КОММУТАТОР ДОСТУПА L2

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

(ВЕРСИЯ 1.1)

РФМД.460526.021РЭ

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Данное руководство предназначено для системных администраторов, инженеров технической поддержки. В руководстве приводятся описание для управления промышленными коммутаторами L2 YN-SI2500AE, YN-SI2510A, YN-SI2550A, YN-SI3400AT, YN-SI3500A, YN-SI3500AE (далее – коммутатор или изделие/устройство).

2 ИНФОРМАЦИЯ О ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ

Для получения дополнительной технической информации воспользуйтесь:

1. Формой обратной связи на сайте Yarus Networks: http://www.yarus-networks.ru/contact.html
2. Обращение в ООО «ЭКСАРА»:
   - Телефон: +7 (495) 128-30-30
   - E-mail: info@exara.ru

При наличии действующего сервисного контракта и/или гарантийных обязательств, вы можете обратиться по адресам, указанным в контракте.

3 ВХОД В СИСТЕМУ

3.1 Особенности программного обеспечения

Промышленные управляемые коммутаторы Yarus Networks поддерживают различные сетевые протоколы и программные функции. Эти протоколы и функции позволяют сетевому администратору дополнительно повысить безопасность и надежность контролируемых ими сетей. Благодаря этим функциям, коммутаторы Yarus Networks хорошо подходят для использования в системах обеспечения безопасности и в системах автоматизации производственных процессов. Ниже приведен список поддерживаемых протоколов и программных функций.

- Пользовательские интерфейсы:
  1. Интернет-браузер
  2. Telnet, SSH
  3. Консоль (RS 232)
- Ретранслятор / клиент протокола динамической конфигурации хост-устройств (DHCP), включая поддержку опции 66/67;
- Синхронизация времени:
  1. Сервер / клиент протокола сетевого времени (NTP)
  2. Простой протокол сетевого времени (SNTP)
  3. Протоколы высокоточной тактовой синхронизации IEEE 1588 (PTP)v2 – аппаратный E2E TC и программный Boundary Clock
- Зеркалирование портов;
- Регулирование трафика для функции качества сервиса (QoS);
- Протокол управления агрегацией каналов (LACP);
- Протокол обнаружения канального уровня (LLDP);
- Фильтрация для управления доступом к среде (по MAC-адресам);
- Базовый протокол регистрации атрибутов (GARP) / протокол многоадресной регистрации GARP (GMRP) / протокол регистрации виртуальных сетей GARP (GVRP);
- Простой протокол управления сетью (SNMP) v1/v2/v3 (с проверкой подлинности по алгоритму MD5 и DES-шифрованием);
- Сообщения SNMP Inform;
- Протокол связующего дерева (STP) / протокол высокоскоростного связующего дерева (RSTP) / протокол множественных связующих деревьев (MSTP) / протокол резервирования среды передачи (MRP);
- Виртуальная локальная сеть (VLAN);
- IEEE 802.1x / открытый протокол проверки подлинности (EAP) / сервис удаленной

проверки подлинности пользователя при коммутируемом подключении (RADIUS) / система управления доступом для контроллера доступа к терминалу (TACACS+);

- Безопасность (функциональность поддерживается не во всех моделях):
  1. Безопасное управление доступом к среде (MACsec)
  2. 802.1AE – проверка подлинности и обмен ключами
- Кольцо.
  1. Защитное переключение для кольца Ethernet (ERPS)
  2. Протокол iA-Ring
  3. Протокол C-Ring
  4. Протокол C-Chain
  5. Протокол U-Ring
- Система аварийной сигнализации (с уведомлением по электронной почте или через релейный выход);
- Промышленные протоколы:
  1. Modbus/TCP
  2. Profinet (включая резервированное кольцо MRP)

3.2 Настройка параметров через интернет-браузер

Для настройки параметров конфигурации данного сетевого коммутатора Ethernet можно использовать следующие три способа:

1. Через интернет-браузер.
2. С помощью консоли Telnet.
3. С помощью последовательной консоли (RS 232).

Используя интернет-браузер и консоль Telnet, пользователь может подключаться к коммутатору через сеть Интернет или Ethernet LAN, в то время как для настройки с помощью последовательной консоли потребуется установить последовательное кабельное соединение между консолью и коммутатором. Упомянутые три метода лишь незначительно отличаются друг от друга. Пользователям рекомендуется метод настройки через интернет-браузер, так как при этом используется интуитивно понятный интерфейс.

Пользователь может без труда получить доступ к управляемому коммутатору через любой интернет-браузер (рекомендуется Internet Explorer 8 или 11, Firefox 44, Chrome 48 или более поздние версии). На примере использования интернет-браузера в данной главе представлены функции управляемого коммутатора.

3.3 Заводские настройки по умолчанию

Ниже приведен список заводских настроек по умолчанию. Эта информация будет использоваться в процессе входа в систему. Удостоверьтесь, что IP-адрес компьютера,

обращающегося к коммутатору, принадлежит той же подсети, и оба устройства имеют одинаковые значения маски подсети.

IP-адрес: 10.0.50.1

Маска подсети: 255.255.0.0

Шлюз по умолчанию: 0.0.0.0

Имя пользователя: admin

Пароль: default

3.4 Процесс входа в систему и интерфейс главного окна

Прежде чем получить доступ к функциям настройки параметров конфигурации, пользователь должен зарегистрироваться в системе. Процедура входа в систему очень проста. Вход выполняется в два этапа:

1. Запустите интернет-браузер.

2. Введите IP-адрес коммутатора (например, http://10.0.50.1), как показано на рисунке.

ПРИМЕЧАНИЕ: если не заполнить поля имени и пароля пользователя, приглашение к входу в систему не будет выведено.

Рисунок 3.1. IP-адрес для настройки параметров через сетевой браузер.

После входа в систему на экране выводится окно главного интерфейса, которое показано на рисунке 3.2.

Главное меню (на экране с левой стороны) содержит верхнеуровневые элементы иерархического меню. При щелчке указателем на любом таком вводе открываются соответствующие нижнеуровневые разделы. Заметьте, что в рассматриваемом примере Порт 5 подсвечен зеленым цветом. Это означает, что данный порт подключен. Подробное описание каждого подраздела меню приводится ниже в порядке следования.

Рисунок 3.2. Сетевой интерфейс по умолчанию.

4 РАЗДЕЛ BASIC

В данном разделе приведена важная информация о коммутаторе, чтобы пользователи могли лучше ознакомиться с устройством. Он также играет роль главного экрана приглашения, который открывается сразу же после входа пользователя в систему.

Приведенная информация упрощает идентификацию различных коммутаторов, подключенных к сети. Раздел **Basic** разделен на шесть подразделов, как показано на рисунке 4.1 с левой стороны.

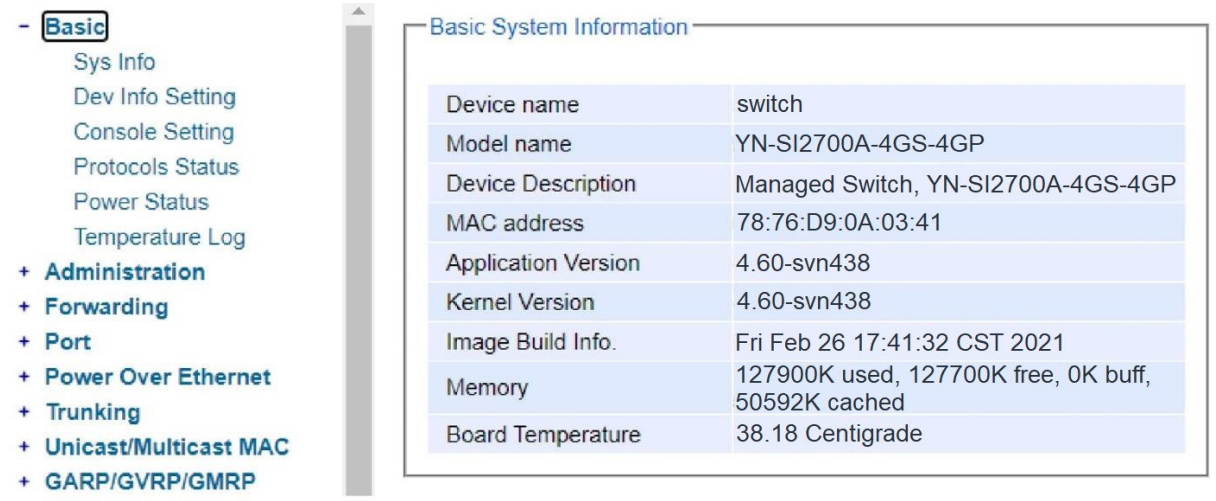


Рисунок 4.1. Раскрывающееся меню раздела Basic.

4.1 Подраздел Sys Info

Этот подраздел содержит основную информацию о системе промышленного управляемого коммутатора Yarus Networks. Пользователь может проверить имя устройства, название модели, описание устройства, MAC-адрес, версию встроенного микропрограммного обеспечения (версию приложения и версию ядра), время сборки образа, использование памяти коммутатора и текущую температуру системной платы.

Следует отметить, что встроенное микропрограммное обеспечение Yarus Networks, как правило, состоит из версии приложения и версии ядра.

На рисунке 4.2 в качестве примера приведена базовая информация о системе устройства модели YN-SI2700A-4GS-4GP.

В таблице 4.1 в сводном виде представлено описание всех пунктов информации.

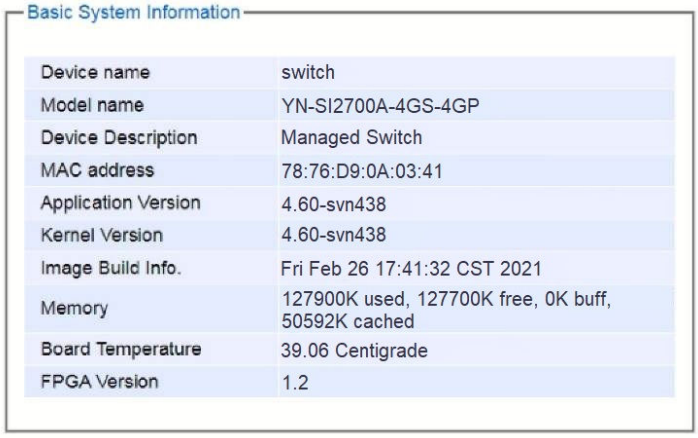


Рисунок 4.2. Информация на сетевой странице Sys Info.

Таблица 4.1. Описание пунктов основной информации.

Имя параметра	Описание
Device name	Псевдоним устройства, который используется, чтобы отличать его от других устройств.
Model name	Полное название модели устройства.
Device Description	Тип устройства.
MAC address	MAC-адрес устройства.
Application Version	Текущая версия приложения для программного обеспечения устройства.
Kernel Version	Текущая версия ядра для программного обеспечения устройства.
Image Build Info.	Информация об образе встроенного микропрограммного обеспечения, например, дата создания образа.
Memory	Текущий размер свободной памяти в ОЗУ, размер кэшируемой и совместно используемой памяти.
Board Temperature	Текущая температура системной платы внутри корпуса в градусах Цельсия.
FPGA Version	Текущая версия программируемой логической интегральной схемы (FPGA) устройства.

4.2 Подраздел Device Information Setting

В этом подразделе пользователь может указать информацию об устройстве. Вводится уникальная и понятная для пользователя информация о системе, такая как имя устройства, описание устройства, местоположение и контактные данные.

Эта информация поможет идентифицировать определенный коммутатор среди остальных устройств в сети, которая поддерживает протокол SNMP. Щелкните с указателем на кнопке "Update", чтобы обновить информацию о коммутаторе.

На рисунке 4.3 показана страница Device Information Setting для управляемого коммутатора.

В таблице 4.2 в сводном виде представлено описание настраиваемых пунктов информации об устройстве и соответствующие заводские настройки по умолчанию.

Рисунок 4.3. Сетевая страница Device Information Settings.

Таблица 4.2. Описание системных настроек.

Имя параметра	Описание	Заводская настройка по умолчанию
Device Name	Ассоциируется с определенной ролью или областью применения различных коммутаторов. Максимальная длина - 63 символа.	(Название модели)
Device Description	Подробное описание устройства. Максимальная длина - 63 символа.	Управляемый коммутатор + (название модели)
Location	Местоположение коммутатора. Максимальная длина - 63 символа.	Местоположение коммутатора
Contact	Приводится контактная информация для обращения с целью обслуживания. Введите имя лица или организации, к которой следует обращаться в случае возникновения проблем. Максимальная длина - 63 символа.	www.yarus-networks.ru

4.3 Подраздел Console Setting

В подразделе Console Setting данного меню приводятся только значения настроенных параметров соединения с последовательной консолью, которое могут использоваться программным обеспечением консоли, таким как Putty.

На рисунке 4.4 ниже показан пример значений параметров соединения с последовательной консолью.

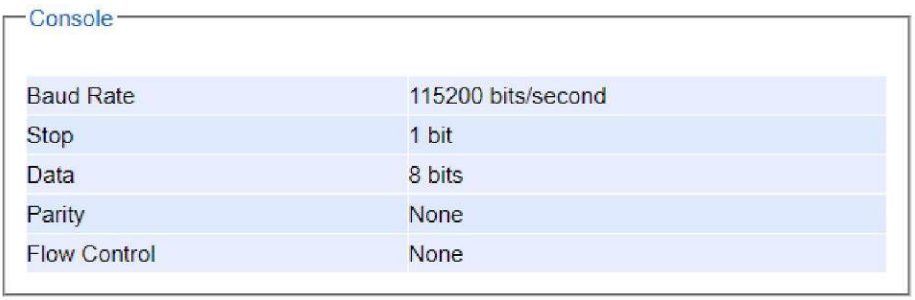


Рисунок 4.4. Параметры для настройки с помощью консоли.

4.4 Подраздел Protocols Status

Подраздел Protocols Status содержит информацию о статусе всех протоколов в коммутаторе. На этой сетевой странице пользователь может просмотреть состояние всех протоколов одновременно. Подробное описание каждого протокола и соответствующих методов

приведено в следующих разделах.

На рисунке 4.5 показан сетевой интерфейс для страницы Protocol Status.

Рисунок 4.5. Сетевая страница Protocol Status.

4.5 Подраздел Power Status

Отличительной особенностью управляемого коммутатора Yarus Networks является наличие двух вводов для подключения электропитания постоянного тока.

Модели, не поддерживающие функцию питания по Ethernet (PoE), запитываются под напряжением 9 – 57 В постоянного тока через вход электропитания 1 (контакты V1+ и V1-) и/или вход электропитания 2 (контакты V2+ и V2-).

Модели, поддерживающие функцию PoE, запитываются под напряжением 45 - 57 В постоянного тока в режиме 802.3af или 51 - 57 В постоянного тока в режиме 802.3at.

Например, устройство может быть запитано в любом из следующих трех вариантов: 9 - 57 В постоянного тока с максимальной силой тока 2,8 ампер (режим без поддержки функции PoE), 45 - 57 В постоянного тока с максимальной силой тока 1,7 ампер (режим 802.3af), 51 - 57 В постоянного тока с максимальной силой тока 2,3 ампер (режим 802.3at).

На рисунке 4.6 показан статус каждого входа электропитания.

Статус "Not Connected" означает, что данный ввод либо не подключен к источнику питания,

либо находится в состоянии отказа, т.е. через него не подается электропитание с заданными характеристиками.

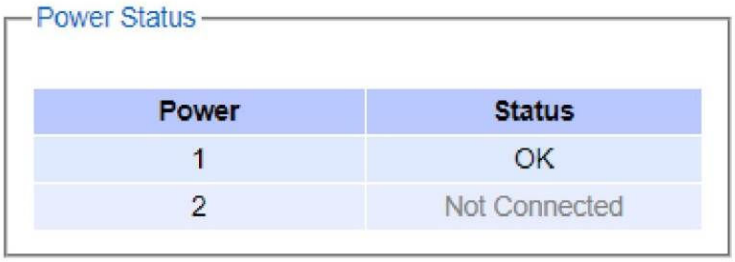


Рисунок 4.6. Сетевая страница Power Status.

4.6 Подраздел Temperature Log

Данный подраздел предоставляет доступ к пользовательскому и системному журналам регистрации температуры. В каждом из упомянутых журналов регистрируется сводная статистика и информация о распределении температур.

Максимальное, минимальное и среднее значения температуры представлены в градусах Цельсия. Помимо того, в поле Recorded Time показано время, истекшее после записи журнала регистрации температуры.

Сводные статистические данные представлены в форме таблицы и включают температурные диапазоны, относительная продолжительность регистрации в процентах для каждого диапазона, а также абсолютная продолжительность удержания температуры в каждом диапазоне.

Пользователь может сбросить пользовательскую статистику, щелкнув с указателем на кнопке Reset, которая расположена в нижней части окна пользовательского журнала регистрации температуры. При этом пользователь не может обнулить системный журнал регистрации температуры.

Следует отметить, что информация в окне не обновляется автоматически. Информация, представленная на этой сетевой странице, может оказаться полезной для пользователя в аспекте контроля состояния промышленного управляемого коммутатора, работающего в неблагоприятных условиях окружающей среды. Для обновления статистических данных пользователь должен щелкнуть с указателем на значке перезагрузки интернет-браузера.

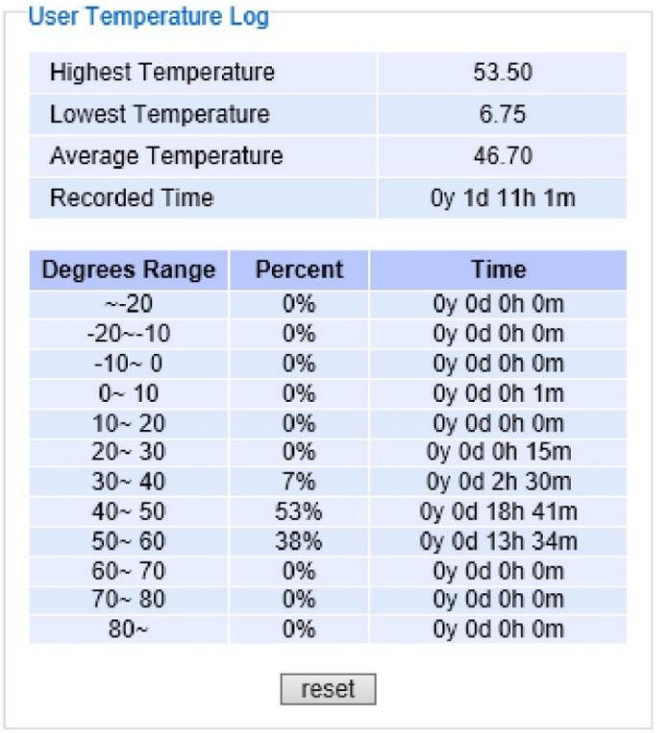
На рисунке 4.7 показано окно пользовательского журнала регистрации температуры, а на рисунке 4.8 - окно системного журнала регистрации температуры.

Следует отметить, что в промышленном управляемом коммутаторе установлен сенсорный компонент, который способен определять температуру внутри корпуса.

Программное обеспечение коммутатора может считывать сигналы датчика и преобразовывать их в температуру, выраженную в градусах Цельсия.

Поскольку устройство упаковано в воздухонепроницаемый корпус, температура внутри корпуса устанавливается приблизительно на 20 градусов выше наружной температуры.

Минимальная допустимая рабочая температура наружного воздуха для коммутатора промышленного класса составляет приблизительно от -20 до -40 градусов Цельсия, в то время как максимальное допустимое значение рабочей температуры (снаружи устройства) может достигать приблизительно 70 - 85 градусов Цельсия.

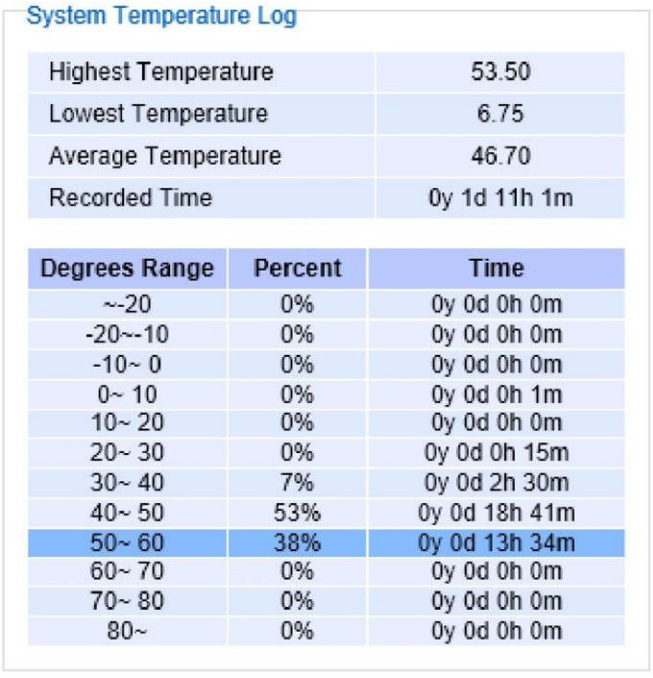

User Temperature Log

Highest Temperature	53.50
Lowest Temperature	6.75
Average Temperature	46.70
Recorded Time	0y 1d 11h 1m

Degrees Range	Percent	Time
~-20	0%	0y 0d 0h 0m
-20~-10	0%	0y 0d 0h 0m
-10~ 0	0%	0y 0d 0h 0m
0~ 10	0%	0y 0d 0h 1m
10~ 20	0%	0y 0d 0h 0m
20~ 30	0%	0y 0d 0h 15m
30~ 40	7%	0y 0d 2h 30m
40~ 50	53%	0y 0d 18h 41m
50~ 60	38%	0y 0d 13h 34m
60~ 70	0%	0y 0d 0h 0m
70~ 80	0%	0y 0d 0h 0m
80~	0%	0y 0d 0h 0m

reset

Рисунок 4.7. Пользовательский журнал регистрации температуры.


System Temperature Log

Highest Temperature	53.50
Lowest Temperature	6.75
Average Temperature	46.70
Recorded Time	0y 1d 11h 1m

Degrees Range	Percent	Time
~-20	0%	0y 0d 0h 0m
-20~-10	0%	0y 0d 0h 0m
-10~ 0	0%	0y 0d 0h 0m
0~ 10	0%	0y 0d 0h 1m
10~ 20	0%	0y 0d 0h 0m
20~ 30	0%	0y 0d 0h 15m
30~ 40	7%	0y 0d 2h 30m
40~ 50	53%	0y 0d 18h 41m
50~ 60	38%	0y 0d 13h 34m
60~ 70	0%	0y 0d 0h 0m
70~ 80	0%	0y 0d 0h 0m
80~	0%	0y 0d 0h 0m

Рисунок 4.8. Системный журнал регистрации температуры.

5 РАЗДЕЛ ADMINISTRATION

В этом разделе пользователь может настраивать параметры в следующих подразделах: Account, Auth Server Setting, IP Settings, IPv6 Setting, Ping, Ping6, Mirror Port, System Time, Modbus Setting, PTP, SSH, Telnet, HTTPS, а также DIP Switch.

На рисунке 5.1 показано окно раздела Administration со списком подразделов в левой части экрана.

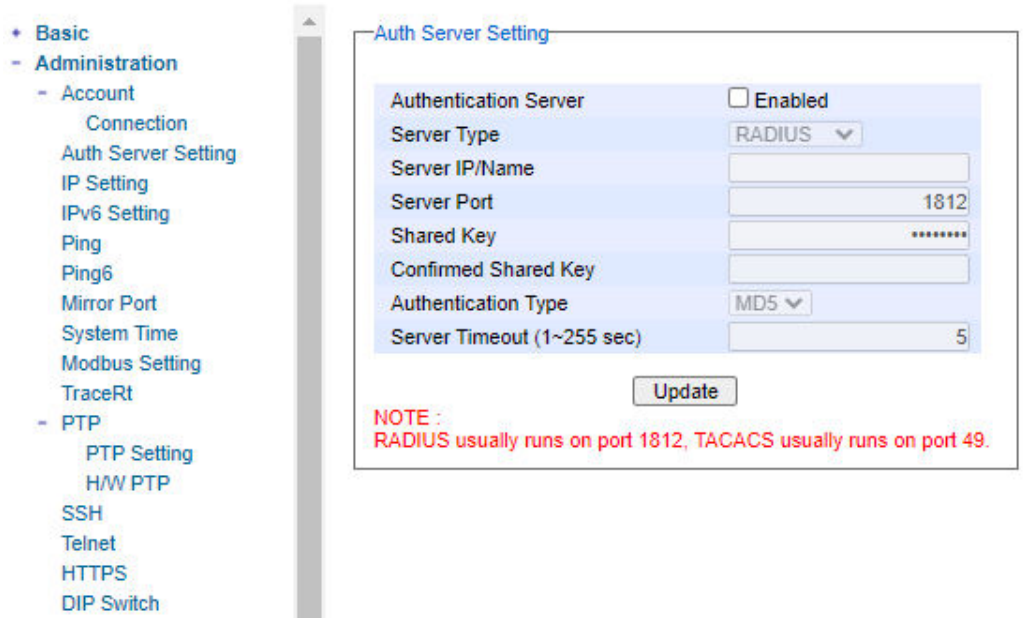


Рисунок 5.1. Раскрывающееся меню Administration.

5.1 Подраздел Account

Пользователи с правами администратора могут создавать и удалять учетные записи через раздел **Administration->Account** как показано на рисунке 5.2. Меню управления учетными записями имеется в общей сложности четыре раздела, которые выглядят следующим образом: **Account list, Add account, Change password** и **Password strength configuration.** В окне списка учетных записей (1-я строка на рис. 5.2) перечислены пользователи и их права доступа. Существует два типа прав доступа: администратор и пользователь. Право доступа администратора имеет разрешение на чтение / запись на управляемом коммутаторе, в то время как право доступа пользователя имеет разрешение только на чтение. Если пользователь с правами администратора хочет удалить какую-либо учетную запись, пользователь может выбрать учетную запись, которую он хотел бы удалить, и нажать кнопку “Delete”. Обратите внимание, что пользователь не может удалить свою собственную учетную запись. Пользователь, чья учетная запись была удалена, будет немедленно выведен из системы.

В поле **Add account** (2-я строка на рис. 5.2) пользователь может ввести имя пользователя в текстовом поле Username, а также ввести пароль в текстовом поле Password. Затем пользователь может выбрать подходящее право доступа из выпадающего списка для пользователя, прежде чем нажать кнопку Добавить. После нажатия на нее в окне списка

учетных записей будет создана новая учетная запись. По умолчанию создается имя пользователя “admin” с правами доступа “admin”. Максимальное количество учетных записей - 15.

Если пользователь желает изменить пароль для какой-либо учетной записи, он может сделать это в поле **Change password** (3-я строка на рис. 5.2). Здесь пользователь должен сначала выбрать имя пользователя из выпадающего списка Username. Затем введите пароль, на который пользователь хотел бы его изменить, в текстовом поле "New password" и "Confirm password". Минимальную и максимальную длину каждого пароля можно настроить с помощью поля **Password strength configuration** в последней строке на рис. 5.2. Обратите внимание, что во время процедуры входа в систему пользователям будет предложено сменить свои пароли, если пароли не менялись в течение последних 30 дней. На рисунке 5.3 показано всплывающее уведомление о смене пароля.

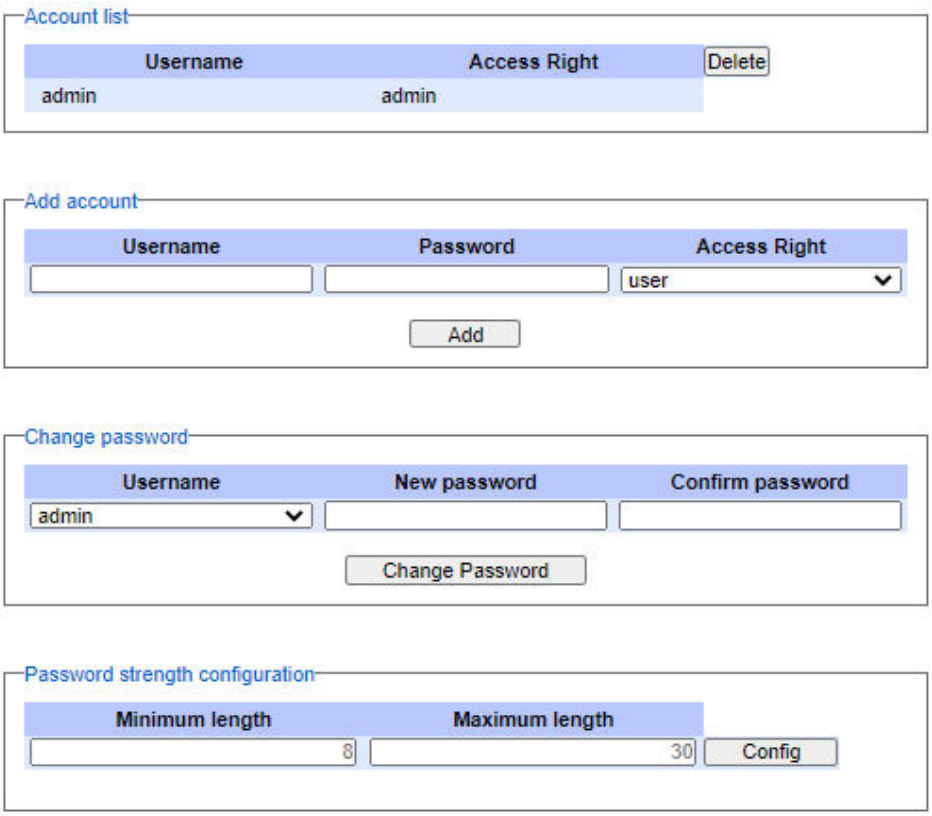


Рисунок 5.2. Сетевая страница настройки аккаунтов.

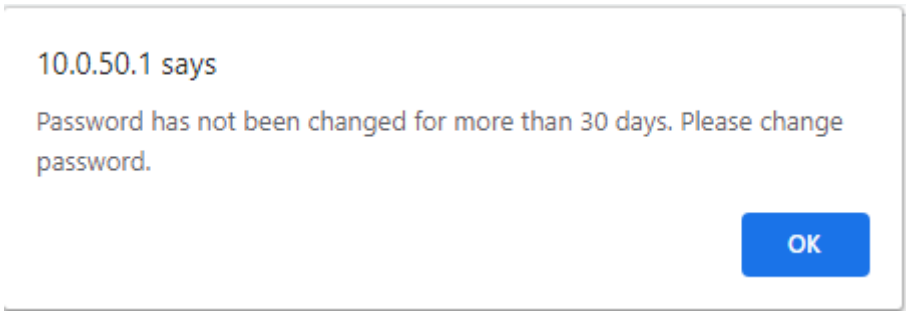


Рисунок 5.3. Всплывающее уведомление о смене пароля

5.2 Подраздел Auth Server Setting

В дополнение к локальной проверке подлинности коммутатор можно настроить под запрос на проверку подлинности через централизованный сервер RADIUS или TACACS+ (в случае неудачного завершения локальной проверки).

На рисунке 5.4 показаны настраиваемые параметры сервера проверки подлинности, а в таблице 5.1 в сводном виде представлено описание этих параметров сервера.

Данные для сравнения серверов RADIUS и TACACS+ приведены в таблице 5.2.

Используя эти данные, пользователь может выбрать решение, наиболее соответствующее его потребностям.

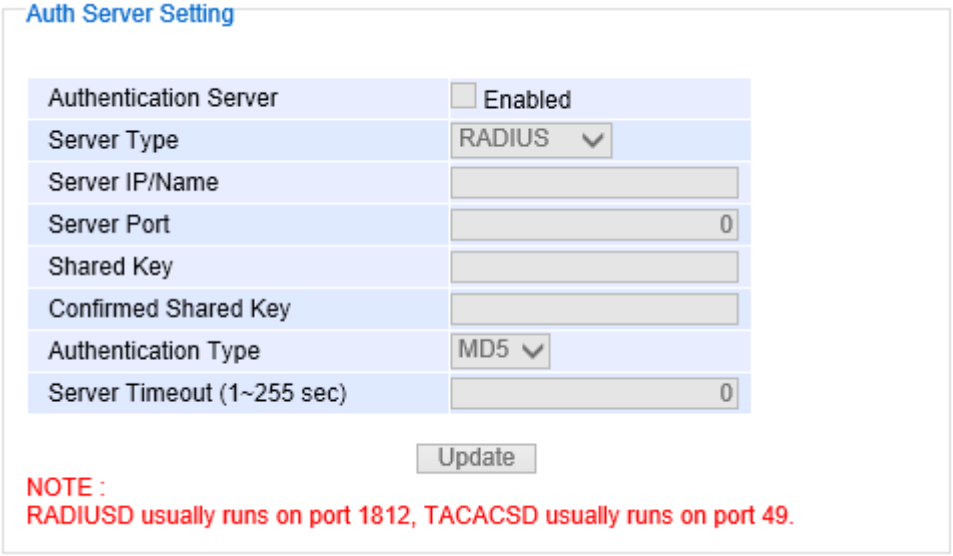


Рисунок 5.4. Настройка сервера проверки подлинности.

Таблица 5.1. Настраиваемые параметры сервера проверки подлинности.

Имя параметра	Описание	Заводская настройка по умолчанию
Authentication Server	Активация / отключение подтверждения подлинности через удаленный сервер проверки подлинности.	Выключено
Server Type	Выбор типа сервера проверки подлинности: RADIUS или TACACS+. Дополнительная информация приведена в примечаниях ниже.	RADIUS
Server IP/Name	IP-адрес сервера проверки подлинности.	Не заполняется
Server Port	Коммуникационный порт сервера проверки подлинности.	1812
Shared Key	Ключ, используемый для подтверждения подлинности через сервер. Максимальная длина - 15 символов.	12345678
Confirmed Shared Key	Повторный ввод общего ключа. Максимальная длина - 15 символов.	Не заполняется
Authentication Type	Механизм проверки подлинности. Для сервера RADIUS: алгоритм MD5. Для сервера TACACS+: ASCII-последовательность, протокол проверки подлинности по паролю (PAP), протокол проверки подлинности по квитированию вызова (CHAP),	Для RADIUS - MD5, для TACACS+ - ASCII

Имя параметра	Описание	Заводская настройка по умолчанию
	протокол проверки подлинности по квитированию вызова Microsoft Challenge (MSCHAP).	
Server Timeout (1 ~ 255 сек.)	Время ожидания ответа от сервера проверки подлинности. Этот параметр определяет время, через которое будет выведено следующее приглашение к входу в систему, если сервер не доступен.	5

Таблица 5.2. Сравнение настраиваемых параметров сервера проверки подлинности для RADIUS и TACACS+.

	RADIUS	TACACS+
Транспортный протокол	UDP	TCP
Аутентификация и авторизация	Раздельное выполнение функций AAA.	Совмещенная проверка подлинности и авторизация.
Поддержка многопротокольности	Нет	Да - поддержка протокола удаленного доступа AppleTalk (ARA) и протокола NetBIOS.
Конфиденциальность	Шифруется только пароль.	Шифруется весь пакет.

5.3 Подраздел IP Setting

Этот подраздел разделен на две части: Настройка IP-адреса и информация о текущем IP-адресе. В этом подразделе пользователь может изменить сетевые настройки интернет-протокола версии 4 (IPv4) для управляемого коммутатора, например, статический IP-адрес, маску подсети, шлюз, первичный DNS (сервер доменных имен) и вторичный DNS. Как показано на рисунке 5.5, пользователь может включить DHCP (протокол динамической настройки IP параметров), установив флажок в соответствующее поле. То есть IP-адрес и связанная с ним информация могут быть автоматически получены с DHCP-сервера в локальной сети. Отключив эту функцию (флажок DHCP снят), пользователь имеет возможность настроить статический IP-адрес и связанные с ним поля вручную. Нажмите на кнопку Update, чтобы обновить IP конфигурацию на коммутаторе. После каждого обновления требуется перезагрузка системы, чтобы новые сетевые настройки могли вступить в силу. Пользователю необходимо вручную обновить новый IP-адрес в поле URL веб-браузера, если IP-адрес управляемого коммутатора будет изменен.

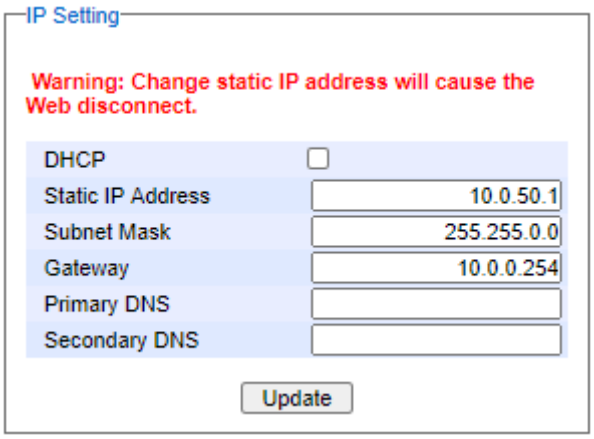


Рисунок 5.5. Настройка параметров IP-протокола на сетевой странице IP Setting.

Вторая часть раздела Настройки IP-адреса — это информация о текущем IP-адресе, как показано на рисунке 5.6. В этой части приведена информация о текущем IP-адресе управляемого коммутатора. Описание каждого поля и его значение по умолчанию приведены в таблице 5.3.

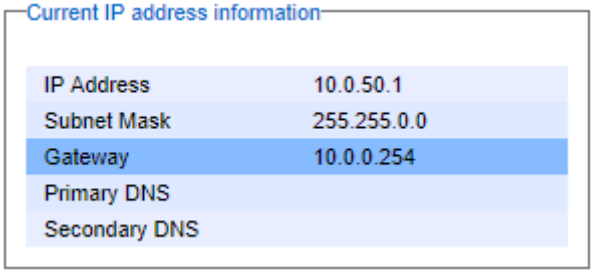


Рисунок 5.6. Текущие параметры IP-протокола на сетевой странице IP Setting.

Таблица 5.3. Описание настраиваемых параметров подраздела IP Setting.

Имя параметра	**Описание**	**Заводская настройка по умолчанию**
DHCP	Если установить флажок в этом поле, IP-адрес и другие связанные значения будут назначаться автоматически. В другом варианте пользователь может назначить статический IP-адрес и связанные с ним значения вручную.	Флажок не установлен
Static IP Address	В поле отображается текущий IP-адрес. Пользователь может указать новый статический IP-адрес для устройства.	10.0.50.1
Subnet Mask	Отображается текущее значение маски подсети, которое может быть изменено пользователем.	255.255.0.0
Gateway	Отображается текущий шлюз, который может быть изменен пользователем.	0.0.0.0
Primary DNS	Указывается IP-адрес первичного DNS-сервера, который будет использоваться данной сетью.	Не заполняется
Secondary DNS	Указывается IP-адрес вторичного DNS-сервера. Если сетевой коммутатор Ethernet не сможет подключиться к первичному DNS-серверу, он найдет вторичный DNS-сервер и попытается подключиться к нему.	Не заполняется

Имя параметра	Описание	Заводская настройка по умолчанию
VID	Указывается идентификационный номер виртуальной локальной сети, т.е. вводится значение идентификатора VLAN, для которой нужно настроить IPv4-адрес.	Не заполняется

5.4 Подраздел IPv6 Setting

Этот подраздел разделен на две части: Настройка IPv6 и текущая информация об IPv6-адресе. Первая часть, называемая Настройкой IPv6, показана на рисунке 5.7 и позволяет пользователям настраивать параметры для сети IPv6.

Следует отметить, что сеть с поддержкой протокола IPv6 поддерживает автоматическую настройку конфигурации трех типов: без сохранения состояния, с сохранением состояния и комбинированную.

В режиме автоматической настройки "Autoconfig" действие выполняется без сохранения состояния, в то время как при выборе опции "DHCPv6" настройка параметров происходит с сохранением состояния.

Если пользователь установит флажки в обоих полях - Autoconfig и DHCPv6, коммутатор будет комбинировать опции с сохранением и без сохранения состояния.

Если пользователь выберет опцию "Manual", он должен будет вручную указать глобальный адрес одноадресной передачи, длину префикса и шлюз в полях Global Unicast Address, Prefix Length и Gateway соответственно.

У пользователей есть выбор включить или отключить ручной DNS, установив флажок в соответствующем поле. Если установлен флажок DNS вручную, пользователи смогут вводить IPv6-адреса основного DNS и дополнительного DNS. Если пользователи изменят какие-либо настройки DNS, нажмите на кнопку Обновить, чтобы новая конфигурация вступила в силу. В таблице 5.4 описываются параметры веб-страницы настроек IPv6.

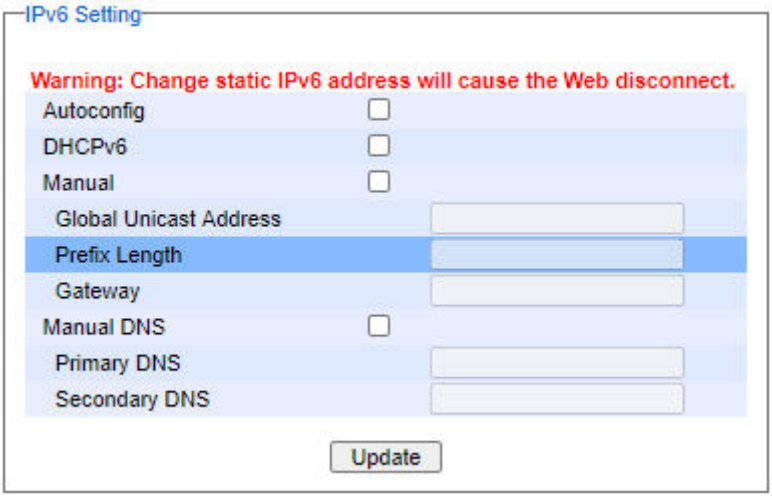


Рисунок 5.7. Окно с настраиваемыми параметрами протокола IPv6 на сетевой странице IPv6 Setting.

Вторая часть, называемая информацией о текущем IPv6-адресе, показана на рисунке 5.8. В этой части веб-страницы обобщается текущая информация об IPv6 адресе управляемого коммутатора, которая представляет собой глобальный одноадресный адрес, локальный адрес канала, шлюз, первичный DNS и вторичный DNS.

Рисунок 5.8. Текущие параметры IPv6 на сетевой странице IPv6 Setting.

Таблица 5.4. Описание настраиваемых параметров IPv6.

Имя параметра	Описание	Заводская настройка по умолчанию
Autoconfig	Если установить флажок в этом поле, все параметры IPv6 будут автоматически настраиваться для пользователей. Эта функция основана на автоматической настройке параметров конфигурации без сохранения состояния, когда коммутатор использует для настройки IPv6-адреса информацию в сообщениях объявления, передаваемых маршрутизатором. Полученный адрес будет результатом конкатенации первых 64 битов адреса источника объявления маршрутизатора с расширенным уникальным идентификатором (EUI-64).	Флажок не установлен
DHCPv6	Если установить флажок в этом поле, IPv6-адрес и другие связанные значения будут автоматически назначаться DHCPv6-сервером в сети. В данном режиме поддерживается автоматическая настройка параметров конфигурации с сохранением состояния. Коммутатор генерирует сообщение запроса по протоколу DHCP, которое передается на адреса многоадресной рассылки всех DHCP-агентов для поиска DHCPv6-сервера. В другом варианте пользователь может установить IPv6-адрес вручную.	Флажок не установлен
Manual	Если пользователь установит флажок в этом поле, он должен будет заполнить поля Global Unicast Address, Prefix Length, и Gateway, которые описаны в данной таблице ниже. Следует отметить, что при выборе данной опции эти поля становятся доступными для ввода информации.	Флажок не установлен
Global Unicast Address	В этом поле указывается IPv6-адрес, маршрутизируемый в сети Интернет, с тремя верхними битами 001. Данный IPv6-адрес имеет формат 2XXX::/3.	Не заполняется
Prefix Length	В этом поле указывается длина префикса для IPv6-адреса, настроенного в предыдущем поле.	Не заполняется
Gateway	В этом поле указывается IPv6-адрес для IPv6-шлюза.	Не заполняется

Имя параметра	Описание	Заводская настройка по умолчанию
Manual DNS	Если пользователь установит флажок в этом поле, он должен будет вручную ввести адреса первичного и вторичного DNS-серверов для протокола IPv6. Следует отметить, что при выборе данной опции соответствующие два поля становятся доступными для ввода информации.	Флажок не установлен
Primary DNS	В этом поле указывается Ipv6-адрес первичного DNS-сервера, который будет использоваться данной сетью.	Не заполняется
Secondary DNS	В этом поле указывается IPv6-адрес вторичного DNS-сервера. Если сетевой коммутатор Ethernet не сможет подключиться к первичному DNS-серверу, он найдет вторичный DNS-сервер и попытается подключиться к нему.	Не заполняется

5.5 Подраздел Ping

Управляемый коммутатор Yarus Networks поддерживает сетевую утилиту под названием Ping, которая используется для тестирования связности узлов в сети.

На рисунке 5.9 показан пользовательский интерфейс для использования команды Ping.

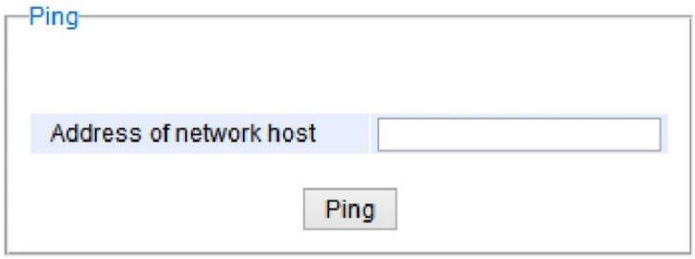


Рисунок 5.9. Сетевая страница утилиты Ping.

Пользователь может ввести в поле IP-адрес или доменное имя для проверки связности узлов в сети, как показано на рисунке 5.10.

Введите IP-адрес или имя домена, затем нажмите на кнопку "Ping" для запуска функции проверки достижимости.

Пример успешного результата проверки связности показан на рисунке 5.11, а результат неудачного тестирования - на рисунке 5.12.

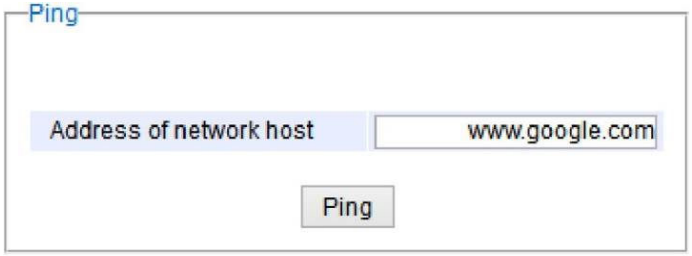


Рисунок 5.10. Пример использования команды Ping.

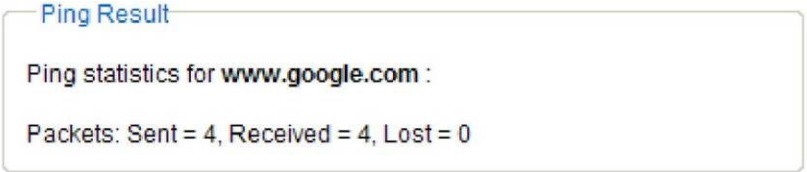


Рисунок 5.11. Пример успешного результата проверки связности.

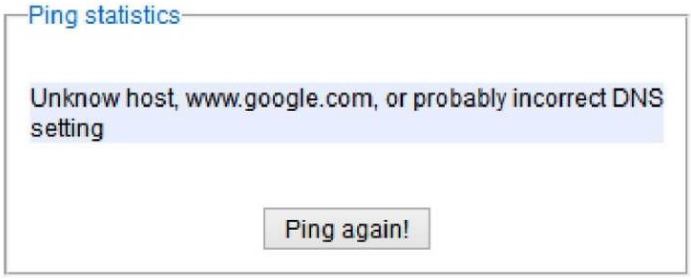


Рисунок 5.12. Пример неудачного результата проверки связности.

*** ПРИМЕЧАНИЕ:**

Чтобы использовать доменное имя вместо IP-адреса, пользователь должен сначала выбрать DNS-сервер. Это можно сделать в подразделе IP Setting раздела меню Administration.

5.6 Подраздел Ping6

Ping6 представляет собой сетевую утилиту диагностики. Эта утилита обычно используется для проверки достижимости устройства назначения для управляемого коммутатора и наоборот в сети с поддержкой протокола IPv6.

На рисунке 5.13 показан пользовательский интерфейс для использования команды Ping.

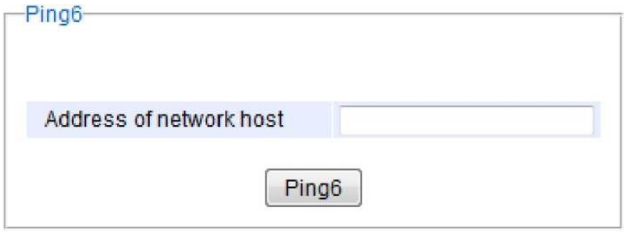


Рисунок 5.13. Сетевая страница утилиты Ping6.

Пользователь может указать в данном поле IPv6-адрес, чтобы проверить связность узлов в сети. Введите IPv6-адрес, затем щелкните с указателем на кнопке "Ping6" для запуска функции проверки достижимости.

Пример успешного результата тестирования с использованием утилиты Ping6 показан на рисунке 5.14.

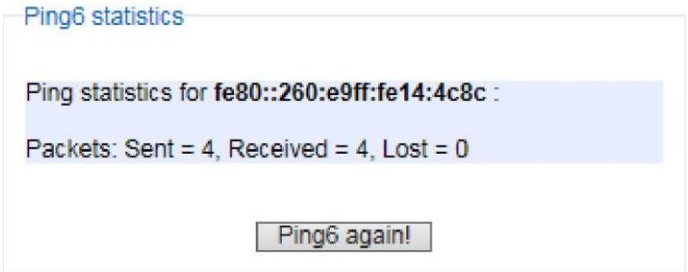


Рисунок 5.14. Пример успешного тестирования командой Ping6.

5.7 Подраздел Mirror Port

Чтобы упростить отслеживание активности в сети сетевым администратором, управляемый коммутатор поддерживает функцию зеркалирования портов.

Эта функция обеспечивает возможность мониторинга входящего и/или исходящего трафика

через один порт, который назначается портом зеркалирования.

Следует отметить, что зеркально отображаемый сетевой трафик может обрабатываться анализатором сетей или сниффером в целях повышения производительности сети или улучшения контроля безопасности.

На рисунке 5.15 показана сетевая страница подраздела Mirror Port.

Описание настраиваемых параметров зеркалирования портов в сводном виде представлено в таблице 5.5.

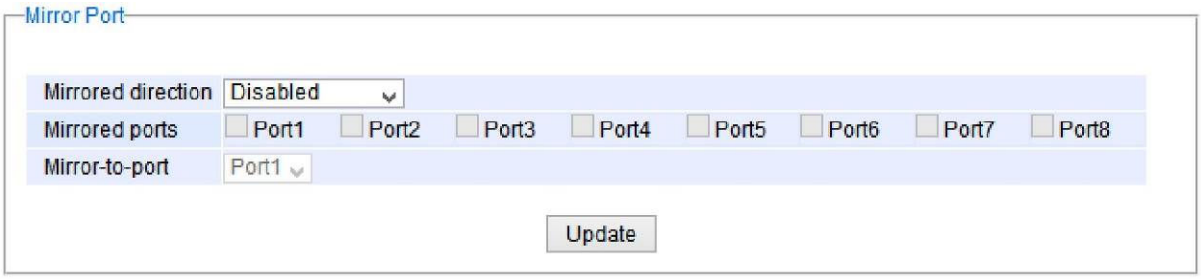


Рисунок 5.15. Сетевая страница подраздела Mirror Port.

*** ПРИМЕЧАНИЕ:**

Если совокупная пропускная способность контролируемых портов превысит объем трафика, который способен пропускать порт зеркалирования, может возникнуть состояние переполнения.

Таблица 5.5. Описание настраиваемых параметров функции зеркалирования портов.

Имя параметра	Описание	Заводская настройка по умолчанию
Monitored direction	Выбор контролируемого направления. - Disable: отключить контроль состояния портов. - Input data stream: контролировать только входящие потоки данных контролируемых портов. - Output data stream: контролировать только исходящие потоки данных контролируемых портов. - Input/Output data stream: контролировать и входящие, и исходящие потоки данных контролируемых портов.	Выключено
Monitored Port	Выбор портов для контроля.	Флажки нигде не установлены
Mirror-to-port	Выбор порта зеркалирования, который будет использоваться для контроля активности контролируемых портов.	Port 1

5.8 Подраздел System Time

Промышленный управляемый коммутатор Yarus Networks поддерживает внутренний календарь и часы (системное время), которые можно настраивать вручную или в автоматическом режиме.

На рисунке 5.16 показана сетевая страница System Time and SNTP.

Пользователь может выбрать вариант ввода текущих значений даты и времени вручную.

На странице имеется раскрывающийся список Time Zone, который можно использовать для выбора пояса местного времени.

Если коммутатор установлен в регионе, где практикуется перевод на летнее время (см. пояснение в примечании ниже), установите флажок для опции Enable в поле Daylight Saving Time.

Затем пользователь должен ввести значения начальной даты, конечной даты и сдвига в часах в полях Start Date, End Date и Offset соответственно.

ПРИМЕЧАНИЕ: чтобы изменить значения даты или времени, пользователь должен выйти из системы.

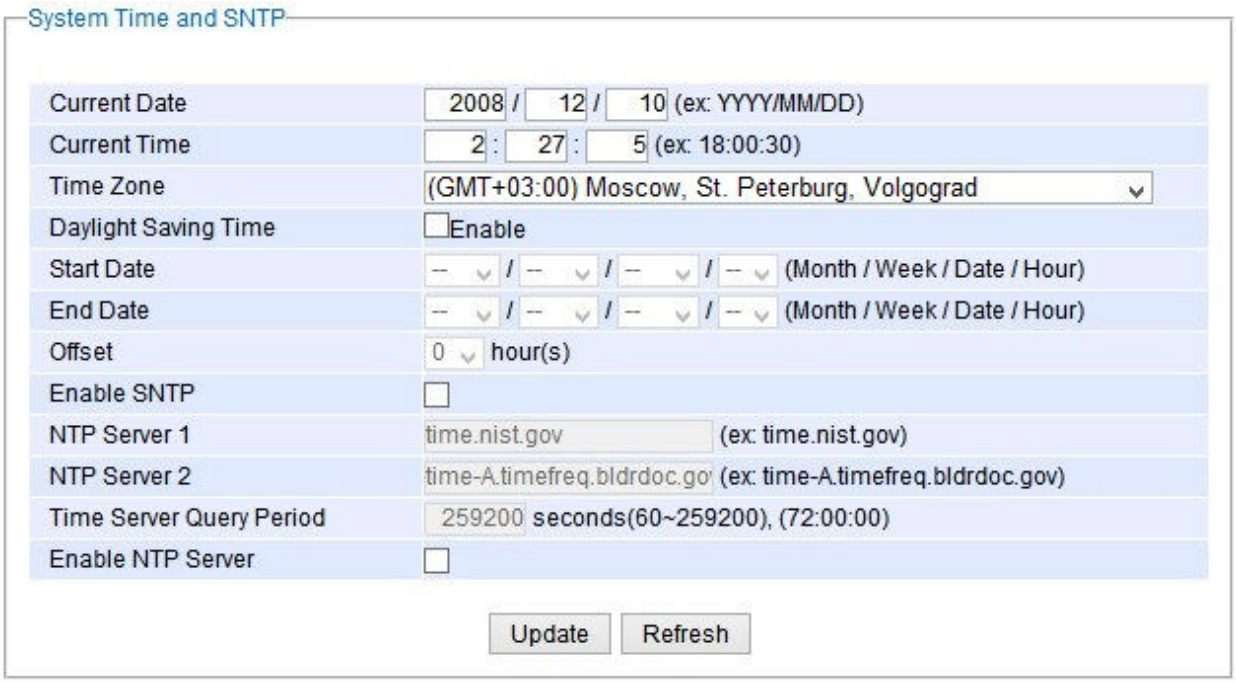


Рисунок 5.16. Сетевая страница для настройки системного времени и протокола SNTP.

Чтобы настроить дату и время в автоматическом режиме, пользователь может активировать простой протокол сетевого времени (SNTP), установив флажок для опции Enable SNTP (см. пояснение в примечании ниже).

Затем пользователь должен заполнить поля NTP Server 1 и NTP Server 2, указав данные NTP-серверов, которые будут использоваться в качестве эталонных серверов для синхронизации даты и времени.

Пользователь может ввести интервал синхронизации в поле Time Server Query Period.

Значение интервала указывается в секундах.

Продолжительность интервала зависит от того, какой уровень точности часов коммутатора требуется пользователю.

И, наконец, управляемый коммутатор можно использовать в качестве сервера протокола сетевого времени для локальных устройств.

Чтобы активировать эту функцию, установите флажок для опции Enable NTP Server. Описание каждого настраиваемого параметра приведено в таблице 5.6.

Таблица 5.6. Описание настраиваемых параметров системного времени и протокола SNTP.

Имя параметра	Описание	Заводская настройка по умолчанию
Current Date	Данное поле можно использовать для ввода местной даты в формате гггг/мм/дд.	Нет
Current Time	Данное поле можно использовать для ввода местного времени в 24-часовом формате.	Нет
Time Zone	Данное поле предназначено для указания часового пояса, в котором находится пользователь.	(GMT+03:00) Moscow, St. Peterburg, Volgograd
Daylight Saving	Активация или отключение функции перехода на летнее время.	Флажок не установлен
Start Date	В данном поле указывается дата начала использования летнего времени.	Не заполняется
End Date	В данном поле указывается дата окончания использования летнего времени.	Не заполняется
Offset	В данном поле указывается величина сдвига в часах при переходе на летнее время и обратно. См. примечание ниже.	0
Enable SNTP	Выбор данной опции активирует функцию протокола SNTP. См. примечание ниже.	Флажок не установлен
NTP Server 1	В данном поле указывается первый IP-адрес или адрес домена NTP-сервера.	time.nist.gov
NTP Server 2	В данном поле указывается второй IP-адрес или адрес домена NTP-сервера. Коммутатор выполнит поиск второго NTP-сервера в случае, если попытка подключения к первому NTP-серверу закончится неудачей.	Time-A.timefreq.bldrdoc.gov
Time Server Query Period	Значение этого параметра определяет частоту обновления времени по данным NTP-сервера. Если для конечного устройства не требуется слишком высокая точность, рекомендуется установить более продолжительный интервал, чтобы уменьшить нагрузку на коммутатор. Значение может быть указано в диапазоне от 60 до 259200 секунд (т.е. до 72 часов).	259 200 секунд
Enable NTP Server	Выбор этой опции активирует присоединенную программу протокола сетевого времени (NTP) на управляемом коммутаторе, что позволит другим устройствам в сети синхронизировать свои часы с часами данного коммутатора, используя протокол NTP.	Флажок не установлен
NTP Server Stratum	Уровень слоя (0 - 15) определяет удаление устройства от эталонного синхрогенератора. Описание слоев для NTP-сервера приведено ниже: • Слой 0 соответствует собственно "эталонным" часам. Обычно в качестве таковых используются атомные часы, часы глобальной системы определения координат (GPS) или радио-часы.	10

Имя параметра	Описание	Заводская настройка по умолчанию
	• Слой 1 соответствует любой машине, которая синхронизирует свои системные часы непосредственно с эталонными часами, которые относятся к слою 0. В качестве примера такой машины можно привести сервер с модулем GPS, подключенным к одному из его последовательных портов. • Слой 2 соответствует любой машине, которая синхронизирует свои системные часы с часами сервера, который относится к слою 1. • Слой 3 соответствует любой машине, которая синхронизирует свои системные часы с часами сервера, который относится к слою 2, и так далее. NTP-протокол не позволяет клиентам принимать время от устройств слоя 15, так как слой 15 является низшим слоем протокола NTP.	

*** ПРИМЕЧАНИЕ:**

- Летнее время: В некоторых регионах местное время корректируется на летний сезон, чтобы предоставить возможность использовать дополнительный час светлого времени суток. При переходе на летнее время и обратно время обычно смещается на один час вперед или назад соответственно.

- SNTP: Простой протокол сетевого времени используется для синхронизации часов компьютерных систем со стандартным NTP-сервером. В качестве примера NTP-сервера можно привести сервера с адресами time.nist.gov и time-A.timefreq.bldrdoc.gov.

5.9 Подраздел Modbus Setting

Управляемый коммутатор Yarus Networks можно подключить к сети Modbus с использованием протокола Modbus TCP/IP, который является стандартным промышленным сетевым протоколом для управления автоматизированным оборудованием.

В такой конфигурации данные состояния управляемого коммутатора и значения настраиваемых параметров можно считывать и записывать через протокол Modbus TCP/IP, который работает подобно браузеру базы управляющей информации.

При этом управляемый коммутатор получает статус подчиненного устройства Modbus, которое можно настраивать удаленно с главного устройства Modbus.

Адрес подчиненного устройства Modbus должен быть согласован с адресными настройками в главном устройстве Modbus.

Чтобы получить доступ к управляемому коммутатору, пользователь должен назначить адрес Modbus согласно описанию в данном подразделе.

Таблица распределения памяти Modbus, в которой перечислены адреса и описание всех

регистров в управляемом коммутаторе, представлена в разделе с описанием схемы распределения памяти Modbus.

На рисунке 5.17 показана сетевая страница подраздела Modbus Setting на которой пользователь может указать идентификационный адрес Modbus.

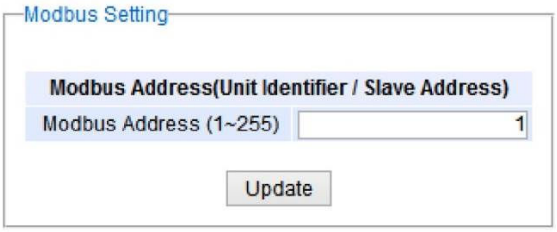


Рисунок 5.17. Сетевая страница для настройки адреса Modbus.

Для настройки параметров коммутатора пользователь может использовать приложения, совместимые с протоколом Modbus TCP/IP, такие как утилита Modbus Poll.

Для сведения: утилиту Modbus Poll можно загрузить, перейдя по ссылке http://www.modbustools.com/download.html.

При подготовке данного документа использовалась версия Modbus Poll 64-bit version 7.0.0, Build 1027.

*** ПРИМЕЧАНИЕ**: Данный коммутатор поддерживает только функциональные коды Modbus 03, 04 (для чтения) и 06 (для записи).

Регистры чтения (на данном примере показано, как считывать IP-адрес коммутатора).

Address	Data Type	Read/Write	Description
0x0051 (81)	2 words	R	IP Address of switch Ex: IP = 10.0.50.1 Word 0 Hi byte = 0x0A Word 0 Lo byte = 0x00 Word 1 Hi byte = 0x32 Word 1 Lo byte = 0x01

Рисунок 5.18. Таблица отображения адресов Modbus для IP-адреса коммутатора.

1. Удостоверьтесь, что компьютер, на котором Вы работаете, имеет статус ведущего устройства (главного устройства Modbus) и подключен к целевому коммутатору (подчиненному устройству Modbus) по сети Ethernet.

2. Запустите утилиту Modbus Poll на ведущем компьютере. Для информации: по истечении 30-дневного периода опробования для использования утилиты Modbus Poll потребуется ввести регистрационный ключ. Более того, в период опробования продолжительность сеанса подключения к управляемому коммутатору ограничивается 10 минутами.

3. Щелкните с указателем на кнопке Connection, расположенной на главной панели инструментов, и выберите пункт Connect..., чтобы открыть диалоговое окно настройки соединения Connection Setup, показанное на рисунке 5.19.

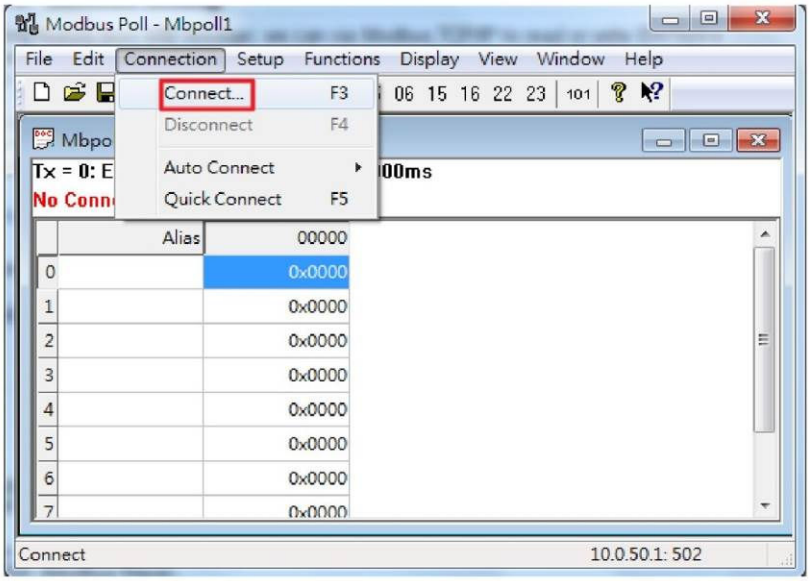


Рисунок 5.19. Вход в меню установления соединения утилиты Modbus Poll.

4. Выберите Modbus TCP/IP в качестве режима подключения и введите IP-адрес коммутатора в поле IP Address или Node Name раздела Remote Server в нижней части окна, как показано на рисунке 5.20.

В качестве номера порта укажите значение 502. Затем щелкните с указателем на кнопке OK.

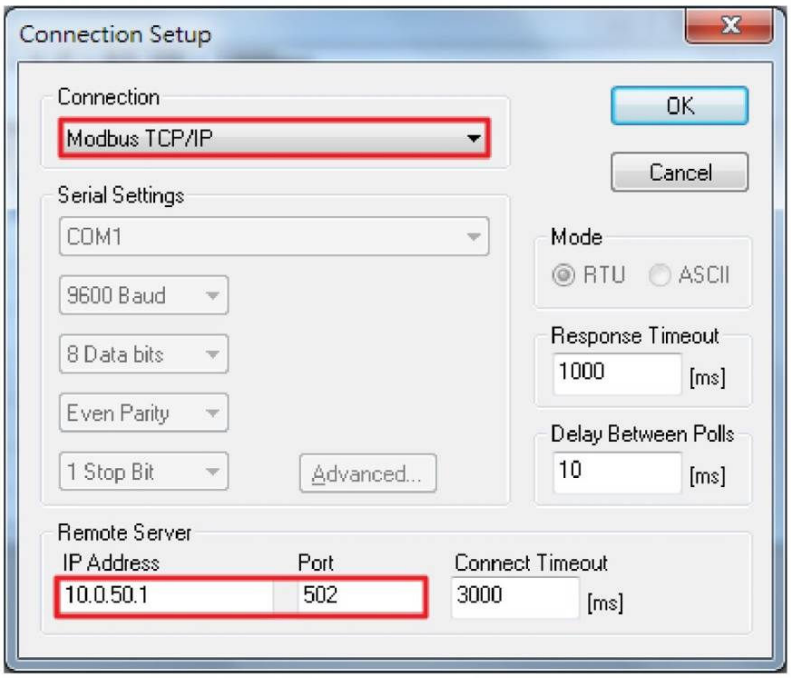


Рисунок 5.20. Установление соединения для утилиты Modbus Poll.

5. В окне Mbpoll1, выберите группу ячеек в строках с 0 по 2, как показано на рисунке 5.21. Для этого щелкните с указателем на ячейках во втором столбце в строках с 0 по 2, удерживая нажатой клавишу Shift.

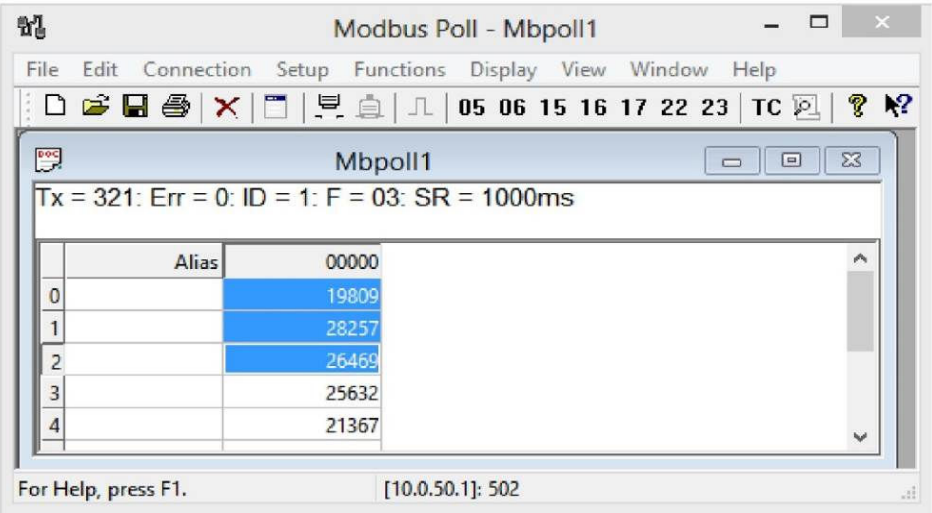


Рисунок 5.21. Выбор группы ячеек в утилите Modbus Poll.

6. Установите для ячеек, выбранных на предыдущем этапе, шестнадцатеричный формат отображения. Для этого откройте выпадающее меню Display и выберите в нем значение Hex, как показано на рисунке 5.22.

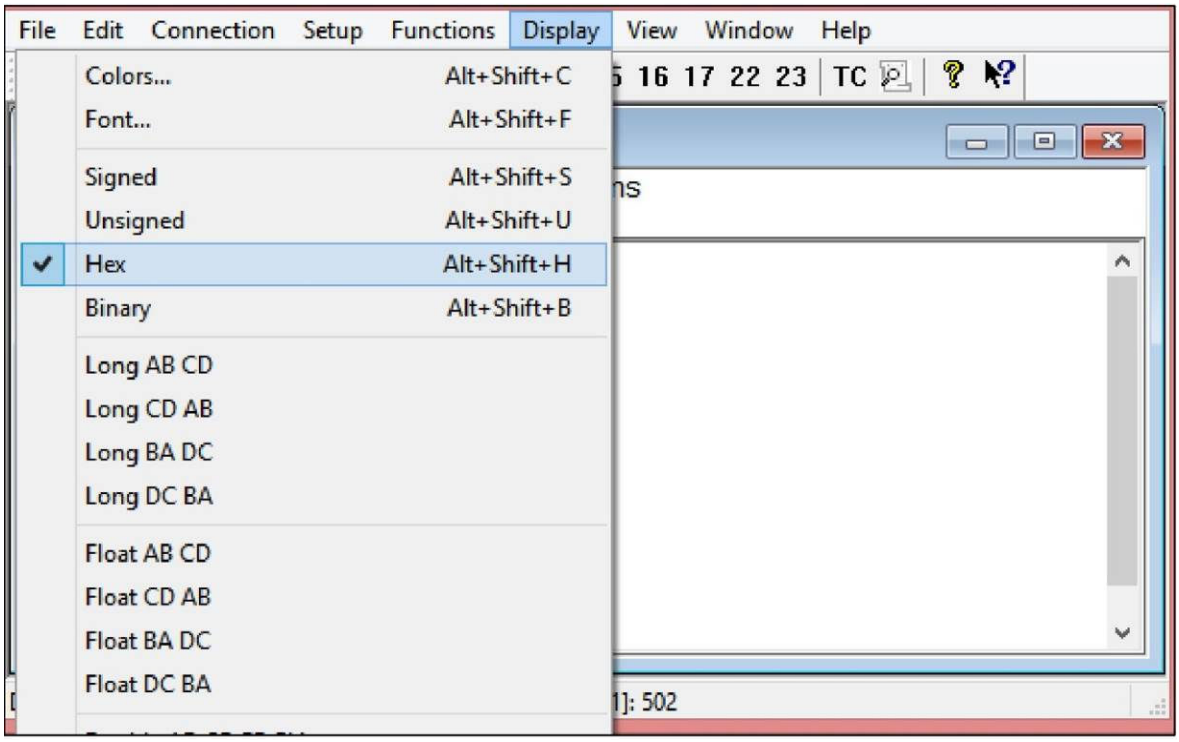


Рисунок 5.22. Выбор шестнадцатеричного формата отображения в утилите Modbus Poll.

7. Щелкните с указателем на кнопке Setup, чтобы открыть выпадающее меню, и выберите в нем опцию Read/Write Definition, как показано на рисунке 5.23.

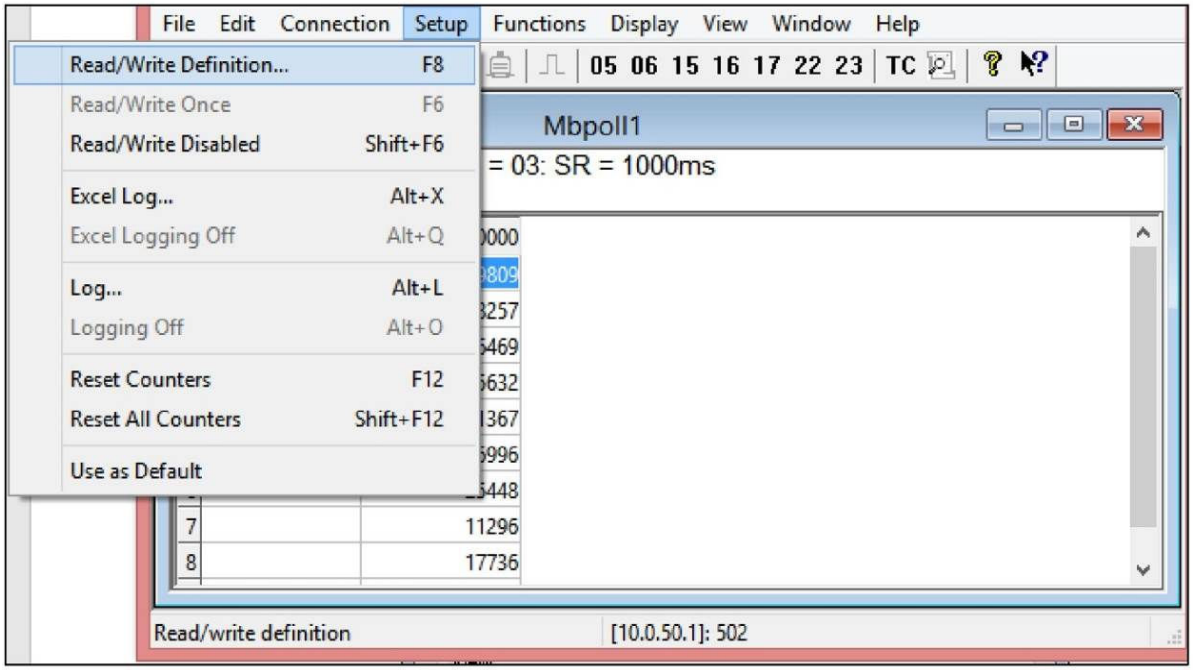


Рисунок 5.23. Опция описания чтения-записи для настройки утилиты Modbus Poll.

8. В поле Slave ID введите идентификатор ведомого устройства для утилиты Modbus Poll, как показано на рисунке 5.24, который должен соответствовать идентификационному адресу Modbus = 1.

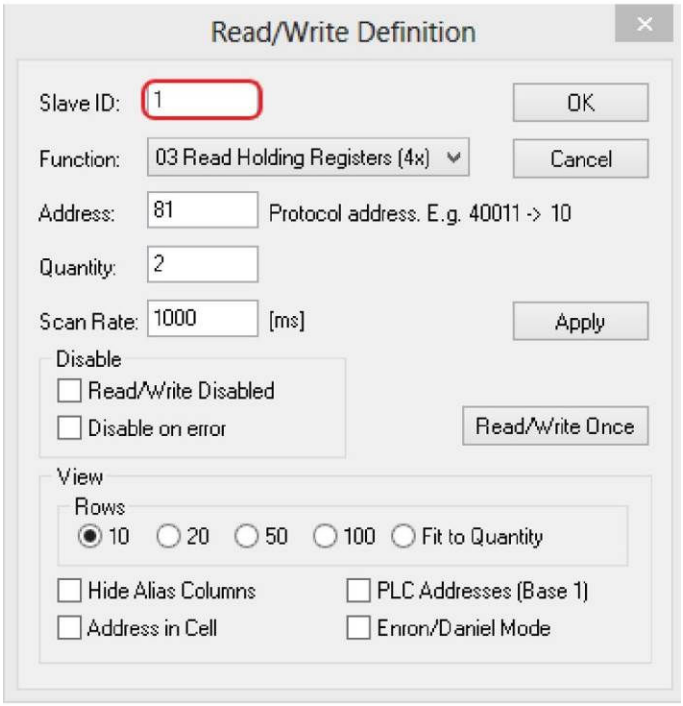


Рисунок 5.24. Устанавливается значение 1 идентификатора ведомого устройства утилиты Modbus Poll.

9. В поле Function выберите значение 03 или 04, как показано на рисунке 5.25, так как управляемый коммутатор поддерживает только функциональные коды 03 и 04.

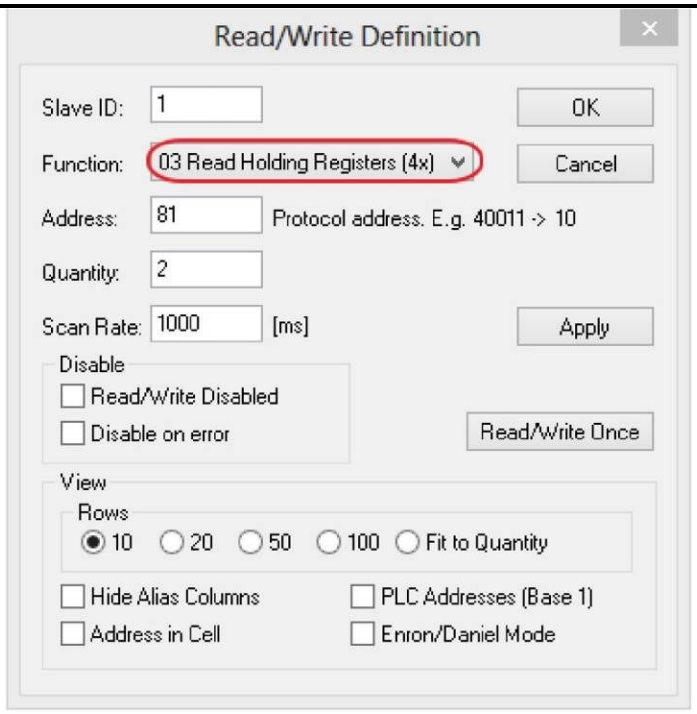


Рисунок 5.25. В поле Function утилиты Modbus Poll выбран код 03.

10. В полях Address и Quantity введите значения 81 и 2 соответственно, как показано на рисунке 5.26.

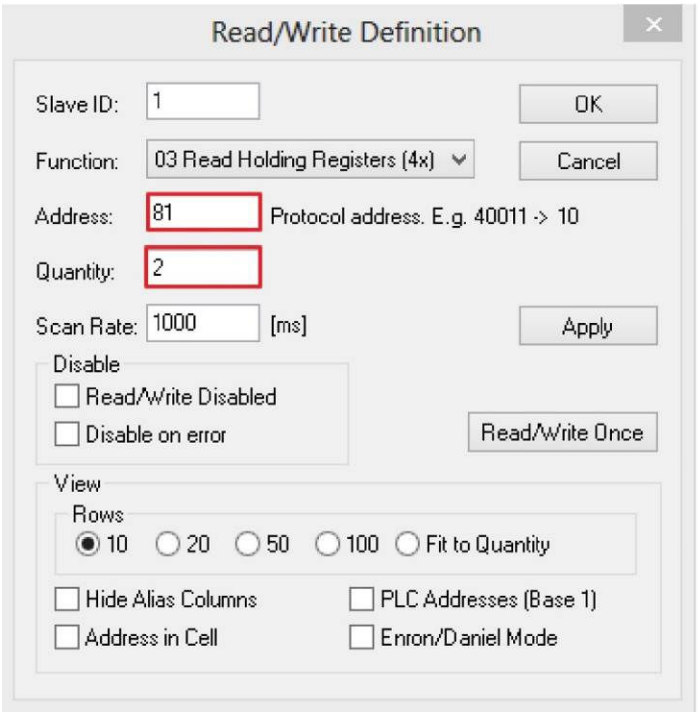


Рисунок 5.26. Настройка начального адреса и количества в утилите Modbus Poll.

11. Щелкните на кнопке OK, чтобы считать IP-адрес коммутатора.

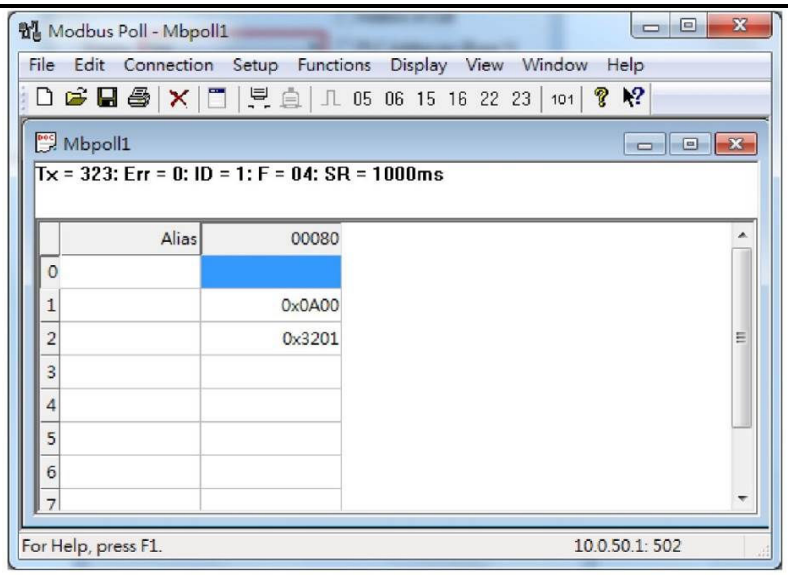


Рисунок 5.27. Адреса 81 и 82 в памяти Modbus определяют местоположение IP-адреса устройства.

12. Утилита Modbus Poll получит значения 0x0A, 0x00, 0x32, 0x01. Это означает, что коммутатору назначен IP-адрес 10.0.50.1, как показано на рисунке 5.28.

Регистры записи (на данном примере показано, как удалять статистику по портам).

Address	Data Type	Read/Write	Description
0x0100 (256)	1 word	W	Clear Port Statistics 0x0001: Do clear action

Рисунок 5.28. Таблица отображения адресов Modbus для удаления статистики по портам.

1. Просмотрите данные по входящему и исходящему трафику для портов на странице Port Statistics как показано на рисунке 5.29.

Port Statistics

Port	Enable	Link	Tx	Tx Error	Tx Rate(Kbps)	Rx	Rx Error	Rx Rate(Kbps)
Port1	On	Up	11700	0	0	35115	0	0
Port2	On	Down	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0
Port4	On	Down	0	0	0	0	0	0
PortG1	On	Down	0	0	0	0	0	0
PortG2	On	Down	0	0	0	0	0	0

Clear Refresh

Рисунок 5.29. Данные по портам на сетевой странице Port Statistics.

2. Выберите функциональный код 06 на панели инструментов, как показано на рисунке 5.30.

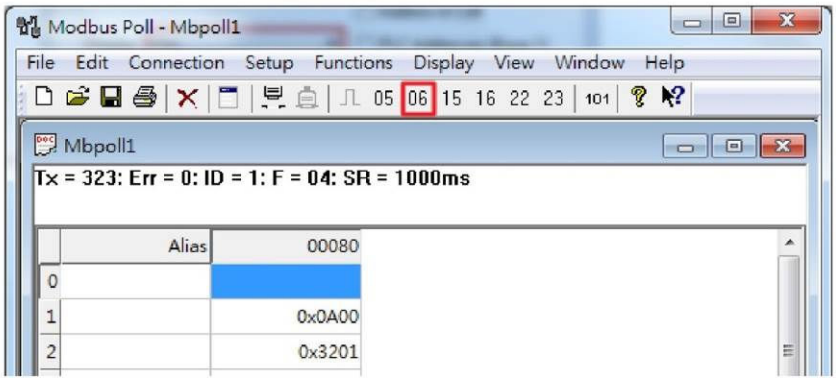


Рисунок 5.30. Выбор функционального кода 06 для утилиты Modbus Poll.

3. В поле Address введите значение 256, а в поле Value (HEX) - значение 1, как показано на рисунке 5.31, затем щелкните с указателем на кнопке "Send".

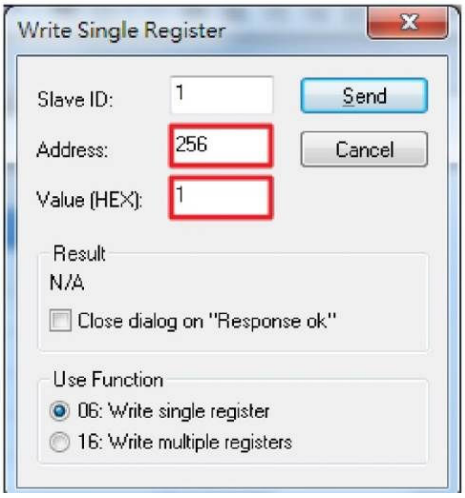


Рисунок 5.31. Очистка статистики по портам коммутатора с помощью утилиты Modbus.

4. Проверьте статистику по портам в подразделе Web UI меню управляемого коммутатора, как показано на рисунке 5.32. Статистические данные по обработке пакетов удалены.

Port Statistics

Port	Enable	Link	Tx	Tx Error	Tx Rate(Kbps)	Rx	Rx Error	Rx Rate(Kbps)
Port1	On	Up	8	0	0	27	0	0
Port2	On	Down	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0
Port4	On	Down	0	0	0	0	0	0
PortG1	On	Down	0	0	0	0	0	0
PortG2	On	Down	0	0	0	0	0	0

Clear Refresh

Рисунок 5.32. Статистика по портам после обнуления.

5.10 Подраздел TraceRT

Управляемый коммутатор Yarus Networks также предоставляет другой инструмент диагностики сети, называемый TraceRT или traceroute, для проверки возможных сетевых маршрутов и определения задержки прохождения пакетов по IP-сети. Веб-страница TraceRT показана на рисунке 5.33. Пользователи могут ввести URL-адрес или IP-адрес пункта назначения в поле Destination Address. После нажатия на кнопку Trace коммутатор выдаст

список статистических данных трассировки, как показано на рисунке 5.34 в качестве примера. Каждая запись в отчете будет содержать адрес каждого последующего хоста вдоль маршрута или траектории до тех пор, пока он не достигнет пункта назначения, вместе с суммой среднего времени (в миллисекундах) каждого перехода.

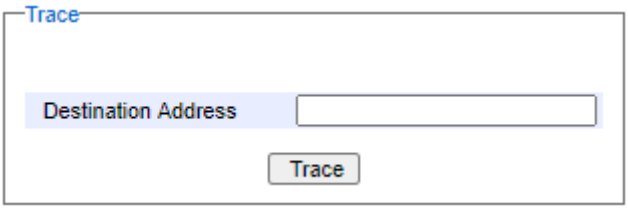


Рисунок 5.33. Веб страница TraceRT.

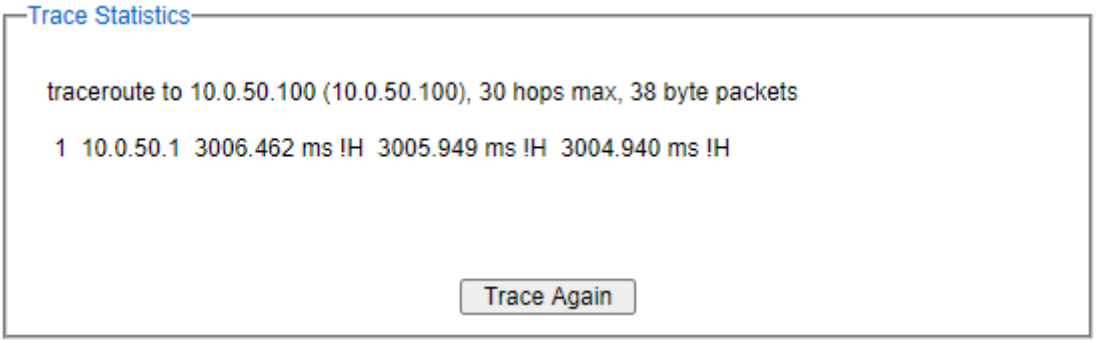


Рисунок 5.34. Результат трассировки.

5.11 Подраздел Precision Time Protocol (PTP)

Протокол точного времени (PTP) используется для высокоточного отсчета времени.

Он может использоваться системами измерения и управления в локальной сети, которые требуют точной синхронизации времени.

Соответствующий раздел меню состоит из двух подразделов: PTP Setting и H/W PTP, как показано на рисунке 5.35.

Рисунок 5.35. Подразделы меню PTP.

5.11.1 Подраздел PTP Setting

Сетевая страница PTP Setting предназначена для настройки параметров PTP-протокола. На рисунке 5.36 показана сетевая страница конфигурации PTP-протокола, на которой пользователь может не только настраивать параметры, но и проверять состояние протокола.

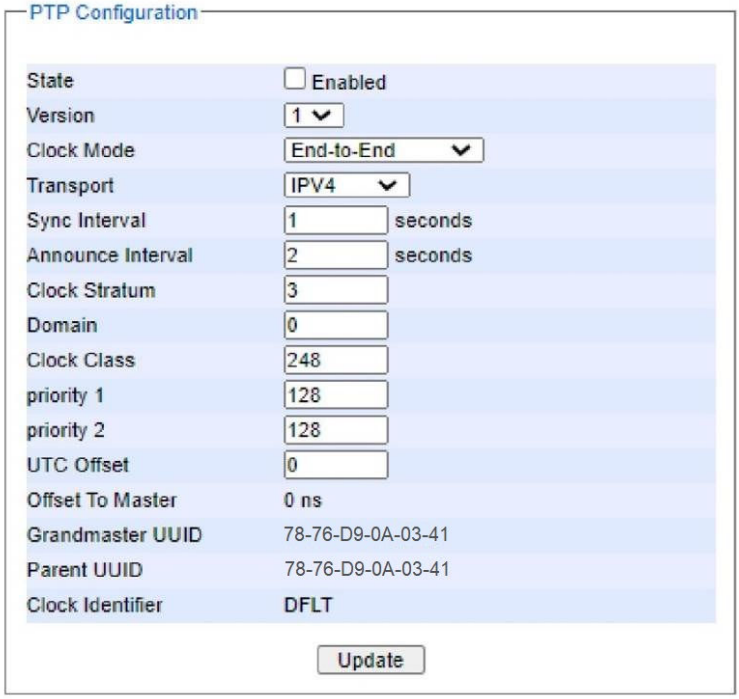
В окне, показанном в нижней части рисунка, пользователь может активировать или отключать функцию PTP-протокола отдельно для каждого порта и проверять текущий статус функции.

Чтобы активировать PTP-протокол на управляемом коммутаторе установите флажок для опции Enable в поле State, как показано на рисунке.

Следует понимать, что PTP-протокол не будет активирован для порта без флажка активации в поле состояния.

См. описание параметров конфигурации PTP-протокола в таблице 5.7 и описание данных о портах с поддержкой PTP-протокола в таблице 5.8.

После завершения настройки параметров PTP-протокола нужно щелкнуть с указателем на кнопке Update, чтобы новая конфигурация вступила в силу.



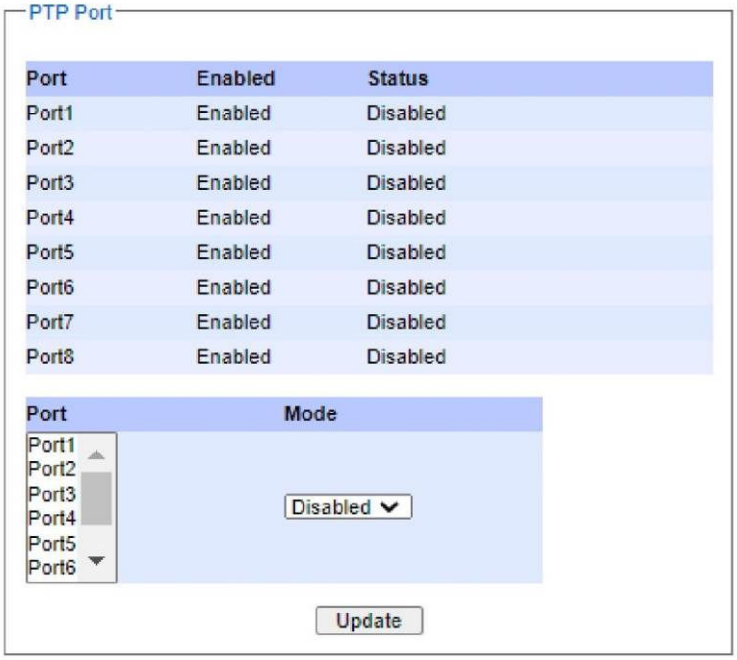


Рисунок 5.36. Сетевая страница настройки параметров PTP-протокола..

Таблица 5.7. Описание настраиваемых параметров PTP-протокола.

Имя параметра	Описание	Заводская настройка по умолчанию
State	Активация и отключение функции PTP-протокола. Это - основная опция. Функция PTP-протокола должна быть активирована, чтобы она работала согласно значениям остальных параметров, указанным в этой таблице (Таблица 2 - 10).	Флажок не установлен
Version	Укажите рабочую версию PTP-протокола. Следует учитывать, что поддерживаются версии 1 (IEEE 1588 - 2002) и 2 (IEEE 1588 - 2008).	1
Clock Mode	Выберите режим синхрогенератора для PTP-протокола (протокола точного времени). Данный коммутатор поддерживает следующие четыре режима: End-End Boundary Clock (сквозной граничный тактовый генератор), End-End Transparent Clock (сквозной прозрачный тактовый генератор), Peer-Peer Boundary Clock (граничный тактовый генератор для одноранговых узлов) и Peer-Peer Transparent Clock (прозрачный тактовый генератор для одноранговых узлов).	End-to-End
Transport	Выберите многоадресный транспортный протокол Ethernet (второго уровня) или протокол передачи пользовательских датаграмм (UDP/IPv4) третьего уровня для передачи сообщений PTP-протокола (протокола точного времени).	IPV4
Sync Interval	Установите интервалы времени для передачи синхропакетов. Чем меньше интервал, тем чаще выполняется синхронизация, и тем больше нагрузка на устройство и сеть.	1
Announce Interval		2
Clock Stratum	Установите значение слоя для синхрогенератора. Меньшие значения получают приоритет при выборе основного тактового генератора с использованием алгоритма выбора оптимального основного тактового генератора (BMCA).	3
Domain		0

Имя параметра	Описание	Заводская настройка по умолчанию
Clock Class	В поле Clock Class указывается уровень точности синхрогенератора. Этот атрибут применяется для обычных или граничных тактовых генераторов. Он обозначает трассируемость времени или частоту, распределяемую тактовым генератором гроссмейстера. Соответствующие определения, допустимые значения и пояснения приведены в стандарте IEEE 1588 – 2008 (Таблица 5).	248
priority 1	В этом поле указывается приоритет 1 синхрогенератора (только в версии 2 PTP-протокола). Меньшие значения получают приоритет при выборе основного тактового генератора с использованием алгоритма выбора оптимального основного тактового генератора. Значение 0 соответствует наивысшему приоритету, а значение 255 – наинизшему.	128
priority 2	В этом поле указывается приоритет 2 синхрогенератора (только в версии 2 PTP-протокола). Меньшие значения получают приоритет при выборе основного тактового генератора с использованием алгоритма выбора оптимального основного тактового генератора (BMCA). Значение 0 соответствует наивысшему приоритету, а значение 255 – наинизшему.	128
UTC Offset	Величина коррекции для всемирного скоординированного времени (UTC).	0
Offset to Master	Время смещения относительно основного тактового генератора.	Нет
Grandmaster UUID	Универсальный уникальный идентификатор ведущего устройства для версии 1 PTP-протокола.	Нет
Parent UUID	Универсальный уникальный идентификатор родительского основного устройства для версии 1 PTP-протокола.	Нет
Clock Identifier	Идентификатор тактового генератора для версии 1 PTP-протокола.	Нет

Таблица 5.8. Описание настраиваемых параметров портов с поддержкой PTP-протокола.

Имя параметра	Описание	Заводская настройка по умолчанию
Port	Номер порта.	-
Enabled	Информация о режиме порта в данном поле указывает статус функции PTP-протокола для порта – активирована или отключена.	Активировано
Status	В этом поле указывается рабочее состояние PTP-протокола на порте. Если функция на порте активирована, но не работает, нужно активировать функцию в основных настройках PTP-протокола.	Выключено
Mode	Активация и отключение функции PTP-протокола для порта.	Выключено

5.11.2 Подраздел Hardware PTP Setting

В этом подразделе пользователь может активировать аппаратный прозрачный тактовый генератор. Прозрачный тактовый генератор способен компенсировать переменную латентность коммутатора.

Эта функция может быть реализована посредством измерения времени прохождения

сообщения о событии PTP-протокола через коммутатор, которое также называется временем пребывания.

Время пребывания сообщается получателю непосредственно в сообщении о событии PTP-протокола.

С этой целью в сообщение добавляется специальное поле под названием Correction Field, в котором указывается продолжительность времени задержки, накопленная суммированием значений времени пребывания в различных узлах сети (сообщение в процессе передачи может пройти через несколько коммутаторов).

Чтобы активировать аппаратный прозрачный тактовый генератор, установите флажок в поле H/W TC Enabled, затем щелкните с указателем на кнопке Update, как показано на рисунке 5.37.

Рисунок 5.37. Настройка аппаратных параметров для PTP-протокола.

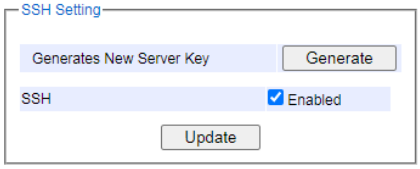
5.12 Подраздел Secure Shell – SSH

Управляемым коммутатором можно управлять через интерфейс командной строки. Пользователь может удаленно подключаться к управляемому коммутатору через любой его порт, используя на собственное усмотрение протокол безопасной оболочки (SSH) или Telnet. В данном подразделе представлен протокол SSH. Использование Telnet рассматривается в следующем подразделе.

Чтобы активировать протокол SSH, установите флажок для опции Enabled в поле SSH, как показано на рисунке 5.38.

Сначала сервер передает клиенту открытый ключ, а клиент проверяет корректность принятого открытого ключа. Если ключ передан неправильно, сервер отказывает в установлении соединения.

Щелкните с указателем на кнопке "Generate", чтобы изменить и повторно генерировать ключ сервера, затем получите от сервера другой открытый ключ, как показано на рисунке.



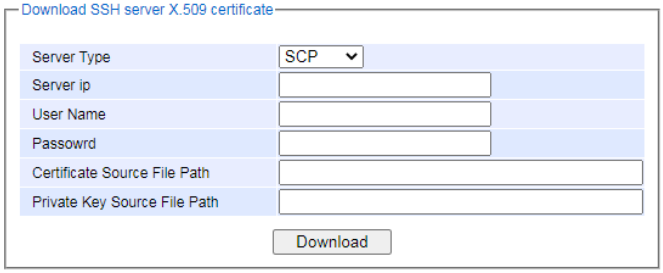


Рисунок 5.38. Сетевая страница настройки параметров протокола SSH.

Таблица 5.9. Описания копирования сертификата SSH.

Имя параметра	Описание
Server Type	Выберите тип сервера для копирования файла, поддерживаемые параметры: SFTP/ SCP
Server IP	IP адрес сервера
User Name	Пароль пользователя для файлового сервера
Password	Имя пользователя для файлового сервера
Certificate Source File Path	Путь к файлу сертификата, хранящемуся на файловом сервере
Private Key Source File Path	Путь к файлу закрытого ключа, хранящемуся на файловом сервере.
Download	Загрузка файл с файлового сервера на устройство

ПРИМЕЧАНИЕ:

1. Управляемый коммутатор поддерживает обе версии протокола SSH - 1 (SSH1) и 2 (SSH2).

2. Сервер генерирует ключ повторно, если параметры управляемого коммутатора сбрасываются на заводские настройки, либо если принятый ключ не существует.

Версии 1 и 2 протокола SSH поддерживают следующие общие функции:

1. Клиентские программы, которые используют протокол SSH, могут удаленно выполнять вход в систему, команды и безопасное копирование файлов во всей сети.

2. Протоколом SSH поддерживает несколько выбираемых алгоритмов шифрования и механизмов проверки подлинности.

3. Агент протокола SSH может кэшировать ключи для упрощения доступа при установлении следующих сеансов.

В версии 2 протокола SSH добавлен целый ряд новых возможностей, которые сделали продукт более мощным и универсальным. Эти новые возможности включают:

1. Применение новых стандартов шифрования: стандарт тройного шифрования данных (стандарт DES с тремя ключами) и улучшенный стандарт шифрования (AES).

2. Использование алгоритма звукового криптографического кода проверки подлинности

сообщений (MAC) для проверки целостности. В качестве примеров алгоритмов (функций) безопасного хеширования, которые используются в качестве MAC-алгоритмов в версии 2 протокола SSH, можно привести алгоритм MD5 и алгоритм безопасного хеширования 1 (SHA-1).

3. Поддержка сертификатов с открытым ключом.

5.13 Подраздел Telnet

Данный подраздел позволяет пользователю настраивать параметры протокола Telnet для управляемого коммутатора.

При использовании интерфейса командной строки для настройки параметров конфигурации протокол Telnet практически ничем не отличается от протокола SSH (см. описание в предыдущем разделе) за исключением того, что протокол SSH шифрует все передаваемые данные.

Для управления протоколом Telnet данный управляемый коммутатор поддерживает только функцию активации или отключения, которая настраивается в данном подразделе меню. По умолчанию протокол Telnet активирован.

После изменения значения щелкните с указателем на кнопке Update, чтобы сохранить измененные настройки управляемого коммутатора.

На рисунке 5.39 показана сетевая страница настройки параметров протокола Telnet.

Следует отметить, что по соображениям обеспечения безопасности управляемого коммутатора пользователям рекомендуется использовать протокол SSH, а не Telnet.

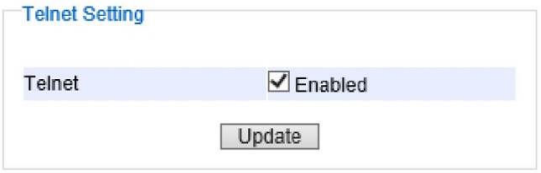


Рисунок 5.39. Сетевая страница настройки параметров протокола Telnet.

5.14 Подраздел HTTPS

В данном подразделе меню пользователь настраивать параметры протокола HTTPS (протокол защищенной передачи гипертекста) для сетевого пользовательского интерфейса администрирования.

Эта функция шифрует стандартные сообщения протокола HTTP, передаваемые между коммутатором и клиентским ПК, для защиты данных, передаваемых по сети.

Чтобы получить доступ к сетевому графическому пользовательскому интерфейсу, когда эта опция активирована, пользователь должен обращаться к коммутатору через https://10.0.50.1, чем обеспечивается дополнительная защита в процессе настройки параметров конфигурации устройства.

Следует отметить, что после активации данной функции любой HTTP-запрос на доступ к сетевой консоли управляемого коммутатора будет принудительно перенаправлен по соединению https.

После изменения значения щелкните с указателем на кнопке Update, чтобы сохранить измененные настройки управляемого коммутатора см. рисунок 5.40.

HTTPS создает защищенный канал по небезопасной сети с помощью ключа сертификата, пользователь может загрузить сертификат x.509 в качестве асимметричного ключа.

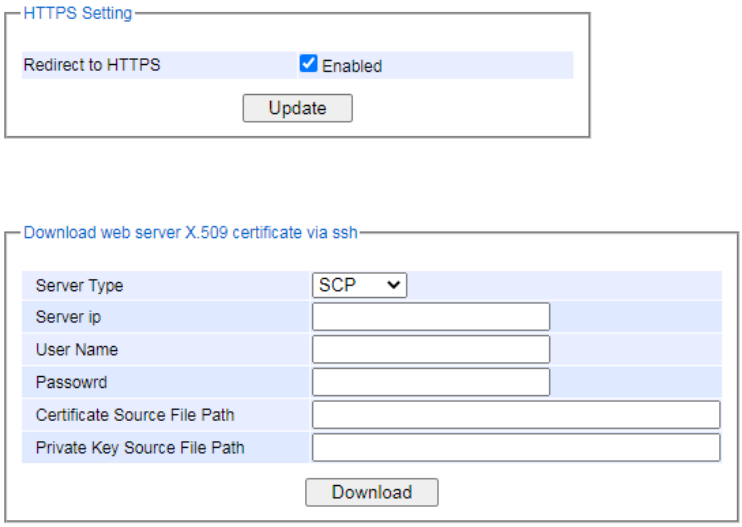


Рисунок 5.40. Сетевая страница настройки HTTPS

Таблица 5.10. Описания копирования сертификата HTTPS.

Имя параметра	**Описание**
Server Type	Выберите тип сервера для копирования файла, поддерживаемые параметры: SFTP/ SCP
Server IP	IP адрес сервера
Password	Пароль пользователя для файлового сервера
User Name	Имя пользователя для файлового сервера
Certificate Source File Path	Путь к файлу сертификата, хранящемуся на файловом сервере
Private Key Source File Path	Путь к файлу закрытого ключа, хранящемуся на файловом сервере.
Download	Загрузка файл с файлового сервера на устройство

5.15 Подраздел DIP Switch

В данном подразделе отображается состояние DIP-переключателей, установленных сверху на корпусе управляемого коммутатора. На рисунке 5.41 показана сетевая страница с данными о DIP - переключателях.

В нижней части страницы пользователь может активировать или заблокировать физическое управление DIP-переключателями, выбрав или отменив выбор опции DIP Switch Control.

Этот переключатель предоставляет простой и удобный альтернативный способ настройки защитного переключения для кольца Ethernet (ERPS), iA-кольца или совместимого кольца вместо изменения значений настраиваемых параметров через интернет-браузер.

После выбора или отмены выбора данной опции щелкните с указателем на кнопке Update,

чтобы изменения вступили в силу на управляемом коммутаторе.

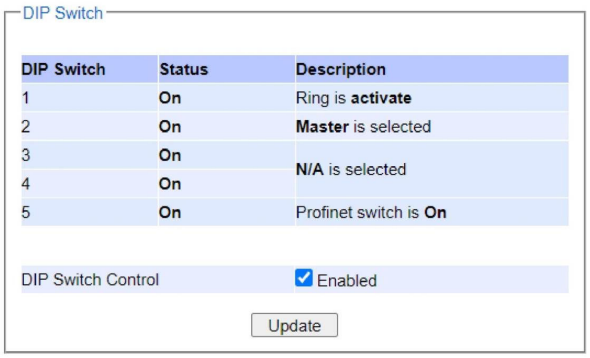


Рисунок 5.41. Сетевая страница состояния DIP–переключателей.

5.16 Подраздел sFlow

Технология sFlow (сокращенно "выборка из потока") представляет собой отраслевой стандарт для экспорта пакетов на втором уровне модели взаимодействия открытых систем.

Данная функция применяется для мониторинга коммутируемых сетей посредством случайной выборки пакетов на портах коммутатора и выборочной проверки счетчиков портов в определенное время.

Выбранные пакеты и счетчики (называются образцами потока и образцами счетчиков соответственно) передаются в форме UDP-датаграмм sFlow на центральный сервер, контролирующий сетевой трафик.

Упомянутый центральный сервер называется sFlow-получателем или sFlow-коллектором.

Сегмент полезных данных UDP-пакета содержит sFlow датаграмму.

В каждой датаграмме представлена информация о версии sFlow, IP-адресе инициирующего устройства, порядковом номере, числе образцов, которые она содержит, а также один или несколько образцов потоков и/или счетчиков.

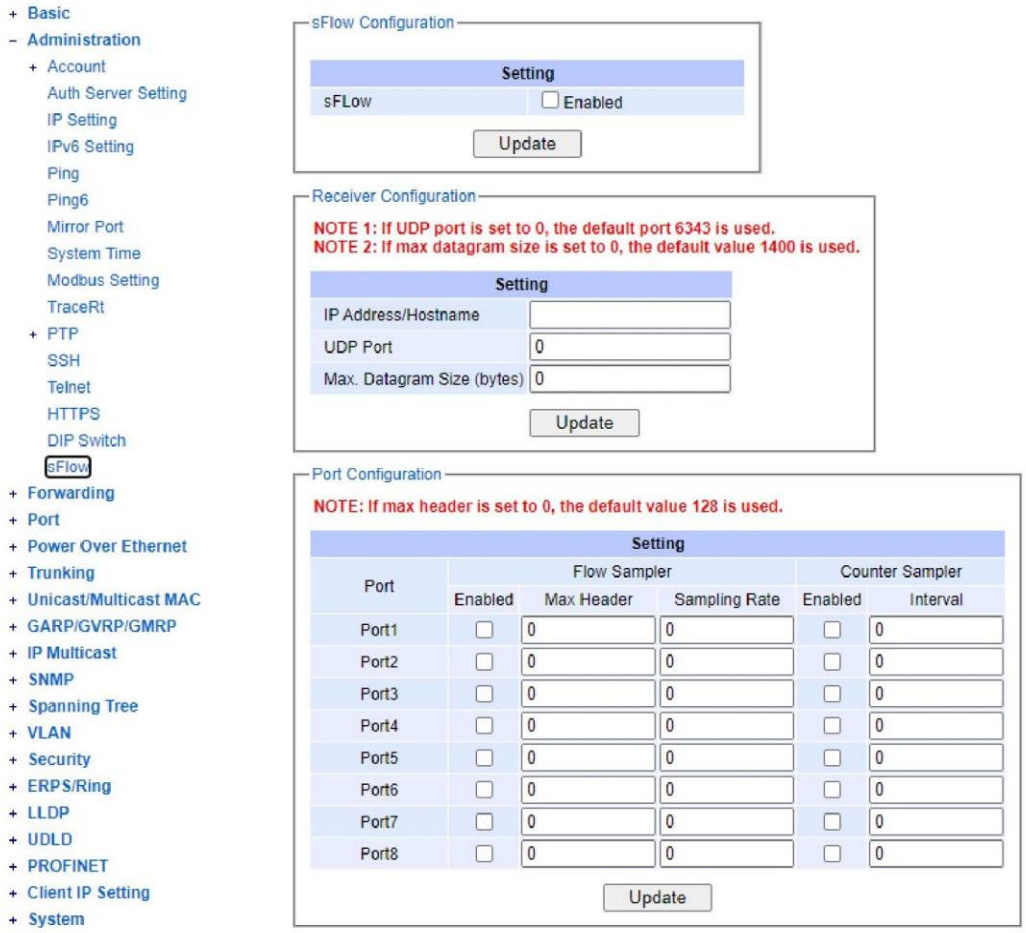


Рисунок 5.42. Сетевая страница настройки параметров функции sFlow.

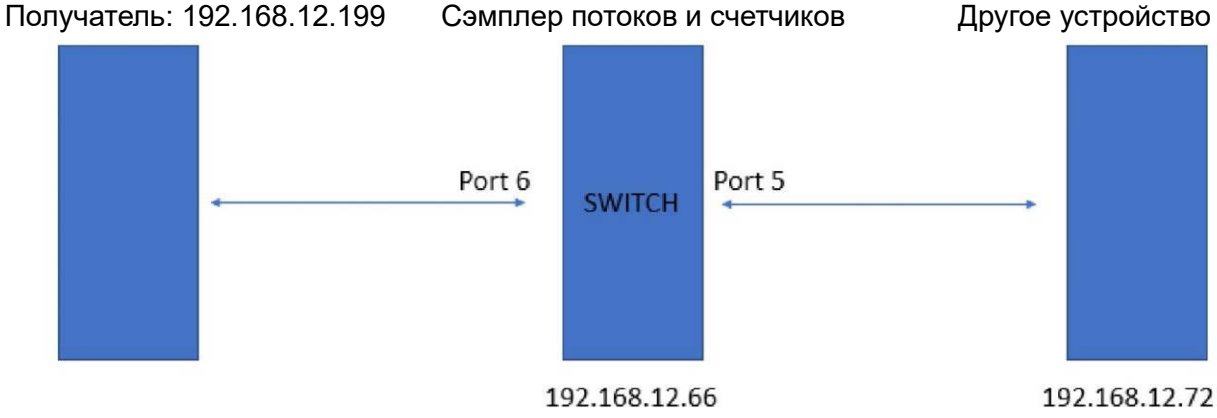


Рисунок 5.43. Представительная схема работы функции sFlow.

Таблица 5.11. Описание настраиваемых параметров функции sFlow.

Имя параметра	**Описание**	**Заводская настройка по умолчанию**
Настройка параметров функции sFlow:		
Enabled	Установите или снимите флажок для активации или отключения функции sFlow соответственно.	Флажок не установлен
Настройка параметров получателя:		
IP Address/Hostname	IP-адрес получателя для функции sFlow.	Не заполняется

Имя параметра		Описание	Заводская настройка по умолчанию
UDP Port		Номер UDP-порта получателя функции sFlow.	0
Maximum Datagram Size (bytes)		Максимальное число байтов данных, которые могут быть переданы в одной датаграмме сэмплирования.	0
Настройка параметров портов:			
Flow Sampler	**Enabled**	Установите или снимите флажок, чтобы активировать / отключить выборку из потока на определенном порте (портах).	Флажок не установлен
	Max Header	Максимальное число байтов, которые могут быть скопированы из выбранного пакета в датаграмму функции sFlow.	0
	Sampling Rate	Укажите значение N, определяющее частоту выборки - выбирается в среднем 1/N пакетов переданных или принятых через порт.	0
Counter Sampler	**Enabled**	Установите или снимите флажок, чтобы активировать / отключить опрос счетчиков на определенном порте (портах).	Флажок не установлен
	Interval	Если опрос счетчиков активирован, в данном поле указывается продолжительность интервала опроса в секундах.	0

6 РАЗДЕЛ FORWARDING

Для переадресации пакетов в сети разработано множество различных технологий.

В данном промышленном управляемом коммутаторе реализованы следующие три основные технологии: управление качеством сервисов (QoS), управление скоростью передачи и контроль шторма.

На рисунке 6.1 показаны подразделы меню в разделе Forwarding.

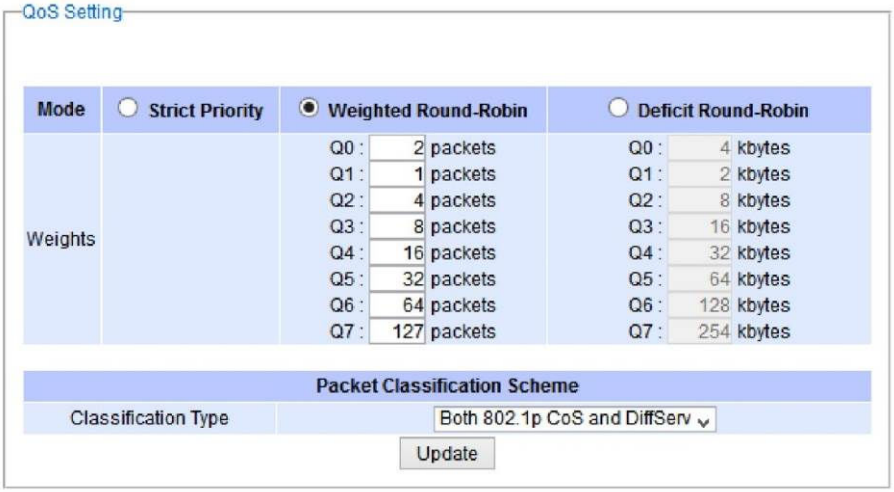


Рисунок 6.1. Раскрывающееся меню Forwarding.

6.1 Подраздел QoS

Функция управления качеством сервисов (QoS) может быть использована для назначения различных приоритетов различным приложениям, пользователям или потокам данных. Функция QoS гарантирует определенный уровень производительности при обработке определенных потоков данных по следующим показателям: скорость передачи данных, коэффициент битовых ошибок, задержка, погрешность синхронизации и вероятность отбрасывания пакетов.

Данный управляемый коммутатор способен проверять теги класса сервиса 802.1p CoS и DiffServ (поле кода дифференцирования трафика (DSCP)), чтобы обеспечить непротиворечивую классификацию.

Подраздел QoS включает три механизма реализации функции QoS: методы организации очередей или алгоритмы планирования пакетов в разделе Setting, раздел CoS Queuing Mapping и раздел DSCP Mapping, как показано на рисунке 6.2. Описание настраиваемых параметров функции QoS в сводном виде представлено в таблице 6.1.

Рисунок 6.2. Раскрывающееся меню QoS.

Таблица 6.1. Описание настраиваемых параметров функции QoS.

Имя параметра	Описание	Заводская настройка по умолчанию
Setting	Методы организации очередей (алгоритмы планирования пакетов) включают Strict Priority (строгий приоритет), Weighted Round Robin (циклический взвешенный алгоритм) и Deficit Round Robin (циклический дефицитный алгоритм) Смотрите примечания в следующем подразделе для подробного описания и сравнения.	Strict Priority
Header Mapping	CoS Queuing Mapping и DSCP Mapping. Если установлено значение 802.1p CoS, коммутатор проверяет только приоритетные биты класса сервиса (CoS) на втором уровне. Если установлено значение DiffServ, коммутатор проверяет поле кода дифференцирования трафика DiffServ (DSCP). Более подробное описание приведено в примечаниях ниже.	Both 802.1p CoS and DiffServ

6.1.1 Подраздел QoS Setting

Пользователь может выбрать один из трех методов организации очередей, поддерживаемых данным управляемым коммутатором: Strict Priority, Weighted Round Robin и Deficit Round Robin.

Если выбран метод Strict Priority, планировщик функции QoS назначает приоритеты очередям, и если в очереди с наивысшим приоритетом появляются пакеты, ожидающие переадресации, они передаются в обход пакетов, ожидающих в других очередях.

Этот режим первоочередную передачу трафика в очереди с наивысшим приоритетом во всех случаях.

Пакеты, ожидающие в очередях с более низкими приоритетами, передаются только при условии, что все очереди с более высокими приоритетами пусты.

Приоритеты очередей назначаются в диапазоне от 0 (Q0) до 7 (Q7). Значение 0 соответствует наинизшему, а 7 - наивысшему приоритету.

Таким образом, пакеты в очереди Q7 всегда будут передаваться в обход пакетов в очереди Q6, пакеты в очереди Q6 – в обход пакетов в очереди Q5 и так далее в порядке убывания номеров приоритетов.

Алгоритм Weighted Round Robin (WRR) представляет собой простейшую аппроксимацию алгоритма обобщенного разделения процессорного времени.

При использовании алгоритма WRR для каждого потока пакетов или для каждого соединения создается собственная очередь пакетов в контроллере сетевого интерфейса.

Тем самым для всех классов обслуживания гарантируется доступ к, по крайней мере, некоторой (настраиваемой) части пропускной способности сети, что позволяет избежать исчерпания ресурсов пропускной способности.

Но у этого алгоритма есть определенное ограничение, которое заключается в том, что его неудобно использовать для обработки пакетов переменной длины.

Алгоритм WRR может выделить адекватную долю пропускной способности, соответствующую классу обслуживания, только при условии, что все пакеты во всех очередях имеют одинаковый размер, либо если средний размер пакета известен заранее.

Как правило, вес каждой очереди устанавливается в зависимости от требуемой скорости передачи данных.

Каждая очередь обслуживается в зависимости от ее веса в сервисном цикле.

Циклический дефицитный алгоритм (DWRR) позволяет решить проблему ограничений алгоритма WRR для пакетов с переменным размером.

Каждой очереди назначается вес, счетчик дефицита (общее количество байтов, которое разрешено передать очереди при каждом обращении к ней планировщика) и квант сервиса (в байтах).

Алгоритм DWRR поочередно сканирует все непустые очереди. При выборе непустой очереди счетчик дефицита этой очереди увеличивается на значение ее кванта.

Новое значение счетчика дефицита соответствует максимальному числу байтов, которые могут быть переданы при данном обращении.

Если значение счетчика дефицита больше размера пакета, ожидающего в начале очереди, этот пакет передается, а значение счетчика уменьшается на значение размера пакета. Затем размер следующих пакетов сравнивается с полученным значением счетчика.

Если очередь пуста, либо значение счетчика недостаточно для передачи следующего пакета, планировщик переходит к следующей очереди.

При этом, если очередь пуста, значение счетчика дефицита сбрасывается на 0. Чем меньше размеры пакетов, тем больше циклов придется выполнить планировщику прежде, чем он обслужит каждую очередь до конца.

Но если размер пакета слишком большой, может возникнуть некоторая краткосрочная неравнодоступность.

Более или менее равный доступ возможен только при условии масштаба времени дольше продолжительности цикла приема-передачи. При более коротком масштабе времени возможно неравномерное распределение сервиса по потокам.

Продолжительность цикла приема-передачи зависит от размера пакета и скорости передачи.

На рисунке 6.3 показана сетевая страница подраздела QoS Setting.

По умолчанию функция QoS в управляемом коммутаторе запускается в режиме Strict Priority. Для циклического взвешенного алгоритма веса очередей с Q0 по Q7, выраженные в числе пакетов, распределяются следующим образом:

- очередь Q0 CoS = 2 пакета,
- очередь Q1 CoS = 1 пакет,
- очередь Q2 CoS = 4 пакета,
- очередь Q3 CoS = 8 пакетов,
- очередь Q4 CoS = 16 пакетов,
- очередь Q5 CoS = 32 пакета,
- очередь Q6 CoS = 64 пакетов,
- очередь Q7 CoS = 127 пакетов.

Значения весов при использовании циклического дефицитного алгоритма вдвое превышают соответствующие значения для алгоритма WRR, но для алгоритма WDRR эти значения выражены в килобайтах, а не в числе пакетов, как можно видеть в последнем столбце таблицы на рисунке 6.3.

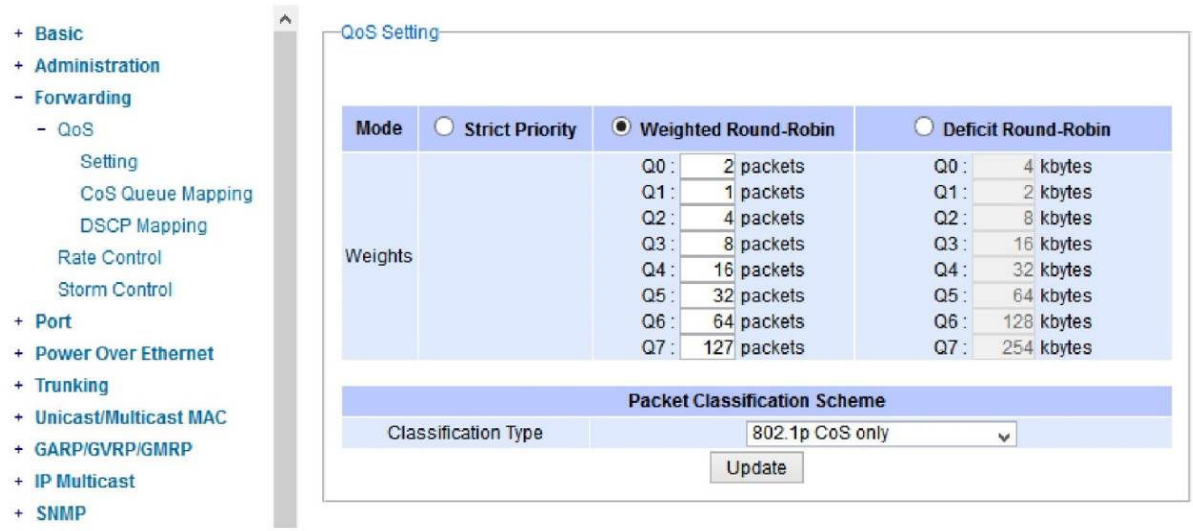


Рисунок 6.3. Сетевая страница настройки параметров функции QoS.

В нижней части сетевой страницы настройки параметров функции QoS, показанной на рисунке 6.3, пользователь может выбрать систему классификации пакетов, которая будет использоваться управляемым коммутатором.

Из раскрывающегося списка можно выбрать один из следующих двух типов классификации: 802.1 p CoS only или Both 802.1 p CoS and DiffServ.

По умолчанию принимается система классификации 802.1 p CoS only.

После изменения алгоритма планировщика, ввода значений веса (если требуются) для алгоритма WRR или DWRR, а также после выбора типа классификации пользователь должен щелкнуть с указателем на кнопке Update, чтобы изменения вступили в силу на коммутаторе.

6.1.2 Подраздел CoS Queue Mapping

Технология 802.1p CoS, разработанная для функции QoS рабочей группой IEEE P802.1p, представляет собой механизм, использующий классы сервиса для управления доступом на уровне среды передачи данных.

Для этого в составе заголовка кадра Ethernet (второй уровень) предусмотрено 3-разрядное поле, которое называется "поле кода приоритета".

Используются тегированные кадры VLAN согласно описанию в спецификации IEEE 802.1Q. В упомянутом поле указывается значение приоритета в диапазоне от 0 до 7 включительно. Это значение использует функция QoS для дифференциации трафика.

Если эта опция активирована, коммутатор проверяет тег класса сервиса (802.1p CoS) в MAC-кадре, и по нему определяет приоритет каждого кадра.

Коммутатор способен классифицировать трафик на основе тегов приоритета 802.1p (тегов класса сервиса (CoS)) при условии, что тег имеет действительное значение.

Эта опция позволяет пользователю связывать поле кода приоритета в заголовке кадра Ethernet с очередями, имеющими различные значения приоритета CoS, как показано на рисунке 6.4. Пользователь может выбрать требуемую очередь (от Q1 до Q7) в столбце CoS Priority Queue из раскрывающегося списка для каждого значения поля кода приоритета в столбце PCP value. Описание приоритетных очередей на странице CoS Queue Mapping в сводном виде представлено в таблице 6.2.

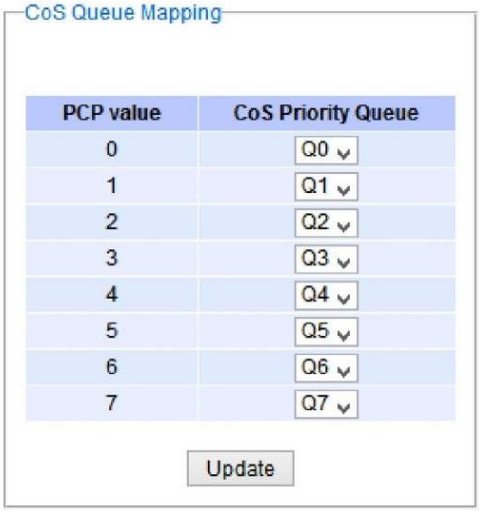


Рисунок 6.4. Таблица связывания на сетевой странице класса сервиса.

Таблица 6.2. Описание приоритетных очередей.

Имя параметра	Описание	Заводская настройка по умолчанию
PCP	Поле кода приоритета в заголовке кадра Ethernet. Значение 0 соответствует наинизшему, а значение 7 - наивысшему приоритету.	PCP 0 -> Q 0 PCP 1 -> Q 0 PCP 2 -> Q 1 PCP 3 -> Q 1

Имя параметра	Описание	Заводская настройка по умолчанию
CoS Priority Queue	Приоритетная очередь, в которую должен быть поставлен определенный кадр Ethernet.	PCP 4 -> Q 2 PCP 5 -> Q 2 PCP 6 -> Q 3 PCP 7 -> Q 3

6.1.3 Подраздел DSCP Mapping

Сокращение DiffServ/ToS обозначает "дифференцированные службы / тип служб".

Это – сетевая архитектура, которая описывает простой, но масштабируемый механизм классификации сетевого трафика и обеспечения гарантированного выделения пропускной способности функцией QoS в сети.

Технология DiffServ использует для классификации пакетов 6-разрядное поле кода дифференцирования трафика в 8-разрядном поле дифференцированных сервисов в IP-заголовке.

Поле дифференцированных сервисов и поле явного объявления о перегруженности (ECN) заменяют устаревшее поле типа сервиса (TOS), которое используется в версии IPv4 для принятия решений о режиме классификации пакетов на каждом транзитном участке и использовании функций регулирования трафика, таких как измерение, разметка, формирование и управление на основе политик.

Для типов сервиса коммутатора можно назначить значения веса очереди по умолчанию, как показано на рисунке 6.5.

Следует учитывать, что поле типа сервиса состоит из поля кода дифференцирования трафика (DSCP) длиной 6 битов и явного объявления о перегруженности (ECN) длиной 2 бита.

Пользователь может назначать значения типа сервиса (DSCP) предопределенным типам очередей (Priority) вручную на сетевой странице DSCP Mapping, которая показана на рисунке 6.5.

Значение приоритета может быть назначено в диапазоне от 0 до 7 включительно, где число 7 соответствует наивысшему, а число 0 - наинизшему приоритету.

После ввода нового значения приоритета для поля DSCP щелкните с указателем на кнопке Update внизу страницы, чтобы измененные связи вступили в силу.

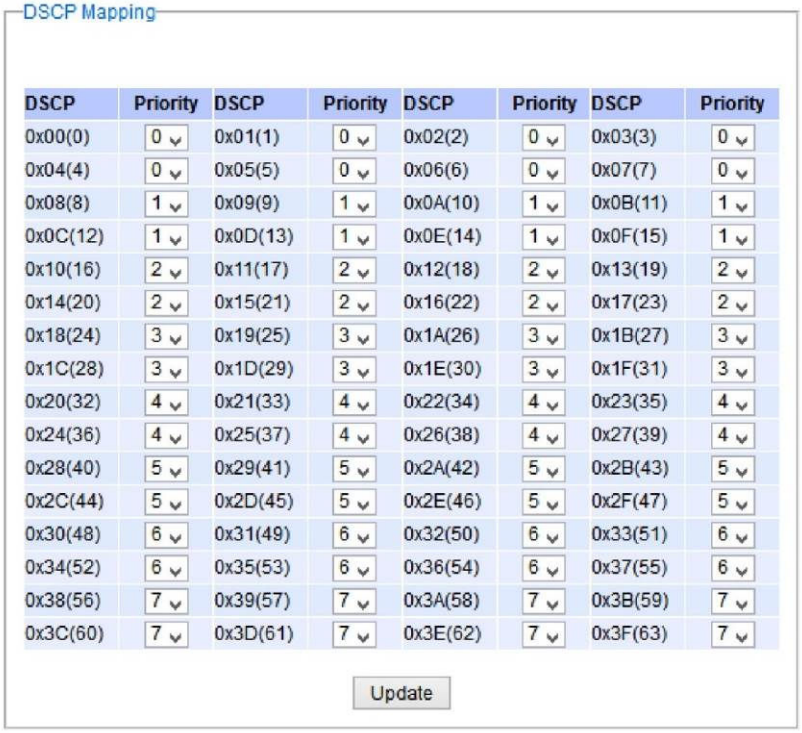


Рисунок 6.5. Сетевая страница с таблицей связывания DSCP and ECN.

6.2 Подраздел Rate Control

В этом подразделе пользователь может настроить параметры режима управления скоростью передачи для каждого порта управляемого коммутатора, как показано на рисунке 6.6. Механизм управления скоростью передачи устанавливает предельную или максимальную скорость передачи данных, которую может поддерживать порт.

Следует отметить, что управление скоростью передачи может быть реализовано в обоих направлениях: для входящего трафика (Ingress) и для исходящего трафика (Egress).

Однако следует учитывать определенные ограничения, которые применяются для значений этих двух параметров управления скоростью передачи.

Далее в сводном виде представлены правила настройки параметров в подразделе Rate Control:

- Значения для исходящего (Egress) и входящего (Ingress) трафика можно устанавливать в диапазоне от 0 до 102 400 (для порта с пропускной способностью 100 Мбит в сек.) или до 1 024 000 (для порта с пропускной способностью 1000 Мбит в сек).
- Значение 0 указывается для отключения механизма управления скоростью передачи.
- Значения должны быть целыми числами, кратными 64, если скорость передачи составляет меньше 1 792 кБ/сек. Например: 64 кБ/сек, 128 кБ/сек, 512 кБ/сек, 1 792 кБ/сек.
- Значения должны быть целыми числами, кратными 1 024, если скорость передачи составляет от 1 792 кБ/сек до 102 400 кБ/сек (для порта с пропускной способностью 100 Мбит/сек.) или 106 496 кБ/сек (для порта с пропускной способностью 1000 Мбит/сек.). Пример: 2 048 кБ/сек, 3 072 кБ/сек, 102 400 кБ/сек.

- Значения должны быть целыми числами, кратными 8 192, если скорость передачи составляет больше 106 496 кБ/сек.

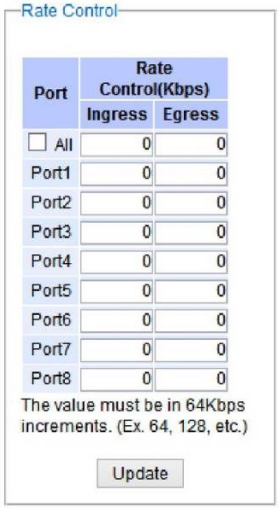


Рисунок 6.6. Сетевая страница подраздела Rate Control.

Описание настраиваемых параметров подраздела Rate Control в сводном виде представлено в таблице 6.3.

После завершения настройки параметров управления скоростью передачи для каждого порта щелкните с указателем на кнопке Update, чтобы изменения вступили в силу на коммутаторе.

Таблица 6.3. Описание настраиваемых параметров подраздела Rate Control.

Имя параметра		Описание	Заводская настройка по умолчанию
Port		Номер порта управляемого коммутатора.	-
Rate Control (Kbps)	**Ingress**	Данная опция устанавливает предельную скорость передачи для входящего трафика. Следует помнить, что значение должно быть указано в килобитах в секунду (кБ/сек).	0 (отключено)
	Egress	Данная опция устанавливает предельную скорость передачи для исходящего трафика. Следует помнить, что значение должно быть указано в килобитах в секунду (кБ/сек).	0 (отключено)

6.3 Подраздел Storm Control

Данный подраздел меню предназначен для настройки параметров функций контроля шторма или шторм-фильтра для управляемого коммутатора.

Функция контроля шторма предназначена для предотвращения нарушения трафика в локальной сети под воздействием принимаемого через порт входящего трафика широковещательной или многоадресной передачи, либо сообщений о невозможности определения порта назначения (DLF).

На рисунке 6.7 показана сетевая страница подраздела Storm Control.

Пользователь может применить одни и те же ограничивающие параметры одновременно на всех портах.

Для этого нужно установить флажок в поле выбора перед строкой All и ввести значения скорости передачи в кБ/сек для контроля различных видов трафика в каждом столбце таблицы Storm Control (Kbps) (DLF limiting, Multicast limiting, Broadcast limiting).

В другом варианте можно установить ограничения для контроля шторма отдельно для каждого порта.

Следует отметить, что если установлено предельное значение 0, функция контроля шторма отключена.

Также следует помнить, что введенное значение должно быть кратно 64 кбит в сек.

После достижения установленной предельной скорости избыточный входящий трафик будет отбрасываться.

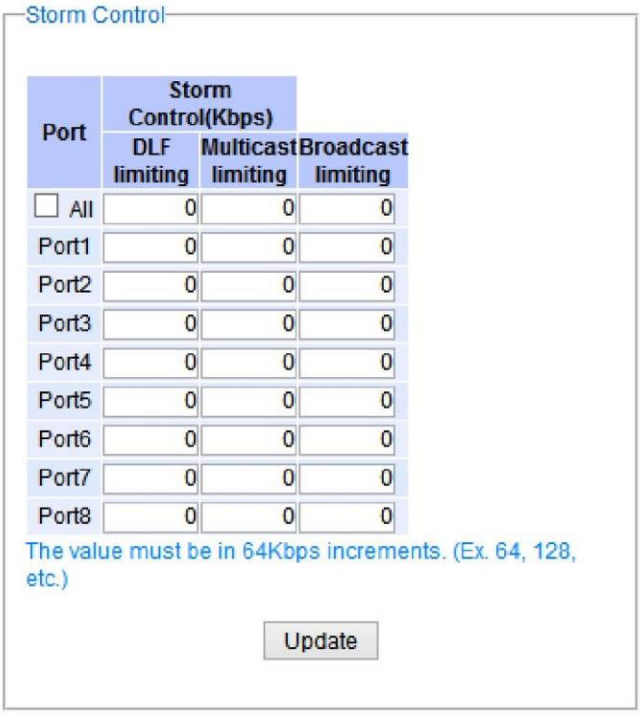


Рисунок 6.7. Сетевая страница подраздела Storm Control.

Описание настраиваемых параметров функции контроля шторма в сводном виде представлено в таблице 6.4.

Описание ограничиваемых режимов для контроля шторма в сводном виде представлено в таблице 6.5.

Таблица 6.4. Описание настраиваемых параметров функции контроля шторма.

Имя параметра	**Описание**	**Заводская настройка по умолчанию**
All	В данной строке можно активировать или отключить режим контроля шторма или фильтр на всех портах одновременно. В каждом столбце данной строки можно ввести значение предельной скорости передачи данных для каждого типа штормовых пакетов (DLF, Multicast и Broadcast). Следует помнить, что введенное значение должно быть кратно 64 кбит в сек.	Флажок не проставлен, функция отключена

Имя параметра	Описание	Заводская настройка по умолчанию
Port 1 – Port 8	В этих строках в соответствующих столбцах можно ввести значения, ограничивающие скорость передачи штормовых пакетов различных типов (DLF, Multicast и Broadcast) для каждого порта отдельно. Следует помнить, что введенное значение должно быть кратно 64 кбит в сек. В примечаниях ниже можно найти более подробное описание и информацию для сравнения.	Disable

Таблица 6.5. Описание ограничиваемых режимов.

Имя параметра	Описание	Заводская настройка по умолчанию
DLF limiting (Destination Lookup Failure)	Ограничение для трафика пакетов невозможности определения порта назначения (0 ~ 9876480) кбит.	0 (отключено)
Multicast limiting	Ограничение для многоадресного трафика (0 ~ 9876480) кбит.	0 (отключено)
Broadcast limiting	Ограничение для широковещательного трафика (0 ~ 9876480) кбит.	0 (отключено)

Типы пакетов, формирующих штормовой трафик:

- DLF: невозможность определения порта назначения. Коммутатор во всех случаях сначала ищет MAC-адрес назначения в своей таблице MAC-адресов. В случае если соответствующий MAC-адрес не найден в таблице MAC-адресов (что означает невозможность определения порта назначения), коммутатор передает пакеты на все порты, которые находятся в той же сети LAN.

- Multicast: Режим передачи, в котором сообщения от одного хост-устройства одновременно передаются нескольким хост-устройствам. При этом принимать многоадресную передачу могут только те хост-устройства, которые принадлежат к определенной группе многоадресной передачи. Кроме того, сетевые устройства, поддерживающие режим многоадресной передачи, передают только один экземпляр информации до точки, в которой путь до членов группы начинает разветвляться. В точках ветвления создаются копии многоадресных пакетов, которые затем соответственно переадресовываются. Такая схема позволяет ограничить объем передаваемого трафика, сократив количество адресов назначения, и более эффективно использовать пропускную способность сети.

- Broadcast: Сообщения передаются одновременно на все устройства в сети.

7 РАЗДЕЛ PORT

Промышленный управляемый коммутатор Yarus Networks обеспечивает возможность полного контроля всех его сетевых интерфейсов.

В этом разделе меню пользователь может включать или отключать отдельные порты и устанавливать предпочтительный режим физического уровня (Copper – подключение по медному проводу, либо Fiber – подключение по оптоволоконной линии).

Помимо того, пользователь может настраивать параметры механизма согласования, скорость передачи данных, выбирать тип дуплексного режима и управлять потоками данных отдельно для каждого порта.

В этом разделе можно просматривать состояние всех портов и статистику по всем портам.

На рисунке 7.1 показана сетевая страница раздела Port. Раздел меню Port включает следующие четыре подраздела:

- Port Setting
- Port Status
- Mini-GBIC Port Status
- Port Statistics

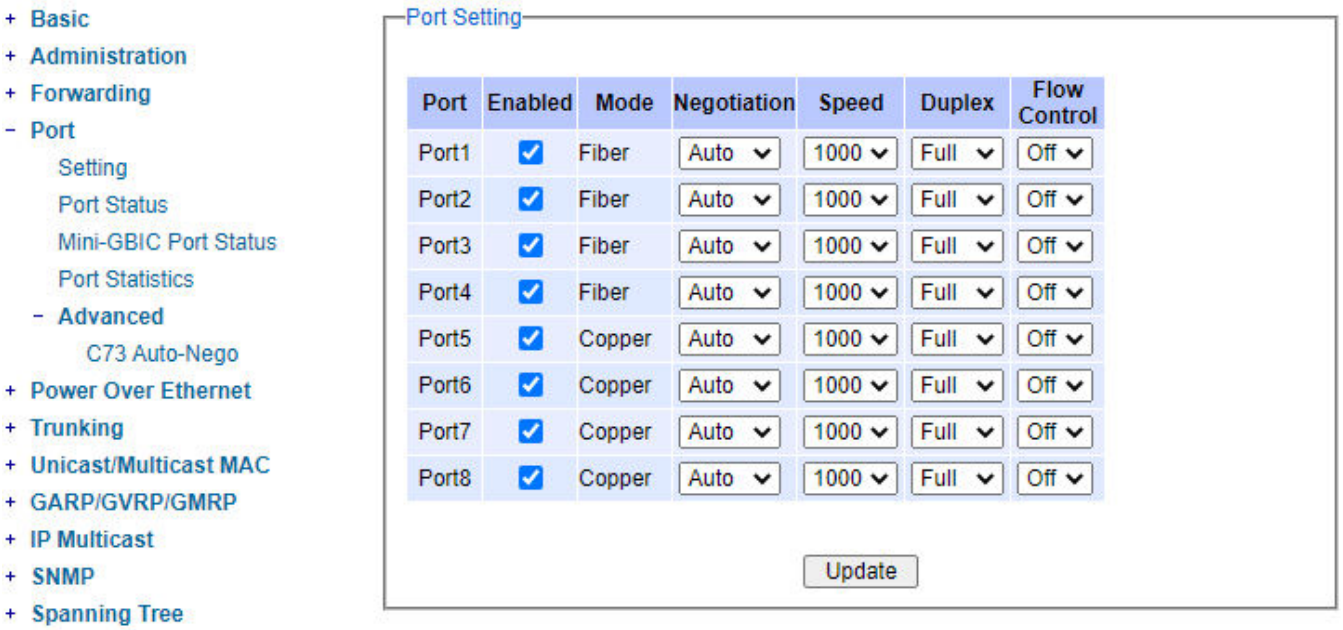


Рисунок 7.1. Раскрывающееся меню раздела Port.

7.1 Подраздел Port Setting

Сетевая страница Port Setting показана на рисунке 7.2.

Пользователь может управлять состоянием каждого порта, устанавливая или снимая флажок в поле Enabled в соответствующей строке.

Соединения физического уровня для каждого порта указаны в столбце Mode. На некоторых управляемых коммутаторах Yarus Networks (YN-SI2510A) пользователь может выбрать из

перечисленных вариантов предпочтительную физическую среду.

Например, гигабитный порт Ethernet (PortG1) на физическом уровне может поддерживать подключение как по медному проводу, так и по волоконно-оптической линии.

Пользователь может щелкнуть с указателем на селективной кнопке у опции Fiber, чтобы установить подключение с выбором волоконно-оптической линии в качестве предпочтительного варианта физической среды.

Следует отметить, что если оба режима выбраны одновременно, порт функционирует в комбинированном режиме (получает статус комбинированного порта).

Пример, показанный на рисунке 7.2, приведен для устройства YN-SI2510A-4GX-4GP, которое не имеет комбинированных портов и не поддерживает выбор предпочтительного режима.

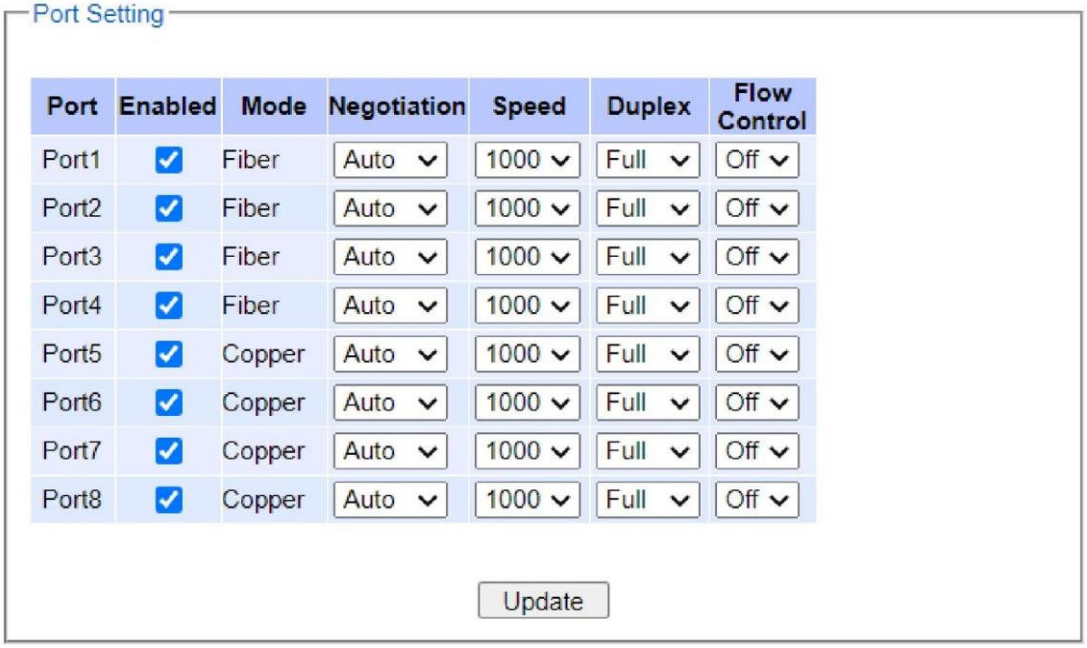


Рисунок 7.2. Сетевая страница настройки параметров портов.

В четвертом столбце (Negotiation) таблицы, показанной на рисунке, пользователь может выбрать из выпадающего списка механизм согласования для порта, который может быть автоматическим (Auto) или принудительным (Force).

Если выбран режим принудительного согласования, значения скорости передачи данных через порт и типа дуплексного режима фиксируются строго в соответствии с уставками, заданными пользователем.

В режиме автоматического согласования коммутатор может самостоятельно определять фактическую скорость передачи данных и тип дуплексного режима для порта.

Следует отметить, что гигабитный порт компактного форм-фактора (SFP-порт) коммутатора YN-SI2510A обратно совместим с приемопередающими устройствами 125/155 Мбит/сек, однако скорость передачи должна быть установлена вручную на 100.

ПРИМЕЧАНИЕ: Гигабитный SFP-порт коммутатора YN-SI3400AT не поддерживает обратную совместимость.

В пятом столбце можно установить скорость передачи для каждого порта, выбрав нужное значение из выпадающего списка (10, 100 или 1000 Мбит в сек). Значение скорости, устанавливаемое по умолчанию, зависит от максимальной скорости передачи данных, которая поддерживается портом. Далее выбирается тип дуплексного режима (Duplex) для порта – Full (полнодуплексный) или Half (полудуплексный).

В полудуплексном режиме поддерживается только односторонняя передача, в то время как в полнодуплексном режиме передача данных может осуществляться в обоих направлениях одновременно.

В восьмом столбце (Flow Control) можно активировать (On) или отключить (Off) механизм управления потоками данных для каждого порта.

Режим управления потоками данных рекомендуется использовать для предотвращения потери пакетов в условиях перегрузки сети.

При этом по умолчанию для параметра Flow Control устанавливается значение Off, т.е. режим отключен.

После завершения настройки параметров портов щелкните с указателем на кнопке Update, чтобы все новые значения параметров конфигурации коммутатора вступили в силу.

Описание настраиваемых параметров портов в сводном виде представлено в таблице 7.1.

Таблица 7.1. Описание настраиваемых параметров портов.

Имя параметра	**Описание**	**Заводская настройка по умолчанию**
Port	Номер порта управляемого коммутатора.	-
Enable	Установите флажок в данном поле для разрешения передачи и приема данных через этот порт.	Все порты включены
Mode	Режим с подключением по медному проводу или и/или оптоволоконной линии. Если оба варианта (Copper и Fiber) выбраны одновременно, порт работает в режиме комбинированного порта.	В зависимости от конфигурации
Negotiation	Можно выбрать один из двух вариантов – принудительное (Force) или автоматическое (Auto). См. описание в тексте выше.	Для всех портов устанавливается режим автоматического согласования.
Speed	Можно выбрать одно из значений - 10, 100 или 1000 Мбит в сек.	Максимальная поддерживаемая скорость
Duplex	Можно выбрать полудуплексный (Half) или полнодуплексный (Full) режим. См. описание в тексте выше.	Полнодуплексный режим
Flow Control	Эту функцию можно включить (On) или отключить (Off). Механизм управления потоками используется во избежание потерь пакетов в условиях перегрузки сети.	Выключено

7.2 Подраздел Port Status

На этой сетевой странице пользователь может просматривать информацию о состоянии портов управляемого коммутатора.

Для каждого порта можно сравнить данные о его фактическом состоянии со значениями параметров, настроенных в предыдущем подразделе.

Режим управления скоростью передачи для входящего и исходящего трафика можно настроить согласно инструкциям.

На рисунке 7.3 показана сетевая страница подраздела Port Status.

Обратите внимание, что в последнем столбце указан статус режима безопасности (On или Off) для каждого порта.

Защиту можно настроить в статическом режиме или в режиме 802.1x.

Чтобы обновить данные о состоянии всех портов, щелкните с указателем на кнопке Refresh в верхней или нижней части сетевой страницы.

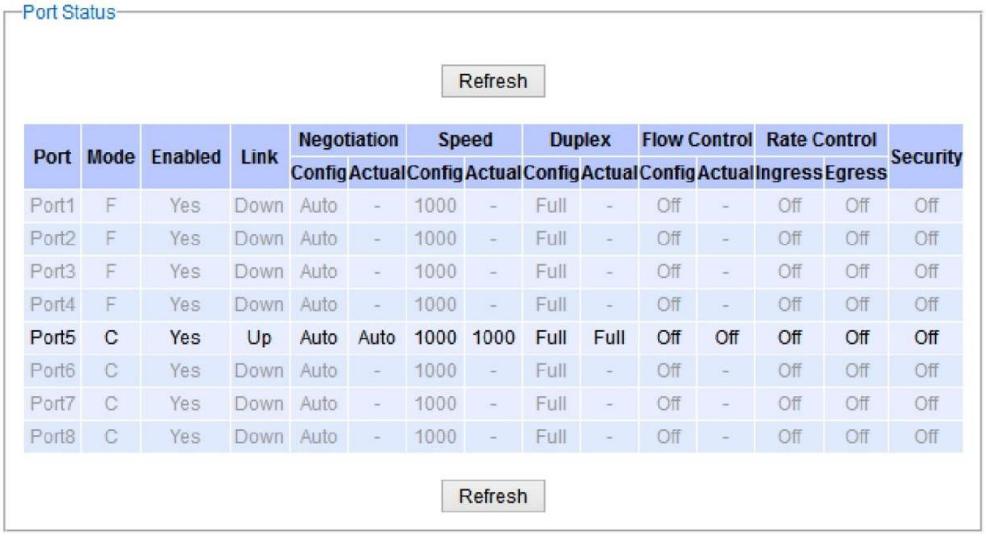


Рисунок 7.3. Сетевая страница Port Status.

Ниже перечислены заголовки столбцов таблицы и допустимые значения состояния портов:

- Mode (по медному проводу (C) или по оптоволоконной линии (F)).
- Enable (Yes (да) или No (нет)).
- Link (Up (активен) или Down (отключен)).
- Negotiation (Auto (автоматический) или Force (принудительный)).
- Speed (единица измерения: Мбит в сек.).
- Duplex (Full (полнодуплексный) или Half (полудуплексный)).
- Flow Control (On (активировано) или Off (отключено)).
- Rate Control (On (активировано) или Off (отключено)).
- Security (On (активировано) или Off (отключено)): Защита порта работает в статическом режиме или в режиме 802.1x.

7.3 Подраздел Mini-GBIC Port Status

Подключаемый порт компактного форм-фактора (SFP-порт) иногда также называют компактным портом с преобразователем гигабитного интерфейса (Mini-GBIC-порт).

В данном подразделе можно проверить состояние всех Mini-GBIC-портов, если такие порты поддерживаются управляемым коммутатором.

На рисунке 7.4 показана сетевая страница под названием Module Status, отображающая статус Mini-GBIC-портов.

Следует отметить, что в данной таблице отображаются только коды соответствия Ethernet и данные вендора.

Фактическое состояние канала (активен или отключен) можно проверить в предыдущем подразделе.

Module Status

SFP Port	Com. Codes	Vendor Name	Vendor PN	L.W.	Vendor SN	Con. Type
Port 1	-	-	-	-	-	-
Port 2	-	-	-	-	-	-
Port 3	-	-	-	-	-	-
Port 4	-	-	-	-	-	-

ПРИМЕЧАНИЕ:

Com. Codes: коды соответствия гигабитному Ethernet.

Vendor PN: номер части, присвоенный вендором.

L.W.: длина лазерной волны.

Vendor SN: серийный номер, присвоенный вендором.

Con. Type: тип разъемного соединителя.

Рисунок 7.4. Сетевая страница состояния Mini-GBIC-портов.

7.4 Подраздел Port Statistics

На данной сетевой странице в сводном виде представлены статистические данные по портам. Окно подраздела показано на рисунке 7.5.

Пользователь может использовать данный подраздел в целях диагностирования некоторых проблем, например, для определения качества канала каждого порта.

Ключевые статистические данные включают суммарное количество нормальных кадров (OK frames), количество отброшенных кадров (Error frames) и скорость передачи данных в байтах в сек. (Rate in Bps).

Эти данные указываются для трафика, переданного (Tx) и принятого (Rx) каждым портом. Чтобы очистить или обнулить все статистические данные на этой странице, щелкните с указателем на кнопке Clear.

Чтобы получить обновленные данные на этой странице, щелкните с указателем на кнопке Refresh.

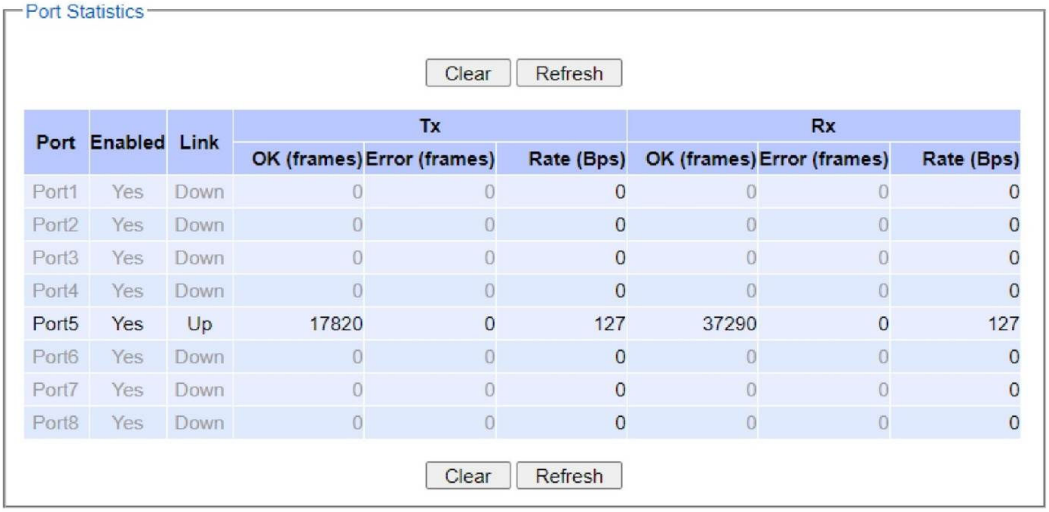


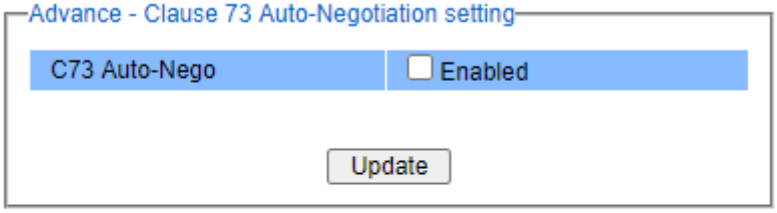
Рисунок 7.5. Сетевая страница Port Statistics.

Ниже перечислены заголовки столбцов таблицы и допустимые значения статистики по портам:

- Enable (Yes или No): данный порт включен (Yes) или отключен (No).
- Link (Up или Down): фактическое состояние канала порта (активен или отключен).
- Tx OK (frames): общее количество переданных пакетов.
- Tx Error (frames): Общее количество исходящих пакетов, которые были отброшены, то есть, были исключены из передачи (включая пакеты, в которых не были обнаружены никакие ошибки).
- Tx Rate (Bps): скорость передачи в байтах в секунду.
- Rx OK (frames): суммарное количество принятых пакетов (не включая пакеты с ошибками).
- Rx Error (frames): суммарное количество пакетов с ошибками (включая пакеты с размером больше или меньше допустимого, пакеты с нарушенной последовательностью проверки кадров в заголовке, с ошибками синхронизации, бессмысленными данными и ошибками фрагментации).
- Rx Rate (Bps): скорость приема в байтах в секунду.

7.5 Подраздел Advanced

В меню Advanced пользователи могут включить автоматическое согласование Backplane Ethernet на основе пункта 73 (C 73) стандарта IEEE 802.3-2008. Чтобы включить C73 Auto-Neg, установите флажок Enabled и щелкните с указателем на кнопке Update, как показано на рисунке 7.6.



Note: Only for Port1,Port2,Port3,Port4

New setting will be activated the next time you boot the switch.

Рисунок 7.6. Сетевая страница C73 Auto-Nego.

8 РАЗДЕЛ POWER OVER ETHERNET

Питание по Ethernet (PoE) представляет собой необязательную функцию управляемого коммутатора, которая позволяет коммутатору обеспечивать электропитание на конечные (питаемые) устройства, подключенные к его портам Ethernet.

Это означает, что электроэнергия для питания передается по кабелям Ethernet вместе с данными.

Эта функция может оказаться полезной для обеспечения электропитания конечных устройств, которые расположены в местах, где нет возможности подключиться к источникам питания. Использование этой технологии также позволяет уменьшить количество кабелей, прокладываемых до конечных устройств.

Чтобы узнать, поддерживается эта функция управляемым коммутатором или нет, проверьте, есть ли ключевое слово "PoE" в названии модели устройства Yarus Networks.

Если в названии модели коммутатора есть обозначение "XX-X**P**", это означает, что данный коммутатор относится к категории "питающего оборудования", и может передавать электроэнергию для "питаемых устройств".

На рисунке 8.1 показано раскрывающееся меню управления функцией питания по Ethernet.

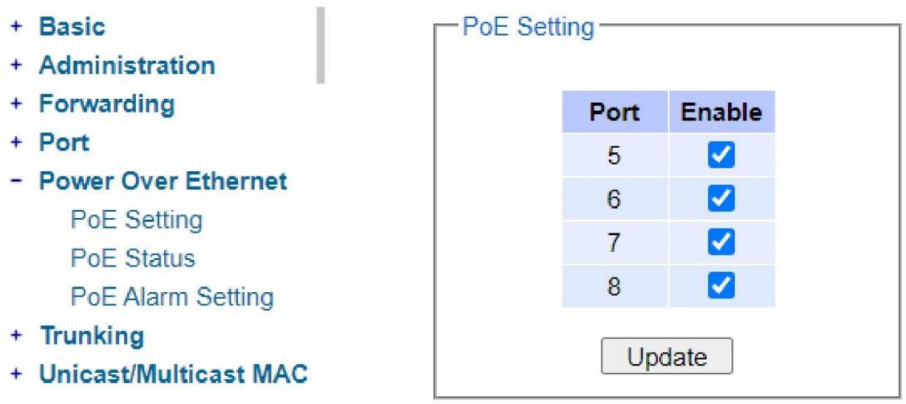


Рисунок 8.1. Раскрывающееся меню управления функцией питания по Ethernet.

8.1 Подраздел PoE Setting

Как показано на рисунке 8.2, на этой сетевой странице можно настроить функцию PoE для каждого порта управляемого коммутатора при условии, что коммутатор данной модели поддерживает эту функцию.

Пользователь может установить флажок в поле Enable для соответствующего порта.

Затем щелкните с указателем на кнопке Update, чтобы измененные параметры функции PoE вступили в силу на коммутаторе.

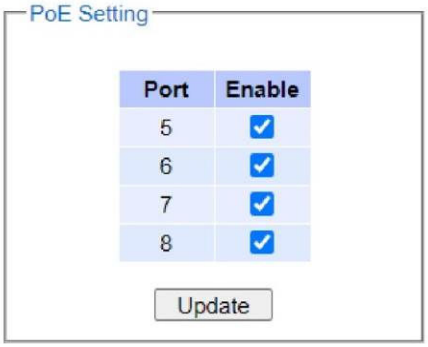


Рисунок 8.2. Сетевая страница настройки функции PoE.

* **ПРИМЕЧАНИЕ:** число портов зависит от модели используемого управляемого коммутатора.

Таблица 8.1. Описание настраиваемых параметров функции PoE (для моделей с 8 портами с поддержкой питания по Ethernet).

Имя параметра	Описание	Заводская настройка по умолчанию
Port 1	Включение или отключение функции PoE для порта 1.	Включено
Port 2	Включение или отключение функции PoE для порта 2.	Включено
Port 3	Включение или отключение функции PoE для порта 3.	Включено
Port 4	Включение или отключение функции PoE для порта 4.	Включено
Port 5	Включение или отключение функции PoE для порта 5.	Включено
Port 6	Включение или отключение функции PoE для порта 6.	Включено
Port 7	Включение или отключение функции PoE для порта 7.	Включено
Port 8	Включение или отключение функции PoE для порта 8.	Включено

8.2 Подраздел PoE Status

На этой сетевой странице в сводном виде представлены данные о статусе функции PoE для каждого порта.

Например, как видно на рисунке 8.3, данная функция активирована для порта 8, через который подается питание на питаемое устройство класса 2 (класс устройства указывается в столбце Classification).

Номинальные характеристики электропитания для питаемого устройства - 49 В и 33 мА. Суммарная электрическая мощность, потребляемая питаемым устройством, составляет 1,617 Вт.

Чтобы проверить текущее состояние портов с поддержкой функции PoE, щелкните с указателем на кнопке Refresh.

В таблице 8.2 приведено описание каждого столбца в таблице PoE Status.

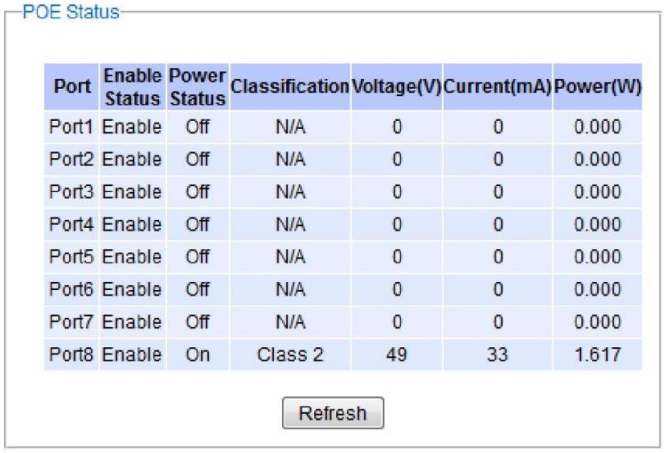


Рисунок 8.3. Сетевая страница состояния функции PoE.

Таблица 8.2. Описание параметров функции PoE.

Имя параметра	Описание	Заводская настройка по умолчанию
Port	Номер порта.	-
Enable Status	Активация или отключение функции PoE.	Включено
Power Status	On, если питаемое устройство на другом конце присутствует, или Off если такое устройство отсутствует на другом конце соединения.	-
Classification	Отображается класс питаемого устройства на другом конце соединения.	-
Voltage (V)	Отображается значение напряжения в вольтах, подаваемого на данный порт.	-
Current (mA)	Отображается значение силы тока в миллиамперах, подаваемой на данный порт.	-
Power (W)	Отображается значение электрической мощности в ваттах, подаваемой на данный порт.	-

8.3 Подраздел PoE Alarm Setting

На этой сетевой странице пользователь может настроить аварийные события, чтобы получать предупреждения о непреднамеренном прерывании питания через Ethernet, а также об изменениях в состоянии питаемого устройства или превышении заданной суммарной потребляемой мощности.

На рисунке 8.4 показана сетевая страница настройки параметров аварийной сигнализации питания по Ethernet.

На этой странице пользователь может установить предельное значение суммарной потребляемой мощности в ваттах.

Управляемый коммутатор, обнаружив превышение этого значения, инициирует аварийный сигнал.

Пользователь также может на собственное усмотрение активировать все или отдельные аварийные события.

На этой странице представлены три категории аварийных событий функции PoE: PoE PD Power On, PoE PD Power Off и Detect Total Power. Пользователь также может на собственный выбор указать способ уведомления о срабатывании аварийной сигнализации: Relay, Email или Alarm LED.

Для этого пользователь должен установить флажки для каждого выбранного способа уведомления.

Описание настраиваемых параметров функции PoE приведено в таблице 8.3.

ПРИМЕЧАНИЕ: Аварийные события могут также быть записаны в журнал регистрации событий (если проставлен флажок в соответствующем поле "Enabled"), либо переданы в уведомлении по электронной почте.

Если установлены флажки в полях "Relay", "Alarm" и "Email", журнал событий будет отображать события предупреждающей и аварийной сигнализации.

Рисунок 8.4. Подраздел PoE Alarm Setting.

Таблица 8.3. Описание настраиваемых параметров аварийной сигнализации функции PoE.

Имя параметра		**Описание**	**Заводская настройка по умолчанию**
Detect Total Power Value		В данном поле указывается значение суммарной потребляемой мощности в ваттах, при достижении которого будет инициировано аварийное событие. Обратите внимание, что значение '0' означает, что аварийное событие не инициируется.	0
Enable		Установите флажок в этом поле, чтобы активировать аварийное событие.	Флажок не установлен
PoE Alarm Event	Select All	Установите флажок перед этой опцией, чтобы активировать все аварийные события.	-
	PoE PD Power On	Установите флажок перед этой опцией, чтобы активировать аварийное событие при включении питания питаемого устройства.	-
	PoE PD Power Off	Установите флажок перед этой опцией, чтобы активировать аварийное событие при отключении питания питаемого устройства.	-
	Detect Total Power	Установите флажок перед этой опцией, чтобы активировать аварийное событие в случае, если	

Имя параметра		Описание	Заводская настройка по умолчанию
		управляемый коммутатор обнаружит превышение суммарной потребляемой мощности, указанное в поле Detect Total Power Value выше.	
Relay		Установите флажок в этом столбце, чтобы аварийный сигнал передавался во внешнюю релейную цепь.	Флажок не установлен
Email		Установите флажок в этом столбце, чтобы уведомление о срабатывании аварийной сигнализации передавалось по электронной почте.	Флажок не установлен
Alarm LED		Установите флажок в этом столбце, чтобы аварийный сигнал передавался во внешнюю цепь светодиодных индикаторов.	Флажок не установлен

9 ПОДРАЗДЕЛ TRUNKING

Данный управляемый коммутатор поддерживает функцию агрегирования (или "транкирования") каналов, которая позволяет объединять несколько каналов в группу, чтобы создать одно логическое соединение с большей пропускной способностью.

Основное преимущество этой функции заключается в том, что она предоставляет пользователям возможность более гибкой настройки сетевых соединений.

Пропускная способность логического соединения может быть удвоена или даже утроена.

В случае если один из физических каналов в группе отключится, передававшийся по нему трафик будет разделен между оставшимися транкированными портами в группе агрегации. Эта функция создает избыточность каналов, что подразумевает более высокую надежность сетевых коммуникаций.

На рисунке 9.1 показано раскрывающееся меню раздела Trunking.

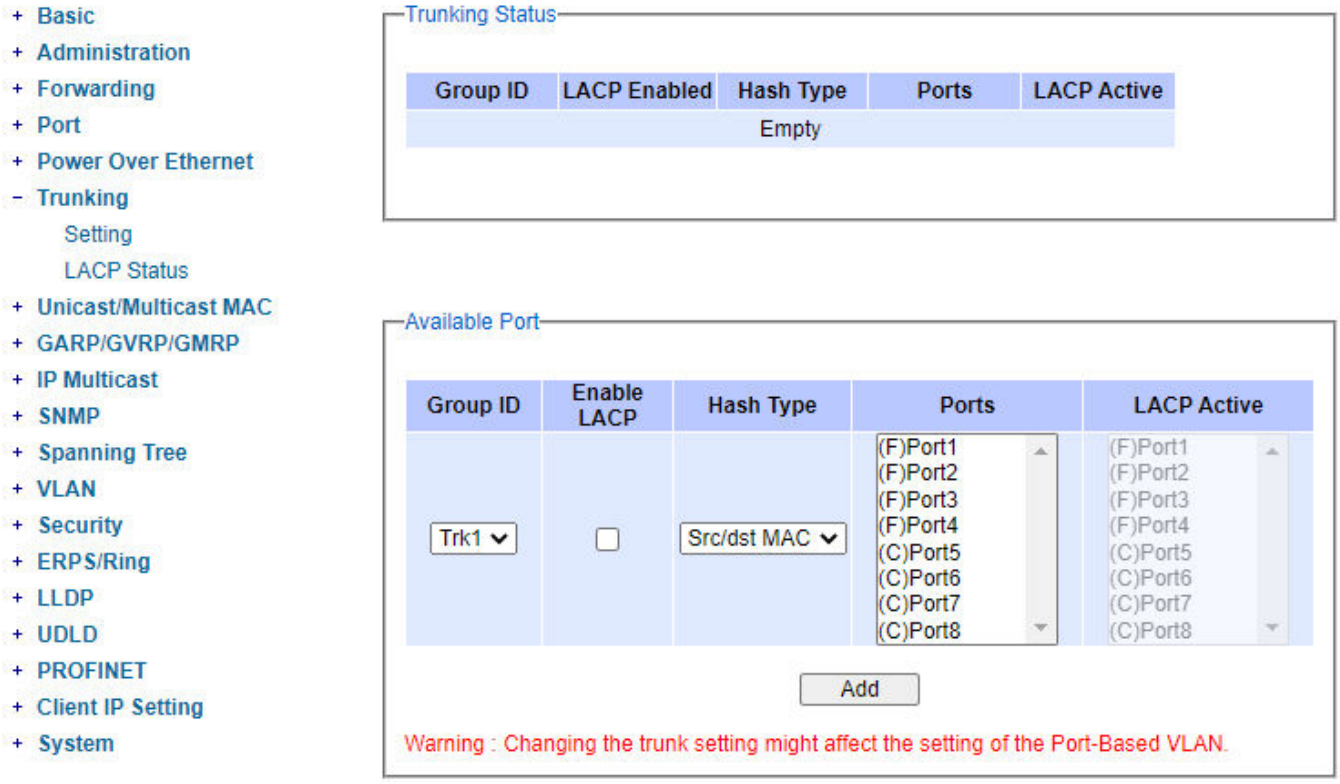


Рисунок 9.1. Раскрывающееся меню раздела Trunking.

9.1 Подраздел Trunking Setting

В этом подразделе пользователь может создавать новые и удалять существующие связи в группе агрегации.

На рисунке 9.2 показана сетевая страница настройки параметров агрегирования.

В верхней части страницы под названием Trunking приведен список существующих групп агрегации, которые можно удалять, щелкая с указателем на кнопке Remove в последнем столбце.

В каждой строке таблицы агрегирования представлена информация о группе (агрегации) каналов с определенным групповым идентификатором, имеющем формат Trkx, где x - целое число в диапазоне от 1 до 8.

ПРИМЕЧАНИЕ: Для различных типов интерфейсов (например, Fast Ethernet, Gigabit Ethernet и Fiber) транкинг портов необходимо комбинировать отдельно.

Обратите внимание, что (F) относится к оптоволоконному порту, в то время как (C) относится к медному порту.

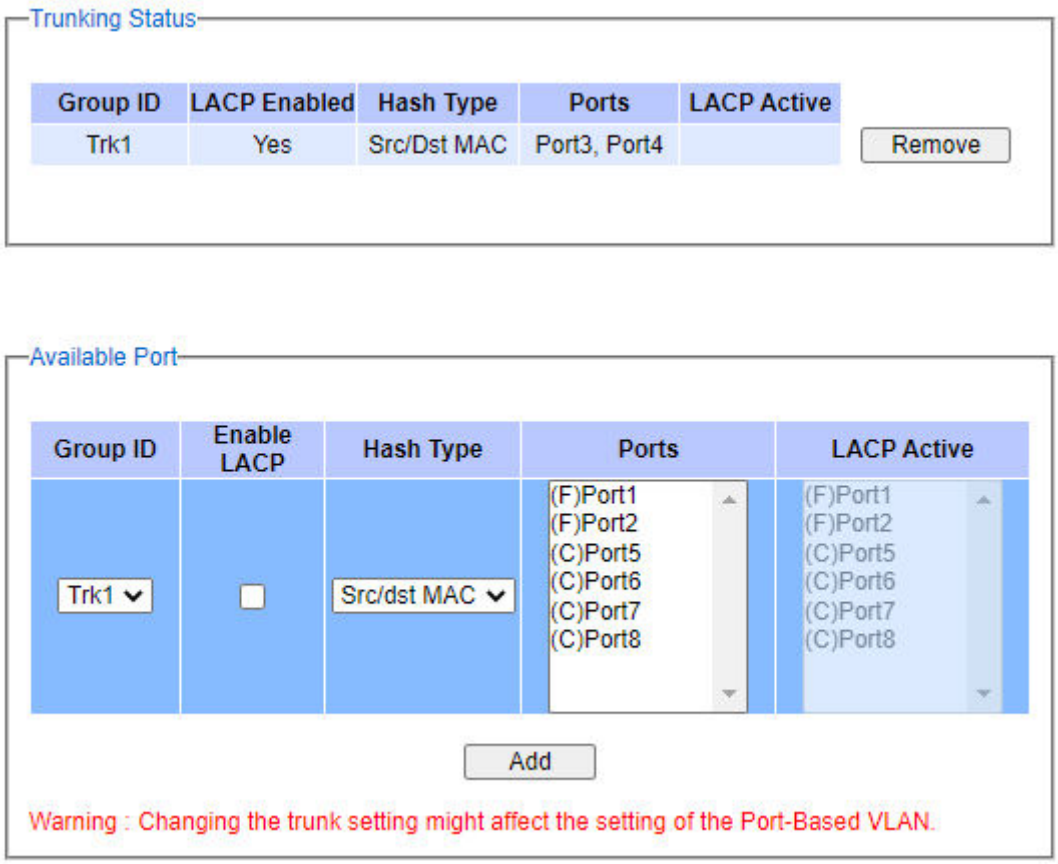


Рисунок 9.2. Сетевая страница настройки параметров агрегирования.

Пользователь может на собственное усмотрение активировать протокол управления агрегацией каналов (LACP), который является стандартным протоколом IEEE (IEEE 802.3ad, IEEE 802.1AX-2008).

Для этого нужно установить флажок в столбце Enable LACP для каждой группы.

Протокол LACP позволяет управляемому коммутатору согласовывать автоматическое связывание каналов посредством передачи LACP-пакетов сетевому партнеру, поддерживающему протокол LACP, или любому другому устройству при условии, что оно подключено непосредственно к управляемому коммутатору и также поддерживает протокол LACP. LACP-пакеты передаются на MAC-адрес группы многоадресной передачи.

Если протокол LACP на данном коммутаторе обнаружит на другом конце канала устройство, на котором также активирован этот протокол, он будет независимо передавать пакеты по одним и тем же каналам, чтобы эти два устройства обнаружили между собой множественные каналы и затем сгруппировали их в одно логическое соединение.

В течение периода обнаружения LACP-пакеты передаются каждую секунду.

В дальнейшем алгоритм проверки работоспособности каналов-членов группы будет передавать такие пакеты периодически. Каждый отдельный порт в составе группы может функционировать в LACP-активном или LACP-пассивном режиме.

LACP-активный режим означает, что протокол LACP активируется на порте безусловно, в любом случае, в то время как в LACP-пассивном режиме порт активирует протокол LACP только в случае обнаружения партнера, поддерживающего этот протокол.

Следует отметить, что порт, поддерживающий протокол LACP в активном режиме, будет постоянно передавать LACP-пакеты по соответствующим каналам.

В пассивном же режиме порт, поддерживающий протокол LACP, функционирует по принципу "отвечаю, когда обращаются", благодаря чему такой порт можно использовать для контроля случайных петель (при условии, что другое устройство установлено в активном режиме).

Чтобы агрегировать несколько портов в одну группу, пользователь должен выполнить следующую процедуру:

Действие 1: Выберите идентификатор Trkx (x = 1 - 8) из выпадающего списка групповых идентификаторов.

Действие 2: При необходимости активируйте протокол LACP (стандартный протокол IEEE для управления агрегацией каналов).

Действие 3: Выберите значение Hash Type из выпадающего списка.

Действие 4: Выберите из текстового блока отдельные порты для включения в создаваемую группу агрегации.

Действие 5: Выберите порты в этой группе агрегации для использования в LACP-активном режиме.

Действие 6: Щелкните с указателем на кнопке Apply, чтобы сохранить измененные параметры конфигурации управляемого коммутатора.

Описание настраиваемых параметров функции агрегации в сводном виде представлено в таблице 9.1.

Таблица 9.1. Описание настраиваемых параметров функции агрегации.

Имя параметра	Описание
Group ID	Можно создать до 4 групп агрегации: Trk1 ~ Trk4
LACP	В этом поле активируется или отключается протокол LACP (протокол управления агрегацией каналов). Краткое описание протокола LACP приведено в предыдущем параграфе.
Hash Type	Результат хеширования определяет порт, который будет использоваться для определенного кадра. Доступные варианты хеширования включают: Src MAC, Dst MAC, Src/dst MAC, Src IP, Dst IP и Src/dst IP.
Ports	Это поле используется для назначения портов - членов создаваемой группы агрегации. Для выбора нескольких портов за один раз удерживайте нажатой клавишу CTRL.

Имя параметра	Описание
LACP Active	В этом поле указываются порты - члены группы, которые будут функционировать в LACP-активном режиме. Все не выбранные порты будут использоваться в LACP-пассивном режиме.
Apply	Щелкните с указателем на кнопке Apply, чтобы подтвердить внесенные изменения.
Remove	Щелкните с указателем на этой кнопке, чтобы удалить любую существующую группу агрегации.

9.2 Подраздел LACP Status

На рисунке 9.3 показана сетевая страница с информацией о транкировании портов текущего коммутатора. В верхней части страницы указано состояние протокола LACP на данном управляемом коммутаторе – активирован или отключен.

На этой странице пользователь может указать системный приоритет в поле System Priority. Протокол LACP использует значение системного приоритета и MAC-адрес коммутатора для создания системного идентификатора, а также в процессе согласования с партнером, поддерживающим протокол LACP.

Системный идентификатор протокола LACP представляет собой комбинацию значения системного приоритета протокола (указывается на этой сетевой странице) и MAC-адреса управляемого коммутатора. Системный приоритет определяет, какой управляемый коммутатор принимает решения о портах, объединяемых в логическое соединение.

Чем меньше значение, тем выше приоритет. То есть, устройство с наинизшим значением является главным.

Таблица под названием LACP Status содержит информацию об отдельных портах, которая включает номер порта, состояние протокола LACP, групповой идентификатор и ссылку на партнера, поддерживающего протокол LACP.

Описание параметров в таблице LACP Status в сводном виде представлено в таблице 9.2. Чтобы изменить системный приоритет, введите требуемое значение в поле System Priority, затем щелкните с указателем на кнопке Update.

Чтобы получить обновленные данные о состоянии протокола LACP, щелкните с указателем на кнопке Refresh.

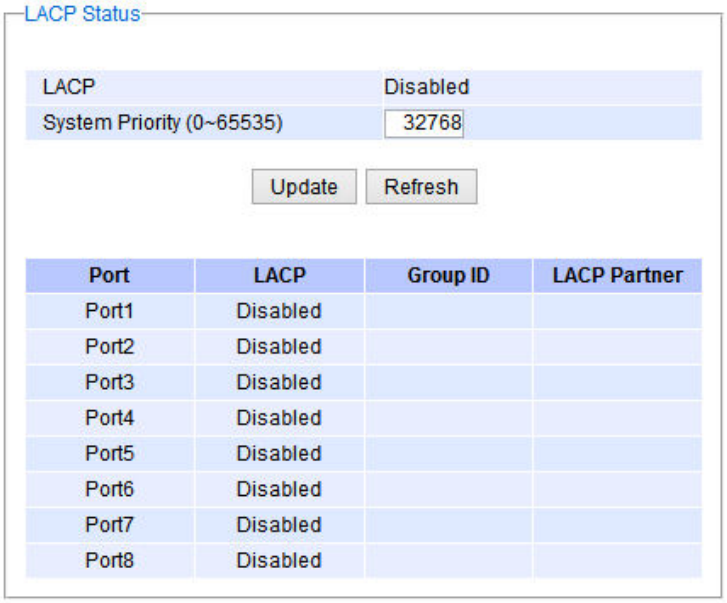


Рисунок 9.3. Сетевая страница с данными о состоянии протокола LACP.

Таблица 9.2. Описание параметров в таблице LACP Status.

Имя параметра	Описание	Заводская настройка по умолчанию
System Priority	Укажите значение системного приоритета для данного управляемого коммутатора в диапазоне от 1 до 65535. Системный приоритет используется в процессе согласования с другими системами. Системный приоритет и MAC-адрес коммутатора используются для создания системного идентификатора. Следует помнить, что чем больше значение, тем ниже приоритет.	32768
Group ID	Значение в этом поле указывает на группу агрегации, в которую входит данный порт.	-
LACP	Disabled: протокол LACP отключен. Passive: протокол LACP функционирует только в пассивном режиме, отвечая на LACP-запросы. Active: протокол LACP осуществляет поиск партнеров, поддерживающих протокол LACP, в активном режиме.	-
LACP Partner	Указывает возможность присутствия партнера, поддерживающего протокол LACP, на другой стороне соединения.	

10 РАЗДЕЛ UNICAST/MULTICAST MAC

В данном разделе меню управляемого коммутатора пользователь может управлять таблицей MAC-адресов, добавляя в нее статические MAC-адреса или фильтруя определенные адреса, чтобы исключить их из переадресации коммутатором.

Управляемый коммутатор Yarus Networks также предоставляет пользователю возможность устанавливать вручную время устаревания MAC-адреса.

Следует понимать, что время устаревания соответствует продолжительности периода, в течение которого распознанный MAC-адрес будет храниться в таблице MAC-адресов. По истечении указанного времени адрес будет удален для экономии памяти.

Данный коммутатор поддерживает управление MAC-адресами одноадресной передачи и многоадресной рассылки.

В этом раздел в общих чертах рассматривается концепция одноадресной и многоадресной переадресации, а также преимущества этих режимов.

Для лучшего понимания схемы организации одноадресной передачи и многоадресной рассылки представлены на рисунке 10.1.

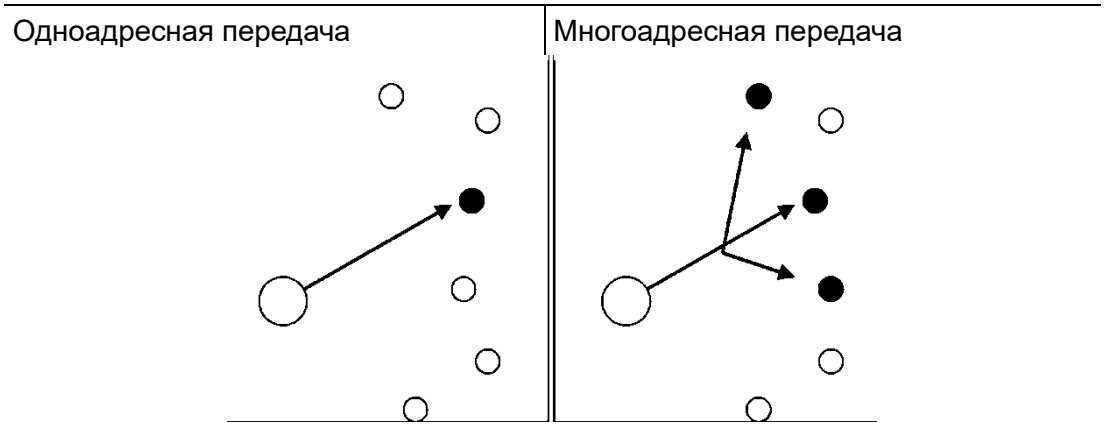


Рисунок 10.1. Одноадресная передача по сравнению с многоадресной рассылкой.

- Одноадресная передача: в этом режиме сообщения передаются в единственное место назначения в сети, которое идентифицируется по уникальному MAC-адресу. Этот метод прост. Он предусматривает наличие только одного источника и одного места назначения.
- Многоадресная передача: в этом режиме используется более сложная схема организации передачи. Сообщения передаются от одного источника в несколько мест назначения. При этом принимать многоадресную передачу могут только те узлы или хост-устройства, которые принадлежат к определенной группе многоадресной передачи. Помимо того, в сети, поддерживающей многоадресную передачу, передается только один экземпляр информации до точки, в которой путь до членов группы начинает разветвляться. В точках ветвления создаются копии многоадресных пакетов, которые затем соответственно переадресовываются. Такой подход обеспечивает

возможность управления большим объемом трафика, адресованного в различные места назначения, с эффективным использованием пропускной способности сети. Многоадресная фильтрация повышает производительность сетей, передающих многоадресный трафик.

На рисунке 10.2 показано раскрывающееся меню раздела Unicast/Multicast MAC, которое позволяет пользователям управлять таблицей MAC-адресов и просматривать ее состояние.

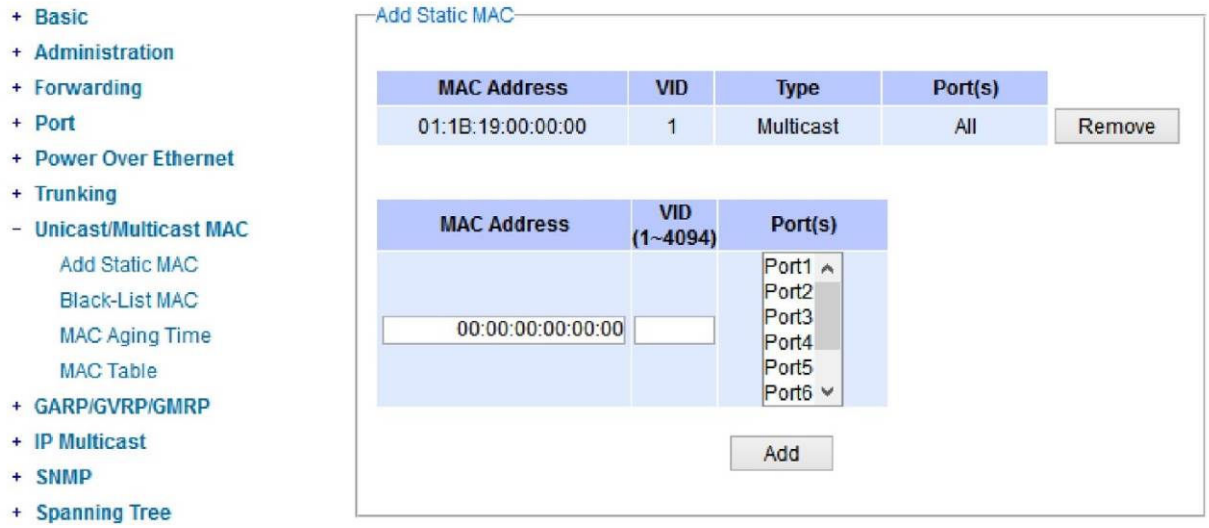


Рисунок 10.2. Раскрывающееся меню в разделе Unicast/Multicast MAC.

10.1 Подраздел Add Static MAC

Данный управляемый коммутатор позволяет пользователю вручную сохранять статические MAC-адреса в памяти устройства. Используя статические MAC-адреса, записанные в его памяти, управляемый коммутатор переадресовывает трафик, основанный на MAC-адресах, на порты назначения с определенными идентификаторами виртуальной локальной сети (VLAN). Ниже приведено описание нескольких простых действий, которые нужно выполнить, чтобы добавить статический MAC-адрес.

Действие 1: введите MAC-адрес, который может быть адресом одноадресной передачи или многоадресной рассылки.

Действие 2: укажите идентификатор соответствующей VLAN.

Действие 3: выберите порты, для которых применяется этот статический MAC-адрес. Чтобы выбрать одновременно несколько портов, удерживайте нажатой клавишу Ctrl.

Действие 4: Щелкните с указателем на кнопке Add.

На рисунке 10.3 показана сетевая страница для добавления статических адресов одноадресной или многоадресной передачи.

На рисунке показан пример таблицы со статическим MAC-адресом в верхней части сетевой страницы.

В последнем столбце таблицы для каждой записи предусмотрена кнопка Remove. Пользователь может удалить любой существующий MAC-адрес из таблицы, щелкнув с

указателем на кнопке Remove.

В нижней части сетевой страницы пользователь может ввести новый статический MAC-адрес и указать для него идентификатор VLAN, выполнив описанную выше процедуру.

В таблице 10.1 в сводном виде представлено описание полей на сетевой странице Add Static MAC.

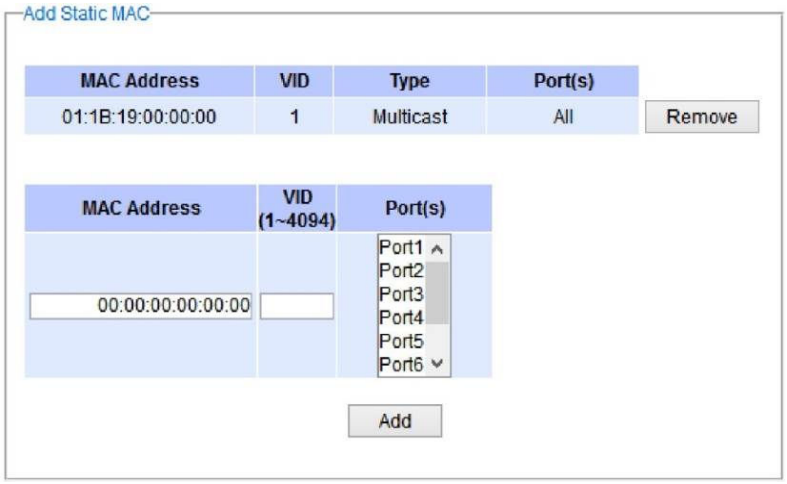


Рисунок 10.3. Сетевая страница добавления статических MAC-адресов.

Таблица 10.1. Описание полей на сетевой странице Add Static MAC.

Имя параметра	Описание
MAC address	Введите MAC-адрес вручную.
VID	Укажите идентификатор VLAN, к которой относится этот статический MAC-адрес (1 - 4096).
Type	Тип MAC-адреса - многоадресный (Multicast) или одноадресный (Unicast).
Port(s)	Выберите порты, для которых применяется этот статический MAC-адрес.
Add	Подтвердите MAC-адрес и добавьте его в таблицу, щелкнув с указателем на этой кнопке.
Remove	Щелкните с указателем на этой кнопке, чтобы удалить существующий статический MAC-адрес из таблицы.

10.2 Подраздел Black-List MAC

Как уже упоминалось выше, управляемый коммутатор также позволяет пользователям вручную настраивать режим фильтрации по MAC-адресам.

На рисунке 10.4 показана сетевая страница подраздела Black-List MAC.

В верхней части страницы имеется таблица существующих фильтруемых MAC-адресов.

В этой таблице пользователь может отменить фильтрацию любой записи, щелкнув с указателем на кнопке Remove в соответствующей строке.

В нижней части страницы пользователь может добавить новый MAC-адрес источника, трафик которого будет блокироваться в режиме фильтрации по MAC-адресам ("черный список").

В таблице 10.2 в сводном виде представлено описание полей на сетевой странице фильтрации MAC-адресов.

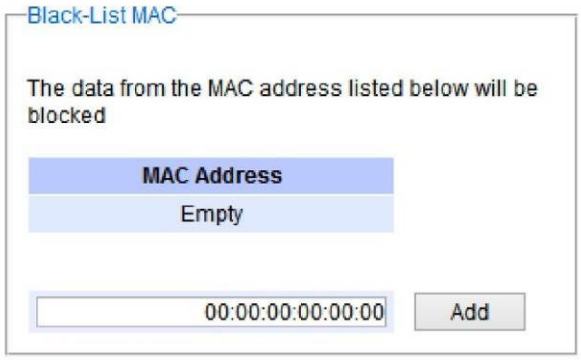


Рисунок 10.4. Сетевая страница настройки черного списка MAC-адресов.

Таблица 10.2. Описания сетевой страницы режима фильтрации по MAC-адресам.

Имя параметра	Описание
MAC Address	Введите вручную MAC-адрес, который будет помещен в черный список или отфильтрован.
Remove	Удалите соответствующую запись из таблицы фильтрации по MAC-адресам.
Add	Добавьте MAC-адреса в таблицу фильтрации по MAC-адресам.

10.3 Подраздел MAC Aging Time

Эта функция позволяет пользователям вручную устанавливать время устаревания MAC-адресов, как показано на рисунке 10.5.

Пользователь может указать время устаревания в диапазоне от 0 до 600 секунд. Следует учитывать, что значение времени устаревания по умолчанию составляет 300 секунд.

В управляемом коммутаторе таблица MAC-адресов хранится в памяти устройства и используется для связывания MAC-адресов с номерами портов для передачи кадров данных. Время устаревания соответствует продолжительности периода, в течение которого MAC-адрес хранится в таблице MAC-адресов.

Чем больше значение времени устаревания, тем дольше связанный MAC-адрес остается в памяти коммутатора.

Используя адрес из этой таблицы, коммутатор может переадресовывать соответствующие кадры данных сразу же на определенный порт, а не передавать их на все порты в режиме лавинной рассылки.

Более короткое время устаревания позволит коммутатору раньше удалять из таблицы устаревшие записи, чтобы освободить место для запоминания новых MAC-адресов.

Такой подход может оказаться полезным в условиях сетевого окружения с большим количеством MAC-адресов (или конечных устройств), а также если передача трафика между двумя конечными устройствами быстро завершается.

Рисунок 10.5. Сетевая страница подраздела MAC Aging Time.

10.4 Подраздел MAC Table

На этой сетевой странице отображается информация о текущих MAC-адресах одноадресной передачи и многоадресной рассылки, записанных в памяти управляемого коммутатора (таблица MAC-адресов), как показано на рисунке 10.6.

Сначала выводится список MAC-адресов одноадресной передачи, а затем - список MAC-адресов многоадресной рассылки.

Если все записи не помещаются на одной странице, для просмотра следующих адресов пользователь может щелкнуть с указателем на кнопке Next Page.

Пользователь также может на собственное усмотрение удалить все динамические записи из таблицы MAC-адресов, щелкнув с указателем на кнопке Clear Dynamic Entries в нижней части сетевой страницы.

Описание полей таблицы MAC-адресов в сводном виде представлено в таблице 10.3.

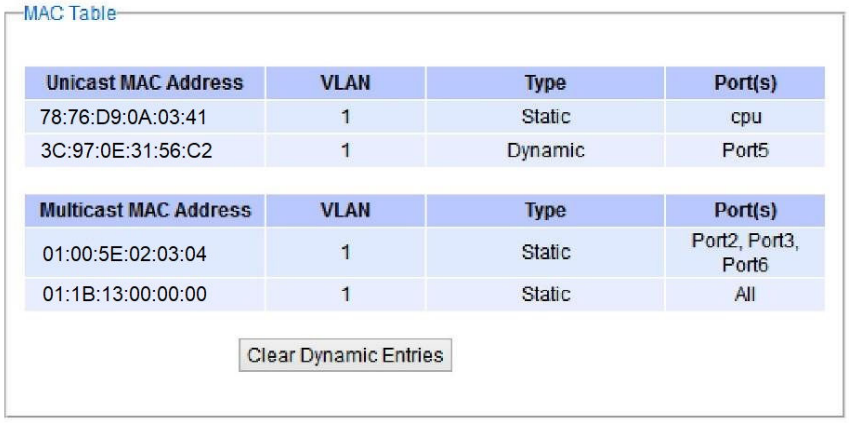


Рисунок 10.6. Сетевая страница подраздела MAC Table.

ПРИМЕЧАНИЕ: Статический адрес многоадресной передачи можно взять из подраздела "Add Static MAC" раздела меню "Unicast/Multicast MAC", либо из подраздела "Static IP Multicast" в разделе меню "IP multicast" .

Таблица 10.3. Описание полей таблицы MAC-адресов.

Имя параметра	Описание
Unicast/Multicast MAC	В данном поле отображается MAC-адрес.
VLAN	В данном поле отображается идентификатор VLAN.
Type	В данном поле отображается тип MAC-адреса - динамический или статический. Напоминаем, что динамическим называется адрес,

Имя параметра	Описание
	который устройство распознает автоматически, в то время как статический адрес вводится пользователем вручную.
Ports	В данном поле отображается порт, которому принадлежит этот MAC-адрес.
Clear Dynamic Entries	Щелкните с указателем на этой кнопке для удаления всех динамических MAC-адресов.
Next Page	Щелкните с указателем на этой кнопке, чтобы перейти на следующую страницу для просмотра MAC-адресов, которые не поместились в окне.

11 РАЗДЕЛ GARP/GVRP/GMRP

Данная страница используется для настройки параметров трех протоколов - GARP, GVRP и GMRP. Все три упомянутых протокола предназначены для решения одной основной задачи – очистки сети от ненужного трафика посредством предотвращения передачи / ретрансляции пакетов данных незарегистрированным пользователям.

Все эти функции активируются по умолчанию.

Они могут быть отключены только при условии, что в таблице групп многоадресной передачи нет ни одного MAC-адреса.

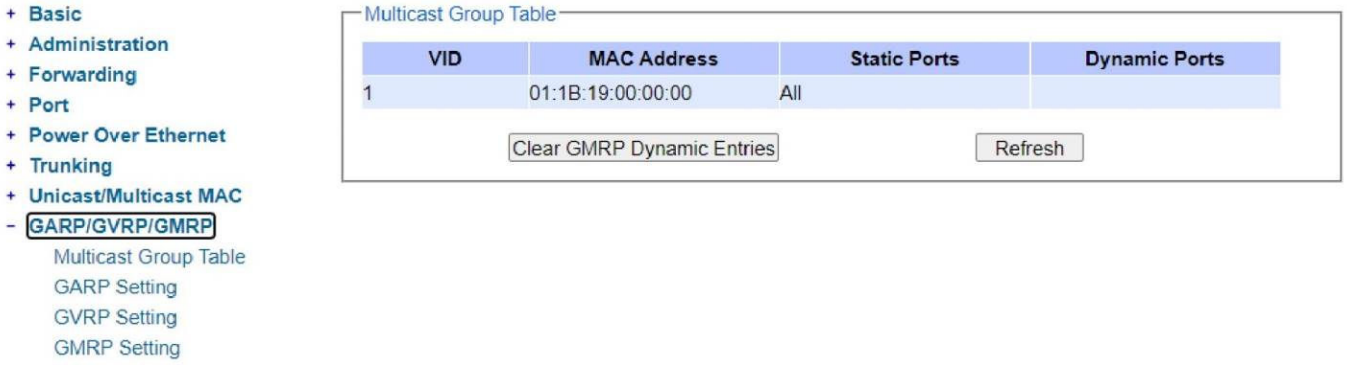


Рисунок 11.1. Раскрывающееся меню раздела GARP/GVRP/GMRP.

11.1 Подраздел Multicast Group Table

В данном подразделе пользователь может просмотреть список MAC-адресов, которые регистрировались протоколом GMRP в динамическом режиме с записью в таблицу групп многоадресной передачи.

Таблица групп многоадресной передачи, показанная на рисунке 11.2, включает следующую информацию для каждого MAC-адреса: идентификатор VLAN (VID), статические порты (Static Ports) и динамические порты (Dynamic Ports) протокола GMRP.

Пользователь может полностью удалить информацию из таблицы, щелкнув с указателем на кнопке Clear GMRP Dynamic Entries, либо просмотреть последние обновления в таблице, щелкнув с указателем на кнопке Refresh.

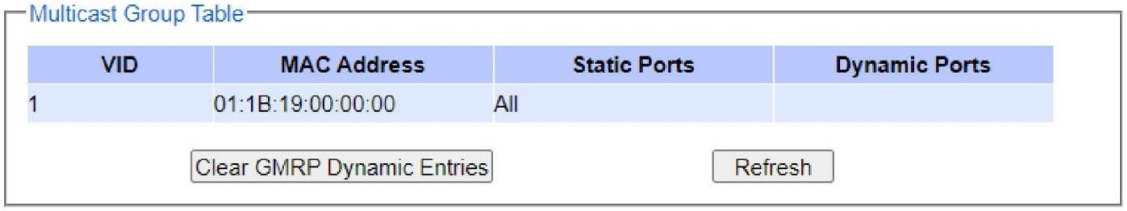


Рисунок 11.2. Таблица групп многоадресной передачи.

11.2 Подраздел GARP Setting

На рисунке 11.3 показана сетевая страница подраздела GARP Setting, на которой можно настроить различные таймеры (Join, Leave и LeaveAll). На всех устройствах, которые

обмениваются атрибутами, должны быть установлены одинаковые значения этих таймеров. Следует отметить, что для таймеров протокола GARP указываются значения, кратные 10 миллисекундам.

В таблице 11.1 в сводном виде представлены описание и значения всех таймеров в разделе GARP Setting.

После ввода новых значений щелкните с указателем на кнопке Update.

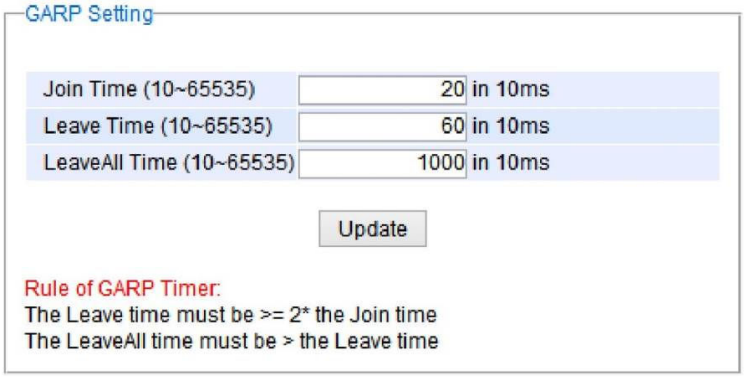


Рисунок 11.3. Сетевая страница подраздела GARP Setting.

Таблица 11.1. Описание настраиваемых параметров таймеров протокола GARP.

Имя параметра	Описание	Заводская настройка по умолчанию
Join Timer	В данном поле устанавливается значение таймера Join протокола GARP. Диапазон значений - от 0 до 65535 секунд.	20 x 10 мсек
Leave Timer	В данном поле устанавливается значение таймера Leave протокола GARP. Диапазон значений - от 0 до 65535 секунд.	60 x 10 мсек
Leave All Timer	В данном поле устанавливается значение таймера Leave All протокола GARP. Диапазон значений - от 0 до 65535 секунд.	1000 x 10 мсек

11.3 Подраздел GVRP Setting

В этом подразделе можно активировать протокол GVRP на коммутаторе, после чего этот протокол может быть активирован для всех или определенных портов и групп агрегации.

С каждого порта можно получить доступ к IP-адресу многоадресной рассылки с указанным идентификатором VLAN.

На рисунках 11.4 и 11.5 ниже показаны окна настройки параметров и статистики протокола GVRP соответственно.

После активации протокола GVRP сети VLAN могут быть добавлены в коммутатор, который является конечным узлом сети, только локально.

Другие коммутаторы могут в динамическом режиме запоминать остальные VLAN в любых местах в сети, используя протокол GVRP.

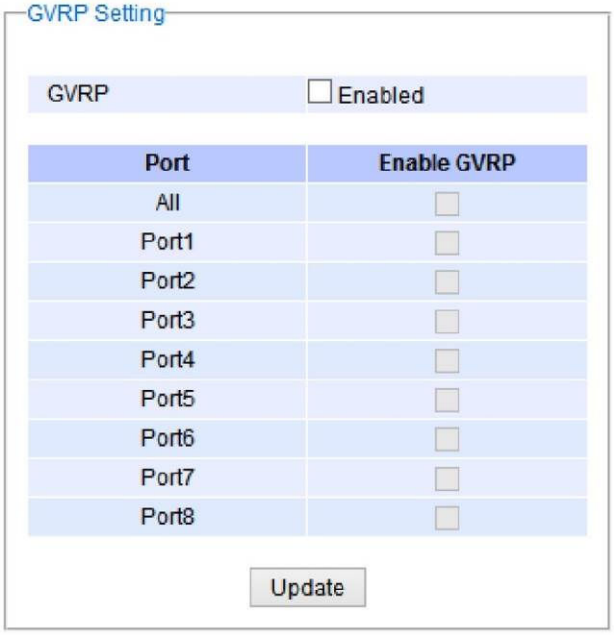


Рисунок 11.4. Окно настройки параметров протокола GVRP с активацией протокола на портах.

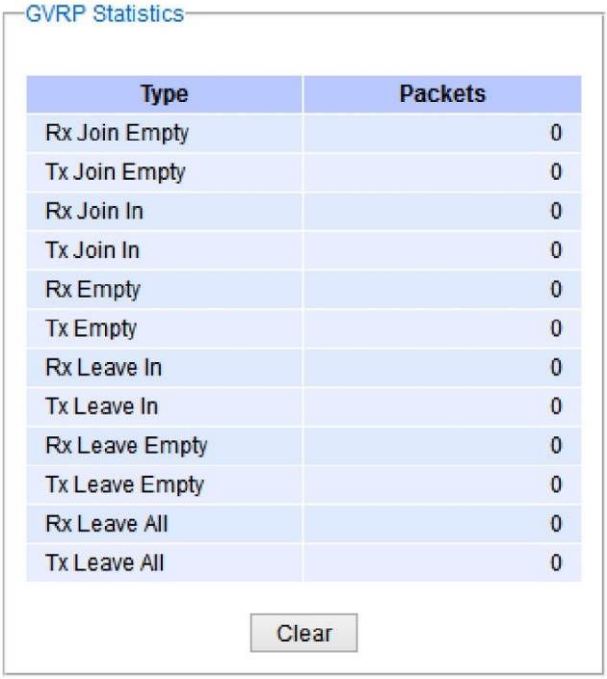


Рисунок 11.5. Статистика протокола GVRP.

Чтобы активировать протокол GVRP, в окне, установите флажок Enabled в поле GVRP, а затем выберите порты, которые будут поддерживать этот протокол, установив флажки в соответствующих полях.

Для сохранения изменений в памяти коммутатора щелкните с указателем на кнопке Update.

На рисунке показано окно сводной статистики количества переданных пакетов протокола GVRP с разделением на следующие типы пакетов: Rx Join Empty, Tx Join Empty, Rx Join In, Tx Join In, Rx Empty, Tx Empty, Rx Leave In, Tx Leave In, Rx Leave Empty, Tx Leave Empty, Rx Leave All и Tx Leave All.

Чтобы удалить все статистические данные из таблицы, щелкните с указателем на кнопке Clear, которая находится под таблицей.

В таблице 11.2 приведено описание настраиваемых параметров протокола GVRP.

Таблица 11.2. Описание настраиваемых параметров протокола GVRP.

Имя параметра	Описание	Заводская настройка по умолчанию
GVRP	Данное поле используется для активации или отключения протокола GVRP. Протокол GVRP может быть активирован при условии, что коммутатор установлен в режиме VLAN 802.1q.	Выключено
Port	Данное поле используется для активации или отключения протокола GVRP на отдельных портах. Если пользователь уже создал группу агрегации (например, Trk1), ее также можно активировать. Чтобы активировать протокол сразу на всех портах, установите флажок в поле All Ports.	Отключено на всех портах
Clear Statistics	Обнуляет все счетчики статистики протокола GVRP.	Удаление записи

11.4 Подраздел GMRP Setting

В этом подразделе пользователь может активировать протокол GMRP глобально, а также для всех или отдельных портов и групп агрегации.

Чтобы активировать протокол GMRP, в окне, показанном на рисунке 11.6, установите флажок Enabled в поле GMRP, а затем выберите порты, которые будут поддерживать этот протокол, установив флажки в соответствующих полях.

Для сохранения изменений в памяти коммутатора щелкните указателем на кнопке Update.

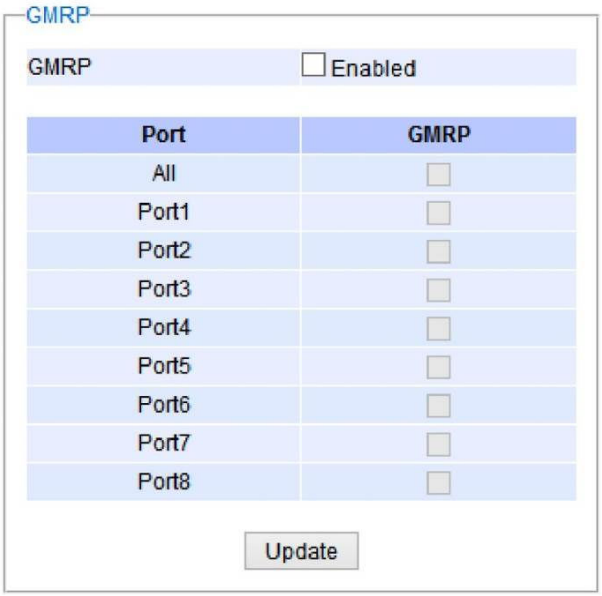


Рисунок 11.6. Окно настройки параметров протокола GMRP.

В нижней части этой страницы также можно просмотреть статистику протокола GMRP. Соответствующее окно показано на рисунке 11.7.

В окне GMRP Statistics приведена сводная статистика количества переданных пакетов протокола GMRP с разделением на следующие типы пакетов: Rx Join Empty, Tx Join Empty, Rx Join In, Tx Join In, Rx Empty, Tx Empty, Rx Leave In, Tx Leave In, Rx Leave Empty, Tx Leave

Empty, Rx Leave All и Tx Leave All.

Чтобы удалить все статистические данные из таблицы, щелкните с указателем на кнопке Clear, которая находится под таблицей.

В таблице 11.3 приведено краткое описание настраиваемых параметров протокола GMRP и статистики.

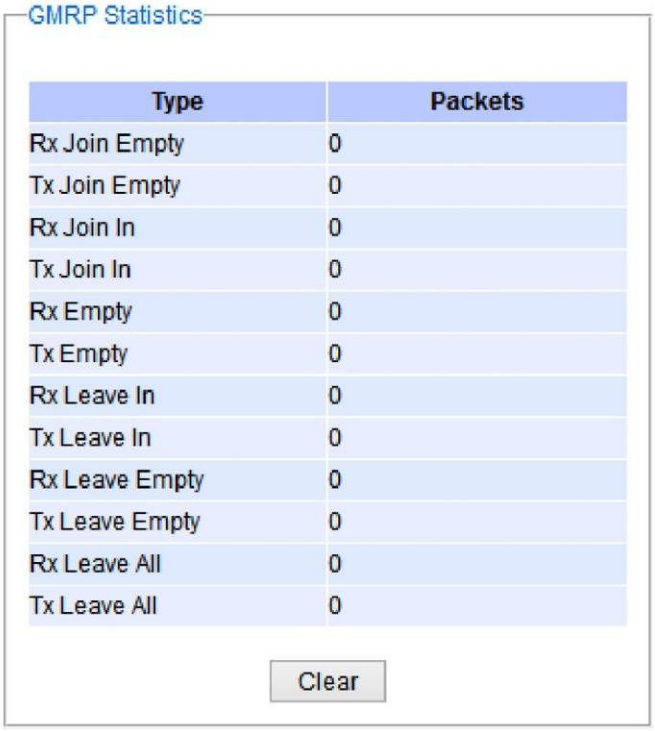


Рисунок 11.7. Окно GMRP Statistics.

Таблица 11.3. Описание настраиваемых параметров протокола GMRP и статистики.

Поле	Описание поля	Заводская настройка по умолчанию
GMRP	В этом поле можно активировать или отключить протокол GMRP, установив или сняв флажок соответственно. Протокол GMRP может быть активирован при условии, что коммутатор установлен в режиме VLAN 802.1q.	Выключено
Port	В этом поле можно активировать или отключить протокол GMRP для отдельных портов, установив или сняв соответствующие флажки. Если пользователь уже создал группу агрегации (например, Trk1), ее также можно активировать. Чтобы активировать протокол сразу на всех портах, установите флажок в поле All Ports.	Отключено на всех портах
Clear Statistics	В этом поле можно обнулить все статистические данные протокола GMRP.	Удаление записей

12 РАЗДЕЛ IP MULTICAST

Управляемый коммутатор поддерживает протокол управления группами пользователей сети Интернет (IGMP), который представляет собой коммуникационный протокол, используемый в сетях IP версии 4 для привязки коммутаторов к группам многоадресной передачи.

IGMP является неотъемлемой частью многоадресной рассылки IPv4. Он работает над сетевым уровнем модели OSI. Одной из наиболее важных функций, связанных с этим протоколом, является отслеживание IGMP, которое поддерживается управляемым коммутатором и значительно расширяет функциональность сети.

IGMP Snooping — это процесс “прослушивания” сетевого трафика IGMP. Прослушивая разговоры между различными устройствами, он поддерживает карту ссылок и многоадресных потоков IP. Это означает, что многоадресный трафик может быть отфильтрован по каналам управляемого коммутатора, которые в нем не нуждаются. Таким образом, IGMP Snooping позволяет управляемому коммутатору перенаправлять многоадресный трафик только по тем ссылкам, которые его запросили. Этот раздел содержит три подменю, как показано на рисунке 12.1:

- IGMP
- Static IP Multicast
- MLD

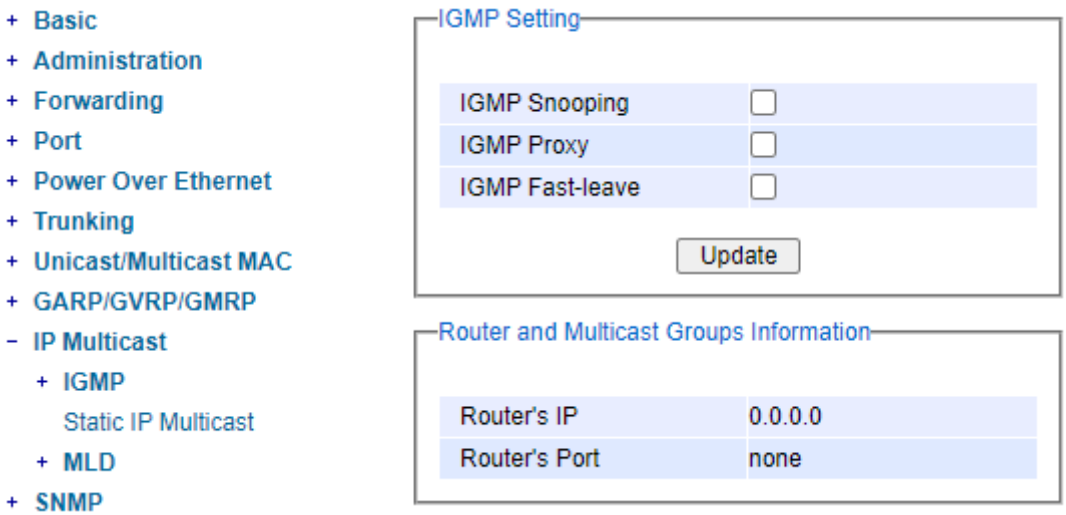


Рисунок 12.1. Раскрывающееся меню в разделе IP Multicast.

12.1 Подраздел IGMP

Подраздел IGMP (протокол управления группами пользователей в сети Интернет), в свою очередь, делится на три подраздела нижнего уровня: Setting, IP Multicast Table и Statistics.

Эти три подраздела нижнего уровня в подразделе меню IGMP показаны на рисунке 12.2.

Рисунок 12.2. Подразделы нижнего уровня подраздела меню IGMP.

12.1.1 Подраздел IGMP Settings

На этой сетевой странице пользователь может настроить параметры протокола IGMP на управляемом коммутаторе. При этом можно активировать следующие три функции: IGMP Snooping, IGMP Proxy и IGMP Fast-leave.

Установив флажки в нужных полях, щелкните с указателем на кнопке Update, чтобы изменения вступили в силу.

В нижней части страницы расположено окно с информацией о маршрутизаторе и группах многоадресной передачи, которая включает IP-адрес маршрутизатора и данные о порте. Описание настраиваемых параметров протокола IGMP в сводном виде представлено в таблице 12.1.

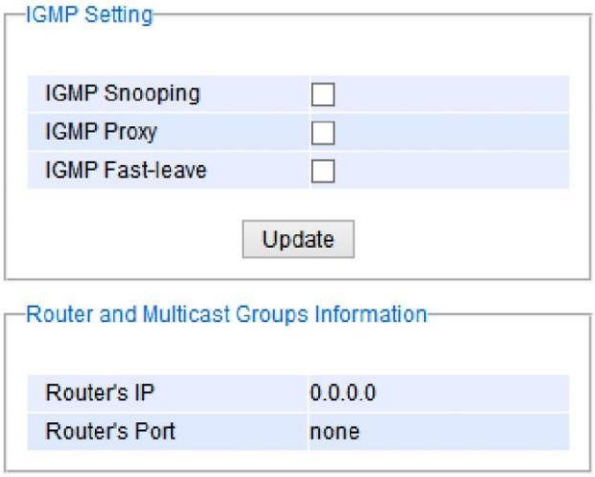


Рисунок 12.3. Сетевая страница настройки параметров протокола IGMP.

Таблица 12.1. Описание настраиваемых параметров протокола IGMP.

Имя параметра	Описание	Заводская настройка по умолчанию
IGMP Snooping	Установите флажок в данном поле, чтобы активировать функцию IGMP Snooping.	Выключено
IGMP Proxy	Установите флажок в данном поле, чтобы активировать функцию IGMP Proxy. См. примечание ниже.	Выключено
IGMP Fast-leave	Установите флажок в данном поле, чтобы активировать функцию IGMP Fast-Leave. См. примечание ниже.	Выключено
Router's IP	В данном поле отображается IP-адрес маршрутизатора многоадресной рассылки.	-
Router's Port	В данном поле отображается порт, подключенный к маршрутизатору многоадресной рассылки.	-

ПРИМЕЧАНИЕ:

IGMP Proxy работает как промежуточный сервер, как показано на рисунке 12.4. Когда он получает сообщение с запросом о членстве от маршрутизатора, он отправляет сообщение с отчетом о членстве на порт маршрутизатора. Когда он получает сообщение с отчетом о членстве от компьютера в новой группе многоадресной рассылки, он отправляет сообщение с отчетом о членстве обратно на порт маршрутизатора. Когда он получает сообщение о выходе из группы от компьютера, который является единственным в группе, он отправляет сообщение о выходе из группы на порт маршрутизатора и удаляет компьютер из группы многоадресной рассылки. Прокси-сервер подобен посреднику, который обрабатывает информацию о группе многоадресной рассылки между маршрутизаторами и компьютерами.

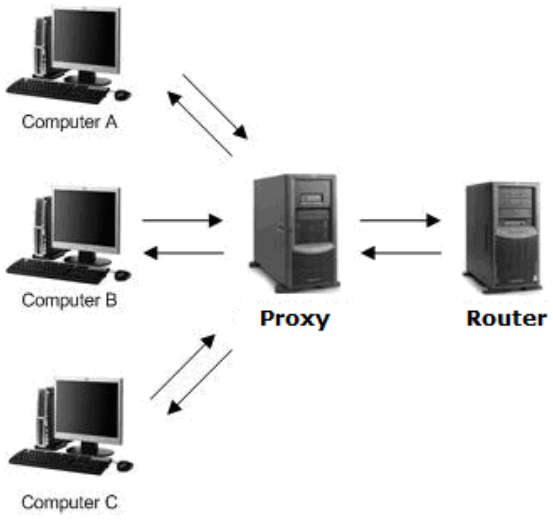


Рисунок 12.4. Пример работы IGMP Proxy.

IGMP Fast-leave: При получении сообщения о выходе из группы порты в группе будут немедленно удалены из записи многоадресной рассылки IP.

12.1.2 Подраздел IGMP IP Multicast Table

На этой сетевой странице представлена информация о таблице членства протокола IGMP и таблице многоадресной IP-рассылки.

На рисунке 12.5 показана сетевая страница таблицы многоадресной IP-рассылки по протоколу IGMP.

В верхней части окна находится таблица членства протокола IGMP, а в нижней - таблица многоадресной IP-рассылки, которая содержит и статические адреса многоадресной IP-рассылки, и IP-адреса, включенные в группу многоадресной рассылки в динамическом режиме. Статические атрибуты порта, добавляемого в группу, вводятся пользователем вручную, а в динамическом режиме функция IGMP Snooping управляемого коммутатора присоединяет порты к группе автоматически.

Чтобы получить обновленные данные в каждой упомянутой таблице, щелкните с указателем на кнопке Refresh.

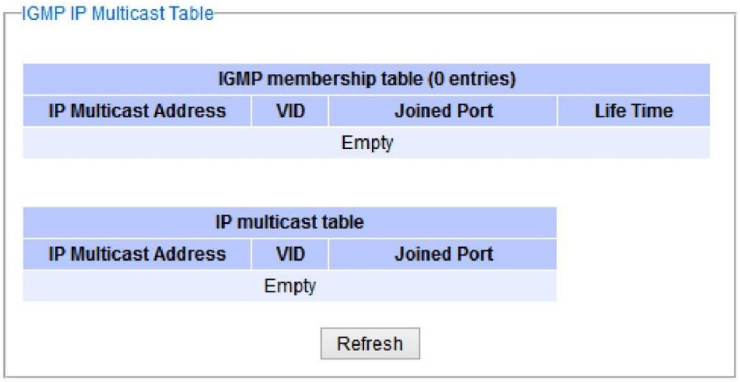


Рисунок 12.5. Таблица многоадресной IP-рассылки протокола IGMP.

На рисунке 12.6 показаны примеры таблицы членства протокола IGMP и таблицы многоадресной IP-рассылки.

Эти таблицы используют информацию из памяти управляемого коммутатора. Таблица членства протокола IGMP содержит столбцы IP Multicast Address, VLAN ID, Joined Port и Life Time.

Следует отметить, что время жизни в поле Life Time указывается в секундах. Таблица многоадресной IP-рассылки состоит из трех столбцов: IP Multicast Address, VLAN ID и Joined Port.

Обратите внимание на букву (S) или (D) рядом с номером присоединенного порта, которая обозначает режим включения – статический или динамический соответственно.

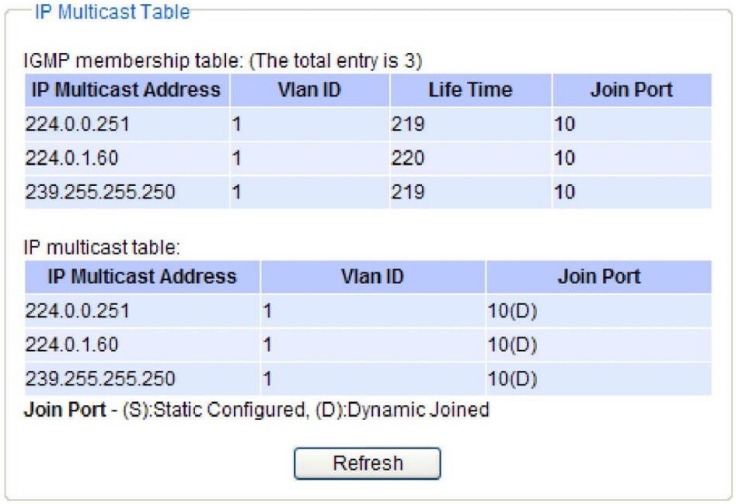


Рисунок 12.6. Пример таблицы многоадресной IP-рассылки протокола IGMP.

12.1.3 Подраздел IGMP Statistics

На этой сетевой странице, которая показана на рисунке 12.7, предоставлена статистическая информация протокола IGMP.

Пользователь может проверить число IGMP-пакетов различных категорий: Rx Total, Rx Valid, Rx Invalid, Rx General Queries, Tx General Queries, Rx Group-Specific Queries, Tx Group-Specific Queries, Rx Leaves, Tx Leaves, Rx Reports, Tx Reports и Rx Others.

Пользователь может обнулить данные во всех категориях одновременно, щелкнув с указателем

на кнопке Clear.

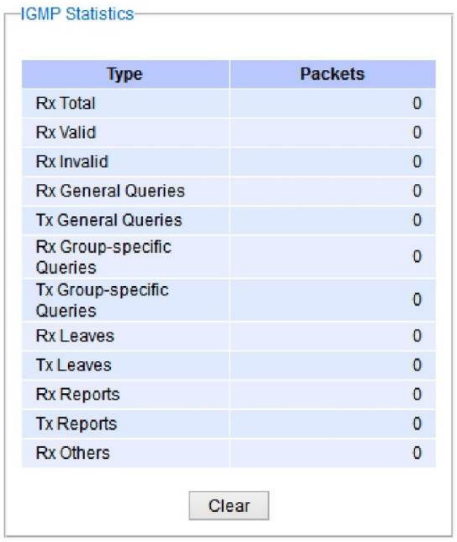


Рисунок 12.7. Сетевая страница раздела IGMP Statistics.

Пример окна с таблицей статистики протокола IGMP показан на рисунке 12.8.

В этом окне отображаются значения статистики пакетов протокола IGMP, переданных и принятых управляемым коммутатор со времени последнего обнуления.

Описание статистических параметров протокола IGMP в сводном виде представлено в таблице 12.2.

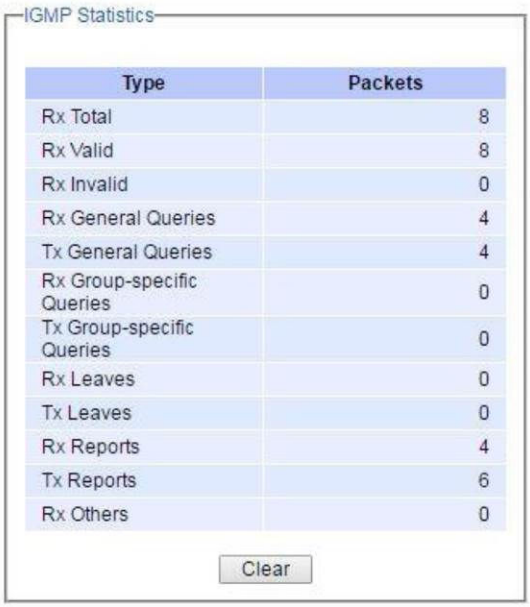


Рисунок 12.8. Пример статистики протокола IGMP.

Таблица 12.2. Описание статистических параметров протокола IGMP.

Имя статистического параметра	Описание	Заводская настройка по умолчанию
Rx Total	Общее количество IGMP-пакетов, принятых управляемым коммутатором.	-
Rx Valid	Количество действительных IGMP-пакетов, принятых управляемым коммутатором.	-

Имя статистического параметра	Описание	Заводская настройка по умолчанию
Rx Invalid	Количество недействительных IGMP-пакетов, принятых управляемым коммутатором.	-
Rx General Queries	Количество IGMP-пакетов с общим запросом членства, принятых управляемым коммутатором.	-
Tx General Queries	Количество IGMP-пакетов с общим запросом членства, переданных управляемым коммутатором.	-
Rx Group Specific Queries	Количество IGMP-пакетов с запросом членства в определенной группе, принятых управляемым коммутатором.	-
Tx Group Specific Queries	Количество IGMP-пакетов с запросом членства в определенной группе, переданных управляемым коммутатором.	-
Rx Leaves	Количество IGMP-пакетов с уведомлением о выходе из группы, принятых управляемым коммутатором.	-
Tx Leaves	Количество IGMP-пакетов с уведомлением о выходе из группы, переданных управляемым коммутатором.	-
Rx Reports	Количество IGMP-пакетов с отчетом о членстве, принятых управляемым коммутатором.	-
Tx Reports	Количество IGMP-пакетов с отчетом о членстве, переданных управляемым коммутатором.	-
Rx Others	Количество прочих IGMP-пакетов, принятых управляемым коммутатором.	-

12.2 Подраздел Static IP Multicast

Этот подраздел позволяет пользователям вручную добавлять новые или удалять существующие статические IP-записи многоадресной рассылки и присоединенные порты. На рисунке 12.9 показана веб-страница статической многоадресной IP-рассылки, где верхняя часть страницы представляет собой таблицу существующих записей многоадресных IP-адресов, а нижняя часть страницы содержит поля для добавления новой записи многоадресного IP-адреса в таблицу. Пользователи должны указать IP-адрес многоадресной рассылки, идентификатор VLAN (VID) и списки номеров портов, которые присоединятся к статической группе многоадресной рассылки IP (присоединенный порт).

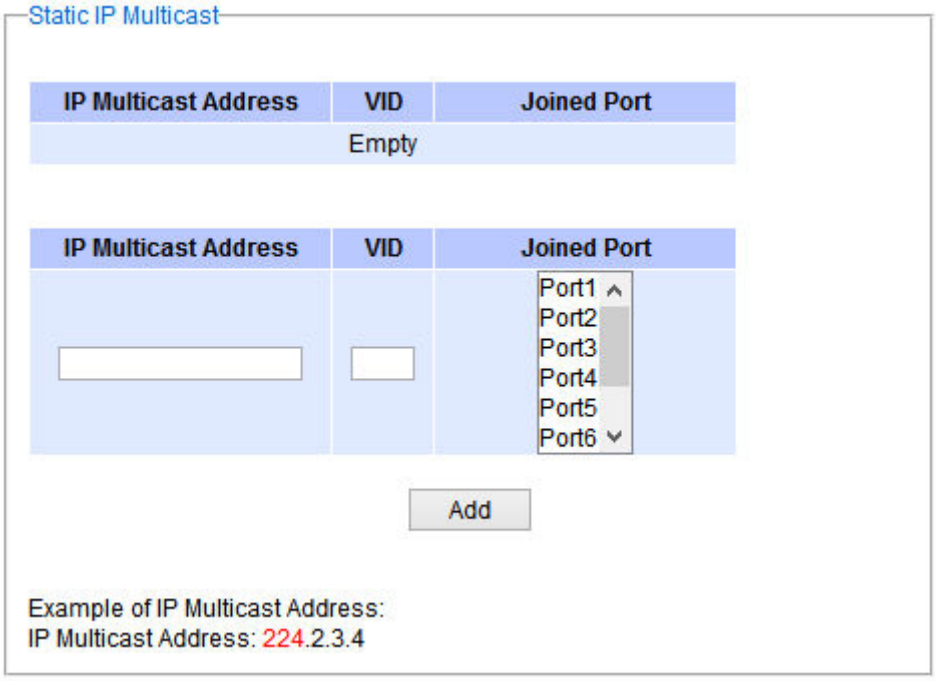


Рисунок 12.9. Сетевая страница настройки статической многоадресной рассылки.

Пример записи группы многоадресной рассылки показан на рисунке 12.10, где существующий IP адрес многоадресной рассылки 224.2.3.4, который принадлежит VLAN 1 и имеет номера портов 2, 3 и 6 в группе. В следующих процедурах описано, как добавить новую группу многоадресной рассылки.

Например: Групповой IP-адрес многоадресной рассылки равен 224.1.1.1, а соединяющими портами являются Port1, Port2 и Port5 с VLAN = 1.

- Сначала пользователи должны ввести IP = 224.1.1.1 в столбец IP-адрес многоадресной рассылки.
- Затем пользователи должны ввести идентификатор VLAN = 1 в столбце идентификатор VLAN (VID).
- Затем, удерживая клавишу “Ctrl” на клавиатуре, щелкните по всем соответствующим номерам портов в столбце "Joined Port" (в данном примере Port1, Port2 и Port5), чтобы выбрать, какие порты будут присоединяться к группе многоадресной рассылки IP.
- Далее нажмите на кнопку Add. Затем добавляется IP-адрес, как показано на рисунке 12.10.
- Чтобы удалить существующий статический IP-адрес многоадресной рассылки из таблицы, нажмите кнопку Remove рядом с этой записью.

Эти процедуры аналогичны процедурам для добавления или удаления Одноадресных/многоадресных MAC-адрес записей как показано в пункте 10.1. Разница лишь в том, что IP-адрес многоадресной рассылки имеет форма 224.XX.XX.XX.

Примечание. Адрес многоадресной рассылки IPv4 (класс D) находится в диапазоне от 224.0.0.0 до 239.255.255.255.

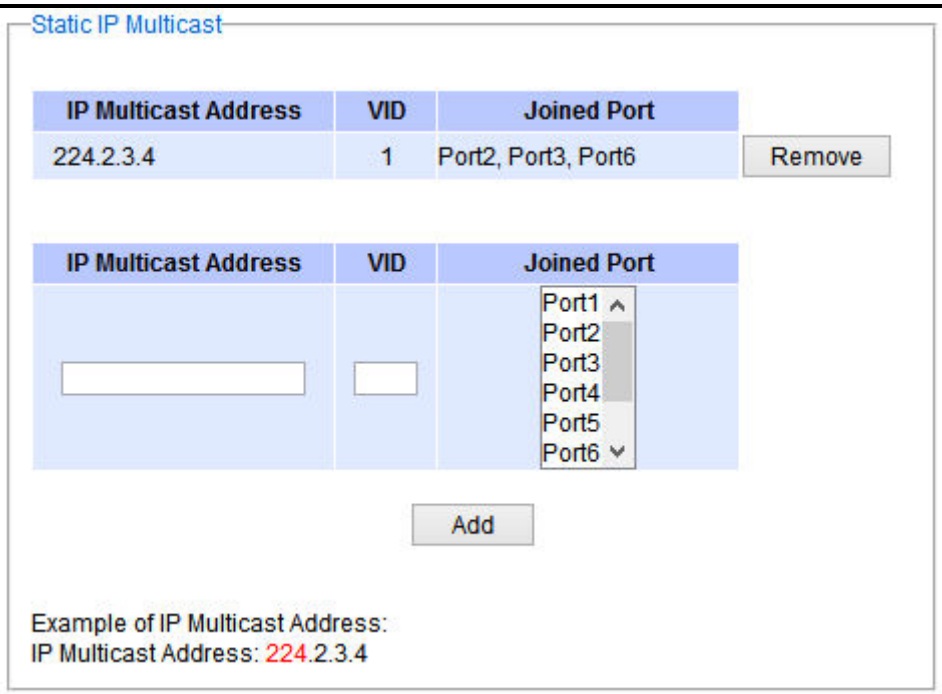


Рисунок 12.10. Пример настройки статического IP Multicast.

12.3 Подраздел MLD

Функция поиска групповых слушателей (MLD) используется в сетях с поддержкой интернет-протокола версии 6 (IPv6) для обнаружения узлов, непосредственно подключенных к интерфейсам устройства, которые желают принимать многоадресные пакеты. Такие соседние узлы называются "многоадресными прослушивателями".

Функция MLD встроена в протокол ICMPv6 (версия 6 протокола межсетевых управляющих сообщений), который входит в стандартный инструментарий протоколов IPv6.

По принципу действия она подобна протоколу управления группами в сети Интернет (IGMP). Этот протокол специально ищет адреса многоадресной рассылки, которые представляют интерес для соседних узлов устройства.

В версии IPv6 для многоадресной рассылки зарезервирован диапазон адресов FF00::/8. Затем функция MLD передает эту информацию протоколу многоадресной маршрутизации, активированному на коммутаторе, чтобы передавать многоадресные пакеты на все соответствующие интерфейсы, то есть, всем подписавшимся многоадресным прослушивателям.

Следует отметить, что функция MLD представляет собой асимметричный протокол, который устанавливает различные режимы для многоадресных прослушивателей и для маршрутизаторов (или управляемых коммутаторов в нашем случае).

Как показано на рисунке 12.11, подраздел MLD раздела меню IP Multicast, в свою очередь, состоит из трех подразделов нижнего уровня: Setting, IPv6 Multicast Table и Statistics.

Рисунок 12.11. Подразделы нижнего уровня подраздела меню MLD.

Как правило, устройство, поддерживающее функцию MLD, относится к одному из следующих функциональных типов: генератор запросов, устройство слежения или прокси.

Генератор запросов функции MLD представляет собой устройство, которое отвечает за координацию многоадресных потоков и информацию о членстве для функции MLD.

Генератор запросов может передавать сообщения с запросом членства, чтобы проверить, какие узлы являются членами группы.

Он также может обрабатывать сообщения с отчетами о членстве и о выходе из группы. Устройство слежения функции MLD представляет собой "устройство-шпион", которое отслеживает MLD-сообщения с целью оптимизации потоков, чтобы только подписанные интерфейсы могли принимать многоадресные пакеты.

Устройство слежения функции MLD может выбрать оптимальный путь для передачи многоадресных пакетов на втором уровне; однако оно не может изменять такие пакеты или генерировать собственные MLD-сообщения.

Прокси функции MLD представляет собой устройство, которое передает отчеты о членстве в восходящем направлении к источнику в другой подсети.

В нисходящем направлении MLD-прокси переадресовывает многоадресные пакеты и запросы для одной или нескольких IP-подсетей.

12.3.1 Подраздел MLD Setting

Сетевая страница настройки параметров функции MLD показана на рисунке 12.12.

Чтобы настроить функцию MLD на устройстве, пользователь должен сначала настроить параметры VLAN во втором окне под заголовком MLD VLAN Setting.

Порядок настройки параметров VLAN в окне MLD VLAN Setting: сначала выберите идентификатор VLAN из раскрывающегося списка.

Соответствующая VLAN будет настроена для поддержки функции отслеживания MLD. Во-вторых, пользователь может активировать или отключить опцию Fast Done для функции отслеживания MLD, установив флажок в соответствующем поле.

Эта опция позволит отменять членство многоадресного прослушивателя сразу же после приема сообщения MLD Done коммутатором.

В-третьих, функцию отслеживания MLD можно активировать или отключить для выбранной VLAN, соответственно установив или сняв флажок в поле Snooping.

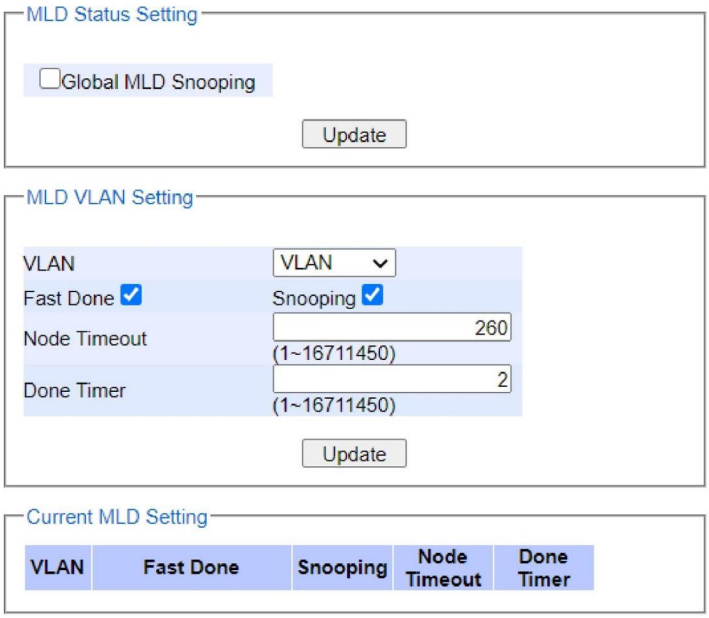


Рисунок 12.12. Настройка параметров функции MLD.

В-четвертых, пользователь может указать время, по истечении которого узел, подключенный к порту, не будет рассматриваться в качестве многоадресного прослушивателя. Соответствующий столбец в таблице называется Node Timeout.

Значение времени ожидания узла по умолчанию составляет 260 секунд.

В-пятых, пользователь может указать время, в течение которого группа многоадресной передачи будет храниться в памяти коммутатора после приема коммутатором от группы многоадресной передачи сообщения Done без отчета о прослушивании узлов. Соответствующий столбец в таблице называется Done Timer. Значение Done Timer по умолчанию составляет 2 секунды. И, наконец, щелкнув с указателем на кнопке Update, пользователь может обновить конфигурацию функции MLD для выбранного идентификатора VLAN.

Запись настроенной VLAN должна появиться в следующей части сетевой страницы.

Завершив настройку параметров VLAN согласно приведенному выше описанию, пользователь может активировать опцию Global MLD Snooping в окне MLD Status Setting.

Затем щелкните с указателем на кнопке Update, чтобы активировать функцию MLD на устройстве.

Следует отметить, что функция MLD Snooping играет ключевую роль в аспекте оптимизации потоков многоадресного трафика в сети второго уровня с использованием управляемого коммутатора.

Если не настроена ни одна VLAN с поддержкой функции MLD, система выдаст сообщение об ошибке, показанное на рисунке 12.13.

Рисунок 12.13. Сообщение об ошибке: для функции MLD не настроена ни одна виртуальная сеть.

Существующие VLAN, настроенные для поддержки функции MLD, перечислены в последней части сетевой страницы в окне под заголовком Current MLD Setting.

Все настроенные параметры представлены в форме таблицы и привязаны к определенному идентификатору VLAN.

Чтобы удалить любую запись, пользователь может щелкнуть с указателем на кнопке Delete в поле соответствующей записи.

12.3.2 Подраздел MLD IPv6 Multicast Table

На этой сетевой странице представлена информация о таблице многоадресной Ipv6-рассылки и таблице членства функции MLD.

На рисунке 12.14 показана сетевая страница таблицы многоадресной Ipv6-рассылки по протоколу MLD.

Внутри окна находится таблица членства MLD, которая содержит записи о членах, поддерживающих протокол MLD. Каждая запись состоит из полей Port Listener, VID, Multicast group, MAC address, Reports и Life Time.

В столбце Multicast показаны IPv6-адреса групп многоадресной передачи.

В столбце MAC address в каждой записи выводится MAC-адрес соответствующей группы многоадресной передачи.

В столбце Reports отображается число групповых отчетов для соответствующей группы многоадресной передачи.

В столбце Port Listener каждой записи указывается соответствующий номер порта для прослушивания. Чтобы получить обновленные данные в каждой упомянутой таблице, щелкните с указателем на кнопке Refresh.

Чтобы получить обновленные данные в каждой упомянутой таблице, щелкните с указателем на кнопке Refresh.

Рисунок 12.14. Таблица многоадресной IPv6-рассылки функции MLD.

12.3.3 Подраздел MLD Statistics

На данной сетевой странице, показанной на рисунке 12.15 представлена статистическая информация о функции MLD, которая в основном подобна статистике протокола IGMP. Пользователь может проверить число MLD-пакетов различных категорий: Rx Total, Rx Valid, Rx Invalid, Rx General Queries, Tx General Queries, Rx Group-Specific Queries, Tx Group-Specific Queries, Rx Leaves, Tx Leaves, Rx Reports, Tx Reports и Rx Others.

Пользователь может обнулить данные во всех категориях одновременно, щелкнув с указателем

на кнопке Clear.

Описание статистических параметров протокола IGMP в сводном виде представлено в таблице 12.3.

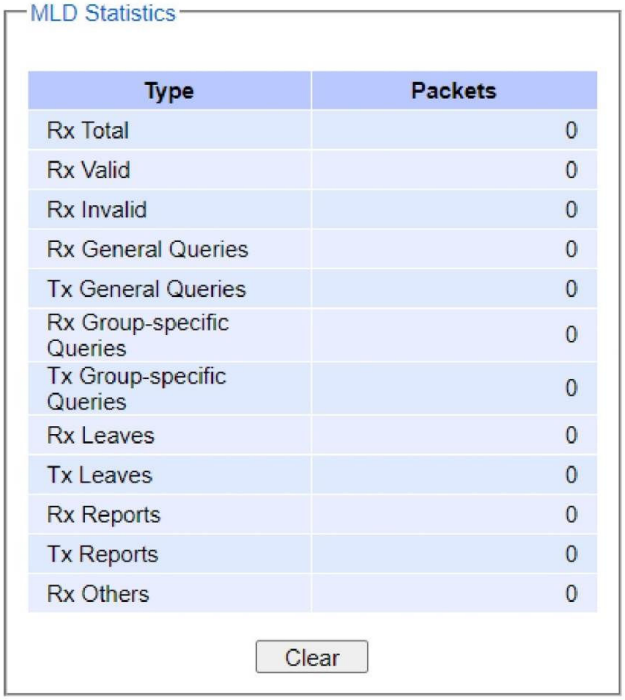


Рисунок 12.15. Статистика функции MLD.

Таблица 12.3. Описание статистических параметров функции MLD.

Имя статистического параметра	Описание
Rx Total	Общее количество MLD-пакетов, принятых управляемым коммутатором.
Rx Valid	Количество действительных MLD-пакетов, принятых управляемым коммутатором.
Rx Invalid	Количество недействительных MLD-пакетов, принятых управляемым коммутатором.
Rx General Queries	Количество MLD-пакетов с общим запросом членства, принятых управляемым коммутатором.
Tx General Queries	Количество MLD-пакетов с общим запросом членства, переданных управляемым коммутатором.
Rx Group Specific Queries	Количество MLD-пакетов с запросом членства в определенной группе, принятых управляемым коммутатором.
Tx Group Specific Queries	Количество MLD-пакетов с запросом членства в определенной группе, переданных управляемым коммутатором.
Rx Leaves	Количество MLD-пакетов с уведомлением о выходе из группы, принятых управляемым коммутатором.
Tx Leaves	Количество MLD-пакетов с уведомлением о выходе из группы, переданных управляемым коммутатором.
Rx Reports	Количество MLD-пакетов с отчетом о членстве, принятых управляемым коммутатором.
Tx Reports	Количество MLD-пакетов с отчетом о членстве, переданных управляемым коммутатором.
Rx Others	Количество прочих MLD-пакетов, принятых управляемым коммутатором.

13 РАЗДЕЛ SNMP

Простой протокол управления сетью (SNMP) используется для управления устройствами в IP-сетях. В управляемых системах он представляет данные управления в форме переменных, которые описывают конфигурацию системы.

Эти переменные затем могут быть запрошены или определены пользователями.

Протокол SNMP используется системой управления сетью или сторонним программным обеспечением, чтобы контролировать устройства в сети, такие как управляемые коммутаторы, получать информацию о состоянии сети и настраивать параметры сети.

Управляемые коммутаторы Yarus Networks поддерживают протокол SNMP, параметры которого можно настроить в рассматриваемом разделе меню.

Раскрывающееся меню подраздела показано на рисунке 13.1. Настраиваемые параметры протокола SNMP делятся на следующие четыре группы:

- SNMP Agent
- SNMP V1/V2c Community Setting
- Trap Setting
- SNMP V3 Auth Setting
- Trap Event Settings

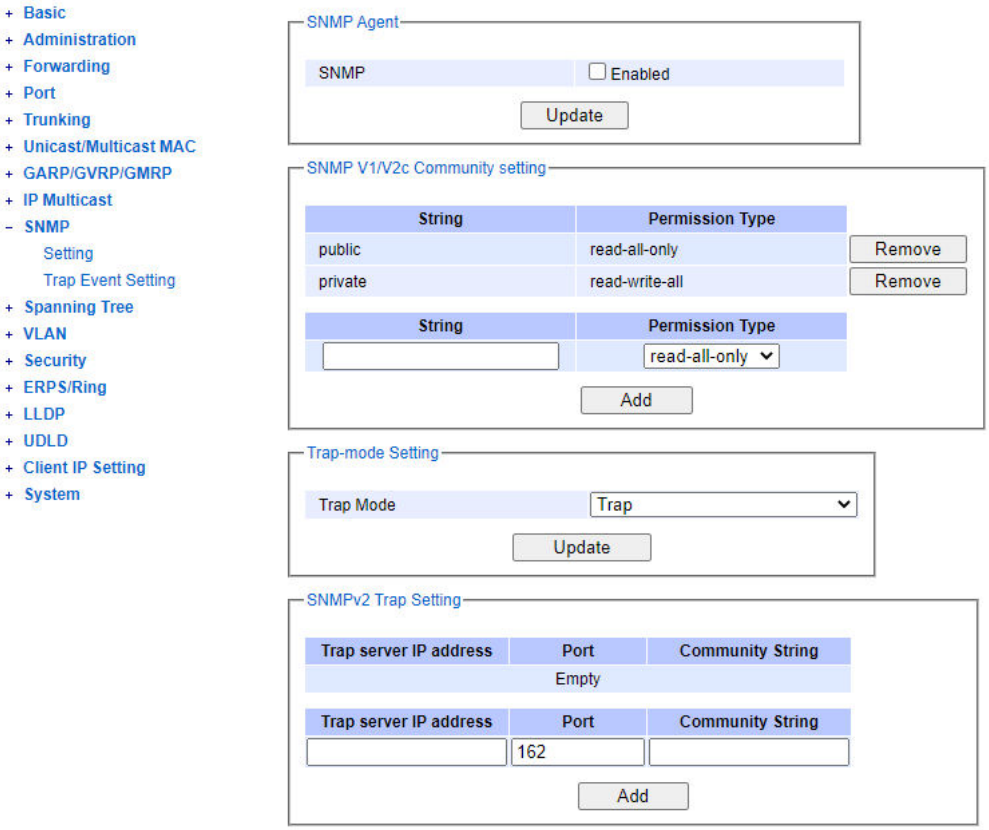


Рисунок 13.1. Раскрывающееся меню раздела SNMP.

13.1 Подраздел SNMP Agent

Чтобы активировать SNMP-агента на управляемом коммутаторе установите флажок в поле Enable и щелкните с указателем на кнопке Update, как показано на рисунке 13.2.

Управляемые коммутаторы Yarus Networks поддерживают версии 1 (V1), 2c (V2c) и 3 протокола SNMP. Соответствующие данные в сводном виде представлены в таблице 13.1. В основе своей протоколы SNMP V1 и SNMP V2c построены на защитном механизме, который использует простой протокол проверки подлинности по имени и паролю, в то время как протокол SNMP V3 отличается повышенной криптографической безопасностью.

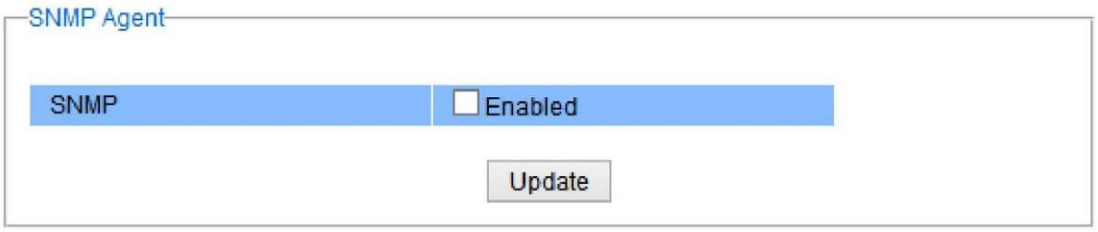


Рисунок 13.2. Окно активации протокола SNMP.

Таблица 13.1. Описание настраиваемых параметров протокола SNMP.

Имя параметра	Описание	Заводская настройка по умолчанию
SNMP	Установите флажок в данном поле, чтобы активировать протокол SNMP V1/V2c/V3.	Выключено

13.2 Подраздел SNMP V1/V2c Community Setting

Данный управляемый коммутатор поддерживает версии V1, V2c и V3 протокола SNMP. В версиях V1 и V2c протокола SNMP для проверки подлинности используется строка доступа. После успешной проверки подлинности программное обеспечение управления сетью получает доступ к информации или объектам данных, описанных в базах управляющей информации, хранящимся в памяти управляемого коммутатора.

Следует отметить, что столь простая проверка подлинности сейчас считается слабым защитным механизмом.

Поэтому рекомендуется по возможности использовать версию V3 протокола SNMP. Устройства поддерживают два уровня проверки подлинности или типа полномочий - read-all-only или read-write-all.

Например, при настройках по умолчанию, показанных на рисунке 13.3, агент SNMP, который является программным модулем управления сетью, установленным на управляемом коммутаторе, может получать ко всем объектам доступ с полномочиями "только для чтения", используя строку public.

В другом варианте настройки с использованием строки private предоставляется доступ с полномочиями "для чтения и записи".

В окне SNMP V1/V2c Community Setting пользователь может создать новую строку доступа

для проверки подлинности или удалить существующую строку из списка, щелкнув с указателем на кнопке Remove в конце соответствующей записи со строкой доступа. Пользователь может указать имя строки в поле String и выбрать тип полномочий из выпадающего списка, как показано на рисунке 13.3.

Описание настраиваемых параметров строки доступа протокола SNMP приведено в таблице 13.2.

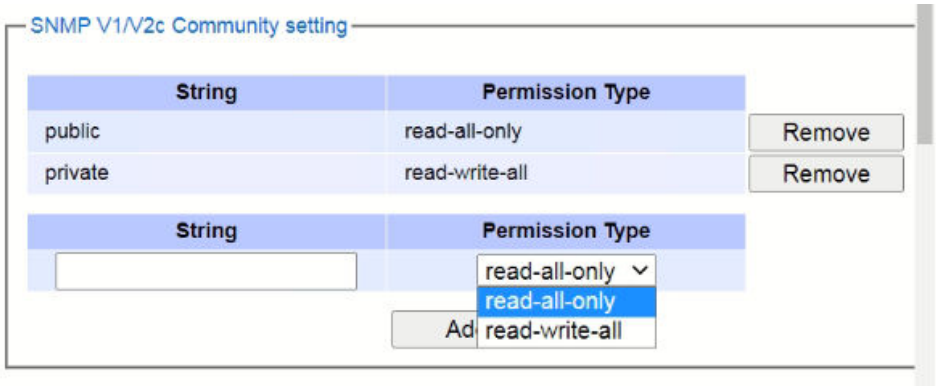


Рисунок 13.3. Строки доступа протокола SNMP.

Таблица 13.2. Описание настраиваемых параметров строки доступа.

Имя параметра	Описание	Заводская настройка по умолчанию
(Community) Strings	В данном поле указывается имя строки для проверки подлинности. Длина имени не может превышать 15 символов.	Public (read-all-only) Private (read-write-all)
Permission Type	В данном поле можно выбрать тип из выпадающего списка: read-all-only или read-write-all. Описание значений приведено в примечаниях ниже.	

*** ПРИМЕЧАНИЕ:**

Read-all-only: Разрешение на чтение поддерева с идентификатором объекта 1.

Read-write-all: Разрешение на чтение и запись поддерева с идентификатором объекта 1.

13.3 Подраздел Trap Setting

13.3.1 SNMP Trap Setting

Управляемый коммутатор поддерживает функцию прерывания, посредством которой он передает агентам уведомления с прерываниями SNMP или запросы. Уведомление передается в случае изменения состояния коммутатора. Такие изменения могут включать подключение канала, отключение канала, горячий старт или холодный старт.

В режиме информирования, если коммутатор, передав SNMP-запрос на получение информации, не примет ответ в течение 10 секунд, он отправит запрос информации повторно. Коммутатор повторит передачу три раза.

13.3.2 SNMPv2 Trap

В подразделе SNMP Trap Setting пользователь может настраивать параметры прерываний протокола SNMP, задавая IP-адрес назначения сервера прерываний, номер порта сервера прерываний, а также создавая строку доступа для проверки подлинности. В таблице 13.3 приведено описание параметров, настраиваемых в разделе Trap Setting.

В первой строке Trap Mode пользователь может выбрать режим прерываний, который может быть Trap или Inform.

После выбора требуемого режима прерываний щелкните с указателем на кнопке Update. Заполните все обязательные поля в последней строке в окне Trap Setting и щелкните с указателем на кнопке Add.

Описание настраиваемых параметров приемника прерываний в сводном виде представлено в таблице 13.3.

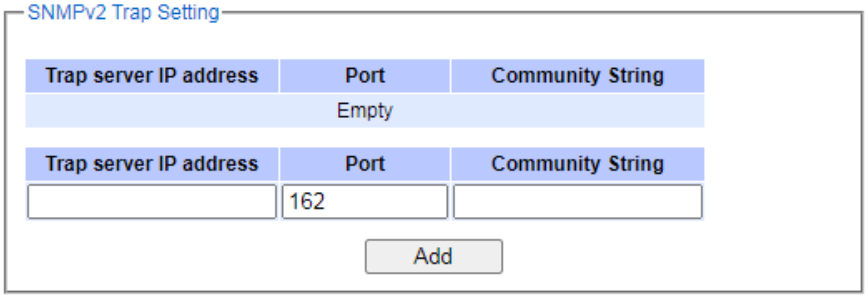


Рисунок 13.4. Пример настройки параметров приемника прерываний.

Таблица 13.3. Описание настраиваемых параметров приемника прерываний.

Имя параметра	Описание	Заводская настройка по умолчанию
Trap Mode	Выберите режим - Trap или Inform.	Trap
Trap server IP address	Введите IP-адрес своего сервера прерываний.	Не заполняется
Port	Укажите номер порта для сервера прерываний.	162
Community String	Введите строку доступа для проверки подлинности. Длина строки не может превышать 15 символов.	Не заполняется

13.3.3 SNMPv3 Trap

SNMPv3 использует модель безопасности на основе пользователя (USM) для защиты сообщений и модель управления доступом на основе представления (VACM) для контроля доступа.

Модель безопасности SNMPv3 содержит аутентификацию и шифрование:

a. Аутентификация используется для гарантии того, что ловушки будут прочитаны конкретным получателем. Специальный ключ является общим для конкретного получателя и используется для получения сообщения.

b. Полезная нагрузка SNMP-сообщения будет зашифрована, чтобы гарантировать, что оно не

может быть прочитано неавторизованным пользователем.

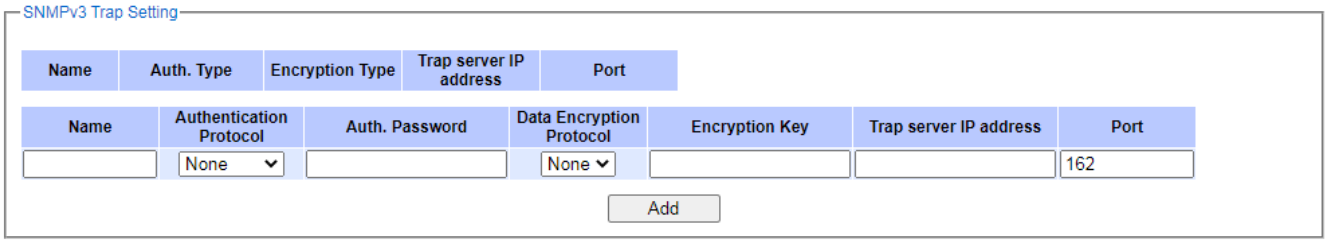


Рисунок 13.5. Окно раздела SNMPv3 Trap Settings

Таблица 13.4. Описание настраиваемых параметров SNMPv3 Trap Settings.

Имя параметра	Описание	Заводская настройка по умолчанию
Name	Имя пользователя для проверки подлинности SNMPv3 trap	Не заполняется
Authentication Protocol	Выберите параметры протокола проверки подлинности SNMPv3 trap, коммутатор поддерживает указанные ниже тип протокола: Без шифрования (None) MD5 SHA SHA-256	Без шифрования (None)
Auth. Password	Настройка пароля для проверки подлинности SNMPv3 trap	Не заполняется
Data Encryption Protocol	Настройте протокол шифрования данных SNMPv3 trap, поддерживаемый управляемым коммутатором приведенного ниже типа: Без шифрования (None) DES AES	Без шифрования (None)
Encryption Key	Настройка ключа шифрования SNMPv3 trap	Не заполняется
Trap server IP address	Настройка ip-адреса сервера SNMPv3 trap	Не заполняется
Port	Настройка номера UDP-порта SNMPv3 trap	162

13.4 Подраздел SNMPv3 Auth Setting

Как уже упоминалось выше, версия V3 протокола SNMP отличается более высокой безопасностью. В данном подразделе пользователь может настроить пароль и ключ шифрования, чтобы обеспечить надежную защиту данных. Используя этот подраздел меню, пользователь может настраивать параметры проверки подлинности и шифрования для протокола SNMP V3.

Для пароля подтверждения подлинности используется алгоритм MD5 (алгоритм выборки сообщений 5), а алгоритм шифрования данных соответствует стандарту DES (стандарт шифрования данных).

На рисунке 13.6 показана сетевая страница настройки параметров проверки подлинности для протокола SNMP версии V3. В верхней таблице пользователь может просматривать параметры существующих пользователей протокола SNMP V3.

В таблице содержится информация об имени пользователя, типе проверки подлинности и стандарте шифрования данных.

Пользователь может на собственное усмотрение удалять существующих пользователей протокола SNMP V3. Для этого достаточно щелкнуть с указателем на кнопке Remove в последнем столбце соответствующей записи.

Чтобы добавить нового пользователя протокола SNMP V3, нужно выбрать имя пользователя из выпадающего списка - Admin или User. Затем введите пароль подтверждения подлинности (максимальная длина - 31 символ) в поле Auth Password, после чего повторно введите тот же пароль в поле Confirmed Password.

ПРИМЕЧАНИЕ: пароль является обязательным атрибутом, без пароля проверка подлинности по протоколу SNMP V3 невозможна.

Далее введите ключ шифрования (максимальная длина - 31 символ) в поле Encryption Key, после чего повторно введите тот же ключ в поле Confirmed Key.

Заполнив все обязательные поля, щелкните с указателем на кнопке Add, чтобы обновить информацию в памяти управляемого коммутатора.

Описание настраиваемых параметров протокола SNMP V3 в сводном виде представлено в таблице 13.5.

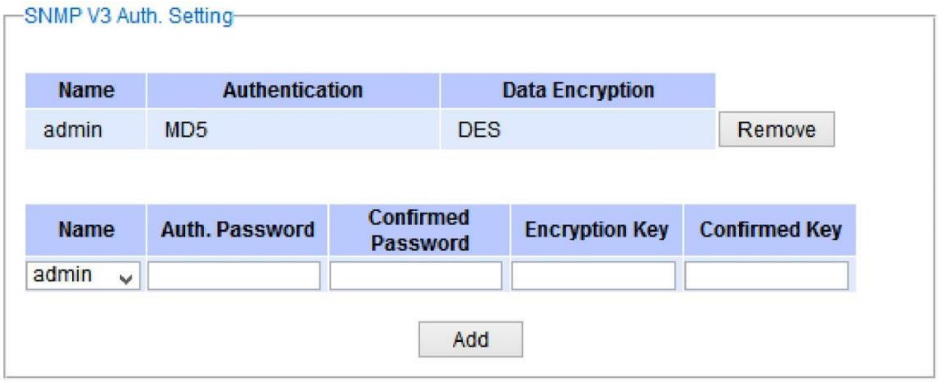


Рисунок 13.6. Настраиваемые параметры пользователя протокола SNMPv3.

Таблица 13.5. Описание настраиваемых параметров протокола SNMP V3.

Имя параметра	Описание	Заводская настройка по умолчанию
Name	Можно выбрать один из следующих вариантов: Admin: с полномочиями администратора. User: с полномочиями обычного пользователя.	Admin
Authentication Protocol	Выберите тип procotol для проверки подлинности пользователя, управляемый коммутатор поддерживает следующие типы протоколов: Без шифрования (None) MD5 SHA SHA-256	Без шифрования (None)

Имя параметра	Описание	Заводская настройка по умолчанию
Auth. Password	В этом поле вводится пароль подтверждения подлинности для имени пользователя, выбранного в предыдущем поле. Если поле оставить незаполненным, проверка подлинности будет невозможна. **Примечание:** пароль подтверждения подлинности основан на алгоритме MD5. Максимальная длина - 31 символ.	Не заполняется
Confirmed Password	Введите пароль подтверждения подлинности повторно для подтверждения.	Не заполняется
Encryption Key	В этом поле вводится ключ шифрования для более надежной защиты передачи данных по протоколу SNMP. **Примечание:** в качестве алгоритма шифрования используется стандартный алгоритм DES. Максимальная длина - 31 символ.	Не заполняется
Confirmed Key	Введите тот же ключ шифрования повторно.	Не заполняется

13.5 Trap Event Setting

В меню Trap Event Settings управляемый коммутатор позволяет осуществлять настройку события trap, что дает возможность пользователю управлять тем, какое событие будет отправлять сообщение trap. События SNMP Trap имеют следующие параметры сообщений для выбора пользователем; “WarmStart”, “coldStart”, “AuthenticationFailure”, “LinkUp”, “linkDown”.

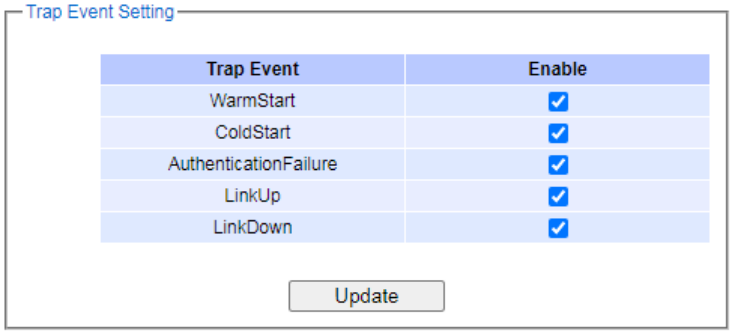


Рисунок 13.7 Окно настройки Trap Event Setting.

14 РАЗДЕЛ SPANNING TREE

Управляемые коммутаторы Yarus Networks поддерживают функциональность связующего дерева согласно стандарту IEEE 802.1D.

Основными задачами протокола связующего дерева (STP) являются предотвращение зацикливания при коммутации и распространения широковещательной рассылки на втором уровне взаимодействия открытых систем.

Управляемыми коммутаторами Yarus Networks также поддерживается протокол RSTP (протокол высокоскоростного связующего дерева), соответствующий спецификации IEEE 802.1W. Он представляет собой усовершенствованный протокол STP, обратно совместимый с исходным протоколом.

Протокол RSTP имеет целый ряд преимуществ по сравнению с протоколом STP. Если происходит изменение в топологии сети, например, сбой канала, протокол RSTP значительно быстрее выполняет перестройку топологии связующего дерева.

Протокол RSTP обеспечивает более эффективную конвергенцию двухточечных каналов, благодаря сокращению максимального срока жизни до значения, равного трем интервалам передачи пакетов приветствия, отказу от состояния прослушивания, присущего протоколу STP, и обмену пакетами квитирования между двумя коммутаторами, чтобы быстро перевести порт в состояние переадресации.

Протокол MSTP (протокол множественных связующих деревьев) также представляет собой стандартный протокол, описанный в спецификации IEEE 802.1s. Этот протокол позволяет привязывать несколько VLAN к одному экземпляру множественного связующего дерева, которое поддерживает множественные пути в сети.

Этот протокол совместим с протоколами STP и RSTP. В больших сетях протокол MSTP объединяет мосты/коммутаторы в регионы.

Другие устройства видят каждый регион, как один мост. В каждом регионе может быть несколько экземпляров множественного связующего дерева.

Протокол MSTP использует общие параметры с протоколом RSTP, например, стоимость пути для порта. Протокол MSTP также способствует предотвращению петель коммутации и быстро перестраивает дерево при обнаружении изменений в топологии.

Для различных экземпляров множественного связующего дерева могут быть созданы различные пути переадресации. Это позволяет сбалансировать нагрузку по сетевому трафику в избыточных каналах.

В данном разделе описывается порядок настройки параметров протокола связующего дерева (STP), протокола высокоскоростного связующего дерева (RSTP) и протокол множественных связующих деревьев (MSTP). На рисунке 14.1 показано раскрывающееся меню раздела Spanning Tree.

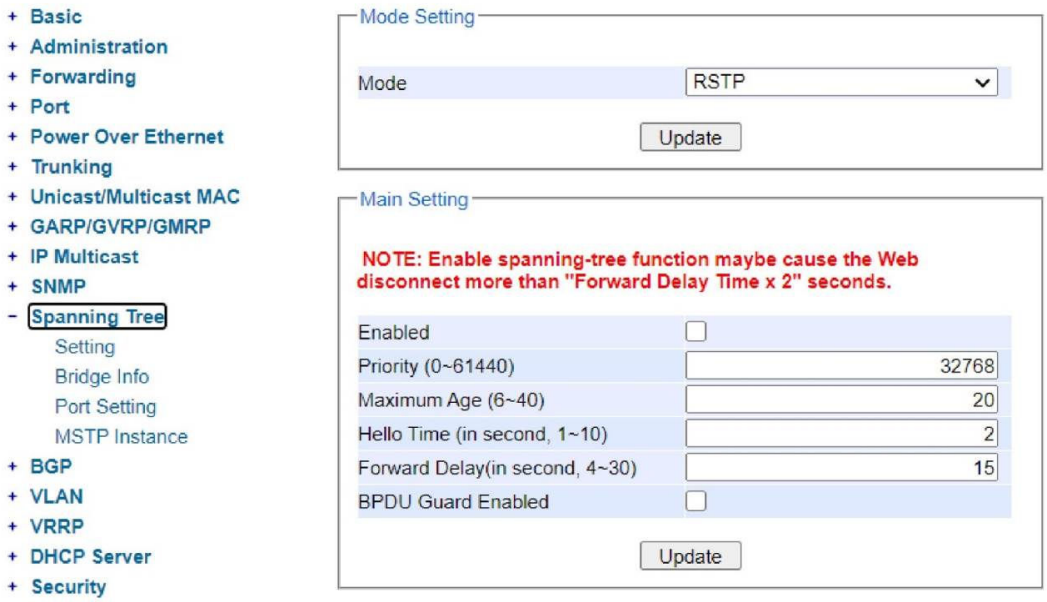


Рисунок 14.1. Раскрывающееся меню раздела Spanning Tree.

14.1 Подраздел Spanning Tree Setting

На этой сетевой странице пользователь может выбрать режим, то есть - используемый протокол связующего дерева. На рисунке 14.2 показано окно выбора режима связующего дерева. В раскрывающемся меню можно выбрать один из трех режимов: протокол связующего дерева (STP), протокол высокоскоростного связующего дерева (RSTP) и протокол множественных связующих деревьев (MSTP). Выбрав требуемый режим, щелкните с указателем на кнопке Update, чтобы изменения вступили в силу.

Рисунок 14.2. Выбор режима связующего дерева.

Под окном выбора режима распложено окно Main Setting для настройки глобальных параметров связующего дерева. Упомянутое окно показано на рисунке 14.3. В окне Main Setting пользователь может активировать или отключить протокол связующего дерева, соответственно установив или сняв флажок в поле Enabled. Для точной настройки пользователь должен заполнить поля Priority, Maximum Age, Hello Time и Forward Delay. Также можно активировать функцию BPDU Guard Enabled. Завершив настройку глобальных параметров связующего дерева, щелкните с указателем на кнопке Update, чтобы изменения вступили в силу. Описание каждого настраиваемого параметра приведено в таблице 14.1.

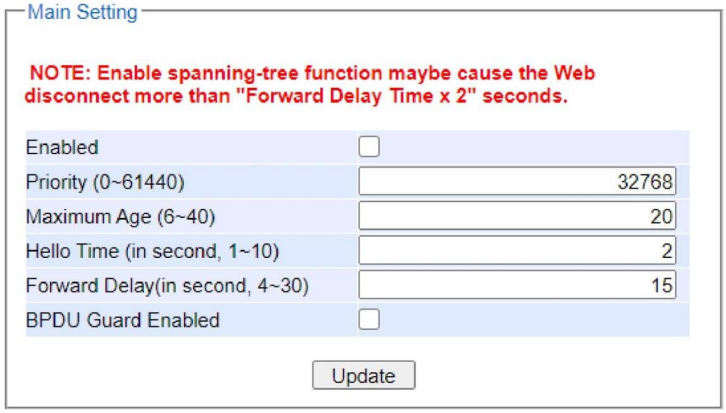


Рисунок 14.3. Настройка глобальных параметров связующего дерева в режимах STP и RSTP.

Если пользователь выберет в качестве режима связующего дерева протокол MSTP и щелкнет указателем на кнопке Update в окне Mode Setting, показанном на рисунке 14.3, окно Main Setting изменится и примет вид, показанный на рисунке 14.4. Как можно заметить, поле Priority исчезло, зато появились три новых поля: Max Hops, Revision Level и Region Name. Помимо того, в окне настройки параметров отдельных портов под названием Per-port Setting будет выведено уведомление о том, что выбран режим протокола MSTP, который не поддерживает агрегацию портов.

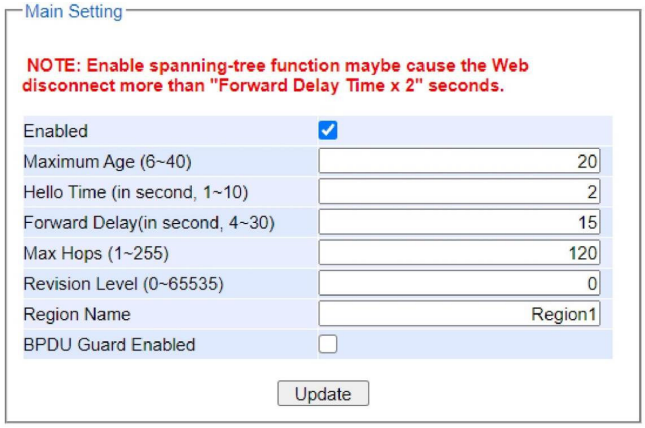


Рисунок 14.4. Настройка глобальных параметров связующего дерева для протокола MSTP.

Таблица 14.1. Описание настраиваемых параметров связующего дерева.

Имя параметра	Описание	Заводская настройка по умолчанию
Enabled	Установите флажок, чтобы активировать функциональность связующего дерева.	Выключено
Priority	Введите число, определяющее приоритет устройства. Данный параметр может принимать значение в диапазоне от 0 до 61440. Чем меньше число, тем выше приоритет.	32768
Maximum Age	Максимальное ожидаемое время поступления приветственного сообщения. Значение, указанное в этом поле, должно больше значения в поле Hello Time.	20

Имя параметра	Описание	Заводская настройка по умолчанию
Hello Time	В этом поле указывается длина интервала передачи сообщений приветствия в секундах. Данный параметр может принимать значение в диапазоне от 1 до 10.	2
Forward Delay	Укажите время в состоянии прослушивания и распознавания в секундах. Данный параметр может принимать значение в диапазоне от 4 до 30.	15
Max Hops (только для протокола MSTP)	Данный параметр может принимать значение в диапазоне от 1 до 255.	120
Revision Level (только для протокола MSTP)	Данный параметр может принимать значение в диапазоне от 0 до 65535.	0
Region Name (только для протокола MSTP)	В данном поле вводится текстовая строка с именем региона.	Region1
BPDU Guard Enabled	Установите флажок в данном поле, чтобы активировать функцию BPDU Guard для защиты протокольных данных.	Выключено

В нижней части подраздела Spanning Tree Setting расположено окно настройки параметров для отдельных портов, которое показано на рисунке 14.5.

Пользователь может активировать функциональность связующего дерева на отдельных портах или на всех портах одновременно, установив флажки в соответствующих полях в столбце Port Enable.

По умолчанию функция активируется на всех портах.

После внесения изменений в окне настройки параметров для отдельных портов щелкните с указателем на кнопке Update, чтобы изменения вступили в силу на управляемом коммутаторе.

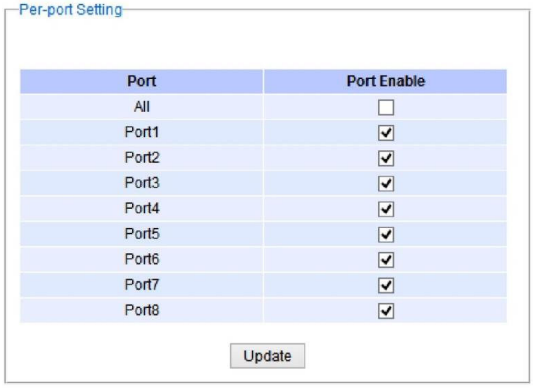


Рисунок 14.5. Настройка параметров связующего дерева в режимах STP и RSTP для отдельных портов.

14.2 Подраздел Bridge Info

В подразделе Bridge Info, который показан на рисунке 14.6, приведены значения статистики протокола связующего дерева.

Информация в окне разделена на две части: Root Information и Topology Information. Чтобы получить обновленную информацию, щелкните с указателем на кнопке Refresh.

В таблицах 14.2 и 14.3 в сводном виде представлено описание значений в таблице с данными о корне и в таблице с данными о топологии соответственно.

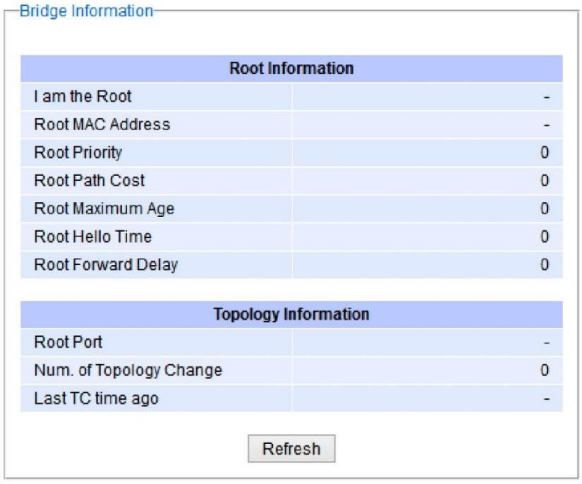


Рисунок 14.6. Сетевая страница Bridge Information.

Таблица 14.2. Таблица Root Information.

Имя параметра	Описание	Заводская настройка по умолчанию
I am the Root	В данном поле указывается, является ли данный коммутатор выбранным корневым коммутатором в топологии связующего дерева.	-
Root MAC Address	MAC-адрес корня связующего дерева.	-
Root Priority	Значение приоритета корня: чем ниже значение, тем выше приоритет. Коммутатор с наименьшим значением получает наивысший приоритет и выбирается корнем связующего дерева.	0
Root Path Cost	Стоимость пути для корня зависит от скорости передачи данных через соответствующий порт коммутатора.	0
Root Maximum Age	Максимальное время жизни корня – это максимальное время, в течение которого коммутатор поддерживает протокольную информацию, принятую в канале.	0
Root Hello Time	Длина интервала передачи сообщений приветствия корнем – это продолжительность интервала между приветственными сообщениями, передаваемыми протоколом RSTP на соседние узлы с целью обнаружения изменений в топологии.	0
Root Forward Delay	Задержка переадресации корнем – это период времени, в течение которого коммутатор находится в состоянии распознавания и прослушивания до начала передачи данных по каналу.	0

Таблица 14.3. Таблица Topology Information.

Имя параметра	Описание	Заводская настройка по умолчанию
Root Port	Порт переадресации, который является лучшим портом для передачи от некорневого моста/коммутатора на корневой мост / коммутатор. Следует отметить, что корневой порт не может быть назначен для корневого коммутатора.	
Num. of Topology Change	Общее количество изменений в топологии со времени последнего обнуления.	0
Last TC time ago	Продолжительность времени, прошедшего с момента последнего изменения топологии связующего дерева.	-

14.3 Подраздел Port Setting

В подразделе Port Setting раздела Spanning Tree отображаются значения параметров протокола связующего дерева, настроенные для каждого порта, как показано на рисунке 14.7. Информация о настроенных параметрах каждого порта включает разделы State, Role, Path Cost, Priority, Link Type, Edge, BPDU Guard, Cost и Designated.

Чтобы получить обновленные статистические данные на этой странице, щелкните с указателем на кнопке Refresh.

В таблице 14.4 в сводном виде представлено описание параметров связующего дерева на отдельных портах после активации протокола MSTP. Обратите внимание, что после активации протокола STP или RSTP в верхней части таблицы не выводится поле Instance ID.

После активации связующего дерева таблица, показанная на рисунке ниже, становится доступной для редактирования.

Щелкните с указателем на кнопке Update, чтобы сохранить настройки.

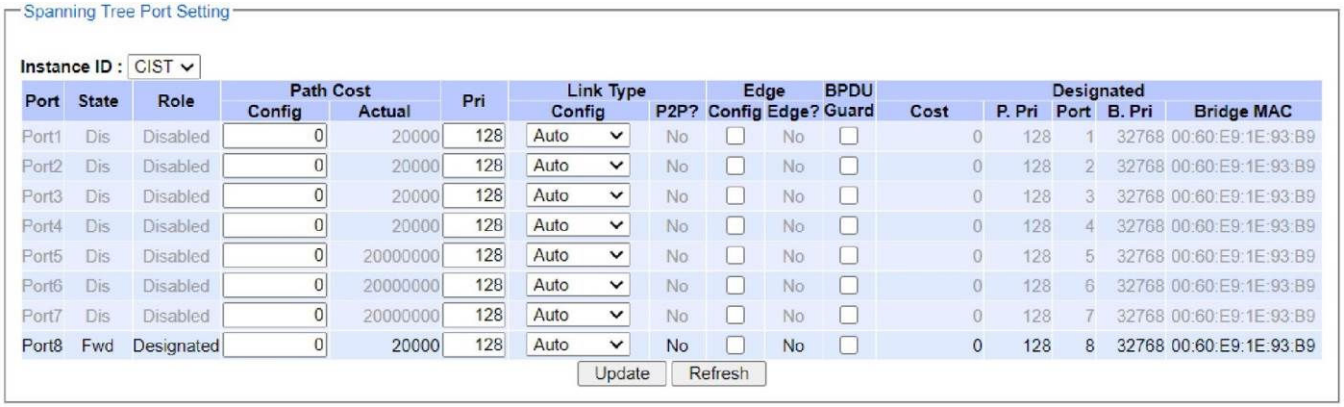


Рисунок 14.7. Сетевая страница настройки параметров портов для связующего дерева.

Таблица 14.4. Описание настраиваемых параметров портов для связующего дерева.

Имя параметра		Описание	Заводская настройка по умолчанию
Port		В данном поле указывается имя порта коммутатора.	-
State		Состояние порта: 'Disc': отбрасывание - через данный порт не передаются никакие пользовательские данные. 'Lrn': распознавание - порт еще не передает кадры данных, но уже заполняет свою таблицу MAC-адресов. 'Fwd': переадресация - порт является полностью функциональным.	Не применяется
Role		Поддерживается или не поддерживается протокол STP. Роли для портов моста с поддержкой протокола RSTP: 'Root': порт переадресации, который является лучшим портом для передачи от некорневого моста на корневой мост. 'Designated': порт переадресации для всех сегментов локальной сети. 'Alternate': альтернативный путь до корневого моста. Этот путь отличается от пути, который использует корневой порт. 'Backup': резервный/избыточный путь до сегмента, с которым уже соединен другой порт моста. 'Disabled': следует отменить, что эта роль не определяется протоколом STP – порт может быть отключен сетевым администратором вручную.	Протокол STP не поддерживается
Path Cost		Настройка стоимости пути для каждого порта коммутатора.	
	Config	Настройка стоимости внутреннего пути (значение по умолчанию: 0 - означает, что, используется системное значение по умолчанию (в зависимости от скорости канала)).	0
	Actual	Фактическое значение стоимости пути (для протокола STP и RSTP, см. примечание 1 ниже и таблицу 2 - 42).	0
Pri		Значение приоритета порта, используется в поле идентификатора порта в пакете с блоками данных BPDU, значение = 16 x N (N: 0 ~ 15) См. примечание 2 ниже.	128
Link Type		Соединение между несколькими переключателями (для протокола RSTP).	
	Config	Настройка типа канала. P2P: Порт работает в полнодуплексном режиме и, как предполагается, является портом двухточечного канала.	Auto

Имя параметра		Описание	Заводская настройка по умолчанию
		Non-P2P: Полудуплексный порт (работает через концентратор). Auto: Тип канала определяется автоматически.	
	P2P?	Yes: Этот порт поддерживает двухточечное соединение. No: Этот порт не поддерживает двухточечное соединение.	No
Edge		Граничный порт – это порт, к которому не подключен никакой другой коммутатор, использующий протокол STP/RSTP (для протокола RSTP). Граничный порт может быть непосредственно переведен в состояние переадресации.	
	Config	Настроена ли функция граничного порта: Yes или No.	No
	Edge?	Yes: Данный порт является граничным портом. No: Данный порт не является граничным портом.	No
Designated		Здесь отображается определенная информация для оптимального пакета с блоками данных BPDU, передаваемого через данный порт.	
	Cost	Стоимость корневого пути.	0
	P. Pri. (приоритет порта)	Приоритет порта (4 верхних бита идентификатора порта), значение = 16 x N (N: 0 ~ 15)	128
	Port	Номер интерфейса (12 нижних битов идентификатора порта).	-
	Bri. Pri. (приоритет моста)	Приоритет моста, значение = 4096 x N (N: 0 ~ 15)	32768
	Bridge MAC	MAC-адрес коммутатора, который передал обрабатываемый блок данных BPDU.	-

ПРИМЕЧАНИЕ:

1. В общем случае стоимость пути зависит от скорости передачи данных по каналу. Значения стоимости пути по умолчанию для протоколов STP и RSTP приведены в таблице 14.5.

Таблица 14.5. Стоимость пути по умолчанию для протоколов STP и RSTP.

Скорость передачи данных	Стоимость пути для протокола STP (802.1D - 1998)	Стоимость пути для протокола RSTP (802.1W - 2004)
4 Мбит/сек.	250	5 000 000
10 Мбит/сек.	100	2 000 000
16 Мбит/сек.	62	1 250 000
100 Мбит/сек.	19	200 000
1 Гбит/сек.	4	20 000
2 Гбит/сек.	3	10 000
10 Гбит/сек.	2	2 000

2. Последовательность событий для определения оптимального принятого блока данных

BPDU (который, в свою очередь, определяет оптимальный путь к корню).

- Корневым становится мост с наименьшим значением идентификатора корневого моста.
- По стоимости пути до корневого моста преимущество получает восходящий коммутатор с наименьшим значением стоимости пути до корня.
- Если несколько восходящих коммутаторов имеют равную стоимость пути до корня, преимущество получает мост отправителя с наименьшим значением идентификатора.
- Если коммутатор соединяется с восходящим коммутатором через несколько портов (не Ethernet), преимущество получает порт отправителя с наименьшим значением идентификатора.
- Идентификатор моста состоит из следующих элементов: значение приоритета (4 бита), локально назначенное расширение системного идентификатора (12 битов), идентификатор [MAC-адрес] (48 битов).

Значение приоритета моста по умолчанию равно 32768.

Идентификатор порта состоит из следующих элементов: значение приоритета (4 бита), значение идентификатора (номер интерфейса) (12 битов).

Значение приоритета порта по умолчанию равно 128.

14.4 Подраздел MSTP Instance

Протокол MSTP позволяет группировать VLAN и связывать их с различными экземплярами связующего дерева. Таким образом, экземпляр множественного связующего дерева (экземпляр дерева MST) представляет собой определенный набор VLAN, которые используют одно связующее дерево. Следует отметить, что экземпляр дерева MST имеет идентификационный номер, который имеет локальное значение в пределах региона MST.

На рисунке 14.8 показана сетевая страница раздела MSTP Instance.

В этом разделе пользователь может добавлять или удалять экземпляры протокола MSTP. В верхней части сетевой страницы находится таблица с данными текущего экземпляра протокола MSTP, используемого управляемым коммутатором.

Пользователь может добавить новый экземпляр протокола MSTP, выбрав идентификатор экземпляра из выпадающего списка. Затем нужно ввести идентификационный номер VLAN в поле VID и ввести значение приоритета в поле Priority.

После завершения ввода информации щелкните с указателем на кнопке Add, чтобы обновить запись с экземпляром протокола MSTP. Для настройки экземпляра протокола MSTP выполните следующую процедуру:

- Активируйте протокол MSTP.
- Внесите необходимые изменения в глобальные настройки связующего дерева.
- Выберите порты, на которых нужно активировать функции протокола MSTP.
- Добавьте экземпляр дерева MST на сетевой странице MSTP Instance (данный раздел).

Выберите идентификатор экземпляра.

Добавьте идентификационные номера VLAN, которые будут связаны с данным экземпляром протокола MSTP.

Укажите значение приоритета коммутатора.

Щелкните с указателем на кнопке Add/Modify.

Описание пунктов информации о протоколе MSTP в сводном виде представлено в таблице 14.6.

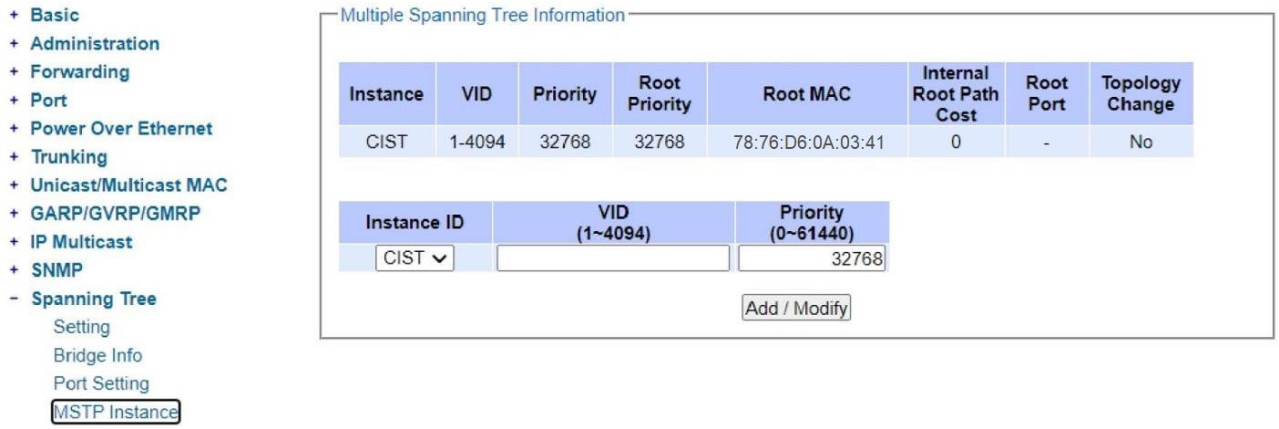


Рисунок 14.8. Сетевая страница MSTP Instance.

Таблица 14.6. Описание пунктов информации о протоколе MSTP.

Имя параметра	Описание	Заводская настройка по умолчанию
Instance ID	Выберите из выпадающего списка значение CIST (единое связующее дерево) или укажите значение от 1 до 63.	CIST
VID	Введите значение идентификатора VLAN в диапазоне от 1 до 4094.	-
Priority	Введите значение приоритета управляемого коммутатора в диапазоне от 0 до 61440. Чем меньше значение, тем выше приоритет. Если значение приоритета равно 0, данный коммутатор является корневым мостом данного экземпляра дерева MST.	32768
Root Priority	Отображается значение приоритета корня.	32768
Root MAC	Отображается MAC-адрес корневого моста.	-
Internal Root Path Cost	Отображается значение стоимости корневого пути.	0
Root Port	Отображается корневой порт.	-
Topology Change	Отображается одно из значений - Yes или No.	No

15 РАЗДЕЛ VLAN

Виртуальная локальная вычислительная сеть (VLAN) образуется группой устройств, которые могут быть расположены в любых сегментах сети. При этом все устройства в группе логически связываются друг с другом.

Другими словами, VLAN позволяет группировать оконечные станции, даже если они связаны с различными сетевыми коммутаторами.

При любых изменениях в структуре традиционной сети пользователям приходится тратить немало времени на перемещение устройств, в то время как для перенастройки VLAN не требуется вмешательство в аппаратную конфигурацию – все необходимые действия выполняются только на программном уровне.

Использование функции VLAN также обеспечивает дополнительную защиту сети, потому что устройства в группе VLAN могут связываться с другими устройствами только в той же группе.

В определенной степени и в определенных условиях технология виртуальных сетей позволяет улучшить управление сетевым трафиком.

В традиционной сети данные передаются в широковещательном режиме на все устройства, независимо от того, нужны передаваемые данные устройствам или нет.

При использовании VLAN каждый член группы, привязанной к определенной виртуальной сети, может принимать данные только от других членов той же группы.

При этом нет нужды передавать данные в широковещательном режиме, что позволяет существенно повысить эффективность информационного обмена (см. рисунок 15.1).

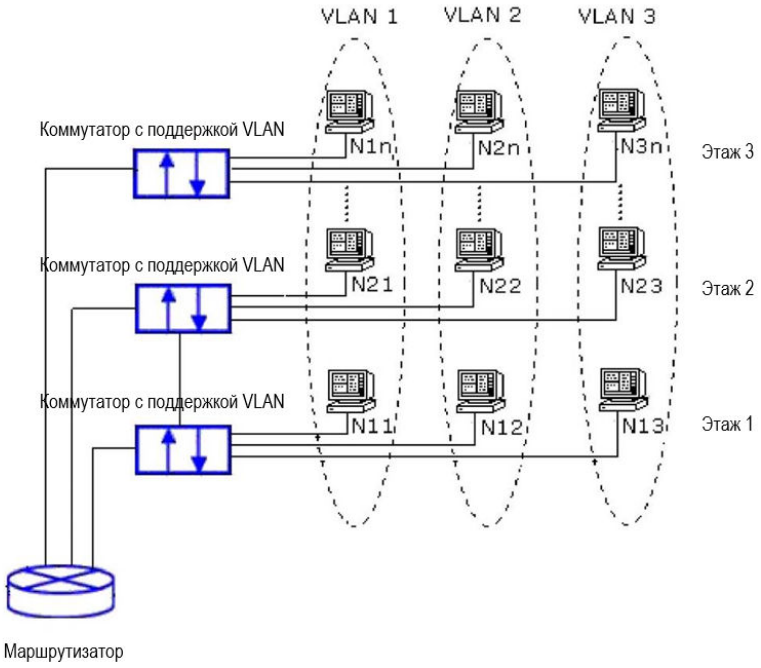


Рисунок 15.1. Пример конфигурации сети VLAN.

Управляемые коммутаторы поддерживают шесть вариантов создания VLAN, а именно:

- VLAN на основе тегов (802.1Q),

- VLAN на основе портов,
- VLAN на основе MAC-адресов,
- VLAN на основе масок IP-подсетей,
- VLAN на основе протоколов,
- QinQ или VLAN на основе двойных тегов.

На рисунке 15.2 показано раскрывающееся меню раздела VLAN.

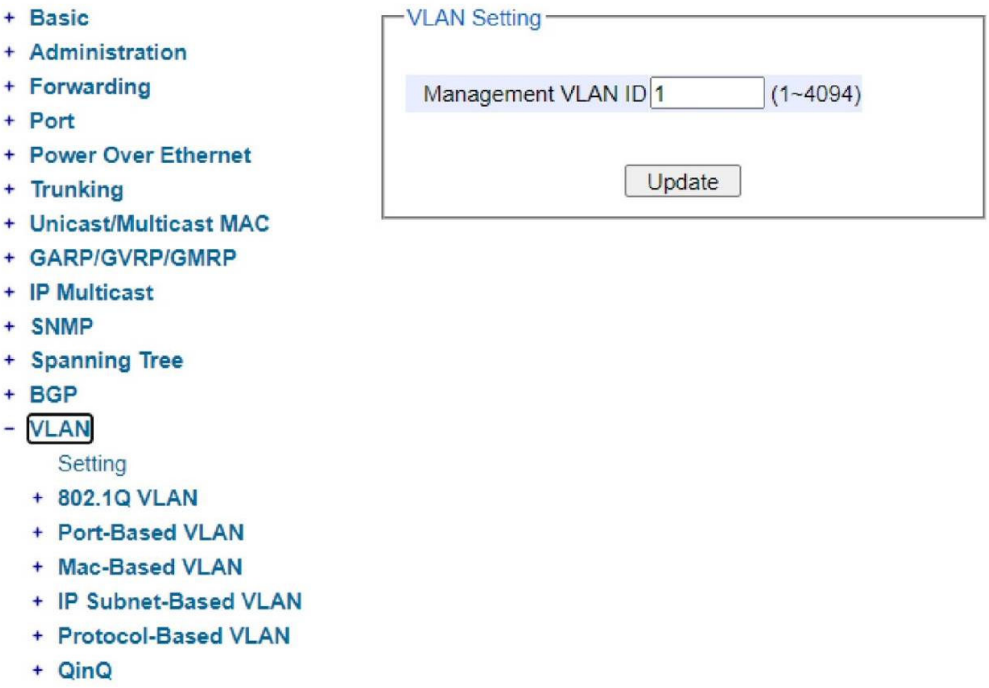


Рисунок 15.2. Раскрывающееся меню раздела VLAN.

15.1 Подраздел VLAN Setting

Первый подраздел меню VLAN называется VLAN Setting и предназначен для настройки параметров VLAN.

В поле Management VLAN Identification ID в окне этого подраздела настраивается идентификационный номер (идентификатор) VLAN на основе стандарта IEEE 802.1Q. Значение идентификатора по умолчанию равно 1.

Следует учитывать, что идентификатор может принимать значения в диапазоне от 1 до 4096. Если пользователь изменил значение идентификатора VLAN, он должен щелкнуть с указателем на кнопке Update, чтобы сохранить новое значение в памяти управляемого коммутатора.

На рисунке 15.3 показана сетевая страница подраздела VLAN Setting.

В таблице 15.1 приведено описание параметров VLAN, настраиваемых на этой сетевой странице.

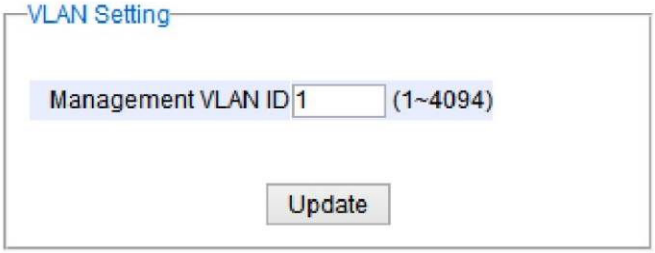


Рисунок 15.3. Сетевая страница настройки параметров VLAN.

Таблица 15.1. Описание настраиваемых параметров VLAN.

Имя параметра	Описание	Заводская настройка по умолчанию
Management VLAN ID	В данном поле указывается административный идентификатор VLAN для обращения с данного коммутатора. Принимает значения в диапазоне от 1 до 4094.	1

15.2 Подраздел 802.1Q VLAN

VLAN на основе тегов (802.1Q VLAN) представляет собой стандартную сетевую технологию, которая используется для поддержки LAN в сети Ethernet.

Этот стандарт описывает систему тегирования VLAN в кадрах данных Ethernet и процедуры обработки таких кадров мостами и коммутаторами.

Стандарт также содержит положения касательно схемы установления приоритетов качества сервиса, известной под названием IEEE 802.1Q.

Кадры тегирования VLAN представляют собой кадры данных с тегами 802.1Q (VLAN), которые содержат ссылки на действительные идентификаторы VLAN.

Нетегированными кадрами являются кадры данных без тегов или с тегами приоритетов 802.1p. Такие кадры содержат только информацию об установлении приоритетов и идентификатор VLAN = 0.

Когда коммутатор принимает тегированный кадр, он извлекает идентификатор VLAN и передает этот кадр на другие порты, включенные в указанную VLAN.

В каждый пакет 802.1Q VLAN добавляется тег (32-разрядное поле).

Поле тега вставляется между полем с MAC-адресом источника и полем EtherType/length.

Что представляет собой тег: первые 16 битов тега образуют поле идентификатора протокола тегирования (TPID), в котором для тегированного кадра IEEE 802.1Q указывается значение 0x8100.

Это поле находится в том месте, где в нетегированном кадре расположено поле EtherType/length. Таким образом, его можно использовать для отличения тегированных кадров от нетегированных.

Следующие три бита образуют поле информации управления тегами (TCI), которое содержит ссылку на класс сервиса IEEE 802.1p и привязывается к определенному уровню приоритета

кадров.

Следующий один бит образует поле индикатора допустимости удаления (DEI) поле, которое можно использовать отдельно или в комбинации с полем кода приоритета (PCP), чтобы обозначать кадры, которые могут быть отброшены при возникновении перегрузки.

И, наконец, последние 12 битов образуют поле идентификатора VLAN (VID).

Идентификатор обозначает VLAN, к которой относится данный кадр.

Подраздел 802.1Q VLAN, в свою очередь, содержит три подраздела нижнего уровня, которые включают Setting, PVID Setting и VLAN Table, как показано на рисунке 15.4.

Рисунок 15.4. Раскрывающееся меню подраздела 802.1Q VLAN.

15.2.1 Подраздел Setting

На рисунке 15.5 показана сетевая страница подраздела Setting меню 802.1Q VLAN, на который пользователь может настраивать новые VLAN на основе тегов на управляемом коммутаторе. Чтобы настроить 802.1Q VLAN на коммутаторе, выполните описанную ниже процедуру.

1. Перейдите в меню 802.1Q VLAN и откройте подраздел Setting.

2. Введите или выберите нужные значения в полях Name, VID, Member Ports и Tagged Ports, как показано на рисунке 15.5. Описание всех полей в сводном виде представлено в таблице 15.2. Затем щелкните с указателем на кнопке Add/Modify.

ПРИМЕЧАНИЕ: чтобы выбрать несколько значений в полях Member Ports и Tagged Ports, при выборе удерживайте нажатой клавишу Ctrl.

3. Перейдите в подраздел PVID Setting меню VLAN 8021Q (см. описание в следующем разделе).

4. Выберите те же порты и введите в столбце PVID значения, которые должны совпадать с соответствующими идентификаторами VLAN в поле VID, см. рисунок 15.6.

Чтобы удалить VLAN из списка 802.1Q VLAN, щелкните с указателем на кнопке Remove в конце соответствующей записи VLAN, как показано на рисунке 15.5.

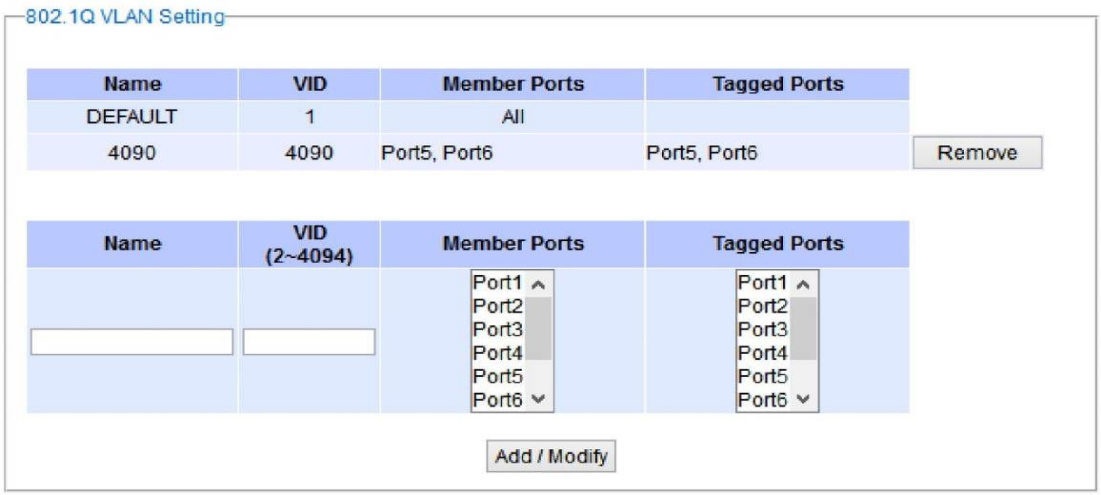


Рисунок 15.5. Сетевая страница Setting меню 802.1Q VLAN.

Таблица 15.2. Описание настраиваемых параметров подраздела Settings меню 802.1Q VLAN.

Имя параметра	Описание	Заводская настройка по умолчанию
Name	Произвольное имя идентификатора VLAN, назначаемое пользователем.	-
VID	Указывается идентификатор VLAN, который будет добавлен в статическую таблицу VLAN в коммутаторе. Идентификатор VLAN может принимать значения в диапазоне от 2 до 4094.	Обусловленное
Member Ports	Указываются порты, связанные с данным идентификатором VLAN.	Все порты
Tagged Ports	Выбираются порты для тегирования исходящих пакетов. Если порт выбран: исходящие пакеты, передаваемые через данный порт, тегируются. Если порт не выбран: исходящие пакеты, передаваемые через данный порт, не тегируются.	Обусловленное

*** ПРИМЕЧАНИЕ**: Значение идентификатора VLAN по умолчанию может быть только 1. Чтобы установить другое значение идентификатора VLAN (отличное от 1), пользователь должен включить порты в соответствующую группу VLAN.

15.2.2 Подраздел PVID Setting меню 802.1Q VLAN

Каждому порту присваивается номер, соответствующий идентификатору VLAN этого порта. Этот номер называется VLAN-идентификатор порта (PVID). Когда через порт проходит нетегированный кадр, этому кадру назначается VLAN-идентификатор этого порта.

То есть, кадр тегируется идентификатором VLAN, настроенным согласно описанию в данном разделе.

На рисунке 15.6 показана сетевая страница PVID Setting подраздела меню 802.1Q VLAN.

На этой странице в верхней таблице приведены текущие значения VLAN-идентификаторов, назначенных портам.

Пользователь может изменять VLAN-идентификаторы, выбрав один или несколько портов

(удерживая нажатой клавишу Ctrl) и привязав к ним требуемое значение из раскрывающегося списка в поле PVID в диапазоне от 2 до 4094.

Щелкните с указателем на кнопке Update, чтобы новая конфигурация коммутатора вступила в силу.

Описание параметров, настраиваемых на сетевой странице PVID Setting, в сводном виде представлено в таблице 15.3.

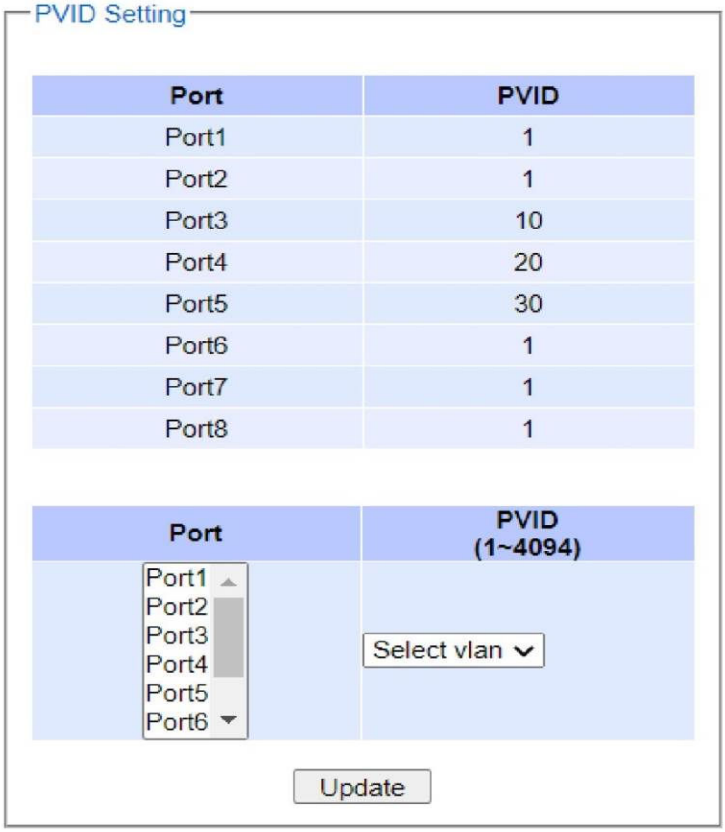


Рисунок 15.6. Сетевая страница PVID Setting меню 802.1Q VLAN.

Таблица 15.3. Описание настраиваемых параметров подраздела PVID Setting меню 802.1Q VLAN.

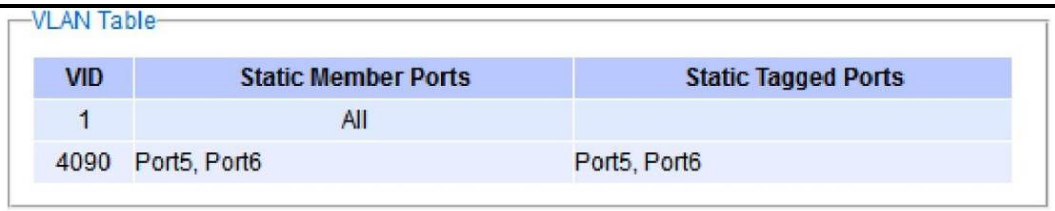
Имя параметра	Описание	Заводская настройка по умолчанию
Port	Выберите определенный порт или порты для назначения VLAN-идентификаторов.	-
PVID	Выберите для порта значение идентификатора 802.1Q VLAN по умолчанию. Идентификатор VLAN может принимать значения в диапазоне от 1 до 4094.	1

15.2.3 Подраздел VLAN Table меню 802.1Q VLAN

На этой сетевой странице, показанной на рисунке 15.7, отображается таблица 802.1Q VLAN, в которой перечислены все VLAN, настроенные на управляемом коммутаторе автоматически или вручную.

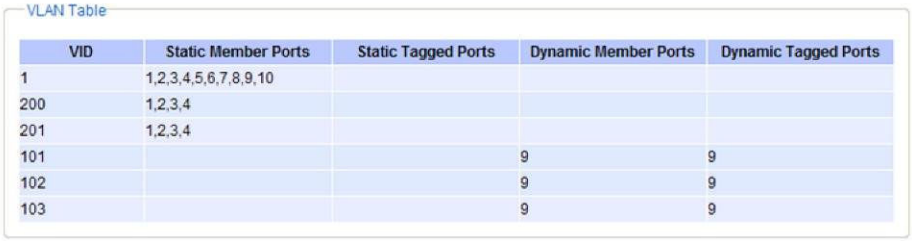
На рисунке 15.8 показан пример информации о статических и динамических VLAN, привязанных к определенным идентификаторам.

Описание параметров VLAN Table в сводном виде представлено в таблице 15.4.


VLAN Table

VID	Static Member Ports	Static Tagged Ports
1	All	
4090	Port5, Port6	Port5, Port6

Рисунок 15.7. Сетевая страница VLAN Table меню 802.1Q VLAN.


VLAN Table

VID	Static Member Ports	Static Tagged Ports	Dynamic Member Ports	Dynamic Tagged Ports
1	1,2,3,4,5,6,7,8,9,10			
200	1,2,3,4			
201	1,2,3,4			
101			9	9
102			9	9
103			9	9

Рисунок 15.8. Пример таблицы 802.1Q VLAN.

Таблица 15.4. Описание параметров в таблице 802.1Q VLAN.

Имя параметра	Описание	Заводская настройка по умолчанию
VID	В этом поле указывается идентификационный номер VLAN.	Обусловленное
Static Member Ports	В этом поле указываются порты, привязанные к данному идентификатору VLAN. Эта запись создается пользователем.	Все порты
Static Tagged Ports	В этом поле указываются порты для тегирования исходящих пакетов. Если порт отображается: исходящие пакеты, передаваемые через данный порт, тегируются. Если порт не отображается: исходящие пакеты, передаваемые через данный порт, не тегируются. Эта запись создается пользователем.	Обусловленное
Dynamic Member Ports	В этом поле указываются порты, привязанные к данному идентификатору VLAN. Эта запись создается протоколом GVRP.	Обусловленное
Dynamic Tagged Ports	В этом поле указываются порты-члены для тегирования исходящих пакетов. Если порт отображается: исходящие пакеты, передаваемые через данный порт, тегируются. Если порт не отображается: исходящие пакеты, передаваемые через данный порт, не тегируются. Эта запись создается протоколом GVRP.	Обусловленное

15.3 Подраздел Port-Based VLAN

VLAN на основе портов (другое название - статические VLAN) настраиваются посредством назначения портов для включения в данную виртуальную сеть.

Если устройство подключается к определенному порту, оно включается в VLAN, к которой привязан данный порт.

При переподключении к другому порту связь порт - VLAN для нового соединения должна быть настроена заново. Для настройки VLAN на основе портов выполните следующую процедуру:

1. Щелкните с указателем на вводе меню Port-Based VLAN Setting, чтобы открыть окно, показанное на рисунке 15.9.

2. Выберите порты, которые будут включены в определенную группу, установив флажки в полях столбцов Member ports в строке с идентификатором соответствующей группы VLAN на основе портов.

ПРИМЕЧАНИЕ: если установить флажок в столбце Group ID, то все порты-члены будут привязаны к соответствующему идентификатору группы VLAN.

3. Щелкните с указателем на кнопке Update, чтобы новая конфигурация коммутатора вступила в силу.

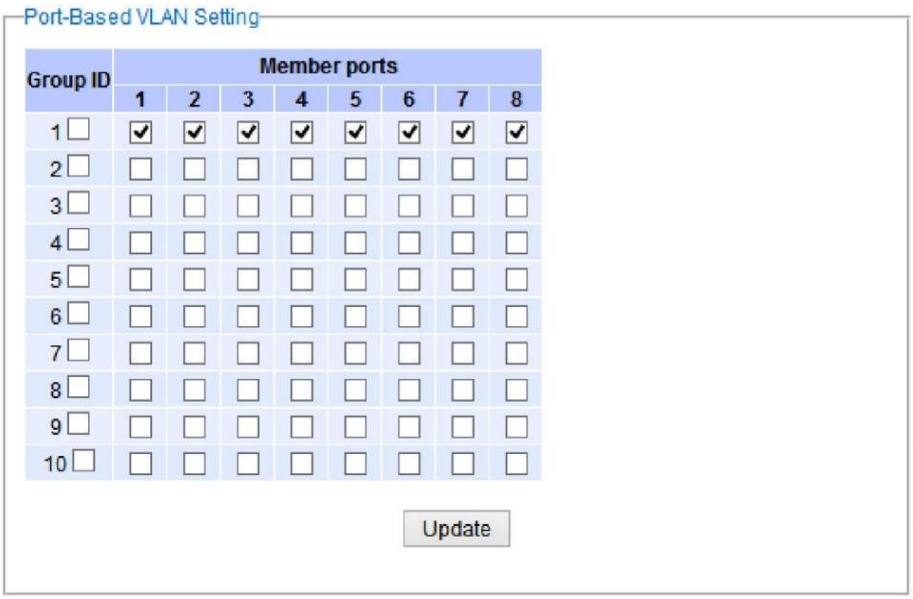


Рисунок 15.9. Сетевая страница настройки параметров VLAN на основе портов.

15.4 Подраздел MAC-Based VLAN

Управляемый коммутатор также поддерживает возможность назначения идентификаторов VLAN нетегированным пакетами на основе MAC-адреса источника.

Это можно сделать в данном подразделе, как показано на рисунке 15.10.

Максимальное количество записей в таблице VLAN на основе MAC-адресов (MAC-адрес источника + идентификатор VLAN) не может превышать 512.

Эта таблица расположена в нижней части сетевой страницы.

Если пользователь введет MAC-адрес, который уже имеется в таблице VLAN на основе MAC-адресов, то новый идентификатор VLAN перезапишет старое значение.

Идентификатор VLAN может принимать значения в диапазоне от 1 до 4096. Если MAC-адрес источника пакета совпадает с адресом в записи в таблице VLAN на основе MAC-адресов, то в пакет будет добавлен идентификатор VLAN, соответствующий MAC-адресу в таблице.

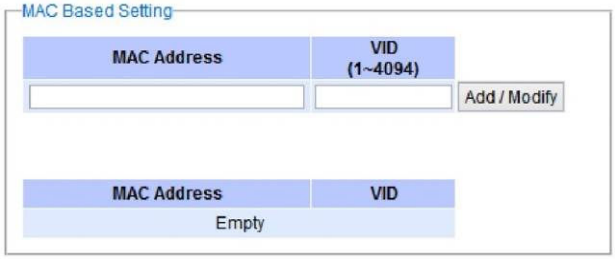


Рисунок 15.10. Сетевая страница настройки параметров VLAN на основе MAC-адресов.

15.5 Подраздел IP Subnet-Based VLAN

В этом подразделе пользователь может присваивать идентификаторы VLAN нетегированным пакетам на основе IP-адреса источника и длины его префикса. Сети, организованные таким образом, называют VLAN на основе масок IP-подсетей.

На рисунке 15.11 показана сетевая страница, на которой пользователь может ввести IP-адрес, длину префикса и идентификатор VLAN, чтобы создать VLAN на основе маски его IP-подсети. Список существующего VLAN на основе масок IP-подсетей выводится в нижней части сетевой страницы.

Эта функция поддерживает до 64 комбинированных записей (IP-адрес + длина префикса + идентификатор VLAN).

Идентификатор VLAN может принимать значения в диапазоне от 1 до 4096. Эта функция настройки VLAN поддерживается обеими версиями IP-протокола (IPv4 и IPv6).

При попытке дублирования комбинации IP-адреса и длины префикса в таблице система выведет сообщение об ошибке.

Длина префикса составляет от 0 до 32 для версии IPv4 или от 0 до 64 для версии IPv6.

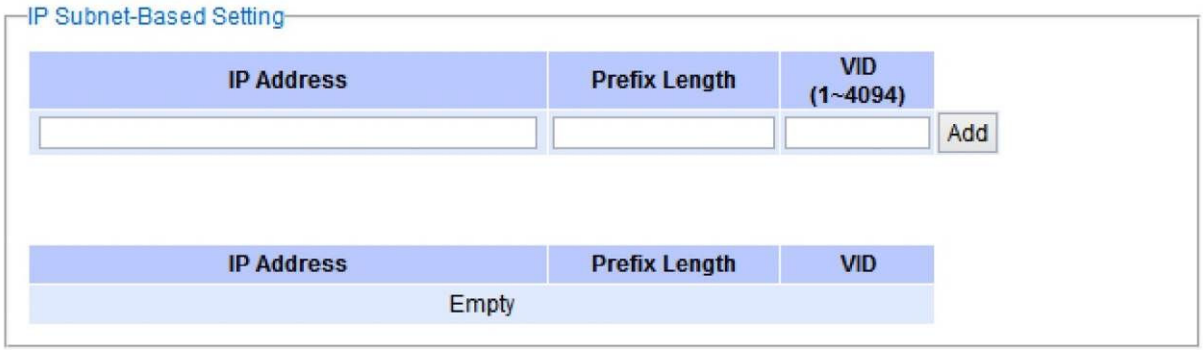


Рисунок 15.11. Сетевая страница настройки параметров VLAN на основе масок IP-подсетей.

15.6 Подраздел Protocol-Based VLAN

Для VLAN на основе протокола коммутатор поддерживает следующие три типа пакетных кадров Ethernet: Ethernet II, 802.3 LLC и 802.3 SNAP.

В таких VLAN коммутатор использует поле EtherType (идентификатор протокола) в кадрах для назначения идентификаторов VLAN всем нетегированным пакетам.

Подраздел Protocol-Based VLAN, в свою очередь, делится на два подраздела нижнего уровня: Protocol to Group Setting и Group to VLAN Setting.

15.6.1 Подраздел Protocol to Group Setting

В этом подразделе меню пользователь может добавлять или изменять идентификаторы групп в поле Group ID, как показано на рисунке 15.12.

При этом поддерживается до 16 правил. Окно "Protocol Group Setting" используется для описания правил протокола и назначения уникальных идентификаторов (идентификаторов групп).

Идентификатор группы в поле Group ID может принимать значения в диапазоне от 1 до 2147483646.

В поле Frame Type может быть указан тип кадров Ethernet, SNAP или LLC.

В поле "Value" на данной сетевой странице указывается значение EtherType (идентификатора протокола).

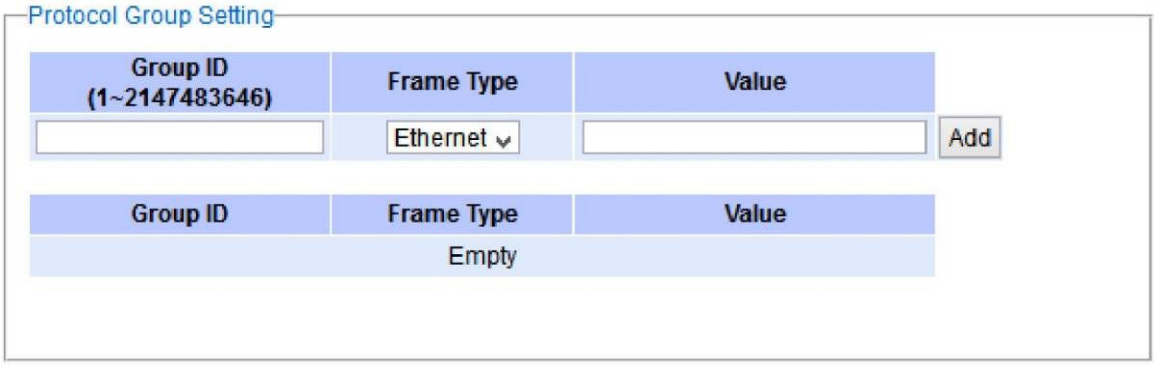


Рисунок 15.12. Сетевая страница подраздела Protocol to Group Setting.

15.6.2 Подраздел Group to VLAN Settings

В этом подразделе меню пользователь может добавлять или изменять идентификаторы групп в поле Group ID для одного или нескольких портов, как показано на рисунке 15.13.

Подраздел "Group to VLAN Setting" используется для связывания идентификаторов групп с идентификаторами VLAN.

Таким образом, поля FrameType и EtherType в кадре данных привязываются к идентификатору VLAN.

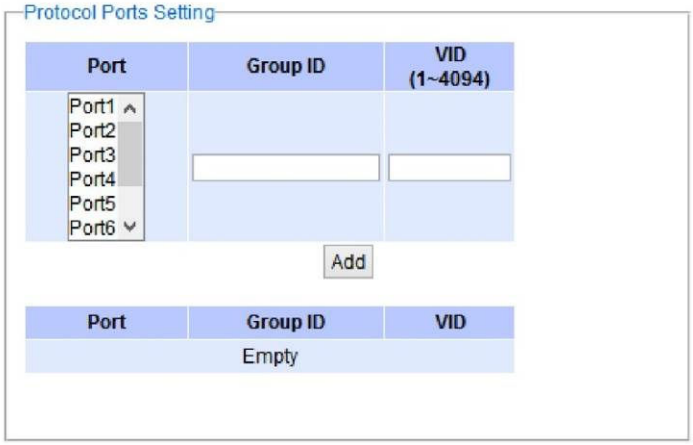


Рисунок 15.13. Сетевая страница Group to VLAN Setting.

15.7 Подраздел QinQ

В исходном варианте стандарт 802.1Q для VLAN допускал добавление в пакет только одного тега VLAN. Но затем появилась функция QinQ, которая рассматривается в данном разделе.

Эта функция позволяет добавлять в пакет два тега VLAN.

Функция QinQ была разработана для провайдеров услуг, чтобы провайдер мог вставить дополнительный тег VLAN для идентификации внешней сети, не удаляя при этом исходный тег VLAN клиента (если имеется).

Для лучшего понимания действий по настройке параметров функции QinQ VLAN, рассмотрим в качестве примера сеть, объединяющую два здания с номерами 1 и 2, и два отдела - A и B одной организации, которые размещаются в обоих зданиях.

Оба отдела (A и B) желают использовать VLAN2 с идентификатором протокола тегирования 0x8100 для передачи данных внутри подразделения, но при этом они не хотят связываться друг с другом.

В такой ситуации сетевой администратор может активировать функцию QinQ VLAN (двойное тегирование VLAN) на управляемых коммутаторах организации.

Если в Здании 1 установлены следующие коммутаторы: A1 (для Отдела A), B1 (для Отдела B), H1 (для магистральной сети), а в Здании 2 - коммутаторы: A2 (для Отдела A), B2 (для Отдела B), и H2 (для магистральной сети), тогда все коммутаторы можно настроить, как показано на рисунке 15.14.

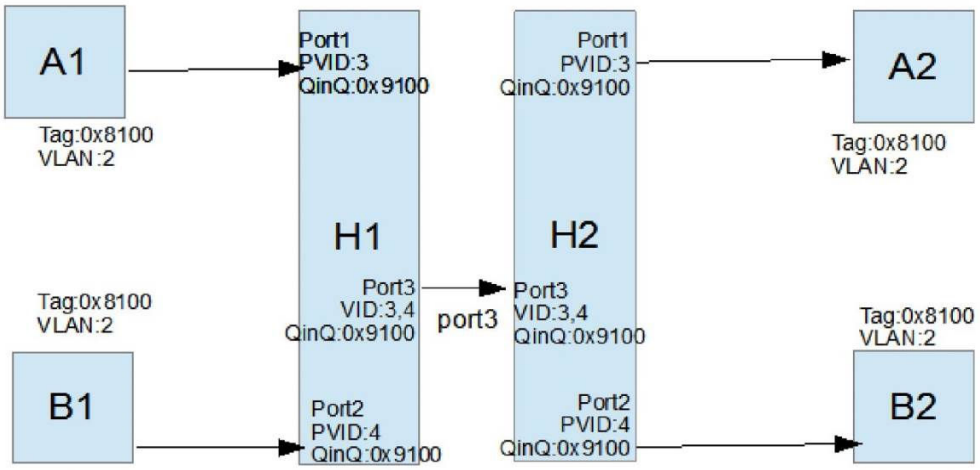


Рисунок 15.14. Пример развертывания сети с поддержкой функции QinQ.

Сеть, поддерживающая настройку VLAN с использованием функции QinQ, показанная на рисунке, работает следующим образом.

1. Коммутаторы A1 и B1 передают пакеты с определенным тегом VLAN (идентификатор протокола тегирования = 0x8100, идентификатор VLAN = 2) на коммутатор H1.

2. Коммутатор H1 рассматривает принятые пакеты с тегом VLAN (TPID = 0x8100), как нетегированные, потому что идентификатор TPID функции QinQ на принимающих портах имеет значение 0x9100. В каждый такой пакет вставляется второй тег VLAN (идентификатор TPID = 0x9100, идентификатор VLAN = VLAN-идентификатор порта).

3. Коммутатор H1 переадресовывает эти пакеты на порт 3 (идентификатор VLAN = 3 или 4 - в зависимости от номера порта входящего пакета - A1 или B1).

4. Коммутатор H2 принимает эти пакеты и переадресовывает их согласно правилу VLAN. Пакеты с идентификатором VLAN = 3 передаются на порт 1, а пакеты с идентификатором VLAN = 4 – на порт 2.

5. Прежде чем Коммутатор H2 передаст эти пакеты через порт 1 или 2, он удалит из них теги VLAN (идентификатор TPID = x9100, идентификатор VLAN = 3 или 4).

На рисунке 15.15 показана сетевая страница настройки параметров функции QinQ, на которой можно активировать эту функцию для каждого порта на управляемом коммутаторе.

После установки флажка в поле Enabled в строке каждого порта активируется поле идентификатора протокола тегирования (TPID). По умолчанию для идентификатора TPID устанавливается значение 0x8100, что означает, что функция QinQ отключена.

Чтобы активировать функцию QinQ на порте, пользователь должен указать соответствующее значение идентификатора TPID.

В общем случае должно быть установлено значение, отличное от исходного тега 0x8100, например, 0x9100.

Значение идентификатора TPID должно быть в диапазоне от 0x0000 до 0xFFFF.

Если функция QinQ настраивается для агрегированного порта, настройки QinQ всех физических портов – членов агрегации должны быть одинаковыми. Это означает, что значения в полях QinQ Enabled и TPID должны быть одинаковыми для всех физических портов в составе агрегированного порта.

Ниже приведено краткое описание правил настройки функции QinQ:

• Для входящих портов и исходящих портов: решение о наличии тега VLAN в пакете принимается в зависимости от значения в поле TPID.

- Пакет считается нетегированным (без тега VLAN), если значение в его поле TPID не совпадает со значением идентификатора протокола TPID, заданным для порта при настройке параметров функции QinQ.
- Пакет считается тегированным (с тегом VLAN), если значение в его поле TPID совпадает со значением идентификатора протокола TPID, заданным для порта при настройке параметров функции QinQ.

• Любой тегированный или нетегированный пакет обрабатывается согласно общему правилу VLAN, то есть, либо в пакет включается тег, либо тег удаляется из пакета, либо пакет остается в неизменном виде, после чего выполняется переадресация.

• Если в пакет вставляется тег VLAN: значение идентификатора TPID для тега принимается равным значению этого идентификатора, настроенному для функции QinQ входящего порта, а значение идентификатора VLAN для тега принимается соответственно значению VLAN-

идентификатора входящего порта.

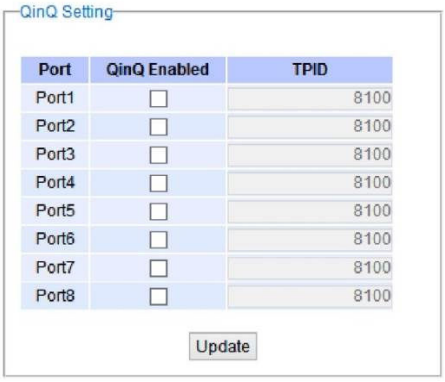


Рисунок 15.15. Сетевая страница настройки параметров функции QinQ.

Завершив настройку параметров функции QinQ на любом порте, щелкните с указателем на кнопке Update, чтобы изменения вступили в силу на управляемом коммутаторе.

15.8 Подраздел Voice VLAN

Voice VLAN - это VLAN (виртуальная локальная сеть), которая специально выделена для потоков голосовых данных пользователя. Он может управлять приоритетом передачи проходящего голосового трафика при передаче с другим трафиком. То есть, когда другие услуги (данные, видео и т.д.) передаются одновременно, голосовая услуга может быть установлена как передача с высоким приоритетом или передача с низким приоритетом, чтобы гарантировать, что голосовая услуга может передаваться с более высоким приоритетом переадресации или другие услуги могут передаваться с более высоким.

15.8.1 Voice VLAN Settings

Пользователям необходимо обратиться к разделу 15.2.1 “802.1Q VLAN Setting”, чтобы создать одну vlan, затем добавить порты в vlan и снять метки для голосовой vlan. Затем следует настроить параметры голосовой VLAN в этом пункте меню, как показано на рис. 15.16.

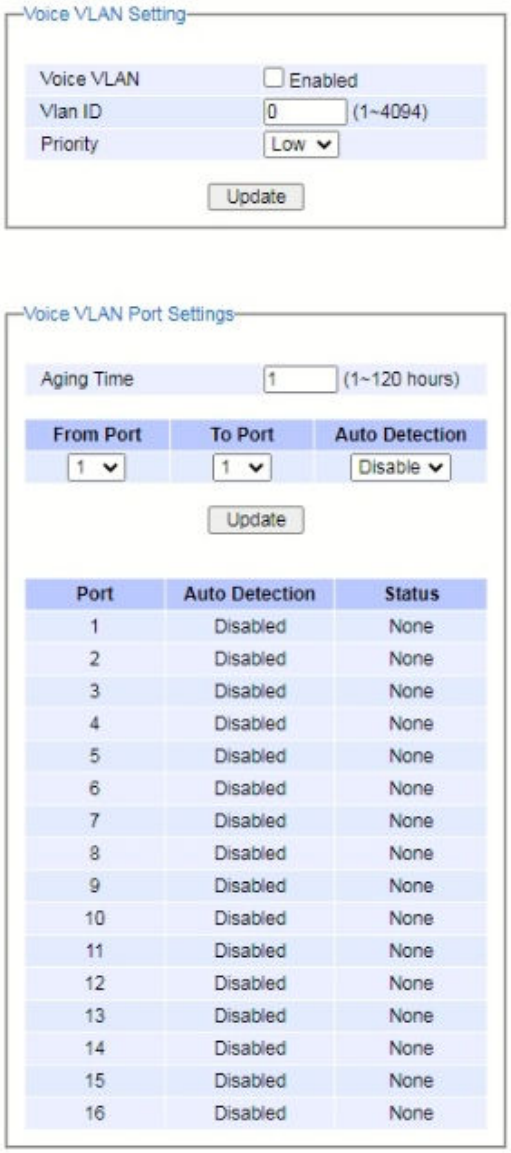


Рисунок 15.16. Сетевая страница настройки параметров Voice VLAN

Таблица 15.5. Описание параметров в таблице 802.1Q VLAN.

Имя параметра	Описание	Заводская настройка по умолчанию
Voice VLAN State	В этом поле устанавливается флажок, чтобы включить или отключить голосовую VLAN	отключено
VLAN ID	В этом поле задается идентификатор VLAN, которому вы хотите назначить голосовой трафик. **Примечание.** Сначала нужно создать VLAN на странице 802.1Q VLAN, прежде чем назначить выделенную голосовую VLAN.	-
Priority	Уровни приоритета трафика 802.1p в голосовой VLAN.	Low

Имя параметра	Описание	Заводская настройка по умолчанию
Aging Time	Введите период (в часах) для удаления порта из голосовой VLAN, если порт является автоматическим участником VLAN. Когда последнее голосовое устройство перестанет отправлять трафик и MAC-адрес этого голосового устройства устареет, запустится таймер старения голосовой VLAN. Порт будет удален из голосовой VLAN по истечении таймера старения голосовой VLAN. Выбираемый диапазон составляет от 1 до 120 часов.	1
From Port / To Port	Настройка последовательной группы портов, начиная с выбранного порта.	1-1
Auto Detection	Автоматическое добавление портов в голосовую VLAN. Если обнаружит, что OUI устройства соответствует OUI телефонии, настроенному на странице настроек OUI голосовой VLAN. Используйте выпадающее меню, чтобы включить или отключить функцию автоматического определения OUI.	Отключено
Status	Показывает статус порта, если IP-телефон подключен к портам, статус изменяет значение на “Подключен”, в противном случае “Нет”.	None

15.8.2 Voice VLAN OUI Settings

Данный подраздел позволяет настроить пользовательский интерфейс голосового трафика. Уникальный идентификатор организации (OUI) — это первые три байта MAC-адреса. Этот идентификатор однозначно определяет поставщика, производителя или другую организацию.

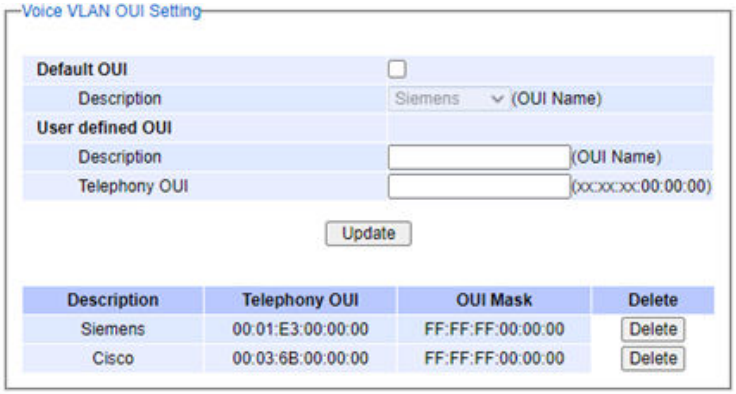


Рисунок 15.17. Сетевая страница настройки параметров Voice VLAN OUI

Default OUI: предварительно определенные значения OUI, включая названия брендов 3COM, Cisco, H3C, Pingtel, Siemens, NEC/Philips, Huawei 3COM и Avaya как показано на рисунке 15.18.

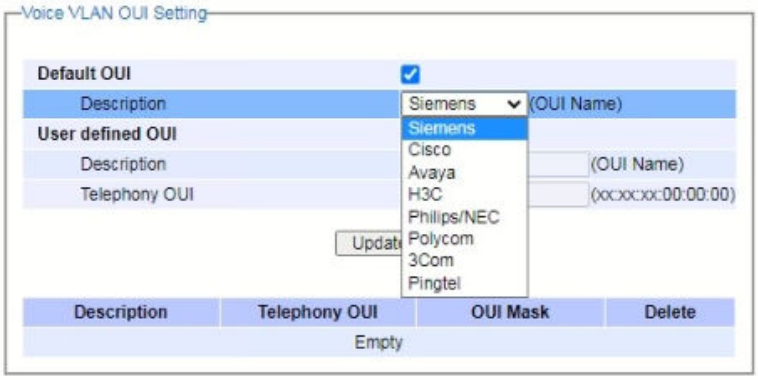


Рисунок 15.18. Сетевая страница настройки параметров Voice VLAN OUI

User defined OUI: Этот пункт позволяет вручную создать пользовательский интерфейс телефонии с описанием как показано на рисунке 15.19.

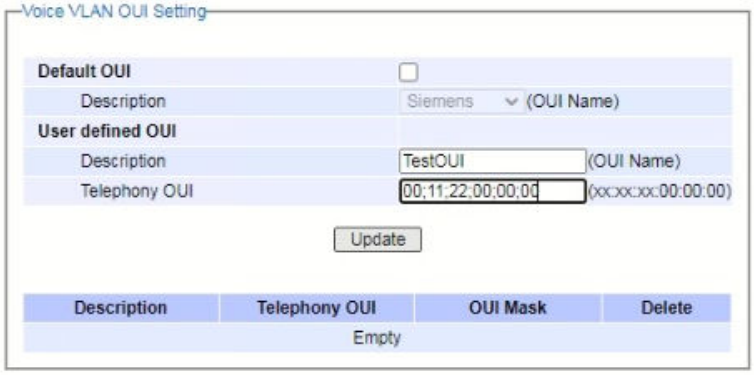


Рисунок 15.19. Сетевая страница настройки параметров Voice VLAN OUI

16 РАЗДЕЛ SECURITY

Коммутаторы поддерживают следующие функции безопасности:

- Port Security (в статическом режиме)
- 802.1 X
- IP Source Guard
- ARP Spoof Prevention
- DHCP Snooping
- ACL (список управления доступом).
- Dynamic ARP Inspection

На рисунке 16.1 показано раскрывающееся меню раздела Security для управляемого коммутатора.

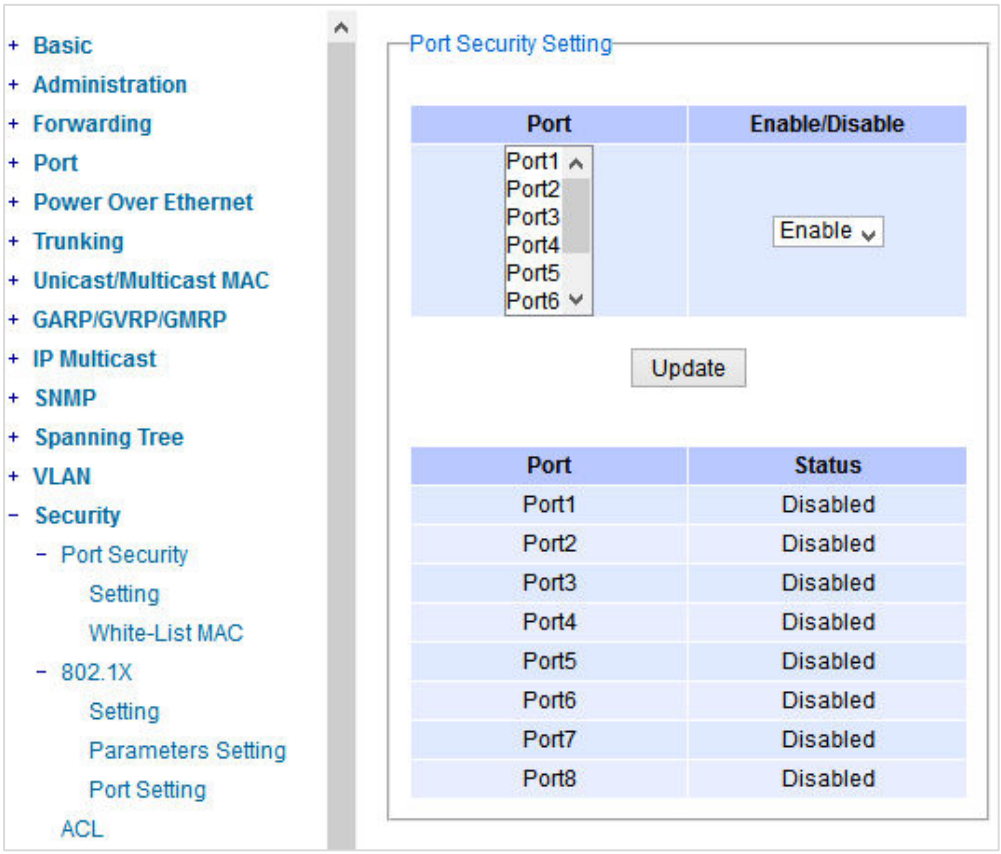


Рисунок 16.1. Раскрывающееся меню раздела Security.

16.1 Подраздел Port Security

В подразделе Port Security (или Static Port Security) пользователь может управлять безопасностью каждого порта управляемого коммутатора, а также создать и вести таблицу MAC-адресов, которым разрешен доступ к коммутатору.

Подраздел Port Security, в свою очередь, разделен на два подраздела нижнего уровня: Setting и White-List MAC.

16.1.1 Подраздел Settings меню Port Security

На рисунке 16.2 показана сетевая страница Port Security Setting, на которой пользователь может активировать или отключить статическую функцию безопасности на одном или нескольких портах.

Чтобы активировать или отключить функцию на нескольких портах одновременно, удерживайте нажатой клавишу Ctrl при выборе нужных портов из списка в поле Port.

Затем выберите нужное действие в поле Enable/Disable и щелкните с указателем на кнопке Update.

В нижней части сетевой страницы Port Security Setting отображается текущий статус функции безопасности для каждого порта на управляемом коммутаторе.

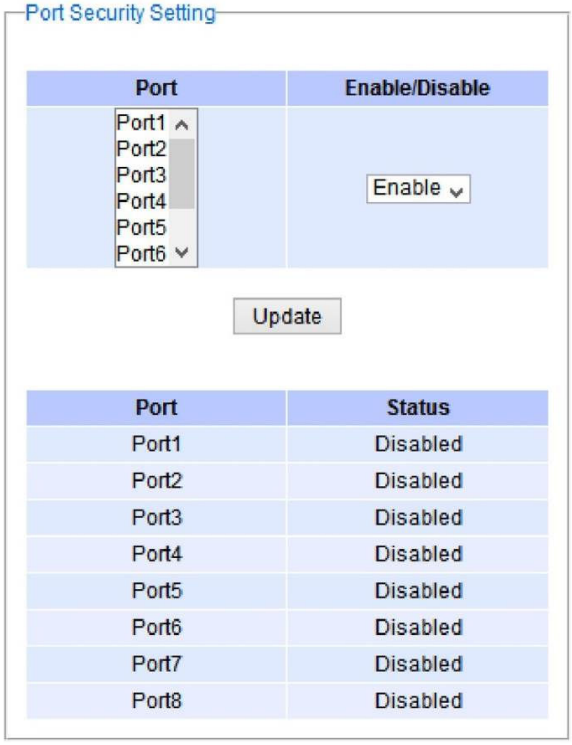


Рисунок 16.2. Сетевая страница Port Security Setting.

16.1.2 Подраздел White-List MAC меню Port Security

Сетевая страница White-List MAC показана на рисунке 16.3. Здесь пользователь может создать список MAC-адресов, которым будет разрешен доступ к управляемому коммутатору.

Для каждого MAC-адреса, добавляемого в этот список, пользователь должен указать идентификатор VLAN в поле VID и номер порта в поле Port.

После ввода значений во всех обязательных полях щелкните с указателем на кнопке Add, чтобы добавить новый MAC-адрес в так называемый "белый список".

Напоминаем, что двум различным портам нельзя назначить один и тот же MAC-адрес. В такой ситуации система выдаст сообщение об ошибке.

Если в списке имеются ранее назначенные MAC-адреса, которые нужно удалить, щелкните с указателем на кнопке Remove в конце каждой соответствующей записи.

В таблице в сводном виде представлено описание полей на сетевой странице White-List MAC.

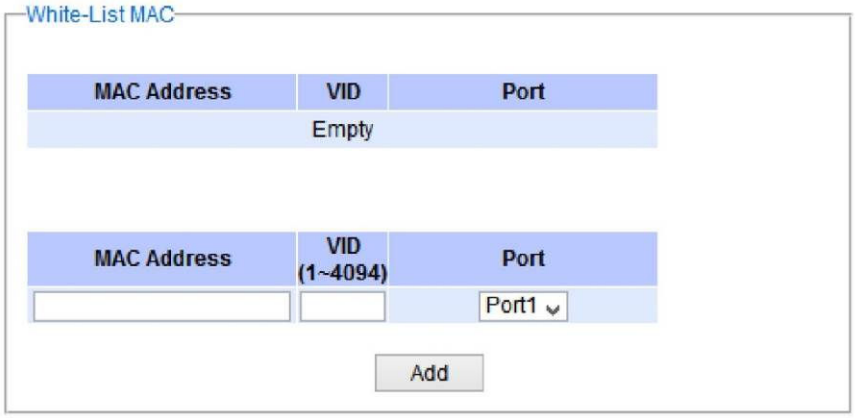


Рисунок 16.3. Сетевая страница настройки белого списка MAC-адресов.

Таблица 16.1. Описание полей на сетевой странице White-List MAC.

Имя параметра	Описание
MAC Address	Введите с клавиатуры любое действительное значение MAC-адреса.
Ports	Выберите требуемые порты.
Remove	Данная опция используется для удаления MAC-адресов при необходимости.
Add	Щелкните с указателем на этом кнопке, чтобы добавить MAC-адрес.
VLAN	Укажите адрес VLAN, к которой относится данный MAC-адрес.

16.2 Подраздел MAC Learning Limits

MAC Learning Limits защищает от переполнения таблицы коммутации Ethernet (также известной как таблица переадресации MAC или таблица переадресации уровня 2). Эта функция используется на интерфейсах (портах) коммутатора.

MAC Learning Limits устанавливает ограничение на количество MAC-адресов, которые могут быть динамически изучены на одном интерфейсе доступа уровня 2 или на всех интерфейсах доступа уровня 2.

Управляемый коммутатор поддерживает 3 исходных MAC-адреса (первые 3 MAC-адреса), которые запоминаются на настроенном интерфейсе. Пользователь может очистить выученные MAC-адреса для повторного изучения новых MAC-адресов на определенном порту (ах). См. рисунок 16.4.

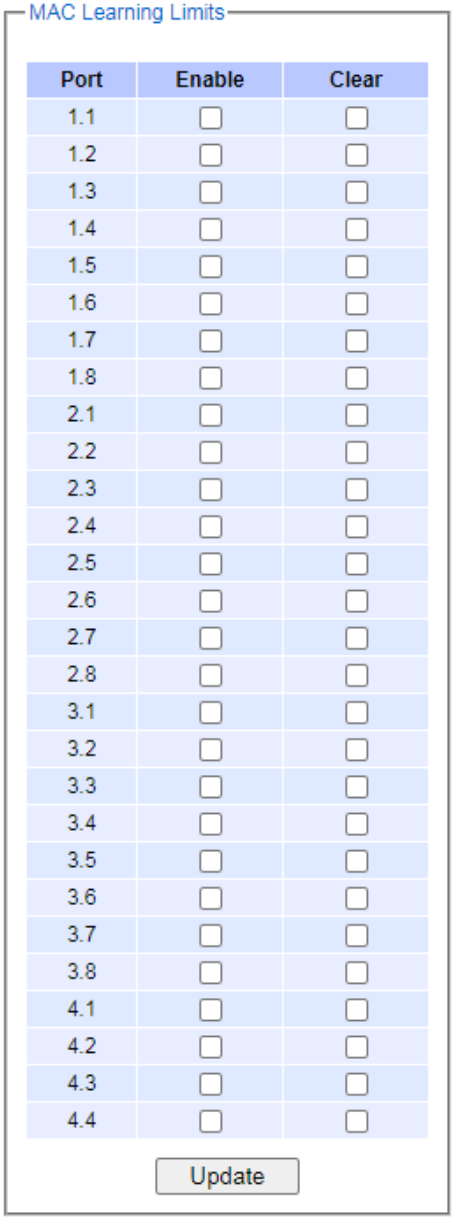


Рисунок 16.4. Сетевая страница настройки MAC Learning Limits.

Таблица 16.2. Описание полей на сетевой странице MAC Learning Limits.

Имя параметра	Описание
Enable	Включение/выключение функции ограничения изучения MAC-адресов на определенных портах
Clear	Очистить выученные MAC-адреса для повторного изучения новых MAC-адресов на соответствующих портах
Update	Обновление настроек

16.3 Подраздел 802.1x

Технология 802.1X представляет собой стандартную технологию, разработанную IEEE для управления доступом к сети на основе портов.

Соответствующая функция поддерживает механизм проверки подлинности устройств, желающих подключиться к LAN или WLAN. Этот протокол препятствует подключению неавторизованных клиентов к LAN через порты, открытые для доступа из сети Интернет.

В процессе проверки подлинности участвуют три основные стороны (см. рисунок 16.5): запрашивающее устройство, аутентификатор и сервер проверки подлинности.

- Запрашивающее устройство: любое клиентское устройство, которое запрашивает доступ к LAN.
- Сервер проверки подлинности: этот сервер непосредственно выполняет проверку подлинности. В качестве сервера проверки подлинности мы используем сервер RADIUS (службы удаленной проверки подлинности пользователей по коммутируемым линиям).
- Аутентификатор: аутентификатор – это сетевое устройство, которое выполняет функции прокси между запрашивающим устройством и сервером проверки подлинности. Оно передает информацию, сверяет информацию с сервером и ретранслирует ответы сервера на запрашивающее устройство.

Аутентификатор выполняет функции "охранника" в защищенной сети.

Запрашивающее устройство сможет получить доступ через аутентификатора к защищенной части сети только после того, как идентификационные данные этого устройства будут проверены и авторизованы.

При проверке подлинности по протоколу 802.1X запрашивающее устройство и аутентификатор обмениваются пакетами протокола EAP (открытый протокол аутентификации, инструментарий которого, широко используется IEEE для проверки подлинности). Затем аутентификатор передает полученную информацию серверу проверки подлинности для верификации.

Если сервер подтвердит запрос, то запрашивающему (клиентскому) устройству будет разрешен доступ к ресурсам, размещенным в защищенной части сети.

RADIUS: протокол RADIUS представляет собой протокол организации сети, который обеспечивает управление проверкой подлинности, авторизацией и учетом (функции AAA) для подключения устройств и использования ими сетевых сервисов.

На рисунке 16.5 показана схематическая последовательность проверки подлинности по протоколу RADIUS.

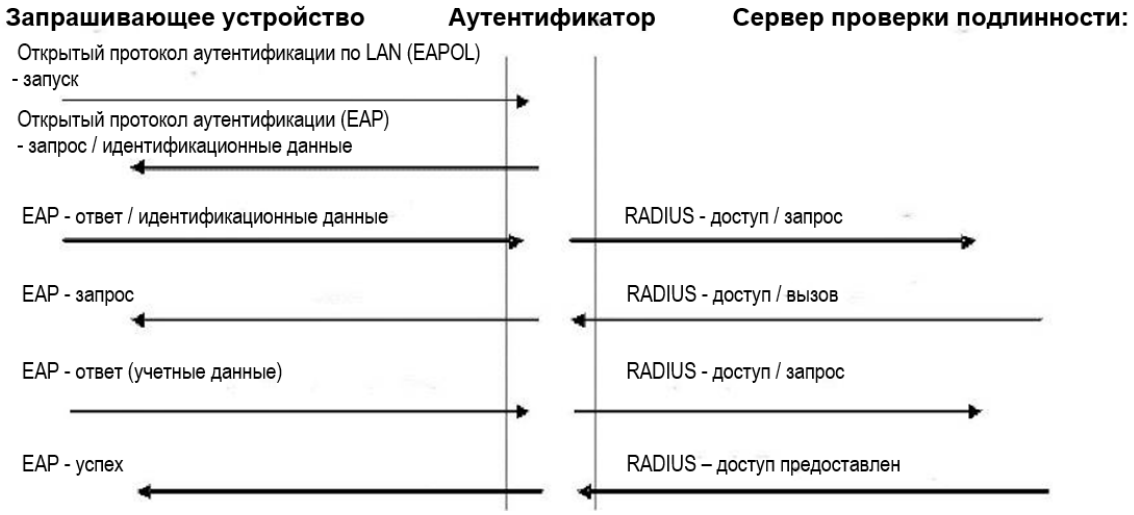


Рисунок 16.5. Последовательность проверки подлинности по протоколу RADIUS.

Подраздел 802.1X в разделе Security, в свою очередь, подразделяется на три подраздела нижнего уровня, а именно: Setting, Parameters Setting и Port Setting.

16.3.1 Подраздел Setting раздела 802.1X

На данной сетевой странице можно активировать защитный механизм 802.1X. Окно подраздела показано на рисунке 16.6.

Если установить флажок в поле Enabled, остальные поля в окне станут доступными для редактирования.

Чтобы успешно активировать протокол 802.1X, нужно правильно заполнить все обязательные поля в окне 802.1X Setting, указав IP-адрес сервера RADIUS, номера порта сервера RADIUS, номер порта учета сервера RADIUS, идентификатор сервера доступа к сети и общий ключ в полях RADIUS Server IP, Server Port, Accounting Port, NAS Identifier и Confirmed Shared Key соответственно.

Описание настраиваемых параметров протокола 802.1X в сводном виде представлено в таблице 16.3. Завершив ввод значений во всех обязательных полях, щелкните с указателем на кнопке Update.

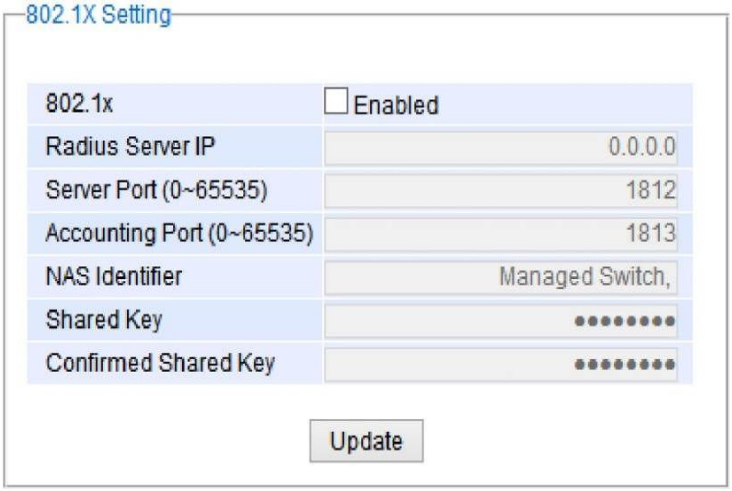


Рисунок 16.6. Сетевая страница подраздела 802.1X.

Таблица 16.3. Описание настраиваемых параметров функции 802.1X.

Имя параметра	Описание	Заводская настройка по умолчанию
802.1x	В этом поле можно активировать или отключить функцию 802.1X для всех портов.	Отключено
Radius Server IP	В этом поле указывается IP-адрес сервера RADIUS.	0.0.0.0
Server Port	В этом поле указывается номер порта сервера RADIUS. Диапазон допустимых значений: от 0 до 65535.	1812
Accounting Port	В этом поле указывается номер порта учета для сервера RADIUS. Диапазон допустимых значений: от 0 до 65535.	1813
NAS Identifier	В этом поле вводится строка идентификатора для сервера доступа к сети 802.1X. Максимальная длина - 30 символов.	Управляемый коммутатор
Shared Key	Общий ключ, совместно используемый управляемым коммутатором и сервером RADIUS. На обеих сторонах соединения должен быть задан одинаковый ключ. Максимальная длина - 30 символов.	Не заполняется
Confirm Shared Key	Повторный ввод общего ключа для подтверждения.	Обусловленное

16.3.2 Подраздел Parameters Setting раздела 802.1X

Для протокола 802.1X предусмотрен целый ряд параметров точной настройки, значения которых пользователь может изменять при необходимости. Это можно сделать в данном подразделе, как показано на рисунке 16.7. Настраиваемые параметры включают периоды проверки подлинности, продолжительность времени ожидания и максимальное количество аутентификационных запросов.

Описание упомянутых настраиваемых параметров в сводном виде представлено в таблице 16.4.

После изменения любых значений щелкните с указателем на кнопке Update.

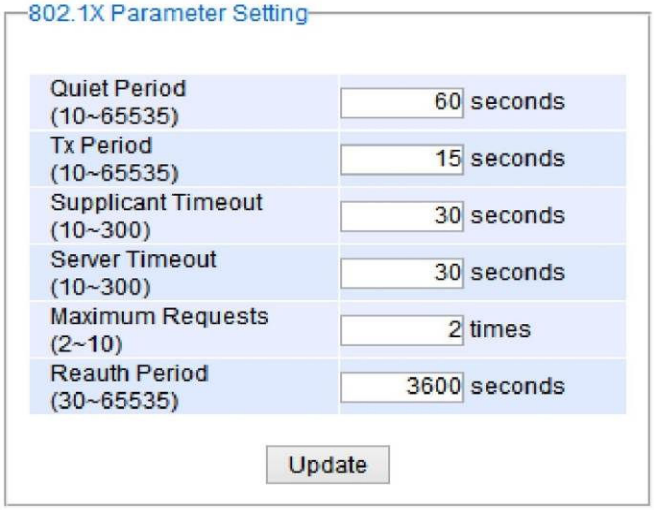


Рисунок 16.7. Сетевая страница подраздела настройки параметров протокола 802.1X.

Таблица 16.4. Описание настраиваемых параметров функции 802.1X.

Имя параметра	Описание	Заводская настройка по умолчанию
Quiet Period	Время ожидания следующего запроса после неудачной авторизации. Принимает значения в диапазоне от 10 до 65535 секунд.	60
Tx Period	Время ожидания EAP-пакета с ответом от запрашивающего устройства до ретрансляции следующего EAP-пакета с запросом. Принимает значения в диапазоне от 10 до 65535 секунд.	15
Supplicant Timeout	Время ожидания ответа от запрашивающего устройства на EAP-пакет, переданный сервером проверки подлинности. Принимает значения в диапазоне от 10 до 300 секунд.	30
Server Timeout	Время ожидания ответа от сервера проверки подлинности на EAP-пакет, переданный запрашивающим устройством. Принимает значения в диапазоне от 10 до 300 секунд.	30
Maximum Requests	Максимальное число EAP-запросов, повторно передаваемых сервером проверки подлинности на запрашивающее устройство до истечения времени сеанса проверки подлинности. Принимает значения в диапазоне от 2 до 10.	2
Reauth Period	Интервал периодической повторной проверки подлинности запрашивающего устройства. Принимает значения в диапазоне от 30 до 65535 секунд.	3600

16.3.3 Подраздел Port Setting раздела 802.1X

Пользователь может настроить защитный механизм протокола 802.1x отдельно на каждом порте управляемого коммутатора, как показано на рисунке 16.8.

Для каждого порта можно выбрать один из четырех режимов авторизации, а именно: Force Authorization, Force Unauthorization, IEEE 802.1X Standard Authorization и no authorization (N/A). Описание перечисленных режимов приведено в таблице 16.5.

В нижней части сетевой страницы расположена таблица, в которой отображается текущий режим проверки подлинности и состояние каждого порта на управляемом коммутаторе.

Чтобы активировать на любых портах функцию защиты по протоколу 802.1X, щелкните указателем на одном порте или, удерживая нажатой клавишу Ctrl, выделите несколько портов в списке, затем выберите режим авторизации из выпадающего списка и щелкните с указателем на кнопке Update.

Чтобы проверить текущее состояние функции 802.1X на портах, щелкните с указателем на кнопке Refresh.

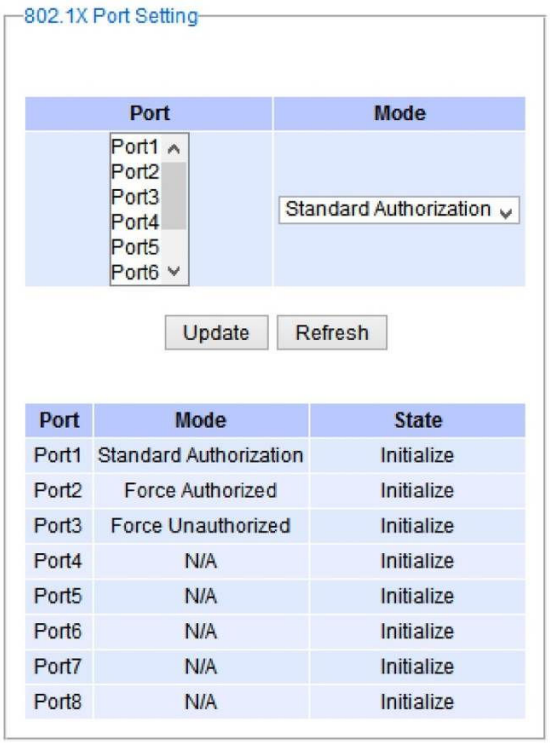


Рисунок 16.8. Сетевая страница Port Setting раздела 802.1X.

Таблица 16.5. Описание настраиваемых параметров в подразделе Port Setting раздела 802.1X.

Имя параметра	Описание	Заводская настройка по умолчанию
Port	Выбор определенных портов для настройки параметров.	Набор значений для выбора
Mode	Варианты: Force Unauthorized: принудительный отказ в авторизации. Force Authorized: принудительная авторизация. Standard Authorization: стандартный режим авторизации согласно спецификации IEEE 802.1X. N/A: авторизация отключена.	N/A

16.4 Подраздел IP Source Guard

Функция IP Source Guard представляет собой другую функцию защиты управляемого коммутатора, которая поддерживает фильтрацию IP-адресов источников на портах второго уровня.

Эта функция предусмотрена с целью воспрепятствовать злоумышленнику в его намерении использовать IP-адрес легального хост-устройства с целью перехвата его функций для выполнения на хост-устройстве злоумышленника.

Эта функция безопасности использует динамическую функцию отслеживания DHCP-пакетов и статическую привязку к источнику для связывания IP-адресов с хост-устройствами на незащищенных портах доступа второго уровня.

На рисунке 16.9 показаны подразделы нижнего уровня в подразделе IP Source Guard.

Рисунок 16.9. Раскрывающееся меню подраздела IP Source Guard.

16.4.1 Подраздел Setting меню IP Verify Source

Функция IP Verify Source представляет собой динамическую реализацию функции IP Source Guard, которая запускает фильтрацию пакетов второго уровня на каждом порте устройства.

Типы фильтров, доступные для выбора, включают IP и IP-mac. Если выбран тип фильтра IP, коммутатор проверяет только IP-адрес источника пакета. Если выбран тип фильтра IP-mac, коммутатор проверяет IP-адрес и MAC-адрес источника пакета.

На рисунке 16.10 показана сетевая страница подраздела Setting меню IP Verify Source. Чтобы активировать на порте фильтрацию в режиме IP Verify Source, установите флажок в поле Enable в соответствующей строке и выберите тип фильтра из выпадающего списка.

После завершения настройки параметров щелкните с указателем на кнопке Update, чтобы активировать фильтрацию.

После активации фильтра все входящие пакеты, передаваемые на выбранный порт, будут отбрасываться.

Порт будет пропускать только пакеты с IP-адресами источников и MAC-адресами, указанными пользователем при настройке.

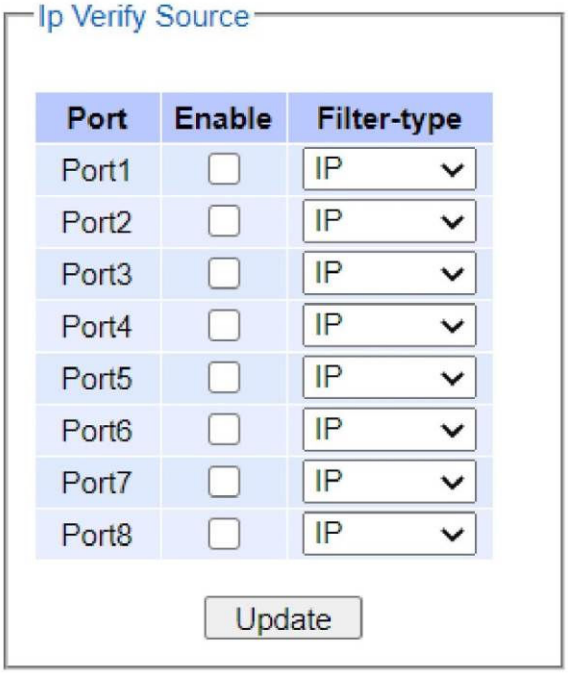


Рисунок 16.10. Сетевая страница Setting подраздела IP Verify Source.

16.4.2 Подраздел Status меню IP Verify Source

На этой странице, показанной на рисунке 16.11, пользователь может проверить состояние функции IP Verify Source guard для каждого порта.

В каждой записи в таблице состояния указываются номер порта, тип фильтра, режим фильтрации, IP-адрес и MAC-адрес (столбцы Port, Filter-type, Filter-mode, IP Address и MAC Address соответственно).

Если функция отслеживания DHCP-пакетов не была активирована, либо при отсутствии трафика через порты, в соответствующих записях таблицы выводится уведомление "inactive-no-snooping".

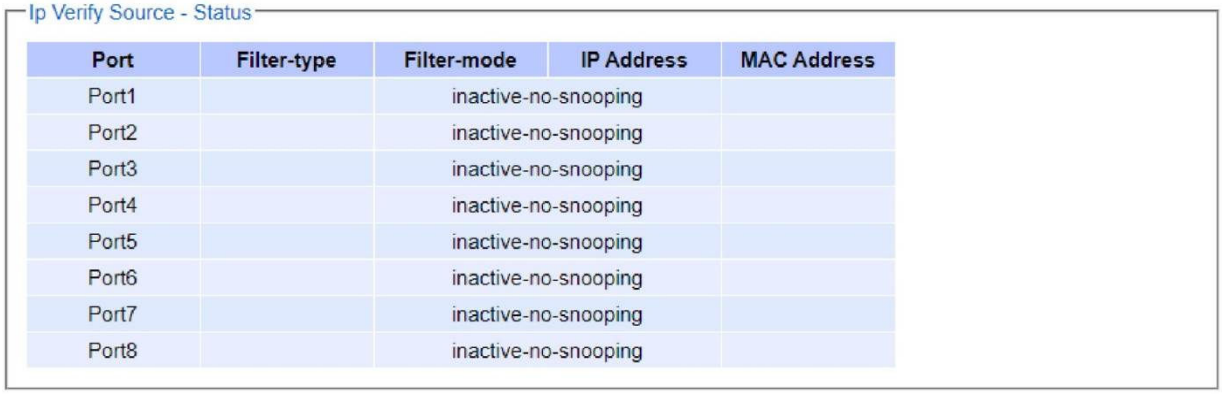


Рисунок 16.11. Сетевая страница Status в подразделе IP Verify Source.

16.4.3 Подраздел Setting меню IP Source Binding

Функция IP Verify Source представляет собой статический вариант реализации функции IP Source Guard, которая запускает фильтрацию пакетов второго уровня на каждом порте устройства.

При настройке этого режима фильтрации пакетов потребуется указать для каждого порта определенный IP-адрес и MAC-адрес источника.

Чтобы активировать фильтрацию в режиме IP Source Binding на одном или нескольких портах, пользователь должен указать MAC-адрес и IP-адрес источника в текстовых полях Source MAC Address и Source IP Address соответственно, как показано на рисунке 16.12.

Затем установите флажки для всех необходимых портов. Затем щелкните с указателем на кнопке Add, чтобы добавить запись фильтрации для функции IP Source Binding.

Новая запись фильтра IP Source Binding появится в таблице в нижней части сетевой страницы.

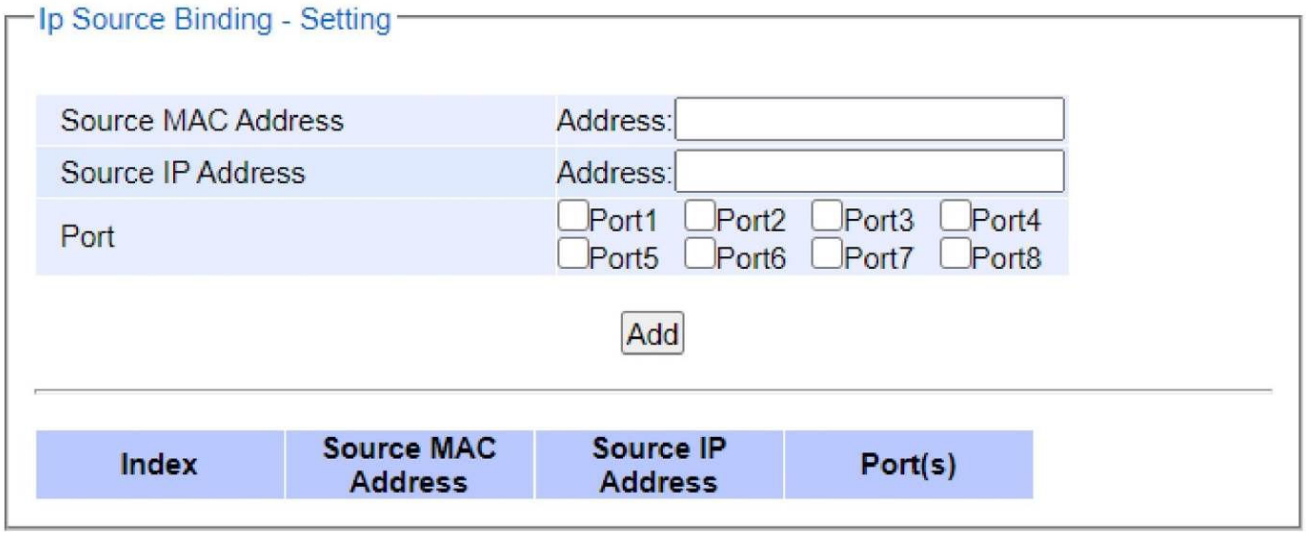


Рисунок 16.12. Сетевая страница Setting в подразделе IP Source Binding.

16.4.4 Подраздел Status меню IP Source Binding

На этой странице, показанной на рисунке 16.13, пользователь может проверить для каждого порта состояние функции IP Source Binding guard, основанной на парах MAC-адресов и IP-адресов.

В каждой записи в таблице состояния указываются MAC-адрес, IP-адрес, время владения в секундах, тип фильтрации и список портов (столбцы MAC Address, IP Address, Lease (sec), Type и Port(s) соответственно).

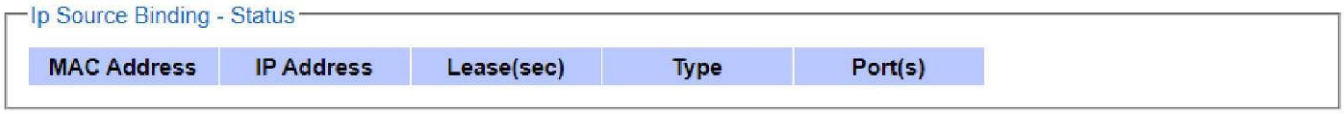


Рисунок 16.13. Сетевая страница Status в подразделе IP Source Binding.

16.5 Подраздел ARP Spoof Prevention

Функция предотвращения имитации протокола ARP (протокол определения адресов) представляет собой механизм защиты от атак с имитацией протокола, поддерживаемый коммутаторами Yarus Networks.

Атака с имитацией протокола ARP заключается в попытке скомпрометировать сетевую безопасность посредством распространения в локальной вычислительной сети ложных сообщений протокола ARP с хост-устройства или узла злоумышленника. Атаки этого типа называются ARP spoofing, ARP cache poisoning или ARP poison routing.

Как правило, злоумышленник стремится к тому, чтобы остальные хост-устройства и узлы в сети связали MAC-адрес Ethernet злоумышленника с легальным IP-адресом хост-устройства или узла, подвергшегося атаке.

Чтобы активировать этот защитный механизм, установите флажок в поле Enabled в строке ARP Spoof Prevention, как показано на рисунке 16.14, затем щелкните с указателем на кнопке Update.

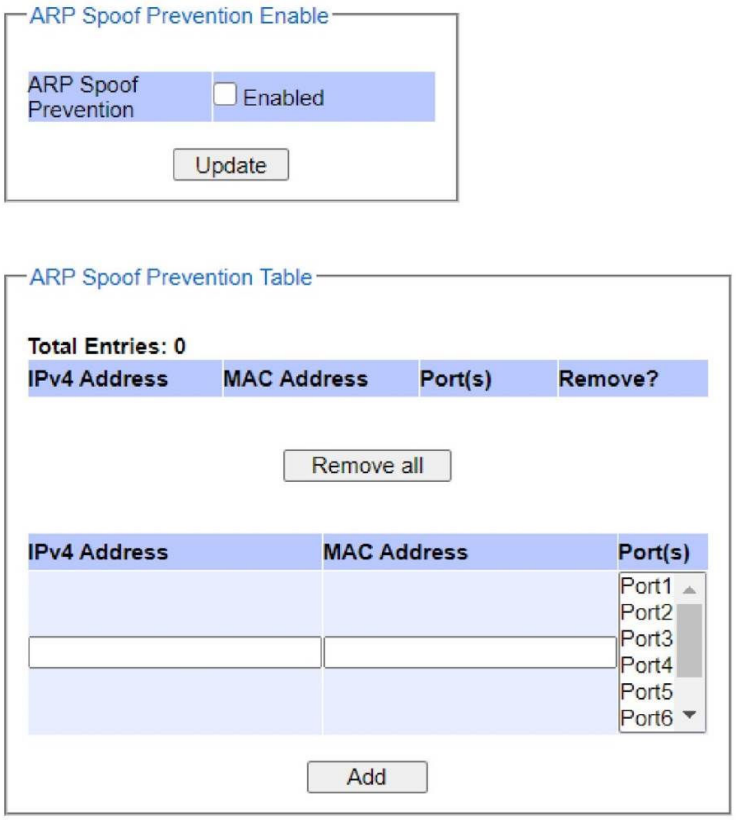


Рисунок 16.14. Сетевая страница ARP Spoof Prevention.

Если функция предотвращения имитации протокола ARP активируется на устройстве, нужно создать соответствующие записи в таблице ARP Spoof Prevention.

Каждая запись состоит из полей IPv4 Address, MAC Address и Port number(s).

В полях IP Address и MAC address каждой записи указываются адреса легального (действительного) хост-устройства или узла, назначенные или подтвержденные администратором коммутатора, которые администратор намерен защитить от атак с имитацией протокола ARP.

В поле Port Number указывается номер отдельного порта или номера группы портов, либо номера всех портов на коммутаторе, которые будут принимать входящие ARP-пакеты от других устройств в сети.

Если коммутатор принимает ARP-пакеты, IP-адреса и MAC-адреса которых совпадают с соответствующими адресами в одной из записей в таблице, то система коммутатора пропускает такие пакеты.

Если IP-адрес отправителя ARP-пакета совпадает с IP-адресом в одной из записей в таблице, а MAC-адрес отправителя ARP-пакета не совпадает, такой ARP-пакет отбрасывается на порте коммутатора.

Следует отметить, что коммутатор будет пропускать или принимать другие ARP-пакеты, IP-адреса отправителей которых не записаны в таблице ARP Spoof Prevention.

Чтобы заполнить поля в записи, перейдите в окно ARP Spoof Prevention Table, показанное на рисунке 16.14.

Затем введите значения IP-адреса в первом текстовом поле в столбце IPv4 Address и MAC-

адреса во втором текстовом поле в столбце MAC Address.

Затем выберите один или несколько номером портов из списка в поле в столбце Port(s).

Следует учитывать, что если не будут выбраны определенные порты из списка, защитная функция будет по умолчанию применена ко всем портам.

Затем щелкните с указателем на кнопке Add, чтобы сохранить созданную запись в таблице. В завершение убедитесь, что поле Enabled в строке ARP Spoof Prevention помещено флажком, затем щелкните с указателем на кнопке Update в окне ARP Spoof Prevention Enable.

В таблице должна появиться новая запись, подтверждающая активацию защитного механизма.

Чтобы удалить из таблицы любую отдельную запись, щелкните с указателем на кнопке Remove в соответствующей записи.

Чтобы удалить из таблицы все записи одновременно, щелкните с указателем на кнопке Remove all под таблицей в окне ARP Spoof Prevention.

16.6 Подраздел DHCP Snooping

Злоумышленник может создать в сети поддельный сервер DHCP (протокола динамической конфигурации хост-устройства), чтобы фальсифицировать параметры конфигурации сети, сообщаемые DHCP-клиентам, т.е. указывать неправильные IP-адреса и маски подсети, другие шлюзы и поддельные DNS-серверы.

Цель спуфинг-атаки с имитацией протокола DHCP обычно заключается в том, чтобы перенаправить трафик DHCP-клиента в домен злоумышленника и попытаться перехватить этот трафик.

Иногда это делается с целью просто попытаться помешать установлению сетевого соединения.

Чтобы не позволит злоумышленнику скомпрометировать сетевую безопасность посредством атаки с поддельного DHCP-сервера (спуфинг-атаки с имитацией протокола DHCP), на изделиях Yarus Networks поддерживается функция отслеживания DHCP-пакетов (DHCP Snooping).

Если эта функция активирована на определенных портах управляемого коммутатора, то коммутатор будет пропускать DHCP-сообщения только от защищенных портов, в то время как такие сообщения, принятые от незащищенных портов, будут отбрасываться.

Чтобы активировать функцию отслеживания DHCP-пакетов, установите флажок в поле Enable в строке DHCP Snooping на сетевой странице DHCP Snooping, как показано на рисунке 16.15.

По умолчанию функция отслеживания DHCP-пакетов считает все интерфейсы незащищенными. Чтобы присвоить определенным портам статус защищенных портов, просто установите флажок в поле Trust в соответствующих строках.

В завершение щелкните с указателем на кнопке Update в нижней части сетевой страницы, чтобы активировать функцию отслеживания DHCP-пакетов на выбранных портах.

ПРИМЕЧАНИЕ: в нижней части окна имеется таблица DHCP Data, в которой выводится

информация о связывании IP адресов с MAC-адресами, запрашивающих портах и времени владения для протокола DHCP. Чтобы просмотреть актуальные данные в таблице связывания, щелкните с указателем на кнопке Refresh.

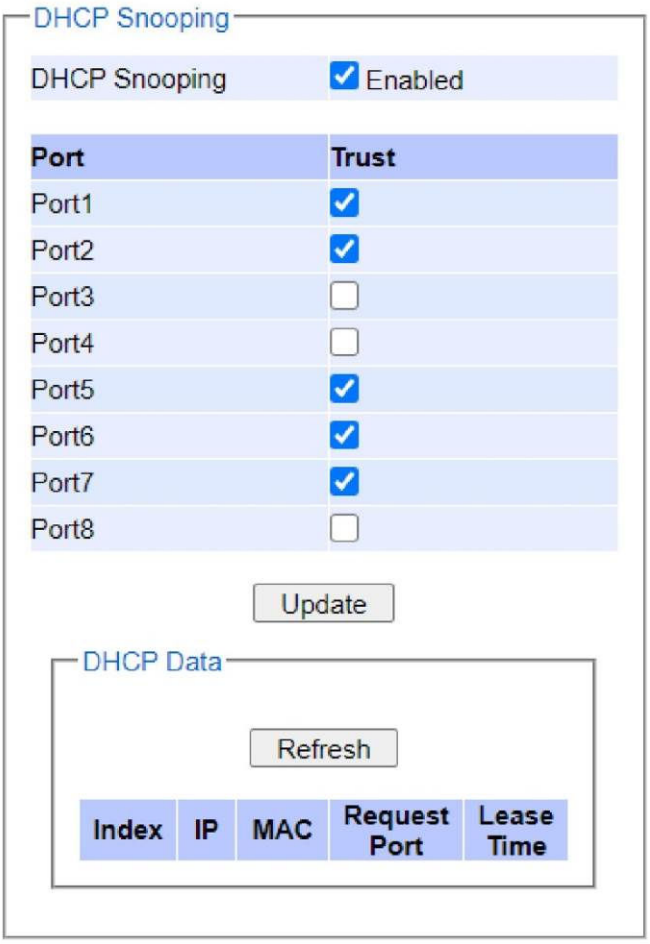


Рисунок 16.15. Сетевая страница подраздела DHCP Snooping.

16.7 Подраздел ACL (список управления доступом)

Список управления доступом (ACL) представляет собой механизм, который используется для управления доступом к сети.

В этом подразделе пользователь может настроить правила фильтрации, используя которые коммутатор будет принимать или отбрасывать определенные пакеты.

Коммутаторы поддерживают фильтры следующих двух типов:

1) на уровне управления доступом к среде передачи,

2) на уровне IP-протокола.

В общей сложности можно задать до 128 правил сопоставления. Однако существуют основные правила, которые используются чаще всего.

Правила для фильтрации на уровне управления доступом к среде передачи включают MAC-адрес, идентификатор VLAN или тип Ethernet.

Правила для фильтрации на уровне интернет-протокола включают протокол IP, IP-адрес, порт TCP/UDP, тип сервиса для версии IPv4 или класс трафика для версии IPv6.

Когда активирован режим фильтрации, для проверки соответствия принятых пакетов применяются правила сопоставления.

Если совпадение найдено, пакет отбрасывается; если нет - принимается.

ПРИМЕЧАНИЕ: далее по тексту правила сопоставления будут упоминаться, как записи в списке управления доступом (списке ACL).

Сетевая страница ACL показана на рисунке 16.16.

Для упрощения идентификации всем записям в списке ACL присваиваются порядковые номера от 1 до 128.

Сначала в списке ACL проверяются записи с более высоким приоритетом.

Записи с низким приоритетом проверяются в последнюю очередь.

Поле Name используется для указания имени правила.

В поле Filter можно выбрать тип фильтрации: на уровне управления доступом к среде передачи ("Mac Base") или на уровне интернет-протокола ("IPv4 Base" или "IPv6 Base").

Следует учитывать, что при изменении значения в поле с Mac Base на IP Base и наоборот обязательные параметры для настройки списка ACL также изменятся соответственно.

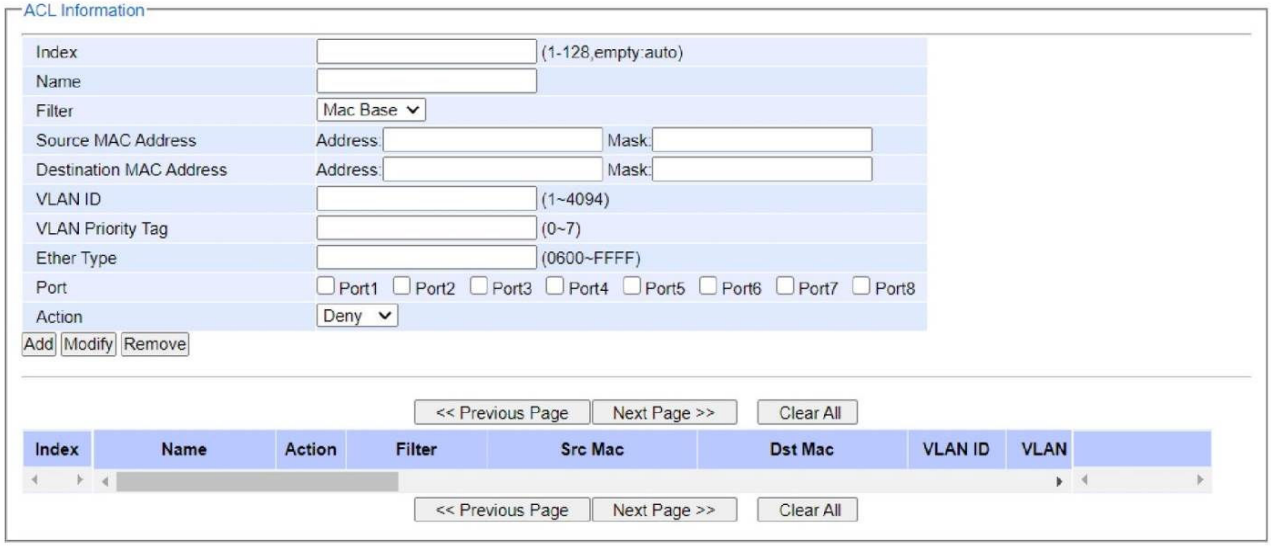


Рисунок 16.16. Сетевая страница информации о списке управления доступом (для режима фильтрации на основе MAC-адресов).

Как показано на рисунке, основные записи в списке ACL для фильтрации на уровне управления доступом к среде передачи (также называется фильтрацией второго уровня) включают: MAC address, VLAN ID, VLAN Priority Tag и Ether Type.

Подробное описание каждой записи приведено в таблице 16.6.

Здесь следует отметить, если какое-либо поле останется незаполненным, соответствующая запись в списке ACL будет проигнорирована.

Таблица 16.6. Описание основных записей в списке ACL для фильтрации второго уровня, которые отображаются на странице раздела ACL.

Запись в списке ACL	Определение	Диапазон
Source MAC Address, Destination MAC Address	MAC-адреса указываются в полях заголовка кадра Ethernet. В поле Mask указывается битовая маска для сравнения диапазонов.	Каждый ненулевой бит в маске сравнивается с соответствующим битом в IP-адресе. Если указано значение маски 0.0.0.0, ограничение по этому параметру не применяется. Если пользователь не заполняет поле Mask, принимается значение маски 255.255.255.255. При таком значении сравниваются все биты в IP-адресе.
VLAN ID	В поле VLAN ID указывается тег 802.1Q VLAN в заголовке кадра Ethernet. Если созданы агрегированные порты, они также выводятся в списке портов. Если нужно выбрать агрегированный порт, убедитесь, в списке ACL отсутствуют записи с физическими портами, которые являются членами выбираемого агрегированного порта.	Данный параметр может принимать значение в диапазоне от 1 до 4094.
VLAN Priority Tag	В поле VLAN Priority Tag указывается значение, проверяемое в поле Priority тега 802.1Q VLAN в заголовке кадра Ethernet.	Данный параметр может принимать значение в диапазоне от 0 до 7.
Ether Type	Соответствует значению в поле Ethernet type в заголовке кадра Ethernet. Ниже приведены примеры. Значение 0x8000 указывает на IPv4-пакет. Значение 0x86DD указывает на IPv6-пакет. Значение 0x8100 указывает на 802.1Q-пакет.	Данный параметр может принимать значение в диапазоне от 0x0600 до 0xFFFF.

Основные записи ACL для фильтрации по IP-уровню (также называемой фильтрацией L3), как показано на рисунке 16.17, включают IP-протокол, IP-адрес источника, IP-адрес назначения, порт источника TCP/UDP, порт назначения TCP/UDP и TOS. В таблице 16.7 подробно описано определение каждого из них. Обратите внимание, что если какое-либо поле пусто, то эта запись ACL будет проигнорирована.

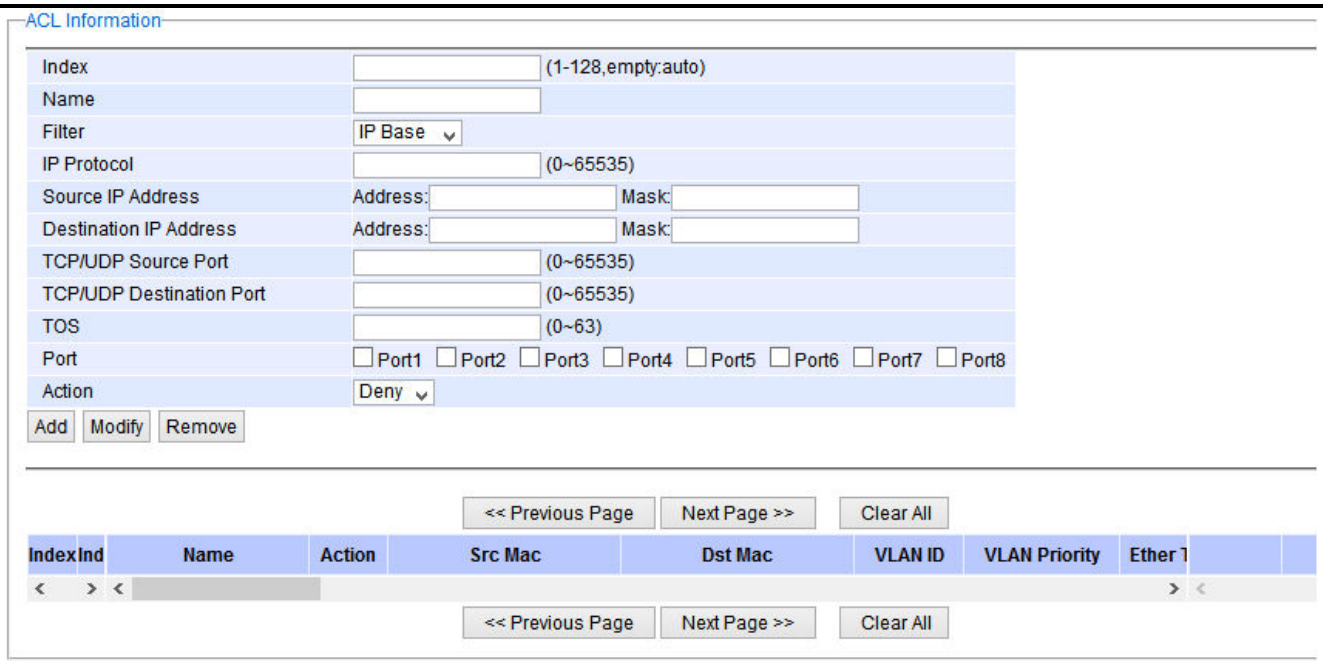


Рисунок 16.17. Сетевая страница информации о списке управления доступом (для режима фильтрации на основе IPv4-адресов).

Таблица 16.7. Описание основных записей в списке ACL для фильтрации третьего уровня, которые отображаются на странице раздела ACL.

Запись в списке ACL	Определение	Диапазон
IP Protocol	Соответствует значению в поле Protocol заголовка IPv4-пакета. Ниже приведены примеры. Значение 1 указывает на пакет протокола ICMP. Значение 6 указывает на пакет протокола TCP. Значение 17 указывает на пакет протокола UDP.	Данный параметр может принимать значение в диапазоне от 0 до 255.
Source or Destination IP Addresses	IP-адреса указываются в полях заголовка IPv4 или IPv6-пакета. В поле Mask указывается битовая маска для сравнения диапазонов.	Для версии IPv4: Каждый ненулевой бит в маске сравнивается с соответствующим битом в IP-адресе. Если указано значение маски 0.0.0.0, ограничение по этому параметру не применяется. Если пользователь не заполняет поле Mask, принимается значение маски 255:255:255:255. При таком значении сравниваются все биты в IP-адресе. Для версии IPv6: Каждый ненулевой бит в маске сравнивается с соответствующим битом в IP-адресе. Если указано значение маски 0.0.0.0.0.0, ограничение по этому параметру не применяется. Если пользователь не заполняет поле Mask, принимается значение маски FF:FF:FF:FF:FF:FF. При таком значении сравниваются все биты в IP-адресе.

Запись в списке ACL	Определение	Диапазон
TCP/UDP Source Port / TCP/UDP Destination Port	Соответствующие значения указываются в полях заголовка кадра TCP/UDP. Значение в этом поле используется для фильтрации по прикладным сервисам. Например, порт назначения 21 протокола TCP предназначен для сервиса протокола передачи файлов (FTP), порт назначения 23 протокола TCP - для сервиса Telnet, а порт назначения 80 протокола TCP - для сервиса гипертекстового транспортного протокола (HTTP). Для выбора портов, на которых будет применяться это правило фильтрации, и выполняемого действия установите флажки у соответствующих портов и выберите опцию "Deny" или "Permit" в поле выбора действия. Если выбрана опция 'Deny', то в случае обнаружения совпадения с записью в списке ACL пакет будет отброшен. При выборе опции 'Permit' пакет будет пропускаться только при обнаружении совпадения.	Данный параметр может принимать значение в диапазоне от 0 до 65535.
TOS (Type of Service)	Соответствует значению в поле кода дифференцирования трафика (DSCP) в заголовке IPv4-пакета. Значение в этом поле используется для обеспечения качества сервиса (QoS).	Данный параметр может принимать значение в диапазоне от 0 до 255.

Таблица 16.8. Сводная информация по именам параметров, описанию и заводским настройкам по умолчанию для фильтрации по списку ACL.

Имя параметра	Описание	Заводская настройка по умолчанию
Index	Уровень приоритета (1 – 128)	Не заполняется
Name	Максимальная длина – 32.	Не заполняется
Filter	Режим фильтрации: Mac Base / IPv4 Base / IPv6 Base.	Mac Base
Source MAC Address, Mask	MAC-адрес указывается в формате A:B:C:D:E:F. Значение Mask указывается для проверки битовой маски. Если вводится значение 0.0.0.0.0.0, ограничение не применяется. Если поле не заполняется, по умолчанию принимается значение FF:FF:FF:FF:FF:FF.	Не заполняется
Destination MAC Address, Mask	MAC-адрес указывается в формате A:B:C:D:E:F. Значение Mask указывается для проверки битовой маски. Если вводится значение 0.0.0.0.0.0, ограничение не применяется. Если поле не заполняется, по умолчанию принимается значение FF:FF:FF:FF:FF:FF.	Не заполняется
VLAN ID	1 - 4094	Не заполняется
VLAN Priority Tag	0 ~ 7	Не заполняется
Ether Type	0x0600 - 0xFFFF	Не заполняется
IP Protocol	0 - 255	NONE
Next Header	0 - 255	Не заполняется

Имя параметра	Описание	Заводская настройка по умолчанию
Source IP Address	IP-адрес указывается в формате A.B.C.D. Значение Mask указывается для проверки битовой маски. Если вводится значение 0.0.0.0, ограничение не применяется. Если поле не заполняется, по умолчанию принимается значение 255.255.255.255.	Не заполняется
Destination IP Address	IP-адрес указывается в формате A.B.C.D. Значение Mask указывается для проверки битовой маски. Если вводится значение 0.0.0.0, ограничение не применяется. Если поле не заполняется, по умолчанию принимается значение 255.255.255.255.	Не заполняется
TCP/UDP Source Port	0 - 65535	Не заполняется
TCP/UDP Destination Port	0 - 65535	Не заполняется
TOS	0 - 255	Не заполняется
Port	1, 2, 3, 4, 5, 6, 7,8	Не заполняется
Action	Deny/Permit	Не заполняется

Пользователь может использовать кнопки Add, Modify или Remove для удаления записи из списка ACL. Выбор записи для совершения действия осуществляется в поле Index, как показано на рисунках. В нижней части сетевой страницы ACL Information выводится список всех записей в списке ACL.

При необходимости список можно перелистывать в любую сторону, используя кнопки Previous Page и Next Page.

Чтобы удалить все записи из списка ACL, щелкните с указателем на кнопке Clear All.

16.8 Подраздел Dynamic ARP Inspection

Функция динамического контроля протокола ARP (DAI) представляет собой еще одну функцию безопасности, поддерживаемую управляемыми коммутаторами. Она предназначена для защиты от атак через посредника.

Во время такой атаки узел злоумышленника перехватывает пакеты, предназначенные для других узлов, отравляя кэши протокола ARP ничего не подозревающих соседей.

Инициируя атаку, узел злоумышленника передает ARP-пакеты с запросами или ответами, в которых IP-адреса других узлов привязываются к его собственному MAC-адресу.

Чтобы обеспечить надежную защиту от атак этого класса, управляемый коммутатор выполняет переадресацию только действительных запросов и ответов протокола ARP.

При этом недействительные и подозрительные ARP-пакеты отбрасываются коммутатором. Функция DAI использует механизм функции отслеживания DHCP-пакетов, которая контролирует обмен сообщениями по протоколу DHCP. По результатам отслеживания функция DAI создает базу данных допустимых кортежей MAC-адресов и IP-адресов.

Функция DAI связана с функцией предотвращения имитации протокола ARP.

Функция DAI отбросит любой ARP-пакет, если связка IP-адреса и MAC-адреса в пакете не совпадает с записью в базе данных функции отслеживания DHCP-пакетов. Если нужно пропускать пакеты, переданные с определенных статических IP-адресов, пользователь должен добавить соответствующие пары IP-адресов и MAC-адресов на сетевой странице ARP Spoof Prevention.

Статическое связывание может оказаться полезным для узлов со статическими IP-адресами, а также в условиях, когда функция отслеживания DHCP-пакетов не может быть использована, либо другие коммутаторы в сети не поддерживают динамический режим.

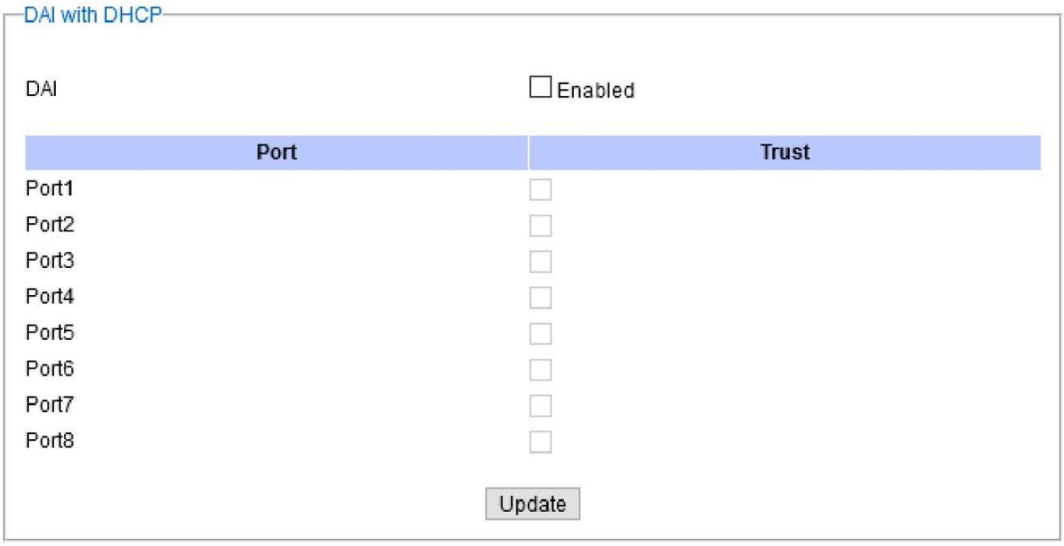


Рисунок 16.18. Сетевая страница Dynamic ARP Inspection with DHCP.

Чтобы активировать функцию DAI, установите флажок в поле Enabled в строе DAI в окне DAI with DHCP, которое показано на рисунке 16.18.

Затем установите флажки в столбце Trust в строках с номерами портов, которым присвоен статус защищенных потов.

После этого щелкните с указателем на кнопке Update. В таблице в окне DHCP Data выводится информация о связывании IP адресов с MAC-адресами, запрашивающих портах и времени владения для протокола DHCP.

Чтобы просмотреть актуальные данные в таблице связывания, щелкните с указателем на кнопке Refresh.

ПРИМЕЧАНИЕ: если функция отслеживания DHCP-пакетов не была активирована перед попыткой активации функции динамического контроля протокола ARP с использованием протокола DHCP, система выдаст сообщение об ошибке, показанное на рисунке 16.19.

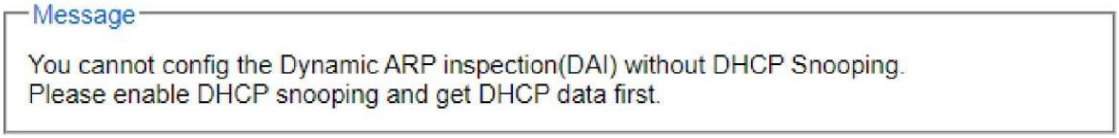


Рисунок 16.19. Сообщение об ошибке динамического контроля протокола ARP (не активирована функция отслеживания DHCP-пакетов).

17 РАЗДЕЛ ERPS RING

Протокол защитного переключения для кольца Ethernet предназначен для использования в кольцевых сетях уровня Ethernet. Этот протокол поддерживает защитный механизм восстановления при отказе с задержкой не больше 50 мсек (sub-50ms).

Применение кольцевой топологии позволяет сократить количество каналов и оптимизировать многоточечную связность.

Функция ERPS обеспечивает высоконадежную и устойчивую защиту сети с кольцевой топологией, предотвращая образование петель, которые могут нарушать нормальную работу сети и влиять на доступность сервисов.

На рисунке 17.1 приведен пример кольцевой топологии, образованной четырьмя управляемыми коммутаторами серии YN-SI2510A.

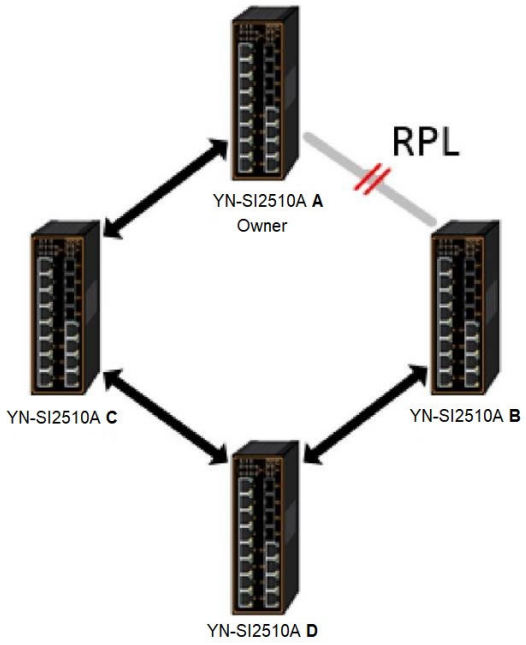


Рисунок 17.1. Пример кольцевой топологии (в качестве примера приведен коммутатор YN-SI2510A-4GC-8FE).

Как показано на рисунке, каждый узел Ethernet-кольца соединяется со смежными узлами того же Ethernet-кольца по двум независимым каналам. Чтобы в Ethernet-кольце не образовывались петли, один канал кольца должен быть все время свободен от трафика, то есть трафик в любой момент времени может протекать по всем кольцевым каналам, кроме одного.

Этот специальный канал называется каналом защиты кольца (RPL).

Активация и отключение канала RPL осуществляется посредством передачи специальных сообщений.

Такое сообщение называется "переключатель автоматической защиты кольца" (R-APS). В нормальных условиях этот канал блокируется узлом Owner.

Таким образом этот механизм обеспечивает защиту от петель.

В случае сбоя в Ethernet-кольце специально назначенный узел этого Ethernet-кольца, который

называется RPL Owner, разблокирует RPL-канал со своей стороны, чтобы использовать его в качестве резервного соединения.

Таким образом, канал RPL используется исключительно в качестве резервного канала, предусмотренного на случай отказа в рабочем канале.

Промышленные управляемые коммутаторы поддерживают различные протоколы Ethernet-кольца.

Как показано на рисунке 17.2, раздел ERPS/Ring состоит из шести подразделов, а именно: ERPS Setting, iA-Ring Setting, C-Ring Setting, U-Ring Setting, Compatible-Chain Setting и MRP.

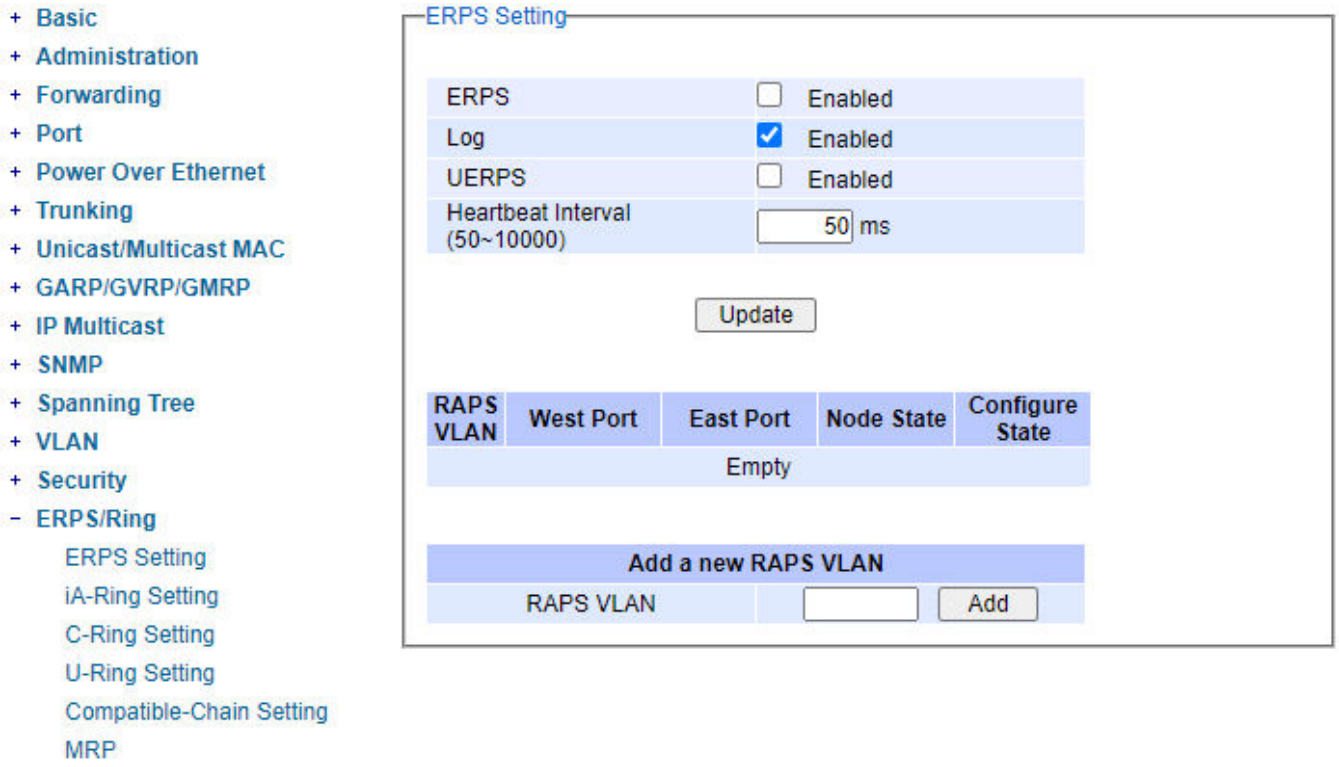


Рисунок 17.2. Раскрывающееся меню раздела ERPS/Ring.

17.1 Подраздел ESRP Setting

Сетевая страница ERPS Setting показана на рисунке 17.3. Следует отметить, что прежде, чем приступать к настройке параметров функции защитного переключения для кольца Ethernet (ERPS), пользователь должен сначала отключить режим управления DIP-переключателями.

Чтобы настроить защитную функцию ERPS на управляемом коммутаторе, выполните следующие действия:

1. Активируйте защитную функцию ERPS, установив флажок в поле Enabled в строке ERPS в окне ERPS Setting.

2. Если пользователь желает регистрировать события, он должен также активировать функцию журналирования, установив флажок в поле Enabled в строке Log.

3. Если пользователь желает, чтобы коммутатор периодически проверял состояние соседних коммутаторов в кольцевой топологии, передавая контрольные heartbeat-пакеты, он может на собственное усмотрение установить флажок в поле Enabled в строке UERPS. Следует отметить,

что после активации этой функции потребуется более длительное время на восстановление кольцевой топологии после отказа.

4. При необходимости пользователь может точно настроить интервал передачи heartbeat-пакетов, введя собственное значение вместо значения по умолчанию, которое составляет 50 миллисекунд.

5. Щелкните с указателем на кнопке Update.

6. Перейдите в окно под названием Add new RAPS VLAN в нижней части сетевой страницы. Введите в поле значение идентификатора VLAN с коммутацией автоматической защиты кольца и щелкните с указателем на кнопке Add.

Упомянутый идентификатор может принимать любое значение в диапазоне от 1 до 4094.

В таблице 17.1 в сводном виде представлено описание полей на сетевой странице настройки параметров функции ERPS.

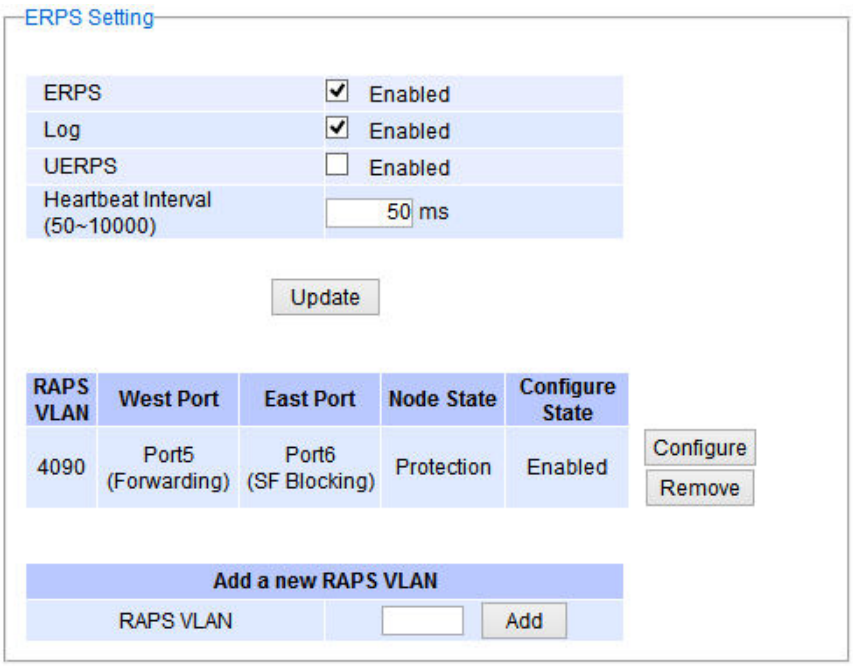


Рисунок 17.3. Сетевая страница настройки параметров функции ERPS.

Таблица 17.1. Описание настраиваемых параметров функции ERPS.

Имя параметра	**Описание**	**Заводская настройка по умолчанию**
ERPS	В этом поле можно активировать или отключить защитную функцию ERPS.	Отключено
Log	В этом поле можно активировать журналирование.	Активировано

Имя параметра	Описание	Заводская настройка по умолчанию
UERPS	В этом поле можно активировать режим UERPS. Если функция UERPS активирована, порты устройства, подключенные к кольцевой сети, периодически передают heartbeat-пакеты на порты одноранговых устройств в той же кольцевой сети, чтобы определить рабочее состояние канала (например, беспроводного моста). Если порт однорангового устройства в кольцевой сети не получает heartbeat-пакет в течение трех интервалов передачи, то соответствующий порт коммутатора, подключенный к кольцевой сети, переводится в режим защиты. **Примечание:** после активации этой функции время восстановления увеличивается больше, чем на 20 миллисекунд.	Отключено
Heartbeat Interval	Устанавливается интервал передачи heartbeat-пакетов. Принимает значения в диапазоне от 50 до 10000 миллисекунд.	50 мсек.
RAPS VLAN	Для создания кольца указывается идентификатор VLAN с коммутацией автоматической защиты кольца. Идентификатор VLAN принимает значения в диапазоне от 1 до 4094.	4090

7. Щелкните с указателем на кнопке Configure, которая находится в правой части окна в строке VLAN с коммутацией автоматической защиты кольца, идентификатор которой был введен ранее. При этом откроется новая сетевая страница, на которой пользователь может настроить дополнительные параметры VLAN с коммутацией автоматической защиты кольца, как показано на рисунке 17.4.

8. Настраиваемые параметры в окне ERPS RAPS VLAN Setting включают Status, West Port, East Port, RPL Owner, RPL Port, WTR Timer, Holdoff Timer, Guard Timer, MEL и Propagate TC. Подробное описание всех этих параметров в сводном виде представлено в таблице 17.2. После ввода значений щелкните с указателем на кнопке Update, чтобы завершить настройку новой VLAN с коммутацией автоматической защиты кольца.

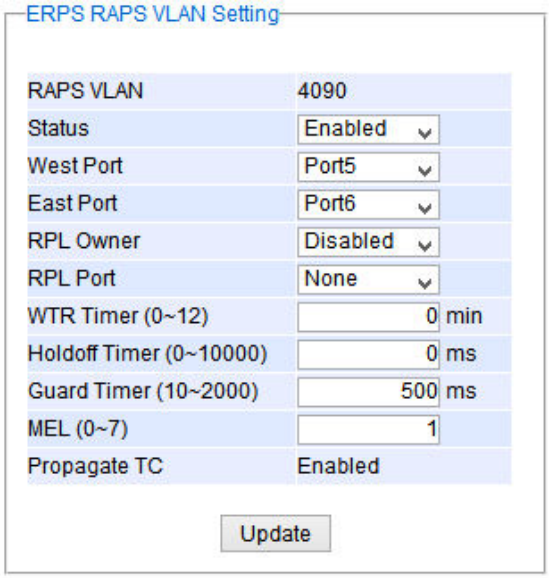


Рисунок 17.4. Сетевая страница настройки параметров VLAN с коммутацией автоматической защиты кольца.

Таблица 17.2. Описание настраиваемых параметров VLAN, использующей функцию ERPS.

Имя параметра	Описание	Заводская настройка по умолчанию
ERPS VLAN	В этом поле выводится идентификатор VLAN с коммутацией автоматической защиты кольца, выбранной для настройки параметров.	4090
Status	Выберите опцию Enable, чтобы активировать защитную функцию ERPS для данной VLAN.	Отключено
West Port	Выберите западный порт канала RPL.	Port1
East Port	Выберите восточный порт канала RPL.	Port2
RPL Owner	В этом поле можно активировать функцию Owner.	Отключено
RPL Port	В этом поле выбирается порт Owner, через который контролируется резервный канал. В качестве такового можно назначить западный или восточный порт, либо не назначать никакой порт вообще, выбрав опцию None.	None
WTR Timer	В этом поле устанавливается время ожидания восстановления кольца в минутах. Чем меньше значение, тем меньше время защиты. Параметр WTR Timer может принимать значения в диапазоне от 0 до 12 минут.	5
Holdoff Timer	Установите время задержки срабатывания защиты кольца. Параметр Holdoff Timer может принимать значения в диапазоне от 0 до 10000 миллисекунд.	0
Guard Timer	Установите продолжительность защитного временного интервала для кольца. Параметр Guard Timer может принимать значения в диапазоне от 0 до 2000 миллисекунд.	500
MEL	Установите уровень группы объектов обслуживания для кольца. Параметр MEL может принимать значения в диапазоне от 0 до 7.	1
Propagate TC	В этой строке указывается возможность распространения изменений в топологии кольца.	Активировано

17.1.1 Пример настройки параметров функции ERPS

Для лучшего понимания пользователями процесса настройки защитной функции ERPS на промышленных управляемых коммутаторах YN-SI2510A в данном разделе рассматривается пример настройки параметров этой функции на четырех управляемых коммутаторах Yarus Networks.

Топология кольца показана на рисунке 17.5.

Допустим, кольцевая сеть состоит из коммутаторов YN-SI2510A A, YN-SI2510A B, YN-SI2510A C и YN-SI2510A D. Между устройствами A и B создан канал RPL.

ПРИМЕЧАНИЕ: на рисунке показана модель YN-SI2510A, но схема и описание применимы к коммутаторам любых моделей.

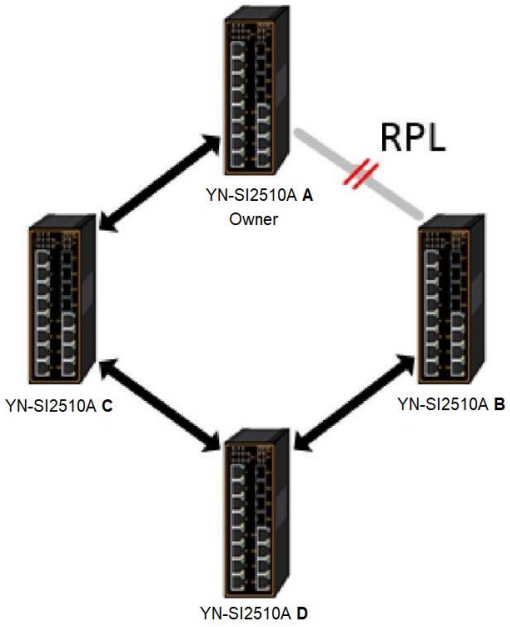


Рисунок 17.5. Пример кольцевой топологии для настройки защитной функции ERPS (в качестве примера приведен коммутатор YN-SI2510A-4GC-8FE).

На каждом коммутаторе следует выполнить процедуру, описанную в предыдущем разделе. Сначала активируем защитную функцию ERPS, затем добавляем VLAN с коммутацией автоматической защиты кольца с идентификатором 8.

На каждом управляемом коммутаторе настроим параметры VLAN с коммутацией автоматической защиты кольца согласно таблице 17.3.

Таблица 17.3. Настройка параметров конфигурации коммутаторов A, B, C и D.

	A	B	C	D
RAPS VLAN	8	8	8	8
ERPS RAPS	Enabled	Enabled	Enabled	Enabled
West Port	1	1	1	1
East Port	2	2	2	2
RPL Owner	Enabled	Disabled	Disabled	Disabled
RPL Port	West	None	None	None

17.1.2 Настройка режима UERPS (необязательно)

Ниже описана процедура настройки режима передачи heartbeat-пакетов (UERPS) в процессе настройки защитной функции ERPS. Данное описание приведено исключительно в качестве примера.

1. Подготовьте два управляемых коммутатора (Коммутаторы A и B). Для избыточности мы будем использовать Порт 7 и Порт 8 на каждом коммутаторе.

2. Подключите Коммутаторы A и B к сети или к ПК, чтобы получить к ним доступ. Чтобы упростить процесс настройки через сеть, пользователь может использовать Порт 1 на каждом коммутаторе.

3. Измените IP-адрес Коммутатора B или адреса обоих коммутаторов, чтобы избежать конфликта IP-адресов.

4. Откройте пользовательский сетевой интерфейс на Коммутаторах A и B и настройте параметры защитной функции ERPS согласно приведенному ниже описанию. Установите флажки в полях Enable в строках ERPS, Log, UERPS, как показано на рисунке 17.6. Затем щелкните с указателем на кнопке Update, чтобы внесенные изменения вступили в силу.

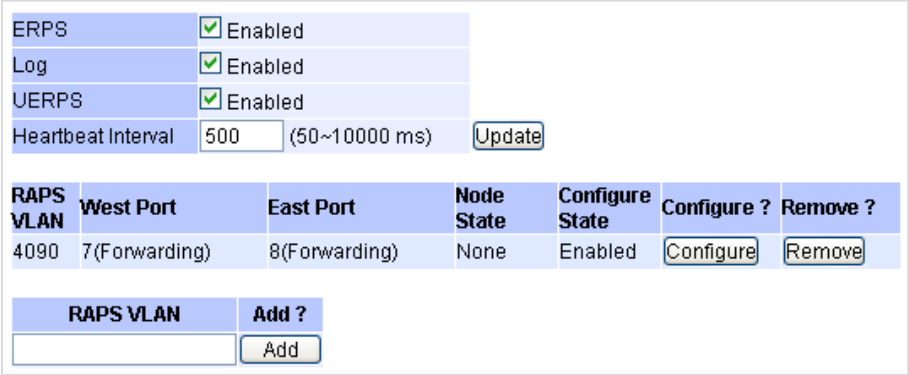


Рисунок 17.6. Пример настройки параметров защитной функции ERPS для Коммутатора A.

5. На Коммутаторе A щелкните с указателем на кнопке Configure в строке с соответствующим идентификатором RAPS VLAN и введите значения настраиваемых параметров, как показано на рисунке 17.7.

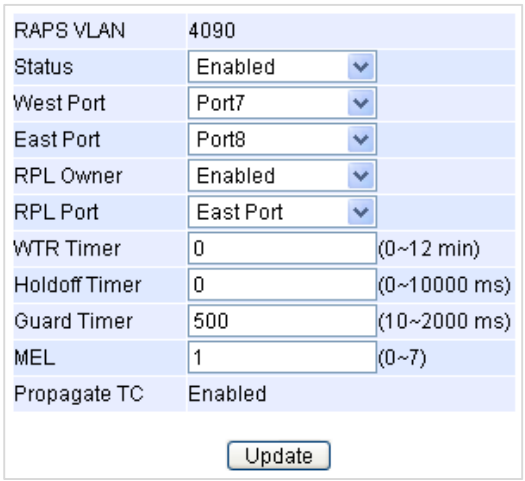


Рисунок 17.7. Пример настройки параметров VLAN с коммутацией автоматической защиты кольца для Коммутатора A.

6. Откройте сетевой пользовательский интерфейс Коммутатора B и введите значения настраиваемых параметров защитной функции ERPS, как показано на рисунке 17.8.

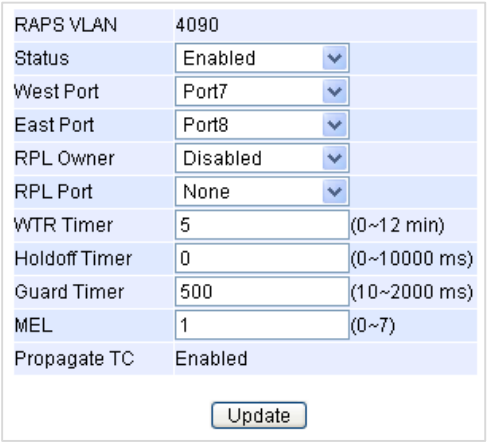


Рисунок 17.8. Пример настройки параметров VLAN с коммутацией автоматической защиты кольца для Коммутатора B.

7. Подключите Порт 7 Коммутатора A к Порту 8 Коммутатора B, а Порт 8 Коммутатора A – к Порту 7 Коммутатора B (как перекрестное соединение) для резервирования портов.

8. Если все выполнено правильно, для Коммутатора A должны отображаться значения параметров защитной функции ERPS, показанные на рисунке 17.9. При этом для Порта 8 должна быть установлена автоматическая блокировка во избежание образования петель в сети.

RAPS VLAN	West Port	East Port	Node State	Configure State	Configure ?	Remove ?
4090	7(Forwarding)	8(Blocking)	Idle	Enabled	Configure	Remove

Рисунок 17.9. Состояние защитной функции ERPS на коммутаторе A.

9. После этого пользователь может добавить другой мост между двумя упомянутыми управляемыми коммутаторами.

17.2 Подраздел iA-Ring Settings

Управляемый коммутатор совместим с протоколом iA-Ring.

Поддержка упомянутого протокола позволяет повысить надежность сети и сократить время восстановления в сетях с топологией кольца с резервированием.

Эта функция подобна функции резервированного кольца, но поддерживает собственный протокол. Технология оказалась весьма успешной. Ее применение позволило сократить время восстановления до меньше 20 миллисекунд.

Протокол iA-Ring может быть применен для любого одинарного кольца, пример которого показан на схеме на рисунке 17.10.

Рисунок 17.10. Пример топологии iA-Ring (в качестве примера приведен коммутатор YN-SI2510A-4GC-8FE).

На рисунке 17.11 показана сетевая страница подраздела iA-Ring Setting.

На этой странице можно активировать протокол избыточности iA-Ring.

ПРИМЕЧАНИЕ: чтобы активировать iA-Ring и настраивать параметры протокола через интернет-браузер, пользователь должен сначала отключить режим управления DIP-переключателями и защитную функцию ERPS.

Для настройки протокола iA-Ring выполните описанные ниже простые действия, сверяясь с рисунком 17.11.

1. Активируйте протокол iA-Ring, выбрав опцию Enabled из выпадающего списка.

2. Активируйте опцию Ring Master, если собираетесь назначить текущий управляемый коммутатор главным устройством кольца.

3. Выберите первый порт кольца из выпадающего списка в строке 1st Ring Port.

4. Выберите второй порт кольца из выпадающего списка в строке 2nd Ring Port.

5. Щелкните с указателем на кнопке Update и сохраните внесенные изменения, чтобы новая конфигурация вступила в силу.

6. Чтобы проверить актуальные настройки протокола iA-Ring, щелкните с указателем на кнопке Refresh.

Обратите внимание, что в нижней части сетевой страницы iA-Ring Setting расположена таблица состояния протокола iA-Ring под заголовком Status, которая включает строки State, 1st Ring Port Status и 2nd Ring Port Status.

Описание настраиваемых параметров протокола iA-Ring в сводном виде представлено в таблице 17.4.

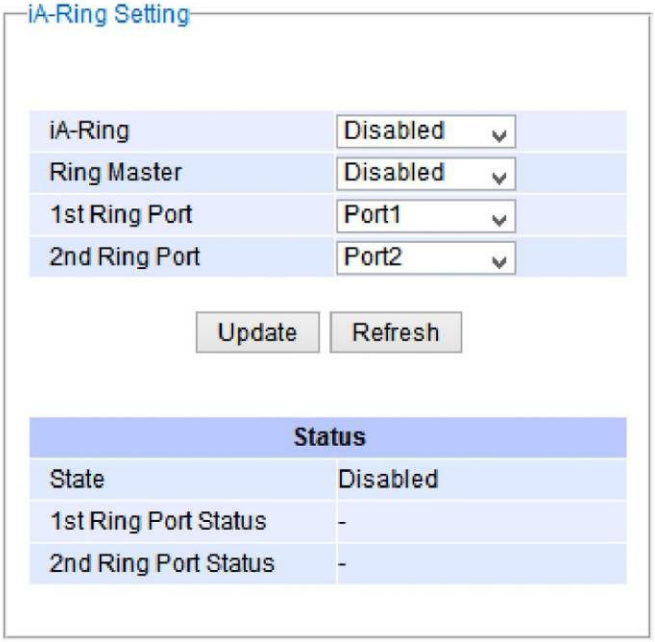


Рисунок 17.11. Сетевая страница настройки параметров протокола iA-Ring.

Таблица 17.4. Описание настраиваемых параметров протокола iA-Ring.

Имя параметра	Описание	Заводская настройка по умолчанию
iA-Ring	Активация или отключение протокола iA-Ring.	Отключено
Ring Master	При выборе опции Enabled: устанавливается режим главного устройства. При выборе опции Disabled: устанавливается режим подчиненного устройства.	Отключено
1st Ring Port	Выбирается первичный порт для протокола iA-Ring.	Port1
2nd Ring Port	Выбирается резервный порт для протокола iA-Ring.	Port2

17.3 Подраздел C-Ring (Compatible Ring) Settings

Протокол кольцевого резервирования C-Ring (совместимое кольцо) в основе своей подобен протоколу iA-Ring. Единственное отличие заключается в том, что первый протокол также можно использовать для колец MOXA.

На рисунке 17.12 показано окно настройки параметров протокола кольцевого резервирования C-Ring.

ПРИМЕЧАНИЕ: чтобы активировать функцию C-Ring и настраивать параметры протокола через интернет-браузер, пользователь должен сначала отключить режим управления DIP-переключателями и защитную функцию ERPS.

Для настройки протокола C-Ring выполните описанные ниже простые действия, сверяясь с рисунком 17.12.

1. Активируйте протокол C-Ring, выбрав опцию Enabled из выпадающего списка.
2. Выберите первый порт кольца из выпадающего списка в строке 1st Ring Port.
3. Выберите второй порт кольца из выпадающего списка в строке 2nd Ring Port.

4. Щелкните с указателем на кнопке Update и сохраните внесенные изменения, чтобы новая конфигурация вступила в силу.

Обратите внимание, что в нижней части сетевой страницы C-Ring Setting расположена таблица состояния протокола C-Ring под заголовком Status, которая включает строки State, 1st Ring Port Status и 2nd Ring Port Status. Описание настраиваемых параметров протокола C-Ring в сводном виде представлено в таблице 17.5.

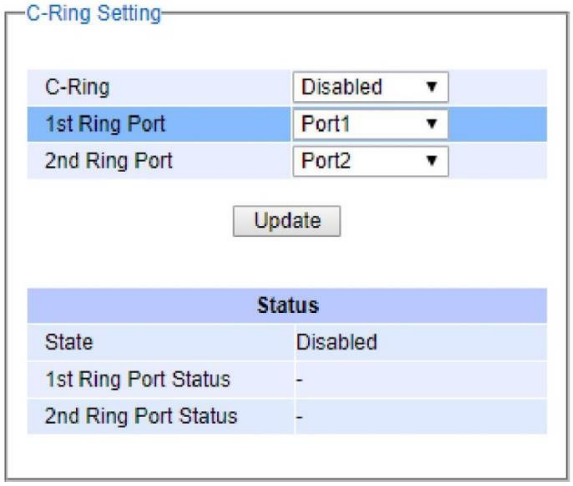


Рисунок 17.12. Сетевая страница настройки параметров протокола C-Ring.

Таблица 17.5. Описание настраиваемых параметров протокола C-Ring.

Имя параметра	Описание	Заводская настройка по умолчанию
C-Ring (Compatible Ring)	Активация или отключение протокола C-Ring.	Отключено
1st Ring Port	Выбирается первичный порт для протокола C-Ring.	Port1
2nd Ring Port	Выбирается резервный порт для протокола C-Ring.	Port2

17.4 Подраздел U-Ring

В данном подразделе пользователь может настраивать параметры протокола U-Ring (одноадресное кольцо) на управляемом коммутаторе.

Протокол U-Ring позволяет устанавливать резервируемое соединение между двумя промышленными управляемыми коммутаторами YN-SI2510A, которые не соединены непосредственно друг с другом на физическом уровне, но связываются через дополнительные сетевые устройства - по два устройства на каждый коммутатор.

Ниже приведены два примера практической реализации протокола U-Ring, которые, как представляется, помогут принять решения о целесообразности применения этой функции.

В первом примере, показанном на рисунке 17.13, представлены два управляемых коммутатора YN-SI2510A-4GC-8FE.

Каждый коммутатор подключается к двум беспроводным точкам доступа через два различных порта Ethernet LAN.

Каждая пара беспроводных точек доступа связывается с другой парой беспроводных точек

доступа, образуя два отдельных беспроводных мостовых соединения.

На схеме, показанной на рисунке 17.13, коммутатор YN-SI2510A A подключается к точке доступа AP 1 через порт 8 и к точке доступа AP 3 через порт 7, а коммутатор YN-SI2510A B - к точке доступа AP 2 через порт 7 и к точке доступа AP 4 через порт 8.

Точки доступа AP 1 и AP 2 поддерживают беспроводное мостовое соединение 1, а точки доступа AP 4 и AP 3 - беспроводное мостовое соединение 2.

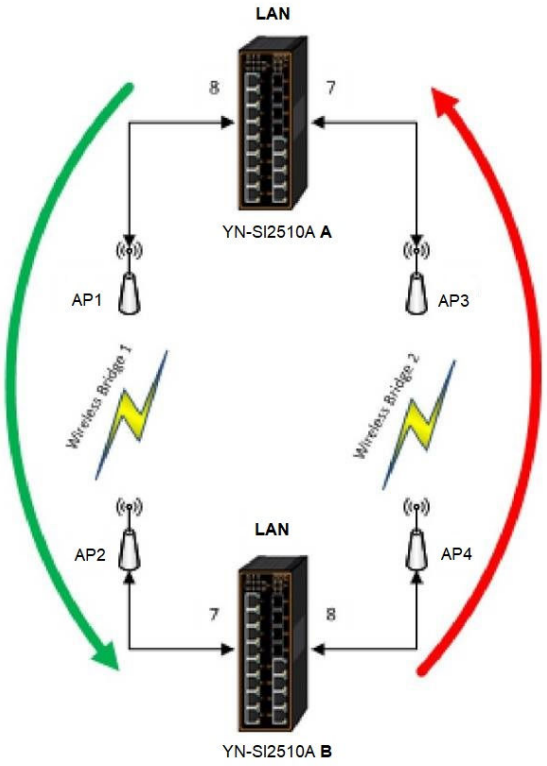


Рисунок 17.13. Пример 1 реализации протокола U-Ring в топологии с двумя беспроводными мостами (в качестве примера приведен коммутатор YN-SI2510A-4GC-8FE).

Во втором примере, показанном на рисунке 17.14, также используются два управляемых коммутатора YN-SI2510A-4GC-8FE.

Каждый коммутатор подключается к двум проводным точкам доступа через два различных порта Ethernet LAN.

Каждая пара проводных точек доступа связывается с другой парой проводных точек доступа, образуя два отдельных проводных мостовых соединения.

На схеме, показанной на рисунке 17.14, коммутатор YN-SI2510A A подключается к точке доступа AP 1 через порт 8 и к точке доступа AP 3 через порт 7, а коммутатор YN-SI2510A B - к точке доступа AP 2 через порт 7 и к точке доступа AP 4 через порт 8.

Точки доступа AP 1 и AP 2 поддерживают проводное мостовое соединение 1, а точки доступа AP 4 и AP 3 - проводное мостовое соединение 2.

Таким образом, между двумя парами точек доступа установлено два физических соединения. В этой среде можно использовать протокол U-Ring. Различие между примерами заключается в том, что во втором примере в качестве устройства точки доступа можно использовать:

- неуправляемый коммутатор,
- трансивер,
- мост xDSL.

Обратите внимание, что если в качестве точки доступа на одной стороне используется неуправляемый коммутатор, то коммутатор с другой стороны соединения также должен быть неуправляемым.

И еще одно важное замечание: внимательно подключайте кабели к портам, чтобы все соединения были выполнены правильно.

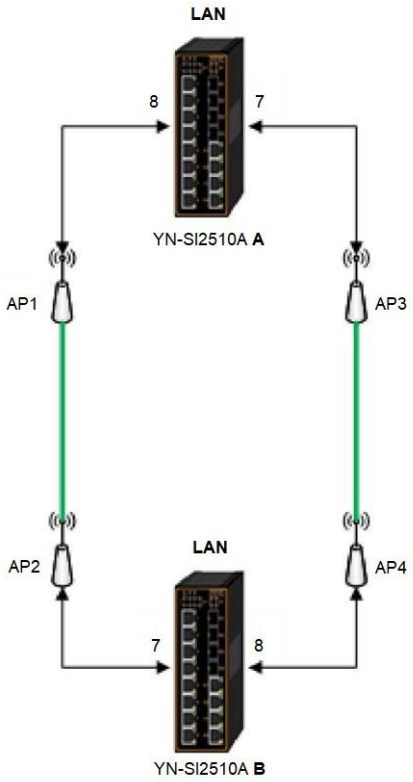


Рисунок 17.14. Пример 2 реализации протокола U-Ring в топологии с двумя проводными мостами (в качестве примера приведен коммутатор YN-SI2510A-4GC-8FE).

Чтобы задействовать протокол U-Ring пользователь должен настроить определенные параметры на сетевой странице U-Ring Setting, показанной на рисунке 17.15.

Для настройки протокола U-Ring выполните следующие простые действия:

1. Активируйте протокол U-Ring, выбрав опцию Enabled из выпадающего списка.

2. Активируйте опцию Ring Master, если собираетесь назначить текущий управляемый коммутатор главным устройством кольца.

3. Выберите первый порт кольца из выпадающего списка в строке 1st Ring Port.

4. Выберите второй порт кольца из выпадающего списка в строке 2nd Ring Port.

5. При необходимости укажите срок жизни heartbeat-пакета в поле Heartbeat Expire, который может принимать значения в диапазоне от 100 до 10000 миллисекунд. Следует отметить, что срок жизни по умолчанию равен 100 миллисекундам.

6. Щелкните с указателем на кнопке Update и сохраните внесенные изменения, чтобы новая

конфигурация вступила в силу.

7. Чтобы проверить актуальные настройки протокола U-Ring, щелкните с указателем на кнопке Refresh.

Обратите внимание, что в нижней части сетевой страницы U-Ring Setting расположена таблица состояния протокола U-Ring под заголовком Status, которая включает строки State, 1st Ring Port Status и 2nd Ring Port Status. Описание настраиваемых параметров протокола U-Ring в сводном виде представлено в таблице 17.6.

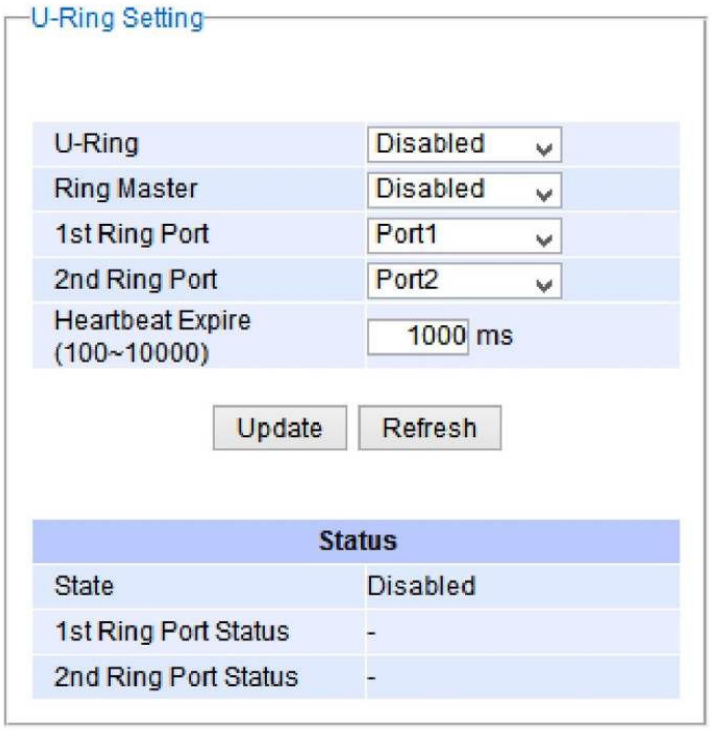


Рисунок 17.15. Сетевая страница настройки параметров протокола U-Ring.

Таблица 17.6. Описание настраиваемых параметров протокола U-Ring.

Имя параметра	Описание	Заводская настройка по умолчанию
U-Ring	Активация или отключение протокола U-Ring.	Отключено
Ring Master	Данная функция активируется только в том случае, если текущий коммутатор предполагается использовать в качестве главного устройства одноадресного кольца. Если коммутатор будет работать, как подчиненное устройство, эта функция должна быть отключена.	Отключено
1st Ring Port	Выбирается порт управляемого коммутатора, который будет первичным портом кольцевой сети.	Port1
2nd Ring Port	Выбирается порт управляемого коммутатора, который будет резервным портом кольцевой сети.	Port2
Heartbeat Expire	Продолжительность интервала передачи контрольных пакетов.	1000
Update	Щелкните с указателем на этой кнопке, чтобы новая конфигурация вступила в силу.	-

Имя параметра	Описание	Заводская настройка по умолчанию
Refresh	Чтобы проверить актуальные настройки протокола U-Ring, щелкните с указателем на этой кнопке.	-
State	Выводится состояние устройства - нормальное или защищенное.	Disable
1st Ring Port Status	Отображается состояние первичного порта кольца.	-
2nd Ring Port Status	Отображается состояние резервного порта кольца.	-

17.5 Подраздел Compatible-Chain Setting

Подраздел Compatible-Chain Setting в меню управляемого коммутатора Yarus Networks предназначен для обеспечения совместимости с протоколом Turbo Chain, который используется на коммутаторах Moxa.

Протокол MOXA Turbo Chain предназначен для использования в сетях с цепочечной топологией для подключения двух оконечных узлов цепи (двух сетевых устройств, таких как промышленные управляемые коммутаторы) к общей LAN.

Такую схему также можно рассматривать, как один из вариантов реализации кольцевой топологии.

Протокол Turbo Chain способен поддерживать избыточность в сетях с топологией любого типа, либо с комплексной топологией, например, в сетях с многокольцевой архитектурой.

Протокол Turbo Chain позволяет создать гибкую и масштабируемую топологию при минимальном времени восстановления среды передачи данных.

Первый коммутатор в сети с топологией Compatible-Chain назначается на роль ведущего устройства (Head). Остальные коммутаторы в сети с топологией Compatible-Chain получают роль устройства-члена (Member).

Последний коммутатор в сети с топологией Compatible-Chain получает роль концевого устройства (Tail).

Первый порт ведущего коммутатора, который подключается к общей LAN, называется ведущим портом, а второй порт, который подключается к следующему коммутатору в топологии Compatible-Chain, называется портом-членом.

Подключаемые порты коммутатора-члена называются первым и вторым портом-членом. Первый порт концевого коммутатора, который подключается к следующему коммутатору, называется портом-членом, а второй порт, который подключается к общей LAN, называется концевым портом.

В конфигурации протокола Turbo Chain ведущий порт образует основной путь, а концевой порт - резервный путь, в результате чего получается избыточная топология.

В процессе нормальной работы цепочки весь трафик в общую LAN передается через ведущей

порт.

В случае если в цепочке происходит отказ, к передаче трафика в общую LAN подключается концевой порт.

Чтобы настроить параметры протокола, выберите пункт меню Compatible-Chain в разделе ERPS/Ring. На рисунке 17.16 показана сетевая страница подраздела Compatible-Chain Setting.

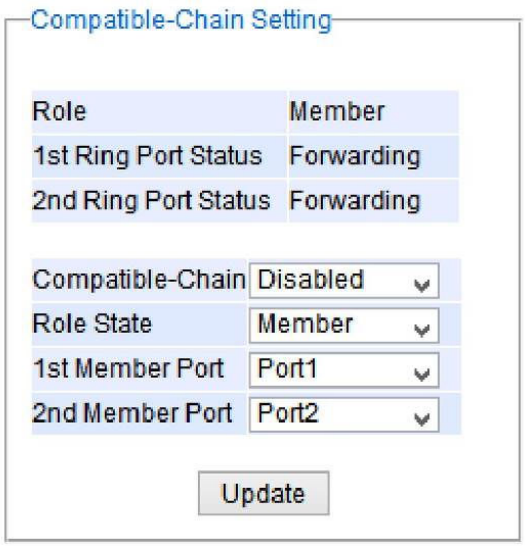


Рисунок 17.16. Сетевая страница настройки параметров протокола Compatible-Chain.

Для настройки протокола Compatible-Chain выполните следующие простые действия:

1. Активируйте протокол Compatible-Chain, выбрав опцию Enabled из выпадающего списка.

2. Выберите роль текущего коммутатора из выпадающего списка в поле Role State – Head (ведущий), Member (член) или Tail (концевой).

3. Если текущему коммутатору присвоен статус ведущего устройства, выберите ведущий порт из выпадающего списка в поле Head Port и порт-член из выпадающего списка в поле Member Port.

4. Если текущий коммутатор выполняет функции устройства-члена, выберите первый порт-член из выпадающего списка в поле 1st Member Port и второй порт-член из выпадающего списка в поле 2nd Member Port.

5. Если текущему коммутатору присвоен статус концевого устройства, выберите концевой порт из выпадающего списка в поле Tail Port и порт-член из выпадающего списка в поле Member Port.

6. Щелкните с указателем на кнопке Update и сохраните внесенные изменения, чтобы новая конфигурация вступила в силу.

Обратите внимание, что в верхней части сетевой страницы Compatible-Chain Setting расположена таблица с данными о статусе текущего коммутатора под заголовком Status, которая включает строки Role, 1st Ring Port Status и 2nd Ring Port Status. Описание настраиваемых параметров протокола Compatible-Chain в сводном виде представлено в таблице 17.7.

Таблица 17.7. Описание настраиваемых параметров протокола Compatible-Chain.

Имя параметра	Описание	Заводская настройка по умолчанию
Role	Отображается роль текущего коммутатора в сети с топологией Compatible-Chain: ведущий, концевой или член.	Член
1st Ring Port Status	Отображается состояние первичного порта кольца.	Переадресация
2nd Ring Port Status	Отображается состояние резервного порта кольца.	Переадресация
Compatible-Chain	Активация или отключение протокола Compatible-Chain.	Отключено
Role State	Выбор роли текущего коммутатора в сети с топологией Compatible-Chain: ведущий, концевой или член.	Член
Head Port	Выбор определенного порта из выпадающего списка на роль ведущего порта протокола Compatible-Chain.	Port1
Tail Port	Выбор определенного порта из выпадающего списка на роль концевого порта протокола Compatible-Chain.	Port1
Member Port	Выбор определенного порта из выпадающего списка на роль порта-члена протокола Compatible-Chain.	Port2
1st Member Port	Выбор определенного порта из выпадающего списка на роль порта-члена протокола Compatible-Chain.	Port1
2nd Member Port	Выбор определенного порта из выпадающего списка на роль порта-члена протокола Compatible-Chain.	Port2

17.6 Подраздел MRP

Протокол резервирования среды передачи (MRP) представляет собой стандартный сетевой протокол передачи данных, разработанный для коммутаторов Ethernet

Международной электротехнической комиссией (IEC) и описанный в стандарте IEC 62439 - 2. Протокол MRP применяется, главным образом, в промышленных Ethernet-системах, для которых он и был разработан.

Его применение позволяет решить проблему единичных отказов в кольцах сетевых коммутаторов Ethernet.

При этом восстановление происходит намного быстрее по сравнению с протоколом связующего дерева.

Он действительно обеспечивает очень быстрое восстановление после отказа. Например, в наихудшем сценарии время восстановления после отказа в сети с 14 коммутаторами составляет приблизительно 10 миллисекунд, а в сети с 50 коммутаторами - приблизительно 30 миллисекунд.

Протокол MRP имеет следующие отличительные особенности:

- Работает на уровне управления доступом к среде передачи сетевых коммутаторов Ethernet.

- Поддерживает кольцевую топологию.
- Обеспечивает восстановление после любого единичного отказа.
- Коммутатору в сети можно назначить один из двух статусов:
  1. менеджер кольца (менеджер протокола MRP),
  2. клиент кольца (клиент протокола MRP).
- Для портов кольцевой сети предусмотрено три возможных состояния: отключен, заблокирован или включен в режиме переадресации.
  1. Отключенные порты кольцевой сети отбрасывают все принятые кадры.
  2. Заблокированные порты кольцевой сети отбрасывают все принятые кадры, за исключением управляющих кадров протокола MRP.
  3. Порты кольцевой сети в состоянии переадресации переадресовывают все принятые кадры.
- В нормальных условиях один из портов кольцевой сети менеджера протокола MRP всегда заблокирован, чтобы избежать образования петель, а оба порта кольцевой сети каждого клиента протокола MRP работают в режиме переадресации.
- В случае отказа в кольце другой порт менеджера протокола MRP активируется и начинает работать в режиме переадресации.

Меню протокола резервирования среды передачи (MRP) в разделе EPRS/Ring позволяет настроить резервируемую связь по протоколу PROFINET в сети с кольцевой топологией без использования дополнительных коммутаторов. На рисунке 17.17 показана сетевая страница подраздела MRP Setting. Для настройки функции MRP протокола PROFINET выполните следующие действия:

1. Введите значение идентификатора VLAN в поле VLAN в нижней части сетевой страницы MRP Setting и щелкните с указателем на кнопке Add, как показано на рисунке 17.17.

Рисунок 17.17. Сетевая страница настройки параметров протокола MRP.

2. После того как будет создано резервированное кольцо MRP с заданной VLAN, появится соответствующая запись в таблице в верхней части страницы, как показано на рисунке 17.18. В конце записи появятся две кнопки: Configure и Remove. Пользователь может щелкнуть с указателем на кнопке Configure, чтобы продолжить настройку параметров резервированного кольца MRP на управляемом коммутаторе.

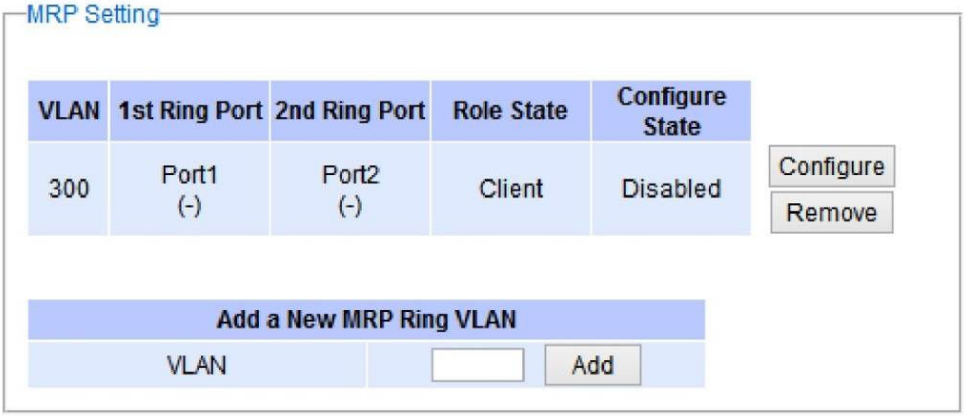


Рисунок 17.18. Пример записи VLAN с поддержкой протокола MRP в сети PROFINET.

Таблица 17.8. Описание настраиваемых параметров протокола MRP.

Имя параметра	Описание	Заводская настройка по умолчанию
VLAN	Идентификатор VLAN резервированного кольца MRP.	В зависимости от конфигурации
Role State	Выбор роли устройства (менеджер или клиент).	Клиент
1st Ring Port	Номер порта и состояние порта (Link Down, Blocked, Forwarding).	Port1
2nd Ring Port	Номер порта и состояние порта (Link Down, Blocked, Forwarding).	Port2
Configure State	Активация или отключение функции резервированного кольца MRP.	Отключено

3. После щелчка на кнопке Configure в соответствующей записи откроется сетевая страница настройки параметров резервированного кольца MRP под заголовком MRP Ring Setting, которая показана на рисунке 17.19.

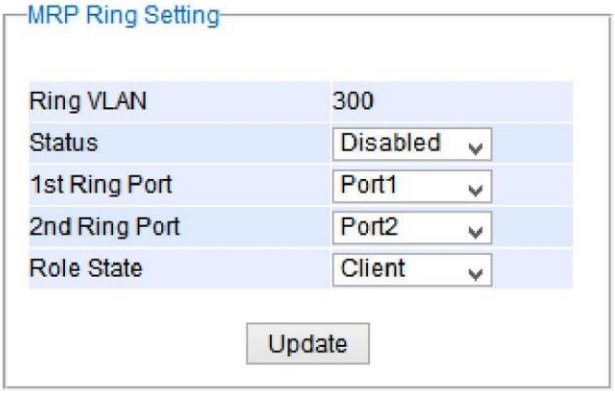


Рисунок 17.19. Сетевая страница настройки параметров резервированного кольца MRP.

4. Здесь пользователь может выбирать значения настраиваемых параметров резервированного кольца MRP для текущего коммутатора в полях Status, 1st Ring Port, 2nd Ring Port и Role State согласно описанию, приведенному выше. Описание настраиваемых параметров резервированного кольца MRP в сводном виде представлено в таблице 17.9.

5. Щелкните с указателем на кнопке Update, чтобы новая конфигурация вступила в силу.

ПРИМЕЧАНИЕ: если на управляемом коммутаторе уже настроена другая кольцевая

топология с поддержкой защитной функции ERPS, система выведет сообщение об ошибке, показанное на рисунке 17.20. Поэтому, прежде чем настраивать резервированное кольцо MRP, пользователь должен отключить функцию ERPS/Ringи режим управления DIP-переключателями.

Рисунок 17.20. Сообщение об ошибке при настройке параметров резервированного кольца MRP.

Таблица 17.9. Описание настраиваемых параметров протокола MRP.

Имя параметра	**Описание**	**Заводская настройка по умолчанию**
Ring Vlan	Выбор роли устройства (менеджер или клиент).	В зависимости от конфигурации
Status	Отключена или включена функция кольца.	Отключено
1st Ring Port	Выберите 1-й кольцевой порт из выпадающего списка.	Port1
2nd Ring Port	Выберите 2-й кольцевой порт из выпадающего списка.	Port2
Configure State	Выберите статус роли, чтобы быть либо клиентом Ring, либо менеджером Ring.	клиент

18 РАЗДЕЛ LLDP

Протокол обнаружения канального уровня (LLDP) представляет собой стандартный протокол второго уровня взаимодействия открытых систем, описанный в спецификации IEEE802.1ab. Протокол LLDP позволяет устройствам в сети Ethernet распространять информацию о себе, включая данные о конфигурации устройства и его возможностях, а также идентификационные данные.

Пакеты-объявления периодически передаются на непосредственно подключенные устройства, которые также используют протокол LLDP, или так называемые "LLDP-соседи".

Протокол LLDP представляет собой "одноперехoдный" однонаправленный протокол, который работает в режиме распространения объявлений.

Данные протокола LLDP могут быть только переданы или приняты устройством без запросов и изменения состояния. На любом устройстве можно независимо активировать или отключить передачу и прием таких сообщений.

Сообщения с объявлениями не переадресовываются на другие устройства в сети.

Протокол LLDP работает под управлением протокола SNMP. Задачи, для решения которых используется этот протокол, включают распознавание топологии, управление ресурсами, экстренное обслуживание, назначение VLAN и управление питанием через кабели передачи данных.

Как показано на рисунке 18.1, раздел LLDP состоит из двух подразделов - LLDP Setting и LLDP Neighbors.

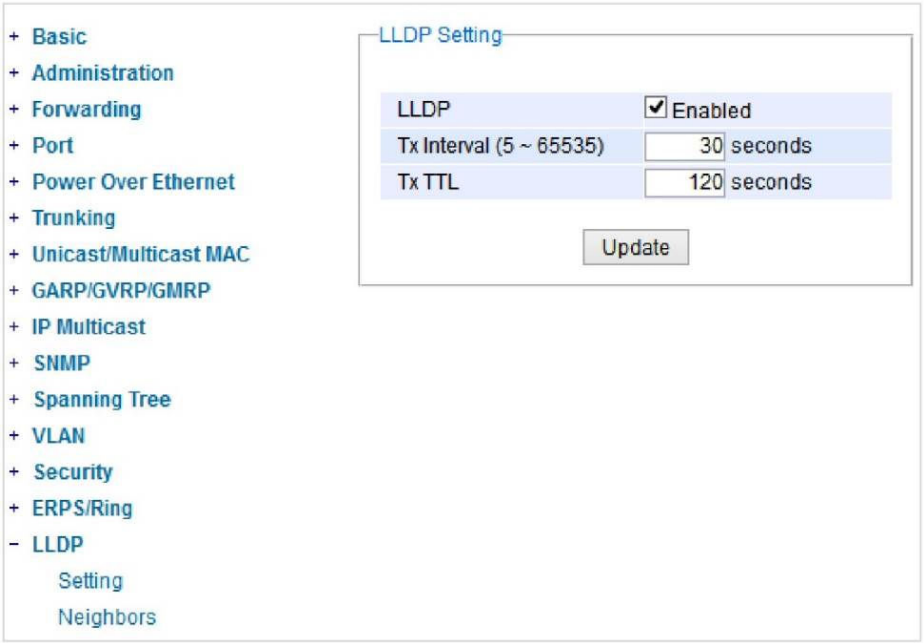


Рисунок 18.1. Раскрывающееся меню раздела LLDP.

18.1 Подраздел LLDP Settings

На рисунке 18.2 показана сетевая страница подраздела LLDP Setting, на которой пользователь

может на собственное усмотрение активировать или отключать протокол LLDP, а также настраивать параметры передачи по этому протоколу.

В таблице 18.1 представлено описание настраиваемых параметров протокола LLDP, которые включают интервал передачи и время существования пакетов-объявлений протокола LLDP.

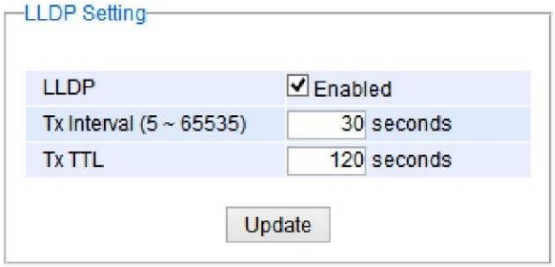


Рисунок 18.2. Сетевая страница настройки параметров протокола LLDP.

Таблица 18.1. Описание настраиваемых параметров протокола LLDP.

Имя параметра	Описание	Заводская настройка по умолчанию
LLDP	Активация или отключение протокола LLDP.	Активировано
Tx Interval	Устанавливается интервал передачи сообщений протокола LLDP. Принимает значения в диапазоне от 5 до 65535 секунд.	30
TxTTL	Время существования пакета. Время, в течение которого хранится информация о соседях. Рекомендованное значение TTL – в четыре раза больше значения Tx Interval. Информация удаляется только после завершения отсчета заданного времени. Принимает значения в диапазоне от 5 до 65535 секунд.	120

18.2 Подраздел LLDP Neighbors

В этом подразделе пользователь может вводить в систему управляемого коммутатора данные о соседе, использующем протокол LLDP.

Страница подраздела показана на рисунке 18.3. Таблица информации о соседях под заголовком Neighbor Information состоит из столбцов Chassis ID, Port ID, Port Description, Device Name, Device Description и Management Address, в которых указывается информация для каждого порта управляемого коммутатора.

Пользователь может щелкнуть с указателем на кнопке Refresh, чтобы получить актуальную информацию в таблице Neighbor Information, или на кнопке Clear, чтобы удалить всю информацию из таблицы.

Пример таблицы с информацией о соседях показан на рисунке 18.4.

Следует отметить, что в данном примере показано окно, применявшееся в ранней версии управляемого коммутатора YN-SI2510A.

В последней версии микропрограммного обеспечения коммутаторов столбец Device Name

переименован в System Name, а столбец Device Description – в System Description.

В таблице 18.2 в сводном виде представлено описание всех столбцов таблицы информации о соседях, использующих протокол LLDP.

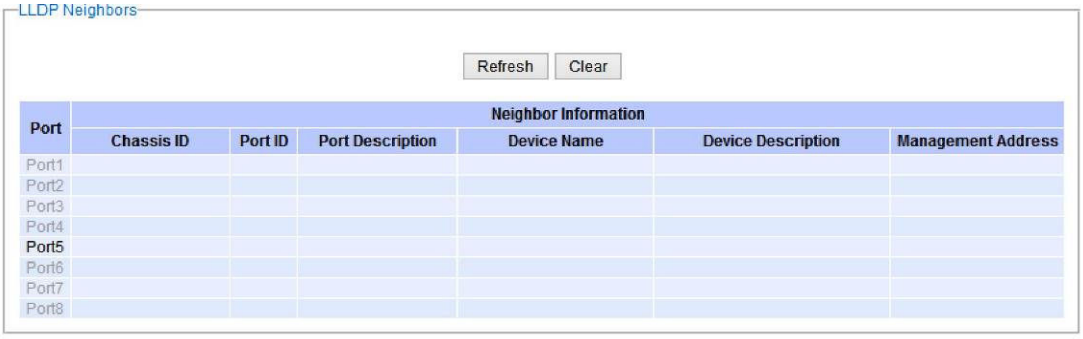


Рисунок 18.3. Сетевая страница подраздела LLDP Neighbors.

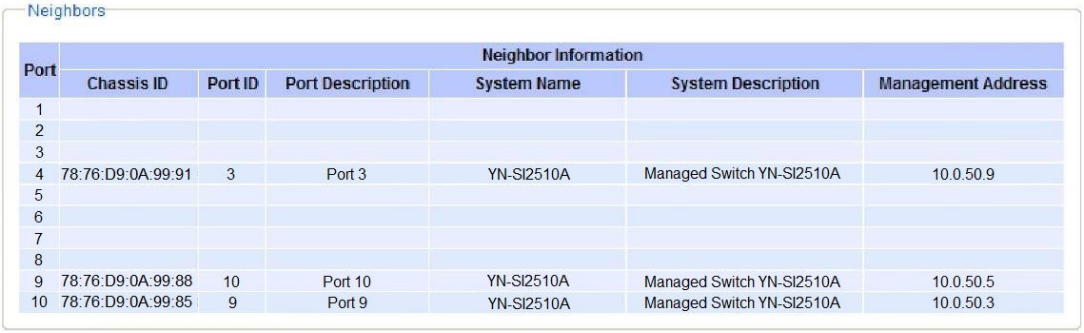


Рисунок 18.4. Пример сетевой страницы с информацией о соседях, поддерживающих протокол LLDP.

Таблица 18.2. Описание сетевой страницы подраздела LLDP Neighbors.

Имя параметра	Описание
Port	Указан номер порта коммутатора.
Chassis ID	Указаны идентификационные данные соседа, соединенного с этим портом.
Port ID	Указан номер порта данного соседа.
Port Description	Приведено текстовое описание порта соседа.
Device Name	Указано имя устройства / хост-устройства соседа.
Device Description	Приведено подробное описание устройства соседа.
Management Address	Указан административный IP-адрес соседа.

19 РАЗДЕЛ UDLD

Протокол обнаружения однонаправленного канала (UDLD) можно использовать для предотвращения образования петель в процессе коммутации второго уровня в сети. Проблема сетевых петель чаще всего возникает в сетях с топологией связующего дерева в результате неправильной разводки кабелей или нарушения функционирования сетевого интерфейса. Протокол обнаружения однонаправленного канала (UDLD) работает на канальном (втором) уровне.

Этот протокол отслеживает конфигурацию на физическом уровне (оптоволокно или медь). Он помогает обнаруживать петли коммутации и односторонние соединения.

Для обнаружения однонаправленного канала с помощью протокола UDLD требуется, чтобы два соседних коммутатора передавали UDLD-пакеты.

Коммутатор периодически (с интервалом передачи пакетов приветствия) передает UDLD-пакеты своим соседям через порты LAN, на которых активирован протокол UDLD.

Если в течение определенного времени коммутатор не получает отраженный UDLD-пакет, он отключает соответствующий порт и маркирует соответствующий канал, как однонаправленный.

Коммутаторы поддерживают этот протокол: пользователь может настроить его в разделе меню UDLD, как показано на рисунке 19.1.

Раздел UDLD делится на следующие три подраздела: Setting, Port-info и Reset.

Рисунок 19.1. Раздел меню UDLD.

19.1 Подраздел Setting раздела UDLD

Чтобы активировать протокол UDLD на коммутаторе, пользователь должен сначала настроить VLAN для этого протокола. Для этого нужно открыть подраздел Setting в разделе UDLD. Прежде чем активировать протокол UDLD, пользователь должен настроить VLAN с поддержкой протокола UDLD в окне настройки портов под заголовком UDLD Port Setting.

Для этого нужно выбрать идентификатор VLAN из раскрывающегося списка, а затем - один или несколько порты из списка в окне UDLD Port Setting на сетевой странице подраздела, как показано на рисунке 19.2.

Затем щелкните с указателем на кнопке Update в конце сетевой страницы, чтобы подтвердить выбор и настройки VLAN с поддержкой протокола UDLD.

Соответствующие значения идентификатора VLAN и UDLD-порта появятся в окне Current UDLD Setting, которое расположено в середине сетевой страницы.

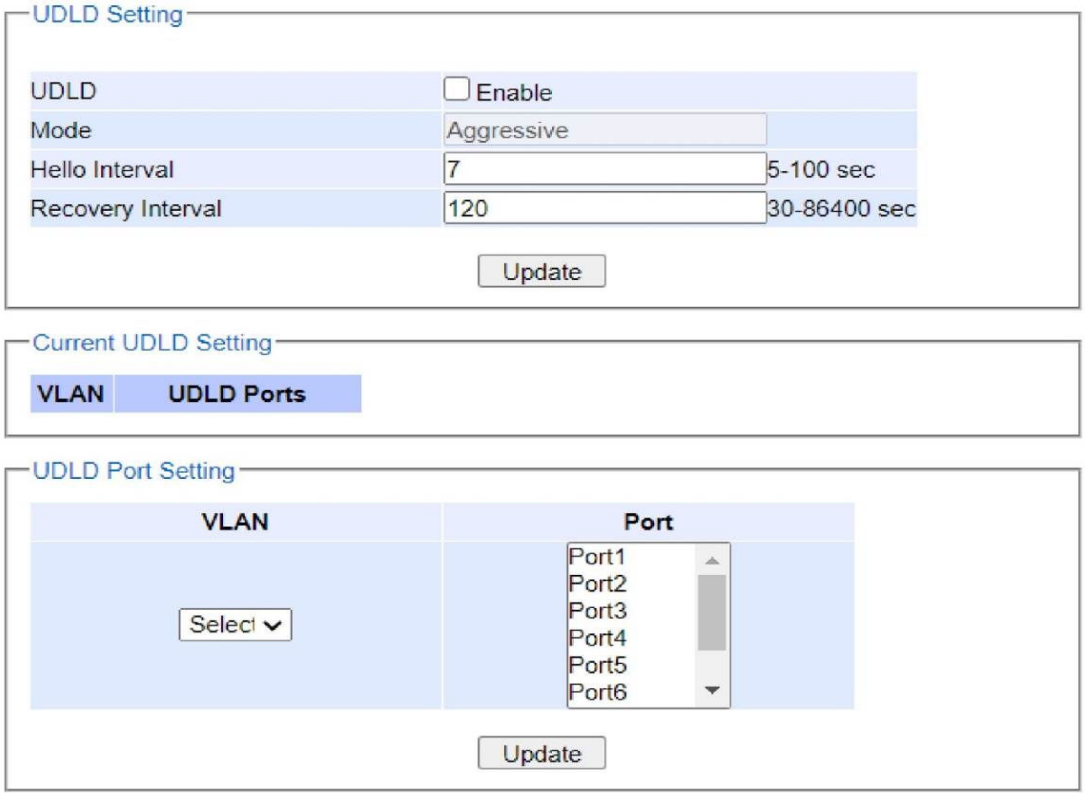


Рисунок 19.2. Сетевая страница настройки параметров протокола UDLD.

Затем пользователь может настроить параметры протокола UDLD, которые включают интервал передачи пакетов приветствия и интервал восстановления (поля Hello interval и Recovery interval соответственно).

Интервал передачи пакетов приветствия может принимать значения в диапазоне от 5 до 100 секунд. Величина этого интервала определяет время, через которое коммутатор передаст следующий эхо-пакет.

Значение по умолчанию равно 7 секундам.

Интервал восстановления может принимать значения в диапазоне от 30 до 86400 секунд. Величина этого интервала определяет время, в течение которого коммутатор будет пытаться восстановить работоспособность отключенного UDLD-порта.

Значение по умолчанию равно 120 секундам.

Протокол UDLD можно использовать в одном из двух рабочих режимов: Normal и Aggressive. В режиме Aggressive протокол UDLD может обнаруживать однонаправленные каналы, обусловленные односторонним трафиком в волоконно-оптических линиях и витых парах, а также неправильным подключением волоконно-оптических каналов.

В режиме Normal протокол UDLD способен обнаруживать однонаправленные каналы, обусловленные неправильно подключенными волоконно-оптическими линиями.

В текущем исполнении все устройства поддерживает только режим Aggressive, то есть, пользователь не может выбирать функциональный режим протокола.

После завершения всех описанных выше действий установите флажок в поле Enable в строке UDLD в верхней части окна UDLD Setting и щелкните с указателем на кнопке Update под

окном UDLD Setting, чтобы активировать протокол UDLD на управляемом коммутаторе.

ПРИМЕЧАНИЕ: чтобы успешно обнаруживать однонаправленную передачу, пользователь должен соответственно настроить другой управляемый коммутатор на другой стороне соединения с портом.

Если пользователь, не выполнив все описанные выше действия, сразу же установит в поле Enable и щелкнет с указателем на кнопке Update в верхней части сетевой страницы, система выдаст сообщение об ошибке, которое показано на рисунке 19.3.

Рисунок 19.3. Сообщение об ошибке, если не настроена VLAN с поддержкой протокола UDLD.

19.2 Подраздел Port-info раздела UDLD

На этой странице, показанной на рисунке, можно просматривать информацию о портах, контролируемых на предмет однонаправленной передачи (так называемых UDLD-портах).

В каждой записи таблицы пользователь может проверить идентификатор VLAN, номер порта, состояние канала и порта, а также информацию о соседе.

Информация о соседе включает идентификатор и название устройства, идентификатор порта и интервал передачи пакетов приветствия. Пример записи протокола UDLD показан на рисунке 19.4.

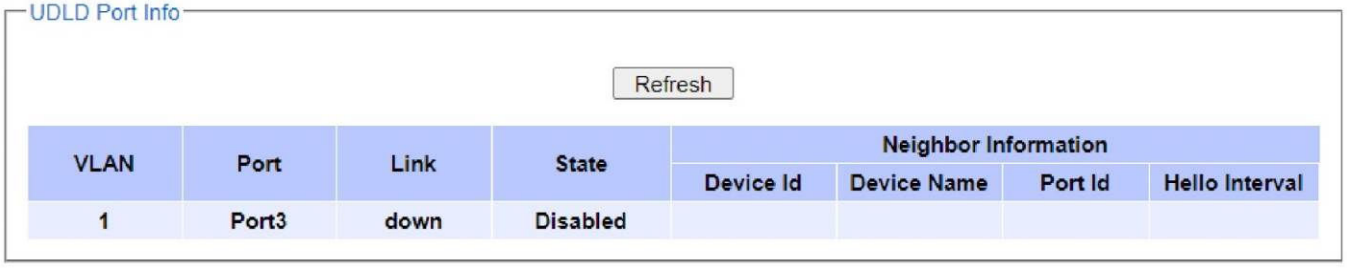


Рисунок 19.4. Пример сетевой страницы с информацией о порте в подразделе Port-info раздела меню UDLD.

19.3 Подраздел Reset раздела UDLD

В этом подразделе, сетевая страница которого показана на рисунке 19.5, пользователь может переустанавливать все UDLD-порты, отключенные протоколом UDLD.

Чтобы переустановить UDLD-порты, щелкните с указателем на кнопке Reset.

Рисунок 19.5. Сетевая страница подраздела Reset раздела UDLD.

20 PROFINET

PROFINET (Process Field Net) — это открытый и продвинутый стандарт промышленной автоматизации, основанный на промышленном Ethernet.

PROFINET позволяет пользователям обмениваться технологическими данными с компьютерами пользователя. В этом случае, вместо использования системы fieldbus, пользователи используют Ethernet в качестве механизма связи. На рисунке 20.1 показано выпадающее меню PROFINET на промышленном управляемом коммутаторе YN-SI2510A. В PROFINET есть два подраздела, Setting и I&M.

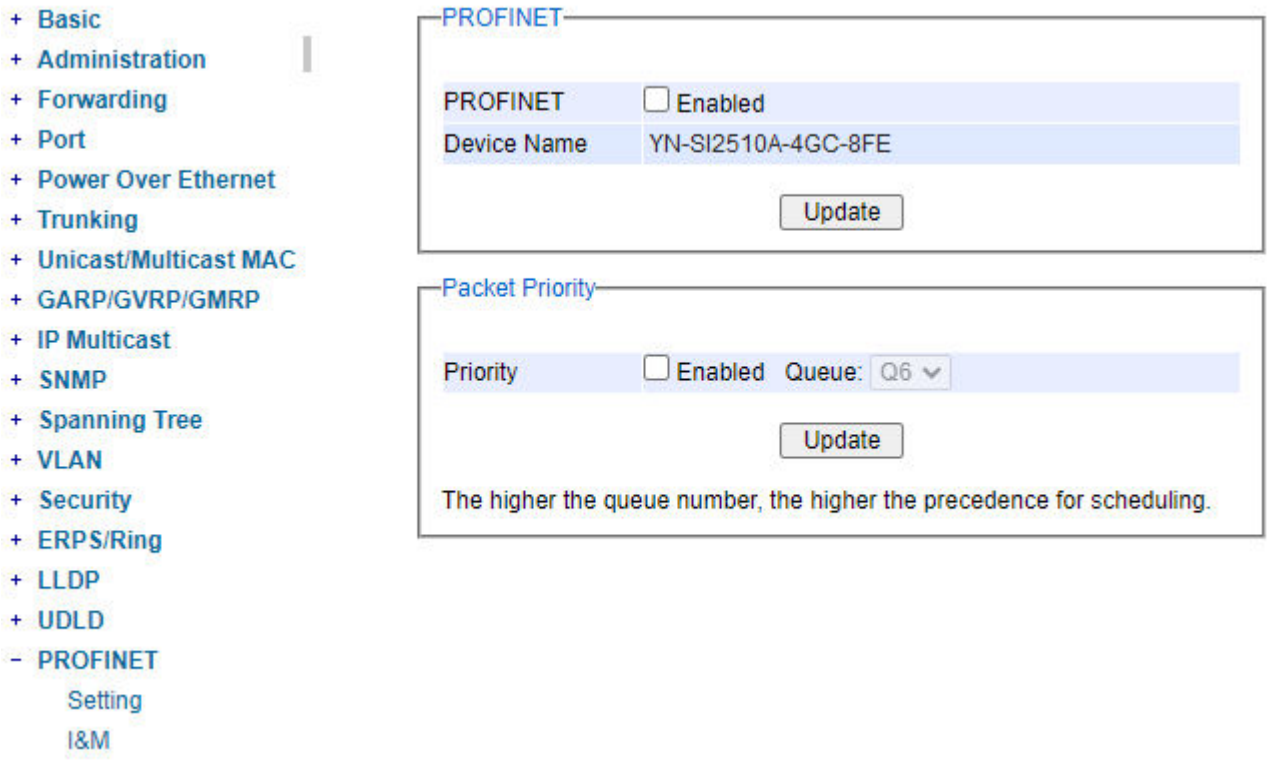


Рисунок 20.1. Сетевая страница настройки параметров протокола PROFINET.

20.1 Подраздел Setting раздела PROFINET

В это разделе можно включить PROFINET на промышленном управляемом коммутаторе YN-SI2510A. Чтобы включить PROFINET, нужно установить флажок Enabled в поле PROFINET. На веб-странице также отображается название устройства, как показано на рис. 20.2. Опция Приоритет пакетов PROFINET может быть включена на этой веб-странице, также можно выбрать номер приоритетной очереди из выпадающего списка. Обратите внимание, что чем выше номер очереди, тем выше приоритет для планирования пакетов.

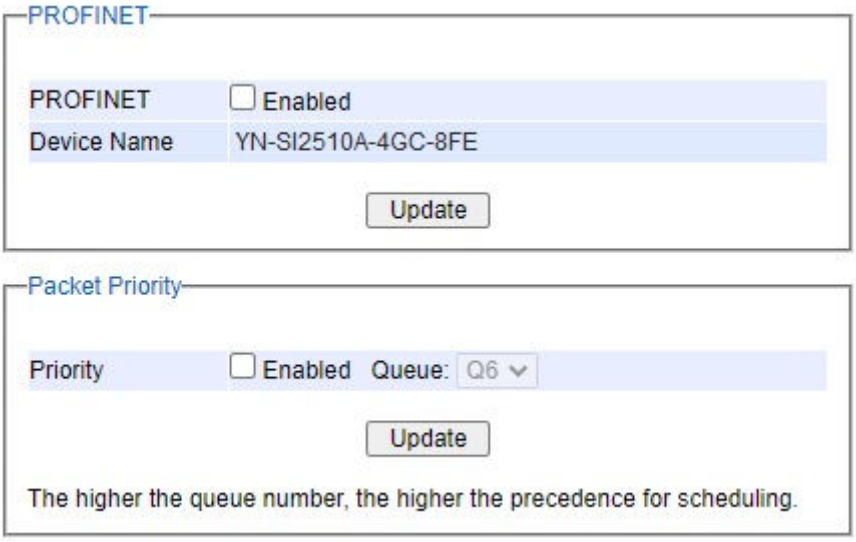


Рисунок 20.2. Сетевая страница Setting протокола PROFINET.

20.2 Подраздел I&M раздела PROFINET

Идентификация и техническое обслуживание (Identification and Maintenance - I&M) является неотъемлемой частью реализации каждого устройства PROFINET. Предоставляет собой стандартизированную информацию об устройстве и его частях.

Информация I&M доступна через объекты записи PROFINET и всегда привязана к подмодулю, принадлежащему описываемому элементу. Существует два объекта I&M: I&M0 и I&M1.

Объекты I&M0 предоставляют идентификатор поставщика и версию программного обеспечения управляемом коммутатора, как показано на рисунке 20.3.

Объекты I&M1 обеспечивают энергонезависимое хранилище информации, связанной с PROFINET, называемое функциональным тегом и тегом местоположения, в которое пользователи могут вводить информацию и сохранять ее на коммутаторе, как показано на рисунке 20.3. Информация хранится устройством в энергонезависимой памяти. После ввода желаемой информации на I&M1, нажмите кнопку Обновить, чтобы сохранить ее на управляемом коммутаторе.

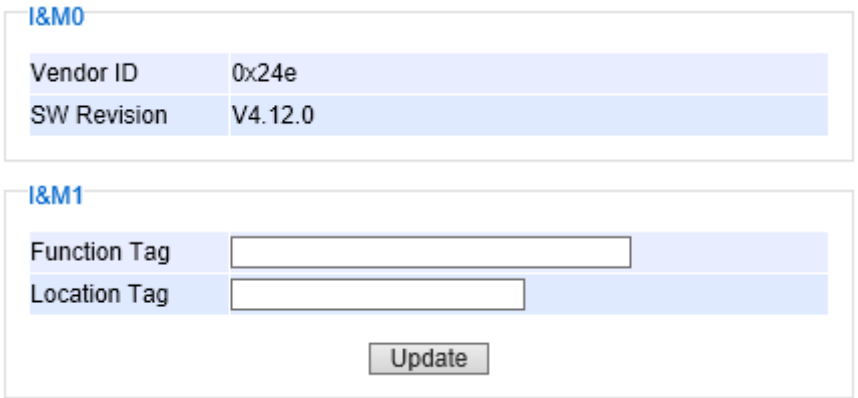


Рисунок 20.3. Сетевая страница I&M протокола PROFINET.

21 РАЗДЕЛ CLIENT IP SETTING

Для промышленного управляемого коммутатора предусмотрено два различных сценария назначения IP-адресов устройствам, подключенным к его портам.

Раздел Client IP Setting включает следующие два подраздела:

1. DHCP Relay Agent,
2. DHCP Mapping IP.

На рисунке 21.1 показано раскрывающееся меню раздела Client IP Setting.

Рисунок 21.1. Раскрывающееся меню раздела Client IP Setting.

21.1 Подраздел DHCP Relay Agent

Агент-ретранслятор DHCP – это простая программа, которая ретранслирует сообщения протокола DHCP / протокола начальной загрузки (BOOTP), передаваемые между клиентами и серверами в различных подсетях.

Согласно соответствующим спецификациям RFC агенты - ретрансляторы DHCP/BOOTP являются стандартными функциями в составе протоколов DHCP и BOOTP.

Агент – ретранслятор ретранслирует DHCP/BOOTP-сообщения, которые передаются в широковещательном режиме через один из его подключенных физических интерфейсов (например, сетевой адаптер) в другие удаленные подсети, с которыми он соединяется через другие физические интерфейсами.

На рисунке 21.2 показана сетевая страница настройки параметров агента-ретанслятора протокола DHCP.

Пользователь может ввести до четырех IP-адресов DHCP/BOOTP-серверов в поля Server IP 1, Server IP 2, Server IP 3 и Server IP 4. Затем пользователь может активировать DHCP-ретранслятор, установив флажок в поле Enable в конце строки DHCP Relay.

Пользователь также может на собственное усмотрение активировать функцию Option 82 протокола DHCP, которая используется агентом-ретранслятором DHCP в качестве информационной опции.

Если активирована функция Option 82, коммутатор вставляет информацию о местоположении сети клиента в заголовок пакета с DHCP-запросом, принятым от клиента через незащищенный интерфейс.

Затем коммутатор передает измененный запрос на DHCP-сервер. DHCP-сервер находит информацию функции Option 82 в заголовке пакета и использует ее при создании IP-адреса и других атрибутов для клиента.

Когда DHCP-сервер передает ответ на коммутатор, коммутатор удаляет информацию функции Option 82 из ответного пакета, а затем переадресовывает пакет клиенту.

В поле Option 82 Type, показанном на рисунке, можно выбрать тип функции из вариантов IP, MAC, Client-ID или Other.

Если пользователь выберет тип Other, станет доступным для редактирования поле Option 82 Value, в котором пользователь должен будет ввести нужное значение.

После завершения настройки параметров агента-ретранслятора DHCP нужно щелкнуть с указателем на кнопке Update, чтобы внесенные изменения вступили в силу.

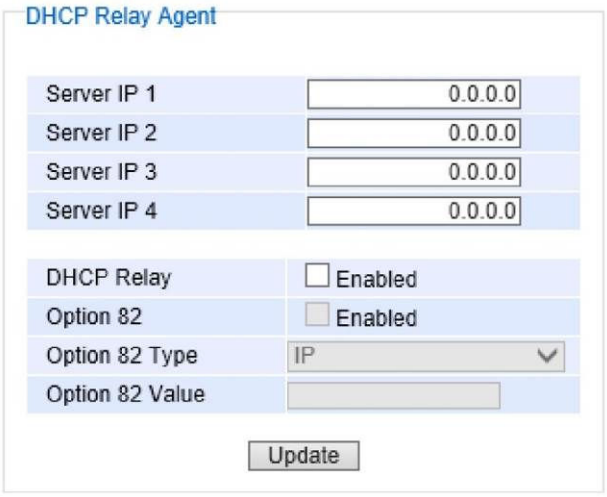


Рисунок 21.2. Сетевая страница подраздела DHCP Relay Agent.

21.2 Подраздел DHCP Mapping IP

В этом подразделе пользователь может зарезервировать или привязать IP-адреса для устройства, подключенного к выбранным портам.

На рисунке 21.3 показана сетевая страница подраздела DHCP Mapping IP, на которой можно указать IP-адрес для каждого порта в соответствующем поле.

После завершения привязки IP-адресов для протокола DHCP нужно щелкнуть с указателем на кнопке Update, чтобы внесенные изменения вступили в силу.

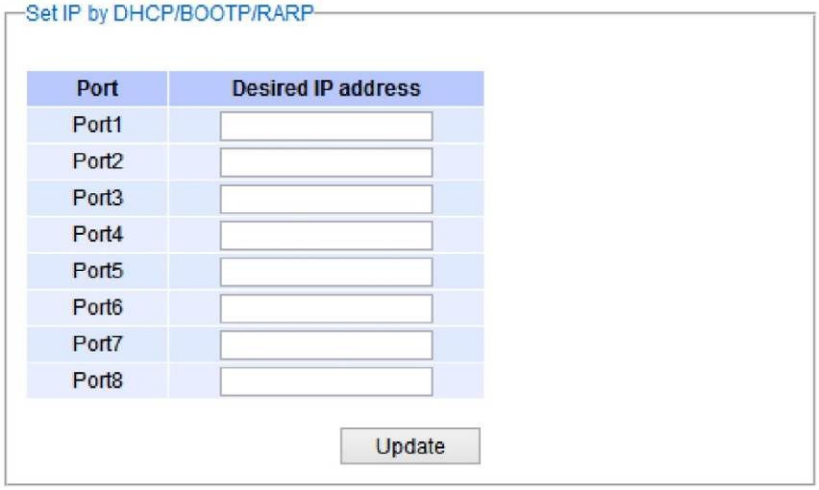


Рисунок 21.3. Сетевая страница подраздела DHCP Mapping IP.

22 РАЗДЕЛ SYSTEM

Раздел System является последним разделом меню сетевого пользовательского интерфейса управляемого коммутатора.

В этом разделе предусмотрены различные инструментальные средства для сетевого администратора, используя которые, он может контролировать внутреннее состояние коммутатора по системному журналу, предупреждениям и уведомлениям аварийной сигнализации.

В этом разделе администратор также может выполнять определенные задачи по техническому обслуживанию устройства, такие как создание резервных копий, восстановление конфигурации устройства, обновление встроенного микропрограммного обеспечения, сброс на заводские настройки, перезагрузка системы/устройства и т.д.

На рисунке 22.1 в развернутом виде показано раскрывающееся меню раздела System.

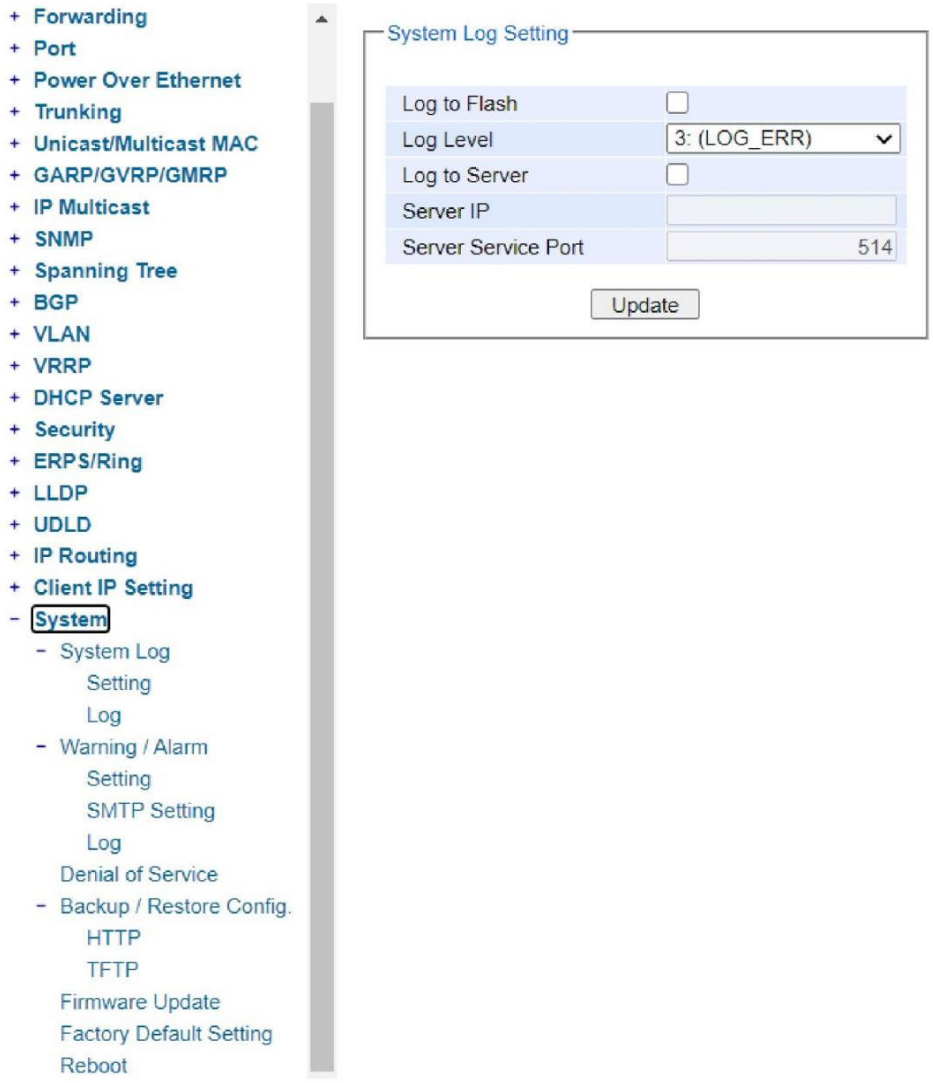


Рисунок 22.1. Раскрывающееся меню раздела System.

Для сетевого администратора очень важно знать, что происходит в его сети и контролировать все события.

Однако бывает затруднительно быстро определить местоположение сетевых устройств,

которые находятся в конечных точках системы.

Поэтому сетевые коммутаторы Ethernet, подключенные к таким устройствам, играют важную роль первичной аварийной сигнализации.

Они сразу же уведомляют сетевого администратора о любых происшествиях и нештатных ситуация, предоставляя ему возможность своевременно принять меры.

В разделе System можно настроить вывод предупреждений по электронной почте и релейный выход, чтобы быстро передавать достоверные предупреждения администраторам.

22.1 Подраздел System Log

Подраздел System Log, в свою очередь, делится на два подраздела нижнего уровня: Setting и Log.

22.1.1 Подраздел Setting меню System Log

На рисунке 22.2 показано окно для настройки параметров системного журнала. Фактически записанные события отображаются в журнале регистрации в следующем подразделе меню. В этом подразделе пользователь может настроить процедуры сохранения журнала и/или его доставки в другие системы.

Журнал можно сохранить во флэш-памяти управляемого коммутатора и/или передать его на удаленный сервер журналов.

Пользователь также должен выбрать уровень регистрации данных и указать IP-адрес удаленного сервера журналов и служебный порт для сервиса журналирования.

После завершения настройки параметров щелкните с указателем на кнопке Update.

В таблице 22.1 приведено описание настраиваемых параметров системного журнала.

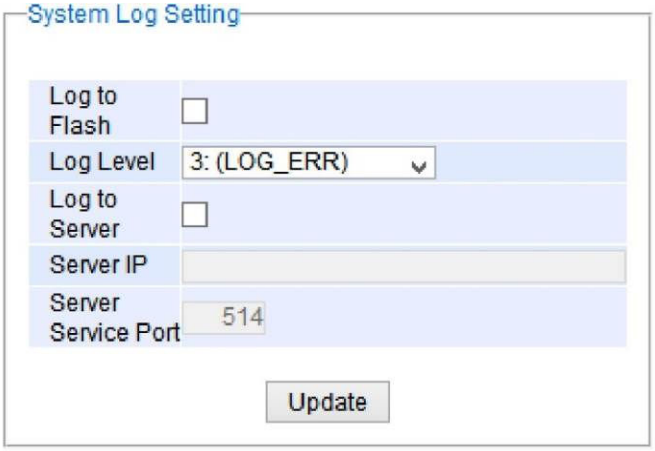


Рисунок 22.2. Сетевая страница подраздела Setting меню System Log.

Таблица 22.1. Описание настраиваемых параметров системного журнала.

Имя параметра	Описание	Заводская настройка по умолчанию
Enable Log Event to Flash	Флажок установлен: журналируемые события сохраняются во флэш-памяти устройства. Файлы журнала сохраняются во флэш-памяти даже после перезагрузки коммутатора. Флажок не установлен: журналируемые события сохраняются в оперативной памяти устройства. После каждой перезагрузки оперативная память полностью очищается, и файлы с журналируемыми событиями удаляются.	Флажок не установлен
Log Level	Устанавливается уровень регистрации данных, который определяет события, отображаемые на сетевой странице в следующем подразделе меню (Log). Значение в поле является инклюзивным. Это означает, что если, например, указано значение 3:(Log_ERR), то в журнале будут регистрироваться события всех уровней, включая третий, т.е. 0, 1, 2 и 3. Принимает значения в диапазоне от Log 0 до Log 7.	3:(LOG_ERR)
Enable System Log Server	Флажок установлен: сервер системных журналов активирован. Флажок не установлен: сервер системных журналов отключен. Если флажок установлен, все зарегистрированные в журнале события будут передаваться на удаленный сервер системных журналов.	Флажок не установлен
System Log Server IP	Настраивается IP-адрес сервера системных журналов.	0.0.0.0
System Log Server Service Port	В этом поле указывается номер порта сервера системных журналов. Принимает значения в диапазоне от Port 1 до Port 65535.	514

22.1.2 Подраздел Log меню System Log

На рисунке 22.3 показан пример всех журналов событий. Обратите внимание, что журналы сортируются по дате и времени.

В таблице 22.2 приведено описание содержания каждого столбца и назначения каждой кнопки на сетевой странице с системным журналом.

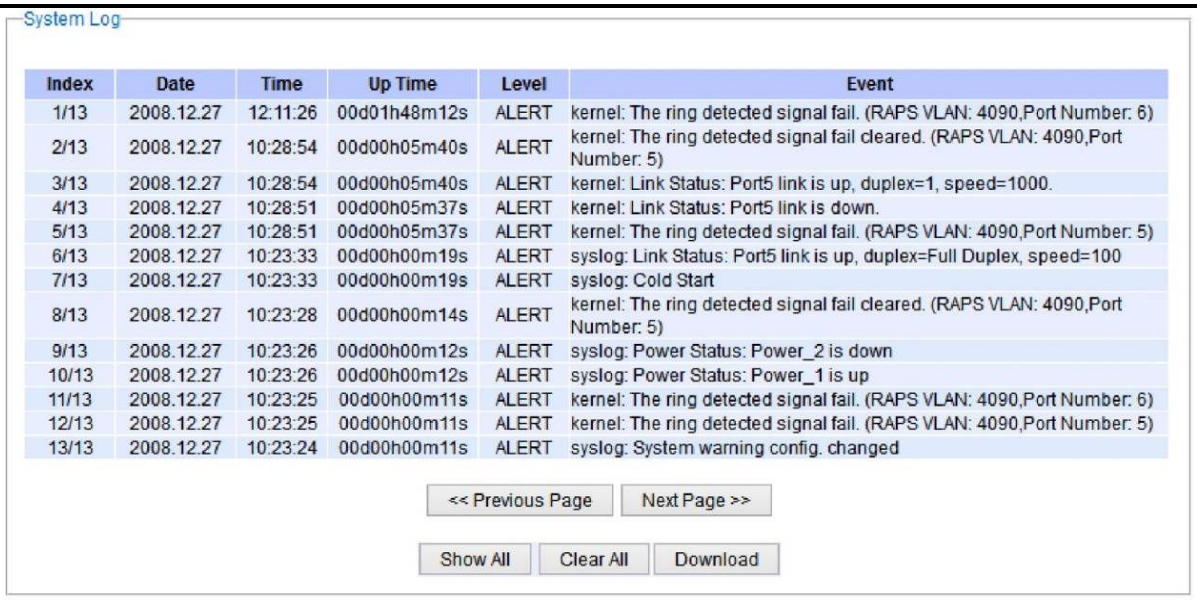


Рисунок 22.3. Сетевая страница журнала регистрации событий.

Таблица 22.2. Описание столбцов и кнопок управления в таблице на сетевой странице подраздела Log.

Имя параметра	Описание
Index	В этом поле указываются порядковые номера журналируемых событий.
Date	В этом поле указывается системная дата события.
Time	В этом поле указывается метка времени события.
Up Time	В этом поле указывается продолжительность пребывания системы (управляемого коммутатора) в рабочем состоянии после возникновения события.
Level	В этом поле указывается уровень события.
Event	В этом поле приводится подробное описание события.
Previous Page	При щелчке с указателем на этой кнопке отображаются события на предыдущей странице.
Next Page	При щелчке с указателем на этой кнопке отображаются события на следующей странице.
Show All	При щелчке с указателем на этой кнопке отображаются все события.
Clear All	При щелчке с указателем на этой кнопке все события удаляются.
Download	При щелчке с указателем на этой кнопке выполняется выгрузка журнала регистрации событий или его сохранение на локальном компьютере.

22.2 Подраздел Warning/Alarm

Подраздел предупреждающей и аварийной сигнализации состоит из следующих трех подразделов: Setting, SMTP Setting и Log.

22.2.1 Подраздел Warning/Alarm

Используются предупреждающие и аварийные сигналы трех различных типов: аварийные сигналы состояния канала, аварийные сигналы состояния питания и аварийные сигналы системного журнала.

Соответствующие окна на странице (Link Status Alarms, Power Status Alarms и System Log Alarms) показаны на рисунке 22.4.

Аварийные сигналы состояния канала связаны с активностью определенных портов. Аварийная сигнализация состояния питания отслеживает текущие параметры питания коммутатора на контактах входного разъемного соединителя.

Аварийные сигналы системного журнала связаны с общей функциональностью коммутатора. На данной сетевой странице пользователь может настроить способы доведения аварийных событий каждого типа до сведения пользователей.

Для аварийных сигналов состояния канала и состояния питания предусмотрено три возможных способа уведомления: Relay, E-mail и Alarm LED.

Для аварийных сигналов системного журнала имеется только два способа уведомления: Relay и E-mail.

Завершив настройку параметров аварийной сигнализации, щелкните с указателем на кнопке Update.

Обратите внимание на кнопку Assert Relay. С ее помощью можно тестировать внешнее реле, подключенное к управляемому коммутатору.

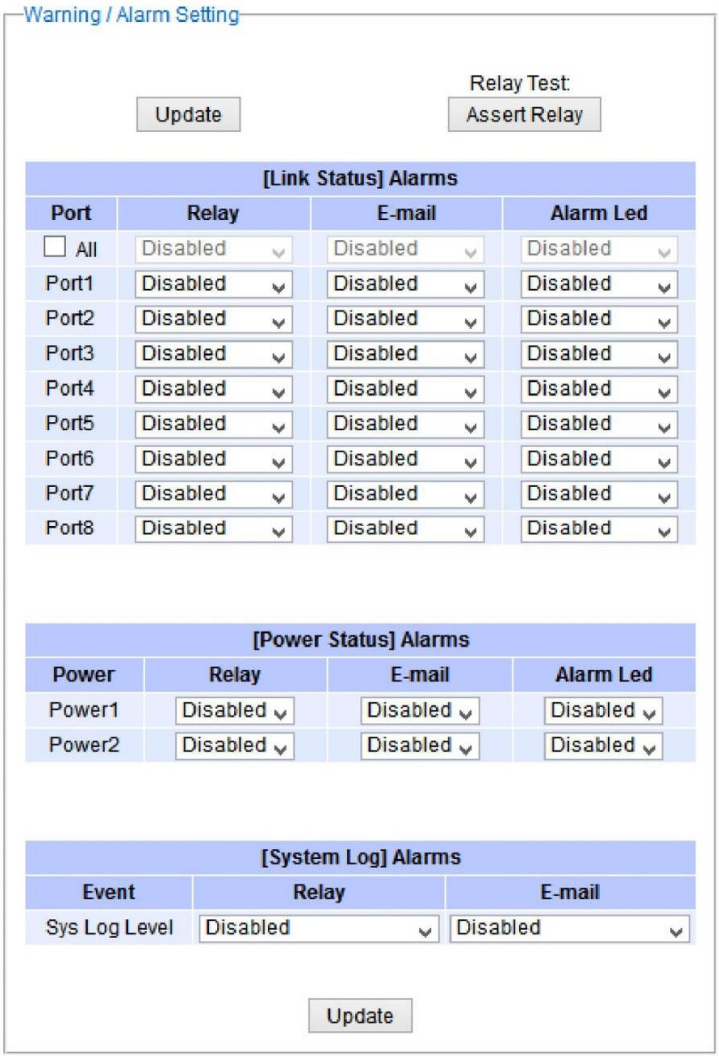


Рисунок 22.4. Сетевая страница выбора событий для предупреждающей и аварийной сигнализации.

В окне Link Status Alarms пользователь может выбрать условия срабатывания сигнализации для передачи уведомления выбранным способом (Relay, E-mail или Alarm LED): включение канала, выключение канала или включение и выключение канала.

В таблице 22.3 в сводном виде представлено описание параметров для выбора аварийного события состояния канала.

Обратите внимание, что пользователь может активировать аварийные события для всех портов одновременно, установив флажок в поле All в верхней строке.

Таблица 22.3. Описание параметров для выбора аварийного события состояния канала.

Имя параметра	Описание	Заводская настройка по умолчанию
Port	Указывается номер порта.	-
Port state event	Disabled: Функция аварийной сигнализации отключена, никакие аварийные сообщения не передаются.	Disabled
	Link Up: аварийное сообщение будет передано при активации данного порта / канала и установлении соединения. Link Down: аварийное сообщение будет передано при отключении данного порта / канала и прерывании соединения. Link Up /Down: аварийное сообщение будет передаваться при любом изменении состояния, то есть, как при установлении, так и при прерывании соединения.	

Для аварийной сигнализации питания пользователь может выбрать одни из двух вариантов условий передачи уведомления выбранным способом (Relay, E-mail или Alarm LED) . - Power On или Power Off.

В таблице 22.4 в сводном виде представлено описание параметров для выбора аварийного события состояния питания.

Таблица 22.4. Описание параметров для выбора аварийного события состояния питания.

Имя параметра	Описание	Заводская настройка по умолчанию
Power	Указывается определенный источник электропитания.	Отключено
Power status event	Disable: функция аварийной сигнализации отключена. Power On: аварийный сигнал передается при включении питания. Power Off: аварийный сигнал передается при выключении питания.	Disabled

Для аварийных сигналов системного журнала предусмотрено только два способа уведомления: Relay и E-mail.

В таблице 22.5 приведено описание уровней регистрируемых событий, которые можно выбирать для передачи уведомлений об аварийных событиях системного журнала.

Таблица 22.5. Описание параметров для выбора аварийного события системного журнала.

Имя параметра	Описание	Заводская настройка по умолчанию
System log event	Disable: режим отслеживания состояния питания отключен. 0: (LOG_EMERG): активировано отслеживание на уровнях регистрации данных 0 ~ 7. 1: (LOG_ALERT): активировано отслеживание на уровнях регистрации данных 1 ~ 7. 2: (LOG_CRIT): активировано отслеживание на уровнях регистрации данных 2 ~ 7. 3: (LOG_ERR): активировано отслеживание на уровнях регистрации данных 3 ~ 7. 4: (LOG_WARNING): активировано отслеживание на уровнях регистрации данных 4 ~ 7. 5: (LOG_NOTICE): активировано отслеживание на уровнях регистрации данных 5 ~ 7. 6: (LOG_INFO): активировано отслеживание на уровнях регистрации данных 6 ~ 7. 7: (LOG_DEBUG): активировано отслеживание на уровне регистрации данных 7. Описание уровней регистрации данных приведено в примечаниях ниже.	Disabled

*** ПРИМЕЧАНИЕ:** Уровни регистрации данных являются инклюзивными. Иными словами, если установить уровень регистрации данных 0, аварийная сигнализация будет срабатывать каждый раз при регистрации события на уровне 0, 1, 2... 6 или 7. Если установить уровень регистрации данных 5, аварийная сигнализация будет срабатывать каждый раз при регистрации события на уровне 5, 6 или 7.

0: аварийная ситуация: система стала нестабильной.

1: тревога: требуются немедленные действия.

2: критическое событие: критическое состояние системы.

3: ошибка: состояние ошибки.

4: предупреждение: предупреждение о возможности неблагоприятного развития ситуации.

5: уведомление: состояние в целом нормальное, но событие требует внимания.

6: для справки: информационное сообщение.

7: отладка: сообщение уровня отладки.

22.2.2 Подраздел SMTP Settings

Простой протокол обмена почтовыми сообщениями (SMTP) представляет собой стандартный интернет-протокол, который используется для передачи электронной почты по IP-сети.

В случае возникновения любого настораживающего события, соответствующего критериям, установленным, система может передать аварийное сообщение пользователю по электронной

почте.

В данном подразделе пользователь может настраивать параметры электронной почты для передачи системных аварийных сигналов (состояния канала, состояние питания и системного журнала), как показано на рисунке 22.5.

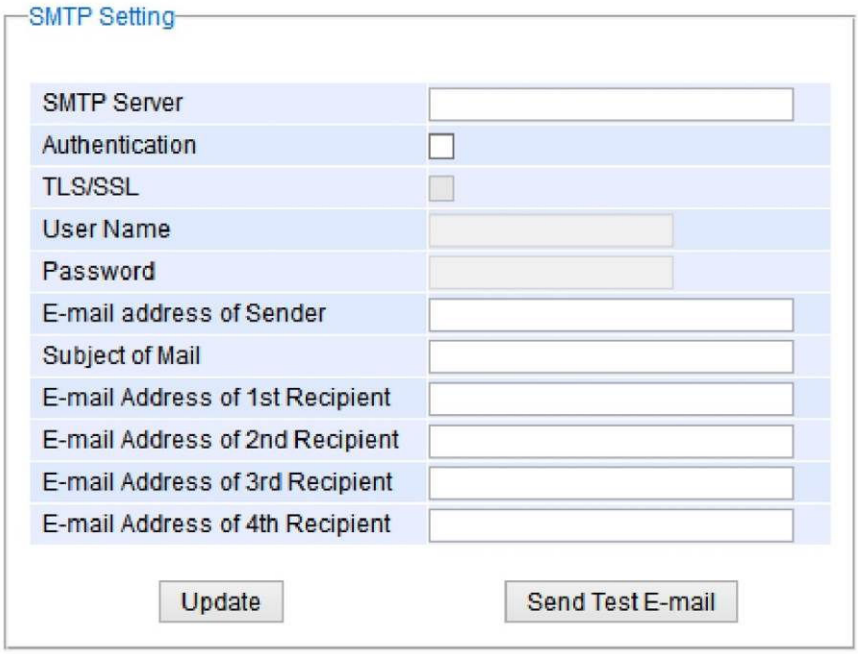


Рисунок 22.5. Сетевая страница настройки параметров SMTP-протокола.

Пример настройки параметров протокола SMTP показан на рисунке 22.6.

Заполнив все обязательные поля, щелкните с указателем на кнопке Update, чтобы новая конфигурация вступила в силу.

ПРИМЕЧАНИЕ: на этой сетевой странице пользователь может отправить тестовое электронное письмо для проверки настроек протокола SMTP.

Для этого нужно щелкнуть с указателем на кнопке Send Test E-mail. Описание всех параметров в окне SMTP Setting в сводном виде представлено в таблице 22.6.

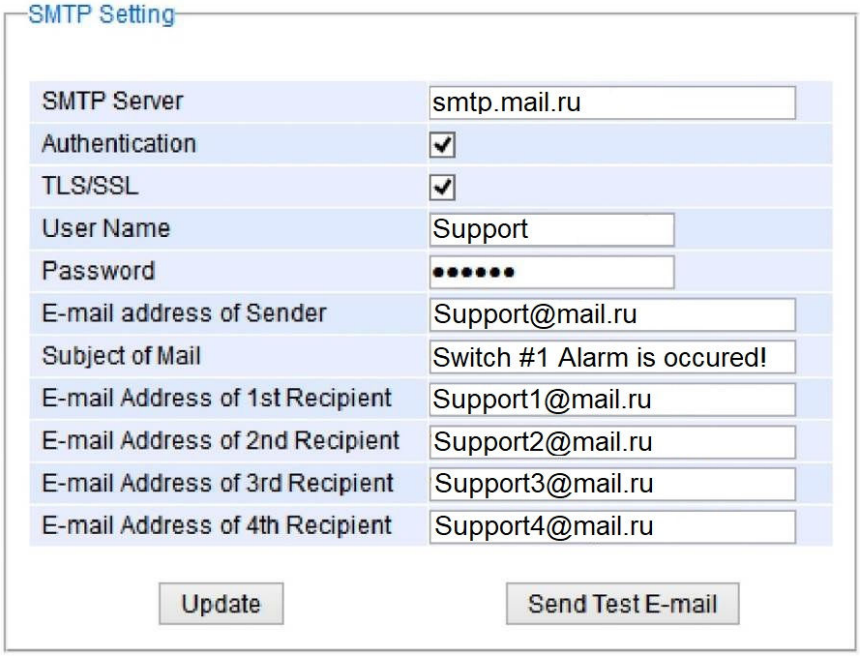


Рисунок 22.6. Пример окна настройки параметров протокола SMTP.

Таблица 22.6. Описание настраиваемых параметров протокола SMTP.

Имя параметра	Описание	Заводская настройка по умолчанию
SMTP Server	Указывается IP-адрес почтового сервера для исходящих сообщений.	Не заполняется
Authentication	При установке или снятии флажка в этом поле соответственно активируется или отключается режим входа в систему с проверкой подлинности. Если опция активирована, SMTP-сервер потребует подтвердить подлинность для схода в систему. В этом режиме также нужно указать имя пользователя и пароль для подключения к SMTP-серверу.	Отключено (флажок не установлен)
TLS/SSL	Активация или отключение функции безопасности на транспортном уровне (TLS) или протокола безопасных соединений (SSL), которая поддерживает алгоритм шифрования для связи с SMTP-сервером.	Отключено (флажок не установлен)
Username	В этом поле указывается имя пользователя (или имя учетной записи) для входа в систему. Максимальная длина - 31 символ.	Не заполняется
Password	В этом поле указывается пароль учетной записи для входа в систему. Максимальная длина - 15 символов.	Не заполняется
E-mail Address of Sender	В этом поле указывается адрес электронной почты отправителя.	Не заполняется
Mail Subject	В этом поле указывается тема предупреждающего сообщения. Максимальная длина - 31 символ.	Не заполняется
E-mail Address of 1st Recipient	В этом поле указывается адрес электронной почты первого получателя.	Не заполняется
E-mail Address of 2nd Recipient	В этом поле указывается адрес электронной почты второго получателя.	Не заполняется
E-mail Address of 3rd Recipient	В этом поле указывается адрес электронной почты третьего получателя.	Не заполняется
E-mail Address of 4th Recipient	В этом поле указывается адрес электронной почты четвертого получателя.	Не заполняется
Update	Щелкните с указателем на этой кнопке для сохранения изменений в памяти управляемого коммутатора.	-
Send Test E-mail	Щелкните с указателем на этой кнопке, чтобы отправить тестовое электронное письмо указанным выше получателям для проверки правильности настроек.	-

22.2.3 Подраздел Log

Управляемый коммутатор предупреждает пользователя о возникновении событий. Как показано на рисунке 22.7, информация о настораживающих событиях выводится в данном подразделе в таблице под названием Warning/Alarm Log.

Пользователь может щелкнуть с указателем на кнопке Reset Relay, расположенной в верхней части окна, чтобы сбросить реле.

Щелчком на соседней кнопке Clear Log можно удалить все записи из таблицы.

Чтобы просмотреть актуальную информацию в таблице, щелкните с указателем на кнопке Refresh.

Рисунок 22.7. Сетевая страница Warning/Alarm Log.

Пример заполненной таблицы Warning/Alarm Log показан на рисунке 22.8.

Обратите внимание, что формат представления информации и управляющие кнопки несколько отличаются от текущего формата, используемого на коммутаторах, который показан на рисунке выше.

Краткий список аварийных сообщений отображается в верхней части интерфейса интернет-браузера.

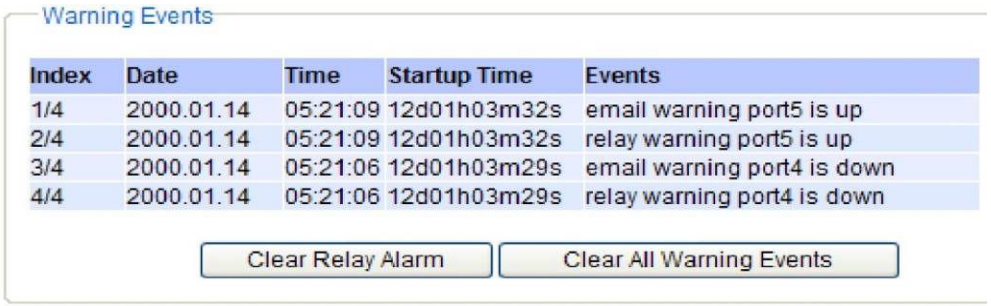


Рисунок 22.8. Пример таблицы со списком настораживающих событий.

Таблица 22.7. Описание столбцов и кнопок управления в таблице на сетевой странице подраздела Warning/Alarm Log.

Имя параметра	Описание	Заводская настройка по умолчанию
Reset Relay	Щелчком с указателем на этой кнопке сбрасывается аварийное состояние реле на аппаратном уровне.	Реле отключено
Clear Log	Щелчком с указателем на этой кнопке удаляются все записи о настораживающих событиях, выведенные на экране.	-
Refresh	Щелчком с указателем на этой кнопке обновляется информация о настораживающих и аварийных событиях.	-
Index	Отображается порядковый номер записи о настораживающем или аварийном событии с указанием общего количества записей.	-
Date	Дата возникновения события, инициировавшего срабатывание аварийной сигнализации.	-
Time	Время возникновения события, инициировавшего срабатывание аварийной сигнализации.	-
Startup Time	Время, прошедшее с момента запуска коммутатора до возникновения события, инициировавшего срабатывание аварийной сигнализации.	-

Имя параметра	Описание	Заводская настройка по умолчанию
Events	Описание события, инициировавшего срабатывание аварийной сигнализации.	-

22.3 Подраздел Denial of Service

Атака типа "отказ в обслуживании" (DoS-атака) представляет собой злонамеренную попытку сделать недоступной машину или сетевой ресурс для его легальных пользователей и, таким образом, временно или постоянно приостановить или прервать обслуживание хост-устройства, подключенного к сети Интернет.

Промышленный управляемый коммутатор поддерживает фильтрацию, обеспечивающую защиту от атак различных типов.

Для этого предусмотрена сетевая страница в подразделе Denial of Service, которая показана на рисунке 22.9.

Ниже перечислены некоторые виды атак, которые способна предотвращать система коммутатора.

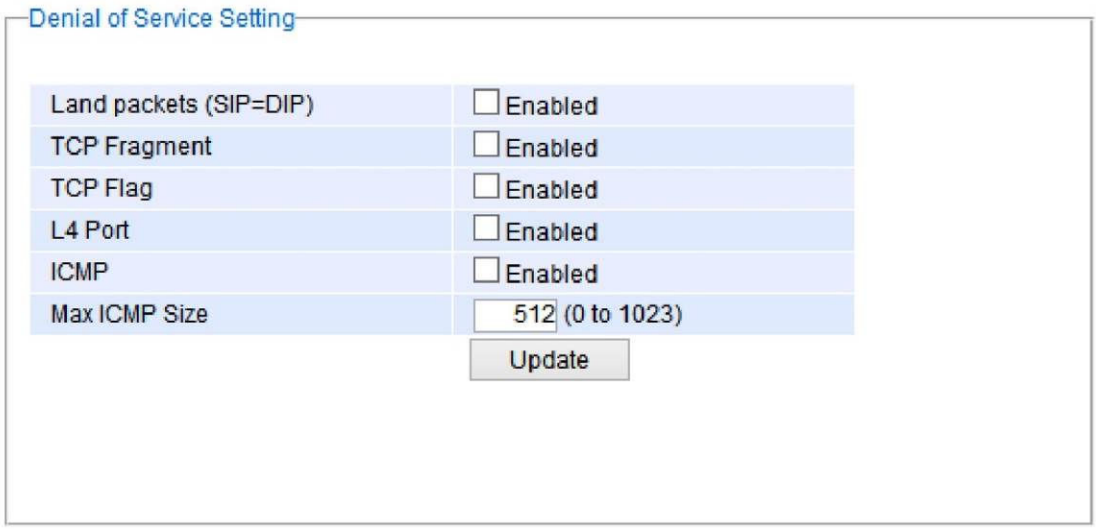


Рисунок 22.9. Сетевая страница подраздела Denial of Service Setting.

Сначала рассмотрим DoS-атаку типа "атака отказа в локальной сети" (LAND-атака). LAND-атака — это DoS-атака четвертого уровня, в ходе которой злоумышленник выдает одинаковую информацию об источнике и месте назначения TCP-сегмента.

Специально создается пакет синхронизации протокола TCP, в котором для источника и назначения указываются одинаковые IP-адрес и порт, которые обычно соответствуют открытому порту на атакуемой машине. Атакуемая машина принимает такое сообщение и передает ответ на адрес назначения, тем самым передавая пакет на обработку в бесконечном цикле.

В результате она откажет и зависнет по причине многократной обработки одного и того же пакета протоколами из стека TCP.

Чтобы активировать или отключить защиту от атак отказа в локальной сети (LAND-атак), установите флажок в поле Enable в строке LAND packet (SID=DID).

Атака уязвимости второго типа представляет собой атаку посредством фрагментации TCP-пакетов. Она также известна под названием "атака крошечными фрагментами".

Эта атака нацелена на механизм повторной сборки протокола TCP/IP. Она препятствует сборке фрагментов пакетов данных.

В результате пакеты данных накапливаются и быстро переполняют серверы, что в итоге приводит к их отказу.

Чтобы активировать или отключить защиту от DoS-атак посредством фрагментации TCP-пакетов, установите флажок в поле Enable в строке TCP Fragment.

Однако в данном случае может потребоваться дополнительная настройка правил фильтрации для некоторых вводов.

Например, разрешить или не разрешить первый фрагмент, указать минимальный разрешенный размер заголовка протокола TCP. В некоторых канальных протоколах, таких как Ethernet, только первый фрагмент содержит полный заголовок верхнего уровня, то есть, остальные фрагменты представляют собой "обезглавленные" датаграммы.

При этом на сеть не создается дополнительная нагрузка благодаря тому, что каждый фрагмент содержит собственный заголовок IP-уровня. Только первый фрагмент содержит заголовок протокола ICMP, остальные фрагменты создаются без этого заголовка.

Третий тип атак называют DoS-атакой флагами протокола TCP. Злоумышленник передает TCP-пакеты с флагами, обозначающими пакеты подтверждения.

Эта атака подобна атаке SYN-флуд, за исключением того, что SYN-флуд также устанавливает соединение с сервером. Защита устройств чаще рассчитана на противодействие атаке SYN-флуд, так как такие атаки более распространены.

DoS-атака флагами протокола TCP вынуждает сервер непрерывно отбрасывать пакеты, что приводит к исчерпанию ресурса. Чтобы активировать или отключить защиту от DoS-атак флагами протокола TCP, установите флажок в поле Enable в строке TCP Flag.

Атака четвертого типа называется DoS-атакой на порты четвертого уровня. Этот вид атак, в свою очередь, также делится на несколько типов.

При UDP-атаке на целевое устройство передается большое количество UDP-пакетов, что в итоге вызывает его перегрузку. UDP-Lag атака происходит с перерывами, чтобы целевое устройство не отключилось от сети полностью. SUDP-атака подобна UDP-атаке, но дополнительно имитирует запрос, что затрудняет противодействие.

Атаки SYN/SSYN/ESSYM непрерывно инициируют квитирование по протоколу TCP, до тех пор, пока не произойдет перегрузка целевого устройства.

Атаки DNS/NTP/CHARGEN/SNMP представляют собой усиленные UDP-атаки, которые перегружают уязвимый сервер, передавая поддельный запрос с указанием IP-адреса целевого

устройства в качестве адреса отправителя.

Сервер начинает передавать на целевое устройство информацию и перегружает систему. Чтобы активировать или отключить защиту от DoS-атак на порты четвертого уровня, установите флажок в поле Enable в строке L4 Port.

И, наконец, рассмотрим еще один тип атак, так называемые атаки фрагментации ICMP-пакетов. В ходе такой атаки злоумышленник передает поддельные пакеты протокола ICMP, размер которых превышает максимальный размер передаваемого полезного блока данных в сети. Система данного коммутатора позволяет администратору отфильтровывать эти пакеты.

Для этого нужно активировать функцию ICMP и установить максимальный размер ICMP-пакета в диапазоне от 512 до 1023 байтов.

Поддельные пакеты протокола ICMP невозможно собрать повторно, поэтому при обработке таких пакетов ресурсы сервера быстро истощаются, и сервер становится недоступным.

Чтобы активировать или отключить защиту от DoS-атак ICMP-пакетами, установите флажок в поле Enable в строке ICMP.

Описание настраиваемых параметров подраздела Denial of Service в сводном виде представлено в таблице 22.8.

Таблица 22.8. Описание настраиваемых параметров защиты от атак типа "отказ в обслуживании".

Имя параметра	Описание	Заводская настройка по умолчанию
LAND packets	При выборе опции Enabled: действует защита от атак, использующих пакеты синхронизации протокола TCP, в которых указаны одинаковые IP-адрес и порт для источника и места назначения.	Отключено
TCP Fragment	При выборе опции Enabled: действует защита от атак посредством фрагментации TCP-пакетов, нацеленных на механизм повторной сборки фрагментированных TCP/IP-пакетов.	Отключено
TCP Flag	При выборе опции Enabled: действует защита от атак флагами протокола TCP, которые вынуждают сервер непрерывно отбрасывать пакеты, что приводит к исчерпанию ресурса.	Отключено
L4 Port	При выборе опции Enabled: действует защита от различных DoS-атак на порты четвертого уровня, которые имеют целью перегрузить сервер.	Отключено
ICMP	При выборе опции Enabled: активируется функция фильтрации пакетов протокола ICMP, размер которых превышает максимальный допустимый размер ICMP-пакета, указанный в следующем поле	Отключено
Max ICMP Size	От 512 до 1023 байтов.	512

22.4 Подраздел Backup/Restore Config

В подразделе Backup/Restore Config пользователь может загрузить конфигурацию промышленного управляемого коммутатора на локальный компьютер для хранения и

использования в качестве резервной копии.

Пользователь также может восстановить ранее сохраненную конфигурацию промышленного управляемого коммутатора из резервной копии на локальном компьютере.

При этом текущая конфигурация устройства будет удалена.

Для реализации функций резервного копирования и восстановления можно использовать один из двух различных протоколов: HTTP или TFTP.

На рисунке 22.10 показано раскрывающееся меню подраздела Backup/Restore Configuration.

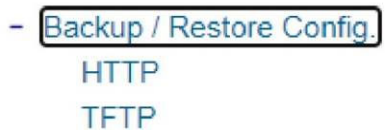


Рисунок 22.10. Раскрывающееся меню подраздела Backup/Restore Config.

22.4.1 Подраздел HTTP меню Backup/Restore Config

На рисунке 22.11 показана сетевая страница для настройки параметров резервного копирования и восстановления через протокол HTTP.

Данный подраздел разделен на две части: Backup the Configuration и Restore the Configuration.

Если щелкнуть с указателем на кнопке Download в верхнем окне на странице (Backup the Configuration), система выведет подсказку с запросом открыть файл с именем IP-10.0.50.1.bin или сохранить файл в месте назначения, указанном пользователем.

После выбора опции Save File резервная копия текущей конфигурации коммутатора будет сохранена на локальном устройстве хранения локального компьютера.

Чтобы восстановить файл с параметрами конфигурации на коммутаторе из резервной копии, перейдите в нижнее окно под названием Restore the Configuration и щелкните с указателем на кнопке Browse, чтобы выбрать нужный файл с параметрами конфигурации на локальном устройстве хранения.

Прежде чем щелкнуть с указателем на кнопке Upload, пользователь может установить флажки для опций под именем загружаемого файла, чтобы сохранить текущие настройки имени пользователя и пароля и текущие настройки сети.

Это позволит избежать необходимости входа в систему с использованием ранее сохраненного имени и пароля пользователя или изменения параметров конфигурации сети после восстановления конфигурации коммутатора.

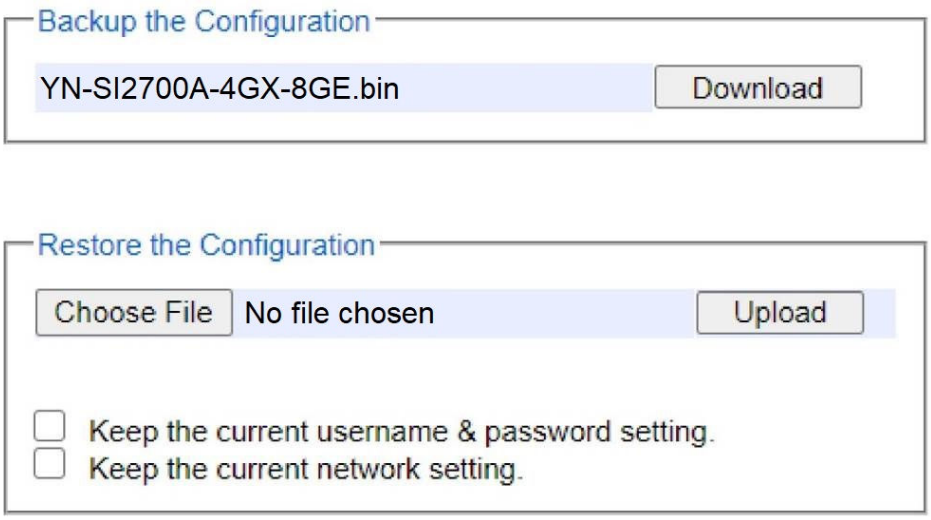


Рисунок 22.11. Подраздел HTTP меню Backup/Restore Config.

22.4.2 Подраздел TFTP меню Backup/Restore Config

Тривиальный протокол передачи файлов (TFTP) представляет собой компактный интуитивно понятный протокол. Пользователь может выгрузить параметры конфигурации на TFTP-сервер для создания резервной копии, а также загрузить резервную копию с TFTP-сервера, если возникнет необходимость восстановить или заменить текущую конфигурацию промышленного управляемого коммутатора.

На рисунке 22.12 показана сетевая страница подраздела TFTP, которая разделена на три части: Download the Configuration from TFTP, Upload the Configuration to TFTP и DHCP Option 66/67 Setting. Описание настраиваемых параметров протокола TFTP в сводном виде представлено в таблице 22.9.

• Чтобы выгрузить файл с параметрами конфигурации на TFTP-сервер, пользователь должен указать IP-адрес TFTP-сервера и имя удаленного файла. После завершения ввода щелкните с указателем на кнопке Download.

• Чтобы загрузить файл с параметрами конфигурации с TFTP-сервера, пользователь должен указать IP-адрес TFTP-сервера и имя удаленного файла. После завершения ввода щелкните с указателем на кнопке Upload.

• В нижней части сетевой страницы подраздела TFTP расположено окно настройки функции Option 66/67 под названием DHCP Option 66/67 Setting. Эта опция позволяет управляемому коммутатору распознавать имя TFTP-сервера и имя файла начальной загрузки, которые передаются в блоке данных IPv4-пакетов протокола DHCP с функцией Option 66 (RFC 2132), и имя файла, которое передается в блоке данных IPv4-пакетов протокола DHCP с функцией Option 67 (RFC 2132). Чтобы активировать эту функцию, установите флажок в поле Enable и щелкните с указателем на кнопке Update.

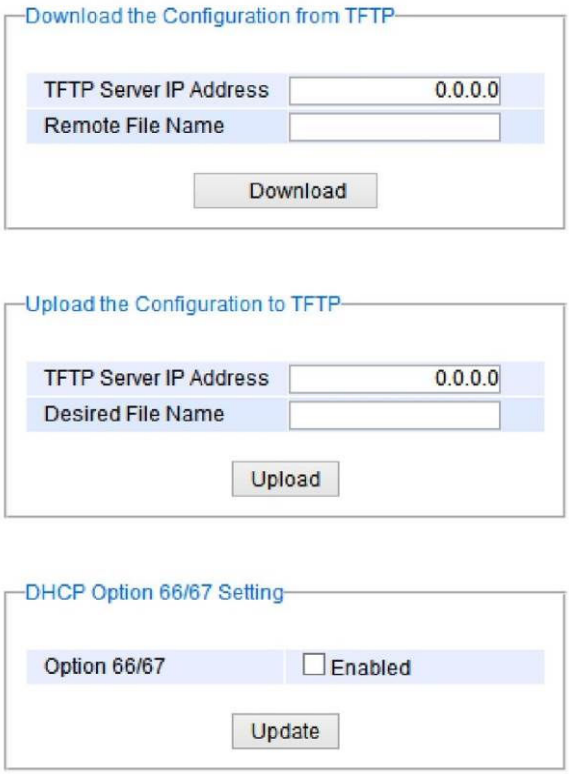


Рисунок 22.12. Подраздел TFTP меню Backup/Restore Config.

Таблица 22.9. Описание настраиваемых параметров протокола TFTP.

Имя параметра	Описание	Заводская настройка по умолчанию
TFTP Server IP Address	Указывается IP-адрес доменного имени удаленного TFTP-сервера.	Не заполняется
Remote File Name	Вводится с клавиатуры имя выгружаемого файла.	Не заполняется
Download	Щелкните с указателем на этой кнопке, чтобы начать выгрузку удаленного файла с конфигурацией в коммутатор.	
Desired File Name	Вводится с клавиатуры имя загружаемого файла.	Не заполняется
Upload	Щелкните с указателем на этой кнопке, чтобы загрузить файл с конфигурацией коммутатора на удаленный TFTP-сервер.	
Option 66/67	Активируйте эту опцию, чтобы управляемый коммутатор распознавал имя TFTP-сервера и имя файла по данным в пакетах протокола DHCP.	Отключено
Update	Щелкните с указателем на этой кнопке, чтобы сохранить настройки функции Option 66/67 протокола DHCP.	

22.4.3 Подраздел SCP меню Backup/Restore Config

Пользователям разрешается загружать параметры конфигурации на сервер защищенного копирования (SCP) в качестве резервной копии и загружать эти параметры с сервера SCP, когда это необходимо, для восстановления или замены конфигурации промышленного управляемого коммутатора. На рисунке 22.13 показана веб-страница SCP: Сервер SCP, имя пользователя,

пароль и путь к удаленному файлу.

В таблице 22.10 обобщены описания настроек SCP.

• Чтобы скачать файл конфигурации с SCP-сервера, пользователю необходимо указать IP-адрес SCP-сервера, имя пользователя SCP-сервера, пароль и имя удаленного файла. Затем нажмите кнопку Download.

• Чтобы загрузить файл конфигурации на SCP-сервер, пользователю необходимо указать IP-адрес SCP-сервера, имя пользователя SCP-сервера, пароль и имя файла. Затем нажмите кнопку Upload.

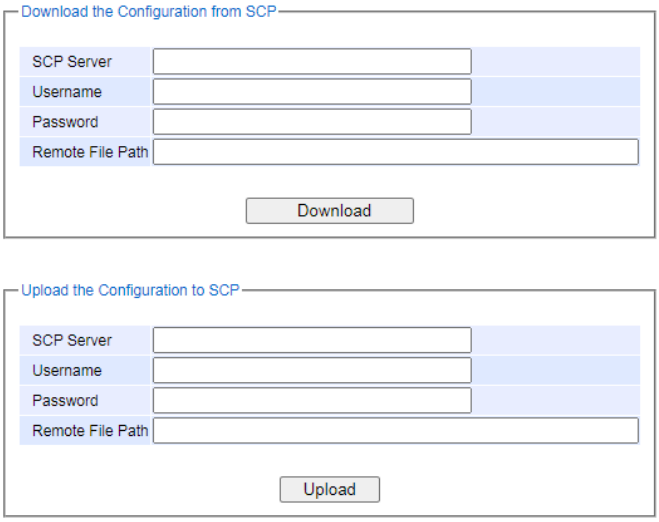


Рисунок 22.13. Подраздел SCP меню Backup/Restore Config.

Таблица 22.10. Описание настраиваемых параметров протокола SCP.

Имя параметра	Описание
SCP Server	IP-адрес сервера защищенного копирования (SCP)
Username	Имя пользователя для файлового сервера
Password	Пароль для файлового сервера
Remote File Path	Путь к файлу ПО, хранящемуся на файловом сервере

22.4.4 Подраздел SFTP меню Backup/Restore Config

Пользователям разрешается загружать параметры конфигурации на SSH сервер передачи файлов (SFTP) в качестве резервной копии и загружать эти параметры с сервера SFTP, когда это необходимо, для восстановления или замены конфигурации промышленного управляемого коммутатора. На рисунке 22.14 показана веб-страница SFTP: Сервер SFTP, имя пользователя, пароль и путь к удаленному файлу.

В таблице 22.11 обобщены описания настроек SFTP.

• Чтобы скачать файл конфигурации с SFTP-сервера, пользователю необходимо указать IP-адрес SFTP-сервера, имя пользователя SFTP-сервера, пароль и имя удаленного файла. Затем нажмите кнопку Download.

Чтобы загрузить файл конфигурации на SFTP-сервер, пользователю необходимо указать IP-адрес SFTP-сервера, имя пользователя SFTP-сервера, пароль и имя файла. Затем нажмите кнопку Upload.

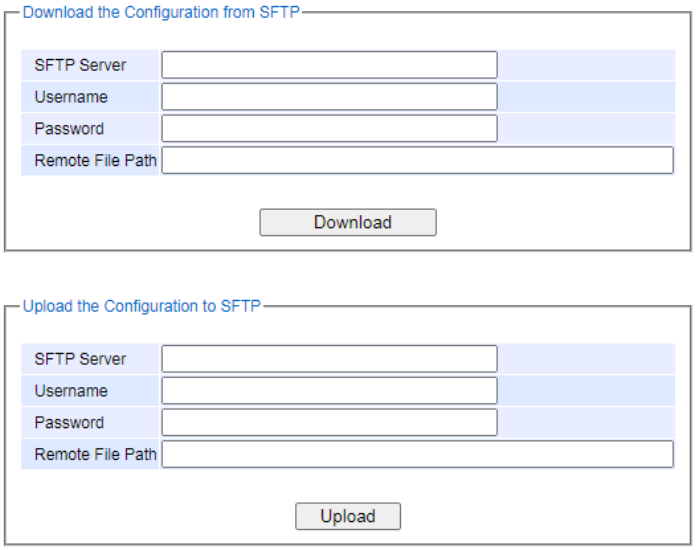


Рисунок 22.14. Подраздел SCP меню Backup/Restore Config.

Таблица 22.11. Описание настраиваемых параметров протокола SCP.

Имя параметра	Описание
SFTP Server	IP-адрес сервера протокола передачи файлов (SFTP)
Username	Имя пользователя для файлового сервера
Password	Пароль для файлового сервера
Remote File Path	Путь к файлу ПО, хранящемуся на файловом сервере

22.5 Подраздел Firmware Update

Пользователь может обновить встроенное микропрограммное обеспечение устройства через сетевой интерфейс, как показано на рисунке 22.15.

Чтобы обновить встроенное микропрограммное обеспечение, пользователь может запросить новый файл в компании Yarus Networks и сохранить его на локальном компьютере.

Затем нужно щелкнуть с указателем на кнопке Browse и выбрать нужный файл со встроенным микропрограммным обеспечением.

Такой файл для данного коммутатора имеет расширение ".dld", например: как YN-SI2700A-4GX-8GE.dld. После этого пользователь должен щелкнуть с указателем на кнопке Update и дождаться завершения процесса обновления.

В альтернативном варианте встроенное микропрограммное обеспечение можно обновить, используя утилиту управления устройствами.

ПРИМЕЧАНИЕ: не отключайте питание коммутатора и не разрывайте соединение с компьютером во время обновления встроенного микропрограммного обеспечения.

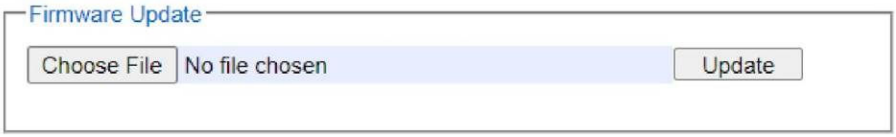


Рисунок 22.15. Сетевая страница подраздела Firmware Update.

22.6 Подраздел Factory Default Setting

Если управляемый коммутатор работает со сбоями, пользователь может сбросить его параметры на заводские настройки по умолчанию.

Для этого нужно щелкнуть с указателем на кнопке Reset, как показано на рисунке 22.16.

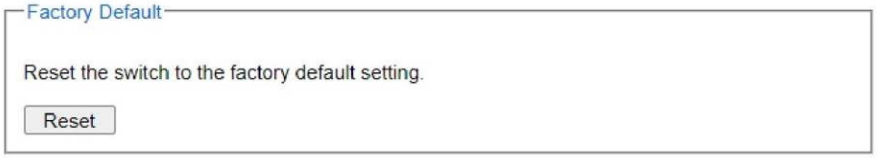


Рисунок 22.16. Сетевая страница подраздела Factory Default Setting.

22.7 Подраздел Reboot

Для перезагрузки коммутатора на этой сетевой странице не требуется никаких сложных действий.

Достаточно просто щелкнуть с указателем на кнопке Reboot, как показано на рисунке 22.17.

Рисунок 22.17. Сетевая страница подраздела Reboot.

22.8 Подраздел Logout

Для выхода из системы на этой сетевой странице не требуется никаких сложных действий. Достаточно просто щелкнуть с указателем на кнопке Logout, как показано на рисунке 22.18.

Рисунок 22.18. Сетевая страница подраздела Logout.

23 НАСТРОЙКА ПАРАМЕТРОВ С ИСПОЛЬЗОВАНИЕМ ПОСЛЕДОВАТЕЛЬНОЙ КОНСОЛИ

Параметры конфигурации управляемого коммутатора также можно настраивать с помощью последовательной консоли. Следует отметить, что для подключения последовательной консоли к консольному порту, который расположен в верхней части корпуса коммутатора, потребуется специальный кабель.

Такой кабель можно заказать, в том числе, у компании Yarus Networks.

Метод настройки в основном подобен методу настройки через интернет-браузер.

23.1 Настройка параметров последовательной консоли

Сначала нужно установить программу Putty, а затем - выполнить следующие действия для получения доступа к утилите последовательной консоли.

Запустите программу Putty.

В первоначальном разделе Session, рисунок 23.1, установите флажок в поле Serial, выберите используемый COM порт (Serial line) и установите скорость соединения 115200 (Speed). Дополнительные параметры сессии изменяются в разделе Serial, эти значения для полей Stop bits и Data bits остаются неизменны, 1 и 8 соответственно.

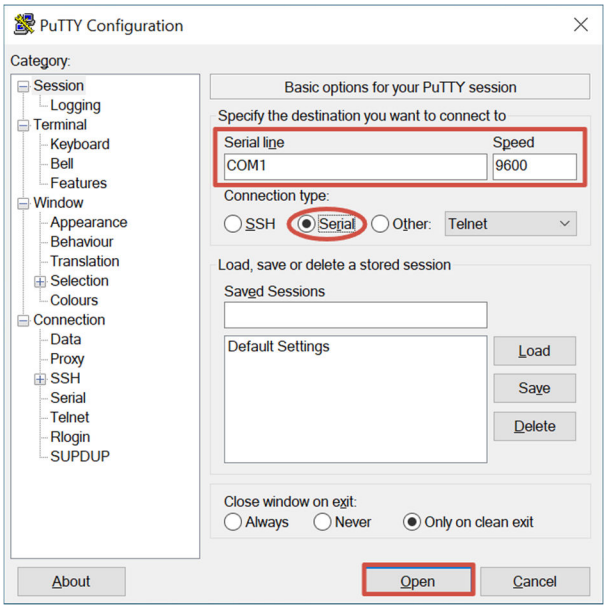


Рисунок 23.1. Создание нового соединения в программе Putty.

После завершения ввода параметров щелкните по кнопке Open, чтобы перейти в интерфейс командной строки.

23.2 Введение в интерфейс командной строки

На уровне интерфейса командной строки действует два типа полномочий - оператора и менеджера. Пользователи с полномочиями оператора могут только просматривать

информацию, в то время как пользователи с полномочиями менеджера могут не только просматривать информацию, но и изменять значения параметров конфигурации.

Полномочия оператора и менеджера исходно настраиваются без паролей, но для подтверждения полномочий оператора или менеджера можно настроить соответствующие пароли пользователей.

Если настроены пароли, то при попытке пользователя получить доступ к интерфейсу командной строки система запросит имя пользователя и пароль.

Если пользователь, работающий в непривилегированном режиме, желает переключиться в привилегированный режим, он может просто ввести команду "enable", после чего система выведет подсказки, где нужно будет ввести правильное имя пользователя и пароль:

Switch > enable

Username: (здесь указывается имя пользователя)

Password: (здесь указывается пароль)

Switch#

Чтобы получить доступ к настройке параметров, нужно войти с полномочиями менеджера, а затем ввести команду "configure":

Switch# configure

Switch(config)#

В качестве иллюстрации режимов на рисунке 23.2 показаны полномочия и соответствующие подсказки.

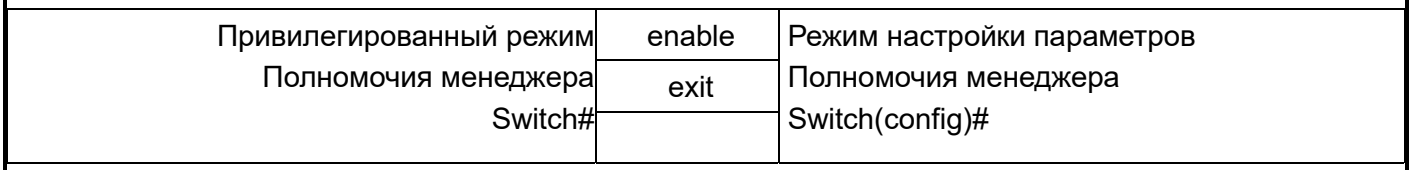


Рисунок 23.2. Режимы, полномочия и подсказки.

В командном режиме пользователь может в любой момент ввести опцию "?", и интерфейс командной строки выдаст все возможные команды, соответствующие ключевым словам:

Switch(config)# ip ?

ip Configure network setting

ipv6 Configure network setting

ip-routing IP Routing configuration

Пользователь может использовать клавишу табуляции для автоматического завершения ключевого слова:

Switch(config)# sysl <Tab>

Switch(config)# syslog

23.3 Общие команды

В таблице ниже приведены некоторые полезные команды, которые можно в любое время

использовать в режиме настройки через последовательную консоль.

Таблица 23.1. Описание команд.

Команды	Описание
Configure	Вход в режим настройки параметров конфигурации.
?	Перечисление всех доступных вариантов.
Exit	Возврат к предыдущему меню.
Logout	Выход из интерфейса командной строки.
No history	Отключение записи истории команд.
Show history	Вывод списка последних команд, записанных в истории.

24 ПРИМЕРЫ КОМАНД

Последовательная консоль предназначена для добавления, удаления или изменения значений параметров конфигурации, то есть, она используется с той же целью, что и интернет-браузер при настройке сетевым методом.

Оба метода поддерживают подобную функциональность.

На рисунке ниже показаны все опции, доступные в режиме интерфейса командной строки.

В следующих подразделах приведено описание двух примеров настройки административных параметров и параметров связующего дерева с использованием последовательной консоли. Очевидно, что функции и последовательность аналогичны таковым, описанным в соответствующих разделах (Administration и Spanning Tree).

Рисунок 24.1. Примеры команд.

24.1 Настройка административных параметров с помощью последовательной консоли

В этом разделе объясняется, как пользователь может находить нужную административную информацию и вносить изменения, используя команды.

В таблице ниже в сводном виде представлено описание команд, используемых для проверки и настройки административных параметров.

Таблица 24.1. Описание команд, используемых для проверки и настройки административных параметров.

Команда	Описание
vlan ip address 1 dhcp enable	Активировать протокол DHCP.
show vlan ip address 1	Показать состояние протокола DHCP.
vlan ip address 1 <IP-адрес> <маска подсети>	Настроить IP-адрес и маску подсети.
Ip default-gateway <IP-адрес>	Настроить IP-адрес шлюза (должен быть предварительно активирован протокол DHCP).
show vlan ip address	Показать IP-адрес и маску подсети.
reload	Эта команда используется для перезагрузки коммутатора.
show running-config	Показать текущую конфигурацию коммутатора.
copy running-config startup-config	Создать резервную копию конфигурации коммутатора.
erase startup-config	Во время следующей начальной загрузки выполнить сброс на заводские настройки по умолчанию.
show arp	Показать таблицу преобразования IP-адресов протокола ARP.
ping ip-addr <1 ~ 999>	Передать эхо-запрос протокола ICMP на хост-устройство в сети. Значение параметра <1 ~ 999> задает число повторов.

24.2 Настройка параметров связующего дерева (STP) с помощью последовательной консоли

В этом разделе объясняется, как пользователь может находить нужную информацию о связующем дереве и вносить изменения, используя команды.

Таблица 24.2. Описание команд, используемых для настройки параметров связующего дерева.

Команда	Описание
[no] spanning-tree enable	Активация / отключение функции связующего дерева.
[no] spanning-tree bpdu-guard enable	Активация / отключение функции BPDU-guard для защиты топологии связующего дерева.
spanning-tree forward-delay <4 ~ 30>	Установить продолжительность задержки переадресации в секундах. Пример: spanning-tree forward-delay 20: устанавливается значение времени задержки, равное 20 секундам.
spanning-tree hello-time <1 ~ 10>	Установить продолжительность интервала передачи сообщений приветствия в секундах.
spanning-tree maximum-age <6 ~ 40>	Установить максимальное время жизни связующего дерева в секундах.
spanning-tree priority <0 ~ 61440>	Установить приоритет моста связующего дерева.

Команда	Описание
spanning-tree protocol-version <mstp/rstp/stp>	Выбрать версию протокола. Подробное описание вариантов (MSTP, RSTP и STP) можно найти в разделе с описанием связующих деревьев.
[no] spanning-tree port edge-port <номер порта>	Установить порт в качестве граничного соединения.
[no] spanning-tree port enable-stp <номер порта>	Активация / отключение функции связующего дерева на определенном порте.
[no] spanning-tree port enable-bpdu-guard <номер порта>	Активация / отключение функции BPDU-guard для защиты топологии связующего дерева на определенном порте.
[no] spanning-tree port non-stp <номер порта>	Активация или отключение протокола связующего дерева на данном порте.
spanning-tree port path-cost <0 ~ 2E8><номер порта>	Указать стоимость пути для определенного порта.
spanning-tree port priority <0 ~ 240><номер порта>	Назначить приоритет указанному порту.
[no] spanning-tree port point-to-point-mac <auto | true | false> <номер порта>	Установить порт в качестве двухточечного соединения. Auto: установить режим автоматического обнаружения двухточечного канала. True: установить значение "истинно" для двухточечного канала. False: установить значение "ложно" для канала.
show spanning-tree	Показать информацию о связующем дереве.
show spanning-tree port <номер порта>	Показать информацию о порте.

25 НАСТРОЙКА ПАРАМЕТРОВ С ИСПОЛЬЗОВАНИЕМ КОНСОЛИ TELNET

В качестве еще одного альтернативного метода настройки параметров конфигурации коммутатора можно использовать метод подключения по протоколу Telnet, который описан в данной главе.

25.1 Программа Telnet

Telnet представляет собой программу, с помощью которой можно с удаленного терминала входить в систему любого удаленного сервера telnet.

Эта программа входит в состав пакета большинства операционных систем.

Чтобы использовать эту программу, пользователь должен перейти в режим командной строки (например, ввести команду cmd.exe в операционной системе Windows).

25.2 Вход с регистрацией в программу Telnet

Когда откроется терминал командной строки, введите с клавиатуры команду "telnet 10.0.50.1", как показано на рисунке 25.1.

Обратите внимание, что команда telnet всегда вводится с последующим параметром, которым может быть IP-адрес или доменное имя. В данном примере значение IP-адреса по умолчанию равно 10.0.50.1.

Если пользователь изменит IP-адрес коммутатора, он также должен будет использовать новый адрес для входа в систему.

Рисунок 25.1. Команда Telnet.

25.3 Интерфейс командной строки для Telnet

После ввода командной строки telnet открывается окно интерфейса коммутатора, показанное на рисунке 25.2.

Рисунок 25.2. Экран входа в систему при использовании программы Telnet.

Пользователь увидит экран приглашения в интерфейс коммутатора.

Система автоматически регистрирует пользователя в привилегированном режиме. Команды настройки параметров также подобны командам, используемым для последовательной консоли.

25.4 Команды в привилегированном режиме

Если пользователь не знает, какие команды используются для настройки параметров в режиме командной строки, он может ввести знак вопроса ("?") для отображения всех команд на экране, как показано на рисунке 25.3.

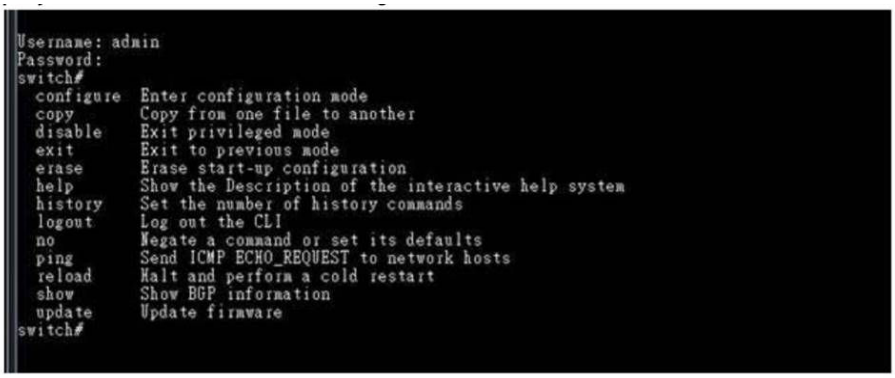


Рисунок 25.3. Команды в привилегированном режиме.

25.5 Команды в режиме настройки параметров

Если ввести знак вопроса ("?") в режиме настройки параметров, на экране будет выведен длинный перечень команд, как показано на рисунке 25.4.

В таблице 25.1 перечислены все команды, которые можно использовать для настройки параметров коммутатора в этом режиме.

Рисунок 25.4. Команды в режиме настройки параметров.

Таблица 25.1. Команды в режиме настройки параметров.

Команда	Описание
alert	Предупреждающая информация
boot	Перезагрузите коммутатор
cos-mapping	Информация CoS mapping
clear	Очистить значения в целевом протоколе
copy	Скопировать конфигурацию
cring	Конфигурация Compatible-Ring
disable	Отключите команду привилегированного режима
dscp-mapping	Информация DSCP mapping
dhcp	Настройка параметров протокола DHCP
dot1x	Настройка параметров протокола 802.1x
dipswitch	Информация о DIP-переключателе
daylight-saving-time	Переход на летнее время
exit	Выйдите из текущего режима и перейдите в предыдущий режим
erase	Удалить конфигурацию
erps	Информация о ERPS
filter	Отфильтруйте информацию об исходном MAC-адресе
garp	Информация о GARP
gvrp	Информация о GVRP
help	Описание интерактивной справочной системы
history	Установите количество команд для ведения журнала
ip	Информация об IP-адресе
igmp	Информация о IGMP
ia-ring	Конфигурация iA-кольца
logout	Выйдите из системы
lldp	Информация о LLDP
lacp	Информация о LACP
mac-age-time	Включите время истечения срока действия для MAC-адреса
mirror-port	Информация о мониторинге порта
mac-address-table	Информация из таблицы MAC-адресов
no	Отменить команду или установить значения по умолчанию
password	Информация о пароле
port	Информация о порте
ping	Отправить ICMP ECHO_REQUEST узлам сети
ptp	Информация о PTP

Команда	Описание
qos	Информация о QoS
radius-server	Информация о сервере Radius
show	Отображать информацию о текущей запущенной системе
stormfilter	Штормовой фильтр для всех видов трафика (широковещательный, многоадресный, Unitcast)
security	Конфигурация безопасности статического порта
system	Системная информация
sntp	Включить SNTP
systemtime	Настройка системного времени
syslog	Информация системного журнала
smtp	Конфигурация SMTP
snmp	Информация SNMP
spanning-tree	Протокол связующего дерева
timeout	Установите текущий тайм-аут CLI
trunk	Транкинговая информация
uring	Конфигурация U-образного кольца
vlan	Информация о VLAN

26 ГЛОССАРИЙ

Термин	Описание
802.1	Рабочая группа по стандартам Института инженеров электротехники и электроники (IEEE), имеющим отношение к локальным сетям.
802.1p	Реализованы механизмы поддержки функции качества сервиса (QoS) на уровне управления доступом к среде (MAC).
802.1x	Стандарт IEEE для управления доступом к сети на основе портов. Он включает поддержку механизма проверки подлинности устройств, желающих подключиться к LAN или WLAN.
Широковещательная передача	Передача пакетов данных в широковещательном режиме всем узлам локальной сети.
Клиент	Устройство, которое используют услуги, предоставляемые другими участниками сети.
DES	Стандарт шифрования данных, описывающий блочный шифр, в котором применяется алгоритм шифрования с помощью совместно используемого секретного ключа. Он основан на алгоритме с симметричным ключом, который использует 56-разрядный ключ.
DHCP	Протокол динамической конфигурации хост-устройств поддерживает автоматическую настройку параметров конфигурации компьютера без необходимости вмешательства сетевого администратора. Он также автоматически блокирует назначение одного IP-адреса двум компьютерам одновременно. Протокол DHCP используется в двух версиях: одна для интернет-протокола версии 4 (IPv4), а другая - для версии 6 (IPv6).
DNS	Система доменных имен представляет собой иерархическую структуру, используемую для именования компьютеров, сервисов и любых других ресурсов, работающих в интернет-сетях. Эта система привязывает доменные имена к числовым идентификаторам. Например, доменное имя www.google.com преобразовывается в адрес 74.125.153.104.
EAP	Открытый протокол аутентификации - инструментарий проверки подлинности, широко используемый в стандартах IEEE.
Ethernet	В звездообразной физической транспортной среде все станции могут передавать данные одновременно. Возникающие при этом конфликты обнаруживаются и исправляются с помощью сетевых протоколов.
Шлюз	Предоставляет доступ к другим компонентам сети на основе многоуровневой модели взаимодействия открытых систем. Пакеты данных, которые не направляются непосредственно локальному партнеру, передаются на шлюз. Шлюз поддерживает обмен данными с удаленными сетями.
IEEE	Институт инженеров по электротехнике и электронике.
IGMP	Протокол управления группами в сети Интернет используется в IPv4-сетях для включения пользователей в группы многоадресной передачи.
IP	Интернет-протокол.
IPv4	Версия 4 интернет-протокола представляет собой четвертую редакцию протокола сети Интернет. Вместе с протоколом версии IPv6 образует ядро интернет-сети. В данной версии используются 32-разрядные адреса. Таким образом, протокол этой версии позволяет назначить в общей сложности только 2^32 различных уникальных адресов. По причине этого ограничения в настоящее время наблюдается нехватка IPv4-адресов, которые стали дефицитным ресурсом. Эта проблема стимулировала разработку версии IPv6, которая пока еще находится на относительно ранней стадии.

Термин	Описание
LAN	Локальная вычислительная сеть представляет собой сеть, которая объединяет устройства в пределах географически ограниченной зоны, такой как компания или компьютерная лаборатория.
MAC	Управление доступом к среде представляет собой подуровень канального уровня, который описан в модели взаимодействия открытых систем. Этот подуровень поддерживает механизмы управления адресацией и доступом к каналам, позволяющие узлам сети связываться друг с другом в пределах LAN.
MAC-адрес	Уникальный идентификатор, который назначается сетевому интерфейсу для связи в сегменте сети. Он формируется согласно правилам нумерации пространств имен, которые регулируются стандартами IEEE.
MD5	Алгоритм выборки сообщений 5 широко используется для шифрования. Поддерживает хэш-функцию с 128-разрядным значением.
Многоадресная передача	Режим передачи, в котором сообщения от одного хост-устройства одновременно передаются нескольким хост-устройствам. При этом принимать многоадресную передачу могут только те хост-устройства, которые принадлежат к определенной группе многоадресной передачи. Кроме того, в сети, поддерживающей многоадресную передачу, передается только один экземпляр информации до точки, в которой путь до членов группы начинает разветвляться. В точках ветвления создаются копии многоадресных пакетов, которые затем соответственно переадресовываются. Такой подход обеспечивает возможность управления большим объемом трафика, адресованного в различные места назначения, с эффективным использованием пропускной способности сети.
Модель взаимодействия открытых систем	Модель взаимодействия открытых систем предоставляет возможность деления системы передачи данных на меньшие части, которые называются уровнями. Уровень представляет собой набор концептуально подобных функций, которые предоставляют сервисы для следующего верхнего уровня и получают сервисы от предыдущего нижнего уровня.
QoS	Качество сервиса.
RADIUS	Сервис удаленной проверки подлинности пользователя при коммутируемом подключении поддерживает протокол аутентификации и мониторинга на прикладном уровне для проверки подлинности, защиты целостности и учета доступа к сети.
Сервер	Устройство, которое предоставляет сервисы в сети.
SMTP	Простой протокол обмена почтовыми сообщениями SMTP представляет собой стандартный интернет-протокол, который используется для передачи электронной почты по IP-сети.
SNMP	Простой протокол управления сетью используется для управления устройствами в IP-сетях. В управляемых системах он представляет данные управления в форме переменных, которые описывают конфигурацию системы.

27 ТАБЛИЦА РАСПРЕДЕЛЕНИЯ ПАМЯТИ ДЛЯ ПРОТОКОЛА MODBUS

1. Регистры чтения (поддерживают функциональные коды 3, 4).

2. Регистры записи (поддерживают функциональный код 6).

3. 1 слово = 2 байта.

Адрес	Тип данных	Чтение / запись	Описание
Информация о системе			
0 x 0000 (0)	32 слова	Чтение	Описание система = "Managed Switch" Слово 0, старший байт = 'M' Слово 0, младший байт = 'a' Слово 1, старший байт = 'n' Слово 1, младший байт = 'a' Слово 2, старший байт = 'g' Слово 2, младший байт = 'e' Слово 3, старший байт = 'd' Слово 3, младший байт = ' ' Слово 4, старший байт = 'S' Слово 4, младший байт = 'w' Слово 5, старший байт = 'i' Слово 5, младший байт = 't' Слово 6, старший байт = 'c' Слово 6, младший байт = 'h' Слово 7, старший байт = ' ' Слово 7, младший байт = 'E' Слово 8, старший байт = 'H' Слово 8, младший байт = '7' Слово 9, старший байт = '5' Слово 9, младший байт = '1' Слово 10, старший байт = '0' Слово 10, младший байт = '10'
0 x 0020 (32)	1 слово	Чтение	Версия встроенного микропрограммного обеспечения = Пример: Версия = 1.02 Слово 0, старший байт = 0 x 01 Слово 0, младший байт = 0 x 02
0 x 0021 (33)	3 слова	Чтение	MAC-адрес Ethernet Пример: MAC = 00-01-02-03-04-05 Слово 0, старший байт = 0 x 00 Слово 0, младший байт = 0 x 01

Адрес	Тип данных	Чтение / запись	Описание
			Слово 1, старший байт = 0 x 02 Слово 1, младший байт = 0 x 03 Слово 2, старший байт = 0 x 04 Слово 2, младший байт = 0 x 05
0 x 0024 (36)	1 слово	Чтение	Версия ядра Пример: Версия = 1.03 Слово 0, старший байт = 0 x 01 Слово 0, младший байт = 0 x 03
Информация о консоли			
0 x 0030 (48)	1 слово	Чтение	Скорость передачи в бодах 0 x 0000: 4800
			0 x 0001: 9600 0 x 0002: 14400 0 x 0003: 19200 0 x 0004: 28800 0 x 0005: 38400 0 x 0006: 57600 0 x 0007: 144000 0 x 0008: 115200
0 x 0031 (49)	1 слово	Чтение	Информационные биты 0 x 0007: 7 0 x 0008: 8
0 x 0032 (50)	1 слово	Чтение	Четность 0 x 0000: Нет 0 x 0001: Нечетные 0 x 0002: Четные
0 x 0033 (51)	1 слово	Чтение	Стоповый бит: 0 x 0001: 1 0 x 0002: 2
0 x 0034 (52)	1 слово	Чтение	Управление потоками: 0 x 0000: Нет
Информация о питании			
0 x 0040 (64)	1 слово	Чтение	Состояние питания Питание 1 OK, старший байт = 0 x 01 Питание 1 отказ, старший байт = 0 x 00 Питание 2 OK, младший байт = 0 x 01 Питание 2 отказ, младший байт = 0 x 00
Информация о стеке IP-протоколов			
0 x 0050 (80)	1 слово	Чтение	Состояние протокола DHCP 0 x 0000: Отключено

Адрес	Тип данных	Чтение / запись	Описание
			0 x 0001: Активировано
0 x 0051 (81)	2 слова	Чтение	IP-адрес коммутатора Пример: IP = 192.168.1.1 Слово 0, старший байт = 0 x C0 Слово 0, младший байт = 0 x A8 Слово 1, старший байт = 0 x 01 Слово 1, младший байт = 0 x 01
0 x 0053 (83)	2 слова	Чтение	Маска подсети коммутатора Пример: IP = 255.255.255.0 Слово 0, старший байт = 0 x FF Слово 0, младший байт = 0 x FF Слово 1, старший байт = 0 x FF Слово 1, младший байт = 0 x 00
0 x 0055 (85)	2 слова	Чтение	Адрес шлюза коммутатора Пример: IP = 192.168.1.254 Слово 0, старший байт = 0 x C0 Слово 0, младший байт = 0 x A8 Слово 1, старший байт = 0 x 01 Слово 1, младший байт = 0 x FE
0 x 0057 (87)	2 слова	Чтение	DNS-сервер 1 коммутатора Пример: IP = 168.95.1.1 Слово 0, старший байт = 0 x A8 Слово 0, младший байт = 0 x 5F Слово 1, старший байт = 0 x 01 Слово 1, младший байт = 0 x 01
0 x 0059 (89)	2 слова	Чтение	DNS-сервер 2 коммутатора Пример: IP = 168.95.1.1 Слово 0, старший байт = 0 x A8 Слово 0, младший байт = 0 x 5F Слово 1, старший байт = 0 x 01 Слово 1, младший байт = 0 x 01
Очистка данных о состоянии системы			
0 x 0100 (256)	1 слово	Запись	Очистка данных статистики портов 0 x 0001: выполнить действие очистки
0 x 0101 (257)	1 слово	Запись	Очистка данных статистики реле 0 x 0001: выполнить действие очистки
0 x 0102 (258)	1 слово	Запись	Очистка данных обо всех настораживающих событиях 0 x 0001: выполнить действие очистки
Информация о настораживающих событиях			

Адрес	Тип данных	Чтение / запись	Описание
0 x 0200 (512)	64 слова	Чтение	Информация о первом настораживающем событии
0 x 0300 (768)	64 слова	Чтение	Информация о втором настораживающем событии
0 x 0400 (1024)	64 слова	Чтение	Информация о третьем настораживающем событии
0 x 0500 (1280)	64 слова	Чтение	Информация о четвертом настораживающем событии
0 x 0600 (1536)	64 слова	Чтение	Информация о пятом настораживающем событии
Состояние портов			
0 x 1000 (4096)	5 слов	Чтение	Состояние порта: 0 x 0000: Отключено 0 x 0001: Активировано Слово 0, старший байт = состояние порта 1 Слово 0, младший байт = состояние порта 2 Слово 1, старший байт = состояние порта 3 Слово 1, младший байт = состояние порта 4 Слово 2, старший байт = состояние порта 5 Слово 2, младший байт = состояние порта 6 Слово 3, старший байт = состояние порта 7 Слово 3, младший байт = состояние порта 8 Слово 4, старший байт = состояние порта 9 Слово 4, младший байт = состояние порта 10
0 x 1020 (4128)	5 слов	Чтение	Согласование портов: Принудительный режим = 0 x 00 Автоматический режим = 0 x 01 Слово 0, старший байт = состояние порта 1 Слово 0, младший байт = состояние порта 2 Слово 1, старший байт = состояние порта 3 Слово 1, младший байт = состояние порта 4 Слово 2, старший байт = состояние порта 5 Слово 2, младший байт = состояние порта 6 Слово 3, старший байт = состояние порта 7 Слово 3, младший байт = состояние порта 8 Слово 4, старший байт = состояние порта 9 Слово 4, младший байт = состояние порта 10
0 x 1040 (4160)	5 слов	Чтение	Скорость передачи через порт: Состояние 10 M = 0 x 01 Состояние 100 M = 0 x 02 Состояние 1000 M = 0 x 03 Слово 0, старший байт = состояние порта 1 Слово 0, младший байт = состояние порта 2

Адрес	Тип данных	Чтение / запись	Описание
			Слово 1, старший байт = состояние порта 3 Слово 1, младший байт = состояние порта 4 Слово 2, старший байт = состояние порта 5 Слово 2, младший байт = состояние порта 6 Слово 3, старший байт = состояние порта 7 Слово 3, младший байт = состояние порта 8 Слово 4, старший байт = состояние порта 9 Слово 4, младший байт = состояние порта 10
0 x 1060 (4192)	5 слов	Чтение	Тип дуплексного режима порта: Полудуплексный режим = 0 x 00 Полнодуплексный режим = 0 x 01 Слово 0, старший байт = состояние порта 1 Слово 0, младший байт = состояние порта 2 Слово 1, старший байт = состояние порта 3 Слово 1, младший байт = состояние порта 4 Слово 2, старший байт = состояние порта 5 Слово 2, младший байт = состояние порта 6 Слово 3, старший байт = состояние порта 7 Слово 3, младший байт = состояние порта 8 Слово 4, старший байт = состояние порта 9 Слово 4, младший байт = состояние порта 10
0 x 1080 (4224)	5 слов	Чтение	Управление потоками на порте: Состояние "отключено" = 0 x 00 Состояние "активировано" = 0 x 01 Слово 0, старший байт = состояние порта 1 Слово 0, младший байт = состояние порта 2 Слово 1, старший байт = состояние порта 3 Слово 1, младший байт = состояние порта 4 Слово 2, старший байт = состояние порта 5 Слово 2, младший байт = состояние порта 6 Слово 3, старший байт = состояние порта 7 Слово 3, младший байт = состояние порта 8 Слово 4, старший байт = состояние порта 9 Слово 4, младший байт = состояние порта 10
0 x 10A0 (4256)	5 слов	Чтение	Состояние канала порта: Состояние "отключен" = 0 x 00 Состояние "активен" = 0 x 01 Слово 0, старший байт = состояние порта 1

Адрес	Тип данных	Чтение / запись	Описание
			Слово 0, младший байт = состояние порта 2 Слово 1, старший байт = состояние порта 3 Слово 1, младший байт = состояние порта 4 Слово 2, старший байт = состояние порта 5 Слово 2, младший байт = состояние порта 6 Слово 3, старший байт = состояние порта 7 Слово 3, младший байт = состояние порта 8 Слово 4, старший байт = состояние порта 9 Слово 4, младший байт = состояние порта 10
0 x 1200 (4608)	20 слов	Чтение	Скорость передачи данных через порт: Пример: Порт 1 работает со скоростью передачи данных (1024 кБ/сек = 0 x 400). Слово 0 для порта 1 = 0 x 0000 Слово 1 для порта 1 = 0 x 0400 Слова 0, 1 = скорость передачи данных через порт 1 Слова 2, 3 = скорость передачи данных через порт 2 Слова 4, 5 = скорость передачи данных через порт 3 Слова 6, 7 = скорость передачи данных через порт 4 Слова 8, 9 = скорость передачи данных через порт 5 Слова 10, 11 = скорость передачи данных через порт 6 Слова 12, 13 = скорость передачи данных через порт 7 Слова 14, 15 = скорость передачи данных через порт 8 Слова 16, 17 = скорость передачи данных через порт 9 Слова 18, 19 = скорость передачи данных через порт 10
0 x 1280 (4736)	20 слов	Чтение	Скорость приема данных через порт: Пример: Порт 1 работает со скоростью приема данных (1024 кБ/сек = 0 x 400). Слово 0 для порта 1 = 0 x 0000 Слово 1 для порта 1 = 0 x 0400 Слова 0, 1 = скорость приема данных через порт 1 Слова 2, 3 = скорость приема данных через порт 2 Слова 4, 5 = скорость приема данных через порт 3 Слова 6, 7 = скорость приема данных через порт 4 Слова 8, 9 = скорость приема данных через порт 5 Слова 10, 11 = скорость приема данных через порт 6 Слова 12, 13 = скорость приема данных через порт 7 Слова 14, 15 = скорость приема данных через порт 8 Слова 16, 17 = скорость приема данных через порт 9 Слова 18, 19 = скорость приема данных через порт 10

Адрес	Тип данных	Чтение / запись	Описание
0 x 1300 (4864)	40 слов	Чтение	Количество переданных нормальных пакетов данных: Пример: Порт 1 передал 0 x 2EEEE1 FFFF нормальных пакетов данных. Слово 0 для порта 1 = 0 x 0000 Слово 1 для порта 1 = 0 x 002E Слово 2 для порта 1 = 0 x EEE1 Слово 3 для порта 1 = 0 x FFFF Слова 0, 1, 2, 3 = количество нормальных пакетов, переданных через порт 1 Слова 4, 5, 6, 7 = количество нормальных пакетов, переданных через порт 2 Слова 8, 9, 10, 11 = количество нормальных пакетов, переданных через порт 3 Слова 12, 13, 14, 15 = количество нормальных пакетов, переданных через порт 4 Слова 16, 17, 18, 19 = количество нормальных пакетов, переданных через порт 5 Слова 20, 21, 22, 23 = количество нормальных пакетов, переданных через порт 6 Слова 24, 25, 26, 27 = количество нормальных пакетов, переданных через порт 7 Слова 28, 29, 30, 31 = количество нормальных пакетов, переданных через порт 8 Слова 32, 33, 34, 35 = количество нормальных пакетов, переданных через порт 9 Слова 36, 37, 38, 39 = количество нормальных пакетов, переданных через порт 10
0 x 1400 (5120)	40 слов	Чтение	Количество переданных пакетов данных с ошибками: Пример: Порт 1 передал 0 x 2EEEE1 FFFF пакетов данных с ошибками. Слово 0 для порта 1 = 0 x 0000 Слово 1 для порта 1 = 0 x 002E Слово 2 для порта 1 = 0 x EEE1 Слово 3 для порта 1 = 0 x FFFF Слова 0, 1, 2, 3 = количество пакетов с ошибками, переданных через порт 1 Слова 4, 5, 6, 7 = количество пакетов с ошибками, переданных через порт 2 Слова 8, 9, 10, 11 = количество пакетов с ошибками, переданных через порт 3 Слова 12, 13, 14, 15 = количество пакетов с ошибками, переданных через порт 4 Слова 16, 17, 18, 19 = количество пакетов с ошибками, переданных через порт 5

Адрес	Тип данных	Чтение / запись	Описание
			Слова 20, 21, 22, 23 = количество пакетов с ошибками, переданных через порт 6 Слова 24, 25, 26, 27 = количество пакетов с ошибками, переданных через порт 7 Слова 28, 29, 30, 31 = количество пакетов с ошибками, переданных через порт 8 Слова 32, 33, 34, 35 = количество пакетов с ошибками, переданных через порт 9 Слова 36, 37, 38, 39 = количество пакетов с ошибками, переданных через порт 10
0 x 1500 (5376)	40 слов	Чтение	Количество принятых нормальных пакетов данных: Пример: Порт 1 принял 0 x 2EEEE1 FFFF нормальных пакетов данных. Слово 0 для порта 1 = 0 x 0000 Слово 1 для порта 1 = 0 x 002E Слово 2 для порта 1 = 0 x EEE1 Слово 3 для порта 1 = 0 x FFFF Слова 0, 1, 2, 3 = количество нормальных пакетов, принятых через порт 1 Слова 4, 5, 6, 7 = количество нормальных пакетов, принятых через порт 2 Слова 8, 9, 10, 11 = количество нормальных пакетов, принятых через порт 3 Слова 12, 13, 14, 15 = количество нормальных пакетов, принятых через порт 4 Слова 16, 17, 18, 19 = количество нормальных пакетов, принятых через порт 5 Слова 20, 21, 22, 23 = количество нормальных пакетов, принятых через порт 6 Слова 24, 25, 26, 27 = количество нормальных пакетов, принятых через порт 7 Слова 28, 29, 30, 31 = количество нормальных пакетов, принятых через порт 8 Слова 32, 33, 34, 35 = количество нормальных пакетов, принятых через порт 9 Слова 36, 37, 38, 39 = количество нормальных пакетов, принятых через порт 10
0 x 1600 (5632)	40 слов	Чтение	Количество принятых пакетов данных с ошибками: Пример: Порт 1 принял 0 x 2EEEE1 FFFF пакетов данных с ошибками. Слово 0 для порта 1 = 0 x 0000 Слово 1 для порта 1 = 0 x 002E Слово 2 для порта 1 = 0 x EEE1 Слово 3 для порта 1 = 0 x FFFF

Адрес	Тип данных	Чтение / запись	Описание
			Слова 0, 1, 2, 3 = количество пакетов с ошибками, принятых через порт 1 Слова 4, 5, 6, 7 = количество пакетов с ошибками, принятых через порт 2 Слова 8, 9, 10, 11 = количество пакетов с ошибками, принятых через порт 3 Слова 12, 13, 14, 15 = количество пакетов с ошибками, принятых через порт 4 Слова 16, 17, 18, 19 = количество пакетов с ошибками, принятых через порт 5 Слова 20, 21, 22, 23 = количество пакетов с ошибками, принятых через порт 6 Слова 24, 25, 26, 27 = количество пакетов с ошибками, принятых через порт 7 Слова 28, 29, 30, 31 = количество пакетов с ошибками, принятых через порт 8 Слова 32, 33, 34, 35 = количество пакетов с ошибками, принятых через порт 9 Слова 36, 37, 38, 39 = количество пакетов с ошибками, принятых через порт 10
Информация о резервировании			
0 x 2000 (8192)	1 слово	Чтение	Протокол резервирования: 0 x 0000: Нет 0 x 0001: STP 0 x 0002: RSTP 0 x 0004: ERPS 0 x 0008: iA-Ring 0 x 0010: Compatible Ring
0 x 2100 (8448)	1 слово	Чтение	Корень протокола STP: 0 x 0000: Не корень 0 x 0001: Корень 0 x FFFF: Протокол RSTP не активирован
0 x 2101 (8449)	5 слов	Чтение	Состояние порта с поддержкой протокола STP: 0 x 00: Отключено 0 x 01: Прослушивание 0 x 02: Распознавание 0 x 03: Переадресация 0 x 04: Блокирование 0 x 05: Отбрасывание 0 x FF: Протокол RSTP не активирован Слово 0, старший байт = состояние порта 1 Слово 0, младший байт = состояние порта 2

Адрес	Тип данных	Чтение / запись	Описание
			Слово 1, старший байт = состояние порта 3 Слово 1, младший байт = состояние порта 4 Слово 2, старший байт = состояние порта 5 Слово 2, младший байт = состояние порта 6 Слово 3, старший байт = состояние порта 7 Слово 3, младший байт = состояние порта 8 Слово 4, старший байт = состояние порта 9 Слово 4, младший байт = состояние порта 10
0 x 2200 (8704)	5 слов	Чтение	Идентификатор VLAN кольца для защитной функции ERPS: Пример: Идентификатор третьей VLAN = 1, слово 2 = 0 x 0001 1 ~ 4094: Диапазон значений идентификаторов 0 x 0000: Идентификатор VLAN не задан Слово 0 = идентификатор первой VLAN Слово 1 = идентификатор второй VLAN Слово 2 = идентификатор третьей VLAN Слово 3 = идентификатор четвертой VLAN Слово 4 = идентификатор пятой VLAN
0 x 2230 (8752)	5 слов	Чтение	Западный порт защитной функции ERPS: Пример: Третий западный порт = порт 2, слово 2 = 0 x 0002 0 x 0001: Порт 1 0 x 0002: Порт 2 0 x 000A: Порт 10 0 x 000C: Агрегированный порт 1 0 x 000D: Агрегированный порт 2 0 x 000E: Агрегированный порт 3 0 x 000F: Виртуальный канал 0 x 00FF: Идентификатор VLAN существует, но западный порт не выбран 0 x FFFF: Защитная функция ERPS не активирована Слово 0 = западный порт первой VLAN Слово 1 = западный порт второй VLAN Слово 2 = западный порт третьей VLAN Слово 3 = западный порт четвертой VLAN Слово 4 = западный порт пятой VLAN
0 x 2240 (8768)	5 слов	Чтение	Восточный порт защитной функции ERPS: Пример: Третий восточный порт = порт 3, слово 2 = 0 x 0003 0 x 0001: Порт 1

Адрес	Тип данных	Чтение / запись	Описание
			0 x 0002: Порт 2 0 x 000A: Порт 10 0 x 000C: Агрегированный порт 1 0 x 000D: Агрегированный порт 2 0 x 000E: Агрегированный порт 3 0 x 000F: Виртуальный канал 0 x 00FF: Идентификатор VLAN существует, но восточный порт не выбран 0 x FFFF: Защитная функция ERPS не активирована Слово 0 = восточный порт первой VLAN Слово 1 = восточный порт второй VLAN Слово 2 = восточный порт третьей VLAN Слово 3 = восточный порт четвертой VLAN Слово 4 = восточный порт пятой VLAN
0 x 2250 (8784)	5 слов	Чтение	Состояние западного порта защитной функции ERPS: Пример: Состояние третьего западного порта = переадресация, слово 2 = 0 x 0001 0 x 0001: Переадресация 0 x 0002: Блокирование 0 x 0003: Блокирование по причине сбоя сигнала 0 x 000F: Виртуальный канал 0 x 00FF: Идентификатор VLAN существует, но западный порт не выбран 0 x FFFF: Защитная функция ERPS не активирована Слово 0 = состояние западного порта первой VLAN Слово 1 = состояние западного порта второй VLAN Слово 2 = состояние западного порта третьей VLAN Слово 3 = состояние западного порта четвертой VLAN Слово 4 = состояние западного порта пятой VLAN
0 x 2260 (8800)	5 слов	Чтение	Состояние восточного порта защитной функции ERPS: Пример: Состояние третьего восточного порта = блокирование, слово 2 = 0 x 0002 0 x 0001: Переадресация 0 x 0002: Блокирование 0 x 0003: Блокирование по причине сбоя сигнала 0 x 000F: Виртуальный канал 0 x 00FF: Идентификатор VLAN существует, но восточный порт не выбран 0 x FFFF: Защитная функция ERPS не активирована

Адрес	Тип данных	Чтение / запись	Описание
			Слово 0 = состояние восточного порта первой VLAN Слово 1 = состояние восточного порта второй VLAN Слово 2 = состояние восточного порта третьей VLAN Слово 3 = состояние восточного порта четвертой VLAN Слово 4 = состояние восточного порта пятой VLAN
0 x 2270 (8816)	5 слов	Чтение	Состояние узла защитной функции ERPS Пример: Состояние третьего узла = защита, слово 2 = 0 x 0001 0 x 0001: Нет 0 x 0002: Не используется 0 x 0003: Защита 0 x FFFF: Защитная функция ERPS не активирована Слово 0 = состояние узла первой VLAN Слово 1 = состояние узла второй VLAN Слово 2 = состояние узла третьей VLAN Слово 3 = состояние узла четвертой VLAN Слово 4 = состояние узла пятой VLAN
0 x 2280 (8832)	5 слов	Чтение	Владелец канала RPL защитной функции ERPS: 0 x 0000: Отключено 0 x 0001: Активировано
0 x 2300 (8960)	1 слово	Чтение	Состояние главного устройства защитной функции iA-Ring. 0 x 0000: Отключено 0 x 0001: Активировано 0 x FFFF: Защитная функция iA-Ring не активирована.
0 x 2301 (8961)	1 слово	Чтение	Первый порт кольцевой сети: Пример: Первый порт кольцевой сети = порт 2, слово 0 = 0 x 0002 0 x 0001: Порт 1 0 x 0002: Порт 2 0 x 000A: Порт 10 0 x FFFF: Защитная функцияyf не активирована.
0 x 2302 (8962)	1 слово	Чтение	Второй порт кольцевой сети: Пример: Второй порт кольцевой сети = порт 3, слово 0 = 0 x 0003 0 x 0001: Порт 1 0 x 0002: Порт 2 0 x 000A: Порт 10 0 x FFFF: Защитная функция iA-Ring не активирована.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ изм.	Номера листов и страниц				Всего листов (стр.) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					