User Guide

Campus Controller Usage Guide

Asterfusion Data Technologies Co., Ltd

Contents

1 Controller Deployment Environment Preparation

1.1 On-premises Deployment

Recommended deployment environment:

X86 sever

Linux Version: Ubuntu 18.04 LTS or later

Docker Version: 20 or late

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

1.2 Cloud Deployment

- Open the business port

Deploying an ACC controller on a cloud host requires opening some business ports, with the following ports and their purposes:

Network Type	Authorization Direction	Authorization Policy	IP Protocol	Port Range	Priority	Source IP Address Range	Describe
intranet	ingress	Accept	TCP	16011/16011	1	0.0.0.0/0	owom (operation and maintenance alarm) external HTPPS service port (component under development, not yet released)
intranet	ingress	Accept	TCP	16006/16006	1	0.0.0.0/0	0wsub (subscription) external HTTPS service port
intranet	ingress	Accept	TCP	15002/15002	1	0.0.0.0/0	owgw Southbound Interface, Device Connection

							Controller Service Port
intranet	ingress	Accept	TCP	16002/16003	1	0.0.0.0/0	owgw (Gateway) external HTTPS service port
intranet	ingress	Accept	TCP	16004/16004	1	0.0.0.0/0	owfms (Firmware) external HTTPS service port
intranet	ingress	Accept	TCP	16009/16009	1	0.0.0.0/0	owanalytics (analysis) external HTTPS service port
intranet	ingress	Accept	TCP	16005/16005	1	0.0.0.0/0	owprov (configuration) external HTTPS service port
intranet	ingress	Accept	TCP	16001/16001	1	0.0.0.0/0	owsec (Authentication) external HTTPS service port
intranet	ingress	Accept	TCP	5912/1913	1	0.0.0.0/0	owgw service, RTTY remote connection function
intranet	ingress	Accept	TCP	443/443	100	0.0.0.0/0	owgw-ui （WEBUI） external service port
intranet	ingress	Accept	TCP	22/22	100	0.0.0.0/0	System created rule.SSH port

- Generate certificate

Assuming the domain name is: cloudswitch.io

Apply for a certificate on the cloud server using Let's Encrypt's official tool, Certbot:

```
sudo apt install certbot
certbot certonly --standalone -d cloudswitch.io --key-type rsa
```

The new certificate is located at:/etc/letsencrypt/live/cloudswitch.io

Introduction to Certificate File Generation by Certbot:

- privkey.pem

Server private key file. Used for encrypting and decrypting SSL communication, it can only be held by the server and must be strictly kept confidential.

- fullchain.pem

Complete certificate chain file. Contains your server certificate and all intermediate CA certificates, typically used for configuring SSL_certificate for web servers such as nginx and Apache.

- chain.pem

Only includes intermediate CA certificates. Used for client verification of the legitimacy of your server certificate, some services (such as nginx's OCSP sampling) require separate configuration.

- cert.pem

Only includes your server certificate (excluding intermediate certificates). It is generally not recommended to use it alone, as it can lead to incomplete certificate chains and inability for clients to verify.

Practical usage suggestions:

-Web services typically use fullchain.exe and privkey.exe.

-Chain.Pem is used in scenarios where a separate CA chain is required.

-It is not recommended to use Cert.Pem directly unless there are special requirements.

- Copy the certificate to the controller directory

```
cd /etc/letsencrypt/live/cloudswitch.io
sudo cp -L cert.pem /path-to-ACC-controller/controller_V1.0_R005/wlan-cloud-ucentral-deploy/docker-compose/certs/restapi-cert.pem
sudo cp -L privkey.pem /path-to-ACC-controller/controller_V1.0_R005/wlan-cloud-ucentral-deploy/docker-compose/certs/restapi-key.pem
sudo cp -L chain.pem /path-to-ACC-controller/controller_V1.0_R005/wlan-cloud-ucentral-deploy/docker-compose/certs/restapi-ca.pem
```

2 Deployment Steps

The following deployment commands require root privileges. For non root users, sudo needs to be added before the command.

1. Upload the controller package file to the target deployment environment and perform a one-click installation. Use the –i parameter to specify the controller IP address.

```
./controller_V1.0_R07.bin –i <ip_address>
```

```
aster@ccn:~$ sudo ./controller_V1.0_R07.bin -i 192.168.0.91
[2025-07-08 16:20:19] ============= Start deploying controller controller_V1.0_R07================
[2025-07-08 16:20:19] ============= deploy direction </opt/controller> ================
CONTROLLER_UPGRADE_TASK:check environment
```

Users can directly access the controller via this IP address.

[Note]

When upgrading from versions prior to R7 to versions post-R7 while retaining existing configurations, perform the installation without the –i parameter.

```
./controller_V1.0_R07.bin
```

2. Start the controller using Docker-Compose. The default installation directory for the controller is /opt/controller/

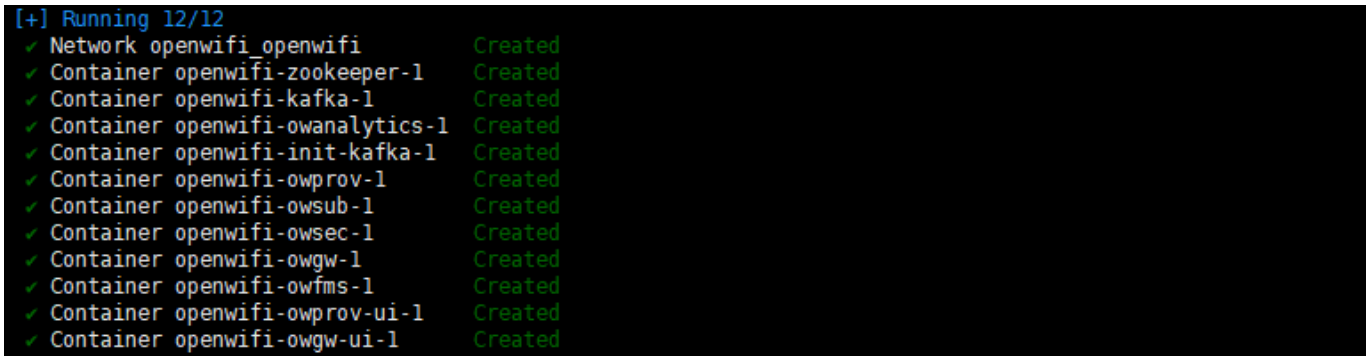
```
cd /opt/controller/controller_V1.0_R07/wlan-cloud-ucentral-deploy/docker-compose/
docker-compose up -d//or ‘docker compose up -d’ Different versions of Docker correspond to slightly different commands
```

[Description]

-d : runs the command in the background.

up : starts the controller.

down : stops the controller.



3 Controller Login

It is recommended to log in using Chrome or Edge browser.

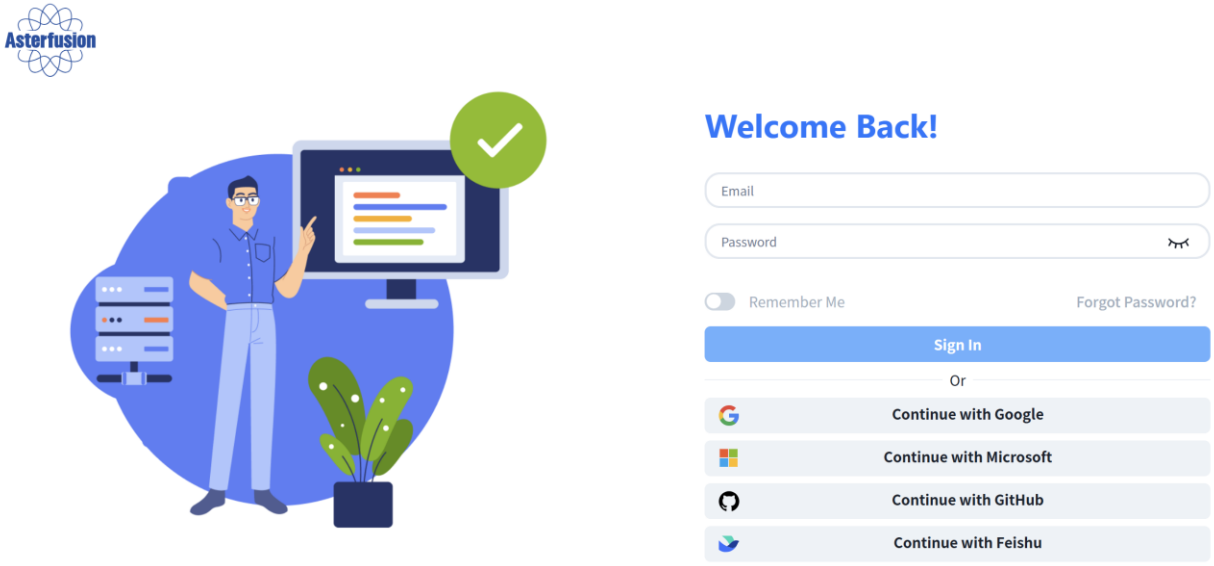
Enter the controller IP address in the browser (for example, 192.168.0.91 in the above use case), and you can enter the controller login page.

3.1 Email & Password

Default login information for the controller:

Email: aster@asterfusion.com

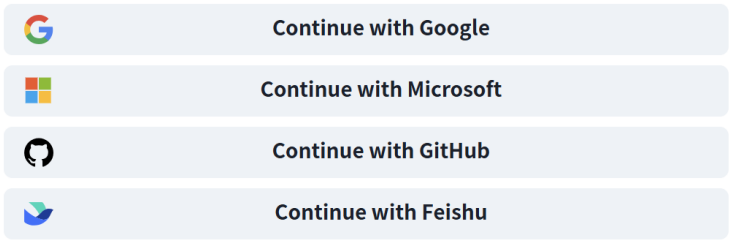
Password: Asteria



3.2 OAuth2.0

OAuth 2.0 is the de facto standard for authorization and is widely used on the Internet. An application securely acquires limited access to another application's protected resources, such as a user's personal profile or data, without exposing passwords or other credentials. The Xingrongyuan controller adopts a more secure and standardized authorization Code process and Proof Key for Code Exchange (PKCE) to ensure the security of user information.

Currently, four common identity providers (IDPs) are supported: Google, Microsoft, GitHub, and Feishu. We strictly follow the open standard OpenID Connect based on the OAuth 2.0 authentication framework, which has been verified in practice.



By default, the user permission for logging into the controller in this way is a normal administrator. Have a freely editable personal space and a Demo environment with only viewing permissions to experience the real live network running environment demo at any time. System administrators can adjust permissions on the **[User]** view.

The configuration of the controller demonstration environment is referred to in Section 10.1.3. For

details on permission adjustments, please refer to Section 9.3.

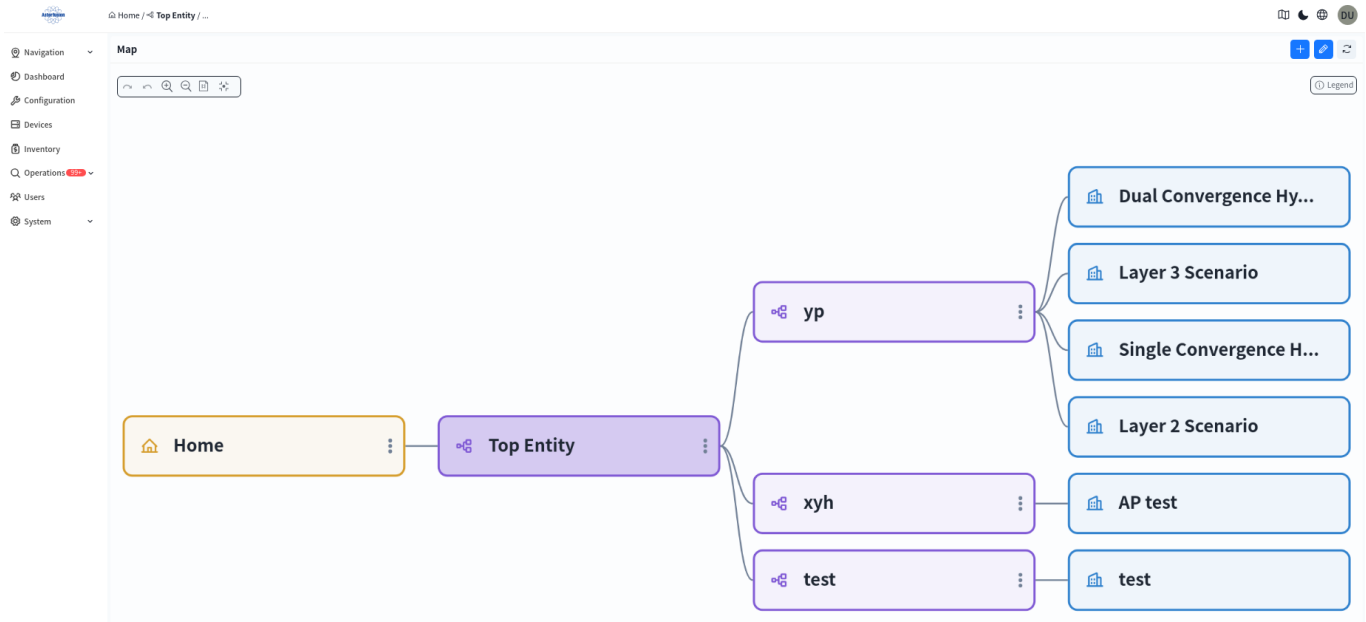
4 Organization and Inventory Management

The controller supports multi-organizational structures, allowing multiple venues to be divided under each organization for independent management. When the controller is deployed in a cloud environment, different organizations can be separately managed by different administrators, enabling parallel usage by multiple organizations and users.

After logging into the controller, the system will default to the **[Navigation] - [Map]** page, as shown below. This page displays all organizations visible within the current user's permissions 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 content within their permissions.

On the Map page, administrators can manage existing organizations and venues or create new organizations or venues as needed. Double-click an organization or venue node switches to the device view under that area, enabling operations such as network device deployment, monitoring, and maintenance.

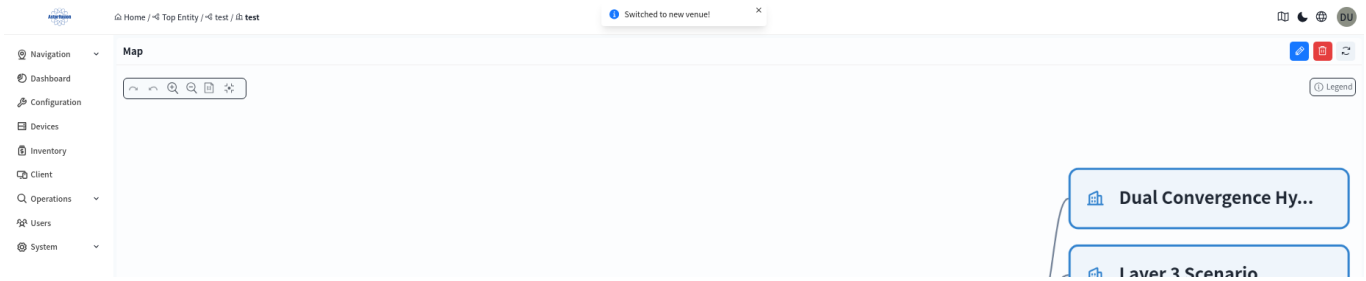
By default, the left-side navigation bar displays aggregated device information across all organizations within the user's permissions. When a user enters a specific organization/venue via the **[Map]**, the system focuses on that area and shows detailed information about all its devices, facilitating refined management.



4.1 Create an Organization

click the **[+]** in the upper right corner to add an organization.

Double-click the created organization to go under the organization:

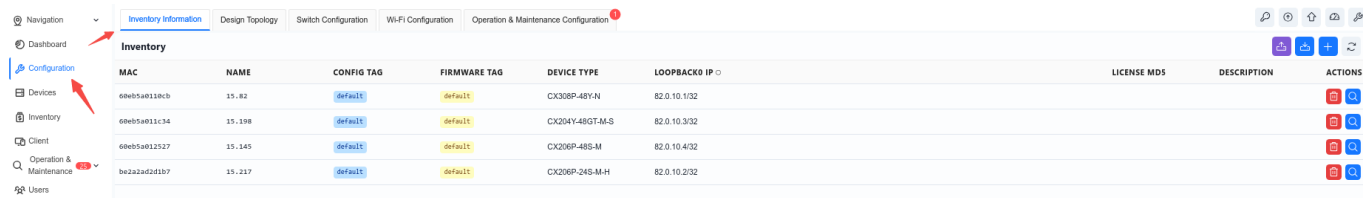


click the **[+]** to add a venue.

The venue is a collection where administrator can monitor, manage, and configure all network devices.

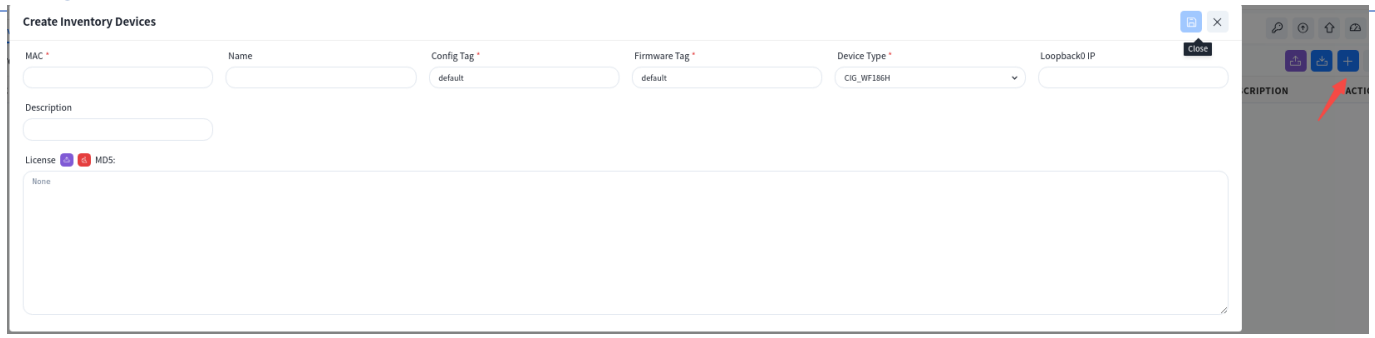
4.2 Adding Inventory

4.2.1 Add Devices

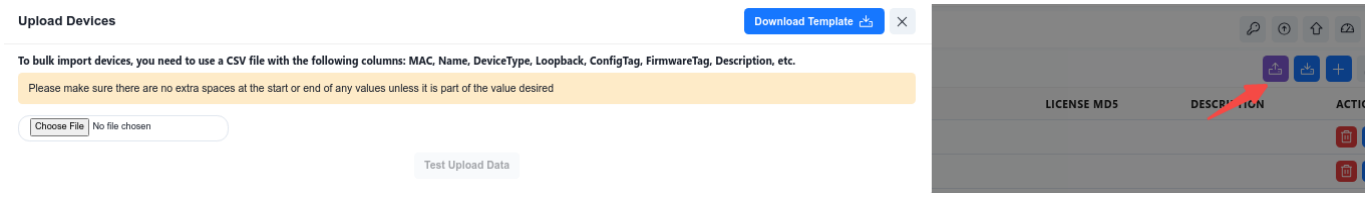


The administrator can add inventory devices to the organization/venue by creating or batch importing them under the venue. Up to this point, once the device is online, the controller will compare the MAC address of the online device, corresponding to the device in the inventory, and assign it to the specific organization/venue.

- Add devices one by one.



- Use the excel file to upload devices.



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

MAC	DeviceType	Name	ConfigTag	FirmwareTag	Loopback	AclScaleProfile	Description

Required Fields:

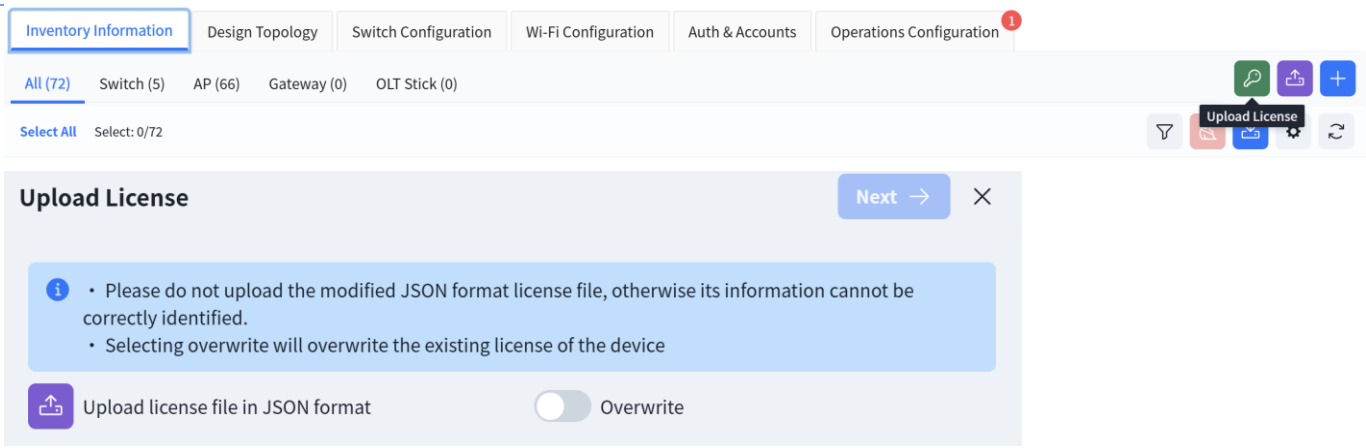
- MAC: The MAC address of the device, usually labeled on the device.
- Device Type: The model of the device.
- Config Tag: After connecting to the controller, the AP will automatically pull the configuration file corresponding to this tag. By default, the tag value is "default".

Optional Fields:

- Name: The hostname of the device.
- Firmware Tag: When upgrading device firmware, you can filter devices to be upgraded by firmware tag type. By default, the tag value is "default".
- Loopback: The Loopback address of the device, which serves as the in-band management address for all Layer 3 devices.
- Description: The information of the device.
- AclScaleProfile: This refers to the support capability and technical parameters of the ACL (Access Control List) function by network devices (switches). Some models of switches offer optional default/large scale. By default, the tag value is set to default.

4.2.2 Upload License

Click **[Configuration]** – **[Inventory]** – **[Upload License]**



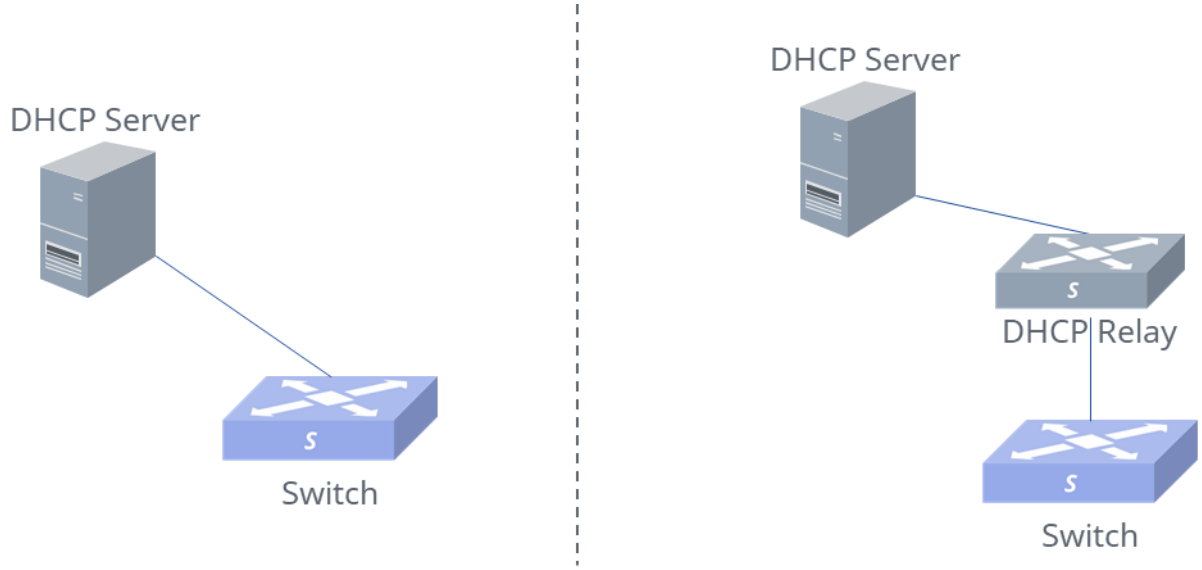
Note: For APs without an authorized License, the radio frequency (RF) function will be turned off by default. Only after the License has been successfully validated can the RF switch be turned on.

5 Device Connect to Controller

5.1 Switch

5.1.1 Dynamically obtain the controller IP through the DHCP server

All Asterfusion devices can act as DHCP clients. Under the factory default configuration, they will actively send DHCP request to obtain the management IP address and the controller IP address.



To ensure that devices can obtain the controller IP through DHCP requests, the DHCP server must be capable of responding to the option 138 field. The following is a configuration example for the ISC-DHCP server:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.0.100 192.168.0.200;
  option routers 192.168.0.1;
```

```
option subnet-mask 255.255.255.0;
option capwap-ac-v4 "192.168.0.91";
```

[Description]

192.168.0.91 is the IP address of the controller.

In this case, configure the DHCP server and DHCP Relay (if any) as needed. After the switch is powered on and the physical connections are completed, you can see the switch go online on the [Devices] page of the controller.

5.1.2 Connect to Controller by Command Line

If the DHCP server does not exist in the network, or the DHCP server cannot be configured with the controller address, the user can use the command **ucentral-client server <A.B.C.D>** to configure the IP address of the controller 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, users need to specify the VRF parameter when designating the management address, for example: **ucentral-client server <A.B.C.D> vrf mgmt**.

The following is a sample configuration for switch:

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

```
sonic# config
sonic(config)# ucentral-client 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
```

Use in-band management to connect to the controller. Take the Ethernet49 port as an example:

```
sonic# config
sonic(config)# ucentral-client enable
```

```
sonic(config)# ucentral-client server 192.168.0.91
sonic(config)# interface ethernet 49
sonic(config-if-49)# ip address 192.168.0.20/24
sonic(config-if-49)# exit
sonic(config)# ip route 0.0.0.0/0 192.168.0.91
```

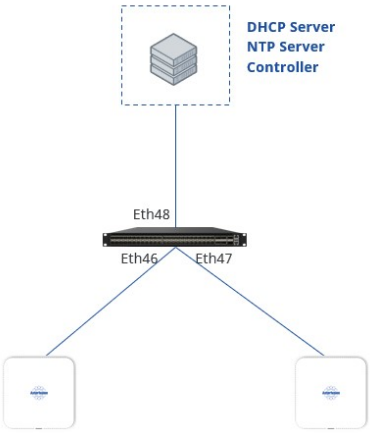
After the configuration is completed, you can see the switch go online on the **[Devices]** page of the controller.

5.2 AP

In the factory default configuration, the AP will actively send a DHCP request to request the management IP address and the controller IP address.

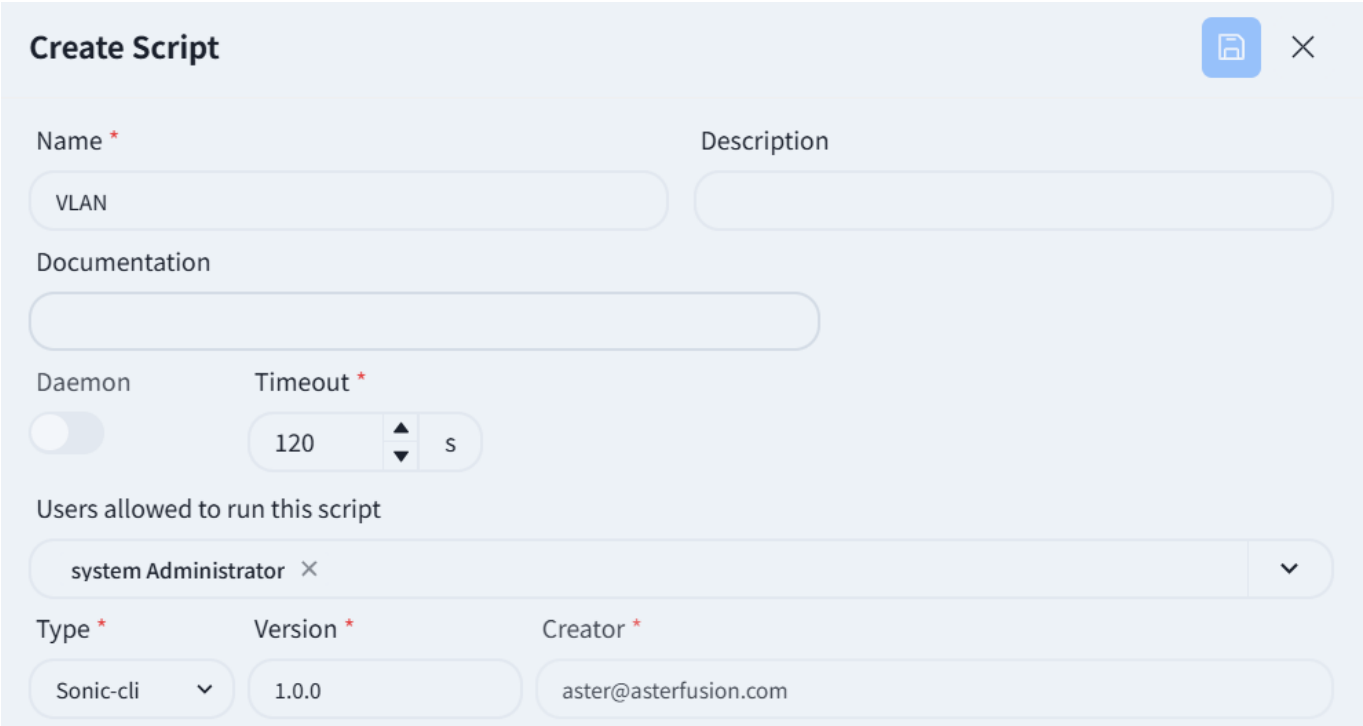
5.2.1 There is Already a DHCP Server in the Network

If there is a DHCP server in the network and the configuration has been completed according to Section 5.1.1.



Since the AP is not directly connected to the DHCP server, it is necessary to use the script function or directly enter the switch background to configure through the command line. Configure the VLAN broadcast domain on the switch device directly connected to the AP to broadcast the DHCP request of the AP to the DHCP server.

After entering the venue, click **[Operation]** - **[Script]** to enter the script editing view. Click the **[+]** in the upper right corner to create a new script, and select the script type as Sonic-cli.

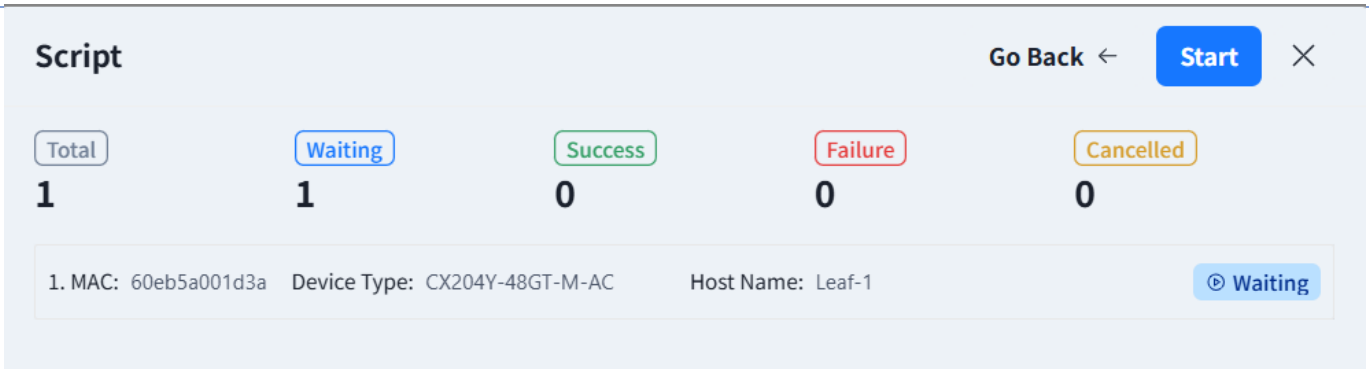


Script content:

```
configure
interface ethernet 48
no router-interface
exit

vlan 4010
exit

port-group ethernet 46-48
switchport access vlan 4010
exit

interface vlan 4010
ip address dhcp-alloc
```

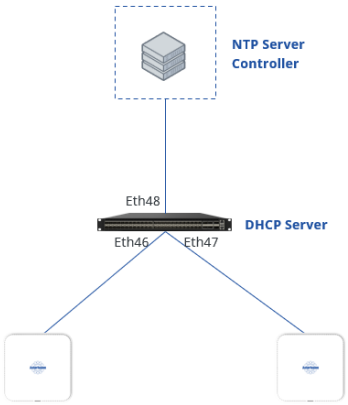
After completing the configuration, click Save.

Enter the device view, select the switch connected to the AP, and click the **[Actions]** - **[Script]** button in the upper right corner. Select the script edited in the previous step, click **[Next]** - **[Start]**, and send the script to the switch.

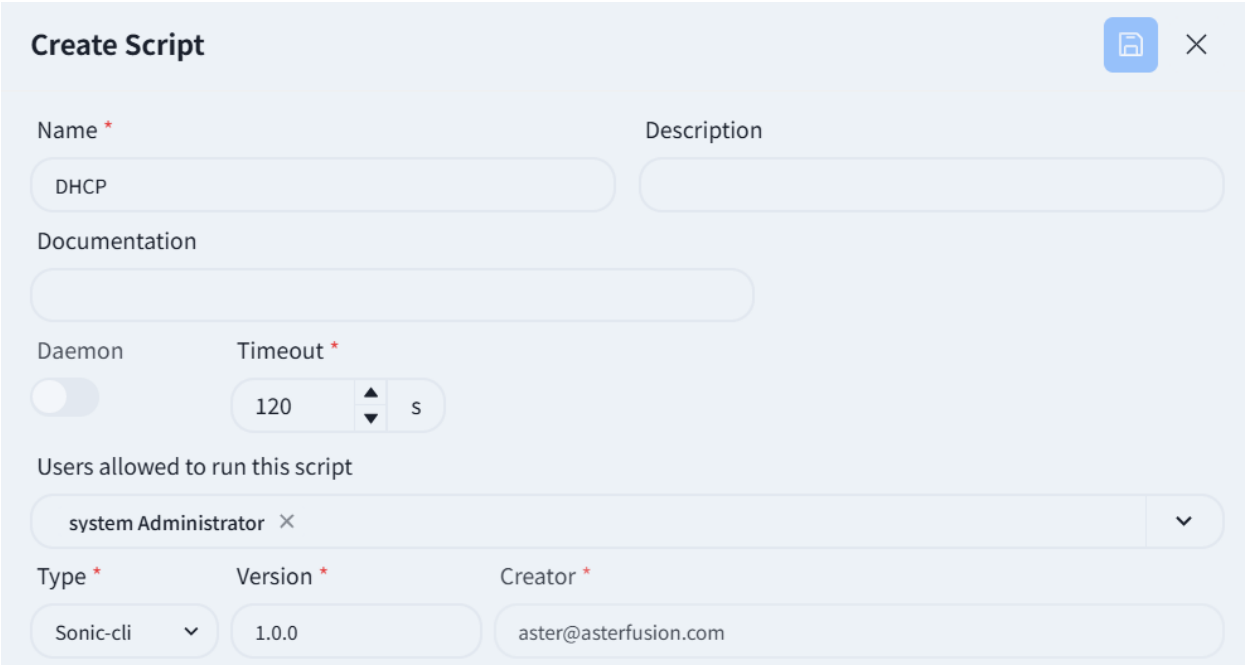


5.2.2 There is no DHCP Server in the Network

If there is no DHCP server in the network, you need to configure the switch to act as a DHCP server, assign management IP addresses to the APs, and inform them of the controller's IP address.



After entering the venue, click **[Operation]** - **[Script]** to enter the script editing view. Click the **[+]** in the upper right corner to create a new script, and select the script type as Sonic-cli.



Script content:

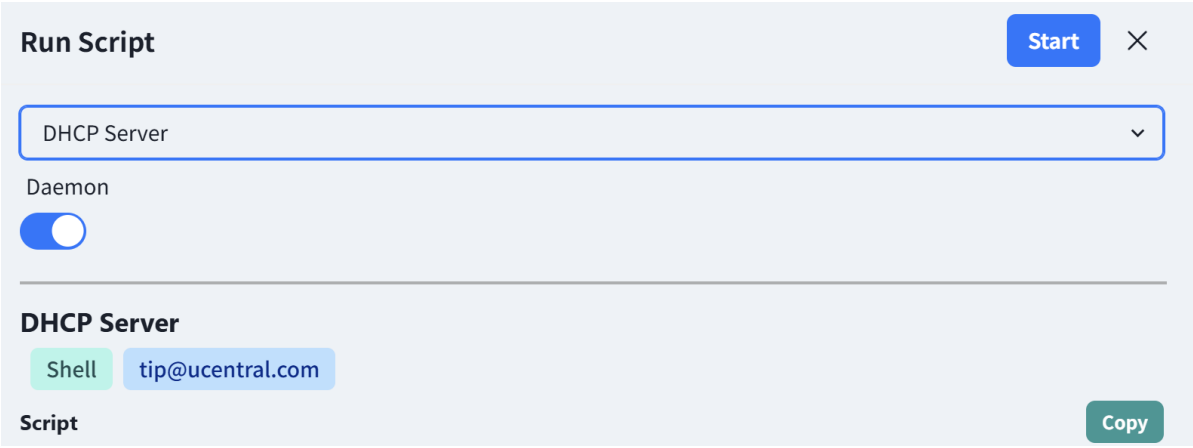
```
configure
interface ethernet 48
```

```
no router interface
exit

vlan 4020
exit

port-group ethernet 46-48
switchport access vlan 4020
exit

interface vlan 4020
ip address 192.168.0.1/24
dhcp select server
exit

dhcp pool ap
address pool 192.168.0.100 192.168.0.200
lease-time 3000 6000
network 192.168.0.0 255.255.255.0
routers 192.168.0.1
capwap-ac 192.168.0.91
```

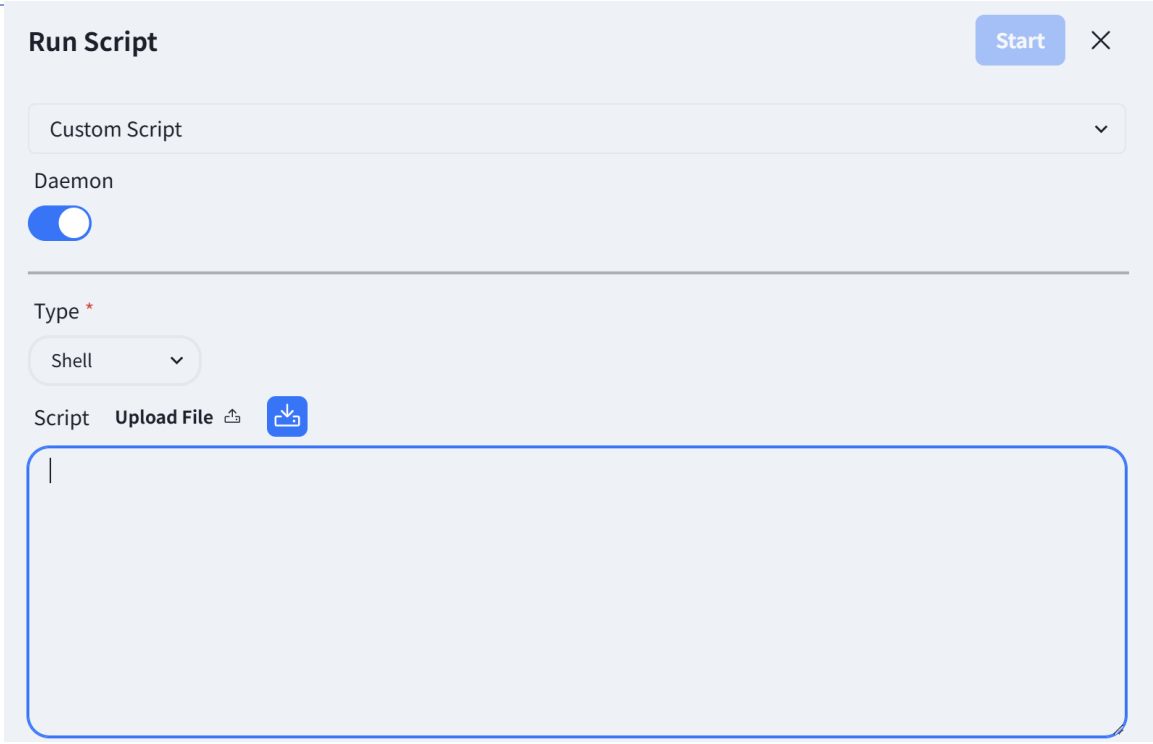
Note: 192.168.0.91 is the IP address of the controller.

After completing the configuration, click Save.

Enter the device view, select the switch connected to the AP, and click the **[Actions]** - **[Script]** button in the upper right corner. Select the script edited in the previous step, click **[Start]**, and send the script to the switch.



Users can also directly select custom scripts on the script running page shown in the picture, fill in script content or upload script files and run them directly on this page.



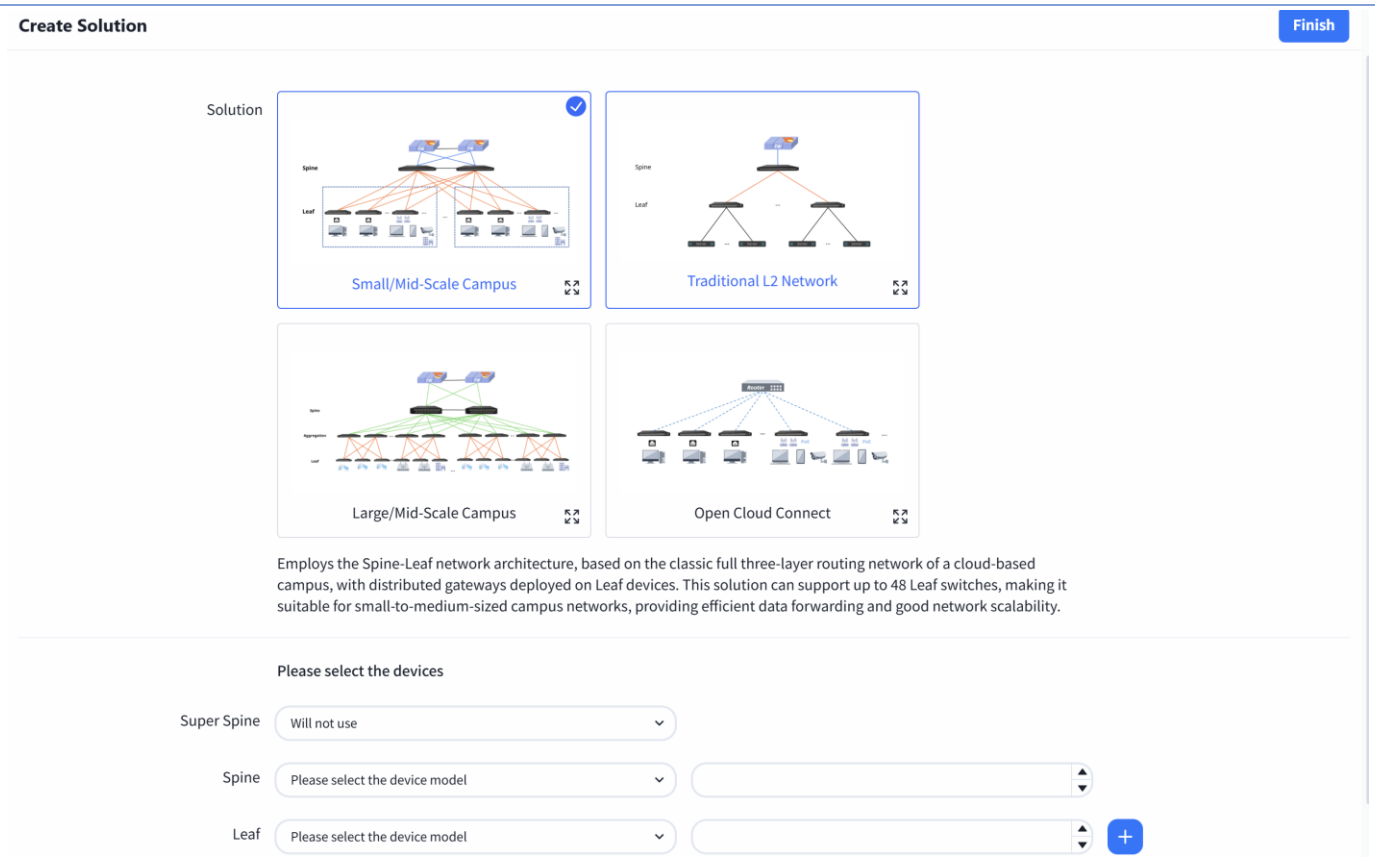
5.3 OLT Stick

In its factory default configuration, the OLT Stick will actively send a DHCP request to obtain a management IP address and a controller IP address. Its online activation method is the same as that of APs.

6 Services Configuration

To simplify the configuration of common typical network setups, the controller has four built-in scenarios: Small/Mid-Scale Campus, Large/Mid-Scale Campus, Traditional L2 Network, and Open Cloud Connect. Administrators can select any network setup according to the network scale to complete topology planning. After all devices in the planned topology are online and connected to the controller, the ACC will automatically detect and identify the connection status between devices to generate a real network topology. Administrators can check whether the topology is correct, and after confirming it is error-free, deploy the configuration to the devices to complete network configuration and deployment.

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



- Small/Mid-Scale Campus

This is a full L3 network solution with a two-tier Spine-Leaf architecture, for example, using the CX308 series as the Spine devices and the CX204Y-48GT series as the Leaf devices: each Spine device can provide up to 48 interfaces to connect with Leaf devices, and each Leaf device offers 48 access interfaces. Thus, the network can support up to **48 x 48 = 2304** access interfaces. This scenario is suitable for smaller scale network.

- Large/Mid-Scale Campus

This is a full L3 network solution with a three-tier Spine-Aggregation-Leaf architecture, for example, using the CX308 series as Spine devices, the CX206P-24S series as Aggregation devices, and the CX204Y-48GT series as Leaf devices: each Spine device can provide up to 48 interfaces to connect with Aggregation devices, each Aggregation device can provide up to 24 interfaces to connect with Leaf devices, and each Leaf device offers 48 access interfaces. Thus, the network can support up to **48 × 24 × 48 = 55,296** access interfaces. This scenario is suitable for larger scale network.

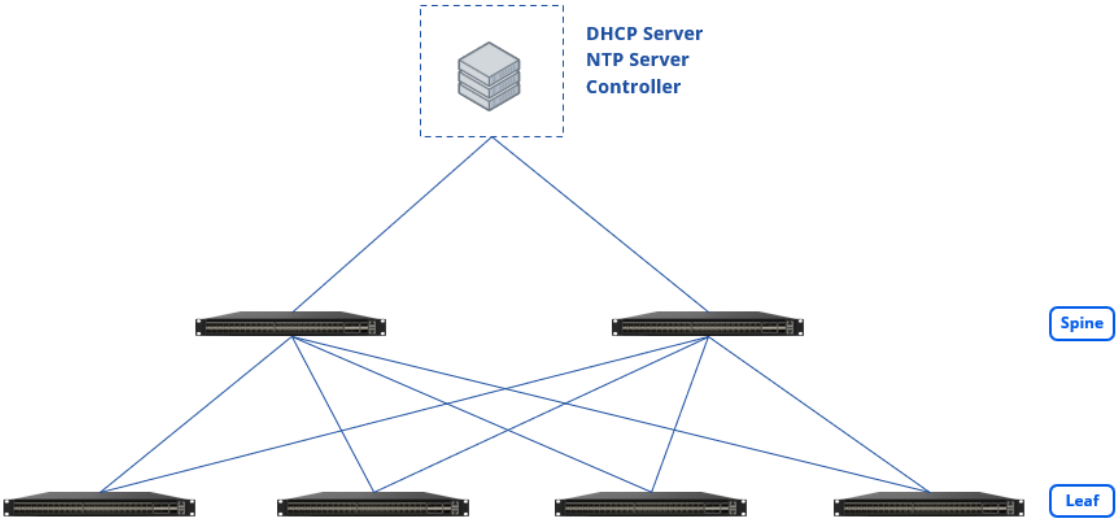
- Traditional L2 Network

Traditional L2 network solution, Spine-Leaf L2 architecture, Leaf for pure L2 access, gateway deployed on Spine device.

- Open Cloud Connect

The gateway is deployed on aggregation or access devices. Suitable for scenarios where there are already aggregation devices or access layer expansion in the park, providing two classic modes: layer 2 forwarding and access layer gateway.

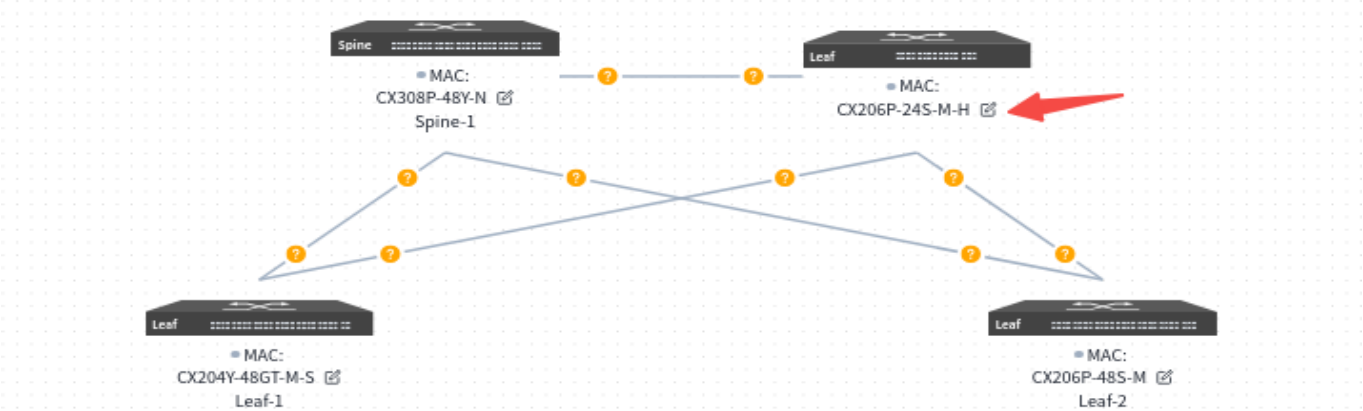
6.1 Small/Mid-Scale Network Deployment



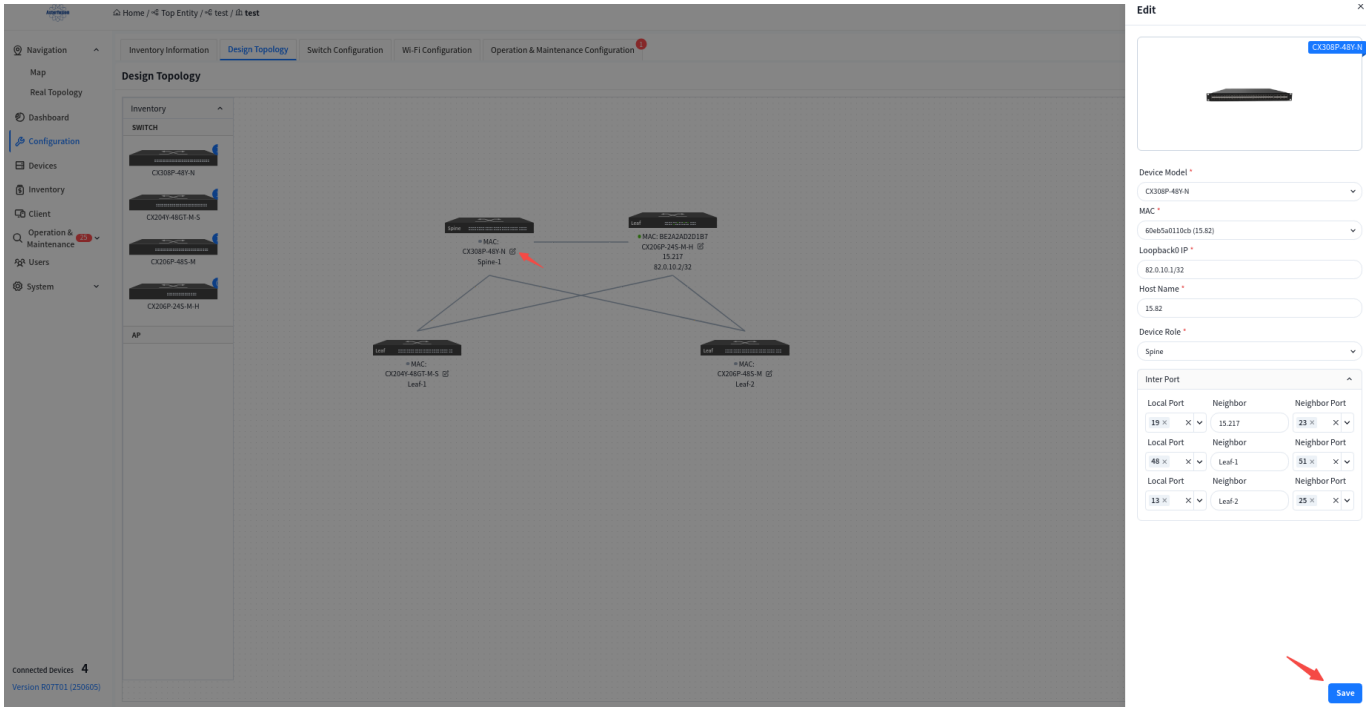
6.1.1 Design Topology

Select the Small/Mid-Scale Campus network scenario, fill in the models and quantities of Spine and Leaf devices, then click **[Save]** to finish the pre-planning of the network topology. The controller will generate a recommended network topology based on the pre-planned typical network architecture.

Note: In Small/Mid-Scale scenarios, devices such as OLT, ONU, and optical splitter are supported. The OLT is connected to the Spine switch, the ONU is connected to the Leaf switch, and they are connected through an optical splitter in between. For the planning of the optical splitter and the configuration related to the OLT, please refer to the Data Center Management Network PON Solution.



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



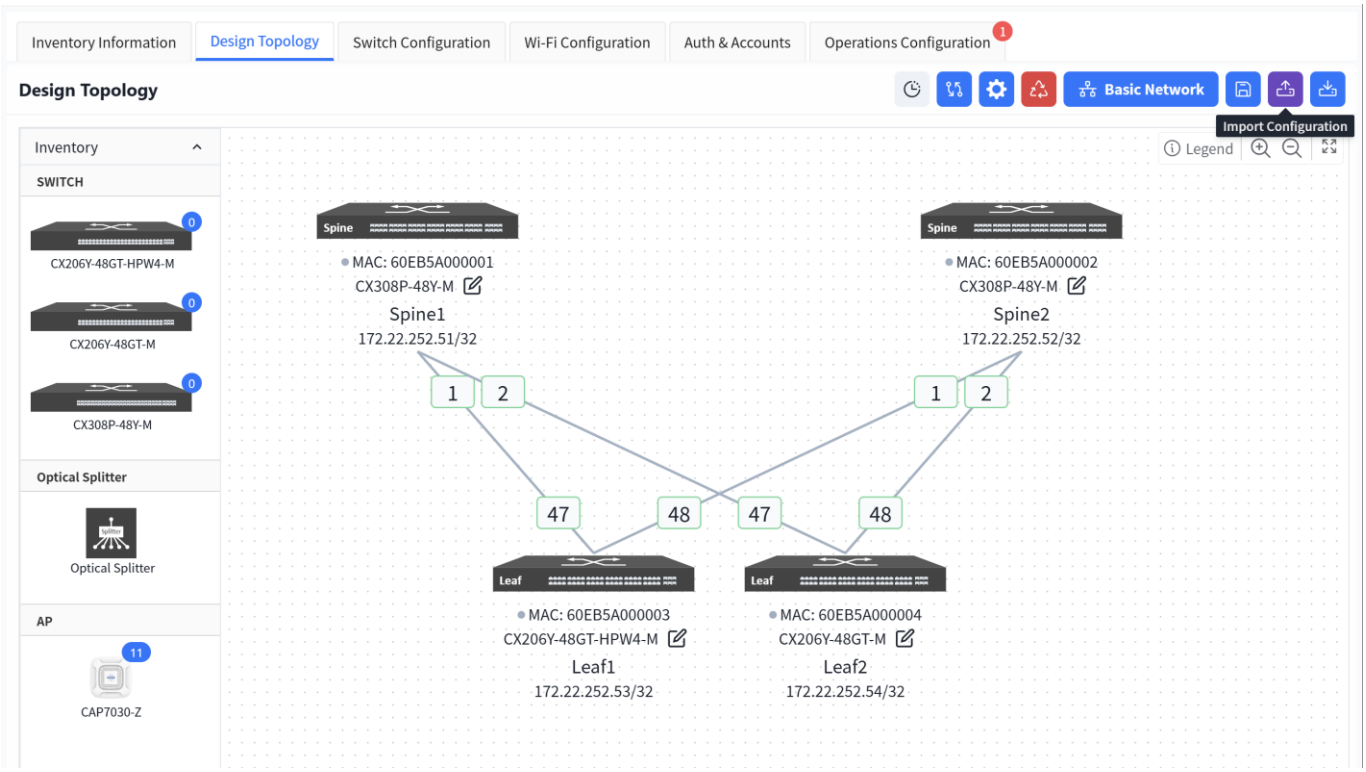
- ✧ MAC: Uniquely select a device via its MAC address.
- ✧ Loopback IP: Configure the IP address for the device's Loopback0 interface, which will be used for in-band management of the device.
- ✧ Hostname: Configure the hostname of the device.
- ✧ Device role: Assign the device role as Spine or Leaf.
- ✧ Inter Port:

  Local Port: 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 importing, users can click **[Export Configuration]** on the right to obtain a blank configuration file.

The format of the configuration file is as follows:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Description	Device A MAC	Device A Hostname	Device A Role	Loopback A	Device A SN	Location A	Real Interface A	Display Interface A	Cable	Device B MAC	Device B Hostname	Device B SN	Location B	Real Interface B	Display Interface B	Custom Description
2	# Description	# Configuration (Required). When prefixed with #, the entire line is treated as description	# Configuration (Conditional optional). Import configuration from inventory if not configured	# Configuration (Required). Example: SuperSpine/Spine/Agg/Leaf	# Configuration (Conditional optional). Import configuration from inventory if not configured	# Description	# Description	# Configuration (Optional). Example: Ethernet1,Ethernet2	# Description	# Description	# Configuration (Optional)	# Description	# Description	# Description	# Configuration (Optional). Example: Ethernet1, Ethernet2	# Description	# Description
3		60eb5a001d3a	Leaf-1	Leaf	172.22.252.60/32			Ethernet49			60eb5a0(	Spine-1			Ethernet51		

You can simply fill in according to the configuration file template and then import it.

Once you have finished editing the topology, click the **[Save]** button in the upper right corner to save your edits to the topology.

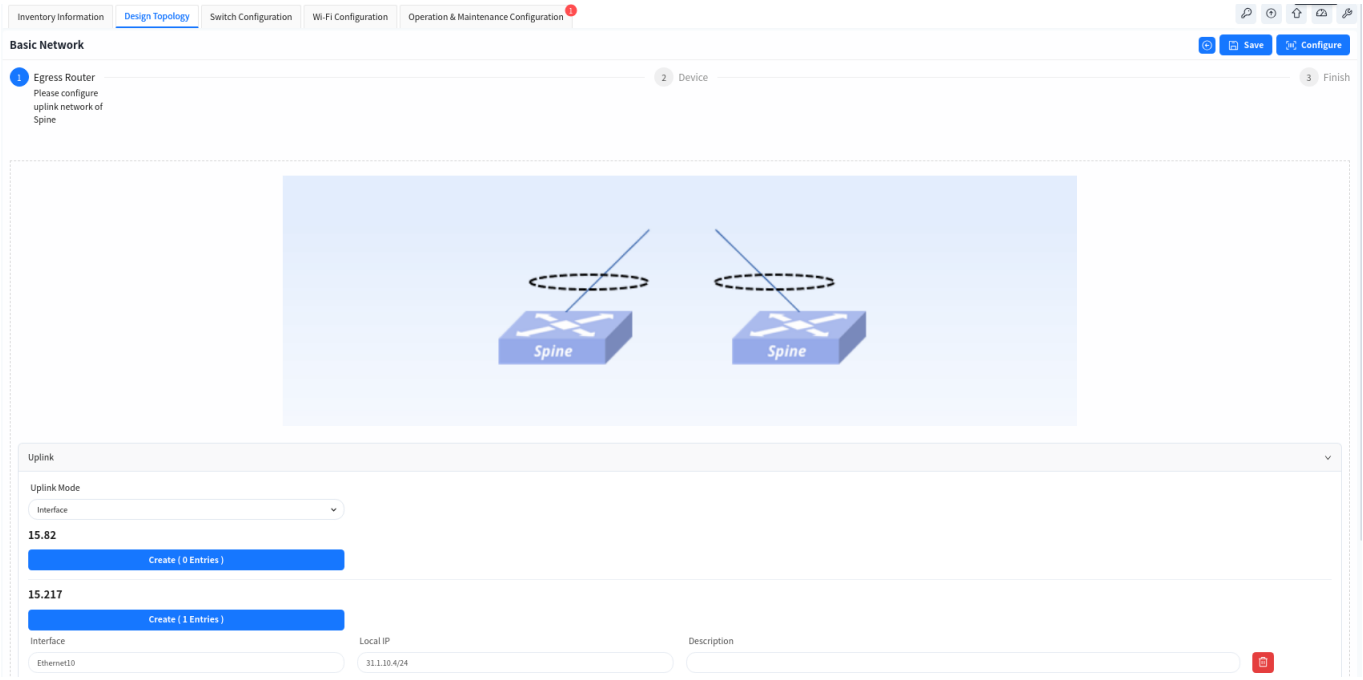
6.1.2 Basic Network

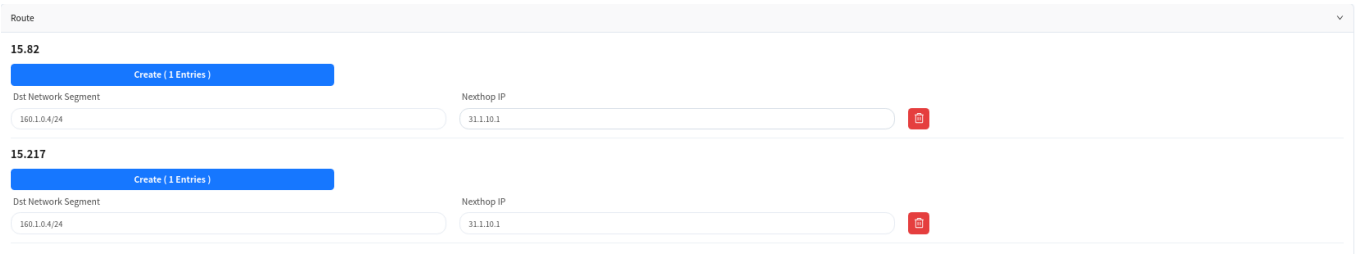
Click **[Basic Network]** to enter the Basic Network Configuration interface to configure the basic network that carries the service network, including the routing protocols between Leaf and Spine, and between Spine and up-link devices. Besides information such as IP addresses that must be specified by the user, the controller will dynamically generate basic configurations based on the network topology that do not require the user's attention.

6.1.2.1 Egress Route

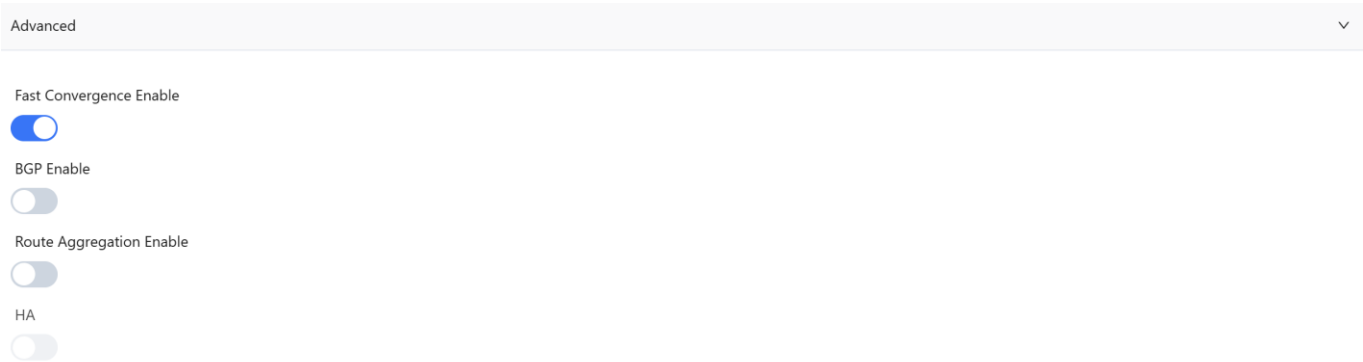
Configuring Spine device up-link interface information.

Configure the IP address of the Spine device uplink interface and static routing information on the Spine device.





If the Spine and the core device do not use static route but use dynamic route, user can click [Advance] button to configure it.



- ✧ **Fast Convergence Enable:** Minimize the convergence time during network topology changes in order to protect the high availability of mission-critical services.
- ✧ **BGP Enable:** Enable the BGP function of Spine device and configure the AS number and IP address

information of the up-link device, so that Spine can establish BGP neighbor relationship with the up-link device.

- ✧ **Route Aggregation Enable:** When the Spine devices enable the BGP function, the routing information of the terminal will be synchronized with the up-link device in form of aggregated routes.
- ✧ **HA:** When enabled, the two Spine devices will provide a cross-device LAG interface to the up-link device through the MC-LAG function.

6.1.2.2 Device Management

Configure device management related information:

- ✧ TimeZone: Configure the system time zone.
- ✧ NTP: Configure NTP Server.
- ✧ SNMP: Configure SNMP community.
- ✧ Syslog: Configure syslog server IP address.
- ✧ TACACS+: Configure TACACS server IP address.
- ✧ Device ACL: Configure ACL rules restricting SSH, SNMP, TELNET connections to device.

6.1.3 Wired Service Configuration

6.1.3.1 Wired Service Configuration

Click **[Switch Configure]** to enter the wired service management interface, where you can configure corresponding service VLANs and IP gateways on switches for wired and wireless users, and specify the IP address of the DHCP server. Multiple service VLANs can be added to handle different service requirements.

6.1.3.1.1 Service Activation

- **[DHCP Relay]**: Configure the DHCP server IP address. When the DHCP server does not support recognizing the option82 field, the option82 option needs to be disabled.
- **[VLAN]**: Create service VLANs. Note that in addition to basic service VLANs, a management VLAN for user APs to connect to the controller must also be created.
- **[IP]**: Configure an address as the gateway for the service VLAN.
- **[Access/Trunk]**: Select the mode according to whether the interface transmits/receives packets with

VLAN tags.

- **Access**: Accepts packets without VLAN tag, typically configured for the AP management VLAN.
- **Trunk**: Accepts packets with VLAN tag, typically configured for service VLANs.

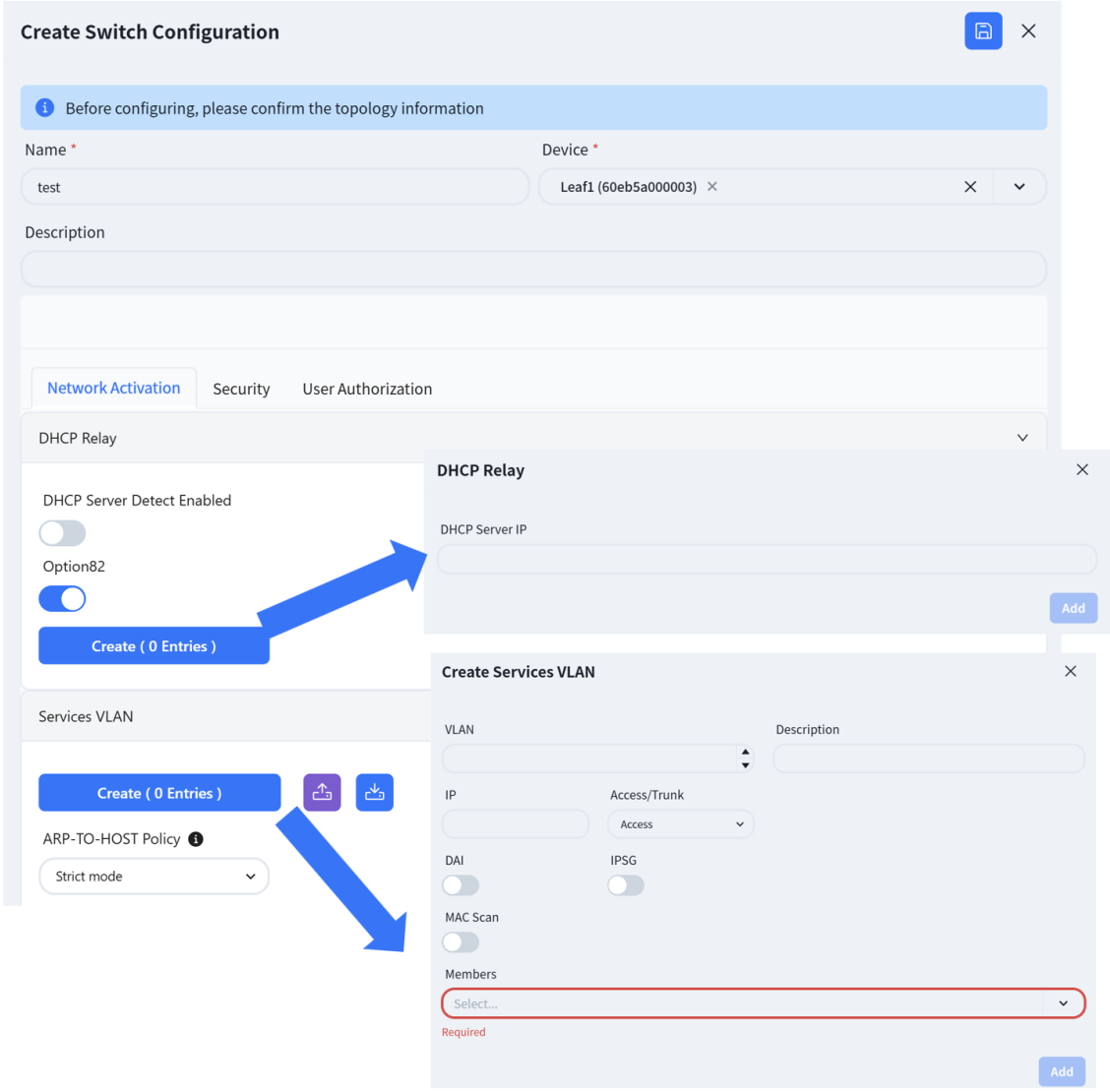
- **[Member Interfaces]**: Click the drop-down arrow to select the member interfaces of the VLAN.
- DAI/IPSG

The controller enables the DHCP Snooping function by default to effectively prevent DHCP Server impersonation attacks, ensuring DHCP clients obtain IP addresses from legitimate DHCP servers. Administrators do not need to manage trusted/untrusted interfaces on different devices-the controller automatically generates configurations based on topology information.

Administrators can enable ARP inspection (DAI) and IP source guard (IPSG) based on network security requirements. These functions validate host legitimacy using global DHCP Snooping entries to prevent malicious hosts from forging legitimate identities or attacking the network via self-assigned IP addresses, thus avoiding potential IP conflicts.

- MAC Scan (optional)

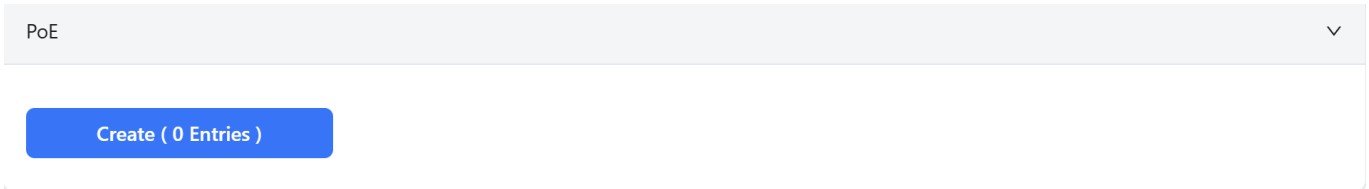
In Ethernet, MAC address table entries guide devices to perform layer 2 data forwarding. After enabling this function, ARP Request packets corresponding to the IP address in the request table can be sent based on the Snooping and User bind table entries, which are commonly used for dumb terminals and server deployment. Proactively update device MAC and ARP table entries.



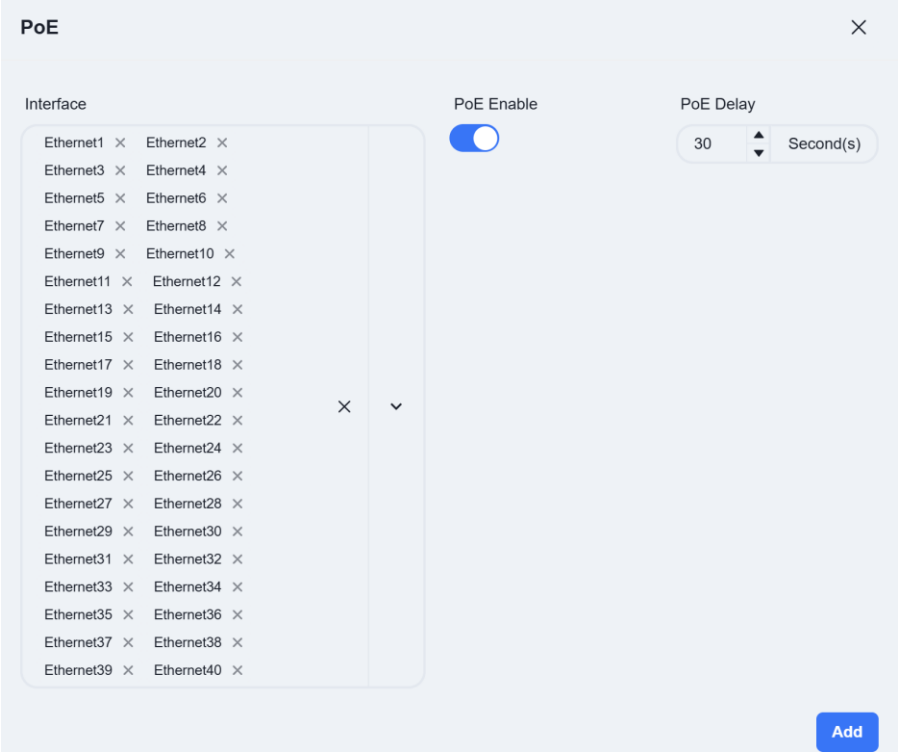
6.1.3.1.2 POE

The access switch features PoE functionality, which can be directly enabled in the wired service configuration to supply power to PD devices.

Click **[Create]**



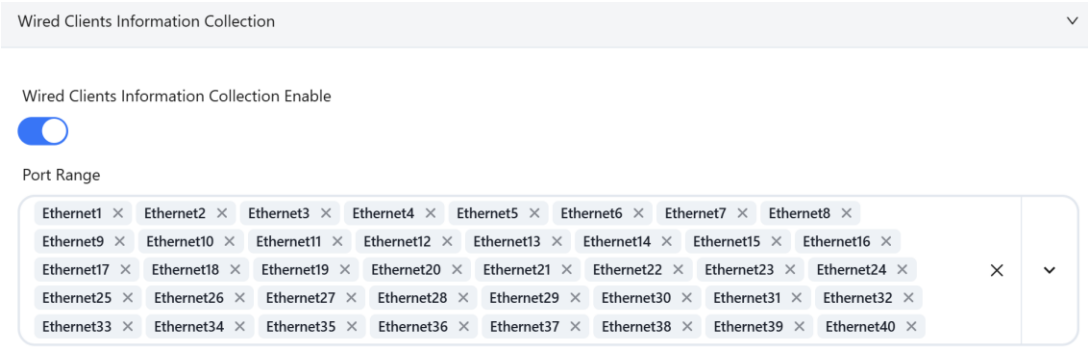
Select the interface where the PoE function is to be enabled and set the startup delay time.



POE Delay: This refers to a brief, intentional time delay introduced at a PoE switch port between when it begins to supply power and when it actually delivers power to the Powered Device (PD).

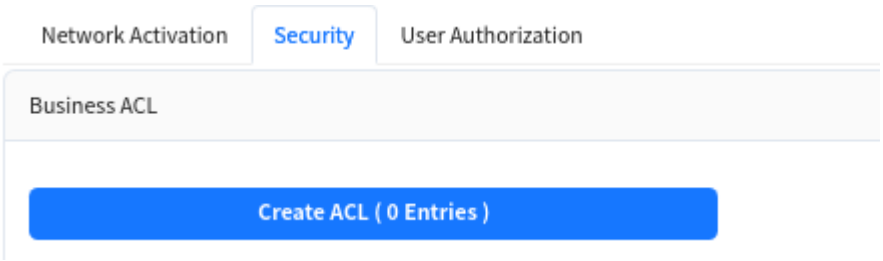
6.1.3.1.3 Wired Clients Information Collection

Interfaces with this feature enabled will report information about the connected wired terminals to the controller.



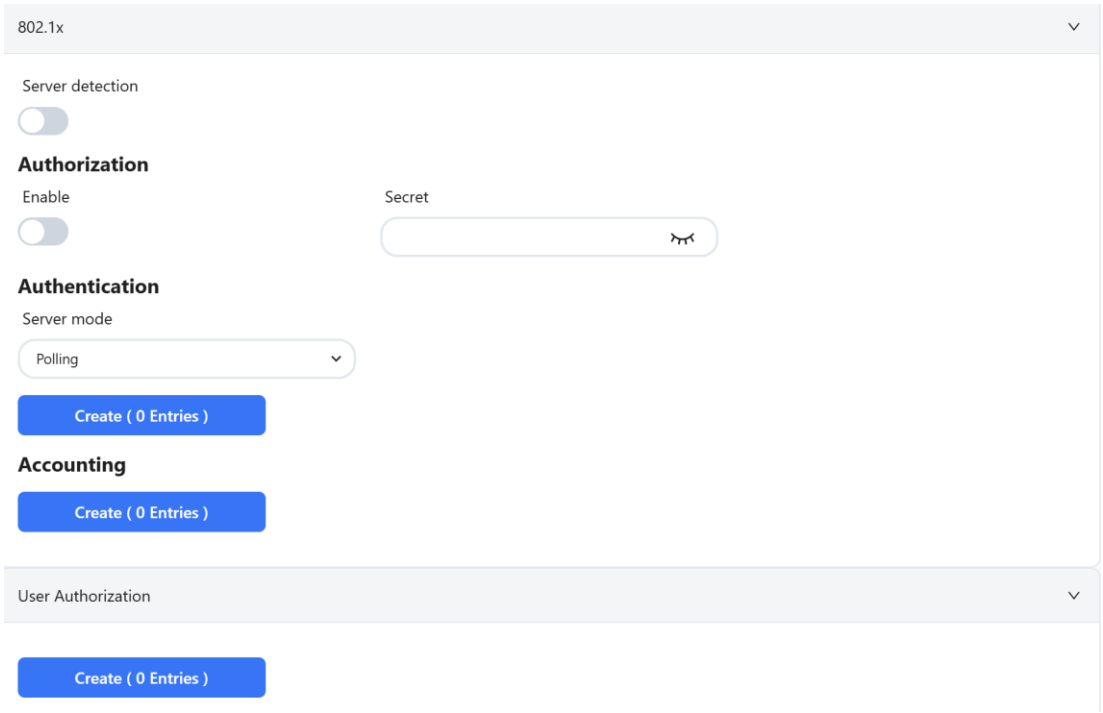
6.1.3.1.4 Network Security Configuration [Optional]

Administrators can further enhance network security by configuring device management ACLs and service ACLs to set blacklists/whitelists for user internet traffic.



6.1.3.1.5 User Authentication Configuration [Optional]

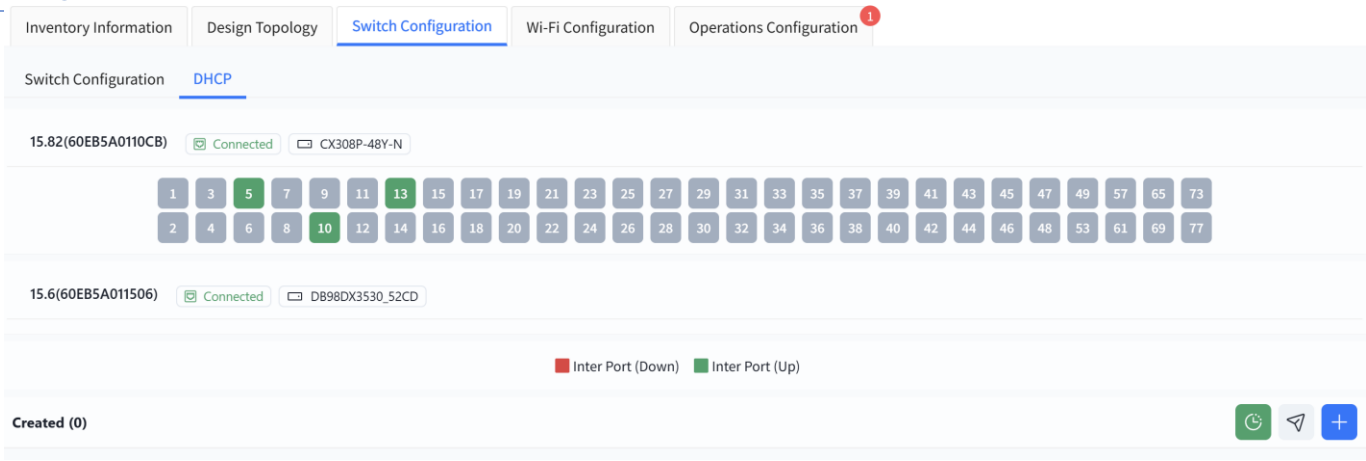
In enterprise networks or public places with high security requirements, enable 802.1x-based user authentication. This ensures only authenticated users and devices can access network resources, enhancing security. Through the graphical interface, administrators can define and apply authentication policies, including specifying ports for 802.1x authentication and setting different authentication rules.



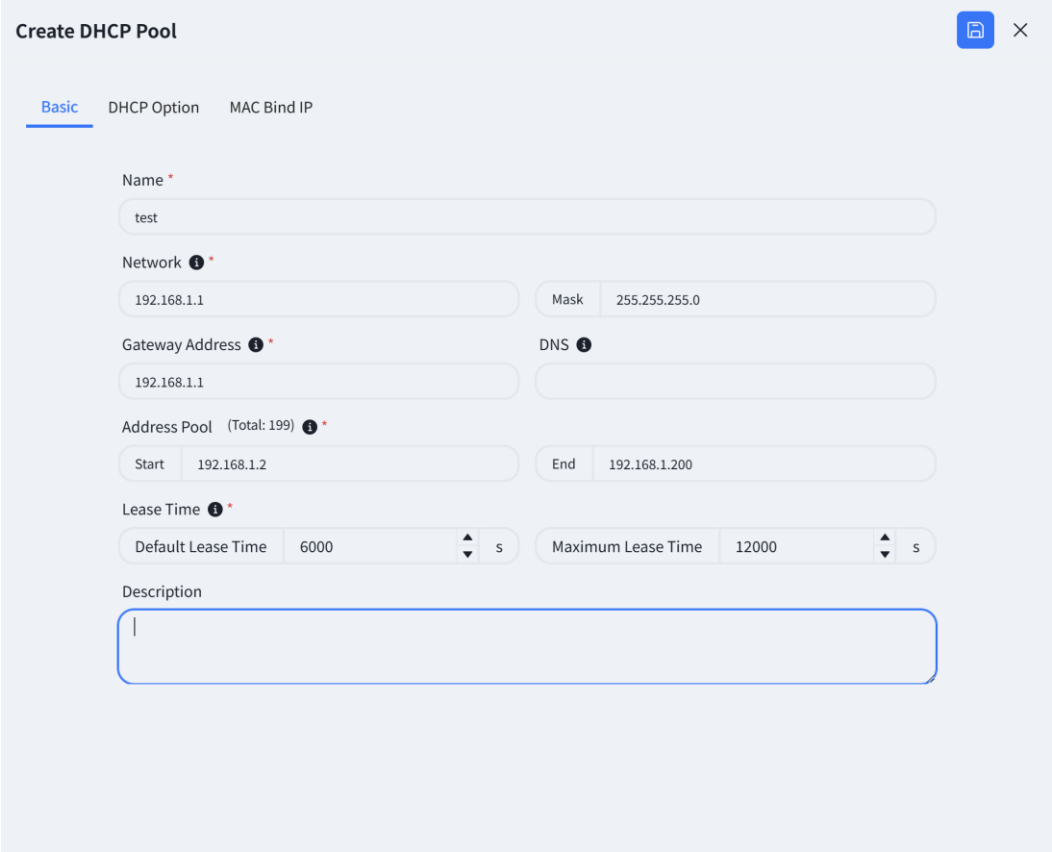
6.1.3.2 DHCP

The controller supports users to configure DHCP Server functionality on Spine devices.

After entering the venue, click on **[Configuration]** - **[Wired Service Configuration]** - **[DHCP]** to enter the DHCP Server configuration interface, and click on the **[+]** button on the page to create a new configuration:



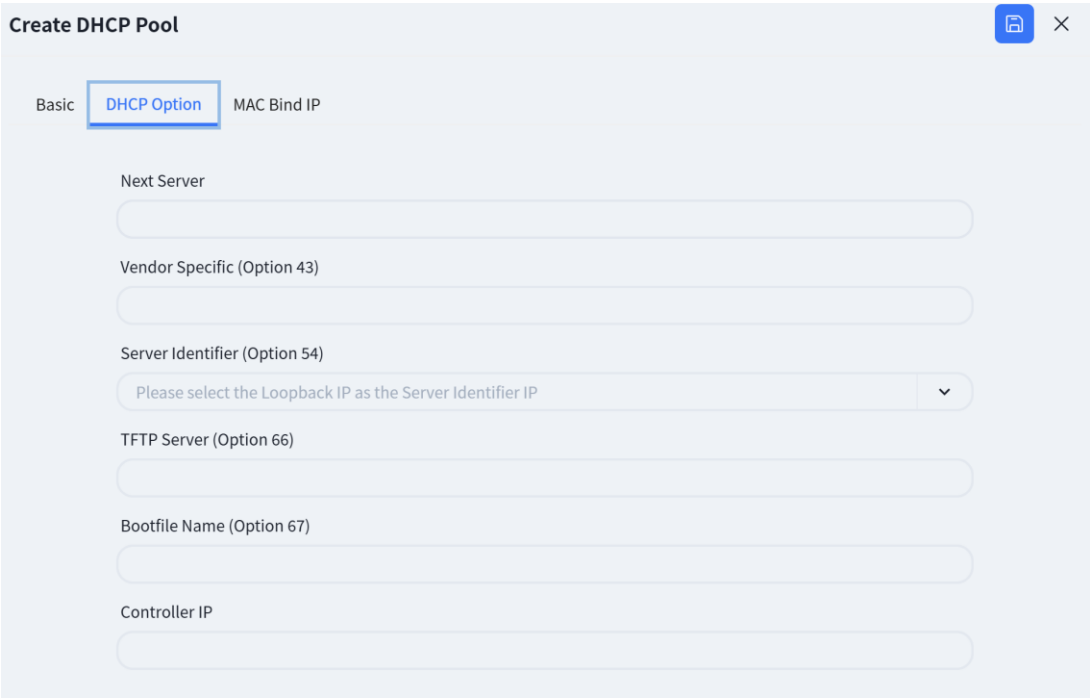
Follow the prompts on the page to configure address pool details. Fields marked with * are mandatory.



- Name: User defined.
- Network: Specify the network segment where the IP address assigned by the DHCP server to the DHCP client is located.
- Gateway Address: Specify the gateway address assigned by the DHCP server to the DHCP client.
- DNS: Specify the DNS server address.
- Address Pool: Specify the address range allocated by the DHCP server to DHCP clients.
- Lease Time: Specify the IP address lease time.

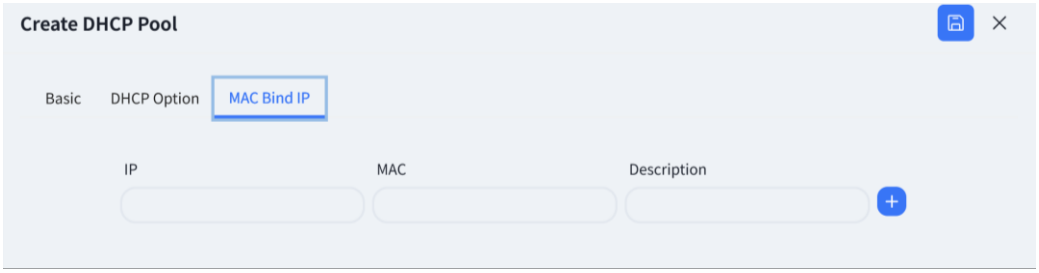
Click on **[DHCP Option]**and fill in the relevant information (optional, if you need to obtain the address of

the device connected to the controller, you need to fill in **[Controller IP]**). Other functions can be expanded as needed by users.



- Next Server：Configure the IP address of the network server to be used in the next step during the DHCP client startup process.
- Vendor Specific (Option 43)：Hexadecimal number used to transmit vendor specific information to client devices of a particular vendor.
- Server Identifier (Option 54)：Notify the client of the address of the DHCP server.
- TFTP Server (Option 66)：Configure the TFTP server address used by DHCP clients.
- Bootfile Name (Option 67)：Configure the startup configuration file name for DHCP clients.
- Controller IP：DHCP options specifically designed for wireless AP discovery controllers, fill in the controller IP address.

The controller supports configuring MAC binding IP function, which users can fill in as needed.



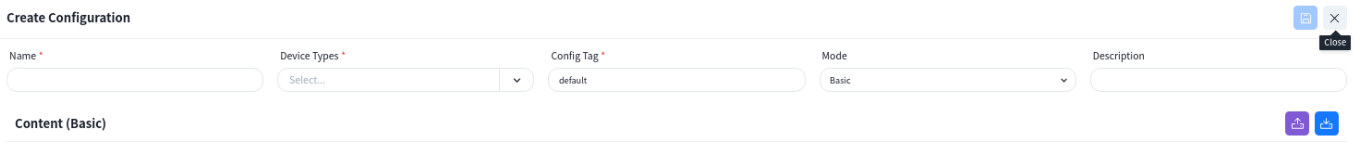
After completing the configuration, click save.

6.1.4 Wireless Service Configuration

6.1.4.1 Wireless Service Configuration

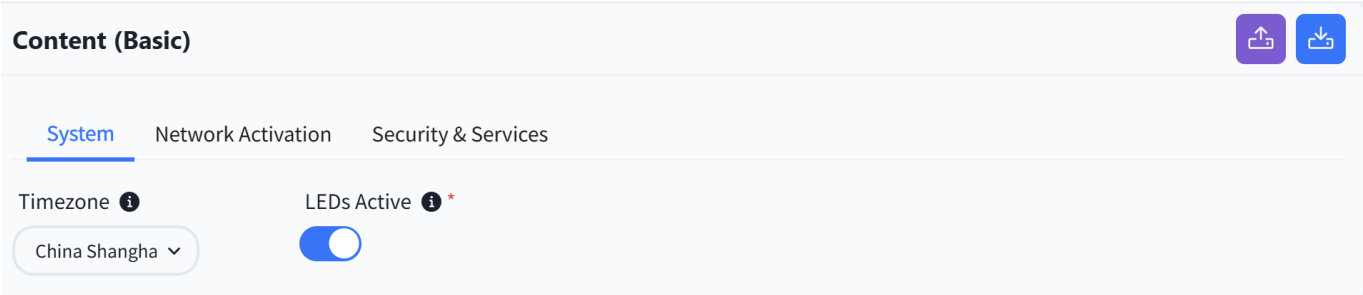
Click **[Wireless Configuration] - [+] - [Create Configuration]** to configure the necessary basic information for the wireless AP, e.g. SSID settings, security policy. The controller can automatically generate the corresponding configuration script based on the administrator's input.

The controller supports the configuration of different wireless service configurations, and after the AP goes online, it will determine which configuration should be issued to the AP based on the **[CONFIG TAG]** attributes of the configuration.



6.1.4.1.1 System

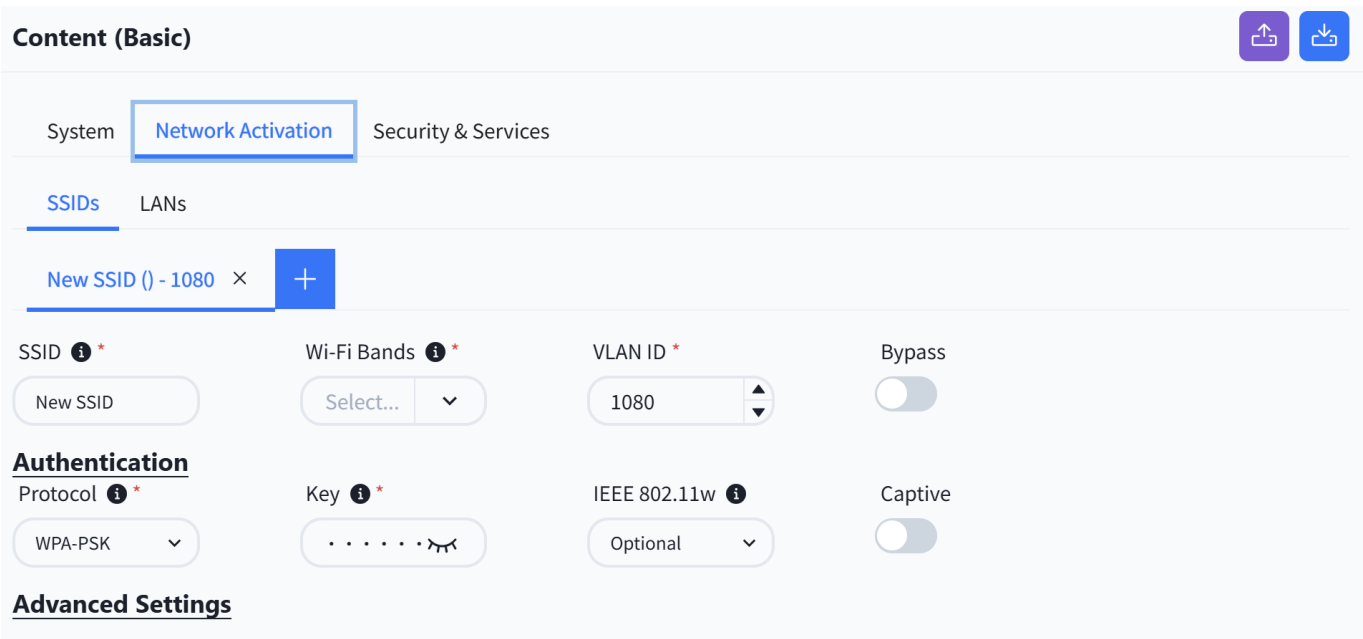
Set time zone and select whether to enable LED.



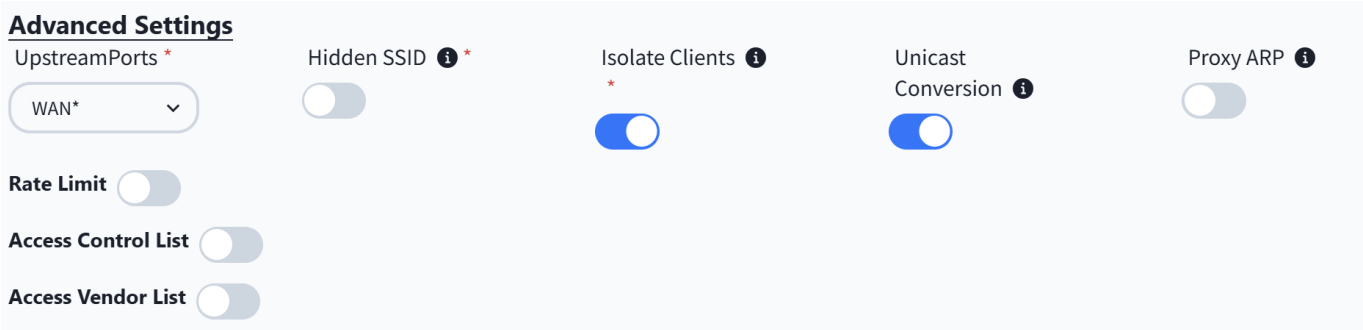
6.1.4.1.2 Network Activation

1. SSID

Configure SSID related content.

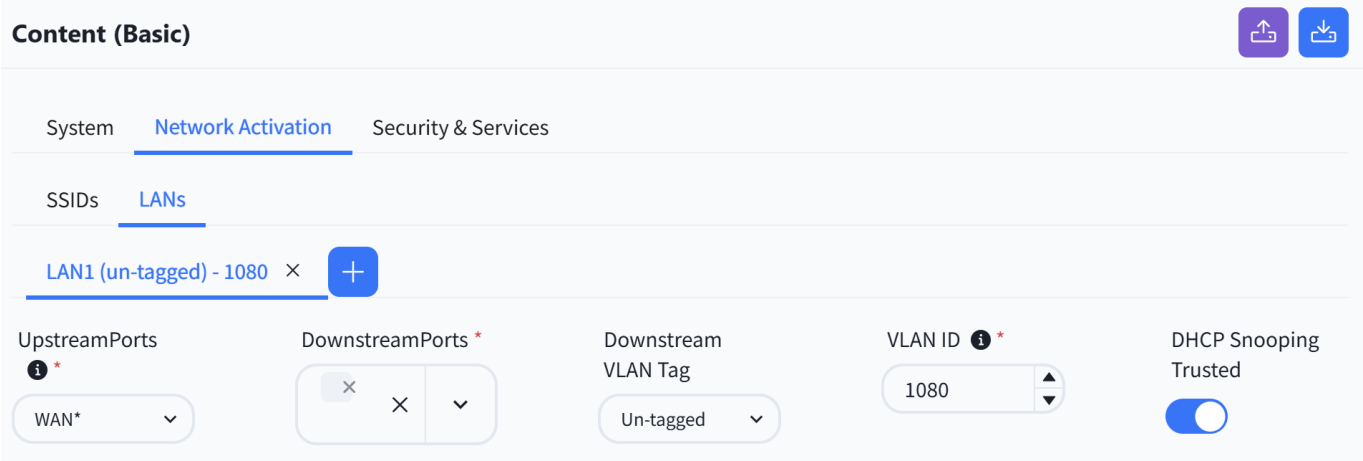


If there is a specific application scenario, the administrator can also customize the default configuration of the AP in the **[advanced settings]**.



2. LAN

When the AP is one that has an extended wired interface and is capable of accessing terminals by wired means, such as a panel AP, the user can configure the access method for wired terminals through the configuration in LANs.



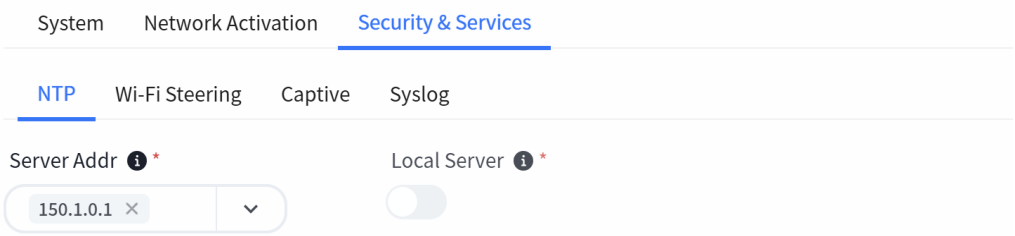
✧ UpstreamPorts: Specify the up-link interfaces for wired terminal to access the network through AP,

usually it is the interface for AP to connect to the switch, and keep the same with [UpstreamPorts] in [SSID] – [Advanced] Settings, the default is: WAN*.

- ✧ DownstreamPorts: Interfaces for wired terminal access.
- ✧ Downstream VLAN Tag: Whether the wired terminal carries VLAN Tag.
- ✧ VLAN ID: The AP receives messages from wired terminals that add this VLAN TAG to identify.
- ✧ DHCP Snooping Trusted: DHCP Snooping Trusted interface, if the wired terminal needs to obtain IP address through DHCP service, this switch needs to be on.

6.1.4.1.3 Security & Services

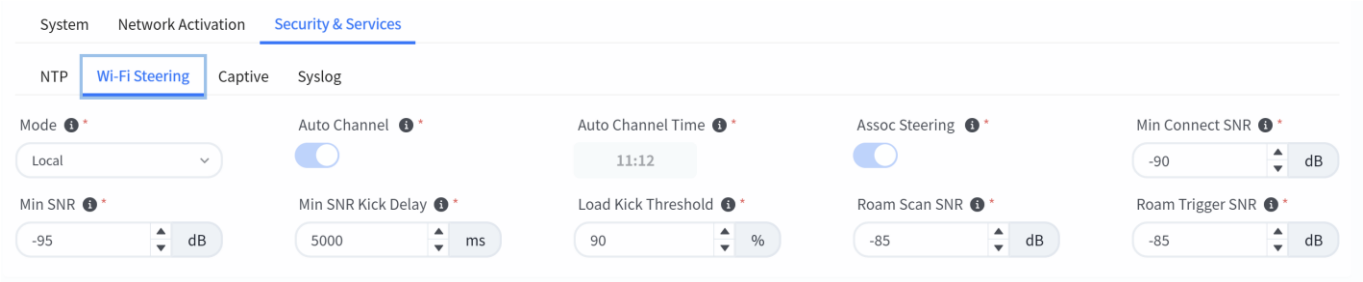
1. NTP



Server Addr: Enter the URL/IP address of the NTP server. The AP will synchronize the time from this address.

Local Server: Start the NTP service on the AP.

2. Wi-Fi Steering



Auto Channel: The wireless access point automatically scans the surrounding radio frequency environment in real time through an intelligent algorithm, and selects the working channel with the least interference and optimal quality to maximize the performance and stability of the wireless network. This is an automated function. After enabling, you can set the **Auto Channel Time**.

Assoc Steering: Assoc Steering is an active control mechanism in wireless networks. When a new client device attempts to connect to an access point (AP), the system makes intelligent decisions based on the global network status (such as signal strength, AP load, etc.).

Min Connect SNR: Minimum signal-to-noise ratio or signal level (dBm) to allow connections.

Min SNR: Minimum signal-to-noise ratio or signal level (dBm) to remain connected.

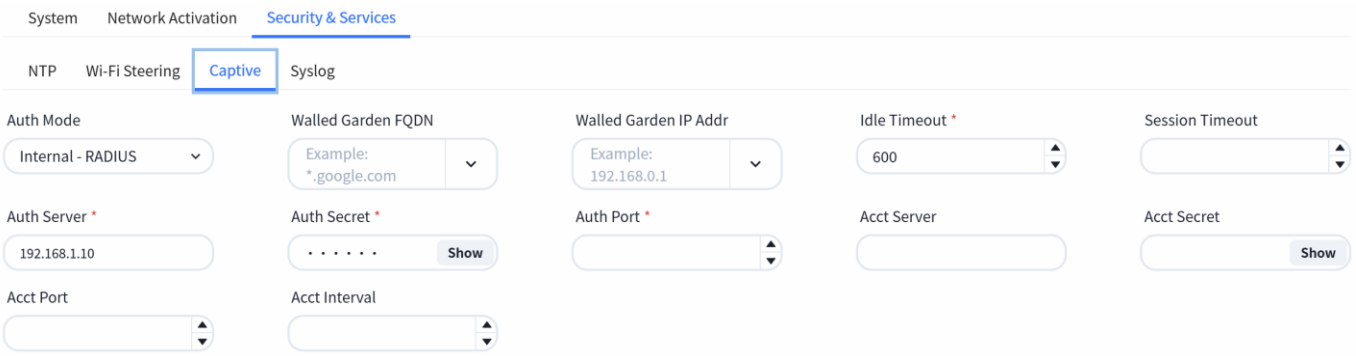
Min SNR Kick Delay: Timeout after which a station with snr < min_snr will be kicked.

Load Kick Threshold: Minimum channel load (%) before kicking clients.

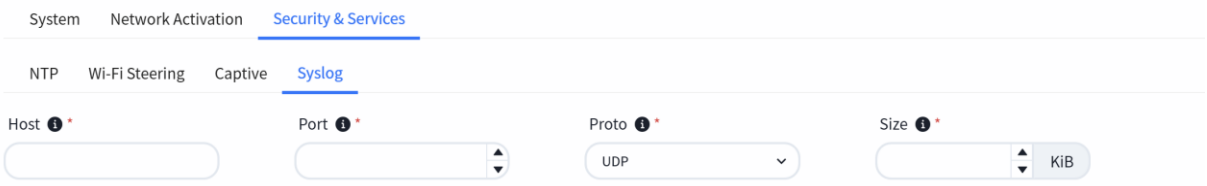
Roam Scan SNR: Minimum signal-to-noise ratio or signal level (dBm) before attempting to trigger client scans for roaming

Roam Trigger SNR: Minimum signal-to-noise ratio or signal level (dBm) before attempting to trigger forced client roaming

3. Captive



4. Syslog



Host: IP address of a syslog server to which the log messages should be sent in addition to the local destination.

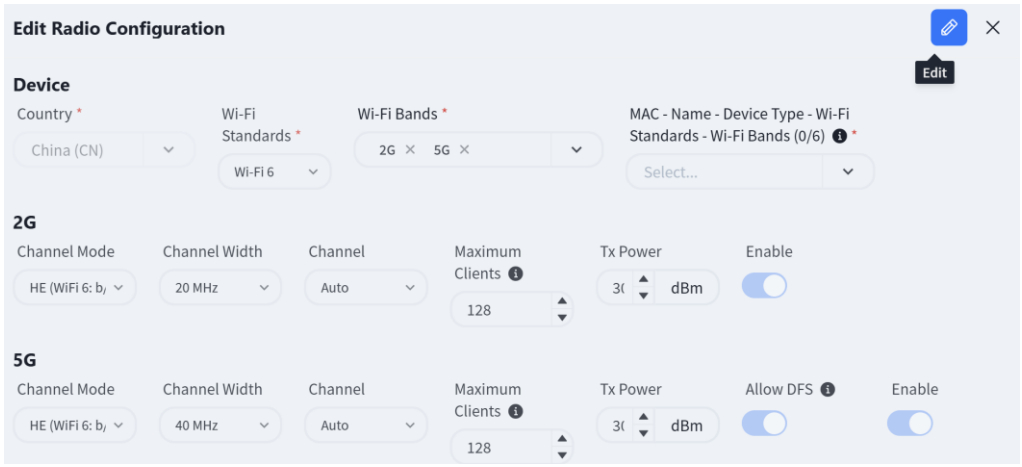
Port: Port number of the remote syslog server specified with log_ip.

Proto: Sets the protocol to use for the connection, either tcp or udp.

Size: Size of the file based log buffer in KiB. This value is used as the fallback value for log_buffer_size if the latter is not specified.

6.1.4.2 Wireless RF Configure

When the AP is online and connected to the controller, according to the actual deployment environment, if you need to adjust the wireless RF related configuration of the AP, you can configure it in the **[Radio Configuration]** page.



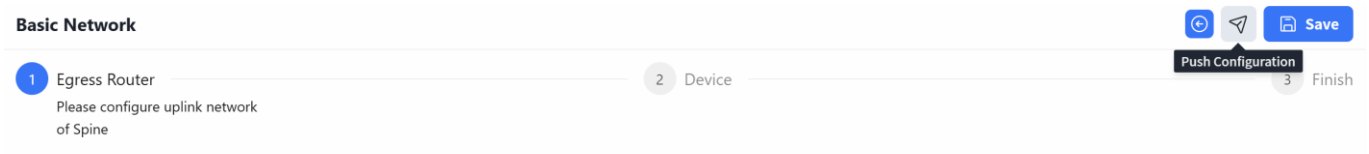
6.1.5 Configuration Release

6.1.5.1 Switch

Switches support both in-band and out-of-band management methods. Operation and maintenance personnel can flexibly choose based on current network conditions. For devices in the factory default state, whenever either the management port or service port is in an "Up" state, they will actively initiate a DHCP request to obtain a temporary management IP address and the IP address of the cloud-based controller from the DHCP server. They will then connect to the controller to retrieve configuration information.

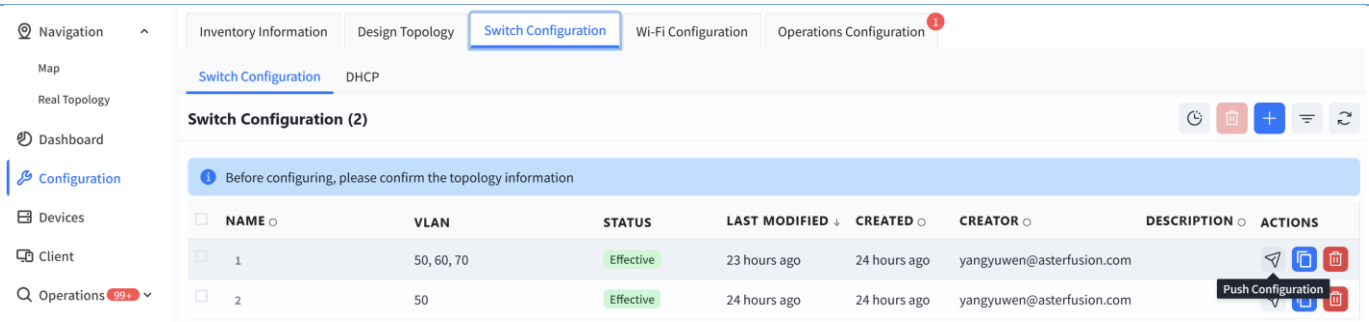
Once all switches are successfully connected to the controller, click **[Topology Consistency Verification]** on the upper right side of the **[Design Topology]** view to confirm whether the generated topology matches the planned topology. After verification, the controller can deploy configurations to the switches.

1. Click **[Configuration]** - **[Design Topology]** - **[Basic Network]** - **[Push Configuration]** to issue the basic configuration for all devices.

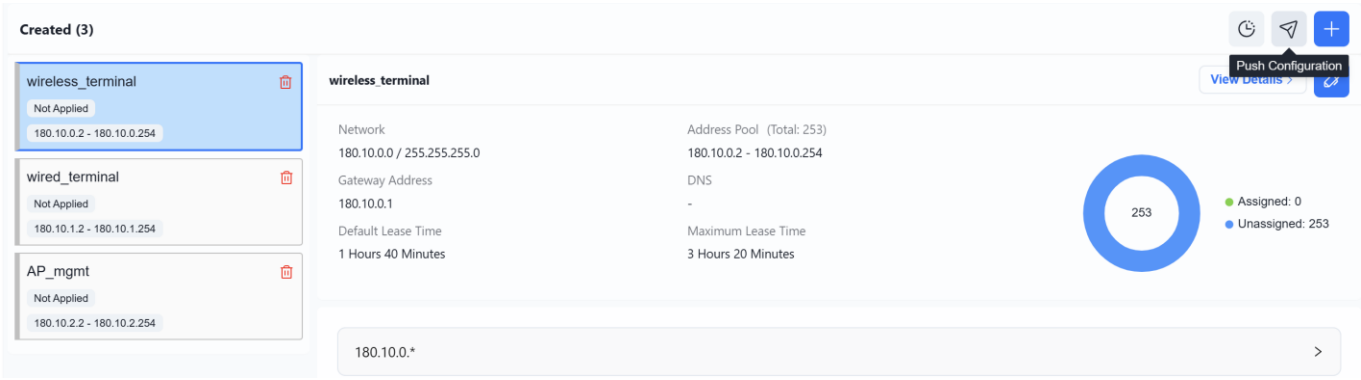


By default, the controller will select all switches. Click the **[Next]** - **[Start]** button to start issuing basic network configurations for the switches.

2. Click [**Configuration]** - **[Switch Configuration]** - **[Push Configuration]**to issue a configuration for the device.



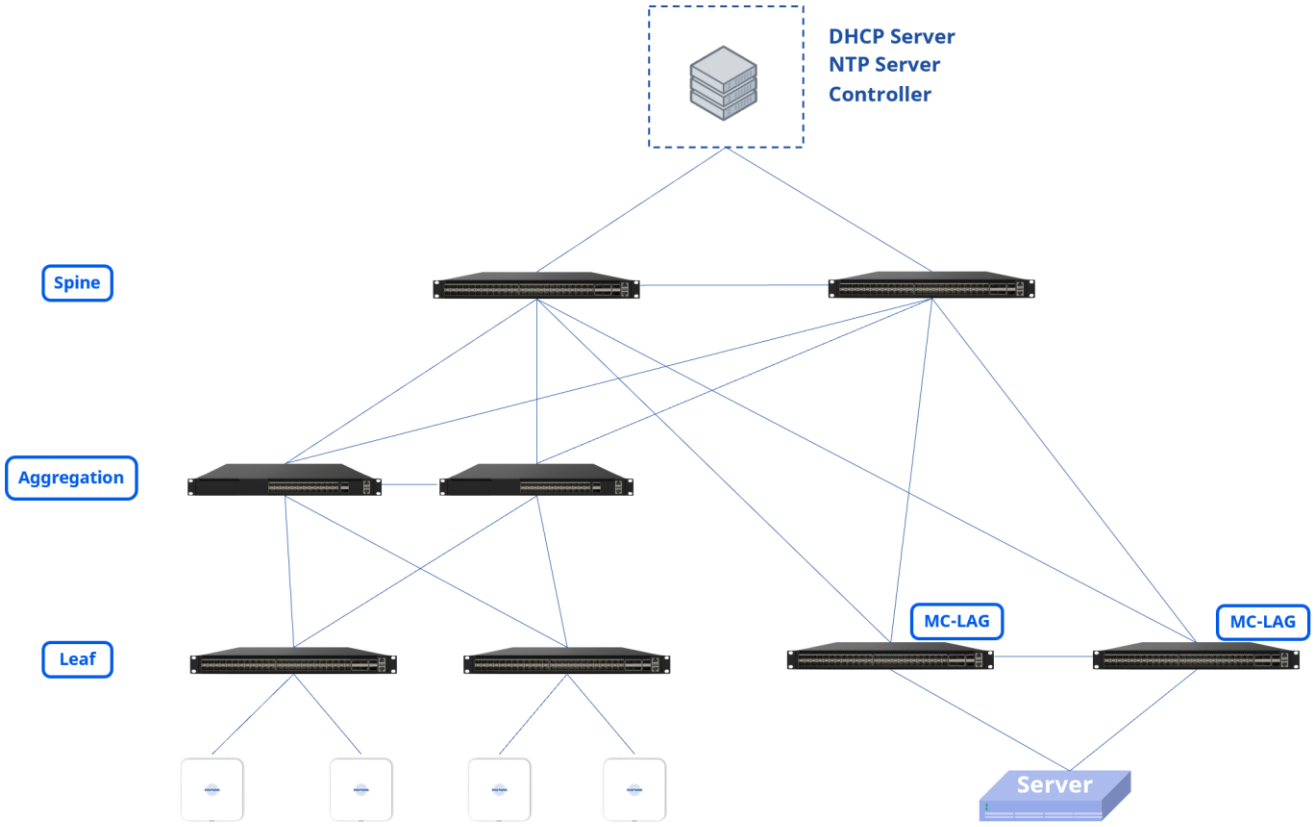
3. On the **[Configuration] - [Switch Configuration] - [DHCP]** interface, select the configuration to be deployed and click the **[Push Configuration]** button to deliver the configuration.



6.1.5.2 AP

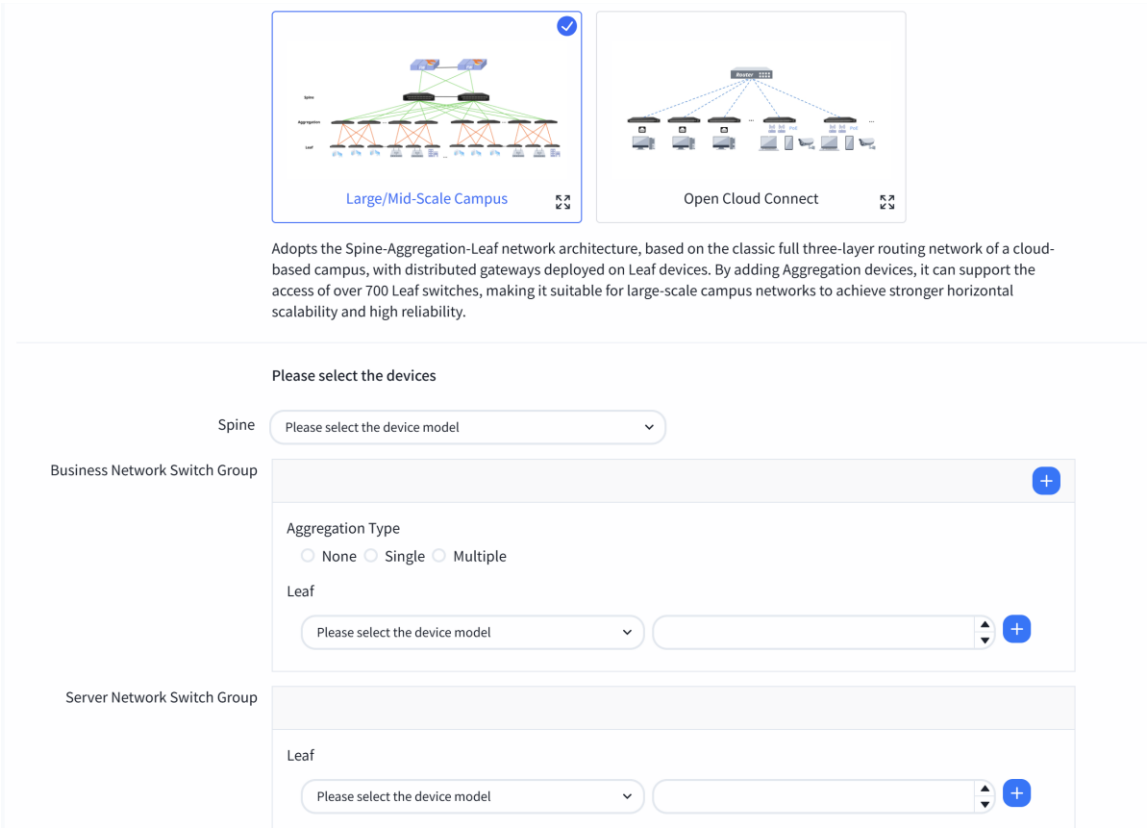
The AP does not need to manually issue the configuration. After the configuration of the device is issued and takes effect, the PoE power supply function of the switch is turned on, and the AP can power on and work. When the AP connects to the controller with the information obtained through the DHCP service, the controller will automatically send the configuration to the corresponding AP based on the comparison between the TAG identification stored in the AP inventory and the TAG identification in the planning configuration.

6.2 Large/Mid-scale Network Deployment

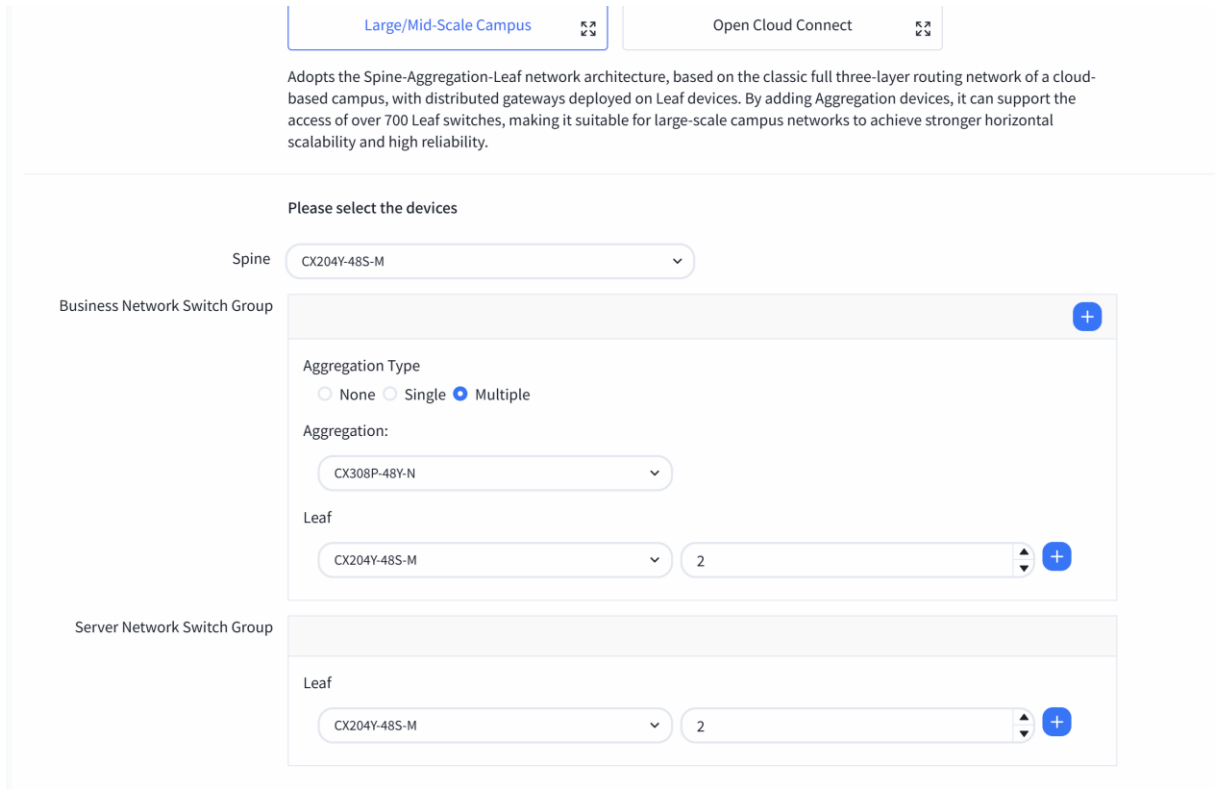


The Large/Mid-Scale Campus network can adopt a Spine-Aggregation-Leaf three-level structure, which expands the number of accessible Leaf devices through Aggregation and further expands the number of access ports. Support configuring MC-LAG access servers on Leaf switches.

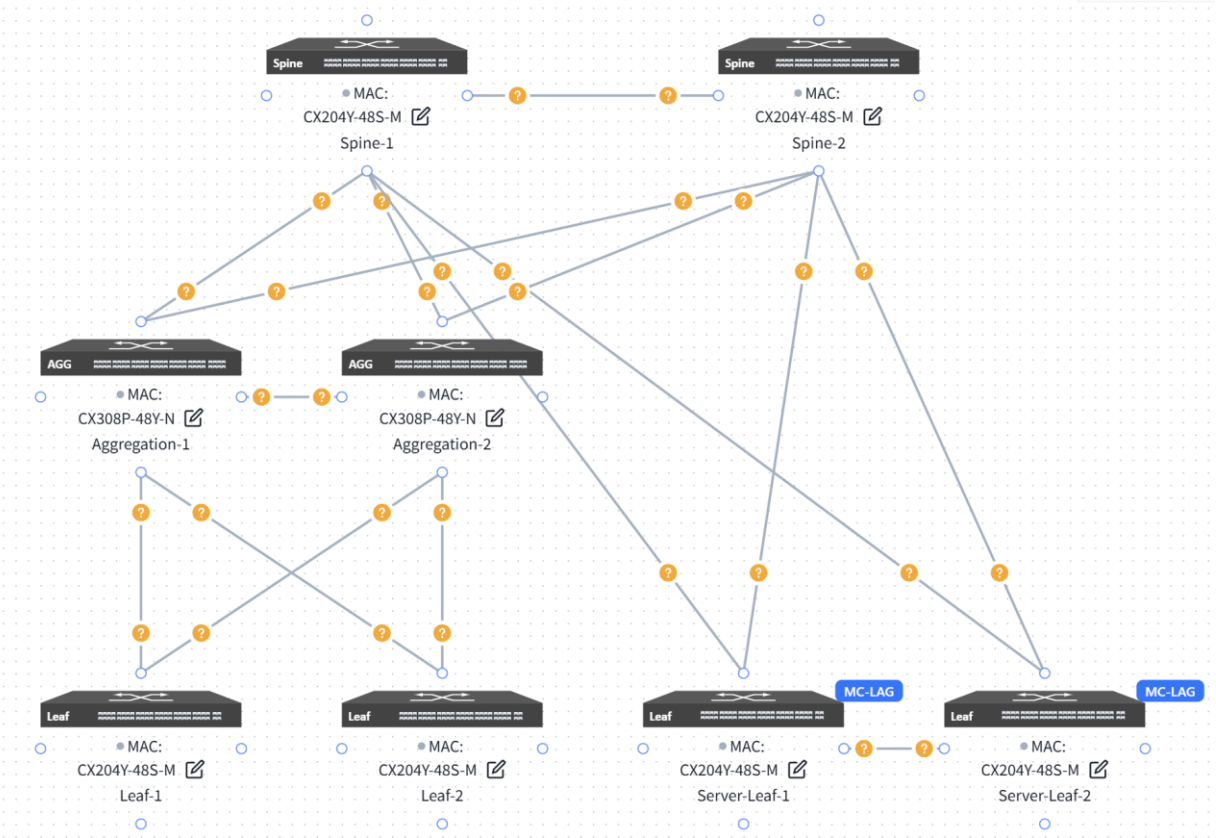
6.2.1 Design Topology



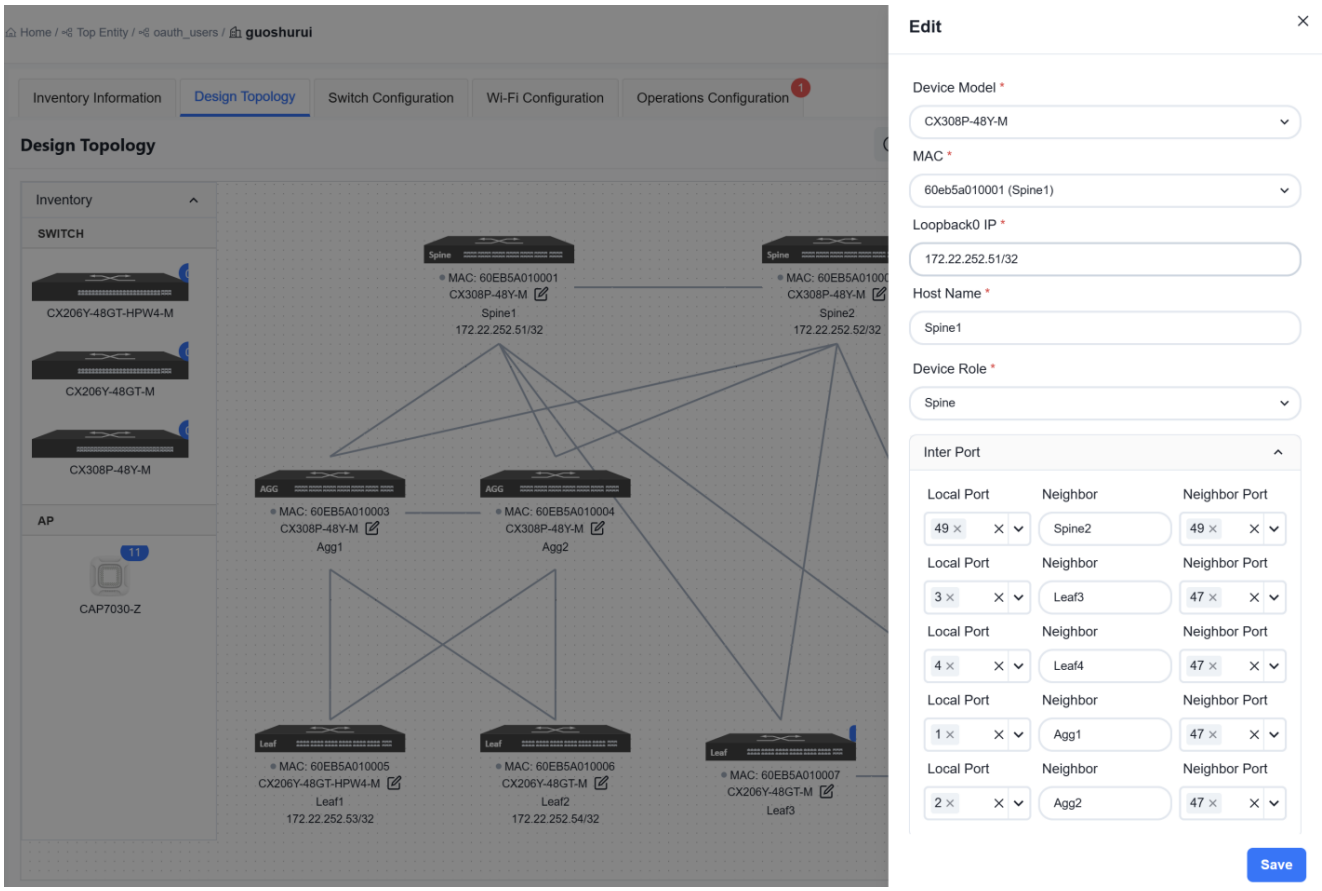
The device selection and topology editing are the same as the Small/Mid-scale campus networks. If MC-LAG needs to be deployed, it is necessary to choose the model and quantity of server network switch group and switches during topology planning, and MC-LAG Enable should be automatically enabled on the server area leaf switch after selection.



The topology overview is shown below:



Users can click the **[Edit]** button on the device end and fill in the corresponding information in the slide-out panel on the right.

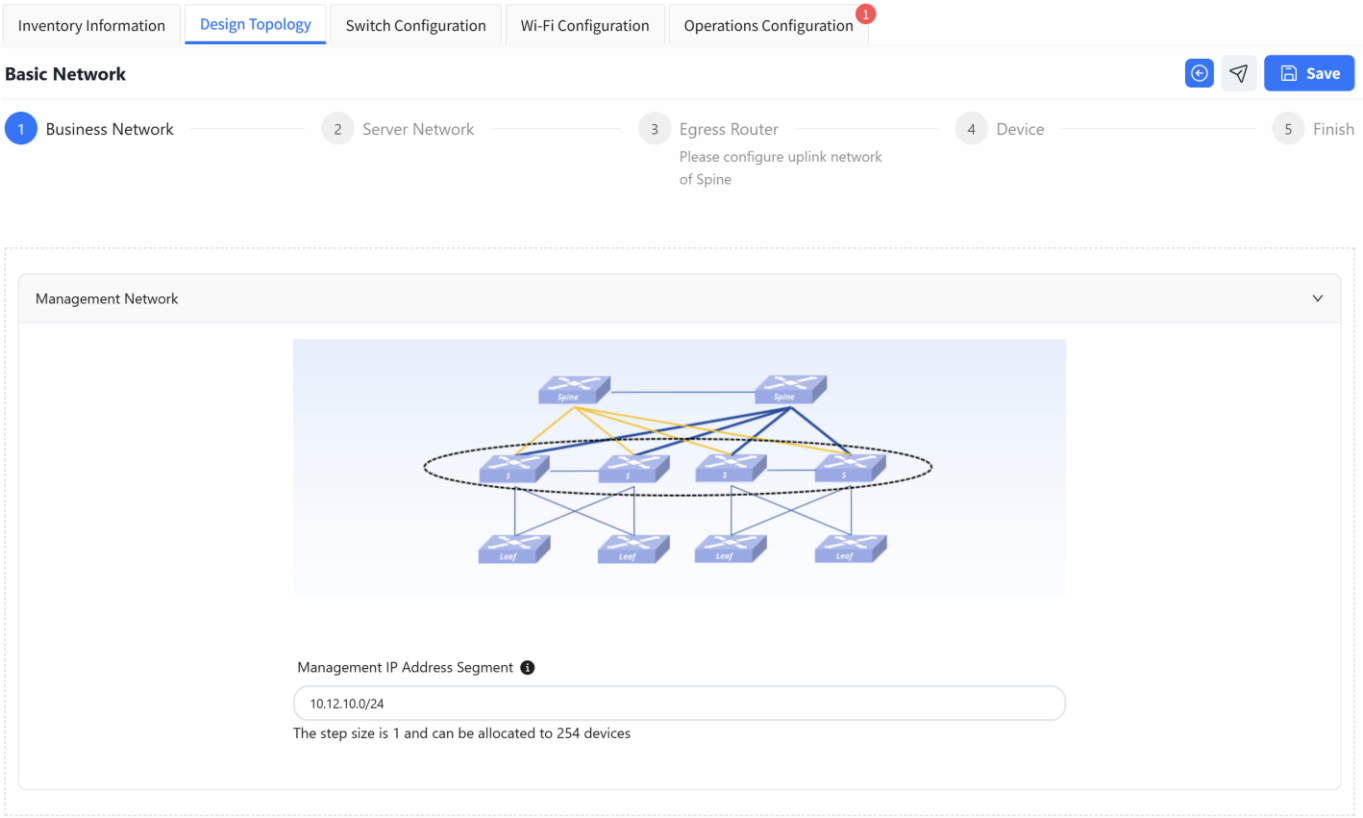


6.2.2 Basic Network

6.2.2.1 Aggregation

Configure the in-band management network for aggregation devices. Typically. the Spine and Leaf devices are Layer 3 devices. in-band management can use the Loopback0 address. while the aggregation device is a Layer 2 device for which you need to configure the management VLAN and IP.

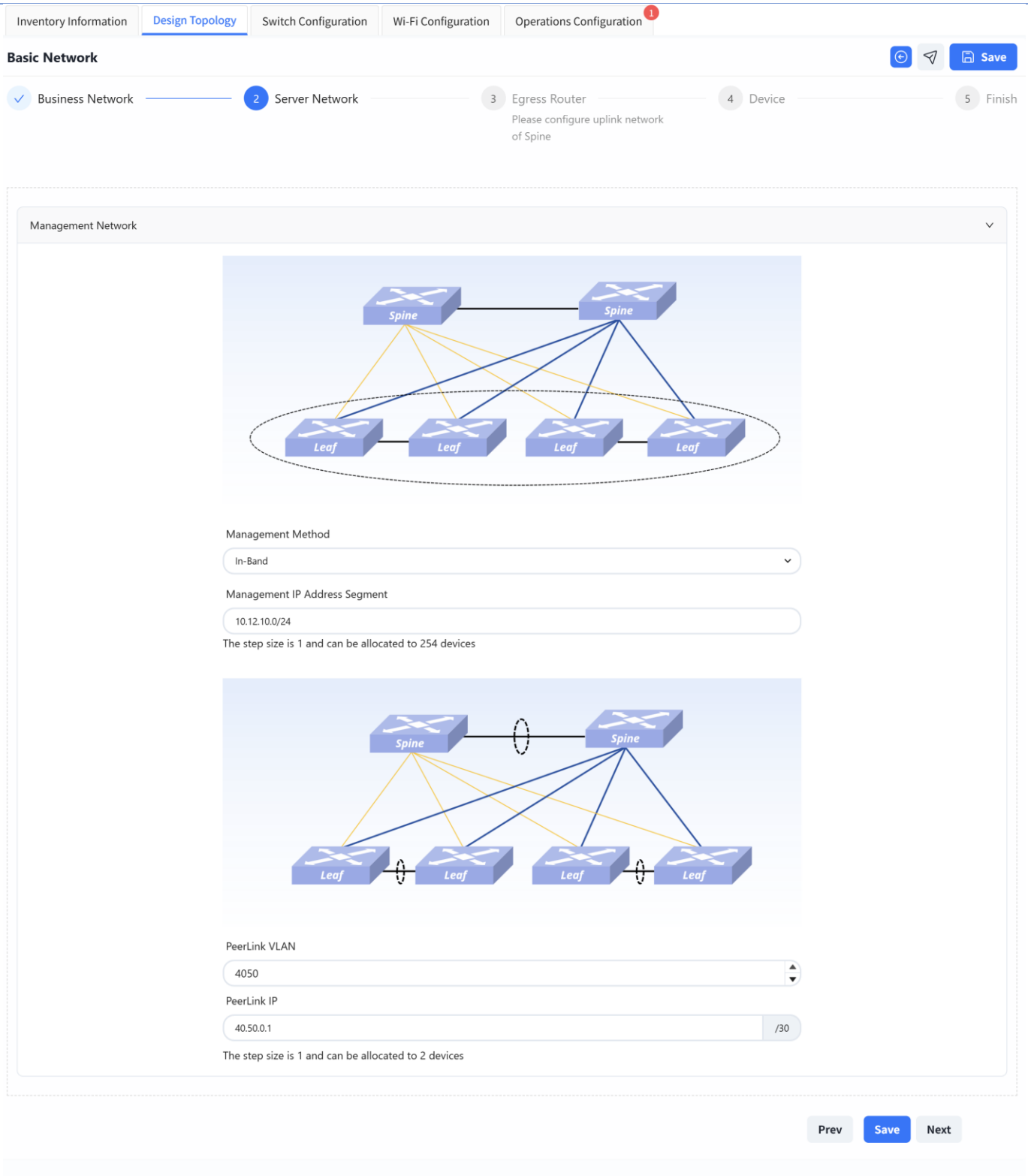
Controller can assign an in-band management address to each aggregation device based on the address segments that are entered by the user.



6.2.2.2 Server Network

Configure in band management network for Leaf devices. (Optional. If out of band management is selected, there is no need to configure the management address range)

Configure the Peerlink interface VLAN and Peerlink IP.



6.2.2.3 Egress Route

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

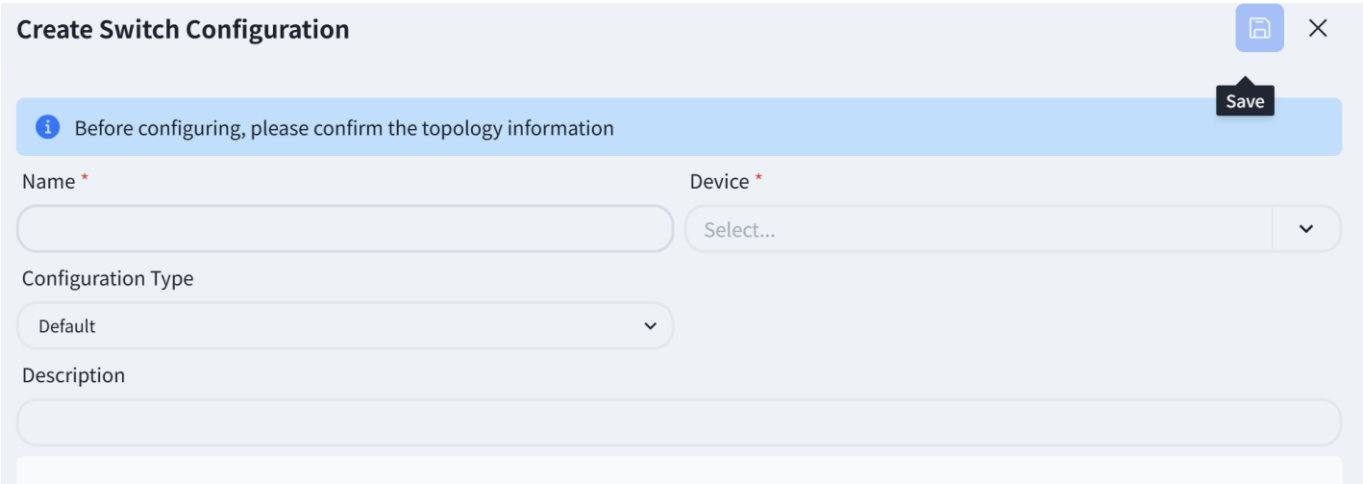
6.2.2.4 Device Management

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network**

Deployment], please refer to the previous section to complete the configuration.

6.2.3 Wired Service Configuration

6.2.3.1 Business Network Switch Group Wired Service Configuration



Default configuration type selection, the rest is the same as **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.2.3.2 Server Network Switch Group Wired Service Configuration

6.2.3.2.1 Server Area Leaf

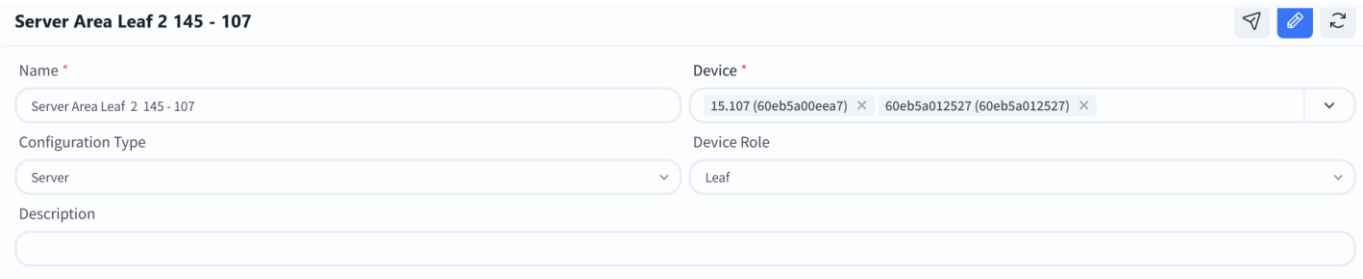
The Leaf switch of MC-LAG network needs to be configured with link aggregation port and business VLAN.

Select **[Configuration Type]**as server area.

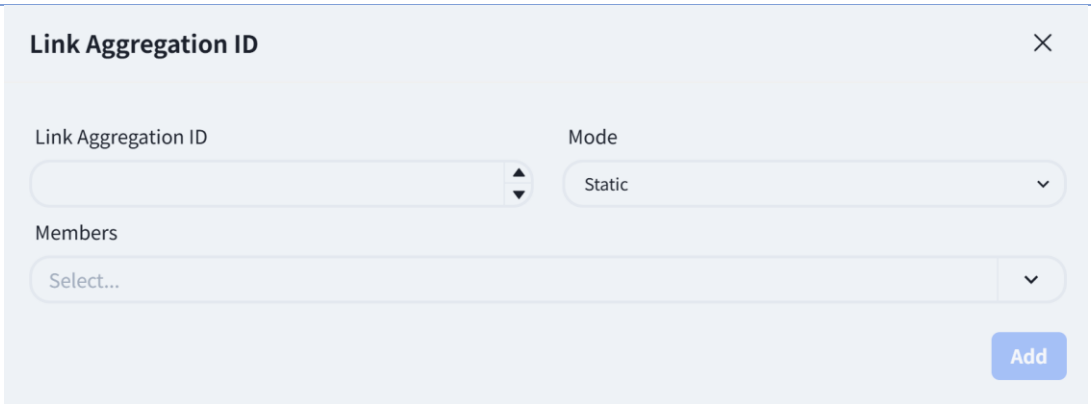
Select **[Device]** as the leaf MC-LAG pair that needs to be configured.

Select **[Device Role]** as leaf.

Follow the prompts on the page to fill in the required business configuration.

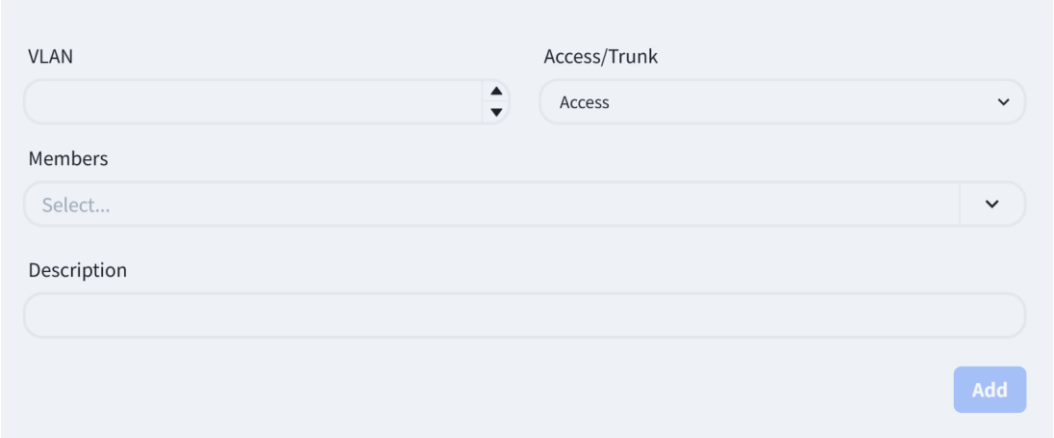


Link Aggregation



- LAG: Link Aggregation ID, users can create IDs within the range of 1501-2000 as needed.
- Mode: Static/LACP, choose whether the link aggregation mode is static or LACP dynamic negotiation.
- Member: Select the member interface connected to this business server.

Services VLAN

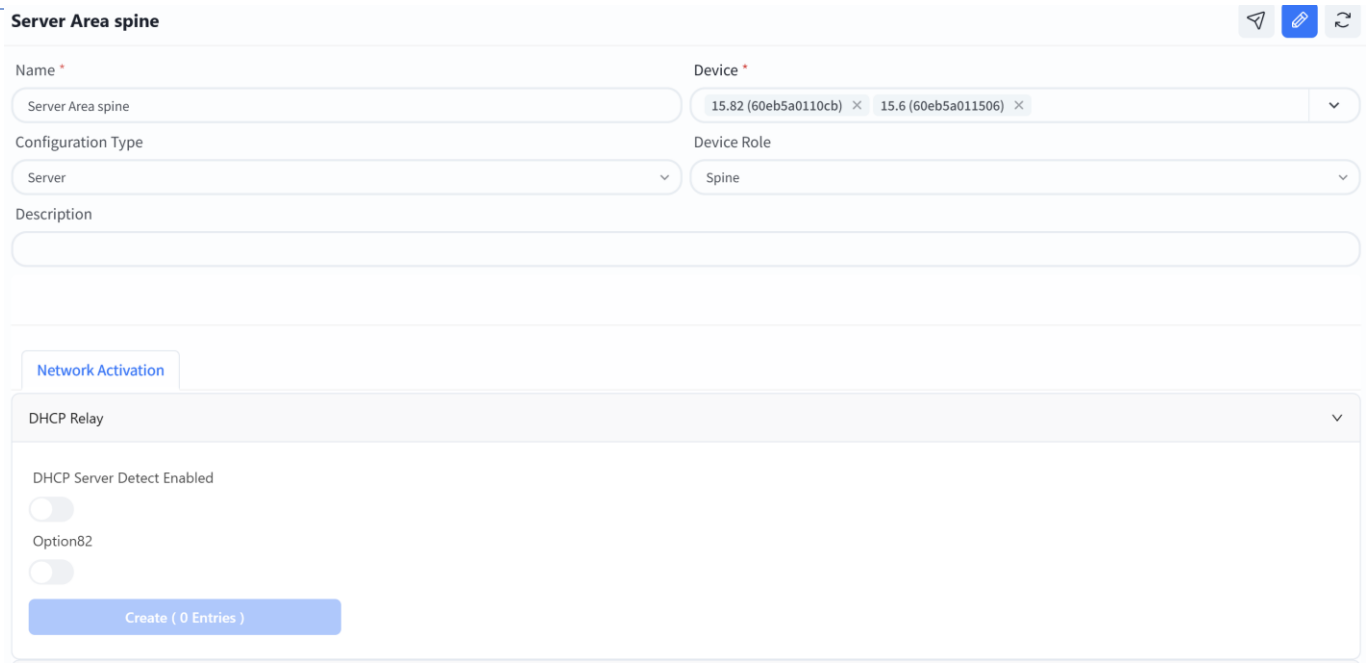


- VLAN: Users can fill in VLAN IDs ranging from 2 to 4050 as needed.
- Access/Trunk: The Access interface is used to connect terminal devices and belongs to a VLAN; The Trunk interface is used to connect network devices and allows traffic from multiple VLANs to pass through.
- Member: Member interfaces can only select LAG ports that have been configured in link aggregation.

6.2.3.2.2 Server Area Spine

The business gateway of MC-LAG network is deployed on Spine devices, and when selecting devices, devices of Spine type also need to be added.

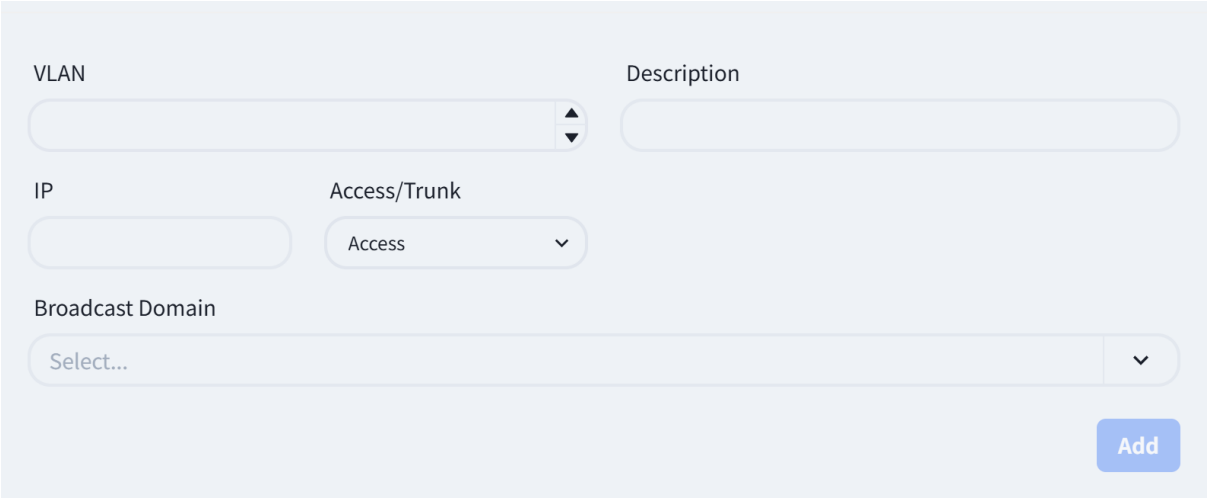
Create a business gateway for the business VLAN corresponding to the Leaf switch in the server area.



If the Spine downstream device needs to obtain an IP address from the Spine upstream DHCP server, a DHCP relay needs to be configured.

- **DHCP Relay:** Configure the IP address of the DHCP server. When the DHCP server does not support recognizing the option82 field, the option82 option needs to be turned off.

Services VLAN



- **VLAN:** The business VLAN corresponding to the Leaf switch in the server area.
- **IP:** Fill in the gateway IP address of the business VLAN.
- **Access/Trunk:** The Access interface is used to connect terminal devices and belongs to a VLAN; The Trunk interface is used to connect network devices and allows traffic from multiple VLANs to pass through.
- **Broadcast domain:** Select the MAC address of the leaf switch corresponding to the VLAN.

6.2.3.3 Network Security Configuration [Optional]

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.2.3.4 User Authentication Configuration [Optional]

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.2.3.5 DHCP

DHCP configuration reference 6.1.3.2, Spine will automatically run DHCP failover to ensure business stability.

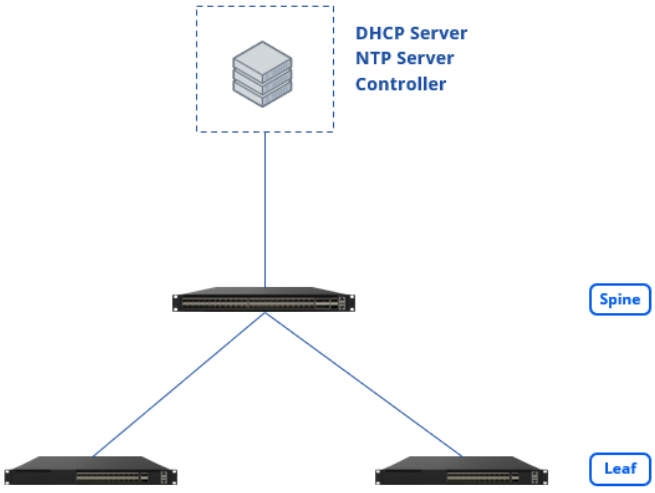
6.2.4 Wireless Service Configuration

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.2.5 Configuration Release

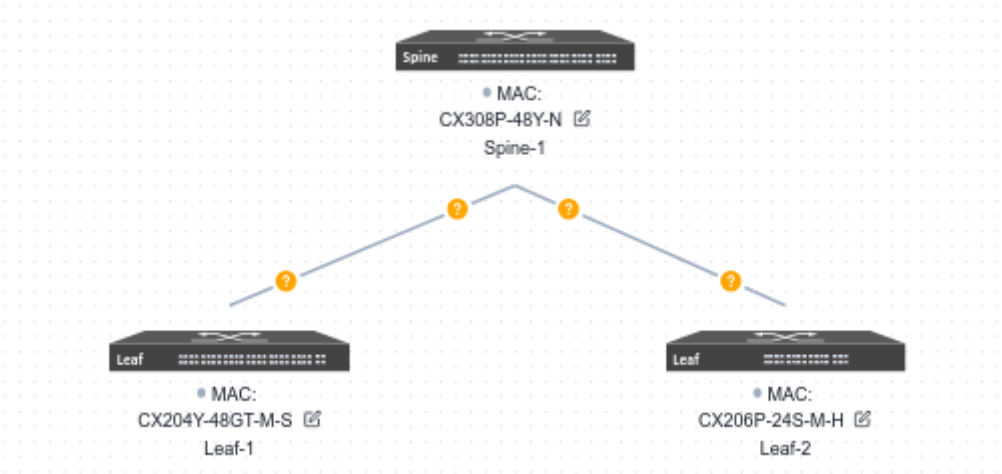
The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.3 Traditional L2 Network Deployment



6.3.1 Design Topology

Device selection and topology editing is the same as for the Small/Mid-Scale Campus network. The topology is summarized as shown below:

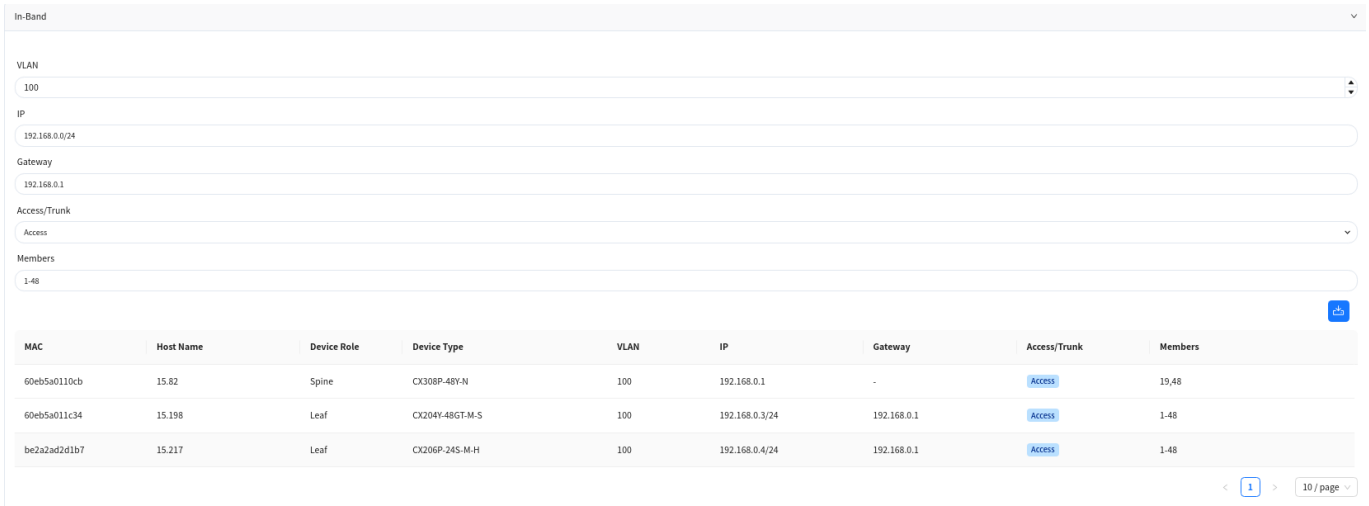


6.3.2 Basic Network

6.3.2.1 In-Band Management

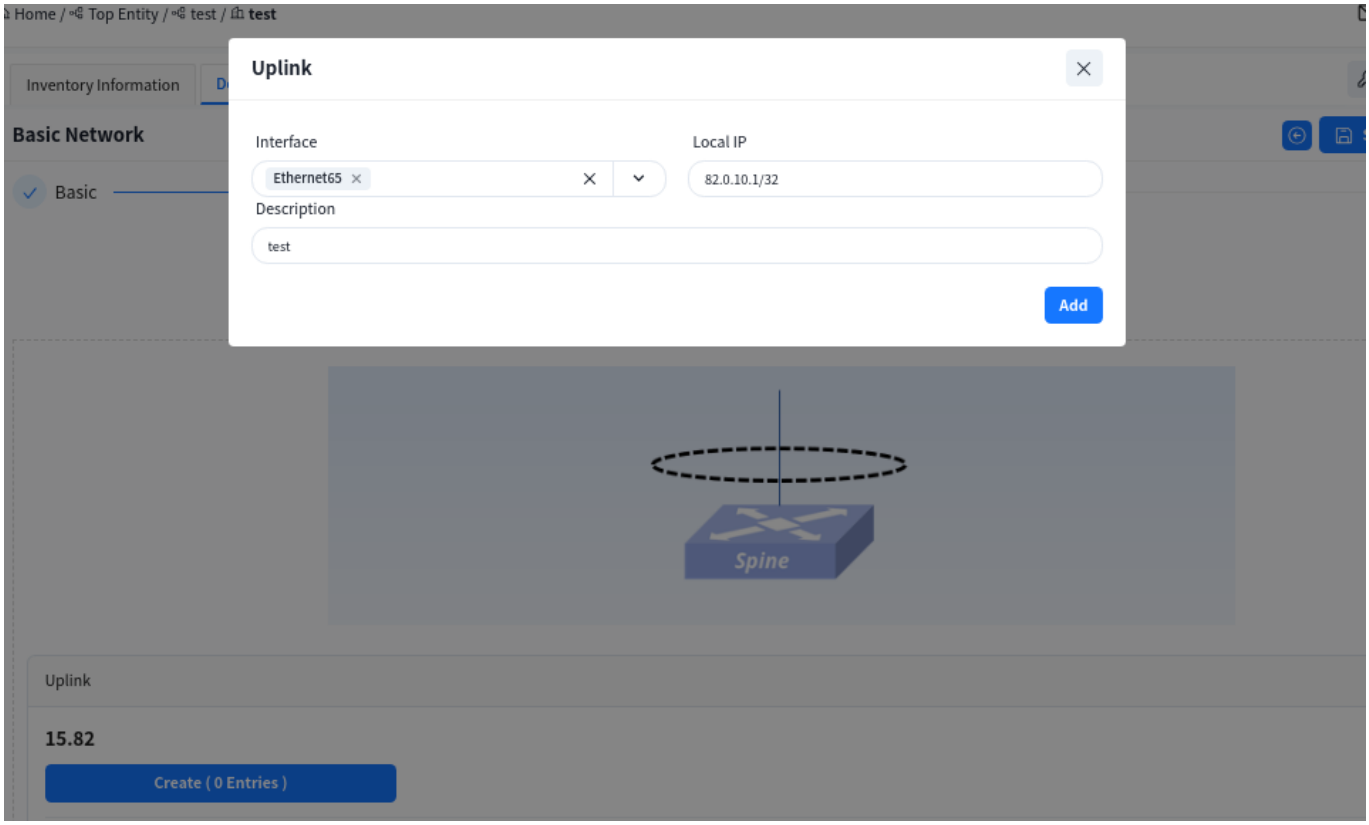
In the traditional Layer 2 network scenario, the in-band management method for Leaf devices is as follows: create a VLAN interface as the in-band management interface to connect to the controller. On the current page, administrator can specify a VLAN ID as the in-band management VLAN, configure the address segment of the management IP and the gateway address for in-band management (this gateway address will be configured on the Spine device), and select the member interfaces of the VLAN and the mode (trunk/access) when joining the VLAN.

The controller will allocate a management IP address from the specified address segment for each Leaf switch and present the allocation results in the table below:

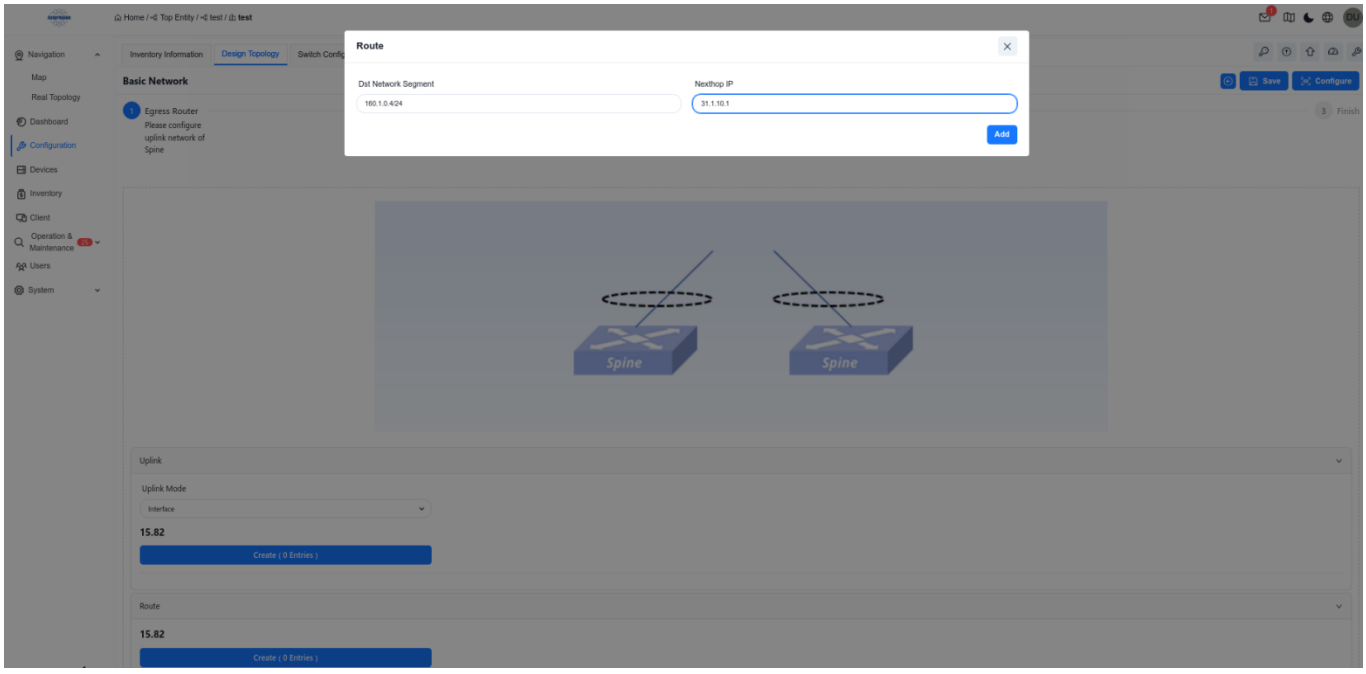


6.3.2.2 Egress Route

Select the interface ID of the Spine device's up-link interface and configure the IP address.



In the traditional L2 scenario, Spine devices only support connecting to external network by configuring static routes. To ensure normal network operation, it is generally necessary to configure a default route.



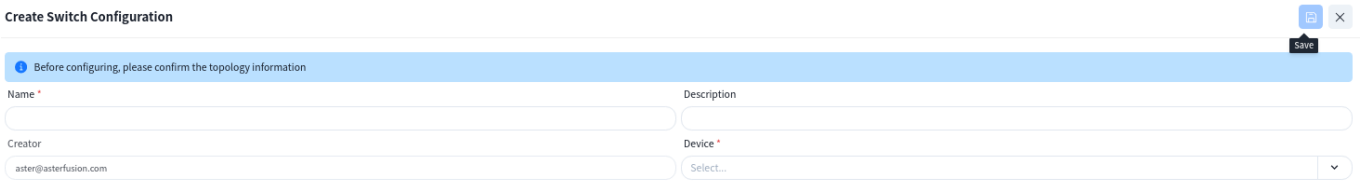
6.3.2.3 Device Management

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network**

Deployment], please refer to the previous section to complete the configuration.

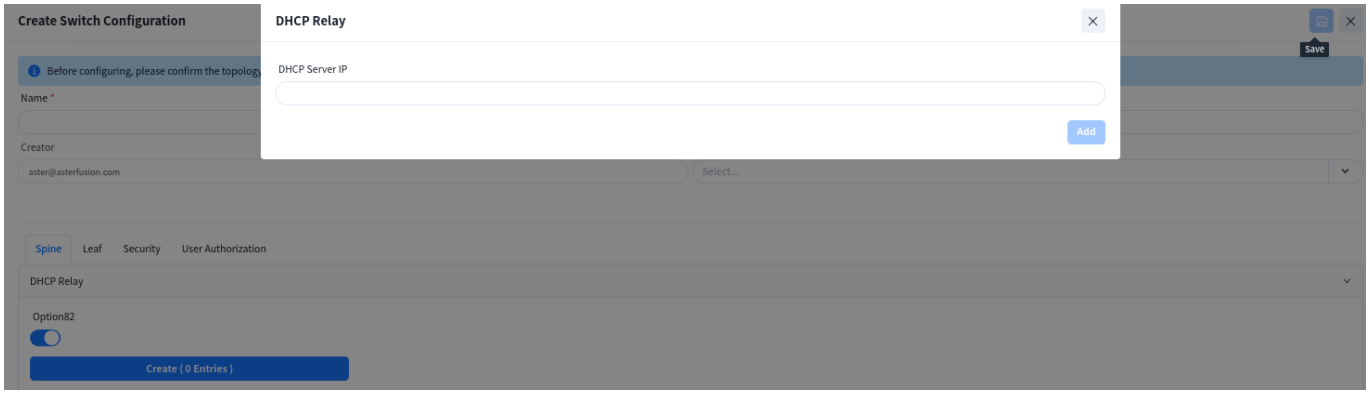
6.3.3 Wired Service Configuration

Unlike full L3 networks, the service network in traditional L2 networks is deployed on Spine devices. Therefore, when selecting devices, Spine-type devices must also be added.

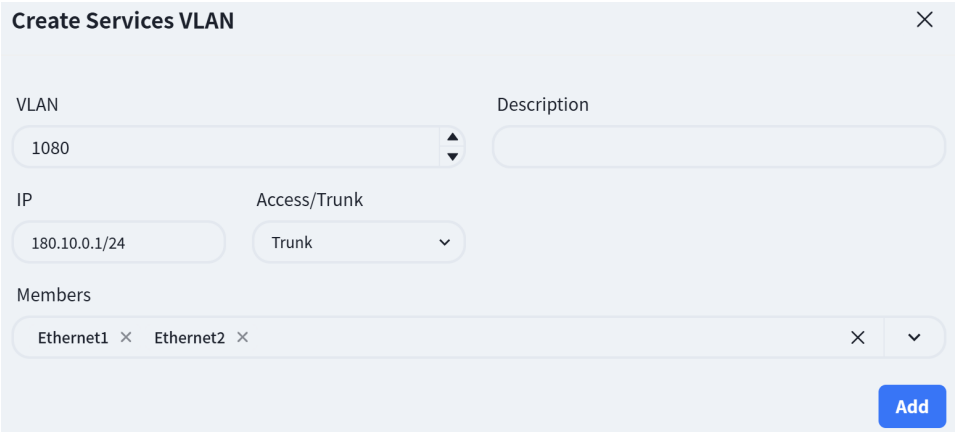


6.3.3.1 Spine

In addition to serving as a service gateway, DHCP relay is enabled on Spine devices, allowing broadcast DHCP requests from APs and terminals to be converted into unicast packets via DHCP relay and sent to the DHCP server.



Create service VLAN:



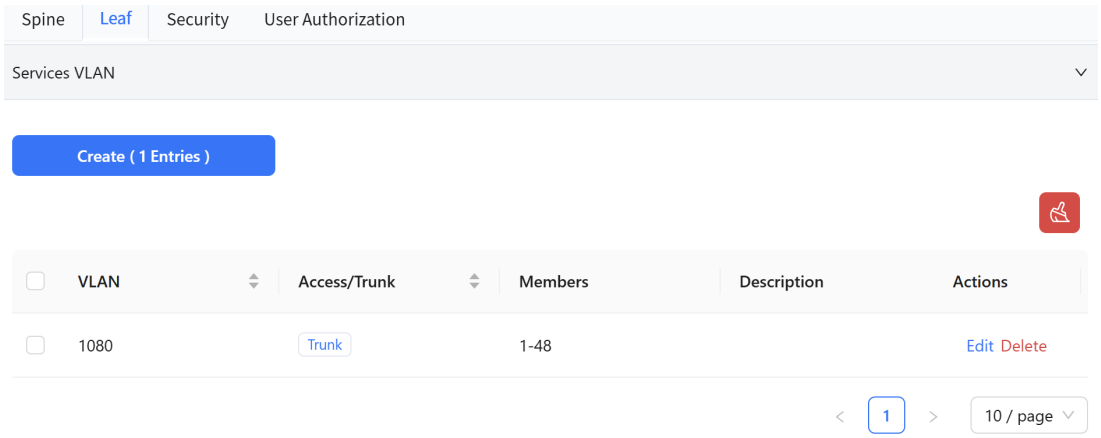
- **[DHCP Relay]**: Configure the IP address of the DHCP server. When the DHCP server does not support recognizing the option82 field, the option82 option needs to be disabled.
- **[VLAN]**: Create service VLANs. Note that in addition to basic service VLANs, a management VLAN for

user APs to connect to the controller must also be created.

- **[IP]**: Configure an address as the gateway for the service VLAN.
- **[Access/Trunk]**: Select the mode according to whether the interface transmits/receives packets with VLAN tags.
  - **Access**: Accepts packets without VLAN tags, typically configured for the AP management VLAN.
  - **Trunk**: Accepts packets with VLAN tags, typically configured for service VLANs
- **[Member Interfaces]:** Click the drop-down arrow to select the member interfaces of the VLAN on the Spine device, usually all interfaces connected to the Leaf switch.

6.3.3.2 Leaf

The Leaf switch is purely configured for Layer 2. On this interface, only the VLAN ID and member interfaces need to be specified, and all other configurations are generated by the controller.



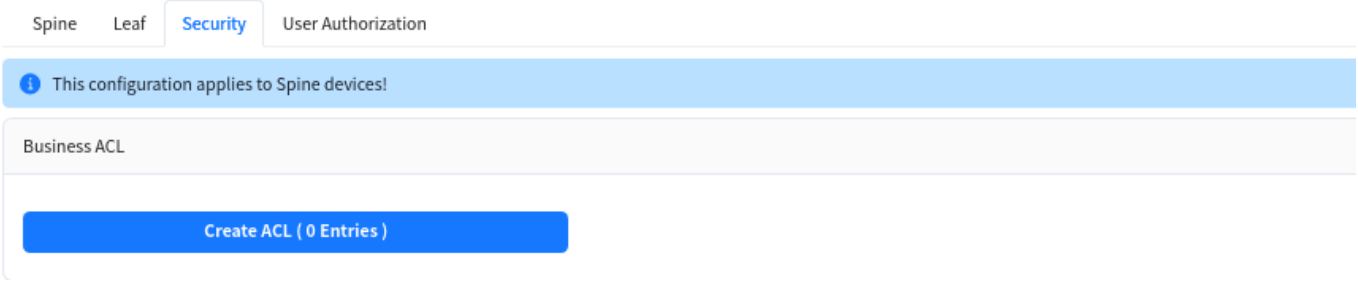
Wired Terminal Information Collection Enable

Enabling this function on an interface will report terminal information under the interface to the controller.

6.3.3.3 security [optional]

Create Service ACLs to configure access control lists between services in different network segments.

Note: This configuration takes effect on Spine devices, and VLAN isolation is applied between Leaf devices.



6.3.3.4 User Access Authentication Configuration [Optional]

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.3.3.5 DHCP

DHCP configuration reference 6.1.3.2

6.3.4 Wireless Service Configuration

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.3.5 Configuration Release

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

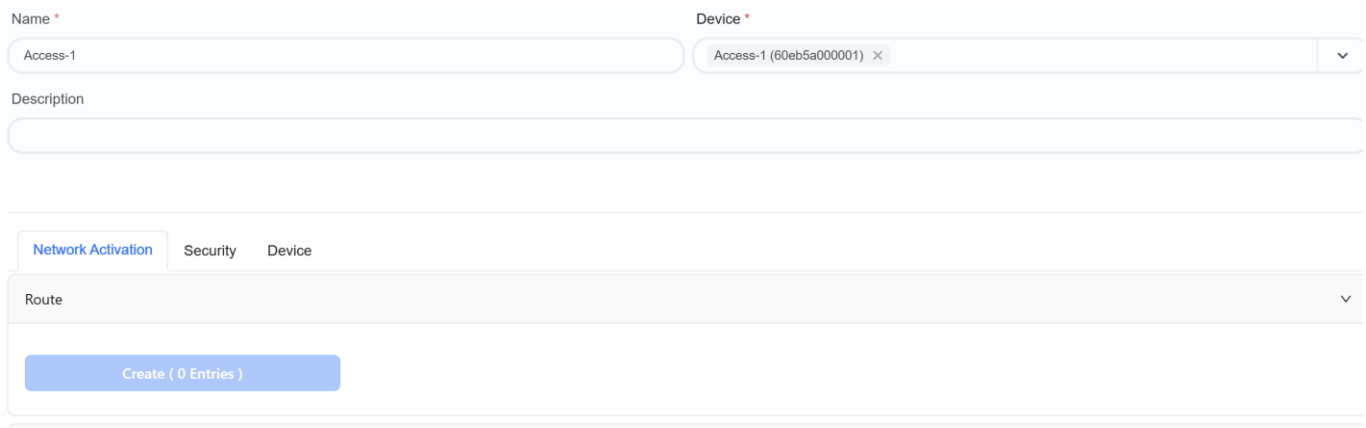
6.4 Open Cloud Connect

The Open Cloud Connect scenario enables classic Layer 2 and Layer 3 functions on standalone devices, providing flexible combination capabilities. Gateways can be deployed on aggregation or access devices. This approach is suitable for standalone device scenarios, scenarios where all devices share the same configuration, and specialized scenarios that cannot be addressed by generic solutions. It also allows users to configure DHCP servers on Leaf devices.

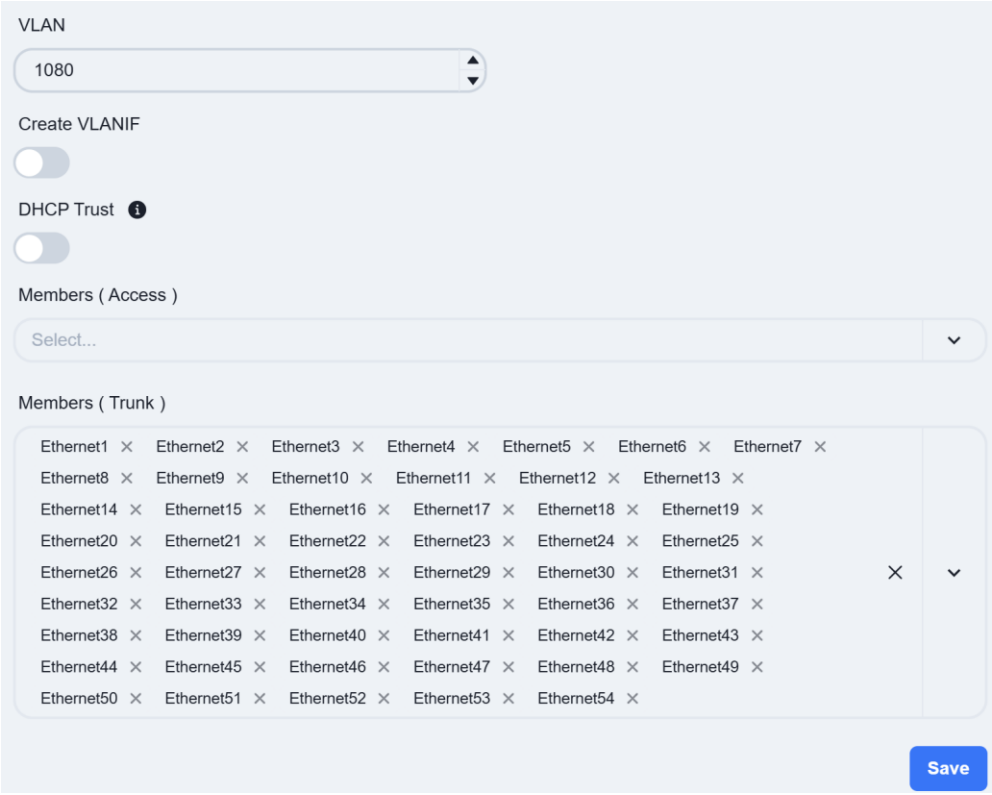
6.4.1 Wired Service Configuration

6.4.1.1 Gateway Deployed on Aggregation Devices

When the gateway is deployed on aggregation devices, the Leaf switches are configured as pure Layer 2 devices. On this view, service VLAN IDs and member interfaces need to be specified, while the remaining configurations are generated by the controller.



Select the downstream and upstream port of the switch for the member interface of the services VLAN.



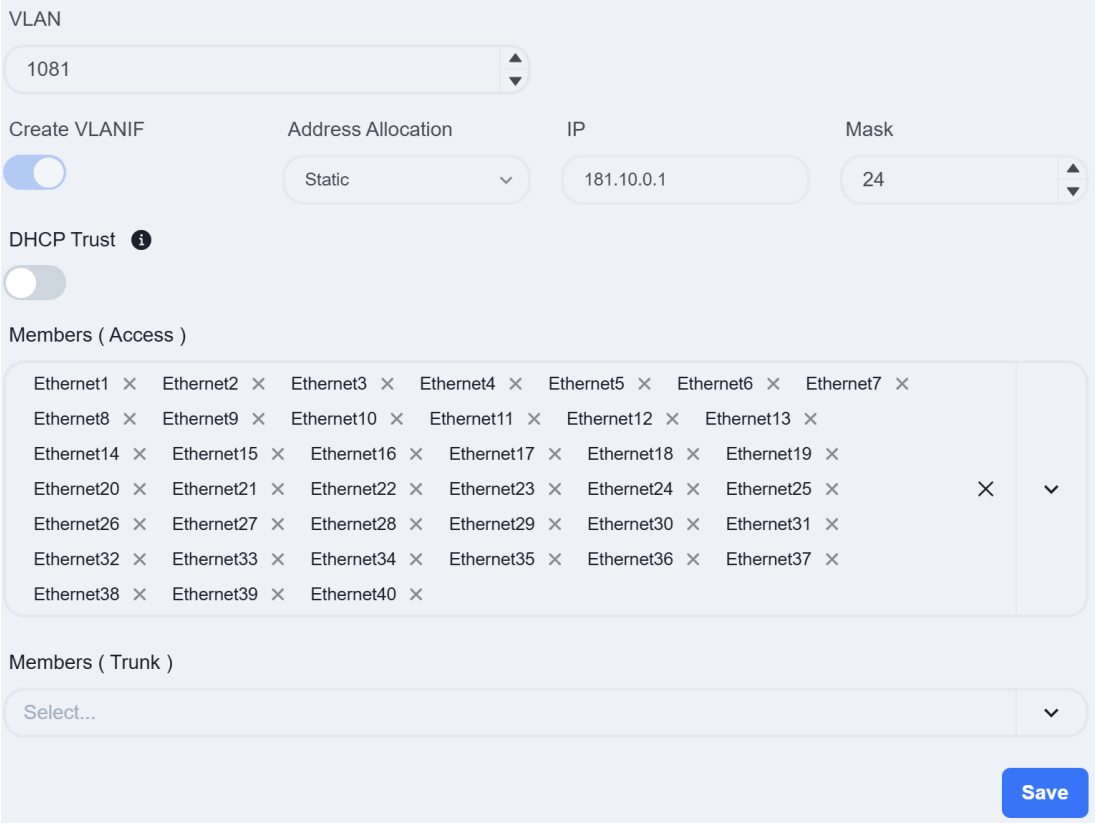
6.4.1.2 Gateway Deployed on Access Devices

If the gateway is deployed on access devices, you need to enable 【Create VLANIF】 when creating the

service VLAN and fill in the 【IP】 as the gateway address for this service. The remaining configurations are consistent with section 6.4.1.1.

Note: When the gateway is deployed on access devices, if downstream terminals need to obtain IP addresses via DHCP to go online, you must configure the required DHCP address pool on the access devices or set up DHCP relay on the access devices to ensure that the request packets from the terminals can reach the designated DHCP server.

Configure the service gateway:

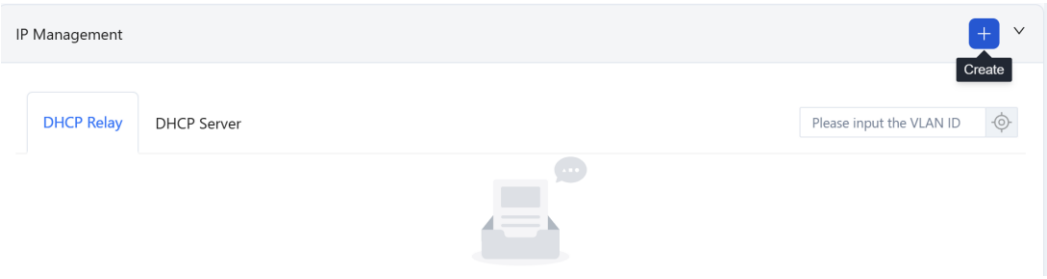


IP: Configure the address as the gateway address for this service VLAN.

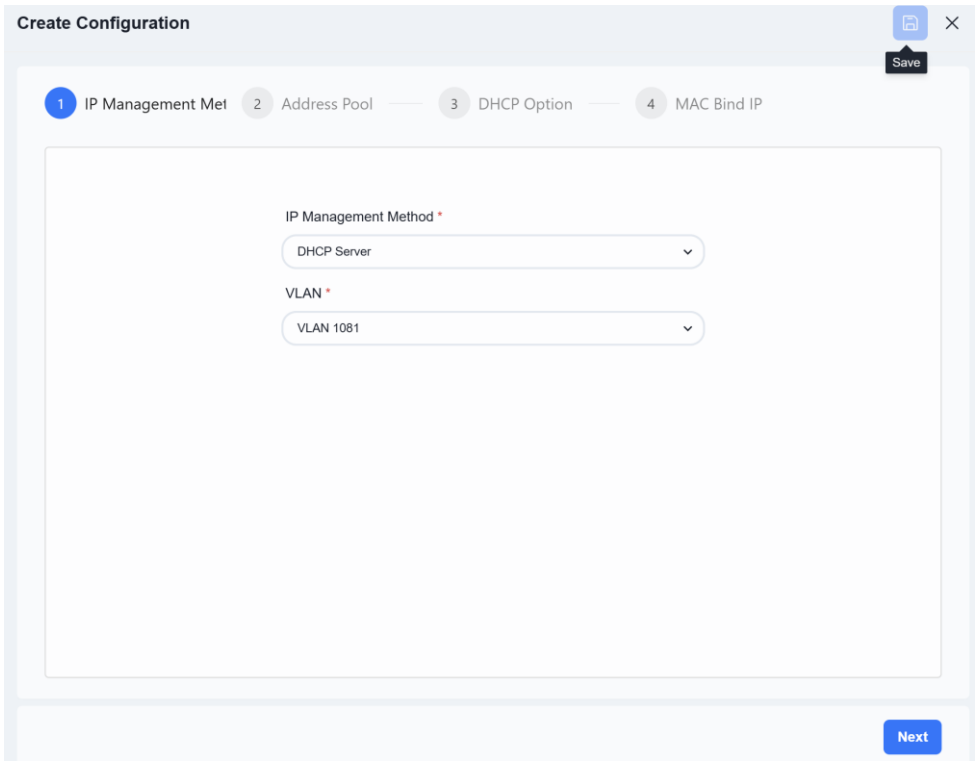
6.4.1.2.1 Configure DHCP Server

The Open Cloud Connect scenario supports users in configuring a DHCP server on access devices.

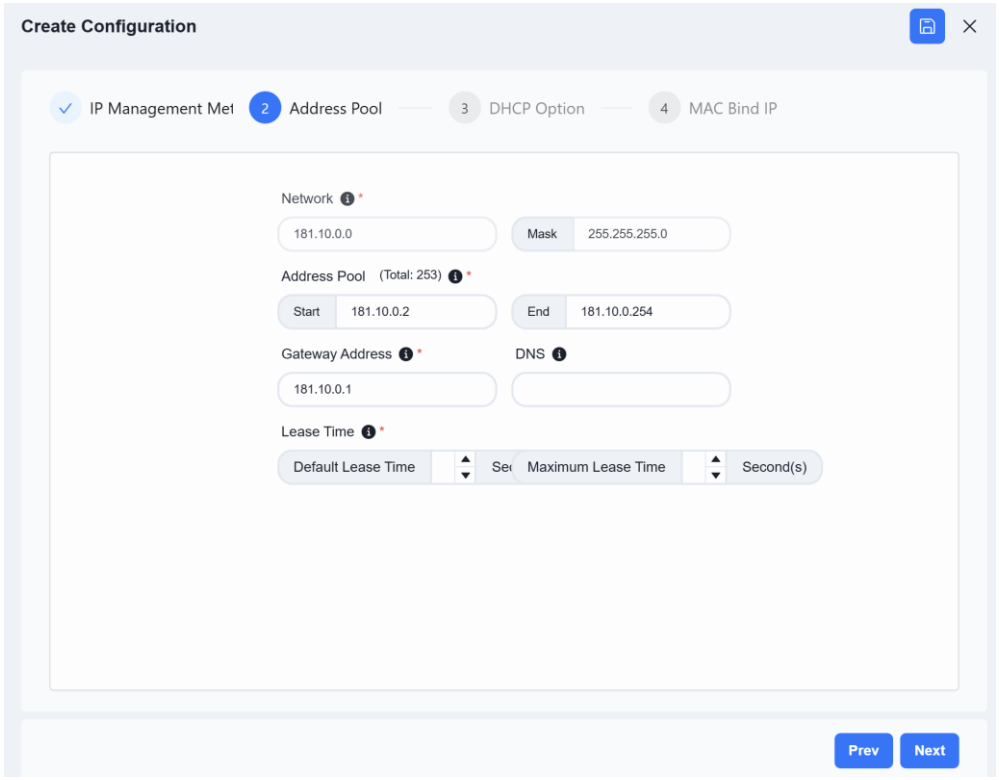
Click the **[+]** on the right side of **[IP Management]** to create a DHCP server.



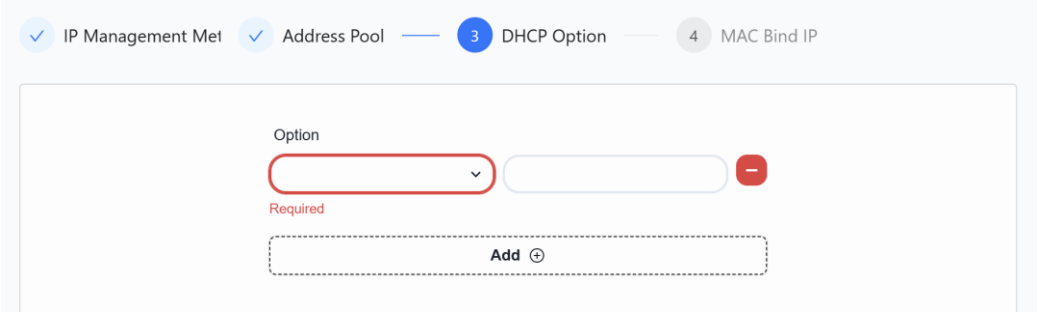
Select the IP Management method as **[DHCP Server]**, choose VLAN and click **[Next]**



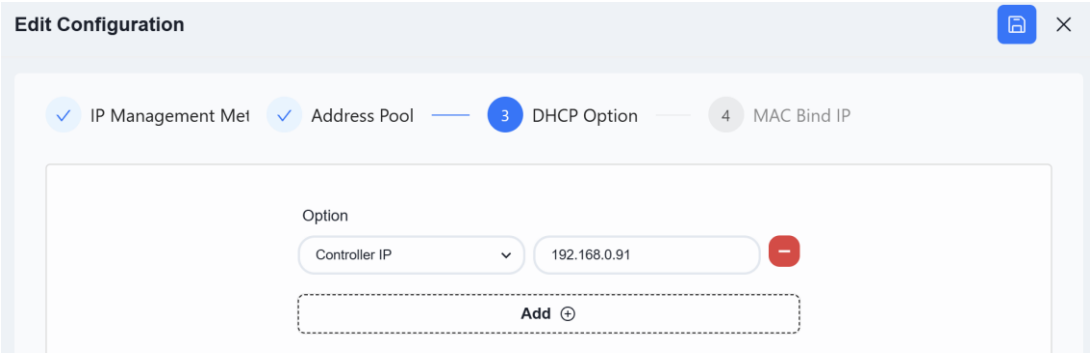
Configure the Network, Address Pool range, Gateway Address, and Lease Time.



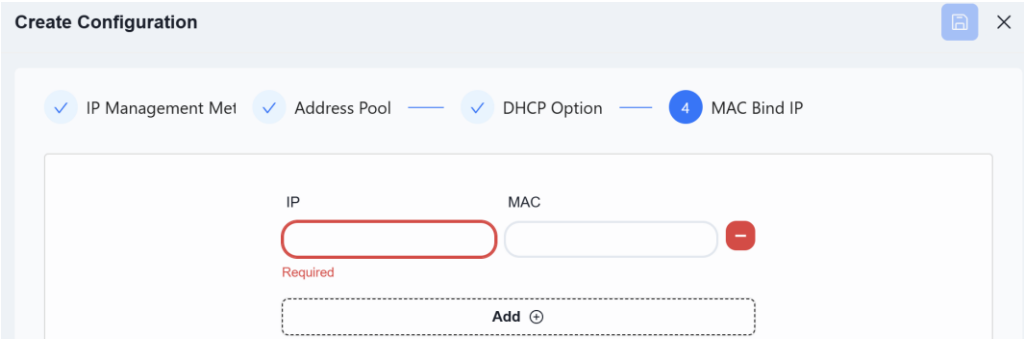
Configure DHCP Option(Optional)



If clients connected under the AP need to access the controller, the controller address must be added in the DHCP Option page when configuring the AP address pool.

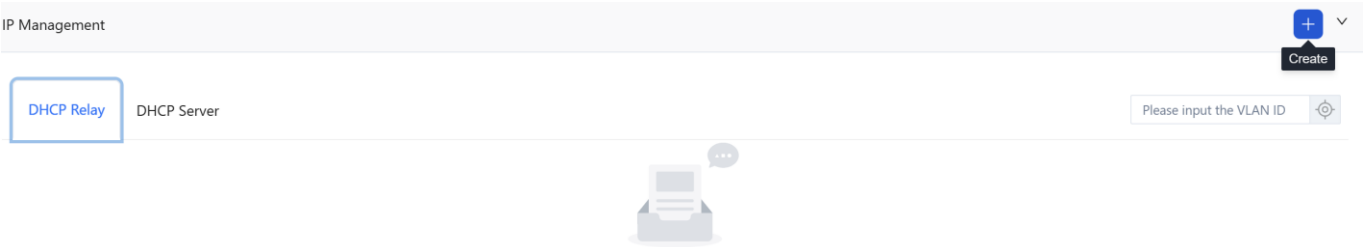


Configure MAC Bind IP (Optional). Once all configurations are complete, click **[Save]** in the upper-right corner.

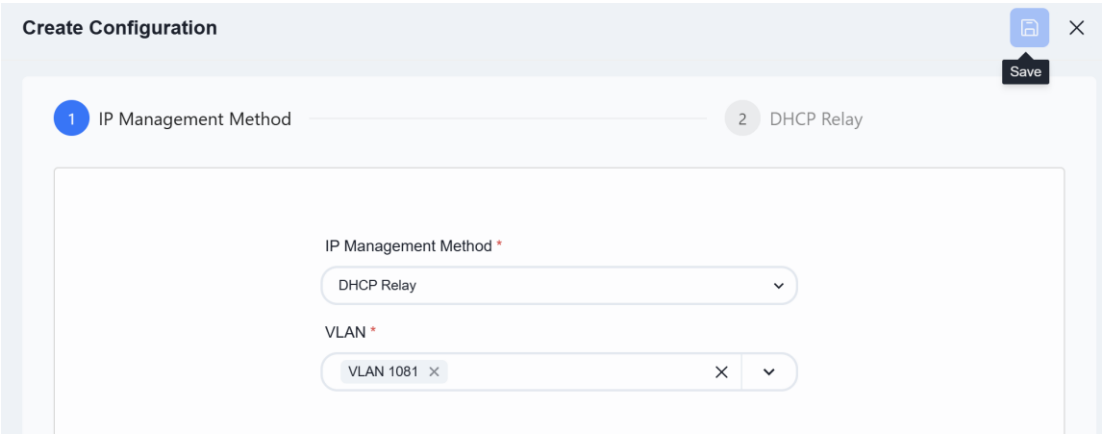


6.4.1.2.2 Configure DHCP Relay

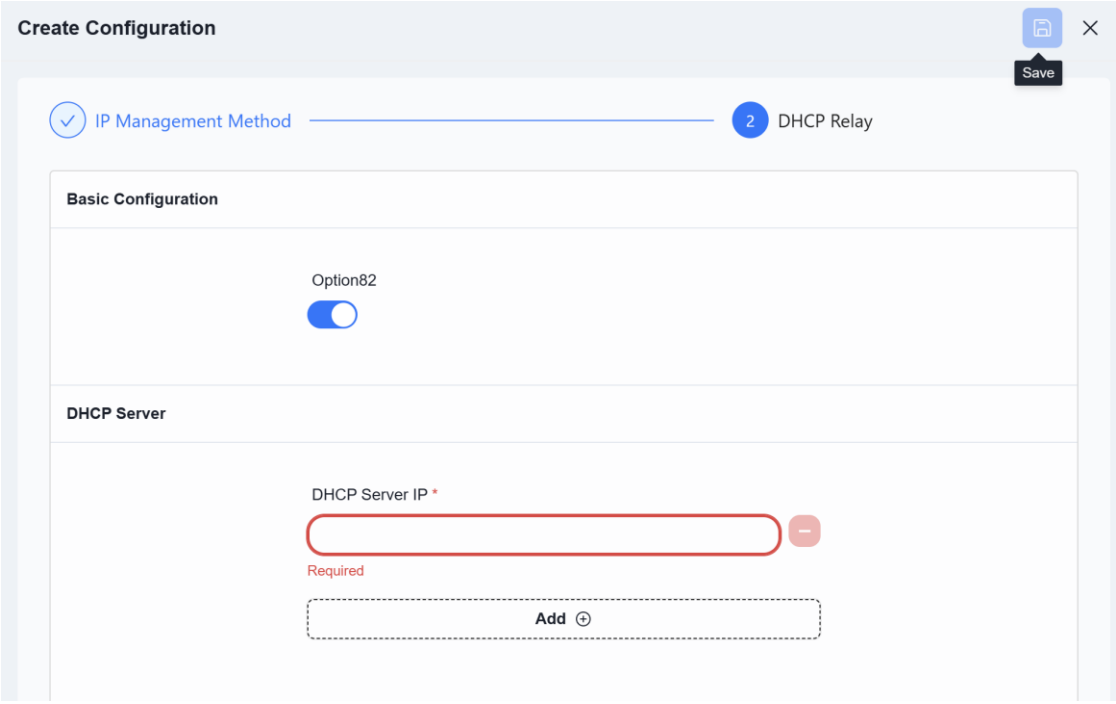
Click the [+] on the right side of [IP Management] to configure the DHCP relay.



Select **[IP Management]** method as **[DHCP Relay]**, and choose the service VLAN that requires relay configuration.



Click **[Next]**, enter the DHCP server IP, and then click **[Save]** in the top right corner to complete the configuration.



Option 82: DHCP Relay Agent Information Option. Option 82 is inserted by the DHCP relay agent when forwarding the DHCP client discovery message. When the relay agent receives a broadcast request from a client, it converts it to unicast and sends it to the DHCP server, along with the Option 82 information. (Optional)

6.4.1.3 Network Security Configuration [Optional]

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.4.1.4 Device Management[Optional]

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network**

Deployment], please refer to the previous section to complete the configuration.

6.4.1.5 POE[Optional]

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.4.1.6 Wired Clients Information Collection[Optional]

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.4.2 WiFi Configuration

The configuration of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.4.3 Configuration Release

The open cloud connect scenario does not require the issuance of basic network configuration, and the rest of this part is consistent with the Egress route of **[Small/Mid-Scale Network Deployment]**, please refer to the previous section to complete the configuration.

6.5 PON

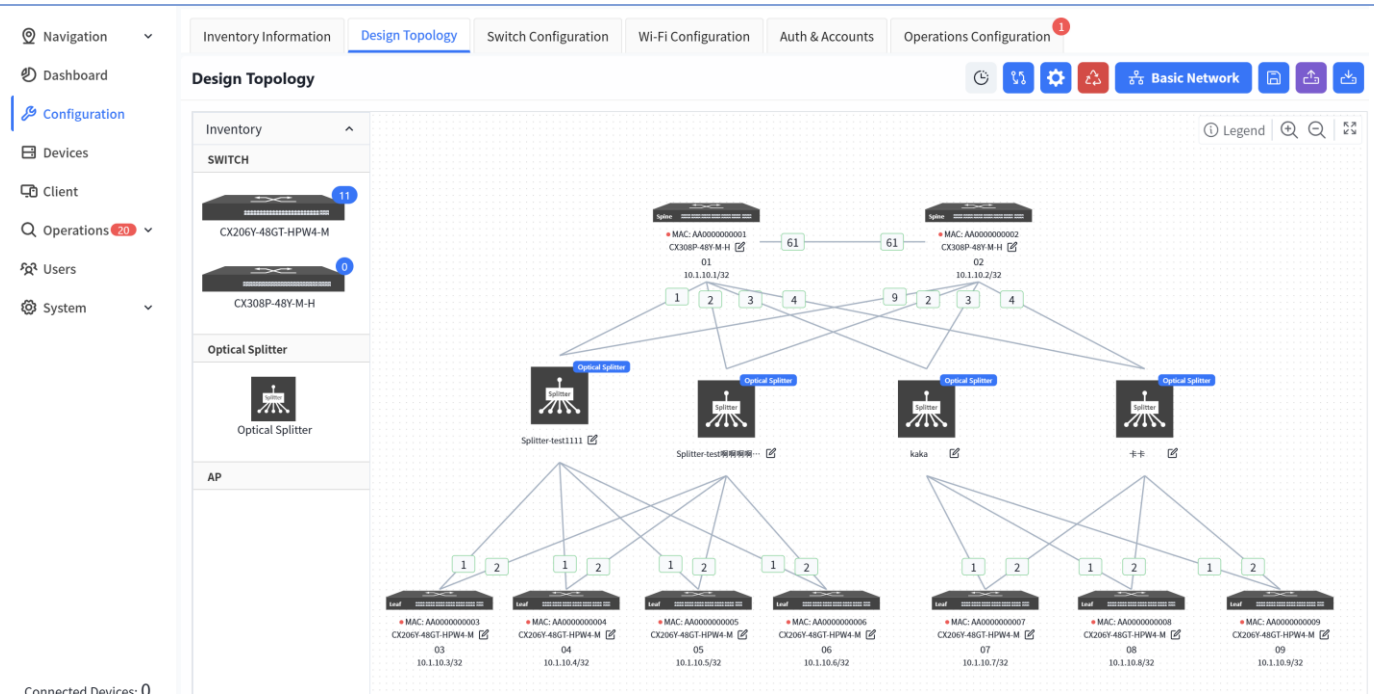
PON is a fiber access technology that achieves single-fiber sharing, high bandwidth and low cost through passive optical distribution networks. The controller currently supports the configuration of OLT Stick and the status viewing of OLT Stick and ONU.

6.5.1 Add Devices

Only the OLT need to be imported. The ONU and splitter do not need to be imported.
The import method can be referred to 4.2.1

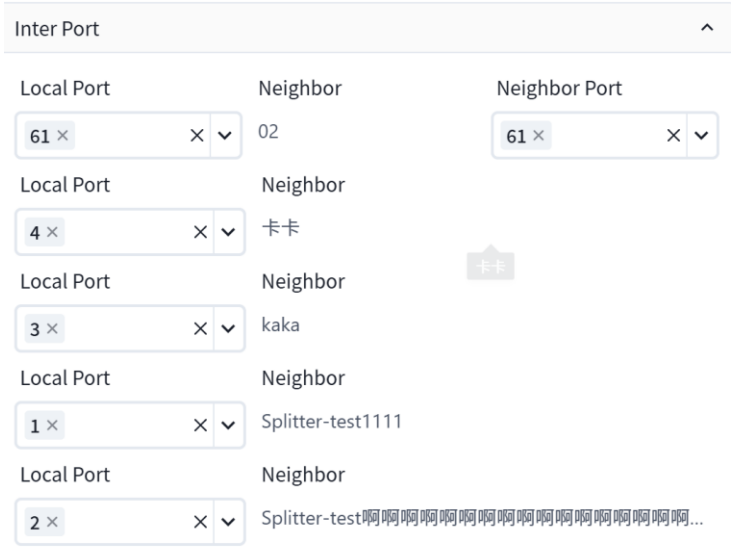
6.5.2 Design Topology

If a splitter is to be used between Spine and Leaf, to make the topological wiring relationship clear, the splitter needs to be incorporated into the topological planning.

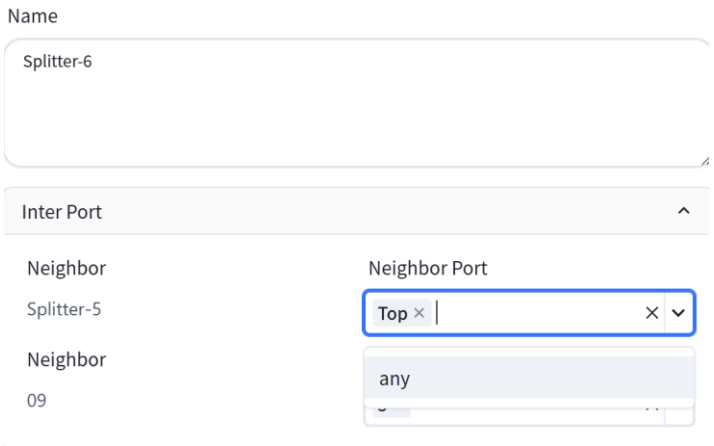


In the scene planning topology of Small/Mid-Scale Network Scenarios, splitters is included by default. Users can freely plan the switch side as needed.

The interface of this end needs to be filled in. For the rest of the content, please refer to 6.1.1



If the user adopts a multi-layer spectrometer, the interface of the opposite end spectrometer needs to be filled in the spectrometer.

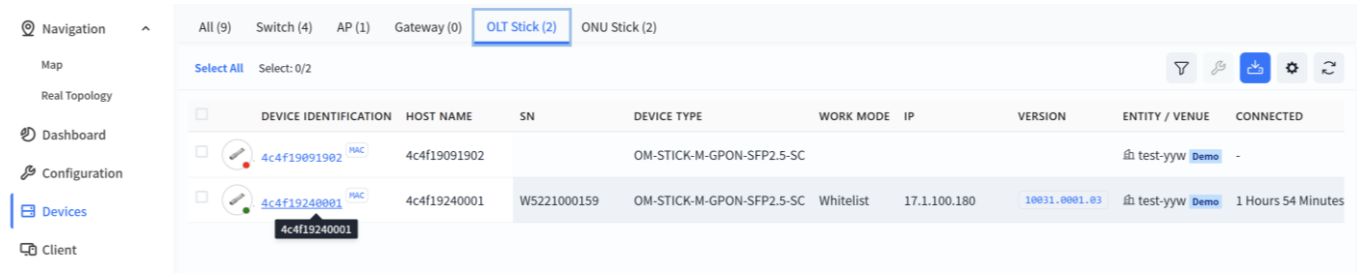


top: Refers to the port in the uplink direction

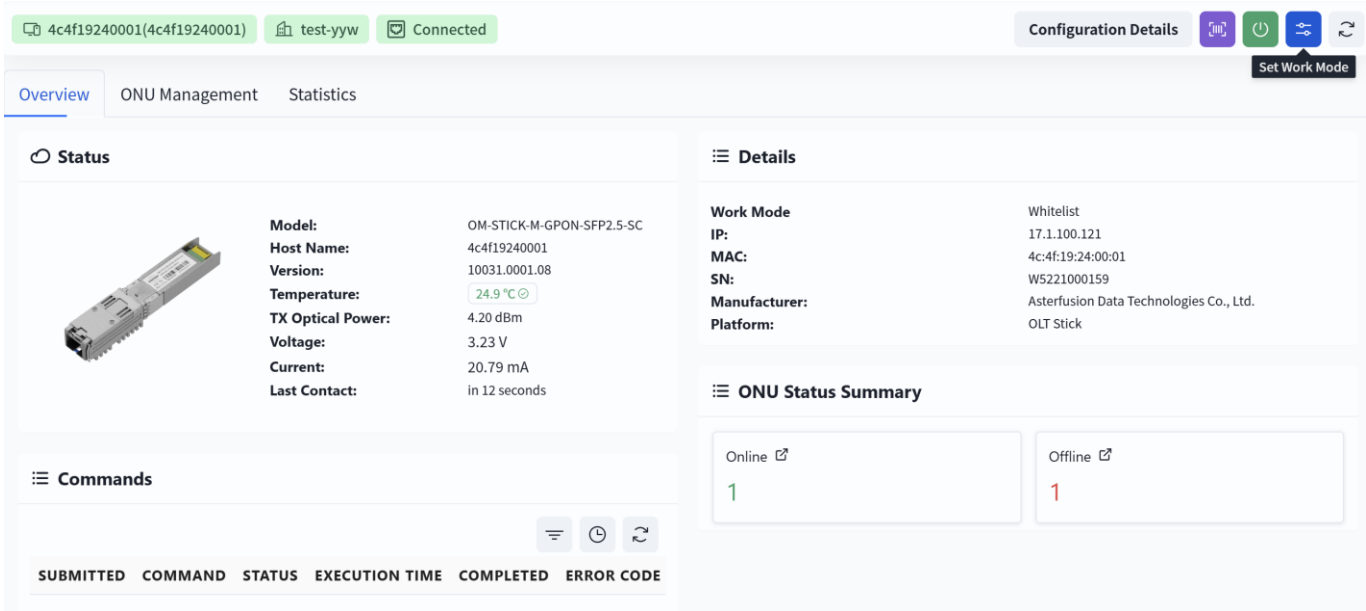
any: Refers to the port in the downlink direction

6.5.3 OLT Stick Configuration

On the **[Devices]** view, click on the OLT device identifier that needs to be configured to enter the device overview.

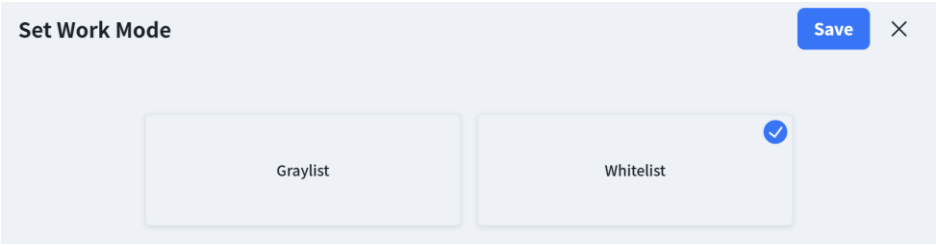


Users can view the basic information of this OLT on this view.



6.5.3.1 Work Mode

Click on the **[Set Work Mode]** button at the top right corner.

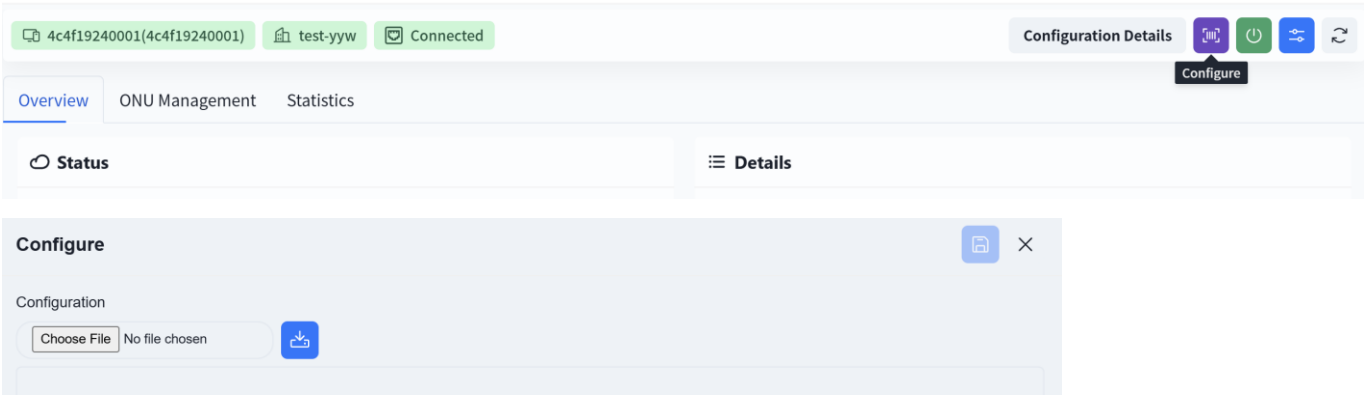


Graylist: In this working mode, the OLT Stick allows all ONUs to access by default and does not impose access restrictions.

Whitelist: In this working mode, access restrictions on ONUs are supported.

6.5.3.2 Configure

Click on the **[Configure]** at the top right corner – **[Choose File]** to issue the configuration for the OLT Stick.



The format of the configuration file content is as follows:

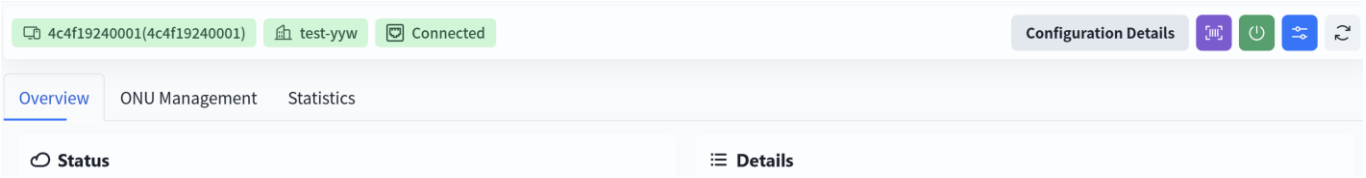
```
#ONU service tpye template
>ONU_service_name:    SFU_type1
>ONU_service_number:  1                              #very important, must be 0~255

<flow 1 start>                      //example for VOIP
         >max_BD    10              //uint16_t, max bandwith , Unit 20Kbit/s    ---10*20 =200K
         >fix_BD     4              //uint16_t, fixed bandwith , Unit 20Kbit/s    ----80K
         >ass_BD     4              //uint16_t, assure bandwith  ,Unit 20Kbit/s    ----80k
         >type       3              //uint8_t, service type
         >priority   7              //uint8_t, priority, 0~7,  0: top priority              ---7
         >weight    100             //uint8_t, range, 1~255, 255: top priority          --- 100
         >valid      0              //uint8_t, enable the flow: 1; disable the flow: 0      ---0
         >vlan1_id   0              //uint16_t, pptep1  VLAN(TCI), 0: no vlan is required
         >vlan2_id   0              //uint16_t, pptep2  VLAN(TCI),
         >vlan3_id   0              //uint16_t, pptep3  VLAN(TCI),
         >vlan4_id   0              //uint16_t, pptep4  VLAN(TCI),
```

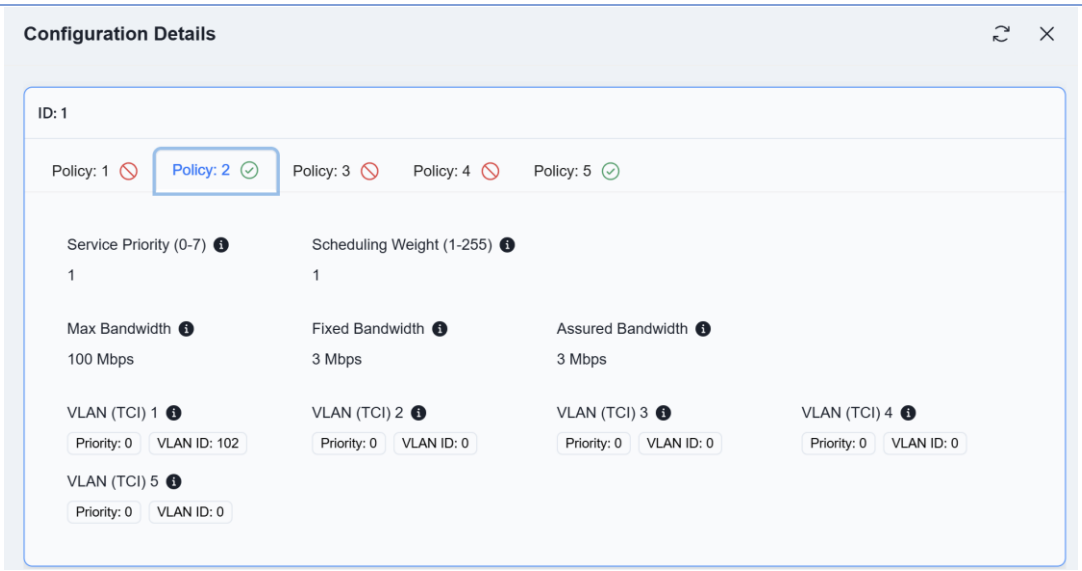
```
         >vlan5_id   0             //uint16_t, pptep5  VLAN(TCI),   ---- priority = 7, vlan =103
<end>

<flow 2 start>                     // for muticast
         >max_BD    5000          //uint16_t, max bandwith , Unit 20Kbit/s   ---5000*20 =100M
         >fix_BD     150          //uint16_t, fixed bandwith , Unit 20Kbit/s    --150*20 = 3M
         >ass_BD     150          //uint16_t, assure bandwith  ,Unit 20Kbit/s     --150*20 = 3M
         >type        3           //uint8_t, service type
         >priority    1           //uint8_t, priority, 0~7,  0: top priority              ---1
         >weight      1           //uint8_t, range, 1~255, 255: top priority          --- 1
         >valid       1           //uint8_t, enable the flow: 1; disable the flow: 0      ---0
         >vlan1_id   102          //uint16_t, pptep1  VLAN(TCI), 0: no vlan is required     ---
priority = 0, vlan =101
         >vlan2_id   0            //uint16_t, pptep2  VLAN(TCI),
         >vlan3_id   0            //uint16_t, pptep3  VLAN(TCI),
         >vlan4_id   0            //uint16_t, pptep4  VLAN(TCI),
         >vlan5_id   0            //uint16_t, pptep5  VLAN(TCI),
<end>

<flow 3 start>                    //reserved
         >max_BD    5000          //uint16_t, max bandwith , Unit 20Kbit/s   ---5000*20 =100M
         >fix_BD     150          //uint16_t, fixed bandwith , Unit 20Kbit/s    --150*20 = 3M
         >ass_BD     150          //uint16_t, assure bandwith  ,Unit 20Kbit/s     --150*20 = 3M
         >type        3           //uint8_t, service type
         >priority    1           //uint8_t, priority, 0~7,  0: top priority              ---1
         >weight      1           //uint8_t, range, 1~255, 255: top priority          --- 1
         >valid       0           //uint8_t, enable the flow: 1; disable the flow: 0      ---0
         >vlan1_id    0           //uint16_t, pptep1  VLAN(TCI), 0: no vlan is required     ---
priority = 0, vlan =101
         >vlan2_id   0            //uint16_t, pptep2  VLAN(TCI),
         >vlan3_id   0            //uint16_t, pptep3  VLAN(TCI),
         >vlan4_id   0            //uint16_t, pptep4  VLAN(TCI),
         >vlan5_id   0            //uint16_t, pptep5  VLAN(TCI),
<end>

<flow 4 start>                    //reserved
         >max_BD    5000          //uint16_t, max bandwith , Unit 20Kbit/s   ---5000*20 =100M
         >fix_BD     150          //uint16_t, fixed bandwith , Unit 20Kbit/s    --150*20 = 3M
         >ass_BD     150          //uint16_t, assure bandwith  ,Unit 20Kbit/s     --150*20 = 3M
         >type        3           //uint8_t, service type 1~5
         >priority    1           //uint8_t, priority, 0~7,  0: top priority              ---1
         >weight      1           //uint8_t, range, 1~255, 255: top weight          --- 1
         >valid       0           //uint8_t, enable the flow: 1; disable the flow: 0      ---0
         >vlan1_id   101          //uint16_t, pptep1  VLAN(TCI), 0: no vlan is required     ---
priority = 0, vlan =101
         >vlan2_id    0           //uint16_t, pptep2  VLAN(TCI),
         >vlan3_id    0           //uint16_t, pptep3  VLAN(TCI),
```

```
         >vlan4_id    0           //uint16_t, pptep4  VLAN(TCI),
         >vlan5_id    0           //uint16_t, pptep5  VLAN(TCI),
<end>

<flow 5 start>                   //for internet
         >max_BD    25000         //uint16_t, max bandwith , Unit 20Kbit/s   ---25000*20 =500M
         >fix_BD     150          //uint16_t, fixed bandwith , Unit 20Kbit/s    --150*20 = 3M
         >ass_BD     150          //uint16_t, assure bandwith  ,Unit 20Kbit/s     --150*20 = 3M
         >type        3           //uint8_t, service type
         >priority    1           //uint8_t, priority, 0~7,  0: top priority              ---1
         >weight      1           //uint8_t, range, 1~255, 255: top priority          --- 1
         >valid       1           //uint8_t, enable the flow: 1; disable the flow: 0      ---0
         >vlan1_id    0           //uint16_t, pptep1  VLAN(TCI), 0: no vlan is required ,         -
priority = 0, vlan =101
         >vlan2_id    0           //uint16_t, pptep2  VLAN(TCI),
         >vlan3_id    0           //uint16_t, pptep3  VLAN(TCI),
         >vlan4_id    0           //uint16_t, pptep4  VLAN(TCI),
         >vlan5_id    0           //uint16_t, pptep5  VLAN(TCI),
<end>

#end of service type definition
```

After the upload is completed, click **[Save]**, and the controller will automatically complete the configuration distribution.

Click on **[Configuration Details]**, and users can see the current configuration of OLT Stick on the controller.





Policy: Each policy represents a type of business, with a maximum of 5 policies supported. The green suffix icon indicates that the policy is in use, while the red one indicates it is not.

Service Priority: The smaller the value, the higher the priority. Used to determine which service flow passes first during network congestion; high-priority services (e.g., Voice) take precedence over low-priority services (e.g., General Data).

Scheduling Weight: Used for Weighted Fair Queuing (WFQ) during bandwidth allocation. It determines the proportional relationship of bandwidth obtained by service flows under equal priority, enabling finer bandwidth allocation control.

Max Bandwidth: Defines the peak bandwidth limit usable by this service flow. Traffic exceeding this limit will be dropped or shaped. Used to prevent a single service from occupying too many network resources.

Fix Bandwidth: A constant bandwidth that is guaranteed to be allocated to this service flow regardless of whether the network is congested or not. Typically used for delay and jitter-sensitive services such as voice calls.

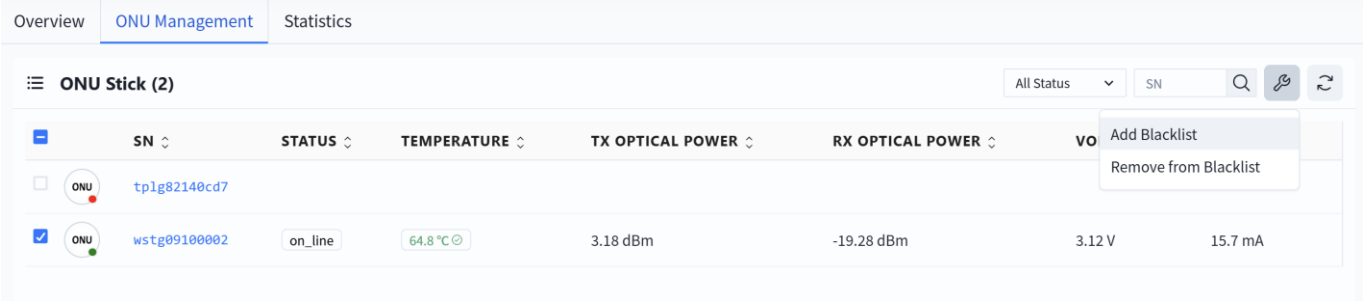
Assure Bandwidth: The minimum bandwidth guaranteed to be available for this service flow during network congestion. When the network is idle, bandwidth exceeding this value can be used. It is used to ensure basic service quality for critical operations.

VLAN(TCI): VLAN Tag Control Information. A 16-bit field encapsulating the complete 802.1Q VLAN tag information, including service priority and network segment identifier. This value is used to control Quality of Service (QoS) classification and packet forwarding within the Ethernet switching network.

6.5.3.3 ONU Management

The controller supports users to manage ONUs through OLT Stick. Click **[ONU Management]**, select the

ONUs to be managed, click **[Operation]** in the upper right corner, and choose the management method.



Add Blacklist: Immediately terminate the service forwarding of this ONU to prevent it from accessing the network.

Remove from Blacklist: Allow ONU to re-initiate the registration process and restore the data forwarding channel.

7 Auth & Accounts

The controller supports users in binding the authentication server and making relevant authentication-related configurations

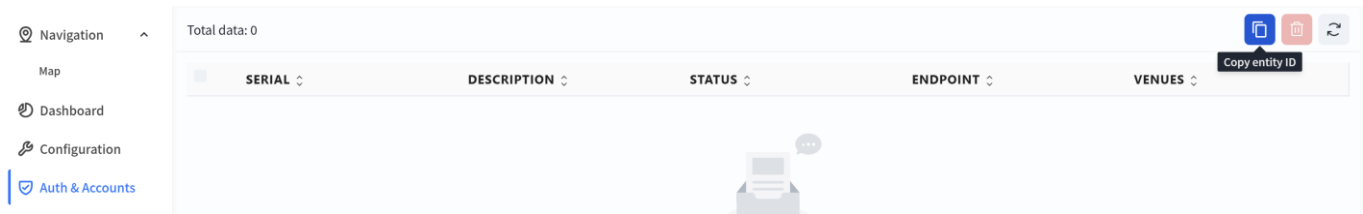
Note: This chapter only configures the authentication server. In actual network usage scenarios, switches proxy the authentication of wired terminals; APs proxy the authentication of wireless terminals. It is necessary to configure the authentication functions of switches and APs respectively in the wired service configuration and wireless service configuration.

7.1 Bind NAC

The current authentication server needs to be launched in the entity through background configuration first, and then bound to the venue under that entity.

7.1.1 Online to the Entity

Enter the entity, click on **[Auth & Accounts]** - **[Copy entity ID]**, and the entity ID will be copied onto the clipboard.



Enter the authentication server to modify the file:

Modify the nac_agent-related configuration in /opt/openwisp2/openwisp2/settings.py

```
NAC_AGENT = {
    'MGMT_INTERFACE': 'Ethernet0',
    'FIRMWARE_VERSION': 'v1.0.0',
    'BUILD_NUMBER': 1002,
    'ENTITY_ID': '3d8bdc44-e96a-4feb-8cf0-328a6a23b976'       # ENTITY_ID The associated organization
id needs to be obtained from the controller
}

WEBSOCKET_SERVER = {
    'HOST': '192.168.0.91',     # HOST Controller ip address
    'PORT': 15008,
    'USE_SSL': True,
    'SSL_VERIFY': False,
    'HEARTBEAT_INTERVAL': 60,
    'WEBSOCKET_CA_CERT': '/opt/openwisp2/nac_agent/certs/ca.crt'
}
```

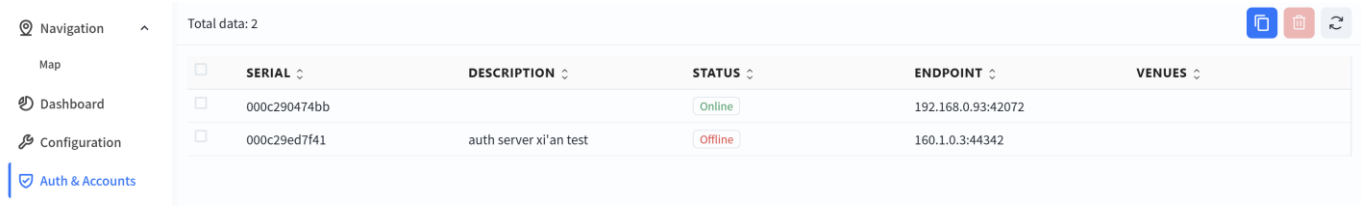
Start the ucentral service

```
systemctl enable openwisp-nac-agent.service
systemctl start openwisp-nac-agent.service
```

Restart the authentication service

```
sudo supervisorctl restart openwisp2
```

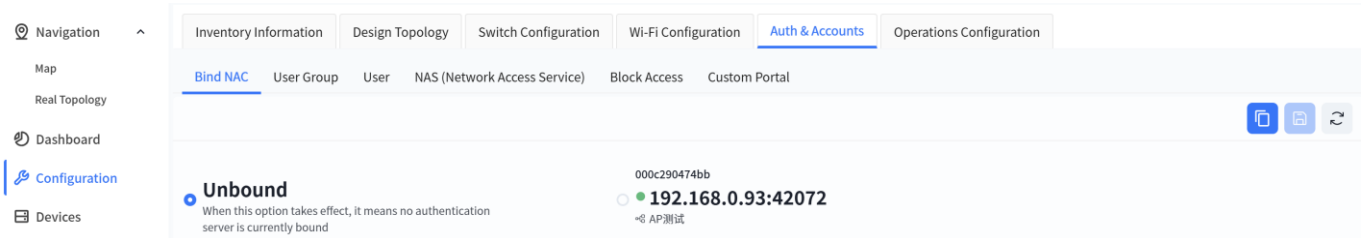
After the configuration is completed, you can see that the authentication server is online in the specified organization.



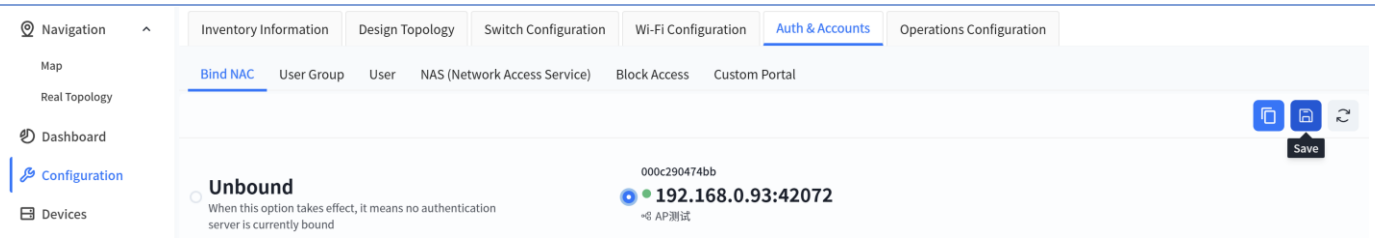
7.1.2 Bind to the Venue

After the authentication server is launched in the entity, all venues within the entity can be bound to this server.

Enter the venue and click on **[Configuration]** - **[Auth & Accounts]**.



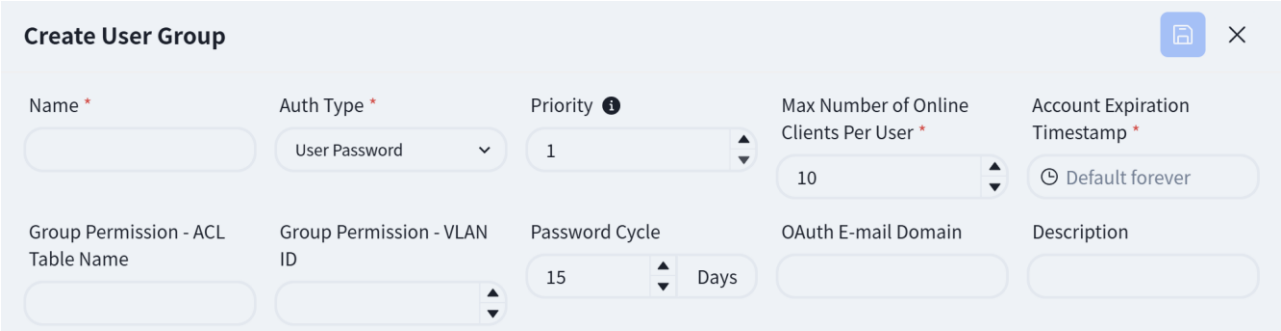
Click on the connected authentication server and click **[Save]** to bind the server to the venue.



7.2 Configuration

The authentication configuration needs to be carried out at the venue.

7.2.1 User Group



Name: The unique identifier of a user group, used for management and identification

Auth Type: The authentication methods that users in this group need to use when logging into the network. Users can choose between username-password authentication and MAC address authentication according to their needs.

Priority: When a user belongs to multiple groups or there are conflicting rules, determine which group's permissions take effect. The larger the number, the higher the priority.

Max Number of Online Clients Per User: Limit the number of devices that each user account in this group can connect to the network simultaneously.

Account Expiration Timestamp: Set the overall validity period for the entire user group, which will automatically expire after the period ends.

Group Permission – ACL Table Name: Bind an Access Control List (ACL). An ACL is a pre-configured set of network access rules (such as allowing/denying access to a certain server or network segment).

Group Permission – VLAN ID: Specify which VLAN the group of users will be assigned to after successful authentication.

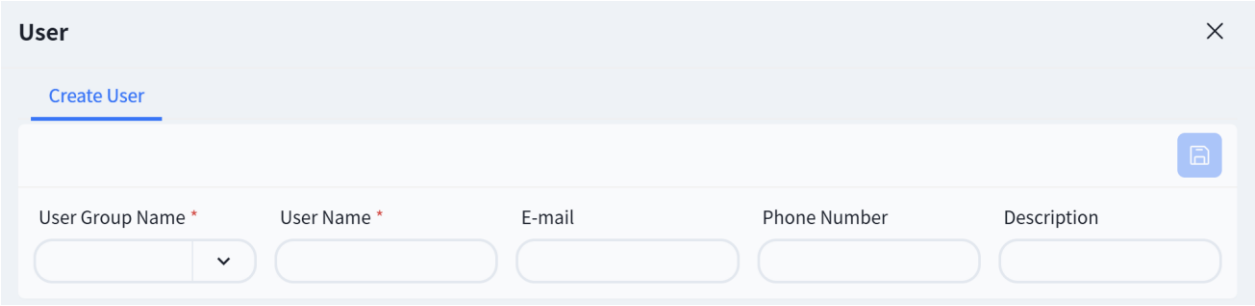
Password Cycle: Set the validity period of the user password. During the password retention period, authentication is automatically completed through device MAC authentication, and the user does not need to re-enter the password. The password needs to be re-entered after expiration.

OAuth E-mail Domain: The email suffix bound to this group during OAuth login, for example: @asterfusion.com

Description: Group description information

Note: The function of Priority and Group Permission -ACL Table Name is not supported in version V9 for the time being.

7.2.2 User



User Group Name: Select the created user group

User Name: The user's unique identifier, used for management and identification

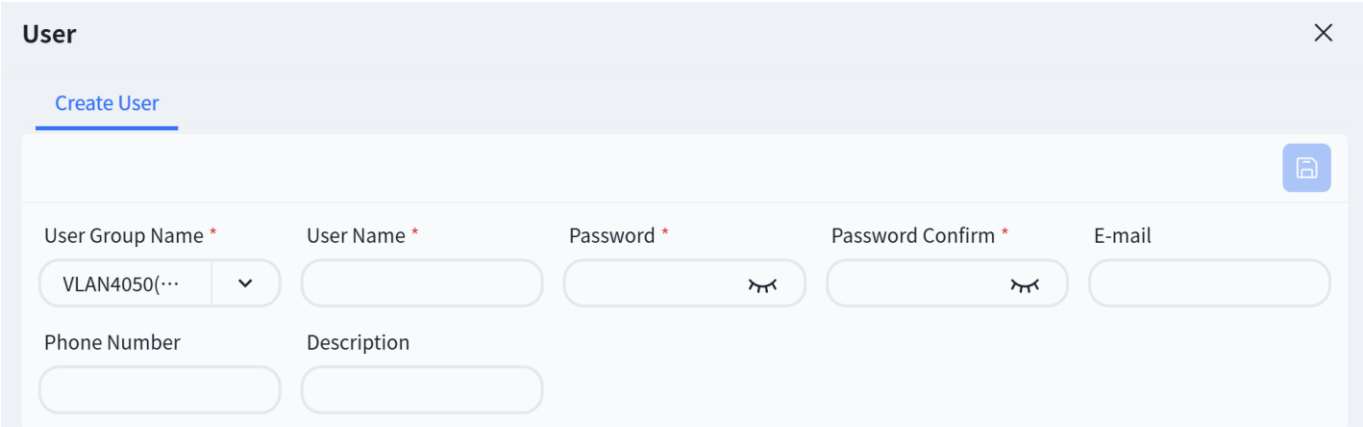
E-mail: User email, currently only serving a presentation function

Phone Number: User's phone number, which currently only serves a display purpose

Description: User description information

7.2.2.1 User Password

When the authentication type of the selected user group is user password, a password needs to be created.

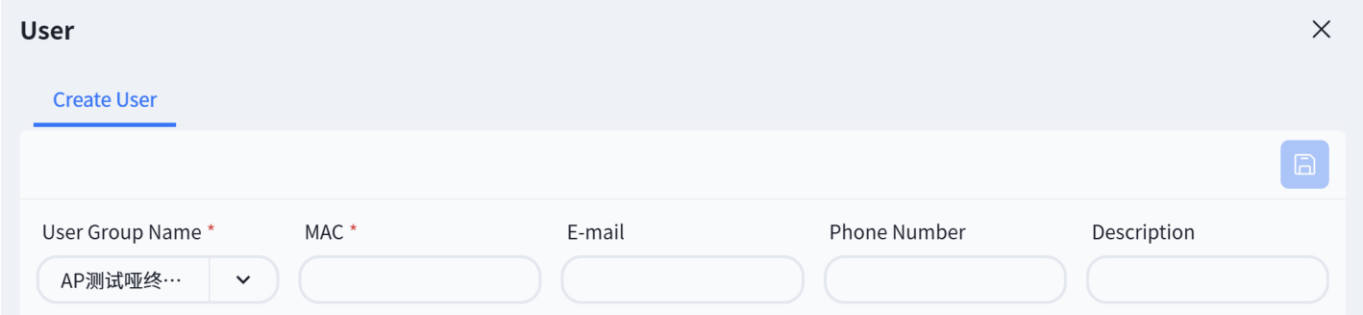


Password: Create it by yourself, and the length must be greater than or equal to 6.

Password Confirm: Must be consistent with the password

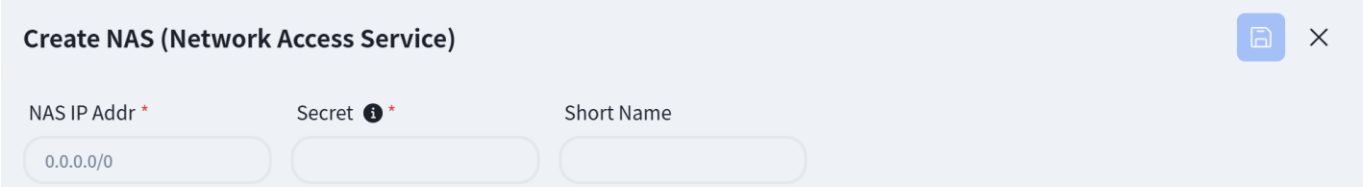
7.2.2.2 MAC

When the user group uses MAC authentication, the MAC address needs to be filled in.



7.2.3 NAS(Network Access Server)

The authentication server will only respond to authentication requests from allowed network segments with matching passwords.

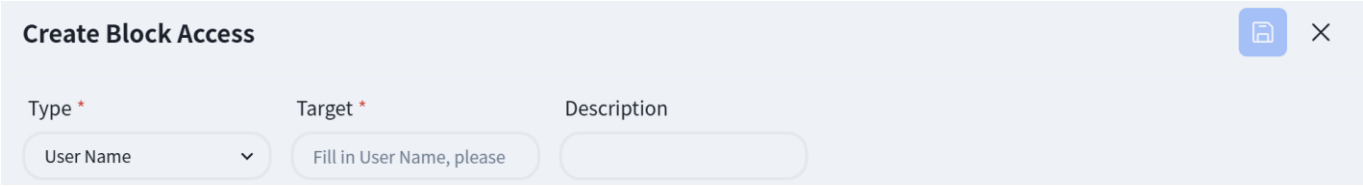


NAS IP Addr: Fill in the address range allowed for access authentication

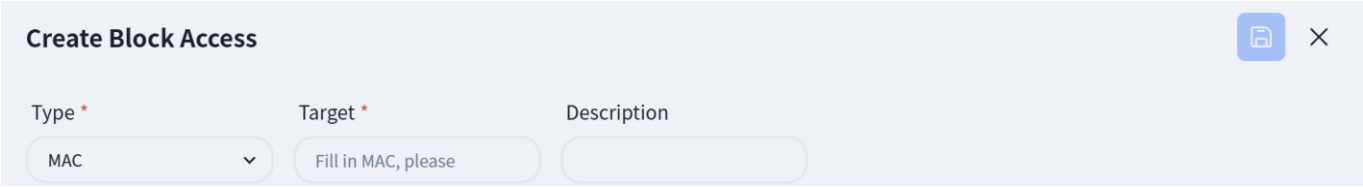
Secret: It needs to be the same as the "Wi-Fi Configuration / Network Activation / SSIDs / RADIUS / Authentication Secret" in this venue

7.2.4 Block Access

7.2.4.1 User Name



7.2.4.2 MAC



8 Status visualization

Controller is equipped with powerful device status monitoring function, which can monitor the working status of switches and wireless APs in real time. Through the detailed dashboard display, administrators can grasp the operating status of the equipment at any time. Based on the acquired monitoring information, the controller evaluates various indicators and intelligently calculates the health value of each device. The health value is evaluated by considering the following factors:

- **Resource utilization:** Based on the memory and CPU utilization, evaluate the use of device resources and whether there is a risk of resource exhaustion.
- **Traffic load:** Based on traffic statistics, analyze the load of the device and determine whether there is a traffic bottleneck.
- **Hardware Status:** Monitor the temperature of each component of the device, the operation of the power supply, fan and other hardware, whether it is within the expected range.
- **Running status:** detect the running status of each major process and container of the device in real time.

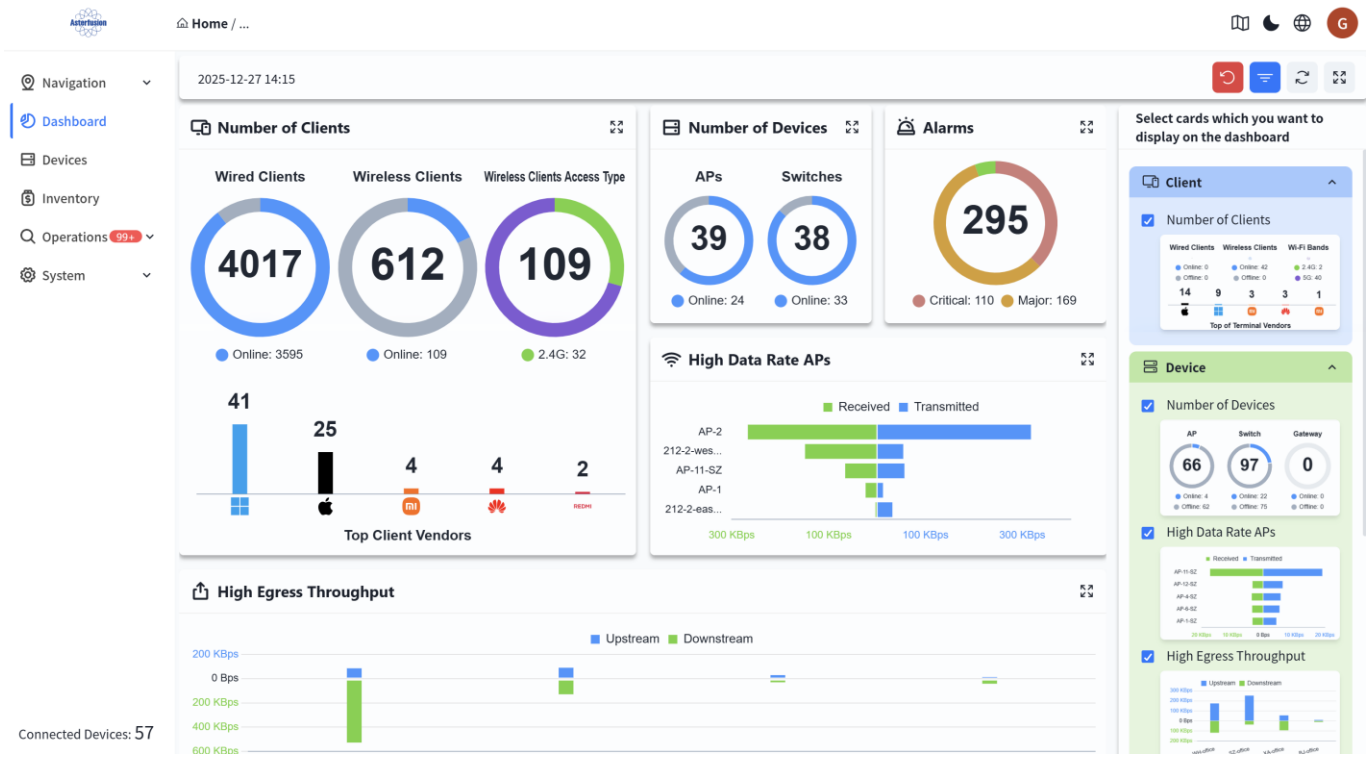
When the monitoring index exceeds the preset threshold, the controller will automatically generate an alarm message to notify the administrator to ensure that the administrator can find and solve the problem in a timely manner to ensure the efficient, safe and stable operation of the network.

8.1 Visual presentation of the whole network status

The controller supports full volume calculation of monitoring data from all online devices, and finally presents them globally as a comprehensive health value.

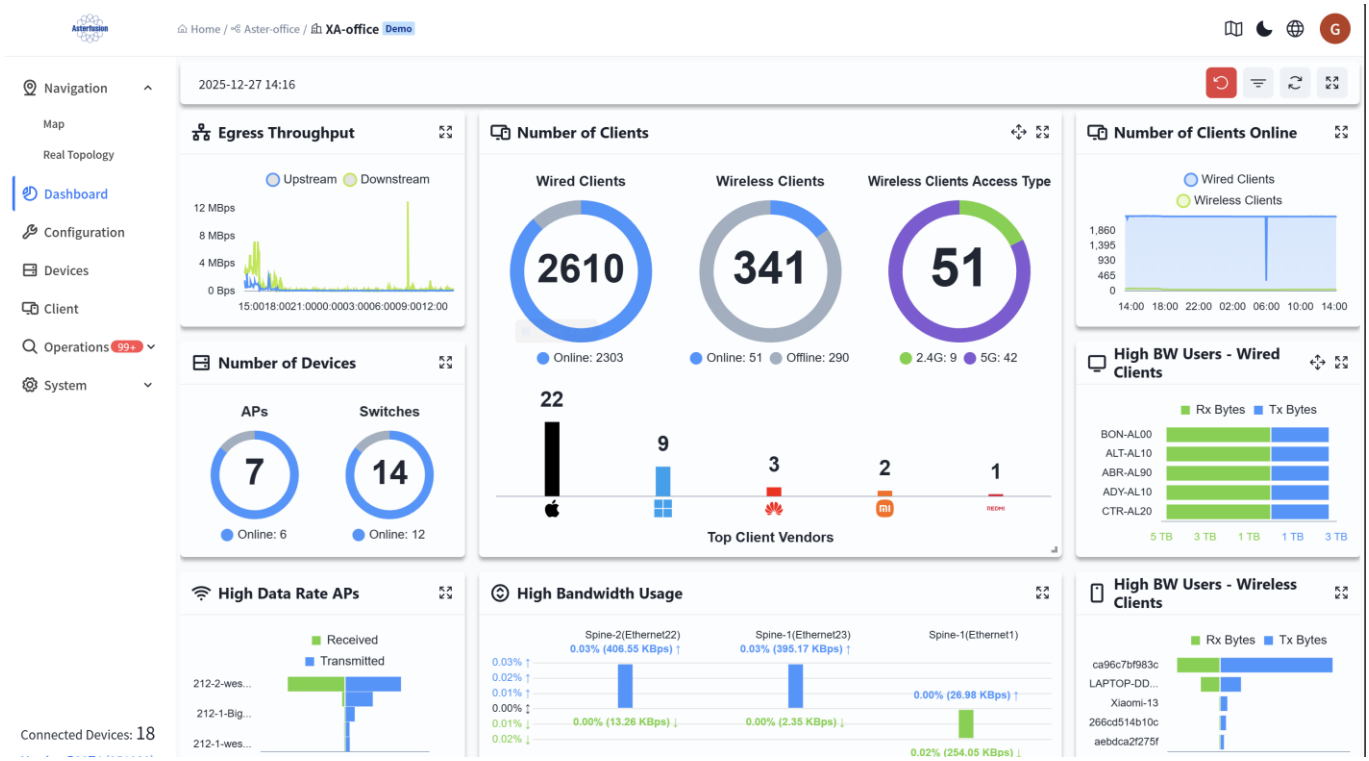
8.1.1 Organization Dashboard

Administrators can enter the specific organization in the **[Navigation]** screen to view an overview of the status of devices and terminals under all premises within the organization. You can also adjust the display cards according to your own preferences.



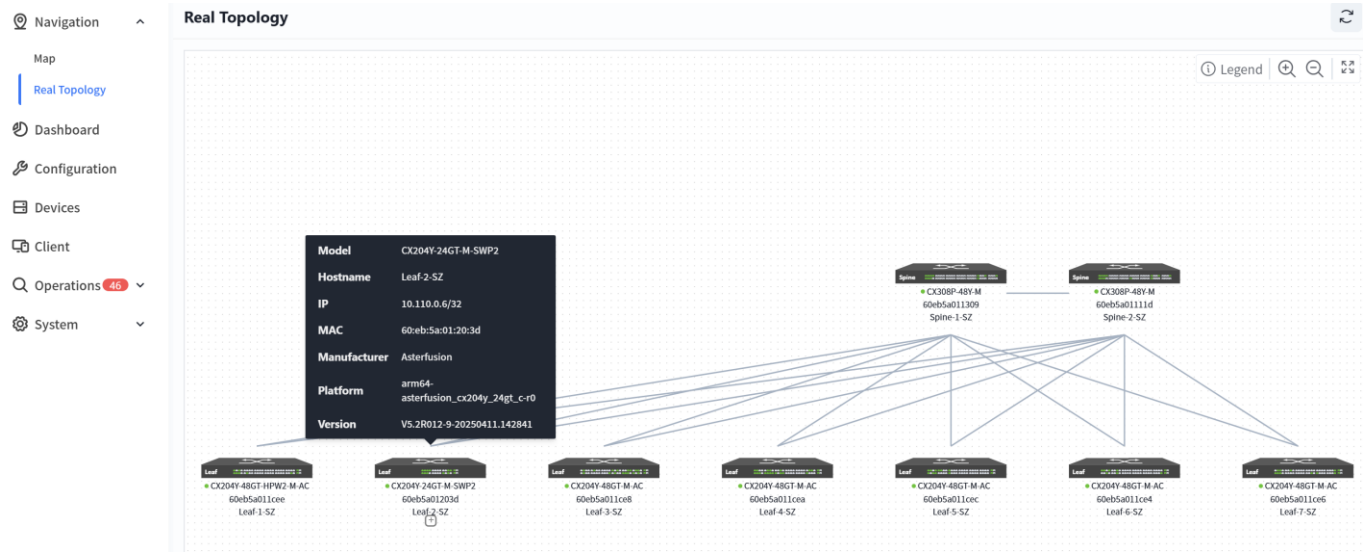
8.1.2 Venue Dashboard

Administrators can enter a specific organization on the **[Navigation]** view to view an overview of the status of devices and terminals under all venues within the organization's scope, and it supports clicking to jump to the selected terminal. Users can adjust the display cards according to their own preferences.

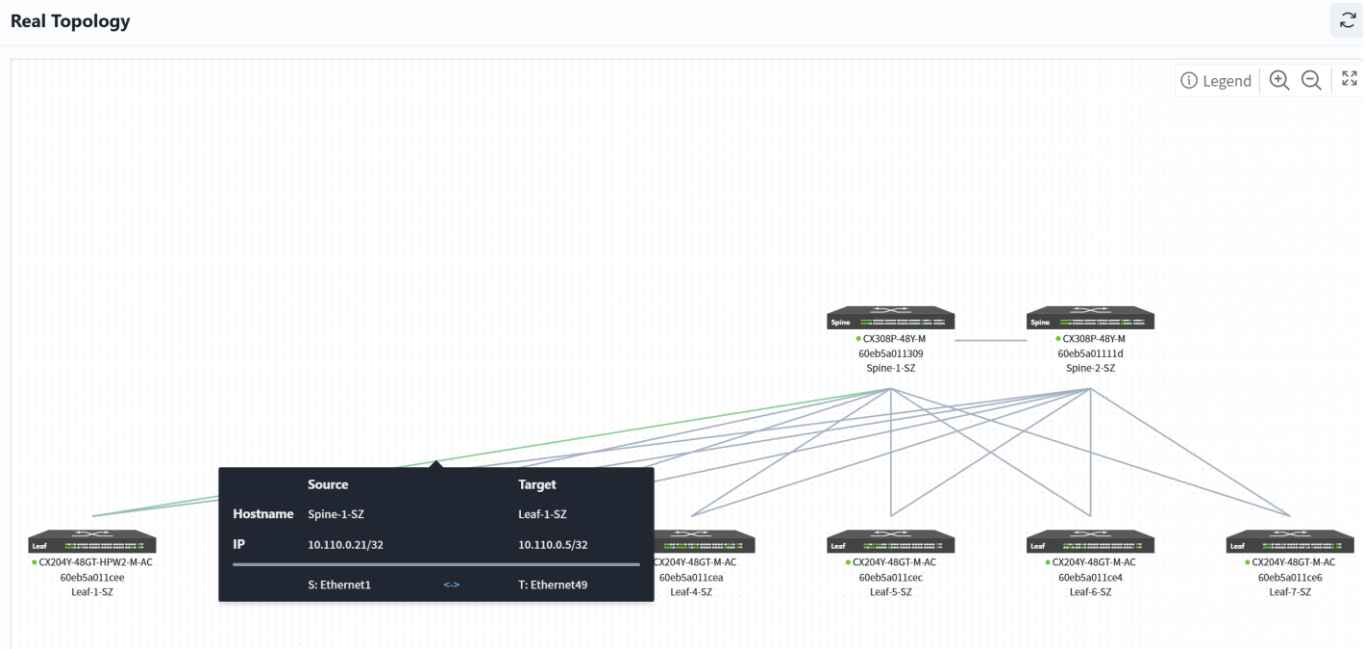


8.1.3 Real Topology

In the venue, users can view device information and connection information on the real topology view. Hover your mouse over the device to view its information, and double-click to enter the device's details interface.

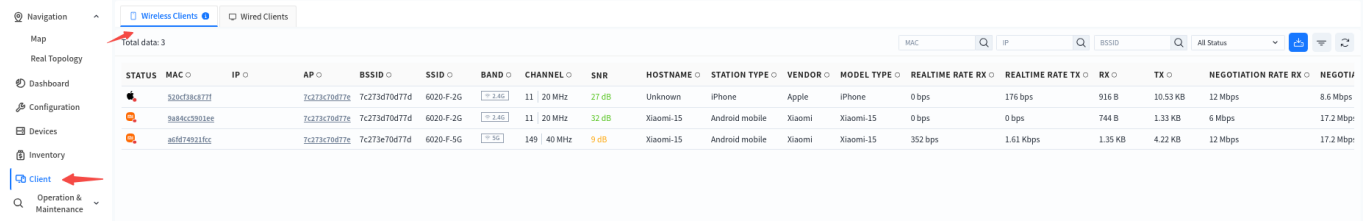


Hover your mouse over the link to view the link information.

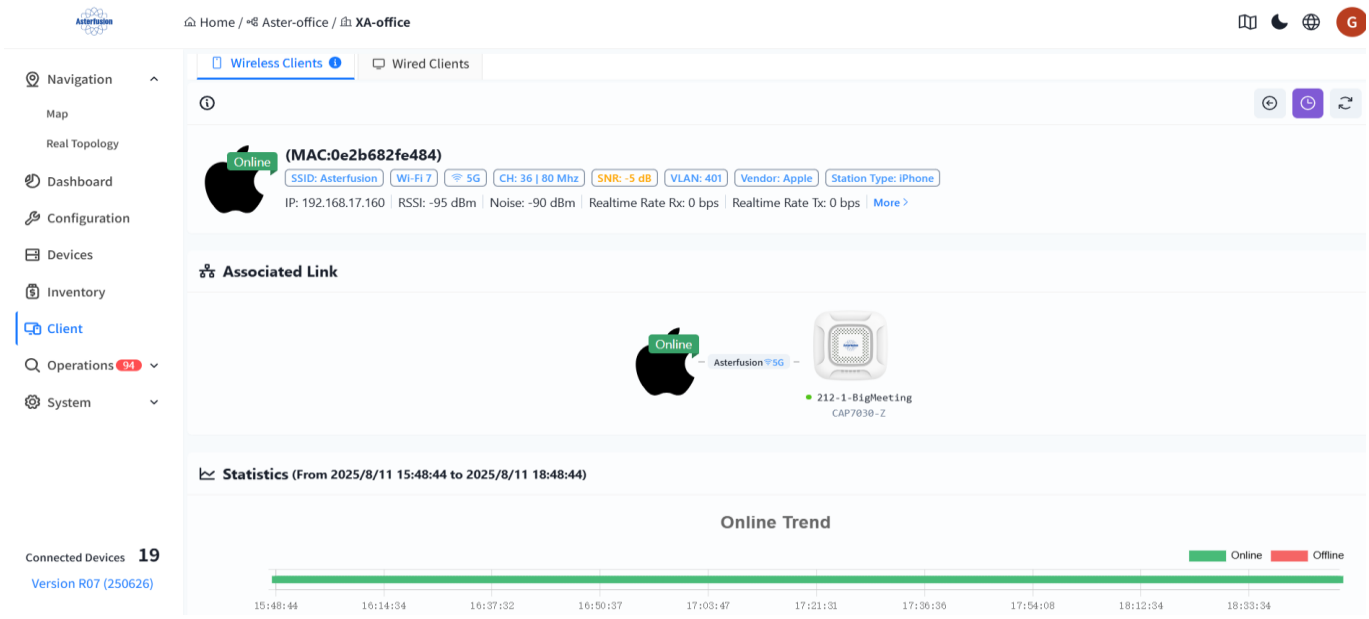


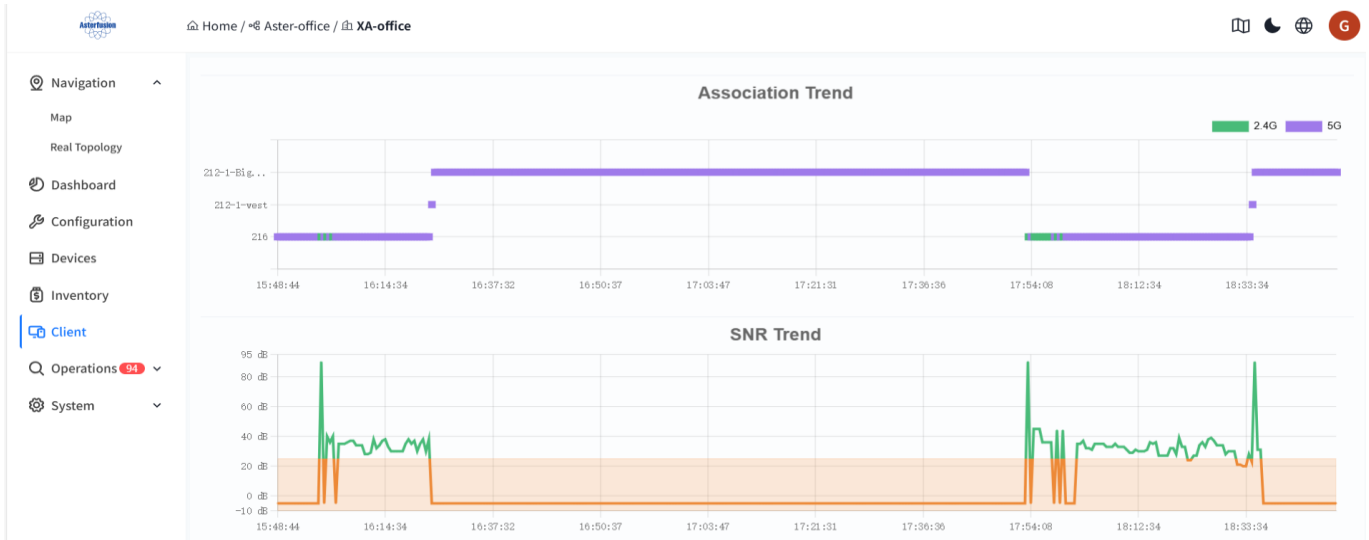
8.2 Terminal Status Visualization

The controller supports collecting data of wired and wireless terminals online and visually presenting the status of online users. After entering a specified organization/venue, administrators can click **[Client]** to view information of all terminals under the organization/venue.



Click on the MAC address of the terminal to enter the detailed view and view detailed data such as the online trend, associated AP trend, SNR trend, and traffic statistics of the terminal. This helps administrators analyze the network connection status of the terminal within a specific time frame.





- **SNR Trend**

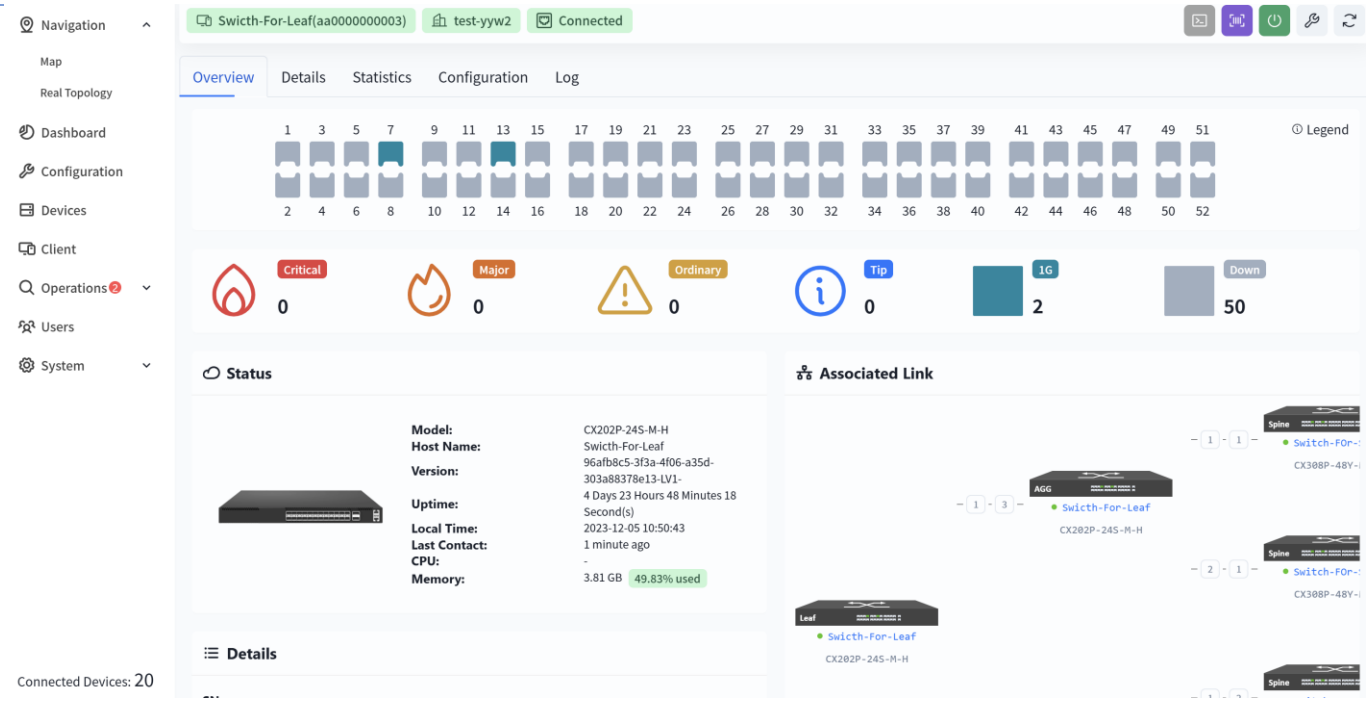
The SNR (Signal-to-Noise Ratio) trend of the terminal is a key dynamic indicator for measuring the quality of the wireless communication link. The baseline value is 25dB. A value lower than this indicates poor signal quality.

- **Traffic Statistics**

Rx represents the amount of data received from the network or other devices, and Tx represents the amount of data sent from the device to the network or other devices.

8.3 Device status visualization

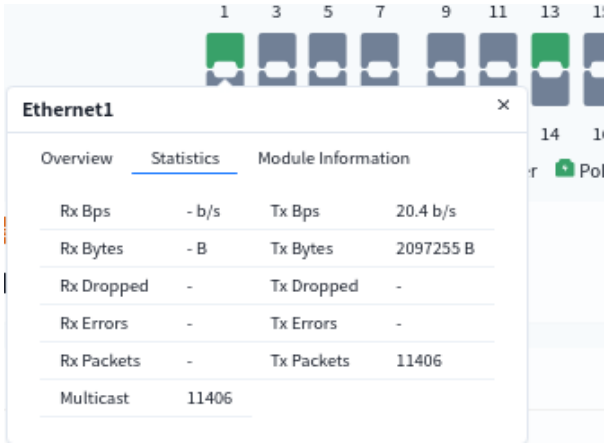
Click **[Device] - [Device MAC]** to enter the management interface of the specified device and view the detailed information of this device:



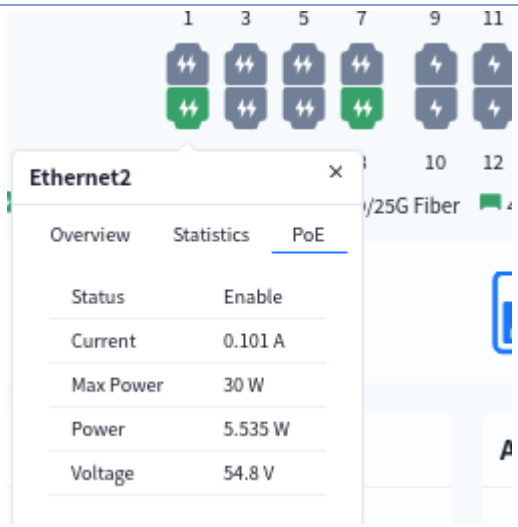
8.3.1 Overview of device information

- View interface information

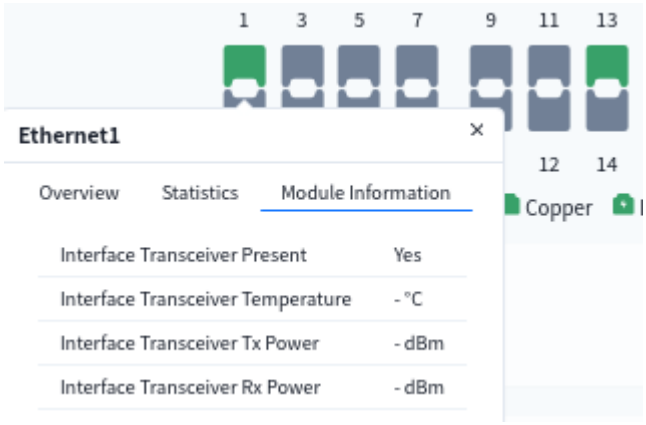
✧ View interface statistics



✧ view interface PoE power supply situation



✧ View interface optical module information



- **Device status:**

Users can view device model, hostname, CPU usage, memory usage, and other information here.

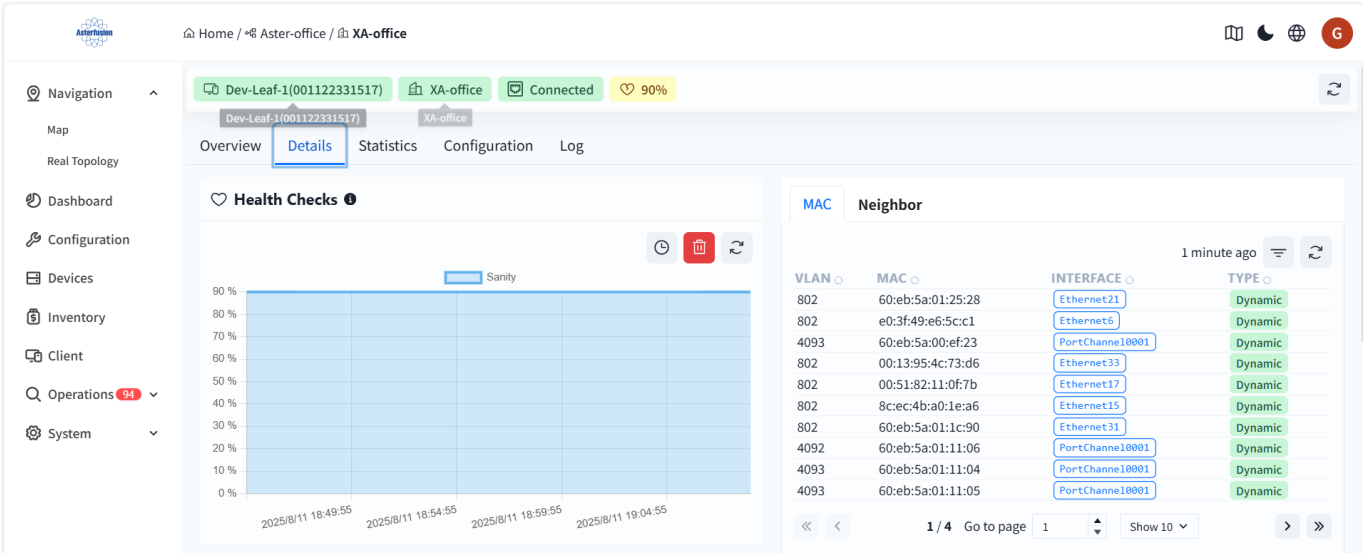
- **Detailed information:**

Including device SN code, MAC address, manufacturer, and other information.

- **Associated link:**

Display the devices associated with this device, click on the name of the associated device to jump to the status visualization interface of a single device.

8.3.2 View device details



- **Health Checks**

The initial health check value for both the switch and the AP is 100%.

✧ Health check calculation specification for the switch:

CPU utilization over 80%, soundness reduced by 10%

Memory utilization over 80%, soundness reduced by 10%

Switch chip/CPU temperature over 85°C, soundness reduced by 10%

PSU any one power supply status abnormality (power module not in position, power supply not powered), soundness minus 10%

Service detection: any critical business service abnormality, soundness minus 10%

✧ AP Health Check Calculation Rule:

interface can successfully detect the DHCP/DNS server information is normal interface, integrity = normal interface / total number of interfaces

- **MAC**

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

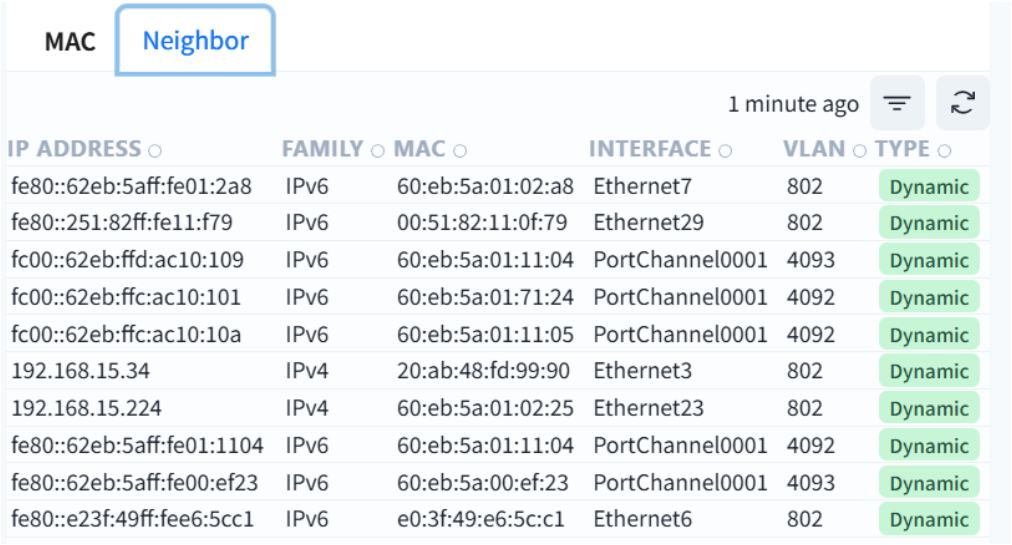
✧ VLAN: The VLAN ID to which the MAC address belongs, used to identify different broadcast domains.

✧ MAC: The learned device MAC address (source MAC address).

✧ Interface: The switch port corresponding to the MAC address (EthernetXX: Physical port, PortChannelXXXX: Link aggregation group).

✧ Type: Item generation method (Dynamic: Automatically learned by monitoring data frames; Static: Manually configured by the administrator)。

- **Neighbor information (ARP)**



IP ADDRESS	FAMILY	MAC	INTERFACE	VLAN	TYPE
fe80::62eb:5aff:fe01:2a8	IPv6	60:eb:5a:01:02:a8	Ethernet7	802	Dynamic
fe80::251:82ff:fe11:f79	IPv6	00:51:82:11:0f:79	Ethernet29	802	Dynamic
fc00::62eb:ffd:ac10:109	IPv6	60:eb:5a:01:11:04	PortChannel0001	4093	Dynamic
fc00::62eb:ffc:ac10:101	IPv6	60:eb:5a:01:71:24	PortChannel0001	4092	Dynamic
fc00::62eb:ffc:ac10:10a	IPv6	60:eb:5a:01:11:05	PortChannel0001	4092	Dynamic
192.168.15.34	IPv4	20:ab:48:fd:99:90	Ethernet3	802	Dynamic
192.168.15.224	IPv4	60:eb:5a:01:02:25	Ethernet23	802	Dynamic
fe80::62eb:5aff:fe01:1104	IPv6	60:eb:5a:01:11:04	PortChannel0001	4092	Dynamic
fe80::62eb:5aff:fe00:ef23	IPv6	60:eb:5a:00:ef:23	PortChannel0001	4093	Dynamic
fe80::e23f:49ff:fee6:5cc1	IPv6	e0:3f:49:e6:5c:c1	Ethernet6	802	Dynamic

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.

✧ IP address: IP address (IPv4/IPv6) of the neighbor device

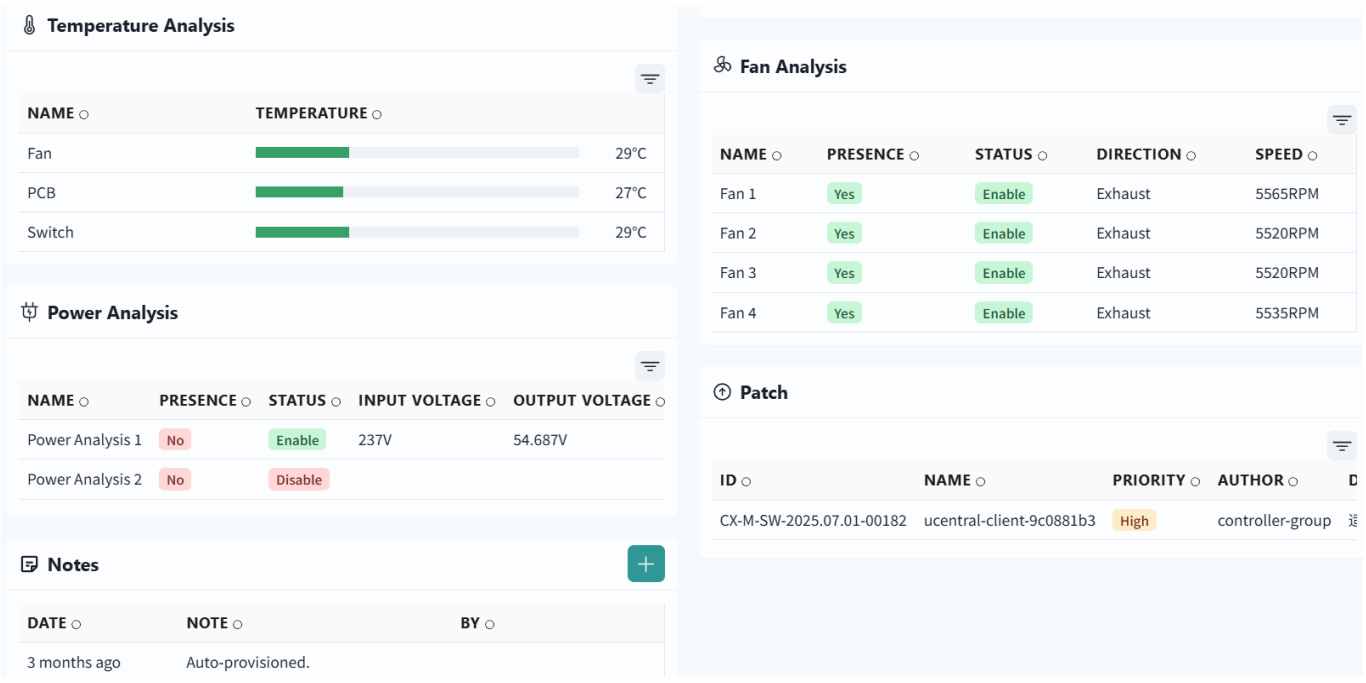
✧ Family: IPv4 or IPv6 protocol type

✧ MAC: The physical address of the neighbor device

✧ Interface: The port of the local switch connected to this neighbor

✧ VLAN: The virtual local area network where the communication takes place

✧ Type: Dynamic (automatic protocol learning) or Static (manual configuration)



- **Temperature Analysis**

Display the temperature information of each component of the display device

- **Fan Analysis**

Display detailed information of each fan module of the display device

- **Power Analysis**

Display device power information

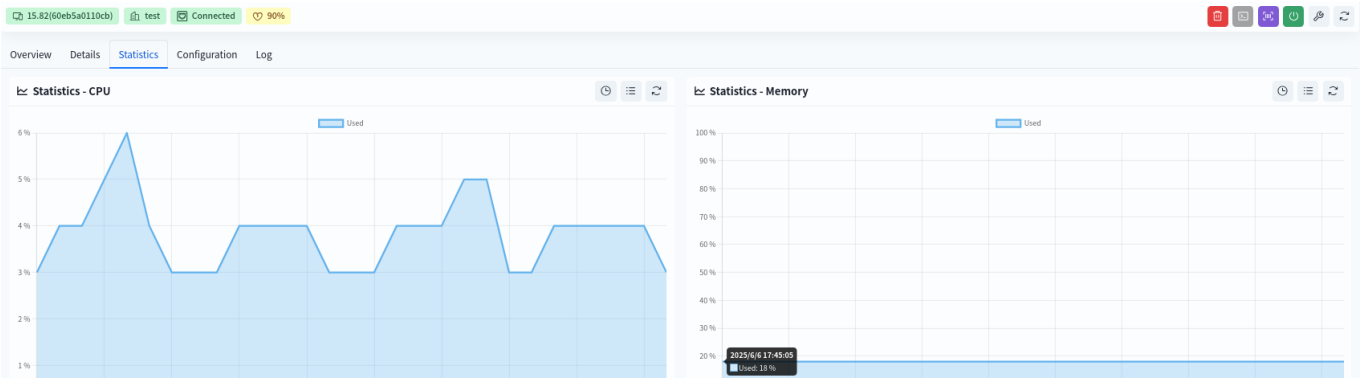
- **Patches**

List of patches already installed on the device

- **Notes**

Remarks information added by the user

8.3.3 View device statistics

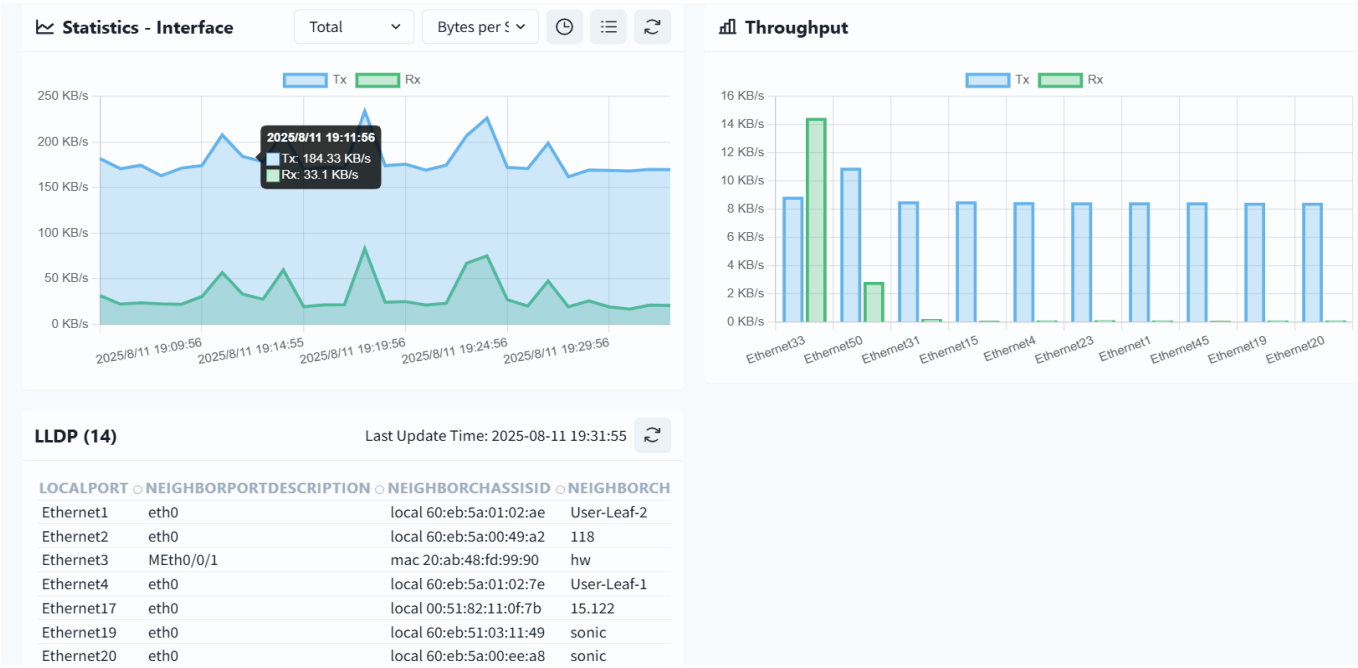


- **CPU Statistics**

  Historical CPU statistics over a three-day period.

- **Memory Statistics**

  Historical memory statistics over a three-day period.



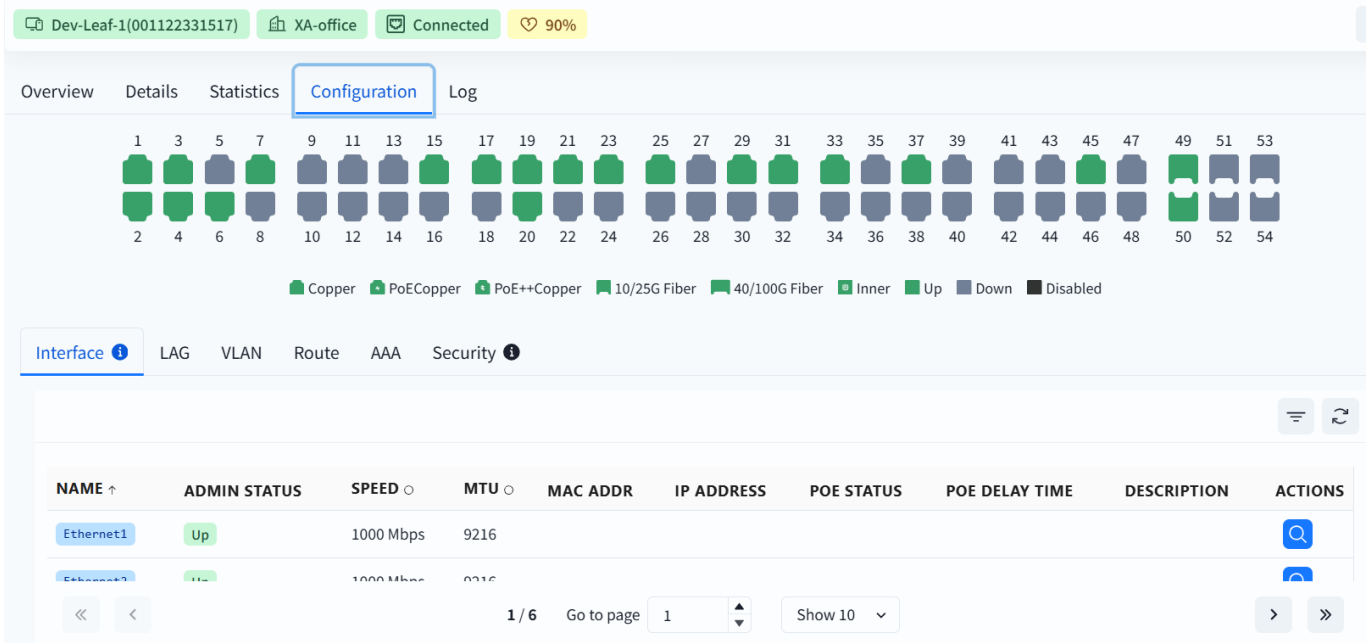
- **Statistics - Interface**

  Statistics of single interface/whole machine interface support two statistical methods: byte rate (bytes per second) and the number of data packets (increment from the previous counting moment).

- **LLDP**

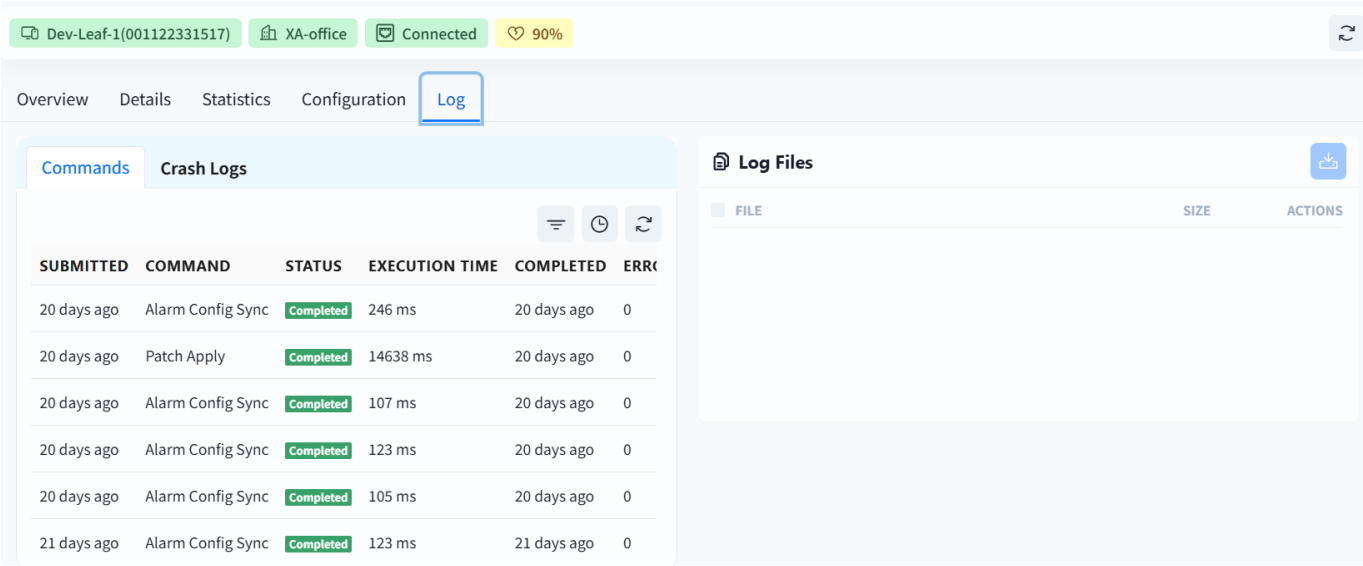
  Display LLDP information on the switch.

8.3.4 View device configuration information



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

8.3.5 View device log information



9 Operation and alarm management

Firmware management is an important feature of the controller for managing version image files and patch files for network devices. Users can upload local images to the controller for easy deployment of new software versions throughout the network, or update network devices directly with the uploaded firmware.

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

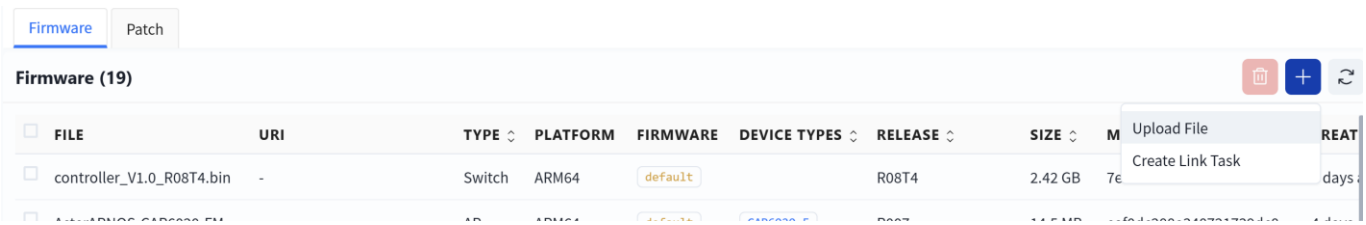
9.1 Firmware Management

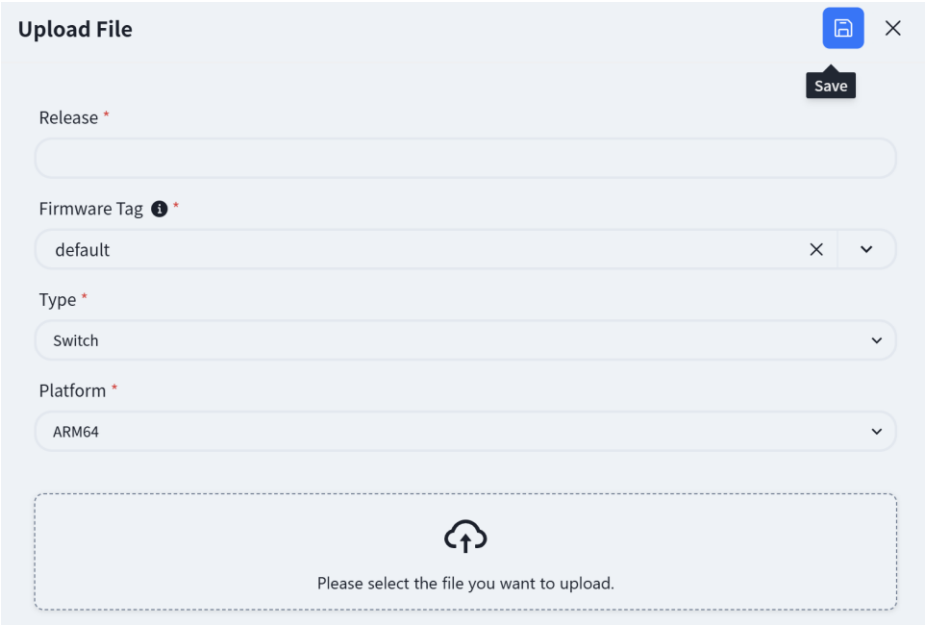
9.1.1 Firmware Upload

The administrator can upload the version image to the controller and record the basic information of the software version.

Go to **[Operation] - [Firmware] - [Firmware]**. Click **[+]** to upload the version image to the controller.

9.1.1.1 Upload Fail





Release: Version Identifier

Firmware Tag: Used to match firmware with the same label during installation.

Type: To distinguish whether the firmware applies to the switch, AP or the OLT Stick.

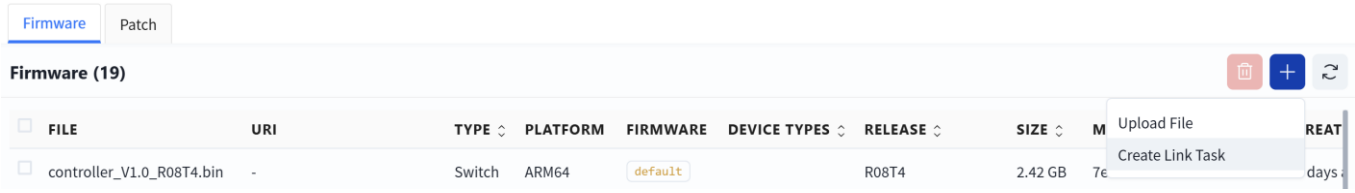
Platform: To specify different hardware models.

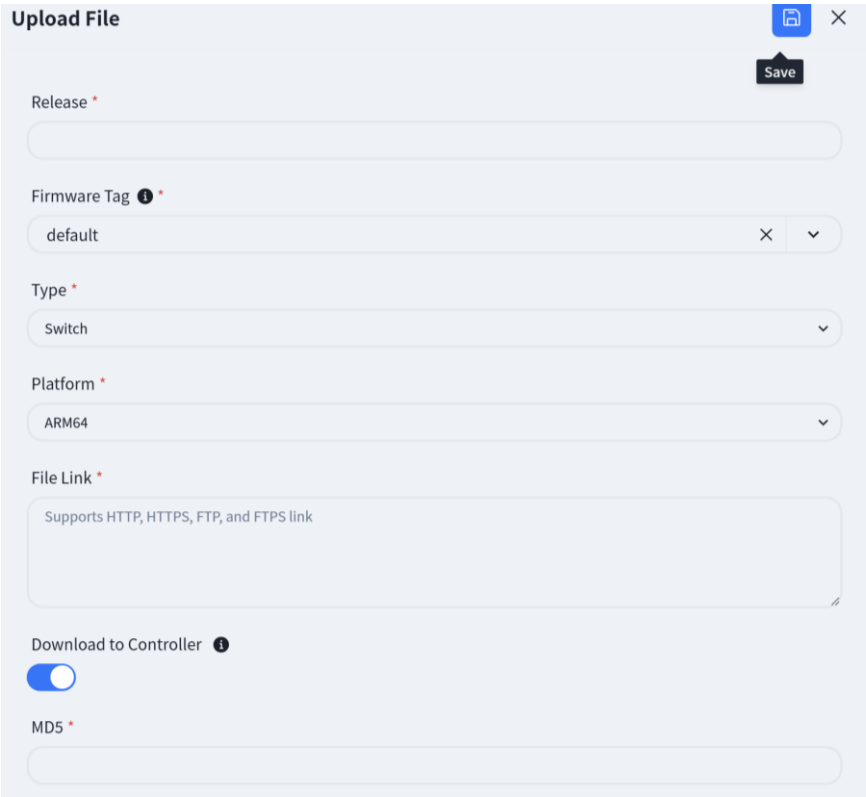
a) ARM64: CX102 series, CX202 series, CX204 series and CX206 series.

b) X86: CX308 series, CX532 series

9.1.1.2 Create Link Task

The controller supports firmware upgrade via creating a connection task. In this way, the user does not need to download the firmware to the local device; instead, they can directly input the file link address on the controller, and the controller will automatically retrieve the file.





File Link: Direct download link for the file

Download to Controller:

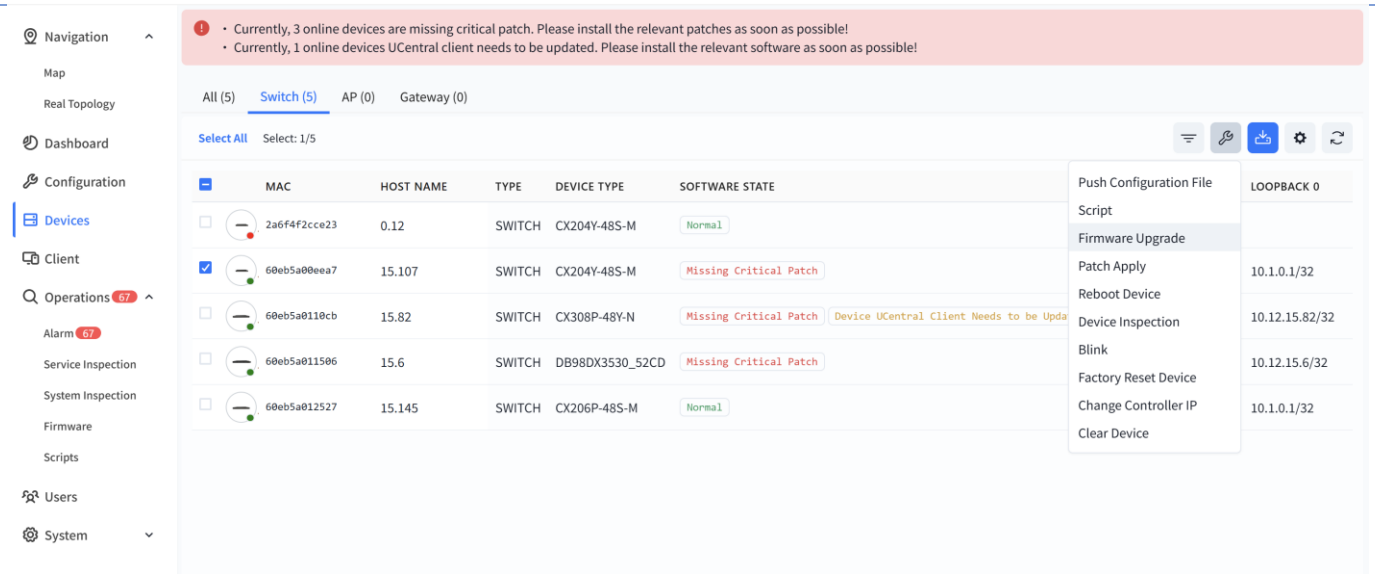
Enable: The controller downloads and saves the firmware first, then devices retrieve it from the controller.

Disable: Devices download the firmware directly from the remote URL.

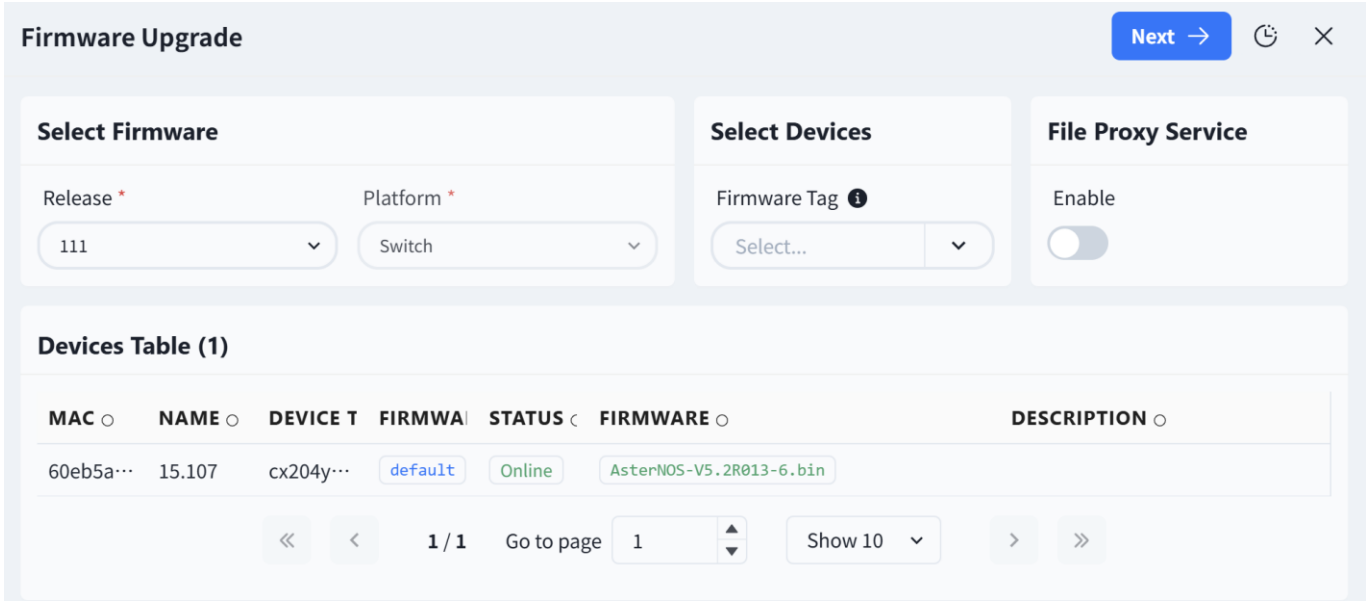
MD5: This is a standard technical phrase. I've provided a direct translation that maintains the original meaning and technical accuracy.

9.1.2 Firmware Use

1. On the **[Device]** interface, select the corresponding device type, choose the device that needs to be upgraded, click the **[Operation]** button in the upper right corner, and select **[Firmware Upgrade]**.



2. In the pop-up window, click on **[Release]** to select the firmware image file that needs to be upgraded, and click **[Next]** to upgrade the firmware



Note: The switch will not reboot automatically after the upgrade is completed, you need to manually perform the reboot operation to make the upgrade take effect.

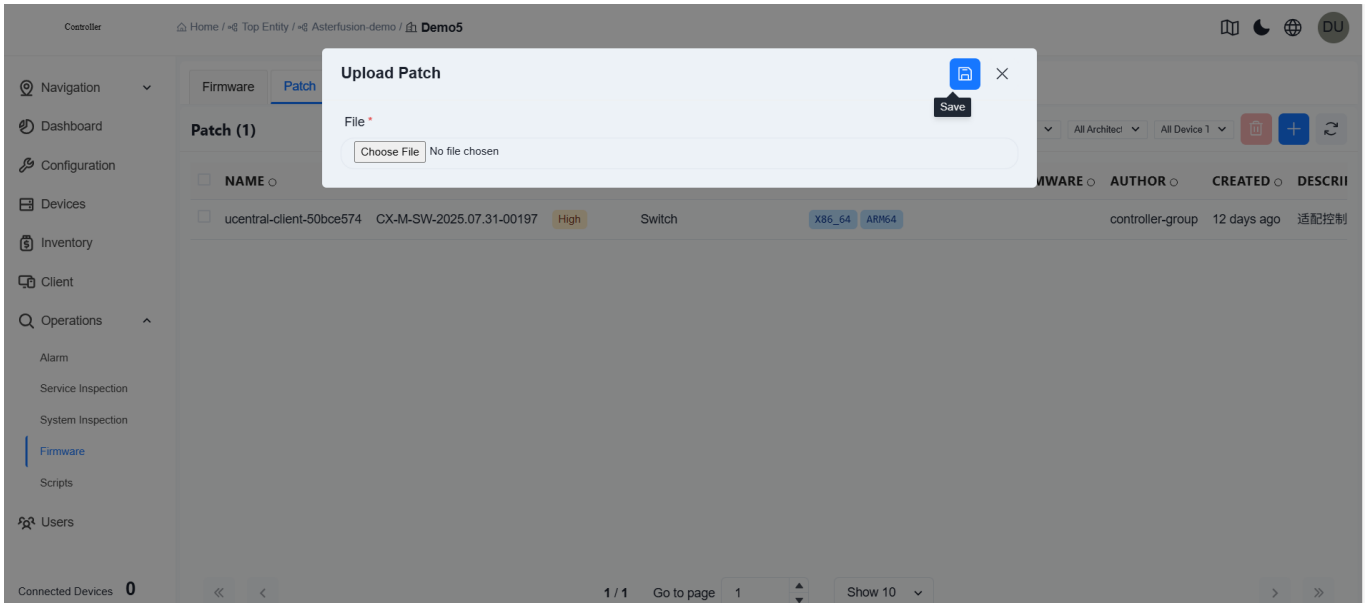
9.2 Patch Management

9.2.1 Patch Upload

Patch management allows administrators to upload patch files to the controller, The controller automatically parses the patch content to ensure that patches are applied to the correct device platforms, thereby enhancing network security and device stability.

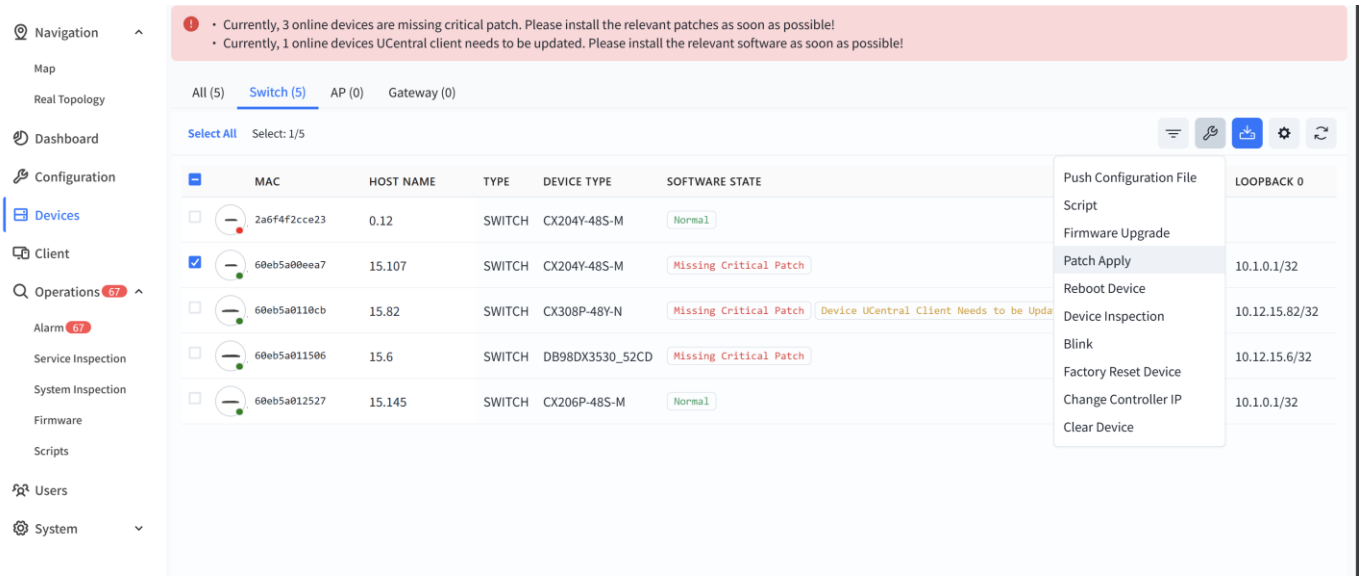
Key Functions:

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

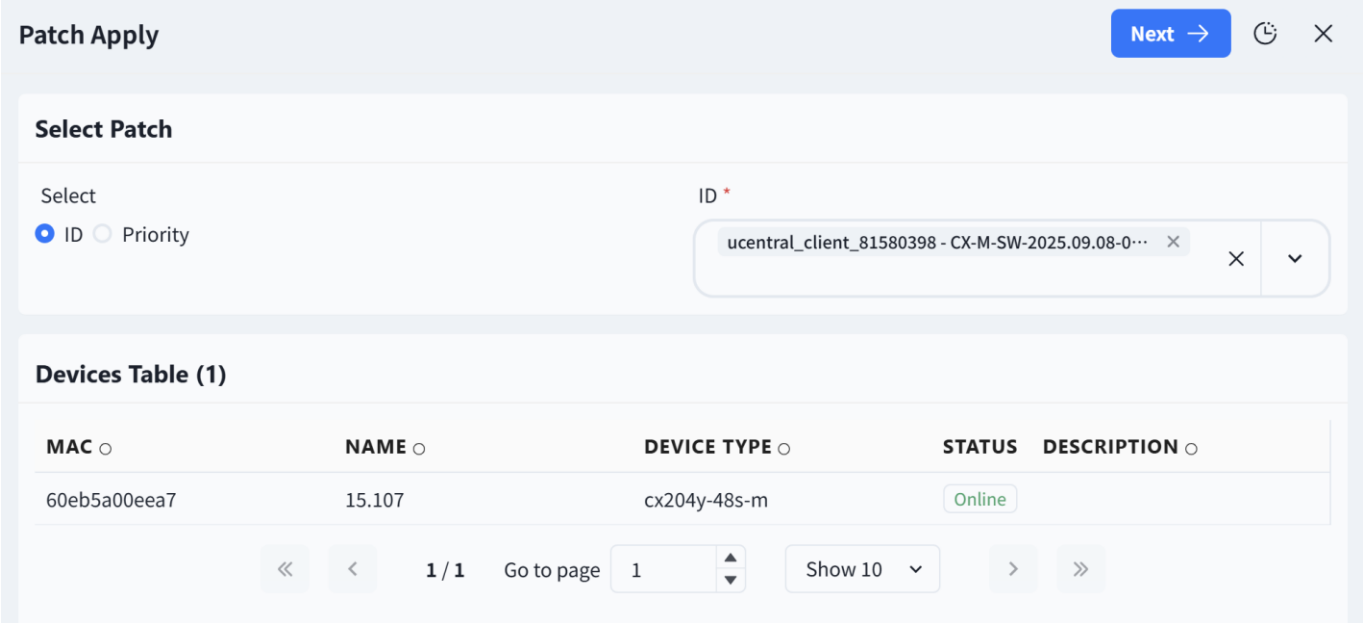


9.2.2 Patch Apply

On the **[Device]** interface, select the corresponding device type, choose the device that needs to be upgraded, click the **[Operation]** button in the upper right corner, and select **[Patch Apply]**.



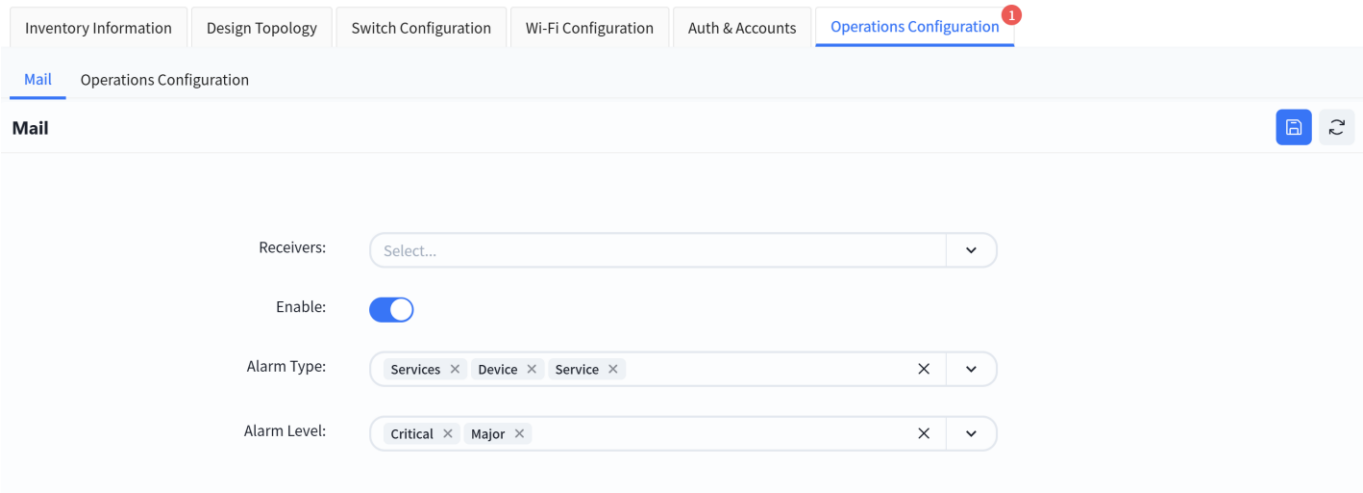
Filter the required patches and devices on the pop-up view, and click **[Next]** to apply the patches.



9.3 Alarm Management

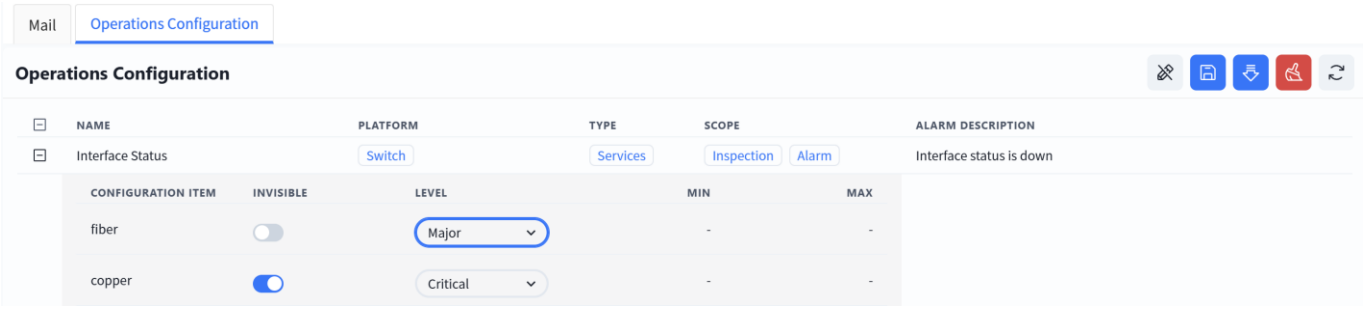
9.3.1 Mail

The administrator can configure the alerts and thresholds that need attention and set recipients in the operation and maintenance configuration interface within the Entity/Venue.



9.3.2 Operations Configuration and Sync

The administrator can modify the alert information as needed in the operation and maintenance configuration by clicking the **[Edit]** button in the upper right corner.

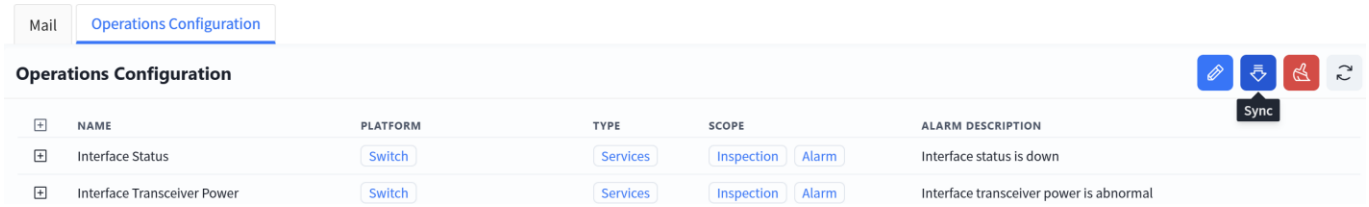


The controller supports the following alarms. By default, all alarms supported by the controller are enabled.

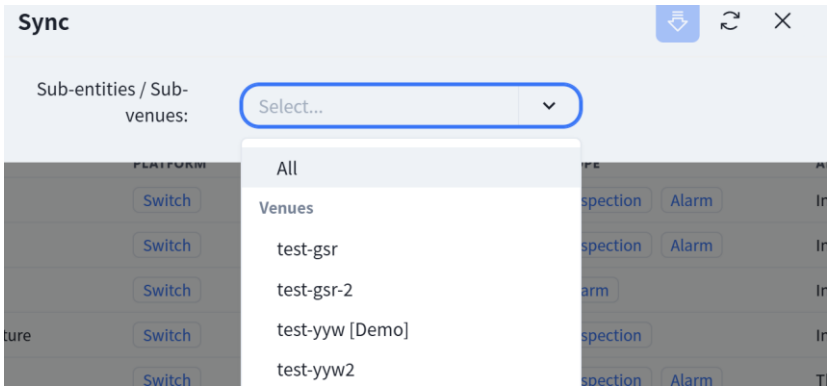
Alarm Type	Alarm Item
Interface Status	Interface UP/Down status change
Wireless Terminal Type	Change in the vendor type corresponding to the MAC address
Interface Module Optical Power	Optical power of the optical module
Interface Module Status	Presence status of the interface module
Bandwidth Utilization	Bandwidth utilization rate
User Table Entries	ARP entry resource utilization
	IPv4-host-route: /32 host route entry resource utilization
	IPv4-route: Route entry resource utilization
	IPv6-host-route: /128 IPv6 host route entry resource utilization
	IPv6-route: IPv6 route entry resource utilization
	MAC entry resource utilization
	Route-nexthop: Next-hop resource utilization of route entries
RADIUS Sever Status	Detected operating status of the RADIUS server
PortalSever Status	Detected operating status of the Portal server
MC-LAGStatus	Operational status of the MC-LAG protocol
IP Flapping	Unusually frequent flapping of IP addresses across different switches
MAC Flapping	Unusually frequent flapping of MAC addresses on different interfaces of the same switch
Interface POE Status	Change in the POE status of the interface
POE Total Power Utilization	Percentage of current total 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 Rate	-

Memory Utilization Rate	-
Disk Utilization Rate	-
temperature	CPU core temperature
	FAN temperature
	PCB PCB temperature
	SWITCH switch chip temperature
Fan	Presence status of the fan module
	Fan speed
Psu	Presence status of the power supply module
	Power supply status
Core Dump File Status	Resource utilization rate of core dump files
Docker Status	Docker status on 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

System/organization administrators can directly sync the operation and maintenance configuration to sub-organizations/sub-locations by clicking the **[Sync]** button in the upper right corner.



Select the sub-entities/sub-venues to be synced.



9.3.3 Mail Sender

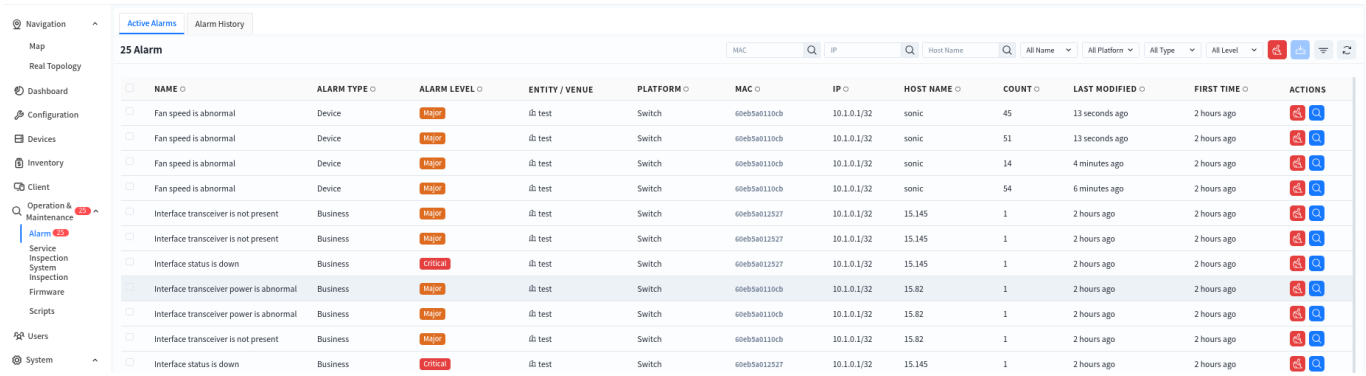
Click **[System] - [Mail Sender]** to modify the source mailbox for sending alerts。

Click **[Connectivity]** to test the connectivity between the controller and the email server, preventing alarm emails from failing to be sent normally due to network connectivity issues.

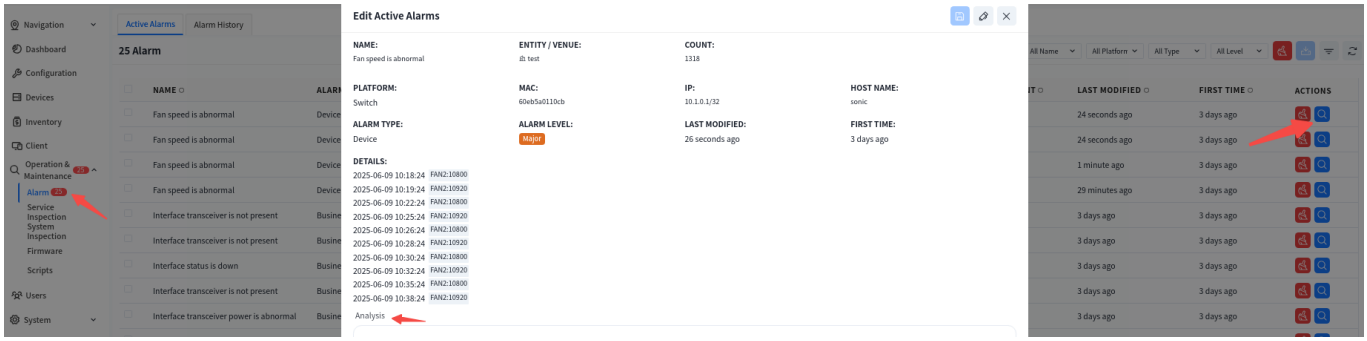
9.3.4 Alarm Message

Administrators can view alarm information for all devices within their management authority in the **[Operations] - [Alarm]** view.

- **Active Alarms:** Displays alarm items that still exist currently.
- **Alarms History:** Displays alarm items that showed abnormalities before but have returned to normal.



Click the alarm item to view specific alarm information and process it. Click the **[Edit]** button, fill in the processing information for the current alarm in the **[Analysis]** section, and click the **[Save]** button to complete the edit. After that, this alarm information will no longer be displayed in **[Active Alarms]** but will be stored as a processed alarm in **[Alarm History]**.



9.4 Device Inspection

The device inspection feature is designed to regularly check and monitor network devices to ensure their normal operation and detect potential faults in a timely manner. Its main functions include:

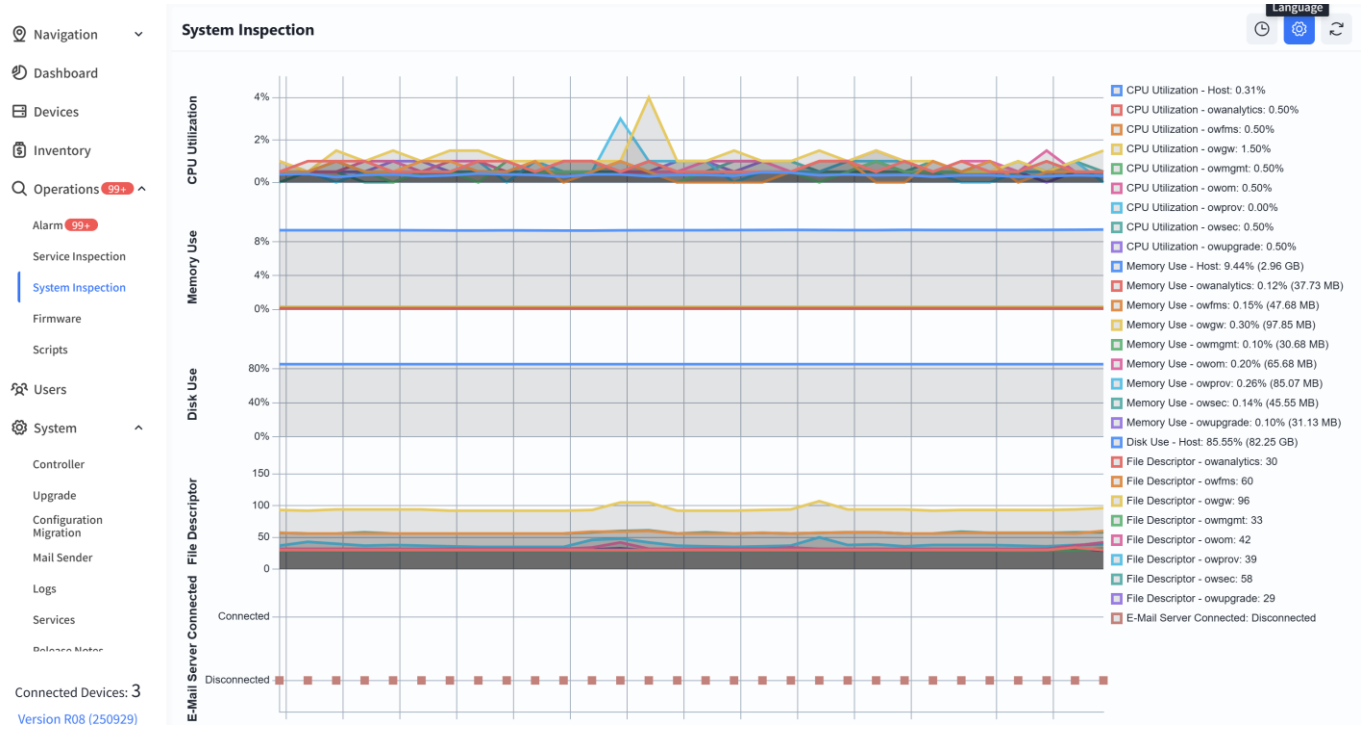
- Device Status Monitoring: Checks critical parameters such as CPU usage, memory usage, storage, and port status to ensure devices are functioning properly.
- Log and Alarm Management: Collects device logs, analyzes abnormal events, and triggers alarm mechanisms.
- Critical Process Status Check: Monitors the status of essential processes to ensure smooth business operations.
- Automated Inspection Tasks: Supports scheduled inspection tasks, generates inspection reports, and facilitates network maintenance.

9.4.1 System Inspection

System inspection refers to the periodic check of the controller's internal system to ensure stable and efficient operation. Key inspection items include:

- **CPU & Memory Usage:** Monitors CPU load and memory consumption to prevent system failures due to resource exhaustion.
- **Disk Usage Check:** Examines disk usage to prevent logs or cached data from consuming all available storage, which could impact system performance.
- **Files Descriptor:** Verifies the proper functioning of critical services (e.g., network management, authentication, logging) and automatically restarts abnormal processes.
- **E-Mail Server Connected:** Tests the controller's connectivity with the email server to ensure alert notifications are successfully sent.

System inspections can be scheduled at fixed intervals (e.g., every 5 minutes or every hour) and automatically generate inspection reports for administrators to analyze and optimize system performance.

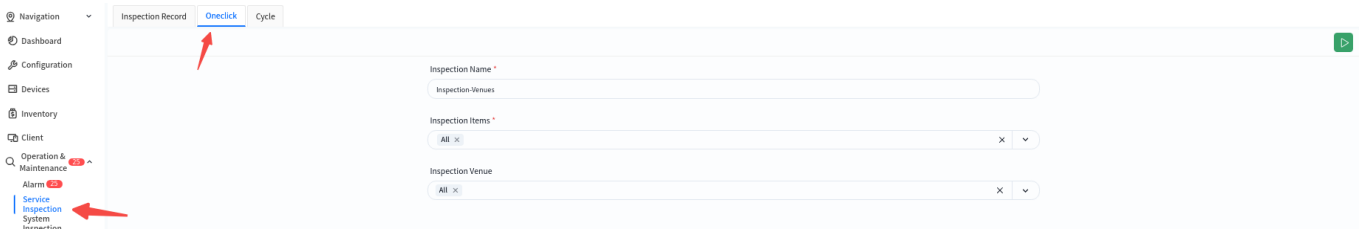


9.4.2 Business Inspection

Business inspection refers to periodic or on-demand checks of network device operation to ensure stable business operations and prevent potential failures.

9.4.2.1 One-Click Inspection

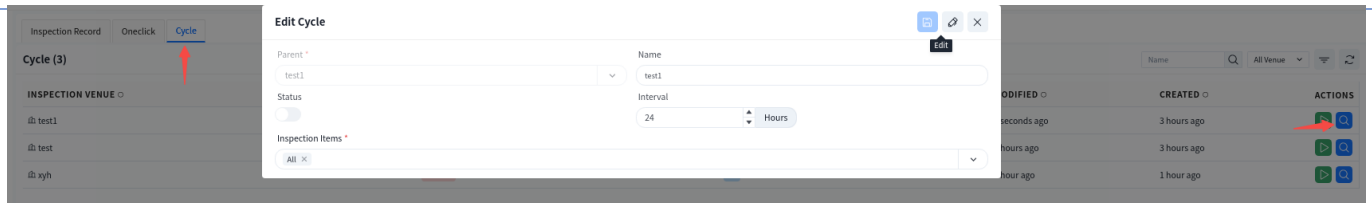
This feature allows users to specify inspection items and target venues for an instant inspection, defining the scope of the inspection accordingly.



9.4.2.2 Cycle Inspection

Cycle inspection is configured based on the needs of different venues, allowing for automated inspections at scheduled intervals without manual intervention, thus improving operational efficiency.

Click the **[View Details]** button to view/edit the periodic inspection settings for the selected venue.



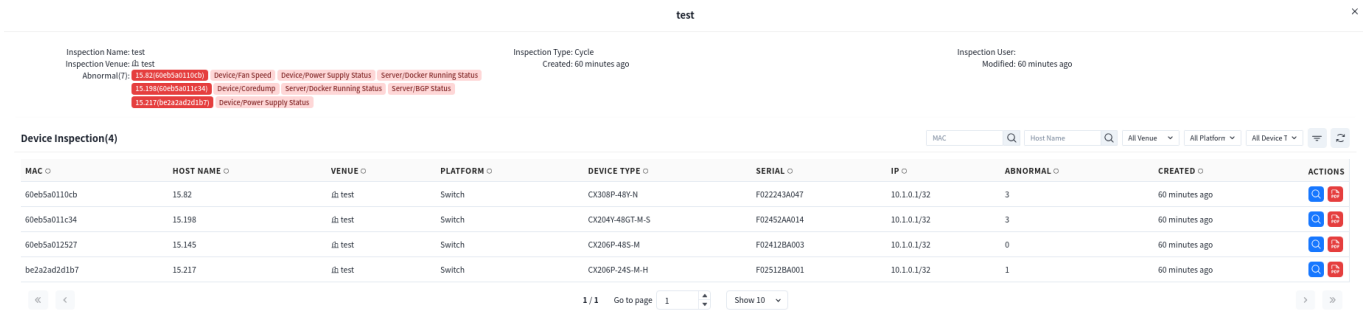
9.4.2.3 Inspection Records

Both one-click inspections and periodic inspections are logged in the inspection records.

Click the **[View Details]** button to check the inspection results. All detected anomalies will be listed under the **[Abnormal]** section. Administrators can:

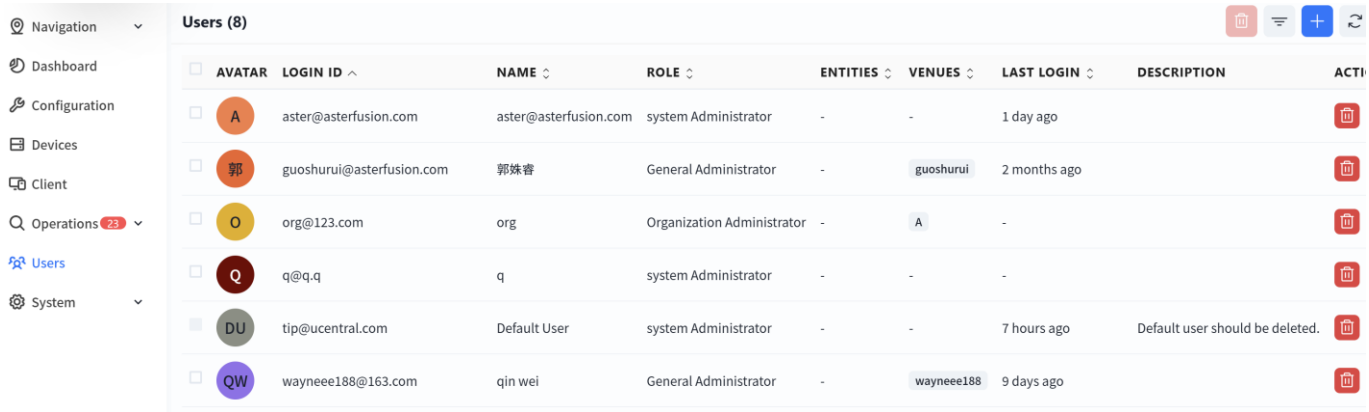
Click **[Actions] - [View Details]** to check the inspection results of a specific device.

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



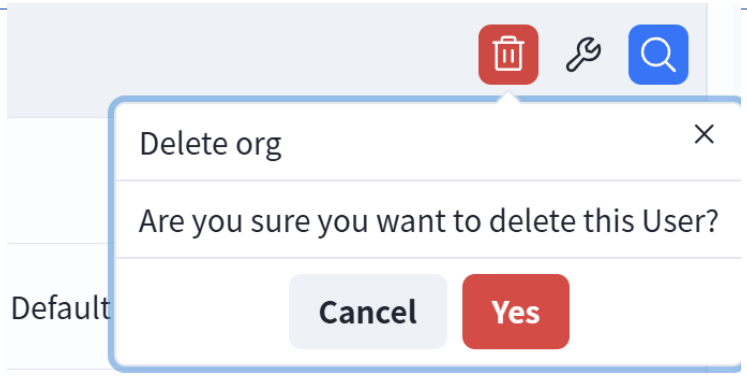
10 Users

Administrators can operate users and adjust user permissions as needed on the **[User]** view.



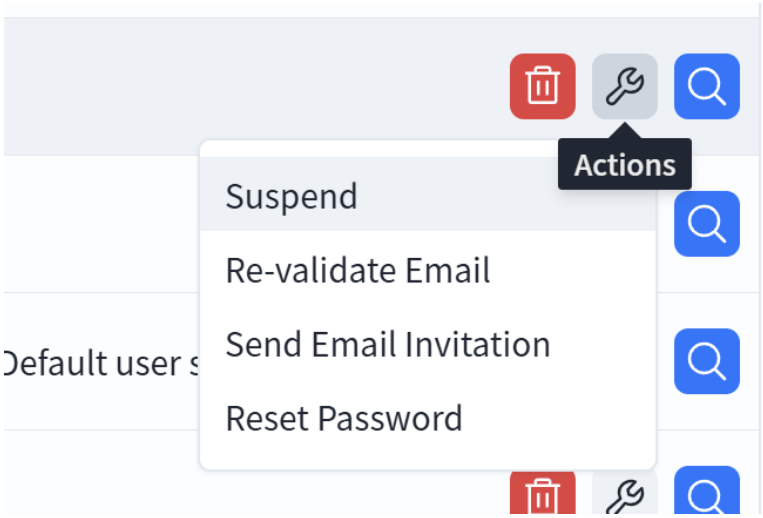
10.1 Delete

Click the **[Delete]** button on the right side of the user to delete the user. The current login of the deleted user will be forced to log out, and it will be restored after logging in again.



10.2 Actions

Click the **[Actions]** button on the right side of the user and select the corresponding operation.



Suspend: Temporarily deny the user login to the controller. If you need to lift the restriction, you can choose to reactivate the user in the same path.

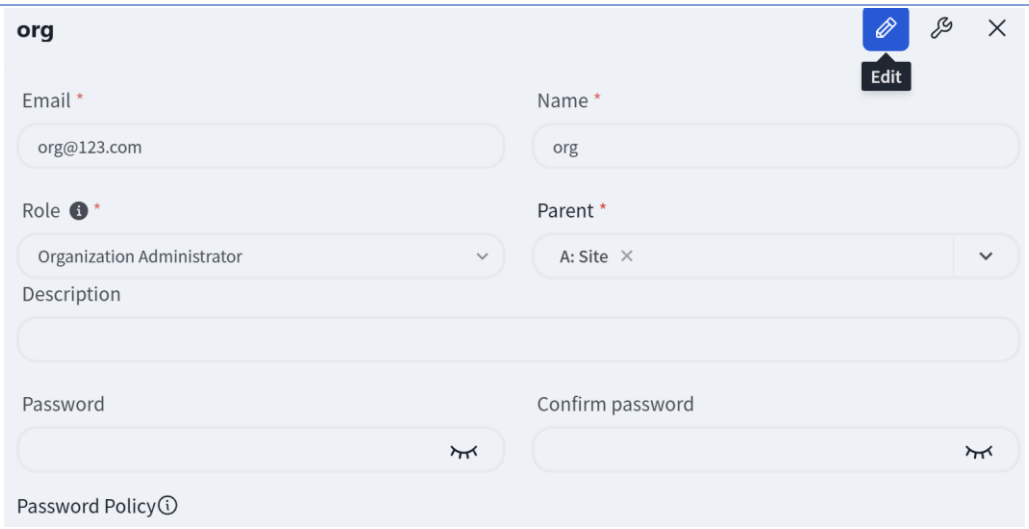
Re-verify Email: Send a verification email to the user's email address. The user clicks on the [Confirm Email Address] in the email to complete the verification. If not clicked, it will show that the user has not verified.

Send Email Invitation: Send an invitation email to the user's email address. After the user clicks on [Accept Invitation] in the email, they will be directly redirected to the controller page.

Reset password: Send a password reset email to the user's mailbox. After the user clicks on the [Reset Password] in the email, they will be directly redirected to the controller's password reset page.

10.3 View Details

Click on the user directly or click on the icon on the far right of the user to enter the detail page. Click on the **[Edit]** button in the upper right corner to adjust user permissions and change passwords.



Email: The email used by the user when logging in

Name: User name

Role:

- **System Administrator:** The user with the highest authority in the system and full control over the system.
- **Organizational Administrator:** Users with organizational management permissions in the system have full control over the organization.
- **General Administrator**: A user responsible for managing the system and user permissions.
- **Normal user:** A user responsible for monitoring and maintaining network operations, only having viewing permissions.

Parent: Manageable venue corresponding to user roles

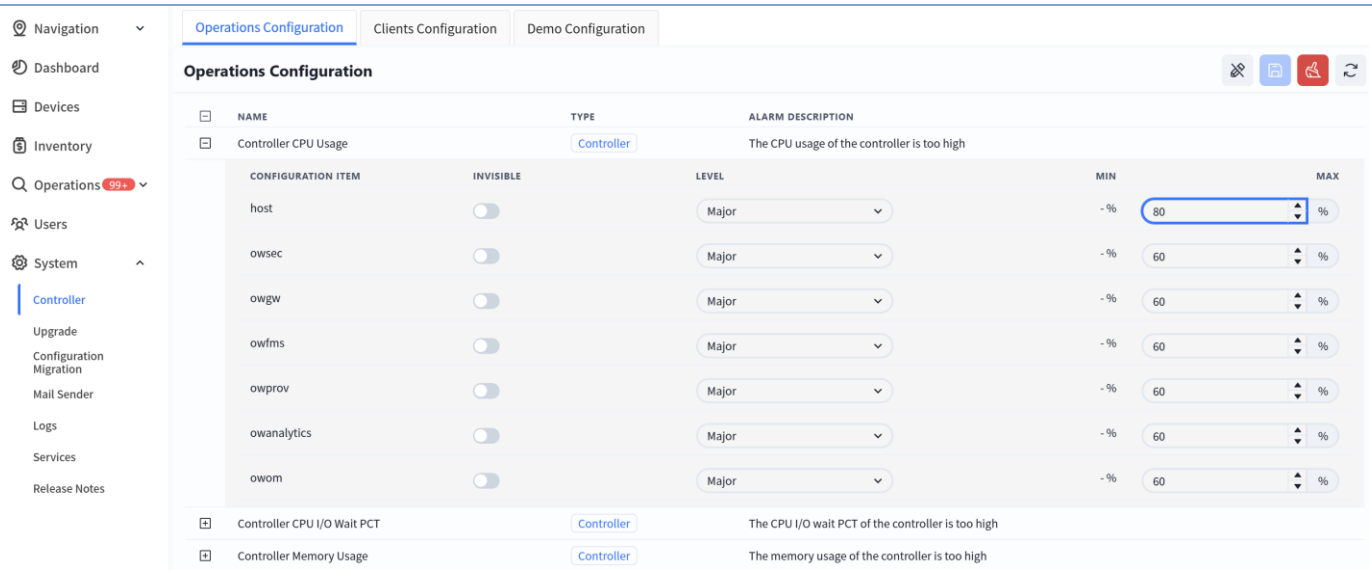
Passwords: User passwords can be modified on this page. The password policy displays the format requirements for setting passwords

11 System Configuration and Upgrade

11.1 Controller configuration

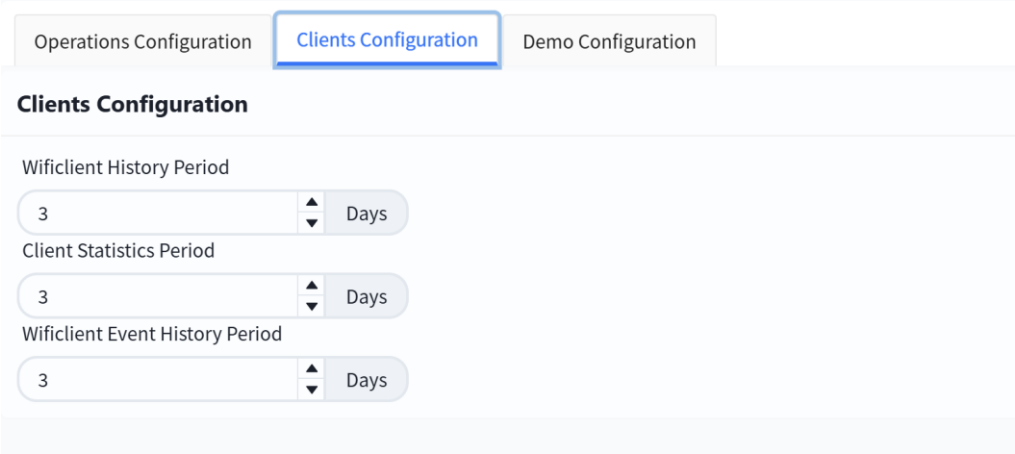
11.1.1 Operations Configuration

Users can freely adjust the alarm levels and maximum values of each item on the **[System]** - **[Controller]** –**[Operations Configuration]** view.



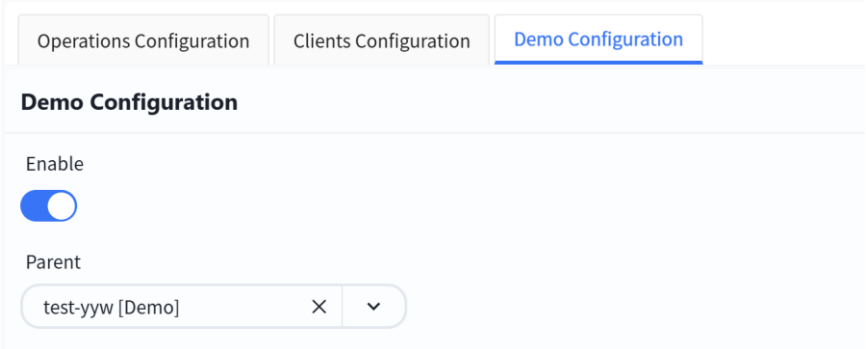
11.1.2 Clients Configuration

Users can adjust the storage period of terminal statistical information as needed on the clients configuration view.



11.1.3 Demo Configuration

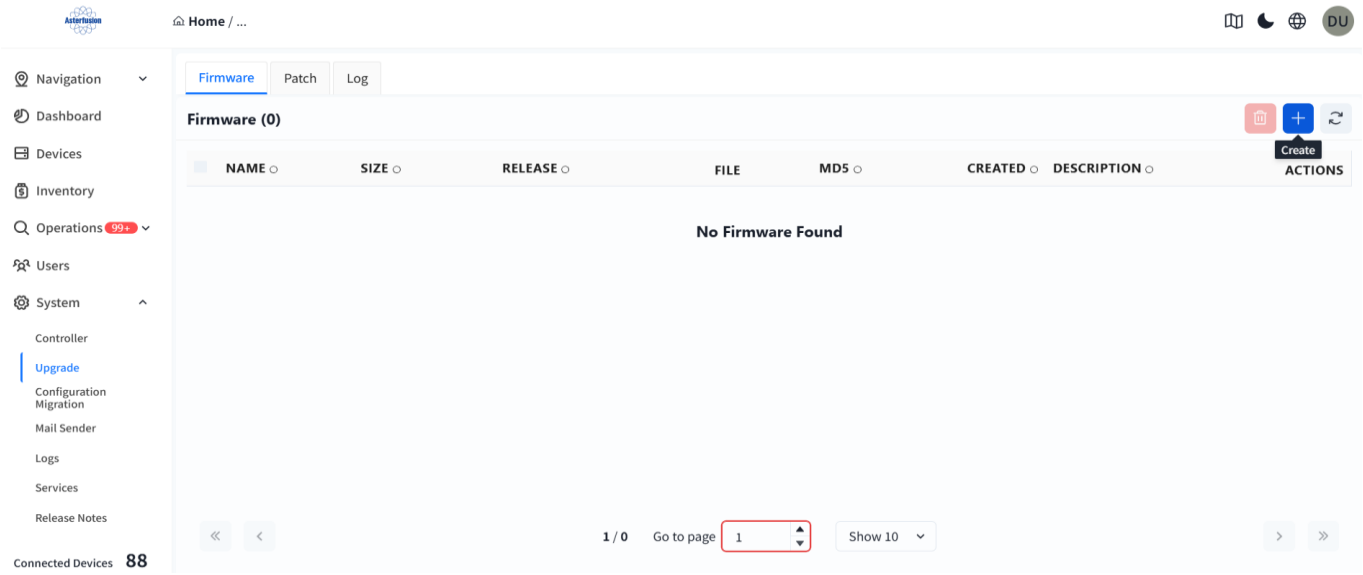
The system administrator can configure the demonstration environment, and all users have the viewing permission of the demo environment.



11.2 Controller Upgrade

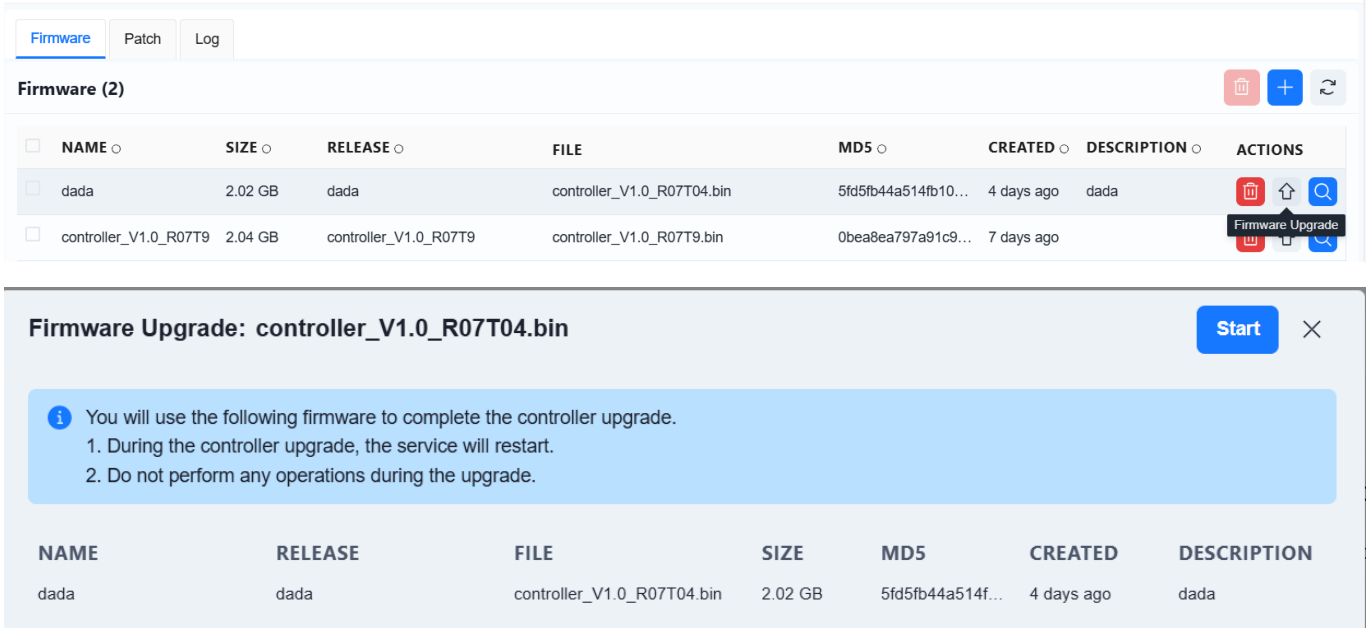
11.2.1 Firmware

Go to the **[System] - [Upgrade] - [Firmware]** view and click the **[+]** in the upper right corner to create a firmware.



Upload the file accor ding to the page prompts, fill in information such as the name and version, and click **[Save]** in the upper right corner.

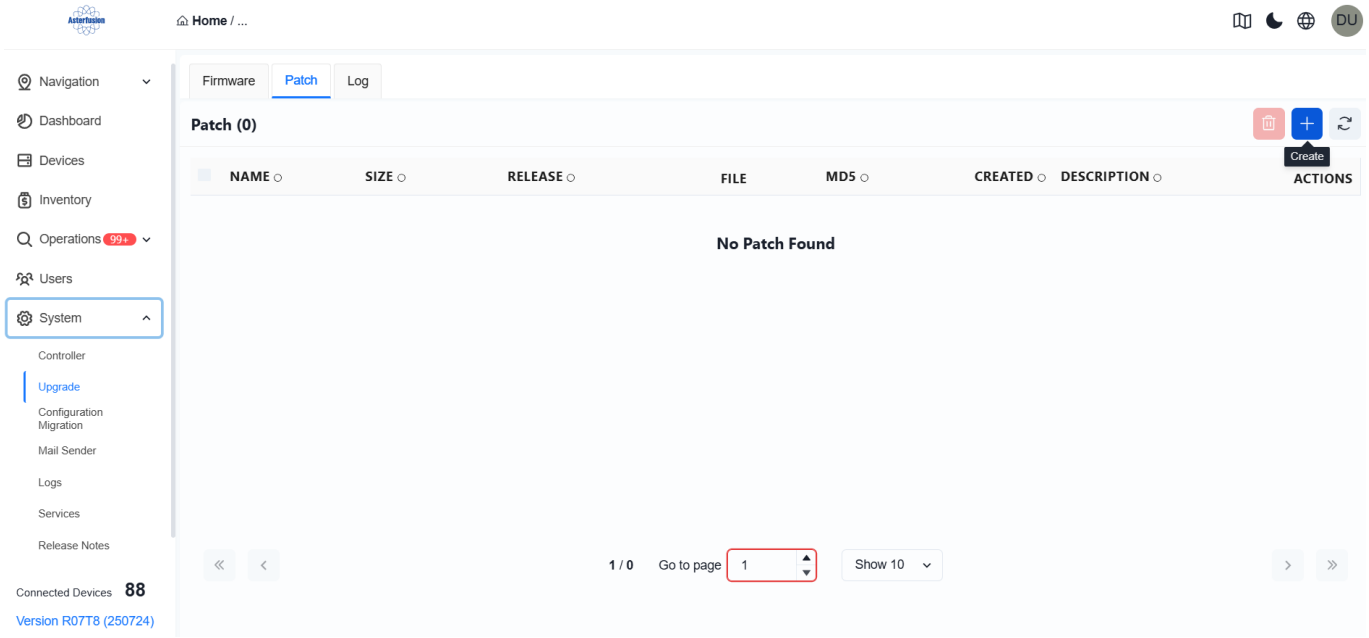
After uploading, click **[Firmware Upgrade] - [Start]** on the right to upgrade the controller firmware.



11.2.2 Patch

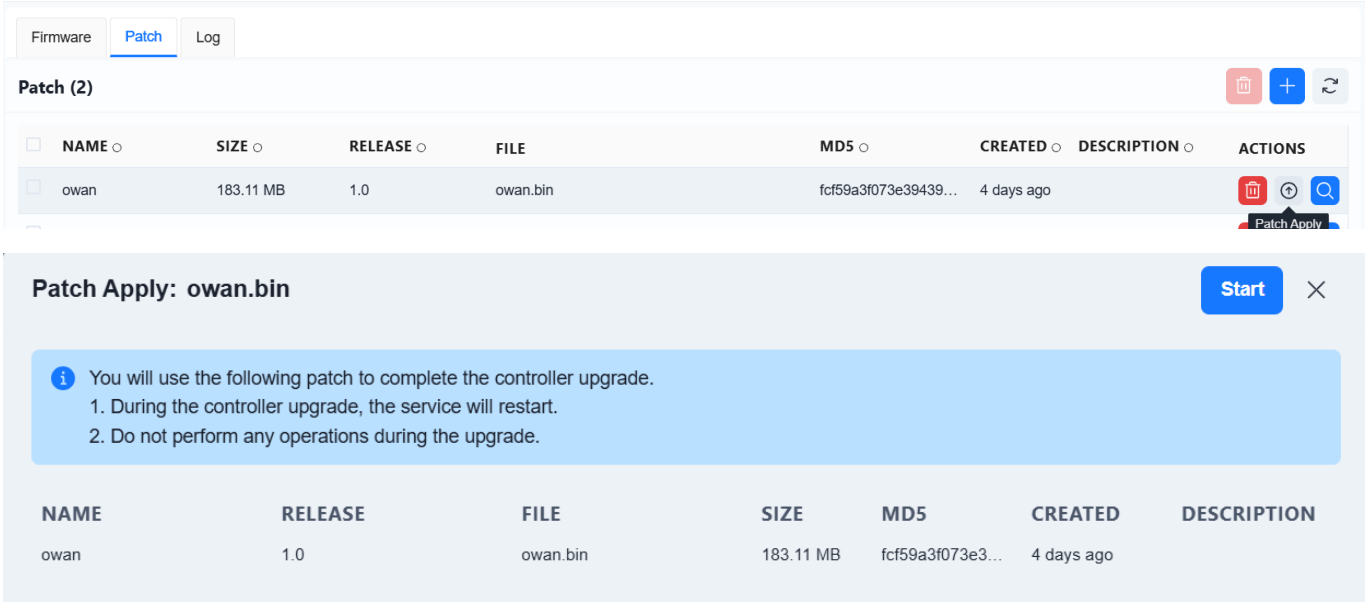
Patches can achieve precise modifications to target files through incremental updates.

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



Upload the file according to the page prompt, fill in information such as the name and version, and click **[Save]** in the upper right corner.

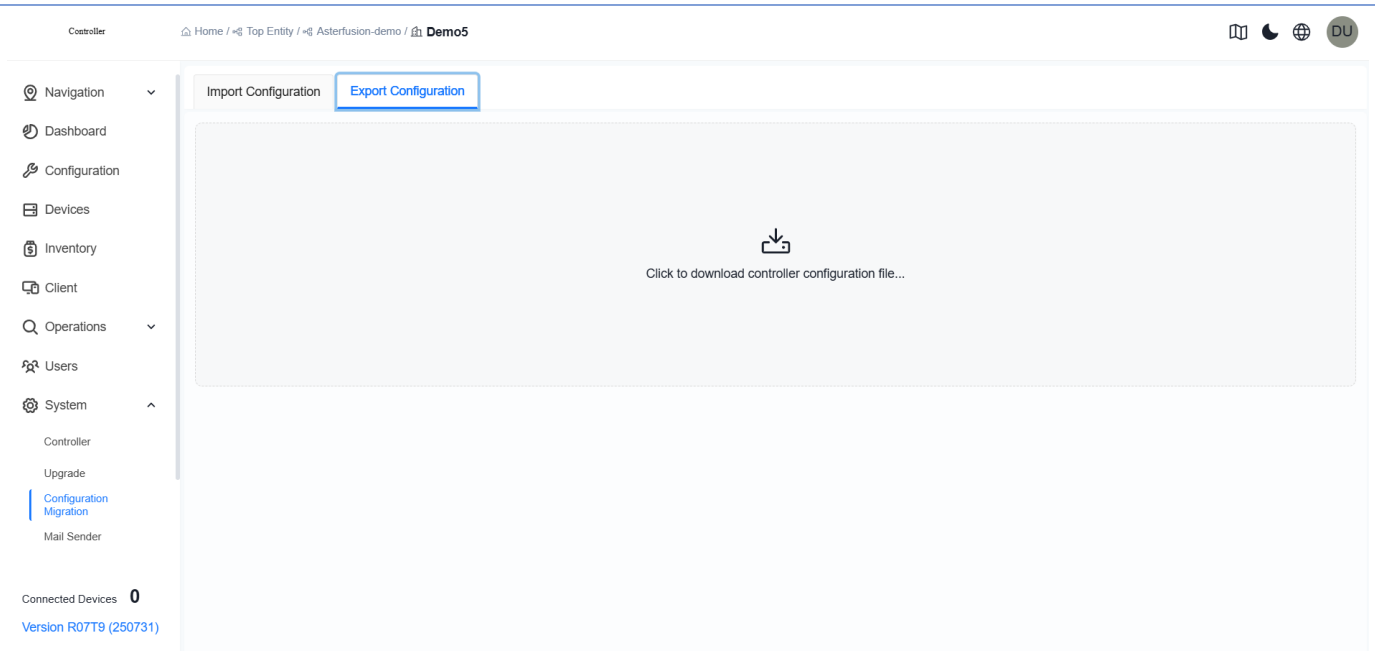
Click **[Patch Apply] - [Start]** on the right side to apply the controller patch.



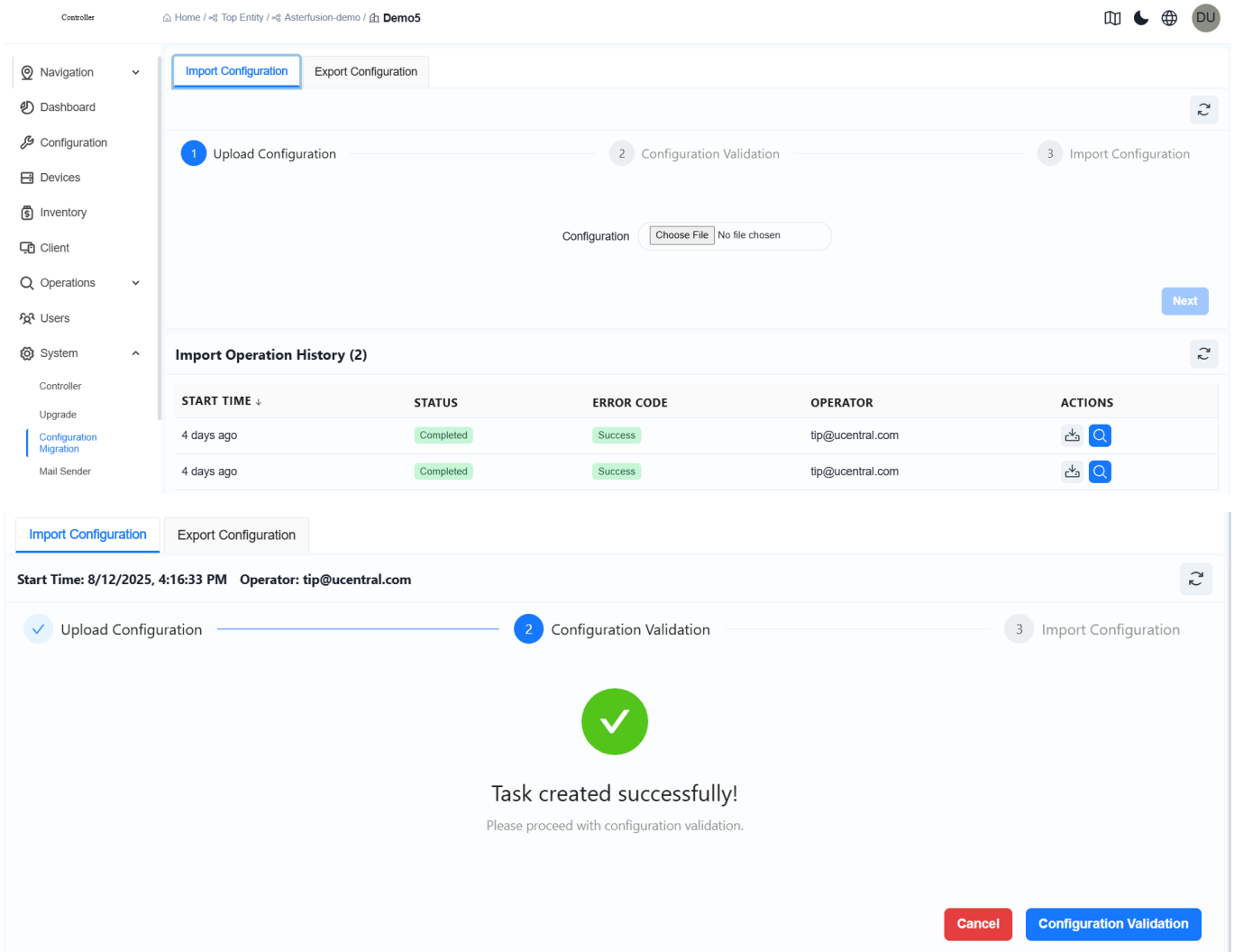
11.3 Configuration Migration

The controller configuration migration function enables the overall configuration migration through a one-click operation, which facilitates users to quickly reuse the existing configuration when creating a new controller.

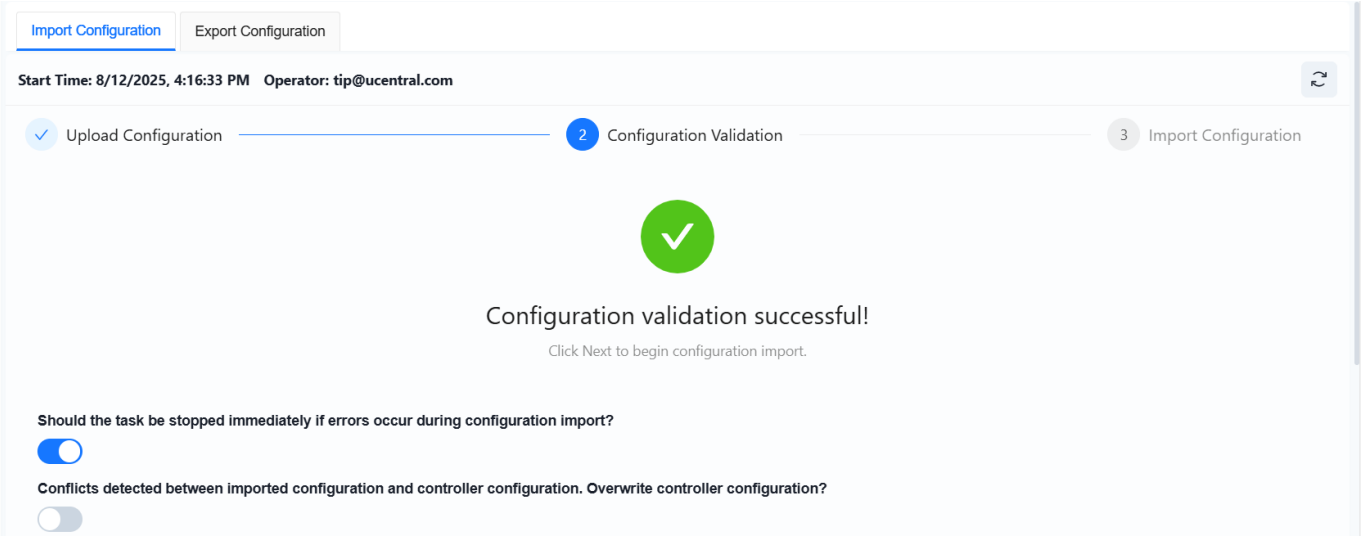
Enter the **[System] - [Configuration Migration]** view of the original controller, click **[Export Configuration]** - **[Click to Download the Controller Configuration File]** to export the configuration file.



In the controller where you need to import the configuration, go to **[System] – [Configuration Migration] – [Import Configuration]**, and click **[Choose File] – [Next]**.



Click on **[Configuration Verification]**



Scroll down the page and click **[Next]** to proceed with the import configuration.

12 Solution Classic Configuration

12.1 Small/Mid-Scale Campus

12.1.1 Scenario Overview

This solution is targeted at small and medium-sized parks and adopts the advanced Spine-Leaf full three-layer network architecture. It realizes the automated deployment, centralized management and intelligent operation and maintenance of the network through a cloud-based park controller. The solution adopts key technologies such as distributed gateways and DHCP high availability, providing a high-performance and highly reliable network foundation for the access of small and medium-sized terminals.

Centrally Intelligent Management Core

The controller automatically translates business intents into device configurations through a graphical interface and deploys them accurately, completely eliminating the traditional tedious process of configuring devices one by one via command-line interface. It offers full lifecycle management, including device onboarding, monitoring, and diagnostics, enabling network automation and high reliability.

Elastic and Reliable Network Backbone

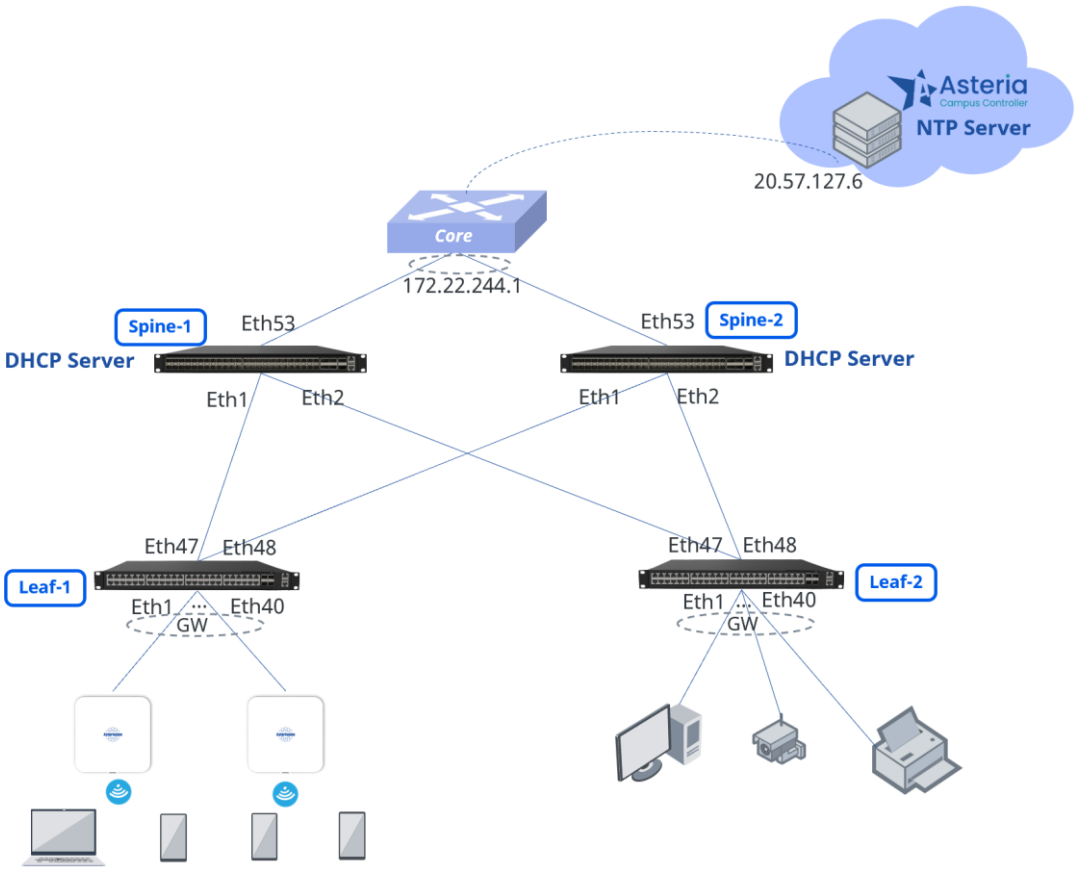
- Simple and flat, efficient forwarding: Adopting a Spine-Leaf two-layer architecture, the structure is simple and the path is optimized. All Leaf devices are fully interconnected with dual Spine, achieving efficient and low-latency data forwarding between any two points.

- Distributed gateway, traffic optimization: Business gateways are distributed and deployed on Leaf switches at each access layer. Cross-subnet communication traffic between terminals can be forwarded nearby at the access layer without detour to the core, effectively reducing transmission delay, enhancing service experience, and simultaneously alleviating the load pressure on the Spine layer.

Stable and reliable access and service

- Leaf Distributed Gateway: Serving wired and wireless terminals within the park. The gateway is lowered to the access Leaf, achieving isolation of the broadcast domain and convergence of the fault domain. While providing flexible subnet planning, it ensures the stability and forwarding efficiency of the access layer.
- High availability of key services: Deploy key network services such as DHCP Server on two Spine devices and automatically build DHCP Failover relationships. This design ensures the continuous availability of the address allocation service. Even if a single Spine device fails, seamless service switching can be achieved, guaranteeing the continuity of terminal business.

12.1.2 Scheme Design



The small and medium-sized campus network adopts the Spine-Leaf networking architecture, based on

the classic full three-layer routing network of the cloud-based campus. eBGP is automatically formed between Spine and Leaf through the controller, and distributed gateways are deployed on Leaf devices.

Access Zone:

Leaf1 and Leaf2 serve as distributed gateways. Leaf1 is responsible for connecting aps and wireless terminals, while Leaf2 is responsible for connecting wired terminals.

DHCP Deployment:

DHCP Servers are deployed on both Spine devices and are automatically configured as a DHCP Failover pair via the controller, ensuring high availability of address services.

Controller Deployment:

The controller is cloud-based and enables centralized policy deployment, configuration management, and status monitoring for all network devices through a graphical interface, significantly improving operational efficiency.

Foundation Link Data Planning

Device	Interface	IP Address
Spine1	Ethernet53	172.22.244.10/24
	Loopback0	172.22.252.51/32
Spine2	Ethernet53	172.22.244.11/24
	Loopback0	172.22.252.52/32
Leaf1	Loopback0	172.22.252.53/32
Leaf2	Loopback0	172.22.252.54/32

Service Network Data Planning

Service Type	IP Segment	Gateway	Service VLAN	SSID
Wireless Service	180.10.0.0/24	180.10.0.1/24	1080	New SSID
Wired Service	180.10.1.0/24	180.10.1.1/24	1081	
AP Management	180.10.2.0/24	180.10.2.1/24	1082	

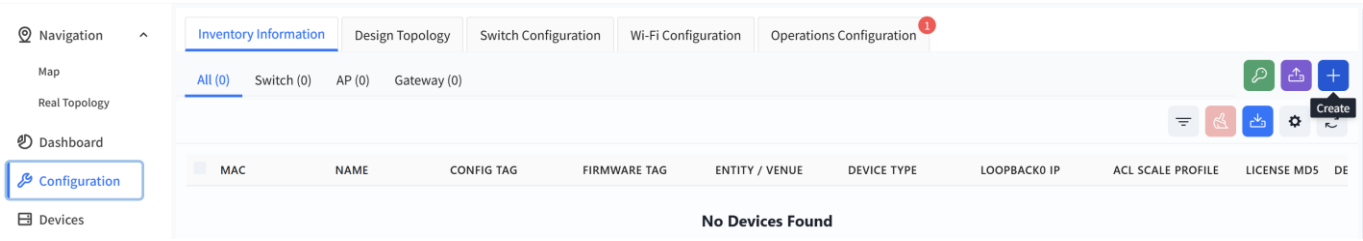
12.1.3 Device Import

Administrators can create or import devices in bulk to specified sites/organizations. When an added

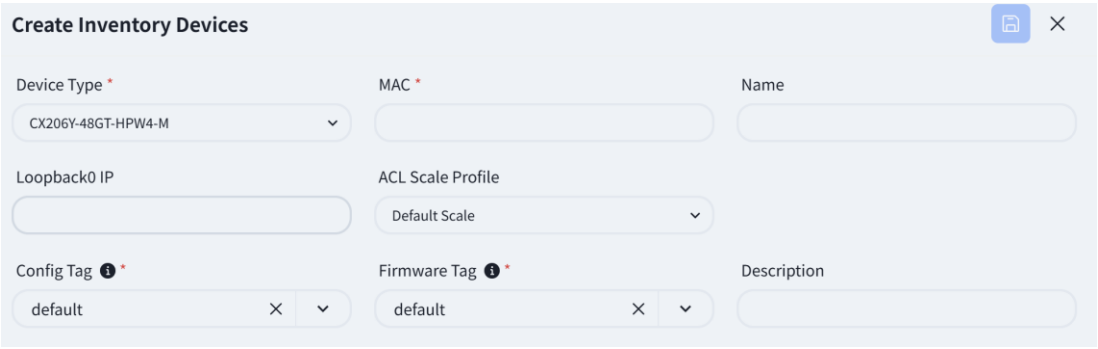
inventory device connects to the controller and comes online, the controller will automatically assign it to the designated organization/site based on its MAC address.

1. Add devices one by one.

Click **[Configuration]** - **[Inventory Information]** - **[+]** to create an inventory device.

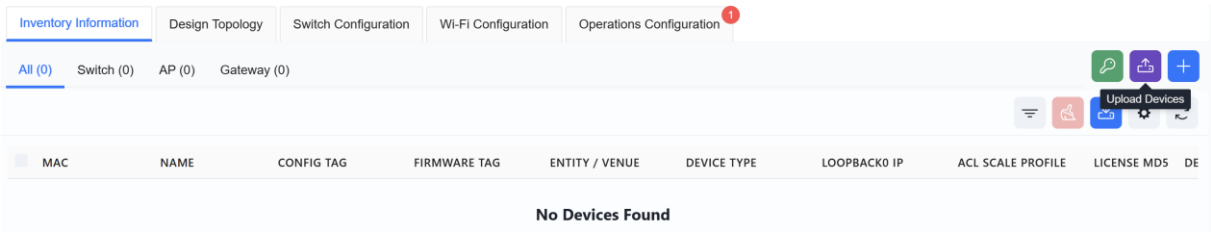


Fill in the relevant information as prompted on the page



2. Import via Excel

Click **[Upload Devices]**



Click **[Download Template]** and enter the information for the devices to be added to the inventory according to the template's specifications.

MAC	DeviceType	Name	ConfigTag	FirmwareTag	Loopback	AclScaleProfile	License	Description
60eb5a000001	CX308P-48Y-M	Spine1						
60eb5a000002	CX308P-48Y-M	Spine2						
60eb5a000005	CX206Y-48GT-HPW4-M	Leaf1						
60eb5a000006	CX206Y-48GT-M	Leaf2						
60eb5a000007	CAP7030-Z			default				
60eb5a000008	CAP7030-Z			default				
60eb5a000009	CAP7030-Z			default				
60eb5a000010	CAP7030-Z			default				
60eb5a000011	CAP7030-Z			default				
60eb5a000012	CAP7030-Z			default				
60eb5a000013	CAP7030-Z			default				
60eb5a000014	CAP7030-Z			default				
60eb5a000015	CAP7030-Z			default				
60eb5a000016	CAP7030-Z			default				
60eb5a000017	CAP7030-Z			default				

MAC: The device's MAC address. This information is typically found on the device's label.

Device Type: The device model.

Name: The device hostname. By default, it is the device's MAC address.

ConfigTag: After an AP connects to the controller, it will automatically pull the configuration file corresponding to this tag. By default, the tag value is default.

FirmwareTag: When performing firmware upgrades, devices requiring an upgrade can be filtered based on their firmware tag type. By default, the tag value is default.

Loopback: The device's loopback address. For all devices operating at Layer 3, this address serves as the device's in-band management address.

AclScaleProfile: Optional values are default or large-scale. By default, the value is default.

License: The AP's license file. For bulk imports, you can either enter the JSON-formatted license file content directly in the Excel sheet, or add all devices to inventory first and then import the license files in bulk afterward.

Description: Descriptive information about the device.

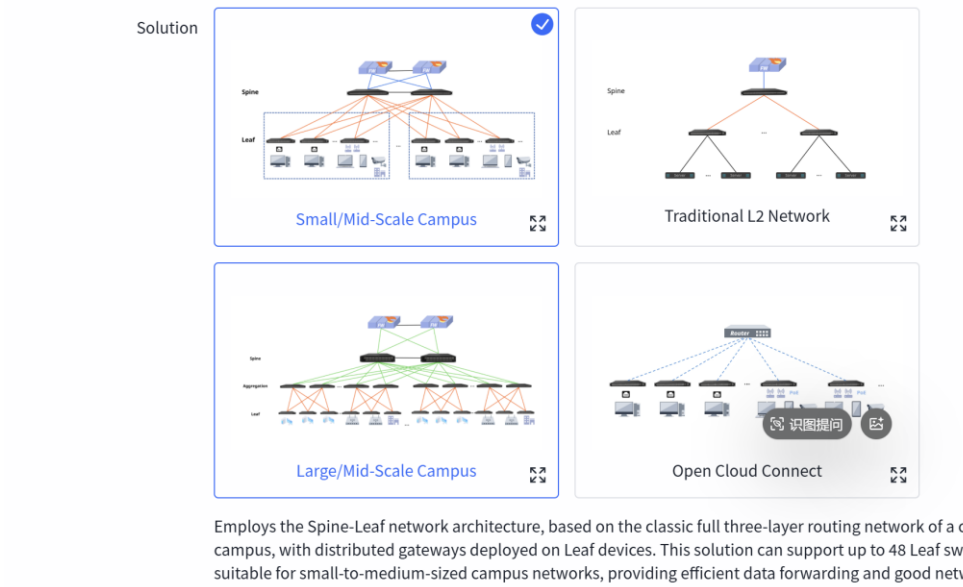
Click **[Choose File]** to upload the completed template, then click **[Test Upload Data]**. The controller will automatically check if the uploaded data complies with the specifications and display the results in the test report.

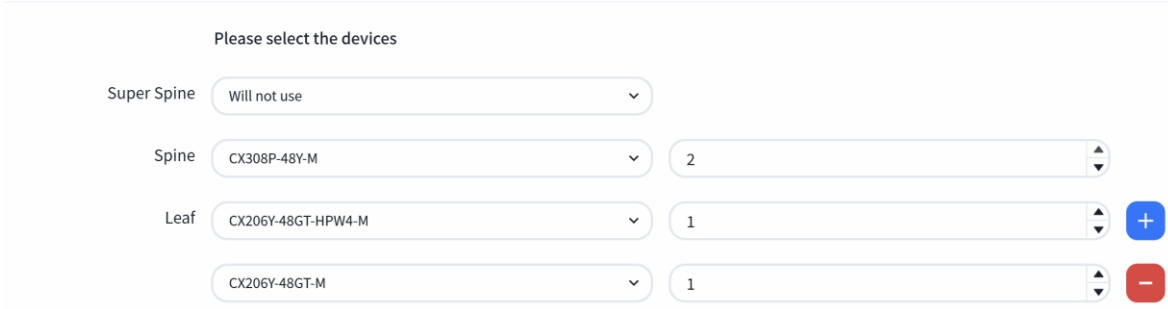
Once completed, users can view the created devices in the **[Inventory Information]** view.

12.1.4 Service Configuration

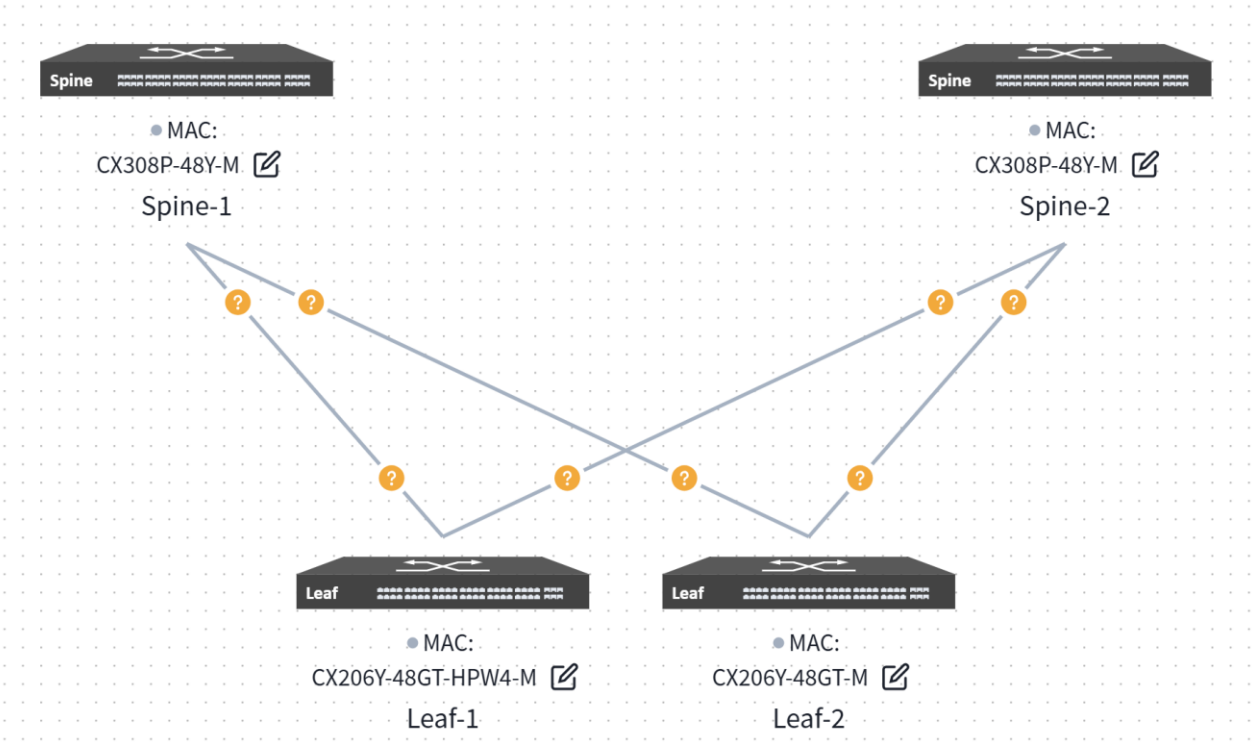
Click **[Design Topology]** to enter the corresponding page, select the Large/Mild-Scale campus deployment, fill in the required device models and quantities according to device roles, and then click

[Save] to finish the network topology pre-planning. The controller will generate the network topology based on the entered information.

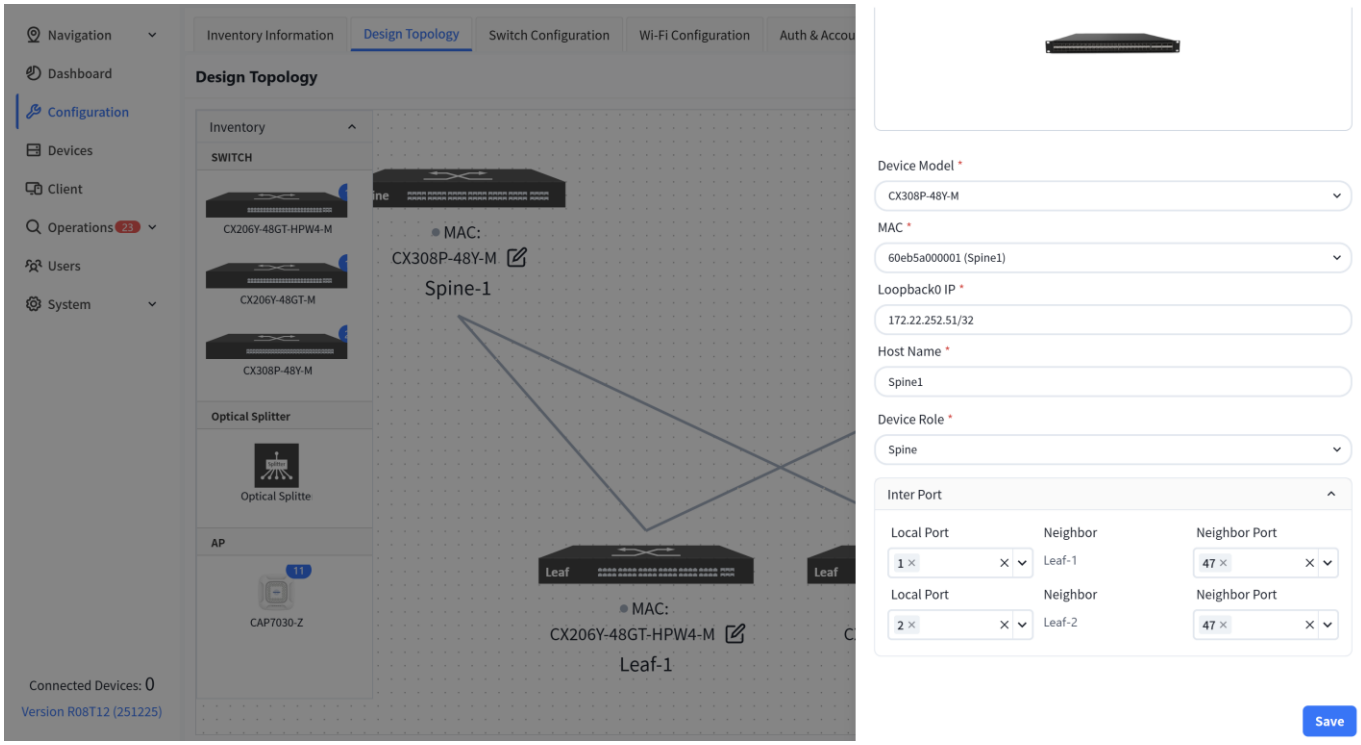




Generated topology:



Users can click the **[Edit]** button on the device end and fill in the corresponding information in the slide-out panel on the right.



MAC: Uniquely select a device via its MAC address.

Loopback0 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.

Inter Port:

Local Port: The interface on the current device.

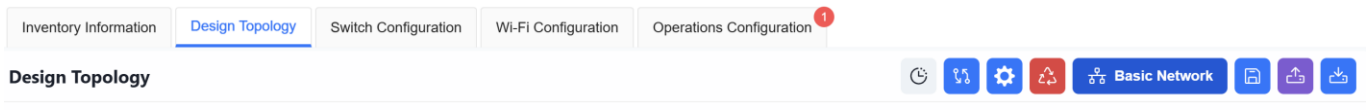
Neighbor: Select the peer device connected to the local interface.

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

Upon completing all configurations, click **[Save]** in the upper right corner of the page, then select **[Confirm]** in the pop-up window.

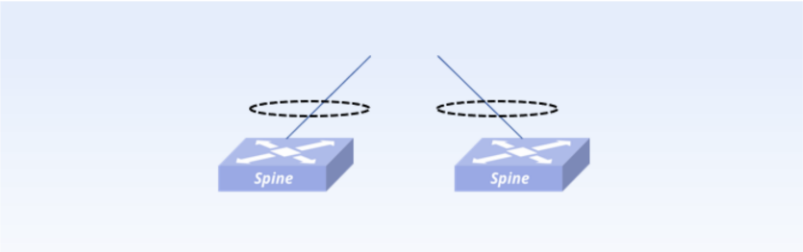
12.1.5 Basic Network

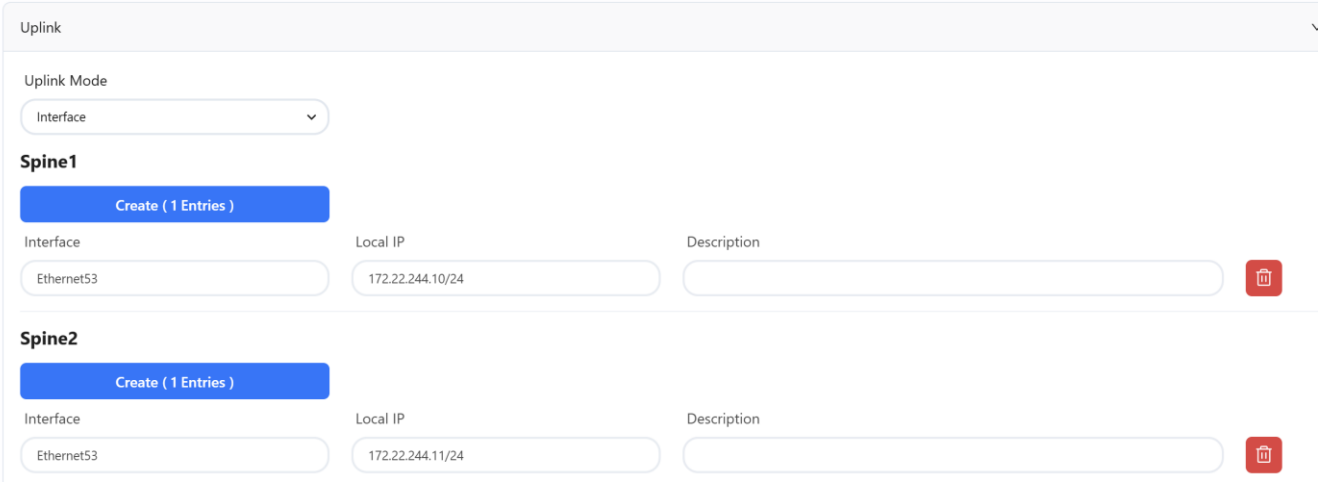
Click the top right corner **[Basic Network]**



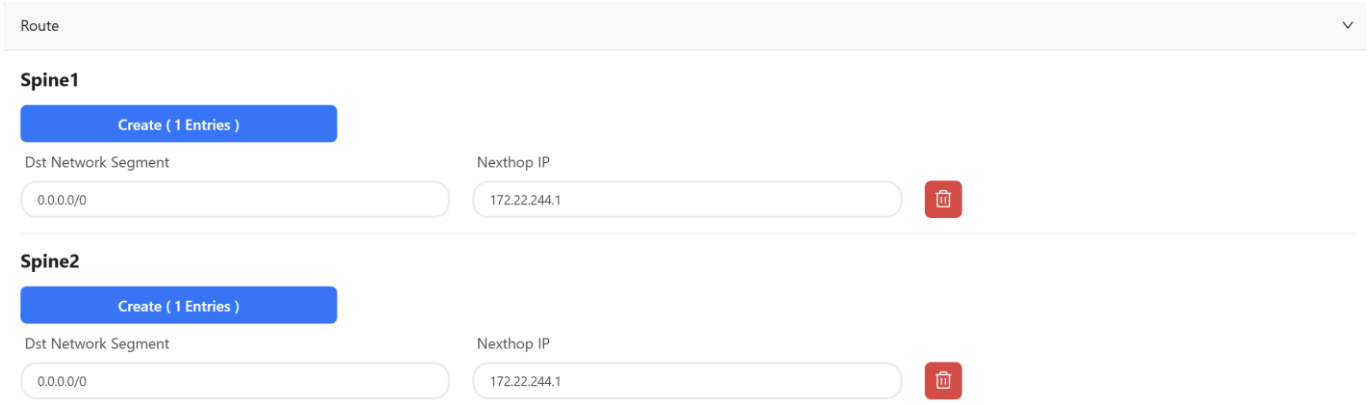
12.1.5.1 Egress Router

Click **[Create]**, select the interface ID of the Spine device's uplink interface, and configure the IP address as per the service plan.





To ensure normal network operation, a default route typically needs to be configured, with the next hop IP set as the peer IP address of the Spine uplink interface.



12.1.5.2 Device

Configure device management related information:

- ✧ TimeZone: Configure the system time zone.
- ✧ NTP: Configure NTP Server.
- ✧ SNMP: Configure SNMP community.
- ✧ Syslog: Configure syslog server IP address.

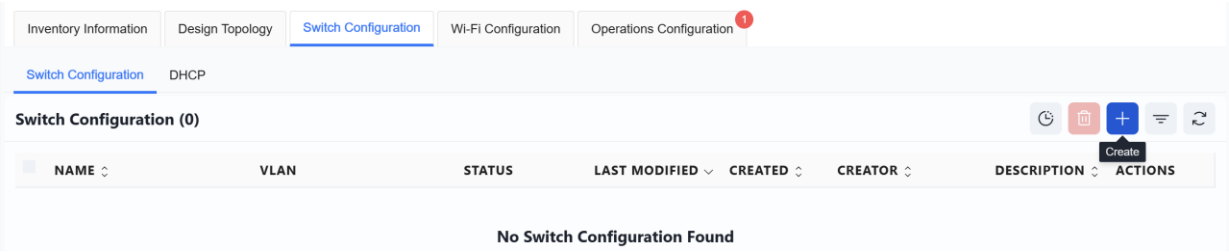
✧ TACACS+: Configure TACACS server IP address.

✧ Device ACL: Configure ACL rules restricting SSH, SNMP, TELNET connections to device.

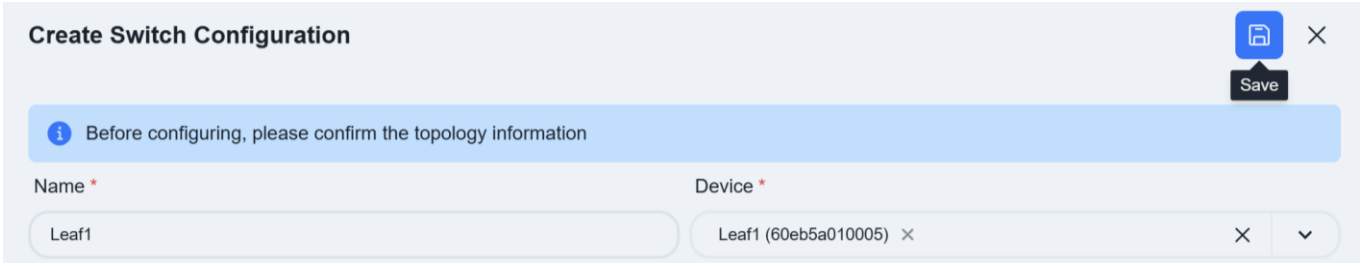
12.1.6 Switch Configuration

12.1.6.1 Switch Configuration

Click **[Create]** on the right to set up the switch configuration.



12.1.6.1.1 Leaf1

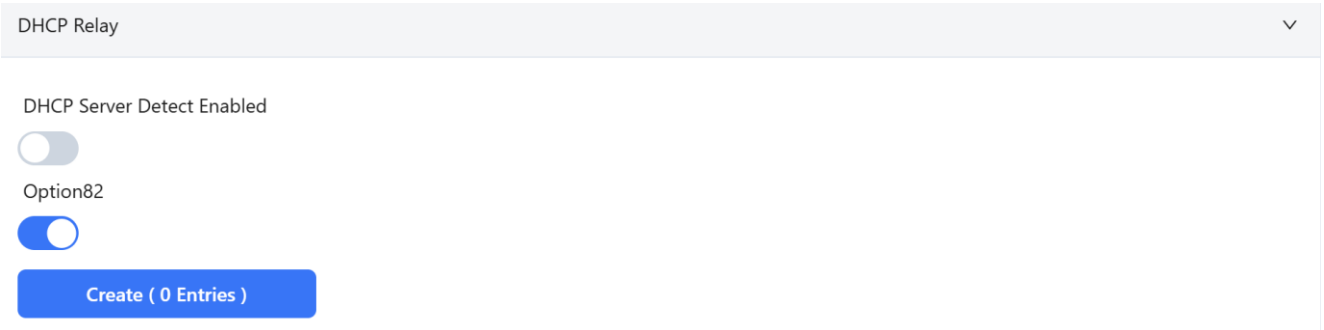


Name: User-defined

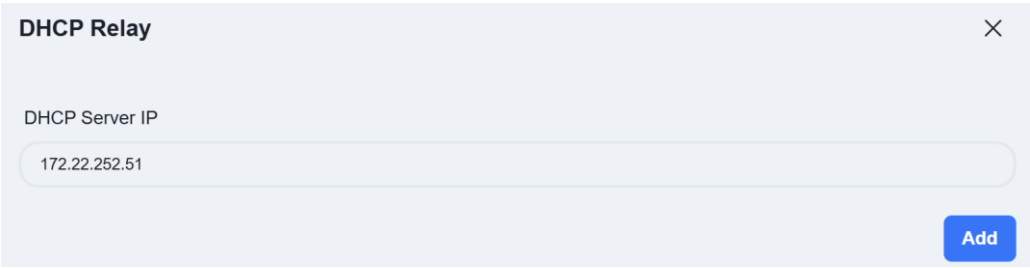
Device: Select the Access-1 device

1. DHCP Relay

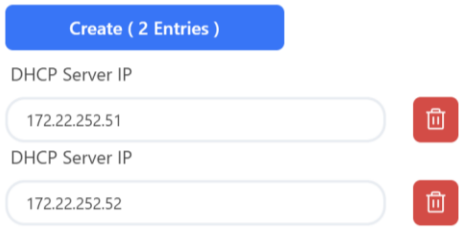
Since the DHCP Server is deployed on the Spine and is not directly connected to the service devices on Leaf1, a DHCP relay needs to be configured.



Click **[Create]**, enter the DHCP server IP in the pop-up page, and then click **[Add]** after completion.



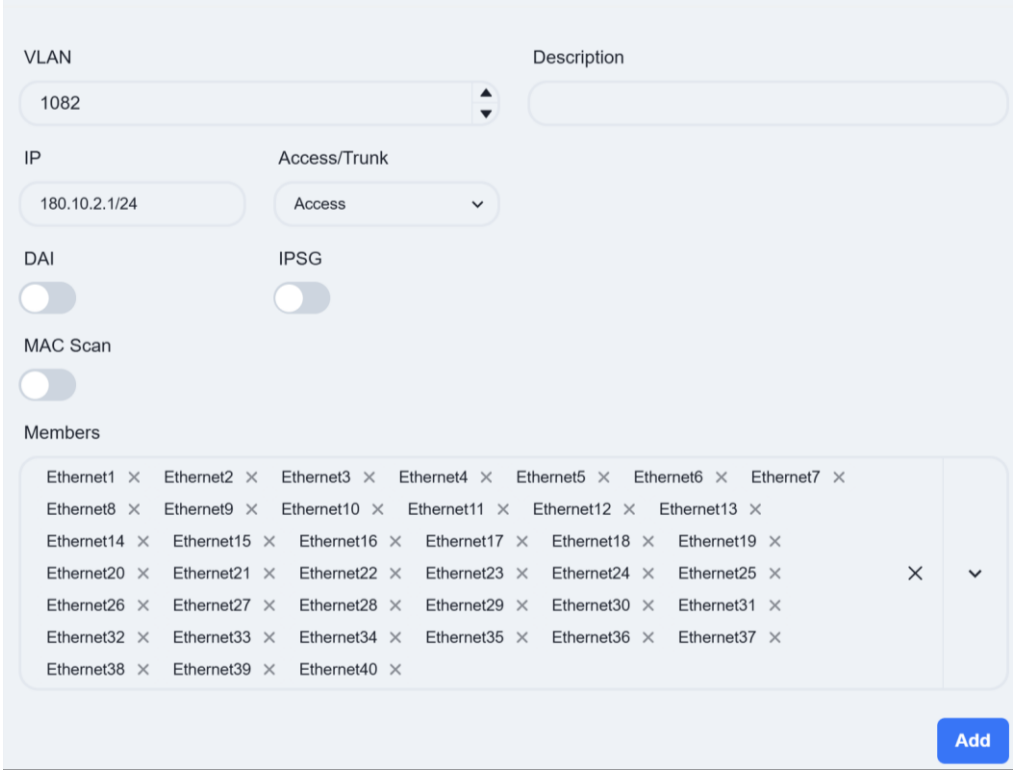
Since DHCP Servers are deployed on both Spine devices with DHCP Failover configured, two DHCP server IP addresses need to be entered.



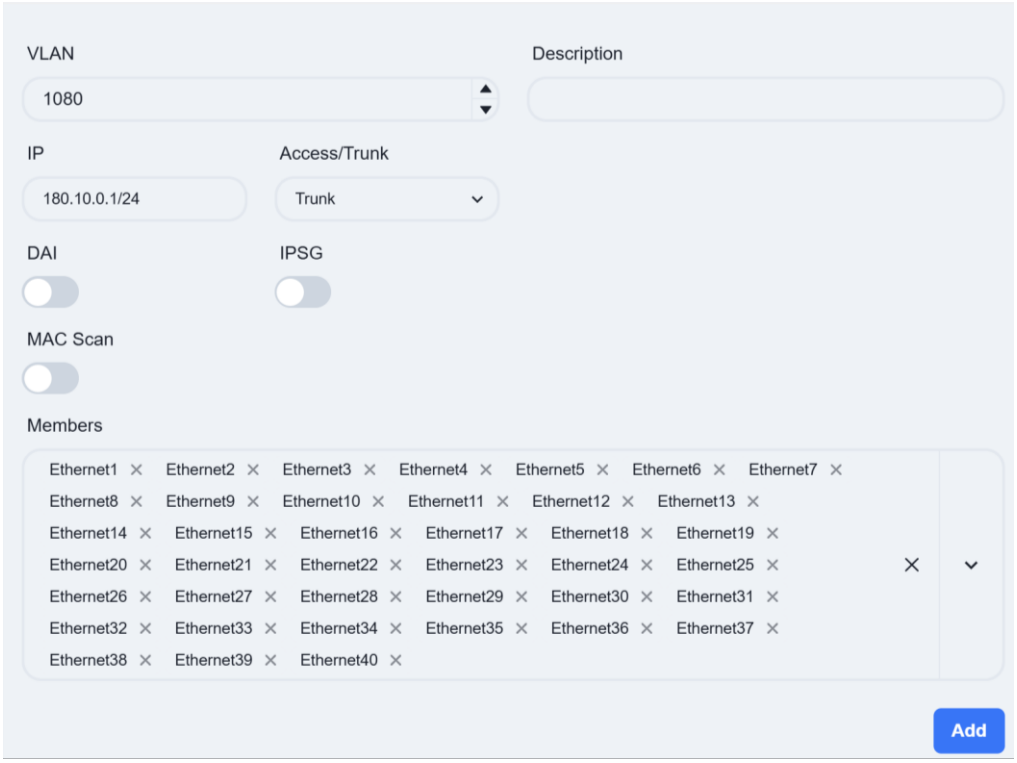
Services VLAN

Deploy wireless service configuration on Leaf1 and set up the service gateway.

1. Configure the AP management VLAN



2. Configure the Wireless Business VLAN



IP: Enter the service gateway address.

Access/Trunk: Select the mode based on whether the interfaces send and receive frames with VLAN tags.

Access: Receives untagged frames. Typically configured for the AP management VLAN and wired service VLANs.

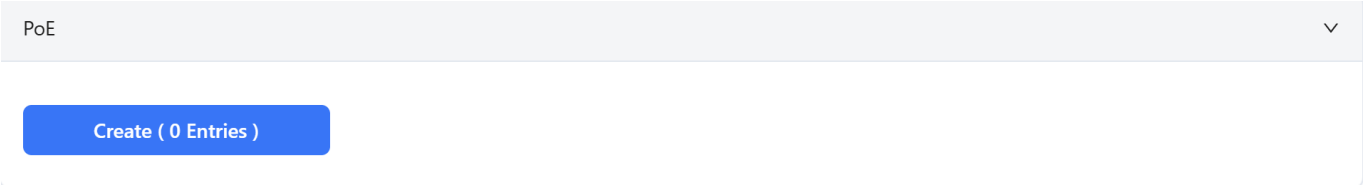
Trunk: Receives tagged frames. Typically configured for wireless service VLANs.

Members: Click the dropdown arrow to select the member interfaces for the VLAN on the device.

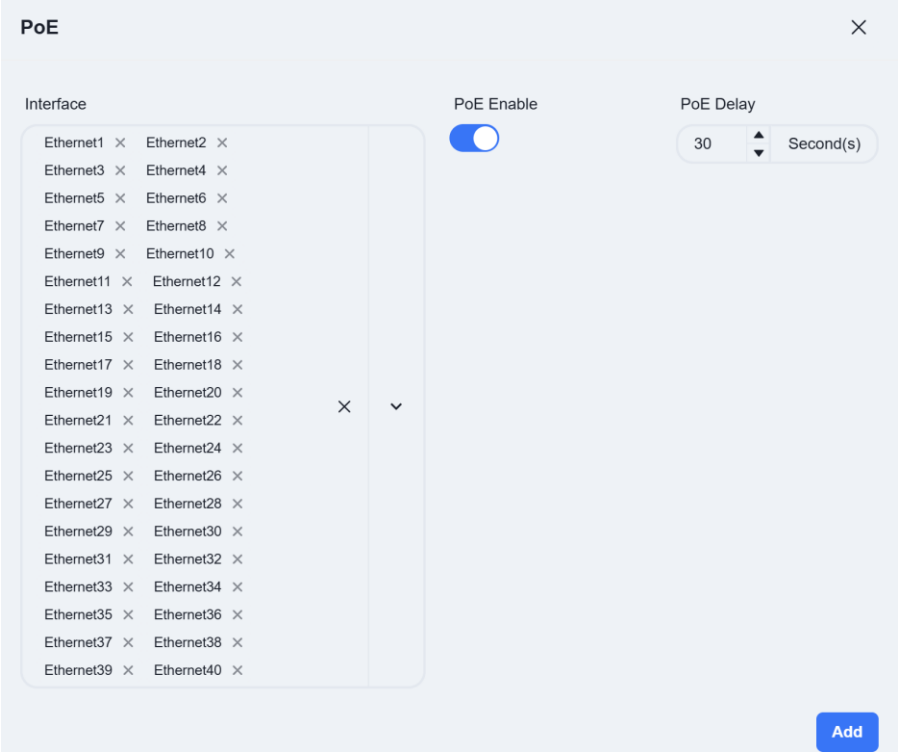
POE

The access switch features PoE functionality, which can be directly enabled in the wired service configuration to supply power to PD devices.

Click **[Create]**

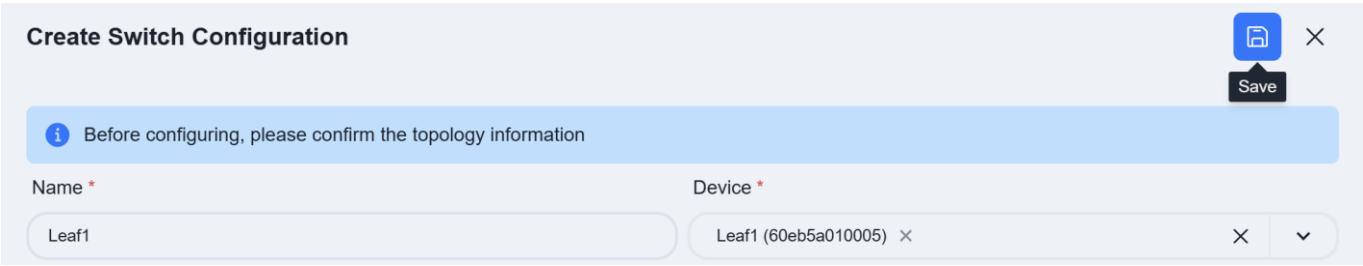


Select the interface where the PoE function is to be enabled and set the startup delay time.

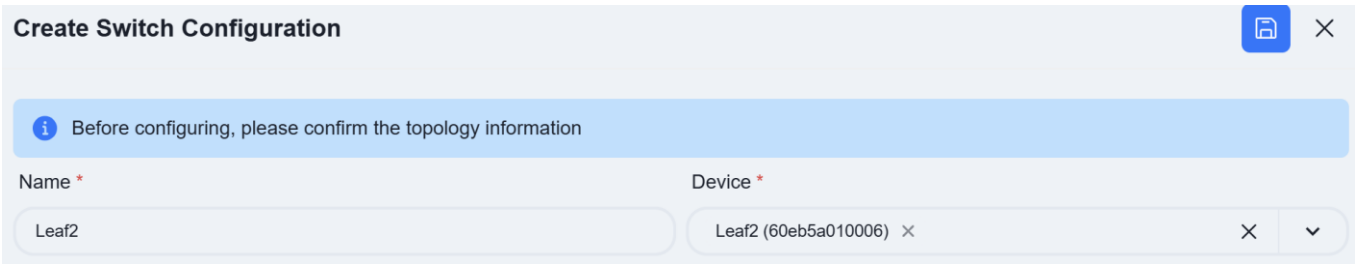


POE Delay: This refers to a brief, intentional time delay introduced at a PoE switch port between when it begins to supply power and when it actually delivers power to the Powered Device (PD).

Once all configurations are completed, click **[Save]** in the top right corner to finish configuring Leaf1.



12.1.6.1.2 Leaf2

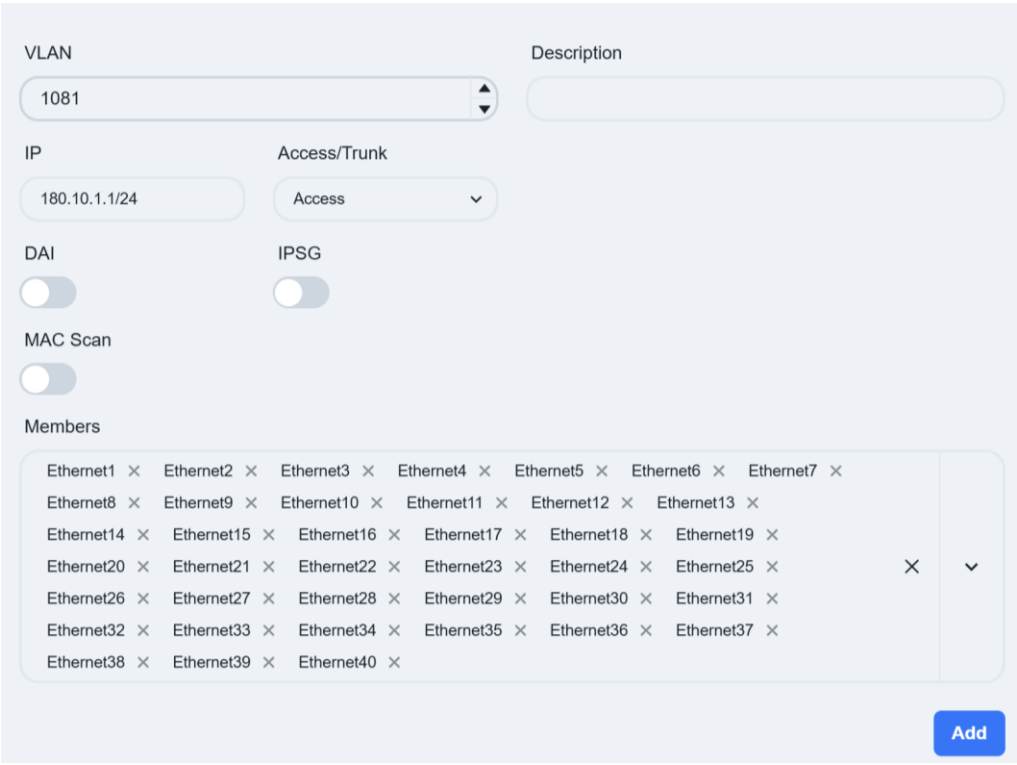


1. DHCP Relay

Same as Leaf1

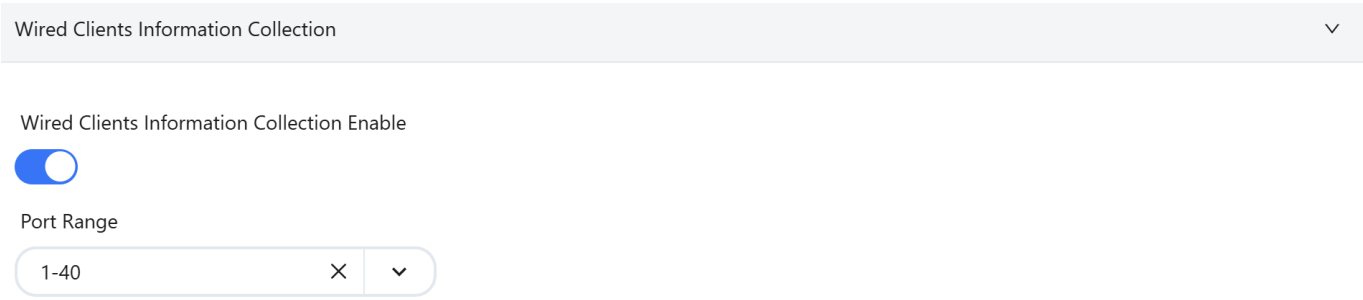
2. Services VLAN

Deploy wired service configuration on Leaf2 and set up the service gateway.



3. Wired Clients Information Collection

Interfaces with this feature enabled will report information about the connected wired terminals to the controller.

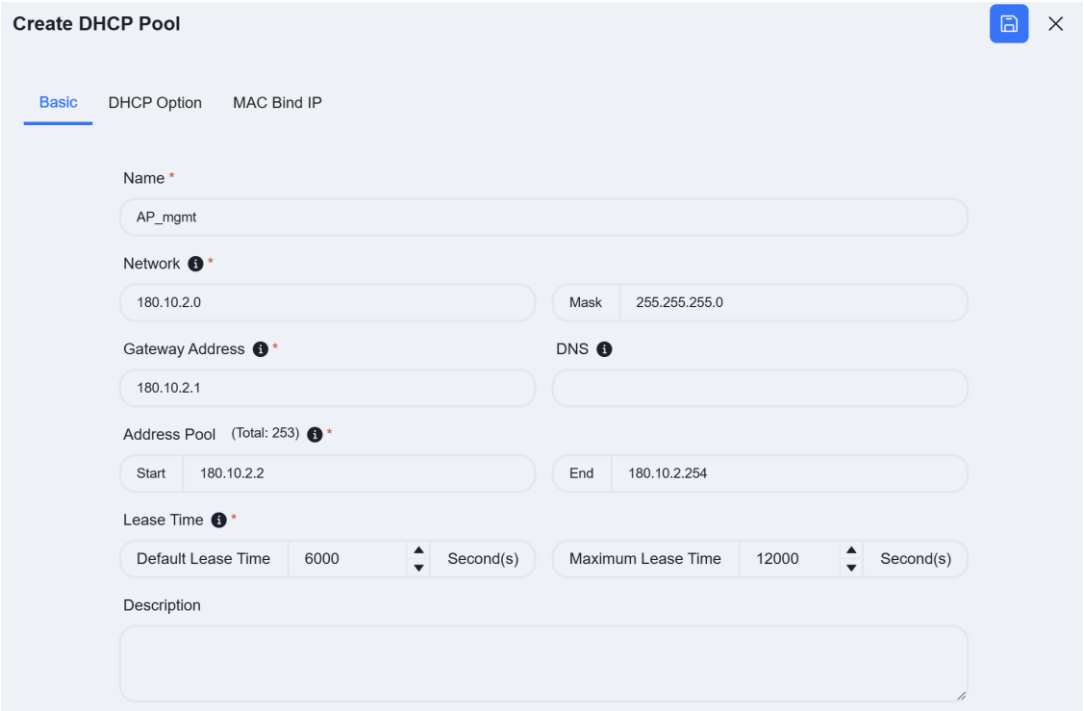


12.1.6.2 DHCP

The controller allows users to configure the DHCP Server function on Spine devices.

After entering the site, click **[Configuration]** - **[Switch Configuration]** - **[DHCP]** to access the DHCP Server configuration interface. Then, click the **[+]** button on the page to create a new configuration:

1. Create AP Management Address Pool.



Name: User defined.

Network: Specify the network segment where the IP address assigned by the DHCP server to the DHCP client is located.

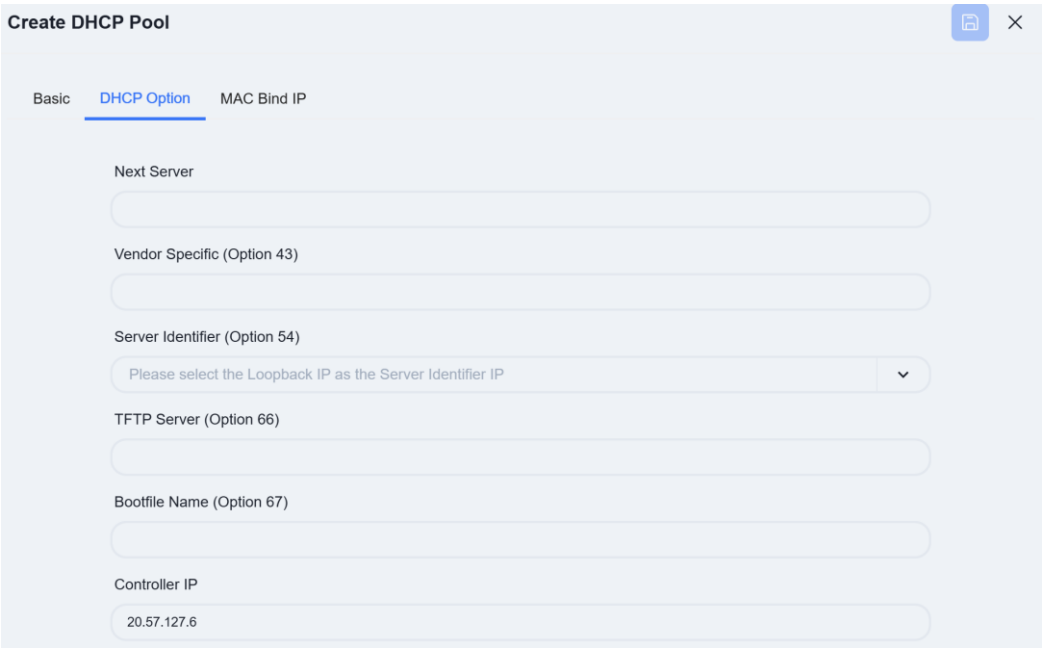
Gateway Address: Specify the gateway address assigned by the DHCP server to the DHCP client.

DNS: Specify the DNS server address.

Address Pool: Specify the address range allocated by the DHCP server to DHCP clients.

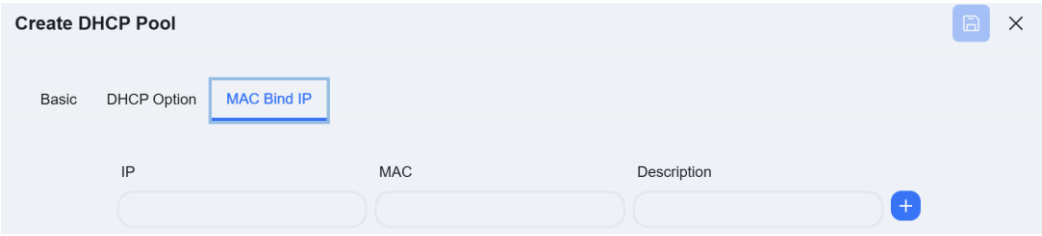
Lease Time: Specify the IP address lease time.

Click on **[DHCP Option]**and fill in the relevant information.



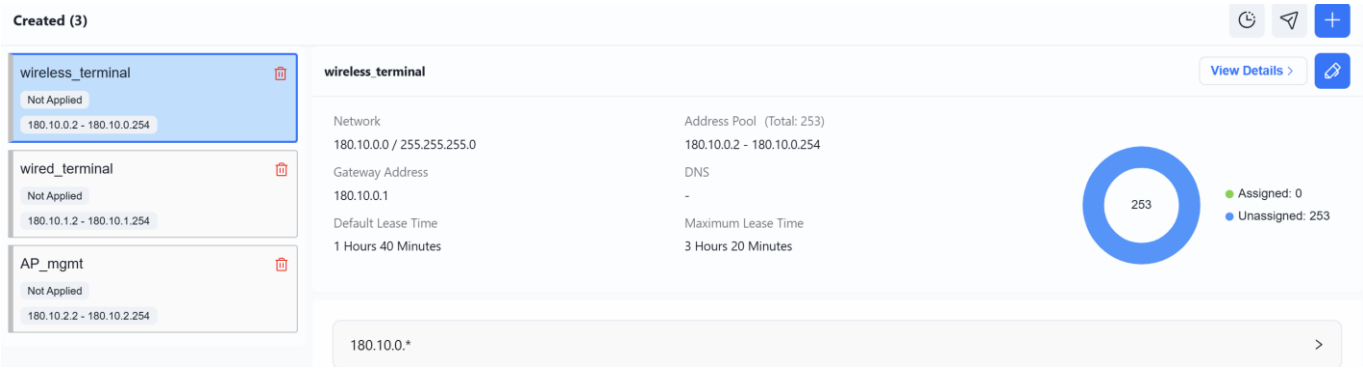
Controller IP: DHCP options specifically designed for wireless AP discovery controllers, fill in the controller IP address.

The controller supports configuring MAC binding IP function, which users can fill in as needed.



Click **[Save]** after completing all configurations.

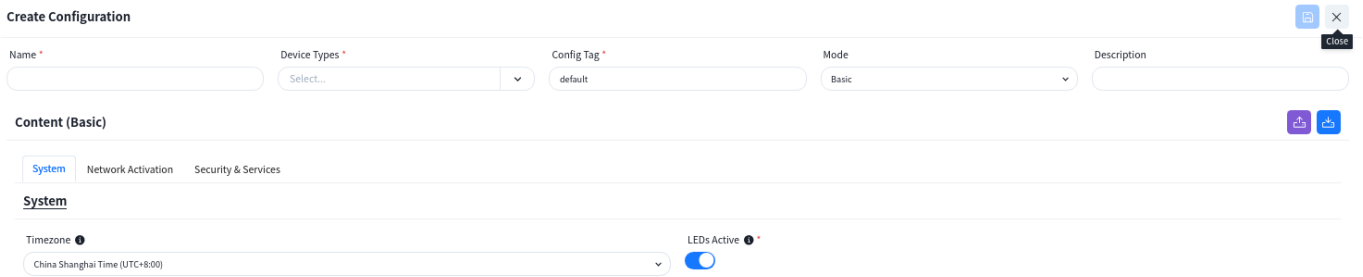
Follow the steps above to sequentially create the DHCP configurations for wireless terminals and wired terminals. Once all configurations are completed, the DHCP view will appear as shown below.



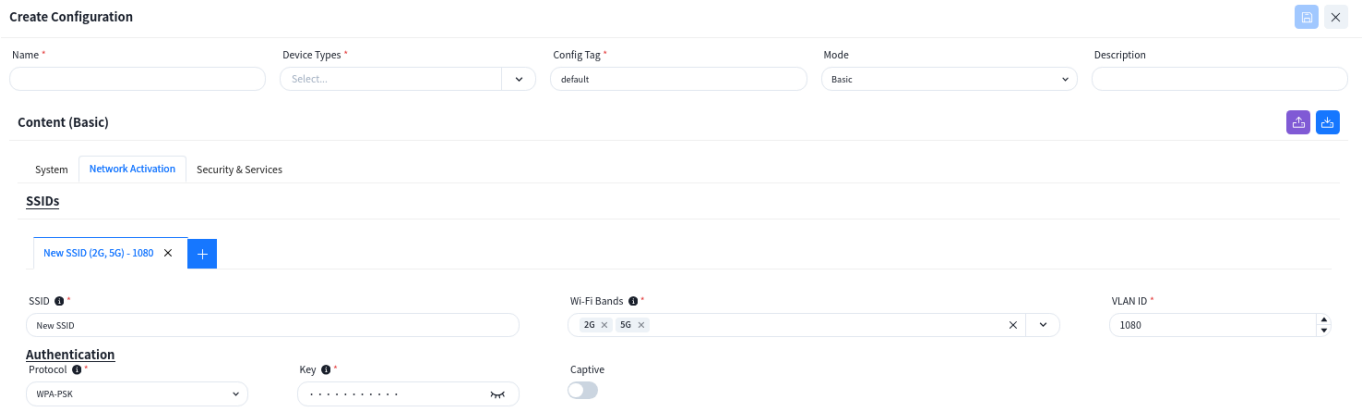
12.1.7 Wi-Fi Configuration

Click **[Wi-Fi Configuration] - [+]** to configure the necessary basic information for the wireless AP, e.g. SSID settings, security policy. The controller can automatically generate the corresponding

The controller supports the configuration of different wireless service configurations, and after the AP goes online, it will determine which configuration should be issued to the AP based on the **[Config Tag]** attributes of the configuration.

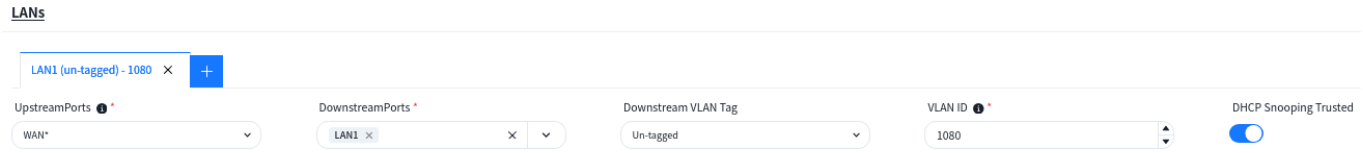


12.1.7.1 SSID



12.1.7.2 LAN

When the AP is one that has an extended wired interface and is capable of accessing terminals by wired means, such as a panel AP, the user can configure the access method for wired terminals through the configuration in LANs.



UpstreamPorts: Specify the up-link interfaces for wired terminal to access the network through AP, usually it is the interface for AP to connect to the switch, and keep the same with **[UpstreamPorts]** in **[SSID]** – **[Advanced]** Settings, the default is: WAN*.

DownstreamPorts: Interfaces for wired terminal access.

Downstream VLAN Tag: Whether the wired terminal carries VLAN Tag.

VLAN ID: The AP receives messages from wired terminals that add this VLAN TAG to identify.

DHCP Snooping Trusted: DHCP Snooping Trusted interface, if the wired terminal needs to obtain IP address through DHCP service, this switch needs to be on.

12.1.8 Configuration Release

12.1.8.1 Switch

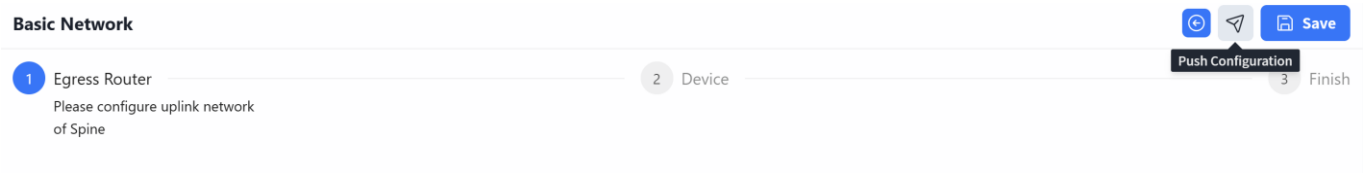
Switches support both in-band and out-of-band management methods. Operation and maintenance personnel can flexibly choose based on current network conditions. For devices in the factory default state, whenever either the management port or service port is in an "Up" state, they will actively initiate a DHCP request to obtain a temporary management IP address and the IP address of the cloud-based

controller from the DHCP server. They will then connect to the controller to retrieve configuration information.

Once all switches are successfully connected to the controller, click **[Topology Consistency Verification]** on the upper right side of the **[Design Topology]** view to confirm whether the generated topology matches the planned topology. After verification, the controller can deploy configurations to the switches.

12.1.8.1.1 Push Basic Network Configuration

Click **[Configuration]** - **[Design Topology]** - **[Basic Network]** - **[Push Configuration]** to issue the basic configuration for all devices.

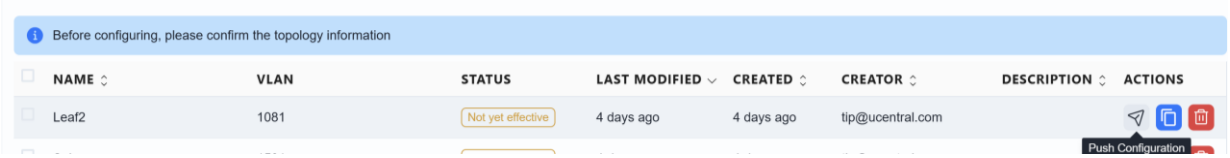


By default, the controller will select all switches. Click the **[Next]** - **[Start]** button to start issuing basic network configurations for the switches.

12.1.8.1.2 Push Switch Configuration

1. Switch Configuration

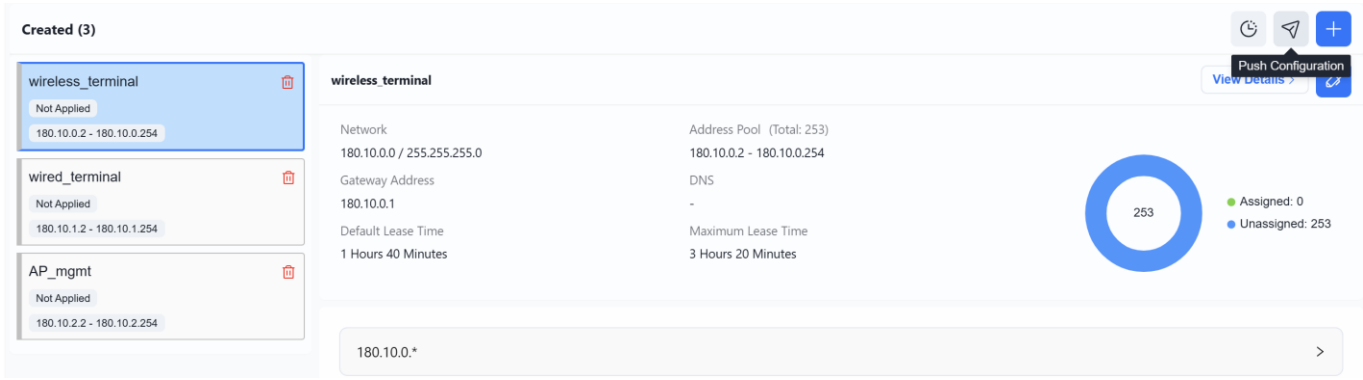
On the **[Configuration]**-**[Switch Configuration]** view, select the configuration to be deployed and click the **[Push Configuration]** button.



In the pop-up window, click **[Next]**-**[Start]** to deploy the switch configuration to the switch.

2. DHCP

On the **[Configuration] - [Switch Configuration] - [DHCP]** interface, select the configuration to be deployed and click the **[Push Configuration]** button to deliver the configuration.



12.1.8.2 AP

The AP does not need to manually issue the configuration. After the configuration of the device is issued and takes effect, the PoE power supply function of the switch is turned on, and the AP can power on and work. When the AP connects to the controller with the information obtained through the DHCP service, the controller will automatically send the configuration to the corresponding AP based on the comparison between the TAG identification stored in the AP inventory and the TAG identification in the planning configuration.

12.2 Traditional L2 Network

12.2.1 Scenario Overview

The traditional Layer 2 network solution is based on the classic Spine-Leaf architecture, enabling visualised, automated deployment and management through a centralised controller.This solution adheres to the design principles of network stratification and separation of responsibilities, providing a stable, efficient, and easily maintainable standardised foundational network platform for environments such as campuses and data centres. It combines a reliable architecture proven over decades with modern centralised management capabilities, ensuring non-blocking, low-latency forwarding of service traffic within Layer 2 domains while achieving centralised and highly available Layer 3 gateway functionality.

Centralised Policy Management and Automated Deployment

Through a unified controller, the solution abstracts complex VLAN, port, Spanning Tree, and gateway configurations into intuitive policy templates. Operations personnel can deploy configurations across the entire network in bulk and with precision via a graphical interface, eliminating the need for individual device logins. This fundamentally prevents misconfigurations and inconsistencies that may arise from manual command-line operations, reducing network deployment time from days to hours.

Intelligent Unified Operations Management and Proactive Insights

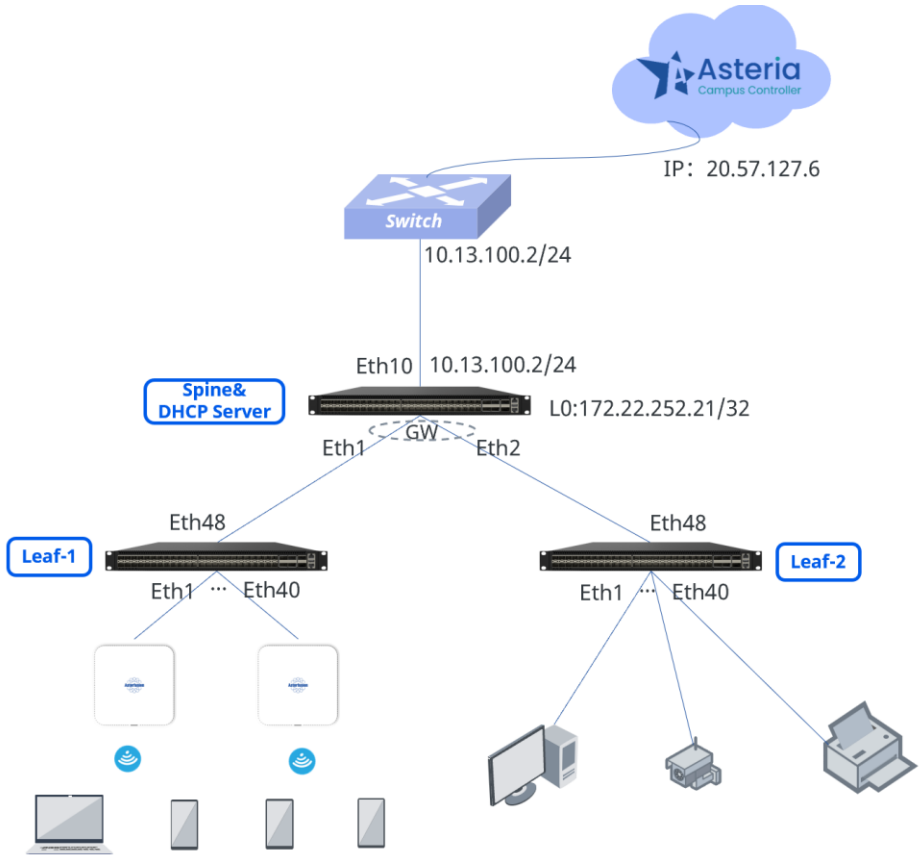
At the deployment and management level, this solution achieves centralised policy distribution and device management through a unified controller. Beyond this, the controller possesses robust real-time monitoring and intelligent analysis capabilities. It continuously collects operational status and performance metrics from all network devices, intelligently calculates health scores for each device based on multi-dimensional data, and provides comprehensive logging with precise real-time alerts. This mechanism significantly simplifies network operations, enabling administrators to proactively identify potential risks, rapidly pinpoint issues, and resolve them, thereby comprehensively enhancing

operational efficiency and network reliability.

Ultimate Reliability and High Performance in Classic Architecture

Employing a Spine-Leaf classic network topology, the Leaf layer functions as pure Layer 2 equipment, dedicated to high-speed access and local switching. The Spine layer acts as Layer 3 gateways and policy enforcement points, enabling centralised, efficient routing of cross-subnet traffic. This clear division of responsibilities renders network behaviour entirely predictable, providing upper-layer services with consistently low-latency, high-bandwidth stable connections.

12.2.2 Scheme Design



Network Architecture:

Traditional Layer 2 gateways are deployed on Spine devices, with Leaf devices operating purely as Layer 2 switches. This approach is suitable for wired networks in campus server zones or traditional access/aggregation networks in small-to-medium campuses. It provides classic Layer 2 forwarding to meet requirements for traditional Layer 2 architectures.

DHCP Deployment:

DHCP is centrally deployed on Spine devices.

Controller Deployment:

Controllers are deployed in the cloud, enabling unified management through a graphical interface. This facilitates centralised policy distribution, configuration management, and status monitoring, significantly enhancing operational efficiency. Particularly for device configuration and deployment, this approach substantially reduces workload.Service Planning:

Service Plan:

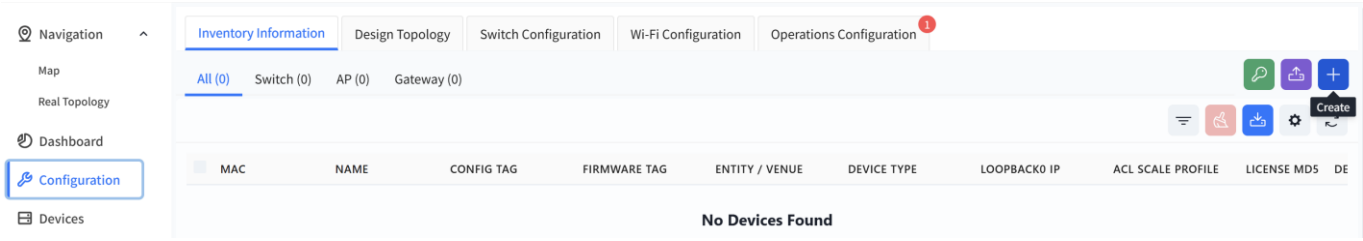
Service Type	IP Segment	Gateway	Service VLAN	SSID
Wireless Service	180.10.0.0/18	180.10.0.1/18	1080	New SSID
Wired Service& AP Management	180.10.18.0/24	180.10.18.1/24	1888	-

12.2.3 Device Import

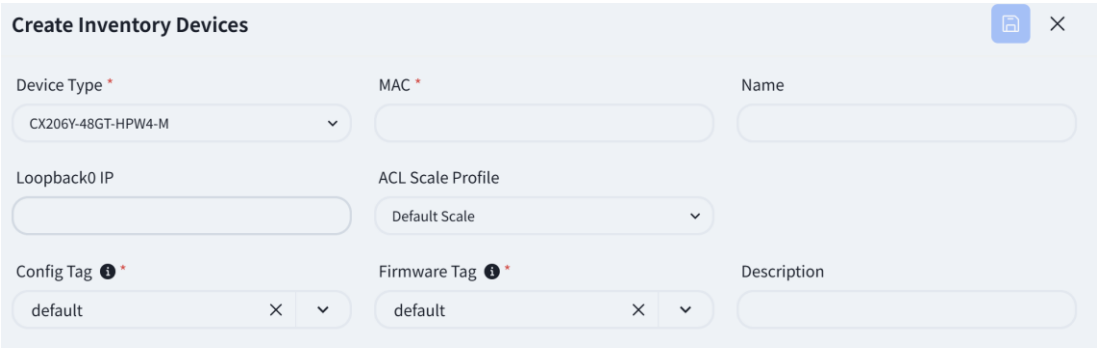
Administrators can create or import devices in bulk to specified sites/organizations. When an added inventory device connects to the controller and comes online, the controller will automatically assign it to the designated organization/site based on its MAC address.

3. Add devices one by one.

Click **[Configuration]** - **[Inventory Information]** - **[+]** to create an inventory device.

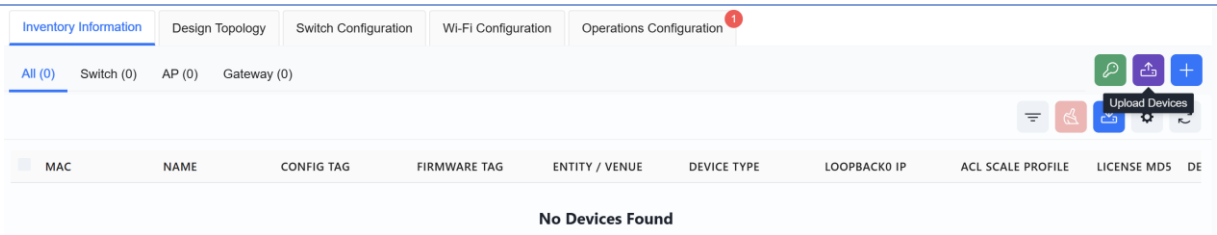


Fill in the relevant information as prompted on the page



4. Import via Excel

Click **[Upload Devices]**



Click **[Download Template]** and enter the information for the devices to be added to the inventory according to the template's specifications.

MAC	DeviceType	Name	ConfigTag	FirmwareTag	Loopback	AclScaleProfile	License	Description
60eb5a000001	CX308P-48Y-M	Spine						
60eb5a000002	CX206Y-48GT-HPW4-M	Leaf-1						
60eb5a000003	CX206Y-48GT-M	Leaf-2						
60eb5a000004	CAP7030-Z			default				
60eb5a000005	CAP7030-Z			default				
60eb5a000006	CAP7030-Z			default				
60eb5a000007	CAP7030-Z			default				
60eb5a000008	CAP7030-Z			default				
60eb5a000009	CAP7030-Z			default				
60eb5a000010	CAP7030-Z			default				
60eb5a000011	CAP7030-Z			default				
60eb5a000012	CAP7030-Z			default				
60eb5a000013	CAP7030-Z			default				
60eb5a000014	CAP7030-Z			default				

MAC: The device's MAC address. This information is typically found on the device's label.

Device Type: The device model.

Name: The device hostname. By default, it is the device's MAC address.

ConfigTag: After an AP connects to the controller, it will automatically pull the configuration file corresponding to this tag. By default, the tag value is default.

FirmwareTag: When performing firmware upgrades, devices requiring an upgrade can be filtered based on their firmware tag type. By default, the tag value is default.

Loopback: The device's loopback address. For all devices operating at Layer 3, this address serves as the device's in-band management address.

AclScaleProfile: Optional values are default or large-scale. By default, the value is default.

License: The AP's license file. For bulk imports, you can either enter the JSON-formatted license file

content directly in the Excel sheet, or add all devices to inventory first and then import the license files in bulk afterward.

Description: Descriptive information about the device.

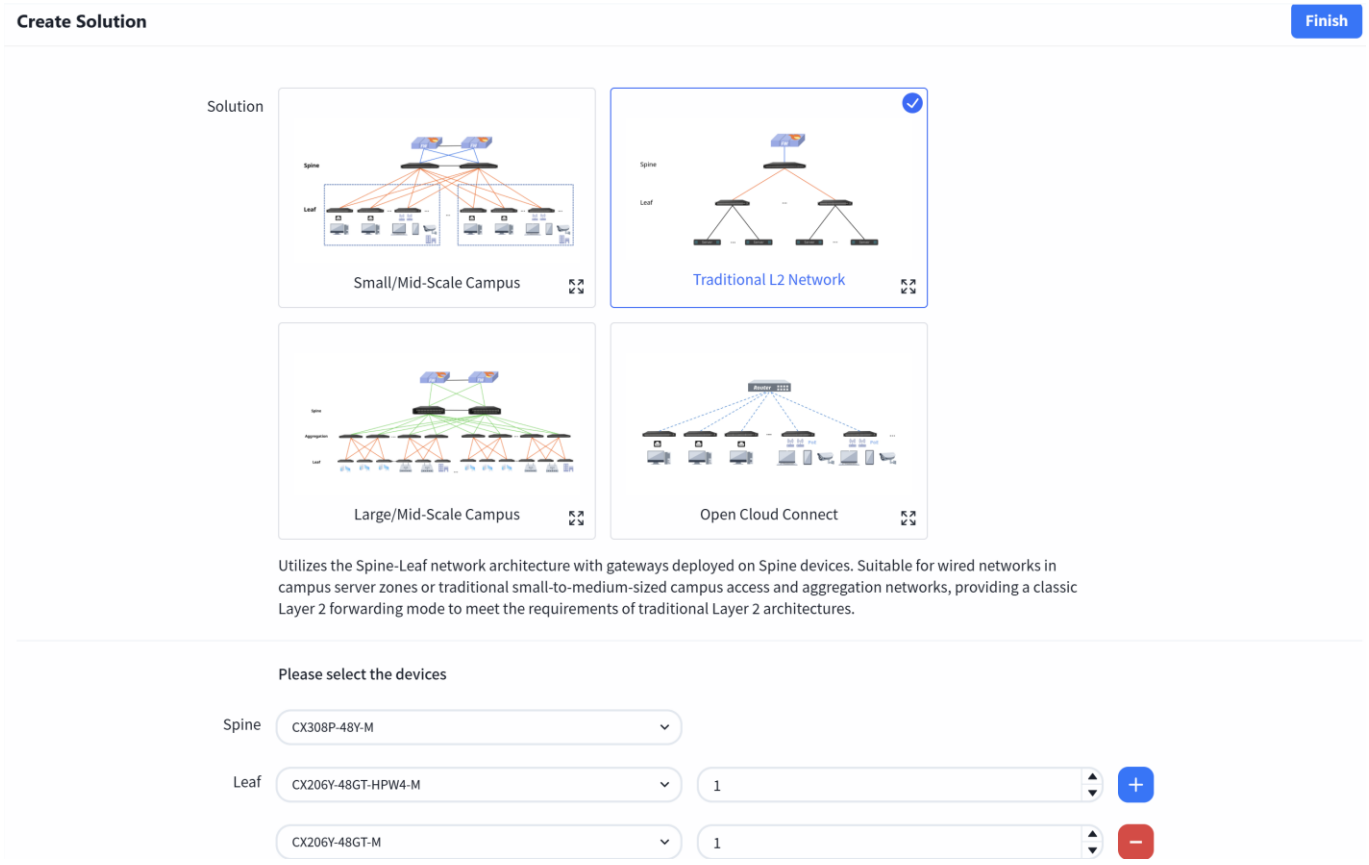
Click **[Choose File]** to upload the completed template, then click **[Test Upload Data]**. The controller will automatically check if the uploaded data complies with the specifications and display the results in the test report.

Once completed, users can view the created devices in the **[Inventory Information]** view.

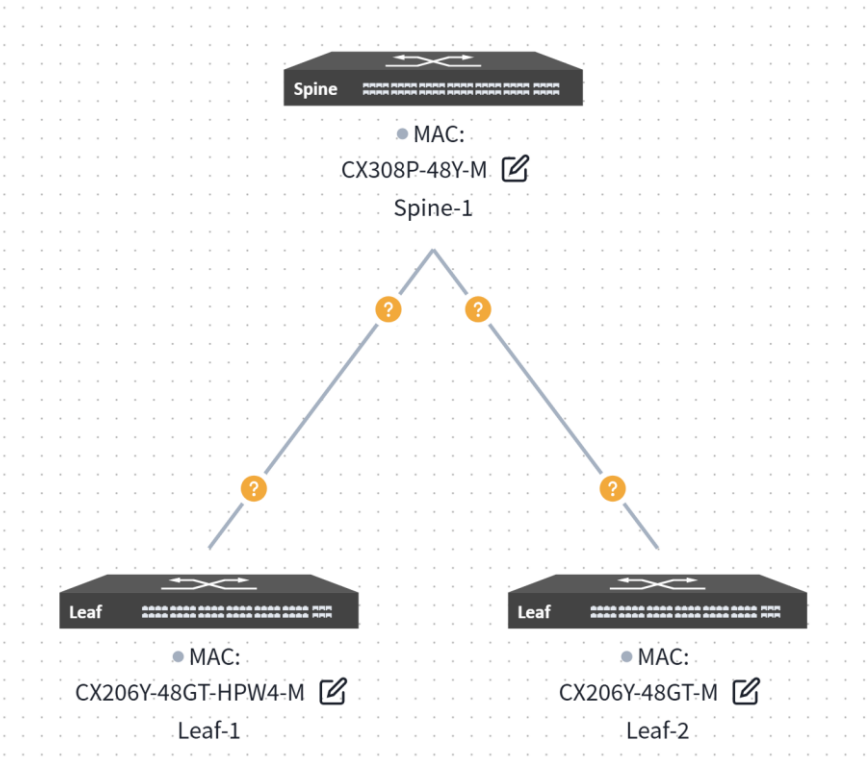
12.2.4 Service Configuration

12.2.4.1 Design Topology

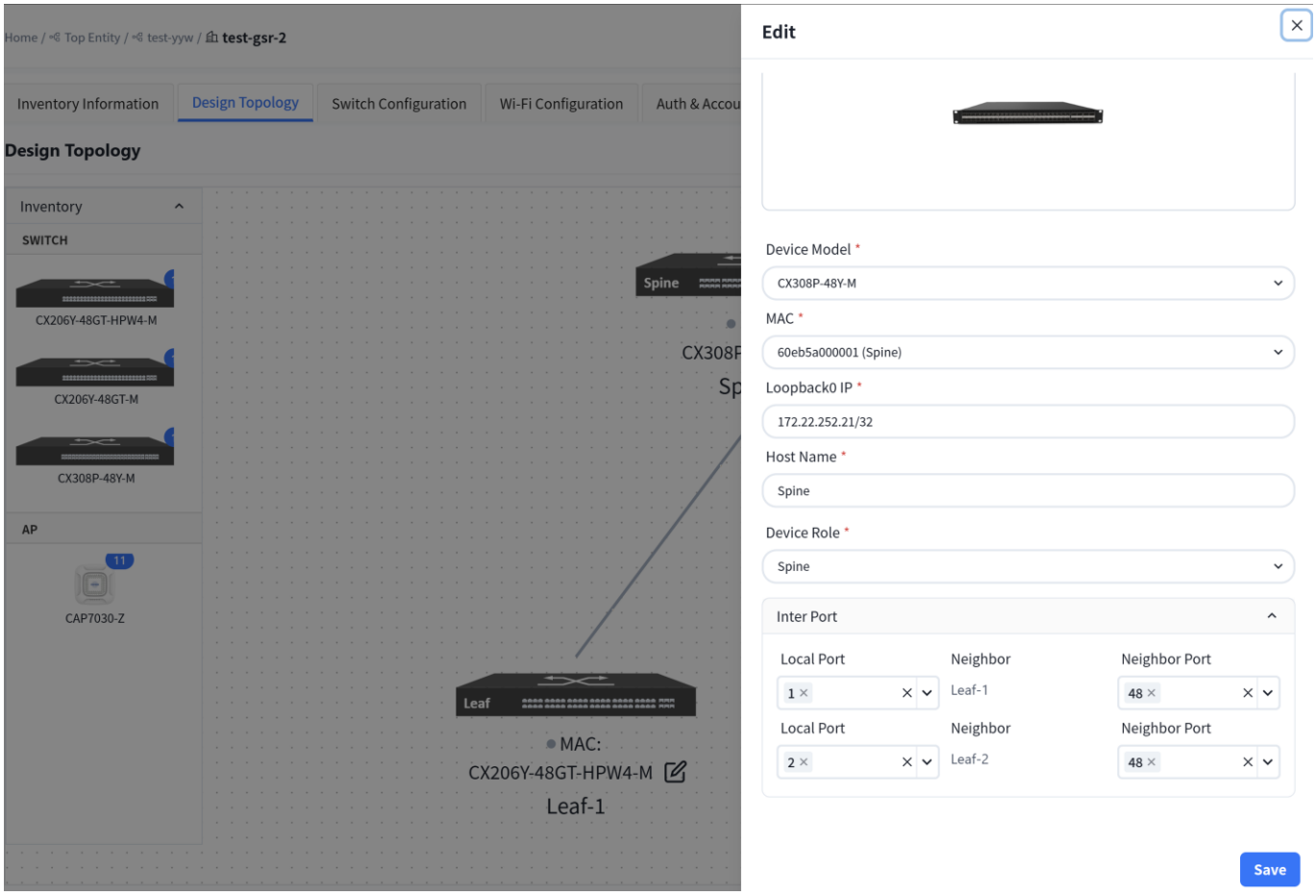
Navigate to the **[Configuration]** page in the controller's navigation bar. Click **[Plan Topology]**, select the **[Traditional L2 network]**, enter the model and quantity of Spine and Leaf devices, then click **[Finish]** to finalise the network topology pre-planning. The controller will generate a recommended network topology based on pre-planned typical network topologies.



The generated topology is displayed as follows:



Users may click the **[Edit]** button on the device side, select the device from inventory to apply to the current topology in the right-hand slide-out panel, then choose the interconnect interface.



MAC: Uniquely select a device via its MAC address.

Loopback0 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.

Inter Port:

Local Port: The interface on the current device.

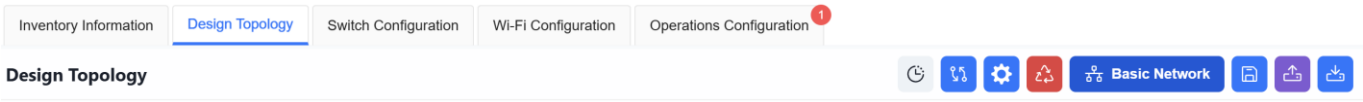
Neighbor: Select the peer device connected to the local interface.

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

Upon completing all configurations, click **[Save]** in the upper right corner of the page, then select **[Confirm]** in the pop-up window.

12.2.4.2 Basic Network

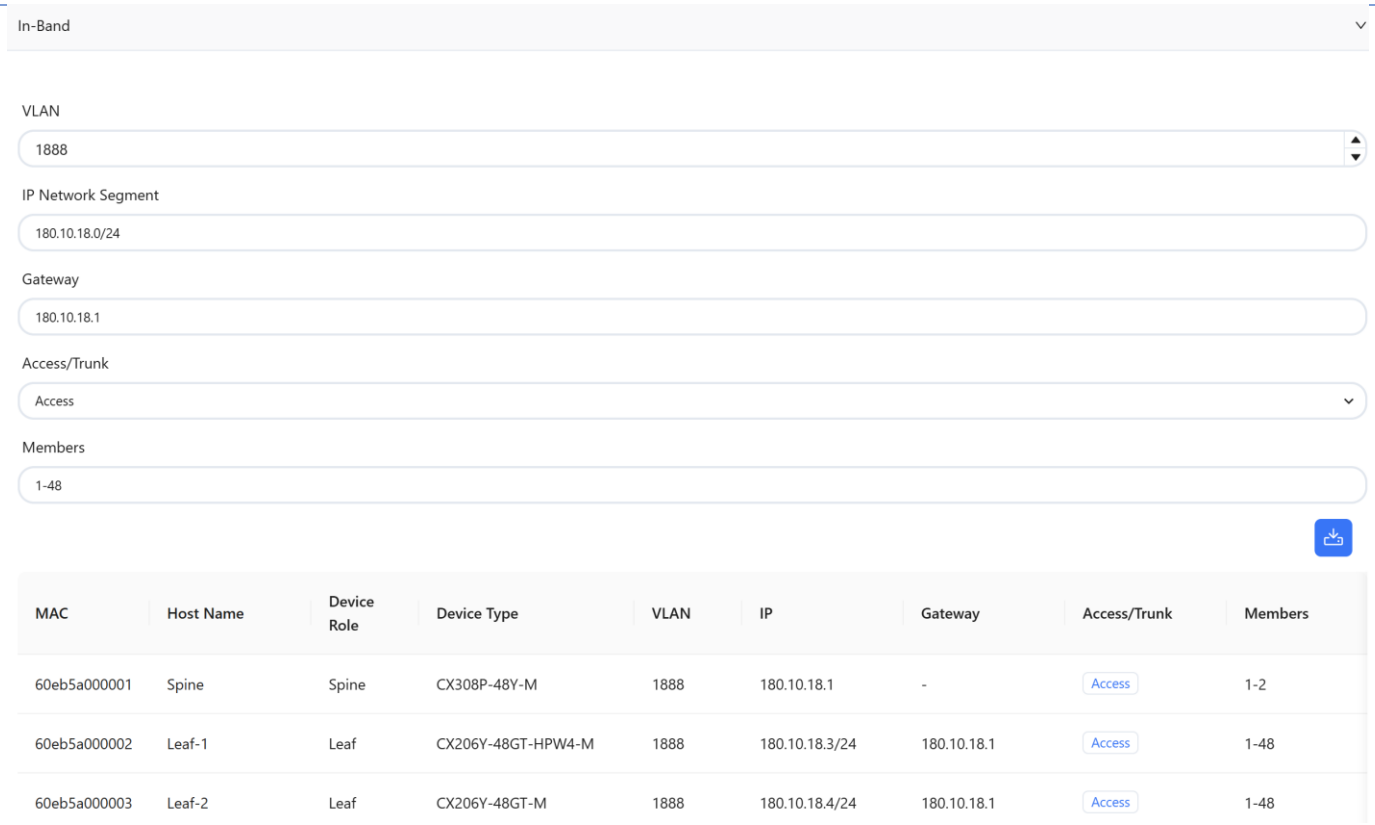
Click the top right corner **[Basic Network]**



12.2.4.2.1 Basic

In traditional Layer 2 network scenarios, the in-band management method for Leaf devices involves creating a VLANif interface as the in-band management interface to connect to the controller. On this page, administrators can specify a VLAN ID as the in-band management VLAN, configure the management IP address range and the in-band management gateway address (which will be configured on the Spine device), select the VLAN member interfaces, and set the mode to access when joining the VLAN.

The controller will allocate a management IP address to each Leaf switch from the specified address range, displaying the allocation results in the table below:



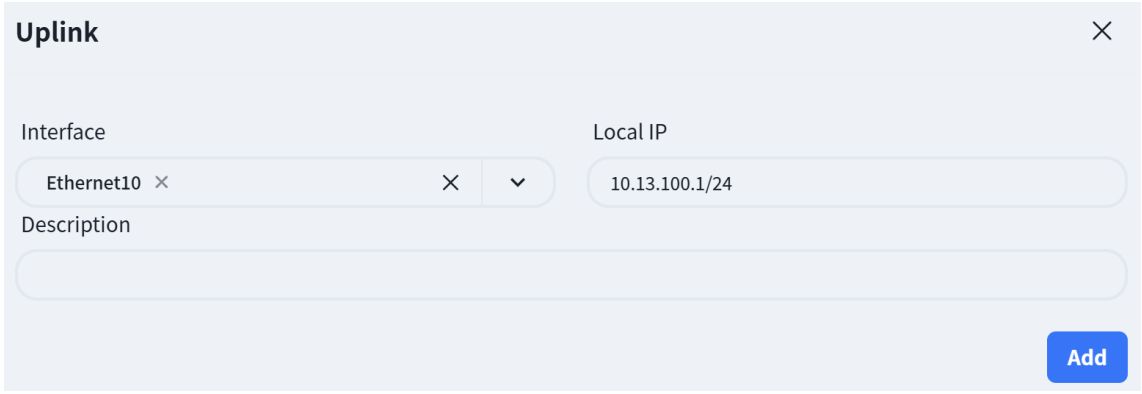
Access/Trunk: Select this mode based on whether the interface transmits and receives VLAN-tagged packets.

- Access: Accepts packets without VLAN tags. Typically configured as the management VLAN for switches or APs, or as a wired service VLAN.
- Trunk: Accepts VLAN-tagged packets, typically configured for wireless service VLANs.

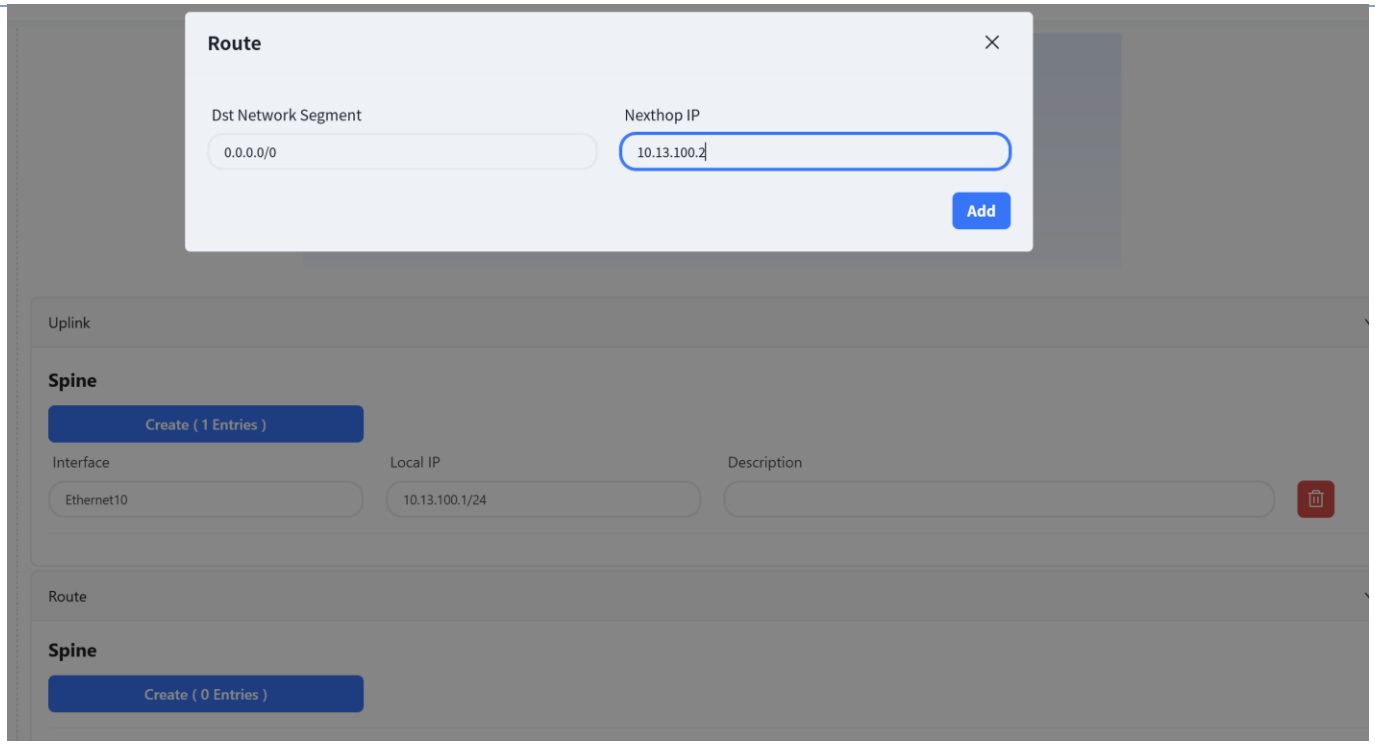
Note: As a switch interface can only be configured with one Access mode VLAN, this in-band management VLAN also serves as both the wired service VLAN and AP management VLAN.

12.2.4.2.2 Egress Router

Select the interface ID for the uplink interface on the Spine device and configure its IP address.



In traditional Layer 2 scenarios, the Spine only supports connecting to external networks via static route configuration. To ensure normal network operation, a default route is typically required.



12.2.4.2.3 Device

Configure device management related information:

TimeZone: Configure the system time zone.

NTP: Configure NTP Server.

SNMP: Configure SNMP community.

Syslog: Configure syslog server IP address.

TACACS+: Configure TACACS server IP address.

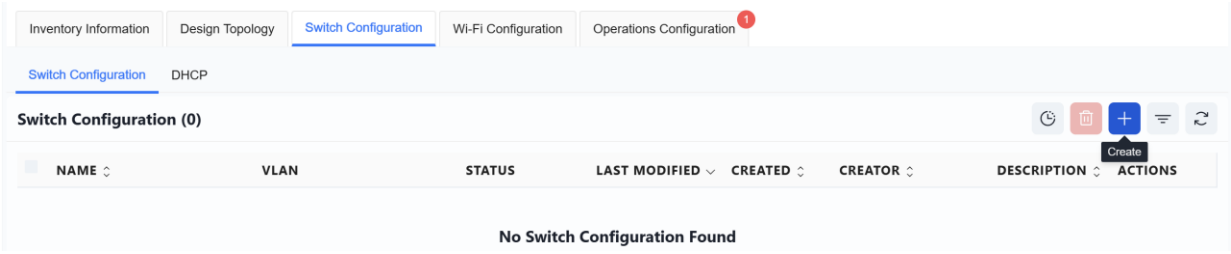
Device ACL: Configure ACL rules restricting SSH, SNMP, TELNET connections to device.

After completing all configurations, click **[Save]**

12.2.4.3 Switch Configuration

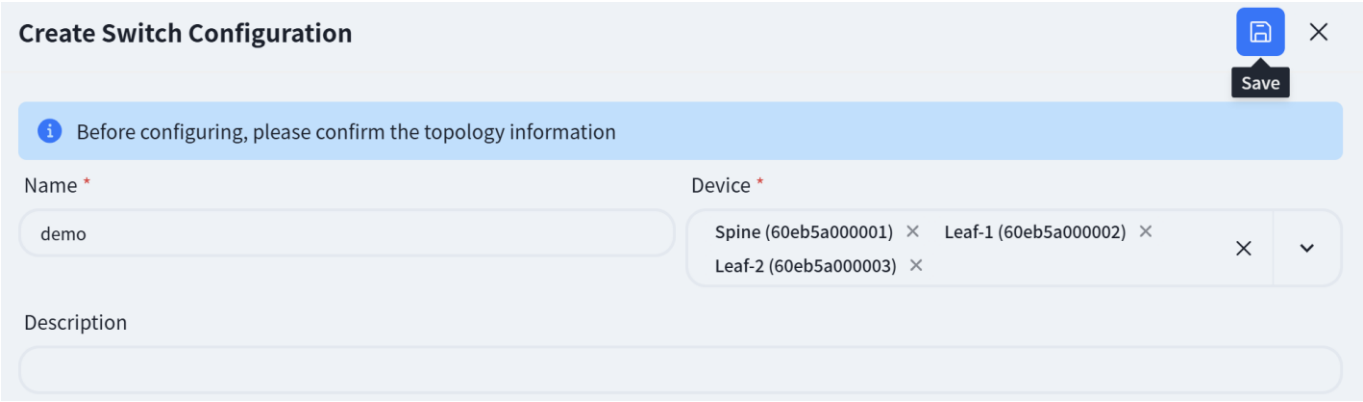
12.2.4.3.1 Switch Configuration

Click **[Create]** on the right to set up the switch configuration.



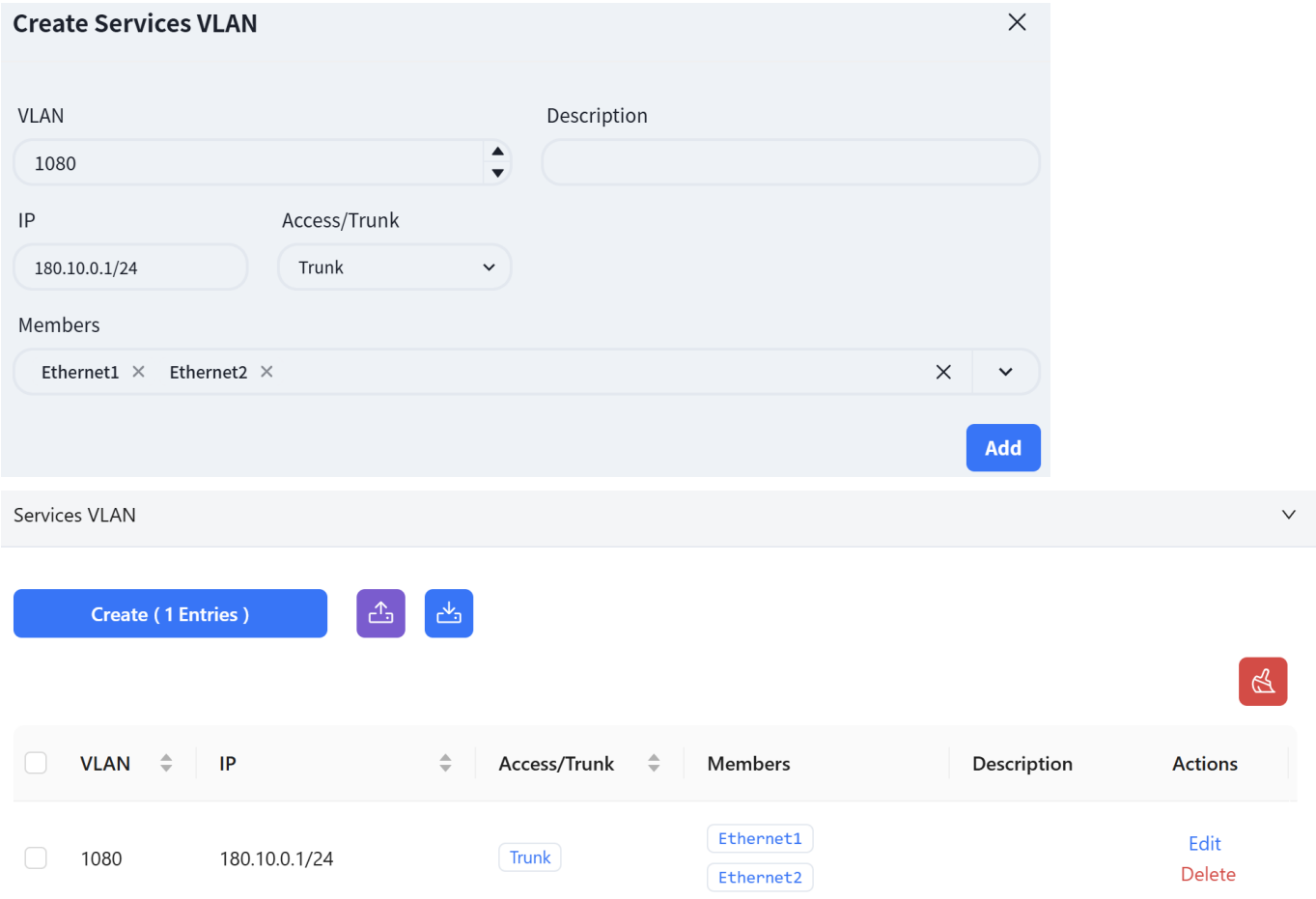
Unlike full three-layer networks, in traditional two-layer networks, the service network is deployed on

Spine devices. Therefore, when selecting devices, it is also necessary to add devices of the Spine type.



1. Spine

Creating a Service VLAN:



VLAN: Create a service VLAN

IP: Configure the address as the gateway for this service VLAN

Access/Trunk: Select this mode based on whether the interface transmits or receives VLAN-tagged packets

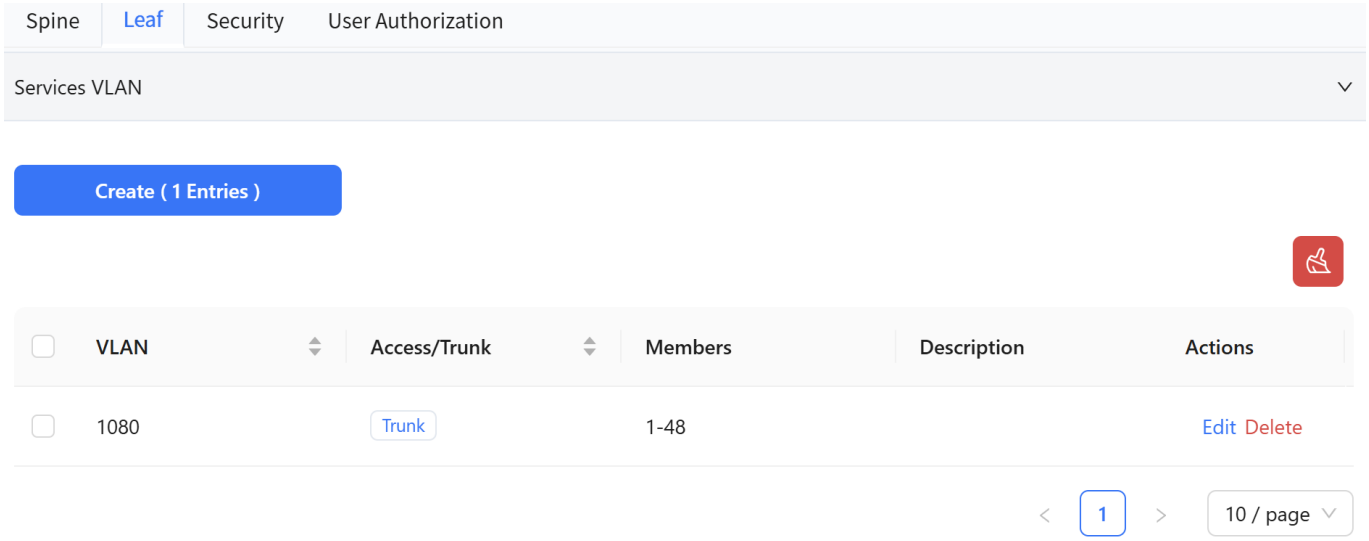
- Access: Accepts packets without VLAN tags, typically configured for AP management VLANs or wired service VLANs

- Trunk: Accepts VLAN-tagged packets, typically configured for wireless service VLANs

Members: Click the dropdown arrow and select the member interfaces for the VLAN on the Spine device. Typically, this includes all interfaces connected to Leaf switches.

2. Leaf

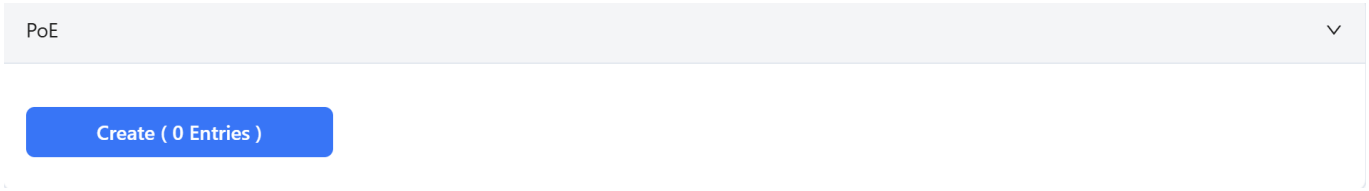
Leaf switches operate in pure Layer 2 configuration. On this interface, only the VLAN ID and member interfaces need to be specified; all other configurations are generated by the controller.



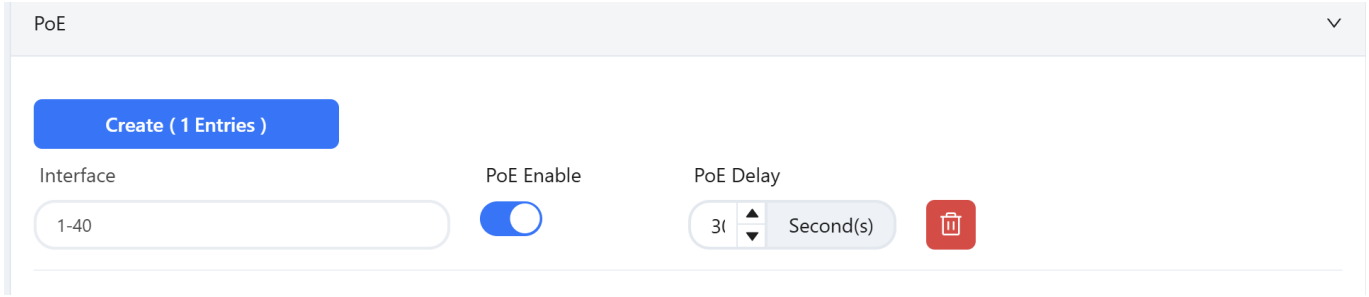
POE

The access switch features PoE functionality, which can be directly enabled in the wired service configuration to supply power to PD devices.

Click **[Create]**



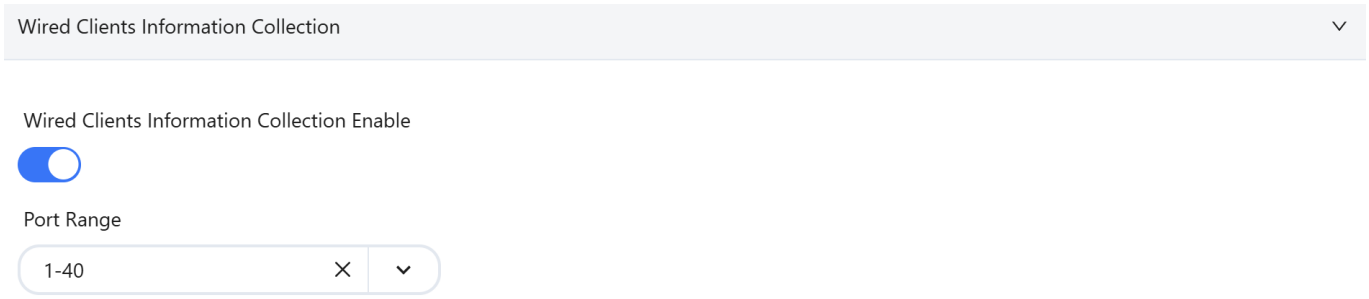
Select the interface where the PoE function is to be enabled and set the startup delay time.



POE Delay: This refers to a brief, intentional time delay introduced at a PoE switch port between when it begins to supply power and when it actually delivers power to the Powered Device (PD).

Wired Clients Information Collection

Interfaces with this feature enabled will report information about the connected wired terminals to the controller.

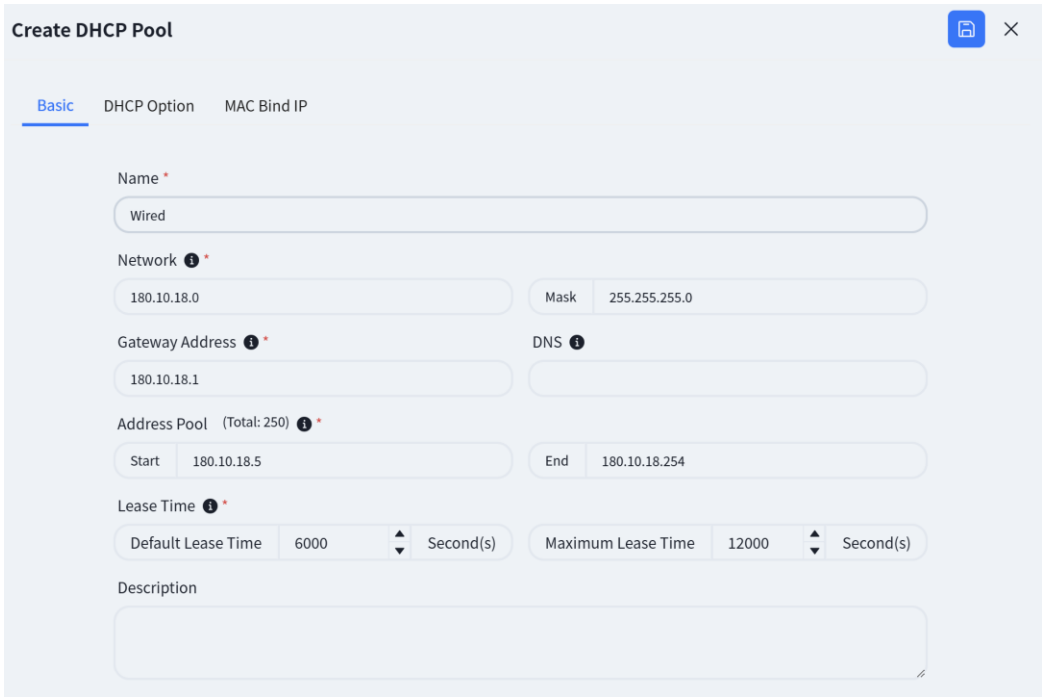


12.2.4.3.2 DHCP

The controller allows users to configure the DHCP Server function on Spine devices.

After entering the site, click **[Configuration]** - **[Switch Configuration]** - **[DHCP]** to access the DHCP Server configuration interface. Then, click the **[+]** button on the page to create a new configuration:

1. Create Wired Services and AP Management Address Pool



Name: User defined.

Network: Specify the network segment where the IP address assigned by the DHCP server to the DHCP client is located.

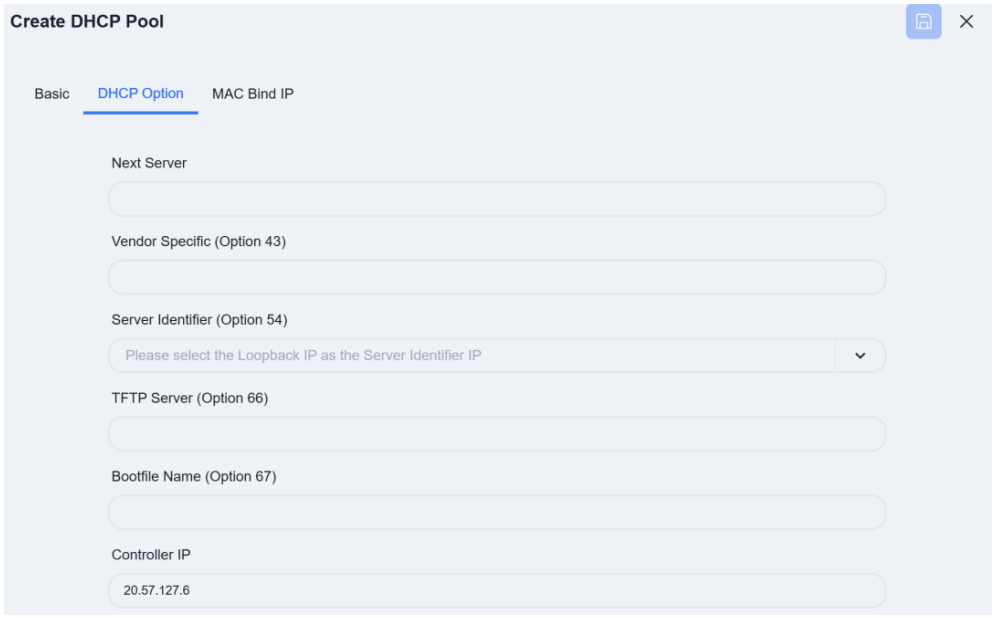
Gateway Address: Specify the gateway address assigned by the DHCP server to the DHCP client.

DNS: Specify the DNS server address.

Address Pool: Specify the address range allocated by the DHCP server to DHCP clients.

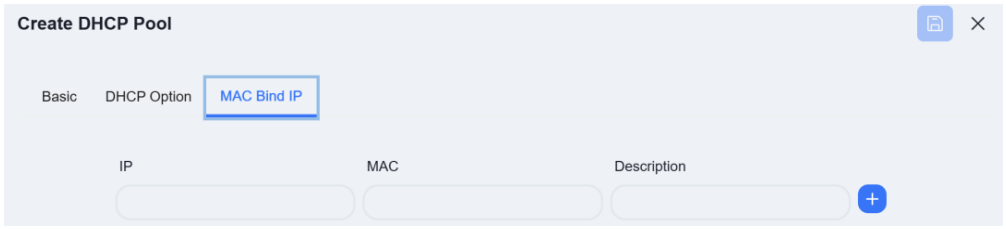
Lease Time: Specify the IP address lease time.

Click on **[DHCP Option]**and fill in the relevant information.

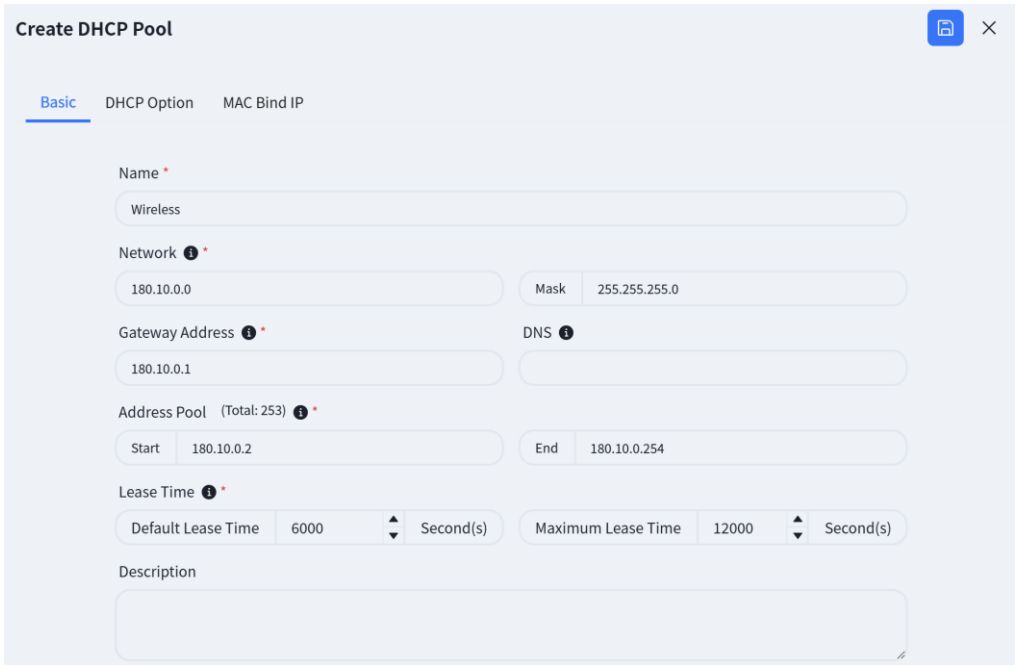


Controller IP: DHCP options specifically designed for wireless AP discovery controllers, fill in the controller IP address.

The controller supports configuring MAC binding IP function, which users can fill in as needed.



2. Create Wireless Services Address Pool

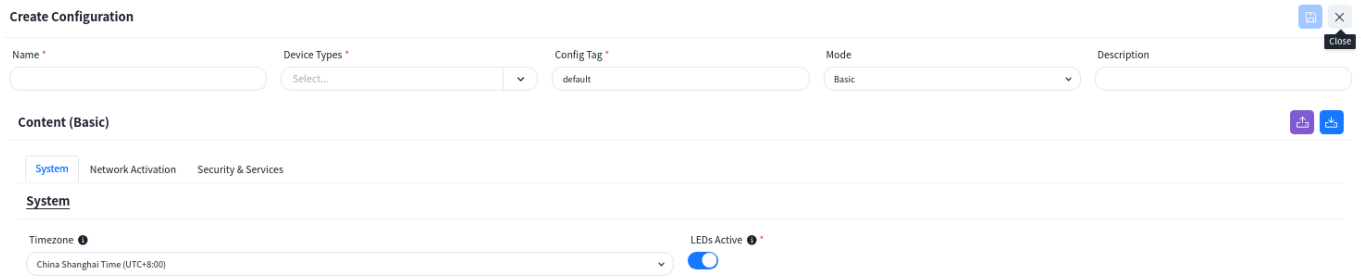


After completing all configurations, click **[Save]**

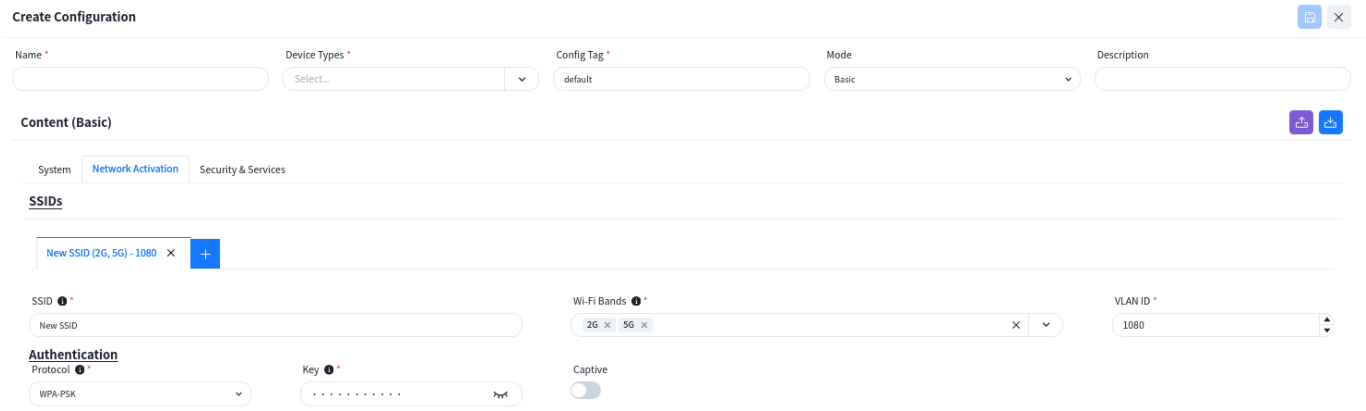
12.2.4.4 Wi-Fi Configuration

Click **[Wi-Fi Configuration] - [+]** to configure the necessary basic information for the wireless AP, e.g. SSID settings, security policy. The controller can automatically generate the corresponding

The controller supports the configuration of different wireless service configurations, and after the AP goes online, it will determine which configuration should be issued to the AP based on the **[Config Tag]** attributes of the configuration.

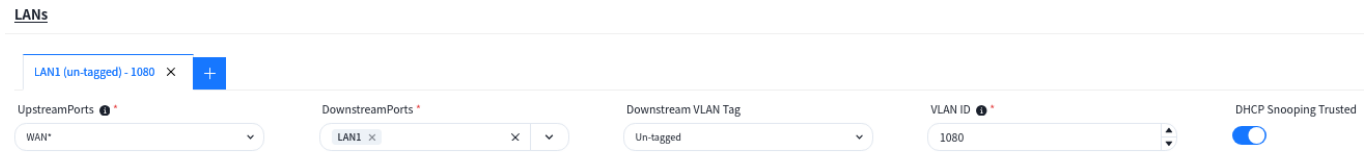


12.2.4.4.1 SSID



12.2.4.4.2 LAN(Optional)

When the AP is one that has an extended wired interface and is capable of accessing terminals by wired means, such as a panel AP, the user can configure the access method for wired terminals through the configuration in LANs.



UpstreamPorts: Specify the up-link interfaces for wired terminal to access the network through AP, usually it is the interface for AP to connect to the switch, and keep the same with **[UpstreamPorts]** in **[SSID]** – **[Advanced]** Settings, the default is: WAN*.

DownstreamPorts: Interfaces for wired terminal access.

Downstream VLAN Tag: Whether the wired terminal carries VLAN Tag.

VLAN ID: The AP receives messages from wired terminals that add this VLAN TAG to identify.

DHCP Snooping Trusted: DHCP Snooping Trusted interface, if the wired terminal needs to obtain IP address through DHCP service, this switch needs to be on.

12.2.5 Configuration Release

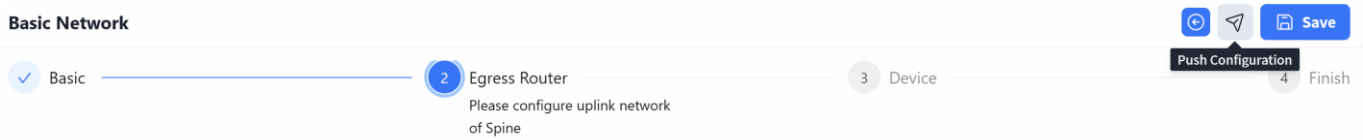
12.2.5.1 Switch

Switches support both in-band and out-of-band management methods. Operation and maintenance personnel can flexibly choose based on current network conditions. For devices in the factory default state, whenever either the management port or service port is in an "Up" state, they will actively initiate a DHCP request to obtain a temporary management IP address and the IP address of the cloud-based controller from the DHCP server. They will then connect to the controller to retrieve configuration information.

Once all switches are successfully connected to the controller, click **[Topology Consistency Verification]** on the upper right side of the **[Design Topology]** view to confirm whether the generated topology matches the planned topology. After verification, the controller can deploy configurations to the switches.

12.2.5.1.1 Push Basic Network Configuration

Click **[Configuration]** - **[Design Topology]** - **[Basic Network]** - **[Push Configuration]** to issue the basic configuration for all devices.

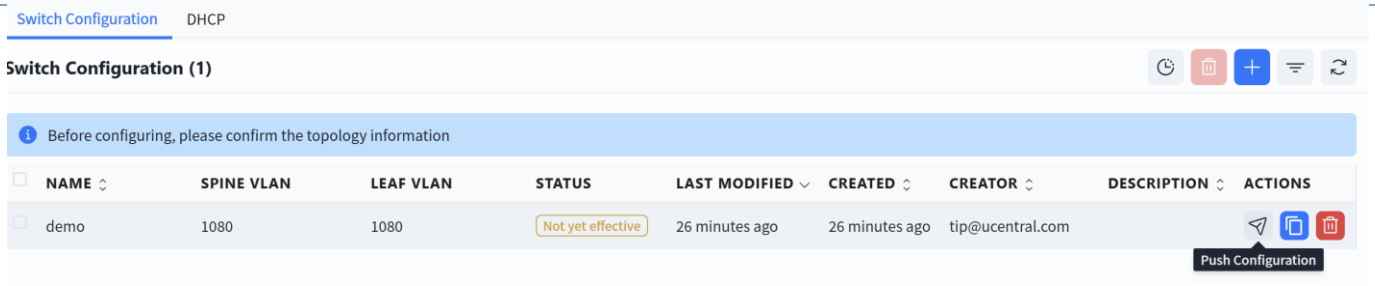


By default, the controller will select all switches. Click the **[Next]** - **[Start]** button to start issuing basic network configurations for the switches.

12.2.5.1.2 Push Switch Configuration

1. Switch Configuration

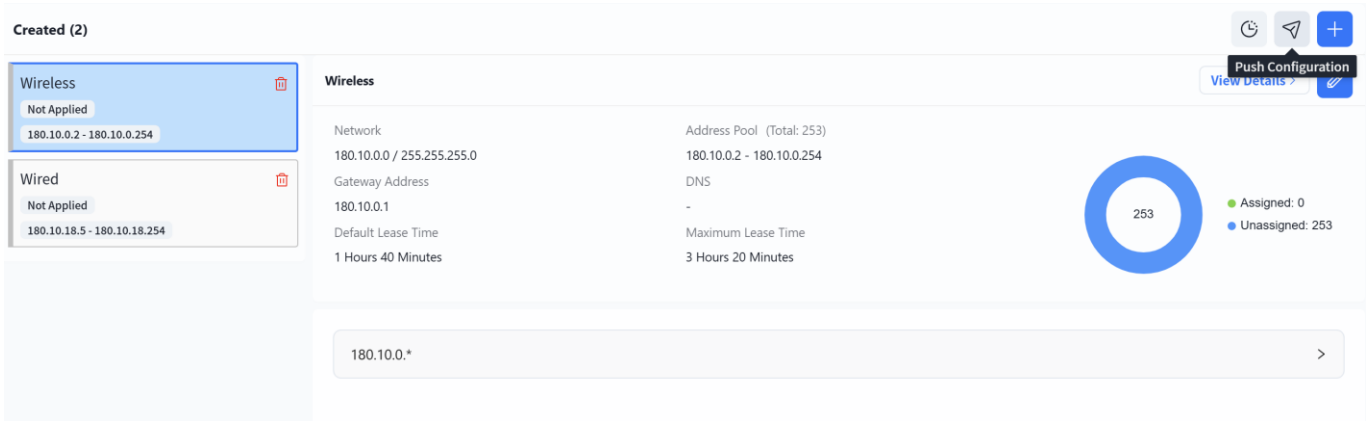
On the **[Configuration]**-**[Switch Configuration]** view, select the configuration to be deployed and click the **[Push Configuration]** button.



In the pop-up window, click **[Next]**-**[Start]** to deploy the switch configuration to the switch.

2. DHCP

On the **[Configuration] - [Switch Configuration] - [DHCP]** interface, select the configuration to be deployed and click the **[Push Configuration]** button to deliver the configuration.



12.2.5.2 AP

The AP does not need to manually issue the configuration. After the configuration of the device is issued and takes effect, the PoE power supply function of the switch is turned on, and the AP can power on and work. When the AP connects to the controller with the information obtained through the DHCP service, the controller will automatically send the configuration to the corresponding AP based on the comparison between the TAG identification stored in the AP inventory and the TAG identification in the planning configuration.

12.3 Large/Mid-Scale Campus

12.3.1 Scenario Overview

This solution is designed for medium to large-scale campus networks, adopting a Spine-Aggregation-Leaf fully layered three-tier network architecture. It leverages a controller for automated management and intelligent operations. The network is divided into a default access zone and a server zone, utilizing key technologies such as distributed gateways and MC-LAG to provide high-performance and highly

reliable network connectivity for large-scale terminal access and high-availability server clusters.

Centrally Intelligent Management Core

The controller automatically translates business intents into device configurations through a graphical interface and deploys them accurately, completely eliminating the traditional tedious process of configuring devices one by one via command-line interface. It offers full lifecycle management, including device onboarding, monitoring, and diagnostics, enabling network automation and high reliability.

Elastic and Reliable Network Backbone

Ultimate Scalability: Horizontal expansion at the aggregation layer supports the integration of large-scale Leaf switches, effortlessly accommodating future network growth.

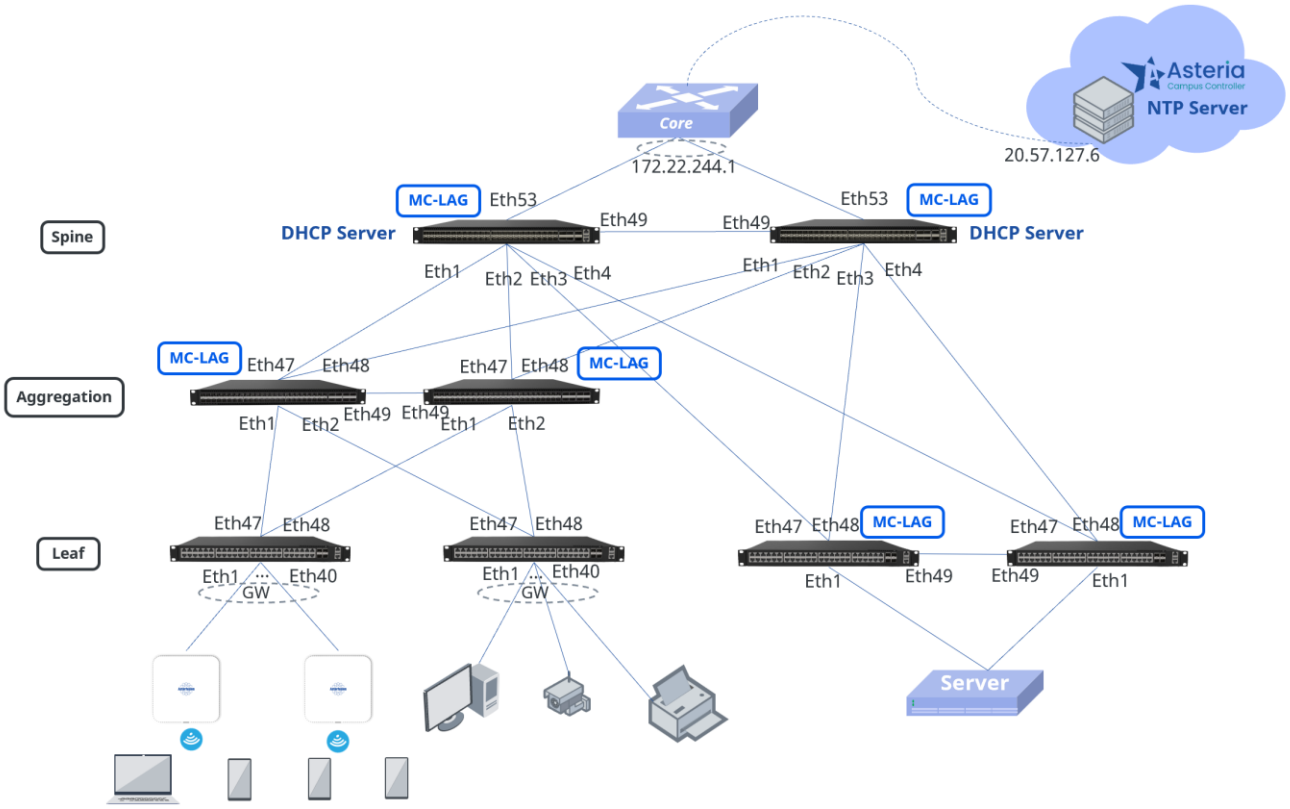
Flexible Gateway Deployment: Distributed service gateways can be deployed at the Leaf layer, confining service traffic to the access layer. This significantly enhances forwarding efficiency and network reliability while effectively reducing the burden on upper-layer devices.

Scenario-Optimized Access Technologies

Leaf Distributed Gateways: Serve wired and wireless terminals in the default access zone. By 下沉 gateways to the access Leaf, cross-subnet communication for terminals no longer needs to traverse the core layer, significantly reducing latency and enabling fault domain isolation.

Leaf MC-LAG: Provides high-availability Layer 2 access for the server zone. Two Leaf switches are virtualized into a single logical device via MC-LAG to connect with servers, achieving link-level and device-level load balancing and seamless failover. This eliminates loops while ensuring uninterrupted continuity for critical business operations..

12.3.2 Scheme Design



This medium to large-scale campus employs a full three-tier Spine-Aggregation-Leaf network architecture, divided into a default access zone and a server zone.

Default Access Zone:

Leaf1 and Leaf2 function as distributed gateways, with Leaf1 dedicated to connecting APs and wireless terminals, and Leaf2 managing wired terminals. Horizontal scaling at the aggregation layer (Agg1, Agg2) ensures high availability and load balancing. MC-LAG operates between the Spine and aggregation devices to guarantee link reliability.

Server Zone:

Leaf3 and Leaf4 connect to servers in pure Layer 2 mode via MC-LAG technology, with gateways centrally deployed on the Spine devices. This simplifies network management in the server zone and enhances forwarding efficiency.

Management Network:

Spine devices and Leaf devices (Leaf1, Leaf2) in the default service zone are Layer 3 devices, using Loopback addresses as their in-band management addresses.

Aggregation layer devices and Leaf devices (Leaf3, Leaf4) in the server zone are Layer 2 devices. In-band management addresses are assigned to each Layer 2 device from the address range provided in the basic network configuration, with all gateways deployed on Spine1.

DHCP Deployment:

DHCP Servers are deployed on both Spine devices and are automatically configured as a DHCP Failover pair via the controller, ensuring high availability of address services.

Controller Deployment:

The controller is cloud-based and enables centralized policy deployment, configuration management, and status monitoring for all network devices through a graphical interface, significantly improving operational efficiency.

Foundation Link Data Planning

Device	Interface	IP Address
Spine1	Ethernet53	172.22.244.10/24
	Loopback0	172.22.252.51/32
Spine2	Ethernet53	172.22.244.11/24
	Loopback0	172.22.252.52/32
Leaf1	Loopback0	172.22.252.53/32
Leaf2	Loopback0	172.22.252.54/32

Service Network Data Planning

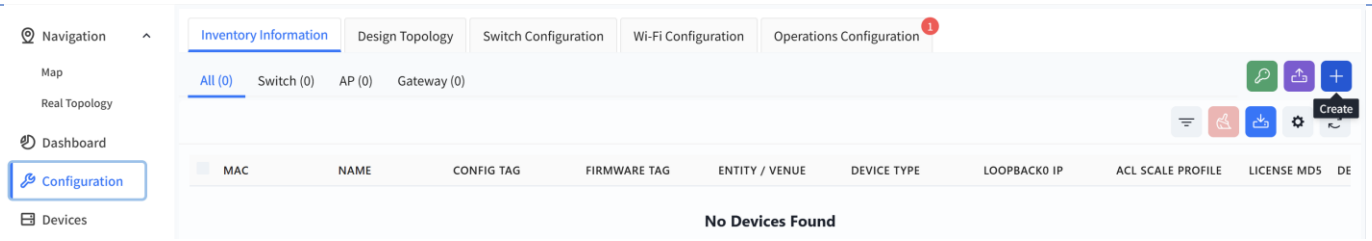
Service Type	IP Segment	Gateway	Service VLAN	SSID
Wireless Service	180.10.0.0/24	180.10.0.1/24	1080	New SSID
Wired Service	180.10.1.0/24	180.10.1.1/24	1081	
AP Management	180.10.2.0/24	180.10.2.1/24	1082	
Server Zone Service	180.10.15.0/24	180.10.15.1/24	1501	
Agg Management	172.22.200.0/24	172.22.200.1/24		
Server Zone Leaf Management	172.22.201.0/24	172.22.201.1/24		

12.3.3 Device Import

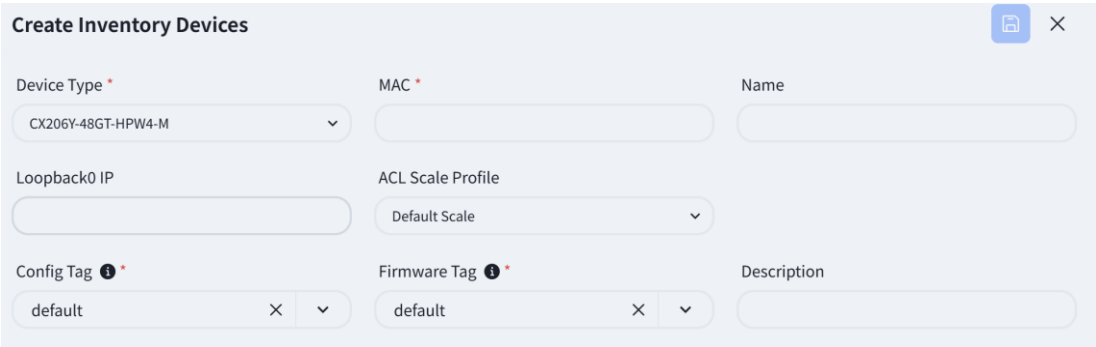
Administrators can create or import devices in bulk to specified sites/organizations. When an added inventory device connects to the controller and comes online, the controller will automatically assign it to the designated organization/site based on its MAC address.

1. Add devices one by one.

Click **[Configuration]** - **[Inventory Information]** - **[+]** to create an inventory device.

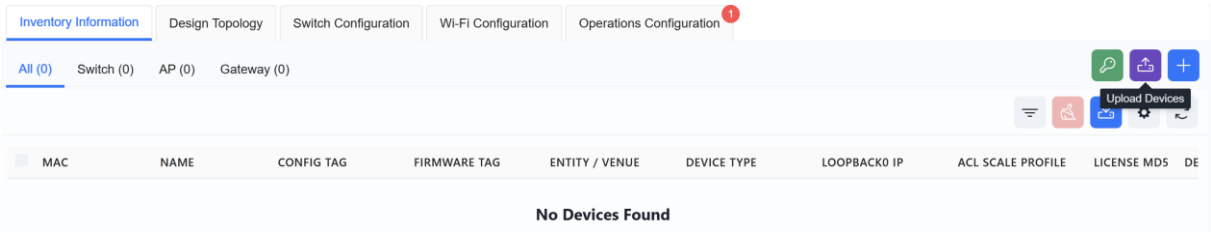


Fill in the relevant information as prompted on the page



2. Import via Excel

Click **[Upload Devices]**



Click **[Download Template]** and enter the information for the devices to be added to the inventory according to the template's specifications.

MAC	DeviceType	Name	ConfigTag	FirmwareTag	Loopback	AclScaleProfile	License	Description
60eb5a010001	CX308P-48Y-M	Spine1						
60eb5a010002	CX308P-48Y-M	Spine2						
60eb5a010003	CX308P-48Y-M	Agg1						
60eb5a010004	CX308P-48Y-M	Agg2						
60eb5a010005	CX206Y-48GT-HPW4-M	Leaf1						
60eb5a010006	CX206Y-48GT-M	Leaf2						
60eb5a010007	CX206Y-48GT-M	Leaf3						
60eb5a010008	CX206Y-48GT-M	Leaf4						
60eb5a010009	CAP7030-Z			default				
60eb5a010010	CAP7030-Z			default				
60eb5a010011	CAP7030-Z			default				
60eb5a010012	CAP7030-Z			default				
60eb5a010013	CAP7030-Z			default				
60eb5a010014	CAP7030-Z			default				
60eb5a010015	CAP7030-Z			default				

MAC: The device's MAC address. This information is typically found on the device's label.

Device Type: The device model.

Name: The device hostname. By default, it is the device's MAC address.

ConfigTag: After an AP connects to the controller, it will automatically pull the configuration file corresponding to this tag. By default, the tag value is default.

FirmwareTag: When performing firmware upgrades, devices requiring an upgrade can be filtered based on their firmware tag type. By default, the tag value is default.

Loopback: The device's loopback address. For all devices operating at Layer 3, this address serves as the device's in-band management address.

AclScaleProfile: Optional values are default or large-scale. By default, the value is default.

License: The AP's license file. For bulk imports, you can either enter the JSON-formatted license file content directly in the Excel sheet, or add all devices to inventory first and then import the license files in bulk afterward.

Description: Descriptive information about the device.

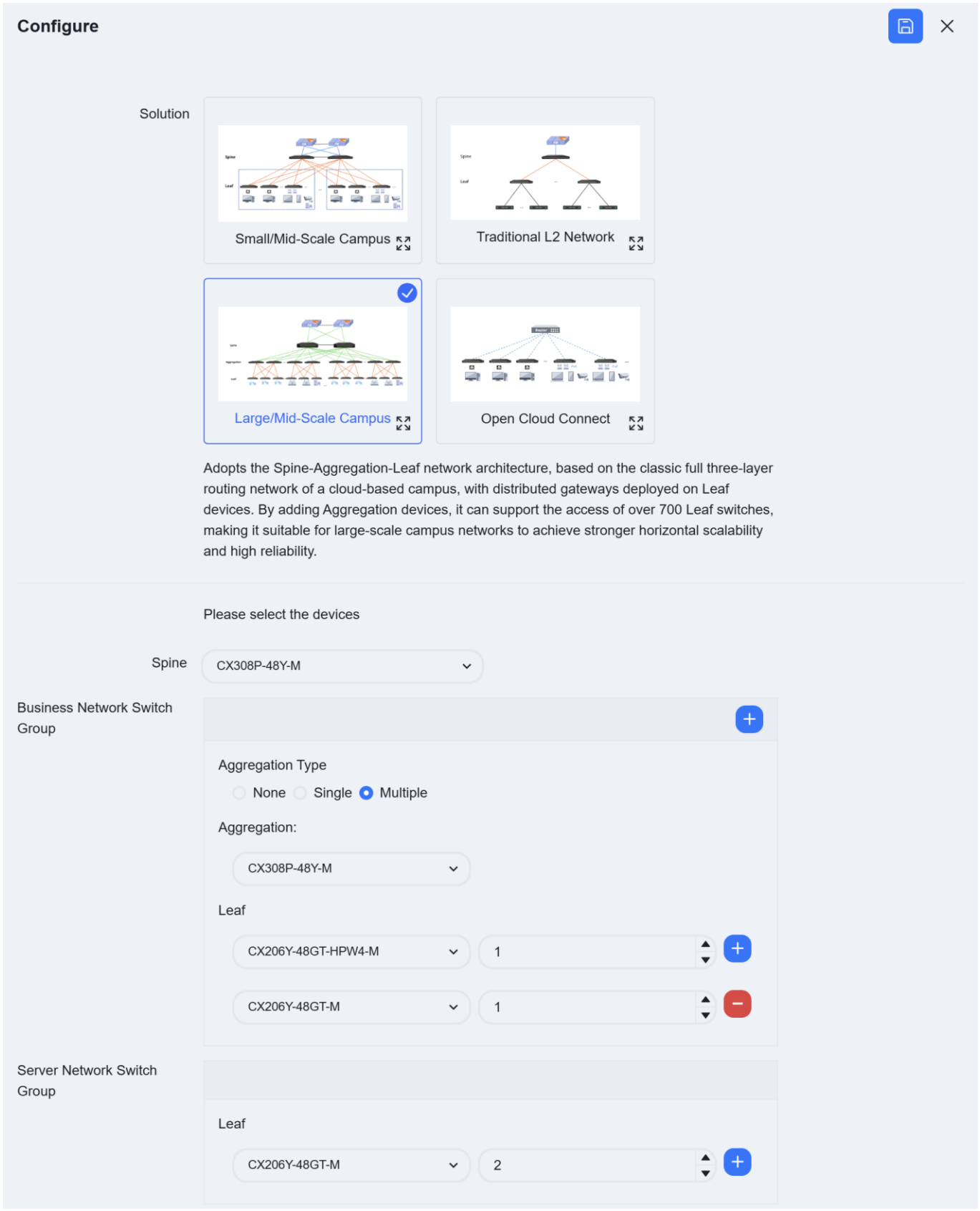
Click **[Choose File]** to upload the completed template, then click **[Test Upload Data]**. The controller will automatically check if the uploaded data complies with the specifications and display the results in the test report.

Once completed, users can view the created devices in the **[Inventory Information]** view.

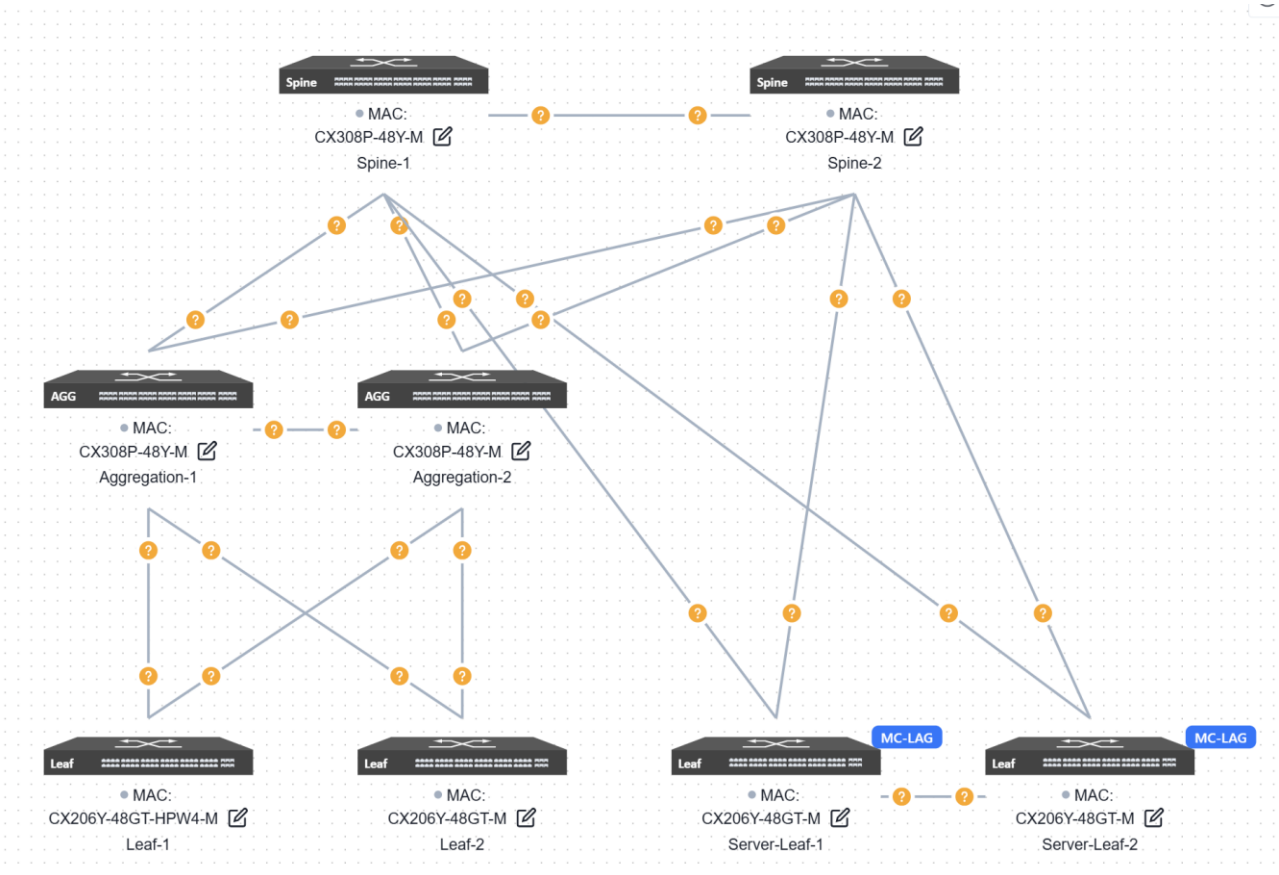
12.3.4 Service Configuration

Click **[Design Topology]** to enter the corresponding page, select the Large/Mild-Scale campus

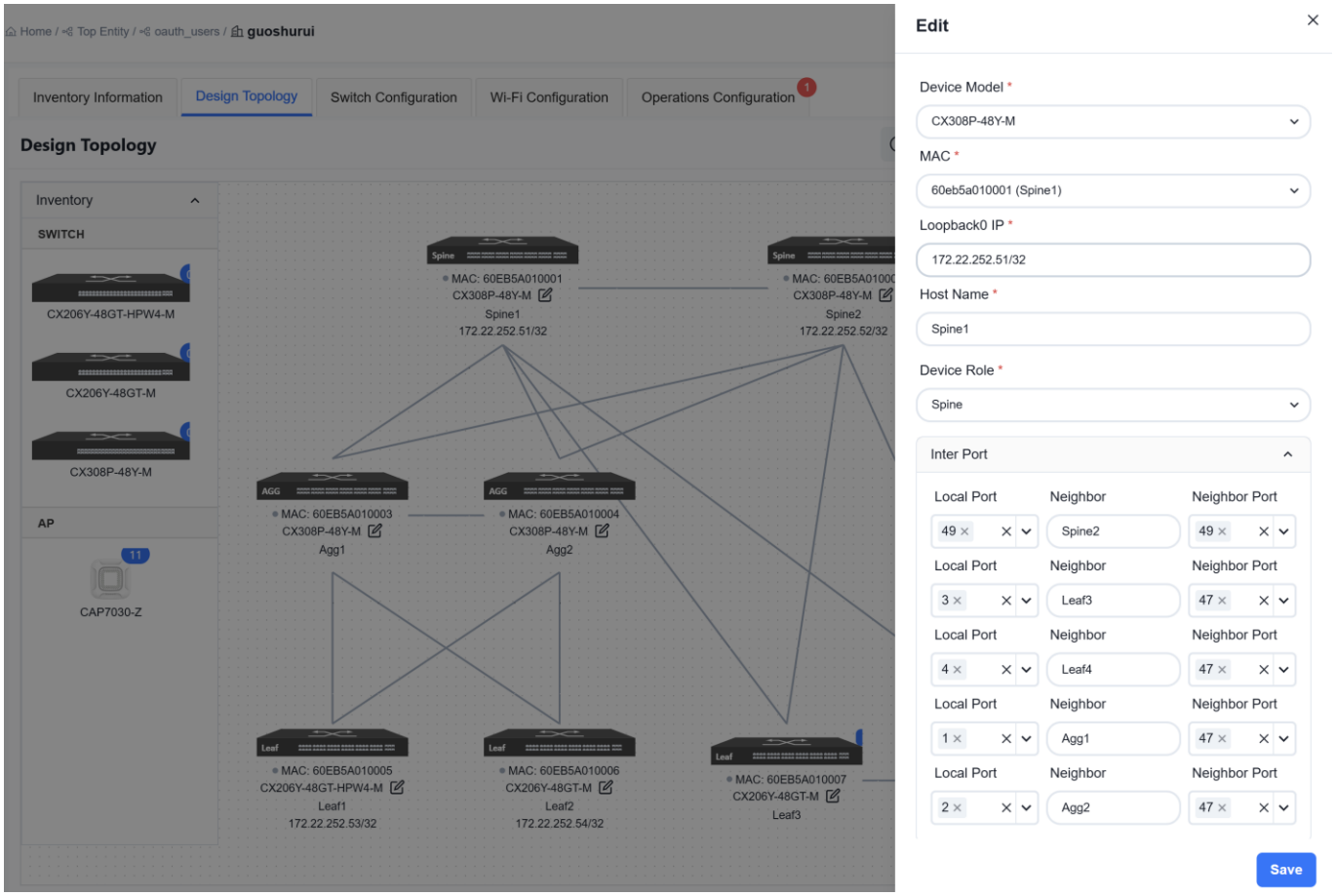
deployment, fill in the required device models and quantities according to device roles, and then click **[Save]** to finish the network topology pre-planning. The controller will generate the network topology based on the entered information.



Generated topology:



Users can click the **[Edit]** button on the device end and fill in the corresponding information in the slide-out panel on the right.



MAC: Uniquely select a device via its MAC address.

Loopback0 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.

Inter Port:

Local Port: The interface on the current device.

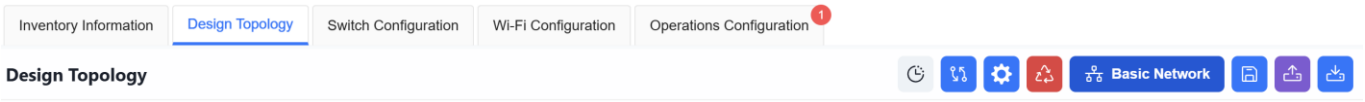
Neighbor: Select the peer device connected to the local interface.

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

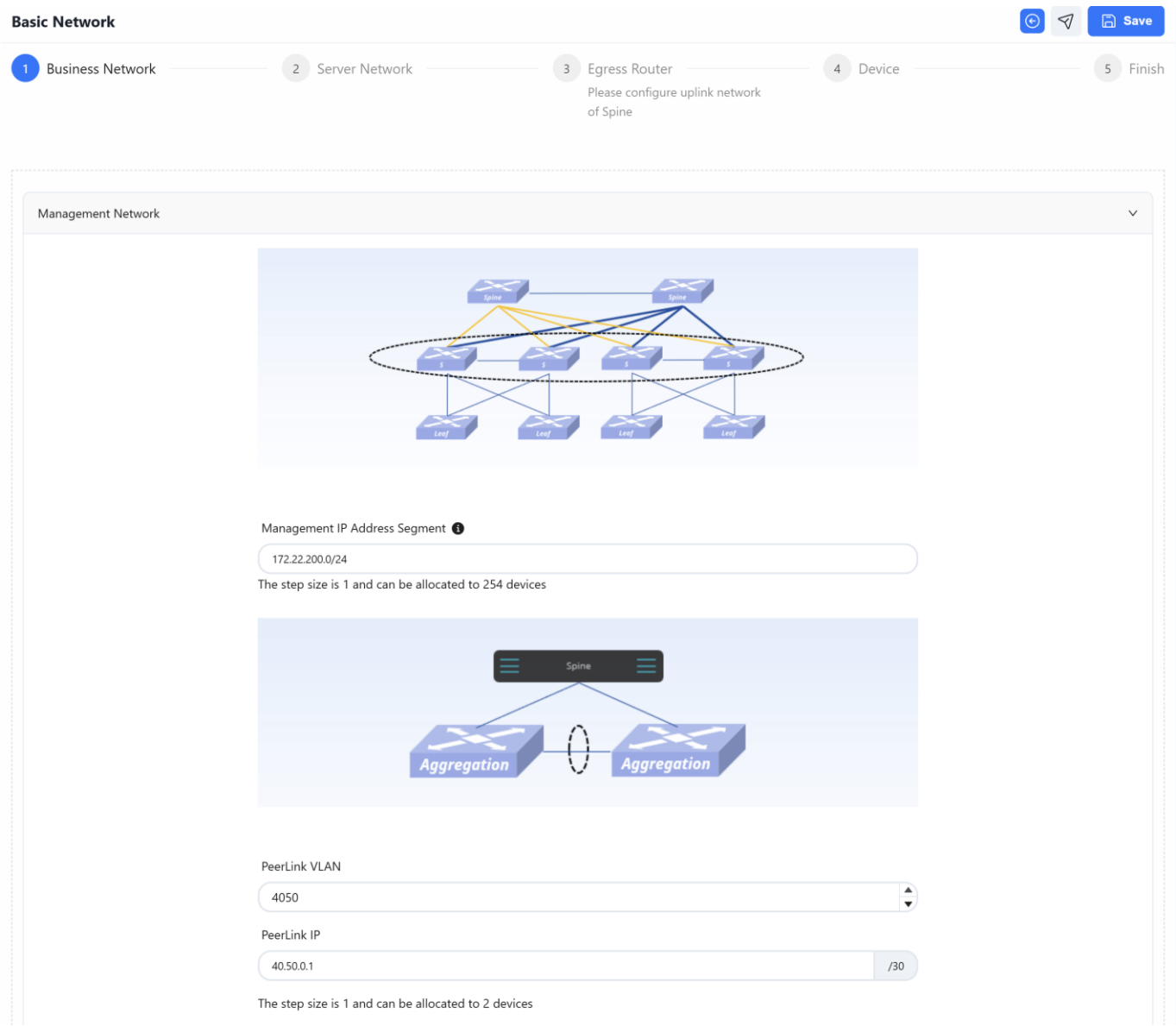
Upon completing all configurations, click **[Save]** in the upper right corner of the page, then select **[Confirm]** in the pop-up window.

12.3.5 Basic Network

Click the top right corner **[Basic Network]**



12.3.5.1 Business Network



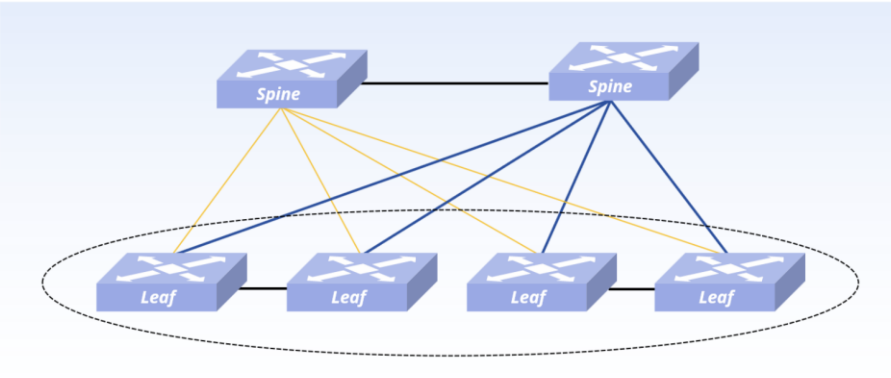
Management Address Segment: Configure an in-band management network for convergence devices. Since both Spine and Leaf devices are Layer 3 devices, the Loopback0 address can be used for in-band management. However, convergence devices are Layer 2 devices and require a VLAN interface to serve as the in-band management interface. The controller can assign an in-band management address to each convergence device based on the address segment entered by the user.

PeerLink VLAN: Configure a PeerLink VLAN for convergence devices. The directly connected interfaces between two devices are referred to as peer-link interfaces, which are primarily used for transmitting protocol packets and forwarding traffic in the event of a failure. The VLAN dedicated to the PeerLink interface is the PeerLink VLAN.

PeerLink IP: Configure an IP address on the PeerLink VLAN interface. After setting the PeerLink IP, the device knows which IP address to send control packets to for communication with the peer device. The

IP addresses of the two peer convergence devices must be within the same subnet.

12.3.5.2 Server Network



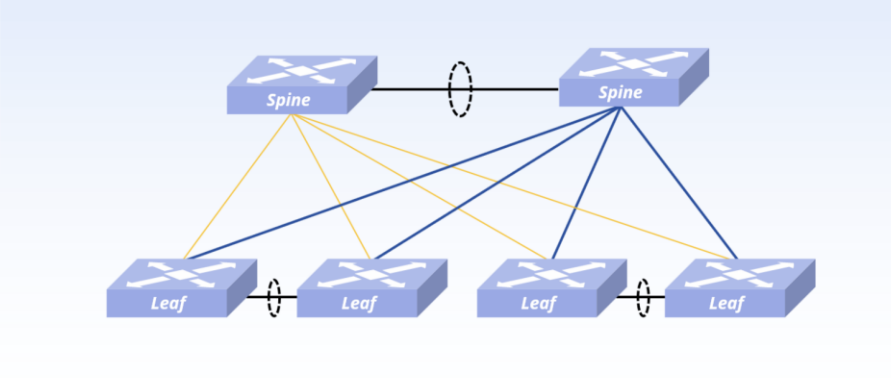
Management Method

In-Band

Management IP Address Segment

172.22.201.0/24

The step size is 1 and can be allocated to 254 devices



PeerLink VLAN

4050

PeerLink IP

40.50.0.1

/30

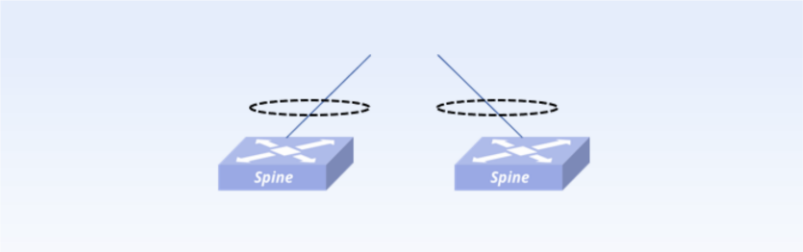
The step size is 1 and can be allocated to 2 devices

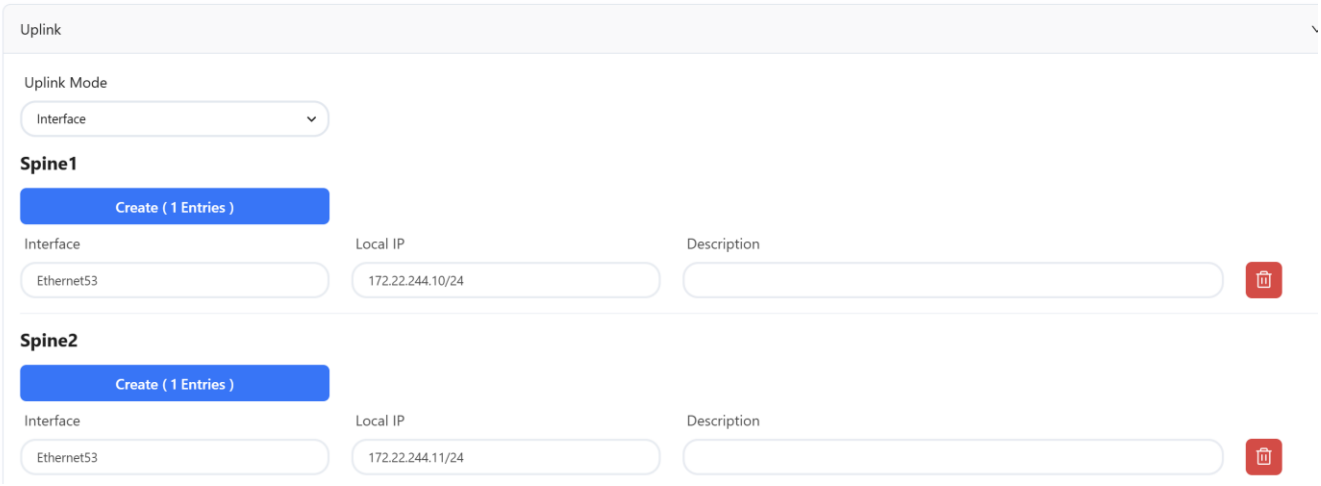
Configure the in-band management network for the server area leaf devices.

Configure the PeerLink interface VLAN and PeerLink IP.

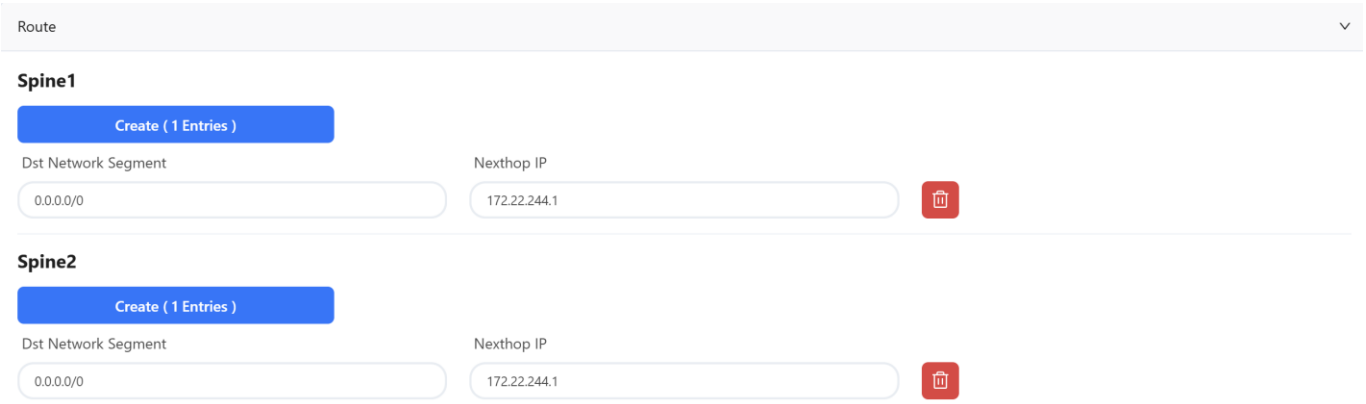
12.3.5.3 Egress Router

Click **[Create]**, select the interface ID of the Spine device's uplink interface, and configure the IP address as per the service plan.

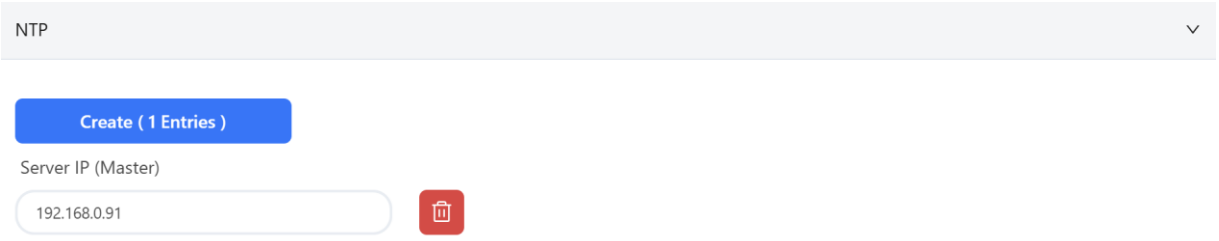




To ensure normal network operation, a default route typically needs to be configured, with the next hop IP set as the peer IP address of the Spine uplink interface.



12.3.5.4 Device

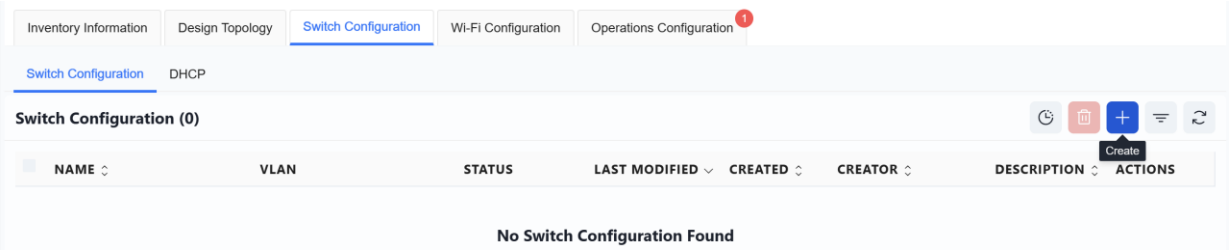


NTP: Configure the NTP server IP address as the Controller's address to provide a unified, accurate, and reliable time reference for the devices.

12.3.5.5 Switch Configuration

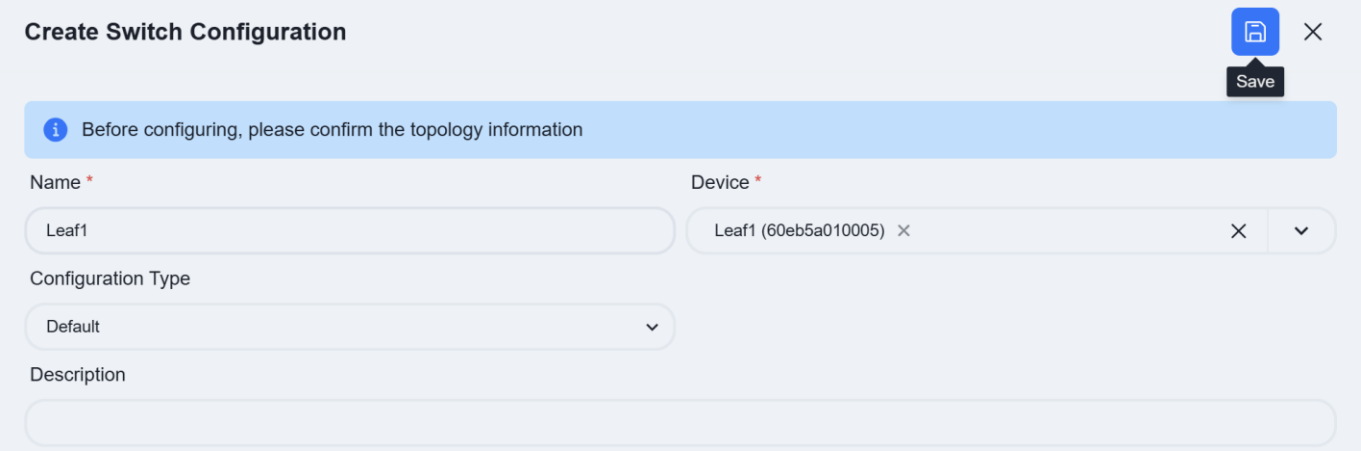
12.3.5.5.1 Switch Configuration

Click **[Create]** on the right to set up the switch configuration.



12.3.5.5.2 Default Zone

1. Leaf1



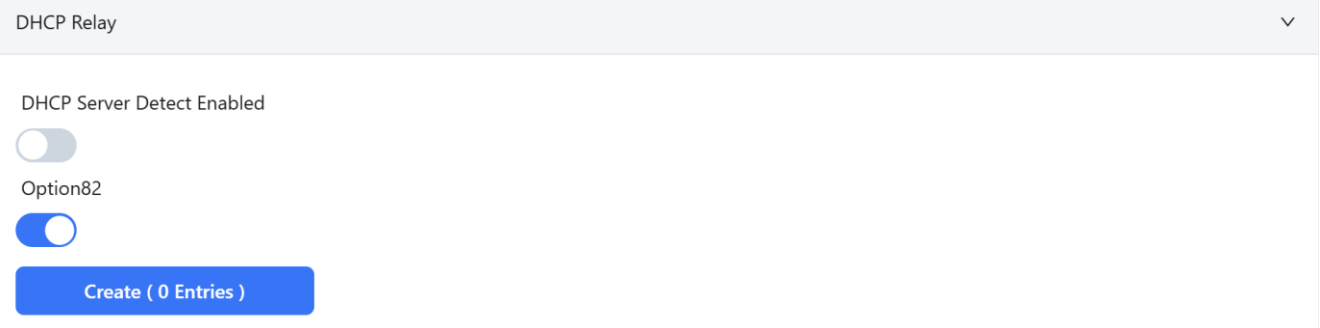
Name: User-defined

Device: Select the Access-1 device

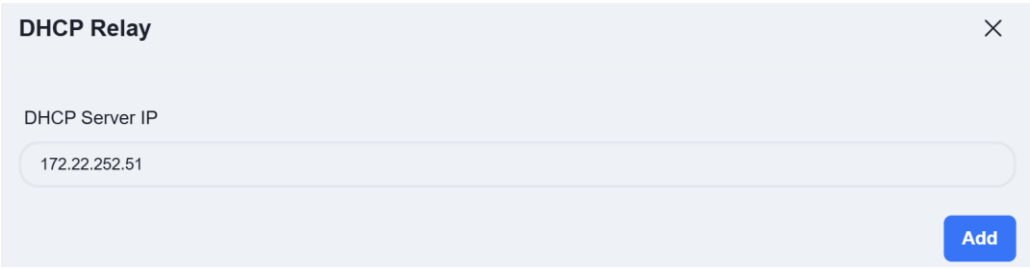
Configuration Type：Select Default

DHCP Relay

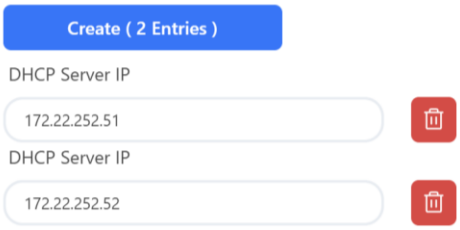
Since the DHCP Server is deployed on the Spine and is not directly connected to the service devices on Leaf1, a DHCP relay needs to be configured.



Click **[Create]**, enter the DHCP server IP in the pop-up page, and then click **[Add]** after completion.



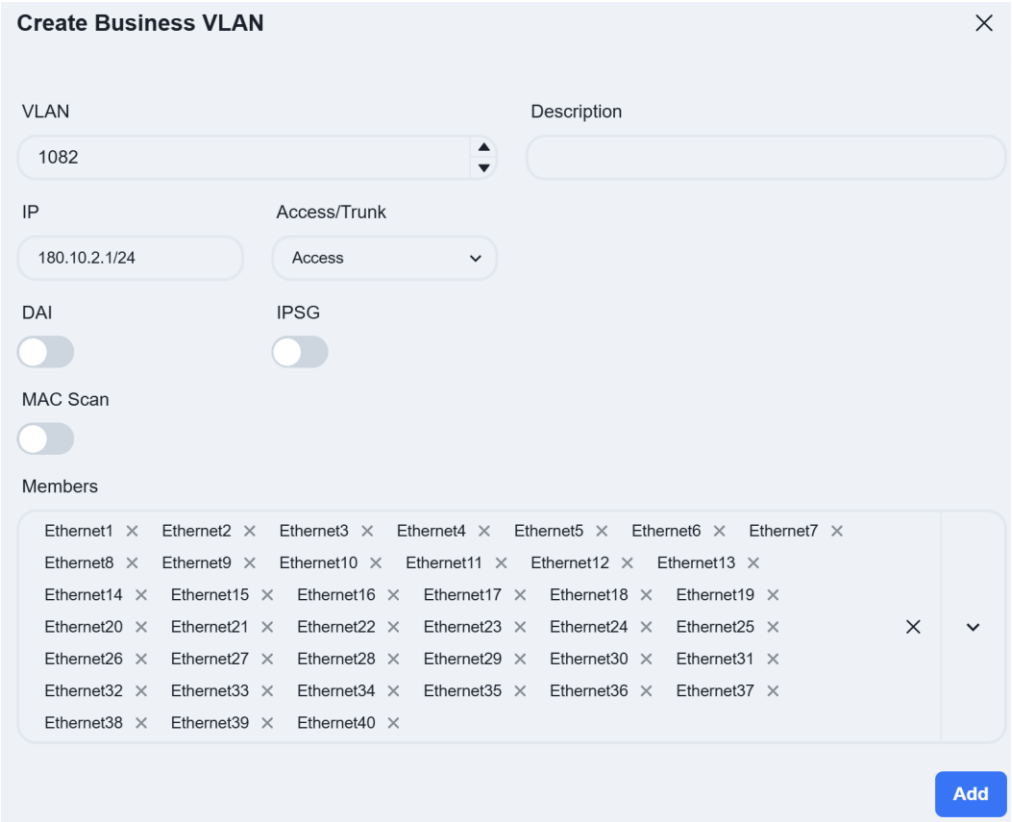
Since DHCP Servers are deployed on both Spine devices with DHCP Failover configured, two DHCP server IP addresses need to be entered.



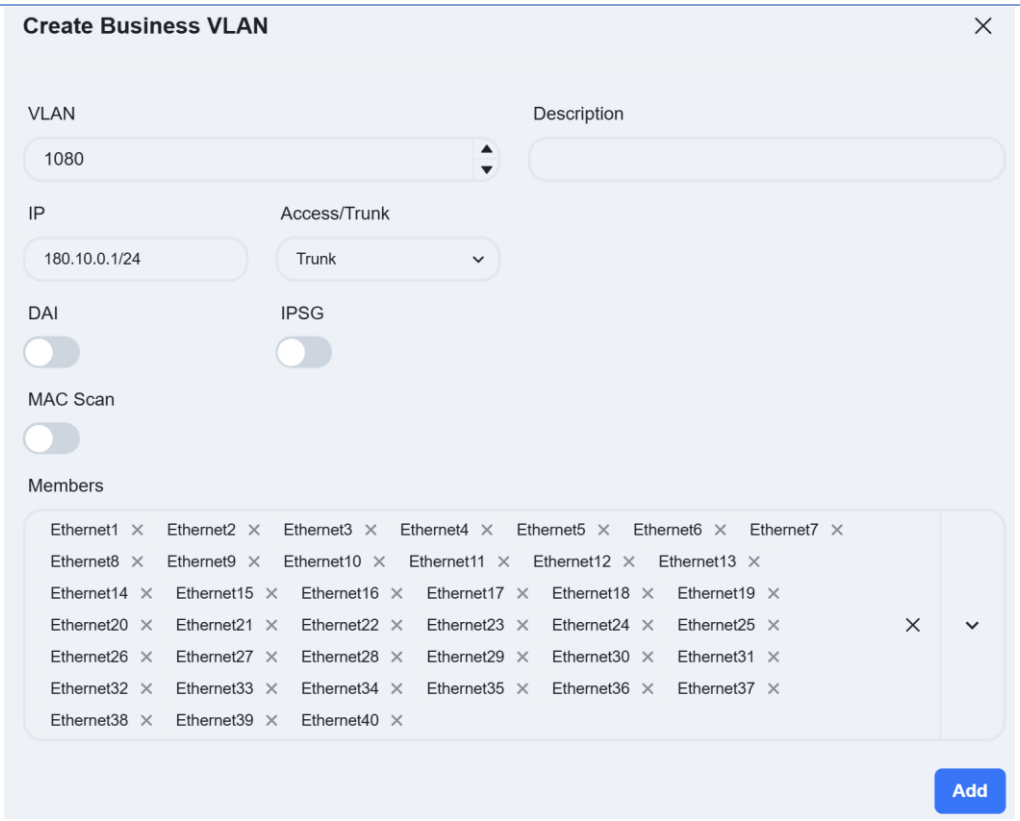
Business VLAN

Deploy wireless service configuration on Leaf1 and set up the service gateway.

1. Configure the AP management VLAN



2. Configure the Wireless Business VLAN



IP: Enter the service gateway address.

Access/Trunk: Select the mode based on whether the interfaces send and receive frames with VLAN tags.

Access: Receives untagged frames. Typically configured for the AP management VLAN and wired service VLANs.

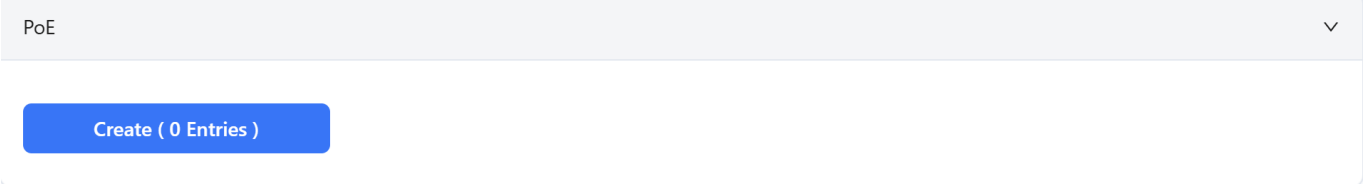
Trunk: Receives tagged frames. Typically configured for wireless service VLANs.

Members: Click the dropdown arrow to select the member interfaces for the VLAN on the device.

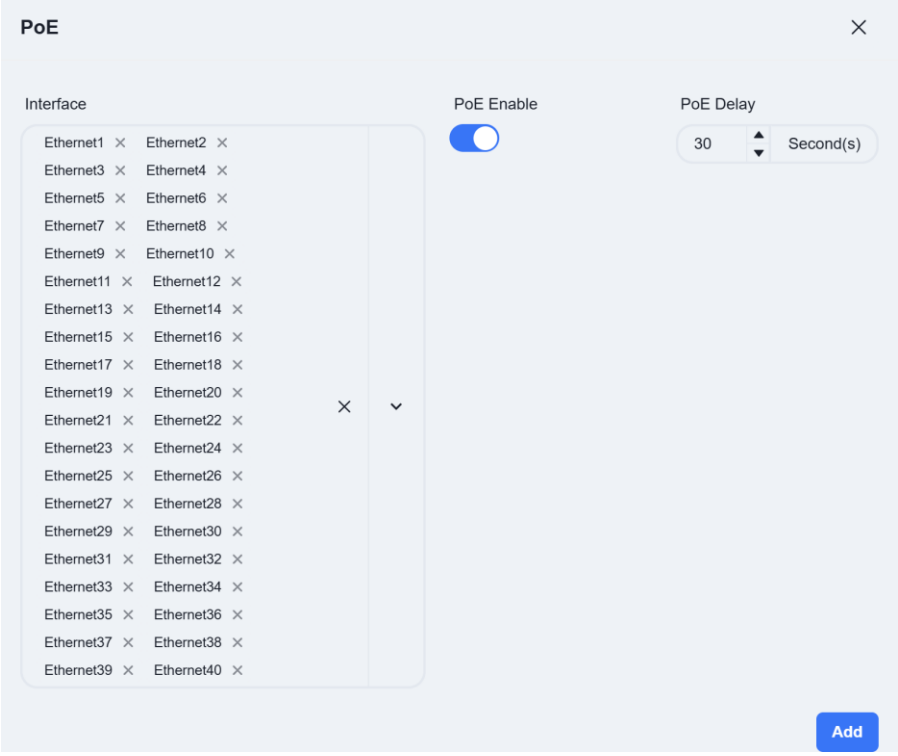
POE

The access switch features PoE functionality, which can be directly enabled in the wired service configuration to supply power to PD devices.

Click **[Create]**

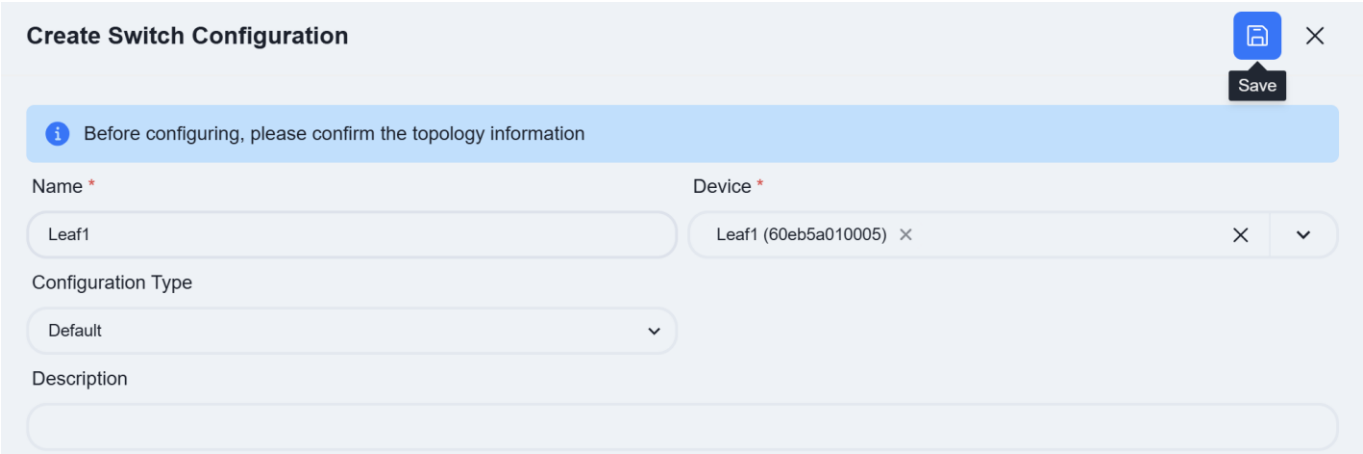


Select the interface where the PoE function is to be enabled and set the startup delay time.

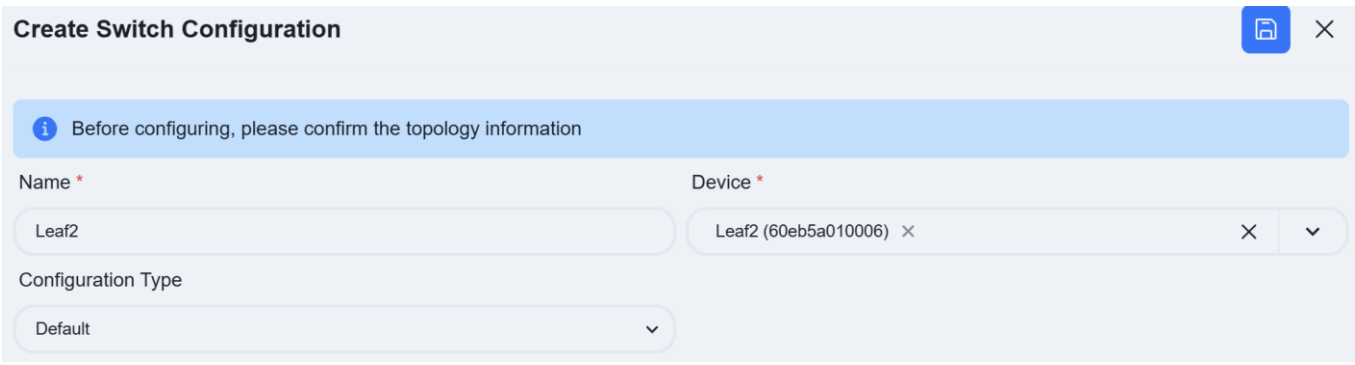


POE Delay: This refers to a brief, intentional time delay introduced at a PoE switch port between when it begins to supply power and when it actually delivers power to the Powered Device (PD).

Once all configurations are completed, click **[Save]** in the top right corner to finish configuring Leaf1.



2. Leaf2

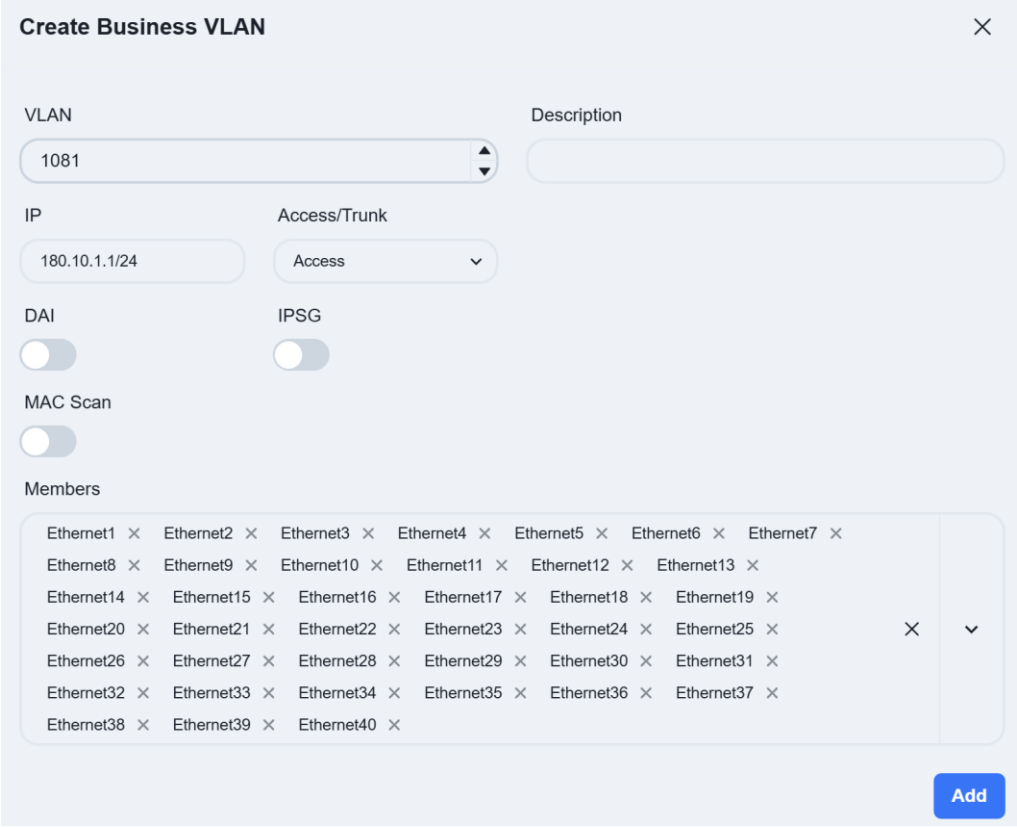


DHCP Relay

Same as Leaf1

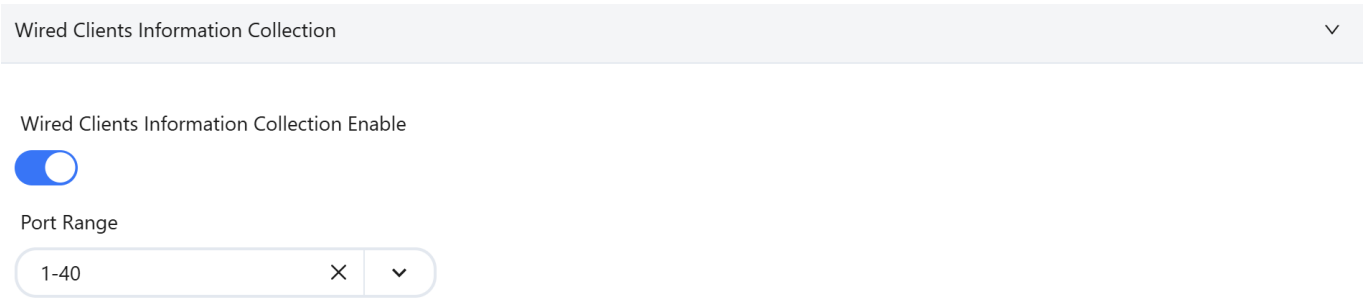
Business VLAN

Deploy wired service configuration on Leaf2 and set up the service gateway.



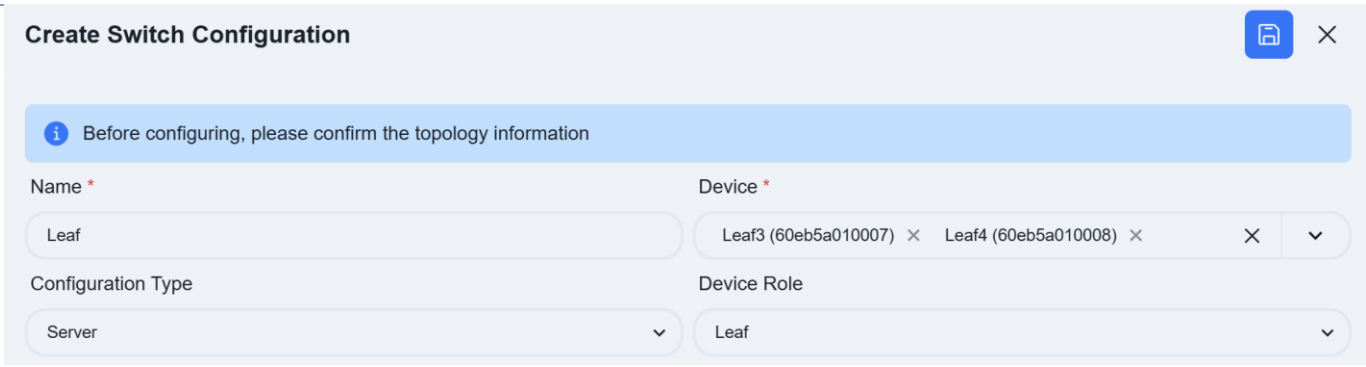
Wired Clients Information Collection

Interfaces with this feature enabled will report information about the connected wired terminals to the controller.



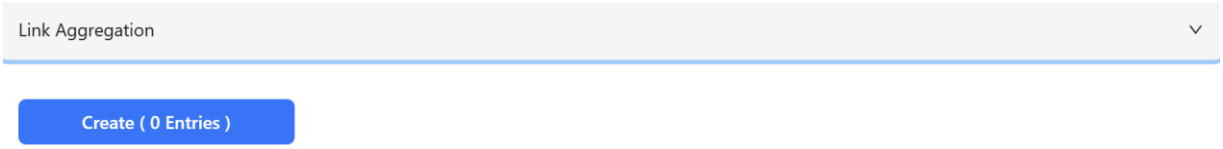
12.3.5.5.3 Server Zone

1. Leaf

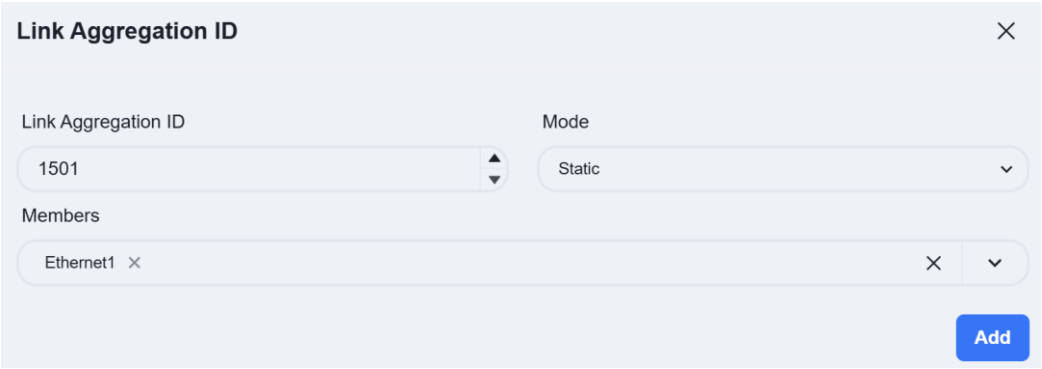


Link Aggregation

Click **[Create]**



Enter the Link Aggregation ID and Members in the pop-up view.



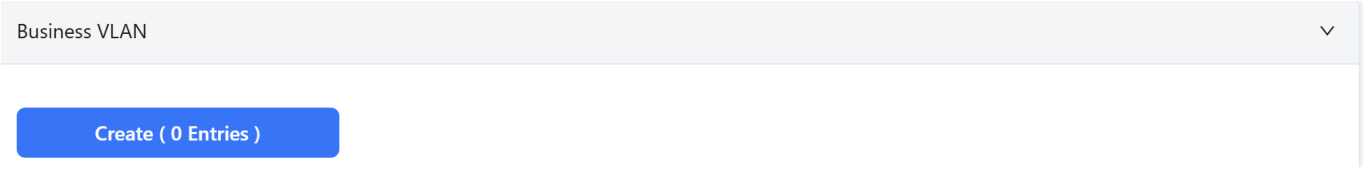
Link Aggregation ID: Users can create an ID within the range of 1501–2000 as needed.

Mode: Static/LACP, select whether the link aggregation mode is static or LACP dynamic negotiation.

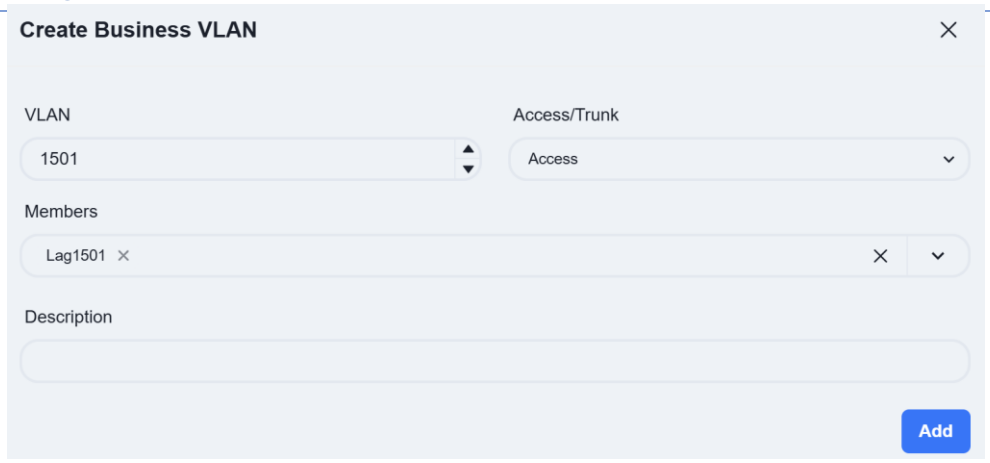
Members: Select the member interfaces connected to this service server.

Business VLAN

Click **[Create]**



Fill in the relevant information in the pop-up view.

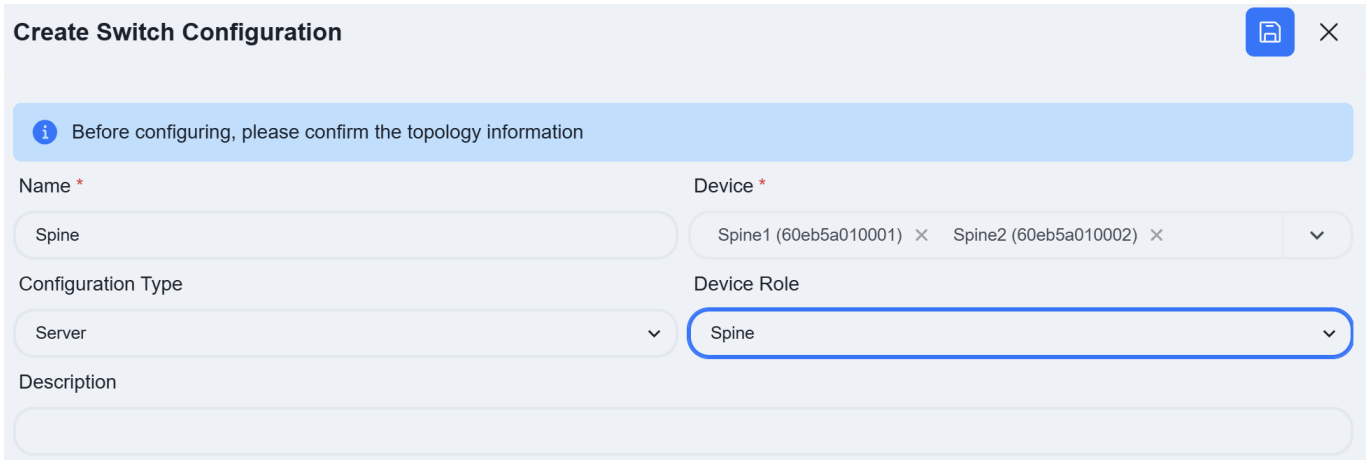


VLAN: Users can enter a VLAN ID between 2 and 4050 according to the service plan.

Members: Only LAG interfaces configured in link aggregation can be selected as member interfaces.

Click **[Save]** after completing all configurations.

2. Spine

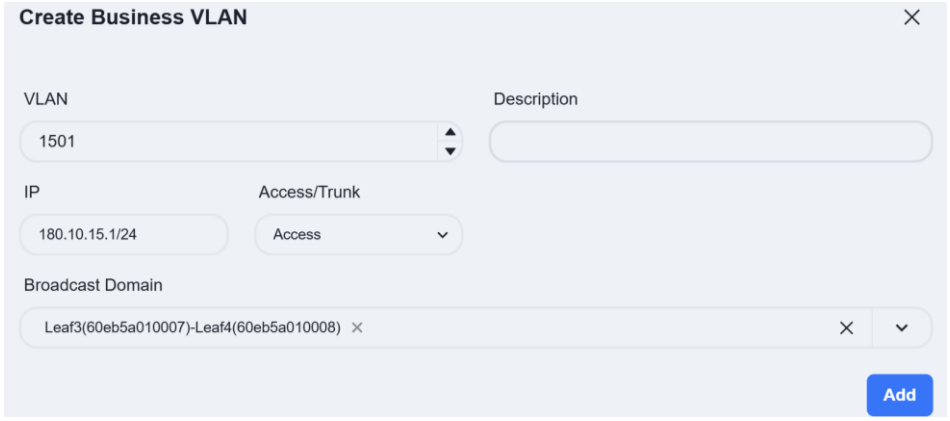


DHCP Relay

Since the DHCP service is deployed on the Spine, no relay configuration is required on the Spine.

Business VLAN

Click **[Create]**



VLAN: Corresponds to the service VLAN of the server area Leaf switch.

IP: Enter the gateway IP address of the service VLAN as planned.

Broadcast Domain: Select the Leaf switch corresponding to the VLAN.

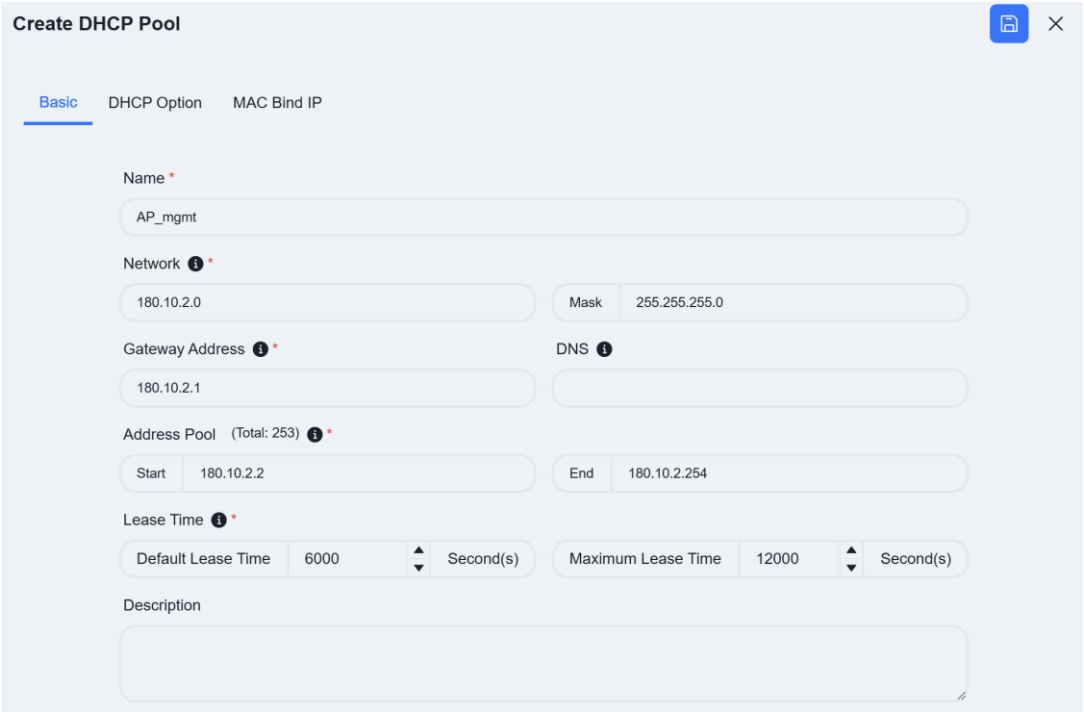
Click **[Save]** after completing all configurations.

12.3.5.6 DHCP

The controller allows users to configure the DHCP Server function on Spine devices.

After entering the site, click **[Configuration]** - **[Switch Configuration]** - **[DHCP]** to access the DHCP Server configuration interface. Then, click the **[+]** button on the page to create a new configuration:

Create AP Management Address Pool.



Name: User defined.

Network: Specify the network segment where the IP address assigned by the DHCP server to the DHCP client is located.

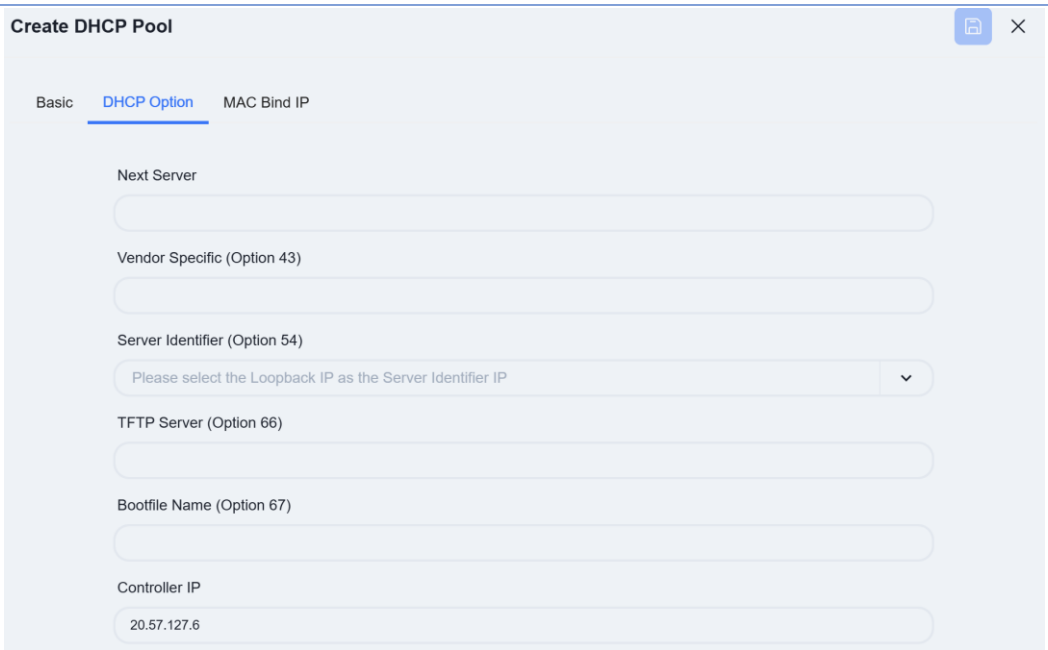
Gateway Address: Specify the gateway address assigned by the DHCP server to the DHCP client.

DNS: Specify the DNS server address.

Address Pool: Specify the address range allocated by the DHCP server to DHCP clients.

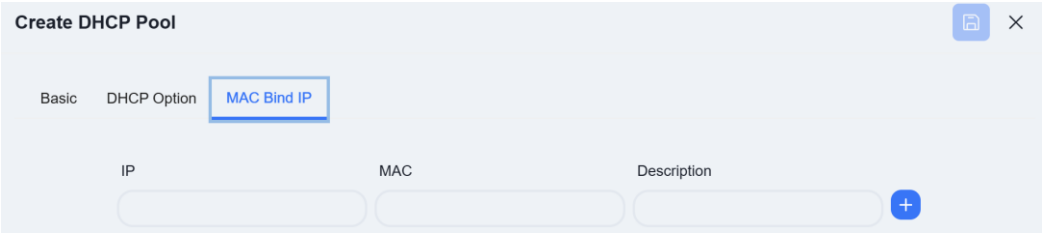
Lease Time: Specify the IP address lease time.

Click on **[DHCP Option]**and fill in the relevant information.



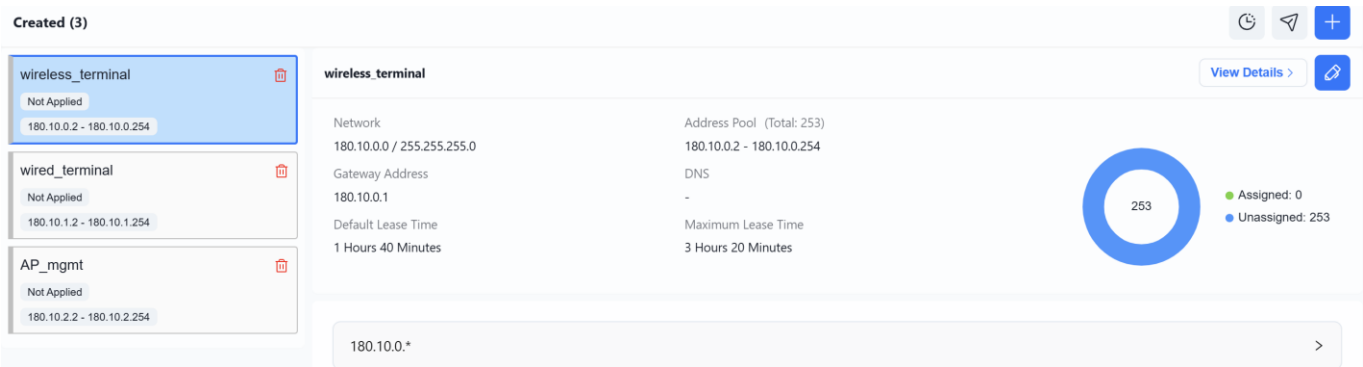
Controller IP: DHCP options specifically designed for wireless AP discovery controllers, fill in the controller IP address.

The controller supports configuring MAC binding IP function, which users can fill in as needed.



Click **[Save]** after completing all configurations.

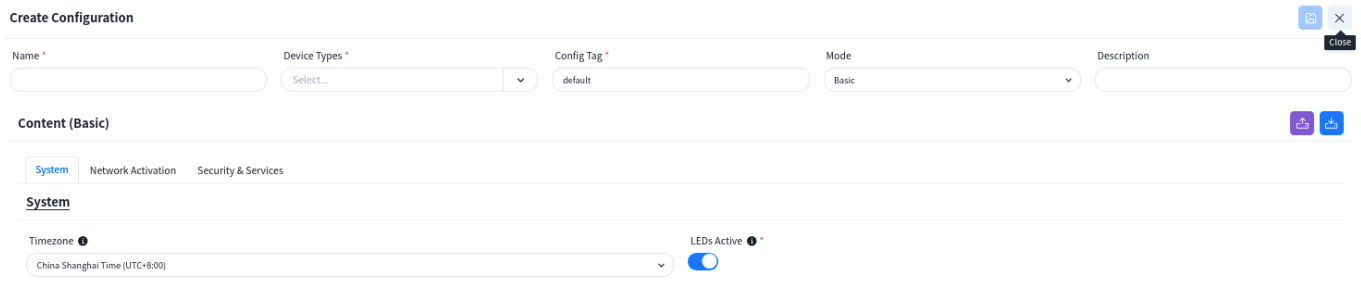
Follow the steps above to sequentially create the DHCP configurations for wireless terminals and wired terminals. Once all configurations are completed, the DHCP view will appear as shown below.



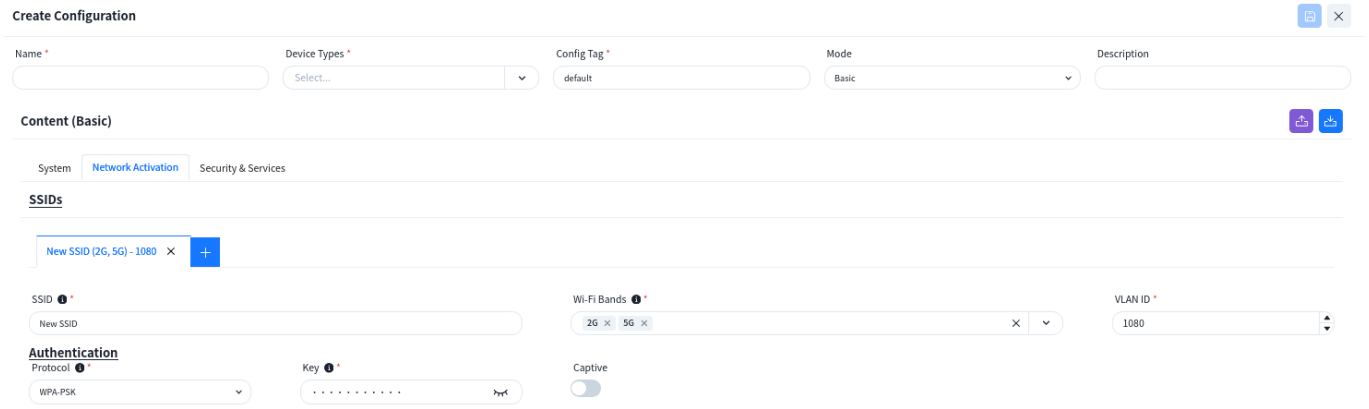
12.3.6 Wi-Fi Configuration

Click **[Wi-Fi Configuration] - [+]** to configure the necessary basic information for the wireless AP, e.g. SSID settings, security policy. The controller can automatically generate the corresponding

The controller supports the configuration of different wireless service configurations, and after the AP goes online, it will determine which configuration should be issued to the AP based on the **[Config Tag]** attributes of the configuration.

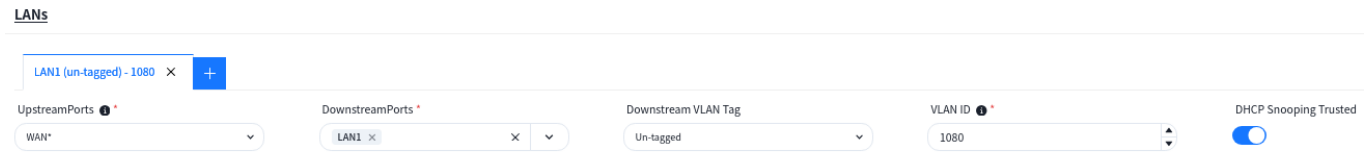


12.3.6.1 SSID



12.3.6.2 LAN

When the AP is one that has an extended wired interface and is capable of accessing terminals by wired means, such as a panel AP, the user can configure the access method for wired terminals through the configuration in LANs.



UpstreamPorts: Specify the up-link interfaces for wired terminal to access the network through AP, usually it is the interface for AP to connect to the switch, and keep the same with **[UpstreamPorts]** in **[SSID] – [Advanced]** Settings, the default is: WAN*.

DownstreamPorts: Interfaces for wired terminal access.

Downstream VLAN Tag: Whether the wired terminal carries VLAN Tag.

VLAN ID: The AP receives messages from wired terminals that add this VLAN TAG to identify.

DHCP Snooping Trusted: DHCP Snooping Trusted interface, if the wired terminal needs to obtain IP

address through DHCP service, this switch needs to be on.

12.3.7 Configuration Release

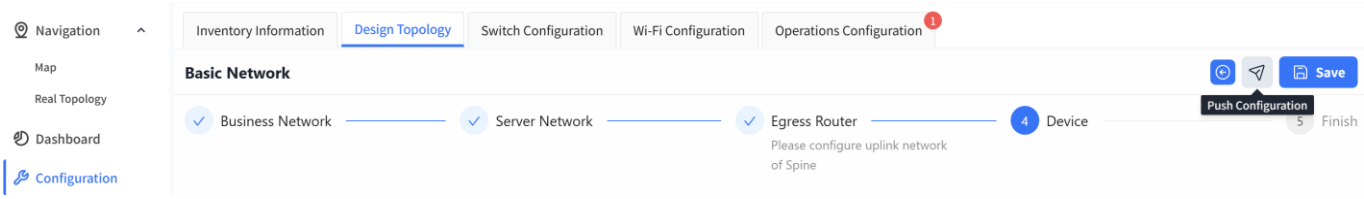
12.3.7.1 Switch

Switches support both in-band and out-of-band management methods. Operation and maintenance personnel can flexibly choose based on current network conditions. For devices in the factory default state, whenever either the management port or service port is in an "Up" state, they will actively initiate a DHCP request to obtain a temporary management IP address and the IP address of the cloud-based controller from the DHCP server. They will then connect to the controller to retrieve configuration information.

Once all switches are successfully connected to the controller, click **[Topology Consistency Verification]** on the upper right side of the **[Design Topology]** view to confirm whether the generated topology matches the planned topology. After verification, the controller can deploy configurations to the switches.

12.3.7.1.1 Push Basic Network Configuration

Click **[Configuration]** - **[Design Topology]** - **[Basic Network]** - **[Push Configuration]** to issue the basic configuration for all devices.

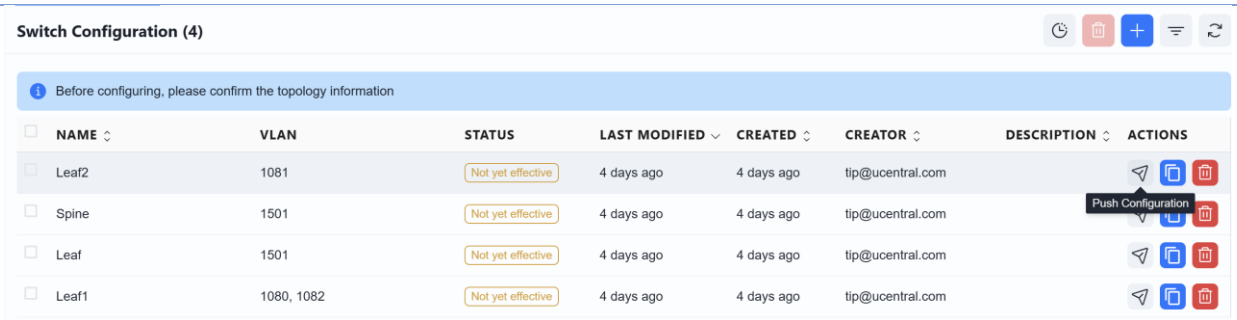


By default, the controller will select all switches. Click the **[Next]** - **[Start]** button to start issuing basic network configurations for the switches.

12.3.7.1.2 Push Switch Configuration

1. Switch Configuration

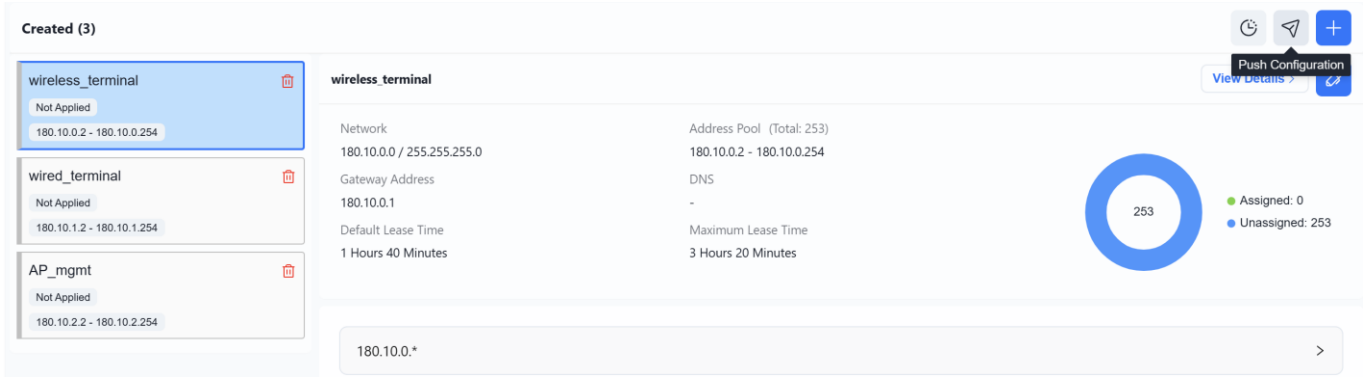
On the **[Configuration]**-**[Switch Configuration]** view, select the configuration to be deployed and click the **[Push Configuration]** button.



In the pop-up window, click **[Next]**-**[Start]** to deploy the switch configuration to the switch.

2. DHCP

On the **[Configuration] - [Switch Configuration] - [DHCP]** interface, select the configuration to be deployed and click the **[Push Configuration]** button to deliver the configuration.



12.3.7.2 AP

The AP does not need to manually issue the configuration. After the configuration of the device is issued and takes effect, the PoE power supply function of the switch is turned on, and the AP can power on and work. When the AP connects to the controller with the information obtained through the DHCP service, the controller will automatically send the configuration to the corresponding AP based on the comparison between the TAG identification stored in the AP inventory and the TAG identification in the planning configuration.

12.4 Open Cloud Connect

12.4.1 Scenario Overview

The Open Cloud Connect scenario fully unleashes the classic Layer 2 switching and Layer 3 routing capabilities in standalone mode. Its modular architecture provides flexible component combination options, allowing users to customize network functions based on actual business needs.

- Visualized Centralized Management and Device-Level Flexible Configuration

This solution offers flexible and open network configuration capabilities. Through a centralized controller, operations staff can deliver configurations to switches via a graphical interface, significantly simplifying the deployment process. At the same time, the solution supports atomic-level, on-demand service configuration for individual devices. This process is independent of the network topology, offering high flexibility and scenario adaptability to precisely meet various business needs—from standardized deployments to highly customized requirements.

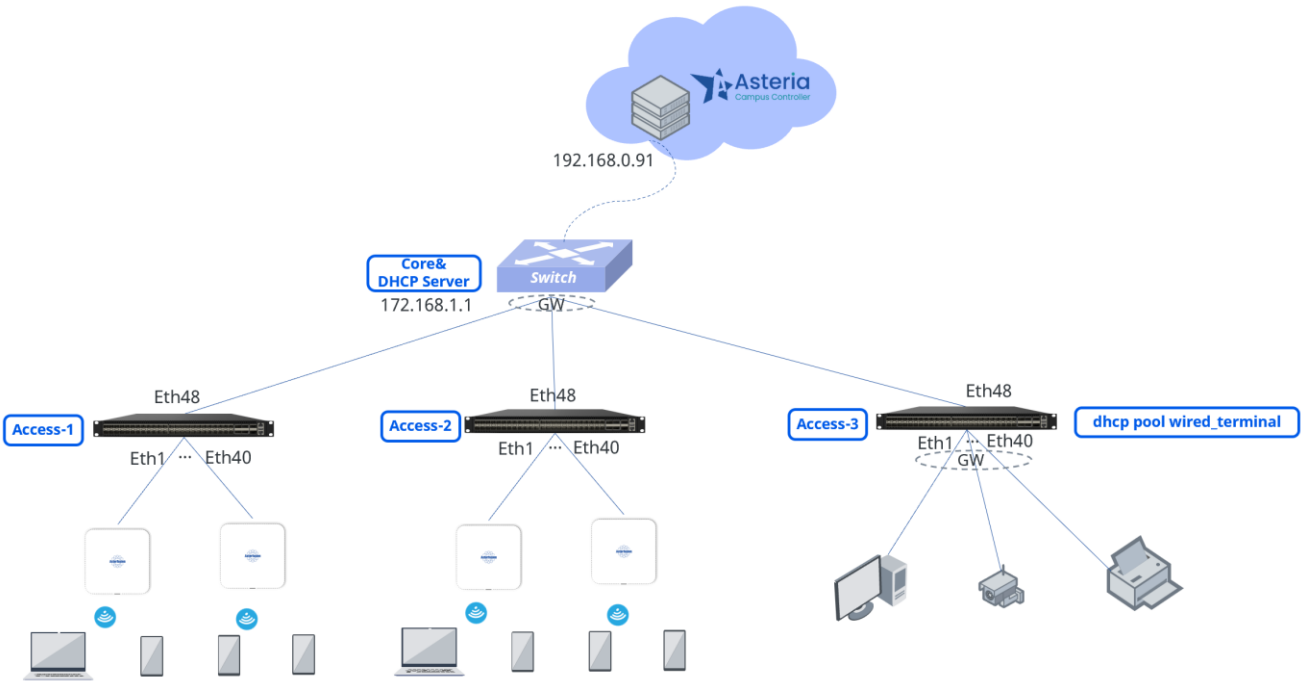
- Intelligent and Unified Operations Management with Proactive Insights

In terms of deployment and management, this solution utilizes a unified controller for centralized policy distribution and device management. Beyond that, the controller boasts powerful real-time monitoring and intelligent analysis capabilities. It continuously collects operational status and performance metrics from across the network, intelligently calculates a health score for each device based on multi-dimensional data, and provides extensive logging and precise real-time alerts. This mechanism greatly simplifies network operations, enabling administrators to proactively identify potential risks, quickly locate issues, and resolve them—thereby comprehensively improving operational efficiency and network reliability.

- Enhanced Network Services and Edge Autonomy

Furthermore, the system supports the direct deployment of DHCP servers on Leaf nodes, further enhancing the autonomy and deployment flexibility of network services. This effectively meets users' address management requirements in diverse network environments.

12.4.2 Scheme Design



Network Architecture:

The Open Cloud Connect scenario allows users to flexibly configure Access devices. In the above network design, wireless networks are deployed on Access-1 and Access-2, while a wired network is deployed on Access-3. The gateways for the wireless networks are uniformly deployed on the Core, whereas the gateways for the wired network are deployed on the Access devices, making management and expansion more convenient.

DHCP Deployment:

The DHCP services for wireless terminals and AP management are deployed on the Core device, providing a consistent IP address acquisition point for wireless terminals and enabling seamless roaming. In contrast, the DHCP service for wired terminals is deployed on the Access devices, facilitating rapid fault localization and streamlining the troubleshooting process.

Controller Deployment:

The controller is cloud-deployed and managed uniformly via a graphical interface. It enables centralized policy distribution, configuration management, and status monitoring, significantly enhancing operational efficiency. Particularly for batch configuration and deployment of Access devices, it greatly reduces the workload.

Service Planning:

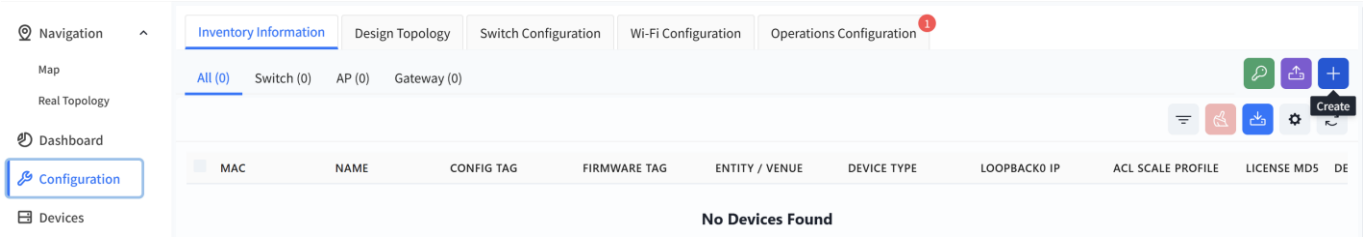
Service Type	IP Segment	Gateway	Service VLAN	SSID
Wireless Service	180.10.0.0/18	180.10.0.1/18	1080	New SSID
Wired Service	181.10.0.0/24	181.10.0.1/24	1081	-
AP Management	182.10.0.0/24	182.10.0.1/24	1082	-

12.4.3 Device Import

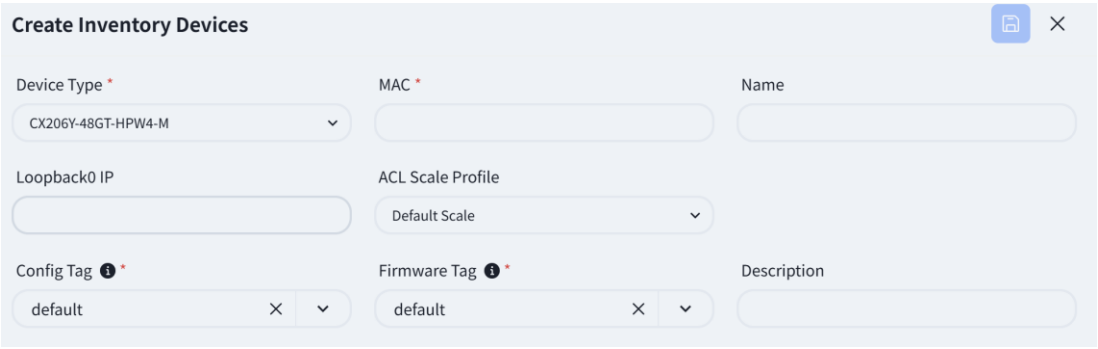
Administrators can create or import devices in bulk to specified sites/organizations. When an added inventory device connects to the controller and comes online, the controller will automatically assign it to the designated organization/site based on its MAC address.

1. Add devices one by one.

Click **[Configuration]** - **[Inventory Information]** - **[+]** to create an inventory device.

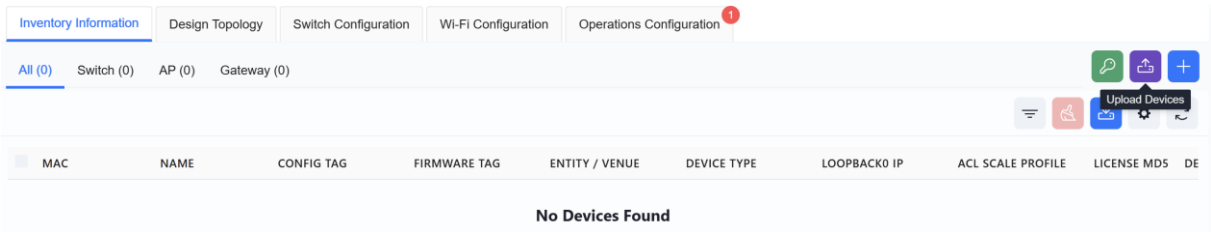


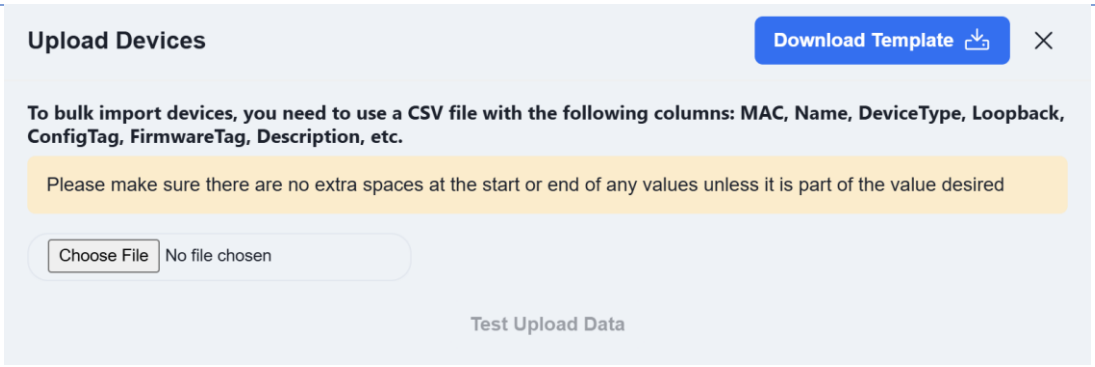
Fill in the relevant information as prompted on the page



2. Import via Excel

Click **[Upload Devices]**





Click **[Download Template]** and enter the information for the devices to be added to the inventory according to the template's specifications.

MAC	DeviceType	Name	ConfigTag	FirmwareTag	Loopback	AclScaleProfile	License	Description
60eb5a000001	CX206Y-48GT-HPW4-M	Access-1						
60eb5a000002	CX206Y-48GT-HPW4-M	Access-2						
60eb5a000003	CX206Y-48GT-M	Access-3						
60eb5a000004	CAP7030-Z			default				
60eb5a000005	CAP7030-Z			default				
60eb5a000006	CAP7030-Z			default				
60eb5a000007	CAP7030-Z			default				
60eb5a000008	CAP7030-Z			default				
60eb5a000009	CAP7030-Z			default				
60eb5a000010	CAP7030-Z			default				
60eb5a000011	CAP7030-Z			default				
60eb5a000012	CAP7030-Z			default				
60eb5a000013	CAP7030-Z			default				
60eb5a000014	CAP7030-Z			default				

MAC: The device's MAC address. This information is typically found on the device's label.

Device Type: The device model.

Name: The device hostname. By default, it is the device's MAC address.

ConfigTag: After an AP connects to the controller, it will automatically pull the configuration file corresponding to this tag. By default, the tag value is default.

FirmwareTag: When performing firmware upgrades, devices requiring an upgrade can be filtered based on their firmware tag type. By default, the tag value is default.

Loopback: The device's loopback address. For all devices operating at Layer 3, this address serves as the device's in-band management address.

AclScaleProfile: Optional values are default or large-scale. By default, the value is default.

License: The AP's license file. For bulk imports, you can either enter the JSON-formatted license file content directly in the Excel sheet, or add all devices to inventory first and then import the license files in bulk afterward.

Description: Descriptive information about the device.

Click **[Choose File]** to upload the completed template, then click **[Test Upload Data]**. The controller will automatically check if the uploaded data complies with the specifications and display the results in the test report.

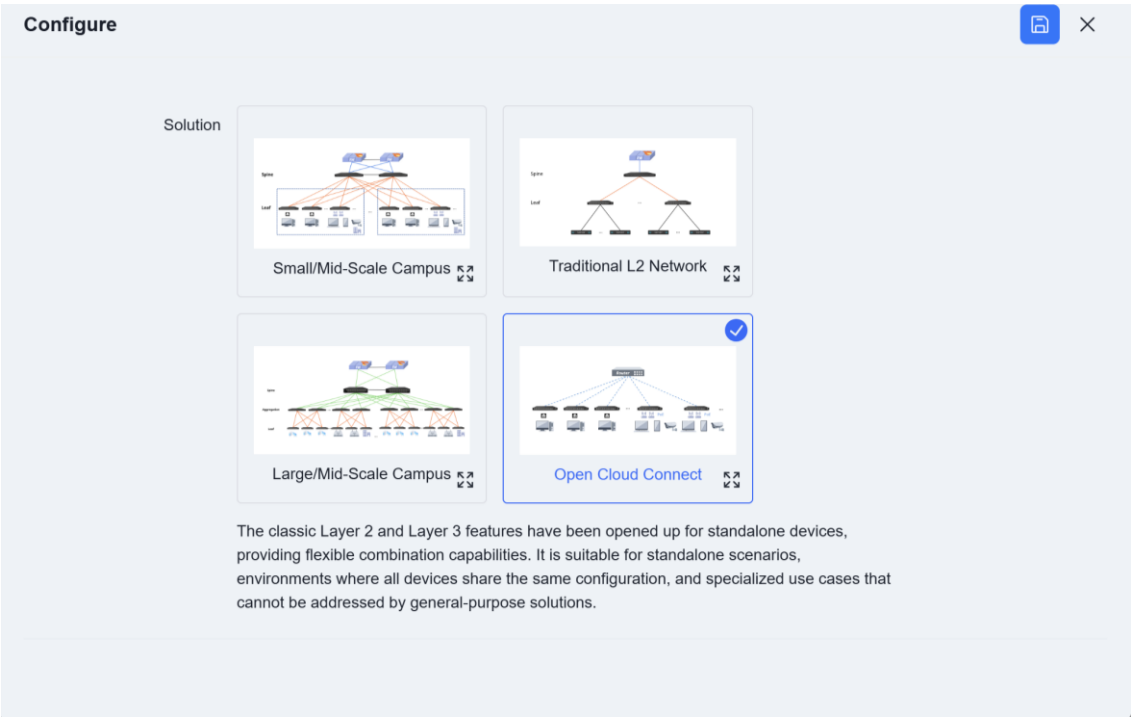
Once completed, users can view the created devices in the **[Inventory Information]** view.

MAC	NAME	CONFIG TAG	FIRMWARE TAG	ENTITY / VENUE	DEVICE TYPE	LOOPBACK0 IP	ACL SCALE PROFILE	LICENSE MD5	D
60eb5a000001	Access-1	default	default	test-gsr-2	CX206Y-48GT-M-HWP4		Default Scale		
60eb5a000002	Access-2	default	default	test-gsr-2	CX206Y-48GT-HPW4-M		Default Scale		
60eb5a000003	Access-3	default	default	test-gsr-2	CX206Y-48GT-M		Default Scale		
60eb5a000004	60eb5a000004	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000005	60eb5a000005	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000006	60eb5a000006	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000007	60eb5a000007	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000008	60eb5a000008	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000009	60eb5a000009	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000010	60eb5a000010	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000011	60eb5a000011	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000012	60eb5a000012	default	default	test-gsr-2	CAP7030-Z		-		
60eb5a000013	60eb5a000013	default	default	test-gsr-2	CAP7030-Z		-		

12.4.4 Service Configuration

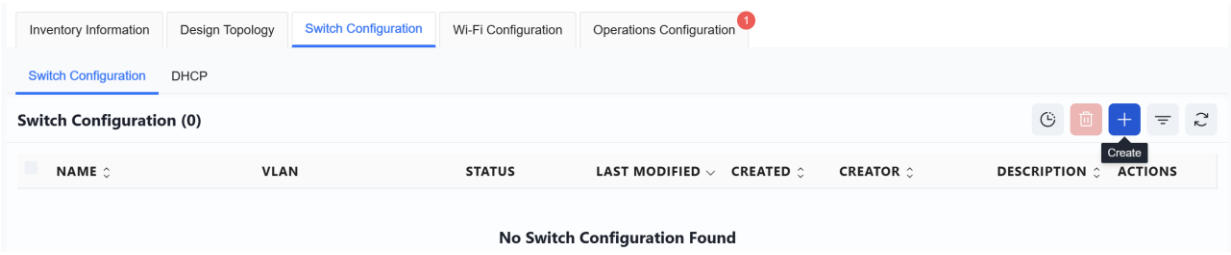
12.4.4.1 Design Topology

Navigate to the **[Configuration]** view from the controller's navigation bar, click **[Design Topology]**, select **[Open Cloud Connect]**, and then click **[Save]**.



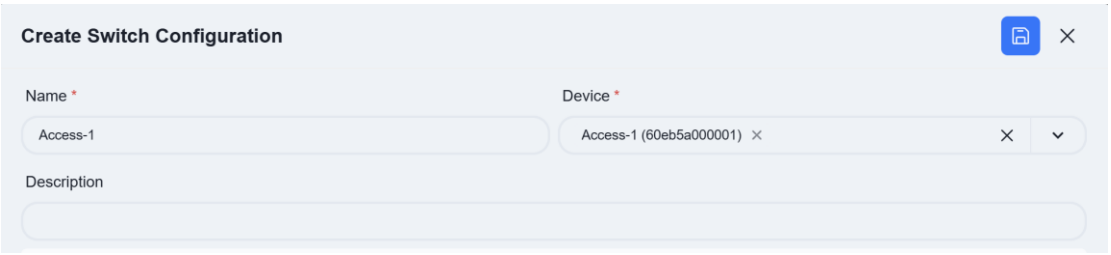
12.4.4.2 Switch Configuration

Click **[Create]** on the right to set up the switch configuration.



12.4.4.2.1 Access-1

1. Create a switch configuration for Access-1:



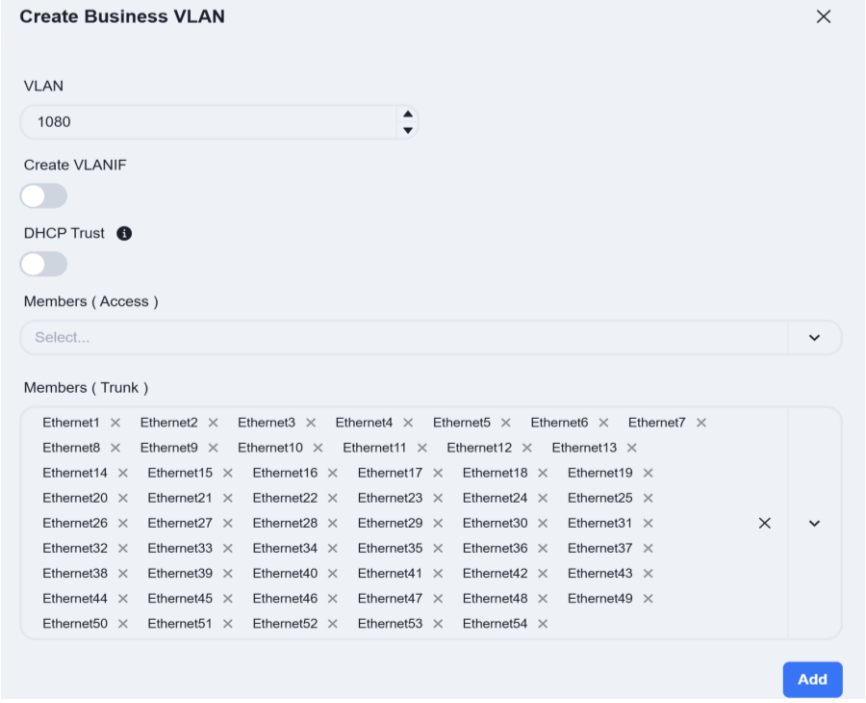
Name: User-defined

Device: Select the Access-1 device

1. Configure Business VLAN

Access-1 is a pure layer 2 configuration, where only business VLAN ID and member interface need to be specified. All other configurations are generated by the controller.

1. Configuring the Wireless Business VLAN



DHCP Trust: Authorizes the selected switch port to forward DHCP messages from legitimate DHCP

servers. Ports not configured as "Trusted" are prohibited from doing so, fundamentally preventing DHCP spoofing attacks.

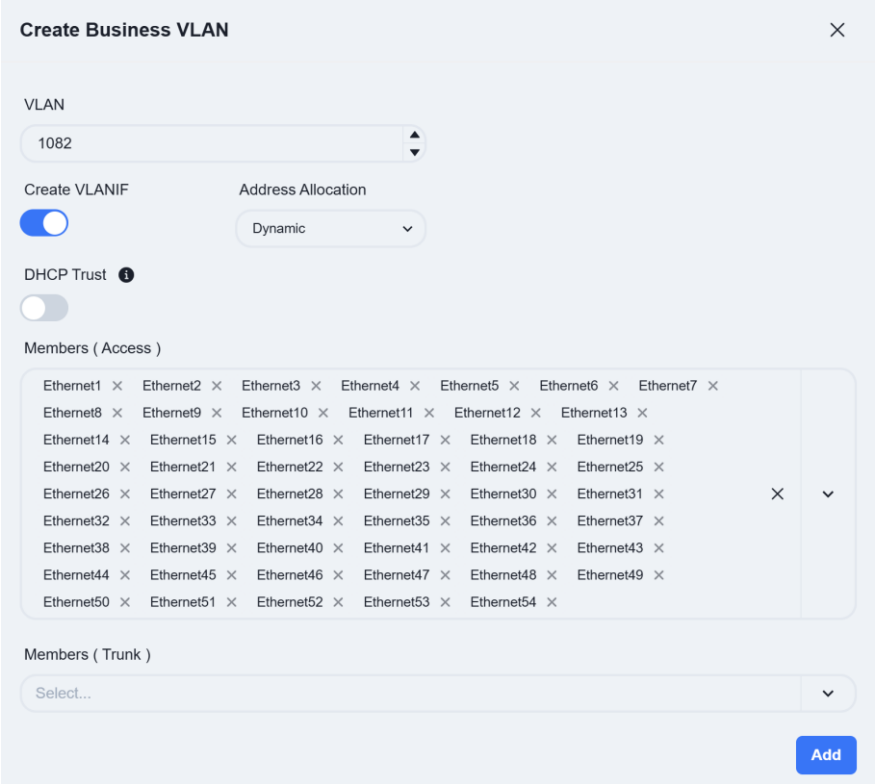
Access/Trunk: Select the mode based on whether the interfaces send and receive frames with VLAN tags.

Access: Receives untagged frames. Typically configured for the AP management VLAN and wired service VLANs.

Trunk: Receives tagged frames. Typically configured for wireless service VLANs.

Members: Click the dropdown arrow to select the member interfaces for the VLAN on the device.

2. Configuring the AP Management VLAN:

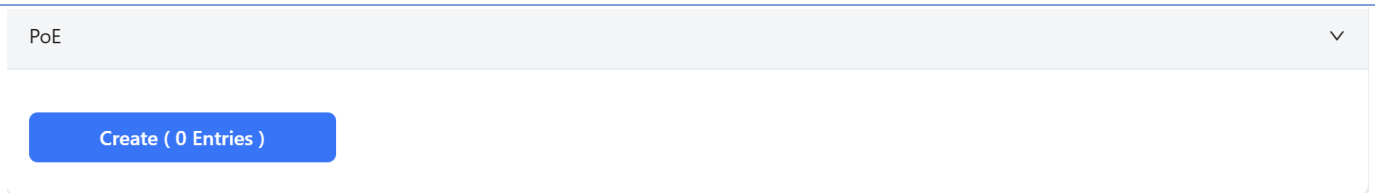


Note: When the address allocation method for the VLANIF interface is set to Dynamic, the switch will obtain an IP address through the DHCP process. This IP address serves as the management address for the switch and resides in the same IP subnet as the management addresses of the APs.

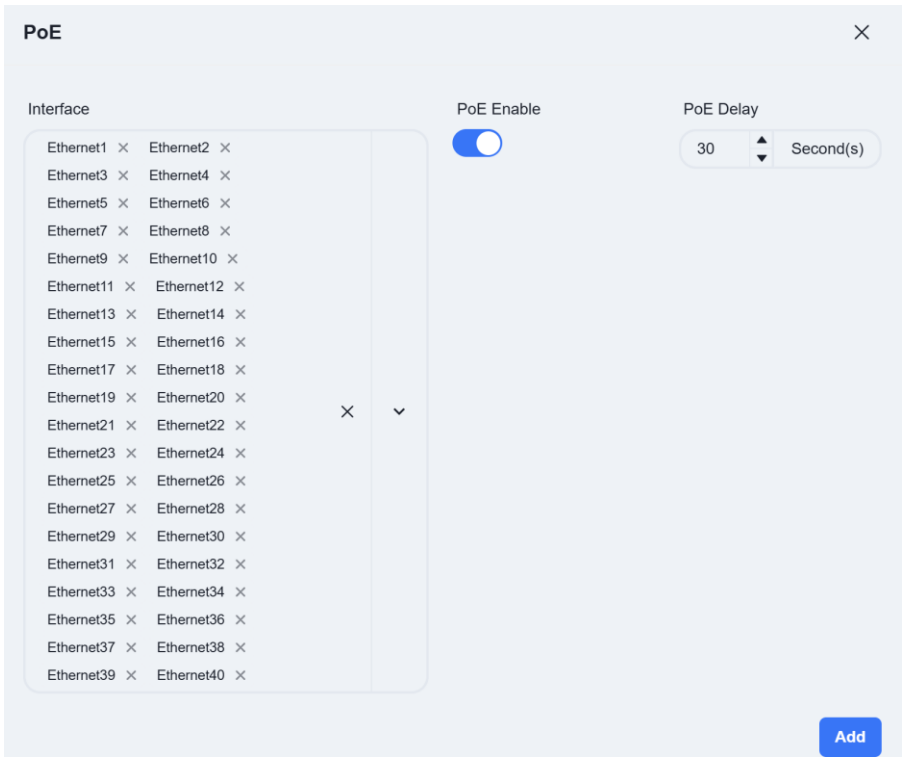
2. POE

The access switch features PoE functionality, which can be directly enabled in the wired service configuration to supply power to PD devices.

Click **[Create]**

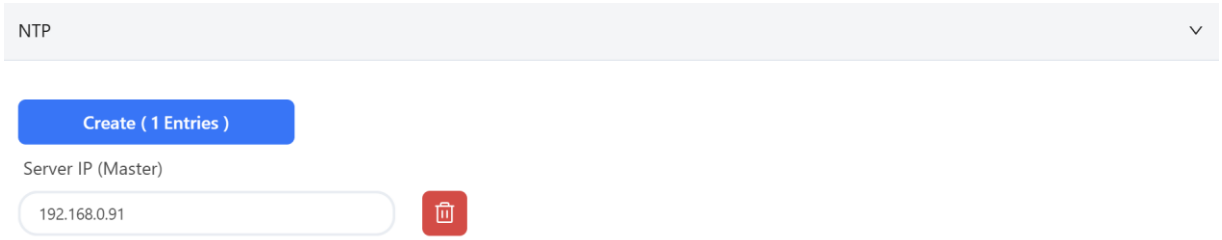


Select the interface where the PoE function is to be enabled and set the startup delay time.



POE Delay: This refers to a brief, intentional time delay introduced at a PoE switch port between when it begins to supply power and when it actually delivers power to the Powered Device (PD).

3. Device

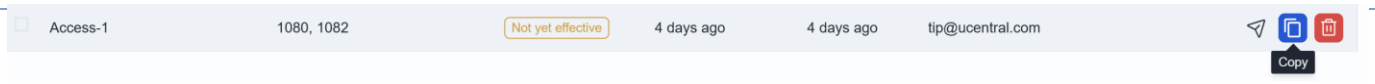


NTP: Configure the NTP server IP address as the Controller's address to provide a unified, accurate, and reliable time reference for the devices.

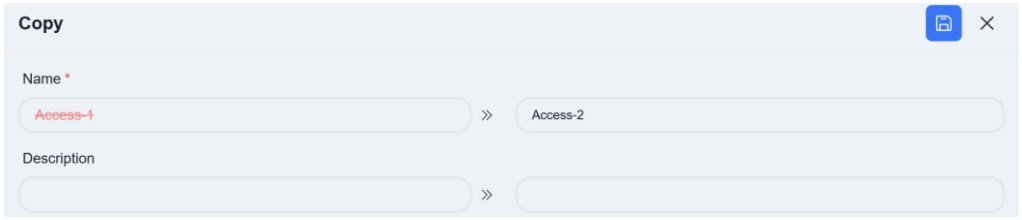
12.4.4.2.2 Access-2

The configuration for Access-2 is identical to that of Access-1. Users can complete the entire setup by copying the configuration from Access-1 and then making targeted modifications.

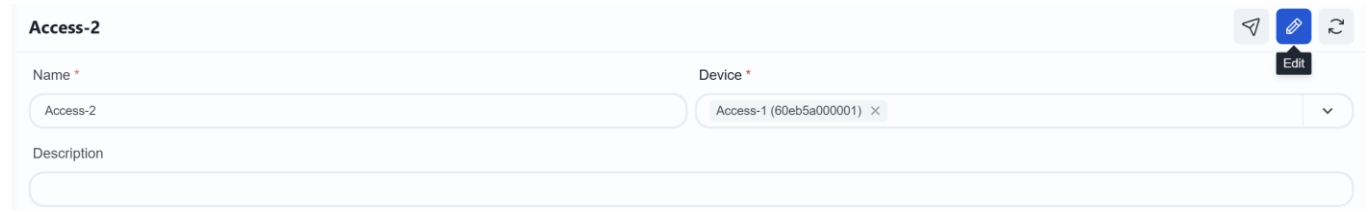
Click the **[Copy]** button on the right.



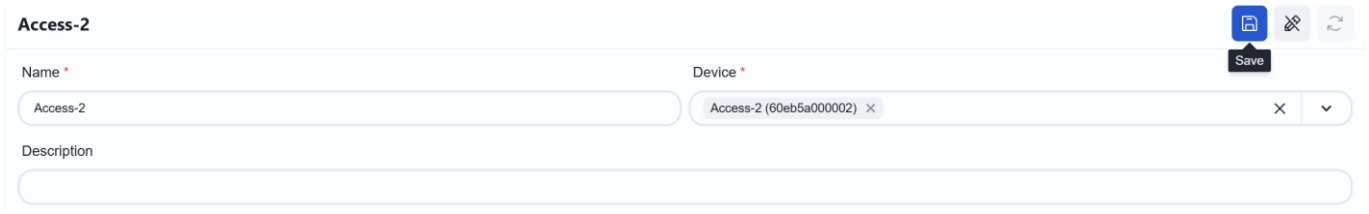
Change the configuration name and click **[Save]**



Click the **[Edit]** button on the right.



Change the device to Access-2. Once completed, click **[Save]** on the right.

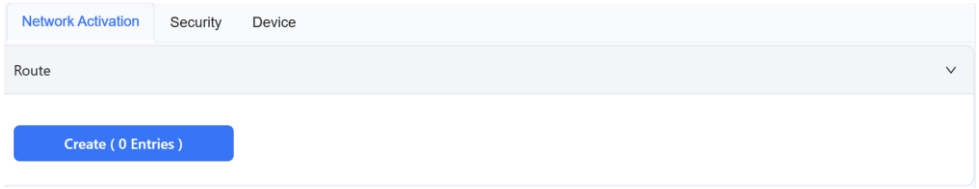


12.4.4.2.3 Access-3

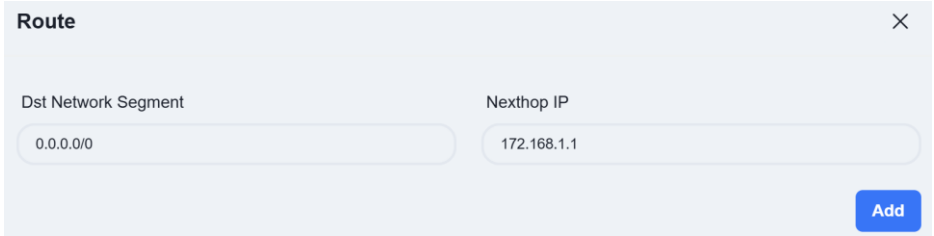
Deploy the wired service configuration on the Access-3 and deploy the wired service gateway.

1. Configuring Routing

Click **[Create]**

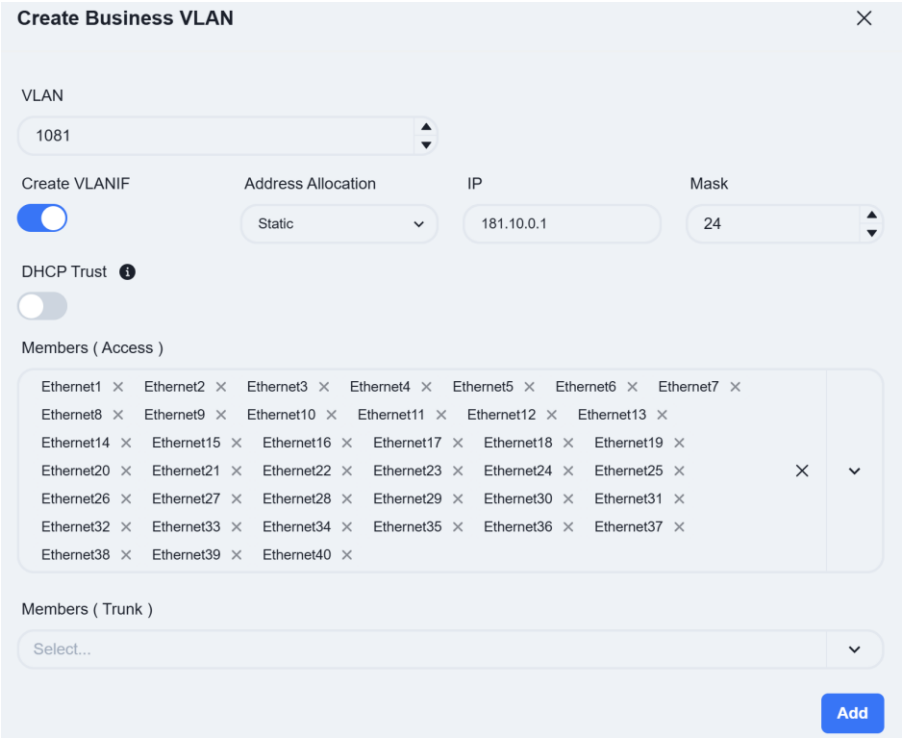


In this scenario, the Access device supports connecting to external networks by configuring static routes. To ensure normal network operation, a default route typically needs to be configured. The next-hop IP should be the uplink address of the Access device. Once completed, click **[Add]**



2. Configure Business VLAN

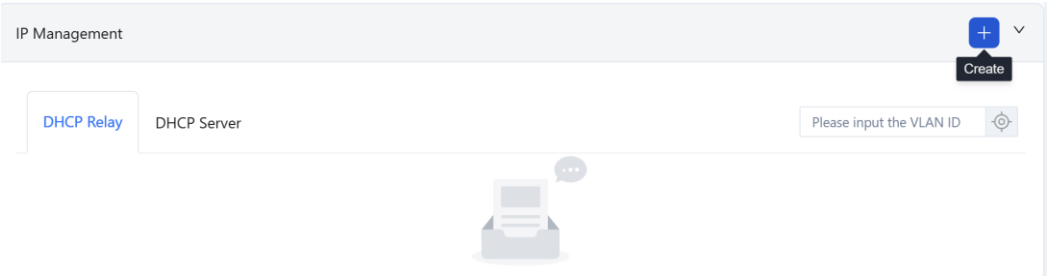
If the gateway is deployed on the Access device, you need to enable **[Create VLANIF]** when creating the service VLAN and fill in the **[IP]** address as the gateway for this service.



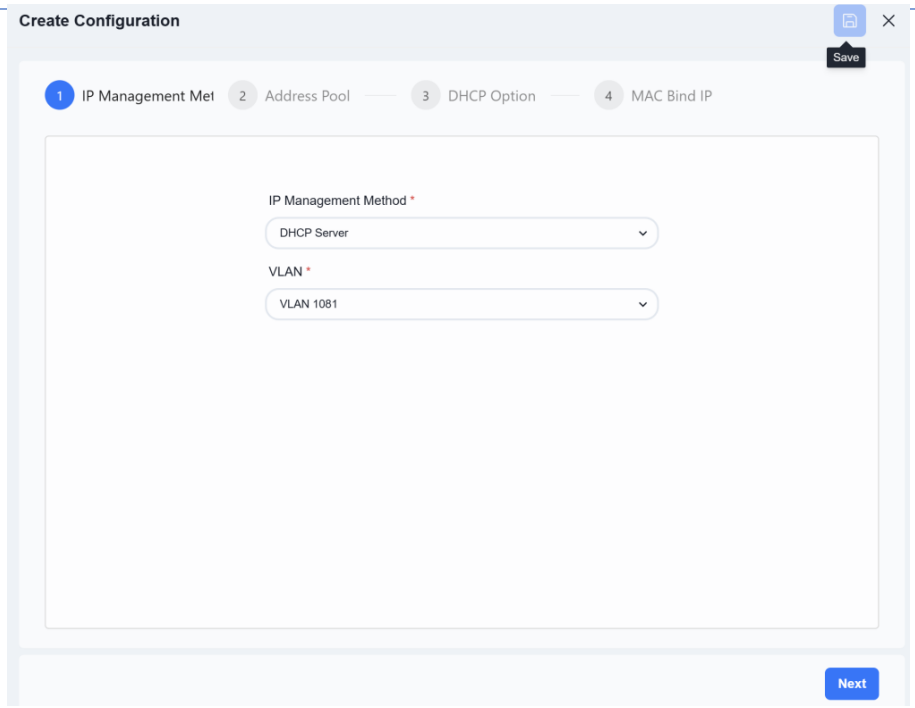
3. DHCP Server

The Open Cloud Connect scenario supports the deployment of a DHCP local service on Access devices.

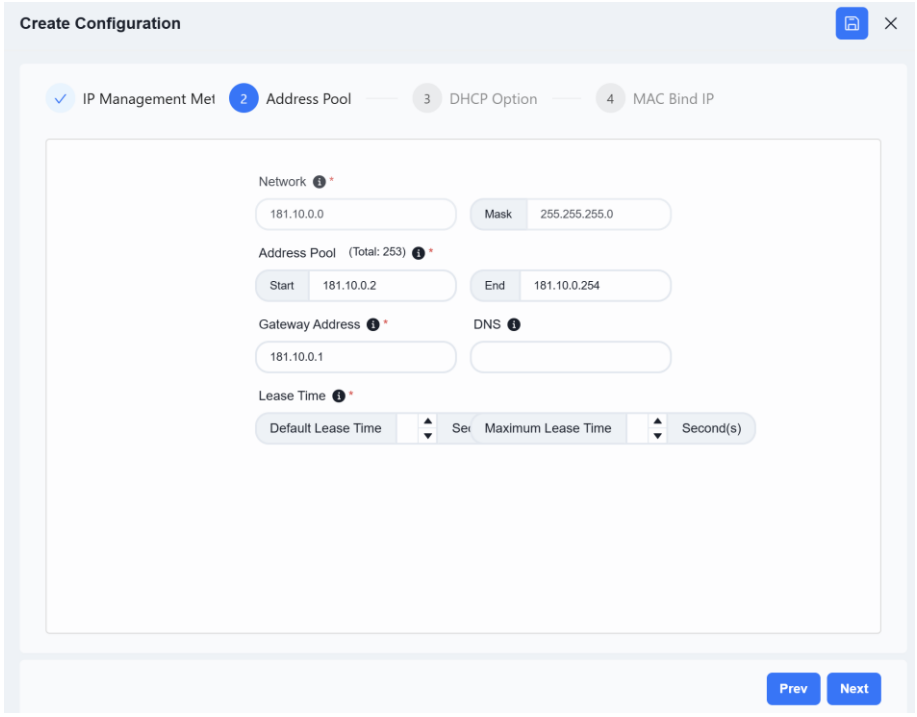
Click **[Create]** on the right side of IP Management.



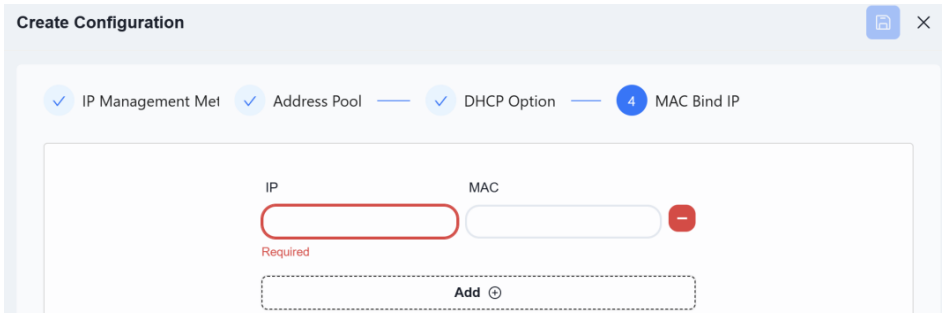
Select the IP Management method as **[DHCP Server]**, choose VLAN as the wired service VLAN 1081, and click **[Next]**



Configure the Network, Address Pool range, Gateway Address, and Lease Time.



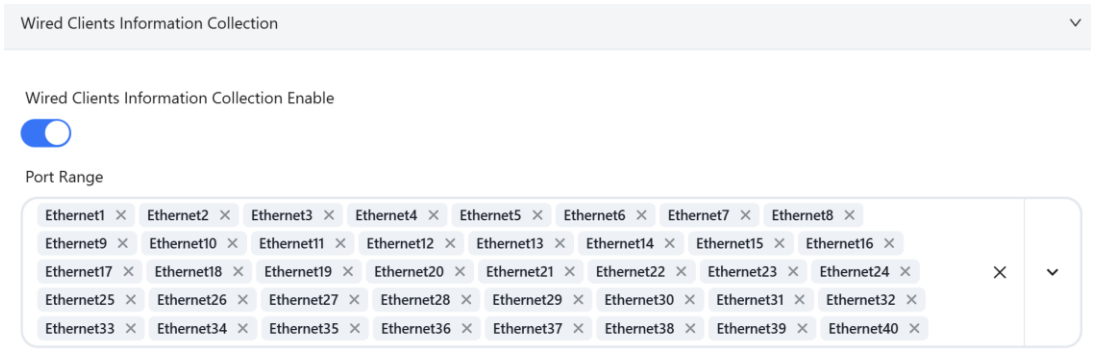
Configure MAC Bind IP (Optional). Once all configurations are complete, click **[Save]** in the upper-right corner.



Once all configurations are complete, click **[Save]** to finalize the Access-3 setup.

4. Wired Clients Information Collection

Interfaces with this feature enabled will report information about the connected wired terminals to the controller.



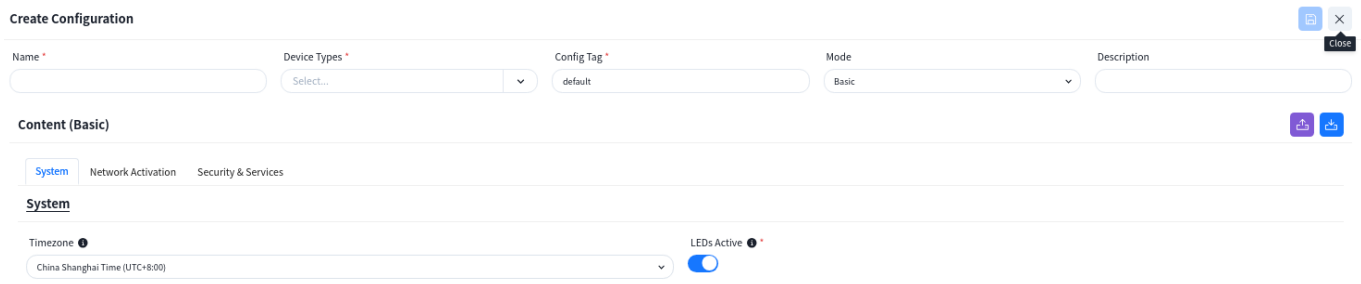
5. Device Management

Same as Access-1

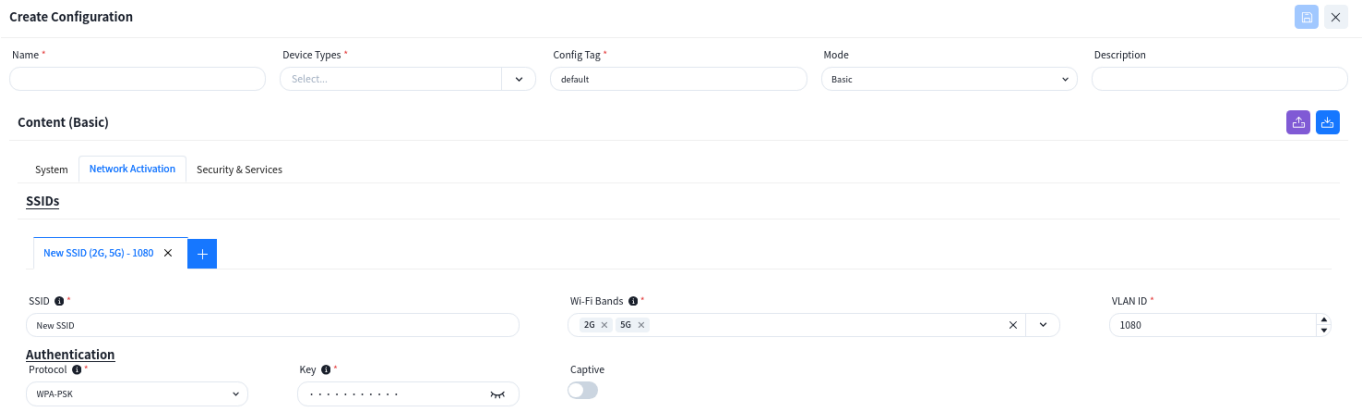
12.4.4.3 Wi-Fi Configuration

Click **[Wi-Fi Configuration] - [+]** to configure the necessary basic information for the wireless AP, e.g. SSID settings, security policy. The controller can automatically generate the corresponding

The controller supports the configuration of different wireless service configurations, and after the AP goes online, it will determine which configuration should be issued to the AP based on the **[Config Tag]** attributes of the configuration.

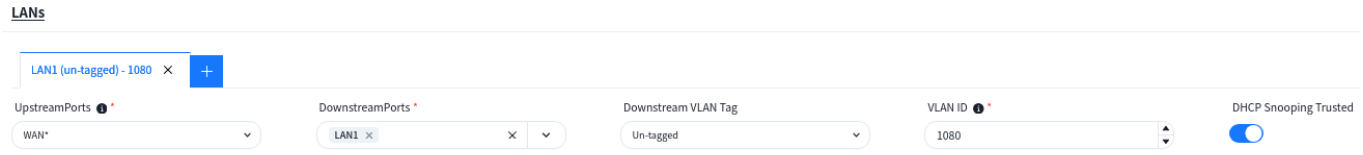


12.4.4.3.1 SSID



12.4.4.3.2 LAN(Optional)

When the AP is one that has an extended wired interface and is capable of accessing terminals by wired means, such as a panel AP, the user can configure the access method for wired terminals through the configuration in LANs.



UpstreamPorts: Specify the up-link interfaces for wired terminal to access the network through AP, usually it is the interface for AP to connect to the switch, and keep the same with **[UpstreamPorts]** in **[SSID]** – **[Advanced]** Settings, the default is: WAN*.

DownstreamPorts: Interfaces for wired terminal access.

Downstream VLAN Tag: Whether the wired terminal carries VLAN Tag.

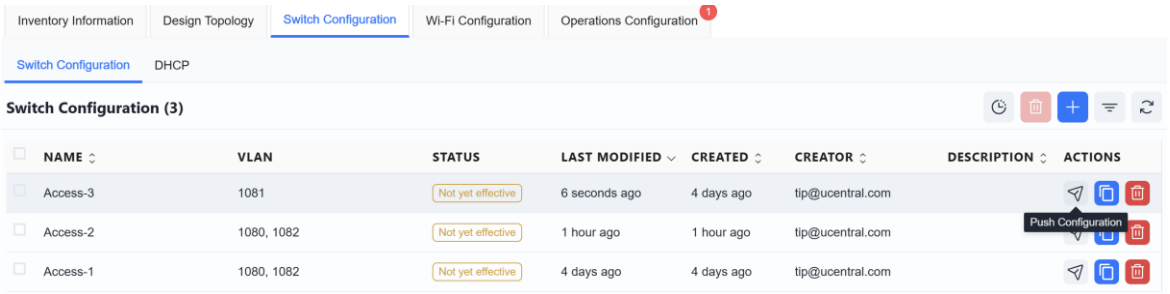
VLAN ID: The AP receives messages from wired terminals that add this VLAN TAG to identify.

DHCP Snooping Trusted: DHCP Snooping Trusted interface, if the wired terminal needs to obtain IP address through DHCP service, this switch needs to be on.

12.4.5 Configuration Release

12.4.5.1 Switch

On the **[Configuration]**-**[Switch Configuration]** view, select the configuration to be deployed and click the **[Push Configuration]** button.



In the pop-up window, click **[Next]**-**[Start]** to deploy the switch configuration to the switch.

12.4.5.2 AP

The AP does not need to manually issue the configuration. After the configuration of the device is issued and takes effect, the PoE power supply function of the switch is turned on, and the AP can power on and work. When the AP connects to the controller with the information obtained through the DHCP service, the controller will automatically send the configuration to the corresponding AP based on the comparison between the TAG identification stored in the AP inventory and the TAG identification in the planning configuration.