ROXTON

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

ВЕРСИЯ **1.0**

УПРАВЛЯЕМЫЙ СЕТЕВОЙ КОММУТАТОР:

- ROXTON **MNS-1008F2S**
- ROXTON **MNS-1008F2SP**
- ROXTON **MNS-1008S2G**

ИНСТРУКЦИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

1. Внимательно ознакомьтесь с данным руководством по эксплуатации.
2. Сохраните данное руководство по эксплуатации для дальнейшего использования.
3. Выполняйте все инструкции и указания данного руководства по эксплуатации.
4. Коммутатор и его части не должны подвергаться воздействию воды (брызгам, каплям и т.п.).
5. Коммутатор запрещается устанавливать вблизи негерметичных емкостей с жидкостью (вазы, чашки и т.п.), источников тепла (радиаторов, каминов и т.п.), а также под воздействием прямых солнечных лучей или открытого огня.
6. Коммутатор и его части не должны соприкасаться с горячими поверхностями или острыми предметами.
7. Коммутатор и его части можно протирать только сухой тканью, предварительно отключив его от сети питания.
8. Запрещается использовать неисправный коммутатор, в том числе с поврежденным блоком питания.
9. Запрещается помещать посторонние предметы коммутатор.
10. Отключайте коммутатор от сети питания во время грозы или когда он не используется в течение длительного периода времени.
11. Запрещается самостоятельно открывать или разбирать коммутатор, а также вносить изменения в его составные части и конструкцию.
12. Запрещается подключать к коммутатору неисправные приборы системы СОУЭ.
13. В случае хранения или транспортировки коммутатора при отрицательных температурах, перед эксплуатацией его следует выдержать в комнатной температуре не менее 4-х часов.

1. ОГЛАВЛЕНИЕ

2. ВВЕДЕНИЕ

Благодарим Вас за покупку коммутатора ROXTON. Пожалуйста, внимательно ознакомьтесь с данным руководством и следуйте инструкциям по распаковке, подключению, настройке и эксплуатации коммутатора. Это позволит правильно использовать все функции устройства и продлит срок его службы.

Данное руководство по эксплуатации не включает в себя все варианты внешнего вида и комплектации, а также не описывает все возможные ситуации, которые могут возникнуть в ходе его распаковки, установки, настройки и эксплуатации.

Производитель оставляет за собой право изменять комплектацию, характеристики и внешний вид коммутатора без предупреждения.

Обозначения, используемые в данном руководстве по эксплуатации:

ВНИМАНИЕ!
Указания, выделенные данным знаком, являются обязательными для исполнения. Их несоблюдение влечет к преждевременному прекращению гарантийных обязательств производителя (продавца или импортёра) в отношении коммутатора.

Всю информацию об оборудовании
ROXTON вы всегда можете найти
на официальном сайте
WWW.ROXTON.RU

3. ВОЗМОЖНОСТИ

Серия управляемых коммутаторов ROXTON представляет собой оптимальное решения для объединения устройств ROXTON IP между собой в общую сеть. Принцип работы коммутатора основан на переключении сетевого трафика между 10-портами. Особенности изделия:

- Возможность установки на DIN-рейке
- 8 высокоскоростных 1 Гбит/с портов RJ-45
- 2 порта 1 Гбит/с для подключения оптических SFP-модулей
- Порт CONSOLE для подключения к ПК через кабель переходник
- Модель ROXTON MNS-1008F2SP обеспечивает питание по PoE до 30 Вт на каждый порт RJ-45 и 240 Вт на все порты суммарно
- Модель ROXTON MNS-1008S2G снабжена портами 12xSFP и 2xRJ45

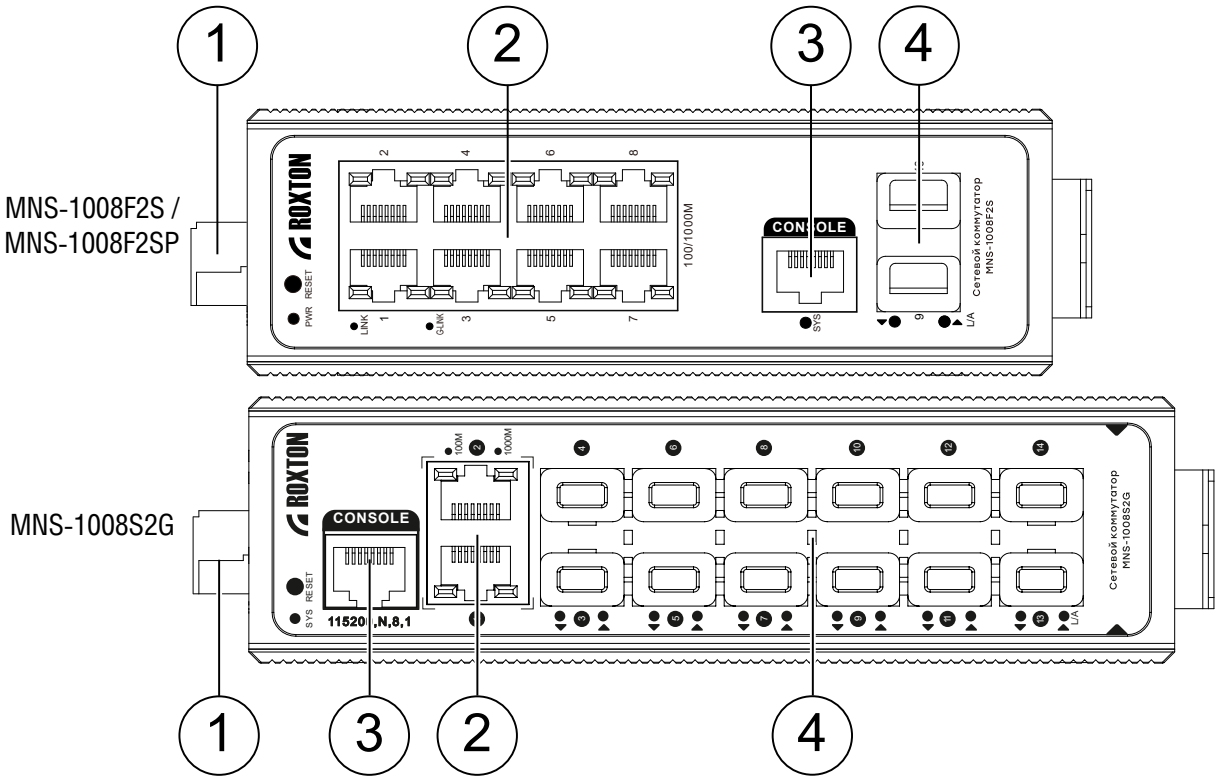
4. КОМПЛЕКТ ПОСТАВКИ

В комплект поставки коммутатора входят:
- Коммутатор (без БП[1]) — 1 шт.
- Кабель-переходник RS-232 – 1 шт.

1 Блок питания DC приобретается отдельно

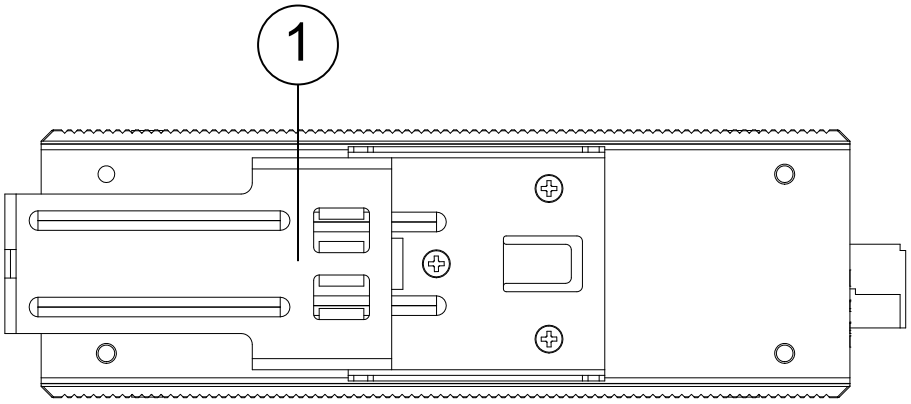
5. ОПИСАНИЕ И ВНЕШНИЙ ВИД КОММУТАТОРА

5.1 ПЕРЕДНЯЯ ПАНЕЛЬ



1. **Клемма питания Phoenix** — ввод основного и резервного питания
2. **Порты RJ-45** — основные порты подключения. 1Гбит/с. Модель ROXTON MNS-1008F2SP обеспечивает питание по PoE до 30 Вт на каждый порт RJ45 и 240 Вт на все порты суммарно
3. **Порт Console** — порт настройки для подключения к ПК через кабель переходник RJ45 - COM/RS232
4. **Оптические порты** — подключение SFP модулей. 1Гбит/с

5.2 ЗАДНЯЯ ПАНЕЛЬ



1. **Кронштейн крепления** — установка на DIN-рейку

5.3 СВЕТОВАЯ ИНДИКАЦИЯ СОСТОЯНИЙ КОММУТАТОРА

Режимы работы портов Ethernet индицируются на светодиодах, расположенных непосредственно на разъемах RJ45. Состояние питания коммутатора индицируется на светодиодах, расположенных на передней панели. Назначение и режимы свечения светодиодов описаны в таблицах **5.3.1** и **5.3.2**

ЦВЕТ СВЕТОДИОДА	НАЗНАЧЕНИЕ	ОПИСАНИЕ
PWR (зелёный)	Состояние ввода питания	Включен постоянно – питание включено Выключен – питание отсутствует
LINK (жёлтый)	Наличие соединения по витой паре/передача данных (LNK/ACT)	Выключен – нет соединения Включен постоянно – соединение установлено Мигает – идет передача данных
PoE* (зелёный)	Состояние PoE	Мигает – функционирует

*только для модели MNS-1008F2SP

Таблица 5.3.1 Назначение светодиодных индикаторов на передней панели

ЦВЕТ СВЕТОДИОДА	НАЗНАЧЕНИЕ	ОПИСАНИЕ
Жёлтый	Наличие соединения по витой паре/передача данных (LNK/ACT)	Выключен – нет соединения Включен постоянно – соединение установлено Мигает – идет передача данных
Зелёный	Скорость соединения	Включен – 1 Гбит/с

Таблица 5.3.2 Назначение светодиодных индикаторов портов Ethernet

6. РАСПАКОВКА

Пожалуйста, распакуйте и осмотрите коммутатор на предмет повреждений полученных в ходе транспортировки. Проверьте соответствие комплекта поставки перечню предметов указанному в руководстве пользователя. При обнаружении повреждений или недостающих предметов незамедлительно свяжитесь с продавцом.

Не выбрасывайте упаковку до выяснения обстоятельств порчи оборудования. Рекомендуется сохранить заводскую упаковку на случай повторной транспортировки.

7. УСТАНОВКА КОММУТАТОРА

Коммутатор предназначен для установки на DIN-рейку, либо на горизонтальную поверхность. В заводской поставке на коммутатор установлен кронштейн, предназначенный для монтажа на DIN-рейку. Для установки коммутатора в 19'' телекоммуникационную стойку или шкаф следует воспользоваться устанавливаемой отдельно DIN-рейкой.
При установке прибора убедитесь, что рядом с местом установки прибора отсутствуют нагревательные приборы, источники влаги и агрессивных сред.

Независимо от места установки, следует оставить не менее 40 мм свободного пространства над коммутатором, не менее 30 мм позади и 10 мм по бокам.

8. ПОДКЛЮЧЕНИЕ ВНЕШНИХ УСТРОЙСТВ

Для подключения к портам Ethernet следует использовать кабель «витая пара» категории 5 или 5e (CAT5 или CAT5e). Допускается использование как экранированного, так и неэкранированного кабеля. Кабель подсоединяется к разъемам RJ45 коммутатора с помощью стандартного штекера 8P8C, при этом не имеет значения, по какой схеме обжат кабель – прямой или перекрестной (crossover). В коммутаторе реализована функция автоматического определения направления передачи (auto MDI/MDI-X).

Для подключения коммутатора к волоконно-оптическим линиями связи используются SFP-порты. Подключение к SFP-порту осуществляется при помощи оптических трансиверов ROXTON SFP-SM1LC1310-T и ROXTON SFP-SM1LC1550-R (используются в паре, поставляются отдельно). Использование подключения волоконно-оптическими линиями позволяет связать коммутаторы на расстоянии до 20 км.

Допускается использование монтажных устройств (шкафов, боксов и т.п.). При смежном расположении блоков расстояние между ними по вертикали и горизонтали должно быть не менее 10 мм.

9. ПОДКЛЮЧЕНИЕ ПИТАНИЯ

Подключение питания осуществляется через блок питания (поставляется отдельно). Распиновка клеммы и описание схемы подключения указаны на **рисунке 9** и **таблице 9.**

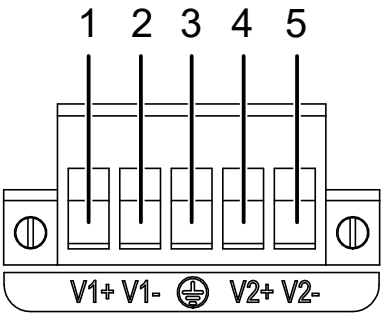


Рисунок 9 Распиновка клеммы питания

НОМЕР КОНТАКТА	ФУНКЦИЯ	ОПИСАНИЕ	
		MNS-1008F2S/MNS-1008S2G	MNS-1008F2SP (POE)
1	V1+	Подключение клеммы «+» внешнего источника питания DC 12 В - 48 В	Подключение клеммы «+» внешнего источника питания DC 48 В - 57 В
2	V1-	Подключение клеммы «-» внешнего источника питания DC 12 В - 48 В	Подключение клеммы «-» внешнего источника питания DC 48 В - 57 В
3	GND	Подключение заземления	Подключение заземления
4	V2+	Подключение клеммы «+» резервного источника питания DC 12 В - 48 В	Подключение клеммы «+» резервного источника питания DC 48 В - 57 В
5	V2-	Подключение клеммы «-» резервного источника питания DC 12 В - 48 В	Подключение клеммы «-» резервного источника питания DC 48 В - 57 В

Таблица 9 Описание клеммы подключения питания

10. НАСТРОЙКА КОММУТАТОРА

Коммутатор является управляемым. При заводских настройках устройство коммутирует трафик между всеми портами. Для настройки дополнительных функций, необходимо подключить и настроить коммутатор через ПК.

10.1 ПОДКЛЮЧЕНИЕ И НАСТРОЙКА КОММУТАТОРА

Для подключения к коммутатору устройства должны быть подключены к одной сети.

По умолчанию коммутатор имеет сетевой адрес 192.168.2.1 и маску подсети 255.255.255.0

В настройках сетевой карты ПК установите вручную настройки IP-адреса для TCP/IPv4 (192.168.2.2-254) как показано на **рисунке 10.1**.

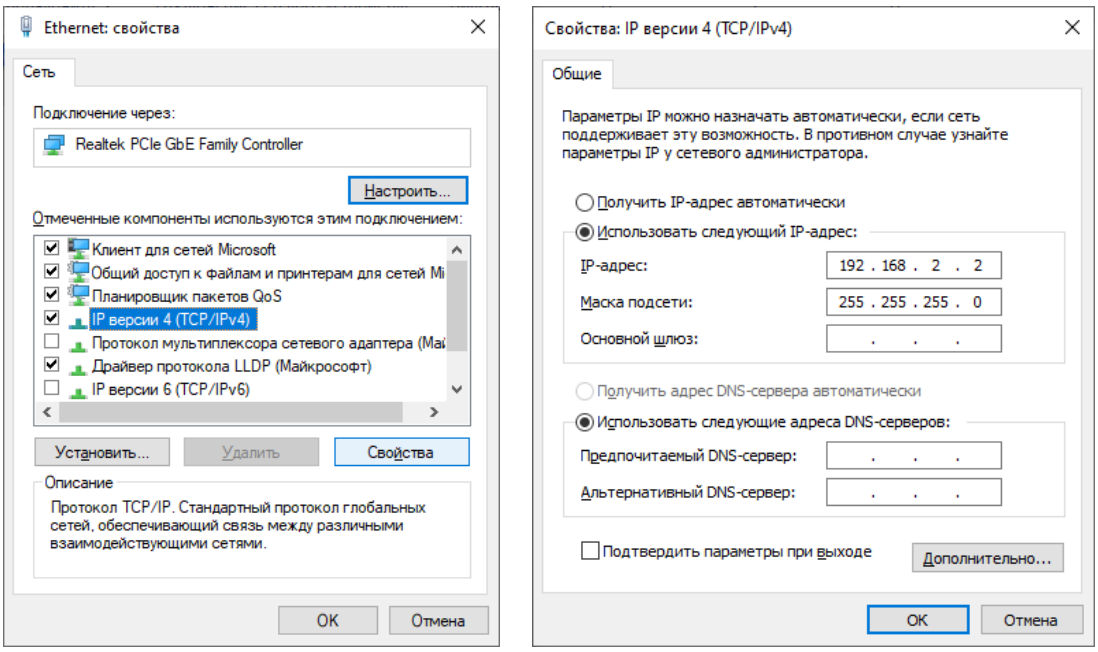
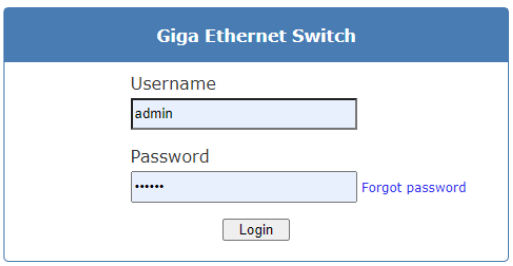


Рисунок 10.1 Настройка TCP/IPv4

Для входа в вэб-интерфейс воспользуйтесь браузером на компьютере.
В адресной строке браузера введите **http://192.168.2.1/en/index.htm** или **http://192.168.2.1** и пройдете авторизацию.



Логин и пароль учетной записи администратора указан на этикетке коммутатора.

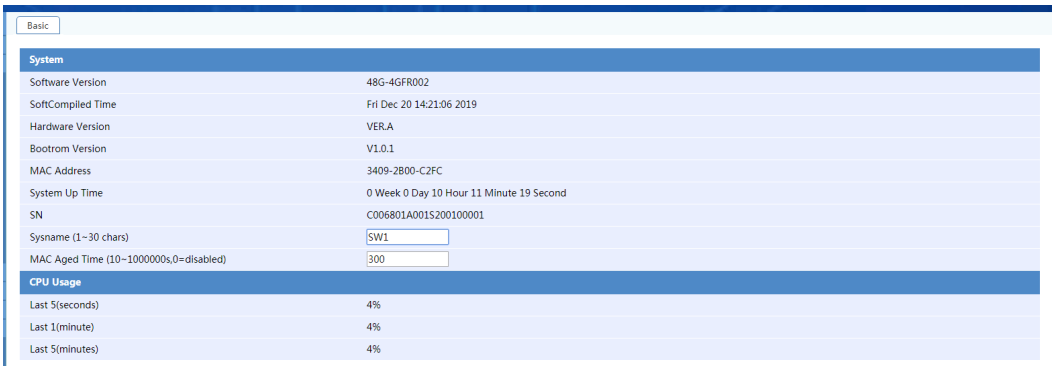
ВНИМАНИЕ!
Для обеспечения безопасности соединения следует изменить стандартный пароль в настройках коммутатора.

10.2 СТРАНИЦА ВЕБ-КОНФИГУРАЦИИ

10.2.1 Управление устройством

10.2.1.1 Системная информация

После входа в веб-интерфейс появляется страница информации о системе. Перейдите по пути «Device Overview» или «Device» → «Basic», чтобы просмотреть информацию о системе коммутатора. На данной странице возможно просмотреть MAC-адрес устройства, версию программного обеспечения, серийный номер и т. д. На странице информации о системе измените имя устройства (по умолчанию 8G-2GF), время устаревания MAC-адреса (по умолчанию 300 секунд).



Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Версия ПО/Аппаратная версия/ Версия загрузчика	Отображение номера версии, номера версии аппаратного обеспечения и номера версии загрузчика текущего программного обеспечения коммутатора
MAC-адрес	Отображение MAC-адреса коммутатора
Время работы	Отображение времени непрерывной работы коммутатора с момента включения
Имя системы	Возможна настройка имени устройства
Время устаревания MAC-адреса	Настройка время устаревания записей динамических MAC-адресов, по умолчанию 300 секунд

10.2.1.2 Техническое обслуживание оборудования

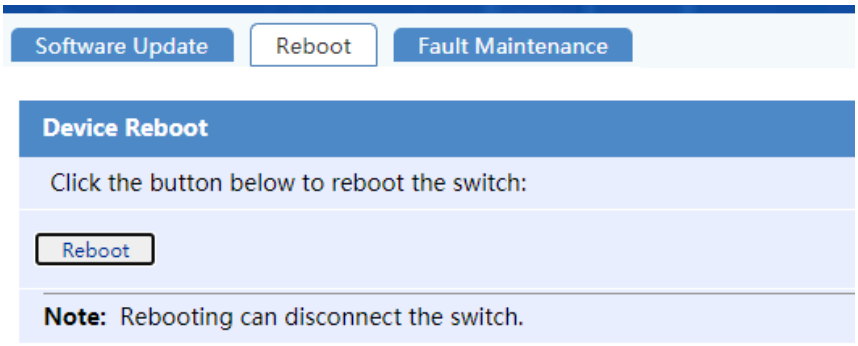
Техническое обслуживание оборудования включает в себя обновление программного обеспечения оборудования, перезапуск и устранение неисправностей.

10.2.1.2.1 Обновление программного обеспечения

Перейдите в меню: Device → Maintenance → Software upgrade, страница показана на рисунке ниже. Обновите программное обеспечение коммутатора до последней версии, что сделает ваше устройство более стабильным и функциональным (нажмите кнопку <Choose File...>, выберите файл последней версии и нажмите кнопку <Apply>, чтобы начать обновление)

10.2.1.2.2 Перезапуск устройства

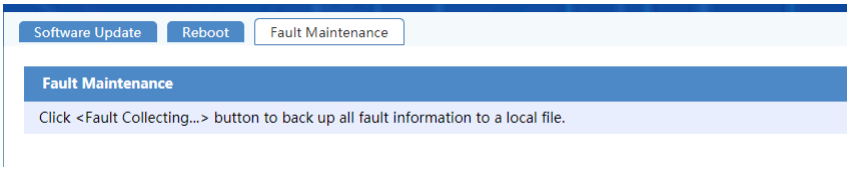
Перейдите в меню: Device → Maintenance → Reboot, страница показана на рисунке ниже. Нажмите кнопку <Reboot> для перезапуска



Перед перезапуском устройства сохраните текущую конфигурацию. В противном случае после перезапуска несохраненная информация о конфигурации будет утеряна.

10.2.1.2.3 Устранение неисправностей

Перейдите в меню: Device → Maintenance → Fault Maintenance, страница показана ниже. Нажмите кнопку <Fault Collection...>, и вся информация об устранении неисправностей будет сохранена на вашем ПК.

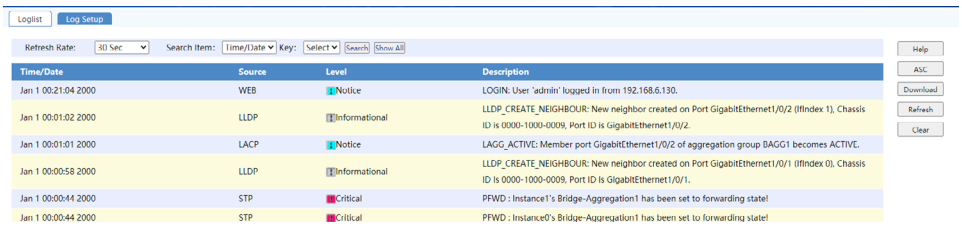


10.2.1.3 Управление журналом

Системный журнал записывает информацию об оборудовании, программном обеспечении и системных проблемах в системе. Он также может отслеживать события, происходящие в системе, предоставляя сетевым администраторам поддержку для мониторинга работы сети и диагностики сетевых сбоев.

10.2.1.3.1 Журнал учета

Перейдите в меню: Device → Syslog → Loglist, страница показана на рисунке ниже.

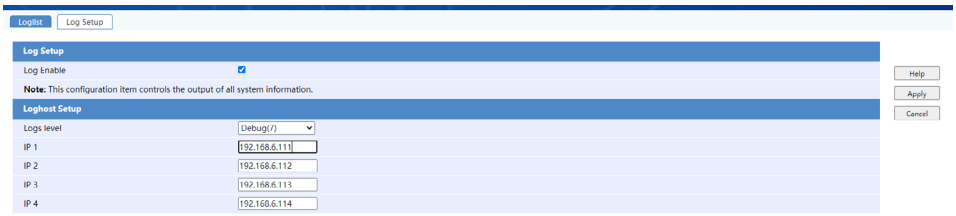


Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Частота обновления	Настройка частоты обновления страницы. Выберите значение в раскрывающемся списке «Refresh Rate»
Элемент запроса	Запросить информацию журнала, которую необходимо выполнить, выбрав раскрывающийся список «Query Item»
Отображение прямой последовательности	Информация журнала отображается в порядке от первого до последнего. Обратный дисплей противоположен
Скачивание журнала	Нажмите кнопку < Download >, чтобы сохранить всю информацию журнала на локальном компьютере
Обновление	Нажмите кнопку < Refresh >, чтобы вручную обновить информацию журнала
Очистка	Нажмите кнопку < Clear >, чтобы удалить всю информацию журнала

10.2.1.3.2 Настройки журнала

Перейдите в меню: Device → Syslog → Log Setup, страница показана на рисунке ниже.



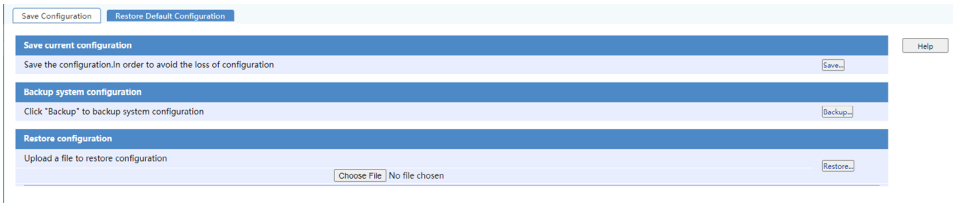
Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Управление журналом учета	Открыть/закрыть информационный центр. По умолчанию информационный центр включен
Отправить уровень журнала	На хост журнала может быть отправлена только информация журнала не выше указанного уровня
IP хоста журнала	Установите IP-адрес хоста журнала

10.2.1.4 Управление конфигурацией

10.2.1.4.1 Сохранение конфигурации

Перейдите в меню: Device → Configuration → Save configuration, страница показана на рисунке ниже.



Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Сохранить текущую конфигурацию	Для сохранения конфигурации нажмите кнопку < Save...>, текущего устройства
Информация о конфигурации системы резервного копирования	Нажмите кнопку < Backup...> и выберите путь резервного копирования файла конфигурации. Можно сохранить текущую конфигурацию устройства на свой компьютер, чтобы использовать этот файл (*.cfg) для восстановления конфигурации в будущем
Восстановить информацию о конфигурации из файла	Нажмите кнопку < Browse..>, выберите ранее сохраненный файл (*.cfg), нажмите <Восстановить Кнопкой «Restore...», после подтверждения можно восстановить предыдущую конфигурацию устройства (после автоматического перезапуска устройства конфигурация вступает в силу)

После настройки всех элементов на странице конфигурации, обязательно сохраните конфигурацию, иначе несохраненная информация о конфигурации будет утеряна из-за перезапуска и других операций.

10.2.1.4.2 Восстановление конфигурации по умолчанию

Перейдите в меню: Device → Configuration → Restore Default Configuration, страница показана на рисунке ниже.

ВНИМАНИЕ!

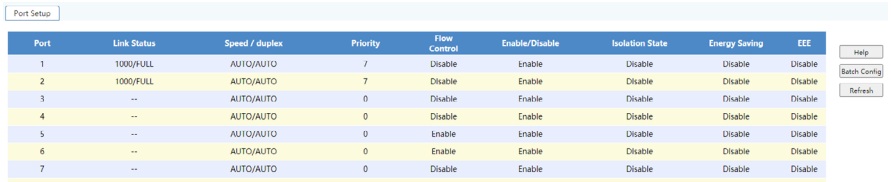
В процессе восстановления заводской конфигурации по умолчанию не выполняйте другие операции с устройством, в противном случае устройство может выйти из строя.

Значение ключевых элементов на странице показано в таблице ниже.

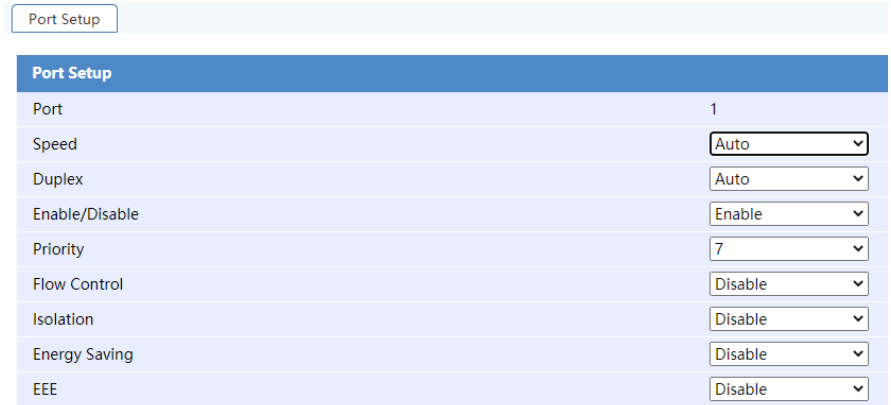
ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Restore factory default configuration (retain IP)	Нажмите данную кнопку, чтобы продолжить использовать текущий IP-адрес для входа на устройство для настройки и управления
Restore factory default configuration	Нажмите данную кнопку, если вам нужно использовать IP-адрес по умолчанию для входа на устройство для настройки и управления

10.2.1.5 Управление портом / Настройки порта

Перейдите в меню: Device → Port Management → Port Setup, на странице настроек порта отобразится текущий статус атрибута порта, страница показана на рисунке ниже.



Настройте свойства указанных портов пакетами (нажмите кнопку < Batch Configuration > на главной странице, чтобы перейти на соответствующую страницу конфигурации).
Настройка свойств одного порта (щелкните запись, соответствующую порту на главной странице, чтобы перейти на соответствующую страницу конфигурации).



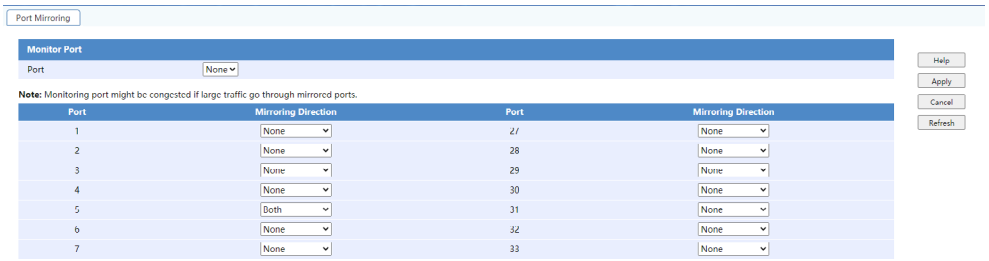
Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Speed	Настроить скорость порта
Duplex	В дуплексном режиме порта возможны три ситуации: • Если вы хотите, чтобы порт принимал пакеты во время отправки пакетов, настройте порт как полнодуплексный (Full) атрибут • Если вы хотите, чтобы порт одновременно отправлял или получал пакеты, настройте порт на атрибут полудуплекса (Half). • При настройке порта в состояние автосогласования (Auto), дуплексное состояние порта определяется автосогласованием между локальным портом и одноранговым портом. По умолчанию скорость и дуплексный режим порта — (Auto) автосогласование.
Enable/Disable	Включить/выключить порт. Если порт отображается закрытым, он не может пересылать данные. По умолчанию порт открыт
Priority	Уровень приоритета порта составляет от 0 до 7, где 0 — самый низкий, а 7 — самый высокий. Для пакетов без заголовка метки 802.1Q коммутатор будет использовать приоритет порта в качестве приоритета 802.1p для порта для получения пакетов, а затем искать таблицу сопоставления локальных приоритетов на основе приоритета, чтобы пометить пакет как локальный. приоритет По умолчанию приоритет порта равен 0.
Flow Control	Включите или выключите функцию управления потоком порта. Если функция управления потоком включена, когда устройство перегружено, оно отправит сообщение одноранговому коммутатору, чтобы уведомить одноранговый коммутатор о необходимости временно прекратить отправку пакетов или снизить скорость отправки пакетов, тем самым избегая потери пакетов и обеспечение нормальной работы сетевого сервиса. По умолчанию управление потоком портов отключено.
Isolation	С помощью функции изоляции портов можно добавить порты, которыми необходимо управлять, в группу изоляции («open» означает присоединиться к группе изоляции; «close» означает выйти из группы изоляции), чтобы получить данные уровня 2 между портами в группе изоляции. Изоляция не только повышает безопасность сети, но и предоставляет пользователям гибкие сетевые решения. По умолчанию порт не добавляется в группу изоляции.
Energy saving	Включите или выключите функцию энергосбережения порта в нерабочем состоянии. По умолчанию функция отключена
EEE	Включите или выключите функцию энергосбережения EEE (Energy Efficient Ethernet) порта. По умолчанию функция энергосбережения EEE выключена

10.2.1.6 Зеркалирование портов

Зеркальное отображение портов заключается в копировании пакетов зеркального порта на порт мониторинга. Порт мониторинга подключен к устройству обнаружения данных. Пользователи используют эти устройства обнаружения данных для анализа пакетов, скопированных на порт мониторинга, для мониторинга сети и устранения неполадок.
Коммутатор обеспечивает зеркальное отображение локального порта, то есть зеркальный порт и порт мониторинга находятся на одном устройстве.

Перейдите в меню: Device → Port Mirroring, нажмите кнопку < No Mirror >, чтобы быстро настроить порт мониторинга на «None» и настроить направление зеркалирования всех портов на «No Mirroring».



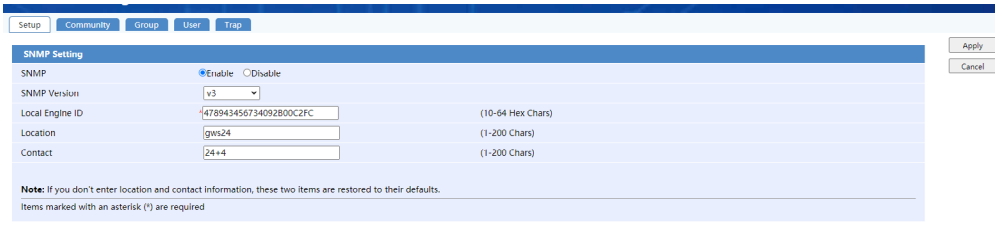
Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Monitoring port	Выберите порт мониторинга, «None» означает, что функция зеркалирования портов коммутатора отключена
Mirroring direction	Выберите зеркальный порт, «None» означает, что порт не зеркальный Смысл направления зеркального отражения следующий: • InBound (Зеркальный входящий порт): только пакеты, полученные портом, дублируются на порт мониторинга. • OutBound (Зеркальный выходной порт): только пакеты, отправленные этим портом, дублируются на порт мониторинга. • Both (Зеркалирование входящих и исходящих портов): пакеты, входящие и исходящие из этого порта, дублируются на порт мониторинга.

10.2.1.7 SNMP

10.2.1.7.1 Настройки SNMP

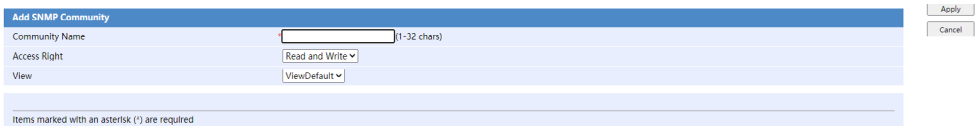
Перейдите в меню: Device → SNMP → Setup, на этой странице можно настроить включение функции SNMP, версию SNMP, идентификатор локального ядра, информацию о физическом местоположении, контактную информацию.



10.2.1.7.2 Настройки SNMP

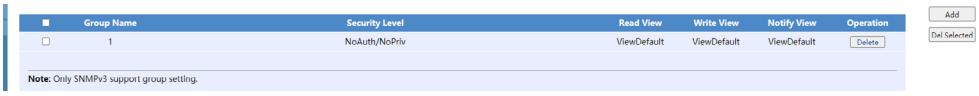
Перейдите в меню: Device → SNMP → Community, на этой странице можно отобразить или создать новое сообщество SNMP.

Нажмите кнопку «New/Add», чтобы открыть новую страницу сообщества SNMP. Пользователь может настроить имя вновь созданного сообщества, права доступа и представления сообщества. Страница конфигурации показана на следующем рисунке:

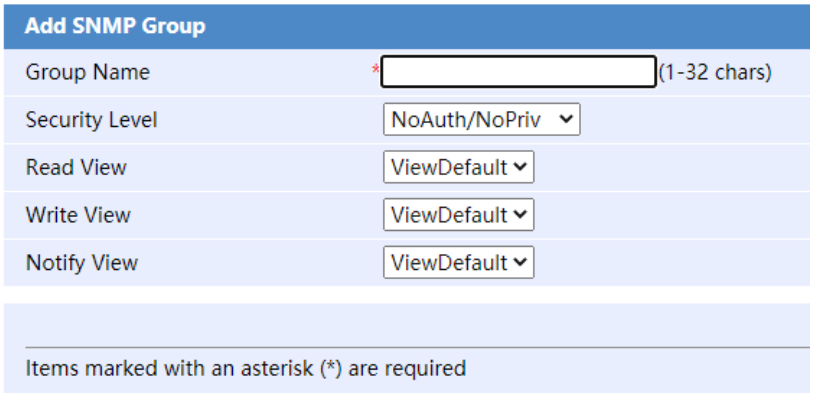


10.2.1.7.3 Настройки группы SNMP

Перейдите в меню: Device → SNMP → Group, на этой странице можно отобразить или создать новую группу SNMP.

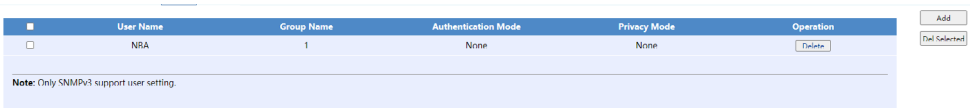


Нажмите «New/Add», чтобы перейти на страницу новой группы SNMP, пользователь может настроить имя группы, уровень безопасности и просмотреть разрешения вновь созданной группы.

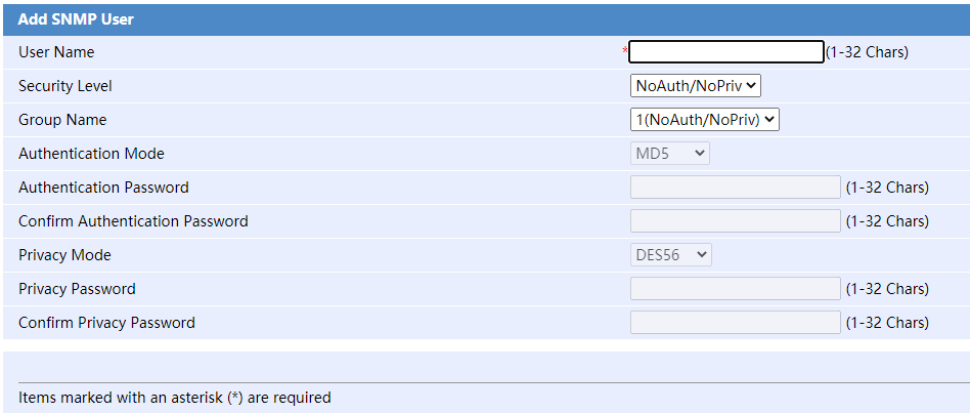


10.2.1.7.4 Пользовательские настройки SNMP

Перейдите в меню: Device → SNMP → User, на этой странице можно отображать или создавать новых пользователей SNMP.

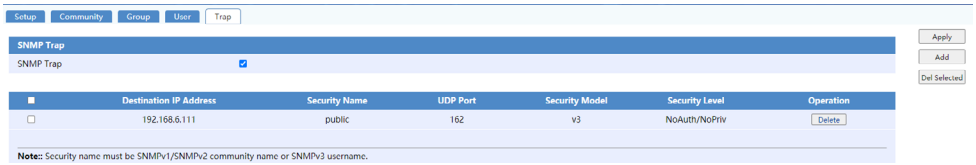


Нажмите «Add», чтобы войти на страницу нового пользователя, пользователь может настроить имя пользователя, уровень безопасности и режим аутентификации нового пользователя, а также другую соответствующую информацию.

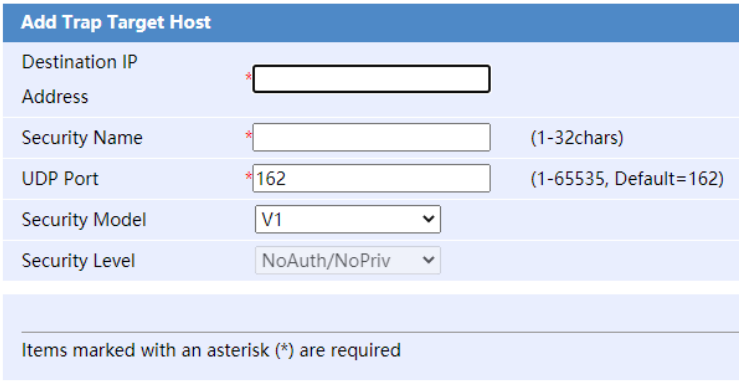


10.2.1.7.5 Настройки фильтра SNMP

Перейдите в меню: Device → SNMP → Trap, на этой странице можно настроить включение/выключение функции SNMP-фильтра, отображение информации об узле прерывания и создание нового узла прерывания.

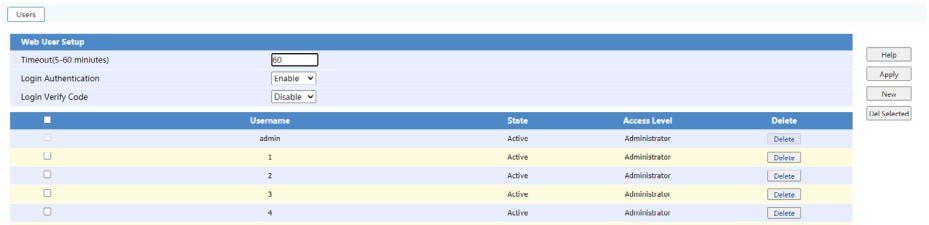


Нажмите «Add», чтобы перейти на новую страницу узла фильтра, пользователь может настроить IP-адрес, имя безопасности, порт UDP, модель безопасности, уровень безопасности нового узла фильтра.

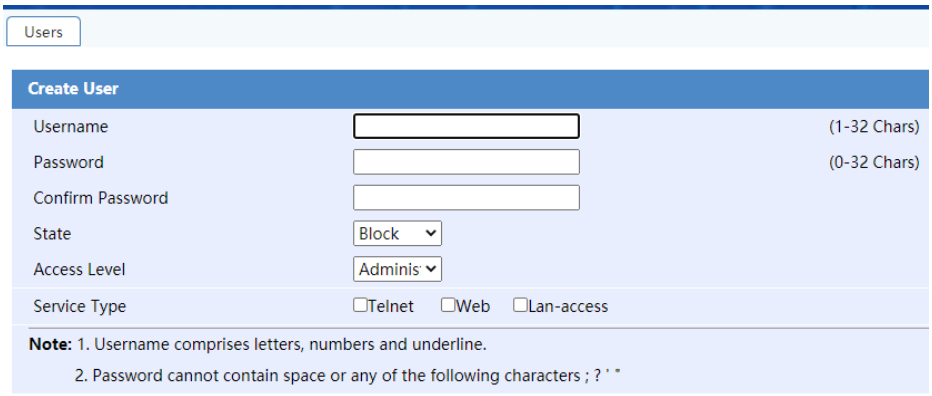


10.2.1.8 Управление пользователями

Перейдите в меню: Device → Users. На этой странице можно настроить время ожидания пользователя, включить/выключить функцию веб-аутентификации и включить/выключить функцию проверочного кода.



Шаги для добавления локального пользователя:
Нажмите кнопку < New > на главной странице, задайте новую информацию о пользователе на странице «Add Local User» и нажмите кнопку <Apply>, чтобы изменения вступили в силу.



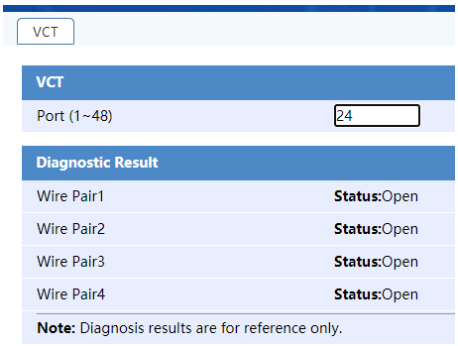
Изменение локальных пользователей:
Нажмите на запись локального пользователя, которую нужно изменить, на главной странице, чтобы перейти на страницу «Modify User» для изменения.

Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Timeout(5-60 miniutes)	Настройка времени ожидания страницы веб-настроек, по умолчанию 5 минут
Login Authentication	Включить/выключить функцию аутентификации пользователя. После закрытия пользователю не нужно проходить верификацию при входе в систему
Login Verify Code	Включить/выключить функцию кода подтверждения входа в сеть. После открытия вам необходимо ввести проверочный код при входе в WEB.
Username	Установите локальное имя пользователя, которое будет добавлено
Confirm password	Установить пароль локального пользователя
State	Установить статус локальных пользователей
Access Level	Установить уровень локальных пользователей

10.2.1.9 Обнаружение неисправности кабеля

При неисправности линии возможно произвести диагностику кабеля подключенного порту.
Перейдите в меню: Device → VCT
Введите номер порта для диагностики в текстовом поле «Port» и нажмите кнопку <Apply>, чтобы завершить диагностику кабеля порта.



Значение ключевых элементов на странице показано в таблице ниже.

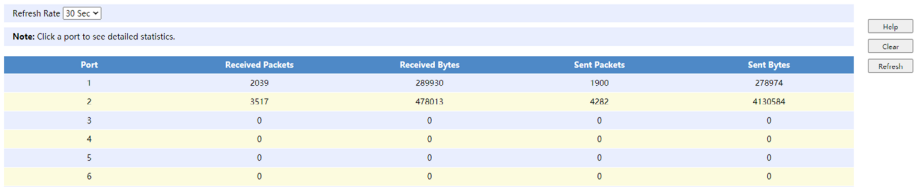
ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Status	Отображение состояния подключения порта. Отображение как «Normal» (нормальное) указывает на то, что порт подключен; отображение «Open» (открыто) указывает на то, что порт не подключен; отображение в виде «Short circuit» (короткого замыкания) означает, что в паре дифференциальных линий произошло короткое замыкание.
Length	Если состояние кабеля «Normal» (нормальное), длина соединительного кабеля не отображается в отображаемой информации. Если состояние кабеля «Short circuit» (короткое замыкание или обрыв), длина отображаемой информации относится к длине от порта до обрыва кабеля.

- Во время диагностики кабеля не подключайте и не отключайте сетевой кабель порта, а диагностируемый порт не может находиться в выключенном состоянии.
- Диагностика кабеля действительна только в том случае, если на другом конце сетевого кабеля нет подключения устройства или сетевой кабель неисправен. Когда оба конца сетевого кабеля подключены, результат диагностики может быть неверным.

10.2.1.10 Мониторинг потока

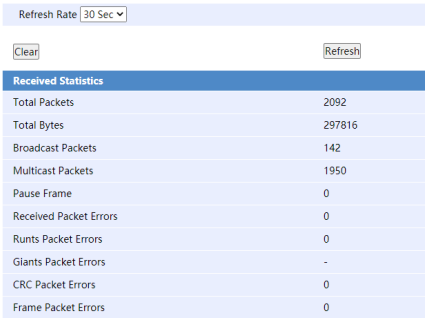
10.2.1.10.1 Статистика порта

Перейдите в меню: Device → Flow Interval → Port Traffic Statistics , на странице статистики порта можно просмотреть количество пакетов данных, полученных/отправленных каждым портом коммутатора.



Port	Received Packets	Received Bytes	Sent Packets	Sent Bytes
1	2039	289930	1900	278974
2	3517	478013	4282	4130584
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0

Чтобы просмотреть количество различных типов пакетов ошибок, полученных/отправленных через назначенный порт коммутатора (щелкните запись, соответствующую порту на главной странице, чтобы перейти на соответствующую страницу статистической информации).



Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Refresh rate	Выбор частоты обновления для автоматического обновления статистики текущей страницы
Clean	Очистка статистики текущей страницы
Refresh	Обновление статистики текущей страницы

Описание пакетов, полученных/отправленных через порт.

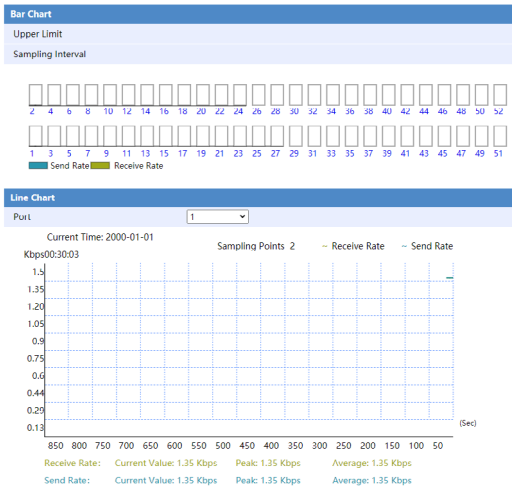
ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Receive statistics	
Total packet	Общее количество полученных сообщений
Total bytes	Всего байтов полученных сообщений
Broadcast package	Общее количество полученных широковещательных сообщений
Multicast package	Общее количество полученных многоадресных сообщений
Receive error packets	Общее количество принятых пакетов ошибок
Runts error package	Количество пакетов с правильным CRC и длиной кадра данных менее 64 байт
Giants error package	Количество пакетов с правильной CRC и длиной кадра данных более 1518 байт
CRC error packet	Количество пакетов с ошибкой CRC и длиной кадра данных от 64 до 1518 байт
Frame error packet	Длина пакета данных составляет от 64 до 1518 байт, а количество байтов FCS (последовательность проверки кадра) сообщения является нецелым сообщением
Aborts error package	Общее количество полученных ошибочных пакетов. К незаконным пакетам относятся: • Фрагментация сообщения: кадры длиной менее 64 байт (длина может быть целой или нецелой) и ошибка проверки CRC • Кадр jabber: больше 1518 или 1522 байт и ошибка проверки CRC (байты сообщения могут быть целыми или нецелыми) • Кадр ошибки символа: сообщение содержит хотя бы один ошибочный символ • Кадр ошибки длины: поле длины 802.3 в сообщении не соответствует фактической длине сообщения (от 46 до 1500 байт)
Ignored error package	Количество пакетов, отброшенных из-за недостаточности приемных буферов на порту
Sent Statistics	
Total packets	Общее количество отправленных сообщений
Total bytes	Общее количество отправленных байтов
Broadcast package	Общее количество отправленных широковещательных сообщений
Multicast package	Общее количество отправленных многоадресных сообщений
Send error packet	Общее количество отправленных сообщений об ошибках
Aborts error package	Общее количество пакетов, которые не удалось отправить, то есть пакеты были отправлены, но по разным причинам (например, из-за конфликта)
Deferred error packet	Количество пакетов, задержанных первым запросом на передачу из-за загруженности сети
Collisions error package	Количество конфликтующих пакетов, сгенерированных портом во время передачи пакета
Late collisions error package	Количество задержанных коллизий. Отложенный кадр коллизии означает, что первые 512 бит кадра были отправлены. Из-за обнаружения столкновения кадр задерживается.

10.2.1.10.2 Статистика порта

С помощью мониторинга трафика портов пользователи могут графически отслеживать текущий трафик каждого порта устройства и изменения трафика за указанный период времени.
Мониторинг потока состоит из гистограммы мониторинга потока и линейной диаграммы мониторинга потока:

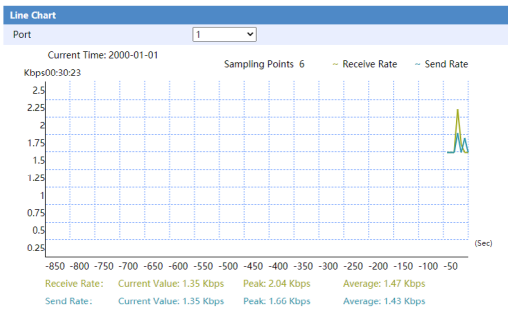
- Гистограмма мониторинга потока: используйте гистограмму для отображения состояния текущей скорости приема и скорости отправки каждого порта.
- Линейная диаграмма мониторинга потока: отображение изменения потока указанного порта за определенный период времени в виде линейных колебаний.

Перейдите в меню: Device → Flow Interval → Traffic Monitoring.



Страница гистограммы мониторинга потока может выполнять следующие функции:

- Мониторинг трафика порта через гистограмму скорости.
- Выберите верхний предел гистограммы в раскрывающемся списке «Traffic Upper Limit», отобразится пропорция скорости приема/отправки каждого порта относительно верхнего предела. Когда пропорция превышает 95%, граница гистограммы будет иметь красное предупреждение.
- Выберите временной интервал в раскрывающемся списке «Sampling Interval», для настройки интервала обновление страницы.
- Наведите указатель мыши на гистограмму порта, и появится желтое текстовое поле, показывающее номер порта, скорость приема и скорость отправки. Нажмите на гистограмму, чтобы увидеть график линейной скорости порта.
- Нажмите кнопку <Stop> на странице, чтобы приостановить мониторинг трафика; нажмите кнопку <Recover>, чтобы возобновить мониторинг трафика.

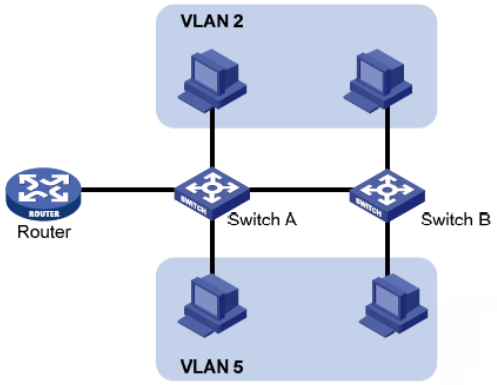


Страница линейной диаграммы мониторинга потока может выполнять следующие функции:

- Мониторинг трафика порта с помощью линейной диаграммы скорости
- Щелкните номер порта на гистограмме для наблюдения за изменением скорости порта в режиме реального времени.
- Текущее значение, пиковое значение и среднее значение скорости приема и скорости отправки отображаются в нижней части линейного графика.

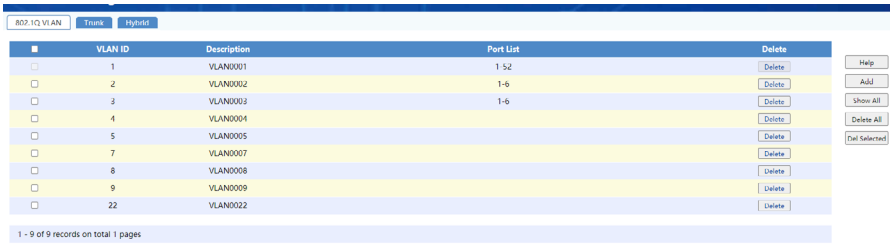
10.3 СЕТЕВЫЕ НАСТРОЙКИ

VLAN (Virtual Local Area Network) - это технология, позволяющая объединять устройства в сети, в сегменты на основе функций, приложений или требований управления. Виртуальные сегменты могут формироваться в независимости от физического расположения устройств. VLAN имеют те же свойства, что и физические LAN, за исключением того, что VLAN представляет собой логическое объединение, а не физическое. Поэтому во VLAN можно объединять устройства, независимо от того, где они находятся физически, а широковещательный, многоадресный и одноадресный трафик в одном VLAN отделен от других VLAN. Стандарт IEEE 802.1Q определяет процедуру передачи трафика VLAN. Основная идея технологии VLAN заключается в том, что большая локальная сеть может быть динамически разделена на отдельные широковещательные области, удовлетворяющие различным требованиям, каждый VLAN представляет собой отдельный широковещательный домен.

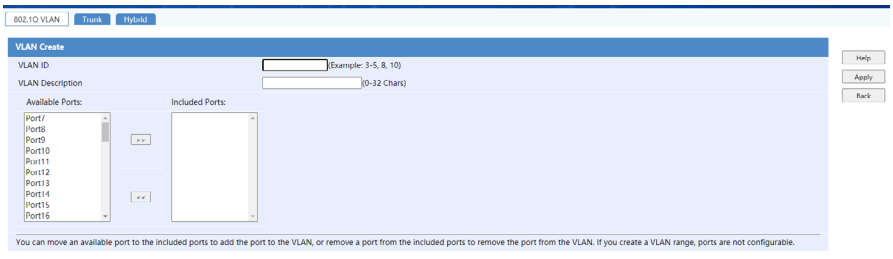


10.3.1 Настройка VLAN 802.1Q

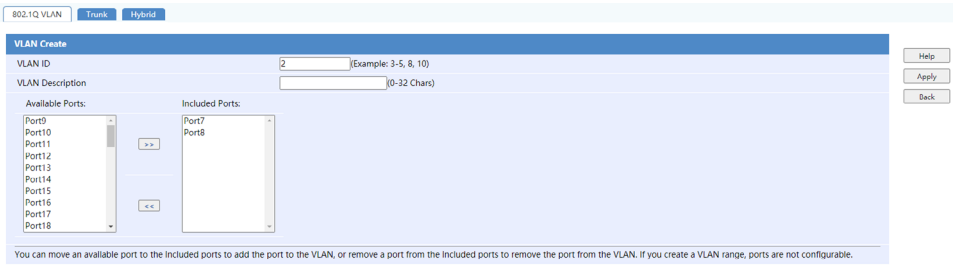
Перейдите в меню: Network → VLAN → 802.1Q VLAN, как показано на рисунке. Данная страница может отображать и запрашивать информацию о VLAN коммутатора и содержащихся в ней портах (главная страница. VLAN 1 по умолчанию включает все порты)



Создайте новую VLAN (нажмите кнопку <Add> на главной странице, чтобы перейти на соответствующую страницу, как показано ниже. Введите VLAN, которую вы хотите создать, в текстовое поле «VLAN ID» и нажмите кнопку <Apply>, чтобы изменения вступили в силу). Создайте новый порт доступа (выберите порт, который нужно добавить в VLAN, и нажмите кнопку <Apply>, чтобы изменения вступили в силу).

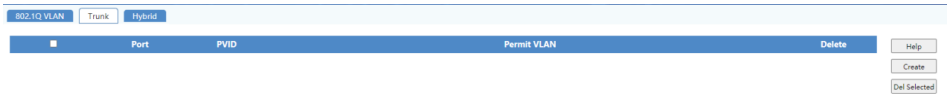


Измените порт доступа в VLAN (щелкните запись, соответствующую VLAN на домашней странице, чтобы перейти на соответствующую страницу, как показано на рисунке ниже. Повторно укажите порт, который необходимо добавить в VLAN, нажмите кнопку <Apply > для вступления в силу).

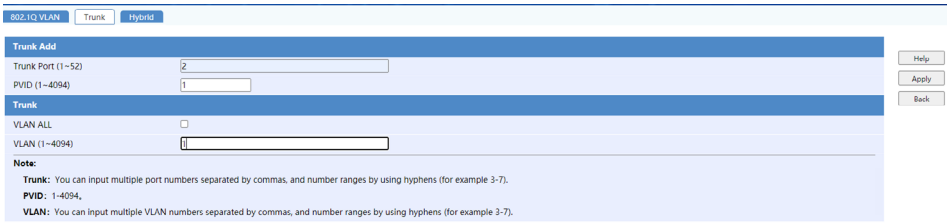


10.3.2 Настройка Trunk порта

Перейдите в меню: Network → VLAN → Trunk, отображение текущей информации о порте.



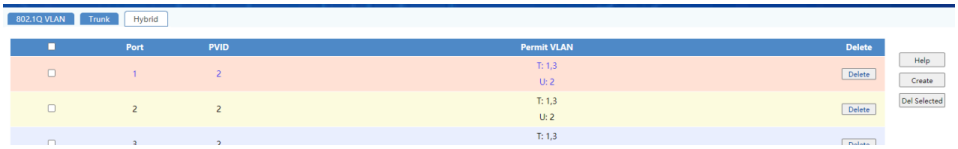
Действия по созданию нового Trunk порта: Нажмите кнопку <Create> на главной странице, чтобы перейти на соответствующую страницу. Укажите магистральный порт, настройте PVID и порт, чтобы разрешить VLAN. Нажмите кнопку <Apply>, чтобы изменения вступили в силу.



Действия по изменению Trunk порта: Щелкните запись, соответствующую порту на главной странице, чтобы перейти на соответствующую страницу. Измените PVID и порт, разрешенный для передачи VLAN, нажмите кнопку < Apply >, чтобы изменения вступили в силу.

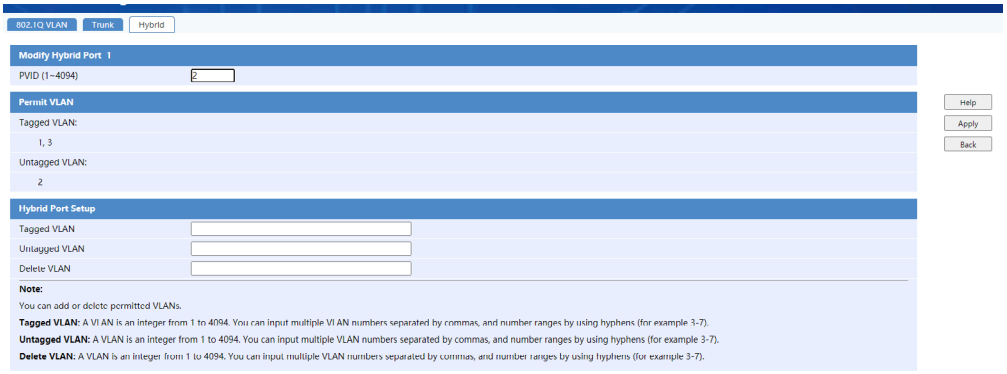
10.3.3 Настройка Hybrid порта

Перейдите в меню: Network → VLAN → Hybrid. Страница показана на рисунке ниже, где указана текущая информация о гибридном порте коммутатора.



Действия по созданию нового гибридного порта: Нажмите кнопку <Create> на главной странице, чтобы перейти на соответствующую страницу. Укажите гибридный порт и настройте PVID и порт для прохождения через VLAN. Нажмите кнопку <Apply>, чтобы изменения вступили в силу.

Действия по изменению гибридного порта: Щелкните запись, соответствующую порту на главной странице, чтобы перейти на соответствующую страницу. Измените PVID и порт, разрешенный для передачи VLAN, нажмите кнопку <Apply>, чтобы изменения вступили в силу.



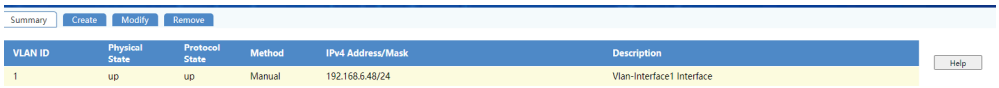
- PVID: число, диапазон значений 1-4094.
- Tagged VLAN: номер, диапазон значений 1-4094, можно ввести несколько значений, разделенных запятыми. Для обозначения диапазона можно использовать короткую линию.
- Untagged VLAN: номер, диапазон значений 1-4094, можно ввести несколько значений, разделенных запятыми. Для обозначения диапазона можно использовать короткую линию.
- Delete VLAN: номер, диапазон значений 1-4094, можно ввести несколько значений, разделенных запятыми. Для обозначения диапазона можно использовать короткую линию.

10.3.3 Интерфейс VLAN

Меню интерфейса VLAN в основном используется для настройки и управления интерфейсами VLAN уровня 3 устройства, включая отображение интерфейса, создание нового интерфейса, изменение интерфейса и удаление интерфейса.

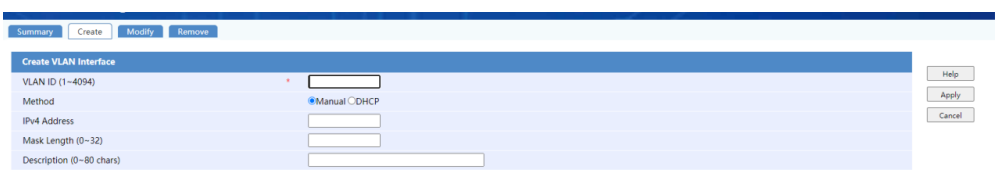
10.3.3.1 Дисплей интерфейса

Перейдите в меню: Network → VLAN Interface → Summary
На этой странице пользователи могут запрашивать интерфейс, статус интерфейса и информацию об интерфейсе текущего устройства.



10.3.3.2 Новый интерфейс

На этой странице пользователи могут создать новый интерфейс VLAN уровня 3 и настроить метод получения адреса интерфейса. Если это статический метод сбора данных, можно настроить конкретную информацию об адресе интерфейса.

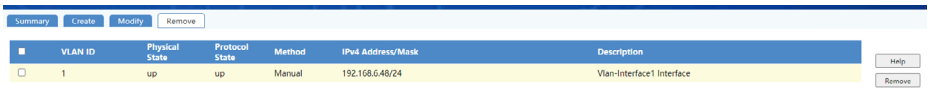


10.3.3.3 Изменить интерфейс

Перейдите в меню: Network → VLAN Interface → Modify
На этой странице пользователь может изменить трехуровневый интерфейс VLAN и изменить метод получения адреса интерфейса. Если это статический метод сбора данных, информация об адресе интерфейса также может быть изменена.

10.3.3.4 Удаление интерфейса VLAN

Перейдите в меню: Network → VLAN Interface → Modify Interface
На этой странице пользователи могут удалить указанный интерфейс VLAN уровня 3. Страница конфигурации выглядит следующим образом:



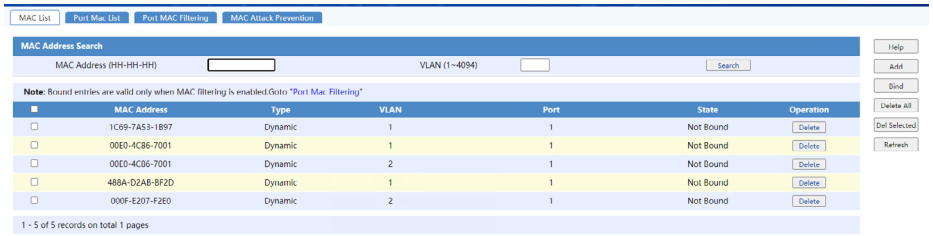
10.3.4 Настройки MAC-адреса

Коммутатор поддерживает следующие три типа записей MAC-адресов:

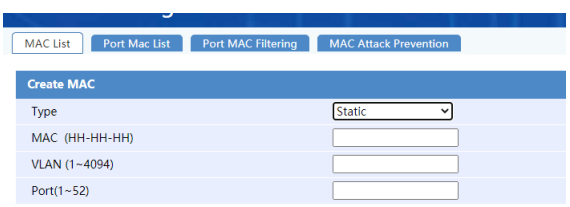
- Static: запись добавляется вручную, запись MAC-адреса не устаревает. После добавления запись находится в «связанном» состоянии (многоадресные записи MAC-адресов не поддерживают операции привязки).
- Dynamic: автоматически узнать или добавить вручную, запись MAC-адреса будет устаревать. При добавлении, запись находится в «несвязанном» состоянии; При выполнении операции привязки, MAC становится статической записью.
- Blackhole: добавляется вручную, все пакеты, адресом назначения которых является MAC-адрес, будут отбрасываться (например, из соображений безопасности пользователь может быть заблокирован от получения пакетов), и не поддерживает операцию привязки.

10.3.4.1 Отображение MAC-адреса

Перейдите в меню: Network → MAC Filter → MAC List, страница показана на рисунке ниже, можно отображать и запрашивать (через комбинацию MAC-адреса и условий VLAN) всю информацию таблицы MAC-адресов устройства и указанного MAC-адреса. элемент таблицы адресов Bind (выберите запись для привязки на главной странице и нажмите кнопку <Binding>, чтобы изменения вступили в силу).



Для добавления новой записи MAC-адреса: Нажмите кнопку <Add> на главной странице, настройте соответствующие параметры записи MAC-адреса на странице, на которую был выполнен переход. Нажмите кнопку <Apply>, чтобы изменения вступили в силу.
Для изменения записи статических или закрытых MAC-адресов (щелкните соответствующую запись MAC-адреса на главной странице, чтобы изменить запись), записи динамических MAC-адресов изменить нельзя.



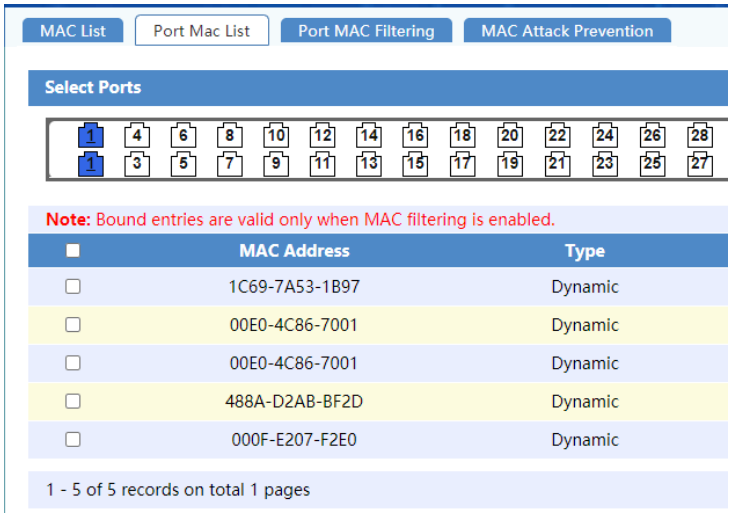
Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Запрос MAC-адреса	Введите MAC-адрес и идентификатор VLAN для запроса и отображения.
Отображение MAC-адреса	Отображение MAC-адреса и соответствующую ему сеть VLAN в коммутаторе. Пользователь может выбрать MAC со статусом «unbound». Добавить соответствующий MAC-адрес в список привязок, нажав кнопку <Binding>.
State	Показать статус привязки MAC-адреса • Not supported: MAC-адрес нельзя добавлять в список привязок, например, MAC-адрес отброшенных, MAC-адрес многоадресной рассылки; • Bound: MAC-адрес добавлен в список привязок; • Unbound: MAC-адрес отсутствует в списке привязки, но его можно добавить.
Add	Открыть страницу добавления MAC-адреса
Binding	Добавить выбранный MAC-адрес, который можно привязать к списку привязки
Delete	Нажмите кнопку <Delete> после элемента, который нужно удалить, чтобы удалить связанное содержимое
Delete all	Удалить все MAC-адреса на устройстве
Del Selected	Удалить выбранные MAC-адреса в пакетах и удалить их

10.3.4.2 Отображение MAC-адреса порта

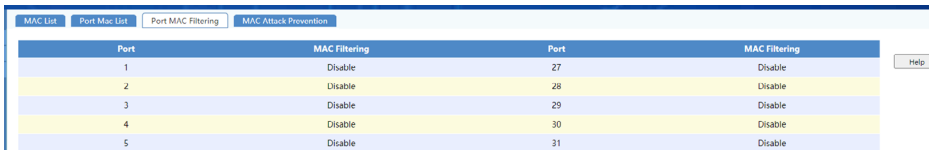
Перейдите в меню: Network → MAC Filter → Port Mac List. Данная страница предоставляет следующие функции:

- Отображение информации таблицы MAC-адресов для указанного порта
- Привязка несвязанных записей MAC-адресов к порту (выберите соответствующий номер порта и выберите несвязанные записи MAC-адресов к порту, нажмите кнопку <Binding>, чтобы изменения вступили в силу)



10.3.4.3 Настройка фильтрации MAC-адресов портов

Перейдите в меню: Network → MAC Filter → Port MAC Filtering, отображение состояния функции фильтрации MAC-адресов каждого порта.



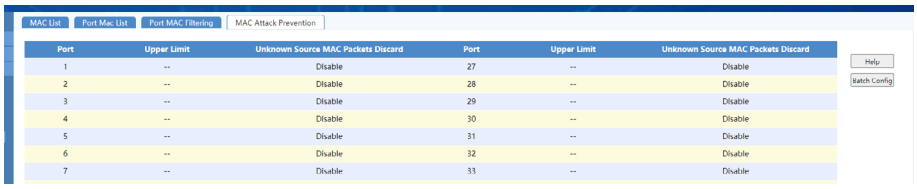
Настройка:

1. Включите функцию фильтрации MAC-адресов указанного порта, щелкните запись, соответствующую порту на главной странице, установите флажок «MAC filtering» и нажмите кнопку <Apply>, чтобы изменения вступили в силу.
2. Добавьте запись статического MAC-адреса указанного порта, щелкните запись, соответствующую порту на главной странице, введите соответствующие параметры в текстовые поля «MAC-адрес» и «VLAN» и нажмите кнопку <Add>, чтобы вступить в силу.

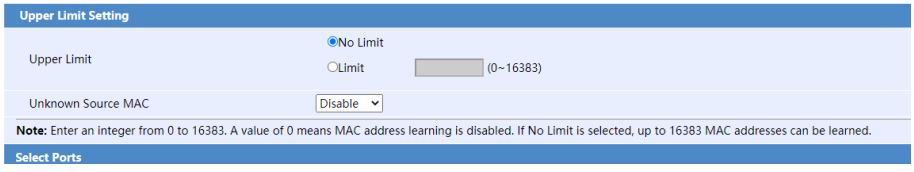
10.3.4.4 Настройка защиты от атаки по MAC-адресу

Функция защиты от атаки по MAC-адресам предотвращает постоянную фильтрацию устройством MAC-адресов большого количества недопустимых пакетов в локальной сети, что делает таблицу переадресации MAC-адресов устройства слишком большой, что приводит к резкому снижению производительности пересылки. Коммутатор выполняет функцию предотвращения атак с использованием MAC-адресов за счет ограничения количества MAC-адресов, полученных на порту.

Перейдите в меню: Network → MAC Filter → Port MAC Attack Prevention, на главной странице показано текущее количество MAC-адресов, которые могут узнать все порты.



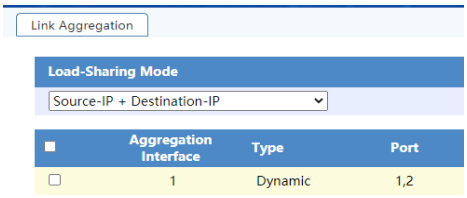
Настройте количество MAC-адресов, которые могут быть изучены одним портом. Щелкните запись, соответствующую порту на главной странице, чтобы перейти на соответствующую страницу.



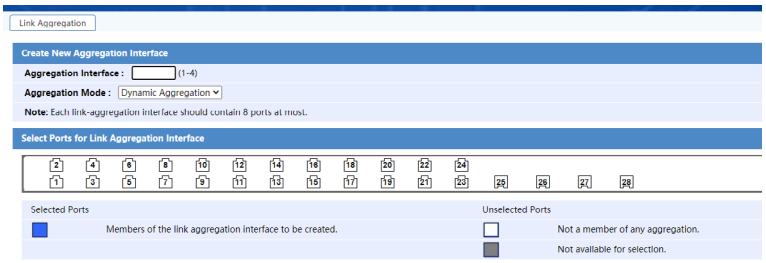
Пакетная настройка количества MAC-адресов, которые могут быть изучены указанным портом. Нажмите кнопку < Batch Config > на главной странице, чтобы перейти на соответствующую страницу.

10.3.5 Агрегирование ссылок

Перейдите в меню: Network → Link Aggregation. На этой странице можно просмотреть текущий статус агрегации ссылок и настроить алгоритм агрегации.



Создание новой агрегации ссылок: Нажмите кнопку <Create> на главной странице, чтобы перейти на соответствующую страницу.



Create New Aggregation Interface: выберите запись на главной странице, дважды щелкните ее или нажмите кнопку <Modify>, чтобы перейти на соответствующую страницу.

Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Aggregation algorithm	Выберите алгоритм агрегации коммутатора: • Based on source MAC address: указывает, что каждый порт в группе агрегации выполняет распределение нагрузки на основе исходного MAC-адреса. • Based on destination MAC address: указывает, что каждый порт-участник в группе агрегации выполняет распределение нагрузки на основе MAC-адреса назначения. • Based on source MAC address and destination MAC address: указывает, что каждый порт-участник в группе агрегации выполняет распределение нагрузки на основе MAC-адреса источника и MAC-адреса назначения. • Based on source IP address and destination IP address: указывает, что каждый порт в группе агрегации выполняет распределение нагрузки на основе IP-адреса источника и IP-адреса назначения. • По умолчанию каждый порт в группе агрегации коммутатора выполняет распределение нагрузки на основе IP-адреса источника и IP-адреса назначения.
Aggregate interface number	Показать совокупный номер интерфейса
Type	Показать тип агрегации
Port	Номера портов, входящие в группу агрегации

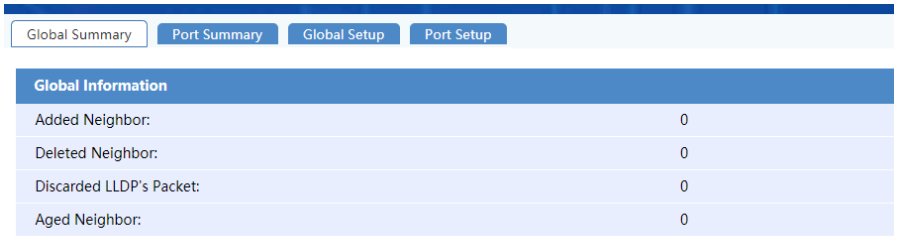
Порты в следующих ситуациях не могут присоединиться к группе агрегации:
- Зеркальный порт мониторинга
- Порт с включенной фильтрацией MAC-адресов
- Порты, настроенные с ограничением обучения MAC-адресов

10.3.5 LLDP

LLDP (Link Layer Discovery Protocol, 802.1ab) - протокол канального уровня, позволяющий коммутатору оповещать оборудование, работающее в локальной сети, о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

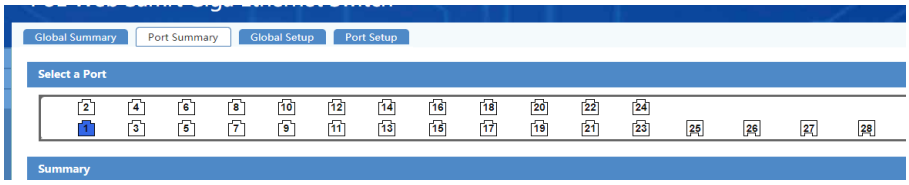
10.3.5.1 Общие сведения LLDP

Перейдите в меню: Network → LLDP → Global Summary. На этой странице можно просмотреть добавленные соседние устройства, удаленные соседние устройства, отброшенные пакеты LLDP и устаревшие соседние устройства.



10.3.5.2 Отображение порта LLDP

Перейдите в меню: Network → LLDP → Port Summary. На этой странице можно выбрать порт, например порт 2, и статистика пакетов LLDP для порта 2 будет отображаться в столбце «Summary».



10.3.5.3 Общая настройка LLDP

Перейдите в меню: Network → LLDP → Global Setup.

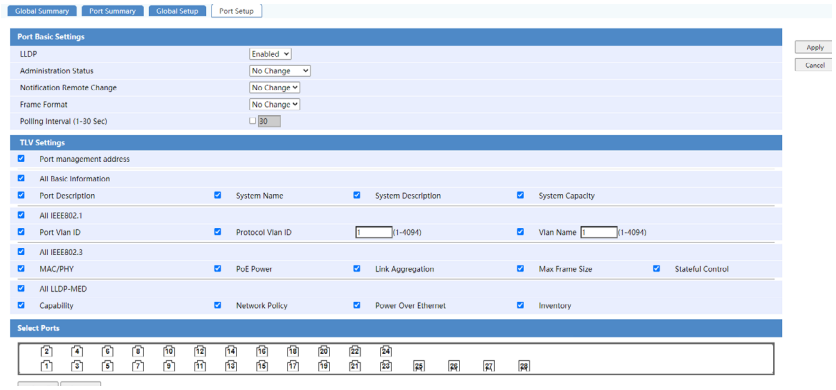
Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
LLDP	Выберите «Disabled» в раскрывающемся списке, чтобы отключить функцию LLDP, выберите «Enabled», для включения LLDP.
Transmit Interval	Интервал передачи пакетов LLDP
TTL Hold Multiplier	Множитель TTL
Fast Count	Количество отправленных пакетов LLDP
Initialization Delay	Время задержки инициализации
Send Packet Delay	Задержка отправки пакетов LLDP
Trap Interval	Интервал отправки trap-пакета

После настройки приведенной выше информации нажмите кнопку <Apply>, чтобы применить ее.

10.3.5.4 Настройки порта LLDP

Перейдите в меню: Network → LLDP → Port Setup.



Значение ключевых пунктов на странице настроек порта показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
LLDP	Выберите «Disabled» в раскрывающемся списке, чтобы отключить функцию LLDP, выберите «Enabled», для включения LLDP.
Administration Status	Режим работы порта LLDP: • send&receive: указывает, что оба пакета LLDP отправляются и принимаются. • receive_Only: указывает, что принимаются и не отправляются только пакеты LLDP. • send_Only: указывает, что не отправляются только пакеты LLDP. • disabled: указывает, что пакеты LLDP не отправляются и не принимаются.
Notification Remote Change	Для уведомления об удаленном изменении выберите «Disabled» в раскрывающемся списке, чтобы отключить функцию удаленного уведомления, выберите «Enabled», даже если возможно использовать функцию уведомления об удаленном изменении.
Frame Format	Выберите формат кадра
Polling Interval (1-30 Sec)	Значение интервала опроса, 0 означает, что функция опроса отключена

Значение ключевых элементов на странице настроек TLV показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Port management address	Адрес управления портом
All Basic Information	Установите флажок, чтобы выбрать все параметры в разделе основной информации, включая описание порта, имя системы, описание системы и емкость системы.
All IEEE802.1	Отметьте, чтобы выбрать все параметры в разделе IEEE802.1, включая идентификатор VLAN порта, идентификатор VLAN протокола и имя VLAN.
All IEEE802.3	Отметьте, чтобы выбрать все параметры в соответствии с IEEE802.3, включая MAC, источник питания POE, агрегацию каналов, самый длинный кадр и контроль состояния.
All LLDP-MED	Отметьте, чтобы выбрать все параметры в LLDP-MED, включая производительность, сетевую стратегию, питание через Ethernet и информацию об активах MED оборудования.

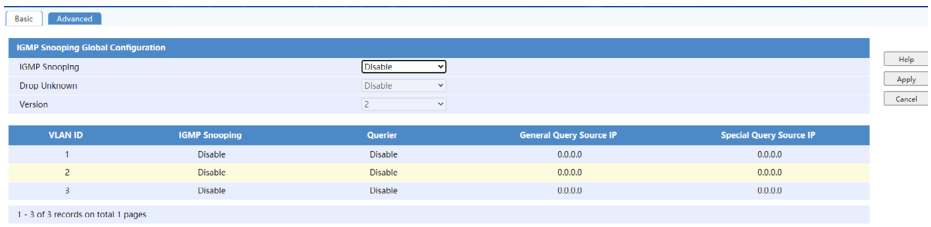
После настройки приведенной выше информации нажмите кнопку <Apply>, чтобы применить ее.

10.3.6 IGMP Snooping

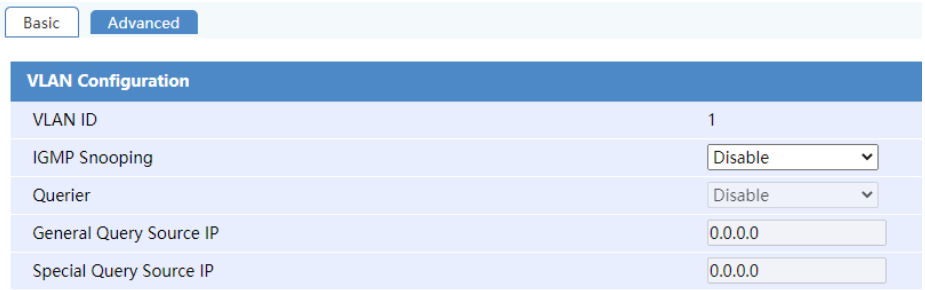
IGMP (Internet Group Management Protocol) - протокол управления групповой (multicast) передачей данных в IP-сетях. IGMP используется маршрутизаторами и хостами для организации присоединения сетевых устройств к группам многоадресной рассылки (multicast). Устройство уровня 2, на котором выполняется отслеживание IGMP, анализирует полученные сообщения IGMP, чтобы установить отношение отображения между портом и MAC-адресом многоадресной рассылки, и пересылает данные многоадресной рассылки на основе этого отношения отображения.

10.3.6.1 Базовая настройка

Перейдите в меню: Network → IGMP Snooping → Basic. Возможно включить/выключить функцию IGMP Snooping, включить/выключить многоадресную передачу местоположения и установить версию. После включения функции IGMP Snooping, после нажатия кнопки <Apply>, на странице появится всплывающее окно «Enable Igmp snooping will clear the IP multicast MAC address in the MAC address table, are you sure?»

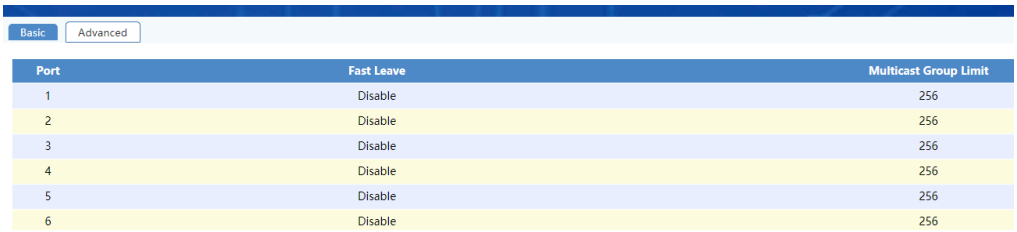


VLAN configuration: щелкните на запись в столбце VLAN ID, чтобы перейти на страницу конфигурации VLAN.

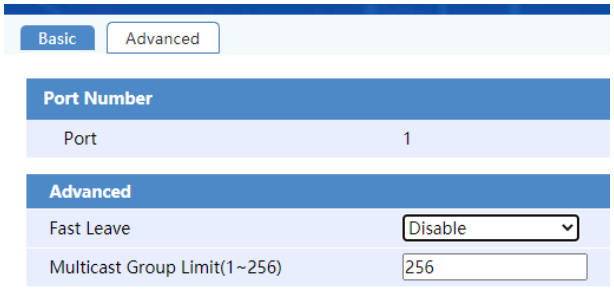


10.3.6.2 Расширенная конфигурация

Перейдите в меню: Network → IGMP Snooping → Advanced.
Конфигурация порта: щелкните запись, соответствующую порту на главной странице, чтобы перейти на соответствующую страницу, открыть/закрыть порт и выйти, а также настроить максимальное количество групп многоадресной рассылки (максимальное количество групп многоадресной рассылки — 256).



VLAN configuration: щелкните на запись в столбце VLAN ID, чтобы перейти на страницу конфигурации VLAN.



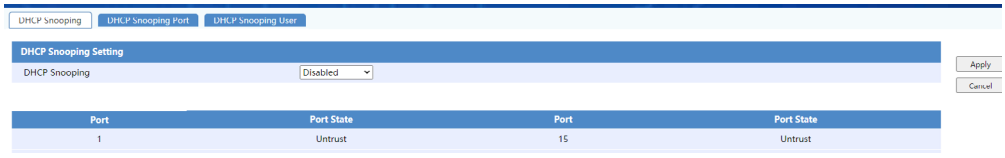
10.3.7 Отслеживание DHCP

Технология DHCP Snooping — это функция безопасности DHCP. Ненадежная информация DHCP фильтруется путем создания и поддержания таблицы привязок DHCP Snooping. Данная информация относится к информации DHCP из ненадежных областей. Таблица привязки DHCP Snooping содержит такую информацию, как MAC-адрес, IP-адрес, lease period и интерфейс VLAN-ID пользователей в запрещенной зоне.

- Основная функция DHCP-snooping — изоляция нелегального DHCP-сервера путем настройки ненадежных портов.
- Синхронизация с коммутатором DAI, чтобы предотвратить распространение вируса ARP.
- Создание и поддержка таблиц привязки DHCP-отслеживания. Данная таблица формируется по IP- и MAC-адресам в пакете DHCP ack, вторая задается вручную. Данная таблица является основой для последующих DAI (динамическая проверка arp) и IP Source Guard. Эти две похожие технологии используют таблицу, чтобы определить, является ли IP или MAC-адрес допустимым, и запрещать пользователям подключаться к сети.

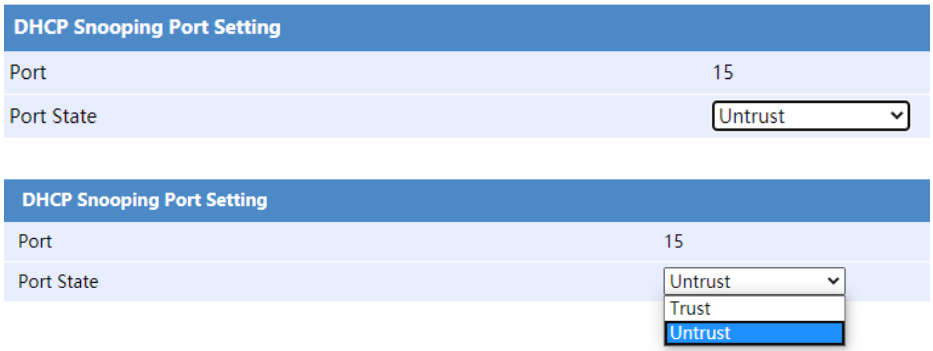
10.3.7.1 Глобальные настройки отслеживания DHCP

Перейдите в меню: Network → DHCP Snooping → DHCP Snooping setting , на этой странице можно включить/отключить функцию отслеживания DHCP.

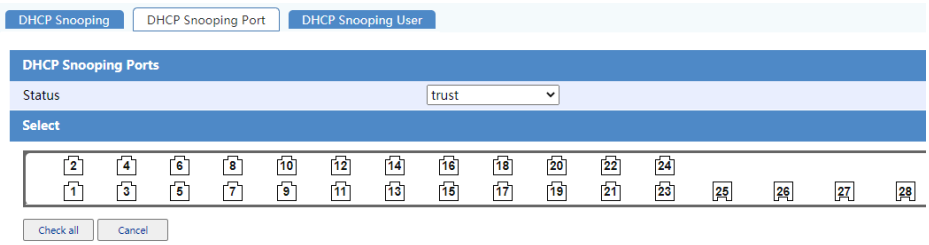


10.3.7.2 Конфигурация порта DHCP Snooping

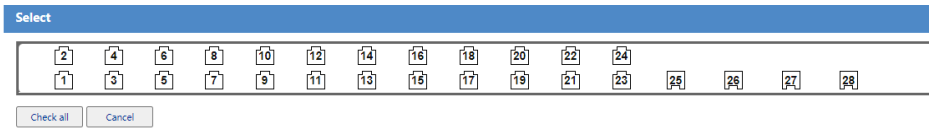
Настройка порта:
Перейдите в меню: Network → DHCP Snooping → DHCP Snooping Port setting, щелкните соответствующую запись в строке состояния портов на странице. Войдите на соответствующую страницу конфигурации и выберите статус доверия порта.



Установка портов:
Перейдите в меню: Network → DHCP Snooping → DHCP Snooping Port, выберите статус доверия порта в столбце Параметры пакета портов.



В столбце Select можно выбирать порты пакетами.



10.3.7.3 Конфигурация порта DHCP Snooping

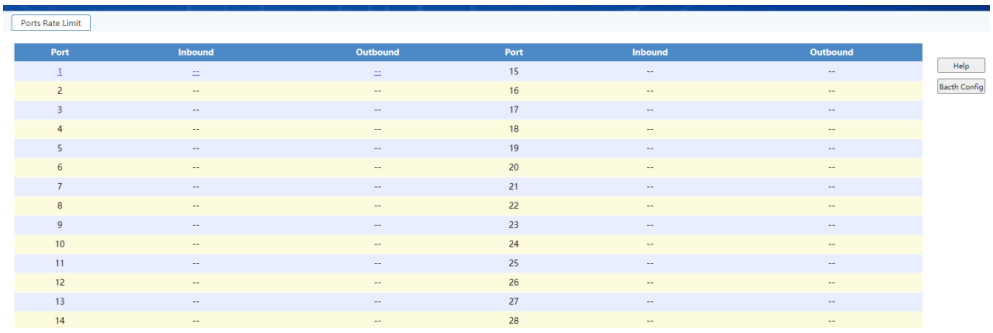
Перейдите в меню: Network → DHCP Snooping → DHCP Snooping User , на этой странице возможно просмотреть MAC-адрес пользователя, IP-адрес, интерфейс VLAN-ID и другую информацию о ненадежной зоне в таблице привязки DHCP Snooping.

10.3.8 QOS

10.3.8.1 Ограничение скорости порта

Перейдите в меню: QOS → port speed limit. На этой странице возможно проверить статус ограничения скорости для входных и выходных портов каждого порта («--» означает, что ограничение скорости не применяется).

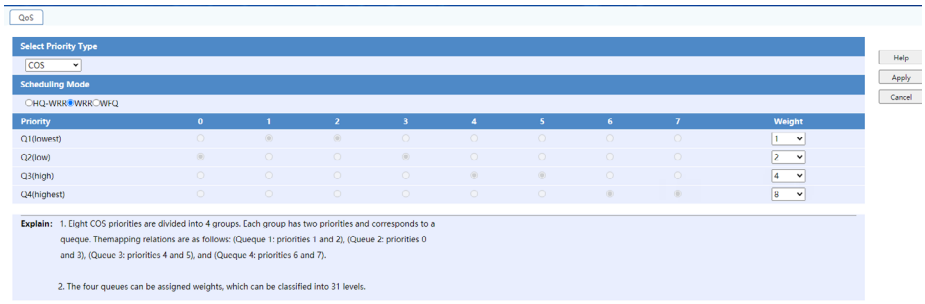
Настройте ограничение скорости входящего/исходящего порта для одного порта: щелкните запись, соответствующую порту на главной странице, чтобы перейти на соответствующую страницу.
Пакетная настройка ограничения скорости входящего/исходящего порта для указанного порта: Нажмите кнопку < Batch Configuration > на главной странице, чтобы перейти на соответствующую страницу.



Ограничение скорости входящего порта отбрасывает пакеты, превышающие ограничение скорости. Это повлияет на эффективность передачи большинства приложений, основанных на протоколе TCP. Реакция заключается в том, что фактическая скорость передачи намного ниже предельной скорости. Пользователям рекомендуется не включать функцию ограничения скорости входящего порта, для ограничения скорости исходящего порта не существует ограничения приложений.

10.3.8.2 Настройка функций QoS

Перейдите в меню: QoS → QoS. На этой странице можно настроить режим приоритетного доверия и режим планирования очереди.



Значение ключевых элементов на странице показано в таблице ниже.

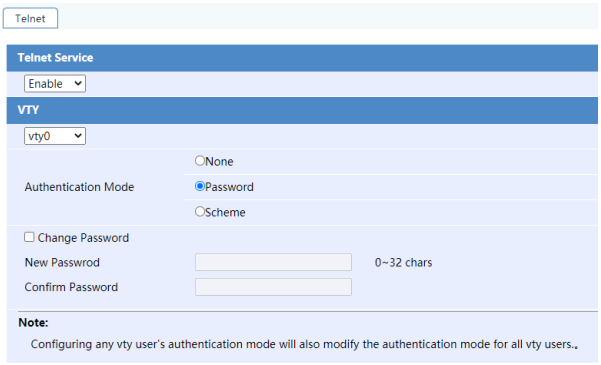
ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Priority	Выберите режим приоритета доверия: • COS: Поместите пакет в очередь вывода порта соответствующего приоритета в соответствии с приоритетом 802.1p. • DSCP: Поместите пакет в очередь вывода порта с соответствующим приоритетом в соответствии с приоритетом DSCP. По умолчанию коммутатор помещает пакеты в очередь вывода порта соответствующего приоритета в соответствии с приоритетом 802.1p.
Scheduling Mode	Выберите режим планирования очереди. По умолчанию коммутатор использует алгоритм планирования WRR. Пример: если соотношение очереди 1, очереди 2, очереди 3 и очереди 4 составляет 1:2:4:8, а режим планирования очереди — WRR. Затем, когда пакеты данных очередей 1, 2, 3 и 4 перегружены на определенном порту, порт будет отправлять пакеты в соответствии с коэффициентом потока 1:2:4:8; если режим планирования выбран как HQ-WRR, коммутатор сначала обеспечит отправку пакетов из очереди 4, а затем реализует планирование WRR для оставшихся 3 очередей.
Priority	Настройте приоритет каждой очереди

10.3.9 Telnet

Устройство поддерживает функцию Telnet. Пользователи могут настроить функцию Telnet через веб-страницу для удаленного управления и обслуживания устройства. Telnet поддерживает три метода аутентификации: none, password и scheme.

10.3.9.1 Служба Telnet

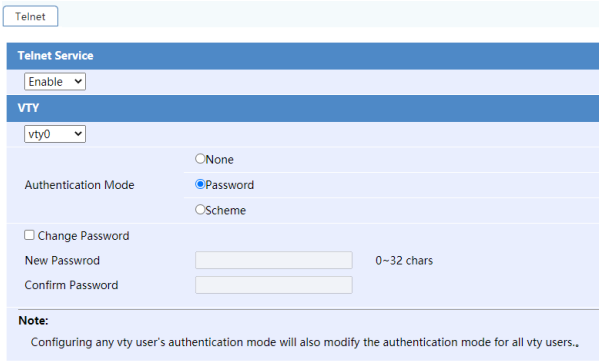
Перейдите в меню: Network → Telnet → Telnet service, в разделе Служба Telnet возможно включить/отключить функцию Telnet.



10.3.9.2 Конфигурация VTY

На странице конфигурации VTY возможно выбрать режим аутентификации Telnet (none, password и scheme). Возможно установить и изменить пароль при выборе режима password и scheme.

- Без аутентификации: указывает, что при следующем входе в устройство с помощью Telnet аутентификация имени пользователя и пароля не требуется, и любой может войти в устройство через Telnet. Данная ситуация может привести к скрытым угрозам безопасности.
- Вход через пароль — password: указывает, что при следующем входе в устройство с помощью Telnet потребуется аутентификация по паролю. Только после успешной аутентификации по паролю пользователь может войти в устройство.
- Расширенный метод — scheme: указывает, что при следующем входе в устройство с помощью Telnet вам необходимо будет аутентифицировать имя пользователя и пароль. Если имя пользователя или пароль неверны, вход невозможен. Аутентификация пользователя делится на локальную аутентификацию и удаленную аутентификацию. Если используется локальная аутентификация, необходимо настроить локальных пользователей и соответствующие параметры. Если используется удаленная аутентификация, имена пользователей и пароли необходимо настроить на удаленном сервере аутентификации.



10.3.10 Протокол VLAN

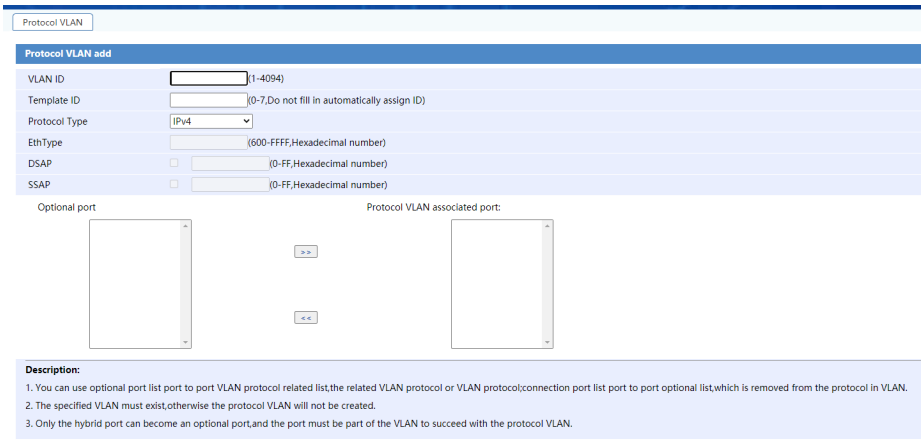
Протокол VLAN, также известный как VLAN на основе протокола, представляет собой еще один метод разделения VLAN для различения VLAN на основе портов. Настроив VLAN на основе протокола, коммутатор может анализировать пакеты, полученные без информации о VLAN по порту, и сопоставлять пакеты с шаблоном протокола, установленным пользователем, в соответствии с различными форматами инкапсуляции и значениями специальных полей, а также автоматически «Успешные пакеты» добавляются с тегом VLAN, настроенным в шаблоне протокола для автоматического распределения данных, принадлежащих указанному протоколу, в соответствующую VLAN для передачи.

10.3.10.1 Отображение и конфигурация Protocol VLAN

Перейдите в меню: Network → Protocol VLAN, на этой странице отображается информация о настройках протокола VLAN.

10.3.10.2 Новый протокол VLAN

Нажмите кнопку < New > на странице отображения протоколов VLAN, чтобы создать протокол VLAN:

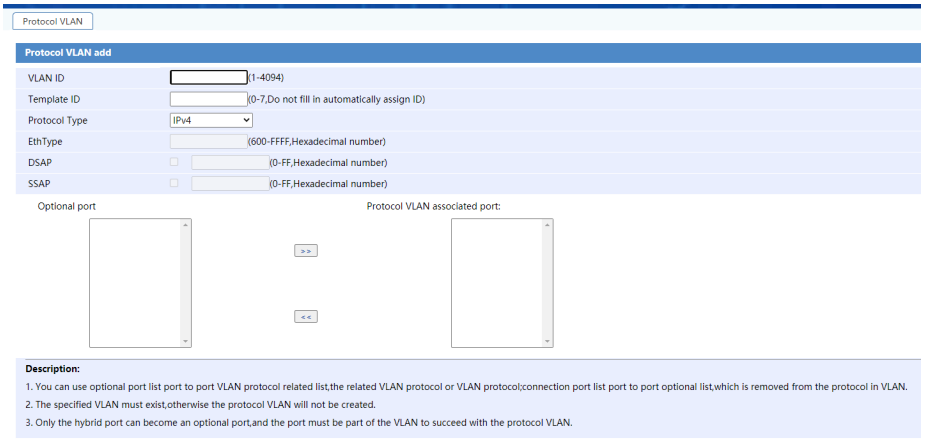


Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
VLAN ID	VLAN ID вновь созданного протокола VLAN
Template ID	Идентификатор шаблона протокола VLAN
Protocol Type	Тип протокола VLAN, поддержка IPv4, IPv6, AT (appletalk), IPx ethernetii, IPx LLC, IPx raw, IPx snap, MODE ethernetii, MODE LLC, MODE snap
EthType	Значение типа протокола Ethernet, если тип протокола — MODE ethernetii или MODE snap.
DSAP	Точка доступа к целевому сервису, если используется тип протокола MODE snap.
SSAP	Исходная точка доступа к службе, когда тип протокола MODE snap

10.3.10.3 Изменение протокола VLAN

Щелкните запись протокола VLAN на странице отображения протокола VLAN, чтобы перейти на страницу модификации соответствующего протокола VLAN, которая может изменить конфигурацию порта, связанного с протоколом VLAN.

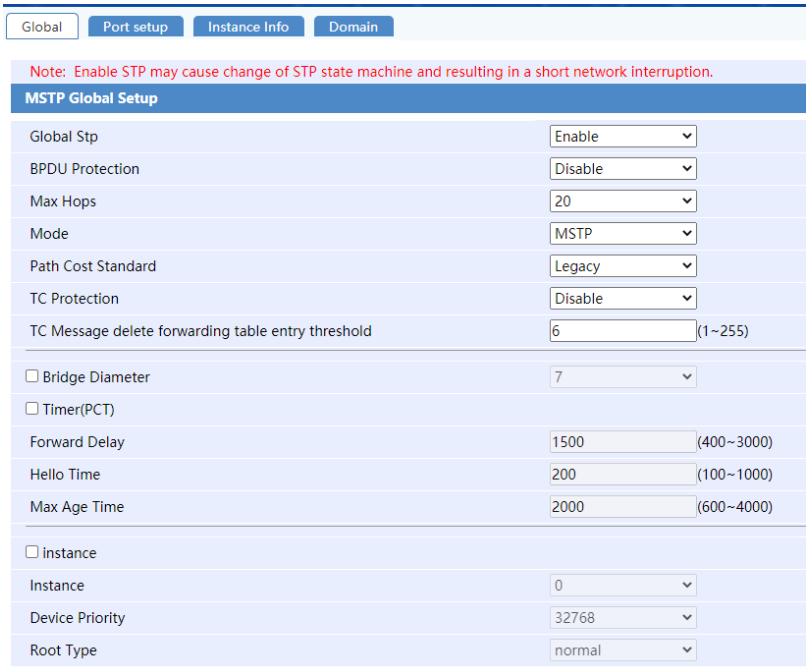


10.3.11 MSTP

Spanning Tree Protocol — это протокол управления 2-го уровня, который устраняет петли 2-го уровня путем выборочной блокировки избыточных каналов в сети, а также имеет функцию резервного копирования каналов.

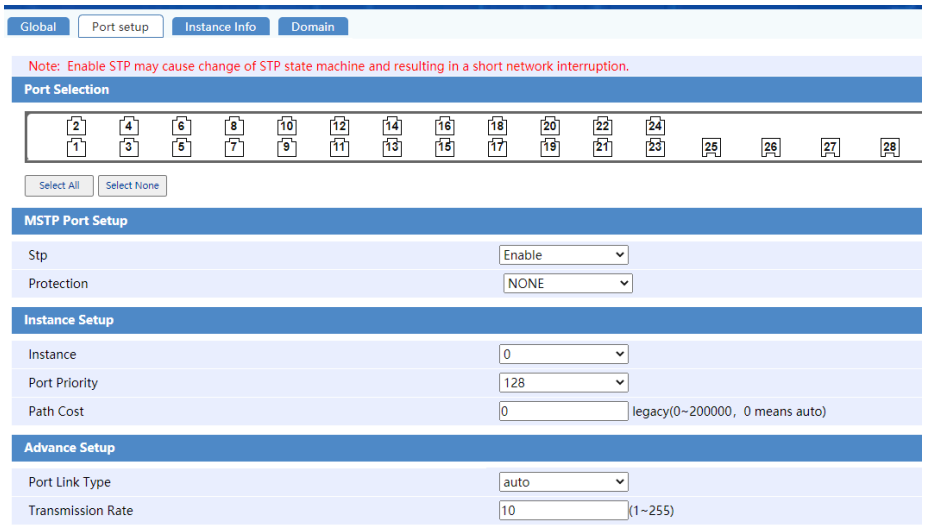
10.3.11.1 Основные настройки MSTP

Перейдите в меню: Network → MSTP → Global, на этой странице можно настроить включение/выключение функции MSTP и связанных с ней параметров.



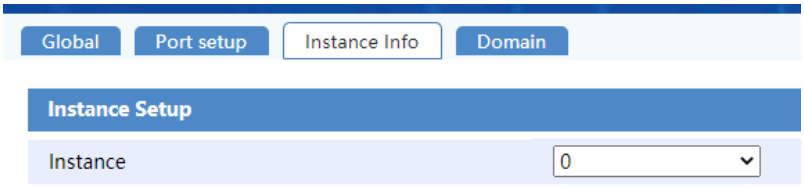
10.3.11.2 Настройки порта MSTP

Перейдите в меню: Network → MSTP → Port setup, на этой странице можно настроить функции включения/выключения порта MSTP и связанных атрибутов MSTP, как показано на следующем рисунке:



10.3.11.3 Отображение MSTP

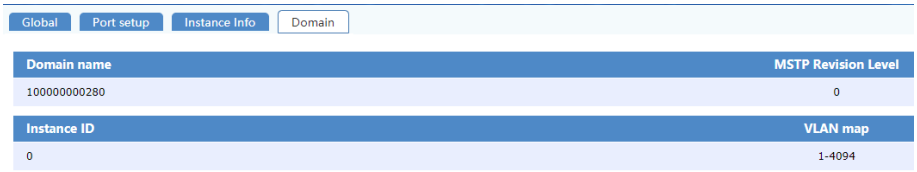
Перейдите в меню: Network → MSTP → Instance Info, на этой странице отображается информацию об MSTP.




```
-------[CIST Global Info][Mode  MSTP]-------

CIST Bridge          :32768.1000-0000-0280

Bridge Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20

CIST Root/ERPC       :32768.1000-0000-0280
 / 0

CIST RegRoot/IRPC    :32768.1000-0000-0280
 / 0

CIST RootPortId      :0.0

BPDU-Protection      :disabled

Bridge Config
Digest Snooping      :disabled

TC or TCN received   :0

Time since last TC   :0 days 0h:30m:41s


----[CIST][Port1(GigabitEthernet1/0/1)][DOWN]----

 Port Protocol       :enabled

 Port Role           :CIST Disabled  Port

 Port Priority       :128

 Port Cost[Legacy standard]    :Config=auto
 / Active=200000

 Desg. Bridge/Port   :32768.1000-0000-0280
 / 128.1
```

10.3.11.4 Отображение и модификация домена MSTP

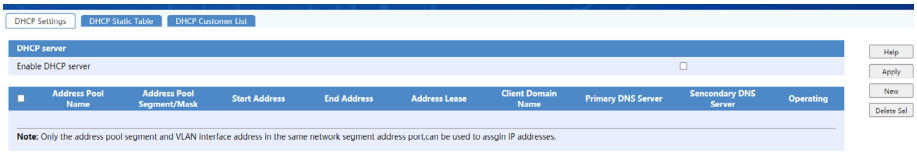
Перейдите в меню: Network → MSTP → Domain, на этой странице отображается информация о конфигурации домена MSTP. Нажмите кнопку <Modify>, чтобы изменить информацию о конфигурации домена, и измененная информация вступит в силу немедленно.



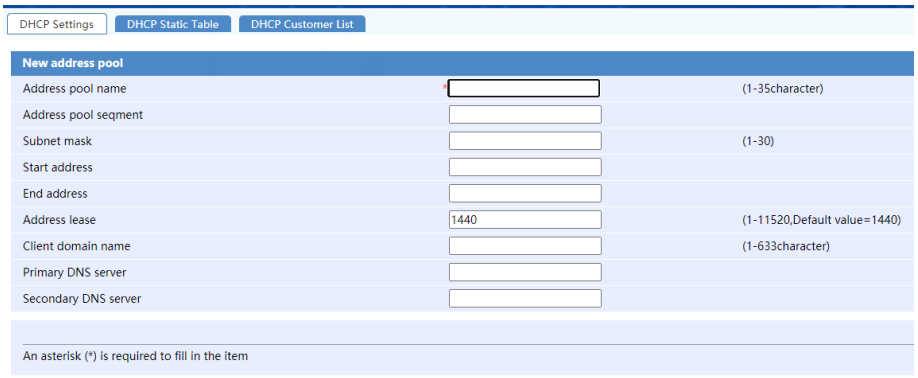
10.3.12 DHCP-сервер

10.3.12.1 Конфигурация DHCP-сервера

Перейдите в меню: Network → DHCP → DHCP settings, на этой странице можно включать/выключать функцию DHCP-сервера и отображать информацию о пуле адресов.



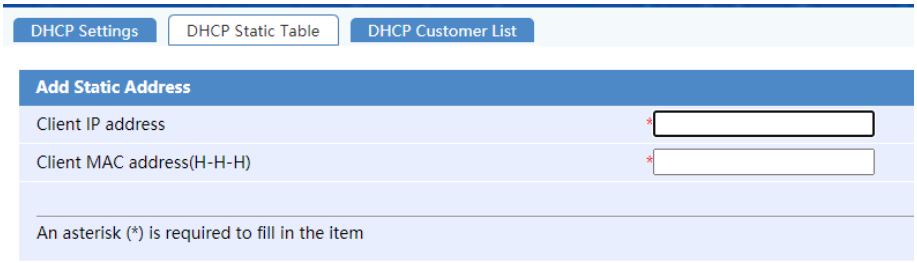
Нажмите кнопку < New > на странице, чтобы создать новый пул адресов DHCP-сервера.
Щелкните соответствующую запись пула адресов на странице настроек DHCP, чтобы перейти на страницу изменения соответствующего пула адресов.



10.3.12.2 Статическая таблица DHCP

Перейдите в меню: Network → DHCP → DHCP Static Table, на этой странице отображаться настроенные в данный момент записи статической таблицы DHCP-клиентов, или можно нажать кнопку < New >, чтобы добавить статический список DHCP-клиентов.

Нажмите кнопку < New >, чтобы добавить статический список DHCP-клиентов.



10.3.12.3 Список клиентов DHCP

Перейдите в меню: Network → DHCP → DHCP Customer List, на этой странице может отображаться список DHCP-клиентов, которые в данный момент находятся в сети.

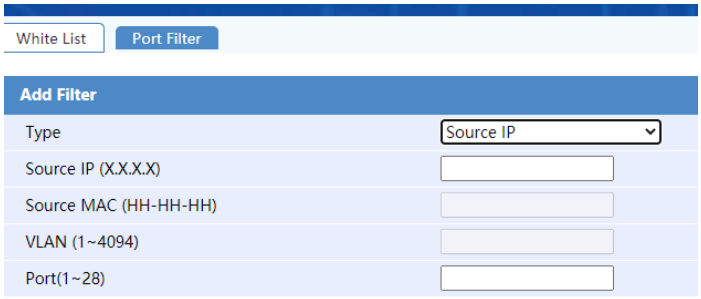
10.4 НАСТРОЙКИ БЕЗОПАСНОСТИ

Включите функцию IP-фильтра для порта, подключенного к пользовательской стороне устройства, который может фильтровать пакеты, полученные через порт, чтобы предотвратить прохождение нелегальных пакетов через порт, тем самым ограничивая незаконное использование сетевых ресурсов (например, незаконную подмену хостов), что повышает безопасность портов.

10.4.1 IP-фильтр

10.4.1.1 Отображение белого списка

Перейдите в меню: Security → IP Filter → White List, на этой странице возможно просматривать и добавлять пользователей из белого списка.



Перед включением функции фильтрации портов добавьте IP-адрес и MAC-адрес управляющего устройства в белый список на странице «White List Display Page» в разделе «Device Information».

Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Type	Доступные типы • Source IP address: просто введите IP-адрес и номер порта • Source MAC address: просто введите MAC-адрес и номер порта • Source IP address + VLAN: необходимо ввести IP-адрес и идентификатор VLAN. • Source MAC address + VLAN: необходимо ввести MAC-адрес и идентификатор VLAN. • Source IP address + MAC address + VLAN: необходимо ввести IP-адрес, MAC-адрес и идентификатор VLAN.
Source IP address	Введите IP-адрес устройства управления
Source MAC address	Введите MAC-адрес устройства управления
VLAN	Введите идентификатор VLAN
Port	Выберите номер порта для внесения в белый список

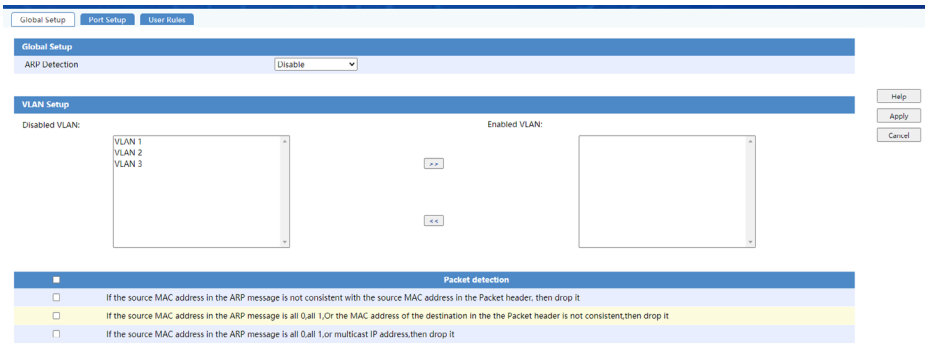
10.4.1.2 IP-фильтрация портов

Перейдите в меню: Security → IP Filter → Port IP Filter. На этой странице возможно включить/выключить функцию IP-фильтрации портов и выбрать выкл/вкл в раскрывающемся списке IP-фильтрации. Возможно выбрать <All On> или <All Off> для пакетной настройки.

10.4.2 Защита от атак ARP

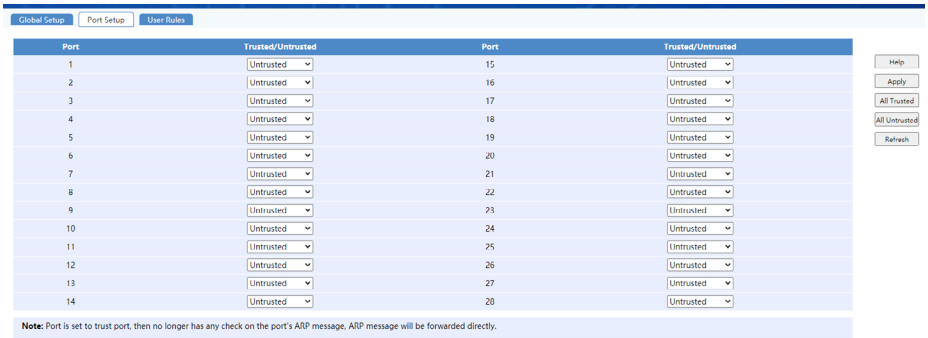
10.4.2.1 Настройка ARP

Перейдите в меню: Security → ARP Defense → Global Setup
На этой странице можно настроить включение/выключение обнаружения ARP. Поле настроек VLAN можно настроить для включения/отключения обнаружения ARP с помощью VLAN. Его также можно настроить для включения/отключения проверки достоверности различных пакетов ARP.



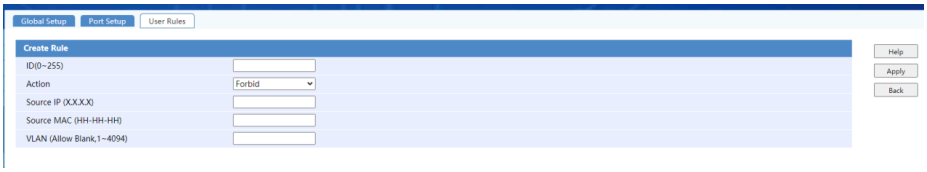
10.4.2.2 Настройки порта

Перейдите в меню: Security → ARP Defense → Port Setup
На этой странице возможно настроить, является ли порт доверенным портом для пакетов ARP.

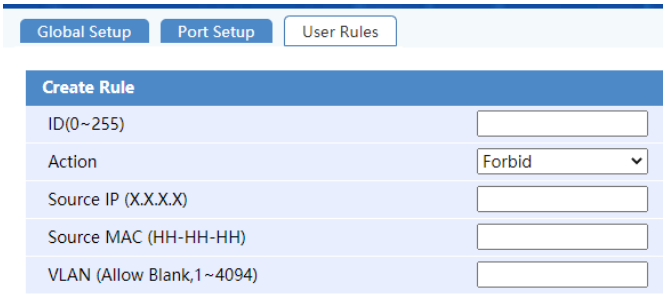


10.4.2.3 Пользовательские правила

Перейдите в меню: Security → ARP Defense → User Rules
На этой странице возможно просматривать и добавлять пользовательские правила проверки ARP. После включения проверки ARP возможно настроить правила для управления поведением пересылки пакетов ARP.



Нажмите кнопку «Create» на странице выше для добавления правила проверки ARP на основе конфигурации пользователя. Страница конфигурации показана ниже:



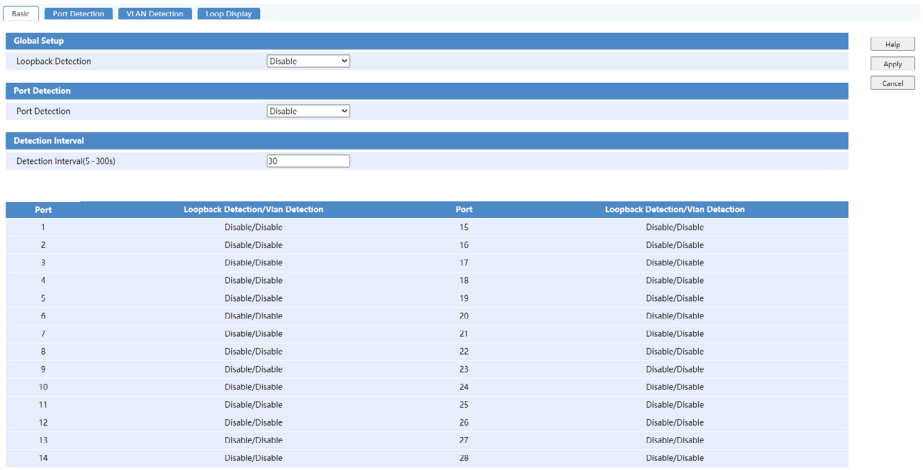
Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
ID	Идентификатор правила пользователя, диапазон значений 0~255
Action	Правила поведения, действие, которое должно быть выполнено при совпадении правила
Source IP address	Исходный IP-адрес протокола ARP
Source MAC address	Исходный MAC-адрес протокола ARP
VLAN	Введите идентификатор VLAN

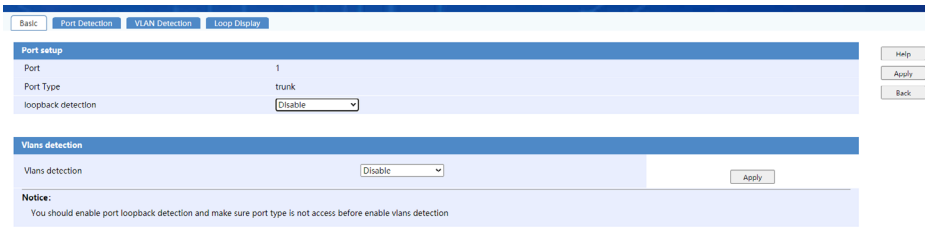
10.4.3 Обнаружение петли

10.4.3.1 Базовая конфигурация

Перейдите в меню: Security → Loop Detection → Basic
На этой странице можно настроить функцию обнаружения петель вкл/выкл, функцию включения/выключения обнаружения многопортовых петель, временной интервал обнаружения петель, а также отображение состояния обнаружения петель портов и состояния включения/выключения при обнаружении VLAN. Нажмите на нужный порт для входа в режим конфигурации.

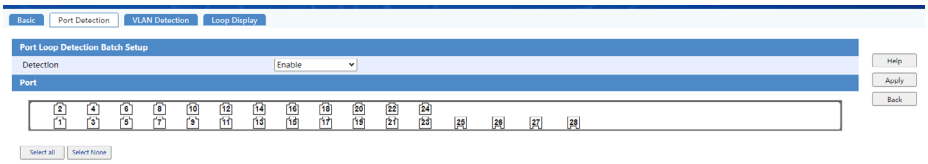


На странице конфигурации одного порта возможно указать, следует ли включать обнаружение петель на порту и включать ли функцию обнаружения VLAN.



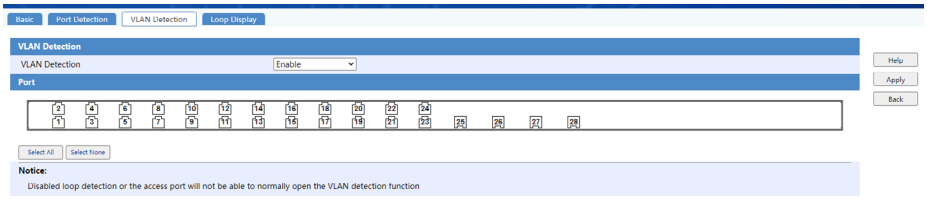
10.4.3.2 Конфигурация обнаружения петли портов

Перейдите в меню: Security → Loop Detection → Port Detection
Данная страница используется для групповой настройки функции обнаружения обрыва/замыкания петли порта.



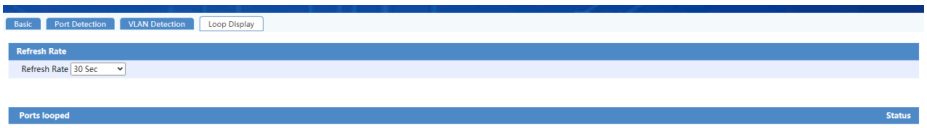
10.4.3.3 Настройка путем обнаружения VLAN

Перейдите в меню: Security → Loop Detection → VLAN Detection
На этой странице можно настроить открытие/закрытие порта с помощью функции обнаружения VLAN в пакетном режиме.



10.4.3.4 Циклическая проверка петли

Перейдите в меню: Security → Loop Detection → Loop Display
Данную страницу можно настроить для отображения частоты обновления веб-страницы состояния петли, а так же можно проверить, есть ли в порту петля, и текущее состояние порта через порт с петлей.



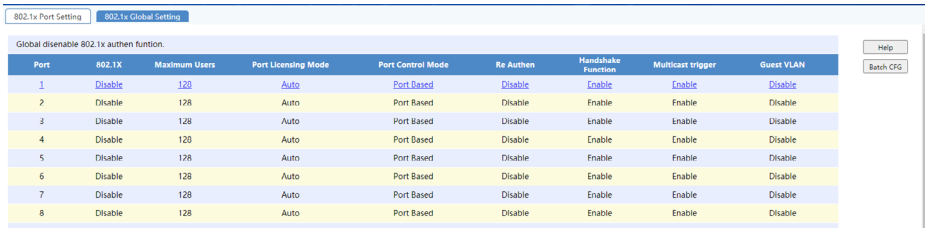
10.5 НАСТРОЙКИ АУТЕНТИФИКАЦИИ

10.5.1 Протокол 802.1X

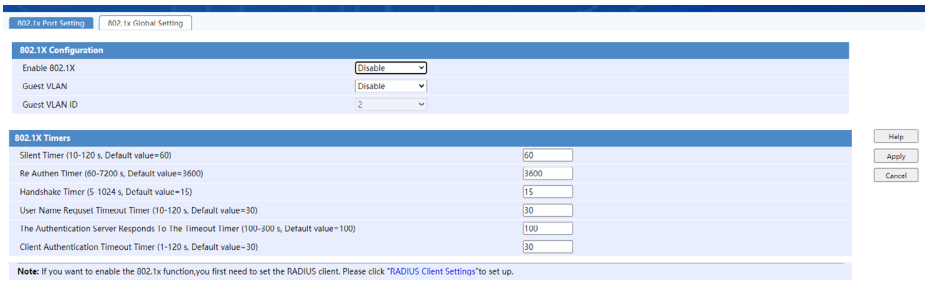
Протокол 802.1x — это протокол управления доступом и аутентификации, основанный на клиент-сервере. Он может ограничить неавторизованным пользователям/устройствам доступ к LAN/WLAN через порты доступа. Перед получением различных услуг, предоставляемых коммутатором или локальной сетью, 802.1x аутентифицирует пользователей/устройства, подключенные к порту коммутатора. Перед прохождением аутентификации 802.1x позволяет передавать только данные EAPoL (протокол расширенной аутентификации на основе локальной сети) через порт коммутатора, к которому подключено устройство; после прохождения аутентификации обычные данные могут беспрепятственно проходить через порт Ethernet.

10.5.1.1 Настройки порта 802.1X

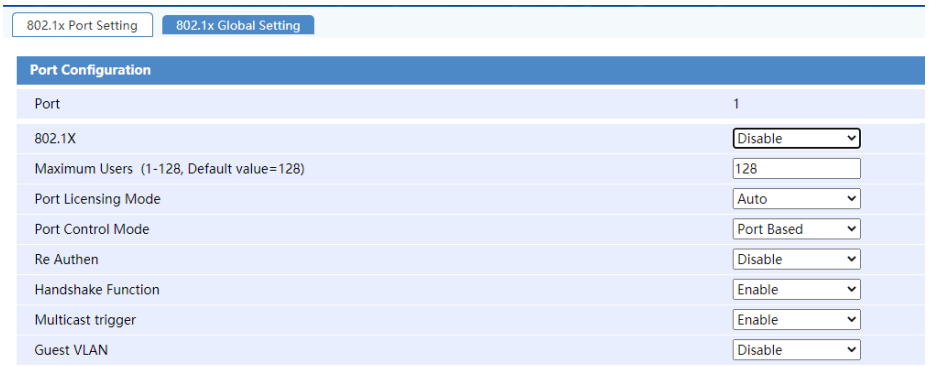
Перейдите в меню: Authentication → 802.1X → 802.1X port setting
На этой странице отображается общее состояние включения/выключения 802.1x и информация о конфигурации 802.1x для порта. Щелкните соответствующую запись порта, чтобы настроить функцию 802.1x для одного порта, и нажмите кнопку < Batch CFG >, чтобы настроить функцию порта 802.1X в пакетном режиме.



Щелкните соответствующий порт, чтобы перейти на страницу конфигурации порта:

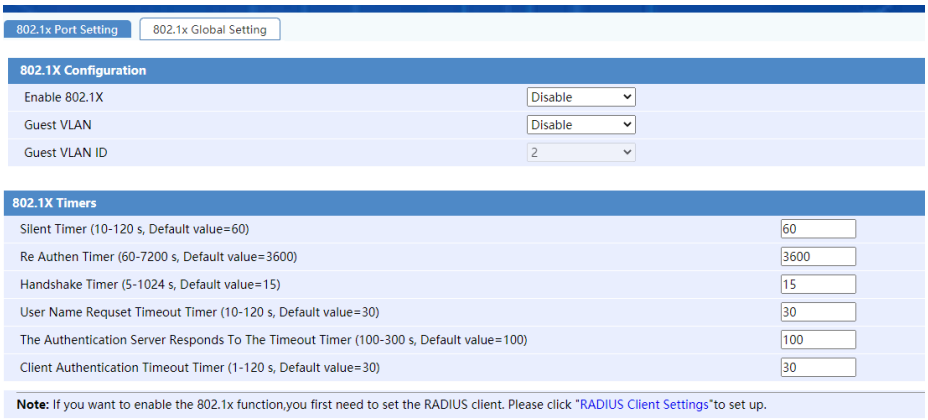


Нажмите кнопку < Batch Configuration >, чтобы настроить функции порта 802.1X в пакетном режиме:



10.5.1.2 Глобальные настройки 802.1X

Перейдите в меню: Authentication → 802.1X → 802.1X Global Settings
На этой странице можно настроить глобальную функцию 802.1x.

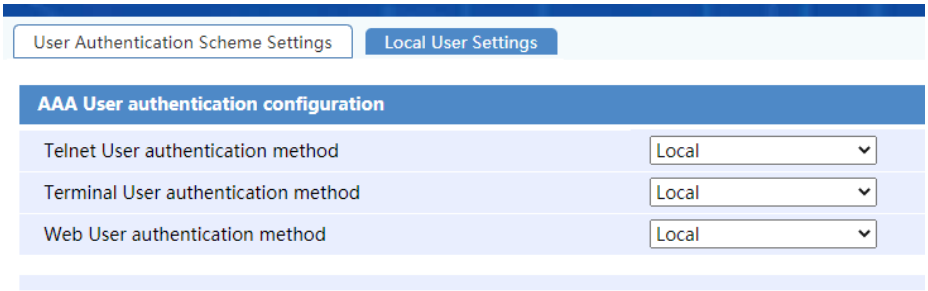


10.5.2 AAA

AAA — это сокращение от Authentication, Authorization, and Accounting (аутентификация, авторизация и учет). Это механизм управления сетевой безопасностью, обеспечивающий три функции безопасности: аутентификацию, авторизацию и учет.

10.5.2.1 Настройки схемы аутентификации пользователя

Данная страница используется для настройки схемы аутентификации для пользователей, вошедших в систему. Пользователи Telnet и пользователи терминала могут отключить аутентификацию, настроить локальную аутентификацию и удаленную аутентификацию. Веб-пользователи могут настраивать только схемы без аутентификации и локальные схемы аутентификации.



10.5.2.2 Локальные пользовательские настройки

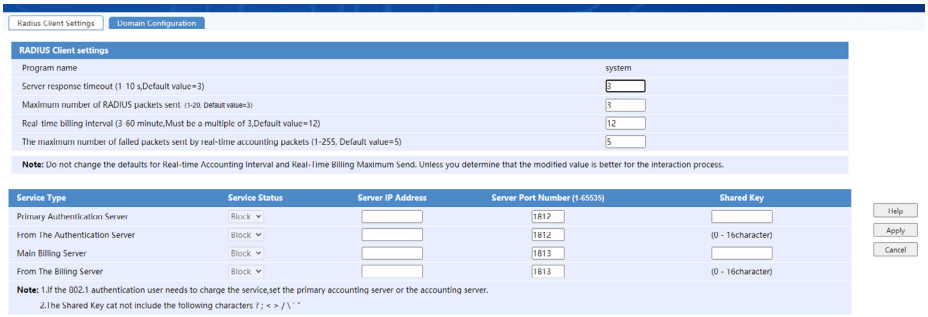
Перейдите в меню: Authentication → AAA → Local User Settings
Данная страница используется для настройки локальных пользователей (пользователей с доступом к локальной сети или пользователей входа в систему) при использовании схемы локальной аутентификации. После нажатия < Local User Settings > они фактически переходят на страницу «Device → User» для настройки. Подробнее см. на странице конфигурации «Device → User» (п.3.1.8).

10.5.3 RADIUS

RADIUS (Remote Authentication Dial-In User Service, Служба удаленной аутентификации Dial-In User Service) — это распределенный протокол взаимодействия информации со структурой клиент/сервер, который может защитить сеть от несанкционированного доступа. Он часто используется как в различных сетевых средах с высоким уровнем безопасности, так и для предоставления доступа удаленным пользователям. Протокол определяет формат сообщений RADIUS и механизм передачи сообщений, а также указывает использование UDP в качестве протокола транспортного уровня для инкапсуляции сообщений RADIUS (порты UDP 1812 и 1813 используются как порты аутентификации и учета соответственно).

10.5.3.1 Настройки клиента RADIUS

Перейдите в меню: Authentication → RADIUS → Radius Client Settings
Данная страница используется для настройки схемы RADIUS.



10.5.3.2 Конфигурация домена

Перейдите в меню: Authentication → RADIUS → DomainConfiguration
Данная страница используется для настройки домена в схеме Radius.

Нажмите кнопку <New> на странице, чтобы создать новый домен.

11. ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ, ИХ ПРИЧИНЫ И СПОСОБЫ УСТРАНЕНИЯ

НЕИСПРАВНОСТЬ	ВОЗМОЖНЫЕ ПРИЧИНЫ	СПОСОБЫ УСТРАНЕНИЯ
Не работает один из портов коммутатора (индикаторы на порте не включаются при подключении кабеля)	Неисправный кабель, либо устройства на другом конце кабеля не включено/неисправно	Проверить исправность кабеля, проверить устройство на другом конце кабеля
Отсутствует питание подключенного устройства по PoE (только для MNS-1008F2SP)	Подключен блок питания недостаточного выходного напряжения. Менее DC 48 В	Установить блок питания DC 48 В - 57 В
Не подключается к вэб-интерфейсу коммутатора	Устройства ПК и коммутатора не находятся в общей сети, не определены настройки IP-адреса ПК	Установить настройки TCP/IPv4 на компьютере

Таблица 11.1 Возможные неисправности и способы устранения

12. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

1. Общие указания

Техническое обслуживание прибора производится по следующему плану:

ПЕРЕЧЕНЬ РАБОТ	ПЕРИОДИЧНОСТЬ
Осмотр	1 раз в месяц
Контроль функционирования	1 раз в 3 месяца

Таблица 12.1 Техническое обслуживание

2. Осмотр включает в себя проверку отсутствия механических повреждений, надёжности крепления, состояния внешних монтажных проводов, контактных соединений.

3. Контроль функционирования

- При наличии напряжения хотя бы на одном из вводов питания на передней панели коммутатора должен включиться индикатор «PWR»
- При наличии соединения по портам Ethernet должны включиться соответствующие индикаторы LNK/ACT. После запуска обмена индикаторы LNK/ACT должны начать мигать, частота мигания зависит от интенсивности обмена

13. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Технические характеристики коммутаторов указаны в **Таблице 13.1**.

МОДЕЛЬ	MNS-1008F2S	MNS-1008F2SP	MNS-1008S2G
Количество входов питания	2		
Количество портов RJ-45	8		2
Количество SFP-портов	2		12
Количество портов Console	2		1
Напряжение источника питания	DC от 12 В до 48 В	DC от 48 В до 57 В	DC от 12 В до 48 В
Потребляемая мощность (максимальная)	20 Вт	120 Вт	15 Вт
Время технической готовности прибора к работе	10 секунд		
Скорость передачи данных по Ethernet	до 1 Гбит/с		
Максимальная длина кабеля UTP (витая пара), на каждый порт	100 м		
Максимальная длина оптического кабеля	20 км		
Степень защиты оболочки по ГОСТ 14254-2015	IP40		
Диапазон рабочих температур	От 0 до + 40 °С		
Температура хранения	От -15°С до +60°С		
Относительная влажность воздуха	До 80%		
Время непрерывной работы прибора	круглосуточно		
Средняя наработка прибора на отказ в дежурном режиме работы	не менее 80000 ч		
Вероятность безотказной работы	0,98758		
Средний срок службы прибора	10 лет		
Размеры (ШхВхГ)	145×134×47мм		165×147×53мм
Масса (нетто)	755 г	760 г	940 г

Таблица 13.1 Технические характеристики управляемых коммутаторов

14. ТРАНСПОРТИРОВКА И ХРАНЕНИЕ

Транспортировка и хранение коммутатора должны осуществляться только в заводской упаковке или её аналоге, удовлетворяющему требованиям данного руководства по эксплуатации.

Транспортировка коммутатора должна осуществляться в упакованном виде любым видом наземного, водного или воздушного транспортного средства при температуре окружающей среды в диапазоне от -50 °С до +50 °С и относительной влажности воздуха до 80 %, при отсутствии воздействия прямого солнечного излучения и атмосферных осадков.

Коммутатор должен храниться в упакованном виде, в сухом помещении на стеллажах или поддонах при температуре окружающей среды в диапазоне от -10 °С до +60 °С и относительной влажности воздуха до 80 %, при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей и отсутствии воздействия прямого солнечного излучения и атмосферных осадков.

Коммутатор в заводской упаковке запрещается штабелировать более чем на 10 ярусов.

Максимальная нагрузка при штабелировании, допущенная для размещения на коммутатор в заводской упаковке, составляет 20 кг.

15. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА И СЕРВИСНОЕ ОБСЛУЖИВАНИЕ

Гарантийный срок на коммутатор составляет 12 месяцев с даты приобретения. Средний срок службы коммутатора составляет не менее 10 лет с даты приобретения.
Если дату приобретения установить невозможно, то гарантийный срок и средний срок службы исчисляются от даты производства, которая указывается на этикетке.

По истечении гарантийного срока, ремонт техники осуществляется на платной основе.

При отсутствии документа, подтверждающего факт приобретения коммутатора, в бесплатном ремонте может быть отказано.

Если неисправный коммутатор был сдан в ремонт до истечения гарантийного срока, то он продлевается на время, в течение которого коммутатор находился в ремонте.

Гарантийные обязательства производителя (продавца или импортёра) не распространяются:
- На коммутатор, чьи неисправности и недостатки вызваны несоблюдением техники безопасности и условий эксплуатации, описанных в руководстве по эксплуатации, прилагаемого к оборудованию.
- На коммутатор, использованный не по назначению.
- На расходные материалы, а также на части коммутатора, неисправность которых стала результатом естественного износа.

Гарантийные обязательства не включают в себя компенсацию за демонтаж и монтаж коммутатора и другие затраты, прямо или косвенно связанные с необходимым ремонтом.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ROXTON	СЕРВИСНЫЙ ЦЕНТР ROXTON
В случае возникновения трудностей с подключением, настройкой и эксплуатацией оборудования и программного обеспечения ROXTON support@roxton.ru	Гарантийный и постгарантийный ремонт, а также техническое обслуживание оборудования ROXTON service@roxton.ru

ПРИЛОЖЕНИЕ А

(справочное)

ГАБАРИТНЫЕ РАЗМЕРЫ

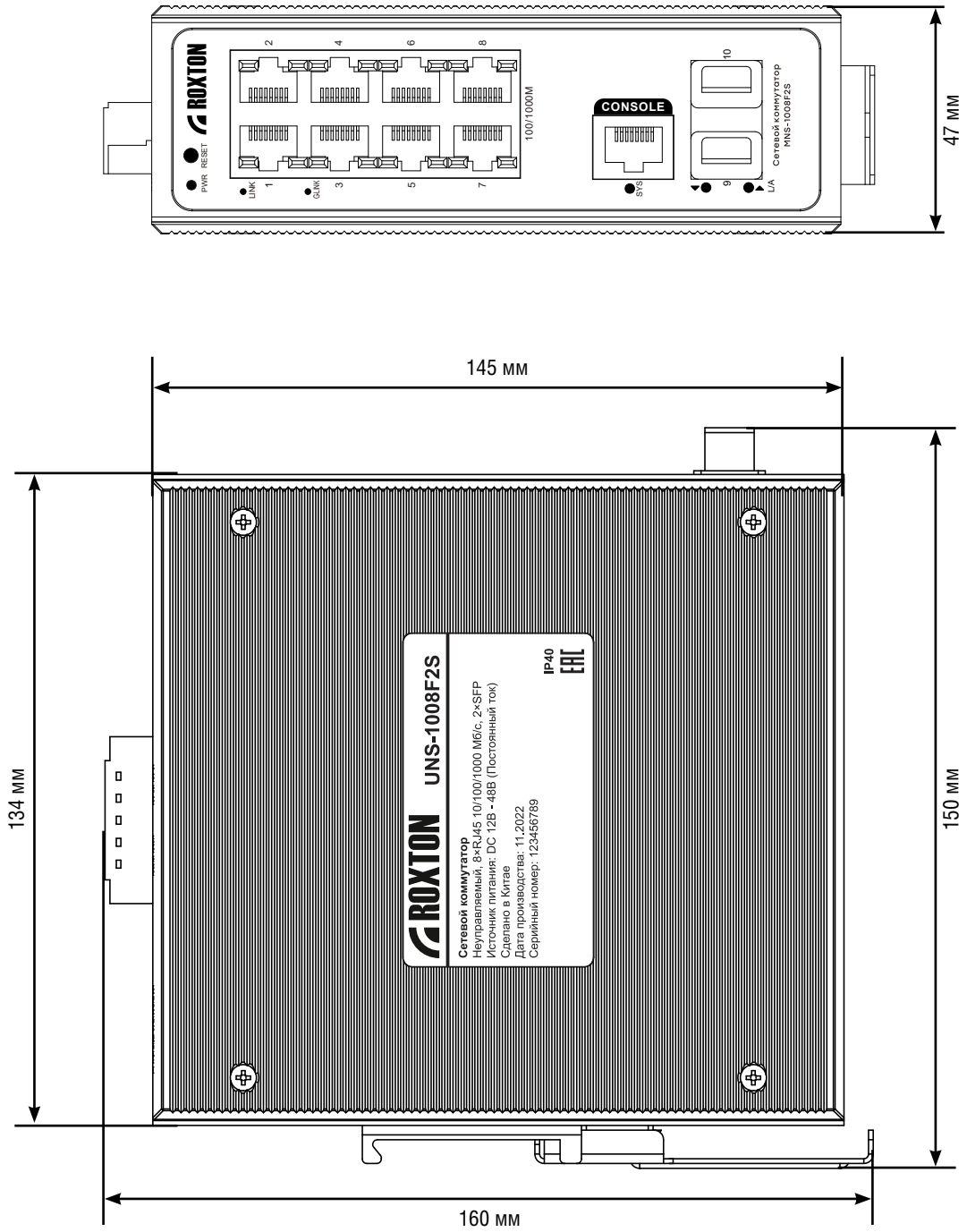


Рисунок А.1 Габаритные размеры ROXTON MNS-1008F2S / MNS-1008F2SP

ПРИЛОЖЕНИЕ А

(справочное)

ГАБАРИТНЫЕ РАЗМЕРЫ

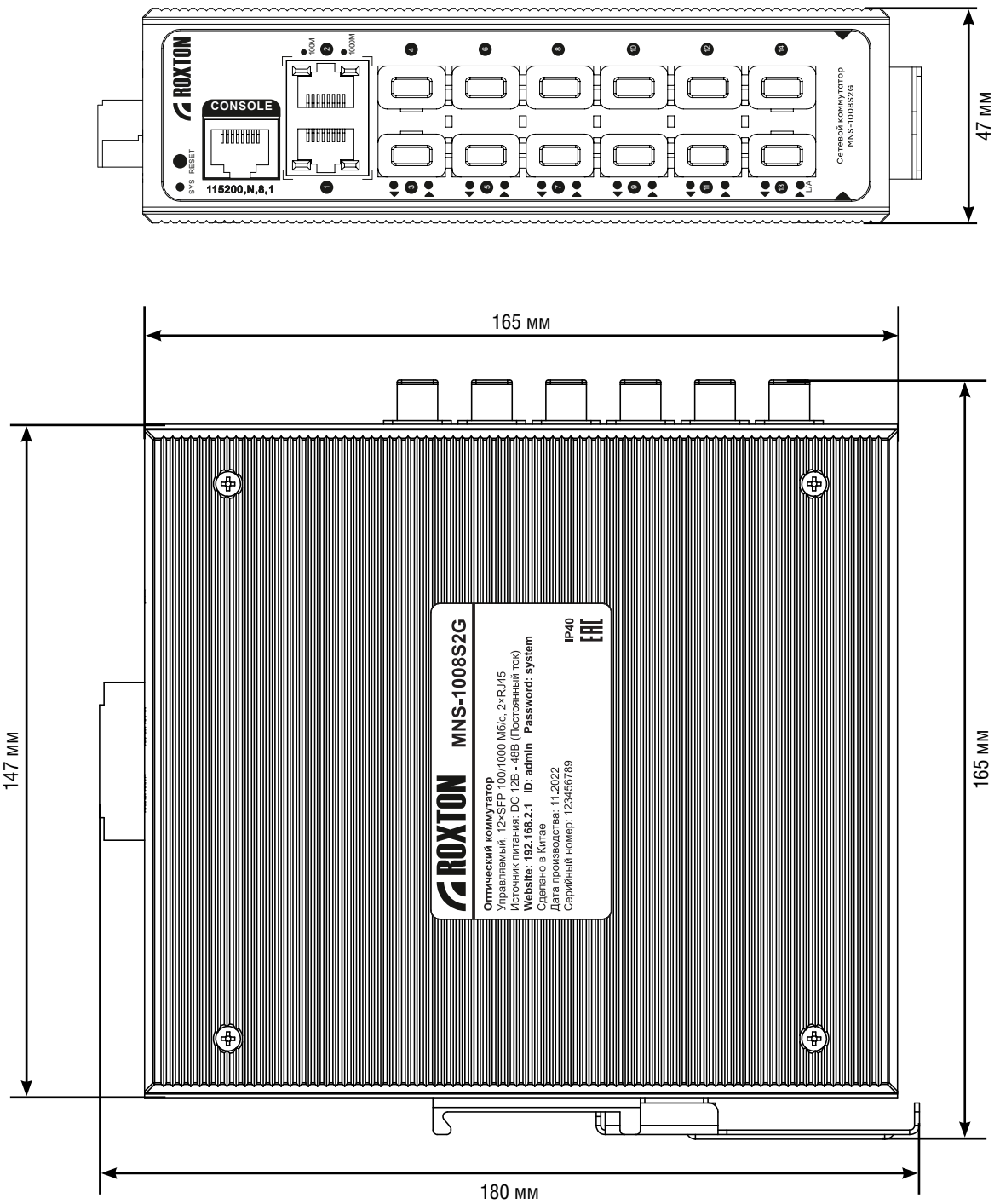


Рисунок А.1 Габаритные размеры ROXTON MNS-1008S2G

WWW.ROXTON.RU