



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 COУЭ.
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

Инструкция по технике безопасности	2
1. Оглавление	3
2. Введение	4
3. Возможности	5
4. Комплект поставки	5
5. Описание и внешний вид коммутатора	6
5.1 Передняя панель	6
5.2 Задняя панель	6
5.3 Световая индикация состояний коммутатора	7
6. Распаковка	8
7. Установка коммутатора	8
8. Подключение внешних устройств	8
9. Подключение питания	9
10. Настройка коммутатора	10
10.1 Подключение и настройка коммутатора	10
10.2 Страница веб-конфигурации.....	11
10.3 Сетевые настройки	25
10.4 Настройки безопасности	45
11. Возможные неисправности, их причины и способы устранения	53
12. Техническое обслуживание	53
13. Технические характеристики	54
14. Транспортировка и хранение	55
15. Гарантийные обязательства и сервисное обслуживание	56
Приложение А (справочное) Габаритные размеры	57

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.

Уведомление об авторских правах и товарных знаках: ROXTON / РОКСТОН являются зарегистрированными товарными знаками компании ООО «Эсорт Групп».

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

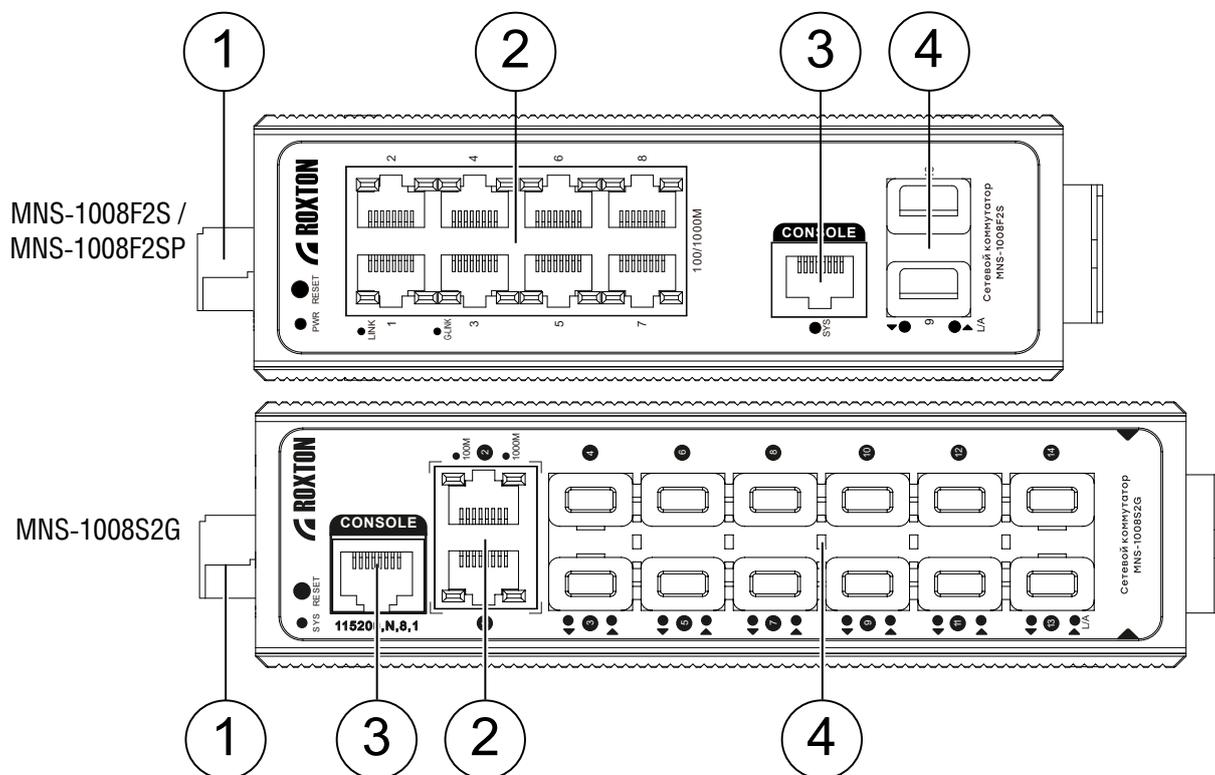
В комплект поставки коммутатора входят:

- Коммутатор (без БП¹) — 1 шт.
- Кабель-переходник RS-232 – 1 шт.

¹ Блок питания DC приобретается отдельно

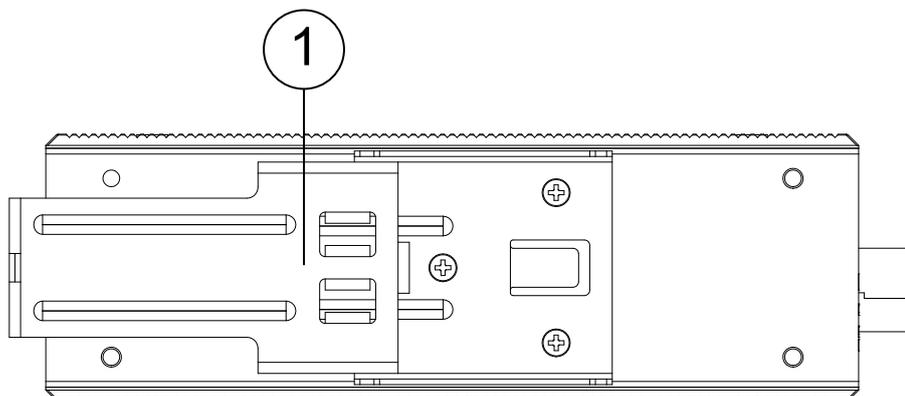
5. ОПИСАНИЕ И ВНЕШНИЙ ВИД КОММУТАТОРА

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 5е (CAT5 или CAT5е). 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 линиям 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**.

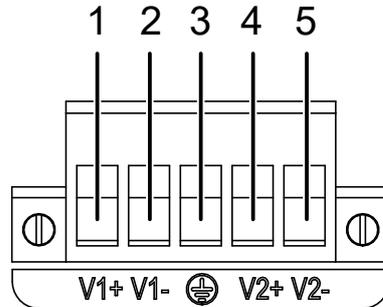


Рисунок 9 Распиновка клеммы питания

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**.

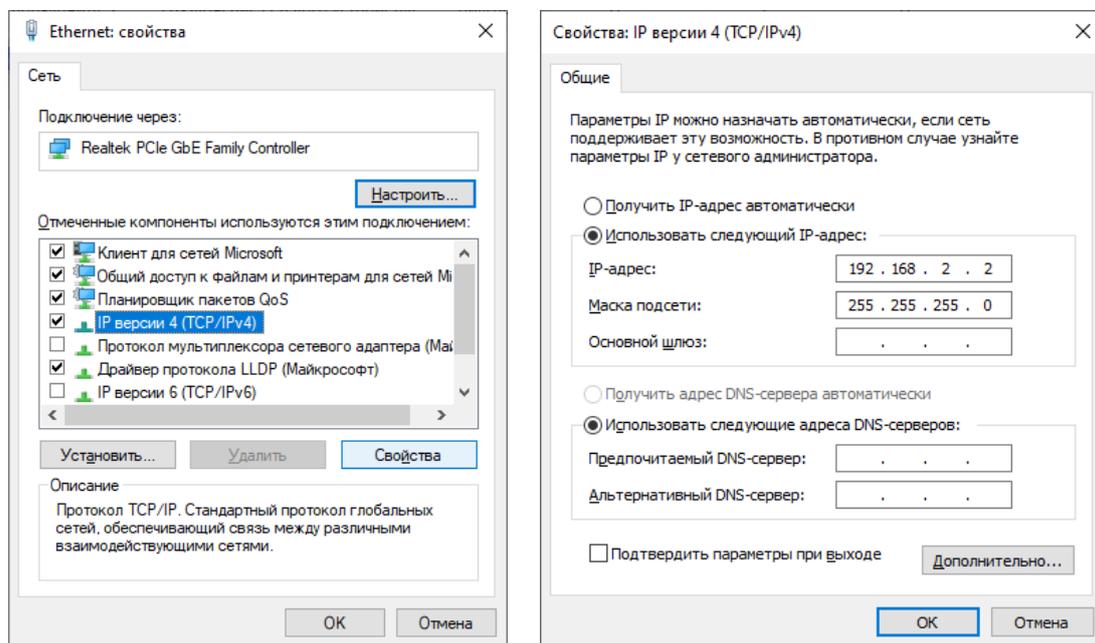


Рисунок 10.1 Настройка TCP/IPv4

Для входа в веб-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. НАСТРОЙКА КОММУТАТОРА

10.2.1.2 Техническое обслуживание оборудования

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

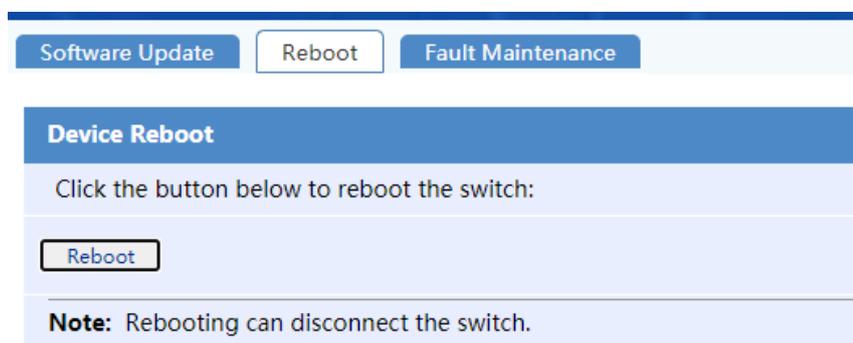
10.2.1.2.1 Обновление программного обеспечения

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

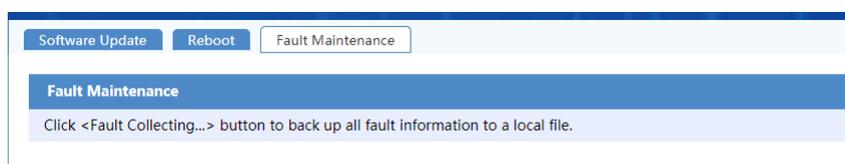
Перейдите в меню: Device → Maintenance → Reboot, страница показана на рисунке ниже. Нажмите кнопку <Reboot> для перезапуска



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.

Time/Date	Source	Level	Description
Jan 1 00:21:04 2000	WEB	Notice	LOGIN: User 'admin' logged in from 192.168.6.130.
Jan 1 00:01:02 2000	LLDP	Informational	LLDP_CREATE_NEIGHBOUR: New neighbor created on Port GigabitEthernet1/0/2 (ifindex 1), Chassis ID is 0000-1000-0009, Port ID is GigabitEthernet1/0/2.
Jan 1 00:01:01 2000	LACP	Notice	LAGG_ACTIVE: Member port GigabitEthernet1/0/2 of aggregation group BAGG1 becomes ACTIVE.
Jan 1 00:00:59 2000	LLDP	Informational	LLDP_CREATE_NEIGHBOUR: New neighbor created on Port GigabitEthernet1/0/1 (ifindex 0), Chassis ID is 0000-1000-0009, Port ID is GigabitEthernet1/0/1.
Jan 1 00:00:44 2000	STP	Critical	PFWD: Instance's Bridge-Aggregation1 has been set to forwarding state!
Jan 1 00:00:44 2000	STP	Critical	PFWD: Instance's Bridge-Aggregation1 has been set to forwarding state!

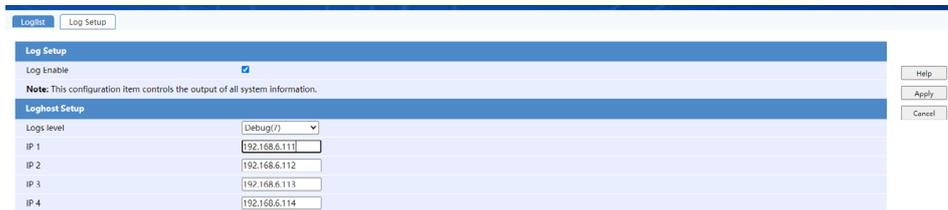
Значение ключевых элементов на странице показано в таблице ниже.

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. НАСТРОЙКА КОММУТАТОРА

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.

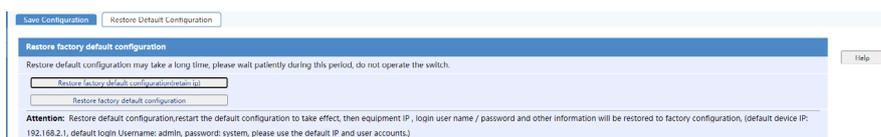
10.2.1.4.2 Восстановление конфигурации по умолчанию

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.

Port	Link Status	Speed / duplex	Priority	Flow Control	Enable/Disable	Isolation State	Energy Saving	EEE
1	1000/FULL	AUTO/AUTO	7	Disable	Enable	Disable	Disable	Disable
2	1000/FULL	AUTO/AUTO	7	Disable	Enable	Disable	Disable	Disable
3	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
4	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
5	--	AUTO/AUTO	0	Enable	Enable	Disable	Disable	Disable
6	--	AUTO/AUTO	0	Enable	Enable	Disable	Disable	Disable
7	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable

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).

Port Setup	
Port	1
Speed	Auto
Duplex	Auto
Enable/Disable	Enable
Priority	7
Flow Control	Disable
Isolation	Disable
Energy Saving	Disable
EEE	Disable

10. НАСТРОЙКА КОММУТАТОРА

Значение ключевых элементов на странице показано в таблице ниже.

ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Speed	Настроить скорость порта
Duplex	<p>В дуплексном режиме порта возможны три ситуации:</p> <ul style="list-style-type: none">• 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. <p>По умолчанию скорость и дуплексный режим порта — (Auto) автосогласование.</p>
Enable/Disable	Включить/выключить порт. Если порт отображается закрытым, он не может пересылать данные. По умолчанию порт открыт
Priority	<p>Уровень приоритета порта составляет от 0 до 7, где 0 — самый низкий, а 7 — самый высокий.</p> <p>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</p> <p>По умолчанию приоритет порта равен 0.</p>
Flow Control	<p>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.</p> <p>По умолчанию управление потоком портов отключено.</p>
Isolation	<p>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.</p> <p>По умолчанию порт не добавляется в группу изоляции.</p>
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».

Port	Mirroring Direction	Port	Mirroring Direction
1	None	27	None
2	None	28	None
3	None	29	None
4	None	30	None
5	Both	31	None
6	None	32	None
7	None	33	None

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	<p>Выберите зеркальный порт, «None» означает, что порт не зеркальный</p> <p>Смысл направления зеркального отражения следующий:</p> <ul style="list-style-type: none"> 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. НАСТРОЙКА КОММУТАТОРА

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.

	User Name	Group Name	Authentication Mode	Privacy Mode	Operation
<input type="checkbox"/>	NRA	1	None	None	<input type="button" value="Delete"/>

Note: Only SNMPv3 support user setting.

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.

Add SNMP User	
User Name	<input type="text"/> (1-32 Chars)
Security Level	<input type="text" value="NoAuth/NoPriv"/>
Group Name	<input type="text" value="1(NoAuth/NoPriv)"/>
Authentication Mode	<input type="text" value="MD5"/>
Authentication Password	<input type="text"/> (1-32 Chars)
Confirm Authentication Password	<input type="text"/> (1-32 Chars)
Privacy Mode	<input type="text" value="DESS56"/>
Privacy Password	<input type="text"/> (1-32 Chars)
Confirm Privacy Password	<input type="text"/> (1-32 Chars)

Items marked with an asterisk (*) are required

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.

SNMP Trap						
	Destination IP Address	Security Name	UDP Port	Security Model	Security Level	Operation
<input checked="" type="checkbox"/>	192.168.6.111	public	162	v3	NoAuth/NoPriv	<input type="button" value="Delete"/>

Note: Security name must be SNMPv1/SNMPv2 community name or SNMPv3 username.

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.

Add Trap Target Host	
Destination IP Address	<input type="text"/> *
Security Name	<input type="text"/> (1-32chars) *
UDP Port	<input type="text" value="162"/> (1-65535, Default=162) *
Security Model	<input type="text" value="V1"/>
Security Level	<input type="text" value="NoAuth/NoPriv"/>

Items marked with an asterisk (*) are required

10. НАСТРОЙКА КОММУТАТОРА

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.

The screenshot shows the 'Users' management interface. At the top, there is a 'Web User Setup' section with the following fields:

- Timeout (5-60 minutes): 60
- Login Authentication: enable
- Login Verify Code: Disable

Below this is a table of users:

	Username	State	Access Level	Delete
<input type="checkbox"/>	admin	Active	Administrator	Delete
<input type="checkbox"/>	1	Active	Administrator	Delete
<input type="checkbox"/>	2	Active	Administrator	Delete
<input type="checkbox"/>	3	Active	Administrator	Delete
<input type="checkbox"/>	4	Active	Administrator	Delete

On the right side, there are buttons for 'Help', 'Apply', 'New', and a status indicator '(3) Selected'.

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.

The screenshot shows the 'Create User' form with the following fields:

- Username: (1-32 Chars)
- Password: (0-32 Chars)
- Confirm Password: (0-32 Chars)
- State: Block
- Access Level: Adminis
- Service Type: Telnet Web Lan-access

Notes:

1. Username comprises letters, numbers and underline.
2. Password cannot contain space or any of the following characters ; ? ' "

Изменение локальных пользователей:

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

The screenshot shows the 'Modify User' form for the user 'admin'. The fields are:

- Username: admin
- Password: Password Modify
- State: active
- Access Level: Adminis
- Service Type: Telnet Web Lan-access

Note: Password cannot contain space or any of the following characters ; ? ' "

Значение ключевых элементов на странице показано в таблице ниже.

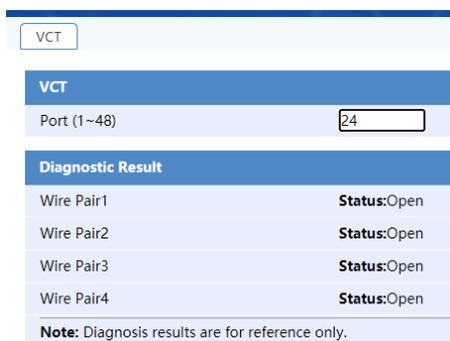
ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Timeout(5-60 minutes)	Настройка времени ожидания страницы веб-настроек, по умолчанию 5 минут
Login Authentication	Включить/выключить функцию аутентификации пользователя. После закрытия пользователю не нужно проходить верификацию при входе в систему
Login Verify Code	Включить/выключить 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 порта.

Перейдите в меню: Device → VCT

Введите номер порта для диагностики в текстовом поле «Port» и нажмите кнопку <Apply>, чтобы завершить диагностику кабеля порта.



VCT	
Port (1~48)	24
Diagnostic Result	
Wire Pair1	Status:Open
Wire Pair2	Status:Open
Wire Pair3	Status:Open
Wire Pair4	Status:Open
Note: Diagnosis results are for reference only.	

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. НАСТРОЙКА КОММУТАТОРА

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).

Received Statistics	
Total Packets	2092
Total Bytes	297816
Broadcast Packets	142
Multicast Packets	1950
Pause Frame	0
Received Packet Errors	0
Runts Packet Errors	0
Giants Packet Errors	-
CRC Packet Errors	0
Frame Packet Errors	0

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: <ul style="list-style-type: none"> • 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.

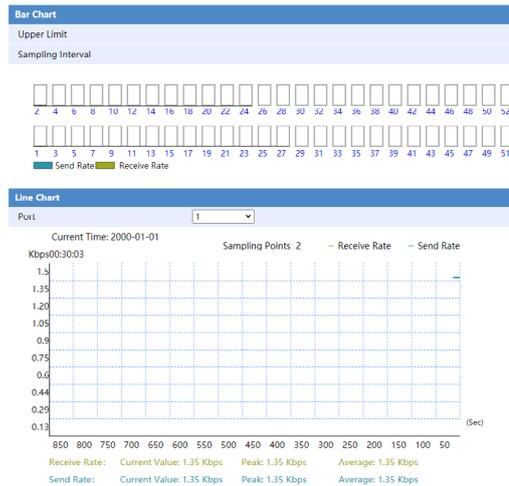
10.2.1.10.2 Статистика порта

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:

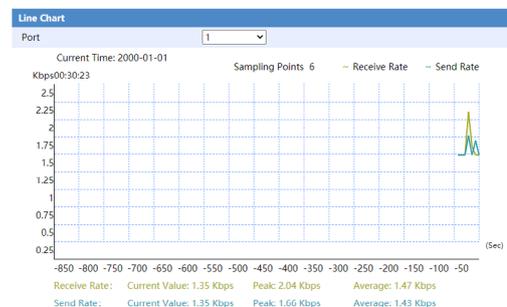
- Гистограмма мониторинга потока: используйте гистограмму для отображения состояния текущей скорости приема и скорости отправки каждого порта.
- Линейная диаграмма мониторинга потока: отображение изменения потока указанного порта за определенный период времени в виде линейных колебаний.

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 обновления 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.

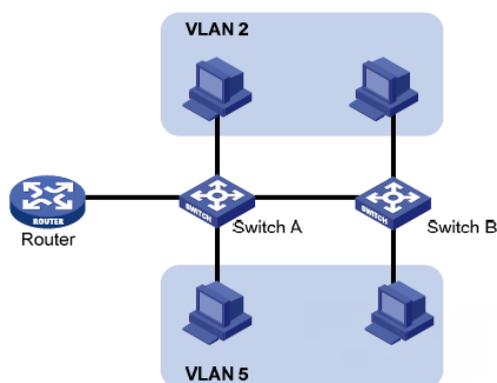


Страница линейной диаграммы мониторинга потока может выполнять следующие функции:

- 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)

VLAN ID	Description	Port List	Delete	
<input type="checkbox"/>	1	VLAN0001	1-52	Delete
<input type="checkbox"/>	2	VLAN0002	1-6	Delete
<input type="checkbox"/>	3	VLAN0003	1-6	Delete
<input type="checkbox"/>	4	VLAN0004		Delete
<input type="checkbox"/>	5	VLAN0005		Delete
<input type="checkbox"/>	7	VLAN0007		Delete
<input type="checkbox"/>	8	VLAN0008		Delete
<input type="checkbox"/>	9	VLAN0009		Delete
<input type="checkbox"/>	22	VLAN0022		Delete

1 - 9 of 9 records on total 1 pages

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).

802.1Q VLAN | Trunk | Hybrid

VLAN Create

VLAN ID: (Example: 3-5, 8, 10)

VLAN Description: (0-32 Chars)

Available Ports:

Included Ports:

Help | Apply | Back

You can move an available port to the included ports to add the port to the VLAN, or remove a port from the included ports to remove the port from the VLAN. If you create a VLAN range, ports are not configurable.

10. НАСТРОЙКА КОММУТАТОРА

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).

802.1Q VLAN Trunk Hybrid

VLAN Create

VLAN ID: 2 (Example: 3-5, 8, 10)

VLAN Description: (0-32 Chars)

Available Ports: Port9, Port10, Port11, Port12, Port13, Port14, Port15, Port16, Port17, Port18

Included Ports: Port7, Port8

Help, Apply, Back

You can move an available port to the Included ports to add the port to the VLAN, or remove a port from the Included ports to remove the port from the VLAN. If you create a VLAN range, ports are not configurable.

10.3.2 Настройка Trunk порта

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

802.1Q VLAN Trunk Hybrid

Port	PVID	Permit VLAN	Delete

Help, Create, Del Selected

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.

802.1Q VLAN Trunk Hybrid

Trunk Add

Trunk Port (1-52): 2

PVID (1-4094): 1

Trunk

VLAN ALL:

VLAN (1-4094): 1

Note:

Trunk: You can input multiple port numbers separated by commas, and number ranges by using hyphens (for example 3-7).

PVID: 1-4094.

VLAN: You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

Help, Apply, Back

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.

802.1Q VLAN Trunk Hybrid

Port	PVID	Permit VLAN	Delete
<input type="checkbox"/>	1	2	T: 1,3 U: 2
<input type="checkbox"/>	2	2	T: 1,3 U: 2
<input type="checkbox"/>	3	2	T: 1,3

Help, Create, Del Selected

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.

VLAN ID	Physical State	Protocol State	Method	IPv4 Address/Mask	Description
1	up	up	Manual	192.168.6.48/24	Vlan-interface1 Interface

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:



VLAN ID	Physical State	Protocol State	Method	IPv4 Address/Mask	Description
1	up	up	Manual	192.168.6.48/24	Vlan-Interface1 Interface

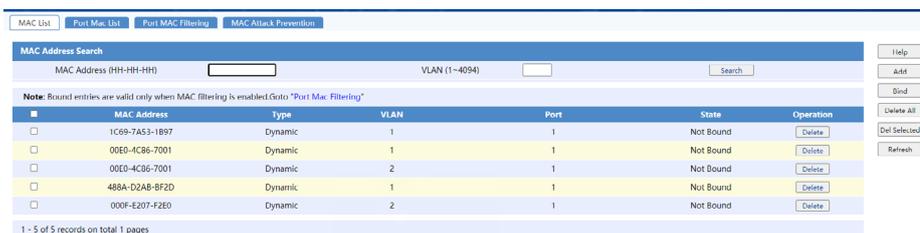
10.3.4 Настройки MAC-адреса

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

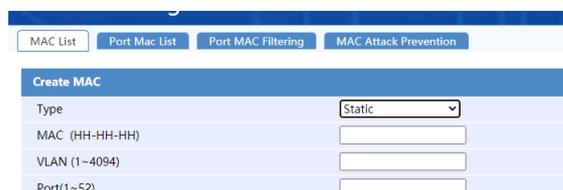
Перейдите в меню: Network → MAC Filter → MAC List, страница показана на рисунке ниже, можно отображать и запрашивать (через комбинацию MAC-адреса и условий VLAN) всю информацию таблицы MAC-адресов устройства и указанного MAC-адреса. элемент таблицы адресов Bind (выберите запись для привязки на главной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



MAC Address	Type	VLAN	Port	State	Operation
1C69-7A53-1B97	Dynamic	1	1	Not Bound	Delete
00E0-4C86-7001	Dynamic	1	1	Not Bound	Delete
00D0-4C86-7001	Dynamic	2	1	Not Bound	Delete
488A-D2AB-BF2D	Dynamic	1	1	Not Bound	Delete
000F-E207-F2E0	Dynamic	2	1	Not Bound	Delete

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.



Type	Static
MAC (HH-HH-HH)	
VLAN (1-4094)	
Port(1-52)	

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 <ul style="list-style-type: none"> 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)

MAC List | Port Mac List | Port MAC Filtering | MAC Attack Prevention

Select Ports

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

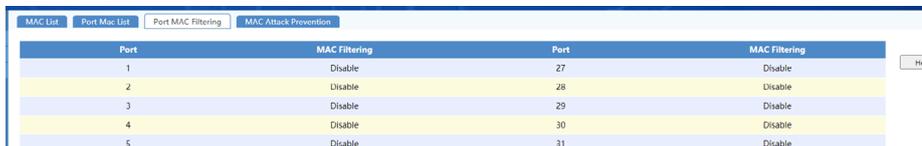
Note: Bound entries are valid only when MAC filtering is enabled.

	MAC Address	Type
<input type="checkbox"/>	1C69-7A53-1B97	Dynamic
<input type="checkbox"/>	00E0-4C86-7001	Dynamic
<input type="checkbox"/>	00E0-4C86-7001	Dynamic
<input type="checkbox"/>	488A-D2AB-BF2D	Dynamic
<input type="checkbox"/>	000F-E207-F2E0	Dynamic

1 - 5 of 5 records on total 1 pages

10.3.4.3 Настройка фильтрации MAC-адресов портов

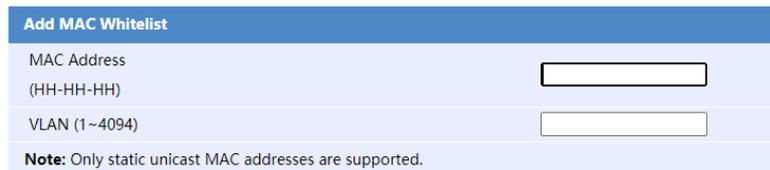
Перейдите в меню: Network → MAC Filter → Port MAC Filtering, отображение состояния функции фильтрации MAC-адресов каждого порта.



Port	MAC Filtering	Port	MAC Filtering
1	Disable	27	Disable
2	Disable	28	Disable
3	Disable	29	Disable
4	Disable	30	Disable
5	Disable	31	Disable

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.



Add MAC Whitelist

MAC Address (HH-HH-HH)

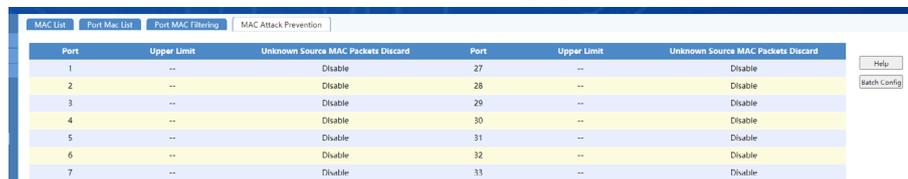
VLAN (1-4094)

Note: Only static unicast MAC addresses are supported.

10.3.4.4 Настройка защиты от атаки по MAC-адресу

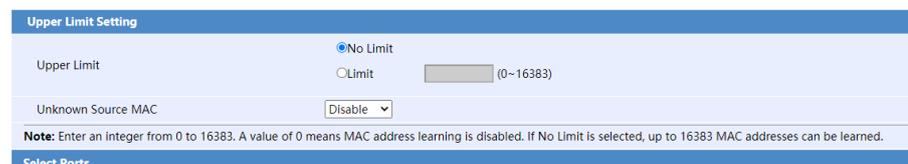
Функция защиты от атаки по MAC-адресам предотвращает постоянную фильтрацию устройством MAC-адресов большого количества недопустимых пакетов в локальной сети, что делает таблицу переадресации MAC-адресов устройства слишком большой, что приводит к резкому снижению производительности пересылки. Коммутатор 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.



Port	Upper Limit	Unknown Source MAC Packets Discard	Port	Upper Limit	Unknown Source MAC Packets Discard
1	--	Disable	27	--	Disable
2	--	Disable	28	--	Disable
3	--	Disable	29	--	Disable
4	--	Disable	30	--	Disable
5	--	Disable	31	--	Disable
6	--	Disable	32	--	Disable
7	--	Disable	33	--	Disable

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



Upper Limit Setting

Upper Limit No Limit Limit

Unknown Source MAC

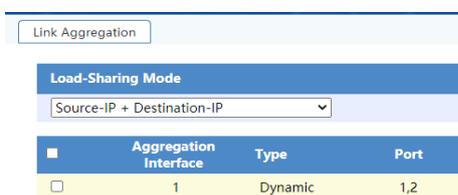
Note: Enter an integer from 0 to 16383. A value of 0 means MAC address learning is disabled. If No Limit is selected, up to 16383 MAC addresses can be learned.

Select Ports

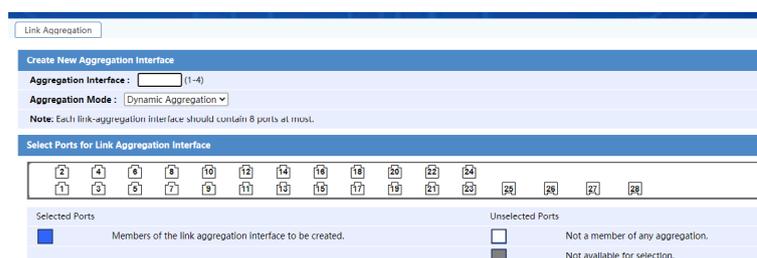
Пакетная настройка количества MAC-адресов, которые могут быть изучены указанным портом. Нажмите кнопку < Batch Config > на главной странице, чтобы перейти на соответствующую страницу.

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	<p>Выберите алгоритм агрегации коммутатора:</p> <ul style="list-style-type: none"> 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. НАСТРОЙКА КОММУТАТОРА

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.

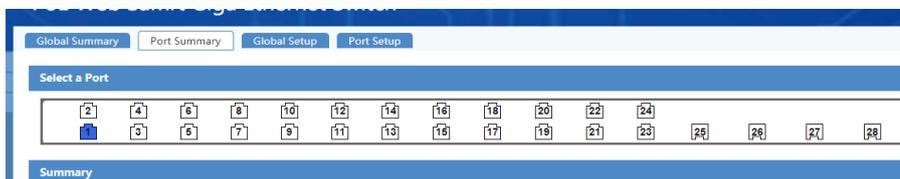


The screenshot shows the 'Global Summary' page with four tabs: 'Global Summary', 'Port Summary', 'Global Setup', and 'Port Setup'. The 'Global Summary' tab is active. Below the tabs is a table with the following data:

Global Information	
Added Neighbor:	0
Deleted Neighbor:	0
Discarded LLDP's Packet:	0
Aged Neighbor:	0

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.



The screenshot shows the 'Global Setup' page with four tabs: 'Global Summary', 'Port Summary', 'Global Setup', and 'Port Setup'. The 'Global Setup' tab is active. Below the tabs is a 'Global Settings' section with the following configuration:

LLDP	Disablec
Transmit Interval	30 (5-32768 Sec)
TTL Hold Multiplier	4 (2-10)
Fast Count	3 (1-10)
Initialization Delay	2 (1-10 Sec)
Send Packet Delay	2 (1-8192 Sec)
Trap Interval	5 (5-3600 Sec)

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: <ul style="list-style-type: none"> 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

10. НАСТРОЙКА КОММУТАТОРА

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.

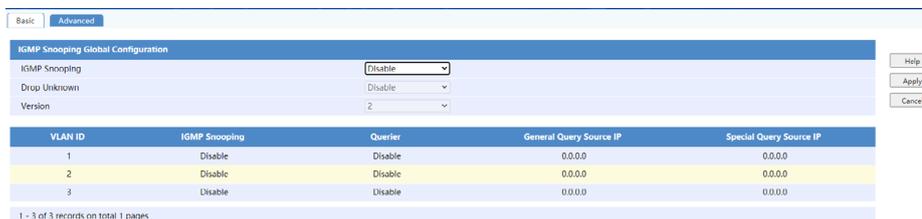
После настройки приведенной выше информации нажмите кнопку <Apply>, чтобы применить ее.

10.3.6 IGMP Snooping

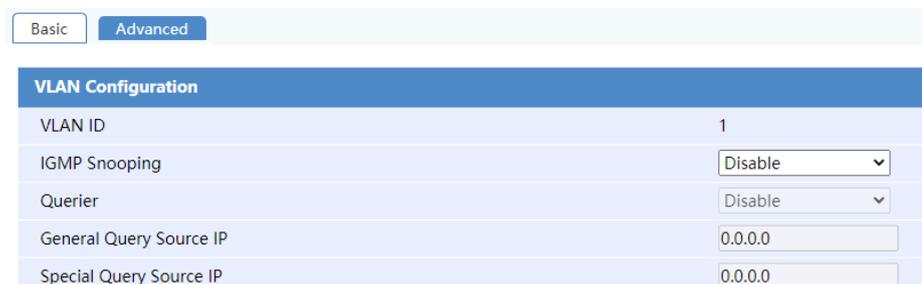
IGMP (Internet Group Management Protocol) - протокол управления групповой (multicast) передачей данных в IP-сетях. IGMP используется маршрутизаторами и хостами для организации присоединения сетевых устройств к группам многоадресной рассылки (multicast). Устройство уровня 2, на котором выполняется отслеживание 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).

Port	Fast Leave	Multicast Group Limit
1	Disable	256
2	Disable	256
3	Disable	256
4	Disable	256
5	Disable	256
6	Disable	256

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

Basic Advanced

Port Number

Port 1

Advanced

Fast Leave

Multicast Group Limit(1~256)

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 ask, 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.

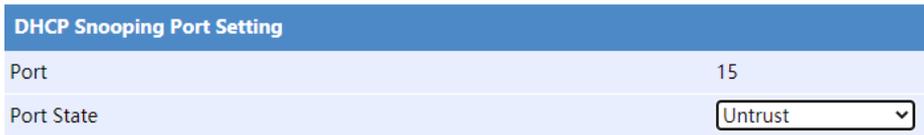
Port	Port State	Port	Port State
1	Untrust	15	Untrust

10. НАСТРОЙКА КОММУТАТОРА

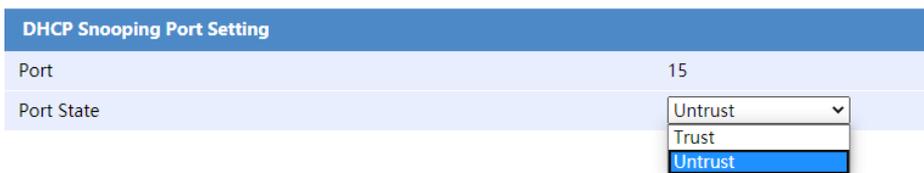
10.3.7.2 Конфигурация порта DHCP Snooping

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.



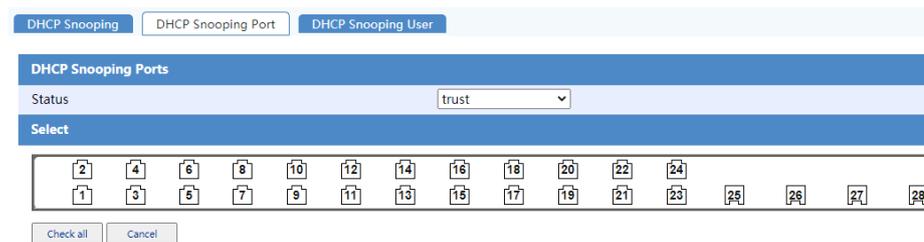
DHCP Snooping Port Setting	
Port	15
Port State	Untrust



DHCP Snooping Port Setting	
Port	15
Port State	Untrust

Установка портов:

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



DHCP Snooping | DHCP Snooping Port | DHCP Snooping User

DHCP Snooping Ports

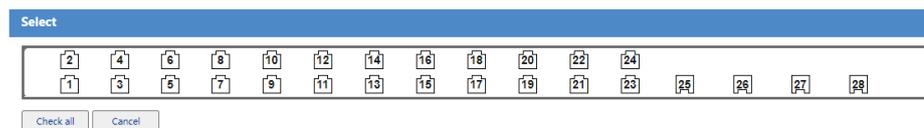
Status: trust

Select

2	4	6	8	10	12	14	16	18	20	22	24				
1	3	5	7	9	11	13	15	17	19	21	23	25	26	27	28

Check all Cancel

В столбце Select можно выбирать порты пакетами.



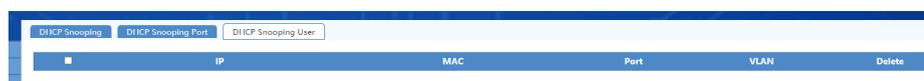
Select

2	4	6	8	10	12	14	16	18	20	22	24				
1	3	5	7	9	11	13	15	17	19	21	23	25	26	27	28

Check all Cancel

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.



DHCP Snooping | DHCP Snooping Port | DHCP Snooping User

IP	MAC	Port	VLAN	Delete
----	-----	------	------	--------

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).

Ports Rate Limit					
Port	Inbound	Outbound	Port	Inbound	Outbound
1	--	--	15	--	--
2	--	--	16	--	--
3	--	--	17	--	--
4	--	--	18	--	--
5	--	--	19	--	--
6	--	--	20	--	--
7	--	--	21	--	--
8	--	--	22	--	--
9	--	--	23	--	--
10	--	--	24	--	--
11	--	--	25	--	--
12	--	--	26	--	--
13	--	--	27	--	--
14	--	--	28	--	--

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.

Ports Rate Limit					
Port	Inbound	Outbound	Port	Inbound	Outbound
1	--	--	15	--	--
2	--	--	16	--	--
3	--	--	17	--	--
4	--	--	18	--	--
5	--	--	19	--	--
6	--	--	20	--	--
7	--	--	21	--	--
8	--	--	22	--	--
9	--	--	23	--	--
10	--	--	24	--	--
11	--	--	25	--	--
12	--	--	26	--	--
13	--	--	27	--	--
14	--	--	28	--	--

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.

Priority	0	1	2	3	4	5	6	7	Weight
Q1(lowest)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	1
Q2(low)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2
Q3(high)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	4
Q4(highest)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	8					

Explain: 1. Eight COS priorities are divided into 4 groups. Each group has two priorities and corresponds to a queue. The mapping relations are as follows: (Queue 1: priorities 1 and 2), (Queue 2: priorities 0 and 3), (Queue 3: priorities 4 and 5), and (Queue 4: priorities 6 and 7).
2. The four queues can be assigned weights, which can be classified into 31 levels.

Значение ключевых элементов на странице показано в таблице ниже.

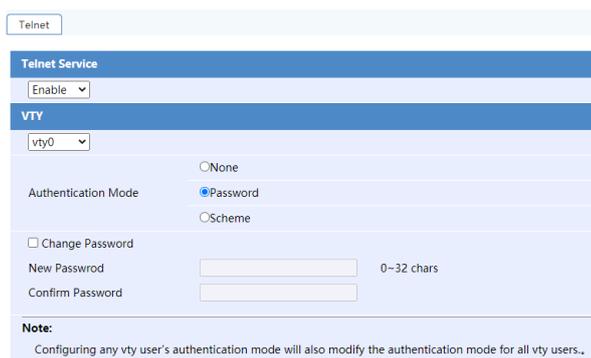
ОПЕРАЦИЯ	ОБЪЯСНЕНИЕ
Priority	<p>Выберите режим приоритета доверия:</p> <ul style="list-style-type: none"> COS: Поместите пакет в очередь вывода порта соответствующего приоритета в соответствии с приоритетом 802.1p. DSCP: Поместите пакет в очередь вывода порта с соответствующим приоритетом в соответствии с приоритетом DSCP. <p>По умолчанию коммутатор помещает пакеты в очередь вывода порта соответствующего приоритета в соответствии с приоритетом 802.1p.</p>
Scheduling Mode	<p>Выберите режим планирования очереди.</p> <p>По умолчанию коммутатор использует алгоритм планирования WRR.</p> <p>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.</p>
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

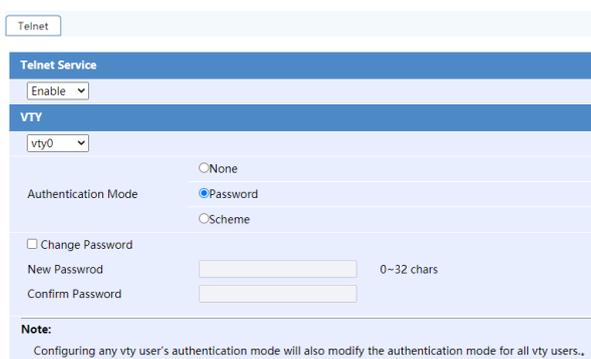
Перейдите в меню: Network → Telnet → Telnet service, в разделе Служба Telnet возможно включить/отключить функцию Telnet.



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 различия 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.

VLAN ID	Template ID	Protocol Type	Associated Port	Delete
---------	-------------	---------------	-----------------	--------

10.3.10.2 Новый протокол VLAN

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

Description:

1. You can use optional port list port to port VLAN protocol related list the related VLAN protocol or VLAN protocol;connection port list port to port optional list,which is removed from the protocol in VLAN.
2. The specified VLAN must exist,otherwise the protocol VLAN will not be created.
3. Only the hybrid port can become an optional port,and the port must be part of the VLAN to succeed with the protocol 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.

Protocol VLAN

Protocol VLAN add

VLAN ID	<input type="text" value=""/>	(1-4094)
Template ID	<input type="text" value=""/>	(0-7, Do not fill in automatically assign ID)
Protocol Type	<input type="text" value="IPv4"/>	
EthType	<input type="text" value=""/>	(600-FFFF, Hexadecimal number)
DSAP	<input type="checkbox"/>	(0-FF, Hexadecimal number)
SSAP	<input type="checkbox"/>	(0-FF, Hexadecimal number)

Optional port

>>

<<

Protocol VLAN associated port:

Description:

1. You can use optional port list port to port VLAN protocol related list, the related VLAN protocol or VLAN protocol/connection port list port to port optional list, which is removed from the protocol in VLAN.
2. The specified VLAN must exist, otherwise the protocol VLAN will not be created.
3. Only the hybrid port can become an optional port, and the port must be part of the VLAN to succeed with the protocol 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.

Global
Port setup
Instance Info
Domain

Note: Enable STP may cause change of STP state machine and resulting in a short network interruption.

MSTP Global Setup

Global Stp	Enable
BPDU Protection	Disable
Max Hops	20
Mode	MSTP
Path Cost Standard	Legacy
TC Protection	Disable
TC Message delete forwarding table entry threshold	6 (1~255)
<input type="checkbox"/> Bridge Diameter	7
<input type="checkbox"/> Timer(PCT)	
Forward Delay	1500 (400~3000)
Hello Time	200 (100~1000)
Max Age Time	2000 (600~4000)
<input type="checkbox"/> instance	
Instance	0
Device Priority	32768
Root Type	normal

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:

Global Port setup Instance Info Domain

Note: Enable STP may cause change of STP state machine and resulting in a short network interruption.

Port Selection

2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28

Select All Select None

MSTP Port Setup

Stp Enable

Protection NONE

Instance Setup

Instance 0

Port Priority 128

Path Cost 0 legacy(0~200000, 0 means auto)

Advance Setup

Port Link Type auto

Transmission Rate 10 (1~255)

10.3.11.3 Отображение MSTP

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

Global Port setup Instance Info Domain

Instance Setup

Instance 0

```
-----[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.

Global		Port setup		Instance Info		Domain	
Domain name				MSTP Revision Level			
10000000280				0			
Instance ID				VLAN map			
0				1-4094			

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.

DHCP Settings		DHCP Static Table		DHCP Customer List																			
DHCP server																							
Enable DHCP server <input type="checkbox"/>																							
<table border="1"> <thead> <tr> <th>Address Pool Name</th> <th>Address Pool Segment/Mask</th> <th>Start Address</th> <th>End Address</th> <th>Address Lease</th> <th>Client Domain Name</th> <th>Primary DNS Server</th> <th>Secondary DNS Server</th> <th>Operating</th> </tr> </thead> <tbody> <tr> <td colspan="9"> <small>Note: Only the address pool segment and VLAN interface address in the same network segment address port can be used to assign IP addresses.</small> </td> </tr> </tbody> </table>						Address Pool Name	Address Pool Segment/Mask	Start Address	End Address	Address Lease	Client Domain Name	Primary DNS Server	Secondary DNS Server	Operating	<small>Note: Only the address pool segment and VLAN interface address in the same network segment address port can be used to assign IP addresses.</small>								
Address Pool Name	Address Pool Segment/Mask	Start Address	End Address	Address Lease	Client Domain Name	Primary DNS Server	Secondary DNS Server	Operating															
<small>Note: Only the address pool segment and VLAN interface address in the same network segment address port can be used to assign IP addresses.</small>																							
<div style="text-align: right;"> <input type="button" value="Help"/> <input type="button" value="Apply"/> <input type="button" value="New"/> <input type="button" value="Delete Sel"/> </div>																							

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.

DHCP Settings		DHCP Static Table		DHCP Customer List	
New address pool					
Address pool name	<input type="text"/>	(1-35character)			
Address pool segment	<input type="text"/>				
Subnet mask	<input type="text"/>	(1-30)			
Start address	<input type="text"/>				
End address	<input type="text"/>				
Address lease	<input type="text" value="1440"/>	(1-11520,Default value=1440)			
Client domain name	<input type="text"/>	(1-633character)			
Primary DNS server	<input type="text"/>				
Secondary DNS server	<input type="text"/>				
An asterisk (*) is required to fill in the item					

10.3.12.2 Статическая таблица DHCP

Перейдите в меню: Network → DHCP → DHCP Static Table, на этой странице отображаются 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.

DHCP Settings | DHCP Static Table | DHCP Customer List

Add Static Address

Client IP address *

Client MAC address(H-H-H) *

An asterisk (*) is required to fill in the item

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.

DHCP Settings | DHCP Static Table | DHCP Customer List

IP Address	MAC Address	Type	Host Name	VLAN Interface	Operation
------------	-------------	------	-----------	----------------	-----------

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 <ul style="list-style-type: none"> • 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. НАСТРОЙКА КОММУТАТОРА

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.



Port	Filter	Port	Filter
1	Disable	15	Disable
2	Disable	16	Disable
3	Disable	17	Disable
4	Disable	18	Disable
5	Disable	19	Disable
6	Disable	20	Disable
7	Disable	21	Disable
8	Disable	22	Disable
9	Disable	23	Disable
10	Disable	24	Disable
11	Disable	25	Disable
12	Disable	26	Disable
13	Disable	27	Disable
14	Disable	28	Disable

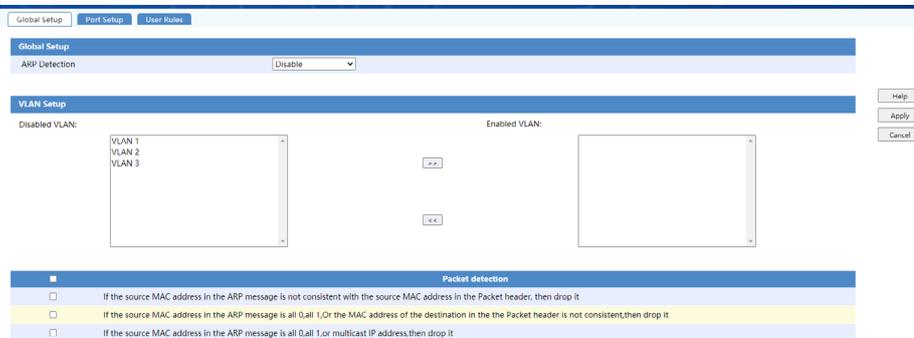
Note: Enable Port Filter, prevent the illegal message through the port.

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.



Global Setup

Global Setup

ARP Detection: Disable

VLAN Setup

Disabled VLAN: VLAN 1, VLAN 2, VLAN 3

Enabled VLAN:

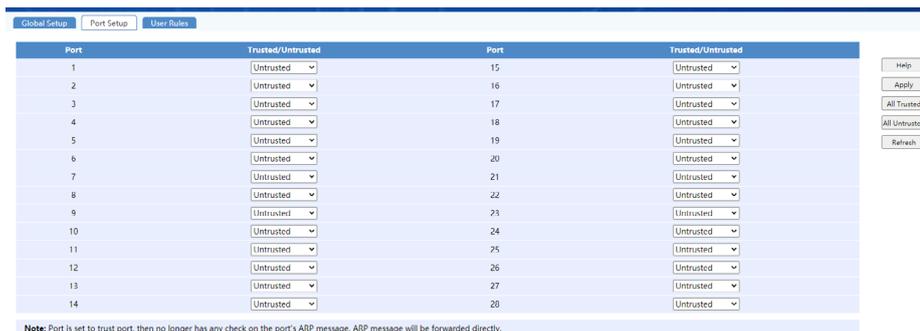
Packet detection

- If the source MAC address in the ARP message is not consistent with the source MAC address in the Packet header, then drop it
- If the source MAC address in the ARP message is all 0, all 1, or the MAC address of the destination in the the Packet header is not consistent, then drop it
- If the source MAC address in the ARP message is all 0, all 1, or multicast IP address, then drop it

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.



Port	Trusted/Untrusted	Port	Trusted/Untrusted
1	Untrusted	15	Untrusted
2	Untrusted	16	Untrusted
3	Untrusted	17	Untrusted
4	Untrusted	18	Untrusted
5	Untrusted	19	Untrusted
6	Untrusted	20	Untrusted
7	Untrusted	21	Untrusted
8	Untrusted	22	Untrusted
9	Untrusted	23	Untrusted
10	Untrusted	24	Untrusted
11	Untrusted	25	Untrusted
12	Untrusted	26	Untrusted
13	Untrusted	27	Untrusted
14	Untrusted	28	Untrusted

Note: Port is set to trust port, then no longer has any check on the port's ARP message. ARP message will be forwarded directly.

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.

Port	Loopback Detection/Vlan Detection	Port	Loopback Detection/Vlan Detection
1	Disable/Disable	15	Disable/Disable
2	Disable/Disable	16	Disable/Disable
3	Disable/Disable	17	Disable/Disable
4	Disable/Disable	18	Disable/Disable
5	Disable/Disable	19	Disable/Disable
6	Disable/Disable	20	Disable/Disable
7	Disable/Disable	21	Disable/Disable
8	Disable/Disable	22	Disable/Disable
9	Disable/Disable	23	Disable/Disable
10	Disable/Disable	24	Disable/Disable
11	Disable/Disable	25	Disable/Disable
12	Disable/Disable	26	Disable/Disable
13	Disable/Disable	27	Disable/Disable
14	Disable/Disable	28	Disable/Disable

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.

The screenshot shows the configuration page for VLAN Detection. It includes a navigation bar with tabs for 'Basic', 'Port Detection', and 'VLAN Detection'. The 'VLAN Detection' section is active, showing a dropdown menu set to 'Enable'. Below this is a 'Port' section with a grid of checkboxes for ports 2 through 28. A 'Notice' box at the bottom states: 'Disabled loop detection or the access port will not be able to normally open the VLAN detection function'.

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.

The screenshot shows the configuration page for Loop Display. It includes a navigation bar with tabs for 'Basic', 'Port Detection', and 'Loop Display', with 'Loop Display' selected. The 'Refresh Rate' section has a dropdown menu set to '30 Sec'. Below this is a 'Ports looped' section with a 'Status' button.

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.

Port	802.1X	Maximum Users	Port Licensing Mode	Port Control Mode	Re Authen	Handshake Function	Multicast trigger	Guest VLAN
1	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
2	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
3	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
4	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
5	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
6	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
7	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
8	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable

Щелкните соответствующий порт, чтобы перейти на страницу конфигурации порта:

802.1X Configuration

Enable 802.1X:

Guest VLAN:

Guest VLAN ID:

802.1X Timers

Silent Timer (10-120 s, Default value=60):

Re Authen Timer (60-7200 s, Default value=3600):

Handshake Timer (5-1024 s, Default value=15):

User Name Request Timeout Timer (10-120 s, Default value=30):

The Authentication Server Responds To The Timeout Timer (100-300 s, Default value=100):

Client Authentication Timeout Timer (1-120 s, Default value=30):

Note: If you want to enable the 802.1x function, you first need to set the RADIUS client. Please click "RADIUS Client Settings" to set up.

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

Port Configuration

Port: 1

802.1X:

Maximum Users (1-128, Default value=128):

Port Licensing Mode:

Port Control Mode:

Re Authen:

Handshake Function:

Multicast trigger:

Guest VLAN:

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.

802.1X Configuration	
Enable 802.1X	Disable
Guest VLAN	Disable
Guest VLAN ID	2

802.1X Timers	
Silent Timer (10-120 s, Default value=60)	60
Re Authen Timer (60-7200 s, Default value=3600)	3600
Handshake Timer (5-1024 s, Default value=15)	15
User Name Request Timeout Timer (10-120 s, Default value=30)	30
The Authentication Server Responds To The Timeout Timer (100-300 s, Default value=100)	100
Client Authentication Timeout Timer (1-120 s, Default value=30)	30

Note: If you want to enable the 802.1x function, you first need to set the RADIUS client. Please click "RADIUS Client Settings" to set up.

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.

AAA User authentication configuration	
Telnet User authentication method	Local
Terminal User authentication method	Local
Web User authentication method	Local

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.

Radius Client Settings | Domain Configuration

RADIUS Client settings

Program name: system

Server response timeout (1-10, Default value=3): 3

Maximum number of RADIUS packets sent (1-30, Default value=5): 5

Real-time billing interval (3-60 minutes, Must be a multiple of 3, Default value=12): 12

The maximum number of failed packets sent by real-time accounting packets (1-255, Default value=5): 5

Note: Do not change the defaults for Real-time Accounting Interval and Real-time Billing Maximum Send. Unless you determine that the modified value is better for the interaction process.

Service Type	Service Status	Server IP Address	Server Port Number (1-65535)	Shared Key
Primary Authentication Server	Block		1812	
From The Authentication Server	Block		1812	(0 - 16character)
Main Billing Server	Block		1813	
From The Billing Server	Block		1813	(0 - 16character)

Note: 1.If the 002:1 authentication user needs to charge the service, set the primary accounting server or the accounting server.
2.The Shared Key cat not include the following characters: ; < > / \ ' "

Help Apply Cancel

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 веб-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 $-50\text{ }^{\circ}\text{C}$ до $+50\text{ }^{\circ}\text{C}$ 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 $-10\text{ }^{\circ}\text{C}$ до $+60\text{ }^{\circ}\text{C}$ 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

В случае возникновения трудностей с подключением, настройкой и эксплуатацией оборудования и программного обеспечения ROXTON

support@roxton.ru

СЕРВИСНЫЙ ЦЕНТР ROXTON

Гарантийный и постгарантийный ремонт, а также техническое обслуживание оборудования ROXTON

service@roxton.ru

ПРИЛОЖЕНИЕ А

(справочное)

ГАБАРИТНЫЕ РАЗМЕРЫ

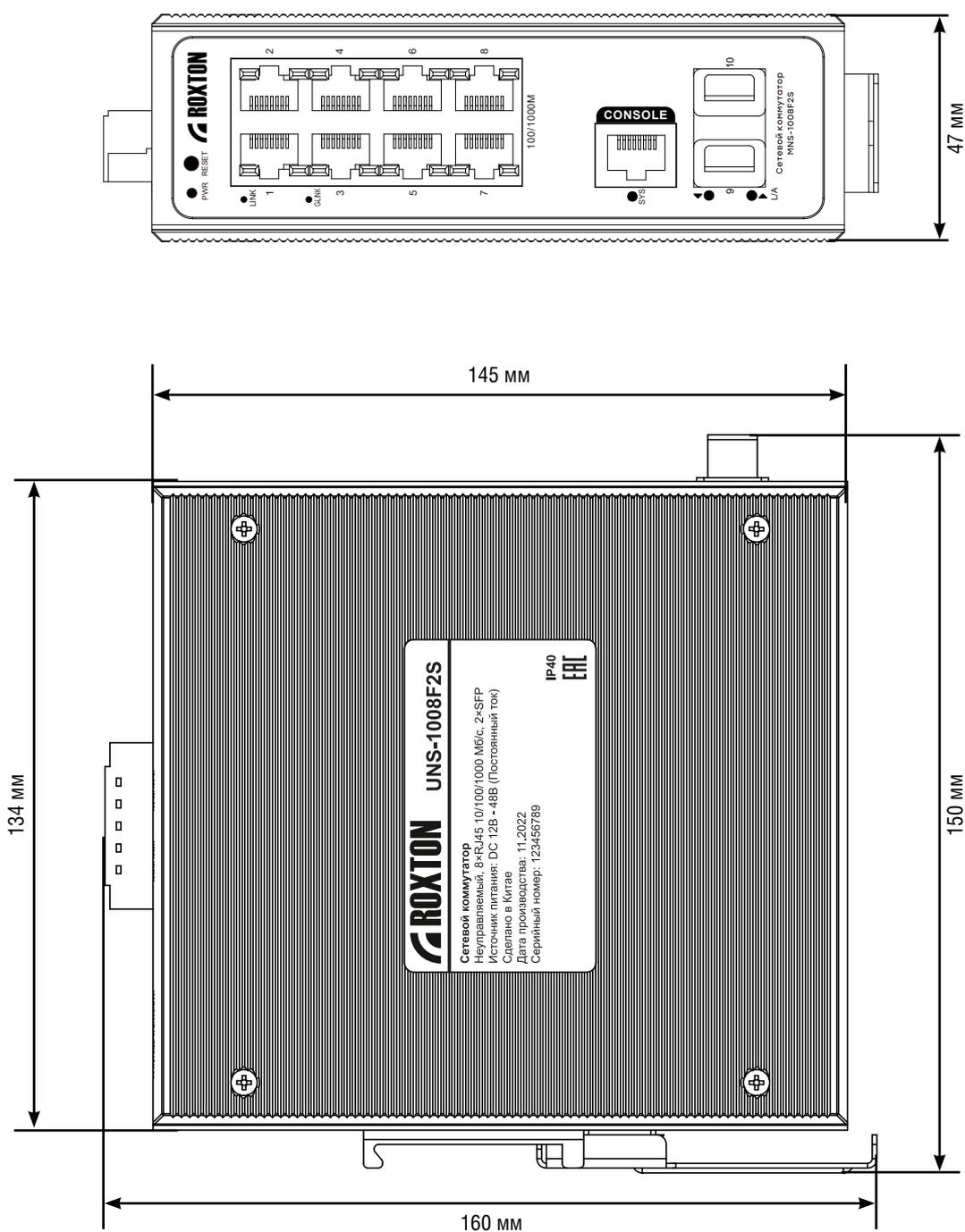


Рисунок А.1 Габаритные размеры ROXTON MNS-1008F2S / MNS-1008F2SP

ПРИЛОЖЕНИЕ А

(справочное)

ГАБАРИТНЫЕ РАЗМЕРЫ

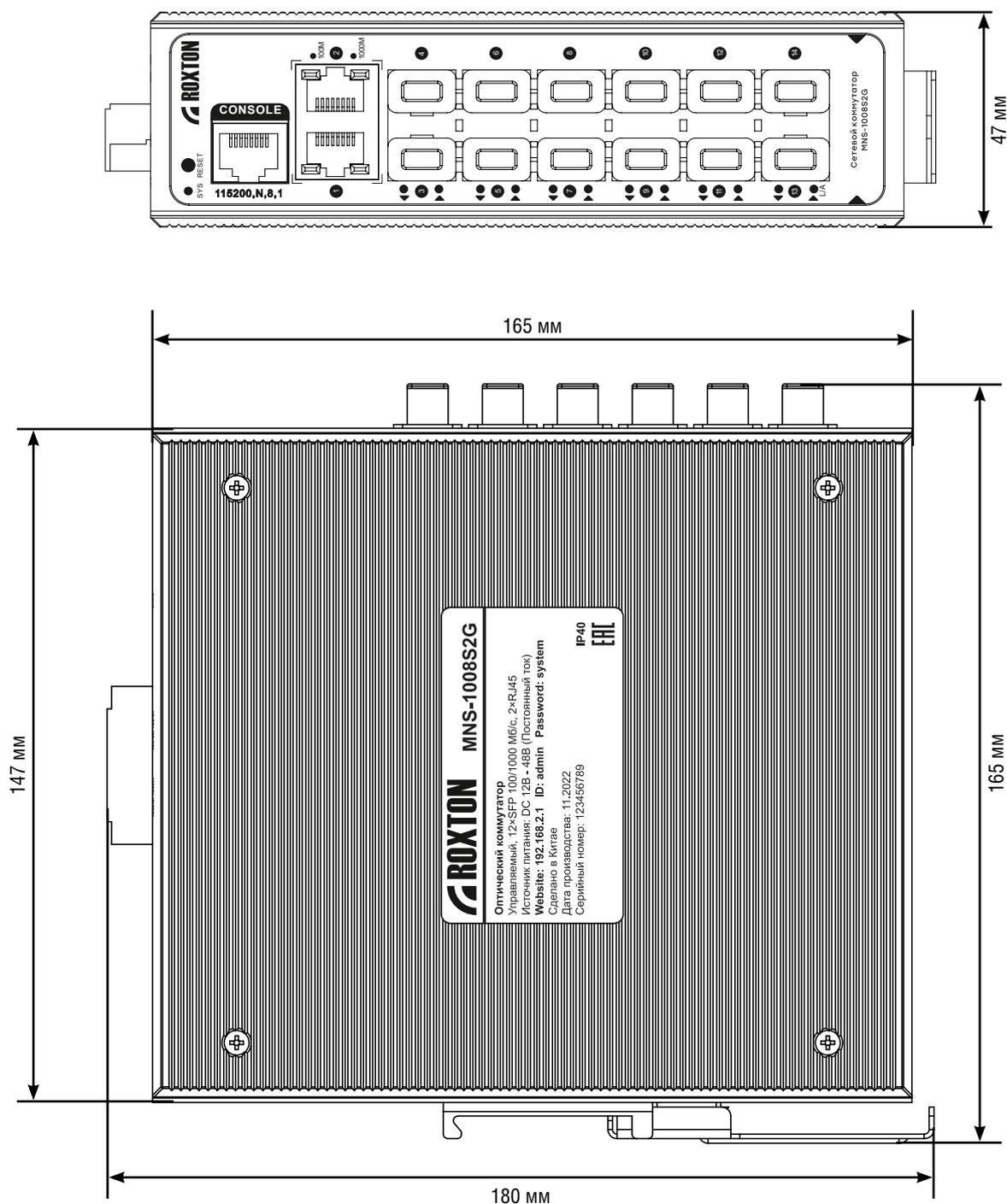


Рисунок А.1 Габаритные размеры ROXTON MNS-1008S2G

WWW.ROXTON.RU