User Guide

AIDC Controller Usage Guide

Version 3.1 R0409P00

Asterfusion Data Technologies Co., Ltd.

Preface

This document primarily introduces the usage methods of the AIDC Controller. It covers, but is not limited to, controller deployment, basic operations, and daily maintenance, enabling first-time users to get started quickly while meeting the diverse needs of users, technical support engineers, and developers in various scenarios.

Target Audience

This manual is primarily intended for the following engineers.

- Network planners
- On-site technical support and maintenance staff
- Network administrator responsible for network configuration and maintenance

Modification of Records

Date	Version	Modify Remark
2025-12-30	V1.0	First release

Contents

1 Deployment Preparation

Recommended deployment environment:

x86 sever

Linux Version: Ubuntu 18.04 LTS or later

Docker Version: 20 or late

Table 1-1 Table of Equipment Quantity and Controller Hardware Resource Requirements

Device Number	CPU	Memory	Disk
500	4 Core	8G	500GB
1000	8 Core	16G	1000GB
2000	8 Core	16G	1500GB
5000	16 Core	32G	2000GB

2 Deployment Steps

1. Upload the packaged file of the controller version to the environment to be deployed for one-click installation. Use the -i parameter to specify the controller IP address.

```
./controller_V3.1R0409P00.bin –i <ip_address>
```

```
lzw@sonic:~/AIDC/R0409P00T01/controller_V3.1_R0409P00$ sudo ./controller_V3.1_R0409P00.bin -i 10.250.0.247
[2026-01-13 16:58:11] ============= Start deploying controller controller_V3.1_R0409P00=================
[2026-01-13 16:58:11] ============= deploy direction </opt/controller> =================
```

Figure 2-1 Installing the Controller Image

After successful deployment, users can directly access the controller through this IP address.

2. Use docker-compose to start the controller with one click. The default installation directory of the controller is /opt/controller/:

```
cd /opt/controller/controller_V3.1R0409P00/wlan-cloud-ucentral-deploy/docker-compose/
docker-compose up -d
```

[Explanation]

-d : indicates background execution.

up : indicates starting the controller.

down : indicates stopping the controller.

```
[+] Running 15/15
 ✔ Network openwifi_openwifi              Created
 ✔ Container openwifi-zookeeper-1         Started
 ✔ Container openwifi-postgresql-1        Started
 ✔ Container openwifi-portal-server-1     Started
 ✔ Container openwifi-kafka-1             Started
 ✔ Container openwifi-owsec-1             Started
 ✔ Container openwifi-owfms-1             Started
 ✔ Container openwifi-owanalytics-1       Started
 ✔ Container openwifi-owom-1              Started
 ✔ Container openwifi-owgw-1              Started
 ✔ Container openwifi-owupgrade-1         Started
 ✔ Container openwifi-owprov-1            Started
 ✔ Container openwifi-init-kafka-1        Started
 ✔ Container openwifi-owgw-ui-1           Started
 ✔ Container openwifi-owmgmt-1            Started
```

Figure 2-2 Controller Running Status

3 Controller Web Login and Logout

IE browser, Opera Mini browser, and all versions of browsers that have stopped updating are not supported. It is recommended to use Chrome browser version 114.0.5735.199 or later.

Default controller login information:

Email: aster@asterfusion.com

Password: Asteria

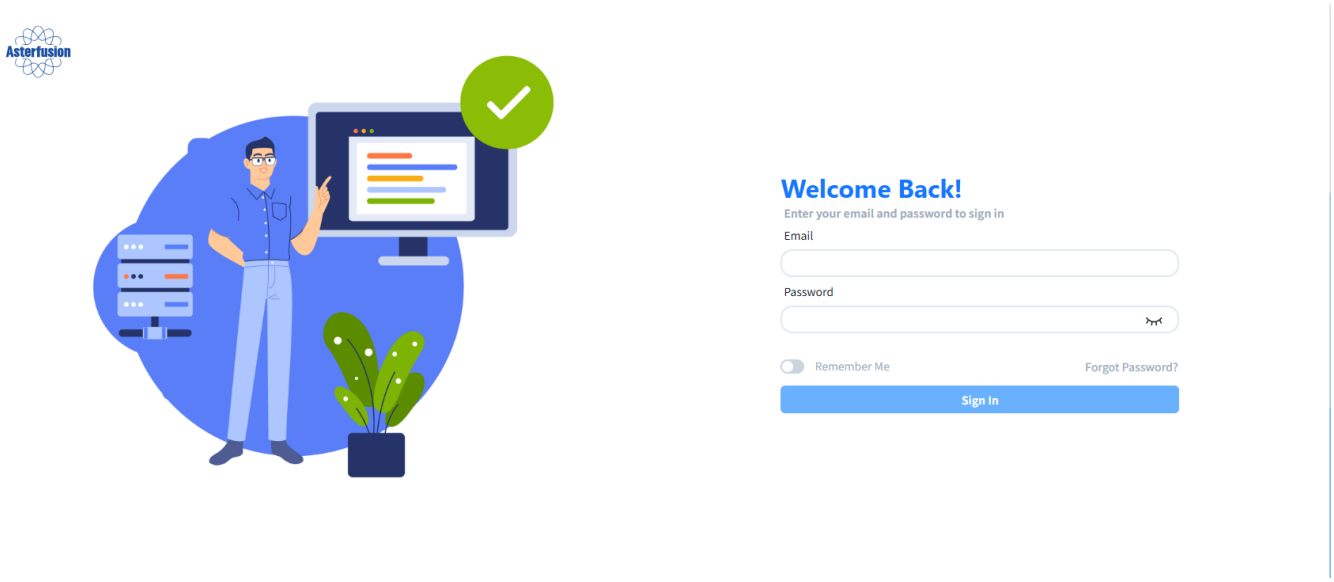


Figure 3-1 Controller Web Login Page

4 Organization and Inventory Management

The controller supports a multi-organization structure, and each organization can be divided into multiple "venues" for independent management. When the controller is deployed in a cloud environment, different organizations can be managed by different administrators to realize parallel use by multiple organizations and users.

After logging in to the controller, the system will automatically enter the [**Navigation**] - [**Map**] page. This page displays all organizations visible within the current user's permission scope and their subordinate venues in a structured view. System administrators can view the entire organization and venue structure under the controller, while ordinary administrators can only view the content within their permission scope.

On the map page, administrators can select existing organizational venues for management, or create new organizations or venues as needed. Double-click an organization or venue node to switch to the device view under that area for network device deployment, monitoring, maintenance and other operations.

By default, the left navigation bar displays the summary information of devices under all organizations within the user's permission scope; when the user enters a specific organization/venue through the map page, the system will focus on that area and display all device details under it to facilitate refined management.

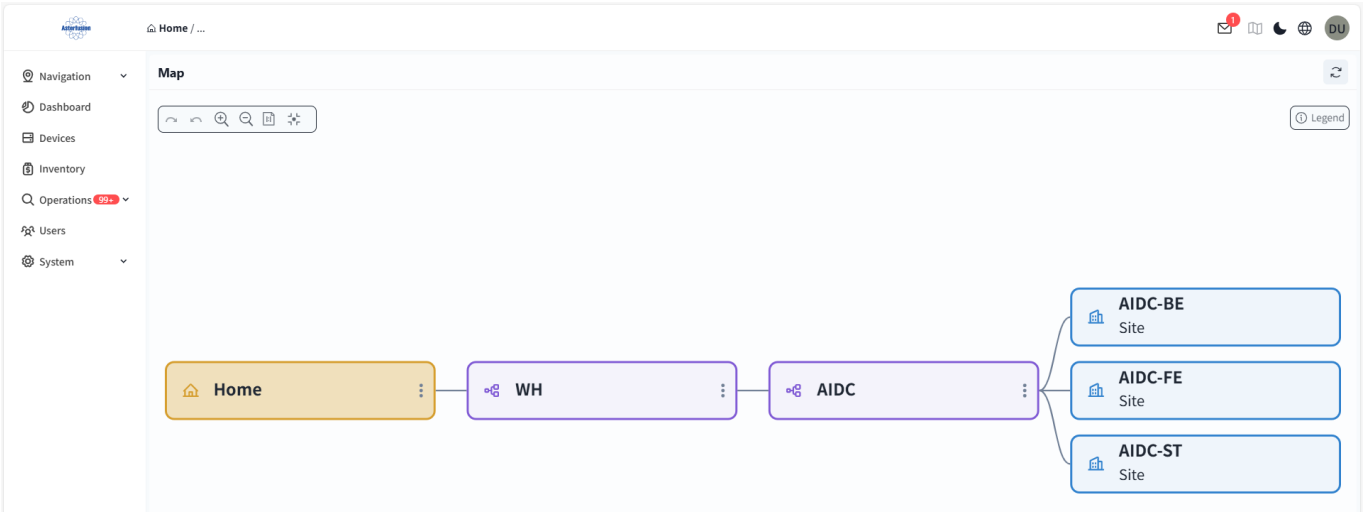


Figure 4-1 Map

4.1 Create an Organization

After logging in to the controller, click the [+] in the upper right corner to add an organization.

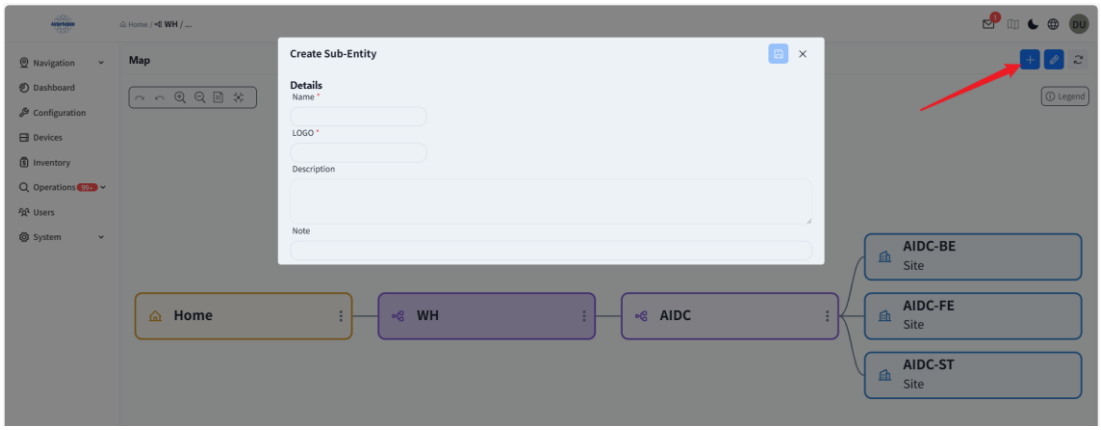


Figure 4.1-1 Creating an Organization

After completing the organization creation, double-click the created organization to enter it.

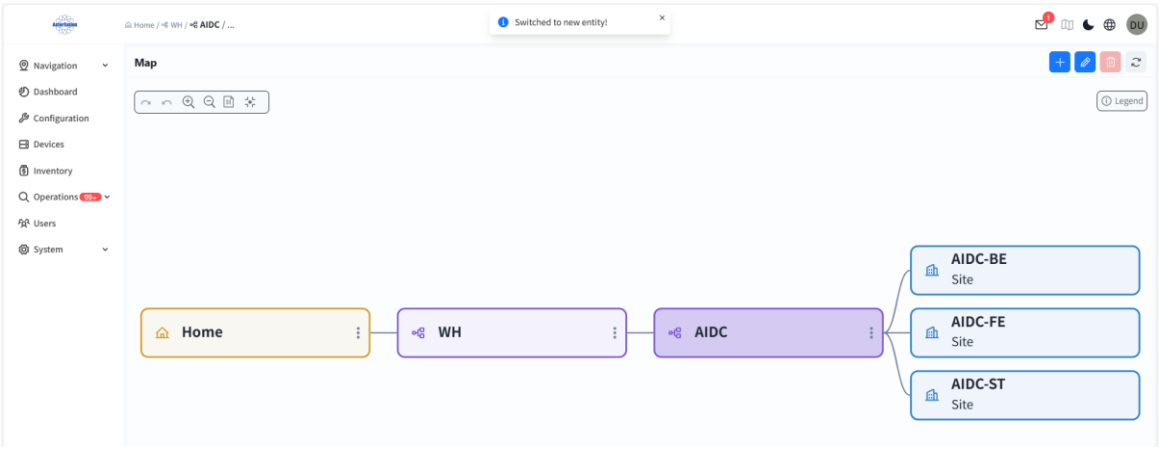


Figure 4.1-2 Switching Organizations

Click the [+] button to create a new venue.

A venue is a collection where administrators can monitor, manage, and configure all network devices.

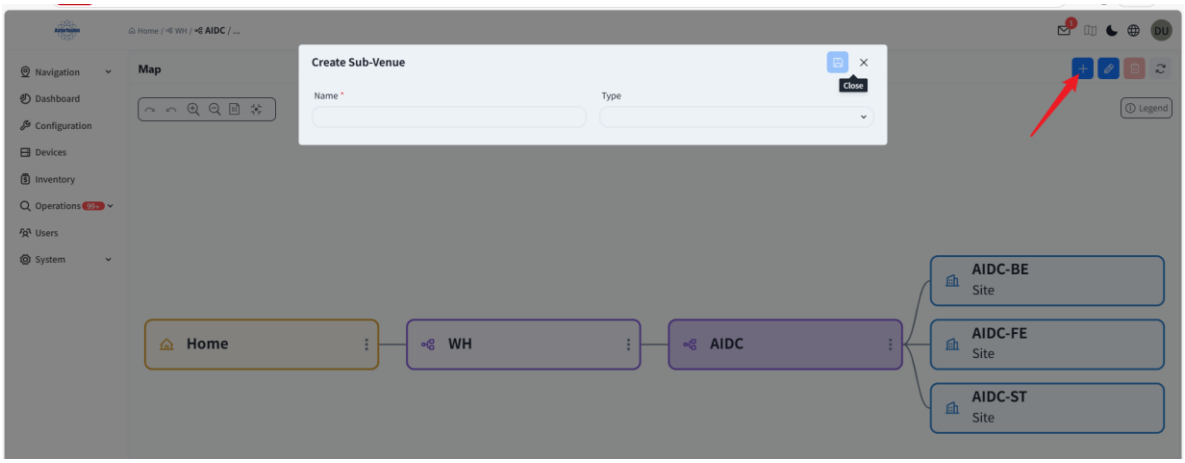


Figure 4.1-3 Creating a Venue

4.2 Adding Inventory

Administrators can create or batch import devices to specified venues/organizations. When the devices added to the inventory are connected to the controller and go online, the controller will automatically assign the devices to the specified organizations/venues according to their MAC addresses.

There are two ways to configure inventory devices:

1. In the organization view, you can specify the organization/venue of the inventory.
2. In the venue view, the added inventory is directly assigned to that venue.

Organization View

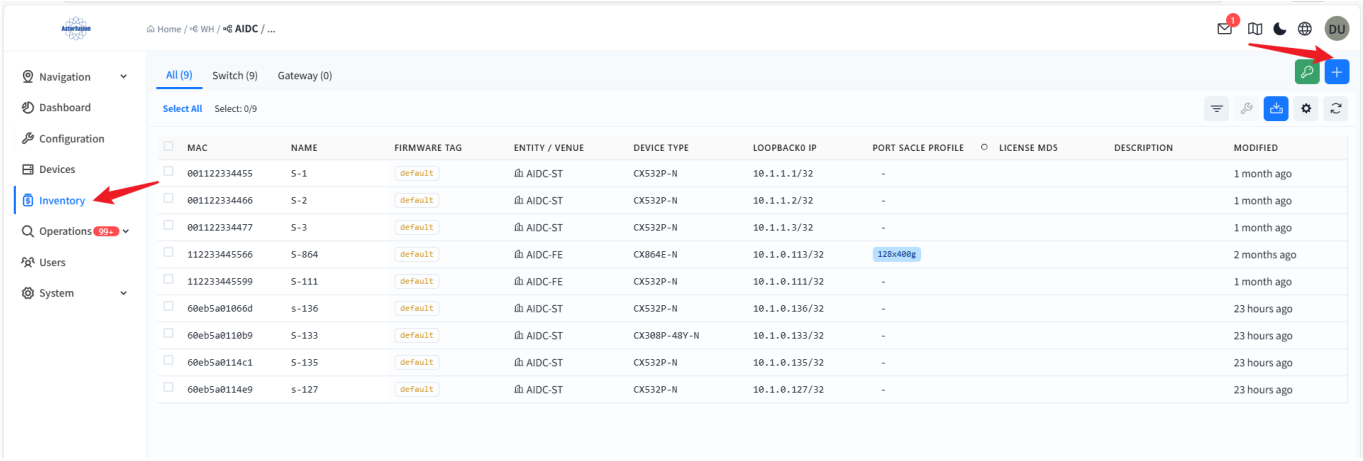


Figure 4.2-1 Organization View

- **Add one by one in the organization view**

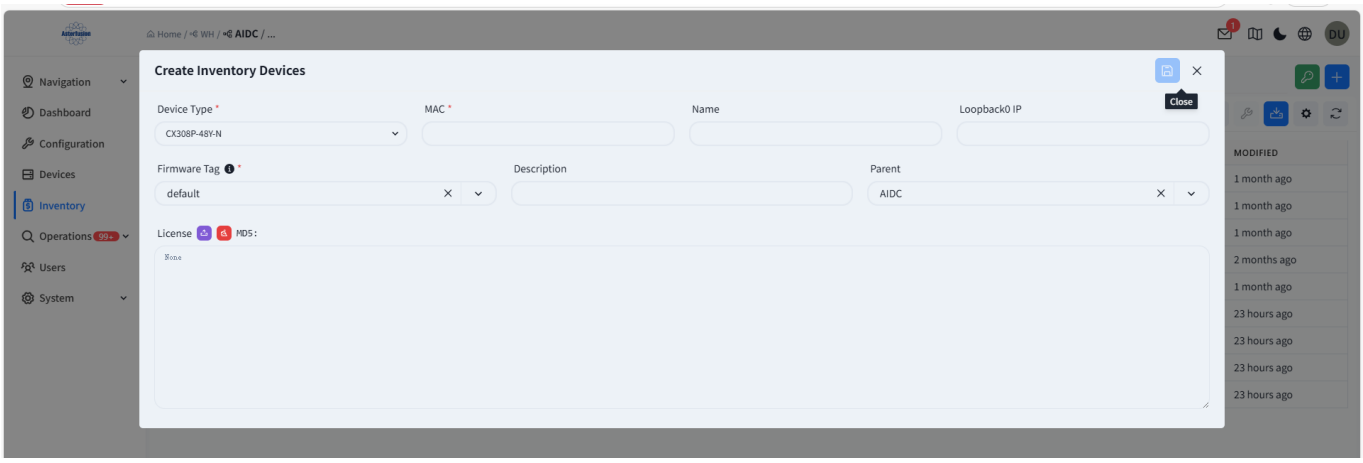


Figure 4.2-2 Adding Inventory in Organization View

Venue View

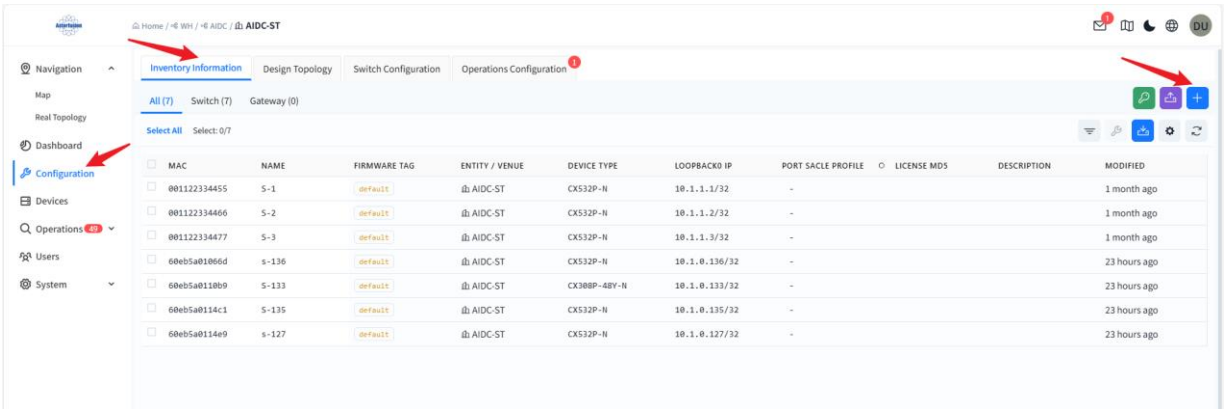


Figure 4.2-3 Venue View

- **Add one by one in the venue view**

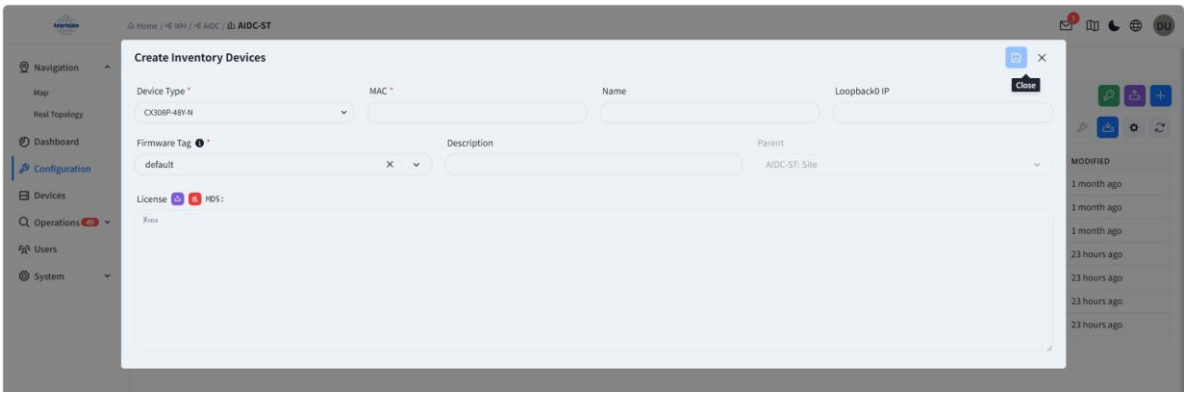


Figure 4.2-4 Adding Inventory in Venue View

- **Excel import in the venue view**

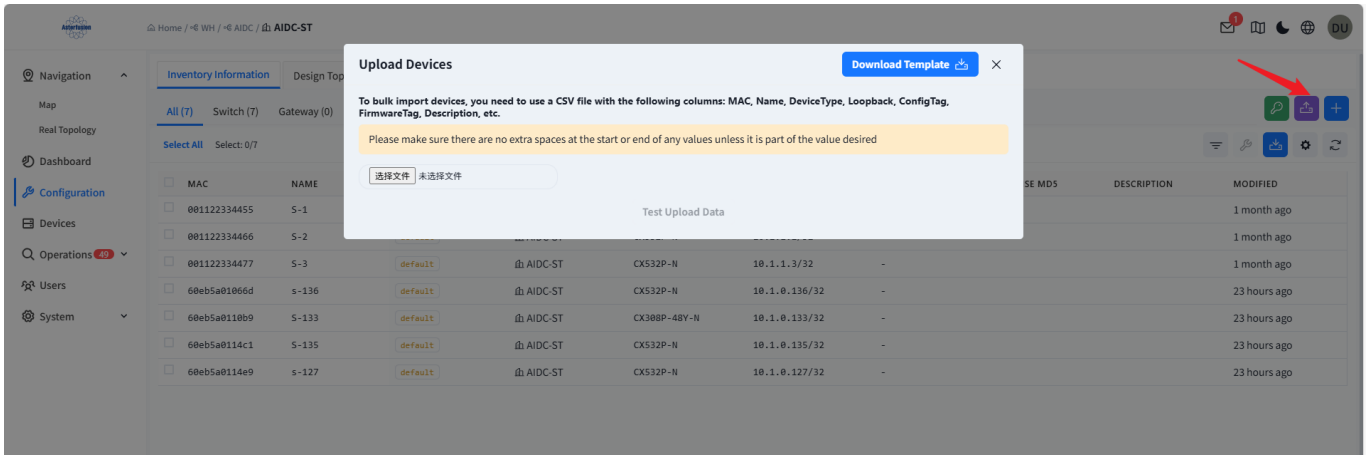


Figure 4.2-5 Importing Inventory via Excel in Venue View

Click [**Download Template**], and fill in the device information to be added to the inventory according to the template specifications.

	MAC	DeviceType	Name	FirmwareT	Loopback	PortScaleProfile	License	Description
1								
2	001A2B3C4D5E	CX864E-N	S-111	default	192.168.1.1/32	128x400g		TEST

Figure 4.2-6 Inventory Template

Required Fields

- MAC: The MAC address of the device, which is usually marked on the device label.
- Device Type: Device model.
- Firmware Tag (ConfigTag): When upgrading the device firmware, you can filter the devices to be upgraded according to the firmware tag type. By default, the tag value is default.
- Loopback Address (Loopback): The Loopback address of the device, which must meet the IPv4/MASK format.

Optional Fields

- Name: Device hostname.
- Interface Specification (PortScaleProfile): Pre-configuration of device interface specifications, only supporting CX864E-N device type, used to switch the initial form of device interfaces.
- Description: Information about the device.

- License: License file. For batch import, you can fill in the content of the License file in JSON format in Excel, or batch import the License after adding all devices to the inventory.

5 Device Connection to Controller

5.1 Switch

5.1.1 Configure Connection to Controller via Command Line

Use the command ucentral-client server <A.B.C.D> to configure the controller's IP address on the switch so that the device can connect to the controller.

If the device uses out-of-band management and the management port belongs to VRF mgmt, the user needs to carry the VRF parameter when specifying the management address, for example: ucentral-client server <A.B.C.D> vrf mgmt.

Example Configuration of Switch:

Figure 5.1-1 Device-to-Controller Connection Diagram

Connect to the controller using the out-of-band management port:

```
sonic# config
sonic(config)# feature ucentral state enable
sonic(config)# feature ucentral autorestart enable
sonic(config)# ucentral-client server 192.168.0.91 vrf mgmt
sonic(config)# interface mgmt 0
sonic(config-if-mgmt) ip address 192.168.0.20/24 192.168.0.91
sonic(config-if-mgmt) vrf mgmt
```

After configuration, you need to restart the ucentral-client service:

```
admin@sonic:~$ sudo service ucentral restart
```

After the configuration is completed, the switch can be seen online on the controller's [**Devices**] page.

6 Business Configuration

To simplify the configuration of typical network topologies, the controller currently has built-in AIDC backend network scenarios/AIDC frontend network scenarios/AIDC storage network scenarios. After selection, the topology planning is automatically completed. When all devices in the planned topology are connected to the controller and go online, ACC will automatically discover and identify the connection status between devices to generate a real network topology. Administrators can check whether the topology is correct. After confirmation, the pre-planned configuration will be delivered to the devices to complete the network configuration and deployment.

After entering a specific venue, the administrator clicks the [**Configuration**] - [**Design Topology**] button to select the specific scenario to be used.

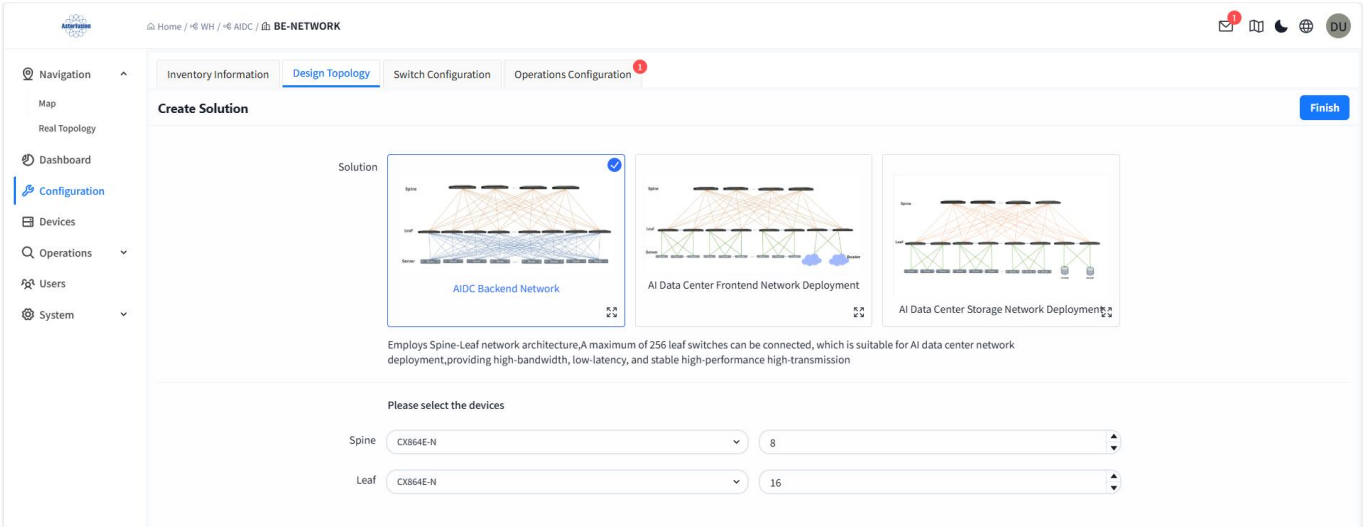


Figure 6-1 Supported Network Scenario

- **AIDC Backend Network**

A full three-layer network solution with a two-level Spine-Leaf structure. Taking Spine/Leaf both using the CX864E-N series as an example, a Spine device can provide up to 128 400G interfaces to interconnect with Leafs, and each Leaf can provide 64 400G access ports. That is, the network can provide a maximum of 128 x 64 = 8192 accesses.

- **AIDC Frontend Network**

Adopting a Spine-Leaf network architecture, it supports up to 64 Leaf switches for access. It is suitable for AIDC frontend network deployment. A distributed gateway is deployed on Leaf devices to provide EVPN MCLAG functions to achieve reliable service transmission and service isolation.

- **AIDC Storage Network**

Adopting a Spine-Leaf network architecture, it supports up to 64 Leaf switches for access. It is suitable for AIDC storage network deployment. A distributed gateway is deployed on Leaf devices to provide MCLAG and RoCE functions to achieve high-speed and reliable service transmission.

6.1 AIDC Backend Network Scenario Deployment

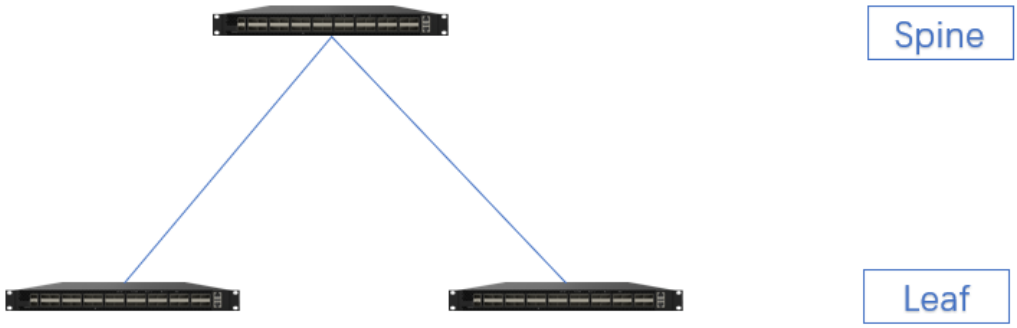


Figure 6.1-1 Backend Network Topology Diagram

6.1.1 Design Topology

Select the AI data center backend network scenario, fill in the model and quantity of Spine and Leaf devices, and then click [**Save**] to complete the pre-planning of the network topology. The controller will generate a recommended network topology according to the pre-planned typical network topology.

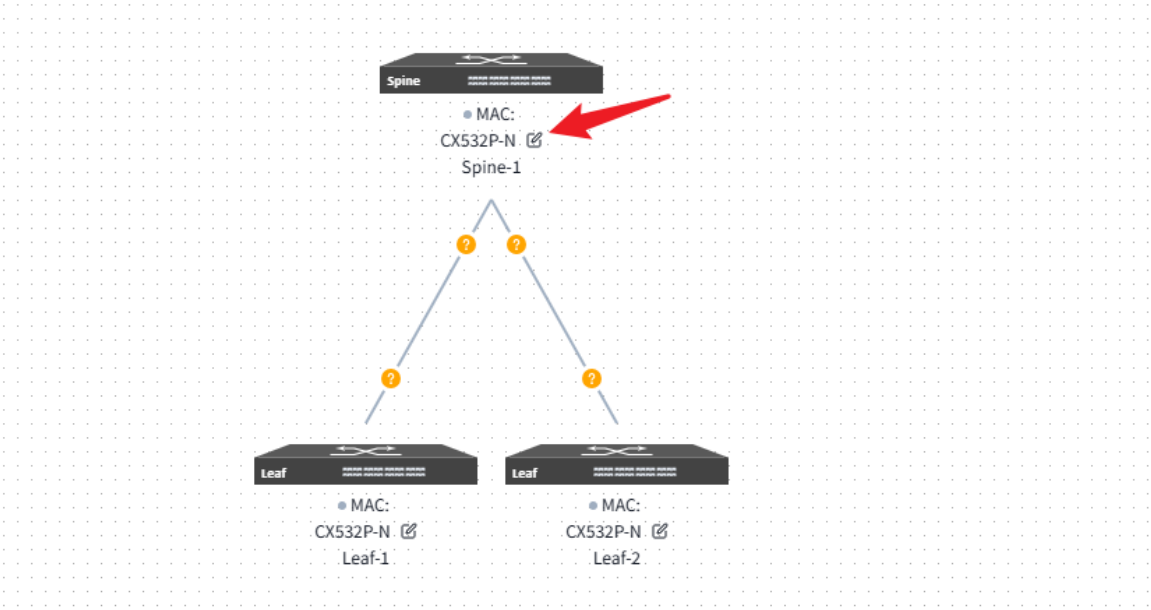


Figure 6.1-2 Backend Network Planned Topology

Users can click the [**Edit**] button on the device to select the devices in the inventory to be applied to the current topology in the slide-out box on the right, and then select the interconnection interfaces.

Note:

➢ It is recommended to separately plan and configure the device MAC and device role before planning the topology interconnection interface. When the controller identifies the planned topology device, it will automatically detect whether the device interface specification configuration in the current topology is consistent with the interface specification pre-configured in the inventory and guide the user to handle it. After processing, configure the interconnection interface to prevent errors or failures in configuring the interconnection interface due to inconsistent interface specifications with the pre-configuration.

Figure 6.1-3 Editing the Planned Topology

MAC: Uniquely select a device via its MAC address.

Loopback IP: Configure the IP address for the device's Loopback0 interface, which will be used for in-band management of the device.

hostname: Configure the hostname of the device.

Device role: Assign the device role as Spine or Leaf.

Interconnection Interfaces:

Local Interface: The interface on the current device.

Neighbor: Select the peer device connected to the local interface.

Neighbor Port: The interface on the peer device interconnected with the current device's local interface.

Or click [**Import Configuration**] in the upper right corner of the page to import the configuration. Before import, users can click [**Export Configuration**] on the right to obtain a blank configuration file. Fill in according to the configuration file template and import it.

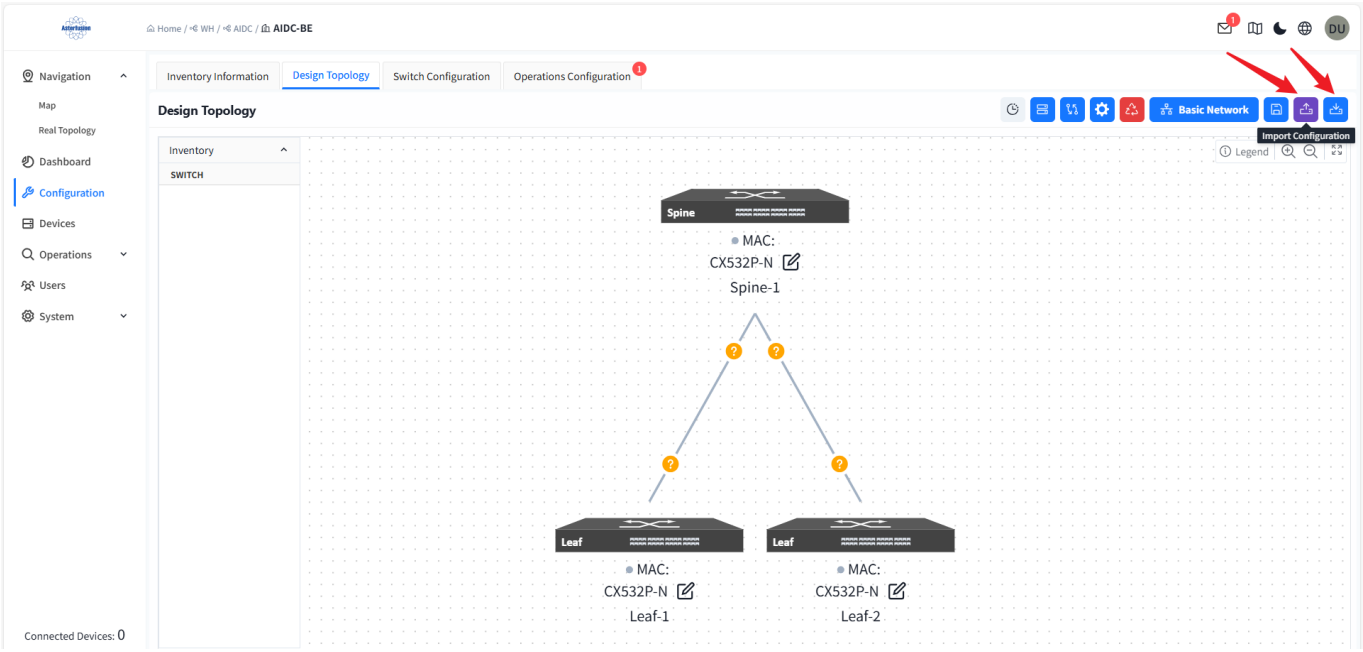
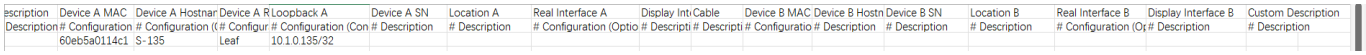


Figure 6.1-4 Importing Planned Topology via CSV

Configuration format:



escription	Device A MAC	Device A Hostnar	Device A R	Loopback A	Device A SN	Location A	Real Interface A	Display Inti	Cable	Device B MAC	Device B Hostn	Device B SN	Location B	Real Interface B	Display Interface B	Custom Description
Description	# Configuration	# Configuration ((	# Configur	# Configuration (Con	# Description	# Description	# Configuration (Optio	# Descripti	# Descripti	# Configuratio	# Description	# Description	# Description	# Configuration (Or	# Description	# Description
	60eb5a0114c1	S-135	Leaf	10.1.0.135/32												

Figure 6.1-5 Topology Import Template File

Note:

➢ When importing the planned topology through CSV, it is recommended that the CSV file first separately plans and configures the device MAC and device role. When the UI identifies the planned topology device, it will automatically detect whether the device interface specification configuration in the current topology is consistent with the interface specification pre-configured in the inventory and guide the user to handle it. After processing, configure the interconnection interface to prevent errors or failures in configuring the interconnection interface due to inconsistent interface specifications with the pre-configuration. The format example of importing device MAC and device role is as follows (that is, the interconnection interface is not filled in temporarily):

Description	Device A MAC	Device A Hostname	Device A Role	Loopback A	Device A SN	Location A	Real Interface A	Display Interface	Cable	Device B MAC	Device B Hostname	Device B SN	Location B	Real Interface	Display Interface	Custom Description
	60eb5a01066d	Spine-1	Spine	10.0.1.136/32												
	60eb5a0114c1	Leaf-1	Leaf	10.1.0.135/32						60eb5a01066d	Spine-1					

Figure 6.1-6 Topology Import Template File

After completing the topology editing, click the save button  in the upper right corner to save the topology editing.

6.1.2 Health Check of Designed Topology Devices

After completing the planned topology, click the [**Device Health Check**] button to verify to ensure that the devices and ports involved in the planned topology are in a normal state.

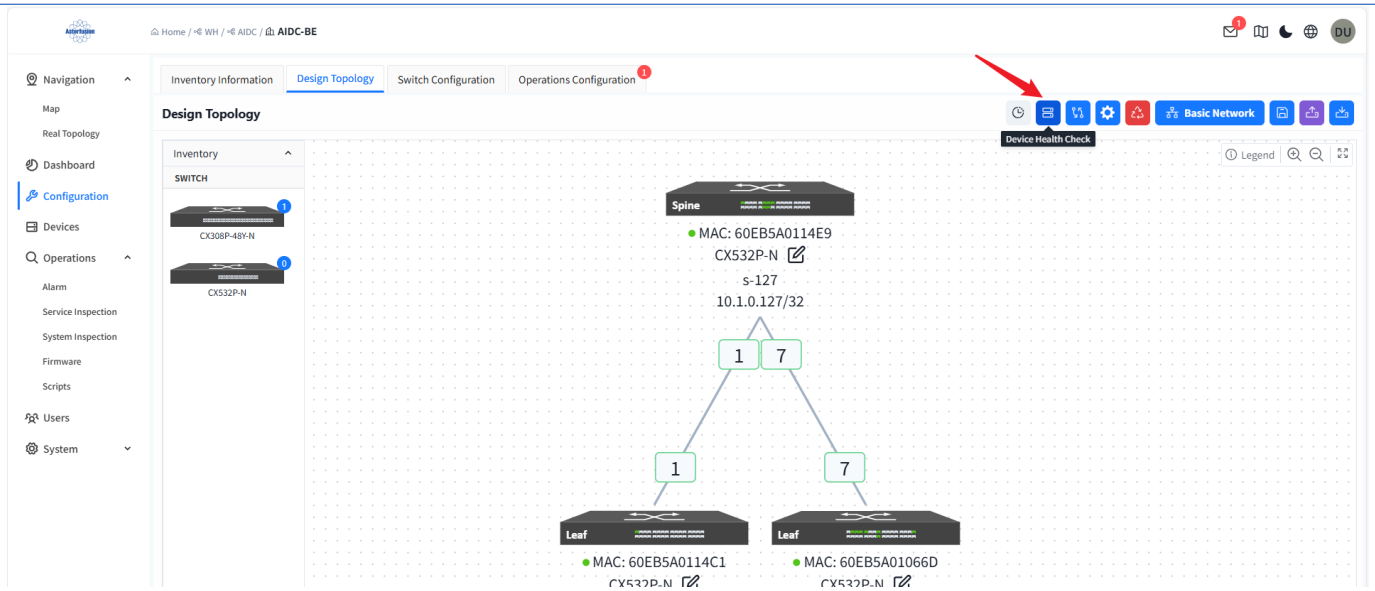


Figure 6.1-7 Device Health Check Button

If there is a problem, the problematic device and specific information will be displayed.

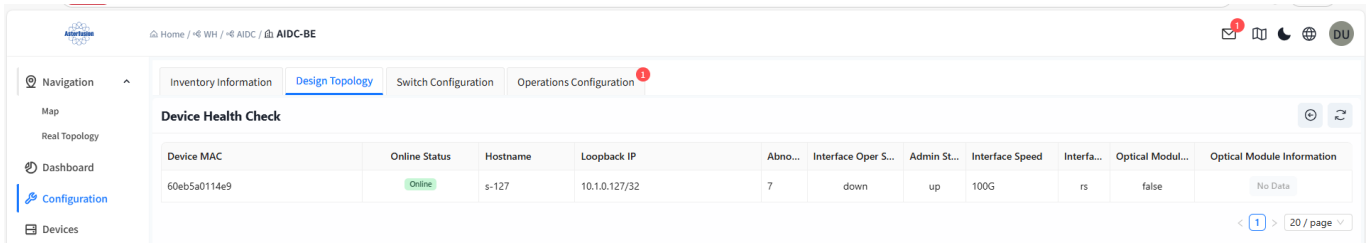


Figure 6.1-8 Device Health Check Results

6.1.3 Designed Topology Verification

After completing the planned topology, click the [**Topology Consistency Verification**] button to verify with the real topology to ensure the accuracy of the planned topology.

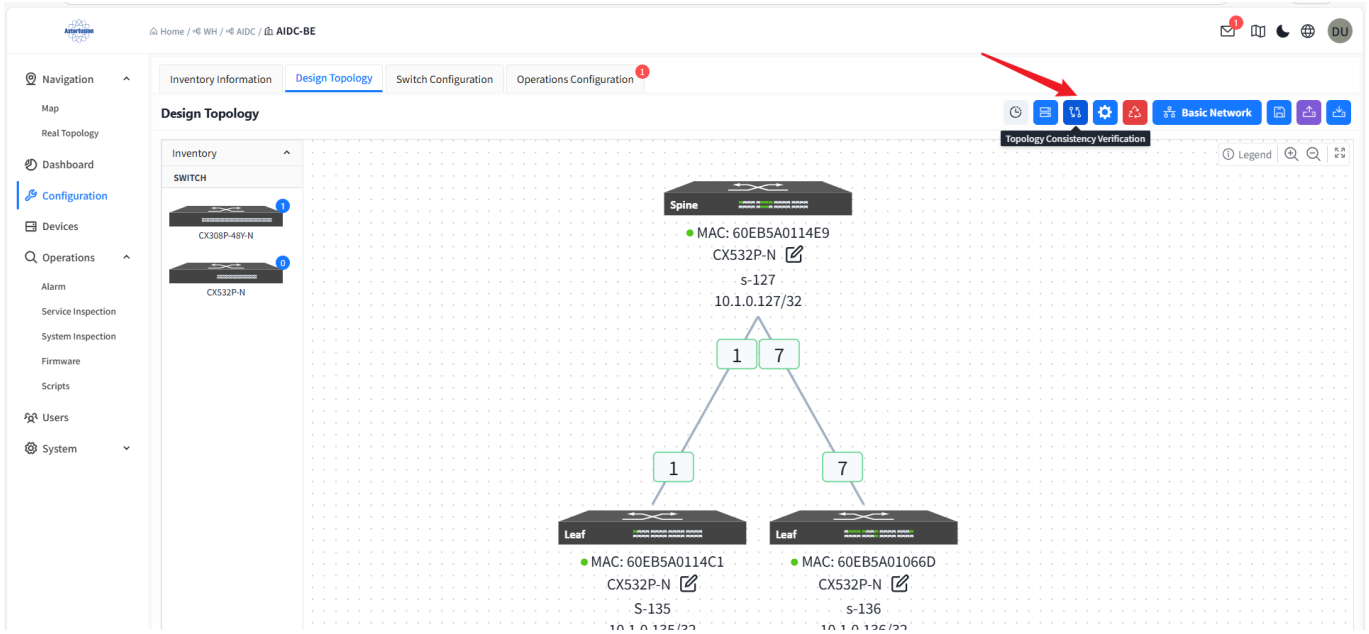


Figure 6.1-9 Planned Topology Validation

If there is a problem, a problem button will pop up. After clicking, the planned topology and real topology

information will be displayed, and the problematic topology can be quickly located.

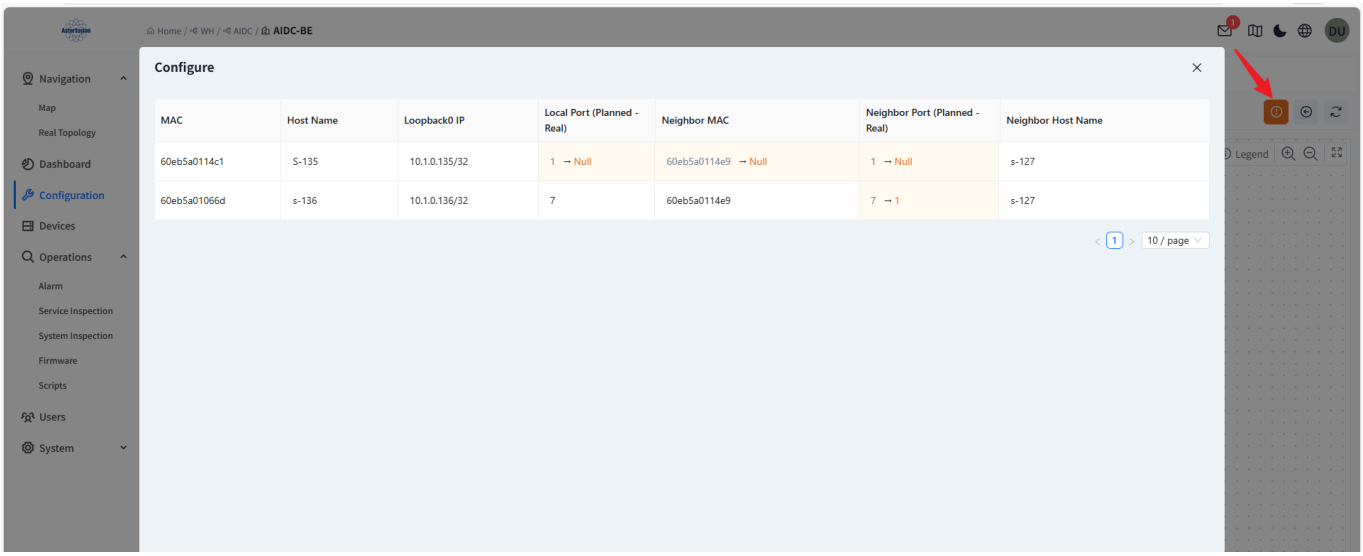


Figure 6.1-10 Planned Topology Validation Results

Hovering over the problematic interface in the topology view can also display specific problems.

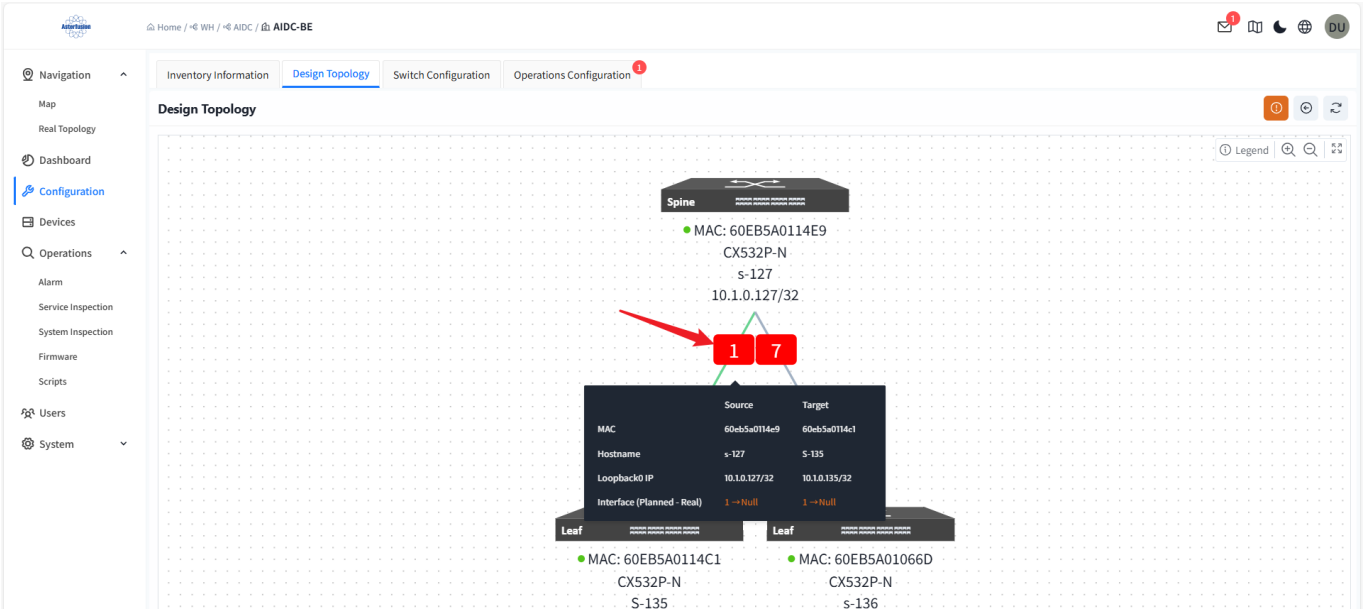


Figure 6.1-11 Viewing Validation Results by Hovering over an Interface

6.1.4 Basic Network Configuration

Click [**Basic Network Configuration**] to enter the basic network configuration interface to configure the basic network carrying the service network, including configuring the IP addresses of the interconnection interfaces between Leaf and Spine, Leaf and downstream devices, and the interconnection BGP protocol configuration.

6.1.4.1 Interface IP

Configure the IP address information of the device's physical interface or LAG interface.

- Physical interface

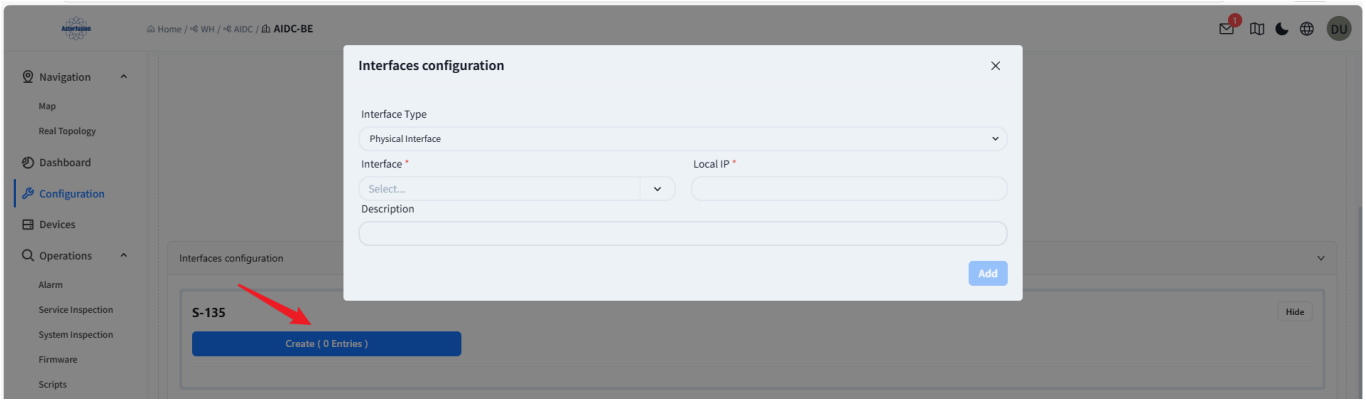


Figure 6.1-12 Configuring Physical Interfaces

- Aggregation interface

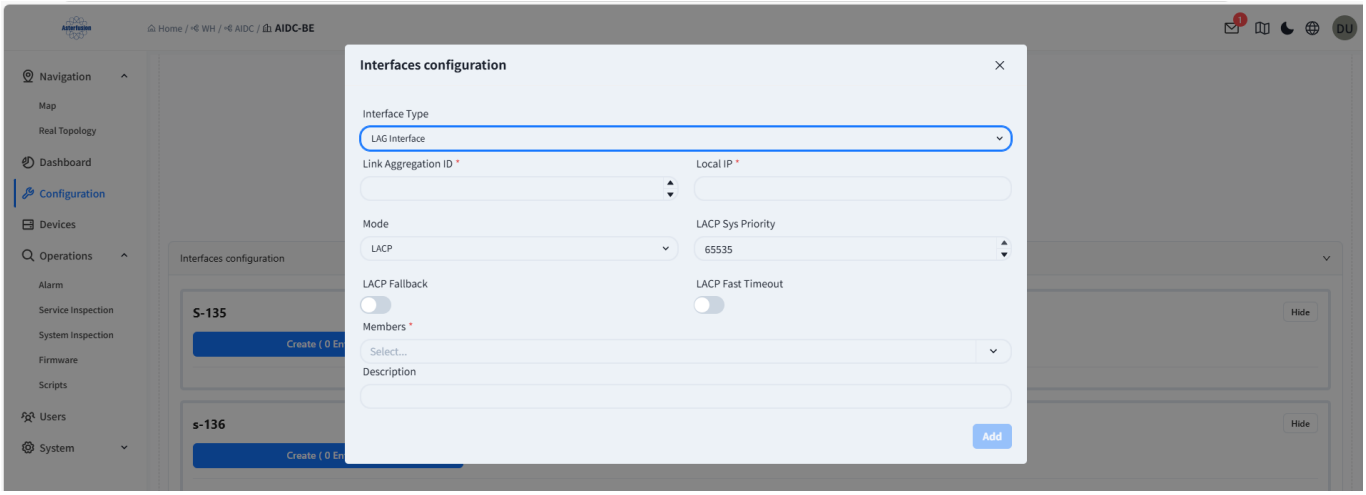


Figure 6.1-13 Configuring Aggregate Interfaces

- Interface configuration results

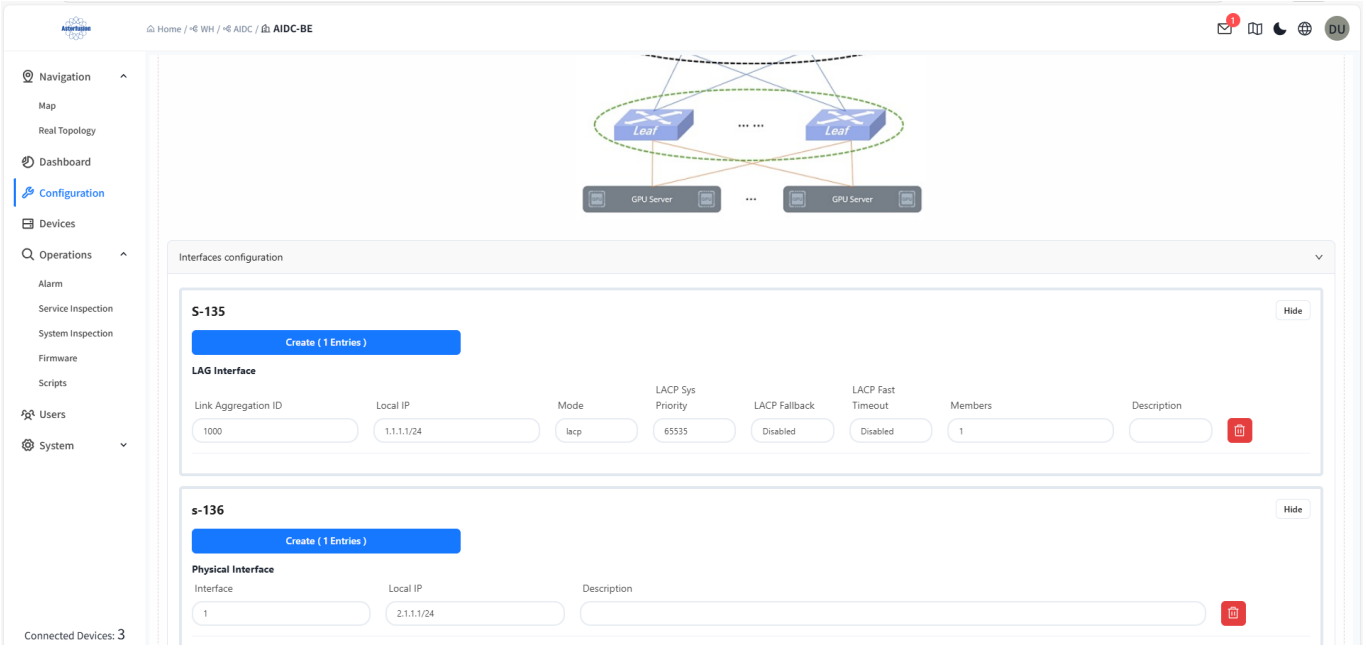


Figure 6.1-14 Interface Configuration Results

6.1.4.2 BGP Configuration

Click the [**Next**] button to enter BGP configuration.

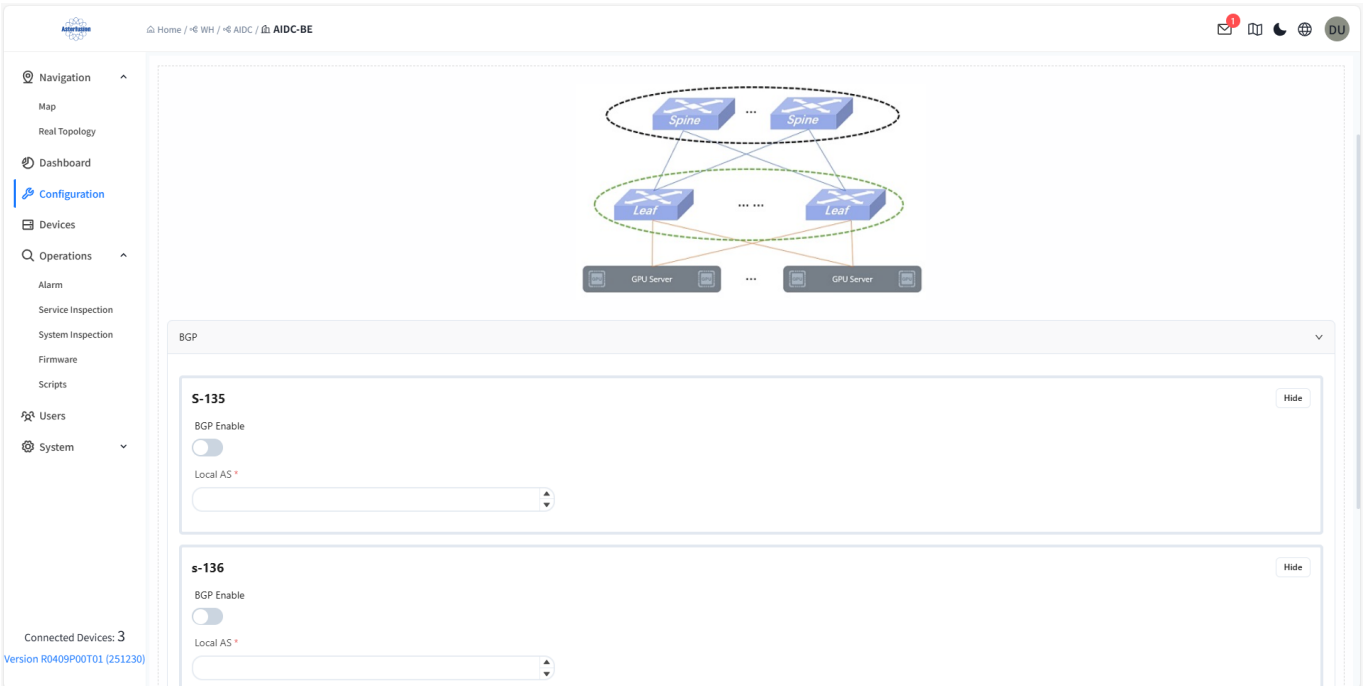


Figure 6.1-15 BGP Configuration Page

After enabling BGP, you can configure the local BGP AS number and display the option to configure BGP neighbors.

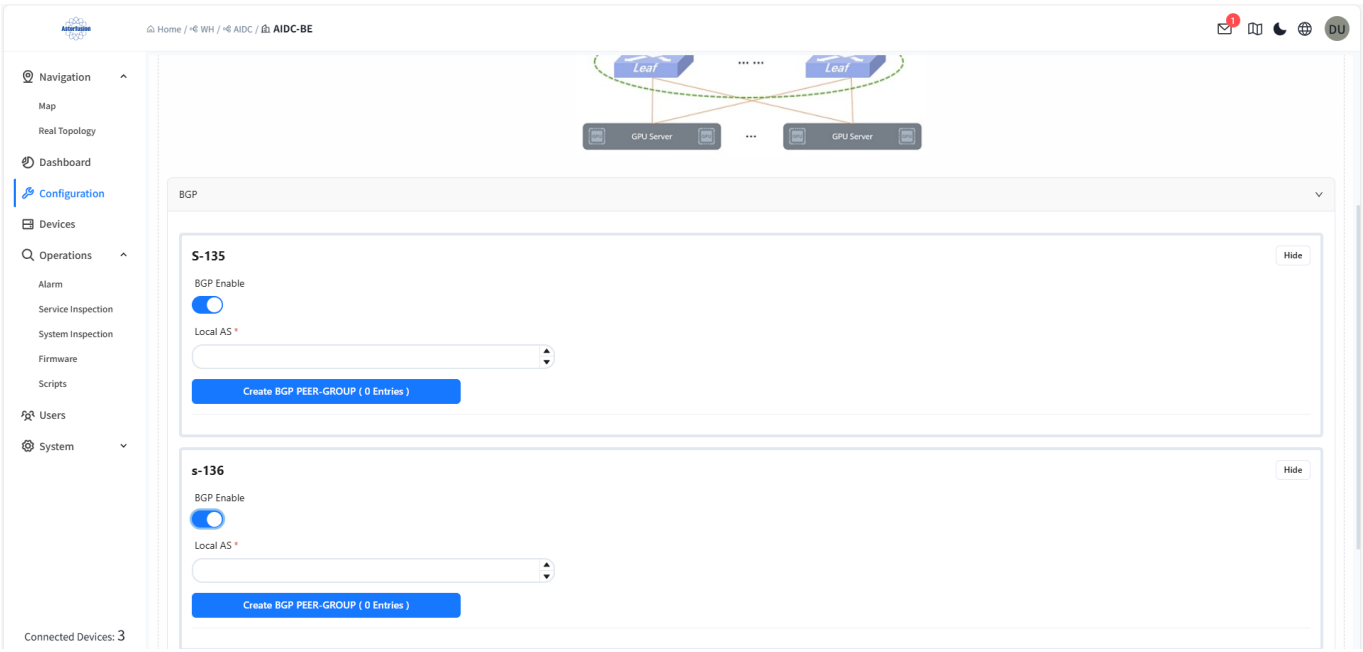


Figure 6.1-16 Enabling BGP

Click the Create BGP Neighbor box to enter the configuration of the device's BGP neighbors.

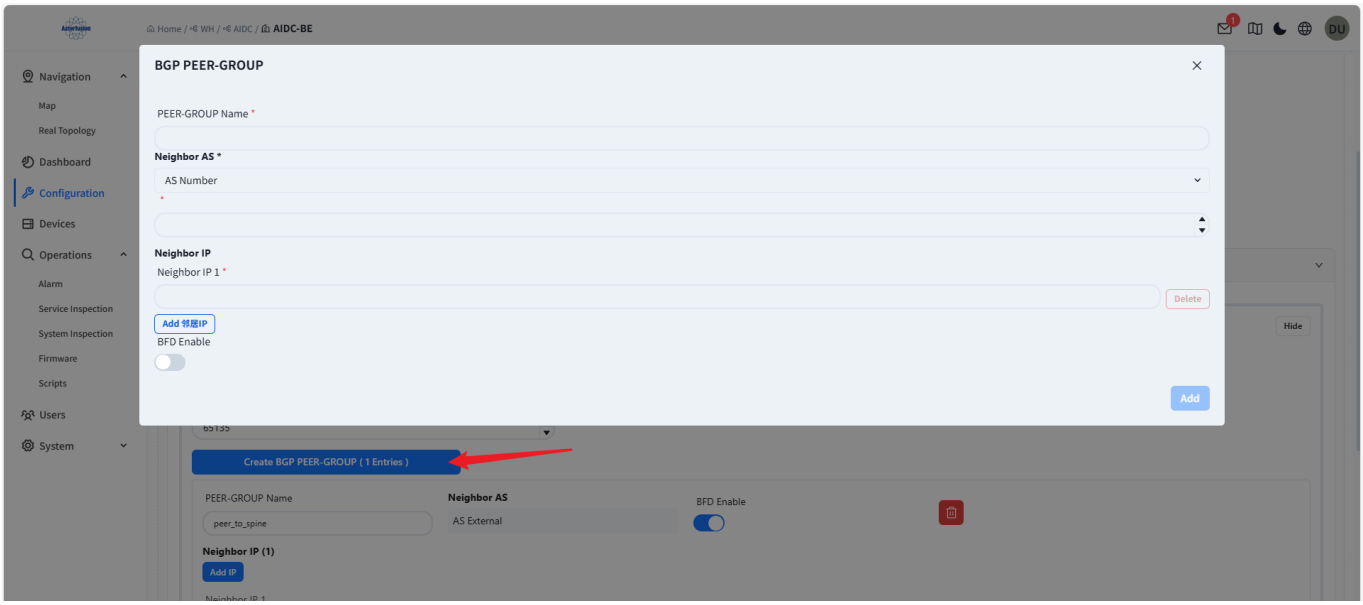


Figure 6.1-17 BGP Neighbor Configuration

After saving, the configuration information will be displayed.

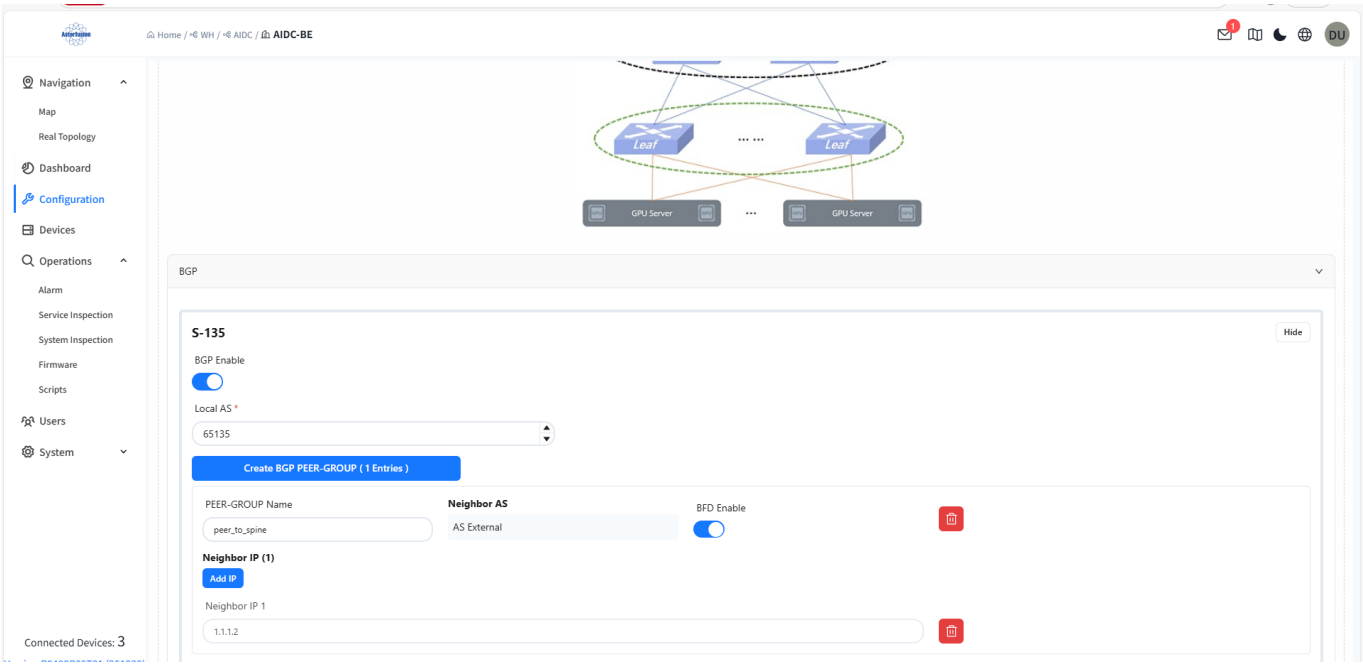


Figure 6.1-18 BGP Configuration Results

Click the [**Next**] button to complete the configuration, and click the [**Save**] button to save the basic network configuration.

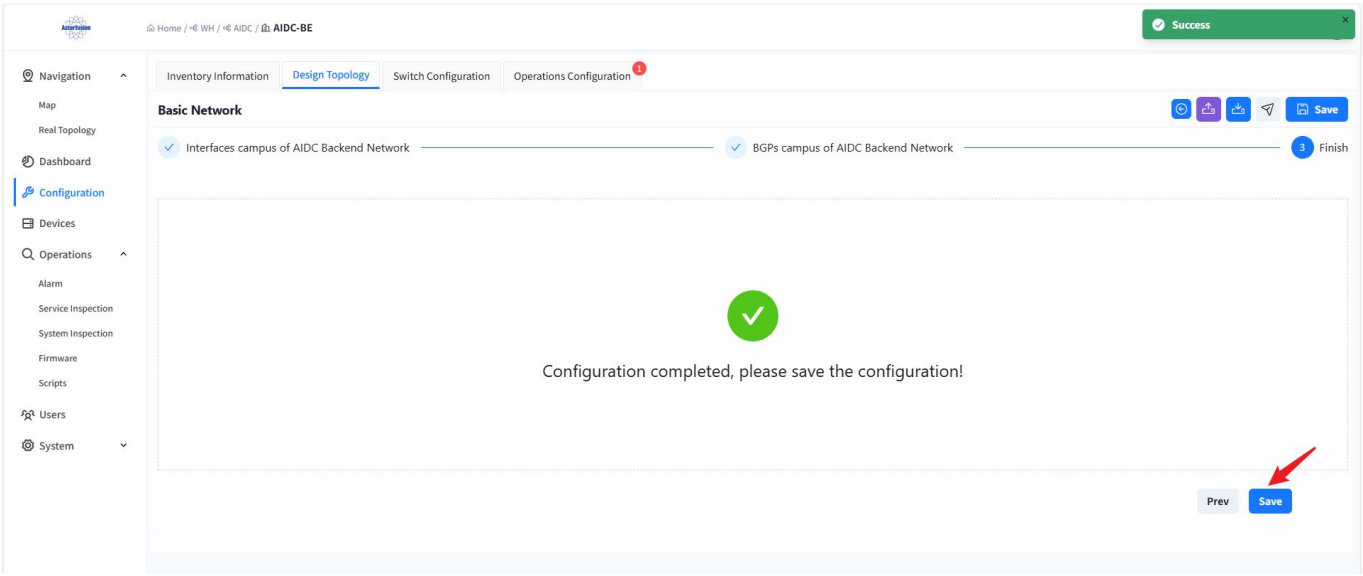


Figure 6.1-19 Saving Basic Network Configuration

6.1.4.3 Batch Import and Export of Basic Network Configuration

Click the [**Import Configuration**] button and You can Batch Import Basic Network Configuration with CSV file.

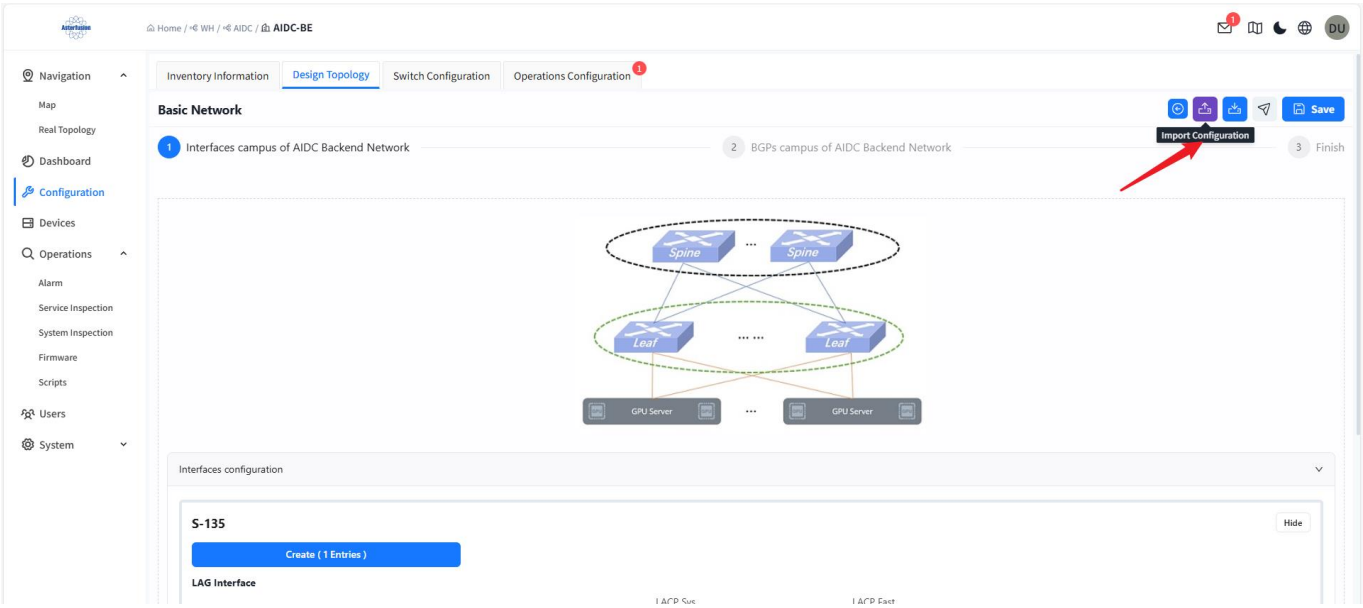


Figure 6.1-20 Importing Basic Network Configuration via CSV

Before uploading the file, users can click [Download Template] to obtain an example configuration file.

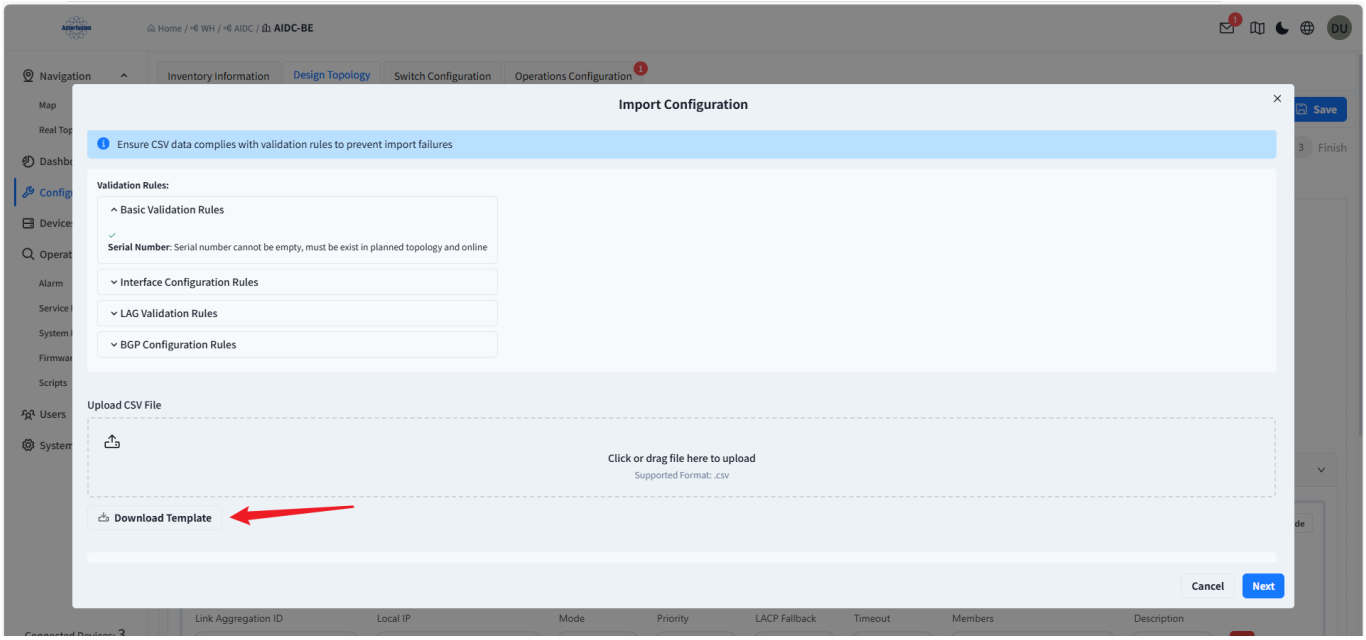
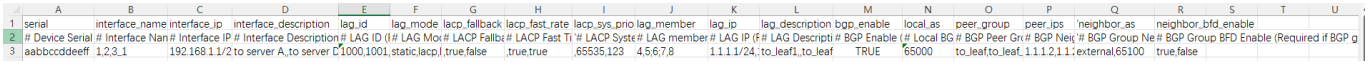


Figure 6.1-21 Template File Download Button

Template format as below:



serial	interface_name	interface_ip	interface_description	lag_id	lag_mode	lacp_fallback	lacp_fast_rate	lacp_sys_prio	lag_member	lag_ip	lag_description	bgp_enable	local_as	peer_group	peer_ips	neighbor_as	neighbor_bfd_enable
# Device Serial	# Interface Nan	# Interface IP	# Interface Description	# LAG ID (I	# LAG Mo	# LACP Fallb	# LACP Fast Ti	# LACP Syste	# LAG member	# LAG IP (F	# LAG Descripti	# BGP Enable	(# Local BG	# BGP Peer Gr	# BGP Neig	# BGP Group Ne	# BGP Group BFD Enable (Required if BGP g
aabbccddeeff	1,2,3_1	192.168.1.1/2	to server A,to server D	1000,1001	static,lacp,l	true,false	true,true	65535,123	4,5,6;7,8	1.1.1.1/24,;	to_leaf1,,to_leaf	TRUE	65000	to_leaf,to_leaf_1	1.1.2,1.1.1	external,65100	true,false

Figure 6.1-22 Template File

Fill in according to the configuration file template and import it. After the import is completed, click Save

to save the basic network configuration.

Users can also click the Export Configuration button to obtain the currently configured interface IP information and BGP configuration information.

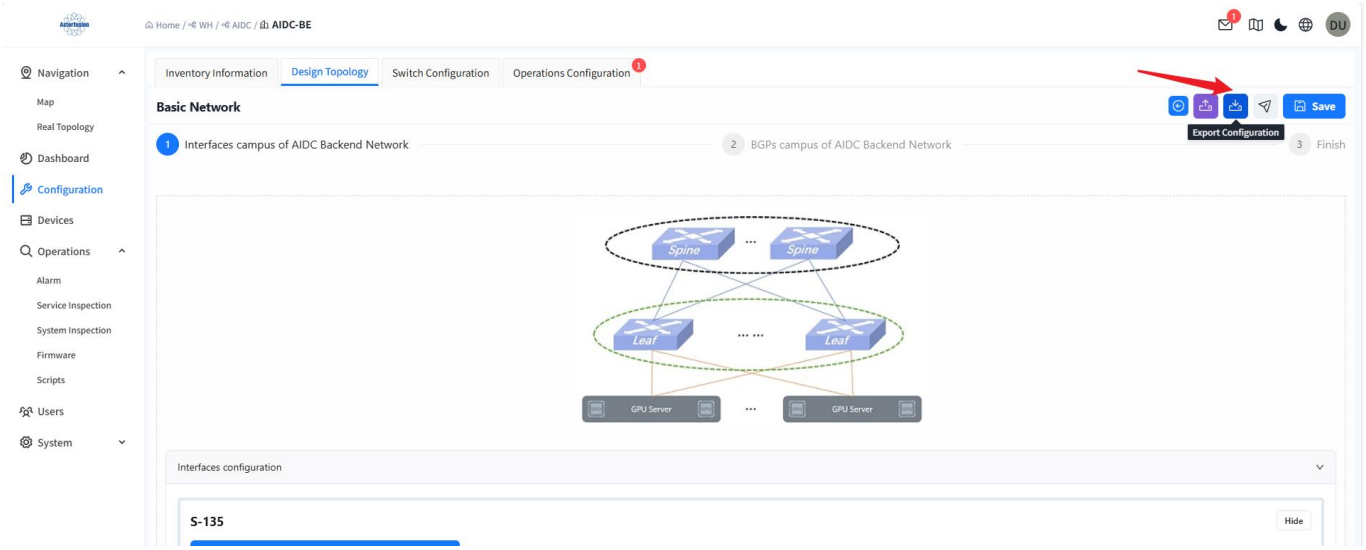


Figure 6.1-23 Exporting Basic Network Configuration

6.1.5 Wired Service Configuration

Click [**Switch Configure**] to enter the wired service management interface to configure the corresponding services on the switch for wired users.

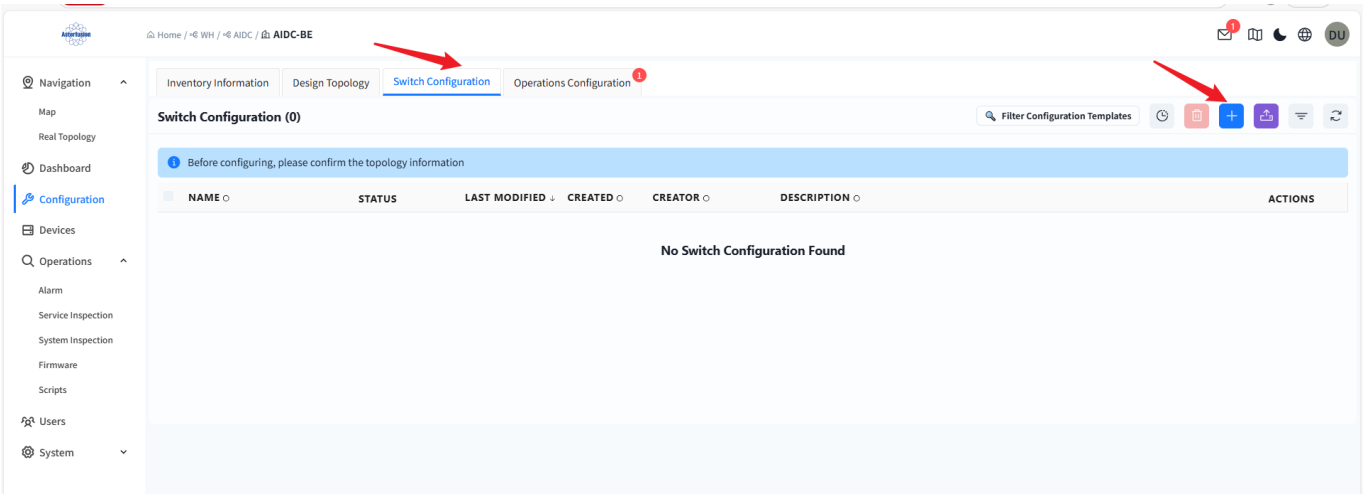


Figure 6.1-24 Wired Service Configuration Page

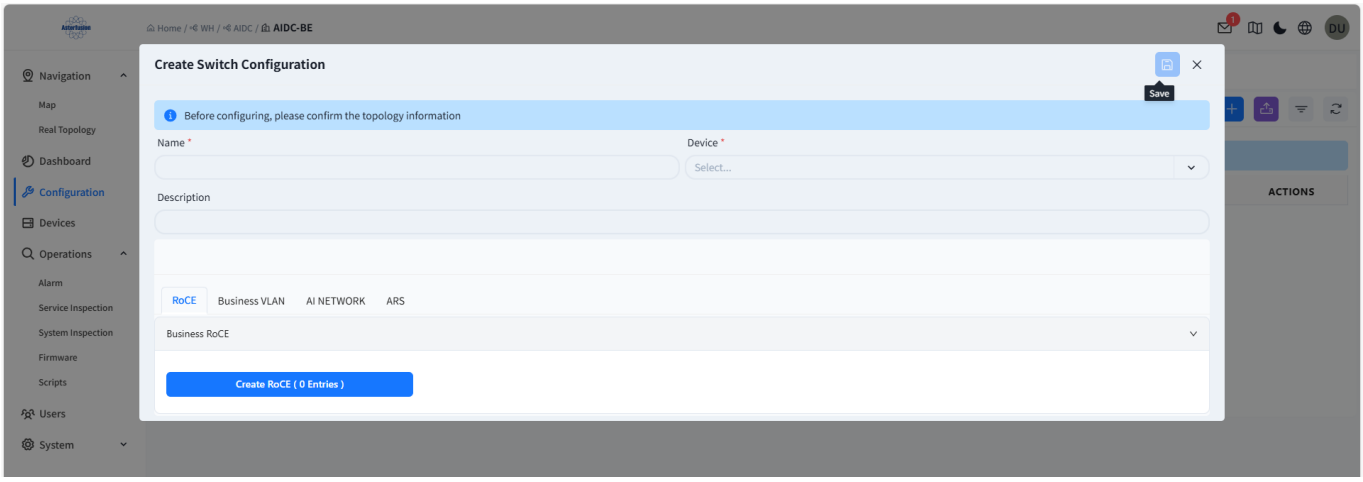


Figure 6.1-25 Creating Wired Service Configuration

6.1.5.1 RoCE Function

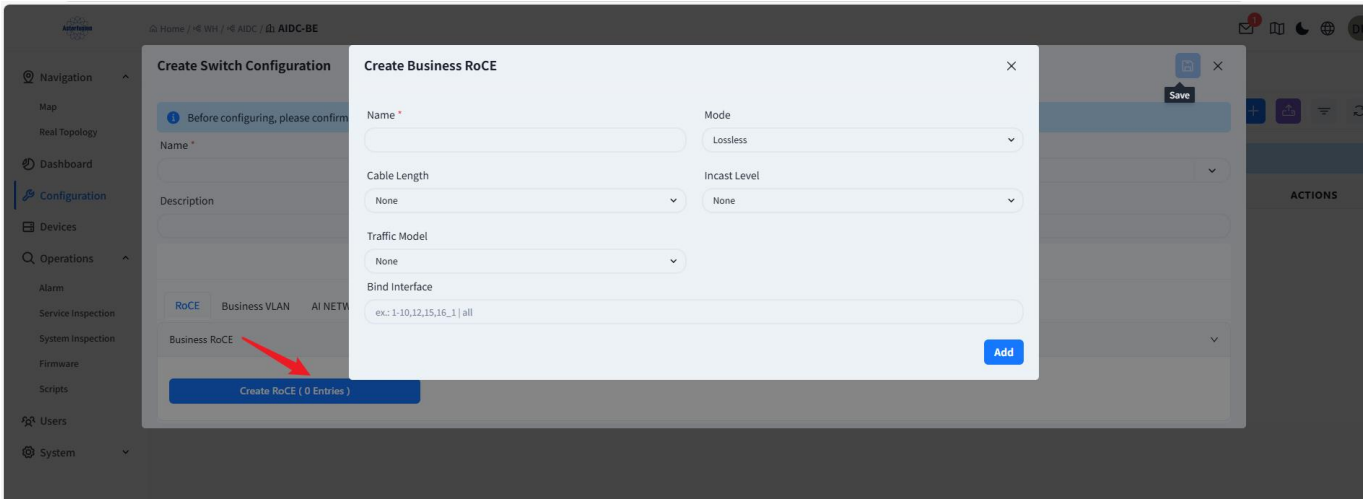


Figure 6.1-26 Creating RoCE Configuration

- Name: The policy name of the configured RoCE, uniquely identified.
- Mode: Configure the RoCE policy mode, which can be selected by clicking the drop-down arrow.
- Cable Length: Configure the cable length parameter of the RoCE policy, which can be selected by

clicking the drop-down arrow.

- Incast Level: Configure the Incast level parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Transmission Mode: Configure the transmission mode parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Bind Interface: Configure the interfaces to which the RoCE policy is applied.

6.1.5.2 Service VLAN Function

Configure the Leaf downstream interface VLAN, which is used to configure the downstream link list in the form of VLAN interfaces in the AI-Network instance.

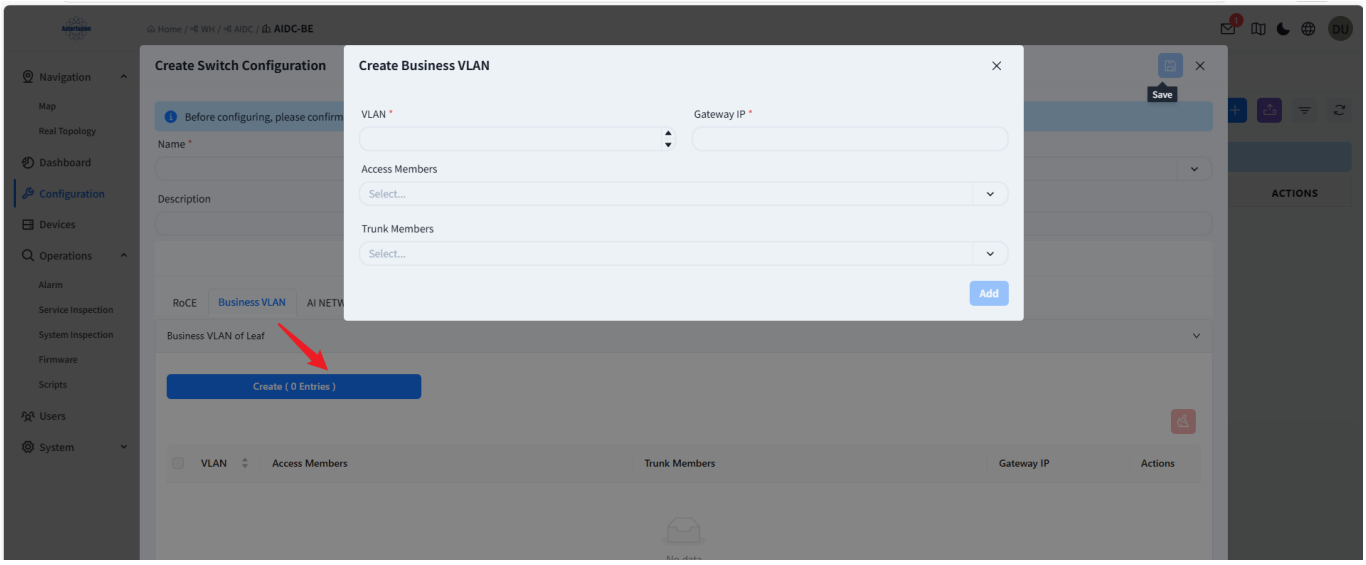


Figure 6.1-27 Creating VLAN Configuration

- VLAN: VLAN ID.
- Gateway IP: VLAN interface IP address.
- Access Members: Interfaces added to the VLAN in untag mode.
- Trunk Members: Interfaces added to the VLAN in tag mode.

6.1.5.3 Intelligent Routing Function

Configure the AI-Network intelligent routing policy. Spine/Leaf need to be configured separately.

6.1.5.3.1 Spine Device

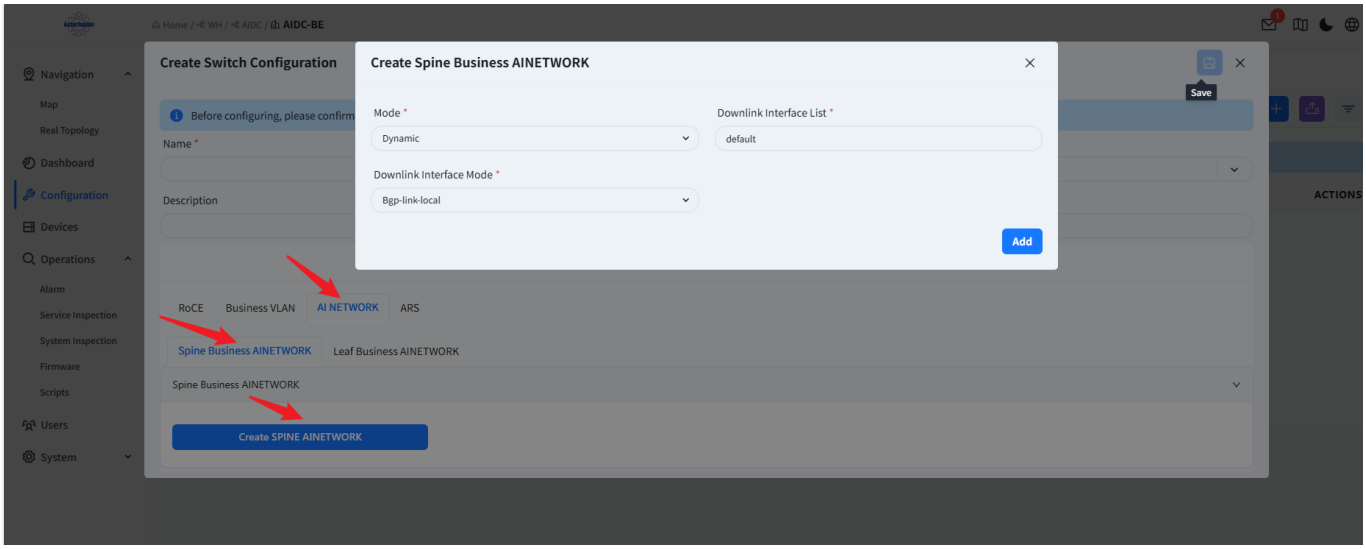


Figure 6.1-28 Configuring Intelligent Routing Function on Spine Devices

- Mode: Configure the intelligent routing mode of the Spine device. It can be selected by clicking the drop-down arrow, supporting dynamic mode and static mode. In static mode, VRF is assigned according to the source IP, service isolation is achieved through VRF, and 1:1 forwarding is achieved according to policy routing; in dynamic mode, VRF is assigned according to the source IP, service isolation is achieved through VRF, and the path weight of the local switch is adjusted through the path quality perceived by the switches in the network, combined with WCMP to achieve more flexible load balancing.
- Downlink Interface List: Configure the intelligent routing downstream link interface, which is generally selected from the interfaces interconnected with Leaf.
- Downlink Interface Mode: Configure the intelligent routing downstream interface mode.

6.1.5.3.2 Leaf Device

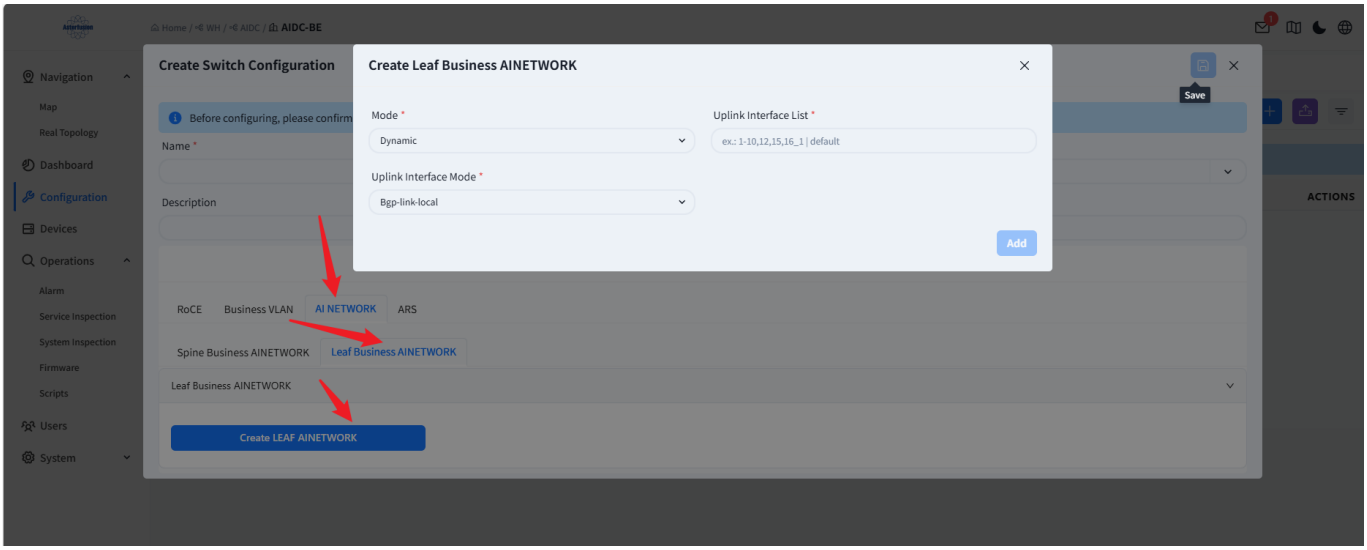


Figure 6.1-29 Configuring Intelligent Routing Function on Leaf Devices

- Mode: Configure the intelligent routing mode of the Leaf device. It can be selected by clicking the drop-down arrow, supporting dynamic mode and static mode. In static mode, VRF is assigned

according to the source IP, service isolation is achieved through VRF, and 1:1 forwarding is achieved according to policy routing; in dynamic mode, VRF is assigned according to the source IP, service isolation is achieved through VRF, and the path weight of the local switch is adjusted through the path quality perceived by the switches in the network, combined with WCMP to achieve more flexible load balancing.

- Uplink Interface List: Configure the intelligent routing upstream link interface, which is generally selected from the interfaces interconnected with Spine.
- Uplink Interface Mode: Configure the intelligent routing upstream interface mode. It can be selected by clicking the drop-down arrow.

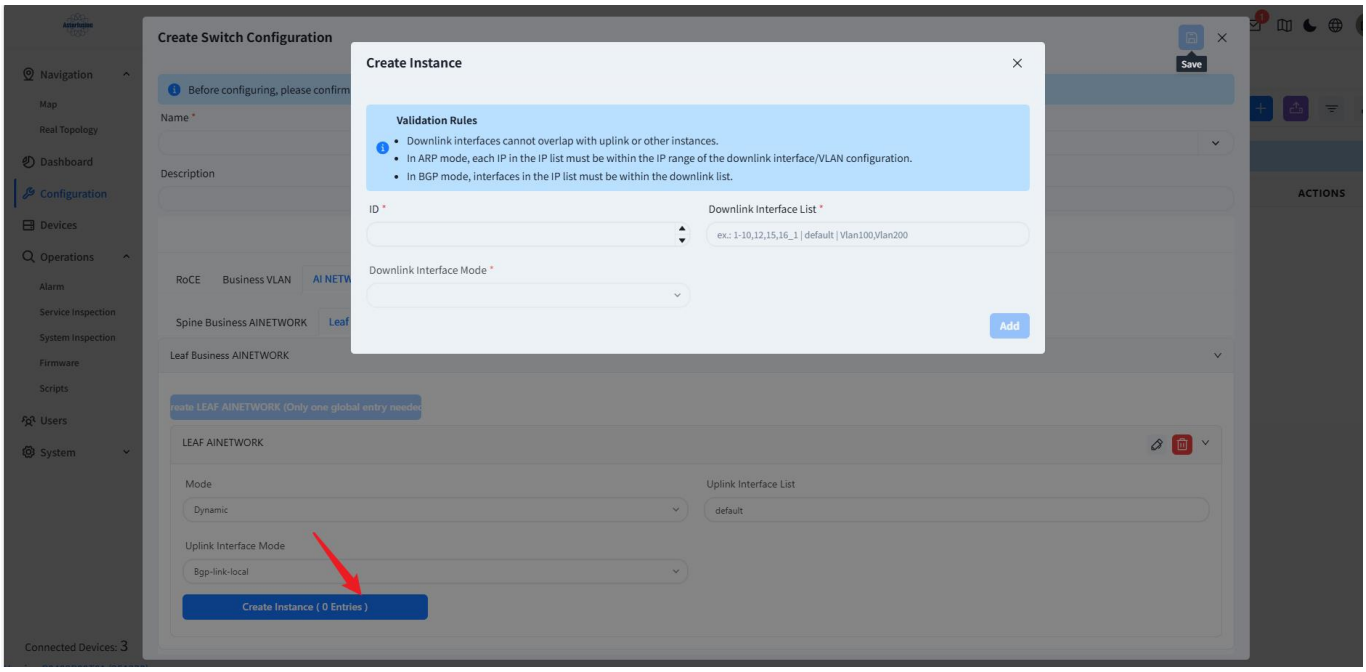


Figure 6.1-30 Configuring Intelligent Routing Instance

- ID: Leaf device intelligent routing instance ID.
- Downlink Interface List: Configure the intelligent routing instance downstream interface list.
- Downlink Interface Mode: Configure the downstream interface mode, which can be selected by clicking the drop-down arrow, Support BGP and ARP mode.
- Downlink IP List: Configure the downstream interface IP address list.

6.1.5.4 ARS Function

Configure the adaptive routing scheduling policy.

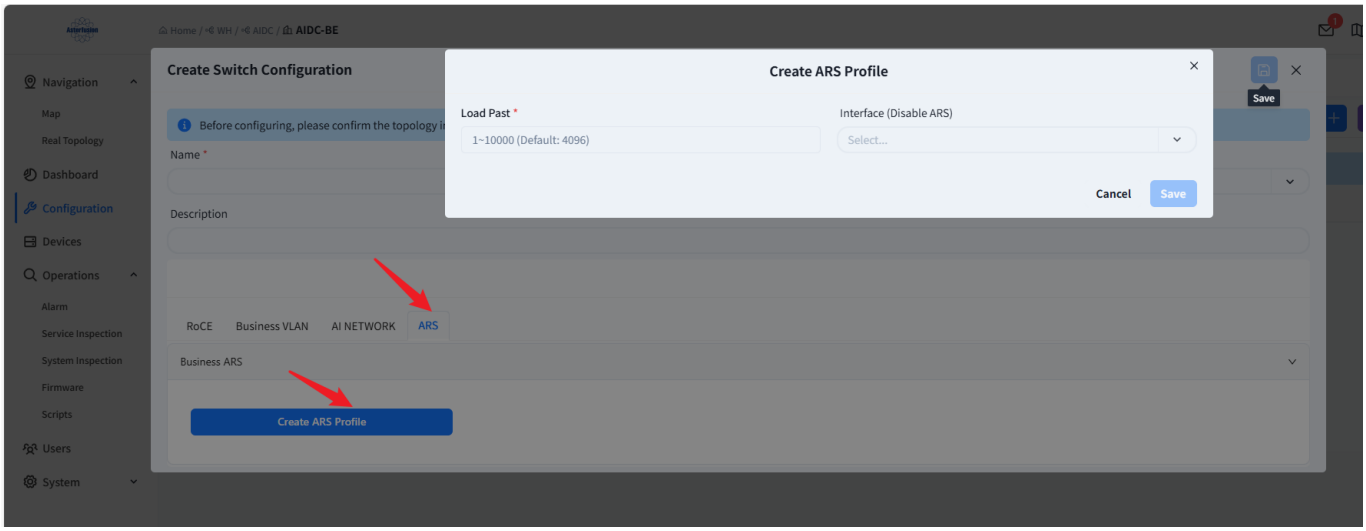


Figure 6.1-31 Configuring ARS Policy

- Load Past: Configure the ARS load past parameter.
- Interfaces: List of interfaces with ARS function disabled.

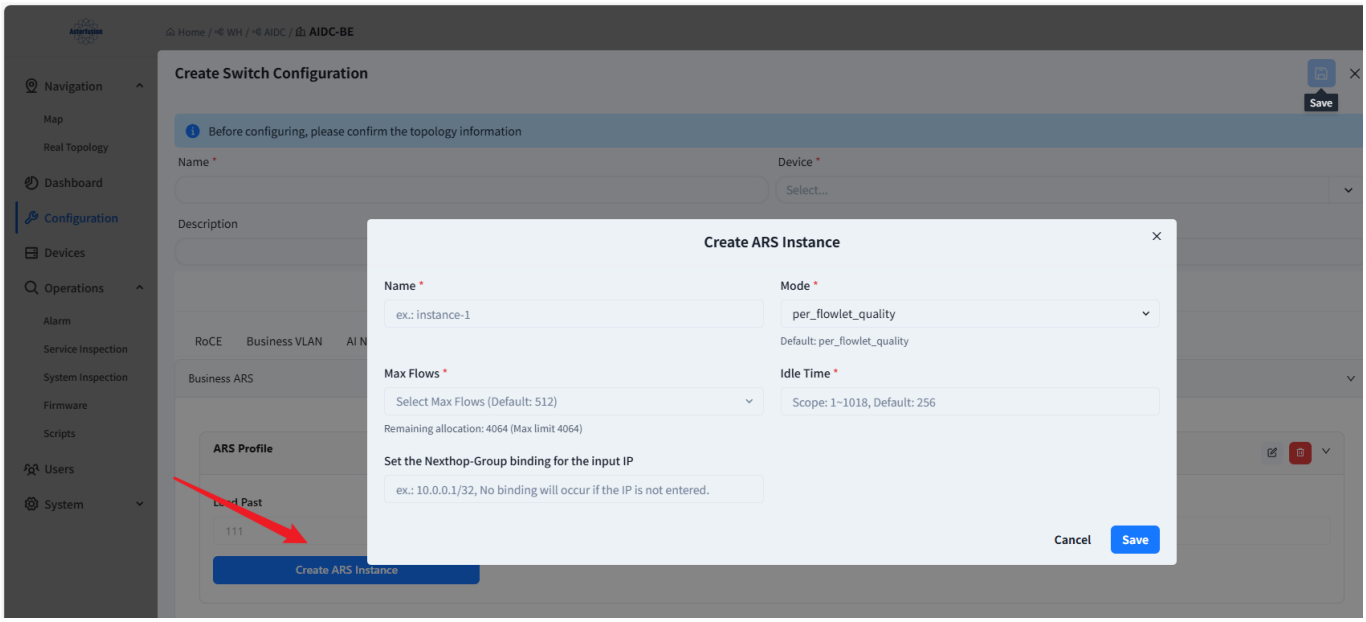


Figure 6.1-32 Configuring ARS Instance

6.1.5.5 Wired Service Configuration Filtering

Click the [**Filter Configuration Templates**] button to filter the configuration templates. After filtering, only the selected configuration templates will be displayed on the page.

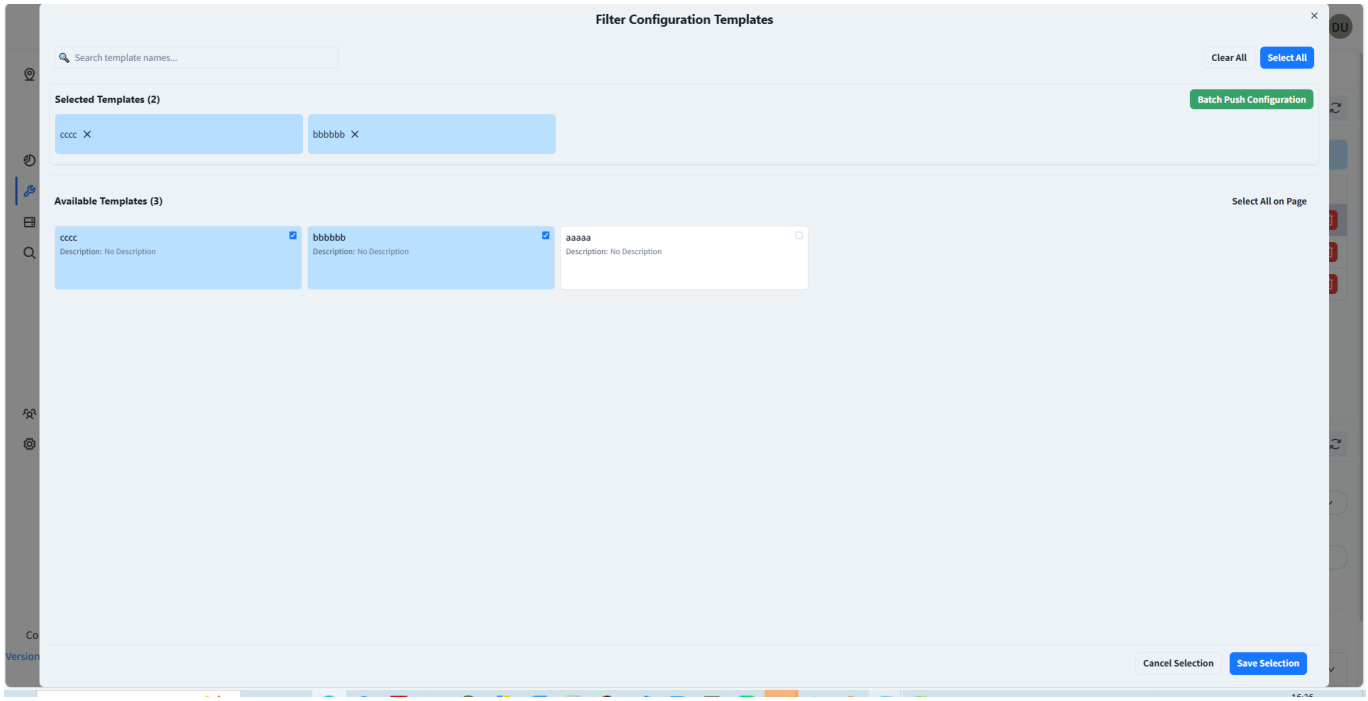


Figure 6.1-33 Wired Service Configuration Filter

6.1.5.6 Batch Import of Wired Service Configuration

Click the [**Import Template**] button to batch import wired service configurations through CSV files to simplify configuration operations.

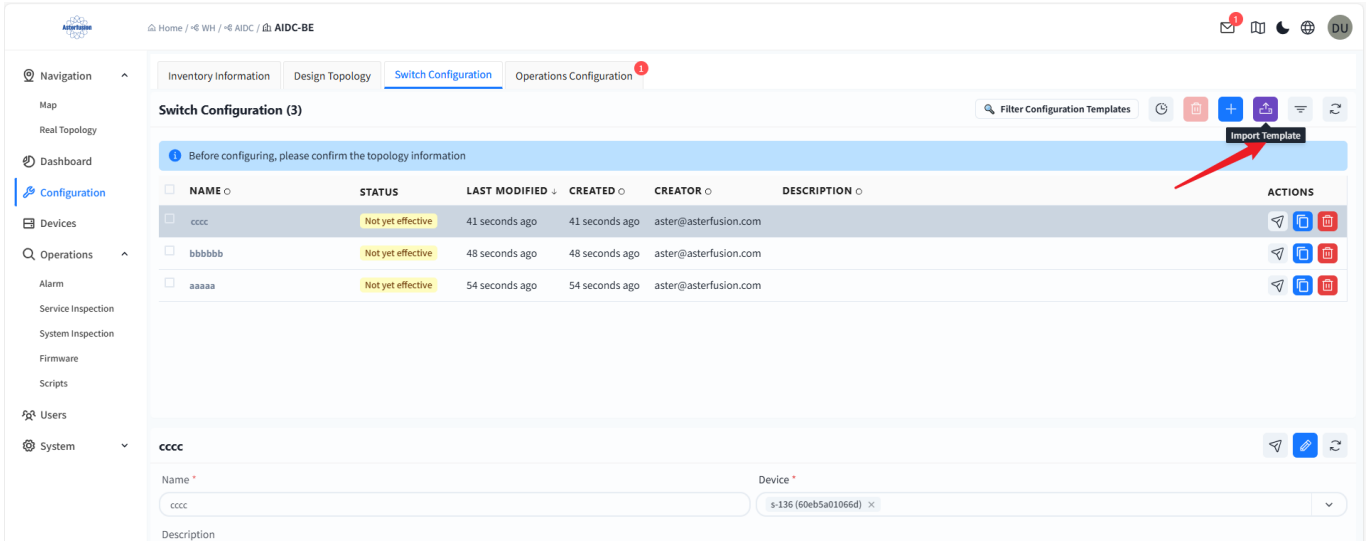


Figure 6.1-34 Wired Service Configuration Import Button

Before importing the CSV file, you can click the [**Download CSV Template**] button to download an example.

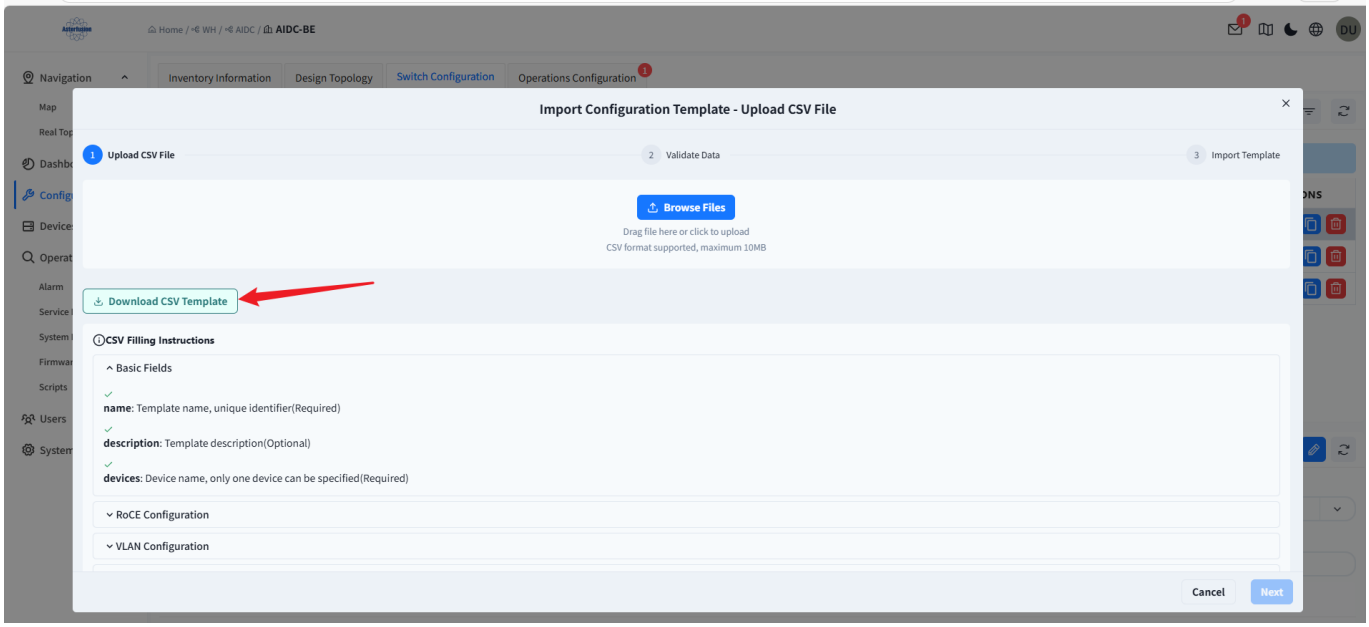


Figure 6.1-35 Wired Service Configuration Import Template Download Button

6.2 AIDC Frontend Network Scenario Deployment

6.2.1 Design Topology

Select the AI data center frontend network scenario, fill in the model and quantity of Spine and Leaf devices, and then click [Complete] to complete the pre-planning of the network topology. The controller will generate a recommended network topology according to the pre-planned typical network topology.

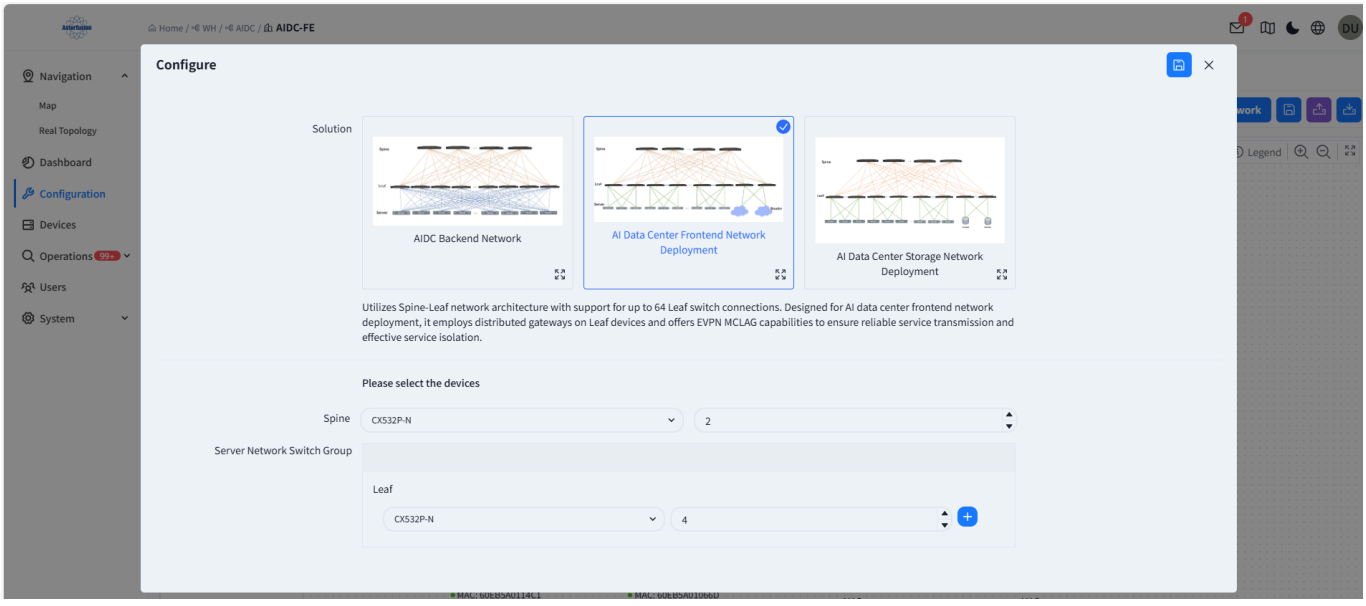


Figure 6.2-1 Switching to Frontend Network Scenario

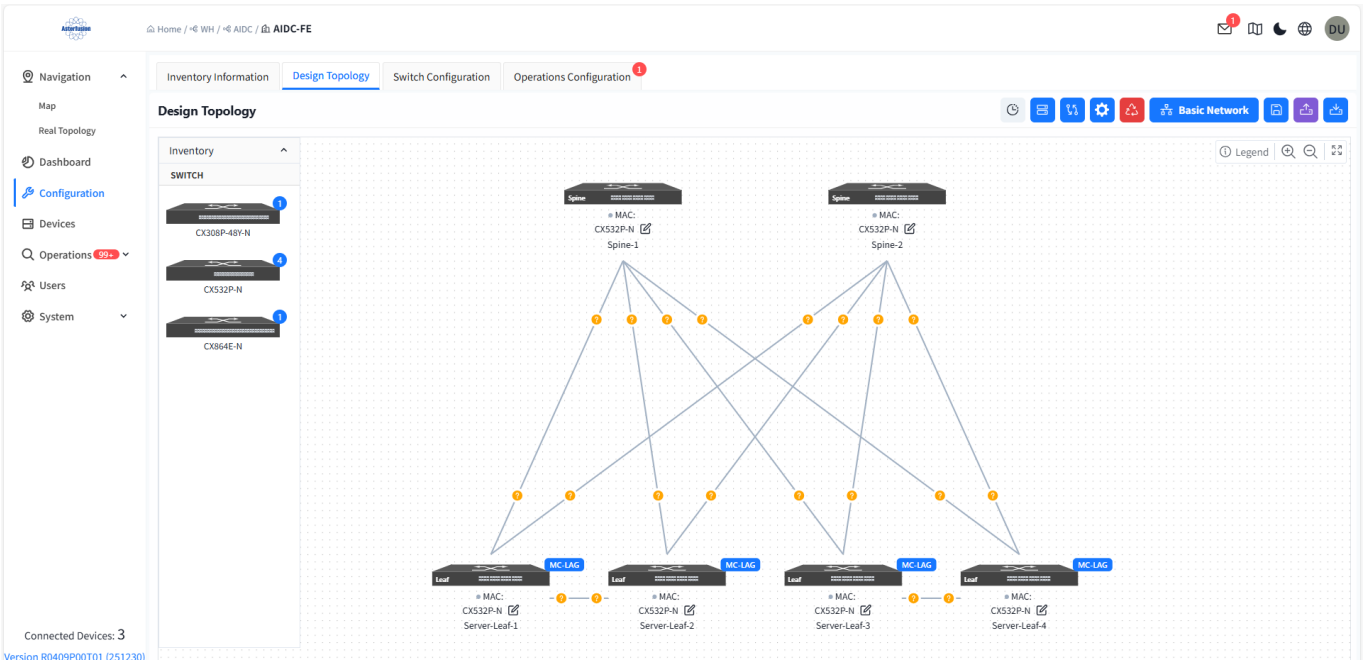


Figure 6.2-2 Frontend Network Scenario Planned Topology

6.2.2 Health Check of Designed Topology Devices

Refer to 6.1.2

6.2.3 Designed Topology Verification

Refer to 6.1.3

6.2.4 Basic Network Configuration

6.2.4.1 Interface IP

Configure device IP address information. It supports configuring physical interfaces, LAG interfaces, and Loopback interfaces.

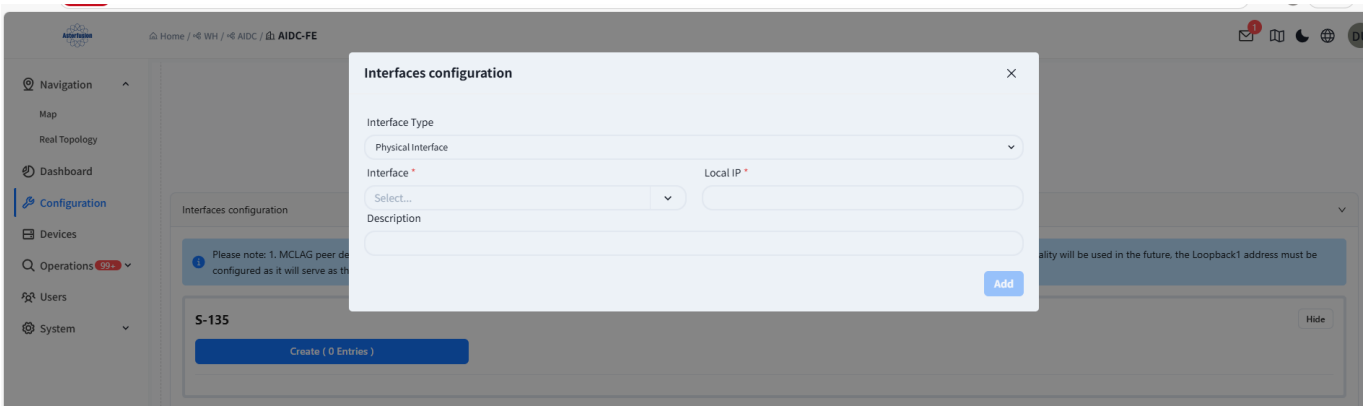


Figure 6.2-3 Configuring Physical Interfaces

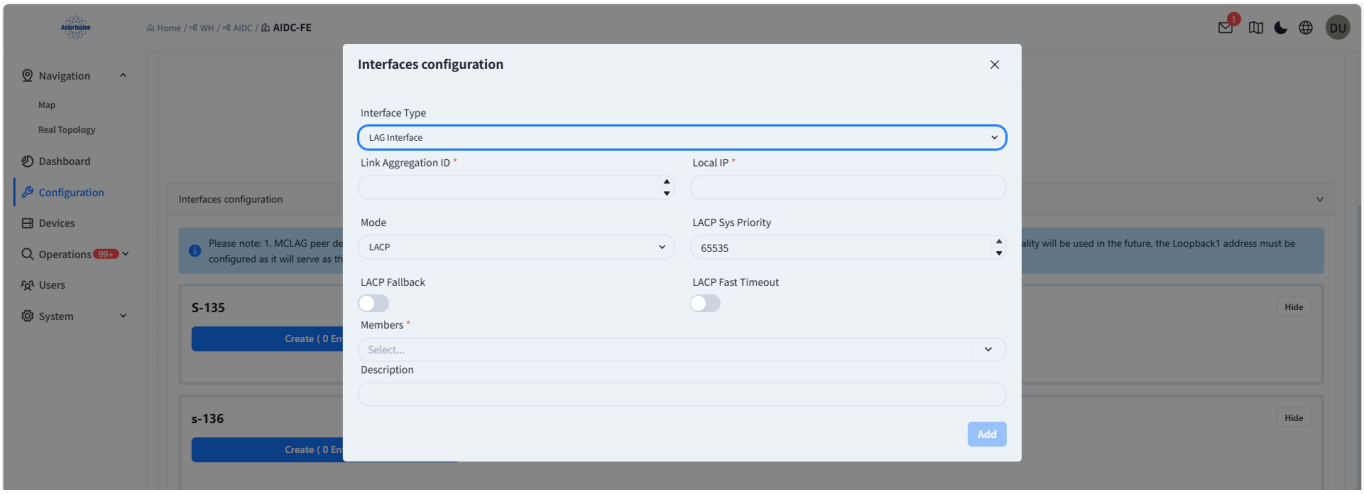


Figure 6.2-4 Configuring Aggregate Interfaces

6.2.4.2 BGP Configuration

Click the [**Next**] button to enter BGP configuration, supporting the configuration of BGP PEER-GROUP, BFD, EVPN, and PEER-IP.

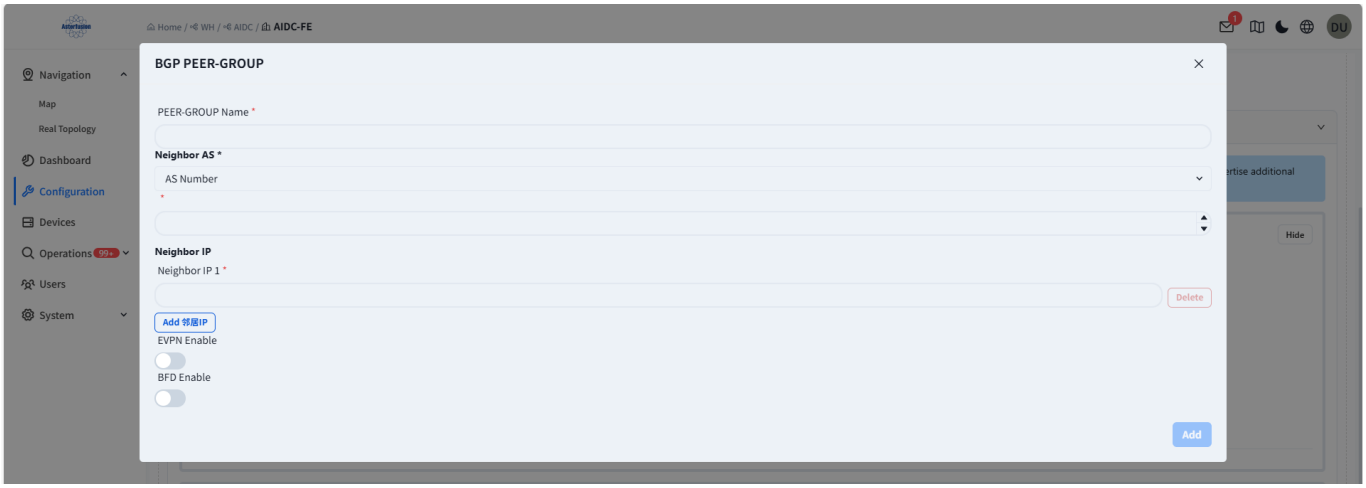


Figure 6.2-5 Configuring BGP

6.2.4.3 MC-LAG Configuration

Create a unified MC-LAG PEER-LINK and DAD-LINK configuration for the LEAF groups in the planned topology.

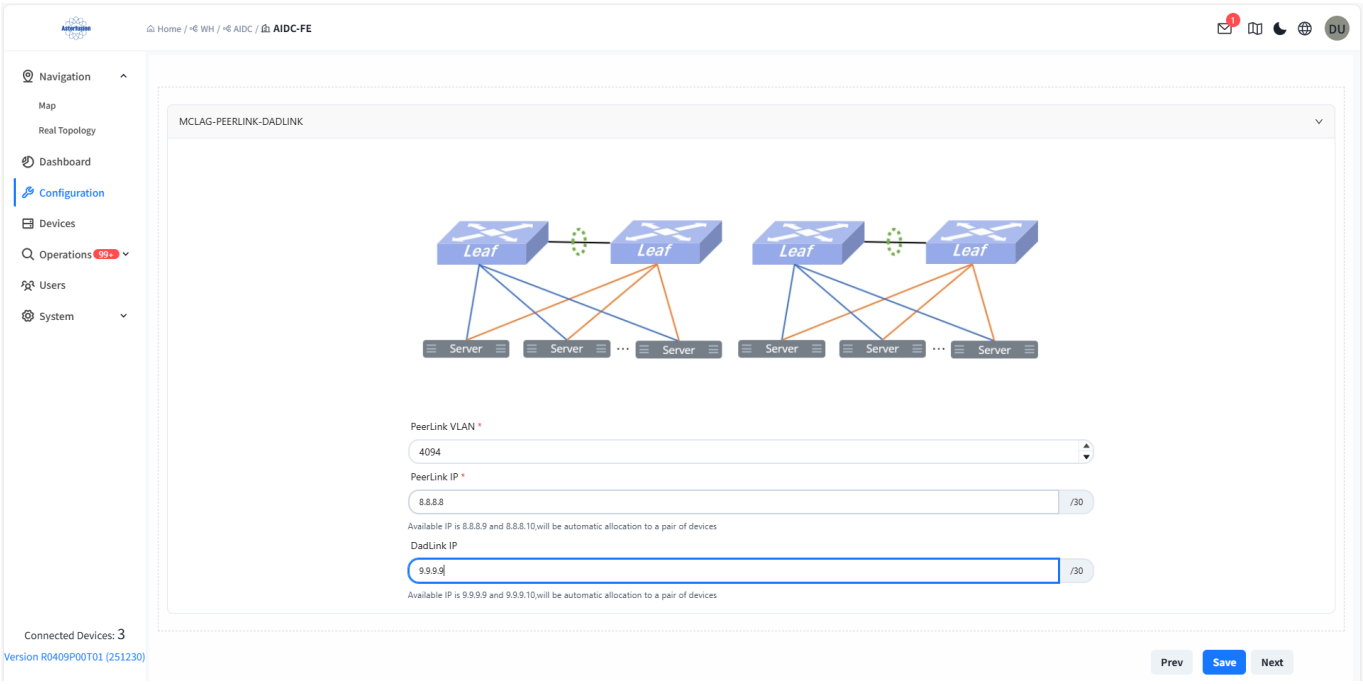


Figure 6.2-6 Configuring MC-LAG

Click the [**Next**] button to complete the configuration, and click the [**Save**] button to save the basic network configuration.

6.2.5 Wired Service Configuration

Click Create Wired Service Configuration to activate the service.

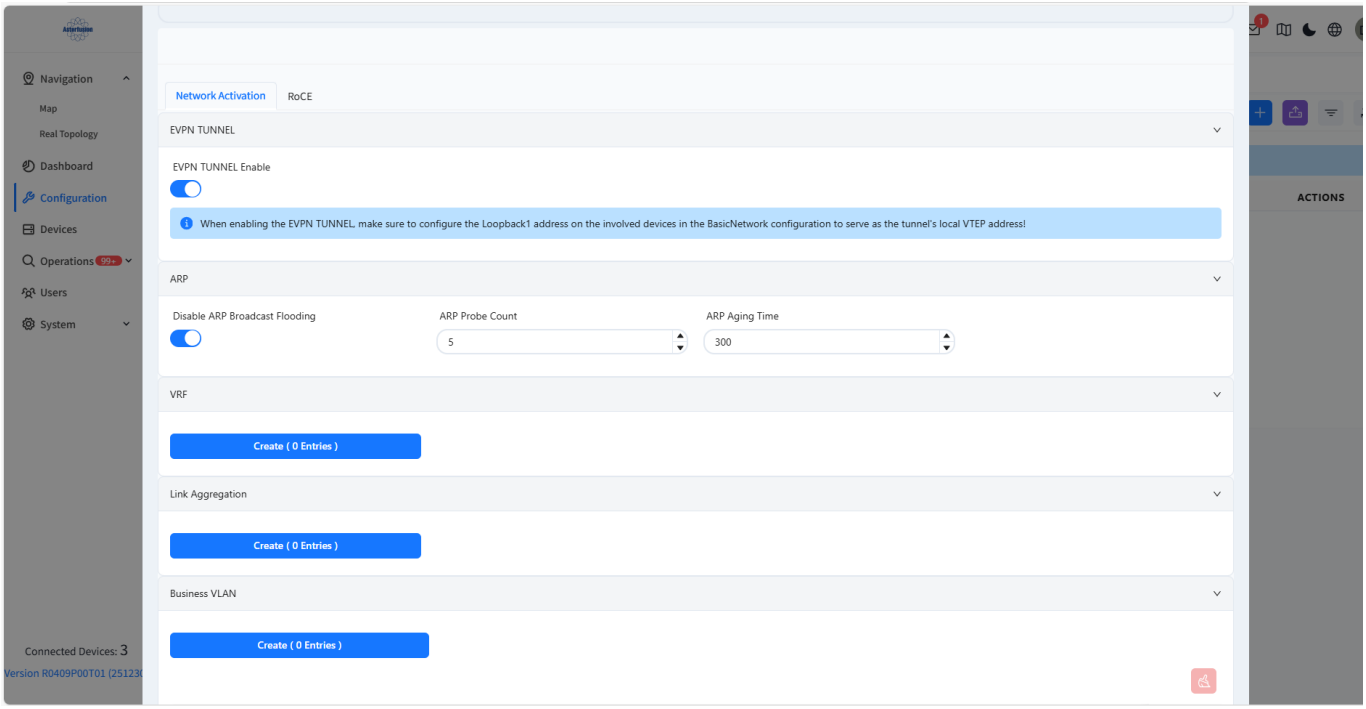


Figure 6.2-7 Configuring Frontend Network Wired Services

6.2.5.1 EVPN Enable Switch

After enabling, the configuration related to the EVPN VXLAN tunnel will be generated.

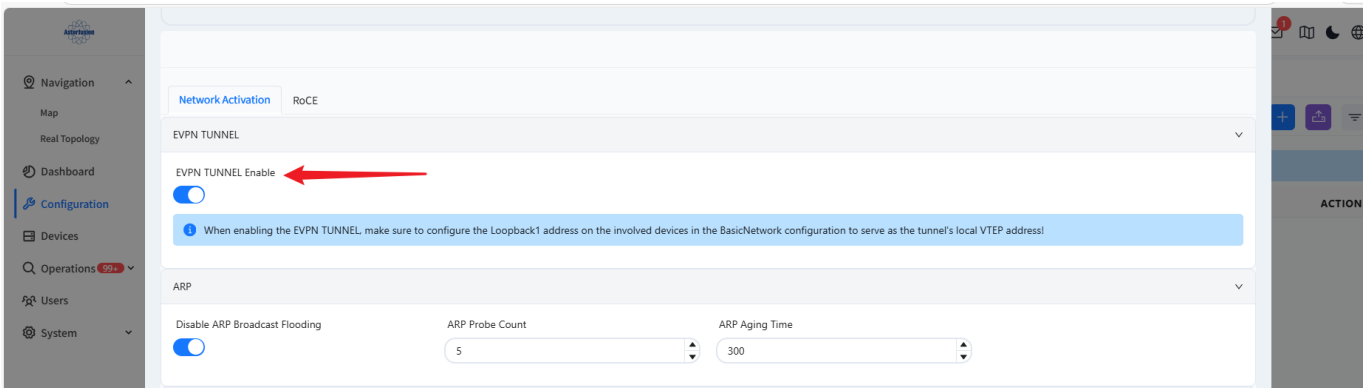


Figure 6.2-8 Configuring EVPN Tunnel Function

6.2.5.2 ARP Configuration

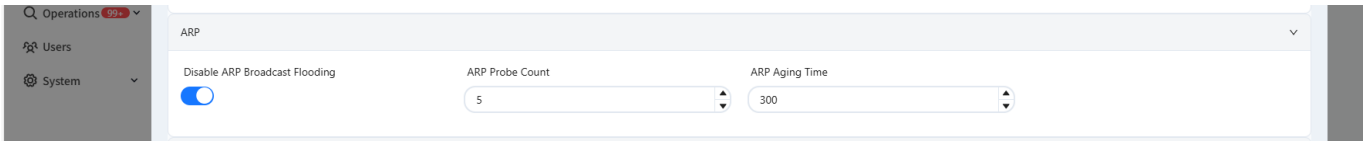


Figure 6.2-9 Configuring ARP

- Disable ARP Broadcast Flooding: When enabled, the device will prohibit ARP broadcast flooding.
- ARP Probe Count: Set the number of ARP Probe detections, the default is 5 times.
- ARP Aging Time: Set the ARP aging time, the default is 300s.

6.2.5.3 VRF Configuration

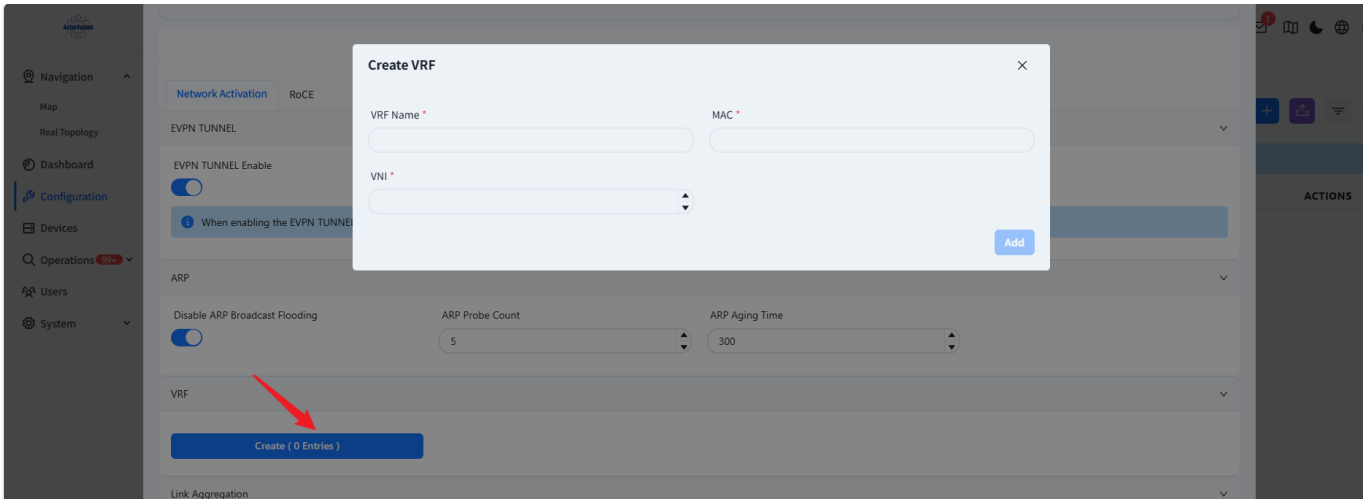


Figure 6.2-10 Configuring VRF

- VRF Name: VRF name, an 11-character string marking a specific VRF.
- MAC: VRF MAC address.

- VNI: The mapping relationship between VRF and VNI, used for the EVPN VXLAN function.

6.2.5.4 Service LAG Configuration

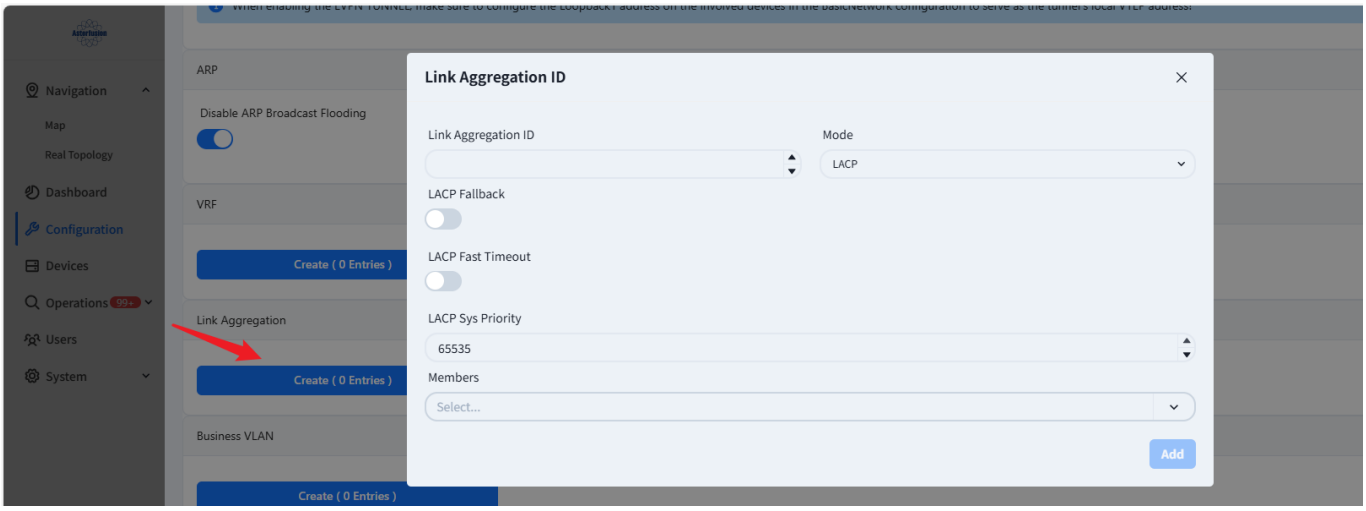


Figure 6.2-11 Configuring Service LAG

- Link Aggregation Group ID: LAG ID name.
- Mode: LAG mode, supporting dynamic and static modes.
- LACP Fallback: By enabling Fallback configuration for LAG, one member port in the LAG group will be set to Active state when no LACP packets are received.
- LACP Fast Timeout: When enabled, LACP will enable fast-rate mode.
- LACP Syst Priority.
- Members: LAG member interfaces.

6.2.5.5 Business VLAN Configuration

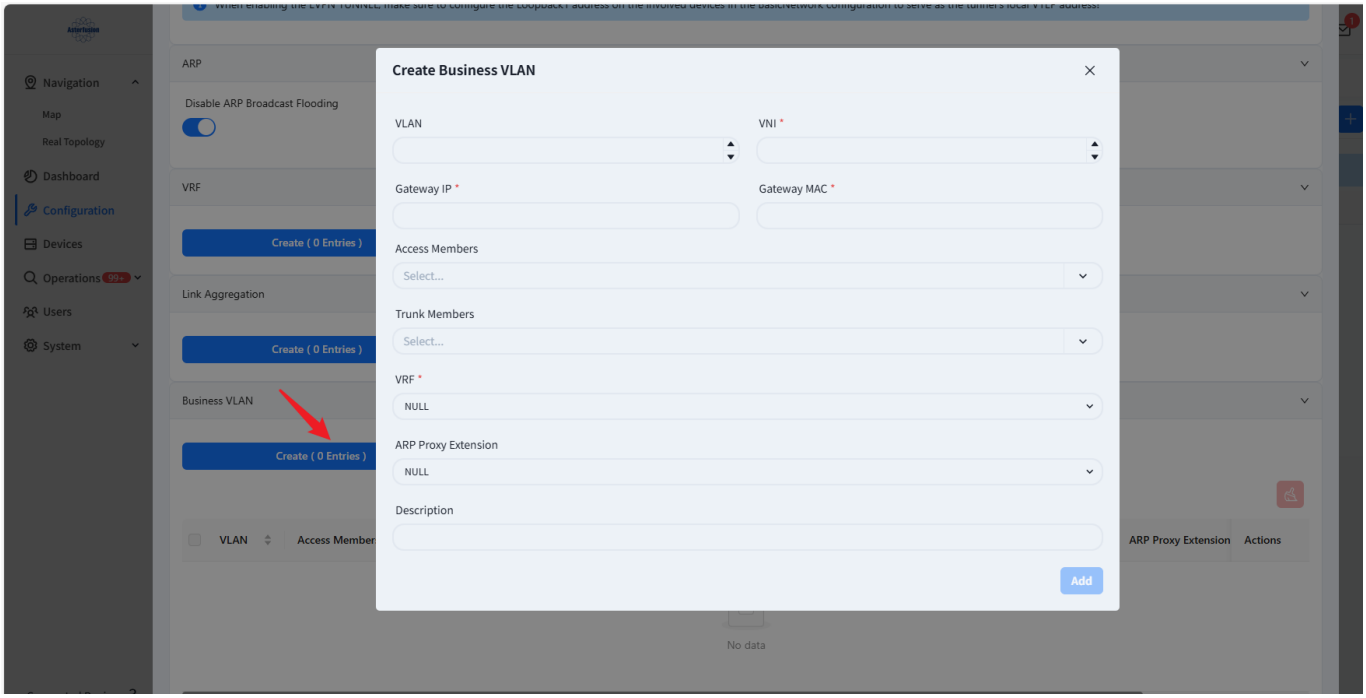


Figure 6.2-12 Configuring Service VLAN

- VLAN: VLAN ID, identifying a unique VLAN.
- VNI: Configure the mapping between VLAN and VNI, used for the EVPN VXLAN function.
- Gateway IP: VLAN IP address.
- Gateway MAC: VLAN MAC address.
- Access Members: Interfaces added to the VLAN in untag mode.
- Trunk Members: Interfaces added to the VLAN in tag mode.
- VRF: The VRF bound to the VLAN interface, used for service isolation.
- ARP Proxy Extension: For silent terminals, ARP proxy extension needs to be configured to support normal ARP interaction.
- Description: VLAN description information.

6.2.5.6 RoCE Configuration

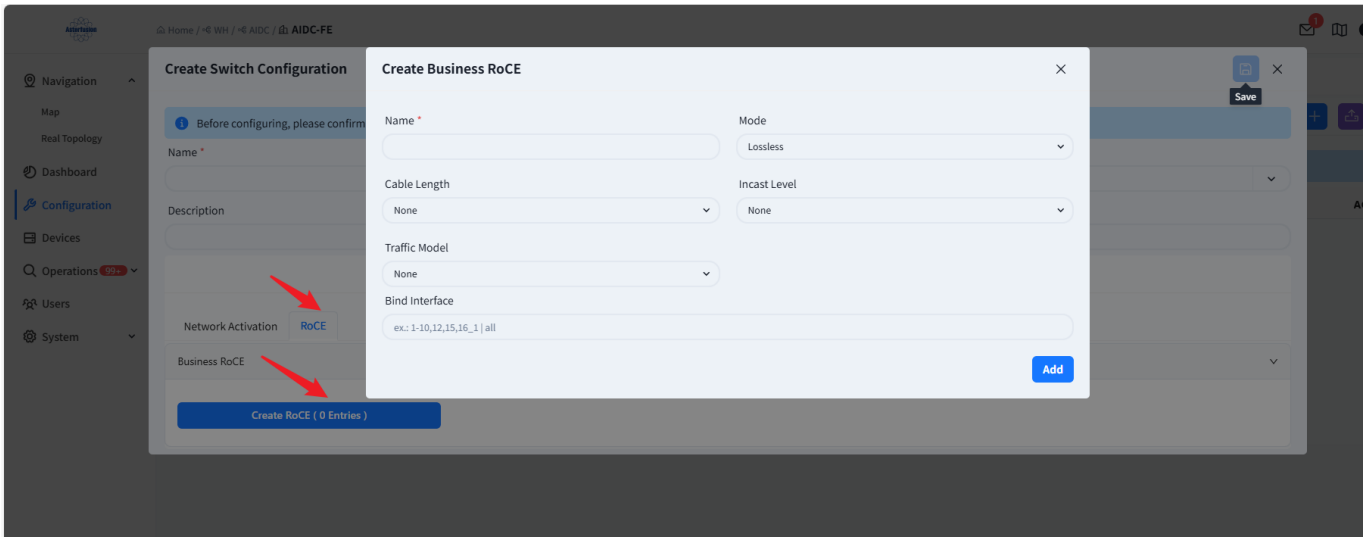


Figure 6.2-13 Configuring RoCE Function

- Name: The policy name of the configured RoCE, uniquely identified.
- Mode: Configure the RoCE policy mode, which can be selected by clicking the drop-down arrow.
- Cable Length: Configure the cable length parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Incast Level: Configure the Incast level parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Transmission Mode: Configure the transmission mode parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Bind Interface: Configure the interfaces to which the RoCE policy is applied.

6.2.5.7 Wired Service Configuration Filtering

Refer to 6.1.5.5

6.2.5.8 Batch Import of Wired Service Configuration

Refer to 6.1.5.6

6.3 AIDC Storage Network Scenario Deployment

6.3.1 Design Topology

Select the AI data center storage network scenario, fill in the model and quantity of Spine and Leaf devices, and then click [Complete] to complete the pre-planning of the network topology. The controller will generate a recommended network topology according to the pre-planned typical network topology.

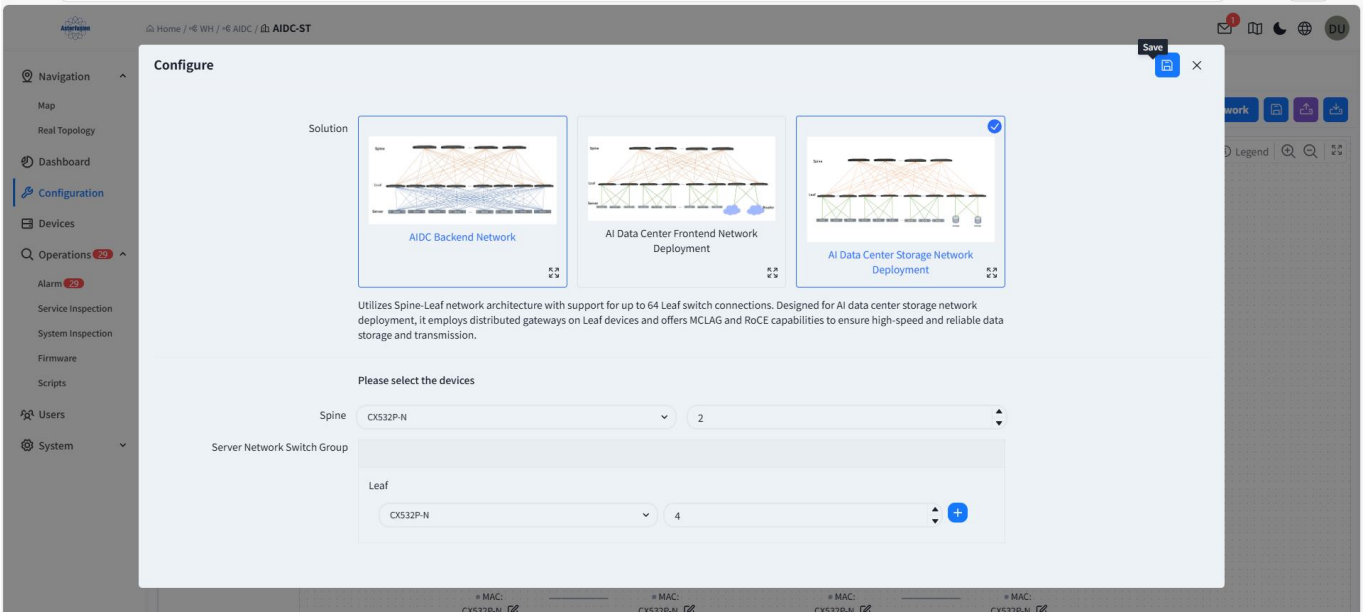


Figure 6.3-1 Switching to Storage Network Scenario

6.3.2 Health Check of Designed Topology Devices

Refer to 6.1.2

6.3.3 Designed Topology Verification

Refer to 6.1.3

6.3.4 Basic Network Configuration

6.3.4.1 Interface IP

Configure device IP address information. It supports configuring physical interfaces and LAG interfaces.

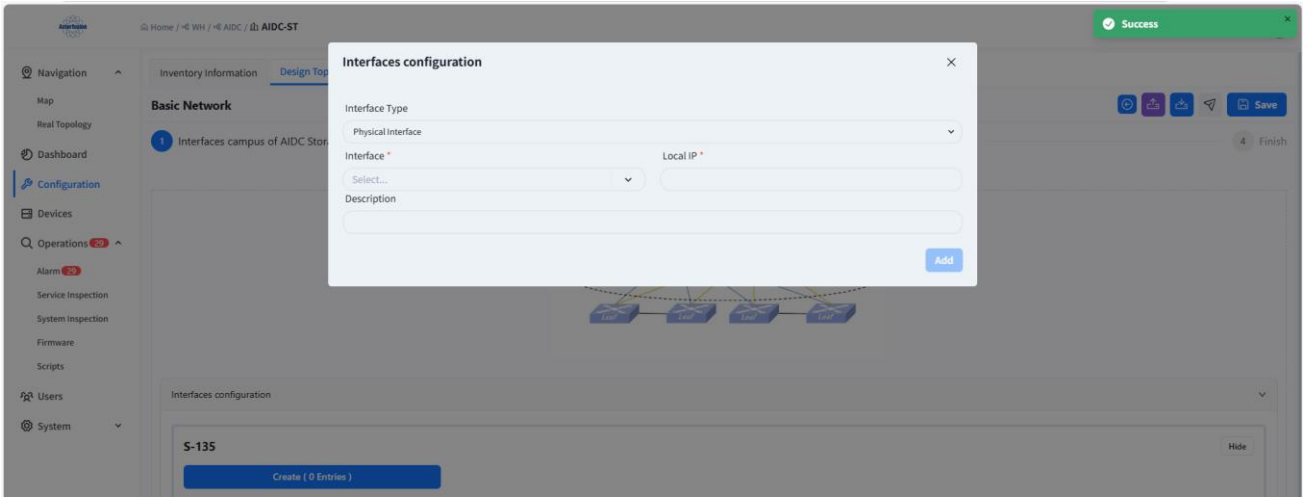


Figure 6.3-2 Configuring Physical Interfaces

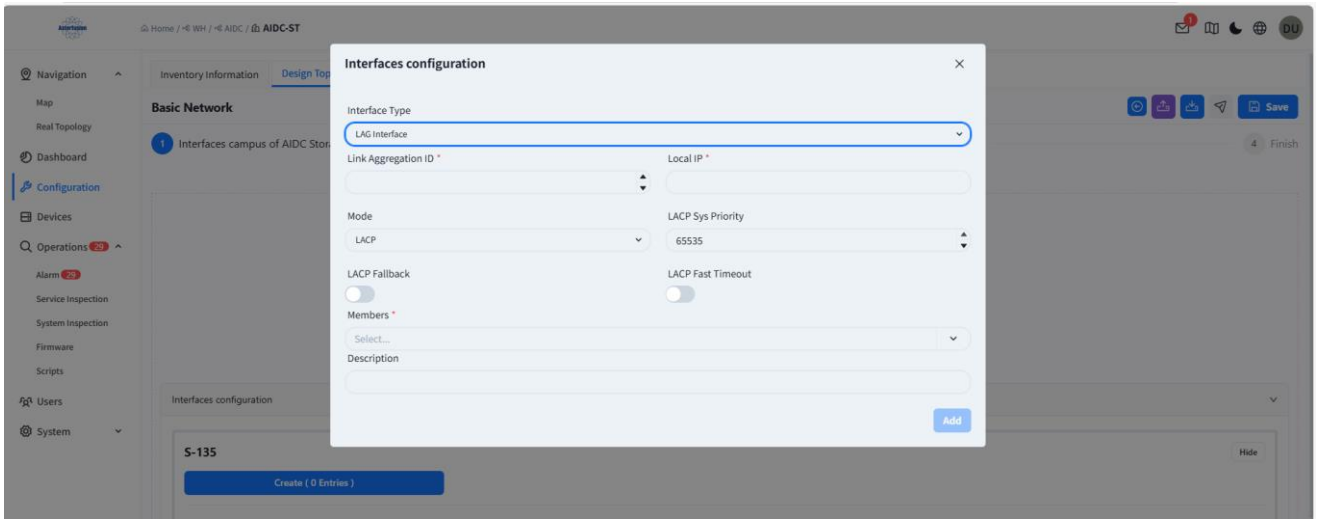


Figure 6.3-3 Configuring Aggregate Interfaces

6.3.4.2 BGP Configuration

Click the [**Next**] button to enter BGP configuration, supporting the configuration of BGP PEER-GROUP, BFD, and PEER-IP.

Figure 6.3-4 Configuring BGP

6.3.4.3 MC-LAG Configuration

Create a unified MC-LAG PEER-LINK and DAD-LINK configuration for the LEAF groups in the planned topology.

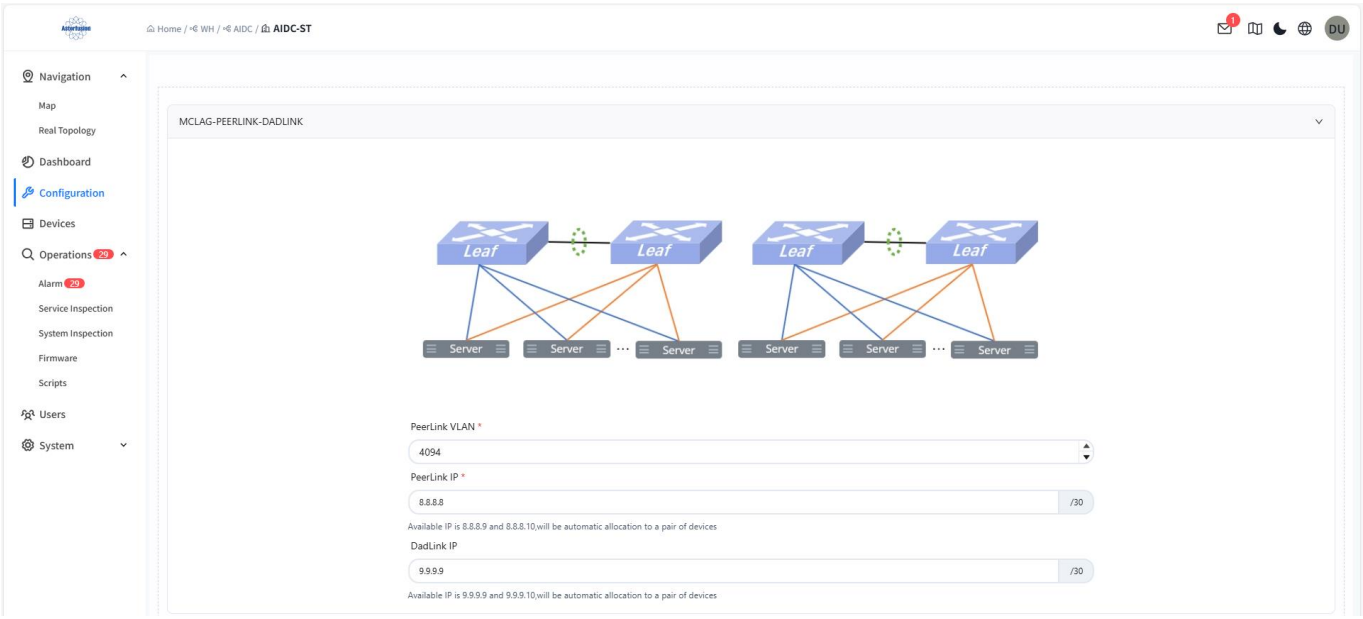


Figure 6.3-5 Configuring MC-LAG

Click the [**Next**] button to complete the configuration, and click the [**Save**] button to save the basic network configuration.

6.3.5 Wired Service Configuration

Click Create Wired Service Configuration to activate the service.

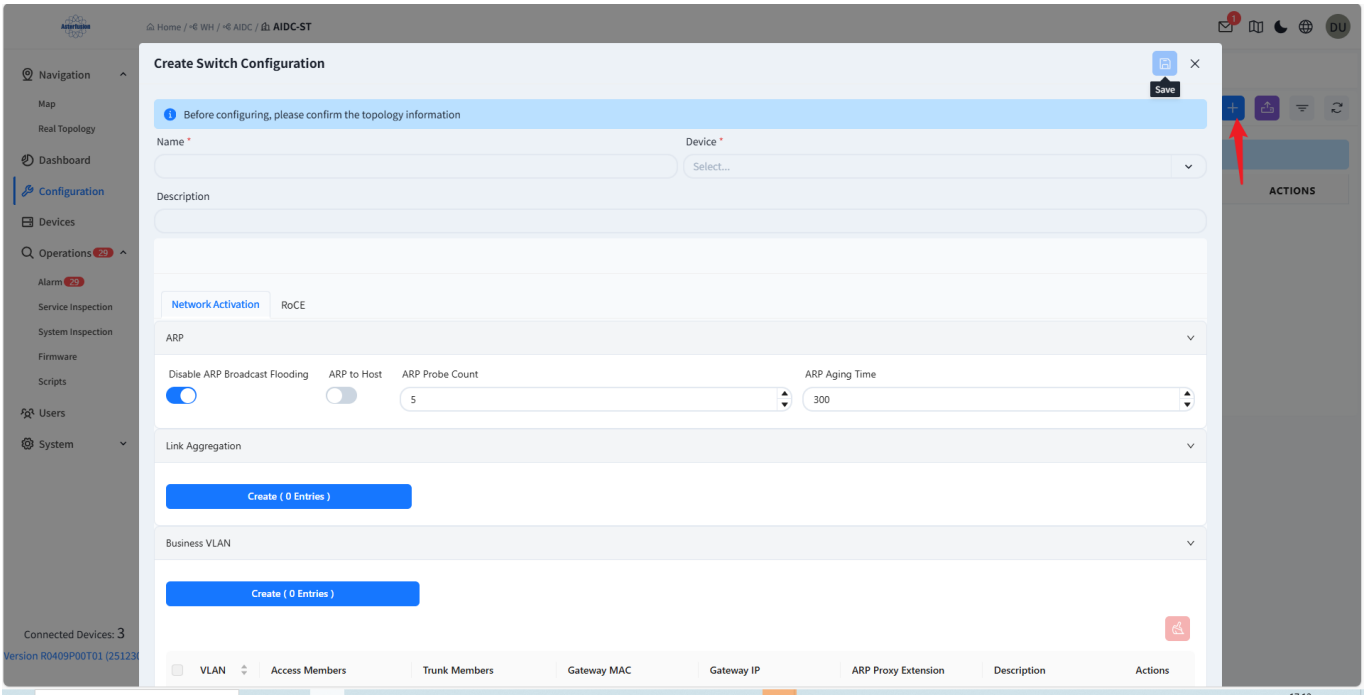


Figure 6.3-6 Configuring Storage Network Wired Services

6.3.5.1 ARP Configuration

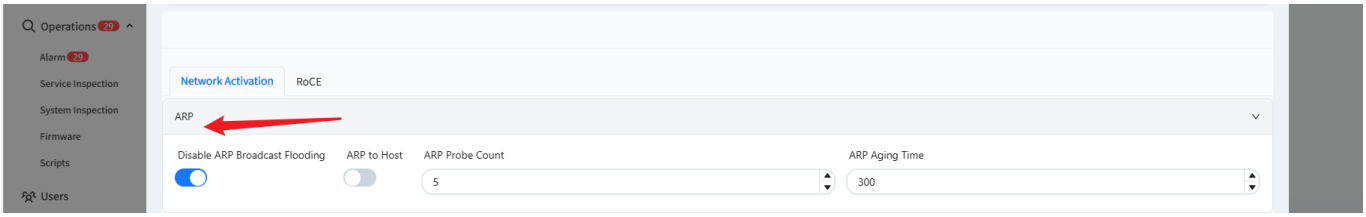


Figure 6.3-7 Configuring ARP

- Disable ARP Broadcast Flooding: When enabled, the device will prohibit ARP broadcast flooding.
- ARP to Host Routing Function: After enabling, ARP will be converted to host routing and then advertised through BGP.
- ARP Probe Count: Set the number of ARP Probe detections, the default is 5 times.
- ARP Aging Time: Set the ARP aging time, the default is 300s.

6.3.5.2 Service LAG Configuration

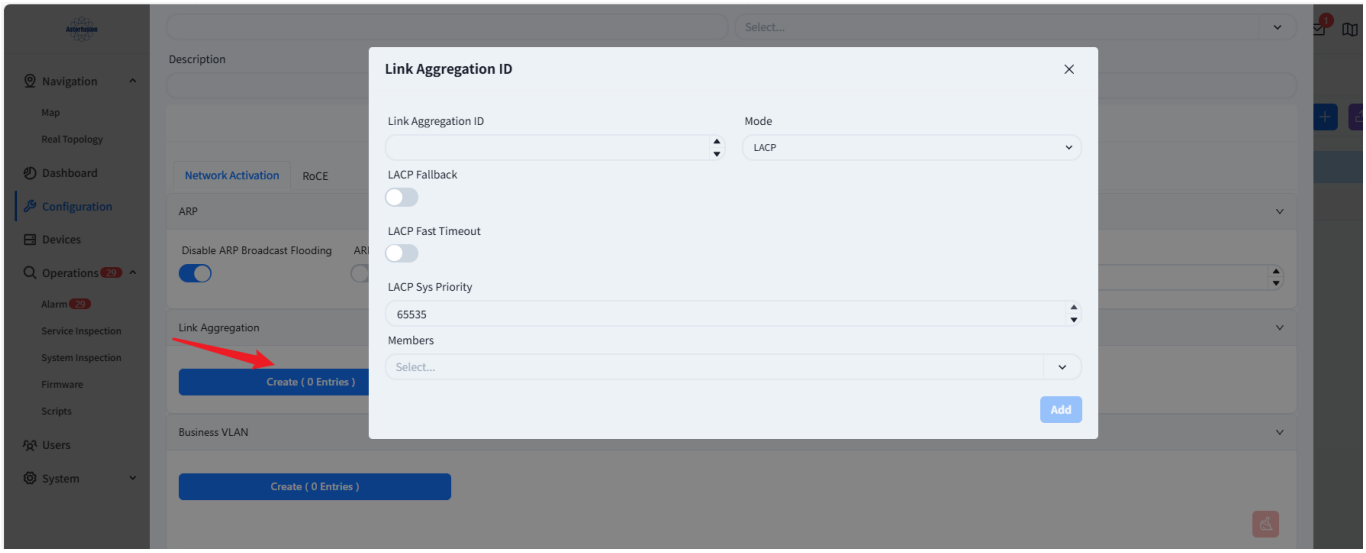


Figure 6.3-8 Configuring Service LAG

- Link Aggregation Group ID: LAG ID name.
- Mode: LAG mode, supporting dynamic and static modes.
- LACP Fallback: By enabling Fallback configuration for LAG, one member port in the LAG group will be set to Active state when no LACP packets are received.
- LACP Fast Timeout: When enabled, LACP will enable fast-rate mode.
- LACP Sys Priority.
- Member Interfaces: LAG member interfaces.

6.3.5.3 Business VLAN Configuration

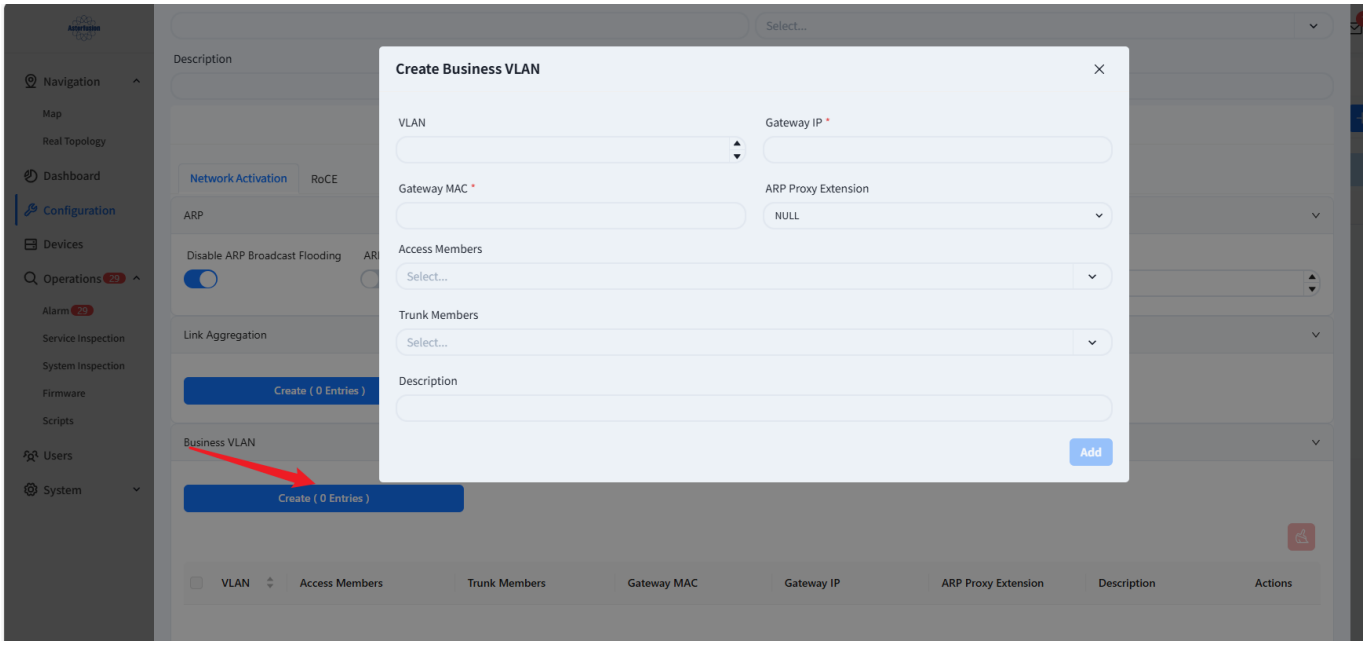


Figure 6.3-9 Configuring Service VLAN

- VLAN: VLAN ID, identifying a unique VLAN.
- Gateway IP: VLAN IP address.
- Gateway MAC: VLAN MAC address.
- Access Members: Interfaces added to the VLAN in untag mode.
- Trunk Members: Interfaces added to the VLAN in tag mode.
- ARP Proxy Extension: For silent terminals, ARP proxy extension needs to be configured to support normal ARP interaction.
- Description: VLAN description information.

6.3.5.4 RoCE Configuration

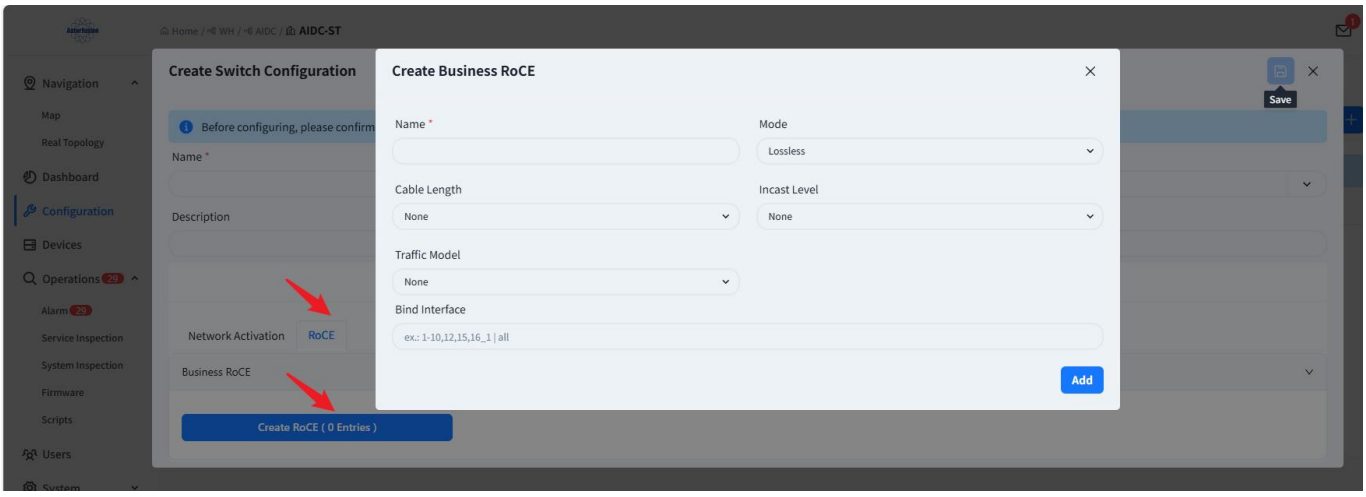


Figure 6.3-10 Configuring RoCE Function

- Name: The policy name of the configured RoCE, uniquely identified.

- Mode: Configure the RoCE policy mode, which can be selected by clicking the drop-down arrow.
- Cable Length: Configure the cable length parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Incast Level: Configure the Incast level parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Transmission Mode: Configure the transmission mode parameter of the RoCE policy, which can be selected by clicking the drop-down arrow.
- Bound Interfaces: Configure the interfaces to which the RoCE policy is applied.

6.3.5.5 Wired Service Configuration Filtering

Refer to 6.1.5.5

6.3.5.6 Batch Import of Wired Service Configuration

Refer to 6.1.5.6

6.4 Configuration Delivery

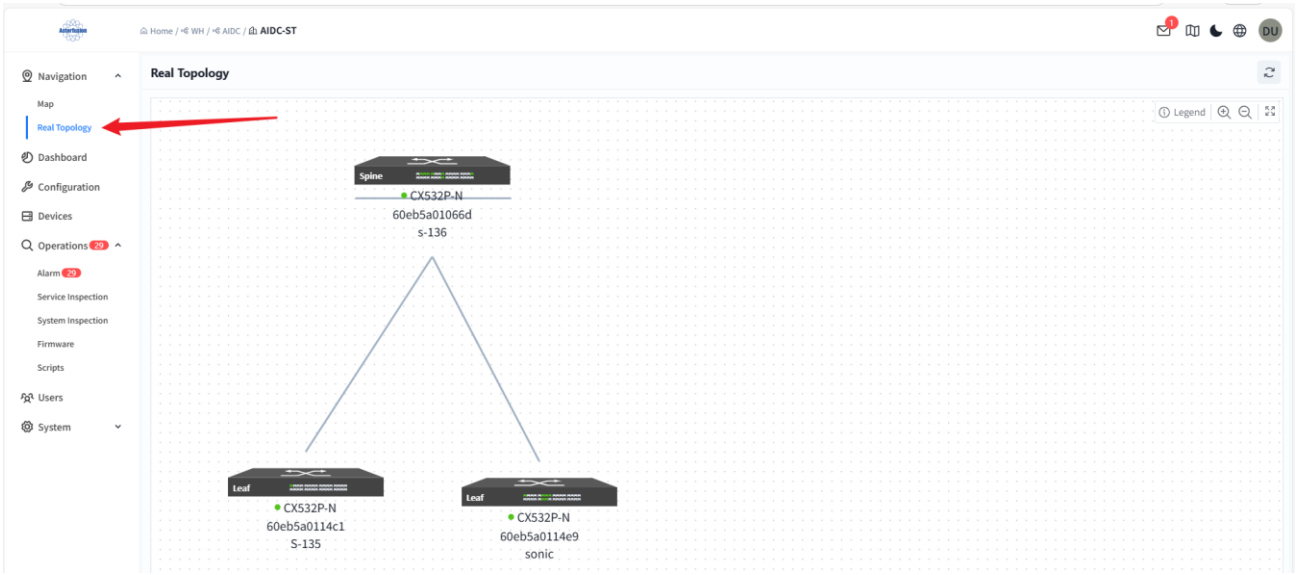


Figure 6.4-1 Viewing Actual Topology

When all switches can be connected to the controller, click [**Real Topology**] to confirm whether the generated topology is consistent with the planned topology. After confirmation, the controller can deliver configurations to the switches:

1. Click [**Configuration**] - [**Design Topology**] - [**Basic Network Configuration**] to enter the basic network configuration view, and click the [**Push Configuration**] button in the upper right corner.

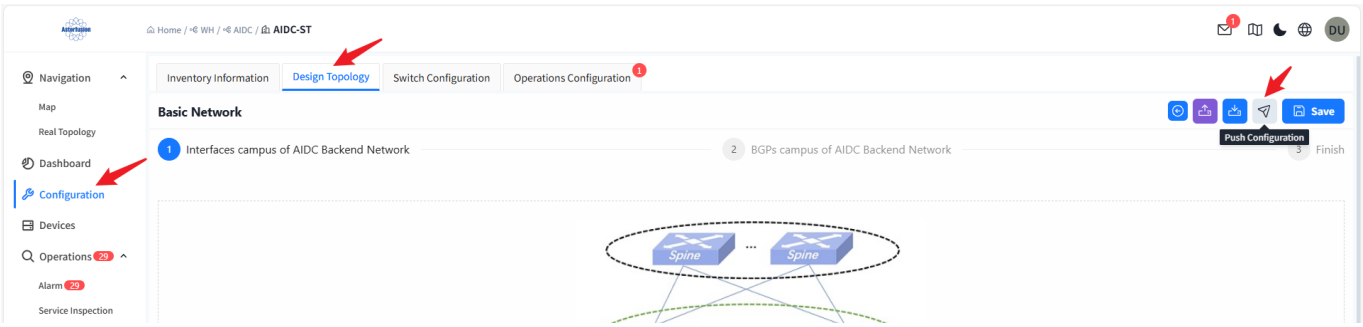


Figure 6.4-2 Deploying Basic Network Configuration

By default, the controller will select all switches. Click [**Next**] - [**Start**] to start delivering the basic network configuration to the switches.

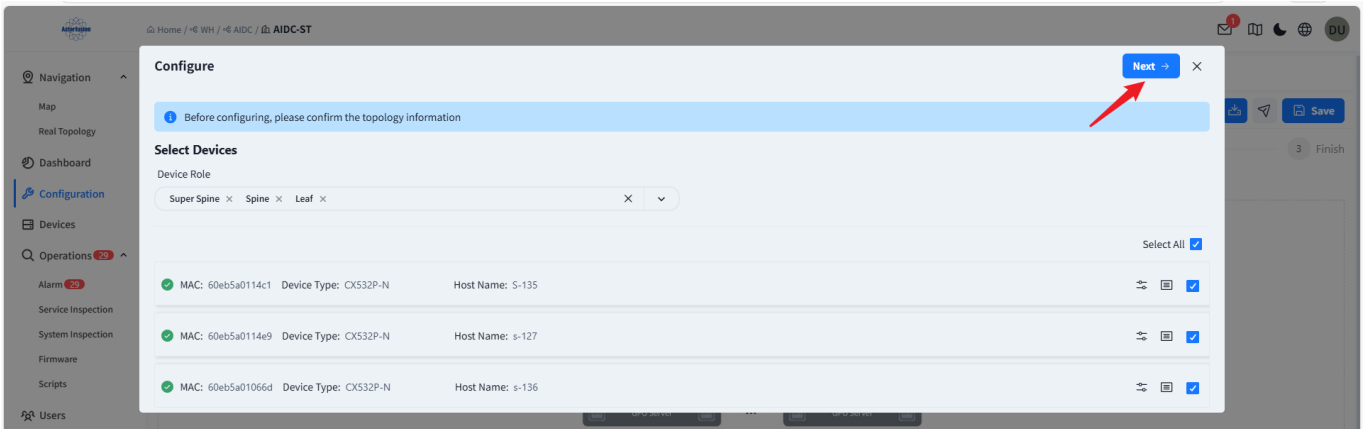


Figure 6.4-3 Selecting Devices and Pushing Configuration

2. In the [**Configuration**] - [**Switch Configuration**] page, select the configuration to be delivered and click the [**Push Configuration**] button:

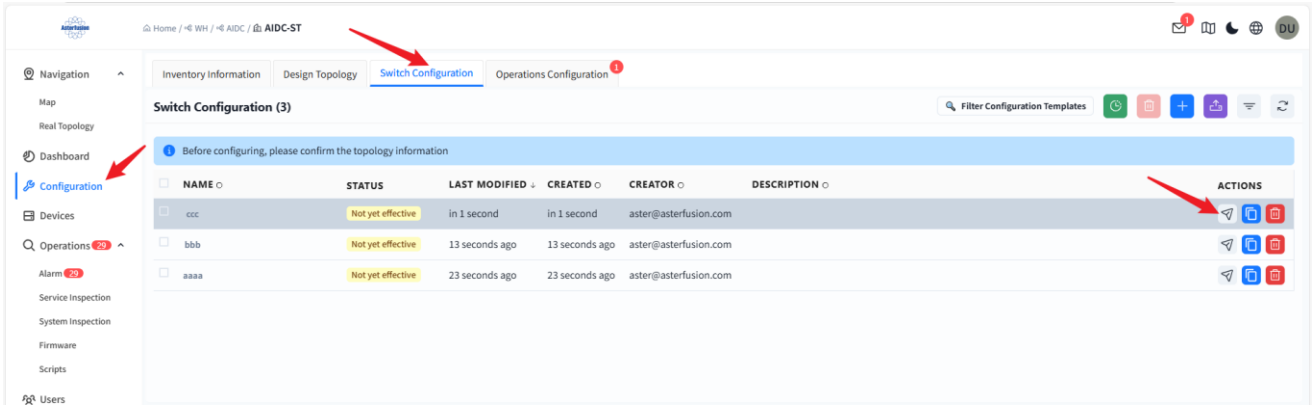


Figure 6.4-4 Deploying Wired Service Configuration

In the pop-up interface, click [**Next**] - [**Start**] to deliver the service configuration to the switches:

Figure 6.4-5 Selecting Devices and Pushing Configuration

Or first enter the filtering page through the Filter Configuration Template button, select multiple wired service configurations for batch push.

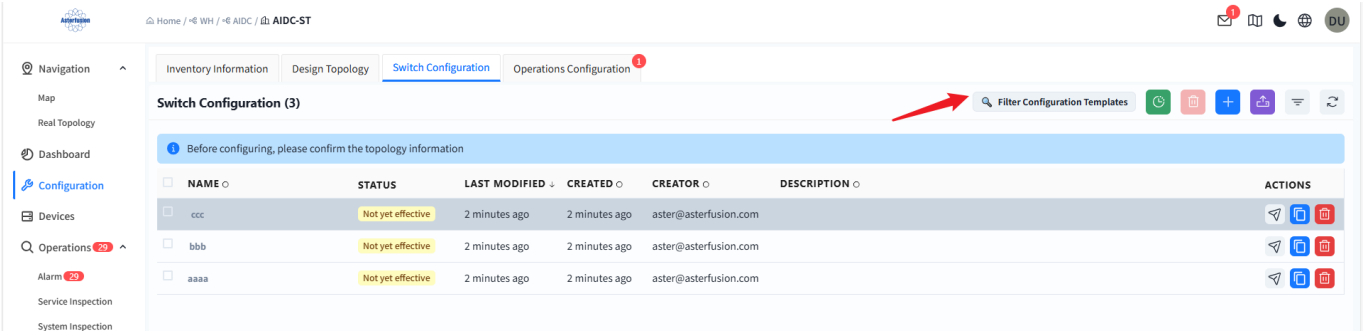


Figure 6.4-6 Batch Deployment of Wired Service Configuration

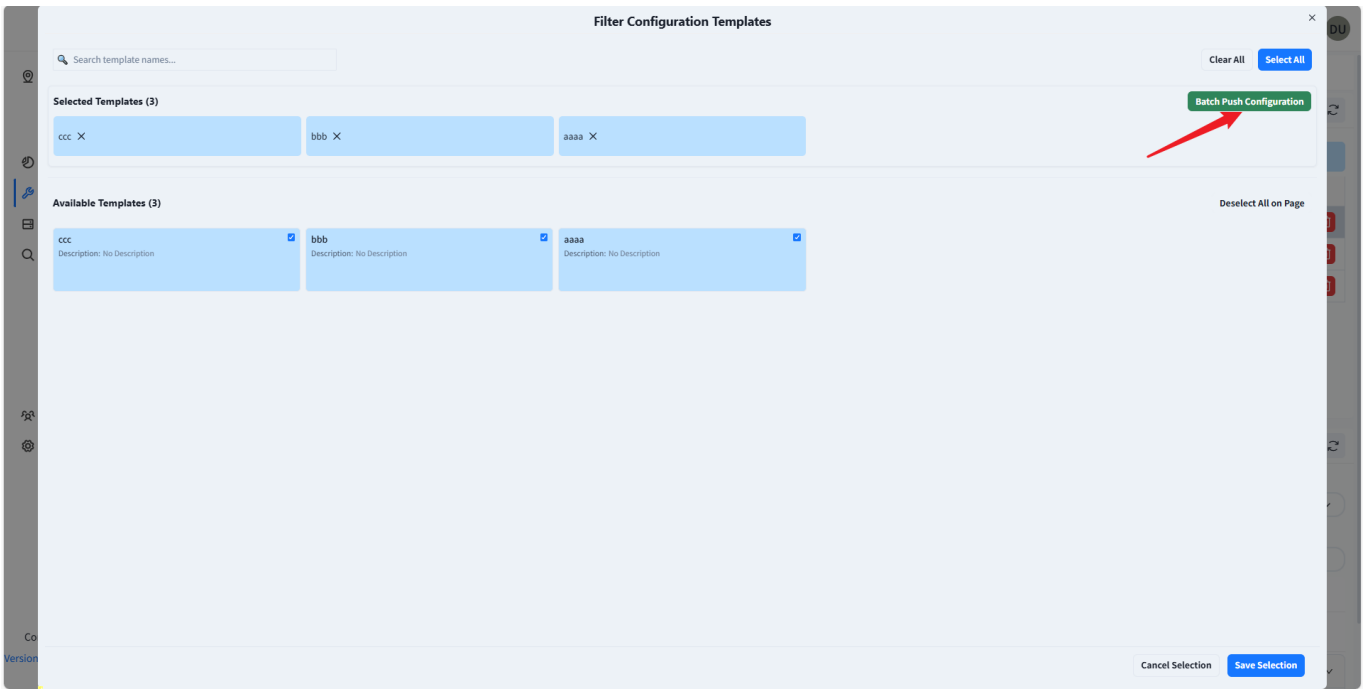


Figure 6.4-7 Batch Deployment Page

In the pop-up interface, click [**Next**] - [**Start**] to batch deliver service configurations to multiple switches.

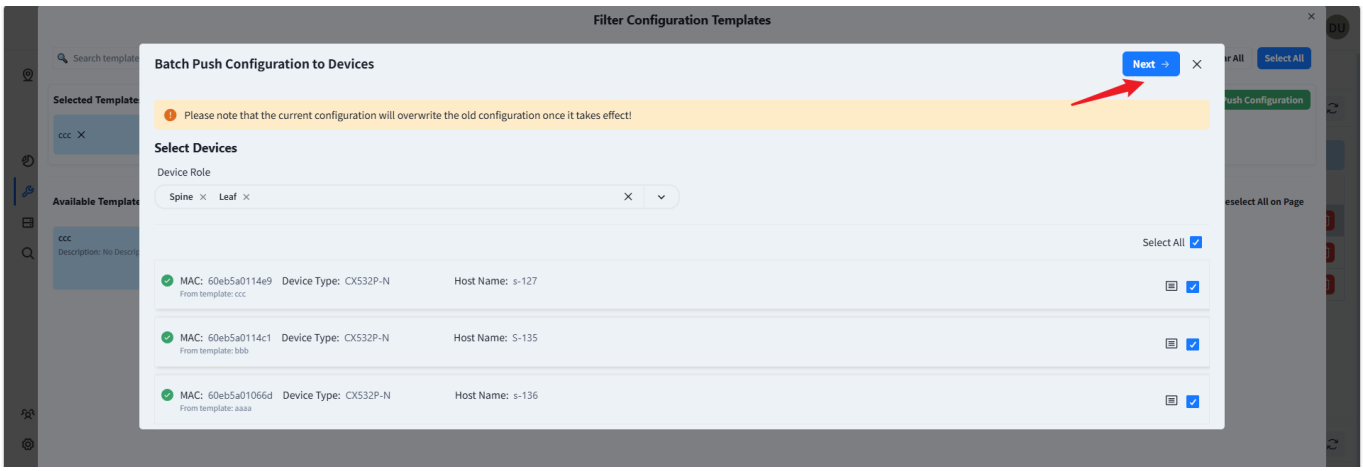


Figure 6.4-8 Executing Batch Deployment Task

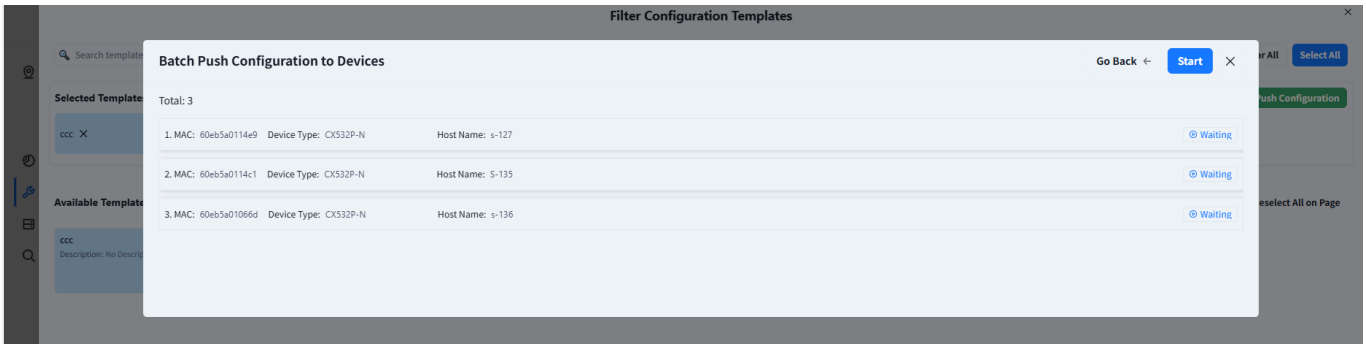


Figure 6.4-9 Starting Batch Deployment Task

7 Status Visualization

The controller has powerful device status monitoring functions and can monitor the working status of switches in real time. Through detailed dashboard displays, administrators can grasp the operation status of devices at any time. Based on the obtained monitoring information, the controller comprehensively evaluates various indicators and intelligently calculates the health value of each device. The evaluation of the health value mainly considers the following factors:

- Resource Utilization: Evaluate the use of device resources based on memory and CPU utilization to determine if there is a risk of resource exhaustion.
- Traffic Load: Analyze the load status of the device based on traffic statistics to determine if there is a traffic bottleneck.
- Hardware Status: Monitor the temperature of various components of the device, the operation status of hardware such as power supplies, fans, and optical modules, and check if they are within the expected range.
- Operation Status: Real-time detection of the operation status of various main processes and containers of the device.

When the monitoring indicators exceed the preset threshold, the controller will automatically generate alarm information to notify the administrator, ensuring that the administrator can promptly discover and solve problems, and ensuring the efficient, safe, and stable operation of the network.

7.1 Overall Network Status Visualization

The controller supports full calculation of the monitoring data of all online devices, and finally presents it through a comprehensive health value.

7.1.1.1 Organization Dashboard

Administrators can enter a specific organization in the [**Navigation**] interface to view the overview of the status of devices and terminals under all venues within the organization, and support clicking to jump to the selected terminal. Users can adjust the display cards according to their own preferences.

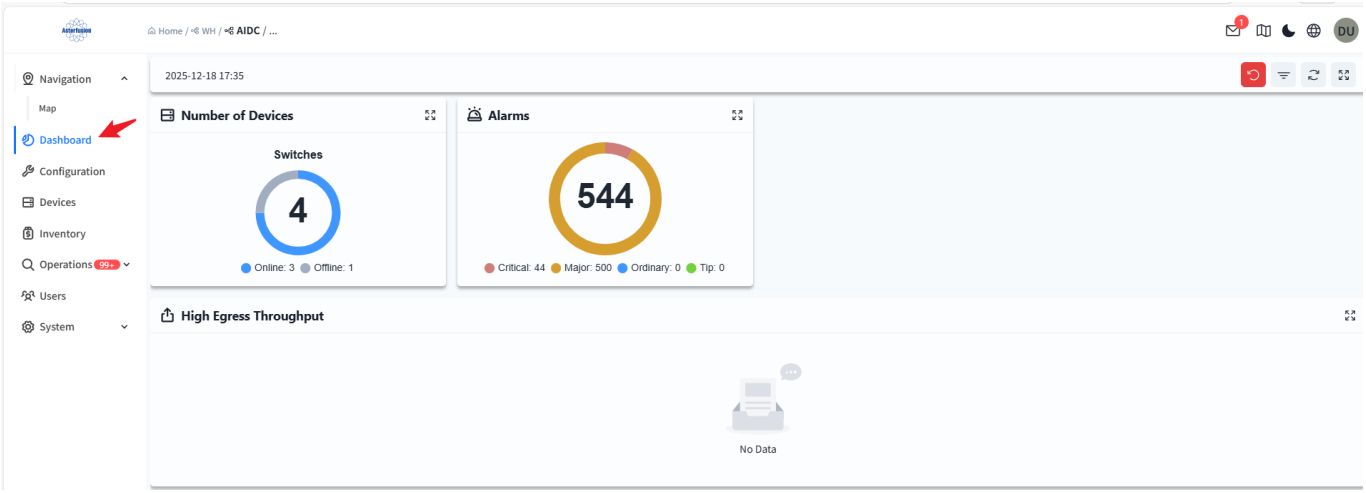


Figure 7.1-1 Organization View Dashboard

7.1.2 Venue Dashboard

Administrators can enter a specified venue under a specific organization in the [**Navigation**] interface to view the overview of the status of all devices and terminals in the venue.

- Historical Statistics of Egress Throughput: Displays the historical statistics of the throughput of the Spine uplink ports under the venue.
- Number of Devices: Displays the online status and quantity of all devices under the venue.
- TOP Interconnection Device Bandwidth Utilization: Displays the TOP5 bandwidth utilization of the interconnection links between Spine and Leaf devices under the venue.

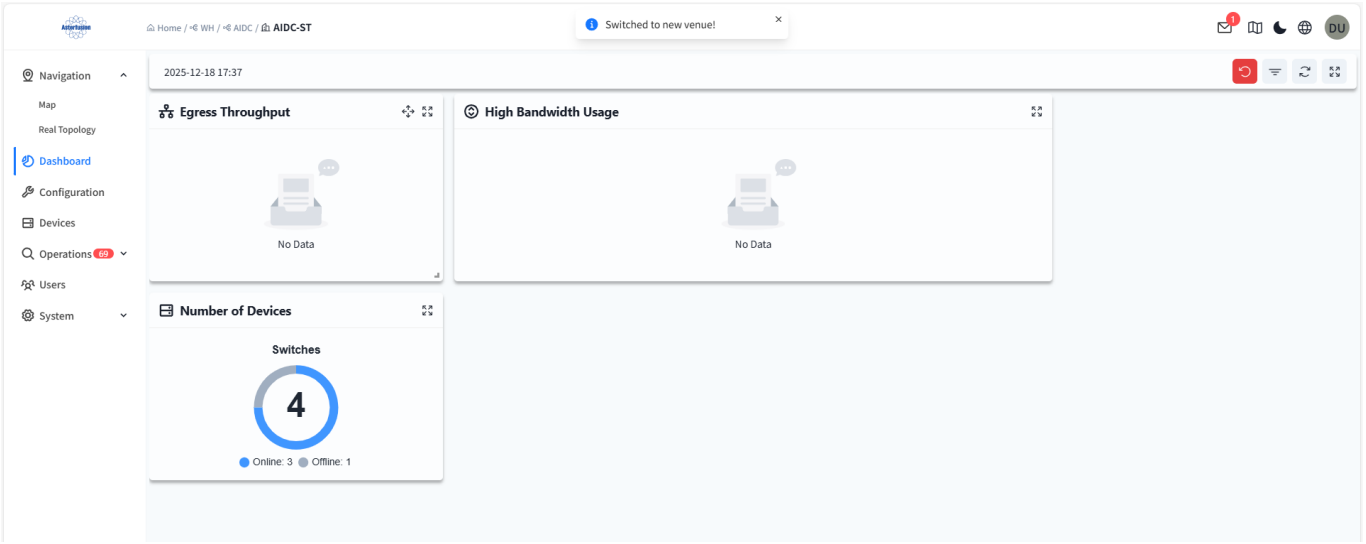


Figure 7.1-2 Venue View Dashboard

7.2 Device Status Visualization

Click [**Device**] - [**Device MAC**] to enter the management interface of the specified device and view the detailed information of this device:

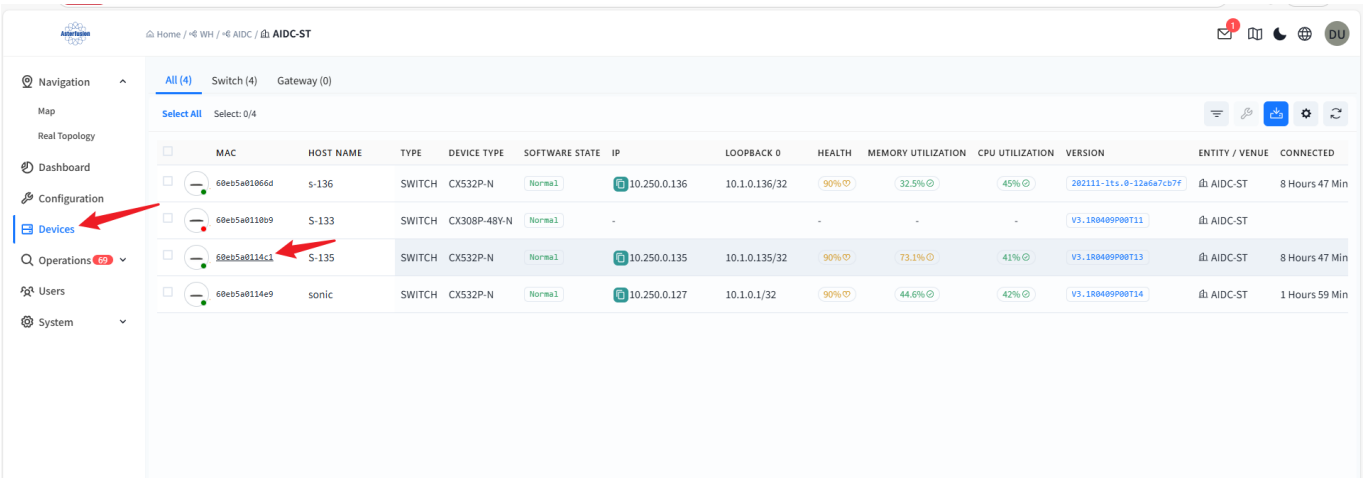


Figure 7.2-1 Device Page

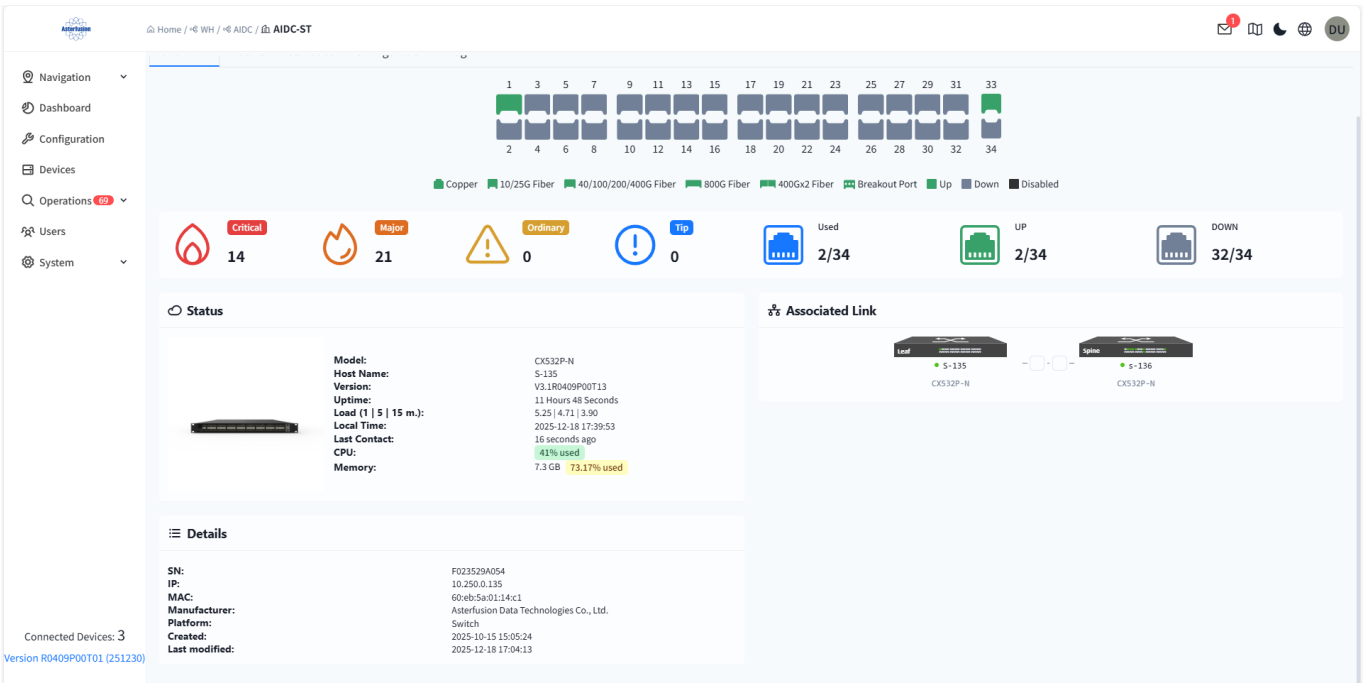


Figure 7.2-2 Device Information Overview Page

7.2.1 Device Information Overview

- View Interface Information

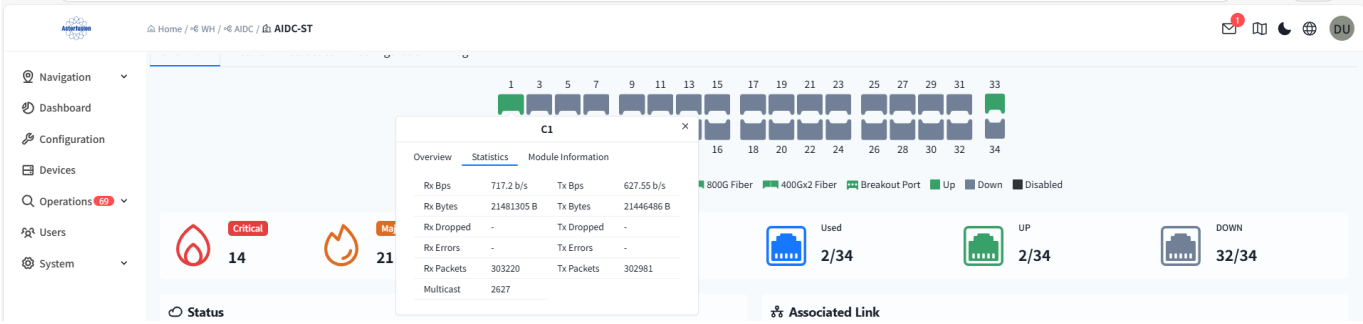


Figure 7.2-3 Device Interfaces and Interface Statistics

- View Interface Statistical Information

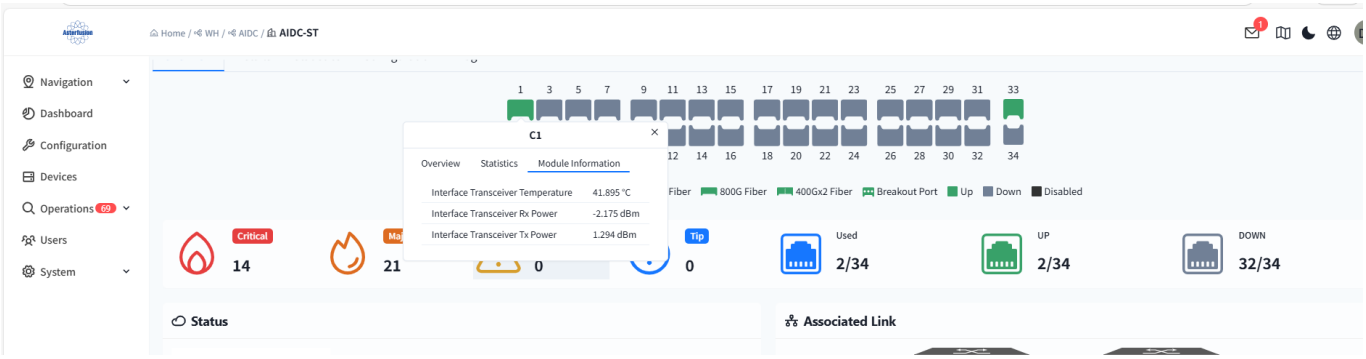


Figure 7.2-4 Interface Optical Module Information

- View Interface Optical Module Information

- Device Status: Users can view information such as device model, hostname, CPU utilization, and memory utilization here.
- Detailed Information: Includes device SN code, MAC address, manufacturer and other information.
- Associated Links: Displays the devices associated with this device. Clicking the name of the associated device can jump to the status visualization interface of a single device.

7.2.2 View Device Detailed Information

- Health Check: The initial health check value of switches is 100%.

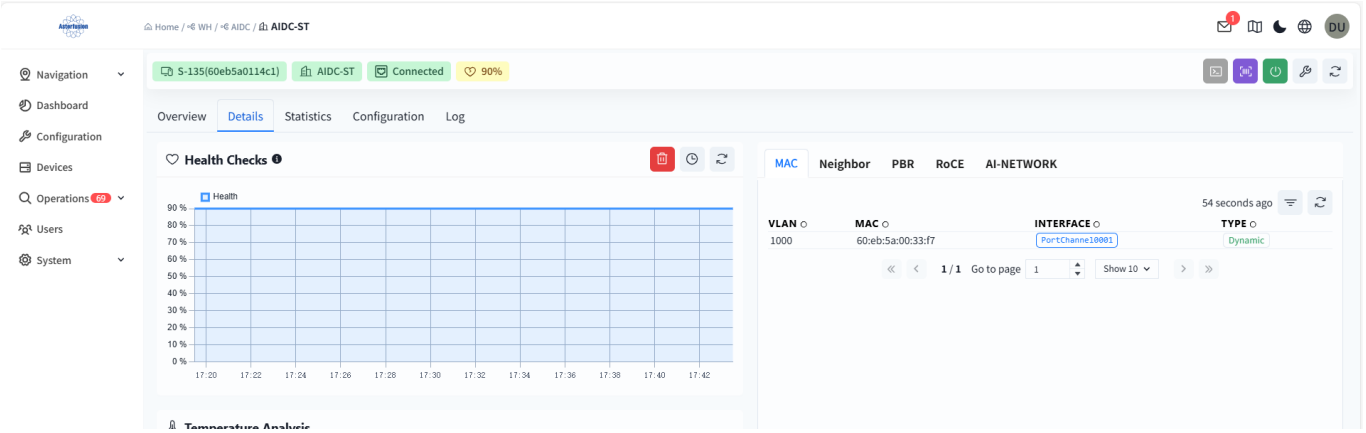


Figure 7.2-5 Detailed Device Information

- Switch Health Check Calculation Specifications:

  - If the CPU utilization exceeds 80%, the health decreases by 10%.
  - If the memory utilization exceeds 80%, the health decreases by 10%.
  - If the temperature of the switch chip/CPU exceeds 85℃, the health decreases by 10%.
  - If the status of any power supply in the PSU is abnormal (power module not in place, power not supplied), the health decreases by 10%.
  - Service Detection: If any key business service is abnormal, the health decreases by 10%.

- MAC: The MAC address table (CAM table) of the switch, which records the mapping relationship between the MAC addresses learned by the switch and ports, VLANs.

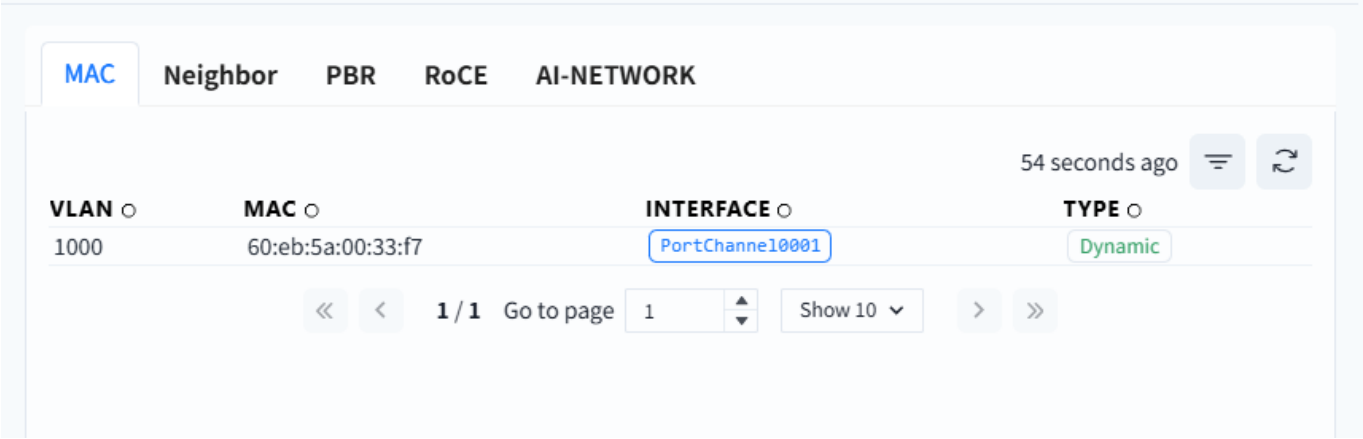


Figure 7.2-6 MAC Table Information

- VLAN: The VLAN ID to which the MAC address belongs, identifying different broadcast domains.
- MAC: The learned device MAC address (source MAC address).
- Interface: The switch port corresponding to the MAC address.
- Type: The way the entry is generated (dynamic: automatically learned by monitoring data frames, static: manually configured by the administrator).

- Neighbor Information: This table is the neighbor discovery table of the switch (NDP for IPv6 / ARP for IPv4), which records the IP-MAC mapping relationship of devices directly connected to the local switch.

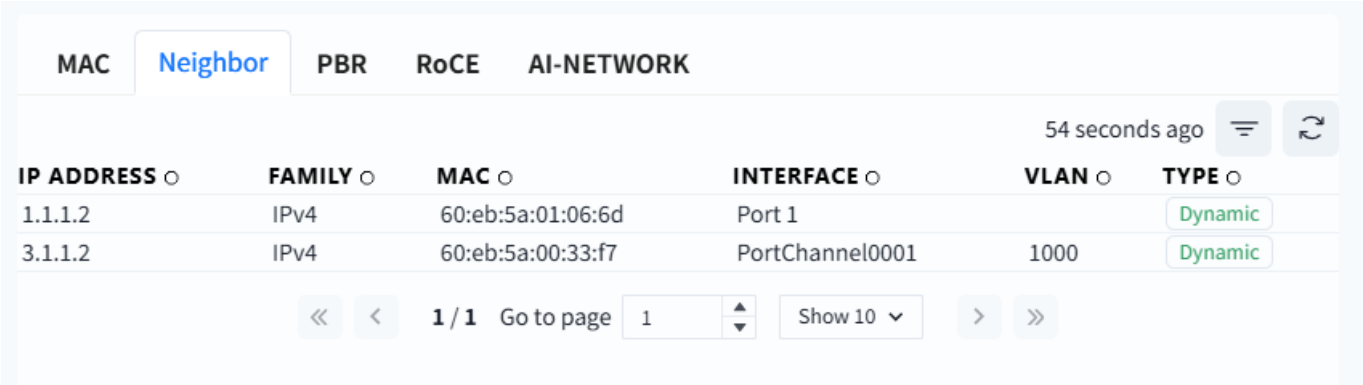


Figure 7.2-7 Device Neighbor Information

- IP Address: The IP address of the neighbor device (IPv4/IPv6).
- IP Address Family: IPv4 or IPv6 protocol type.
- MAC: The physical address of the neighbor device.
- Interface: The port of the local switch connected to the neighbor.
- VLAN: The virtual local area network where the communication takes place.
- Type: Dynamic (automatically learned by the protocol) or static (manually configured).

- PBR: Policy-based routing configuration information.

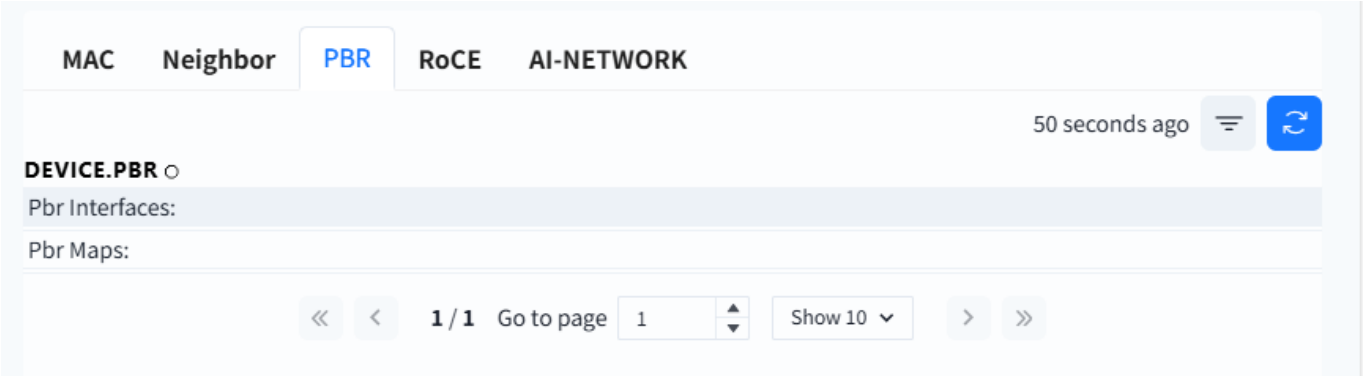


Figure 7.2-8 Device PBR Information

- Pbr Interface: List of interfaces bound to policy-based routing.
- Pbr Maps: Detailed policy-based routing policies.

- RoCE Configuration Information

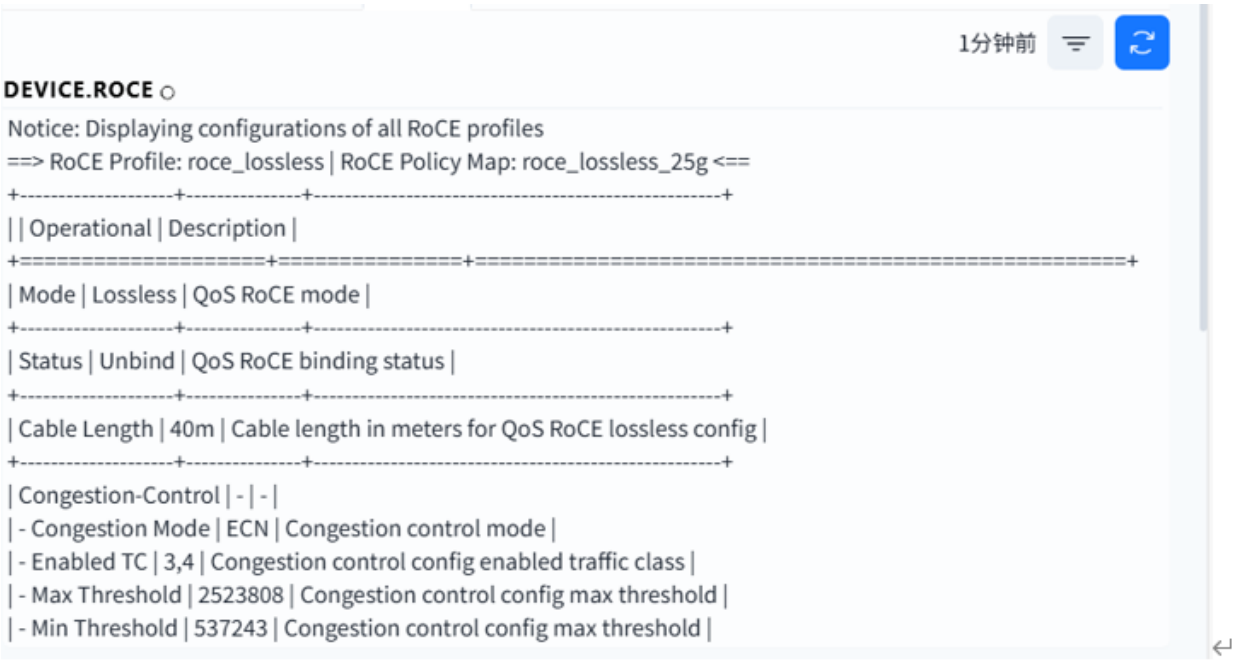


Figure 7.2-9 RoCE Configuration Information

- AI-Network Configuration Information

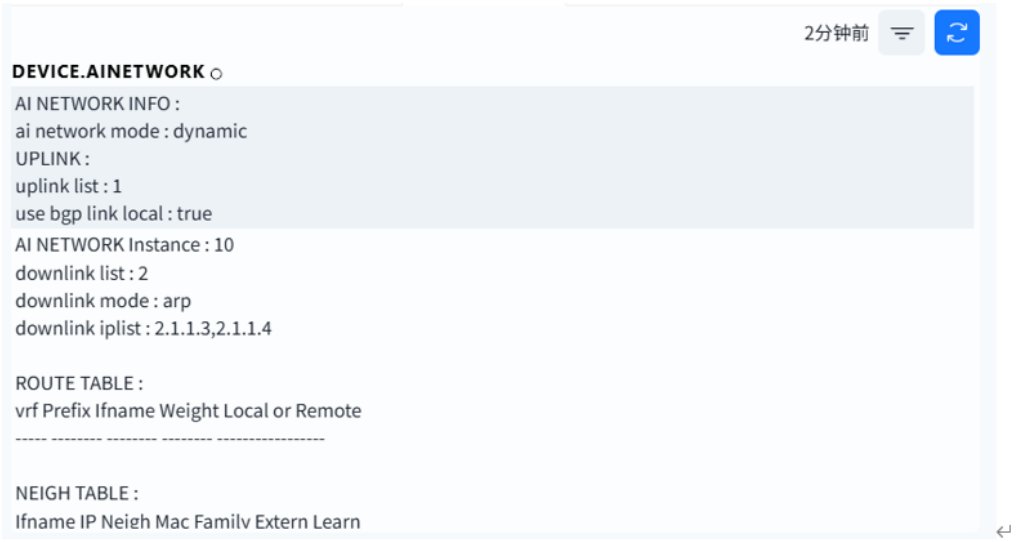


Figure 7.2-10 Intelligent Routing Configuration Information

- Temperature: Displays the temperature information of various components of the device.

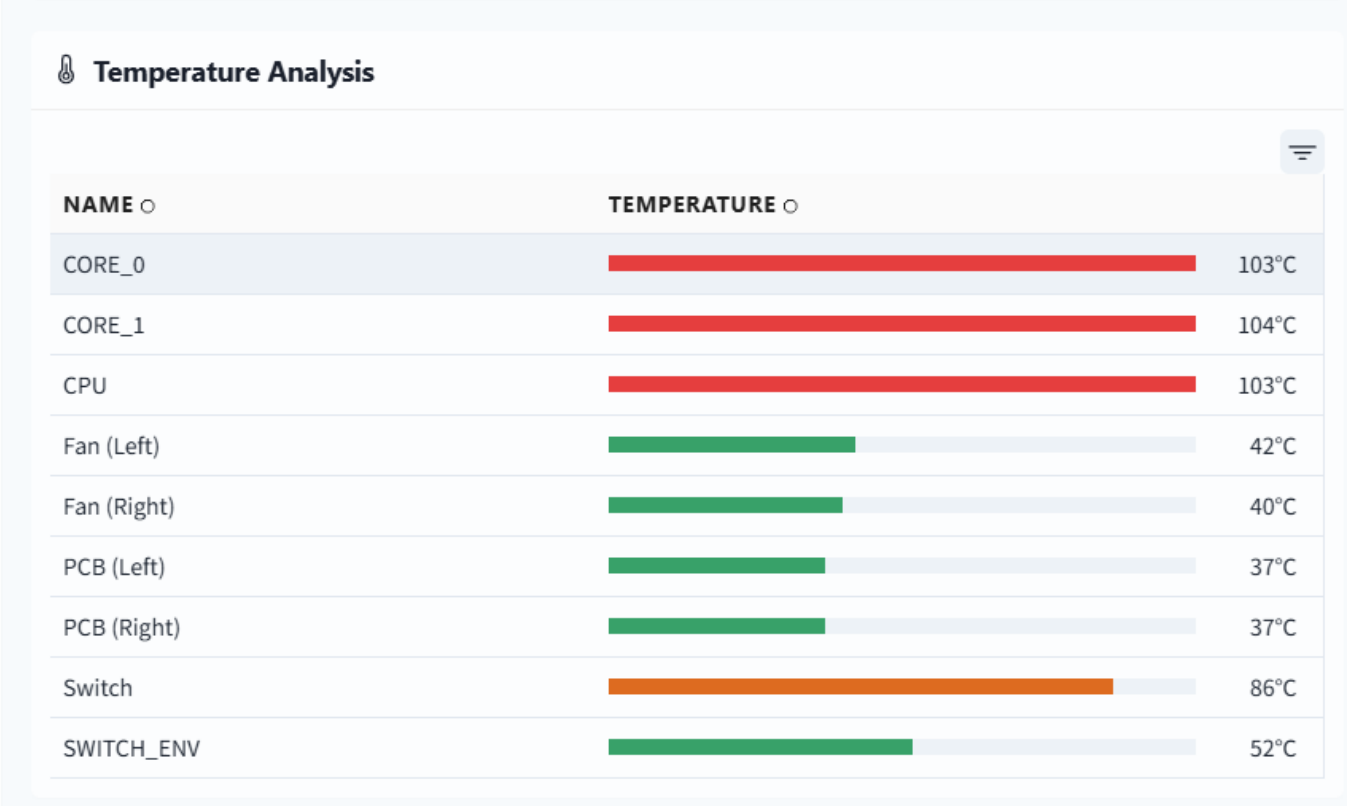


Figure 7.2-11Temperature

- Fan: Displays detailed information of each fan module of the device.

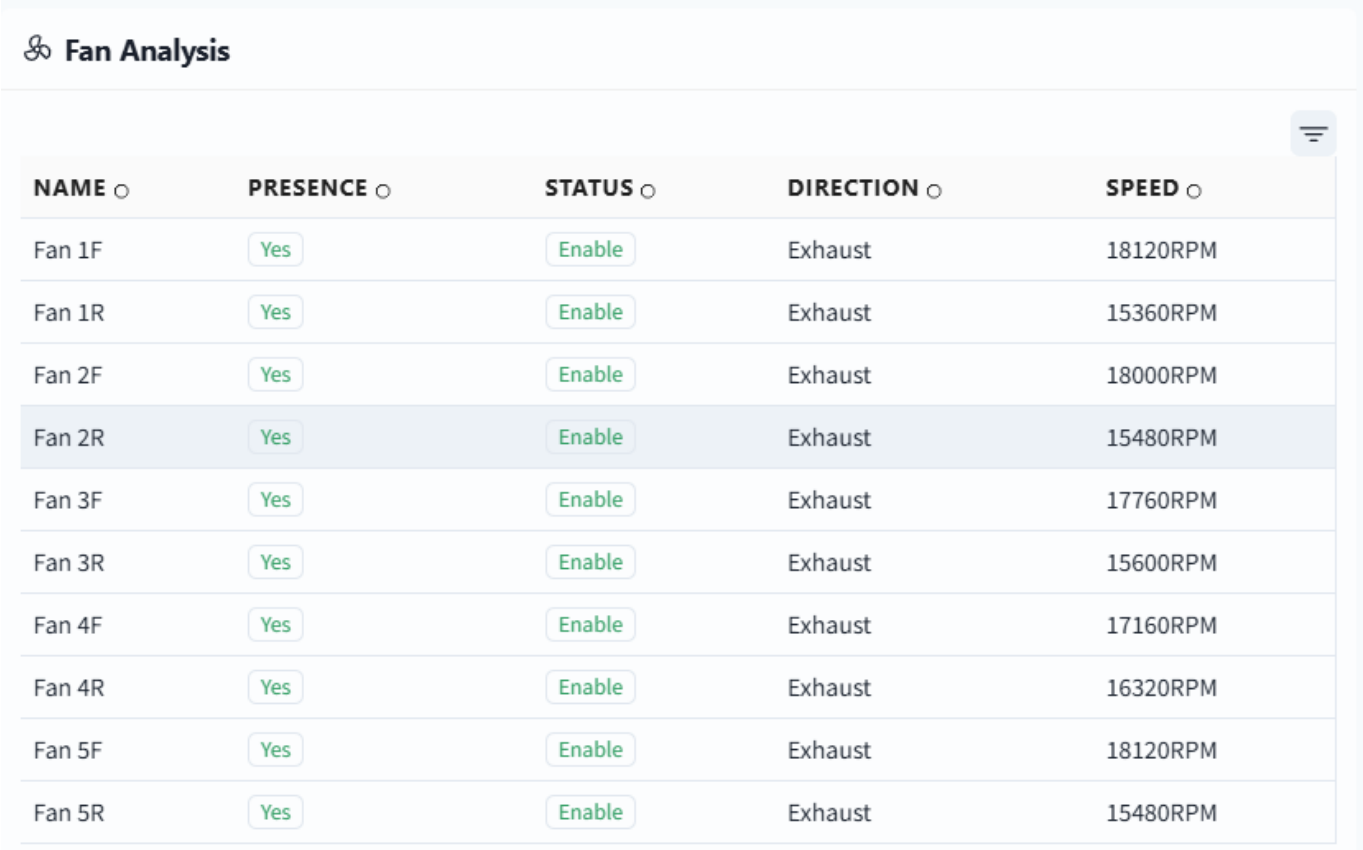


Figure 7.2-12 Fans Information

- Power Supply: Displays the power supply information of the device.

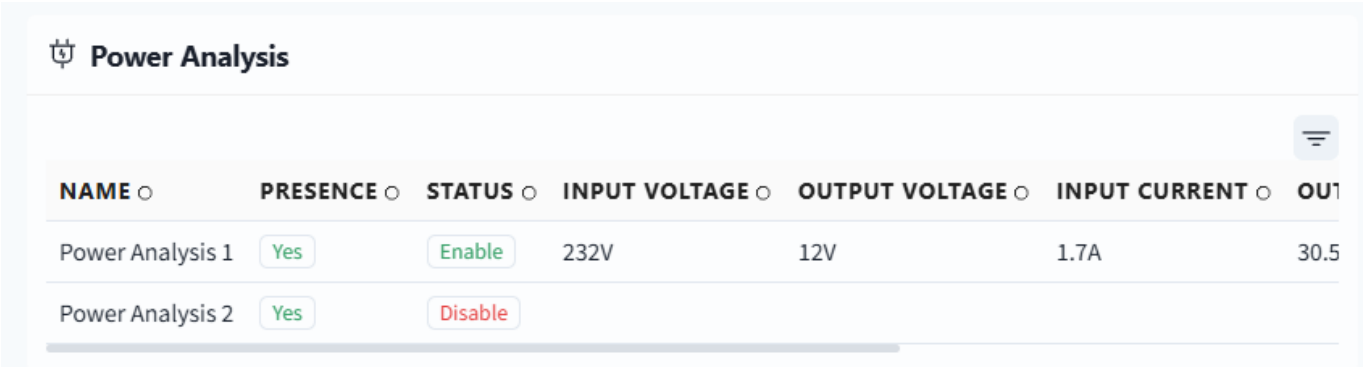


Figure 7.2-13 Power Information

- Patch: List of patches already installed on the device.

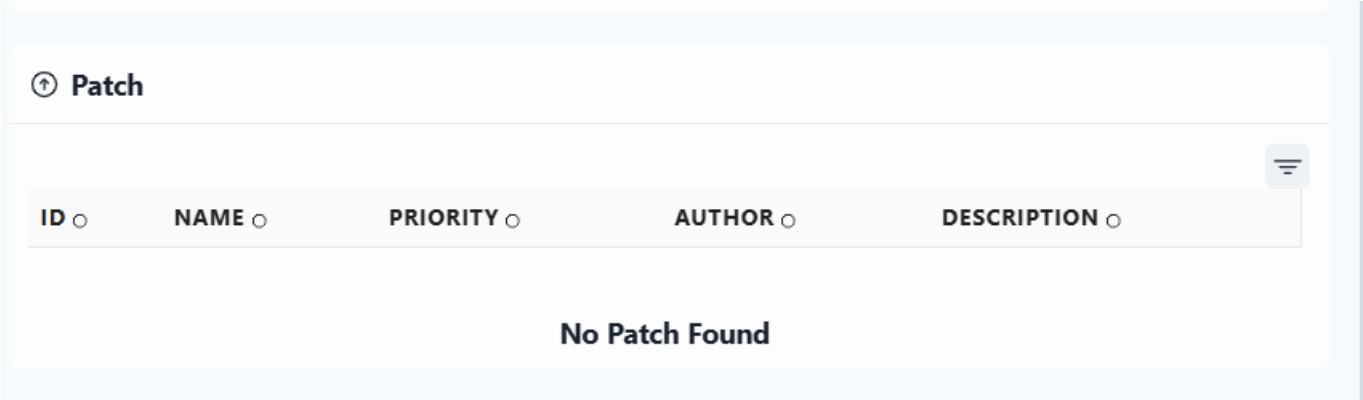


Figure 7.2-14 Patch Information

- Notes: Notes added by the user.

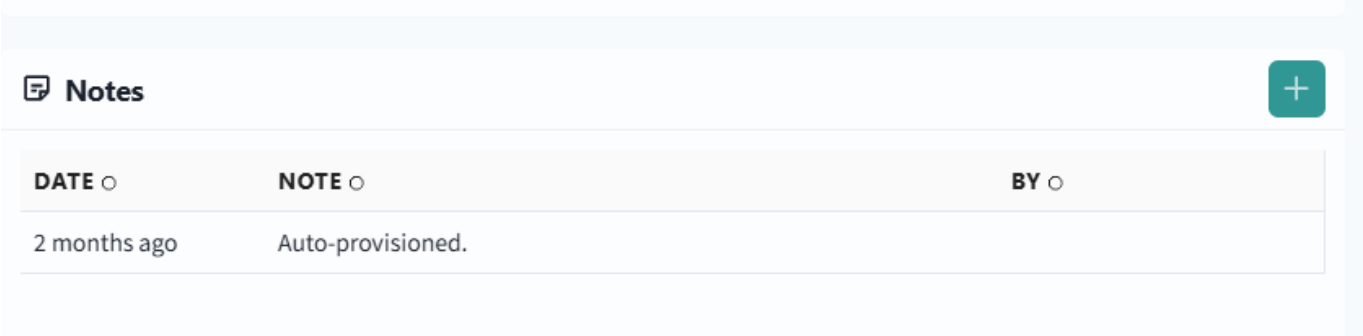


Figure 7.2-15 Note Information

7.2.3 View Device Statistical Information

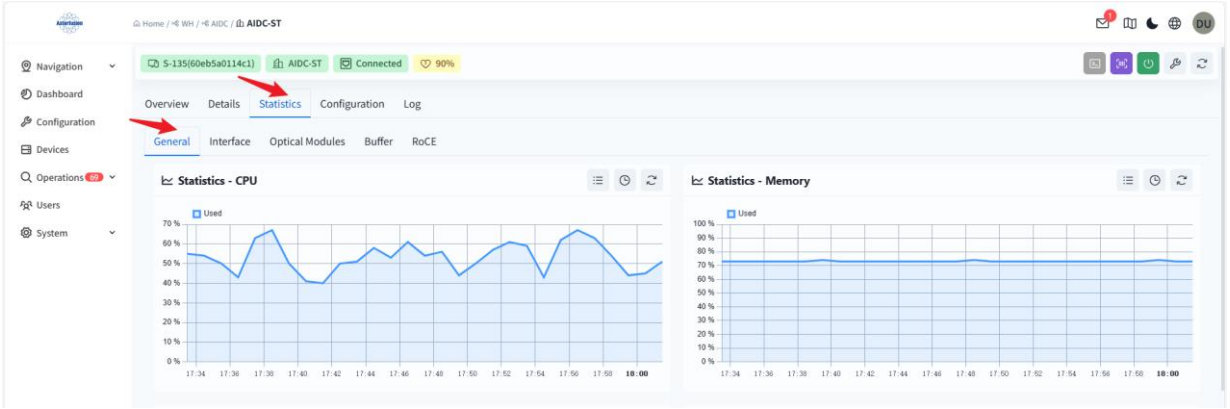


Figure 7.2-16 Device CPU/Memory Information

- CPU Statistics: Historical CPU statistics within three days.
- Memory Statistics: Historical memory statistics within three days.

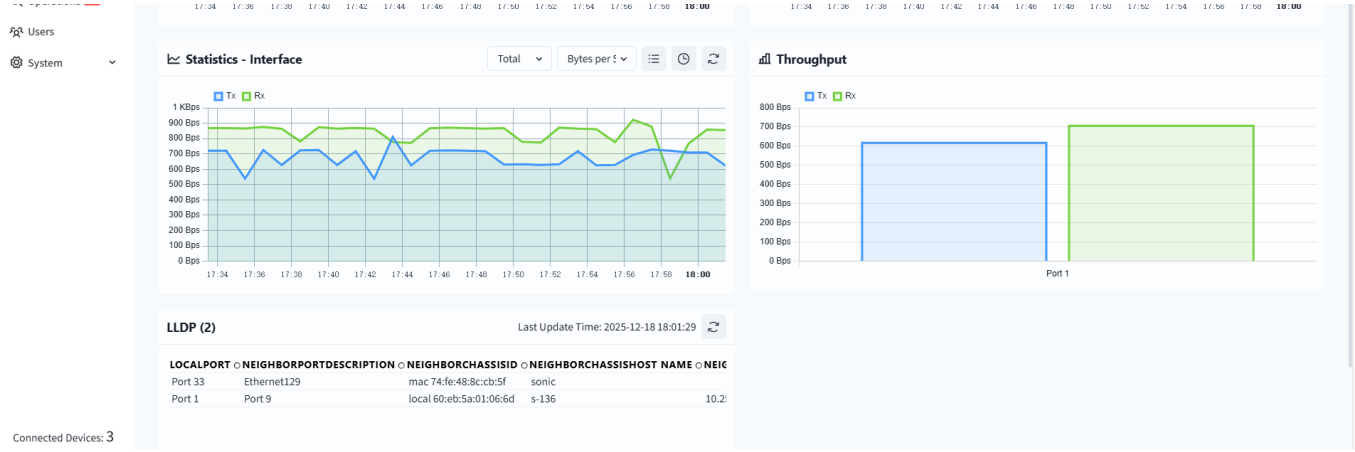


Figure 7.2-17 Device Interface Statistics and LLDP Information

- Interface Statistics: Single interface/overall interface statistics of the device, supporting two statistical methods: byte rate (bytes per second) and number of data packets (increment from the previous counting time).
- LLDP: Displays the LLDP information on the switch.

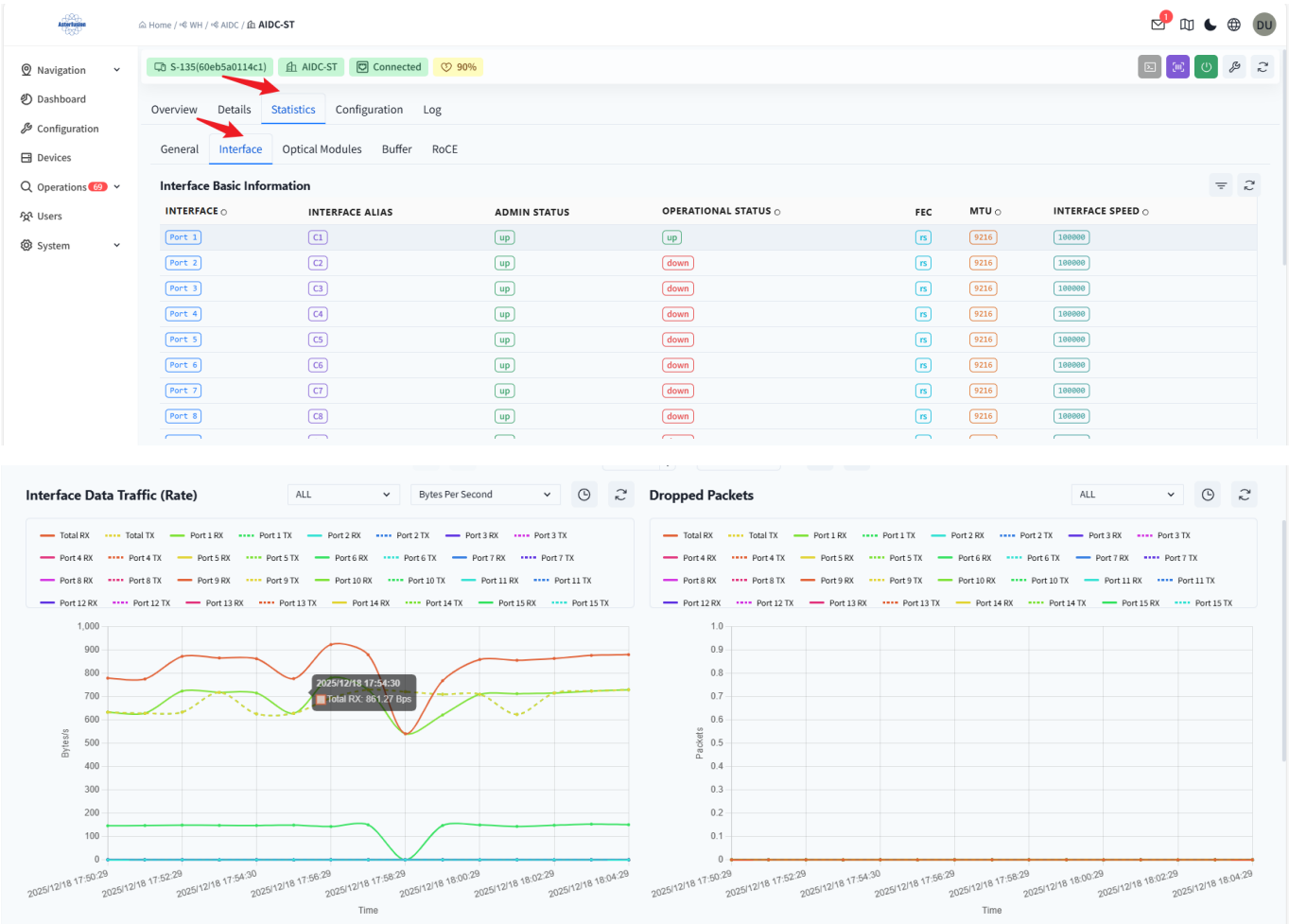


Figure 7.2-18 Interface and Interface Statistics

- Basic Interface Information
- Interface Data Traffic (Rate)
- Interface Packet Loss Statistics: Packet loss statistics of each interface.
- Interface Error Packet Statistics: Error packet statistics of each interface.
- Queue Data Traffic: Traffic statistics of each queue of each interface within 1 minute.
- Queue Data Traffic (Rate): Forwarding rate statistics of each queue of each interface.
- Queue Packet Loss: Packet loss statistics of each queue of each interface.

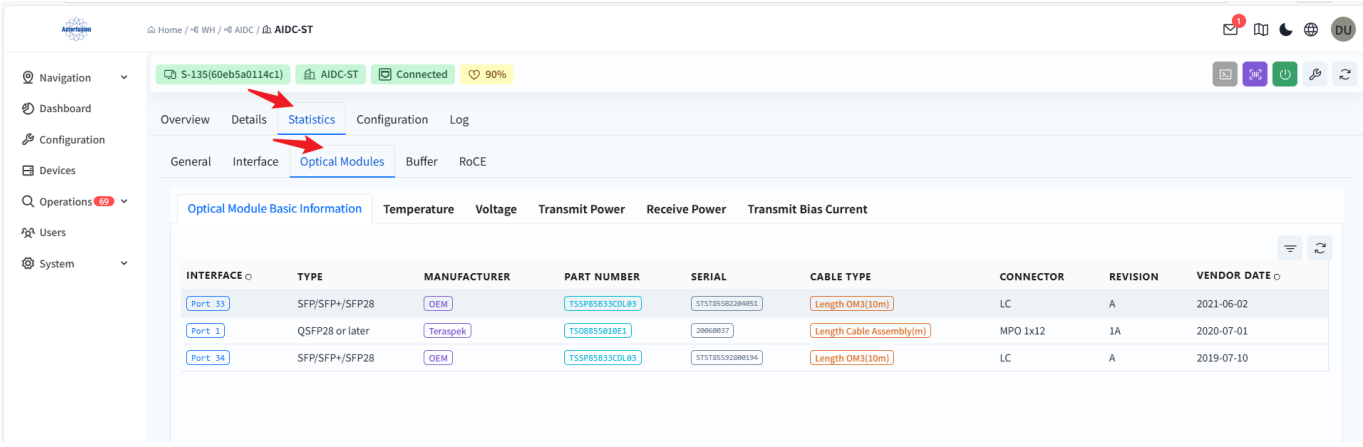


Figure 7.2-19 Basic Interface Optical Module Information

- Basic Optical Module Information

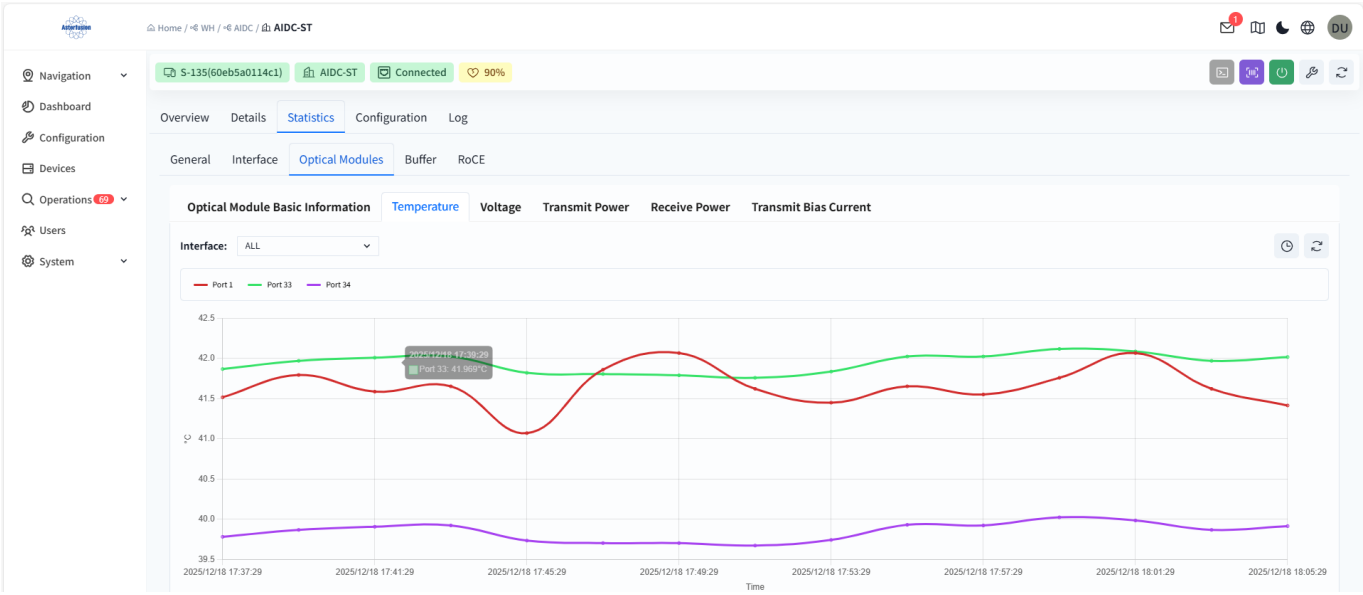


Figure 7.2-20 Optical Module Temperature Information

- Temperature Information

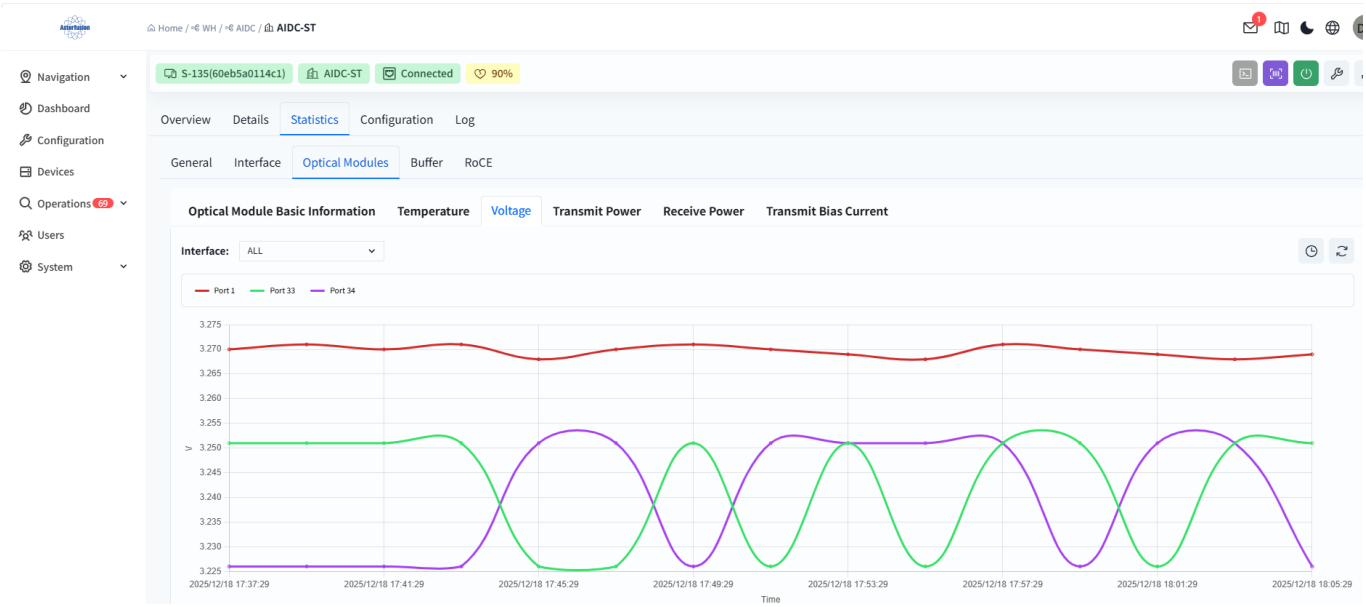


Figure 7.2-21 Optical Module Voltage Information

- Voltage Information

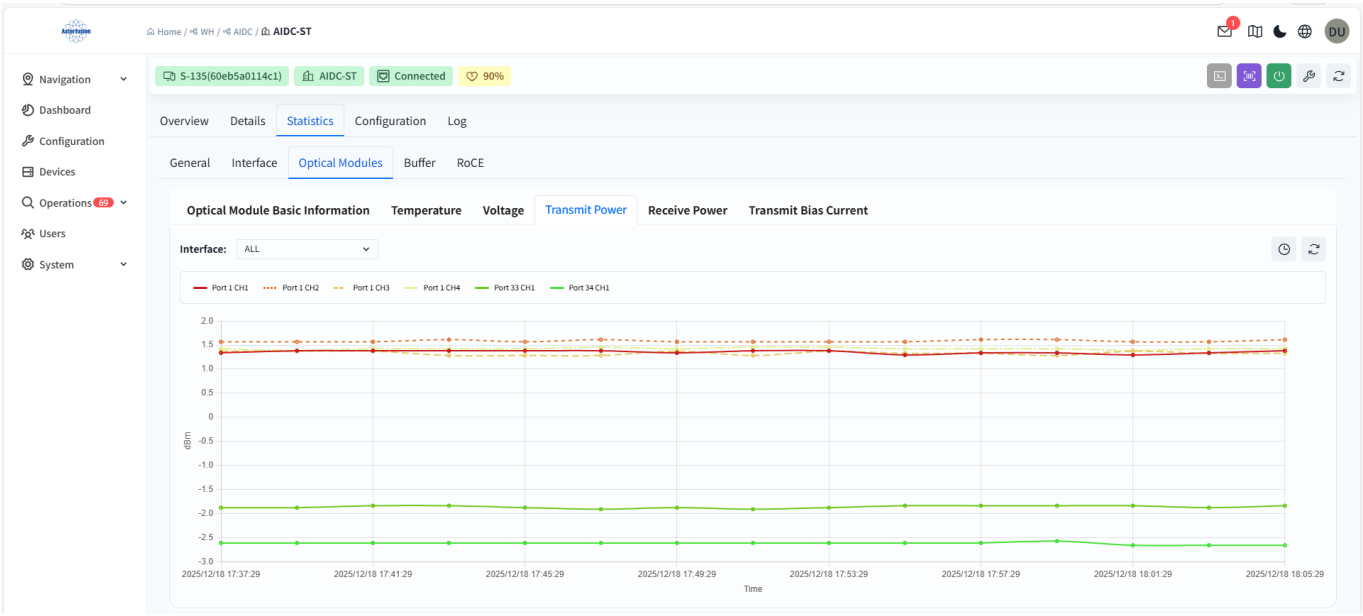


Figure 7.2-22 Optical Module Transmit Power

- Transmit Power: Transmit power of each channel of the optical module.

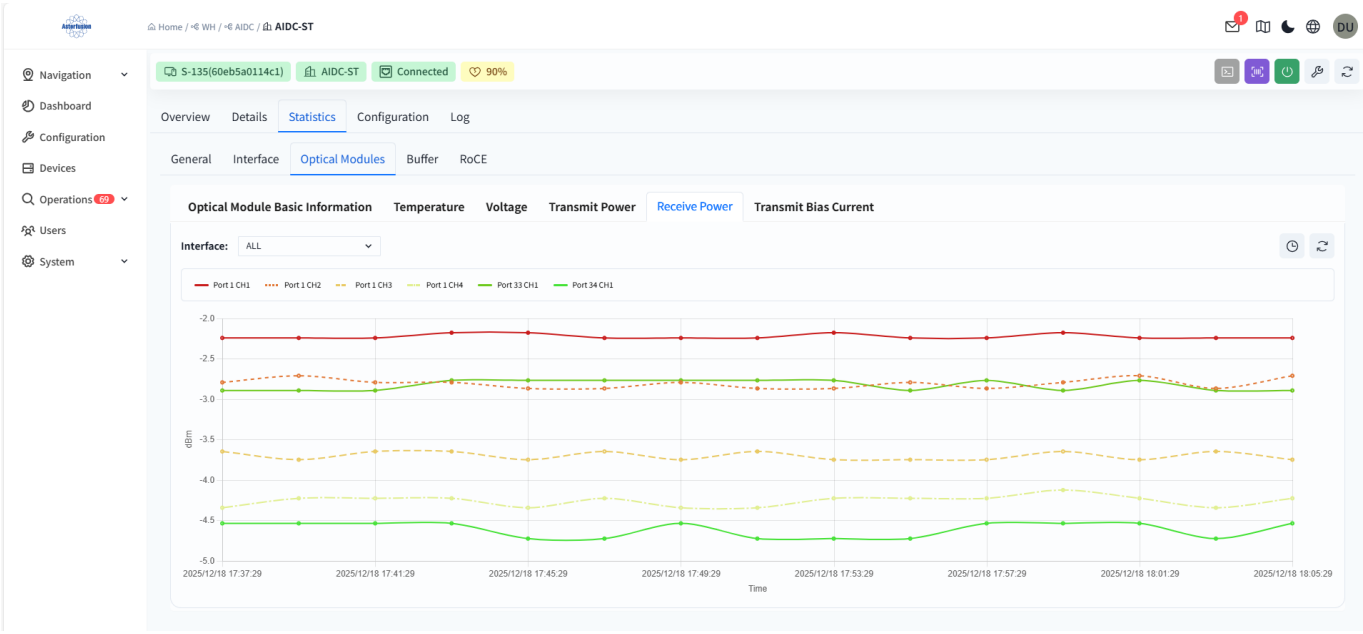


Figure 7.2-23 Optical Module Receive Power

- Receive Power: Receive power of each channel of the optical module.

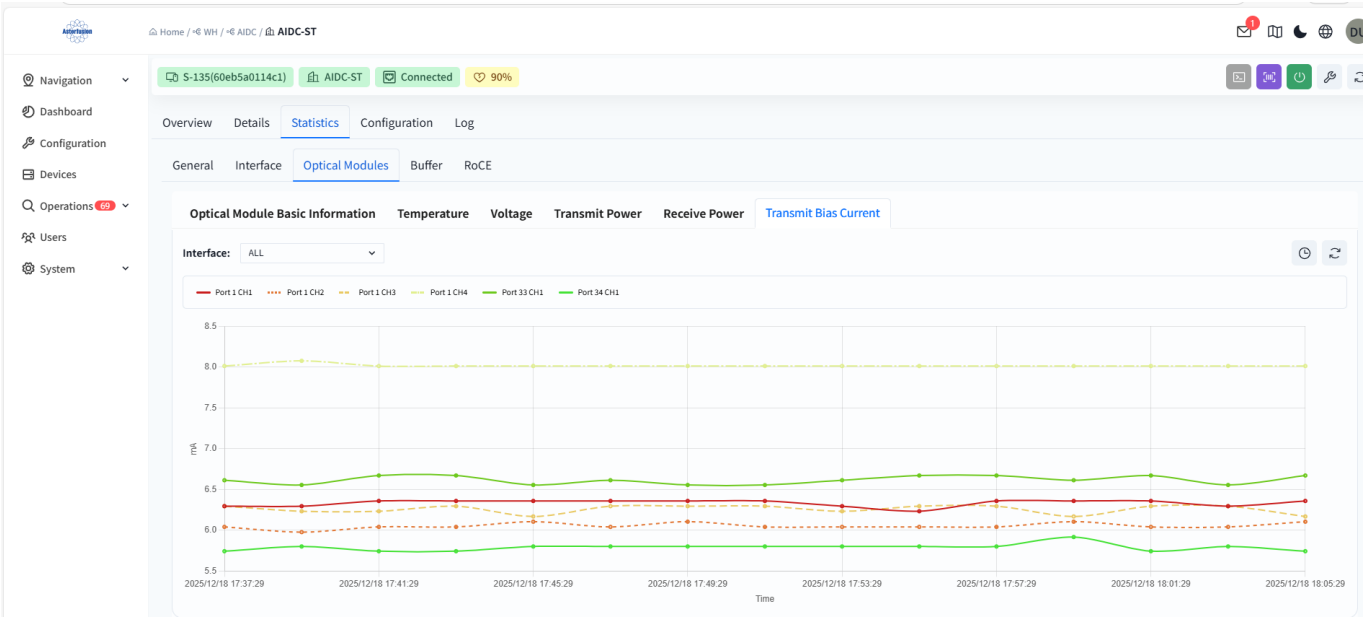
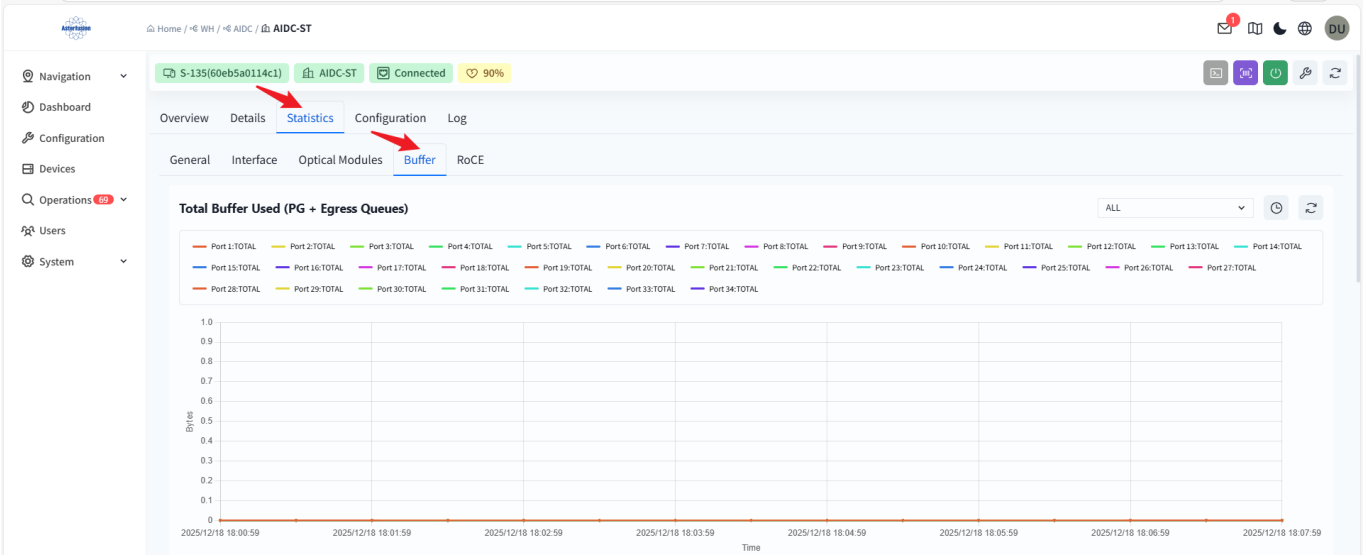
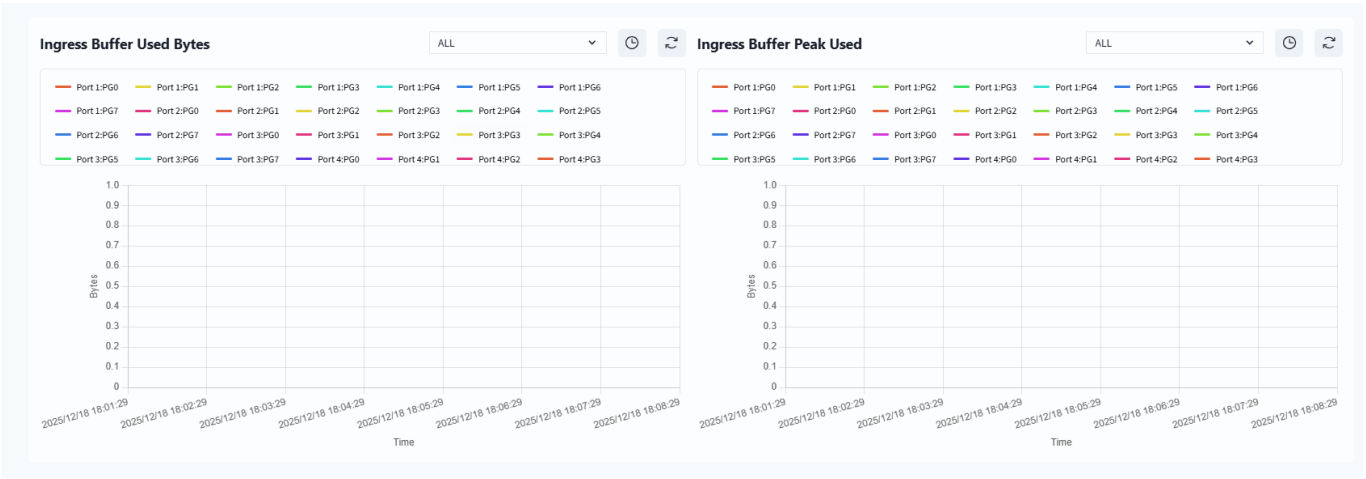


Figure 7.2-24 Optical Module Bias Current

- Transmitter Bias Current: Transmitter bias current information of each channel of the optical module.





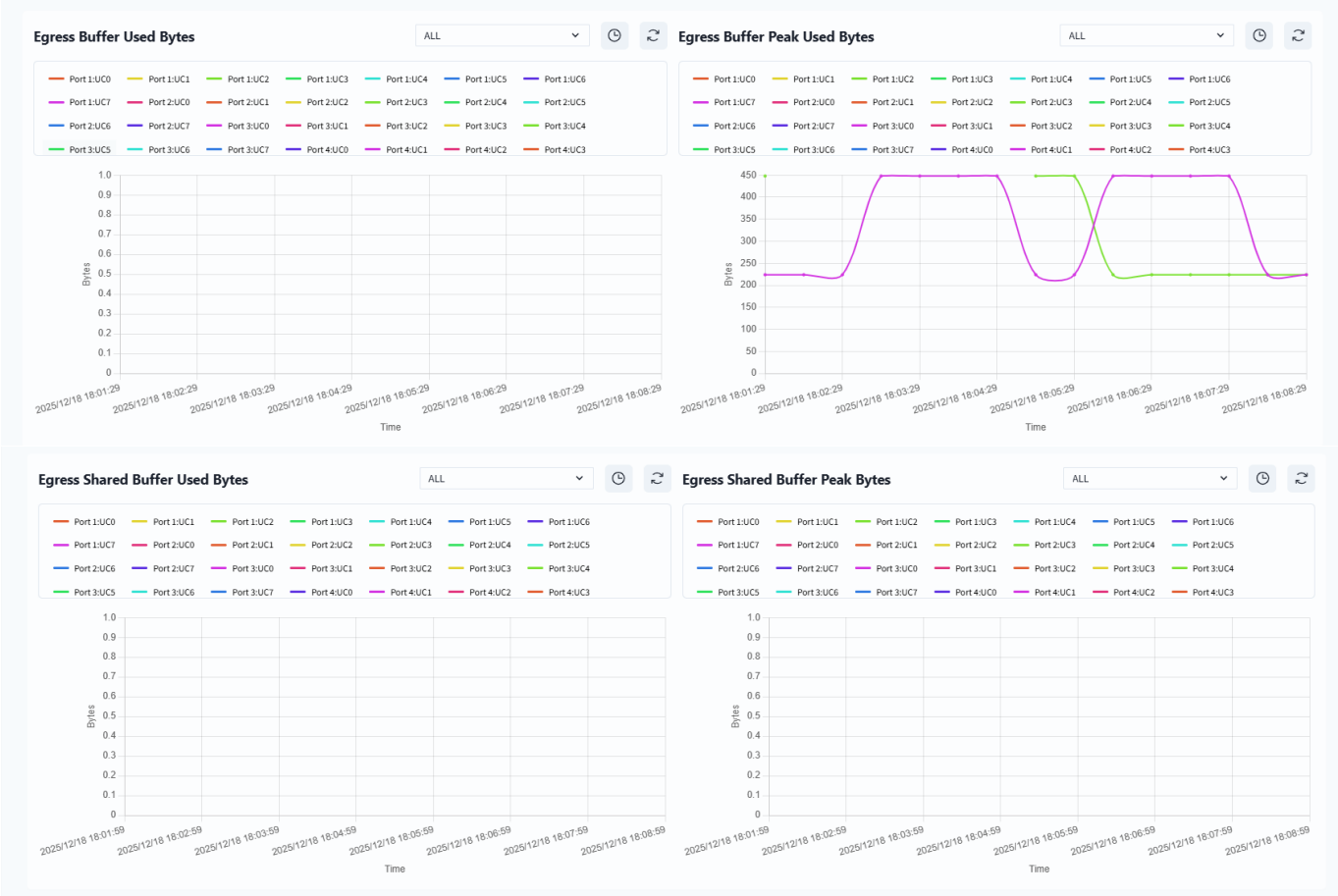
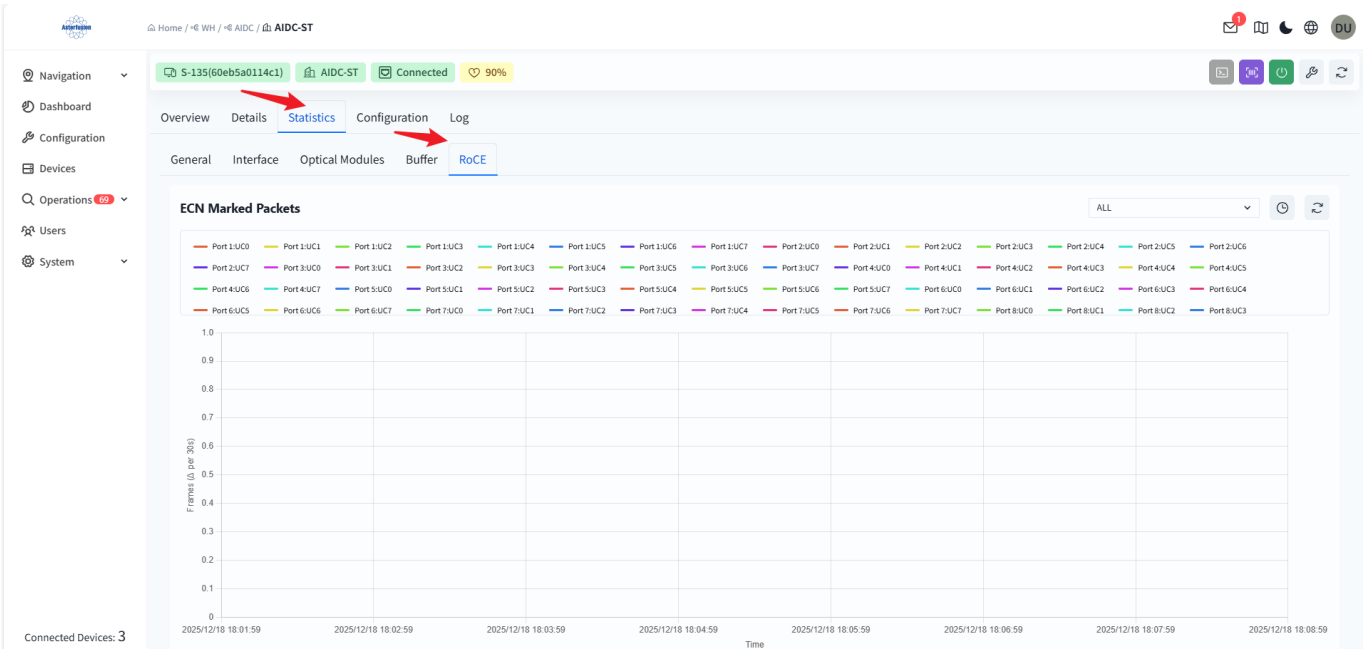
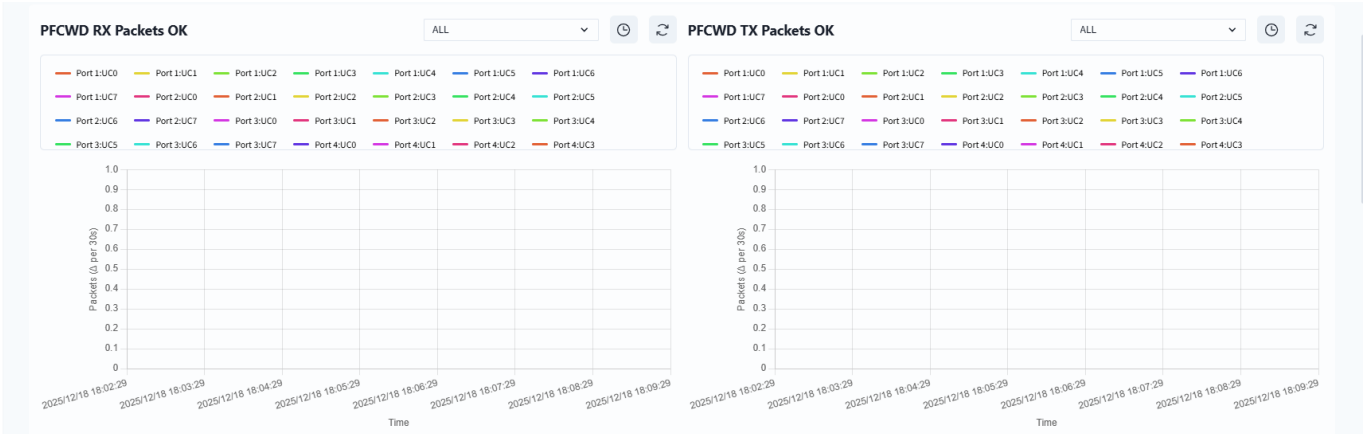
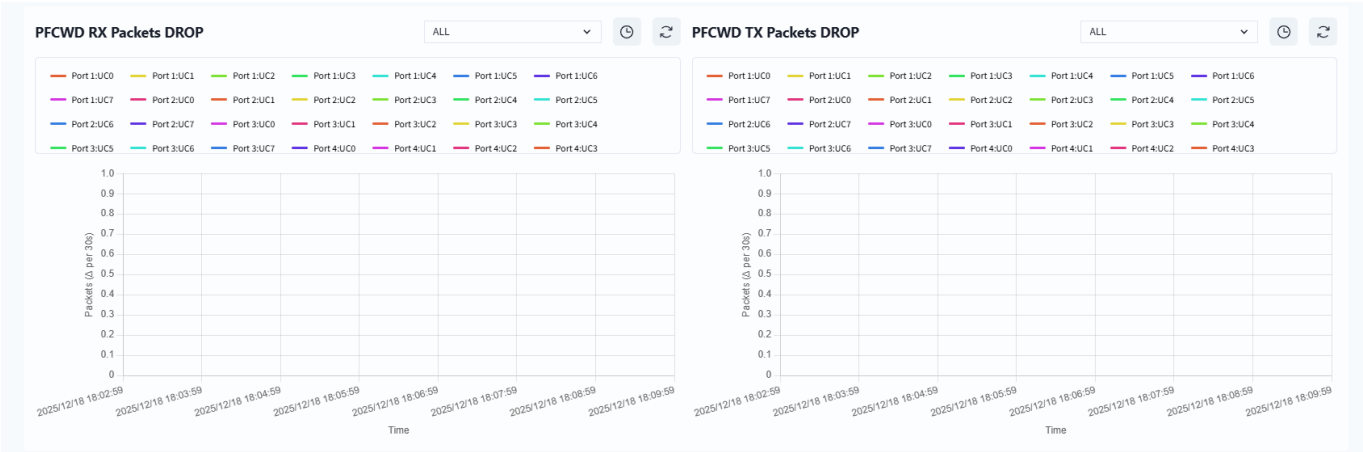


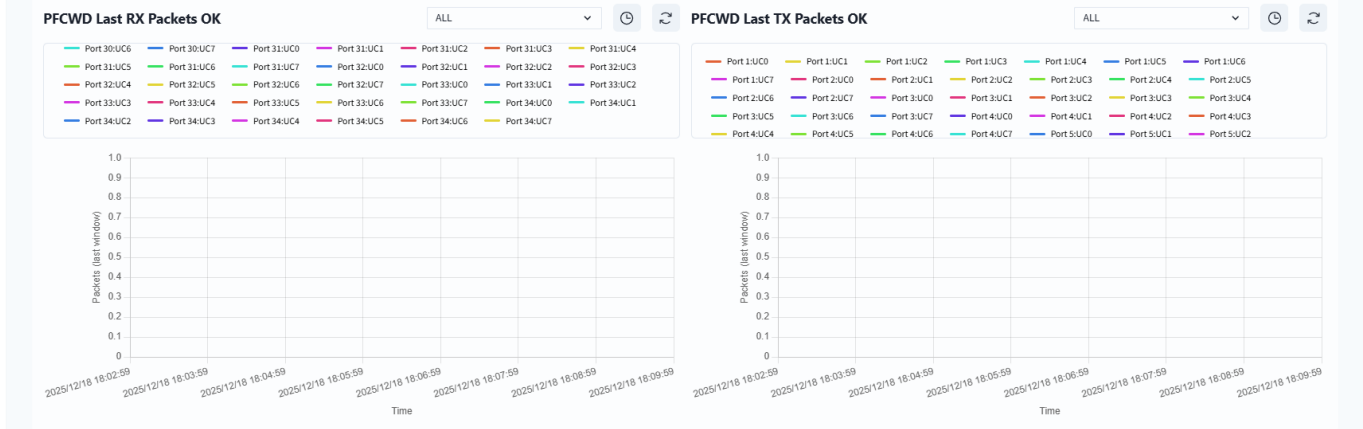
Figure 7.2-25 Device Buffer Statistics

- Total Buffer Used (PG + Egress Queues): Statistics of the BUFFER used by the device.
- Ingress Buffer Used Bytes: Real-time Buffer usage statistics of Ingress.
- Ingress Buffer Peak Used: Peak Buffer occupancy statistics of Ingress.
- Egress Buffer Used Bytes: Real-time Buffer usage statistics of Egress.
- Egress Buffer Peak Used: Peak Buffer occupancy statistics of Egress.
- Egress Shared Buffer Used Bytes: Real-time shared Buffer usage statistics of Egress.
- Egress Shared Buffer Peak Used: Peak shared Buffer occupancy statistics of Egress.









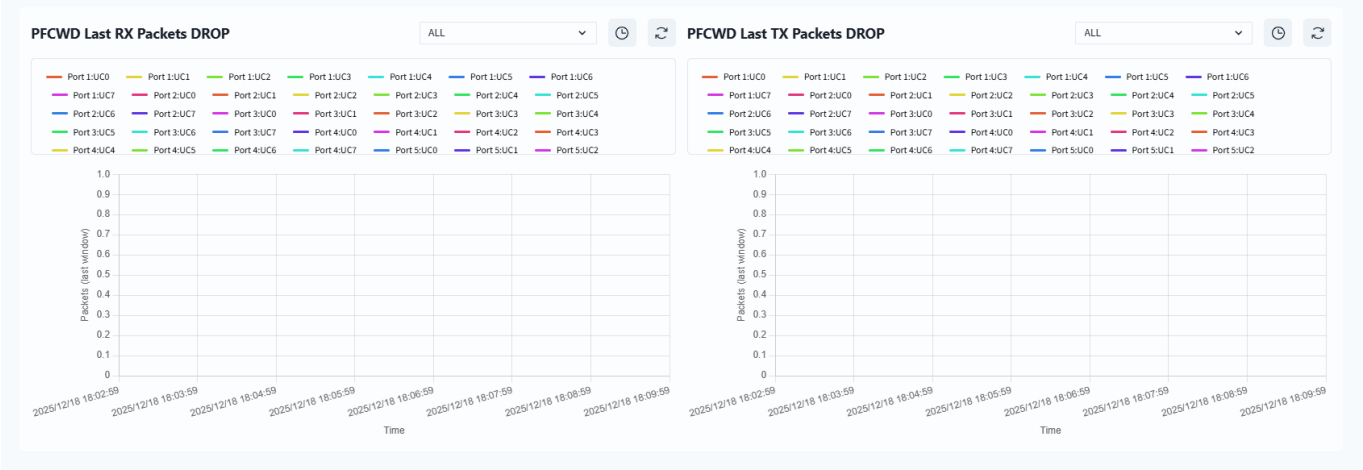


Figure 7.2-26 RoCE Metric Statistics

- ECN Marked Packets: Number of ECN packets marked every 30s.
- Receive PFC Frames
- Transmit PFC Frames
- PFCWD RX Packets OK
- PFCWD TX Packets OK
- PFCWD RX Packets DROP
- PFCWD TX Packets DROP
- PFCWD Last RX Packets OK
- PFCWD Last TX Packets OK
- PFCWD Last RX Packets DROP
- PFCWD Last TX Packets DROP

7.2.4 View Device Configuration Information

Displays the configuration information of device interfaces, LAG, VLAN, routing, authentication, and security.

Figure 7.2-27 Device Configuration Information

7.2.5 View Device Log Information

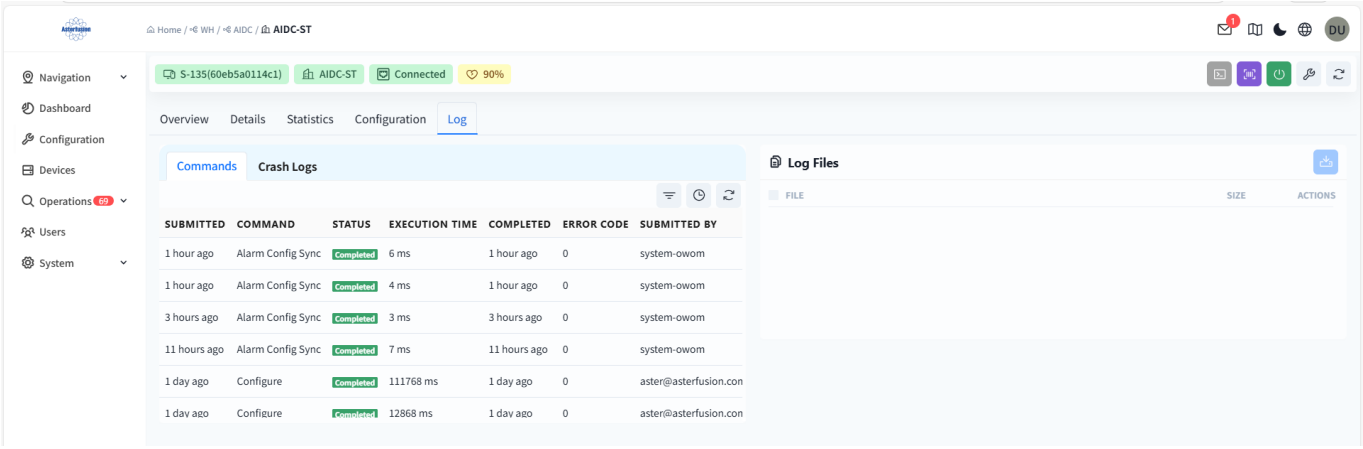


Figure 7.2-28 Device Log Information

8 Operation and Maintenance & Alarm Management

Firmware management is an important function of the controller, used to manage the version image files and patch files of network devices. Users can upload local images to the controller to conveniently deploy new software versions across the entire network, or directly use the uploaded firmware to update network devices.

Administrators can upload local version images to the controller and record basic information about the software version.

8.1 Firmware Management

8.1.1 Upload Firmware

Administrators can upload local version images to the controller and record basic information about the software version.

Operation Steps

1. Enter [**Operations**] - [**Firmware**]
2. Click [+] to upload the version image to the controller
3. Use [Type] to distinguish the device type applicable to the firmware
4. Use [Platform] to specify different hardware models

a) ARM64: None

b) x86: CX532 series, CX564 series, CX664 series, CX732 series, CX864 series

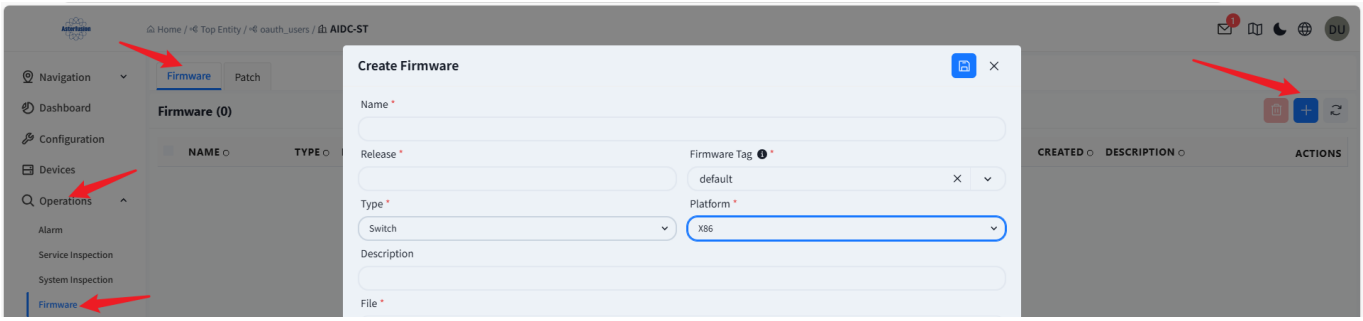


Figure 8.1-1 Creating Firmware

8.1.2 Firmware Application

1. In the [**Device**] page, choose devices to be updated and click the [**Actions**] button in the upper right corner.

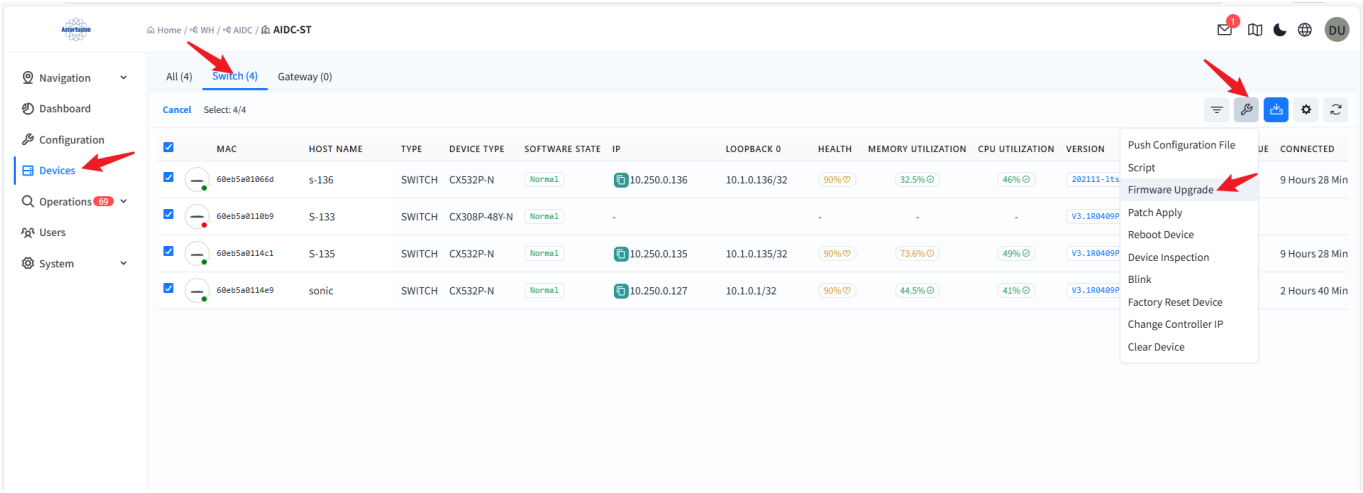


Figure 8.1-2 Firmware Application

2. In the pop-up window, click [**Release**] to select the firmware image file, click [Platform] to select the device type, and after selection, click [**Next**] to perform the firmware upgrade.

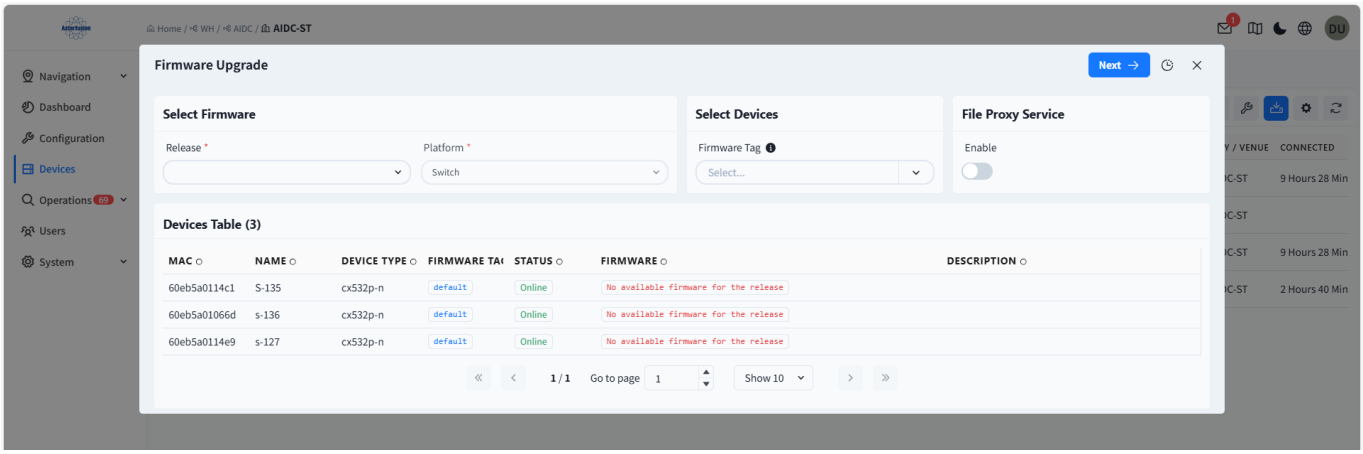


Figure 8.1-3 Executing Firmware Upgrade

➢ Note: After the upgrade is completed, the switch will not restart automatically. You need to manually perform a restart operation to make the upgrade take effect.

8.2 Patch Management

8.2.1 Upload Patch

Patch management allows administrators to upload patch files to the controller. The controller will automatically parse the patch content to ensure that the patch is applicable to the correct device platform, thereby enhancing network security and device stability.

Click [**Operations**] - [**Firmware**] - [**Patch**] - [+] to enter the patch upload interface. Administrators can upload patch files in various formats (such as .bin, .tar.gz, .patch).

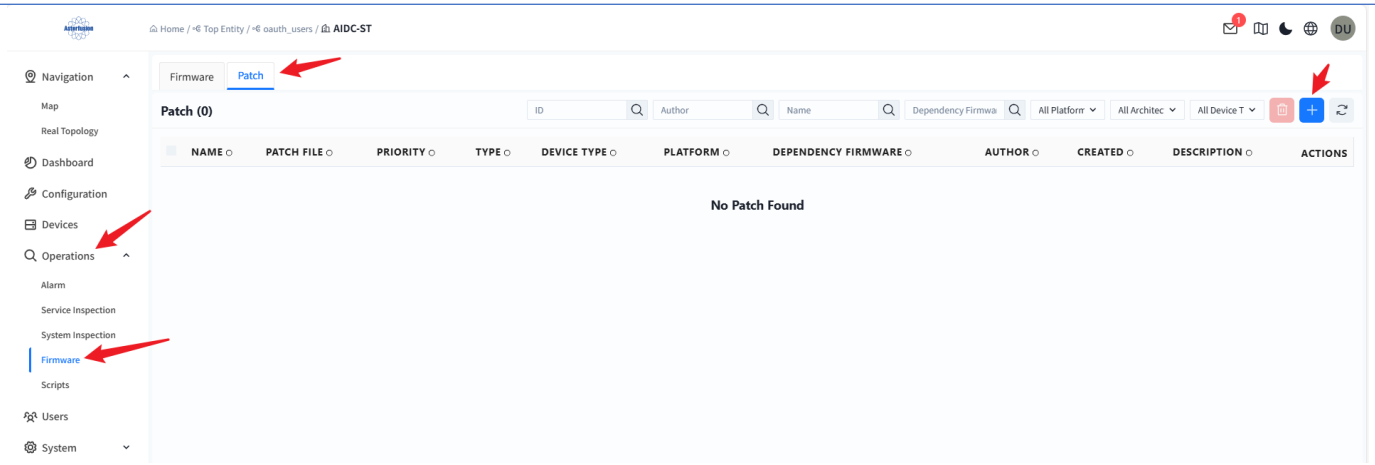


Figure 8.2-1 Uploading Patch

8.2.2 Patch Application

In the [**Device**] page, choose devices to be updated and click the [**Actions**] button in the upper right corner.

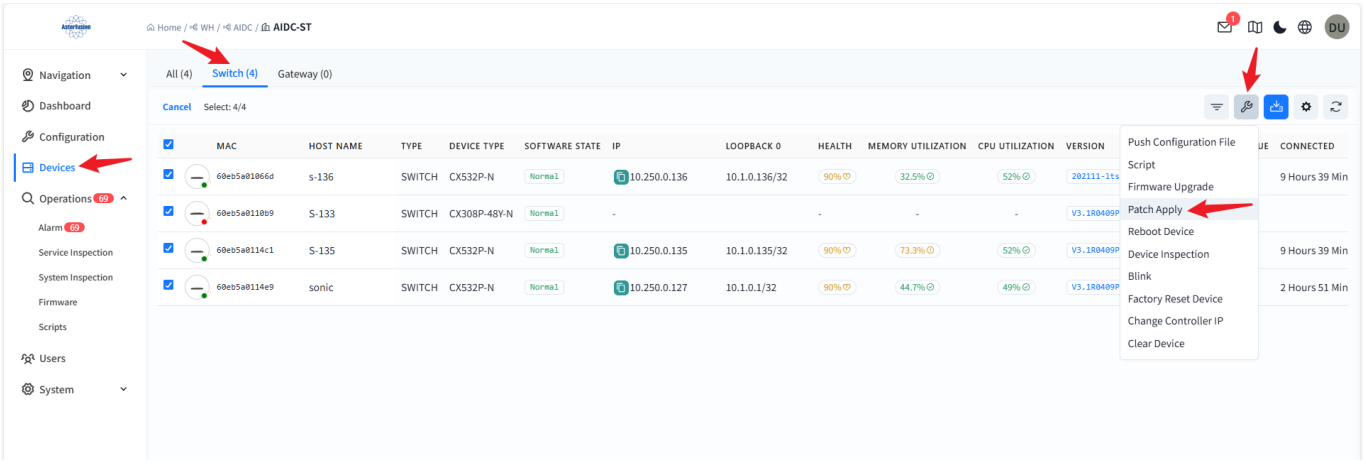


Figure 8.2-2 Patch Application

In the pop-up interface, filter the required patches and devices, and click [Next] to apply the patch.

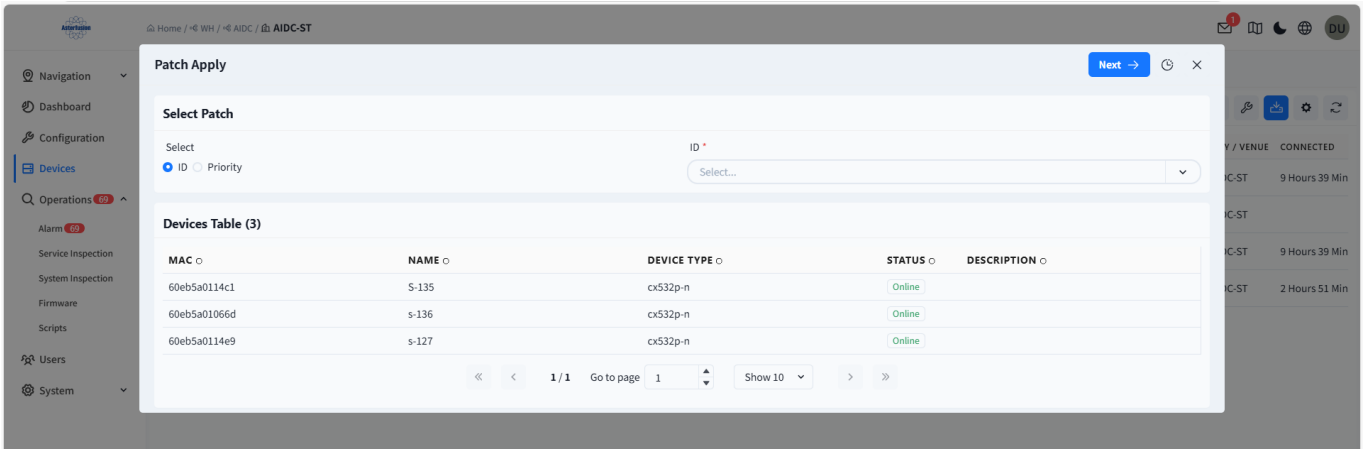


Figure 8.2-3 Executing Patch Application

8.3 Alarm Management

8.3.1 Alarm Item Configuration

Administrators can configure the alarm information and thresholds to be concerned about in the operation and maintenance configuration interface of the venue. By default, all alarms supported by the controller are enabled.

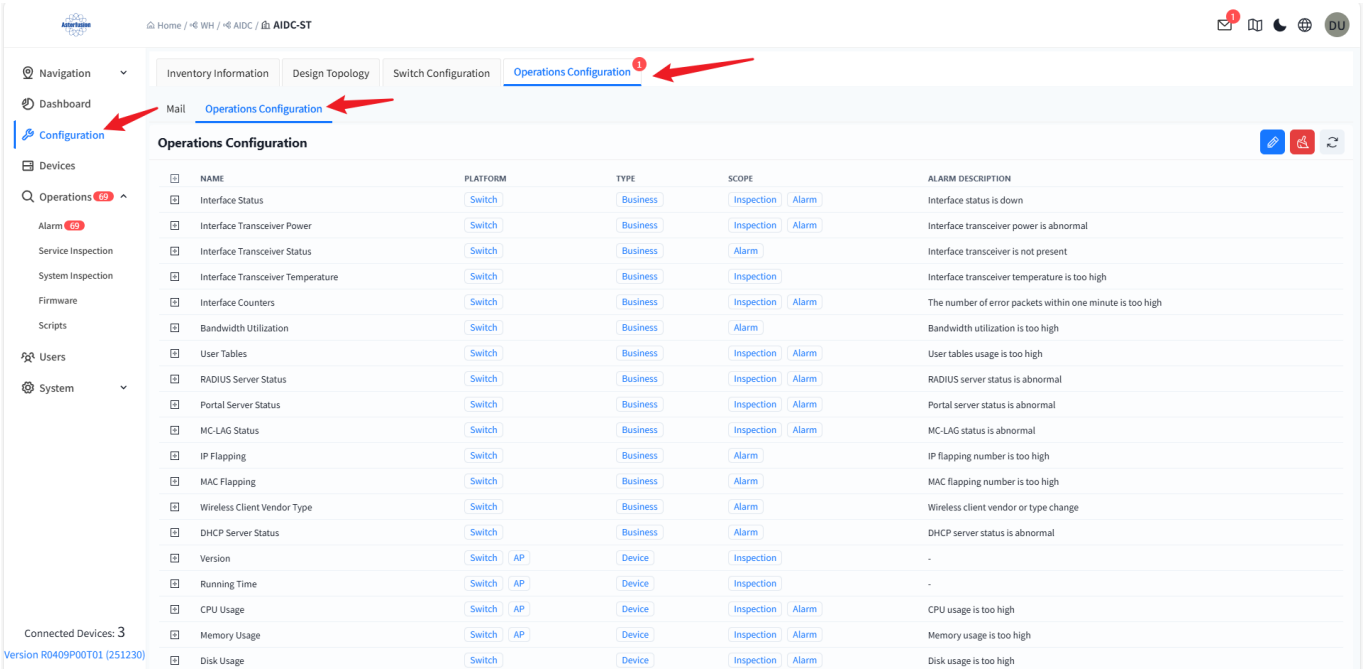


Figure 8.3-1 Alarm Configuration

The alarm content supported by the controller is as follows:

Table 8-1 Alarm content supported

Alarm Category	Alarm Item
Interface Status	Interface UP/Down status switch
Wireless Terminal Type	Manufacturer type corresponding to MAC address changes
Interface Module Optical Power	Optical module optical power
Interface Module Status	Interface module in-place status
Bandwidth Utilization	Bandwidth utilization
User Entry	ARP entry resource utilization
	IPv4-host-route: /32 host route entry resource utilization

Alarm Category	Alarm Item
	IPv4-route: Routing entry resource utilization
	IPv6-host-route: /128 IPv6 host route entry resource utilization
	IPv6-route: IPv6 routing entry resource utilization
	MAC entry resource utilization
	Route-nexthop: Next-hop resource utilization of routing entries
RADIUS Server Status	Detected working status of the RADIUS server
Portal Server Status	Detected working status of the Portal server
MC-LAG Status	MC-LAG protocol working status
IP Drift	Abnormally frequent drift of IP addresses between different switches
MAC Drift	Abnormally frequent drift of MAC addresses between different interfaces of the same switch
Interface POE Status	Interface POE status change
POE Total Power Utilization Rate	The percentage of the current total POE power supply of the POE switch to the rated POE power supply
Device Connection Status	Change in the connection status between the device and the controller
CPU Utilization	-
Memory Utilization	-
Disk Utilization	-
Temperature	CPU core temperature
	FAN fan temperature
	PCB temperature

Alarm Category	Alarm Item
	SWITCH switch chip temperature
Fan	Fan module in-place status
	Fan speed
Power Supply	Power module in-place status
	Power supply status
Core Dump File	Core dump file resource utilization
Container Operation Status	Operation status of each container of the switch
BGP Connection Status	Change in the connection status of BGP neighbors on the switch
BFD Connection Status	Change in the connection status of BFD neighbors on the switch

8.3.2 Sender Email Settings

Click [**System**] - [**Email Sender**] to modify the source email for sending alarm information.

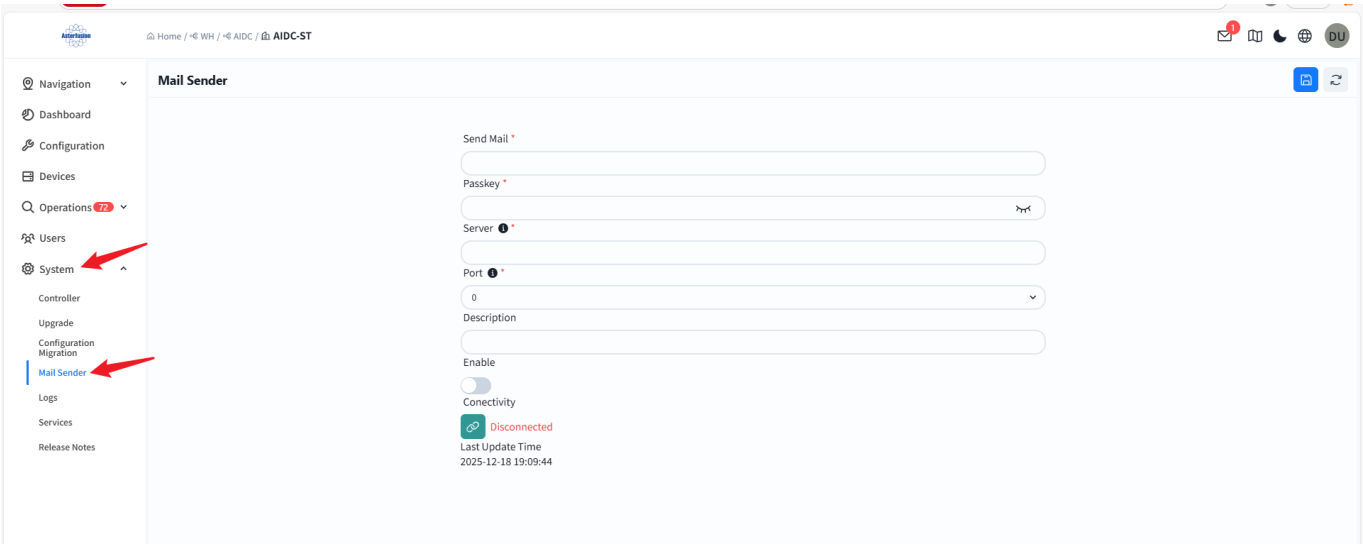


Figure 8.3-2 Configuring Alarm Sender Email

Click the [**Connectivity**] button to test the connectivity between the controller and the email server to avoid failure to send alarm emails due to network connectivity issues.

8.3.3 Alarm Information Viewing

All alarm information under the current organization/venue can be viewed in the [**Alarm**] interface:

- Current Alarms: Displays alarm items that still exist currently.
- Historical Alarms: Displays alarm items that were abnormal before but have returned to normal.

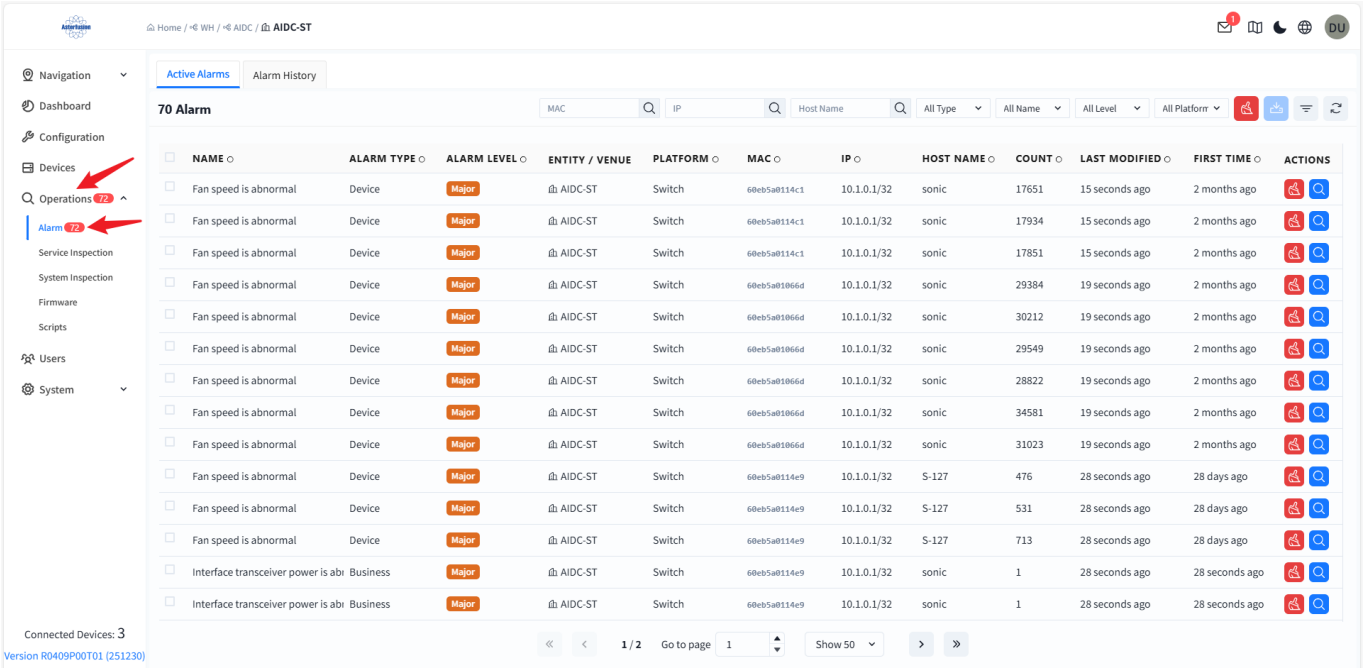


Figure 8.3-3 Viewing Alarm Information

Click the [**View Details**] button to view the specific information of the alarm and process the alarm information. Click the [**Edit**] button, fill in the processing information for the current alarm in [**Analysis**], and click the [**Save**] button to complete the editing. The [Active Alarms] will no longer display this information, but will be stored in [Alarm History] as a processed alarm.

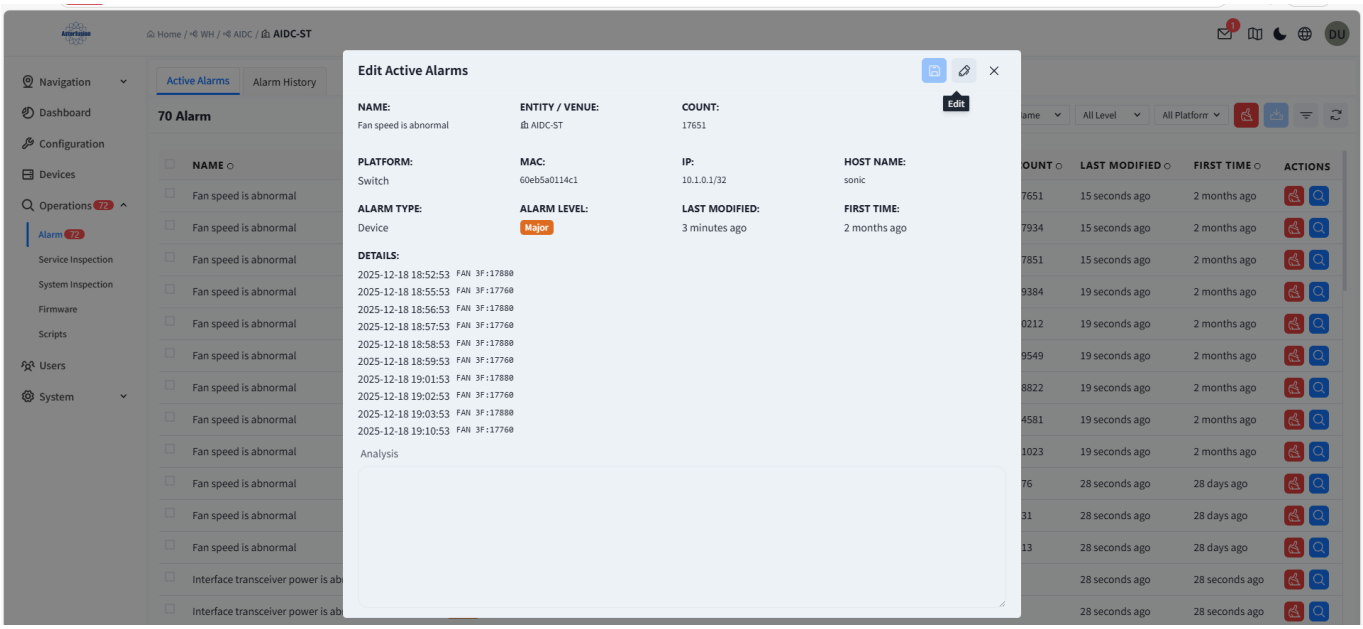


Figure 8.3-4 Editing Current Alarm

8.4 Inspection

The device inspection function aims to regularly check and monitor network devices to ensure their normal operation and timely discover potential faults. Its main functions include:

- Device Status Monitoring: Check CPU utilization, memory utilization, storage status, and port status to ensure the normal operation of the device.
- Log and Alarm Management: Collect device logs, analyze abnormal events, and trigger alarm mechanisms.
- Key Process Status Check: Monitor the operation status of key processes to ensure the normal operation of services.
- Automated Inspection Tasks: Support regular execution of inspection tasks and generate inspection reports to facilitate network maintenance.

8.4.1 system Inspection

System inspection refers to the periodic inspection of the internal system of the controller to ensure its stable and efficient operation. The main inspection items include:

- CPU and Memory Usage: Monitor CPU load and memory consumption to prevent system failures caused by resource exhaustion.
- Storage Status Check: Check disk usage to prevent log or cache data from filling up the storage space and affecting system performance.
- Process and Service Status: Verify whether key services (such as network management, authentication, log recording, etc.) are running normally and automatically restart abnormal processes.
- Email Server Connectivity: Test the connection between the controller and the email server to ensure that alarm notifications can be sent successfully.

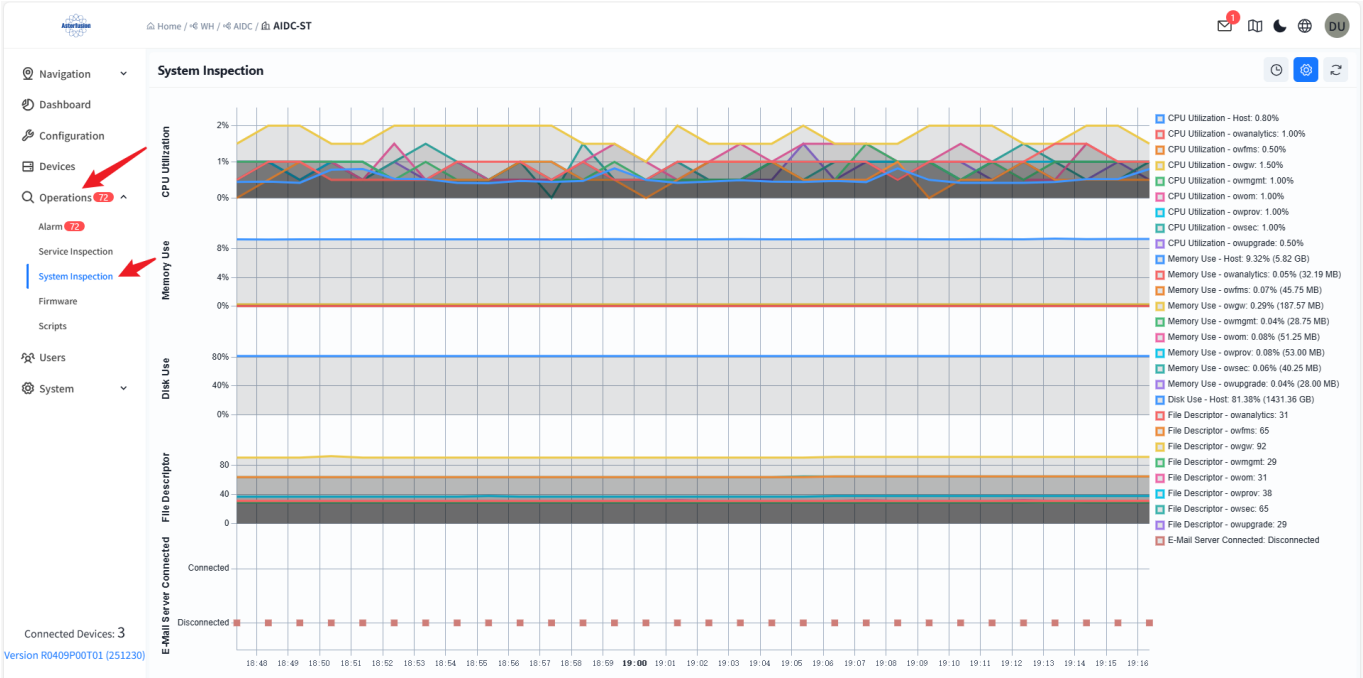


Figure 8.4-1 System Inspection

8.4.2 Service Inspection

Service inspection refers to the regular or on-demand inspection of the operation status of network

devices to ensure stable service operation and prevent potential faults.

8.4.2.1 One-Click Inspection

This function allows users to specify inspection items and devices to be inspected, perform inspections immediately, and define the inspection scope as needed.

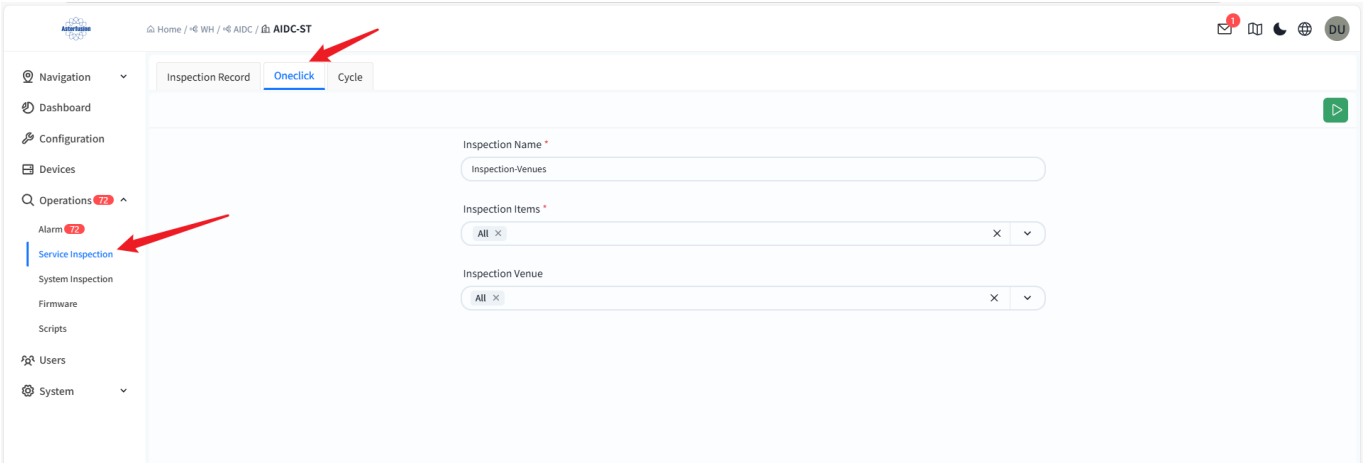


Figure 8.4-2 One-Click Inspection

8.4.2.2 Periodic Inspection

Periodic inspection can be configured according to the needs of different sites, supporting automatic execution of inspections at set time intervals without manual intervention, thereby improving operation and maintenance efficiency.

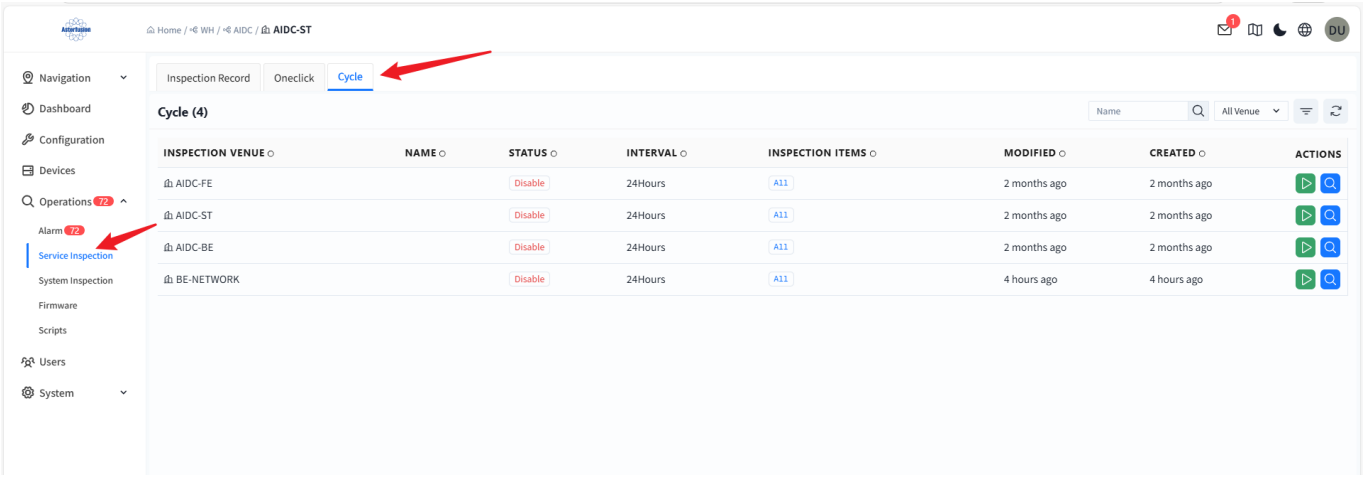


Figure 8.4-3 Periodic Inspection Page

Click the [View Details] button to view/edit the regular inspection settings of the selected site.

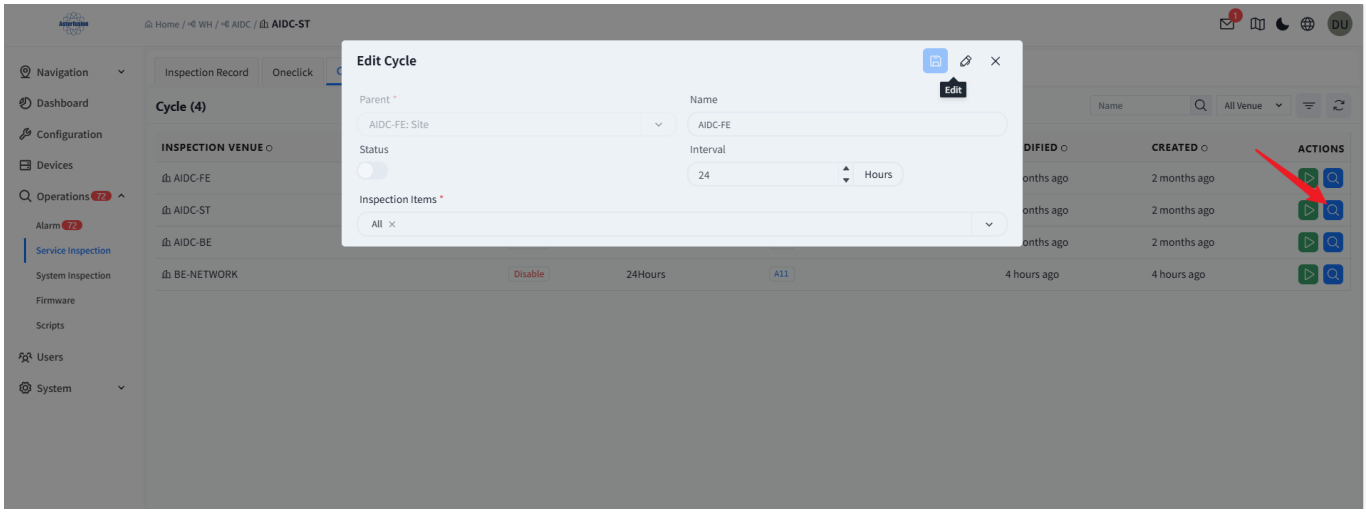


Figure 8.4-4 Edit Periodic Inspection

8.4.2.3 Inspection Records

The results of all one-click inspections and periodic inspections will be recorded in the inspection records. Click the [View Details] button to view the specific inspection results. All detected abnormal items will be listed in the [Abnormal Items] section. Administrators can:

Click [Operation] - [View Details] to view the inspection results of specific devices.

Click the MAC address to directly jump to the device management interface for further analysis.

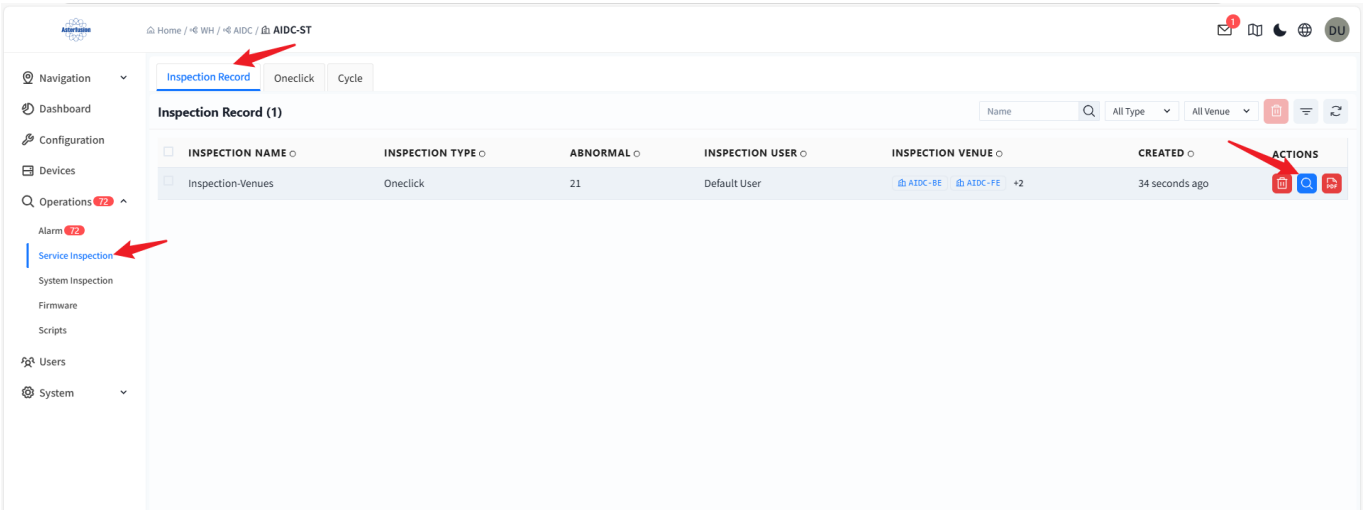


Figure 8.4-5 Inspection Records

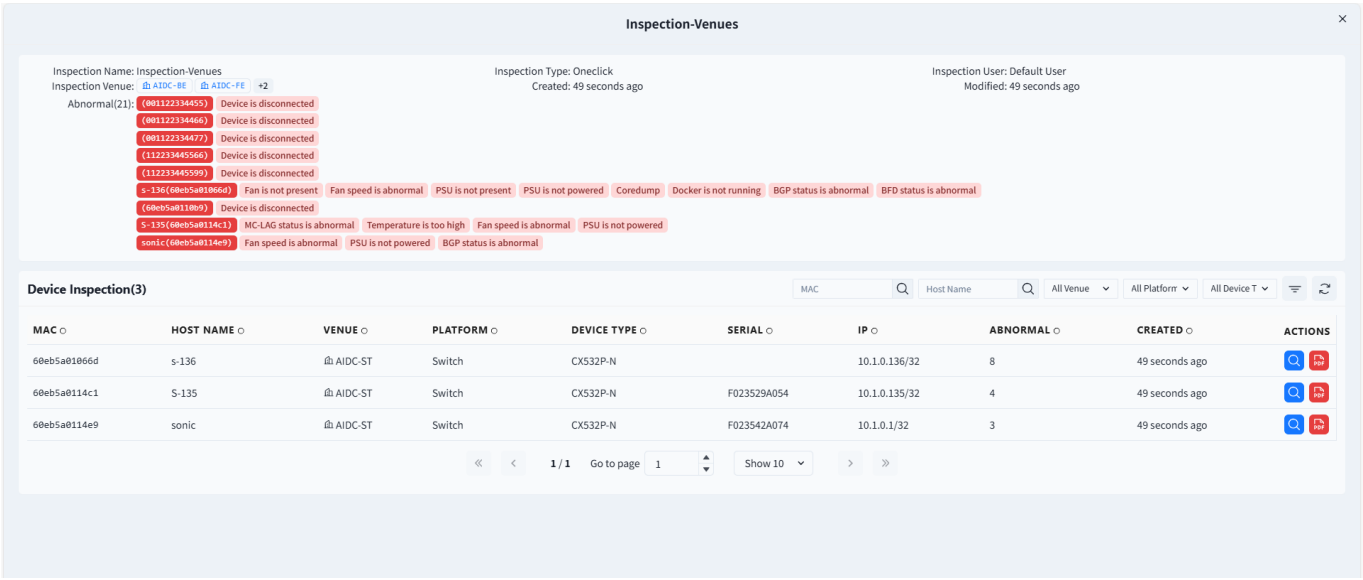


Figure 8.4-6 Detail Inspection Records

9 System Configuration and Upgrade

9.1 Controller Configuration

Users can freely adjust the alarm level and maximum value of each item on the [**System**] - [**Controller**] page.

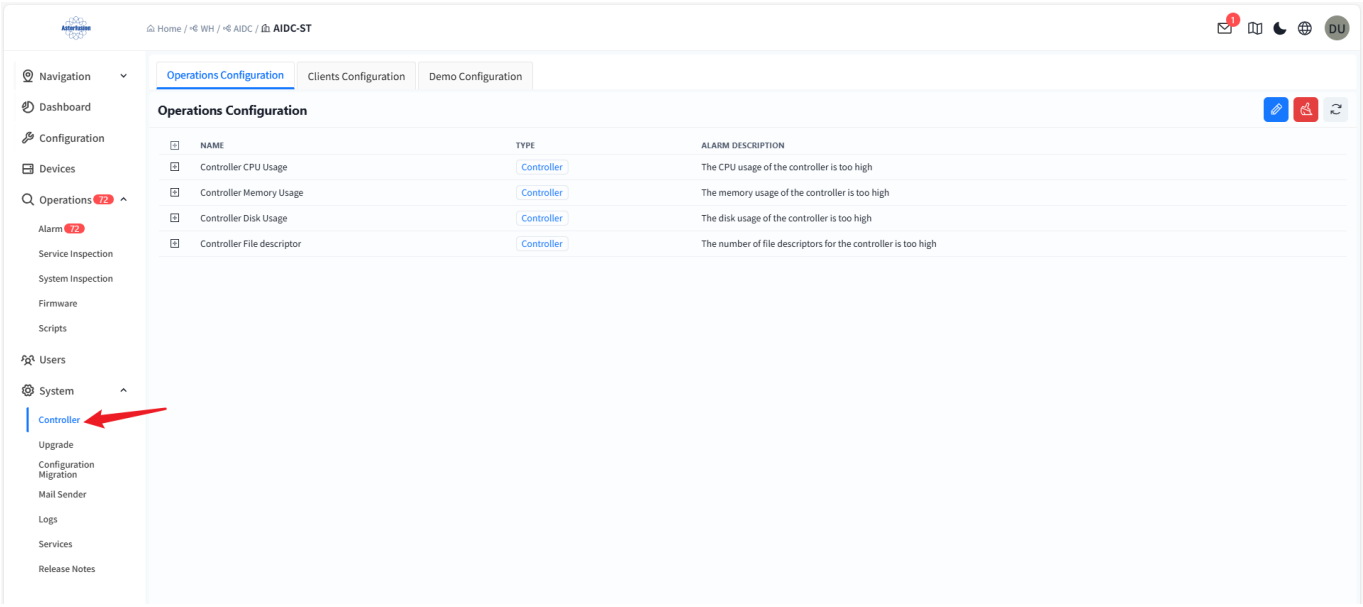


Figure 9.1-1 Controller Configuration

9.2 Controller Upgrade

9.2.1 Firmware Upgrade

Enter the [**System**] - [**Upgrade**] - [**Firmware**] page, click [**+**] in the upper right corner to create firmware.

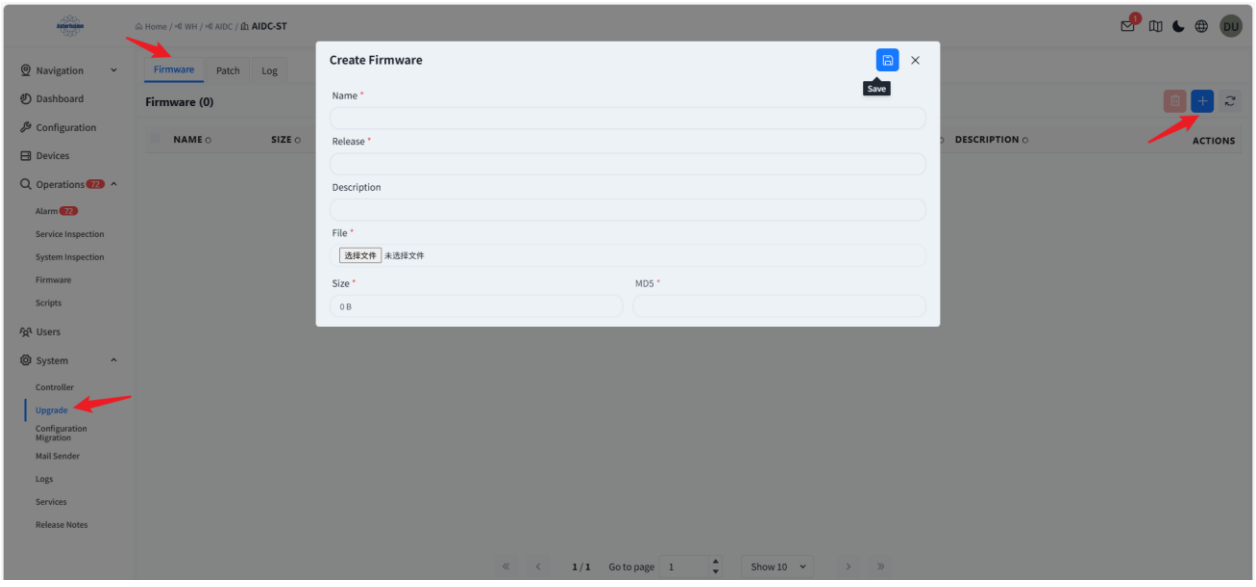


Figure 9.2-1 Creating Controller Upgrade Firmware

Upload the file according to the prompts on the page, fill in the name, version and other information, and click [**Save**] in the upper right corner.

Figure 9.2-2 Creating Controller Upgrade Firmware Details

After uploading, click [**Firmware Upgrade**] - [**Start**] on the right to perform the controller firmware upgrade.

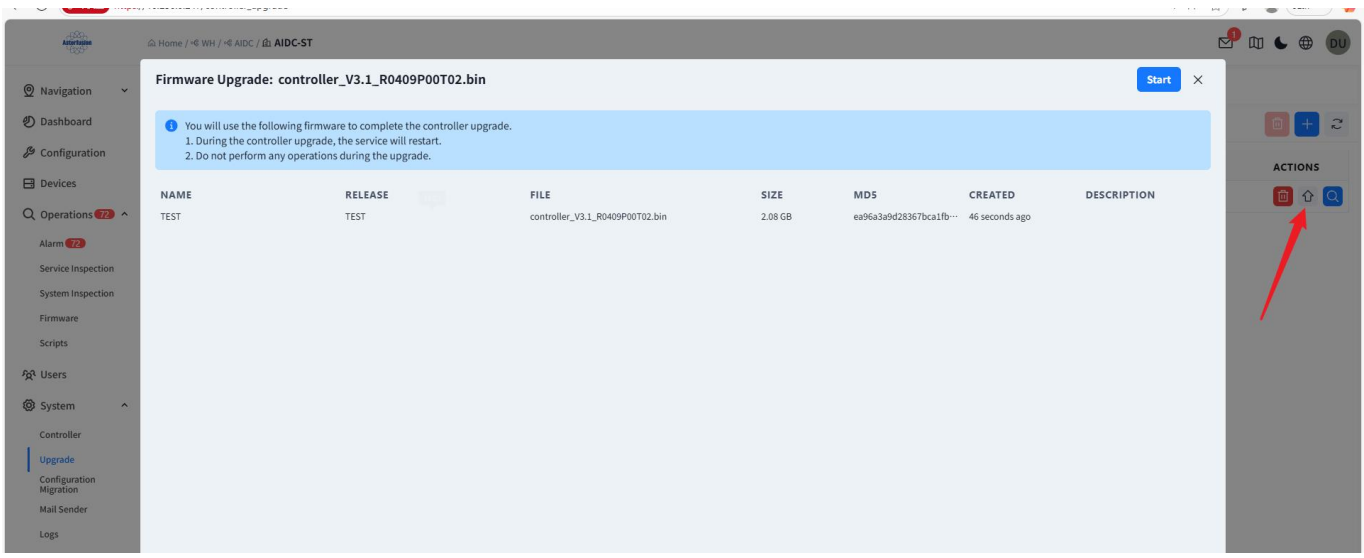


Figure 9.2-3 Executing Controller Upgrade

9.2.2 Patch

Patches can realize precise modification of target files through incremental updates.

Click [**System**] - [**Upgrade**] - [**Patch**] - **[+]** to create a patch.

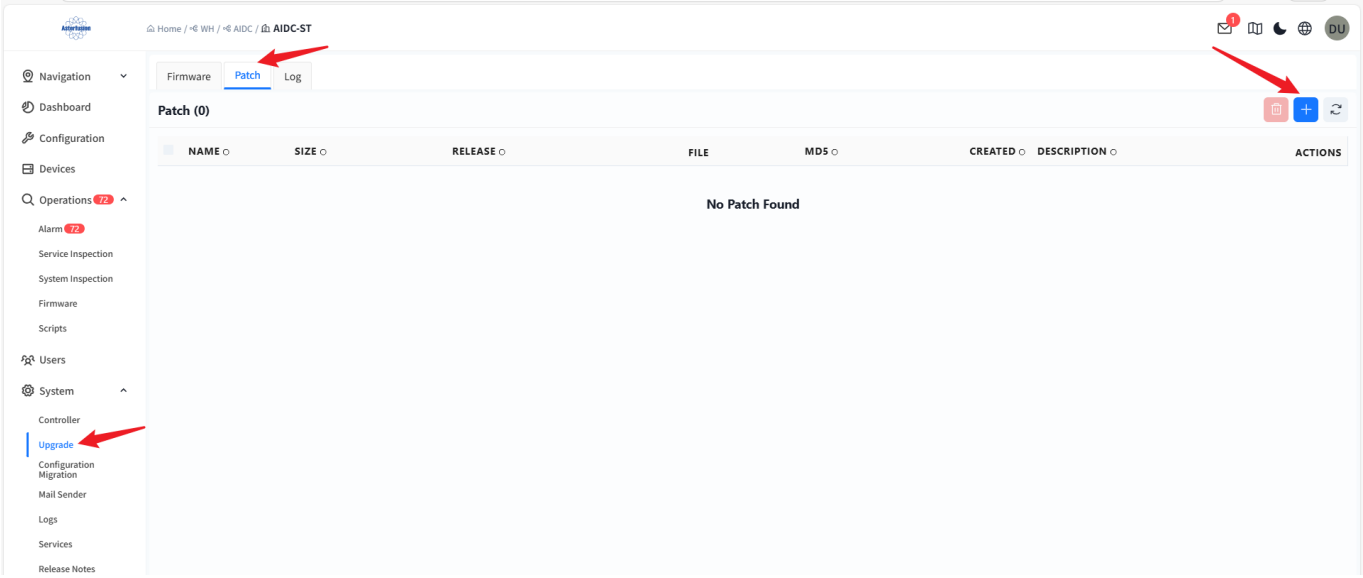


Figure 9.2-4 Creating Controller Upgrade Patch

Upload the file according to the prompts on the page, fill in the name, version and other information, and click [**Save**] in the upper right corner.

Figure 9.2-5 Saving Patch

Click [Patch Application] - [Start] on the right to apply the controller patch.

9.3 Controller Configuration Migration

The controller configuration migration function realizes overall configuration migration through one-click operation, facilitating users to quickly reuse existing configurations when creating a new controller. Enter the [**System**] - [**Configuration Migration**] interface of the original controller, click [**Export Configuration**] - [Click to download the controller configuration file] to export the configuration file.

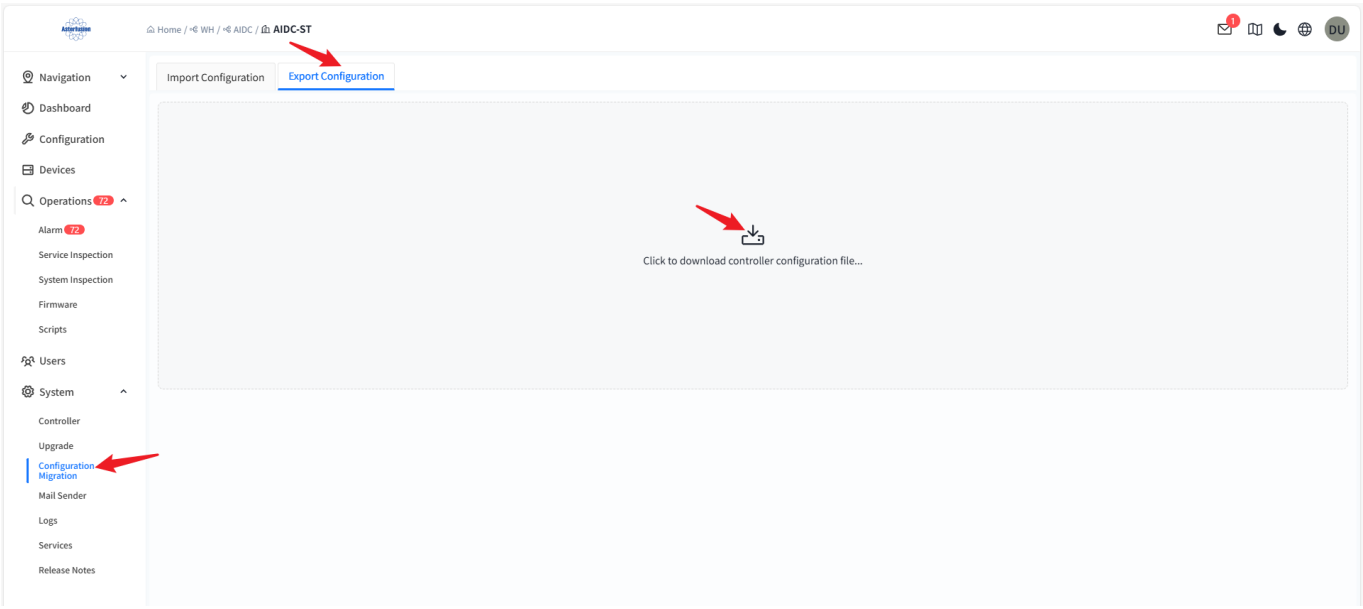


Figure 9.3-1 Exporting Controller Configuration File

In the controller that needs to import the configuration, enter the [**System**] - [**Configuration Migration**] - [**Import Configuration**] interface, click [**Select Fil**e] - [Next].

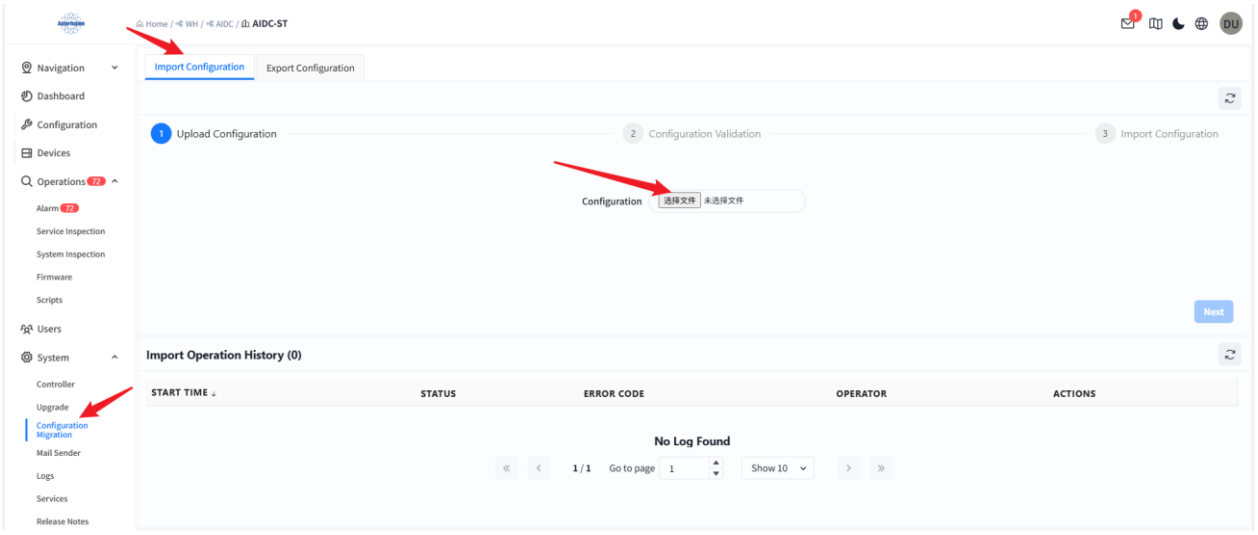


Figure 9.3-2 Uploading Controller Configuration File

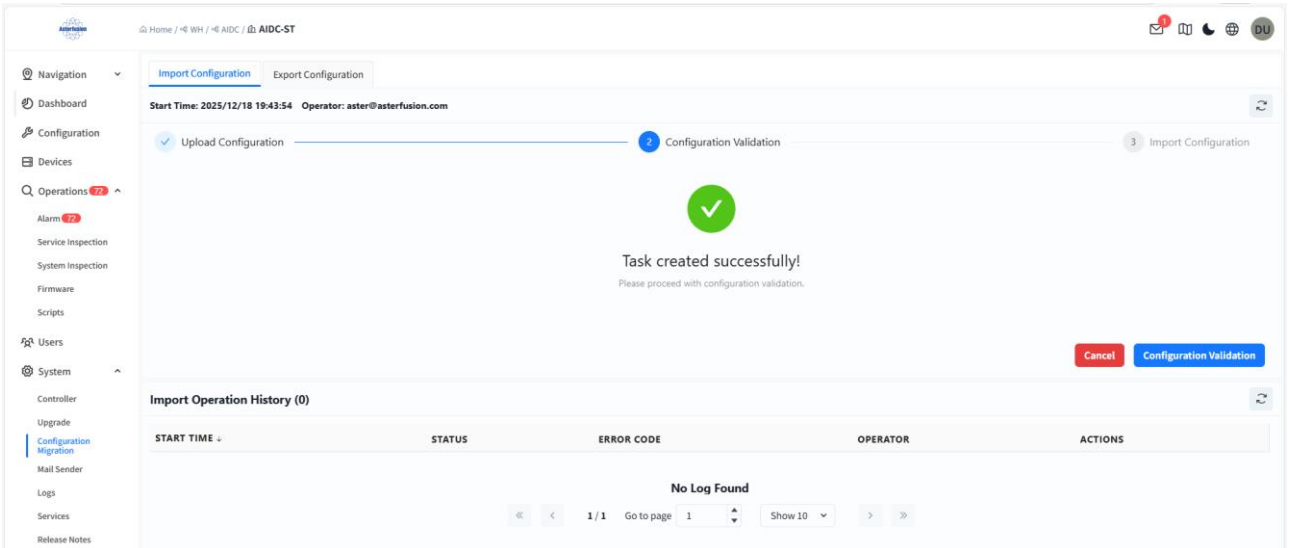


Figure 9.3-3 File Upload Successful

Click [Configuration Verification].

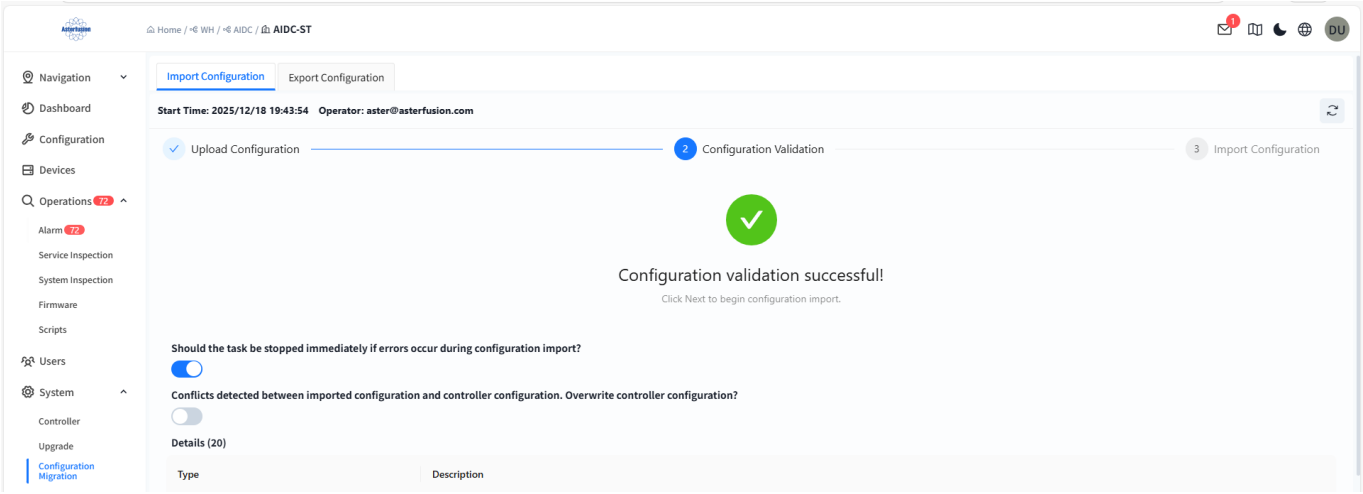


Figure 9.3-4 Configuration File Validation

Pull down the page and click [**Next**] to import the configuration.