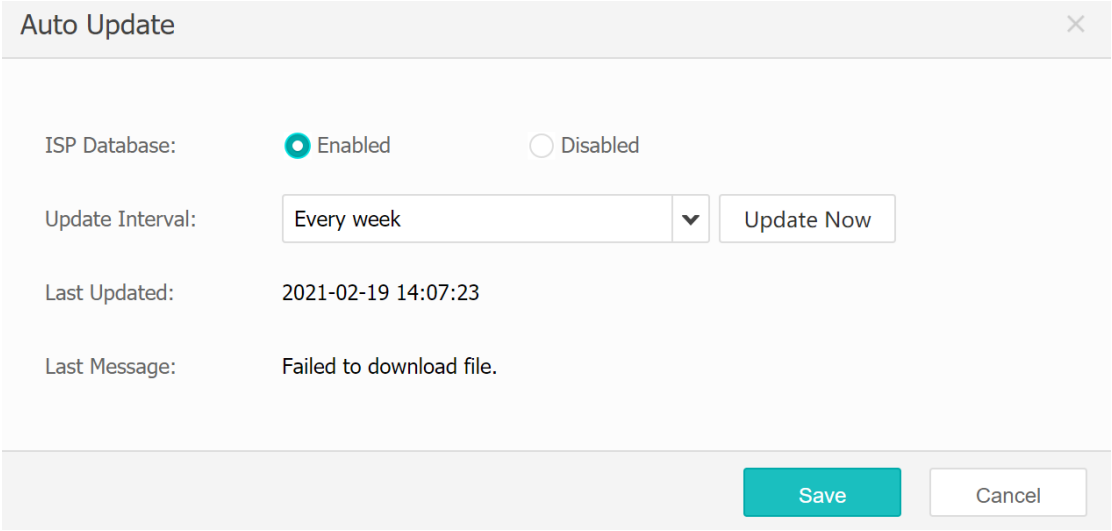
Click New to create a new ISP database. The configuration interface is shown below:



『Address Range』 manually sets the network IP segment owned by a carrier.

『Import Address Range File』manually imports address range files to the ADC, supporting txt files encoded with ANSI.

Click Auto Update to select and finish ISP database update settings, or directly perform Update Now.

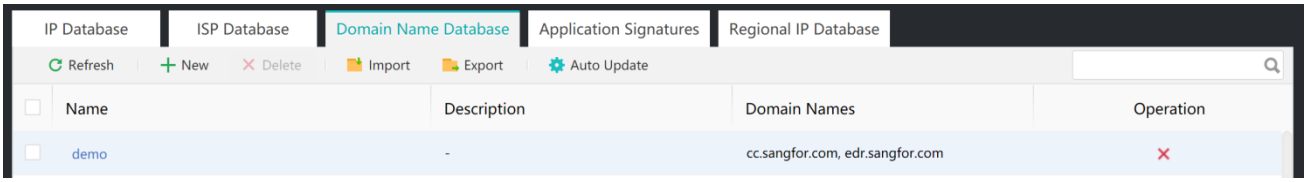


6.3.3 Domain Name Database

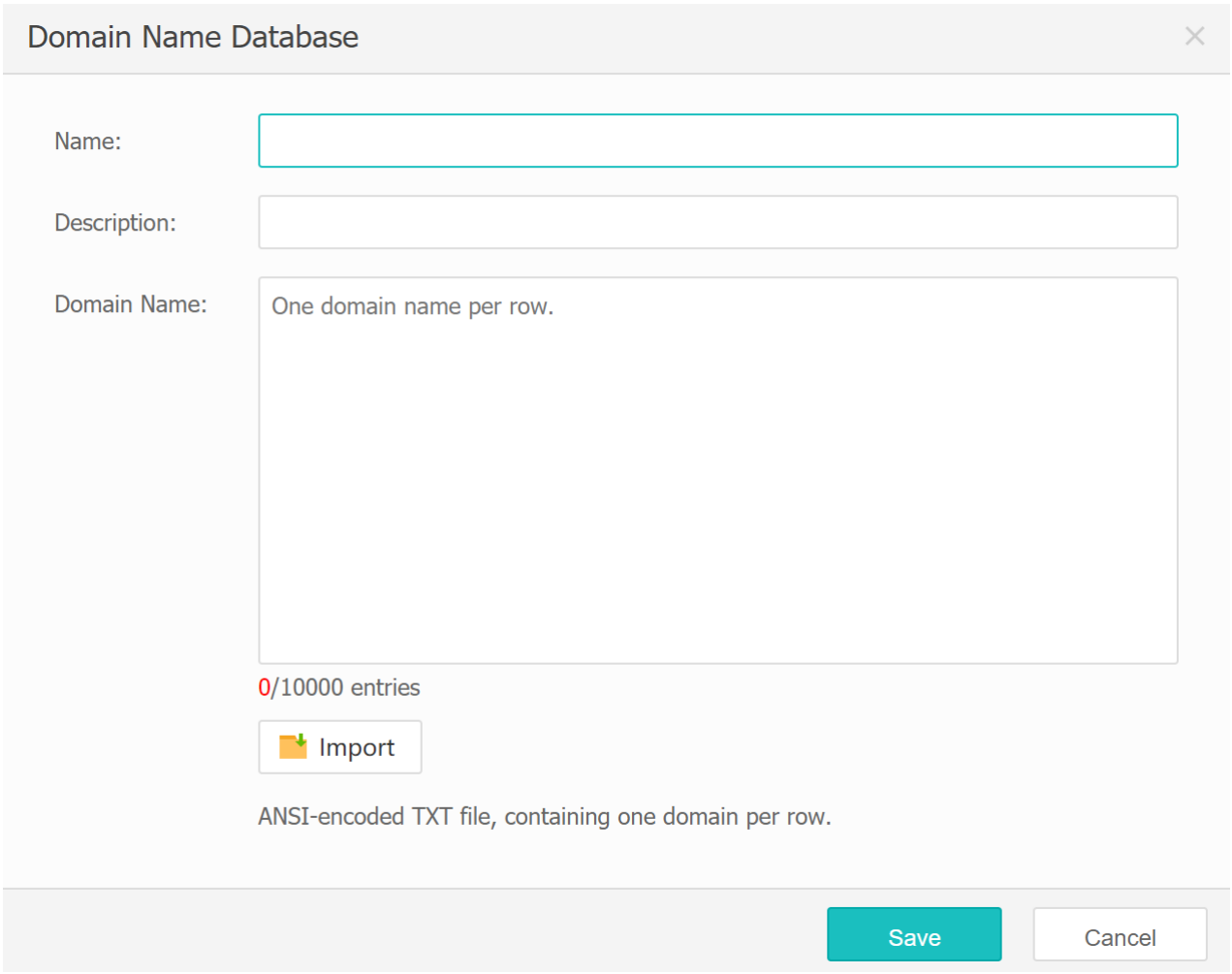
【Operation Scenarios】

"Domain Name Database" defines a domain name database that is mainly used for configuring Policy-Based Routing. The device has already collected data from foreign domain name databases by default.

【Operation Procedure】



Click New to create a new domain name database. The configuration interface is shown below:



『Domain Name』manually sets domain names of the database.

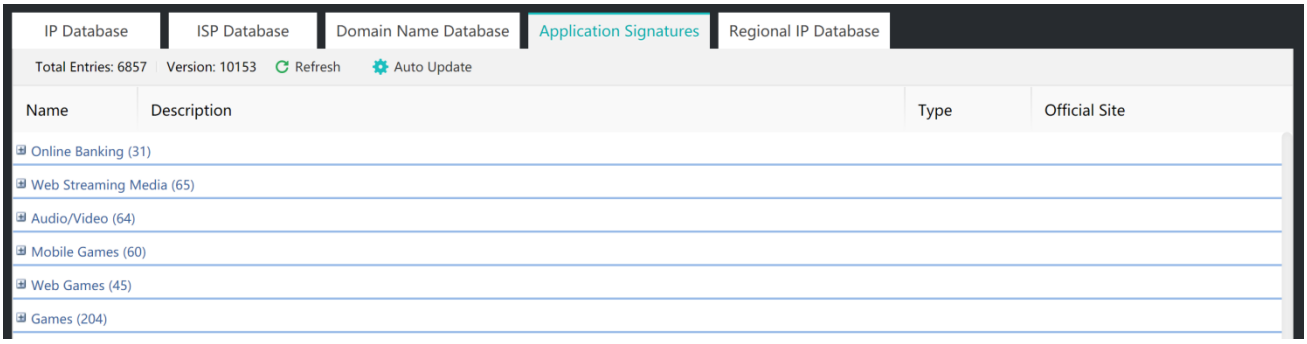
『Import』manually imports domain name files to the ADC, supporting txt files encoded with ANSI.

6.3.4 Application Signatures

【Operation Scenarios】

『Application Signatures』specifies the IP addresses of applications of the same category. Application categories include Online Banking, Web Streaming Media, Audio/Video, Mobile Games, Web Games, and Games. Use Policy-Based Routing to select routes according to applications.

【Operation Procedure】



『Application Signatures』displays Total Entries, Version, and Name of applications.

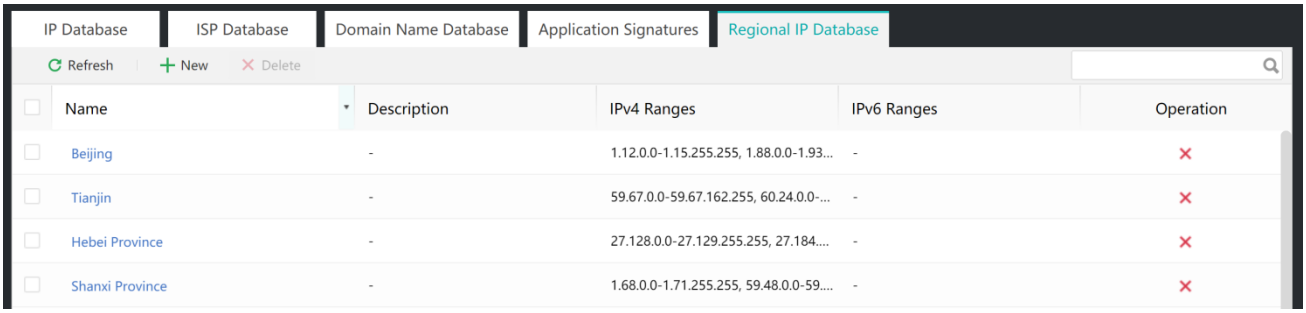
Click Auto Update to update Application Signatures to the latest version.

6.3.5 Regional IP Database

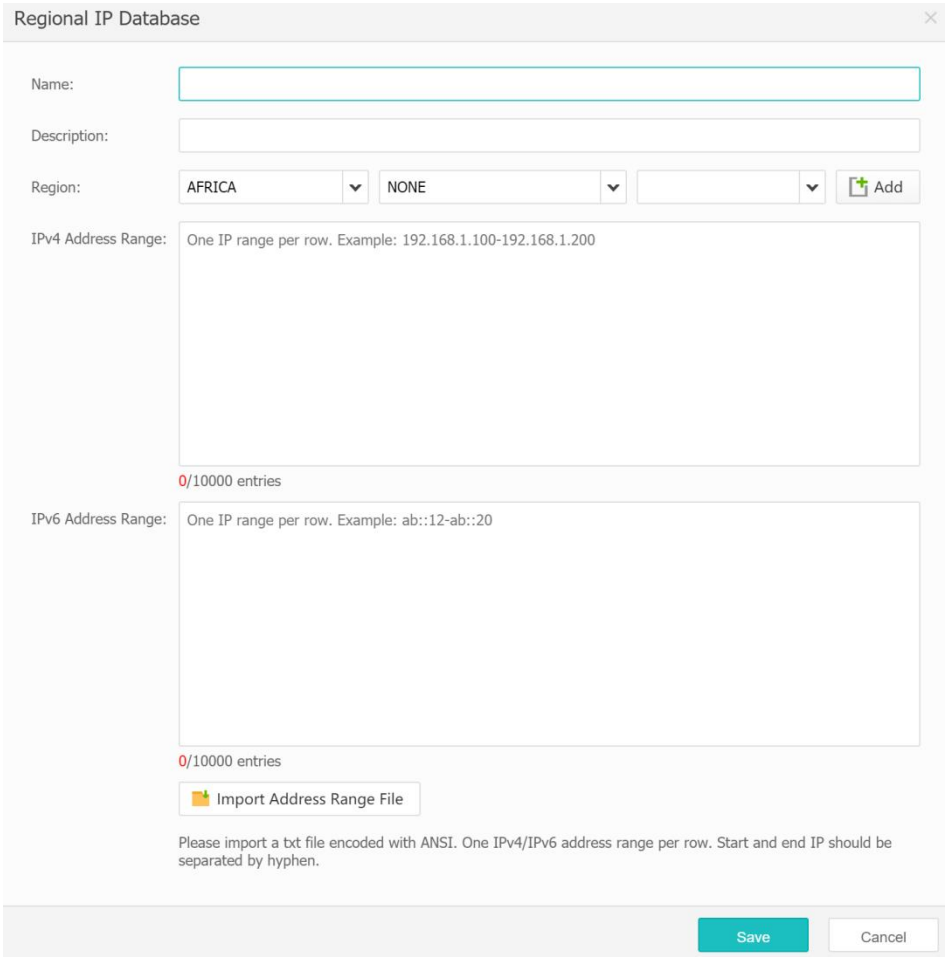
【Operation Scenarios】

『Regional IP Database』configures WHOIS flags corresponding to regions as well as regional IP address ranges, so as to identify the region where a visiting user is located.

【Operation Procedure】



Click New to add a new Regional IP Database, as shown in the figure below:



『Region』 sets the region where you are located by selecting the Plate, Country, Province/State, and City. Click Add to add IP addresses for 『Region』 .

『Address Range』 displays IP ranges added for 『Region』 . You can also manually enter IP range(s).

『Import Address Range File』manually imports address range files to the ADC, supporting txt files encoded with ANSI.

6.4 Multi-Tenancy

【Operation Scenarios】

Multi-Tenancy can provide multiple isolated network environments with configuration information. In a tenant scenario, the service configuration information of a tenant is not visible to others, and each tenant is unaware of others.

Multi-tenancy applies to both cloud and non-cloud scenarios.

The following concepts need to be clarified:

netns: refers to the smallest unit of service configuration in a multi-tenancy scenario. The networks among various netns are isolated. A set of independent app load balancing-dependent configurations can be deployed in a netns environment.

App Delivery Group: refers to a collection of netns. Each netns only belongs to one Group, but one Group can include one or more netns. The resources for tenants are distributed based on the granularity of a Group instead of netns.

Tenant: one tenant can be associated with one or multiple Groups. The tenant can check and edit associated Groups as well as netns configuration contained in Groups.

【Operation Procedure】

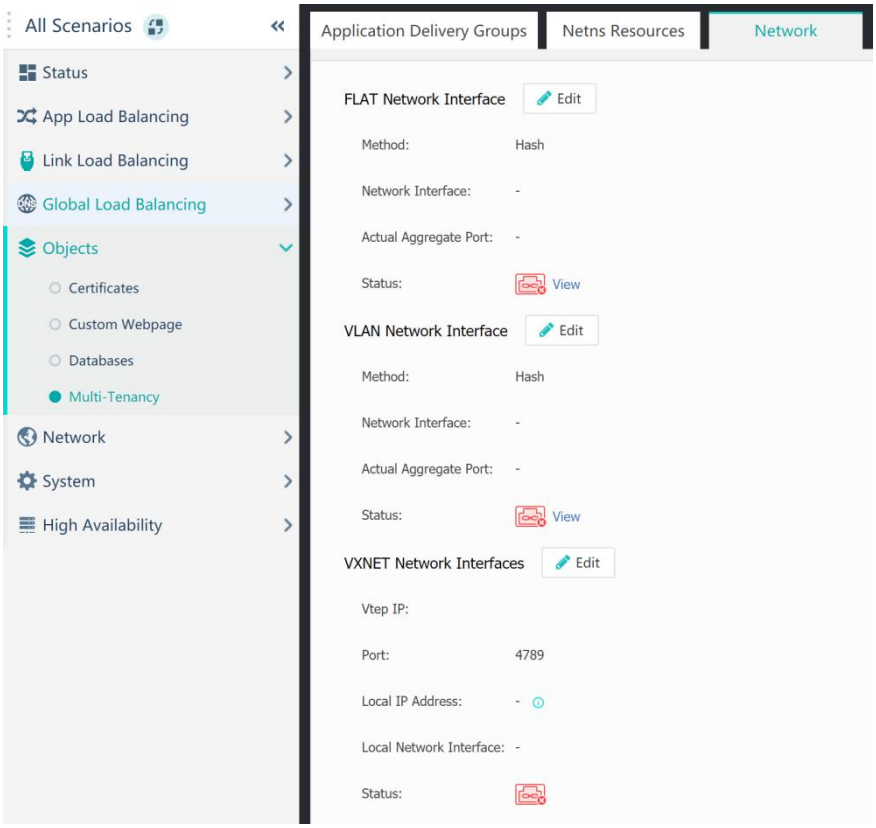
1. Mode Switch

Please firstly enable the multi-tenancy mode before performing mutli-tenancy configuration. Refer to Section 4.5.8 for specific operations.

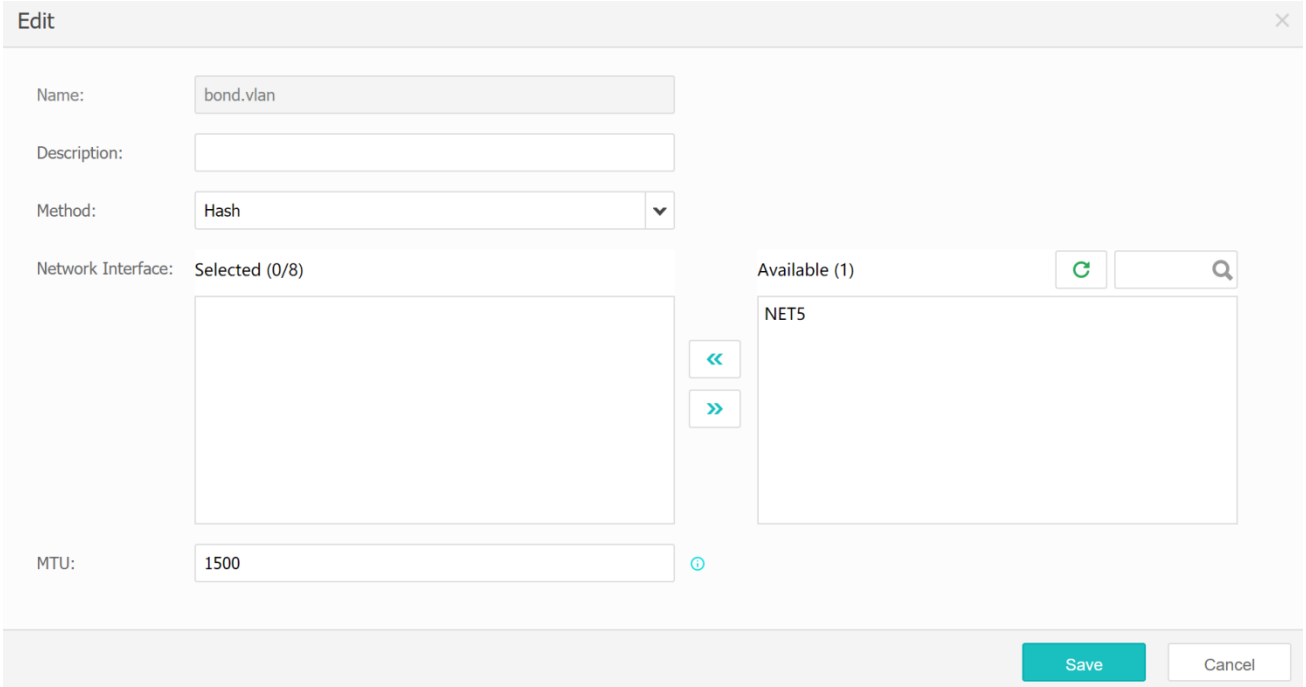
2. Multi-Tenancy Network Configuration

『Objects』 → 『Multi-Tenancy』 → 『Network』

The networks for tenants are isolated in the multi-tenancy scenario. At present, AD7.0.9 supports three types of tenant network, namely FLAT, VLAN and VXLAN.



Click the Edit button following VLAN Network Interface (the same operation should be performed for other types of tenant networks) to create a VLAN network.

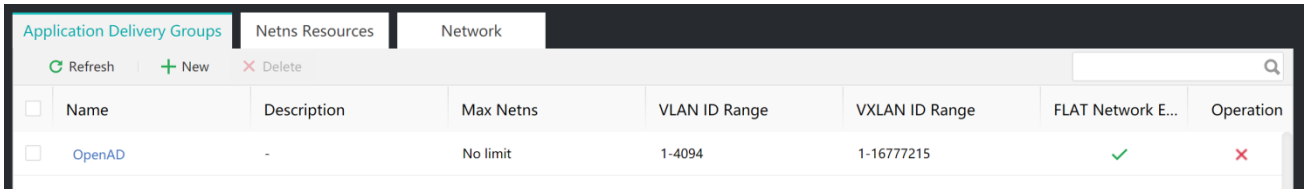


For『Method』, refer to Section 3.3.2. In general, the setting is left as default.

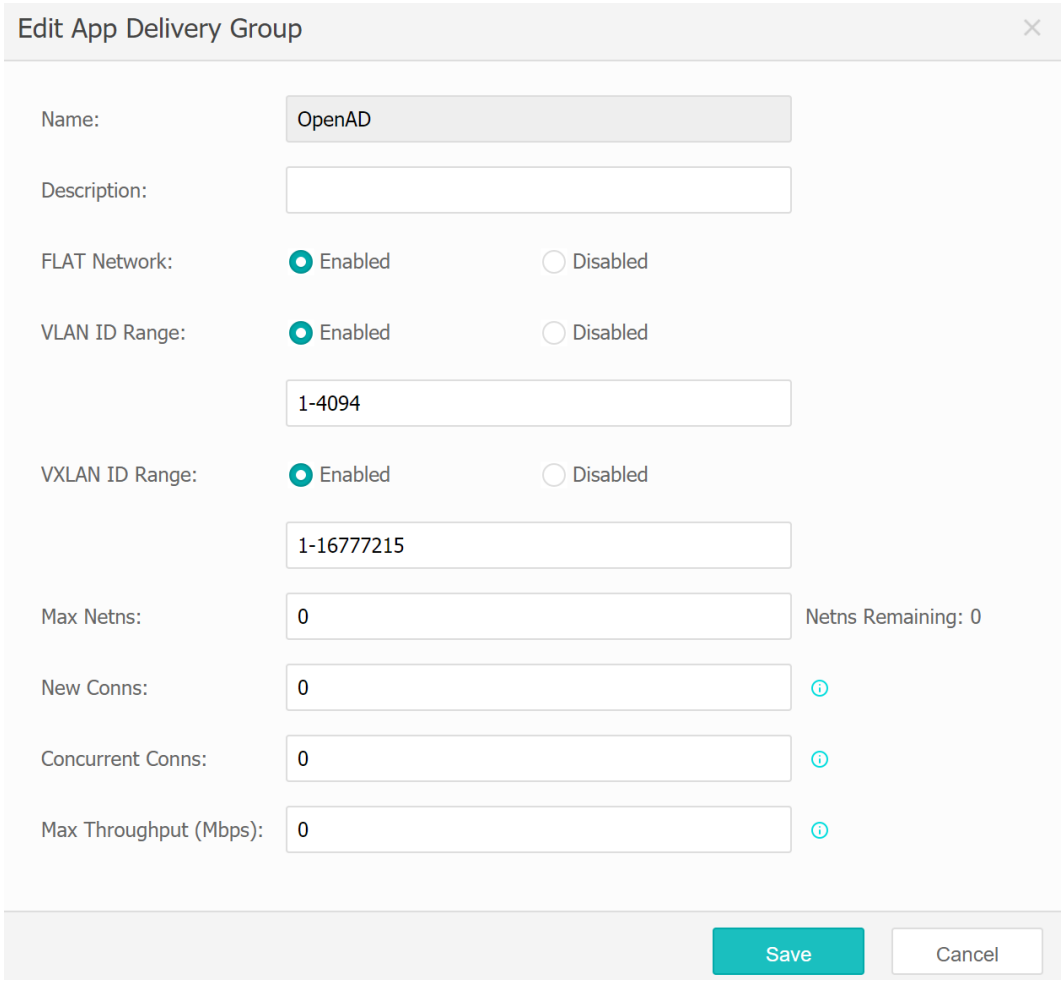
Select an Available interface as the network interface for the VLAN network, and one interface can only be referenced by one network type.

3. Application Delivery Groups

『Objects』 → 『Multi-Tenancy』 → 『Application Delivery Groups』



The network isolation mode as well as the upper limit of service capacity of a Group can be set in the configuration interface of the multi-tenancy group. Three indicators, including New Conns, Concurrent Conns and Max Throughput, are mainly applied to reflect the service capacity.



For 『FLAT Network/VLAN ID Range/VXLAN ID Range』, enable the desired network type based on the practical situation and then place the corresponding restrictions. If a VLAN network

is enabled and the VLAN ID range should be limited to 1-100, then the netns network configuration VLAN ID Range should be 1-100 when the network type of Group is set as VLAN.

『Max Netns』 limits the maximum number of Netns can be set for this Group.

『New Conns』 refers to the upper limit of the number of newly created connections per second of all virtual services in this Group. Please fill in as needed.

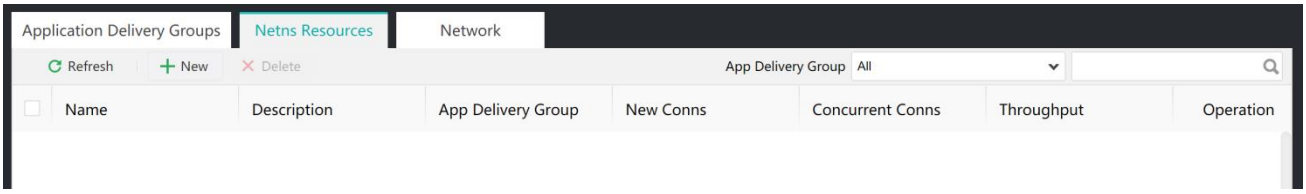
『Concurrent Conns』 refers to the upper limit of the number of connections maintained by all virtual services in this Group. Please fill in as needed.

『Max Throughput (Mbps)』 refers to the upper limit of throughput per second that can be achieved by all virtual services in this Group. Please fill in as needed.

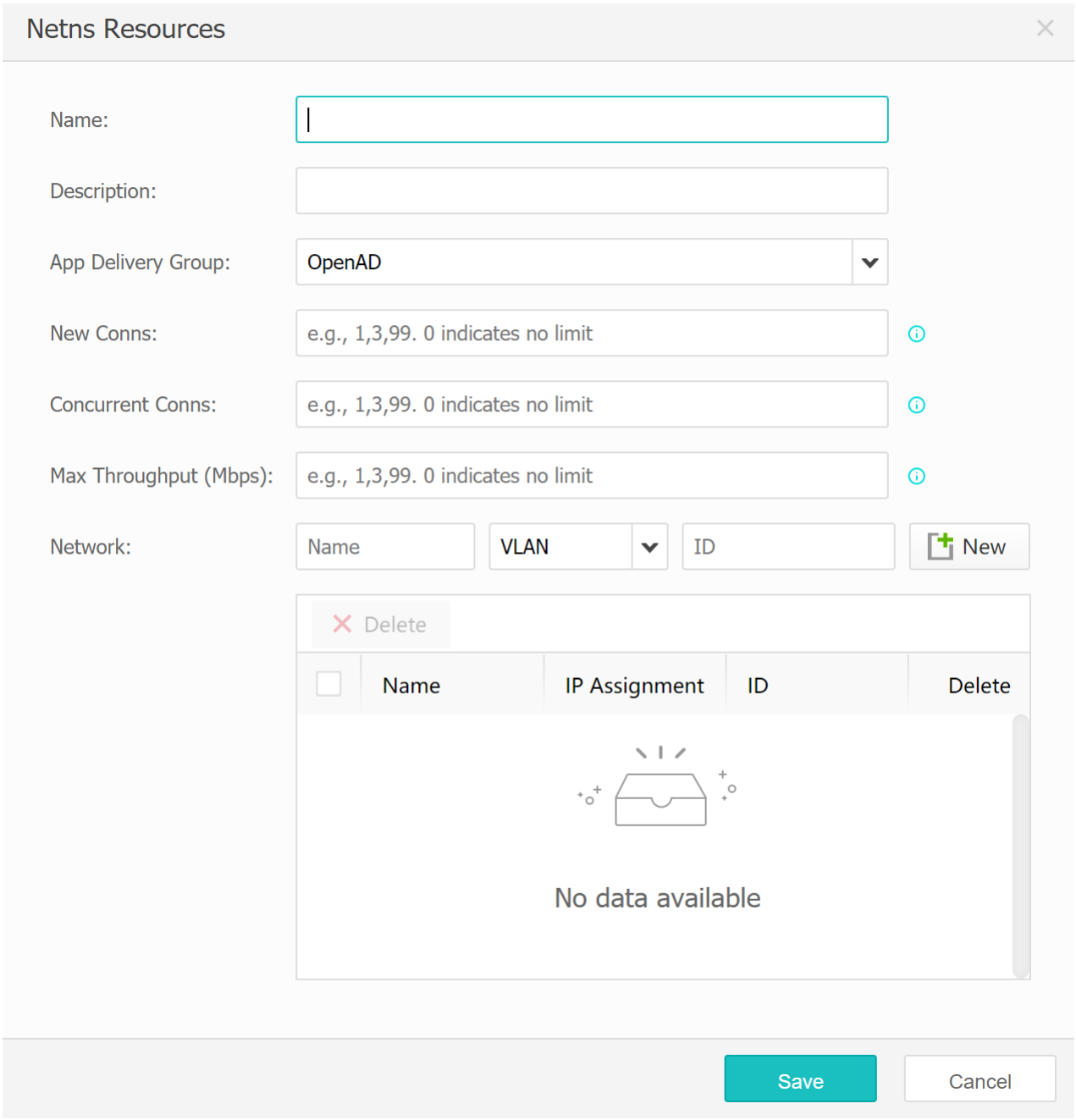
Attention: The system is built with the common Group in the multi-tenancy scenario. The server load balancing, link load balancing, global load balancing, etc. can be configured under this Group. However, only the server load balancing configuration is available under other netns. When upgrading from a previous version to AD7.0.9, the configuration related to app load balancing in the older version will be automatically assigned to the common Group.

4. Netns Resources

『Objects』 → 『Multi-Tenancy』 → 『Netns Resources』



The service capacity of netns can be limited and the network configuration can be set on the Netns Resources page.



『App Delivery Group』selects a created Group and assigns the current Netns resources to the Group.

『New Conns』 refers to the upper limit of the number of newly created connections per second of all virtual services in the netns, which can not exceed the threshold value of its Group.

『Concurrent Conns』refers to the upper limit of the number of connections maintained by all virtual services in the netns, which can not exceed the threshold value of its Group.

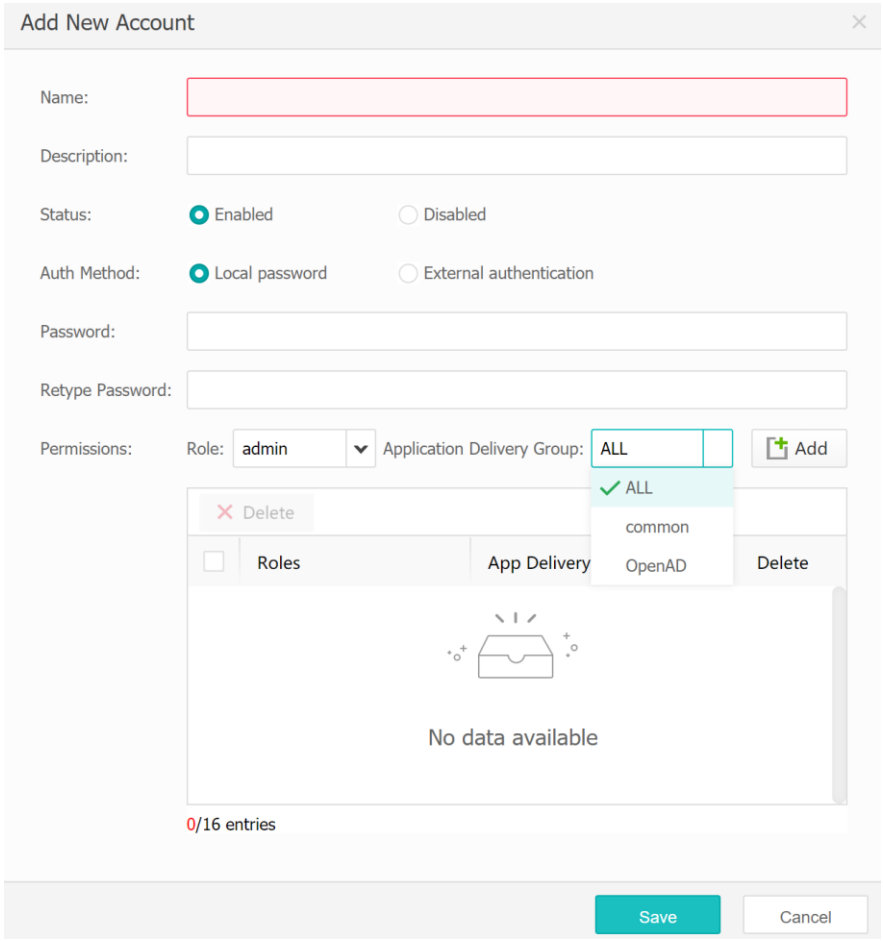
『Max Throughput (Mbps)』 refers to the upper limit of throughput per second that can be achieved by all virtual services in the netns, which can not exceed the threshold value of its Group.

『Network』 configures network(s) for the netns, which shall comply with the network resource range set for its Group.

5. Tenant Configuration

『System』 → 『Administrators』 → 『Administrator』

When creating a new administrator or editing an existing tenant, you can configure a Group associated with the tenant and set permissions for the Group.



Under『Permissions』, in addition to setting restrictions on『Role』, you can set limits on『App Delivery Group』resources and allocate created Group(s) to tenants. One or more Groups can be allocated to one tenant.

Refer to Section 4.2.2 for other basic Administrator configurations.

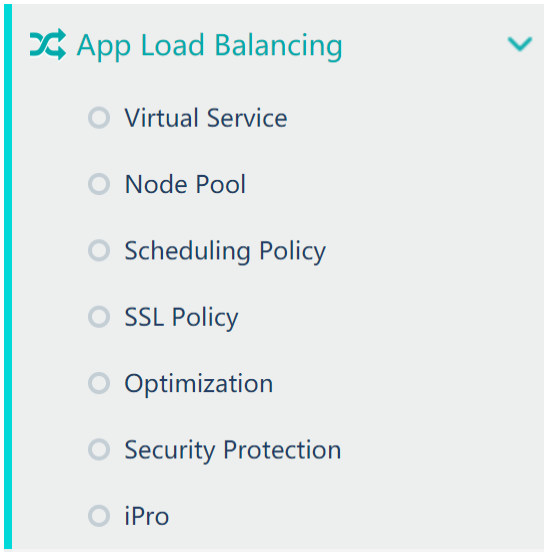
6. Tenant Service Configuration

In a multi-tenancy scenario, all configurations of the associated Groups can be viewed under "Global" after logging into the system via a Tenant account, and the Edit and Delete operations are also supported.

A netns is the smallest unit used for a specific service configuration. Please switch to the netns to be configured from the current view before configuration. Links, virtual services, node pools and IPs sharing the same names could be configured among different netns, because resources and networks are isolated among various netns without any conflicts.

Chapter 7 App Load Balancing

『App Load Balancing』configures load balancing for applications that need to be released to the public, mainly targeting『Virtual Service』. You can configure『Node Pool』,『Scheduling Policy』,『SSL Policy』,『Optimization』,『Security Protection』and『iPro』to flexibly and efficiently implement application release.



App load balancing is divided into Layer 3 load balancing, Layer 4 load balancing and Layer 7 load balancing: Layer 3 load balancing is used for IP-based routing & forwarding, such as policy-based routing configuration. Layer 4 load balancing is used for IP-based and port-based traffic forwarding and TCP optimization, such as forwarding requests from different ports to the corresponding ports of different load balancing servers in a forwarding-only mode. Layer 7 load balancing is used for forwarding based on application policies and for application optimization, such as forwarding traffic to different servers according to different HOST or URI of HTTP applications, and the proxy mode is adopted. All types of load balancing are scheduled after being matched with virtual services.

7.1 Virtual Service

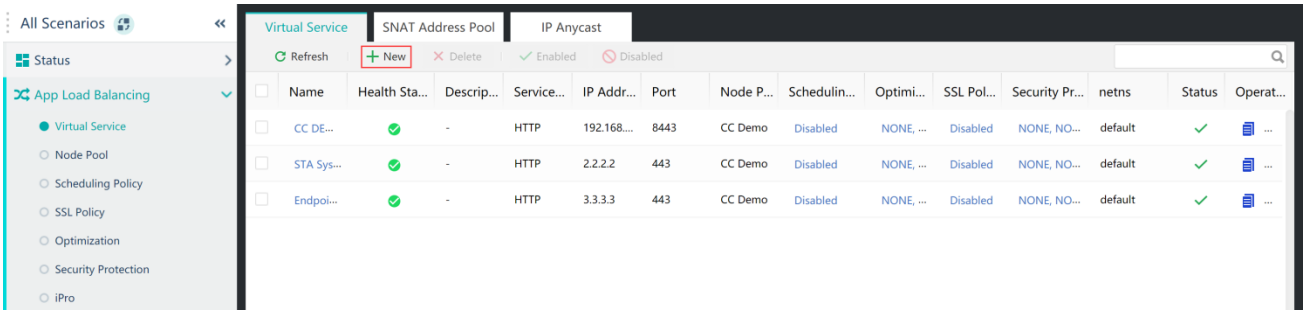
7.1.1 Virtual Service Configuration

【Operation Scenarios】

Virtual Service Configuration is generally used to flexibly configure traffic forwarding, high availability, and safety protection. For example, forward traffic flexibly based on the service data; conduct expansion when one server is not able to bear the large service traffic; guarantee high availability through the health check mechanism; hide the server's real IP or website path; prevent SYN FLOOD attack, HTTP attack, etc.

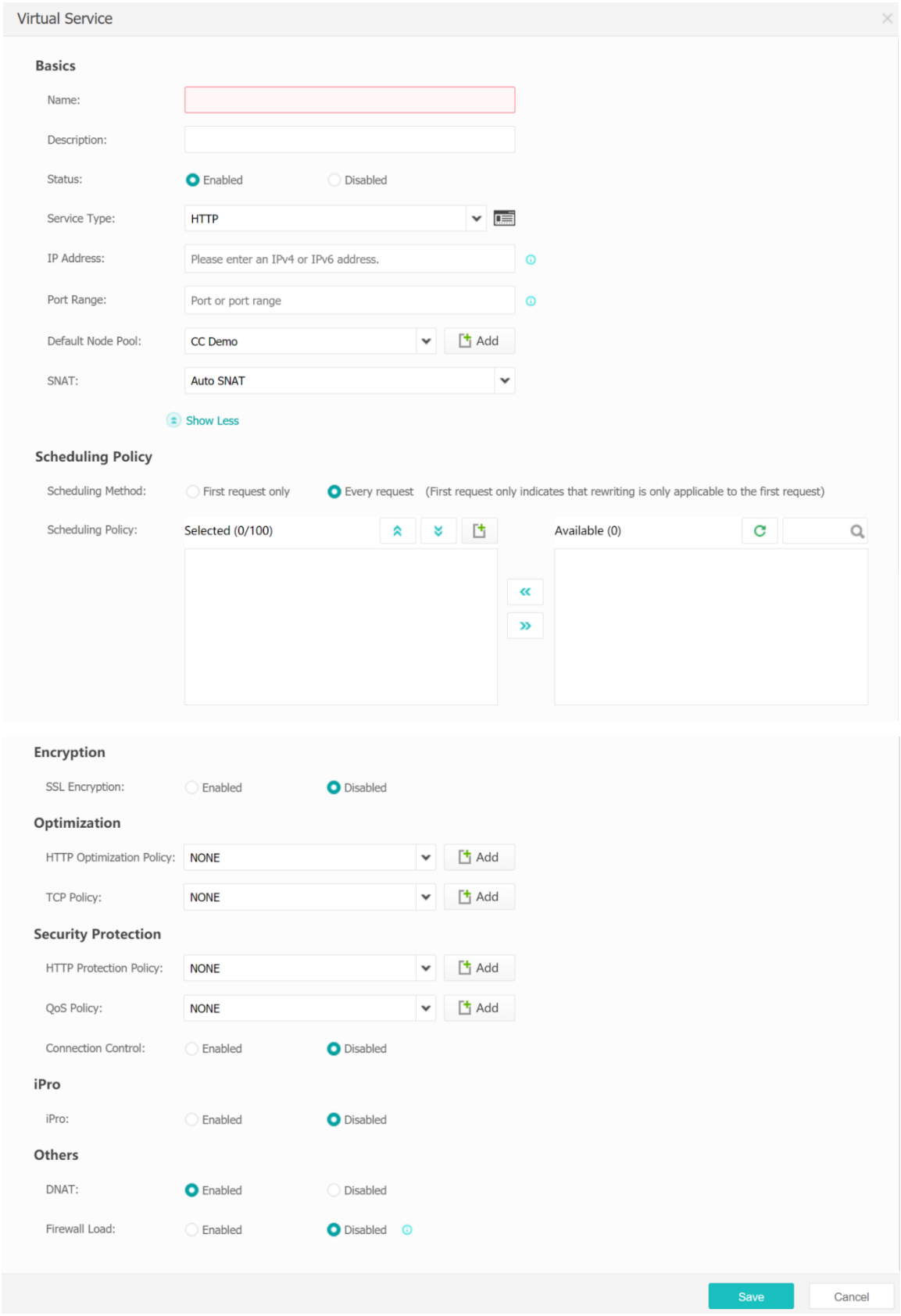
【Operation Procedure】

『App Load Balancing』 → 『Virtual Service』 → 『Virtual Service』. Click Virtual Service on the 『App Load Balancing』 menu, select 『Virtual Service』 in the Virtual Service window shown on the right, and click New.



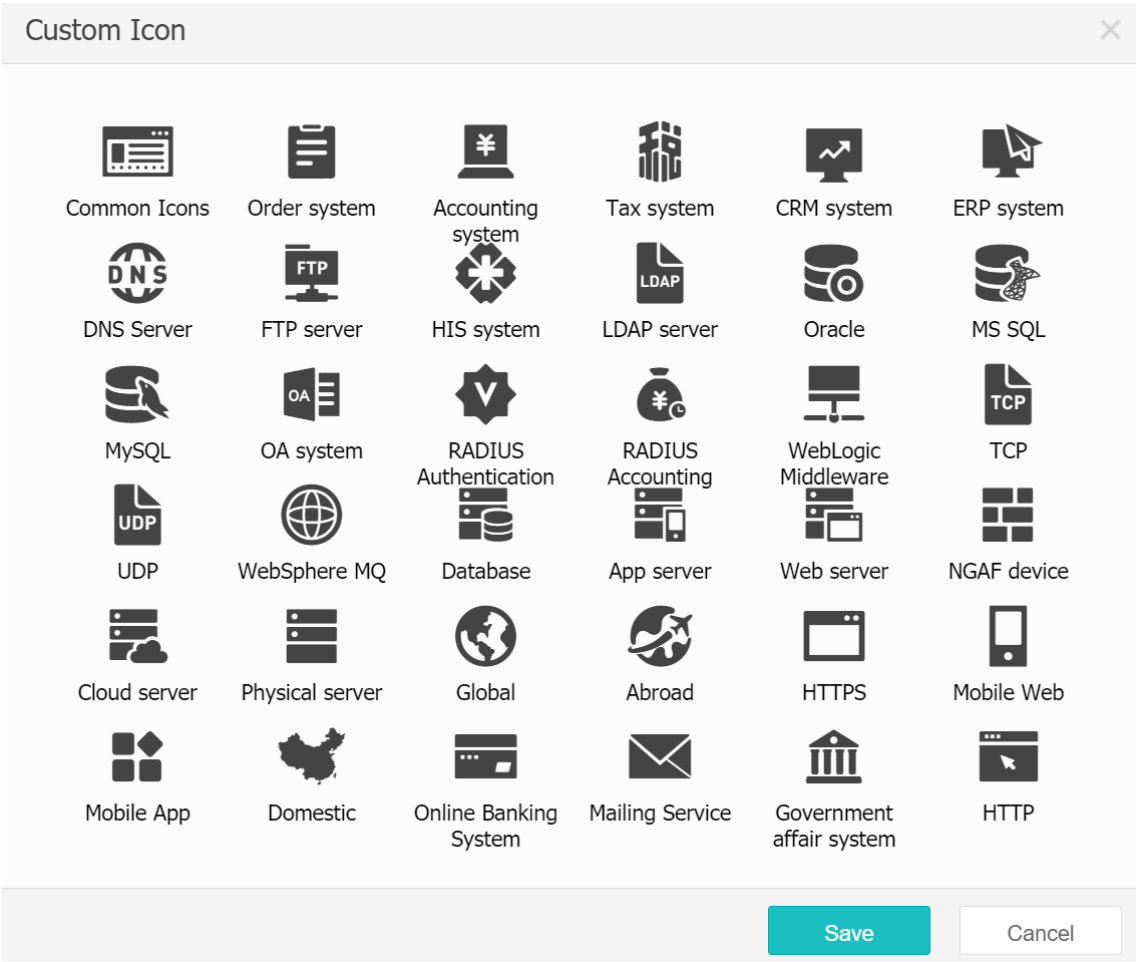
『Virtual Service』displays following information of virtual services:『Name』,『Health Status』, 『Description』, 『Service Type』, 『IP Address』, 『Port』, 『Node Pool』, 『Scheduling Policy』, 『Optimization』, 『SSL Policy』, 『Security Protection』, 『Status』, 『Operation』. 『Operation』 provides a Copy button to quickly create an entry with the same virtual service configuration by copying, and a Delete button to delete a single entry.

Click the New button to open a window as shown in the figure below. General settings include Name, Service Type, IP Address, Port Range, Default Node Pool, SNAT, SSL Offloading (required only when HTTPS is selected for Service Type).


Virtual Service
Basics
Name:
Description:
Status:
Enabled
Disabled
Service Type:
HTTP
IP Address:
Please enter an IPv4 or IPv6 address.
Port Range:
Port or port range
Default Node Pool:
CC Demo
Add
SNAT:
Auto SNAT
Show Less
Scheduling Policy
Scheduling Method:
First request only
Every request
(First request only indicates that rewriting is only applicable to the first request)
Scheduling Policy:
Selected (0/100)
Available (0)
Encryption
SSL Encryption:
Enabled
Disabled
Optimization
HTTP Optimization Policy:
NONE
Add
TCP Policy:
NONE
Add
Security Protection
HTTP Protection Policy:
NONE
Add
QoS Policy:
NONE
Add
Connection Control:
Enabled
Disabled
iPro
iPro:
Enabled
Disabled
Others
DNAT:
Enabled
Disabled
Firewall Load:
Enabled
Disabled
Save
Cancel

『Status』enables or disables virtual services. When a certain service has been taken offline or canceled, it can be disabled firstly until further confirmation of deletion, or it can be pre-configured as disabled, and be enabled when cutover is allowed, such as scenario replacement, etc.

『Service Type』refers to the load balancing type configured for a virtual service and provides various options, including L3, TCP, UDP, L7-TCP, L7-UDP, RADIUS, DNS, FTP, HTTP, SIP-TCP, SIP-UDP, SSL, and HTTPS. You can mark a virtual service more easily by clicking the icon button following the field. Supported icon types are as follows:



『IP Address』refers to IP addresses of virtual services, which are used to match the destination IP addresses of traffic through ADC, supporting configuration of a single IPv4/IPv6 IP address or sub-network per row.

『Port Range』 is not supported for L3 virtual services. The ports published by virtual services are used to match traffic for the corresponding ports, supporting the configuration of a single port or a port range per row.

『Default Node Pool』 is used to match the destination IP address for traffic forwarding of virtual services, generally including the IP addresses of servers on internal and external networks or IP addresses of gateways on the same network segment with interfaces.

『SNAT』 is used to change the source IP address to a specified IP address when forwarding traffic matching a virtual service to a node pool. It is often used in a bypass deployment to guarantee the sever backhaul can be returned to ADC, ensuring consistent sessions.

『SSL Offloading』 is only supported for SSL and HTTPS virtual services, which is used to conduct SSL decryption in regard to the traffic of SSL-related services, such as HTTPS, LDAPS, POP_SSL, SMTP_SSL, IMAP_SSL, SSL_VPN, etc.

For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『Scheduling Method』 is only supported for HTTP and HTTPS virtual services, which is used to select the scheduling method based on the first request or every request in regard to HTTP traffic. The difference lies in the matching method of HTTP rewriting. If "First request only" is selected, indicating that rewriting is only applicable to the first request, no subsequent requests (even being the same with the first one) will be matched to the rewriting policy. If "Every request" is selected, every request will be scheduled to match the rewriting policy.

『Scheduling Policy』 is used to conduct traffic matching and processing again before the traffic of virtual services being forwarded to the node pool. The twice matching can schedule the traffic more flexibly. For example, traffic from different source IP addresses for accessing a virtual service is forwarded to different node pools.

『SSL Encryption』 is only supported for TCP-L7, HTTP, SSL, and HTTPS virtual services, which is used to conduct SSL encryption on plaintext traffic through ADC so as to access the server side.

『HTTP Optimization Policy』 is supported for HTTP and HTTPS only, which is used to optimize HTTP protocol transmission, support HTTP caching, HTTP compression, and IP transparent transmission at the client side.

『TCP Policy』 is only supported for TCP, TCP-L7, HTTP, SSL, and HTTPS. The L4 TCP optimization or L7 TCP optimization policy is available to match with the virtual service types (TCP can only use L4 TCP optimization, and others can only use L7 TCP optimization). The L4 TCP optimization can modify the time-out period of virtual services, and the L7 TCP optimization supports TCP connection multiplexing, etc.

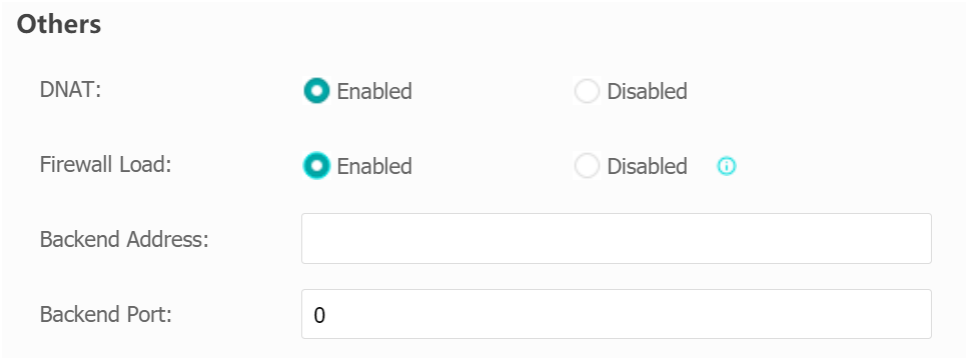
『HTTP Protection Policy』 is only supported for HTTP and HTTPS, which is used for DDoS attack protection for HTTP traffic, and supports HTTP slow attack protection and flood attack protection.

『QoS Policy』 is used to match the traffic of virtual services for traffic control so as to guarantee the bandwidth.

『Connection Control』 is used to match the traffic of virtual services so as to guarantee the service performance within the upper limit and avoid server overload.

『iPro』 can edit traffic control script, which is used to control traffic forwarding flexibly via programming languages based on LUA language.

『DNAT』 matches the traffic of virtual services for further DNAT, which allows the network device to forward the traffic to the corresponding server, and the server will receive traffic based on the destination IP. In general, it should be enabled for non-L3 load balancing, such as mapping the external network IP to the IP of a server on the internal network for forwarding.



『Firewall Load』 is available after enabling DNAT, of which 『Backend Address/Port』 is the virtual service IP address/port of the ADC serving as a backend for loading service.

『TCP Buffered Stream』 is only supported for TCP-L7 and SSL, which is used to intercept contents of TCP data stream for scheduling. If no scheduling policy is configured, the configuration here is meaningless.

『Automatic Jump HTTPS』 is only supported for HTTPS, which is used to redirect HTTP to HTTPS virtual service. The specified HTTP port occupied by the HTTP jump can not be used to configure the virtual service.

Attention: Different types of virtual services will have different functional configuration items. For example, for SSL and HTTPs, SSL policy can be configured; for HTTP and HTTPS, HTTP protection can be enabled. The above-mentioned configuration items can be created by clicking the “New” button when creating a new virtual service, or can also be configured under the corresponding modules by clicking the navigation menu bar on the left.

7.1.2 Health Monitor

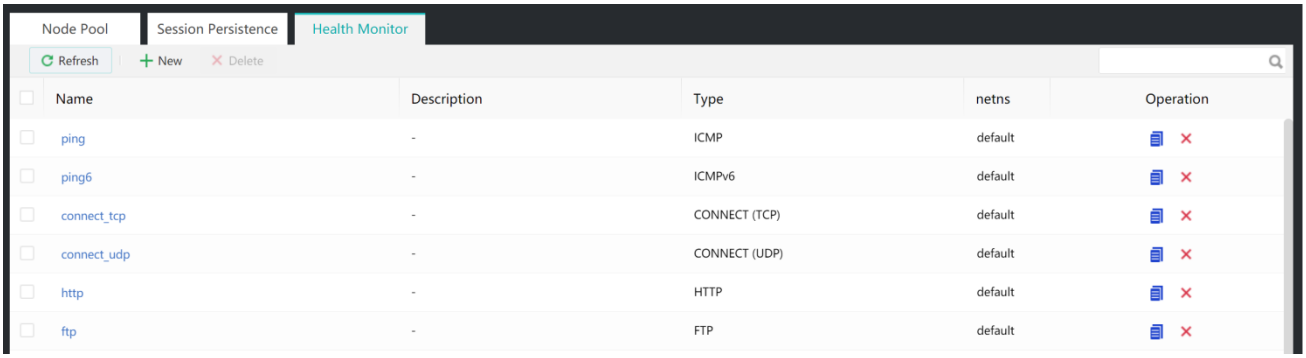
【Operation Scenarios】

In order to ensure the high availability of services published and automatic switchover to other normal nodes in case of load node failures, the ADC should be enabled to check the health status of nodes in real time by configuring 『Health Monitor』.

【Operation Procedure】

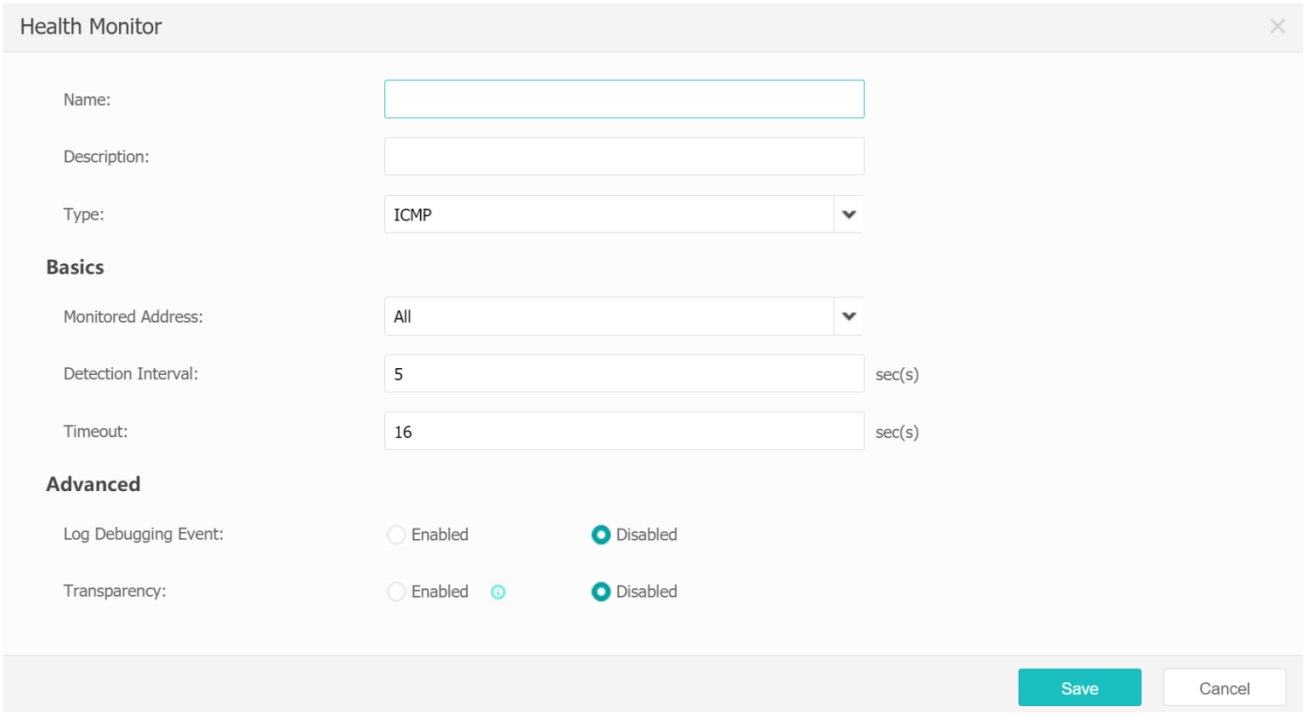
『App Load Balancing』 → 『None Pool』 → 『Health Monitor』. On the 『App Load Balancing』 menu, click Node Pool, select 『Health Monitor』 in the Node Pool window on the right, and click New

The page is shown in the figure below:

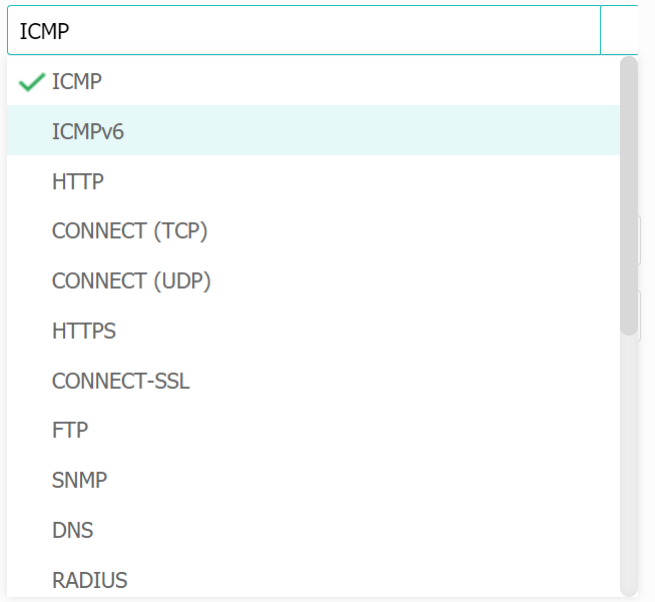


『Name』, 『Description』, 『Type』, and 『Operation』 are displayed under 『Health Monitor』, and a Copy button is under the 『Operation』 column to quickly copy and create the same health check. The Delete button is used to delete a single entry. The 『Health Monitor』 defined here can be used for the configuration of 『Node Pool』 and 『Node』.

Click the New button, as shown in the following figure:



『Type』 drop-down list shows the available service health check types, including [ICMP], [ICMPv6], [CONNECT(TCP)],[CONNECT(UDP)], [HTTP], [HTTPS], [CONNECT-SSL], [FTP], [SNMP], [DNS], [RADIUS], [TCP Half Open], [TCP Passive], [HTTP Passive], [Complex Monitor], [External App Monitor], [ORACLE], [MS SQL], [MYSQL], and [LDAP].



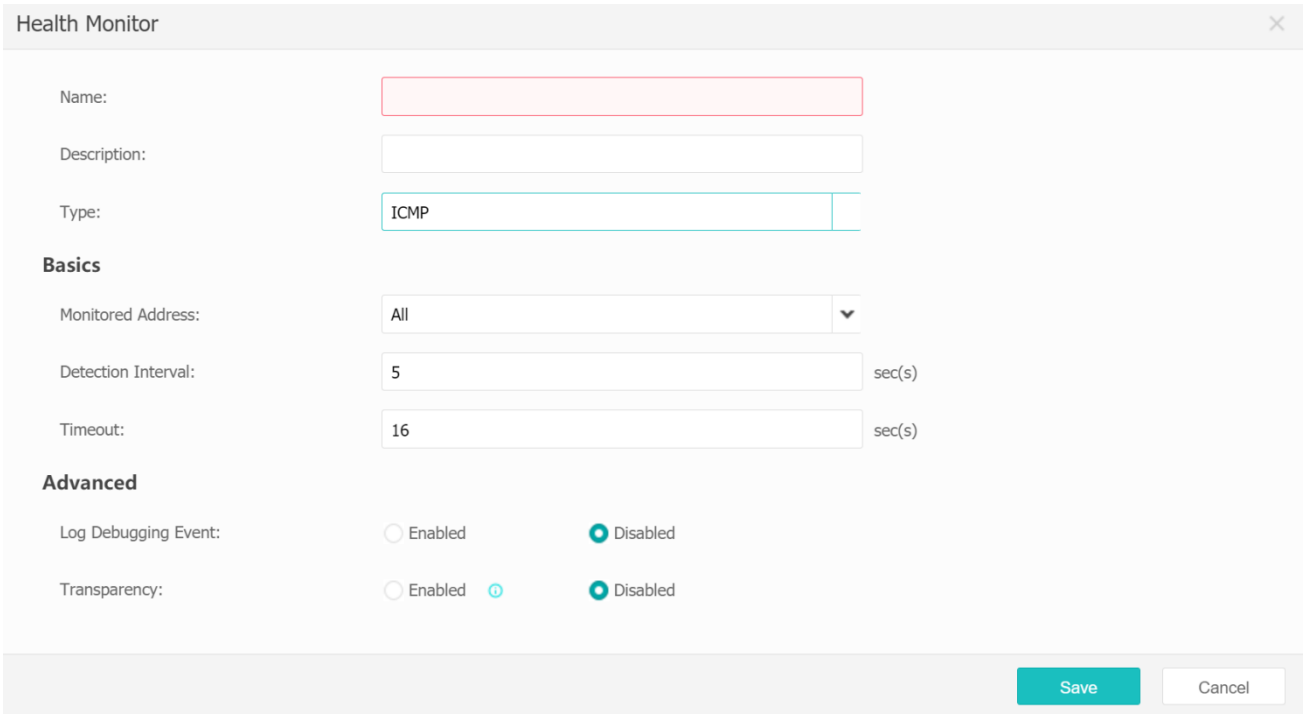
7.1.2.1 ICMP

【Operation Scenarios】

When it is necessary to check whether the IP address of the IPv4 node is accessible, you can configure [ICMP] health check.

[Configuration Instruction]

Select『ICMP』for『Type』and the device will send an ICMP request package in IPv4 address format to detect the node. Determine the health status of the node according to whether the node responds to the ICMP request. The configuration is shown in the following figure: Generally, only Name needs to be set;



For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『Monitored Address』configures the IP address of detection, and all IP addresses are detected by default. It inherits the IP address of the node in the node pool; if a fixed IP address is written, it means that the monitor will only check whether the filled IP address is normal, regardless of which node is associated. Generally, the default value is kept;

『Detection Interval』configures the interval time for the health check, that is, the duration between the previous health check and the current health check (unit: seconds);

『Timeout』configures the timeout for the health check. If no response from the node is received after the configured time, it is considered as timeout (unit: seconds);

『Log Debugging Event』configures whether to enable the debugging log of the health check. After enabling, detailed connection records will be displayed in the log. Generally, the default value is kept. It is required only for troubleshooting;

『Transparency』configures the remote target address of detection. After enabling, the 『Monitored Address』must be configured as the IP for detection. At this point, the node IP in the

node pool will be used as the next gateway IP for detection, which is often used for outbound link load detection of the external network IP.

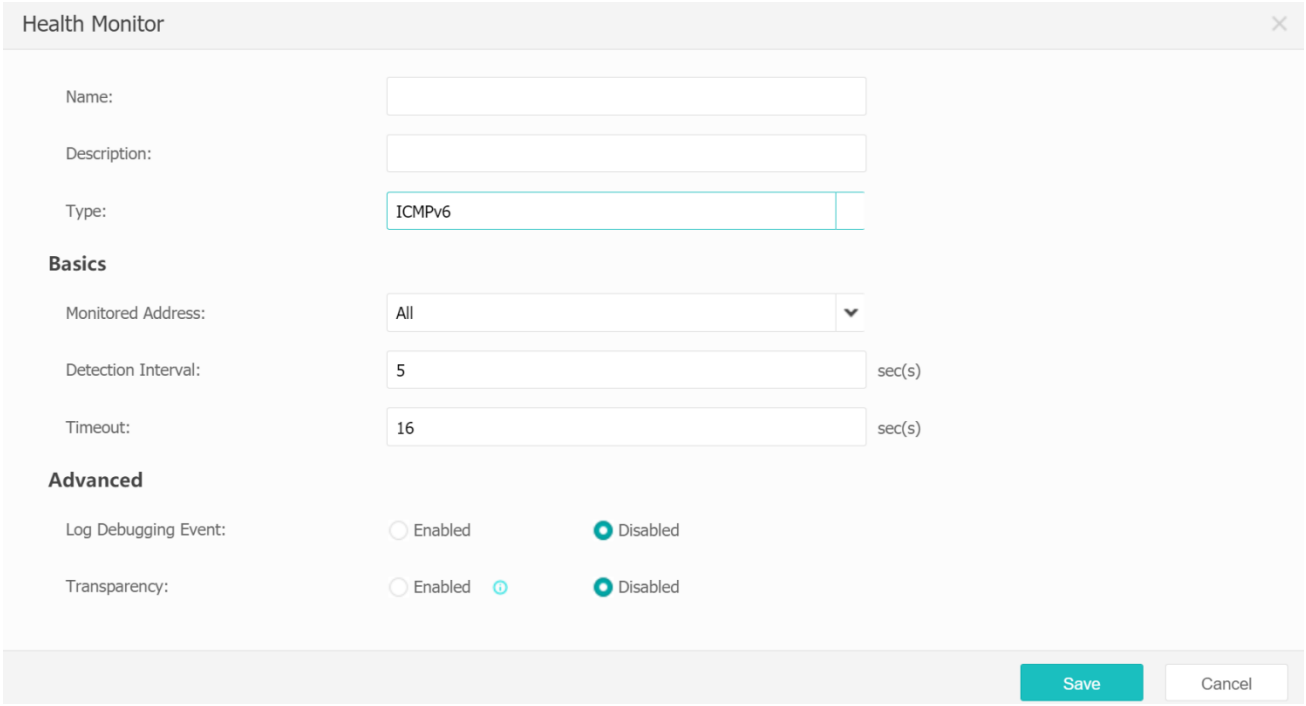
7.1.2.2 ICMPv6

【Operation Scenarios】

When it is necessary to check whether the IP address of the IPv6 node is accessible, you can configure [ICMPv6] health check.

[Configuration Instruction]

Select『ICMPv6』for『Type』and the device will send an ICMPv6 request package in the IPv6 address format to detect the node. Determine the health status of the node according to whether the node responds to the ICMPv6 request. The configuration is shown in the following figure:



For details about the configuration and instruction, see the 『ICMP』health check section.

Attention: The configured IP address of『Monitored Address』in ICMPv6 must be the standard address of IPv6.

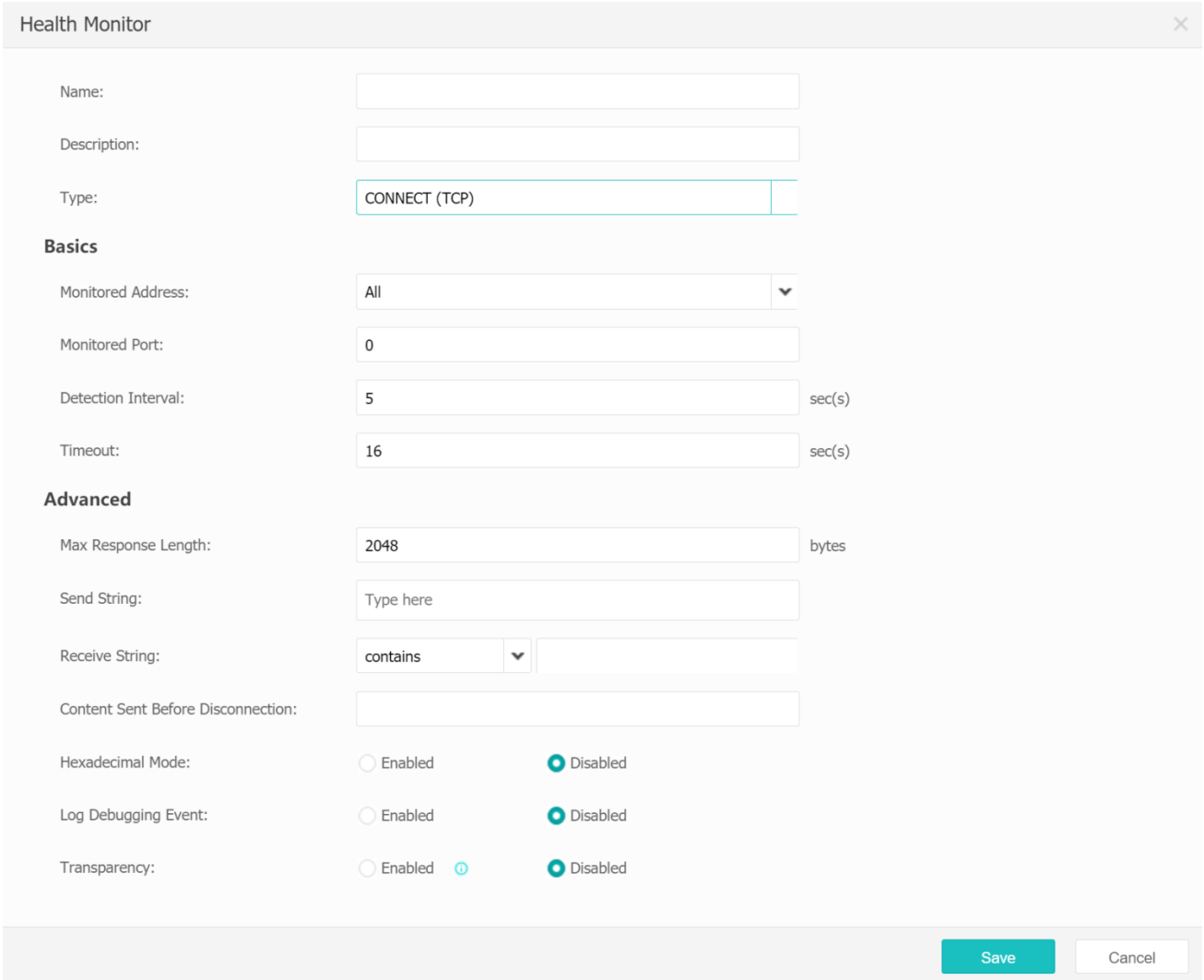
7.1.2.3 CONNECT(TCP)

【Operation Scenarios】

When the IP access cannot correctly reflect the health status of the node or the node prohibits ICMP response, you can confirm the health status of the node by checking the active status of the application port. If TCP protocol is used, the [CONNECT (TCP)] health check can be configured.

[Configuration Instruction]

Select『CONNECT(TCP)』for『Type』and the device will send a TCP connection request to detect the node. Determine the health status of the node according to whether the node responds to the TCP request with "SYN+ACK" or whether it responds to the TCP request with specified contents. The configuration is shown in the following figure: Generally, only Name needs to be set;



For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『Monitored Address』configures the IP address of detection, and all IP addresses are detected by default. It inherits the IP addresses of the nodes in the node pool;

『Monitored Port』 configures the TCP port of detection, which is port 0 by default and inherits the node port; if the node port is 0, this port must not be the 0 port (it should be the detected port);

『Detection Interval』 configures the interval time for the health check, that is, the duration between the previous health check and the current health check (unit: seconds);

『Timeout』 configures the timeout for the health check. If no response from the node is received after the configured time, it is considered as timeout (unit: seconds);

『Max Response Length』 configures the maximum length of the node response data content (unit: byte), and it is 2048 (1-4096) bytes by default;

『Send String』configures the Payload data sent after the connection is established for a health check;

『Receive String』configures the contents that the received packet must contain or not contain, and the health status of the node shall be judged accordingly;

『Content Sent Before Disconnection』 configures the data sent before the health check stops;

『Hexadecimal Mode』 configures whether the hexadecimal mode is enabled for the data content sent and received by the health monitor;

『Log Debugging Event』 configures whether to enable the debugging log of the health check. After enabling, detailed connection records will be displayed in the log;

『Transparency』 configures the remote target address of detection. After enabling, the 『Monitored Address』 must be configured as the IP for detection. At this point, the node IP in the node pool will be used as the next gateway IP for detection, which is often used for outbound link load detection of the external network IP.

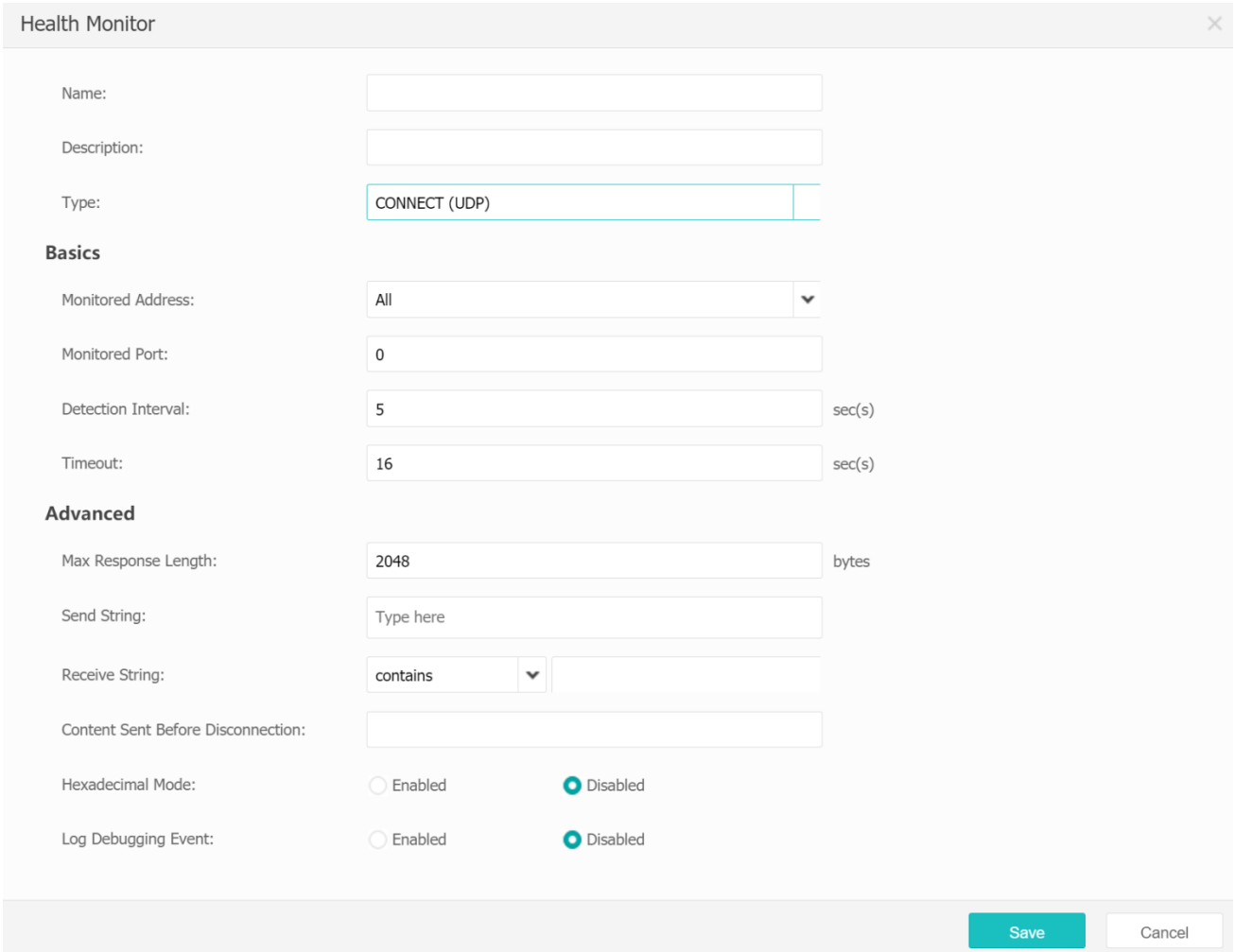
7.1.2.4 CONNECT(UDP)

【Operation Scenarios】

When the IP access cannot correctly reflect the health status of the node or the node prohibits ICMP response, you can confirm the health status of the node by checking the active status of the application port. If UDP protocol is used, the [CONNECT(UDP)] health check can be configured.

[Configuration Instruction]

Select『CONNECT(UDP)』for『Type』and the device will send a UDP request to detect the node. Determine the health status of the node according to whether the node responds to the UDP request, whether it normally responds to the UDP request with ICMP error information "port XX unreachable", or whether it responds to the UDP request with specified contents. If there is no response or normal response, which is "port XX unreachable", it indicates that ICMP is offline. The configuration is shown in the following figure:



For details about the configuration and instruction, see the『CONNECT(TCP)』health check section.

Attention: The data of『Monitored Port』and the health check package for『CONNECT(UDP)』is sent in the form of UDP. Due to the connectionless nature of UDP, it is recommended to configure content check to better understand the health status of the UDP port.

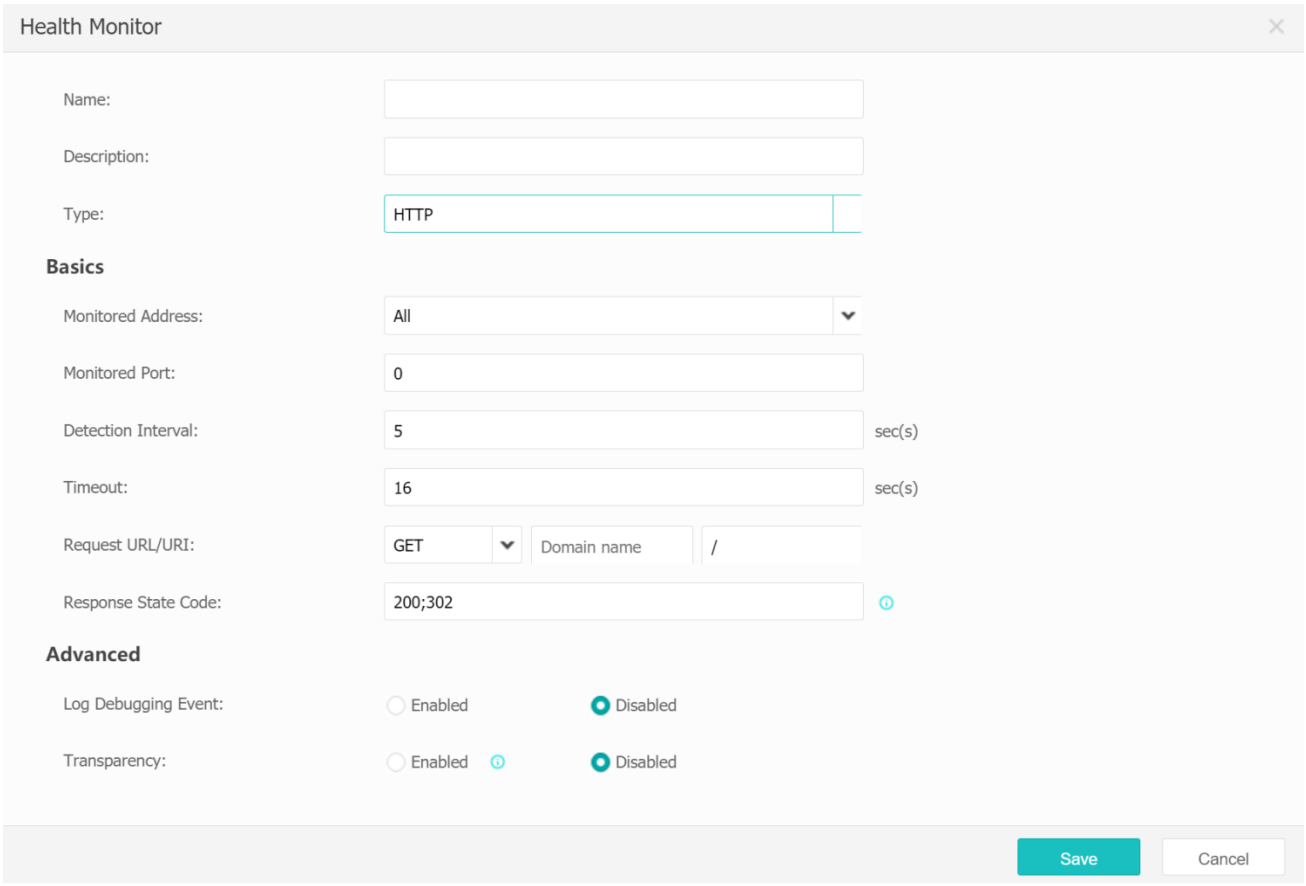
7.1.2.5 HTTP

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as HTTP application server returning the 503 error, you can determine the health status of the node by configuring [HTTP] health check. For this reason, the service must use the HTTP protocol.

[Configuration Instruction]

Select『HTTP』for『Type』and the device will send an HTTP request package to detect the node. Determine the health status of the node according to whether the node responds to the HTTP request with configured state code. The configuration is shown in the following figure: Generally, Name, Request URL/URI, Response State Code need to be set while other parameters can be kept with the default values;



『Request URL/URI』 configures the URL of detection, which is the root directory of the node by default. There are three filling formats, which can automatically identify the host and URI. The following three formats are supported:

1.http://www.abc.com

2.www.abc.com

3./a/b

『Response State Code』 configures the response state code of the HTTP server. If the default server responds 200 or 302, it indicates that the server is normal. You can add 301, 307, 401, and other codes as needed to indicate that the server is normal.

For other details about the configuration and instruction, see the 『CONNECT(TCP)』 health check section.

Attention: Generally, if a node can use an HTTP monitor, it can also use a CONNECT(TCP) monitor, which is a special form of the CONNECT (TCP) monitor.

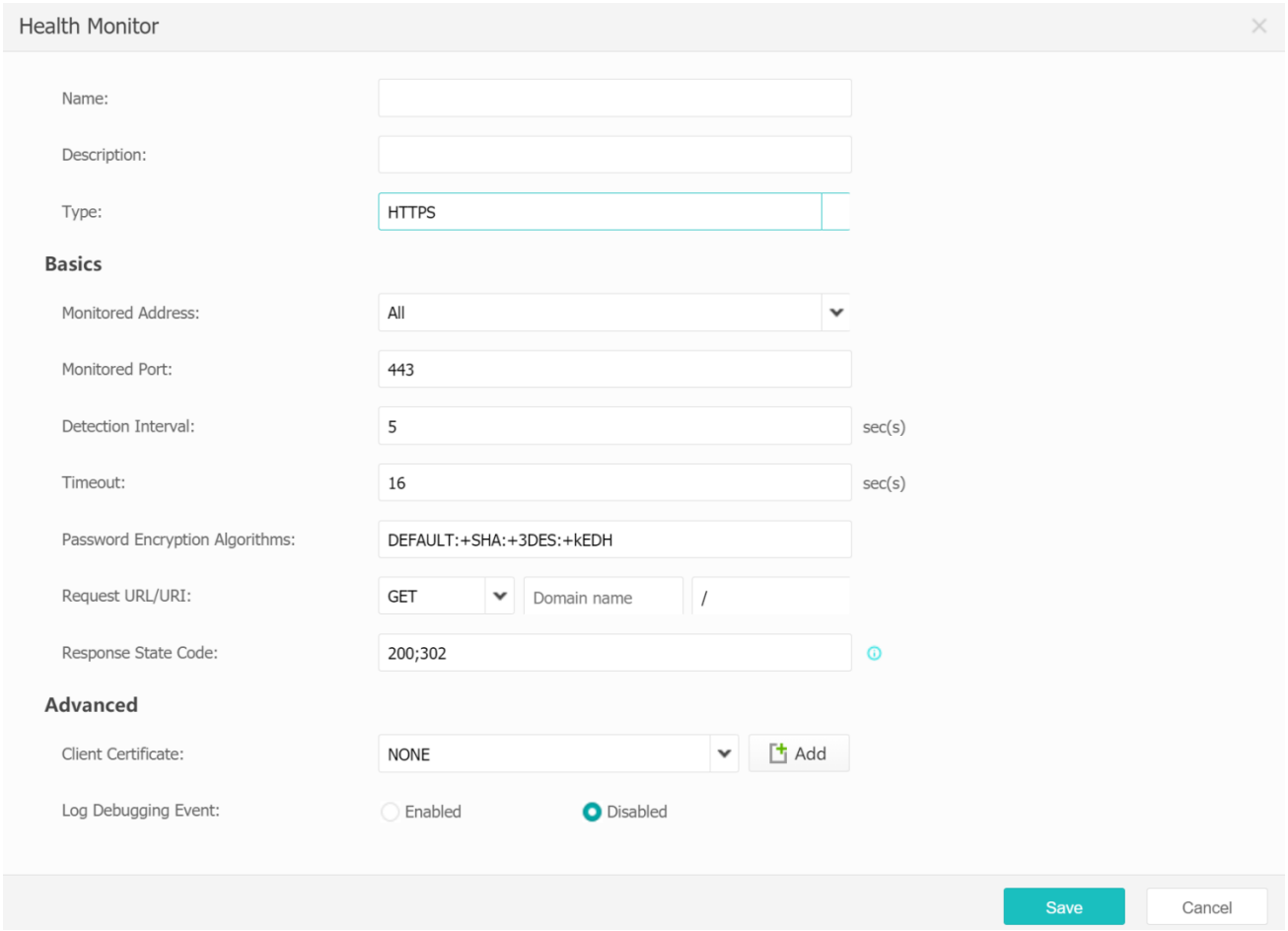
7.1.2.6 HTTPS

【Operation Scenarios】

When an application uses SSL encryption for HTTPS, the common [HTTP] health check will also be invalid. You can check the health status of the node by configuring [HTTPS] health check and using HTTPS traffic.

[Configuration Instruction]

Select『HTTPS』for『Type』and add SSL authentication on the basis of 『HTTPS』health check. The device will send an HTTPS request package to detect the node. Determine the health status of the node according to whether the node responds to the HTTP request with configured response state code. The configuration is shown in the following figure:



『Password Encryption Algorithms』configures the encryption and authentication algorithms used when establishing an HTTPS connection.

『Client Certificate』configures whether the client certificate is submitted for authentication when HTTPS detection is performed. It is used for authenticating an SSL server with two certificates. For details of certificate configuration, see the instruction in『Objects』→『Certificates』.

For other details about the configuration and instruction, see the『HTTP』health check section.

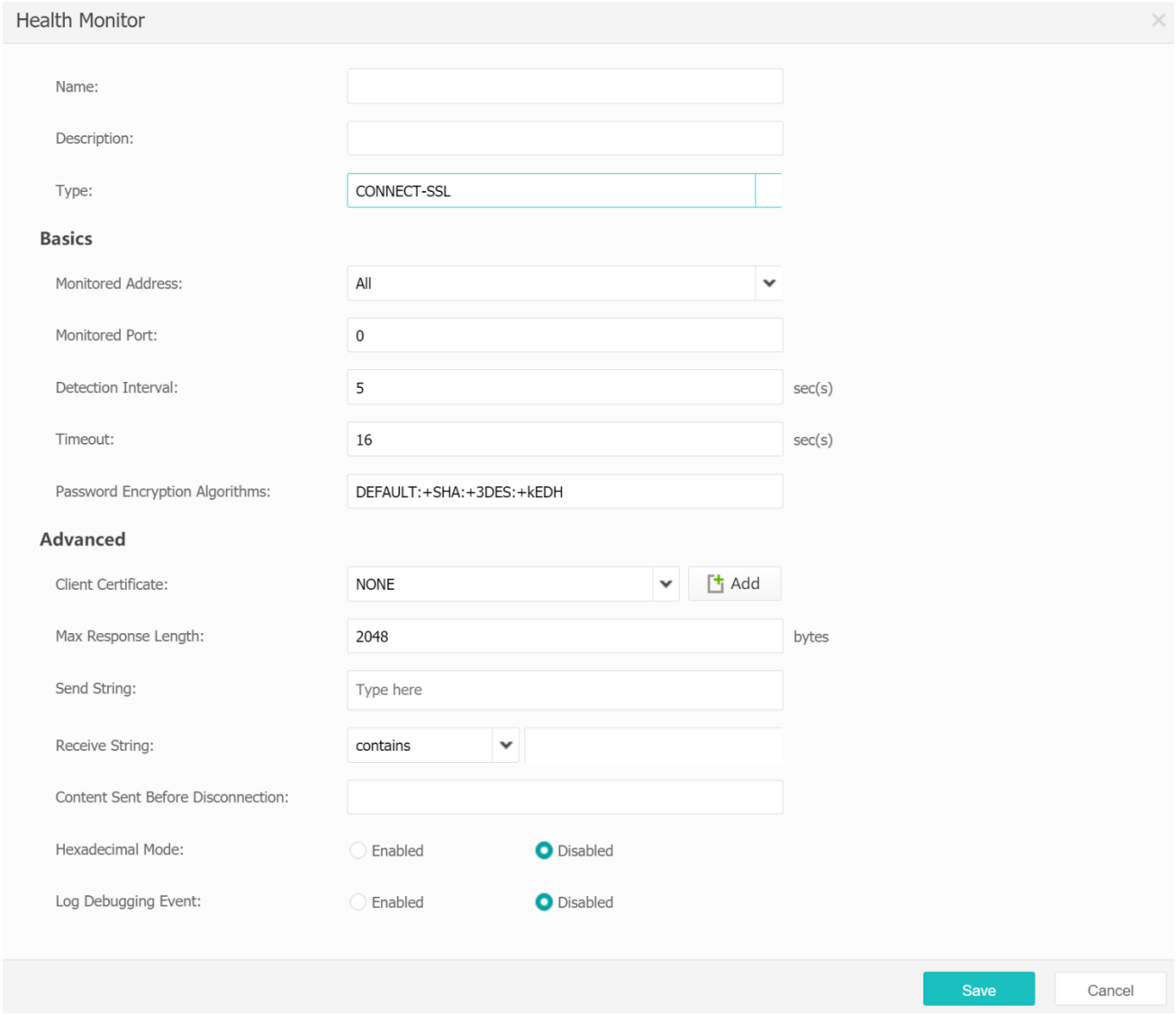
7.1.2.7 CONNECT-SSL

【Operation Scenarios】

For HTTPS applications encrypted by SSL based on the HTTP protocol, you can determine the health status of the node by configuring [HTTPS] health check. However, many other applications use SSL encryption, and they cannot use HTTPS health check. Hence, you can configure [CONNECT-SSL] health check and use the TCP traffic encrypted by SSL to check the health status of the node.

[Configuration Instruction]

Select『CONNECT-SSL』for『Type』and add SSL authentication on the basis of『CONNECT(TCP)』health check. The device will send an SSL connection request package to detect the node. Determine the health status of the node according to whether the node creates a normal SSL handshake, or whether it responds to the TCP request with specified contents after the SSL connection is established. The configuration is shown in the following figure:



『Password Encryption Algorithms』configures the encryption and authentication algorithms used when establishing an SSL connection.

『Client Certificate』configures whether the client certificate is submitted for authentication when SSL detection is performed. It is used for authenticating an SSL server with two certificates. For details of certificate configuration, see the instruction in『Objects』→ 『Certificates』.

For other details about the configuration and instruction, see the『CONNECT(TCP)』health check section.

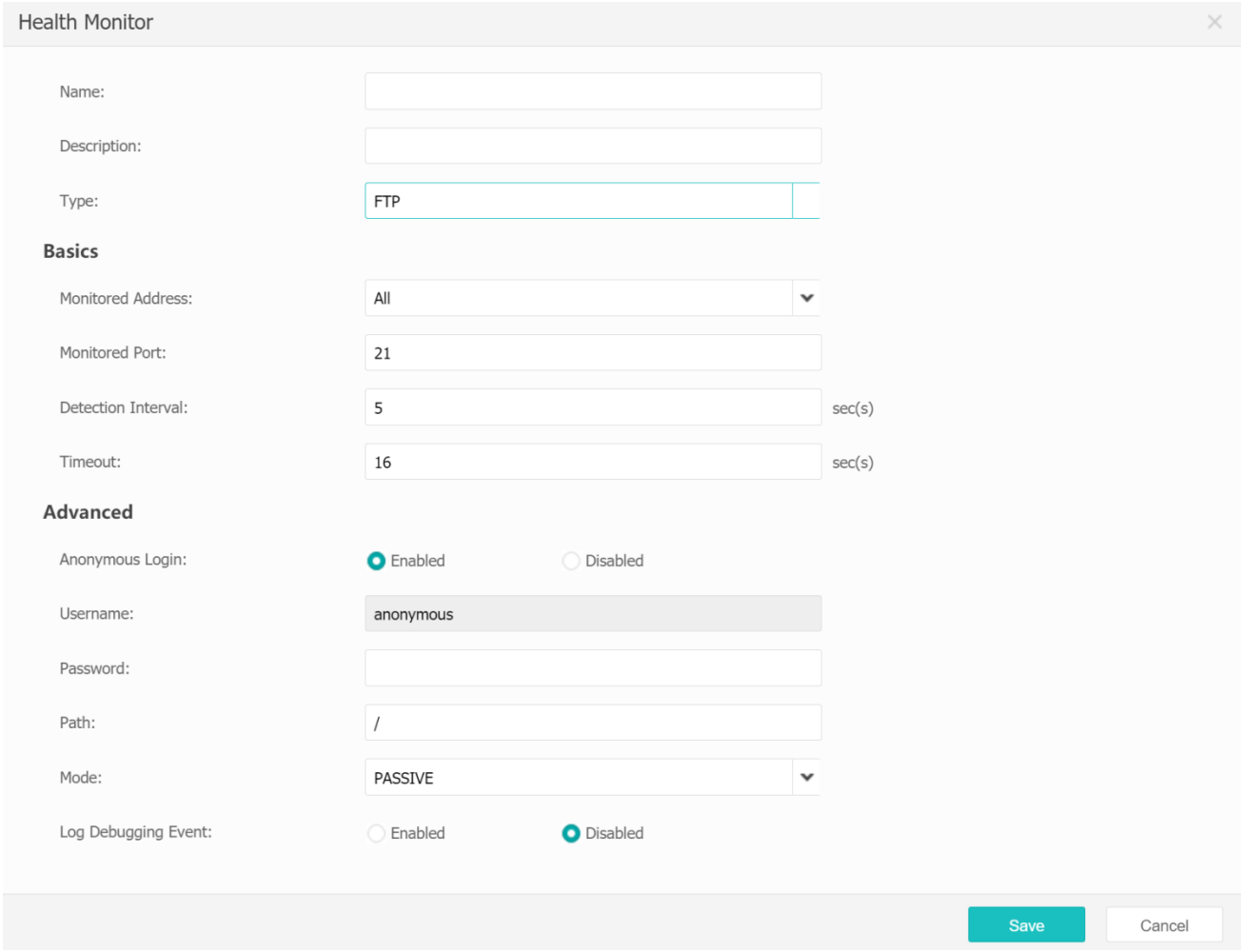
7.1.2.8 FTP

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as the case where the FTP server port can be connected but cannot be accessed, you can configure [FTP] health check to determine the health status of the node.

[Configuration Instruction]

Select『FTP』for『Type』and the device will send an FTP connection request to detect the node. Determine the health status of the node according to whether the node responds to the FTP query request as per the configured path. The configuration is shown in the following figure:



『Anonymous Login』 configures whether to enable FTP anonymous login. By default, it is enabled and uses the anonymous username "anonymous" for login. After enabling, the username cannot be modified.

『Username』 configures the username for logging in to the FTP server.

『Password』 configures the password for logging in to the FTP server.

『Path』 configures the file path for the FTP server of detection, and the root directory is queried by default.

『Mode』 configures the working mode of the FTP server, including PASSIVE and PORT modes.

For other details about the configuration and instruction, see the 『CONNECT(TCP)』 health check section.

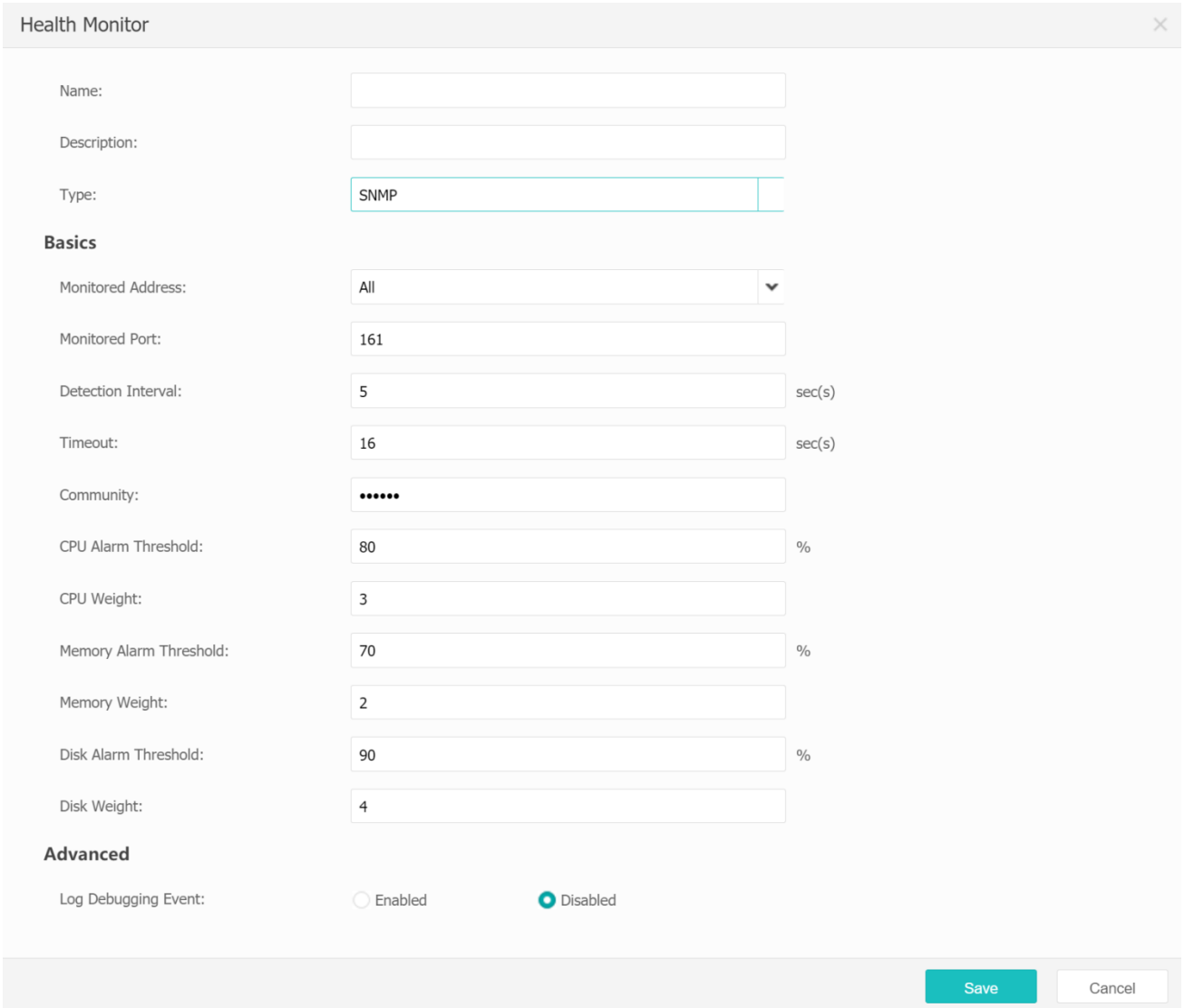
7.1.2.9 SNMP

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, for example, the fast running speed of the CPU or the high occupancy rate of memory leads to the slow response, you can configure the [SNMP] health check to determine the health status of the node, and the weight of the node can be dynamically adjusted through the health check to make the node load more balanced (the node pool selection strategy needs to be configured as a dynamic feedback strategy).

[Configuration Instruction]

Select 『SNMP』 for 『Type』 and the device will send an SNMP query request to detect the node. Determine the health status and adjust the weight of the node according to whether the node responds to the SNMP request, or it responds to the SNMP request with a value over the configured threshold. The configuration is shown in the following figure:



『Community』configures the query password (group name) of detection, which is "public" by default and can be modified according to the actual situation.

『CPU Alarm Threshold』configures the alarm threshold of the monitored CPU. If this value is exceeded, it indicates that the node is busy.

『CPU Weight』 configures the monitored CPU weight, which is used for node selection strategy for dynamic feedback. See the "Node Pool" section for details.

『Memory Alarm Threshold』configures the alarm threshold of the monitored memory. If this value is exceeded, it indicates that the node is busy.

『Memory Weight』 configures the monitored memory weight, which is used for node selection strategy for dynamic feedback. See the "Node Pool" section for details.

『Disk Alarm Threshold』 configures the alarm threshold of the monitored disk. If this value is exceeded, it indicates that the node is busy.

『Disk Weight』 configures the monitored SNMP disk weight, which is used for node selection strategy for dynamic feedback. See the "Node Pool" section for details.

For other details about the configuration and instruction, see the 『CONNECT(TCP)』 health check section.

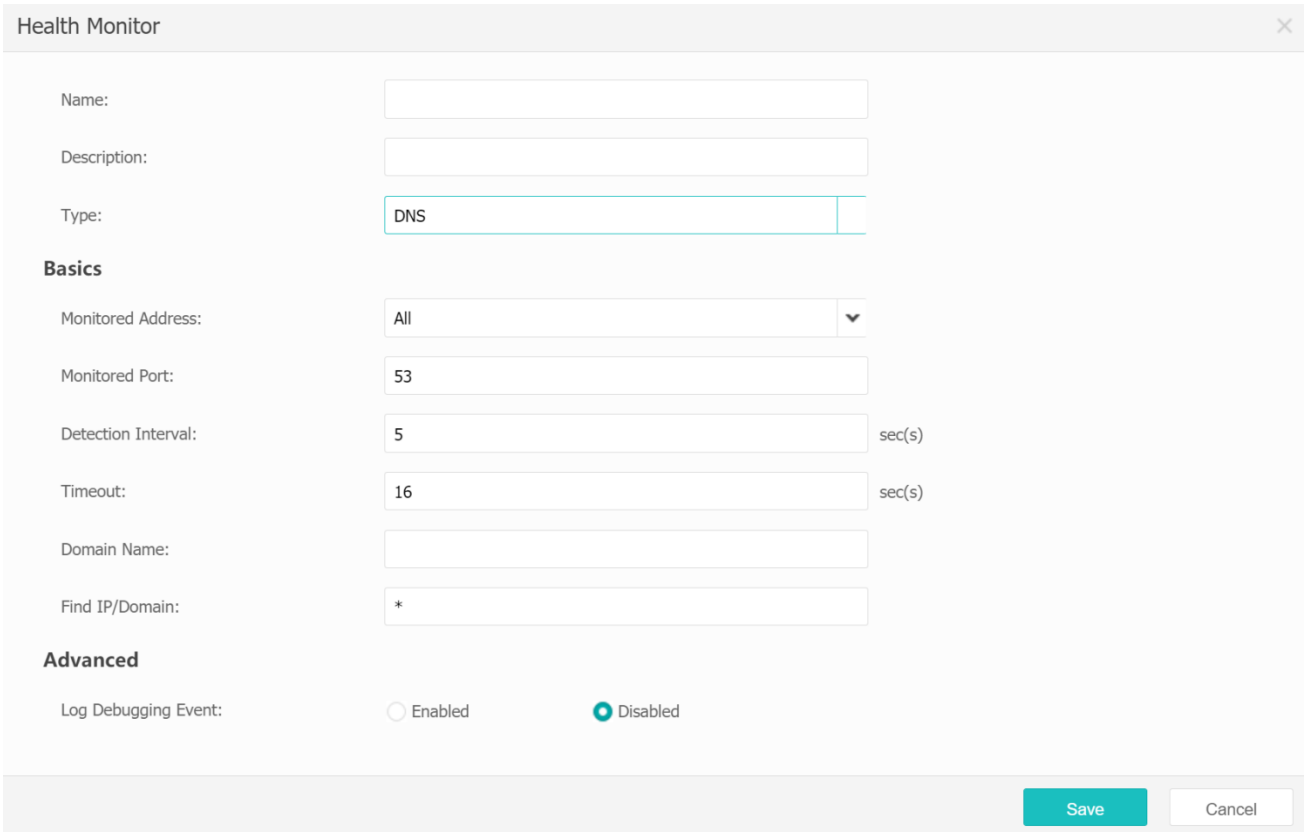
7.1.2.10 DNS

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as the case where the DNS server port can be connected but cannot resolve the domain name, you can configure [DNS] health check to determine the health status of the node.

[Configuration Instruction]

Select 『DNS』 for 『Type』 and the device will send a DNS query request to detect the node. Determine the health status of the node according to whether the node normally responds to the domain name query request, or it responds to the DNS query request with configured Find IP/Domain. The configuration is shown in the following figure:



『Domain Name』 configures the query domain name sent to the node.

『Find IP/Domain』 configures node response information. If you fill in an IPv4 address, the health monitor sends A for query; if you fill in an IPv6 address, it sends AAAA for query; if you fill in a domain name, it sends CNAME for query; if you do not change the default *, it sends ANY for query.

For other details about the configuration and instruction, see the 『CONNECT(TCP)』 health check section.

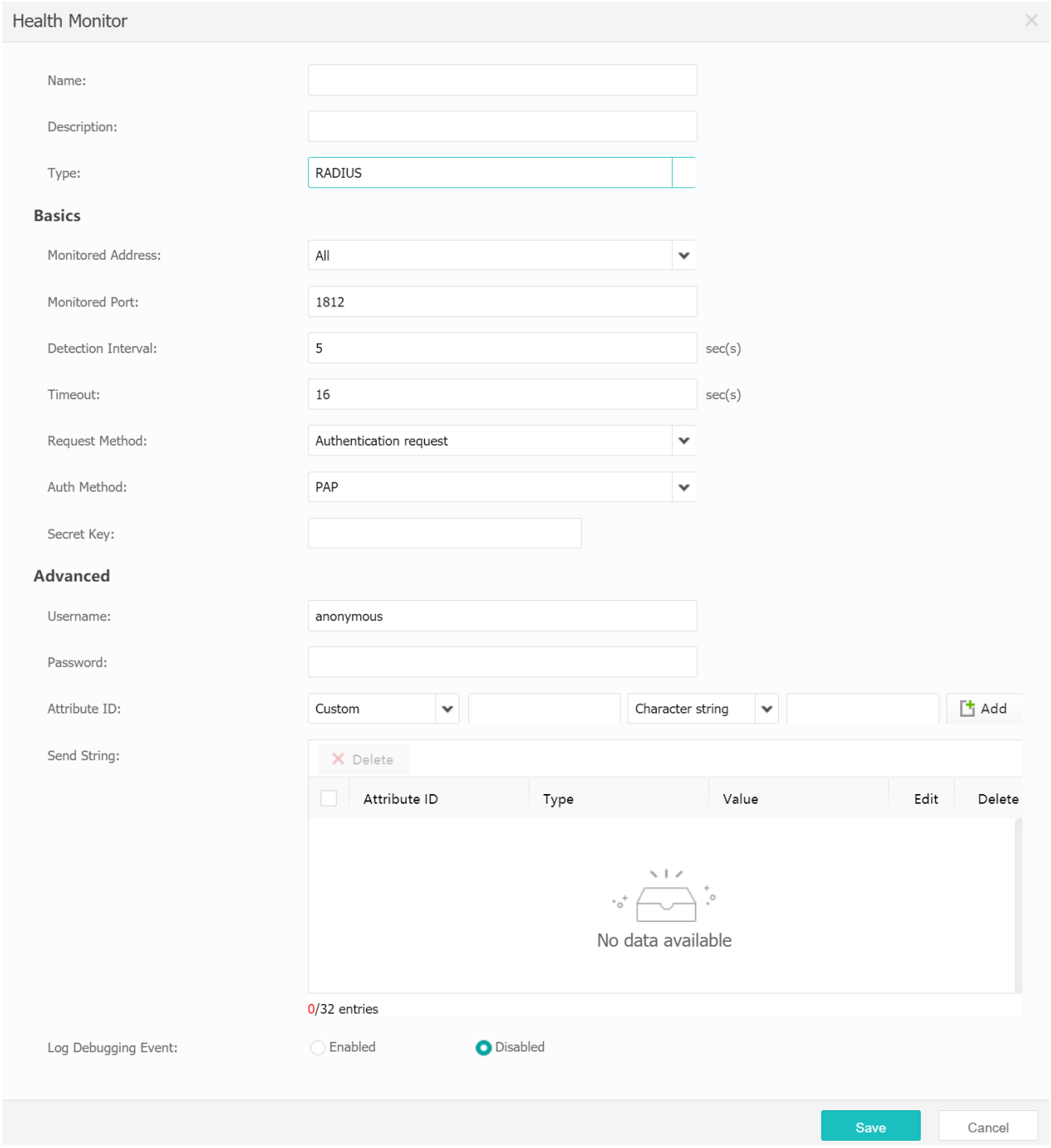
7.1.2.11 RADIUS

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as the case where the RADIUS server port can be connected but cannot respond to the authentication request or billing request, you can configure [RADIUS] health check to determine the health status of the node.

[Configuration Instruction]

Select『RADIUS』for『Type』and the device will send a RADIUS request to detect the node. Determine the health status of the node according to whether the node normally responds to the RADIUS request. The configuration is shown in the following figure:



『Request Method』configures the type of the request package sent. The authentication request sends the authentication request package, and the billing request sends the billing start and end request packages.

『Auth Method』configures the authentication encryption mode used by RADIUS request, which supports PAP and CHAP, and is only required for the authentication request.

『Secret Key』configures the key used by RADIUS service.

『Username』configures the username used by RADIUS request.

『Password』configures the password used for RADIUS request, which is only required when authenticating a request.

『Attribute ID』configures the identifier of attributes in RADIUS request sending. 56 kinds of attribute identifiers are built-in, and the ID can be customized.

『Type』configures attribute format in RADIUS request sending, which is divided into character string, decimal number, hexadecimal character string, IPv4 address, and IPv6 address. All attribute IDs support hexadecimal character string input.

『Value』configures the value of the attribute in the RADIUS request sending.

For other details about the configuration and instruction, see the『CONNECT(TCP)』health check section.

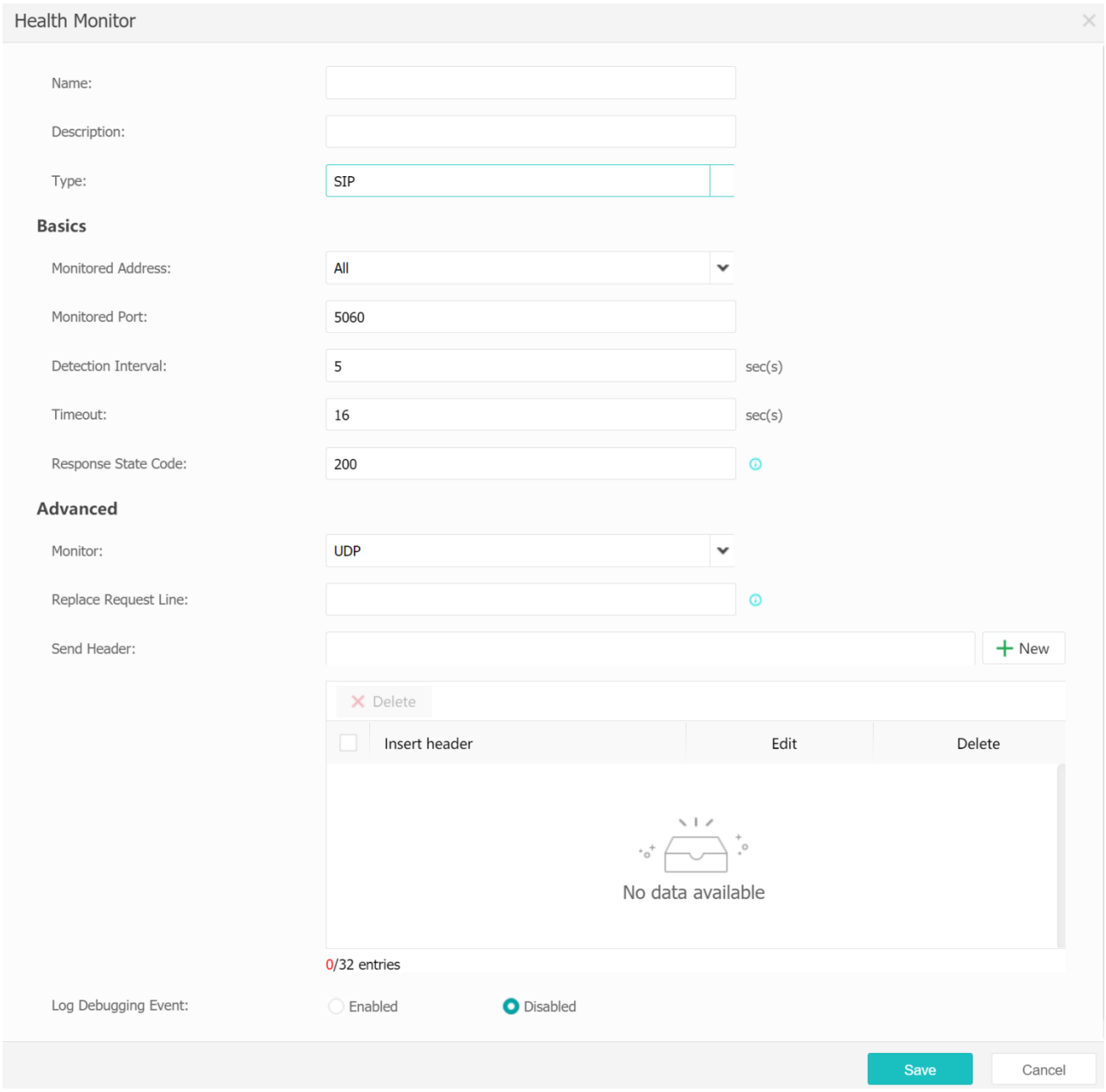
7.1.2.12 SIP

【Operation Scenarios】

It indicates the SIP type service health check. Monitor the SIP nodes at the back end, determine whether the nodes are online or offline, support IPV4 address monitoring, and support TCP and UCP protocol monitoring nodes.

[Configuration Instruction]

Select『SIP』for『Type』



『Monitor』supports the configuration of TCP or UDP.

『Replace Request Line』currently only supports OPTIONS replacement, such as OPTIONS sip: 11.11.11.114:5060 SIP/2.0.

『Send Header』supports header insertion. If no content is sent, the node will be considered online as long as there is a response package. If the server has no response, it indicates that the status is "unavailable".

For other details about the configuration and instruction, see the『CONNECT(TCP)』health check section.

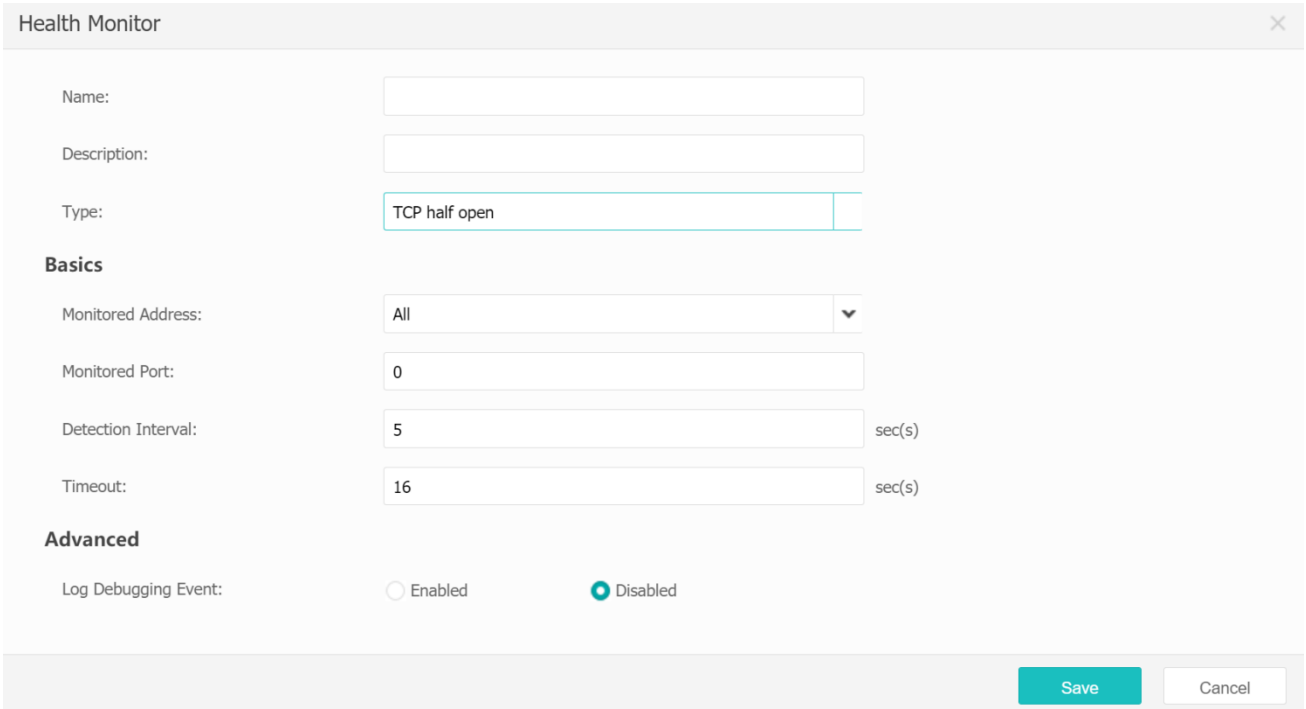
7.1.2.13 TCP Half Open

【Operation Scenarios】

When the IP access cannot correctly reflect the health status of the node or the node prohibits ICMP response, you can confirm the health status of the node by checking the active status of the application port. If TCP protocol is used, the [CONNECT(TCP)] health check can be configured. However, the complete TCP health check will occupy the concurrent connection of the server. In order to reduce the consumption of concurrent resources of the server, you can configure the [TCP Half Open] health check to determine the health status of the node.

[Configuration Instruction]

Select『TCP Half Open』for 『Type』and the device will send a TCP request to detect the node. Determine the health status of the node according to whether the node normally responds to the TCP request with SYN+ACK. The configuration is shown in the following figure:



For details about the configuration and instruction, see the『CONNECT(TCP)』health check section.

Attention: The difference between『TCP Half Open』health check and『CONNECT(TCP)』health check is that 『CONNECT(TCP))』health check first builds a connection through the three-way handshake, and then stop the connection through FIN, while『TCP Half Open』resets the connection through the RST sent after the node returns "SYN+ACK" during the three-way handshake. 『TCP Half Open』health check is faster and more efficient, however, too many RSTs may cause misjudgment by security policies.

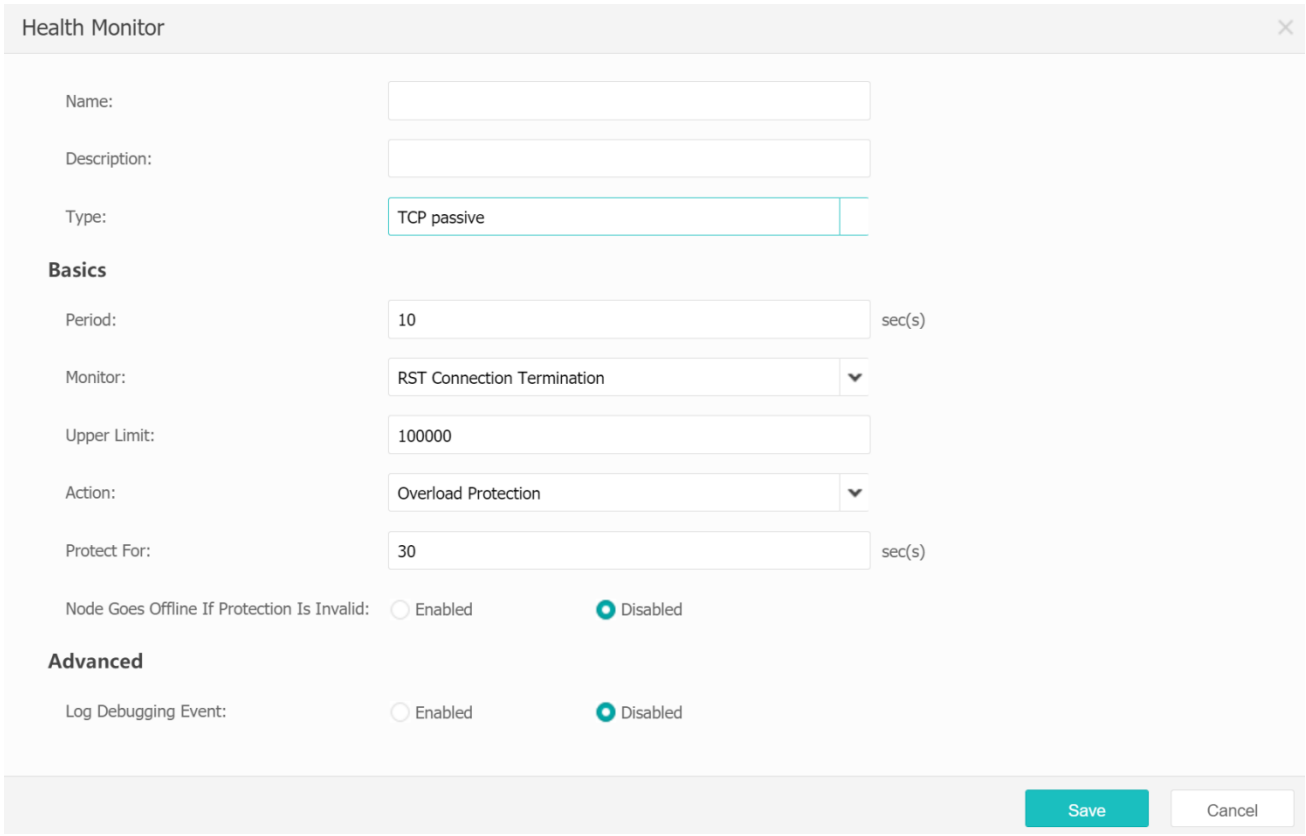
7.1.2.14 TCP Passive

【Operation Scenarios】

When the IP access cannot correctly reflect the health status of the node or the node prohibits ICMP response, you can confirm the health status of the node by checking the active status of the application port. To reduce the consumption of concurrent connection resources of the node, you can configure [TCP Half Open] health check. The health monitor will still send connection requests to the node. In order not to occupy the resources of the node at all, you can configure [TCP Passive] health check to determine the health status of the node.

[Configuration Instruction]

Select『TCP Passive』for『Type』and the device will passively check and count every response from the node to TCP. Determine the health status of the node according to whether the abnormal event reaches the upper limit of the configured monitored type within the statistical time. The configuration is shown in the following figure:



『Period』 configures the time range of health check statistics (unit: seconds), and the default value is 10 seconds.

『Monitor』 configures the monitored TCP event type. You can select RST Connection Termination (the server sends the RST packet to stop the connection, including RST stopping connection during the three-way handshake), or zero window (the server receives the zero window packets sent back after the buffer is full, or RST packets with zero window parameter corresponding to syn).

『Upper Limit』 configures the upper limit of TCP events specified in the statistical time. If the upper limit is exceeded, the following node 『Action』 is triggered. The RST statistical value is the number of packets, and the statistical value of zero window is a percentage.

『Action』 configures the action after an abnormality is detected. Overload Protection (change the node status to busy and prohibit new connections from being forwarded to the node) or Node

Goes Offline (change the node status to unavailable and disconnect all connections on the node) can be selected.

『Protect For』 configures the duration of overload protection action.

『Node Goes Offline If Protection Is Invalid』 configures whether to make node offline when the node is still busy after the overload protection is invalid. It is disabled by default (continuous overload protection on the node).

『Attempt Time』 configures the times of invalid overload protection. After reaching the limit, it makes the node offline, and the number of times is 4 by default.

Attention: Although 『TCP Passive』 health check does not occupy the resources of the node, it may fail to correctly reflect the health status of the node due to insufficient matching thresholds in the slump time period (e.g. night) or no response to the TCP request after the node crashes.

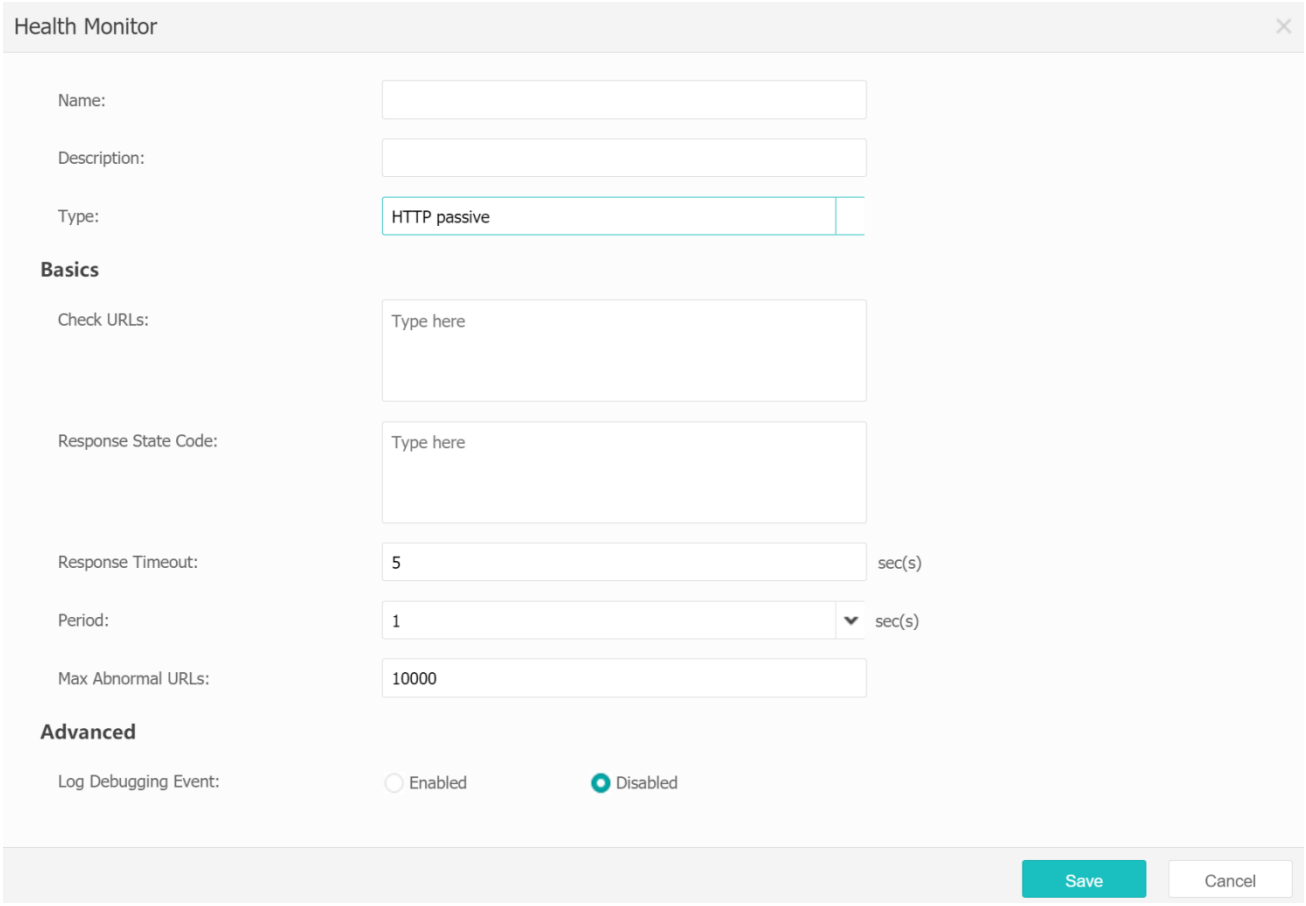
7.1.2.15 HTTP Passive

【Operation Scenarios】

When the HTTP application server's resources, such as CPU and memory, are consumed excessively, the WEB can sometimes be accessed normally and sometimes inaccessible. The [HTTP] health check is periodic, and as long as there is a successful response in the cycle, it is judged that the node is healthy. Therefore, the health status of the node cannot be reflected correctly. At this point, you can determine the health status of the node by configuring the [HTTP Passive] health check.

[Configuration Instruction]

Select 『HTTP Passive』 for 『Type』 and the device will passively check and count every state code from the node to HTTP. Determine the health status of the node according to whether the abnormal event reaches the upper limit of the configured monitored type within the statistical time. The configuration is shown in the following figure:



『Check URLs』 configures the URL prefix that matches the HTTP request to be checked.

『Response State Code』 configures the response state code that determines URL failures. When the response successfully matches the state code, this URL is determined to be invalid.

『Response Timeout』 configures the response timeout of URL response. When the period for responding exceeds the time period limit (ranging from 1 to 255 seconds), it is determined that the URL is invalid.

『Period』 configures the time range for statistics, which is optional from 1 to 5 seconds.

『Max Abnormal URLs』 configures that if the number of abnormal URLs reaches the set value within the statistical period, the node is determined to be invalid.

Attention: Although 『HTTP Passive』 health check can better reflect the health status of the node, it may fail to correctly reflect the health status of the node due to insufficient matching thresholds in the slump time period or no response to the HTTP request after the node crashes.

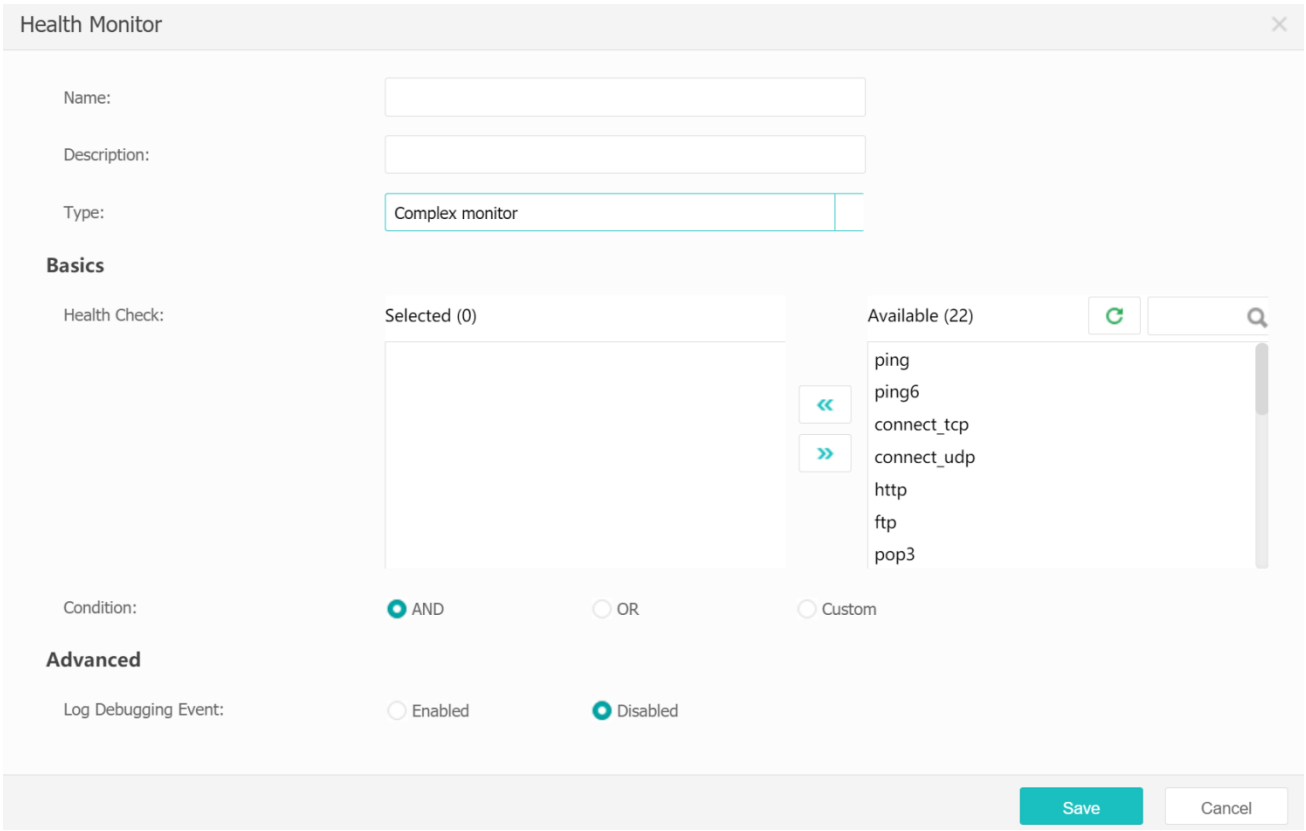
7.1.2.16 Complex Monitor

【Operation Scenarios】

When the result of a health check cannot correctly reflect the health status of the node, such as [HTTP] health check, which may cause the application to be opened slowly due to the busy node and the normal health check. At this point, you can configure the [HTTP Passive] health check, but it cannot correctly reflect the health status, either, due to certain limitations. For the above reasons, you can configure the [Complex Monitor] health check to determine the health status of the node.

[Configuration Instruction]

Select『Complex Monitor』for『Type』and then you can select multiple created health checks. The device monitors the nodes using multiple health checks at the same time. You can comprehensively determine the health status of the nodes according to the results of multiple health checks. The configuration is shown in the following figure:



『Health Check』configures multiple health checks that have been set. Click the required health checks from the Available list, and then click « to add them to the Selected list.

『Condition』 configures the conditions for passing the health checks. You can select from the fields of『AND』, 『OR』, or 『Custom』. The default setting is 『AND』. That is to say, the node is healthy only when the results of all health checks are normal. The complex monitor is mainly used in scenarios where there is a dependency between multiple different services.

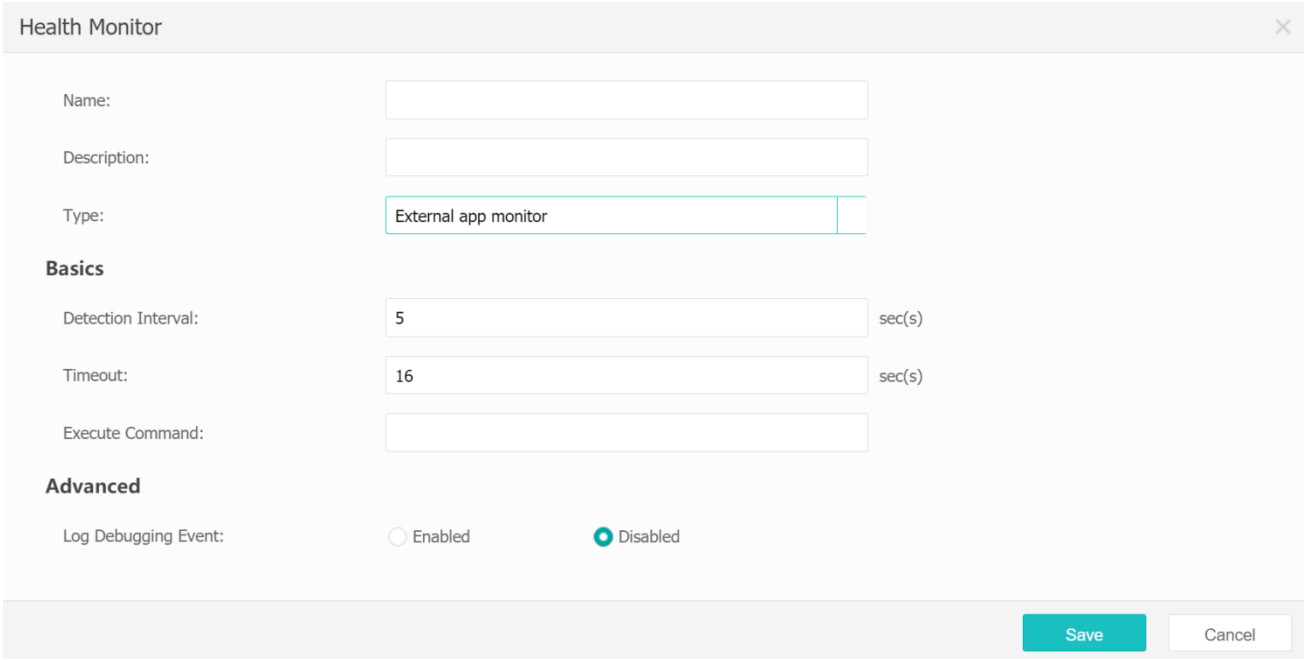
7.1.2.17 External App Monitor

【Operation Scenarios】

Applications supported by the ADC built-in health check are limited. When the built-in health check does not meet the application check requirements, you can better determine the health status of nodes by configuring [External App Monitor] health check, using customized development program scripts.

[Configuration Instruction]

Select『External App Monitor』for『Type』and the device will use the background script to monitor the node. Determine the health status of the node according to the script execution results. The configuration is shown in the following figure:



『Execute Command』 configures the command for ADC background execution script. The script to be executed needs to be uploaded to the /usr/monitor directory of the device through the

SFTP tool. The command can include built-in variables. ${rs_ip} represents the node IP and ${rs_port} represents the node port. If the node status is normal, the command needs to print "monitor:success" to the standard output. The node status is considered abnormal in other cases. For Java, it is java-cp/usr/monitor HttpMonitorDemo${rs_ip}${rs_port}; for Python, it is python/usr/monitor/HttpMonitorDemo. py${rs_ip}${rs_port}. (Note: To ensure the normal operation of the command, if using Java, you need to specify a search path. If using Python, you need to use an absolute path).

Debugging program: If you have enabled SSH permission, you can log in to SSH through port 22345, run "goroot build" to create or restore the programming environment ("goroot delete" can delete the whole programming environment), and then run the "gootor" command to enter the debugging and development environment of external app monitor. The development environment supports J2EE1.6 and Python2.7.3 by default. If other programming environments are required, you can deploy accordingly. Demo of Java and Python can be found in the /usr/monitor/ directory for reference.

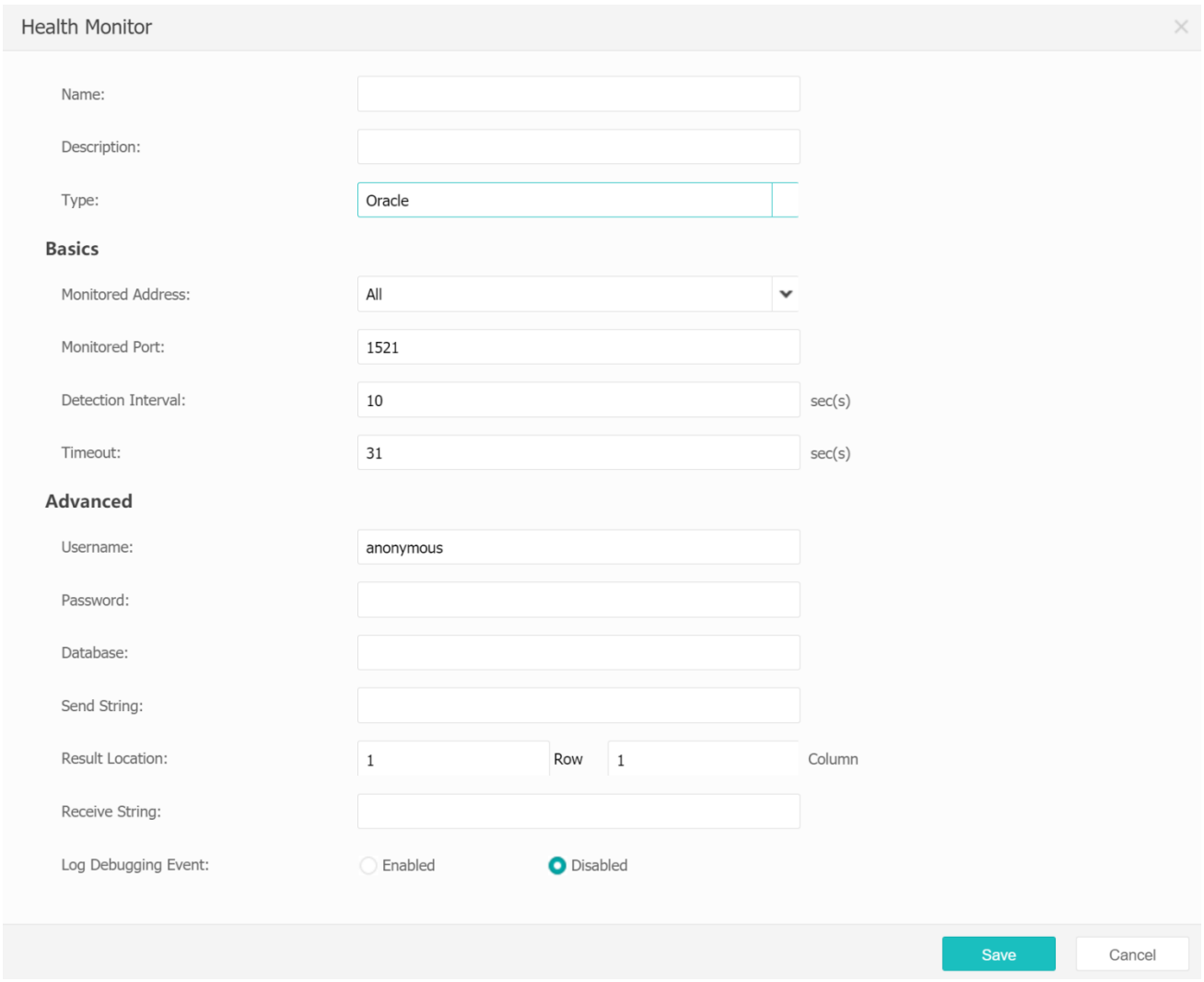
7.1.2.18 ORACLE

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as the case where you cannot log in to the database or the node is busy with query request processing and gives no response, you can configure [Oracle] health check to determine the health status of the node.

[Configuration Instruction]

Select『Oracle』for『Type』and the device will send an Oracle database request package to detect the node. Determine the health status of the node according to whether the node can be connected to the database normally, whether you can log in to the database with the configured username and password, or whether the node responds to the database query request based on the configured contents. The configuration is shown in the following figure:



『Monitored Address』 configures the IP address of detection, and all IP addresses are detected by default. It inherits the IP addresses of the nodes in the node pool.

『Monitored Port』 configures the database port for detection.

『Detection Interval』 configures the interval time for the health check, that is, the duration between the previous health check and the current health check (unit: seconds).

『Timeout』 configures the timeout for the health check. If no response from the node is received after the configured time, it is considered as timeout (unit: seconds).

『Username』 configures the username for logging in to the database to execute SQL statements. To use the function, you should have the SELECT query permission.

『Password』 configures the password for logging in to the database.

『Database』 configures the name of the database that executes the SQL statements.

『Send String』 configures the content to execute the SQL statements. When filling in the content to be sent, try to use executable SQL statements that do not impact performance and have a small amount of data. 『Oracle』 health check only supports the SELECT query statements.

『Result Location』 configures the location where the returned results are after executing the SQL statements.

『Receive String』 configures the content that the result returned in 『Result Location』 must contain.

『Log Debugging Event』 configures whether to enable the debugging log of the health check. After enabling, detailed connection records will be displayed in the log.

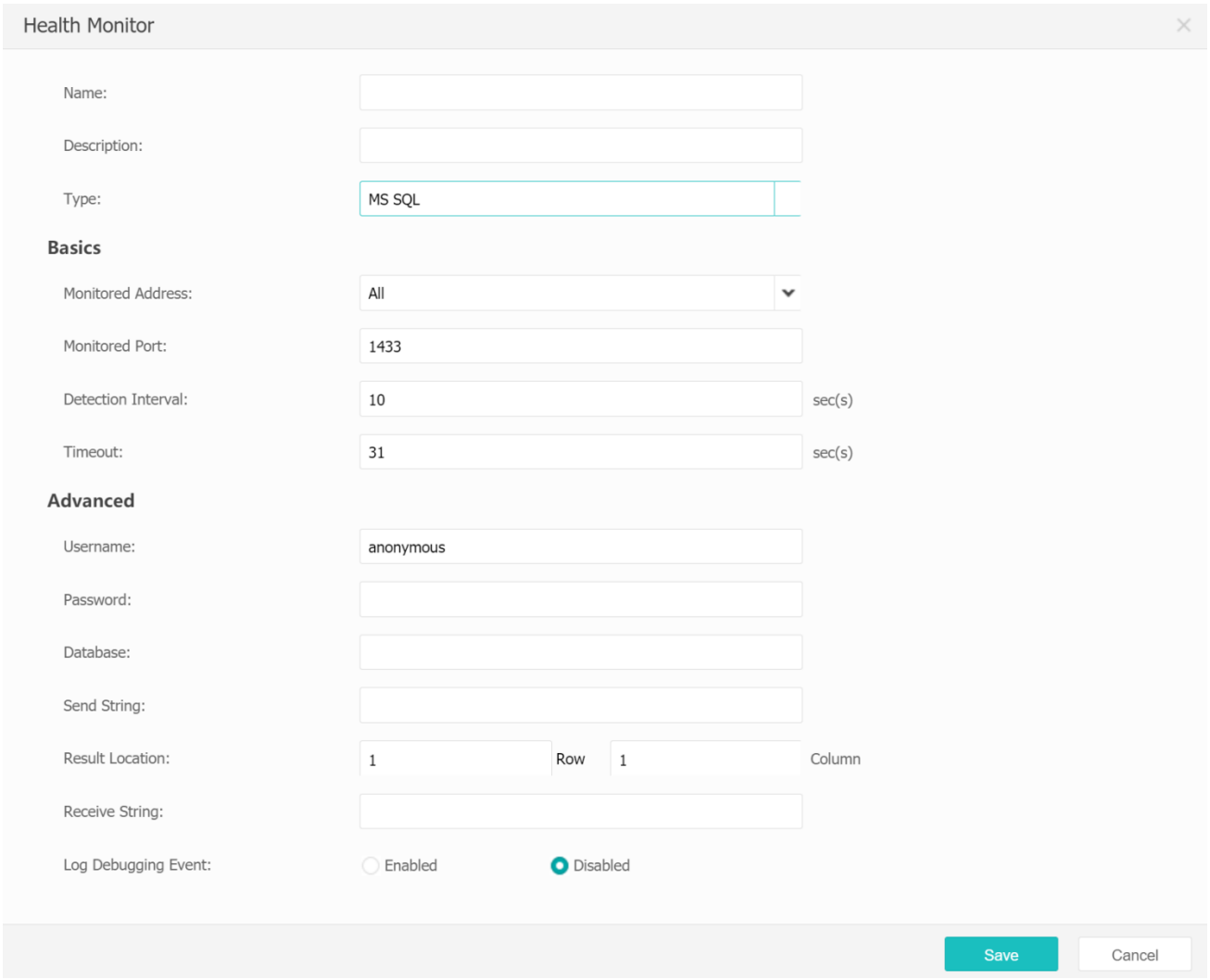
7.1.2.19 MS SQL

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as the case where you cannot log in to the database or the node is busy with query request processing and gives no response, you can configure [Oracle] health check to determine the health status of the node.

[Configuration Instruction]

Select 『MS SQL』 for 『Type』 and the device will send an MS SQL database request package to detect the node. Determine the health status of the node according to whether the node can be connected to the database normally, whether you can log in to the database with the configured username and password, or whether the node responds to the database query request based on the configured contents. The configuration is shown in the following figure:



For details about the configuration and instruction, see the『Oracle』health check section.

Attention: In addition to the SELECT query statements, 『MS SQL』also supports the UPDATE (database update) statements. The login user configured must have permission to execute the corresponding statements.

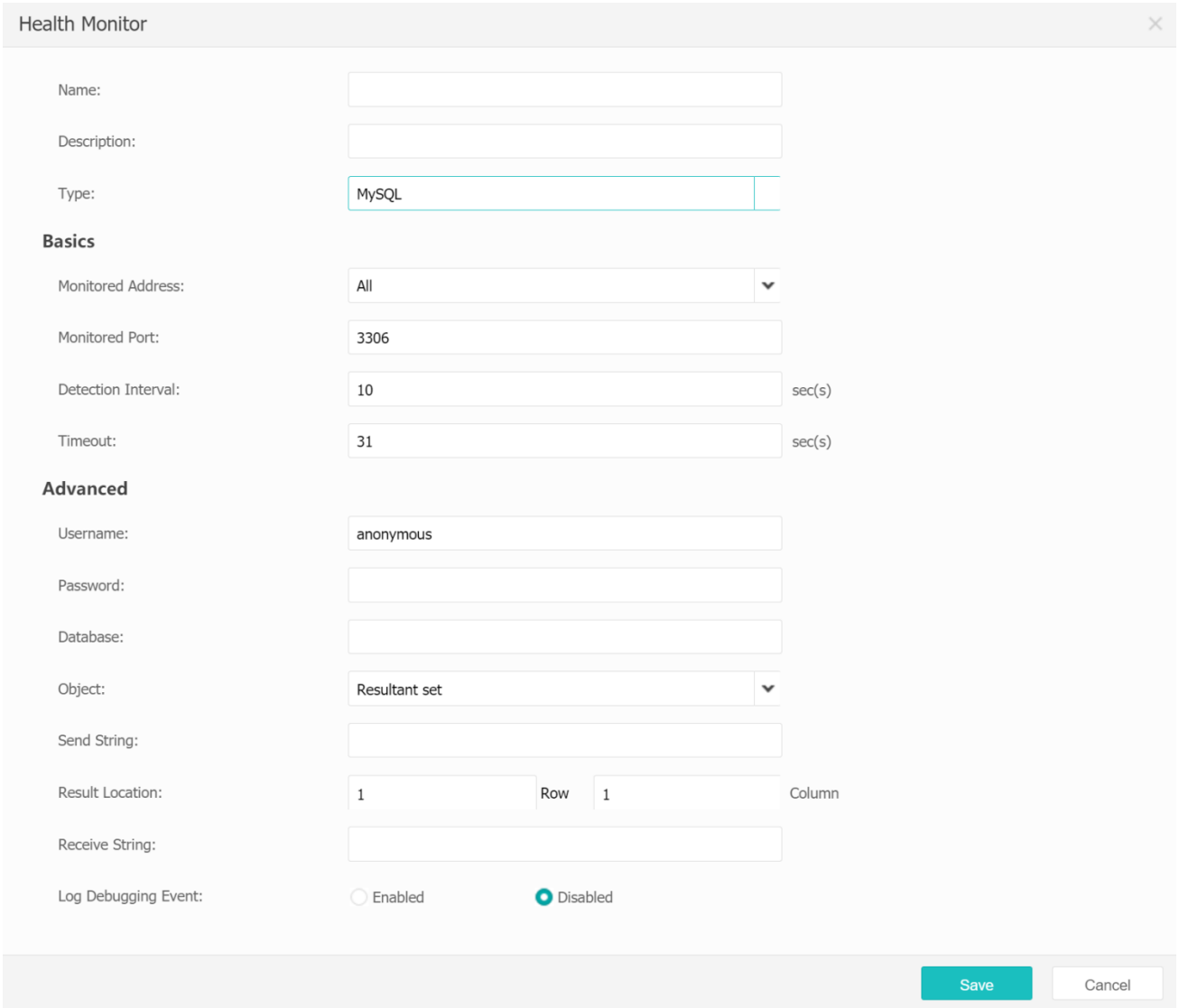
7.1.2.20 MYSQL

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as the case where you cannot log in to the database or the node is busy with query request processing and gives no response, you can configure [Oracle] health check to determine the health status of the node.

[Configuration Instruction]

Select『MySQL』for『Type』and the device will send a MySQL database request package to detect the node. Determine the health status of the node according to whether the node can be connected to the database normally, whether you can log in to the database with the configured username and password, or whether the node responds to the database query request based on the configured contents. The configuration is shown in the following figure:



『Object』configures the result judgment method of the MySQL health check. You can select to query resultant set or synchronization status. All configurations and instructions are the same as that of the『Oracle』health check if you choose to query the resultant set; the unmodifiable "show slave status" synchronization query statement is sent by default if you choose to query the

synchronization status. The built-in『Result Location』and 『Receive String』are used to determine whether the database's slave database completes replication and synchronization, and determine the health status of the database based on it.

『Synchronization Timeout Check』 configures the synchronization timeout check for the MySQL database. If 『Synchronization Status』is selected for『Object』, there will be this function option. After enabling, you need to configure the synchronization timeout, and by obtaining the synchronization timestamp of "slave database", you can determine the maximum time duration for replication, and determine the health of the database based on the duration. This function is disabled by default.

For other details about the configuration and instruction, see the『Oracle』health check section.

Attention: In addition to the SELECT query statements, the 『MySQL』 also supports the SHOW command. The login user configured by health check must have permission to execute the corresponding statements.

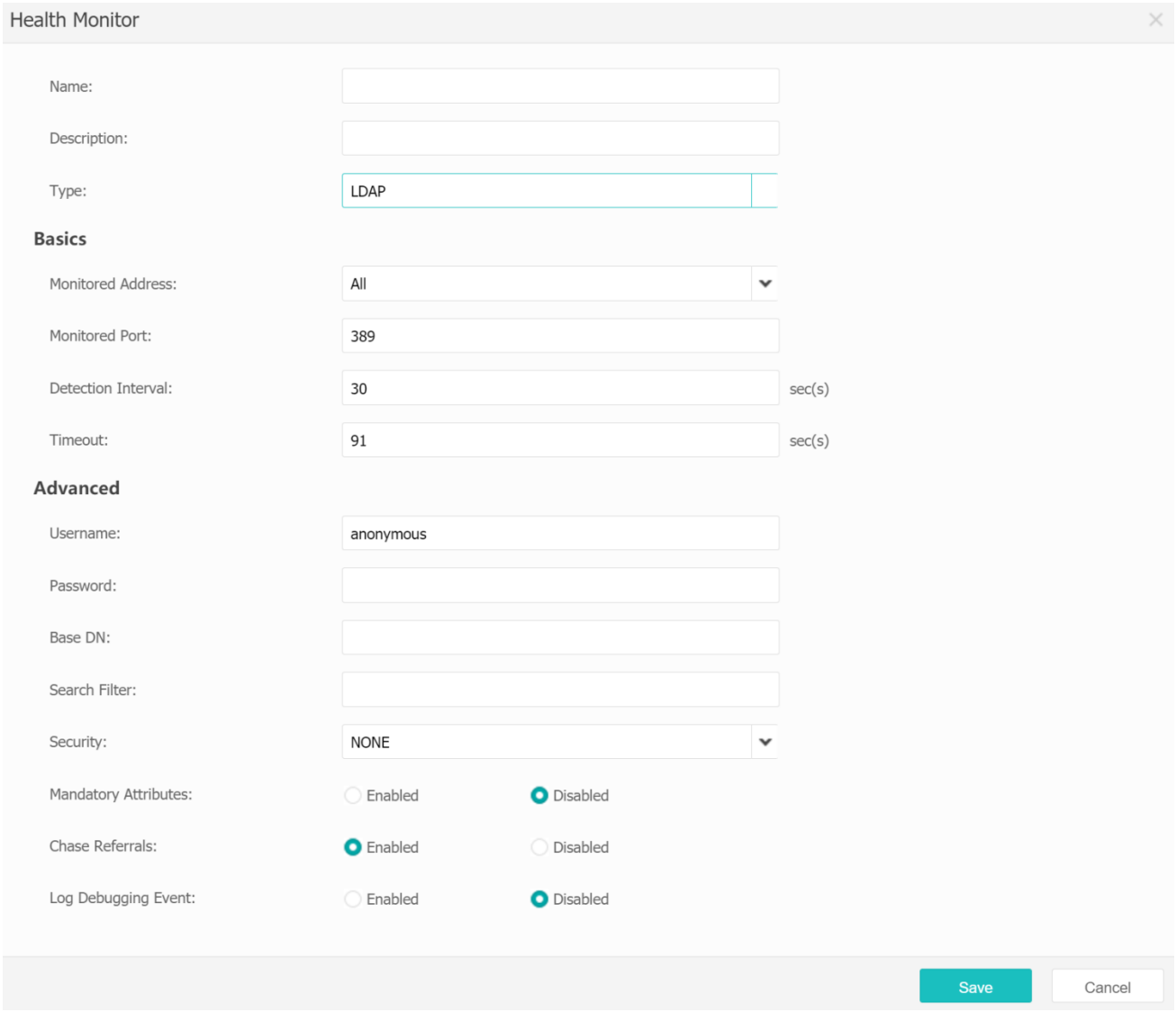
7.1.2.21 LDAP

【Operation Scenarios】

When application port access cannot correctly reflect the health status of the node, as sometimes the application port is open but the service is abnormal, such as the case where you cannot log in to the LDAP, you can configure [LDAP] health check to determine the health status of the node.

[Configuration Instruction]

Select『LDAP』for『Type』and the device will send an LDAP request package to detect the node. Determine the health status of the node according to whether the node responds to the database normally, whether you can log in to the LDAP with the configured username and password, or whether the node responds to the LDAP query request with the configured contents. The configuration is shown in the following figure:



『Username』 configures the username for LDAP login. Only if the monitored target needs to be verified, it is configured.

『Password』 configures the password for LDAP login. Only if the monitored target needs to be authenticated, it is configured.

『Base DN』 configures the location of the LDAP tree for starting a health check from the health monitor. For example: dc=test, dc=com.

『Search Filter』 configures a health check filter to search for a specified attribute, such as (&(|(uid=ZHANGSAN)(uid=LISI)) (objectclass=person)), indicating that the search uid is ZHANGSAN or LISI. The * sign is used to represent any value, such as objectclass=*.

『Security』 configures whether SSL encryption is used for communication with nodes. It is not encrypted by default.

『Mandatory Attributes』 configures whether the response data of the node includes the globally unique Object Identifier (OID). If the account must have a userid, it is disabled by default and will not be checked.

『Chase Referrals』 configures whether to continue tracking and jumping after receiving LDAP referral entries. Disabling it can prevent continued queries of referral entries and jump to other servers, etc. It is enabled by default.

For other details about the configuration and instruction, see the 『CONNECT(TCP)』 health check section.

7.1.3 Session Persistence

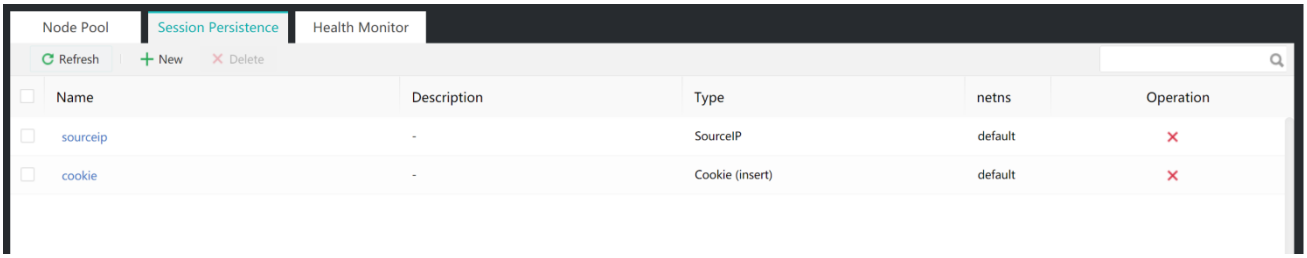
【Operation Scenarios】

As the load balancing strategy is configured, the subsequent requests of the client will be allocated to different nodes due to the load balancing algorithm, resulting in no previous session information on the newly allocated node, and the client is reset. You need to use the ADC to make the connection to the same client always on the same node. This function can be achieved by configuring 『Session Persistence』.

【Operation Procedure】

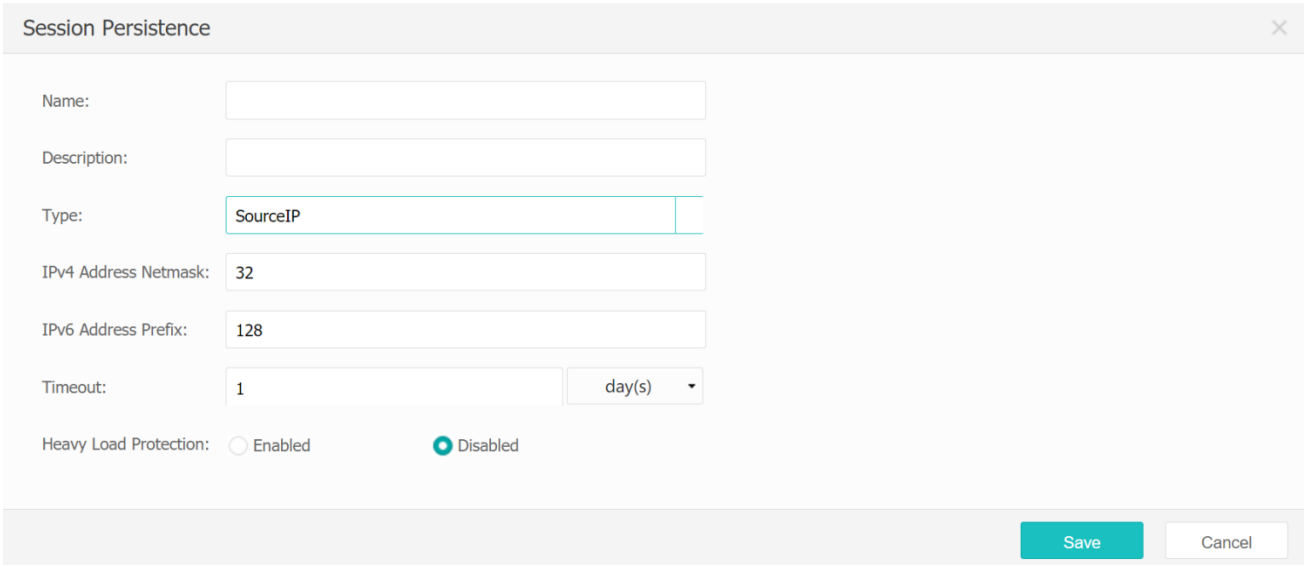
『App Load Balancing』→『None Pool』→『Session Persistence』. On the『App Load Balancing』 menu, click Node Pool, select『Session Persistence』in the node pool window on the right, and click New.

The page is shown in the figure below:

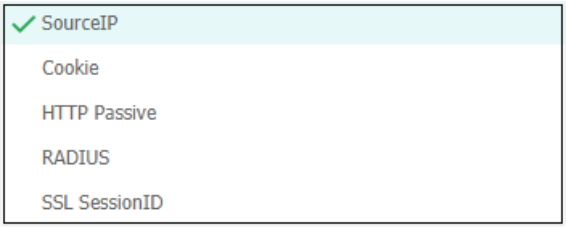


『Name』,『Description』,『Type』, and『Operation』are displayed under『Session Persistence』, and a Delete button is under the『Operation』column for deleting a single entry. The『Session Persistence』defined here can be used for the configuration of『Node Pool』.

Click the New button, as shown in the following figure:



『Type』drop-down list shows the available session persistence types, including [SourceIP], [Cookie], [HTTP Passive], [RADIUS] and [SSL SessionID].



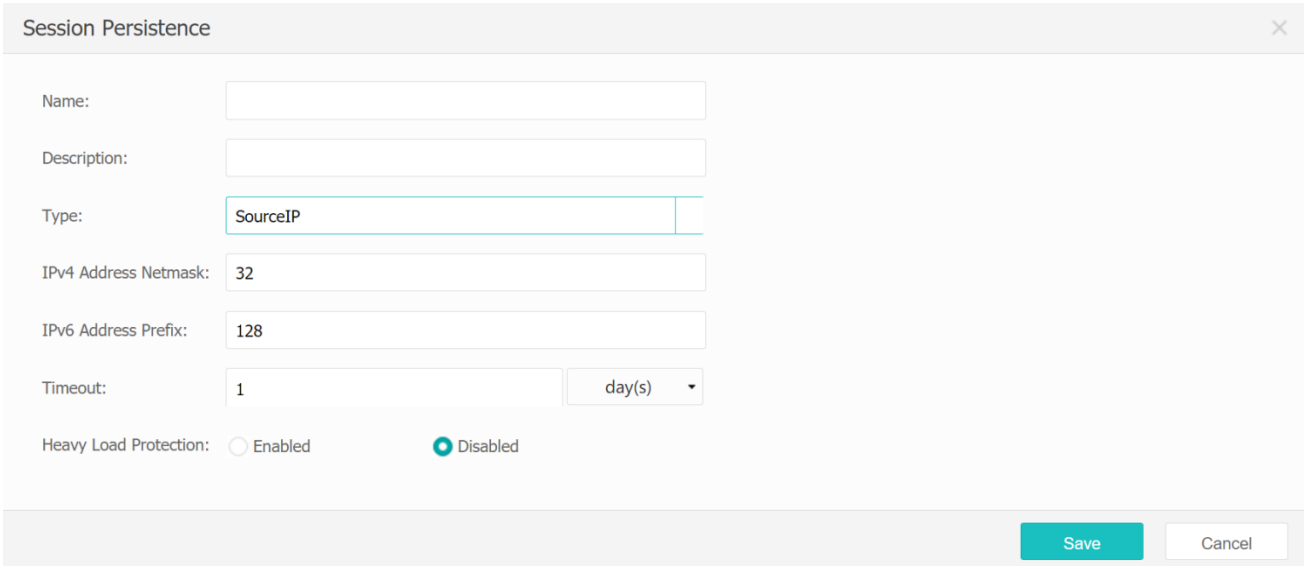
7.1.3.1 SourceIP

【Operation Scenarios】

It is the most basic mode for session persistence and matches only the source IP address of the clients and can forward all traffic from the same IP address or IP address segment to the same node. It is suitable for all protocols. But in some scenarios, the load may not be balanced enough as the clients use the same IP address.

[Configuration Instruction]

Select 『SourceIP』 for 『Type』 and configure the session persistence based on source IP. The device will allocate the traffic of the same source IP to the same node as it takes the source IP as the matching condition. The configuration is shown in the following figure: Generally, only Name needs to be set;



For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『IPv4 Address Netmask』 configures the client IPv4 address netmask for session persistence and determines whether the source IP of a certain visit belongs to an existing session persistence record through the netmask. If it is configured to 32, each IP is matched with corresponding session persistence individually;

『IPv6 Address Prefix』 configures the client IPv6 address prefix for session retention and determines whether the source IP of a certain visit belongs to an existing session persistence

record through the prefix. If it is configured to 128, each IP is matched with corresponding session persistence individually;

『Timeout』configures the maximum time limit for a session record to exist (365 days at most), and the session will be invalid after the limit is exceeded. If there is a new hit within this time period, the session will be reset. The unit of time period supports second(s), minute(s), hour(s) and day(s);

『Heavy Load Protection』 configures whether the connection of hit session persistence is restricted by Heavy Load Protection. After enabling, the session persistence will become invalid when the node is busy, and it is disabled by default.

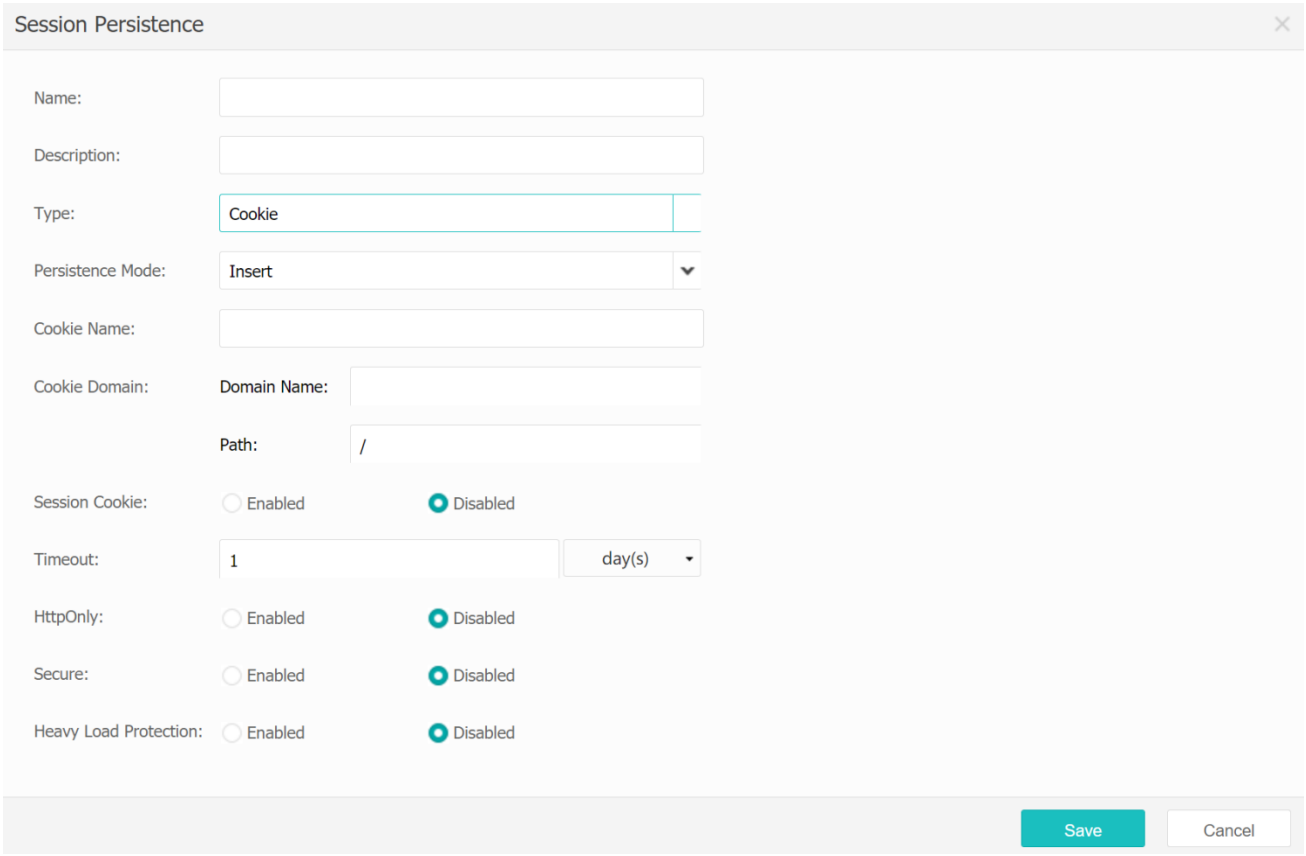
7.1.3.2 Cookie

【Operation Scenarios】

When all source clients use traffic from the same source IP and the applications are based on the HTTP protocol (e.g. education network, corporate network outlet, and CDN drainage), if the source IP is still used for session persistence, all the traffic of the company or school will be fully loaded to the same node, leading to an unbalanced load. At this point, a Cookie-based session persistence mode can be configured, which matches the Cookie field in the HTTP request. Different Cookies can be used to distinguish different clients, and all HTTP traffic carrying the same Cookie can be forwarded to the same node. It is only suitable for HTTP and HTTPS applications that have gone through SSL offloading.

[Configuration Instruction]

Select『Cookie』for『Type』and configure the session persistence based on Cookie. The device will allocate the HTTP traffic of the same Cookie to the same node as it takes the Cookie as the matching condition. The configuration is shown in the following figure: Generally, Name, Type, Cookie Name, Cookie Domain, etc. need to be set;



『Persistence Mode』configures the Cookie session persistence mode, and『Insert』,『Passive』, and『Rewrite』are optional. When ADC receives a response from the server, if『Insert』 is selected, the domain can be configured, and a Set-cookie field will be added to the HTTP protocol header of the response to create session persistence. The content of this field includes the Cookie name, the Cookie domain name, path, and timeout. If 『Passive』 is selected, the corresponding Cookie information will be found by analyzing the Set-cookie field in the HTTP header of the response, and this Cookie and corresponding node information will be recorded for the next scheduling. If the Cookie returned by the node does not have any expiration time, it will be recorded according to the set timeout time. If『Rewrite』is selected, the Cookie name in the Set-cookie field in the HTTP header of the matching response is rewritten, and the node information is inserted. "The original Cookie value" is rewritten as "SANGFOR_node value_original Cookie value", and the session persistence is done according to the node information during requesting. The ADC will rewrite the

Cookie in the subsequent request of the client, removing the "SANGFOR_node value" _", changing it to the original Cookie, and sending it to the server.

『Cookie Name』 configures the name of the Key part in the Cookie field, which cannot conflict with other cookie names (such as the Cookie name in the HTTP response of the server, common path, domain, etc.). If『Insert』 is selected, the Cookie of ADC will be inserted in the first HTTP response package. The cookie value is a value preset for the newly added node when configuring the node pool. It can be viewed by clicking the corresponding node in 『Node Pool』 → 『Nodes』. If the Cookie name is set to "sangfor" and the default value of the node is 66666666, the Cookie field inserted is "Set-Cookie:sangfor=66666666;path=/" (the default path is /). If the content returned by the server contains Cookie, the client will receive a response packet containing two Set-C Cookie headers and include the contents of these two Set-C Cookies at the same time during requesting.

『Cookie Domain』 → 『Domain Name』configures the name of Cookie domain. The default is the domain name first named, which is mainly used in the following scenarios: Issue a virtual service www.test.com and use Cookie session persistence. If it is necessary to access the link news.test.com on the page, the session persistence will not be matched but will be rescheduled, causing access failure. At this point, you need to set the domain name test.com to ensure that the subdomain name is also matched to the session persistence. If you visit test.com for the first time, you can ensure that the current domain name and subdomain name can be matched to the session persistence without setting the domain name.

『Cookie Domain』→ 『Path』is mainly used in the following scenarios: The customer has two different HTTP servers, A and B. When ADC is not deployed, the page can be scheduled to server A through test.com/test1/1.php, and to server B through test.com/test2/2.php. If the above-mentioned requirements need to be fulfilled after the deployment of ADC, it is necessary to use paths to distinguish, so that scheduling to different servers is available through different paths. If the default/root directory is not set, it will cause two pages to be scheduled to the same server.

For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『Session Cookie』 enables or disables session Cookies. After enabling, the lifetime of the Cookie is the browser session time. After disabling, you need to manually set the Cookie timeout.

『Timeout』configures the maximum time limit for a session record to exist (365 days at most), and the session will be invalid after the limit is exceeded. If there is a new hit within this time period, the session will be reset. The unit of time period supports second(s), minute(s), hour(s) and day(s).

『HttpOnly』 configures whether to enable the HttpOnly attribute for Cookie. Set Cookie as HttpOnly to prevent XSS attack, prohibit web page program from stealing Cookie content and increase Cookie security. However, if such a program has been on the page, page loading will be abnormal after enabling it.

『Secure』 configures whether to enable the Secure attribute for Cookie. Set Cookie as Secure to prevent Cookies from being stolen by the middleman during HTTP transmission. Do not use HTTP to transmit Cookies so as to increase security. However, if there is a page or content mixed with HTTP and HTTPS on the website, login is required again when jumping from HTTPS to HTTP, affecting normal access.

『Heavy Load Protection』 configures whether the connection of hit session persistence is restricted by Heavy Load Protection. After enabling, the session persistence will become invalid when the node is busy, and it is disabled by default.

7.1.3.3 HTTP Passive

【Operation Scenarios】

If the client applications use HTTP, and the clients use the same IP, the source IP cannot be used for session persistence and the clients do not support the use of Cookies, then the session

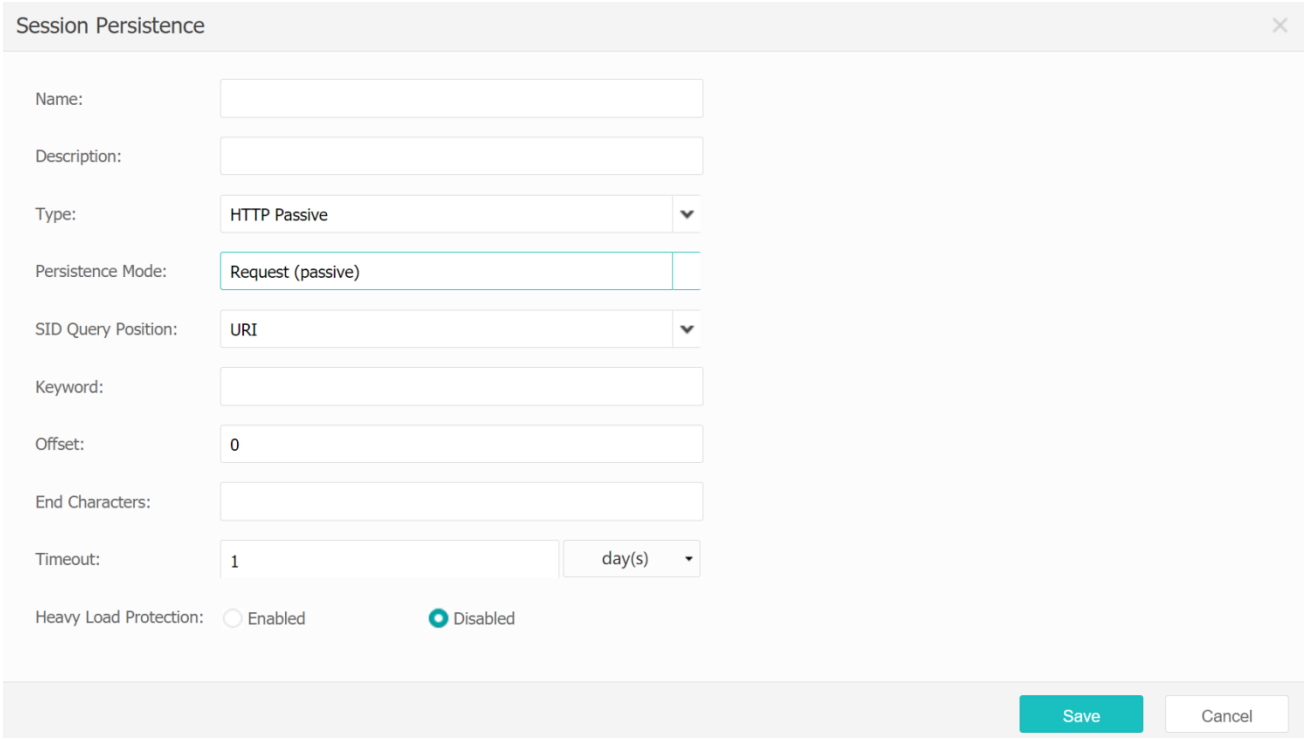
persistence can only be done according to the characteristics of the data packet. You can use 『HTTP Passive』 passive session persistence as a solution.

[Configuration Instruction]

Select『HTTP Passive』for『Type』and configure the passive session persistence based on HTTP. The device will allocate the traffic of the same HTTP request to the same node as it takes the HTTP request as the matching condition. The configuration is shown in the following figure:

7.1.3.3.1 HTTP Request(Passive)

In request direction, learn the content that needs session persistence.



『Persistence Mode』configures session persistence based on a certain field in request and response directions.

『SID Query Position』 configures the query position of session persistence parameters. You can select [Header], [URI] or [Content].

『Header Name』 configures the HTTP header name for querying the request.

『Keyword』 configures the keyword name of the request.

『Offset』 configures the number of bits for the offset from the keyword in request direction (0-255).

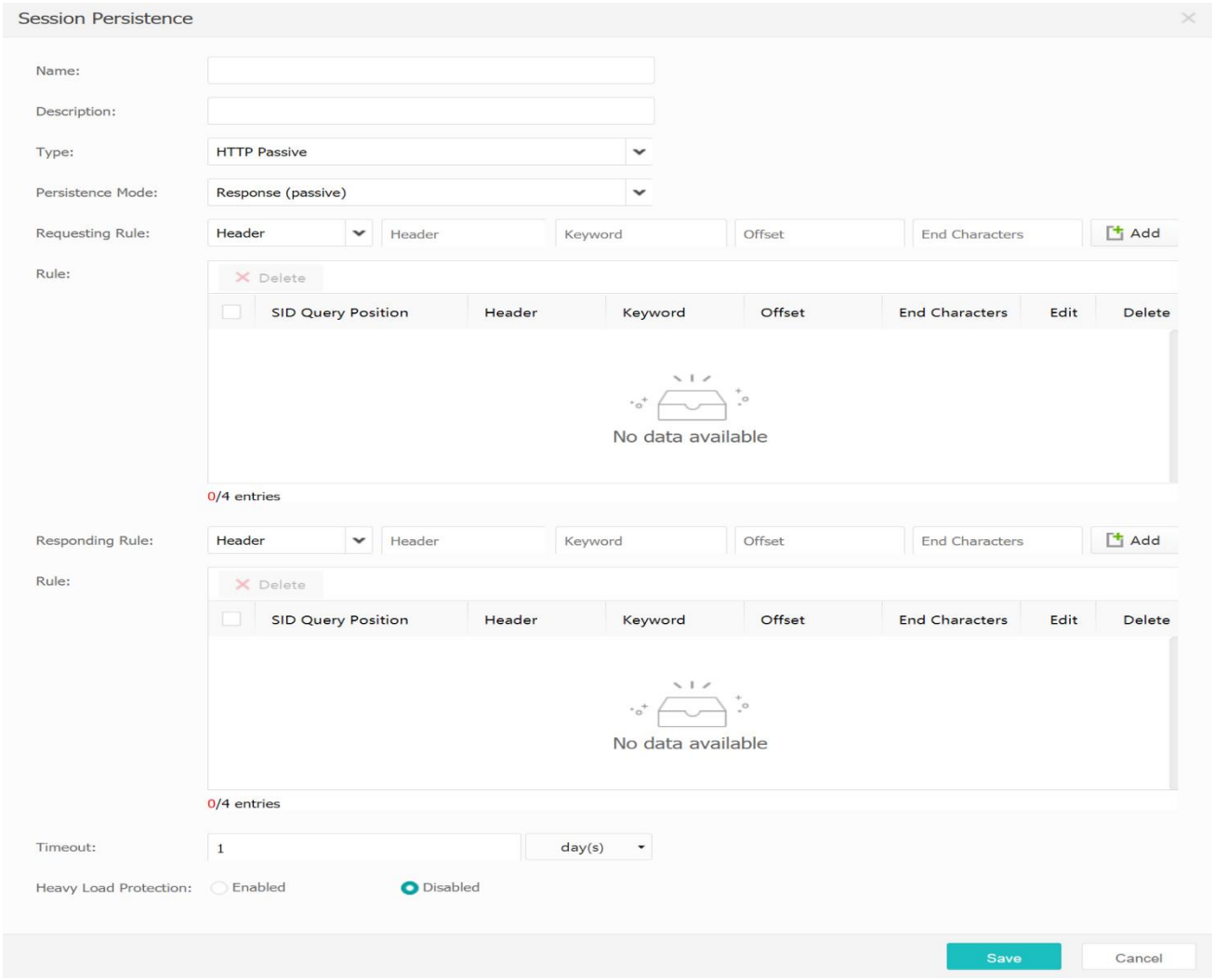
『End Characters』 configures the keyword end character in request direction.

『Timeout』 configures the timeout of the session persistence.

『Heavy Load Protection』 configures whether the connection of hit session persistence is restricted by Heavy Load Protection. After enabling, the session persistence will become invalid when the node is busy, and it is disabled by default.

7.1.3.3.2 HTTP Response(Passive)

In response direction, learn the content that needs session persistence. In request direction, find out whether there is corresponding content in subsequent data packets for session persistence.



『Persistence Mode』 configures session persistence based on a certain field in request and response directions.

『Requesting Rule』 configures the conditions of matching in request direction, and the matching content is the content matched in response direction.

[Header Name] configures the HTTP header name for querying the request.

[Keyword] configures the keyword name in request direction.

[Offset] configures the number of bits for the offset from the keyword in request direction.

[End Characters] configures the keyword end character in request direction.

『Responding Rule』 configures the content matched in response direction, which is used to match the content of session persistence in request direction later.

[Header Name] configures the HTTP header name for querying the response.

[Keyword] configures the keyword name in response direction.

[Offset] configures the number of bits for the offset from the keyword in response direction.

[End Characters] configures the keyword end character in response direction.

『Timeout』 configures the timeout of the session persistence.

『Heavy Load Protection』 configures whether the connection of hit session persistence is restricted by Heavy Load Protection. After enabling, the session persistence will become invalid when the node is busy, and it is disabled by default.

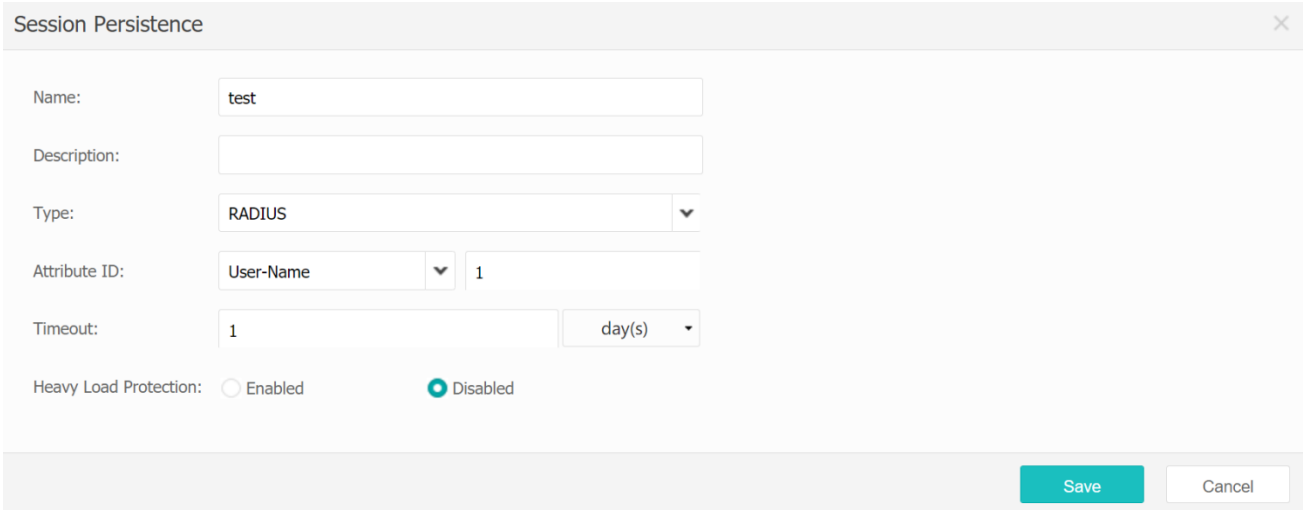
7.1.3.4 RADIUS

【Operation Scenarios】

It is a session persistence mode based on the RADIUS attribute value and can forward all traffic with the same RADIUS attribute value to the same node according to the configuration. It is only suitable for the RADIUS protocol.

[Configuration Instruction]

Select『RADIUS』for『Type』and configure the session persistence based on the RADIUS attribute value. The device will allocate the traffic with the same RADIUS attribute value to the same node as it takes the RADIUS attribute value as the matching condition. The configuration is shown in the following figure:



『Attribute ID』configures which attribute value of RADIUS is used for the session persistence.

You can select the system built-in attribute values or customize the attribute values.

『Timeout』configures the timeout of the session persistence, in second(s), minute(s), hour(s), or day(s).

『Heavy Load Protection』configures whether the connection of hit session persistence is restricted by Heavy Load Protection. After enabling, the session persistence will become invalid when the node is busy, and it is disabled by default.

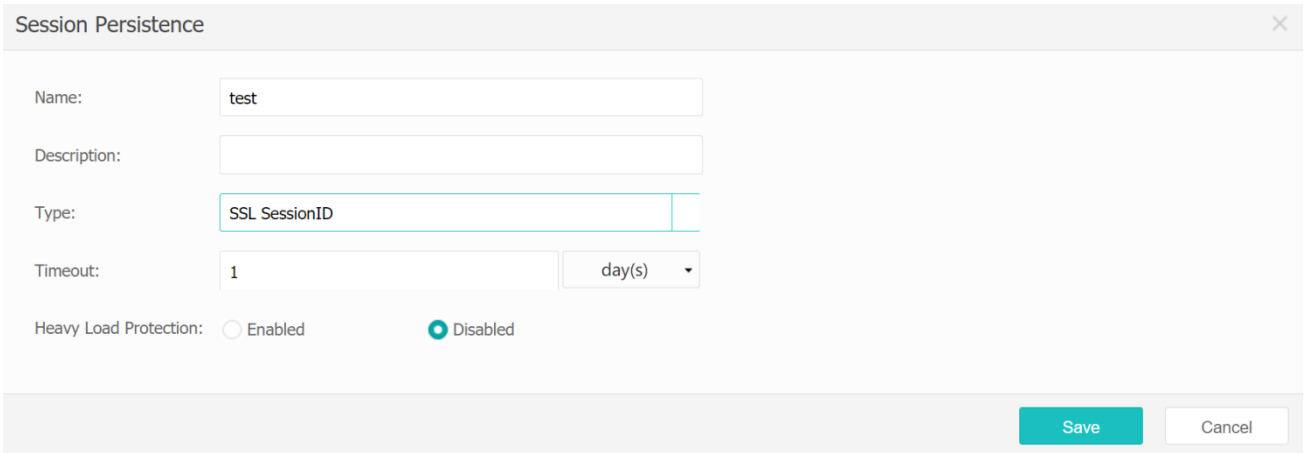
7.1.3.5 SSL SessionID

【Operation Scenarios】

It is a session persistence mode based on SSL SessionID and can forward all traffic from the same SSL SessionID to the same node. It is suitable for HTTPS and SSL protocols.

[Configuration Instruction]

Select『SSL SessionID』for『Type』and configure the session persistence based on SSL SessionID. The device will allocate the traffic from the same SSL SessionID to the same node as it takes SSL SessionID as the matching condition. The configuration is shown in the following figure:



『Timeout』 configures the timeout of the session persistence, in second(s), minute(s), hour(s), or day(s).

『Heavy Load Protection』 configures whether the connection of hit session persistence is restricted by Heavy Load Protection. After enabling, the session persistence will become invalid when the node is busy, and it is disabled by default.

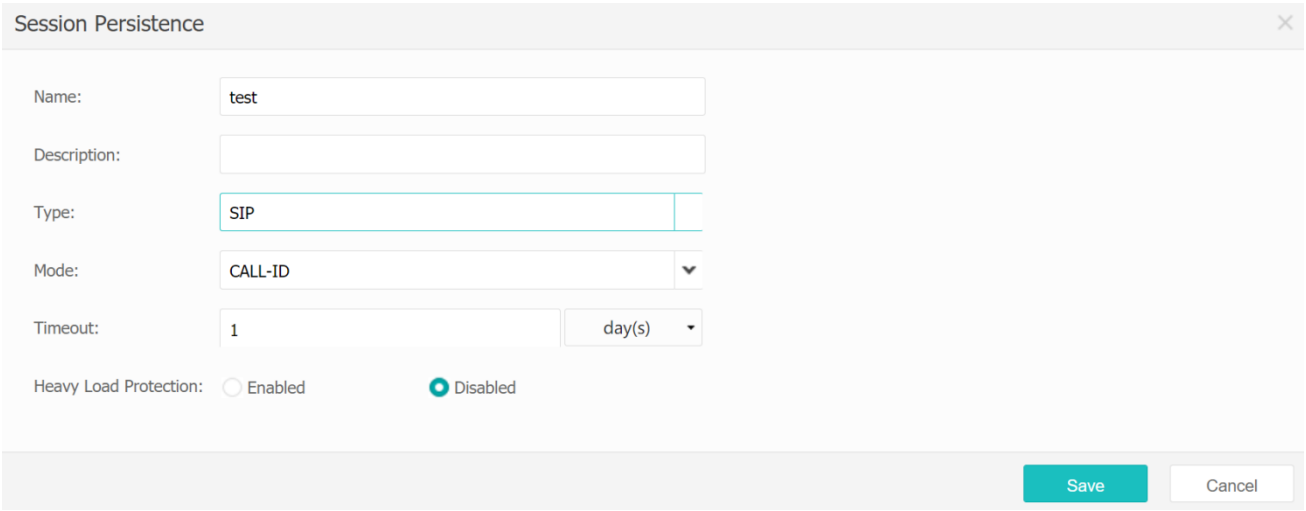
7.1.3.6 SIP

【Operation Scenarios】

It is a session persistence mode based on SIP call-id and can forward the sessions with the same call-id attribute to the same server to achieve session persistence.

[Configuration Instruction]

Select 『SIP』 for 『Type』



For 『Mode』, CALL-ID is currently filled in, that is, the session persistence is based on SIP call-id.

『Timeout』 configures the timeout of the session persistence, in second(s), minute(s), hour(s), or day(s).

『Heavy Load Protection』 configures whether the connection of hit session persistence is restricted by Heavy Load Protection. After enabling, the session persistence will become invalid when the node is busy, and it is disabled by default.

7.1.4 Node Pool

7.1.4.1 Create Node Pool

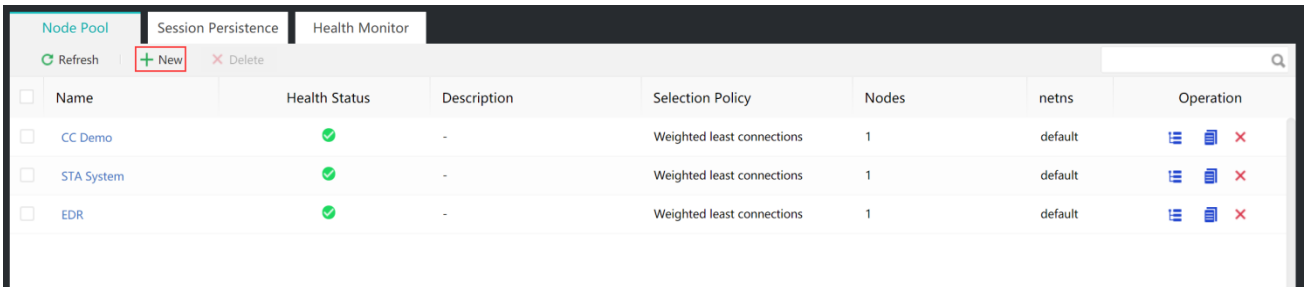
【Operation Scenarios】

Targeting load balancing, you need to deploy multiple server nodes to publish services at the same time. The node pool divides these server nodes into the same resource pool for scheduling, so that when clients access the corresponding services, they can be evenly distributed to these server nodes through the strategy of the node pool.

【Operation Procedure】

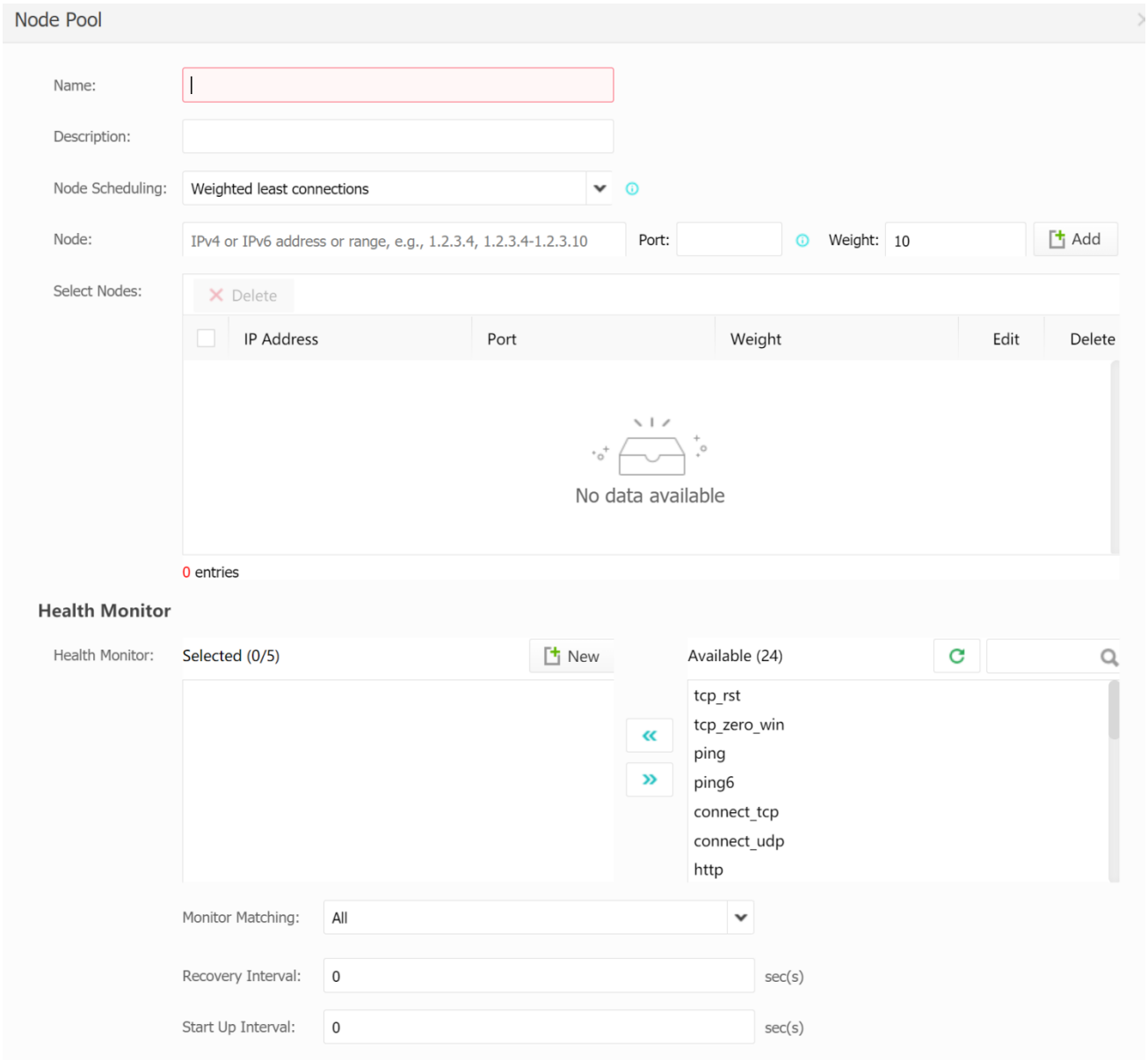
『App Load Balancing』 → 『Node Pool』 → 『Node Pool』. On the 『App Load Balancing』 menu, click Node Pool, select 『Node Pool』 in the node pool window on the right, and click New.

The page is shown in the figure below:

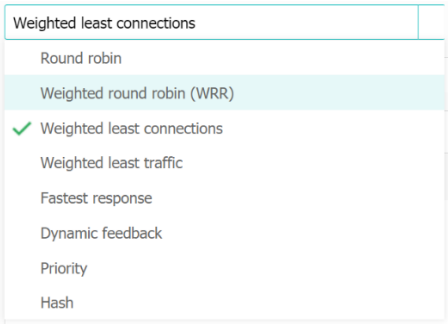


『Name』, 『Health Status』, 『Description』, 『Selection Policy』, 『Nodes』 and 『Operation』 are displayed under 『Node Pool』, and a Nodes button is under the 『Operation』 column to view and edit the node information of the node pool, and also a Copy button is there to quickly copy and create the same node pool. The Delete button is used to delete a single entry. The 『Node Pool』 defined here can be used for the configuration of 『Scheduling Policy』 and 『Virtual Service』.

Click the New button, as shown in the following figure: Generally, Name, Node Scheduling, Node, Health Monitor, and Session Persistence need to be set;



『Node Scheduling』 configures node selection policy type, including [Round robin], [Weighted round robin], [Weighted least connections], [Weighted least traffic], [Fast response], [Dynamic feedback], [Priority] and [Hash], among which, the dynamic feedback type needs to be used in conjunction with the node pool that is configured with the SNMP health check.



For『Node Scheduling』, [Round robin] indicates that valid nodes are alternately returned; [Weighted round robin] indicates that valid nodes are returned according to the proportion of node weight value, which is configured in『Weight』for『Node』; [Weighted least connections] indicates valid nodes are returned according to the weighted calculation results (number of connections/weights) of the number of current node connections, which is configured in『Weight』for『Node』; [Fast response] indicates that valid nodes with the shortest detection time are returned by configuring the detection response time; [Dynamic feedback] indicates that valid nodes are returned according to the weighted calculation results by dynamically changing the weights of 『CPU Weight』,『Memory Weight』, and『Disk Weight』, which correspond to SNMP type of the monitoring results of『SNMP Health Monitor』. It gives more possibility to choose the nodes with less loading, while it gives less possibility to choose the nodes with more loading, so as to make loading of all nodes balanced; [Priority] indicates nodes with a high priority will be scheduled first, and the nodes with a lower priority are scheduled only when the nodes with a higher priority are unavailable; [Hash] indicates that different keywords are averagely scheduled to each node in the node pool as much as possible, and access of the same keyword is scheduled to the same node by obtaining the hash value through hash calculation according to hash keywords (such as URI, HOST, source IP and source PORT).

『Node』configures the scheduling node information, including IP (the IP address of the node for scheduling, which can be a single IP or an IP segment, supporting the mixed use of IPv4 and IPv6 addresses. The device will automatically identify the IP type and the health check method if using IPv4 and IPv6 addresses in a mixed way), port (the opening service port of the node and 0 representing an opening port that inherits the virtual service by default), and weight (range: 1-100, only applicable to Weighted Round Robin, Weighted Least Connections, and Weighted Least Traffic). After configuring, you need to click the Add button to add the node to the scheduling of the node pool.

『Select Nodes』 configures and modifies node information just added. You can edit or delete a piece of information, or check multiple nodes, and then click the Delete button above to delete node information in batches.

『Health Monitor』 checks the service status of the nodes in the node pool. You can select or create the required health checks and can configure multiple (0-5) health checks to check the nodes at the same time. Click the << button to move the selected health checks to the checklist on the left, and the health states of the nodes can be obtained through the selected health checks. If you wish to disable the selected health check, select the health check to be disabled, click > > button to move the selected health check rightward. The newly created health check by clicking the New button will be automatically added to the health checklist. By default, the node health monitor inherits the health check status of the node pool. If a health check is configured separately for the nodes, the health check results of the nodes are preferred.

『Monitor Matching』 configures the valid rules for a node to pass the health check. You can select [At Least] or [All]. If [At Least] is selected, N needs to be configured. The node is valid only when it passes N health check(s). If [All] is selected, the node is valid only when it passes all the health checks.

『Recovery Interval』configures the interval from the time when the node recovers to the start of providing services. After the ADC passes the health check of the device, it will not send client requests to the server within the configured time to prevent nodes with unstable health status from being added to the scheduling. The time range is 0-300 (unit: seconds). 0 means no recovery protection is enabled.

『Warming-up Period』 configures the period for the node to slowly carry services, so as to prevent all requests from being processed immediately after the node recovers, resulting in node crashes with new and concurrent requests. After the node recovers, gradually increase the number of requests to the maximum value within the warming-up period, with a range of 0-300 (unit: seconds). 0 means no warming-up protection is enabled.

『Session Persistence』 configures the session persistence of the node pool. According to the policy, the corresponding traffic is always kept on the corresponding node for a certain period of time to ensure that the application can be normally accessed. You can select the existing session persistence modes from the drop-down list or click the New button to create a new session persistence mode. You can also select to call the mode after configuration in 『App Load Balancing』 → 『Node Pool』 → 『Session Persistence』 .

『Standby Session Persistence』 configures the standby session persistence of the node pool. When the active session persistence fails, the standby session persistence will be used. Firstly, if the preferred session persistence is the source IP session persistence, it is not allowed to configure the standby session persistence; secondly, the preferred [Cookie] session persistence only supports the configuration of [HTTP Response Passive/SouceIP] standby session persistence; thirdly, the preferred [HTTP Passive/RADIUS/SSL SessionID] session persistence only supports the configuration of [SouceIP] standby session persistence. See the "Precautions" section for detailed information.

『Busy Node』 configures the scheduling policy for new connections when the node exceeds the upper limit of connections or the upper limit of requests. You can select [Forced Scheduling], [Wait in Queue], or [Scheduling Failure]. The [Forced Scheduling] policy ignores the busy status of the node, and still schedules according to the [Node Scheduling] until the health check shows that the node is offline. The [Wait in Queue] policy caches the busy connections and puts them into the queue. For which, [Queue Length] (the upper limit of new connections to be cached) and [Timeout] (the upper limit of the duration from the time when a connection is cached to the time when the connection is discarded) need to be configured. The queue length ranges from 1 to 100,000, and the timeout range from 1 to 60 seconds. The [Scheduling Failure] strategy distributes new connections to other nodes that are not busy according to [Node Scheduling] when the node is busy.

『Connection Count Method』 configures the statistics method of connections. You can select [Count All Statuses] or [Count ESTABLISHED Status Connections]. Count All Statuses will count

the number of TCP connections in all statuses. Count ESTABLISHED Status Connections will only count the number of connections in the "established" status (the TCP connections are successfully established). Statistical data is displayed in 『Status』.

『Scheduling By Connection』: Node pool supports scheduling by connection. After enabling, the requests can be scheduled to corresponding nodes according to the original connections.

After configuring the corresponding 『Node Pool』, click Save to complete the configuration or click Cancel to cancel the configuration.

**Attention:** If the preferred session persistence is realized according to the data in request direction, the standby session persistence can only be the session persistence realized according to the data in request direction or the [Source IP Session Persistence]. If the preferred session persistence is realized according to the data in response direction, the standby session persistence can only be the session persistence realized according to the data in response direction or the [Source IP Session Persistence]. The session persistence types based on the data in response direction include [Cookie Session Persistence] and [HTTP Response Passive] session persistence. (If the standby session persistence is in request direction, the timeout is the same as that of the preferred session persistence. If the standby session persistence is in response direction, the timeout is the standby timeout.)

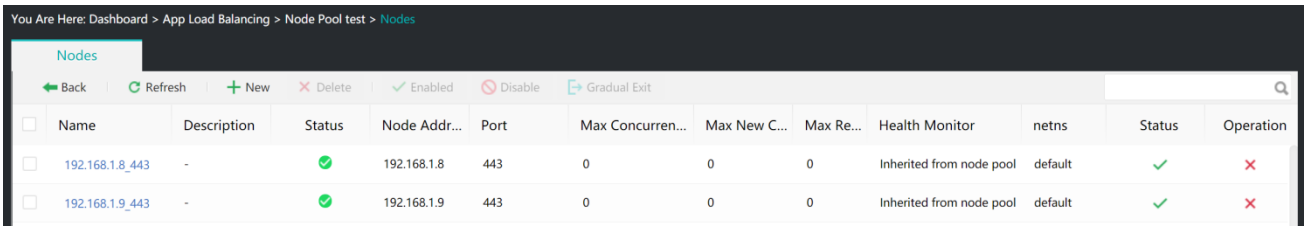
7.1.4.2 View and Edit Node List

【Operation Scenarios】

After the node pool is created, you may need to modify the nodes to be scheduled due to configuration error or demand change. However, the nodes cannot be edited in the node pool after creating the node pool. It is necessary to click the Nodes button in the [Operation] option behind the corresponding node pool on the node pool adding page to enter the node list for editing.

【Operation Procedure】

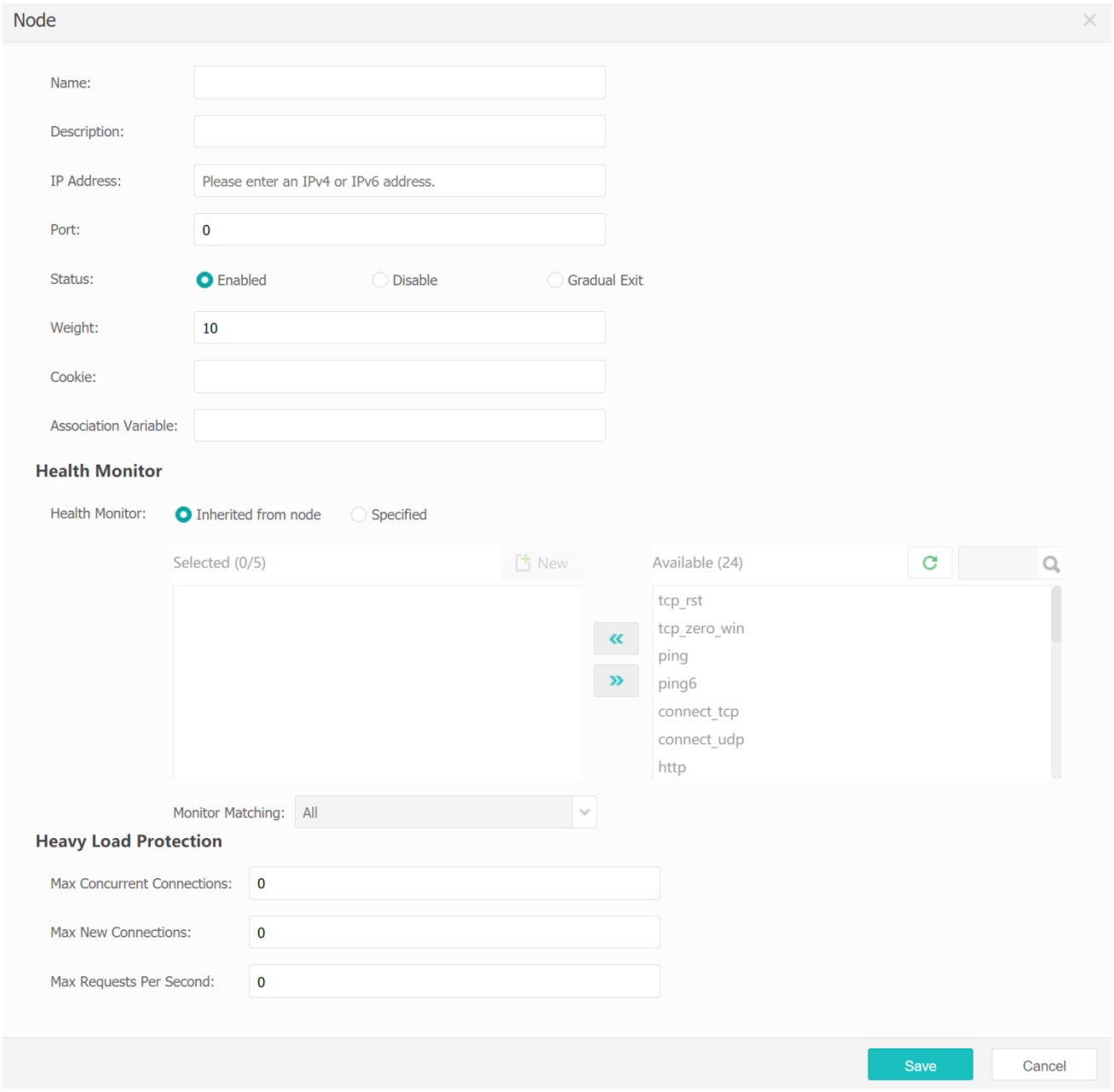
『App Load Balancing』→『Node Pool』→『Node Pool』→ Nodes. The interface is as follows:



『Name』, 『Node Address』, 『Status』, 『Description』, 『Max Concurrent Conns』, 『Max New Conns』, 『Max Requests』, 『Health Monitor』, 『Netns』, 『Status』 are displayed under 『Node Pool』, and a Delete button is under the『Operation』column for deleting a single entry. The『Nodes』 defined here can be used for the configuration of the corresponding 『Node Pool』.

Click the Back button to return to the 『Node Pool』 configuration page. Click the Refresh button to refresh and get the latest 『Nodes』 configuration. Click the New button to add 『Nodes』 under the node pool. Click the Delete button to delete the 『Nodes』 under the node pool in batches. Click the Enabled button to make the 『Nodes』 configuration take effect. Click the Disable and Gradual Exit buttons to make the 『Nodes』 configuration invalid. See the node configuration instructions for details.

Click the New button, as shown in the following figure:



『Name』 configures the node name. You can use a character string that is convenient for memory and recognition. The name format automatically generated for the added nodes on the node pool configuration page is [IP_Port].

『IP Address』 configures the IP address of the node.

『Port』 configures the opening service port of the node. 0 represents an opening port that inherits the virtual service by default.

『Status』 configures whether the node is involved in scheduling. You can select [Enabled], [Disable], or [Gradual Exit]. The disabled node will maintain the connections of existing activities, but not accept new connections. [Gradual Exit] will maintain the existing connections and session persistence, but not schedule new requests until the node completely exits, so as to ensure that the running services will not be interrupted.

『Weight』 configures the weight of the node, which is used for the weighted operation of node selection strategy, and is only applicable to the node selection strategies of Weighted Round Robin, Weighted Least Connections and Weighted Least Traffic, with a range of 1-100.

『Cookie』 configures the Cookie value pre-assigned to the node for Cookie-related scenarios such as Cookie session persistence. A Cookie value will be automatically assigned to the added node on the node pool configuration page. For the node added on the node page, it needs to be manually configured, with a value range of 10,000,000-99,999,999.

『Association Variable』 configures that when rewriting the HTTP header, HTTP is rewritten as the built-in variable.

『Health Monitor』 configures the node health check method. You can select to inherit the node pool configuration or configure it independently. Inheriting node pool configuration indicates that the health check configured in the node pool is used. Configuring it independently indicates that the health check of the node is configured separately. The latter one is mainly for some nodes that may need separate health checks. The node added on the node pool configuration page uses the inherited node pool configuration by default.

『Monitor Matching』 configures the valid rules for a node to pass the health check. You can select [At Least] or [All]. If [At Least] is selected, N needs to be configured. The node is valid only when it passes N health check(s). If [All] is selected, the node is valid only when it passes all the health checks.

『Max Concurrent Connections』configures the maximum connections of nodes, ranging from 0 to 100,000,000, and 0 means no restriction.

『Max New Connections』 configures the maximum new connections of nodes in 1 second, ranging from 0 to 100,000,000, and 0 means no restriction.

『Max Requests Per Second』 configures the maximum HTTP requests per second, ranging from 0 to 1,000,000, and 0 means no restriction.

After configuring the corresponding 『Nodes』 , click Save to complete the configuration or click Cancel to cancel the configuration.

7.1.5 IP Anycast

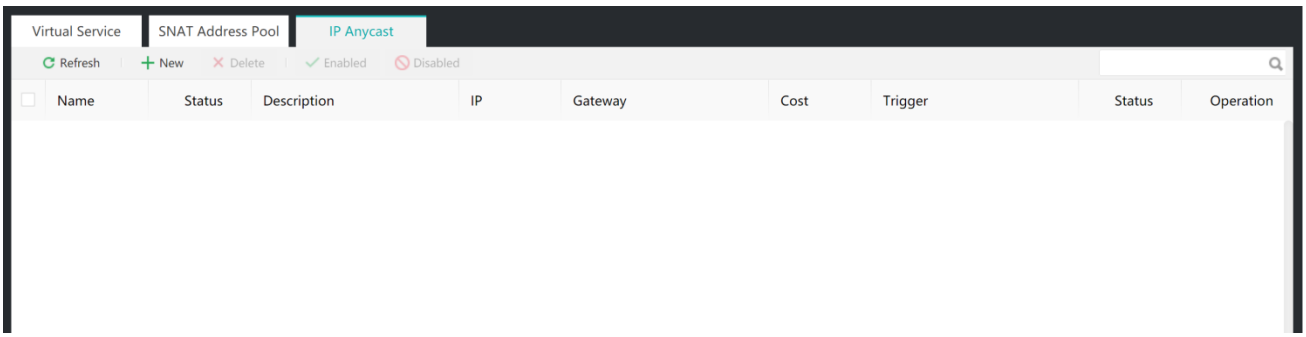
【Operation Scenarios】

It is used in RHI host routing injection scenarios based on the dynamic routing health status. It can publish the host routing information of the virtual service IP address to standard dynamic routing, such as OSPF or BGP, and integrate the virtual service IP and server health status with dynamic routing, realizing the solution of multi-site redundancy through routing.

【Operation Procedure】

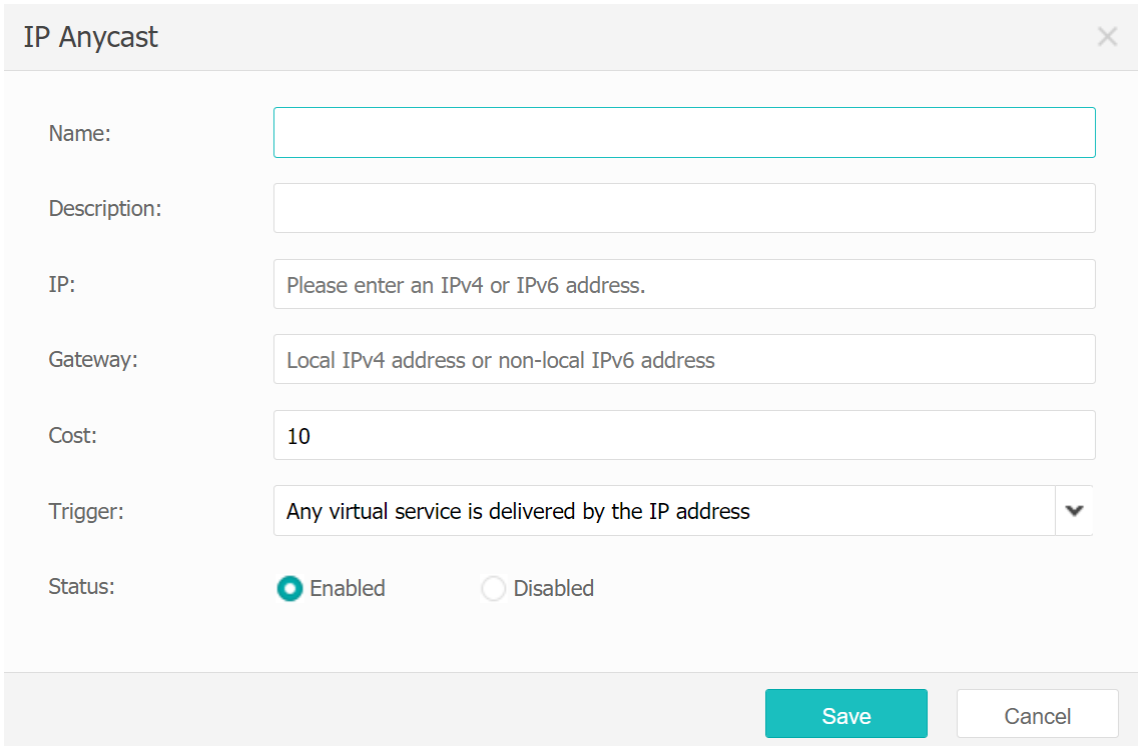
『App Load Balancing』→『Virtual Service』→『IP Anycast』. On the『App Load Balancing』menu, click Virtual Service, select『IP Anycast』in the virtual service window on the right, and click New.

The page is shown in the figure below:



『Name』, 『Status』, 『Description』, 『IP』, 『Gateway』, 『Cost』, 『Trigger』, 『Status』 and 『Operation』are displayed under『IP Anycast』, and a Delete button is under the『Operation』 column for deleting a single entry.

Click the New button, as shown in the following figure:



『IP』 configures the IP address of the virtual service, which is to be injected into dynamic routing.

『Gateway』 configures the next-hop port IP of the virtual service IP, which is to be injected into dynamic routing. The IPv4 address is a local one, while the IPv6 address is a non-local one.

『Cost』 configures the cost value of the virtual service IP that is to be injected into dynamic routing.

『Trigger』 configures the conditions for whether the IP of the virtual service is injected into dynamic routing. There are three methods to trigger broadcast: 1. broadcast when all virtual services published by the IP are available; 2. broadcast when any virtual service published by the IP is available (default); 3. always broadcast.

『Status』 configures whether the IP Anycast is valid. If it is enabled, the IP Anycast configuration is valid. If it is disabled, the IP Anycast configuration is invalid.

7.1.6 SNAT Address Pool

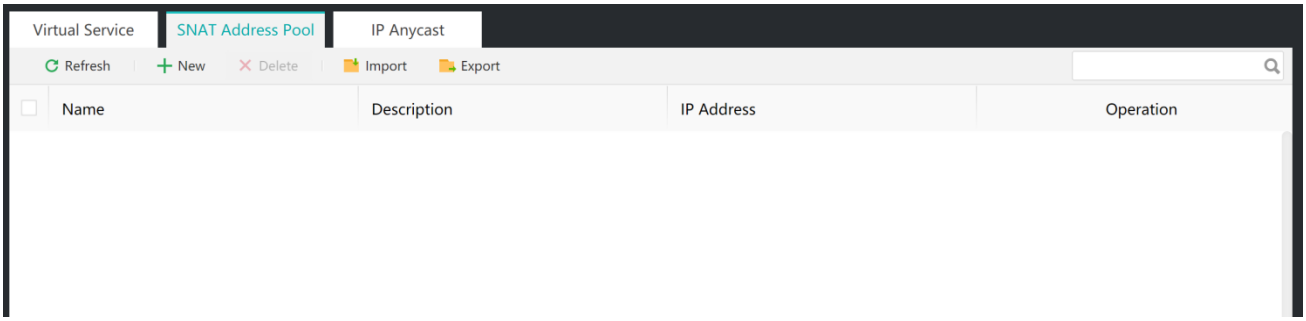
【Operation Scenarios】

To ensure that the traffic of ADC is not intercepted due to security and other requirements after the virtual service starts SNAT policy, you need to specify the SNAT address used by AD, and you can implement it by configuring the 『SNAT Address Pool』.

【Operation Procedure】

『App Load Balancing』 → 『Virtual Service』 → 『SNAT Address Pool』. On the 『App Load Balancing』 menu, click Virtual Service, select 『SNAT Address Pool』 in the virtual service window on the right, and click New.

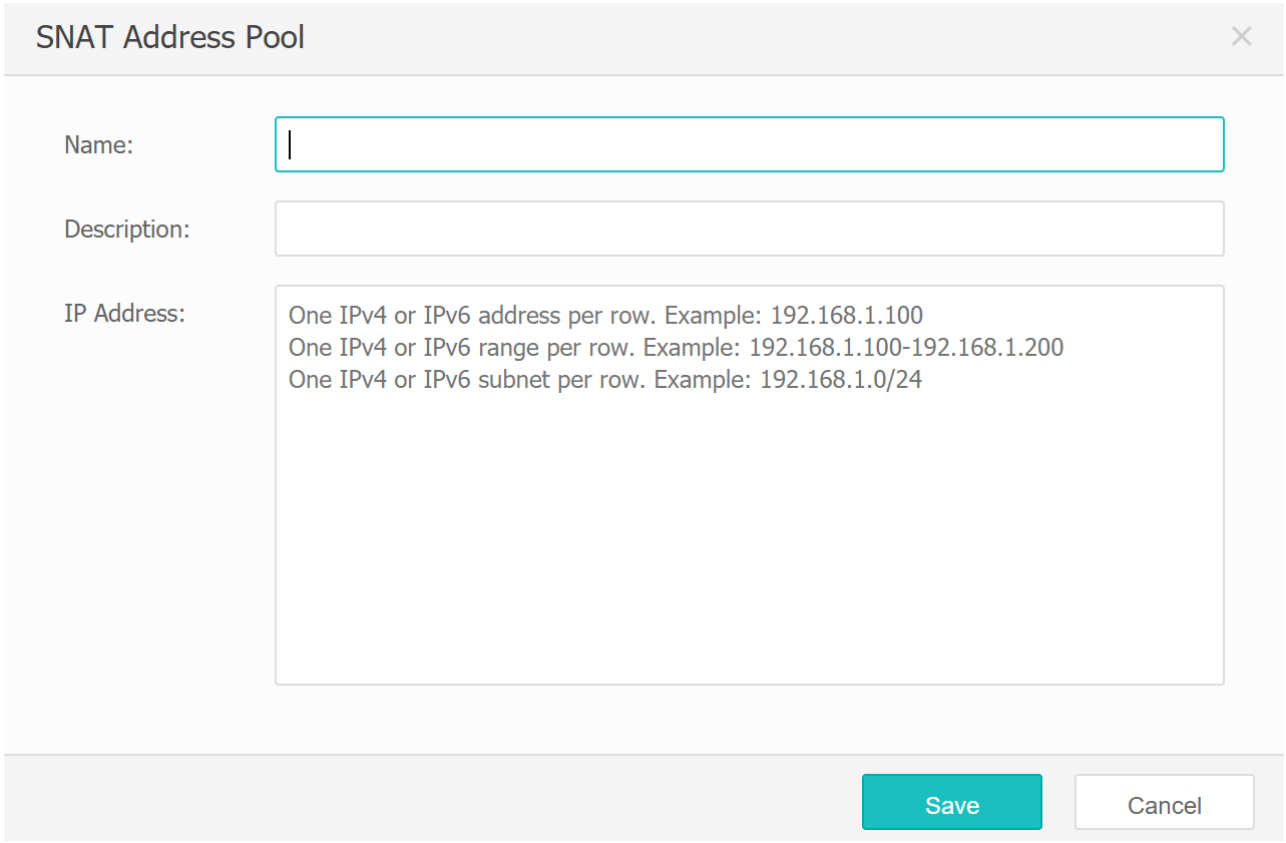
The page is shown in the figure below:



『Name』, 『Description』, 『IP Address』 and 『Operation』 are displayed under 『SNAT Address Pool』, and a Delete button is under the 『Operation』 column for deleting a single entry. The 『NAT Address Pool』 defined here can be used for the configuration of 『Virtual Service』.

The Import and Export buttons are used to import the configurations of『SNAT Address Pool』 in batches and backup the configurations.

Click the New button, as shown in the following figure:



『IP Address』 configures the address for SNAT, supports the configuration of a single IP address, IP address range, or subnet, and supports IPv4/IPv6 address. Each address should be separated by row.

7.1.7 SSL Policy

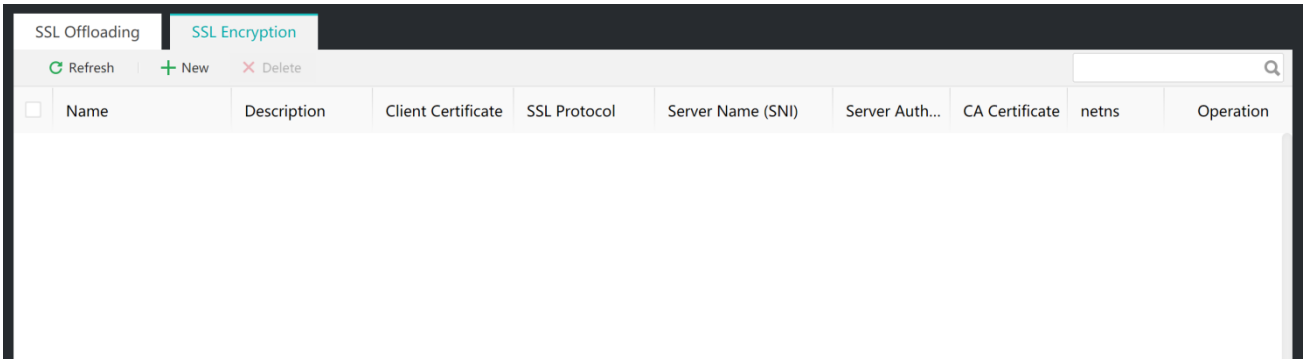
【Operation Scenarios】

To ensure the intranet data security after SSL Offloading or ensure that the agent can access the encrypted SSL application, you can configure 『SSL Encryption』 to encrypt the traffic accessing the virtual service before communicating with the node.

【Operation Procedure】

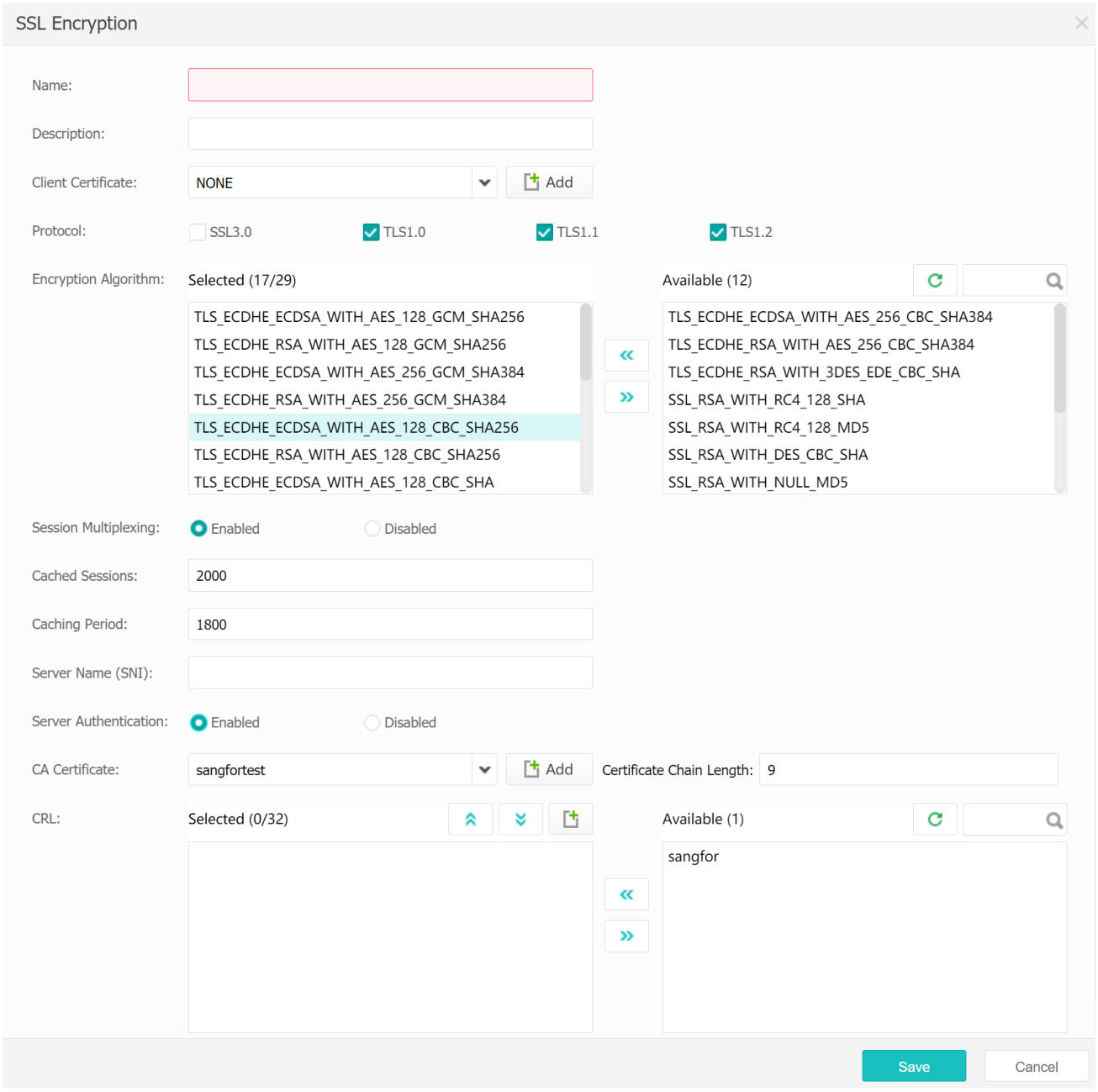
『App Load Balancing』→『SSL Policy』→『SSL Encryption』. On the 『App Load Balancing』 menu, click SSL Policy, and select 『SSL Encryption』 in the SSL policy window on the right

The page is shown in the figure below:



『Name』, 『Description』, 『Client Certificate』, 『SSL Protocol』, 『Server Name (SNI)』, 『Server Authentication』, 『CA Certificate』 and 『Operation』 are displayed under 『SSL Encryption』. In the 『Operation』 column, the Copy button is used to quickly copy and create the same SSL protection policy, and the Delete button is used to delete a single entry. The 『SSL Encryption』 defined here can be used for the configuration of 『Virtual Service』.

Click the New button, as shown in the following figure:



『Client Certificate』 configures the client certificate to be used. The client can use ECDSA commercial secret certificate or RSA commercial secret certificate. If the server does not enable bidirectional authentication, there is no need to configure it.

『Protocol』 configures the SSL protocol version used for SSL communication with nodes.

『Encryption Algorithm』 configures the encryption algorithm used in SSL communication. The client certificate type is different, and the corresponding encryption algorithm can be selected.

『Session Multiplexing』 configures whether to enable SSL session multiplex.

[Cached Sessions] configures the number of cached sessions. The default is 2,000, ranging from 100 to 5,000.

[Caching Period] configures the timeout time of the cache session. The default time is 1,800 seconds, ranging from 10 to 86,400.

『Server Name (SNI)』 configures the server domain name.

『Server Authentication』 configures whether to enable server authentication. [Disabled] will not verify the server's certificate. For [Enabled], communication will only be conducted when the server's certificate is trusted. It is disabled by default.

『CA Certificate』 configures the root certificate of selecting server authentication. CA certificate can be configured through 『Objects』 → 『Certificates』 → 『CA Certificate』 .

『Certificate Chain Length』 configures the maximum number of certificates traversed by the certificate chain of the server.

『CRL』 configures the selected certificate revocation list which can be configured through 『Objects』 → 『Certificates』 → 『CRL』 .

7.1.8 SSL Offloading

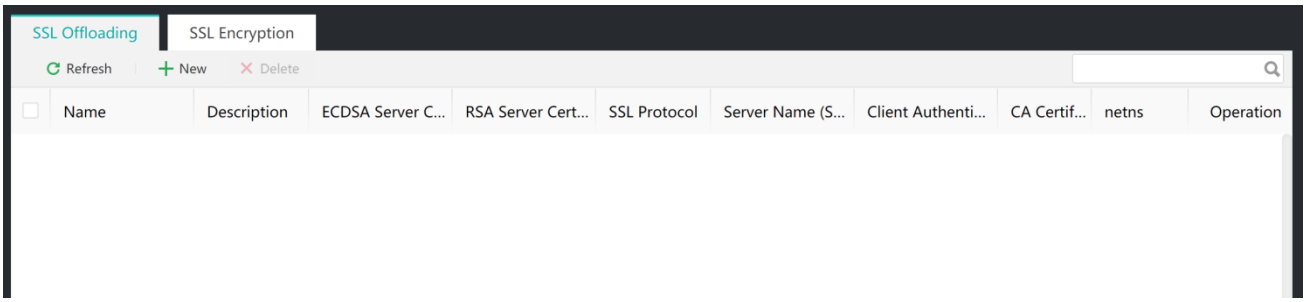
【Operation Scenarios】

In order to directly upgrade HTTP, SMTP, LDAP and other applications to SSL encrypted HTTPS, SMTP_SSL and LDAPS without modifying the server application or in order to reduce the load on the server of unloading the certificate and centrally manage the SSL certificate, you can configure 『SSL Offloading』 to decrypt the traffic accessing the virtual service, so that the client needs to use SSL encryption application for communication.

【Operation Procedure】

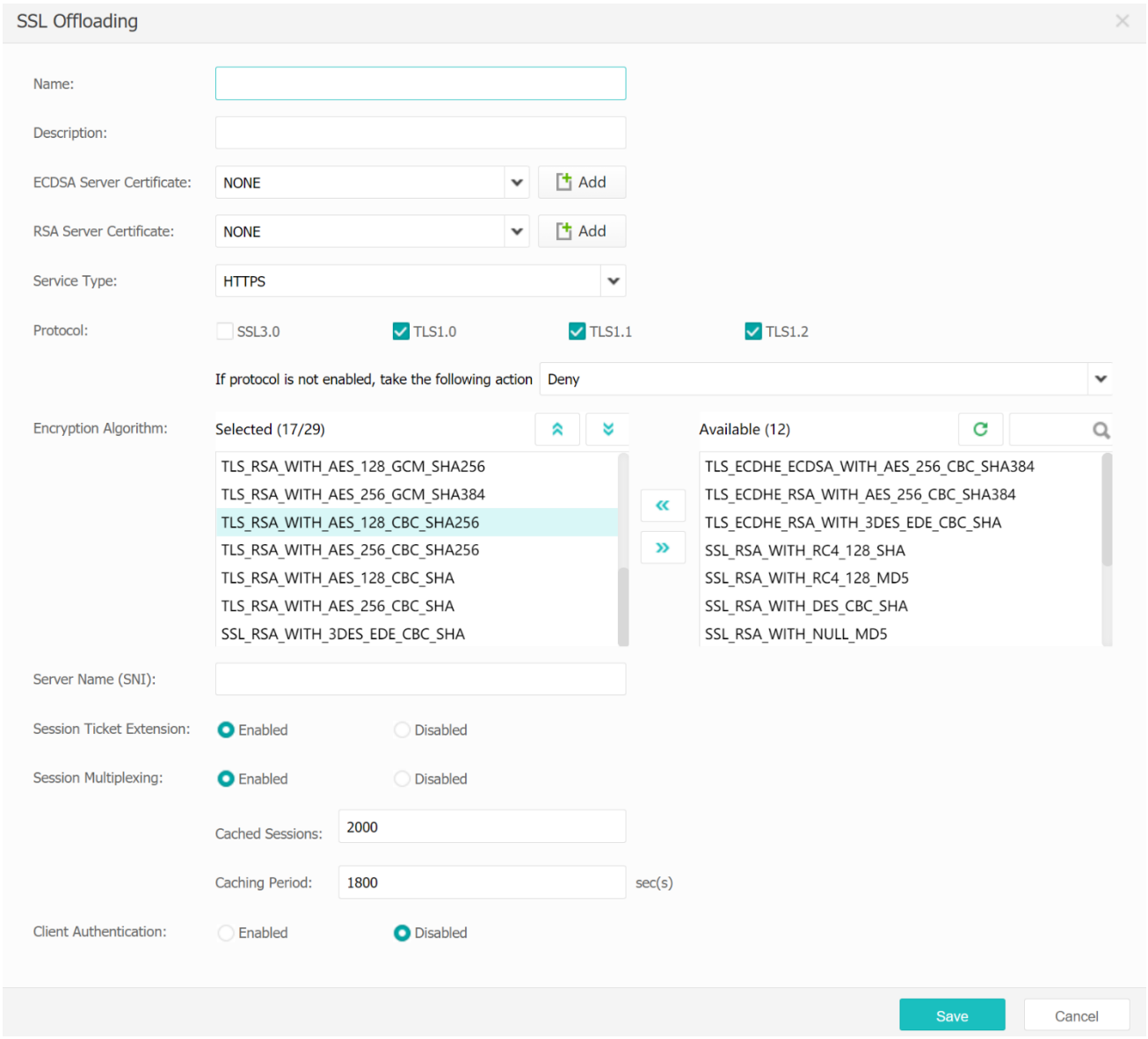
『App Load Balancing』 → 『SSL Policy』 → 『SSL Offloading』. On the 『Load Balancing』 menu, click SSL Policy. In the SSL policy window on the right, select 『SSL Decryption Policy』 and click New.

The page is shown in the figure below:



Under 『SSL Offloading』, the 『Name』, 『Description』, 『ECDSA Server Certificate』, 『RSA Server Certificate』,『SSL Protocol』,『Server Name (SNI)』,『Client Authentication』,『CA Certificate』 and 『Operation』 are displayed. In the 『Operation』 column, the Copy button is used to quickly copy and create the same SSL decryption policy, and the Delete button is used to delete a single entry. The 『SSL Offloading』 defined here can be used for the configuration of 『Virtual Service』.

Click the New button, as shown in the following figure:



『ECDSA Server Certificate』 configures the ECDSA business secret certificate used by the server when the negotiation is a business secret algorithm.

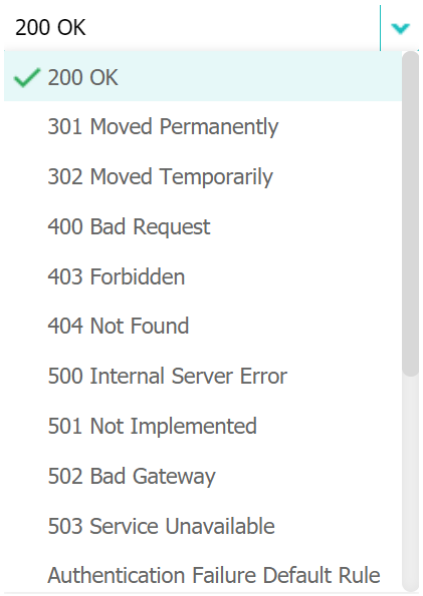
『RSA Server Certificate』 configures the RSA business secret certificate used by the server when the negotiation is a business secret algorithm.

『Service Type』 configures the type of virtual service, either HTTPS or SSL.

『Protocol』 configures the SSL protocol version used for SSL communication with clients.

[If protocol is not enabled, take the following action] configures the action when ADC does not support the protocol used by the client. If SSL is selected for 『Service Type』, it is rejected.

If HTTPS is selected for『Service Type』, you can choose to reject or respond to the custom content. The custom content can be configured through『 Objects』→『Custom Webpage』. The built-in content is as follows:



『Encryption Algorithm』 configures the encryption algorithm used in SSL communication. The server certificate type is different, and the corresponding encryption algorithm can be selected.

『Server Name (SNI)』 configures the server domain name.

『Session Ticket Extension』 configures whether to enable the session ticket extension and optimizes the SSL interaction process after it is enabled. SSL session ticket records encryption parameters and is used for subsequent requests to reduce the number of handshakes, reduce the high delay caused by repeated handshake requests so as to improve the efficiency of SSL handshakes.

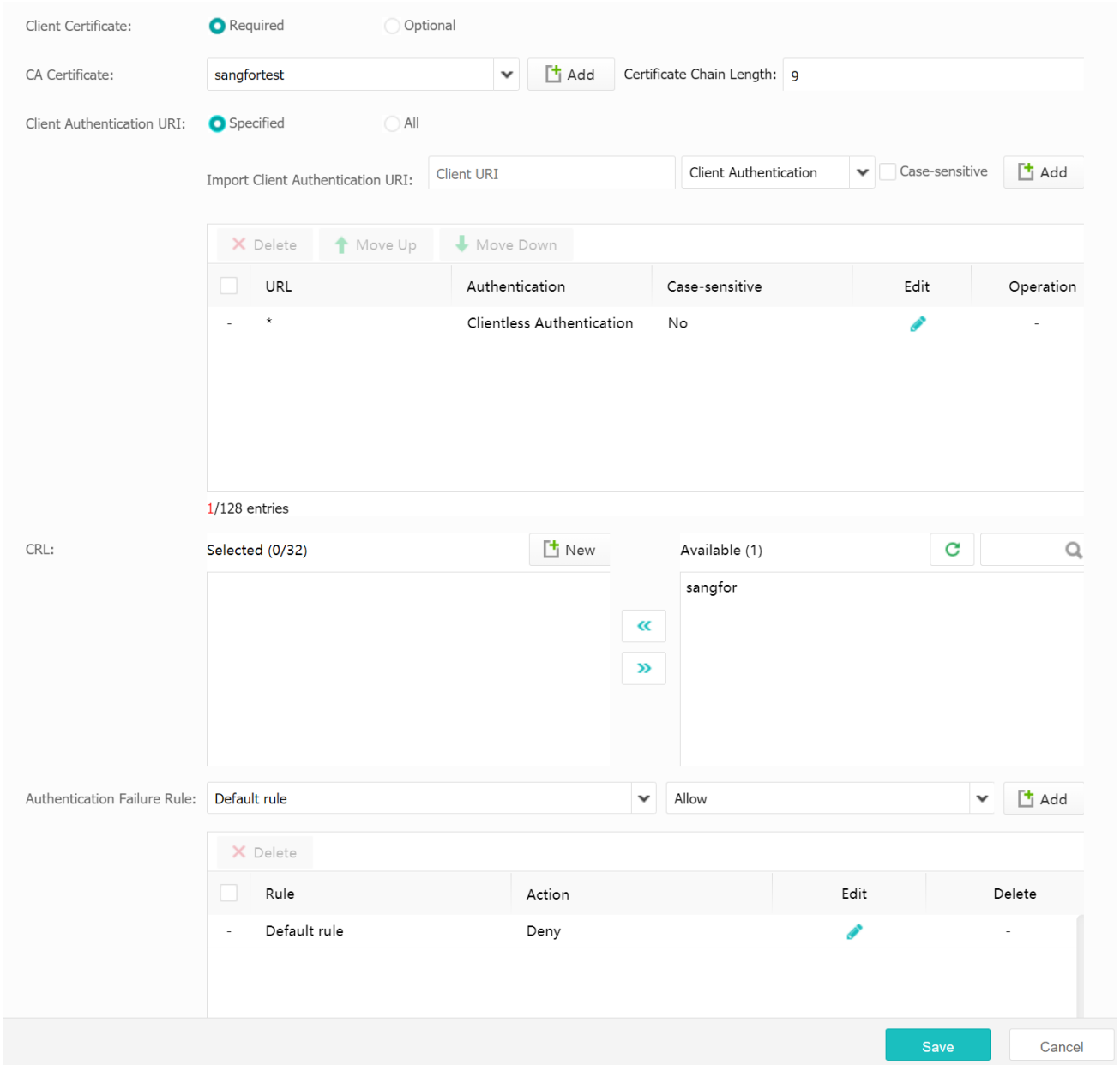
『Session Multiplexing』 configures whether to enable SSL session multiplex.

[Cached Sessions] configures the number of cached sessions. The default is 2,000, ranging from 100 to 5,000.

[Caching Period] configures the timeout time of the cache session. The default time is 1,800 seconds, ranging from 10 to 86,400.

『Client Authentication』configures whether to enable client authentication.『Disabled』only performs server authentication, that is, one-way authentication. 『Enabled』performs both server and client authentication, that is, two-way authentication. It is disabled by default.

After client authentication is enabled, the corresponding configuration is as follows:



『CA Certificate』configures the root certificate of selecting server authentication. CA certificate can be configured through『Objects』→『Certificates』→ 『CA Certificate』.

『Certificate Chain Length』 configures the maximum number of certificates traversed by the certificate chain of the server.

『Client Authentication URI』 configures whether to submit all URIs or specified URIs authenticated by client certificate. All URIs default, that is, all URIs need authentication. Fill in the specified URI to specify whether a URI needs client authentication. For example, /index.html supports wildcards ? and *. After selecting the specified URI, the default * means that all URIs do not need client authentication.

『CRL』 configures the selected certificate revocation list which can be configured through 『Objects』 → 『Certificates』 → 『CRL』 .

『Authentication Failure Rule』 configures actions after the client certificate authentication fails. The authentication failure rule is optional. The actions performed after the failure can be Allow, Reject, or Return the custom content.

7.1.9 TCP Policy

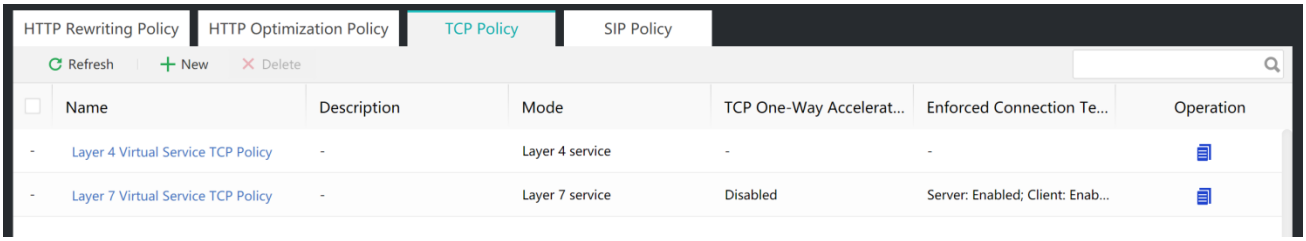
【Operation Scenarios】

When the client's application is a persistent connection application that needs to do app load balancing, the default 10-minute TCP timeout of ADC will cause the connection between the client and the server to be interrupted. When the node health check is abnormal, the client's connection will not be reset, resulting in the traffic that originally connected to the abnormal node always being in an abnormal state. When ADC has closed the connection and the server's connection waiting time has not been timed out, so that ADC may reuse the connection of the previous port to access the node, resulting in an abnormal connection. When the number of connections between the client and the node is too many, large server resources are consumed, etc. The above attributes related to TCP connection can be solved by configuring [TCP policy] to optimize TCP parameters.

【Operation Procedure】

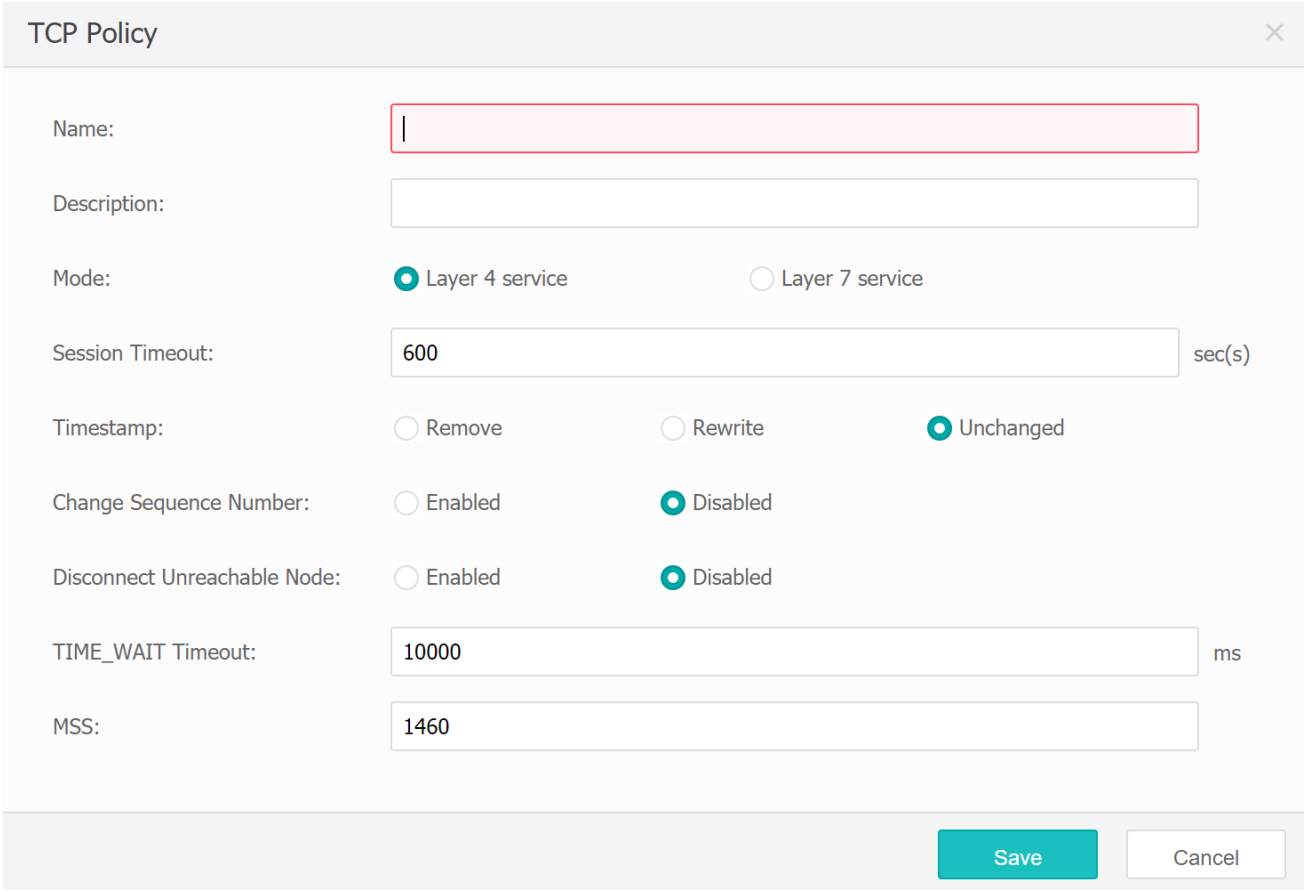
『App Load Balancing』→『Optimization』→『TCP Policy』. On the『App Load Balancing』menu, click Optimization. In the SSL policy window on the right, select『TCP Policy』and click New.

The page is shown in the figure below:



Under the『TCP Policy』, the『Name』,『Description』,『Mode』,『TCP One-Way Acceleration』,『Enforced Connection Termination』and『Operation』of the TCP policy are displayed. In the『Operation』column, the Copy button is used to quickly copy and create the same TCP policy, and the Delete button is used to delete a single entry. The『TCP Policy』defined here can be used for the configuration of『Virtual Service』.

Click the New button, as shown in the following figure:



『Selection Mode』can select the mode of TCP policy. Layer 4 is only applicable to TCP virtual service, and layer 7 is only applicable to TCP-l7, HTTP, SSL and HTTPS.

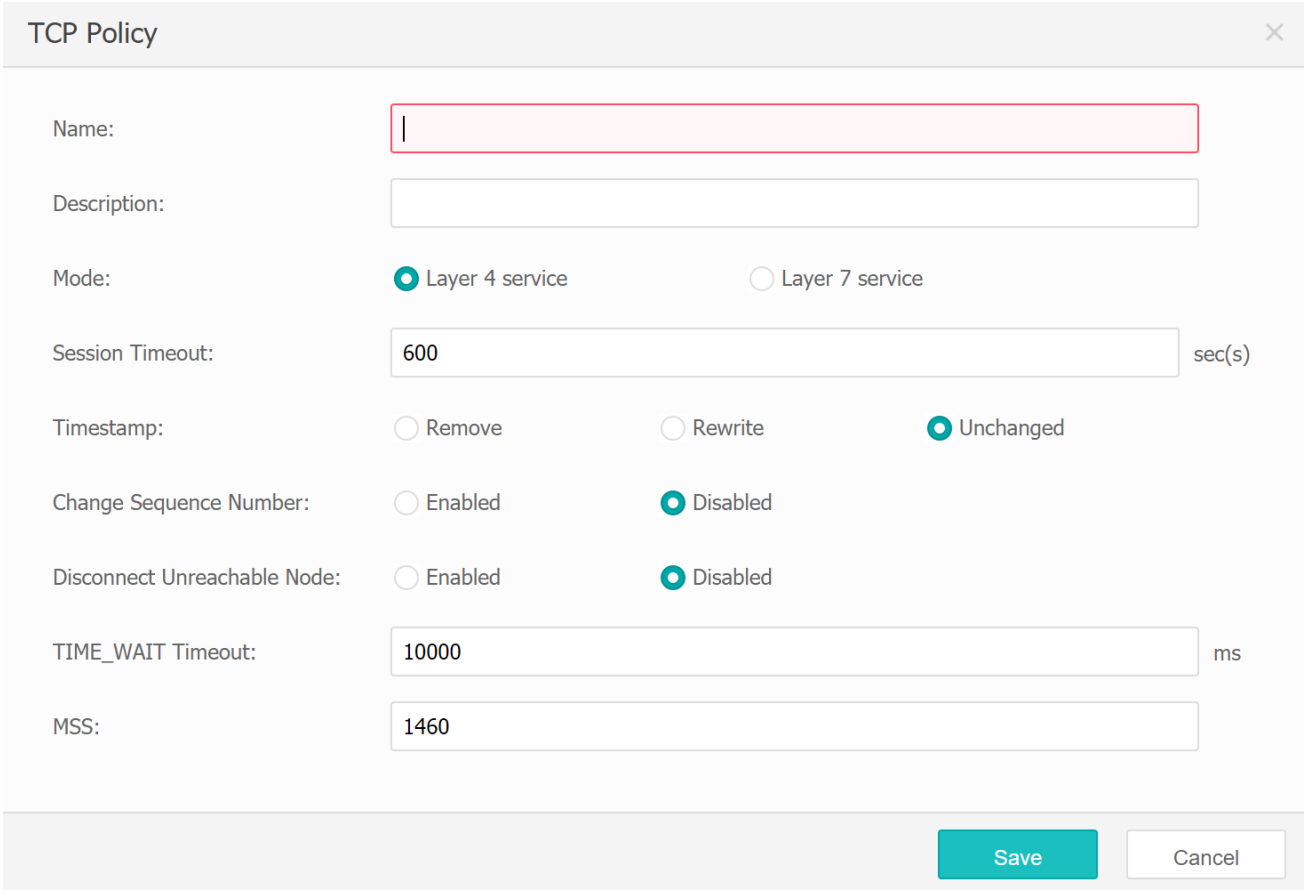
7.1.9.1 Layer 4 Virtual Service

【Operation Scenarios】

When using the [L4-tcp] virtual service as the app load balancing, we need to adjust the TCP parameters to ensure the normal operation of the service and configure this policy when optimizing the TCP parameters.

[Configuration Instruction]

Select the mode『Layer 4 service』and configure the TCP policy based on layer 4 virtual service to optimize the TCP parameters, as shown in the figure below:



『Session Timeout』configures the idle timeout of the layer 4 virtual service TCP. If there is no data transmission within the timeout, the connection will be cleared. If the service is using a persistent connection, the time should be increased, ranging from 1 to 604,800 (unit: seconds).

『Timestamp』 configures whether to modify the timestamp when TCP traffic passes through ADC. Removing or rewriting the timestamp in the handshake phase of layer 4 TCP virtual service is mainly used when the tcp_tw_recycle switch is turned on for nodes and SNAT is started. The timestamp of each client is different. Once a client disconnects, the server will discard the SYN packets of those clients of which timestamp is smaller than the connection timestamp, resulting in service exceptions. It prevents the client from making two requests in the same connection longer than the server's timeout, resulting in the server actively closing the connection and changing the connection status to TIME_WAIT. When the second request comes, ADC cannot reuse this connection, leading to the failure to respond to the client's second request.

『Change Sequence Number』 configures the sequence number to modify the layer 4 TCP virtual service.

『Disconnect Unreachable Node』 configures whether to disconnect previous connections when a node fails. After it is enabled, it can close the client connection in time and schedule the client to other healthy nodes when it reconnects.

『TIME_WAIT Timeout』 configures the waiting time of the device after disconnection, so as to prevent reusing previous connections causing service exceptions.

『MSS』 configures the maximum message length to be sent.

7.1.9.2 Layer 7 Virtual Service

【Operation Scenarios】

When using TCP-L7, HTTP, SSL, HTTPS virtual service as the app load balancing, this policy should be configured if there is a need to adjust the TCP parameters to ensure the normal operation of the service and optimize the TCP parameters.

[Configuration Instruction]

Select the mode『Layer 7 service』and configure the TCP policy based on layer 7 virtual service to optimize the TCP parameters, as shown in the figure below:



『MSS』configures the maximum datagram length of TCP fragmentation. The value should be set according to the network conditions, ranging from 536 to 1,460.

『Syn Timeout』 configures the timeout of a new TCP connection. The default value of this parameter in the protocol stack is 75 seconds, which can be adjusted according to the network conditions. The range is 30 - 180 (seconds).

『Inactivity Timeout』 configures the inactive timeout of the TCP session of the layer 7 virtual service. In the timeout period, if there is no data transmission, the connection will be cleared. If the service uses a persistent connection, the time should be increased, ranging from 1 to 604,800 (seconds).

『TCP One-Way Acceleration』 configures whether to enable one-way acceleration to optimize TCP. Only when the authorization sequence number of TCP one-way acceleration is activated can TCP one-way acceleration be Enabled or Disabled. When there is network delay or serious packet loss, the effect of enabling TCP one-way acceleration is more significant.

『Enforced Connection Termination』 configures whether to send RST to close the connection with the client or the server after the client and the node close the connection four times, so that the client or the node can quickly release the connection and revoke resources without having to wait for 2MSL TIME_WAIT.

『TCP Connection Pool 』 configures whether to enable or disable the connection multiplexing function. After it is enabled, a large number of client connections can be summarized and then a TCP connection can be used to schedule nodes to reduce the number of connections to nodes and the node pressure, and improve the virtual service performance.

『Connection Pool Size』 configures the maximum number of multiplexing client connections for a node, ranging from 1 to 64,000.

『Timeout』 configures the idle timeout of connections in this connection pool before they are released, ranging from 60 to 86,400 (seconds).

『Src IP Mask』configures the multiplexing source IP mask to match the TCP connection pool. During connection multiplexing, the source IP with the same network number can multiplex the

same connection. The network number of the source IP is obtained through the source IP and the source IP netmask. If it is configured as 24, all the traffic in 100.1.1.0/24 that can be multiplexed will use the same connection, and 100.1.2.0/24 traffic will be multiplexed as another connection, ranging from 0 - 32.

『Timestamp』 configures whether to modify the timestamp when TCP traffic passes through ADC. Removing or rewriting the timestamp in the handshake phase of layer 7 TCP virtual service is mainly used when the tcp_tw_recycle switch is turned on for nodes and SNAT is started. The timestamp of each client is different. Once a client disconnects, the server will discard the SYN packets of those clients of which timestamp is smaller than the connection timestamp, resulting in service exceptions. It prevents the client from making two requests in the same connection longer than the server's timeout, resulting in the server actively closing the connection and changing the connection status to TIME_WAIT. When the second request comes, ADC cannot reuse this connection, leading to the failure to respond to the client's second request.

『Reclaim resource (TIME_WAIT)』 configures whether to quickly reclaim the closed connection in TIME_WAIT. If it is enabled, the TCP will be linked in TIME_WAIT. If a new SYN connection request is received, a new connection will be created and the previous connection will be discarded.

『Disconnect Unreachable Node』 configures whether to disconnect previous connections when a node fails. After it is enabled, it can close the client connection in time and schedule the client to other healthy nodes when it reconnects.

『Delayed ACK』 configures responding to the ACK together after receiving 10 valid packets (if less than 10, receive all valid packets within a certain period of time) instead of responding to the ACK immediately when receiving TCP loaded packets. It is enabled by default.

When 『Support SACK』 is enabled, both sides of TCP will send a selection confirmation message to remind the peer device of the out-of-order packets that have been received, so that the

other side can skip the packets that have been selected for confirmation during retransmission, thus improving the network transmission efficiency.

『Support DSACK』 configuration only works when the sack option is turned on. When a duplicate packet is received, the receiver adds the serial number of the duplicate message to the response ACK, which is used to enable the receiver to accurately calculate network parameters such as RTT delay.

『TIME_WAIT Timeout』 configures the waiting time of the device after disconnection, so as to prevent reusing previous connections causing service exceptions.

『Max SYN Retransmissions』 configures the number of retransmissions when SYN + ACK responses cannot be received because SYN packets are lost. If the SYN is lost after a new TCP connection sends SYN, the sender will try to retransmit N (the configured N of this option) times and then give up the new connection and report the connection failure, ranging from 0 to 30 times.

『Max Segment Retransmission』 configures the maximum number of retransmission when TCP fragments cannot receive ACK response. If the sender's loaded packet does not receive the receiver's ACK response due to network or other problems, and there is still no response after (N) attempts, the link will be closed, ranging from 0 to 30 times.

『Window Scale』 configures the multiple of TCP window size expansion. Due to the limitation of TCP protocol, Initial Receive Window Size should be configured to 1,460 at least and 65,535 at most. This option can optimize the problem of the upper limitation. When this option is configured to N and the receive window is W, the total receive window is W * 2 ^ n with a range of 0 - 14 times.

『Initial Receive Window Size』 resets the window size of the TCP receiver, so that ADC can cache the packets sent from the peer device. The maximum number of packets sent by the peer device that can be cached by the TCP receiver ranges from 0 - 65,535.

『Retransmissions in Closing State』: If the FIN packet is lost when the TCP connection is closed, RST is sent to close this link after N attempts of retransmission, with a range of 0 - 30 times.

7.1.10 HTTP Optimization Policy

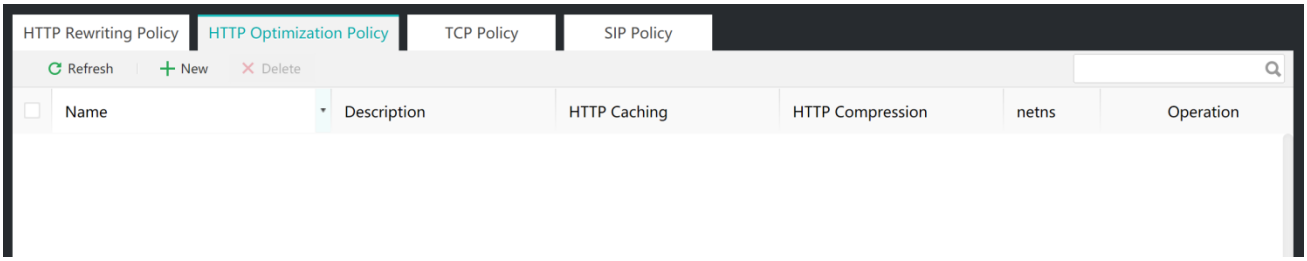
【Operation Scenarios】

In order to optimize the application using the HTTP protocol, reduce the pressure on the server and improve the access efficiency, you can configure 『HTTP Optimization Policy』 to optimize the traffic accessing the virtual service.

【Operation Procedure】

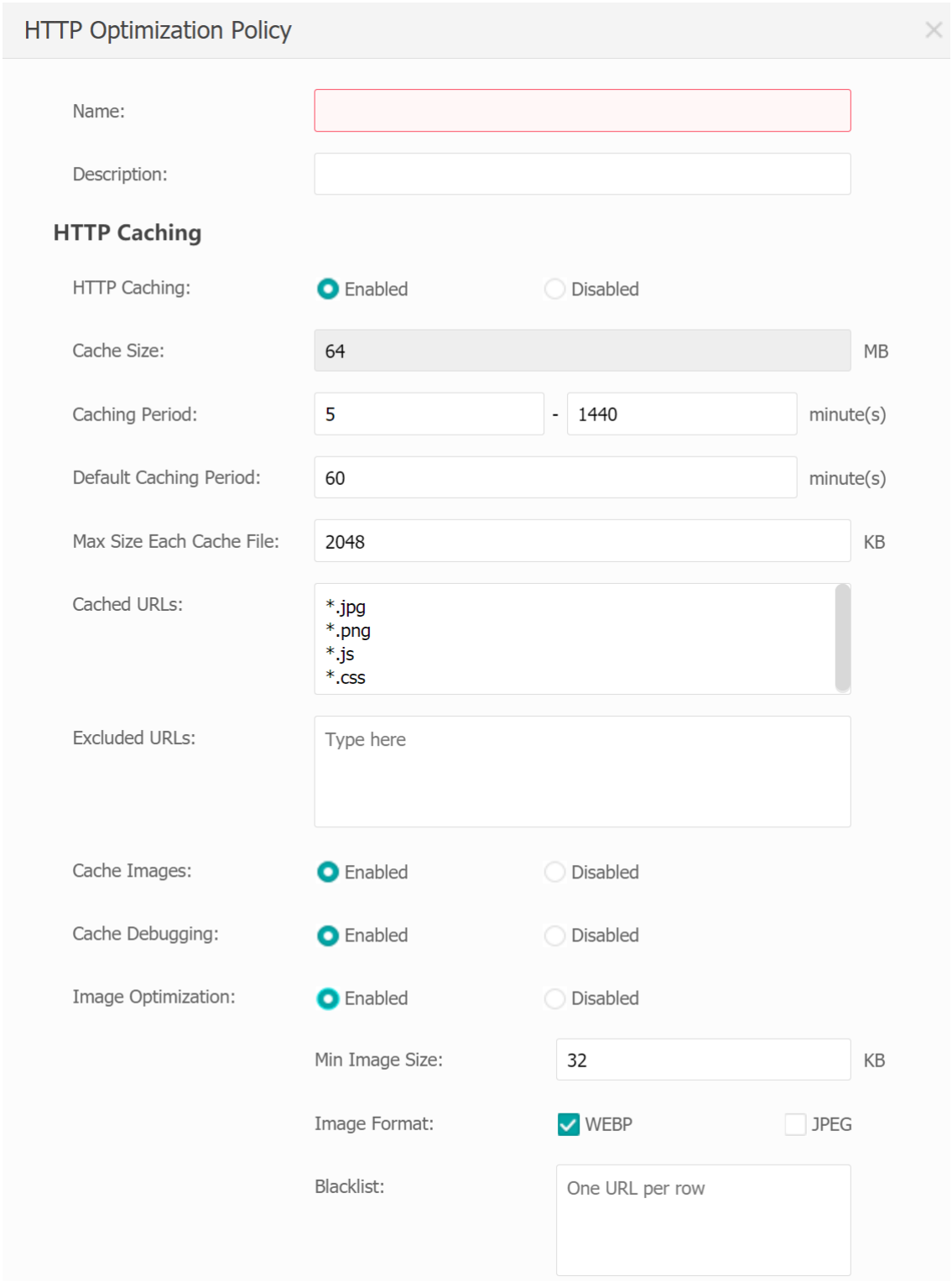
『App Load Balancing』 → 『Optimization』 → 『HTTP Optimization Policy』: On the 『App Load Balancing』 menu, click Optimization. In the optimization window on the right, select 『HTTP Optimization Policy』 and click Add.

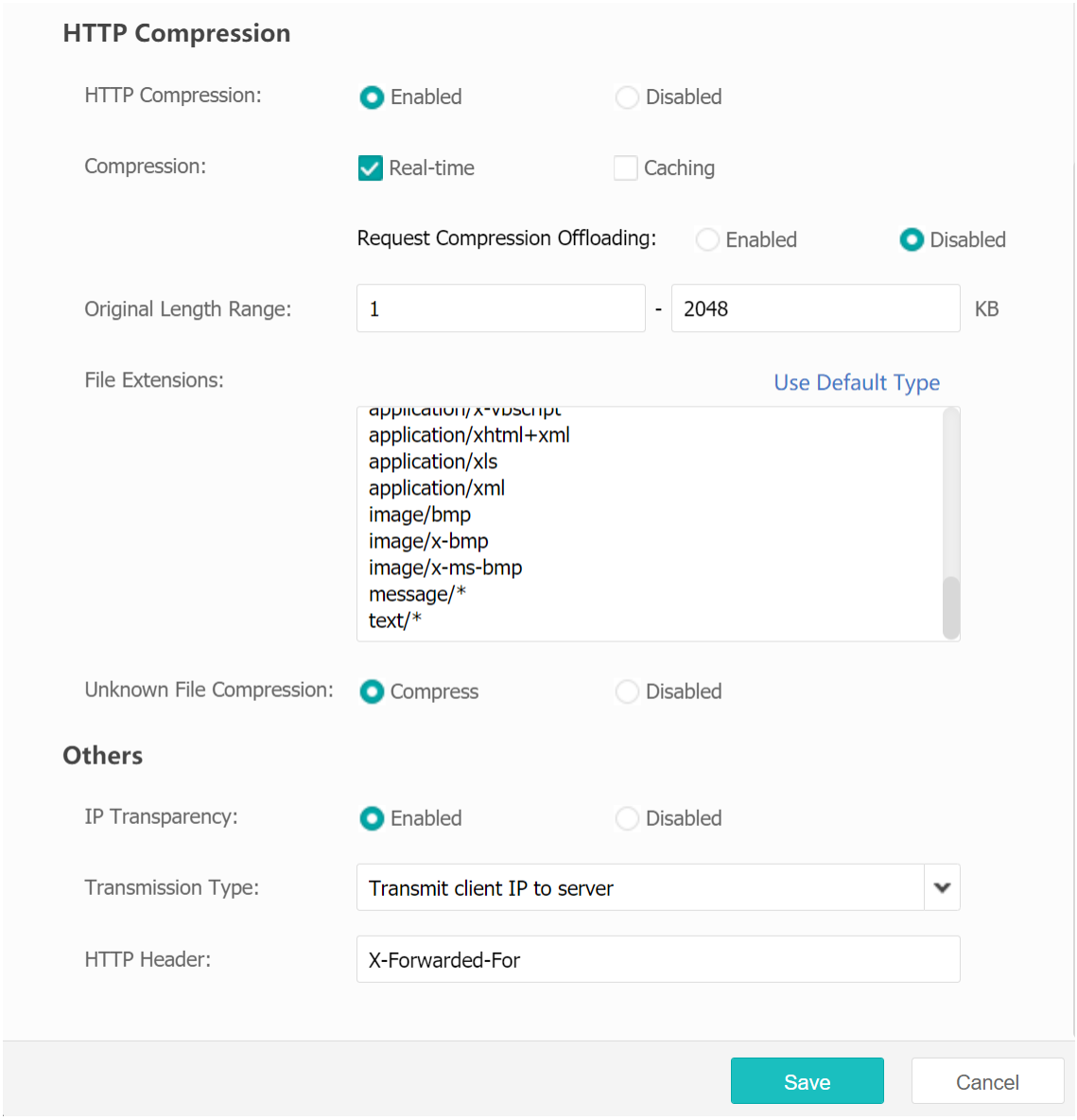
The page is shown in the figure below:



Under 『HTTP Optimization Policy』, the 『Name』, 『Description』, 『HTTP Caching』, 『HTTP Compression』 and 『Operation』 of the HTTP optimization policy are displayed. In the 『Operation』 column, the Copy button is used to quickly copy and create the same HTTP optimization policy, and the Delete button is used to delete a single entry. The『HTTP Optimization Policy』defined here can be used for the 『Virtual Service』 configuration part of the HTTP and HTTPS types.

Click the New button, as shown in the following figure:


HTTP Optimization Policy
Name:
Description:
HTTP Caching
HTTP Caching:
Enabled
Disabled
Cache Size:
64
MB
Caching Period:
5
-
1440
minute(s)
Default Caching Period:
60
minute(s)
Max Size Each Cache File:
2048
KB
Cached URLs:
*.jpg
*.png
*.js
*.css
Excluded URLs:
Type here
Cache Images:
Enabled
Disabled
Cache Debugging:
Enabled
Disabled
Image Optimization:
Enabled
Disabled
Min Image Size:
32
KB
Image Format:
WEBP
JPEG
Blacklist:
One URL per row



『HTTP Caching』 configures whether to enable the HTTP cache function. The device has a built-in HTTP cache, which can reduce the load of a large number of repeated requests on the server.

『Cache Size』 refers to the storage space that provides cache (cannot be modified).

『Caching Period』 configures the time range in which data in this cache is saved. If the cache time in the server response does not reach the lower limit of time, the cache will be retained according to the lower limit of time. If the cache time is within the range of caching period, the retention time will be saved according to the time in the server response and the data exceeding the upper limit of this range will be released.

『Default Caching Period』 configures the default caching period. When accessing the server, if the content of the server response does not contain the cache time or the cache timeout cannot be calculated according to the response content, the default caching period is used.

『Max Size Each Cache File』 configures the maximum storage space occupied by a single cache file. Files larger than this size will not be cached.

『Cached URLs』 configures the response of caching and matching this URL request list, supporting wildcard matching.

『Excluded URLs』 configures the failure to save the response that matches the URL request in this list. It is suitable for URL requests that contain real-time data, supporting wildcard matching.

『Cache Images』configures that images with private information are forced to be saved in the cache space, and the private information in the header includes Set-Cookie and Set-Cookie2.

『Cache Debugging』 configures whether to enable the cache debugging function. After it is enabled, you can turn on the debugging switch in the log to see the cache log information.

『Image Optimization』 configures whether the image is transmitted after being transcoded. Conversion of image format leads to traffic reduction so as to improve the page access speed. Image optimization source format supports BMP, PNG and JPEG, and PNG cannot be converted to JPEG. After this function is turned on, the image format will be converted to the WebP or JPEG format.

[Min Image Size] configures the minimum value of caching a single picture. Picture files smaller than this size will not be optimized.

[Image Format] automatically identifies the type according to the browser type. The target format of Chrome and Opera browsers is Webp, and other browsers are JPEG. Versions later than Chrome 9.0 and Opera 11.10 support Webp.

[Blacklist] keeps the original image format for the image file that matches the URL request in this list. It is suitable for image files that require high image resolution, supporting wildcard matching.

『HTTP Compression』 configures whether to compress the data in the HTTP cache and the background response data. This function requires additional computing resources and client support to make more efficient use of cache and bandwidth.

『Compression』 configures real-time compression or cache compression for HTTP. To use cache compression, HTTP cache must be enabled first. If the server itself has compressed HTTP after selecting real-time compression, the ADC can enable [Request Compression Offloading] to conduct compression by ADC instead of the server so as to reduce the load on the server.

『Original Length Range』configures the length range of compressed content. Content beyond this length range will not be compressed to prevent performance waste resulted from compressing small packets when smaller than the range and response timeout caused by compressing extra-large data when larger than the range.

『File Extensions』 compresses the files of the specified HTTP file type. You can choose the default type or customize it. The file type is determined by the "Content-type" field, and the HTTP responses matching this type list will be compressed.

『Unknown File Compression』 configures whether to compress unknown file types without the "Content-type" field in the compression response. Compression is enabled by default.

『IP Transparency』 configures whether to transmit the client's source IP transparently to the server. After it is enabled, the background server can obtain the client's real source address.

『Transmission Type』 selects the IP that transfers the client IP to the background server or uses the connection server carried by the HTTP header to connect to the server. The former option is applicable to the scenario where ADC has SNAT, and the latter is applicable to the scenario where the traffic diversion of the front end is carried out by CDN.

『HTTP Header』 configures the header name that carries IP or the extracted HTTP header name. The standard header name of the HTTP protocol cannot be used.

After configuring the corresponding『HTTP Optimization Policy』, click Save to complete the configuration or click Cancel to cancel the configuration.

7.1.11 HTTP Protection Policy

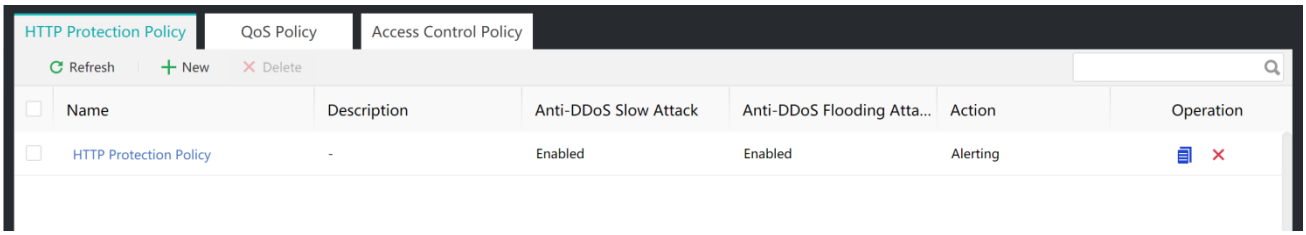
【Operation Scenarios】

In order to protect the application using the HTTP protocol, you can configure 『HTTP Protection Policy』 to control the traffic accessing the virtual service.

【Operation Procedure】

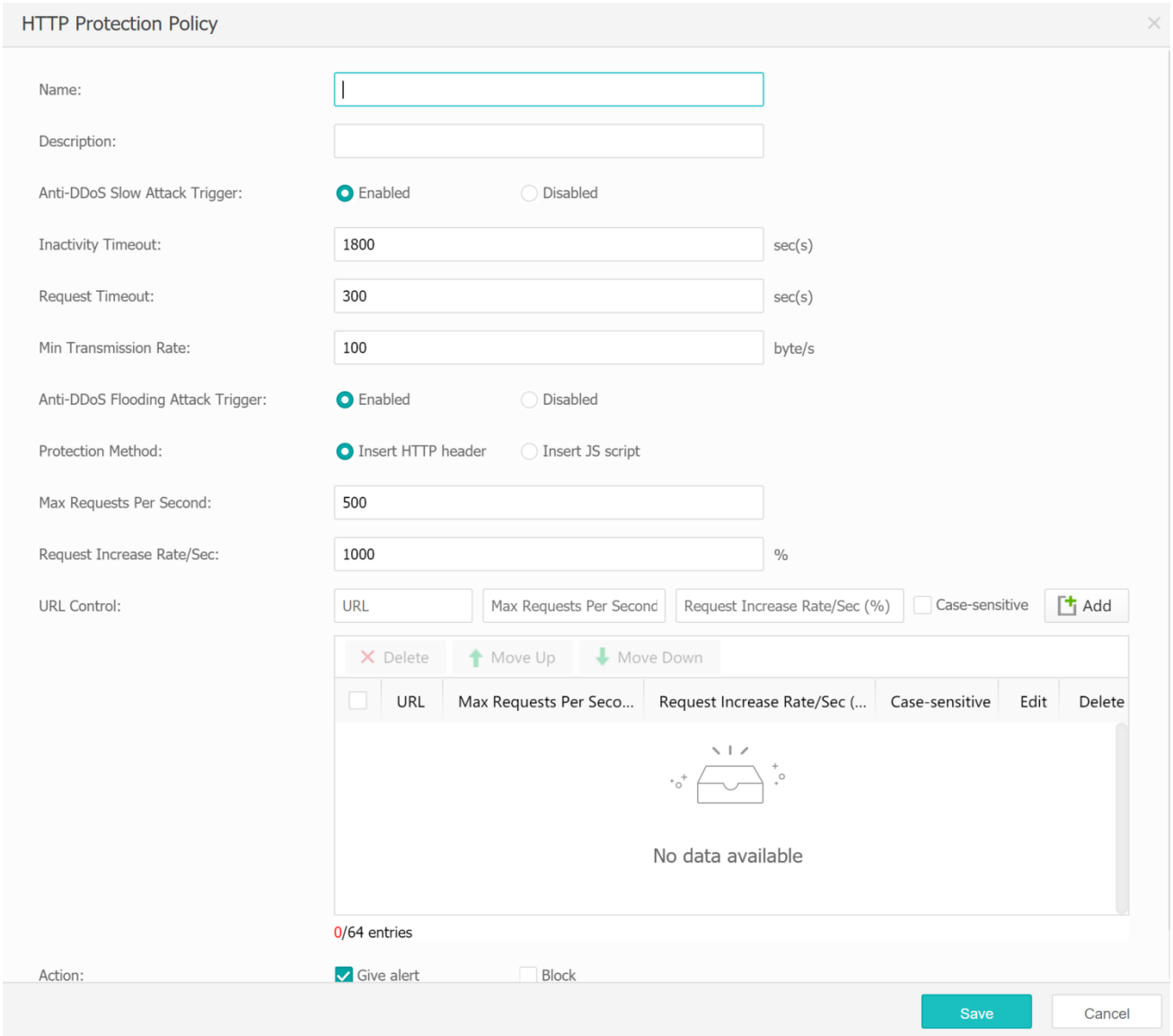
『App Load Balancing』→『Security Protection』→『HTTP Protection Policy』. On the『App Load Balancing』 menu, click Security Protection. In the security protection window on the right, select 『HTTP Protection Policy』 and click New.

The page is shown in the figure below:



Under『HTTP Protection Policy』, the『Name』,『Description』,『Anti-DDoS Slow Attack』,『Anti-DDoS Flooding Attack』,『Action』, and 『Operation』 of the HTTP protection policy are displayed. In the『Operation』column, the Copy button is used to quickly copy and create the same HTTP protection policy, and the Delete button is used to delete a single entry. The 『HTTP Protection Policy』defined here can be used for the『Virtual Service』configuration part of the HTTP and HTTPS types.

Click the New button, as shown in the following figure:



『Anti-DDoS Slow Attack』 configures whether to enable slow attack protection.

『Inactivity Timeout』configures the maximum idle time of a TCP connection. The connection without data transmission beyond this time will perform protection action. The default value is 1,800 (seconds), ranging from 1 to 65,535.

『Request Timeout』configures the maximum time for a TCP connection to receive a complete HTTP request. The TCP connection that has not finished sending the HTTP request beyond this time will perform the protection action. The default value is 300 (seconds), ranging from 1 to 65,535.

『Min Transmission Rate』configures the minimum rate at which HTTP requests are sent over TCP connections. TCP connections that are continuously below this rate for a period of time will perform protection actions. The default value is 100 (byte/s), ranging from 1 to 65,535.

『Anti-DDoS Flooding Attack』 configures whether to enable flooding attack protection.

『Protection Method』 configures the block mode used when 『Protection Action』 is [Block]. You can insert an HTTP header (return 302 redirection) or inject a JS script (return a JS script to be executed by the browser).

『Max Requests Per Second』globally configures that when the number of requests per second exceeds this value, the protection action will be executed. The default value is 500, ranging from 1 to 4,294,967,295.

『Request Increase Rate/Sec』 globally configures that the protection action will be executed when the number of requests per second exceeds half of the threshold value and the growth rate exceeds this value. The default value is 1,000 (%), ranging from 1 to 65,535.

『URL Control』 configures the URLs that need to be protected, supporting wildcards * and ?. The matching form is www.xxx.com/index.html, with Case-sensitive optional.

『Action』 configures the action to be executed when the traffic is judged to be a DDoS attack by the above conditions, with Give alert and Block optional.

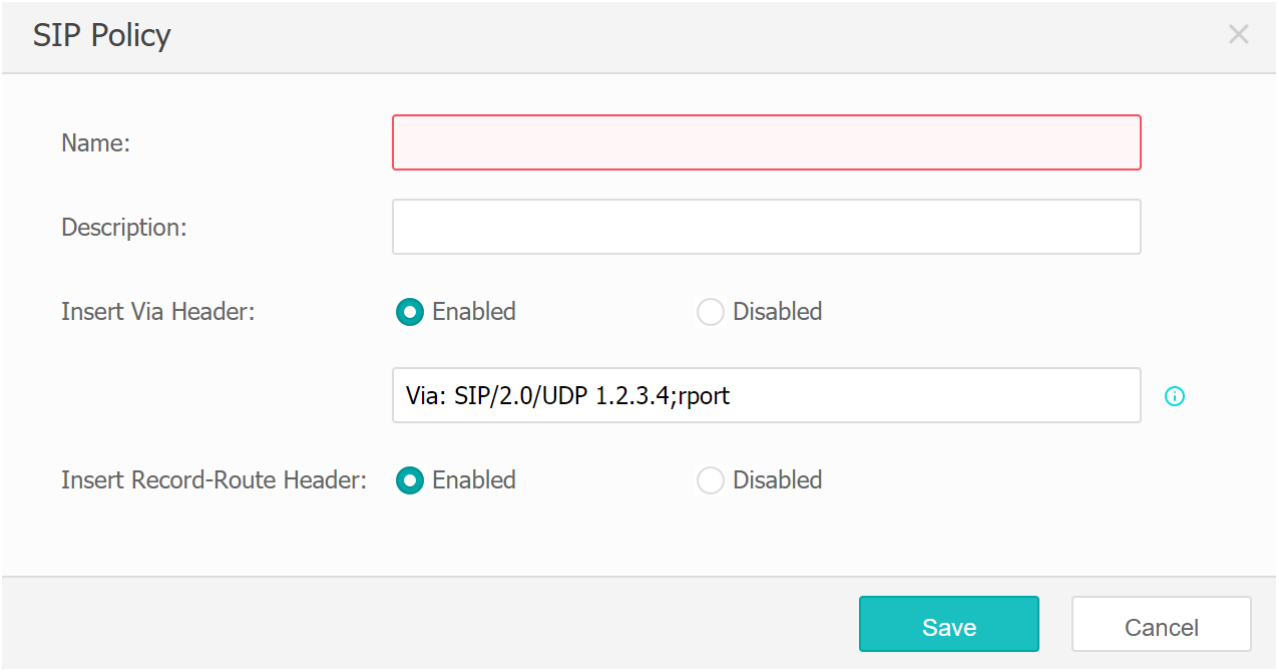
7.1.12 SIP Policy

【Operation Scenarios】

In order to modify the request direction and response direction of SIP protocol sessions, you can configure 『SIP Policy』 to optimize the virtual service.

【Operation Procedure】

『App Load Balancing』→『Optimization』→『SIP Policy』to conduct relevant configuration.



『Insert Via Header 』: when this option is enabled, the customized Via information will be inserted into the SIP request as the top-level Via header. Ensure the validity of Via, including SIP protocol (TCP / UDP) and other attributes (except branch). The inserted Via will affect the response path of the server, and the backhaul path of the response will be composed of the IP filled in multiple Via, such as Via: SIP/2.0/UDP 1.2.3.4;rport

『Insert Record-Route Header』: when this is enabled, the Record-Route header can be inserted. The inserted Record-Route will affect the request path of the next request, and the next request will be forwarded hop by hop according to the content of the Route.

7.1.13 QoS Policy

【Operation Scenarios】

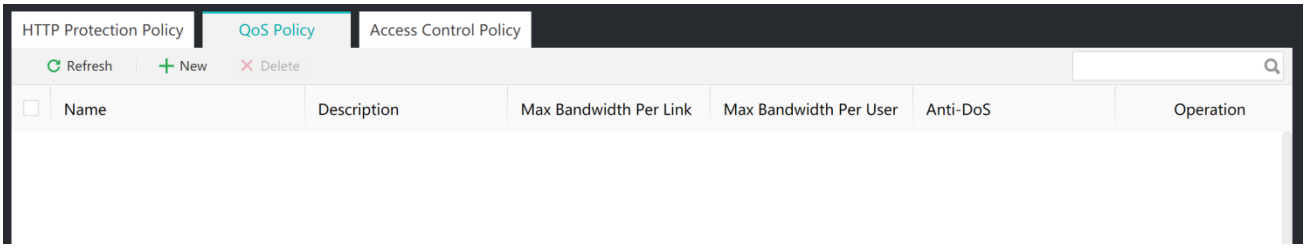
For the sake of ensuring the reasonable utilization of bandwidth, you can configure 『QoS Policy』 to control the traffic accessing the virtual service.

【Operation Procedure】

『App Load Balancing』→『Security Protection』→『QoS Policy』. Under『App Load Balancing』

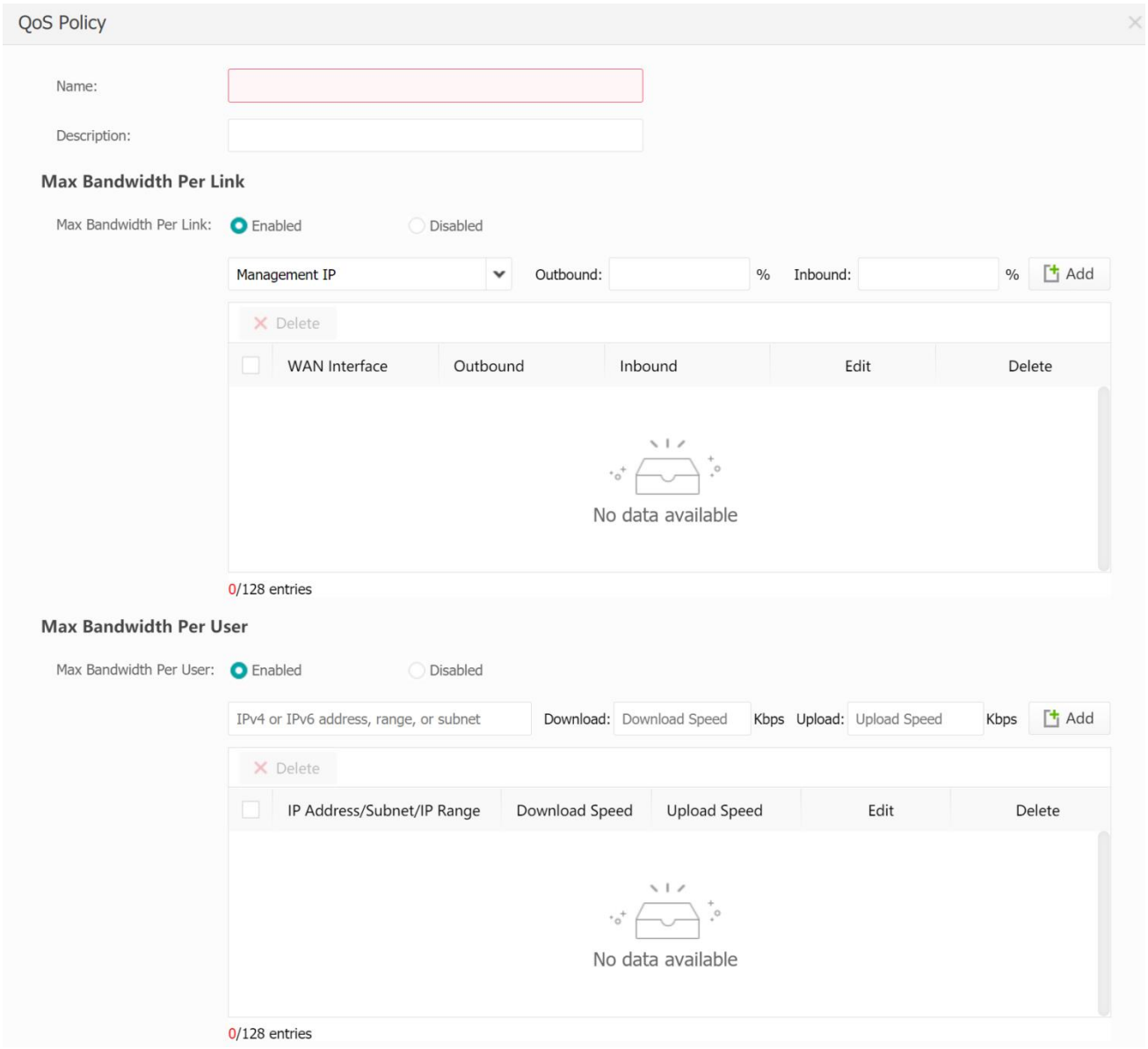
menu, click Security Protection. In the security protection window on the right, choose『QoS Policy』and click New.

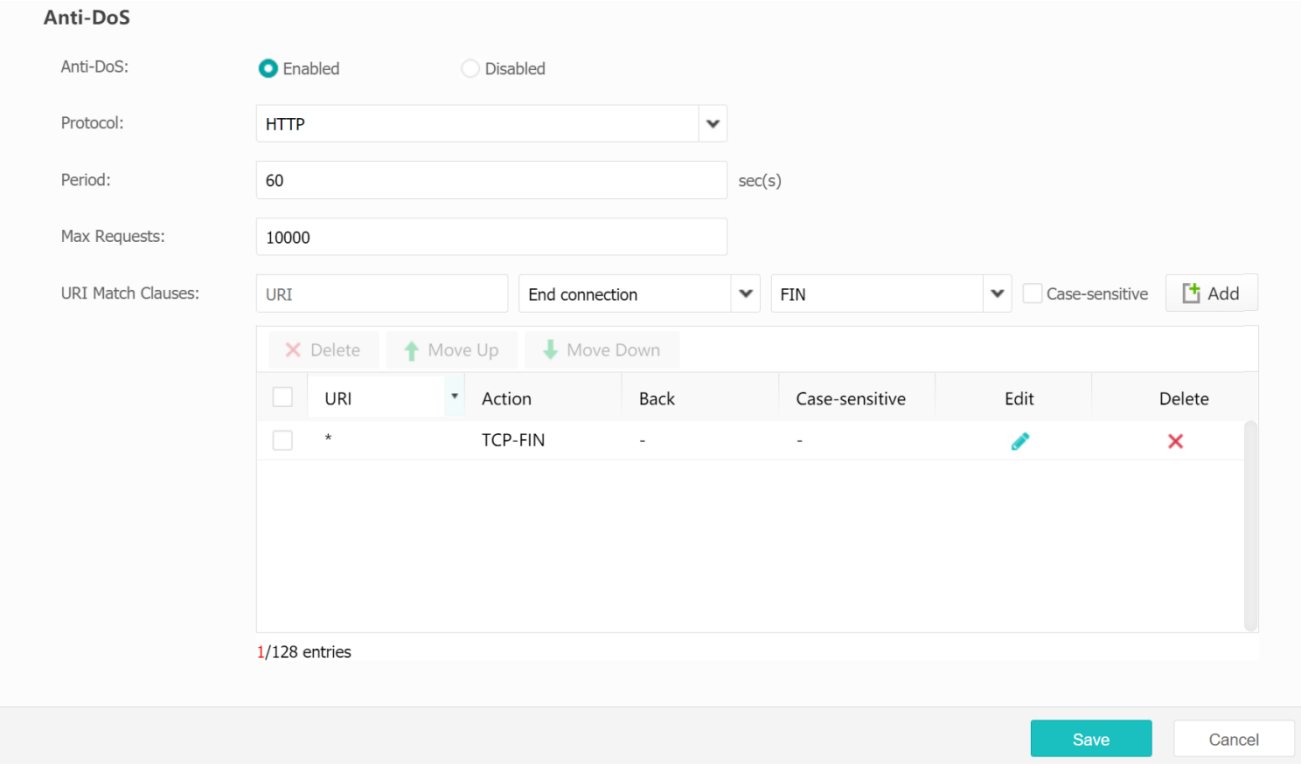
The page is shown in the figure below:



Under『QoS Policy』, the『Name』,『Description』,『Max Bandwidth Per Link』,『Max Bandwidth Per User』,『Anti-Dos』, and『Operation』of the QoS policy are displayed. In the『Operation』column, the Copy button is used to quickly copy and create the same QoS policy, and the Delete button is used to delete a single entry. The『QoS Policy』defined here can be used for the configuration of『Virtual Service』.

Click the New button, as shown in the following figure:


QoS Policy
Name:
Description:
Max Bandwidth Per Link
Max Bandwidth Per Link:
Enabled
Disabled
Management IP
Outbound:
%
Inbound:
%
Add
Delete
WAN Interface
Outbound
Inbound
Edit
Delete
No data available
0/128 entries
Max Bandwidth Per User
Max Bandwidth Per User:
Enabled
Disabled
IPv4 or IPv6 address, range, or subnet
Download:
Download Speed
Kbps
Upload:
Upload Speed
Kbps
Add
Delete
IP Address/Subnet/IP Range
Download Speed
Upload Speed
Edit
Delete
No data available
0/128 entries



『Max Bandwidth Per Link』 configures the link bandwidth used by the virtual service for controlling. Selects the WAN interface that needs to control the bandwidth and set the percentage of uplink and downlink bandwidth.

『Max Bandwith Per User』 controls the client accessing the virtual service. Enter the IP address of the client that needs control of its bandwidth and set the outbound and inbound bandwidth rate. The IP address supports the input of a single IP, network number, or IP range.

『Anti-DoS』 configures whether to enable DOS control.

『Protocol』 configures the protocol type for DoS control. HTTP or DNS can be selected. Other protocols can use 『Network』→『Cyber Security』→『DDoS Protection』 for DoS attack protection.

『Period』configures the time range of DoS control statistics. The default value is 60 (seconds), ranging from 1 to 36,000.

『Max Request 』 limits the number of HTTP or DNS requests in the [Period]. The corresponding action will be executed when the value is exceeded, ranging from 1 to 1,000,000.

『URI Match Clauses』 configures matching URIs that limit the number of HTTP requests. By default, all URIs are matched and the FIN closing action is executed.

After configuring the corresponding QoS policy, click Save to complete the configuration or click Cancel to cancel the configuration.

Attention: If selecting DNS for 『Anti-DoS』, URI Match Clauses are not supported and the Discard action is executed directly.

Attention: If the QoS policy of 『Anti-DoS』 is enabled, the type of virtual service calling the policy must be consistent with the DoS control protocol since HTTP protocol only supports HTTP and HTTPS virtual services while DNS protocol only supports DNS virtual services.

7.1.14 HTTP Rewriting Policy

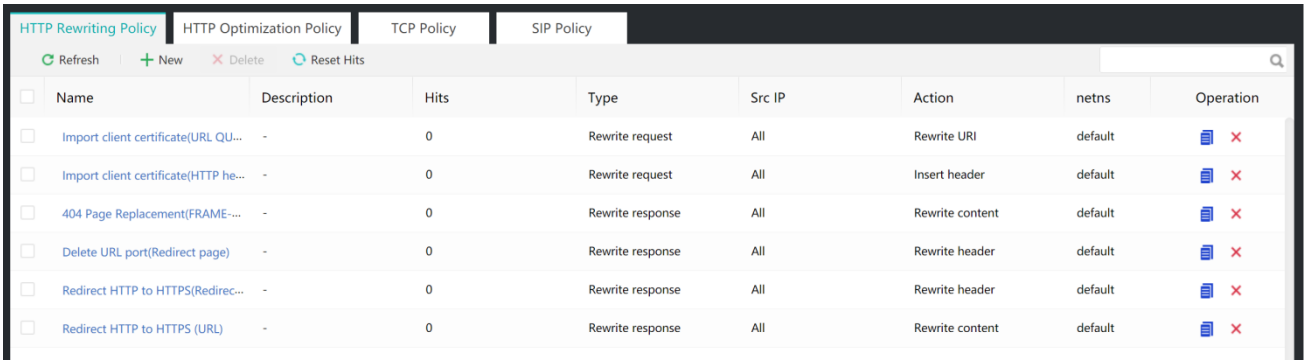
【Operation Scenarios】

When the service is upgraded from HTTP to HTTPS, some absolute path pages and other contents on the page will not be accessible due to cross-domain problems, etc. When the client needs to schedule different directories to the root directory of different nodes, you can configure 『HTTP Rewriting Policy』 to rewrite the client's request or the server's response to meet the corresponding service requirements.

【Operation Procedure】

『App Load Balancing』 → 『Optimization』 → 『HTTP Rewriting Policy』. On the 『App Load Balancing』 menu, click Optimization. In the optimization window on the right, select 『HTTP Rewriting Policy』 and click New.

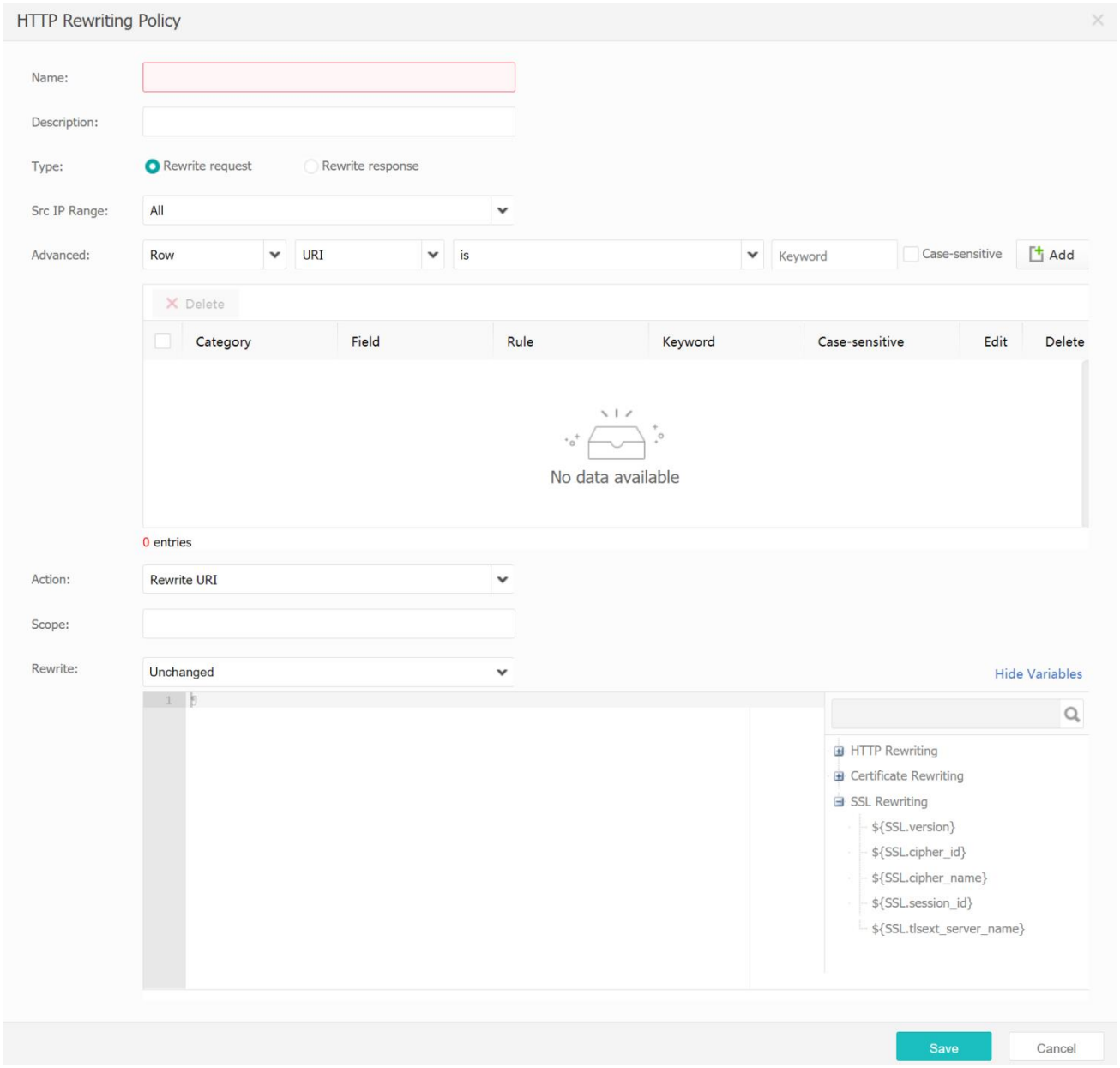
The page is shown in the figure below:



Under『HTTP Rewriting Policy』, the『Name』,『Description』,『Hits』,『Type』,『Src IP』,『Action』and『Operation』of the HTTP rewriting policy are displayed. In the『Operation』column, the Copy button is used to quickly copy and create the same HTTP rewriting policy, and the Delete button is used to delete a single entry. The『HTTP Rewriting Policy』defined here can be used for the『Scheduling』configuration part of the HTTP and HTTPS types.

The Reset Hits button can clear the matching times of the HTTP rewriting policy for re-counting.

Click the New button, as shown in the following figure:



『Type』configures the type of rewriting. You can choose Rewrite request or Rewrite request.

『Src IP Range』configures the source IP address of the user accessing the virtual service, including All, IP Address (single IP, subnet, or IP Range), and IP Database.

『Advanced』configures the matching conditions of HTTP request row, request header, response row, response header or request certificate variable, and performs corresponding actions if matched.

If the request row is selected for『Advanced』, the optional fields include URI, METHOD, and VERSION. The [URI] field can set the conditions of "is", "contains", "wildcard" and "regular

expression", and set the corresponding values. The [METHOD] field can set the condition to GET or POST. The [VERSION] field can set the condition to HTTP / 1.0 or HTTP / 1.1.

If the request header is selected for『Advanced』, the optional fields include HOST, COOKIE, USER-AGENT and custom. [HOST], [COOKIE], [USER-AGENT] and custom fields can set the conditions of "is", "contains", "wildcard" and "regular expression", and set the corresponding values.

If Certificate variable is selected for『Advanced』, the optional fields include Version, Issuer, Subject, Common Name, EmailAddress, Organization, Organizational Unit, Locality, State or Province, Country. The [VERSION] field can set the condition to V1, V2 or V3. Other fields can set the conditions of "is", "contains", "wildcard" and "regular expression", and set the corresponding values.

If the response row is selected for『Advanced』, the optional fields include VERSION and STATUS-CODE. The [VERSION] field can set the condition of HTTP / 1.0 or HTTP / 1.1. The [STATUS-CODE] field can set the conditions of "is", "contains", "wildcard" and "regular expression", and set the corresponding values.

If the response header is selected for『Advanced』, the optional fields include CONTENT-TYPE, SET-COOKIE, LOCATION and custom. [CONTENT-TYPE], [SET-COOKIE], [LOCATION] and custom fields can set the conditions of "is", "contains", "wildcard" and "regular expression", and set the corresponding values.

『Action』configures the actions to be executed after the matching conditions are met, including Rewrite URI, Insert header, Delete header, Rewrite header and Content rewriting.

If Rewrite URI is selected for『Action』, you need to define the [Scope] and [Rewrite]. The rewriting URI is limited to the type of『Request Rewriting』.

If Insert header is selected for『Action』, you need to define inserted [Header Name] and [Insert Content].

If Delete header is selected for『Action』, you need to define deleted [Header Name].

If Rewrite header is selected for『Action』, you need to define rewritten [Header Name], [Match Content] and [Rewrite].

If Content rewriting is selected for『Action』, you need to define rewritten [Match Content] and [Rewrite].

『Header Name』configures the HTTP header name in the search request or response, which is limited to [Insert, Delete, Rewrite] header actions.

『Insert content』configures the content to be inserted, only for [Insert header].

『Scope』configures the scope of rewriting URI. According to the rewriting scope, the maximum number of rewriting times is 255 for the duplicate matching content and only the [Rewrite URI] in『Request Rewrite』is allowed.

『Match Content』configures the content to be matched, supporting regular expression matching, and can be rewritten repeatedly up to 255 times. Among them, regular expression of content rewriting supports simple greedy matching and does not support regular expressions with empty matching, such as ?*, which is only limited to [Rewrite header] and [Content rewriting] actions.

『Rewrite』configures the rewritten content. Among them, header rewriting can be completed by configuring position characters such as $ and ^, and the supported variables can be queried by [Expand Variables], only limited to [Rewrite URI], [Rewrite header] and [Content rewriting] actions.

Click『Expand Variables』to expand the types of rewriting variables supported by ADC. HTTP Rewriting, Certificate Rewriting and SSL Rewriting can be selected.

7.1.15 Scheduling Policy

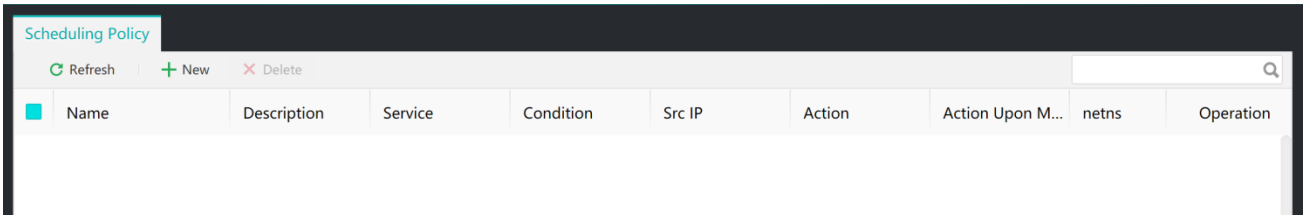
【Operation Scenarios】

In order to schedule the specific user's access to the specified node pool, you can configure the 『Scheduling Policy』 to schedule the traffic accessing the virtual service on demand.

【Operation Procedure】

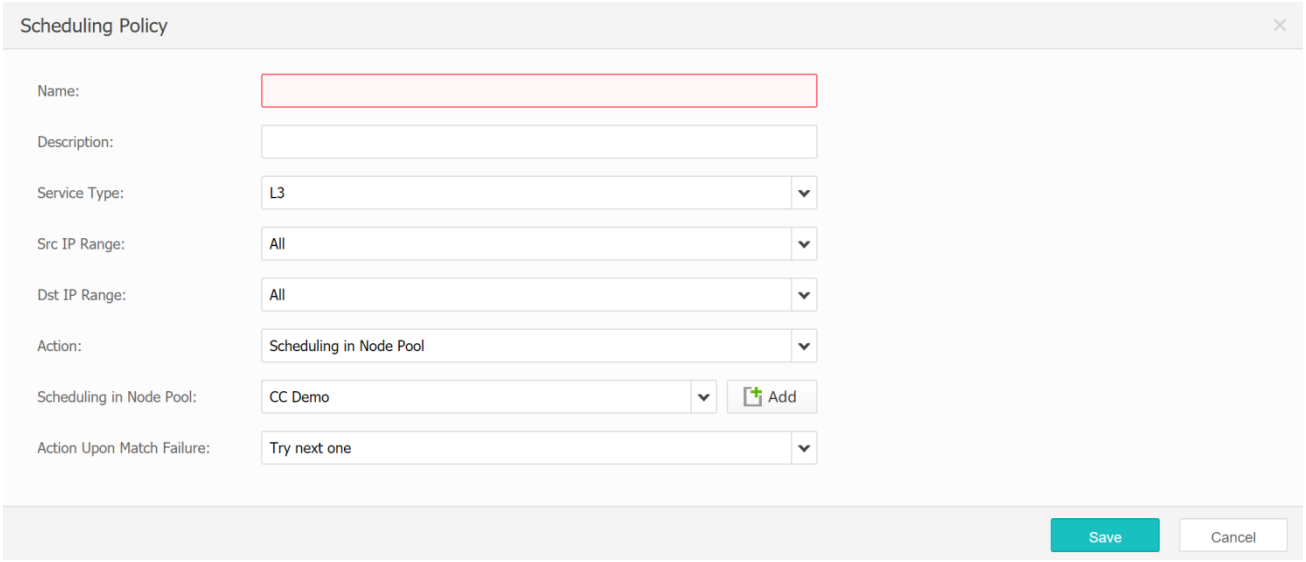
『App Load Balancing』 → 『Scheduling Policy』 → 『Scheduling Policy』. On the 『App Load Balancing』 menu, click Scheduling Policy. In the scheduling policy window on the right, select 『Scheduling Policy』 and click New.

The page is shown in the figure below:

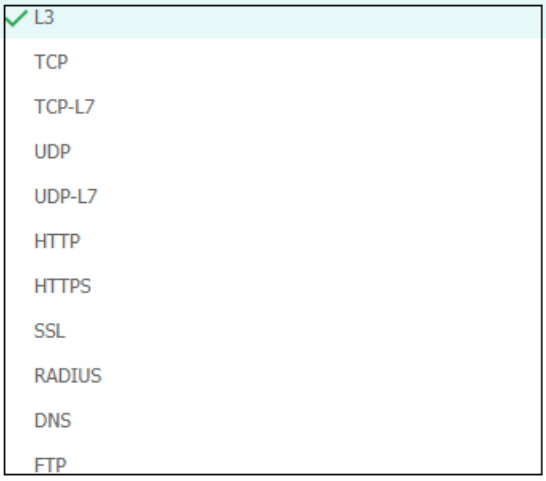


Under 『Scheduling Policy』, the 『Name』, 『Description』, 『Service』, 『Condition』, 『Src IP』,『Action』and 『Action Upon Match Failure』,『Operation』of the scheduling policy are displayed. In the『Operation』column, the Copy button is used to quickly copy and create the same scheduling policy, and the Delete button is used to delete a single entry. The 『Scheduling Policy』 defined here can be used for the configuration of 『Virtual Service』.

Click the New button, as shown in the following figure:



The 『service type』 drop-down displays the service types that can be selected, including [L3], [TCP], [TCP-l7], [UDP], [UDP-l7], [HTTP], [HTTPS], [SSL], [RADIUS], [DNS], [FTP].



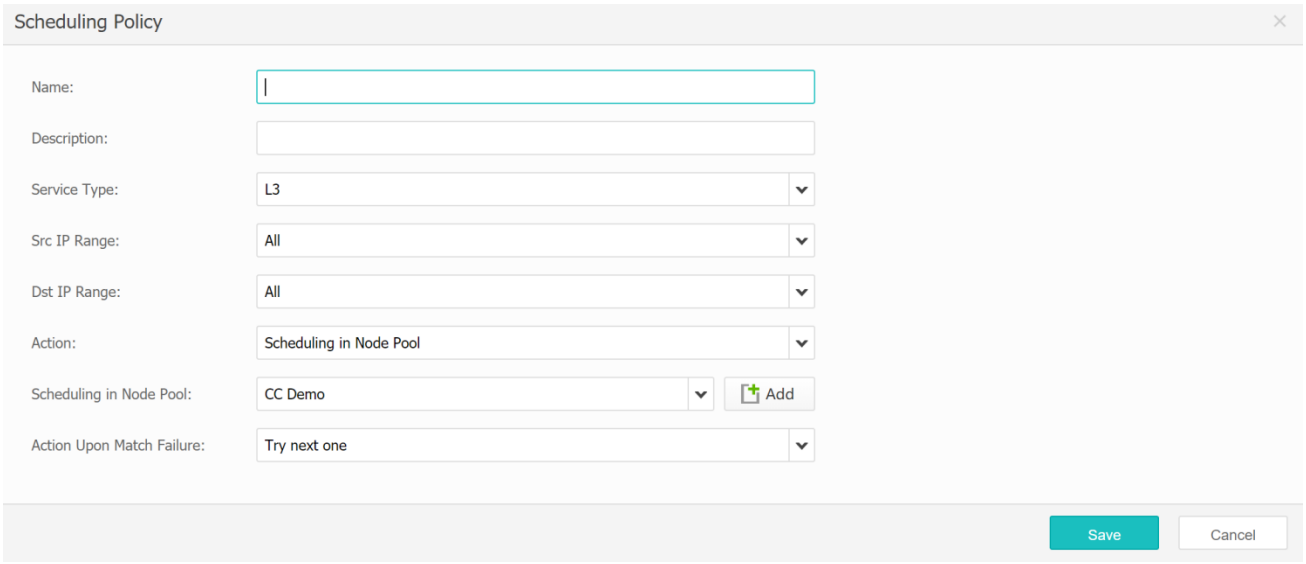
7.1.15.1 L3 Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [L3] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type 『L3』 and configure a scheduling policy based on this service type. The configuration is shown in the following figure.



『Src IP Range』 configures the source IP address of the user accessing the virtual service, including All, IP Address (single IP, subnet, or IP Range), User IP Address Range and ISP IP Address Range.

『Dst IP Range』 configures the access destination IP address range to match the traffic of virtual service. All, User IP Address Range and ISP IP Address Range can be selected.

『Action』 configures the action to be executed after meeting the scheduling policy and [L3] can only select the scheduling node pool.

『Scheduling in Node Pool』 selects the node pool to which the user who meets the scheduling policy is scheduled.

『Action Upon Match Failure』 configures the node scheduling failure action with options [Discard] or [Try next one]. [Discard] indicates that if scheduling fails because the referenced node pool has no nodes online after matching the scheduling policy, there will not be scheduling again. [Try next one] indicates that if scheduling fails because all nodes in the node pool are offline after matching fails or the scheduling succeeds, the node pool will continue to match the next scheduling policy.

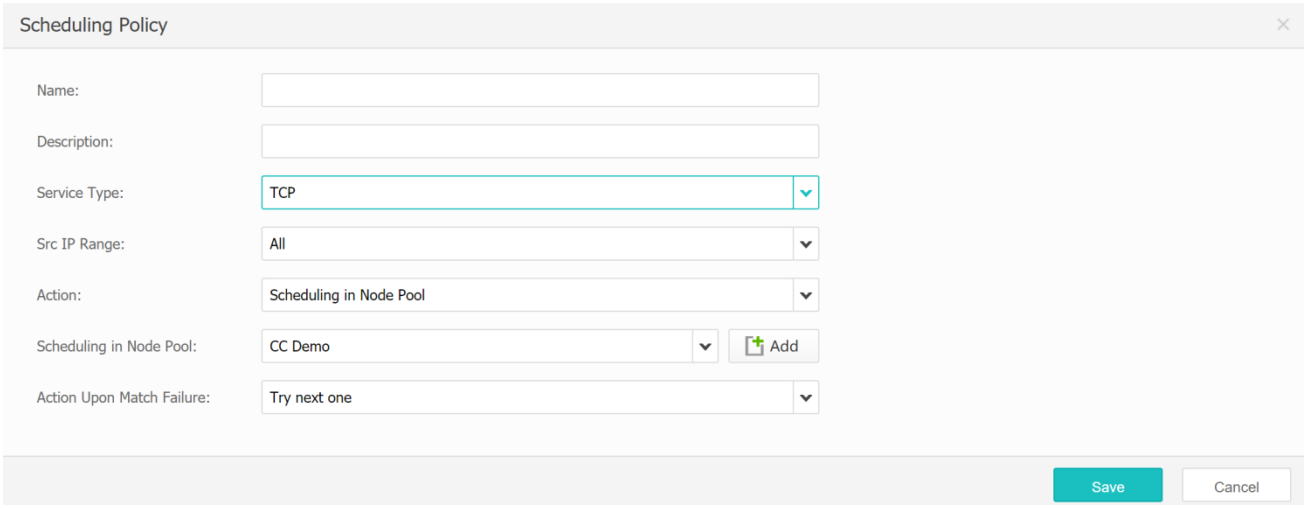
7.1.15.2 TCP Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [TCP] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『TCP』and configure a scheduling policy based on [TCP] service type. The configuration is shown in the following figure.



Please refer to the『L3』scheduling policy for all configurations and instructions.

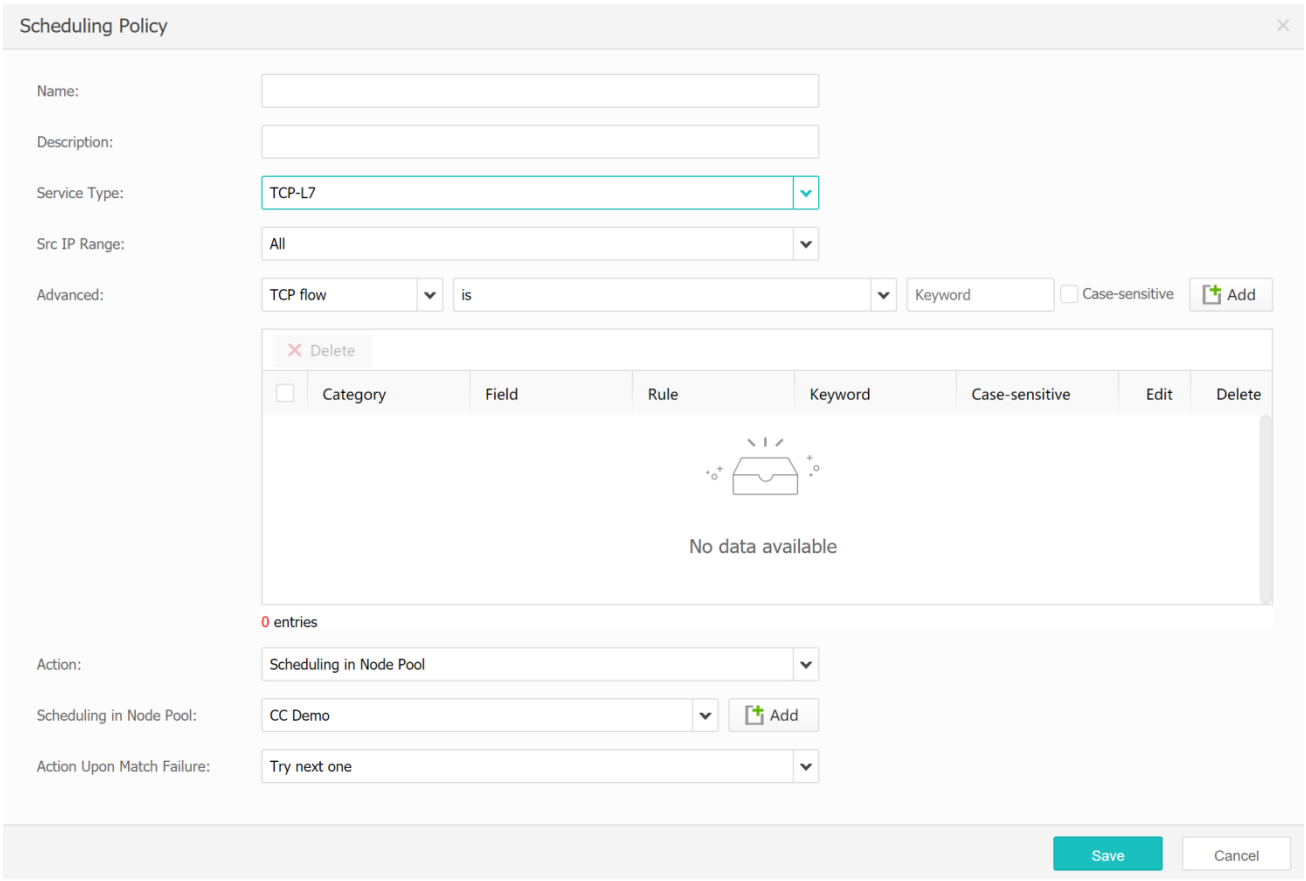
7.1.15.3 TCP-L7 Scheduling Policy

【Operation Scenarios】

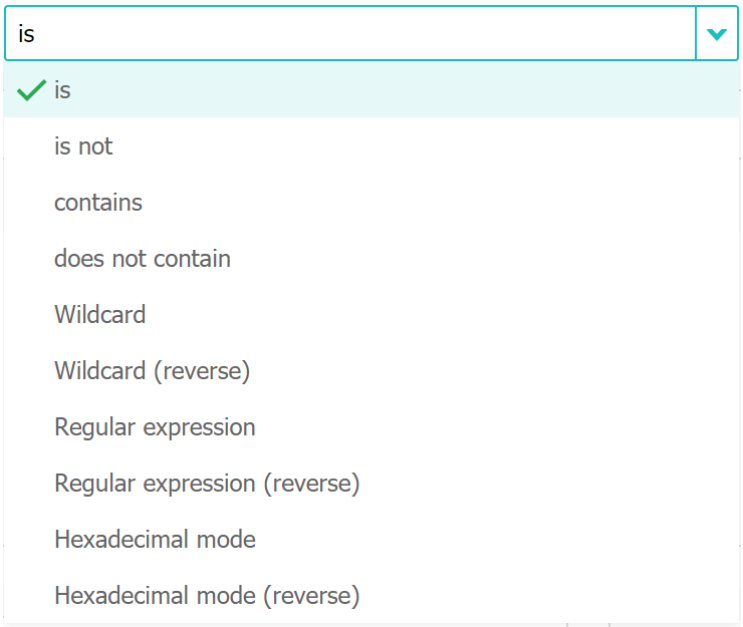
As the virtual service utilizes [TCP-L7] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『TCP-L7』and configure a scheduling policy based on [TCP-L7] service type. The configuration is shown in the following figures.



『Advanced』 configures the condition to match the data contents in the TCP flow. If it matches, the corresponding action will be executed. If it fails to match, the action will be executed according to the failed action.



『Action』 configures the action to be executed after meeting the scheduling policy with options scheduling in node pool and closing connections.

『Action Upon Match Failure』configures the node scheduling failure action with options [FIN close], [RST close] or [Try next one]. [FIN close] or [RST close] indicates that if scheduling fails because the referenced node pool has no nodes online after matching the scheduling policy, there will not be scheduling again. [Try next one] indicates that if scheduling fails because all nodes in the node pool are offline after matching fails or the scheduling succeeds, the node pool will continue to match the next scheduling policy.

『Closing Method』 configures the closing method used when 『Action』 selects to Close the Connection, with options FIN close or RST close.

Please refer to the 『L3』 scheduling policy for all other configurations and instructions.

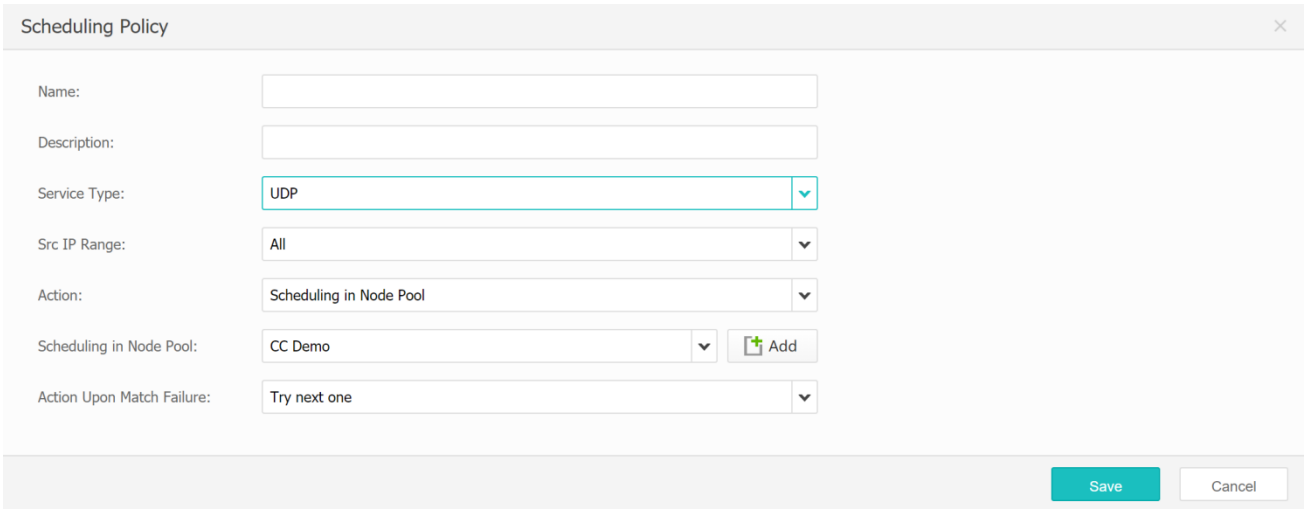
7.1.15.4 UDP Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [UDP] type for load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『UDP』and configure a scheduling policy based on [UDP] service type. The configuration is shown in the following figure.



Please refer to the『L3』scheduling policy for all configurations and instructions.

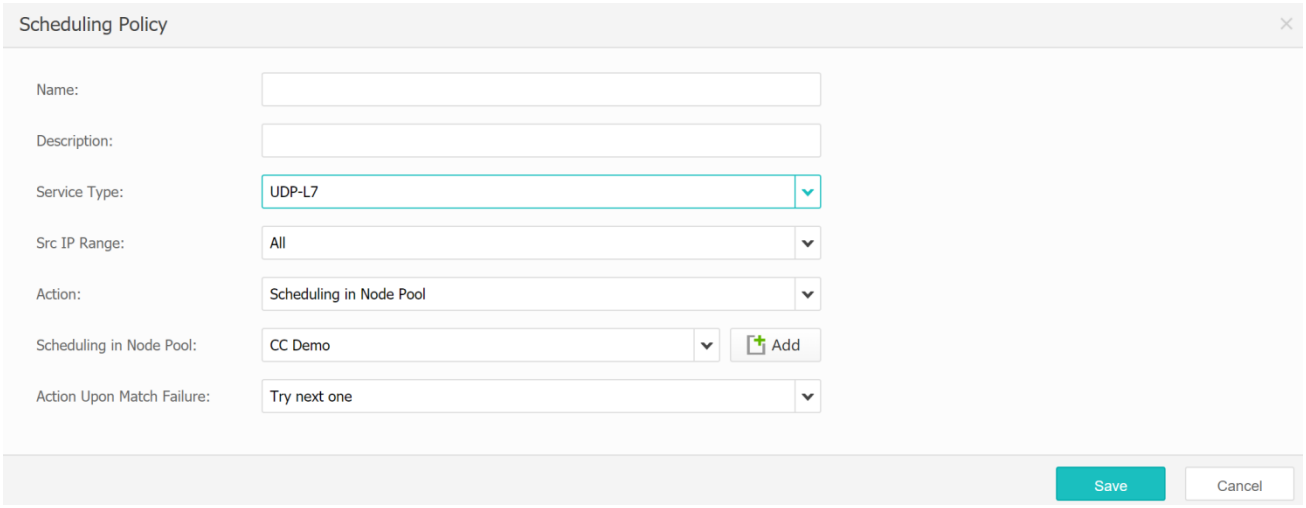
7.1.15.5 UDP-L7 Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [UDP-L7] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『UDP-L7』and configure a scheduling policy based on [UDP-L7] service type. The configuration is shown in the following figure.



Please refer to the『L3』scheduling policy for all configurations and instructions.

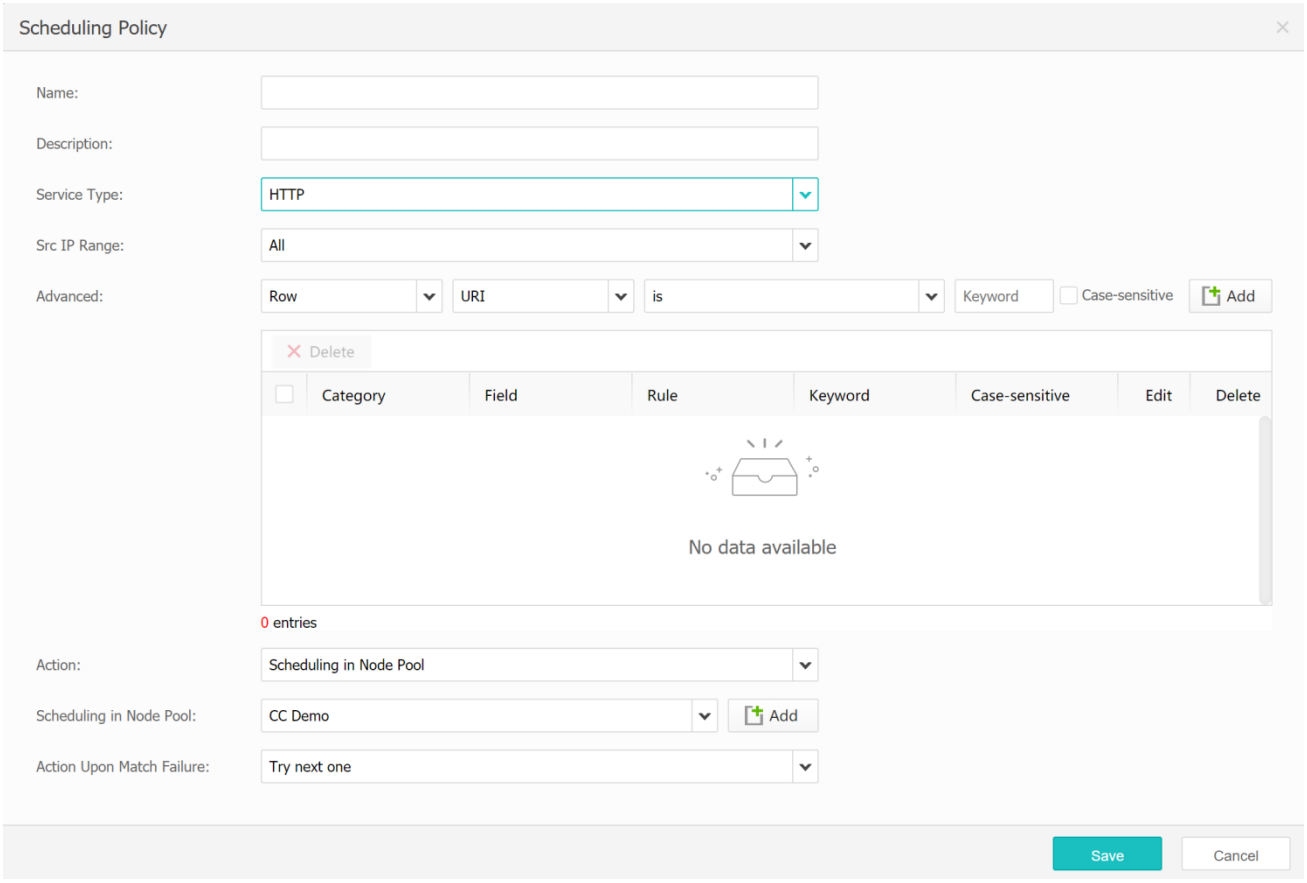
7.1.15.6 HTTP Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [HTTP] type for load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『HTTP』and configure a scheduling policy based on [HTTP] service type. The configuration is shown in the following figure.



『Src IP Range』fills in the source IP address range matching the scheduling strategy. You can select All, Single Address, IP Address Range, Subnets, and User IP Address Range.

『Advanced』selects to match the request row or request header. The request row can set the matching conditions according to [VERSION], [METHOD], [URI], and the request header can set the matching conditions according to the [HOST], [COOKIE], [USER-AGENT] and custom fields.

『Action』 selects Scheduling in Node Pool, Returning Specified Contents, Closing the Connection or Scheduling and Rewriting. After selecting Rewriting, you can select [request rewriting policy] and [reply rewriting policy].

『Scheduling in Node Pool』 selects the node pool to which users who meet the scheduling policy conditions will be scheduled when accessing a virtual service.

『Action Upon Match Failure』configures the node scheduling failure action with options [FIN close], [RST close], [Try next one] or [Returning specified contents]. [FIN close] or [RST close] indicates that if scheduling fails because the referenced node pool has no nodes online after matching the scheduling policy, there will not be scheduling again. [Try next one] indicates that if scheduling fails because all nodes in the node pool are offline after matching fails or the scheduling succeeds, the node pool will continue to match the next scheduling policy. [Returning specified contents] can select the built-in custom content to return.

『Closing Method』 configures the closing method used when 『Action』 selects to Close the Connection, with options FIN close or RST close.

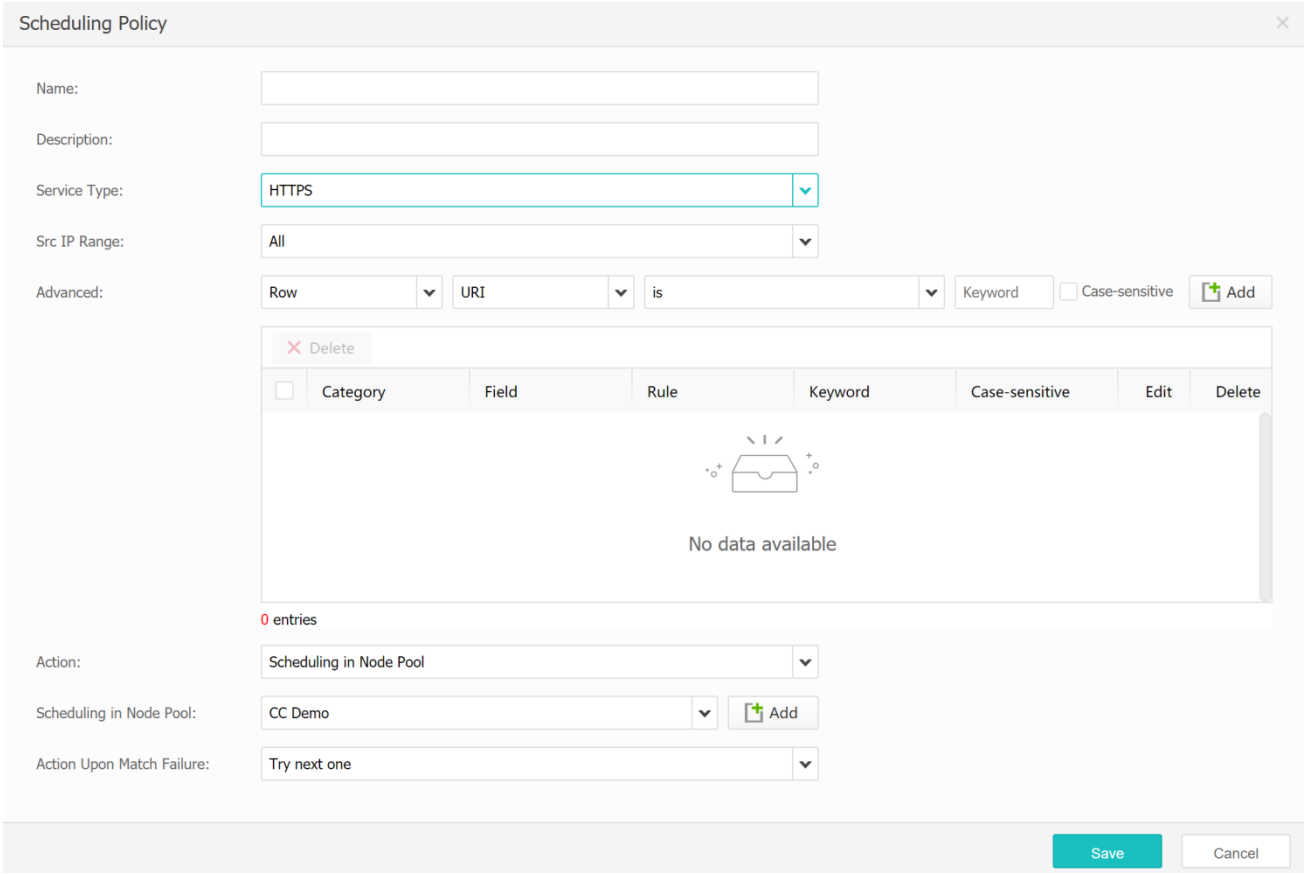
7.1.15.7 HTTPS Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [HTTPS] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『HTTPS』and configure a scheduling policy based on [HTTPS] service type. The configuration is shown in the following figure.



『Advanced』selects to match the request row, request header or certificate variable. The request row can set the matching conditions according to [VERSION], [METHOD], [URI]. The request header can set the matching conditions according to the [HOST], [COOKIE], [USER-AGENT] and custom fields. The certificate variable can set the matching conditions according to the [Version], [Issuer], [Subject], [Common Name], [EmailAddress], [Organization], [Organizational Unit], [Locality], [State or Province] and [Country] fields.

Please refer to the『HTTP』scheduling policy for all other configurations and instructions.

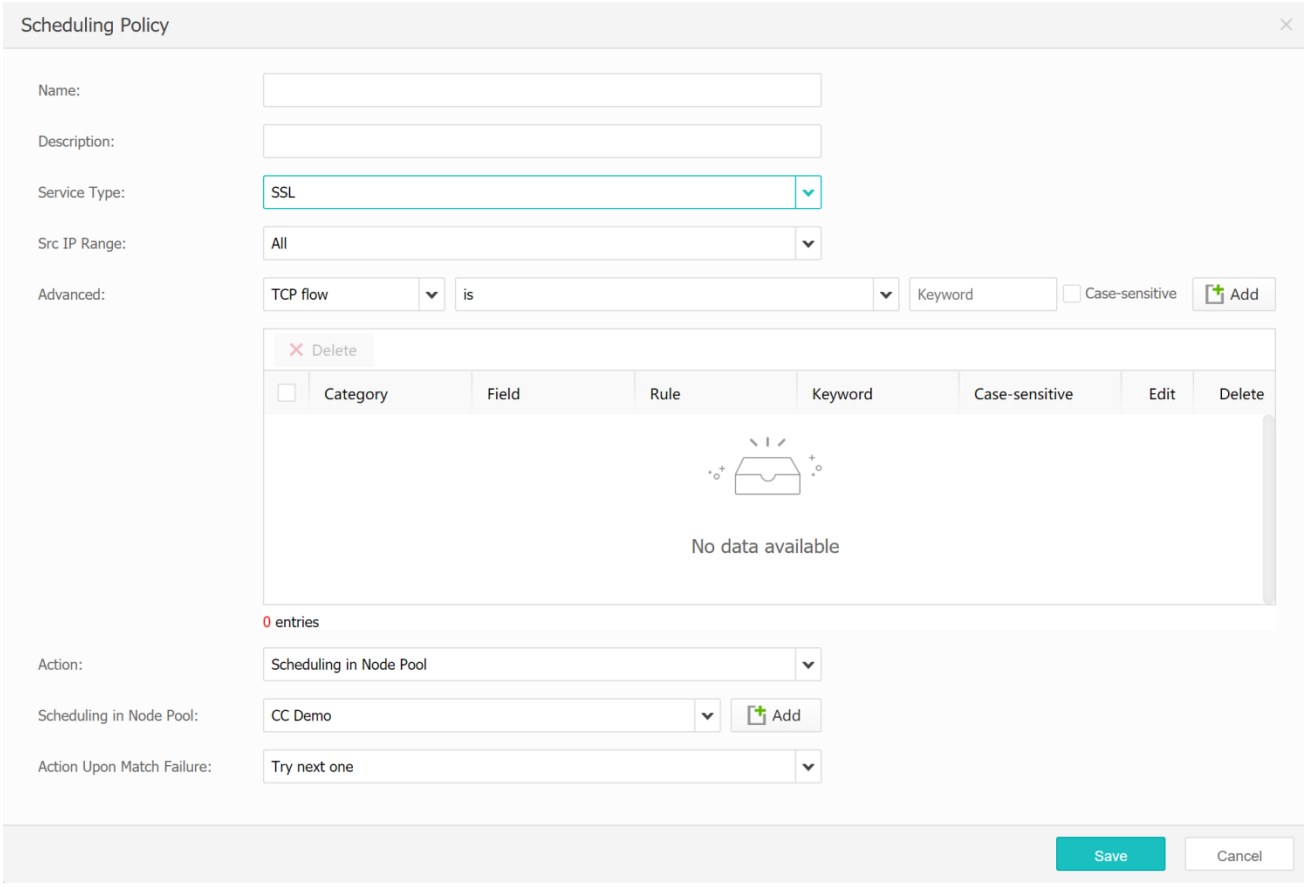
7.1.15.8 SSL Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [SSL] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『SSL』and configure a scheduling policy based on [SSL] service type. The configuration is shown in the following figure.



『Src IP Range』fills in the source IP address range matching the scheduling strategy. You can select All, Single Address, IP Address Range, Subnets, and User IP Address Range.

『Advanced』selects to match certificate variables or TCP flow conditions. The certificate variable can set the matching conditions according to the [Version], [Issuer], [Subject], [Common Name], [EmailAddress], [Organization], [Organizational Unit], [Locality], [State or Province] and [Country] fields. TCP flow can set conditions to be "is", "contains", "wildcard", and "regular expression".

『Action』schedules to the node pool.

『Scheduling in Node Pool』selects the node pool to which users who meet the scheduling policy conditions will be scheduled when accessing a virtual service.

『Action Upon Match Failure』configures the node scheduling failure action with options [Try next one] and [Discard]. [Try next one] indicates that if scheduling fails because all nodes in the node pool are offline after matching fails or the scheduling succeeds, the node pool will continue to match the next scheduling policy. [Discard] indicates that if scheduling fails because the referenced node pool has no nodes online after matching the scheduling policy, there will not be scheduling again.

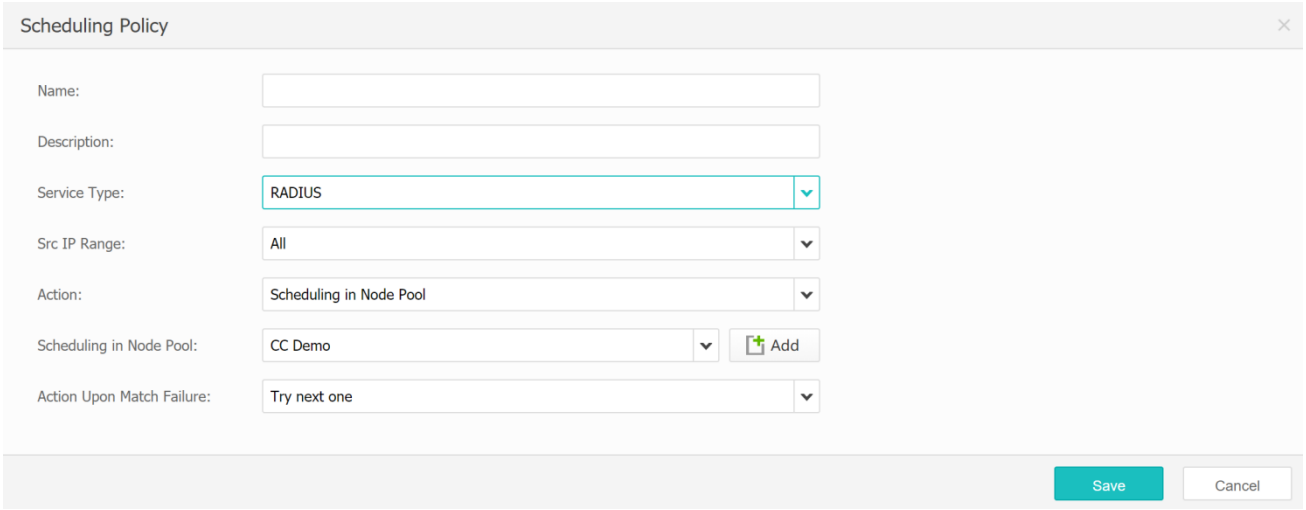
7.1.15.9 RADIUS Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [RADIUS] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『RADIUS』and configure a scheduling policy based on this service type. The configuration is shown in the following figure.



Please refer to the 『L3』 scheduling policy for all configurations and instructions.

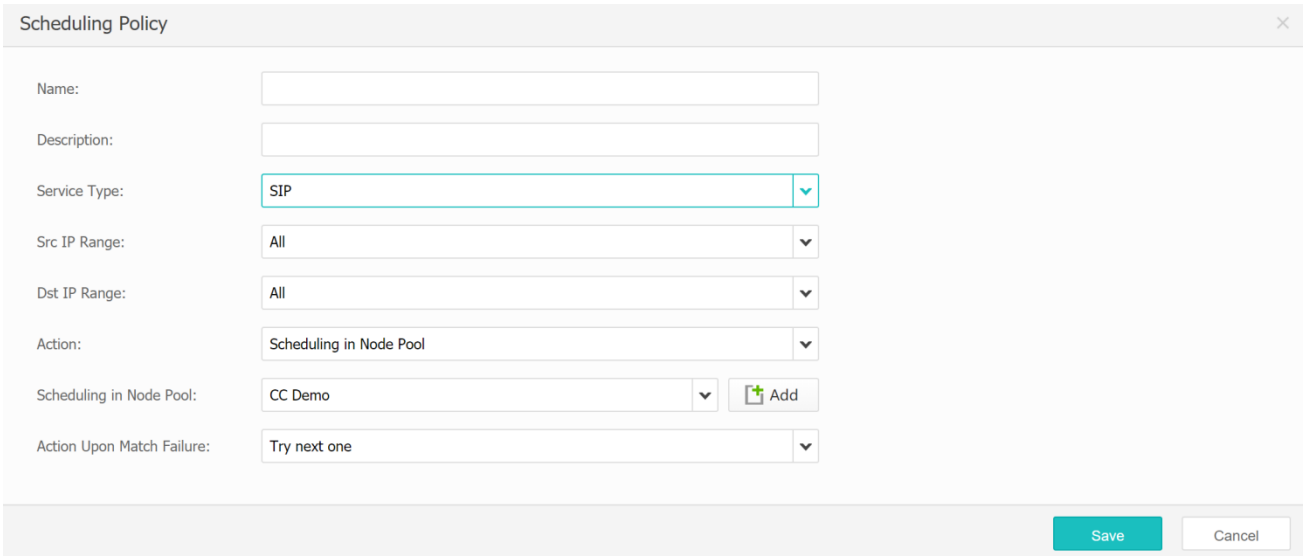
7.1.15.10 SIP Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [SIP] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『SIP』and configure a scheduling policy based on this service type. The configuration is shown in the following figure.



Please refer to the『L3』scheduling policy for all configurations and instructions.

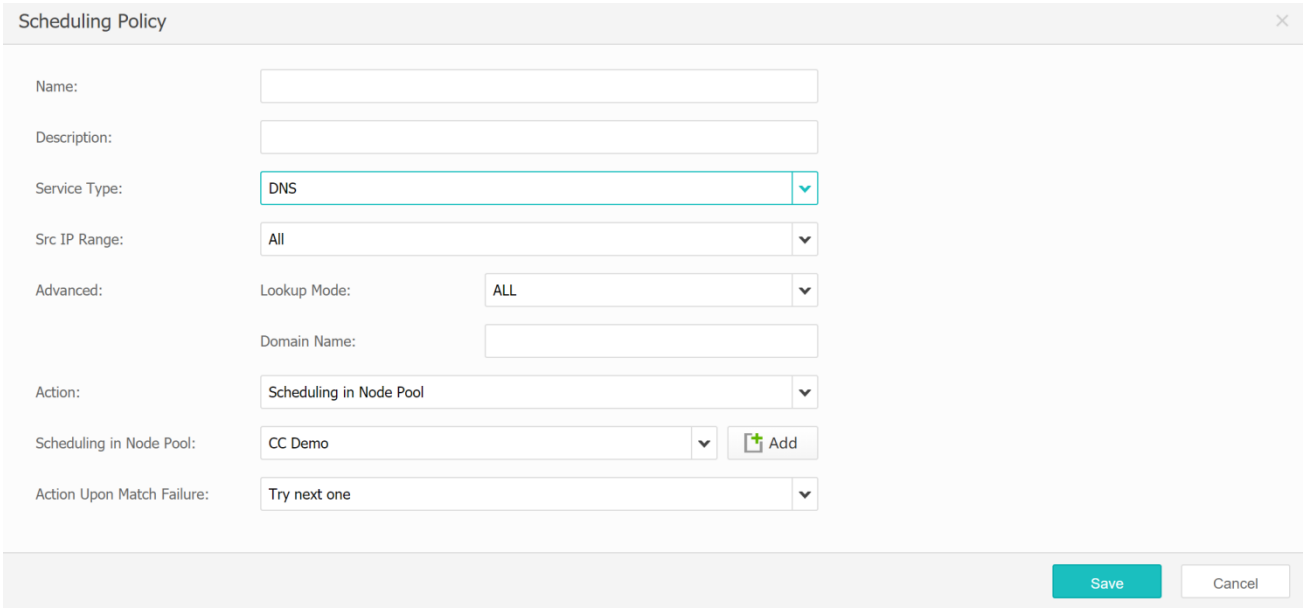
7.1.15.11 DNS Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [DNS] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『DNS』and configure a scheduling policy based on this service type. The configuration is shown in the following figure.



『Advanced』: the advanced match rule of DNS scheduling policy can be entered according to the lookup mode and domain name that DNS requests. Then corresponding actions are performed. Lookup Mode provides the following options: [ALL], [A], [NS], [CNAME], [SOA], [PTR], [MX], [TXT], [AAAA], [SPF], and [Custom]. A domain name address should be entered in Domain Name.

Please refer to the『L3』scheduling policy for all other configurations and instructions.

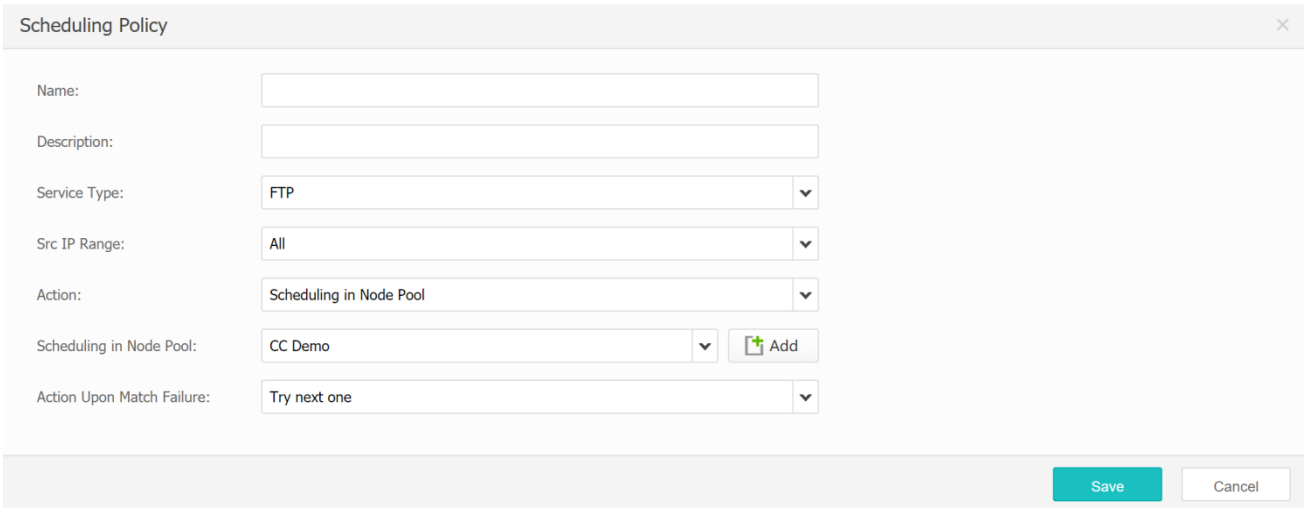
7.1.15.12 FTP Scheduling Policy

【Operation Scenarios】

As the virtual service utilizes [FTP] type for app load balancing, the scheduling policy needs to be configured as such type.

[Configuration Instruction]

Select service type『FTP』and configure a scheduling policy based on this service type. The configuration is shown in the following figure.



Please refer to the『L3』scheduling policy for all configurations and instructions.

7.1.16 Access Control Policy

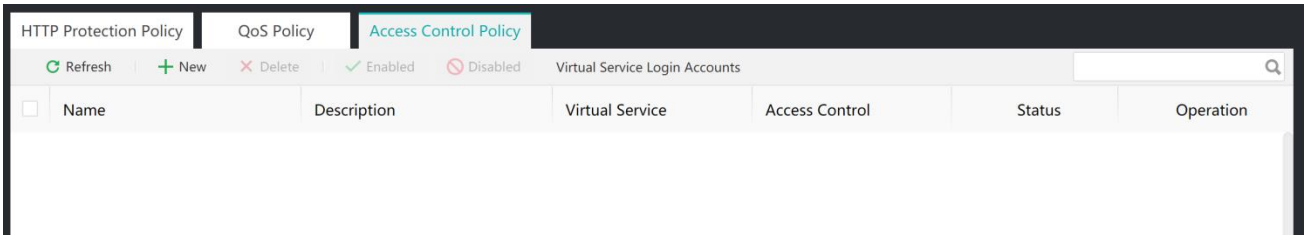
【Operation Scenarios】

The access control policy mainly refers to the access permission in virtual service access settings. By setting this configuration, the client must pass the user authentication to access the protected resources, so as to protect resources.

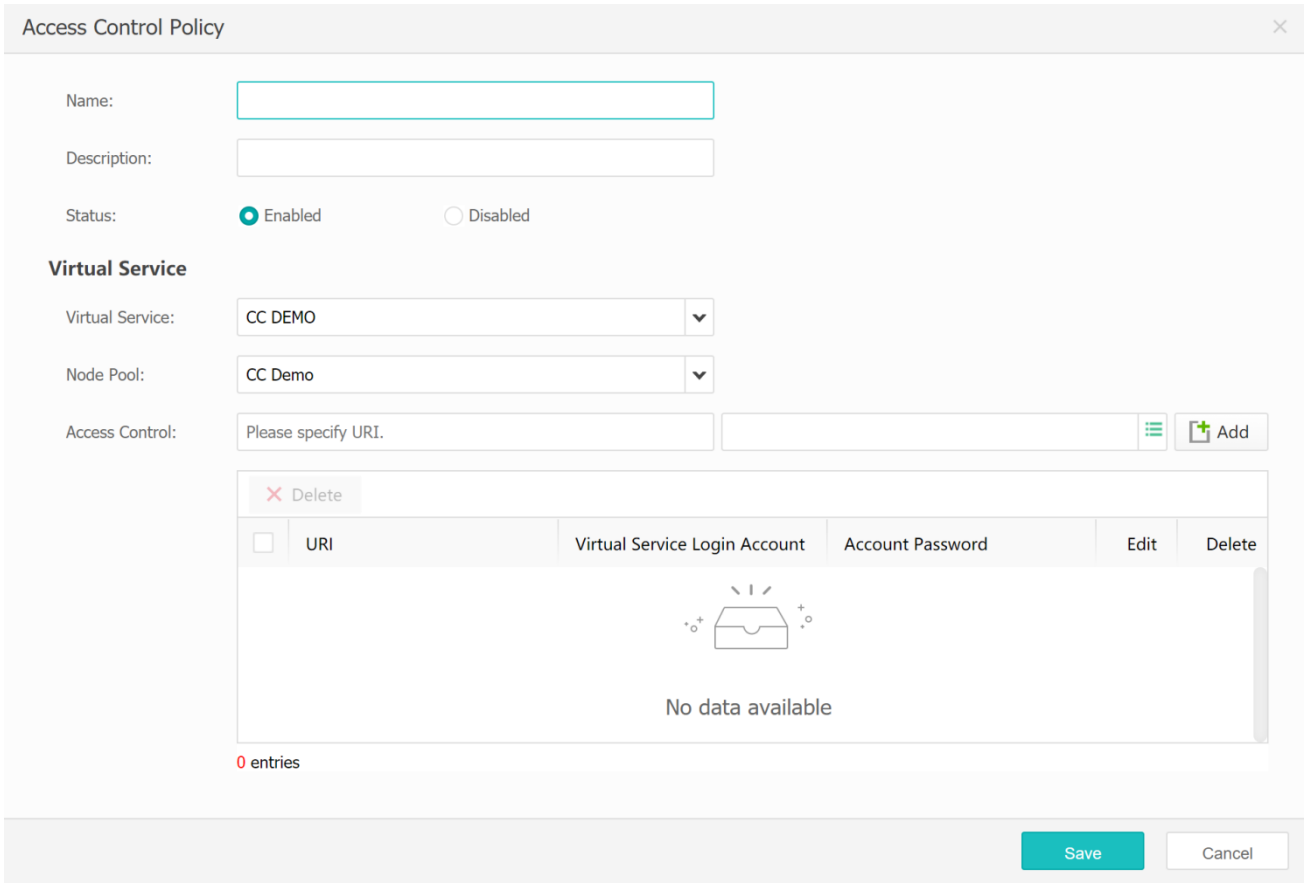
【Operation Procedure】

『App Load Balancing』→『Security Protection』→『Access Control Policy』. On the 『Load Balancing』menu, click Security Protection. In the right security protection window, select 『Access Control Policy』and click New.

The page is shown in the figure below:

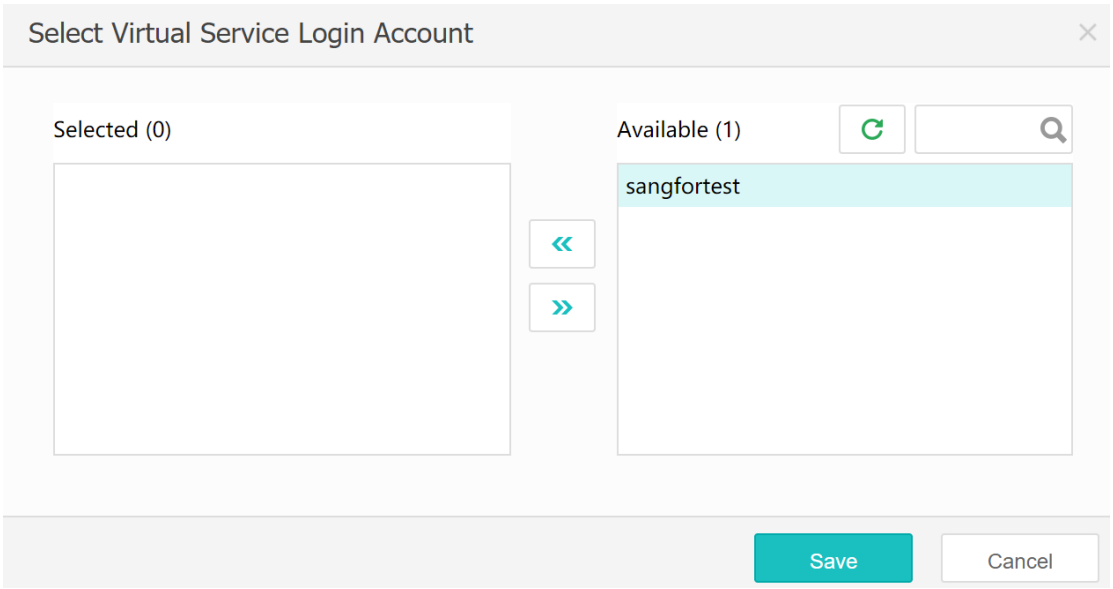


Click the New button, as shown in the following figure:

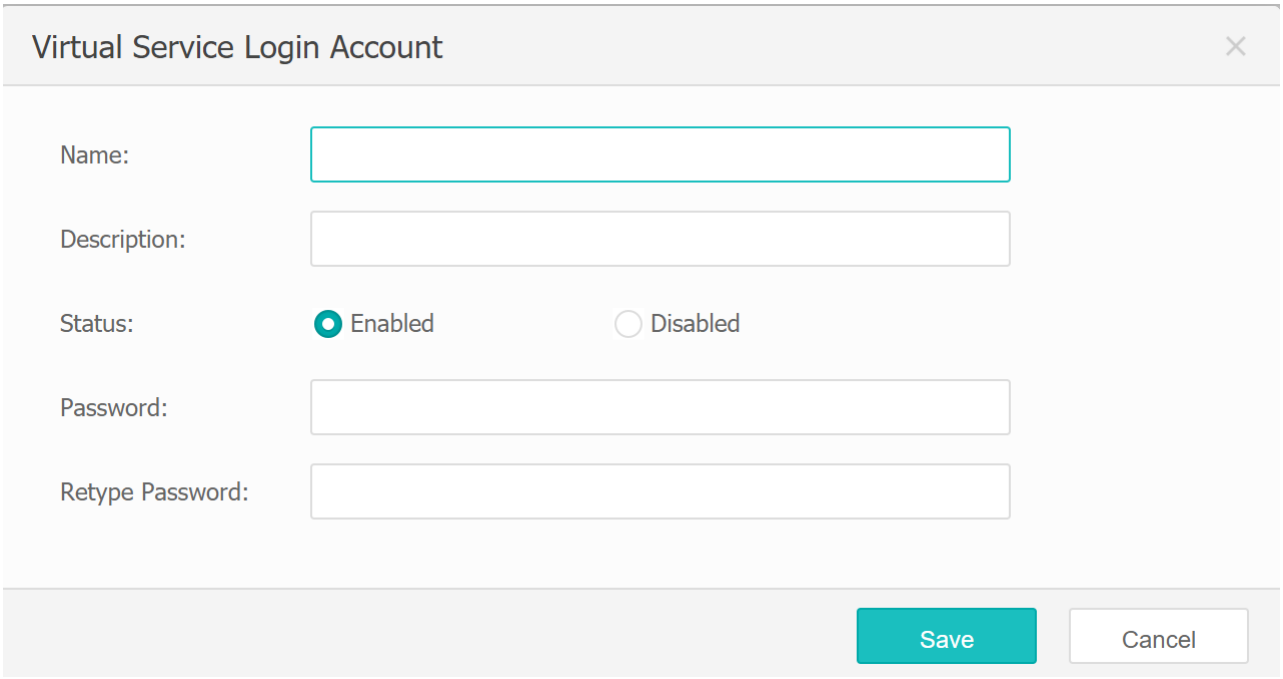


『Virtual Service』and『Node Pool』are virtual service and node pool that need access control setting.

The URI of access control should be entered in『Access Control 』. Click the button on the right side to select a login account as shown in the following figure:



The login account can also be configured on the access control policy page by clicking Virtual Service Login Account and New.



『Name』 refers to the name of the login account.

『Password』 refers to the password of the login account.

Chapter 8 Link Load Balancing

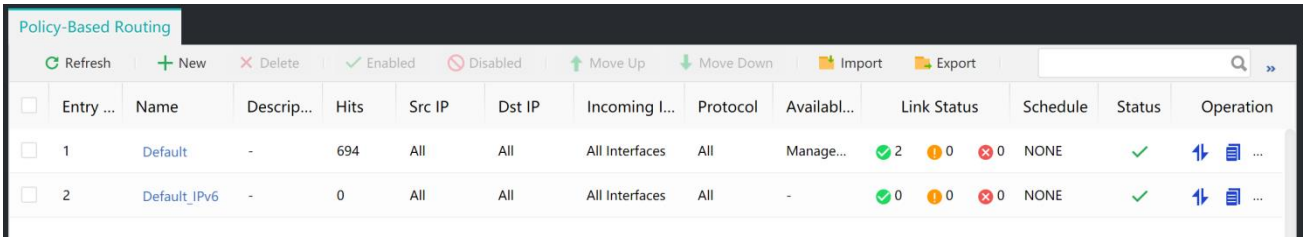
8.1 Policy-based Routing

【Operation Scenarios】

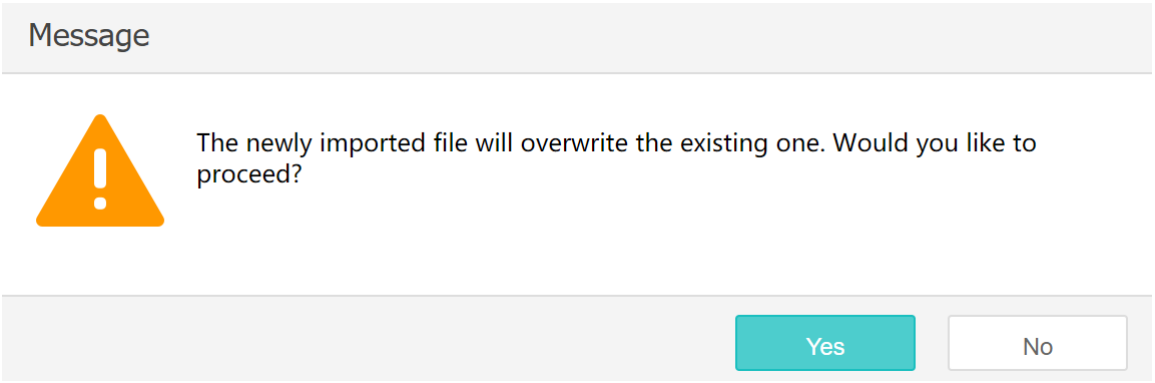
When serving multiple WAN interface links, Policy-Based Routing sets routing based on some policy according to the source/destination IP, link selection policy, and other conditions to determine the WAN interface from which the data is transmitted, so as to realize policy-based routing, and separate traffic and optimize bandwidth for multiple links.

【Operation Procedure】

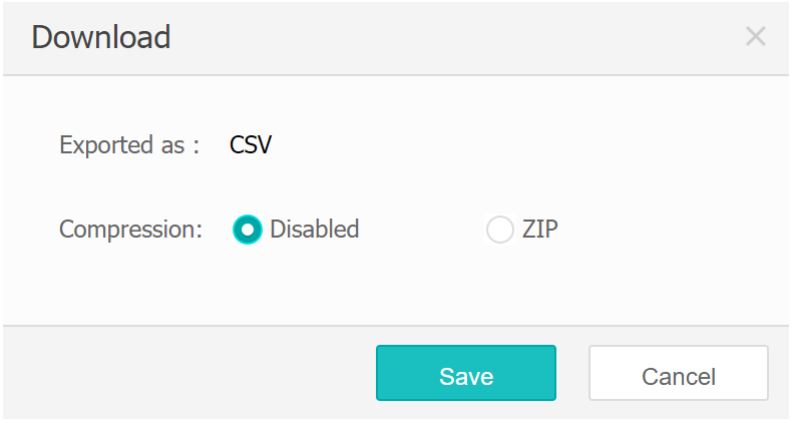
『Link Load Balancing』 → 『Policy-based Routing』. The interface is as follows:



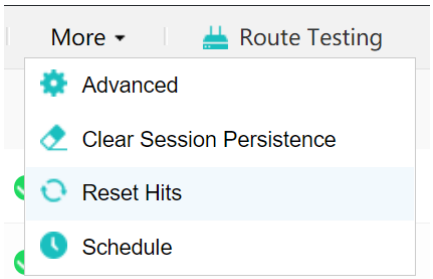
Click Import, select the file to import, and the【Message】box will pop up. Click Yes to import.



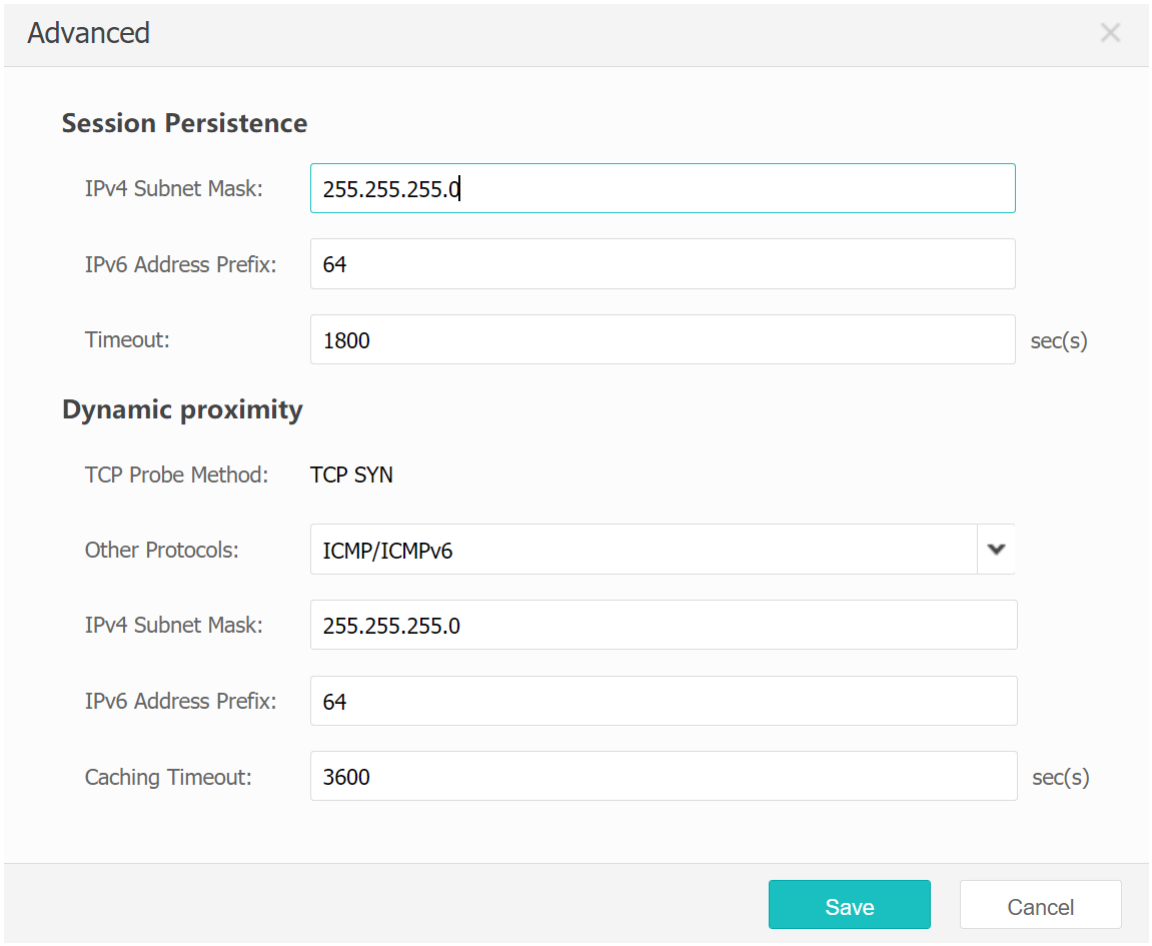
Click Export to back up custom policy-based routing. A【Download】box will pop out. Select the required compression method, click Save, and select a path to complete the export.



Click More to open other function options. See the figure below.



『More』 → 『Advanced』 sets the advanced attribute of outbound data control. The page is shown in the figure below:



『IPv4 Subnet Mask』 keeps the same session persistence for different external IP access of the same net number through this subnet mask.

『IPv6 Address Prefix』 keeps the same session persistence for different external IP access of the same prefix through this address prefix.

『Timeout』 refers to the saving time of outbound session persistence record.

『TCP Probe Method』 shows that when the link selection policy in policy-based routing is [Dynamic proximity] and it requests a destination address based on the TCP protocol outbound, the device sends TCP SYN to the destination address for a probe.

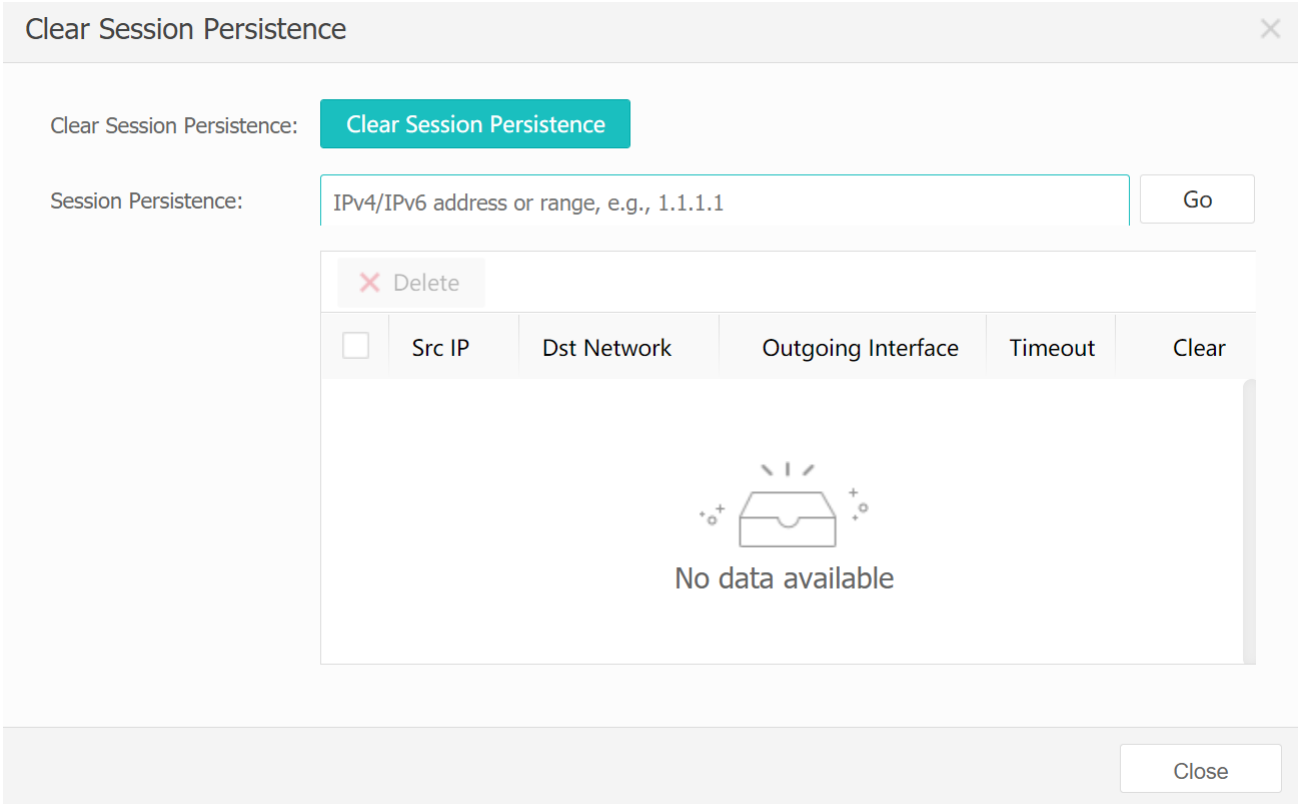
『Other Protocols』is used when the request is based on other protocols in addition to TCP type requests.

『Cache Subnet Mask』 uses the same dynamic proximity selected link for different external IP addresses belonging to the same network number.

『Caching Timeout』 sets the timeout of the dynamic proximity to and from delay cache.

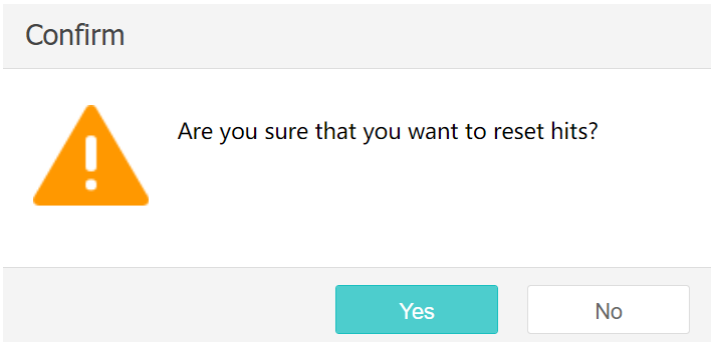
『More』→『Clear Session Persistence』, the【Clear Session Persistence】window will pop up. Click Clear Session Persistence to clear current session persistence data.

Enter the IP address to query in the input box of 『Session Persistence』 , and then click Go. Then qualified session persistence records will be shown in the list box below. Clear relevant session persistence records according to the need.

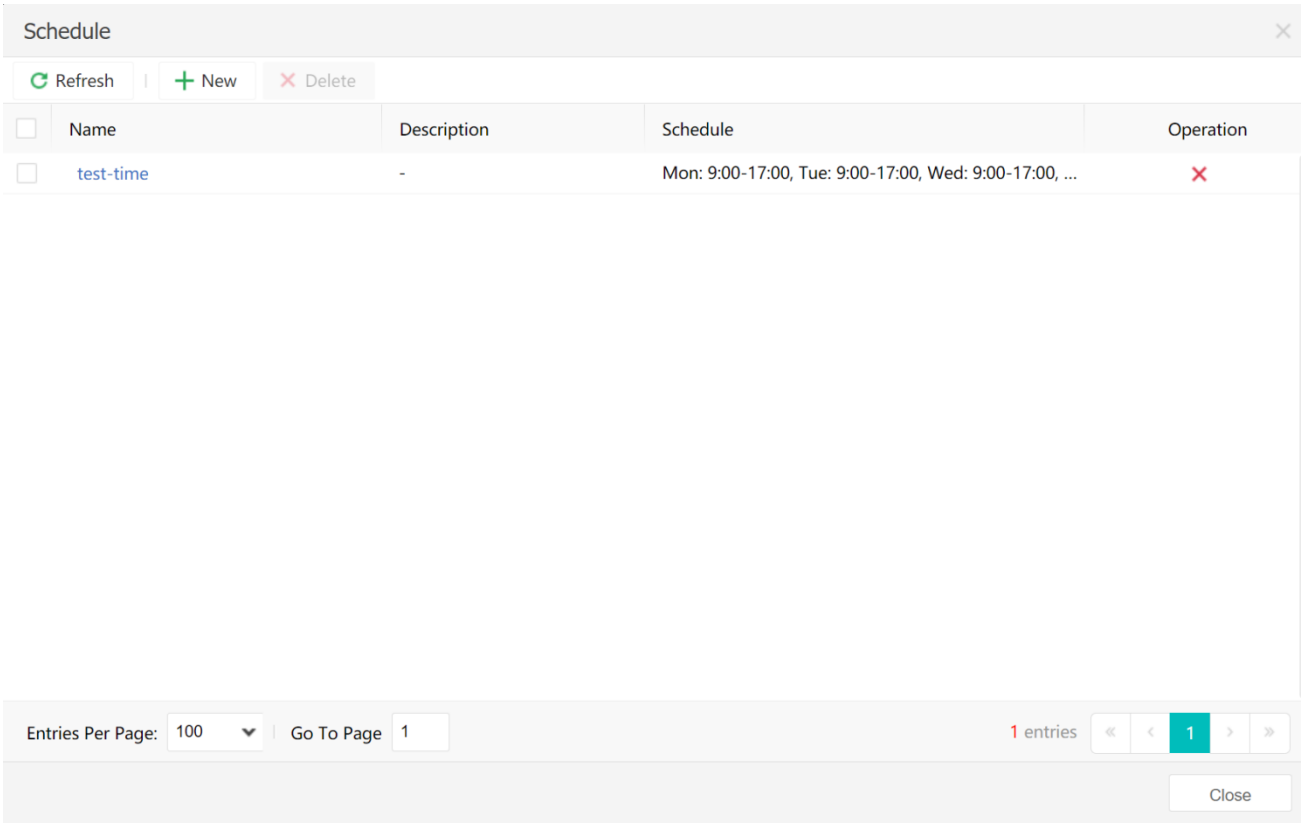


『More』 → 『Reset Hits』 resets the match times of policy-based routing.

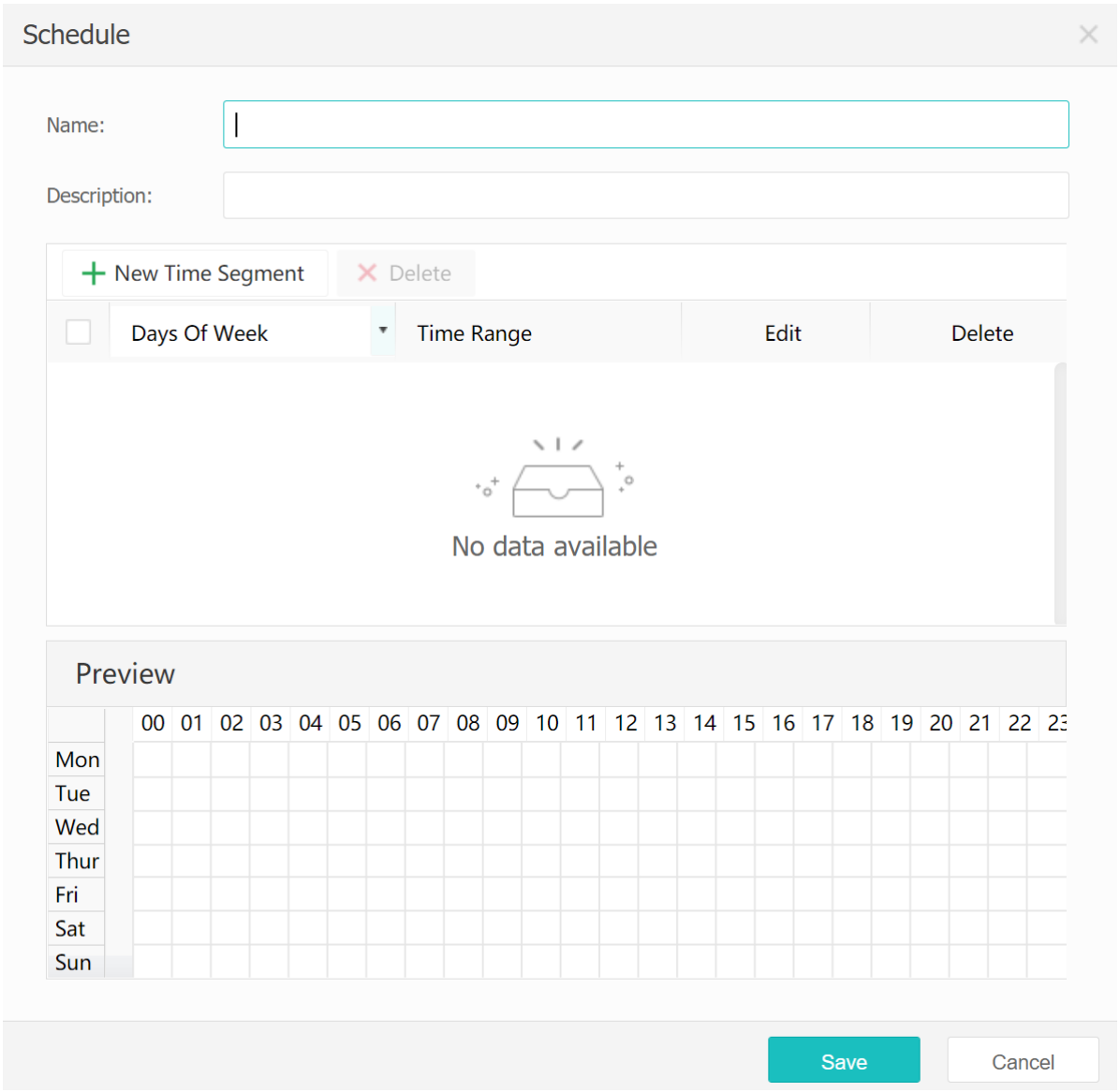
Click Reset Hits and the【Confirm】window will pop out. Click Yes to complete the operation.



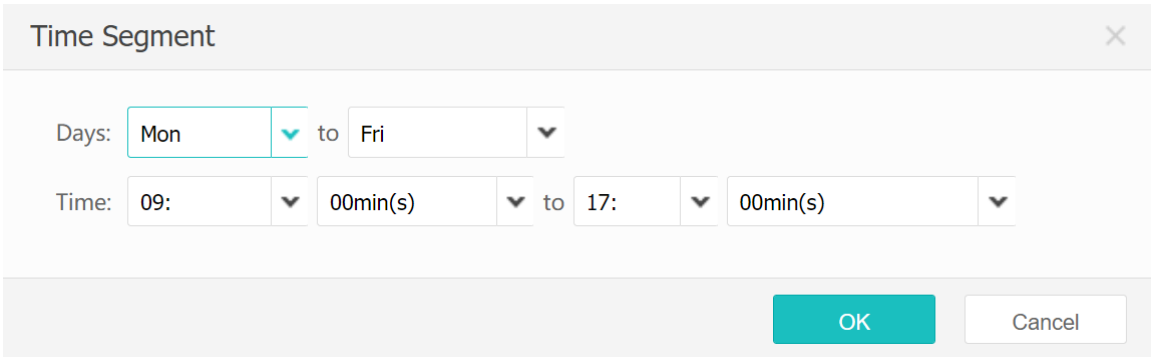
『More』→『Schedule』defines frequently used time range combinations. The policy-based routing will take effect only if the setting is within a certain time segment. Click『Schedule』and the 【Schedule】window will pop out.



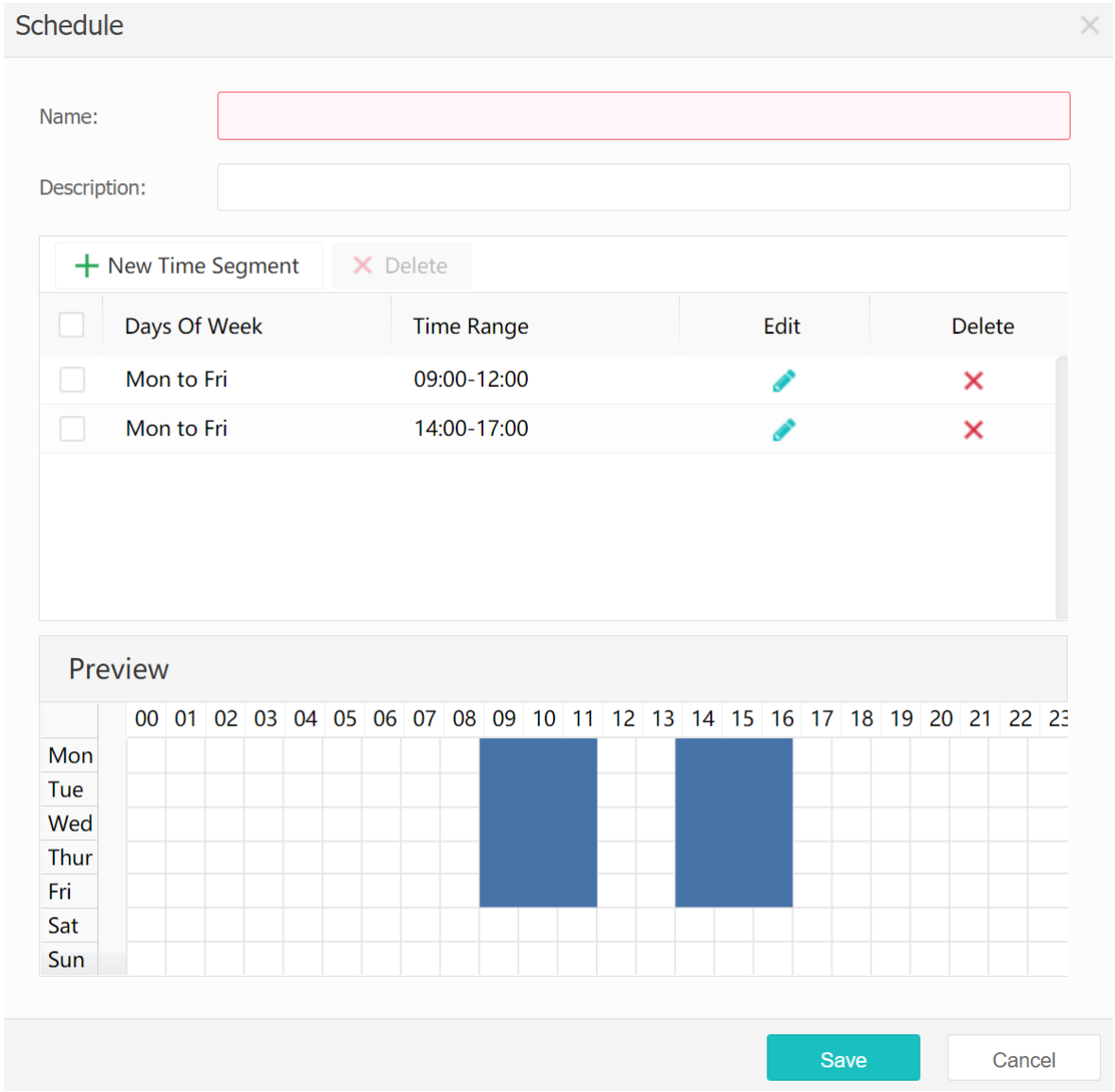
Click『New』and the new【Schedule】window will pop out as shown in the figure below.



Click New Time Segment and the【Time Segment】window will pop out. Set corresponding time.

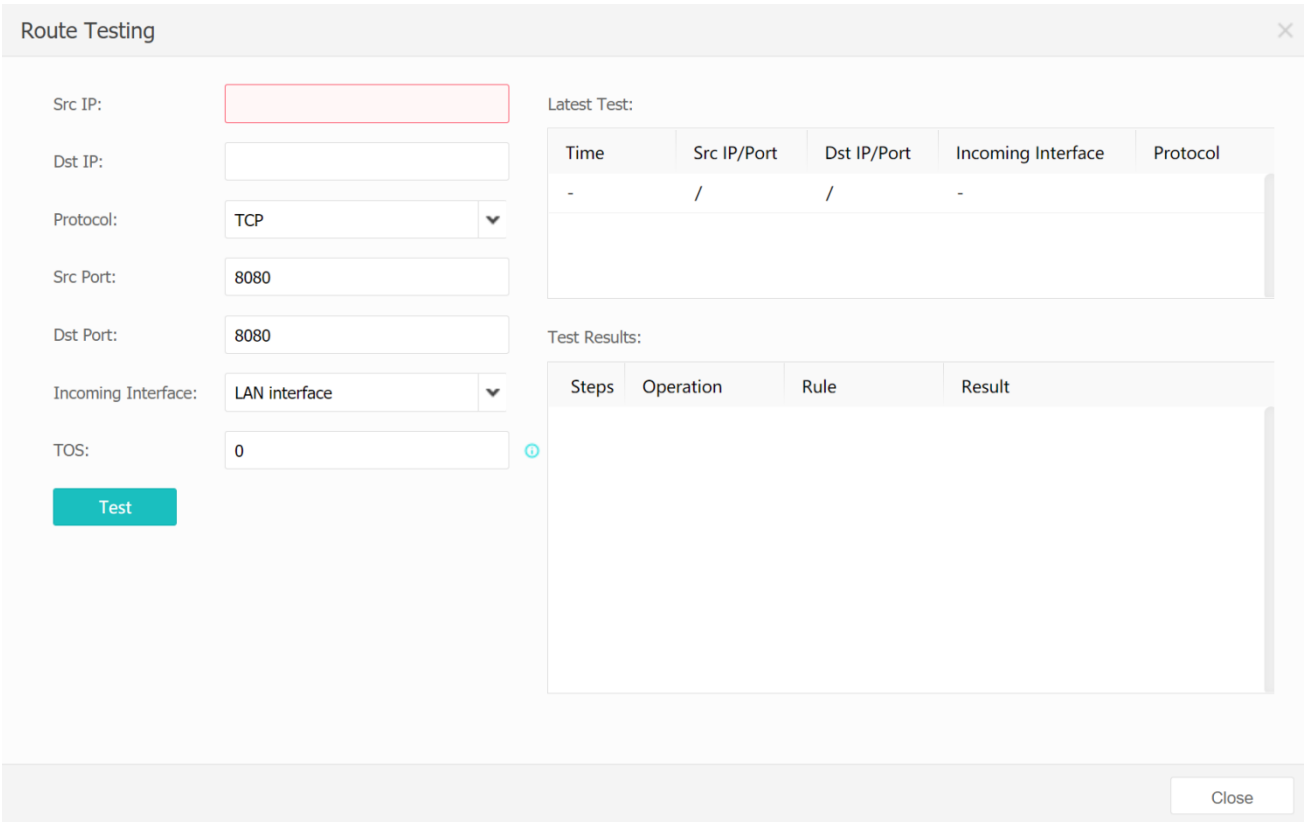


The configuration is shown in the following figure.



If the configured schedule needs to be modified, click the name of the corresponding schedule.

[Route Testing] tests the policy-based routing.



『Src IP』and『Src Port』set the source IP address for routing tests and port number in the case of TCP/UDP protocol respectively.

『Dst IP』and『Dst Port』set the destination IP address for routing tests and port number in the case of TCP/UDP protocol respectively.

『Incoming Interface』 selects the incoming interface that receives data.

『Protocol』 selects the protocol to be tested. If there is no needed protocol, please select 『Others』 to enter the protocol number.

『TOS』 differenciates the traffic in the application layer to provide for policy-based routing for different link selection, supporting app traffic diversion and policy-based routing of app signature.

Click Test and the routing test is conducted according to the configuration.

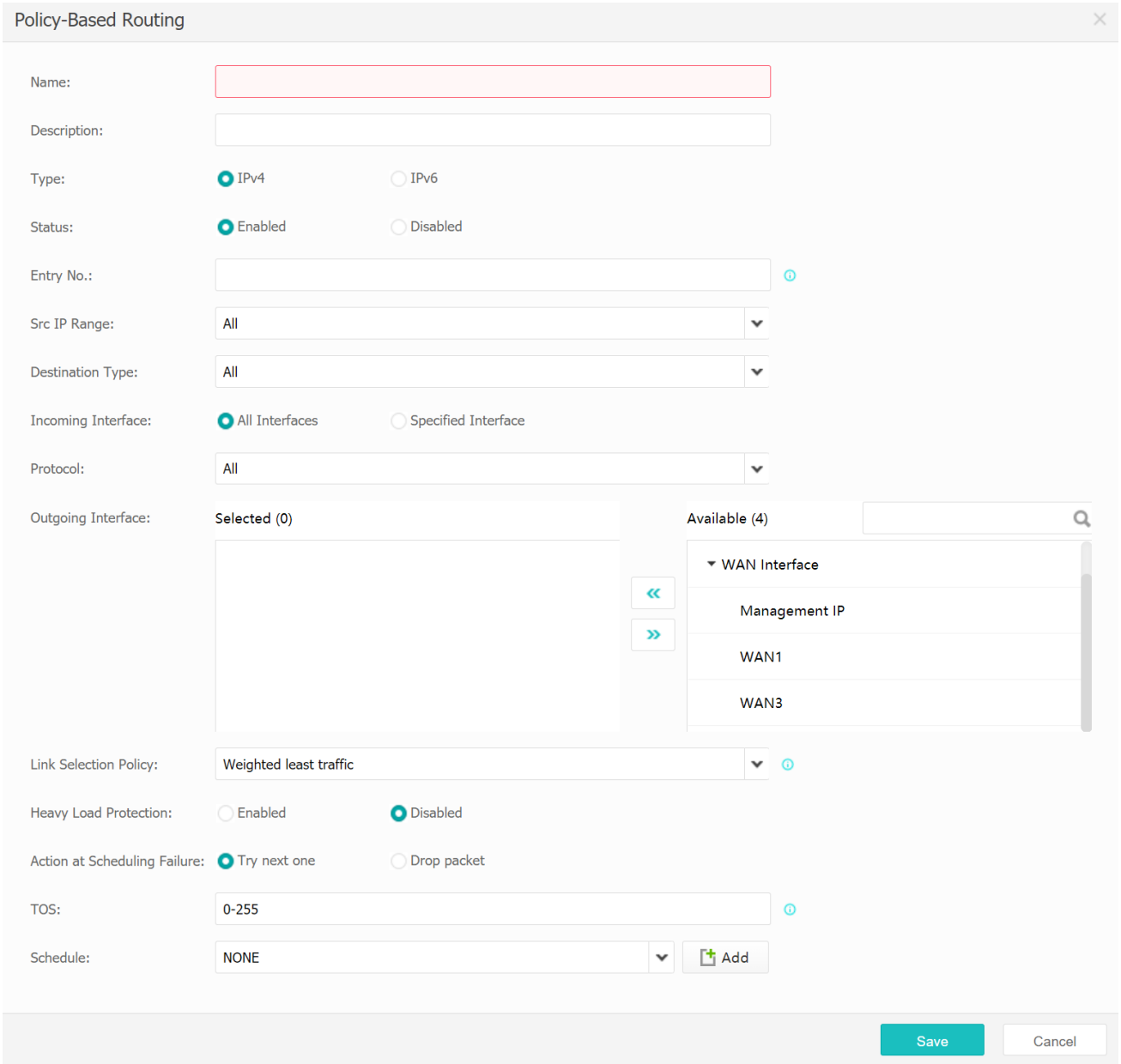
『Test Results』 shows the result of the policy-based routing test of this time.

『Latest Test』shows the result and time of the latest routing test.

8.1.1 Policy-based Routing

【Operation Procedure】

Click New and the【Policy-Based Routing】window will pop out for policy-based routing configuration.



『Type』selects IPv4 or IPv6.

『Status』sets the status of policy-based routing including [Enabled] and [Disabled].

『Entry No.』 is the number of this policy-based routing. The larger the number, the lower the priority.

『Src IP Range』 sets the matching source IP address for this policy-based routing. It could be All, IP Address or the IP range centrally defined in IP Database. When selecting IP Database, you can click New to directly build an IP Database.

『Destination Type』 refers to the destination type that internal network users visit, divided into destination address (All, IP Address, IP Database, ISP Database), domain name database and application signatures.

1. 『Destination Type』 → 『Dst IP』 sets the matching destination IP address for this policy-based routing. It could be [All], [IP Address], [User IP Address Range], [ISP IP Address Range]. The IP database can be configured in 『Objects』 → 『Databases』 → 『IP Database』 and the ISP database in『Objects』→『Databases』→『ISP Database』. Or click the corresponding New to build the corresponding database.

2. 『Destination Type』 → 『Domain Name Database』 refers to the database of a domain name which can be configured through『Objects』→『Databases』→『Domain Name Database』 or click the corresponding New to build the corresponding database. If a domain name that a user accesses is included in the domain name database referenced by the policy, the user's request to access the domain name will hit the policy.

3. 『Destination Type』 → 『Application Signatures』 has three app type options of [Video], [Games]、[Online Banking]. If user access is recognized as a type among them such video, the policy will be hit.

『Incoming Interface』 recieves the network interface of this packet and the default configuration is [All Interfaces] (including WAN interface and LAN interface). It also can be configured as [Specified Interface].

『Protocol』 sets the protocols that match this policy-based routing, including [All], [TCP], [UDP], [ICMP], [Others]. You can customize the source port and destination port range (TCP, UDP) or protocol number (others).

『Outgoing Interface』 sets the selected external network link when matching this policy-based routing.

『Link Selection Policy』 sets the applied routing policy including [Round robin]、[Bandwidth ratio]、[Weighted least traffic]、[Dynamic proximity]、[Weighted source IP hash] when matching this policy-based routing and using two or more links. Each policy is analyzed as follows:

1. [Round robin] schedules selected links in turn with equal opportunities.
2. [Bandwidth ratio] according to the bandwidth ratio of each link, the probability of selecting a link is proportional to the sum of the uplink and downlink bandwidth of the link.
3. [Weighted least traffic] selects the link with the smallest bandwidth usage ratio (current traffic/the sum of the uplink and downlink bandwidth).
4. [Dynamic proximity] detects RTT of a destination address in each link and selects the link with the smallest RTT according to that detected RTT.
5. [Weighted source IP hash] according to the bandwidth ratio of each link, the probability of selecting a link by a different source IP is proportional to the sum of the uplink and downlink bandwidth of the link.

『Heavy Load Protection』 sets whether routing is affected by the busy status of a link when matching this policy-based routing. When it is turned on, the busy link will not be selected and the link scheduling will fail if all the links in the rule are busy.

『Action at Scheduling Failure』 sets the action that is taken if the link scheduling fails when matching this policy-based routing. It is recommended to select Try next one.

『TOS』differenciates the traffic in the application layer to provide for policy-based routing for different link selection, supporting app traffic diversion and policy-based routing of app signature.

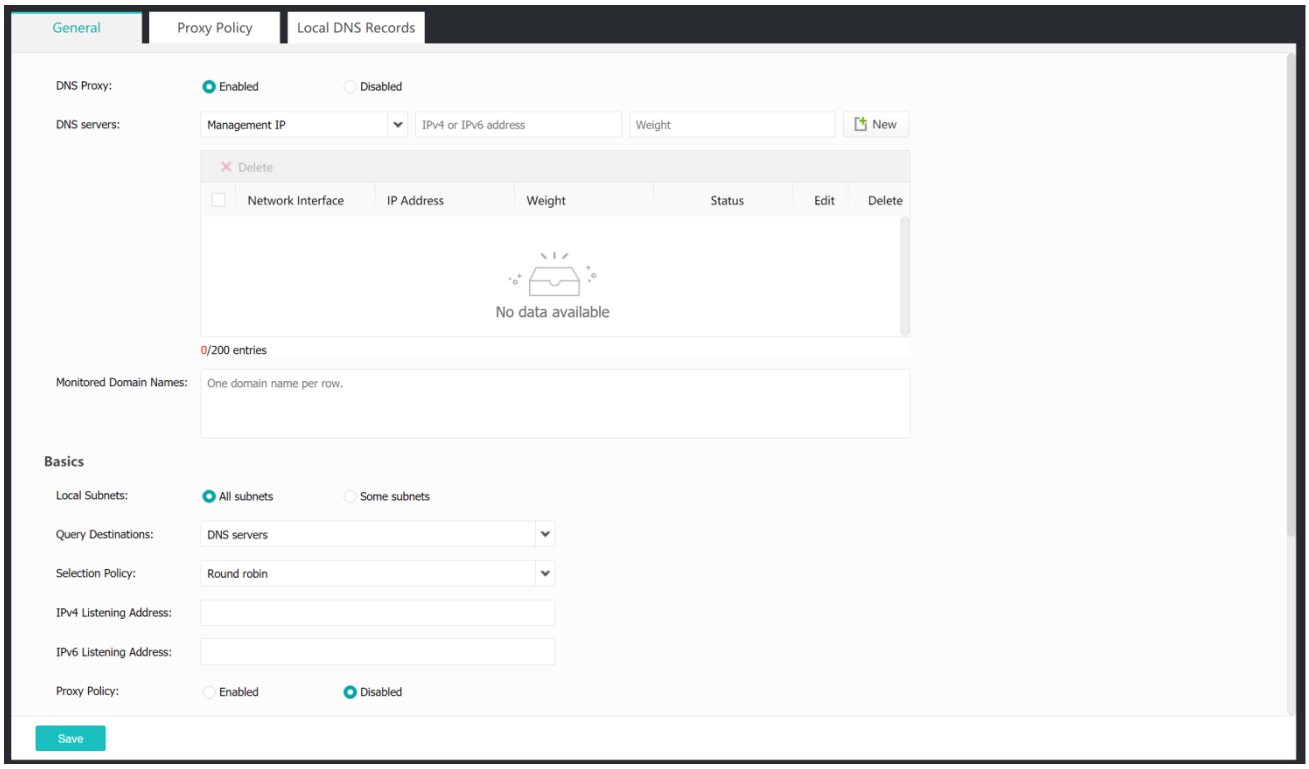
『Schedule』sets the time of this policy-based routing taking effect. The policy-based routing is not effective beyond the effective time. 『More』→『Schedule』defines frequently used time segment combinations. You can also click New on the right to create the corresponding configuration pop-up window.

8.2 DNS Proxy

8.2.1 General

【Operation Scenarios】

DNS proxy is used for setting the DNS server address. The DNS server here is the DNS server address that an ADC connects when needing domain name resolving. It can forward DNS requests on behalf of the local PC.



【Operation Procedure】

Enable DNS proxy to act on the DNS request of the local PC.

『DNS servers』configures the DNS server of the system network interface. You can configure the DNS server and weight of each network interface. The ADC itself only uses the first three DNS servers. Select the corresponding network interface and fill in the IP address and weight of the corresponding DNS server. Click New to add to the list of DNS servers below, click  to modify the existing DNS server, and click  to delete the selected DNS server.

『Monitored Domain Names』determines the validity of DNS by monitoring domain names to perform DNS proxy.

『Local Subnets』 sets the local network segment that needs to provide DNS proxy. Options include [All subnets] or [Some subnets].

『Query Destinations』 performs proxy on [All DNS requests], [DNS servers], [Specified domain name]. [All DNS requests]: performs proxy for the DNS query request of any address.

[DNS servers]: performs proxy for all DNS queries of DNS servers, and all DNS queries of DNS server addresses which are monitoring addresses. [Specified domain name]: performs proxy for DNS queries in scheduling policy or local network record before matching. When the proxy target range is [All DNS requests], you need to specify "proxy local network segment" as part of the network segment. Otherwise, the intelligent DNS will be invalid.

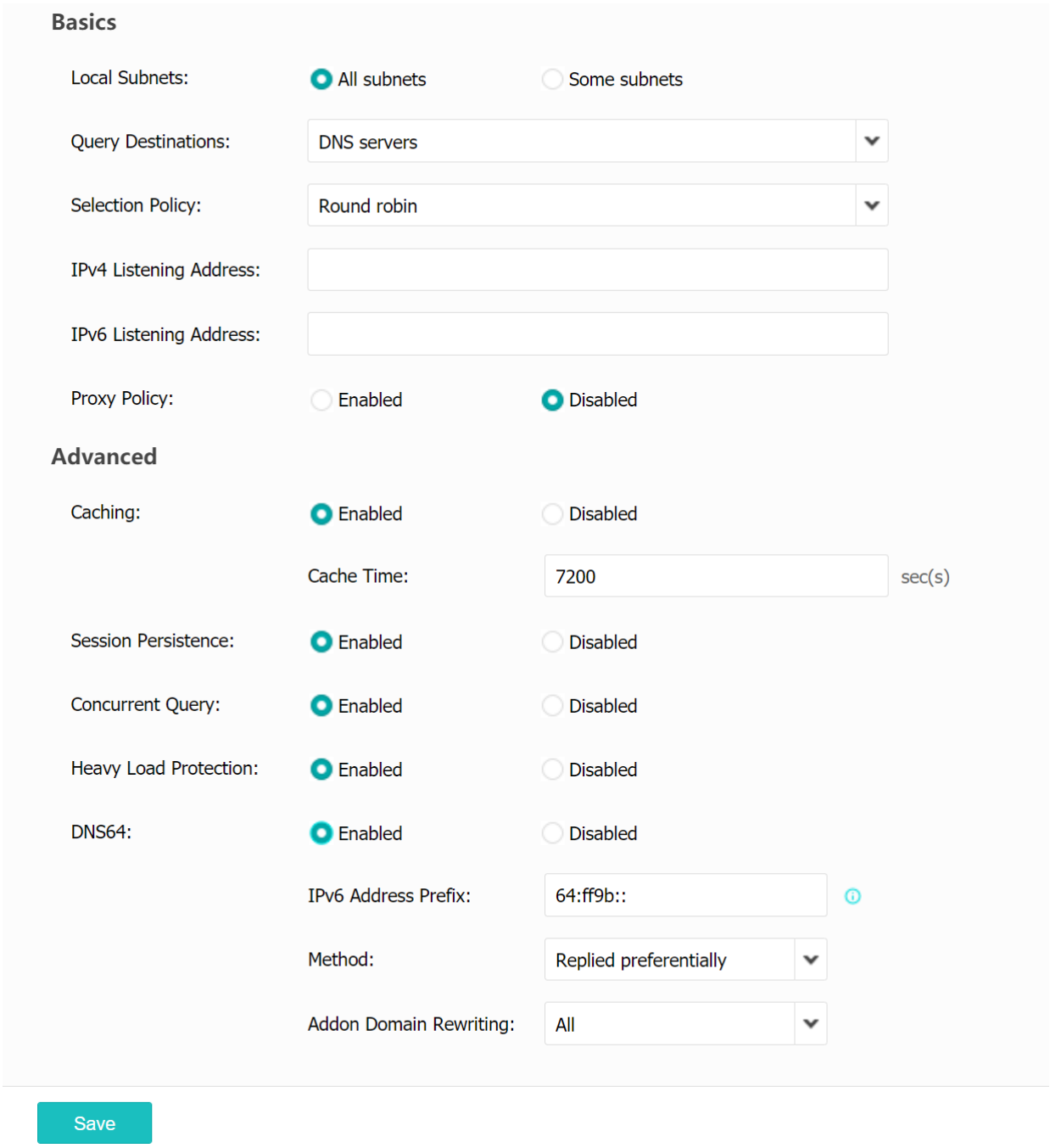
『Selection Policy』 configures the DNS selection policy of DNS proxy. Include [Round robin], [Weighted round robin], [Weighted least traffic], [Priority].

1. [Round robin] takes turns to select DNS servers in the DNS server list for equal opportunities.
2. [Weighted round robin] selects the DNS server in the DNS server list according to the weight ratio of the DNS server.
3. [Weighted least traffic] selects the DNS server from the link with the least traffic according to the weight.
4. [Priority] always selects the server with the highest weight. Only when the DNS server with a higher weight is offline or busy will the DNS server with a lower weight be selected.

After setting the『IPv4 Listening Address』, LAN users can set the DNS server as the listening address.

After setting the『IPv6 Listening Address』, LAN users can set the DNS server as the listening address.

『Proxy Policy』 schedules the access of a specific user to a specified server.



Enabling『Caching』will cache the LDNS response. When receiving the DNS query later, the cache will be searched first. If the cache exists, the client will be answered with the cache. 『Cache Time』refers to the timeout of DNS proxy cache.

『Session Persistence 』enables session persistence by default. When ADC receives one DNS request source address, session persistence needs to be turned off, such as the ADC proxy LAN DNS server scenario.

『Concurrent Query』 forwards the query to all available LDNS when receiving the client query, and replies to the client with the first valid reply. (priority policy takes precedence over concurrent query).

『Heavy Load Protection』configures whether routing is affected by the busy status of the link when setting DNS proxy. When it is enabled, if a link is busy, the link will not be selected; if all links in the rule are busy, the DNS server bound by the link will be randomly scheduled.

『DNS64』 solves the problem that the LAN IPv6 users cannot access the WAN IPv4 portal normally. Refer to Section 2.3.9.2 for the scenario.

『IPv6 Address Prefix』 : 64:ff9b:: by default. For example, the IP of a record by A is 12.5.1.200 through the DNS proxy query of ADC;
ADC adds the IPv6 prefix 64:ff9b:: and returns the AAAA record 64:ff9b::c05:1c8 to client. Note that the prefix should not conflict with the IPv6 address on the network interface. The default value can be used.

『Method』

a. Only A record

ADC queries DNS server for domain name A record, but not for AAAA record.

Applicable scenario: ADC has no IPv6 Internet access link. All need to go through the IPv4 link to access the Internet.

b. AAAA record preferred

ADC first queries the DNS server for the domain name AAAA record and then queries the A record. The client first accesses the Internet through the IP (the real IPv6 address of the website) of the AAAA record.

Applicable scenario: ADC has IPv6 Internet access links. Both v4 and v6 links can access the Internet. The use of the v6 link is preferred.

c. Response preferred

ADC queries domain name AAAA record and domain name A record at the same time, and uses the one that responds first to access the Internet.

Applicable scenario: ADC has iPv6 Internet access link. Both v4 and v6 links can access the Internet. There is no intention to specify a link.

『Addon Domain Rewriting』

a. Only ipv4

Addon domain removes AAAA record with only A record included and A record has been rewritten (add prefix IPv6);

b. Only ipv6

Addon domain removes A record with only AAAA record included (no rewriting)

c. All

Addon domain includes both A (rewritten) record and AAAA record (no rewriting) (add prefix IPv6);

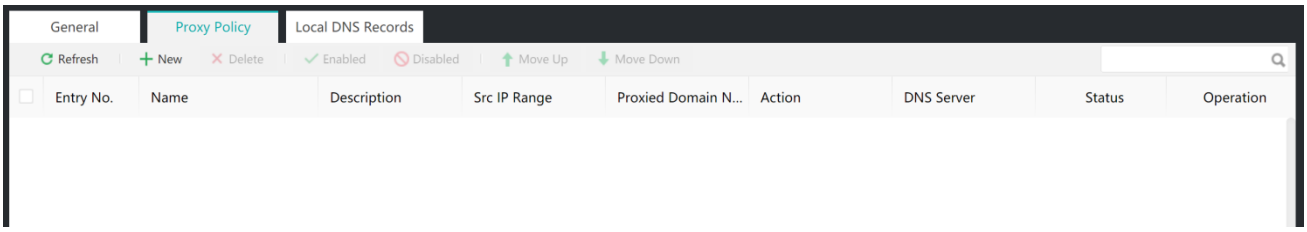
d. Disabled

Addon domain is not rewritten.

8.2.2 Proxy Policy

【Operation Scenarios】

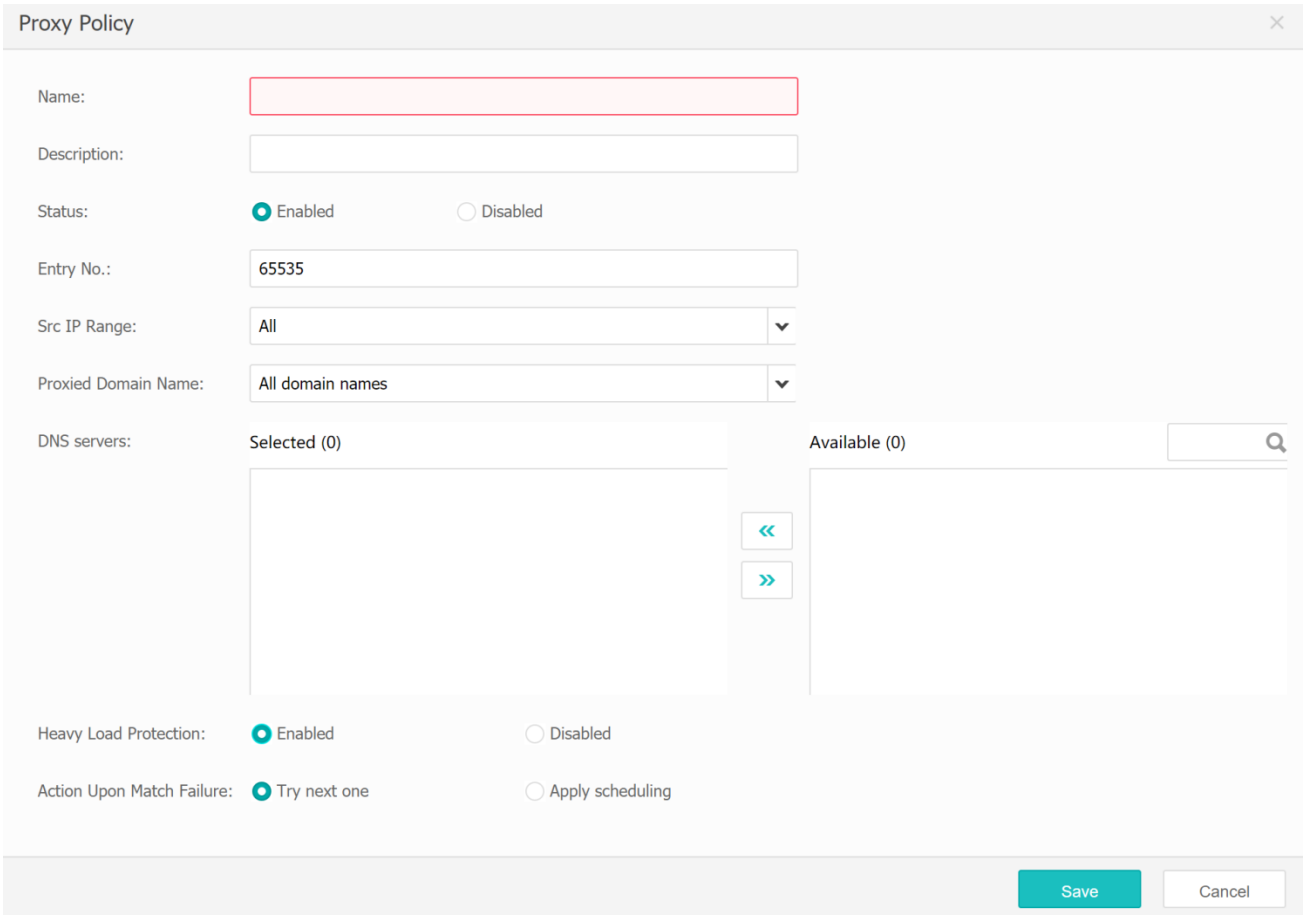
『Proxy Policy』 schedules the access of a specific user to a specified server.



【Operation Procedure】

Click Enable to make the selected proxy policy effective.

Click New to create a new proxy policy. The proxy policy configuration page is shown in the following figure:



『Status』 enables proxy policy when clicking [Enabled] and disables it when clicking [Disabled].

『Entry No.』 determines the priority of the proxy policy. The larger the value, the lower the priority.

『Src IP Range』selects the source IP range that enables the scheduling policy. Options include [All], [IP Address] and [IP Database] (can be added directly on the interface).

『Proxied Domain Name』 configures the destination domain name database that matches the proxy policy. Options include [All domain names], [Specified domain name] and [Domain name database] (can be added directly in the interface).

『DNS Servers』 specifies the DNS server which returns the result for the proxy policy.

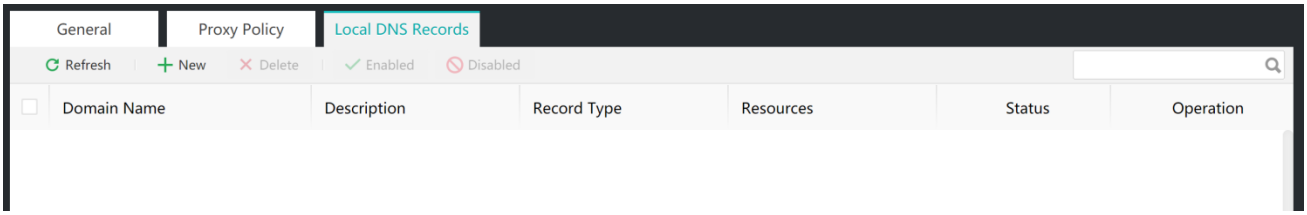
『Heavy Load Protection』 sets whether to allocate links according to the link's busy status.

『Action Upon Match Failure』refers to the processing method when the DNS server in the list fails. [Try next one] skips this rule to match the next policy. [Apply scheduling] always returns the DNS server in the list.

8.2.3 Local DNS Records

【Operation Scenarios】

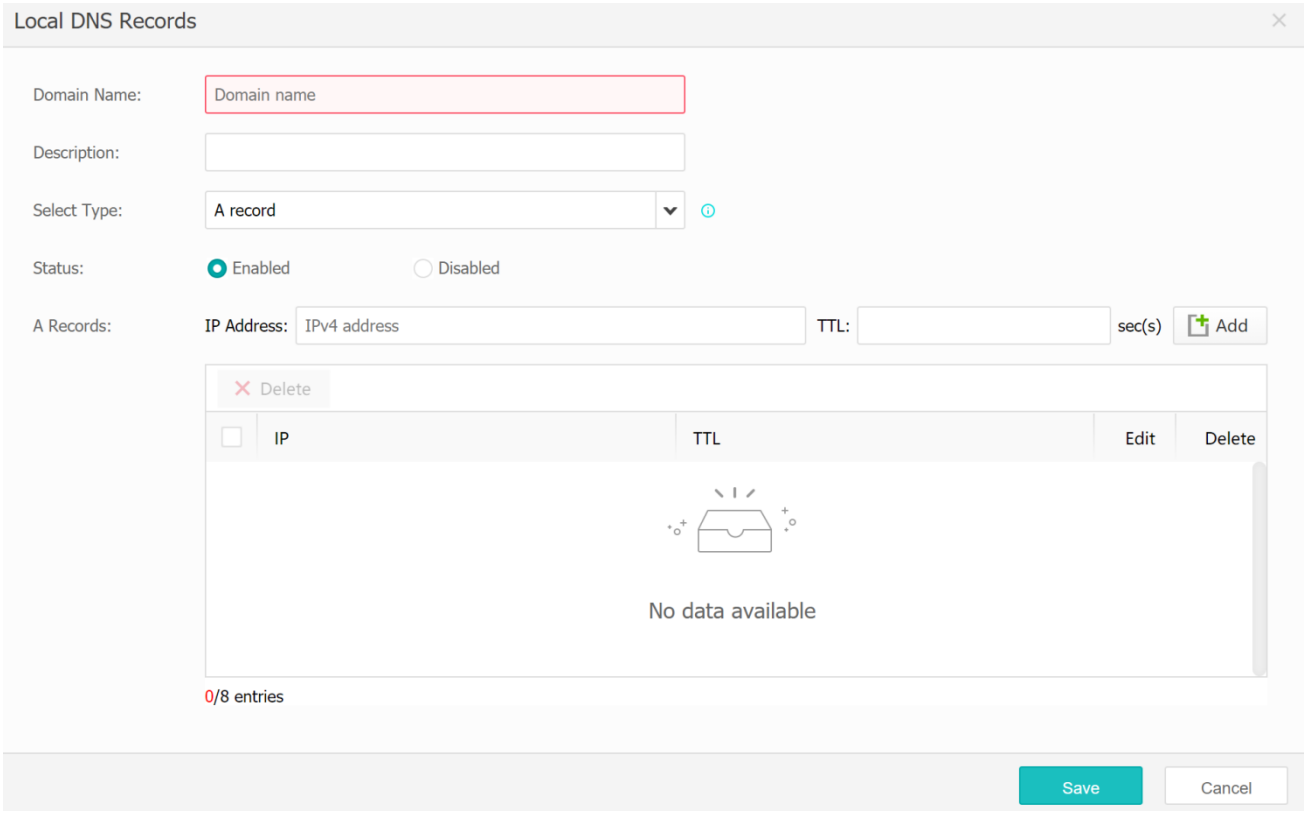
『Local DNS Records』adds DNS entries on the device for DNS resolution, which can directly return the corresponding address on behalf of the local PC.



【Operation Procedure】

Click Enable to make the selected local DNS record effective.

Click New to create a new Local DNS record. The configuration page of【Local DNS Records】is shown in the following figure:



『Status』 configures the [Enabled] and [Disabled] of the DNS record.

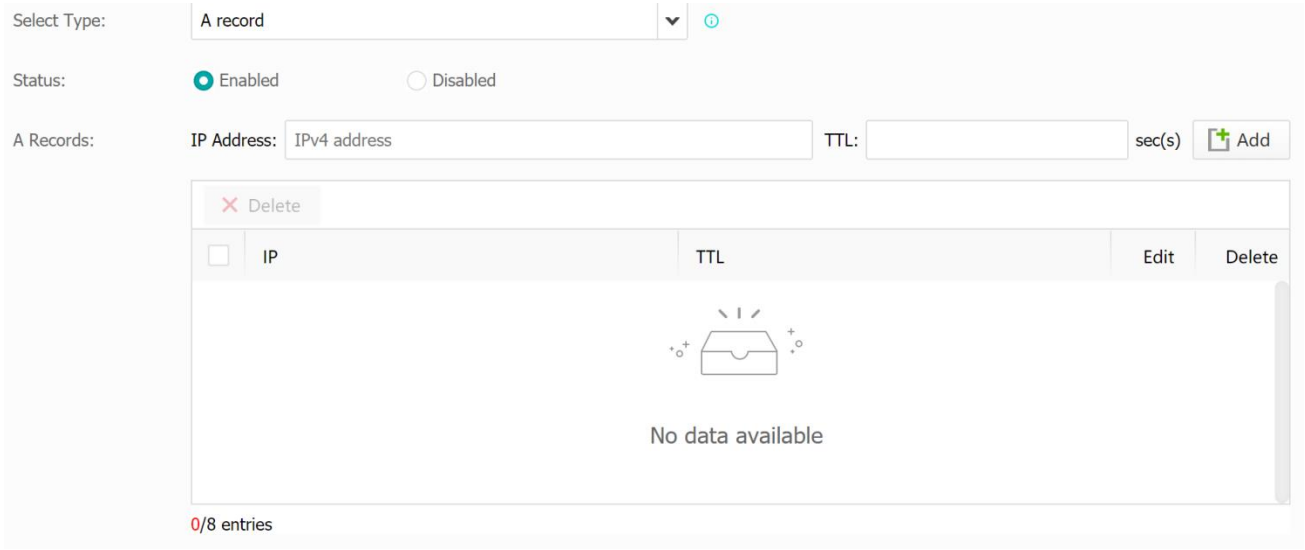
Click Add to configure the DNS record.

Under『Select Type』are optional DNS record types, including [A record], [AAAA record], [MX record], [CNAME record] and [TXT record].

A record (specifies the corresponding IPv4 address record of a specific domain name)

『IP』 configures the corresponding IP address of the domain name of A record.

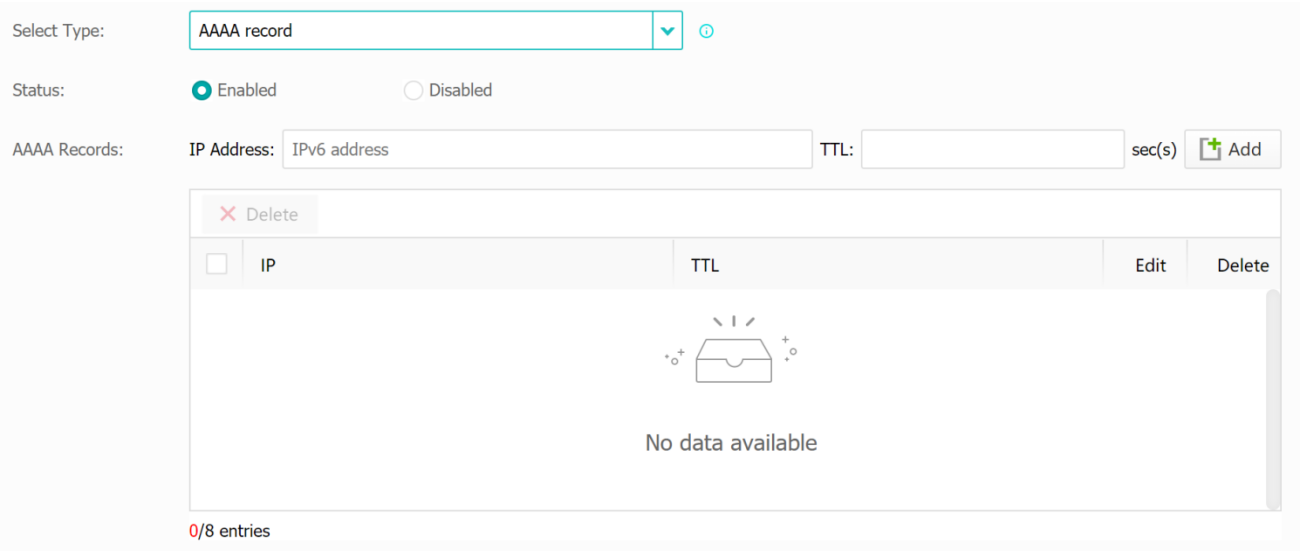
『TTL』 configures the cache time of local DNS of A record (unit: seconds).



AAAA record (specifies the corresponding IPv6 address record of a specific domain name)

『IP』 configures the corresponding IP address of the domain name of AAAA record.

『TTL』 configures the cache time of local DNS of AAAA record (unit: seconds).

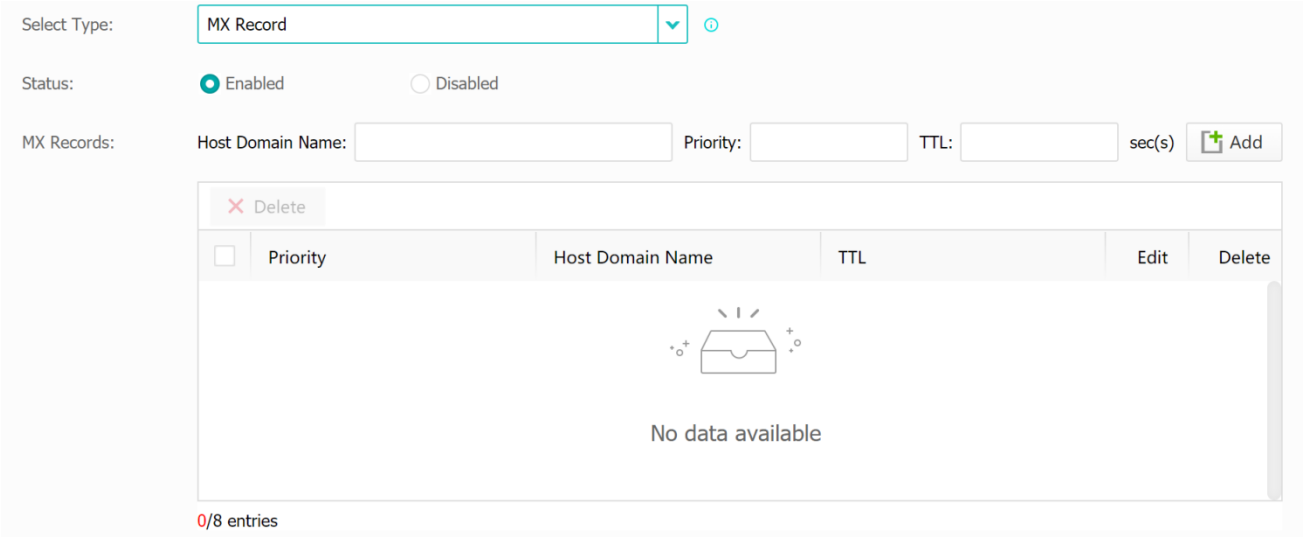


MX record (mailing exchange record to locate mailing server when e-mail system sends mail)

『Host』 configures the domain name of MX record.

『Priority』 sets the priority of MX record in the list.

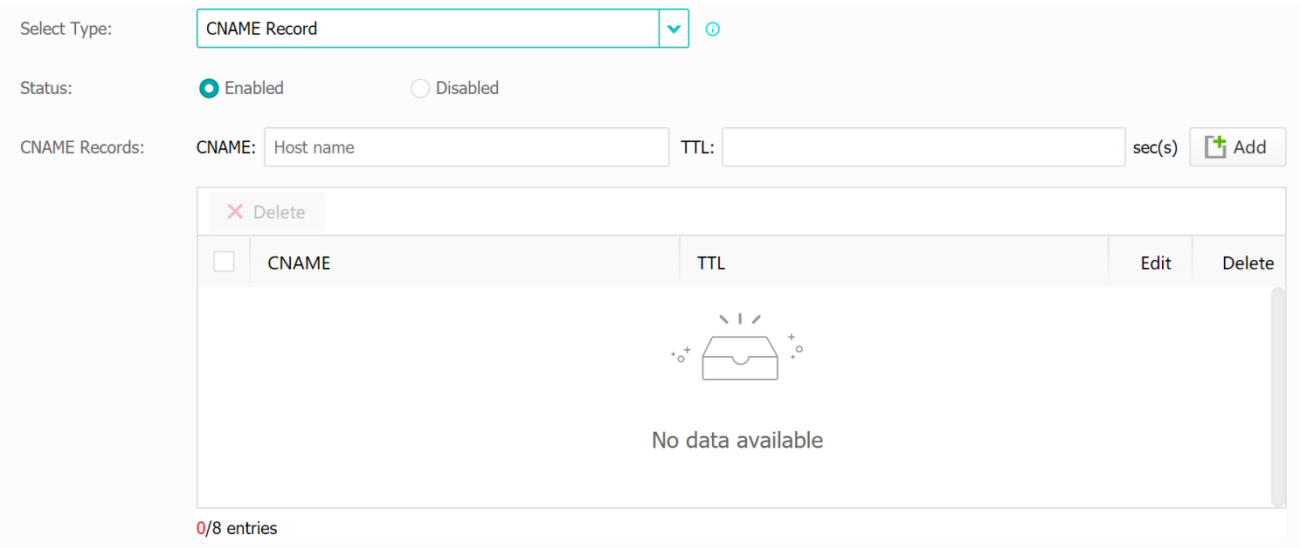
『TTL』 configures the cache time of local DNS of MX record (unit: seconds).



CNAME record (with the alias of canonical name, allows you to map multiple names to a computer)

『CNAME』 configures the domain name of CNAME record.

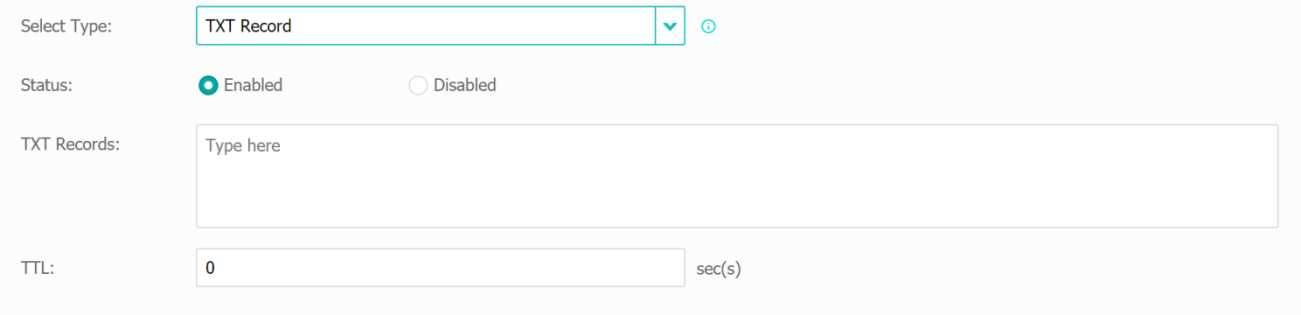
『TTL』 configures the cache time of local DNS of CNAME record (unit: seconds).



TXT record (generally refers to the description set for a hostname or domain name)

『TXT Value』 configures the corresponding TXT value of the domain name of the TXT record.

『TTL』 configures the cache time of local DNS of TXT record, in seconds.



Chapter 9 Global Load Balancing

9.1 Local Intelligent DNS Resolution

9.1.1 Configuring DNS server

【Operation Scenarios】

When using ADC as a DNS server for domain name resolution, it is needed to configure the listening address, that is, the address pointed to by the NS record of the domain name. Generally, the default listening address is port 53 and some basic parameters need to be configured.

【Prerequisites】

Check the NS record to ensure that the domain name to be resolved has pointed NS record to the ADC's monitoring IP address, which is generally set by the domain name provider.

For example: domain name: www.abc.com, ADC's monitoring IP addresses: 1.1.1.1 (China Telecom), 2.2.2.2 (China Unicom)

Record Type	Host Record	Resolution Line (Carrier)	Record Value
NS	www	Default	NS1.abc.com
A	NS1.abc.com	Default	1.1.1.1
NS	www	Default	NS2.abc.com
A	NS2.abc.com	Default	2.2.2.2

Generally, different domain name providers fill in the preceding table in the same format.

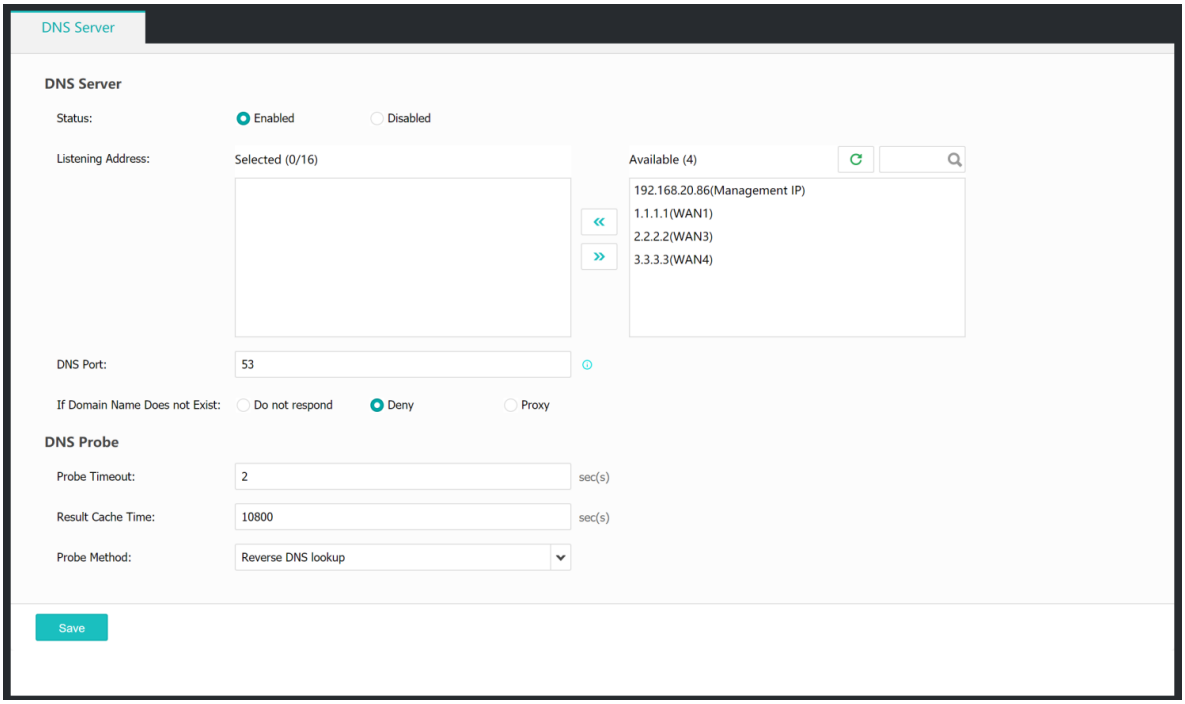
Test method: Test by running the **nslookup** command:

Perform domain name resolution for the ADC's monitoring IP address: 172.10.10.60.

Attention: The NS record changed by the domain name provider takes effect after about 2 hours or 10 minutes (at a quick speed). The time spent updating the NS record worldwide is 24 hours at least.

【Operation Procedure】

Choose『Global Load Balancing』-> 『DNS Server』and select the IP address to be monitored, as shown in the following figure.



For other basic parameters, keep the values as default. If there are special needs, they can be set according to the requirements. The specific explanation is as follows:

『If Domain Name Does not Exist』: Select [Do not respond], [Deny], or [Proxy] to configure a domain name query for the DNS server if the domain name does not exist. If you select [Proxy], when the device receives a query request for the DNS server without the domain name, this request is forwarded to the [DNS Proxy] module for processing.

[Probe Timeout]: configures the timeout during which the DNS server detects the local DNS response speed of the client.

[Result Cache Time]: configures the cache time for results of the local DNS response speed of the client, which are detected by the DNS server (unit: seconds).

[Probe Method]: configures a method for detecting the local DNS response speed of the client based on the DNS server, and includes [DNS root lookup], [Reverse DNS lookup], and [Ping mode]. [DNS root lookup]: indicates that the response time is detected by performing a root query on the local DNS of the client. [Reverse DNS lookup]: indicates that the response time is detected by performing a reverse query on the local DNS of the client. [Ping mode]: indicates that the response time is detected by pinging the local DNS.

9.1.2 Configuring Domain Name Release

9.1.2.1 Local DNS Record

【Operation Scenarios】

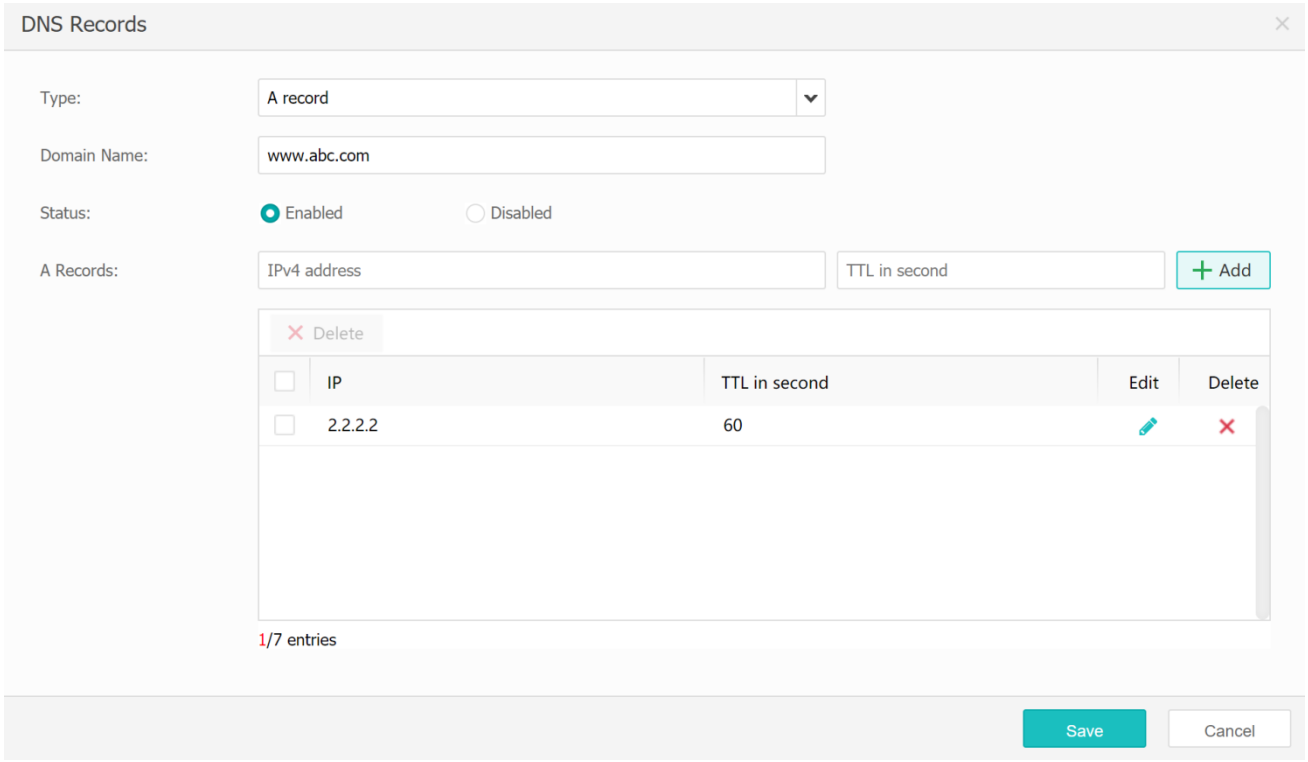
Generally, DNS records are records for resolution that is performed when a local single site equipped with a port uses an ADC as a DNS server, including A records, MX records, NS records, SRV records, CNAME records, TXT records, PTR records, SOA records, and AAAA records.

【Operation Procedure】

Add corresponding records based on your needs. The feature and configuration of each record are as follows:

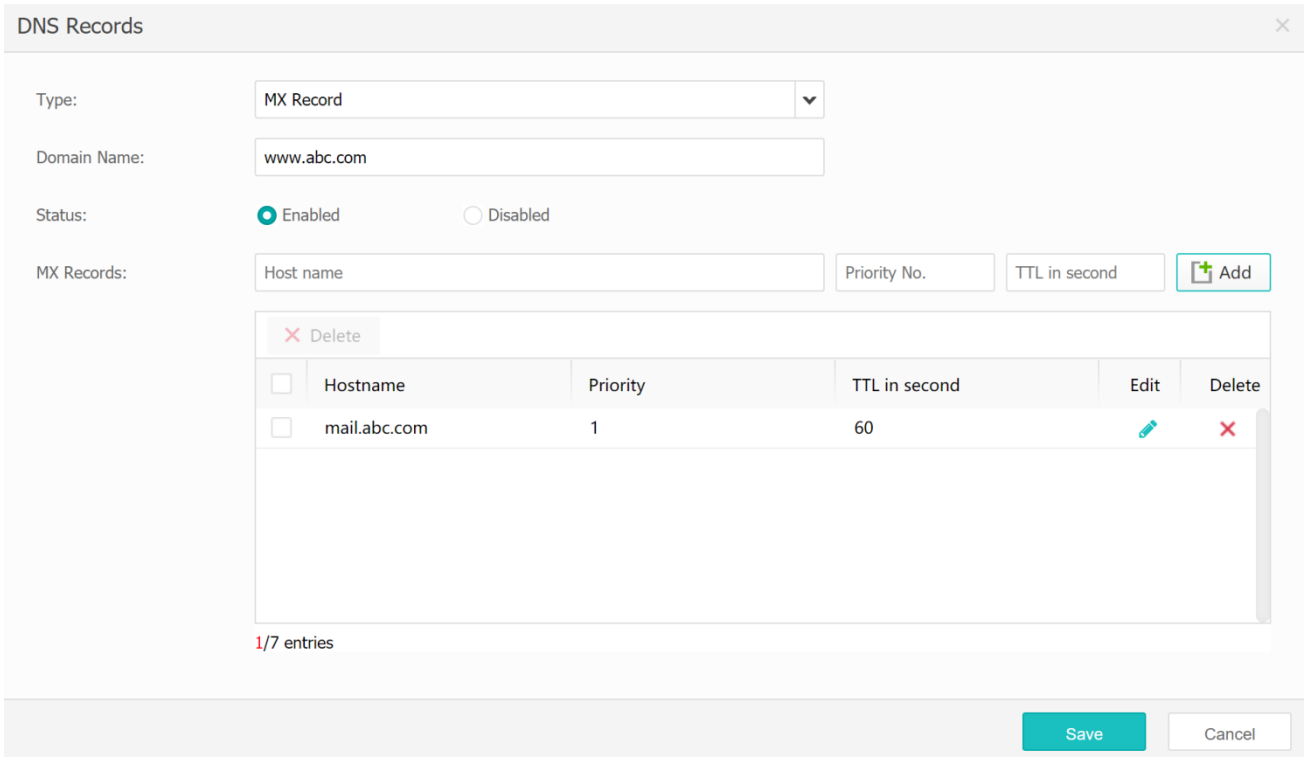
A Record

The A record specifies the IPv4 address record of a specific domain name.



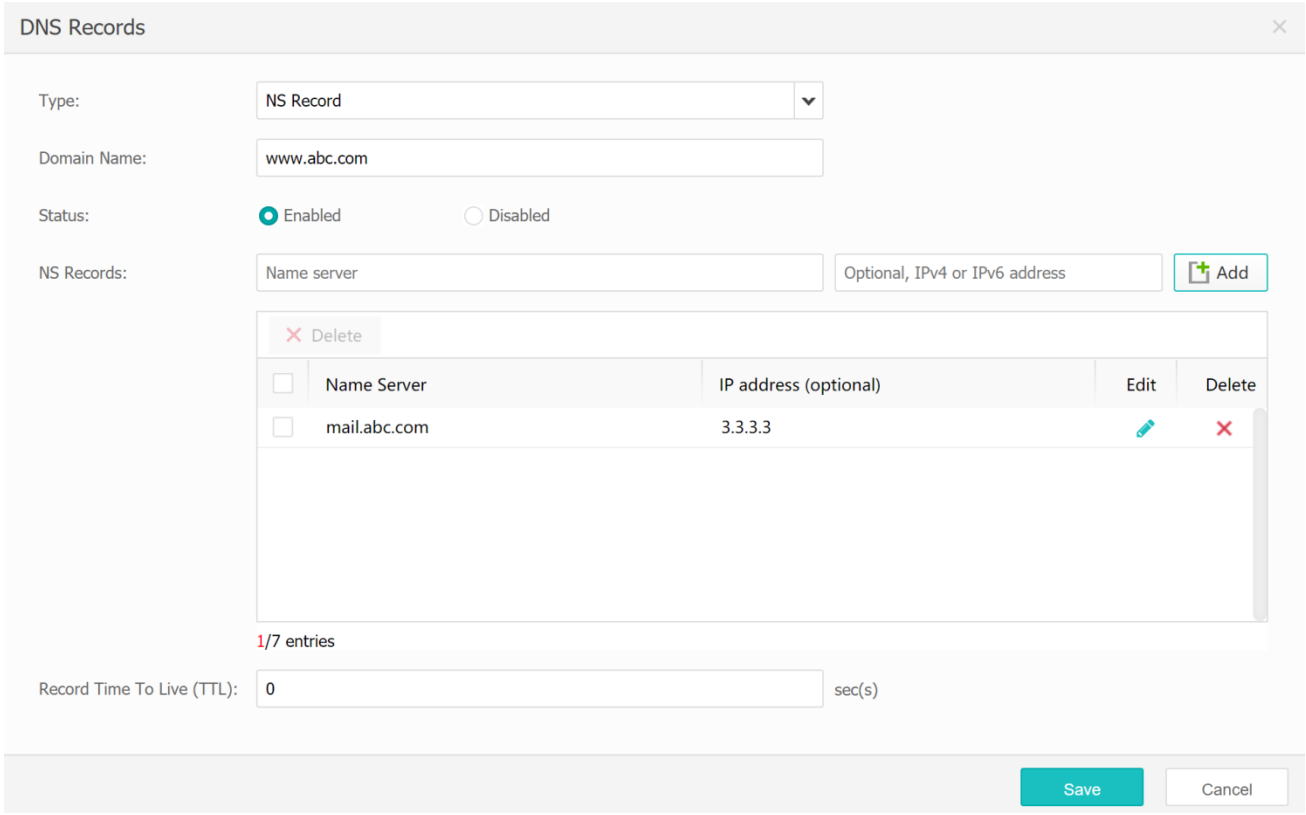
MX Record

The MX record is used to define mail exchange, which helps emails be successfully sent to your mail server.



NS Record

The NS record refers to a DNS server record that specifies a DNS server based on which resolution is performed on the specific domain name.



SRV Record

The SRV record is a resource record that is available for the database of a DNS server. It provides the information about which computer the service belongs to. In general, this record type applies when you configure the Microsoft Active Directory.

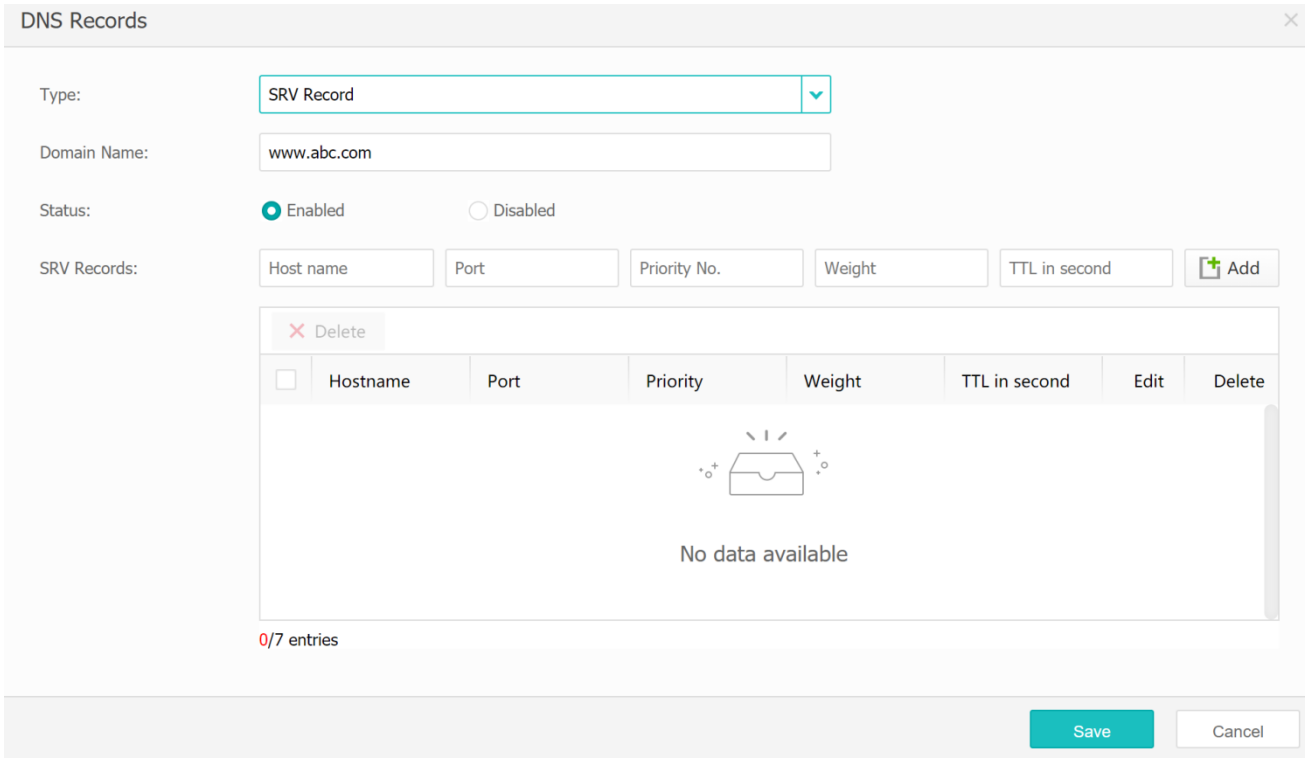
The SRV record is specified based on the following standard format:

Service.Protocol.Domain Name

Assume that the service is _http, the protocol is _tcp, and the domain name is abc.com. The SRV record is specified as follows:

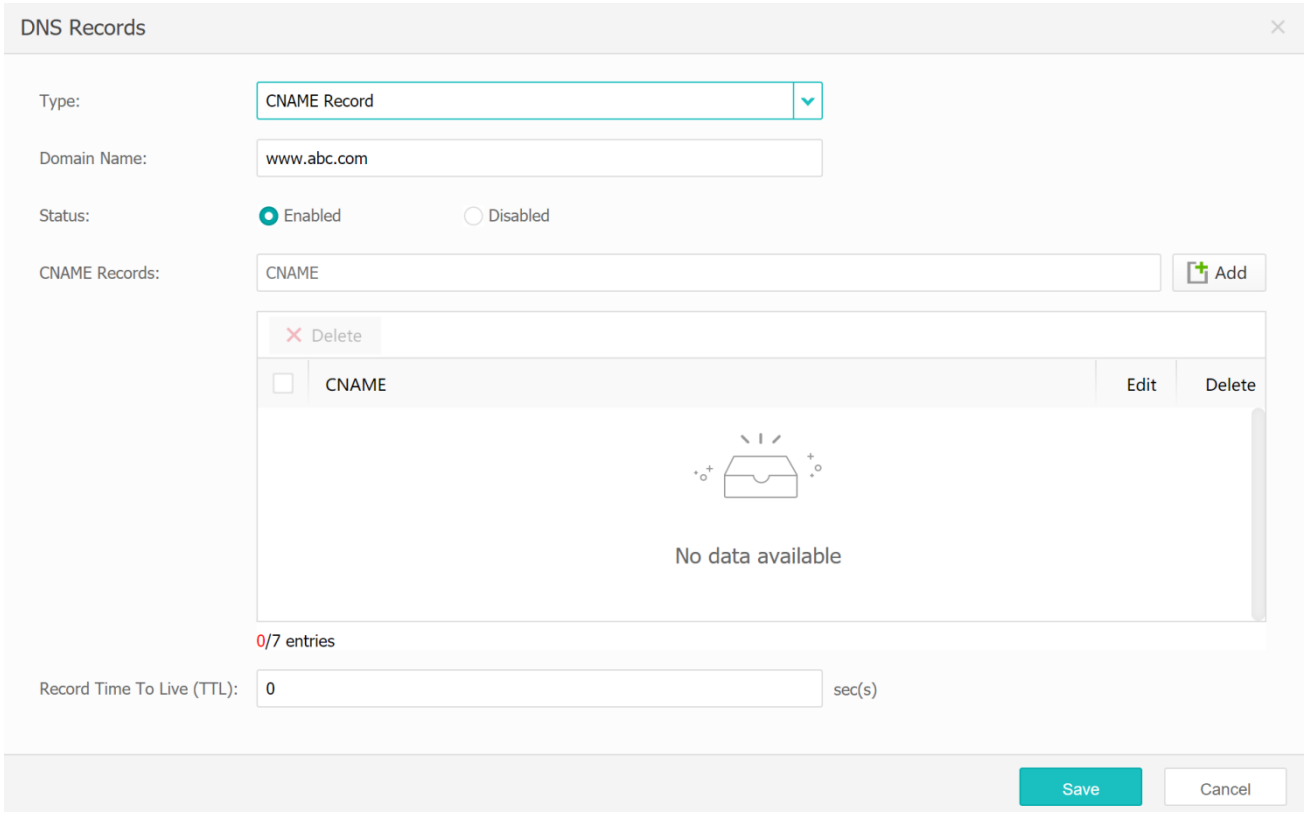
_http._tcp.abc.com

Attention: Both the service and the protocol are prefixed with an underline (_) and a comma (.) is added between the service and protocol. These symbols are necessary for this format.



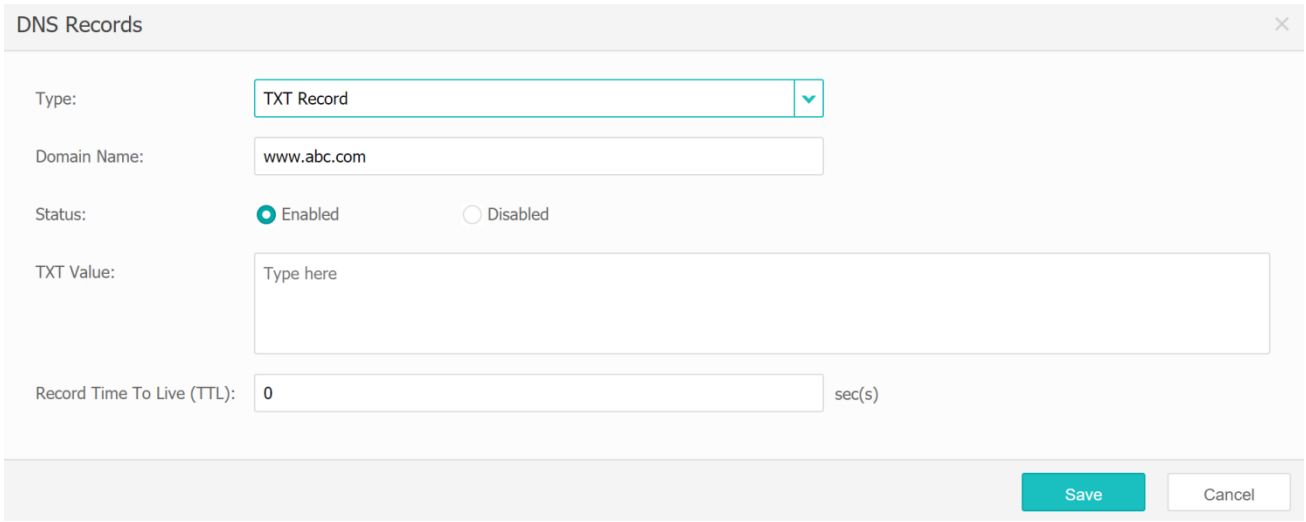
CNAME Record

The CNAME record with the alias of canonical name allows you to map multiple names to a computer.



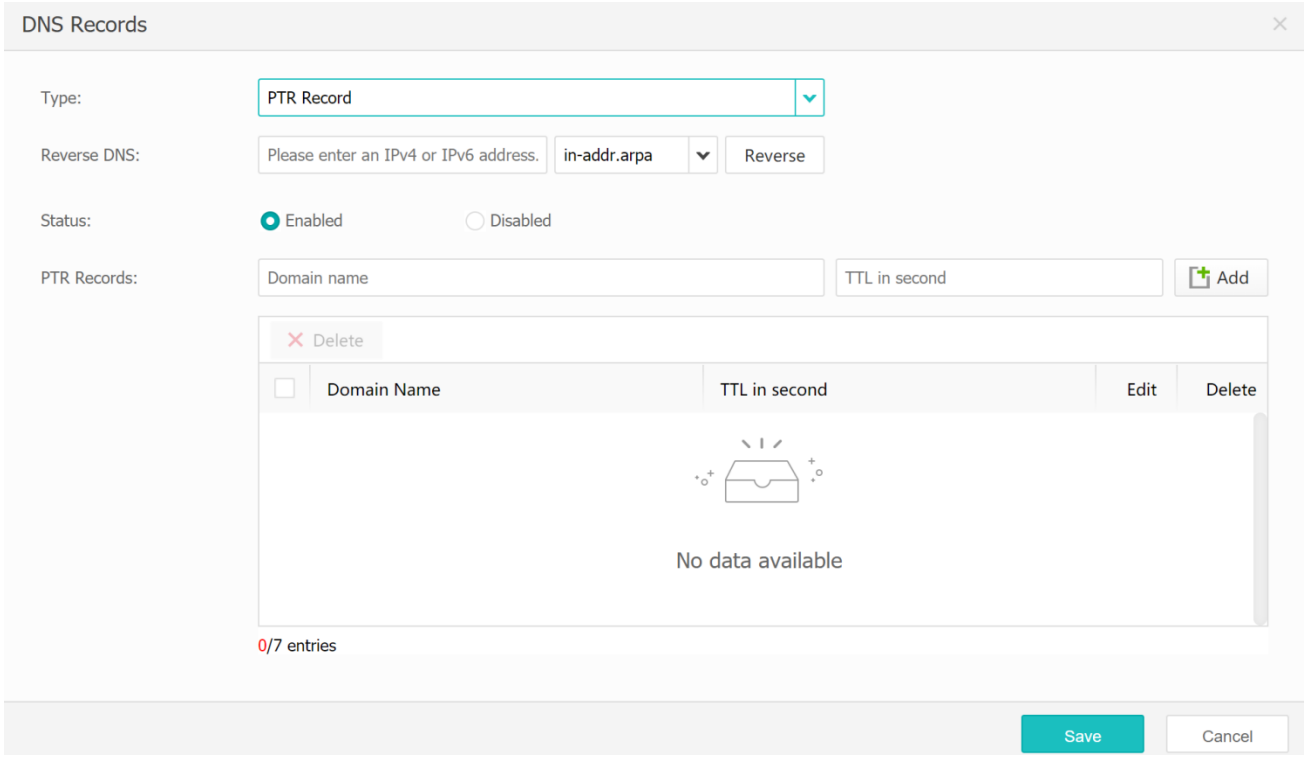
TXT Record

The TXT record provides the instructions when you configure a hostname or domain name,and is often used in combination with emails.



PTR Record

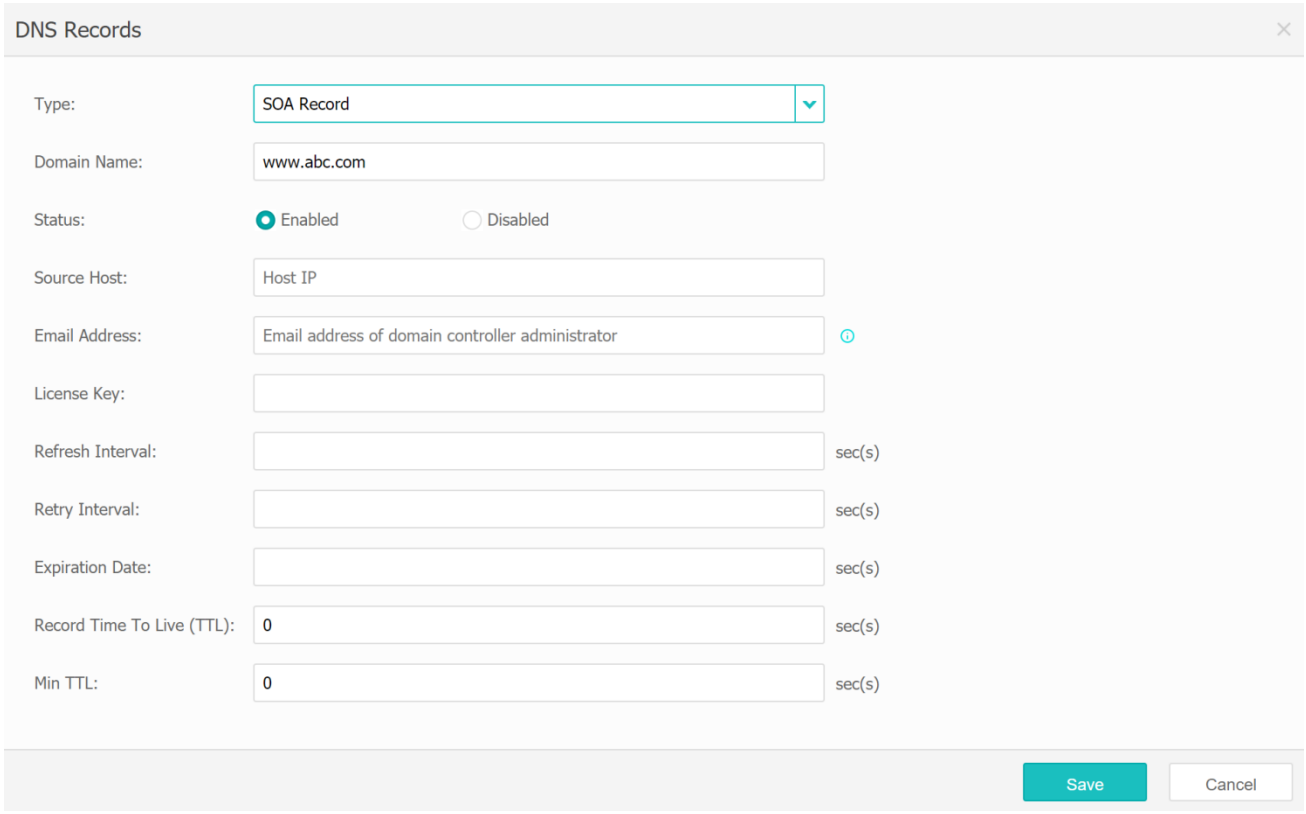
The PTR record is often used to perform a reverse DNS query on a canonical name and is applicable to scenarios in which SMTP reverse DNS resolution is performed.



SOA Record

The SOA record authorizes the server to reply to the querier that this zone is managed by itself and inform the querier of the license key, refresh interval, expiration date, and other

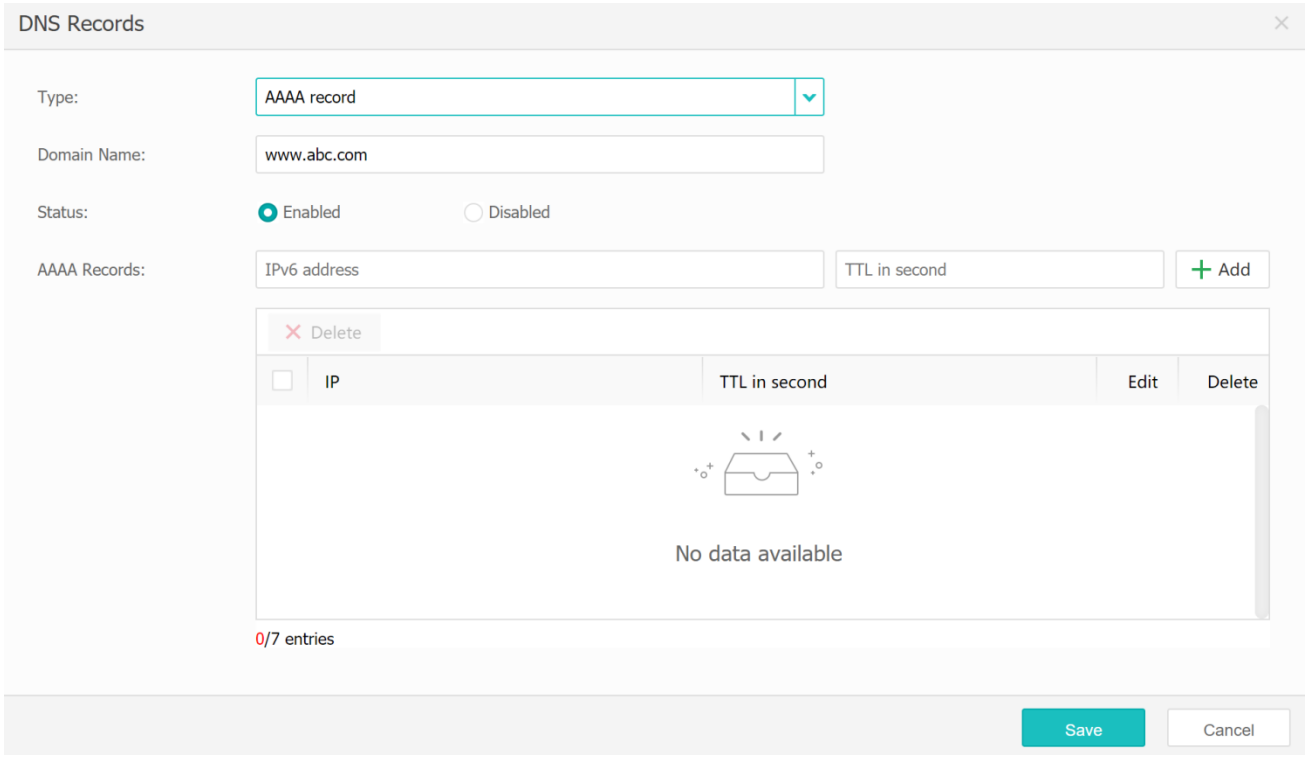
information.



Attention: Replace the At (@) sign in the email address with a comma (.).

AAAA Record

The AAAA record specifies the IPv6 address for the domain name, with the same format and feature as the A record.



9.1.2.2 Local DNS Mapping

【Operation Scenarios】

Generally, a dynamic A record resolution must be performed when a local single site equipped with a port uses an ADC as a DNS server. Compared with the A record, a DNS mapping can dynamically detect the resolution and is used to set level-1 intelligent DNS scheduling for a domain name request from the client. This helps the DNS server schedule the client's access to a virtual IP address pool and then perform level-2 intelligent DNS scheduling on it. In general, the local DNS mapping applies to scenarios in which one domain name maps multiple IP addresses.

【Operation Procedure】

To add a local DNS mapping, set the [Name], [Domain Name Policy], [Selection Policy], and [Virtual IP Address Pool List] parameters. These parameters are described as follows:

『Domain Name Policy』: specifies the domain name for which DNS mapping is performed.

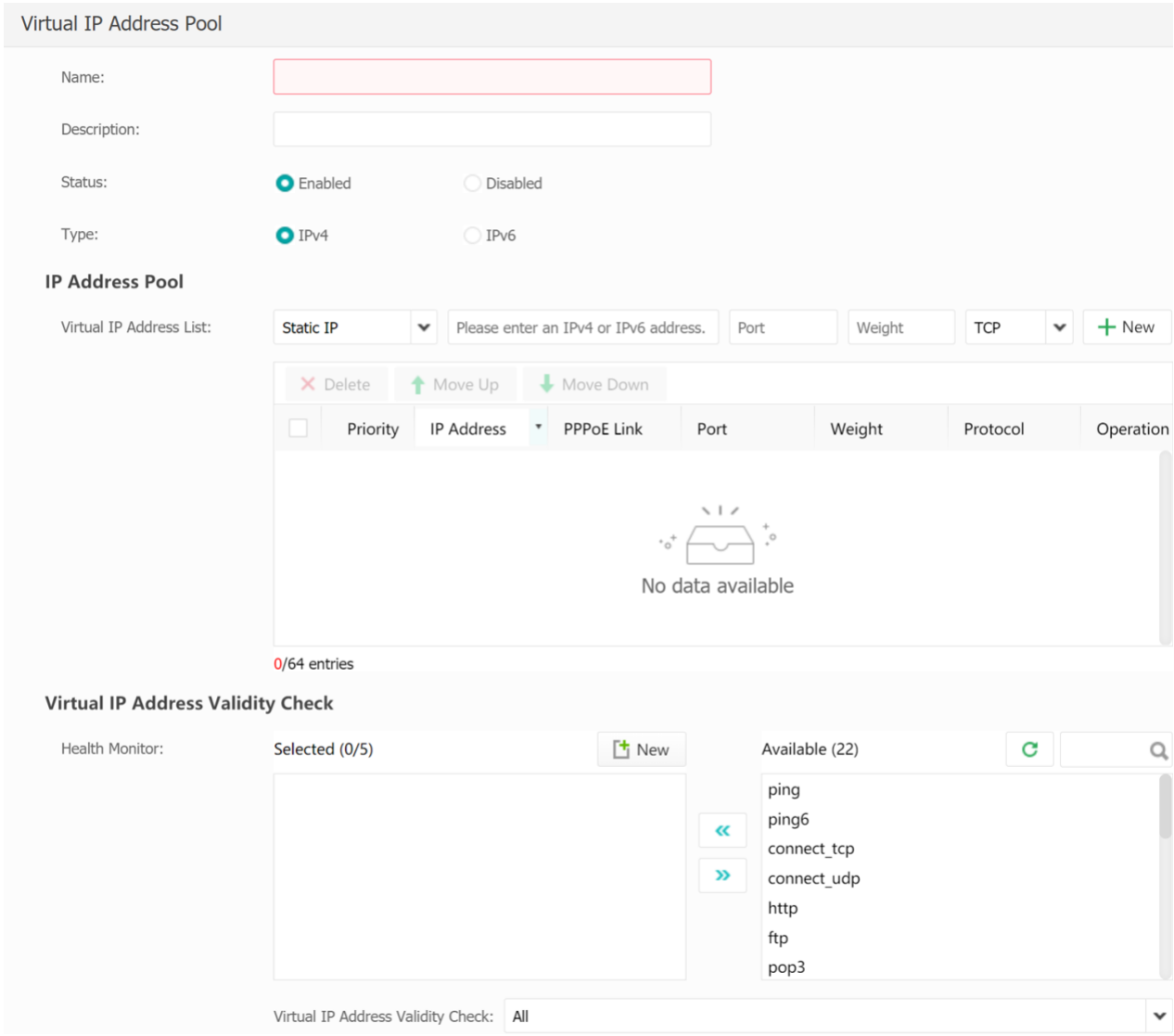
『Selection Policy』: specifies an appropriate scheduling policy selected from [Static Proximity], [Round Robin] and [Weighted Round Robin] as per requirements, which is used to configure DNS mapping scheduling. The policies are described as follows:

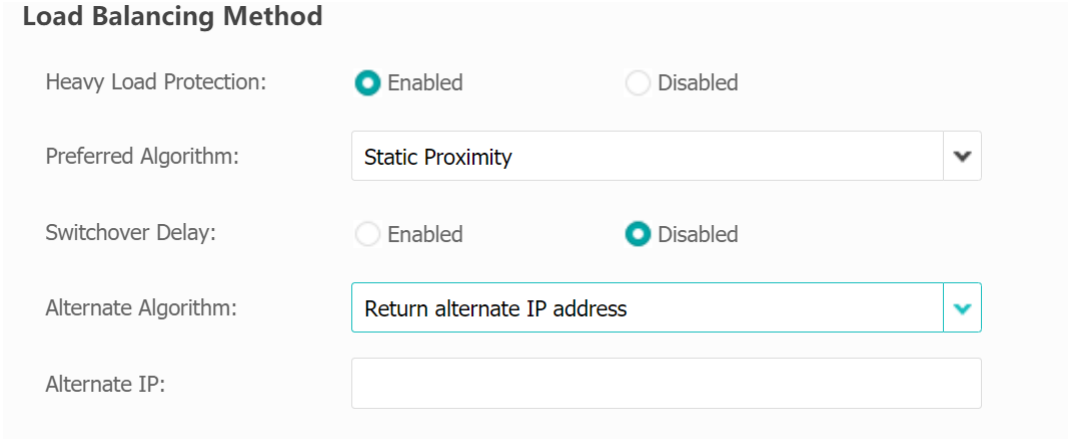
1) [Static Proximity]: Choose『Global Load Balancing』→『Static Proximity』→『DNS Mapping Level』to configure a scheduling algorithm, and determine to schedule the client's access to which virtual IP address pool based on the LDNS set.

2) [Round Robin]: indicates that the access is alternatively scheduled to different virtual IP address pools.

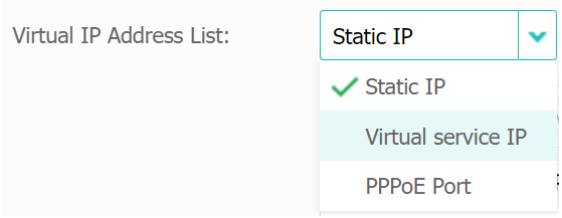
3) [Weighted Round Robin]: used to weight the calculation result by selecting『Weight』in the settings, and schedule the access to a specific virtual IP address pool.

『Virtual IP Address Pool List』: indicates the local virtual IP address pools for local DNS mapping scheduling. To add a virtual IP address pool, you can select a local virtual IP address pool from the drop-down list or directly click Add on the right side, as shown in the following figure:





『Virtual IP Address List』: configures IP addresses and ports in a virtual IP address pool, which need to participate in the level-2 intelligent DNS scheduling; in another word, configures the IP address corresponding to a domain name, which can be the interface address of a physical device or not. You can select [Static IP], [Virtual service IP], or [PPPOE Port] from the Virtual IP Address List drop-down list, as shown in the following figure.

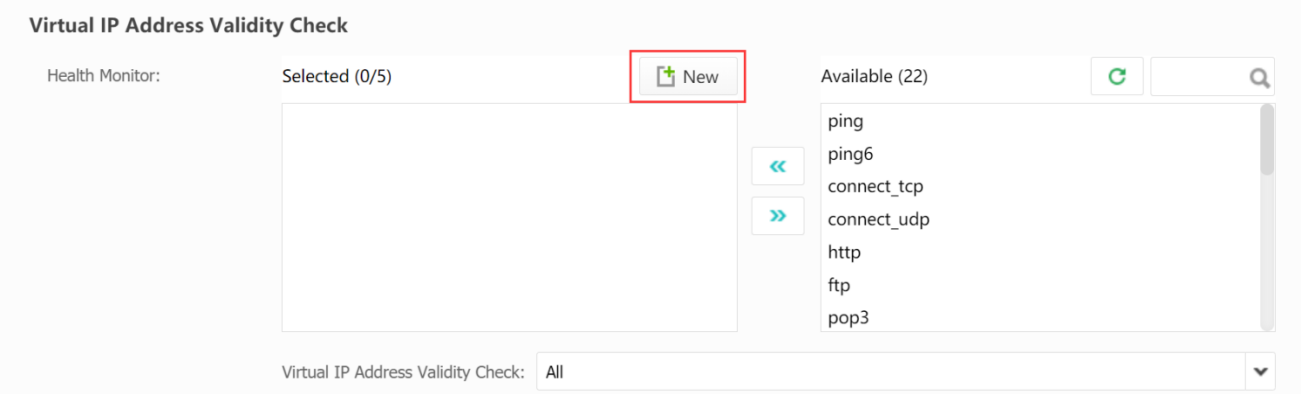


[Static IP]: indicates that a domain name corresponds to a fixed IP address, similar to this example.

[Virtual service IP]: An IP address for analyzing DNS mapping is released by the app load balancing module in the same device to link with a virtual service. In this way, if the virtual service has an error, an exception for this virtual IP address can be detected and the virtual IP address will no longer participate in the scheduling.

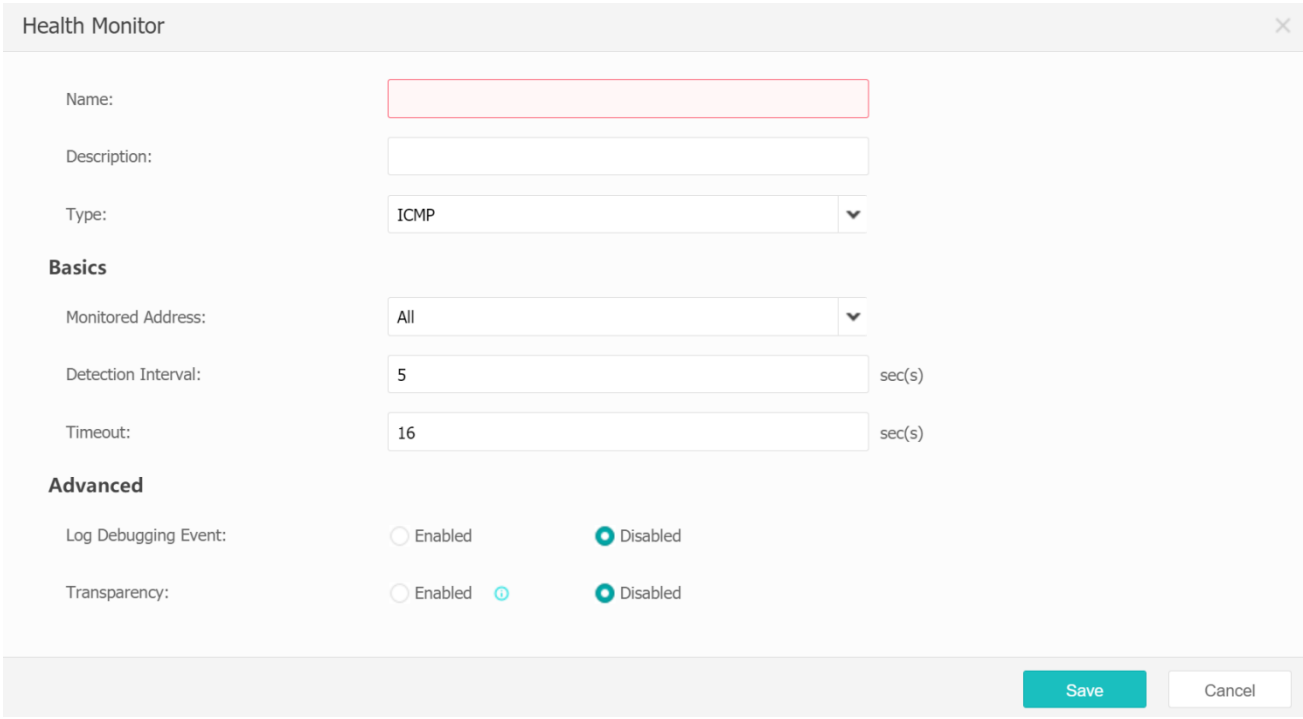
[PPPOE Port]: applicable to WAN dial-up scenarios.

『Virtual IP Address Validity Check』: used to detect whether the virtual IP address is valid. The system provides you with multiple monitors. If you need to set a monitor based on your needs, click New, as shown in the following figure. Alternatively, you can choose 【Global Load Balancing】-> 【Domain Name Release】-> 【Health Monitor】and click New.



『Health Monitor』: detects whether the virtual IP address is online. In general, commonly used monitors include ICMP and CONNECT (TCP). The following example shows you the configuration of ICMP and CONNECT (TCP). If you need to configure other monitors, follow this configuration method.

ICMP: indicates that the device will send an ICMP package in IPv4 address format to detect nodes, as shown in the following figure.



In general, you can directly use the default settings of the ICMP in the system, without the need to add new settings. If you need to set parameters, default ones do not need to be changed, described as follows:

『Monitored Address』: configures an IP address to be monitored. By default, the value of this parameter is All. You can select a specified monitored address from the drop-down list if necessary.

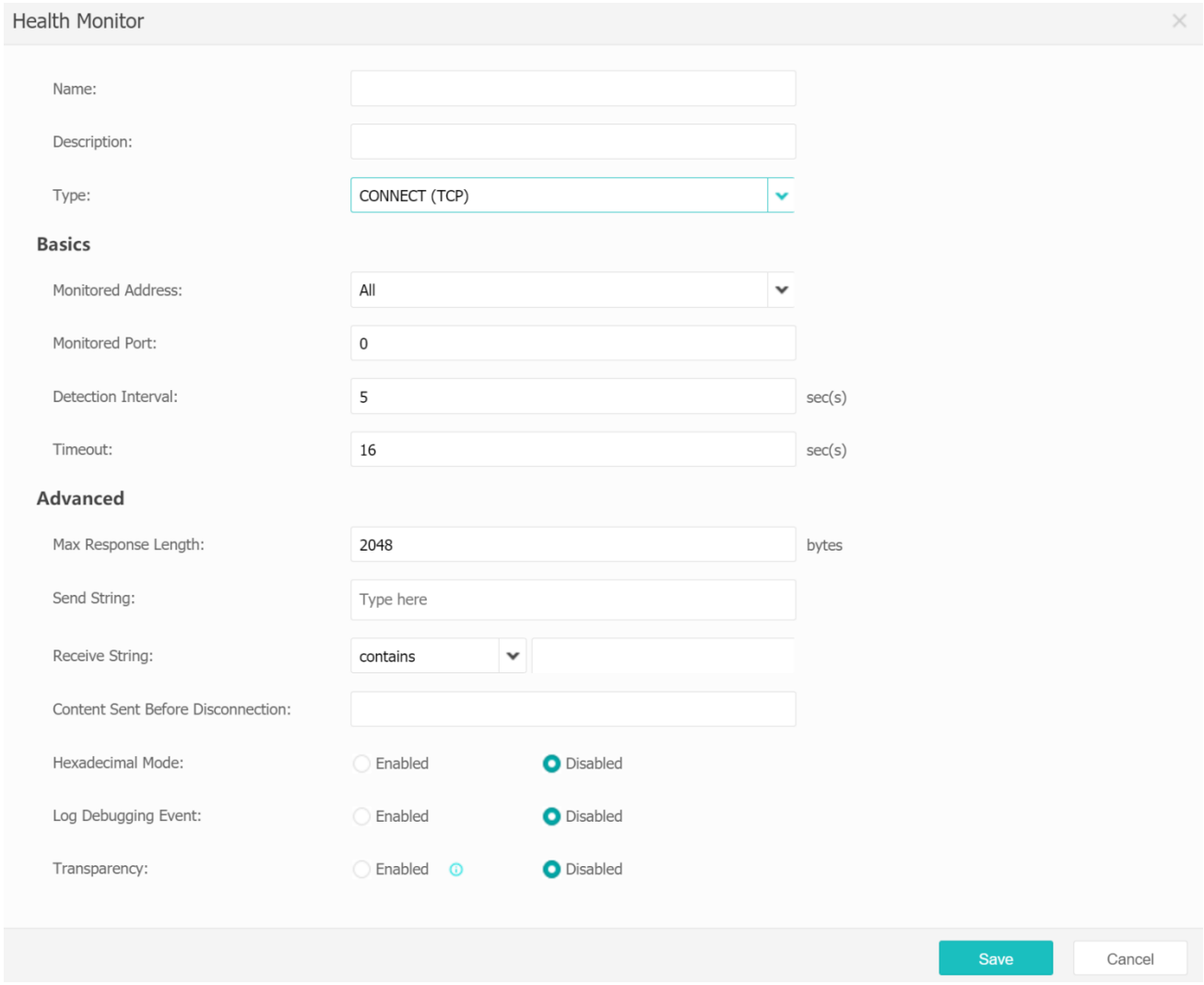
『Detection Interval』: configures the interval time for monitoring, that is, the interval for performing detection (unit: seconds).

『Timeout』: specifies the timeout for monitoring, that is, the time after which the server does not respond (unit: seconds). If no response is received after that time, this request fails.

『Log Debugging Event』: configures whether to enable the debugging log of the monitor. After this parameter is enabled, detailed connection records will be displayed in the log. It is recommended not to enable this parameter.

『Transparency』: applies to firewall load scenarios. Generally, the monitor is a monitoring node, and the transparency mode is a real node bypassing the firewall monitoring.

CONNECT (TCP): indicates that the device will send a TCP connection to detect a node. It is usually used to detect whether the port service is available, as shown in the following figure.



In general, you can use the default monitor, whereas you must change it in some cases, such as specifying Monitored Port, Send String, and Receive String parameters. These parameters are described as follows:

『Monitored Port』: configures a port monitored when the monitoring type is CONNECT TCP.

『Max Response Length』: configures the maximum length of response data for the monitoring type CONNECT TCP (unit: bytes).

『Send String』: configures data content sent after the connection for the monitoring type CONNECT TCP is established.

『Receive String』: configures the content that must be included or excluded in the received data for the monitoring type CONNECT TCP.

『Content Sent Before Disconnection』: configures data content sent before the connection for the monitoring type CONNECT TCP is interrupted.

『Hexadecimal Mode』: indicates that this parameter can be set to [Enabled] or [Disabled], in order to configure whether the hexadecimal mode is enabled for the data content sent and received when the monitoring type is CONNECT TCP.

**Attention**: The Log Debugging Event parameter is enabled only if the device fails, but is disabled in normal cases, preventing excessive debugging logs from overwriting normal logs.

『Preferred Algorithm』: configures the preferred algorithm for scheduling the virtual IP address pool, including [Round Robin], [Weighted Round Robin], [First Available], [Hash], [Weighted Least Connection], [Dynamic Proximity], [Weighted Least Traffic], [Static Proximity], and [Return All IP Addresses].

『Alternate Algorithm』: configures the alternate algorithm for scheduling the virtual IP address pool, including [Round Robin], [Weighted Round Robin], [First Available], [Hash], [Weighted Least Connection], [Dynamic Proximity], [Weighted Least Traffic], [Static Proximity], [Return all IP Addresses], [Return Alternate IP Address], [Deny], and [Discard]. When the alternate algorithm fails, the round robin algorithm prevails. The policies are described as follows:

1) [Round Robin]: indicates that an IP address in the virtual IP address pool is alternatively returned.

2) [Weighted Round Robin]: indicates that an IP address in the virtual IP address pool is returned based on the weighted calculation result for the 『Weight』 parameter.

3) [First Available]: indicates that IP addresses in the virtual IP address pool are matched in a top-down sequence. When the matched IP address is valid, return it.

4) [Hash]: indicates that the operation is conducted on a source IP address of DNS request using the hash algorithm, so as to determine an IP address to be returned.

5) [Weighted Least Connection]: indicates that an IP address is returned in accordance with the weighted calculation results for the [Weight] parameter and the number of connections of a link where the IP address resides.

6) [Dynamic Proximity]: indicates that the Round-Trip Time (RTT) from the link where each IP address resides in the virtual IP address pool to the client's local DNS server is detected by using a detection method configured in the DNS server, and the IP address corresponding to the link with the smallest RTT is returned.

7) [Weighted Least Traffic]: indicates that an IP address in the virtual IP address pool is returned based on the weighted calculation results for the [Weight] parameter and the traffic of a link where the IP address resides.

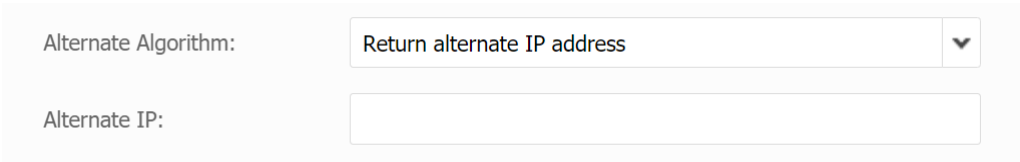
8) [Static Proximity]: Choose『Global Load Balancing』→『Static Proximity』→『Virtual IP Address Pool Level』to configure the scheduling algorithm, and determine to schedule the client's access to which IP address in the virtual IP address pool based on the LDNS set.

9) [Return All IP Addresses]: indicates that all IP addresses of the virtual IP address pool are returned to the client, without any screening.

10) [Deny]: indicates that a rejection message is returned to the client if the preferred algorithm fails to schedule.

11) [Discard]: indicates that the DNS request data package is directly discarded if the preferred algorithm fails to schedule, without any response.

12) [Return Alternate IP Address]: indicates that the IP address that you set is returned if preferred algorithm fails to schedule, as shown in the following figure:



In the『Virtual IP Address Pool』dialog box, other parameters can be left as default. You can set these parameters based on your business needs (if any), described as below:

『Heavy Load Protection』: indicates whether IP addresses in a link in the busy status participate in the scheduling. In general, this parameter is enabled.

『Switchover Delay』: indicates whether the failed link in a virtual IP address pool needs to be resolved and switched. In general, this parameter is enabled only if manual switch is required, but is disabled in other cases.

In the『DNS Mapping』dialog box, other parameters can be left as default. You can set these parameters based on your business needs (if any), described as below:

『Switchover Delay』: indicates whether the failed virtual IP address pool among multiple ones needs to be resolved and switched. In general, this parameter is enabled only if manual switch is required in the multi-data center, but is disabled in other cases.

[Session Persistence]: configures whether to perform session persistence on the virtual IP address returned when the client has an access to the DNS mapping domain name. During the specified timeout, multiple requests from the same source are scheduled to the same virtual IP address pool. In general, this parameter is enabled.

[Session Timeout]: configures the timeout of session persistence method (unit: seconds). In general, this parameter is left as default.

[TTL]: configures the cache time recorded in the local DNS server for a domain name for which DNS mapping scheduling is performed (unit: seconds). In general, this parameter is left as default.

9.1.2.2.1 Static Proximity

【Operation Scenarios】

In most cases, customer's WAN is equipped with multiple external lines, and a domain name corresponds to multiple IP addresses. This helps satisfy the requirements of different carriers and return different IP addresses to the client. Assume that a customer has two external lines including China Telecom and China Unicom, the domain name is www.abc.com, and the corresponding A records are 1.1.1.1 for China Telecom IP address and 2.2.2.2 for China Unicom IP address. To allow China Telecom users to access, return the China Telecom IP address. To allow China Unicom users to access, return the China Unicom IP address. Apart from the two cases, return the China Telecom IP address first.

【Prerequisites】

The NS record is registered by the domain name provider and takes effect, as described in the following table.

Record Type	Host Record	Resolution Line (Carrier)	Record Value

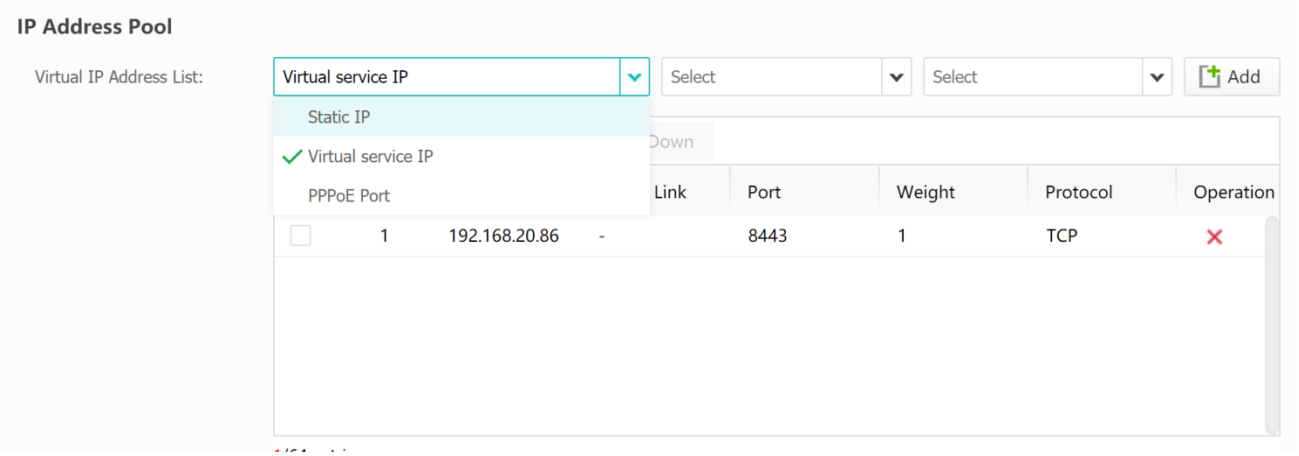
NS	www	Default	NS1.abc.com
A	NS1.abc.com	Default	1.1.1.1
NS	www	Default	NS2.abc.com
A	NS2.abc.com	Default	2.2.2.2

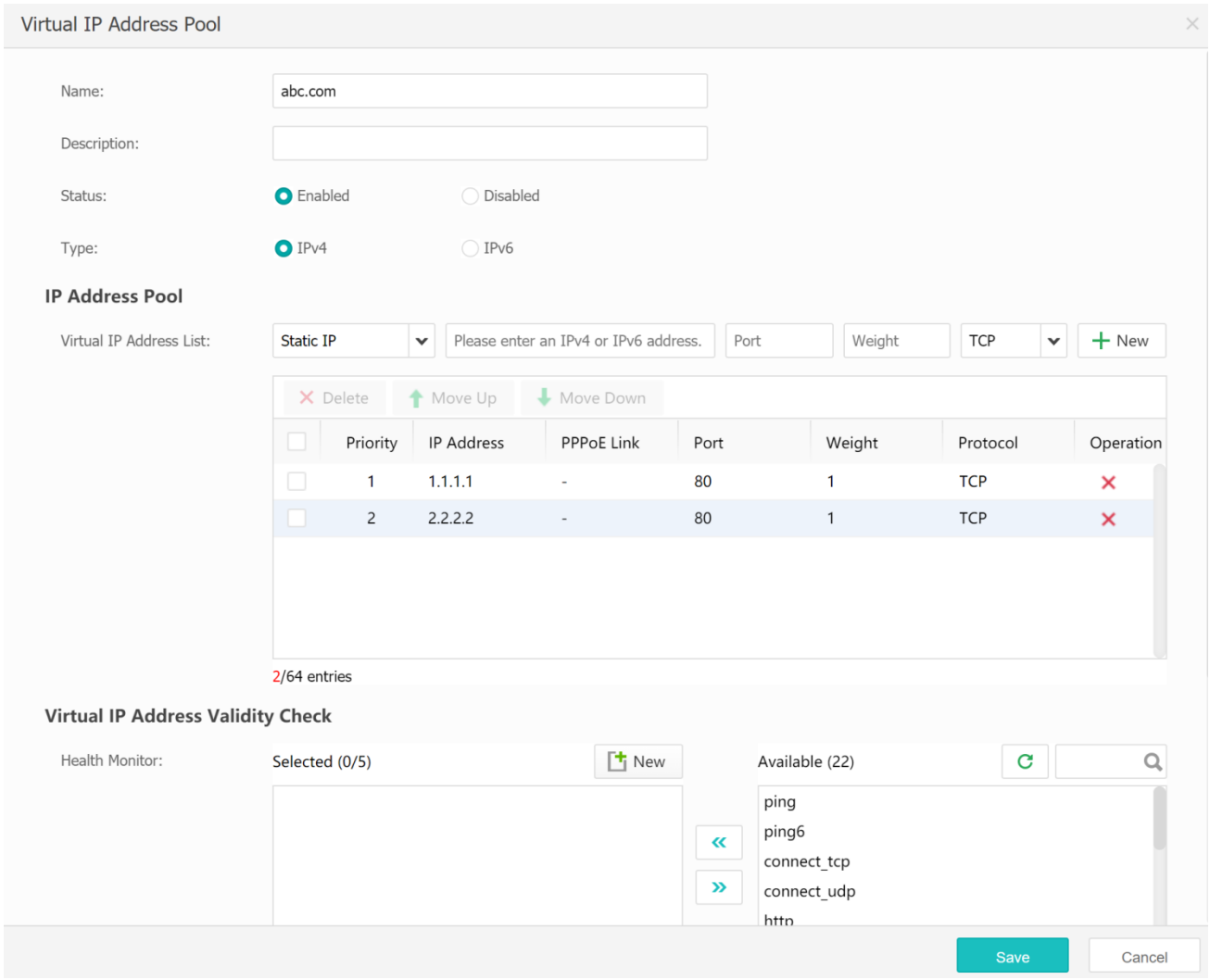
【Operation Procedure】

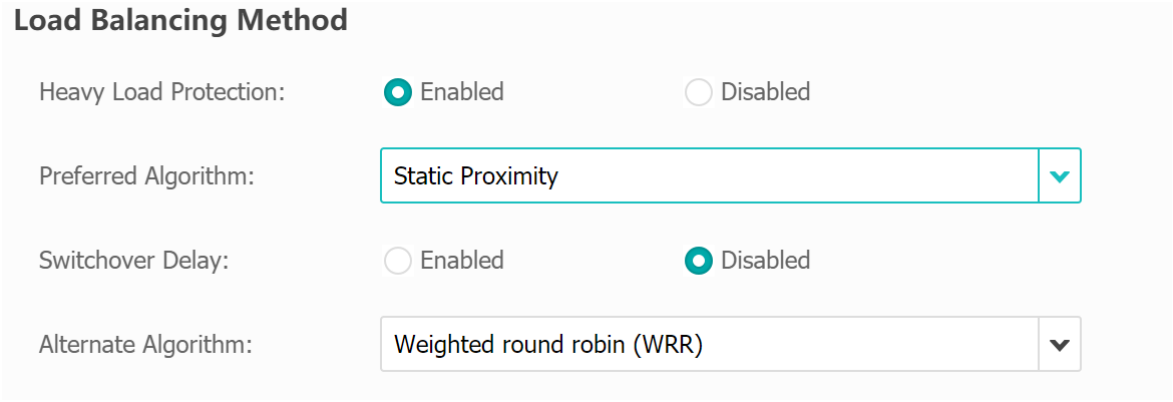
1.Configure a DNS server and configure the monitoring address of it as per Section 9.1.1.

2.Choose『Global Load Balancing』-> 『DNS Mapping』-> 『DNS Mapping』-> 『Local DNS Mapping』 and add a local DNS mapping by setting the following parameters: Description, Domain Name Policy, and Virtual IP Address Pool List.

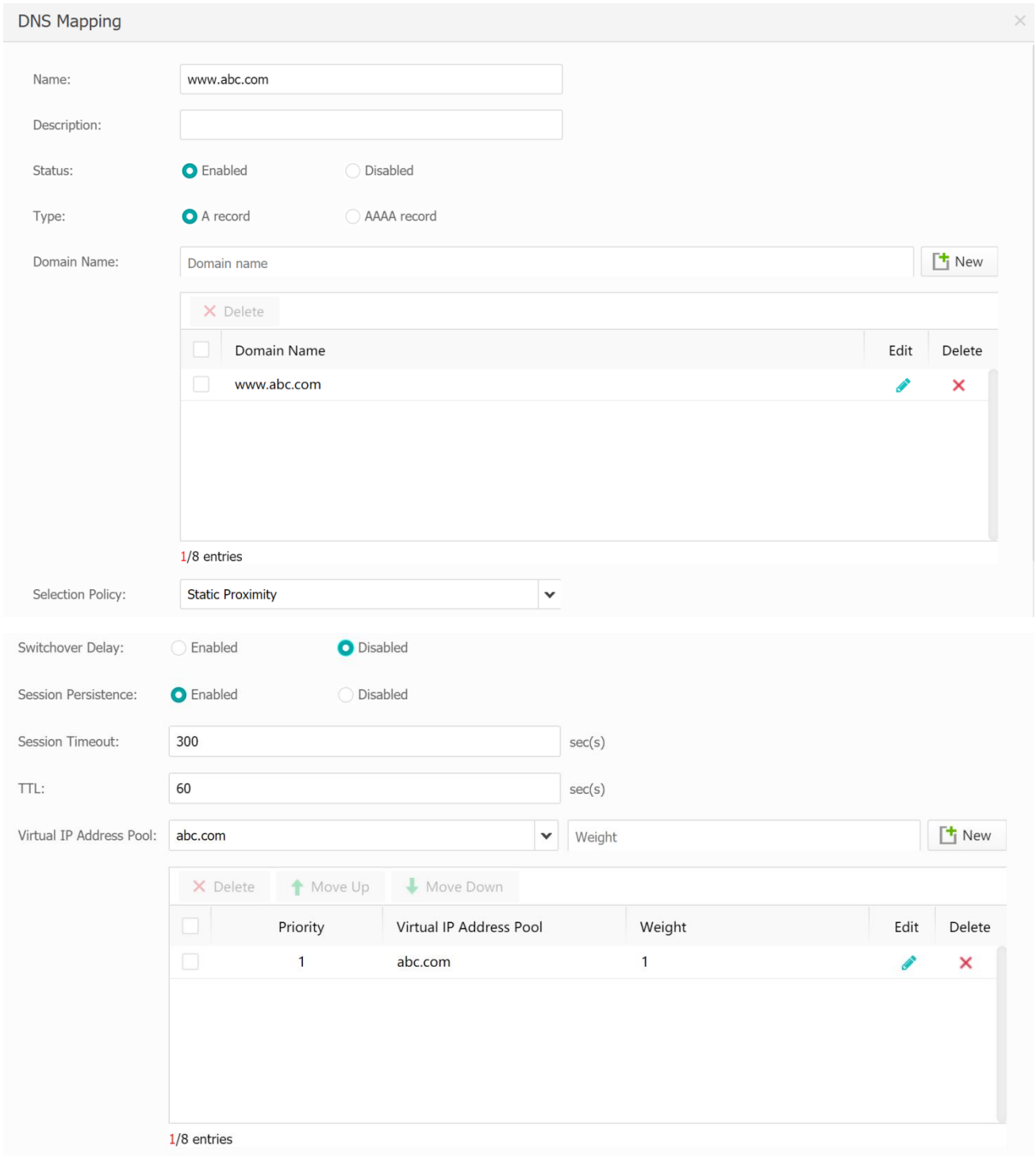
1) Add a virtual IP address pool and set these parameters: Description, Virtual IP Address Pool List, Virtual IP Address Validity Check (Health Check Method), and Load Balancing Method, as shown in the following figures.







After the parameters are set, the DNS mapping is added, as shown in the following figures.



Attention:

1) You must set the Preferred Algorithm parameter for the virtual IP address pool as Static Proximity.

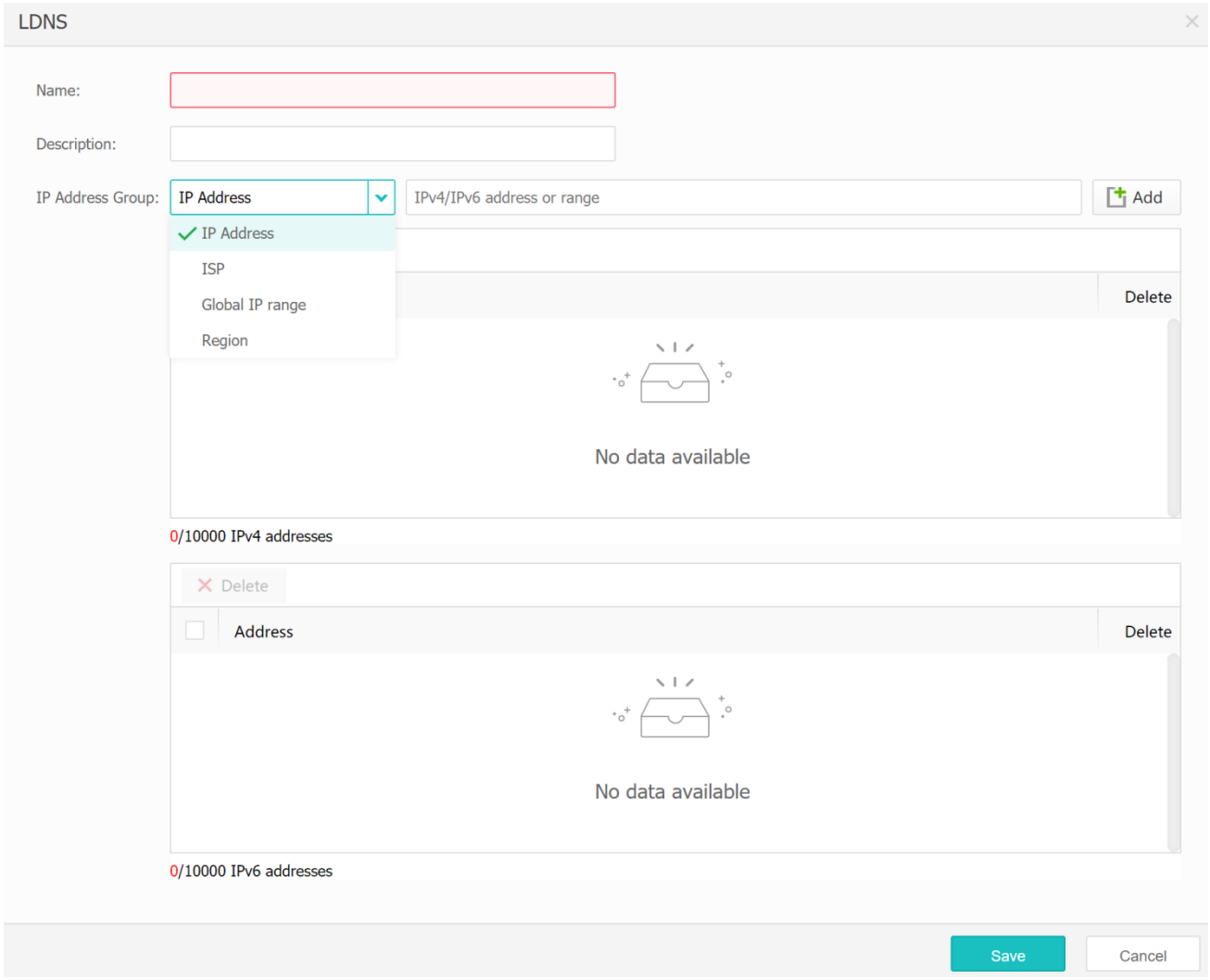
2) Apart from China Telecom and China Unicom clients, the China Telecom IP address should be returned first. This way, you must set the China Telecom IP address in the first place of virtual IP address pool, and set the Alternate Algorithm parameter to First Available.

3) In this example, there is only one site, that is, one virtual IP address pool. In this case, the Selection Policy parameter for the DNS mapping can be left as default.

3.Choose 『Global Load Balancing』-> 『Static Proximity』-> 『IP Address Pool』and add a local virtual IP address pool level by setting the following parameters: Name, Virtual IP Address Pool, LDNS, and IP Addresses in Pool.

『IP Address Pool』: selects the virtual IP address pool referenced by the DNS mapping.

『LDNS』: adds a required LDNS set by adding an IP database and selecting a built-in ISP database, global IP database, or regional IP database.

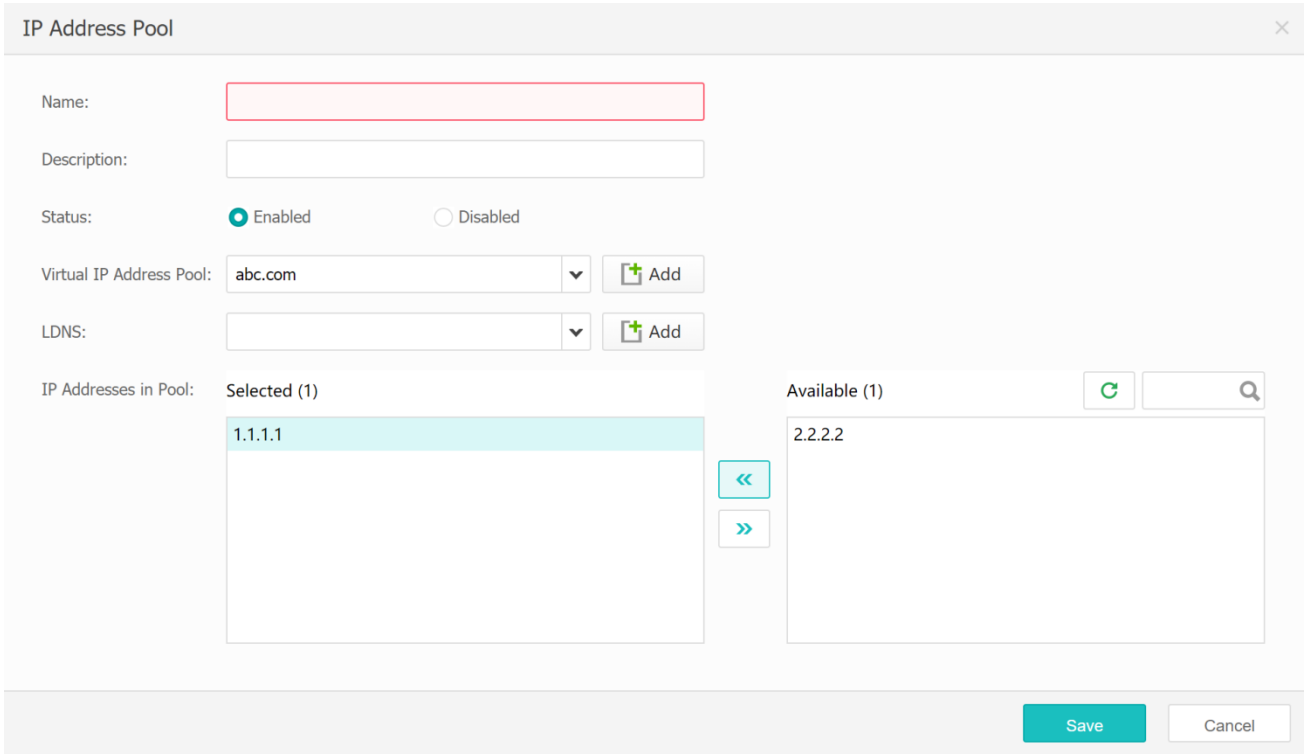


Notes: You can choose 【Objects】-> 【Databases】 to import or add built-in IP address ranges.

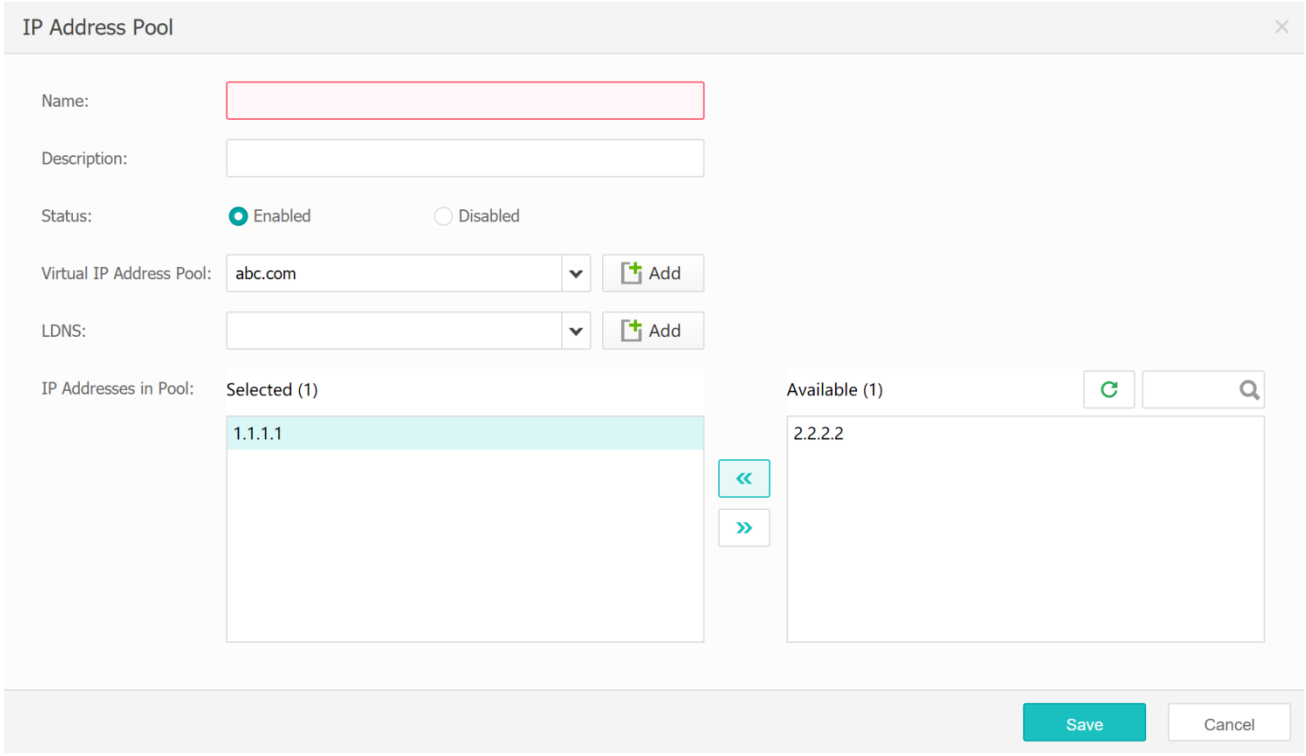
『IP Addresses in Pool』: Select an IP address that reside in the virtual IP address pool, such as Return China Telecom IP Address to China Telecom Client, and Return China Unicom IP Address to China Unicom Client.

After the parameters are set, the local virtual IP address pool level is added, as shown in the following figures.

Return China Telecom IP Address to China Telecom Client:



Return China Unicom IP Address to China Unicom Client:



9.2 Global Intelligent DNS Resolution

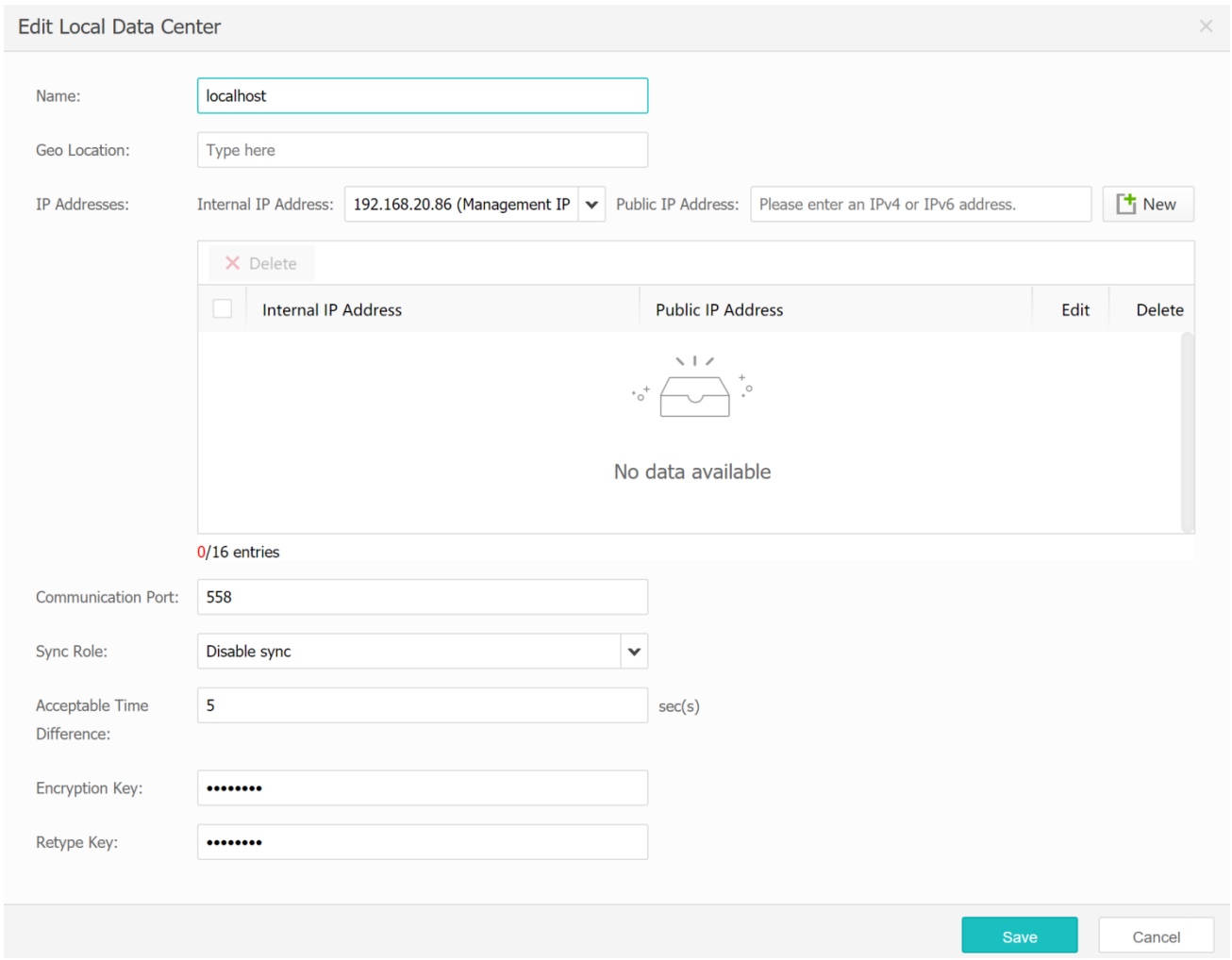
9.2.1 Report Center Options

【Operation Scenarios】

In general, relevant IP addresses of data centers should be configured when multiple data centers are globally loaded. This helps data centers synchronize their configurations.

【Operation Procedure】

1. Firstly, configure a local data center by setting the following parameters: IP Addresses, Sync Role, Encryption Key, and Retype Key, as shown in the following figure.



『IP Addresses』 : selects an internal IP address used to synchronize global files from the drop-down list, or adds an IP address.

『Sync Role』 : sets a role that this data center assumes to synchronize global files.

Disable sync: indicates that the data center will not participate in the synchronization of global files.

Slave: indicates that this data center will download the latest global file configuration from other data centers.

Master: indicates that this data center will upload the updated global file configuration to other data centers.

Bidirectional: indicates that this data center assumes two roles, including uploading and downloading.

『Encryption Key』: indicates an encryption key for communication between data centers.

『Retype Key』: enters your encryption key again to confirm the value that you set for the Encryption Key parameter.

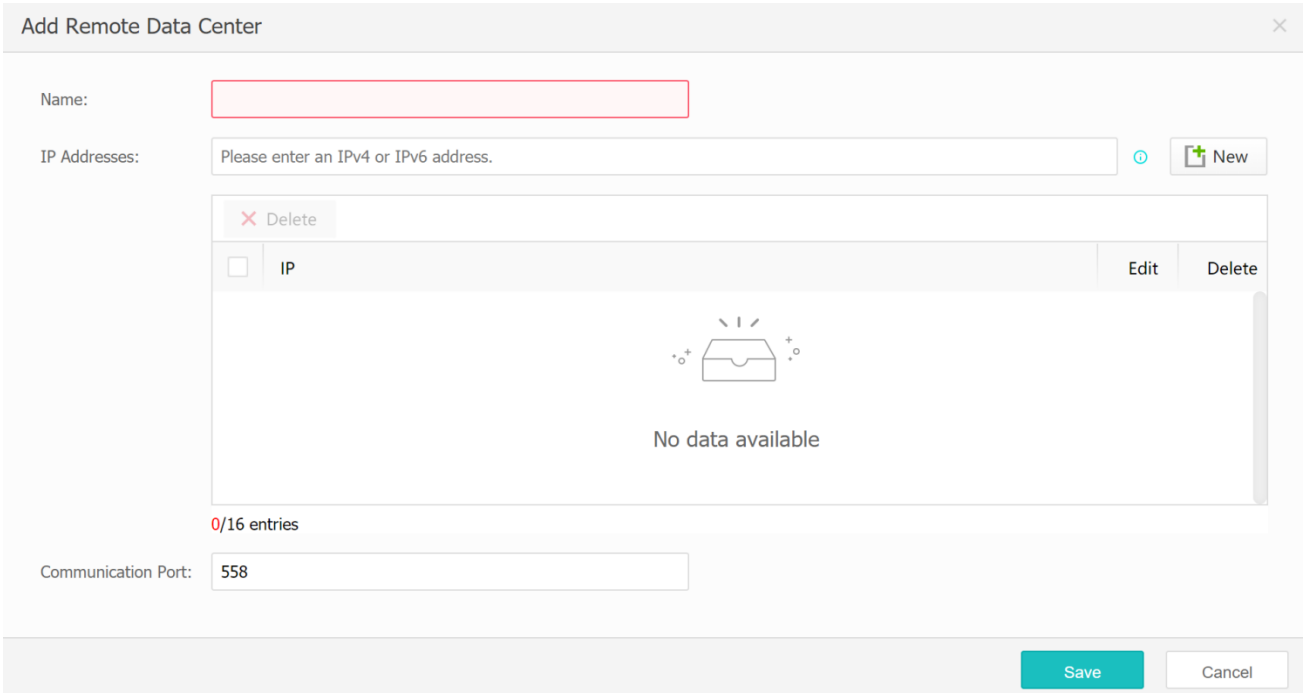
In the『Edit Local Data Center』dialog box, parameters except for the preceding ones can be left as default. You can set these parameters based on your business needs (if any), described as below:

『Geo Location』: enters the geographic position of this data center and other relevant information, which allow users to distinguish data centers easily.

『Communication Port』: sets a communication port for global file synchronization. By default, this parameter is set to 558, or you can change it as required.

『Acceptable Time Difference』: indicates the threshold value of difference between two data centers' modification time of configuration files during the global synchronization. If the difference between two data centers' modification time of configuration files is greater than the value of the [Acceptable Time Difference] parameter, it indicates that configuration files in a data center whose modification time is earlier needs to be updated. Otherwise, it indicates that configuration files of two data centers are considered as equivalent but out-of-sync.

2. Add a remote data center by setting the following parameters: Name and IP Addresses, as shown in the following figure.

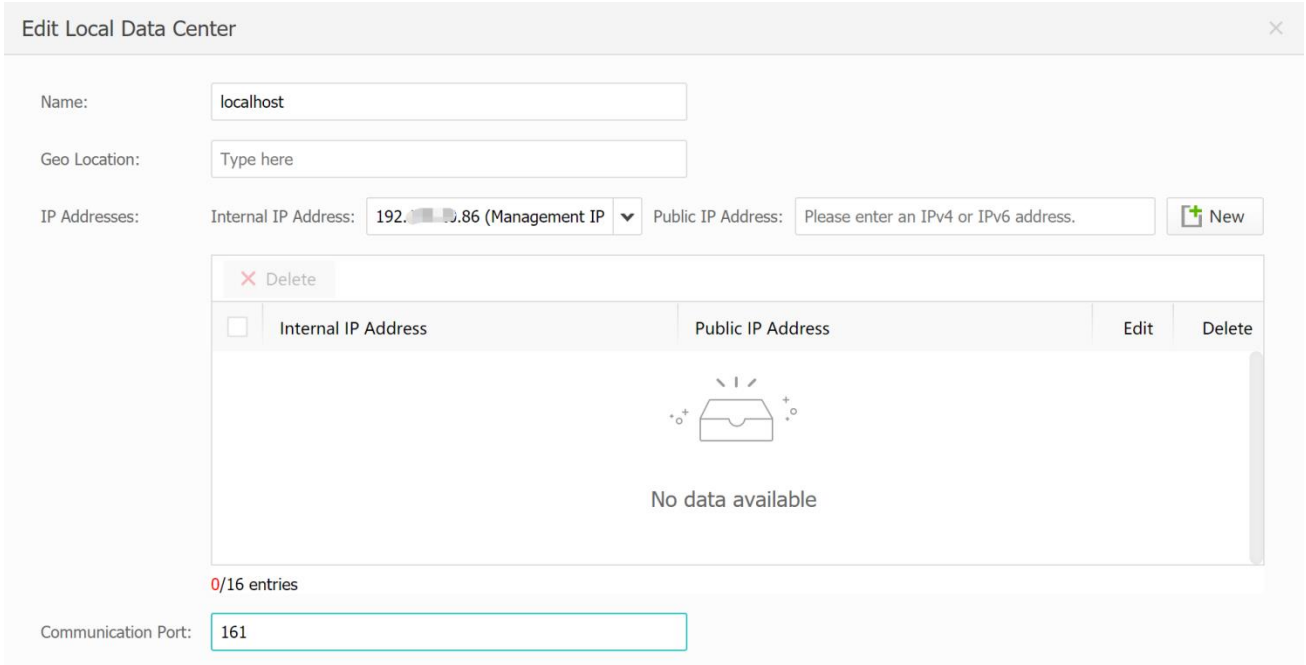


『IP Addresses』: enters an IP address used to synchronize global files, which needs to normally communicate with the IP address of local data center.

3. Configure devices in other data centers by following steps 1 and 2. Configure the local data center and then the remote data center.

After the preceding three steps are completed, a global load balancing device is set up. If this device needs to interact with an app load balancing device in the data center, set the following parameters:

In the Edit Local Data Center dialog box, set the following parameters: Name and IP Addresses, as shown in the following figure.



『IP Addresses』: indicates the IP address of the app load balancing device, which only needs to be capable of communicating with the global load balancing device.

『Communication Port』 : indicates a port for SNMP service of the app load balancing device. In general, this parameter is left as default.

9.2.2 Configuring DNS Server

For more information about the specific configuration, see Section 9.1.1.

9.2.3 Domain Name Release

9.2.3.1 Global DNS Records

【Operation Scenarios】

In general, global DNS records are records to be resolved when the ADC among multiple sites in a distributed environment is regarded as a global DNS server. The 『Global DNS Records』parameter for each site can be set to the same value, including A records, MX records, NS records, SRV records, CNAME records, TXT records, PTR records, SOA records, and AAAA records.

【Operation Procedure】

Add corresponding records as per specific requirements. For more information about the records and respective configurations, see the configurations of local DNS records in Section 9.1.2.1.

9.2.3.2 Global DNS Mapping

【Operation Scenarios】

In general, a global DNS mapping is used to perform level-1 intelligent DNS scheduling on multiple virtual IP address pools among multiple sites in a distributed environment. The configurations of global DNS mappings in all sites are the same. After dynamic resolution is performed on A records, an ADC can be used as a DNS server. Compared with DNS records, the DNS mapping can be used to perform dynamic detection and resolution on A records. It can perform level-1 intelligent DNS scheduling on a domain name request from a client, schedule client's access to a virtual IP address

pool, and then perform level-2 intelligent DNS scheduling on this virtual IP address pool. The DNS mapping applies to scenarios in which one domain name maps multiple IP addresses.

【Operation Procedure】

To add a global DNS mapping, set the [Name], [Domain Name Policy], [Selection Policy], and [Virtual IP Address Pool List] parameters. Follow the same steps as the configuration of a local DNS mapping. The difference is that the global DNS mapping is used to schedule a global virtual IP address pool.

Global virtual IP address pool

『Associated Virtual Service』: A virtual IP address associates with a virtual service while being an IP address group of this service. This way, whether the virtual IP address is valid depends on whether the virtual service is valid.

『Heavy Load Protection』: Different sites will notify each other of whether they are in the busy status every 10 seconds while detecting whether respective links are in a busy state. When the link of a site is in the busy status, the IP address and port, which participate in scheduling, of this link will no longer be scheduled by other sites.

『Preferred Scheduling Policy』: used to schedule current occupancy of resources in the virtual IP address.

9.2.3.2.1 Static Proximity

【Operation Scenarios】

In general, a customer has multiple data centers, each of which is equipped with multiple external lines. These data centers form a dual active or active-standby mode. An external service must have multiple IP addresses by which requests of customers from different regions can be received and different carrier IP addresses of different data centers to a client. Assume that a specified customer has two data centers that form the dual active mode, each data center's WAN is equipped with three external lines including China Telecom, China Unicom, and China Mobile, the domain name is www.abc.com, resolution addresses for the data center A are 1.1.1.1 for China Telecom, 2.2.2.1 for China Unicom and 3.3.3.1 for China Mobile, and resolution addresses for the data center B are 4.4.4.1 for China Telecom, 5.5.5.1 for China Unicom and 6.6.6.1 for China Mobile.

If you want to resolve domain names in Northeast and Northern China, and Northwest and Southwest China to the data center A, and

domain names in other regions to the data center B,

corresponding IP addresses must be returned to customers choosing the same carrier first. If a line fails, domain names must be resolved to other lines.

【Prerequisites】

The NS record is registered by the domain name provider and takes effect. It must record IP addresses monitored by ADCs in two data centers.

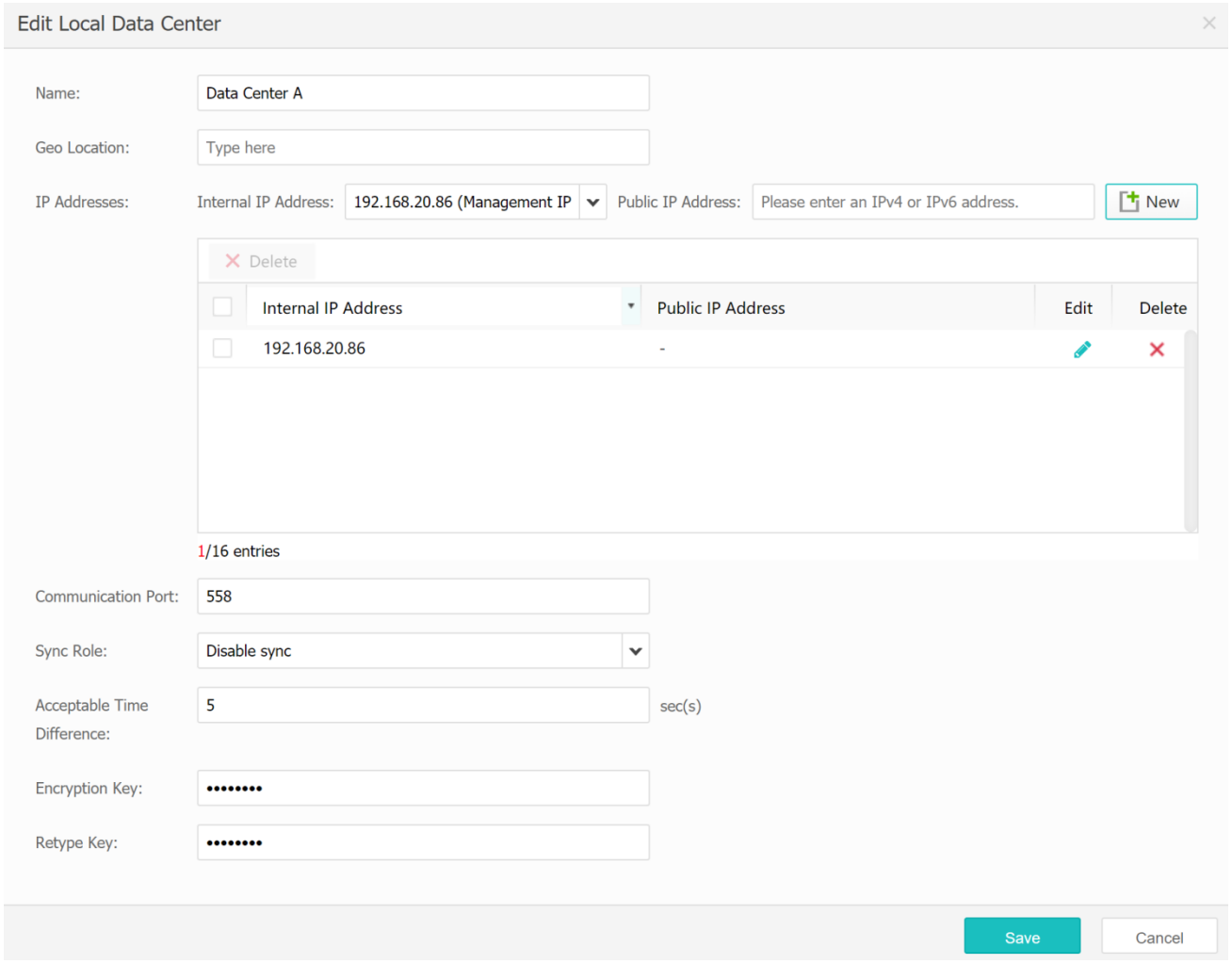
For example, domain name: www.abc.com, and ADC's monitoring IP addresses: 172.10.20.100 (data center A) and 172.10.10.100 (data center B). For more information about formats, see Section 9.1.1.

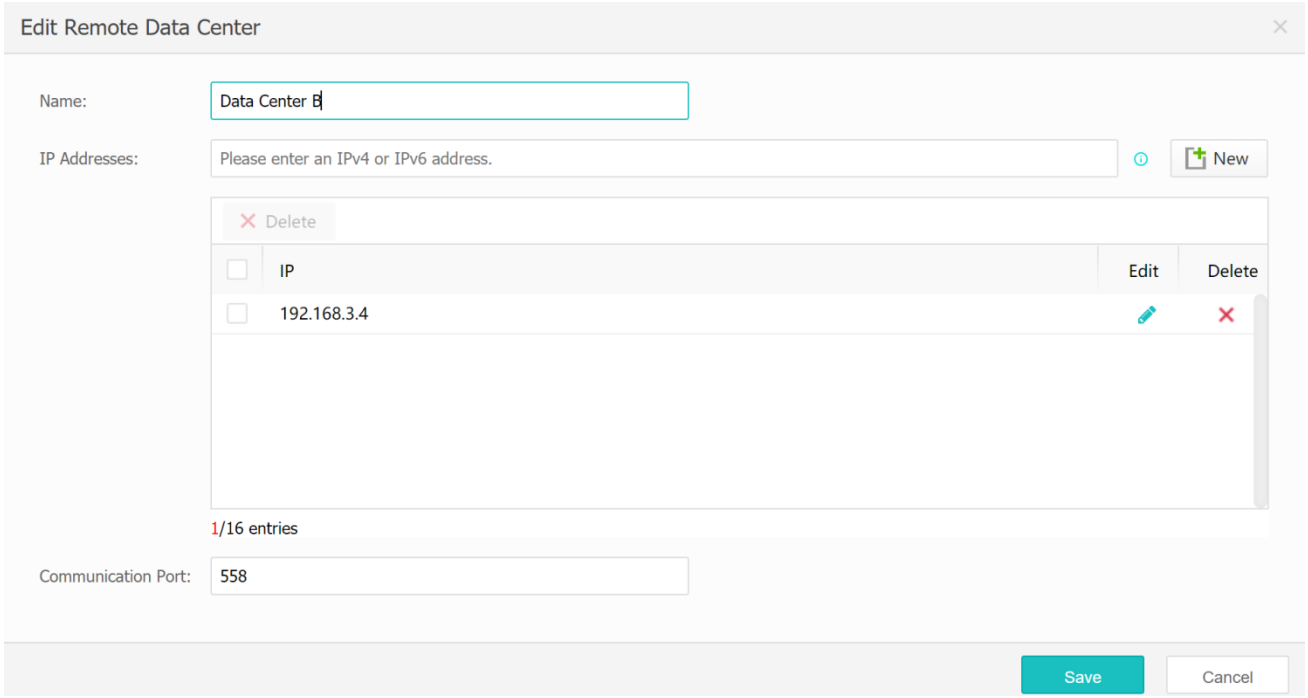
**Attention**: This address is just an example. Normally, the NS record corresponding to a domain name is an external IP address. A data center includes more than one NS record.

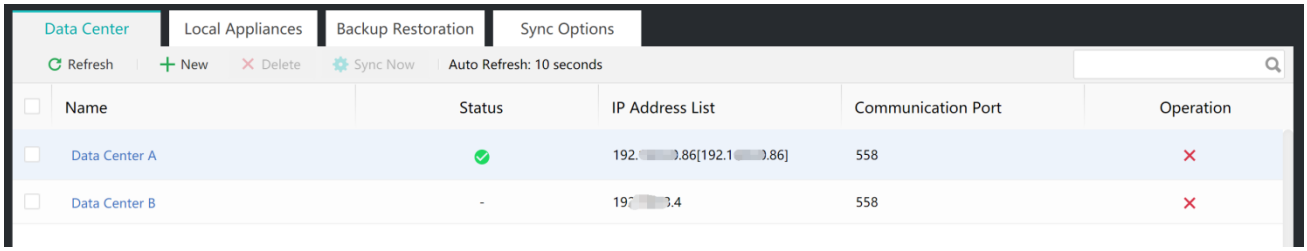
【Operation Procedure】

1. Configure data centers. In this example, two data centers communicate with each other using IP addresses 172.10.10.100 and 172.10.20.100. The specific configuration is as follows:

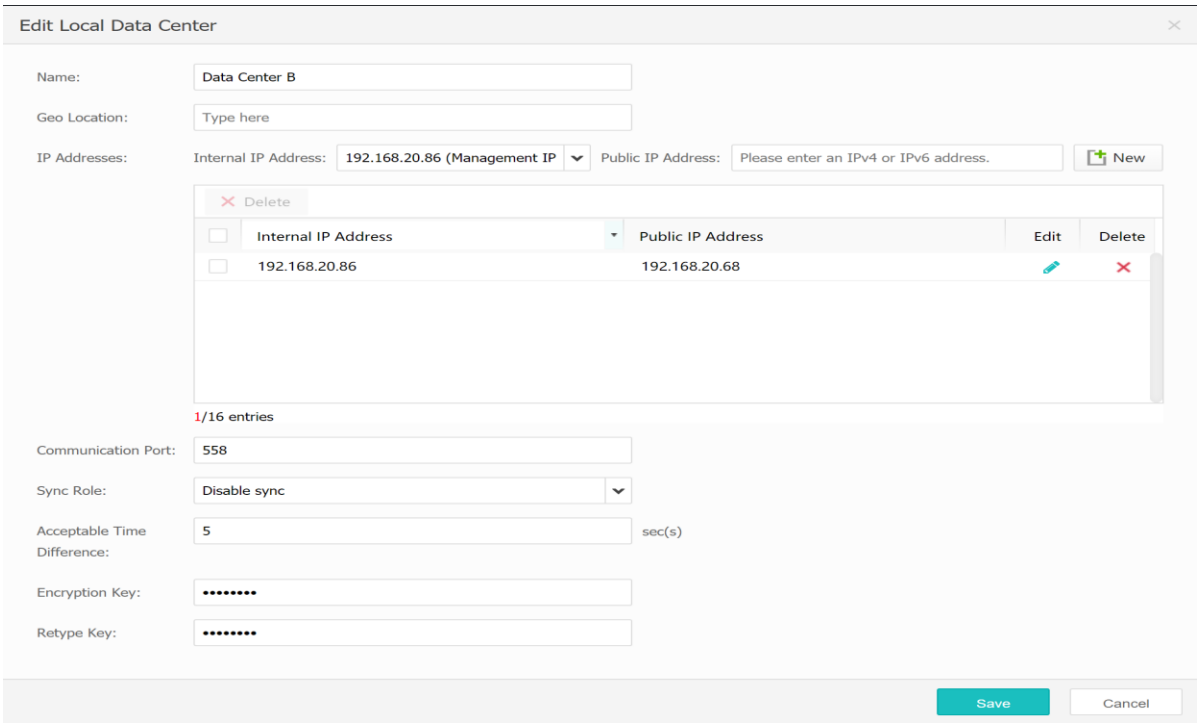
Data center A:

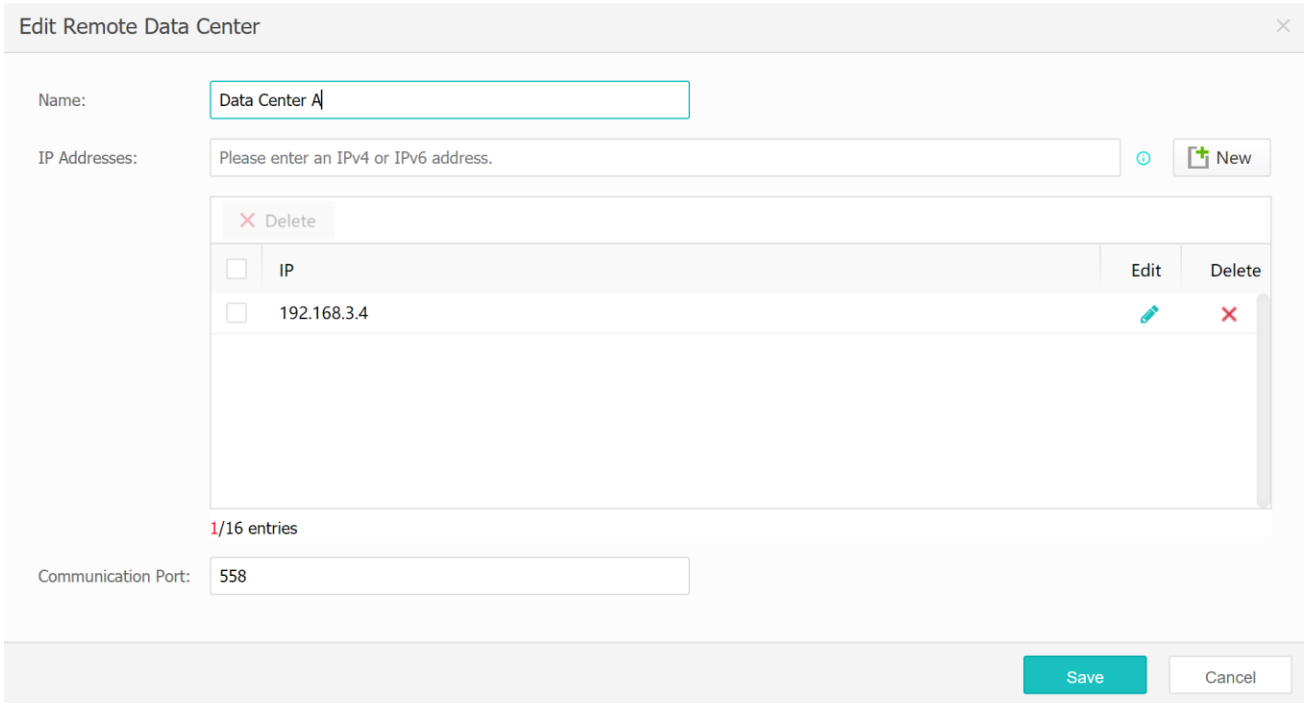

Edit Local Data Center
Name:
Data Center A
Geo Location:
Type here
IP Addresses:
Internal IP Address:
192.168.20.86 (Management IP
Public IP Address:
Please enter an IPv4 or IPv6 address.
New
Delete
Internal IP Address
Public IP Address
Edit
Delete
192.168.20.86
-
1/16 entries
Communication Port:
558
Sync Role:
Disable sync
Acceptable Time Difference:
5
sec(s)
Encryption Key:
Retype Key:
Save
Cancel

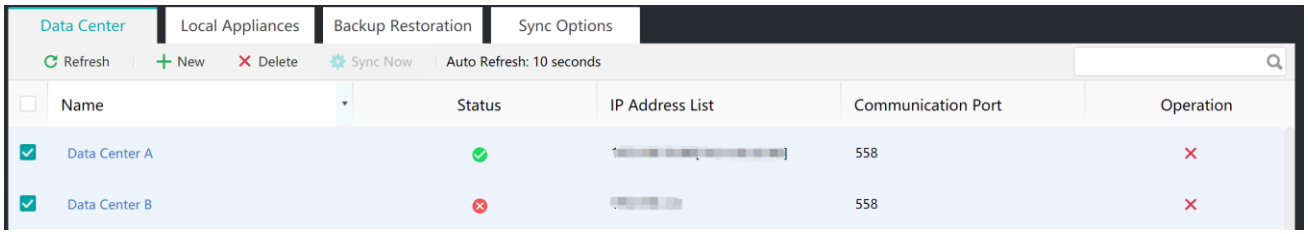

Edit Remote Data Center
Name:
Data Center B
IP Addresses:
Please enter an IPv4 or IPv6 address.
New
Delete
IP
Edit
Delete
192.168.3.4
1/16 entries
Communication Port:
558
Save
Cancel



Data center B:

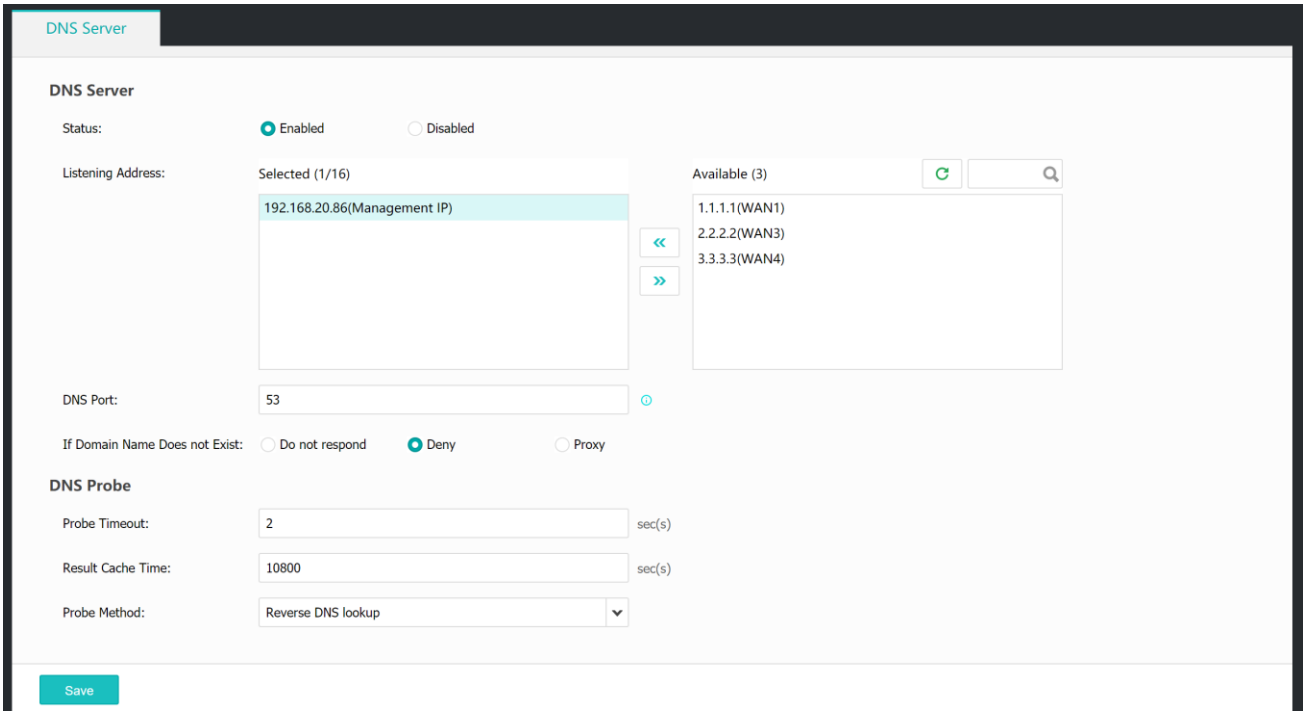






2.Configure a DNS server and configure the monitoring address of it.

Data center A

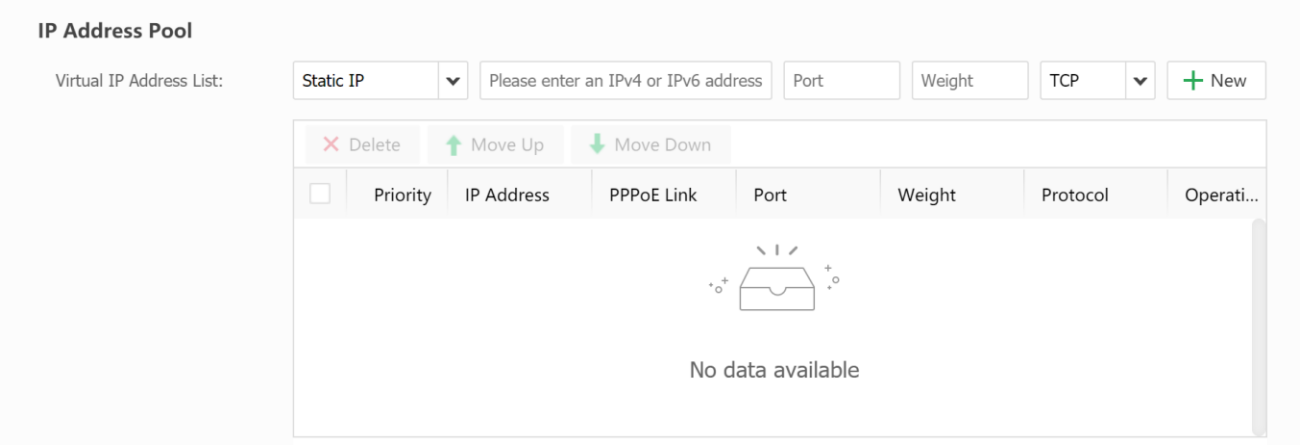


Data center B: The same configuration.

3. Choose『Global Load Balancing』-> 『Domain Name Release』-> 『Global DNS Mapping』 and add a global DNS mapping by setting the following parameters: Description, Domain Name Policy, Selection Policy, and Virtual IP Address Pool List.

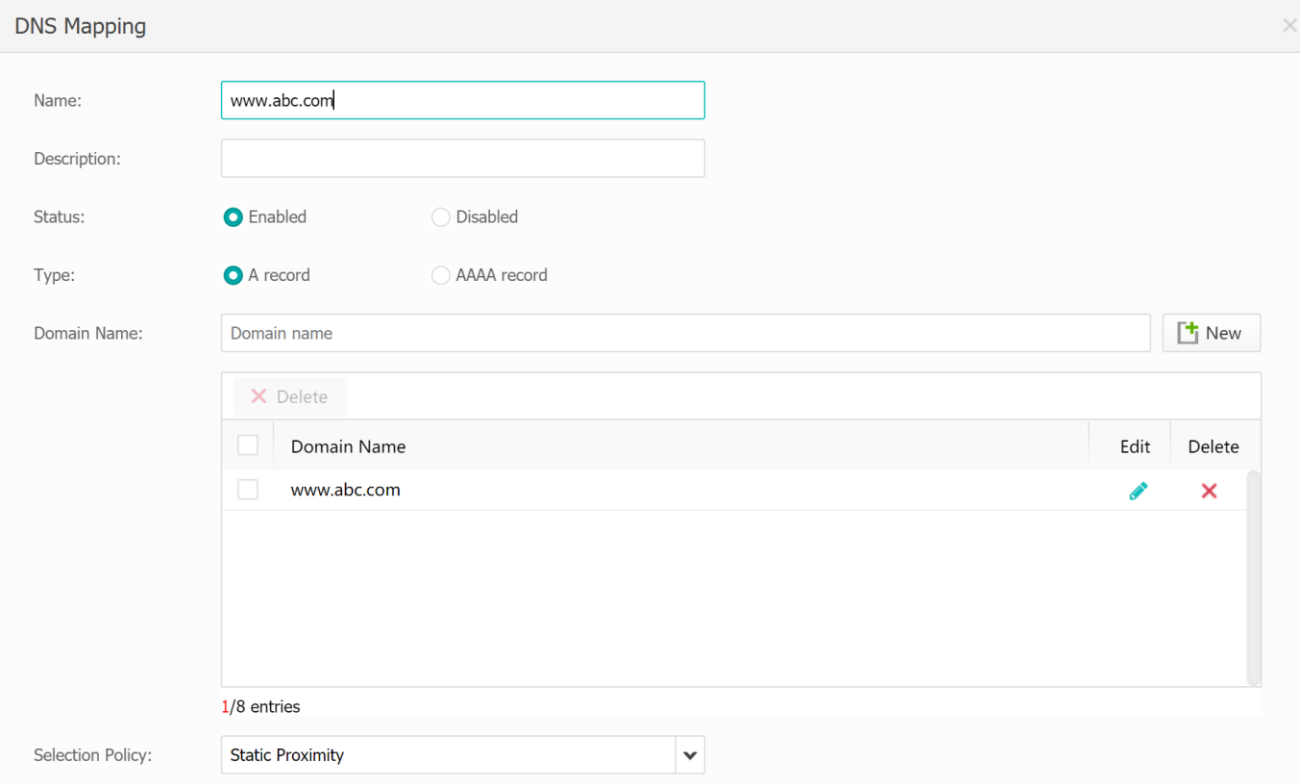
1) Select a policy: Select static proximity to perform level-1 intelligent DNS scheduling and schedule the access to appropriate virtual IP address pools, one of which for the data center A and the other for the data center B.

2) Add a virtual IP address pool and set these parameters: Description, Virtual IP Address Pool List, Virtual IP Address Validity Check (Health Check Method), and Load Balancing Method, as shown in the following figure.



After the parameters are set, the DNS mapping is added, as shown in the following figures.

Data center A



Data center B: The configurations are automatically synchronized to the data center B.

Attention:

1) The Selection Policy parameter for the DNS mapping must be set to Static Proximity.

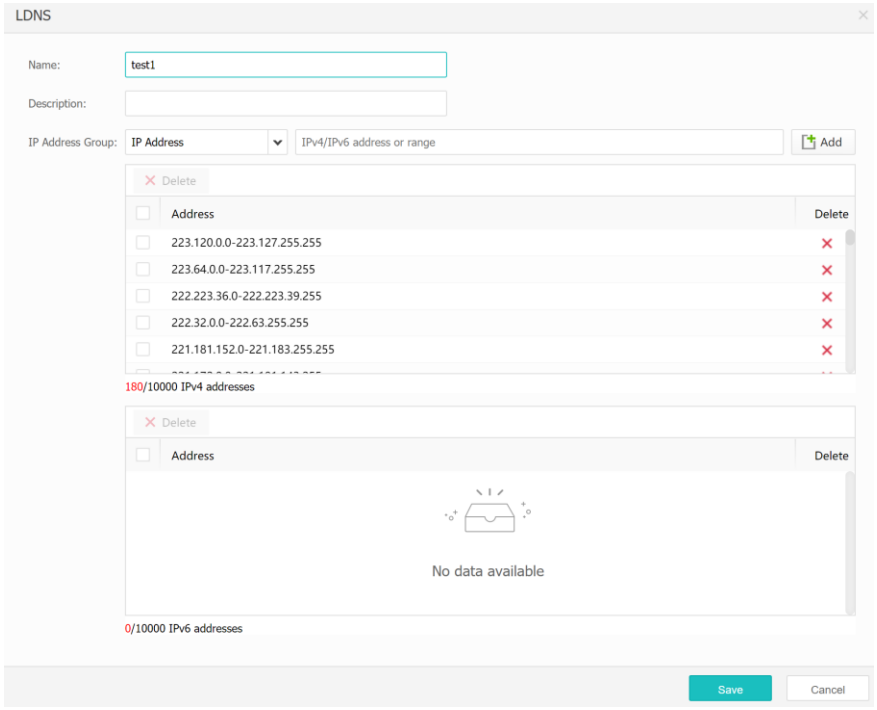
2) You must set the Preferred Algorithm parameter for the virtual IP address pool as Static Proximity.

3）In this example, virtual IP address pools are divided in accordance with data centers because accesses from different regions need to be scheduled to different data centers.

4. Choose 『Global Load Balancing』-> 『Static Proximity』-> 『DNS Mapping Level』 and add a global DNS mapping level by setting the following parameters: Name, DNS Mapping, LDNS, and Virtual IP Address Pool.

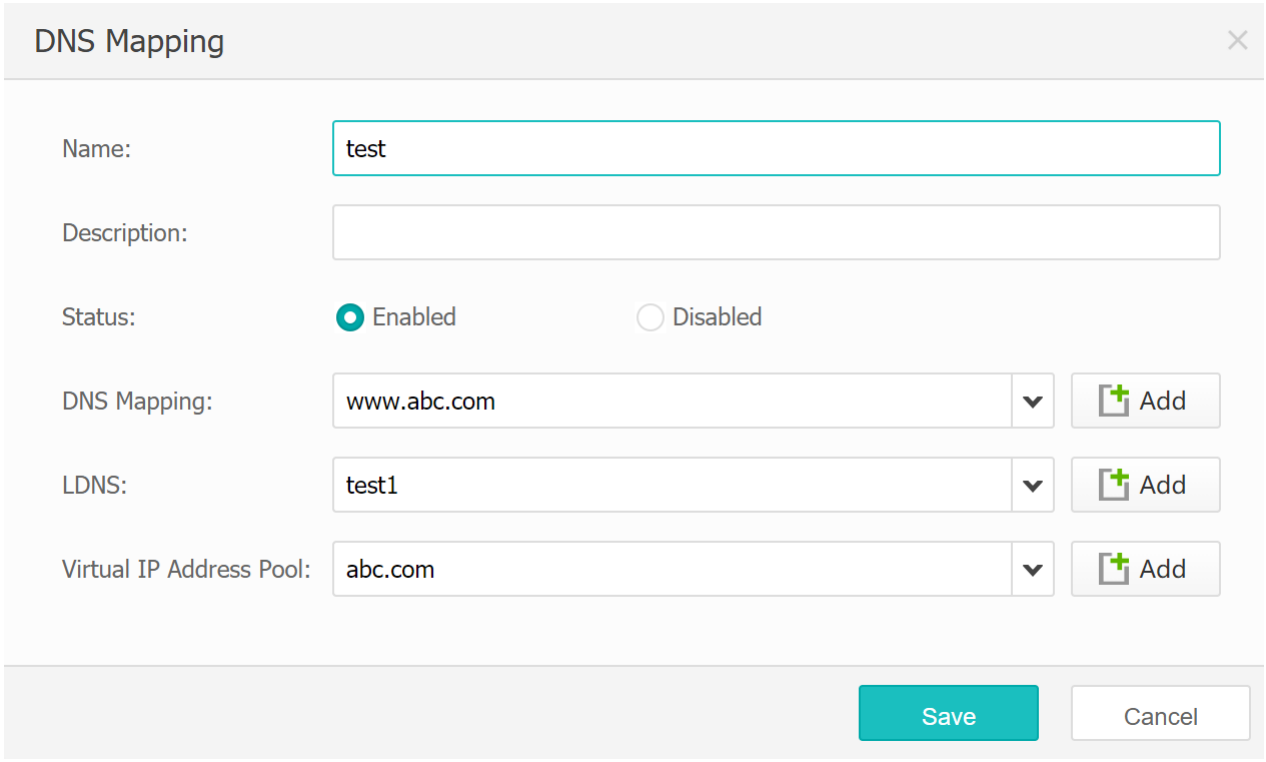
『IP Address Pool』: selects the virtual IP address pool referenced by the global DNS mapping.

『LDNS』: adds a required global LDNS set by adding an IP database and selecting a built-in ISP database, global IP database, or regional IP database.



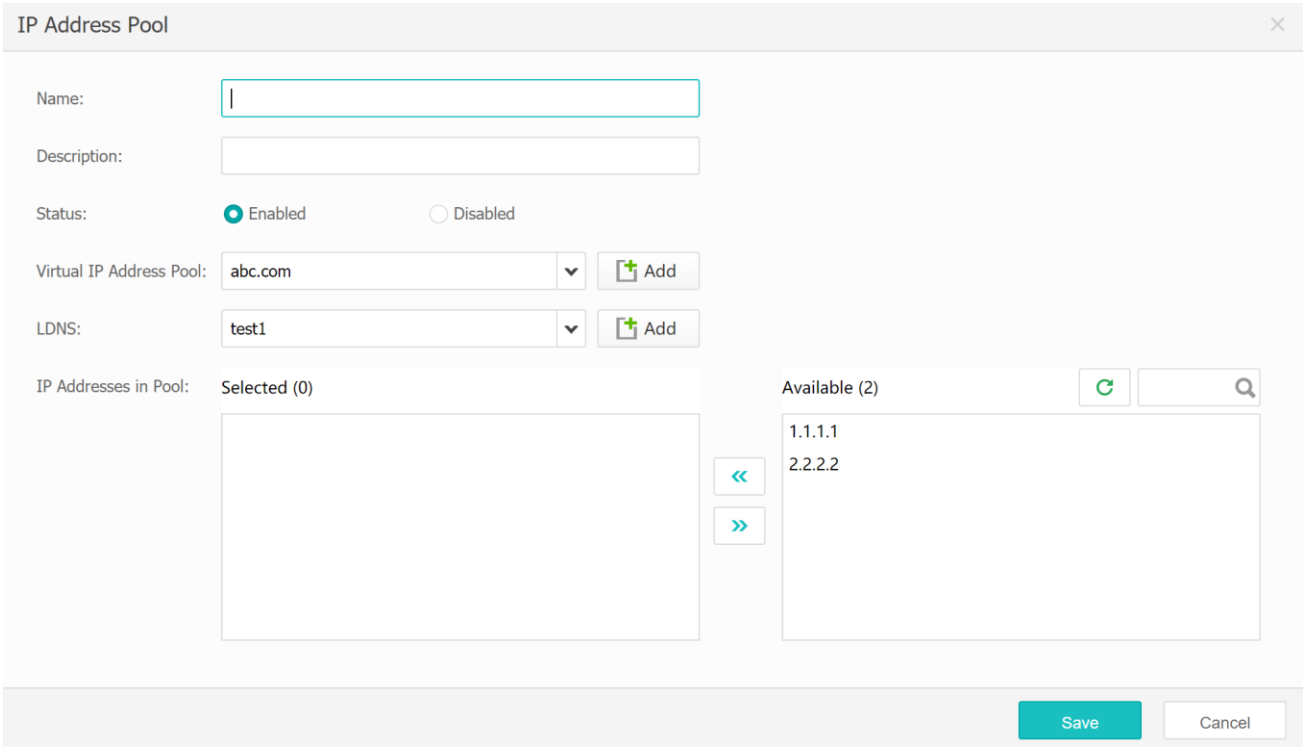
Notes : You can choose 【Objects】->【Databases】 to import or add built-in IP address ranges.

After the parameters are set, the DNS mapping level is added, as shown in the following figures.

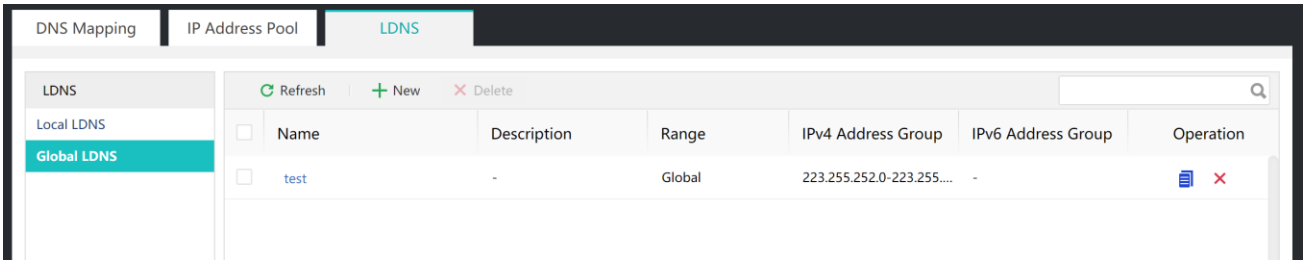


5. Choose『Global Load Balancing』-> 『Static Proximity』-> 『Virtual IP Address Pool Level』and add a global virtual IP address pool level by setting the following parameters: Name, Virtual IP Address Pool, LDNS, and Virtual IP Address Pool.

After these parameters are set according to the requirements in this example, the configuration is completed, as shown in the following figures.



The configurations for data center B are similar to the preceding steps and are not described in details here. After both data centers A and B are configured, a page appears, as shown in the following figure.



9.2.4 Global Configuration

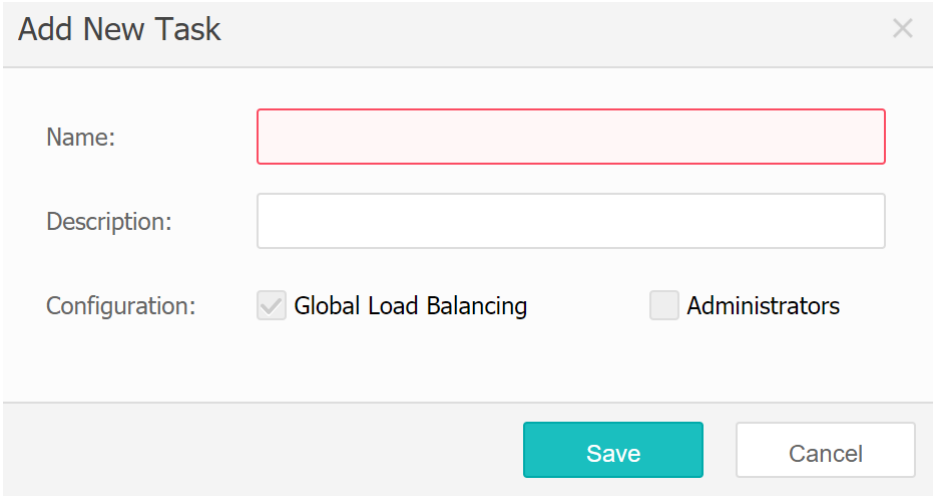
9.2.4.1 Backup Restoration

【Operation Scenarios】

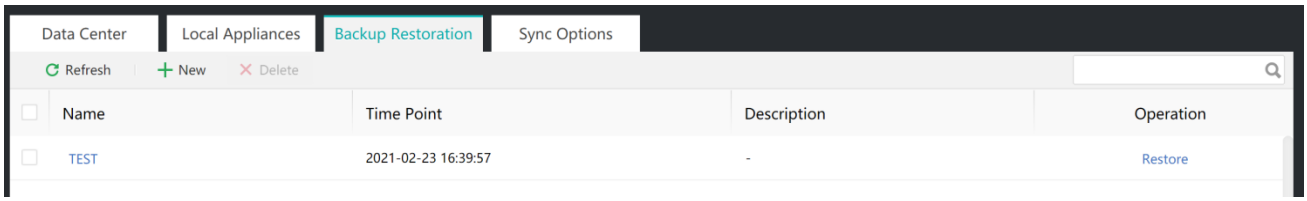
This module is used to add an existing configuration to restore the configuration at a specific time point. For example, if service exceptions or other requirements are caused due to configuration changes, this feature allows global configuration to be restored to that at a specific time point.

【Operation Procedure】

1. Click New to directly add existing configurations.



2. If you want to restore the configuration at a specific time point for some reason, click the Restore button on the right side.



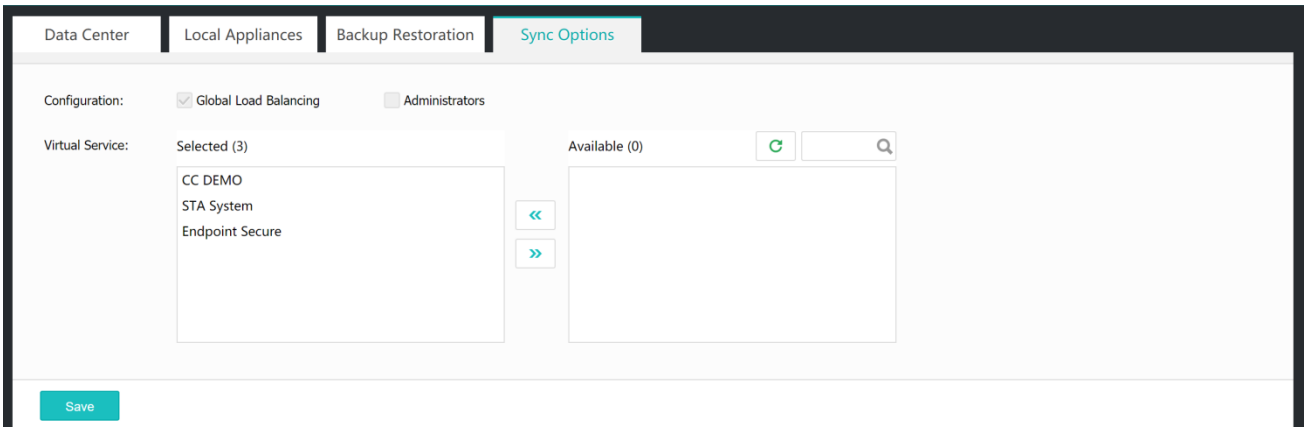
9.2.4.2 Sync Options

【Operation Scenarios】

This module is used to determine which virtual services need to be synchronized to the superior data center or global data center.

【Operation Procedure】

Click the Sync Options tab, as shown in the following figure.



Notes:

1) [Global Load Balancing]: contains configuration information of parameters for global load balancing, including [Global DNS Records], [Global Virtual IP Address Pool], [Global DNS Mapping], [Global LDNS], and [Static Proximity].

2) [Administrators]: contains configuration information of parameters, including [User] and [Role].

Chapter 10 Report Center

10.1 Report Settings

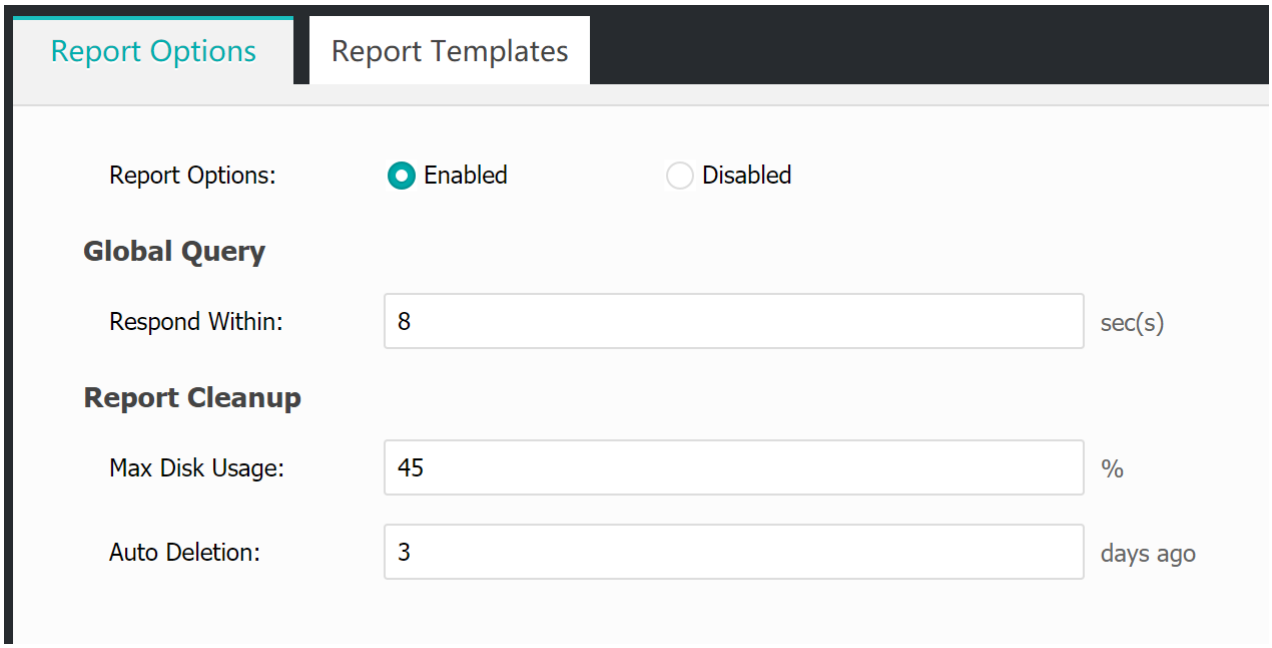
10.1.1 Report Options

【Operation Scenarios】

This module is used to collect statistics on service conditions by writing data into the report center and setting the retention time of reports.

【Operation Procedure】

Choose 【System】-> 【Report Options】-> 【Report Options】, as shown in the following figure.



In general, some parameters can be left as default, or modified as per customers' demands. These parameters are described as follows:

『Respond Within』: indicates the timeout each time you query data of global sites in the Report Center module.

『Max Disk Usage』: sets the upper limit of disk space available for reports.

『Auto Deletion』: sets the device to automatically delete the earliest report data that is retained for specific days when the used disk space does not reach the value of the 『Max Disk Usage』 parameter.

Attention: Assume that you set the Report Options parameter to Enabled and the Max Disk Usage parameter to 50%. If reports are retained for more than one year but the disk usage does not reach 50%, the device will automatically delete the earliest reports that are retained for one year.

10.1.2 Report Templates

【Operation Scenarios】

This module is used to set the statistical form of a report, including automatic generation and manual export.

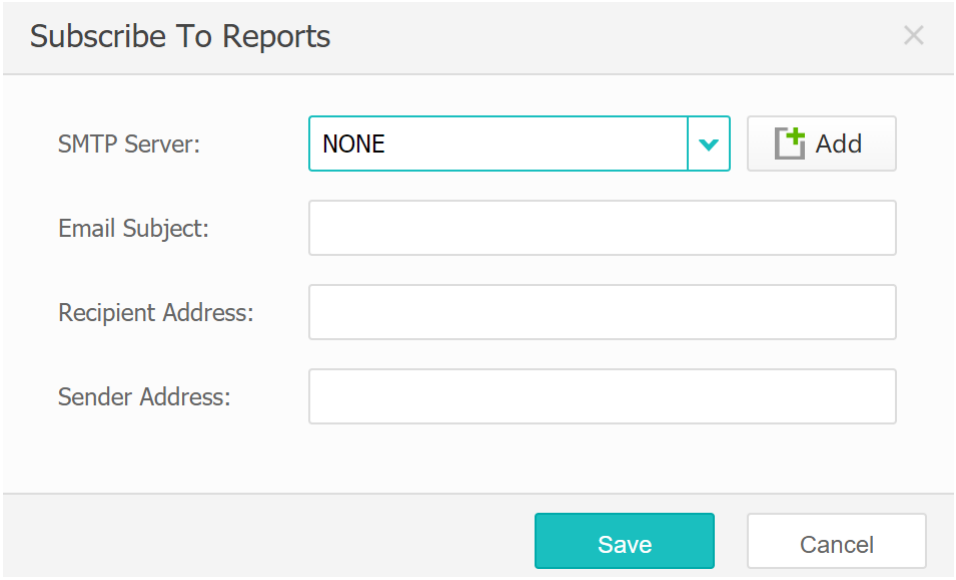
10.1.2.1 Automatic Generation

【Operation Scenarios】

This module is used to set a report generation period, and automatically generates a report based on the report template and sends it to a specified email address.

【Operation Procedure】

Choose『System』-> 『Report Options』-> 『Report Templates』-> 『Subscribe To Reports』, and set the SMTP Server, Email Subject, Recipient Address, and Sender Address parameters, as shown in the following figure.



『SMTP Server』: indicates the SMTP server by which reports are sent. Click Add to add an SMTP server. For more information, see Section 4.1.4.

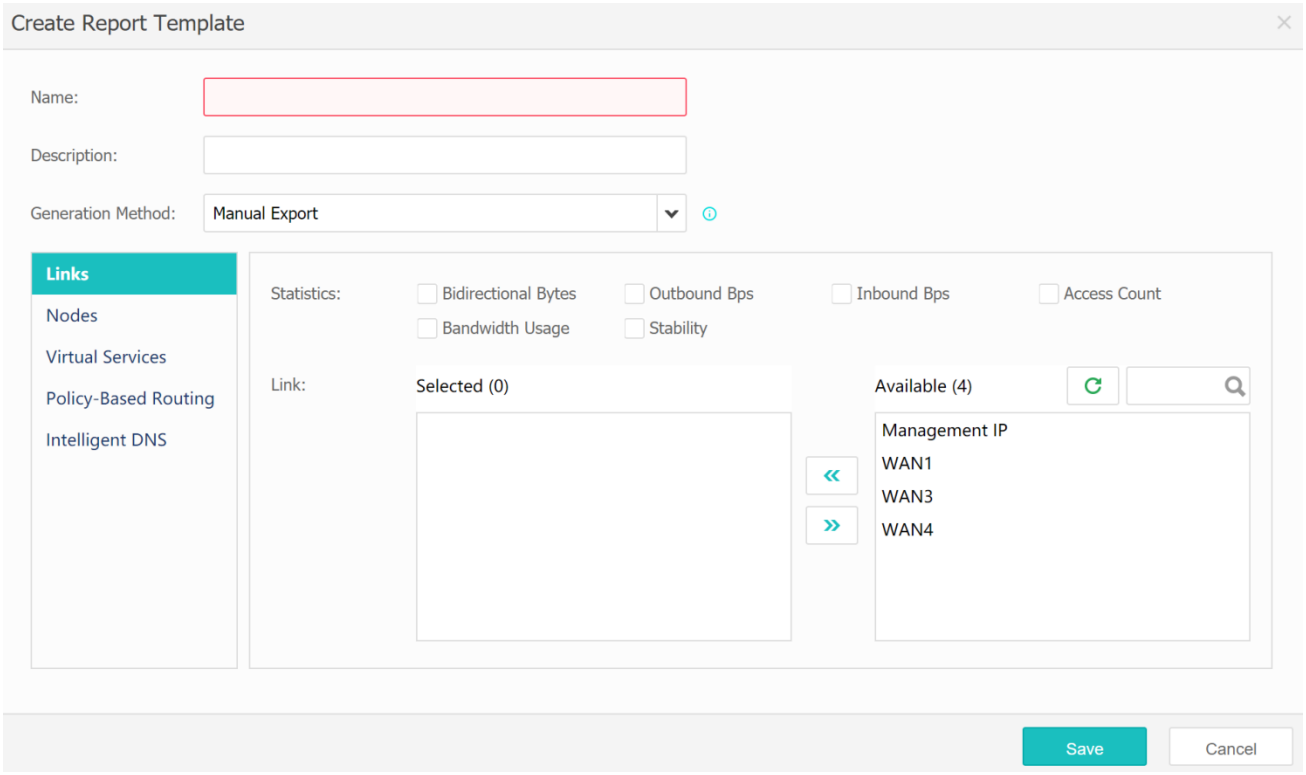
10.1.2.2 Create Report Template

【Operation Scenarios】

This module is used to set a report template and define the information that can be included in a report. You can set the report template as Manual Export or Automatic Generation.

【Operation Procedure】

Choose『System』-> 『Report Options』-> 『Report Templates』 and click Add to create a report template. Select a required statistics module from the following modules based on your business needs: [Links], [Nodes], [Virtual Services], [Policy-Based Routing], and [Intelligent DNS]. After you select the relevant module, the detailed configuration appears on the right side. See the figure below:



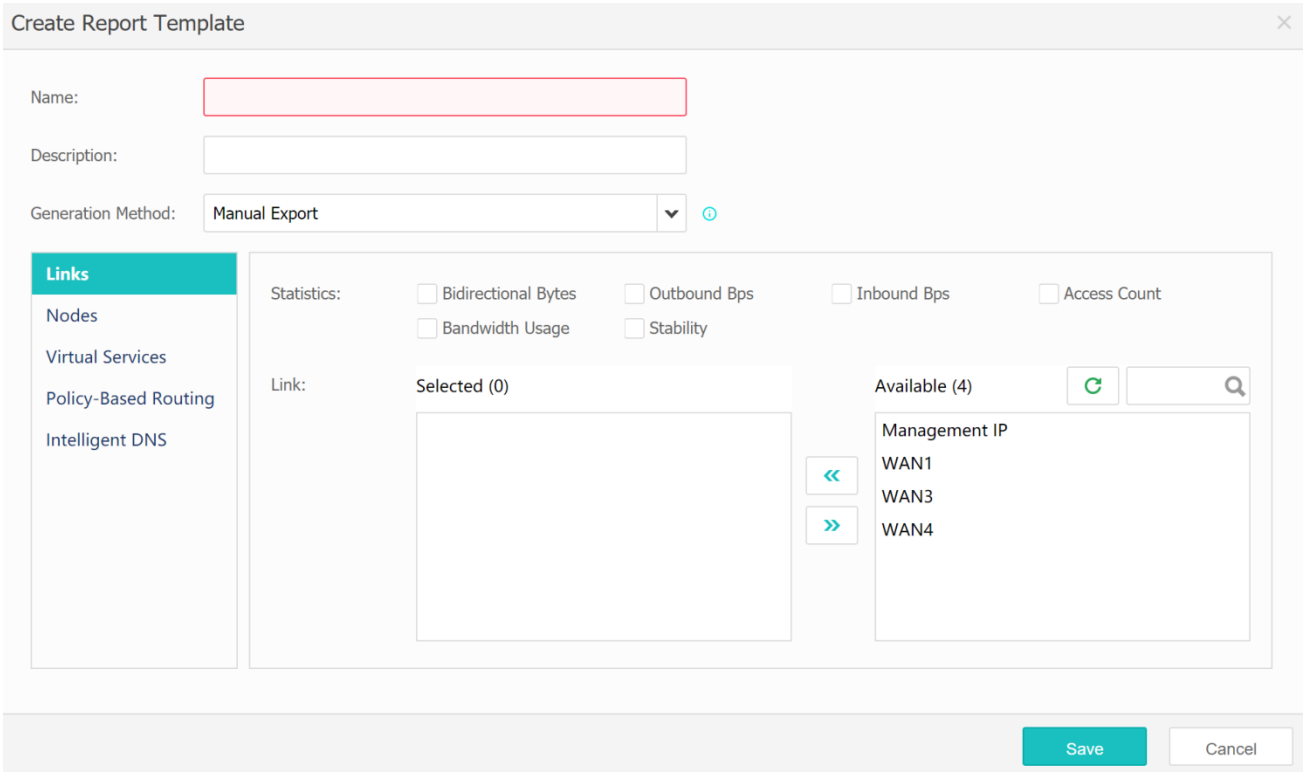
10.1.2.2.1 Links

【Operation Scenarios】

This module is used to collect statistics on the load of each link and determine whether the access load of each link is balanced and whether this link is stable.

【Operation Procedure】

Click Links and set the Name, Generation Method, Statistics, and Link parameters, as shown in the following figure.



『Statistics』: specifies projects to be counted, including bidirectional traffic, outbound traffic, inbound traffic, access count, bandwidth usage, and stability.

『Link』: selects and counts data of links listed in the box under [Selected].

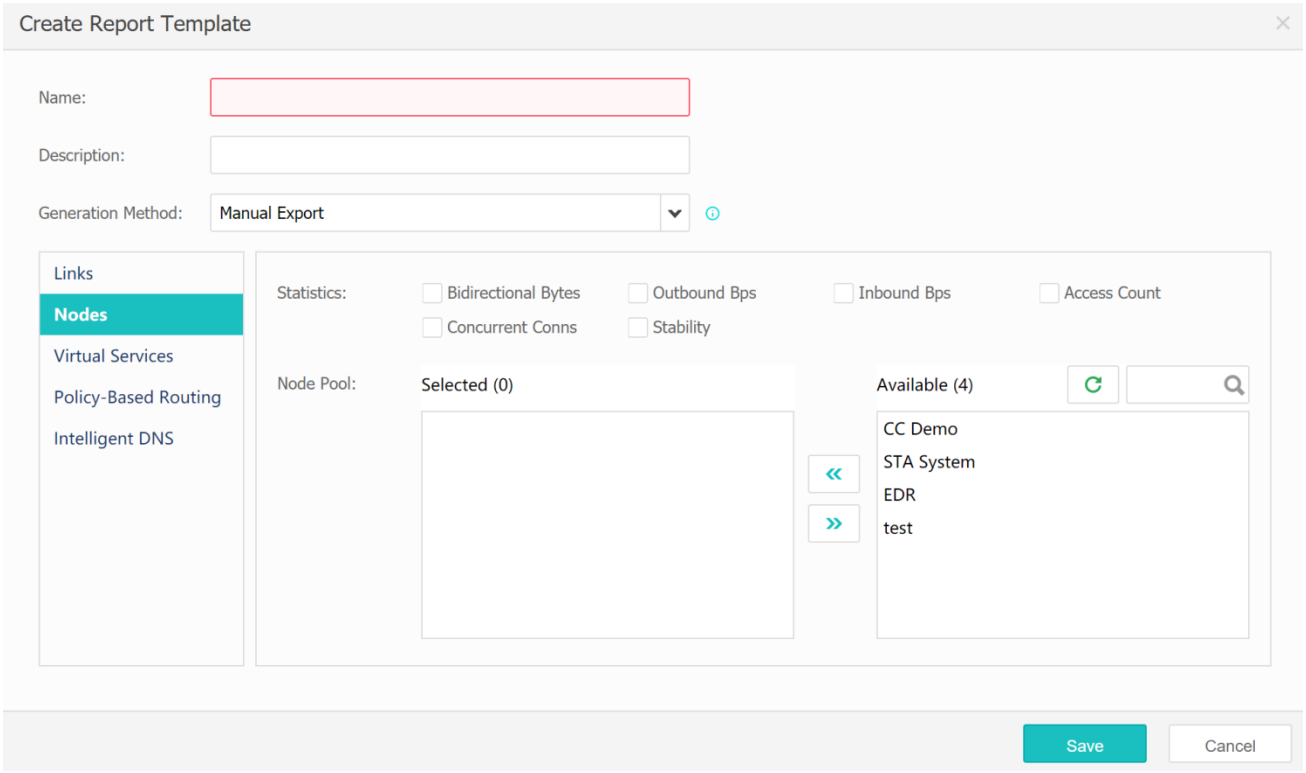
10.1.2.2.2 Nodes

【Operation Scenarios】

This module is used to collect statistics on the load of each node and determine whether the access load of each node is balanced and whether this node is stable.

【Operation Procedure】

Click Nodes and set the Name, Generation Method, Statistics, and Node Pool parameters, as shown in the following figure.



『Statistics』: specifies projects to be counted, including bidirectional traffic, outbound traffic, inbound traffic, access count, concurrent connections, and stability.

『Node Pool』: selects and counts data of node pools listed in the box under [Selected].

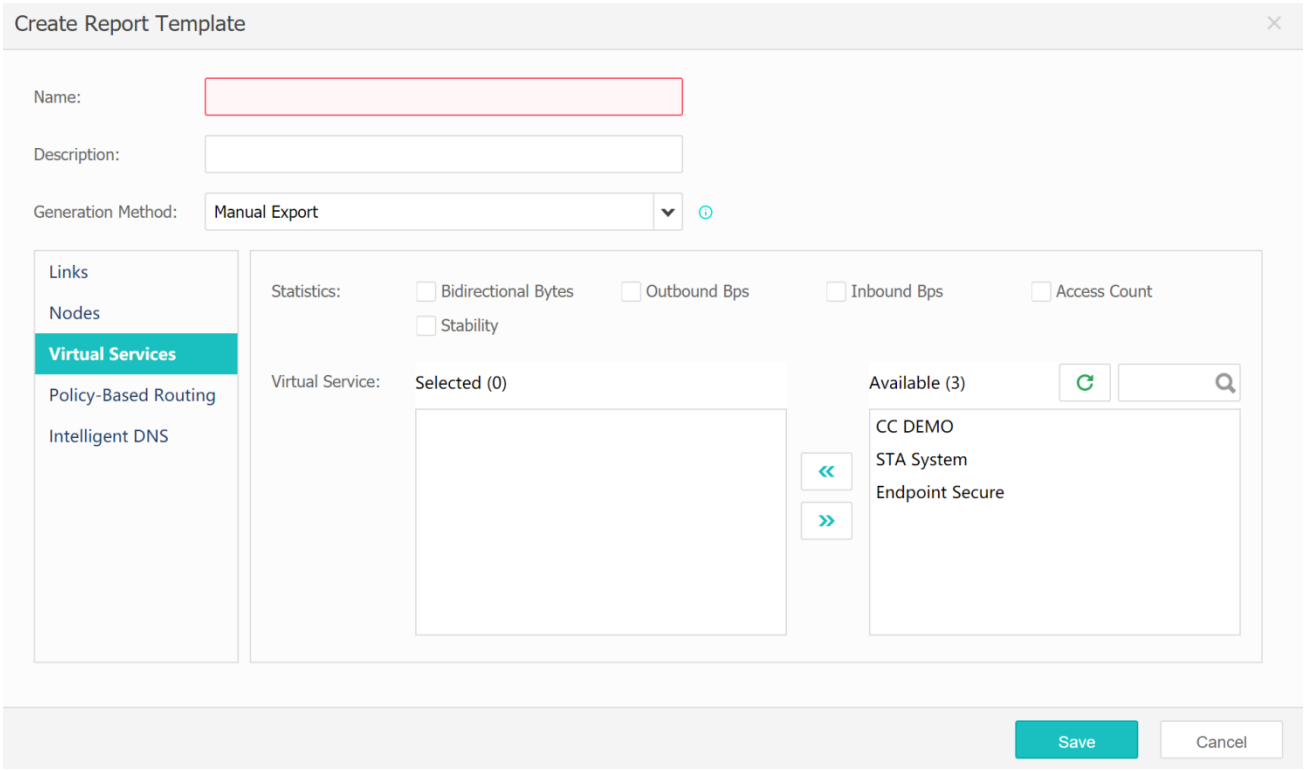
10.1.2.2.3 Virtual Services

【Operation Scenarios】

This module is used to collect statistics on the load of each virtual service and determine whether the access load of each virtual service is balanced and whether this virtual service is stable.

【Operation Procedure】

Click Virtual Services and set the Name, Generation Method, Statistics, and Virtual Service parameters, as shown in the following figure.



『Statistics』: specifies projects to be counted, including bidirectional traffic, outbound traffic, inbound traffic, access count, and stability.

『Virtual Service』: selects and counts data of virtual services listed in the box under [Selected].

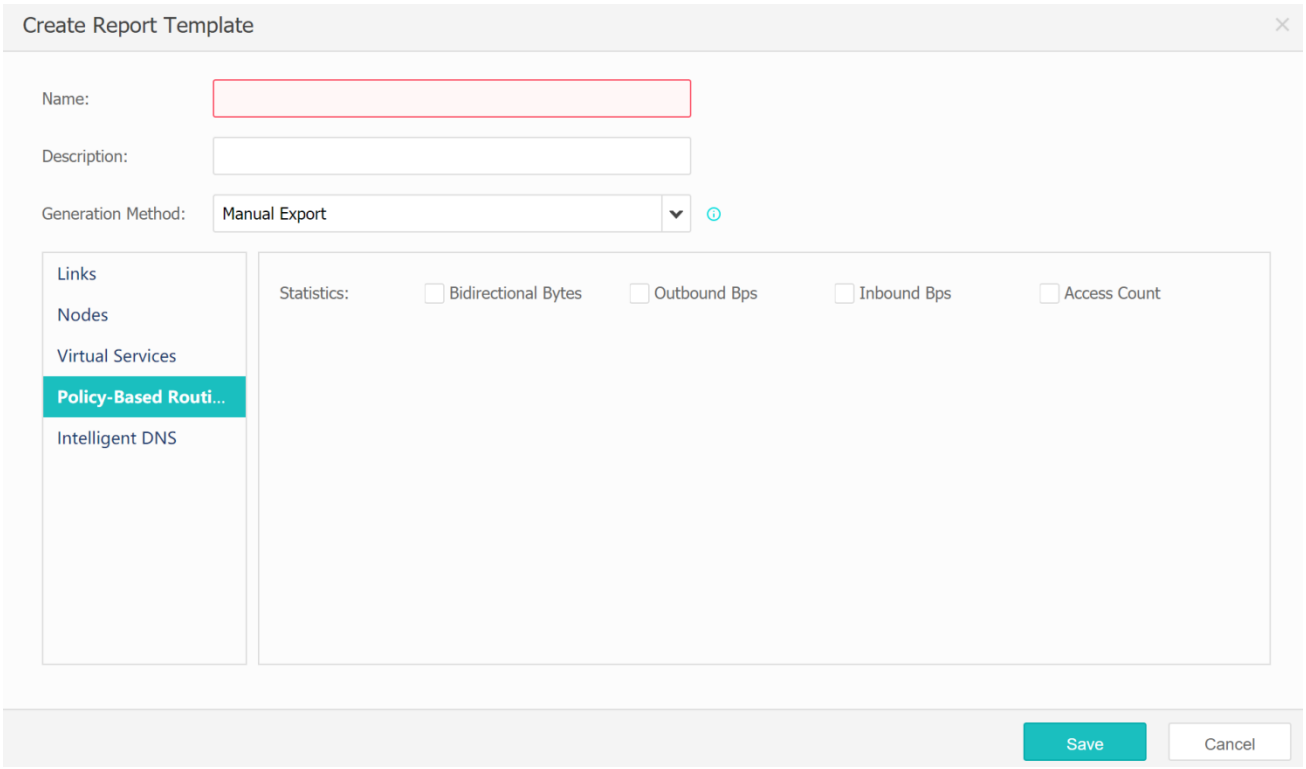
10.1.2.2.4 Policy-Based Routing

【Operation Scenarios】

This module is used to configure the statistical type of statistic reports for policy-based routing, and only data reports for the selected statistical type can be generated.

【Operation Procedure】

Click Policy-Based Routing and set the Name, Generation Method, and Statistics parameters, as shown in the following figure.



『Statistics』: specifies projects to be counted, including bidirectional traffic, outbound traffic, inbound traffic, and access count.

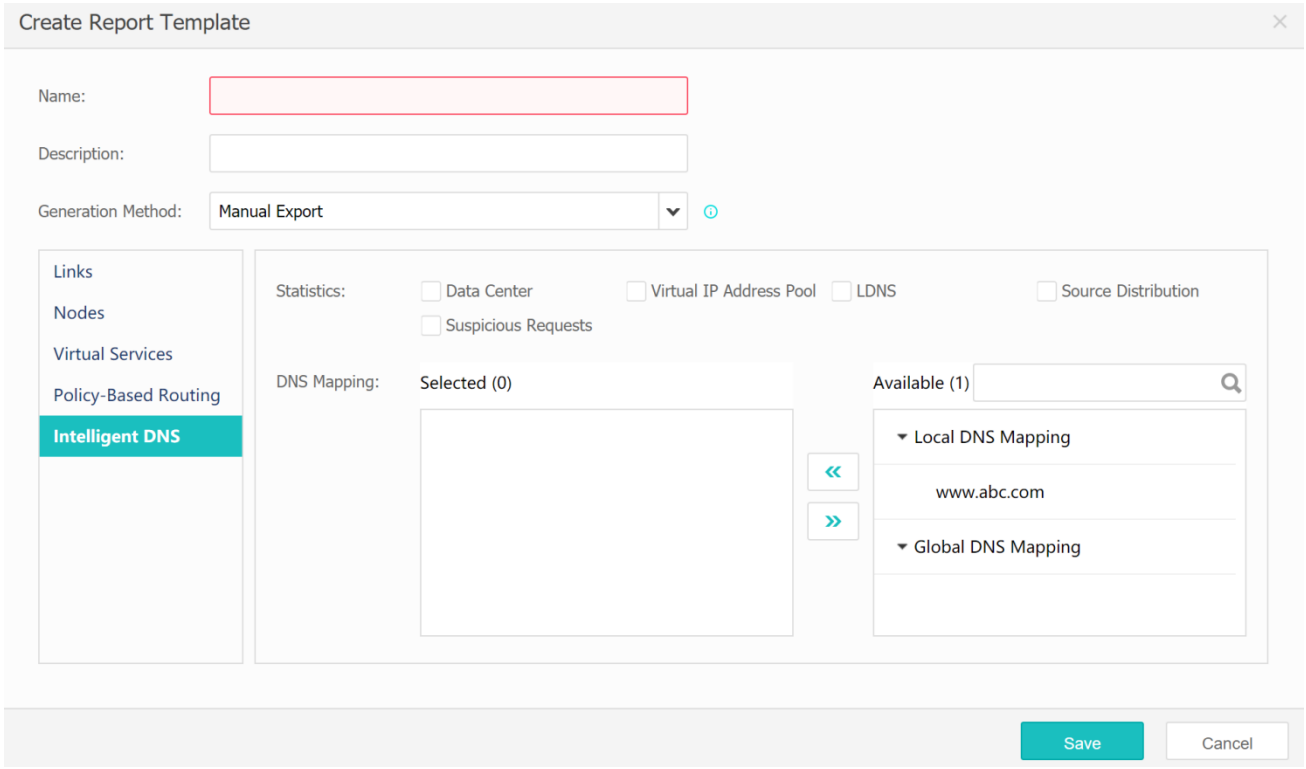
10.1.2.2.5 Intelligent DNS

【Operation Scenarios】

This module is used to configure the statistical type of statistic reports for intelligent DNS, and only data reports for the selected statistical type can be generated.

【Operation Procedure】

Click Intelligent DNS and set the Name, Generation Method, Statistics, and DNS Mapping parameters, as shown in the following figure.



『Statistics』: specifies projects to be counted, including data center, virtual IP address pool, LDNS, source distribution, and suspicious requests.

『DNS Mapping』: selects DNS mappings for which reports are generated, that is a level-1 intelligent DNS scheduling policy. This parameter is available for local and global DNS mappings.

10.2 Report Center

10.2.1 Enter Report Center

【Operation Scenarios】

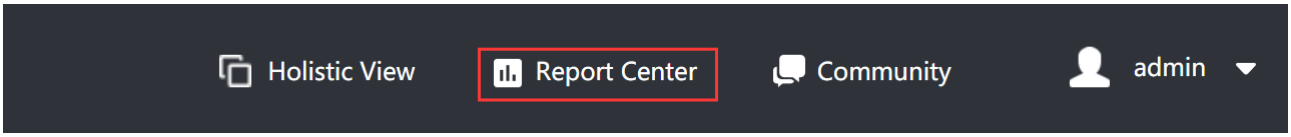
This module allows you to log in to the Report Center and view various statistical information of ADC, including 『Link Statistics』, 『Node Statistics』, 『Virtual Service Statistics』, 『Policy-based Routing』, 『Intelligent DNS Statistics』, and 『Cluster Status Statistics』.

【Prerequisites】

『System』 -> 『Report Options』 -> 『Report Options』 is enabled.

【Operation Procedure】

Click Report Center in the upper-right corner on the console page to open the Report Center page, as shown in the following figure.



10.2.2 Report Center

10.2.2.1 Link Statistics

【Operation Scenarios】

When applying to link load balancing, an ADC needs to collect statistics on situations of link load balancing, and query them in details to know whether links are stable and scheduled. The range for statistics includes『Flow』, 『Visits』,『Bandwidth Usage』, and『Stability』.

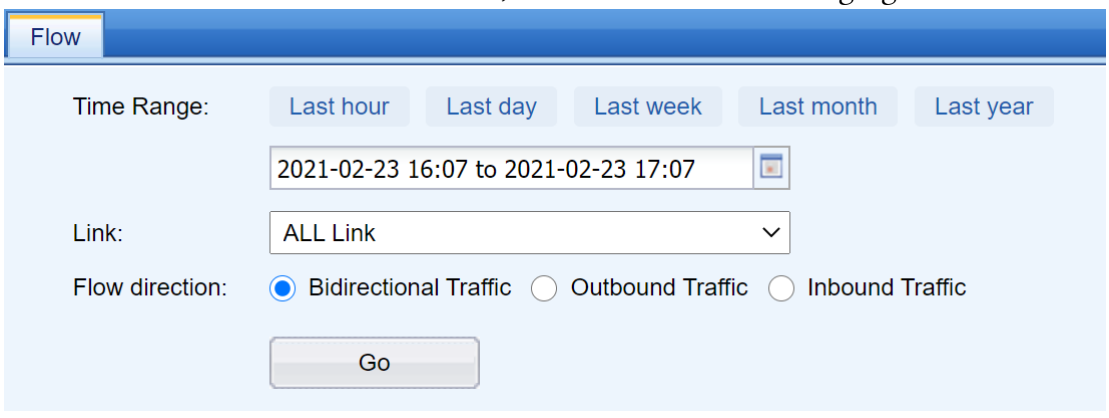
10.2.2.1.1 Flow

【Operation Scenarios】

This module is used to collect statistics on outbound traffic passing the ADC. This helps you know LAN's overall traffic.

【Operation Procedure】

Choose『Link Statistics』-> 『Flow』, and select the time range, link, and flow direction based on your needs to collect statistics on the traffic, as shown in the following figure.



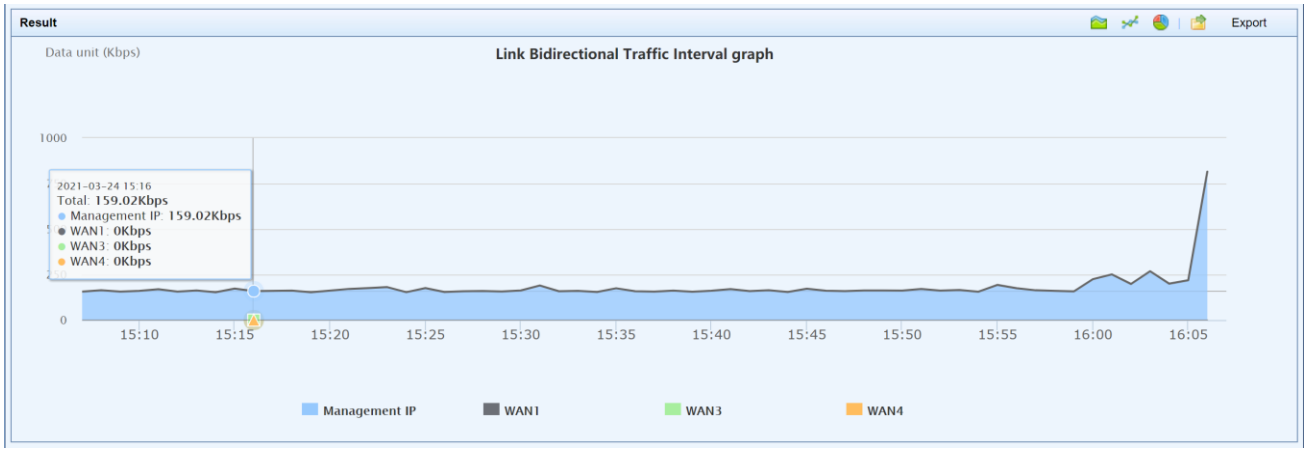
『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Link』: specifies the link through which the traffic passes. You can select ALL Link, LAN, or WAN from the drop-down list.

『Flow direction』: specifies the traffic to be counted, including bidirectional traffic, outbound traffic, and inbound traffic.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the interval graph is

selected.



Click Export to display a traffic graph according to the preceding configurations and then generate a report in a PDF format.

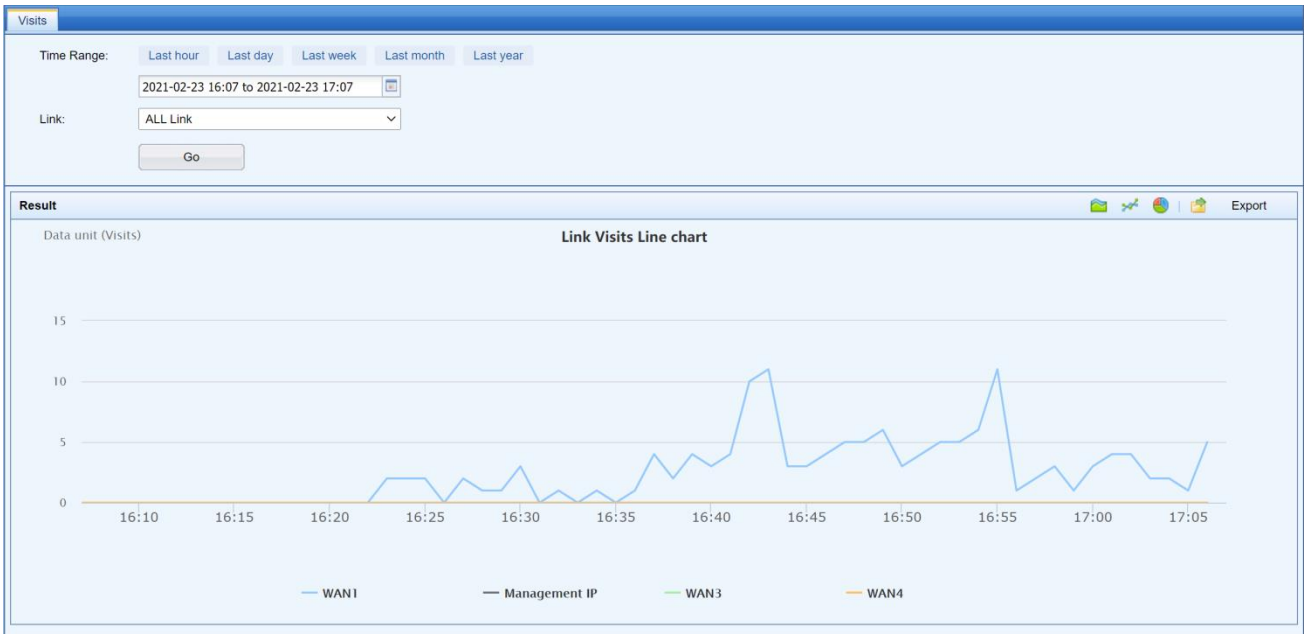
10.2.2.1.2 Visits

【Operation Scenarios】

This module is used to count the number of times a link is accessed. This helps you view the link usage.

【Operation Procedure】

Choose『Report』-> 『Links』-> 『Visits』, and select the time range and link based on your needs to collect statistics on the access count, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Link』: specifies the link through which the traffic passes. You can select ALL Link or WAN from the drop-down list.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the line chart is selected.

Click Export to display a link visits line chart according to the preceding configurations and then generate a report in a PDF format.

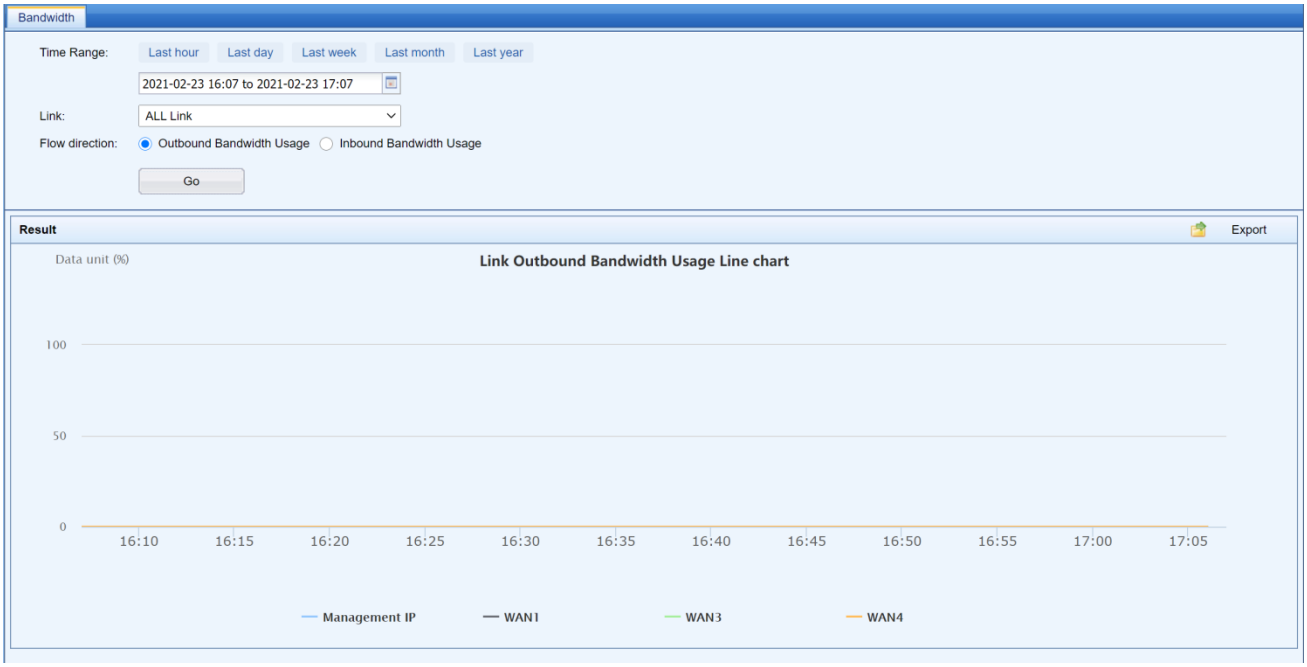
10.2.2.1.3 Bandwidth

【Operation Scenarios】

This module is used to collect statistics on bandwidth usage, and allows you to check whether links are used and scheduled.

【Operation Procedure】

Choose『Report』-> 『Links』-> 『Bandwidth Usage』 and select the time range, link, and flow direction based on your needs to collect statistics on the bandwidth usage, as shown in the following figure.

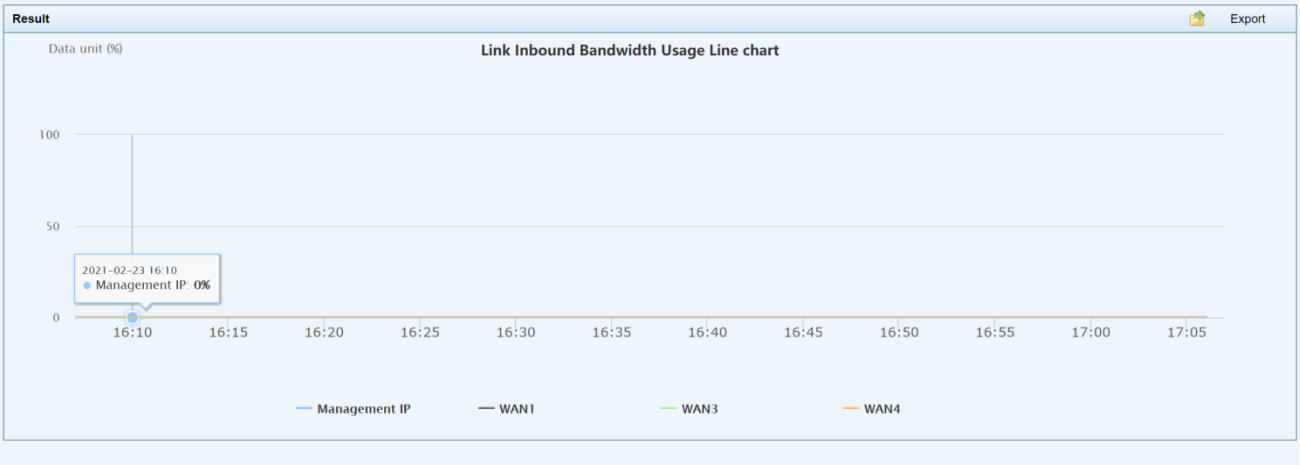


『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Link』: specifies the link through which the traffic passes. You can select ALL Link, LAN, or WAN from the drop-down list.

『Flow direction』: specifies the traffic to be counted, including outbound bandwidth usage and inbound bandwidth usage.

Click Go to generate a query result, that is, a bandwidth usage line chart.



Click Export to display a traffic graph according to the preceding configurations and then generate a report in a PDF format.

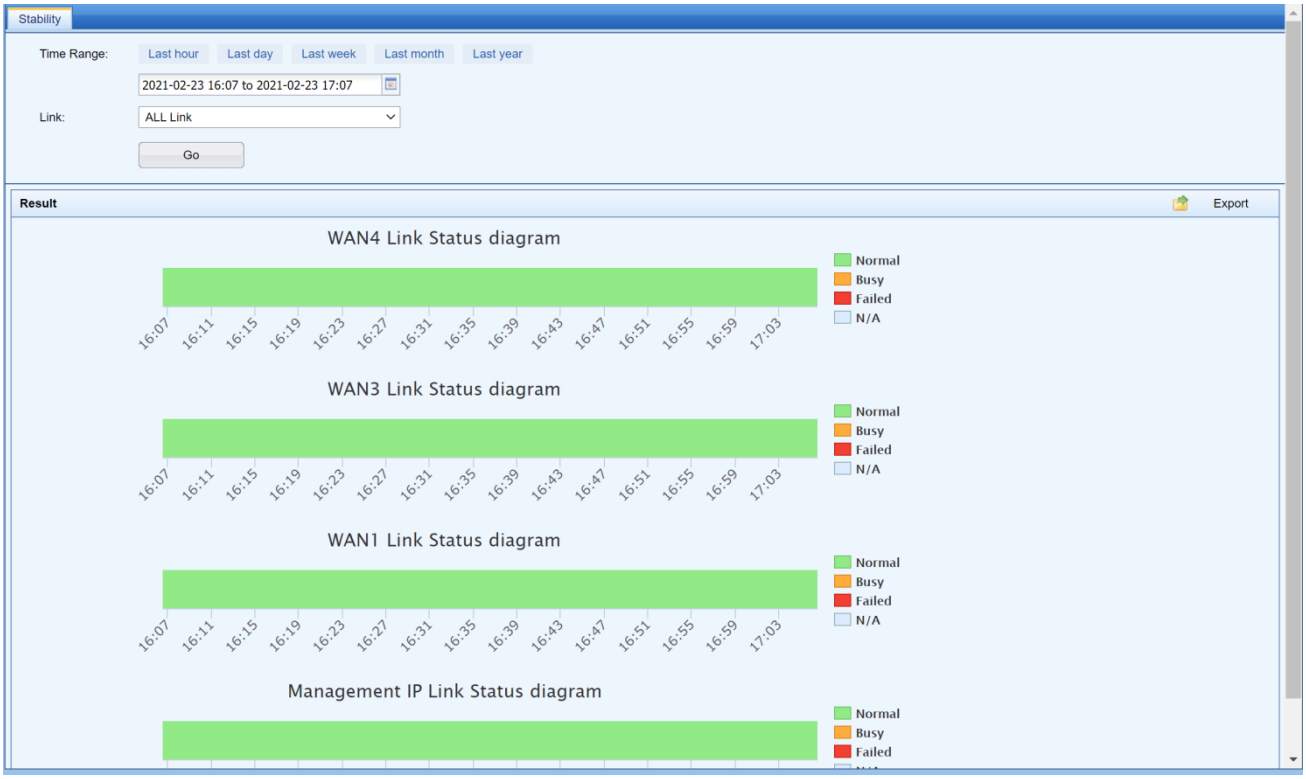
10.2.2.1.4 Stability

【Operation Scenarios】

This module is used to collect statistics on the stability of link status.

【Operation Procedure】

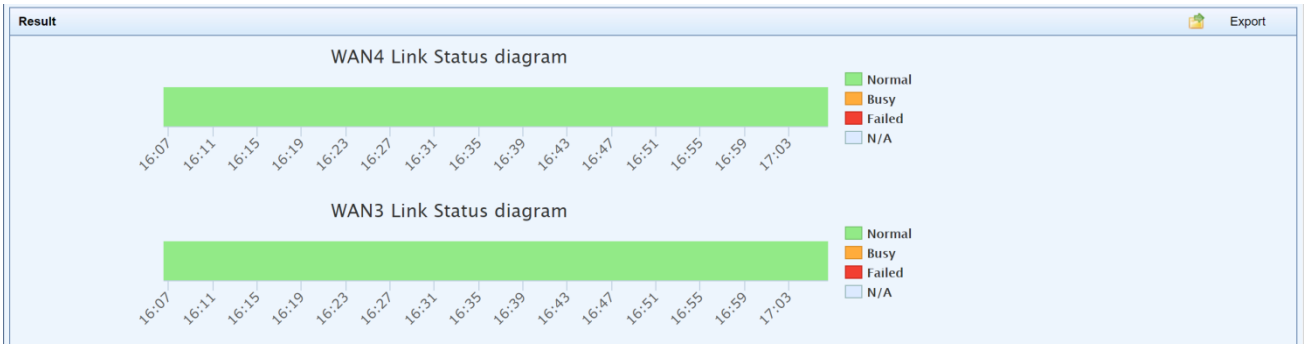
Choose『Report』-> 『Links』-> 『Stability』, and select the time range and link based on your needs to collect statistics on the stability, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Link』: specifies the link through which the traffic passes. You can select ALL Link or WAN from the drop-down list.

Click Go to generate a query result, that is, a WAN interface link status diagram.



Click Export to display a status diagram according to the preceding configurations and then generate a report in a PDF format.

10.2.2.2 Node Statistics

【Operation Scenarios】

When applying to app load balancing, an ADC needs to collect statistics on the load of each node, and query in details to know whether nodes are stable and scheduled. The range for statistics includes『Flow』,『Visits』,『Concurrent connections』, and『Stability』.

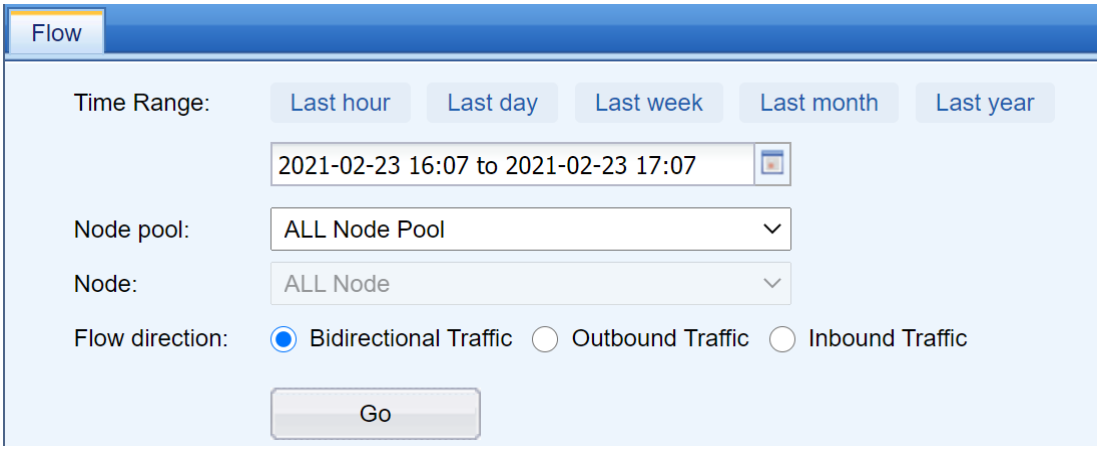
10.2.2.2.1 Flow

【Operation Scenarios】

This module is used to collect statistics on specified node pool and node, and allows you to know whether this node is scheduled.

【Operation Procedure】

Choose『Report』-> 『Nodes』-> 『Flow』and select the time range, node pool, node, and flow direction based on your needs to collect statistics on the traffic, as shown in the following figure.



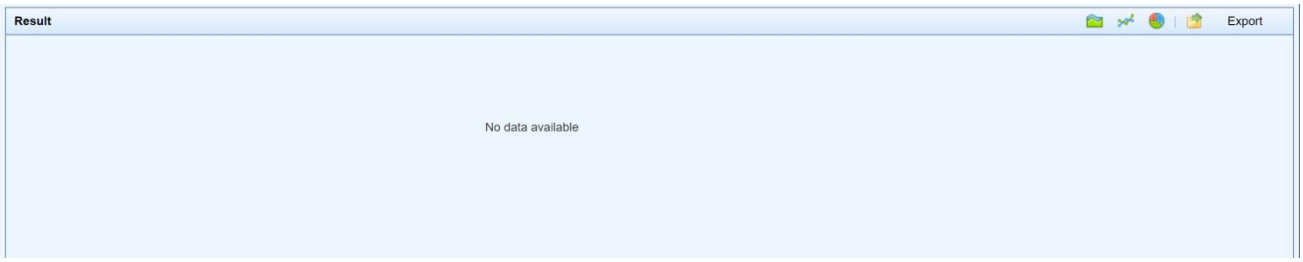
『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Node Pool』: specifies the node pool for which statistics is made on traffic.

『Node』: specifies the node for which statistics is made on traffic.

『Flow direction』: specifies the traffic to be counted, including bidirectional traffic, outbound traffic, and inbound traffic.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart.



Click Export to display a traffic graph according to the preceding configurations and then generate a report in a PDF format.

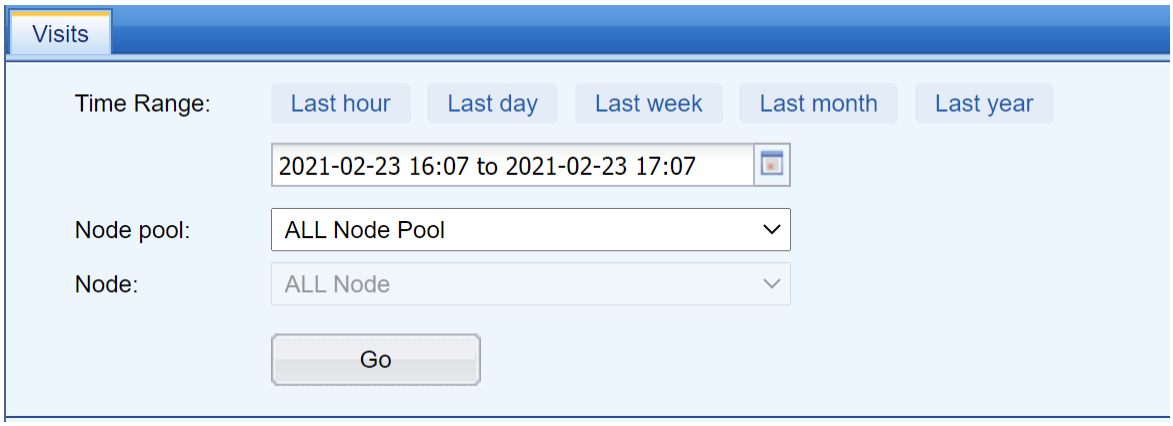
10.2.2.2.2 Visits

【Operation Scenarios】

This module is used to collect statistics on the access count for specified node pool and node.

【Operation Procedure】

Choose『Report』-> 『Nodes』-> 『Visits』, and select the time range, node pool, and node based on your needs to collect statistics on the access count, as shown in the following figure.

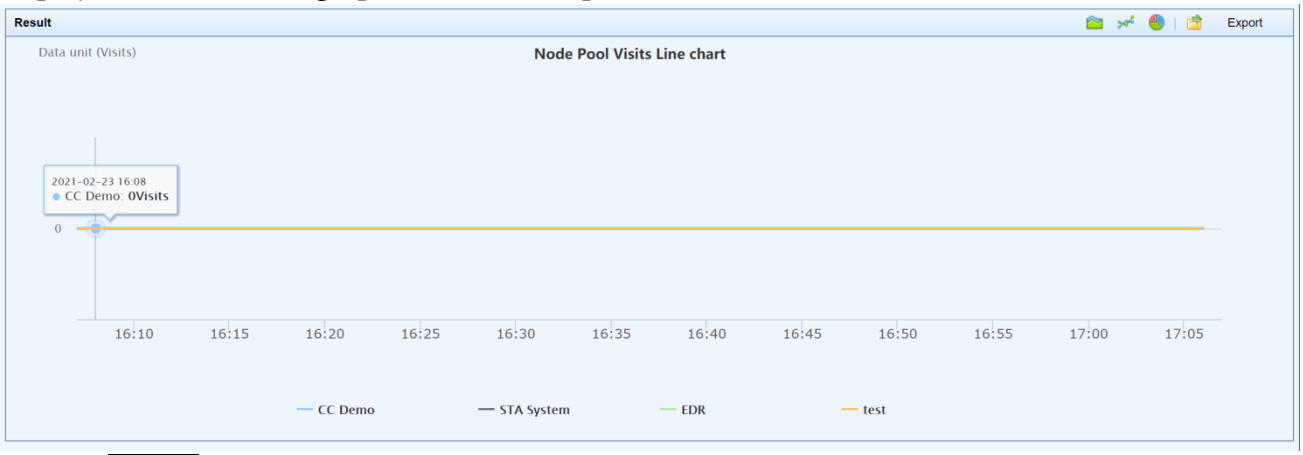


『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Node Pool』: specifies the node pool for which statistics is made on traffic.

『Node』: specifies the node for which statistics is made on traffic.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart.



Click Export to display a node pool visits line chart according to the preceding configurations and then generate a report in a PDF format.

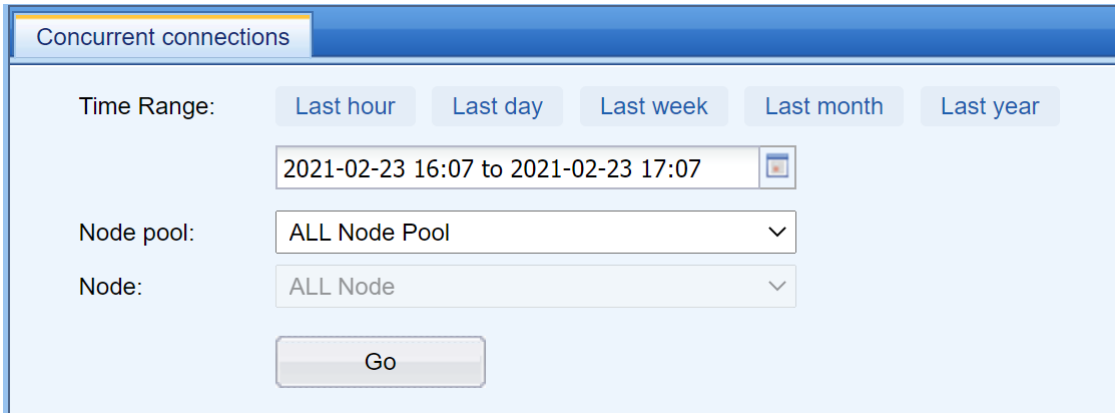
10.2.2.2.3 Concurrent Connections

【Operation Scenarios】

This module is used to collect statistics on the concurrent connections of specified node pool and node, and allows you to know whether this node is scheduled.

【Operation Procedure】

Choose『Report』-> 『Nodes』-> 『Concurrent connections』and select the time range, node pool, and node based on your needs to collect statistics on the concurrent connections, as shown in the following figure.

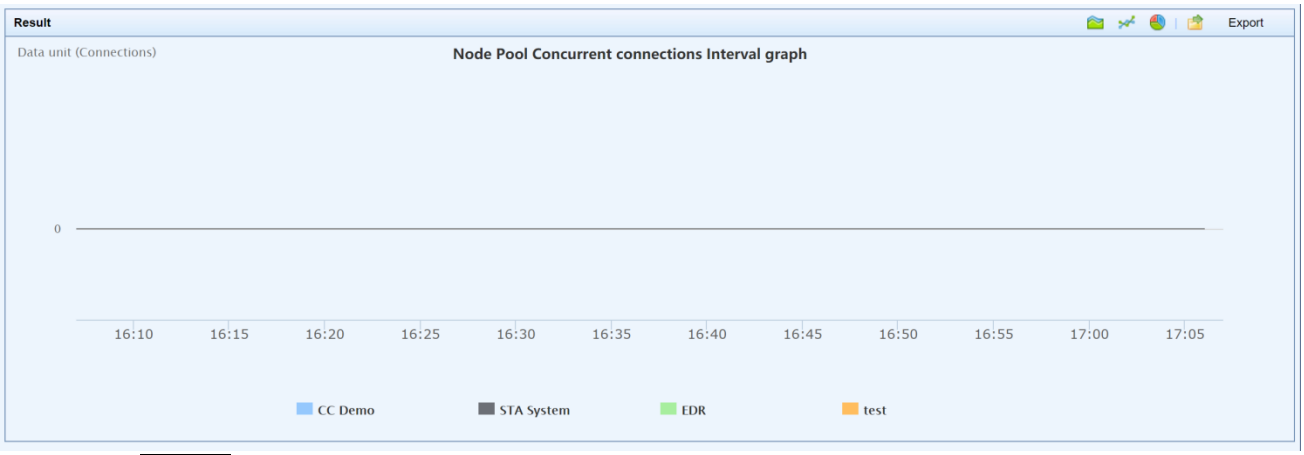


『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Node Pool』: specifies the node pool for which statistics is made on traffic.

『Node』: specifies the node for which statistics is made on traffic.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart.



Click Export to display a node pool concurrent connections interval graph according to the preceding configurations and then generate a report in a PDF format.

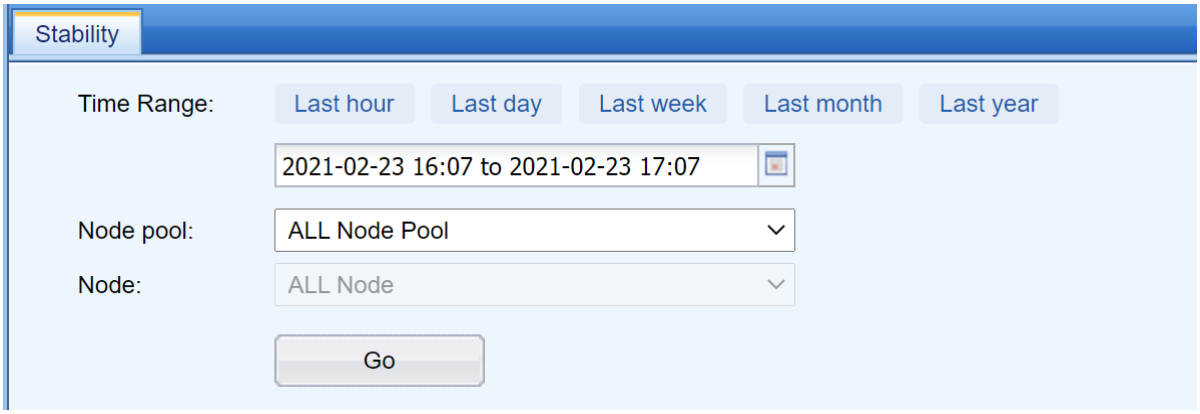
10.2.2.2.4 Stability

【Operation Scenarios】

This module is used to collect statistics on the stability of specified node pool and node.

【Operation Procedure】

Choose『Report』-> 『Nodes』-> 『Stability』and select the time range, node pool, and node based on your needs to collect statistics on the stability, as shown in the following figure.

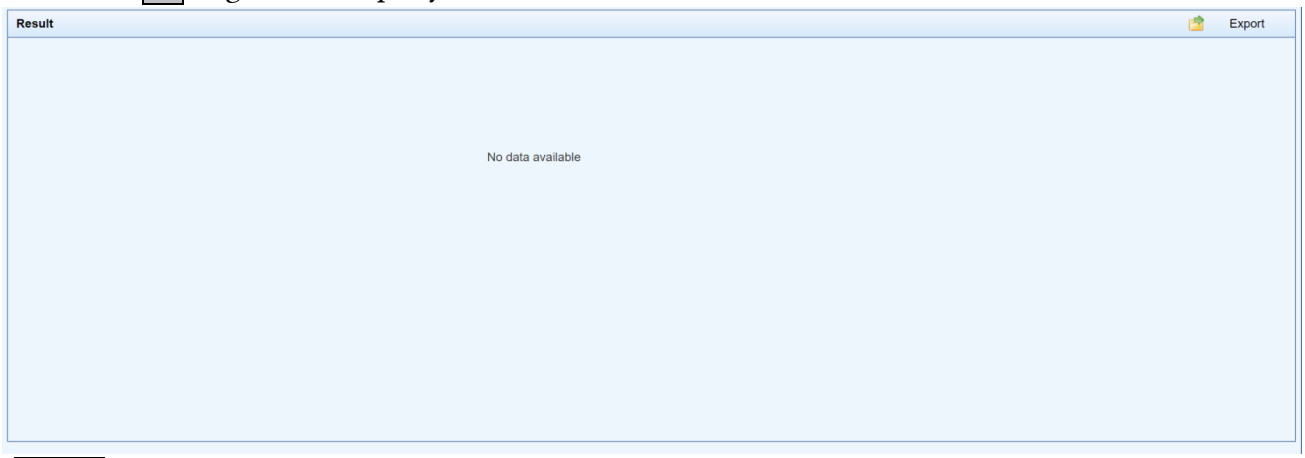


『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Node Pool』: specifies the node pool for which statistics is made on traffic.

『Node』: specifies the node for which statistics is made on traffic.

Click Go to generate a query result.



Click Export to display a node pool status diagram according to the preceding configurations and then generate a report in a PDF format.

10.2.2.3 Virtual Service Statistics

【Operation Scenarios】

When applying to app load balancing, an ADC needs to collect statistics on situations of virtual services, and query them in details. The range for statistics includes 『Flow』, 『Visits』, and 『Stability』.

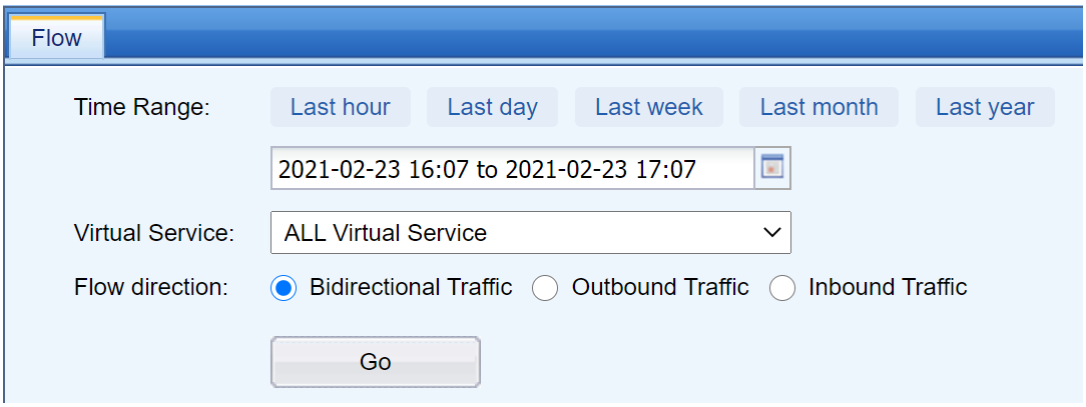
10.2.2.3.1 Flow

【Operation Scenarios】

This module is used to collect statistics on traffic information of virtual services, and allows you to view traffic used by the virtual services.

【Operation Procedure】

Choose『Report』-> 『Virtual Services』-> 『Flow』and select the time range, virtual service, and flow direction based on your needs to collect statistics on the traffic, as shown in the following figure.

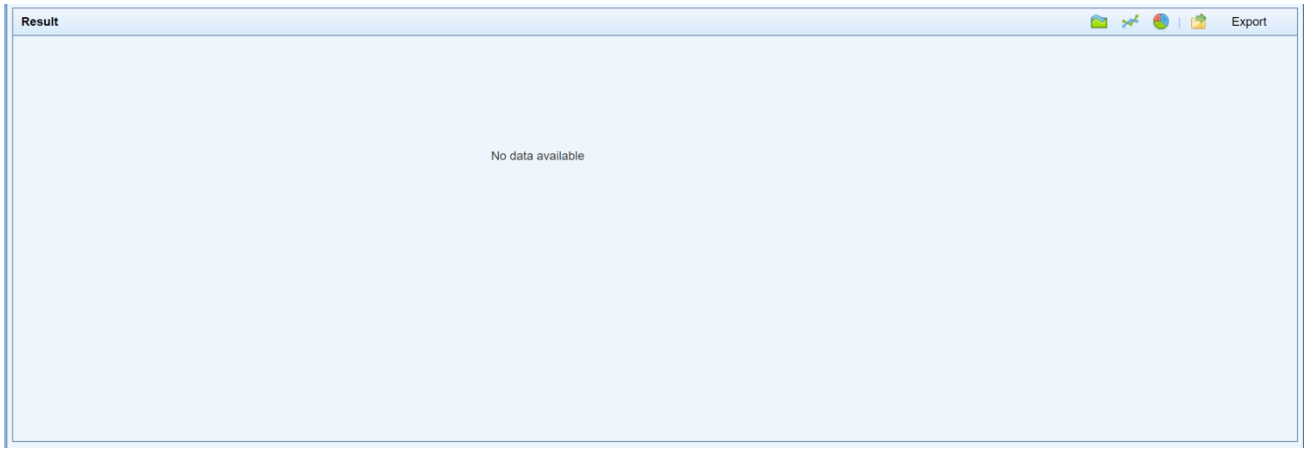


『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Virtual Service』: specifies the virtual service to be counted.

『Flow direction』: specifies the traffic to be counted, including bidirectional traffic, outbound traffic, and inbound traffic.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the interval graph is selected.



Click Export to display a traffic graph according to the preceding configurations and then generate a report in a PDF format.

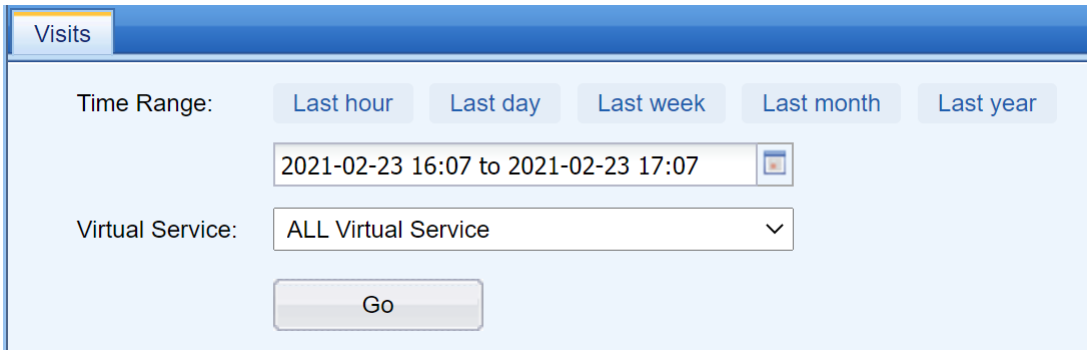
10.2.2.3.2 Visits

【Operation Scenarios】

This module is used to collect statistics on the access count of virtual services.

【Operation Procedure】

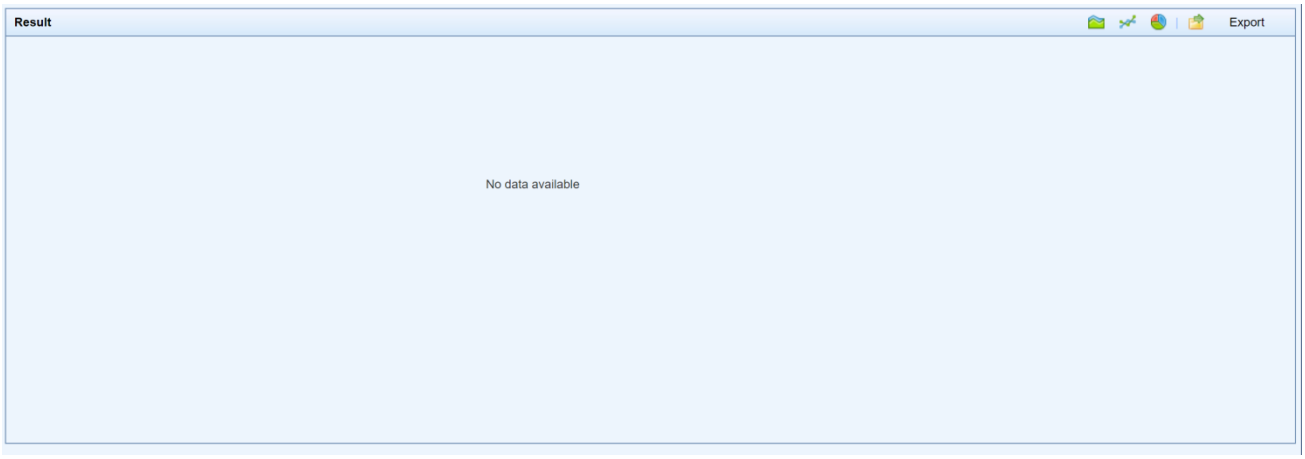
Choose『Report』-> 『Virtual Services』-> 『Visits』and select the time range and virtual service based on your needs to collect statistics on the access count, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Virtual Service』: specifies the virtual service to be counted.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the line chart is selected.



Click Export to display a virtual service visits line chart according to the preceding configurations and then generate a report in a PDF format.

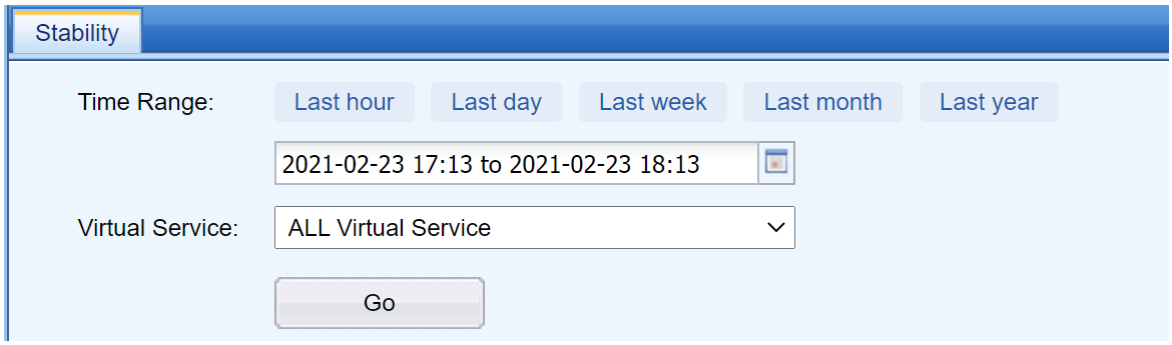
10.2.2.3.3 Stability

【Operation Scenarios】

This module is used to collect statistics on the stability of virtual services, and allows you to know whether the virtual services are stable.

【Operation Procedure】

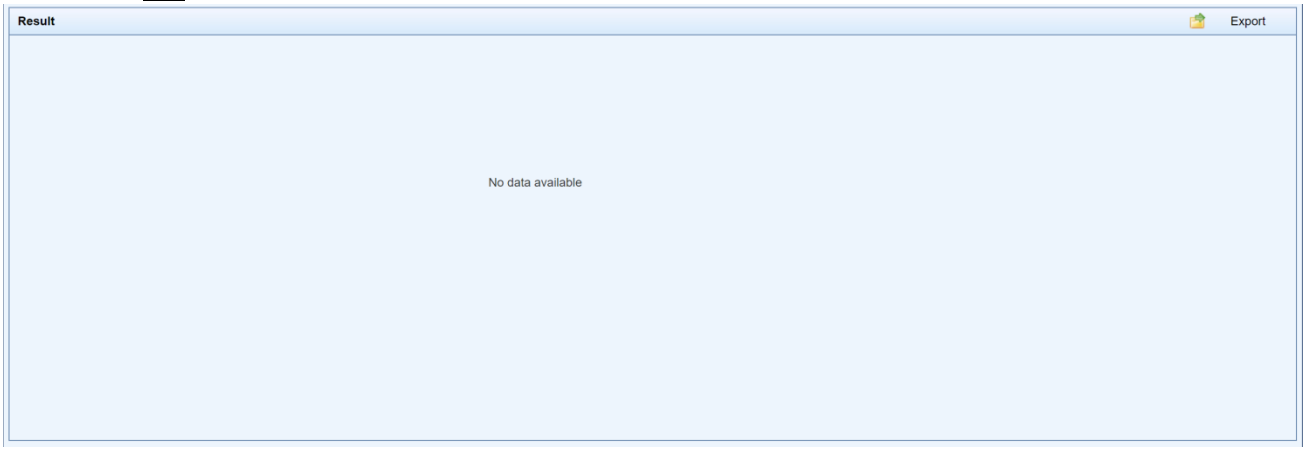
Choose『Report』-> 『Virtual Services』-> 『Stability』and select the time range and virtual service based on your needs to collect statistics on the stability, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Virtual Service』: specifies the virtual service to be counted.

Click Go to generate a query result, that is, a virtual service status diagram.



Click Export to display a virtual service status diagram according to the preceding configurations and then generate a report in a PDF format.

10.2.2.4 Policy-based Routing

【Operation Scenarios】

When applying to outbound link load balancing, an ADC needs to collect statistics on situations of policy-based routing, and query them in details. The range for statistics includes『Flow』and『Visits』.

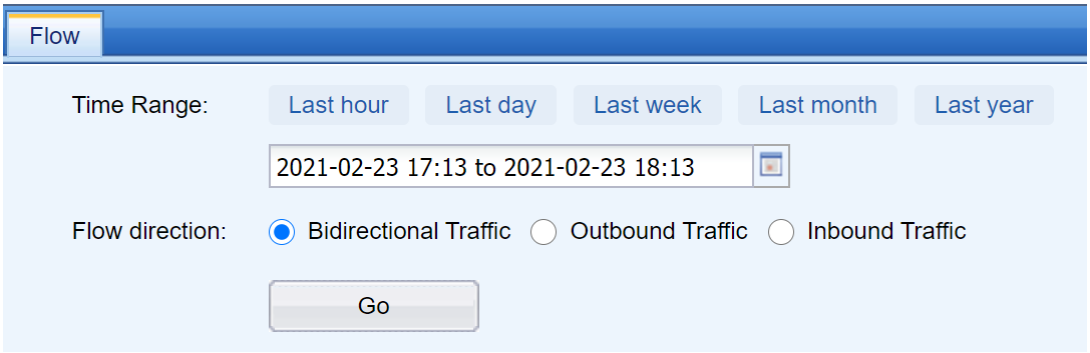
10.2.2.4.1 Flow

【Operation Scenarios】

This module is used to collect statistics on traffic passing an ADC.

【Operation Procedure】

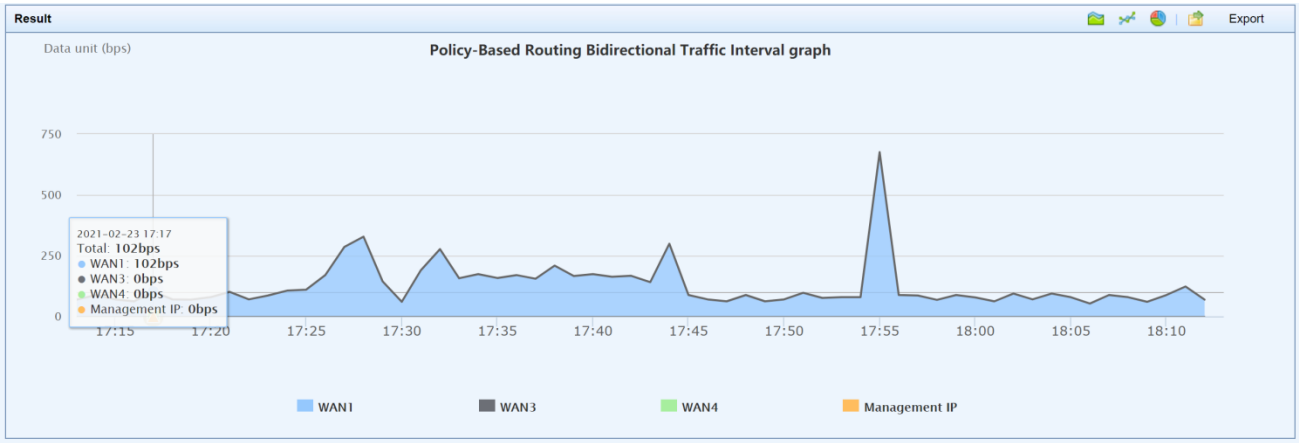
Choose『Report』-> 『Policy-Based Routing』-> 『Flow』and select the time range and flow direction based on your needs to collect statistics on the traffic, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Flow direction』: specifies the traffic to be counted, including bidirectional traffic, outbound traffic, and inbound traffic.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the interval graph is selected.



Click Export to display a traffic graph according to the preceding configurations and then generate a report in a PDF format.

10.2.2.4.2 Visits

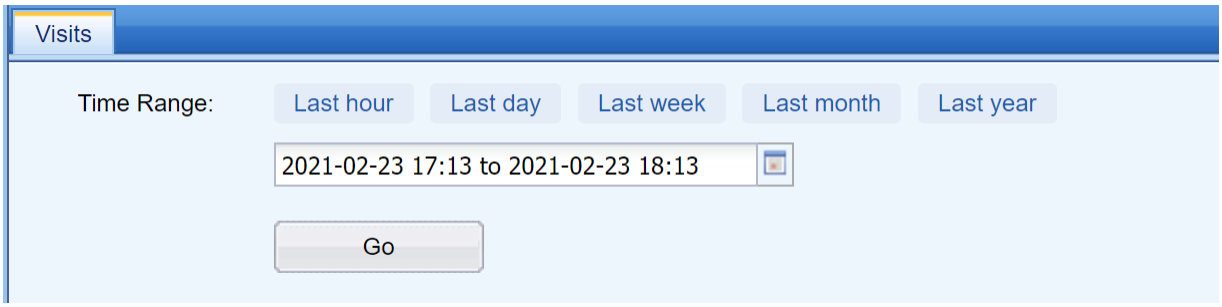
【Operation Scenarios】

WEBUI path: 『Report』→『Policy-Based Routing』→『Visits』.

『Visits』: collects statistics on the access count.

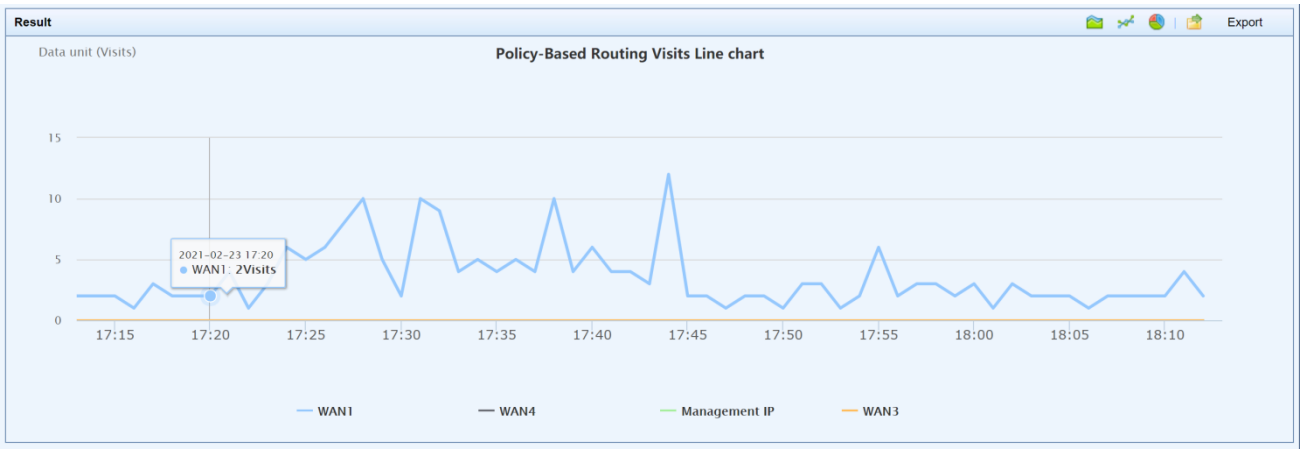
【Operation Procedure】

Choose『Report』-> 『Policy-Based Routing』-> 『Visits』, and select the time range based on your needs to collect statistics on the access count, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the line chart is selected.



Click Export to display a policy-based routing visits line chart according to the preceding configurations and then generate a report in a PDF format.

10.2.2.5 Intelligent DNS Statistics

【Operation Scenarios】

When applying to global load balancing, an ADC needs to collect statistics on situations of intelligent DNS, and query them in details. The range for statistics includes『Visits』,『LDNS source distribution』, and『Local Exceptional Request』.

10.2.2.5.1 Visits

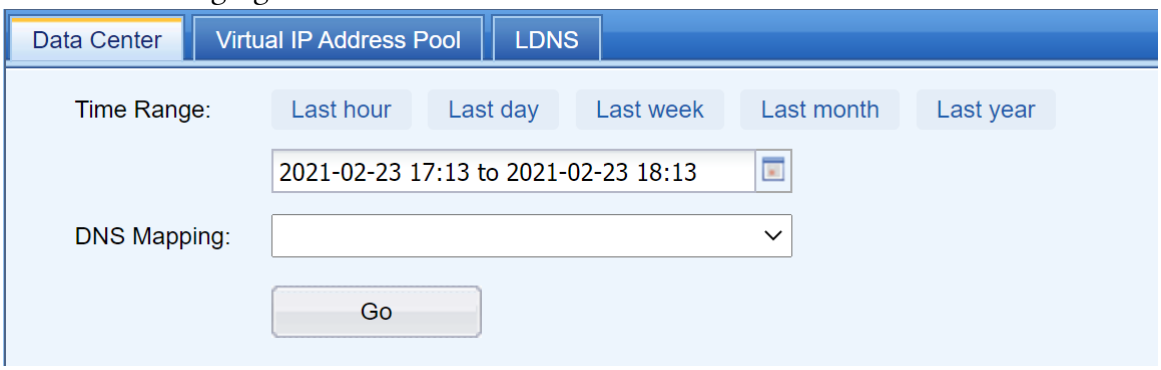
10.2.2.5.1.1 Data Center

【Operation Scenarios】

When applying to global load balancing, that is, multi-data center load balancing, an ADC needs to collect statistics on data centers' access count for DNS mapping.

【Operation Procedure】

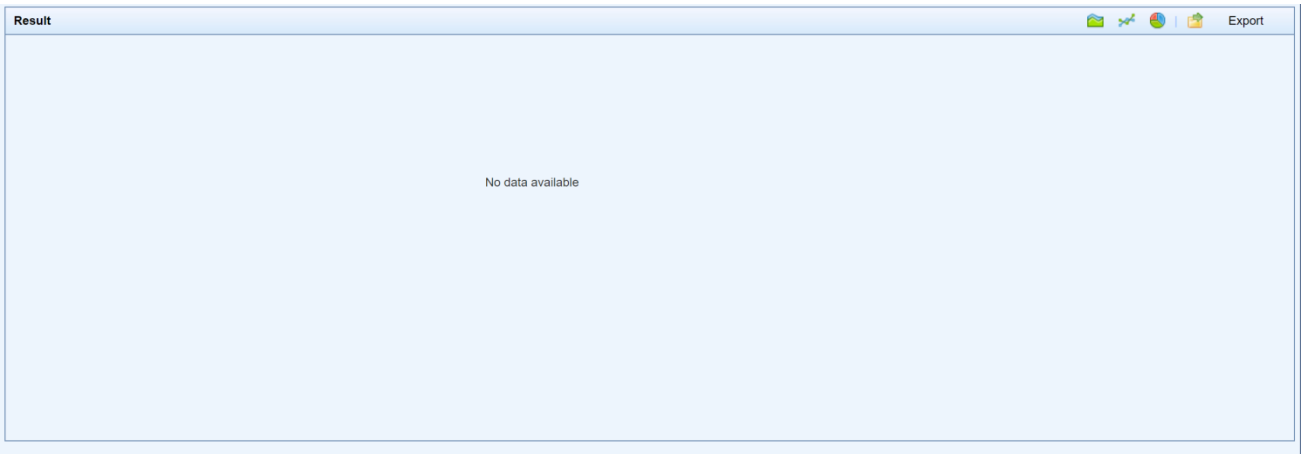
Choose『Report』-> 『Policy-Based Routing』-> 『Visits』-> 『Data Center』and select the time range and DNS mapping based on your needs to collect statistics on the access count, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『DNS Mapping』 : specifies the global DNS mapping to be counted.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the interval graph is selected.



Click Export to display a counted result according to the preceding configurations and then generate a report in a PDF format.

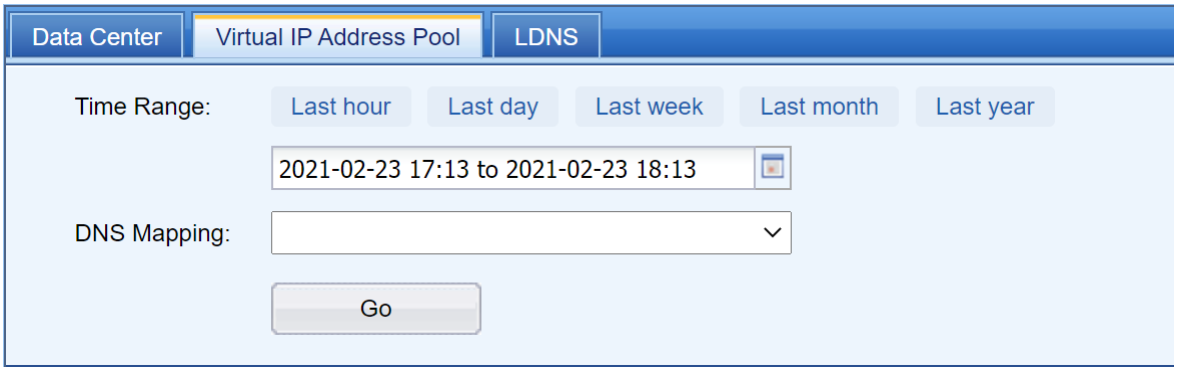
10.2.2.5.1.2 Virtual IPAddress Pool

【Operation Scenarios】

This module is used to count the number of times a DNS mapping is accessed according to a virtual IP address pool.

【Operation Procedure】

Choose 『Report』 -> 『Policy-Based Routing』 -> 『Visits』 -> 『Virtual IP Address Pool』 and select the time range and DNS mapping based on your needs to collect statistics on the access count, as shown in the following figure.



Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the interval graph is selected.



Click Export to display a counted result according to the preceding configurations and then generate a report in a PDF format.

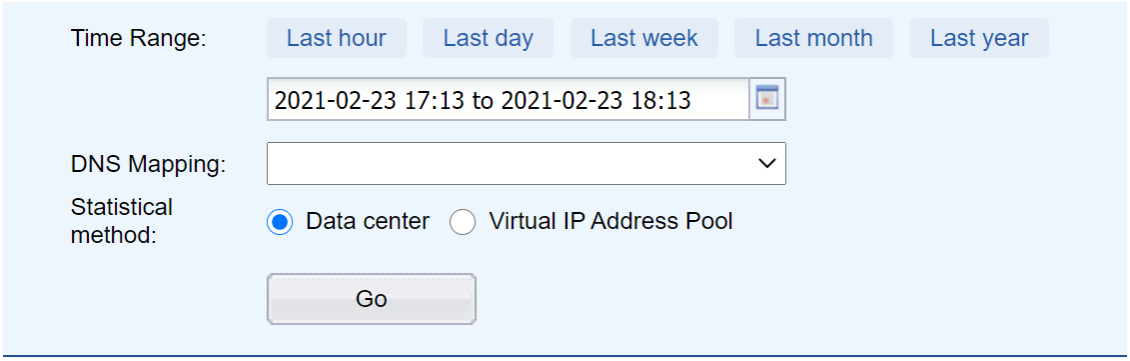
10.2.2.5.1.3 LDNS

【Operation Scenarios】

This module is used to count the number of times an LDNS set is accessed according to a data center or virtual IP address pool. The interface is shown below.

【Operation Procedure】

Choose 『Report』 -> 『Policy-Based Routing』 -> 『Visits』 -> 『LDNS』 and select the time range, DNS mapping, and statistical method based on your needs to collect statistics on the access count, as shown in the following figure.

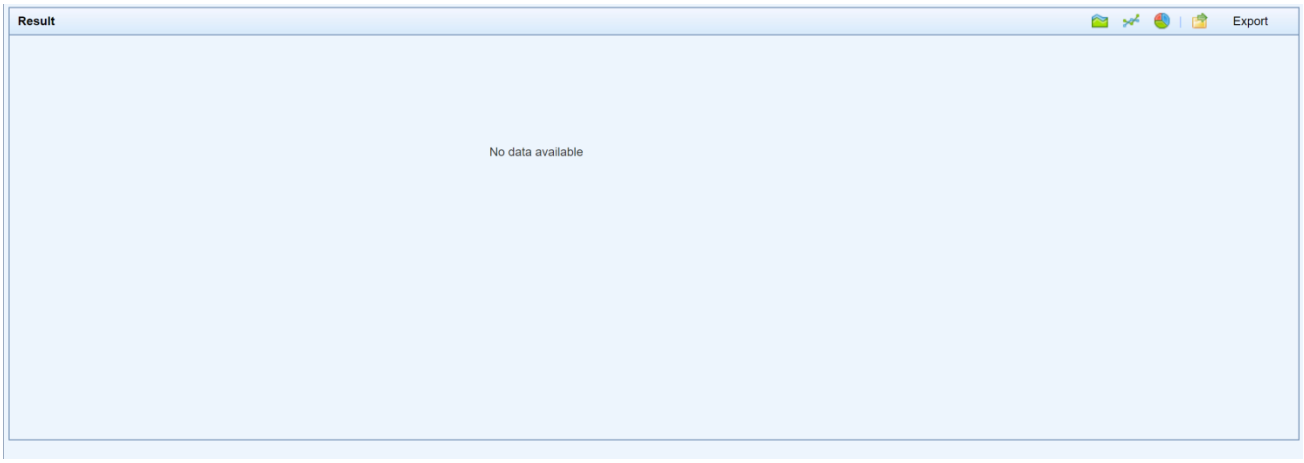


『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『DNS Mapping』: specifies the DNS mapping to be counted.

『Statistical method』: collects statistics on the access count based on a data center or virtual IP address pool.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the interval graph is selected.



Click Export to display a counted result according to the preceding configurations and then generate a report in a PDF format.

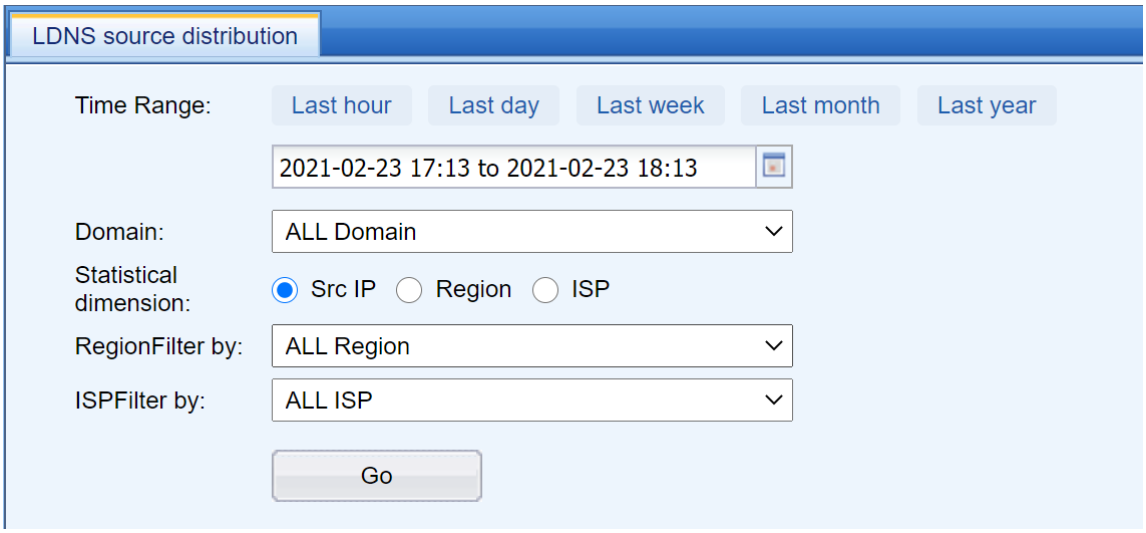
10.2.2.5.2 LDNS Source Distribution

【Operation Scenarios】

This module is used to count the number of times a DNS mapping is accessed according to the domain name, region, ISP, and IP address range type.

【Operation Procedure】

Choose『Report』-> 『Policy-Based Routing』-> 『LDNS source distribution』and select the time range, domain name, statistical dimension, region filter, and ISP filter based on your needs to collect statistics on the access count, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

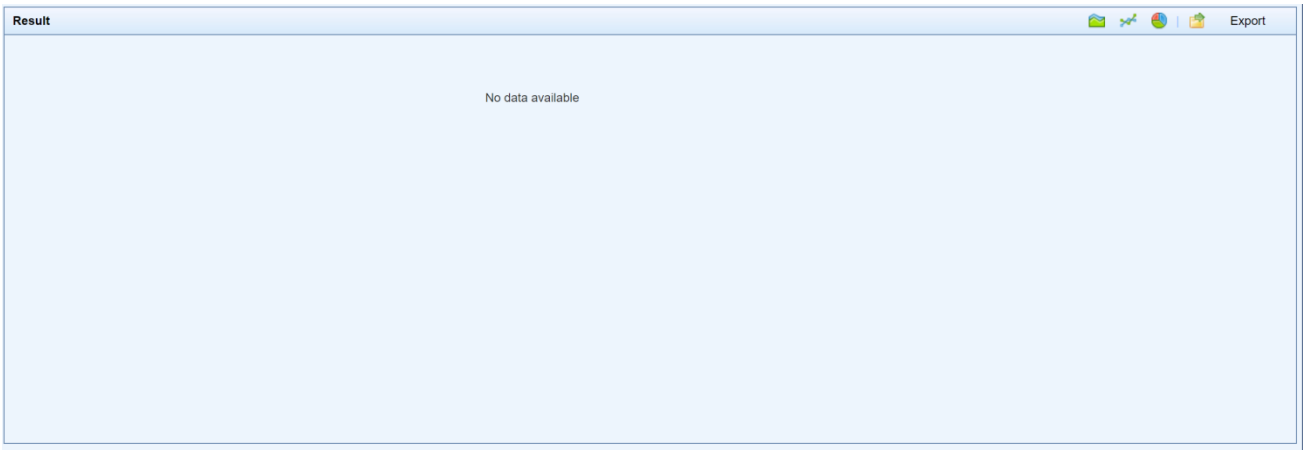
『Domain』: specifies the domain name for which statistics will be made.

『Statistical dimension』: specifies the dimension based on which statistics will be made. You can select Src IP, Region, or ISP for this parameter.

『Region Filter by』: specifies the region for which statistics will be made.

『ISP Filter by』: specifies the ISP for which statistics will be made.

Click Go to generate a query result. You can determine whether the query result is displayed in an interval graph, line chart, or pie chart. By default, the interval graph is selected.



Click Export to display a counted result according to the preceding configurations and then generate a report in a PDF format.

10.2.2.5.3 Exceptional Request

10.2.2.5.3.1 Exceptional Request Record

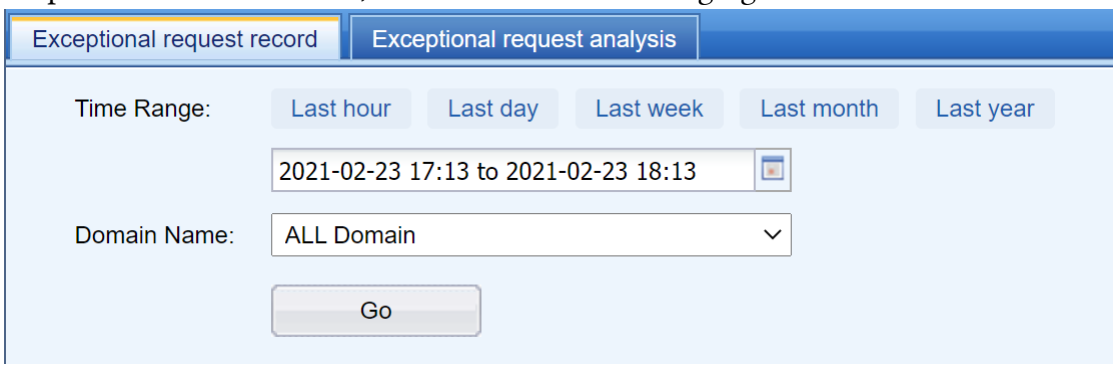
【Operation Scenarios】

This module is used to collect statistics on the counts and causes of exceptional domain name

resolution, and allows you to know problems existing in domain name resolution.

【Operation Procedure】

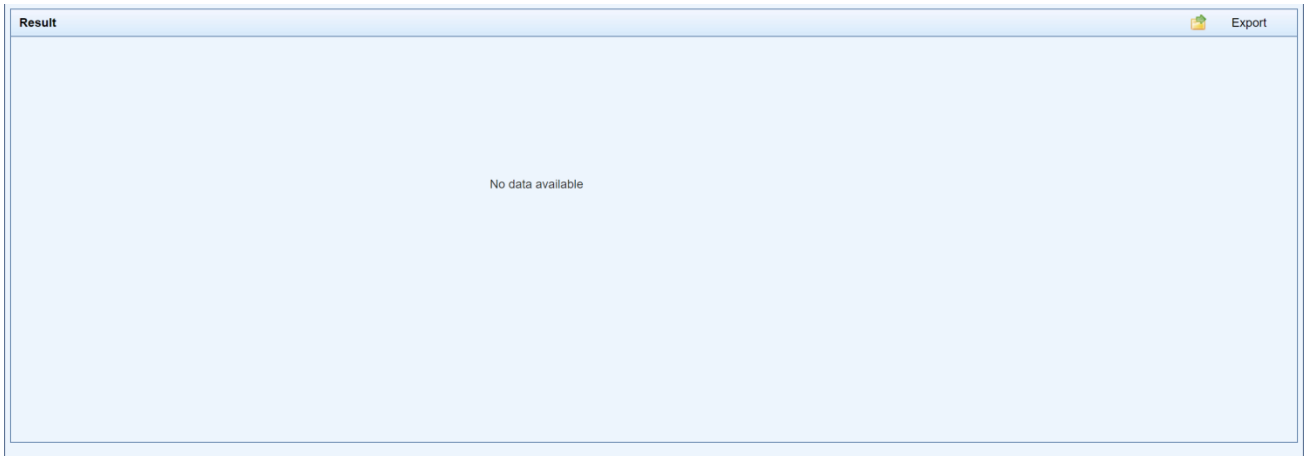
Choose『Report』-> 『Policy-Based Routing』-> 『Exceptional Request』-> 『Exceptional request record』 and select the time range and domain name based on your needs to collect statistics on the exception counts and causes, as shown in the following figure.



『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Domain』: specifies the domain name for which statistics will be made.

Click Go to generate a query result.



Click Export to display a counted result according to the preceding configurations and then generate a report in a PDF format.

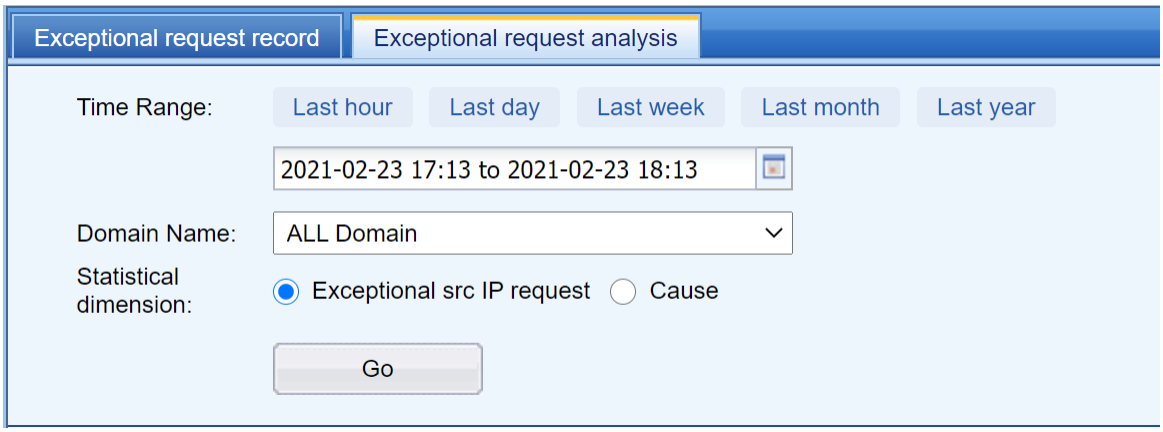
10.2.2.5.3.2 Exceptional Request Analysis

【Operation Scenarios】

This module is used to collect statistics on exceptional domain name resolution requests according to the source IP address or causes, as shown in the following figure.

【Operation Procedure】

Choose『Report』-> 『Policy-Based Routing』-> 『Exceptional Request』-> 『Exceptional request analysis』and select the time range, domain name, and statistical dimension based on your needs to collect statistics on the exceptional requests, as shown in the following figure.

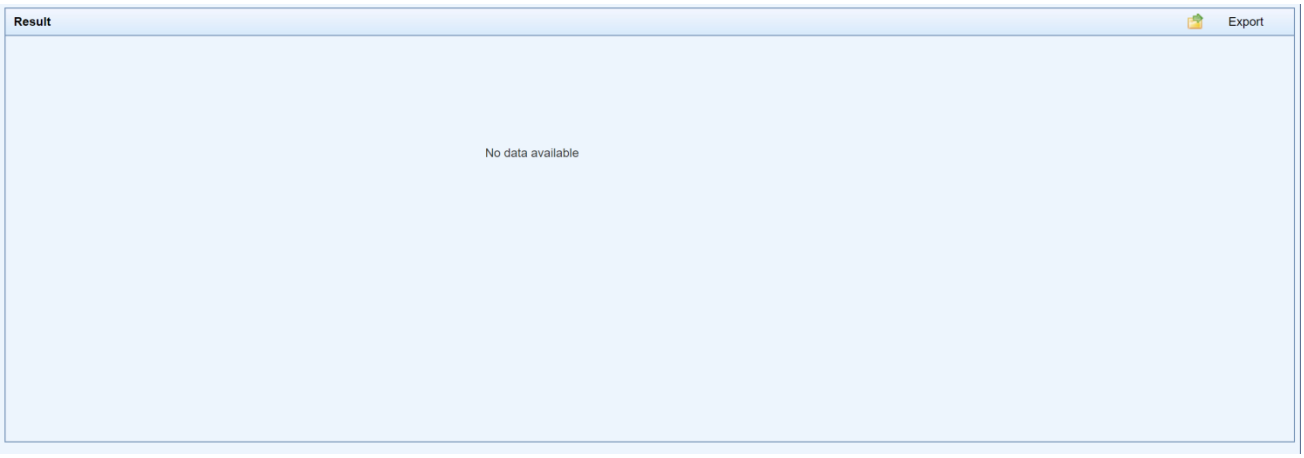


『Time Range』: specifies the time range for traffic statistics, including last hour, last day, last week, last month, and last year. Set the start and end time for traffic statistics.

『Domain』: specifies the domain name for which statistics will be made.

『Statistical dimension』: specifies whether to collect statistics on exceptional requests based on the exceptional source IP request or cause.

Click Go to generate a query result.



Click Export to display a counted result according to the preceding configurations and then generate a report in a PDF format.

Chapter 11 Routine Inspection for Device

【Operation Scenarios】

To ensure stable operation of the device, the device administrator checks the device regularly for risks in advance and copes with them as early as possible. This decreases the probability of failure.

【Operation Procedure】

Routine operation and maintenance includes: precautions for routine maintenance, hardware, software, security, and log compliance. The specific steps are described as follows:

11.1 Precautions for Routine Maintenance

Item	Description
Transferring the device	Disconnect all power cables and external cables before moving the device.
Installing the device	1. Install the device in version AD-2xxxx or later (including AD-2000) on a tray or guide rail. 2. Install the device on a clean workbench if no standard cabinet is available. Make sure that the workbench is rigid for the device and cables, with 10 cm space reserved around the device for heat dissipation. 3. Do not place heavy objects on the device. 4. When installing, take note of other devices in the same cabinet, and do not remove the power unit and network cable interfaces of other devices.
Installing mounting ears	After installing the tray or guide rail for the device, do not mount the ears when appropriate. Install the ears in other cases.
Wiring the power unit	Connect the redundant power unit (if any).
Cabling	1. When laying aisle cables, bind them. The bound cables should be close to each other, with a straight and tidy view. The cable ties are spaced evenly and tightened moderately. When laying channel cables, it is allowed not to bind them. 2. Route signal cables, pigtail fibers, and power cables separately if possible. Do not keep them too close and do not bind them together. Bind cables in the cabinet straightly and neatly, without winding and bending. 3. Check whether there are burrs, sharp edges, or sharp corners near the area close to the routing area of the fibers before binding the pigtail fibers. If so, try to avoid them. When wiring outside the cabinet, install a fiber protection sleeve (a corrugated pipe).
Label	Cables must be labeled. 1. Label for power cables: The text is the information of the opposite position of the cable. Fill in the position information of the opposite device, control cabinet, distribution box, or socket where the label is

	located. 2. Label for signal lines: The two sides of the label respectively provide the position information of the port connected to both ends of the signal line. 3. Fill in or print the label text on the full-page label paper before attaching the label, and then peel off and paste it on the cable or the identification card on the cable tie.

11.2 Checking the Hardware of the Device

11.2.1 Checking the Status Indicator Lights

When a SANGFOR ADC hardware device is working normally, the POWER indicator light stays on. The ALARM indicator light stays on for a long time (about one to five minutes) only when the system is loading after a startup, and is off during normal operation of the device. If the ALARM indicator light stays on during use and the device is not working properly, follow the steps below:

1. Turn off the device immediately, and switch the system to the standby device.

2. Restart the device after half an hour. If the ALARM indicator light still stays on after restart, contact the technical support engineer from Sangfor in time to confirm the device for damage.

11.2.2 Checking the Indicator Lights of the Interfaces

Under normal circumstances, while sensing electrical signals, the LINK indicator light of the network interface remains solid green in a 100 megabit link, but solid orange in a gigabit link. The ACT indicator light of the network interface is in orange and flashes continuously in the case of data transmitting. If the LINK or ACT indicator light does not flash or fails to be on, follow the steps below:

1. Check whether the network cable is damaged.

2. Check whether the registered jack of network interface is damaged.

3. Check whether the NIC duplex mode is negotiated and matched.

4. If none of the said problems exists, restart the device, switch to the standby device, and contact the technical support engineer from Sangfor in time.

11.2.3 Checking the Running Condition of CPU

Check whether the usage ratio of CPU is high for a long time according to the resource usage on the device console. If so, follow the steps below:

1. Choose【Overview】-> 【Activity】-> 【Network Throughput】-> 【All Ports】, and check whether the current bandwidth is in full load all the time.

2. Choose【Overview】-> 【Activity】-> 【Connections】-> 【New Connections】, and check whether the number of connections to the device is large all the time.

3. Check whether any process runs abnormally. (Contact the technical support engineer from Sangfor for confirmation.)

11.2.4 Checking the Abnormal Status

Check whether an abnormal noise arises from the device hardware such as the fan and hard disk.

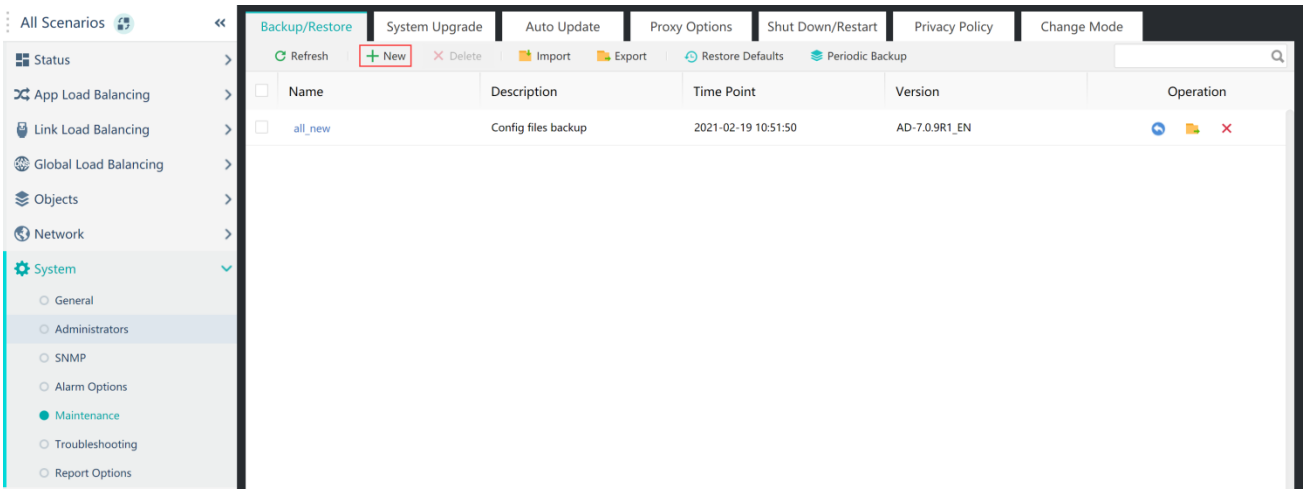
If an abnormal noise arises from the inside of the device, the hard disk or fan may work abnormally. Turn off the device immediately, and switch the system to the standby device (if any) immediately. Contact the technical support engineer from Sangfor in time to confirm the fault, and return the device for repair.

11.3 Checking the Configuration of the Device

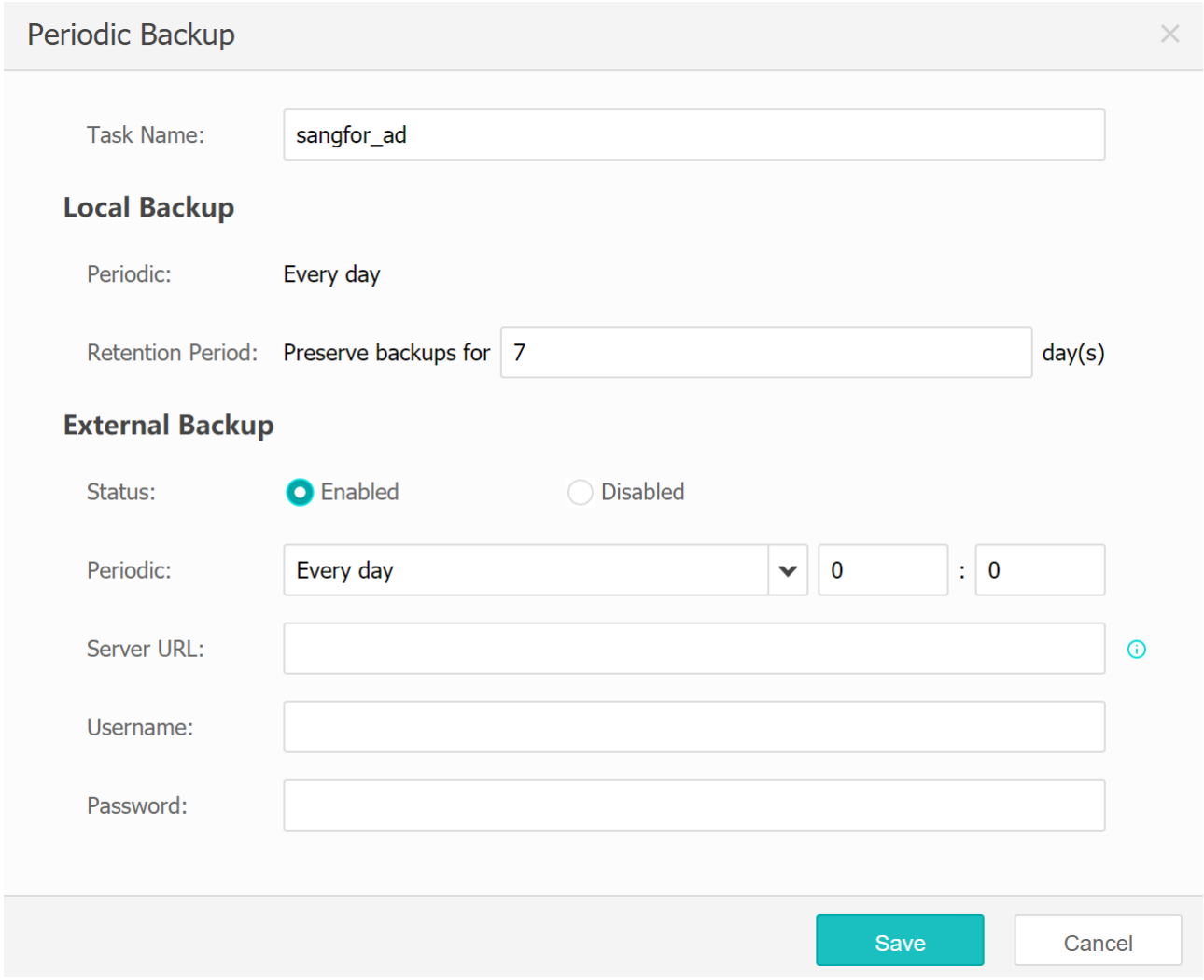
11.3.1 Device Configuration Backup

To make sure stable operation of the network, customers should back up the configuration monthly to rapidly restore the ADC system upon unexpected breakdown.

Method: Log in to the ADC console, choose【System】-> 【Maintenance】-> 【Backup/Restore】 -> 【New】, click <Export> to download the configuration and keep it properly.



Alternatively, make a backup for the configuration regularly and synchronize it to the external server.



11.4 Checking the Security of the Device

11.4.1 Checking the Security of the Console Account

1. Check whether the password of the console administrator is a simple password such as the default "admin" or "123456".

Change the default password or a simple password immediately.

2. Check if the password of the console administrator remains unchanged within one month.

If so, change and the password immediately and keep it safe.

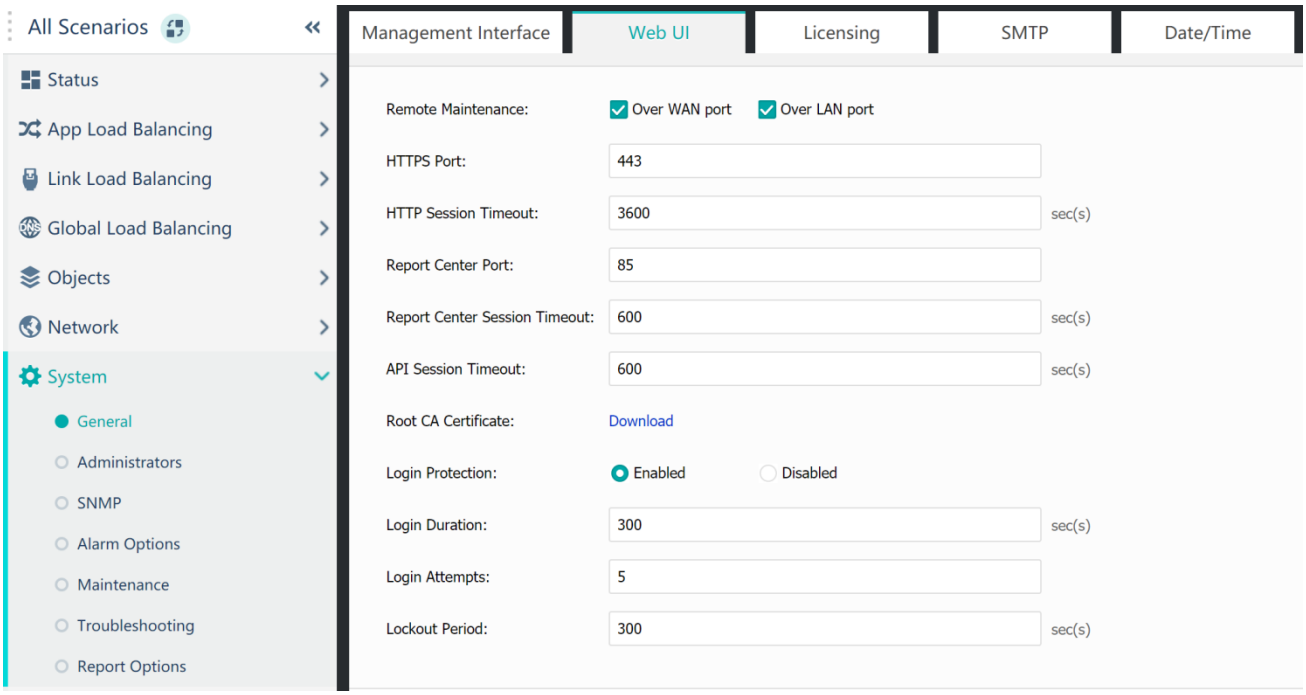
3. Check whether the console has redundant accounts, such as "sangfor", "test", company name in English and other simple undesired accounts.

If so, delete the redundant accounts, and keep the authorized admin account only.

11.4.2 Checking the Remote Maintenance Status of the Console

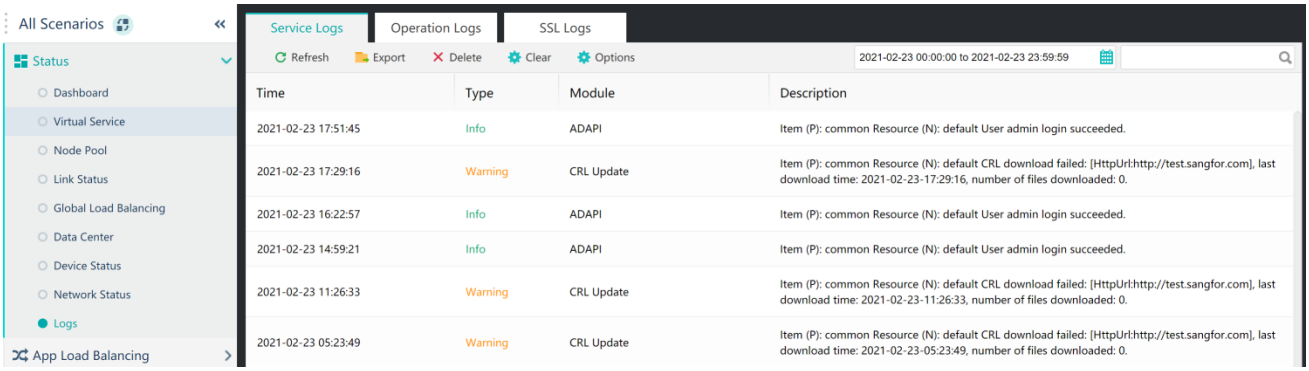
Choose【System】-> 【General】-> 【Web UI】-> 【Remote Maintenance】, and check whether the remote maintenance is enabled, so as to prevent unauthorized personnel from accessing the

device over the WAN interface.

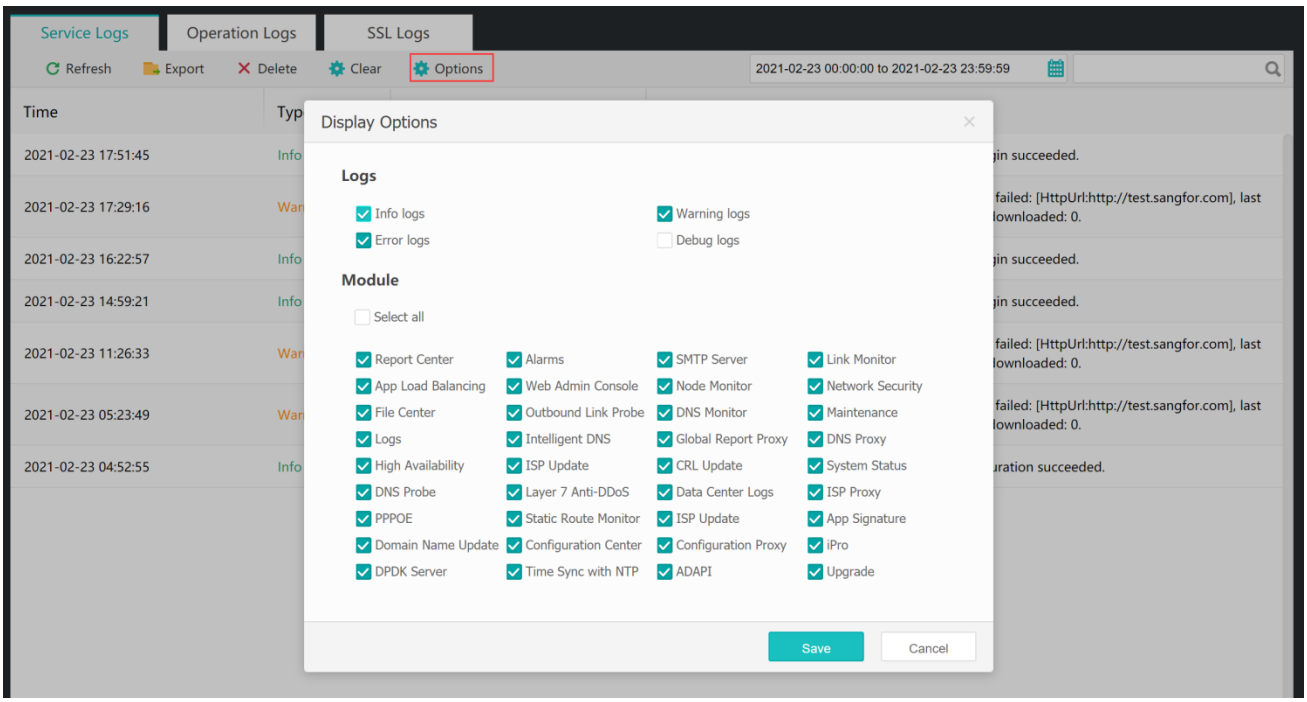


11.5 Checking the Logs of the Device

Choose [System] -> [Logs] -> [Service Logs] to view the running status logs of each module of the device. With these logs, you can determine whether the modules of the device are running normally.



The system logs include four types: Info, Warning, Error, and Debug. Click <Options> to filter the type and the module to be displayed:



If a large number of logs in types Error and Warning exist in the system logs, contact the technical support engineer from Sangfor in time to check the programs of the device for failures.

11.6 Description of Log Compliance for the Device

The new Cyber Security Law of the People's Republic of China (hereinafter referred to as Cyber Security Law) took effect on June 1, 2017,

which specifies the retention time of over 6 months for logs.

As a load balancing device, an ADC does not save users' access logs, but needs to retain its own logs for more than 6 months. However, it can retain the logs for just 6 months (as instructed in the latest version). To prolong the time, you can synchronize logs to the Syslog server and use a disk to expand the storage capacity based on the actual amount of logs.

11.7 Restoring the Password with a USB Flash Drive

【Operation Scenarios】

The password of the admin account is lost, and no other account is available, making the user unable to log in to the console and the background.

【Operation Procedure】

1) Copy a file named reset-password.txt to the root directory of the USB flash drive, without any content in this file. Alternatively, directly create a TXT file named reset-password in the root directory.

2) Insert the USB flash drive, and restart the device.

3) Plug off the USB flash drive when the LED indicator (red) of the device is off.

4) Check the result file named reset-password.log in the USB flash drive. If the restoration is successful, the restored password of the console should be recorded in the file. Otherwise, the restoration failure is recorded.

**Attention:** All services will be interrupted when the device is restarted. Proceed with caution.

Chapter 12 High Risk Operation

【Operation Scenarios】

In order to ensure the stable operation of the device and the safety and integrity of the user data, the O&M personnel are required to perform corresponding operations referring to these Specifications, to reduce the accident rate.

These Specifications are divided into several categories by web front-end high risk operations and hardware high risk operations, and each category is further divided by the operation objects. Before operating corresponding objects, the O&M personnel should have a full understanding of related operations for possible risks.

12.1 Front-end High Risk Operations

High risk operation

Before performing the following operations, learn about possible risks during the operations:

1) Shut down or restart the ADC on the console

Risks: 1. While the device is restarted, all services will be restarted, with customers' services interrupted.

2. After being shut down, the device will not power on any longer, with customers' services interrupted.

3. After the device is restarted, customers' services are interrupted.

2) Delete default IP addresses and modify default ports

Risk: If you forget the login address for the device, you can log in to the device only using the updated client or display.

3) Manually set an interface negotiation mode

Risk: In general, an automatic negotiation mode is recommended because a manually assigned static IP address may lead to negotiation failure and Internet disconnection, especially interruption to customers' services during the operation.

4) Add eight default routes with the subnet mask of 0 (static routes) to multiple lines in a gateway

Risk: The policy-based routing will fail while the default routes are added.

5) Configure the SSL offloading virtual service and use the default HTTPS port 443

Risk: The virtual service whose priority is higher than the console service allows port 443 to log in to the management console over this IP address. If any other IP address exists, the security is not affected.

6) Manually switch between active and standby devices

Risk: 1. Before you manually switch between the active and standby devices, make sure that both session synchronization and service MAC address synchronization are enabled, in order to reduce the delay and jitter during the service switch.

1.Check whether the active and standby devices are in a normal state, and whether service cables of the standby device are connected properly.

2.Switch the active and standby devices when no important service is running.

7) Switch the device having taken effect in an application group

Risk: If a virtual MAC address is not filled, a new device will learn the Address Resolution Protocol (ARP) again each time you switch the device that has taken effect. This will affect the services of the related application group in a short time.

8) Change the number of authorized lines

Risk: If you want to change the number of authorized lines for both active and standby devices, dismantle them for change. Otherwise, both devices may not be installed properly, resulting in service interruption.

9) Restore factory settings

Risk: All configurations in the device will be cleared, resulting in service interruption. Proceed with caution.

【Prohibited Operation】

(1) When adding ACL configuration, you are not allowed to add an ACL rule for which all source IP addresses, destination IP addresses, and ingoing interfaces are selected.

Risk: You are not allowed to log in to the device in all ways, except using the display.

(2) Update the device using the updater over the external network

Risk: The unstable transmission rate over the external network may result in damages to the update package or sudden suspension of update. If the failure caused by the update is serious, the device may not be restarted.

12.2 Hardware High Risk Operation

Do not disassemble the device.

1) Plug and unplug the single power supply (pluggable modular power supply)

Risk: The device may be powered off, resulting in service interruption.

2) Plug and unplug the redundant power supply (pluggable modular power supply)

Risk: The device may be powered off, resulting in service interruption.

3) Power off the device

Risk: The device hardware may be subject to imponderable damages, thus affecting the normal running of the device.

Chapter 13 Troubleshooting Guidance

13.1 Quick Start Guide

13.1.1 Troubleshooting Flow

From the perspective of functional modules and their deployment, common problems of an ADC are divided into problems occurring in different scenarios including virtual services, inbound link load balancing, outbound link load balancing, and active/standby cluster deployment, etc. For each scenario, there are some differences in handling methods, whereas the general handling idea keeps the same. This way, the troubleshooting flow has a common handling idea of collecting fault information (confirming the fault phenomenon and confirming the deployment of device), determining a failure type, locating fault causes, and troubleshooting.

1) Collect fault information:

As the first step in the workflow, whether the fault information collected in this step is comprehensive, objective, and accurate directly determines the difficulty of locating fault causes and the timeliness of subsequent troubleshooting. Therefore, comprehensive, objective and accurate fault information should be effectively collected in this step, and subjective or inaccurate information should be avoided.

2) Determine the fault type:

The IT O&M personnel should determine the fault type of collected fault information, and then handle them according to respective types. The faults mainly include two types: common faults and major faults.



Tips: Major faults refer to the faults that occur suddenly, have a wide range of influence, and result in serious consequences to services, such as faults causing interruption of a large range of services. For example, all virtual services are abnormal, all LAN users cannot access the Internet, the resolution of all DNS servers is abnormal.



Attention: Before you handle major faults, contact the technical support engineer from Sangfor to perform troubleshooting, service recovery, or recover the normal running of the device within the shortest time, striving to recover or reduce loss.

3) Locate fault causes:

This step is to gradually narrow the range of fault causes by means of effective troubleshooting methods and means, to finally determine real fault causes.

4) Troubleshoot:

This step is to locate faults according to the fault causes and take effective measures to clear them. The effective measures include network overhauling, modification of configuration items, restarting relevant processes or the server, and other measures.

5) Confirm whether the faults are cleared:

This step is to confirm whether the services are running normally by detecting the device status and service status.

6) Record troubleshooting key points:

After the faults are cleared, troubleshooting analysis key points and solutions should be recorded in details, to avoid similar faults.

13.1.2 Fault Location Method

13.1.2.1 Basic Skills

To effectively locate faults, you must master the following basic skills necessary to fault location for load balancing devices:

1) When handling problems of ADCs, master the following basic knowledge and information acquisition skills.

2) Be familiar with ADC's installation, deployment, and configuration.

3) Be familiar with the usage of basic Linux commands.

4) Be familiar with the usage of tcpdump and HTTPWATCH packet capture commands in Linux, capable of briefly analyzing the header, URI and contents of a packet, and familiar with the basic programming feature of a regular expression.

5) Be capable of searching for similar faults in the Sangfor community.

13.2 Use of Auxiliary Tools

13.2.1 Web Command Console

The SANGFOR AD Command Console provides a simple command line interface (CLI) of the console for checking simple information about the device. The commands include:

Command Name	Description	Application Mode
df	Viewing the disk usage	df
ethtool	Viewing the network settings of device	1.ethtool DEVNAME 2.ethtool -i DEVNAME 3.ethtool -S DEVNAME
ping	Viewing the connection between the device and other hosts	Being the same as ping commands in Linux. Take note of not using the -c parameter to ping four packets by default. If this parameter is used, place it after the ping command.
sock	Testing the connection to detect whether the specified port of a device is listening	sock host port, such as sock 192.168.1.1 4009
adtcpdump	Capturing packets	Being the same as the tcpdump command in Linux. The -c parameter should be used, such as

		tcpdump -i eth0 -c 10.
ip route	Viewing the route table of device	1.ip route list 2.ip route list table tableName
free	Viewing the memory usage	free
help	List of help commands	help or ?



Choose【System】-> 【General】-> 【Web Console】, directly enter a command on the command line page, and press Enter. The usage of ping, sock, traceroute, and tcpdump commands is the same as that in the PC.

13.3 Fault Information Collection

13.3.1 Collecting Basic Fault Information

When a fault occurs, the range, type, and current situation of it can be roughly known after the basic fault information is effectively collected. Furthermore, possible factors for the fault can be sorted out.

Fault information to be collected on site	Collection result
Scope	
Occuring time	
Phenomenon description	
Change operations performed when the fault occurs	
Whether the fault occurs frequently	
Whether an obvious alarm	

message exists	
Whether the current fault is cleared	



Notes:

1) **Scope:** facilitates follow-up handling and communication
2) **Phenomenon description:** If the phenomenon is too complicated to describe, you can take photos or record videos to provide an auxiliary description.
3) **Change operations performed when the fault occurs:** If the services need to be recovered urgently, you can roll back special operations firstly and attempt to recover them.
4) **Whether an obvious alarm message exists:** If so, it is recommended to clearly describe fault information or take photos for retention.
5) **Whether the current fault is cleared:** If so, collect the troubleshooting method to facilitate subsequent problem handling and recurring.

13.3.2 Collecting Detailed Information On Site

If the IT O&M personnel are familiar with the network and ADC, the following information can be collected when a fault occurs:

1) Failing to access the Internet in the outbound link load balancing scenario and lagging in Internet access

▶Whether a website or all websites cannot be accessed.

▶Whether can a PC having the fault be pinged to a core or an LAN port of the ADC? Or which hop is the tracert command run to?

▶Whether the website domain name pinged to the PC having the fault can be resolved.

▶Whether the ADC can be pinged to Baidu on the Web Console page (【System】-> 【General】 -> 【Web Console】) of the ADC console.

▶On the Status page, check whether CPU, memory, traffic, and connections suddenly increase on the【Device Status】page.

▶Choose【Status】-> 【Logs】to view whether there is exception information in service logs.

▶Capture abnormal packets from the ADC or abnormal PC.

2) Failing to access applications in the server load balancing scenario and interruption of services

1. Choose【Status】-> 【Node Pool】to view whether nodes are in online status.

2. Ping a domain name on a test PC, to detect whether the domain name can be normally resolved and whether it corresponds to the IP address.

3. Whether the test PC can be accessed normally using the IP address.

4. Whether a virtual IP address can be pinged or whether the telnet command can be normally run on the ADC port.

5. Whether the server can be normally accessed by running the sock command on the Web Console page (【System】-> 【General】-> 【Web Console】) of the ADC console.

6. Whether the IP address of the server can be directly accessed without logging on to the ADC.

7. Choose【Status】-> 【Logs】to view whether there is exception information in service logs.

▶Capture abnormal packets from the ADC or abnormal PC.

3) Intelligent DNS scenario

1.Confirm whether the customer's domain name provider has authorized the resolution to the monitoring IP address of ADC.

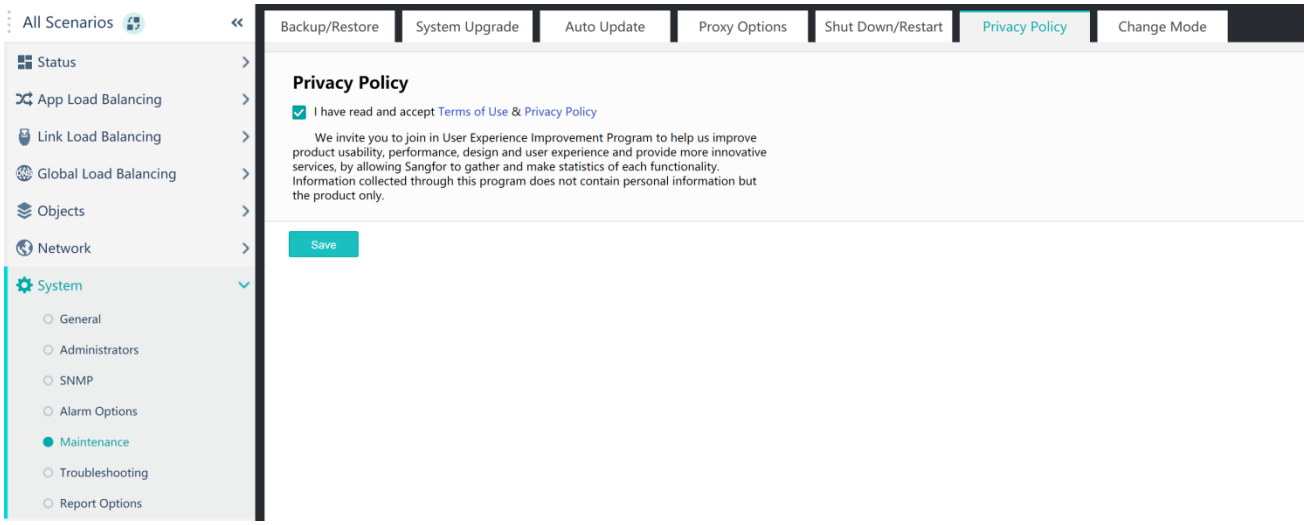
2.Run the NSLOOKUP command to view whether the NS records of DNS server are accurately resolved.

3.Configure the PC as a DNS server, and the server IP address as the monitoring IP address of ADC to view whether the DNS resolution is performed normally.

4.Capture abnormal packets from the ADC or abnormal PC.

13.3.3 Data Reporting Instruction

After the user reads and accepts the privacy policy, the ADC will report device information, helping improve product usability.



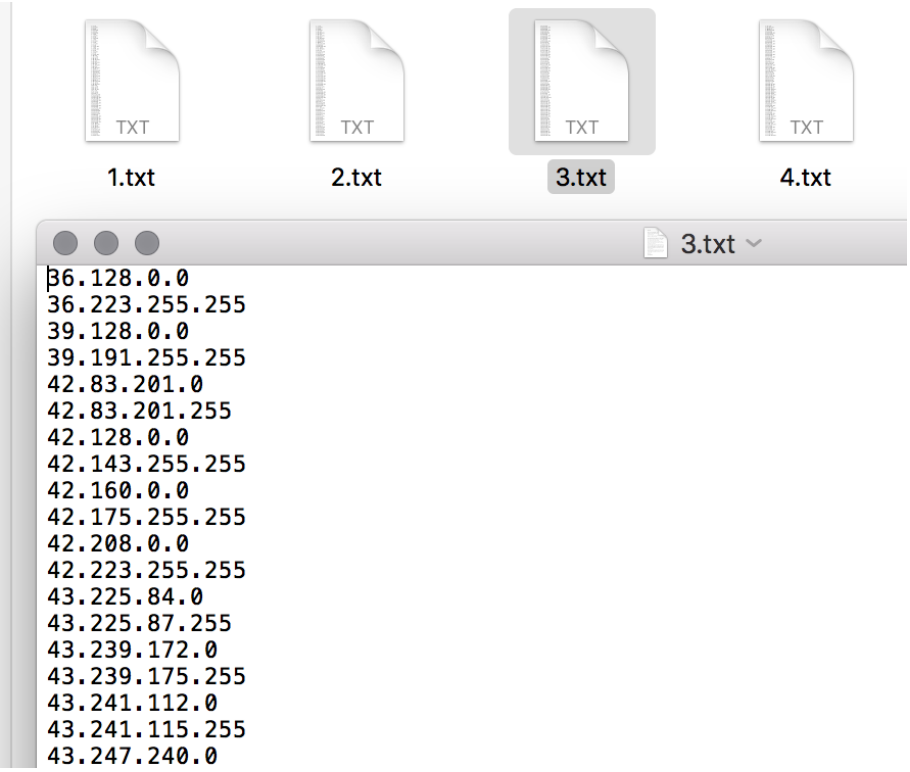
The types of reported data include:

- A list of addresses not identified in the ISP address database
- Device exception information collected by Bugreport
- Log information about application routing

ISP address reporting

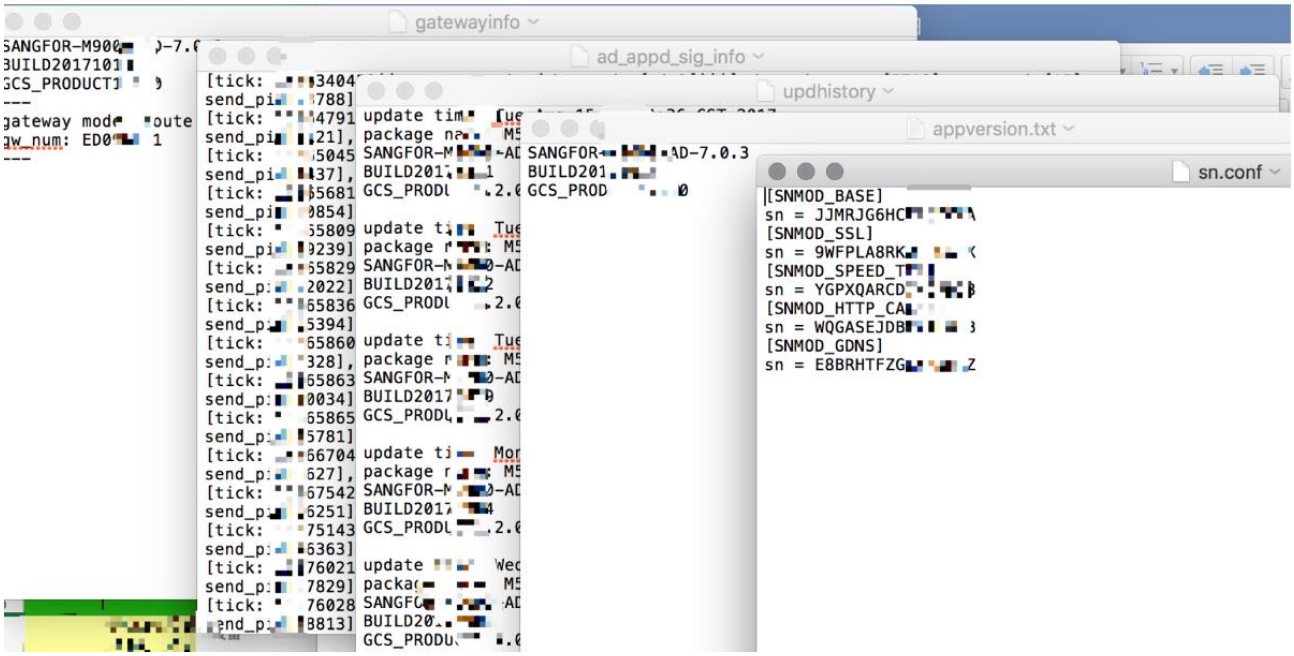
ISP addresses are reported in a binary file format.

A binary file includes a list of addresses not identified. These addresses are reported to Sangfor's internal server for internal identification. The ISP address database is updated regularly and distributed to each public network device. This makes the ISP address database more complete and further improves the user experience.



Bugreport reporting

Reporting device information and process exception information helps an ADC improve its product stability and reliability. Reported information includes: 1. Gateway serial number; 2. Process exception information; 3. Update history; 4. Software version; and 5. Serial number.



Reporting application routing information

A routing policy can be formulated for user's different application types in ADC's link load balancing scenario, ensuring user's bandwidth quality and service stability. The ADC will report the application routing information to a server, including unidentified application information and hit policy information. After that, the intelligent Neural-X identifies the information and uniformly updates it to the rule database for app signature. This increases the routing accuracy.

Field	Type	Null	Key	Default	Extra
ip	int(10) unsigned	NO	PRI	NULL	
port	smallint(5) unsigned	NO	PRI	NULL	
proto	tinyint(3) unsigned	NO	PRI	NULL	
type	int(10) unsigned	NO		NULL	
appcrc	int(10) unsigned	NO		NULL	
ver	int(10) unsigned	NO		NULL	
cnt	bigint(20)	NO		NULL	
gwlt	varchar(256)	NO		NULL	
time	datetime	NO		NULL	

Reported information includes: IP address, port, protocol type, and version of an application, hit counts, device gateway ID, and reporting time.

13.4 Troubleshooting

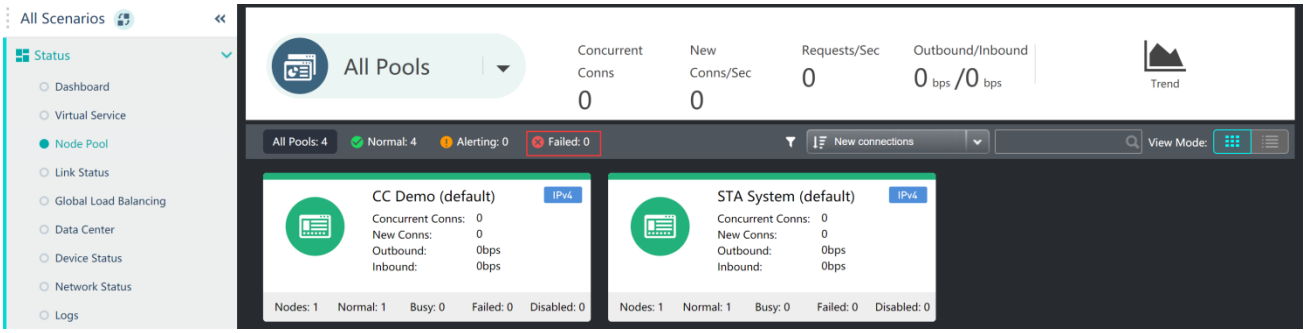
13.4.1 Failing to Log In to the ADC Console

1. Check whether the ALARM light on the panel of the device remains solid red.
2. Check whether the ping command can ping to the LAN interface of the device successfully.
3. Check whether you can telnet to the ports 443 and 51111 of the device from the LAN.
4. Run the tracert command to trace the IP address of the LAN port of the device, and check whether packets can reach the LAN interface of the ADC.
5. After connecting a computer to the MANAGEMENT interface via crossover cables and assigning the IP address 10.252.252.10/24 to the computer, test whether the default IP address 10.252.252.252 for accessing the DMZ interface can be accessed.
6. If you still cannot log in to the device, contact the technical support engineer from Sangfor in time.

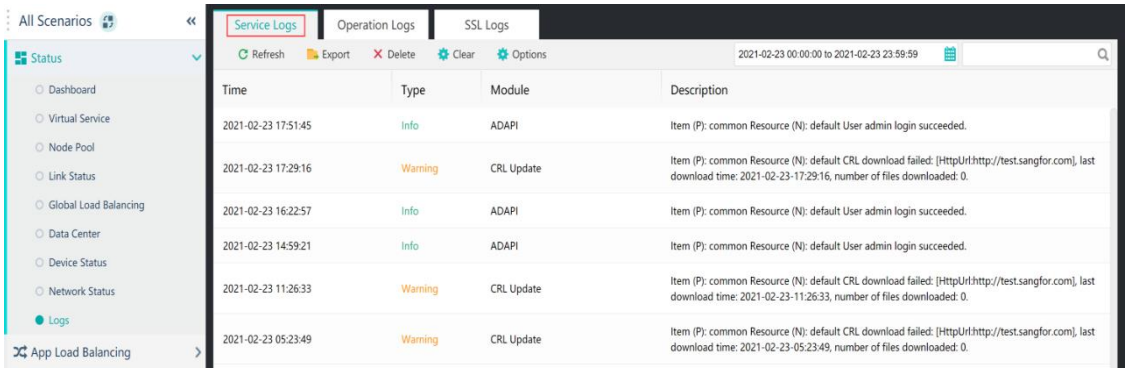
13.4.2 Failing to Access Virtual Services

1. View whether nodes are in offline status.

View whether nodes are offline. When the system reminds Network Unavailable, it indicates that a network problem occurs. Whether the problem is service unavailable or port unavailable can be determined according to the specific configuration of monitor.



2. View whether service logs contain logs indicating the node offline status.

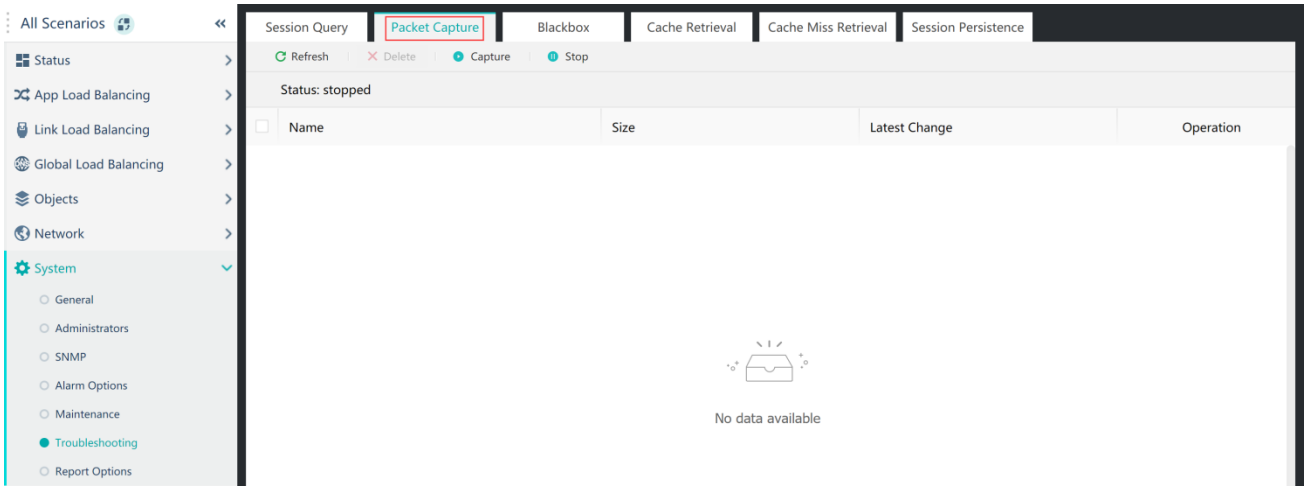


3. On the Web Console module, run the ping command to test whether the network connectivity is normal or run the sock command at the same time to test whether the port

connected to the server is normal.



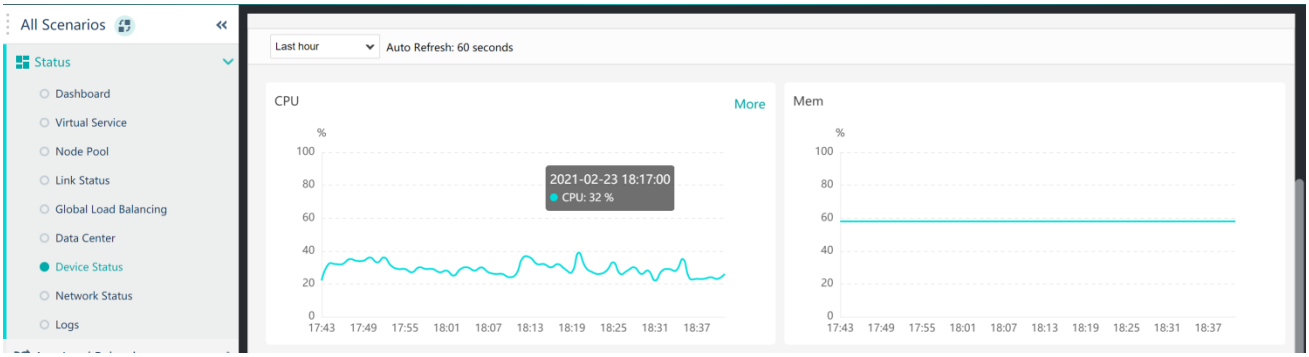
4. Choose【System】-> 【Troubleshooting】-> 【Packet Capture】, and set packet capture conditions on the Packet Capture tab; then perform packet capture analysis and view whether the request sent from a client is received and forwarded by an interface of ADC, as shown in the following figure.



5. If you still cannot access the virtual services, contact the technical support engineer from Sangfor in time.

13.4.3 Slow Access to Virtual Services via ADC

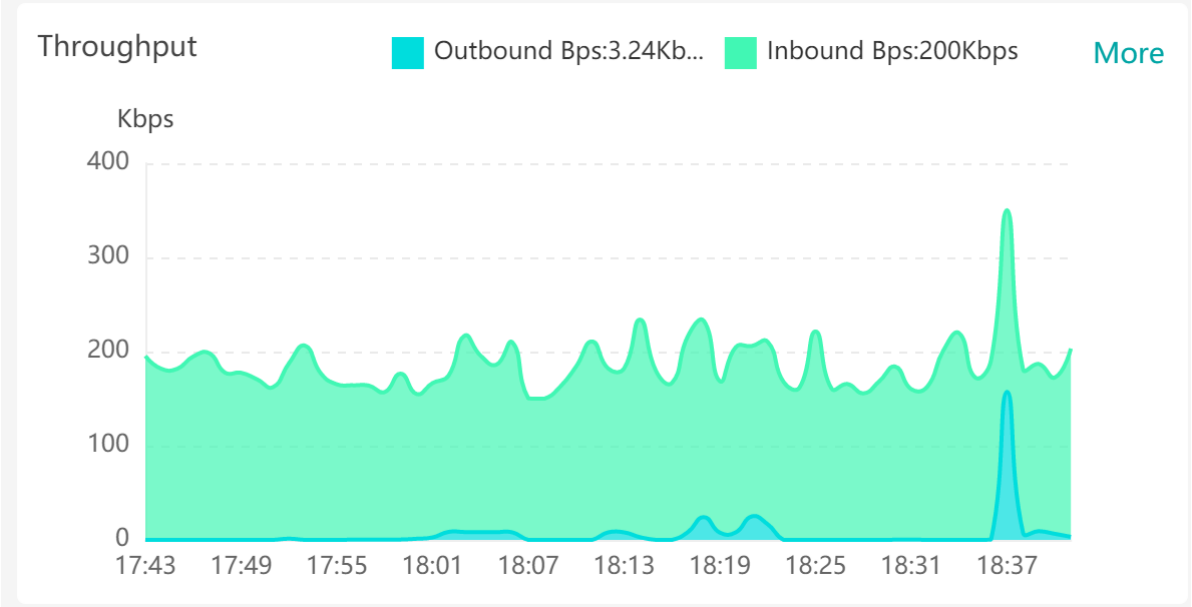
1. Choose【Status】-> 【Device Status】-> 【CPU】to view the current CPU usage of device.



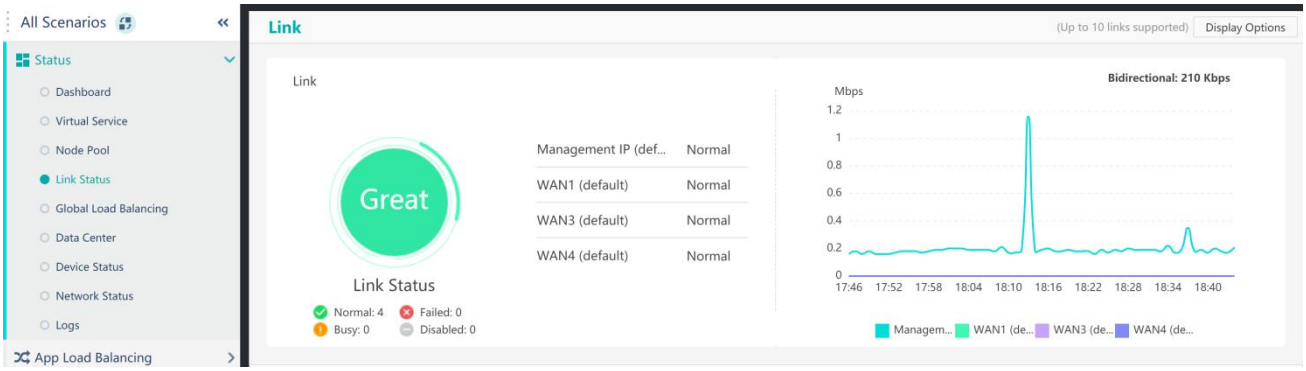
2. Choose【Status】-> 【Device Status】to view whether the number of connections currently in use is much greater than that in the preceding period of time.



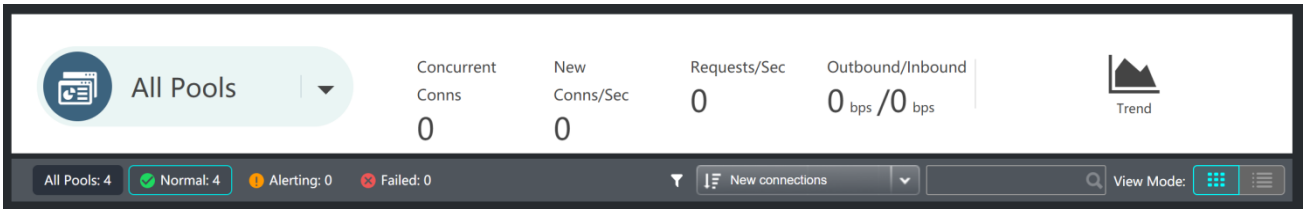
Choose【Status】-> 【Device Status】-> 【Network Throughput】to view the current network status of device and whether the traffic is almost in a full load. By viewing the traffic of a networking interface, you can evaluate the traffic used in the device.



3. Choose【Status】-> 【Link Status】 to view whether the device's link is in a busy status at present.



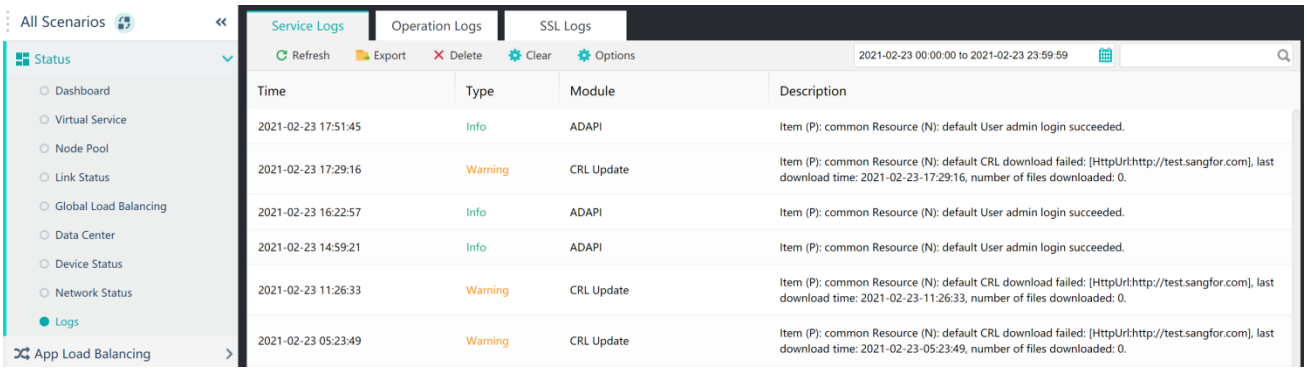
4. Choose【Status】-> 【Node Pool】to view whether the number of new connections and the number of concurrent connections are much greater than those in the preceding period of time.



5. If you still cannot find out exceptions, contact the technical support engineer from Sangfor in time.

13.4.4 Console Reminding Offline Status of Nodes

1. Choose【Status】-> 【Logs】-> 【Service Logs】to view the time when node offline logs are generated.

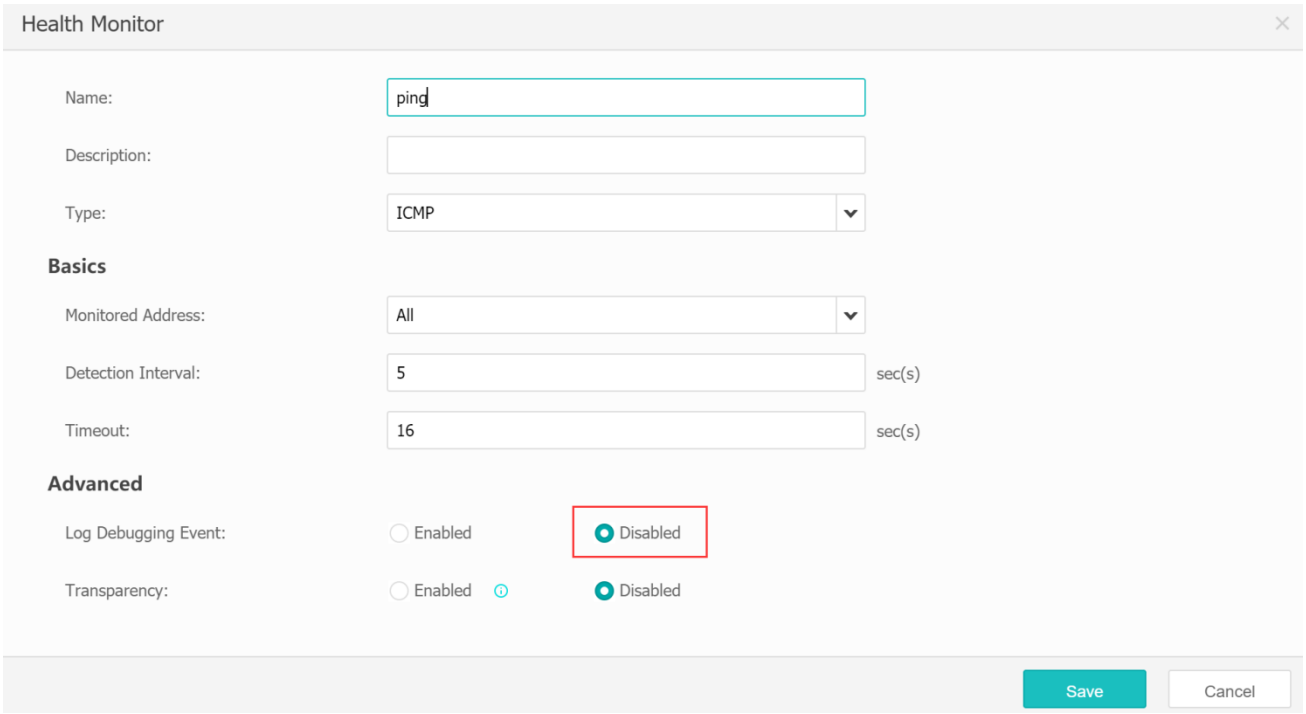


2. Choose【System】-> 【Device Management】-> 【Web Console】, and run the ping and sock commands to test whether the network connectivity and port connectivity to offline nodes are good.



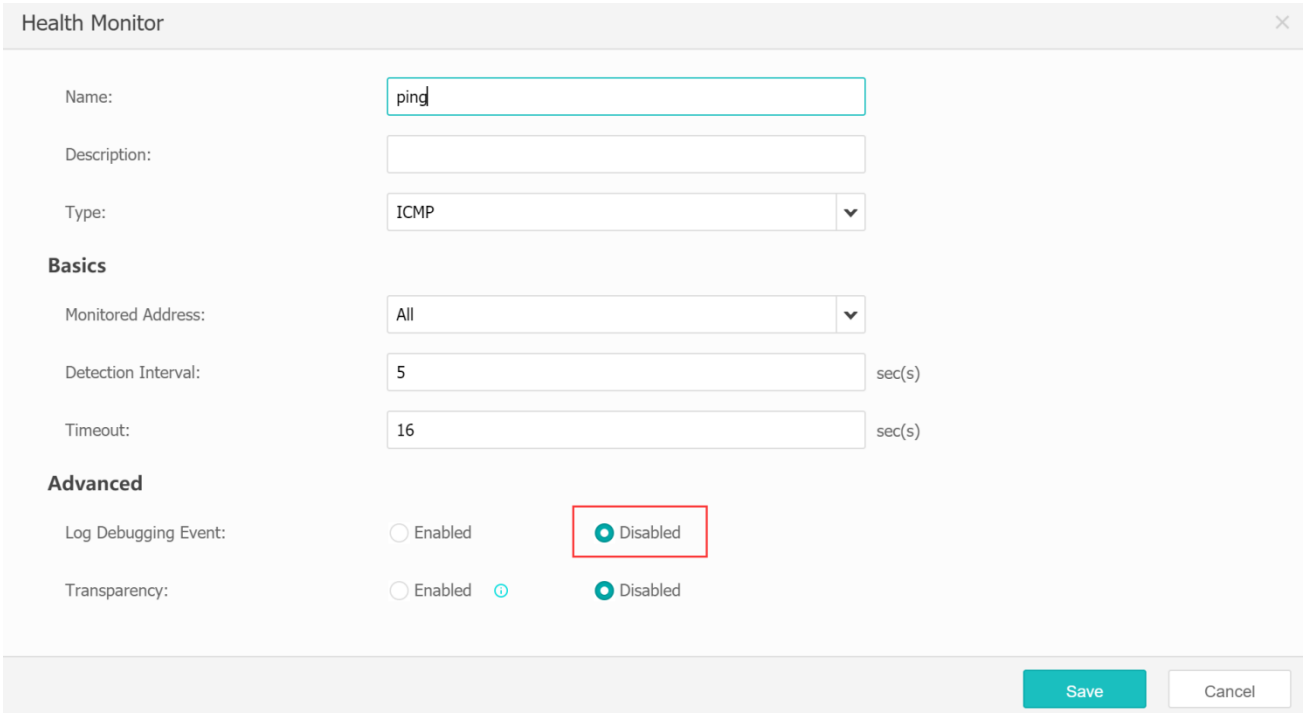
3. Choose【App Load Balancing】-> 【Node Pool】-> 【Node Pool】, and find a node monitor associated with the corresponding node pool.

4. Choose【App Load Balancing】-> 【Node Pool】-> 【Health Monitor】, and enable Log Debugging Event.



5. Choose【Status】-> 【Logs】-> 【Service Logs】to view debugging logs printed for corresponding offline nodes.

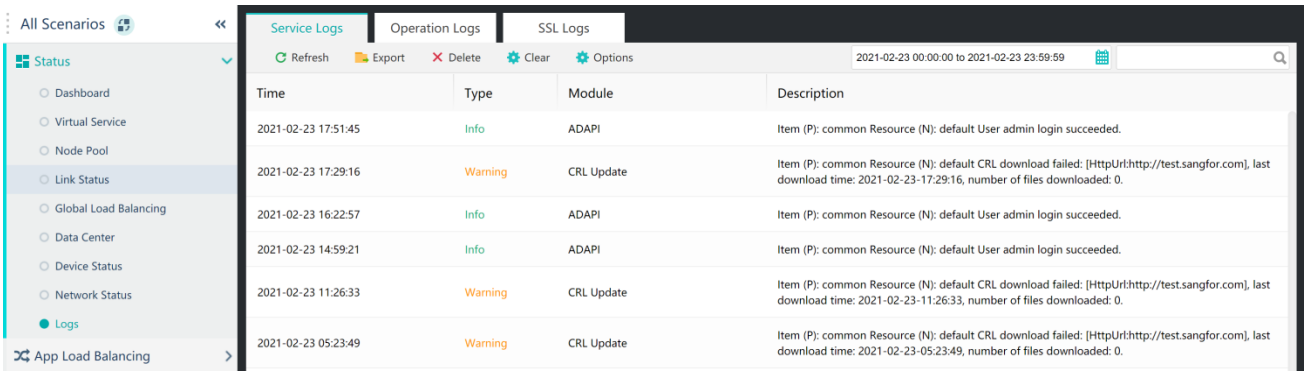
6. If Log Debugging Event for the health monitor in Step 4 is disabled, a debugging log will contain a lot of log information (it is recommended to be disabled).



7. If you still cannot determine the causes, contact the technical support engineer from Sangfor in time.

13.4.5 Failing to Connect to ADC's Internet Port

1.Choose【Status】-> 【Logs】-> 【Service Logs】to view the time when node offline logs are generated, and printed prompt messages.

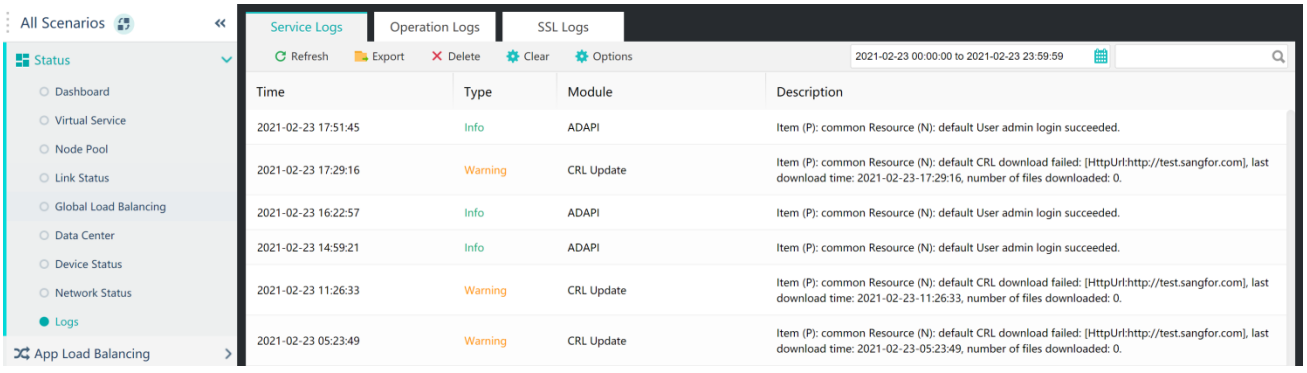


2.Choose【System】-> 【Device Management】-> 【Web Console】, and run the arp command to check whether the corresponding interface learns the MAC address of gateway; run the ping command to test whether the connectivity to gateway is good; and run the ping www.baidu.com –I command to test whether the IP address of this interface can be connected to the Internet.

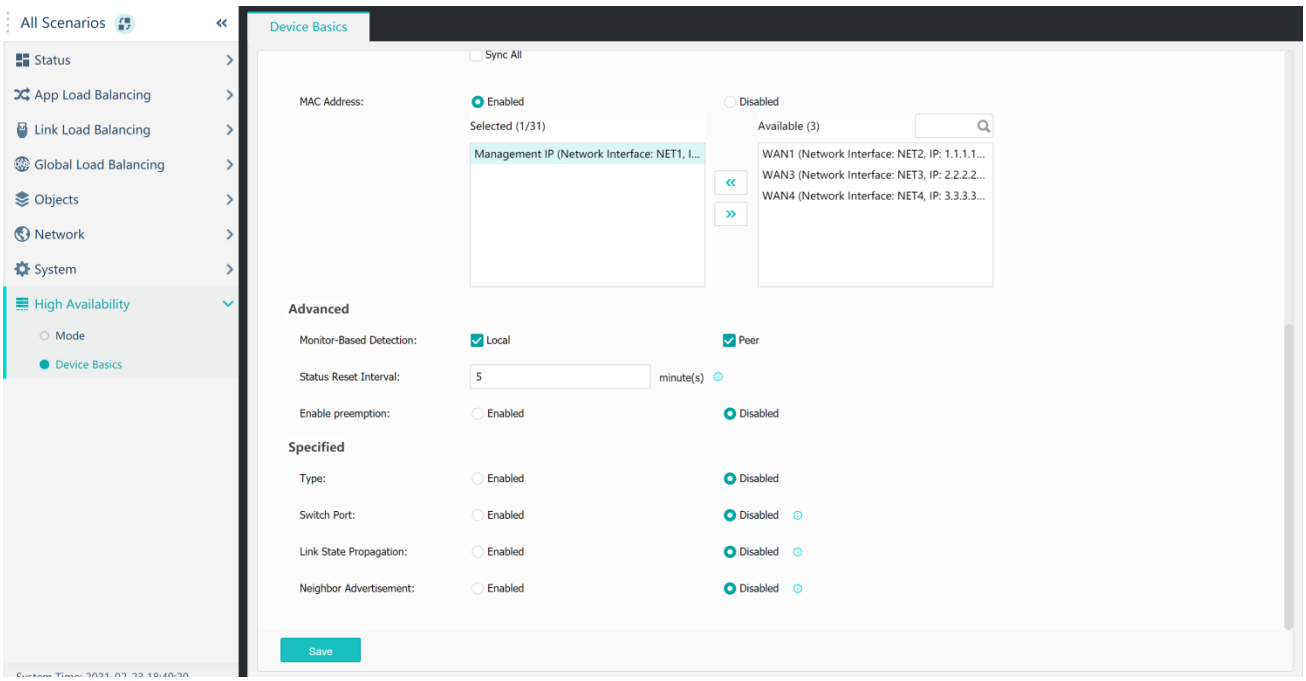
3.If you still cannot determine the causes, contact the technical support engineer from Sangfor in time.

13.4.6 Failing to Access the Internet After Switching Between Active and Standby Devices

2.After checking ADC's active and standby devices, log in to the ADC console and choose【Status】-> 【Logs】-> 【Service Logs】to view whether there are offline links, and determine offline links according to the printed prompt message.

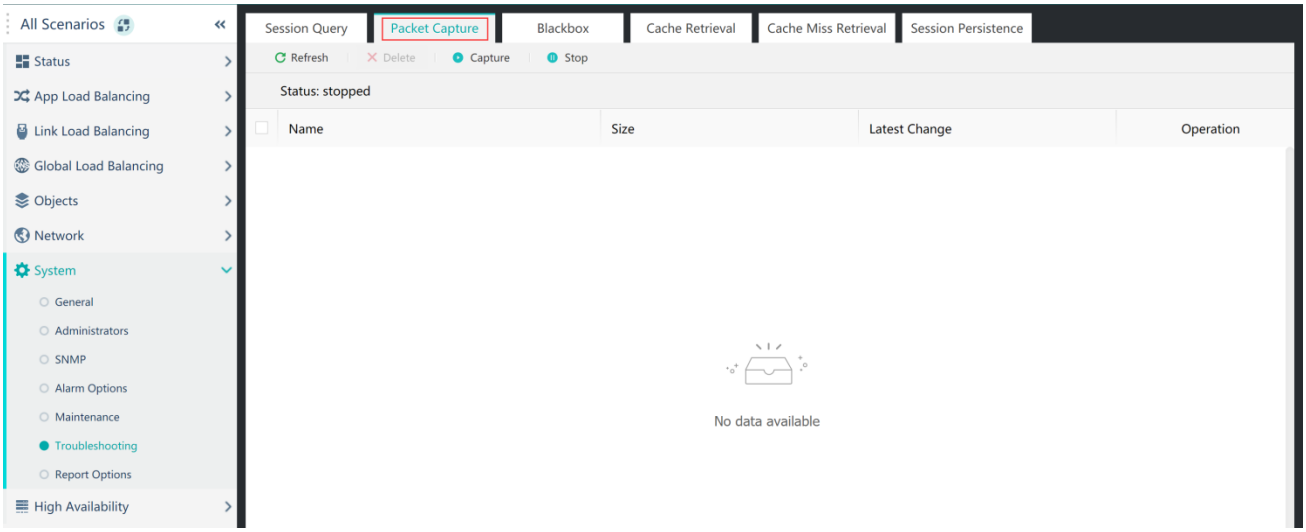


3.Check whether session synchronization and virtual MAC address synchronization are enabled in the configurations of ADC's active and standby devices. If the MAC address synchronization is enabled, the time for refreshing APR can be shortened. If the session synchronization is enabled, session information of the active device can be automatically synchronized to the standby device, thus shortening the service interruption time.



Choose【System】-> 【Device Management】-> 【Web Console】, and run the arp command to check whether the corresponding interface learns the MAC address of gateway; run the ping command to test whether the connectivity to gateway is good; and run the ping –I command to test whether the IP address of this interface can be connected to the Internet.

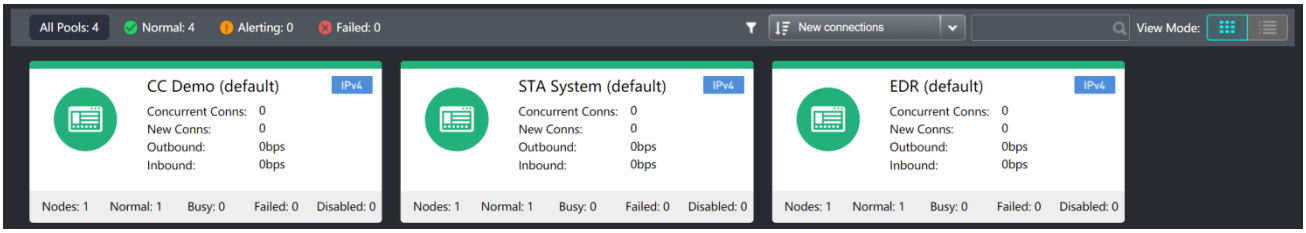
4.Choose【System】-> 【Troubleshooting】-> 【Packet Capture】, and set packet capture conditions on the Packet Capture tab; then perform packet capture analysis and view whether the request sent from a client is received and forwarded by an interface of ADC, as shown in the following figure.



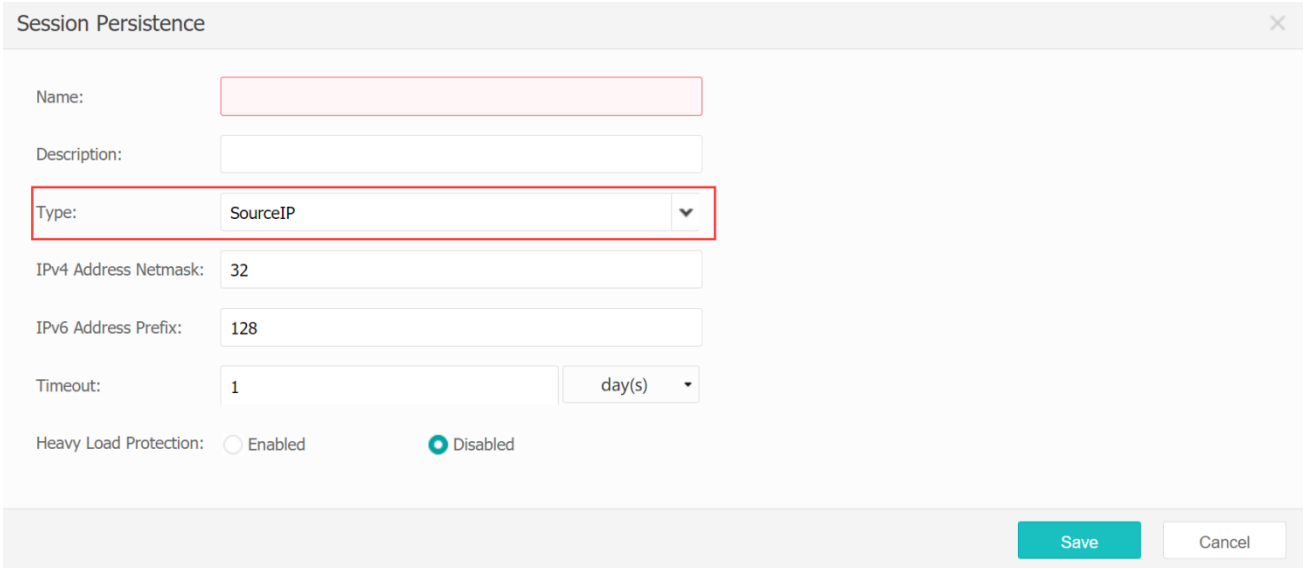
5.If you still cannot access the Internet, contact the technical support engineer from Sangfor in time.

13.4.7 Unbalanced Scheduling of Server Load Balancing Node

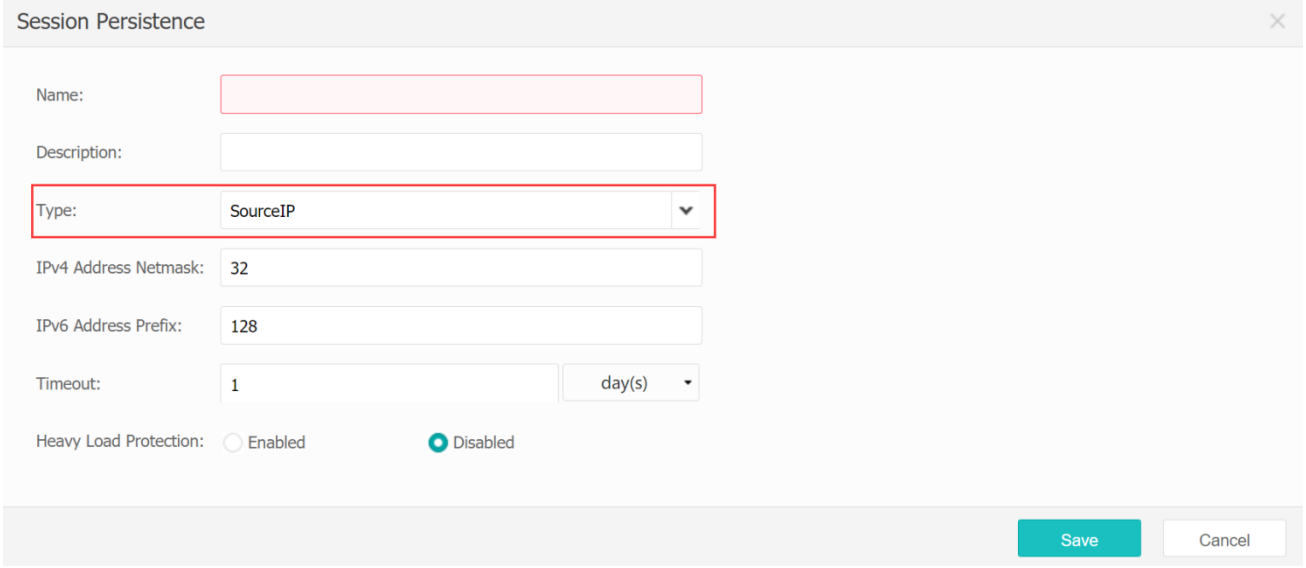
▶ Choose【Status】-> 【Node Pool】, find abnormal nodes, and check whether the new connections are reasonably scheduled.



▶ Choose【App Load Balancing】-> 【Node Pool】to view the session persistence type of this node pool.



▶ Choose【App Load Balancing】-> 【Node Pool】-> 【Session Persistence】to view the configuration of session persistence.



▶ If the scheduling of new connections in the node pool is still unbalanced, contact the technical support engineer from Sangfor in time.

Copyright © SANGFOR Technologies Inc. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.
SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.
Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc

