Ruijie Reyee RG-NBS, комутатори серії NIS3100 ReyeeOS 2.320[300].

Посібник з конфігурації

Версія документа: V1.1 Дата: 6 січня 2025 року
Авторське право© 2025 Ruijie Networks

Авторське право

Авторське право© 2025 Ruijie Networks

Всі права на цей документ і цю заяву захищені.

Без попередньої письмової згоди Ruijie Networks будь-яка організація або фізична особа не має права відтворювати, витягувати, створювати резервні копії, змінювати або поширювати зміст цього документа будь-яким способом або в будь-якій формі, а також перекладати його на інші мови або використовувати окремі або всі частини документа в комерційних цілях.

 та інші логотипи Ruijie Networks є товарними знаками Ruijie Networks.

Усі інші торгові марки або зареєстровані торгові марки, згадані в цьому документі, належать відповідним власникам.

Відмова від відповідальності

Продукти, послуги або функції, які ви купуєте, є предметом комерційних контрактів і умов, і деякі або всі продукти, послуги або функції, описані в цьому документі, можуть бути недоступні придбання або використання. За винятком домовленості в контракті, Ruijie Networks не робить ніяких явних або неявних заяв або гарантій щодо змісту цього документа.

Назви, посилання, описи, скріншоти та будь-яка інша інформація про стороннє програмне забезпечення, згадані в цьому документі, надаються лише для ознайомлення. Ruijie Networks прямо чи опосередковано не схвалює і не рекомендує використання будь-якого стороннього програмного забезпечення, а також не надає жодних запевнень чи гарантій щодо застосовності, безпеки чи законності такого програмного забезпечення. Ви повинні вибирати і використовувати стороннє програмне забезпечення основі ваших бізнес-вимог і отримати відповідний дозвіл. Ruijie Networks не несе відповідальності за будь-які ризики або збитки, що виникають внаслідок використання вами стороннього програмного забезпечення.

Зміст цього документа буде час від часу оновлюватися у зв'язку з оновленням версії продукту або з інших причин, Ruijie Networks залишає за собою право змінювати зміст документа без будь-якого повідомлення або підказки.

Цей посібник розроблений виключно як керівництво користувача. Компанія Ruijie Networks зробила все можливе, щоб забезпечити точність і надійність змісту при складанні цього посібника, але вона не гарантує, що зміст посібника повністю вільний від помилок або упущень, і вся інформація в цьому посібнику не становить жодних явних або неявних гарантій.

Передмова

Цільова аудиторія

Цей документ призначений для:

- Мережевих інженерів
- Інженери з технічної підтримки та обслуговування
- Мережеві адміністратори

Технічна підтримка

- Офіційний веб-сайт Ruijie Reyee: https://reyee.ruijie.com
- Веб-сайт технічної підтримки: https://reyee.ruijie.com/en-global/support
- Портал кейсів: https://www.ruijienetworks.com/support/caseportal
- Спільнота: https://community.ruijienetworks.com
- Електронна пошта технічної підтримкиservice_rj@ruijienetworks.com
- Онлайн-робот/живий чат: https://reyee.ruijie.com/en-global/rita

Домовленості

1. Символи графічного інтерфейсу

Символ інтерфейсу	Опис	Приклад
Жирний шрифт	1. Назви кнопок 2. Назви вікон, назви вкладок, назви полів та пунктів меню 3. Посилання	1. Натисни **ОК**. 2. Виберіть **Майстер конфігурації**. 3. Натисніть на посилання **Завантажити файл**.
>	Багаторівневі пункти меню	Виберіть **Система**> **Час**.

2. Знаки

Знаки, що використовуються в цьому документі, описуються наступним чином:

Попередження

Сповіщення, яке привертає увагу до важливих правил та інформації, нерозуміння або недотримання яких може призвести до втрати даних або пошкодження обладнання.

Застереження

Сповіщення, яке привертає увагу до важливої інформації, нерозуміння або недотримання якої може призвести до збою в роботі або погіршення продуктивності.

Примітка

Попередження, яке містить додаткову або додаткову інформацію, нерозуміння або невиконання якої не призведе до серйозних наслідків.

Специфікація

Сповіщення, яке містить опис підтримки продукту або версії.

3. Примітка

Інформація про конфігурацію (включаючи модель, опис, тип порту, програмний інтерфейс) наведена в посібнику лише для ознайомлення. У разі будь-яких розбіжностей або невідповідностей між посібником та актуальною версією, актуальна версія має переважну силу.

Зміст

1 Опис Змін

У цьому розділі описано основні зміни у програмному та апаратному забезпеченні різних версій, а також відповідну документацію. Детальнішу інформацію про зміни в апаратному забезпеченні див. у примітках до випуску, що публікуються разом з версіями програмного забезпечення.

1.1 ReyeeOS 2.320

1.1.1 Апаратне забезпечення Зміна

ReyeeOS 2.320 є оновленням ReyeeOS 2.300. У наступній таблиці перераховані нові сумісні моделі обладнання, на яких працює ReyeeOS 2.320.

Модель	Апаратна версія
RG-NBS3100-8GT2SFP	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x
RG-NBS3100-48GT4SFP-P	1.0x, 1.1x, 1.2x
RG-NBS3100-24GT4SFP-P-V2	1.0x, 1.1x, 1.2x
RG-NBS3100-24GT4SFP-V2	1.0x, 1.1x
RG-NBS3100-8GT2SFP-P-V2	1.0x
RG-NIS3100-8GT4SFP-HP	1.0x, 1.1x, 1.2x
RG-NIS3100-8GT2SFP-HP	1.0x, 1.1x, 1.2x
RG-NIS3100-4GT2SFP-HP	1.0x, 1.1x, 1.2x
RG-NBS3200-24GT4XS	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 1.7x, 2.0x, 2.1x, 2.2x
RG-NBS3200-48GT4XS	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 2.0x, 2.1x, 2.2x
RG-NBS3200-24SFP/8GT4XS	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x
RG-NBS3200-24GT4XS-P	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 2.0x, 2.1x, 2.2x
RG-NBS3200-48GT4XS-P	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 2.0x, 2.1x, 2.2x
RG-NBS5100-24GT4SFP	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 2.0x, 2.1x, 2.2x, 2.3x, 2.4x
RG-NBS5100-48GT4SFP	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 2.0x, 2.1x, 2.2x
RG-NBS5100-24GT4SFP-P	1.0x, 1.1x, 1.2x
RG-NBS5200-24GT4XS	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 2.0x, 2.1x, 2.2x, 2.3x, 2.4x
RG-NBS5200-48GT4XS	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 2.0x, 2.1x, 2.2x
RG-NBS5200-24SFP/8GT4XS	1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 2.0x, 2.1x, 2.2x
RG-NBS5200-24GT4XS-P	1.0x, 1.1x, 1.2x

Модель	Апаратна версія
RG-NBS5200-48GT4XS-UP	1.0x, 1.1x
RG-NBS5300-8MG2XS-UP	1.0x

1.1.2 Функція програмного забезпечення Зміна

Ця версія має наступні зміни та нові можливості програмного забезпечення на базі ReyeeOS 2.300:

1. Змінено функцію — Покращено максимальну кількість агрегатних інтерфейсів

- До змін:
  На комутаторах серій RG-NBS7006, RG-NBS7003, RG-NBS6002, RG-NBS5300, RG-NBS5200 і RG-NBS5100 можна налаштувати максимум 16 агрегованих інтерфейсів.
- Після зміни:
  На комутаторах RG-NBS7006 і RG-NBS7003 можна налаштувати до 128 агрегованих інтерфейсів, а на комутаторах серій RG-NBS6002, RG-NBS5300, RG-NBS5200 і RG-NBS5100 можна налаштувати до 64 агрегованих інтерфейсів.

Детальніше див. у розділі 7.3.3 Конфігурація агрегованого інтерфейсу.

2. Змінено функцію — Відображення фізичних портів, що відповідають MAC-адресам, на сторінці списку ARP

- До змін:
  Комутатори RG-NBS7006, RG-NBS7003 і RG-NBS6002 підтримують відображення фізичних портів, що відповідають MAC-адресам на сторінці списку ARP.
- Після зміни:
  Серії RG-NBS7006, RG-NBS7003, RG-NBS6002, RG-NBS5300, RG-NBS5200 і RG-NBS5100 підтримують відображення фізичних портів, що відповідають MAC-адресам, на сторінці списку ARP.

Докладні відомості див. у розділі 10.6 Налаштування статичного ARP-запису та 15.1.5 ARP-списку.

3. Нова функція Увімкнення LACP на агрегованих інтерфейсах рівня 3

Ця версія підтримує функцію LACP на агрегованих інтерфейсах рівня 3. Докладні відомості див. у розділі 10.1 Налаштування інтерфейсу рівня 3.

4. Нова функція MSTP

Ця версія підтримує протокол Multiple Spanning Tree Protocol (MSTP). Докладні відомості наведено у розділі 14.1.2 Налаштування MSTP.

5. Нова функція Перегляд та налаштування журналу

Ця версія підтримує перегляд і налаштування журналу. Докладні відомості наведено у розділі 16.1 Системні журнали.

1.2 ReyeeOS 2.300

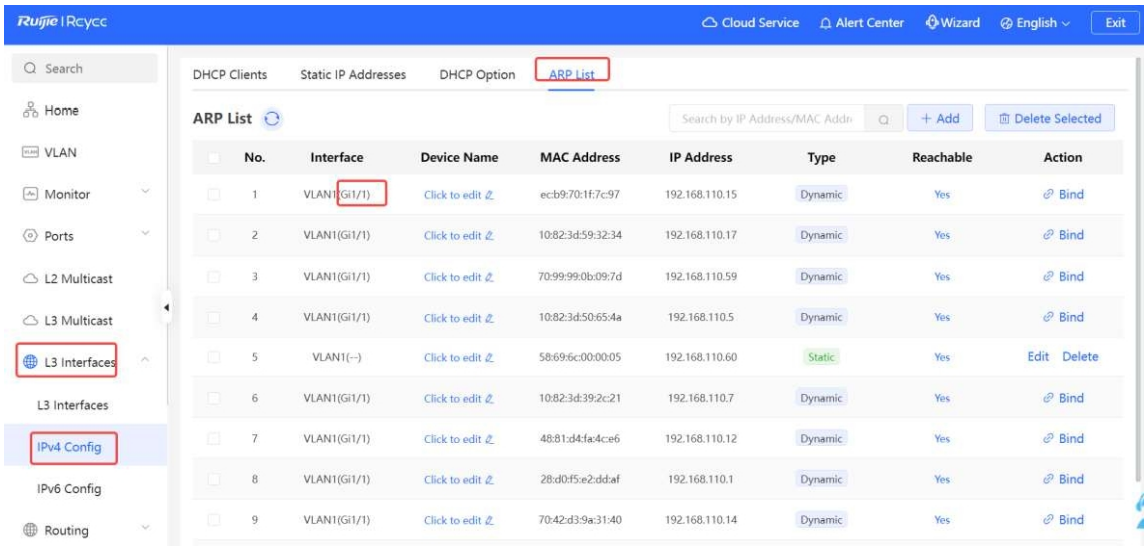
1.2.1 Апаратне забезпечення Зміна

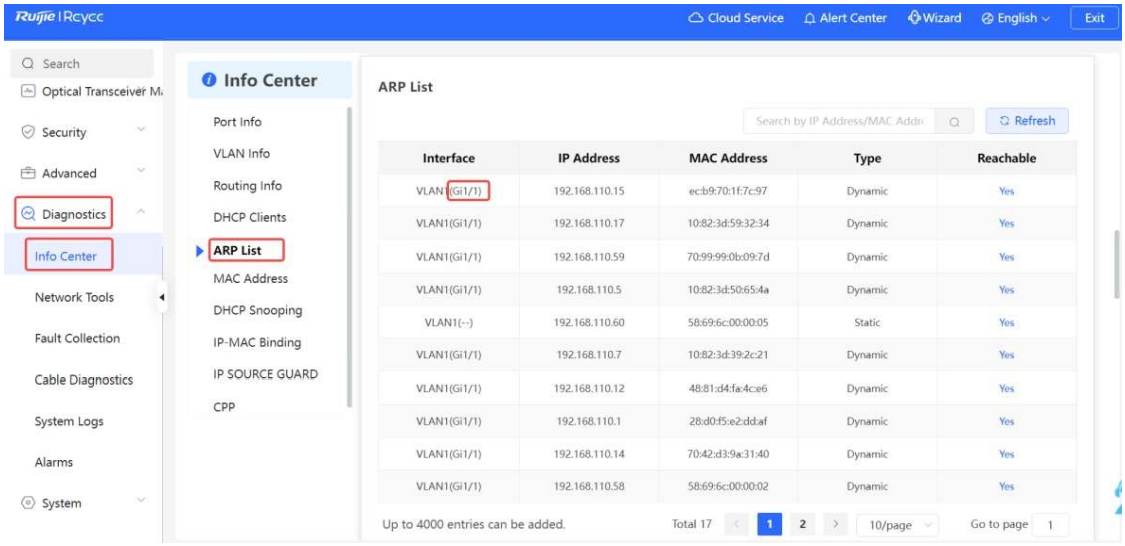
У наступній таблиці перелічено відповідні моделі апаратного забезпечення для цієї версії.

Модель	Апаратна версія
RG-NBS6002	● Шасі: 1.0x, 2.0x ● Лінійна карта: o M6000-24GT2XS: 1.0x, 2.0x o M6000-24SFP2XS: 1.0x o M6000-16GT8SFP2XS: 1.0x, 2.0x o M6000-16SFP8GT2XS: 1.0x, 2.0x
RG-NBS7003	● Шасі: 1.0x ● Line Card: o M7000-48GT2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x M7000- o 24GT24SFP2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x M7000- o 48SFP2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x M7000-8XS-EA: o 1.0x, 1.1x, 1.2x, 2.0x o M7000-24GT2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x o M7000-24SFP2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x o M7000-16XS-EA: 1.0x, 1.1x, 2.0x
RG-NBS7006	● Шасі: 1.0x ● Line Card: o M7000-48GT2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x M7000- o 24GT24SFP2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x M7000- o 48SFP2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x M7000-8XS-EA: o 1.0x, 1.1x, 1.2x, 2.0x o M7000-24GT2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x o M7000-24SFP2XS-EA: 1.0x, 1.1x, 1.2x, 2.0x o M7000-16XS-EA: 1.0x, 1.1x, 2.0x o M7006-CM: 1.0x, 1.1x, 2.0x

1.2.2 Функція програмного забезпечення Зміна

У цій версії ви можете переглянути фізичний інтерфейс, що відповідає MAC-адресам, на сторінці ARP-списку. Для отримання докладнішої інформації див. розділи 10.6 Налаштування статичного ARP-запису і 15.1.5 Список ARP.


Ruijie | Reyee
Cloud Service
Alert Center
Wizard
English
Exit
Search
Home
VLAN
Monitor
Ports
L2 Multicast
L3 Multicast
L3 Interfaces
L3 Interfaces
IPv4 Config
IPv6 Config
Routing
DHCP Clients
Static IP Addresses
DHCP Option
ARP List
ARP List
Search by IP Address/MAC Addr
+ Add
Delete Selected
No.
Interface
Device Name
MAC Address
IP Address
Type
Reachable
Action
1 VLAN1(Gi1/1) Click to edit ec:b9:70:1f:7c:97 192.168.110.15 Dynamic Yes Bind
2 VLAN1(Gi1/1) Click to edit 10:82:3d:59:32:34 192.168.110.17 Dynamic Yes Bind
3 VLAN1(Gi1/1) Click to edit 70:99:99:0b:09:7d 192.168.110.59 Dynamic Yes Bind
4 VLAN1(Gi1/1) Click to edit 10:82:3d:50:65:4a 192.168.110.5 Dynamic Yes Bind
5 VLAN1(--) Click to edit 58:69:6c:00:00:05 192.168.110.60 Static Yes Edit Delete
6 VLAN1(Gi1/1) Click to edit 10:82:3d:39:2c:21 192.168.110.7 Dynamic Yes Bind
7 VLAN1(Gi1/1) Click to edit 48:81:d4:fa:4c:e6 192.168.110.12 Dynamic Yes Bind
8 VLAN1(Gi1/1) Click to edit 28:d0:f5:e2:dd:af 192.168.110.1 Dynamic Yes Bind
9 VLAN1(Gi1/1) Click to edit 70:42:d3:9a:31:40 192.168.110.14 Dynamic Yes Bind


Ruijie | Reyee
Cloud Service
Alert Center
Wizard
English
Exit
Search
Optical Transceiver M
Security
Advanced
Diagnostics
Info Center
Network Tools
Fault Collection
Cable Diagnostics
System Logs
Alarms
System
Info Center
Port Info
VLAN Info
Routing Info
DHCP Clients
ARP List
MAC Address
DHCP Snooping
IP-MAC Binding
IP SOURCE GUARD
CPP
ARP List
Search by IP Address/MAC Addr
Refresh
Interface
IP Address
MAC Address
Type
Reachable
VLAN1(Gi1/1) 192.168.110.15 ec:b9:70:1f:7c:97 Dynamic Yes
VLAN1(Gi1/1) 192.168.110.17 10:82:3d:59:32:34 Dynamic Yes
VLAN1(Gi1/1) 192.168.110.59 70:99:99:0b:09:7d Dynamic Yes
VLAN1(Gi1/1) 192.168.110.5 10:82:3d:50:65:4a Dynamic Yes
VLAN1(--) 192.168.110.60 58:69:6c:00:00:05 Static Yes
VLAN1(Gi1/1) 192.168.110.7 10:82:3d:39:2c:21 Dynamic Yes
VLAN1(Gi1/1) 192.168.110.12 48:81:d4:fa:4c:e6 Dynamic Yes
VLAN1(Gi1/1) 192.168.110.1 28:d0:f5:e2:dd:af Dynamic Yes
VLAN1(Gi1/1) 192.168.110.14 70:42:d3:9a:31:40 Dynamic Yes
VLAN1(Gi1/1) 192.168.110.58 58:69:6c:00:00:02 Dynamic Yes
Up to 4000 entries can be added.
Total 17
1
2
10/page
Go to page 1

2 Вхід

2.1 Конфігураційне середовище Вимоги

- Підтримуються Google Chrome, Internet Explorer 9.0, 10.0 та 11.0, а також деякі браузери на основі ядра Chromium/Internet Explorer (наприклад, 360 Extreme Explorer). У разі використання непідтримуваного браузера можуть виникати винятки, такі як символи сміття або помилки формату.
- Рекомендується роздільна здатність 1024 x 768 або вище. При використанні інших роздільних здатностей шрифти і формати сторінок можуть бути не вирівняні, графічний інтерфейс буде менш художнім, або можуть виникнути інші винятки.

2.2 Вхід до веб-інтерфейсу

2.2.1 Підключення до пристрою

За допомогою мережевого кабелю підключіть порт комутатора до мережевого порту комп'ютера і налаштуйте IP-адресу комп'ютера в тому ж сегменті мережі, що і IP-адреса пристрою за замовчуванням, щоб забезпечити можливість пінгування комп'ютера через комутатор. Наприклад, встановіть IP-адресу ПК на 10.44.77.100.

Таблиця 2-1 Налаштування за замовчуванням

Особливість	Значення за замовчуванням
IP-адреса пристрою	10.44.77.200
Пароль	Ім'я користувача не потрібне при вході в систему. Пароль за замовчуванням - admin.

2.2.2 Вхід до веб-інтерфейсу

(1) Введіть IP-адресу пристрою (10.44.77.200 за замовчуванням) в адресному рядку браузера, щоб відкрити сторінку входу.

Примітка

Якщо статична IP-адреса пристрою змінюється або пристрій динамічно отримує нову IP-адресу, нову IP-адресу можна використовувати для доступу до веб-системи керування пристроєм, якщо комп'ютер і пристрій знаходяться в одній локальній мережі, а їхні IP-адреси - в одному сегменті мережі.

(2) Введіть пароль і натисніть "Увійти", щоб відкрити домашню сторінку веб-системи управління.

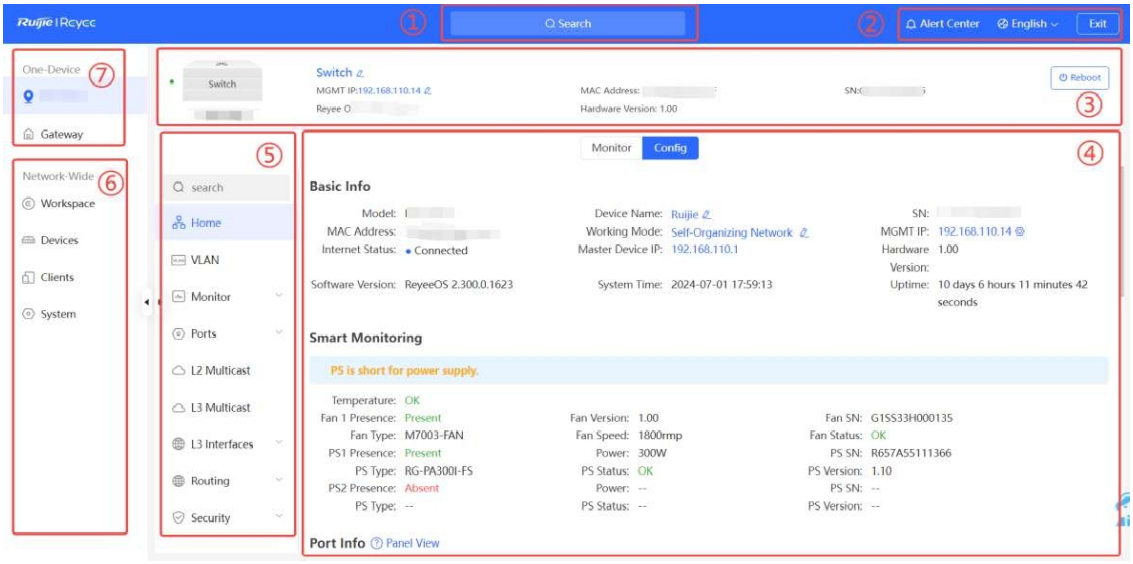
Для входу на пристрій можна використовувати пароль за замовчуванням admin. З міркувань безпеки рекомендується змінити пароль за замовчуванням якомога швидше після входу в систему, а потім регулярно оновлювати його.

Якщо ви забули IP-адресу або пароль, утримуйте кнопку **Reset** панелі пристрою більше 5 секунд, коли пристрій підключено до джерела живлення, щоб відновити заводські налаштування. Після відновлення ви можете використовувати IP-адресу та пароль за замовчуванням для входу в систему.

Застереження

- Відновлення заводських налаштувань призведе до видалення всіх конфігурацій пристрою. Тому будьте обережні при виконанні цієї операції.
- Спосіб відновлення заводських налаштувань залежить від моделі пристрою. Детальніше див. у посібнику з інсталяції пристрою.

2.2.3 Макет Конфігурація



Таблиця 2-2 Конфігурація макета Конфігурація

Ні.	Опис
1	Навігація часто використовуваними функціями пристрою, включно з мережею, шлюзом і функціями, пов'язаними з пристроєм і системою
2	Швидкий перегляд тривог пристрою, зміна мови сторінки Eweb та вихід з Eweb
3	Інформація про пристрій та кнопка перезавантаження пристрою
4	Конфігурація функцій пристрою та область відображення. Натисніть **Монітор**, щоб відобразити трафік інтерфейсу та споживання енергії PoE пристрою (цю функцію підтримують лише комутатори PoE з назвами моделей, що містять P, -LP, -HP та -UP). Натисніть **Конфігурація**, щоб переглянути конфігурацію та робочий стан пристрою
5	Панель навігації розташовується вертикально зліва, коли вона слугує головним пристроєм, і горизонтально зверху, коли вона слугує підлеглим пристроєм
6	Групові налаштування можна застосувати до загальновживаних функцій усіх дротових і бездротових пристроїв Reyee в мережі, що самоорганізується.
7	Дозволяє конфігурувати всі функції локального пристрою, а також швидко налаштувати шлюз

2.3 Швидке налаштування

2.3.1 Конфігурація Підготовка

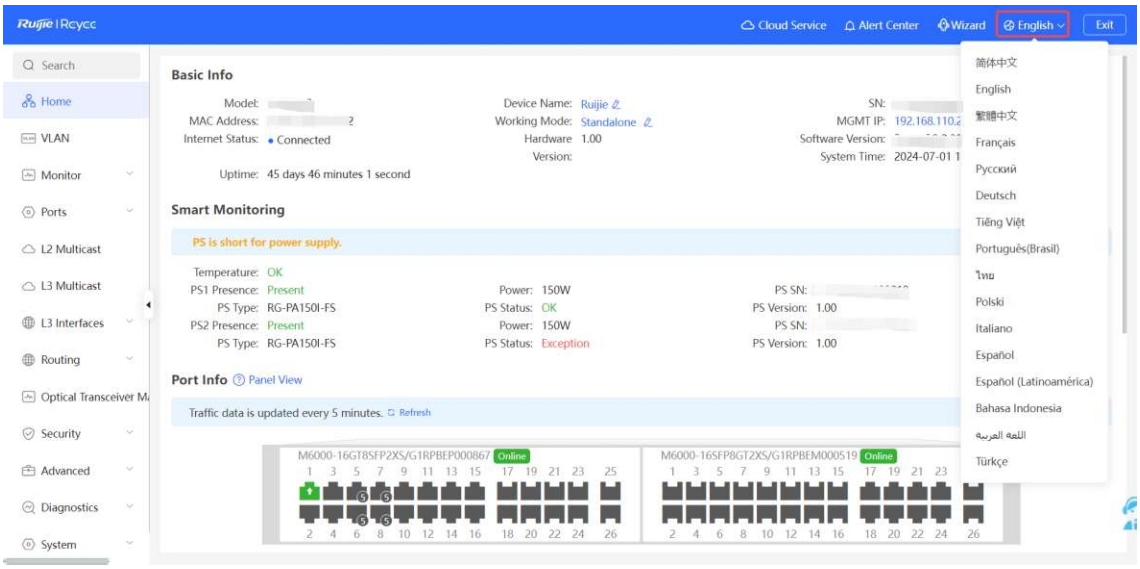
Підключіть пристрій до джерела живлення та з'єднайте порт пристрою з пристроєм висхідної лінії зв'язку за допомогою мережевого кабелю.

2.3.2 Процедура

1. Змінити мову веб-інтерфейсу

Натисніть **англійську** мову у верхньому правому куті веб-інтерфейсу.

Виберіть потрібну мову зі спадного меню, щоб змінити мову веб-інтерфейсу.



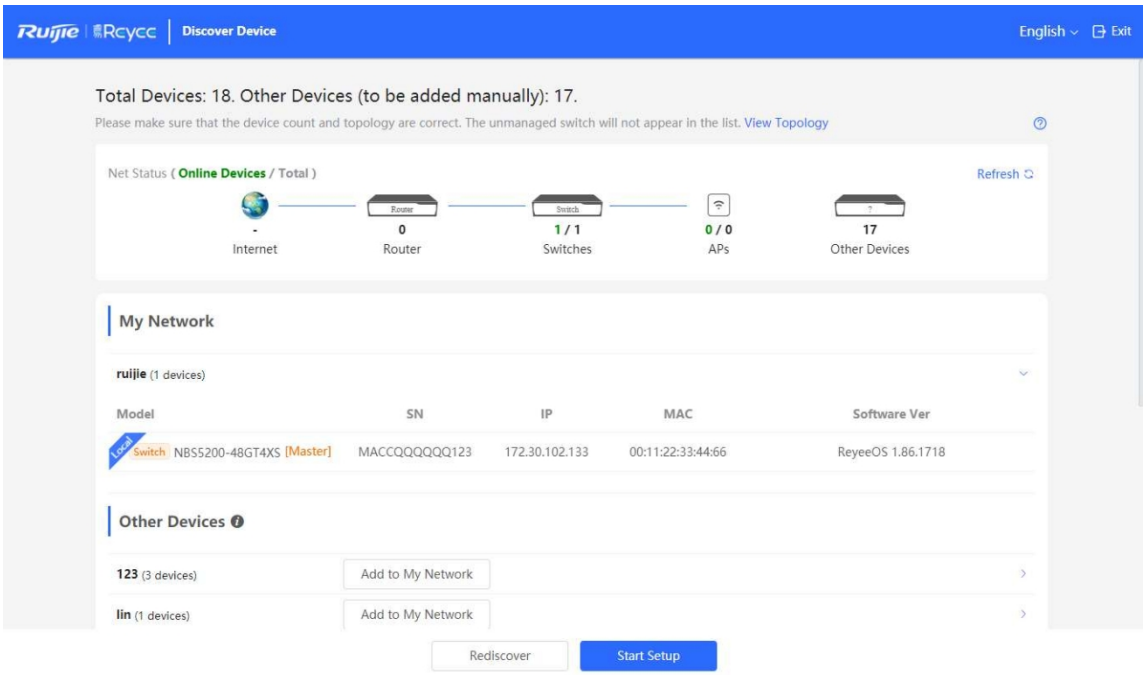
2. Додавання пристрою до мережі

За замовчуванням користувачі можуть виконувати пакетні налаштування і централізовано керувати всіма пристроями в мережі. Тому перед початком налаштування необхідно перевірити та підтвердити кількість пристроїв у мережі та стан мережі в режимі онлайн.

Примітка

За звичайних обставин, коли кілька нових пристроїв вмикаються і підключаються, вони автоматично об'єднуються в мережу, і користувачеві потрібно лише підтвердити, що кількість пристроїв є правильною.

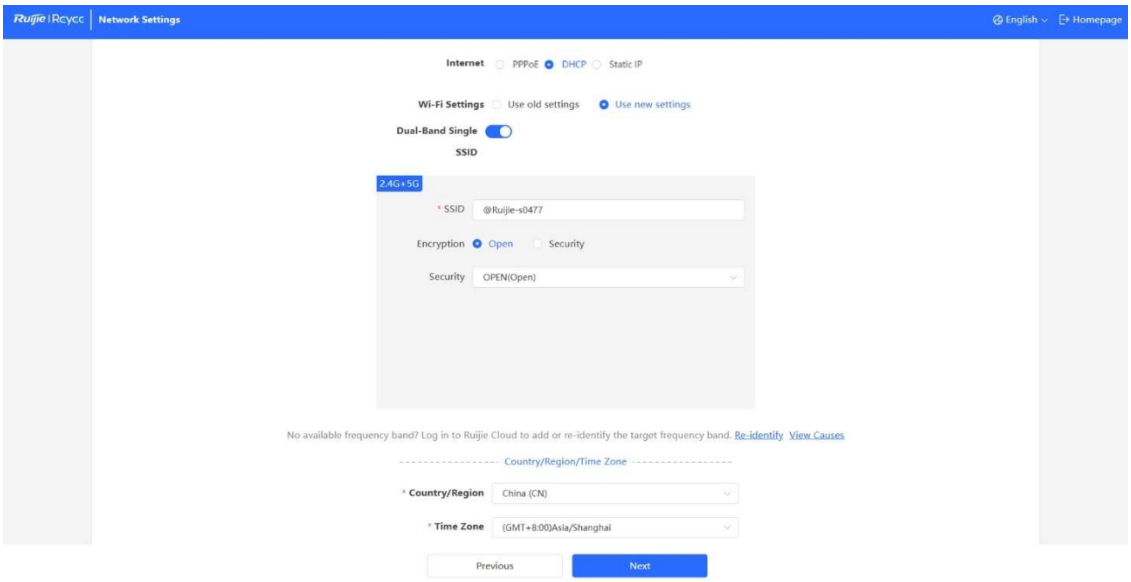
Якщо у мережі є інші пристрої, які не додано до поточної мережі, ви можете додати їх вручну, натиснувши [**Робоча** область/Швидке налаштування/Додати **до моєї мережі**] у розділі Мережа в цілому і ввівши пароль керування кожного пристрою. Після цього відповідні пристрої буде включено до відповідної мережі, що дозволить вам продовжити конфігурацію всієї мережі.



3. Створення веб-проекту

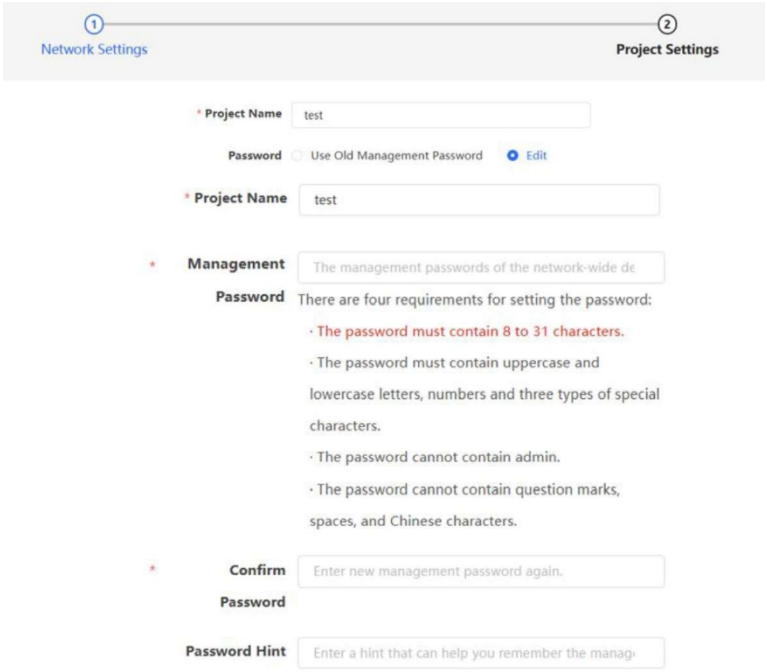
(1) Натисніть **Почати налаштування**, щоб налаштувати тип підключення до Інтернету.

- **Інтернет**: Налаштуйте тип підключення до Інтернету відповідно до вимог місцевого постачальника послуг Інтернету (ISP).
  - DHCP: за замовчуванням точка доступу визначає, чи може вона отримати IP-адресу через DHCP. Якщо точка доступу успішно підключилася до Інтернету, ви можете натиснути кнопку Далі, не вводячи обліковий запис.
  - PPPoE: Натисніть PPPoE і введіть ім'я користувача, пароль і назву служби. Натисніть Далі.
  - Статична IP-адреса: введіть IP-адресу, маску підмережі, шлюз і DNS-сервер і натисніть Далі.
- **Налаштування Wi-Fi**: Виберіть режим конфігурації Wi-Fi. Цей параметр конфігурації недоступний для нового проекту.
  - Використовувати старі налаштування: Використовувати налаштування Wi-Fi існуючого проекту.
  - Використовувати нові налаштування: Налаштувати мережу Wi-Fi за допомогою нових параметрів.
- **SSID та пароль Wi-Fi**: За замовчуванням пристрій не має пароля Wi-Fi, що вказує на те, що мережа Wi-Fi є відкритою. Рекомендується налаштувати складний пароль, щоб підвищити безпеку мережі.
- **Країна/регіон**: Канал Wi-Fi може відрізнятися в різних країнах. Щоб забезпечити успішний пошук клієнтом мережі Wi-Fi, рекомендується вибирати актуальну країну або регіон.
- **Часовий пояс**: Встановіть системний час. За замовчуванням увімкнено мережевий сервер часу надання послуги часу. Рекомендується вибирати актуальний часовий пояс.

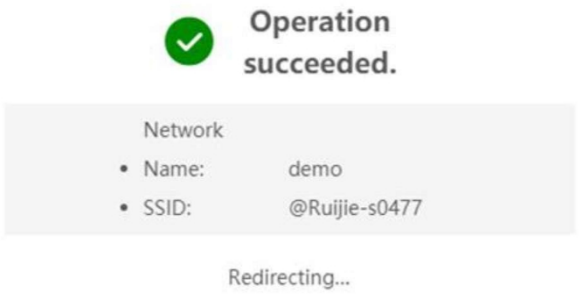


(2) Натисніть "**Далі**". На сторінці, що відобразиться, задайте назву проекту та пароль для керування.

- **Назва проекту**: Визначте мережевий проект, у якому знаходиться пристрій.
- **Пароль управління**: пароль використовується для входу на сторінку управління.



(3) Натисніть **Готово**. Пристрій виконає ініціалізацію і перевірить підключення до мережі.



Тепер пристрій може отримати доступ до Інтернету. Прив'яжіть пристрій облікового запису Ruijie Cloud для віддаленого керування. Дотримуйтесь інструкцій для входу в Ruijie Cloud для подальшого налаштування.

Примітка

- Якщо ваш пристрій не підключено до Інтернету, натисніть **Вийти**, щоб вийти з майстра конфігурації
- Якщо ви змінили пароль керування, будь ласка, увійдіть знову з новим паролем.

2.3.3 Процедура налаштування VCS

VCS підвищує надійність пересилання даних, коли пристрій серії RG-NBS слугує основним комутатором. Два комутатори можуть бути об'єднані в стек, а послуги автоматично переключаються на резервний комутатор, коли активний комутатор виходить з ладу, забезпечуючи безперебійну переадресацію даних у разі однієї несправності.

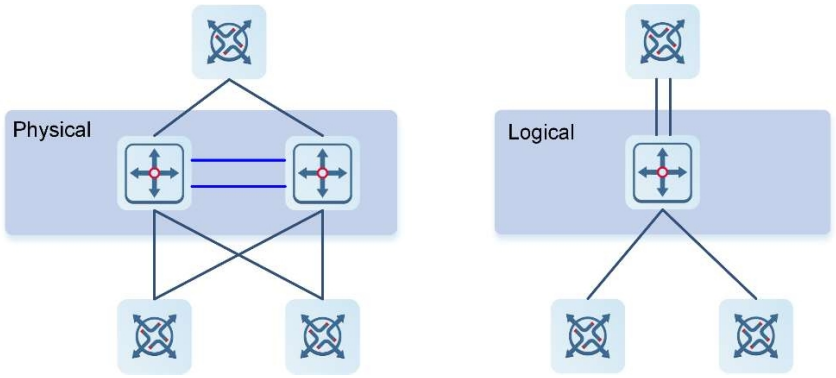
Підтримувані продукти

Цю функцію підтримують лише комутатори серій RG-NBS7006, RG-NBS7003, RG-NBS6002, RG-NBS5300 і RG-NBS5200.

Застереження

- Тільки два комутатори можуть утворювати групу VCS.
- VCS підтримується тільки на комутаторах тієї ж серії. Наприклад, комутатор NBS7003 може групу VCS тільки з іншим комутатором NBS7003, але не з комутатором NBS6002. Слід зазначити, що комутатори NBS7003 і NBS7006, які належать до різних серій, не можуть утворювати групу VCS.
- Комутатори однієї серії, але різних моделей (наприклад, RG-NBS5200-24GT4XS і RG-NBS5200-48GT4XS) можна налаштувати на роботу в режимі гарячого резерву. Якщо два комутатори мають різну ємність, то після конфігурації гарячого резерву переважає менша ємність.
- У режимі гарячого резервного копіювання доступний лише порт MGMT на активному пристрої або основному модулі супервізора.

Стекування: Фізичне з'єднання декількох комутаторів за допомогою стекових кабелів, що дозволяє їм працювати як єдиний логічний блок для пересилання даних.

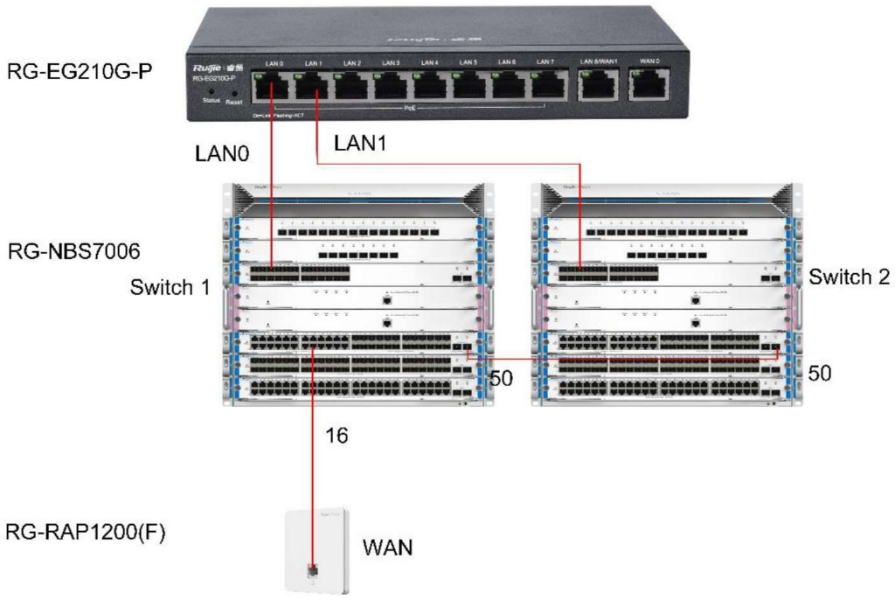


(1) З'єднайте два комутатори кабелями, щоб сформувати групу VCS.

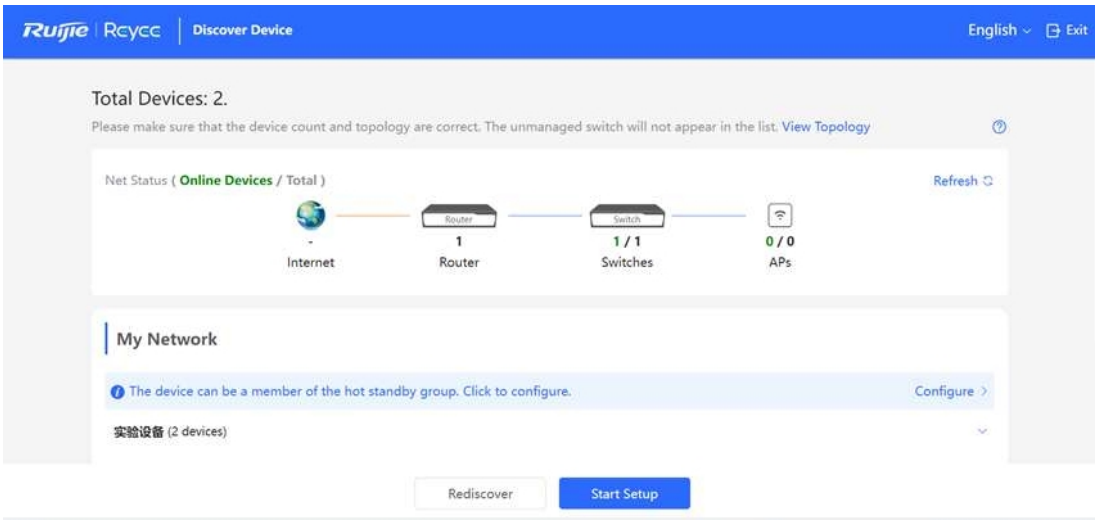
Застереження

Перед налаштуванням VCS між пристроями потрібне лише одне з'єднання, наприклад, з'єднайте порт 50 пристрою 1 з портом 50 пристрою 2, як показано на рисунку 2-1. В іншому випадку може виникнути петля.

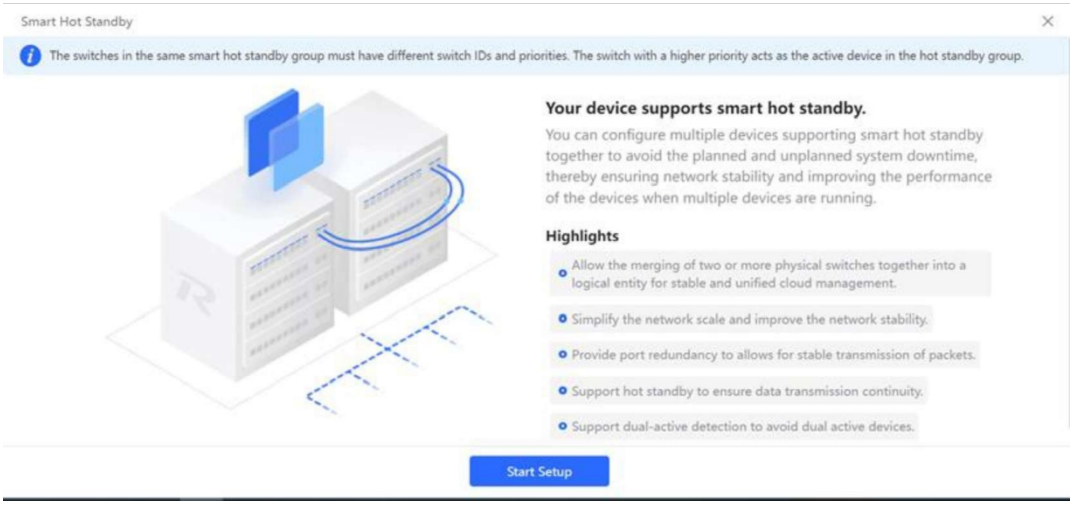
Рисунок 2-1 Підключення комутаторів перед налаштуванням VCS



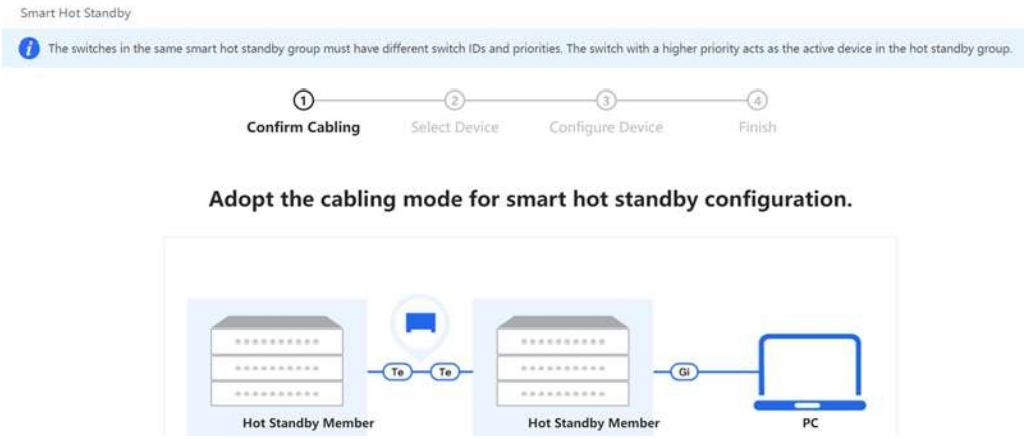
(2) Для доступу до веб-інтерфейсу комутатора RG-NBS введіть в адресному рядку браузера IP-адресу за замовчуванням 10.44.77.200. Натисніть **Налаштувати**.



(3) Натисніть **"Почати налаштування"**.



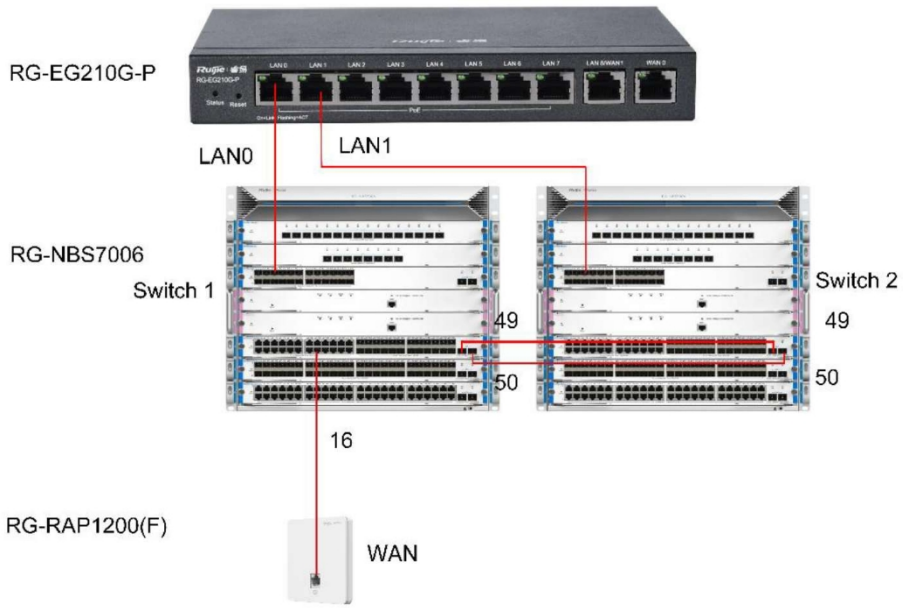
(4) З'єднайте інтерфейси 10GE двох комутаторів за допомогою кабелю (наприклад, з'єднайте інтерфейс 50 пристрою 1 з інтерфейсом 50 пристрою 2, як показано на рисунку 2-1). Потім виберіть **Dual-Device Config** і натисніть **Далі**.



(5) Натисніть перемикач режиму очікування.

(6) Виберіть інший інтерфейс VCS (інтерфейс 49 на наступному малюнку) або декілька інтерфейсів VCS. Рекомендується вибрати два сусідні інтерфейси на комутаторі. На комутаторі вибрати чотирьох інтерфейсів VCS. Ці інтерфейси VCS повинні бути інтерфейсами 10GE. За замовчуванням активний комутатор має пріоритет 200, а резервний - 100. Якщо змінити пріоритет, активним стане комутатор з вищим пріоритетом.

(7) Натисніть "**Далі**". За допомогою кабелю 10GE з'єднайте вибрані вами інтерфейси VCS. (На наступному малюнку показано приклад підключення інтерфейсу 49 пристрою 1 до інтерфейсу 49 пристрою 2).



(8) Після підключення кабелів дотримуйтесь вказівок і дочекайтеся успішного перезавантаження пристрою.

Застереження

Щоб видалити конфігурацію VCS, переконайтеся, що кабель, який з'єднує інтерфейси VCS, від'єднано. Якщо цього не зробити, може утворитися петля, яка призведе до відключення мережі.

2.4 Режим Роботи

Пристрій підтримує два режими роботи: **Автономний** та в режимі **самоорганізованої мережі**. За замовчуванням він працює в режимі **самоорганізованої мережі**. Залежно від режиму роботи в системі представлені різні пункти меню. Щоб змінити режим роботи, див. 4.1 2. Перемикання режиму роботи.

Самоорганізована мережа: Після увімкнення функції виявлення самоорганізованої мережі пристрій можна виявити в мережі та знайти інші пристрої в мережі. Пристрої об'єднуються в мережу один з одним основі статусу пристрою та синхронізують глобальну конфігурацію. Ви можете увійти на веб-сторінку керування пристроєм, щоб перевірити інформацію про керування всіма пристроями в мережі. Після увімкнення функції самоорганізаційного виявлення мережі користувачі можуть ефективніше обслуговувати поточну мережу та керувати нею. Рекомендуємо залишити цю функцію увімкненою.

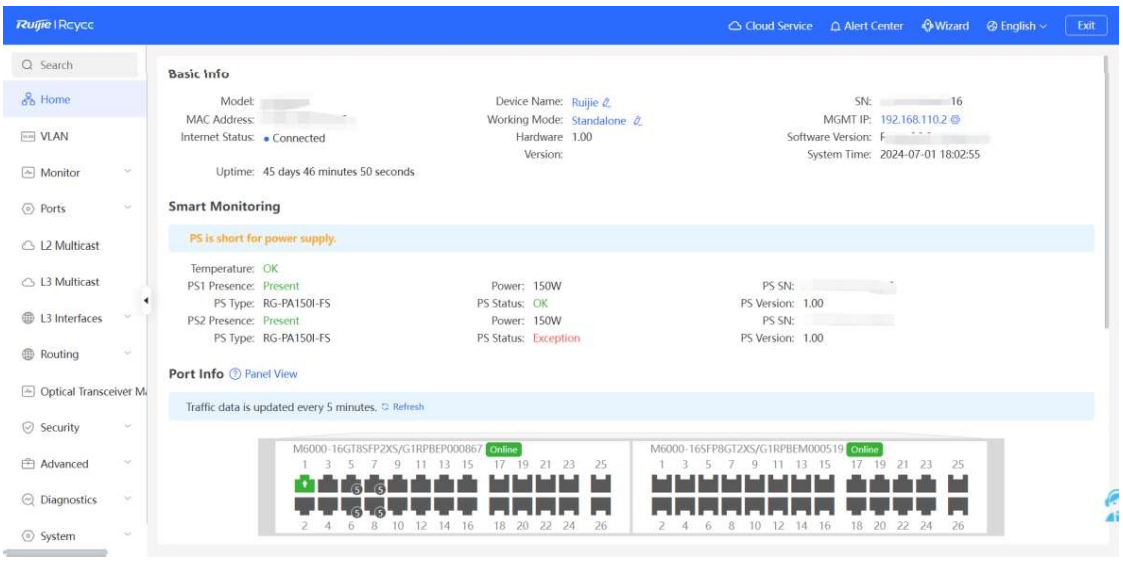
Коли пристрій перебуває в режимі мережі, що самоорганізується, веб-сторінка має два режими конфігурації: режим мережі та режим локального пристрою. Для отримання додаткової інформації див. розділ 2.5 Перемикання режиму керування.

Автономний режим: Якщо функцію самоорганізаційного виявлення мережі вимкнено, пристрій не буде виявлено в мережі. Після входу на веб-сторінку ви можете налаштовувати та керувати лише тим пристроєм, до якого ви увійшли. Якщо налаштовано лише один пристрій або глобальну конфігурацію не потрібно синхронізувати з пристроєм, ви можете вимкнути функцію самоорганізаційного мережевого виявлення.

2.5 Перемикання режиму керування

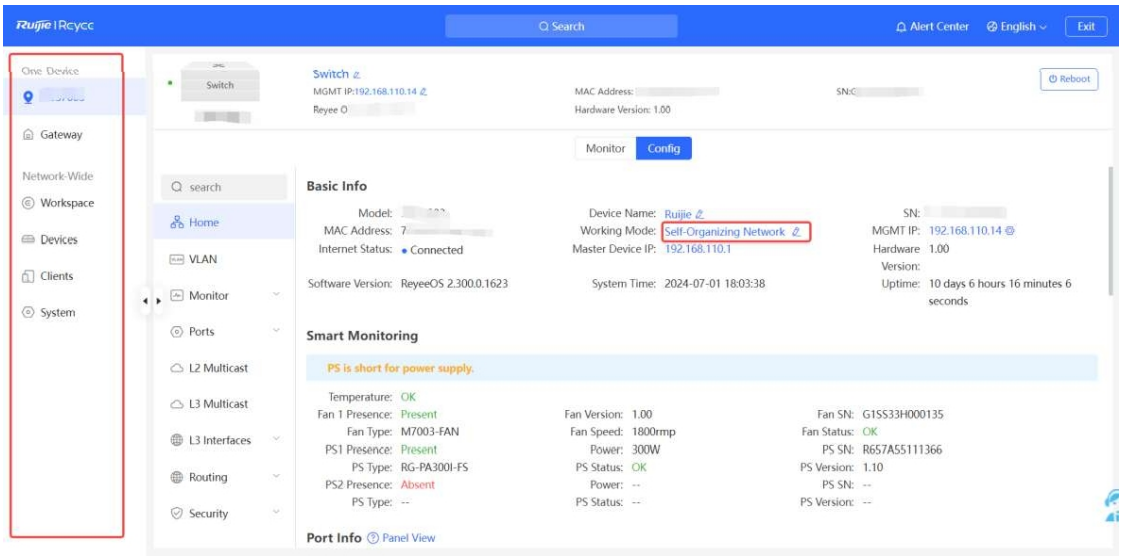
В автономному режимі ви можете налаштовувати і керувати лише пристроєм, який увійшов до системи, без функції самоорганізації мережі. Як показано у розділі

Рисунок 2-2 Веб-інтерфейс в автономному режимі



У режимі самоорганізації ви можете пакетно налаштувати загальновживані функції всіх дротових і бездротових пристроїв Reyee у мережі, що самоорганізується, включно з пристроєм, до якого ви ввійшли в систему. Як показано в

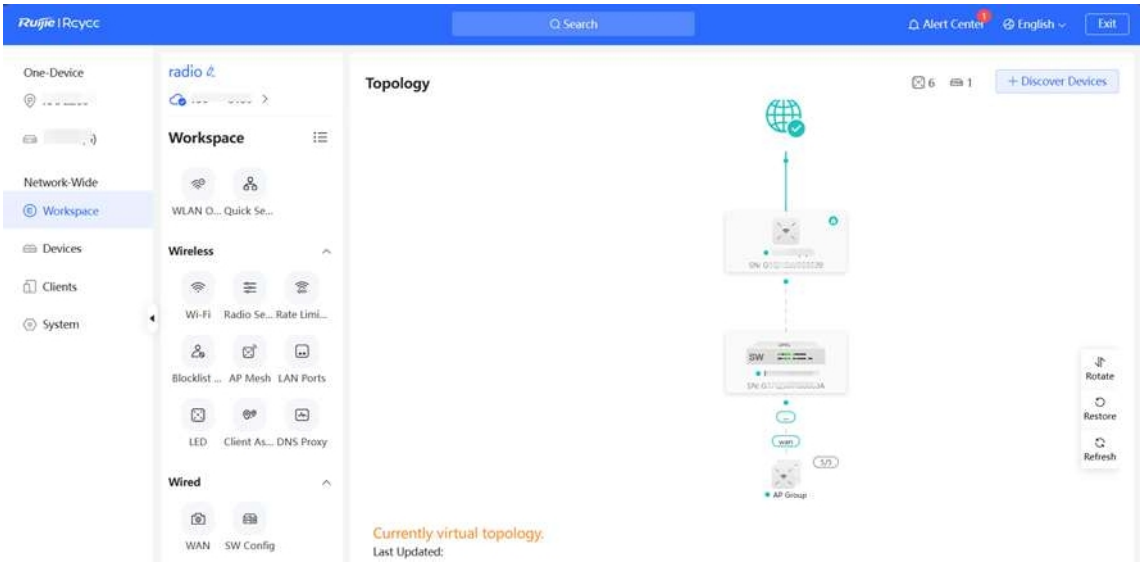
Рисунок 2-3 Веб-інтерфейс у режимі самоорганізації



3 Управління мережею

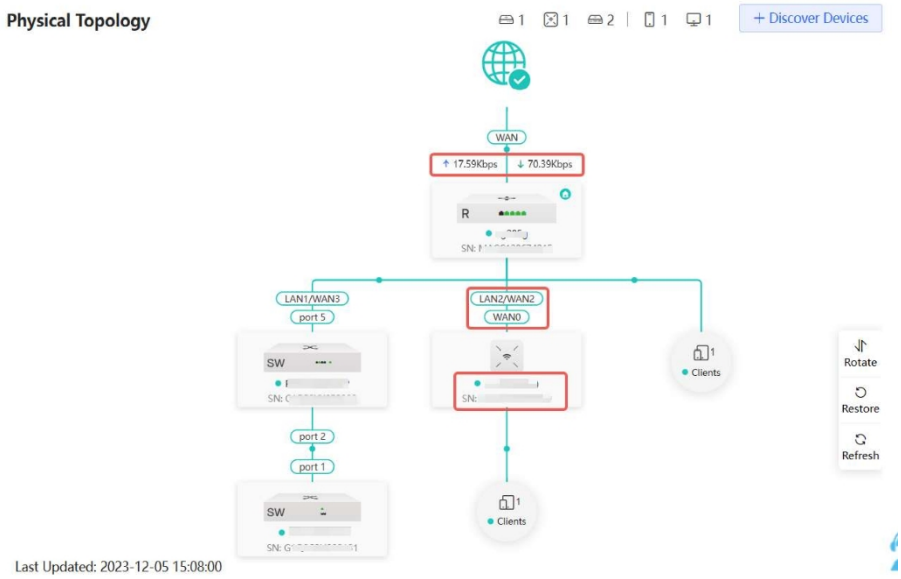
Виберіть **Network-Wide> Робоча область> Топологія**.

Веб-сторінка "**Огляд**" відображає поточну топологію мережі, висхідний і низхідний потік в реальному часі, стан мережі та кількість користувачів. Швидкий доступ до налаштувань мережі та пристроїв також надається на веб-сторінці "**Огляд**". Користувачі можуть відстежувати, налаштовувати і керувати станом мережі на поточній сторінці.

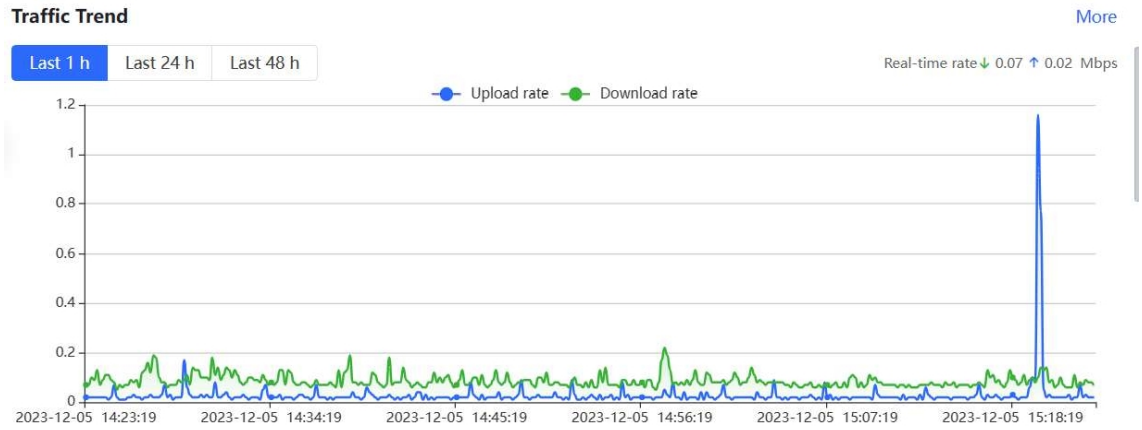


3.1 Перегляд мережі Інформація

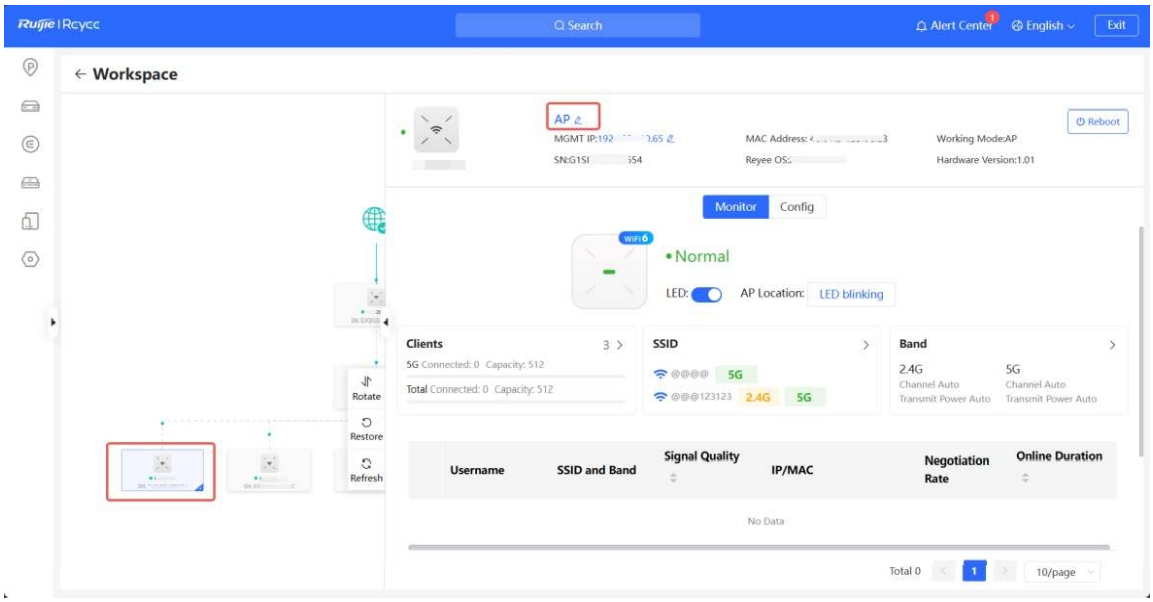
Ви можете переглянути онлайн пристрій, ідентифікатор порту, SN пристрою, а також в режимі реального часу висхідний і низхідний потік в топології мережі.



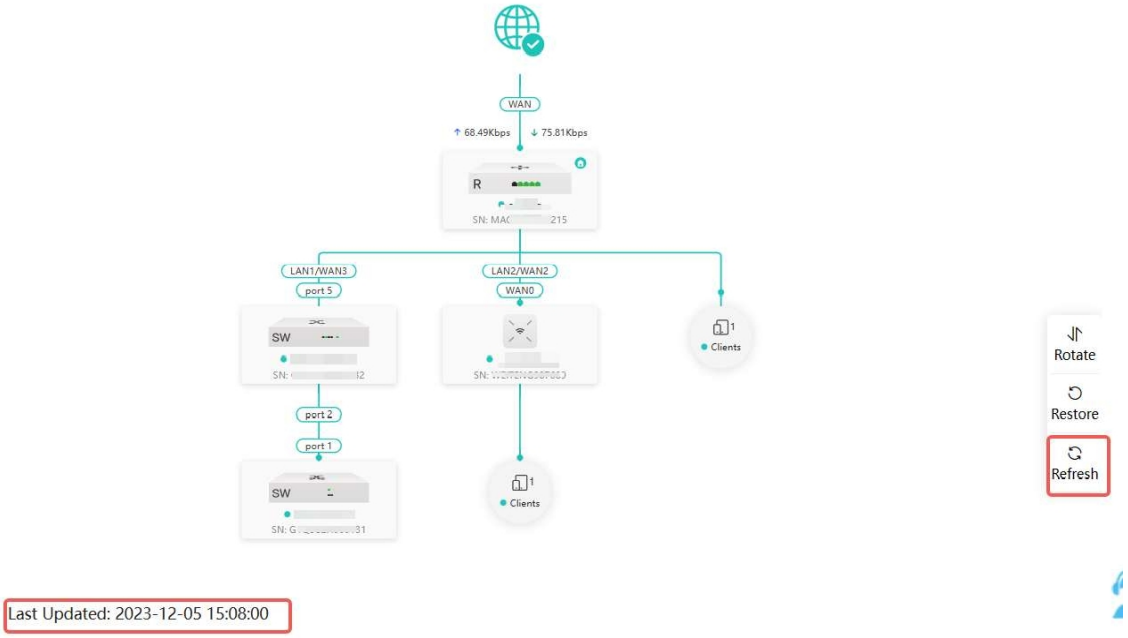
- Натисніть на шлюз евакуації, щоб переглянути інформацію про трафік пристрою в реальному часі.



- Натисніть на пристрій в топології, щоб переглянути робочий стан і конфігурацію пристрою та налаштувати його функціонує пристрій. За замовчуванням ім'я хоста відповідає моделі пристрою. Щоб змінити ім'я хоста, перейдіть за  .



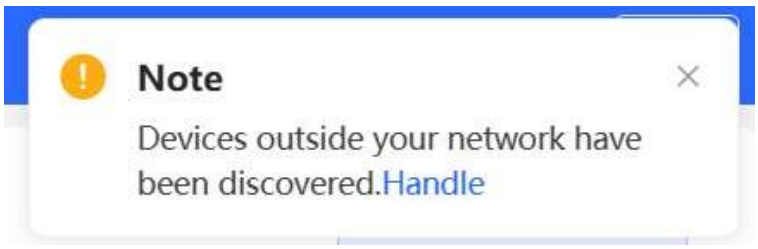
- Час оновлення топології відображається в лівому нижньому кутку. Натисніть **Оновити**, щоб оновити топологію до останнього стану. Будь ласка, зачекайте кілька хвилин на оновлення.



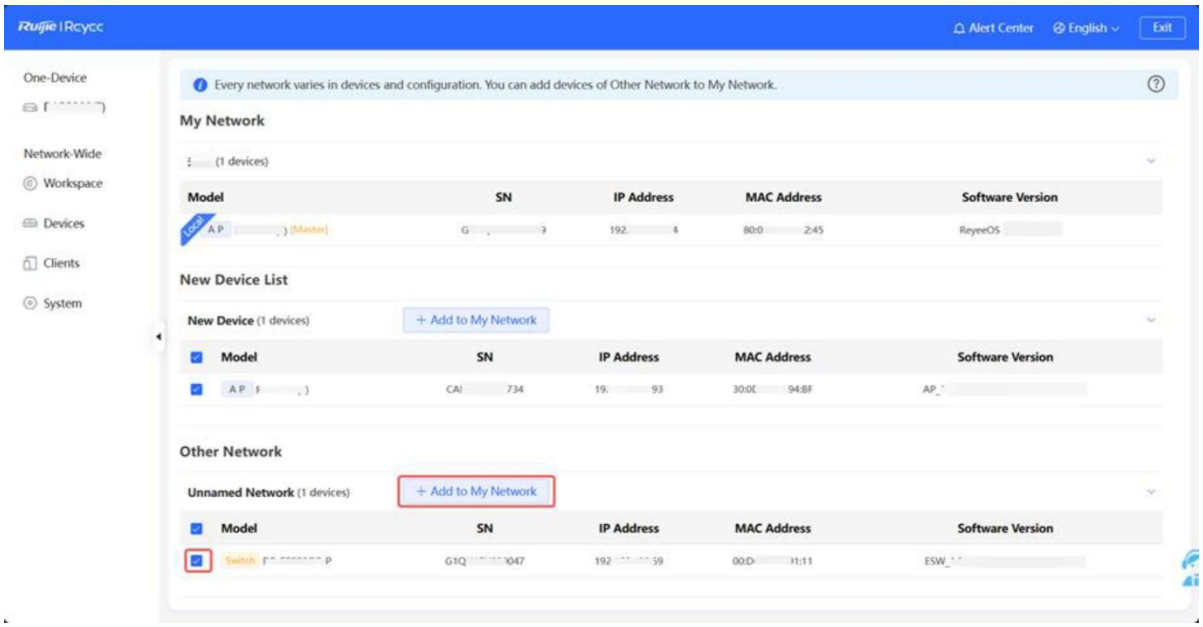
3.2 Додавання мережі Пристрої

3.2.1 Дротовий Підключення

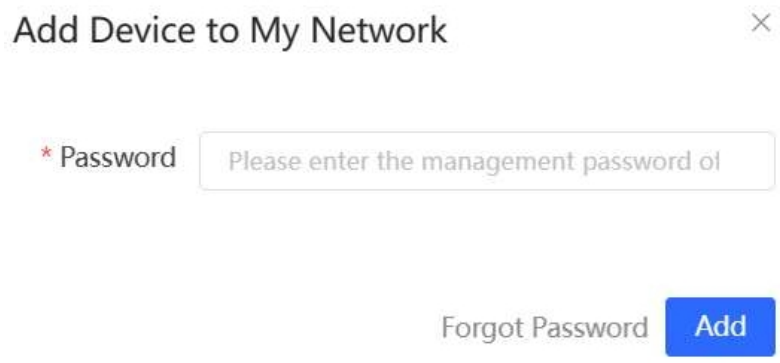
(1) Якщо новий пристрій підключено до пристрою в мережі за допомогою дротового з'єднання, з' підказка, яка вказує на те, що виявлено пристрій, який не входить до SON (самоорганізаційної мережі). Кількість (помаранчевим кольором) пристроїв, які не входять до SON, відображається під заголовком **Пристрої** у верхньому лівому куті сторінки. Натисніть **Ручка**, щоб додати пристрій до поточної мережі.



(2) Перейдіть на сторінку **Список мереж**, натисніть **Інша мережа**, щоб вибрати цільовий пристрій, і натисніть **Додати до моєї мережі**.



(3) Якщо цільовий пристрій ще не налаштовано, ви можете додати його безпосередньо без пароля. Якщо пристрій налаштовано з паролем, введіть пароль керування пристроєм. Якщо пароль неправильний, пристрій не вдасться додати до мережі.



3.2.2 AP Mesh

Примітка

Тільки пристрої Reyee AP, які підтримують функцію AP Mesh, можуть завершити створення мережі через AP Mesh.

1. Огляд

Після увімкнення та активації функції AP Mesh нову точку доступу з підтримкою Mesh можна поєднати з іншими бездротовими пристроями з підтримкою Mesh у цільовій мережі кількома способами. Після цього точка доступу автоматично синхронізує свою конфігурацію Wi-Fi з іншими пристроями. Mesh-мережі вирішують такі проблеми, як складні бездротові мережі та кабелі. Нову точку доступу можна підключити до будь-якого бездротового пристрою з висхідною лінією зв'язку між точкою доступу, маршрутизатором EG та маршрутизатором EGW наступними способами:

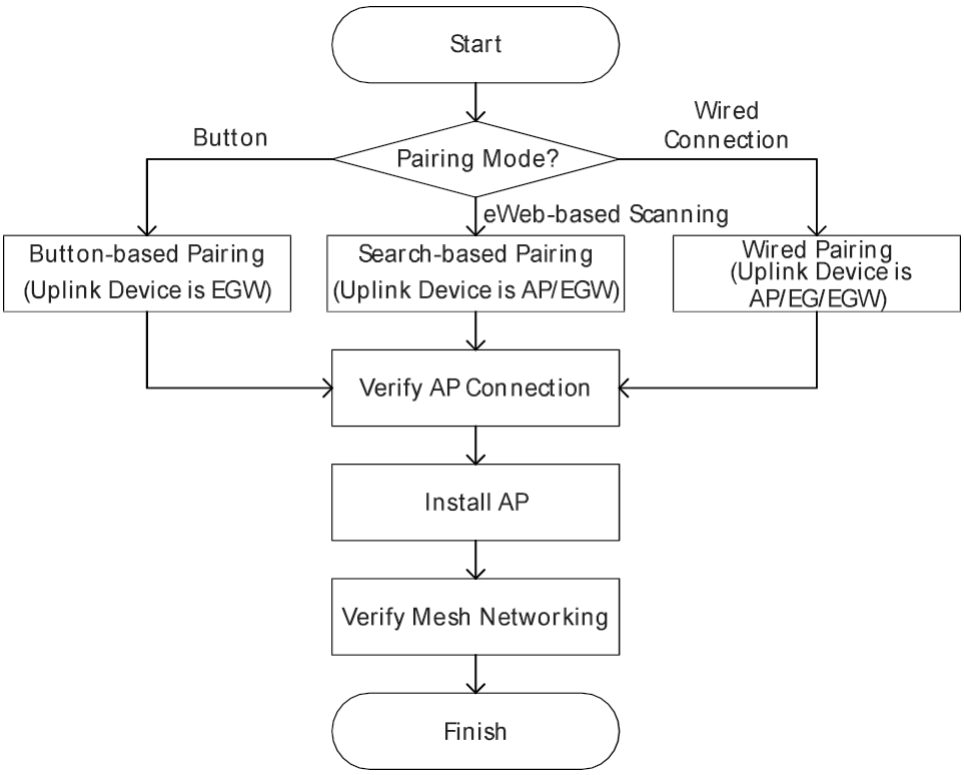
- Кнопкове сполучення: Коротко натисніть кнопку Mesh на маршрутизаторі EGW у цільовій мережі, щоб реалізувати

швидке сполучення точки доступу з роутером EGW.

- Сполучення на основі пошуку: Увійдіть у веб-інтерфейс пристрою в цільовій мережі. Знайдіть і додайте точки доступу для сполучення.
- Дротове сполучення: Підключіть нову точку доступу до бездротового пристрою в цільовій мережі допомогою кабелю Ethernet. Нова точка доступу з'явиться в цільовій мережі.

Після завершення сполучення нова точка доступу отримує інформацію про бездротове з'єднання від сусідніх точок доступу по всій мережі. Встановіть нову точку доступу відповідно до плану, і вона підключиться до оптимальної сусідньої точки доступу.

2. Кроки конфігурації



3. Кроки налаштування для сполучення на основі кнопок

Застереження

- Висхідним пристроєм є маршрутизатор EGW.
- Нова точка доступу повинна бути у заводському стані.
- Його можна сканувати лише тоді, коли в мережі ввімкнена функція Mesh.
- Розмістіть нову точку доступу на відстані не більше ніж 2 метри від пристрою висхідної лінії зв'язку, щоб переконатися, що нова точка доступу може отримувати сигнал Wi-Fi від пристрою висхідної лінії зв'язку. Нова точка доступу може не бути відсканована через велику відстань або перешкоди між нею та пристроєм висхідної лінії зв'язку.

(1) Увімкніть нову точку доступу та розмістіть її біля маршрутизатора EGW у цільовій мережі.

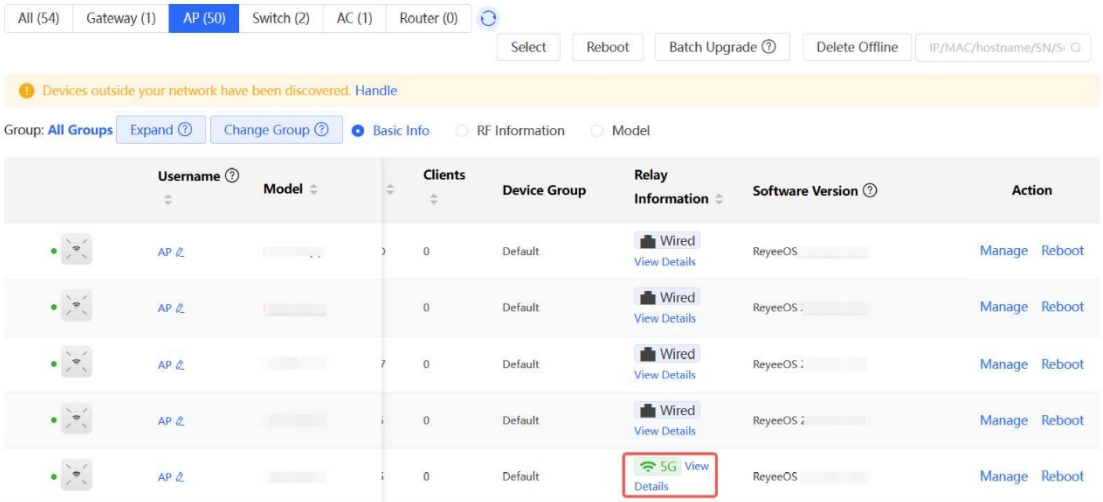
(2) Натисніть і утримуйте кнопку Mesh  на маршрутизаторі EGW не більше двох секунд, щоб почати сполучення. Процес створення пари триває близько однієї хвилини.

(3) Перевірте топологію на сторінці **Фізична топологія**, щоб переконатися, що нова точка доступу підключилася до пристрою висхідної лінії зв'язку у бездротовому режимі.

(4) Вимкніть нову точку доступу та встановіть її за планом.

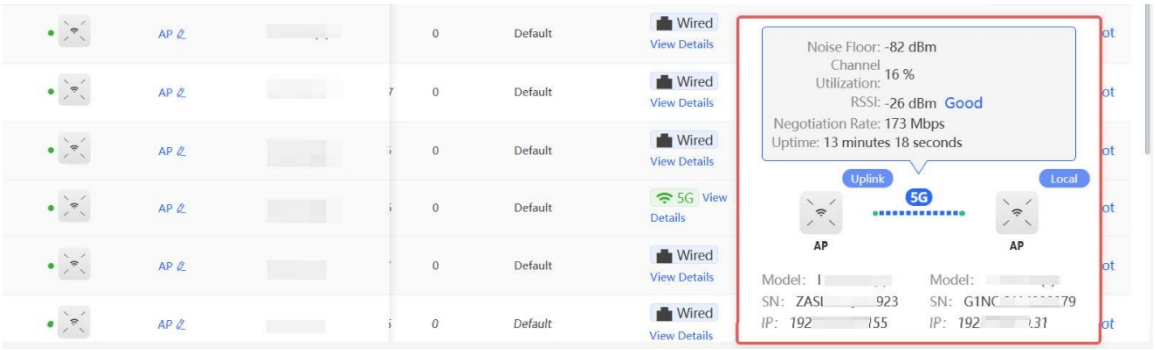
(5) Увійдіть до веб-інтерфейсу пристрою в цільовій мережі. У режимі **Мережа** виберіть **Пристрої**>. Переконайтеся, що нова точка доступу перебуває в мережі, а відповідний запис містить піктограму 

у колонці **Інформація про ретрансляцію**. Піктограма вказує на те, що бездротовий ретранслятор виконується через радіостанцію 5 ГГц.



(6) Натисніть **Переглянути деталі** після іконки 

, щоб отримати інформацію про пристрій висхідної лінії зв'язку та RSSI.



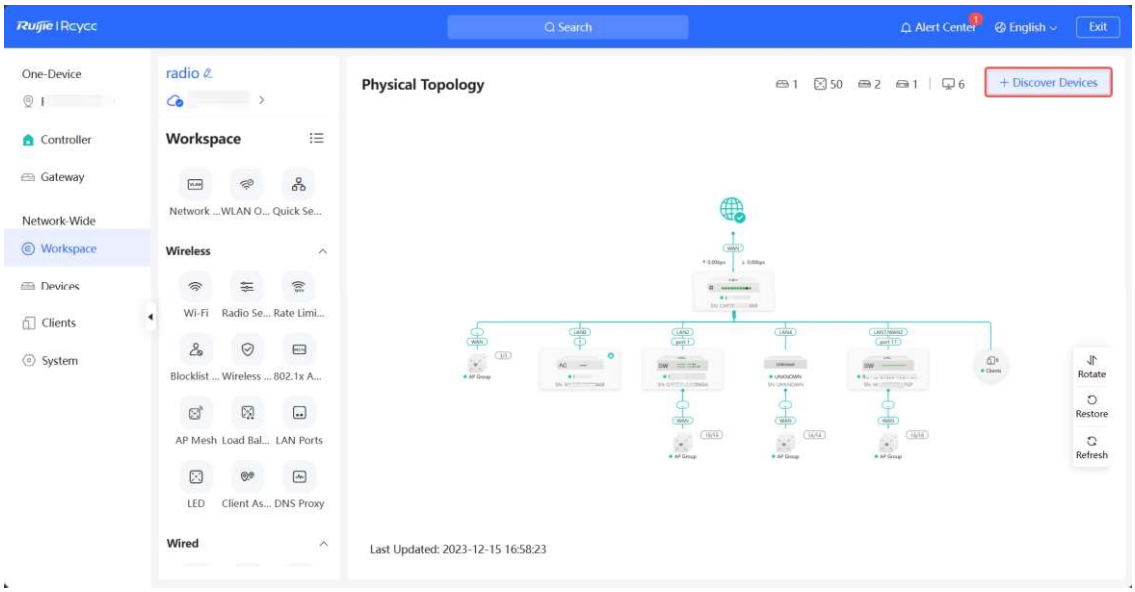
4. Кроки налаштування сполучення на основі пошуку

Застереження

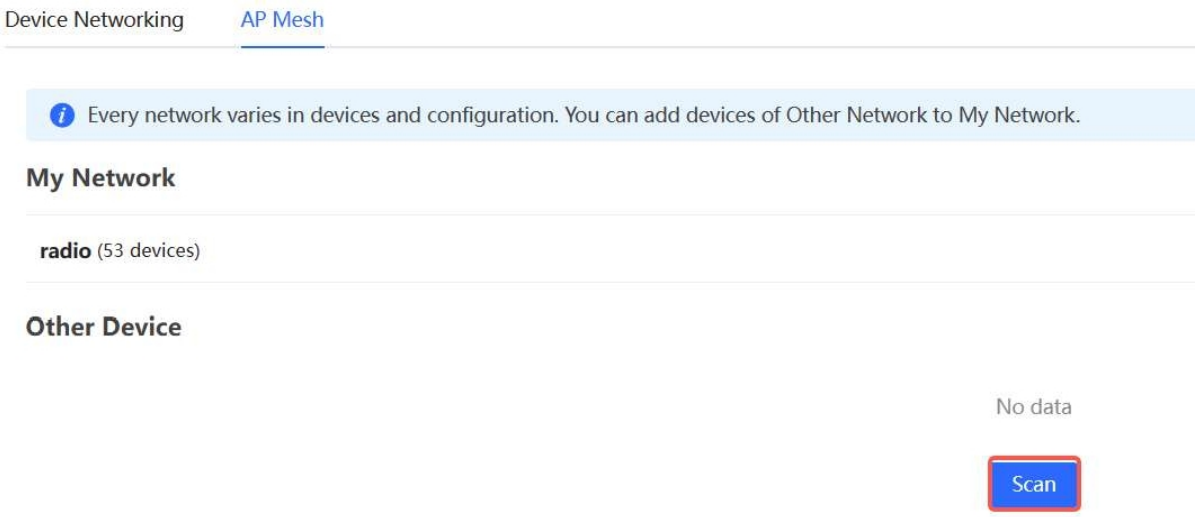
- Пристрій висхідного зв'язку - це точка доступу або маршрутизатор EGW.
- Нова точка доступу повинна бути у заводському стані.
- Його можна сканувати лише тоді, коли в мережі ввімкнена функція Mesh.
- Розмістіть нову точку доступу на відстані не більше ніж 2 метри від пристрою висхідної лінії зв'язку, щоб переконатися, що нова точка доступу може отримувати сигнал Wi-Fi від пристрою висхідної лінії зв'язку. Нова точка доступу може не бути відсканована через велику відстань або перешкоди між нею та пристроєм висхідної лінії зв'язку.

(1) Увімкніть нову точку доступу та розмістіть її біля точки доступу або маршрутизатора EGW у цільовій мережі.

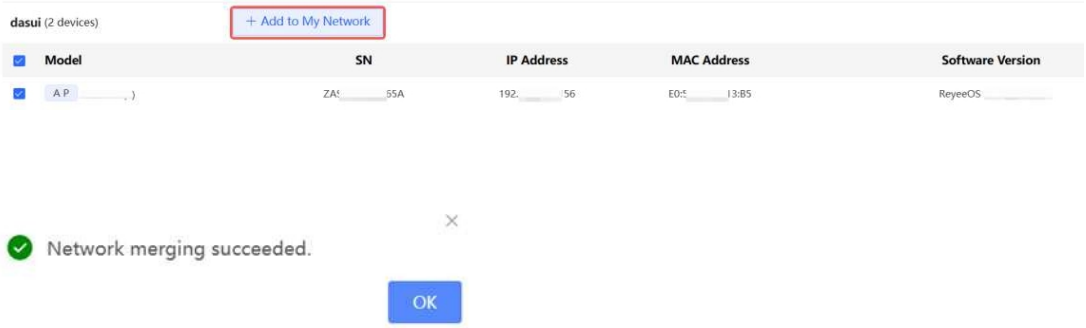
(2) Увійдіть у веб-інтерфейс пристрою в цільовій мережі. У режимі **Network-Wide** натисніть **+Discover Devices** у верхньому правому куті сторінки **Physical Topology (Фізична топологія)**, щоб просканувати точки доступу в інших мережах, не підключених за допомогою кабелів Ethernet.



(3) На сторінці **AP Mesh** натисніть **Сканувати**, щоб просканувати пристрої, не підключені до мережі за допомогою кабелю Ethernet.



(4) Виберіть точки доступу, які потрібно додати, і натисніть **Додати до моєї мережі**. Одночасно дозволено додавати не більше восьми точок доступу. Дочекайтеся завершення об'єднання мереж.

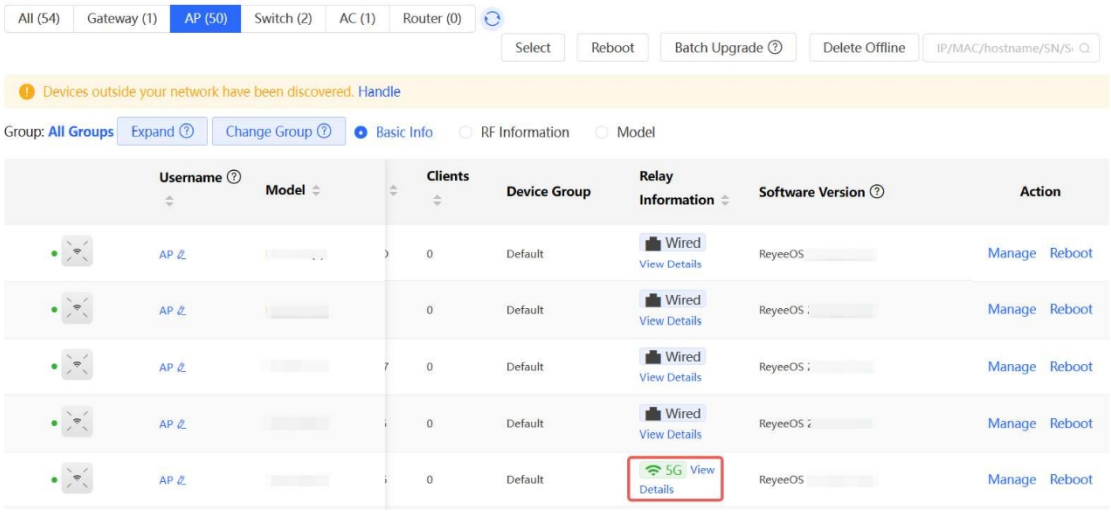


(5) Перевірте топологію на сторінці **Фізична топологія**, щоб переконатися, що нова точка доступу підключилася до пристрою висхідної лінії зв'язку у бездротовому режимі.

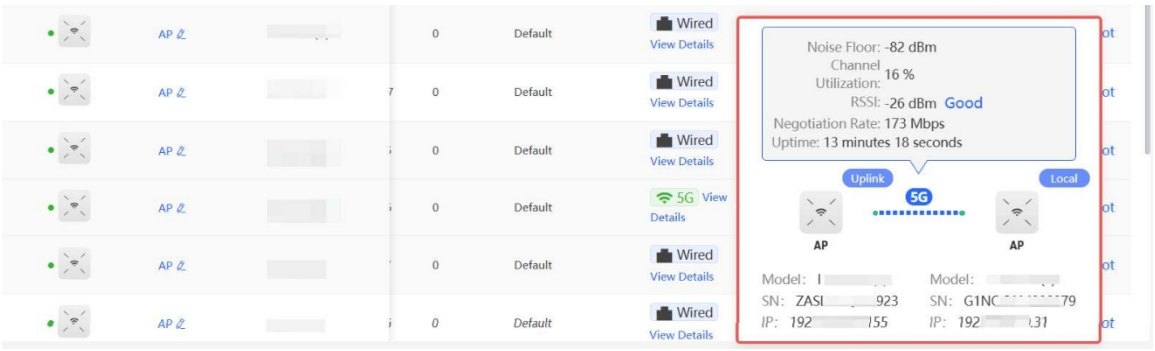
(6) Вимкніть нову точку доступу та встановіть її за планом.

(7) Увійдіть до веб-інтерфейсу пристрою в цільовій мережі. У режимі **Мережа** виберіть **Пристрої**>.

Переконайтеся, що нова точка доступу перебуває в мережі, а відповідний запис містить піктограму 5G у колонці **Інформація про ретрансляцію**. Піктограма вказує на те, що бездротовий ретранслятор виконується через радіоканал 5 ГГц.



(8) Натисніть **Переглянути деталі** після іконки 5G , щоб отримати інформацію про пристрій висхідної лінії зв'язку та RSSI.



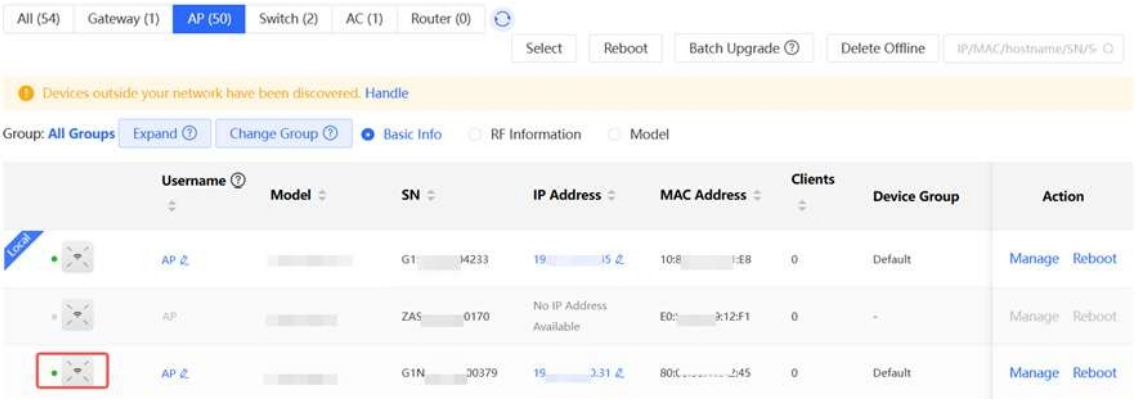
5. Кроки налаштування дротового з'єднання

Застереження

- Пристрій висхідного зв'язку - це точка доступу (AP), маршрутизатор EG або маршрутизатор EGW.
- Нова точка доступу повинна бути у заводському стані.
- Його можна сканувати лише тоді, коли в мережі ввімкнена функція Mesh.

(1) Підключіть один кінець Ethernet-кабелю до висхідного порту нової доступу, а другий - до низхідного порту точки доступу, маршрутизатора EG або маршрутизатора EGW у цільовій мережі. Підключення до mesh-мережі займає від однієї до трьох хвилин. Коли індикатор стану системи світиться постійно, це означає, що створення Mesh-мережі завершено.

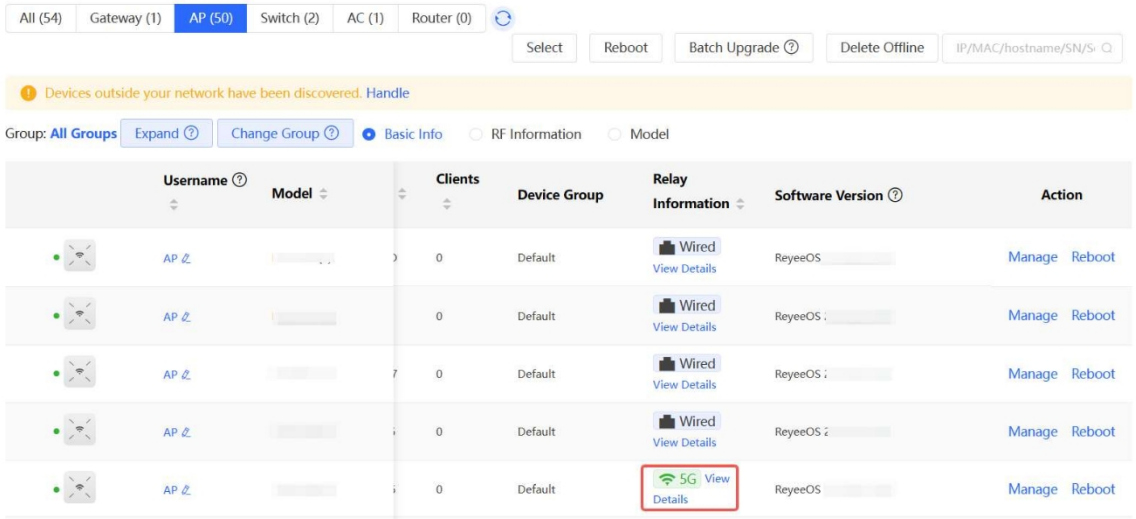
(2) Увійдіть у веб-інтерфейс пристрою в цільовій мережі. У режимі **"Вся мережа"** виберіть **"Пристрої"** і переконайтеся, що нова точка доступу перебуває в **мережі**.



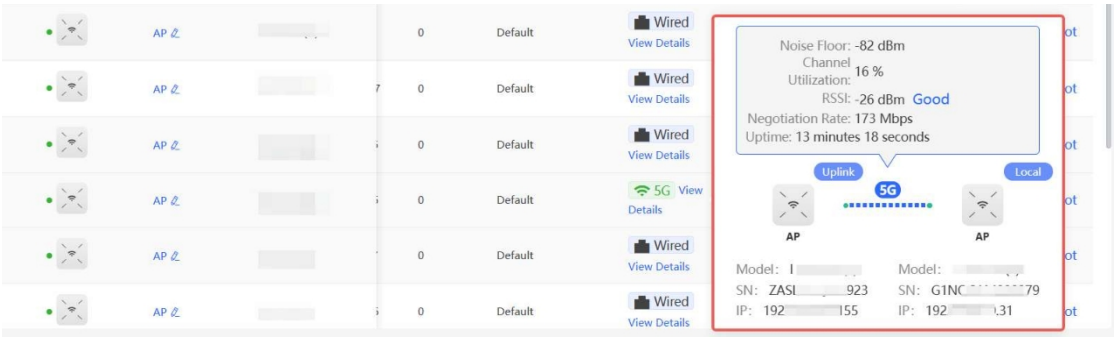
(3) Від'єднайте кабель Ethernet, вимкніть нову точку доступу та встановіть її за планом.

(4) Увійдіть до веб-інтерфейсу пристрою в цільовій мережі. У режимі **Мережа** виберіть **Пристрої**>**AP**.

Переконайтеся, що нова точка доступу перебуває в мережі, а відповідний запис містить піктограму 5G у стовпчику **Інформація про ретрансляцію**. Піктограма вказує на те, що бездротове з'єднання виконується через радіоканал 5 ГГц.



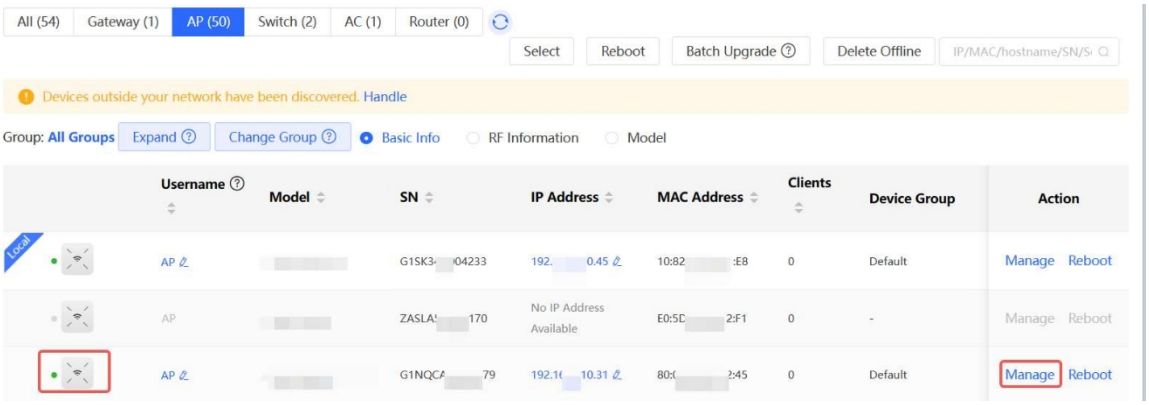
(5) Натисніть **Переглянути деталі** після іконки 5G , щоб отримати інформацію про пристрій висхідної лінії зв'язку та RSSI.



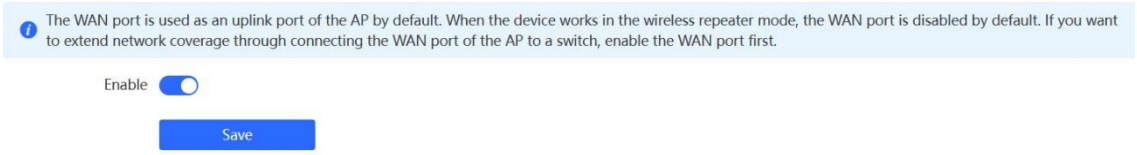
6. Увімкнення порту WAN

За замовчуванням порт WAN працює як дротовий висхідний порт точки доступу. Для точки доступу, доданої до цільової мережі через , порт WAN за замовчуванням вимкнено. Якщо ви хочете підключити точку доступу Mesh до іншого пристрою низхідної лінії зв'язку в дротовому режимі для розширення мережі, увімкніть цей порт.

(1) Увійдіть до веб-інтерфейсу мережевого проекту. Виберіть **Мережа для всієї мережі**> **Пристрої**> **Точка доступу** і натисніть **Керування** поруч пристроєм у списку точок доступу.



(2) Виберіть Конфігурація> **Додатково**> **Увімкнути WAN**, увімкніть **Увімкнути** і натисніть **Зберегти**.

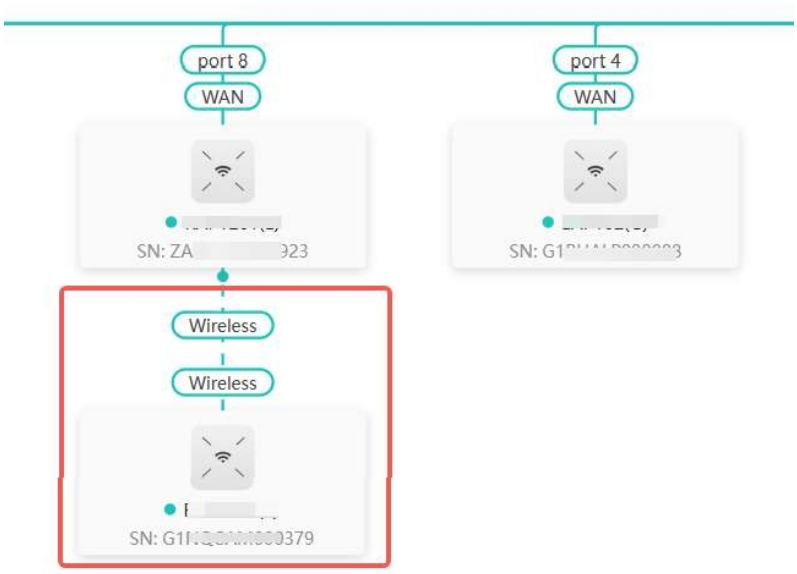


7. Запит точок доступу та відомостей про mesh-мережу

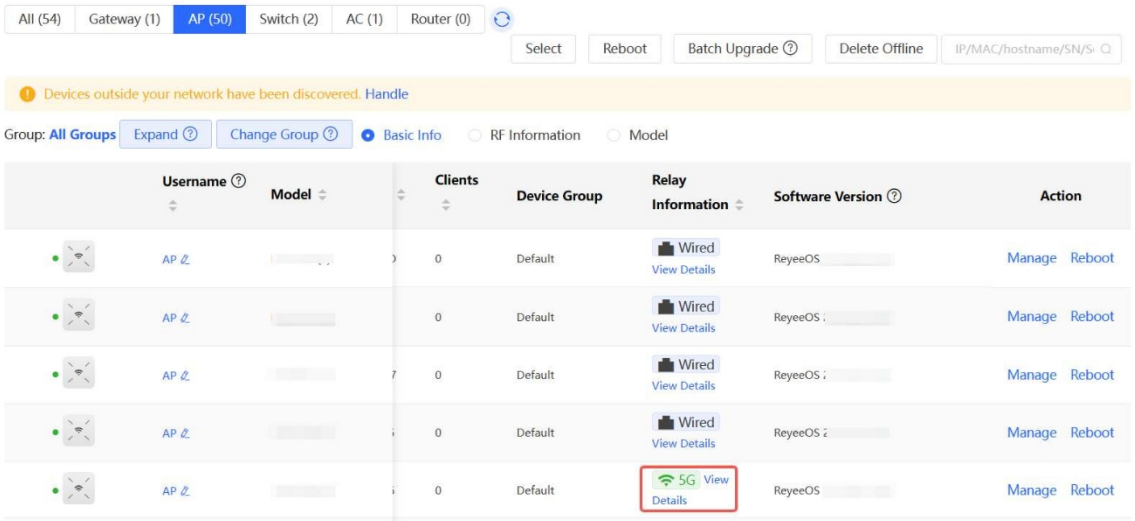
(1) у пристрою в цільовій мережі.

(2) Запитуйте точки доступу Mesh.

- Спосіб 1: У режимі **"Мережа"** перевірте топологію на сторінці **"Фізична топологія"**. Точка доступу, яка підключається до пристрою висхідної лінії зв'язку у бездротовому режимі, є Mesh AP.

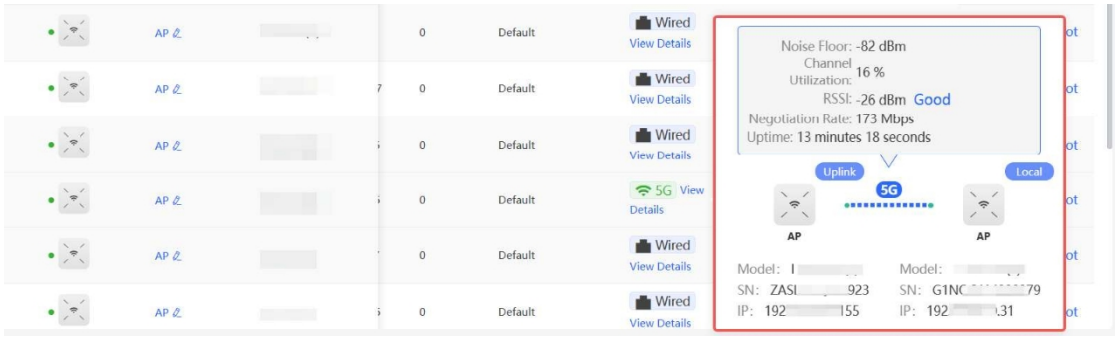


- Спосіб 2: У режимі **Мережа** виберіть **Пристрої> точки доступу**. Якщо запис містить піктограму 5G у стовпчику **Інформація про ретрансляцію**, відповідна точка доступу є Mesh AP.



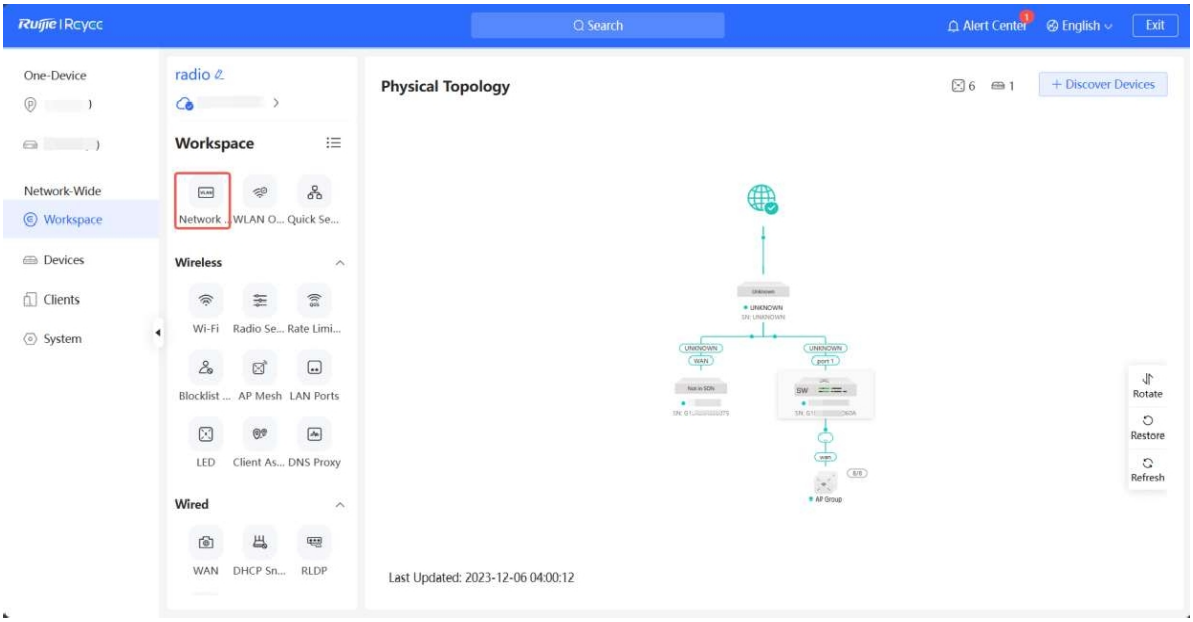
(3) Подробиці про мережу запитів Mesh.

У режимі **Мережа** виберіть **Пристрої> точки доступу**. Виберіть цільову точку доступу і натисніть **Переглянути деталі** у стовпчику **Інформація про ретрансляцію**, щоб отримати відомості про Mesh-мережу.



3.3 Налаштування мережі Планування

Виберіть **Мережа в цілому**> **Робоча область**> **Планування мережі**.

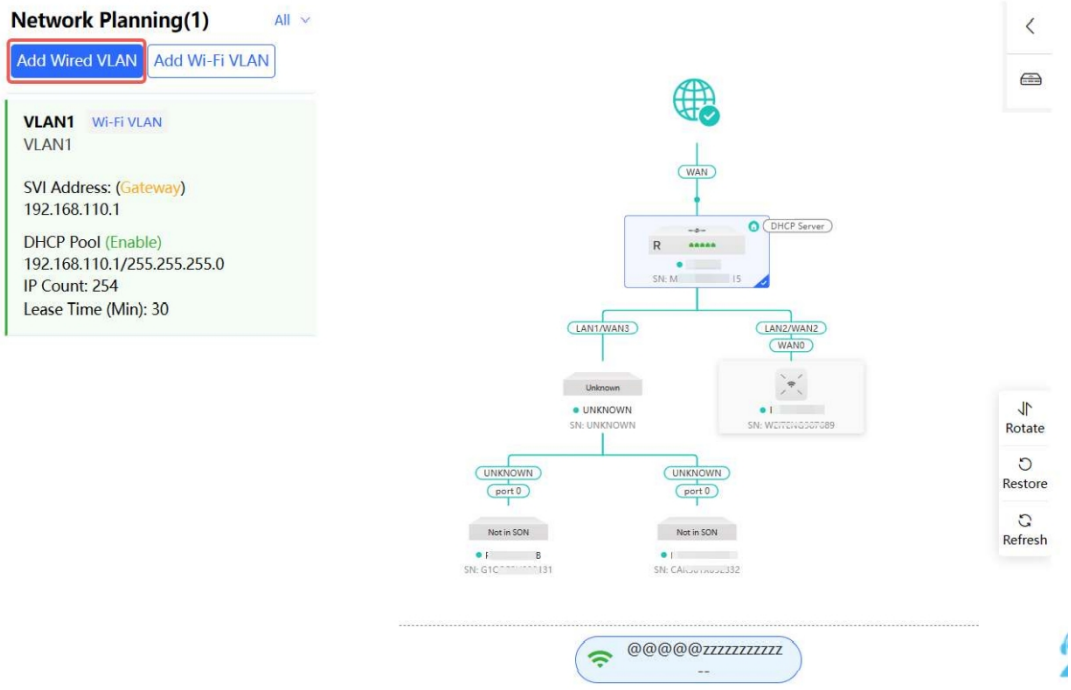


3.3.1 Налаштування дротової VLAN

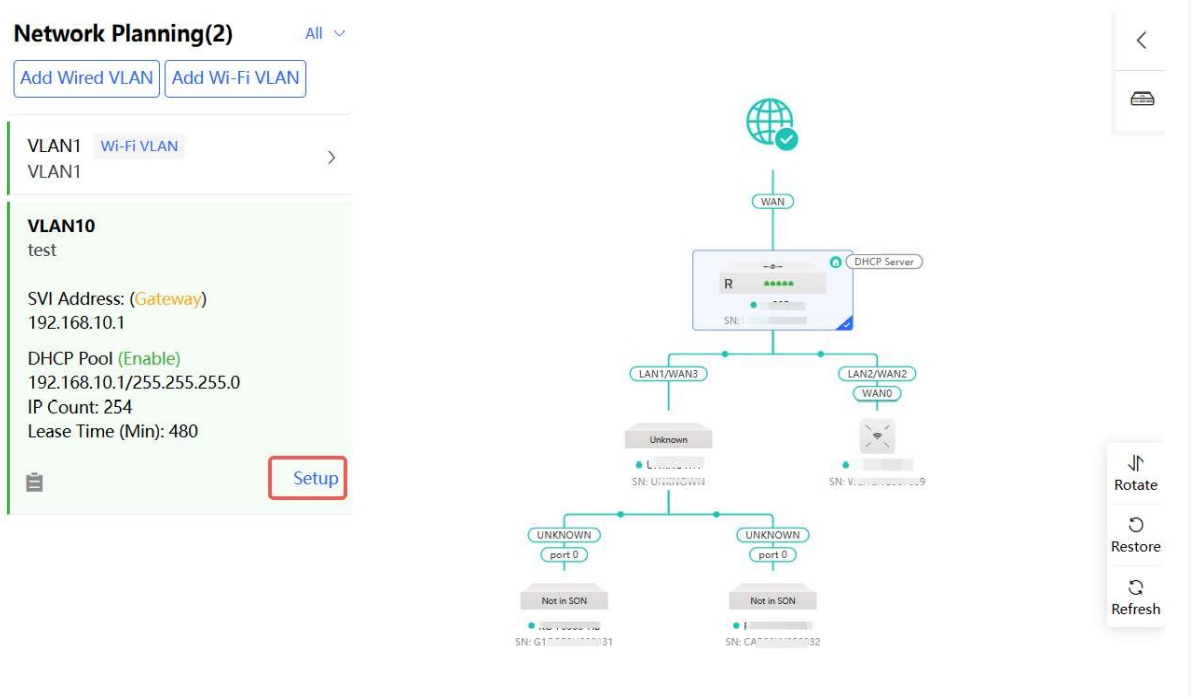
Виберіть **Мережа для всієї мережі**> **Робоча область**>

Планування мережі. На сторінці **Планування мережі** натисніть

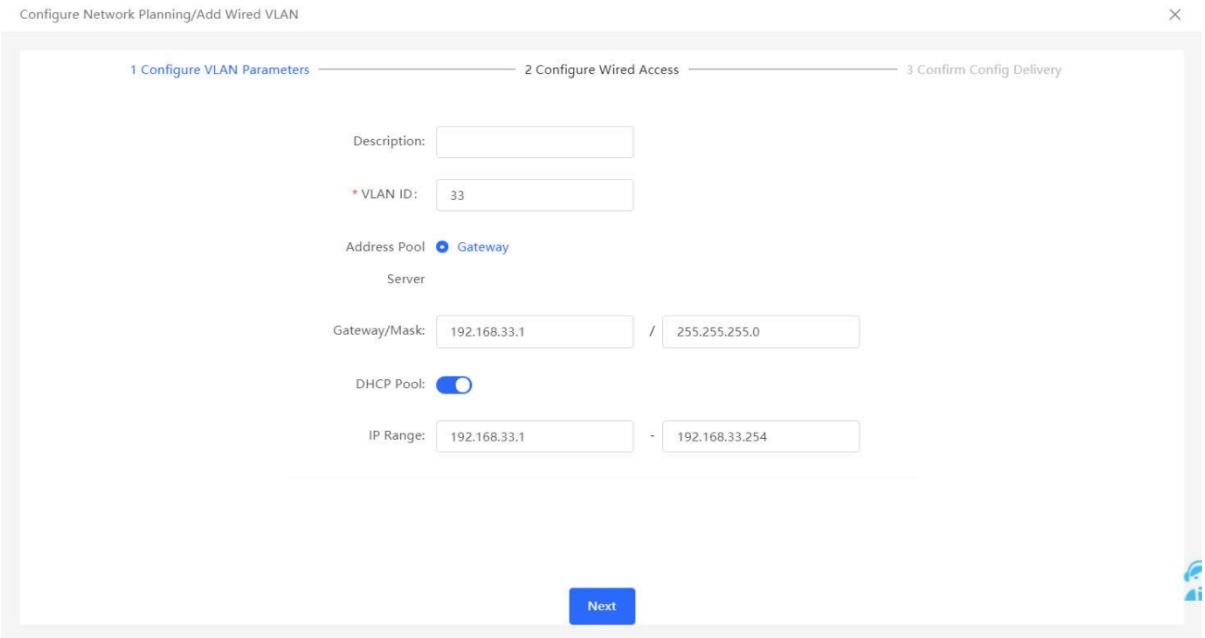
Додати дротову VLAN.



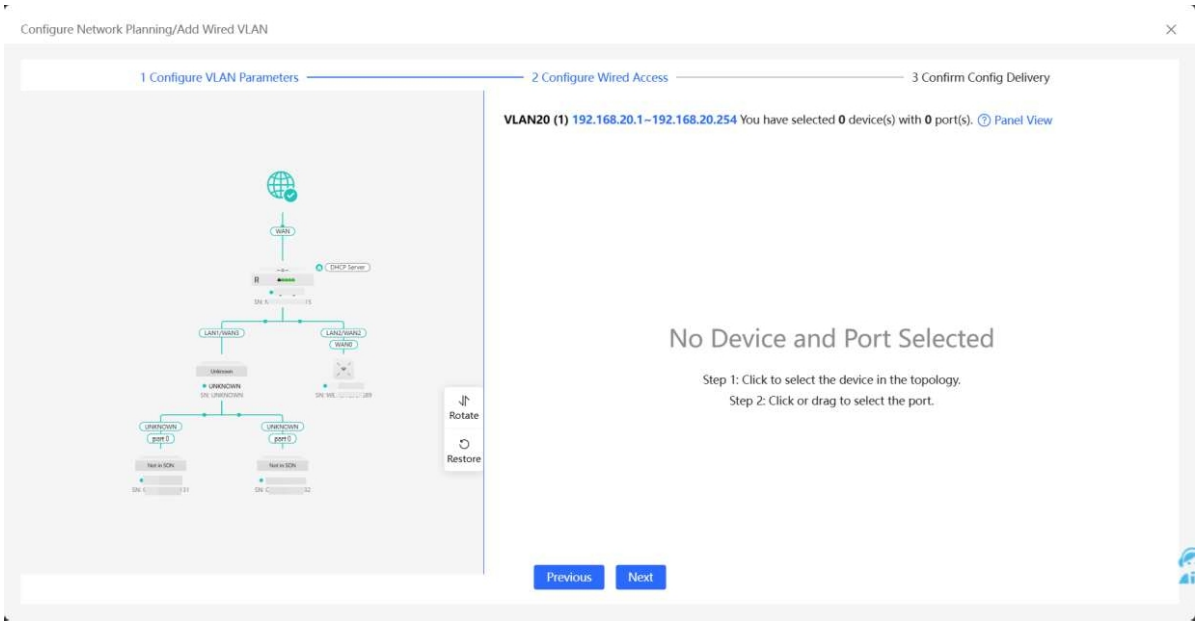
Крім того, ви можете вибрати існуючу дротову мережу VLAN і натиснути кнопку **Налаштування** для редагування VLAN.



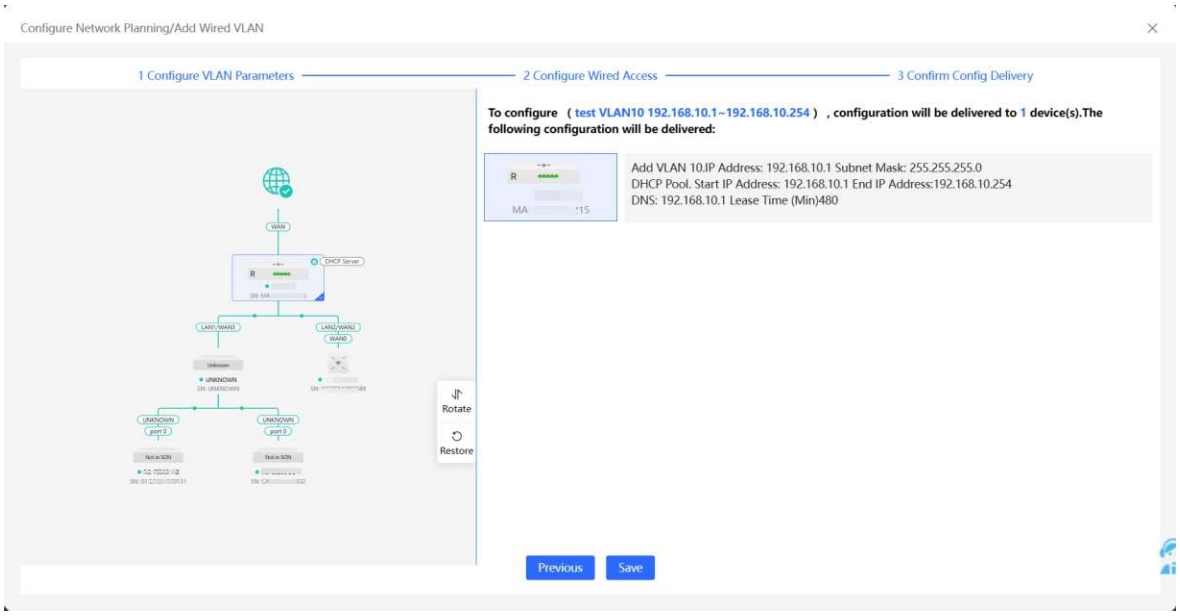
(1) Налаштуйте ідентифікатор VLAN, сервер пулу адрес і пул DHCP. За замовчуванням шлюз налаштовано як сервер пулу адрес для призначення IP-адрес клієнтам. Якщо в мережі є комутатор доступу, ви можете вибрати його як сервер пулу адрес. Натисніть **Далі** після налаштування параметрів VLAN.



(2) Виберіть цільовий комутатор у топології і всі порти у VLAN, а потім натисніть **Далі**.



(3) Будь ласка, підтвердіть доставлені конфігурації та натисніть **Зберегти**. Конфігурації набудуть чинності через кілька хвилин.

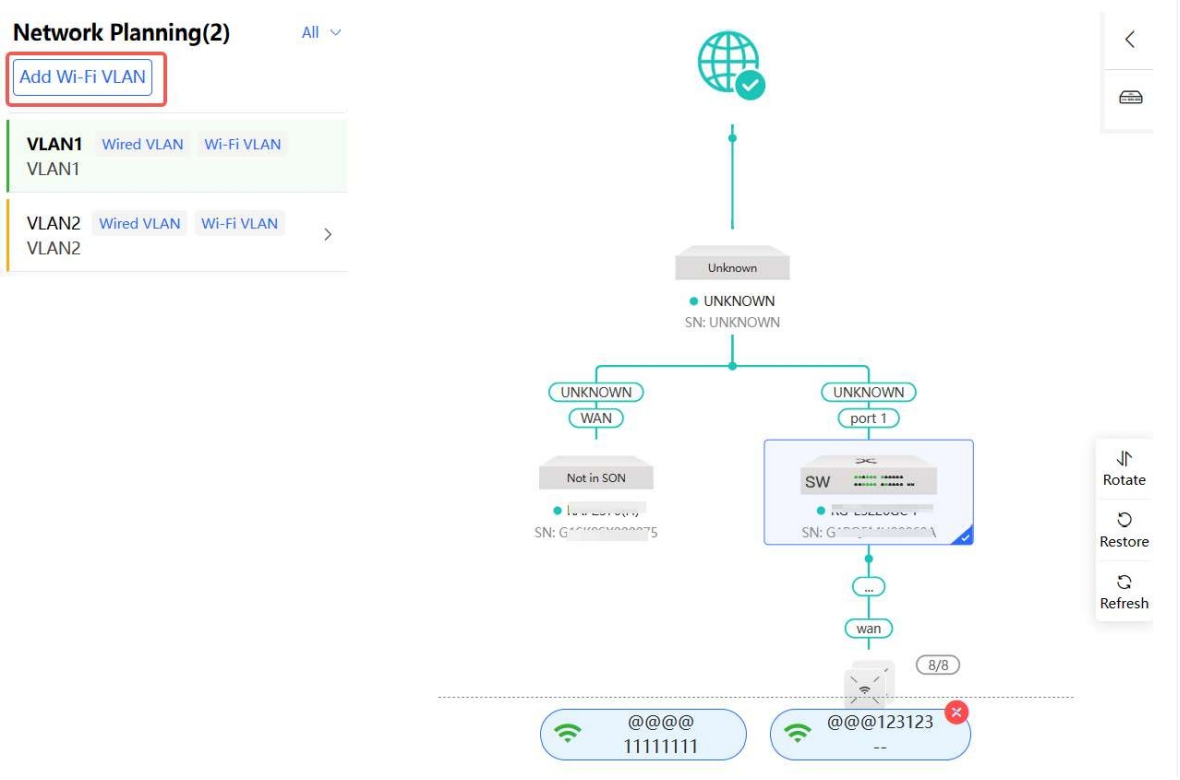


3.3.2 Налаштування Wi-Fi VLAN

Виберіть **Мережа для всієї мережі**> **Робоча область**>

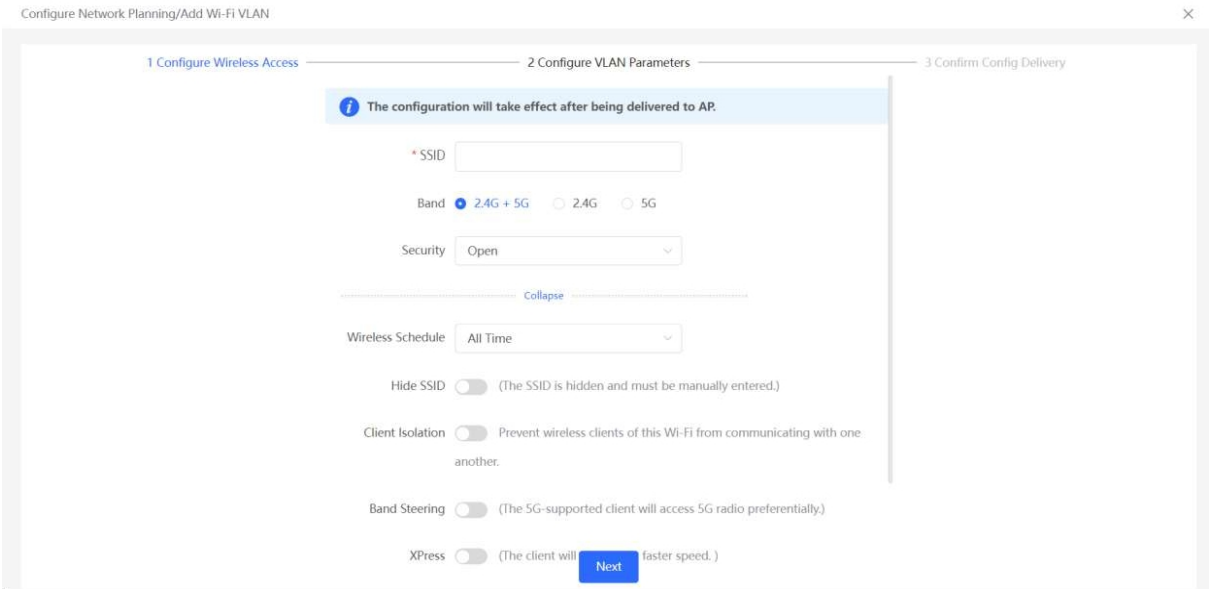
Планування мережі. На сторінці **Планування мережі** натисніть

Додати бездротову мережу.

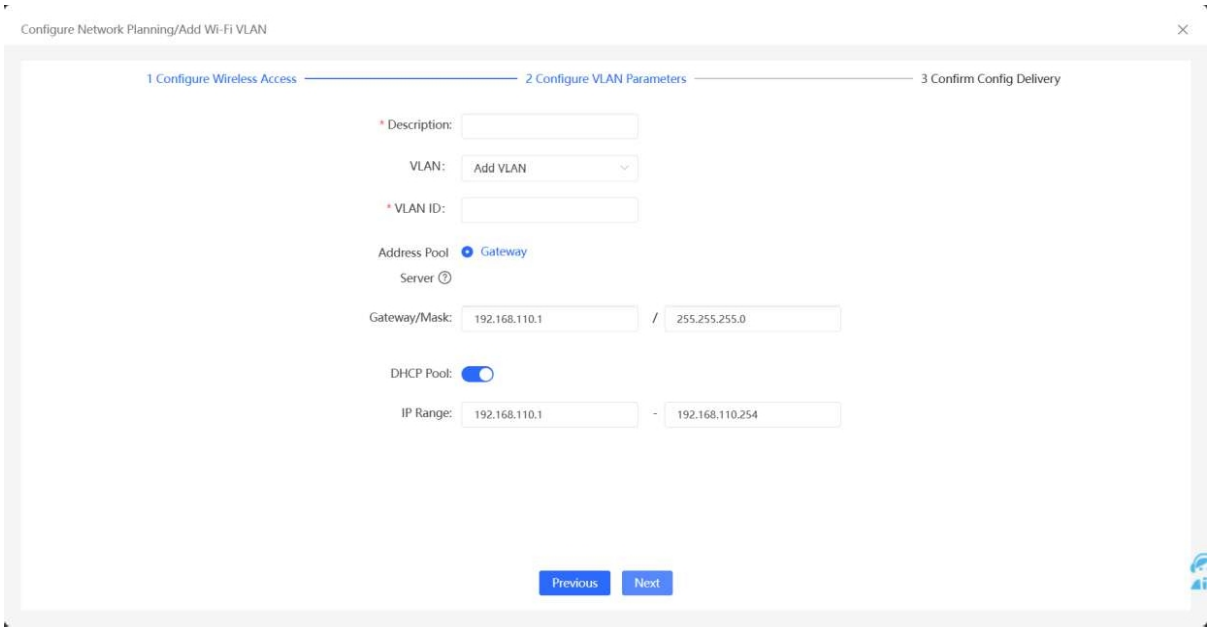


Крім того, ви можете вибрати існуючу бездротову мережу VLAN і натиснути кнопку **Налаштування** для редагування VLAN.

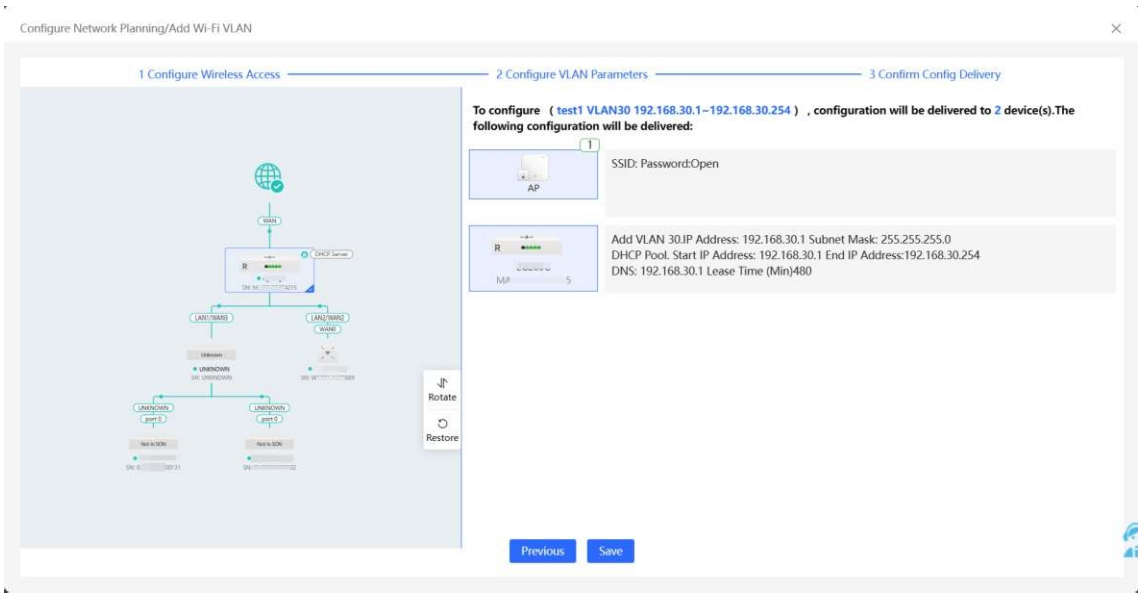
(1) Налаштуйте SSID, пароль Wi-Fi та діапазон. Натисніть **Розгорнути**, щоб розгорнути розширені налаштування і встановити параметри. Потім натисніть **Далі**.



(2) Налаштуйте ідентифікатор VLAN, сервер пулу адрес і пул DHCP. За замовчуванням шлюз налаштовано як сервер пулу адрес для призначення IP-адрес клієнтам. Якщо в мережі є комутатор доступу, ви можете вибрати його як сервер пулу адрес. Натисніть **Далі** після налаштування параметрів VLAN.

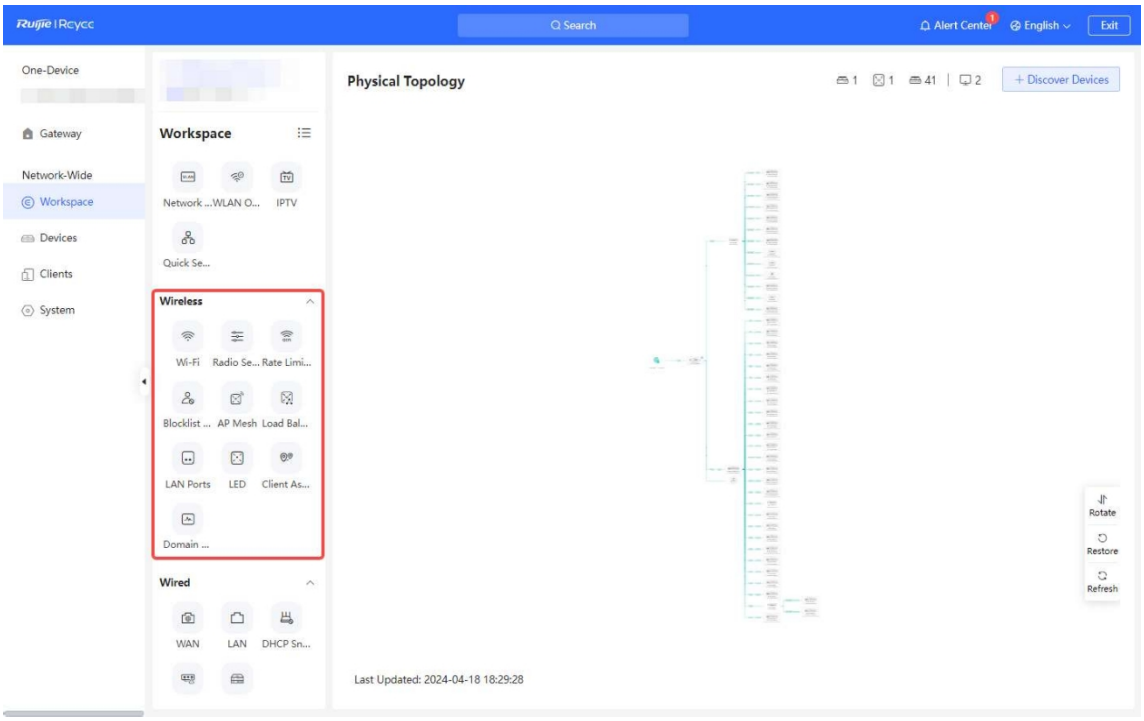


(3) Будь ласка, підтвердіть доставлені конфігурації та натисніть **Зберегти**. Конфігурації набудуть чинності через кілька хвилин.



3.4 Бездротова мережа в масштабі всієї мережі Керування

Виберіть **Мережевий**> **Робоча область**> **Бездротовий**.

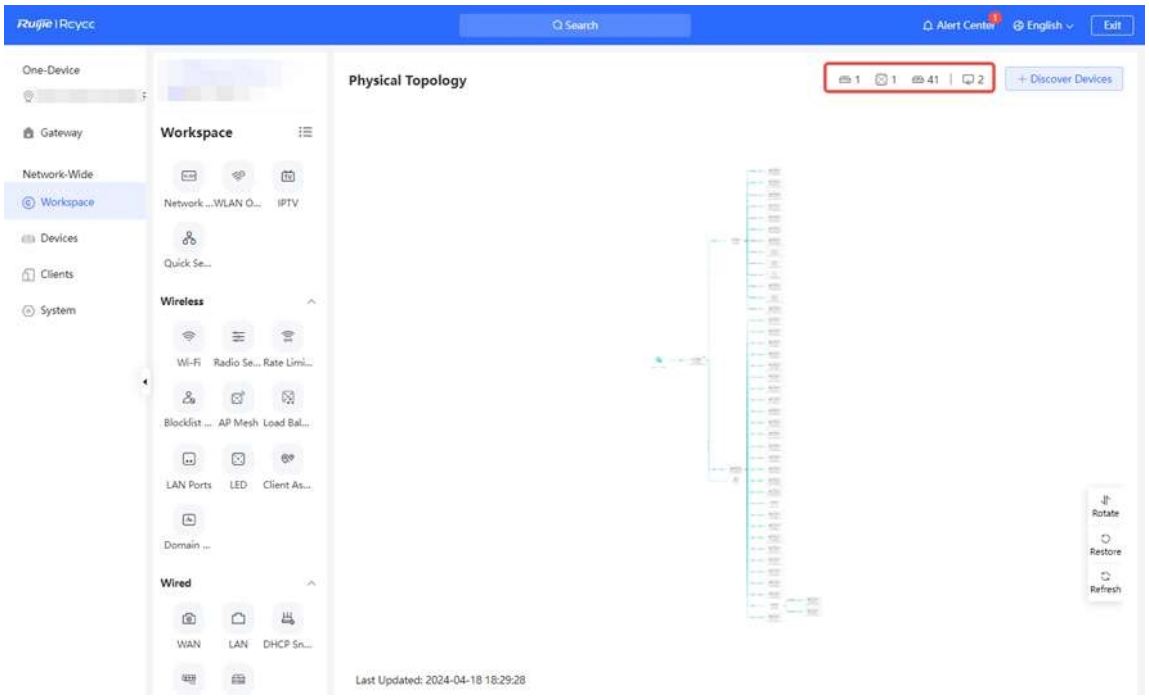


Функції, що підтримуються мережевим керуванням бездротовою мережею, залежать від пристроїв AP у мережі. Детальну інформацію про підтримувані функції можна знайти у веб-посібнику з конфігурації, що додається до пристроїв RG-RAP та RG-EAP. Наприклад, якщо версія програмного забезпечення пристрою точки доступу - ReyeeOS 2.280, функції, що підтримуються функцією Network-wide Wireless Management, можна знайти у веб-посібнику з конфігурації RG-RAP і RG-EAP для версії ReyeeOS 2.280.

3.5 Пристрої Управління

Перегляд інформації про всі пристрої в поточній мережі. Користувачі можуть налаштовувати і керувати всією мережею пристроїв, просто увійшовши до одного пристрою в мережі. Доступ до керування пристроями можна отримати наступними способами:

- Спосіб 1: Натисніть на іконку пристрою у верхньому правому куті **фізичної топології**, щоб перейти до перегляду списку пристроїв.



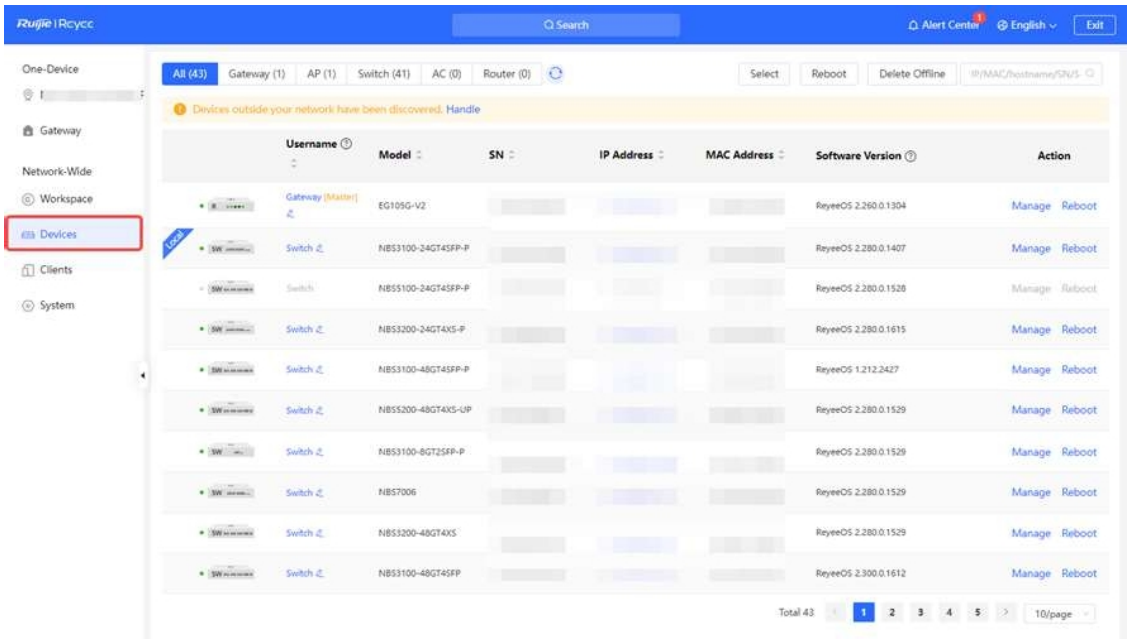
- Спосіб 2: Виберіть **загальномережеві**> пристрої

  Натисніть <Handle>, щоб додати незгрупований пристрій до поточної

  мережі. Натисніть <Керувати>, щоб налаштувати певний пристрій.

  Натисніть <Перезавантажити>, щоб перезавантажити певний пристрій.

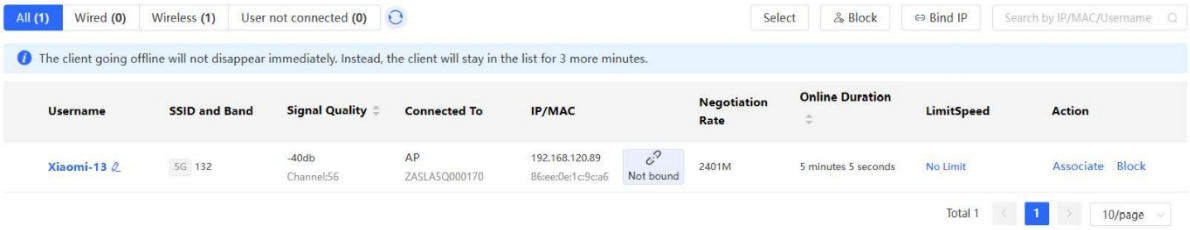
  Натисніть <Вибрати>, перевірте автономні пристрої, натисніть <Видалити автономні>, і пристрої можна буде видалити зі списку і топології мережі.



3.6 Онлайн-клієнт Управління

Виберіть **мережеві клієнти>** .

Список клієнтів відображає дротових, бездротових і не підключених до поточної мережі користувачів, включаючи ім'я користувача, режим підключення, пов'язаний пристрій, IP/MAC-адресу, статус прив'язки IP-адреси, тариф і пов'язані з ним операції.



- Натисніть **Не прив'**в колонці **IP/MAC**, щоб прив'язати клієнта до статичної IP-адреси.
- Натисніть кнопку в колонці Дія, щоб виконати відповідну операцію в онлайн-клієнті.
  - Дротова: Можна налаштувати лише контроль доступу.
  - Бездротовий: Можна налаштувати контроль доступу, асоціювання та блокування.

Примітка

Прив'язка до IP-адреси та контроль доступу підтримуються тільки в режимі роутера.

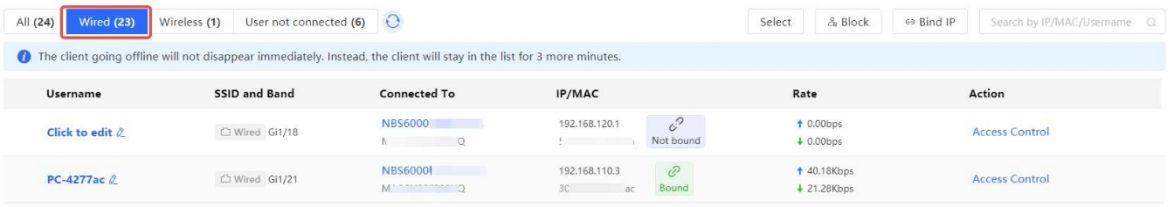
Таблиця 3-1 Параметри конфігурації онлайн-керування клієнтами

Параметр	Опис
Ім'я користувача	Ім'я підключеного клієнта.
SSID та діапазон	Показує режим доступу клієнта, який може бути бездротовим або дротовим. SSID та діапазон частот відображається, якщо клієнт підключений бездротово.
Якість сигналу	Потужність Wi-Fi сигналу клієнта та пов'язаного з ним каналу. **Примітка** Ця інформація відображається лише у списку бездротових онлайн-клієнтів.
Підключено до	Вказує на дротове або бездротове з'єднання, пов'язаний з ним пристрій та SN.
IP/MAC	Вказує IP-адресу та MAC-адресу клієнта.
Договірна ціна	Швидкість висхідної та низхідної лінії зв'язку клієнта. **Примітка** Ця інформація відображається лише у списку бездротових онлайн-клієнтів.

Параметр	Опис
Тривалість онлайн	Тривалість доступу клієнта. **Примітка** Ця інформація відображається лише у списку бездротових онлайн-клієнтів.
Обмеження швидкості	Впровадьте обмеження швидкості бездротового з'єднання для клієнтів щоб запобігти споживанню певними клієнтами великої кількості ресурсів пропускної здатності. Докладні відомості див. у розділі 3.6.4 Налаштування обмеження швидкості для клієнтів. **Примітка** Ця інформація відображається лише у списку бездротових онлайн-клієнтів.
Дія	Ви можете натиснути відповідну кнопку, щоб виконати контроль доступу, асоціювання та блокування операцій з онлайн-клієнтами.

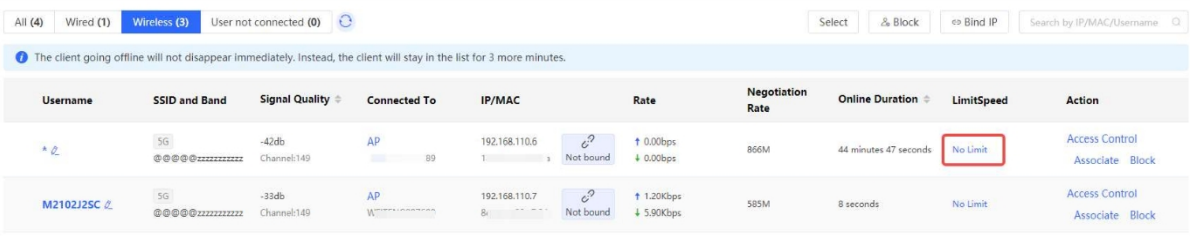
- **Дротові клієнти**

  Перейдіть на вкладку **Дротові**, щоб переглянути інформацію про дротових клієнтів.



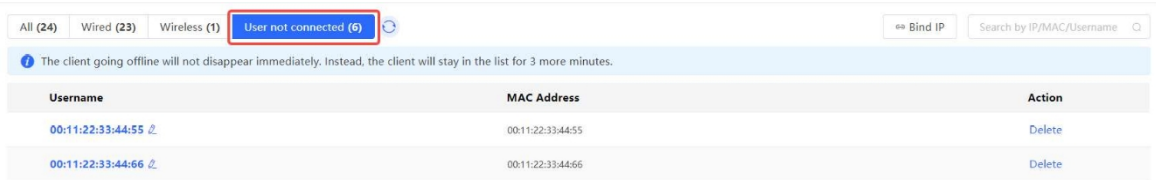
- **Бездротові клієнти**

  Перейдіть на вкладку **Бездротовий зв'**язок, щоб переглянути інформацію про клієнтів wirelss.



- **Користувача не підключено**

  Перейдіть **на вкладку Користувачі, яких не підключено**, щоб переглянути відомості про клієнтів, які очікують на підключення. До цього списку входять клієнти, позначені вручну або розпізнані як пристрої, які раніше було підключено до мережі, але яких наразі немає у списках керування пристроями або в онлайн-списках клієнтів. Щоб видалити клієнтський пристрій, натисніть **Видалити**.



3.6.1 Налаштування IP-адреси клієнта Прив'язка

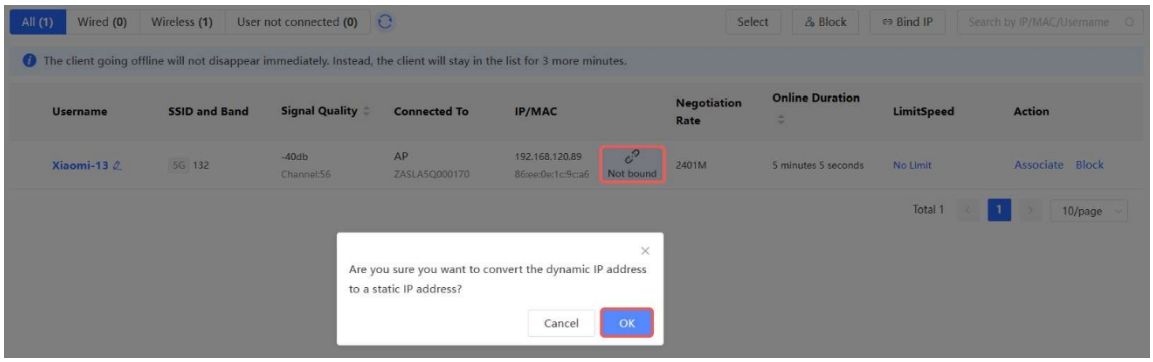
Примітка

Ця функція підтримується тільки в режимі маршрутизатора.

Виберіть **мережеві клієнти>** .

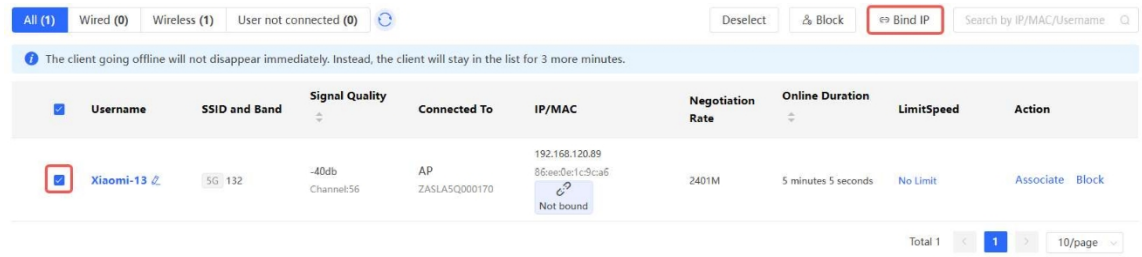
Прив'язка IP-адрес - це політика безпеки та контролю доступу, яка пов'язує певну IP-адресу з певним пристроєм або користувачем для забезпечення автентифікації особи, контролю доступу, моніторингу та обліку.

- Прив'язка IP-адреси одного клієнта
  Виберіть клієнта, якого потрібно прив'язати до IP-адреси, у списку, натисніть **Не прив'язано** і натисніть **OK** у спливаючому вікні, щоб прив'язати клієнта до статичної IP-адреси.

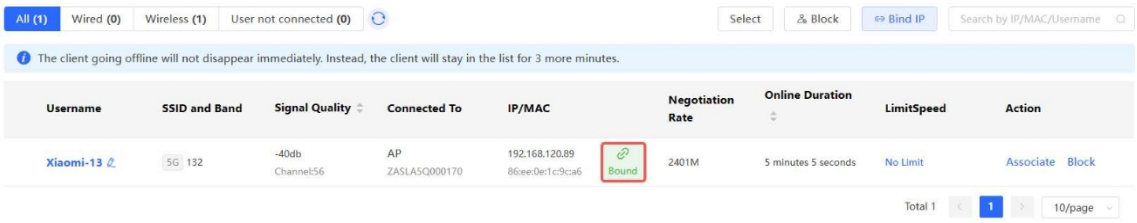


- Пакетна прив'язка IP натисніть **Вибрати**.

Виберіть клієнтів, яких потрібно прив'язати, натисніть **Прив'язати IP** і натисніть **OK** у спливаючому вікні, щоб прив'язати вибраних клієнтів до статичної IP-адреси.



- Відв'язати IP-адресу
  Виберіть клієнта, якого потрібно відв'язати, зі списку, натисніть **Прив'язати** і натисніть **OK** у спливаючому вікні.



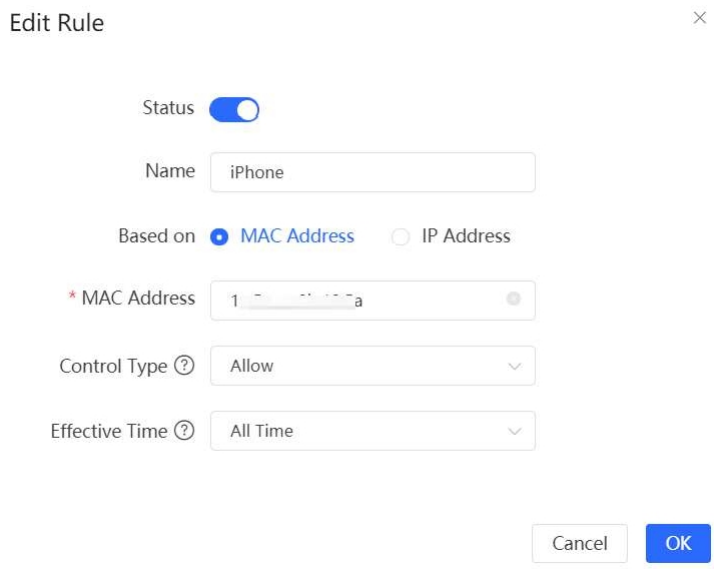
3.6.2 Налаштування клієнтського доступу Контроль

Примітка

Ця функція підтримується тільки в режимі маршрутизатора.

Виберіть **мережеві клієнти>** .

Виберіть клієнта у списку і натисніть **Контроль доступу** в колонці **Дія**. Вас буде перенаправлено на сторінку **Редагування правила**, де буде автоматично створено правило контролю доступу на основі MAC-адреси. Ім'я та MAC-адреса автоматично генеруються на основі вибраного клієнта. Після вибору типу контролю і часу дії натисніть **OK**, щоб створити правило контролю доступу для клієнта.



3.6.3 Блокування Клієнтів

Виберіть **мережеві клієнти>** .

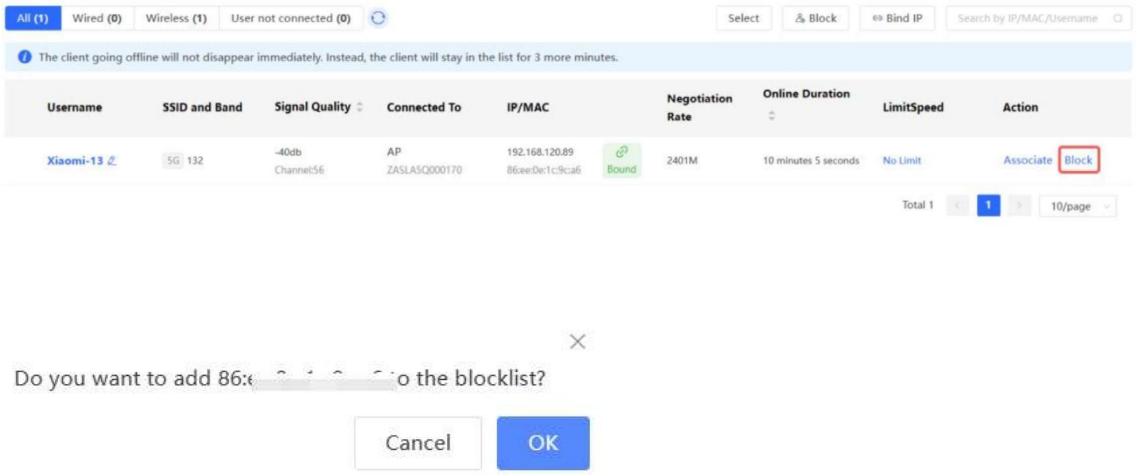
Неавторизований клієнт може займати пропускну здатність мережі і створювати ризики для безпеки. Ви можете заблокувати певних клієнтів, щоб вирішити проблему несанкціонованого доступу.

Примітка

Клієнтський блок доступний лише для бездротових клієнтів.

- Заблокувати одного клієнта

Виберіть клієнта для блокування у списку, натисніть **Блокувати** у колонці **Дія** і натисніть **ОК** у спливаючому вікні, щоб заблокувати вибраного клієнта.



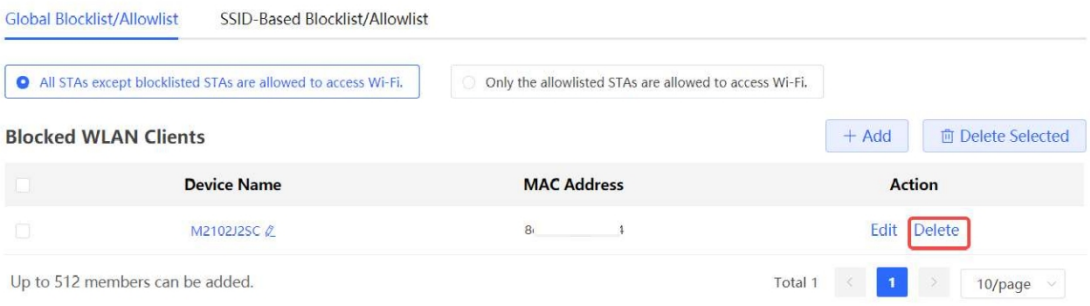
- Клієнти пакетних блоків а Натисніть **"Вибрати"**.

b Виберіть цільових клієнтів, натисніть **Блокувати** і натисніть **ОК** у спливаючому вікні, щоб заблокувати вибраних клієнтів.

- Скасувати блокування

Виберіть **Мережевий> Робоча область> Бездротовий> Список блокування/дозволів> Глобальний список блокування/дозволів.**

Виберіть клієнта, якого потрібно видалити зі списку блокування, у списку блокування бездротових мереж і натисніть **Видалити**.



3.6.4 Налаштування клієнтського тарифу Обмеження

Виберіть **Мережа в цілому> Клієнти> Бездротовий зв'язок**.

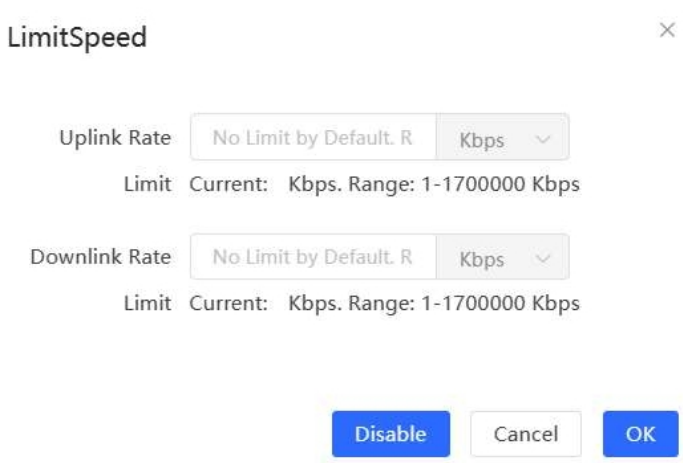
Щоб забезпечити справедливий розподіл ресурсів, мережевий адміністратор може обмежити швидкість бездротового з'єднання, щоб запобігти використанню деякими користувачами або пристроями великої кількості пропускної здатності і погіршенню роботи інших користувачів.

Примітка

Обмеження швидкості застосовується лише до бездротових клієнтів.

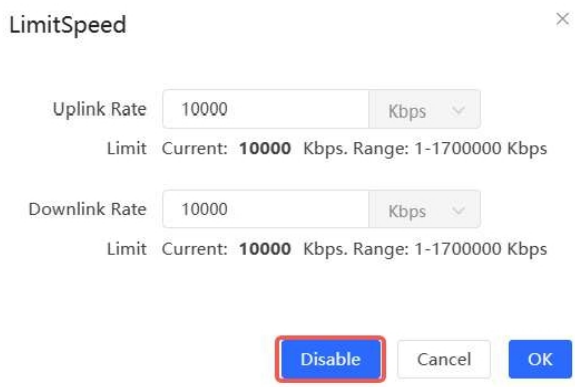
- Налаштуйте ліміти тарифів для клієнтів

  Перейдіть на вкладку **Бездротовий** зв'язок, клацніть стовпчик **LimitSpeed** у таблиці, встановіть ліміт швидкості висхідної лінії зв'язку та ліміт швидкості низхідної лінії зв'язку і натисніть кнопку **OK**.



- Скасування тарифних обмежень

  Перейдіть на вкладку **Бездротовий зв'язок**, клацніть стовпчик **LimitSpeed** у таблиці і натисніть **Вимкнути**.



3.7 Брандмауер Управління

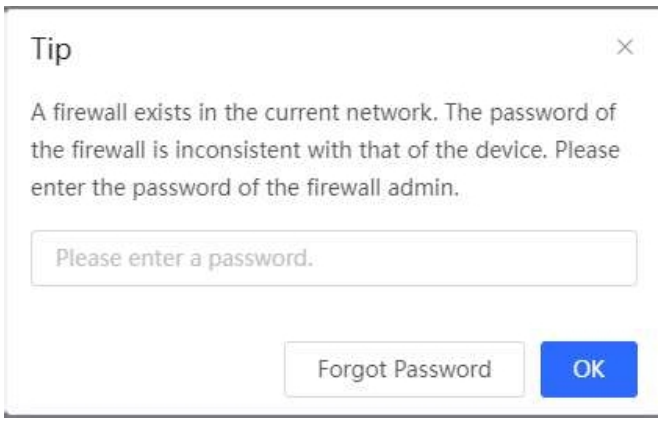
Після додавання брандмауера до мережі ви можете керувати ним і налаштовувати його за допомогою веб-системи керування.

3.7.1 Перегляд брандмауера Інформація

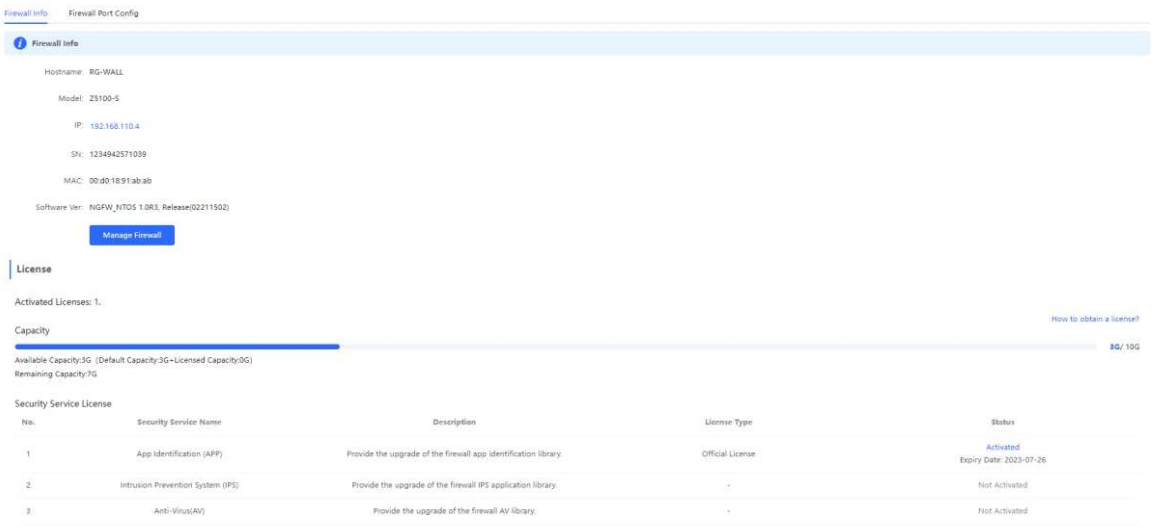
Ви можете переглянути основну інформацію та ліцензію брандмауера у веб-системі керування.

Виберіть **Мережа в цілому > Мережа > Брандмауер**.

(1) Якщо пароль брандмауера не збігається з паролем шлюзу, введіть пароль керування брандмауера і натисніть **OK**.



(2) Основна інформація, пропускна здатність і ліцензія служби безпеки брандмауера відображаються у веб-системі керування.



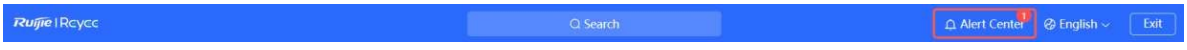
Натисніть **Керування брандмауером**, щоб перейти до веб-інтерфейсу керування . Налаштуйте політику безпеки і активацію ліцензії для брандмауера. Докладні відомості див. у посібнику з веб-налаштування брандмауера.

3.7.2 Налаштування брандмауера Порт

Якщо брандмауер налаштовано на прозорий режим, з'явиться сторінка **Конфігурація порту брандмауера**. Ви можете вибрати WAN-порт, підключений до шлюзу, або LAN-порт, підключений до комутатора, і ввімкнути функцію **Security Guard**.

3.8 Сповіщення

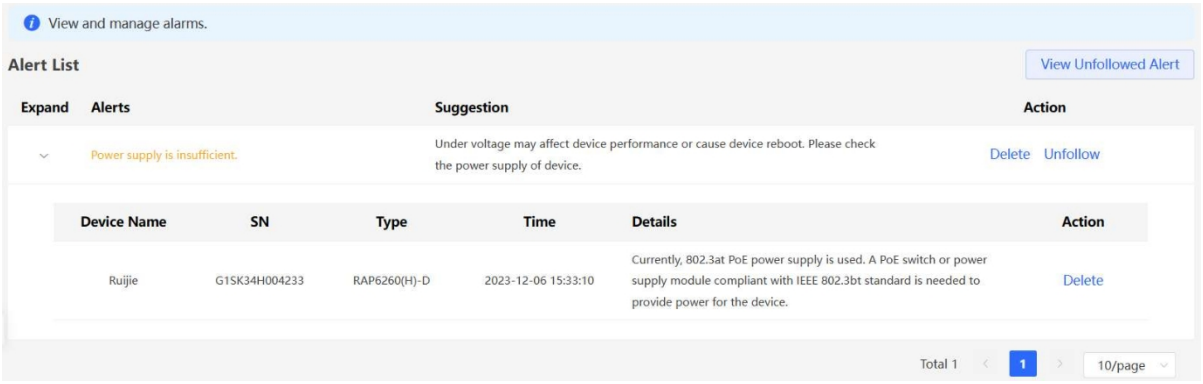
Коли виникає виняток у мережі, на сторінці огляду мережі з'являється сповіщення та рекомендація. Клацніть сповіщення у **Центрі сповіщень**, щоб переглянути несправний пристрій, деталі та опис проблеми. Ви можете усунути несправність на основі підказки.

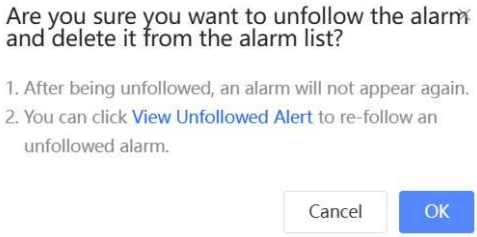


На сторінці **Список тривог** відображаються можливі проблеми у мережевому середовищі та на пристрої. За замовчуванням всі типи тривог відстежуються. Ви можете натиснути кнопку **Відмінити** у стовпчику **Дія**, щоб скасувати відстеження цього типу тривоги.

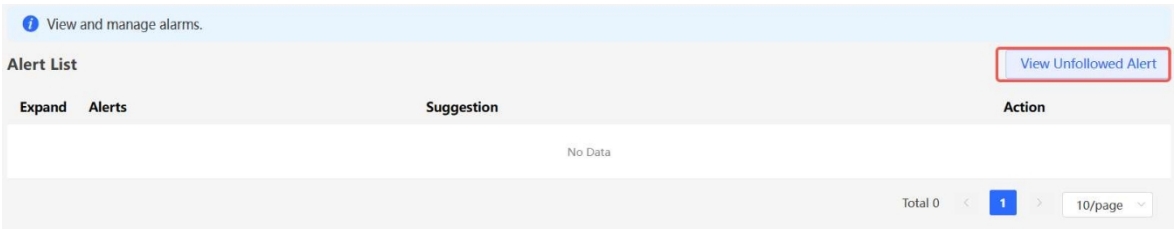
Застереження

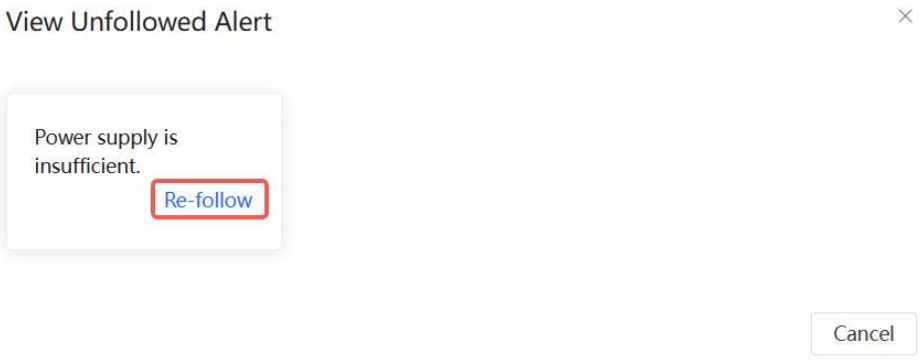
Відмовившись від відстеження певного типу оповіщення, ви не зможете оперативно виявити та обробити всі оповіщення цього типу. Тому будьте обережні, виконуючи цю операцію.





Натисніть **Переглянути** сповіщення, яке не було відстежено, щоб переглянути сповіщення, яке не було відстежено. Ви можете повторно відстежити оповіщення у спливаючому вікні.





3.9 Smart Device Мережа

Застереження

Наразі функція підтримується пристроями серій RG-NBS6002, RG-NBS7003 та RG-NBS7006.

3.9.1 Огляд

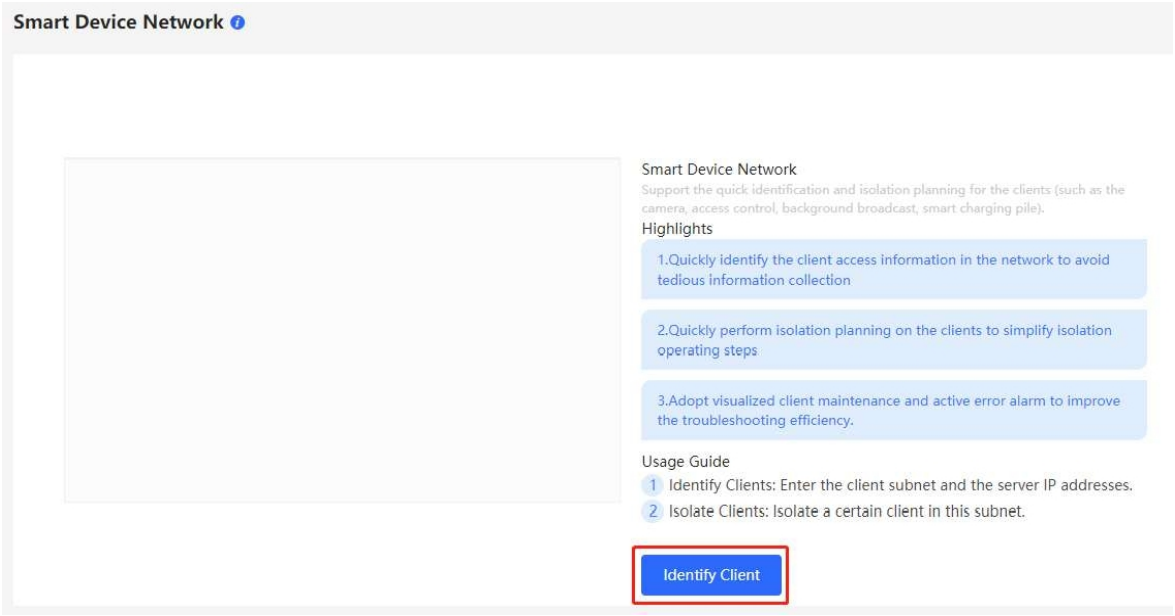
Мережа розумних пристроїв використовується для швидкого планування та налаштування мережі ізоляції для розумних клієнтів, щоб ізолювати клієнтську мережу від звичайної сервісної мережі та інших типів клієнтів, а також підвищити стабільність роботи мережі. Мережа розумних пристроїв підтримує швидку ідентифікацію різних типів клієнтів (таких як камери, контроль доступу, фонове мовлення, розумні зарядні пристрої тощо) та пакетне виконання планування ізоляції клієнтів. У порівнянні з традиційними етапами планування та розгортання клієнтської мережі, це усуває виснажливий процес, збирає інформацію та спрощує кроки з налаштування ізоляції клієнтів.

Після налаштування мережі інтелектуальних пристроїв на сторінці візуально відображається інформація про клієнта, а також активно сповіщається про несправності, що може ефективно підвищити ефективність усунення несправностей.

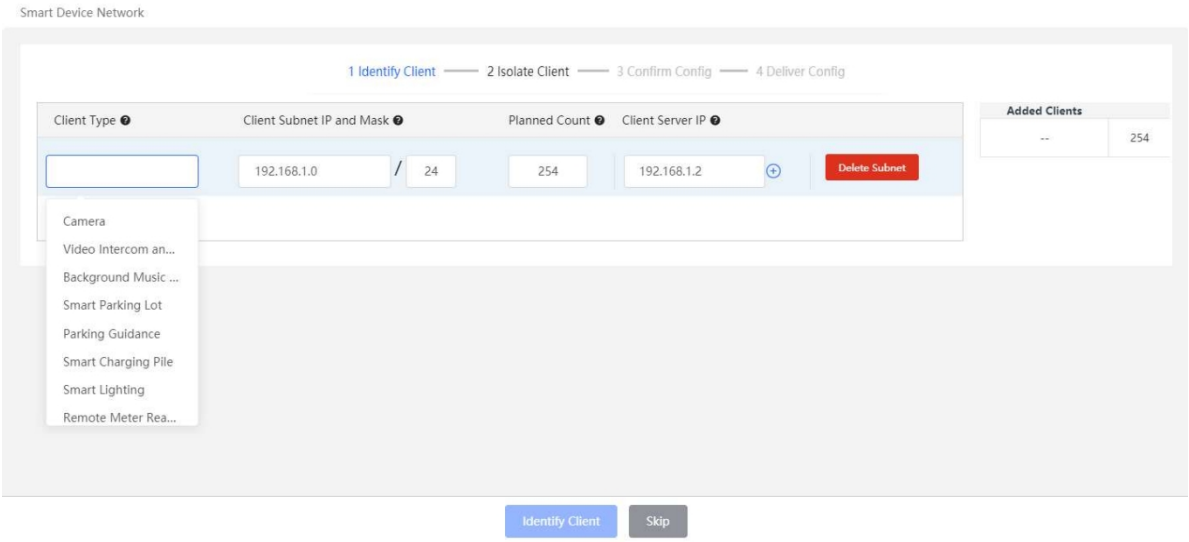
3.9.2 Процедура

Виберіть **Мережа в цілому> Клієнти> Мережа розумних пристроїв**.

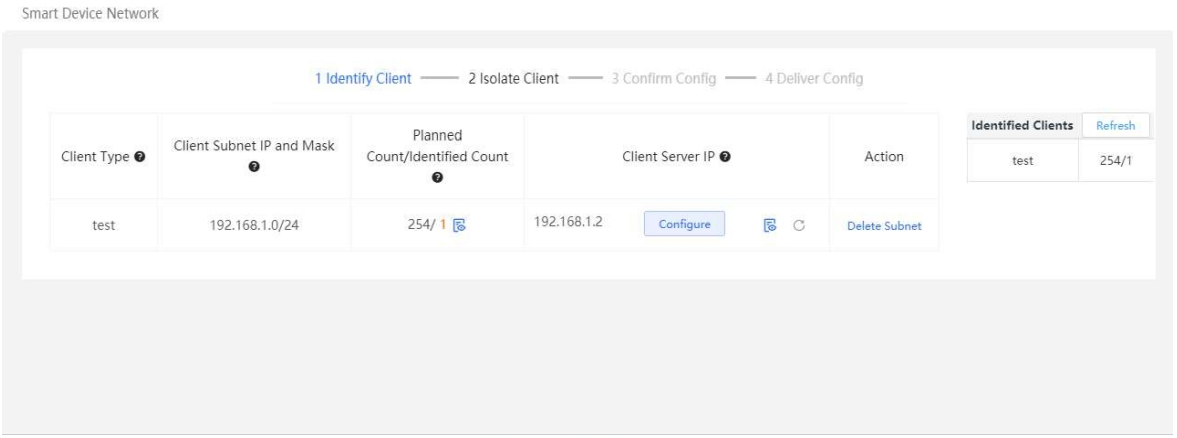
(1) Натисніть **Ідентифікувати клієнта**.

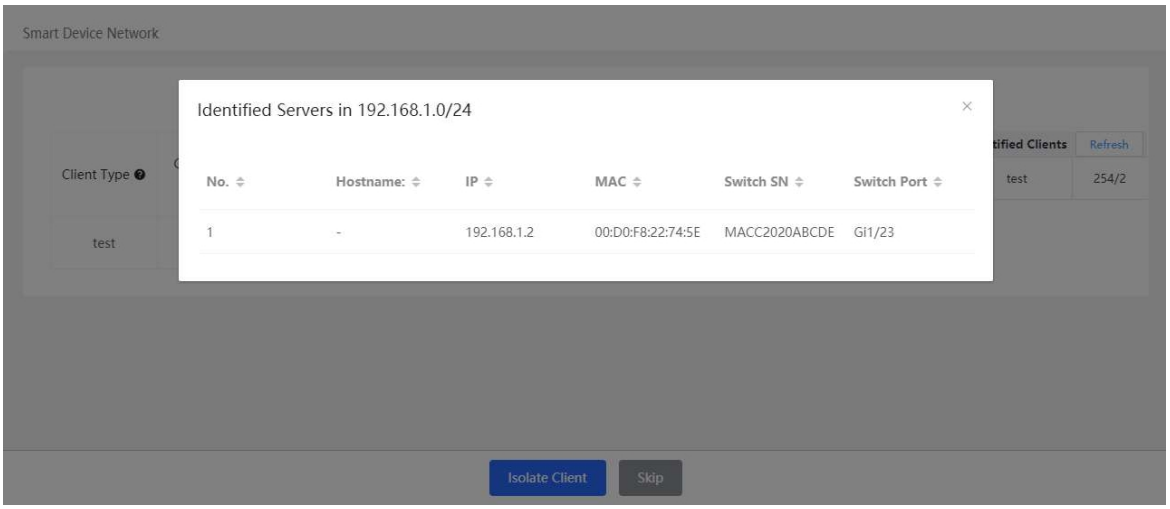


(2) Натисніть **+Client Subnet**, введіть тип клієнта (який можна вибрати або налаштувати у випадаючому списку), мережевий сегмент клієнта, запланований номер і відповідну IP-адресу сервера для ідентифікації клієнта. Можна вказати декілька сегментів мережі клієнта. Після заповнення натисніть **Ідентифікувати клієнта**.

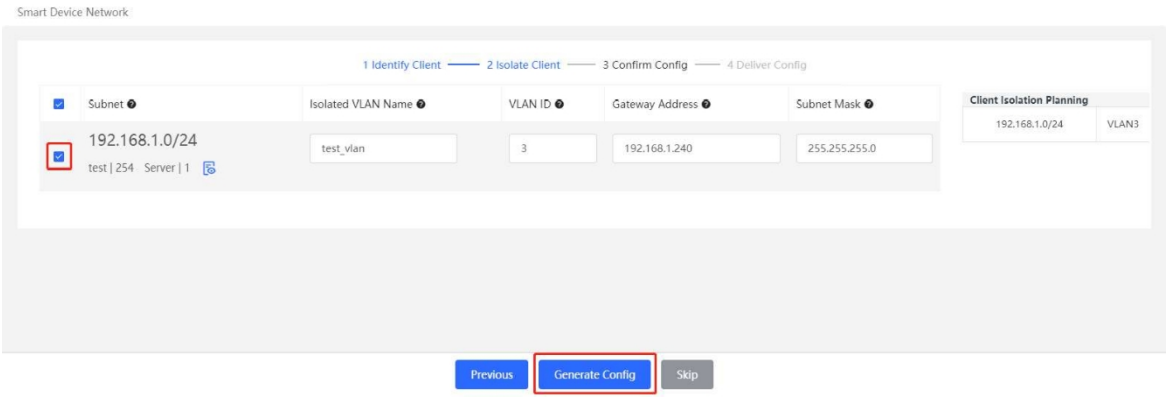


(3) Відображення інформації про ідентифікованого клієнта і клієнт-сервер, включаючи IP-адресу, MAC-адресу, підключеного комутатора і порт підключення. Натисніть, щоб переглянути детальну інформацію. Якщо інформація про з'єднання з клієнт-сервером не ідентифікована, необхідно натиснути **Налаштувати** і заповнити відповідну інформацію вручну. Переконавшись, що інформація про клієнтський пристрій правильна, натисніть **Ізолювати клієнта**.

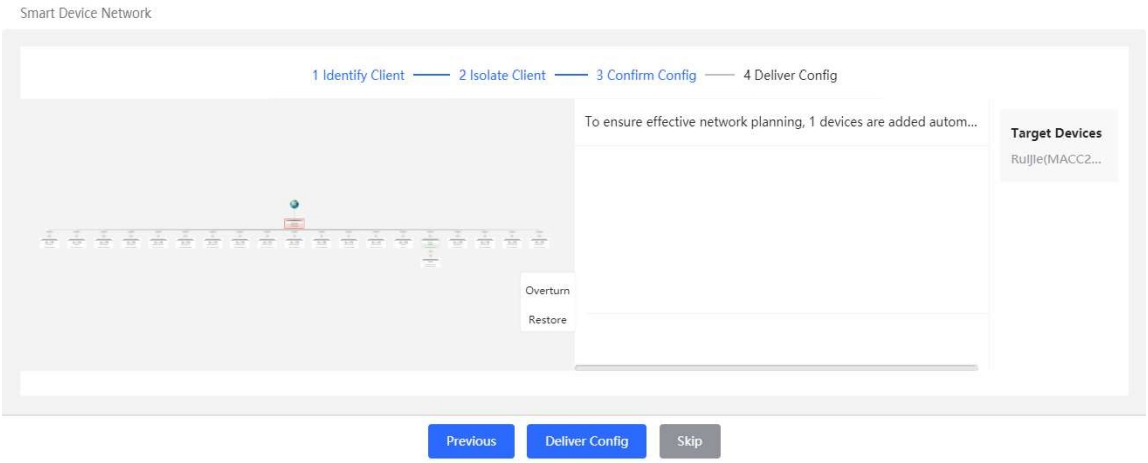




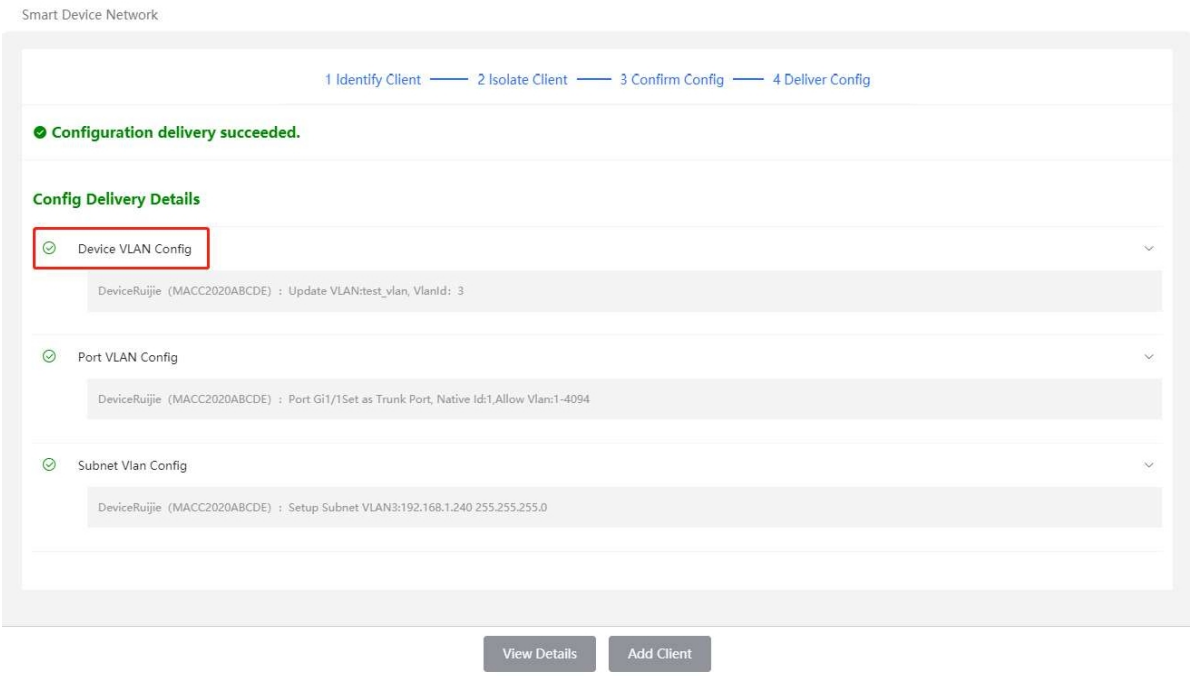
(4) Введіть назву VLAN, ідентифікатор VLAN, адресу шлюзу та маску підмережі ізольованого клієнта. цільовий сегмент мережі і натисніть кнопку **Створити конфігурацію**.



(5) Підтвердивши конфігурацію, натисніть **Deliver Config**. Якщо вам потрібно змінити її, ви можете натиснути **Попередньо**, щоб повернутися на сторінку налаштувань.



(6) На сторінці буде показано, що конфігурацію успішно доставлено, що означає, що налаштування завершено. Клацніть елемент конфігурації, щоб переглянути деталі доставки конфігурації. Після того, як конфігурацію буде доставлено, натисніть **Переглянути деталі**, щоб перейти на сторінку з інформацією про моніторинг мережі інтелектуальних пристроїв; натисніть **Додати клієнта**, щоб продовжити налаштування клієнтського сегмента мережі.

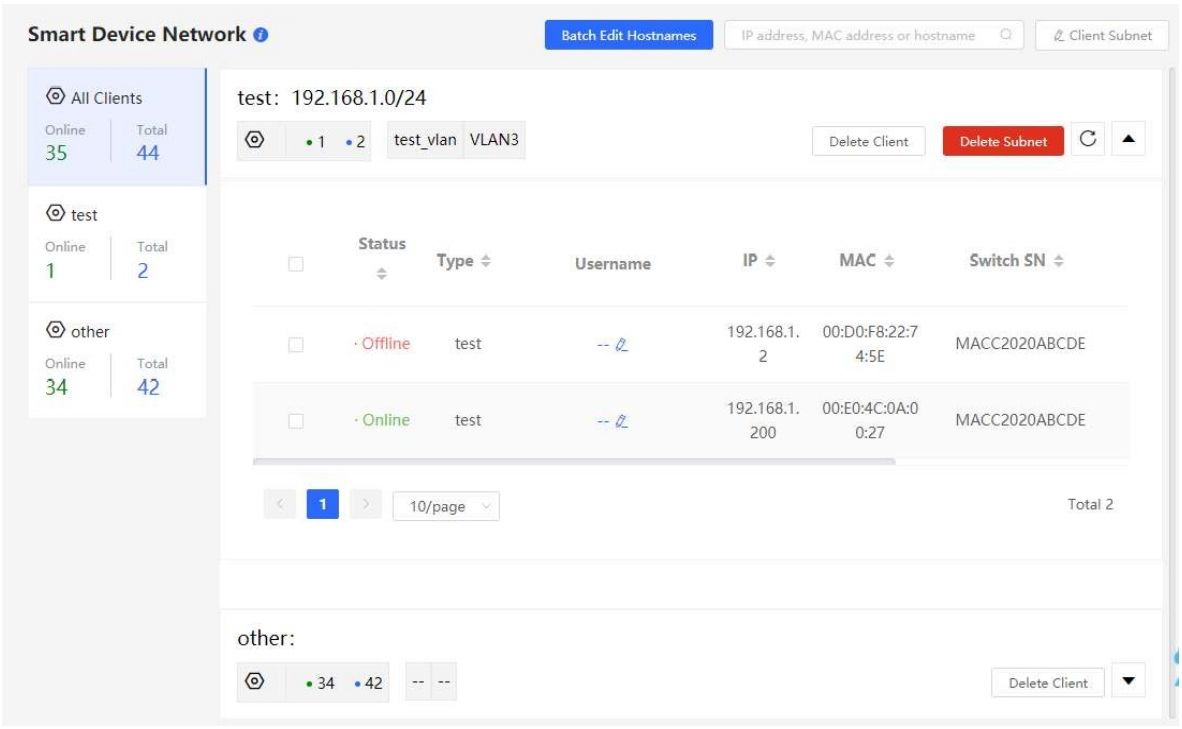


(7) Після завершення мережевих налаштувань смарт-пристрою ви можете переглянути інформацію про моніторинг клієнта на сторінці, включаючи статус клієнта в мережі, інформацію про з'єднання, інформацію про пристрій, а також час перебування в мережі та в автономному режимі.

Виберіть запис клієнта і натисніть **Видалити клієнта**, щоб видалити вказаного клієнта з поточної мережі.

Натисніть **Пакетне редагування імен хостів**, щоб імпортувати txt-файл, що містить IP-адресу та ім'я клієнта (один рядок для кожного клієнта, кожен рядок містить IP-адресу та ім'я, а IP-адреса та ім'я розділяються клавішею Tab), і змінити імена клієнтів у пакетному режимі.

Натисніть **Клієнтська підмережа**, щоб змінити сервери та ізолювати інформацію про VLAN або додати новий сегмент клієнтської мережі. Натисніть **Видалити підмережу**, щоб видалити відповідну мережеву конфігурацію інтелектуального пристрою.

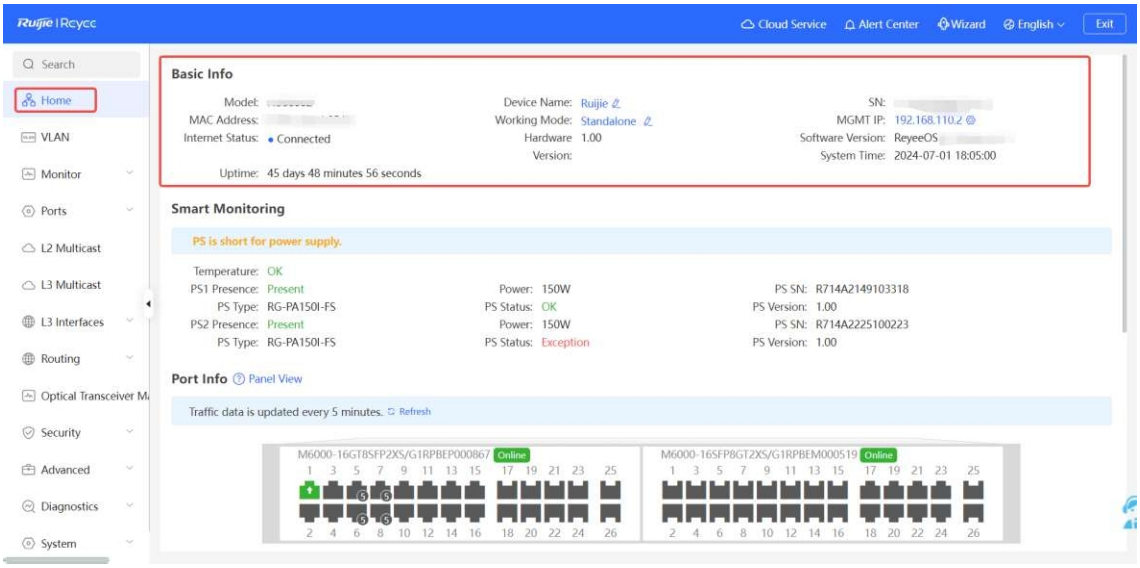


4 One-Device Інформація

4.1 Основна інформація про пристрій One-

Виберіть **Локальний пристрій**> **Головна**> **Основна інформація**.

Основна інформація включає назву пристрою, модель пристрою, номер SN, версію програмного забезпечення, IP-адресу управління, MAC-адресу, стан мережі, системний час, режим роботи тощо.

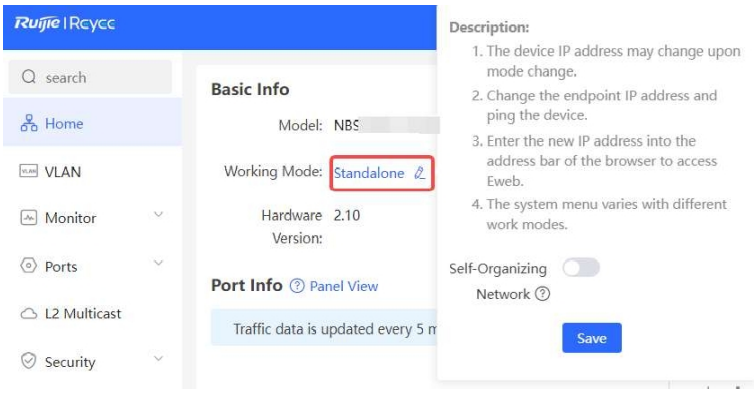


1. Налаштування назви пристрою

Натисніть на назву пристрою, щоб змінити назву пристрою, щоб розрізняти різні пристрої.

2. Перемикання режиму роботи

Натисніть на поточний роботи, щоб змінити його.



3. Налаштування MGMT IP

Натисніть поточну IP-адресу керування, щоб перейти на сторінку конфігурації IP-адреси керування. Для отримання додаткової інформації див. розділ 7.6 Налаштування IP-адреси MGMT.

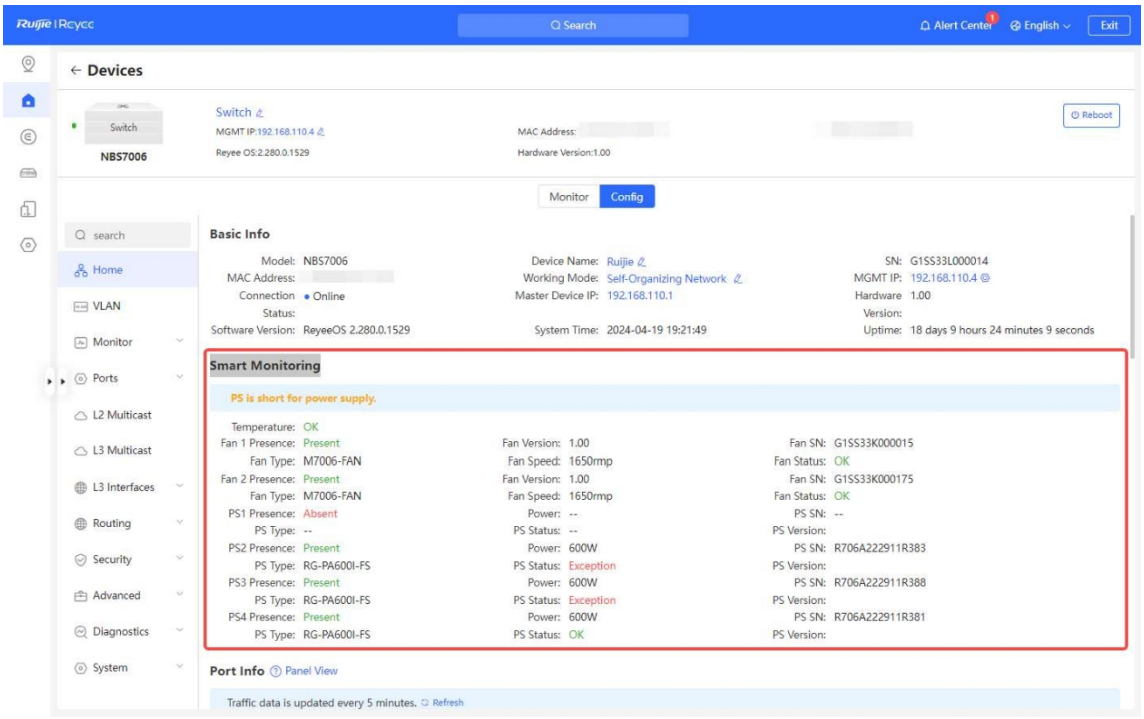
4.2 Smart Моніторинг

Застереження

Тільки пристрої RG-NBS7006, RG-NBS7003 і RG-NBS6002 підтримують відображення цього типу інформації.

Виберіть **Локальний пристрій > Головна> Розумний моніторинг**.

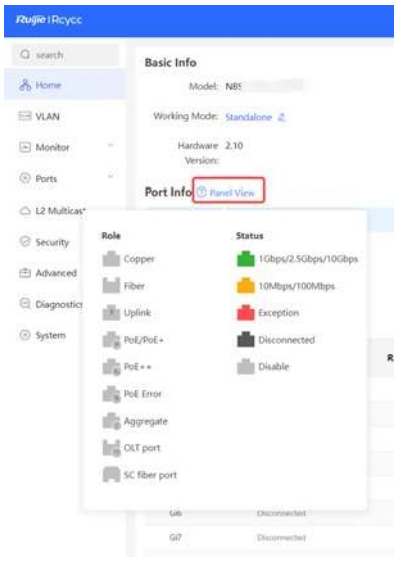
Відображення поточного стану апаратного забезпечення пристрою, наприклад, температури пристрою, стану джерела живлення тощо.



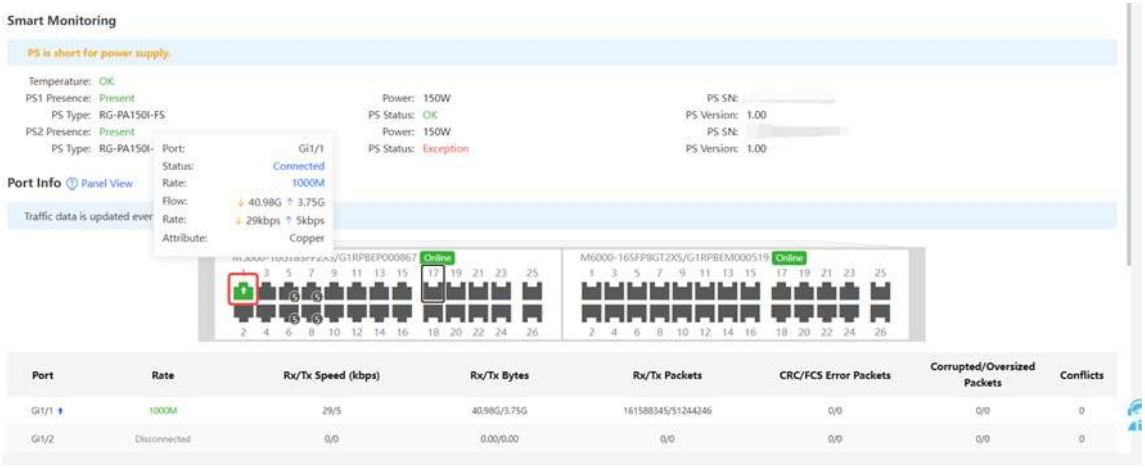
4.3 Порт Інформація

Виберіть **Локальний пристрій**> **Головна**> **Інформація про порт**.

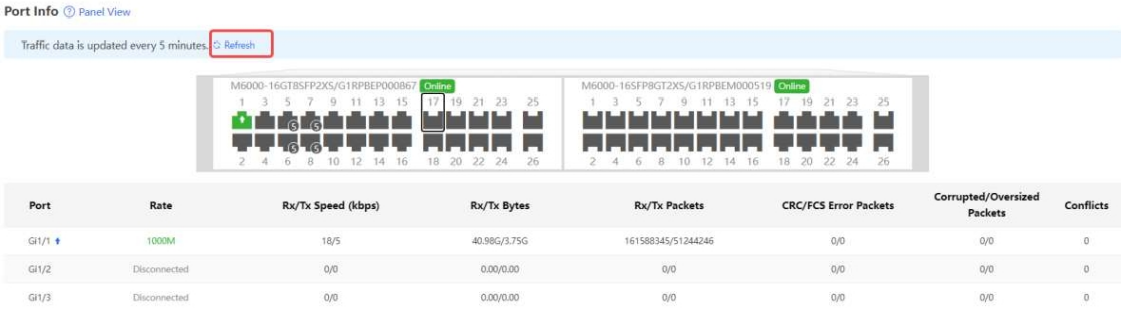
- На сторінці відомостей про порт відображається інформація про всі порти, які наразі підключено до комутатора. Натисніть **Перегляд панелі**, щоб переглянути ролі та стани портів, які відповідають піктограмам портів різного кольору або форми.



- Наведіть курсор на іконку порту (наприклад, Gi14) на панелі портів, і буде показано додаткову інформацію про порт, включаючи ідентифікатор порту, стан порту, швидкість порту, висхідний і низхідний трафік, швидкість передачі та оптичні/електричні атрибути порту.



- Дані про трафік автоматично оновлюються кожні п'ять хвилин. Ви можете натиснути кнопку **Оновити** над панеллю портів, щоб одночасно отримати останню інформацію про трафік і стан порту.



5 VLAN

5.1 VLAN Огляд

Віртуальна локальна мережа (VLAN) - це логічна мережа, створена у фізичній мережі. VLAN має ті ж властивості, що і звичайна фізична мережа, за винятком того, вона не обмежена своїм фізичним розташуванням. Кожна VLAN має незалежний широкомовний домен. Різні VLAN ізольовані на рівні 2. Одноадресні, широкомовні та багатоадресні кадри 2-го рівня пересилаються і поширюються в межах однієї VLAN і не передаються в інші VLAN.

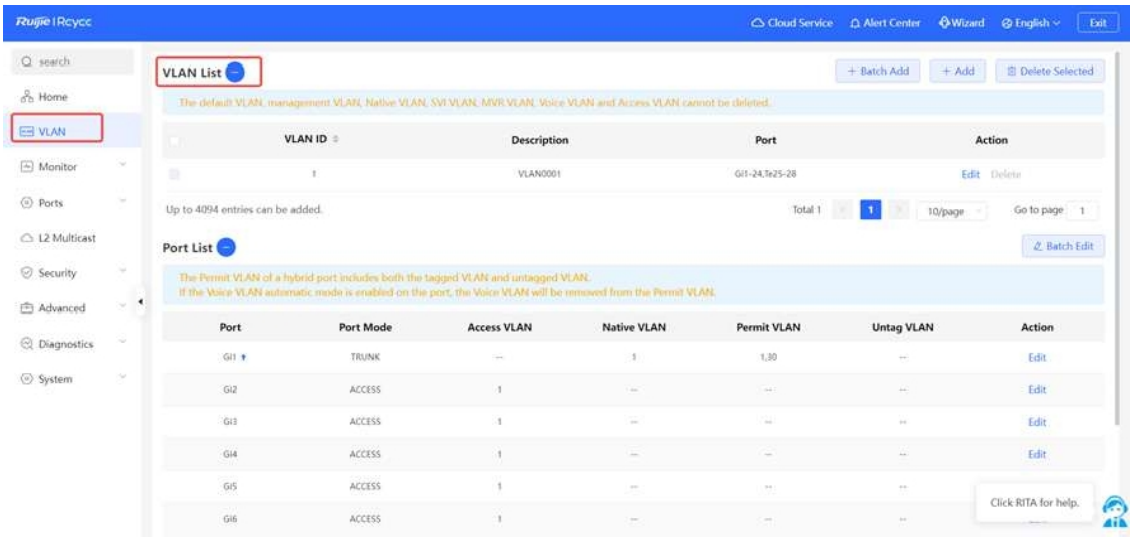
Коли порт визначено як член VLAN, усі клієнти, підключені до порту, є частиною VLAN. Мережа підтримує декілька VLAN. VLAN можуть здійснювати зв'язок на рівні 3 між собою через пристрої рівня 3 або інтерфейси рівня 3.

Поділ VLAN включає дві функції: створення VLAN і налаштування VLAN портів.

5.2 Налаштування VLAN

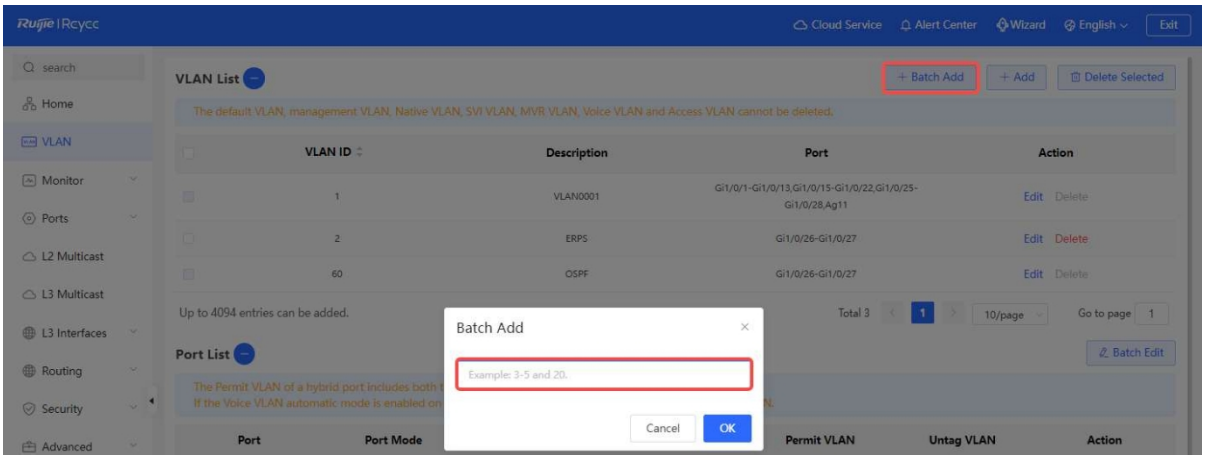
Виберіть **Локальний пристрій**> **VLAN**> **VLAN List**.

Список VLAN містить всю інформацію про існуючі VLAN. Ви можете змінити або видалити існуючу VLAN, або створити нову VLAN.

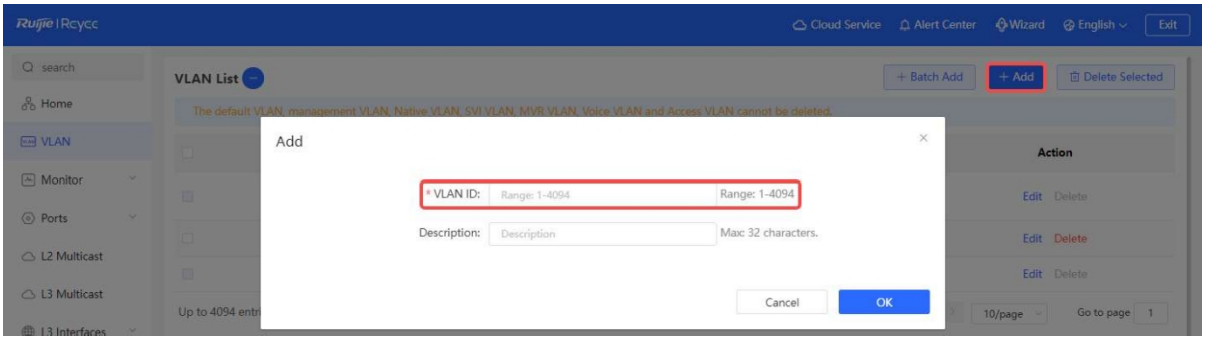


5.2.1 Додавання VLAN

Створіть кілька VLAN: Натисніть **Пакетне додавання**. У діалоговому вікні, що з'явиться, введіть діапазон ідентифікаторів VLAN (розділіть діапазони ідентифікаторів VLAN комами (,)) і натисніть кнопку **OK**. Додані VLAN буде відображено у **списку VLAN List (Список VLAN**).



Створити VLAN: Натисніть **Додати**. Введіть ідентифікатор та опис VLAN і натисніть **OK**. Додана VLAN буде відображена у **списку VLAN**.

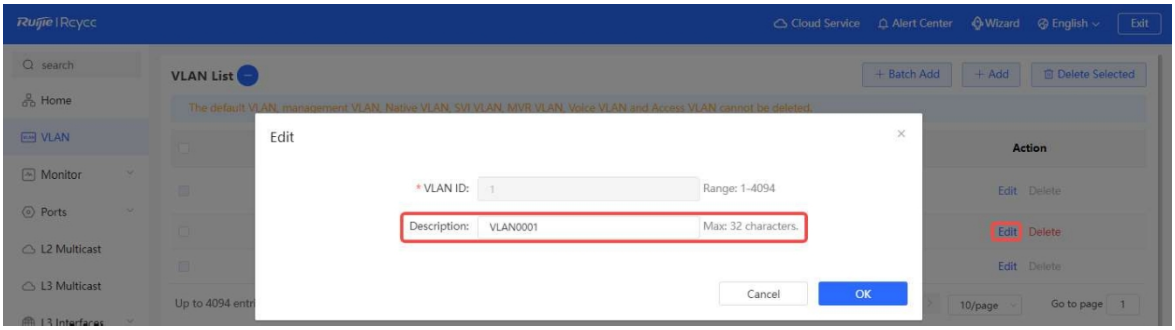


Примітка

- Діапазон ідентифікатора VLAN - від 1 до 4094.
- Ви можете відокремити декілька VLAN, які потрібно додати в пакетах, комами (,), а початковий і кінцевий ідентифікатори VLAN діапазону VLAN - дефісом (-).
- Якщо під час додавання VLAN не налаштовано опис VLAN, система автоматично створює опис VLAN у вказаному форматі, наприклад, VLAN000XX. Описи VLAN різних VLAN повинні бути унікальними.
- Якщо пристрій підтримує функції рівня 3, то VLAN, маршрутизовані порти та агреговані інтерфейси рівня 3 спільно використовують обмежені апаратні ресурси. Якщо ресурсів недостатньо, з'явиться повідомлення про недостатність ресурсів для VLAN.

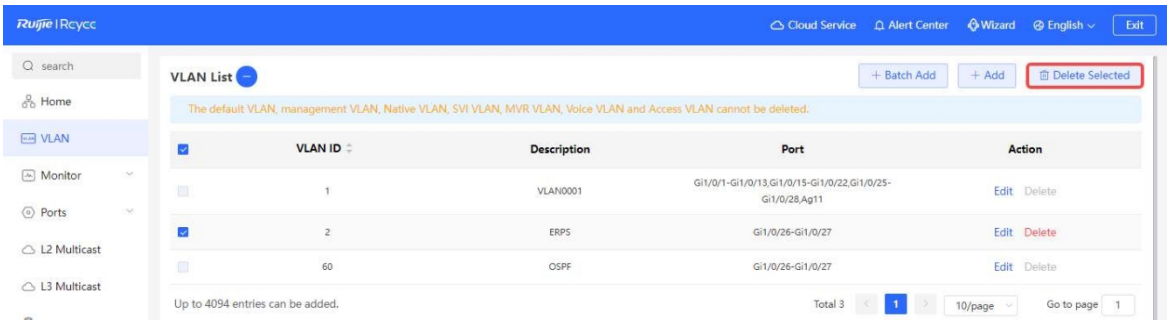
5.2.2 Зміна опису VLAN

У **списку VLAN** натисніть кнопку Змінити в останньому стовпчику Дія, щоб змінити інформацію про опис вказаної VLAN.

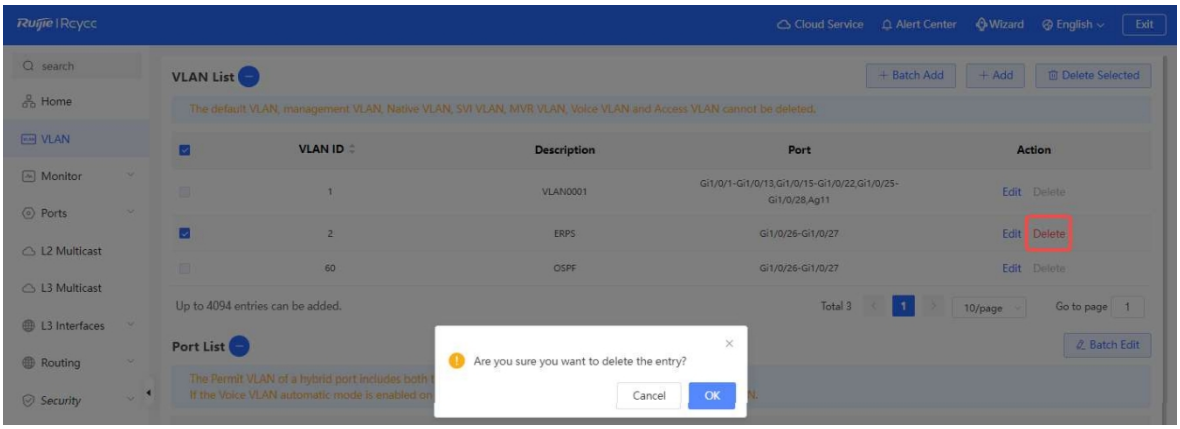


5.2.3 Видалення VLAN

Пакетне видалення VLAN: У **списку VLAN** виберіть записи VLAN, які потрібно видалити, і натисніть кнопку **Видалити вибране**, щоб видалити VLAN у групі.



Видалити VLAN: У **списку VLAN** натисніть **Видалити** в останньому стовпчику **Дія**, щоб видалити вказану **VLAN**.



Примітка

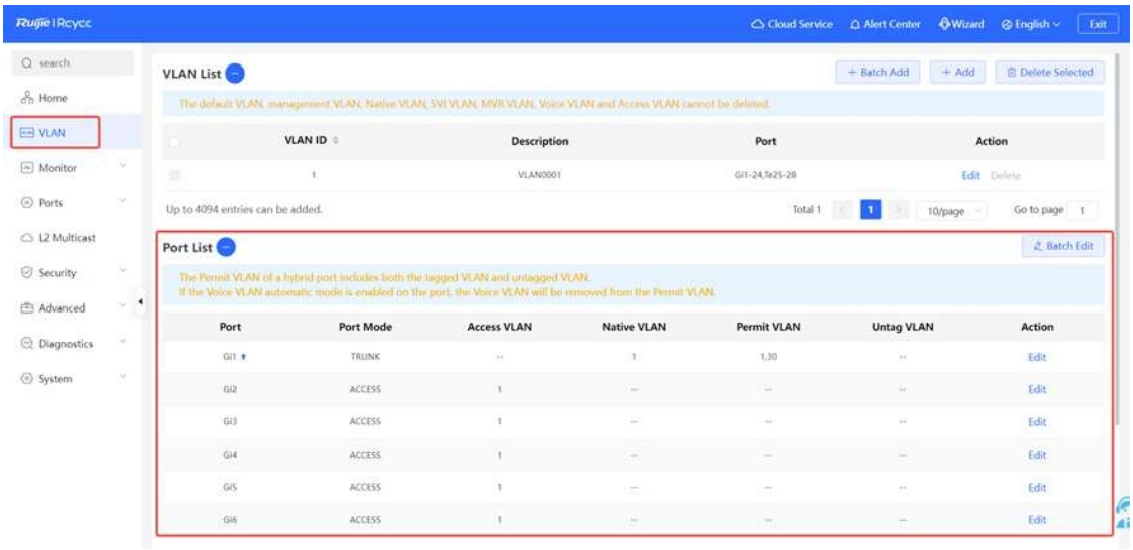
Не можна видалити VLAN за замовчуванням (VLAN 1), керуючу VLAN, власну VLAN і VLAN доступу. Для цих VLAN кнопка Видалити недоступна і позначена сірим кольором.

5.3 Налаштування VLAN порту

5.3.1 Огляд

Виберіть **Локальний пристрій**> **VLAN**> **Список портів**.

Список портів відображає розподіл поточного порту на VLAN. Створіть VLAN на сторінці **Список VLAN** (див. 5.2 Налаштування VLAN), а потім налаштуйте порт на основі VLAN.



Ви можете налаштувати режим порту і членів VLAN для порту, щоб визначити VLAN, яким дозволено проходити через порт, а також те, чи повинні пакети, що пересилаються портом, містити поле тегу.

Таблиця 5-1 Режими порту Опис режимів порту

Режим порту	Функція
Порт доступу	Один порт доступу може належати лише до однієї VLAN і лише кадри з цієї VLAN. Ця VLAN називається VLAN доступу. VLAN доступу має атрибути як власної VLAN, так і дозволеної VLAN Кадри, надіслані з порту доступу, не містять тегів. Коли порт доступу отримує немаркований кадр від однорангового пристрою, локальний пристрій визначає, що кадр з VLAN доступу, і додає ідентифікатор VLAN доступу до кадру.
Магістральний порт	Один магістральний порт підтримує одну власну VLAN і кілька дозволених VLAN. Кадри власної VLAN, що пересилаються магістральним портом, не містять тегів, тоді як кадри дозволеної VLAN, що пересилаються магістральним портом, містять теги. За замовчуванням магістральний порт належить до всіх VLAN пристрою і може пересилати кадри всіх VLAN. Ви можете встановити дозволений діапазон VLAN, щоб обмежити кадри VLAN, які можна пересилати. Зверніть увагу, що магістральні порти на обох кінцях з'єднання мають бути сконфігуровані з однаковою власною VLAN.
Гібридний порт	Гібридний порт підтримує одну власну VLAN і кілька дозволених VLAN. Дозволені VLAN поділяються на VLAN з тегами та VLAN без тегів. Кадри, що пересилаються гібридним портом з VLAN з тегами, містять теги, а кадри, що пересилаються гібридним портом з VLAN без тегів, не містять тегів. Кадри, що пересилаються гібридним портом з Native VLAN, не повинні містити тегів, тому Native VLAN може належати лише до списку Untagged VLAN.

Примітка

Чи підтримується функція гібридного режиму, залежить від версії продукту.

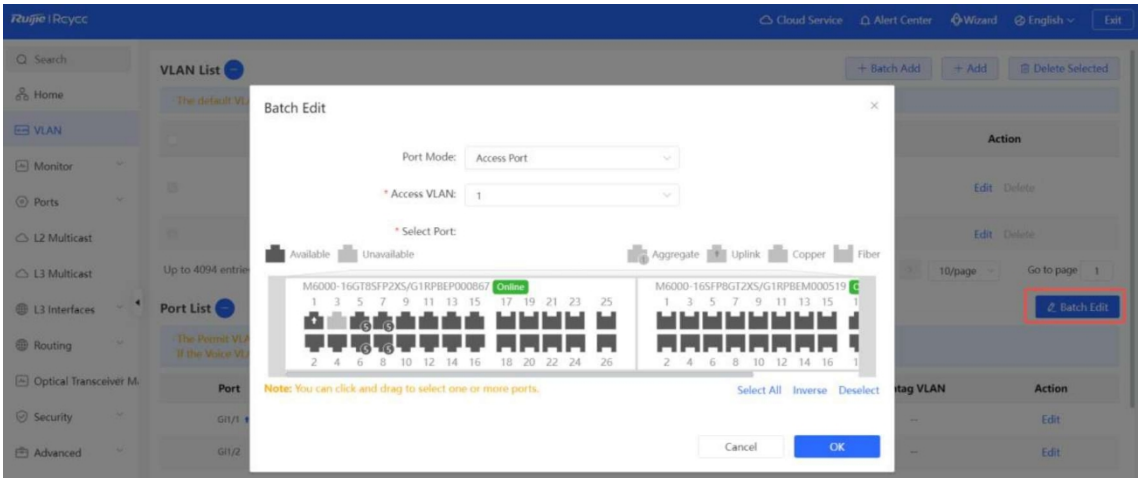
5.3.2 Процедура

Виберіть **Локальний пристрій**> **VLAN**> **Список портів**.

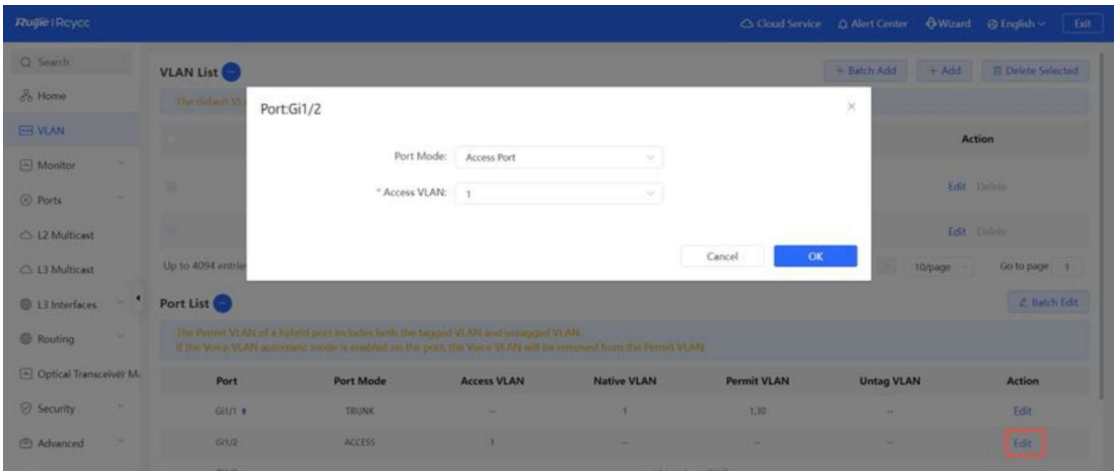
Налаштуйте віртуальні локальні мережі портів у пакетному режимі: Натисніть **Пакетне редагування**, виберіть порт, який потрібно налаштувати на панелі портів, і виберіть режим порту. Якщо режим порту - порт доступу, виберіть Access VLAN; якщо режим порту - магістральний порт, виберіть Native VLAN і введіть дозволений діапазон ідентифікаторів VLAN; якщо режим порту - гібридний порт, виберіть Native VLAN і введіть дозволений діапазон VLAN і діапазон Untagged VLAN. Натисніть **ОК,** завершити пакетне налаштування.

Примітка

У гібридному режимі дозволені VLAN включають Tag VLAN і Untagged VLAN, причому діапазон Untagged VLAN повинен включати Native VLAN.



Налаштуйте один порт: У **Списку портів** натисніть кнопку **Змінити** в останньому стовпчику **Дія** для вказаного порту, налаштуйте режим порту і відповідну VLAN, а потім натисніть кнопку **ОК**.



Примітка

- Діапазон ідентифікаторів VLAN - від 1 до 4094, серед яких VLAN 1 - це VLAN за замовчуванням, яку не можна видалити. ● Якщо апаратних ресурсів недостатньо, система видає повідомлення про помилку створення VLAN.
- Неправильна конфігурація VLAN на порту (особливо на висхідному порту) може призвести до неможливості входу у веб-інтерфейс. Тому будьте обережні при налаштуванні VLAN.

5.4 Конфігурація пакетного перемикача

Специфікація

Функції в цьому розділі не підтримуються на комутаторах RG-NBS7006, RG-NBS7003 і NBS6002.

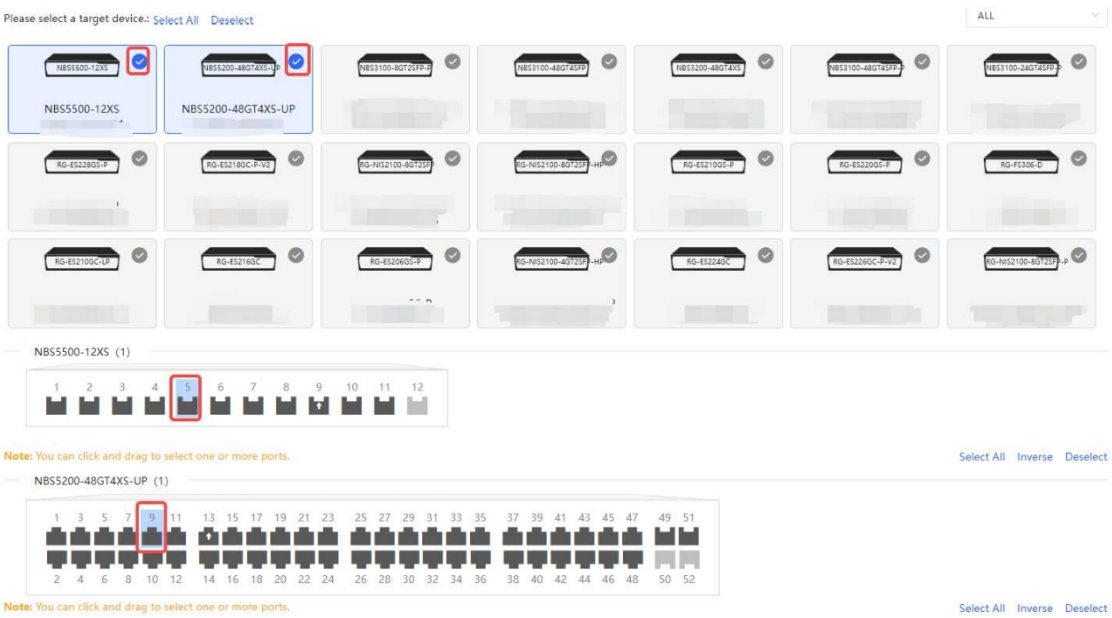
5.4.1 Огляд

Ви можете пакетно створювати VLAN, налаштовувати атрибути портів і розділяти VLAN портів для комутаторів у мережі.

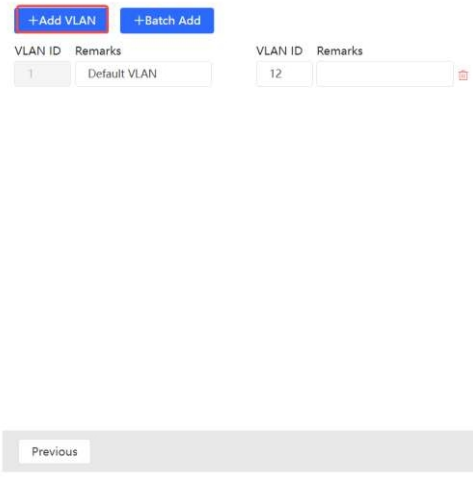
5.4.2 Процедура

Виберіть **Network**> **Batch Config**. Виберіть **Network-Wide**> **Workspace**> **Wired**> **SW Config**.

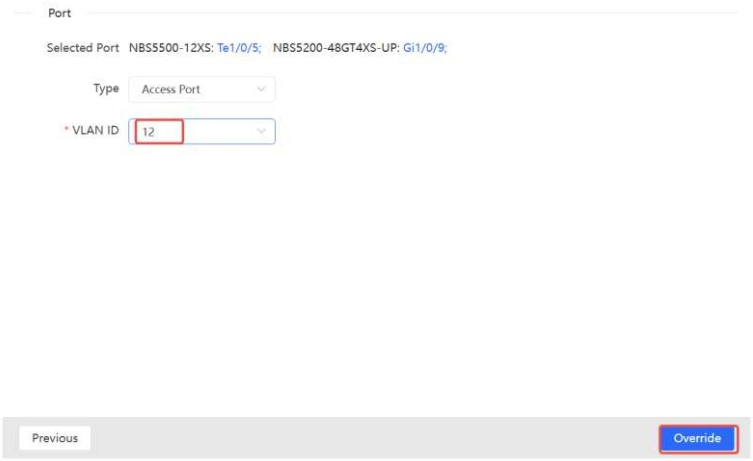
(1) На сторінці відображено всі комутатори у поточній мережі. Виберіть комутатори, які потрібно налаштувати, а потім виберіть потрібні порти у поданні портів пристрою, що з'явиться нижче. Якщо в поточній мережі є велика кількість пристроїв, виберіть модель пристрою зі спадного списку, щоб відфільтрувати їх. Після вибору потрібних пристроїв і портів натисніть кнопку **Далі**.



(2) Натисніть **Додати VLAN**, щоб створити VLAN для вибраних пристроїв у групі. Якщо ви хочете створити кілька VLAN, натисніть **Пакетне додавання** і введіть діапазон ідентифікаторів VLAN, наприклад 3-5,100. Після налаштування VLAN натисніть **Далі**.

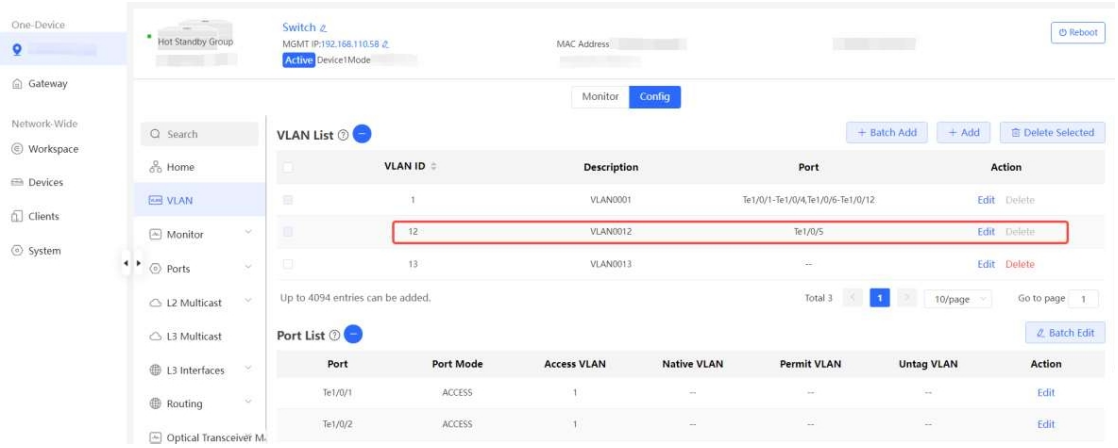


(3) Налаштуйте атрибути портів для портів, вибраних на кроці 1, у пакетному режимі. Виберіть тип порту. Якщо ви вибрали **тип Порт доступу**, вам потрібно налаштувати **ідентифікатор VLAN**. Якщо ви вибрали **Тип - Магістральний порт**, вам потрібно налаштувати **Власна VLAN** і **Дозволена VLAN**. Після налаштування атрибутів порту натисніть **Перевизначити**, щоб застосувати пакетні конфігурації до цільових пристроїв.



5.4.3 Перевірка конфігурації

Перегляньте інформацію про VLAN і порти комутаторів, щоб перевірити, чи успішно доставлені пакетні конфігурації.


One-Device
Gateway
Network-Wide
Workspace
Devices
Clients
System
Hot Standby Group
Switch
MGMT IP:192.168.110.58
Active Device1Mode
MAC Address
Reboot
Monitor
Config
Search
Home
VLAN
Monitor
Ports
L2 Multicast
L3 Multicast
L3 Interfaces
Routing
Optical Transceiver M...
VLAN List
+ Batch Add
+ Add
Delete Selected
VLAN ID
Description
Port
Action
1
VLAN0001
Te1/0/1-Te1/0/4,Te1/0/6-Te1/0/12
Edit Delete
12
VLAN0012
Te1/0/5
Edit Delete
13
VLAN0013
--
Edit Delete
Up to 4094 entries can be added.
Total 3
1
10/page
Go to page 1
Port List
Batch Edit
Port
Port Mode
Access VLAN
Native VLAN
Permit VLAN
Untag VLAN
Action
Te1/0/1
ACCESS
1
--
--
--
Edit
Te1/0/2
ACCESS
1
--
--
--
Edit

6 Моніторинг

6.1 Портовий потік

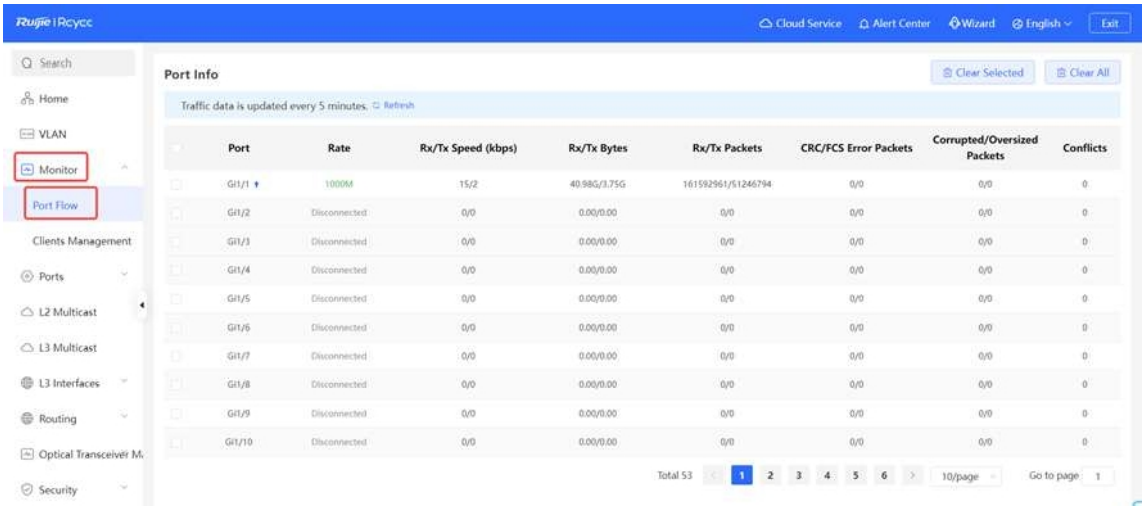
Виберіть **Локальний пристрій**> **Монітор**> **Портовий потік**.

Відображення статистики трафіку, такої як швидкість порту пристрою, кількість надісланих та отриманих пакетів, а також кількість пакетів з помилками. Швидкість порту оновлюється кожні п'ять секунд. Інша статистика трафіку оновлюється кожні п'ять хвилин.

Виберіть порт і натисніть **Очистити вибране**, або натисніть **Очистити все**, щоб очистити статистику, наприклад, поточний трафік порту, і почати збір статистики заново.

Примітка

Агреговані порти можна конфігурувати. Трафік агрегованого інтерфейсу - це сума трафіку всіх портів-учасників.



6.2 Управління клієнтами

6.2.1 Огляд

Таблиця MAC-адрес записує відображення MAC-адрес та інтерфейсів до віртуальних локальних мереж (VLAN).

Пристрій запитує таблицю MAC-адрес на основі MAC-адреси призначення в отриманому пакеті. Якщо пристрій знаходить запис, який відповідає MAC-адресі призначення в пакеті, він пакет через інтерфейс, що відповідає цьому запису, в одноадресному режимі. Якщо пристрій не знаходить такого запису, він пересилає пакет через усі інтерфейси, крім інтерфейсу приймача, у широкомовному режимі.

Записи MAC-адрес поділяються на наступні типи:

- Статичні записи MAC-адрес: Налаштовуються користувачем вручну. Пакети, MAC-адреса призначення яких збігається із зазначеною в такому записі, пересилаються через правильний інтерфейс. Цей тип записів не старіє.

- Динамічні записи MAC-адрес: Автоматично генеруються пристроями. Пакети, MAC-адреса призначення яких збігається з адресою у такому записі, пересилаються через правильний інтерфейс. Цей тип записів старіє.
- Фільтрація записів MAC-адрес: Налаштовується користувачем вручну. Пакети, MAC-адреса джерела або одержувача яких збігається із зазначеною в такому записі, відкидаються. Цей тип записів не старіє.

Примітка

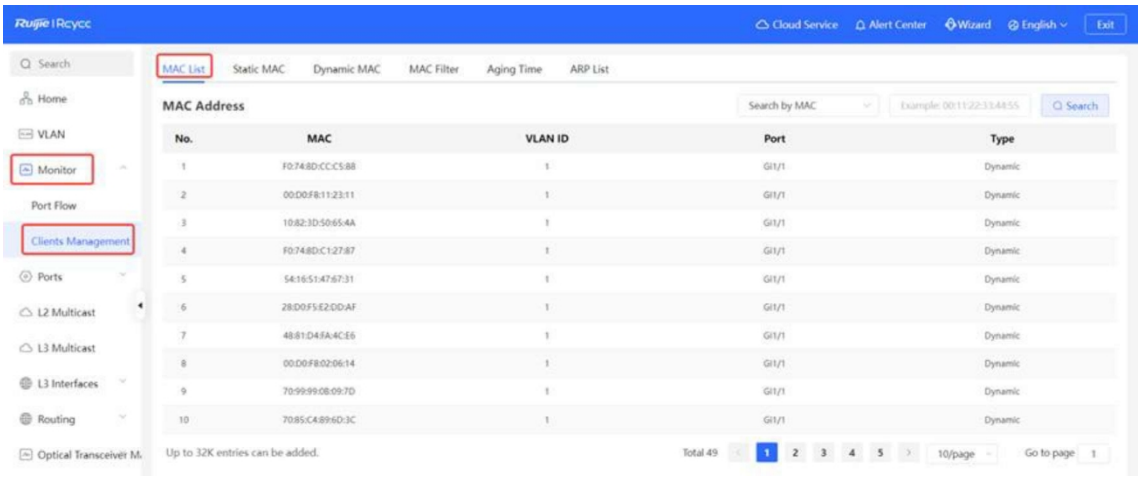
У цьому розділі описано керування статичними, динамічними та фільтрувальними записами MAC-адрес без урахування записів багатоадресної розсилки.

6.2.2 Відображення таблиці MAC-адрес

Виберіть **Локальний пристрій**> **Монітор**> **Клієнти**> **Список MAC-адрес**.

Відображає інформацію про MAC-адресу пристрою, включаючи статичну MAC-адресу, встановлену користувачем вручну, MAC-адресу фільтрації та динамічну MAC-адресу, автоматично отриману пристроєм.

Запит записів MAC-адрес: Підтримується запит записів MAC-адрес на основі MAC-адреси, ідентифікатора VLAN або порту. Виберіть тип пошуку, введіть пошуковий рядок і натисніть **Пошук**. Записи MAC-адрес, які відповідають критеріям пошуку, будуть відображені у списку. Підтримка нечіткого пошуку.

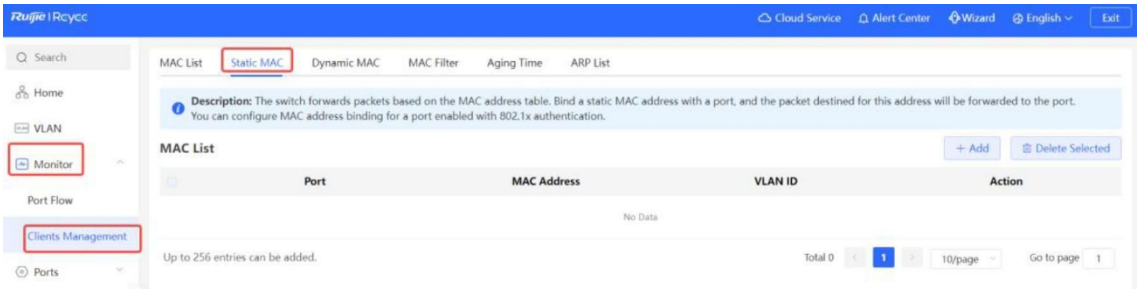


Примітка

Обсяг пам'яті для введення MAC-адрес залежить від пристрою. Наприклад, ємність введення MAC-адреси пристрою, показаного на малюнку вище, становить 32K.

6.2.3 Налаштування статичної прив'язки MAC-адрес

Комутатор пересилає дані на основі таблиці MAC-адрес. Ви можете налаштувати запис статичної MAC-адреси, щоб вручну зв'язати MAC-адресу пристрою низхідної мережі з портом пристрою. Після налаштування запису статичної адреси, коли пристрій отримає від VLAN , призначений для цієї адреси, він переадресує його на вказаний порт. Наприклад, якщо на порту ввімкнено автентифікацію 802.1X, ви можете налаштувати статичну прив'язку MAC-адреси, щоб реалізувати звільнення від автентифікації.



1. Додавання статичних записів MAC-адрес

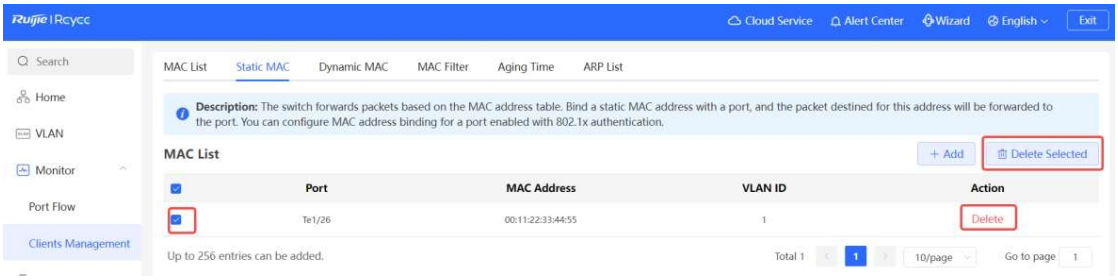
Виберіть **Локальний пристрій**> **Монітор**> **Клієнти**> **Статичний MAC**.

Натисніть **Додати**, введіть MAC-адресу та ідентифікатор VLAN, виберіть порт для переадресації пакетів і натисніть **OK**. Після успішного додавання таблиця MAC-адрес оновить введені дані.

2. Видалення записів статичних MAC-адрес

Виберіть **Локальний пристрій**> **Монітор**> **Клієнти**> **Статичний MAC**.

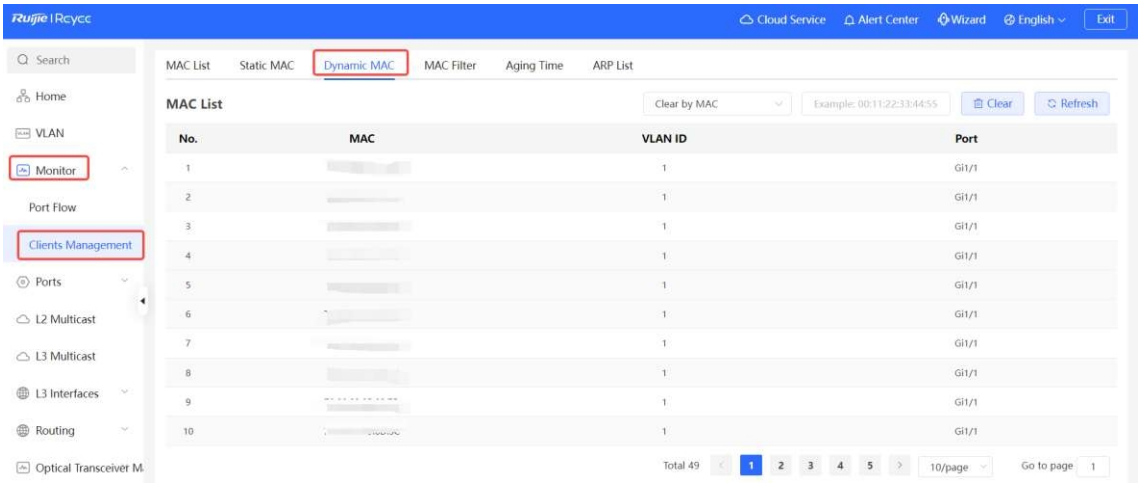
- Пакетне видалення: У **Списку** MAC-адрес виберіть записи MAC-адрес, які потрібно видалити, і натисніть **Видалити вибране**. У діалоговому вікні натисніть **OK**.
- Видалення запису: У **списку MAC-адрес** знайдіть запис, який потрібно видалити, і натисніть **Видалити** в останньому стовпчику **Дія**. У діалоговому вікні, що з'явиться, натисніть **OK**.



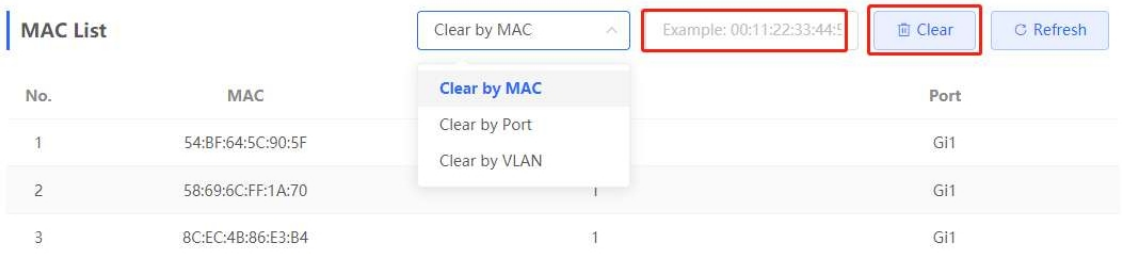
6.2.4 Відображення динамічної MAC-адреси

Виберіть **Локальний пристрій**> **Монітор**> **Клієнти**> **Динамічний MAC**.

Після отримання пакета пристрій автоматично згенерує записи динамічної MAC-адреси на основі MAC-адреси джерела пакета. На поточній сторінці відображаються записи динамічних MAC-адрес, отримані пристроєм. Натисніть **Оновити**, щоб отримати найновіші записи динамічних MAC-адрес.

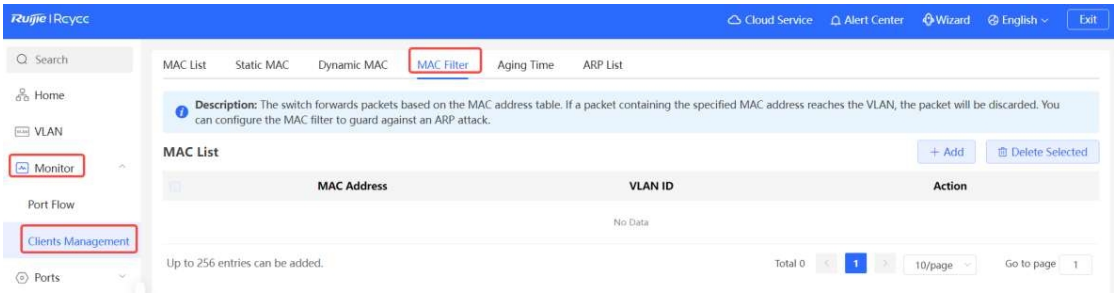


Видалення динамічної MAC-адреси: Виберіть тип очищення (за MAC-адресою, за VLAN або за портом), введіть рядок для відповідності запису динамічної MAC-адреси і натисніть **Очистити**. Пристрій очистить записи MAC-адрес, які відповідають умовам.



6.2.5 Налаштування фільтрації MAC-адрес

Щоб заборонити користувачеві надсилати та отримувати пакети в певних сценаріях, ви можете додати MAC-адресу користувача до запису фільтрації MAC-адрес. Після налаштування запису, пакети, MAC-адреса джерела або призначення яких збігається з MAC-адресою у фільтруючому записі MAC-адреси, безпосередньо відкидаються. Наприклад, якщо користувач ініціює ARP-атаки, MAC-адресу користувача можна налаштувати як адресу для фільтрації, щоб запобігти атакам.



1. Додавання MAC-адреси для фільтрації

Виберіть **Локальний пристрій**> **Монітор**> **Клієнти**> **MAC-фільтр**.

Натисніть **Додати**. У діалоговому вікні, що з'явиться, введіть MAC-адреси та ідентифікатор VLAN, а потім натисніть **OK**.

2. MAC-фільтр

Виберіть **Локальний пристрій**> **Монітор**> **Клієнти**> **MAC-фільтр**.

- Пакетне видалення: У **Списку** MAC-адрес виберіть записи MAC-адрес, які потрібно видалити, і натисніть **Видалити вибране**. У діалоговому вікні натисніть **OK**.
- Видалення запису: У **списку MAC-адрес** знайдіть запис, який потрібно видалити, і натисніть **Видалити** в останньому стовпчику **Дія**. У діалоговому вікні, що з'явиться, натисніть **OK**.

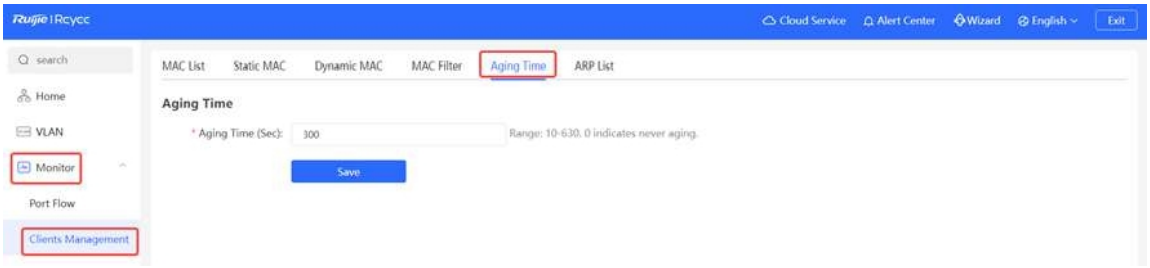
6.2.6 Налаштування часу старіння MAC-адреси

Установіть час старіння динамічних записів MAC-адрес, запам'ятовуваних пристроєм. Статичні записи MAC-адрес і записи фільтрів MAC-адрес не старіють.

Пристрій видаляє непотрібні записи динамічних MAC-адрес основі часу старіння, щоб заощадити ресурси записів на пристрої. Занадто довгий час старіння може призвести до несвоєчасного видалення непотрібних записів, тоді як занадто короткий час старіння може призвести до видалення деяких дійсних записів і повторного запам'ятовування MAC-адрес пристроєм, що збільшує частоту трансляції пакетів. Тому рекомендується налаштувати належний час старіння динамічних записів MAC-адрес, щоб заощадити ресурси пристрою, не впливаючи на стабільність роботи мережі.

Виберіть **локальний пристрій**> **Монітор**> **Клієнти**> **Час старіння**.

Введіть дійсний час старіння і натисніть кнопку **Зберегти**. Діапазон значень часу старіння - від 10 до 630, в секундах. Значення 0 означає відсутність старіння.



6.2.7 Відображення інформації про ARP

Виберіть **Локальний пристрій**> **Монітор**> **Клієнти**> **ARP-список**.

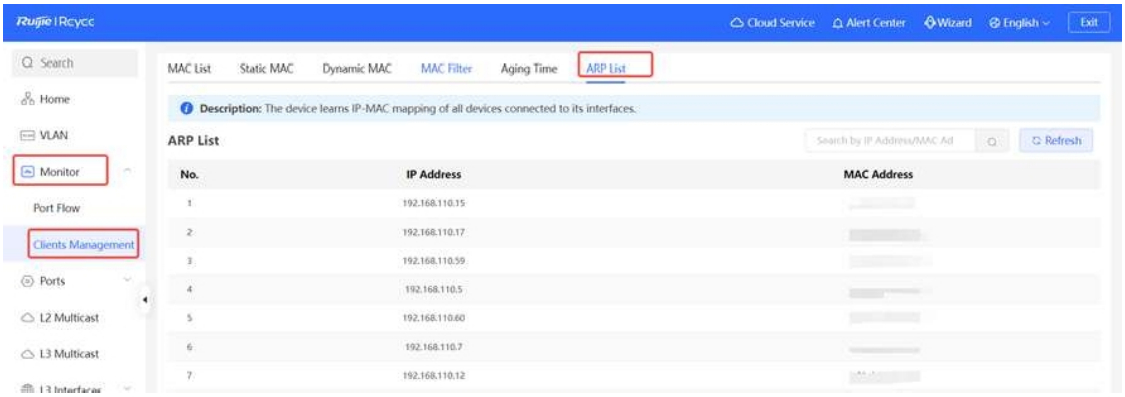
Коли два IP-пристрої повинні зв'язатися один з одним, відправник повинен знати IP-адресу та MAC-адресу однорангового пристрою. За допомогою MAC-адрес IP-пристрій може інкапсулювати кадри канального рівня, а потім надсилати кадри даних у фізичну мережу. Процес отримання MAC-адреси на основі IP-адреси називається дозволом адреси.

Протокол дозволу адрес (ARP) використовується для перетворення IP-адрес в MAC-адреси. ARP може отримати MAC-адресу, пов'язану з IP-адресою. ARP зберігає відповідності між IP-адресами та MAC-адресами в ARP-кеші пристрою.

Пристрій запам'ятовує IP-адреси та MAC-адреси мережевих пристроїв, підключених до його інтерфейсів, і генерує відповідні . На сторінці **Список ARP** відображаються ARP-записи, отримані пристроєм. Список ARP дозволяє шукати вказані ARP-записи за IP- або MAC-адресою. Натисніть **Оновити**, щоб отримати найновіші ARP-записи.

Примітка

Докладнішу інформацію про функцію запису ARP див. у розділі 10.6 Налаштування статичного запису ARP.



7 Порти

7.1 Огляд

Порти є важливими компонентами для обміну даними на мережевих пристроях. Модуль керування портами дозволяє налаштувати базові параметри портів, а також налаштувати агрегацію портів, аналізатор комутованих портів (SPAN), обмеження швидкості порту, керуючу IP-адресу тощо.

Таблиця 7-1 Опис типу порту

Тип порту	Примітка	Зауваження
Порт комутатора	Порт комутатора складається з одного фізичного порту на пристрої і забезпечує лише функцію комутації на рівні 2. Порти комутатора використовуються для керування фізичними портами та пов'язаними з ними протоколами 2-го рівня.	Описано в цьому розділі
Агрегований інтерфейс рівня 2	Інтерфейс пов'язує декілька фізичних елементів, утворюючи логічне з'єднання. Для комутації рівня 2 агрегований інтерфейс схожий на порт комутатора з високою пропускною здатністю. Він може об'єднувати смуги пропускання декількох портів для розширення пропускної здатності каналу. Крім того, для кадрів, що надсилаються через агрегований інтерфейс 2-го рівня, виконується балансування навантаження на портах-учасниках агрегованого інтерфейсу 2-го рівня. Якщо один з портів агрегатного інтерфейсу виходить з ладу, агрегатний інтерфейс 2-го рівня автоматично передає трафік по цьому порту на інші доступні порти, підвищуючи надійність з'єднання.	Описано в цьому розділі
Порт SVI	Віртуальний інтерфейс комутатора (SVI) слугує інтерфейсом керування пристроєм, через який можна керувати пристроєм. Ви також можете створити SVI як інтерфейс шлюзу, який еквівалентний віртуальному інтерфейсу відповідної VLAN і може використовуватися для маршрутизації між VLAN на пристроях 3-го рівня.	Відповідну конфігурацію див. у розділі 10.1 Налаштування інтерфейсу 3-го рівня.
Маршрутизований порт	На пристроях 3-го рівня ви можете налаштувати один фізичний порт як порт маршрутизації і використовувати його як інтерфейс шлюзу для комутації на 3-му рівні. Маршрутні інтерфейси не мають функцій комутації 2-го рівня і не мають відповідного зв'язку з VLAN, а слугують лише інтерфейсами доступу.	Відповідну конфігурацію див. у розділі 10.1 Налаштування інтерфейсу 3-го рівня.

Тип порту	Примітка	Зауваження
Агрегатний інтерфейс рівня 3	Агрегований інтерфейс 3-го рівня - це логічна агрегована група інтерфейсів, що складається з декількох фізичних портів, так само як агрегований інтерфейс 2-го рівня. Об'єднані порти повинні бути однотипними портами 3-го рівня. Агрегований інтерфейс слугує інтерфейсом шлюзу для комутації на рівні 3. Він розглядає кілька фізичних каналів в одній агрегованій групі як один логічний канал. Це важливий спосіб розширення пропускної каналу. Кілька фізичних каналів об'єднуються в один логічний канал, розширюючи пропускну здатність каналу. Кадри, що надсилаються через агрегований інтерфейс рівня 3, балансуються між портами-членами агрегованого інтерфейсу рівня 3. Якщо один з каналів виходить з ладу, агрегований інтерфейс рівня 3 автоматично передає трафік на несправний канал до інших посилань учасників, підвищуючи надійність з'єднань. Агрегатні інтерфейси рівня 3 не підтримують функцію комутації рівня 2.	Відповідну конфігурацію див. у розділі 10.1 Налаштування інтерфейсу 3-го рівня.

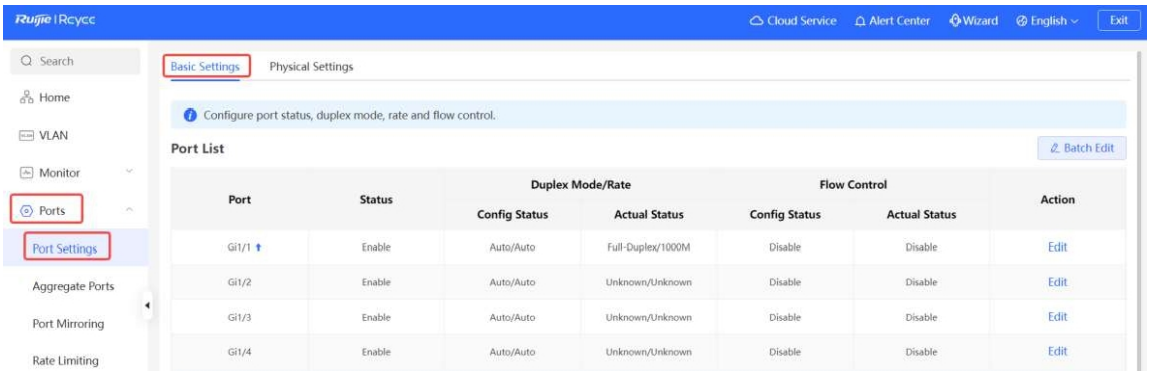
7.2 Конфігурація порту

Конфігурація порту включає загальні атрибути, такі як базові налаштування та фізичні параметри порту. Користувачі можуть налаштувати швидкість порту, встановити перемикач порту, дуплексний режим, режим керування потоком, енергоефективний Ethernet, тип носія порту та MTU тощо.

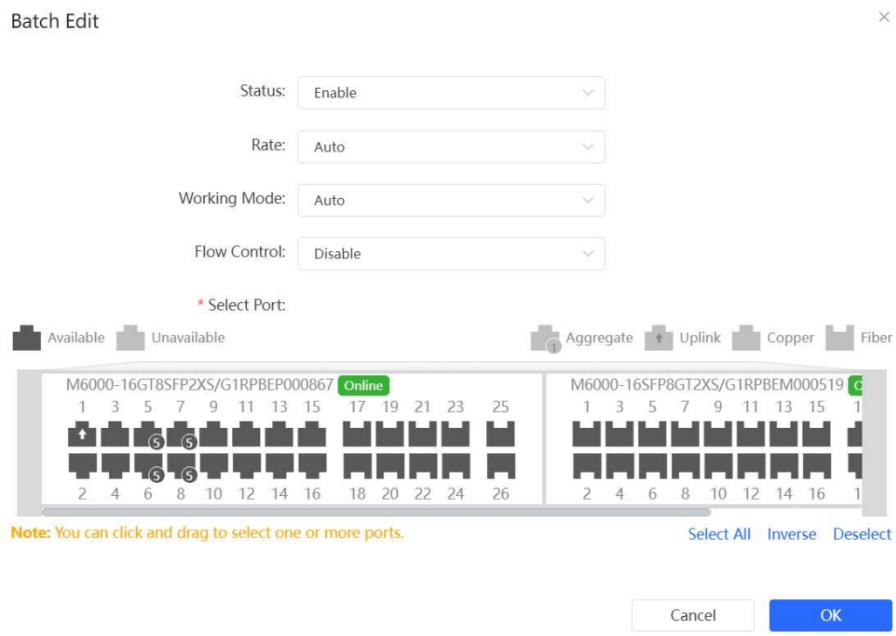
7.2.1 Основні налаштування

Виберіть **Локальний пристрій**> **Порти**> **Базові налаштування**> **Базові налаштування**.

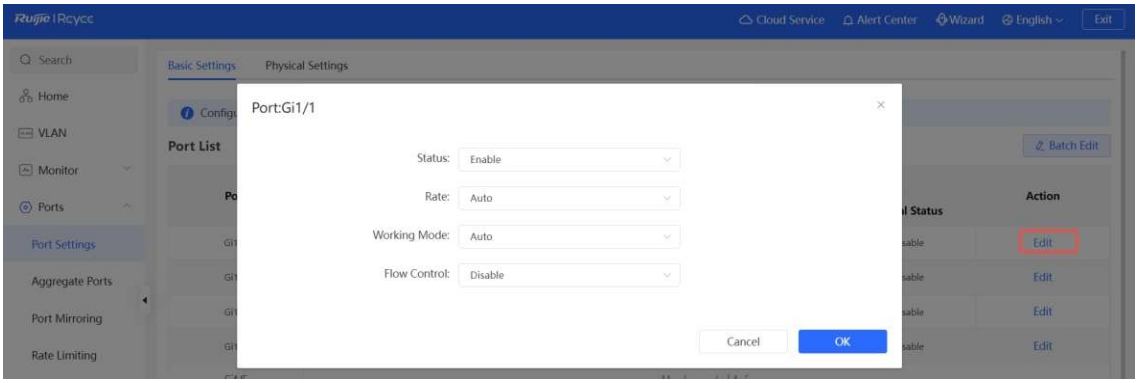
Підтримує налаштування ввімкнення порту, швидкості та дуплексного режиму порту, режиму керування потоком, а також відображення поточного фактичного стану кожного порту.



Налаштуйте пакетну конфігурацію: Натисніть кнопку **Пакетне редагування**, виберіть порт, який потрібно налаштувати У діалоговому вікні, що з'явиться, виберіть перемикач порту, швидкість, режим роботи і режим керування потоком, а потім натисніть кнопку **ОК,** щоб застосувати конфігурацію. У пакетній конфігурації необов'язкові елементи конфігурації є загальною колекцією вибраних портів (атрибутів, які підтримуються вибраними портами).



Налаштуйте один порт: У **Списку портів** виберіть запис про порт і натисніть кнопку **Змінити** у стовпчику **Дія**. У діалоговому вікні, що з'явиться, виберіть стан порту, швидкість, режим роботи та режим керування потоком і натисніть **OK**.



Таблиця 7-2 Опис основних параметрів конфігурації порту

Параметр	Опис	Значення за замовчуванням
Статус	Якщо порт закрито, жоден кадр не буде прийматися і відправлятися через цей порт, і відповідна функція обробки даних буде втрачена.	Увімкнути
Ставка	Дозволяє вказати швидкість, на якій працює фізичний інтерфейс Ethernet. Значення Авто означає, що швидкість порту визначається шляхом автоматичного узгодження між локальним та одноранговими пристроями. Узгоджена швидкість може бути будь-якою в межах можливостей порту.	Авто
Режим роботи	● Повний дуплекс: розуміти, що порт може приймати пакети під час надсилання. ● Напівдуплексний: керування тим, що порт може приймати або надсилати пакети одночасно. ● Авто: визначається дуплексний режим порту	Авто

Параметр	Опис	Значення за замовчуванням
	за допомогою автоматичного узгодження між локальним портом та одноранговим портом	
Контроль потоку	Після увімкнення керування потоком порт оброблятиме отримані кадри керування потоком і надсилатиме кадри керування потоком у разі виникнення перевантаження на порту.	Вимкнути

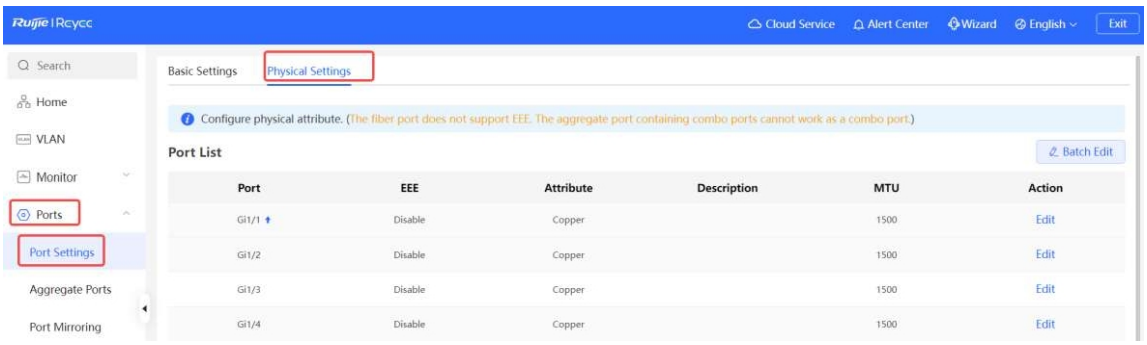
Примітка

Швидкість оптичного порту GE можна встановити на **1000M**, **100M** або **Auto**. Швидкість електричного порту GE можна встановити на **1000M**, **100M**, **10M** або **Авто**. Швидкість порту 10GE можна встановити на **1000M** або **Авто**.

7.2.2 Фізичні налаштування

Виберіть **Локальний пристрій**> **Порти**> **Основні налаштування**> **Фізичні налаштування**.

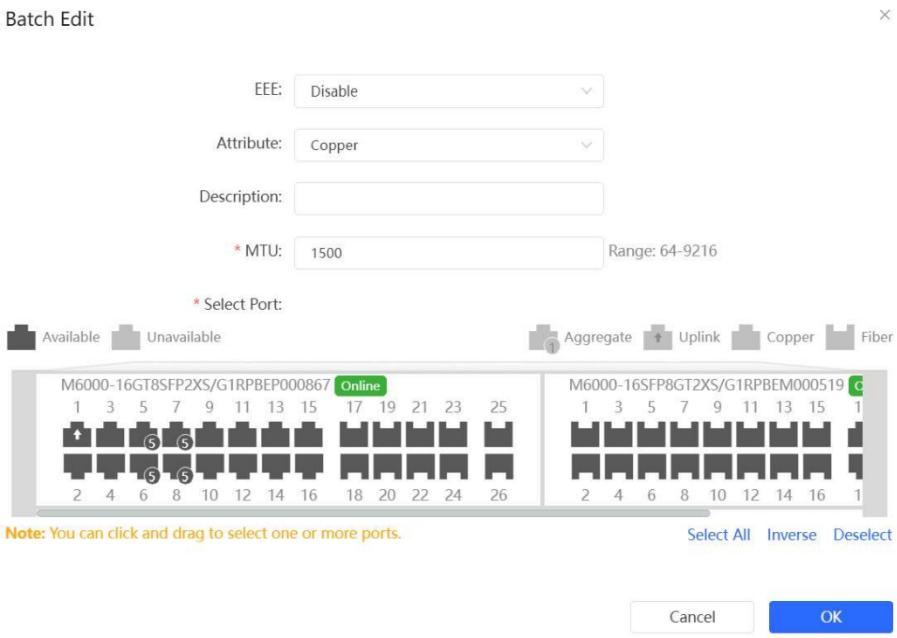
Підтримка ввімкнення функції енергоефективного Ethernet (EEE) порту, а також налаштування типу носія та MTU порту.



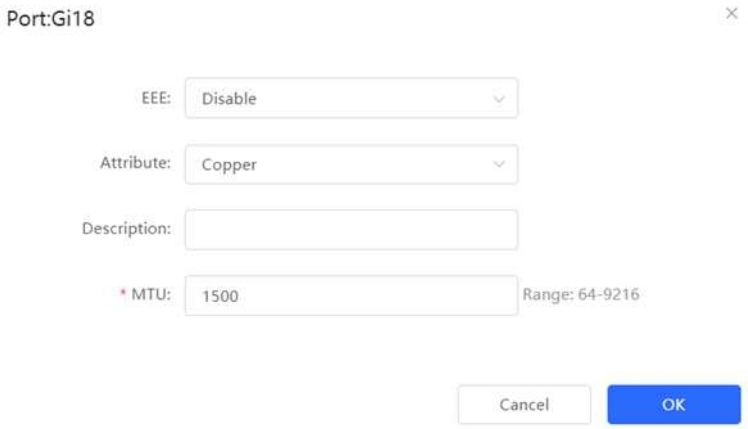
- Налаштуйте пакетну конфігурацію: Натисніть **Пакетне редагування**. У діалоговому вікні, що з'явиться, виберіть порт, який потрібно налаштувати, налаштуйте комутатор EEE, MTU, введіть опис порту і натисніть **OK**.

  Примітка

  Під час пакетної конфігурації не можна одночасно налаштувати мідні та SFP-порти.



- Налаштуйте один порт: Натисніть кнопку **Змінити** у **Дія** у списку. У вікні конфігурації налаштуйте комутатор EEE, режим порту, введіть опис порту і натисніть **OK**.



Таблиця 7-3 Опис фізичних параметрів конфігурації

Параметр	Опис	Значення за замовчуванням
EEE	Це скорочення від енергоефективного Ethernet, який базується на стандартному протоколі IEEE 802.3az. Коли EEE увімкнено, він економить енергію, змушуючи інтерфейс переходити в режим LPI (Low Power Idle), коли Ethernet-з'єднання не використовується. Значення: Вимкнути/Ввімкнути	Вимкнути
Атрибут	Атрибут порту вказує, чи є порт мідним або SFP-портом. Мідний порт: режим міді (не можна змінити);	Залежно від атрибуту порту

Параметр	Опис	Значення за замовчуванням
	Порт SFP: оптоволоконний режим (не може бути змінений); Тільки комбіновані порти підтримують зміну режиму.	
Опис	Ви можете додати опис для позначення функцій порту.	NA
MTU	MTU (Maximum Transmission Unit - максимальна одиниця передачі) використовується для повідомлення однорангового партнера про допустимий максимальний розмір одиниці служби даних. Він вказує на розмір корисного навантаження, прийнятного для відправника. Ви можете налаштувати MTU порту, щоб обмежити довжину кадру, який може бути отриманий або пересланий через цей порт.	1500

Примітка

- Різні порти підтримують різні атрибути та елементи конфігурації. ● Тільки комбіновані порти SFP підтримують перемикання режиму порту.
- Порти SFP не підтримують увімкнення EEE.

7.3 Агрегатні інтерфейси

7.3.1 Огляд агрегованого інтерфейсу

Агрегатний інтерфейс - це логічна ланка, утворена шляхом з'єднання декількох фізичних ланок. Він використовується для розширення пропускної здатності каналу, підвищуючи тим самим надійність з'єднання.

Ця функція підтримує балансування навантаження, а отже, рівномірно розподіляє трафік між посиланнями-учасниками. Вона реалізує резервне копіювання каналів. При відключенні одного з каналів агрегованого інтерфейсу система автоматично розподіляє трафік цього каналу між іншими доступними каналами. Широкомовні або багатоадресні пакети, отримані однією ланкою агрегованого інтерфейсу, не пересилаються іншим ланкам.

- Якщо один інтерфейс, який з'єднує два пристрої, підтримує максимальну швидкість 1000 Мбіт/с (припустимо, що інтерфейси обох пристроїв підтримують швидкість 1000 Мбіт/с), коли службовий трафік на каналі перевищує 1000 Мбіт/с, надлишковий трафік буде відкинуто. Агрегація каналів може вирішити цю проблему. Наприклад, використовуйте *n* мережевих кабелів для з'єднання двох пристроїв і зв'яжіть інтерфейси між собою. Таким чином, інтерфейси будуть логічно пов'язані для підтримки максимального трафіку 1000 Мбіт/с × *n*.
- Якщо два пристрої з'єднані одним кабелем, коли зв'язок між двома інтерфейсами розривається, послуги, що надаються через цей зв'язок, перериваються. Після з'єднання декількох інтерфейсів, доки доступне одне з'єднання, послуги, що надаються через ці інтерфейси, не будуть перериватися.

7.3.2 Огляд

1. Статична адреса агрегації

У режимі статичної агрегації ви можете вручну додати фізичний порт до агрегованого інтерфейсу. Агрегований інтерфейс у режимі статичної агрегації називається статичним агрегованим інтерфейсом, а порти-члени - портами-членами статичного агрегованого інтерфейсу. Статичну агрегацію можна легко реалізувати. Ви можете об'єднати декілька фізичних каналів, виконавши команди для додавання вказаних фізичних портів до агрегованого інтерфейсу.

Після додавання інтерфейсу учасника до агрегованого інтерфейсу, він може надсилати та отримувати дані і балансувати трафік в агрегованому інтерфейсі.

2. Автоматична агрегація

Режим автоматичної агрегації - це спеціальна функція агрегації портів, розроблена для WAN-порту шлюзів серії RG-EG. Максимальна пропускна здатність WAN-порту пристрою RG-EG становить 2000 Мбіт/с, але після підключення порту інтрамережі до комутатора один порт може підтримувати максимальну пропускну здатність лише 1000 Мбіт/с. Щоб запобігти втраті пропускної здатності низхідної лінії зв'язку, необхідно знайти спосіб збільшити максимальну пропускну здатність порту між пристроєм MR і комутатором, і для задоволення цієї потреби з'явилася функція автоматичної агрегації.

Після підключення двох фіксованих портів-членів агрегації на пристрої шлюзу RG-EG до будь-яких двох портів комутатора, за допомогою обміну пакетами, два порти комутатора можуть бути автоматично об'єднані, тим самим подвоюючи пропускну здатність. Агрегований інтерфейс, автоматично створений таким чином на комутаторі, називається автоматичним агрегованим інтерфейсом, а відповідні два порти - портами-учасниками агрегованого інтерфейсу.

Примітка

Автоматичні агреговані інтерфейси не підтримують створення вручну і можуть бути видалені після їх автоматичного створення пристроєм, але порти, що входять до них, не можуть бути змінені.

Специфікація

Тільки серії RG-NBS5300, RG-NBS5200, RG-NBS5100, RG-NBS3200, RG-NBS3100 та RG-NIS3100 продукти підтримують автоматичну агрегацію, а рівноправний пристрій для автоматичної агрегації повинен бути RG-EG310G- E.

3. Балансування навантаження

Агрегований інтерфейс на основі характеристик пакетів, таких як MAC-адреса джерела, MAC-адреса призначення, IP-адреса джерела, IP-адреса призначення, ідентифікатор порту джерела L4 та ідентифікатор порту призначення L4 пакетів, отриманих вхідним інтерфейсом, диференціює потоки пакетів відповідно до одного або декількох комбінованих алгоритмів. Він надсилає той самий потік пакетів через той самий канал-учасник і рівномірно розподіляє різні потоки пакетів між каналами-учасниками. Наприклад, у режимі балансування навантаження на основі вихідних MAC-адрес пакети розподіляються між різними каналами агрегованого інтерфейсу на основі їхніх вихідних MAC-адрес. Пакети з різними вихідними MAC-адресами розподіляються між різними каналами; пакети з однаковими вихідними MAC-адресами пересилаються через один і той самий канал.

Наразі агрегований інтерфейс підтримує режими балансування трафіку на основі наступних параметрів:

- MAC-адреса джерела або MAC-адреса призначення
- MAC-адреса джерела+ MAC-адреса призначення
- IP-адреса джерела або IP-адреса призначення
- IP-адреса джерела+ IP-адреса призначення
- Порт джерела
- L4 порт-джерело або L4 порт-призначення
- L4 порт-джерело + L4 порт-призначення

4. LACP

Протокол управління агрегацією каналів (Link Aggregation Control Protocol, LACP) - це стандартизований протокол для динамічного об'єднання декількох фізичних каналів в один логічний канал з метою підвищення пропускної здатності та надійності мережі. LACP визначає процес узгодження і параметри об'єднання каналів, що дозволяє обмінюватися інформацією про об'єднання каналів і узгоджувати параметри об'єднання каналів між мережевими пристроями, а також забезпечує надійність і стабільність об'єднання каналів. LACP підтримує динамічне додавання та видалення каналів, забезпечуючи динамічне налаштування та оптимізацію каналів.

У LACP визначено дві ролі: актор і партнер. Актор надсилає запит на об'єднання посилань, а партнер відповідає на нього і приєднується до групи об'єднання посилань.

7.3.3 Агрегована конфігурація інтерфейсу

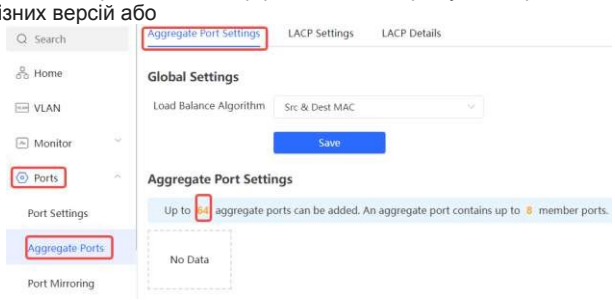
Виберіть **Локальний пристрій**> **Порти**> **Агрегатні порти**> **Налаштування агрегованих портів**.

1. Додавання агрегованого інтерфейсу

Введіть ідентифікатор агрегованого інтерфейсу, виберіть порти-учасники (порти, які вже є учасниками агрегованого інтерфейсу, не можуть бути обрані), увімкніть **LACP** і натисніть кнопку **Зберегти**. Ви можете увімкнути **LACP** для динамічного об'єднання каналів, щоб підвищити надійність і гнучкість мережі. На панелі портів буде показано успішно доданий агрегований інтерфейс.

Специфікація

- Максимальна кількість агрегованих інтерфейсів, які можна налаштувати на комутаторі, залежить від моделі комутатора.
- Починаючи з версії Reyee 2.320, максимальна кількість агрегатних інтерфейсів, що підтримуються моделями комутаторів, починаючи з RG-NBS5, RG-NBS6 або RG-NBS7, збільшилася. Тому максимальна кількість агрегатних інтерфейсів, що підтримується різними версіями програмного забезпечення, також відрізняється.
- Для отримання детальної інформації про максимальну агрегованих інтерфейсів, які можна налаштувати, див. Таблицю 7- 4Кількість агрегованих інтерфейсів, що підтримуються різними серіями продуктів, які працюють під управлінням різних версій або



веб-сторінку.

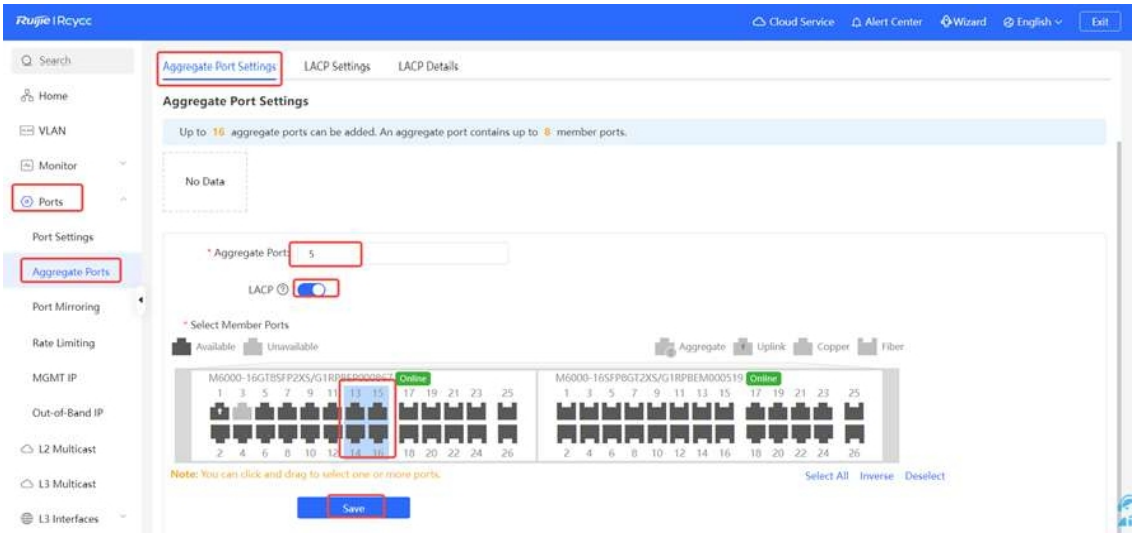
Таблиця 7-4 Кількість агрегатних інтерфейсів, що підтримуються різними серіями продуктів з різними версіями

Серія вимикачів	ReyeeOS 2.300 або новіша версія	ReyeeOS 2.320 або новішої версії
RG-NBS7003 RG-NBS7006	16	128
RG-NBS6002	16	64
RG-NBS5300 RG-NBS5200 RG-NBS5100	16	64

RG-NBS3200 RG-NBS3100	8	8
RG-NIS3100	8	8

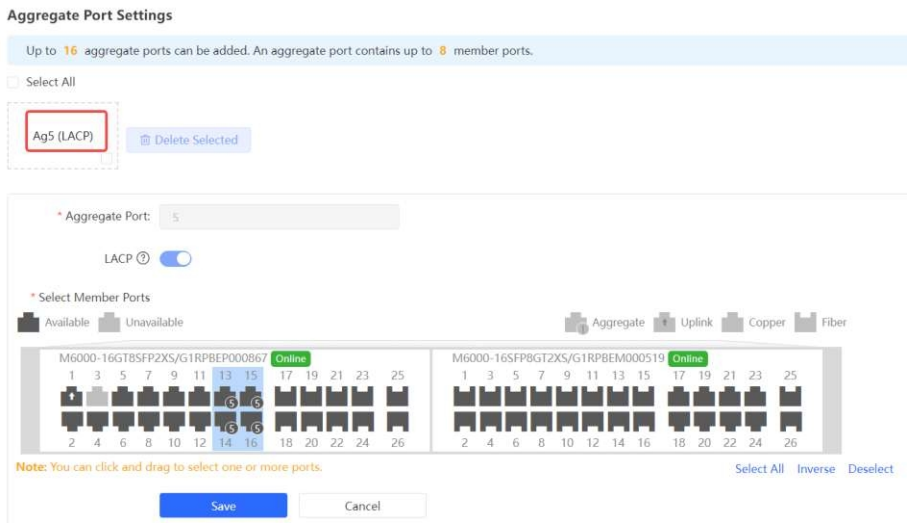
Примітка

- Агрегований інтерфейс містить максимум вісім портів-членів.
- Атрибути агрегованих інтерфейсів повинні бути однаковими, а мідні порти і порти SFP не можуть бути агреговані.
- Автоматичні інтерфейси агрегатів не підтримують створення вручну.
- Стан LACP не може бути змінено після створення статичного агрегованого інтерфейсу.



2. Модифікація портів-членів агрегованого інтерфейсу

Клацніть доданий статичний агрегований інтерфейс. Порти, входять до складу агрегованого інтерфейсу, стануть вибраними. Клацніть порт, щоб позначку; або виберіть інші порти, щоб приєднатися до поточного агрегованого інтерфейсу. Натисніть кнопку **Зберегти**, щоб змінити порти-учасники агрегованого інтерфейсу.

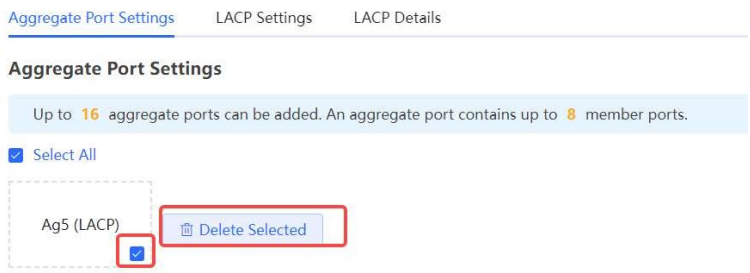


3. Видалення агрегатного інтерфейсу

Наведіть курсор на піктограму агрегованого інтерфейсу і клацніть правою кнопкою миші вгорі, або виберіть агрегований інтерфейс, потрібно видалити, і натисніть кнопку **Видалити вибране**, щоб видалити вибраний агрегований інтерфейс. Після видалення відповідні порти стануть **доступними** на панелі портів для налаштування нового агрегованого інтерфейсу.

Застереження

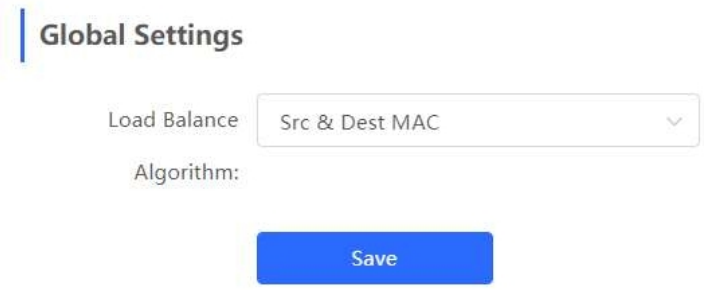
- Після видалення агрегованого інтерфейсу, порти, що входять до нього, відновлюються до налаштувань за замовчуванням і вимикаються.
- Для комутаторів, апаратні моделі яких починаються з RG-NBS7, RG-NBS6 або RG-NBS5, якщо поточна версія програмного забезпечення ReyeeOS 2.320 або новіша, обов'язково видаліть усі агреговані інтерфейси з кількістю портів більше 16 перед оновленням версії програмного забезпечення (наприклад, знизьте версію програмного забезпечення до ReyeeOS 2.300). В іншому випадку може виникнути несумісність версій, ці агрегатні інтерфейси все ще відображатимуться на інтерфейсі веб-сторінки, і їхні конфігурації не можна буде видалити. Крім того, після оновлення програмного забезпечення їхні порти-члени вважатимуться звичайними фізичними портами, що може призвести до збоїв у роботі мережі. У цьому випадку вам потрібно видалити конфігурації сукупних інтерфейсів на однорангових пристроях, підключених до портів учасників, і використовувати загальні порти для відновлення мережевого з'єднання.



7.3.4 Налаштування режиму балансування навантаження

Виберіть **Локальний пристрій**> **Порти**> **Сукупний порт**> **Глобальні налаштування**.

Виберіть **Алгоритм балансування навантаження** і натисніть **Зберегти**. Пристрій розподіляє вхідні пакети між , використовуючи вказаний алгоритм балансування навантаження. Потік пакетів з однаковою характеристикою передається одним каналом, тоді як різні потоки пакетів рівномірно розподіляються між різними каналами.

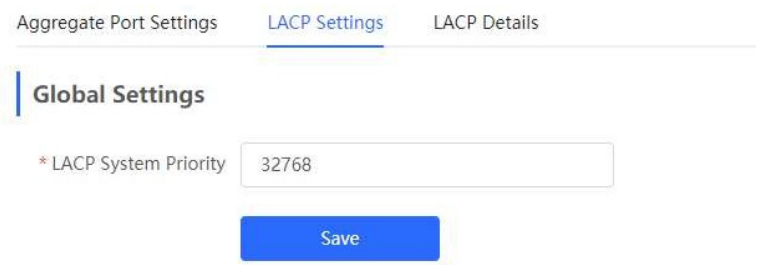


7.3.5 Налаштування параметрів LACP

1. Пріоритет системи LACP

Виберіть **Локальний пристрій**> **Порти**> **Сукупний порт**> **Налаштування LACP**> **Глобальні налаштування**.

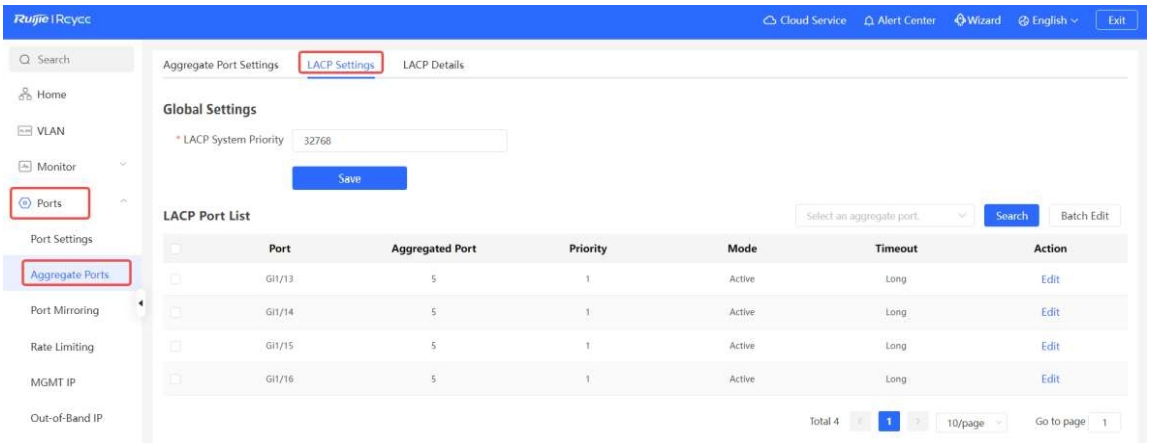
У LACP пристрій з вищим системним пріоритетом стає актором у групі агрегації каналів і контролює робочий стан і параметри групи агрегації каналів. Значення системного пріоритету знаходиться в діапазоні від 1 до 65535, а значення за замовчуванням - 32768. Чим менше значення системного пріоритету, тим вищий пріоритет пристрою. Коли два пристрої мають однаковий системний пріоритет, їхні MAC-адреси порівнюються, і пристрій з меншою MAC-адресою стає учасником групи агрегації каналів.



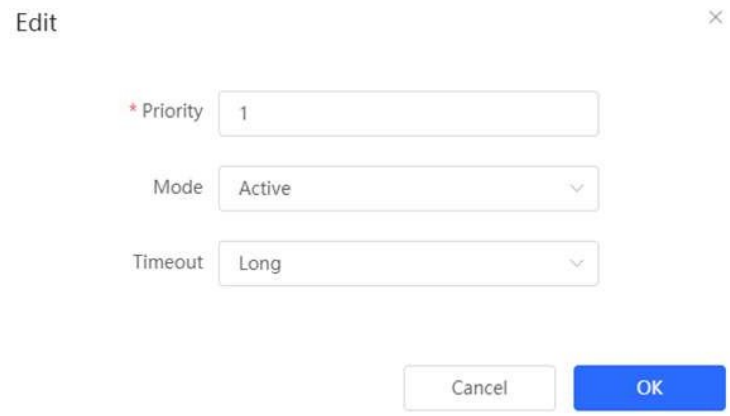
2. Список портів LACP

Виберіть **Локальний пристрій**> **Порти**> **Сукупний порт**> **Налаштування LACP**> **Список портів LACP**.

На сторінці **Список портів LACP** показано ідентифікатор порту, пріоритет, режим і таймаут кожного порту з підтримкою LACP. Ви можете переглянути відомості про порти, що входять до відповідної групи агрегації каналів, вибравши інтерфейс агрегації.



Ви можете вибрати певний порт і натиснути кнопку Змінити, або вибрати кілька портів і натиснути кнопку **Пакетне редагування**, щоб змінити пріоритет, режим і таймаут портів у спливаючому вікні. Потім натисніть **OK,** щоб підтвердити і застосувати зміни.



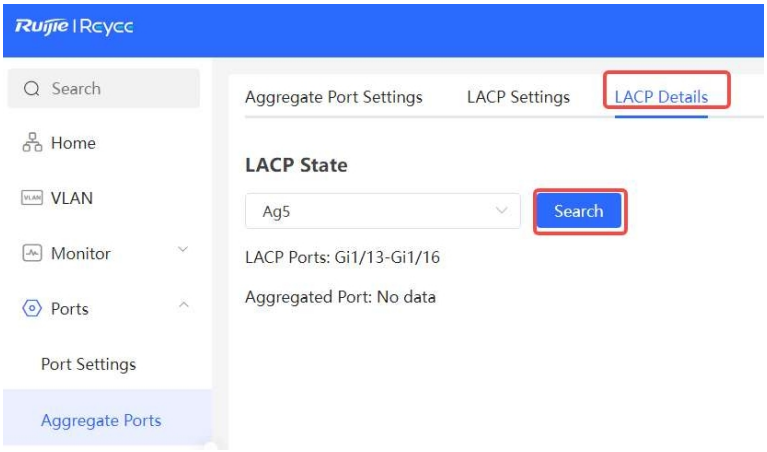
Таблиця 7-5 Опис параметрів конфігурації списку портів LACP

Параметр	Опис	Значення за замовчуванням
Пріоритет	Пріоритет використовується для визначення того, який порт є головним, причому порт з найвищим пріоритетом вибирається як активний. Значення пріоритету варіюється від 1 до 65535, і чим менше значення пріоритету, тим вищий пріоритет. Якщо декілька портів мають однаковий пріоритет, то їхнє ранжування визначається за допомогою оцінки ідентифікаторів портів, і порт з меншим ідентифікатором матиме вищий пріоритет.	32768
Режим	Режим - це метод, за допомогою якого два пристрої в групі агрегації каналів зв'язку узгоджують свій режим роботи. ● Активний: В активному режимі пристрій бере на себе роль актора і надсилає запити на встановлення агрегації каналів. ● Пасивний: У пасивному режимі пристрій бере на себе роль партнера і чекає, поки одноранговий пристрій надішле запит.	Активний
Тайм-аут.	Метою режиму тайм-ауту є визначення періоду тайм-ауту і механізму агрегації LACP-каналів. Якщо протягом заданого тайм-ауту від однорангового пристрою не отримано жодного кадру LACP, вважається, що на одноранговому пристрої стався збій. В результаті механізм виявлення збоїв і відновлення агрегації каналів. ● Довгий: У режимі тривалого тайм-ауту кадри LACP надсилаються кожні 30 секунд, а тривалість тайм-ауту встановлюється на 90 секунд. Цей режим підвищує надійність і стабільність агрегації каналів, але потенційно може призвести до затримки виявлення несправностей. ● Короткий: У режимі короткого тайм-ауту кадри LACP надсилаються щосекунди, а тривалість тайм-ауту встановлюється 3 секунди. Цей режим підвищує швидкість реакції агрегації каналів і забезпечує своєчасне виявлення несправностей, але може спричинити додаткове навантаження на мережу та споживання ресурсів.	Довгий

3. Перегляд стану LACP

Виберіть **Локальний пристрій**> **Порти**> **Сукупний порт**> **Деталі LACP**.

Ви можете вибрати агрегований інтерфейс з підтримкою LACP і натиснути **Пошук**, щоб переглянути порти учасників з підтримкою LACP та інформацію про агрегований інтерфейс на цій сторінці.



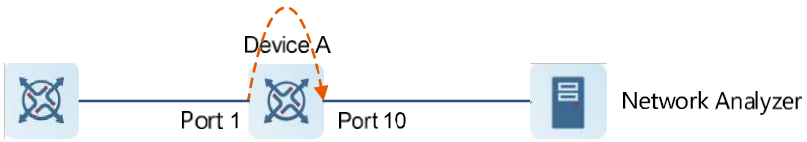
7.4 Дзеркальне відображення портів

7.4.1 Огляд

Функція аналізатора комутованих портів (SPAN) - це функція, яка копіює пакети певного порту на інший порт, підключений до пристрою мережевого моніторингу. Після налаштування дзеркального відображення портів пакети на порту-джерелі будуть копіюватися і пересилатися на порт призначення, а до порту призначення зазвичай підключається аналізатор пакетів для аналізу стану пакетів на порту-джерелі, щоб контролювати всі вхідні та вихідні пакети на портах-джерелах.

Як показано, налаштувавши віддзеркалення портів на пристрої A, пристрій копіює пакети з порту 1 на порт 10. Хоча пристрій мережевого аналізу, підключений до порту 10, не підключений безпосередньо до порту 1, він може отримувати пакети через порт 1. Таким чином, мета моніторингу потоку даних, що передається через порт 1, реалізована.

Рисунок 7-1 Принципи дзеркалювання портів Рисунок



Функція SPAN не тільки реалізує аналіз трафіку даних підозрілих вузлів мережі або портів пристроїв, але й не впливає на переадресацію даних пристрою, що моніториться. Вона в основному використовується в сценаріях моніторингу мережі та усунення несправностей.

7.4.2 Процедура

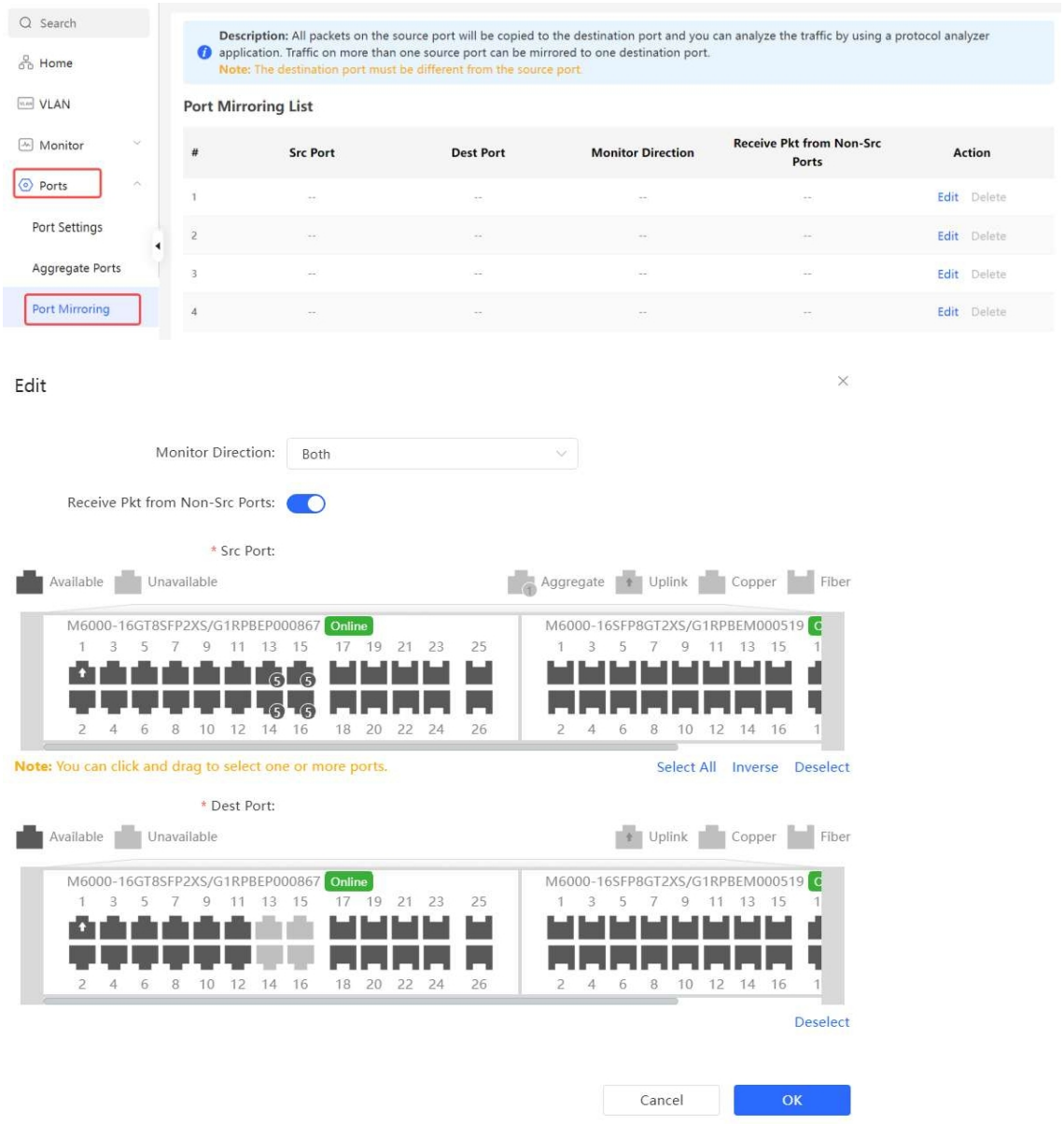
Виберіть **Локальний пристрій**> **Порти**> **Дзеркалення портів**.

Натисніть кнопку **Змінити**, виберіть порт-джерело, порт-приймач, напрямок моніторингу і вкажіть, чи потрібно приймати пакети з портів, які не є джерелом, і натисніть кнопку **ОК**. Можна налаштувати максимум чотири записи SPAN.

Щоб видалити конфігурацію дзеркалювання портів, натисніть **Видалити** у відповідному стовпчику **Дія**.

Застереження

- Ви можете вибрати кілька портів моніторингу вихідного трафіку, але тільки один порт призначення. Крім того, порти моніторингу вихідного трафіку не можуть містити порт призначення.
- Агрегований інтерфейс не можна використовувати як порт призначення.
- Можна налаштувати максимум чотири записи SPAN. SPAN не можна налаштувати для портів, які вже використовувалися для SPAN.



Таблиця 7-6 Опис параметрів дзеркалювання портів

Параметр	Опис	Значення за замовчуванням

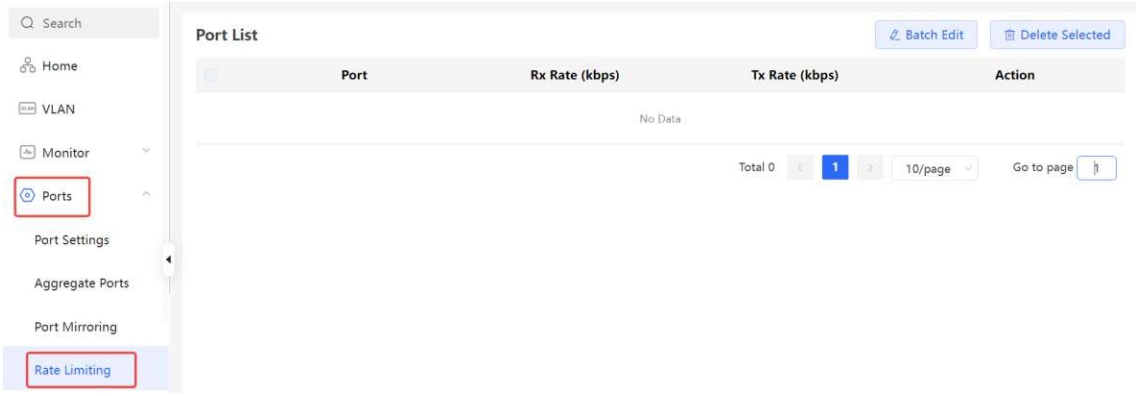
Src Порт	Порт-джерело також називають контрольованим портом. Потоки даних на порту-джерелі відстежуються для аналізу мережі або усунення несправностей. Підтримує вибір декількох портів-джерел і віддзеркалення декількох портів на один порт призначення	Н/Д

Параметр	Опис	Значення за замовчуванням
Порт призначення	Порт призначення також називається моніторинговим портом, тобто портом, підключеним до пристрою моніторингу, і пересилає отримані пакети з порту-джерела на пристрій моніторингу.	Н/Д
Напрямок монітора	Тип пакетів (напрямок потоку даних), який має відстежувати порт-джерело. ● Обидва: всі пакети, що проходять через порт, включаючи вхідні та вихідні пакети ● Вхідні: Всі пакети, отримані портом-джерелом, копіюються на порт призначення ● Вихідний: Всі пакети, передані портом-джерелом, копіюються на порт призначення	Обидва
Отримання Pkt з інших портів	Він застосовується до порту призначення і вказує, чи пересилає порт призначення інші пакети під час моніторингу пакетів. ● Увімкнено: Під час моніторингу пакетів порту-джерела пакети інших портів, що не є джерелом, зазвичай пересилаються ● Вимкнено: Відстежувати лише пакети вихідного порту	Увімкнути

7.5 Обмеження ставок

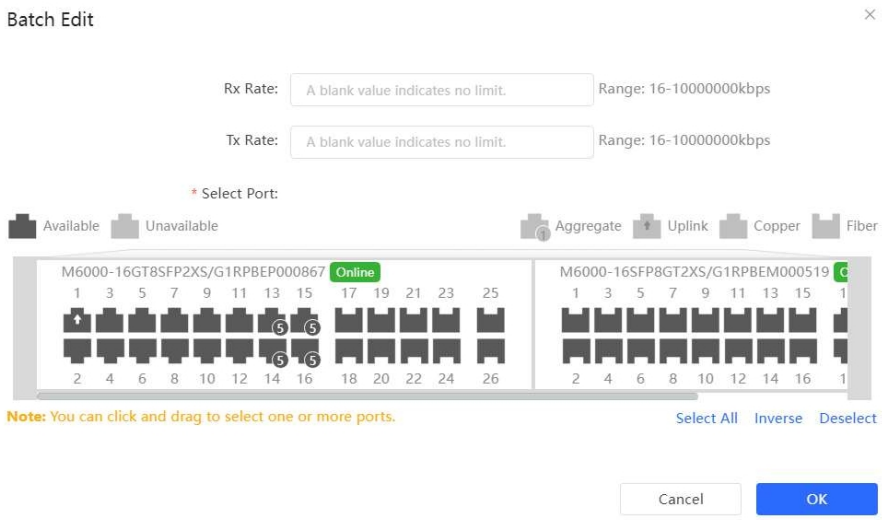
Виберіть **Локальний пристрій**> **Порти**> **Обмеження швидкості**.

Модуль Обмеження трафіку дозволяє налаштувати ліміти трафіку для портів, включаючи ліміти трафіку для вхідного і вихідного напрямку портів.



1. Конфігурація обмеження швидкості

Натисніть **Пакетне редагування**. У діалоговому вікні, що з'явиться, виберіть порти і введіть ліміти швидкості, а потім натисніть **OK**. Ви повинні налаштувати принаймні швидкість вхідного або вихідного трафіку. Після завершення конфігурації вона буде відображена у списку правил обмеження швидкості портів.



Таблиця 7-7 Опис параметрів обмеження швидкості

Параметр	Опис	Значення за замовчуванням
Швидкість передачі даних	Максимальна швидкість, з якою пакети надсилаються від порту до комутатора, у кбіт/с.	Не обмежено
Швидкість передачі даних	Максимальна швидкість, з якою пакети надсилаються з через порт, у кбіт/с.	Не обмежено

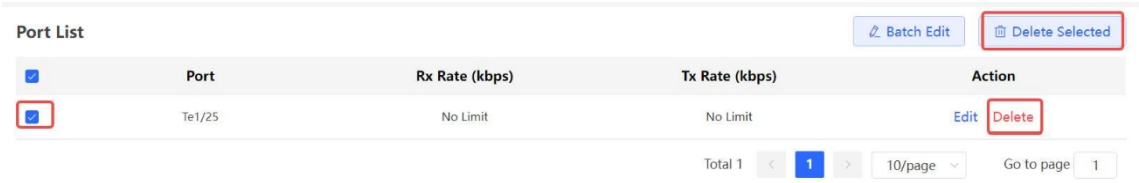
2. Зміна лімітів ставок в одному порту

У списку портів, для яких встановлено обмеження швидкості, натисніть кнопку **Змінити** на відповідному записі порту, введіть швидкість входу і швидкість виходу у діалоговому вікні, що з'явиться, і натисніть кнопку **OK**.

3. Обмеження швидкості видалення

Пакетне налаштування: Виберіть кілька записів у **списку портів**, натисніть кнопку **Видалити вибране** і натисніть кнопку **OK** у діалоговому вікні підтвердження.

Налаштуйте один порт: У **Списку портів** натисніть **Видалити** для відповідного запису порту і натисніть **OK** у діалоговому вікні підтвердження.



Примітка

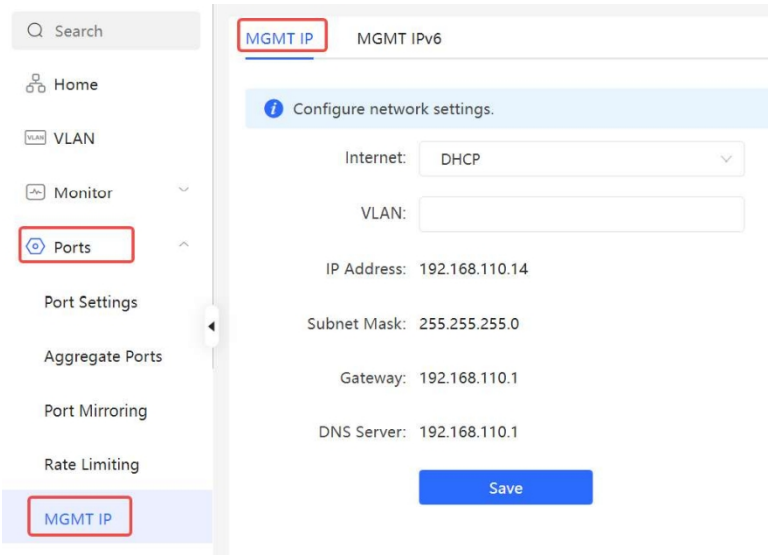
● Налаштовуючи обмеження швидкості для порту, ви повинні налаштувати принаймні вхідного або вихідного трафіку. ● Якщо швидкість вхідного або вихідного трафіку не задано, швидкість порту не обмежується.

7.6 Конфігурація MGMT IP

7.6.1 Налаштування адреси керування IPv4

Виберіть **Локальний пристрій> Порти> MGMT IP> MGMT IP**.

Сторінка **MGMT IP** дозволяє налаштувати IP-адресу керування для пристрою. Користувачі можуть налаштовувати та керувати пристроєм, отримавши доступ до керуючої IP-адреси.



Пристрій може працювати мережі в двох режимах:

● DHCP: використовує тимчасову IP-адресу, динамічно призначену попереднім DHCP-сервером для доступу до Інтернету. ● Статична IP-адреса: для доступу до Інтернету використовується статична IP-адреса, яку користувачі налаштовують вручну.

Якщо ви виберете DHCP, пристрій отримає параметри від сервера DHCP. Якщо Статичний IP, вам потрібно ввести керуючу VLAN, IP-адресу, маску підмережі, IP-адресу шлюзу за замовчуванням та адресу DNS-сервера. Натисніть **Зберегти**, щоб конфігурація набула чинності.

Примітка

- Якщо керуюча VLAN дорівнює нулю або не вказана, за замовчуванням діє VLAN 1.
- Керуючу VLAN потрібно вибрати з існуючих VLAN. Якщо VLAN не створено, перейдіть до списку VLAN, щоб додати VLAN (докладніше див. розділ 5.2 Налаштування VLAN).
- Рекомендується прив'язати сконфігуровану мережу керування VLAN до порту висхідної лінії зв'язку. В іншому випадку ви не зможете отримати доступ до веб-інтерфейсу.

7.6.2 Налаштування адреси керування IPv6

Налаштуйте IPv6-адресу для входу на сторінку керування пристроєм. Виберіть

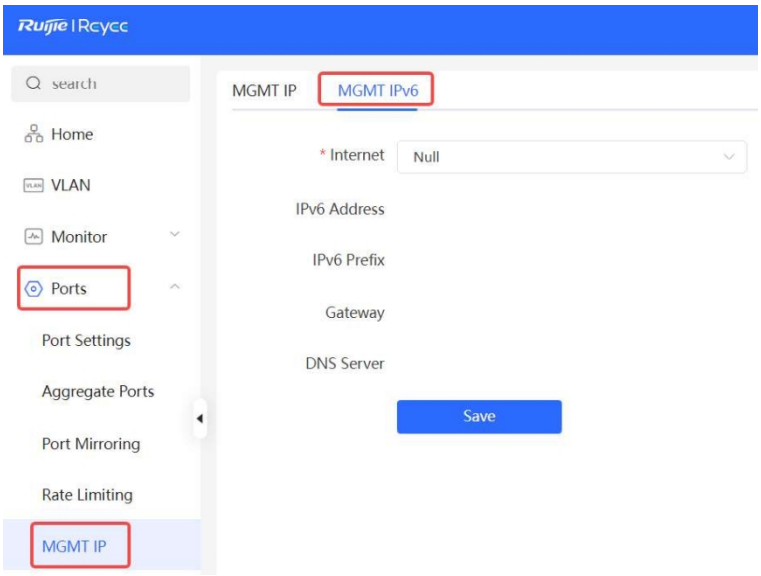
Локальний пристрій> Порти> MGMT IP> MGMT IPv6.

Налаштуйте керуючу IPv6-адресу так, щоб можна було увійти на сторінку керування пристроєм, використовуючи IPv6-адресу пристрою.

Пристрій підтримує наступні типи підключення до Інтернету:

- **Null**: Функцію IPv6 вимкнено на поточному порту.
- **DHCP**: Пристрій динамічно отримує IPv6-адресу від попереднього пристрою.
- **Статичний IP**: Вам потрібно вручну налаштувати адресу IPv6, довжину, адресу шлюзу та DNS-сервер.

Натисніть **Зберегти**.



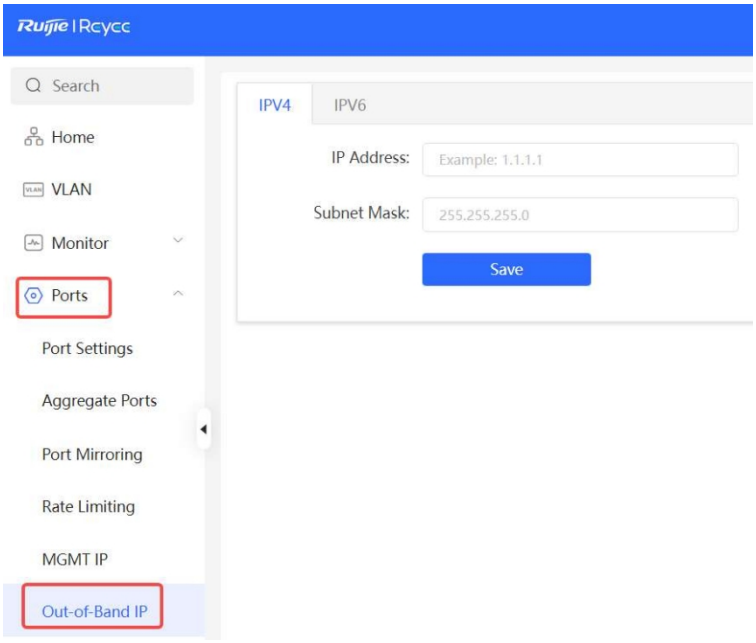
7.7 Конфігурація позасмугового IP

Специфікація

Цю функцію підтримують лише моделі RG-NBS7006, RG-NBS7003 та RG-NBS6002.

Виберіть **Локальний пристрій> Порти> Позасмуговий IP**.

Встановіть IP-адресу порту керування MGMT на шасі, щоб централізовано керувати модулями в декількох слотах пристрою.



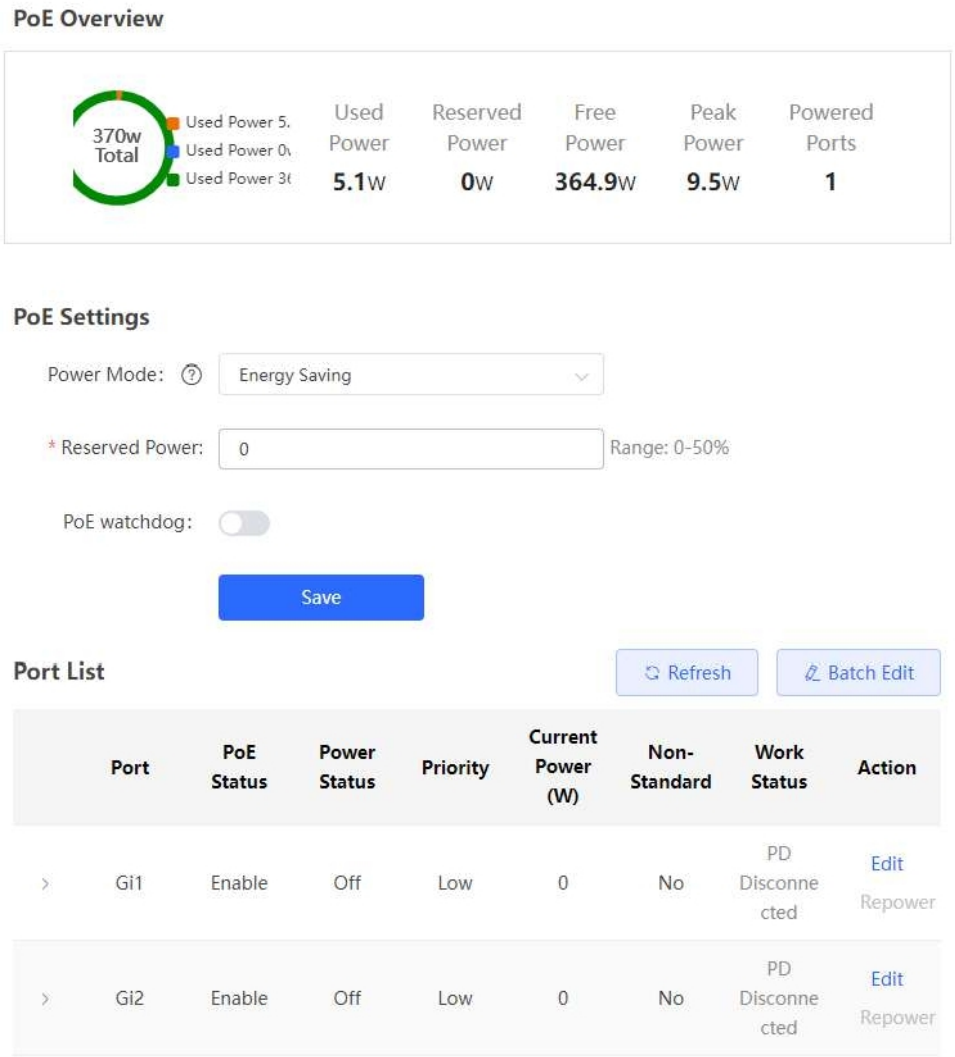
7.8 Конфігурація PoE

Специфікація

Цю функцію підтримують лише комутатори PoE (назва моделі містить P, -LP, -HP та -UP).

Виберіть **Локальний пристрій**> **Порти**> **PoE**.

Пристрій подає живлення на пристрої з живленням PoE через порти. Користувачі можуть переглядати поточний стан живлення, а також встановлювати політики живлення системи та живлення портів відповідно, щоб досягти гнучкого розподілу живлення.



7.8.1 Глобальні налаштування PoE

Виберіть **Локальний пристрій**> **Порти**> **PoE**> **Налаштування PoE**.

Режим передачі живлення PoE - це спосіб, у який пристрій розподіляє живлення на підключений PD (пристрій з живленням). Він підтримує автоматичний режим і режим енергозбереження.

У режимі Auto система розподіляє живлення на основі класів PD, виявлених на портах. Пристрій розподіляє потужність для PD-пристроїв класу 0~4 на основі фіксованого значення: Клас 0 - 15,4 Вт, клас 1 - 4 Вт, клас 2 - 7 Вт, клас 3 - 15,4 Вт, клас 4 тип 1 - 15,4 Вт, клас 4 тип 2 - 30 Вт. У цьому режимі, якщо порт підключено до пристрою класу 3, навіть якщо фактичне енергоспоживання становить лише 11 Вт, пристрій живлення PoE виділятиме живлення порту, виходячи з потужності 15,4 Вт.

У режимі енергозбереження PoE-пристрій динамічно регулює виділену потужність на основі фактичного споживання PD. У цьому режимі, щоб запобігти живлення порту через коливання фактичного енергоспоживання PD при повному навантаженні, ви можете встановити Резервну потужність передачі, і зарезервована потужність не буде використовуватися для живлення, щоб загальна потужність, споживається поточною системою, не перевищувала ліміт пристрою PoE. Розмір зарезервованої потужності виражається у відсотках від загальної потужності PoE. Значення знаходиться в діапазоні від 0 до 50.

Сторожовий таймер PoE: Ця функція переважно застосовується для сценаріїв спостереження за безпекою. Якщо цю функцію увімкнено, якщо порт PoE пристрою раптово перестає отримувати пакети під час інтервалу пінгування, пристрій з живленням (PD) буде перезавантажено після закінчення інтервалу пінгування для відновлення нормальної роботи.

Таблиця 7-8 Конфігурація сторожового таймера PoE Опис

Стан отримання пакетів порту PoE	Сторожовий таймер PoE увімкнено	**Вжиті заходи щодо ПД**
Під час інтервалу пінгу PoE-порт пристрою раптово перестає приймати пакети.	Так.	PD перезапускається для відновлення нормальної роботи, а інтервал пінгування скидається.
	Ні.	Жодних дій щодо ПД не ініціюється.
час інтервалу ping порт PoE пристрою все ще перестає приймати пакети.	Так.	Жодних дій щодо ПД не ініціюється.
	Ні.	Жодних дій щодо ПД не ініціюється.
Під час інтервалу ping на PoE-порт пристрою починають надходити пакети.	Так.	Інтервал опитування скинуто.
	Ні.	Жодних дій щодо ПД не ініціюється.

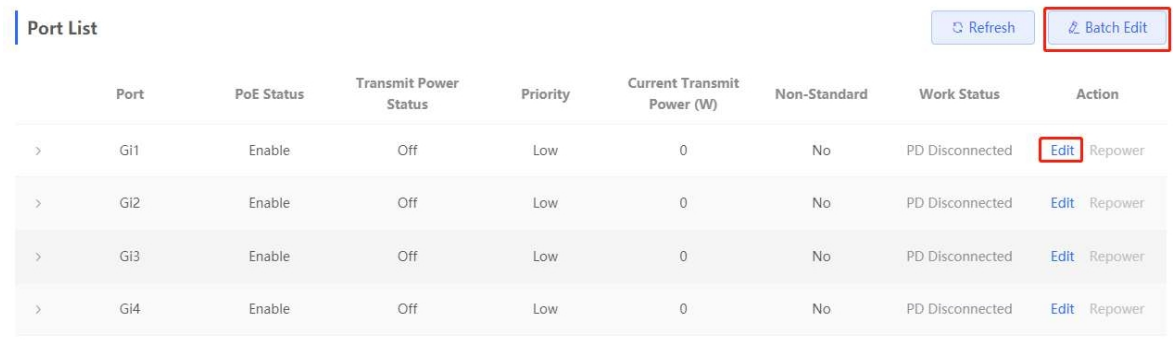
Примітка

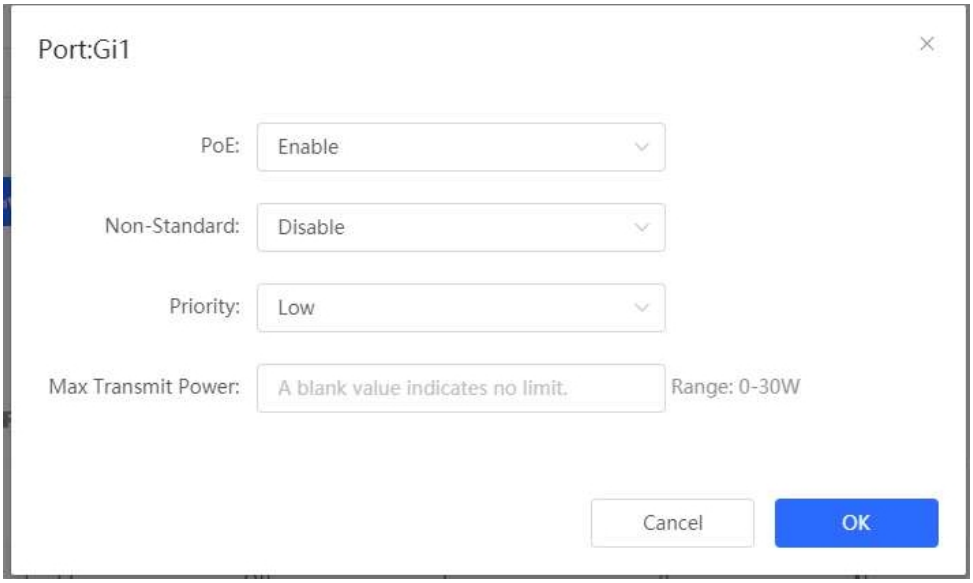
Якщо до порту цього пристрою з підтримкою PoE підключено не-PD, наприклад, комп'ютер, сторожовий таймер PoE не ініціює жодних дій на не-PD, навіть якщо виконано умову запуску.

7.8.2 Конфігурація живлення портів

Виберіть **Локальний пристрій**> **Порти**> **PoE**> **Список портів**.

Натисніть кнопку **Редагувати** у записі порту або натисніть кнопку **Пакетне редагування**, щоб налаштувати функцію живлення PoE для порту.





Таблиця 7-9 Опис параметрів конфігурації живлення портів

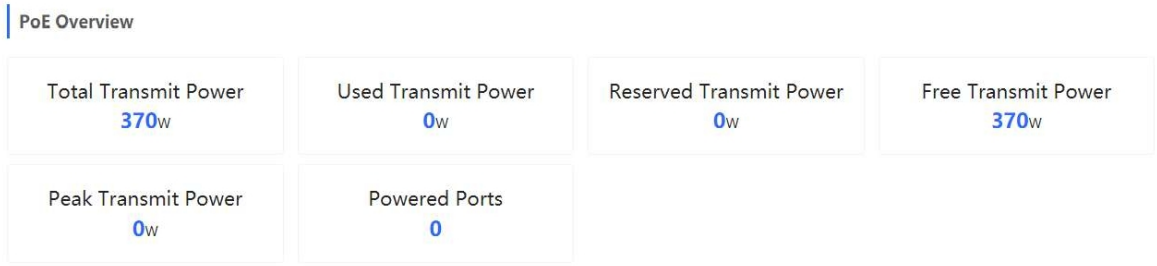
Параметр	Опис	Значення за замовчуванням
PoE	Чи вмикати функцію живлення на портах	Увімкнути
Нестандартний	За замовчуванням пристрій подає живлення тільки на PD, які відповідають стандартам IEEE 802.3af і 802.3at. У практичному застосуванні можуть зустрічатися PD, які не відповідають стандартам. Після увімкнення нестандартного режиму порт пристрою може подавати живлення на деякі нестандартні PD-пристрої.	Вимкнути
Пріоритет	Пріоритет живлення порту поділяється на три рівні: Високий, Середній та Низький В автоматичному та енергозберігаючому режимах першими вмикаються порти з високими пріоритетами. Якщо системної потужності PoE-пристрою недостатньо, першими вимикаються порти з низькими пріоритетами. Порти з однаковим пріоритетом сортуються за номером порту. Менший номер порту означає вищий пріоритет.	Низький

Параметр	Опис	Значення за замовчуванням
Максимальна потужність передачі	Максимальна потужність, яку може передавати порт, від 0 до 30, у ватах (Вт). Порожнє значення означає відсутність обмежень	Це не межа

7.8.3 Відображення інформації про глобальну мережу PoE

Виберіть **Локальний пристрій> Порти> PoE> Огляд PoE**.

Відображає глобальну інформацію про живлення функції PoE, зокрема загальну потужність системи, використану потужність, зарезервовану потужність, залишкову доступну потужність, пікову максимальну потужність і кількість портів, які наразі живляться.

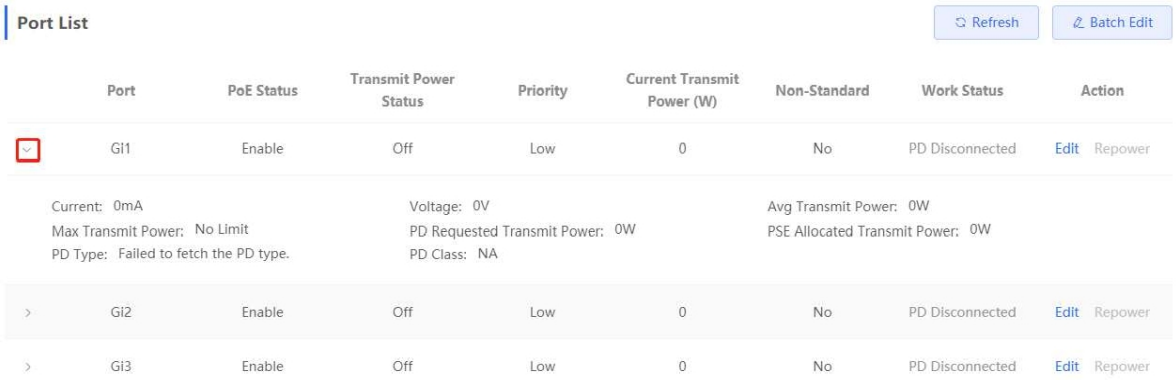


7.8.4 Відображення інформації про порт PoE

Виберіть **Локальний пристрій> PoE> Список портів**.

Список портів відображає конфігурацію PoE та інформацію про стан кожного порту. Клацніть, щоб розгорнути детальну інформацію.

Якщо пристрій PD, підключений до порту, потрібно перезапустити, наприклад, якщо підключена до порту точка доступу несправна, ви можете натиснути кнопку **Перезапустити**, щоб ненадовго вимкнути живлення порту, а потім знову увімкнути його, щоб перезапустити пристрій, підключений до порту живлення.



Таблиця 7-10 Опис інформації про джерело живлення порту

Поле	Опис
Порт	Ідентифікатор порту пристрою
Стан PoE	Чи вмикати функцію PoE на портах.
Стан потужності передачі	Чи подає порт живлення на PD в даний момент.

Поле	Опис
Пріоритет	Пріоритет живлення порту поділяється на три рівні: Високий, Середній та Низький.
Поточна потужність передачі	Показує вихідну потужність поточного порту у ватах (Вт).
Нестандартний	Показує, чи увімкнено режим нестандартної сумісності.
Статус роботи	Поточний стан роботи портів PoE.
Течія	Показує поточний струм порту в міліамперах (мА).
Напруга	Показує поточний струм порту у вольтах (V).
Середня потужність передачі	Показує поточну середню потужність порту, а саме, середнє арифметичне значення поточної потужності після увімкнення порту, у ватах (Вт).
Максимальна потужність передачі	Максимальна вихідна потужність порту у ватах (Вт).
PD Запитувана потужність передачі	Потужність, яку PD запитує у PSE (Power Sourcing Equipment, обладнання живлення), у ватах (Вт).
PSE Виділена потужність передачі	Показує потужність, яку PSE виділяє PD у ватах (Вт).
Тип PD	Інформація про тип ПД, отримана за допомогою класифікації LLDP, поділяється на Тип 1 та Тип 2.
Клас PD	Рівень класифікації PD, підключеного до порту, поділяється на класи 0~4 відповідно до стандарту IEEE 802.3af/802.3at.

8 Багатоадресна передача на рівні 2

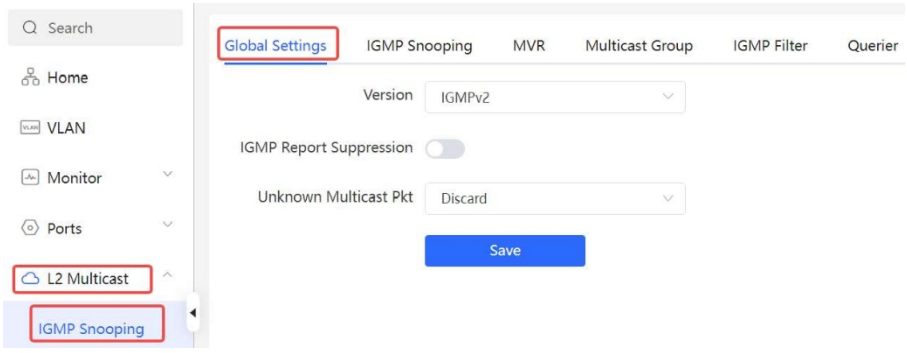
8.1 Огляд багатоадресної розсилки

Методи передачі IP поділяються на одноадресні, багатоадресні та широкомовні. При багатоадресній передачі IP-пакет відправляється з джерела і пересилається певній групі одержувачів. Порівняно з одноадресною та широкомовною передачею, багатоадресна IP-розсилка економить смугу пропускання і зменшує навантаження на мережу. Тому багатоадресна IP-розсилка застосовується для різних мережевих сервісів, які мають високі вимоги до реальної оперативності, наприклад, інтернет-телебачення, дистанційна освіта, прямі трансляції та мультимедійні конференції.

8.2 Глобальні налаштування багатоадресної розсилки

Виберіть **Локальний пристрій > Багатоадресна розсилка L2> IGMP Snooping> Глобальні налаштування**.

Глобальні налаштування дозволяють вказати версію протоколу IGMP, ввімкнути придушення пакетів звітів і поведінку обробки невідомих багатоадресних пакетів.



Таблиця 8-1 Опис параметрів конфігурації глобальної багатоадресної розсилки

Параметр	Опис	Значення за замовчуванням
Версія	Протокол керування групами в Інтернеті (IGMP) - це протокол TCP/IP, який керує учасниками групи багатоадресної розсилки IPv4 і працює на пристроях багатоадресної розсилки та хостах, розташованих на заглушці мережі багатоадресної розсилки, створюючи і підтримуючи членство в групі багатоадресної розсилки між хостами і підключеними до них пристроями багатоадресної розсилки. Існує три версії IGMP: IGMPv1, IGMPv2 і IGMPv3. Цей параметр використовується для встановлення найвищої версії IGMP-пакетів, які можуть оброблятися багатоадресною передачею 2-го рівня, і може мати значення IGMPv2 або IGMPv3.	IGMPv2

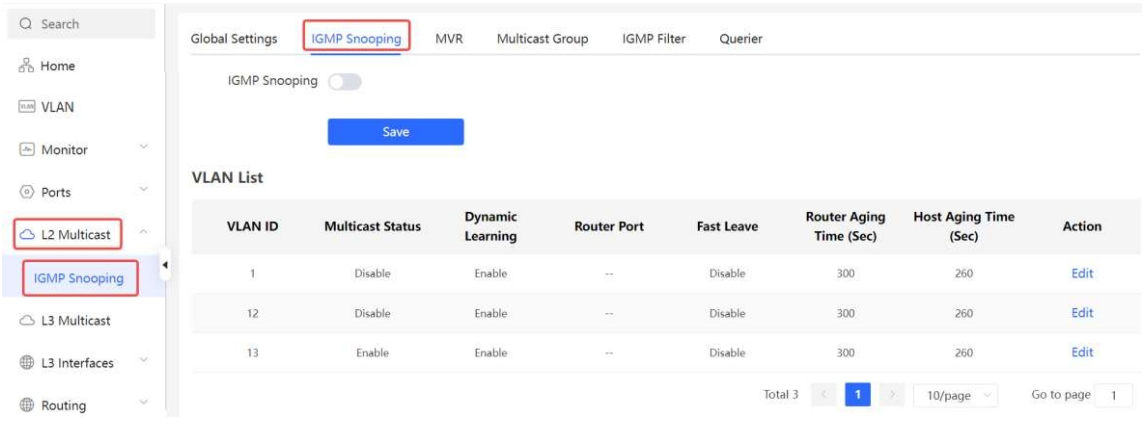
Параметр	Опис	Значення за замовчуванням
Придушення звітів IGMP	Після ввімкнення цієї функції, щоб зменшити кількість пакетів у мережі, заощадити пропускну здатність мережі та забезпечити продуктивність пристрою багатоадресної розсилки IGMP, комутатор пересилає лише один пакет звіту на маршрутизатор багатоадресної розсилки, якщо кілька клієнтів низхідної лінії, підключених до комутатора, одночасно надсилають пакет звіту з запитом до однієї і тієї ж групи багатоадресної розсилки.	Вимкнути
Невідомий Pkt багатоадресної розсилки	Якщо увімкнено функції глобальної багатоадресної розсилки та багатоадресної розсилки у локальній мережі, метод обробки невідомих багатоадресних пакетів можна встановити як "**Відкинути**" або "**Переповнити**".	Викинути

8.3 IGMP Snooping

8.3.1 Огляд

Відстеження протоколу управління групами в Інтернеті (IGMP) - це механізм відстеження багатоадресної IP-розсилки, який працює у віртуальній локальній мережі для управління та контролю переадресації багатоадресного IP-трафіку в межах віртуальної локальної мережі. Він реалізує функцію багатоадресної розсилки на рівні 2.

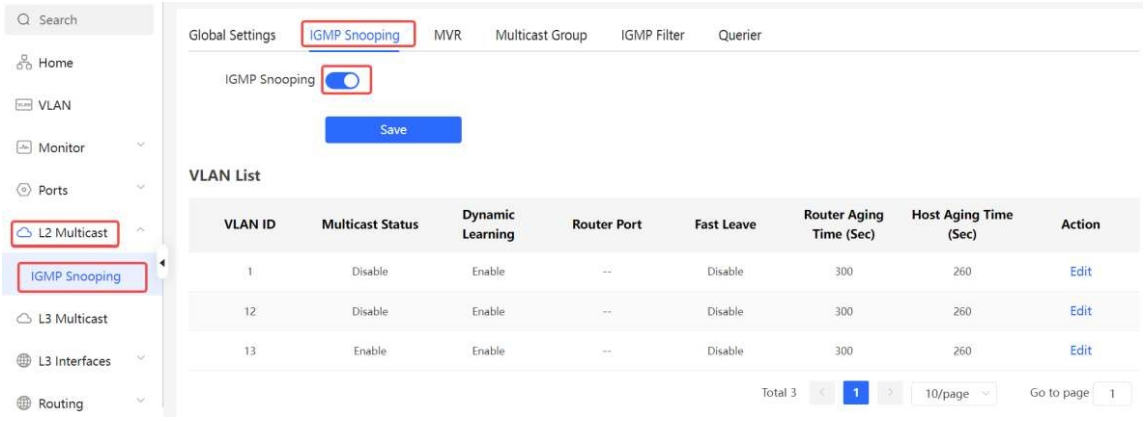
Як правило, багатоадресні пакети повинні проходити через комутатори рівня 2, особливо в деяких локальних мережах (LAN). Якщо на комутаторі 2-го рівня не працює функція IGMP Snooping, IP-пакети багатоадресної розсилки передаються в широкомовному режимі у ВЛВС; якщо на 2-го рівня працює IGMP Snooping, пристрій 2-го рівня може відстежувати пакети протоколу IGMP від хоста користувача і пристрою багатоадресної розсилки PIM, що знаходиться вище за течією. Таким чином, створюється запис багатоадресної розсилки на рівні 2, і IP-пакети багатоадресної розсилки контролюються, щоб надсилатися тільки на приймачі членів групи, запобігаючи трансляції даних багатоадресної розсилки в мережі рівня 2.



8.3.2 Увімкнення глобального IGMP Snooping

Виберіть **Локальний пристрій**> **L2 Multicast**> **IGMP Snooping**> **IGMP Snooping**.

Увімкніть **IGMP Snooping** і натисніть **Зберегти**.



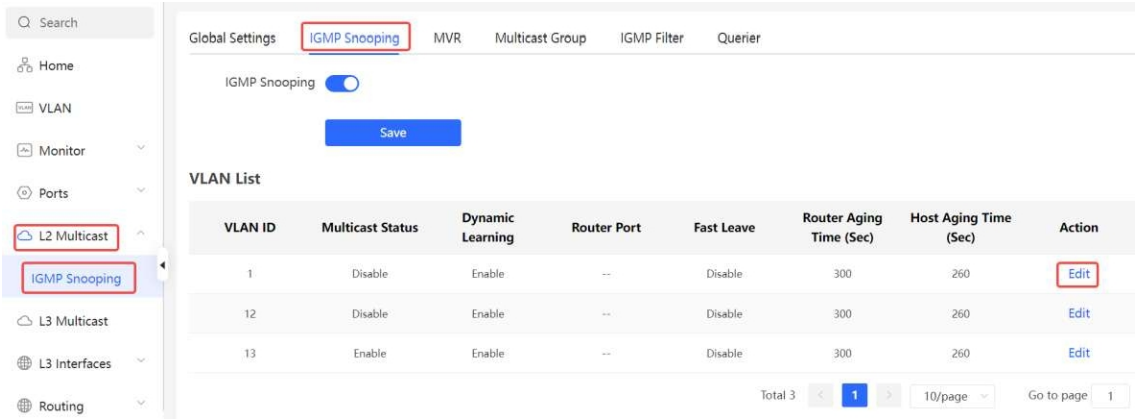
8.3.3 Налаштування параметрів обробки пакетів протоколу

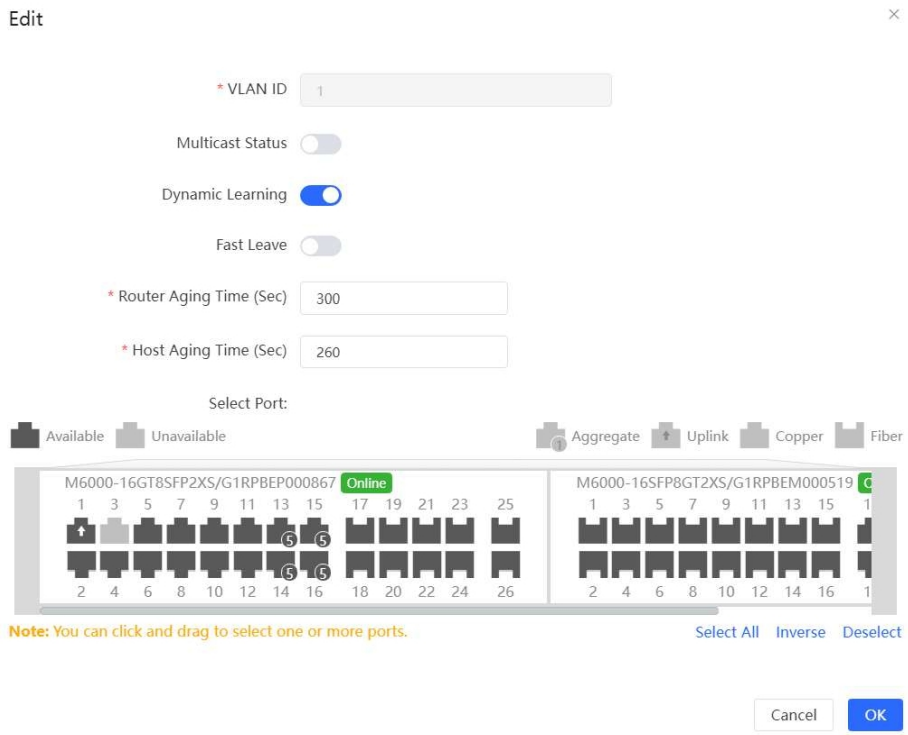
Керуючи обробкою пакетів протоколу, пристрій багатоадресної розсилки 2-го рівня може створювати статичні або динамічні записи переадресації багатоадресної розсилки. Крім того, пристрій може налаштовувати параметри для швидкого оновлення динамічних записів переадресації багатоадресної розсилки та членства в IGMP snooping.

Виберіть **Локальний пристрій**> **L2 Multicast**> **IGMP Snooping**> **IGMP Snooping**.

Функція IGMP Snooping реалізована на основі VLAN. Тому кожній VLAN відповідає запис налаштування IGMP Snooping. Існує стільки записів IGMP Snooping, скільки VLAN на пристрої.

Натисніть кнопку **Змінити** в пункті VLAN. У діалоговому вікні, що з'явиться, увімкніть/вимкніть функцію багатоадресної розсилки VLAN, динамічного навчання, функцію швидкого виходу і порт підключення статичного маршруту, а також встановіть час старіння маршрутизатора і час старіння хоста, після чого натисніть кнопку **OK**.





Таблиця 8-2 Опис параметрів конфігурації VLAN для IGMP Snooping

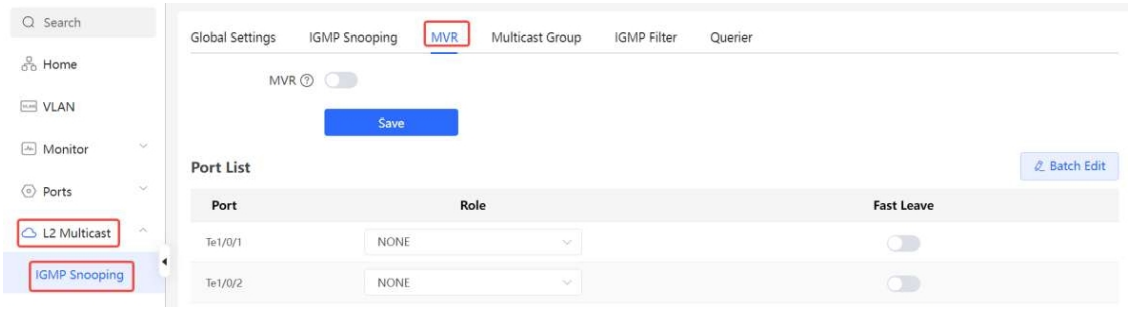
Параметр	Опис	Значення за замовчуванням
Статус багатоадресної розсилки	Увімкнення або вимкнення функції багатоадресної розсилки VLAN. Функція багатоадресної розсилки VLAN вступає в дію лише тоді, коли ввімкнено як глобальне IGMP-спостереження, так і функцію багатоадресної розсилки VLAN.	Вимкнути
Динамічне навчання	Пристрій, на якому запущено IGMP Snooping, ідентифікує порти у VLAN як порти маршрутизатора або порти учасника. Порт маршрутизатора - це порт на пристрої багатоадресної розсилки рівня 2, який підключений до пристрою багатоадресної розсилки рівня 3, а порт учасника - це порт хоста, підключений до групи на пристрої багатоадресної розсилки рівня 2. Переглядаючи пакети IGMP, пристрій багатоадресної розсилки 2-го рівня може автоматично виявляти і підтримувати динамічні порти маршрутизатора багатоадресної розсилки.	Увімкнути
Порт роутера	Список поточних портів багатоадресного маршрутизатора включає динамічно навчені маршрутизовані порти (якщо функцію динамічного навчання) та статично налаштовані маршрутизовані порти.	NA

Параметр	Опис	Значення за замовчуванням
Швидка відпустка	Після увімкнення цієї опції, коли порт отримує пакети Leave, він негайно видаляє порт з групи багатоадресної розсилки, не чекаючи таймауту старіння. Після цього, коли пристрій отримуватиме відповідні пакети запитів певної групи та пакети багатоадресних даних, він більше не пересилатиме їх на цей порт. Ця функція застосовується, коли до одного порту пристрою підключено лише один хост, і зазвичай вмикається на комутаторі доступу, безпосередньо підключеному до кінцевої точки.	Вимкнути
Час старіння маршрутизатора (сек)	Час старіння портів багатоадресного маршрутизатора, що динамічно навчаються, становить від 30 до 3600 секунд.	300 секунд
Час старіння хоста (сек)	Час старіння динамічно вивчених портів учасників групи багатоадресної розсилки, в секундах.	260 секунд
Виберіть порт	У діалоговому вікні, що з'явиться, виберіть порт і налаштуйте його як статичний порт маршрутизатора. Коли порт налаштовано як статичний порт маршрутизатора, він не застаріває	NA

8.4 Налаштування MVR

8.4.1 Огляд

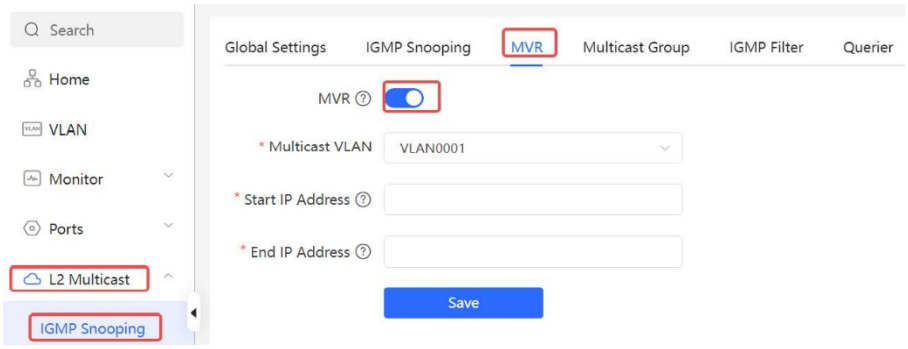
IGMP-сканування може пересилати багатоадресний трафік лише в одній VLAN. Якщо багатоадресний трафік потрібно переадресувати в різні VLAN, джерело багатоадресної розсилки має надсилати багатоадресний трафік у різні VLAN. Щоб заощадити пропускну здатність висхідного каналу і зменшити навантаження на джерела багатоадресної розсилки, з' регістр багатоадресної VLAN (MVR). MVR може копіювати багатоадресний трафік, отриманий з VLAN MVR, у VLAN, до якої належить користувач, і переадресовувати трафік.



8.4.2 Налаштування глобальних параметрів MVR

Виберіть **Локальний пристрій**> **L2 Багатоадресна розсилка**> **IGMP Snooping**> **MVR**.

Натисніть, щоб увімкнути MVR, виберіть VLAN MVR, задайте групу багатоадресної розсилки, яка підтримується VLAN, і натисніть кнопку **Зберегти**. Можна вказати кілька груп багатоадресної розсилки, ввівши початкову і кінцеву IP-адреси багатоадресної розсилки.



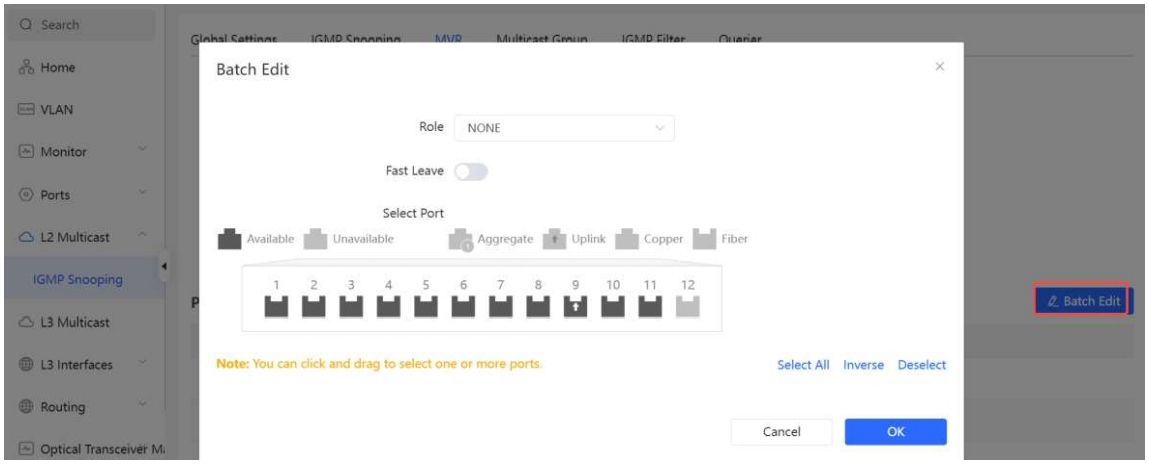
Таблиця 8-3 Опис налаштування глобальних параметрів MVR

Параметр	Опис	Значення за замовчуванням
MVR	Вмикає/вимикає MVR глобально	Вимкнути
Багатоадресна VLAN	VLAN джерела багатоадресної розсилки	1
Початкова IP-адреса	Вивчена або налаштована стартова IP-адреса багатоадресної групи багатоадресної розсилки MVR.	NA
Кінцева IP-адреса	Вивчена або налаштована кінцева IP-адреса групи багатоадресної розсилки MVR.	NA

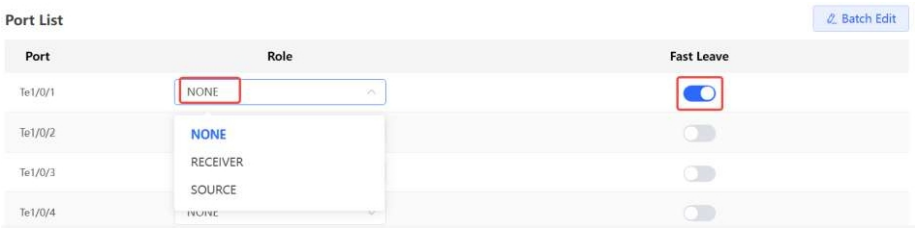
8.5 Налаштування портів MVR

Виберіть **Локальний пристрій**> **L2 Багатоадресна розсилка**> **IGMP Snooping**> **MVR**.

- Налаштування пакетів: Натисніть **Batch Edit**, виберіть роль порту, порт, який потрібно налаштувати, і чи потрібно ввімкнути функцію Fast Leave на порту, а потім натисніть **OK**.



- Налаштуйте один порт: Клацніть розкривний список, щоб вибрати тип ролі MVR для порту. Клацніть перемикач у стовпчику **Fast Leave**, щоб вказати, чи ввімкнути функцію швидкого виходу з порту.



Таблиця 8-4 Опис параметрів конфігурації портів MVR

Параметр	Опис	Значення за замовчуванням
Роль	**HI**: Вказує на те, що функція MVR вимкнена. **SOURCE**: Вказує на порт-джерело, який отримує багатоадресні потоки даних. **RECEIVER**: Вказує на порт приймача, підключений до клієнта.	HI
Швидка відпустка	Дозволяє налаштувати функцію швидкого видалення для порту. Після увімкнення цієї функції, якщо порт отримує пакет звільнення, його буде негайно видалено з групи багатоадресної розсилки.	Вимкнути

Примітка

- Якщо налаштовано порт-джерело або порт-приймач, порт-джерело повинен належати до VLAN MVR, а порт-приймач не повинен належати до VLAN MVR.
- Функція швидкого виходу діє тільки на порту приймача.

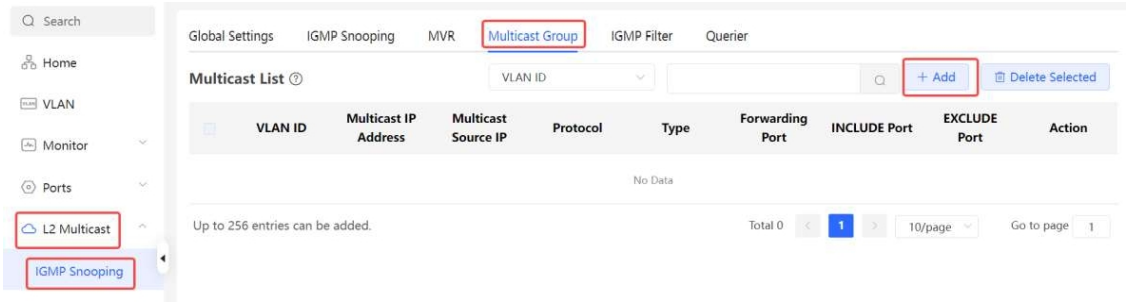
8.6 Налаштування групи багатоадресної розсилки

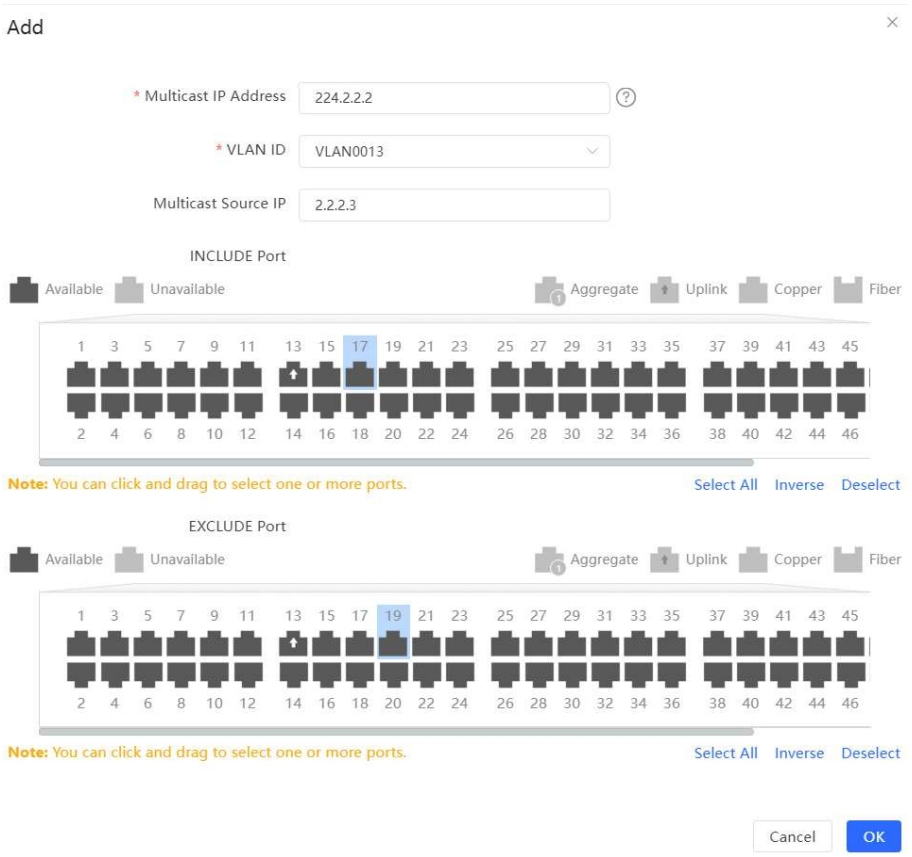
Виберіть **Локальний пристрій**> **L2 Multicast**> **IGMP Snooping**> **Multicast Group**.

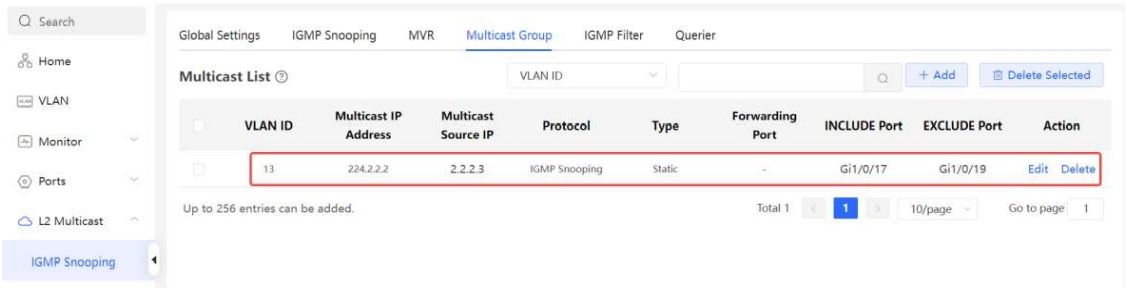
Група багатоадресної розсилки складається з портів призначення, на які мають надсилатися багатоадресні пакети. Багатоадресні пакети надсилаються на всі порти в групі багатоадресної розсилки.

Ви можете переглянути **список багатоадресної розсилки** на поточній сторінці. Поле пошуку у верхньому правому куті підтримує пошук записів груп багатоадресної розсилки на основі ідентифікаторів VLAN або адрес багатоадресної розсилки.

Натисніть **Додати**, щоб створити групу багатоадресної розсилки.







Таблиця 8-5 Опис параметрів конфігурації групи багатоадресної розсилки

Параметр	Опис	Значення за замовчуванням
ІДЕНТИФІКАТОР VLAN	VLAN, до якої належить отриманий багатоадресний трафік	NA
Багатоадрес на IP-адреса	Багатоадресна IP-адреса. Діапазон значень від 224.0.1.0 до 239.255.255.255.	NA

Параметр	Опис	Значення за замовчуванням
IP-адреса джерела багатоадресної розсилки	IP-адреса джерела багатоадресної розсилки. **Примітка** Якщо версія програмного забезпечення ReyeeOS 2.320 або новіша, а глобально налаштована версія IGMP - IGMPv3, цей параметр можна встановити і відобразити у списку багатоадресної розсилки.	NA
Протокол	Якщо ідентифікатор VLAN є багатоадресною VLAN і адреса багатоадресної розсилки знаходиться в межах діапазону IP-адрес багатоадресної розсилки MVR, протокол MVR. В інших випадках використовується протокол IGMP snooping.	NA
Тип	Режим генерації груп багатоадресної розсилки може бути статично налаштований або динамічно вивчений. У звичайних випадках порт може приєднатися до групи багатоадресної розсилки тільки після того, як порт отримає пакет IGMP Report від групи багатоадресної розсилки, тобто в режимі динамічного навчання. Якщо ви додаєте порт до групи вручну, він може бути статично доданий до групи і обмінюватися інформацією про групу багатоадресної розсилки з маршрутизатором PIM без обміну пакетами IGMP.	NA
Порт переадресації	Список портів, які переадресовують багатоадресний трафік	NA
INCLUDE Порт	Порт INCLUDE приймає трафік лише із зазначених адрес джерел багатоадресної розсилки. Як показано на попередньому рисунку, порт INCLUDE є Te1/0/4 і приймає лише трафік з адресою джерела 2.2.2.6 з багатоадресного трафіку з адресою 224.2.2.2. **Примітка** Якщо версія програмного забезпечення ReyeeOS 2.320 або новіша, а глобально налаштована версія IGMP - IGMPv3, цей параметр можна встановити і відобразити у списку багатоадресної розсилки.	NA
ВИКЛЮЧИТИ порт	Порт EXCLUDE не приймає трафік із зазначених адрес джерел багатоадресної розсилки. Як показано на попередньому рисунку, порт EXLUDE є Te1/0/5 і не приймає багатоадресний трафік з адресою джерела 2.2.2.6 від багатоадресного трафіку з адресою 224.2.2.2. **Примітка** Якщо версія програмного забезпечення ReyeeOS 2.320 або новіша, а глобально налаштована версія IGMP - IGMPv3, цей параметр можна встановити і відобразити у списку багатоадресної розсилки.	NA

Примітка

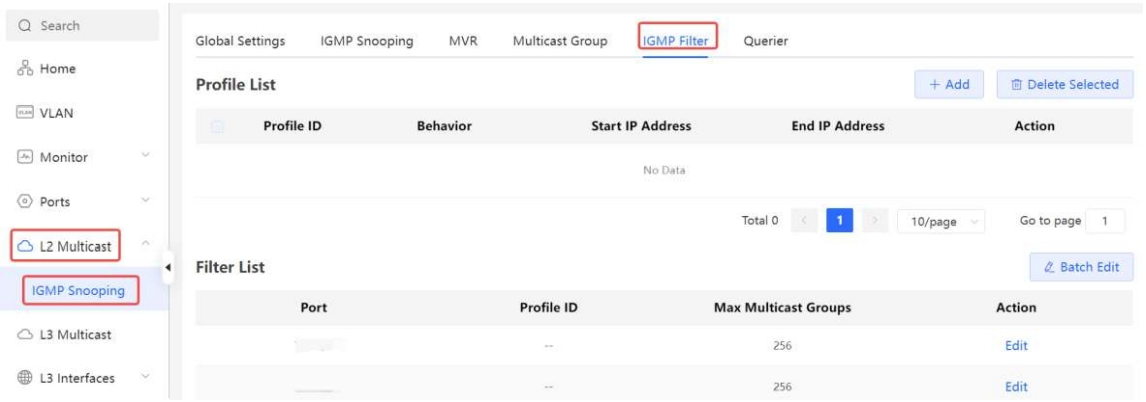
Статичні групи багатоадресної розсилки не можуть дізнатися інші динамічні порти переадресації.

8.7 Налаштування фільтра портів

Виберіть **Локальний пристрій**> **L2 Багатоадресна розсилка**> **IGMP Snooping**> **IGMP Filter**.

Як правило, пристрій, на якому працюють порти, може приєднатися до будь-якої групи багатоадресної розсилки. За допомогою фільтра портів можна налаштувати діапазон груп багатоадресної розсилки, які дозволяють або забороняють доступ користувачам, ви можете налаштувати обсяг послуг багатоадресної розсилки для користувачів, щоб гарантувати інтерес операторів і запобігти недійсному багатоадресному трафіку.

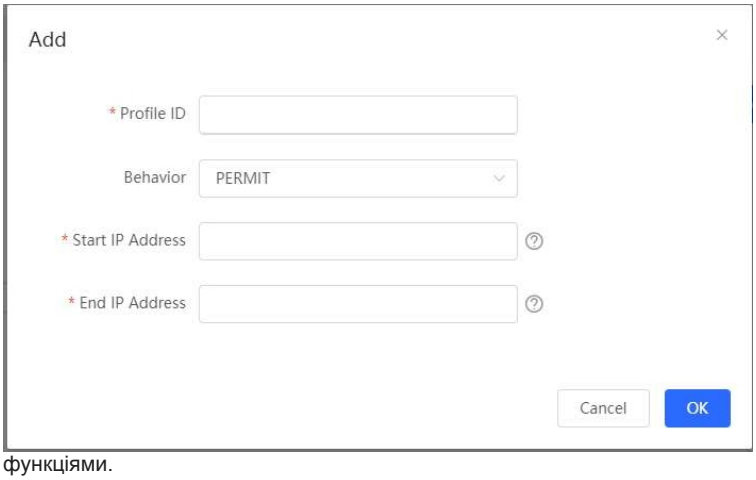
Налаштування фільтра портів складається з 2 кроків: налаштування профілю та встановлення обмеження на діапазон адрес групи портів.



8.7.1 Налаштування профілю

Виберіть **Локальний пристрій**> **L2 Multicast**> **IGMP Snooping**> **IGMP Filter**> **Список профілів**.

Натисніть **Додати**, щоб створити **профіль**. Профіль використовується для визначення діапазону груп багатоадресної розсилки, які дозволяють або забороняють доступ користувачам для використання іншими



функціями.

Таблиця 8-6 Опис параметрів конфігурації профілю

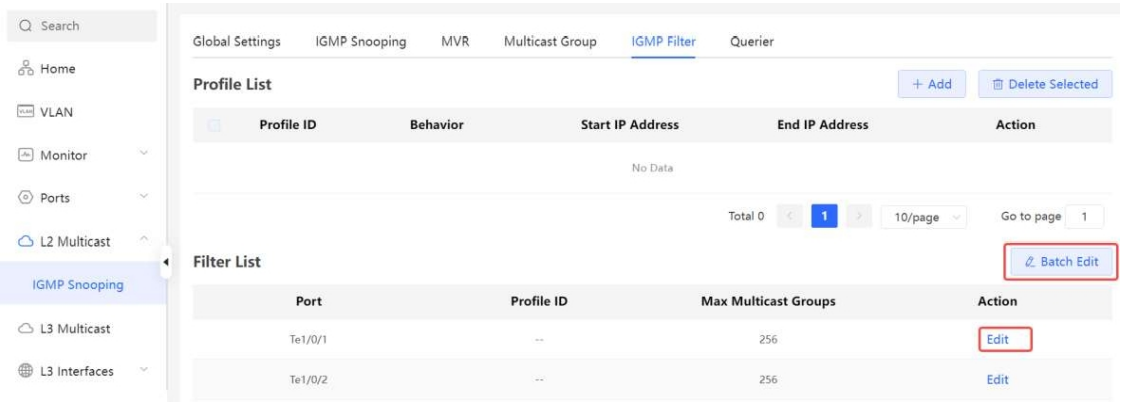
Параметр	Опис	Значення за замовчуванням
Ідентифікатор профілю	Ідентифікатор профілю	NA
Поведінка	**DENY**: Заборонити вимагати розсилку IP-адрес у вказаному діапазоні. **PERMIT**: Дозволяє запитувати лише IP-адреси розсилки у вказаному діапазоні.	NA
Початкова IP-адреса	Початок багатоадресної розсилки IP-адреса діапазону групових адрес багатоадресної розсилки	NA
Кінцева IP-адреса	Кінцева багатоадресна IP-адреса діапазону групових адрес багатоадресної розсилки	NA

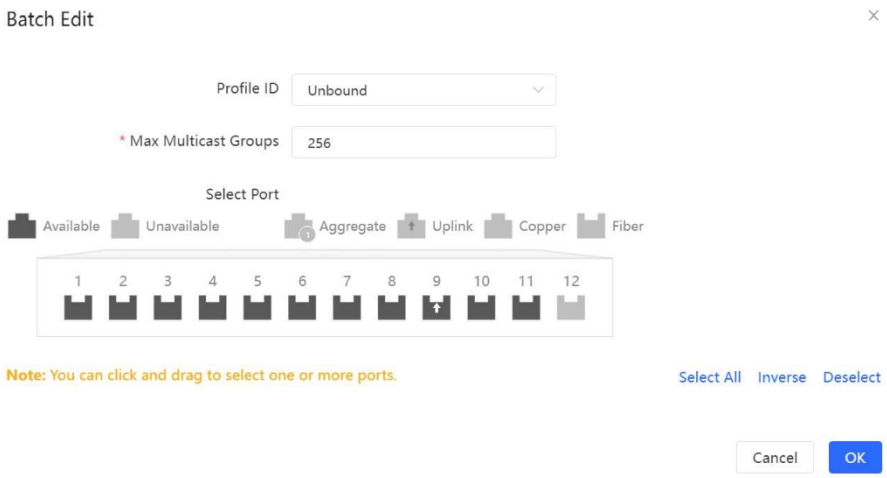
8.7.2 Налаштування діапазону груп багатоадресної розсилки для профілю

Виберіть **Локальний пристрій> L2 Multicast> IGMP Snooping> IGMP Filter> Список фільтрів**.

Портовий фільтр може посилатися на профіль для визначення діапазону групових адрес багатоадресної розсилки, які можуть або не можуть бути затребувані користувачами на порту.

Натисніть **Пакетне редагування** або **Редагування** окремого запису порту. У діалоговому вікні, що з'явиться, виберіть ID профілю і введіть максимальну кількість груп багатоадресної розсилки, дозволену для порту, а потім натисніть **OK**.





Таблиця 8-7 Опис параметрів конфігурації фільтра портів

Параметр	Опис	Значення за замовчуванням
Ідентифікатор профілю	Профіль, який застосовується до порту. Якщо його не встановлено, жодне правило профілю не буде прив'язано до порту.	NA
Максимальна кількість груп багатоадресної розсилки	Максимальна кількість груп багатоадресної розсилки, до яких може приєднатися порт. Якщо одночасно запитується занадто багато багатоадресного трафіку, пристрій багатоадресної розсилки буде сильно перевантажений. Тому налаштування максимальної кількості груп багатоадресної розсилки, дозволеної для порту, може гарантувати пропускну здатність.	256

8.8 Налаштування IGMP Querier

8.8.1 Огляд

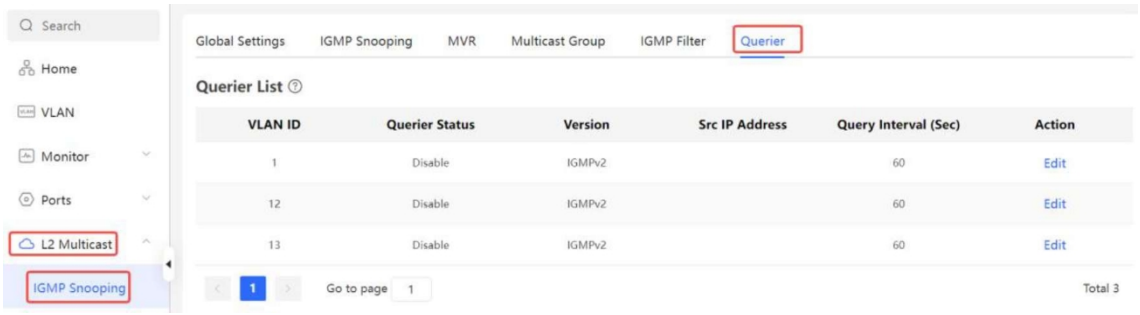
У трирівневій багатоадресній мережі багатоадресний пристрій 3-го рівня виконує роль запитувача і запускає IGMP для підтримки членства в групі. Пристроям багатоадресної розсилки 2-го рівня потрібно лише прослуховувати пакети IGMP, щоб створювати і підтримувати записи переадресації та реалізовувати багатоадресну розсилку 2-го рівня. Коли джерело багатоадресної розсилки і користувацький хост перебувають в одній мережі рівня 2, функція запиту недоступна оскільки пристрій рівня 2 не підтримує IGMP. Щоб вирішити цю проблему, ви можете налаштувати функцію IGMP snooping querier на пристрої 2 рівня так, щоб пристрій 2 рівня надсилав пакети IGMP Query на хост-комп'ютери користувачів від імені пристрою багатоадресної розсилки 3 рівня, а також прослуховував і підтримував пакети IGMP Report, отримані від хост-комп'ютерів користувачів, для створення записів переадресації багатоадресної розсилки 2 рівня.

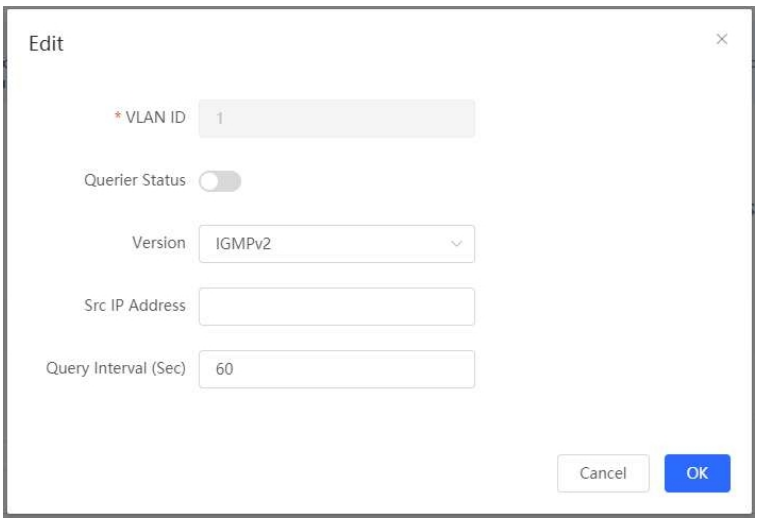
8.8.2 Процедура

Виберіть **Локальний пристрій**> **L2 Multicast**> **IGMP Snooping**> **Querier**.

Для кожної VLAN встановлюється один querier. Кількість запитувачів така сама, як і для VLAN пристроїв.

У **Списку запитувачів** натисніть кнопку **Змінити** в останньому стовпчику **Дія**. У діалоговому вікні, що з'явиться, виберіть, чи потрібно увімкнути запитувач, встановіть версію запитувача, IP-адресу джерела запитувача і інтервал запиту пакетів, а потім натисніть кнопку **OK**.





Таблиця 8-8 Опис параметрів конфігурації Querier

Параметр	Опис	Значення за замовчуванням
Статус запитувача	Увімкнути або вимкнути функцію запиту VLAN.	Вимкнути
Версія	Версія протоколу IGMP для пакетів запитів, що надсилаються . Може бути встановлений на IGMPv2 або IGMPv3.	IGMPv2
Src IP-адреса	IP-адреса джерела, що міститься в пакетах запитів, які надсилає запитувач.	NA
Інтервал запиту (сек)	Інтервал передачі пакетів, діапазон значень якого становить від 30 до 18000, в секундах.	60 секунд

Примітка

- Версія запитувача не може бути вищою за глобальну версію IGMP. Коли глобальна версія IGMP знижується, версія запитувача відповідно знижується.
- Якщо IP-адресу джерела запитувача не налаштовано, як IP-адресу джерела запитувача буде використано IP-адресу керування пристроєм.

9 Рівень 3 Багатоадресна передача

Застереження

Цей розділ стосується лише комутаторів серії NBS, які підтримують функції рівня 3. Вироби, які не підтримують функції рівня 3, такі як комутатори серії RG-NBS3100 і RG-NBS3200, не підтримують функції, згадані в цьому розділі.

9.1 Огляд

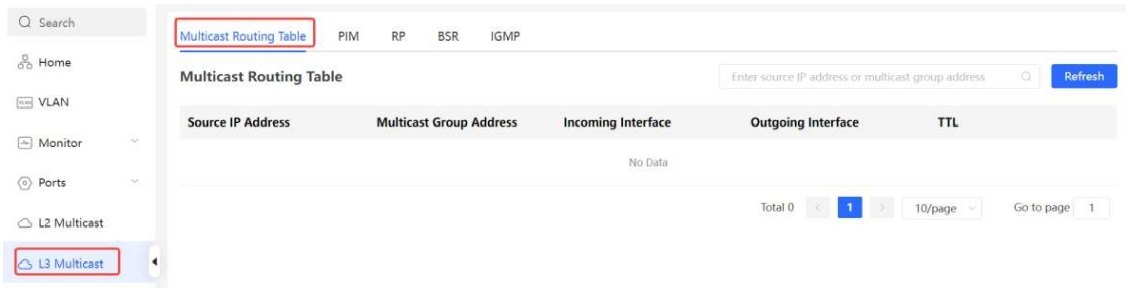
Багатоадресна розсилка 3-го рівня - це метод зв'язку, який використовує багатоадресну адресацію на мережевому рівні для надсилання даних. Багатоадресна розсилка дозволяє відправнику надсилати пакети групі одержувачів одночасно, що зменшує використання пропускної здатності мережі та знижує навантаження на мережу. Багатоадресна передача на рівні 3 широко використовується в таких додатках, як відеоконференції, потокове мультимедіа, VoIP та інших.

У багатоадресній передачі на рівні 3 кожна адреса групи багатоадресної розсилки відповідає певній групі багатоадресної розсилки, а члени групи багатоадресної розсилки мають одну й ту саму адресу групи багатоадресної розсилки. Відправник надсилає пакети даних на адресу групи багатоадресної розсилки, а маршрутизатори в мережі пересилають пакети всім членам групи багатоадресної розсилки основі адреси групи багатоадресної розсилки і використовуваних протоколів маршрутизації.

9.2 Таблиця багатоадресної маршрутизації

Виберіть **Локальний пристрій**> **L3 Багатоадресна розсилка**> **Таблиця багатоадресної розсилки**.

На сторінці **Multicast Routing Table** відображається інформація таблиці багатоадресної маршрутизації 3-го рівня зокрема IP-адреса джерела, адреса групи багатоадресної розсилки, вхідний інтерфейс, вихідний інтерфейс і час життя (TTL). Ви можете шукати інформацію про маршрутизацію за джерела або за адресою групи багатоадресної розсилки. Ви можете натиснути кнопку **Оновити**, щоб переглянути актуальну інформацію таблиці багатоадресної маршрутизації.



Таблиця 9-1 Опис параметрів таблиці багатоадресної маршрутизації

Параметр	Опис	Значення за замовчуванням
IP-адреса джерела	IP-адреса пристрою-джерела, що надсилає багатоадресний пакет.	Н/Д
Адреса групи багатоадресної розсилки	Спеціальна IP-адреса, яка ідентифікує групу багатоадресної розсилки. У таблиці маршрутизації адреса групи багатоадресної розсилки - це IP-адреса групи призначення.	Н/Д

Параметр	Опис	Значення за замовчуванням
Вхідний інтерфейс	Інтерфейс прийому багатоадресних пакетів	Н/Д
Вихідний інтерфейс	Коли маршрутизатор отримує багатоадресний пакет, він пересилає його на відповідний вихідний інтерфейс згідно значенням у полі **Вихідний інтерфейс** у таблиці маршрутизації.	Н/Д
TTL	Значення TTL - це час, протягом якого запис таблиці маршрутизації залишається дійсним. Після закінчення цього часу запис таблиці маршрутизації вважається вичерпаним і більше не використовується.	Н/Д

9.3 Налаштування PIM

Застереження

Поточний продукт ще не підтримує PIM-DM. PIM-SM підтримується виключно комутаторами серій RG-NBS7006, RG-NBS7003, RG-NBS6002, RG-NBS5300, RG-NBS5200, RG-NBS5100.

9.3.1 Огляд

Protocol Independent Multicast (PIM) - це незалежний від протоколу протокол внутрішньодоменної багатоадресної маршрутизації. PIM дозволяє реалізувати багатоадресний зв'язок з використанням різних одноадресних протоколів маршрутизації, включаючи статичну маршрутизацію, RIP, OSPF та інші. Завдяки реалізації протоколу PIM маршрутизатори можуть обмінюватися інформацією про багатоадресну маршрутизацію, що дозволяє створювати і підтримувати дерева багатоадресної розсилки, ефективно доставляючи пакети багатоадресних даних від джерела до одержувачів в межах групи багатоадресної розсилки.

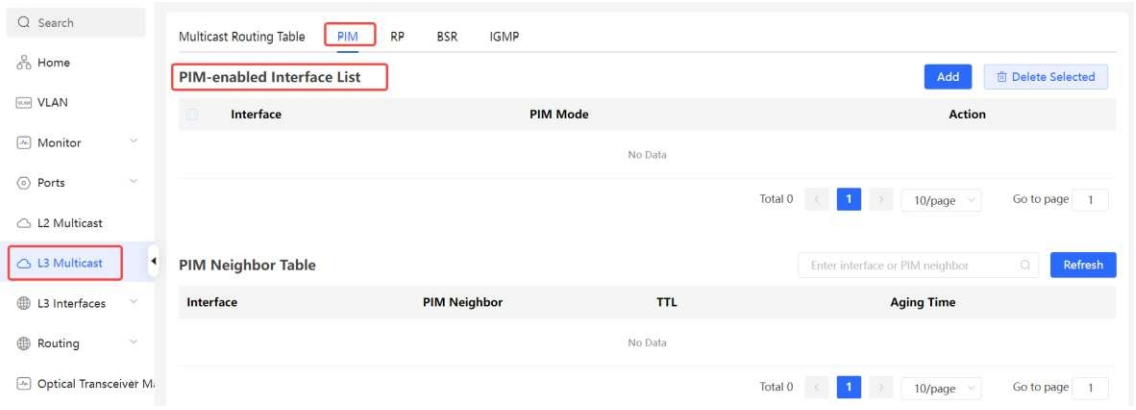
Протокол PIM має два широко використовувані режими:

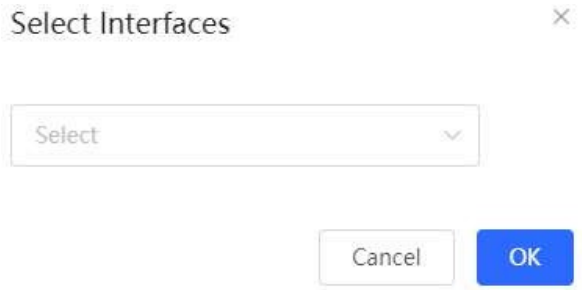
- Щільний режим PIM (PIM-DM)
  Цей режим застосовується для невеликих мереж або сценаріїв зі щільним багатоадресним трафіком. У режимі PIM-DM багатоадресні пакети передаються всіма доступними шляхами, що призводить до збільшення пропускної здатності мережі та споживання ресурсів.
- Розріджений режим PIM (PIM-SM)
  Цей режим застосовується у великомасштабних мережах або сценаріях з розрідженим багатоадресним трафіком. У режимі PIM-SM маршрутизатори пересилають багатоадресні пакети лише за потрібними маршрутами, ефективно зменшуючи використання пропускної здатності мережі.

9.3.2 Увімкнення PIM

Виберіть **Локальний пристрій**> **L3 Багатоадресна розсилка**> **PIM**> **Список інтерфейсів з підтримкою PIM**.

Натисніть кнопку **Додати**. З'явиться спливаюче вікно. У спливаючому вікні виберіть інтерфейс, на якому потрібно ввімкнути PIM, і натисніть **OK**. На вибраному інтерфейсі може бути реалізовано пересилання багатоадресних пакетів. За замовчуванням режим PMI - це PIM-SM.



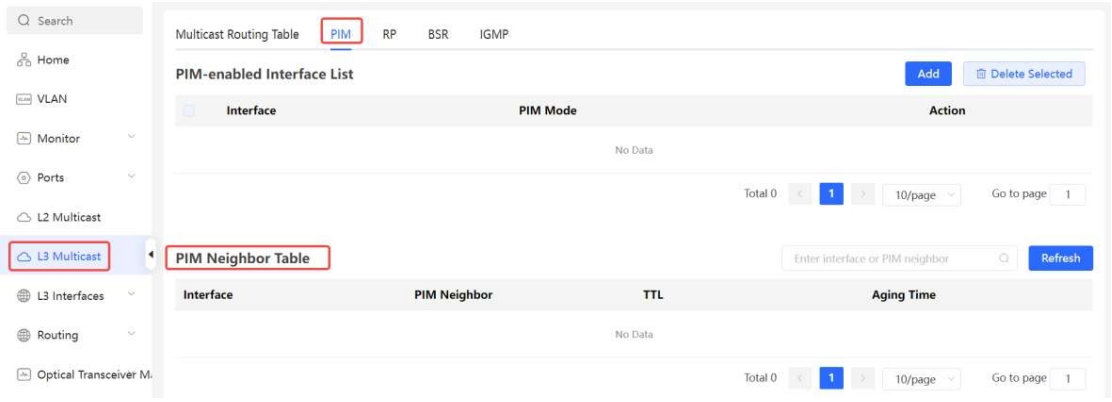


9.3.3 Перегляд таблиці сусідів PIM

У протоколі PIM маршрутизатори виявляють сусідні маршрутизатори і встановлюють відносини з ними за допомогою обміну повідомленнями Hello. Після встановлення відносин між двома маршрутизаторами з підтримкою PIM вони можуть обмінюватися інформацією про багатоадресну розсилку, включаючи членство в групах багатоадресної розсилки і стани переадресації багатоадресної розсилки. Постійно оновлюючи і підтримуючи таблицю сусідів PIM, маршрутизатори з підтримкою PIM можуть ефективно пересилати і обробляти багатоадресні пакети на основі інформації про сусідів, забезпечуючи таким чином ефективний багатоадресний зв'язок.

Виберіть **Локальний пристрій**> **L3 Багатоадресна розсилка**> **PIM**> **Таблиця сусідів PIM**.

На сторінці **Таблиця сусідів PIM** відображається інформація про сусідів PIM, така як інтерфейс, сусід PIM, TTL і час старіння. Ви можете шукати інформацію в таблиці сусідів PIM, ввівши інтерфейс або сусід PIM у вікні пошуку. Ви можете натиснути кнопку **Оновити**, щоб переглянути актуальну інформацію таблиці сусідів PIM.



Таблиця 9-2 Опис параметрів таблиці сусідів PIM

Параметр	Опис	Значення за замовчуванням
Інтерфейс	Інтерфейс, що з'єднує сусідній з локальним.	Н/Д
PIM Сусід	IP-адреса сусіднього роутера.	Н/Д
TTL	Значення TTL вказує на тривалість, протягом якої повідомлення Hello, надіслані сусідніми маршрутизаторами, залишаються дійсними. Якщо локальний маршрутизатор не отримає жодного нового повідомлення Hello від сусіда протягом часу TTL, він вважатиме сусідній маршрутизатор неактивним або таким, термін дії якого закінчився.	Н/Д
Час старіння	Якщо сусідній маршрутизатор стає неактивним або перестає надсилати повідомлення Hello, відповідний запис у таблиці сусідів PIM буде видалено після перевищення зазначеного часу старіння.	105 секунд.

9.4 Налаштування RP

9.4.1 Огляд

Точка зустрічі (RP) є ключовим поняттям у протоколі PIM. У багатоадресному зв'язку, коли відправник надсилає багатоадресний пакет даних, він повинен визначити певну точку як точку рандеву, з якої кілька одержувачів можуть отримати багатоадресний пакет. RP - це маршрутизатор точки зустрічі в дереві багатоадресної розсилки. RP може бути налаштована вручну або динамічно обрана за допомогою механізму BSR (Bootstrap Router).

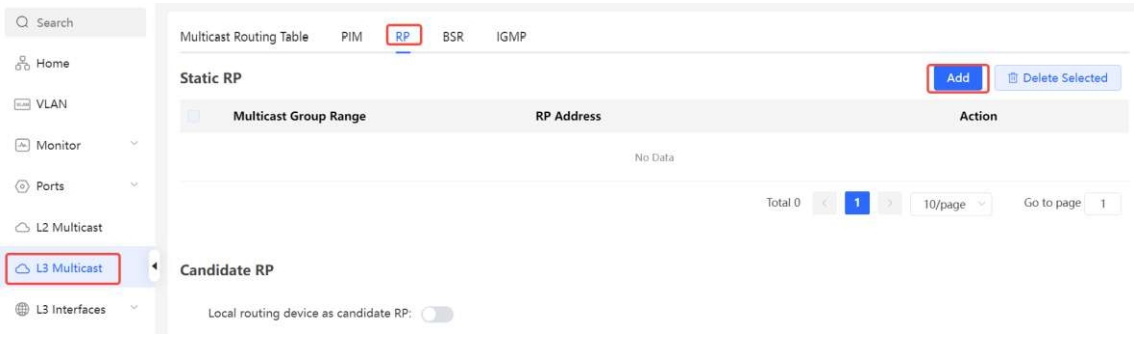
Примітка

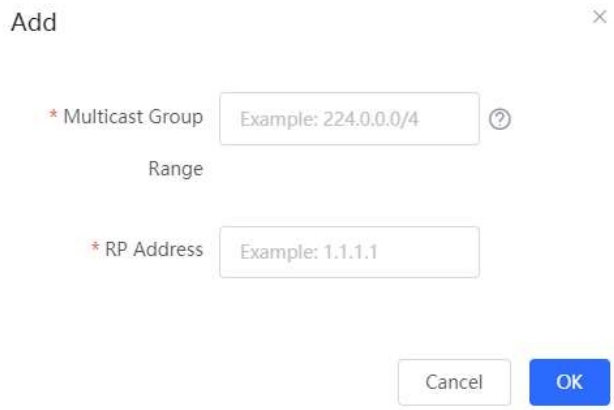
RP може надавати послуги для кількох або всіх груп багатоадресної розсилки. Однак лише один RP може одночасно пересилати трафік багатоадресної розсилки для групи багатоадресної розсилки.

9.4.2 Налаштування статичного RP

Виберіть **Локальний пристрій**> **L3 Багатоадресна розсилка**> **RP**> **Статичний RP**.

Натисніть **Додати**. У спливаючому вікні, що з'явиться, введіть діапазон груп багатоадресної , який охоплює RP, і адресу RP, а потім натисніть **OK**.



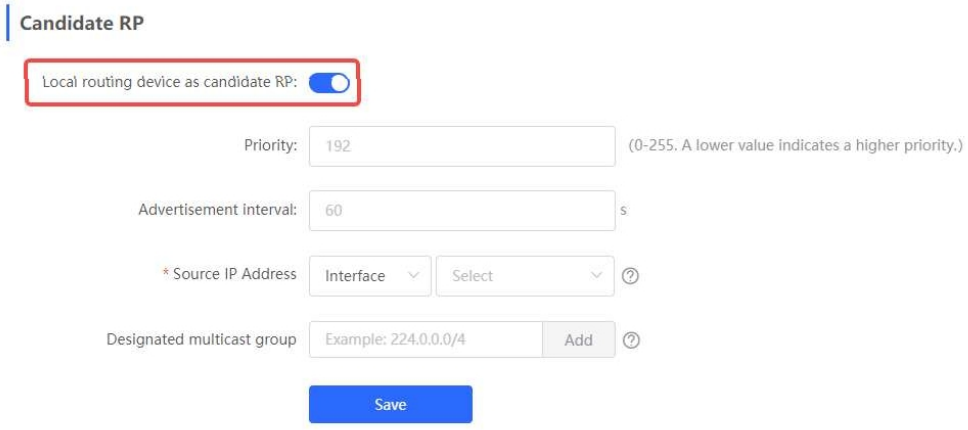


9.4.3 Конфігурація кандидата на РП

У мережі PIM кандидат на роль опорного пристрою - це маршрутизатор, який має право стати опорним пристроєм. Ви можете налаштувати кілька маршрутизаторів з підтримкою PIM у домені PIM як кандидатів на роль RP, щоб врешті-решт було обрано відповідний RP. Цей процес має на меті підвищити ефективність і надійність багатоадресного зв'язку.

Виберіть **локальний пристрій**> **L3 Multicast**> **RP**> **Candidate RP**.

Увімкніть **Локальний пристрій маршрутизації як кандидат на роль RP:** щоб призначити локальний пристрій кандидатом на роль RP. Введіть пріоритет, інтервал реклами, IP-адресу джерела і призначену групу багатоадресної розсилки. Потім натисніть кнопку **Зберегти**.



Таблиця 9-3 Опис параметрів конфігурації РП-кандидата

Параметр	Опис	Значення за замовчуванням
Пріоритет	Пріоритет визначає, хто з кандидатів стане РП під час виборчого процесу. Значення пріоритету варіюється від 0 до 255, де менше значення означає вищий пріоритет. Кандидат РП з вищим пріоритетом має більше шансів бути обраним РП.	192

Параметр	Опис	Значення за замовчуванням
Інтервал реклами	Кандидат РП оголошує про свою присутність і доступність, надсилаючи PIM-повідомлення. Інтервал оголошення визначає частоту, з якою кандидат на роль маршрутизатора надсилає ці повідомлення. Коротший інтервал оголошення може швидше сповістити інші маршрутизатори про присутність кандидата на роль RP, але це також навантаження на мережу.	60 секунд
IP-адреса джерела	IP-адреса джерела PIM-повідомлень, що надсилаються кандидатом у РП, яка може бути як інтерфейсом, так і IP-адресою.	Н/Д
Призначена група багатоадресної розсилки	PIM-повідомлення, які надсилає RP-кандидат, повинні містити адресу групи багатоадресної розсилки, що лежить у діапазоні від 224.0.0.0.0/4 до 239.255.255.255/32. Зазвичай кандидати на роль RP надсилають кілька повідомлень, кожне з яких містить різні адреси груп багатоадресної розсилки, щоб повідомити інші маршрутизатори про те що вони можуть стати RP для цих груп багатоадресної розсилки. Ви можете натиснути кнопку **Додати**, щоб налаштувати кілька адрес груп багатоадресної розсилки.	Н/Д

9.5 Налаштування BSR

9.5.1 Огляд

У режимі PIM-SM RP потрібно налаштовувати вручну, що є нудним завданням для великих мереж. Механізм BSR (Bootstrap Routerможе автоматично вибирати RP, процес конфігурації RP. BSR слугує ядром управління доменом PIM-SM, відповідальним за збір та розміщення інформації про RP в межах домену. BSR обирається кандидатами BSR.

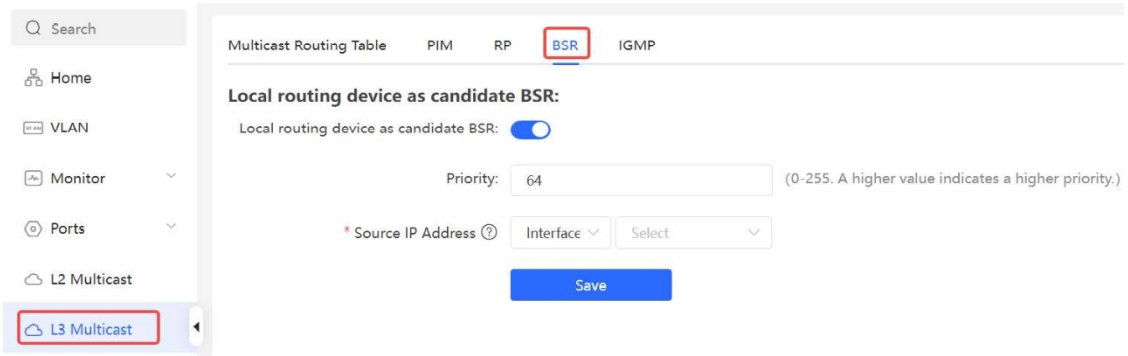
Примітка

Домен PIM-SM може мати лише один BSR, але може мати декілька кандидатів на роль BSR.

9.5.2 Налаштування BSR

Виберіть **Локальний пристрій**> **L3 Multicast**> **BSR**> **Локальний пристрій маршрутизації як кандидат BSR**.

Увімкніть **Локальний пристрій маршрутизації як кандидат** на роль **BSR:** щоб призначити локальний пристрій кандидатом на роль BSR. Введіть пріоритет і IP-адресу джерела. Потім натисніть кнопку **Зберегти**.



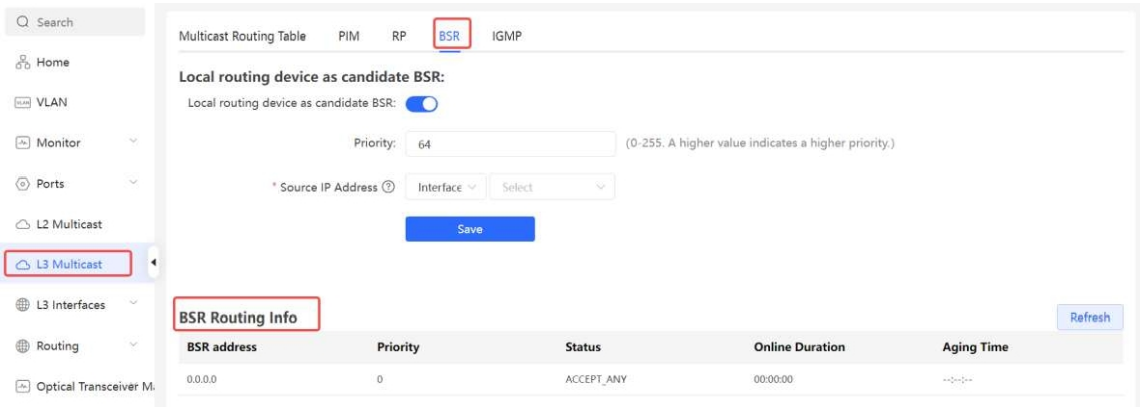
Таблиця 9-4 Опис параметрів конфігурації BSR кандидата

Параметр	Опис	Значення за замовчуванням
Пріоритет	Кандидати з вищим пріоритетом мають більше шансів бути обраними на посаду . Значення пріоритету варіюється від 0 до 255, де менше значення означає вищий пріоритет.	192
IP-адреса джерела	IP-адреса джерела PIM-повідомлень, що надсилаються кандидатом BSR, яка може бути як інтерфейсом, так і IP-адресою.	Н/Д

9.5.3 Перегляд інформації про маршрути BSR

Виберіть **Локальний пристрій> L3 Багатоадресна розсилка> BSR> Інформація про маршрутизацію BSR**.

На сторінці Інформація про маршрутизацію BSR відображається інформація про маршрутизацію BSR, зокрема адреса BSR, пріоритет, статус, тривалість роботи в мережі та час старіння. Ви можете натиснути кнопку **Оновити**, щоб переглянути актуальну інформацію про маршрутизацію BSR.



9.6 Налаштування IGMP

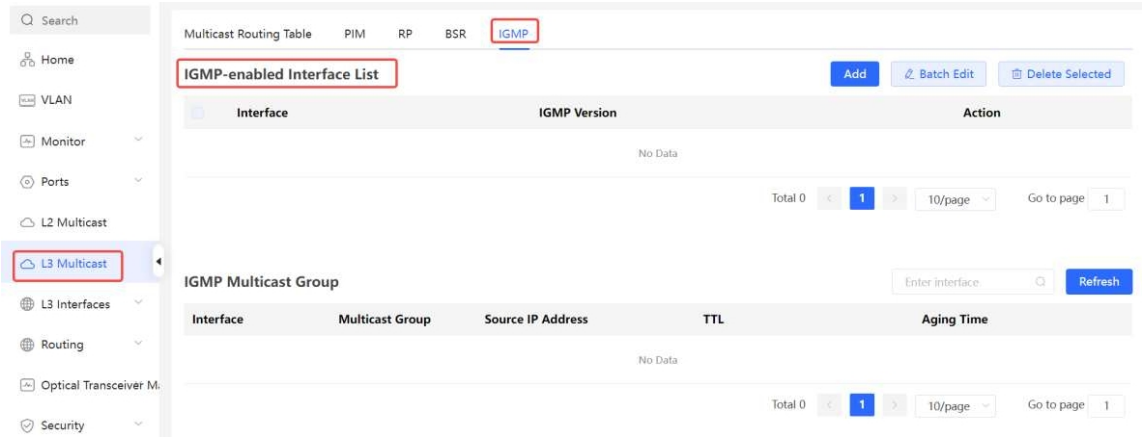
9.6.1 Огляд

Протокол керування групами в Інтернеті (IGMP) використовується для забезпечення багатоадресного зв'язку в мережах IPv4. IGMP відповідає за керування членством у групах багатоадресної розсилки і полегшує зв'язок між хостами і багатоадресними маршрутизаторами. За допомогою IGMP хости можуть приєднуватися до певної групи багатоадресної розсилки або виходити з неї, а також повідомляти про своє членство в ній маршрутизаторам багатоадресної розсилки. Багатоадресні маршрутизатори використовують IGMP для визначення того, які хости є членами багатоадресної групи, що дозволяє ефективно переадресовувати багатоадресний трафік.

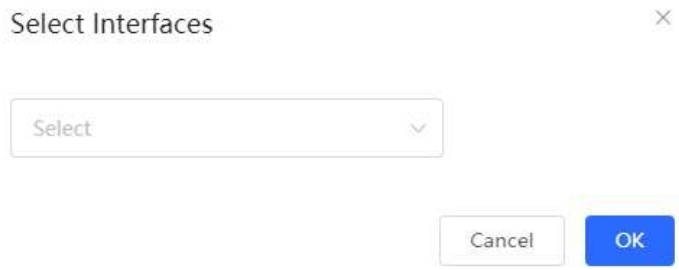
9.6.2 Увімкнення IGMP

Виберіть **Локальний пристрій> L3 Багатоадресна розсилка> IGMP> Список інтерфейсів з підтримкою IGMP**.

Сторінка **Список інтерфейсів з підтримкою IGMP** відображає основну інформацію про інтерфейси з підтримкою IGMP, включаючи інтерфейс і версію IGMP.



Додати: Натисніть кнопку **Додати**. З'явиться спливне вікно **Вибір інтерфейсів**. У спливаючому вікні виберіть інтерфейс, на якому буде ввімкнено IGMP. Натисніть **кнопку OK**. IGMP буде ввімкнено на відповідній VLAN.



Пакетне редагування: Виберіть інтерфейси і натисніть **Пакетне редагування**. У спливаючому вікні виберіть версію IGMP і натисніть **OK**.

IGMPv3 має покращену функціональність і гнучкість порівняно з IGMPv2. Він підтримує більше функцій управління групами багатоадресної розсилки, забезпечує більш точний контроль над членством і методами запитів, а також впроваджує механізми безпеки. Завдяки цим вдосконаленням IGMPv3 можна застосовувати в сценаріях, які вимагають більш високого рівня управління багатоадресною розсилкою і безпеки.

Пакетне видалення: Виберіть інтерфейси і натисніть **Пакетне видалення**. IGMP буде вимкнено на вибраних інтерфейсах.

9.6.3 Перегляд групи багатоадресної розсилки IGMP

Виберіть **Локальний пристрій**> **L3 Багатоадресна розсилка**> **IGMP**> **Група багатоадресної розсилки IGMP**.

На сторінці Групи **багатоадресної розсилки IGMP** відображається інформація про групи багатоадресної розсилки IGMP, зокрема кількість груп багатоадресної розсилки, IP-адреси джерел, час очікування TTL і час старіння. Ви можете розгорнути групу багатоадресної розсилки, щоб переглянути докладні IP-адреси, пов'язані з групою багатоадресної розсилки на цьому інтерфейсі.

Ви можете шукати інформацію про групу багатоадресної розсилки IGMP, ввівши інтерфейс у пошуку. Ви можете натиснути **Оновіть**, щоб переглянути актуальну інформацію про групу багатоадресної розсилки IGMP.

10 Управління на рівні 3

Застереження

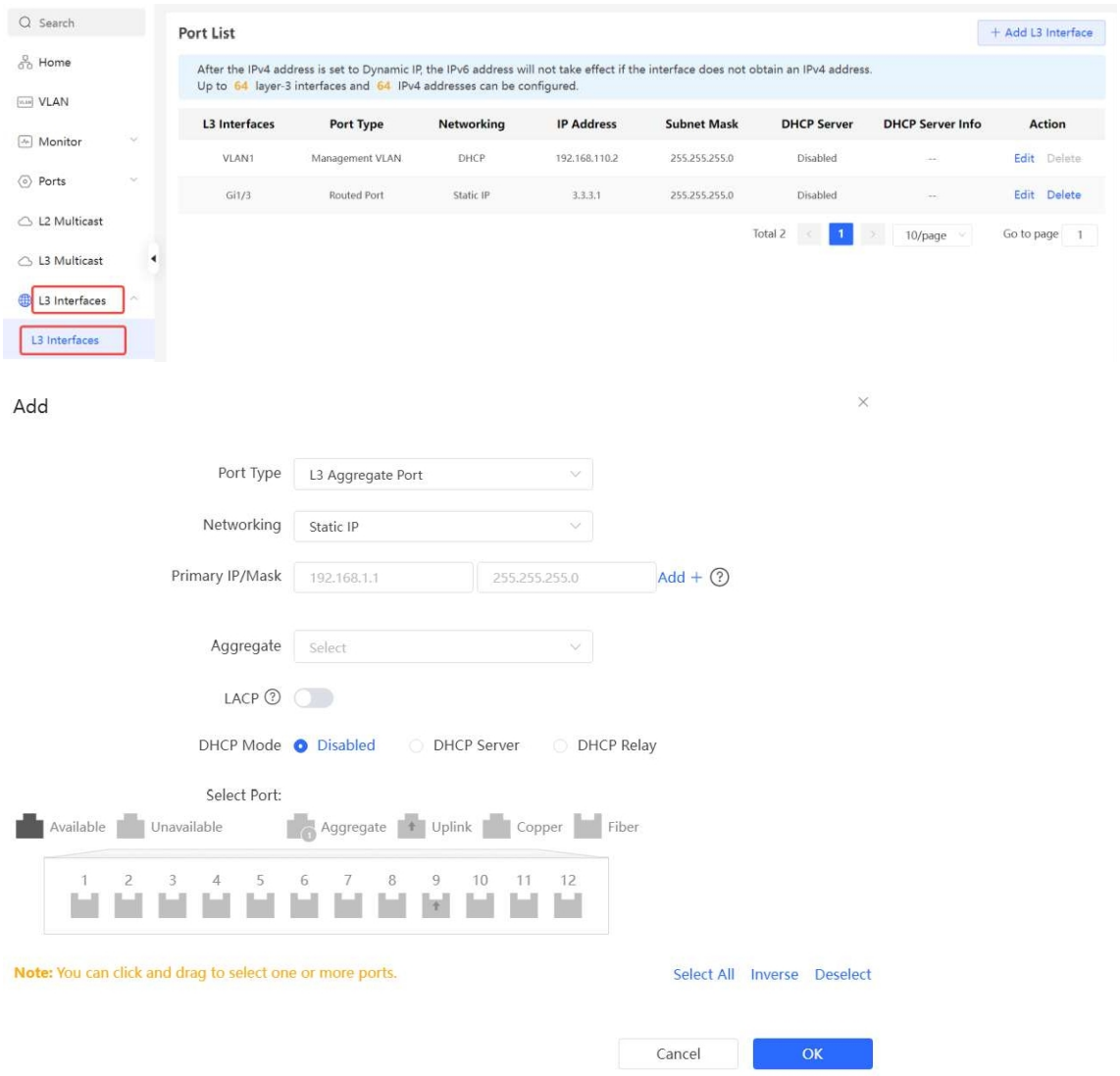
Цей розділ стосується лише комутаторів серії NBS, які підтримують функції рівня 3. Вироби, які не підтримують функції рівня 3, такі як комутатори серії RG-NBS3100 і RG-NBS3200, не підтримують функції, згадані в цьому розділі.

10.1 Налаштування інтерфейсу 3-го рівня

Виберіть **Локальний пристрій**> **Інтерфейси L3**> **Інтерфейси L3**.

Список портів відображає різні типи інтерфейсів 3-го рівня на пристрої, зокрема SVI, маршрутизовані порти та агреговані інтерфейси 3-го рівня.

Натисніть **Додати інтерфейси L3**, щоб створити новий інтерфейс третього рівня.



Таблиця 10-1 Опис параметрів конфігурації інтерфейсів рівня 3

Параметр	Опис
Тип порту	Тип створеного інтерфейсу 3-го рівня. Це може бути SVI, маршрутизований порт або агрегований інтерфейс рівня 3. Докладнішу інформацію наведено у Таблиці 7-1.
Нетворкінг	Вказує DHCP або статичний режим для порту для отримання IP-адреси.
VLAN	Вказує VLAN, до якої належить SVI.
IP/Маска	Якщо для параметра **Мережа** встановлено значення **Статичний IP**, вам потрібно вручну ввести IP-адресу та маску підмережі.
Виберіть порт	Виберіть порт пристрою, який потрібно налаштувати.
Агрегат	Вказує ідентифікатор агрегованого інтерфейсу, наприклад, Ag1, коли створюється агрегований інтерфейс 3-го рівня.
LACP	Після ввімкнення LACP на агрегованому інтерфейсі 3-го рівня можна динамічно агрегувати та дезагрегувати канали. Підтримка версій Тільки ReyeeOS 2.320 або новіші версії підтримують увімкнення LACP на агрегованому інтерфейсі рівня 3. **Примітка** Якщо комутатор працює під управлінням ReyeeOS 2.320 або новішої версії, вимкніть LACP на агрегованому інтерфейсі рівня 3, перш ніж оновлювати версію програмного забезпечення. Інакше може виникнути несумісність версій.
Режим DHCP	Виберіть, чи потрібно вмикати службу DHCP на інтерфейсі 3-го рівня. **Вимкнено**: Вказує на те, що службу DHCP вимкнено. Клієнтам, підключеним до інтерфейсу, не може бути призначено жодної IP-адреси. **Сервер DHCP**: Вказує на те, що пристрій функціонує як сервер DHCP для призначення IP-адрес низхідним пристроям, підключеним до інтерфейсу. Вам потрібно встановити початкову IP-адресу пулу адрес, кількість IP-адрес, які можна призначити, та оренду адрес; для отримання додаткової інформації див. розділ 10.2. Налаштування IPv6-адреси для інтерфейсу 3-го рівня. **DHCP-ретранслятор**: Вказує на те, що пристрій виконує функції DHCP-ретранслятора, отримує IP-адреси від зовнішнього сервера та призначає IP-адреси нижчестоящим пристроям. Необхідно налаштувати IP-адресу інтерфейсу та IP-адресу DHCP-сервера. IP-адреса інтерфейсу повинна знаходитися в тому ж сегменті мережі, що і пул адрес сервера DHCP.
Виключена IP-адреса (діапазон)	Коли пристрій працює як DHCP-сервер, встановіть IP-адресу в пулі адрес, яка не використовується для призначення

Примітка

- VLAN 1 - це SVI пристрою за замовчуванням. Її не можна ні змінити, ні видалити.
- Керуюча VLAN лише відображається на сторінці **L3 Interfaces**, але не може бути змінена. Щоб змінити її, виберіть **Порти**> **MGMT IP**. Для отримання додаткової інформації див. розділ 7.6 Налаштування MGMT IP.
- Функції DHCP-ретранслятора і DHCP-сервера інтерфейсу рівня є взаємовиключними і не можуть бути налаштовані одночасно.
- Порти-члени інтерфейсу 3-го рівня повинні бути маршрутизованими портами.
- Якщо для IPv4-адреси встановлено DHCP і інтерфейсу не вдається отримати , IPv6-адреса також не набуде чинності.

10.2 Налаштування IPv6-адреси для інтерфейсу 3-го рівня

IPv6 - це набір стандартних протоколів для мережевого рівня Інтернету. IPv6 вирішує наступні проблеми IPv4:

- Виснаження адреси:

  Для перетворення декількох приватних мережевих адрес у загальнодоступну мережеву адресу на шлюзі необхідно ввімкнути NAT. Це призводить до додаткової затримки, спричиненої перетворенням адрес, і може перервати з'єднання між пристроями всередині і зовні шлюзу. Крім того, потрібно додати мапування, щоб забезпечити доступ до пристроїв інтрамережі з Інтернету.

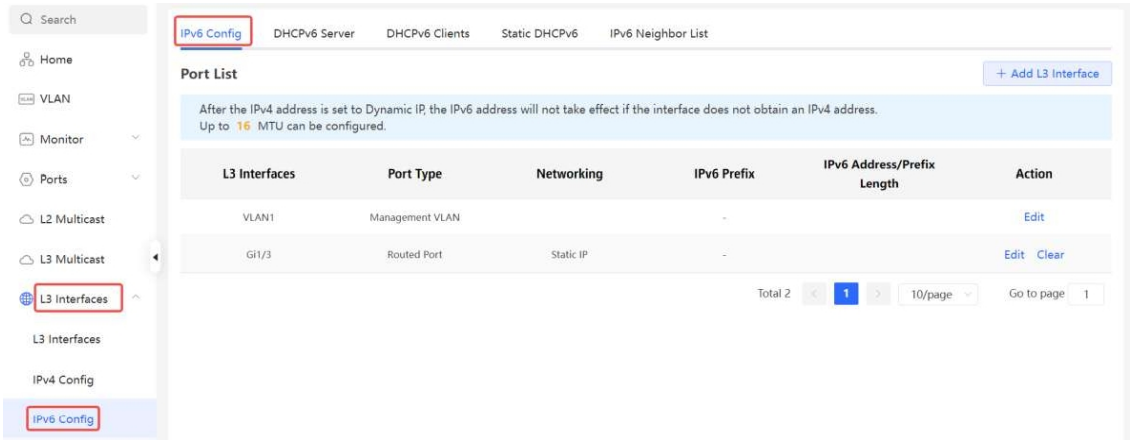
- Дефект конструкції:

  IP-адреси не можуть бути сформовані за допомогою відображення топології мережі, для цього потрібна масштабна таблиця маршрутизації.

- Відсутність вбудованої автентифікації та конфіденційності:

  IPv4 сам по собі не вимагає шифрування. Після трансляції адреси важко відстежити джерело. Оскільки кількість адрес в сегменті мережі обмежена, зловмисникам легко сканувати всі хости в локальній мережі. IPv6 інтегрує IPsec за замовчуванням. Наскрізні з'єднання можуть бути встановлені без трансляції адрес, і легко відстежити джерело. IPv6 має величезний адресний простір. 64-розрядна префіксна адреса підтримує 64 біти хоста, що збільшує складність і вартість сканування, а отже, запобігає атакам.

Виберіть **Local Device**> **L3 Interfaces**> **IPv6 Config**.

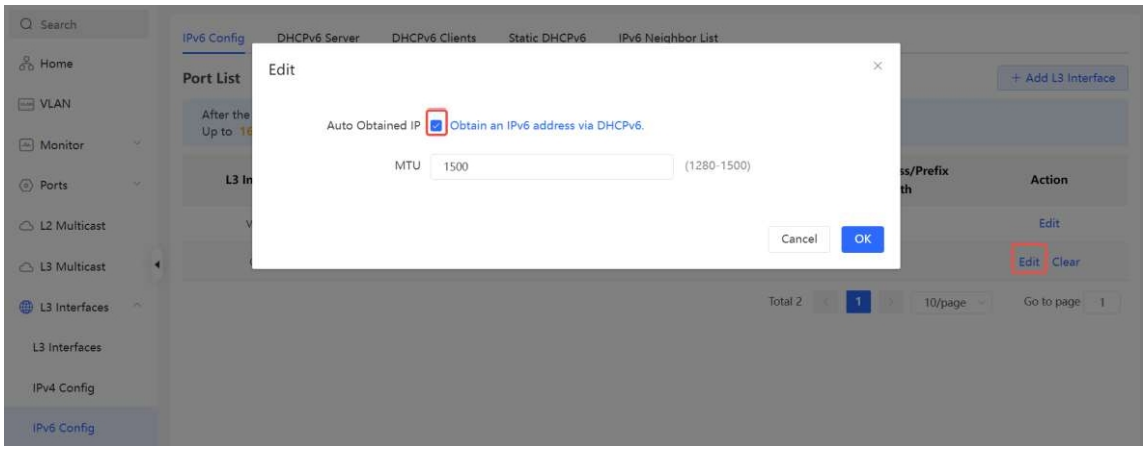


Застереження

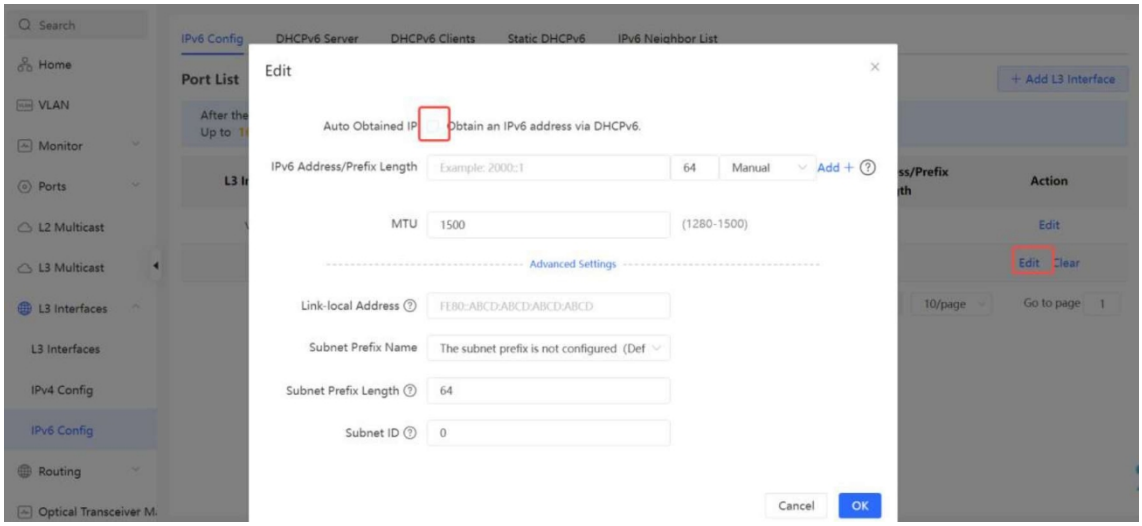
- Спочатку додайте інтерфейс IPv4 3-го рівня. Потім виберіть інтерфейс на сторінці конфігурації інтерфейсу IPv6 3-го рівня і натисніть кнопку **Змінити**.

- Якщо для IPv4-адреси інтерфейсу встановлено **DHCP** і не отримано жодної IPv4-адреси, IPv6-адреса цього інтерфейсу не набуде чинності.

- Якщо доступний висхідний сервер DHCPv6, виберіть **Автоматично отриманий IP** і вкажіть MTU. За замовчуванням MTU дорівнює **1500**. Рекомендується залишити значення за замовчуванням. Потім натисніть кнопку **OK**.



- Якщо сервер DHCPv6 недоступний для призначення IP-адреси, налаштуйте інформацію про IPv6 наступним чином:



Таблиця 10-2 Параметри конфігурації адреси IPv6 інтерфейсу рівня 3

Параметр	Опис
Отримання IPv6-адреси через DHCPv6	Якщо висхідний сервер DHCPv6 недоступний, не вибирайте **Автоматично отримувати IP-адресу**. Замість цього додайте адресу IPv6 вручну.
Адреса/префікс IPv6 Довжина	Налаштуйте IPv6-адресу та довжину префікса. Ви можете натиснути **Додати**, щоб додати кілька IPv6-адреси. Якщо первинна IP-адреса порожня, налаштована вторинна IP-адреса буде недійсним.

Параметр	Опис
	Для ручної конфігурації довжина префікса становить від 1 до 128. Для автоматичного налаштування довжина префікса становить від 1 до 64. Якщо довжина префікса IPv6 інтерфейсу 3-го рівня становить від 48 до 64, цю адресу можна призначити.
MTU	Налаштуйте MTU. За замовчуванням MTU дорівнює **1500**.
Додаткові налаштування	Натисніть **Додаткові налаштування**, щоб налаштувати локальну адресу посилання, ім'я префікса підмережі, довжину префікса підмережі та ідентифікатор підмережі.
Посилання-локальна адреса	Локальна адреса посилання використовується для нумерації хостів в одному мережевому каналі. Перші 10 біт адреси посилання у двійковій системі числення мають бути '1111111010'.
Ім'я префікса підмережі	Він ідентифікує вказане посилання (підмережу).
Довжина префікса підмережі	Вказує на довжину (в бітах) префікса підмережі в адресі. Значення знаходиться в діапазоні від 48 до 64 (довжина префікса підмережі повинна бути більшою за довжину префікса, призначеного сервером).
Ідентифікатор підмережі	Налаштуйте ідентифікатор підмережі інтерфейсу в шістнадцятковій системі числення. доступних ідентифікаторів підмережі дорівнює (2^N - 1), де **N** дорівнює (довжина префікса підмережі інтерфейсу - довжина префікса, призначеного сервером).

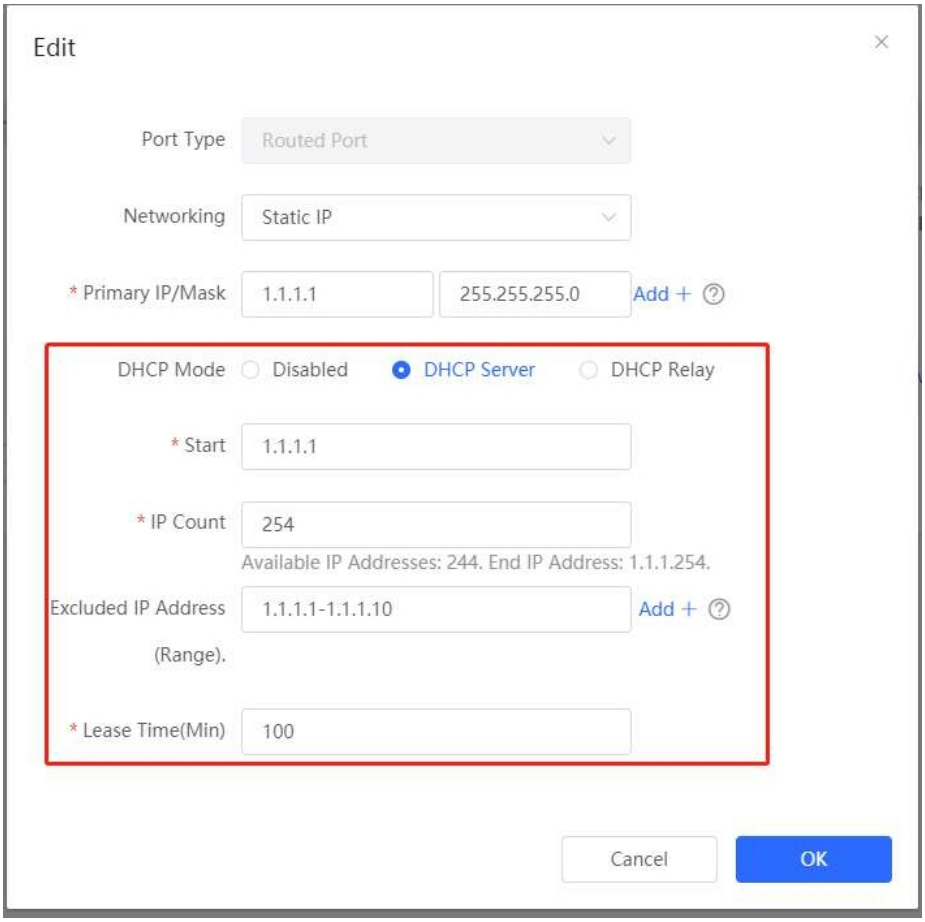
10.3 Налаштування служби DHCP

Після ввімкнення функції DHCP-сервера на інтерфейсі 3-го рівня пристрій може призначати IP-адреси низхідним пристроям, підключеним до порту.

10.3.1 Увімкнути служби DHCP

Виберіть **Локальний пристрій**> **Інтерфейси L3**> **Інтерфейси L3**.

Натисніть **Редагувати** на вказаному порту або **Додати інтерфейс L3**, щоб додати інтерфейс рівня 3, виберіть режим DHCP для локального розподілу і введіть початкову IP-адресу пулу адрес, кількість виділених IP-адрес, діапазон виключених IP-адрес і час оренди адреси.



Таблиця 10-3 Опис параметрів конфігурації сервера DHCP

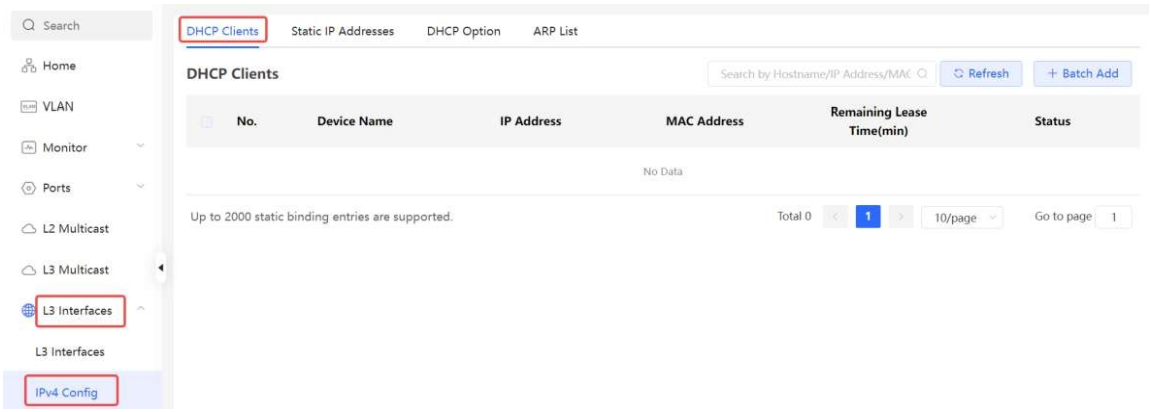
Параметр	Опис
Режим DHCP	Щоб вибрати DHCP-сервер
Старт	Сервер DHCP автоматично призначає початкову IP-адресу, яка є початковою IP-адресою пулу адрес DHCP. Клієнт отримує з пулу адрес. Якщо всі адреси в адресному пулі вичерпано, з нього не можна отримати жодної IP-адреси.
Кількість IP-адрес	Кількість IP-адрес в пулі адрес
Виключена IP-адреса (діапазон)	IP-адреси в пулі адрес, які не використовуються для розподілу, підтримують введення однієї IP-адреси або сегмента IP-мережі, а також додавання до 20 адресних сегментів.
Час оренди (хв)	Час оренди адреси, в хвилинах. **Час оренди (хв)**: Коли підключається клієнт низхідної лінії зв'язку, орендована IP-адреса автоматично поновлюється. Якщо орендована IP-адреса не поновлюється через відключення клієнта або нестабільність мережі, IP-адреса буде повернута після закінчення терміну оренди. Після відновлення клієнтського з'єднання клієнт може знову IP-адресу

10.3.2 Перегляд клієнта DHCP

Виберіть **Локальний пристрій**> **Інтерфейси L3**> **Клієнти DHCP**.

Перегляньте адреси, автоматично призначені клієнтам низхідної лінії зв'язку після того, як інтерфейси 3-го рівня увімкнули служби DHCP. Ви можете знайти інформацію про клієнта на основі MAC-адреси, IP-адреси або імені користувача.

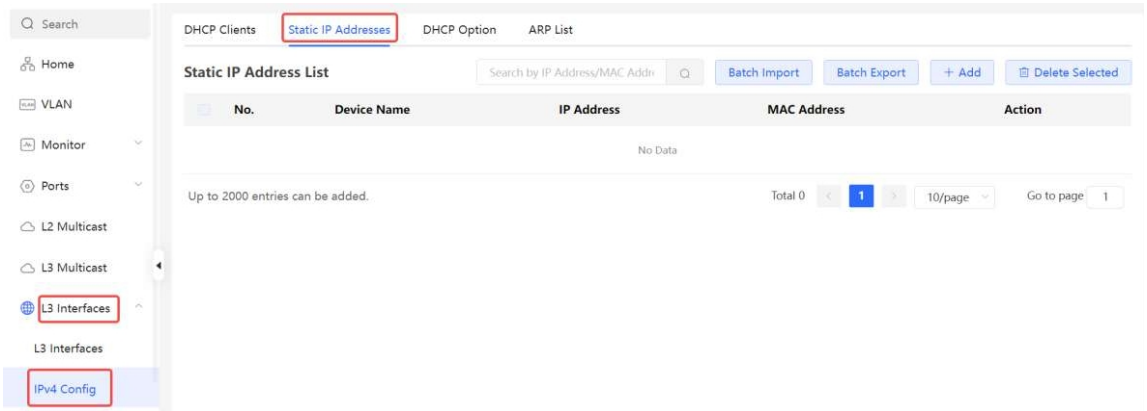
Знайдіть цільового клієнта і натисніть **Перетворити на статичну IP-адресу** в колонці **Статус** або виберіть потрібних клієнтів і натисніть **Пакетне перетворення**. Зв'язок динамічного розподілу адрес додається до списку статичного розподілу адрес, щоб хост міг отримати прив'язану IP-адресу для кожного з'єднання. Докладні відомості про те, як переглянути список статичних адрес, див. у розділі 10.3.3 Налаштування розподілу статичних IP-адрес.



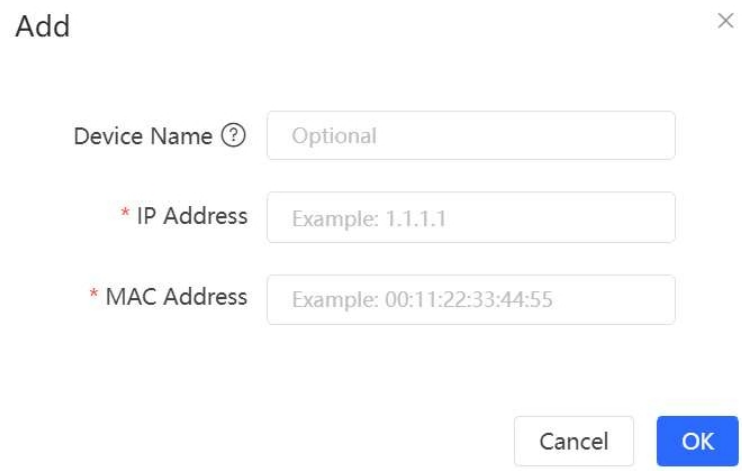
10.3.3 Налаштування розподілу статичних IP-адрес

Виберіть **Локальний пристрій**> **Інтерфейси L3**> **Статичні IP-адреси**.

Відображає записи клієнтів, перетворені на статичні адреси у списку клієнтів а також записи статичних адрес, додані вручну. Верхнє праве поле пошуку підтримує пошук відповідних записів на основі призначеної IP-адреси або MAC-адреси пристрою



Натисніть **Додати**. У діалоговому вікні Прив'язка статичної IP-адреси введіть MAC-адресу та IP-адресу клієнта, який потрібно прив'язати, і натисніть кнопку **ОК**. Після прив'язки статичної IP-адреси прив'язана IP-адреса буде отримуватися щоразу, коли відповідний клієнт низхідної лінії зв'язку підключатиметься до мережі.

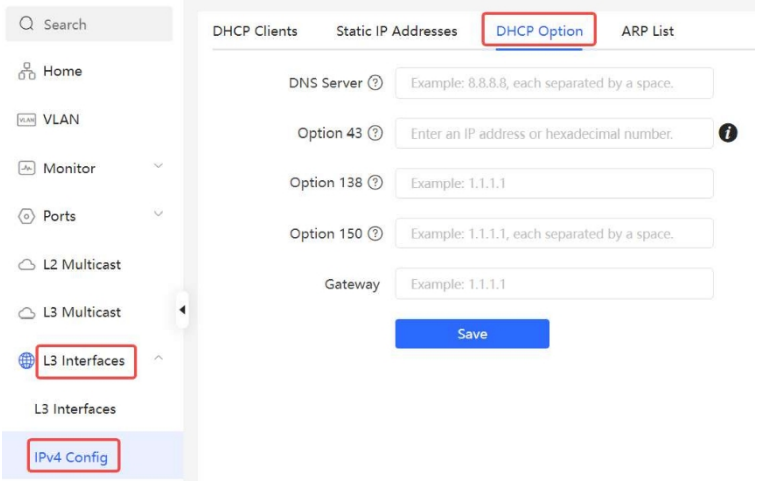


Щоб видалити статичну адресу, виберіть статичний запис, який потрібно видалити, у **Списку статичних IP-адрес** і натисніть **Видалити вибране**; або натисніть **Видалити** в останньому стовпчику **Дія** відповідного запису.

10.3.4 Налаштування параметрів DHCP-сервера

Виберіть **Локальний пристрій**> **Інтерфейси L3**> **Параметр DHCP**.

Конфігурація, що передається на низхідні пристрої, є необов'язковою і набуває чинності в глобальному масштабі, коли інтерфейс 3-го рівня виконує функції DHCP-сервера.



Таблиця 10-4 Опис параметрів DHCP-сервера Параметри конфігурації

Параметр	Опис
DNS-сервер	Адреса DNS-сервера, надана провайдером. Можна ввести кілька IP-адрес, розділених пробілами.
Варіант 43	Якщо контролер бездротового доступу і точка доступу не перебувають в одній локальній мережі, доступу не може виявити контролер бездротового доступу через широкомовну передачу після отримання IP-адреси від сервера DHCP. Щоб дозволити точці доступу виявити точку доступу, потрібно налаштувати параметр 43, який міститься у пакеті відповіді DHCP на сервері DHCP.

Параметр	Опис
Варіант 138	Введіть IP-адресу кондиціонера. Подібно до параметра 43, якщо кондиціонер і точка доступу не належать до однієї локальної мережі, ви можете налаштувати параметр 138, щоб увімкнути отримання точкою доступу IPv4-адреси кондиціонера.
Варіант 150	Введіть IP-адресу сервера TFTP. Введіть IP-адресу сервера TFTP, щоб вказати адресу сервера TFTP, призначену клієнту. Можна ввести кілька IP-адрес, розділяючи їх пробілами.

Примітка

Параметри DHCP є додатковою конфігурацією, коли пристрій функціонує як DHCP-сервер 3-го рівня. Ця конфігурація набуває чинності в глобальному масштабі і не потребує налаштування за замовчуванням. Якщо адресу DNS-сервера не вказано, за замовчуванням IP-адреса DNS, призначена низхідному порту, є IP-адресою шлюзу.

10.4 Налаштування сервера DHCPv6

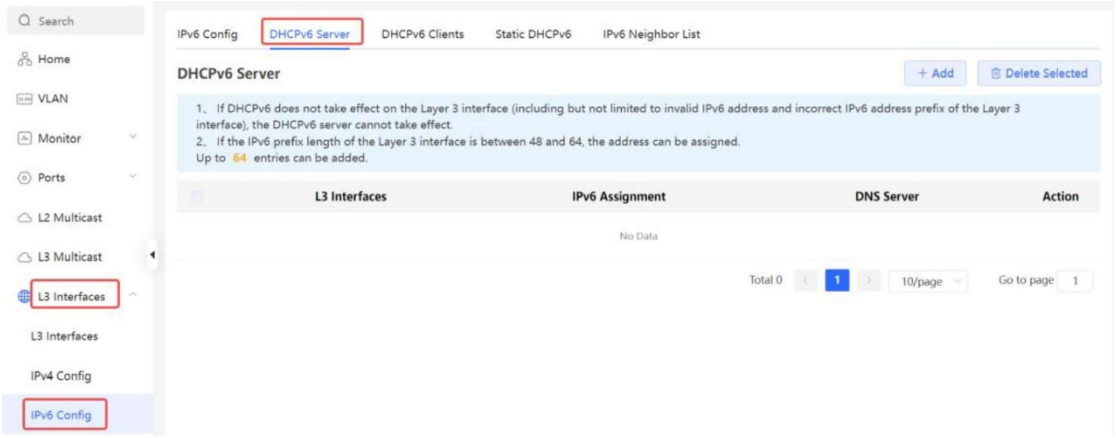
Протокол динамічної конфігурації хоста для IPv6 (DHCPv6) - це протокол, який дозволяє DHCP-серверу передавати інформацію про конфігурацію (наприклад, мережеву адресу IPv6) вузлам IPv6.

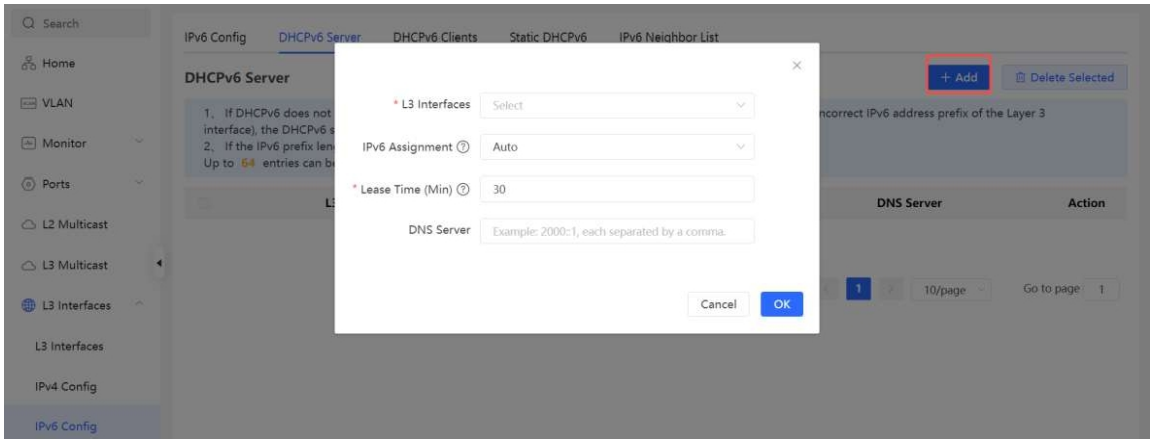
У порівнянні з іншими методами призначення адрес IPv6 (такими як ручне налаштування і автоконфігурація адрес без стану), DHCPv6 надає функції призначення адрес, делегування префіксів (PD) і призначення параметрів конфігурації.

- DHCPv6 - це одночасно протокол автоконфігурації адрес зі станом і протокол конфігурації адрес без стану. Він підтримує гнучке додавання і повторне використання мережевих адрес, а також може записувати призначені адреси, покращуючи таким чином керування мережею.
- Функція призначення параметрів конфігурації DHCPv6 може вирішити проблему, пов'язану з неможливістю отримання параметрів за протоколом автоконфігурації адрес без статусу, і надати хосту інформацію про конфігурацію, наприклад, адресу DNS-сервера і доменне ім'я.

Виберіть **Local Device**> **L3 Interfaces**> **IPv6 Config**.

(1) Натисніть **Додати**, виберіть інтерфейс 3-го рівня та метод призначення IP-адреси, введіть термін оренди адреси та адресу DNS-сервера. За замовчуванням термін оренди адреси становить 30 хвилин. Рекомендується залишити значення за замовчуванням. Потім натисніть кнопку **OK**.





Таблиця 10-5 Параметри конфігурації адреси IPv6 інтерфейсу рівня 3

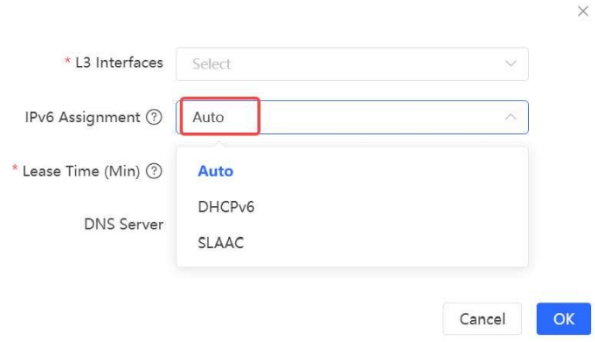
Параметр	Опис
L3 Інтерфейси	Виберіть інтерфейс 3-го рівня, для якого потрібно додати сервер DHCPv6.
Присвоєння IPv6	Якщо для цього параметра встановлено значення **Авто**, для призначення IPv6-адрес використовуються як DHCPv6, так і SLAAC.
Час оренди	Значення за замовчуванням - **30** хвилин. Значення варіюється від 30 до 2880 хвилин. Коли пристрій залишається онлайн і мережа нормальна, цей параметр періодично оновлюється (скидається до 0).
DNS-сервер	Введіть адресу DNS-сервера.

10.4.1 Перегляд клієнтів DHCPv6

інформацію про клієнта, який отримує IPv6-адресу від пристрою, зокрема ім'я хоста, IPv6-адресу, термін оренди, що залишився, унікальний ідентифікатор DHCPv6 (DUID) і стан. **+Bind Selected** щоб прив'язати IP-адреси і хости до пакетів, щоб IP-адреси, отримані хостами від комутатора, залишалися незмінними.

Примітка

Кожен сервер або клієнт має лише один DUID для ідентифікації.

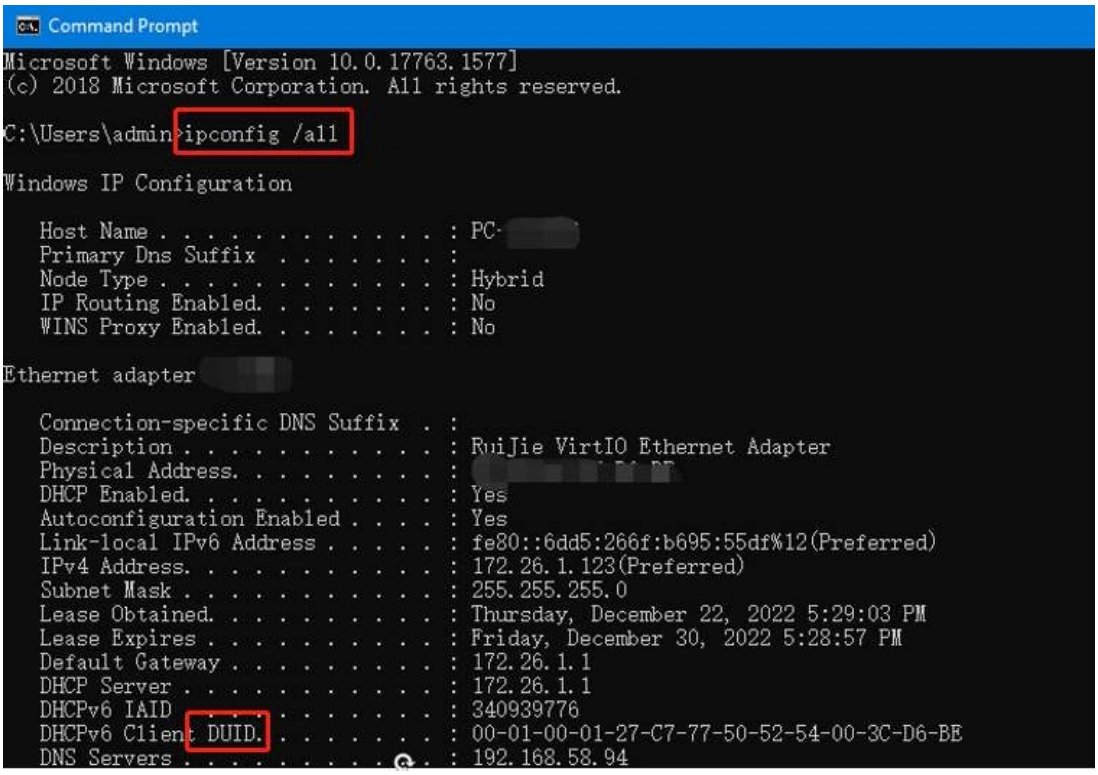


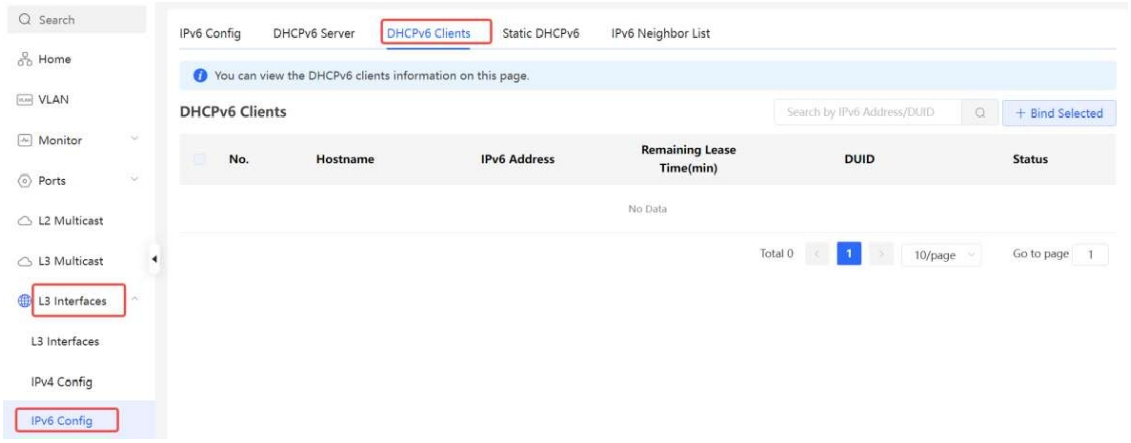
10.4.2 Налаштування статичної адреси DHCPv6

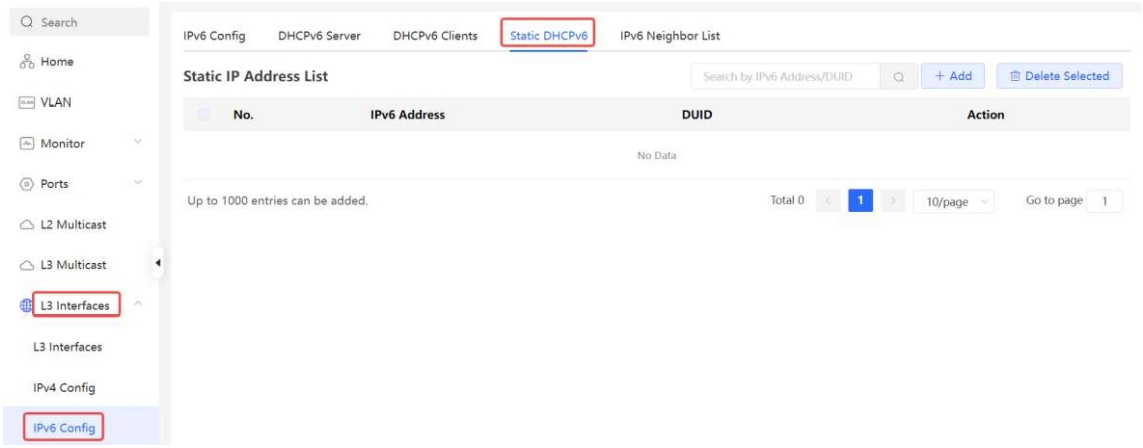
Налаштуйте IPv6-адресу, статично прив'язану до DUID клієнта, щоб клієнт міг щоразу отримувати вказану адресу.

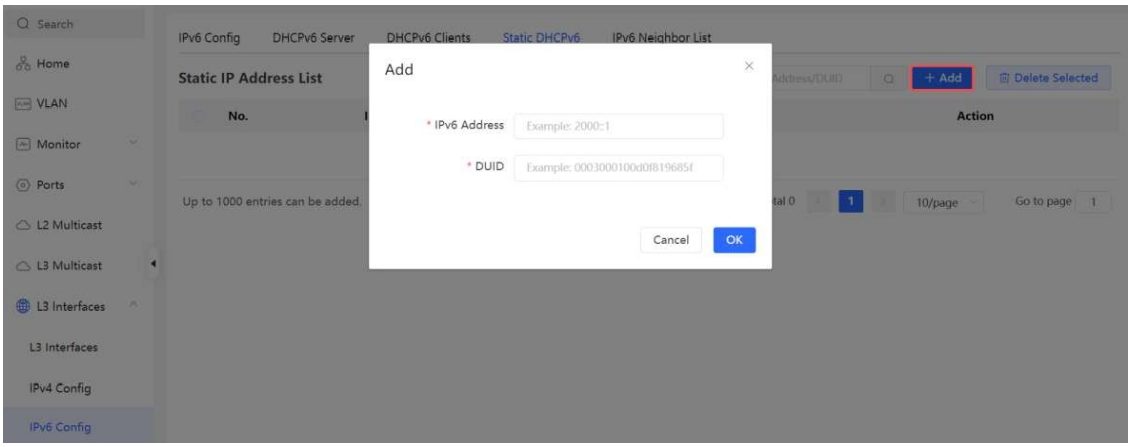
Виберіть **Локальний пристрій> Інтерфейси L3> Конфігурація IPv6> Статичний DHCPv6**.

Натисніть **Додати** і введіть IPv6-адресу та DUID. Рекомендується прив'язати IPv6-адресу та DUID до списку клієнтів. Ви можете виконати команду **ipconfig/all** у командному рядку Windows, щоб переглянути DUID.









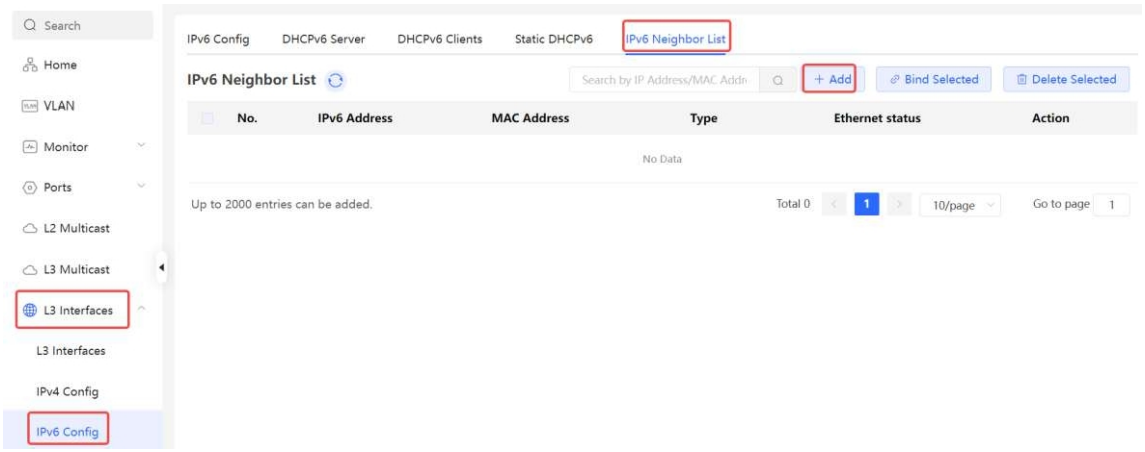
10.5 Налаштування списку сусідів IPv6

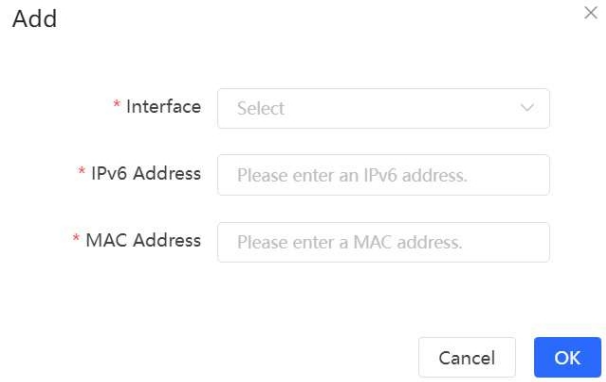
В IPv6 протокол виявлення сусідів (Neighbor Discovery Protocol, NDP) є важливим базовим протоколом. NDP замінює протоколи виявлення маршрутів ARP і ICMP в IPv4 і підтримує такі функції: дозвіл адрес, відстеження стану сусіда, виявлення дублікатів адрес, виявлення маршрутизатора і перенаправлення.

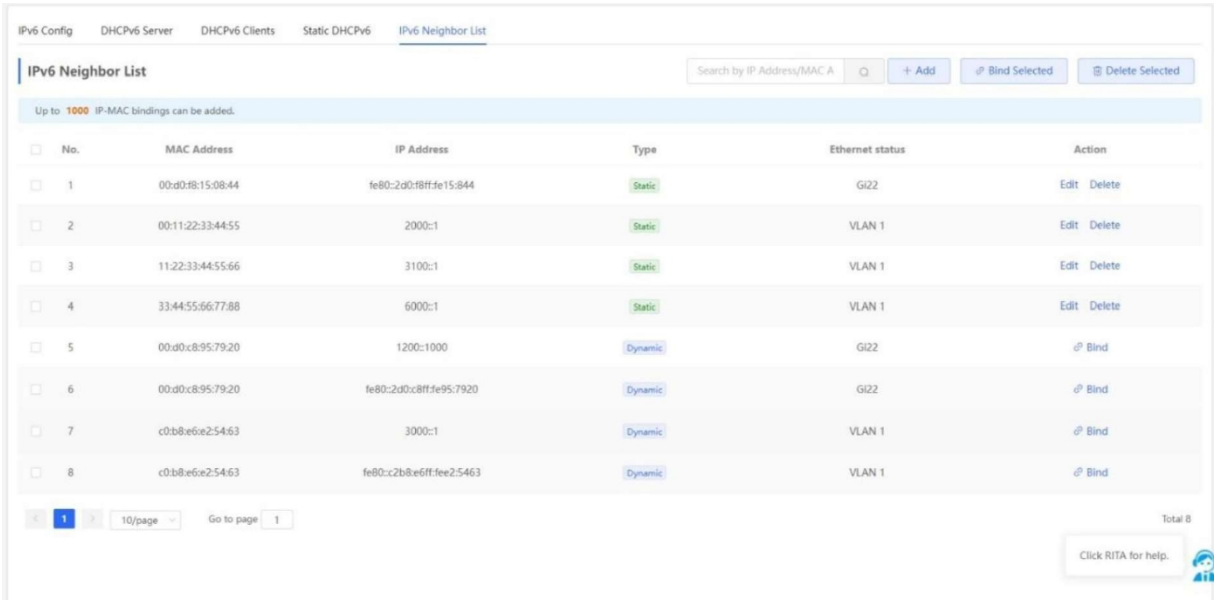
Виберіть **Локальний пристрій**> **Інтерфейси L3**> **Конфігурація IPv6**> **Список сусідів IPv6**.

Натисніть **Додати** і вручну додайте інтерфейс, IPv6-адресу і MAC-адресу сусіда.

Натисніть **Прив'язати вибране**, щоб прив'язати IPv6-адресу та MAC-адресу до списку для запобігання ND-атакам. Ви також можете змінювати, видаляти, групово видаляти або шукати сусідів (за або MAC-адресою).







10.6 Налаштування статичного ARP-запису

Виберіть **Локальний пристрій**> **Інтерфейси L3**> **ARP-список**.

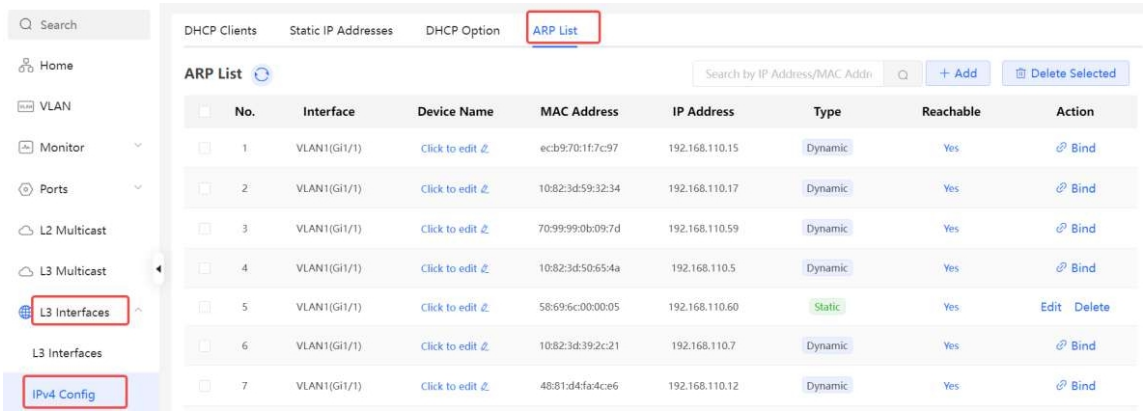
Пристрій запам'ятовує IP-адреси та MAC-адреси мережевих пристроїв, підключених до його інтерфейсів, і генерує відповідні ARP-записи. Підтримує прив'язку ARP-відображення або ручне визначення відповідності між IP-адресою та MAC-адресою, щоб запобігти пристроями неправильних ARP-записів і підвищити безпеку мережі.

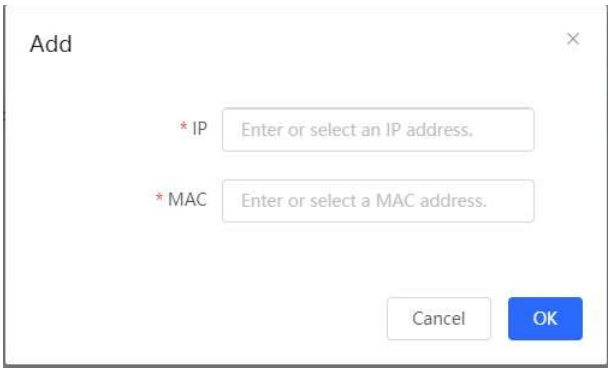
ARP-список відображає доступність, тип, IP-адресу, MAC-адресу та фізичний інтерфейс, що відповідає кожній MAC-адресі.

- Щоб прив'язати динамічний запис ARP до статичного запису: Виберіть запис ARP-відображення, динамічно отриманий в розділі

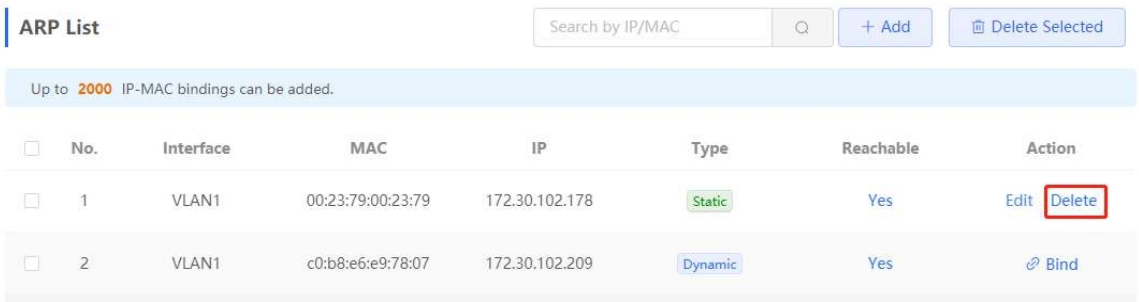
  ARP List і натисніть **Прив'**язати, щоб завершити прив'язку.

- Щоб вручну налаштувати статичний ARP-запис: Натисніть **Додати**, введіть IP-адресу і MAC-адресу для прив'язки і натисніть **OK**.





Щоб видалити прив'язку між статичною IP-адресою і MAC-адресою, натисніть **Видалити** в колонці **Дія**.



11 Налаштування маршруту

11.1 Налаштування статичних маршрутів

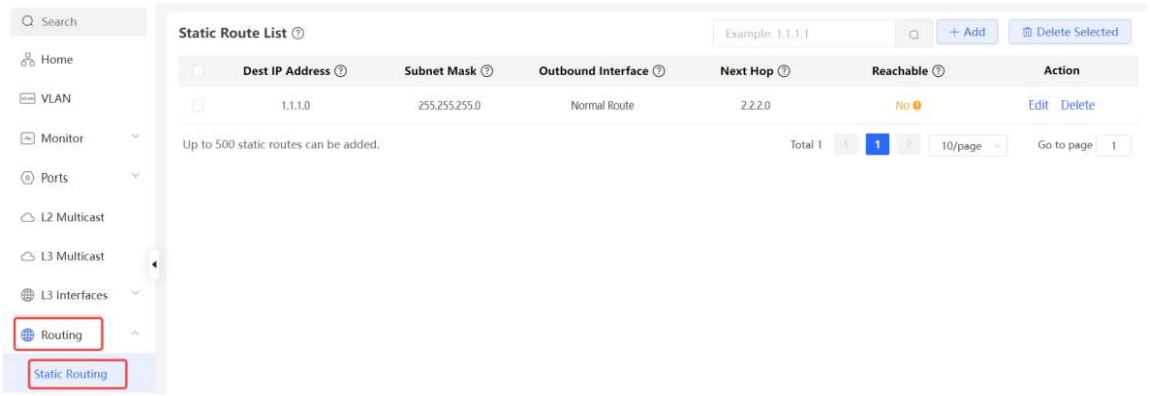
Виберіть **локальний пристрій> Маршрутизація> Статична маршрутизація**

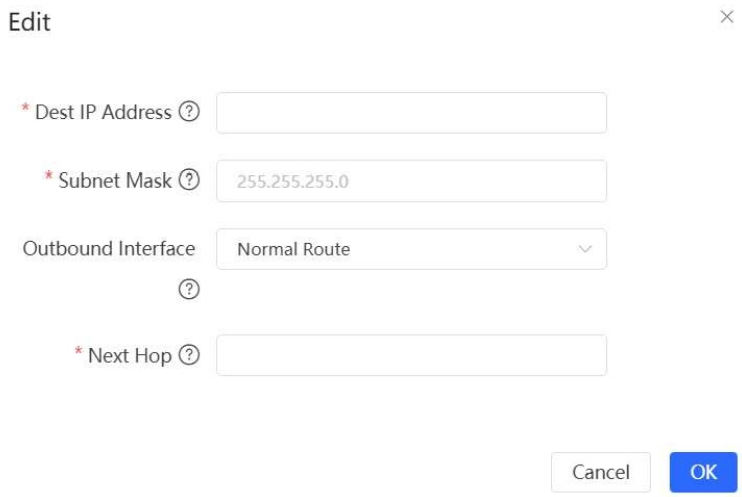
Статичні маршрути налаштовуються користувачем вручну. Коли пакет даних відповідає статичному маршруту, він буде переадресований відповідно до вказаного режиму переадресації.

Застереження

Статичні маршрути не можуть автоматично адаптуватися до змін топології мережі. Коли топологія мережі змінюється, потрібно переналаштувати статичні маршрути.

Натисніть кнопку **Додати**. У діалоговому вікні, що з'явиться, введіть адресу призначення, маску підмережі, вихідний інтерфейс і IP-адресу наступного переходу, щоб створити статичний маршрут.



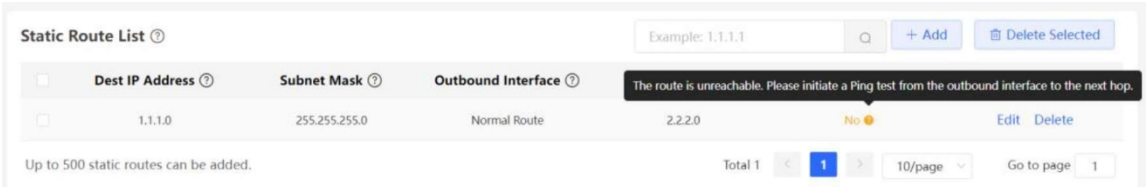


Таблиця 11-1 Опис параметрів конфігурації статичних маршрутів

Параметр	Опис
IP-адреса призначення	Вкажіть мережу призначення, до якої буде надіслано пакет даних. Пристрій

Параметр	Опис
	відповідає пакету даних на основі адреси призначення та маски підмережі.
Маска підмережі	Вкажіть маску підмережі мережі призначення. Пристрій підбирає пакет даних на основі адреси призначення та маски підмережі.
Вихідний інтерфейс	Вкажіть інтерфейс, який пересилає пакет даних.
Next Hop	Вказати IP-адресу наступного переходу в маршруті для пакету даних

Після створення статичного маршруту ви можете переглянути інформацію про нього та його стан у списку статичних маршрутів. Параметр **Досяжний** вказує, чи знаходиться наступна адреса переходу у локальному безпосередньо підключеному сегменті мережі. Якщо наступна адреса переходу знаходиться у безпосередньо підключеному сегменті мережі, відображається значення **Так,** і маршрут набуває чинності. В іншому випадку відображається значення **Ні**, і маршрут не набуває чинності. У цьому випадку перевірте конфігурацію.



Щоб видалити або змінити статичний маршрут, у **Списку статичних маршрутів** ви можете натиснути **Видалити** або **Змінити** в останньому стовпчику **Дія**; або виберіть запис статичного маршруту, який потрібно видалити, і натисніть **Видалити вибране**, щоб видалити кілька записів статичних маршрутів.

11.2 Налаштування статичного маршруту IPv6

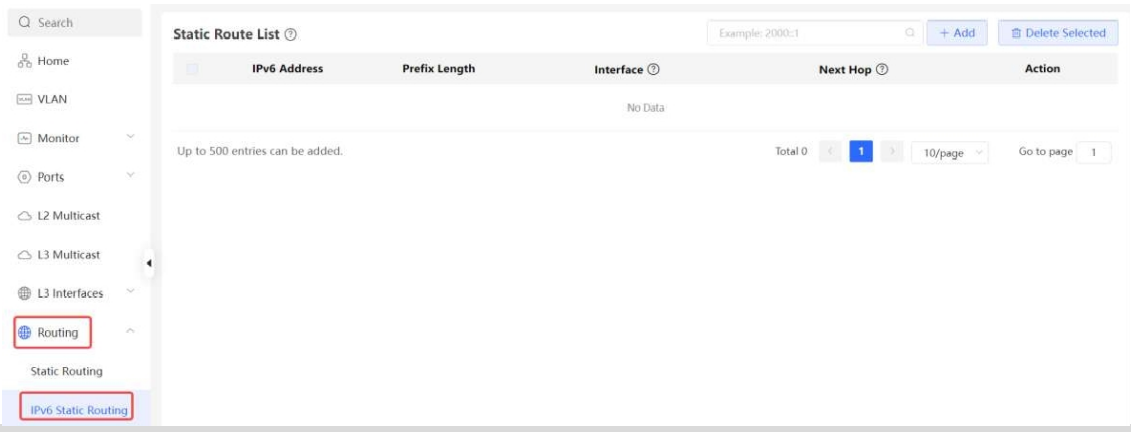
Виберіть **Локальний пристрій**> **Маршрутизація**> **Статична маршрутизація IPv6**.

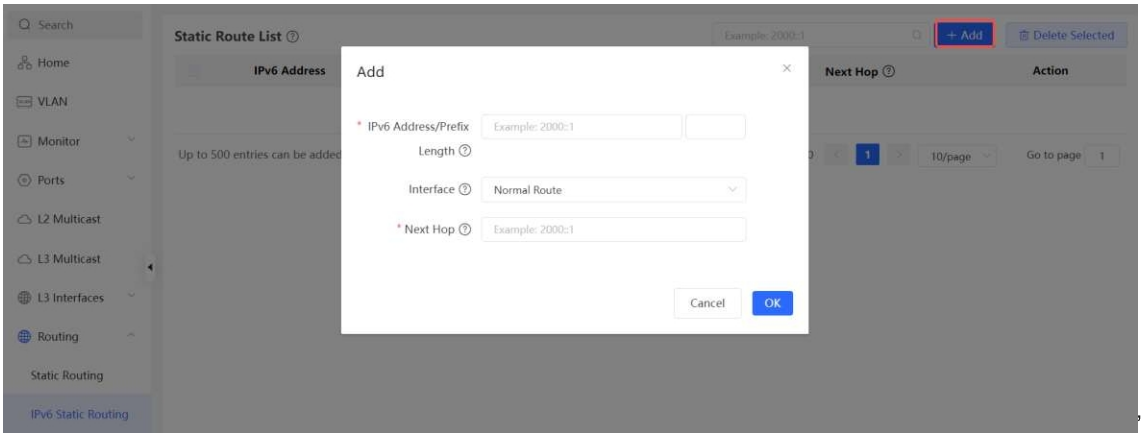
Вам вручну налаштувати статичний маршрут IPv6. Коли пакет зі статичним маршрутом, він буде переадресований відповідно до вказаного методу переадресації.

Застереження

Статичний маршрут не може автоматично адаптуватися до змін топології мережі. Коли топологія мережі змінюється, вам потрібно вручну переналаштувати статичний маршрут.

Натисніть **Додати** і введіть IPv6-адресу призначення, довжину, вихідний інтерфейс і IP-адресу наступного вузла, щоб створити статичний маршрут.





Таблиця 11-2 Параметри конфігурації статичного маршруту IPv6

Параметр	Опис
Довжина адреси/префікса IPv6	Мережа призначення пакета. Адреса призначення пакета підбирається відповідно до адреси IPv6 та довжини префікса.
Вихідний інтерфейс	Інтерфейс, який пересилає пакет.
Next Hop	IP-адреса наступного вузла маршрутизації, на який надсилається пакет.

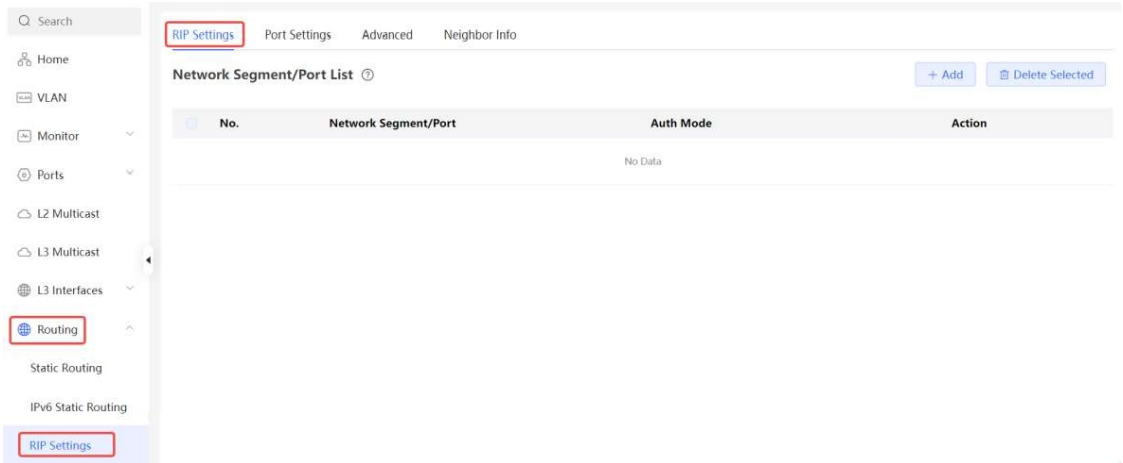
11.3 Налаштування RIP

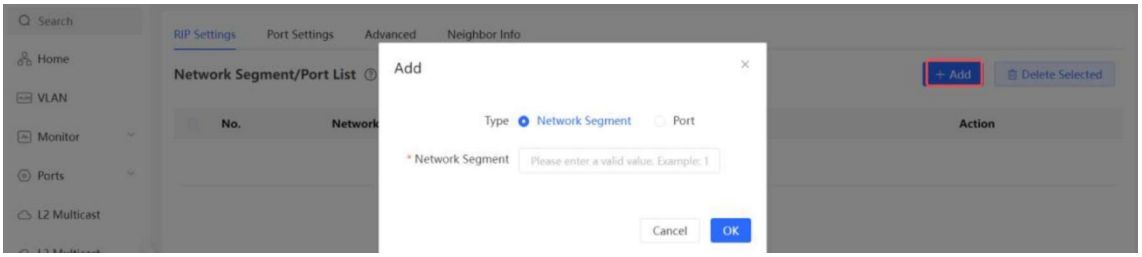
Інформаційний протокол маршрутизації (Routing Information Protocol, RIP) застосовується в малих і середніх мережах і є динамічним протоколом маршрутизації, який легко налаштовувати. RIP вимірює мережеву відстань на основі кількості переходів і вибирає маршрут на основі цієї відстані. RIP використовує UDP порт 520 для обміну інформацією про маршрутизацію.

11.3.1 Налаштування основних функцій RIP

Виберіть **Локальний пристрій**> **Маршрутизація**> **Налаштування RIP**.

Натисніть **Додати** і налаштуйте мережевий сегмент та інтерфейс.



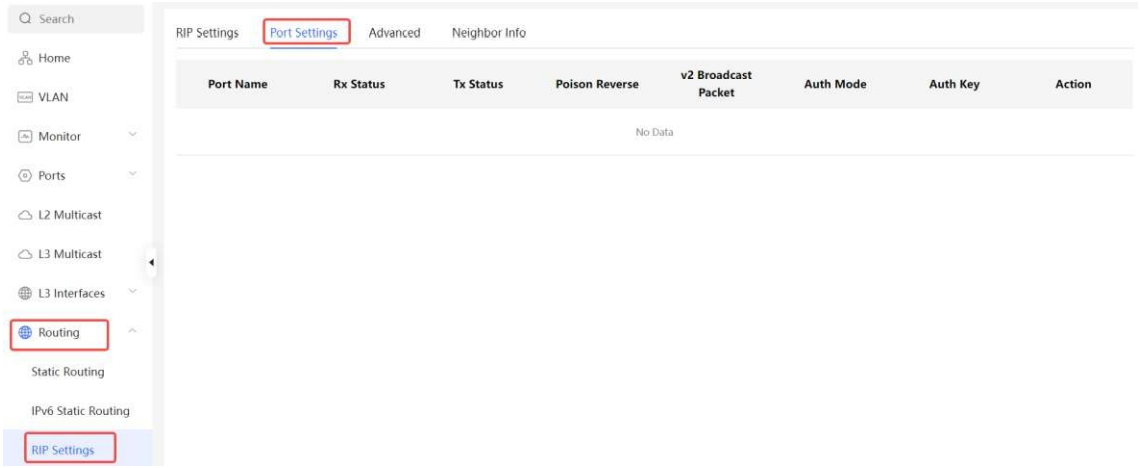


Таблиця 11-3 Параметри конфігурації RIP

Параметр	Опис
Тип	**Сегмент мережі**: Увімкнути RIP у вказаному сегменті мережі. IP-адреси цього сегмента мережі додаються до таблиці маршрутизації RIP. Пристрій і сусідні пристрої з увімкненим RIP дізнаються таблицю маршрутизації один від одного. **Порт**: Увімкнути RIP на вказаному порту. Усі IP-адреси цього порту додаються таблиці маршрутизації RIP. Пристрій і його сусідні пристрої з увімкненим RIP дізнаються таблицю маршрутизації один від одного.
Мережевий сегмент	Введіть мережевий сегмент, наприклад, **10.1.0.0.0/24**, якщо для параметра **Тип** встановлено значення **Сегмент мережі**. RIP буде ввімкнено на всіх інтерфейсах пристрою, що входить до цього сегмента мережі.
Порт	Виберіть інтерфейс VLAN або фізичний порт, якщо для **параметра Тип** встановлено значення **Порт**.
Режим авторизації	**Немає автентифікації**: Пакети протоколу не автентифіковано. **Зашифрований текст**: Пакети протоколу автентифікуються, а ключ автентифікації передається з пакетами протоколу у вигляді зашифрованого тексту. **Звичайний текст**: Пакети протоколу автентифікуються, а ключ автентифікації передається з пакетами протоколу у вигляді простого тексту.
Ключ авторизації	Введіть ключ автентифікації для автентифікації пакетів протоколу, коли **режим автентифікації** встановлено на **Зашифрований текст** або **звичайний текст**.

11.3.2 Налаштування порту RIP

Виберіть **Локальний пристрій**> **Маршрутизація**> **Налаштування RIP**> **Налаштування порту**.

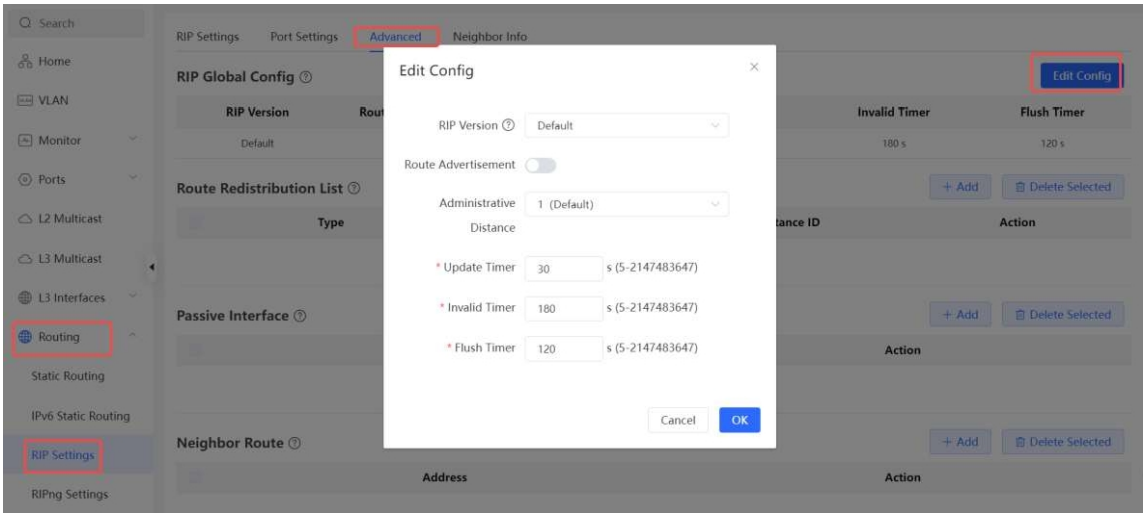


Таблиця 11-4 Параметри конфігурації списку портів

Параметр	Опис
Ім'я порту	Ім'я порту, на якому ввімкнено RIP.
Статус приймача	RIP-версії пакетів, що отримуються в даний момент.
Статус передачі даних	RIP-версії пакетів, що передаються в даний момент.
Зворотний бік отрути	Після того, як порт дізнається маршрут, значення параметра route overhead дорівнює **16** (вказує на те, що маршрут недосяжний), і маршрут надсилається назад до сусіда з початкового порту, щоб уникнути зациклення.
v2 Broadcast Packet	Якщо сусід не підтримує багатоадресну розсилку, можна надсилати широкомовні пакети. Рекомендується вимкнути широкомовні пакети RIPv2 для підвищення продуктивності мережі.
Режим авторизації	**Немає автентифікації**: Пакети протоколу не автентифіковано. **Зашифрований текст**: Пакети протоколу автентифікуються, а ключ автентифікації передається з пакетами протоколу у вигляді зашифрованого тексту. **Звичайний текст**: Пакети протоколу автентифікуються, а ключ автентифікації передається з пакетами протоколу у вигляді простого тексту.
Ключ авторизації	Введіть ключ автентифікації для автентифікації пакетів протоколу, якщо для параметра **Режим автентифікації** встановлено значення **Зашифрований текст** або **Звичайний текст**.
Дія	Натисніть Змінити, щоб змінити параметри RIP порту.

11.3.3 Налаштування глобальної конфігурації RIP

Виберіть **Локальний пристрій**> **Маршрутизація**> **Налаштування RIP**> **Додатково**, натисніть **Редагувати конфігурацію** і налаштуйте параметри глобальної конфігурації RIP.



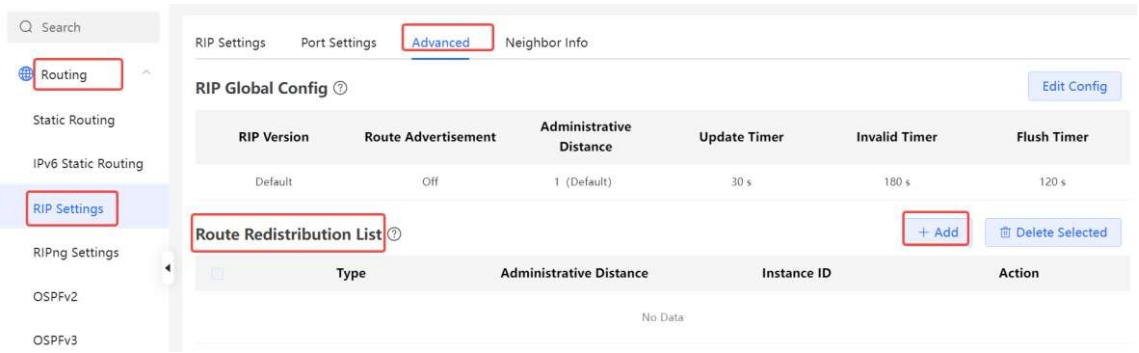
Таблиця 11-5 Параметри глобальної конфігурації RIP

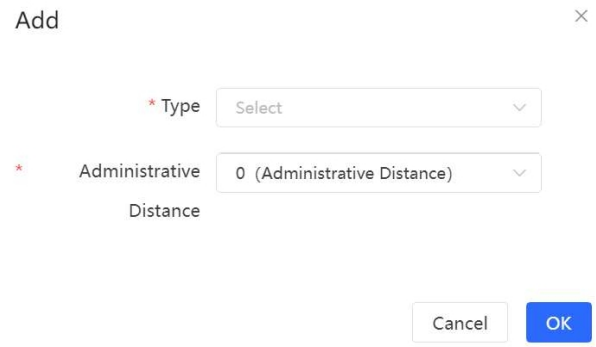
Параметр	Опис
RIP-версія	**За замовчуванням**: Виберіть RIPv2 для надсилання пакетів і RIPv1/v2 для отримання пакетів. **V1**: Виберіть RIPv1 для надсилання та отримання пакетів. **V2**: Виберіть RIPv2 для надсилання та отримання пакетів.
Реклама маршруту	Після увімкнення реклами маршрутів поточний пристрій генерує маршрут за замовчуванням і надсилає його сусідові.
Адміністративна відстань	Перерозподіл маршрутів інших протоколів у домені RIP, щоб RIP міг взаємодіяти з іншими доменами маршрутизації.
Таймер оновлення	Цикл оновлення RIP. За замовчуванням інформація про маршрути оновлюється кожні 30 секунд.
Неправильний таймер	Якщо до того, як маршрут стане недійсним, не буде отримано жодного оновлення, маршрут вважається недосяжним. Значення за замовчуванням - 180 секунд.
Таймер змиву	Якщо до закінчення таймера очищення недійсного маршруту не отримано жодних оновлень, маршрут буде повністю видалено з таблиці маршрутизації RIP. Значення за замовчуванням - 120 секунд.

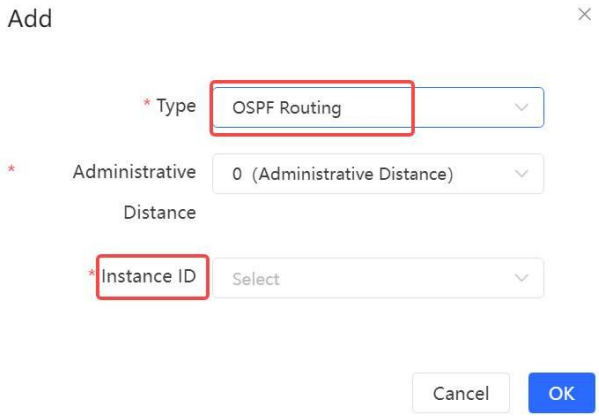
11.3.4 Налаштування списку перерозподілу маршрутів RIP

Перерозподіл маршрутів інших протоколів у домені RIP, щоб RIP міг взаємодіяти з іншими доменами маршрутизації.

Виберіть **Локальний пристрій**> **Маршрутизація**> **Налаштування RIP**> **Додатково > Список перерозподілу маршрутів**, натисніть **Додати**, виберіть тип і адміністративну відстань.







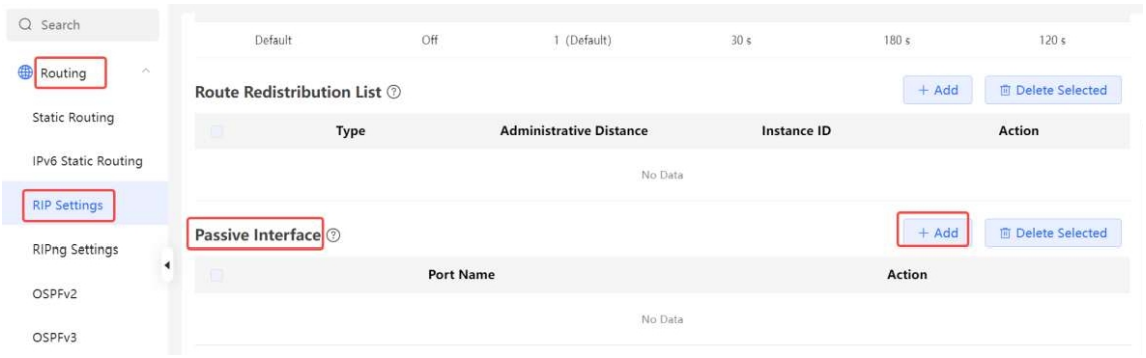
Таблиця 11-6 Параметри перерозподілу маршрутів RIP

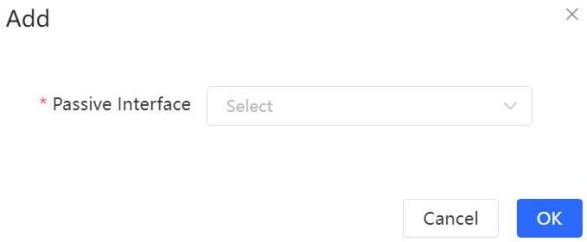
Параметр	Опис
Тип	Пряма маршрутизація Статична маршрутизація OSPF Routing
Адміністративна відстань	Чим менша адміністративна відстань, тим вищий пріоритет. Значення за замовчуванням **- 0**. Значення варіюється від 0 до 16.
Ідентифікатор екземпляра	Виберіть ідентифікатор екземпляра OSPF, який потрібно перерозподілити. На локальному пристрої має бути ввімкнено OSPFv2.

11.3.5 Налаштування пасивного інтерфейсу

Якщо інтерфейс налаштовано як пасивний, він пригнічуватиме пакети оновлень RIP. Якщо на підключеному одноранговому пристрої не запущено RIP, рекомендується увімкнути пасивний інтерфейс.

Виберіть **Локальний пристрій> Маршрутизація> Налаштування RIP> Додатково > Пасивний інтерфейс**, натисніть **Додати** і виберіть пасивний інтерфейс.

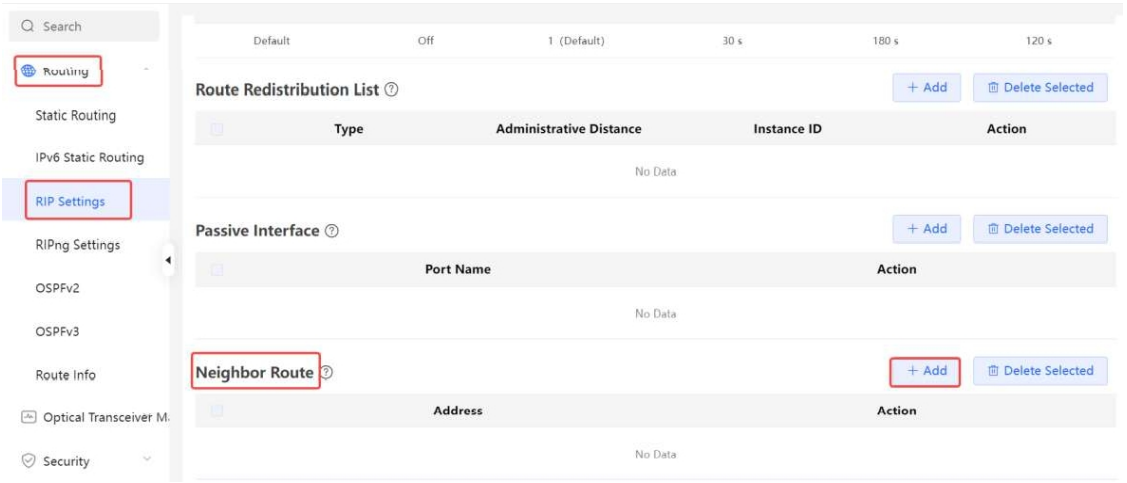


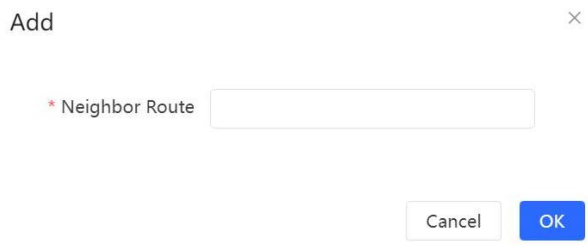


11.3.6 Налаштування сусіднього маршруту

Якщо маршрутизатор не може обробити широкомовні пакети, інший маршрутизатор можна призначити сусіднім для встановлення прямого з'єднання RIP.

Виберіть **Локальний пристрій> Маршрутизація> Налаштування RIP> Додатково > Сусідній маршрут**, натисніть **Додати** і введіть IP-адресу сусіднього маршрутизатора.





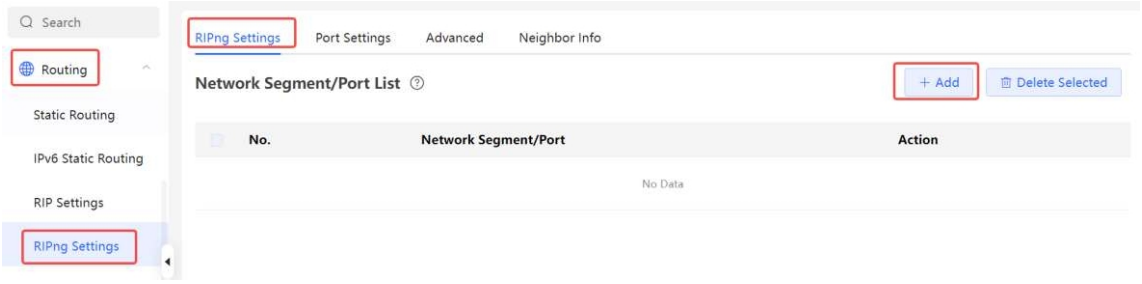
11.4 Налаштування RIPng

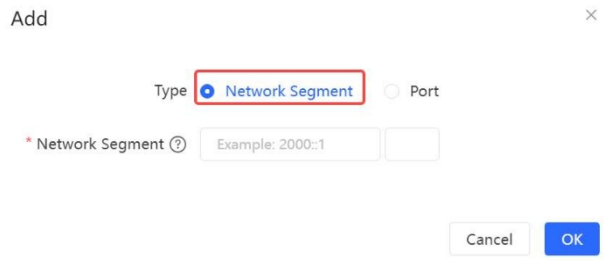
11.4.1 Налаштування основних функцій RIPng

RIP наступного покоління (RIPng) забезпечує функцію маршрутизації для мереж IPv6. RIPng використовує UDP порт 512 для обміну інформацією про маршрутизацію.

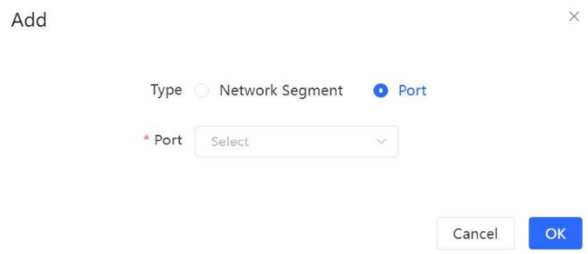
Виберіть **Локальний пристрій> Маршрутизація> Налаштування RIPng**.

Натисніть **Додати**, встановіть **Тип** на **Сегмент мережі** або **Порт** і вкажіть мережевий сегмент або порт відповідно.





Якщо довжина адреси становить від 48 до 64, адреса буде використовуватися як префікс. Крім того, увімкніть RIPng на вказаному порту:



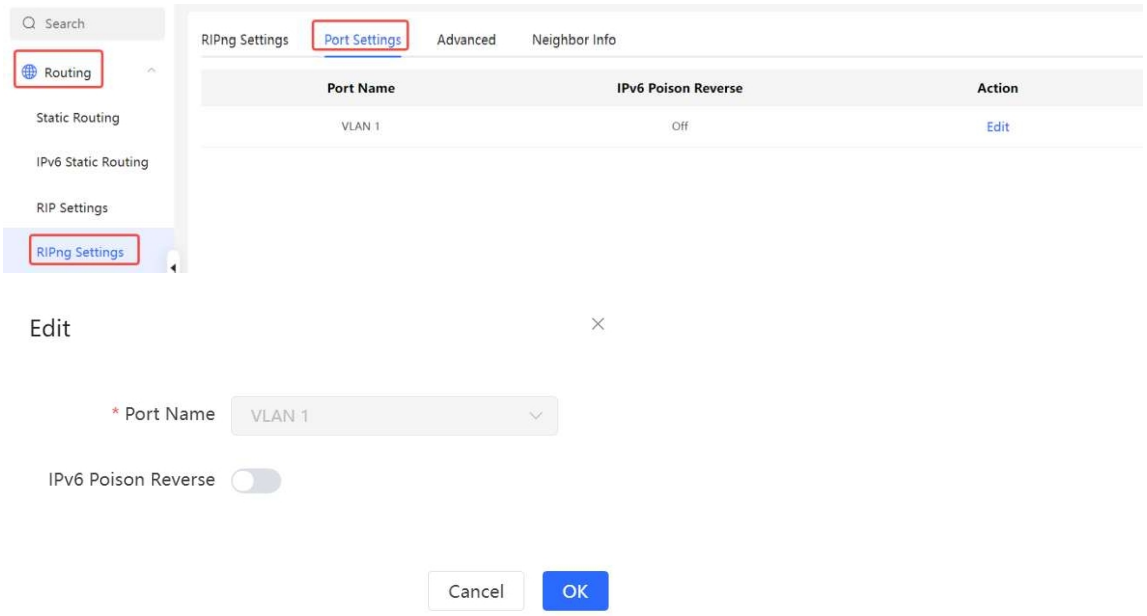
Таблиця 11-7 Параметри конфігурації RIPng

Параметр	Опис
Тип	**Сегмент мережі**: Увімкнути RIP у вказаному сегменті мережі. IP-адреси цього сегмента мережі додаються до таблиці маршрутизації RIP, а пристрій і сусідні пристрої з увімкненим RIP дізнаються таблицю маршрутизації один від одного. **Порт**: увімкнути RIP на вказаному порту. Усі IP-адреси цього порту додаються до таблиці маршрутизації RIP, і пристрій та його сусідні пристрої з увімкненим RIP дізнаються таблицю маршрутизації один від одного.
Мережевий сегмент	Введіть IPv6-адресу та довжину префікса, якщо для **параметра Тип** встановлено значення **Сегмент мережі**. RIPng буде ввімкнено на всіх інтерфейсах пристрою, що перебуває у цьому сегменті мережі.
Порт	Виберіть інтерфейс VLAN або фізичний порт, якщо для **параметра Тип** встановлено значення **Порт**.

11.4.2 Налаштування порту RIPng

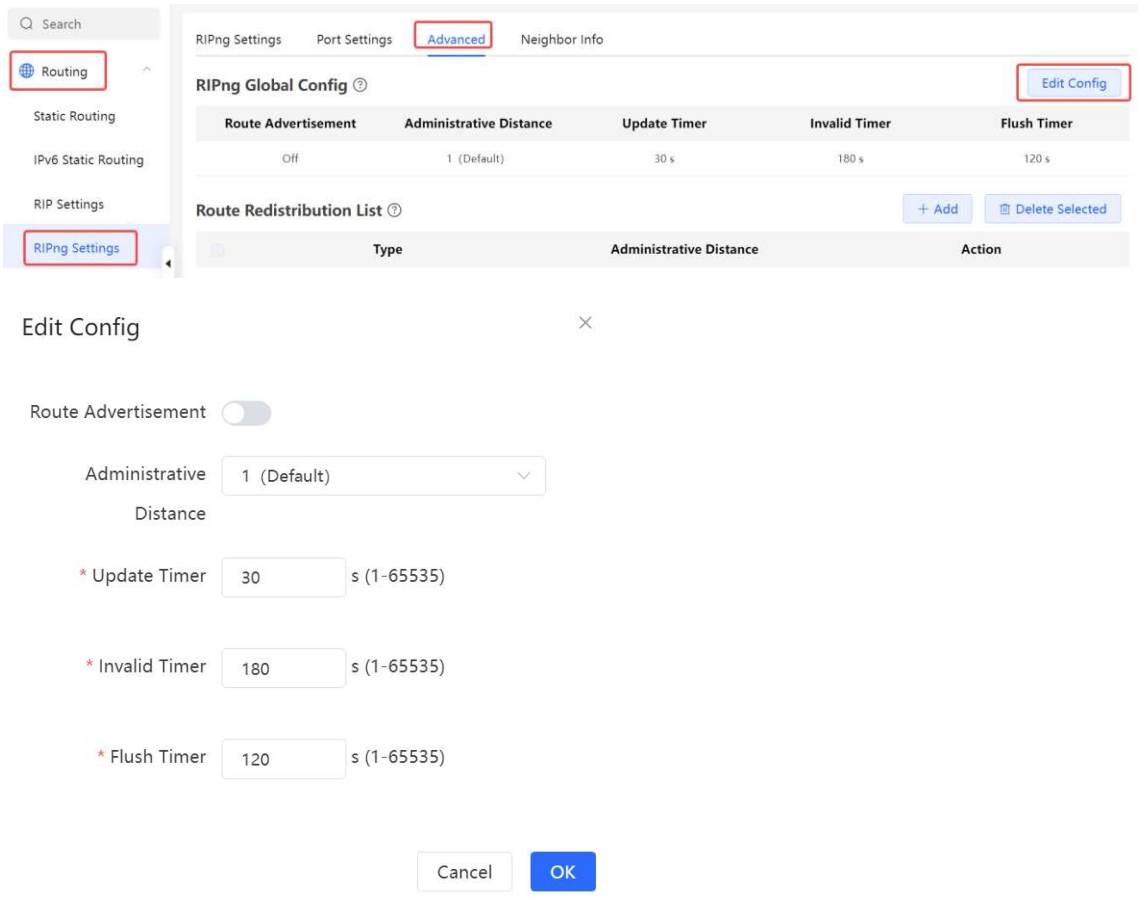
RIPng отрута навпаки: Після того, як порт дізнається маршрут, верхня межа маршруту встановлюється на **16** (що означає, що маршрут недосяжний), і маршрут надсилається назад до сусіда з початкового порту, щоб уникнути зациклення.

Виберіть **Локальний пристрій**> **Маршрутизація**> **Налаштування RIPng**> **Налаштування портів**, натисніть Редагувати і увімкніть зворотне отруєння IPv6.



11.4.3 Налаштування глобальної конфігурації RIPng

Виберіть **Локальний пристрій**> **Маршрутизація**> **Налаштування RIPng**> **Додатково**> **Глобальна конфігурація RIPng** і натисніть **Змінити конфігурацію**.



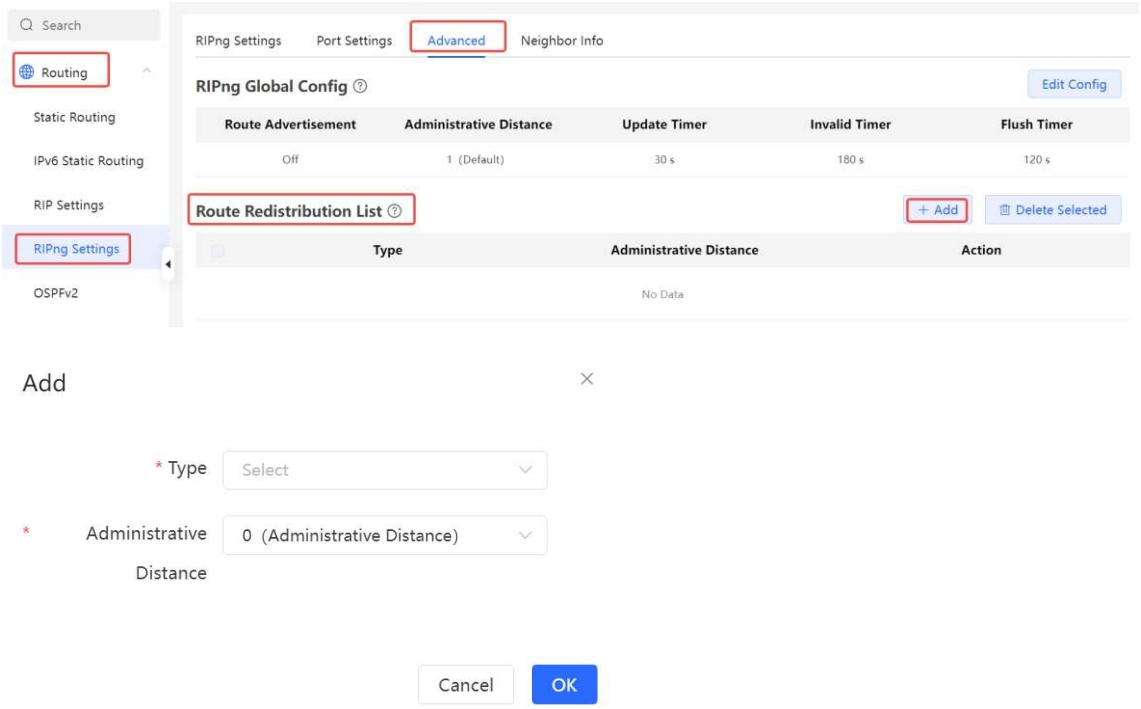
Таблиця 11-8 Параметри глобальної конфігурації RIPng

Параметр	Опис
Реклама маршруту	Після увімкнення реклами маршрутів поточний пристрій генерує маршрут за замовчуванням і надсилає його сусідові.
Адміністративна відстань	Перерозподіл маршрутів інших протоколів у домен RIP, щоб RIP міг взаємодіяти з іншими доменами маршрутизації.
Таймер оновлення	Цикл оновлення RIP. За замовчуванням інформація про маршрути оновлюється кожні 30 секунд.
Неправильний таймер	Якщо до того, як маршрут стане недійсним, не буде отримано жодного оновлення, маршрут вважається недосяжним. Значення за замовчуванням - 180 секунд.
Таймер змиву	Якщо до закінчення таймера очищення недійсного маршруту не отримано жодних оновлень, маршрут буде повністю видалено з таблиці маршрутизації RIP. Значення за замовчуванням - 120 секунд.

11.4.4 Налаштування списку перерозподілу маршрутів RIPng

Перерозподіл маршрутів інших протоколів у домен RIPng для взаємодії з іншими доменами маршрутизації.

Виберіть **Локальний пристрій> Маршрутизація> Налаштування RIPng> Додатково> Список перерозподілу маршрутів** і натисніть**+ Додати**.



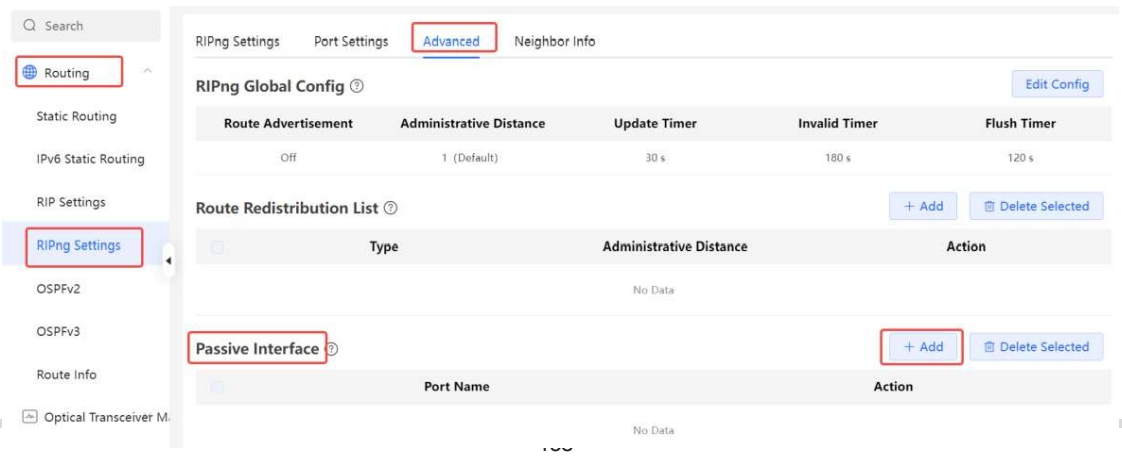
Таблиця 11-9 Параметри перерозподілу маршрутів RIP

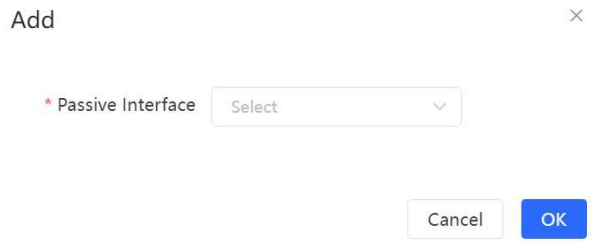
Параметр	Опис
Тип	Пряма маршрутизація Статична маршрутизація OSPF Routing
Адміністративна відстань	Діапазон значень: 0-16. Значення за замовчуванням **- 0**.

11.4.5 Налаштування пасивного інтерфейсу RIPng

Якщо інтерфейс налаштовано як пасивний, він пригнічуватиме пакети оновлень RIPng. Якщо на підключеному одноранговому пристрої не запущено RIP, рекомендується увімкнути пасивний інтерфейс.

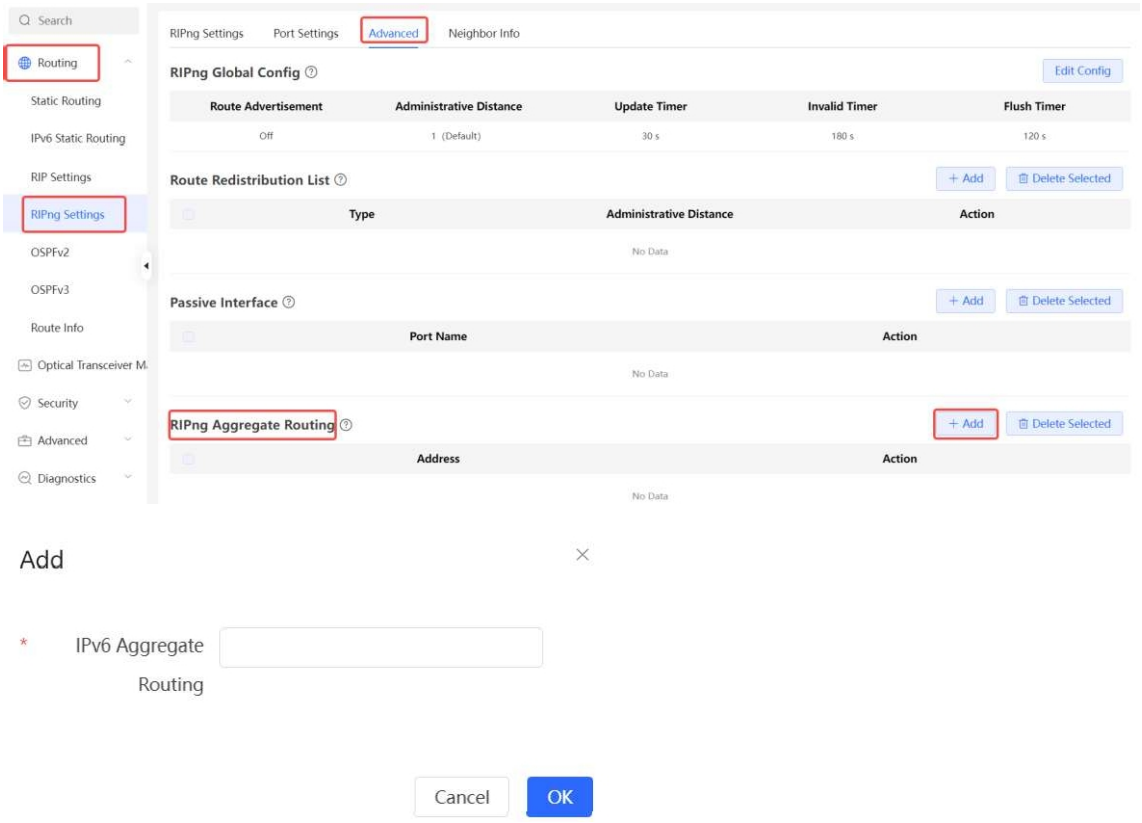
Виберіть **Локальний пристрій> Маршрутизація> Налаштування RIPng> Додатково> Пасивний інтерфейс**, натисніть **Додати** і введіть IP-адресу сусіднього маршрутизатора.





11.4.6 Налаштування агрегованого маршруту RIPng

Виберіть **Локальний пристрій> Маршрутизація> Налаштування RIP> Додатково> Агрегований маршрут RIPng**, натисніть **Додати** і введіть IPv6-адресу та довжину префікса (діапазон значень: 0─ 128).



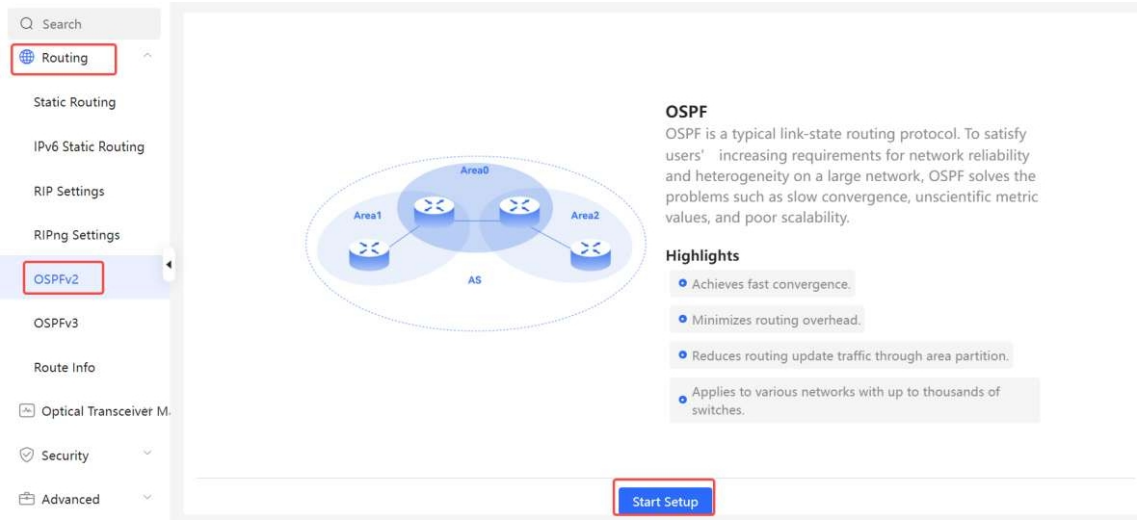
11.5 OSPFv2

Метод Open Shortest Path First (OSPF) можна застосовувати у великих мережах. IPv4 використовує OSPFv2, а IPv6 - OSPFv3.

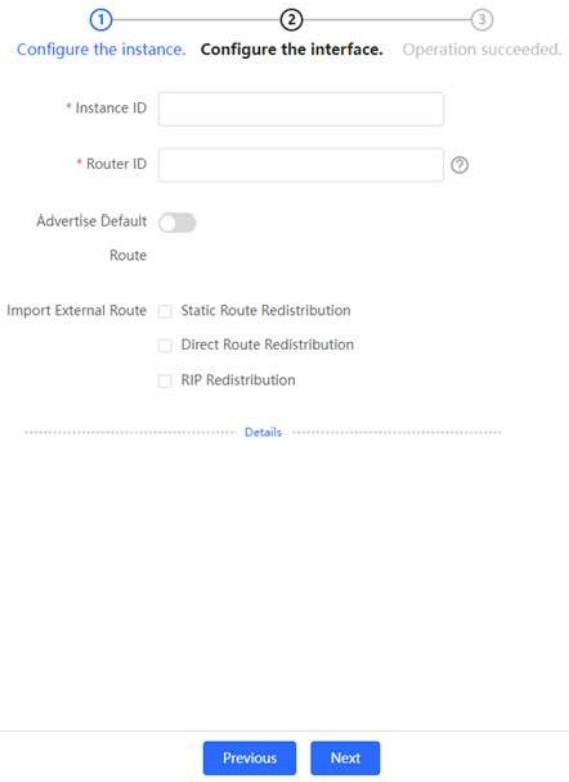
OSPF - це типовий протокол маршрутизації за станом каналу, який може вирішити проблеми повільного оновлення маршрутів, неточних вимірювань і поганої масштабованості у великих мережах. Він підходить для мереж різного розміру, і навіть для мереж з тисячами пристроїв.

11.5.1 Налаштування основних параметрів OSPFv2

Виберіть **Локальний пристрій> Маршрутизація> OSPFv2**, натисніть Почати **налаштування**, а потім налаштуйте екземпляр та інтерфейс відповідно.



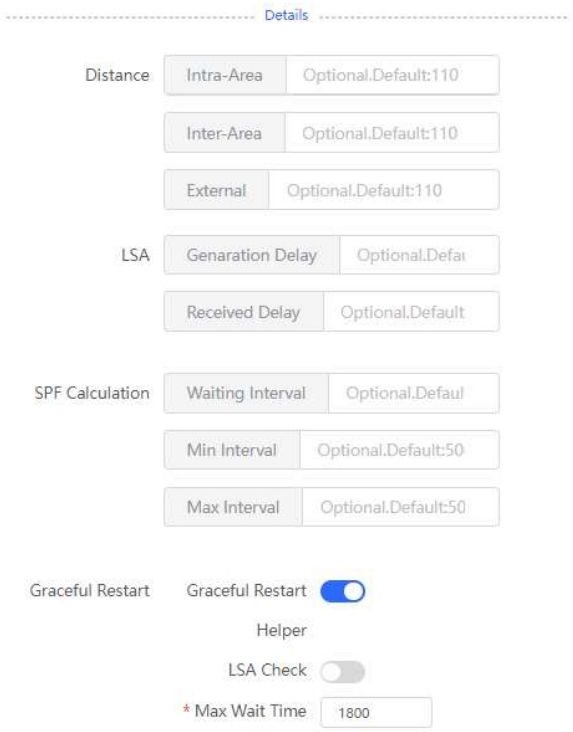
(1) Налаштуйте екземпляр.



Таблиця 11-10 Параметри конфігурації екземпляра

Параметр	Опис
Ідентифікатор екземпляра	Створіть екземпляр OSPF на основі типу служби. Екземпляр діє лише локально і не впливає на обмін пакетами з іншими пристроями.
Ідентифікатор маршрутизатора	Він ідентифікує маршрутизатор у домені OSPF.

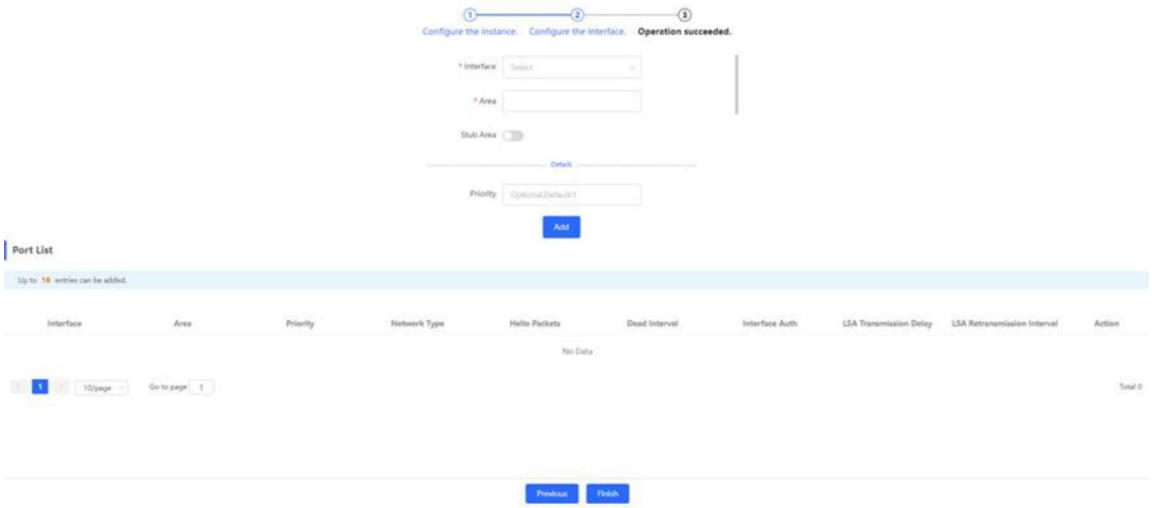
Параметр	Опис
	Застереження Ідентифікатори маршрутизаторів у межах одного домену мають бути унікальними. Однакова конфігурація може призвести до збоїв у виявленні сусідів.
Рекламувати маршрут за замовчуванням	Згенеруйте маршрут за замовчуванням і надішліть його сусідові. Після ввімкнення цієї функції вам потрібно ввести метрику і вибрати тип. За замовчуванням метрика дорівнює **1**. Тип 1: Показники, що відображаються на різних маршрутизаторах, відрізняються. Тип 2: Показники, що відображаються на всіх маршрутизаторах, однакові.
Імпорт Зовнішній маршрут	Перерозподіл маршрутів інших протоколів в домені OSPF для взаємодії з іншими доменами маршрутизації. Якщо вибрано **Статичний перерозподіл маршрутів**, введіть метрику, яка за замовчуванням дорівнює **20**. Якщо вибрано **Прямий перерозподіл маршрутів**, введіть метрику, яка за замовчуванням дорівнює **20**. Якщо вибрано RIP-перерозподіл, введіть метрику, яка за замовчуванням дорівнює **20**.
Деталі	Розгорніть детальну конфігурацію.



Таблиця 11-11 Параметри у детальній конфігурації екземпляра

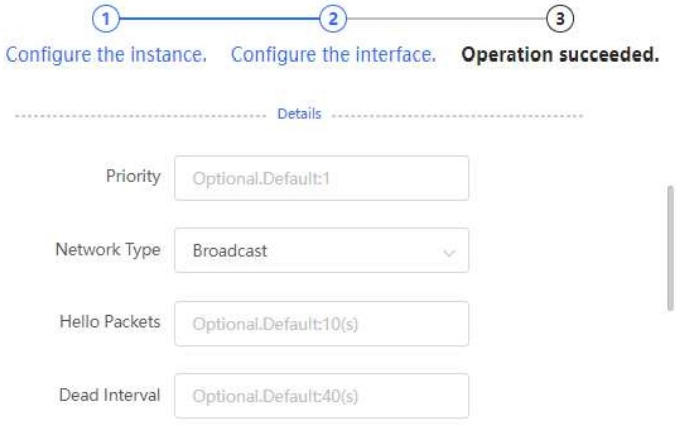
Параметр	Опис
Відстань	Використовується для вибору протоколу. За замовчуванням, внутрішні, міжобласні та зовнішні відстані дорівнюють **110**.
LSA	Часті зміни мережі та перемикання маршрутів можуть займати занадто багато пропускної здатності мережі та ресурсів пристрою. Затримки генерації та отримання LSA визначені в OSPF за замовчуванням. Значення за замовчуванням - 1000 мс.
Розрахунок SPF	Коли база даних стану каналу (LSDB) змінюється, OSPF перераховує найкоротший шлях і встановлює інтервал, щоб запобігти частим змінам мережі, які займають велику кількість ресурсів **Інтервал очікування**: Коли стан змінюється, таймер спрацьовує. Затримка обчислюється вперше після закінчення таймера. Значення за замовчуванням - 0 мс. **Мінімальний інтервал**: Зі збільшенням кількості змін час кожного інтервалу буде збільшуватися відповідно до алгоритму, і значення за замовчуванням становить 50 мс. **Максимальний інтервал**: Коли розрахований інтервал досягає максимального інтервалу, наступний інтервал завжди дорівнює максимальному інтервалу. Якщо час від останнього розрахунку перевищує максимальний інтервал, а LSDB не оновлюється, таймер вимикається.
Граціозний перезапуск	Плавний перезапуск (GR) дозволяє уникнути перекидання маршруту, спричиненого перериванням трафіку та перемиканням активної/резервної плати, забезпечуючи тим самим стабільність ключових сервісів. **Помічник плавного перезапуску**: Якщо цей перемикач увімкнено, вмикається функція Помічник плавного перезапуску. **Перевірка LSA**: Коли цей перемикач увімкнено, перевіряються пакети LSA за межами домену. **Максимальний час очікування**: відлік часу починається після того, як пристрій отримує пакет GR від однорангового пристрою. Якщо одноранговий пристрій не завершує GR протягом **максимального часу очікування**, пристрій виходить з режиму помічника GR. Значення за замовчуванням - 1800 секунд.

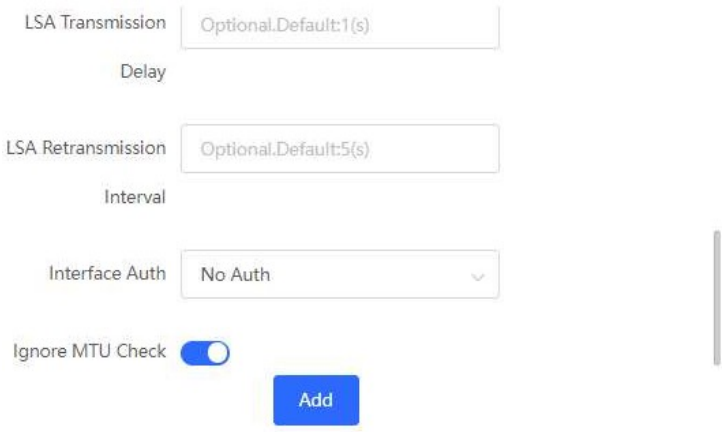
(2) Налаштуйте інтерфейс.



Таблиця 11-12 Параметри конфігурації інтерфейсу

Параметр	Опис
Інтерфейс	Виберіть інтерфейс 3-го рівня з підтримкою OSPF.
Площа	Налаштуйте ідентифікатор області. Діапазон значень: 0-4294967295
Область заглушки	Якщо увімкнено опцію **Stub Area**, вам потрібно налаштувати тип області та ізоляцію міжобласних маршрутів. Заглушка: Маршрутизатори на краю області не рекламують маршрути за її межами, а таблиця маршрутизації в цій області невелика. Не дуже заросла територія (NSSA): Можна імпортувати кілька зовнішніх маршрутів. Ізоляція міжрайонних маршрутів: Після увімкнення цієї функції міжобласні маршрути не будуть імпортовані до цієї області.
Деталі	Розгорніть детальну конфігурацію.



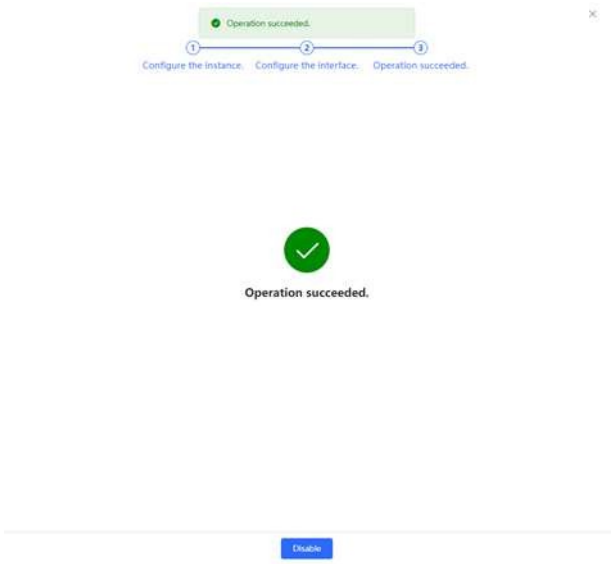


Таблиця 11-13 Параметри у детальній конфігурації інтерфейсу

Параметр	Опис
Пріоритет	За замовчуванням дорівнює 1.
Тип мережі	Трансляція Одноадресна багатоадресна Мультиплексний доступ до нерозповсюджуваного контенту
Привіт, пакети	Інтервал для періодичної передачі, який використовується для виявлення і підтримки відносин з сусідами OSPF. Значення за замовчуванням - 10 секунд.
Мертвий інтервал	Час, через який сусід стає недійсним. Значення за замовчуванням - 40 секунд.
Затримка передачі LSA	Затримка передачі LSA інтерфейсу. Значення за замовчуванням - 1 секунда.
Інтервал ретрансляції LSA	Час, через який LSA повторно передається після втрати LSA. Значення за замовчуванням - 5 секунд.
Авторизація інтерфейсу	**Без** автентифікації: пакети протоколу не автентифікуються. Це за замовчуванням. **Звичайний текст**: Пакети протоколу автентифікуються, а ключ автентифікації передається з пакетами протоколу у вигляді простого тексту. **MD5**: Пакети протоколу автентифікуються, а ключ автентифікації зашифровується в MD5 і передається разом з пакетами протоколу.
Ігнорувати перевірку MTU	Увімкнено за замовчуванням.

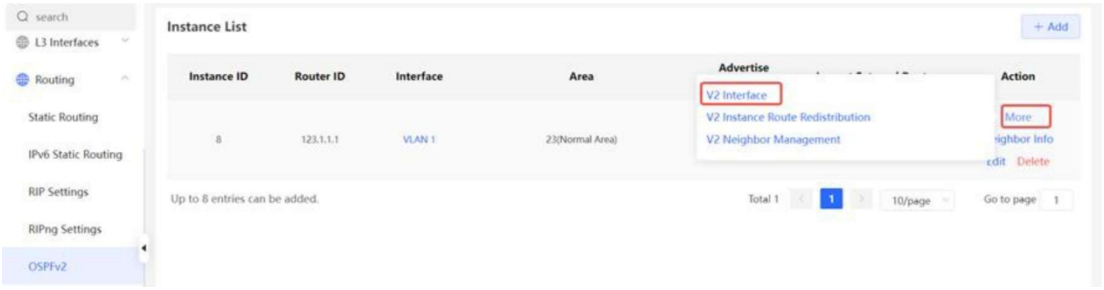
(3) Завершіть конфігурацію.

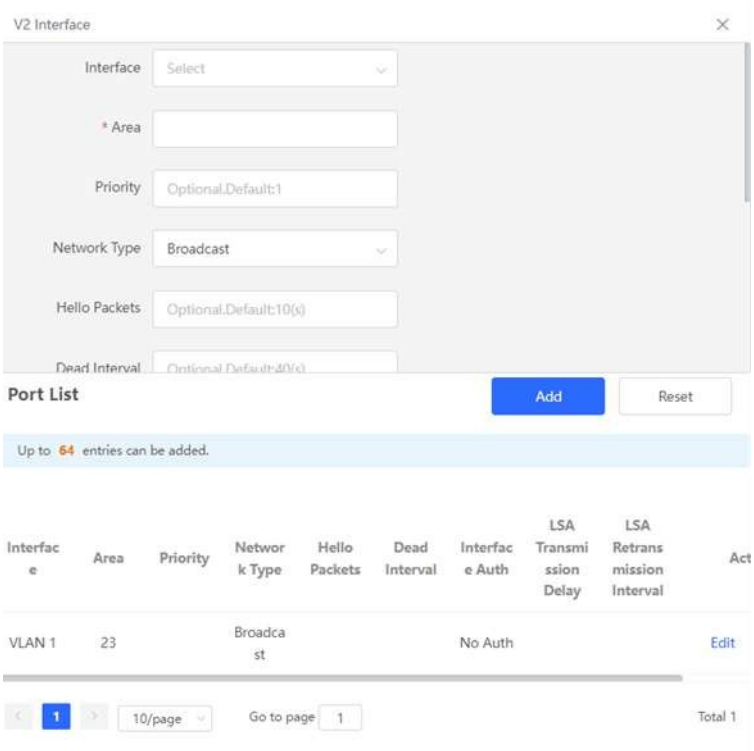
Після завершення налаштування ви можете вибрати **Локальний пристрій**> **Маршрутизація**> **OSPFv2** і переглянути список екземплярів.



11.5.2 Додавання інтерфейсу OSPFv2

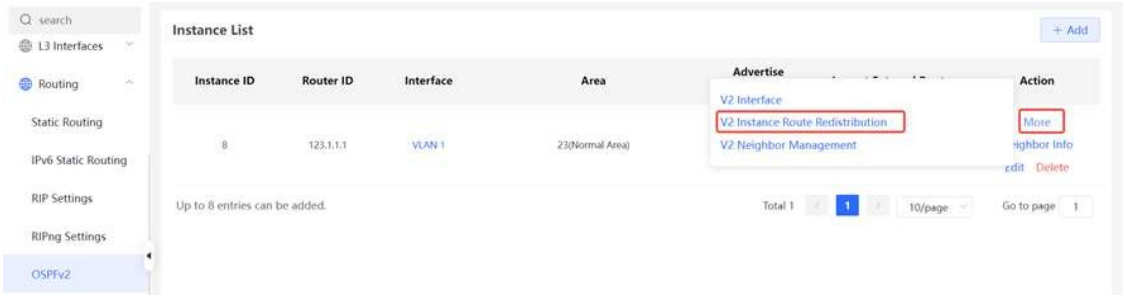
Виберіть **Локальний пристрій**> **Маршрутизація**> **OSPFv2**, натисніть **Більше** у колонці **Дія** і виберіть **Інтерфейс V2**.

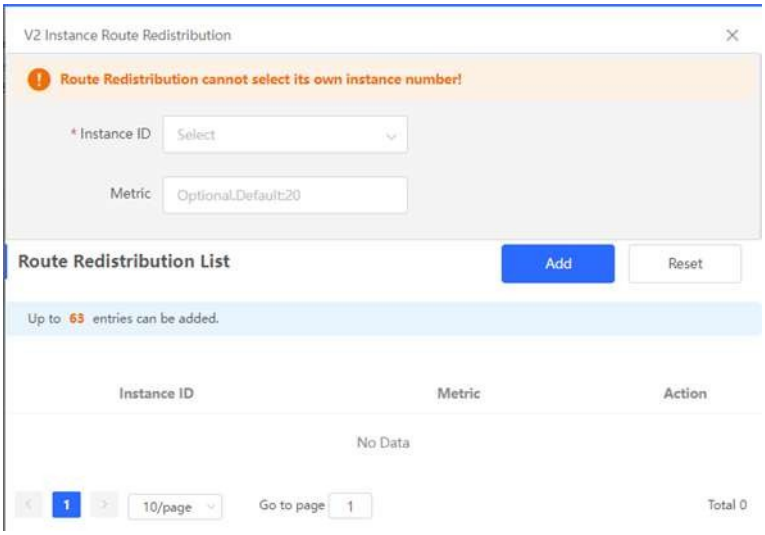




11.5.3 Перерозподіл маршрутів екземплярів OSPFv2

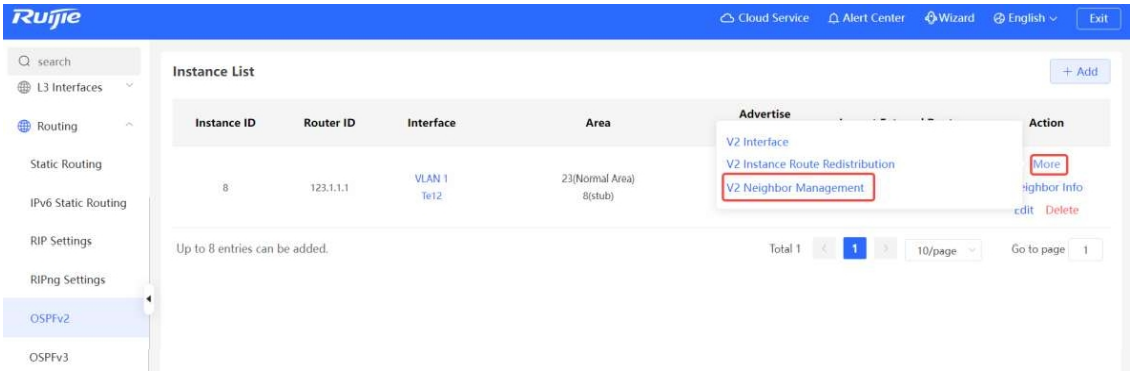
Виберіть **Локальний пристрій**> **Маршрутизація**> OSPFv2, натисніть **Більше** у стовпчику **Дія** і виберіть **Перерозподіл маршрутів екземплярів V2**.

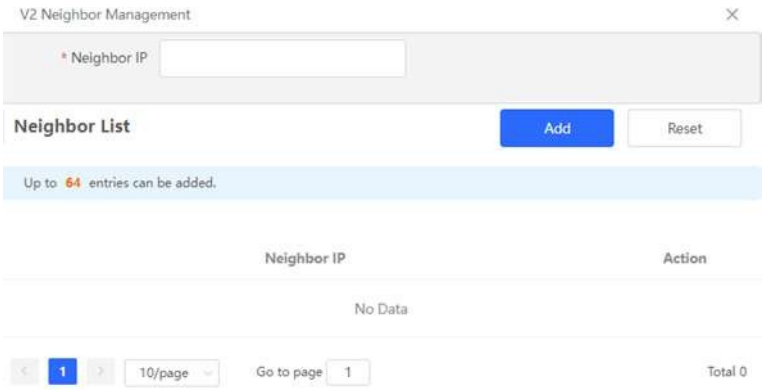




11.5.4 Керування сусідами OSPFv2

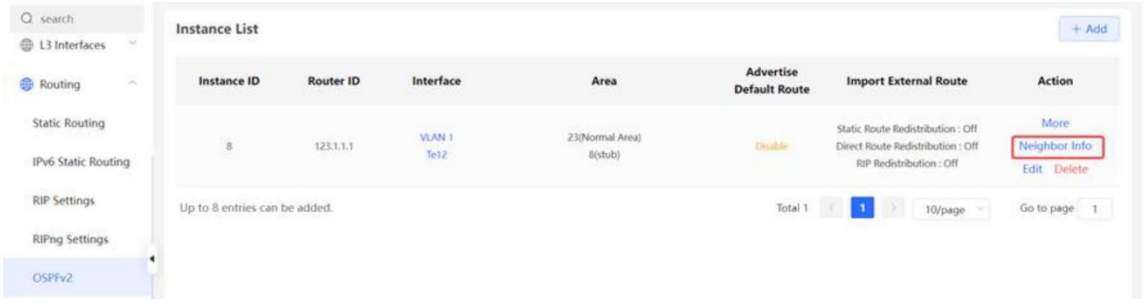
Виберіть **Локальний пристрій> Маршрутизація> OSPFv2**, натисніть **Більше** у стовпчику **Дія** і виберіть **Управління сусідами V2**.

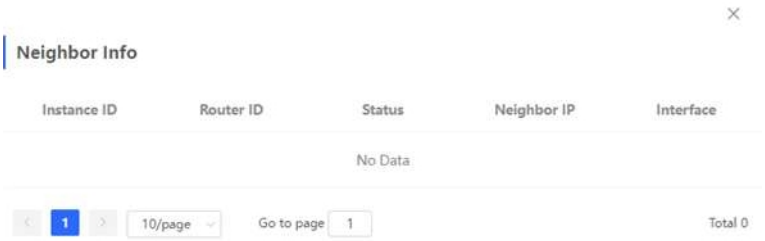




11.5.5 Перегляд інформації про сусідів OSPFv2

Виберіть **Локальний пристрій> Маршрутизація>** OSPFv2 і натисніть **Інформація про сусіда** у колонці **Дія**.





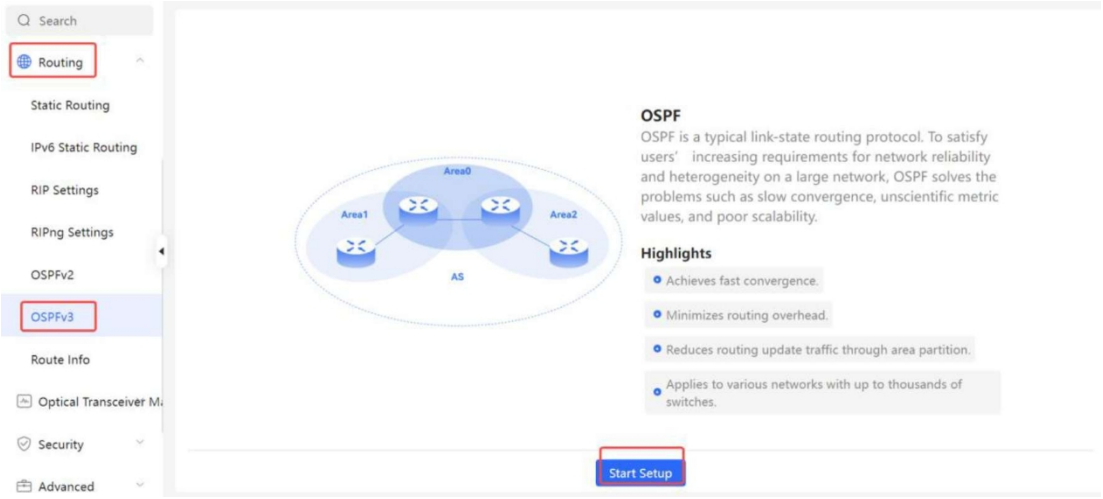
11.6 OSPFv3

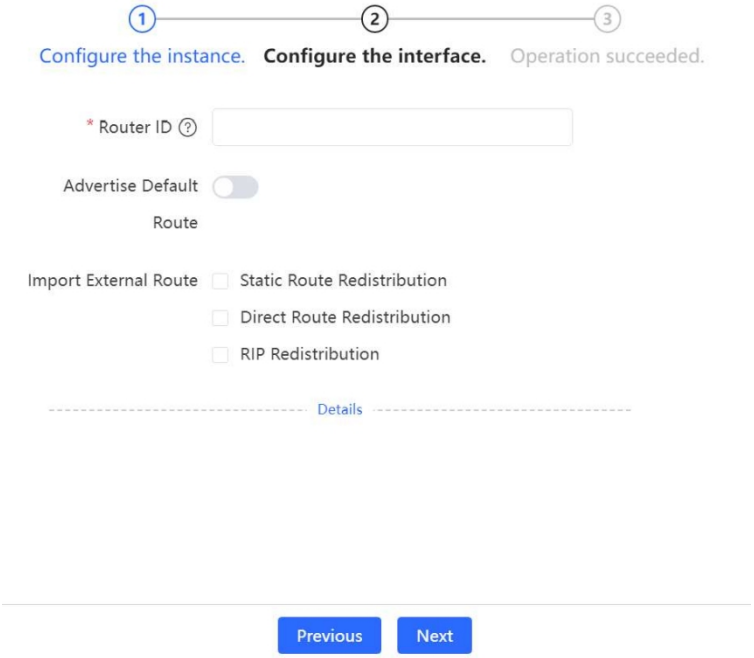
Метод Open Shortest Path First (OSPF) можна застосовувати у великих мережах. IPv4 використовує OSPFv2, а IPv6 - OSPFv3.

11.6.1 Налаштування основних параметрів OSPFv3

Виберіть **Локальний пристрій**> **Маршрутизація**> **OSPFv3**, натисніть Почати **налаштування**, а потім налаштуйте екземпляр та інтерфейс відповідно.

(1) Налаштуйте екземпляр.

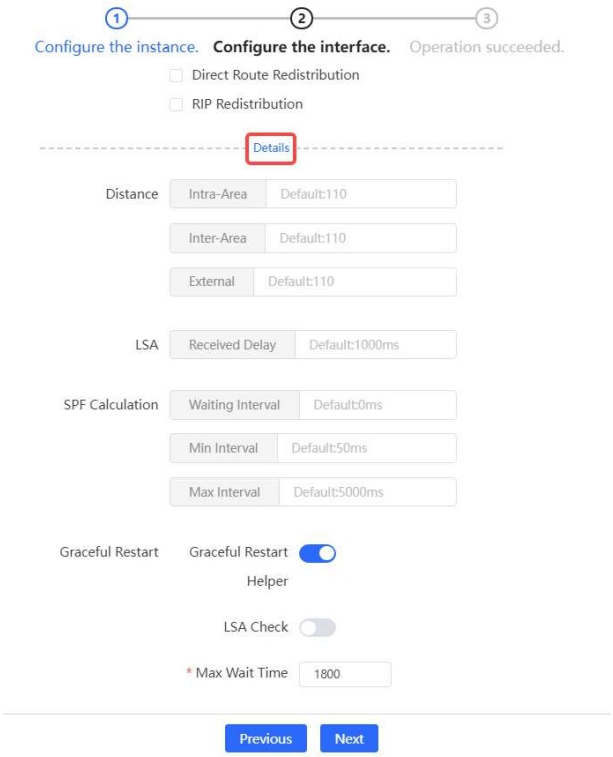




Таблиця 11-14 Параметри конфігурації екземпляра

Параметр	Опис
Ідентифікатор екземпляра	Створіть екземпляр OSPF основі типу служби. Екземпляр діє лише локально і не впливає на обмін пакетами з іншими пристроями.
Ідентифікатор маршрутизатора	Він ідентифікує маршрутизатор у домені OSPF. **Застереження** Ідентифікатори маршрутизаторів у межах одного домену мають бути унікальними. Однакова конфігурація може призвести до збоїв у виявленні сусідів.
Рекламувати маршрут за замовчуванням	Згенеруйте маршрут за замовчуванням і надішліть його сусідові. Після ввімкнення цієї функції вам потрібно ввести метрику і вибрати тип. За замовчуванням метрика дорівнює **1**. Тип 1: Показники, що відображаються на різних маршрутизаторах, відрізняються. Тип 2: Показники, що відображаються на всіх маршрутизаторах, однакові.
Імпорт Зовнішній маршрут	Перерозподіл маршрутів інших протоколів в домені OSPF для взаємодії з іншими доменами маршрутизації. Якщо вибрано **Статичний перерозподіл маршрутів**, введіть метрику, яка за замовчуванням дорівнює **20**. Якщо вибрано **Прямий перерозподіл маршрутів**, введіть метрику, яка за замовчуванням дорівнює **20**. Якщо вибрано RIP-перерозподіл, введіть метрику, яка за замовчуванням дорівнює **20**.

Параметр	Опис
Деталі	Розгорніть детальну конфігурацію.

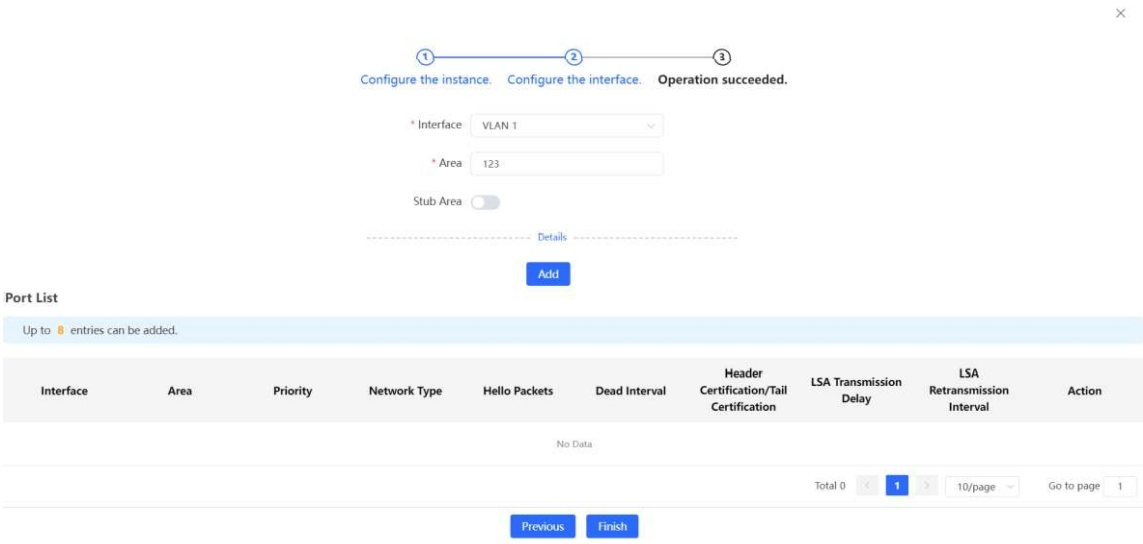


Таблиця 11-15 Параметри у детальній конфігурації екземпляра

Параметр	Опис
Відстань	Використовується для вибору протоколу. За замовчуванням, внутрішні, міжобласні та зовнішні відстані дорівнюють **110**.
LSA	Часті зміни мережі та перемикання маршрутів можуть займати занадто багато пропускної здатності мережі та ресурсів пристрою. Затримки генерації та отримання LSA визначені в OSPF за замовчуванням. Значення за замовчуванням - 1000 мс.
Розрахунок SPF	Коли база даних стану каналу (LSDB) змінюється, OSPF перераховує найкоротший шлях і встановлює інтервал, щоб запобігти частим змінам мережі, які займають велику кількість ресурсів **Інтервал очікування**: Коли стан змінюється, таймер спрацьовує. Затримка обчислюється вперше після закінчення таймера. Значення за замовчуванням - 0 мс. **Мінімальний інтервал**: Зі збільшенням кількості змін час кожного інтервалу буде збільшуватися відповідно до алгоритму, і значення за замовчуванням становить 50 мс. **Максимальний інтервал**: Коли розрахований інтервал досягає максимального інтервалу, значення

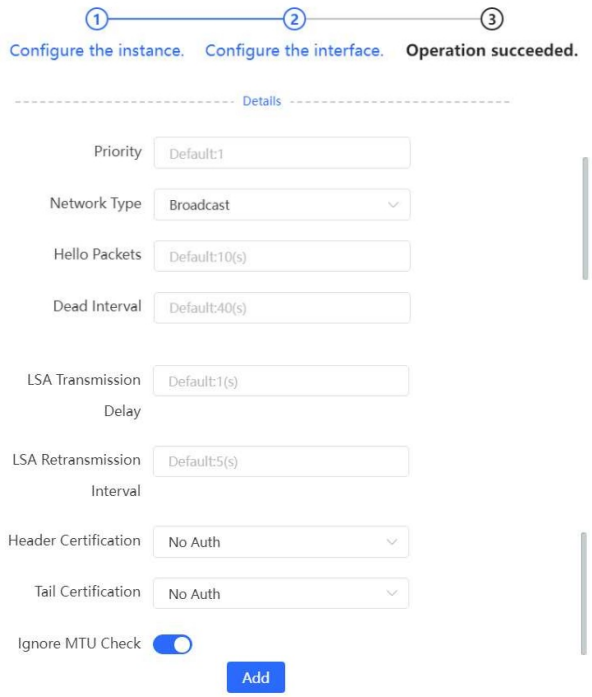
Параметр	Опис
	наступний інтервал завжди дорівнює максимальному інтервалу. Якщо час від останнього розрахунку перевищує максимальний інтервал, а LSDB не оновлюється, таймер вимикається.
Граціозний перезапуск	Плавний перезапуск (GR) дозволяє уникнути перекидання маршруту, спричиненого перериванням трафіку та перемиканням активної/резервної плати, забезпечуючи тим самим стабільність ключових сервісів. **Помічник плавного перезапуску**: Якщо цей перемикач увімкнено, вмикається функція Помічник плавного перезапуску. **Перевірка LSA**: Коли цей перемикач увімкнено, перевіряються пакети LSA за межами домену. **Максимальний час очікування**: відлік часу починається після того, як пристрій отримує пакет GR від однорангового пристрою. Якщо одноранговий пристрій не завершує GR протягом **максимального часу очікування**, пристрій виходить з режиму помічника GR. Значення за замовчуванням - 1800 секунд.

(2) **Налаштуйте інтерфейс.**



Таблиця 11-16 Параметри конфігурації інтерфейсу

Параметр	Опис
Інтерфейс	Виберіть інтерфейс 3-го рівня з підтримкою OSPF.
Площа	Налаштуйте ідентифікатор області. Діапазон значень: 0-4294967295
Область заглушки	Якщо увімкнено опцію **Stub Area**, вам потрібно налаштувати тип області та ізоляцію міжобласних маршрутів. Заглушка: Маршрутизатори на краю області не рекламують маршрути за її межами, а таблиця маршрутизації в цій області невелика. Не дуже заросла територія (NSSA): Можна імпортувати кілька зовнішніх маршрутів.
Деталі	Розгорніть детальну конфігурацію.



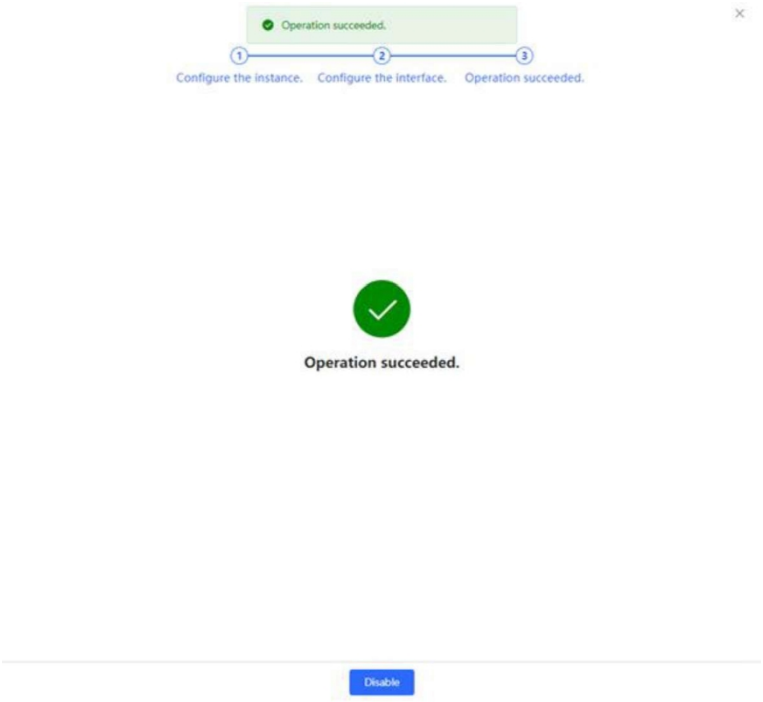
Таблиця 11-17 Параметри у детальній конфігурації інтерфейсу

Параметр	Опис
Пріоритет	За замовчуванням дорівнює 1.
Тип мережі	Трансляція Одноадресна багатоадресна Мультиплексний доступ до нерозповсюджуваного контенту
Привіт, пакети	Інтервал для періодичної передачі, який використовується для виявлення і підтримки відносин з сусідами OSPF. Значення за замовчуванням - 10 секунд.
Мертвий інтервал	Час, через який сусід стає недійсним. Значення за замовчуванням - 40 секунд.
Затримка передачі LSA	Затримка передачі LSA інтерфейсу. Значення за замовчуванням - 1 секунда.
Інтервал ретрансляції LSA	Час, через який LSA повторно передається після втрати LSA. Значення за замовчуванням - 5 секунд.
Сертифікація заголовків	Без перевірки **auth**:default. **MD5 auth**: Перевіряє повідомлення протоколу. Секретний ключ автентифікації шифрується за допомогою MD5 і передається разом з повідомленням протоколу. **SHA1 auth**: Перевіряє повідомлення протоколу. Секретним ключем аутентифікації є

	зашифровані за допомогою SHA1 і передаються разом з протоколом

Параметр	Опис
	повідомлення. **SHA256 auth**: Перевіряє повідомлення протоколу. Секретний ключ автентифікації шифрується за допомогою SHA256 і передається разом з повідомленням протоколу. Після вибору автентифікації MD5, SHA1 або SHA256 вам потрібно ввести Kid і Key. Серед них Kid - це ідентифікатор ключа, а Key - власне секретний ключ, що використовується.
Сертифікація хвоста	Без перевірки **auth**:default. **MD5 auth**: Перевіряє повідомлення протоколу. Секретний ключ автентифікації шифрується за допомогою MD5 і передається разом з повідомленням протоколу. **SHA256 auth**: Перевіряє повідомлення протоколу. Секретний ключ автентифікації шифрується за допомогою SHA256 і передається разом з повідомленням протоколу. Після вибору автентифікації MD5, SHA1 або SHA256 вам потрібно ввести Kid і Key. Серед них Kid - це ідентифікатор ключа, а Key - власне секретний ключ, що використовується.
Авторизація інтерфейсу	**Без** автентифікації: пакети протоколу не автентифікуються. Це за замовчуванням. **Звичайний текст**: Пакети протоколу автентифікуються, а ключ автентифікації передається з пакетами протоколу у вигляді простого тексту. **MD5**: Пакети протоколу автентифікуються, а ключ автентифікації зашифровується в MD5 і передається разом з пакетами протоколу.
Ігнорувати перевірку MTU	Увімкнено за замовчуванням.

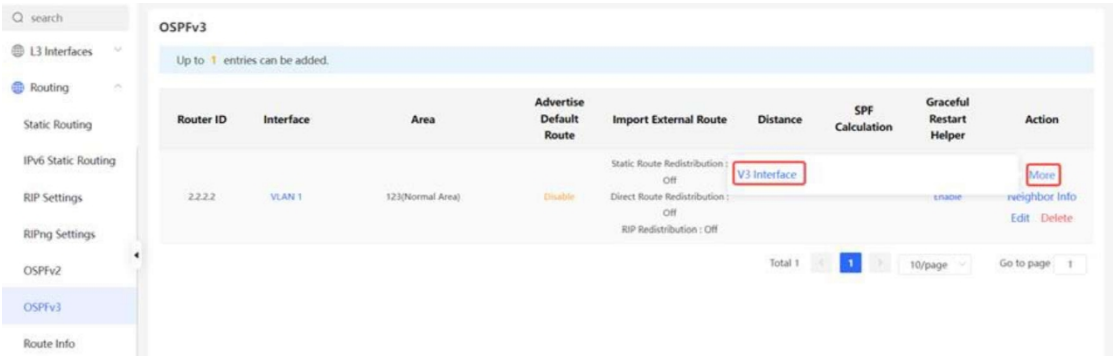
(3) Завершіть конфігурацію.

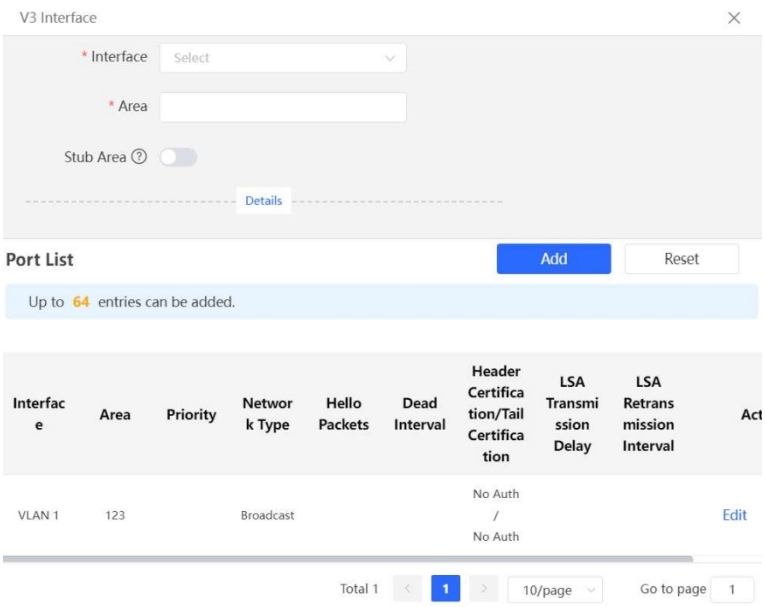


Після завершення налаштування ви можете вибрати **Локальний пристрій**> **Маршрутизація**> OSPFv3 і переглянути список екземплярів.

11.6.2 Додавання інтерфейсу OSPFv3

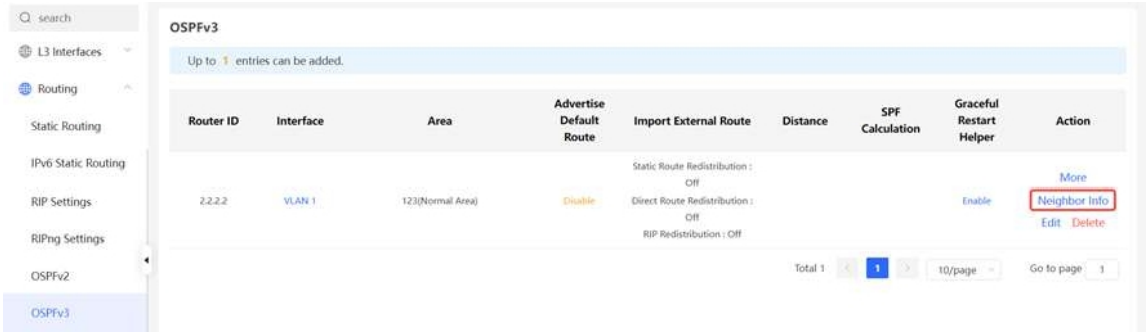
Виберіть **Локальний пристрій**> **Маршрутизація**> **OSPFv3**, натисніть **Більше** у колонці **Дія** і виберіть **Інтерфейс V3**.

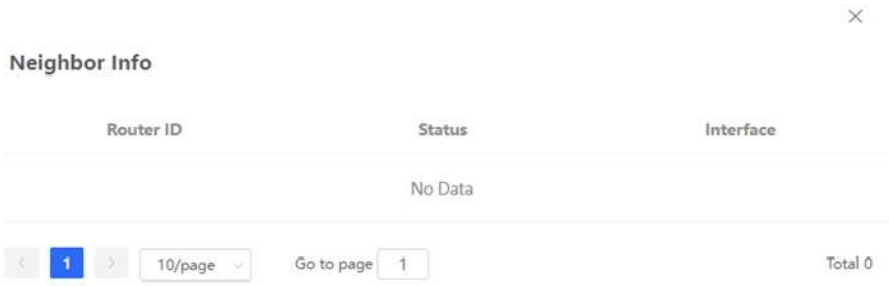




11.6.3 Перегляд інформації про сусідів OSPFv3

Виберіть **Локальний пристрій**> **Маршрутизація**> OSPFv3 і натисніть **Інформація про сусіда** у колонці **Дія**.

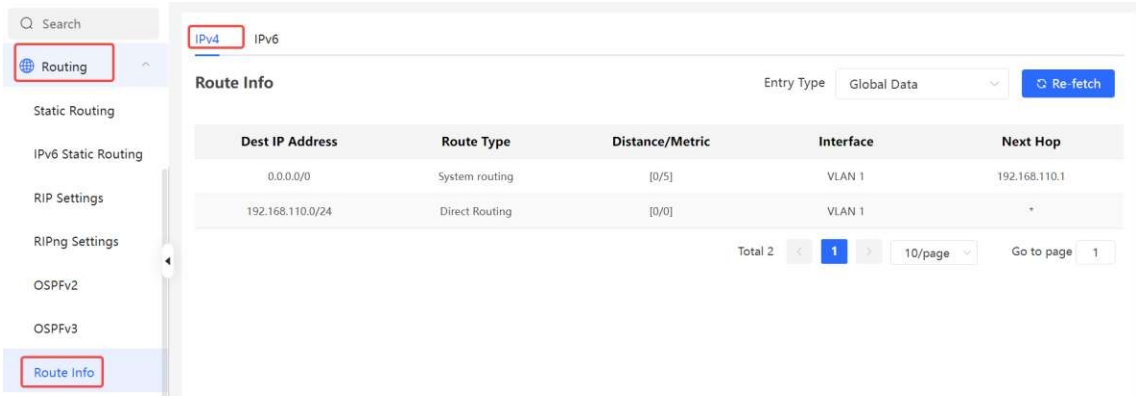




11.7 Інформація про таблицю маршрутизації

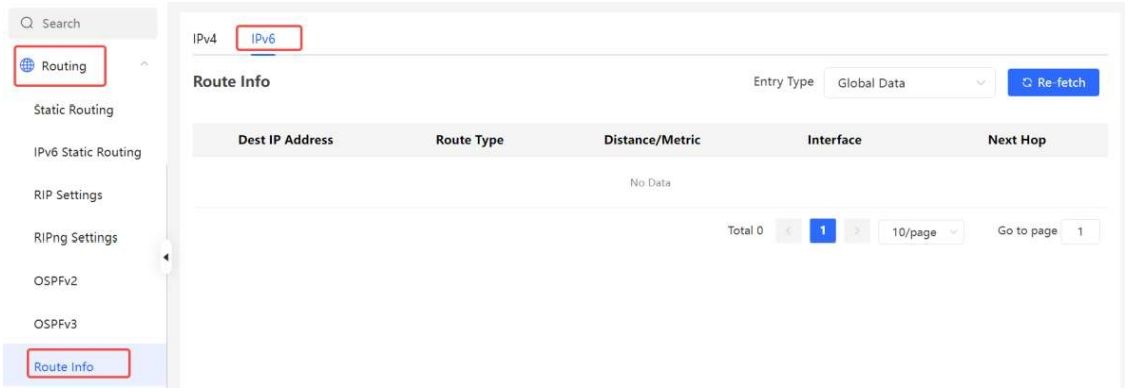
1. Інформація про маршрут IPv4

Виберіть **Локальний пристрій> Маршрутизація > Інформація про маршрут >** IPv4, щоб переглянути деталі таблиці маршрутизації IPv4.



2. Інформація про маршрут IPv6

Виберіть **Локальний пристрій > Маршрутизація > Інформація про маршрут> IPv6**, щоб переглянути деталі таблиці маршрутизації IPv6.



12 Перегляд інформації про оптичний приймач

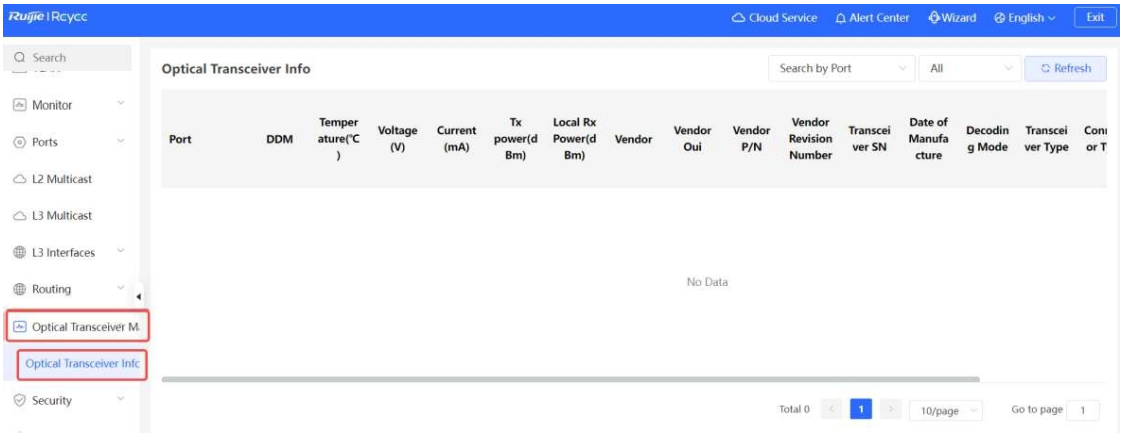
Специфікація

Інформація залежить від конкретного продукту.

Виберіть **Локальний пристрій> Моніторинг оптичного приймача> Інформація про оптичний приймач**.

На сторінці **Інформація** про **оптичний трансивер** відображається основна інформація про оптичний трансивер, зокрема порт, до якого він підключений, DDM, температура, напруга, струм, потужність Tx, локальна потужність Rx і так далі. Ви можете запросити інформацію про оптичний трансивер, ввівши порт, до якого він підключений, у вікно пошуку.

Дані на цій сторінці автоматично оновлюються кожні 5 секунд. Ви також можете натиснути кнопку **Оновити**, щоб оновити інформацію про оптичний приймач.



13 Безпека

13.1 DHCP Snooping

13.1.1 Огляд

Функція прослуховування протоколу динамічної конфігурації хоста (DHCP) дозволяє пристрою прослуховувати DHCP-пакети, якими обмінюються клієнти та сервер, щоб записувати та контролювати використання IP-адрес і відфільтровувати недійсні DHCP-пакети, включно з пакетами запитів від клієнтів і пакетами відповідей від сервера. DHCP-шпигун записує згенеровані користувацькі дані для використання у програмах безпеки, таких як IP Source Guard.

13.1.2 Конфігурація автономного пристрою

Виберіть **Локальний пристрій> Безпека> DHCP Snooping**.

Увімкніть функцію DHCP-сканування, виберіть порт, який потрібно додати до довірених портів, на панелі портів і натисніть кнопку **Зберегти**. Після увімкнення DHCP Snooping пакети запитів від DHCP-клієнтів пересилатимуться лише на довірені порти, а пакети відповідей від DHCP-серверів пересилатимуться лише з довірених портів.

Примітка

Як правило, порт висхідного каналу, підключений до DHCP-сервера, налаштовано як довірений порт.

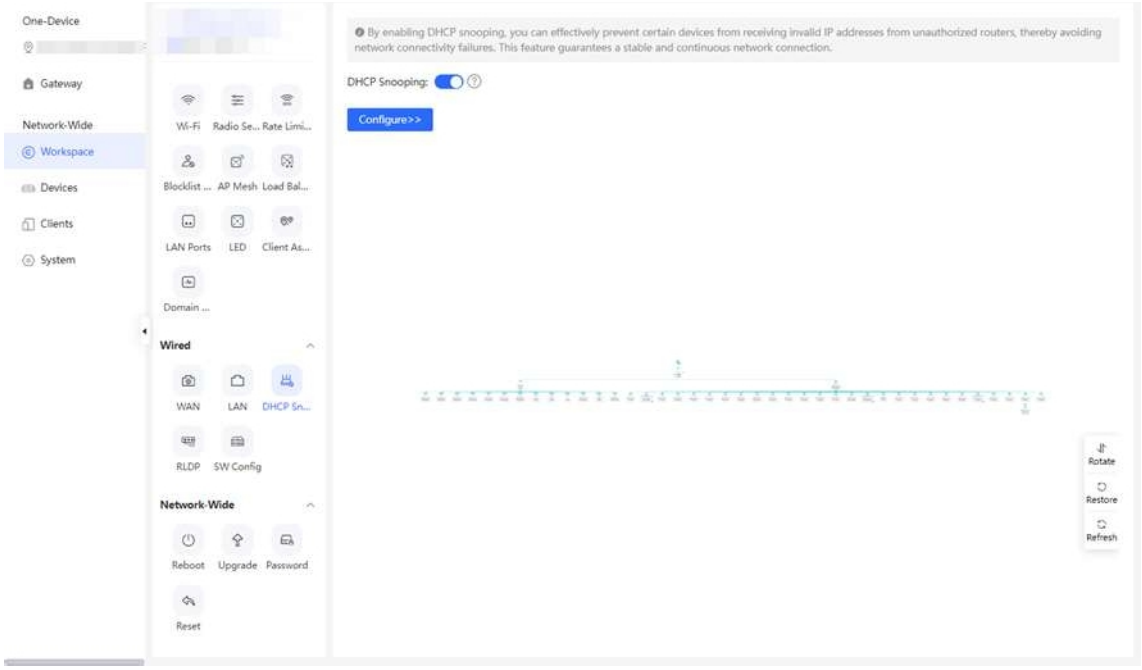
Параметр 82 використовується для підвищення безпеки DHCP-сервера та оптимізації політики призначення IP-адрес. Інформація про опцію 82 буде міститися у пакеті запиту DHCP, якщо опцію 82 увімкнено.

13.1.3 Пакетне налаштування мережевих комутаторів

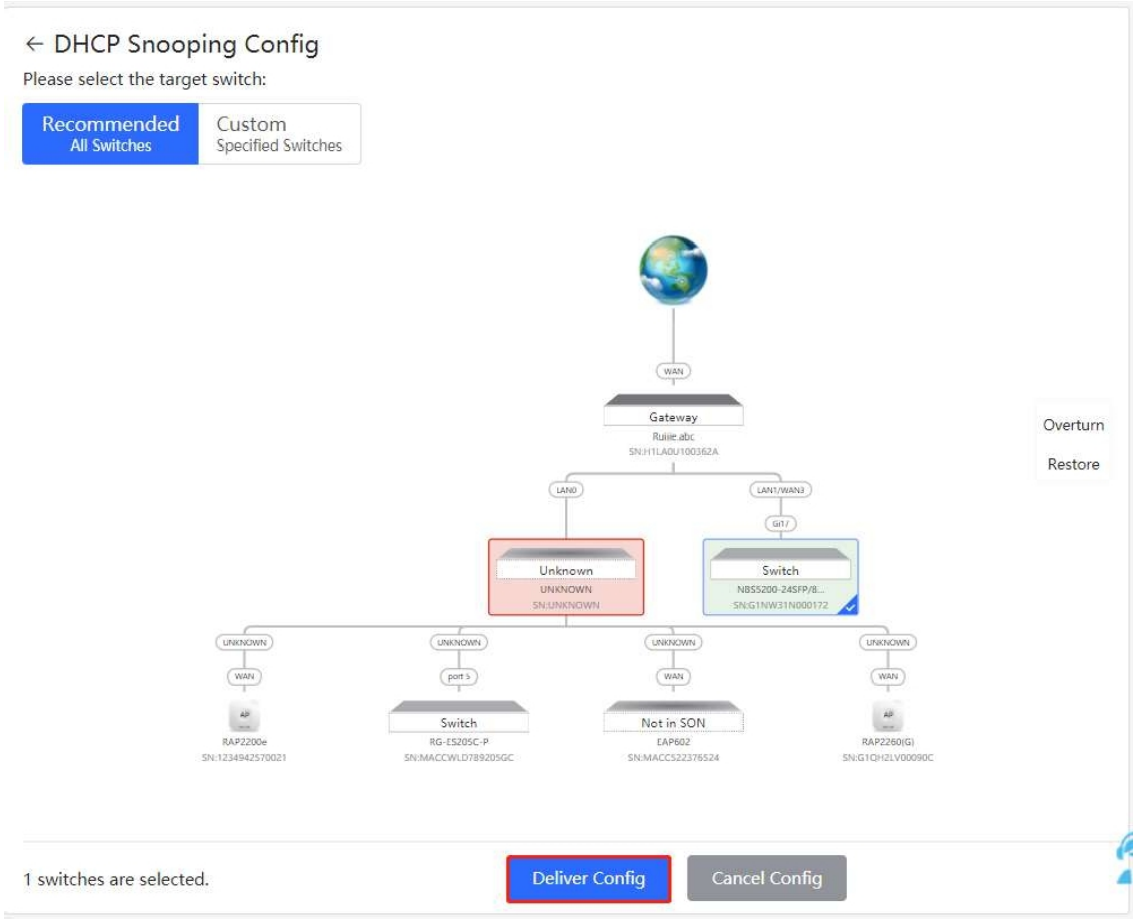
Виберіть **Мережевий> Робочий простір Дротовий> > DHCP Snooping**.

Увімкнення DHCP Snooping на мережевих комутаторах може гарантувати, що користувачі зможуть отримувати параметри мережевої конфігурації від DHCP-сервера лише в межах діапазону контролю, а також уникнути отримання хостом у вихідній мережі IP-адреси, призначеної несанкціонованим маршрутизатором, щоб гарантувати стабільність мережі.

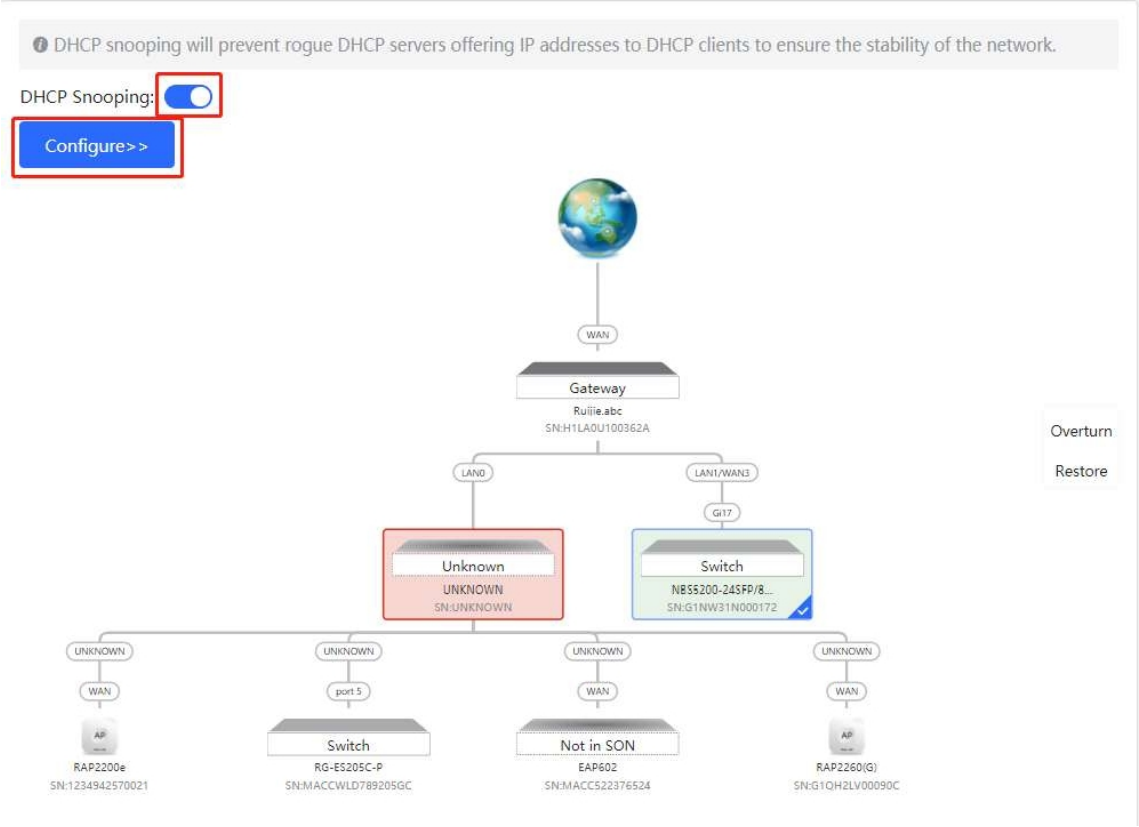
(1) Натисніть **Увімкнути**, щоб перейти на сторінку **налаштування DHCP Snooping**.



(2) У топології мережі ви можете вибрати комутатори доступу, на яких ви хочете ввімкнути DHCP Snooping у рекомендованому або користувацькому режимі. Якщо ви виберете рекомендований режим, всі комутатори в мережі будуть обрані автоматично. Якщо ви виберете користувацький режим, ви зможете вручну вибрати потрібні комутатори. Натисніть **Надати конфігурацію**. На вибраних комутаторах буде увімкнено DHCP Snooping.



(3) Після того, як конфігурацію буде доставлено, якщо вам потрібно змінити діапазон дії функції захисту приватних з'єднань, натисніть **Налаштувати**, щоб повторно вибрати комутатор, який увімкне захист приватних з'єднань у топології. Після конфігурації, якщо вам потрібно змінити діапазон дії функції DHCP Snooping, натисніть **Налаштувати**, щоб знову вибрати потрібні комутатори в топології. Вимкнути **DHCP Snooping**, щоб вимкнути DHCP Snooping на всіх комутаторах одним клацанням миші.



13.2 Штормовий контроль

13.2.1 Огляд

Коли локальна мережа (LAN) має надлишкові широкомовні, багатоадресні або невідомі одноадресні потоки даних, швидкість мережі сповільнюється, а передача пакетів має підвищену ймовірність тайм-ауту. Це називається "шторм у локальній мережі", який може бути спричинений помилками у виконанні топологічного протоколу або неправильною конфігурацією мережі.

Користувачі можуть виконувати штормовий контроль окремо для широкомовних, багатоадресних і невідомих одноадресних потоків даних. Коли швидкість широкомовних, багатоадресних або невідомих одноадресних потоків даних, отриманих через порт пристрою, перевищує заданий діапазон, пристрій передає лише пакети в межах зазначеного діапазону і відкидає пакети, що виходять за межі діапазону, доки швидкість пакета не впаде в межах діапазону. Це запобігає потраплянню переповнених даних у локальну мережу та спричиненню "шторму".

13.2.2 Процедура

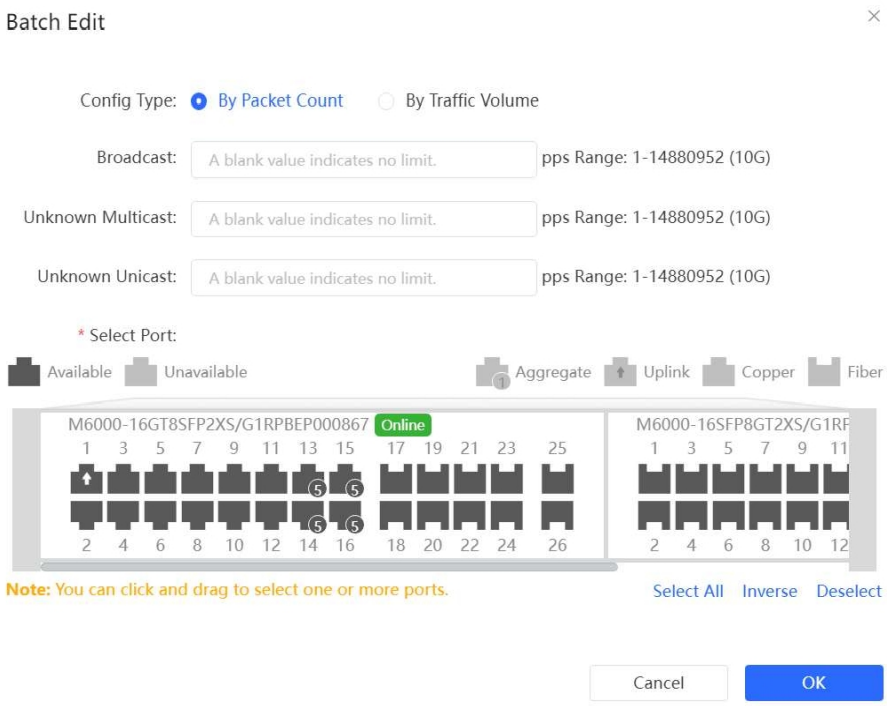
Виберіть **Локальний пристрій**> **Безпека**> **Контроль шторму**.

Натисніть **Пакетне редагування**. У діалоговому вікні, що з'явиться, виберіть типи конфігурації і порти, введіть обмеження швидкості для широкомовної передачі, невідомої багатоадресної передачі і невідомої

одноадресної передачі та натисніть **кнопку OK**. Щоб змінити або видалити правила обмеження швидкості після завершення конфігурації, ви можете натиснути кнопку **Змінити** або **Видалити** у стовпчику **Дія**.

Існує два типи конфігурацій:

- Контроль шторму на основі пакетів в секунду: якщо швидкість потоків даних, що надходять через порт пристрою, перевищує налаштований поріг пакетів в секунду, надлишкові потоки даних відкидаються до тих пір, поки швидкість не знизиться до порогового значення.
- Контроль шторму на основі кілобайтів на секунду: якщо швидкість потоків даних, що надходять через порт пристрою, перевищує налаштований поріг у кілобайтах на секунду, надлишкові потоки даних відкидаються доти, доки швидкість не впаде до порогового значення.



13.3 ACL

13.3.1 Огляд

Список контролю доступу (ACL) в деяких документах часто називають фільтром пакетів. ACL визначає низку правил дозволу або заборони і застосовує ці правила до інтерфейсів пристроїв для контролю пакетів, що надсилаються на інтерфейси та з них, щоб підвищити безпеку мережевого пристрою.

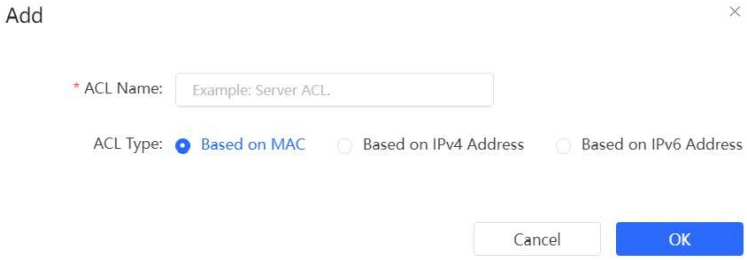
Ви можете додавати ACL на основі MAC-адрес або IP-адрес і прив'язувати ACL до портів.

13.3.2 Створення правил ACL

Виберіть **Локальний пристрій**> **Безпека**> **ACL**> **Список ACL**.

(1) Натисніть **Додати**, щоб задати тип контролю ACL, введіть ім'я ACL і натисніть кнопку **OK**.

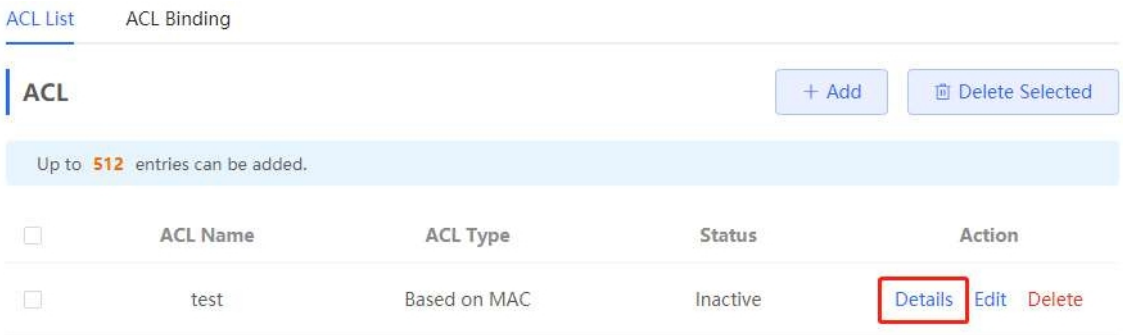
- На основі MAC-адреси: Для керування пакетами 2-го рівня, що входять/виходять з порту, а також для заборони або дозволу певних пакетів 2-го рівня, призначених для мережі.
- На основі IP-адреси: Керування пакетами Ipv4, що входять/виходять з порту, а також заборона або дозвіл певних пакетів Ipv4, призначених для мережі.

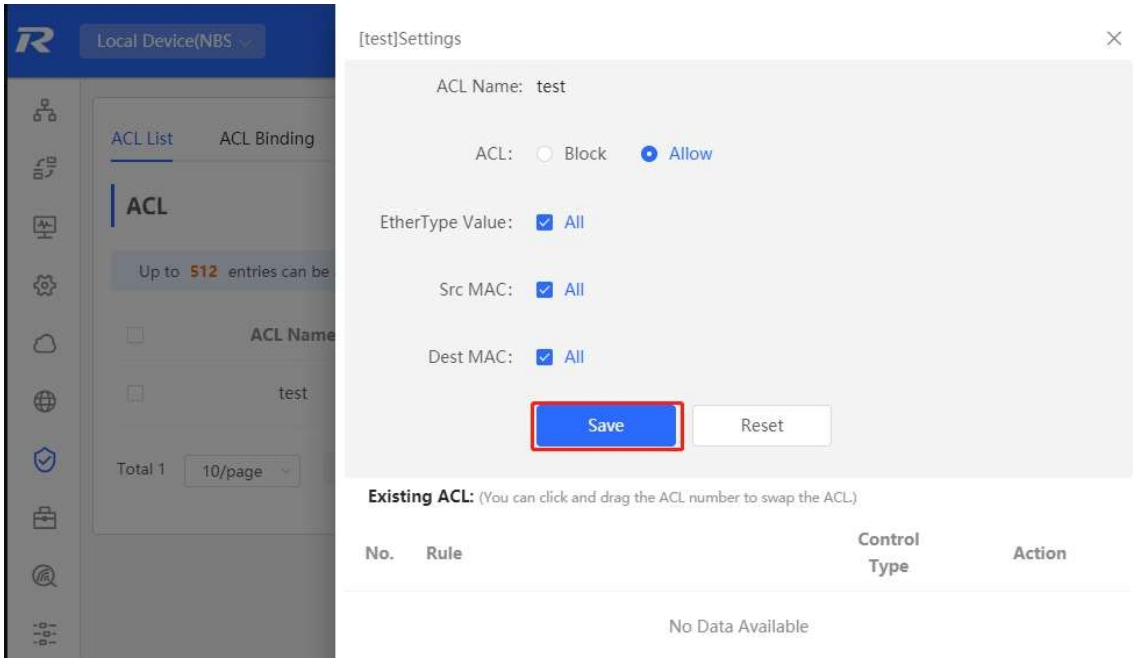


(2) Натисніть **Деталі** в стовпчику **Дія** для запису ACL, встановіть правила фільтрації у спливаючій бічній панелі та натисніть

Збережіть, щоб додати правила для ACL. Можна додати кілька правил.

Правила включають дві дії: **дозволити** або **заблокувати**, а також правила відповідності пакетів. Послідовність правила в ACL визначає пріоритет правила в ACL. Під час обробки пакетів мережевий пристрій порівнює пакети з ACE на основі порядкових номерів правил. Натисніть **Перемістити** у списку правил, щоб змінити порядок зіставлення.





Таблиця 13-1 Опис параметрів конфігурації правил ACL

Параметр	Опис
ACL	Налаштування дії правил ACL Блокувати: Якщо пакети відповідають цьому правилу, їх буде відхилено. Дозволити: Якщо пакети відповідають цьому правилу, пакети дозволяються.
Номер IP-протоколу	Відповідність номеру IP-протоколу Значення в діапазоні від 0 до 255. Позначте **Всі**, щоб зіставити всі IP-протоколи.
Src IP-адреса	Зіставити IP-адресу джерела з пакетом. Позначте пункт **Усі**, щоб зіставити всі IP-адреси джерела.
IP-адреса призначення	Зіставити IP-адресу призначення пакета. Позначте **Всі**, щоб зіставити всі IP-адреси призначення
Значення EtherType	Відповідність типу протоколу Ethernet. Діапазон значень 0x600~0xFFFF. Позначте пункт **Усі**, щоб збігалися всі номери типів протоколів.
Сержант Мак.	Зіставити MAC-адресу хоста-джерела. Позначте **Всі**, щоб зіставити всі MAC-адреси джерела
Місцезнаходження MAC	Зіставити MAC-адресу хоста призначення. Позначте **Всі**, щоб зіставити всі MAC-адреси призначення

Примітка

- Списки ACL не можуть мати однакові назви. Редагувати можна лише назву створеного ACL.
- ACL, застосований портом, не можна редагувати або видаляти. Щоб редагувати, спочатку відв'яжіть ACL від порту. ● Існує одне правило ACL за замовчуванням, яке забороняє всі пакети, приховані в кінці ACL.

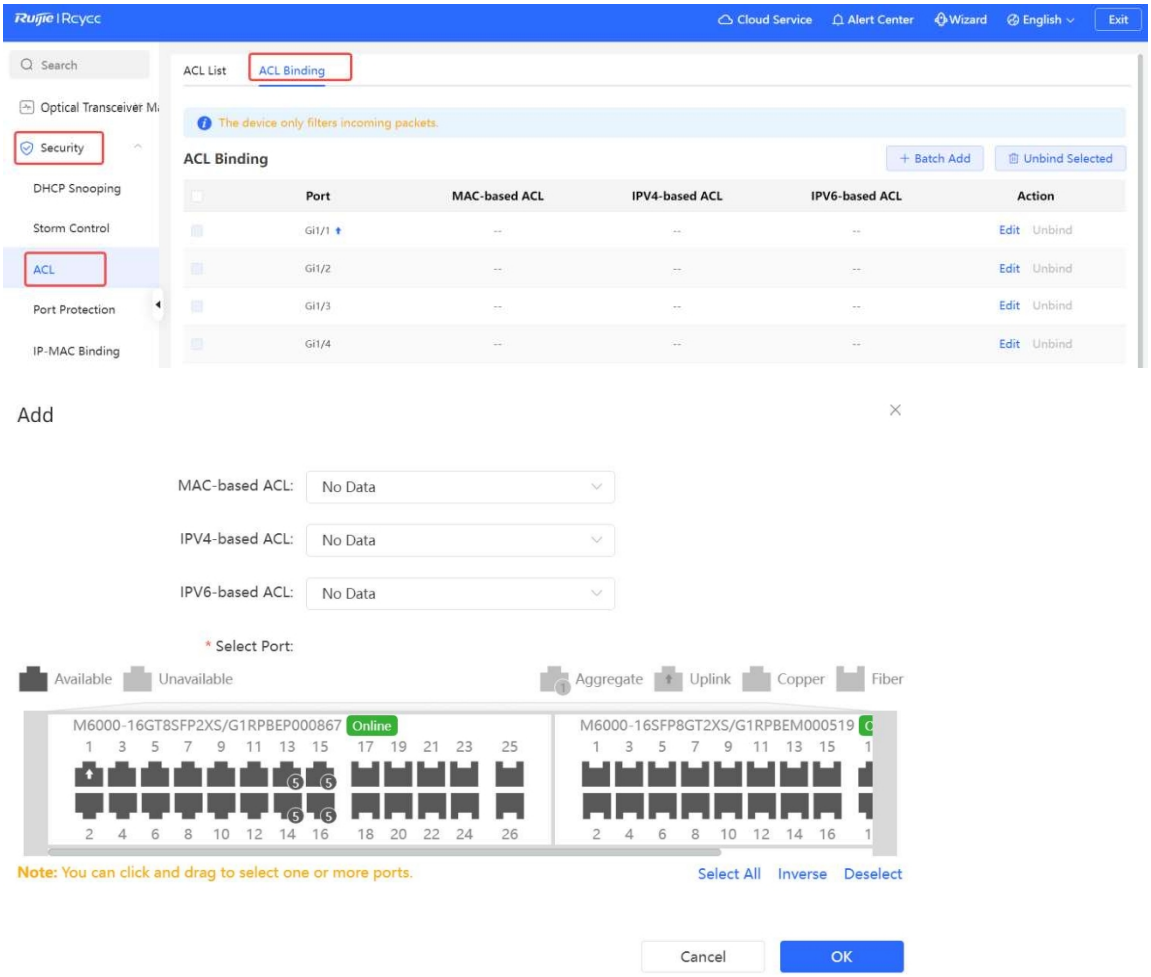
13.3.3 Застосування правил ACL

Виберіть **Локальний пристрій**> **Безпека**> **ACL**> **Список ACL**.

Натисніть **Пакетне додавання** або **редагування** у стовпчику **Дія**, виберіть потрібні MAC ACL і IP ACL для портів і натисніть **OK**.

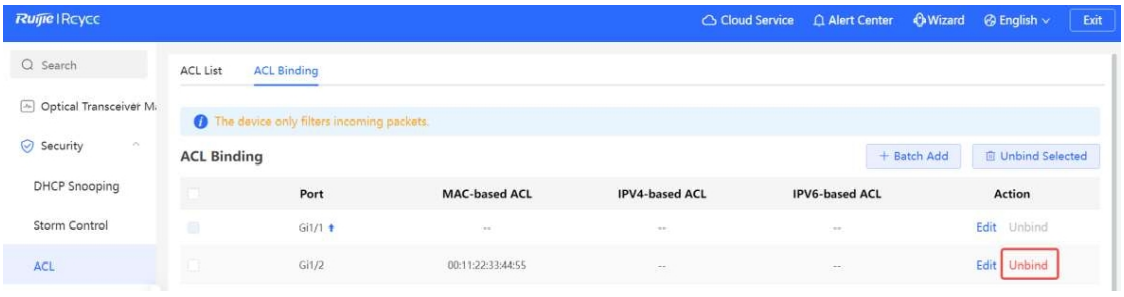
Примітка

Наразі ACL можна застосовувати лише у вхідному напрямку портів, тобто для фільтрації вхідних пакетів.



Після застосування ACL до порту ви можете натиснути кнопку Відв**'язати** у стовпчику **Дія** або перевірити запис про порт і натиснути

Видалити Вибрано, щоб відв'язати ACL від порту.

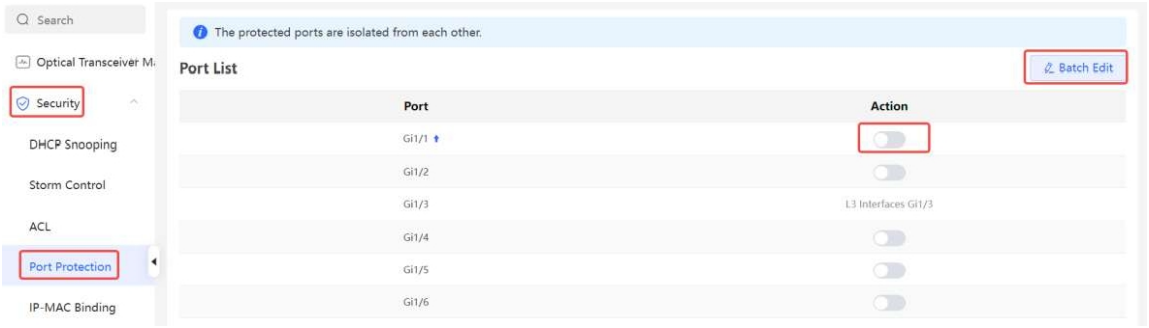


13.4 Захист портів

Виберіть **Локальний пристрій> Безпека> Захист портів**.

У деяких сценаріях потрібно, щоб зв'язок між деякими портами на пристрої було вимкнено. Для цього ви можете налаштувати деякі порти як захищені. Порти, на яких увімкнено захист портів (захищені порти), не можуть взаємодіяти один з одним, користувачі на різних портах ізольовані на 2-му рівні. Захищені порти можуть взаємодіяти з незахищеними портами.

За замовчуванням захист портів вимкнено, але його можна увімкнути, натиснувши кнопку пакетного увімкнення захисту портів для декількох портів, ви можете натиснути **кнопку Пакетне редагування**, щоб увімкнути захист портів**,** вибрати потрібний порт і натиснути **кнопку OK.**



13.5 Прив'язка IP-MAC

13.5.1 Огляд

Після налаштування IP-MAC прив'язки на порту, для підвищення безпеки, пристрій перевіряє, чи відповідають IP-адреси джерела і MAC-адреси джерела IP-пакетів тим, що налаштовані для пристрою, відфільтровує IP-пакети, що не відповідають прив'язці, і суворо контролює достовірність джерел вхідного сигналу.

13.5.2 Процедура

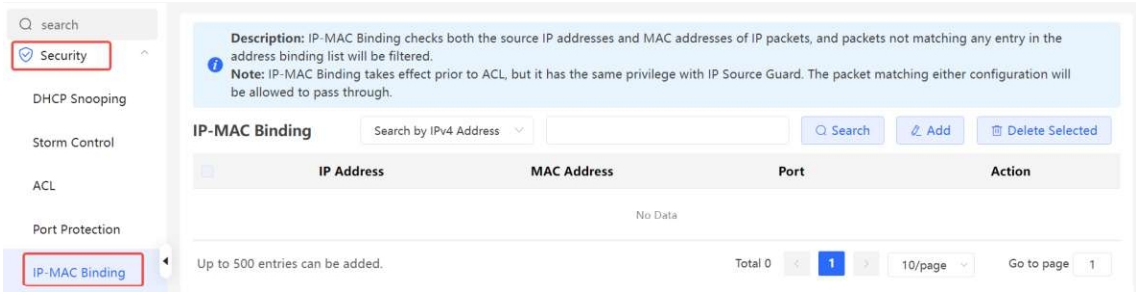
Виберіть **Локальний пристрій> Безпека> Прив'язка IP-MAC**.

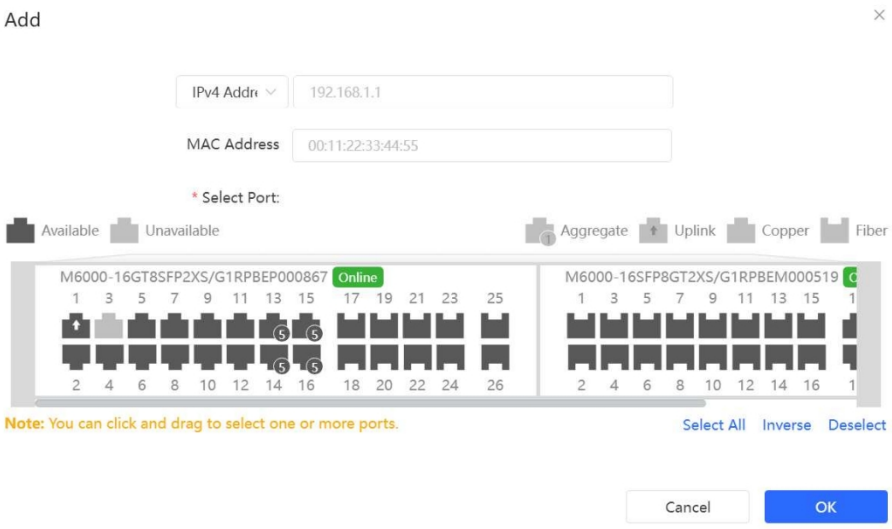
1. Додавання запису прив'язки IP-MAC

Натисніть **Додати**, виберіть потрібний порт, введіть IP-адресу та MAC-адресу для прив'язки і натисніть **OK**. Потрібно ввести хоча б одну з і MAC-адрес. Щоб змінити прив'язку, ви можете натиснути **Редагувати** в колонці **Дія**.

Застереження

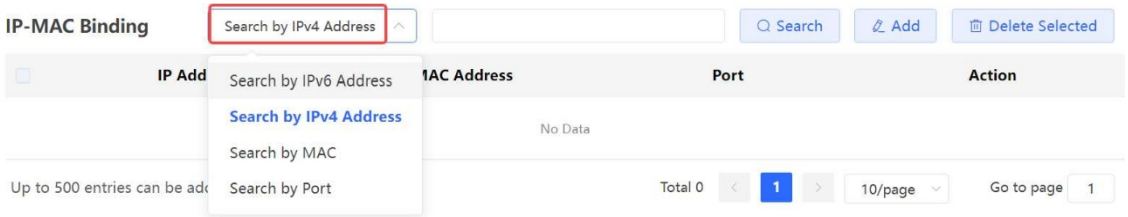
Прив'язка IP-MAC вступає в дію раніше, ніж ACL, але має ті ж самі привілеї, що і IP Source Guard. Пакети, що відповідають будь-якій з конфігурацій, буде пропущено.





2. Пошук записів зв'язування

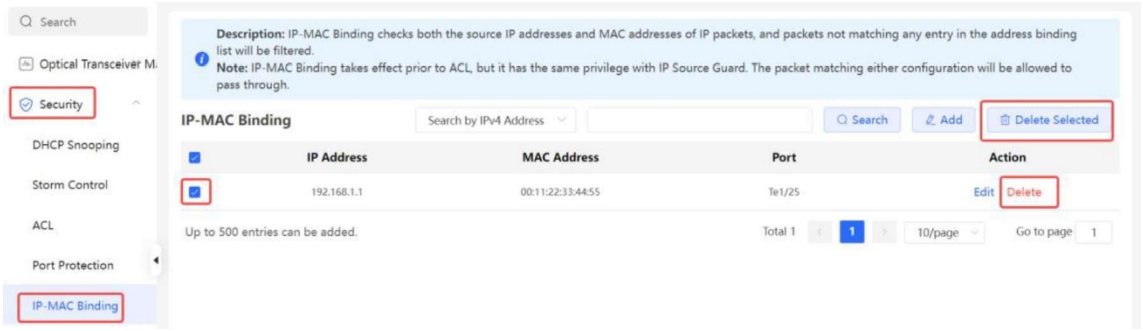
Поле пошуку у верхньому правому куті підтримує пошук записів прив'язок на основі IP-адрес, MAC-адрес або портів. Виберіть тип пошуку, введіть пошуковий рядок і натисніть **Пошук**. Записи, які відповідають критеріям пошуку, відображаються у списку.



3. Видалення запису прив'язки IP-MAC

Пакетне налаштування: У **списку IP-MAC прив'язок** виберіть запис, який потрібно видалити, і натисніть **Видалити вибране**. У діалоговому вікні натисніть **OK**.

Видаліть один запис прив'язки: натисніть кнопку **Видалити** в останньому стовпчику **Дія** для запису в списку. У діалоговому вікні, що з'явиться, натисніть **OK**.



13.6 Захист джерела IP-адреси

13.6.1 Огляд

Після увімкнення функції захисту IP-джерел пристрій перевіряє IP-пакети з ненадійних портів DHCP. Ви можете налаштувати пристрій на перевірку лише поля IP або поля IP+MAC, щоб відфільтрувати IP-пакети, які не відповідають списку прив'язок. Це може запобігти встановленню користувачами приватних IP-адрес і підробці IP-пакетів.

Застереження

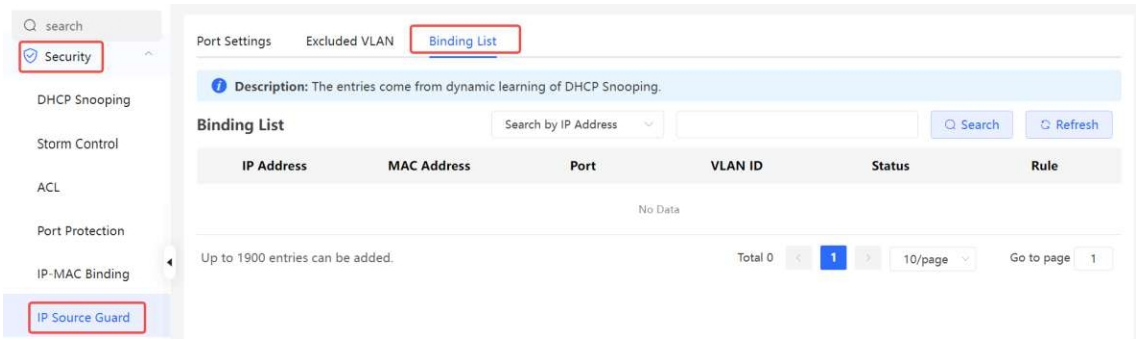
Захист IP-джерел слід увімкнути разом із DHCP-скануванням. Інакше це може вплинути на переадресацію IP-пакетів. Щоб налаштувати функцію DHCP Snooping, див. розділ 13.1 Відстеження DHCP для отримання докладніших відомостей.

13.6.2 Перегляд списку прив'язок

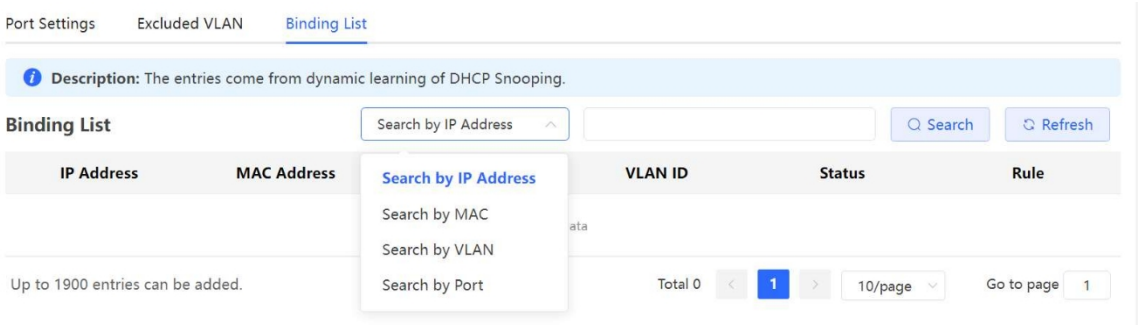
Виберіть **Локальний пристрій**> **Безпека**> **Захист IP-джерела**> **Список прив'язок**.

Список прив'язок є основою для IP Source Guard. Наразі дані у **списку прив'язок** отримуються з результатів динамічного навчання бази даних прив'язок DHCP Snooping. Коли IP Source Guard увімкнено, дані бази даних прив'язок DHCP Snooping синхронізуються зі списком прив'язок IP Source Guard. У цьому випадку IP-пакети фільтруються строго через IP Source Guard на пристроях з увімкненим DHCP Snooping.

Натисніть **Оновити**, щоб отримати останні дані у **списку прив'язок**.



Поле пошуку у верхньому правому куті дозволяє знайти вказаний запис у **списку прив'язок** за IP-адресами, MAC-адресами, VLAN або портами. Клацніть розкривний список, щоб вибрати тип пошуку, введіть пошуковий рядок і натисніть **Пошук**.



13.6.3 Увімкнення захисту джерела IP-адреси порту

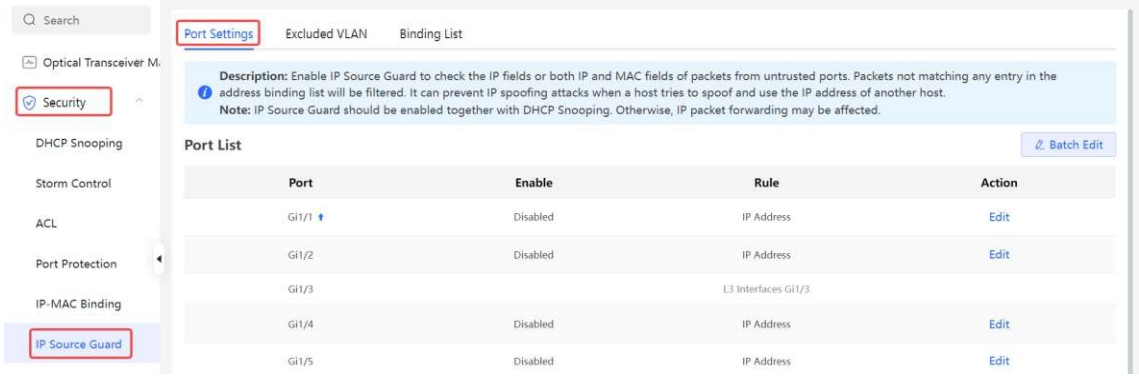
Виберіть **Локальний пристрій> Безпека> Захист IP-джерела> Основні налаштування**.

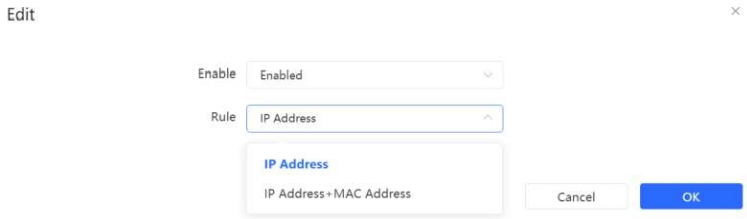
У Списку портів натисніть **Редагувати** у стовпчику **Дія**. Виберіть **Увімкнено**, виберіть правило зіставлення і натисніть **OK**. Існує два правила зіставлення:

- IP-адреса: Перевіряються вихідні IP-адреси всіх IP-пакетів, що проходять через порт. Пакетам дозволяється проходити через порт лише тоді, коли IP-адреси джерел цих пакетів збігаються зі списком прив'язки.
- IP-адреса + MAC-адреса: Перевіряються IP-адреси джерела та MAC-адреси IP-пакетів, що проходять порт. Пакети проходять через порт лише тоді, коли MAC-адреси джерела 2-го рівня та IP-адреси джерела 3-го рівня цих пакетів збігаються із записами у списку прив'язки.

Застереження

- IP Source Guard не можна ввімкнути на довіреному порту DHCP Snooping.
- IP Source Guard можна ввімкнути лише на інтерфейсі 2-го рівня.





13.6.4 Налаштування виняткових адрес VLAN

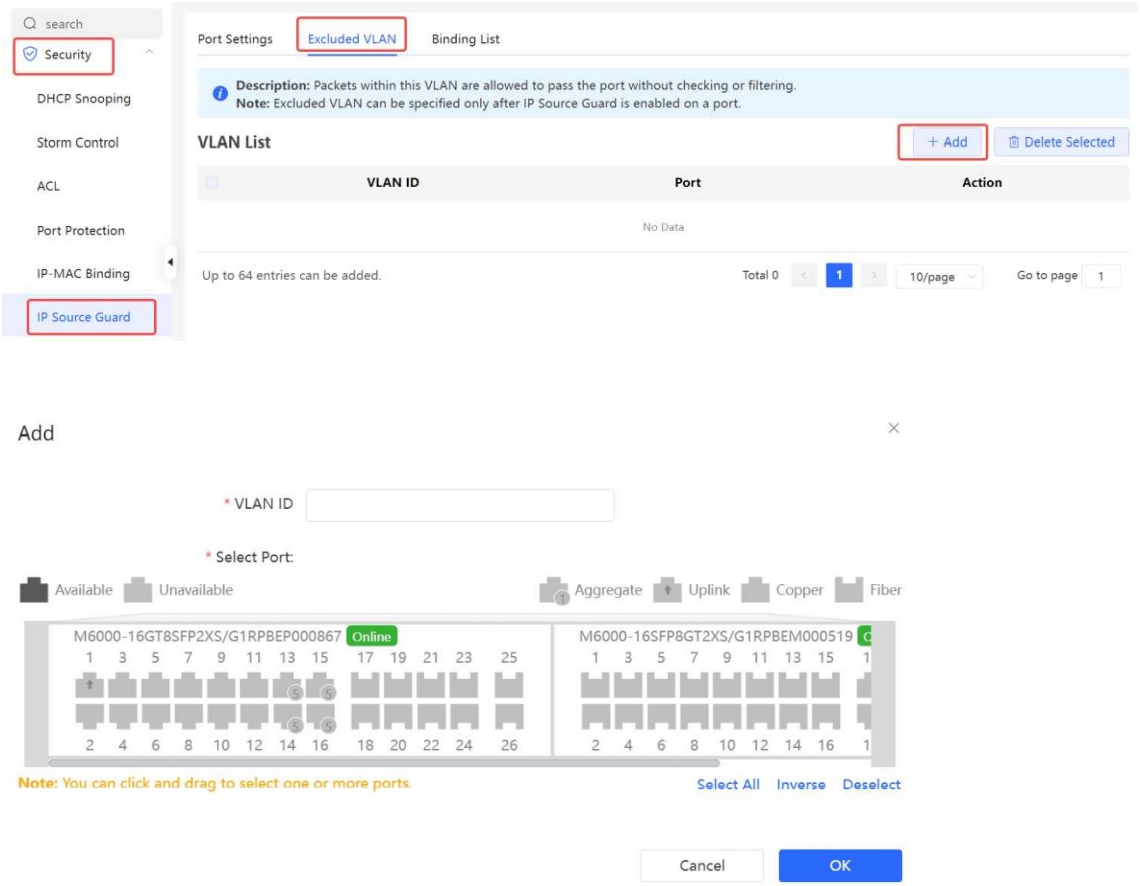
Виберіть **Локальний пристрій> Безпека> Захист IP-джерела> Виключена VLAN**.

Коли IP Source Guard увімкнено на інтерфейсі, за замовчуванням він діє для всіх віртуальних локальних мереж (VLAN), підключених до цього інтерфейсу. Користувачі можуть вказати виключені VLAN, в межах яких IP-пакети не перевіряються і не фільтруються, тобто такі IP-пакети не контролюються IP Source Guard.

Натисніть кнопку **Змінити**, введіть ідентифікатор виключеної VLAN і потрібний порт, а потім натисніть кнопку **ОК**.

Застереження

Виключені VLAN можна вказати на лише після того, як на ньому увімкнено IP Source Guard. Зазначені заборонені VLAN буде автоматично видалено, коли функцію IP Source Guard на порту буде вимкнено.



13.7 Налаштування автентифікації 802.1X

13.7.1 Введення функції

1. Огляд автентифікації IEEE 802.1X

IEEE 802.1X, стандарт IEEE для управління доступом до мережі на основі портів (PNAC), забезпечує захищену автентифікацію для безпечного доступу до локальних мереж. Його основна мета - визначення доступності порту. Якщо автентифікація пройшла успішно, IEEE 802.1X вмикає порт. В іншому випадку порт відключається.

У традиційній локальній мережі, сумісній зі стандартом IEEE 802, користувачі можуть отримати доступ до мережевих ресурсів без автентифікації, що створює ризики для безпеки. Саме тут з'являється IEEE 802.1X.

У порівнянні з традиційними методами доступу, IEEE 802.1X має наступні переваги:

- Безпека і надійність: Автентифікація IEEE 802.1X виконується для користувача або пристрою перед тим, як вони отримають доступ до комутатора або послуг локальної мережі. Дані можуть проходити через порти Ethernet тільки після успішної аутентифікації.
- Ідентифікація користувачів: Автентифікація особистості запобігає доступу неавторизованих користувачів і пристроїв до локальних і бездротових мереж, а також реєструє час їхнього входу і виходу з мережі.
- Проста та ефективна якість: IEEE 802.1X використовує технологію Ethernet, щоб зберегти природу IP-мереж без підключення, зменшуючи непотрібні накладні витрати і надмірність.

IEEE 802.1X забезпечує автентифікацію, авторизацію та облік (AAA) для додатків безпеки.

- Автентифікація: Визначає, чи може користувач отримати доступ до мережевих ресурсів, і відмовляє неавторизованим користувачам.
- Авторизація: Надає користувачам доступ до ресурсів і контролює дозволи авторизованих користувачів. ○ Облік: Записує мережеві ресурси, використані користувачами, для подальшого обліку.

IEEE 802.1X можна розгортати в мережах для контролю доступу користувачів, аутентифікації користувачів і авторизації послуг.

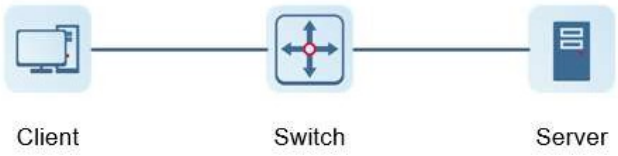
Примітка

Комутатори серії RG-NBS підтримують тільки аутентифікацію.

2. Архітектура автентифікації IEEE 802.1X

IEEE 802.1X має типову модель клієнт-сервер, яка складається з трьох елементів: клієнт, пристрій доступу до мережі та сервер автентифікації, як показано на рисунку 13-1 Типова архітектура IEEE 802.1X. Контроль доступу а також автентифікація та авторизація клієнтського пристрою можуть бути реалізовані тільки тоді, коли всі три об'єкти беруть участь в автентифікації IEEE 802.1X.

Рисунок 13-1 Типова архітектура IEEE 802.1X



- Клієнт автентифікації: Вказує на клієнтський пристрій, який підключається до мережі та ініціює автентифікацію доступу, наприклад, ПК. Користувачі повинні увімкнути клієнти автентифікації IEEE 802.1X на своїх пристроях і ввести необхідні імена користувачів і паролі, щоб запустити автентифікацію. Поширені клієнти автентифікації включають програмне забезпечення клієнта автентифікації IEEE 802.1X, вбудоване в операційні системи Windows, macOS і Linux.
- Пристрій доступу: Вказує на мережевий пристрій з підтримкою IEEE 802.1X, яким у більшості випадків може бути комутатор. Пристрій доступу забезпечує доступ до мережі для клієнта автентифікації та слугує посередником між клієнтом автентифікації та сервером автентифікації. Пристрій доступу взаємодіє з клієнтом за допомогою протоколу Extensible Authentication Protocol over LAN (EAPOL) і з сервером за допомогою протоколу Remote Authentication Dial in User Service (RADIUS).
- Сервер автентифікації: Перевіряє ідентифікаційну інформацію (наприклад, ім'я користувача та пароль), надіслану клієнтом, щоб визначити, чи має він дозвіл на доступ до мережевих служб. Сервер автентифікації виконує авторизацію та облік клієнтів на основі мережевих вимог. Для надання послуг автентифікації зазвичай використовуються FreeRADIUS і Ruijie SMP з відкритим вихідним кодом.

3. Динамічне призначення VLAN IEEE 802.1X

Динамічне призначення VLAN за стандартом IEEE 802.1X означає, що сервер автентифікації може вказати ідентифікатор VLAN автентифікованого користувача. Динамічне призначення VLAN IEEE 802.1X призначає ідентифікатор VLAN користувачеві під час автентифікації та автоматично додає його до відповідної VLAN після успішної автентифікації. Ідентифікатори VLAN можуть бути призначені різним користувачам.

Примітка

Динамічні ідентифікатори VLAN на пристроях серії RG-NBS необхідно створити .

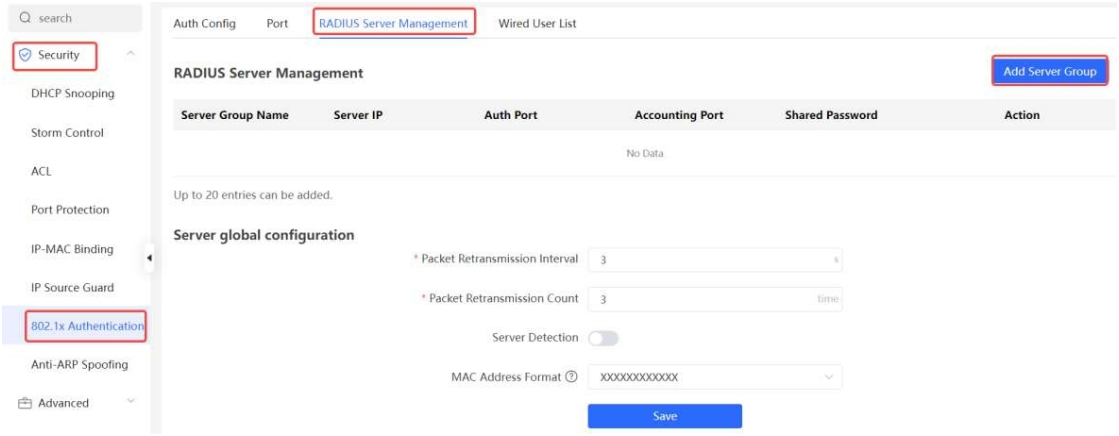
13.7.2 Конфігурація 802.1X

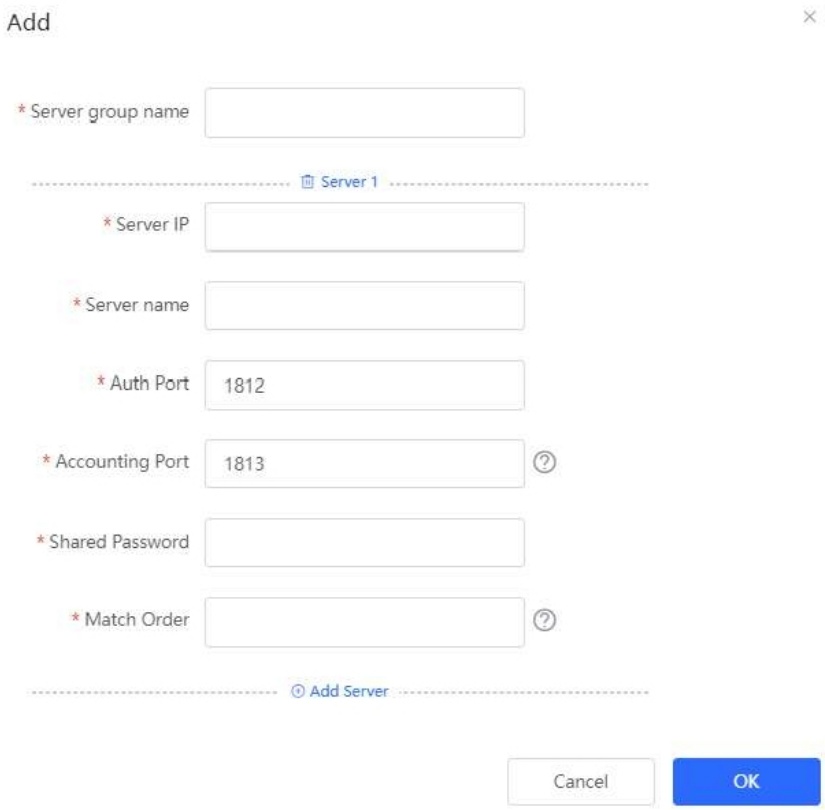
1. Додати сервер

Виберіть **локальний пристрій> Безпека> Автентифікація 802.1X> Керування сервером RADIUS**

Перед налаштуванням, будь ласка, підтвердіть:

- Сервер Radius повністю зібраний і налаштований наступним чином.
  - Додайте ім'я користувача та пароль для входу в систему.
  - Закрийте брандмауер, інакше повідомлення автентифікації може бути перехоплено, що призведе до помилки автентифікації.
  - Довірена IP-адреса на сервері Radius.
- Мережеве з'єднання між пристроєм автентифікації та сервером Radius.
- IP-адреси сервера Radius і пристрою автентифікації отримано. Натисніть **Додати групу серверів**, налаштуйте параметри групи серверів і натисніть **Зберегти**.



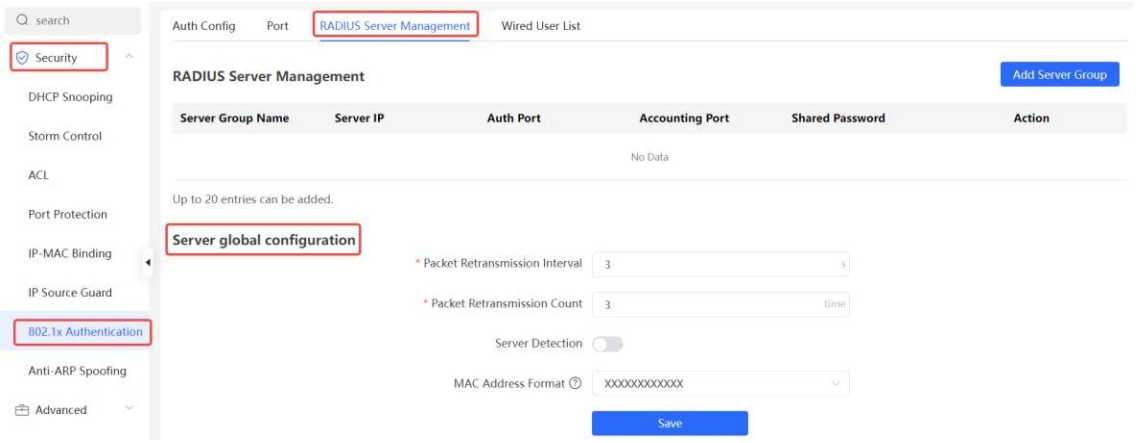


Таблиця 13-2 Параметри додавання групи серверів

параметр	Опис
Назва групи серверів	Назва групи серверів. Ви можете додати кілька серверів до групи. Якщо сервер з вищим пріоритетом не відповідає на запит клієнта, інші сервери в групі виконають відповідь відповідно до послідовності, що збігається. **Примітка** Щоб скористатися цією функцією, увімкніть виявлення серверів. Для отримання додаткової інформації див. 13.7.2 2. Налаштуйте сервер.
IP-адреса сервера	Адреса сервера Radius.
Порт авторизації	Номер порту, який використовується для доступу до автентифікації користувача на сервері Radius.
Обліковий порт	Номер порту, який використовується для доступу до процесу обліку на сервері Radius.
Спільний пароль	Спільний ключ сервера Radius.
Замовлення матчів	Система підтримує додавання до 5 серверів Radius. Чим більше значення порядку збігу, тим вищий пріоритет.

2. Налаштування сервера

Виберіть **локальний пристрій> Безпека> Автентифікація 802.1X> Керування сервером RADIUS**



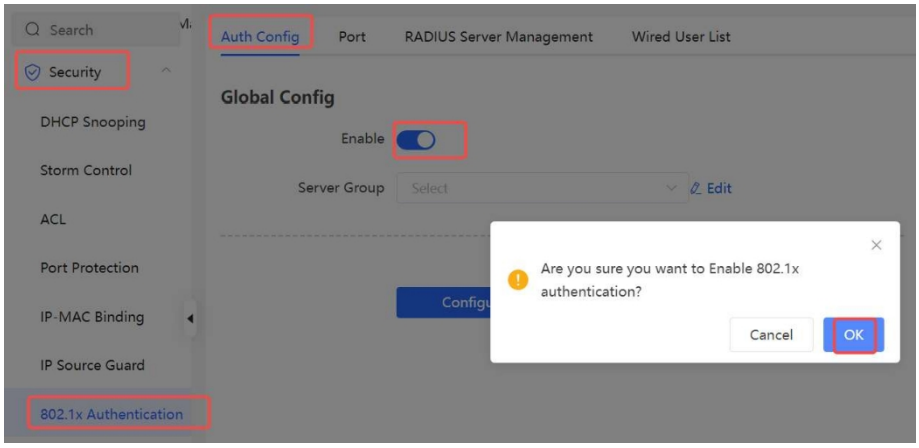
Таблиця 13-3 Опис налаштування параметрів групи глобальних серверів

Параметр	Опис
Інтервал повторної передачі пакетів	Налаштуйте інтервал, з яким пристрій надсилатиме пакети запитів до підтвердження відсутності відповіді від RADIUS
Кількість повторних передач пакетів	Налаштуйте, скільки разів пристрій надсилатиме пакети запитів, перш ніж підтвердити відсутність відповіді від RADIUS
Виявлення сервера	Якщо цю функцію увімкнено, вам потрібно встановити "Період виявлення сервера", "Час виявлення сервера" та "Ім'я користувача для виявлення сервера". Вона використовується для визначення статусу сервера, щоб вирішити, чи вмикати такі функції, як escape.
Формат MAC-адреси	Налаштуйте формат MAC-адреси RADIUS-атрибута №31 (Calling-Stationg-ID). Підтримуються наступні формати: ● Точковий шістнадцятковий формат, наприклад, 00d0.f8aa.bbcc● Формат IETF, наприклад, 00-D0-F8-AA-BB-CC ● Без формату (за замовчуванням), наприклад, 00d0f8aabbcc

3. Увімкніть автентифікацію IEEE 802.1X

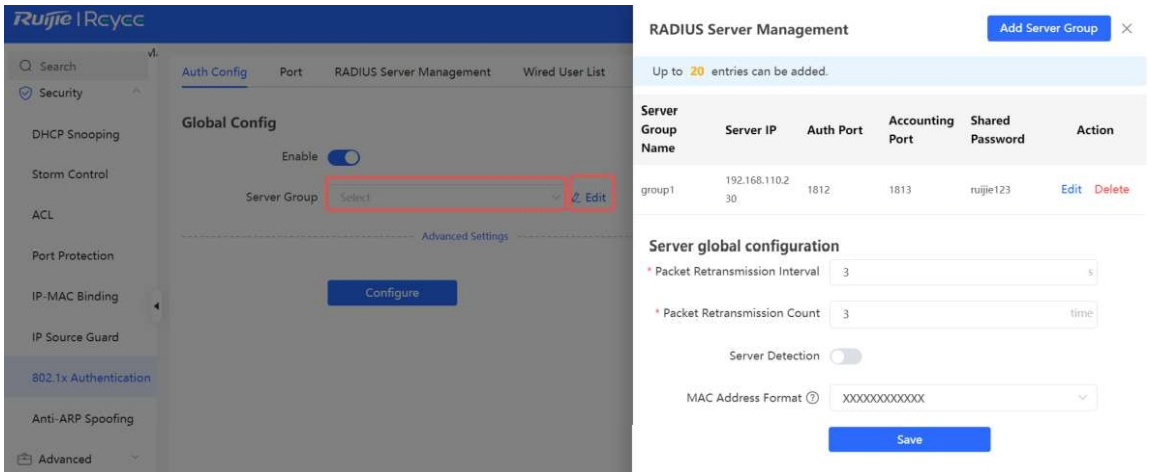
Виберіть **Локальний пристрій> Безпека**> **Автентифікація 802.1X**> **Auth Config**

(1) Увімкніть **Global 802.1X**, система запитає, чи потрібно її ввімкнути, натисніть **Налаштувати**.

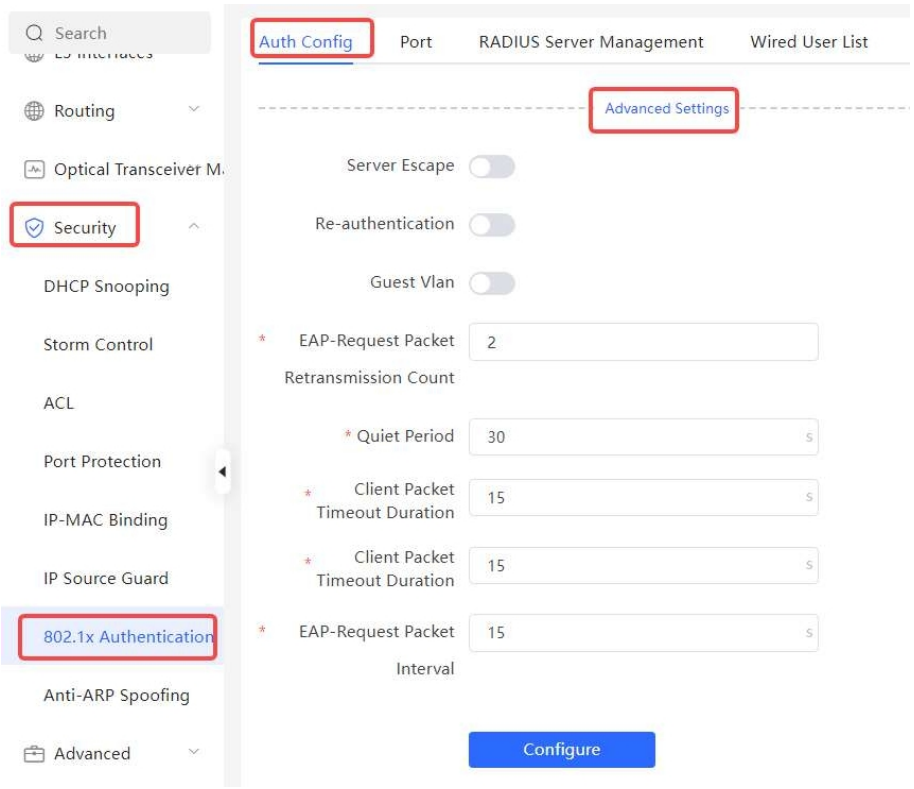


(2) Виберіть групу серверів. Якщо групу серверів не створено, натисніть **Редагувати**, щоб перейти до **керування сервером RADIUS**

і додайте групу серверів. Докладнішу інформацію наведено у розділі 13.7.2 1. Додайте сервер.



(3) Натисніть **Додаткові** параметри, щоб налаштувати такі параметри, як Гостьова VLAN.



Таблиця 13-4 Опис параметрів у розширених налаштуваннях IEEE 802.1X

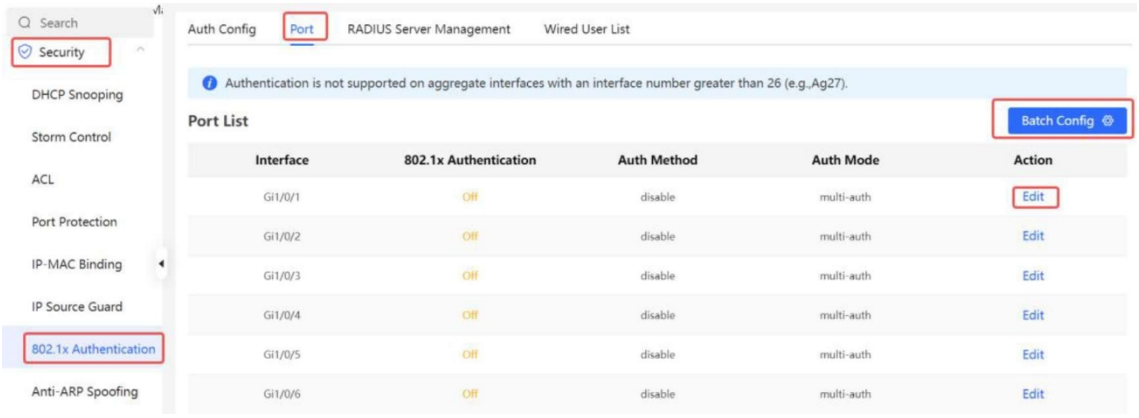
параметр	Опис
Втеча з сервера	Якщо буде виявлено відключення сервера, всім користувачам буде дозволено доступ до Інтернету
Повторна автентифікація	Вимагати від клієнтів повторної автентифікації через певні проміжки часу для забезпечення мережевої безпеки
Гостьовий VLAN	Створіть VLAN для неавторизованих клієнтів, щоб обмежити їхній доступ
Кількість повторних передач пакетів EAP-запиту	Визначити, скільки разів буде повторно надіслано повідомлення із запитом EAP, якщо відповідь не отримано, діапазон значень: 2- 10 разів
Період затишшя	Під час процесу автентифікації час простою між клієнтом і сервером, коли клієнт і сервер не обмінюються автентифікаційними повідомленнями, діапазон значень: 0- 65535 секунд
Тривалість таймауту клієнтських пакетів	Час, протягом якого сервер чекає на відповідь від клієнта. Перевищення цього часу буде вважатися помилкою автентифікації. Діапазон значень: 1- 65535 секунд
Тривалість таймауту клієнтських пакетів	Час очікування клієнтом відповіді сервера, перевищення якого буде вважатися помилкою автентифікації, діапазон значень: 1- 65535 секунд

параметр	Опис
Інтервал між пакетами EAP-запитів	Задайте інтервал часу між відправленням EAP-запитів для контролю швидкості процесу автентифікації, діапазон значень: 1-65535 секунд

4. Налаштуйте ефективний інтерфейс

Виберіть **Локальний пристрій> Безпека> Автентифікація 802.1X> Порт**

Натисніть **Редагувати** для окремого інтерфейсу або **Пакетна конфігурація** для редагування параметрів автентифікації для інтерфейсів.



Таблиця 13-5 Опис параметрів конфігурації порту

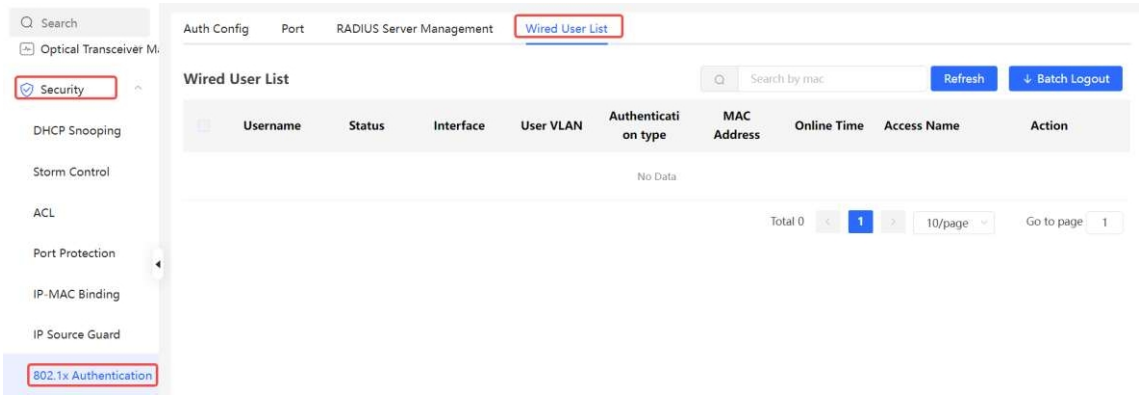
Параметр	Опис
Аутентифікація 802.1X	Якщо увімкнено, вибраний інтерфейс увімкне автентифікацію 8.02.1x.
Метод авторизації	• вимкнути: Вимкнути метод автентифікації, що має такий самий ефект, як і вимкнення перемикача автентифікації 802.1X • force-auth: Обов'язкова автентифікація, клієнт може отримати прямий доступ інтернету без пароля • force-unauth: заборонити автентифікацію, клієнт не може автентифікуватися і не може отримати доступ до Інтернету • auto: автоматична автентифікація, пристрій потребує автентифікації та може отримати доступ до Інтернету після проходження автентифікації

Параметр	Опис
	Рекомендується вибрати метод автоматичної автентифікації.
Режим авторизації	• multi-auth: підтримує кілька пристроїв, які використовують один порт для автентифікації, але кожен пристрій має бути автентифікований незалежно • багатохостовий: Кілька пристроїв можуть використовувати один і той самий порт. один користувач проходить автентифікацію, наступні користувачі можуть отримати доступ до Інтернету • single-host: кожен порт дозволяє автентифікацію лише одному пристрою, який може отримати доступ до Інтернету після успішної автентифікації
Гість Влад	Якщо увімкнено, пристрої, які не пройшли автентифікацію, будуть динамічно призначені до вказаної гостьової VLAN **Повідомлення** Спочатку потрібно створити ідентифікатор VLAN і застосувати його до інтерфейсу, потім в Керуванні безпекою > Аутентифікація 802.1X> Додаткові налаштування в конфігурації аутентифікації увімкнути Гостьову VLAN і ввести ідентифікатор
Ліміт кількості користувачів на порт	Обмеження кількості користувачів під інтерфейсом **Примітка** Максимальна кількість користувачів, яку підтримує комутатор серії RG-NBS3100 та його окремий порт, становить від 1 до 256 користувачів. Максимальна кількість користувачів, яку підтримують комутатори інших серій та їх окремі порти, становить від 1 до 1000 користувачів.

13.7.3 Переглянути список користувачів дротової автентифікації

8.02.1x функція налаштована у всій мережі, а термінал автентифікований і підключений до мережі, ви можете переглянути список автентифікованих користувачів.

Виберіть **Локальний пристрій**> Управління безпекою> Автентифікація 802.1X, щоб отримати конкретну інформацію про користувача.



Натисніть **Оновити**, щоб отримати останню інформацію про список користувачів.

Якщо ви хочете відключити певного користувача від мережі, ви можете вибрати користувача і натиснути Вимкнути в колонці "Операція"; ви також можете вибрати декількох користувачів і натиснути **Пакетне** вимкнення.

13.8 Anti-ARP Spoofing

13.8.1 Огляд

Функція запобігання підміні ARP-пакетів, орієнтованих на шлюз, використовується для перевірки того, чи встановлено IP-адресу джерела ARP-пакета через порт доступу на IP-адресу шлюзу. Якщо так, то пакет буде відкинуто, щоб запобігти отриманню хостами неправильних пакетів ARP-відповідей. Якщо ні, пакет не буде оброблено. Таким чином, тільки висхідні пристрої можуть надсилати ARP-пакети, а ARP-пакети-відповіді, надіслані від інших клієнтів, які проходять через шлюз, відфільтровуються.

13.8.2 Процедура

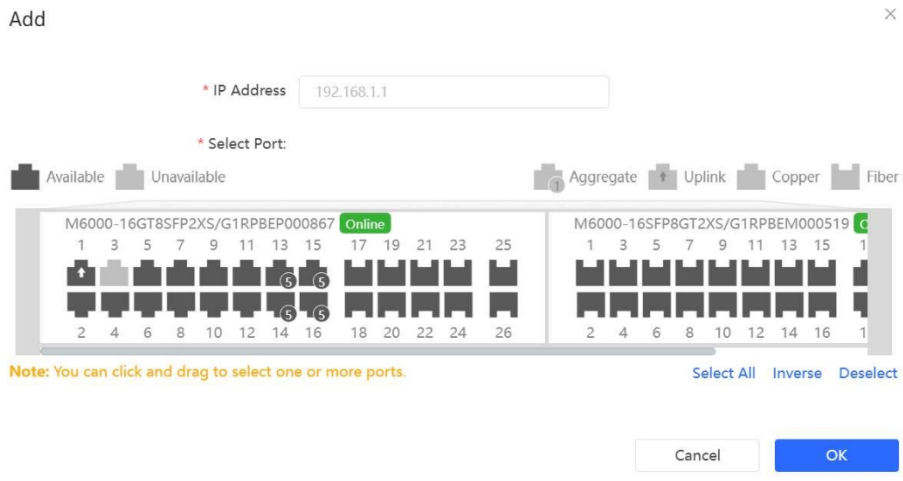
Виберіть **Локальний пристрій**> **Безпека**> **Захист IP-джерела**> **Виключена VLAN**.

1. Увімкнення підробки Anti-ARP

Натисніть **Додати**, виберіть потрібний порт і введіть IP-адресу шлюзу, натисніть **ОК**.

Примітка

Як правило, функція анти-ARP спуфінгу увімкнена на низхідних портах пристрою.



2. Вимкнення підміни Anti-ARP

Вимкнути пакетну обробку: Виберіть запис, який потрібно видалити, у списку і натисніть Видалити **вибране**. Вимкнення одного порту: натисніть **Видалити** в останньому стовпчику **Дія** відповідного запису.


search
Security
DHCP Snooping
Storm Control
ACL
Port Protection
IP-MAC Binding
IP Source Guard
802.1x Authentication
Anti-ARP Spoofing
Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.
Anti-ARP Spoofing
Add
Delete Selected
IP Address
Port
Action
172.30.102.1
Gi1/24
Edit
Delete
Up to 256 entries can be added.
Total 1
1
10/page
Go to page
1

14 Розширена конфігурація

14.1 STP

Комутатори серії RG-NBS підтримують наступні режими з'єднувального дерева:

- Протокол Spanning Tree Protocol (STP) - це протокол управління 2-го рівня, який усуває петлі 2-го рівня шляхом вибіркового блокування надлишкових каналів у мережі та забезпечує функцію резервування каналів.
- Заснований на STP, протокол Rapid Spanning Tree Protocol (RSTP) забезпечує швидку конвергенцію мережевої топології. Однак, як і STP, MSTP також має недолік: всі VLAN використовують одне покриваюче дерево, і розподіл навантаження не може бути досягнутий.
- Протокол Multiple Spanning Tree Protocol (MSTP) може подолати попередній недолік. Він може досягти швидкої конвергенції і перенаправлення трафіку різних VLAN за відповідними маршрутами, забезпечуючи тим самим кращий механізм балансування навантаження для надлишкових каналів.

Підтримка версій

ReyeeOS 2.320 або новіші версії підтримують MSTP. Версії раніше ReyeeOS 2.320 підтримують лише STP та RSTP.

14.1.1 Глобальні налаштування STP

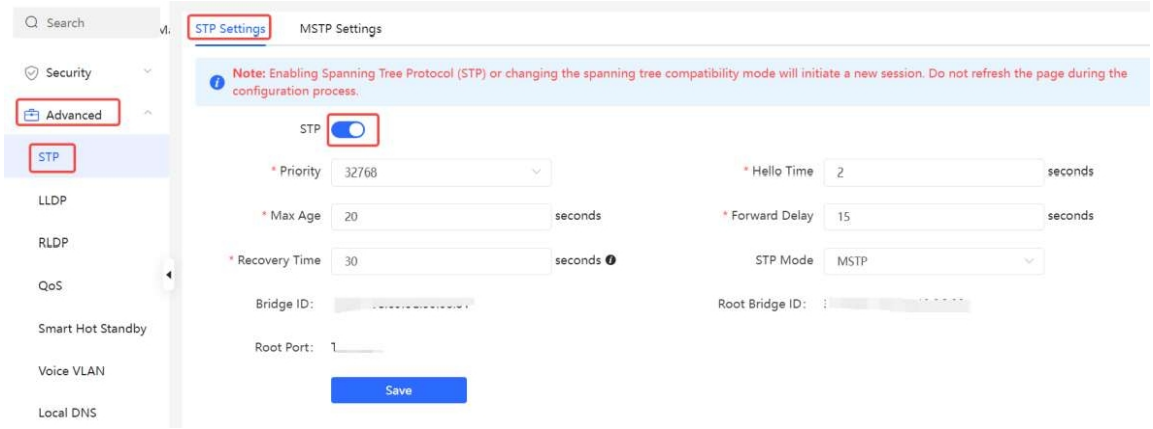
Виберіть **Локальний пристрій**> **Додатково**> **STP**> **STP**.

1. Глобальні конфігурації STP

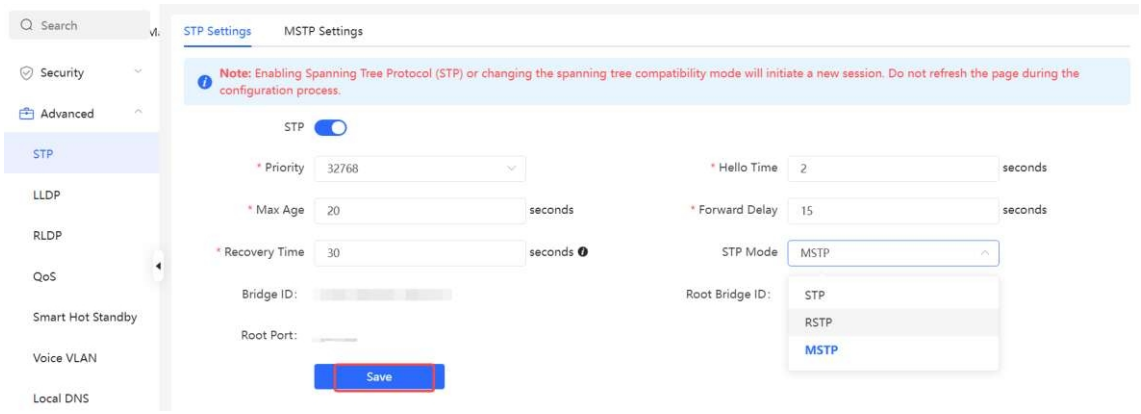
(1) Клацніть, щоб увімкнути функцію STP, і натисніть OK у , що з'явиться. За замовчуванням функцію STP вимкнено.

Застереження

- Після увімкнення конфігурації STP пристрою конфігурація ERPS не може нормально працювати.
- Увімкнення STP або зміна режиму STP ініціює новий сеанс. Не оновлюйте сторінку під час налаштування.



(2) Налаштуйте глобальні параметри STP і натисніть **Зберегти**.



Таблиця 14-1 Опис параметрів глобальної конфігурації STP

Параметр	Опис	Значення за замовчуванням
STP	Чи вмикати функцію STP. Вона набуває чинності глобально. Атрибути STP можна налаштовувати лише після ввімкнення STP.	Вимкнути
Пріоритет	Пріоритет моста. Під час вибору кореневого моста пристрій спочатку порівнює пріоритет моста. Менше значення вказує на вищий пріоритет.	32768
Привіт, час.	Інтервал для надсилання двох сусідніх BPDU	2 секунди.
Максимальний вік	Максимальний час вичерпання BPDU Пакети, що вичерпали свій час, будуть відкинуті. Якщо некореневий міст не отримує BPDU від кореневого моста до закінчення часу старіння, кореневий міст або канал зв'язку з кореневим мостом вважається несправним	20 секунд.
Пряма затримка	Інтервал, з яким змінюється стан порту, тобто інтервал, з яким порт переходить від прослуховування до навчання або від навчання до переадресації.	15 секунд.
Час відновлення	Час відновлення мережі, коли в мережі виникають надлишкові зв'язки.	30 секунд
Режим STP	Версії протоколу Spanning Tree Protocol. Наразі пристрій підтримує STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) та MSTP (Multiple Spanning Tree Protocol).	RSTP
Ідентифікатор мосту	STP ідентифікує комутатор за ідентифікатором моста, який складається з пріоритету моста і MAC-адреси моста.	NA
Ідентифікатор кореневого мосту	Як кореневий вузол дерева STP, кореневий міст ідентифікується ідентифікатором кореневого моста і функціонує як логічний центр всієї мережі 2-го рівня.	NA
Кореневий порт	Кореневий порт існує на некореневому мості і має найменшу вартість шляху до кореневого мосту. Кожен некореневий міст має лише один кореневий	NA

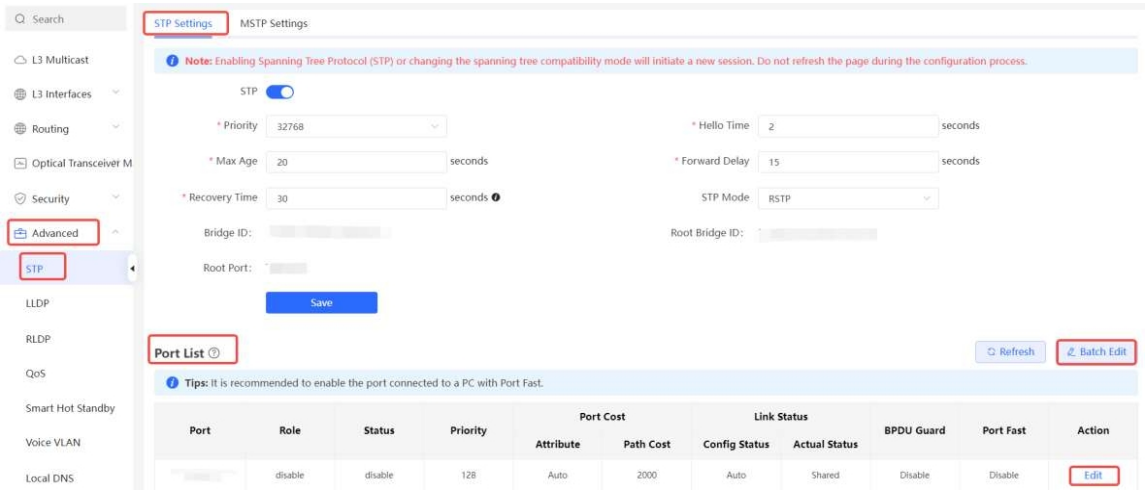
	порт.	

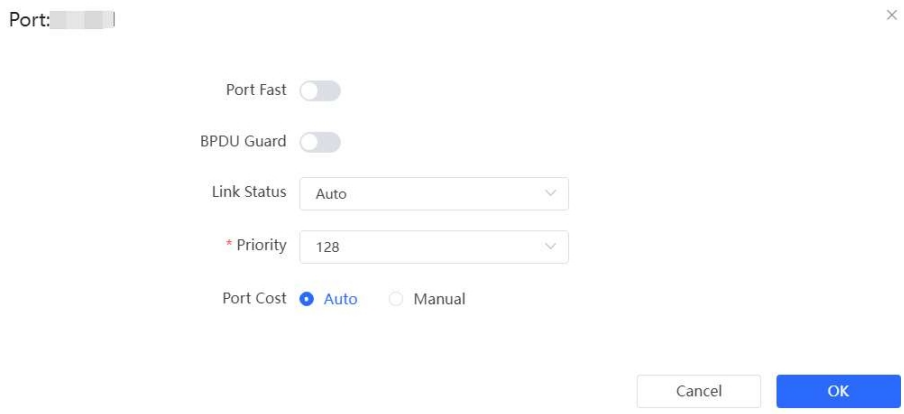
2. Застосування STP до порту

Виберіть **Локальний пристрій**> **Додатково**> **STP**> **STP**.

Налаштування властивостей STP для порту Натисніть **Пакетне редагування**, щоб вибрати порти і налаштувати параметри STP, або натисніть

Відредагуйте стовпчик **Дія** у **Списку портів**, щоб налаштувати призначені порти.





Таблиця 14-2 Опис параметрів конфігурації портів STP

Параметр	Опис	Значення за замовчуванням
Роль	● Корінь: Порт з найкоротшим шляхом до кореня ● Альтернативний: Резервний порт кореневого порту. Якщо кореневий порт виходить з ладу, альтернативний порт негайно стає кореневим. ● Призначені (призначені порти): Порт, який з'єднує кореневий міст або міст вищого рівня з пристроєм нижчого рівня. ● Відключити (заблоковані порти): Порти, які не мають жодного впливу у покривному дереві.	NA

Параметр	Опис	Значення за замовчуванням
Статус	● Вимкнений: Порт закрито вручну або через несправність, він не бере участі в остовному дереві і не пересилає дані, і може бути переведений у стан блокування після ініціалізації або відкриття. ● Блокування: Порт у стані блокування не може пересилати пакети даних або дізнаватися адреси, але може надсилати або отримувати конфігураційні BPDU і надсилати їх до центрального процесора. ● Прослуховування: Якщо порт може стати кореневим або призначеним портом, він перейде у стан прослуховування. **Прослуховування**: Порт у стані прослуховування не пересилає дані і не дізнається адреси, але може отримувати і надсилати конфігураційні BPDU. ● Навчання: Порт у стані навчання не може пересилати дані, але починає запам'ятовувати адреси і може отримувати, обробляти та надсилати конфігураційні BPDU. ● Пересилання: Як тільки порт входить у стан, він може пересилати будь-які дані, дізнаватися адреси, а також отримувати, обробляти та надсилати конфігураційні BPDU.	NA
Пріоритет	Пріоритет порту використовується для вибору ролі порту, і порт з високим пріоритетом переважно вибирається для переходу у стан переадресації	128
Атрибут витрат порту	Його можна встановити на **Авто** або **Вручну**: ● **Авто**: Вартість порту розраховується автоматично на основі портового тарифу. ● **Вручну**: Налаштоване значення використовується як вартість порту.	Авто
Вартість порту Вартість шляху	Фактична вартість шляху.	NA
Стан зв'язку Статус конфігурації	Налаштуйте тип посилання, серед варіантів є такі: Загальний, Точка-точка і Авто. В автоматичному режимі тип інтерфейсу визначається на основі дуплексного режиму. Для повнодуплексних портів тип інтерфейсу - точка-точка, а для напівдуплексних портів - спільний.	Авто
Статус посилання Фактичний статус	Фактичний тип посилання: Загальний, Точка-точка	NA
Охорона БНОН	Чи вмикати функцію захисту BPDU. Після увімкнення функції, якщо на порту увімкнено Port Fast або порт автоматично визначено як граничний порт, підключений до кінцевого пристрою, але порт отримує BPDU, порт буде вимкнено і він перейде у стан Error-disabled (Вимкнено помилково). Це означає, що неавторизований користувач може додати мережевий пристрій до мережі, що призведе до зміни топології мережі.	Вимкнути

Параметр	Опис	Значення за замовчуванням
Швидкий порт	Чи вмикати функцію Port Fast. Після ввімкнення функції Port Fast на порту, порт не буде ані отримувати, ані надсилати BPDU. У цьому випадку хост, безпосередньо підключений до порту, не може отримувати BPDU. Якщо порт, на якому увімкнено Port Fast, автоматично виходить зі стану Port Fast, коли він отримує BPDU, функція фільтрації BPDU автоматично вимикається. Зазвичай порт, підключений до комп'ютера, увімкнено за допомогою Port Fast.	Вимкнути

Примітка

- Рекомендується увімкнути Port Fast на порту, підключеному до ПК.
- Порт переходить у стан переадресації після того, як STP увімкнено більше ніж на 30 секунд. Тому може статися перехідний розрив зв'язку, і пакети не можуть бути переадресовані.

14.1.2 Налаштування MSTP

Виберіть **Локальний пристрій**> **Додатково**> **STP**> **Налаштування MSTP**.

1. Глобальні конфігурації MSTP

Конфігурація MSTP набуває чинності лише тоді, коли для параметра **STP Mode** у глобальних конфігураціях STP встановлено значення **MSTP**.

Таблиця 14-3 Опис параметрів у глобальних конфігураціях MSTP

Параметр	Опис	Значення за замовчуванням
Назва регіону MST	Назва регіону MST. Назва є ідентифікатором, довжиною від 1 до 32 символів, і розрізняє різні регіони MST.	NA
Номер версії	Рівень доопрацювання регіону MST, який використовується для розрізнення різних регіонів MST.	0

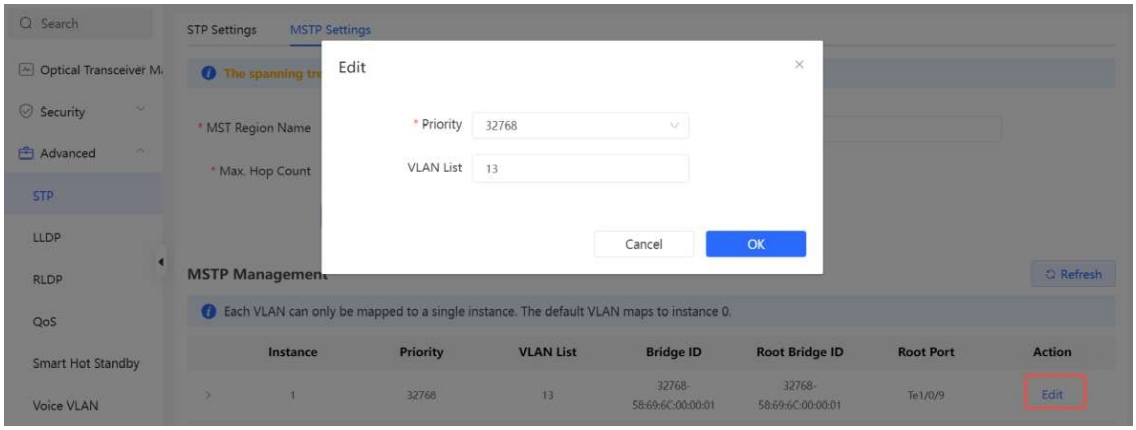
Макс. Підрахунок Переходів.	Максимальна кількість переходів пакетів BPDU в регіоні MST. Це також відноситься до максимальної кількості переходів від кореневого моста до інших мостів або кінцевих пристроїв.	20

2. Застосування MSTP

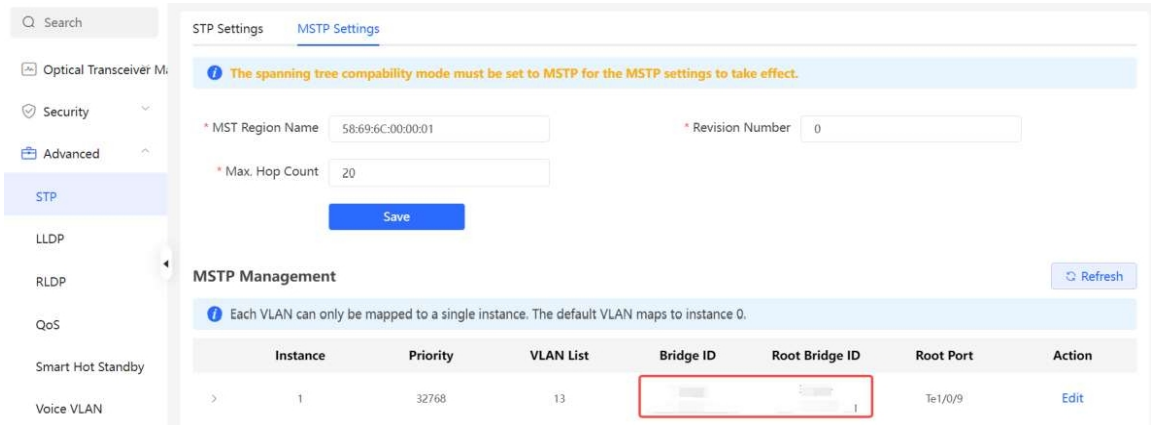
Натисніть кнопку **Змінити** у стовпчику **Дія** для вказаного екземпляра, встановіть **Пріоритет** і **Список VLAN** і натисніть кнопку **ОК**.

Примітка

Якщо ви хочете додати кілька ідентифікаторів VLAN, розділіть їх комами (,). Якщо ви намагаєтеся додати послідовні VLAN, розділяйте їх дефісом (-), наприклад, 14-15.



Ідентифікатор моста, ідентифікатор кореневого моста і номер кореневого порту екземпляра можна відобразити у списку лише після додавання ідентифікатора VLAN.

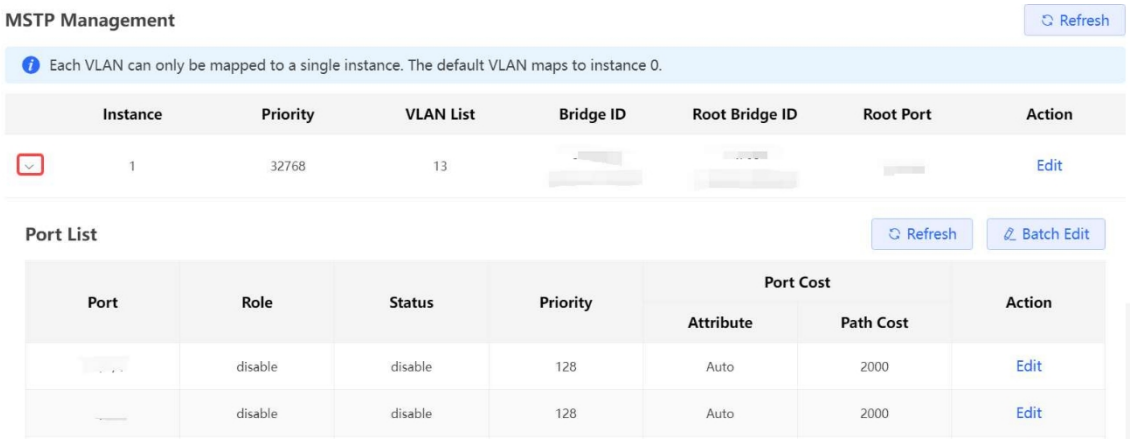


Примітка

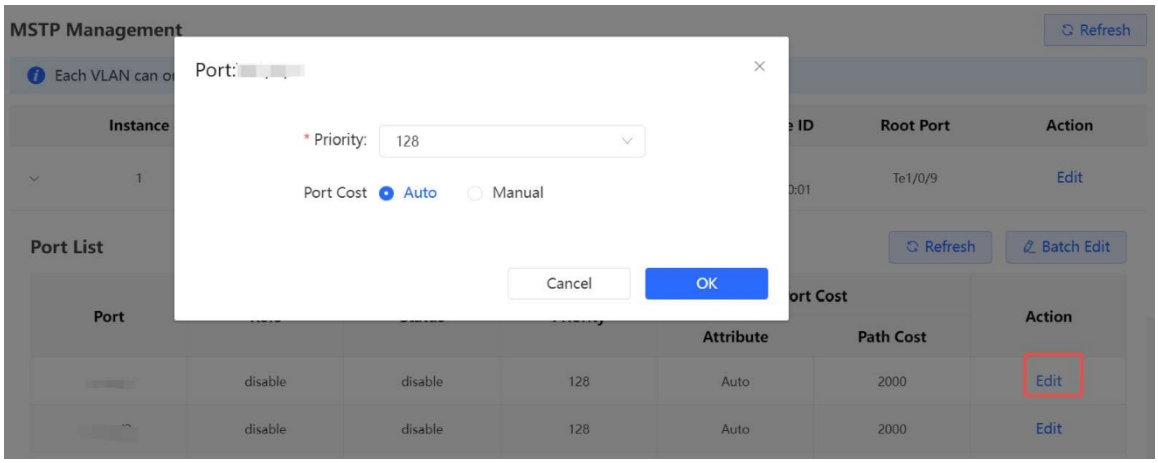
Якщо пристрій працює як кореневий міст, він не має кореневого порту, і номер порту не відображається у **кореневому порту**

колонку.

Натисніть кнопку зі спадним списком перед екземпляром, щоб відобразити відповідну конфігурацію порту.



Натисніть кнопку **Змінити** у стовпчику **Дія**, щоб змінити пріоритет і вартість порту.



14.2 LLDP

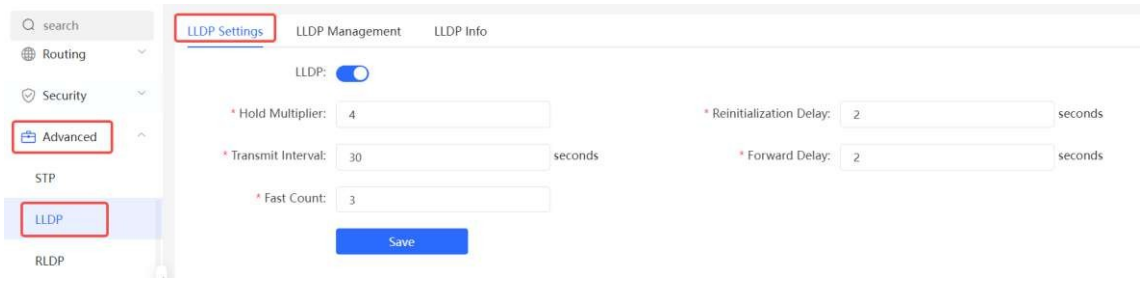
14.2.1 Огляд

LLDP (Link Layer Discovery Protocol - протокол виявлення канального рівня) визначається стандартом IEEE 802.1AB. LLDP може виявляти пристрої та виявляти зміни топології. За допомогою LLDP веб-інтерфейс може дізнатися топологічний статус з'єднання, наприклад, порти пристрою, які підключені до інших пристроїв, швидкість портів на обох кінцях з'єднання і стан узгодження дуплексного режиму. На основі цієї інформації адміністратор може швидко знайти та усунути несправності.

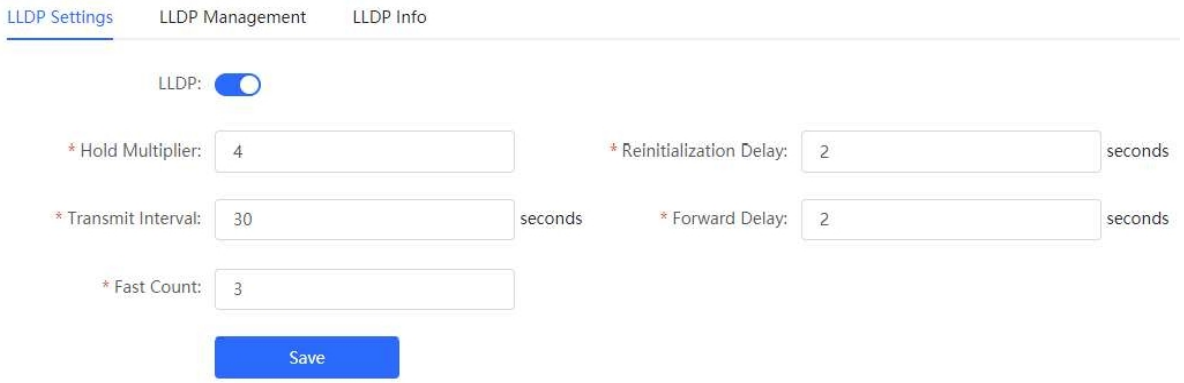
14.2.2 Глобальні налаштування LLDP

Виберіть **Локальний пристрій**> **Додатково LLDP**>> **Налаштування LLDP**.

(1) Клацніть, щоб увімкнути функцію LLDP, і натисніть **OK** у , що з'явиться. За замовчуванням увімкнено функцію STP. Якщо увімкнено LLDP, цей крок можна пропустити.



(2) Налаштуйте глобальні параметри LLDP і натисніть **Зберегти**.



Таблиця 14-4 Опис параметрів глобальної конфігурації LLDP

Параметр	Опис	Значення за замовчуванням
LLDP	Показує, чи ввімкнено функцію LLDP.	Увімкнути
Мультиплікатор утримання	TTL множник LLDP У LLDP-пакетах TTL TLV вказує на час очікування локальної інформації про сусіда. Значення TTL TLV розраховується за наступною формулою: TTL TLV= Множник TTL× Інтервал передачі пакетів+ 1. Значення TTL TLV може бути змінено шляхом налаштування множника TTL та інтервалу передачі пакетів LLDP.	4
Інтервал передачі	Інтервал передачі LLDP-пакетів, у секундах Значення TTL TLV розраховується за наступною формулою: TTL TLV= Мультиплікатор TTL× Інтервал передачі пакетів+ 1. Значення TTL TLV може бути змінено шляхом налаштування множника TTL та інтервалу передачі пакетів LLDP.	30 секунд

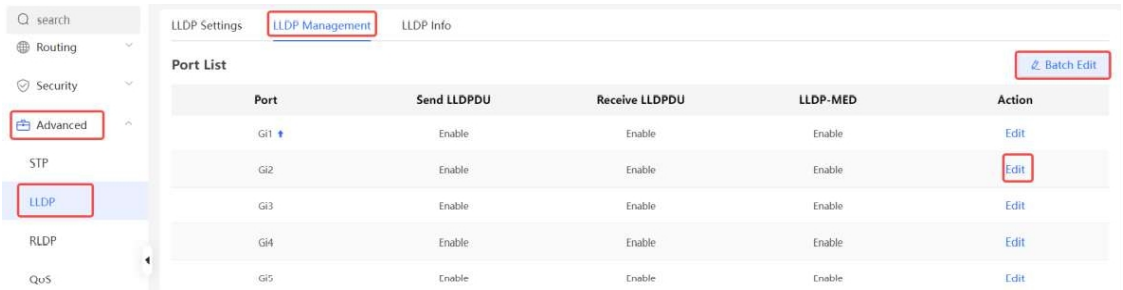
Параметр	Опис	Значення за замовчуванням
Швидкий підрахунок	Кількість пакетів, які швидко передаються При виявленні нового сусіда або зміні режиму роботи LLDP пристрій запускає механізм швидкої передачі, щоб дозволити сусіднім пристроям дізнатися інформацію про пристрій якомога швидше. Механізм швидкого передавання скорочує інтервал передавання LLDP-пакетів до 1 с, надсилає певну кількість LLDP-пакетів безперервно, а потім відновлює нормальний інтервал передавання. Ви можете налаштувати кількість LLDP-пакетів, які можуть бути передані швидко для механізму швидкого передавання.	3
Затримка повторної ініціалізації	Затримка ініціалізації порту, у секундах Ви можете налаштувати затримку ініціалізації, щоб запобігти частій ініціалізації машини стану, частою зміною режиму роботи порту.	2 секунди.
Пряма затримка	Затримка надсилання LLDP-пакетів, у секундах. Коли локальна інформація пристрою змінюється, пристрій негайно передає LLDP-пакети своїм сусідам. Ви можете налаштувати затримку передавання, щоб запобігти частому передаванню LLDP-пакетів, спричиненому частими змінами локальної інформації. Якщо затримку встановлено на дуже мале значення, часта зміна локальної інформації призведе до частої передачі LLDP-пакетів. Якщо затримку встановлено на дуже велике значення, жоден LLDP-пакет не буде передано навіть у разі зміни локальної інформації. Встановіть відповідну затримку відповідно до реальних умов.	2 секунди.

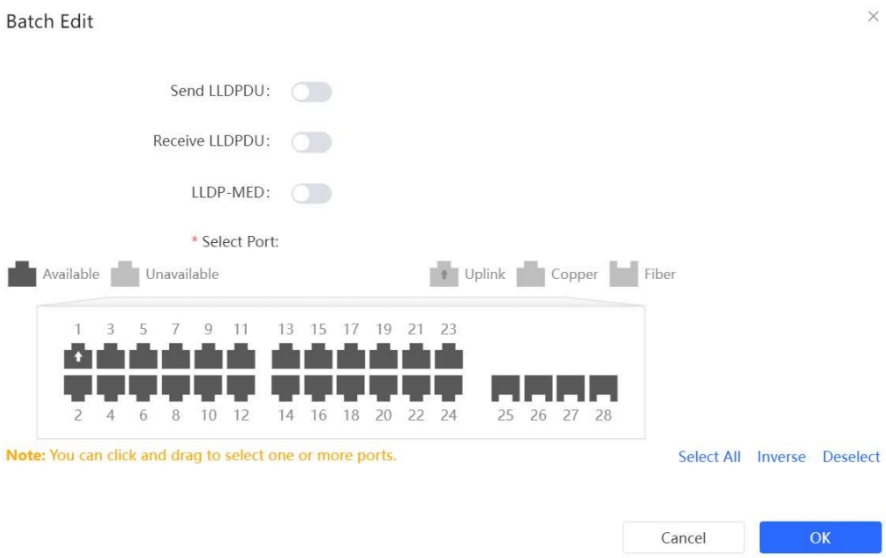
14.2.3 Застосування LLDP порту

Виберіть **Локальний пристрій**> **Додатково**> **LLDP**> **Керування LLDP**.

У **Списку портів** натисніть **Редагувати** у стовпчику **Дія** або натисніть **Пакетне редагування**, виберіть потрібний порт, налаштуйте режим роботи LLDP на порту і ввімкніть LLDP-MED, а потім натисніть кнопку **ОК**.

- **Надіслати LLDPDU**: Після ввімкнення опції **Надіслати LLDPDU** на порту, порт може надсилати LLDPDU.
- **Отримувати LLDPDU**: Після ввімкнення опції **Отримувати LLDPDU** на порту, порт може отримувати LLDPDU.
- **LLDPMED**: Після ввімкнення **LLDPMED** пристрій може виявляти сусідів, якщо його однорангова кінцева точка підтримує LLDP-MED (протокол виявлення на рівні зв'язку - виявлення медіа-кінцевих точок).



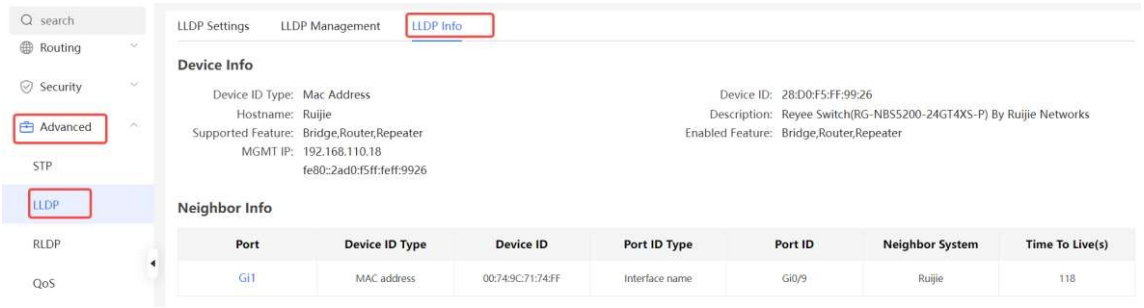


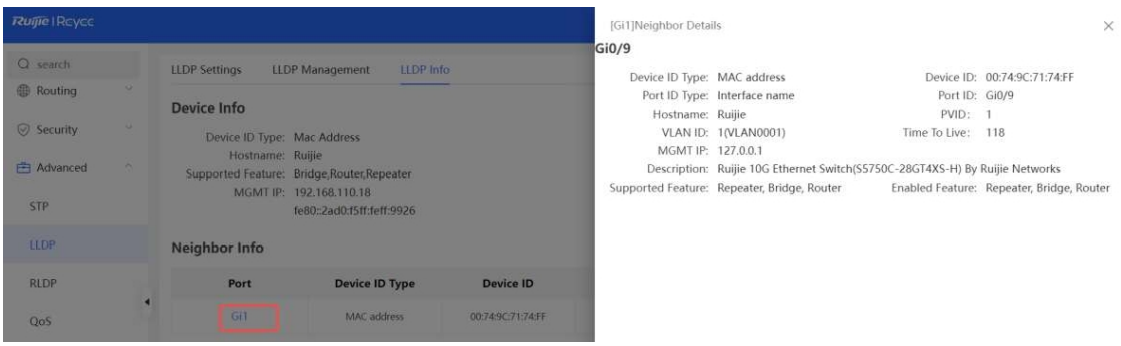
14.2.4 Відображення інформації про LLDP

Виберіть **Локальний пристрій**> **Додатково**> **LLDP**> **Інформація про LLDP**.

Відображення інформації LLDP, зокрема інформації LLDP локального пристрою та пристроїв-сусідів кожного порту. Клацніть назву порту, щоб відобразити відомості про сусідні порти.

Ви можете перевірити топологію з'єднання за допомогою інформації LLDP або використовувати LLDP для виявлення помилок. Наприклад, якщо топології мережі два з'єднані безпосередньо. Коли адміністратор налаштовує VLAN, швидкість порту, дуплексний режим, з'явиться повідомлення про помилку, якщо конфігурації не збігаються з конфігураціями на підключеному сусідньому пристрої.





14.3 RLDP

14.3.1 Огляд

Протокол швидкого виявлення збоїв (RLDP) - це протокол виявлення збоїв у мережі Ethernet, який використовується для швидкого виявлення односпрямованих збоїв у мережі, двоспрямованих збоїв у мережі та збоїв у низхідному шлейфі. При виявленні збою RLDP автоматично відповідні порти або просить користувачів вручну вимкнути порти відповідно до налаштованих методів обробки збоїв, щоб уникнути неправильної переадресації трафіку або петель Ethernet 2-го рівня.

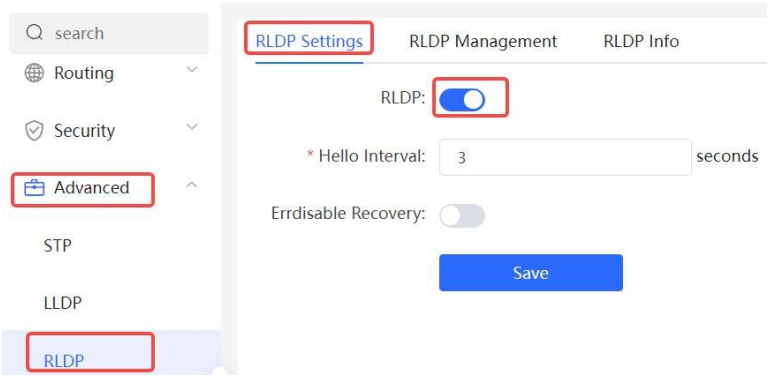
Підтримує пакетне ввімкнення функції RLDP на комутаторах доступу в мережі. За замовчуванням порти комутатора автоматично вимикаються, коли виникає петля. Ви також можете налаштувати один комутатор, щоб налаштувати, чи ввімкнути виявлення петель на кожному порту і методи обробки після виявлення несправності каналу зв'язку

14.3.2 Конфігурація автономного пристрою

1. Глобальні налаштування RLDP

Виберіть **Локальний пристрій**> **Додатково**> **RLDP**> **Налаштування RLDP**.

(1) Увімкніть функцію RLDP і натисніть **OK** у діалоговому вікні, що з'явиться. За замовчуванням функцію RLDP вимкнено.



(2) Налаштуйте глобальні параметри RLDP і натисніть **Зберегти**.

Таблиця 14-5 Опис параметрів глобальної конфігурації RLDP

Параметр	Опис	Значення за замовч.
RLDP	Показує чи ввімкнено функцію RLDP.	Вимкнути
Привіт, Інтервал.	Інтервал, з яким RLDP надсилає пакети виявлення, у секундах	3 секунди.
Незворотне відновлення	Якщо його , порт автоматично повертається до ініціалізованого стану після зациклення.	Вимкнути
Невиправний інтервал відновлення	Інтервал, з яким порти, що вийшли з ладу, регулярно повертаються до ініціалізованого стану, а виявлення з'єднань перезапускається, у секундах.	30 секунди

2. Застосування RLDP до порту

Виберіть **Локальний пристрій**> **Додатково**> **RLDP**> **Управління RLDP**.

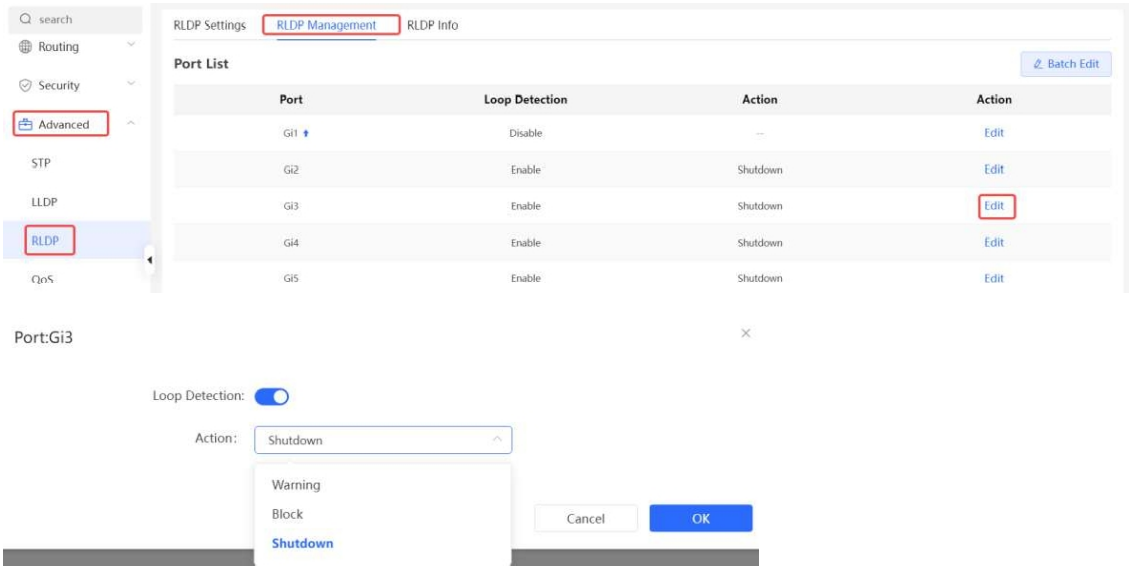
У **Списку портів** натисніть **Редагувати** у стовпчику Дія або натисніть **Пакетне редагування**, виберіть потрібний порт, вкажіть, чи потрібно увімкнути виявлення зациклення на порту і метод обробки після виявлення несправності, та натисніть кнопку **ОК**.

Існує три способи усунення збоїв у роботі портів:

- Попередження: Буде запропоновано лише відповідну інформацію, щоб вказати несправний порт і тип несправності.
- Блокувати: Після попередження про несправність налаштувати несправний порт на заборону пересилання отриманих пакетів
- Вимкнути порт: Після попередження про несправність вимкніть порт.

Застереження

- Коли RLDP застосовано до агрегованого інтерфейсу, для параметра **Дія** можна встановити лише значення **Попередження** та **Вимкнення**.
- При виконанні виявлення RLDP на агрегованому інтерфейсі, якщо пакети виявлення отримано на одному пристрої, навіть якщо VLAN порту, що надсилає пакети, і порту, що їх отримує, відрізняються, це не буде розцінено як збій петлі.



3. Відображення інформації про RLDP

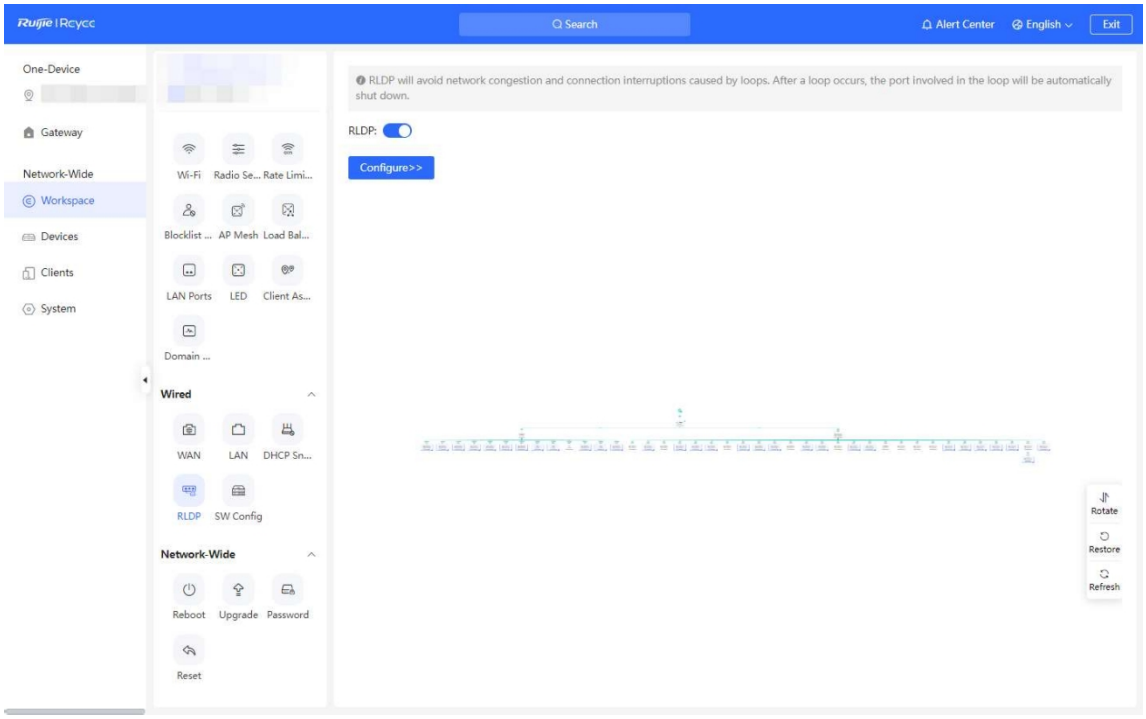
Виберіть **Локальний пристрій> Додатково> RLDP> Інформація про RLDP**.

Ви можете переглянути стан виявлення, методи обробки збоїв і порти, які з'єднують сусідній пристрій з локальним. Ви можете натиснути кнопку **Скинути**, щоб відновити нормальний стан RLDP, викликаний несправністю порту.

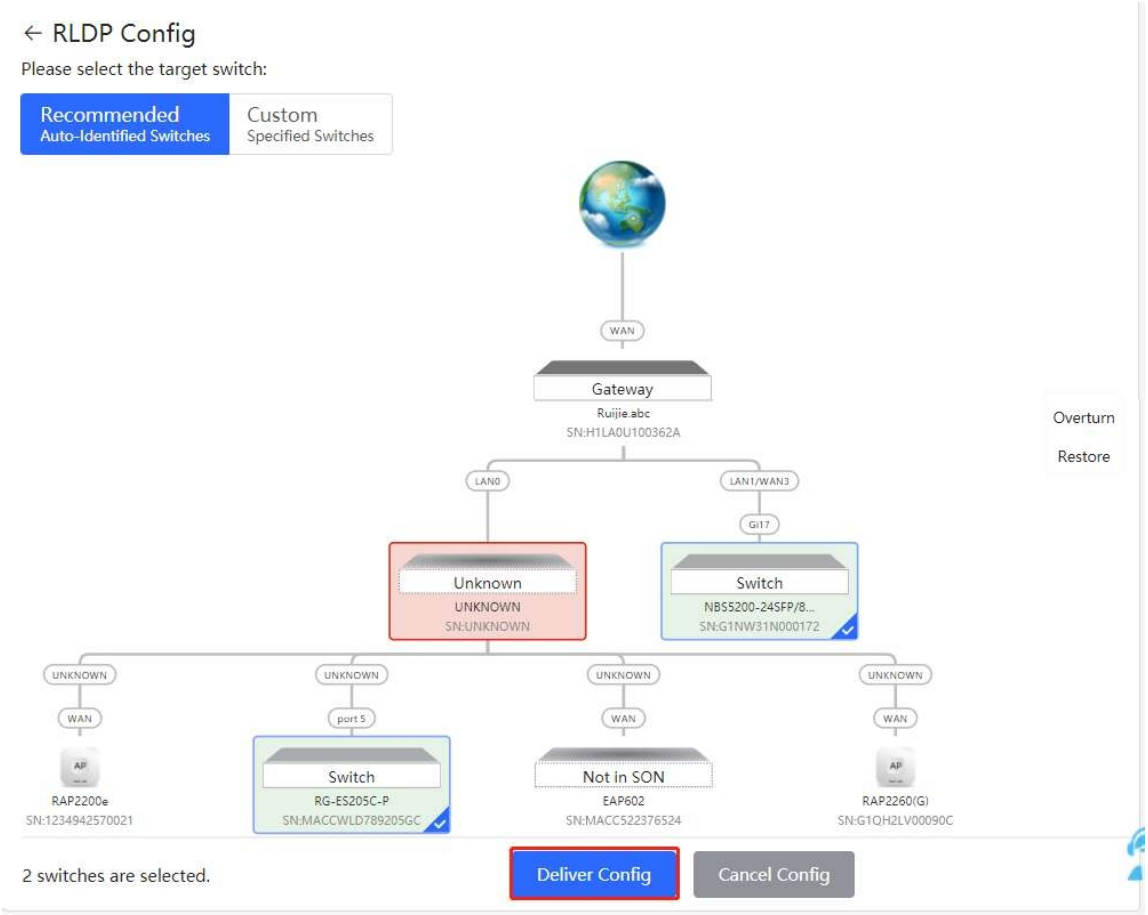
14.3.3 Пакетне налаштування мережевих комутаторів

Виберіть **Мережа в цілому > Робоча область > Дротовий RLDP>**

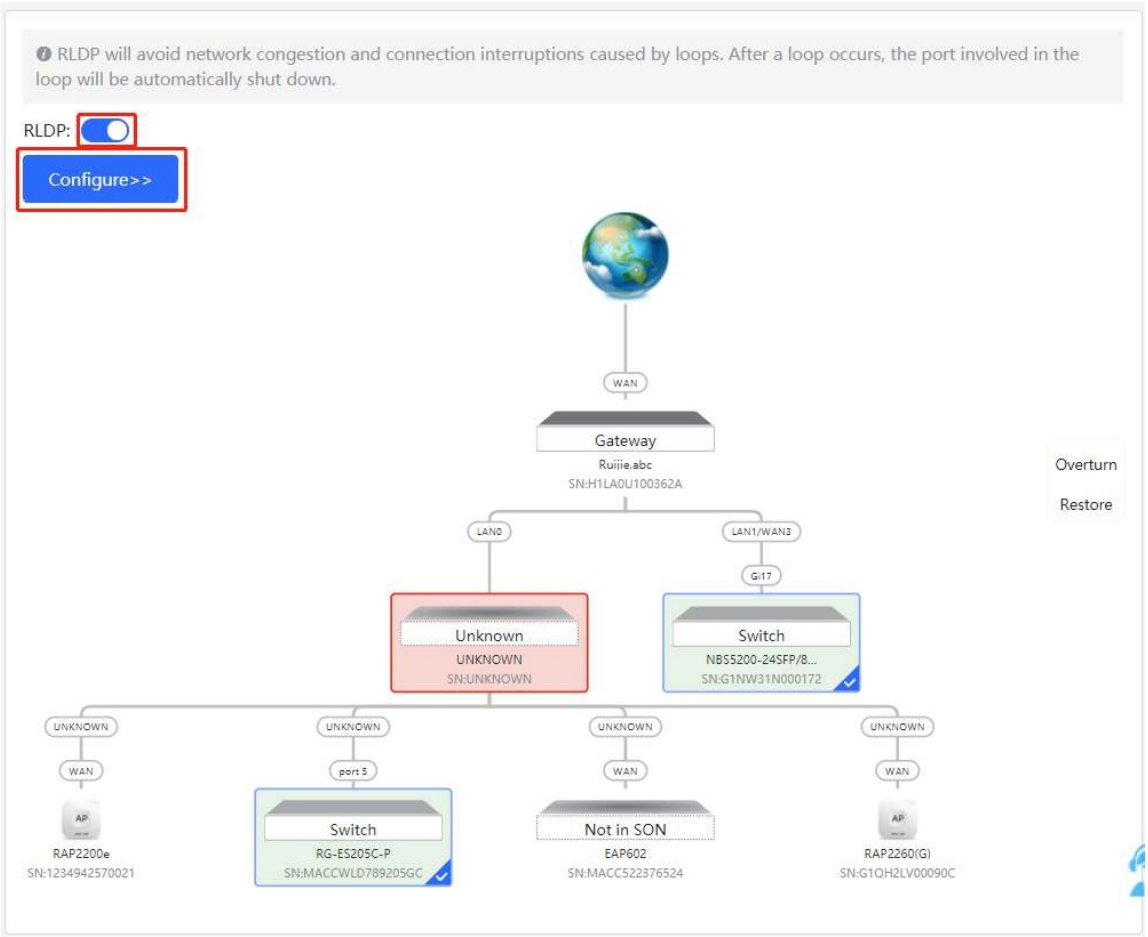
(1) Натисніть **Увімкнути**, щоб перейти на сторінку **налаштування RLDP**.



(2) У топології мережі ви можете вибрати комутатори доступу, на яких ви хочете ввімкнути RLDP у рекомендованому або користувацькому режимі. Якщо ви виберете рекомендований режим, всі комутатори доступу в мережі будуть обрані автоматично. Якщо ви виберете користувацький режим, ви зможете вручну вибрати потрібні комутатори доступу. Натисніть **Надати конфігурацію**. RLDP буде ввімкнено на вибраних комутаторах.



(3) Після того, як конфігурація буде доставлена, якщо ви хочете змінити діапазон дії функції RLDP, натисніть **Налаштувати**, щоб знову вибрати потрібні комутатори в топології. Вимкнути **RLDP**, щоб вимкнути RLDP на всіх комутаторах одним натисканням.



14.4 ERPS

Специфікація

Комутатори серії RG-NIS3100, RG-NBS3100, RG-NBS3200 і RG-NBS5100 під управлінням ReyeeOS 2.280 або новішої версії підтримують ERPS.

14.4.1 Огляд

Ethernet Ring Protection Switching (ERPS), також відомий як G.8032, - це протокол захисту кілець, розроблений Міжнародним союзом електрозв'язку (ITU). Це протокол канального рівня, спеціально розроблений для кілець Ethernet. ERPS запобігає широкомовним штормам, викликаним петлями даних, коли кільцева мережа Ethernet не пошкоджена, і може швидко виконувати перемикання каналів і відновлювати зв'язок між вузлами при розриві 'язку в кільці Ethernet, щоб реалізувати надмірність каналу передачі даних.

В даний час протокол Spanning Tree Protocol (STP) є ще одним рішенням проблеми мережевих петель на рівні 2. STP знаходиться на стадії зрілого застосування, але вимагає відносно тривалого (в межах секунд) збіжності. У порівнянні з STP, ERPS забезпечує швидшу конвергенцію, з часом конвергенції на рівні 2 менше 50 мс.

14.4.2 VLAN керування та VLAN даних

ERPS підтримує два типи віртуальних локальних мереж (VLAN): керуючі VLAN і VLAN даних.

- Контрольна VLAN: також відома як VLAN з комутацією кільця з автоматичним захистом (R-APS VLAN) для передачі пакетів протоколу ERPS. На пристрої порти, що підключаються до кільця ERPS, належать до керуючої

VLAN, і тільки такі

порти можна додати до керуючої VLAN.

- VLAN даних: VLAN даних використовується для передачі пакетів даних. До VLAN даних можуть бути призначені як порти ERPS, так і не-ERPS. VLAN даних також відома як захищена VLAN.

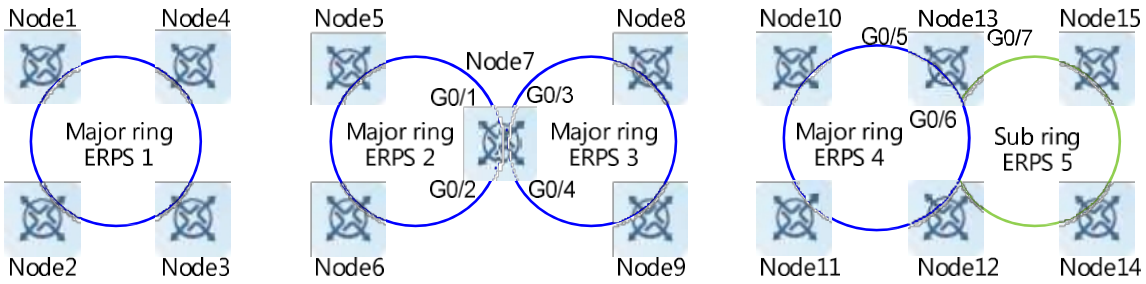
14.4.3 Базова модель кільця Ethernet

Група взаємопов'язаних пристроїв в одній керуючій VLAN (R-APS VLAN) утворює кільце Ethernet (кільце ERPS), в якому кожен пристрій називається вузлом. Кільця ERPS можна класифікувати на основні кільця та підкільця залежно від того, чи є кільце замкнутим.

1. Основне кільце та підкільце

- Велике кільце і велике кільцеве з'єднання: Основне кільце - це топологія замкненої мережі, з'єднаної в кільце, як, наприкладсині кільця, показані на Рисунку 14-1. У кільці ERPS ланки, які належать основного кільця і контролюються ним, називаються ланками основного кільця.
- Підкільце та підкільцеве з'єднання: Підкільце - це топологія незамкненої мережі, приєднаної до основного кільця, наприклад, зеленого кільця, показаного на Рисунку 14-1. У кільці ERPS канали, які належать до підкільця і контролюються ним, називаються каналами підкільця.
- Віртуальний канал R-APS підкільця: Як показано на Рисунку 14-1, всі канали основного кільця можна розглядати як віртуальні канали R-APS підкілець, які використовуються для пересилання пакетів протоколів підкілець. Вони належать до основного кільця, а не до підкільця. Основне кільце повинно асоціюватися з керуючою VLAN підкільця і пропускати пакети з цієї VLAN.

Рисунок 14-1 Основні топології кілець Ethernet



2. Основні топології

Основні кільця, підкільця та вузли можуть утворювати базові топології з різними характеристиками, залежно від режимів з'єднання, як показано на Рисунку 14-1.

- Одиночне кільце: кільце ERPS 1 (вузли 1-2-3-4) являє собою однокільцеву топологію.
- Дотичні кільця: Топологія, в якій два кільця ERPS поділяють один пристрій, називається дотичними кільцями. Основне кільце ERPS 2 (вузли 5-6-7) і основне кільце ERPS 3 (вузли 7-8-9) утворюють топологію дотичних кілець і є дотичними один до одного в одному вузлі, а саме в вузлі 7.
- Кільця, що перетинаються: Топологія, в якій два кільця ERPS поділяють два пристрої, називається кільцями, що перетинаються. Основне кільце ERPS 4 (вузол 13-10-11-12) і підкільце ERPS 5 (вузол 13-15-14-12) утворюють топологію кілець, що перетинаються, і перетинаються на двох безпосередньо з'єднаних перехресних вузлах, а саме на вузлі 13 і вузлі 12.

На практиці мережа - це комбінація декількох базових топологій, з кількома основними кільцями та кількома підкільцями.

3. Вузол

Відповідно до різних топологічних взаємозв'язків між вузлами і кільцями Ethernet, за роллю вузли класифікуються на однокільцеві, дотичні та перехресні.

- Вузол одного кільця: У кільці Ethernet вузли, які належать лише до одного кільця Ethernet (основного або підкільця), називаються однокільцевими вузлами. На однокільцевому вузлі необхідно забезпечити два інтерфейси, щоб вузол можна було додати до одного кільця ERPS. Як показано на Рисунку 14-1, вузли 1-4 в однокільцевій топології, вузли 5, 6, 8 і 9 в топології дотичного кільця і вузли 10, 11, 14 і 15 в топології перехресного кільця є однокільцевими вузлами.
- Дотичний вузол: Пристрій, спільний для дотичних кілець, називається дотичним вузлом. На кожному дотичному вузлі необхідно передбачити чотири інтерфейси, два з яких додаються до основного кільця, а два інших - до іншого основного кільця. Як показано на Рисунку 14-1, вузол 7 у топології дотичних кілець є дотичним вузлом.
- Вузол, що перетинається: Вузли в кільцях, що перетинаються, які належать до декількох кілець, називаються перехресними вузлами. На дотичному вузлі потрібно забезпечити три інтерфейси, два з яких до основного кільця, а третій - до підкільця. Як показано на Рисунку 14-1, вузли 12 і 13 в топології пересічних кілець є вузлами, що перетинаються. Кільця ERPS можуть перетинатися з іншими кількома кільцями ERPS і використовувати спільні канали для реалізації надмірності каналів передачі даних. Сервіси можуть бути швидко переключені з несправного каналу в одному кільці ERPS на нормальний канал.

4. Порт члена кільця

Кільце Ethernet має два порти-члени кільця на кожному вузлі, через який воно проходить: **західний** і **східний** порти. Як показано на Рисунку 14-1:

- Якщо кільце ERPS є замкнутим основним кільцем, кожен вузол, через який проходить кільце, має два інтерфейси, які використовуються як **західний і східний** порти для додавання вузла до кільця ERPS. Наприклад, на вузлі 7 інтерфейси GigabitEthernet 0/1 і 0/2 додаються до основного кільця ERPS 2, а інтерфейси GigabitEthernet 0/3 і 0/4 додаються до основного кільця ERPS 3. На вузлі 13 до основного кільця ERPS 4 додаються GigabitEthernet 0/5 і 0/6.
- Якщо кільце ERPS є незамкнутим підкільцем (у топології кільця, що перетинається), вузол, що не перетинається, має два інтерфейси, які використовуються як **західний** і **східний** порти для додавання вузла до підкільця ERPS, наприклад, вузол 15. На вузлі, що перетинається, лише один фізичний порт додається до підкільця ERPS як порт члена кільця, а інший порт члена кільця є віртуальним каналом (позначається **як virtual-channel**). Наприклад, на вузлі 13 до підкільця ERPS 5 додається тільки GigabitEthernet 0/7.

Існує два стани порту, що працює за протоколом ERPS: переадресація та блокування. Їхні функції наведено у Таблиці 14-6.

Таблиця 14-6 Держави порту протоколу ERPS

Держава порту	Отримання пакетів протоколу	Надсилання пакетів протоколу	Адресне навчання	Отримання пакетів даних	Надсилання пакетів даних
Блок	Так.	Так.	Ні.	Ні.	Ні.
Експедиція	Так.	Так.	Так.	Так.	Так.

14.4.4 RPL та вузли

Кільце Ethernet може перебувати в будь-якому з наступних двох станів, незалежно від того, чи є воно основним кільцем або підкільцем:

- Стан **очікування**: Фізичні ланки всієї кільцевої мережі з'єднані.
- Стан **захисту**: Фізичне з'єднання в кільцевій мережі відключено.

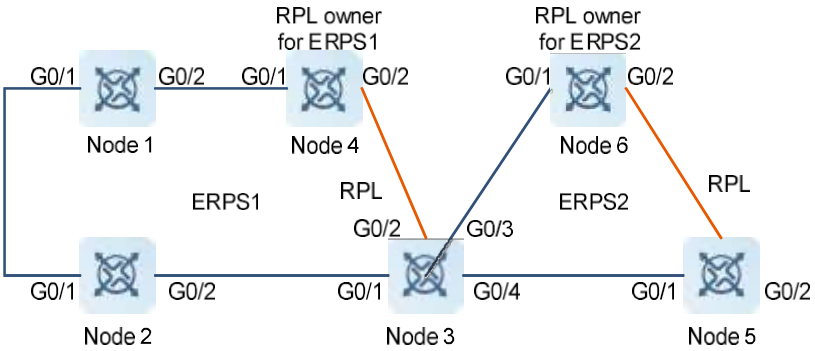
Кільцева захисна ланка (RPL): Коли фізичні ланки в кільцевій мережі з'єднані, кільце ERPS перебуває в стані очікування, а ланки в стані логічного блокування є RPL. Кожне кільце Ethernet має тільки один RPL. Наприклад, посилання, позначені помаранчевими лініями на Рисунку 14-2, є RPL, посилання між вузлом 3 і вузлом 4 є RPL кільця Ethernet ERPS 1 (вузол 1-2-3-4), а посилання між вузлом 5 і вузлом 6 є RPL кільця Ethernet ERPS 2 (вузол 3-5-6).

Вузол, який суміжним з RPL і використовується для блокування RPL, щоб запобігти виникненню петель, коли кільце Ethernet вільне від несправностей, називається вузлом-власником RPL. Як показано на рисунку 14-2, вузол 4 вузлом-власником RPL кільця Ethernet ERPS 1 (вузли 1-2-3-4), а вузол 6 є вузлом-власником RPL ERPS 2 (вузол 3-5-6).

Будь-які вузли, крім вузла-власника RPL у кільці Ethernet, не є RPL. Як показано на Рисунку 14-2, вузли, крім вузла 4 і вузла 6, не є вузлами-власниками RPL у кільцях.

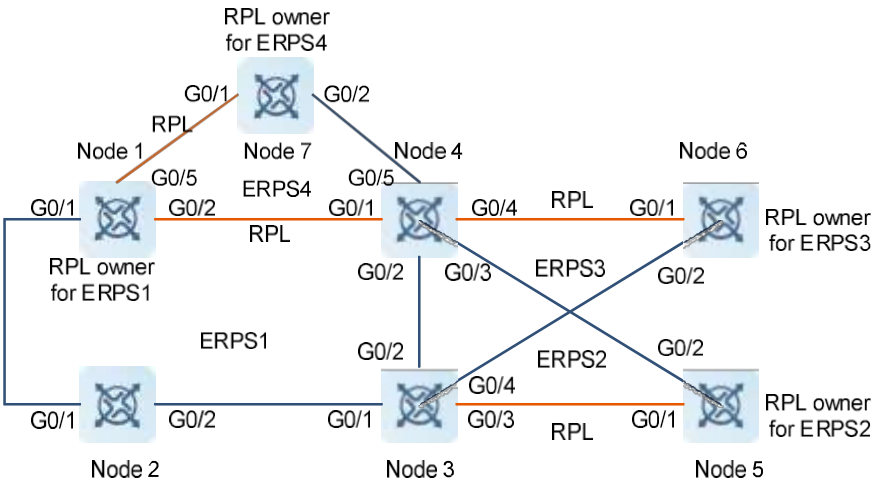
Заблоковані порти на RPL - це порти RPL, а порти RPL не пересилають пакети даних, щоб запобігти зациклюванню. Порти RPL знаходяться на вузлах-власниках RPL а вузли-власники RPL блокують порти RPL. Кожне кільце Ethernet має лише один вузол-власник RPL.

Рисунок 14-2 Типова топологія дотичних кілець



Як показано на рисунку 14-2, сполучною ланкою між вузлами 3 і 4 RPL кільця Ethernet ERPS 1. Як вузол-власник RPL ERPS 1, вузол 4 блокує порт RPL. Зв'язком між вузлом 5 і вузлом 6 є RPL кільця Ethernet ERPS 2. Як вузол-власник RPL для ERPS 2, вузол 6 блокує порт RPL. ERPS 1 (вузли 1-2-3-4) і ERPS 2 (вузли 3-5-6) мають спільний вузол 3, утворюючи топологію тангенціального кільця. Вузол 3 є дотичним вузлом.

Рисунок 14-3 Типова топологія кілець, що перетинаються



Як показано на Рисунку 14-3, ERPS 1 (вузли 1-2-3-4) є основним кільцем, а ERPS 2 (вузли 3-4-5) - підкільцем. ERPS 1 і ERPS 2 мають спільні вузли 3 і 4, утворюючи топологію кільця, що перетинаються. З'єднання між вузлом 4 і вузлом 5, а також між вузлом 3 і вузлом 5 є з'єднаннями підкільця ERPS 2 і контролюються ERPS 2. З'єднання між вузлом 3 і вузлом 4 належить до основного кільця, а не до підкільця і не контролюється підкільцем. Однак, пакети протоколу підкільця передаються через прямий канал між вузлом 3 та вузлом 4. Це пряме з'єднання є віртуальним каналом R-APS підкільця ERPS 2. Вузол 2 належить тільки до основного кільця ERPS 1 і називається однокільцевим вузлом. Вузол 6 належить лише до підкільця ERPS 3 і також називається однокільцевим вузлом. Вузли 3 і 4 є дотичними вузлами.

14.4.5 Пакет ERPS

Пакети ERPS (також звані пакетами R-APS) класифікуються на пакети відсутності сигналу (SF), пакети відсутності запитів (NR), пакети відсутності запитів-RPL заблоковані (NR-RB) і пакети Flush.

- SF-пакет: Коли канал зв'язку вузла не працює, вузол надсилає SF-пакет, щоб повідомити інші вузли про несправність зв'язку.
- NR-пакет: Коли несправне з'єднання відновлено, вузол надсилає NR-пакет, щоб повідомити вузол-власник RPL про відновлення з'єднання.
- Пакет NR-RB: Коли всі вузли в кільці ERPS функціонують належним чином, вузол-власник RPL періодично надсилає пакети NR-RB.
- Скидальний пакет: У кільцях, що перетинаються, коли в підкільці відбувається зміна топології, вузли, що перетинаються, надсилають пакети змиву, щоб повідомити інші пристрої в кільці Ethernet, до якого підключено підкільце.

14.4.6 Таймер ERPS

ERPS підтримує три : таймер затримки, охоронний таймер і таймер **очікування відновлення** (WTR).

- Таймер **затримки**: Таймер використовується для мінімізації частих перемикань топології ERPS через періодичні обриви зв'язку. Після налаштування таймера затримки ERPS виконує перемикання топології, тільки якщо після закінчення часу таймера несправність каналу все ще триває.
- Охоронний таймер: таймер використовується для запобігання отриманню пристроєм прострочених пакетів R-APS PMDU. Коли таймер

пристрій виявляє, що несправність зв'язку усунуто, він надсилає пакети відновлення зв'язку і запускає таймер **охорони** (**Guard timer**). До закінчення таймера всі пакети, крім пакетів Flush, які вказують на зміну топології підкільця, будуть відкинуті.

- Таймер WTR: Таймер діє лише для вузлів-власників RPL. Він використовується, щоб уникнути неправильної оцінки стану кільця RPL. Коли вузол-власник RPL виявляє, що збій усунуто, він не виконує перемикання топології негайно, а лише якщо кільце Ethernet буде відновлено після закінчення таймера WTR. Якщо у кільці буде виявлено знову до закінчення таймера, вузол-власник RPL скасовує таймер і не виконує перемикання топології.

14.4.7 Захист кільця

Функція захисту кільця запобігає широкомовним штормам, спричиненим зацикленням даних, і може швидко зв'язок між вузлами при розриві зв'язку в кільці Ethernet.

- Нормальний стан
  - Всі вузли фізичної топології з'єднані в кільцевому режимі. o

    ERPS блокує RPL, щоб запобігти виникненню петель.
  - ERPS виявляє збої на кожному з'єднанні між сусідніми вузлами.
- Несправність зв'язку

  Вузол, що знаходиться поруч з вузлом, який вийшов з ладу, виявляє несправність.

  Вузол, що знаходиться поруч з несправним з'єднанням, блокує несправне з'єднання і надсилає SF-пакети, щоб сповістити інші вузли в тому ж кільці.

  SF-пакет запускає вузол-власник RPL, щоб увімкнути порт RPL, а також запускає всі вузли, щоб оновити свої записи MAC-адрес і записи ARP/ND і перейти в стан захисту.
- Відновлення зв'язку

  Коли несправне з'єднання відновлюється, сусідній вузол все одно блокує з'єднання і надсилає пакети NR, що вказують на відсутність локальної несправності.

  Коли вузол-власник RPL отримує перший пакет NR, він запускає таймер WTR.

  Коли WTR закінчується, вузол-власник RPL блокує RPL і надсилає пакет NR-RB.

  Після отримання цього NR-RB пакета інші вузли оновлюють свої записи MAC-адрес і ARP/ND, а вузол, який надсилає NR-пакет, припиняє надсилання NR-пакетів і розблоковує заблоковані порти.
  - Кільцева мережа відновлюється до нормального стану.

14.4.8 Протоколи та стандарти

- ITU-T G.8032/Y.1344: Захисна комутація кільця Ethernet

14.4.9 Налаштування ERPS

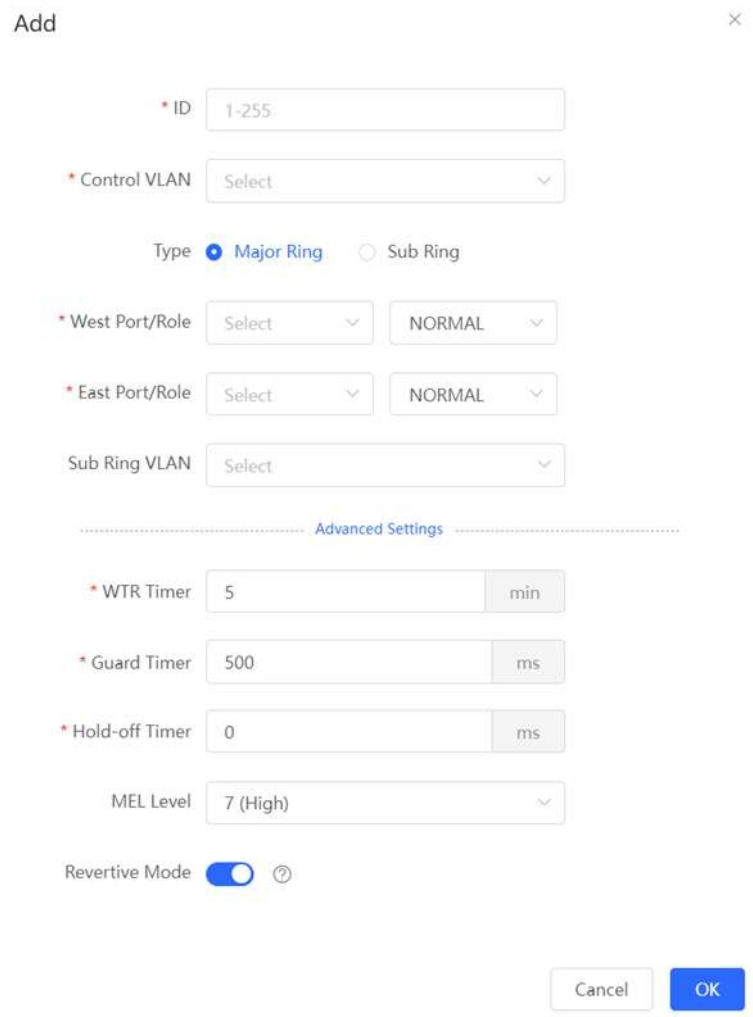
1. Додавання та видалення кільця ERPS

Виберіть **Локальний пристрій**> **Додатково**> **ERPS**

(1) Натисніть **Додати** на сторінці **списку дзвінків ERPS**.

(2) Як показано на Рисунку 14-4, налаштуйте параметри на сторінці відповідно до вимог сервісу.

Рисунок 14-4 Додавання кільця ERPS



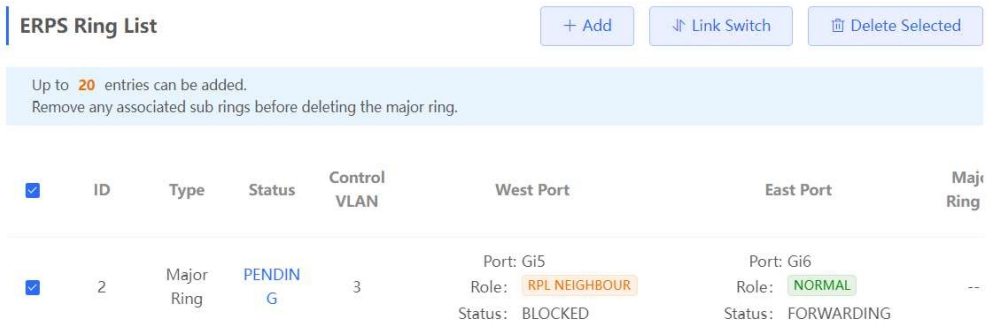
Таблиця 14-7 Параметр Опис

Параметр	Опис	Значення за замовч.
ІДЕНТИФІКАТОР	Вказує ідентифікатор екземпляра ERPS.	Н/Д
Контрольна мережа VLAN	Використовується для пересилання пакетів протоколу ERPS.	Н/Д
Тип	Вказує на тип кільця ERPS. Кільце може бути основним або підкільцем.	Н/Д
Західний порт/Роль	Вказує західний порт у кільці ERPS та його роль. Значення ролі порту включають ● НОРМАЛЬНИЙ: вказує на нормальний вузол. ● ВЛАСНИК RPL: Вказує на вузол власника RPL. ● RPL NEIGHBOR: Вказує на сусідній вузол RPL.	Н/Д
Східний порт/Роль	Вказує східний порт у кільці ERPS та його роль.	Н/Д

	Цінності ролі порту включають ● НОРМАЛЬНИЙ: вказує на нормальний вузол. ● ВЛАСНИК RPL: Вказує на вузол власника RPL. ● RPL NEIGHBOR: Вказує на сусідній вузол RPL.	
Підкільцева VLAN	Вказує керуючу VLAN підкільця.	Н/Д
Таймер WTR	Задає інтервал роботи таймера WTR.	5 хв
Таймер охорони	Задає інтервал роботи таймера охорони.	500 мс
Таймер очікування	Вказує інтервал таймера затримки.	0 мс, що вказує на те, що перемикання топології відбувається одразу після виявлення обриву зв'язку.
Рівень MEL	Вказує на рівень групи суб'єктів технічного обслуговування (MEG). Рівень MEL пристроїв в одному кільці ERPS повинен бути однаковим.	7
Відновлювальний режим	Якщо цей перемикач увімкнено, після усунення умови, що спричинила перемикання, трафік блокується на RPL.	Увімкнено.

(3) (Необов'язково) Як показано на Рисунок 14-5, виберіть наявні кільця ERPS, а потім натисніть **Видалити вибране**, щоб видалити вибрані кільця ERPS.

Рисунок 14-5 Видалення вибраних кілець ERPS



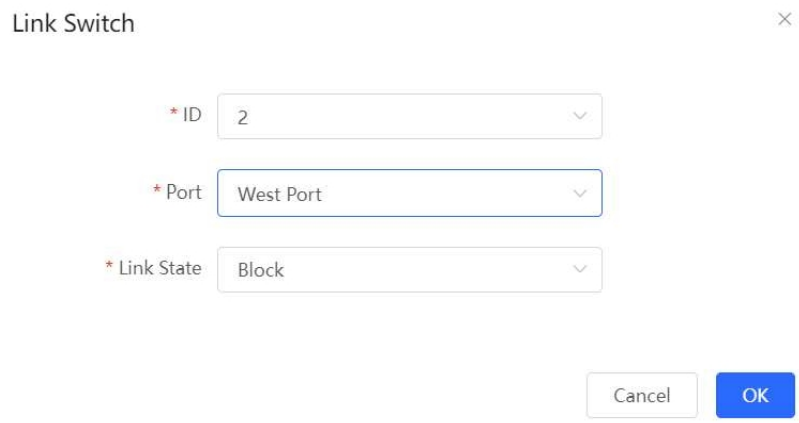
2. Комутатор зв'язку

Виберіть **Локальний пристрій**> **Додатково**> **ERPS**

(1) Натисніть **Перемикач посилань** на сторінці **Список дзвінків ERPS**.

(2) Як показано на Рисунку 14-6, налаштуйте параметри на сторінці відповідно до вимог сервісу.

Рисунок 14-6 Перемикач каналів зв'язку



Таблиця 14-8 Параметр Опис

Параметр	Опис	Значення за замовчуванням
ІДЕНТИФІКАТОР	Вказує ідентифікатор екземпляра ERPS.	Н/Д
Порт	Вказує порт у кільці ERPS. Значення включають Західний порт та Східний порт.	Н/Д
Стан зв'язку	Вказує стан з'єднання вибраного порту. Значення включають "Очистити" та "Заблокувати". ● Clear: вказує на те, що порт заблоковано примусовим перемиканням. ● Заблоковано: Вказує на те, що порт заблоковано ручним перемиканням.	Н/Д

14.4.10 Приклади типових конфігурацій ERPS

1. Вимоги

У мережі користувача є три пристрої, які повинні сформувати ERPS-кільце. Конкретна топологія показана нижче.

2. Топологія

3. Примітки

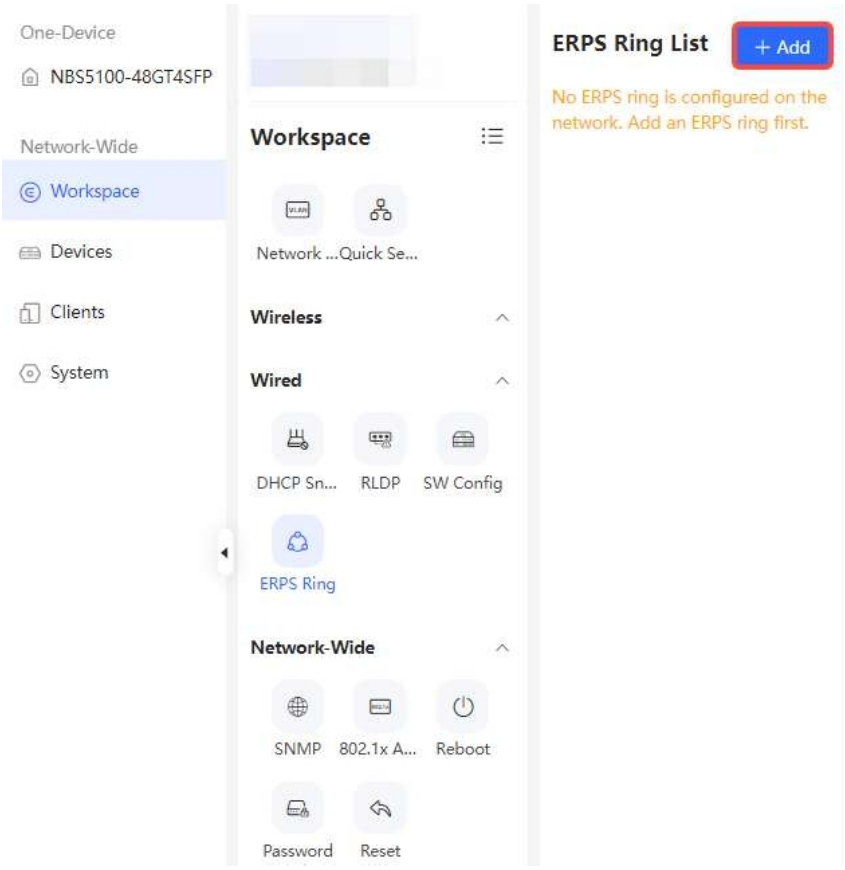
Щоб уникнути зациклення, налаштуйте ERPS перед виконанням кабельних з'єднань.

Для кільця ERPS лише один інтерфейс може бути власником RPL, а його одноранговий інтерфейс повинен бути сусідом RPL.

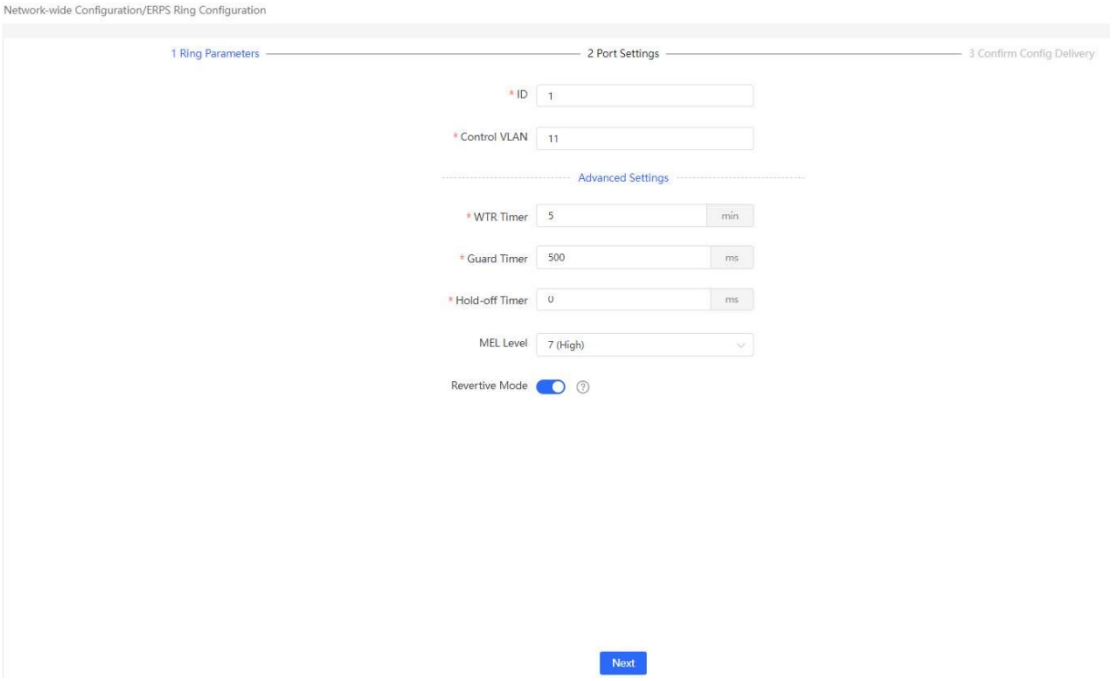
4. Процедура

(1) Виберіть **Network-Wide**> **Workspace**> **Wired**> **ERPS Ring**, щоб отримати доступ до сторінки конфігурації **ERPS Ring**.

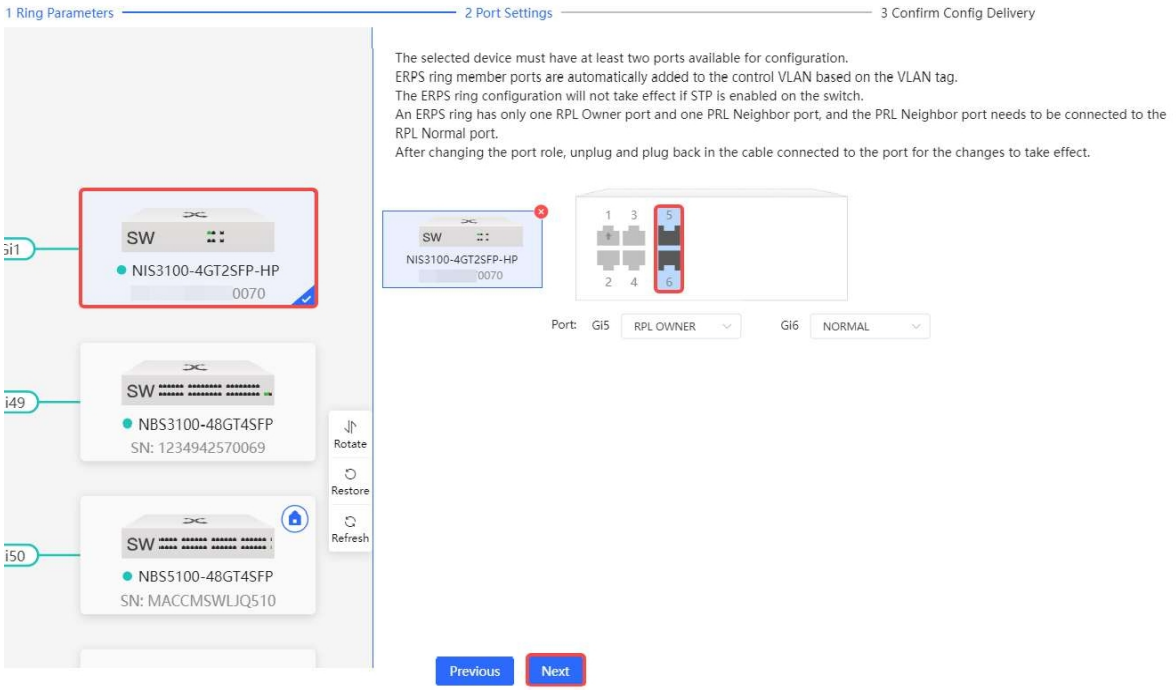
(2) Натисніть **+Додати** на сторінці, щоб додати кільце ERPS.



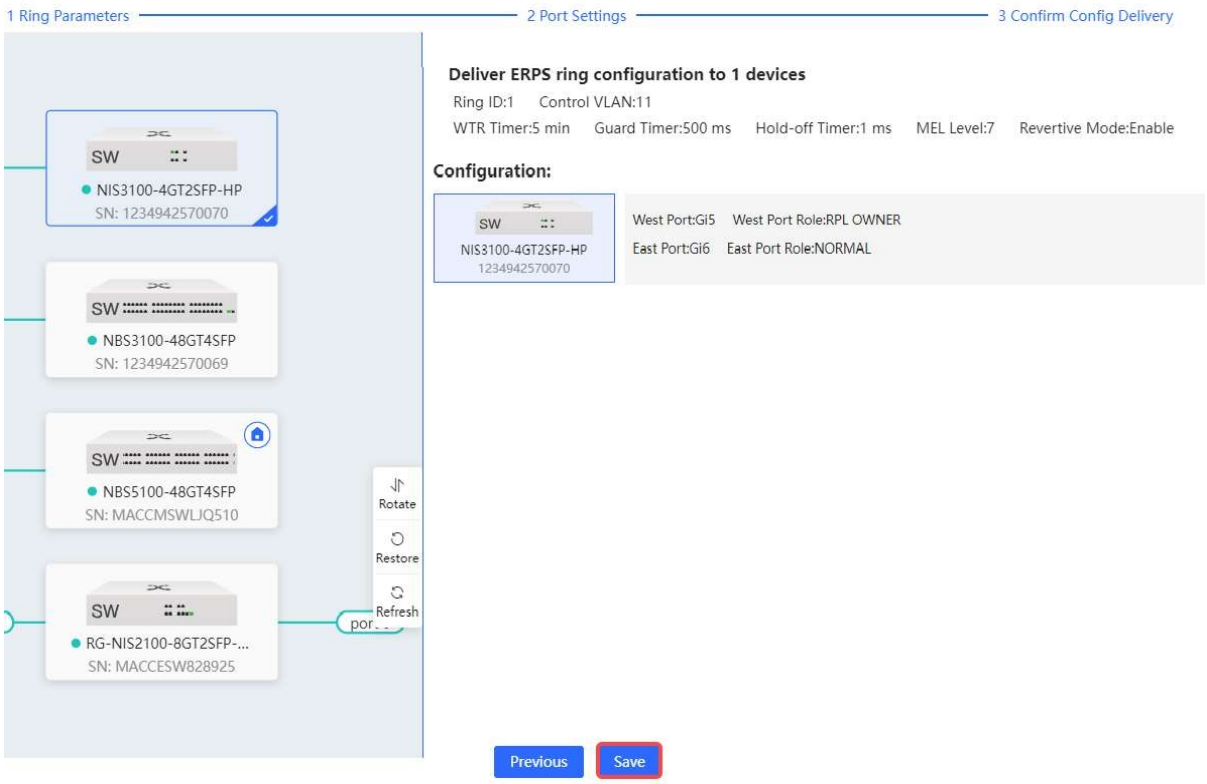
(3) Як показано наступному малюнку, встановіть параметри кільця ERPS (тільки **ID** і **Control VLAN** є обов'язковими і повинні бути налаштовані відповідно до налаштувань мережі користувача). Інші параметри можна залишити за замовчуванням). Потім натисніть кнопку **Далі**.



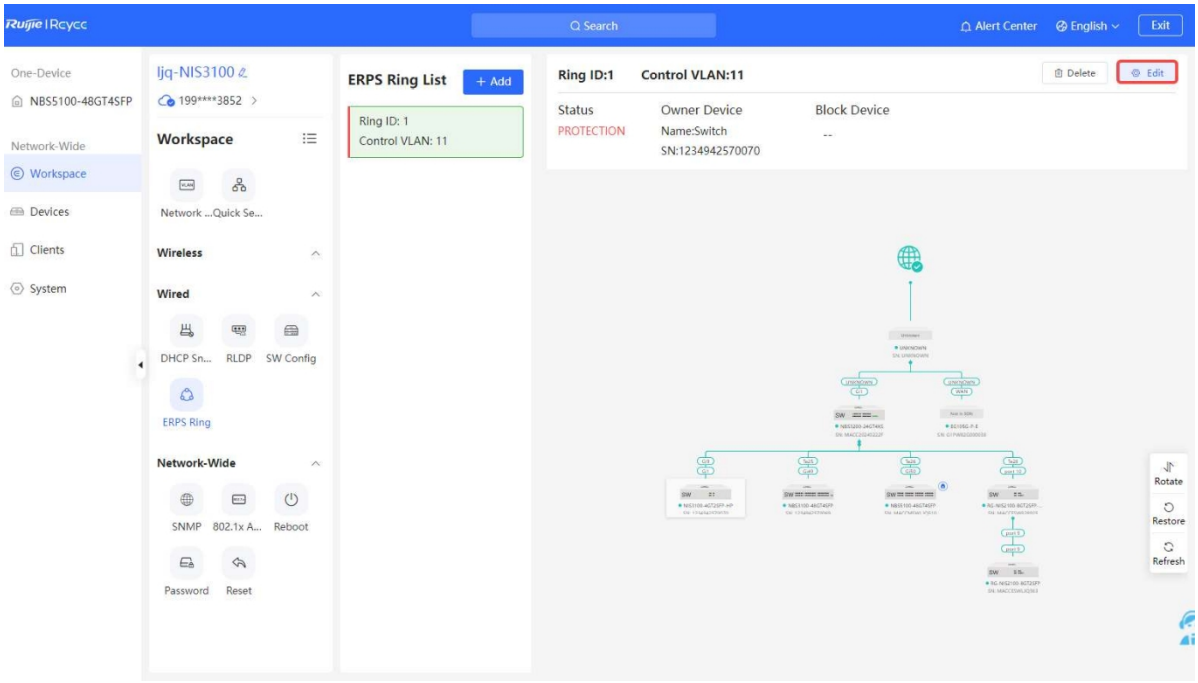
(4) Як показано на наступному малюнку, виберіть пристрій для кільця ERPS, встановіть Gi5 на **RPL OWNER**, а Gi6 на **НОРМАЛЬНО**. Натисніть "**Далі**".



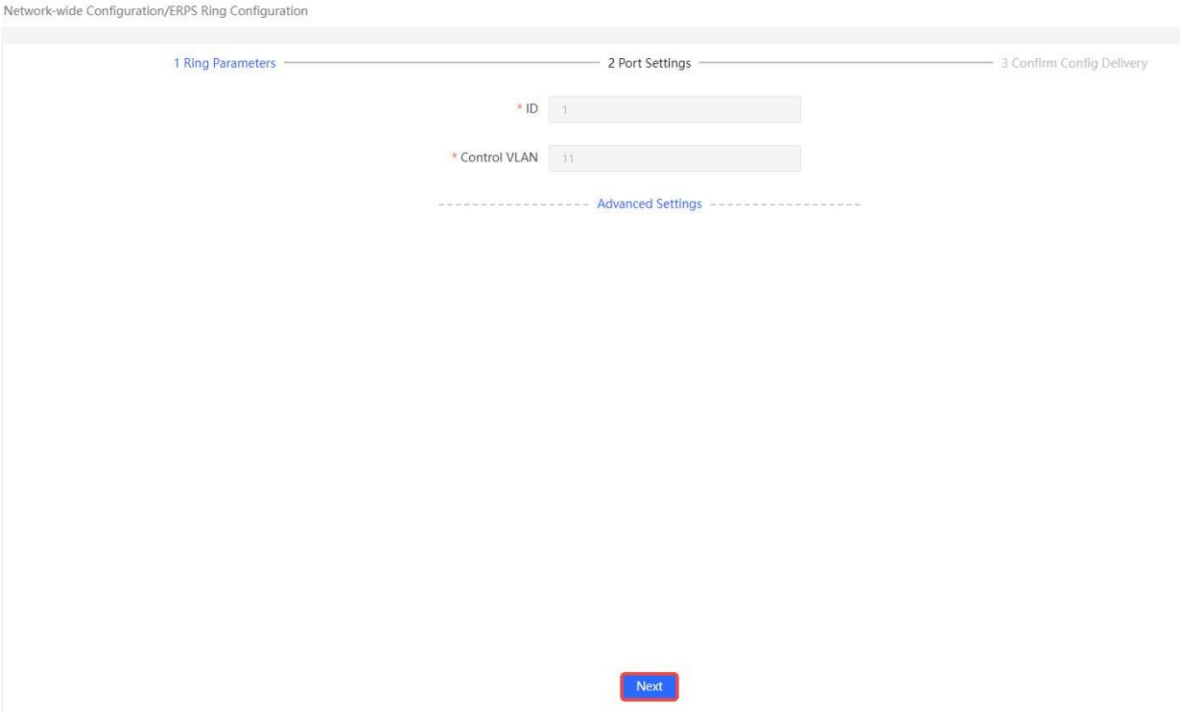
(5) Як показано на наступному малюнку, натисніть кнопку **Зберегти**, щоб зберегти конфігурацію.



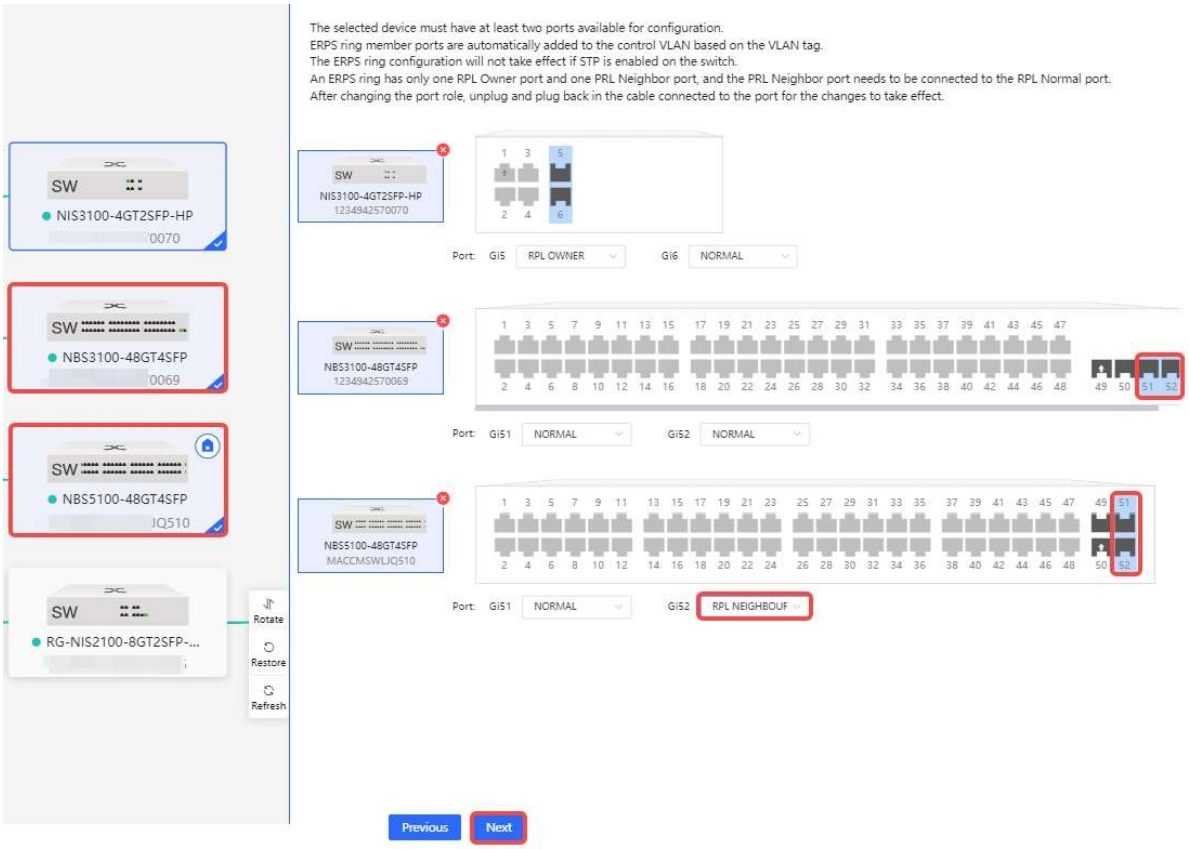
(6) Як показано на наступному малюнку, виберіть **Мережевий**> **Робоча область**> **Дротовий**> **ERPS-кільце**. На сторінці, що відкриється, натисніть **Редагувати**.



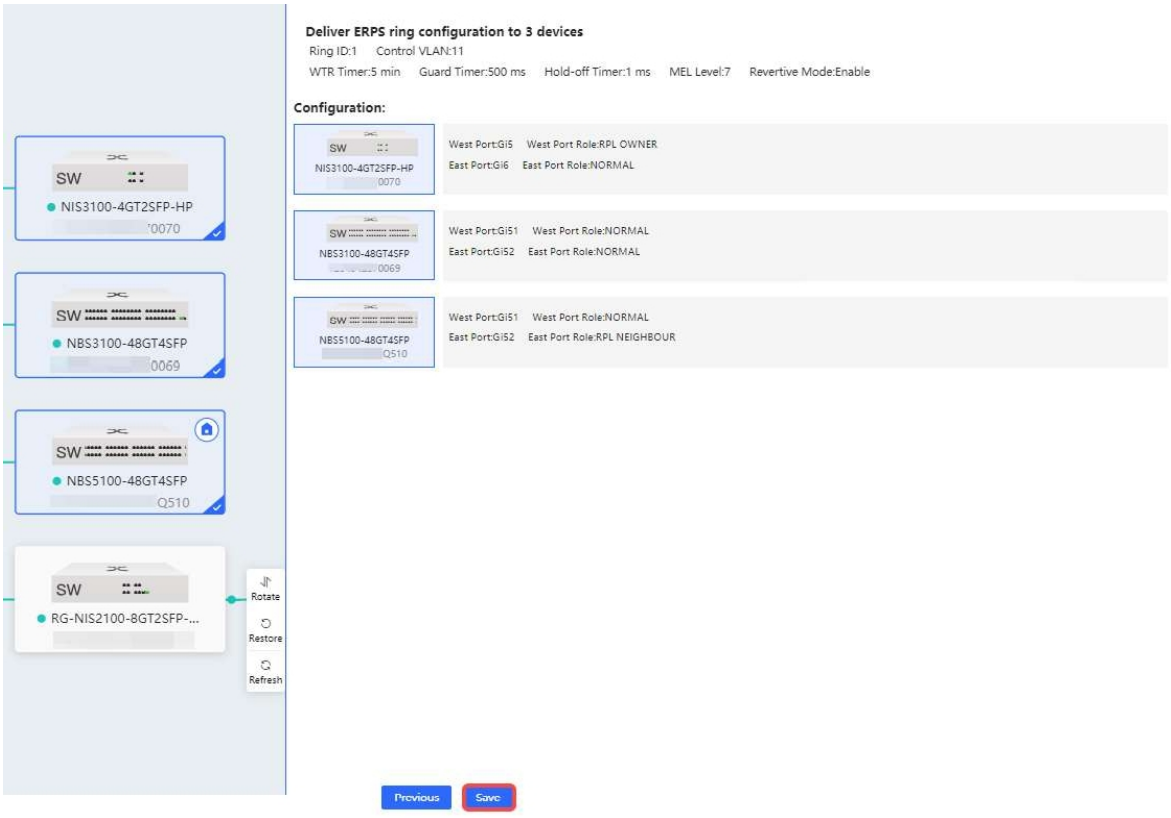
(7) Як показано на наступному малюнку, натисніть **Далі**, щоб перейти на сторінку **Конфігурація кільця ERPS**.



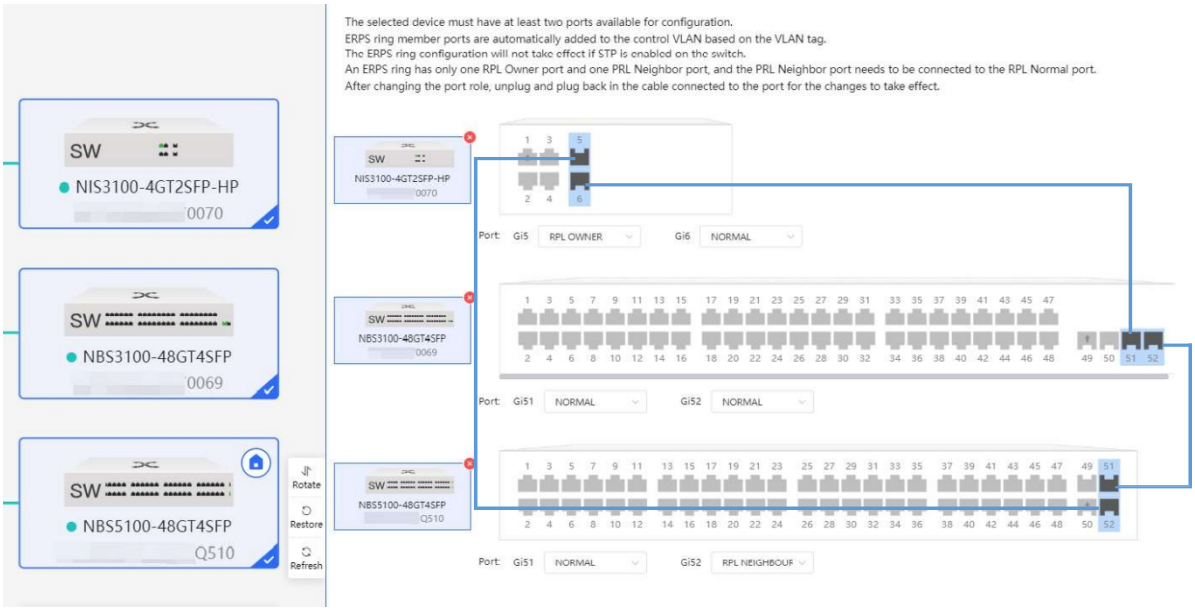
(8) Як показано на наступному малюнку, додайте решту пристроїв на сторінці **конфігурації кільця ERPS**. Виберіть оптичні порти на пристроях і налаштуйте інтерфейси, підключені до RPL OWNER, як RPL NEIGHBOR, як показано на прикладі Gi52 на малюнку нижче. Інші інтерфейси налаштуйте як НОРМАЛЬНІ. Після завершення конфігурації натисніть **Далі**.



(9) Як показано на наступному малюнку, натисніть **Зберегти**, щоб застосувати всі конфігурації.



(10) Як показано на малюнку нижче, після підключення всіх кабелів відповідно до топології, пристрої автоматично сформують кільце ERPS.



14.5 QoS

Специфікація

QoS можна переглядати або налаштовувати лише на пристроях під управлінням ReyeeOS 2.280 або новіших версій.

14.5.1 Огляд

Якість обслуговування (QoS) може задовольнити вимоги користувачів для різних додатків і різних рівнів якості обслуговування. Вона розподіляє і планує ресурси на основі вимог користувачів і забезпечує різні рівні якості обслуговування для різних пакетів.

У традиційній IP-мережі пристрій обробляє всі пакети однаково, тобто він обробляє пакети на основі часу їхнього надходження відповідно до стратегії черги "першим прийшов - першим пішов" (FIFO) і передає пакети до місця призначення за принципом "найкращих зусиль". Коли пропускна здатність мережі достатня, всі пакети обробляються належним чином; коли мережа перевантажена, всі пакети можуть бути відкинуті.

QoS призначає пріоритет передачі пакетам певного типу, щоб підкреслити важливість пакетів. Потім пристрої надають спеціальні послуги передачі для цих пакетів відповідно до політик переадресації для різних пріоритетів, уникнення перевантажень та інших механізмів. Завдяки QoS пристрій обробляє важливі пакети в реальному часі переважно, а пакети не в реальному часі та звичайні пакети обробляє з нижчими пріоритетами і навіть відкидає пакети в разі перевантаження мережі.

QoS підвищує передбачуваність продуктивності мережі, ефективно розподіляє пропускну здатність мережі та розумно використовує мережеві ресурси.

14.5.2 Принципи

1. Основні поняття

- Модель DiffServ

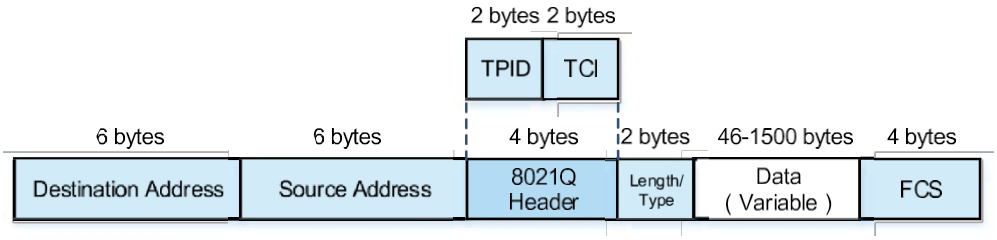
  Модель диференційованих послуг (DiffServ) класифікує всі пакети, що передаються в мережі, на різні типи. Класифікаційна інформація, пов'язана з маркуванням пріоритетів QoS, записується в деяких полях пакетів 2-го або 3-го рівнів, наприклад, у полі PRI кадрів IEEE 802.1Q, полі типу послуги (ToS) пакетів IPv4, полі класу трафіку (TC) пакетів IPv6 і полі експериментальних бітів (EXP) пакетів MPLS з багатопротокольною комутацією за мітками (MPLS).

  У мережі моделі DiffServ класифікаційна інформація пакетів може призначатися хостами або іншими мережевими пристроями, або на основі різних політик додатків, або на основі різного вмісту пакетів. Пристрій застосовує однакову політику обслуговування передачі до пакетів, що містять однакову класифікаційну інформацію, і застосовує різні політики обслуговування передачі до пакетів, що містять різну класифікаційну інформацію. На основі класифікаційної інформації, що міститься в пакетах, пристрій може надавати різні пріоритети передачі для різних пакетів, резервувати смугу пропускання для певного типу пакетів, відкидати певні пакети з нижчими пріоритетами або виконувати деякі інші дії.

- Поле PRI кадрів IEEE 802.1q

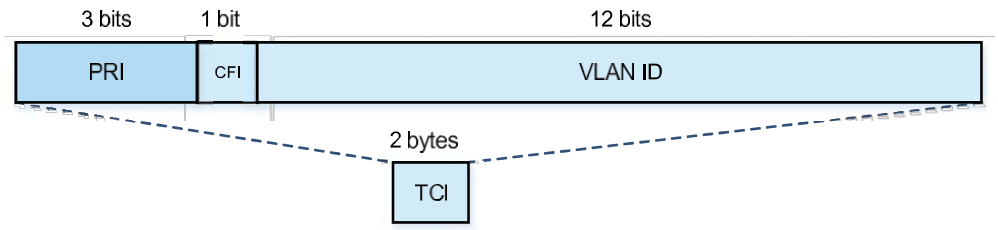
  Поле PRI кадрів IEEE 802.1Q (а саме, пріоритет IEEE 802.1p) знаходиться в заголовку пакета 2-го рівня, що містить заголовок тегу IEEE 802.1Q, як показано на рисунку 14-7.

Рисунок 14-7 Формат кадру рівня 2 із заголовком тегу IEEE 802.1Q



4-байтовий заголовок тегу IEEE 802.1Q містить 2-байтовий ідентифікатор протоколу тегу (TPID) та 2-байтову керуючу інформацію тегу (TCI). TCI містить 3-бітне поле PRI, як показано на рисунку 14-8.

Рисунок 14-8 Поле PRI фреймів IEEE 802.1q

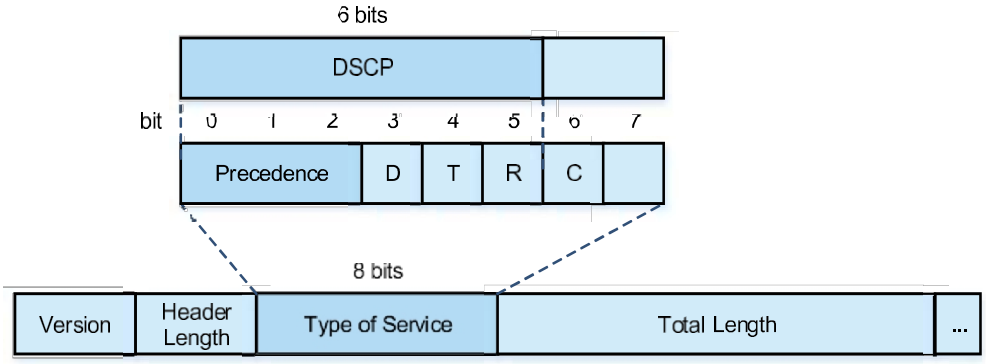


Поле PRI представляє вісім пріоритетів для передачі пакетів, а значення пріоритету від високого до низького - 7, 6, ..., 1 і 0. Пріоритет IEEE 802.1p застосовується в сценаріях, де не аналізувати заголовки 3-го рівня, а QoS потрібно реалізувати тільки на 2-му рівні.

- Поле ToS пакетів IPv4

  Пакети IPv4 використовують поле ToS в IP-заголовку для вказівки пріоритету пакетів, як показано на рисунку 14-9.

Рисунок 14-9 Поле ToS у заголовку IP-адреси



Поле ToS містить вісім бітів, з яких перші три біти є полем IP PRE (precedence) і представляють вісім пріоритетів для передачі пакетів, зі значеннями пріоритету від більшого до меншого: 7, 6, ..., 1 і 0.

RFC 2474 перевизначає поле ToS в IP-заголовку, в якому перші 6 бітів (біти від 0 до 5) представляють кодову точку диференційованих послуг (DSCP). DSCP використовується для класифікації пакетів на максимум 64 різні категорії.

- Поле ToS пакетів IPv6

  Пакети IPv6 використовують поле TC у заголовку IPv6 для вказівки пріоритету пакета, як показано на рисунку 14-10Рисунок 14-10.

Рисунок 14-10 Поле TC у заголовку IPv6

Поле TC містить вісім бітів і виконує ту саму функцію, що й поле ToS у пакетах IPv4. Перші шість бітів поля TC вказують на DSCP.

2. Мапування пріоритетів

Пріоритети використовуються для визначення вагових коефіцієнтів планування або пріоритетності пересилання пакетів. Для різних типів пакетів визначено різні типи пріоритетів: Кадри IEEE 802.1q використовують пріоритет IEEE 802.1p, IP-пакети використовують DSCP і так далі.

Після того, як пакет потрапляє на інтерфейс пристрою, пріоритет пакета зіставляється з CoS відповідно до режиму довіри, налаштованого для інтерфейсу. У Таблиці 14-9 показано відповідність між режимом довіри, налаштованим для інтерфейсу, і пріоритетами.

Таблиця 14-9 Режим довіри інтерфейсу та відображення пріоритетів

Режим довіри	Мапування пріоритетів
Ненадійний	● Пристрій не довіряє жодній інформації про пріоритет, що міститься у пакеті. ● Пакет, отриманий інтерфейсом, призначається до черги на основі таблиці відповідності 802.1p-черги використанням значення 802.1p (пріоритету інтерфейсу), налаштованого для інтерфейсу. ● Для пакета з тегом VLAN, надісланого інтерфейсом, пристрій повторно позначає значення 802.1p пакета на основі таблиці зіставлення queue-802.1p. ● Для пакетів без мітки VLAN, надісланих інтерфейсом, пристрій не повторно позначає значення 802.1p пакета. ● Якщо пакет, надісланий інтерфейсом, є IP-пакетомпристрій повторно значення DSCP пакета на основі таблиці зіставлення черги-DSCP.
802.1p	● Після того, як інтерфейс отримує пакет: o Якщо пакет містить тег VLAN, значення 802.1p, що міститься в пакеті, буде використано як вхідні дані для зіставлення, і пакет буде призначено до черги на основі таблиці зіставлення 802.1p-черги. o Якщо пакет не містить жодної мітки VLAN, він буде оброблений пристроєм так само, як і в ненадійному режимі. ● Для пакета з тегом VLAN, надісланого інтерфейсом, пристрій повторно позначає значення 802.1p пакета на основі таблиці зіставлення queue-802.1p. ● Для пакетів без мітки VLAN, надісланих інтерфейсом, пристрій не повторно позначає значення 802.1p пакета. ● Якщо пакет, надісланий інтерфейсом, є IP-пакетомпристрій повторно значення DSCP пакета на основі таблиці зіставлення черги-DSCP.
DSCP	● Після того, як інтерфейс отримує пакет: o Якщо пакет не є IP-пакетом, він буде оброблений пристроєм так само, як і в режимі 802.1p. o Якщо пакет є IP-пакетом, значення DSCP пакета буде використано як вхідні дані для зіставлення, і пакет буде призначено до черги основі таблиці зіставлення DSCP-черги. ● Якщо пакет, надісланий інтерфейсом, є IP-пакетомпристрій повторно значення DSCP пакета на основі таблиці зіставлення черги-DSCP. ● Якщо пакет, надісланий інтерфейсом, не є IP-пакетом, він обробляється залежно від того, чи містить він мітку VLAN: o Якщо пакет містить VLAN, пристрій повторно позначає значення 802.1p для пакетів на основі таблиці зіставлення queue-802.1p. o Якщо пакет не містить мітки VLAN, пристрій не повторно значення 802.1p пакета.

3. Управління заторами

Коли швидкість отримання пакетів перевищує швидкість відправлення, на інтерфейсі відправника виникає перевантаження. Якщо немає достатнього буфера для зберігання цих пакетів, може статися втрата пакетів. Механізм керування перевантаженням визначає порядок надсилання пакетів на основі їхніх локальних пріоритетів. Функція керування перевантаженням контролює перевантаження і покращує локальні пріоритети пакетів для деяких важливих даних. Коли виникає перевантаження, пакети з вищими пріоритетами надсилаються першими, щоб гарантувати, що ключові послуги надаються вчасно.

Управління перевантаженнями використовує механізм планування черги. Обробка відбувається наступним чином:

(1) Кожному пакету призначається черга на основі зіставлення пріоритету з чергою.

(2) Вихідний інтерфейс вибирає пакети в черзі для відправки відповідно до різних політик планування черги (наприклад, SP, WRR і SP+WRR).

- Політика планування SP

  При плануванні із суворим пріоритетом (SP) пакети плануються строго основі їхніх пріоритетів у черзі від високого до низького (більший ідентифікатор черги вказує на вищий пріоритет). Перш ніж надсилати пакет, перевірте, чи є пакет, який ви хочете надіслати, у черзі з високим пріоритетом. Якщо є, відправте його. Якщо ні, перевірте, чи є пакет для відправки в черзі наступного рівня, і так далі.

  Слабкість SP-планування полягає в тому, що при виникненні перевантаження, якщо пакети в черзі з вищим пріоритетом існують протягом тривалого часу, пакети в черзі з нижчим пріоритетом не мають можливості бути запланованими.

- Політика планування WRR

  Weighted Round Robin (WRR) гарантує, що всі черги плануються по черзі. На прикладі восьми вихідних черг пристрій розподіляє ресурси пропускної здатності на основі ваги кожної черги. Наприклад, якщо ваги WRR для порту 1000 Мбіт/с встановлені як 50, 50, 30, 30, 10, 10, 10, 10 і 10, WRR гарантує, що принаймні 50 Мбіт/с пропускної здатності буде виділено для черги з найнижчим пріоритетом. WRR також дозволяє ефективно використовувати пропускну здатність, негайно перемикаючись на наступну чергу, коли черга звільняється.

- Політика планування SP+WRR

  Планування SP налаштовується для однієї або декількох черг відправлення, а інші черги плануються в режимі WRR. Серед черг SP, тільки після того, як всі пакети в черзі SP з вищим пріоритетом відправлені, можуть бути відправлені пакети в черзі SP з наступним вищим пріоритетом. Між чергами SP і WRR тільки після відправлення всіх пакетів у черзі SP можна відправляти пакети в черзі WRR.

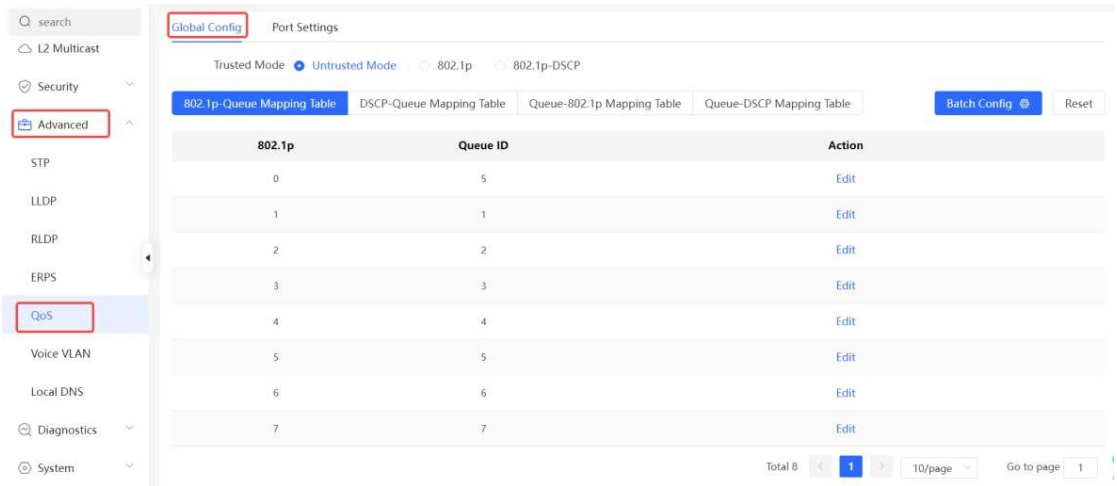
14.5.3 Налаштування QoS

1. Глобальна конфігурація

У режимі локального пристрою виберіть **Advanced QoS**> > **Global Config**.

На сторінці **Global Config** ви можете налаштувати режим довіри, змінити таблицю зіставлення 802.1p-черги для вхідних пакетів, змінити таблицю зіставлення DSCP-черги для вхідних пакетів, змінити таблицю зіставлення Queue-802.1p для вихідних пакетів і змінити таблицю зіставлення Queue-DSCP для вихідних пакетів.

Натисніть **Пакетна конфігурація** для пакетного налаштування цих таблиць зіставлення. Натисніть **Скинути**, щоб відновити значення таблиці зіставлення за замовчуванням.



Таблиця 14-10 Глобальна конфігурація Опис параметра

Параметр	Опис	Значення за замовчуванням
Довірений режим	Позначення пріоритетів вхідного пакета: **Недовірливий режим**: Пристрій не довіряє жодній інформації про пріоритет, що міститься в пакеті, і використовує пріоритет інтерфейсу як значення 802.1p для пакета. Пристрій призначає пакет до черги на основі таблиці зіставлення черг 802.1p. Якщо вибрано **режим Untrusted Mode**, будь-які пакети, отримані будь-яким інтерфейсом пристрою, будуть призначені до черг на основі пріоритету інтерфейсу, незалежно від стану режиму довіри, налаштованого на сторінці **Port Settings (Налаштування порту**). **802.1p**: Пристрій довіряє значенню 802.1p, що міститься в пакеті, і використовує значення 802.1p для призначення пакета до черги на основі таблиці відповідності 802.1p-черги. Якщо пакет не містить значення 802.1p, тобто не містить тегу VLAN, пристрій оброблятиме пакет так само, як і в ненадійному режимі. Якщо вибрано **802.1p**, а вказаний інтерфейс перебуває у ненадійному режимі на сторінці **налаштувань порту**, пристрій обробить пакет так само, як і у ненадійному режимі. **802.1p-DSCP**: Пристрій довіряє значенню 802.1p (для не-IP-пакетів) або DSCP (для IP-пакетів) пакета і призначає пакет до черги на основі таблиці відповідності 802.1p-черги або таблиці відповідності DSCP-черги залежно від значення 802.1p або DSCP пакета. Якщо вибрано **802.1p-DSCP**, а вказаний інтерфейс перебуває у ненадійному режимі на сторінці **Port Settings**, пристрій оброблятиме пакет так само, як і у ненадійному режимі.	Режим ненадійності
Таблиця зіставлення черг 802.1p	Вхідна таблиця зіставлення черг, яка містить між значенням 802.1p та черги. Наприклад, якщо значення 802.1p дорівнює 0, а ідентифікатор черги дорівнює 1, пакети зі значенням 802.1p 0 будуть призначені до черги 1.	Як показано в Таблиці 14-11
Таблиця відображення DSCP-черги	Таблиця зіставлення вхідних черг, яка містить відповідність між значенням DSCP та черги. Наприклад, якщо значення DSCP лежить у діапазоні від 0 до 7, а ідентифікатор черги дорівнює 0, пакети зі значенням DSCP від 0 до 7 будуть призначені до черги 0.	Як показано в Таблиці 14-12

Таблиця відображення черги-802.1p	Таблиця відображення вихідної черги, яка містить відображення між ідентифікатором черги та значенням 802.1p. Значення 802.1p вихідного пакета у черзі на основі відповідності. Наприклад, якщо черги дорівнює 0, а пакети з тегом VLAN у черзі 0 мають значення 802.1p, то значення 802.1p пакетів у черзі 0 буде на 2. Якщо пакет не містить жодного значення 802.1p, тобто пакет не містить жодного тегу VLAN, пристрій не змінює значення 802.1p пакета.	Як показано в Таблиці 14-13

Параметр	Опис	Значення за замовчуванням
Таблиця зіставлення черги-DSCP	Таблиця відображення вихідної черги, яка містить відображення між ідентифікатором черги та значенням DSCP. Значення DSCP пакетів у вихідній черзі перемарковується на основі відображення. Наприклад, якщо ідентифікатор черги дорівнює 0, а відображене значення DSCP дорівнює 8, то значення DSCP пакетів у черзі 0 буде змінено на 8.	Як показано в Таблиці 14-14

Таблиця 14-11 Стандартна таблиця зіставлення черг 802.1p на пристрої

802.1p Значення	Ідентифікатор черги
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Таблиця 14-12 Таблиця відображення DSCP-черги пристрою за замовчуванням

Значення DSCP	Ідентифікатор черги
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Таблиця 14-13 Черга за замовчуванням– 802.1p Таблиця зіставлення пристрою

Ідентифікатор черги	802.1p Значення після зауваження
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

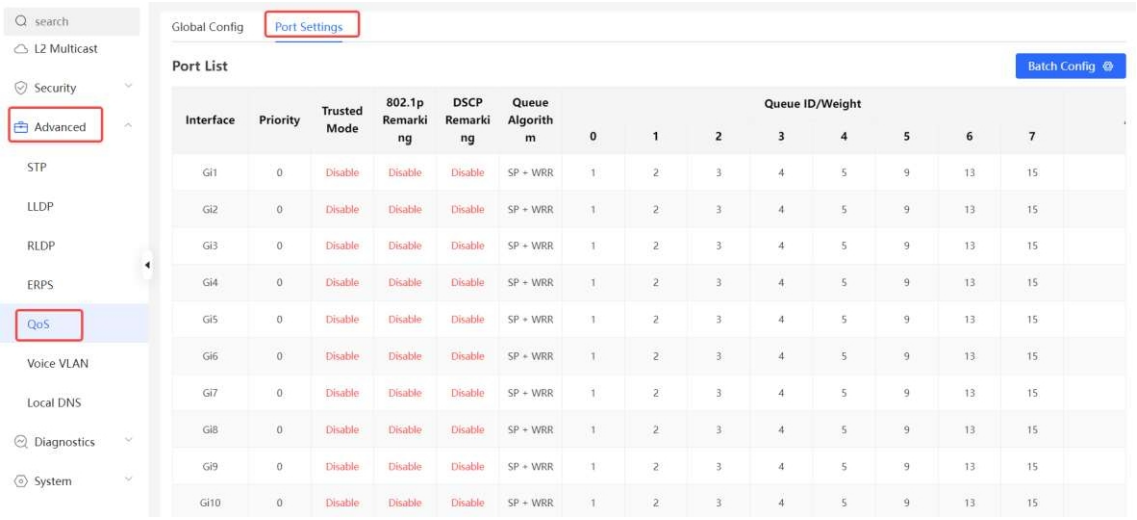
Таблиця 14-14 Таблиця зіставлення черги-DSCP пристрою за замовчуванням

Ідентифікатор черги	Значення DSCP після повторного маркування
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

2. Налаштування порту

У режимі локального пристрою виберіть **Додаткові**> **QoS**> **Налаштування порту**.

На сторінці **Port Settings** (**Налаштування порту**) ви можете встановити пріоритет, режим довіри, примітки 802.1p, примітки DSCP, алгоритм черги та ідентифікатор/вагу черги для визначеного інтерфейсу.



Таблиця 14-15 Конфігурація порту Опис параметра

Параметр	Опис	Значення за замовчуванням
Пріоритет	Пріоритет інтерфейсу. Коли пристрій перебуває в ненадійному режимі, пакети призначаються до черги на основі цього пріоритету, який еквівалентний значенню пакета 802.1p.	0
Довірений режим	Позначення пріоритетів вхідного пакета: Вимкнути: Пристрій не довіряє жодній інформації про пріоритет, що міститься у пакеті, і використовує пріоритет інтерфейсу як значення 802.1p для пакета. Пристрій призначає пакет черги на основі таблиці відповідності 802.1p-черги. Увімкнути: Пристрій довіряє значенню 802.1p (для не-IP-пакетів) або значенню DSCP (для IP-пакетів) пакета і призначає пакет до черги на основі таблиці відповідності 802.1p-черги або таблиці відповідності DSCP-черги залежно від значення 802.1p або DSCP пакета. Якщо на сторінці Global Config вибрано режим Untrusted Mode, будь-які пакети, отримані будь-яким інтерфейсом пристрою, будуть розподілені в черги на основі пріоритету інтерфейсу, незалежно від статусу режиму довіри, налаштованого на сторінці Port Settings (Налаштування порту). Якщо на сторінці Global Config вибрано 802.1p або 802.1p-DSCP, пристрій оброблятиме пакети, отримані вказаним інтерфейсом, так само, як і в довіреному режимі, якщо для параметра Trusted Mode вказаного інтерфейсу встановлено значення Enable (Увімкнути) на сторінці Port Settings (Налаштування порту).	Вимкнути

802.1p Примітка	Увімкнути: Значення 802.1p пакетів у черзі буде перемарковано основі таблиці відображення черги-802.1p. Вимкнути: Пристрій не повторно позначає значення 802.1p пакетів у черзі на основі таблиці зіставлення Queue-802.1p і позначає пріоритет вихідних пакетів на основі пріоритету вхідної черги.	Увімкнути
Зауваження ДКЗС	Увімкнути: Значення DSCP пакетів у черзі перемарковується основі таблиці відображення DSCP-802.1p. Вимкнути: Пристрій не повторно позначає значення DSCP пакетів у черзі на основі таблиці відображення Queue-802.1p і позначає пріоритет вихідних пакетів на основі пріоритету вхідної черги.	Увімкнути
Алгоритм черги	Алгоритм черги, прийнятий інтерфейсом.	SP+WRR
Ідентифікатор/вага черги	WRR вага черги. Значення 0 вказує на те, що для черги прийнято алгоритм SP. Після відправлення всіх пакетів у всіх SP-чергах пристрій переходить до відправлення пакетів у . Серед SP-черг першою планується черга з більшим ідентифікатором.	Як показано в Таблиці 14-16

Таблиця 14-16 Ідентифікатор черги інтерфейсу за замовчуванням/вага пристрою

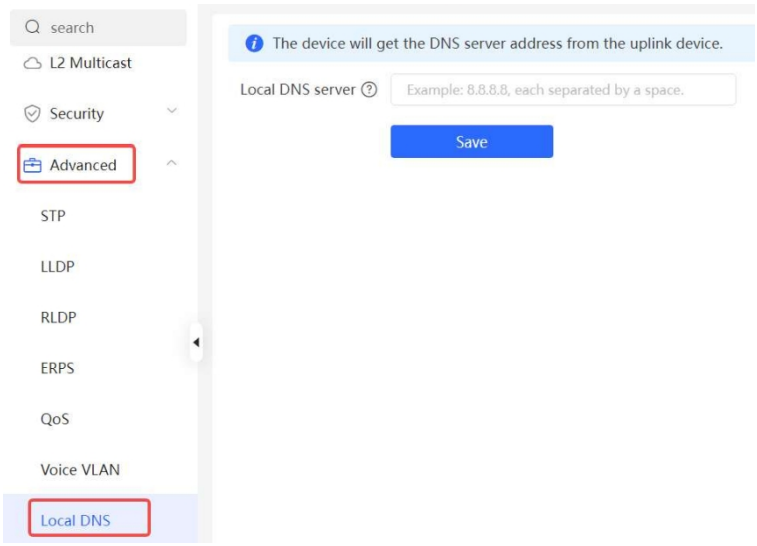
Ідентифікатор черги	Вага WRR
0	1
1	2
2	3
3	4
4	5
5	9
6	13
7	15

14.6 Налаштування локального DNS

Локальний DNS-сервер не є обов'язковим. За замовчуванням пристрій отримує адресу DNS-сервера від підключеного пристрою висхідної лінії зв'язку.

Виберіть **Локальний пристрій**> **Додатково**> **Локальний DNS**.

Введіть адресу DNS-сервера, який використовується локальним пристроєм. Якщо існує декілька адрес, розділіть їх пробілами. Натисніть **Зберегти**. Після налаштування локальної DNS пристрій спочатку використовує DNS IP-адреси керування для розбору доменних імен. Якщо пристрій не може розібрати доменні імена, використовуйте цю DNS-адресу.



14.7 Голосова VLAN

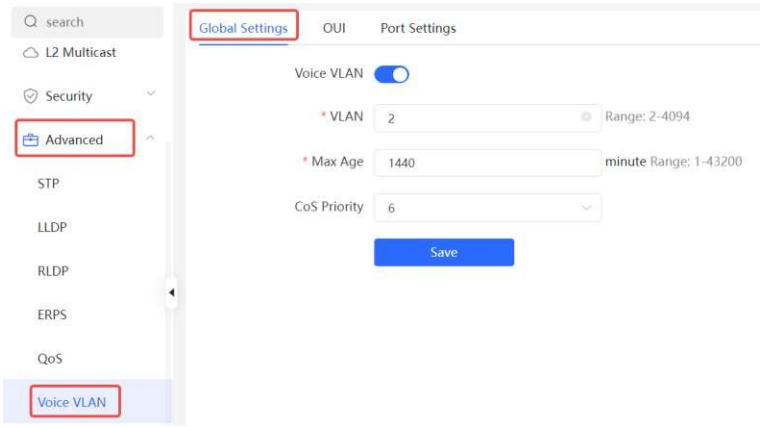
14.7.1 Огляд

Голосова віртуальна локальна мережа (VLAN) - це VLAN, призначена для голосового трафіку користувачів. Створивши голосову VLAN і додавши до неї порти, підключені до голосових пристроїв, ви можете передавати голосові дані в голосовій VLAN і забезпечувати задану політику якості обслуговування (QoS) для голосових потоків, щоб поліпшити пріоритет передачі голосового трафіку і забезпечити якість зв'язку.

14.7.2 Глобальна конфігурація голосової VLAN

Виберіть **Локальний пристрій> Додатково> Голосова локальна мережа> Глобальні налаштування**.

Увімкніть функцію голосової VLAN, налаштуйте глобальні параметри та натисніть **Зберегти**.



Таблиця 14-17 Опис параметрів глобальної конфігурації VLAN

Параметр	Опис	Значення за замовчуванням
Голосова VLAN	Чи вмикати функцію Voice VLAN	Вимкнути

Параметр	Опис	Значення за замовчуванням
VLAN	Ідентифікатор VLAN як голосова VLAN	NA
Максимальний вік	Час старіння голосової VLAN, у хвилинах. В автоматичному режимі, після старіння MAC-адреси в голосовому пакеті, якщо протягом часу старіння на порт більше не надходять голосові пакети, пристрій видаляє цей порт з голосової VLAN	1440 хвилин
Пріоритет Угоди про партнерство та співробітництво	Пріоритет 2-го рівня для пакетів голосового потоку в голосовій VLAN. Діапазон значень від 0 до 7. Більше значення означає вищий пріоритет. Ви можете змінити пріоритет голосового трафіку для покращення якості дзвінків.	6

14.7.3 Налаштування інтерфейсу користувача голосової VLAN

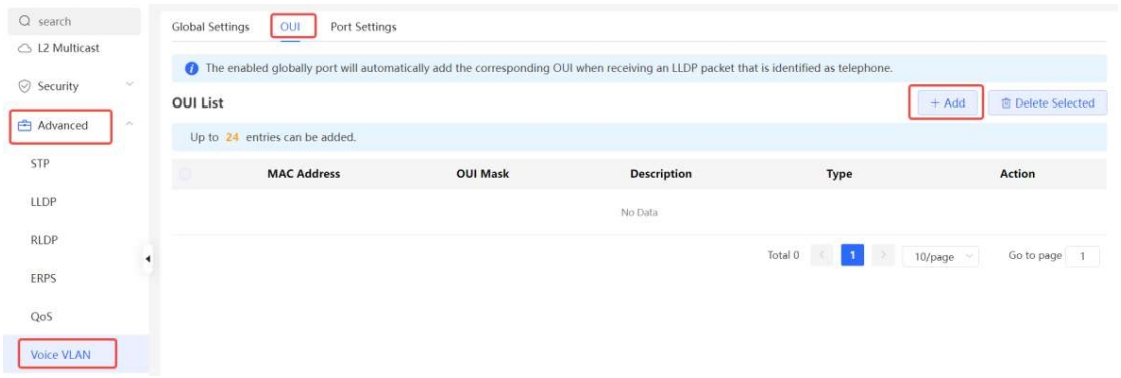
Виберіть **Локальний пристрій**> **Додатково**> **Голосова локальна мережа**> **OUI**.

MAC-адреса джерела голосового пакета містить організаційно унікальний ідентифікатор (OUI) виробника голосового пристрою. Після налаштування OUI голосової VLAN пристрій порівнює OUI голосової VLAN з MAC-адресою джерела в отриманому пакеті для ідентифікації пакетів голосових даних і надсилає їх до голосової VLAN для передавання.

Примітка

Після функції голосової VLAN на порту, коли порт отримує пакети LLDP, надіслані IP-телефонами, він може ідентифікувати поля можливостей пристрою в пакетах та ідентифікувати пристрої з функцією **"Телефон"** як голосові пристрої. Він також витягує вихідну MAC-адресу пакету протоколу і обробляє її як MAC-адресу голосового пристрою. Таким чином, OUI може бути додано автоматично.

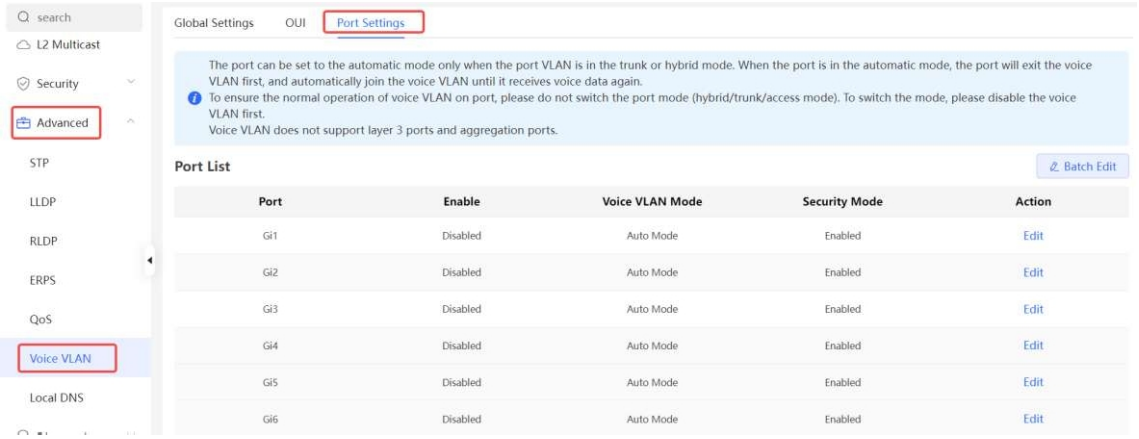
Натисніть **Додати**. У діалоговому вікні, що з'явиться, введіть MAC-адресу та OUI і натисніть **OK**.

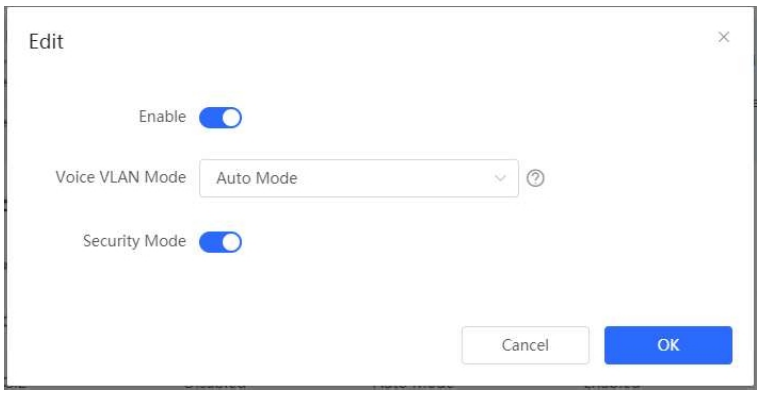


14.7.4 Налаштування функції голосової VLAN на порту

Виберіть **Локальний пристрій> Додатково> Голосова локальна мережа> Налаштування портів**.

Натисніть кнопку **Змінити** у записі порту або натисніть кнопку **Пакетне редагування** у верхньому правому куті. У діалоговому вікні, що з'явиться, виберіть, чи потрібно ввімкнути функцію голосової VLAN на порту, режим голосової VLAN, який буде застосовано, і чи потрібно ввімкнути режим безпеки, а потім натисніть кнопку **OK**.





Таблиця 14-18 Опис параметрів конфігурації голосової VLAN на порту

Параметр	Опис	Значення за замовчуванням
Голосовий режим VLAN	Залежно від способу ввімкнення функції VLAN на порту, режим Voice VLAN може бути автоматичним або ручним: ● **Автоматичний режим**: У цьому режимі пристрій перевіряє, чи містять дозволені VLAN порту голосову VLAN після ввімкнення функції голосової VLAN на порту. Якщо так, пристрій видаляє голосову VLAN із дозволених VLAN порту, доки порт не отримає голосовий пакет, що містить вказаний OUI. Після цього пристрій автоматично додає голосову VLAN до дозволених VLAN порту. Якщо порт не отримує голосовий пакет зазначеним OUI протягом глобального часу старіння, пристрій видаляє голосову VLAN із дозволених VLAN порту. ● **Ручний режим**: Якщо дозволені VLAN порту містять голосову VLAN, голосові пакети можна передавати в голосову VLAN.	Автоматичний режим
Режим безпеки	Коли режим безпеки увімкнено, у голосовій VLAN можна передавати лише голосовий трафік. Пристрій перевіряє MAC-адресу джерела в кожному пакеті. Якщо MAC-адреса джерела в пакеті збігається з OUI голосової VLAN, пакет може бути переданий у голосову VLAN. В іншому випадку пристрій відкидає пакет. Коли режим безпеки , MAC-адреси джерел пакетів не перевіряються, і всі пакети можуть передаватися в голосову VLAN.	Увімкнути

Застереження

- Режим голосової VLAN порту може бути встановлений як авторежим, тільки якщо режим VLAN порту - магістральний. Якщо режим голосової VLAN порту працює в автоматичному режимі, порт спочатку виходить з голосової VLAN і автоматично додається до голосової VLAN тільки після отримання голосових даних.
- Після ввімкнення функції голосової VLAN на порту не перемикайте порт режим 2-го рівня (магістральний або режим доступу), щоб забезпечити нормальну функції. Якщо вам потрібно порт у режим 2-го рівня, спочатку вимкніть функцію голосової VLAN на порту.
- Не рекомендується передавати голосові та службові дані через голосову VLAN. Якщо ви хочете передавати голосові та службові дані через голосову VLAN, вимкніть функцію голосової VLAN у режимі безпеки.
- Функція голосової VLAN недоступна на портах 3-го рівня або агрегованих інтерфейсах.

14.8 Налаштування інтелектуального гарячого резерву

Інтелектуальне гаряче резервування дозволяє декільком комутаторам діяти як пристрої гарячого резервування один для , забезпечуючи безперебійну переадресацію даних у разі збою в одній точці.

Примітка

Інтелектуальний гарячий резерв підтримується тільки на комутаторах серій RG-NBS7006, RG-NBS7003, RG-NBS5300 і RG-NBS5200.

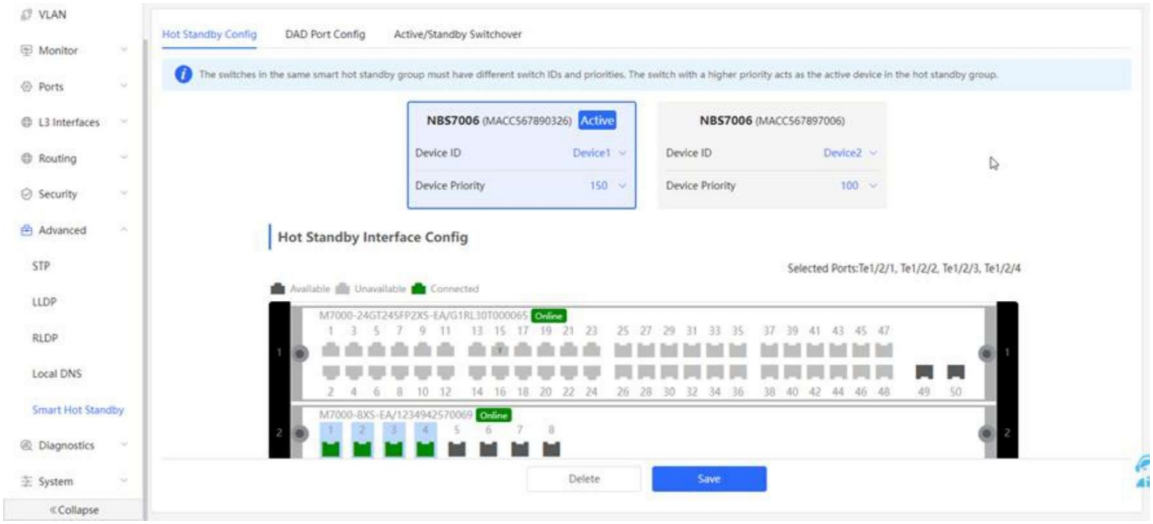
14.8.1 Налаштування гарячого резерву

Перегляд або зміна вибраних інтерфейсів гарячого резерву, ідентифікаторів пристроїв і пріоритетів. Перемикач з вищим пріоритетом обирається активним перемикачем у групі гарячого резерву.

Застереження

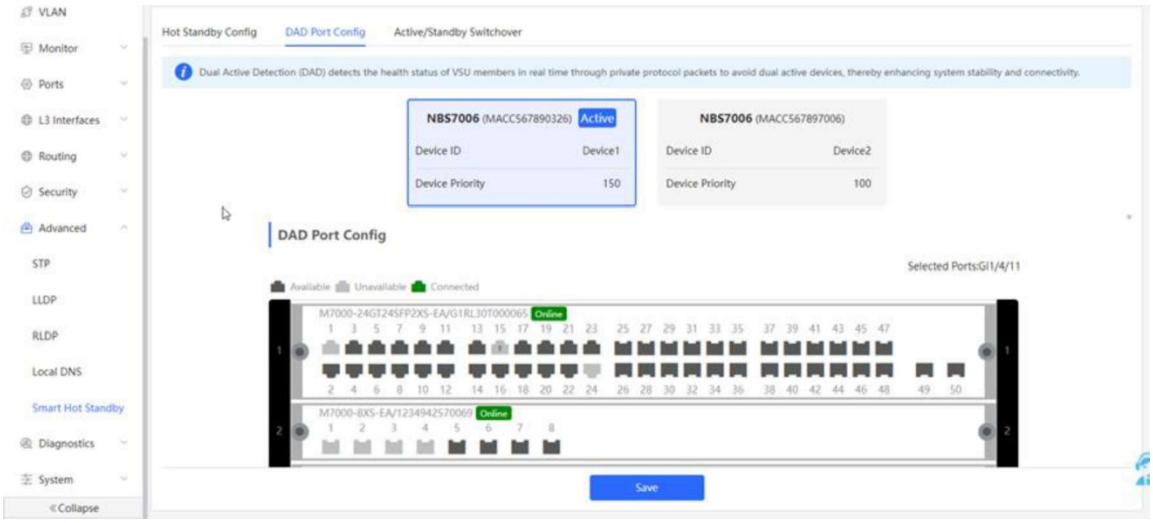
Пристрої в групі гарячого резерву повинні мати унікальні ідентифікатори пристроїв і налаштовані пріоритети.

Виберіть **Локальний пристрій**> **Додатково**> **Розумний гарячий режим очікування**.



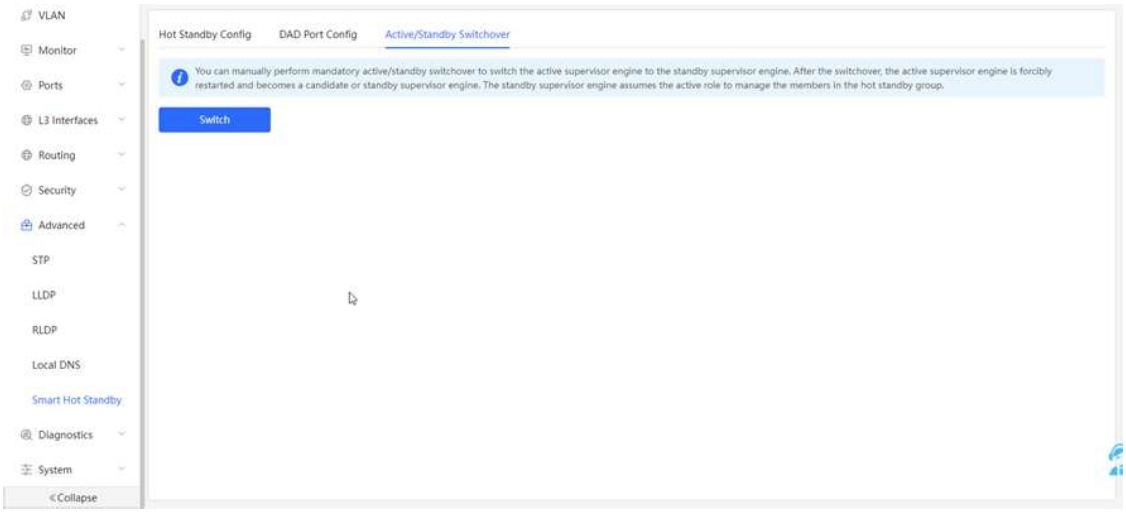
14.8.2 Налаштування інтерфейсів DAD

Після вибору інтерфейсів DAD активного і резервного комутаторів з'єднайте ці інтерфейси DAD мережевим кабелем, щоб запобігти збоям у мережі, спричиненим двома активними пристроями.



14.8.3 Перемикання між активним і резервним режимами

Перемикання між активним і резервним двигунами дозволяє вручну перемикатися між активним і резервним двигунами супервізора. Натискання кнопки Перемикання перезапустить двигун супервізора. Будь ласка, будьте обережні.


VLAN
Monitor
Ports
L3 Interfaces
Routing
Security
Advanced
STP
LLDP
RLDP
Local DNS
Smart Hot Standby
Diagnostics
System
Collapse
Hot Standby Config
DAD Port Config
Active/Standby Switchover
You can manually perform mandatory active/standby switchover to switch the active supervisor engine to the standby supervisor engine. After the switchover, the active supervisor engine is forcibly restarted and becomes a candidate or standby supervisor engine. The standby supervisor engine assumes the active role to manage the members in the hot standby group.
Switch

15 Діагностика

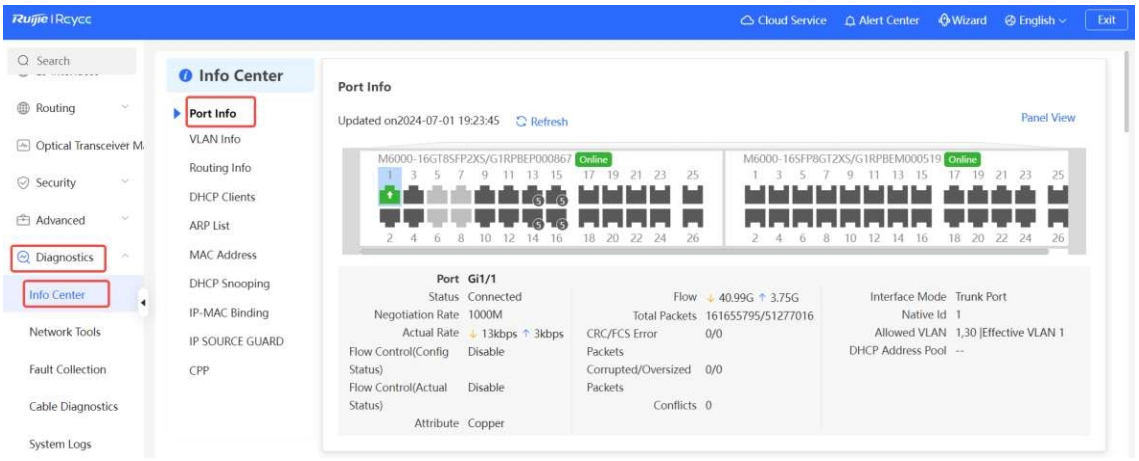
Застереження

Якщо проблема не зникає, незважаючи на методи усунення несправностей, наведені в цьому розділі, вам може знадобитися віддалена підтримка технічного спеціаліста, який увімкне режим розробника, щоб вирішити проблему. Ми забезпечимо захист ваших даних під час цього процесу.

15.1 Інформаційний центр

Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**.

В Інфоцентрі ви можете переглянути трафік портів, інформацію про VLAN, інформацію про маршрутизацію, список клієнтів, список ARP, MAC-адреси, DHCP-сканування, прив'язку IP-MAC, IP Source Guard і CPP-статистику пристрою та відповідних конфігурацій.



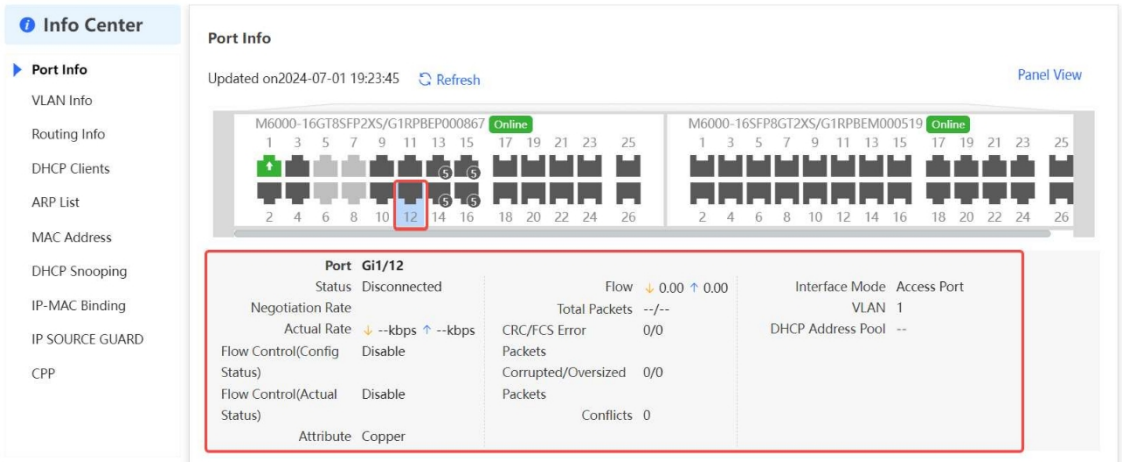
15.1.1 Інформація про порт

Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**> **Інформація про порт**.

Інформація про порт відображає інформацію про стан і конфігурацію порту. Натисніть на іконку порту, щоб переглянути детальну інформацію про порт.

Примітка

- Щоб налаштувати керування потоком порту або оптичні/електричні атрибути комбінованого порту, див. розділ 7.2 Конфігурація порту.
- Щоб налаштувати режим 2-го рівня порту і VLAN, до якої він належить, див. розділ 5.3 Налаштування VLAN порту.



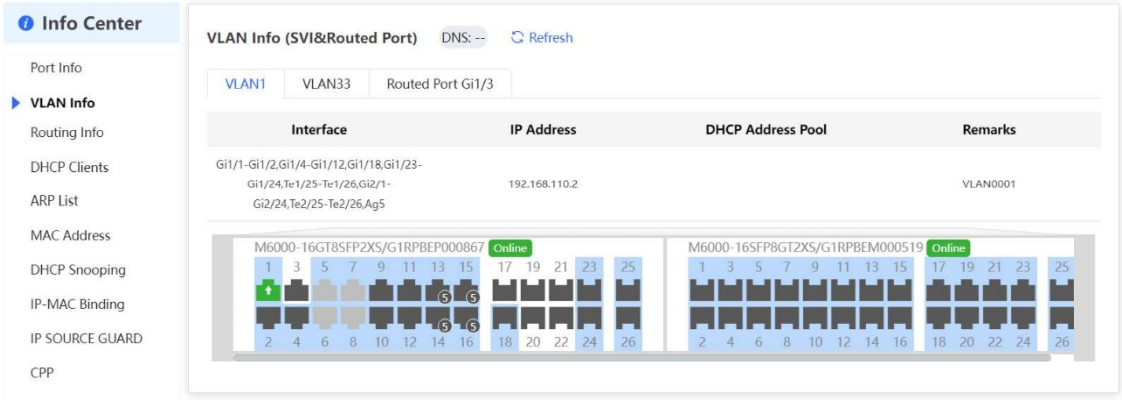
15.1.2 Інформація про мережу VLAN

Виберіть **Локальний пристрій> Діагностика> Інформаційний центр> Інформація про локальну мережу**.

Відображення інформації про SVI-порт і маршрутизований порт, включаючи інформацію про порт, включений до VLAN, IP-адресу порту і те, чи ввімкнено пул адрес DHCP.

Примітка

- Щоб налаштувати VLAN, див. розділ 5 VLAN.
- Щоб налаштувати порти SVI і маршрутизовані порти, див. розділ 10.1 Налаштування інтерфейсу 3-го рівня.



15.1.3 Інформація про маршрут

Специфікація

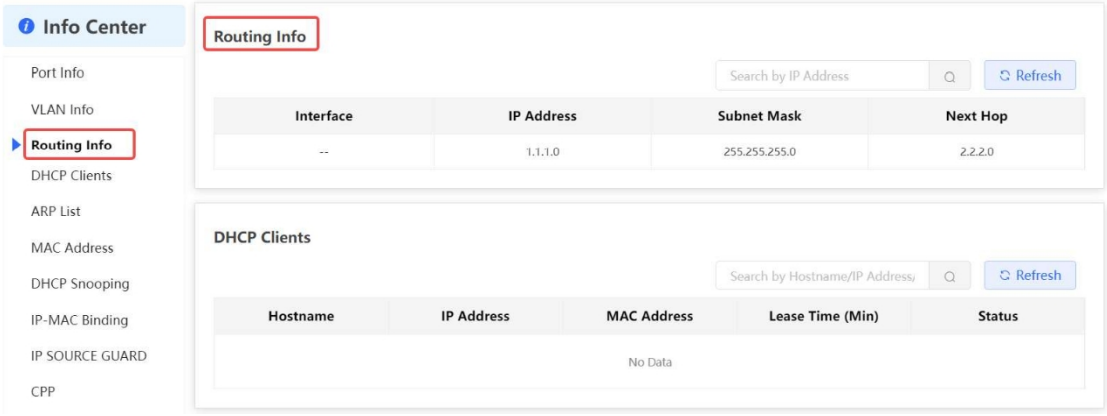
Якщо пристрій не підтримує функції рівня 3 (наприклад, комутатори RG-NBS3100 і RG-NBS3200), ця інформація не відображається.

Виберіть **Локальний пристрій> Діагностика> Інформаційний центр> Інформація про маршрутизацію**.

Відображає інформацію про маршрутизацію на пристрої. Поле пошуку у правому верхньому куті підтримує пошук маршрутів за IP-адресами.

Примітка

Щоб налаштувати статичні маршрути, див. розділ 11.1 Налаштування статичних маршрутів.



15.1.4 Клієнти DHCP

Специфікація

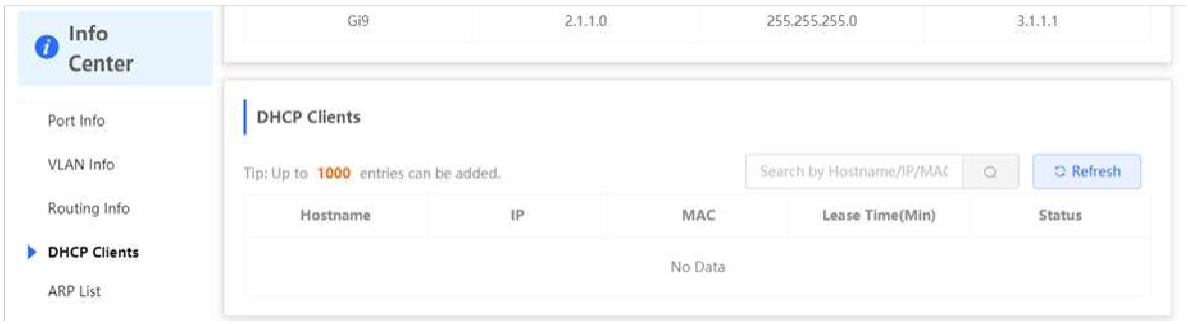
Якщо пристрій не підтримує функції рівня 3 (наприклад, комутатори RG-NBS3100 і RG-NBS3200), ця інформація не відображається.

Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**> **Клієнти DHCP**.

Відображає інформацію про IP-адреси, призначені кінцевим точкам пристроєм як DHCP-сервером.

Примітка

Щоб налаштувати функції, пов'язані з DHCP-сервером, див. розділ 10.3.2 Перегляд клієнта DHCP.



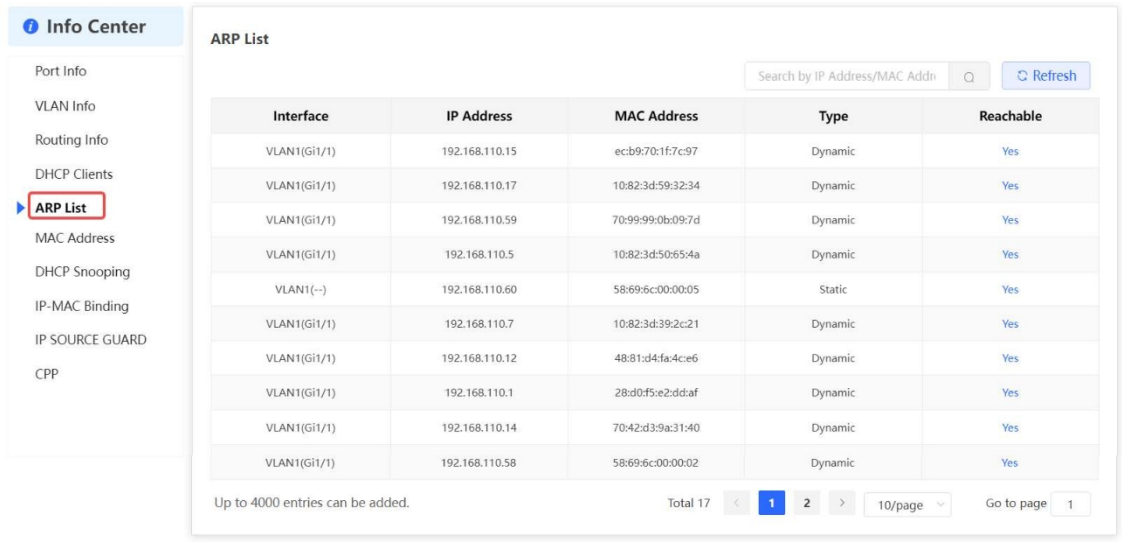
15.1.5 ARP-список

Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**> **ARP-список**.

Список ARP відображає динамічно вивчені і статично налаштовані записи ARP на пристрої. Ви можете переглянути доступність, тип, IP-адресу, MAC-адресу та фізичний інтерфейс, що відповідає кожній MAC-адресі.

Примітка

Щоб прив'язати динамічний ARP або вручну налаштувати статичний ARP, див. розділ 10.6 Налаштування статичного запису ARP.



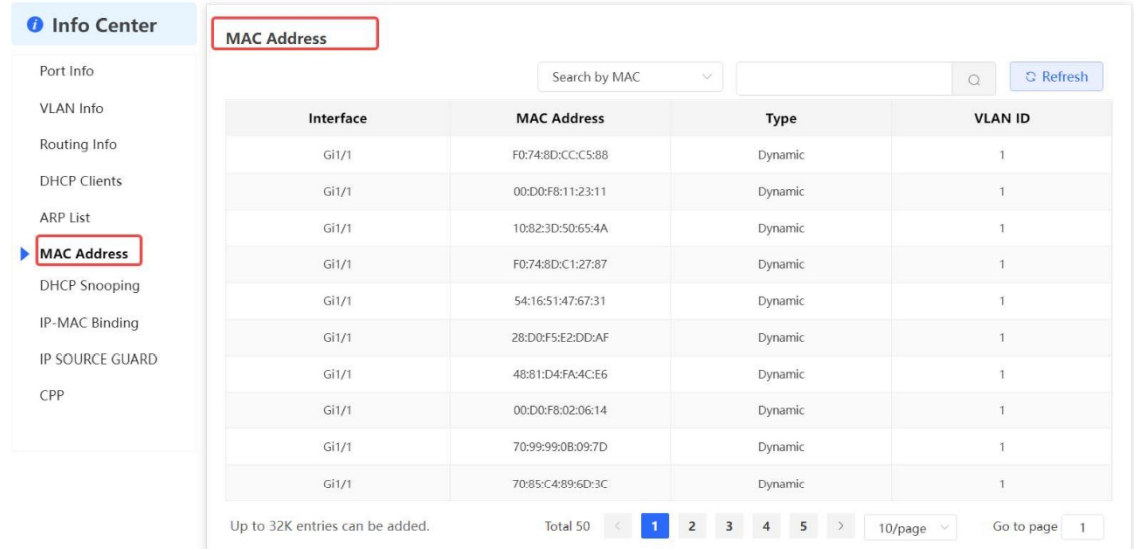
15.1.6 MAC-адреса

Виберіть **Локальний пристрій> Діагностика> Інформаційний центр> MAC-адреса**.

Відображає інформацію про MAC-адресу пристрою, включаючи статичну , налаштовану користувачем вручну, MAC-адресу фільтрації та динамічну MAC-адресу, автоматично отриману пристроєм.

Примітка

Щоб налаштувати та керувати MAC-адресами, див. розділ 6.2 Керування клієнтами.



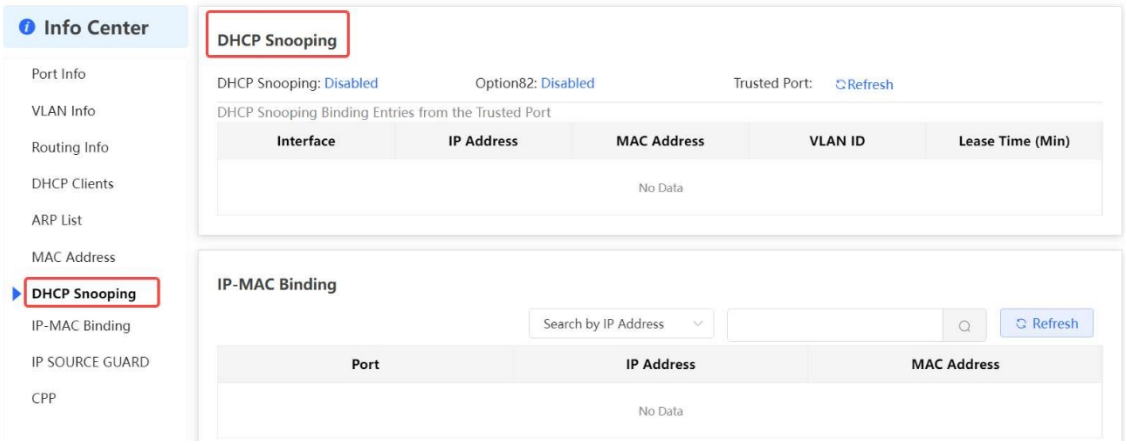
15.1.7 DHCP Snooping

Виберіть **Локальний пристрій> Діагностика> Інформаційний центр> DHCP Snooping**.

Відображає поточну конфігурацію функції DHCP-сканування та інформацію про користувача, динамічно отриману довірчим портом.

Примітка

Щоб змінити конфігурацію, пов'язану зі спостереженням DHCP, див. розділ 13.1 DHCP Snooping.



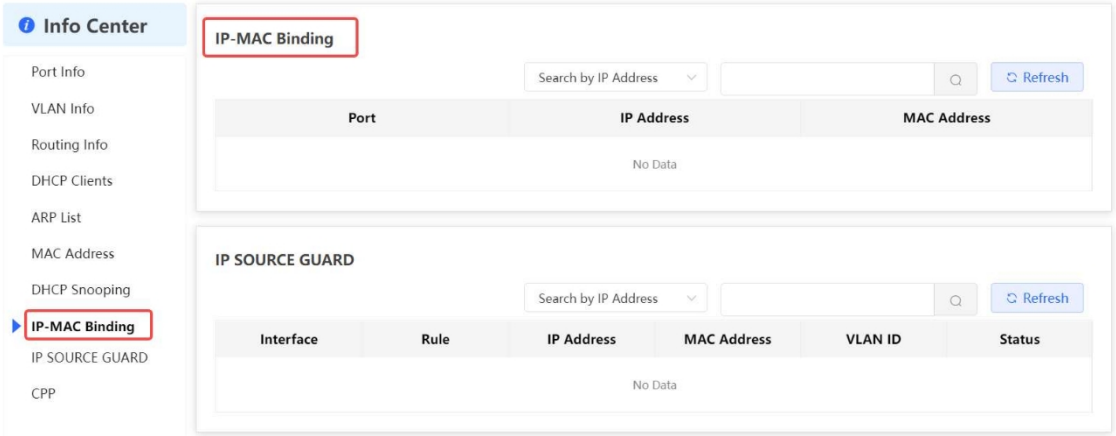
15.1.8 Прив'язка IP-MAC

Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**> **Прив'язка IP-MAC**.

Відображає налаштовані записи прив'язки IP-MAC. Пристрій перевіряє, чи відповідають IP-адреси джерела та MAC-адреси джерела IP-пакетів тим, що налаштовані для пристрою, і відфільтровує IP-пакети, які не відповідають прив'язці.

Примітка

Щоб додати або змінити прив'язку IP-MAC, див. розділ 13.5 Прив'язка IP-MAC.



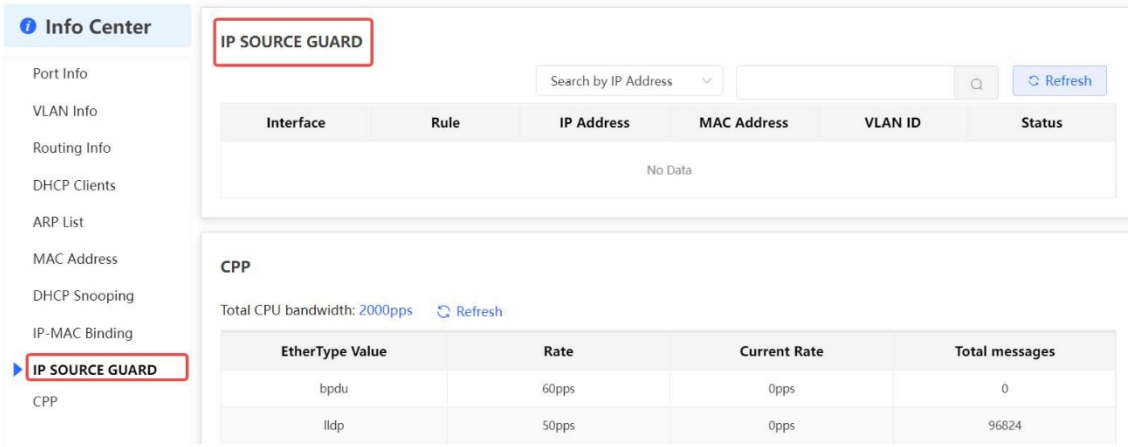
15.1.9 Захист джерела IP-адреси

Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**> **Захист джерел**.

Відображає список прив'язок функції захисту IP-джерел. Функція IP Source Guard перевірятиме IP-пакети з портів, яким не довіряє DHCP, згідно зі списком, і відфільтровуватиме IP-пакети, яких немає у списку прив'язки.

Примітка

Щоб налаштувати функцію захисту IP-джерел, див. розділ 13.5 Прив'язка IP-MAC.

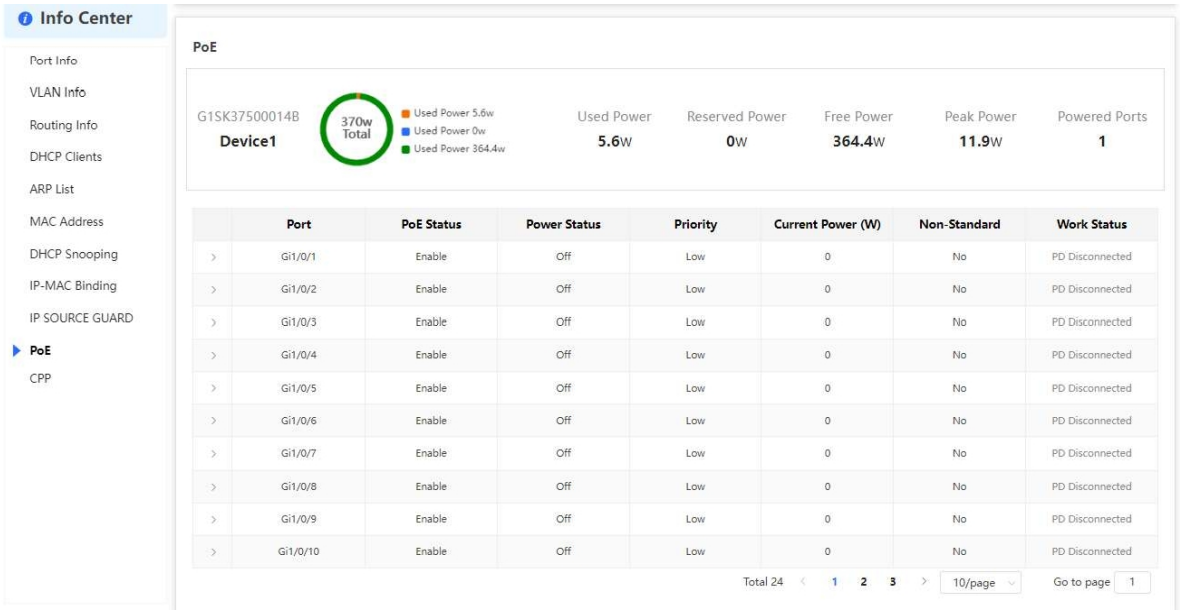


15.1.10 PoE

Специфікація

Цю функцію підтримують лише комутатори PoE (назва моделі містить– P, -LP, -HP та -UP).

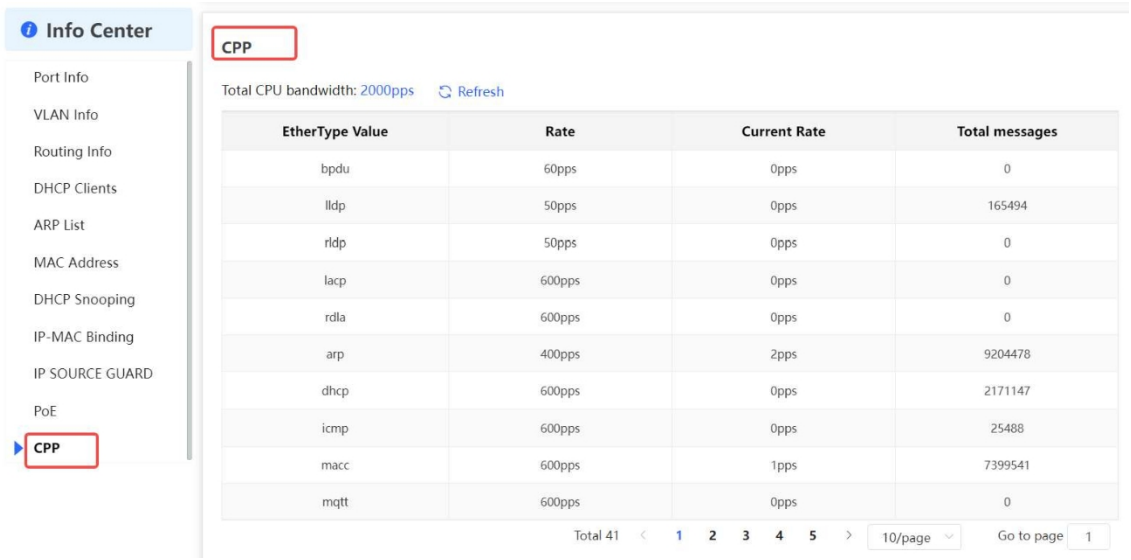
Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**> **PoE.**



15.1.11 Інформація про CPP

Виберіть **Локальний пристрій**> **Діагностика**> **Інформаційний центр**> **CPP**.

Відображає поточну загальну пропускну здатність процесора і статистику різних типів пакетів, зокрема пропускну здатність, поточну швидкість і загальну кількість пакетів.



15.2 Мережеві інструменти

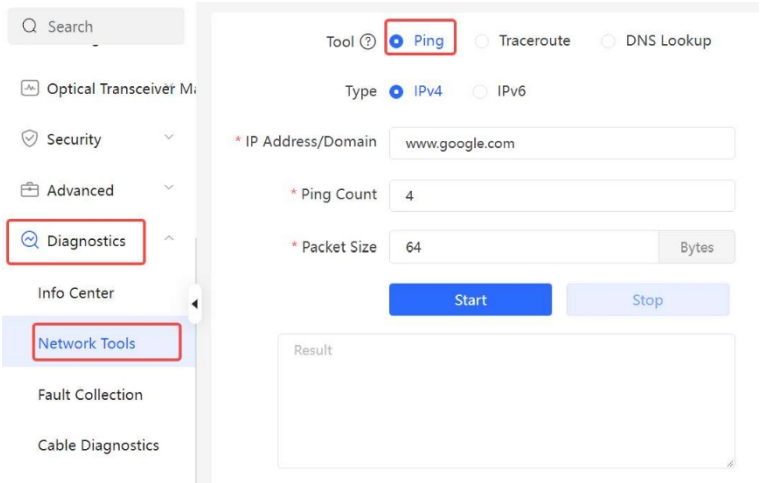
Сторінка **Мережеві інструменти** містить три інструменти для визначення стану мережі: **Ping**, **Traceroute** і **DNS Lookup**.

15.2.1 Пінг!

Виберіть **Локальний пристрій> Діагностика> Мережеві інструменти**.

Команда **Ping** використовується для виявлення підключення до мережі.

Виберіть **Ping** як режим діагностики, введіть IP-адресу призначення або адресу веб-сайту, налаштуйте кількість пінгів і розмір пакетів та натисніть кнопку **Почати**, щоб перевірити мережеве з'єднання між пристроєм та IP-адресою або веб-сайтом. Якщо з'явиться повідомлення "Ping не вдалося", це означає, що пристрій не може зв'язатися з IP-адресою або веб-сайтом.



15.2.2 Маршрут

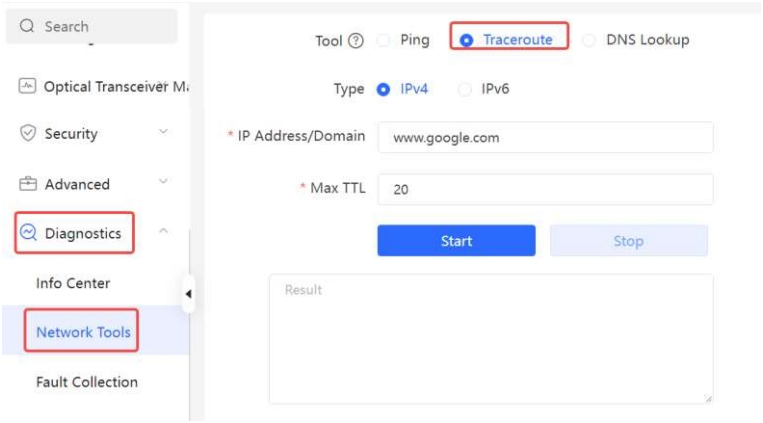
Виберіть **Локальний пристрій> Діагностика> Мережеві інструменти**.

Функція **Traceroute** використовується для визначення мережевого шляху від одного пристрою до іншого. У простій мережі мережевий шлях може проходити лише через один вузол маршрутизації або не проходити

взагалі. У складній мережі пакети можуть

проходять через десятки вузлів маршрутизації, перш ніж досягти місця призначення. Функція трасування маршруту може бути використана для оцінки шляху передачі пакетів даних під час комунікації.

Виберіть **Traceroute** як режим діагностики, введіть IP-адресу призначення або максимальне значення TTL, що використовується URL-адресою і трасуванням, і натисніть кнопку **Почати**.

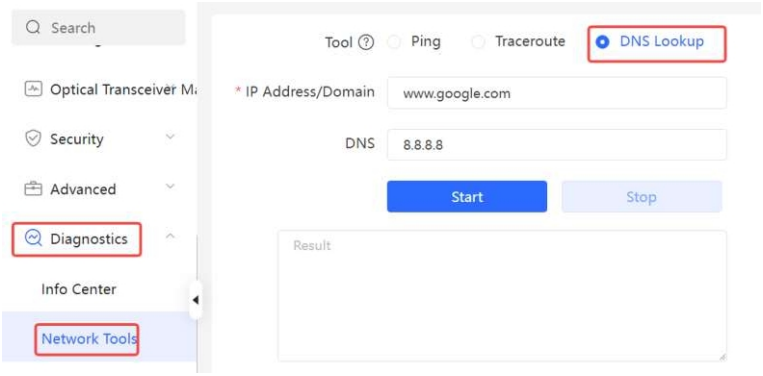


15.2.3 Пошук DNS

Виберіть **Локальний пристрій> Діагностика> Мережеві інструменти**.

Пошук DNS використовується для запиту інформації про мережеве доменне ім'я або діагностики проблем з DNS-сервером. Якщо пристрій може пінгувати IP-адресу Інтернету з вашої веб-сторінки, але браузер не може відкрити веб-сторінку, ви можете скористатися функцією пошуку DNS, щоб перевірити, чи нормальний дозвіл доменних імен.

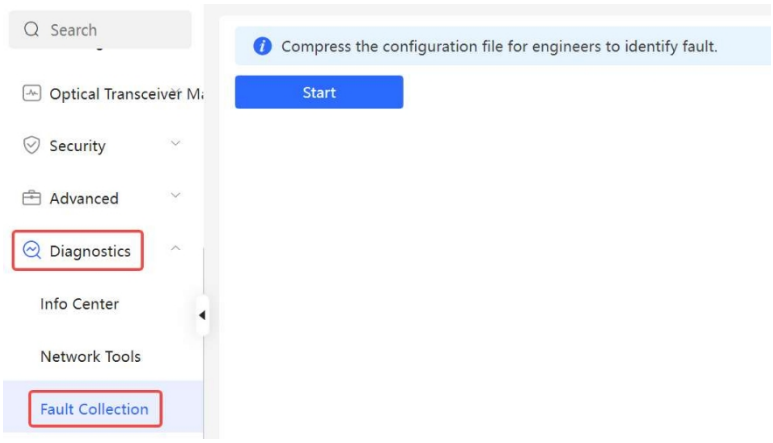
Виберіть режим діагностики **Пошук DNS**, введіть IP-адресу або URL-адресу призначення і натисніть кнопку **Почати**.



15.3 Збір несправностей

Виберіть **Локальний пристрій> Діагностика> Збір несправностей.**

Коли на пристрої виникає невідома несправність, ви можете зібрати інформацію про несправність одним натисканням на цій сторінці. Натисніть кнопку **Почати**. Файли конфігурації пристрою будуть упаковані в стислий файл. Завантажте стиснутий файл локально і надайте його співробітникам відділу досліджень і розробок для пошуку несправностей.

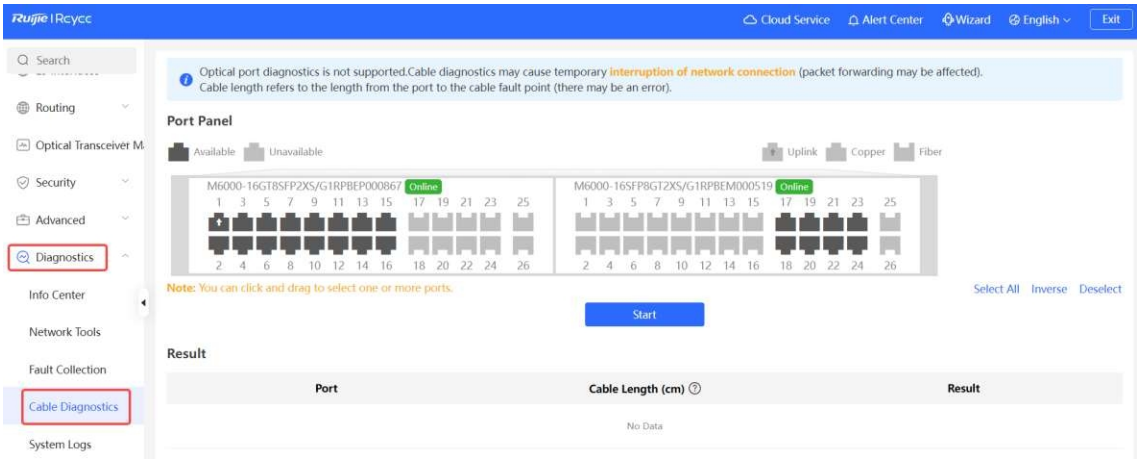


15.4 Діагностика кабелю

Виберіть **Локальний пристрій**> **Діагностика**> **Діагностика кабелю**.

Функція діагностики кабелю дозволяє визначити приблизну довжину кабелю, підключеного до порту, і визначити, чи несправний він.

Виберіть порт, який потрібно виявити, на панелі портів і натисніть **Старт**. Нижче буде показано результати виявлення.



Застереження

- Порт SPF не підтримує цю функцію.
- Якщо виявлений порт містить порт висхідної лінії зв'язку, мережа може періодично відключатися. Будьте обережні під час виконання цієї операції.

15.5 Сповіщення

Виберіть **Локальний пристрій**> **Діагностика**> **Сповіщення**.

Примітка

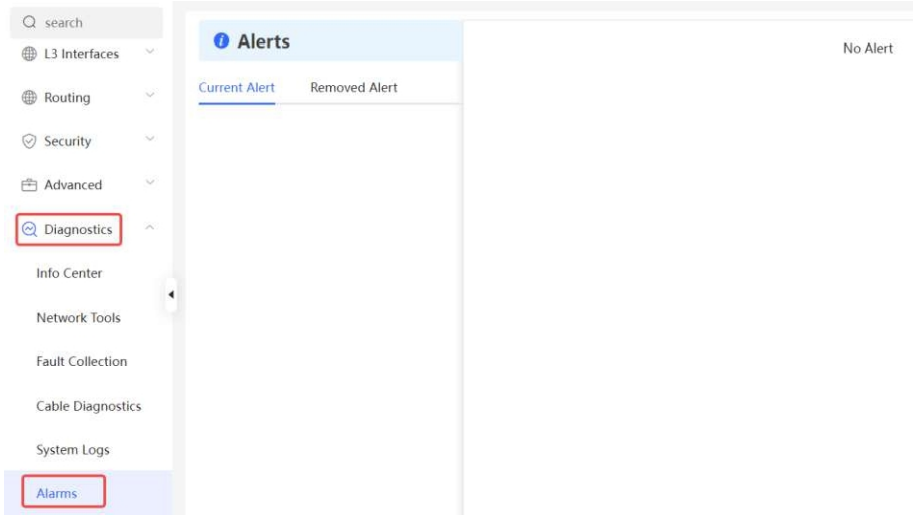
Клацніть сповіщення в **Центрі сповіщень**, щоб переглянути несправний пристрій, деталі та опис проблеми.

Відображає можливі проблеми у мережевому середовищі, щоб полегшити запобігання несправностям та їх усунення. Ви можете переглянути час появи попередження, порт, вплив попередження та рекомендації щодо усунення несправностей, а також усунути несправності пристрою відповідно до рекомендацій.

За замовчуванням це стосується всіх типів сповіщень. Ви можете натиснути **Скасувати** підписку, щоб скасувати підписку на цей тип сповіщень. Система більше не буде відображати цей тип сповіщень. Щоб знову увімкнути функцію сповіщення про тип оповіщення, перейдіть за типом оповіщення на сторінку **Видалені оповіщення**.

Застереження

Якщо не виконати попередження, система не видаватиме попередження для цього типу несправностей, і користувачі не зможуть вчасно знайти та усунути несправність. Будьте обережні, виконуючи цю операцію.



Таблиця 15-1 Типи сповіщень та підтримка продукту

Тип оповіщення	Опис	Опис підтримки
Адреси у пулі адрес DHCP буде вичерпано.	працює як DHCP-сервер, і кількість виділених адрес наближається до максимальної кількості адрес, які можна виділити в адресному пулі.	Застосовується лише до пристроїв, які підтримують функції рівня 3. Вироби, які не підтримують функції рівня 3, такі як комутатори серій RG-NBS3100, RG-NBS3200, не підтримують цей тип оповіщення.
IP-адреса локального пристрою конфліктує з IP-адресою іншого пристрою.	IP-адреса локального пристрою конфліктує з IP-адресою іншого клієнта в локальній мережі.	NA
Конфлікт IP-адрес виникає на низхідних пристроях, підключених до пристрою.	Серед пристроїв, підключених до поточного пристрою в локальній мережі, на одному або декількох пристроях виникає конфлікт IP-адрес.	NA

Тип оповіщення	Опис	Опис підтримки
Таблиця MAC-адрес переповнена записами.	Кількість записів MAC-адрес 2-го рівня наближається до межі апаратних можливостей пристрою.	NA
Таблиця ARP записами ARP.	Кількість ARP-записів у мережі перевищує ARP-можливість пристрою.	NA
Процес PoE не виконується.	Служба PoE пристрою не працює, і живлення не подається.	Застосовується тільки до комутаторів серії NBS, які підтримують функцію PoE. (Моделі пристроїв позначені символом "-P").
Загальна потужність PoE перевантажена.	Загальна потужність PoE пристрою перевантажена, і новий підключений PD не може отримати належне живлення.	Застосовується тільки до комутаторів серії NBS, які підтримують функцію PoE. (Моделі пристроїв позначені символом "-P").
Пристрій має циклічну тривогу.	У локальній мережі виникає мережева петля.	NA

16 Конфігурація системи

16.1 Системні журнали

Підтримка версій

Системні журнали можна переглядати або налаштовувати лише на пристроях під управлінням ReyeeOS 2.320 або новіших версій.

У середніх і великих мережевих проектах мережевий адміністратор зазвичай використовує стороннє програмне забезпечення для підключення до всіх пристроїв, моніторингу кожного показника даних системи і визначення наявності будь-яких аномальних явищ, таким чином забезпечуючи безпеку системи. Пристрої зазвичай використовують протоколи мережевого управління, такі як Simple Network Management Protocol (SNMP) і Syslog, для підключення до стороннього програмного забезпечення.

16.1.1 Перегляд журналів

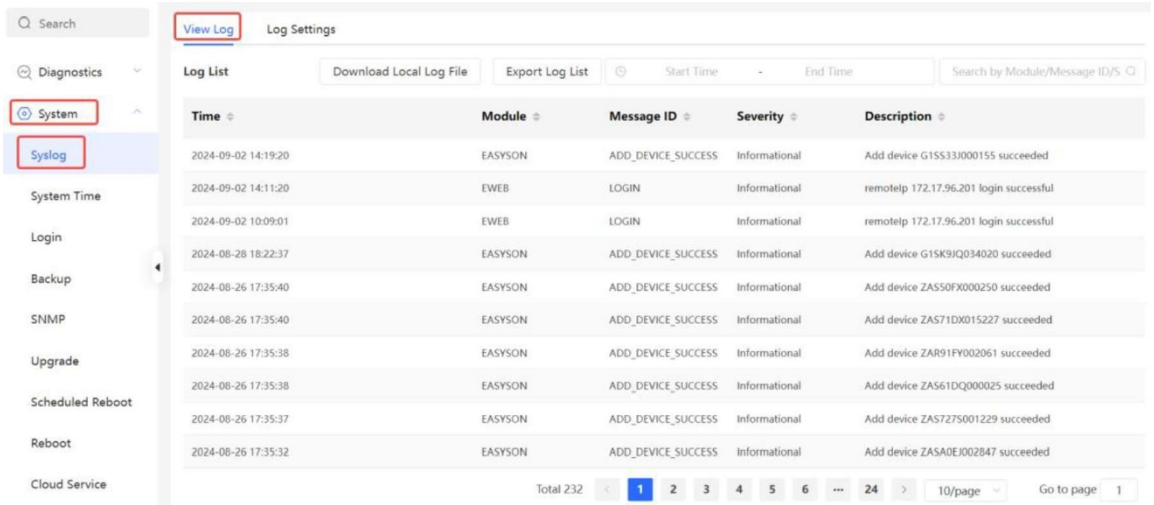
Виберіть **Network Wide**> **System**> **Syslog**> **Переглянути журнал**.

Підтримка версій

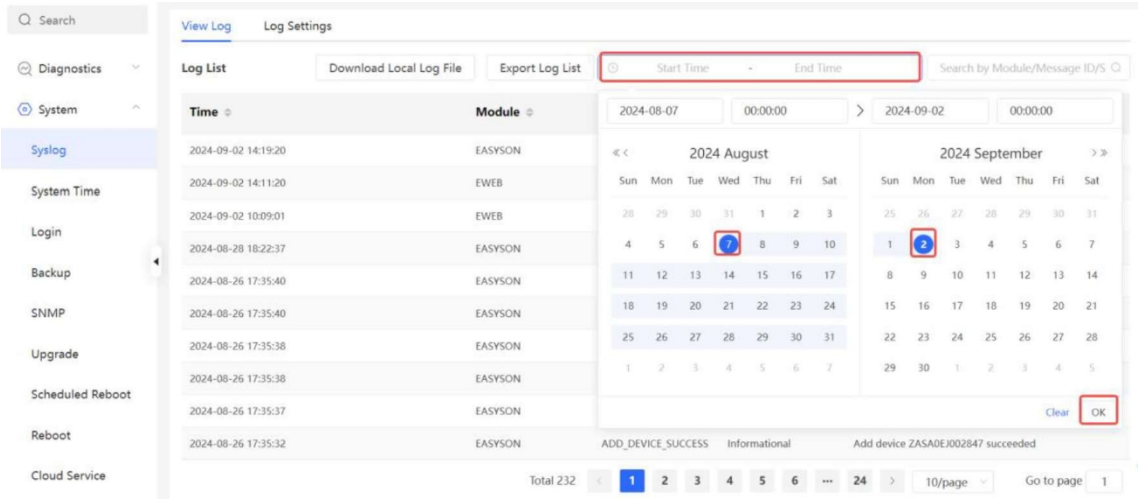
Системні журнали можна відображати або налаштовувати лише тоді, коли версія програмного висхідного шлюзу або маршрутизатора комутатора - ReyeeOS 2.320 або новіша.

Виберіть **Локальний пристрій**> **Система**> **Переглянути журнал**.

Список журналів відображає журнали роботи локального пристрою. На сторінці **Перегляд журналу** ви можете вказати тривалість або модуль для перегляду журналів, або експортувати список журналів і файл журналу на локальний пристрій для резервного копіювання або перегляду.

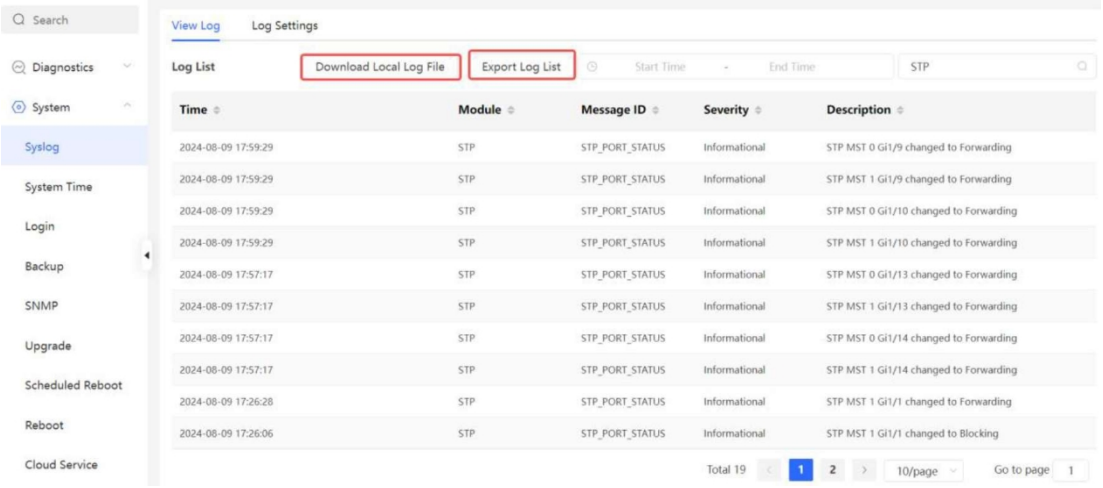


- Перегляд журналів за вказаний проміжок часу. Натисніть **Час початку**, виберіть дати початку і закінчення та натисніть **OK**, щоб відфільтрувати журнали за датою.



- Перегляд журналів певного модуля. Введіть назву модуля в поле пошуку щоб журнали операцій вказаного модуля.

- Завантажте файл журналу та експортуйте список журналів. Натисніть **Завантажити локальний файл журналу**, щоб завантажити стислий пакет файлів журналу на локальний пристрій для зберігання і резервного копіювання. Натисніть **Експортувати список журналів**, щоб завантажити список журналів у форматі .csv на локальний пристрій для перегляду.

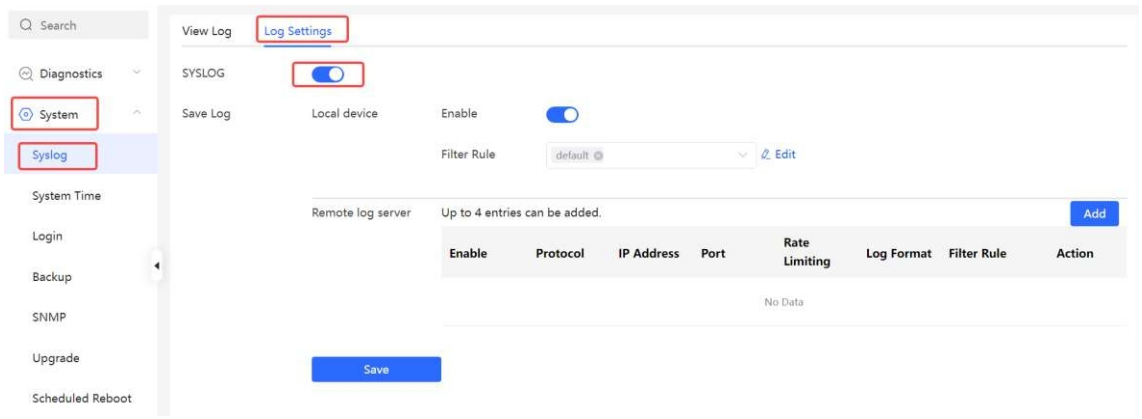


16.1.2 Налаштування журналів

Виберіть **Локальний пристрій> Система> Syslog> Налаштування журналу**.

1. Увімкнення Syslog

Після ввімкнення **SYSLOG** комутатор може з'єднуватися з віддаленим сервером журналів через Syslog і надсилати інформацію журналу на віддалений сервер журналів через мережу.

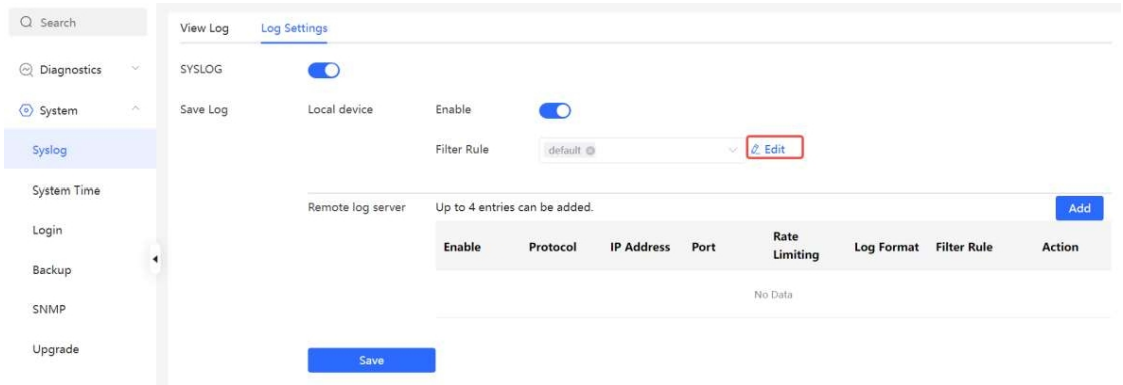


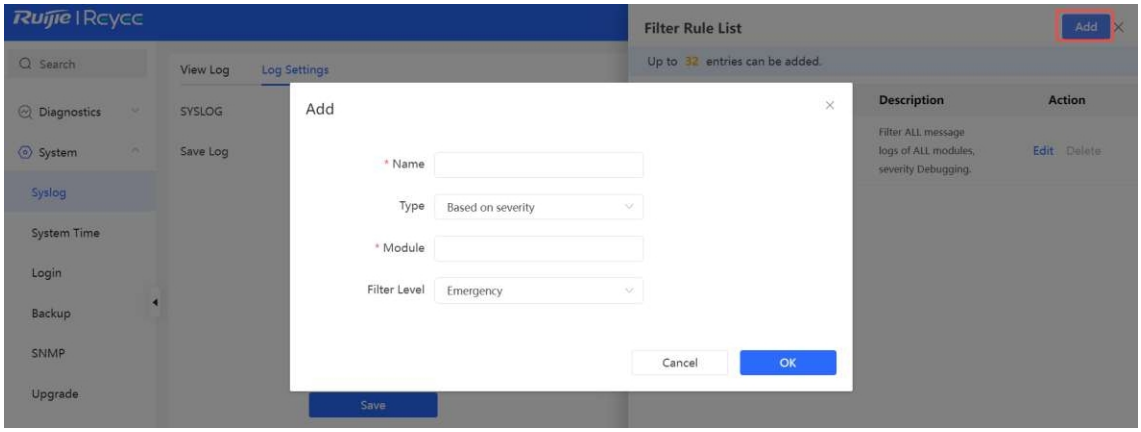
2. Налаштування локальних журналів

Зберігання журналів на локальному пристрої увімкнено за замовчуванням. Натисніть **Редагувати**, а потім **Додати**, щоб додати правило фільтрації для журналів роботи пристрою. Наприклад, ви можете відфільтрувати інформацію про налагодження всіх модулів, щоб запобігти їх відображенню у списку журналів.

Застереження

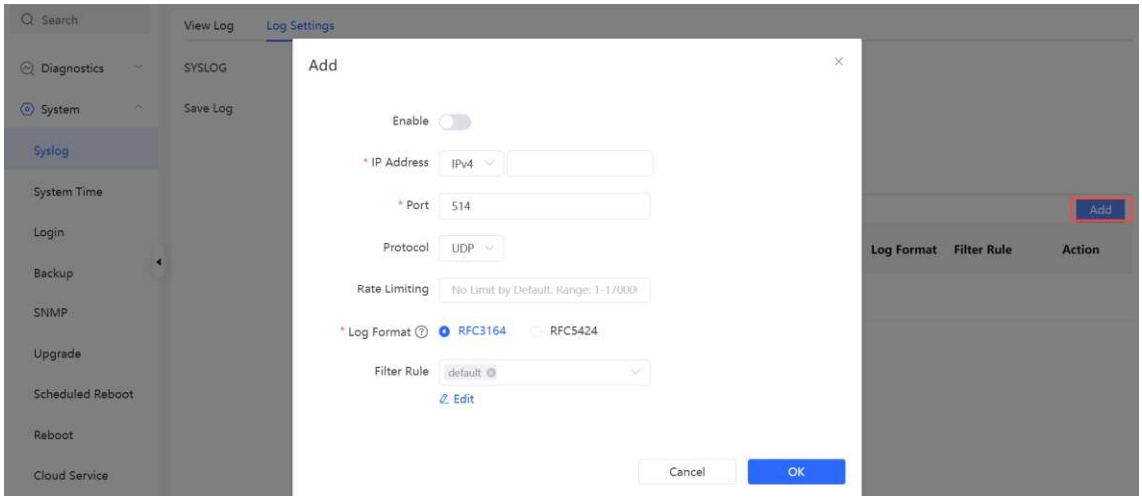
Якщо функцію ведення журналу локального пристрою , жодна операція, виконана на пристрої, не відображатиметься у списку журналу. Будьте обережні, вимикаючи збереження журналу на локальному пристрої.





3. Налаштування віддаленого сервера журналів

Натисніть **Додати** поруч з віддаленим , щоб додати основну інформацію про нього.



Таблиця 16-1 Опис налаштування параметрів віддаленого сервера

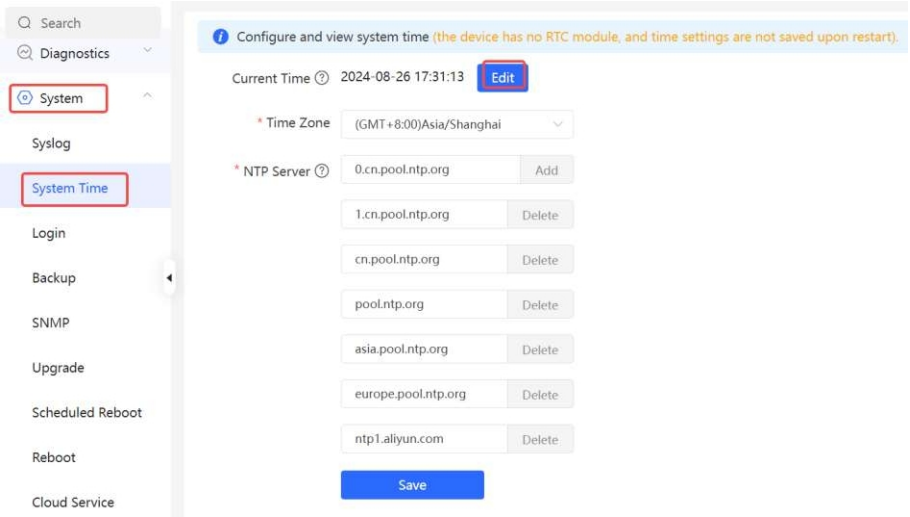
Параметр	Опис	Значення за замовчуванням
Увімкнути	Чи вмикати віддалений сервер. Якщо так, пристрій журнали роботи локального пристрою на віддалений сервер.	Увімкнено за замовчуванням.
IP-адреса	IP-адреса віддаленого сервера. Можна ввести IPv4 або IPv6 адресу.	NA
Порт	Номер порту віддаленого сервера.	NA
Протокол	Протоколи, що використовуються пристроєм для зв'язку з віддаленим сервером. Наразі підтримується лише UDP.	UDP за замовчуванням.

Параметр	Опис	Значення за замовчуванням
Обмеження ставок	Максимальна швидкість передачі даних, яку використовує пристрій для надсилання інформації журналу на віддалений сервер.	За замовчуванням немає ліміту за ставкою.
Формат журналу	Формат журналів пристрою, що надсилаються на віддалений сервер журналів. ● RFC3164: <Пріоритет> Локальний час у секундах Назва хоста Назва модуля% ідентифікатор повідомлення: Вміст журналу ● RFC5424: <Пріоритет> UTC час у мікросекундах Назва хоста Назва модуля Ідентифікатор процесу Прапор повідомлення - Вміст журналу	RFC3164
Правило фільтрації	Правила фільтрації журналів роботи пристрою. Відфільтровані журнали операцій не надсилатимуться на сервер журналів.	NA

16.2 Налаштування системного часу

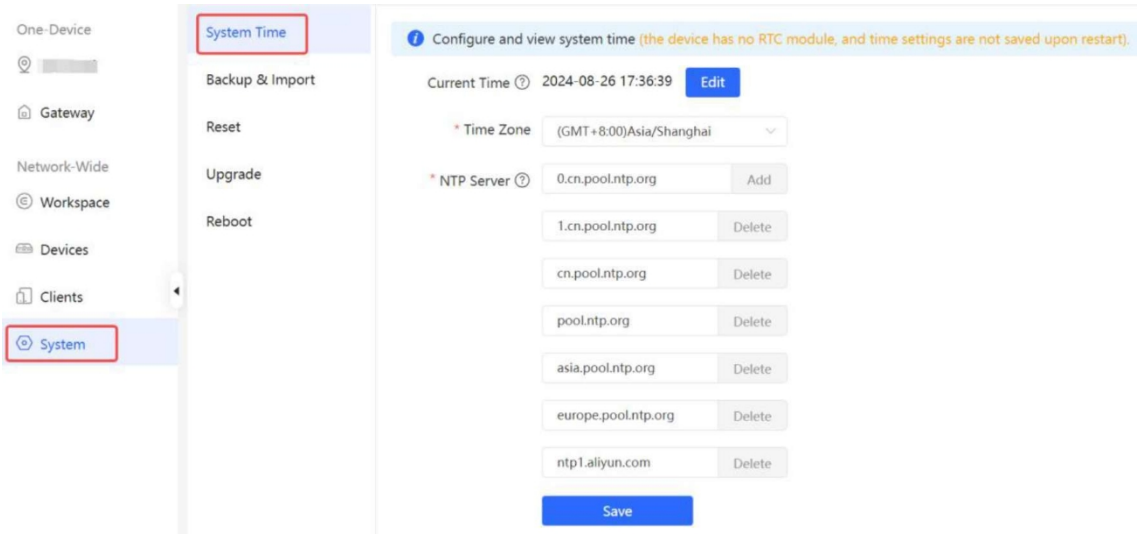
Виберіть **Локальний пристрій**> **Система**> **Системний час**.

Ви можете переглянути поточний системний час. Якщо час неправильний, перевірте і виберіть місцевий часовий пояс. Якщо часовий пояс вибрано правильно, але час все одно невірний, натисніть **Редагувати**, щоб встановити час вручну. Крім того, пристрій підтримує сервери протоколу мережевого часу (NTP). За замовчуванням декілька серверів слугують резервним копіюванням один одного. Ви можете додати або видалити локальний сервер за потреби.



Натисніть **Поточний час** при зміні часу, і системний час пристрою, на якому ви зараз перебуваєте, буде автоматично заповнено.

Виберіть **мережевий> Системний> Системний час**



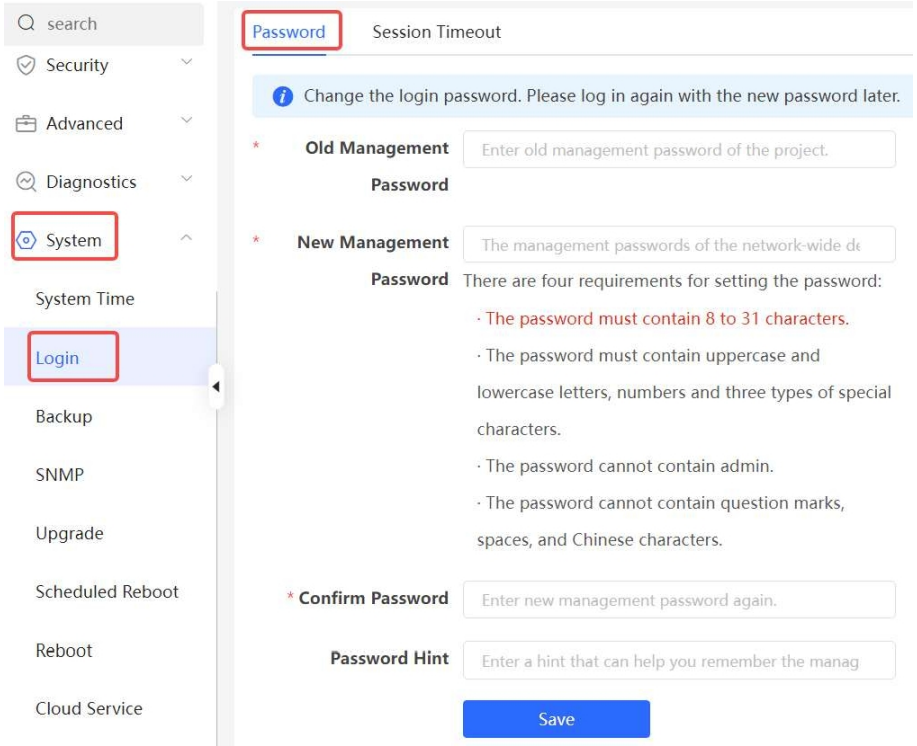
16.3 Налаштування пароля для входу в систему

Виберіть **Локальний пристрій> Система> Логін> Пароль**.

Введіть старий і новий пароль. Після збереження конфігурації використовуйте новий пароль для входу.

Застереження

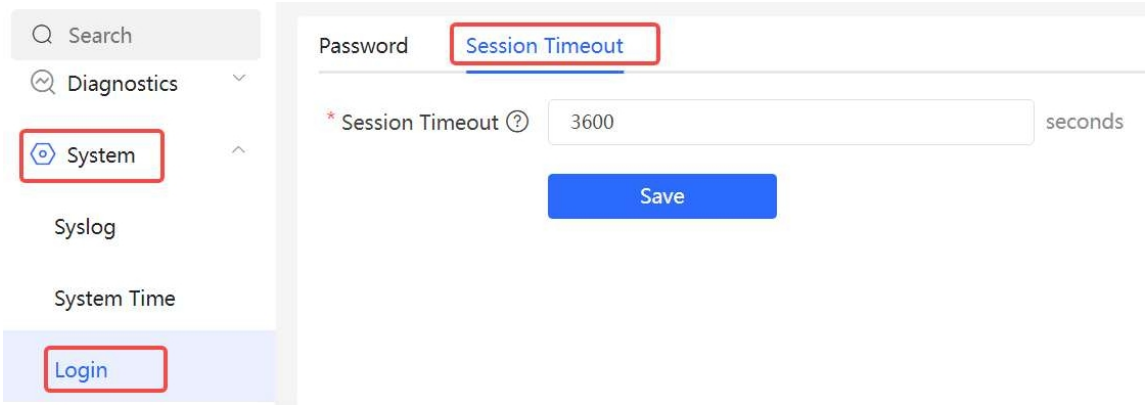
Якщо увімкнено самоорганізаційне виявлення мережі, пароль для входу на всіх пристроях у мережі буде змінено синхронно.



16.4 Налаштування тривалості тайм-ауту сеансу

Виберіть **Локальний пристрій**> **Система**> **Вхід**> **Тайм-аут сеансу**.

Якщо ви не вийшли з системи після входу, веб-інтерфейс за замовчуванням дозволяє продовжити доступ без автентифікації в поточному браузері протягом однієї години. Через одну годину веб-інтерфейс автоматично оновлює сторінку, і вам потрібно знову увійти в систему, щоб продовжити . Ви можете змінити тривалість тайм-ауту сеансу.



16.5 Налаштування SNMP

16.5.1 Огляд

Простий протокол управління мережею (SNMP) - це протокол для управління мережевими пристроями. Заснований на моделі клієнт/сервер, він дозволяє здійснювати віддалений моніторинг і керування мережевими пристроями.

SNMP використовує архітектуру менеджера та агентів. Менеджер взаємодіє з агентами через протокол SNMP для отримання такої інформації, як стан пристрою, деталі конфігурації та дані про продуктивність. Його також можна використовувати для налаштування та керування пристроями.

SNMP можна використовувати для управління різними мережевими пристроями, включаючи маршрутизатори, комутатори, сервери, брандмауери тощо. Ви можете керувати користувачами за допомогою інтерфейсу конфігурації SNMP, а також здійснювати моніторинг і керування пристроями за допомогою стороннього програмного забезпечення.

16.5.2 Глобальна конфігурація

1. Огляд

Метою глобальної конфігурації є увімкнення служби SNMP і введення в дію версії протоколу SNMP (v1/v2c/v3), щоб виконати базову конфігурацію локального порту, місцезнаходження пристрою та контактної інформації.

SNMP v1: Як найперша версія SNMP, SNMP v1 має низький рівень безпеки і підтримує лише просту автентифікацію за рядком спільноти. SNMP v1 має певні недоліки, такі як передача рядків спільноти відкритим текстом і вразливість до атак. Тому SNMP v1 не рекомендується для сучасних мереж.

SNMP v2c: Як покращена версія SNMP v1, SNMP v2c підтримує більш багаті функції та складніші типи даних, з підвищеним рівнем безпеки. SNMP v2c працює краще, ніж SNMP v1 з точки зору безпеки і функціональності, і є більш гнучким. Його можна налаштувати відповідно до різних потреб.

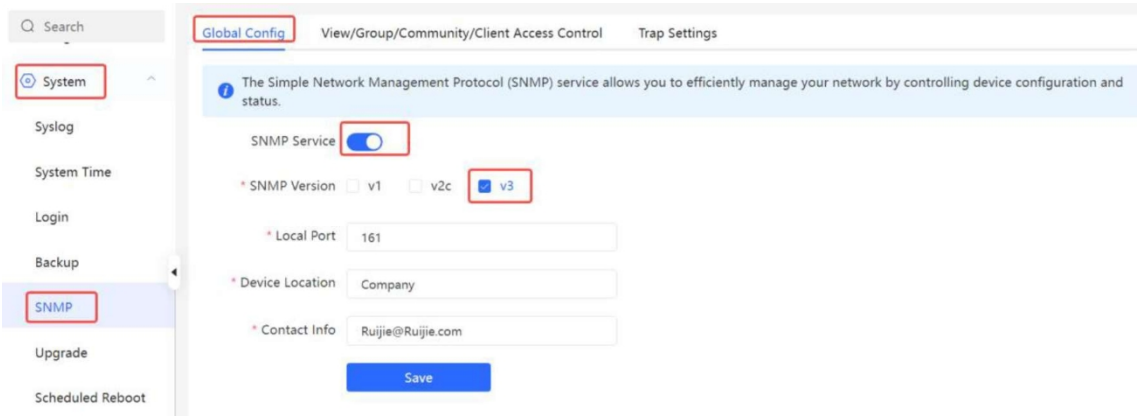
SNMP v3: Як найновіша версія, SNMP v3 підтримує такі механізми безпеки, як автентифікація та шифрування повідомлень, порівняно з SNMP v1 та SNMP v2c. У SNMP v3 було досягнуто значних поліпшень в області

безпеки і контролю доступу.

2. Кроки конфігурації

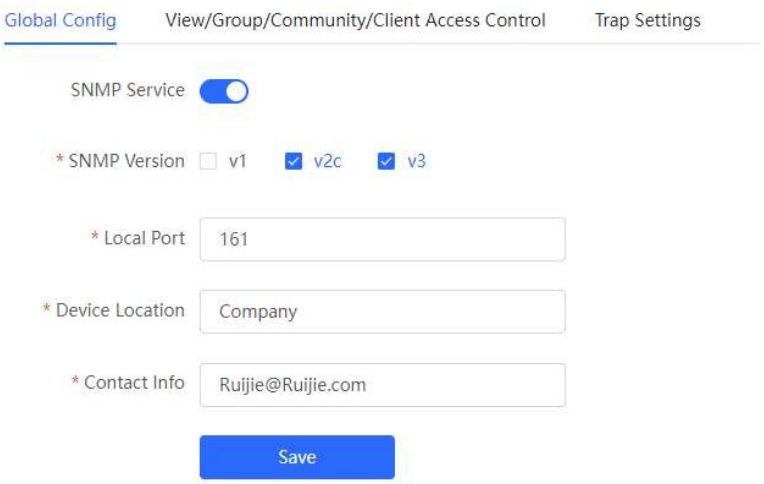
Виберіть **Локальний пристрій> Система> SNMP> Глобальна конфігурація**

(1) Увімкніть службу SNMP.



Під час першого ввімкнення SNMP v3 увімкнено за замовчуванням. Натисніть **кнопку OK**.

(2) Налаштування глобальних параметрів конфігурації служби SNMP.



Таблиця 16-2 Глобальні параметри конфігурації

Параметр	Опис
Сервер SNMP	Показує, чи ввімкнено службу SNMP.
Версія SNMP	Вказує на версію протоколу SNMP, включаючи версії v1, v2c і v3.
Місцевий порт	Діапазон портів від 1 до 65535.
Розташування пристрою	1-64 символи. Китайські ієрогліфи, повні , знаки питання та пробіли не допускаються.
Контактна інформація	1-64 символи. Китайські ієрогліфи, повні , знаки питання та пробіли не допускаються.

(3) Натисніть "**Зберегти**".

Після ввімкнення служби SNMP натисніть кнопку **Зберегти**, щоб базові налаштування, такі як номер версії протоколу SNMP, набули чинності.

16.5.3 Перегляд/Група/Спільнота/Керування доступом клієнтів

1. Перегляд/Група/Спільнота/Керування доступом клієнтів

Інформаційну базу управління (MIB) можна розглядати як базу даних, що зберігає інформацію про стан і дані про продуктивність мережевих пристроїв. Вона містить велику кількість ідентифікаторів об'єктів (OID) для ідентифікації інформації про стан і дані про продуктивність цих мережевих пристроїв.

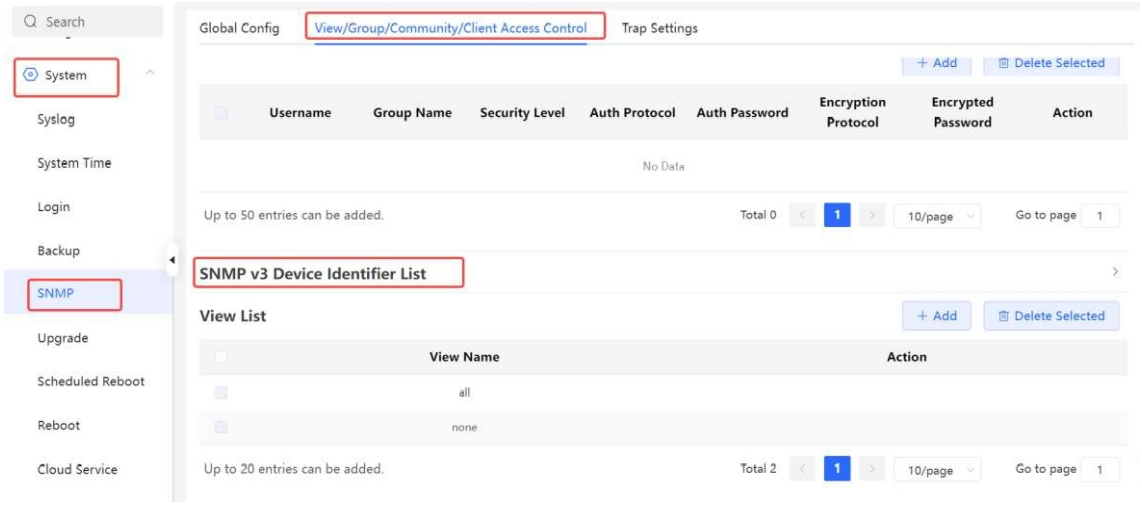
Подання в SNMP можуть обмежувати діапазон вузлів MIB, до яких може отримати доступ система управління, тим самим підвищуючи безпеку і надійність управління мережею. Подання є невід'ємною частиною SNMP і повинні бути налаштовані відповідно до конкретних вимог управління.

Подання може мати декілька піддерев. Система керування може отримати доступ лише до вузлів MIB у цих піддеревах і не може отримати доступ до інших несанкціонованих вузлів MIB. Це може запобігти доступу неавторизованих системних адміністраторів до важливих вузлів MIB, тим самим захищаючи безпеку мережевих пристроїв. Крім того, подання також можуть підвищити ефективність управління мережею і прискорити реакцію системи управління.

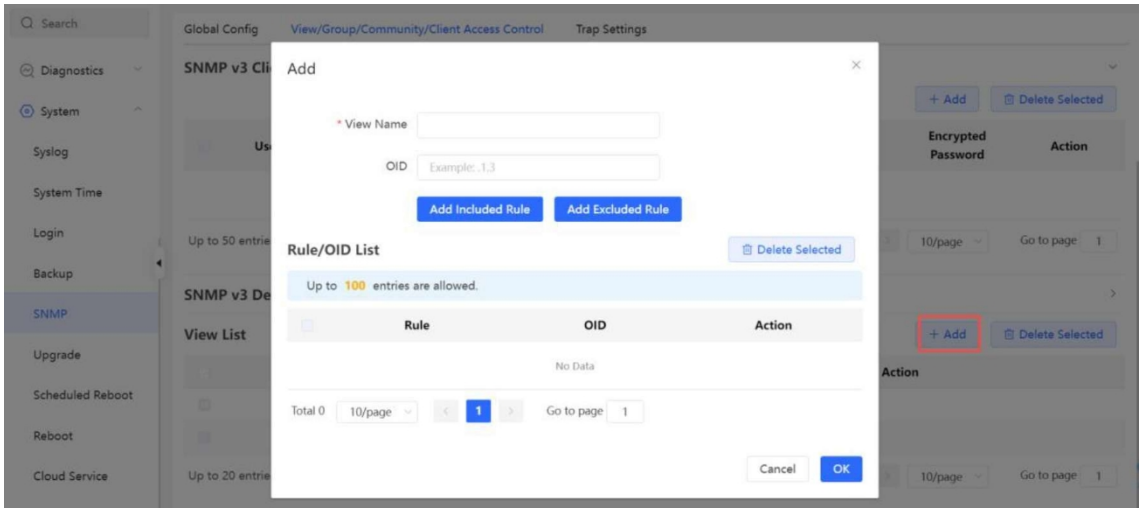
- Кроки конфігурації

Виберіть **Локальний пристрій> Система> SNMP> View/Group/Community/Client Access Control.**

(1) Натисніть **Додати** під **списком видів**, щоб додати вид.



(2) Налаштуйте основну інформацію .



Таблиця 16-3 Перегляд параметрів конфігурації

Параметр	Опис
Назва виду	Вказує на назву виду. 1-32 символи. Китайські символи або символи на всю ширину не .
OID	Вказує діапазон OID, включених до подання, який може бути одним OID або піддеревом OID.
Тип	Існує два типи правил: включені та виключені правила. ● Включене правило дозволяє доступ лише до OID в межах діапазону OID. Натисніть **Додати включене правило**, щоб встановити цей тип подання. ● Виключені правила дозволяють доступ до всіх OID, окрім тих, що знаходяться в діапазоні OID. Натисніть **Додати виключене правило**, щоб налаштувати цей тип подання.

Примітка

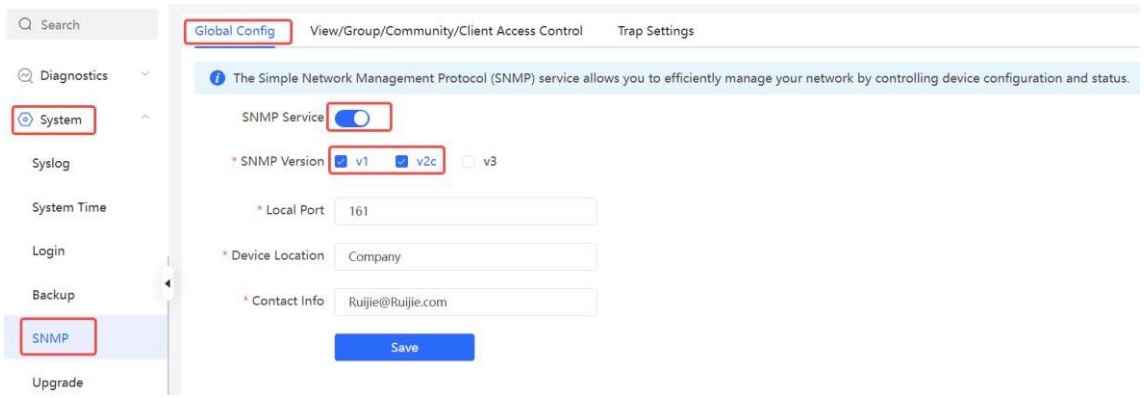
Принаймні одне правило OID має бути налаштоване для подання. Інакше з'явиться тривожне повідомлення.

(3) Натисни **OK**.

2. Налаштування користувачів v1/v2c

- Огляд

  Якщо версію SNMP встановлено на v1/v2c, потрібна конфігурація користувача.



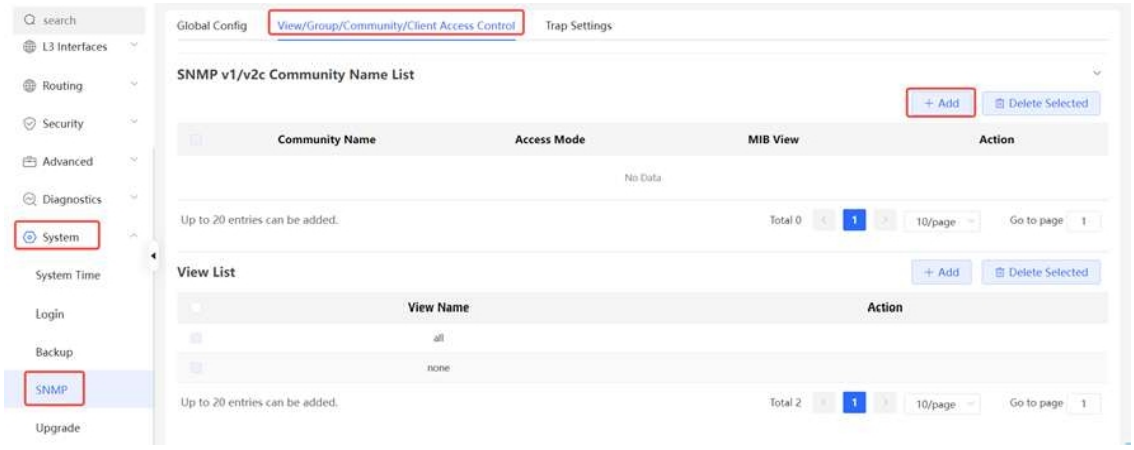
Примітка

Виберіть версію протоколу SNMP і натисніть **Зберегти**. Відповідні параметри конфігурації з'являться на сторінці Сторінка **Перегляд/Група/Спільнота/Керування доступом користувачів.**

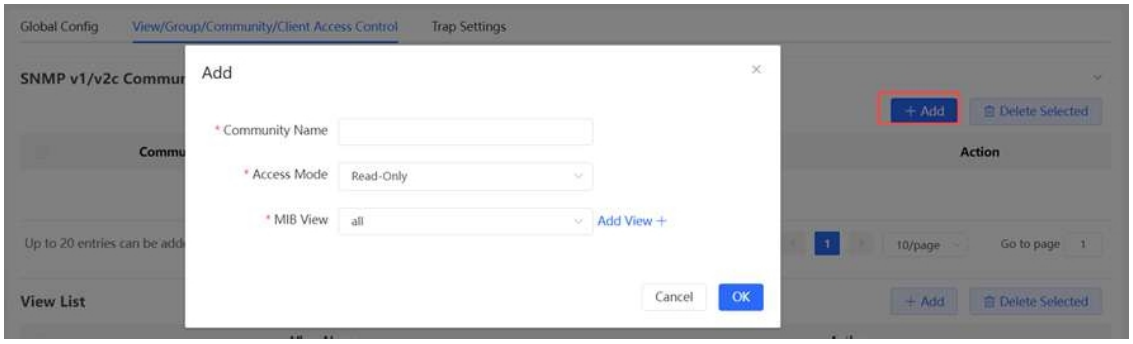
- Кроки конфігурації

Виберіть **Локальний пристрій**> **Система**> **SNMP**> **View/Group/Community/Client Access Control.**

(1) Натисніть **Додати** на панелі Список імен спільнот SNMP v1/v2c.



(2) Додайте користувача v1/v2c.



Таблиця 16-4 v1/v2c Параметри конфігурації користувача

Параметр	Опис
Назва спільноти	Мінімум 8 символів. Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Імена адміністратора, публічні або приватні імена спільноти не допускаються. Знаки питання, пробіли та китайські ієрогліфи не допускаються.
Режим доступу	Вказує дозвіл доступу (тільки для читання або читання і запис) для назви спільноти.
MIB View	Опції під випадаючим списком - це налаштовані подання (за замовчуванням: всі, жодного).

Примітка

- Назви спільнот не можуть бути однаковими серед користувачів v1/v2c.
- Натисніть **Додати подання**, щоб додати подання.

3. Налаштування груп v3

- Огляд

  SNMP v3 вводить концепцію групування для досягнення кращого рівня безпеки і контролю доступу. Група - це група користувачів SNMP з однаковими політиками безпеки і налаштуваннями контролю доступу. За допомогою SNMP v3 можна налаштувати кілька груп, кожна з яких має власні політики безпеки і налаштування контролю доступу. Кожна група може мати одного або більше користувачів.

- Передумови

  Якщо версію SNMP встановлено на v3, потрібна конфігурація групи v3.

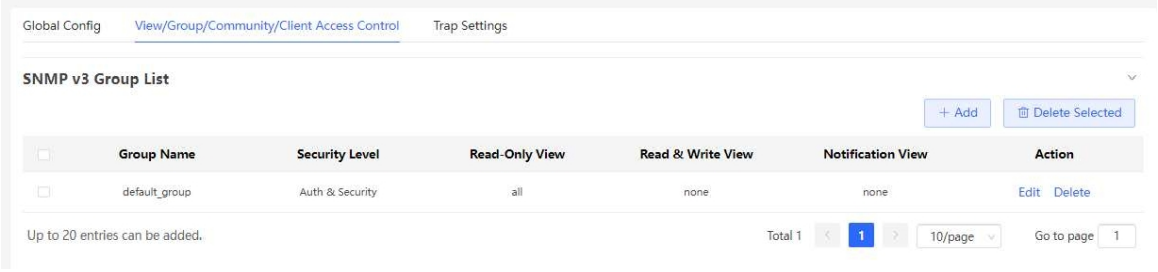
Примітка

Виберіть версію протоколу SNMP і натисніть **Зберегти**. Відповідні параметри конфігурації з'являться на сторінці Сторінка **Перегляд/Група/Спільнота/Керування доступом користувачів.**

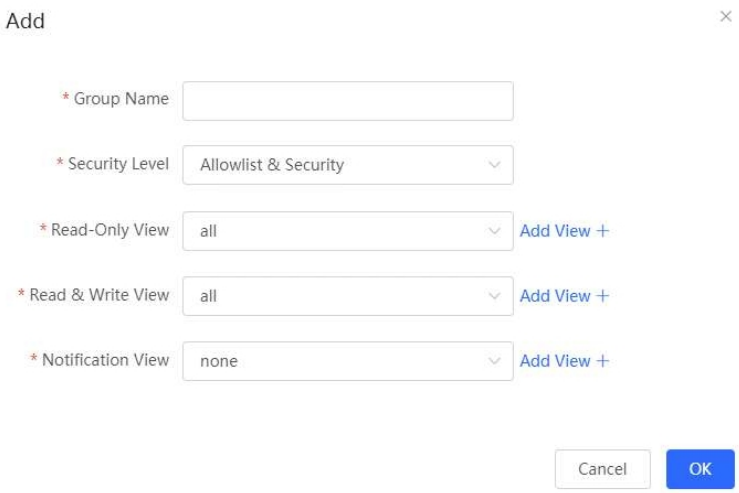
- Кроки конфігурації

Виберіть **Локальний пристрій> Система> SNMP> View/Group/Community/Client Access Control.**

(1) Натисніть **Додати** на панелі Список груп SNMP v3, щоб створити групу.



(2) Налаштуйте параметри групи v3.



Таблиця 16-5 v3 Параметри конфігурації групи

Параметр	Опис
Назва групи	Вказує на назву групи. 1-32 символи. Китайські ієрогліфи, символи на всю ширину, знаки питання та пробіли не допускаються.
Рівень безпеки	Показує мінімальний рівень безпеки (автентифікація та шифрування, автентифікація, але без шифрування, без автентифікації та шифрування) групи.
Перегляд в режимі "Тільки для читання	Опції під випадаючим списком - це налаштовані подання (за замовчуванням: всі, жодного).
Перегляд читання та запису	Опції під випадаючим списком - це налаштовані подання (за замовчуванням: всі, жодного).
Сповістити про перегляд	Опції під випадаючим списком - це налаштовані подання (за замовчуванням: всі, жодного).

Примітка

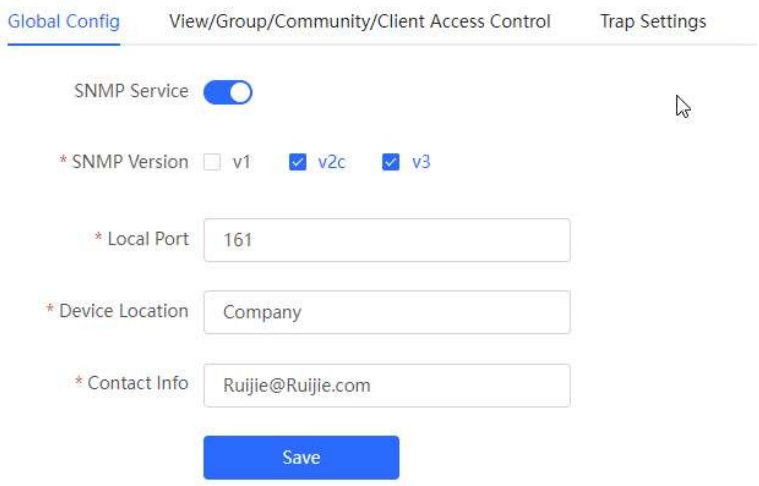
- Група визначає мінімальний рівень безпеки, дозволи на читання і запис, а також сферу дії для користувачів у групі.
- Назва групи має бути унікальною. Щоб додати подання, натисніть **Додати подання**.

(3) Натисни **ОК**.

4. Налаштування користувачів v3

- Передумови

  Якщо версію SNMP встановлено на v3, потрібна конфігурація групи v3.



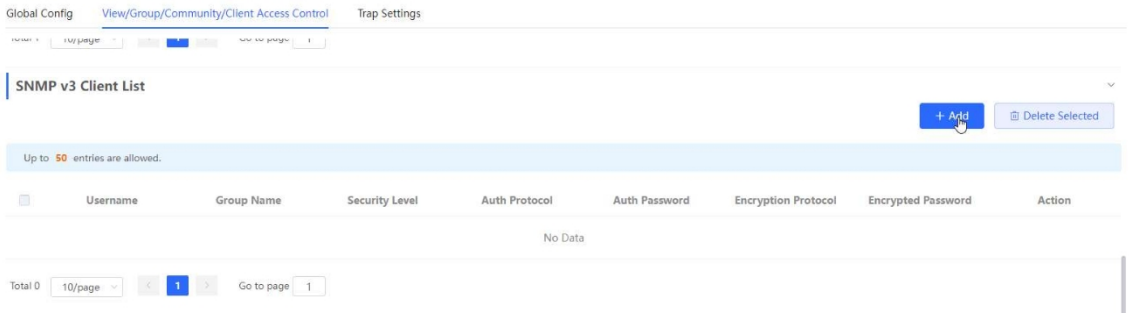
Примітка

Виберіть версію протоколу SNMP і натисніть **Зберегти**. Відповідні параметри конфігурації з'являться на сторінці Сторінка **Перегляд/Група/Спільнота/Керування доступом користувачів.**

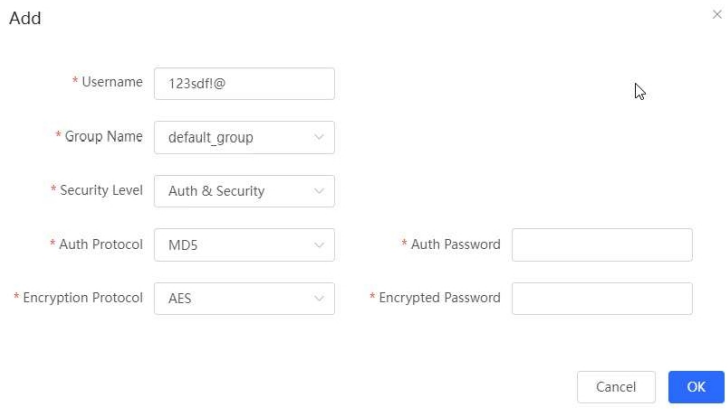
- Кроки конфігурації

Виберіть **локальний пристрій> Система> SNMP> View/Group/Community/Client Access Control**

(1) Натисніть **Додати** на панелі **Список клієнтів SNMP v3** щоб додати користувача v3.



(2) Налаштуйте параметри користувача v3.



Таблиця 16-6 v3 Параметри конфігурації користувача

Параметр	Опис
Ім'я користувача	Ім'я користувача Мінімум 8 символів. Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Імена адміністратора, публічні або приватні імена спільноти не допускаються. Знаки питання, пробіли та китайські ієрогліфи не допускаються.
Назва групи	Вказує на групу, до якої належить користувач.
Рівень безпеки	Показує рівень безпеки (автентифікація та шифрування, автентифікація, але без шифрування, без автентифікації та шифрування) користувача.
Протокол авторизації, пароль авторизації	Підтримуються протоколи автентифікації: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Пароль автентифікації: 8-31 символів. Китайські ієрогліфи, повноформатні символи, знаки питання та пробіли не . Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Примітка: Цей параметр є обов'язковим, якщо рівень безпеки - автентифікація та шифрування, або автентифікація, але без шифрування.
Протокол шифрування, пароль шифрування	Підтримуються протоколи шифрування: DES/AES/AES192/AES256. Пароль шифрування: 8-31 символів. Китайські ієрогліфи, повні символи, знаки питання та пробіли не допускаються. Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Примітка: Цей параметр обов'язковим, якщо рівень безпеки - автентифікація та шифрування.

Примітка

- Рівень безпеки користувачів v3 повинен бути вищим або дорівнювати рівню безпеки групи.
- Існує три рівні безпеки, серед яких автентифікація та шифрування вимагають протоколу автентифікації, паролю автентифікації, протоколу шифрування та паролю шифрування. Автентифікація, але без шифрування вимагає лише налаштування протоколу автентифікації та протоколу шифрування, тоді як відсутність автентифікації та шифрування не вимагає жодних налаштувань.

16.5.4 Приклади типових конфігурацій служби SNMP

1. Налаштування SNMP v2c

- Сценарій застосування

Вам потрібно лише відстежувати інформацію про пристрій, але не потрібно встановлювати та доставляти її. Для моніторингу даних вузлів типу 1.3.6.1.2.1.1 можна використовувати стороннє програмне забезпечення, якщо налаштована версія v2c.

- Специфікація конфігурації

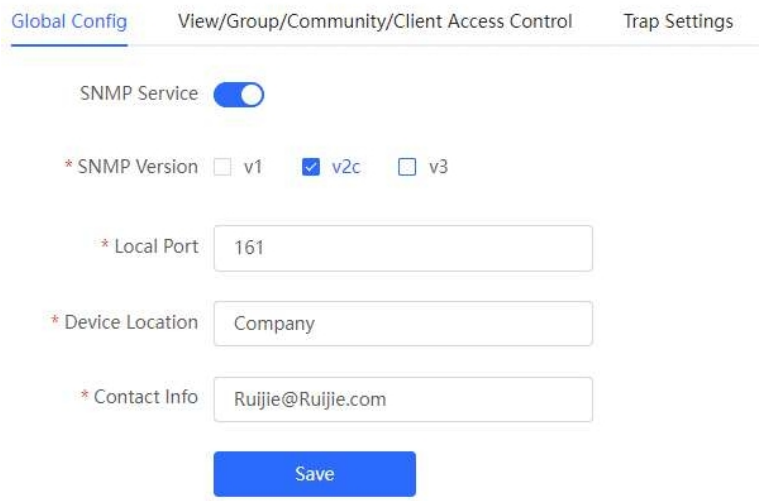
  According to the user's application scenario, вимоги наведені в наступній таблиці:

Таблиця 16-7 Специфікація вимог до користувача

Пункт	Опис
Діапазон огляду	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Версія	For SNMP v2c, the custom community name is "public". Порт за замовчуванням номер 161.
Дозвіл на читання та запис	Дозвіл тільки для читання.

- Кроки конфігурації

(1) Виберіть **Локальний пристрій**> **Система**> **SNMP**> **Глобальна конфігурація**, виберіть v2c та встановіть інші налаштування за замовчуванням. Потім натисніть **Зберегти**.

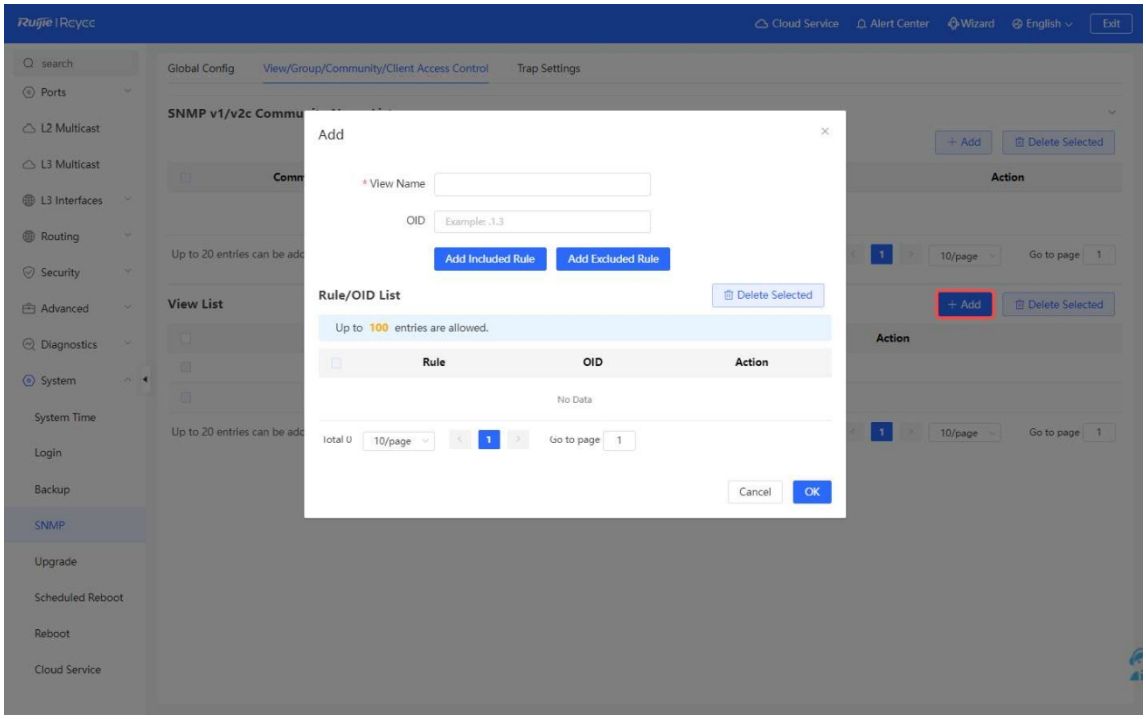


(2) Виберіть **Локальний пристрій**> **Система**> **SNMP**> **View/Group/Community/Client Access Control** ,Додайте подання в інтерфейсі View/Group/Community/Client Access Control.

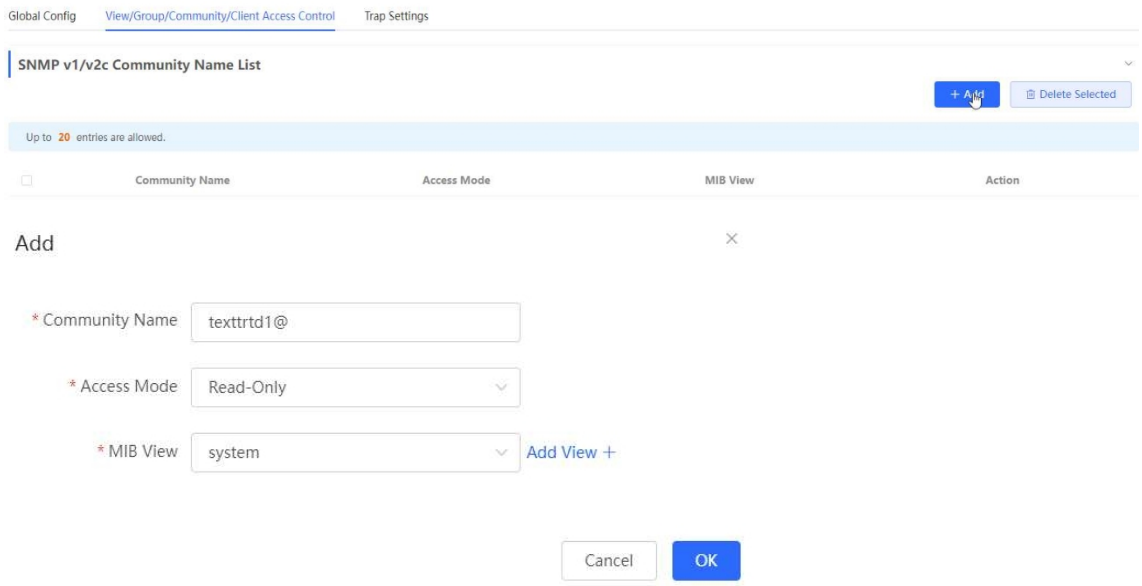
a Натисніть **Додати** на панелі **Список видів**.

b У спливаючому вікні введіть назву подання та OID і натисніть **Додати включене правило**.

c Натисни **ОК**.



(3) Натисніть **Додати** у списку назв спільнот SNMP v1/v2c, введіть назву спільноти, режим доступу і вид у спливаючому вікні і натисніть **OK** після завершення операції.



2. Конфігурація служби SNMP версії v3

- Сценарій застосування

  Вам потрібно відстежувати та контролювати пристрої, а також використовувати стороннє програмне забезпечення для моніторингу та передачі інформації про пристрої на загальнодоступні вузли (1.3.6.1.2.1). Рівень безпеки v3 - це автентифікація та шифрування.

- Специфікація конфігурації

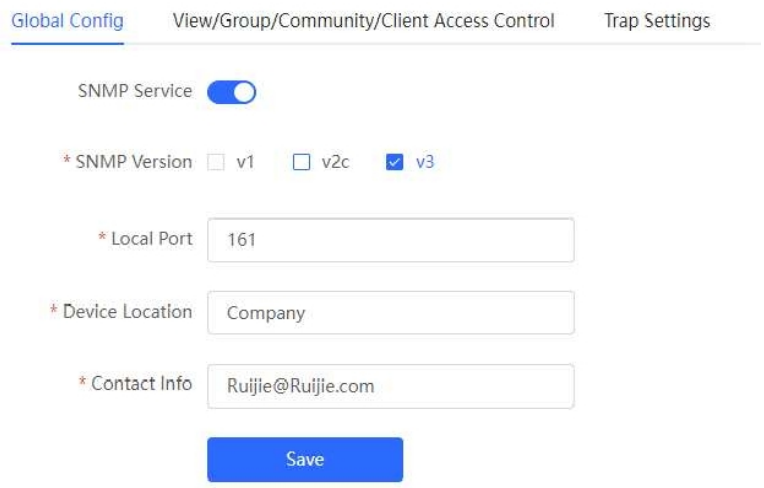
According to the user's application scenario, the reВимоги до кандидатів наведені в наступній таблиці:

Таблиця 16-8 Форма опису вимог користувача

Пункт	Опис
Діапазон огляду	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is “public_view”.
Конфігурація групи	Назва групи: group Рівень безпеки: автентифікація та шифрування Виберіть public_view для перегляду тільки для читання. Виберіть public_view для перегляду на читання та запис. Виберіть "ні", щоб не отримувати сповіщення.
Налаштування користувачів v3	Ім'я користувача: v3_user Назва групи: group Рівень безпеки: автентифікація та шифрування Протокол/пароль автентифікації: MD5/Ruijie123 Протокол/пароль шифрування: AES/Ruijie123
Версія	Для SNMP v3 номер порту за замовчуванням - 161.

- Кроки конфігурації

(1) Виберіть **Локальний пристрій**> **Система**> **SNMP**> **Глобальна конфігурація**, виберіть v3 і змініть номер порту на 161. Інші налаштування залиште за замовчуванням. Потім натисніть **Зберегти**.

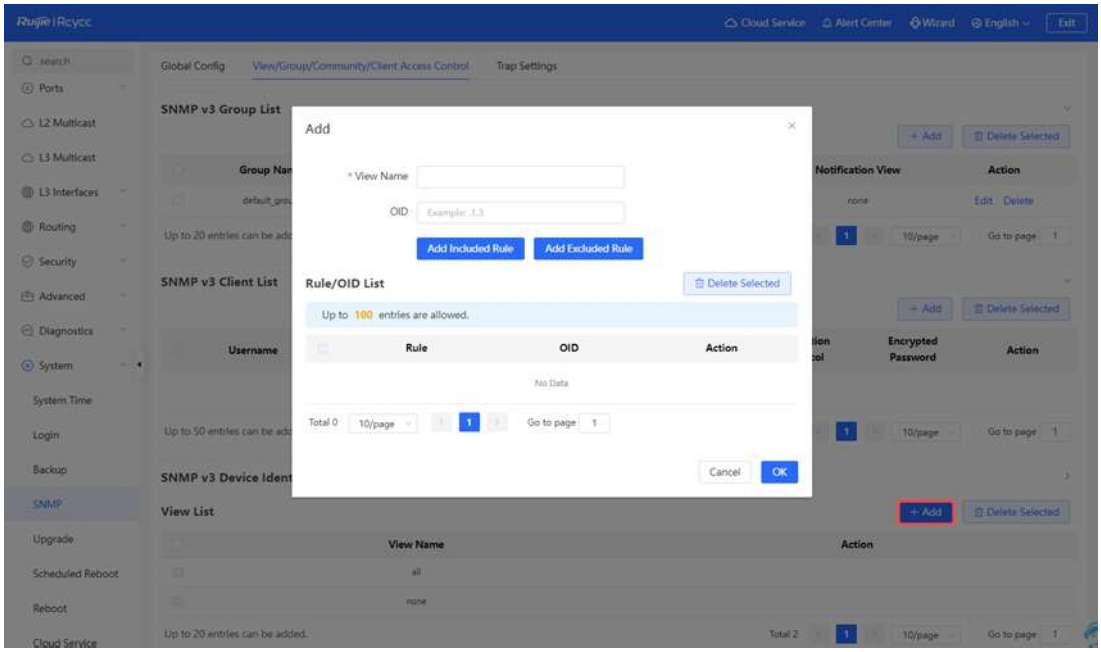


(2) Виберіть **Локальний пристрій**> **Система**> **SNMP**> **Перегляд/Група/Спільнота/Керування доступом клієнтів**. Додайте подання на інтерфейсі Перегляд/Група/Спільнота/Керування доступом клієнтів.

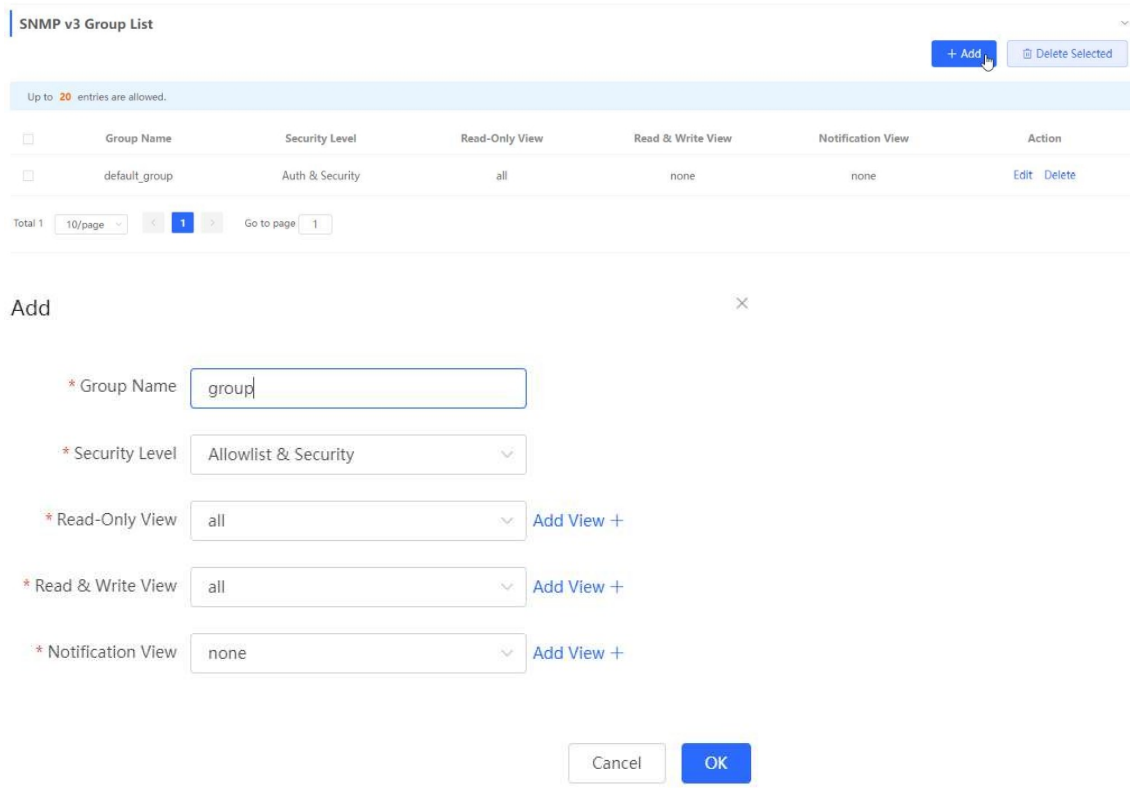
a Натисніть кнопку **Додати** на панелі **Список видів**.

b У спливаючому вікні введіть назву подання та OID і натисніть **Додати включене правило**.

c Натисни **ОК**.

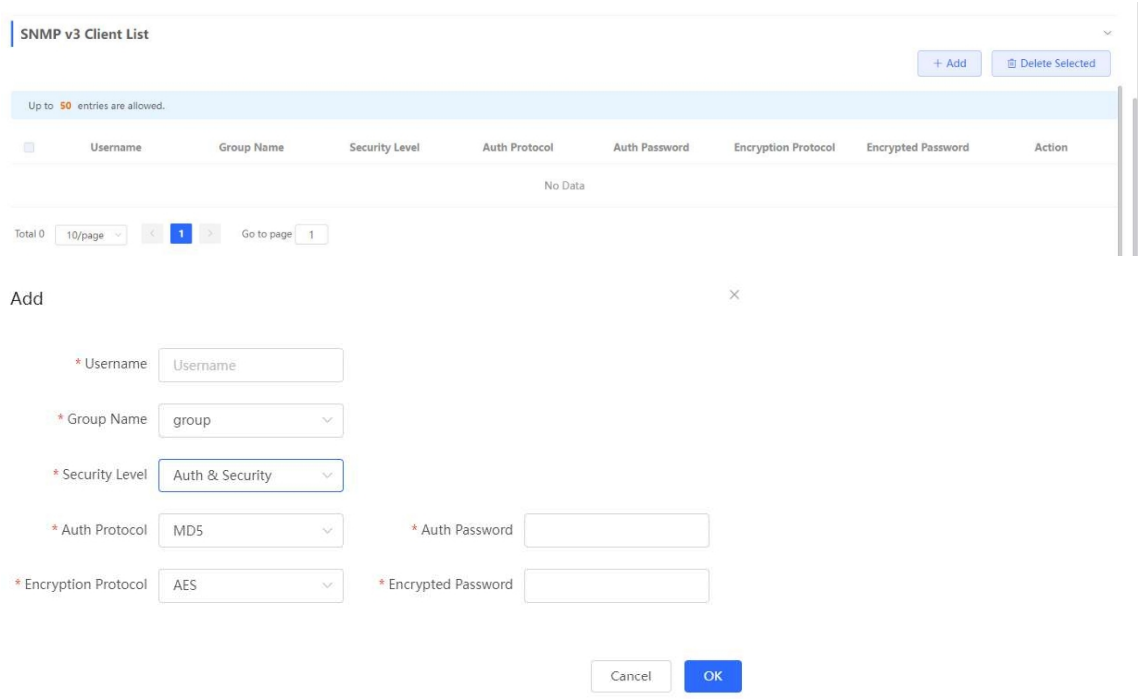


(3) Натисніть Додати у списку груп SNMP v3, у спливаючому вікні введіть назву групи і рівень безпеки, , чи має користувач права на читання і запис, виберіть "public _view" для перегляду для читання і перегляду для читання і запису, а для перегляду сповіщень встановіть нульове значення. Після завершення операції натисніть кнопку **OK**.



(4) Натисніть Додати у списку користувачів SNMP v3, введіть ім'я користувача та назву групи у спливаючому вікні, рівень безпеки користувача приймає режим автентифікації та шифрування, введіть відповідний протокол автентифікації, пароль автентифікації, протокол шифрування та пароль шифрування і натисніть

кнопку **ОК**.



16.5.5 Налаштування служби пасток

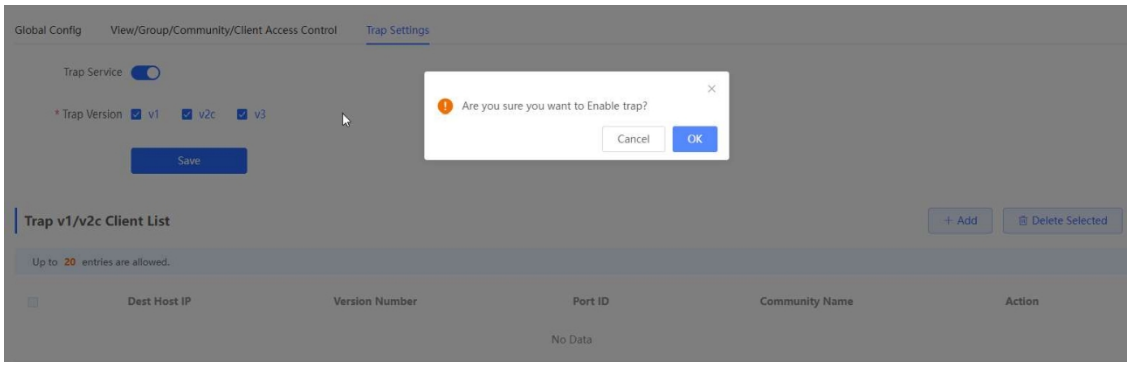
Trap - це механізм сповіщення протоколу SNMP (Simple Network Management Protocol), який використовується для повідомлення про стан і події мережевих пристроїв адміністраторам, включаючи звіти про стан пристроїв, звіти про несправності, звіти про продуктивність, звіти про конфігурацію і управління безпекою. Trap може забезпечити моніторинг мережі в режимі реального часу і діагностику несправностей, щоб допомогти адміністраторам вчасно знайти і вирішити мережеві проблеми.

1. Налаштування відкриття пастки

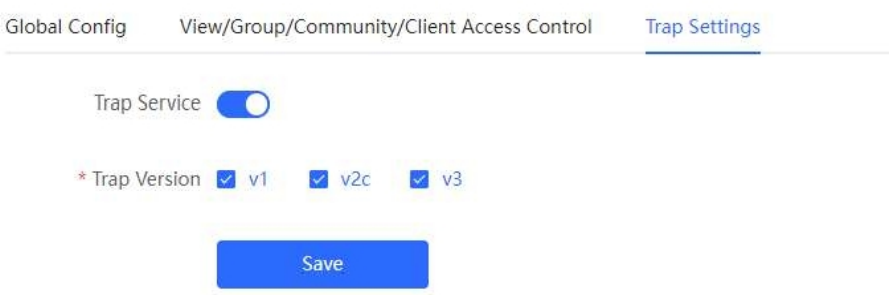
Увімкніть службу пасток і виберіть ефективну версію протоколу пасток, включаючи v1, v2c і v3.

Виберіть **Локальний пристрій> Система> SNMP> Налаштування пасток**

(1) Увімкніть перемикач служби пасток.



Коли буде увімкнено перше відкриття, система видасть . Натисніть **OK**.



(2) Встановіть версію пастки.

Номер версії протоколу пастки включає v1, версію v2c та версію v3.

(3) Натисни **ОК**.

Після увімкнення служби пасток потрібно натиснути кнопку **Зберегти** і конфігурація номера версії протоколу пастки набуде чинності.

2. Конфігурація користувача пастки v1/v2c

- Вступ

Пастка - це механізм сповіщення, який використовується для надсилання попередження адміністраторам про важливі події або збої на пристрої чи сервісі. Trap v1/v2c - це дві версії протоколу SNMP, які використовуються для управління та моніторингу мережі.

Trap v1 - це перша версія протоколу SNMP, яка підтримує базові функції сповіщення про тривоги. trap v2c - це друга версія протоколу SNMP, яка підтримує більше опцій сповіщення про тривоги та більш просунутий рівень безпеки.

Використовуючи пастки v1/v2c, адміністратор може вчасно дізнатися про проблеми в мережі та вжити відповідних заходів.

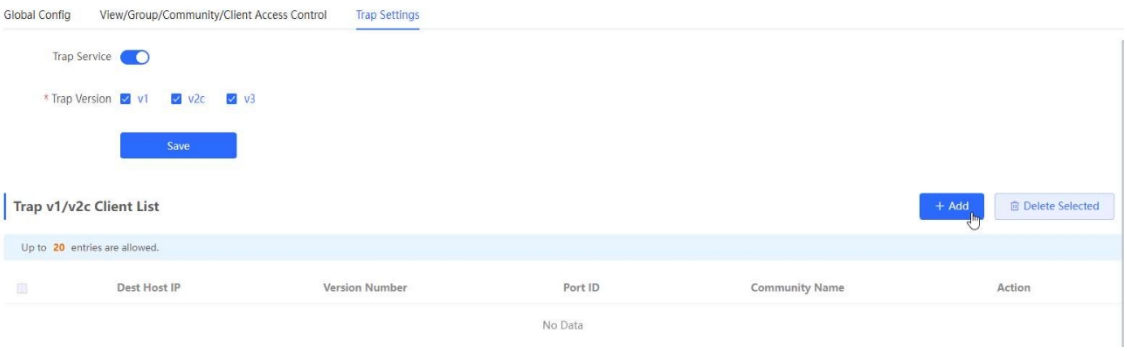
- Передумови

Якщо версія служби пасток вибрана v1 або v2c, потрібно створити користувача пастки v1v2c.

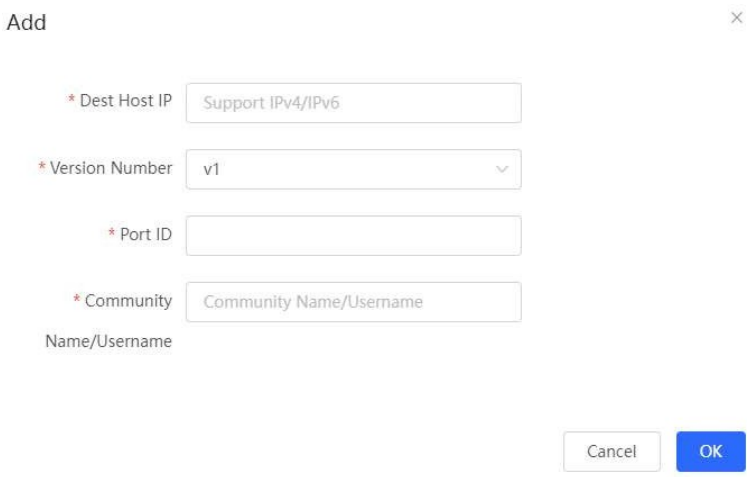
- Кроки конфігурації

Виберіть **Локальний пристрій> Система> SNMP> Налаштування пасток.**

(1) Натисніть Додати у списку Користувач пастки v1v2c, щоб створити користувача пастки v1v2c.



(2) Налаштуйте параметри пастки v1v2c, пов'язані з користувачем.



Таблиця 16-9 Таблиця опису інформації про користувача Trap v1/v2c

Параметр	Опис
IP-адреса хоста призначення	IP-адреса однорангового пристрою пастки. Підтримується IPv4 або IPv6 адреса.
Номер версії	Версія пастки, включаючи v1 та v2c.
Ідентифікатор порту	Діапазон портів пристрою-пастки - від 1 до 65535.
Назва спільноти/Ім'я користувача	Ім'я спільноти користувача пастки. Мінімум 8 символів. Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Імена адміністратора, публічні або приватні імена спільноти не допускаються. Знаки питання, пробіли та китайські ієрогліфи не .

Примітка

- IP-адреса хоста призначення користувачів пастки v1/v1/v2c не може бути однаковою.
- Назви спільнот користувачів пастки v1/v1/v2c не можуть бути однаковими.

(3) Натисни OK.

3. конфігурація користувача trap v 3

- Вступ

  Trap v3 - це механізм управління мережею на основі протоколу SNMP, який використовується для надсилання сповіщень про тривоги управлінському персоналу. На відміну від попередніх версій, trap v3 надає більш безпечні та гнучкі можливості конфігурації, включаючи аутентифікацію та шифрування.

  Trap v3 можна налаштувати так, щоб вибрати умови та способи надсилання сповіщень, а також те, хто і як отримуватиме сповіщення. Це дозволяє адміністраторам точніше розуміти стан мережевих пристроїв і вчасно вживати заходів для забезпечення безпеки та надійності мережі.

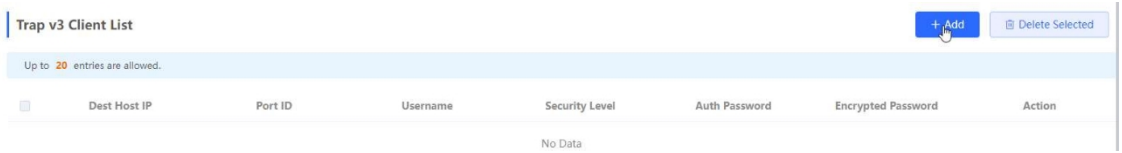
- Передумови

  Якщо вибрано v3 як версію служби пасток, потрібно створити користувача пастки v3.

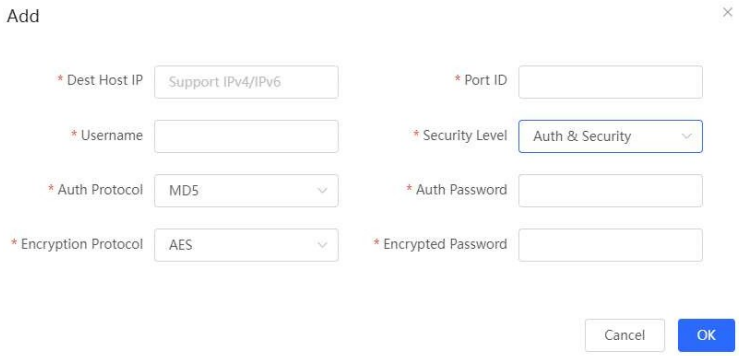
- Кроки конфігурації

Виберіть **Локальний пристрій> Система> SNMP> Налаштування пасток.**

(1) Натисніть Додати у списку "Користувач пастки v3", щоб створити користувача пастки v3.



(2) Налаштуйте параметри, пов'язані з користувачами t rap v3.



Таблиця 16-10 Таблиця опису інформації про користувача trap v3

Параметр	Опис
IP-адреса хоста призначення	IP-адреса однорангового пристрою пастки. Підтримується IPv4 або IPv6 адреса.
Ідентифікатор порту	Діапазон портів пристрою-пастки - від 1 до 65535.
Ім'я користувача	Ім'я користувача пастки v3. Мінімум 8 символів. Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Імена адміністратора, публічні або приватні імена спільноти не допускаються. Знаки питання, пробіли та китайські ієрогліфи не допускаються.
Рівень безпеки	Показує рівень безпеки користувача пастки v3. Рівні безпеки включають автентифікацію та шифрування, автентифікацію, але без шифрування, а також без автентифікації та шифрування.
Протокол авторизації, пароль авторизації	Підтримуються протоколи автентифікації: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Пароль автентифікації: 8-31 символів. Китайські ієрогліфи, повноформатні символи, знаки питання та пробіли не допускаються. Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Примітка: Цей параметр є обов'язковим, якщо рівень безпеки - автентифікація та шифрування, або автентифікація, але без шифрування.

Параметр	Опис
Протокол шифрування, пароль шифрування	Підтримуються протоколи шифрування: DES/AES/AES192/AES256. Пароль шифрування: 8-31 символів. Китайські ієрогліфи, повні символи, знаки питання та пробіли не допускаються. Він повинен містити щонайменше три категорії символів, включаючи великі та малі літери, цифри та спеціальні символи. Примітка: Цей параметр обов'язковим, якщо рівень безпеки - автентифікація та шифрування.

Примітка

IP користувачів t rap v1/v2c/v3 не можуть повторюватися.

16.5.6 Типові приклади конфігурації служби trap

1. Конфігурація пастки версій v2c

- Сценарії застосування

  Коли користувач здійснює моніторинг пристрою, якщо пристрій раптово переривається або працює ненормально, стороннє програмне забезпечення для моніторингу не може вчасно виявити і вирішити ненормальну ситуацію, тому налаштуйте пристрій з IP-адресою призначення 1 92.1 68.110.85 і номером порту 1 66, щоб пристрій надсилав пастку версії v2c у разі виникнення винятків.

- Специфікація конфігурації

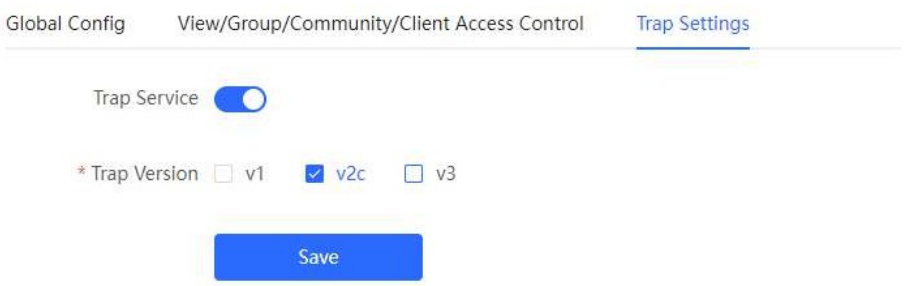
  Відповідно до аналізу сценарію використання користувача, вимоги наведені в таблиці:

Таблиця 16-11 Форма опису вимог користувача

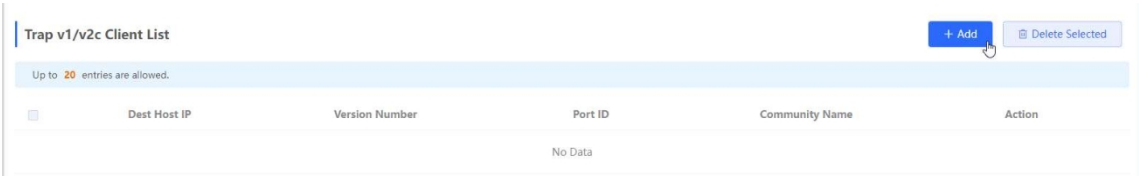
Пункт	Опис
IP-адреса та номер порту	IP-адреса хоста призначення - 192.168.110.85, а номер порту - 166.
Версія	Виберіть версію v2.
Назва спільноти/Ім'я користувача	Trap_user

- Кроки конфігурації

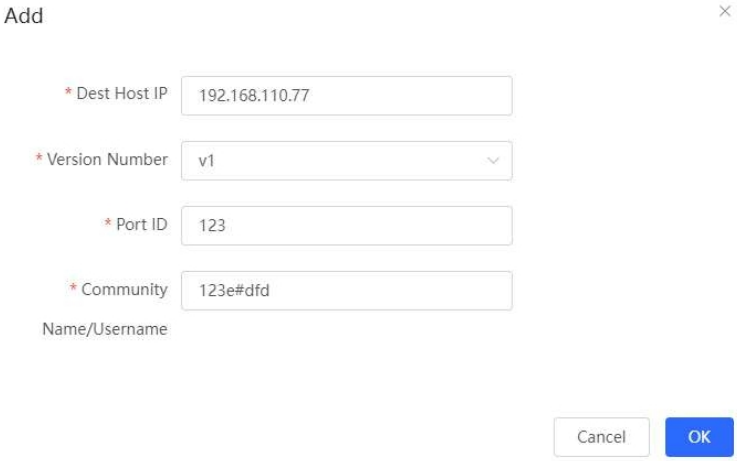
(1) Виберіть **Локальний пристрій**> **Система**> **SNMP**> **Налаштування пастки**, виберіть версію v2c в інтерфейсі налаштування пастки, натисніть **Зберегти**.



(2) Натисніть Додати в "списку користувачів пастки v1 / v2c".



(3) Введіть IP-адресу цільового хоста, номер версії, номер порту, ім'я користувача та іншу інформацію і натисніть OK після завершення налаштування.



2. Конфігурація пастки версій V3

- Сценарії застосування

  Коли користувач здійснює моніторинг пристрою, якщо пристрій раптово переривається або працює ненормально, стороннє програмне забезпечення для моніторингу не може вчасно виявити і вирішити ненормальну ситуацію, а пристрій з IP-адресою призначення 1 92.1 68.110.87 і номером порту 1 67 налаштований, і використовує більш безпечну версію v3 для надсилання пасток.

- Специфікація конфігурації

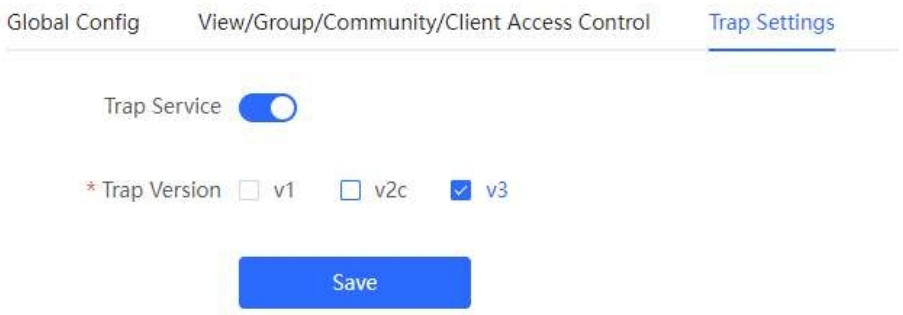
  Відповідно аналізу сценарію використання користувача, вимоги наведені в таблиці:

Таблиця 16-12 Форма опису вимог користувача

Пункт	Опис
IP-адреса та номер порту	IP-адреса хоста призначення - 192.168.110.87, а номер порту - 167.
Версія та ім'я користувача	Виберіть версію v3 і trapv3_user для імені користувача.
Протокол автентифікації/пароль автентифікації Протокол шифрування/пароль шифрування	Протокол/пароль автентифікації: MD5/Ruijie123 Протокол/пароль шифрування: AES/Ruijie123

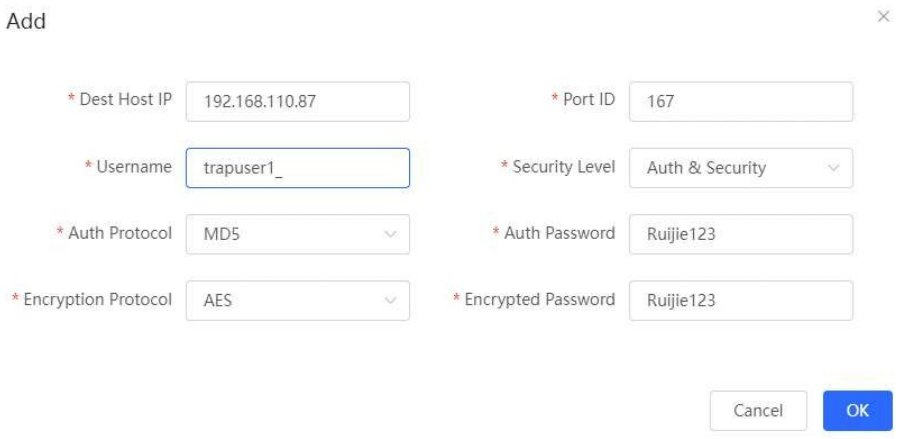
- Кроки конфігурації

(1) Виберіть версію v3 в інтерфейсі налаштувань пастки і натисніть кнопку Зберегти.



(2) Натисніть Додати у списку користувачів пастки v3.

(3) Введіть IP-адресу цільового хоста, номер порту, ім'я користувача та іншу інформацію і натисніть OK після завершення налаштування.

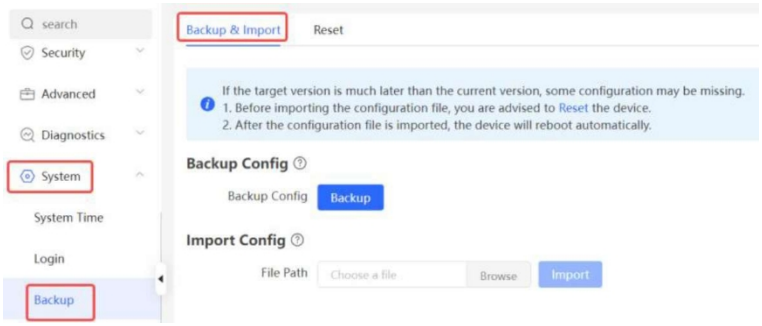


16.6 Резервне копіювання та імпорт конфігурації

Виберіть **Локальний пристрій> Система> Керування> Резервне копіювання та імпорт.**

Налаштуйте резервне копіювання: Натисніть **Резервне копіювання**, щоб створити конфігурацію резервного копіювання та завантажити її локально.

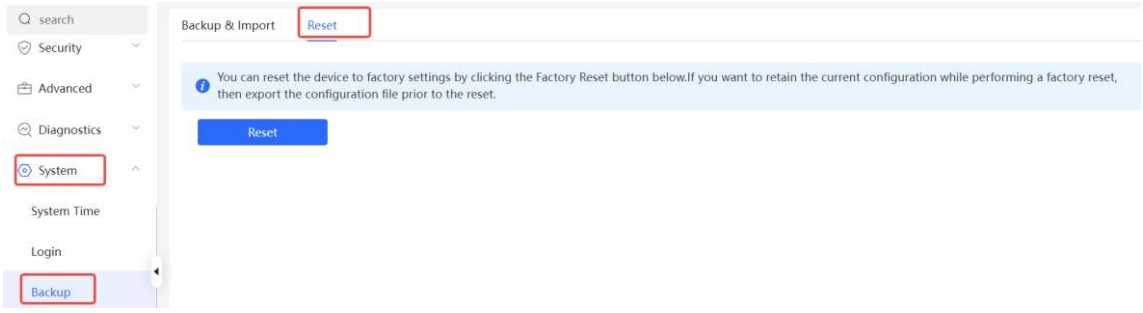
Налаштуйте імпорт: Натисніть **Огляд,** виберіть файл резервної копії конфігурації локально і натисніть **Імпорт**, щоб застосувати конфігурацію, вказану у файлі, до пристрою Після імпорту конфігурації пристрій перезавантажиться.



16.7 Перезавантаження

16.7.1 Скидання налаштувань пристрою

Виберіть **Локальний пристрій> Система> Керування> Скидання**. Натисніть **Скинути**, а потім натисніть **OK**, щоб відновити заводські налаштування.



Застереження

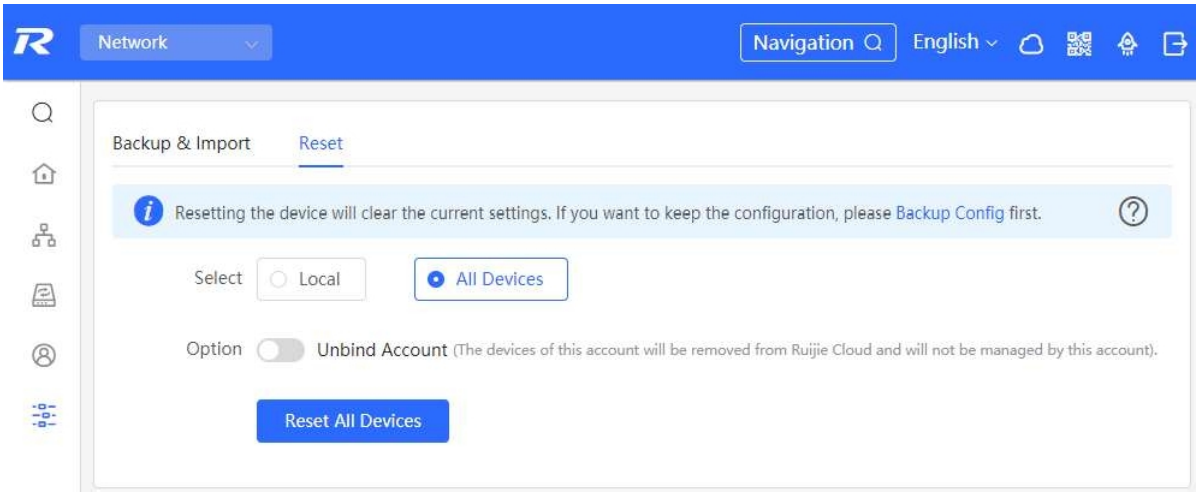
Перезавантаження пристрою призведе до очищення поточних налаштувань і перезавантаження пристрою. Якщо у поточній системі існує корисна конфігурація, ви можете експортувати поточну конфігурацію (див. 16.6 Резервне копіювання та імпорт конфігурації) перед відновленням заводських налаштувань. Будьте обережні під час виконання цієї операції.

16.7.2 Скидання пристроїв у мережі

Виберіть **Мережевий> Система> Керування> Скидання**.

Виберіть **Всі пристрої** і виберіть, чи потрібно від**'язати обліковий запис**, натисніть **Скинути всі пристрої**, і

всі пристрої в поточній мережі будуть відновлені до заводських налаштувань.



Застереження

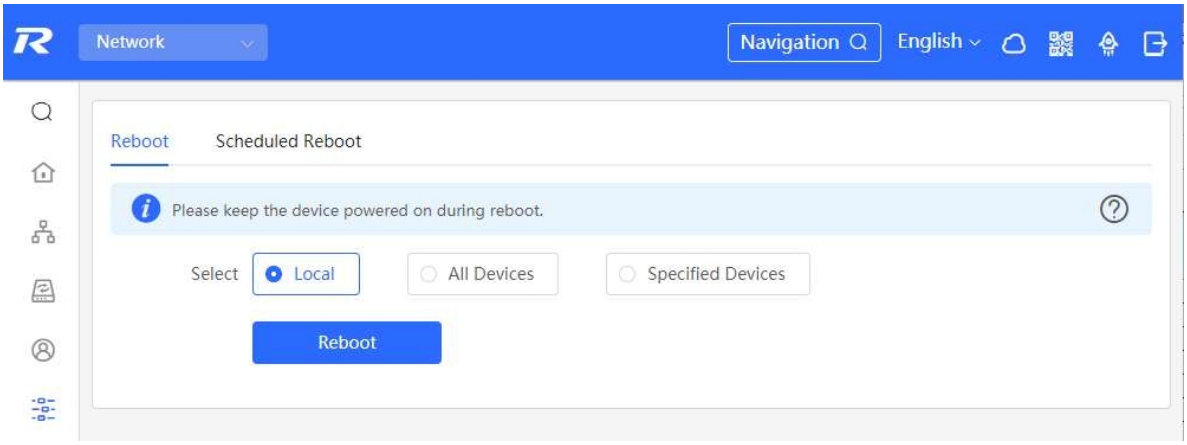
Скидання мережі призведе до очищення поточних налаштувань усіх пристроїв у мережі та перезавантаження пристроїв. Будьте обережні під час виконання цієї операції.

16.8 Перезавантаження пристрою

16.8.1 Перезавантаження пристрою

Виберіть **режим самоорганізації> Мережа> Система> Керування> Перезавантаження**. Вибрати **автономний режим> Система> Перезавантажити**.

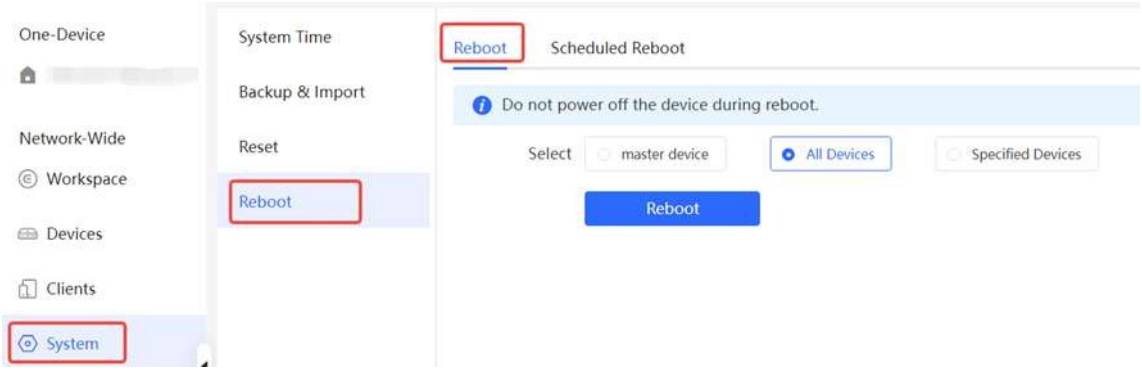
Не оновлюйте сторінку і не закривайте браузер під час перезавантаження. Після успішного перезавантаження пристрою і отримання доступу до веб-сервісу пристрій автоматично перейде на сторінку входу.



16.8.2 Перезавантаження пристроїв у мережі

Виберіть **Мережа> Система> Перезавантажити> Перезавантажити**.

Виберіть **Усі пристрої** і натисніть Перезавантажити, щоб перезавантажити всі пристрої у поточній мережі.



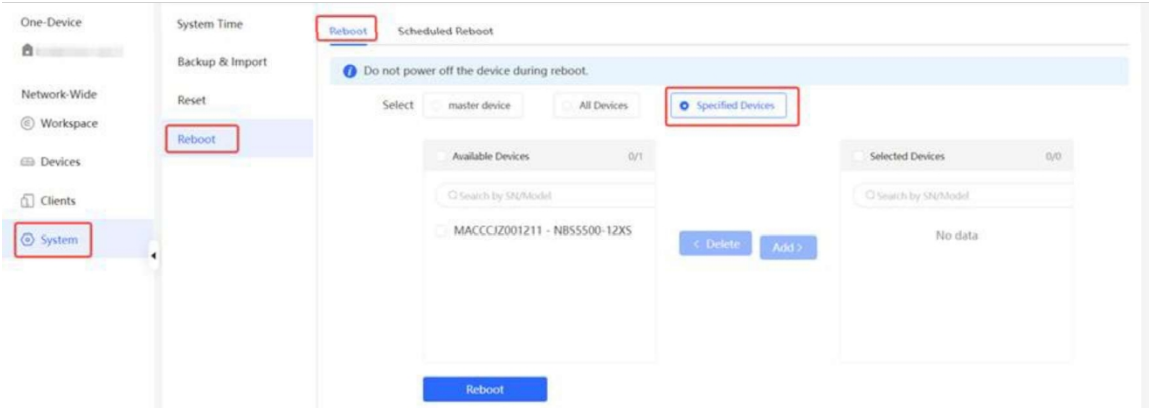
Застереження

Перезавантаження мережі займе деякий час, будь ласка, наберіться терпіння. Операція перезавантаження вплине всю мережу. Тому будьте обережні при виконанні цієї операції.

16.8.3 Перезавантаження визначених пристроїв у мережі

Виберіть **Мережа**> **Система**> **Перезавантажити**> **Перезавантажити**.

Натисніть **Зазначені пристрої**, виберіть потрібні пристрої зі списку **Доступні пристрої** і натисніть **Додати**, щоб додати пристрої до списку **Вибрані пристрої** праворуч. Натисніть **Перезавантажити**. Зазначені пристрої у списку **Вибрані пристрої** буде перезавантажено.



16.9 Налаштування перезавантаження за розкладом

Переконайтеся, що системний час є точним. Докладно про те, як налаштувати системний час, див. розділ 16.1

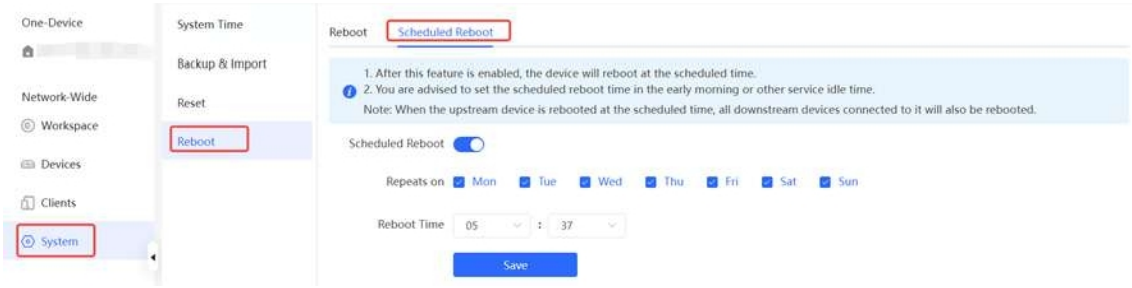
Щоб уникнути переривання роботи мережі, спричиненого перезавантаженням пристрою у невідповідний час.

Виберіть **режим самоорганізації**> **Мережа**> **Система**> **Перезавантаження за розкладом**. Виберіть **автономний режим**> **Система**> Перезавантаження за розкладом.

Натисніть **Увімкнути** та виберіть дату і час запланованого перезавантаження щотижня. Натисніть **Зберегти**. Коли системний час збігатиметься з часом запланованого перезавантаження, пристрій перезавантажиться.

Застереження

Після увімкнення перезавантаження за розкладом у мережевому режимі всі пристрої в мережі перезавантажуватимуться, коли системний час збігатиметься з часом за розкладом. Тому будьте обережні



при виконанні цієї операції.

16.10 Оновлення

Застереження

- Перед оновленням програмного забезпечення рекомендується створити резервну конфігурації.
- Оновлення версії призведе до перезавантаження пристрою. Не оновлюйте і не закривайте браузер під час процесу оновлення.

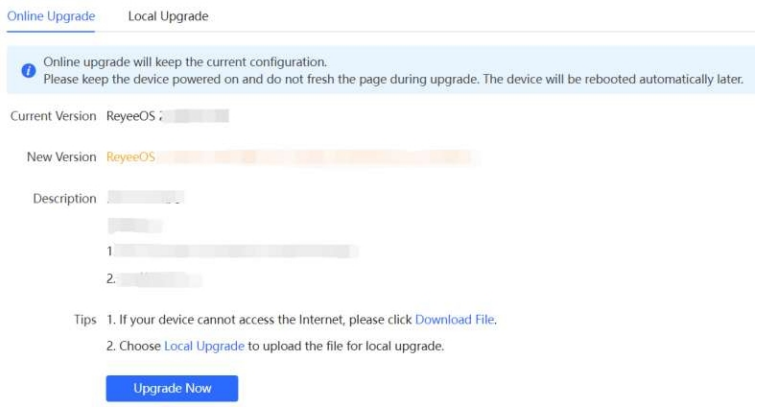
16.10.1 Оновлення онлайн

Виберіть **Локальний пристрій**> **Система**> **Оновлення**> **Оновлення онлайн**.

На поточній сторінці відображається поточна версія системи і ви можете дізнатися, чи доступна новіша версія. Якщо нова версія доступна, натисніть кнопку **Оновити зараз**, щоб виконати оновлення онлайн. Якщо мережеве середовище не підтримує оновлення через Інтернет, натисніть **Завантажити файл**, щоб завантажити інсталяційний пакет оновлення локально, а потім виконати оновлення локально.

Примітка

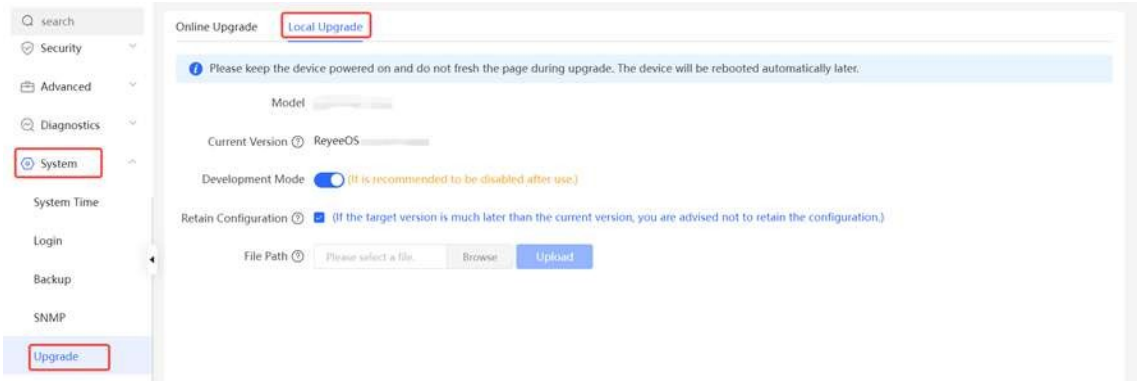
- Онлайн-оновлення збереже поточну конфігурацію.
- Не оновлюйте сторінку і не закривайте браузер під процесу оновлення. Після успішного оновлення ви будете автоматично перенаправлені на сторінку входу.



16.10.2 Локальне оновлення

Виберіть **Локальний пристрій**> **Система**> **Оновлення**> **Локальне оновлення**.

Відображає модель пристрою та поточну версію програмного забезпечення. Ви можете вибрати, чи зберігати оновлення конфігурації, чи ні. Натисніть **Огляд**, щоб вибрати локальний інсталяційний пакет програмного забезпечення, натисніть **Завантажити**, щоб завантажити інсталяційний пакет і оновити його.



16.11 Хмарний сервіс

16.11.1 Огляд

Функція "Хмарний сервіс" надає потужні можливості віддаленого керування та експлуатації мережі, що зручно та ефективно керувати географічно розподіленими мережами з різноманітними типами пристроїв. Ця функція підтримує бездротові пристрої, комутатори та шлюзи, забезпечуючи уніфіковане керування мережею та візуалізований моніторинг і експлуатацію. Крім того, вона також пропонує різні компоненти, такі як автентифікація реального імені, виділений Wi-Fi та аналіз пасажиропотоку, що дозволяє гнучко розширювати мережеві сервіси.

Налаштувавши хмарний сервіс, ви можете зручно керувати мережами через Ruijie Cloud або додаток Ruijie Reyee.

16.11.2 Кроки конфігурації

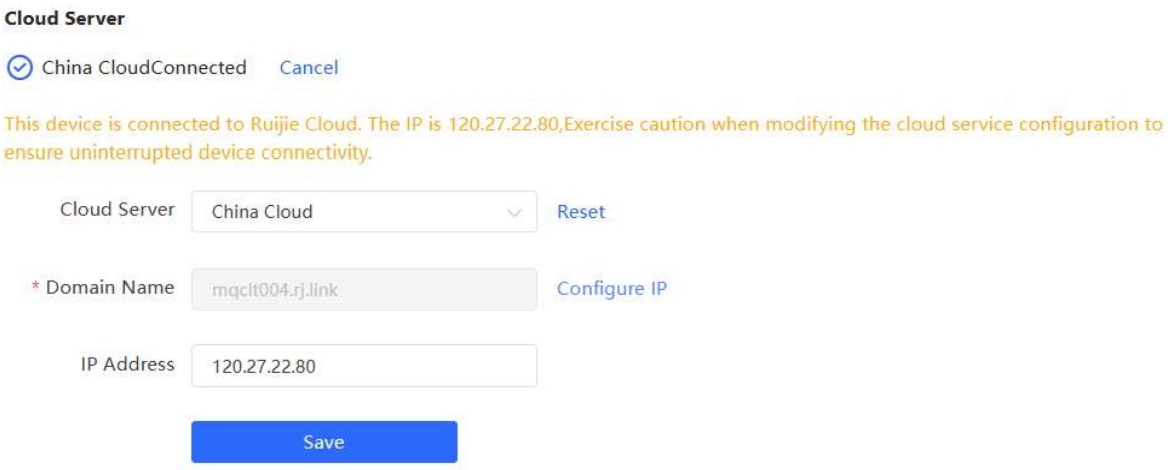
Виберіть **One-Device**> **Config**> **Система**> **Хмарний сервіс**.

Якщо пристрій ще не пов'язаний з хмарним обліковим записом, просто дотримуйтесь інструкцій на екрані, щоб додати його до мережі. Відкрийте програму Ruijie Reyee, натисніть піктограму сканування у верхньому лівому кутку на сторінці **проекту** та введіть пароль керування пристроєм.

Щойно пристрій буде пов'язано з хмарним обліковим записом, його буде автоматично прив'язано до хмарного сервера на основі його географічного розташування.

Застереження

Будьте обережні, змінюючи конфігурацію хмарного сервісу, оскільки неналежні зміни можуть призвести до проблем зі зв'язком між пристроєм і хмарним сервісом.



Щоб змінити конфігурацію хмарного сервісу, виберіть хмарний сервер зі спадного списку **Хмарний сервер**, введіть доменне ім'я та IP-адресу і натисніть кнопку **Зберегти**.

Примітка

Якщо вибраний сервер не є **Іншим хмарним**, система автоматично заповнює доменне ім'я та IP-адресу хмарного сервера. Якщо вибрано "**Інша хмара**", вам потрібно вручну налаштувати доменне ім'я та IP-адресу, а також завантажити сертифікат хмарного сервера.

Таблиця 16-13 Опис хмарного сервера

Параметр	Опис
Хмарний сервер	Географічне розташування хмарного сервера, включаючи Китайську хмару, Азійську хмару, Європейську хмару, Американську хмару та інші.
Доменне ім'я	Доменне ім'я хмарного сервера.
IP-адреса	IP-адреса хмарного сервера.

16.11.3 Відв'язування хмарного сервісу

Виберіть **один пристрій**> **Конфігурація**> **Система**> **Хмарний сервіс**

Ви можете натиснути кнопку Відв**'язати**, щоб відв'язати обліковий запис, якщо ви більше не бажаєте керувати цим проектом віддалено.