

Веб-интерфейс коммутатора 100 Мбит/с с PoE

Руководство пользователя

Правовая информация

Информация о документе

- Руководство содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначена только для ознакомления.
- Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. При использовании данного документа обращайтесь за помощью к профессионалам, обученным работе с продуктом.

О продукте

- Послепродажное обслуживание данного продукта возможно только в той стране или регионе, где была совершена покупка.
- Если выбранный вами продукт является видеопродуктом, сканируйте QR-код, чтобы ознакомиться с программой по использованию продукции видеомониторинга.

Признание прав интеллектуальной собственности

- iFLOW владеет авторскими правами и/или патентами, связанными с технологиями, реализуемыми в продукции и описанными в данном документе, которые могут включать лицензии, полученные от третьих лиц.
- Любая часть документа, включая текст, изображения, графику и т. д., принадлежит iFLOW. Никакая часть этого документа не может быть извлечена, скопирована, переведена или изменена полностью или частично любыми способами без письменного разрешения.
- Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

Введение

Модели

Данное руководство предназначено для коммутатора серии F-SW-EM4XXPOE-VM.

Значения по умолчанию

- Имя пользователя по умолчанию для учетной записи администратора: admin.
- IP-адрес по умолчанию: 192.168.1.64.

Условные обозначения

В настоящем документе используются следующие символы.

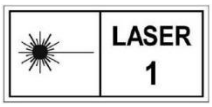
Символ	Описание
Предупреждение	Указывает на опасную ситуацию, которая, если не удастся ее избежать, может привести к летальному исходу или серьезным травмам.
Предостережение	Указывает на потенциально опасную ситуацию, которая может привести к повреждению оборудования, потере данных, ухудшению рабочих характеристик, либо к получению незапланированных результатов.
Примечание	Предоставляет дополнительную информацию, чтобы подчеркнуть или дополнить важные пункты основного текста.

Инструкция по технике безопасности

- **Предупреждения**. Это продукт класса A. В домашних условиях этот продукт может создавать радиопомехи, и в этом случае пользователю может потребоваться принять необходимые меры по их устранению.
- Корпуса устройств, подключенных через порт PoE, должны быть защищены огнестойким покрытием, поскольку коммутаторы не соответствуют стандарту Limited Power Source (LPS).
- Использование продукта должно строго соответствовать нормам электробезопасности страны и региона.
- Розетка должна располагаться рядом с устройством, необходимо обеспечить легкий доступ к розетке.

- Устройство должно быть подключено к розетке с заземлением.
- Установите устройство в соответствии с инструкциями в этом руководстве.
- ϟ указывает на наличие опасного напряжения. Внешняя проводка должна быть установлена квалифицированным персоналом.
- Не прикасайтесь к лопастям вентилятора. Во время обслуживания отключите источник питания.
- Запрещено размещать устройство на неустойчивой поверхности. Падение устройства может привести к серьезным травмам или смерти.
- Данное устройство не подходит для использования в местах, где могут присутствовать дети.
- **Предостережение**. При замене батареи батареей несоответствующего типа, существует риск взрыва.
- Замена батареи на батарею несоответствующего типа может привести к нарушению мер предосторожности (например, в случае некоторых типов литиевых батарей).
- Запрещено помещать батарею в огонь или работающий духовой шкаф, разбивать и или резать батарею, так как это может привести к взрыву.
- Запрещено оставлять батарею в окружающей среде при очень высоких температурах, так как это может привести к взрыву или утечке горючей жидкости или газа.
- Запрещено подвергать батарею воздействию крайне низкого давления воздуха, так как это может привести к взрыву или утечке горючей жидкости или газа. Использованные батареи необходимо утилизировать в соответствии с инструкциями.

- ⚠ **Предупреждения**. Двухполюсный/нейтральный предохранитель. После срабатывания предохранителя части устройства, которые остаются под напряжением, могут представлять опасность во время обслуживания.
- Устройство было специально разработано для ситуации, когда необходимо подключиться к IT-системе распределения питания.
- Устройство необходимо устанавливать на бетонную поверхность или на другие поверхности, не подвергаемые воспламенению.
- Не закрывайте вентиляционные отверстия такими предметами, как газеты, скатерти, шторы и т. д. Запрещается закрывать отверстия, помещая устройство на кровать, диван, коврик или другую подобную поверхность.
- Запрещается ставить на устройство источники открытого огня, например, зажженные свечи.
- На устройство не должны попадать капли или брызги. Запрещено ставить на него предметы, наполненные жидкостью, например, вазы.
- При работе с такими деталями возможен ожег пальцев. После выключения необходимо подождать полчаса, прежде чем работать с деталями.
- Класс 1 Лазерные изделия



Содержание

Раздел 1 Представление продукта 1
Раздел 2 Активация устройства и вход в систему 2
Раздел 3 Управление устройствами 4
Раздел 4 Конфигурация устройства 7
4.1 Настройка портов 7
4.1.1 Настройка атрибутов 7
4.3.2 Настройка зеркалирования портов 8
4.1.3 Настройка режима дальнего действия 9
4.1.4 Настройка изоляции портов 10
4.2 Настройка агрегации каналов 10
4.3 Настройка VLAN 12
4.3.1 Добавление VLAN 12
4.3.2 Настройка порта 12
4.4 Настройка QoS 14
4.5 Настройка SNMP 17
4.5.1 Настройки SNMP-прокси 17
4.5.2 Настройки SNMP-ловушек 17
4.6 Настойка STP 19
4.6.1 Глобальная настройка 19
4.6.2 Настройка порта STP 21
4.6.3 Просмотр состояния STP 22
4.7 Управление PoE 23
Раздел 5 Управление системой 24
5.1 Синхронизация времени 24
5.2 Эксплуатация устройства 25
5.3 Экспорт файла конфигурации 25
5.4 Импорт файла конфигурации 26
5.5 Обновление устройства 26
5.6 Управление журналом 27

5.7 Диагностика сети 28
5.8 Управление пользователями 28
5.9 Управление безопасностью 29

Раздел 1 Представление продукта

Данный PoE-коммутатор 2-го уровня с передовой технологией питания PoE применяют для обеспечения высокоэффективного доступа и стабильной загрузки данных. Коммутаторы поддерживают управление клиентскими ПО, управление топологией сети, агрегацию каналов, управление портами и т. д. Коммутаторы подходят для доступа к небольшим устройствам локальной сети.

Раздел 2 Активация устройства и вход в систему

При первом использовании необходимо активировать коммутатор и установить пароль.

Перед началом

Убедитесь, что коммутатор и компьютер находятся в одном сегменте сети.

Шаги

Примечание

Представленные изображения носят исключительно справочный характер.

1. Введите IP-адрес по умолчанию 192.168.1.64 в адресную строку браузера.

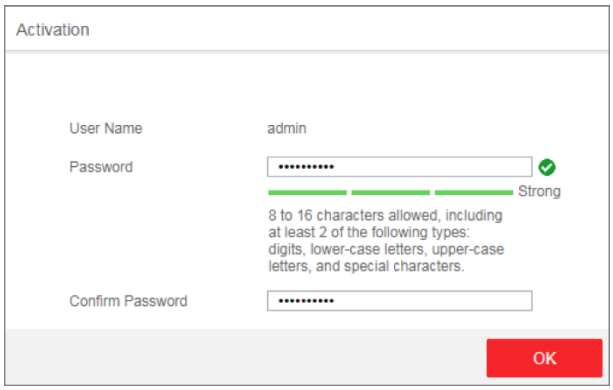


Рисунок 2-1. Активация

Примечание

Рекомендуется использовать последние версии следующих браузеров: IE 10+, Edge и Chrome 31+.

2. Укажите пароль и подтвердите его.
3. Нажмите **OK**.
   Перейдите на страницу входа в систему.

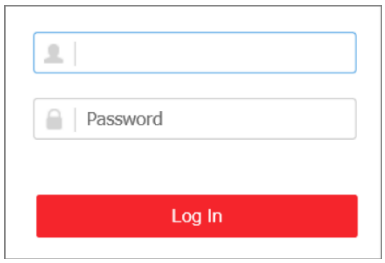


Рисунок 2-2. Вход

4. Введите имя пользователя и пароль, затем нажмите **Log In** («Войти»).

5. Опционально. Измените параметры сети.
   1) Перейдите в меню **System Management** → **Network Configuration** («Управление системой → Настройка параметров сети»).

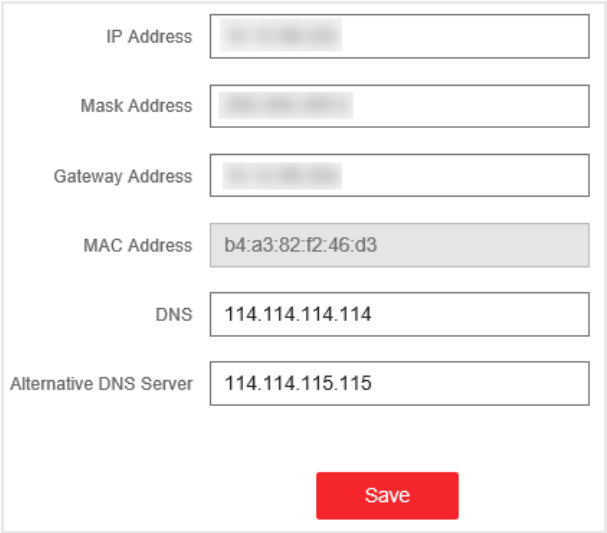


Рисунок 2-3. Настройка сетевых параметров

   2) При необходимости измените IP-адрес, маску-адрес, адрес шлюза, DNS и альтернативный DNS сервер. При следующем входе можно будет использовать новый IP-адрес.

Примечание

Для удобного управления устройством рекомендуется изменить параметры сети.

Раздел 3 Управление устройствами

После входа в веб-интерфейс можно перейти в раздел **Device Status** («Состояние устройства»), чтобы просмотреть информацию о устройстве, включая данные об устройстве, рабочее состояние, состояние портов, статистику портов и состояние PoE.

Информация об устройстве

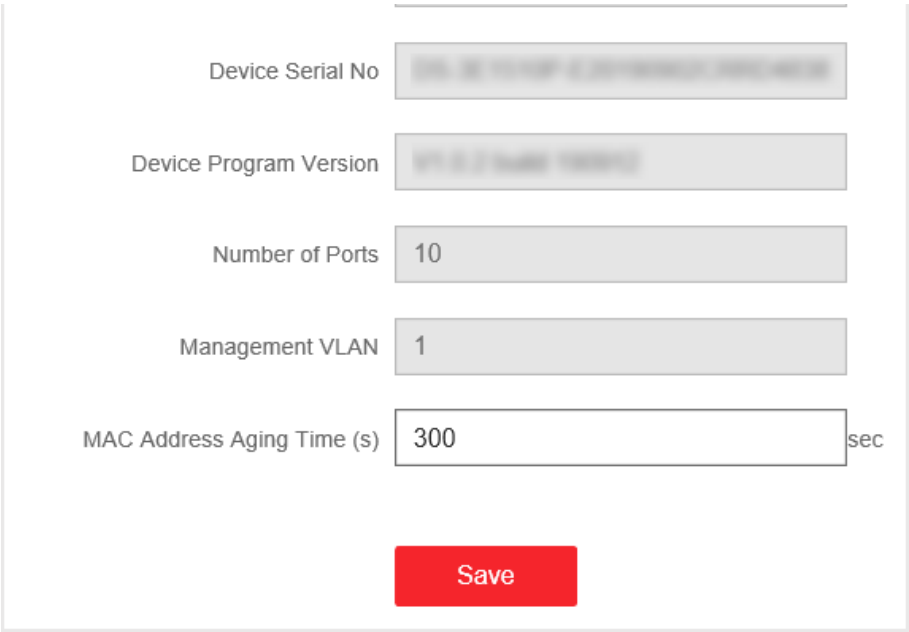


Рисунок 3-1. Информация об устройстве

- **Управляющая VLAN.** По умолчанию управляющая VLAN — это VLAN 1, ее нельзя изменить.
- **Время устаревания MAC-адреса.** Время устаревания записей в таблице MAC-адресов. Значение по умолчанию — 300 секунд, его нельзя изменить.

Состояние режима работы

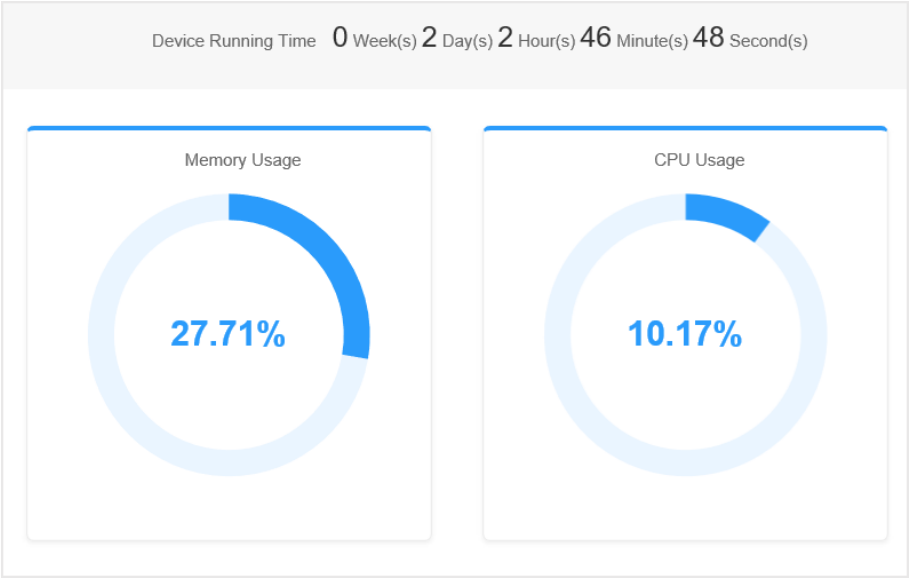


Рисунок 3-2. Состояние работы

Просмотрите время работы устройства, использование памяти и загрузку процессора.

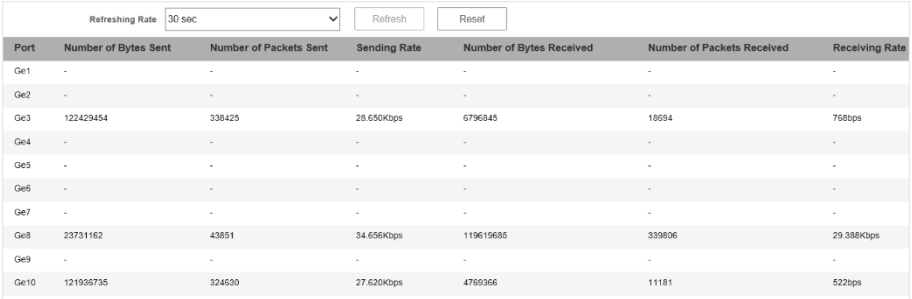
Состояние порта

Port Name	Connection Status	Rate	Duplex	Flow Control
Ge1	Disconnected	-	-	-
Ge2	Connected	1000M	Full-Duplex	Off
Ge3	Disconnected	-	-	-
Ge4	Connected	1000M	Full-Duplex	Off
Ge5	Disconnected	-	-	-
Ge6	Disconnected	-	-	-
Ge7	Disconnected	-	-	-
Ge8	Connected	1000M	Full-Duplex	On
Ge9	Connected	1000M	Full-Duplex	On
Ge10	Disconnected	-	-	-

Рисунок 3-3. Состояние порта

Просмотрите состояние соединения, скорость, режим дуплекса и управление потоком для всех портов.

Статистика порта

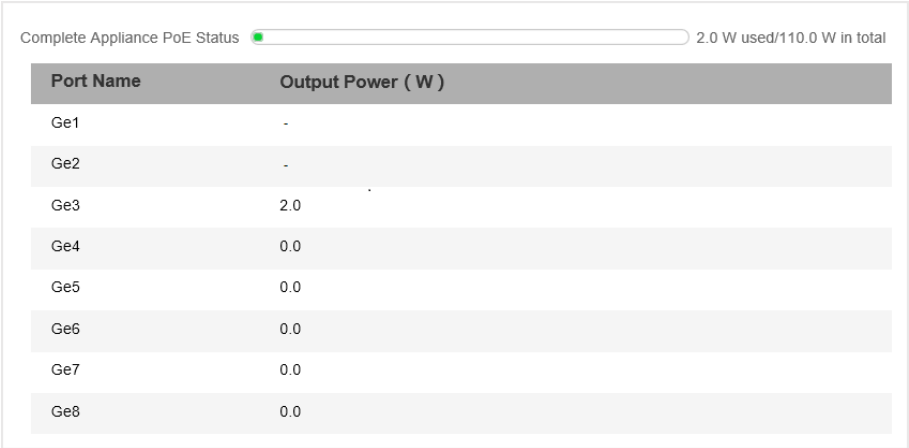


Port	Number of Bytes Sent	Number of Packets Sent	Sending Rate	Number of Bytes Received	Number of Packets Received	Receiving Rate
Ge1	-	-	-	-	-	-
Ge2	-	-	-	-	-	-
Ge3	122429454	338425	28.650Kbps	6796845	18694	768bps
Ge4	-	-	-	-	-	-
Ge5	-	-	-	-	-	-
Ge6	-	-	-	-	-	-
Ge7	-	-	-	-	-	-
Ge8	23731162	43851	34.656Kbps	119619685	339806	29.388Kbps
Ge9	-	-	-	-	-	-
Ge10	121936735	324530	27.620Kbps	4769366	11181	522bps

Рисунок 3-4. Статистика порта

- **Частота обновления.** Доступны интервалы обновления 10, 30, 60 секунд, а также **Manually Refresh** («Обновление вручную»).
- **Обновить.** При выборе опции **Manually Refresh** («Обновить вручную») можно нажать **Refresh** («Обновить»), чтобы обновить статистику.
- **Сброс**. Нажмите **Reset** («Сбросить») для сброса всей статистики.

Состояние PoE



Port Name	Output Power (W)
Ge1	-
Ge2	-
Ge3	2.0
Ge4	0.0
Ge5	0.0
Ge6	0.0
Ge7	0.0
Ge8	0.0

Рисунок 3-5. Состояние PoE

Просмотрите полное состояние PoE устройства и выходную мощность каждого порта PoE.

Раздел 4 Конфигурация устройства

4.1 Настройка портов

4.1.1 Настройка атрибутов

Основные параметры могут влиять на рабочее состояние портов. Настройте необходимые параметры.

Шаги

1. Нажмите **Switch Configuration** → **Basic Configuration** → **Port Configuration** → **Attribute Configuration** («Настройка коммутатора → Базовая настройка → Настройка портов → Настройка атрибутов»).

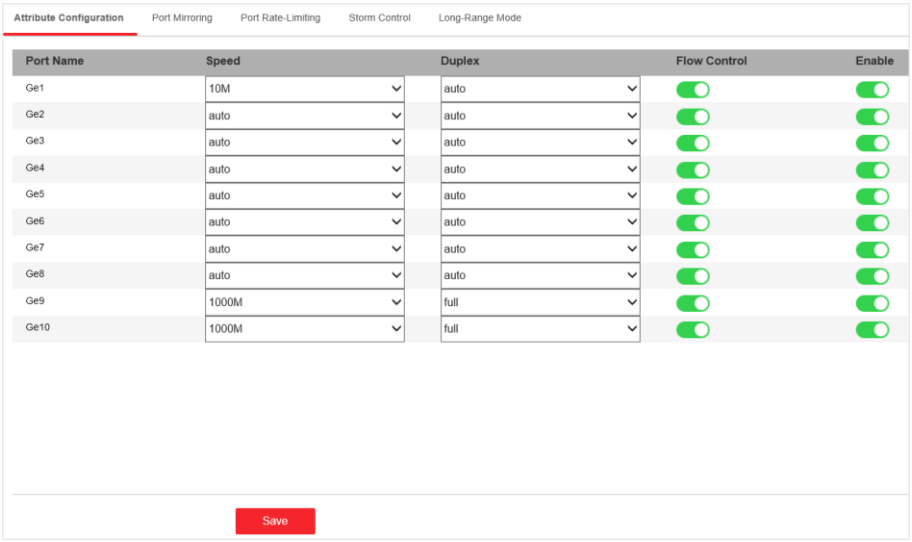


Рисунок 4-1. Настройка атрибутов порта

2. Настройте параметры.

Скорость

Скорость передачи данных через порт.

- Порт PoE: значение по умолчанию — **auto** («Автоматически»).
- Оптоволоконный порт SFP: по умолчанию установлено значение **Auto** («Автоматически»), которое нельзя изменить.

Дуплекс

Дуплексный режим порта.

- Порт PoE: по умолчанию установлено значение **auto** («Автоматически»), которое нельзя изменить.
- Оптоволоконный порт SFP: по умолчанию установлено значение **auto** («Автоматически»), которое нельзя изменить.

Контроль потока

Включение управления потоком данных может предотвратить потерю данных при передаче.

Включить

Включить или отключить соединение портов.

3. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

4.3.2 Настройка зеркалирования портов

Функция зеркалирования портов отслеживает сетевой трафик, отправляя копии всех входящих и исходящих пакетов с одного порта на зеркалирующий порт.

Шаги

1. Нажмите **Switch Configuration** → **Basic Configuration** → **Port Configuration** → **Port Mirroring** («Настройка коммутатора → Базовая настройка → Настройка портов → Зеркалирование портов»).
2. Нажмите **Enable** («Включить») в поле **Port Mirroring** («Зеркалирование портов»).
3. Выберите один порт в качестве зеркального порта, который будет отслеживать и анализировать пакеты с зеркала исходного порта.
4. Выберите **Mirror Direction** («Направление зеркалирования»).

Отключить зеркалирование

Порт не находится под наблюдением.

Входящие

Данные, полученные через зеркало исходного порта, находятся под наблюдением.

Исходящие

Данные, отправляемые с зеркала исходного порта, находятся под наблюдением.

Входящие и исходящие

Как полученные, так и отправленные данные с зеркала исходного порта находятся под наблюдением.

5. Включите параметр **Set as Mirror Source** («Установить в качестве источника зеркалирования»), если хотите выбрать определенные порты из списка в качестве источника зеркалирования, находящегося под наблюдением.

Примечание

Можно установить один или несколько портов в качестве источника зеркалирования.

6. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

4.1.3 Настройка режима дальнего действия

После включения режима дальней связи для порта дальность передачи данных может достигать 300 метров при скорости 10 Мбит/с.

Шаги

1. Нажмите **Switch Configuration** → **Basic Configuration** → **Port Configuration** → **Long-Range Mode** («Настройка коммутатора → Базовая настройка → Настройка портов → Режим дальней связи»).

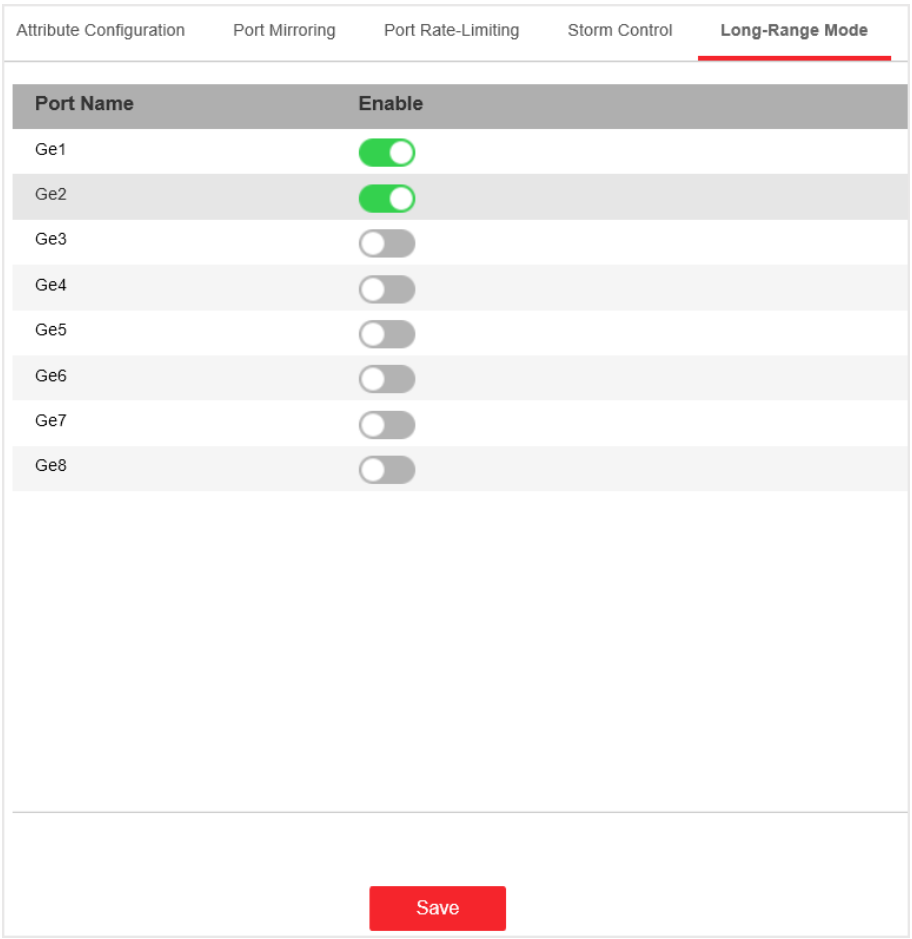


Рисунок 4-2. Настройка режима дальнего действия

2. Нажмите **Enable** («Включить»), чтобы включить порт.
3. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

4.1.4 Настройка изоляции портов

Настройте порты на разные VLAN, чтобы изолировать различные пакеты на уровне 2. Порты, входящие в одну группу изоляции, не могут взаимодействовать друг с другом, но могут взаимодействовать с портами, входящими в разные группы.

Шаги

1. Нажмите **Switch Configuration** → **Basic Configuration** → **Port Configuration** → **Port Isolation** («Настройка коммутатора → Базовая настройка → Настройка портов → Изоляция портов»).
2. Выберите порты для включения в группу изоляции.
3. Нажмите **Save** («Сохранить»).

4.2 Настройка агрегации каналов

Агрегация каналов используется для объединения физических портов с целью создания логического канала. Преимущества агрегации каналов заключаются в более высокой скорости передачи данных и более широкой полосе пропускания.

Шаги

1. Нажмите **Switch Configuration** → **Basic Configuration** → **Link Aggregation** → **Load Balancing Configuration** («Настройка коммутатора → Основные настройки → Агрегация каналов → Настройка балансировки нагрузки»), для настройки балансировки нагрузки.

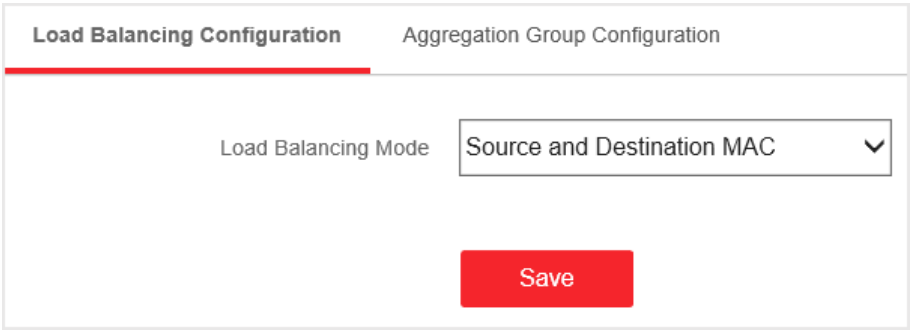


Рисунок 4-3. Балансировка нагрузки

MAC-адреса источника и назначения

Балансировка нагрузки осуществляется на основе MAC-адресов источника и назначения всех пакетов.

2. Добавьте группу агрегации каналов в разделе **Aggregation Group Configuration** («Настройка группы агрегации»).

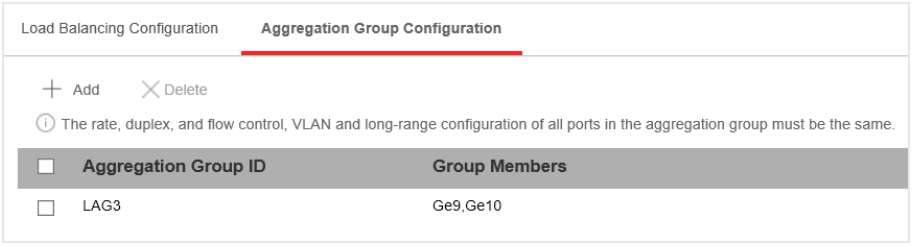


Рисунок 4-4. Группа агрегации каналов

1) Нажмите **Add** («Добавить»)

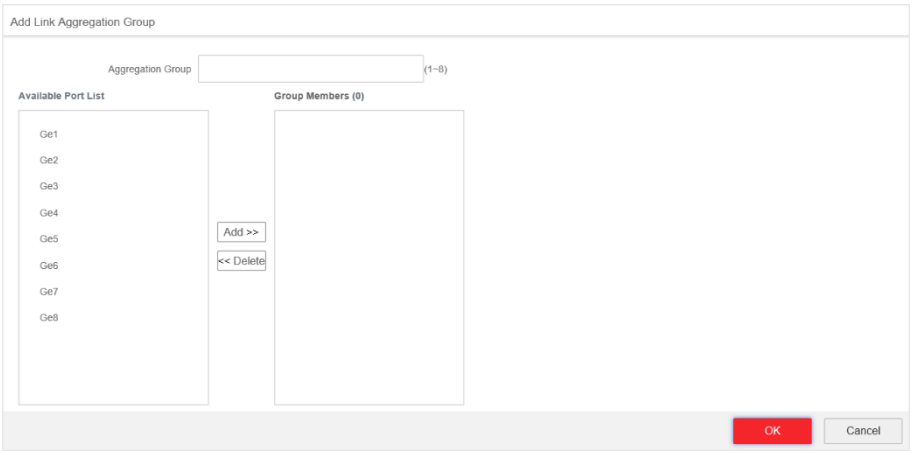


Рисунок 4-5. Добавление группы агрегации каналов

2) Введите номер группы в поле **Aggregation Group** («Группа агрегации»). Диапазон от 1 до 8.

3) Переместите порты, которые должны быть назначены группе, из **Available Port List** («Список доступных портов») в **Group Members** («Список членов группы»).

Примечание

- Удалить порты из списка участников группы можно, нажав **Delete** («Удалить»).
- Скорость передачи данных, режим дуплекса, управление потоком, VLAN и конфигурация для дальней связи всех портов в одной группе агрегации должны быть одинаковыми.

4) Нажмите ОК, чтобы добавить группу агрегации каналов.

4.3 Настройка VLAN

Виртуальная локальная сеть (VLAN) — это группа устройств, расположенных в разных сегментах локальной сети, и они настроены на взаимодействие так, как если бы они были подключены к одному и тому же проводу. Локальные сети основаны на логических, а не

физических соединениях, что обеспечивает гибкость при подключении устройств.

4.3.1 Добавление VLAN

Шаги

1. Нажмите **Switch Configuration** → **Basic Configuration** → **VLAN** → **802.1Q VLAN** («Настройка коммутатора → Базовая настройка → VLAN → 802.1Q VLAN»).
2. Нажмите **Add** («Добавить»).

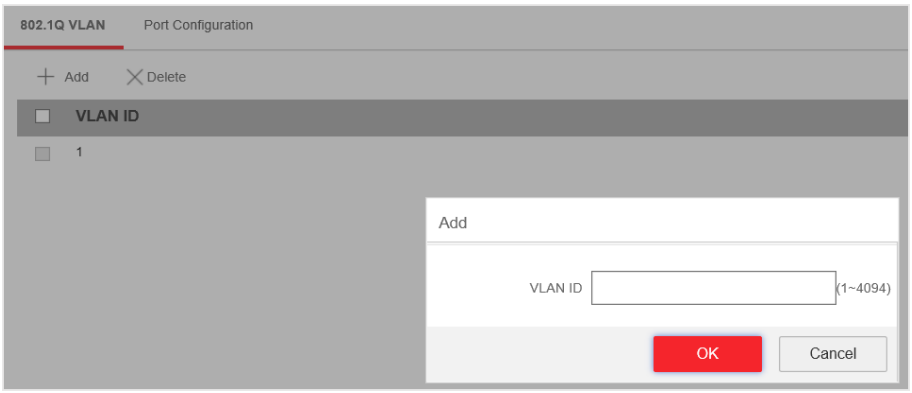


Рисунок 4-6. Добавление VLAN

3. Введите идентификатор VLAN.

Примечание

- Поддерживается максимум 128 VLAN.
- Диапазон от 1 до 4094.

4. Опционально. Также можно удалить VLAN, нажав **Delete** («Удалить»).

Примечание

Удалить VLAN 1 невозможно, поскольку VLAN 1 является управляющей.

4.3.2 Настройка порта

Шаги

1. На странице **Port Configuration** («Настройка портов») выберите порт для настройки.

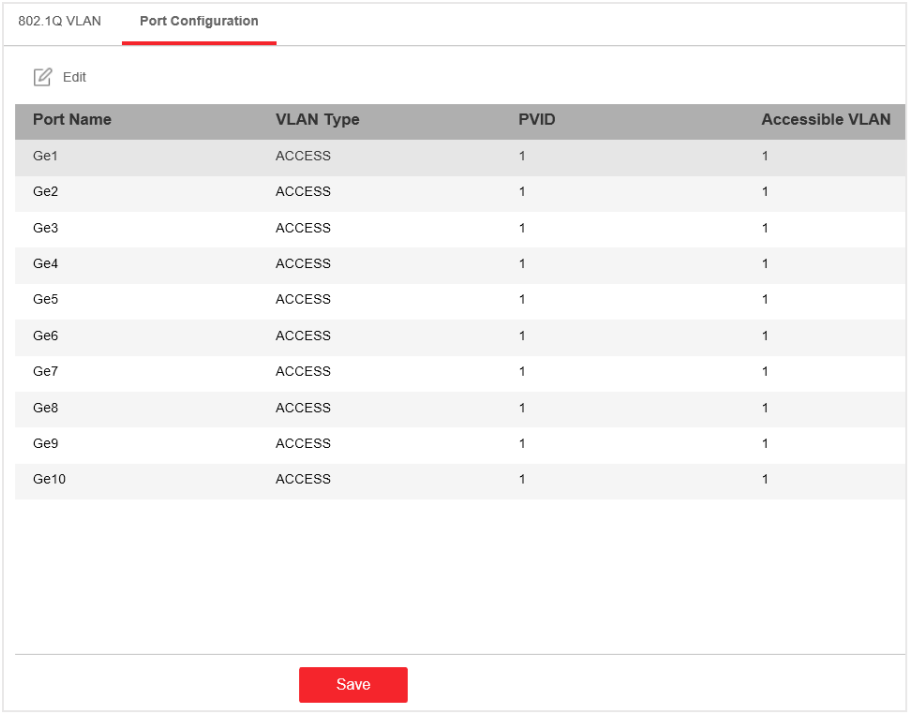


Рисунок 4-7. Настройка портов VLAN

2. Нажмите **Edit** («Редактировать»).
3. Настройте VLAN для порта.

Порт доступа

- Порт доступа передает трафик только в указанную VLAN и из нее, обычно это VLAN по умолчанию, VLAN 1.
- Выберите тип VLAN порта как **ACCESS** и укажите **PVID**.

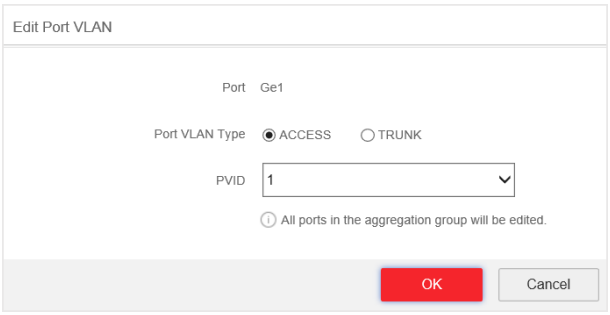


Рисунок 4-8. Редактирование VLAN порта доступа

Примечание

Все порты в одной группе агрегации будут автоматически отредактированы одновременно.

Транковый порт

- Транковый порт — это порт, предназначенный для передачи трафика для всех VLAN.
- Выберите тип VLAN порта как TRUNK, выберите PVID и введите VLAN, к которым разрешен доступ.

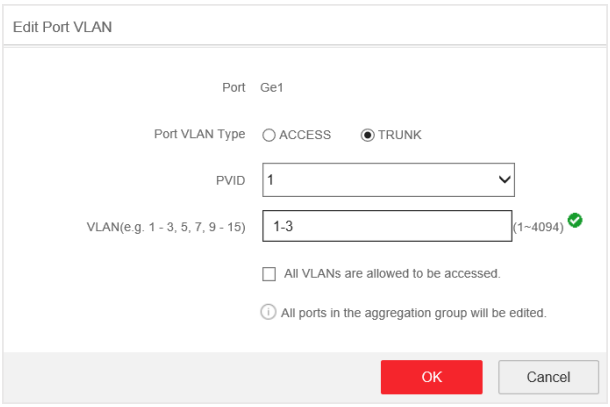


Рисунок 4-9. Редактирование VLAN транкового порта

Примечание

- Все порты в одной группе агрегации будут автоматически отредактированы одновременно.
- Нажмите **All VLANS are allowed to be accessed.** («Доступ ко всем VLAN разрешен.») и назначьте порт всем VLAN.

4. Нажмите **OK**.
5. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

4.4 Настройка QoS

Качество обслуживания (QoS) включает в себя пропускную способность сети, задержку, коэффициент потери пакетов и т. д. Увеличение пропускной способности сети, уменьшение задержки в сети и снижение потерь пакетов могут улучшить качество обслуживания в сети. Можно настроить режим планирования и приоритет порта для QoS.

Шаги

1. Перейдите в раздел **Switch Configuration** → **Basic Configuration** → **QoS** → **Scheduling Mode** («Настройка коммутатора → Основные настройки → QoS → Режим планирования»), чтобы выбрать тип планирования.

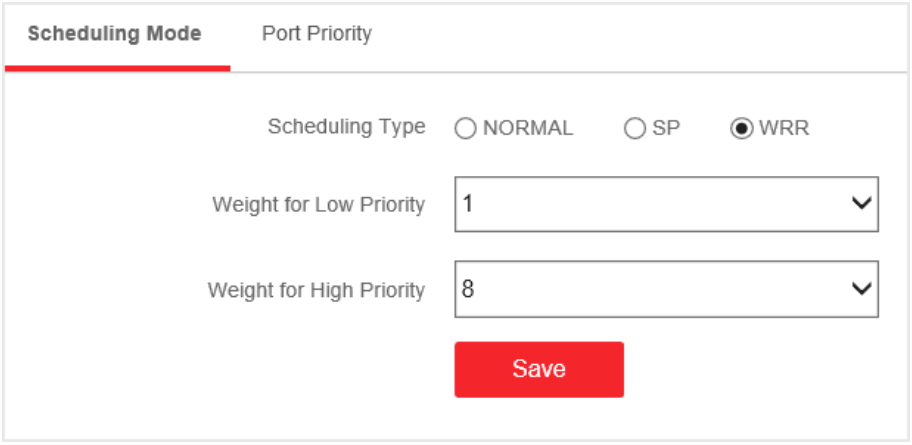


Рисунок 4-10. Режим планирования

Обычный режим

Режим «первым пришел — первым вышел» (FIFO). Передача первого входящего сообщения. QoS не включен.

SP

Режим строгого приоритета. Передача сообщения в соответствии с фактической конфигурацией приоритета.

WRR

Режим взвешенного циклического перебора. Передайте сообщение в соответствии с весом, соответствующим низкому и высокому приоритету.

2. Настройте приоритет порта в разделе **Port Priority** («Приоритет порта»).

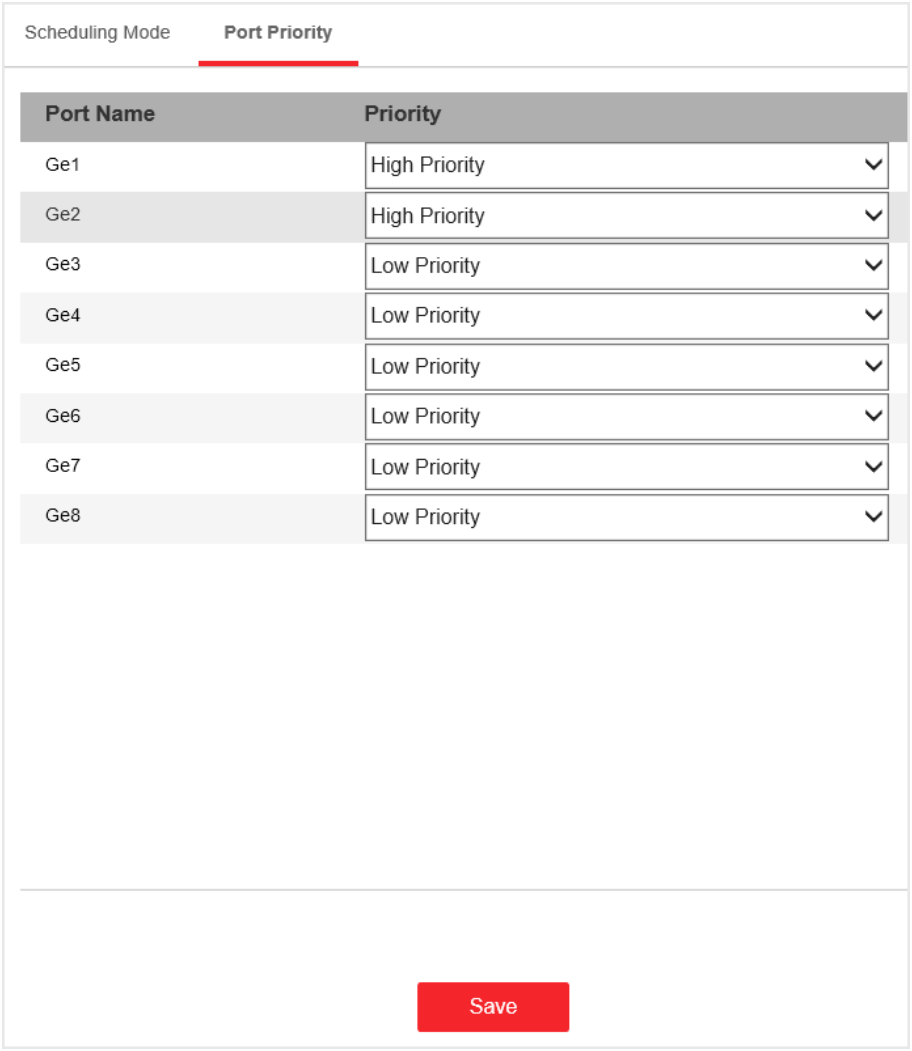


Рисунок 4-11. Приоритет порта

3. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

4.5 Настройка SNMP

Простой протокол сетевого управления (SNMP) — это протокол связи прикладного уровня, используемый для мониторинга рабочих характеристик сети. Сеть SNMP состоит из системы управления сетью (NMS) и агента. NMS является менеджером SNMP, а агент отправляет ловушки в NMS. Настройка SNMP включает в себя базовые настройки, настройки сообщества

и настройки целевого хоста ловушек.

4.5.1 Настройки SNMP-прокси

Шаги

1. Для настройки SNMP-прокси перейдите в раздел **Switch Configuration** → **L2 Configuration** → **SNMP Configuration** → **SNMP Proxy Settings** («Настройки коммутатора → Настройки L2 → Настройки SNMP → Настройки SNMP-прокси»).

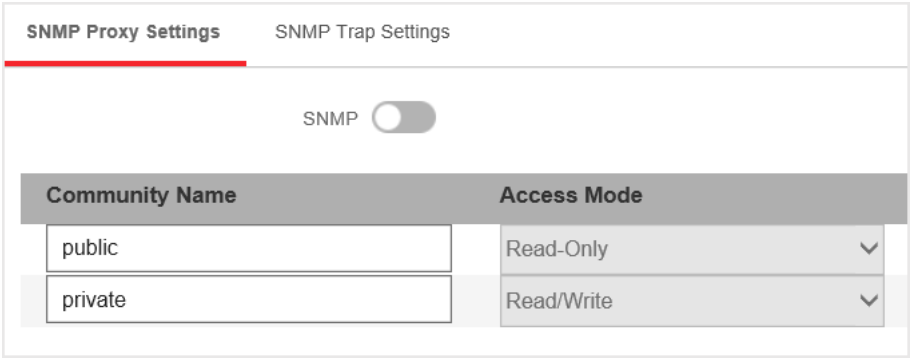


Рисунок 4-12. Настройки прокси

1) Включите **SNMP**.
2) Определите **Community Name** («Имя сообщества»).

Имя сообщества

Имя сообщества — это механизм аутентификации, аналогичный паролю, используемый для ограничения передачи данных между NMS и Agent.

- Имя сообщества **только для чтения**. Название сообщества, доступное для NMS с правами на чтение. По умолчанию — **public** («Общедоступно»).
- Имя сообщества **для чтения/записи**. Название сообщества, доступное для NMS с правами на чтение и запись. По умолчанию — **private** («Приватный режим»).

3) Нажмите **Save** («Сохранить»).

4.5.2 Настройки SNMP-ловушек

Шаги

1. Включите функцию **Trap** («Ловушка») на странице настроек SNMP-ловушек.

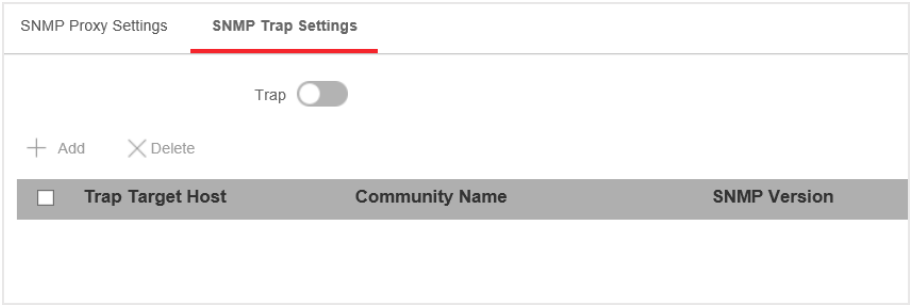


Рисунок 4-13. Настройки ловушки

2. Нажмите **Add** («Добавить»), чтобы добавить ловушку.

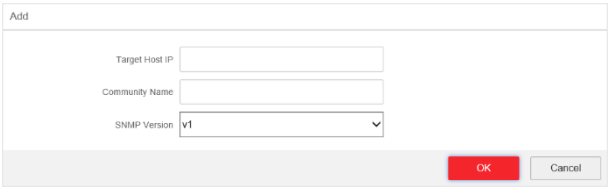


Рисунок 4-14. Добавление ловушки

Таблица 4-1. Параметры ловушки

Параметр	Описание
IP-адрес целевого хоста	IP-адрес NMS. Это не может быть широковещательный или многоадресный адрес.
Имя сообщества	Пароль, используемый для аутентификации. Можно установить до 32 байт.
Версия SNMP	Агент поддерживает протоколы SNMP версии 1 (SNMPv1) и SNMP версии 2c (SNMPv2c). **Примечание** Необходимым условием успешного соединения между NMS и Agent является совпадение версий SNMP в NMS и Agent.

3. Нажмите **OK**.
4. Нажмите **Save** («Сохранить»), чтобы добавить ловушку.
5. Опционально. Можно отметить ловушку и нажать **Delete** («Удалить»), чтобы удалить ловушку.

4.6 Настойка STP

Протокол STP (Spanning-Tree Protocol) — это протокол управления каналами связи уровня 2,

который обеспечивает избыточность путей и предотвращает образование петель в сети. Протокол STP использует алгоритм построения остовного дерева для выбора одного коммутатора в качестве корня остовного дерева. Протокол STP определяет топологию путем передачи пакетов данных протокола моста (BPDU) между устройствами. Принцип работы связующего дерева (Spanning-tree) обеспечивает стабильность сети.

4.6.1 Глобальная настройка

Шаги

1. Нажмите **Switch Configuration** → **L2 Configuration** → **STP Configuration** → **Global Configuration** («Настройка коммутатора → Настройка L2 → Настройка STP → Глобальные настройки»).
2. Нажмите **Enable STP** («Включить STP»).

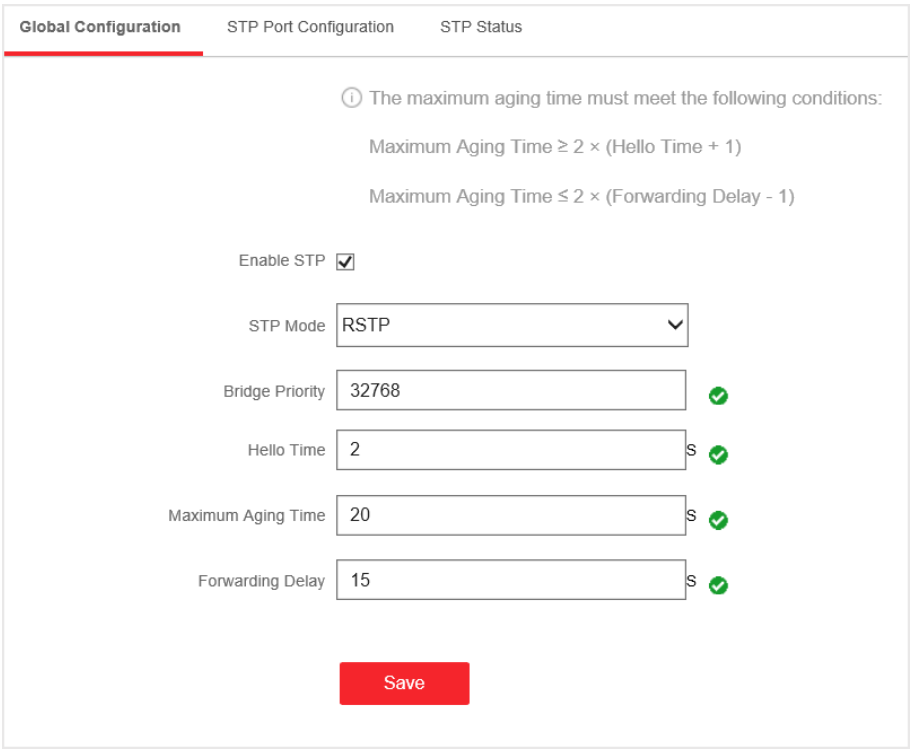


Рисунок 4-15. Глобальные настройки

3. Настройте параметры.

Таблица 4-2. Параметры STP

Параметр	Описание
Режим STP	● **STP**. Протокол остовного дерева. ● **RSTP**. Быстрый протокол остовного дерева Протокол RSTP обеспечивает более быструю сходимость остовного дерева после изменения топологии.
Приоритет моста	Чем меньше число, тем выше приоритет. Диапазон значений составляет от 0 до 61 440 секунд с шагом 4096; значение по умолчанию — 32 768. Допустимые значения: 0, 4096, 12288, 16384 ... и 61440. Коммутатор с более высоким приоритетом моста с большей вероятностью станет корневым мостом.
Время приветствия	Время между отправкой каждого BPDU-пакета на порт, используемое для диагностики состояния соединения. Диапазон от 1 до 10 секунд. По умолчанию — 2 секунды.
Максимальное время старения	Максимальное время, которое проходит до того, как порт моста сохранит информацию о конфигурации в формате BPDU. Диапазон от 6 до 40 секунд. По умолчанию — 20 секунд. **Примечание** Максимальное время старения должно соответствовать следующим условиям. ● Максимальное время старения ≥ (Время приветствия + 1) ● Максимальное время старения ≤ (Задержка пересылки - 1)
Задержка пересылки	Интервал времени состояния прослушивания и обучения при изменении топологии. Диапазон от 4 до 30 секунд. По умолчанию — 15 секунд.

4. Нажмите **Save** («Сохранить»).

4.6.2 Настройка порта STP

В случае возникновения зацикливания можно установить приоритет порта, чтобы протокол STP мог выбрать порт с наивысшим приоритетом для пересылки данных.

Шаги

1. Порт включен по умолчанию на странице **STP Port Configuration** («Настройка порта STP»).

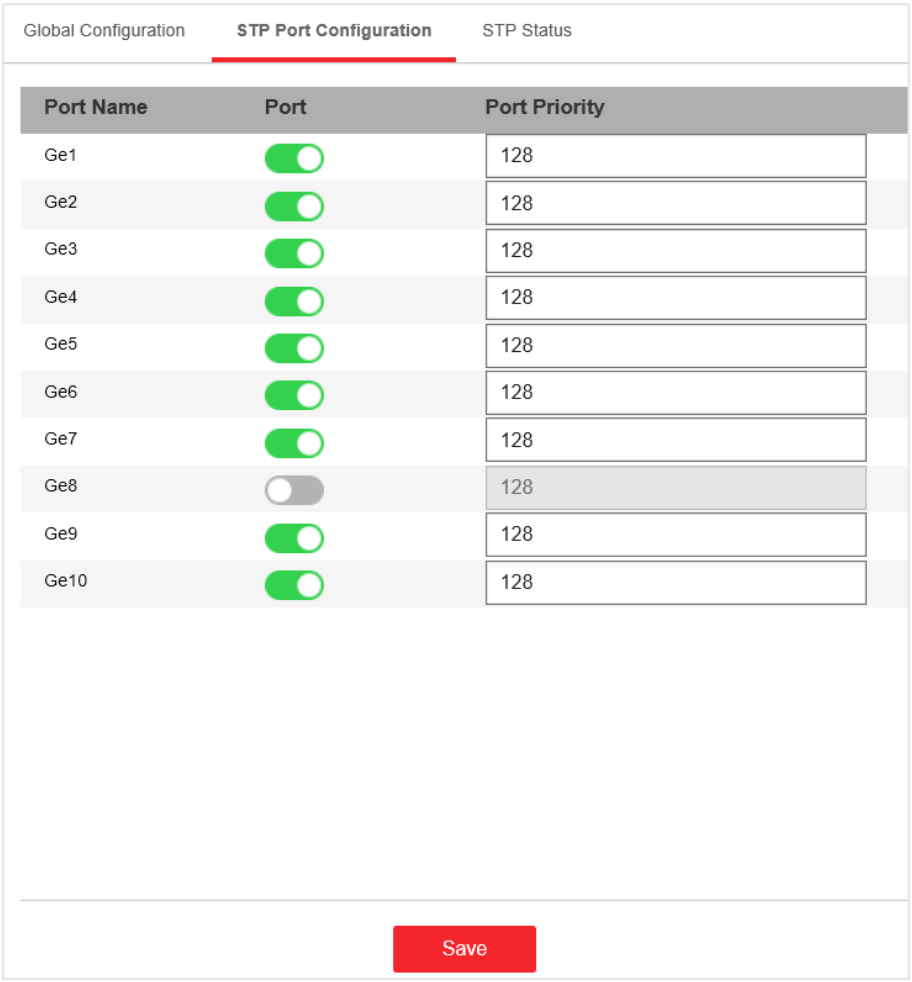


Рисунок 4-16. Приоритет порта

2. Настройте приоритет порта.

Приоритет порта

- Чем меньше число, тем выше приоритет и тем вероятнее, что порт станет корневым портом.
- Диапазон значений — от 0 до 240 с шагом увеличения 16; значение по умолчанию — 128. Допустимые значения: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 и 240.

Примечание

Если приоритеты портов одинаковы, протокол STP использует идентификатор порта для выбора порта в качестве корневого.

3. Нажмите **Save** («Сохранить»).

4.6.3 Просмотр состояния STP

Можно проверить глобальное состояние настроек STP и состояние каждого порта. Нажмите **Switch Configuration** → **L2 Configuration** → **STP Configuration** → **STP Status** («Настройка коммутатора → Настройка L2 → Настройка STP → Состояние STP»).

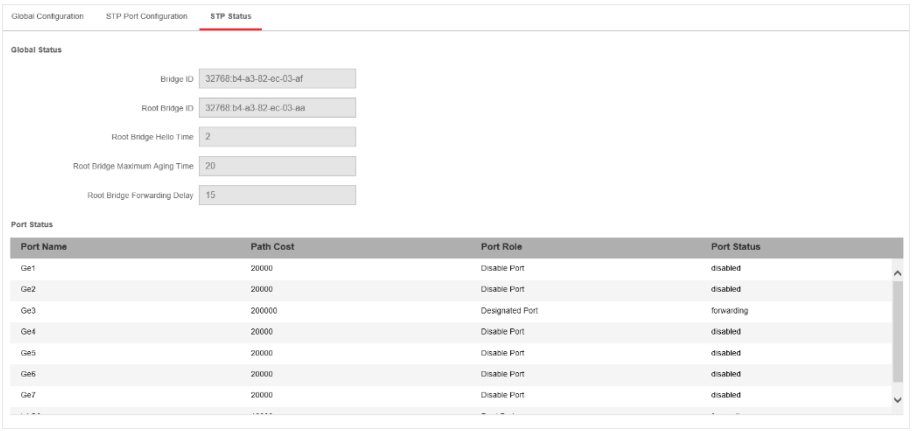


Рисунок 4-17. Состояние STP

4.7 Управление PoE

Настройки PoE

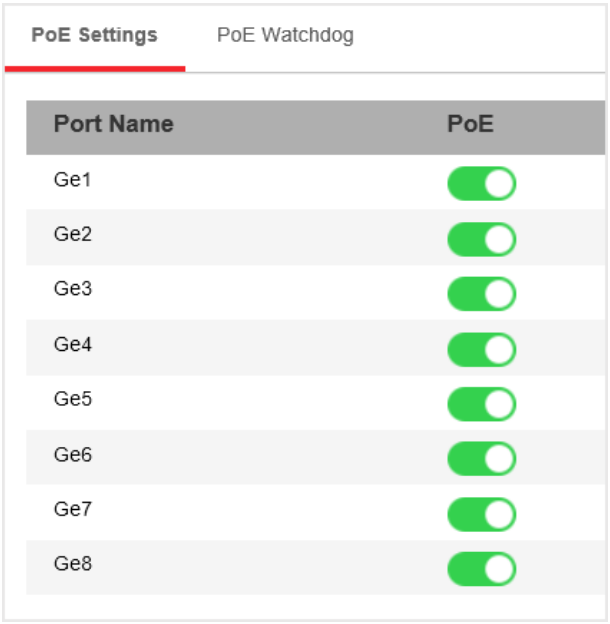


Рисунок 4-18. Настройки PoE

Позволяет использовать PoE для подачи питания на питаемые устройства.

Примечание

Включение или отключение PoE не влияет на передачу данных через порт.

Функция PoE-сторожевого таймера



Рисунок 4-19. Сторожевой таймер PoE

Можно включить сторожевой таймер PoE для автоматического обнаружения и перезапуска камер, которые не отвечают.

Раздел 5 Управление системой

5.1 Синхронизация времени

Шаги

1. Перейдите в **System Settings** → **Time Settings** («Системные настройки → Настройки времени»). Можно просмотреть время устройства.

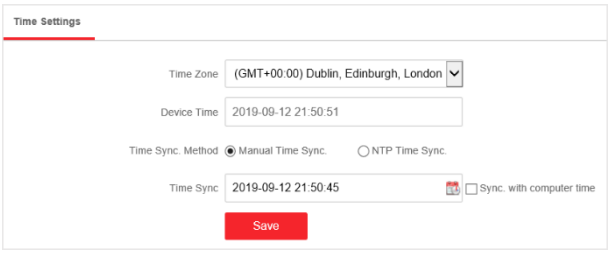


Рисунок 5-1. Настройки времени

2. Выберите **Time Zone** («Часовой пояс»).
3. Выберите **Time Sync** («Синхронизация времени»)**. Метод**
4. Настройка режима синхронизации времени.
   – **Синхронизация времени вручную.** Нажмите или нажмите **Sync. with computer time** («Синхронизировать со временем компьютера»), чтобы синхронизировать время устройства.

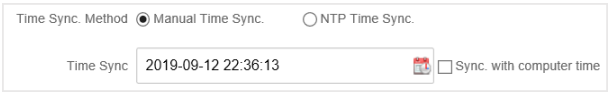


Рисунок 5-2. Синхронизация вручную

   – **Синхронизация времени с NTP-сервером.** Введите адрес NTP-сервера и установите интервал синхронизации времени.

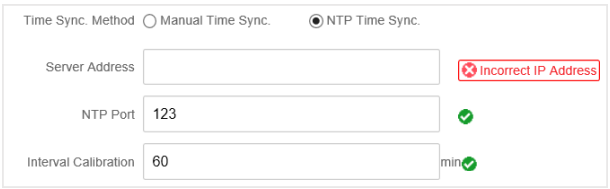


Рисунок 5-3. Синхронизация с NTP-сервером

5. Нажмите **Save** («Сохранить»).

5.2 Эксплуатация устройства

Если устройство работает со сбоями или некорректно, перейдите в раздел **System Management** → **System Maintenance** → **Device Operation** («Управление системой →

Обслуживание системы → Эксплуатация устройства»), чтобы перезапустить или восстановить работу устройства.

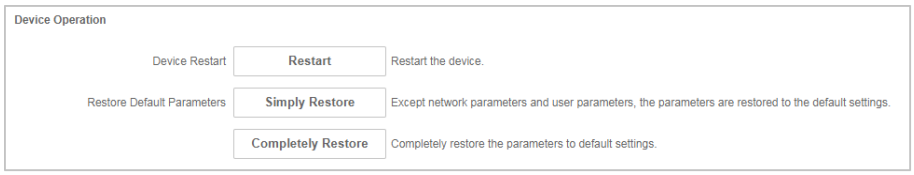


Рисунок 5-4. Эксплуатация устройства

Примечание

После перезагрузки или восстановления коммутатора страница входа в систему будет открываться автоматически.

Перезагрузка

Нажмите **Restart** («Перезапустить»), чтобы удаленно перезапустить коммутатор.

Восстановить

- **Простое восстановление.** За исключением конфигурации сети и пользовательских параметров, все остальные параметры восстанавливаются до значений по умолчанию.
- **Полное восстановление.** Полное восстановление параметров до значений по умолчанию.

Предостережение

После возврата устройства к заводским настройкам восстановить параметры невозможно.

5.3 Экспорт файла конфигурации

Можно экспортировать файл конфигурации для локального резервного копирования.

Шаги

1. Перейдите в раздел **System Management** → **System Maintenance** → **Export & Import** («Управление системой → Обслуживание системы → Экспорт и импорт»).
2. Нажмите **Export** («Экспорт»).
3. Установите пароль для экспортированного файла конфигурации.

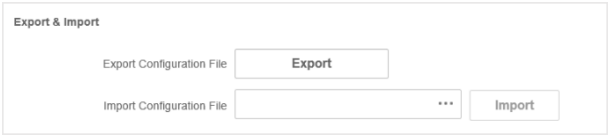


Рисунок 5-5. Экспорт файла конфигурации

Примечание

Для импорта файлов конфигурации требуется пароль.

4. Нажмите **OK**.

5.4 Импорт файла конфигурации

Можно импортировать файл конфигурации для простой настройки системы.

Шаги

1. Перейдите в раздел **System Management** → **System Maintenance** → **Export & Import** («Управление системой → Обслуживание системы → Экспорт и импорт»).

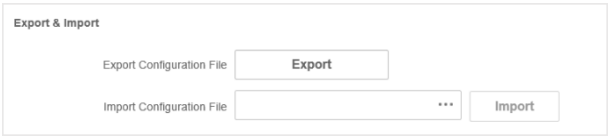


Рисунок 5-6. Импорт файла конфигурации

2. Нажмите ⋯, чтобы выбрать файл конфигурации.
3. Нажмите **Import** («Импорт»).
   После импорта файла конфигурации устройство автоматически перезагрузится и перейдет на страницу входа в систему.

5.5 Обновление устройства

Можно загрузить файл обновления для обновления коммутатора.

Шаги

1. Перейдите в раздел **System Management** → **System Maintenance** → **Device Upgrade** («Управление системой → Обслуживание системы → Обновление устройства»).

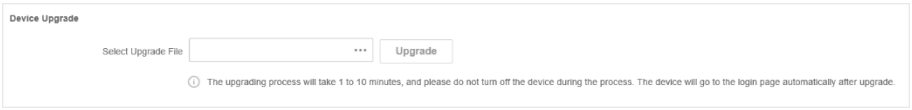


Рисунок 5-7. Обновление

2. Нажмите ⋯, чтобы выбрать патч обновления.
3. Нажмите **Upgrade** («Обновление»).

Примечание

Если обновление не удалось или устройство не работает, обратитесь к инженерам технической поддержки.

Результат

После завершения обновления устройство автоматически перезагрузится и перейдет на страницу входа в систему.

5.6 Управление журналом

Журналы работы системы можно просматривать и экспортировать для резервного копирования.

Шаги

1. Нажмите **System Management** → **Log Management** («Управление системой → Управление журналами»).

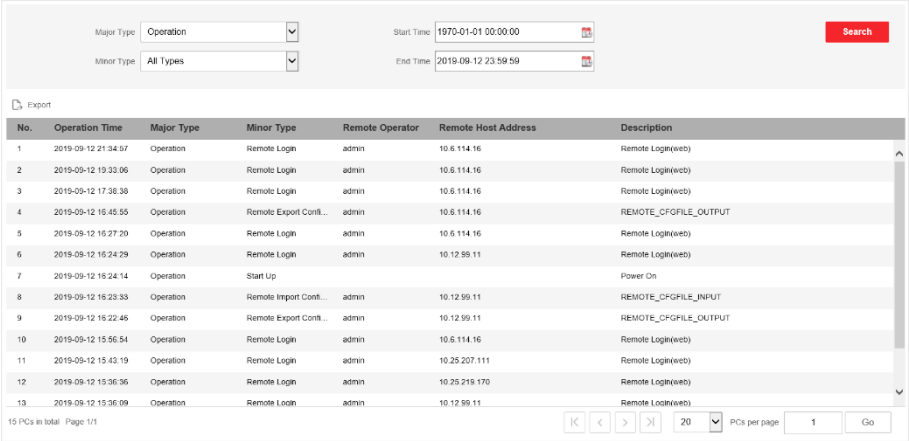


Рисунок 5-8. Управление журналами

2. Задайте условия поиска: включая **Major Type** («Тип»), **Minor Type** («Подтип»), **Start Time** («Время начала») и **End Time** («Время окончания»).
3. Нажмите **Search** («Поиск»).

Примечание

В результате поиска может отображаться максимум 2000 результатов. Если результатов поиска слишком много, сузьте область поиска.

4. Опционально. Нажмите **Export** («Экспорт»), чтобы экспортировать все результаты поиска.

Примечание

Журналы можно экспортировать в Excel. После успешного экспорта журналов появится всплывающее окно с подсказкой.

5.7 Диагностика сети

Благодаря средствам сетевой диагностики инженеры могут быстро обнаруживать сетевые

сбои.

Шаги

1. Перейдите в раздел **System Management** → **System Tools** → **Network Diagnostics** («Управление системой → Системные инструменты → Сетевая диагностика»).

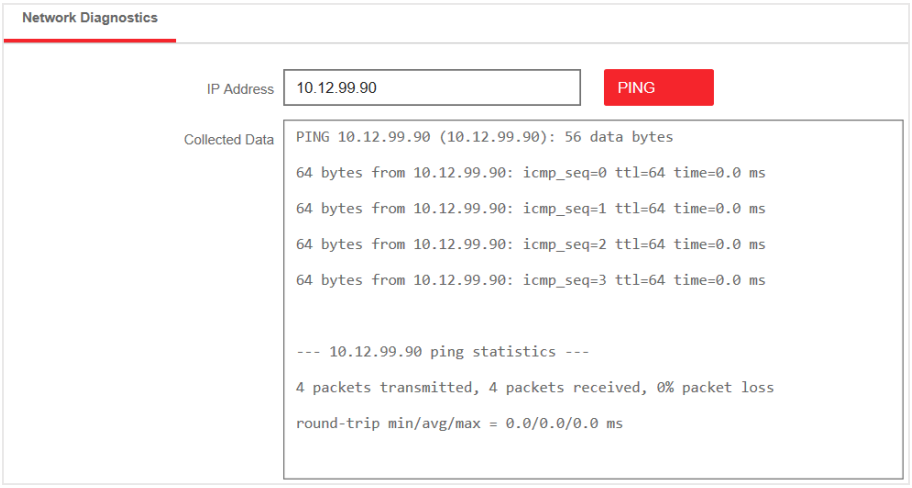


Рисунок 5-9. Диагностика сети

2. Введите IP-адрес сервера и нажмите **PING**.

5.8 Управление пользователями

Регулярно меняйте пароль для повышения безопасности устройства.

Шаги

1. Нажмите **System Management** → **User Management** («Управление системой → Управление пользователями»).
2. Нажмите **Edit** («Редактировать»).

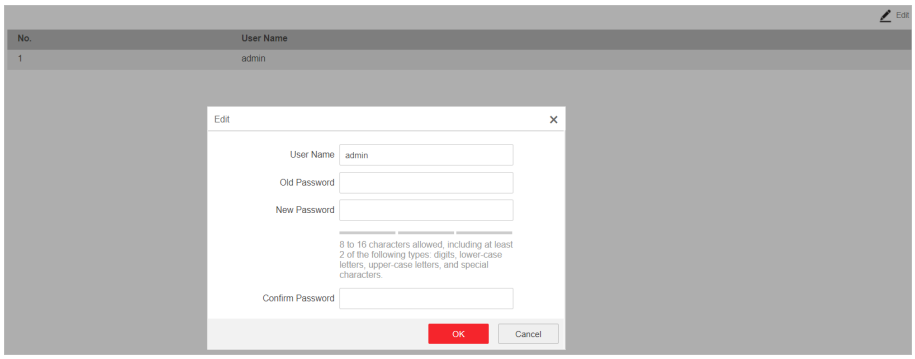


Рисунок 5-10. Управление пользователями

3. Введите старый пароль.
4. Создайте новый пароль и подтвердите его.
5. Нажмите **OK**.

5.9 Управление безопасностью

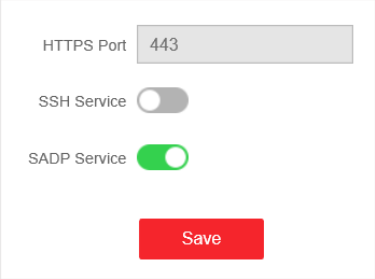


Рисунок 5-11. Управление безопасность

SSH

Устройство поддерживает службу безопасности SSH. SSH может предотвратить утечку информации при удаленном управлении устройством. По умолчанию функция SSH отключена.

Примечание

Имя пользователя для SSH — root, а пароль — это пароль для входа в устройство.

SADP

После включения SADP можно активировать устройство, изменить пароль и сетевую информацию и т. д. SADP включен по умолчанию.


FLOW