SYMANITRON

Инновационные
промышленные сети

Руководство по настройке коммутаторов SEWM-RB-3GC, модулей PRP/HSR, PRP/HSR-GSFP

Дата издания: март 2021г.
Редакция: V1.1

Оглавление

Введение

Данный документ содержит информацию о настройках и возможностях программного обеспечения коммутаторов серий SEWM-RB-3GC. Кроме того, в документе приводится детальная информация по настройке коммутаторов с помощью WEB-интерфейса.

Структура документа

Данное руководство включает следующую информацию:

Основная информация	Описание
1. Информация о продукте	• Описание продукта • Модели • Возможности программного обеспечения
2. Способы подключения к устройству	• Обзор возможностей • Подключение через консольный порт • Подключение с использованием Telnet • Подключение через Web-интерфейс
3. Сведения об устройстве	• Основные сведения о коммутаторе
4. Основные настройки	• Пользовательские настройки • Настройка IP адресов • Системная информация • Выгрузка файлов • Обновление программного обеспечения • Загрузка файлов • Перезагрузка
5. Функционал	• Резервирование • PTP • Статистика
6. Другие настройки	• Настройка сигнализации • Настройка портов • Настройка MAC-адреса • SNTP • NTP • МЭК61850 MMS • SNMPv2 • SNMPv3 • Файл-сервер • LLDP • DDMI • Виртуальное тестирование кабеля • RADIUS • TACACS+ • AAA • LINE

Условные обозначения

1. Условные обозначения в тексте

Формат	Описание
< >	Скобки < > обозначают «кнопки». Например, нажмите кнопку <Apply>
[ ]	Скобки [ ] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]
{ }	Скобки { } обозначают группу. Например {IP address, MAC address} означает, что IP адрес и MAC адрес составляют группу и могут быть настроены и показаны вместе.
→	Мультиуровневое меню разделяется посредством знака «→». Например, Start→AllPrograms→Accessories. Нажмите меню [Start], войдите в подменю [All programs], затем войдите в подменю [Accessories].
/	Выбор одной, двух или более опций при помощи символа «/». Например, «Add/Subtract» означает добавить или удалить.
~	Знак «~» обозначает диапазон значений. Например, «1~255» указывает на диапазон от 1 до 255

2. Условные символы

Символ	Описание
 **Предостережение**	Эти вопросы требуют внимания во время работы с устройством при настройке, а также дают дополнительную информацию.
 **Заметка**	Необходимые пояснения к содержимому выполняемых операций с устройством.
 **Внимание**	Вопросы, требующие особого внимания. Некорректная работа с устройством может привести к потере данных или повреждению.

1. Информация об устройстве

1.1. Основная информация о коммутаторе

Коммутаторы серии SEWM-RB-3GC с функциями резервирования PRP/HSR специально разработаны для промышленных сетей высокой надежности с реализацией протоколов PRP (параллельного резервирования) и HSR (высоконадежного «бесшовного» резервирования) в соответствии со стандартом IEC62439-3. Устройства серии SEWM-RB-3GC могут обеспечить нулевую потерю данных в случае сбоя сети, гарантируя максимальную надежность ее работы. Полноценное аппаратное решение FPGA позволяет устройству серии SEWM-RB-3GC реализовать функционал протоколов HSR и PRP, обеспечивающих минимальную задержку восстановления сети. Устройство серии SEWM-RB-3GC поддерживает стандарт IEEE 1588v2 и позволяет обеспечить высокоточную синхронизацию времени.

1.2. Функциональные возможности ПО

Программное обеспечение коммутатора SEWM-RB-3GC поддерживает множество различных функций:

Позиция	описание
HSR/PRP	Поддержка протокола PRP,время восстановления – 0 мс Поддержка протокола HSR, время восстановления – 0 мс Поддержка PRP/HSR Coupling
IEEE1588v2	Поддержка режима TC (Transparent Clock) (IEEE1588-2008) Точность менее 1 мкс
VLAN и Порты	Скорость портов (1000M/100M/10M/авто) (Полно-/Полу-) дуплексный режим 802.1Q (1~4093) VLAN на основе портов
MAC-адрес	Настраиваемое автоматическое запоминание адресов и функция VLAN aware До 2000 MAC-адресов Поддержка функций MAC-Address Auto-Aging и Aging Timer
Протокол синхронизации времени	SNTP/NTP
Безопасность сети	Централизованное управление пользователями с использованием SSH, SSL

LLDP	Поддержка функций обучения LLDP-соседей, информации о соседях, статистики сообщений
Сервер IEC61850 MMS	Поддержка сервера IEC61850 MMS
Управление	DHCP-клиент FTP клиент/FTP сервер/SFTP клиент Утилита Ping Управление с консоли TELNET клиент/TELNET сервер Централизованное управление с использованием WEB SNMP (v1,v2c,v3) Работа ЦП Аварийный сигнал питания Аварийный сигнал порта (LinkDown) Перезагрузки (Reboot) для восстановления заводских настроек (set default) Отображение общего времени работы устройства

1.3. Поддерживаемые данной документацией продукты

SEWM-RB-3GC-HI-XX
SEWM-RB-3GC-24E-24E
Модуль PRP/HSR для коммутаторов серии GKT
Модуль PRP/HSR-GSFP для коммутаторов серии GKT

2. Подключение к устройству

Устройство можно настраивать одним из четырех нижеперечисленных способов:

- через консольный порт
- посредством Telnet/SSH
- с использованием WEB-интерфейса

2.1. Варианты просмотра и отображения

Когда пользователь (администратор сети) подключается к устройству посредством CLI через консольный порт или Telnet, он имеет возможность, используя различные команды, получать информацию о состоянии устройства и выполнять настройки коммутатора:

Подсказка	Тип отображения	Функция	Команда
SWITCH>	Основной режим	• Просмотр системного времени и даты • Отобразить версию ПО	Введите «Enable» для входа в привилегированный режим
SWITCH #	Привилегированный режим	• Настройка системного времени и даты • Загрузить/выгрузить конфигурационный файл • Удалить файл • Просмотр конфигурации коммутатора и системную информацию • Возврат к заводским настройкам • Запись текущих настроек • Перезагрузка коммутатора	Введите «**config**» для переключения из привилегированного режима в режим настройки Введите «**exit**» для возврата в основной режим
SWITCH (config) #	Режим Настройки	Настроить все функциональные возможности коммутатора	Введите «**exit**» для возврата в привилегированный режим

Когда выполняется настройка коммутатора посредством сервиса CLI, символ «?» может использоваться для получения помощи по используемым командам. Для получения помощи, нужно ввести описание параметров, например, <1,255> означает диапазон чисел, <H.H.H.H> означает IP адрес, <H:H:H:H:H:H> означает MAC адрес, word<1,31> означает диапазон строк. Также символы ↑ и ↓ могут использоваться для просмотра последних 10 команд.

2.2. Подключение через консольный порт

Пользователь может подключиться к устройству посредством консольного порта с помощью HyperTerminal операционной системы Windows или с помощью другого программного обеспечения, которое поддерживает подключение по последовательному порту, например HTT3.3. В примере ниже показано, как использовать консольный порт и HyperTerminal для доступа к коммутатору.

1. Подключите USB кабель к ПК и консольному интерфейсу устройства (кабель должен быть оснащён разъёмом DB9 с одной стороны и RJ45 с другой).
2. Запустите HyperTerminal в основном окне Windows, нажмите [Start]—>[All Programs]—>[Accessories]—>[Communications]—>[Hyper Terminal] (см. Рис. 1).

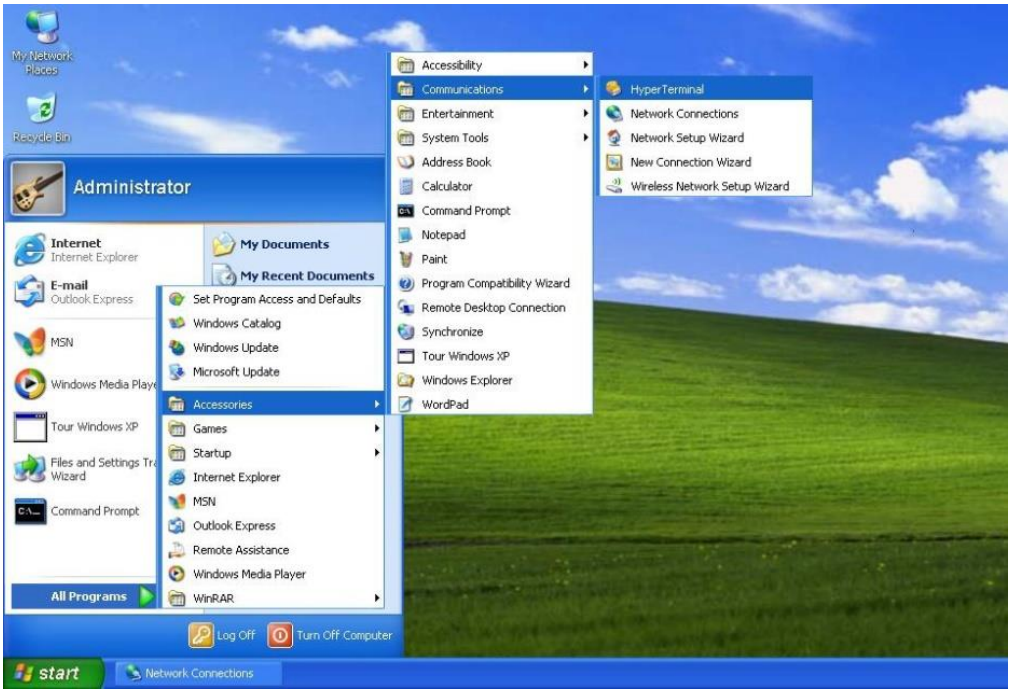


Рис. 1. Запуск HyperTerminal

3. Создайте новое подключение, например, с именем «Switch» (см. рис. 2).

Рис. 2. Создание нового подключения

4. Выберите COM порт для подключения.

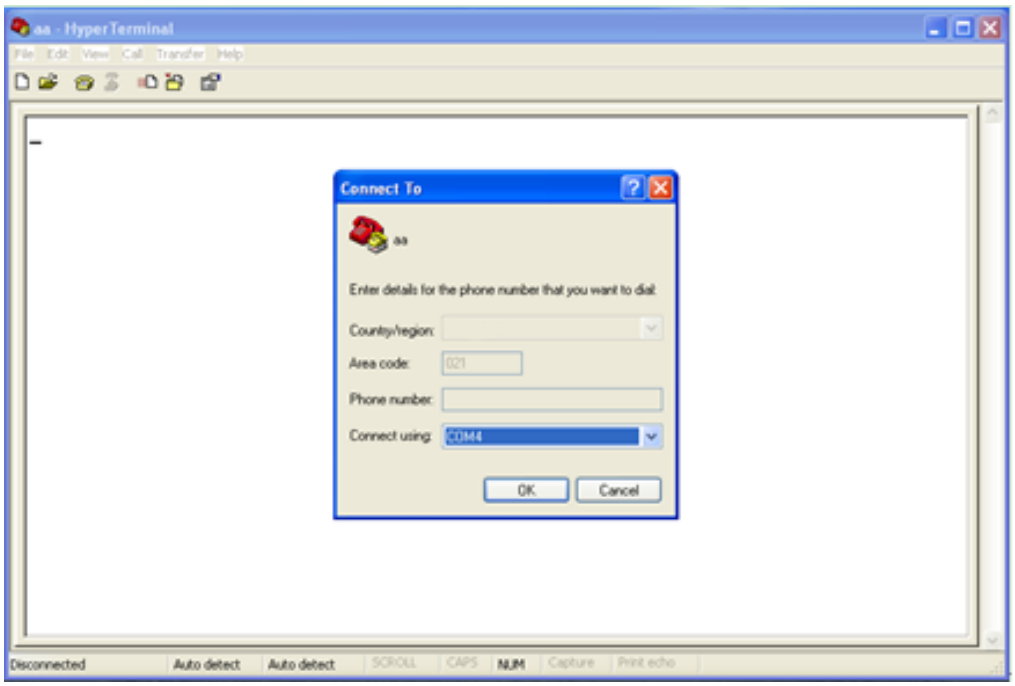


Рис. 3. Выбор COM порта для подключения

Для подтверждения COM порта нажмите [My Computer]->[Property]->[Hardware]->[Device Manager]->[Port] и проверьте работу порта, который используется как консольный.

5. Настройте параметры COM порта. Скорость (Baud rate): 115200, Биты данных (Data bits): 8, Чётность (Parity): None, Стоповые биты (Stop bits): 1, Контроль потока (Flow control): None.

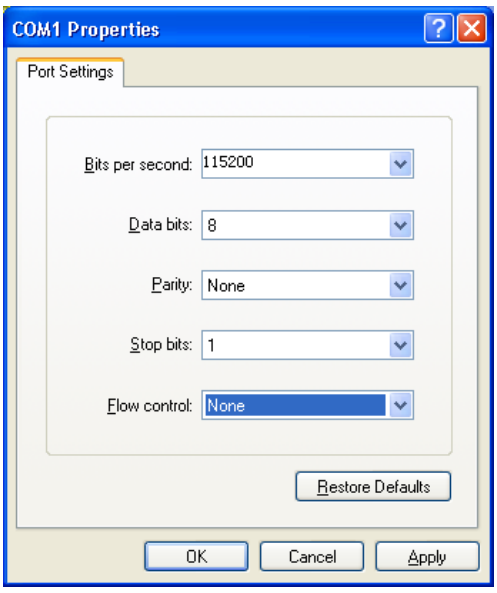


Рис. 4. Настройка параметров COM порта

6. Нажмите <OK> для входа в командную строку CLI. Нажмите <Enter> для входа в пользовательский режим.

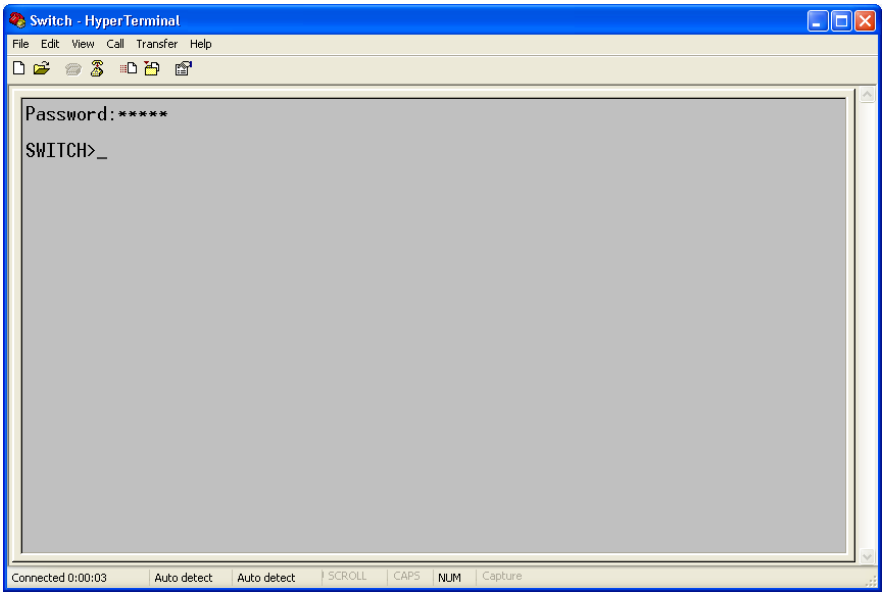


Рис. 5. Экран CLI

7. Введите команду «enable», пользователь по умолчанию «123», и пароль «123», чтобы войти в привилегированный режим. Вы также можете ввести имена других созданных пользователей и пароль, как показано ниже (рис. 6).

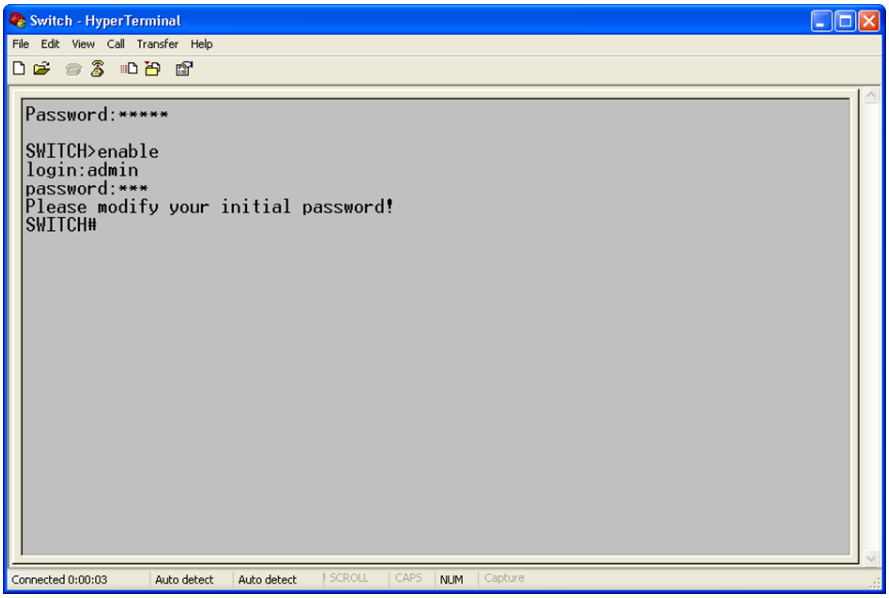


Рис. 6. Привилегированный режим

2.3. Подключение к коммутатору посредством Telnet

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.
2. Введите «telnet IP-адрес» в диалоговое окно «Запуск программы», по умолчанию IP-адрес - 192.168.0.2.

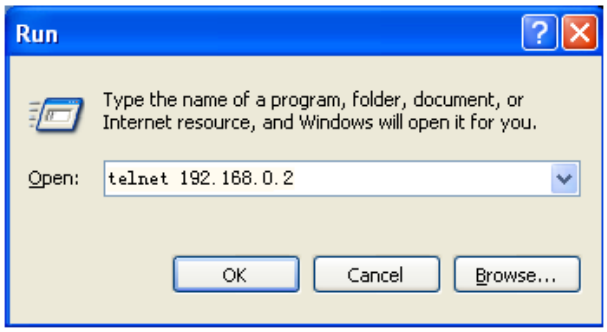


Рис. 7. Доступ через Telnet

При подтверждении IP-адреса, пожалуйста, обратитесь к разделу «IP-адрес» настоящего руководства для получении информации о IP-адресе.

3. В интерфейсе Telnet введите пароль по умолчанию «admin», чтобы войти в коммутатор. Вы можете также вводить других созданных пользователей и пароль, как показано ниже.

```
Password: *****
SWITCH> en
Password: *****
SWITCH#
```

Рис. 8. Интерфейс терминала Telnet

2.4. Доступ через WEB-интерфейс

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.
2. Введите IP адрес коммутатора в web-браузере (IP адрес по умолчанию - 192.168.0.2). Появится диалоговое окно авторизации. Введите: Логин – admin, пароль – 123. Нажмите кнопку <OK>. Вы можете также ввести другие логин и пароль созданные ранее.

При подтверждении IP-адреса, пожалуйста, обратитесь к разделу «IP-адрес» настоящего руководства для получении информации о IP-адресе.

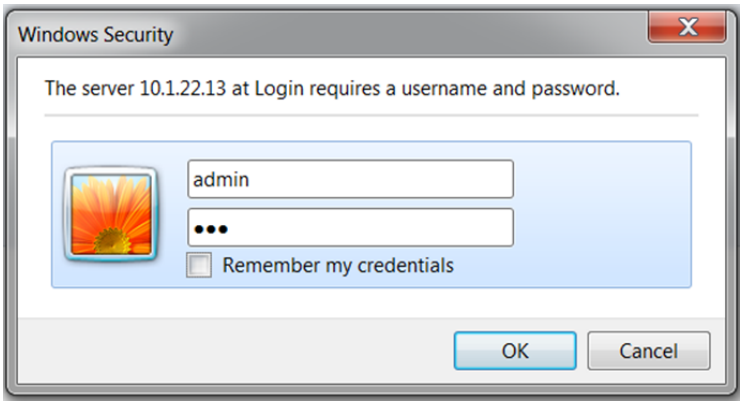


Рис. 9. Авторизация через WEB-интерфейс

3. После успешной авторизации на веб-странице управления коммутатором в верхней области отобразится дерево навигации по настройкам. Можно переключить режим конфигурации в левой области экрана. Зеленым цветом обозначен базовый режим, а красным цветом – расширенный режим. Расширенный режим предлагает больше прав, чем базовый режим. В нем пользователи могут выполнять настройки большего количества модулей устройства.

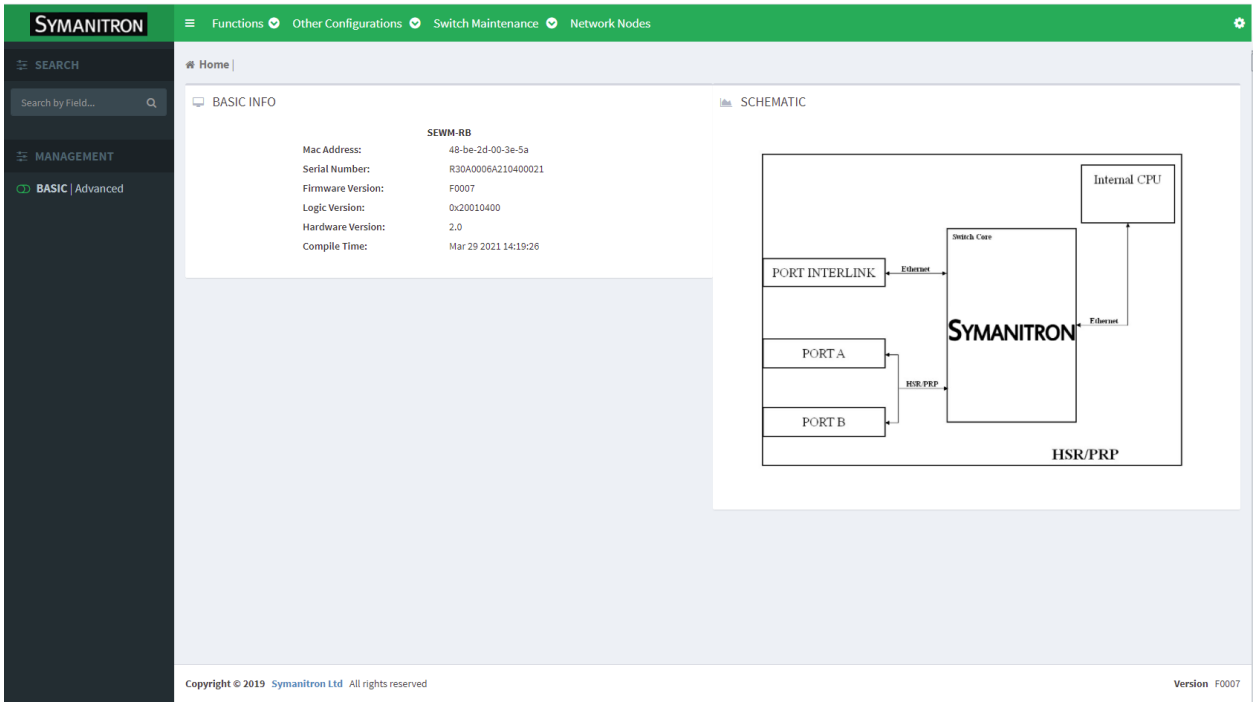


Рис. 10. Страница WEB-интерфейса

Нажав на значок «Symanitron» в верхнем левом углу, вы подключитесь к веб-интерфейсу, показанному на рис. 10. Нажмите на значок в виде «шестеренки» в верхнем правом углу и выберете «Logout», чтобы выйти обратно в режим входа в учетную запись. Здесь также можно производить конфигурацию других функций коммутатора.

3. Информация об устройстве

3.1. Основная информация о коммутаторе

Меню BASIC INFO, в основном, содержит базовую информацию о конфигурации устройства серии SEWM-RB-3GC, включая MAC-адрес, заводской номер, версию прошивки, версию логической схемы, аппаратную версию, время компиляции, как показано ниже (рис.11).

Рис. 11. Основная информация о коммутаторе

3.2. Схема коммутатора

Ниже представлена структурная схема коммутатора (рис. 11,12).

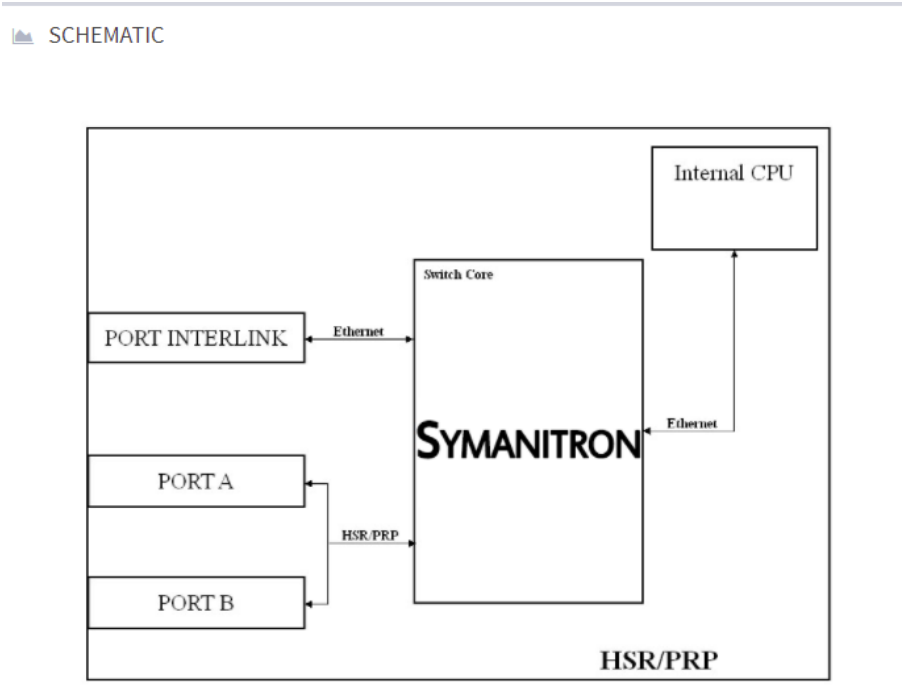


Рис. 12. Структурная схема коммутатора

4. Основные настройки коммутатора

Нажмите на значок шестеренки в правом верхнем углу главного интерфейса, чтобы настроить базовые данные о пользователе. Существует два режима – базовый и расширенный, где базовый режим предлагает различные базовые опции конфигурации. Расширенный режим предоставляет расширенные права и больше настраиваемых

элементов. Ниже показаны настраиваемые элементы коммутатора в расширенном и базовом режимах.

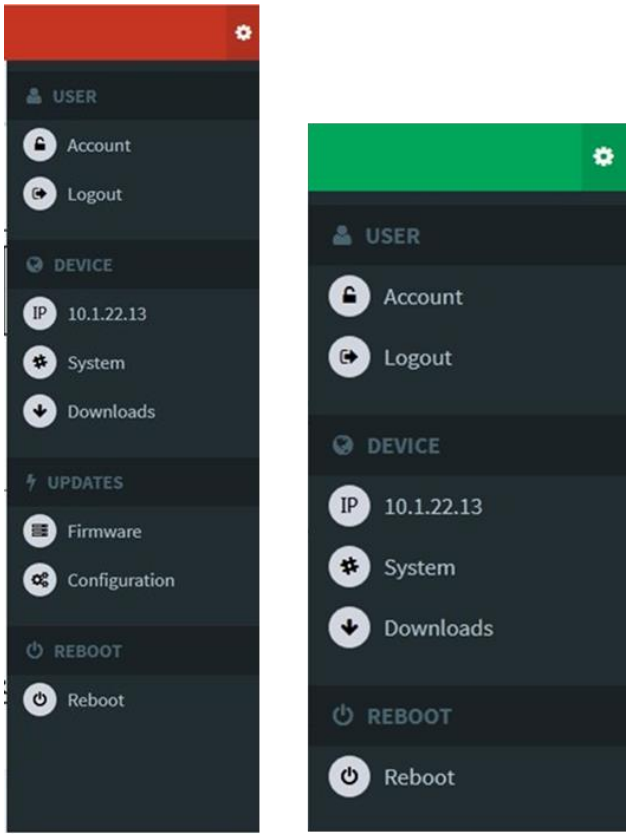


Рис. 13. Расширенный и базовый режимы

4.1. Настройка пользователя

Учетная запись в разделе User («Пользователь») служит для изменения пароля пользователя. Logout («Выход из системы») – это операция для выхода на веб-страницу входа.

4.2. Настройка IP

1. Просмотр IP-адреса коммутатора с использованием консольного порта

Войдите в интерфейс командной строки через порт консоли в режиме конфигурации под учетной записью привилегированного пользователя, введите команду «show interface ip brief». Отобразится IP-адрес коммутатора, как показано ниже:

```
SWITCH# show interface ip brief
Interface            Kname          IP-mode       Ipaddress            Mask                 Gateway
-------------------------------------------------------------------------------------------------------
port_interlink       eth1           Static        10.1.22.13           255.0.0.0            0.0.0.0
mgmt                 eth0           Static        192.168.10.2         255.255.255.0        --

SWITCH#
```

Рис. 14. Отображение IP-адреса

2. Нажмите на значок шестеренки в верхнем правом углу на главной веб-странице, выберете опцию IP в разделе [DEVICE] и войдите на страницу конфигурации IP. IP-адреса портов L и M также будут отображены в данном разделе, как показано ниже:

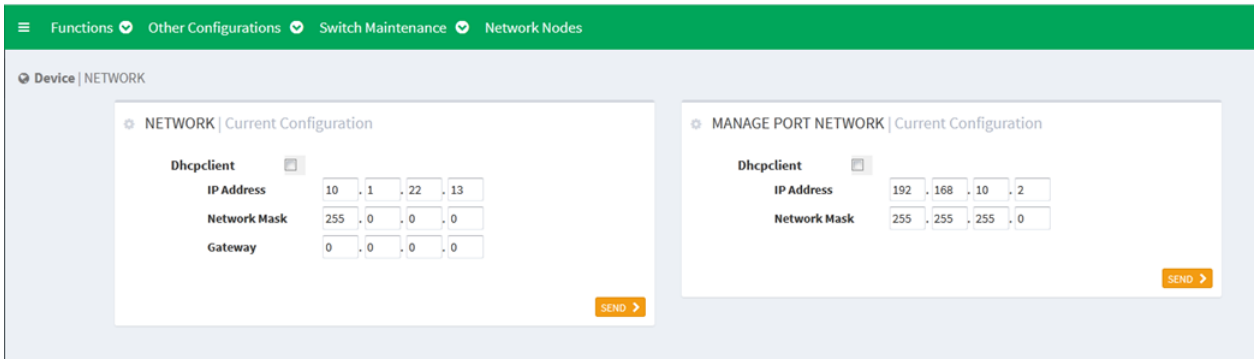


Рис. 15. Страница настроек IP-адресов коммутатора

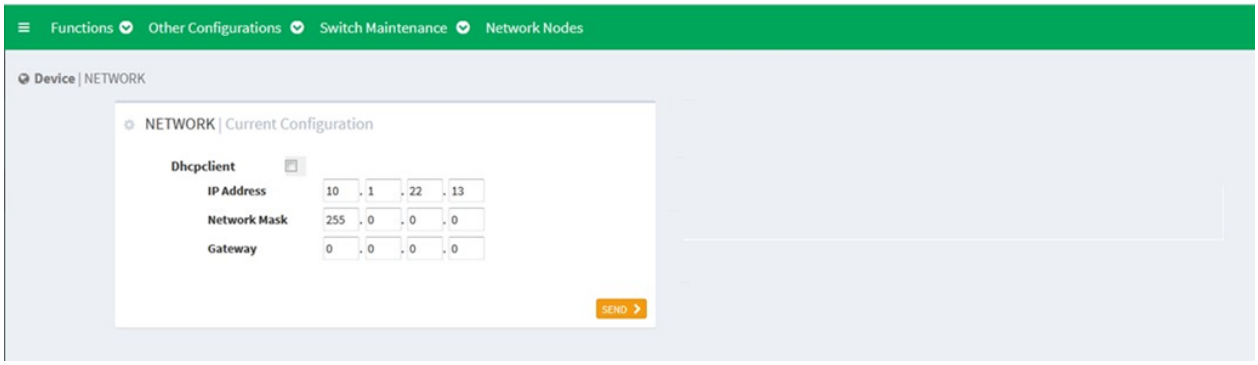


Рис. 16. Страница настроек IP-адресов модуля PRP/HSR

Сеть (NETWORK)

Функция: настройка IP-адреса порта L.

Управление сетевым портом (MANAGE PORT NETWORK)

Описание функции: настройка IP-адреса порта управления.

На данной странице настроек левая область служит для конфигурации IP-адреса порта L, а правая область – для конфигурации IP-адреса порта M.

Имеется поддержка настроек динамического IP-адреса и статического IP-адреса.

Устройство серии SEWM-RB-3GC имеет независимый порт управления, а модуль HSR/PRP независимого порта управления не имеет.

4.3. Настройка DHCP

4.3.1. Краткое описание DHCP

С постоянным расширением масштабов сетей и ростом их сложности, а также в условиях частого перемещения компьютеров (таких, например, как ноутбук) и их количества, превышающих количество выделяемых IP-адресов, протокол BootP, специально

предназначенный для конфигурации статического хоста, постоянно теряет способность удовлетворять реальные потребности в IP-адресах. Для быстрого доступа к сети, а также повышения коэффициента использования ресурсов IP-адресов действительно было необходимо разработать автоматический механизм для назначения IP-адресов на основе BootP. Для решения этих проблем был создан протокол DHCP (Dynamic Host Configuration Protocol, Протокол динамической настройки хостов).
Протокол DHCP использует модель взаимодействия клиент-сервер. Клиент отправляет запрос о конфигурации серверу, а сервер отвечает на параметры конфигурации, обеспечивая динамическую конфигурацию IP-адресов. Схема типичного варианта использования протокола DHCP показана на рисунке ниже.

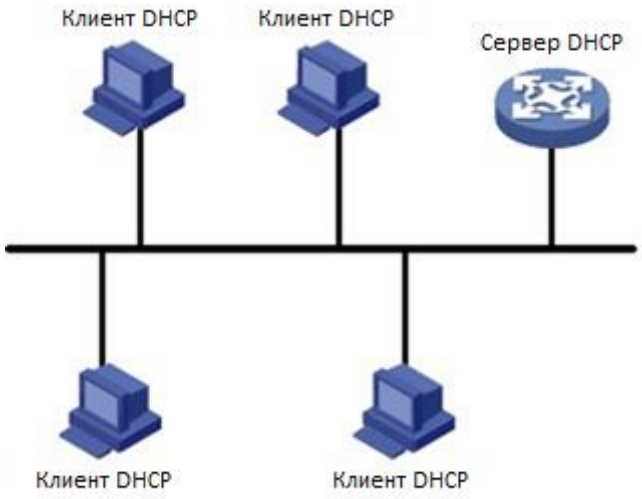


Рис. 17. Протокол DHCP

В процессе активного получения IP-адресов сообщения рассылаются путем широковещательной рассылки, поэтому требуется, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте. Если они находятся в разных сегментах, клиент может связаться с сервером через DHCP Relay, чтобы получить IP-адреса и параметры конфигурации.

Протокол DHCP поддерживает два механизма распределения IP-адресов.
Статическое распределение: сетевой администратор статично привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как, например, WWW-сервер, и отсылает привязанные IP-адреса клиентам через протокол DHCP. Динамическое распределение: DHCP-сервер производит динамическую раздачу IP-адреса клиенту. Этот механизм распределения может назначить постоянный IP-адрес или IP-адрес с ограниченным сроком пользования для клиента. Когда время аренды адреса истекает, клиент должен повторно запросить IP-адрес. Сетевой администратор может выбирать для каждого клиента свой механизм распределения по протоколу DHCP.

4.3.2. Настройка DHCP

Настоящее устройство не поддерживает настройки DHCP-сервера, только DHCP-клиента.

На рисунке ниже показана страница IP конфигурации порта L:

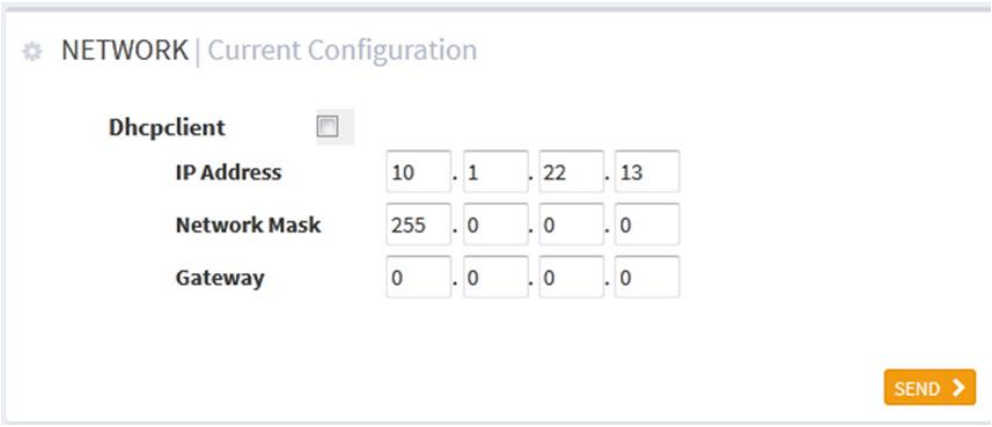


Рис. 18. Настройка IP-адреса порта L

Когда для порта значение <Dhcpclient> включено, клиент может получает IP-адрес у удаленного сервера. При этом, когда <Dhcpclient> находится в активном состоянии, другие элементы конфигурации на странице невозможно выбрать для изменения. Обновив страницу, мы увидим, что DHCP-клиент успешно получил IP-адрес. Если получить IP-адрес не удается, в качестве текущего адреса можно использовать предыдущий IP-адрес. Маска и шлюз те же самые, восстанавливается последнее значение конфигурации.

4.4. Настройка статического IP-адреса

IP-адрес и маску сети порта L можно выполнить путем настройки вручную, как показано на рис. 18.

IP-адрес (IP Address)

Формат: A.B.C.D

Функция: настройка IP-адреса вручную

Сетевая маска (Network Mask)

Формат: A.B.C.D

Функция: настройка вручную маски сети.

- Данная модель коммутатора поддерживает настройку IP-адреса только порта L и порта M. Каждый IP-интерфейс относится к одному IP-адресу.
- Разные IP-интерфейсы должны быть настроены на IP-адреса для разных сегментов сети.

Шлюз (Gateway)
Формат: A.B.C.D
Функция: настройка адреса шлюза вручную
Адрес шлюза должен принадлежать к тому же сегменту сети, что и IP-адрес, в противном случае возможно возникновение ошибок.

5. Сведения о системе

Нажмите на значок шестеренки в правом верхнем углу на главной веб-странице, выберите [SYSTEM] в разделе [DEVICE] и войдите на страницу System information («Сведения о системе»), как показано ниже.

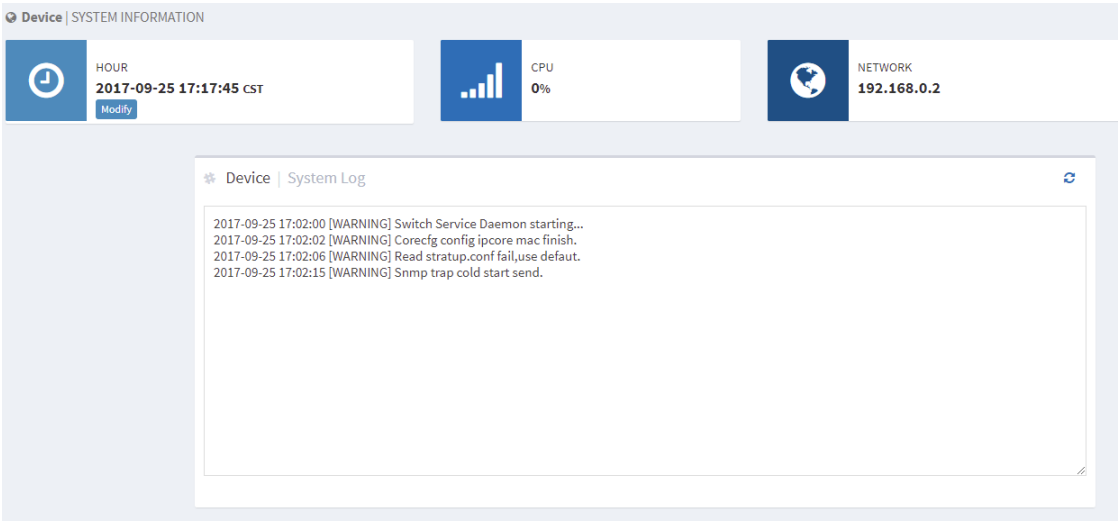


Рис. 19. Страница информации о системе

Данная страница, в основном, служит для просмотра сведений о системе и конфигурации коммутатора, включая время выполнения настроек, CPU, сети и системного журнала.

5.1. Настройка времени и даты

Чтобы настроить системное время и дату, нажмите на значок шестеренки в правом верхнем углу на главной веб-странице, выберете меню [SYSTEM] и войдите на страницу Clock Configuration («Настройка часов»), как показано ниже.

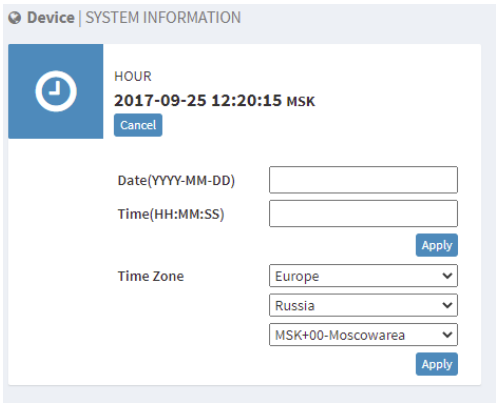


Рис. 20. Настройка часов

На этой странице можно просмотреть текущее время и настроить время вручную.

Дата (YYYY.MM.DD / ГГГГ.ММ.ДД)

Диапазон настроек: YYYY-ГГГГ (год) с диапазоном 1970~2099, MM-ММ (месяц) с диапазоном 1~12, DD-ДД (дата) с диапазоном 1~31.

Время (HH:MM: SS / ЧЧ:ММ:СС)

Диапазон настроек: HH-ЧЧ (часы) с диапазоном 0~23, MM-ММ (минуты) и SS-СС (секунды) с диапазоном 0~59.

Часовой пояс (Time Zone)

Настройка часового пояса. Выберете соответствующий континент, страну и населенный пункт.

5.2. Статус CPU

Статус CPU показывает текущий средний коэффициент использования центрального процессора.

Рис. 21. Статус загрузки ЦП

5.3. Статус сети

Отображает IP-адрес веб-интерфейса для входа в систему. Указывает, какой используется интерфейс.

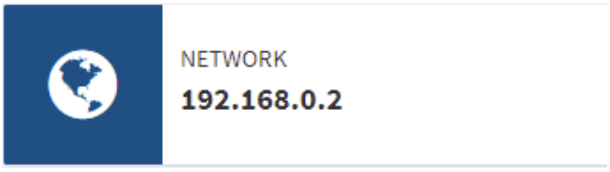


Рис. 22. Статус сети

5.4. Системный журнал

В системный журнал коммутатора записывается информация об изменении состояния, ошибки, процессы отладки, действия пользователя и другая информацию о системе коммутатора, которая полезна при выявлении неисправностей. Сведения из журнала могут выгружаться на сервер, поддерживающий протокол syslog, в режиме реального времени.
Информация в сообщениях журнала включает различные сведения об аварийных сигналах, широковещательном шторме, перезапуске, памяти и действиях пользователя.

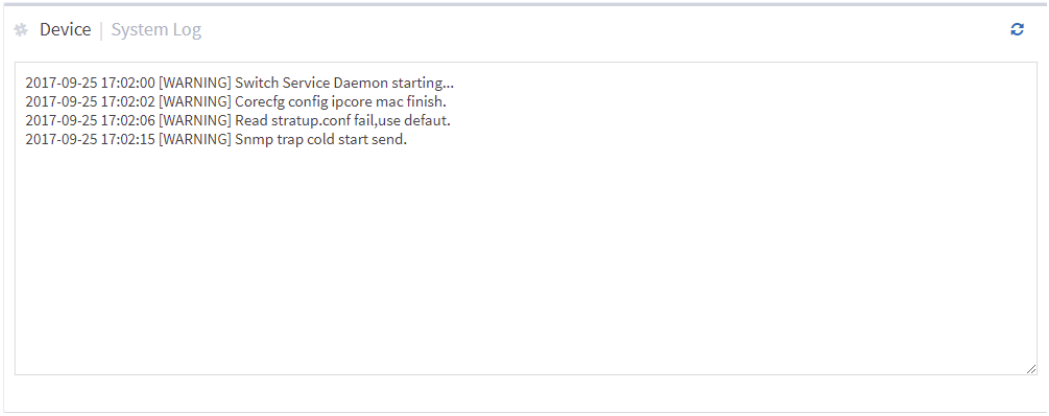


Рис. 23. Информация системного журнала

Нажмите на клавишу обновления в правом верхнем углу, чтобы вручную обновить информацию в журнале.

5.5. Загрузка файлов

Нажмите на значок шестеренки в правом верхнем углу на главной веб-странице, выберете [downloads] в меню [DEVICE] и войдите на страницу File download («Загрузка файлов»). Как показано на рис. ниже, можно загрузить файлы MIB и Startup-config. Файл startup-config – это файл запуска коммутатора, в котором сохранена конфигурация коммутатора.

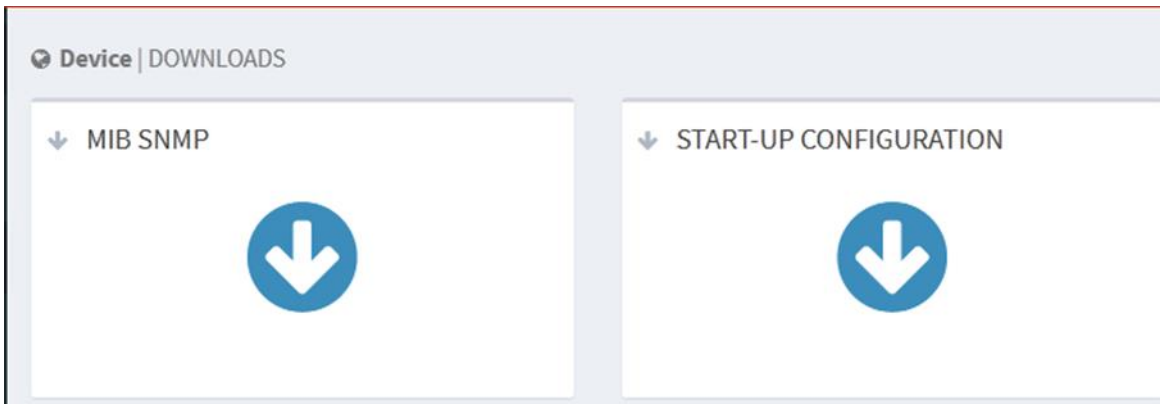


Рис. 24. Загрузка файлов

5.6. Загрузка файлов MIB

Нажмите на кнопку в MIB SNMP. На экране появится окно, указанное ниже. Нажмите OK, чтобы загрузить файл SWITCH-DESING-MIB.mib по указанному маршруту согласно рисунку ниже:

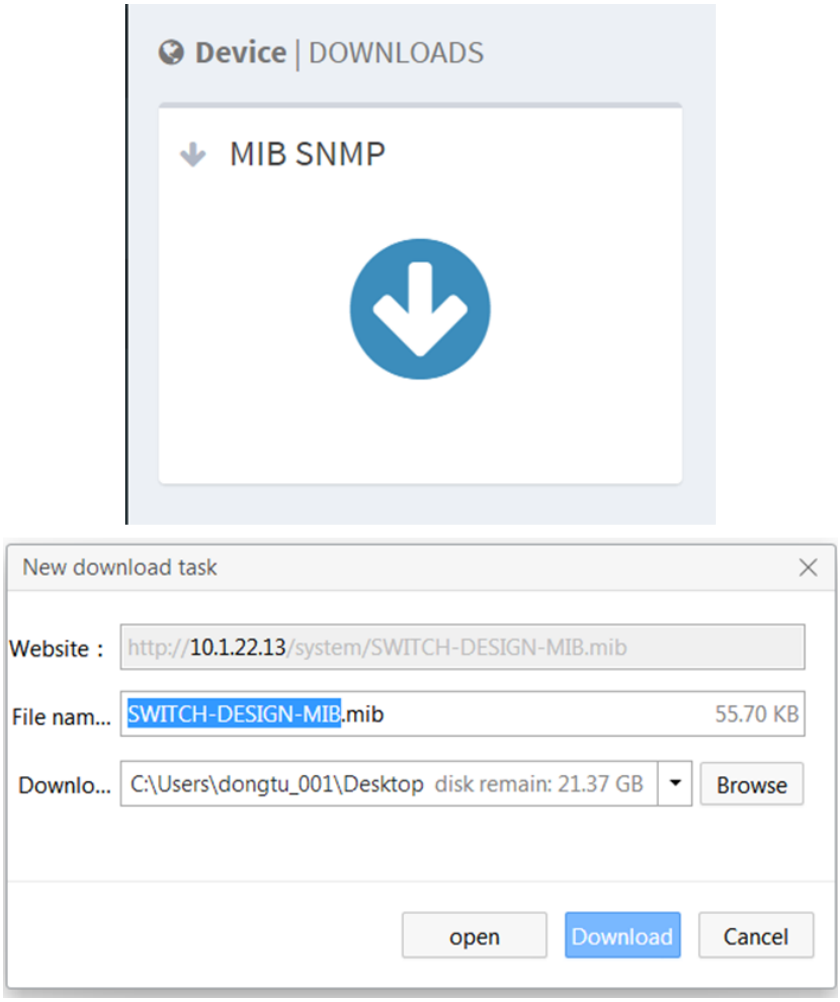
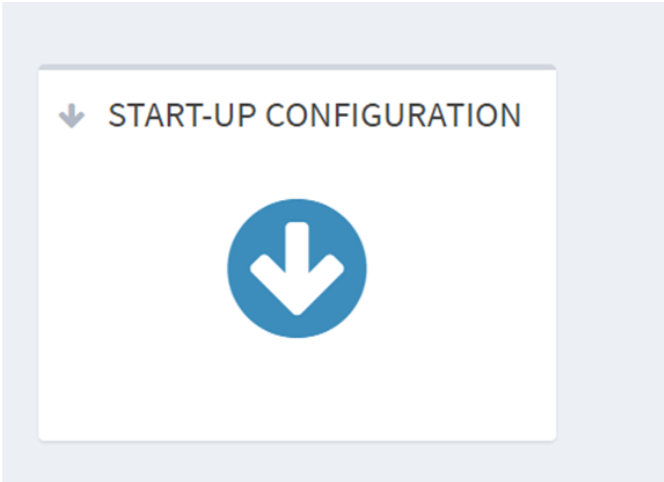


Рис. 25. Страница загрузки файлов MIB

5.7. Загрузка файлов конфигурации

Нажмите на кнопку в меню START-UP CONFIGURATION. На экране появится окно, указанное ниже. Нажмите OK, чтобы загрузить файл startup_config.conf по указанному маршруту согласно рис. ниже:



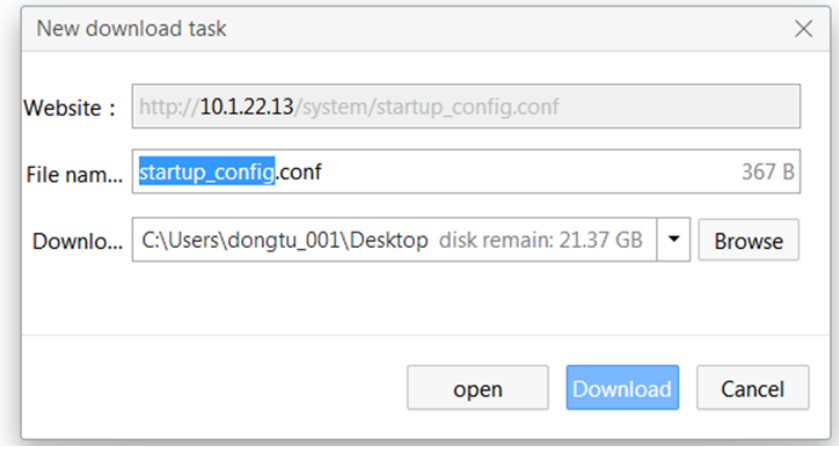


Рис. 26. Страница загрузки конфигурационного файла

6. Обновление прошивки (Firmware)

Обновление прошивки коммутатора предназначено для повышения его производительности. В данной модели поддерживается возможность как локального обновления, так и обновление посредством FTP/SFTP-сервера.

6.1. Локальное обновление

Нажмите на значок шестеренки в правом верхнем углу на главной веб-странице, выберете [Firmware] и войдите на страницу обновления устройства, как показано на рисунке ниже.

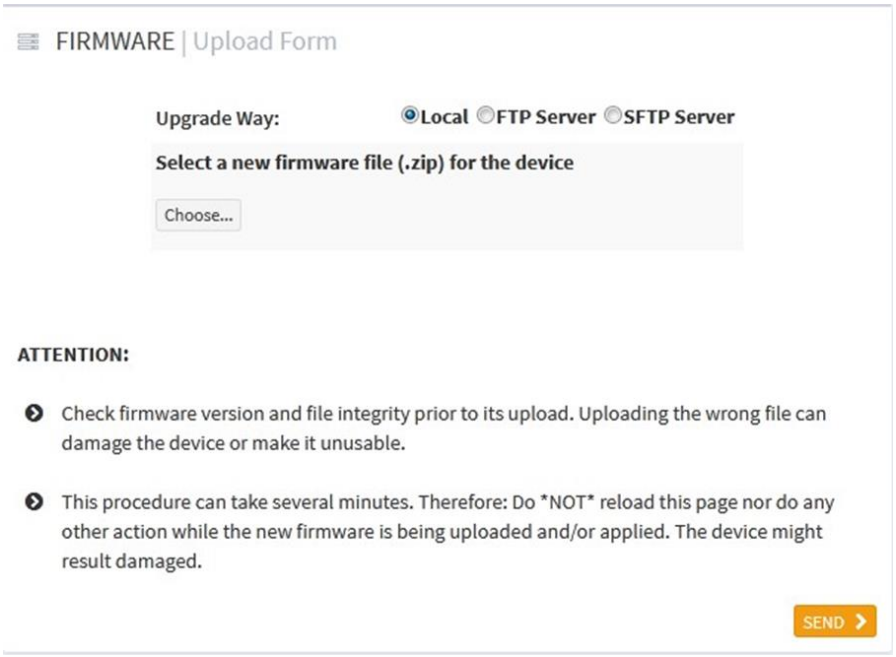


Рис. 27. Страница выбора варианта обновления прошивки

Варианты обновления ПО

Настраиваемые опции: Local/FTP server/SFTP server

Local (Локальное обновление)

Нажмите на кнопку <Choose>, чтобы выбрать соответствующий файл для обновления, затем нажмите на кнопку <SEND>, чтобы обновить прошивку.

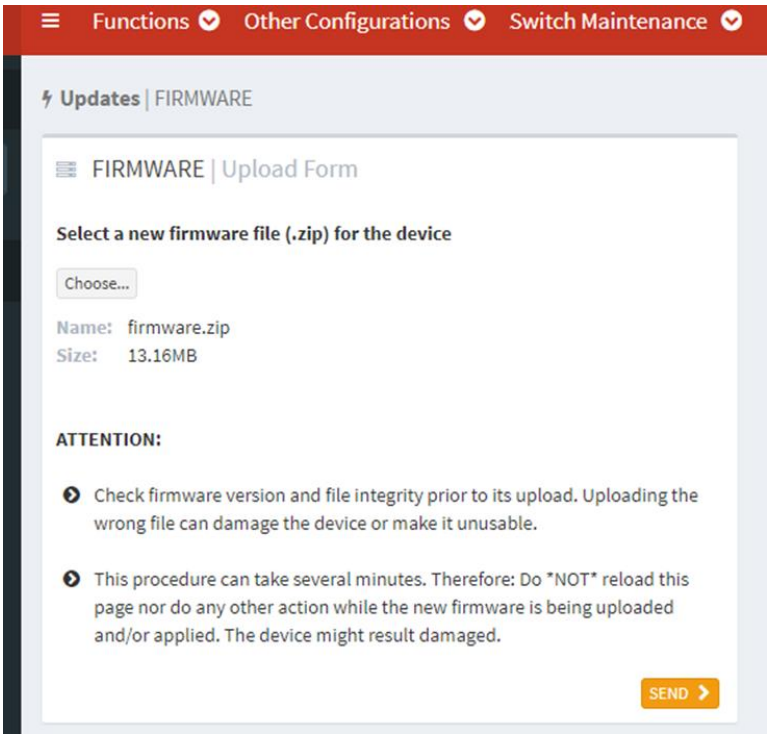


Рис. 28. Страница локального обновления прошивки

После выбора нажмите на кнопку <SEND>, чтобы начать обновление. Отобразится страница ожидания, как указано на рисунке ниже:

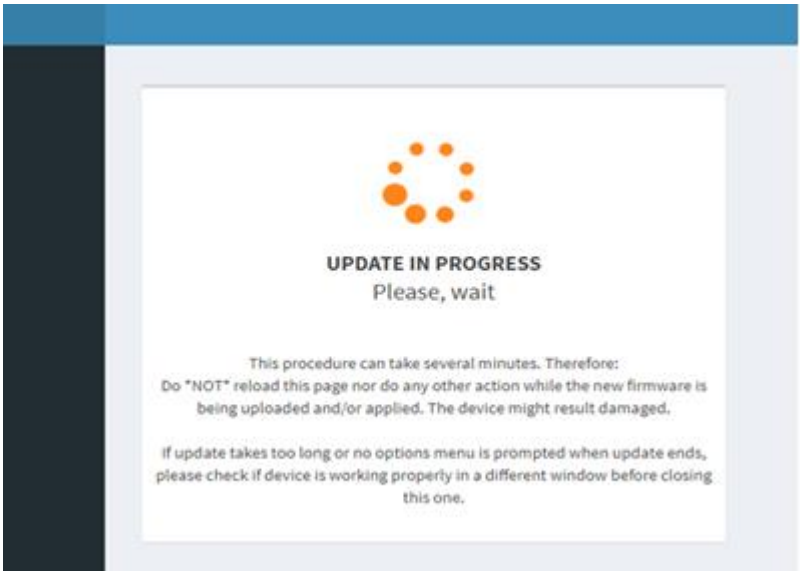


Рис. 29. Страница ожидания

Не выполняйте никаких других действий, в особенности не выключайте питание! Любые производимые действия могут вызвать сбой обновления и даже отмену его запуска.

Обновление не считается успешным до тех пор, пока на экране не отобразится следующая страница, как показано на рисунке ниже:

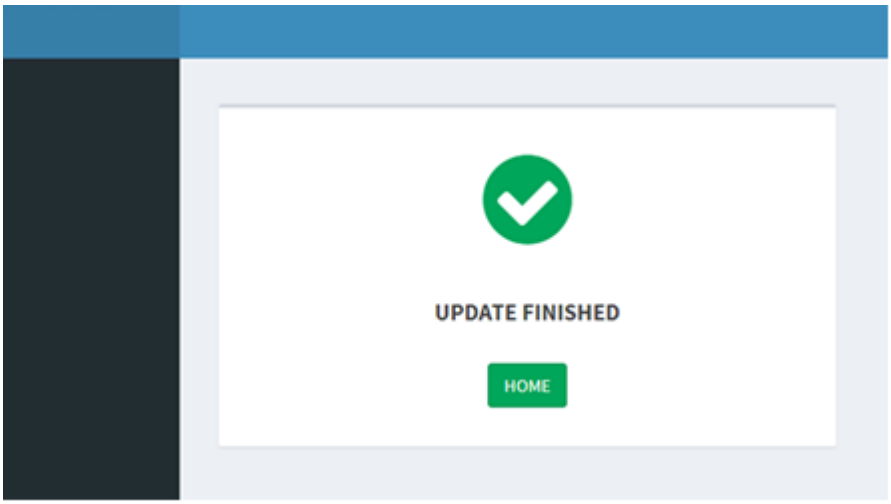


Рис. 30. Обновление прошивки завершено

Перезагрузите устройство. Нажмите на значок шестеренки в верхнем правом углу, выберете <Reboot>.

6.2. Обновление через FTP

Установите сервер FTP. В нашем примере мы покажем, как настроить сервер FTP и выполнить процедуру обновления ПО с помощью программы WFTPD.

1. Нажмите [Security]→[Users/Right], чтобы открыть раздел «Users/Right Security Dialog»; Нажмите кнопку <New User> для создания нового пользователя сервера FTP, как показано на рис. 31. Создайте имя пользователя и пароль, например, имя «admin» и пароль «123», затем нажмите <OK>.

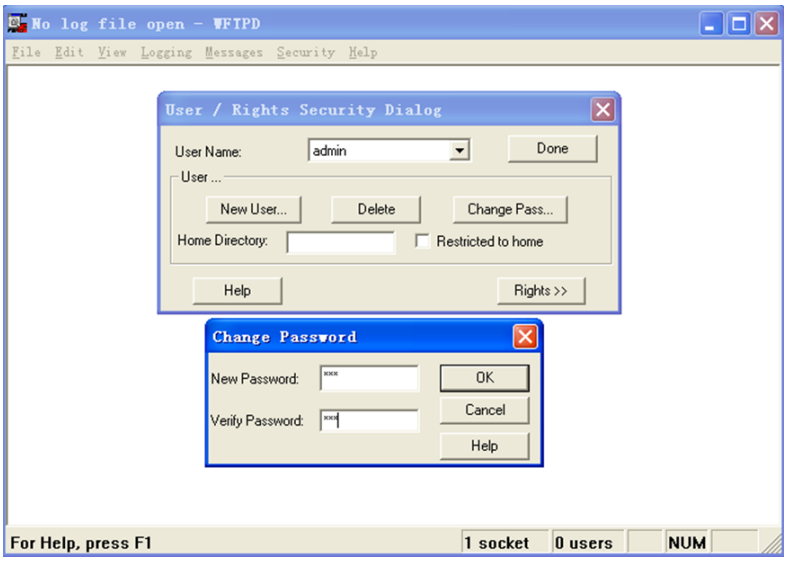


Рис. 31. Создание нового пользователя FTP

2. Укажите путь к месторасположению файла обновления в разделе «Home Directory», как показано на рис. 32 и нажмите <Done>.

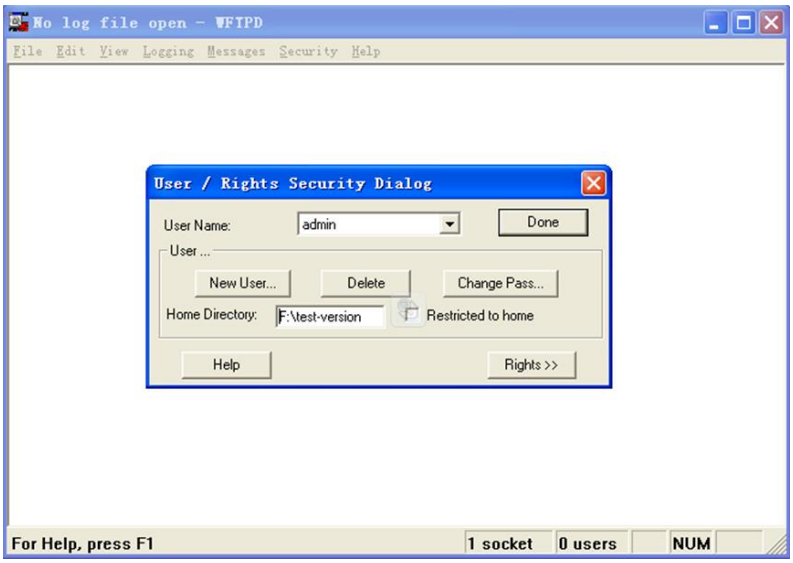


Рис. 32. Местоположение файла

3. Нажмите на значок шестеренки в правом верхнем углу, выберете [Firmware] и войдите на страницу обновления устройства. Затем выберете «FTP Server», как показано на рисунке ниже, введите IP-адрес FTP, имя пользователя, пароль и имя файла на сервере. Нажмите кнопку <SEND>.

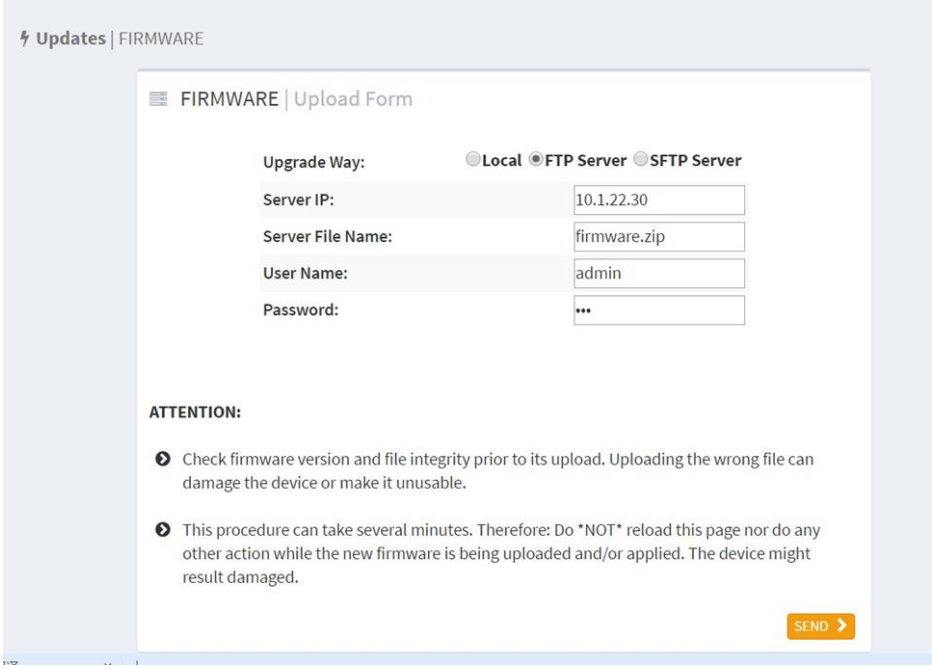


Рис. 33. Обновление ПО через FTP

Имя файла обновления по умолчанию - firmware.zip. Имя файла можно редактировать, но окончание имени должно обязательно быть «zip», иначе обновление будет невозможно.

4. Убедитесь в нормальном соединении сервера FTP и коммутатора:

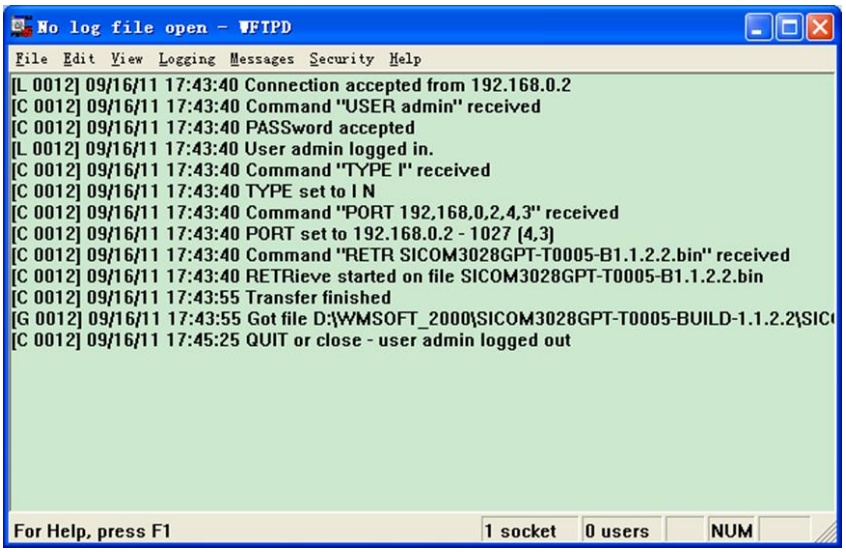


Рис. 34. Соединение коммутатора и сервера FTP

Чтобы отобразить информацию журнала обновлений, как показано на рис. 34, нужно нажать [Logging]->[Log Option] в WFTPD и выбрать режим «Enable Logging» и информация журнала будет отображена на экране.

5. На рисунке ниже показан процесс обновления:

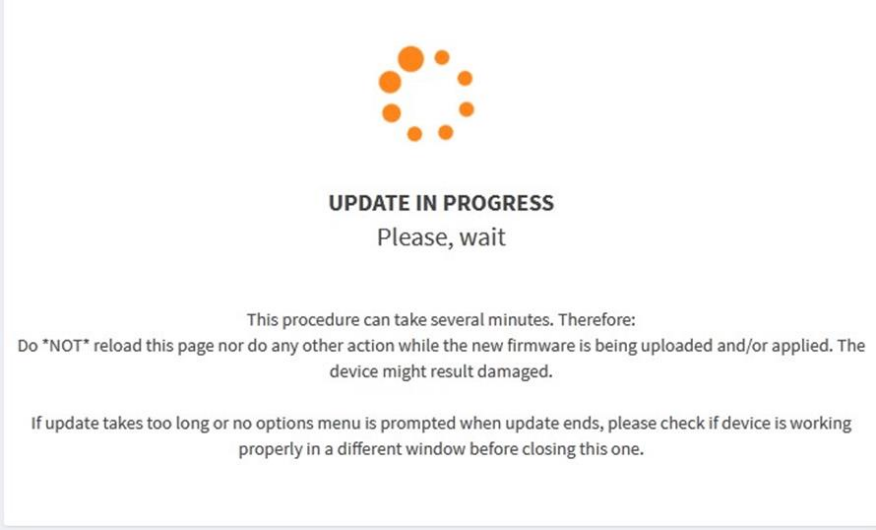


Рис. 35. Процесс обновления

6. На рисунке ниже показано завершение обновления:

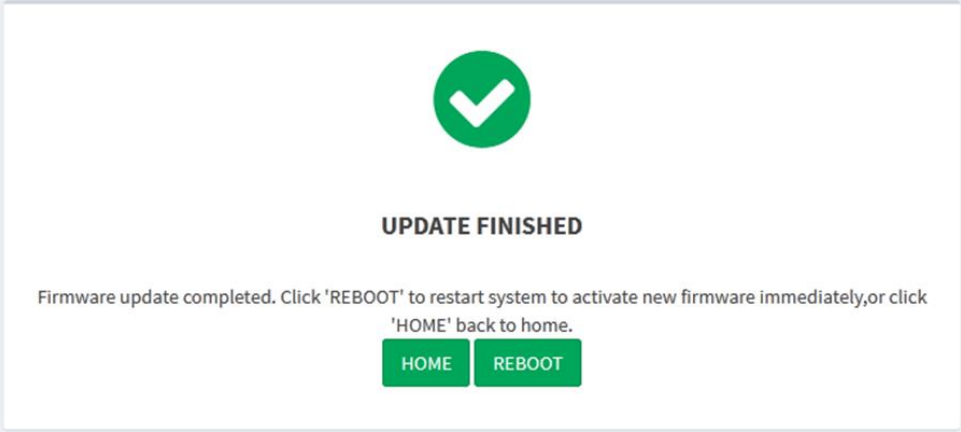


Рис. 36. Обновление через FTP завершено

После завершения обновления можно выбрать действия [HOME] и [REBOOT]. Новая версия активируется только после перезагрузки устройства.

- В процессе обновления ПО сервер FTP должен быть постоянно загружен.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию ПО.
- Если обновление завершено с ошибкой, не перезагружайте устройство, чтобы избежать потери файла с ПО. Есть вероятность того, коммутатор не сможет функционировать корректно.

6.3. Обновление через SFTP

Протокол прикладного уровня передачи файлов (SFTP) – это протокол передачи данных на основе алгоритма SSH. Он обеспечивает передачу зашифрованных файлов для обеспечения безопасности.
В следующем примере для описания конфигурации SFTP сервера и процесса обновления прошивки используется сетевой протокол MSFTPD.

1. Добавьте пользователя SFTP, как показано на Рисунке 37. Введите имя пользователя и пароль, например, «admin» и «123». Настройте номер порта 22. Введите путь к корневому каталогу для сохранения файла с версией прошивки.

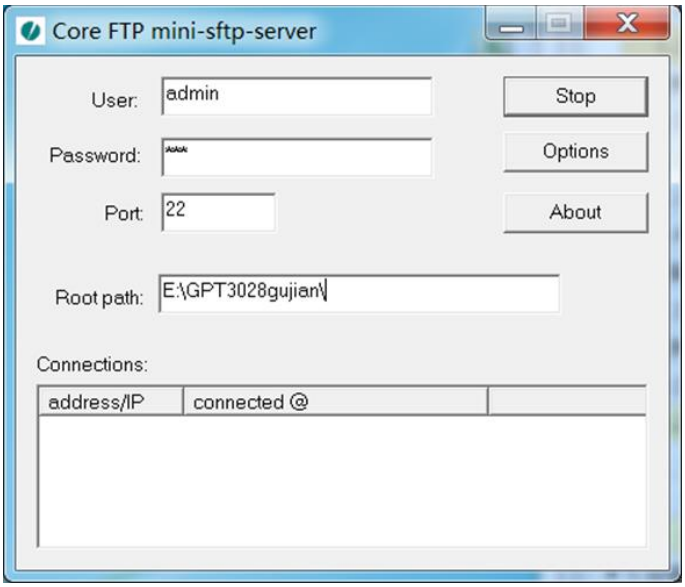


Рис. 37. Добавление пользователя SFTP

2. Нажмите на значок шестеренки в правом верхнем углу, выберете опцию [Firmware] и войдите на страницу обновления устройства, затем выберете SFTP сервер, как показано на рисунке ниже. Введите IP-адрес устройства SFTP, имя пользователя, пароль и имя файла на сервере. Нажмите кнопку <SEND>.

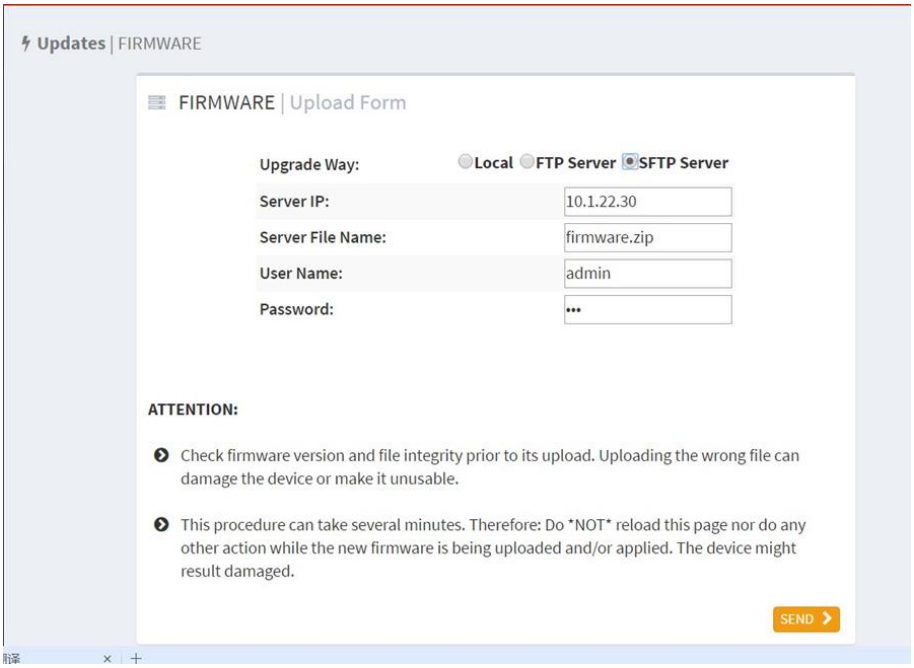


Рис. 38. Обновление ПО через SFTP

Имя файла обновления по умолчанию - firmware.zip. Имя файла можно редактировать, но окончание имени должно обязательно быть «zip», иначе обновление будет невозможно.

3. На рисунке ниже показан процесс обновления:

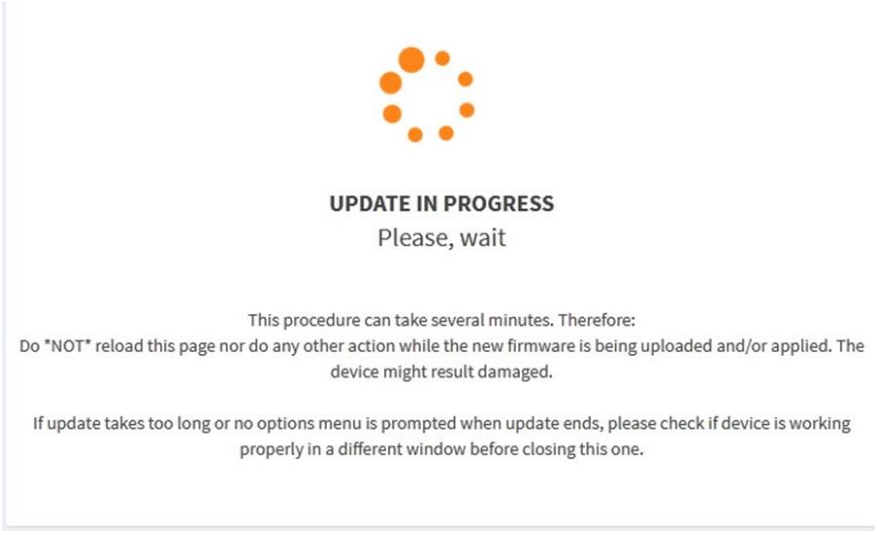


Рис. 39. Процесс обновления

4. На рисунке ниже показано завершение обновления:

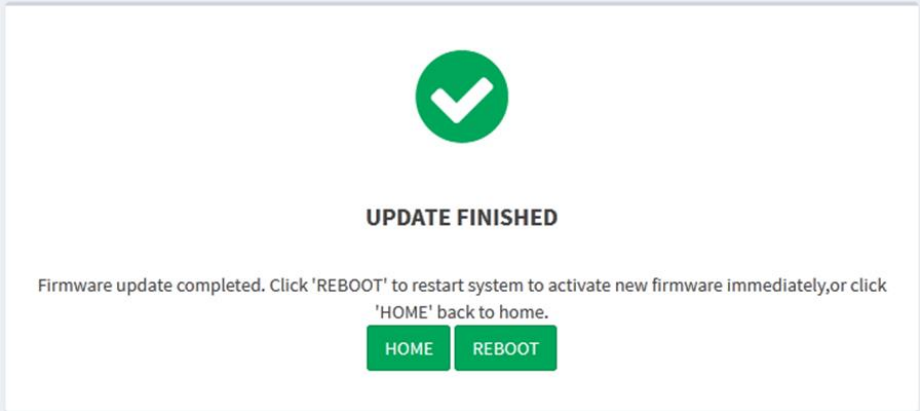


Рис. 40. Обновление через SFTP завершено

После завершения обновления можно выбрать действия [HOME] и [REBOOT]. Новая версия активируется только после перезагрузки устройства.

- В процессе обновления ПО сервер FTP должен быть постоянно загружен.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию ПО.
- Если обновление завершено с ошибкой, не перезагружайте устройство, чтобы избежать потери файла с ПО. Есть вероятность того, коммутатор не сможет функционировать корректно.

6.4. Загрузка файлов

Нажмите на значок шестеренки в правом верхнем углу на главной веб-странице, выберете [Configuration] в меню [Updates], чтобы загрузить файл конфигурации из локального сервера в коммутатор как файл запуска коммутатора.

Рис. 41. Загрузка конфигурационного файла

Загруженный конфигурационный файл хранится в каталоге коммутатора под именем /etc/switch_service, а устройство запускается из файла startup.conf, который служит файлом запуска со всей информацией о конфигурации коммутатора.

Загруженный конфигурационный файл должен быть текстовым файлом с суффиксом .conf.

6.5. Перезагрузка

Когда устройству требуется перезагрузка, нажмите на значок шестеренки в правом верхнем углу на главной веб-странице, выберете Reboot «перезагрузить». Устройство перезапустится как показано на рисунке ниже.

Рис. 42. Перезагрузка коммутатора

7. Функции коммутатора

7.1. Резервирование

7.1.1. Основные принципы

Описание терминов:

- SAN (Single Attached Node) – узел, который подключается только к одной сети (LAN A или LAN B) и посылает/принимает обычные фреймы;
- RedBox – устройство резервирования. Это коммутатор используется, когда необходимо резервировано подключить устройство, имеющее один Ethernet-интерфейс, и без поддержки протокола PRP. На RedBox'е кадр от устройства дублируется и передается в сеть PRP или HSR, так словно данные передаются от DAN. Более того, устройство, которое находится за RedBox'ом, видится для остальных устройств как DAN.
- DAN (Dual Attached Node) – узел, который подключается к обеим сетям и посылает/принимает дублированные фреймы.
- DANH (Double Attached Node сети HSR) – узел, который может обмениваться данными внутри HSR-кольца (может посылать/принимать дублированные фреймы).
- DANP (Double Attached Node сети PRP) – узел, который подключается к двум независимым сетям (может посылать/принимать дублированные фреймы).

1. Протокол PRP

Основной задачей протокола PRP является обеспечение резервирования в системе через узлы сети, поддерживающие PRP. Его основной принцип работы продемонстрирован на рисунке ниже.

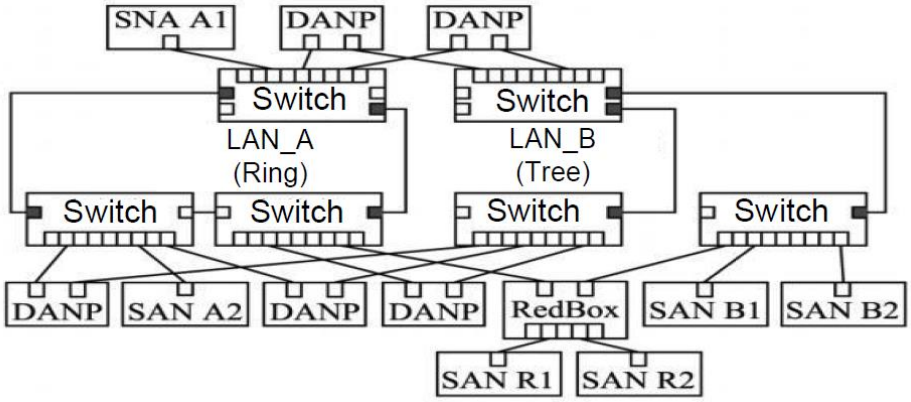


Рис. 43. Схема принципа работы протокола PRP

На рис. 43 отображена схема принципа работы протокола PRP. На ней можно увидеть, что каждый узел DANP одновременно подключен к двум отдельным параллельно работающим сетям LAN A и B. Сообщения сохраняются в 2 копии, отдельно отправляются через два полнодуплексных порта, а затем перенаправляются на DANP назначения по сетям LAN A и B соответственно. При этом для улучшения резервирования системы каждая независимая сеть LAN имеет разные структуры связи (например, сеть LAN B обладает структурой типа дерева и/или шинной структурой, сеть LAN A - кольцевой структурой типа RSTP и т.д.). Что касается узла SAN, не поддерживающего протокол PRP, допускается подключать его напрямую к LAN (например, узел SAN A2 на рисунке 43), либо его необходимо подключить к специальному коммутатору (модулю) RedBox (например, SAN R1 и SAN R2), который обеспечит подключение такого узла SAN к сетям LAN A и B. Принцип работы портов PRP показан на рисунке 44. Два параллельно работающих порта (порт A и порт B) одновременно подключены к уровню LRE (link redundancy entity / точка резервирования связи). Когда этот объект принимает сетевые кадры от протокола дейтаграмм верхнего уровня (UDP) или протокола управления передачей (TCP), кадры сохраняются в 2 копии и отправляются одновременно через 2 порта (Tx). Принимающий уровень LRE отсылает первый пришедший кадр от портов (Rx) в модули UDP или TCP. Кадр, пришедший вторым, отбрасывается. Очевидно, что данный механизм является прозрачным для протокола и выполняет параллельное резервирование физического уровня над канальным уровнем. Таким образом, протокол PRP совместим с другими протоколами верхнего уровня, как, например, RSTP и VLAN. Кроме того, объект с резервированием каналов регулярно отсылает сообщение мониторинга сети, которое используется для обнаружения разрывов в сети и других возможных сбоев.

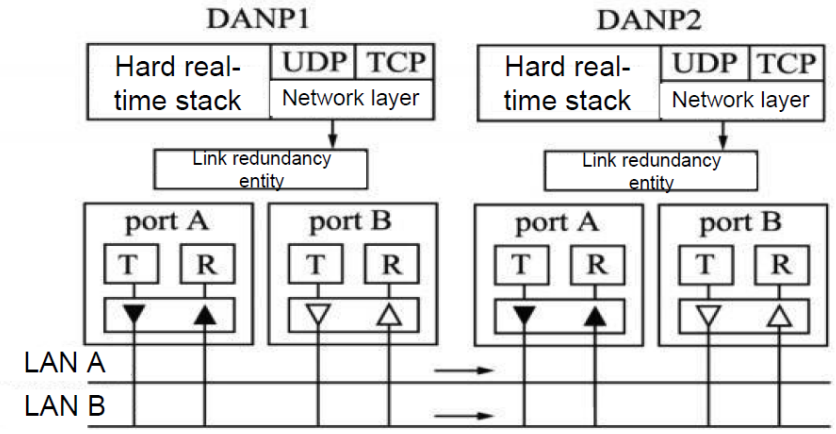


Рис. 44. Схема принципа работы портов PRP

2. Протокол HSR

Основная задача протокола HSR такая же, как у протокола PRP. Он также обеспечивает резервирование в системе через два независимых физических порта, но при этом сеть имеет кольцевую структуру. Ее принцип работы изображен на рисунке ниже.

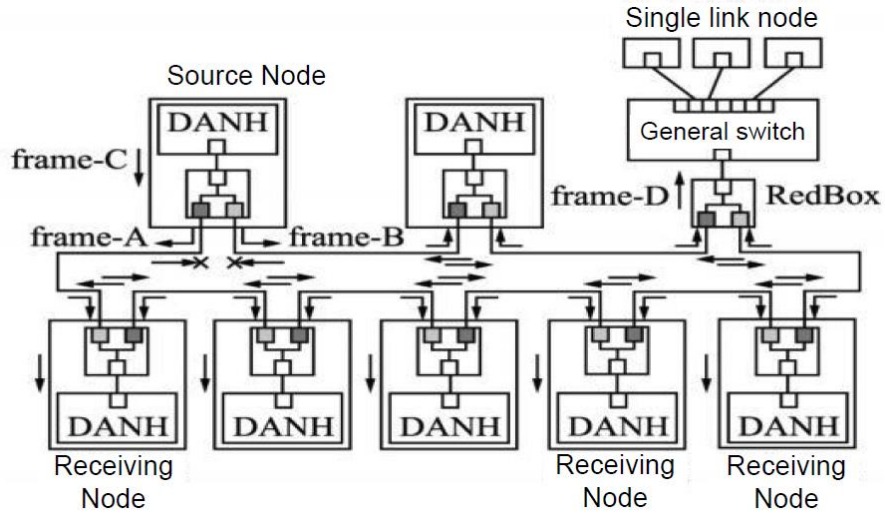


Рис. 45. Схема принципа работы протокола HSR

DANH: устройства с двумя независимыми интерфейсами, могут напрямую подключаться в кольцо HSR. «Frame A», «Frame B» и «Frame C» – это номера кадров.

Предположим, что исходный узел DANH получает один кадр от протокола верхнего уровня как кадр «Frame C», сораняет его в 2 копии, добавляет тег «Frame A» и «Frame B» и отправляет их отдельно в два разных порта. Узел DANH в кольце принимает «Frame A», проверяет, является ли он широковещательным кадром. Если это так, то принимает и пересылает его. В противном случае выполняет проверку, является ли MAC-адрес назначения адресом этого узла. Если нет, то «Frame A» перенаправляется с другого порта на следующий узел. Если да, то выполняется проверка, получен ли «Frame B», пришедший на второй порт первым. Если «Frame B» поступил первым, то «Frame A» отбрасывается. В противном случае «Frame A» отправляется на обработку протоколом верхнего уровня.

Когда «Frame A» возвращается на порт исходного узла, узел определяет, что это кадр, отправленный им самим, и отбрасывает его, таким образом избегая «шторма» в кольце. Принцип передачи «Frame B» в точности совпадает с принципом передачи «Frame A». Таким образом, каждый кадр протокола верхнего уровня сохраняется в 2 копии и передается в разных направлениях в кольце. Если происходит обрыв в какой-то точке, это влияет на передачу только в одном направлении. Соответственно, сети не требуется время на восстановление. Данный механизм также полностью прозрачен для протоколов верхнего уровня. Протокол HSR также направляет сообщение мониторинга сети. Если порт не получает сообщение мониторинга длительное время, значит в сети присутствует обрыв.
Для устройств, не поддерживающих протокол HSR, доступ к сети HSR может быть осуществлен через RedBox также как и для протокола PRP.

7.1.2. Настройка через WEB-интерфейс

Откройте дерево навигации [Functions]→[Redundancy] и войдите на страницу настроек резервирования сети, как показано на рисунке ниже.

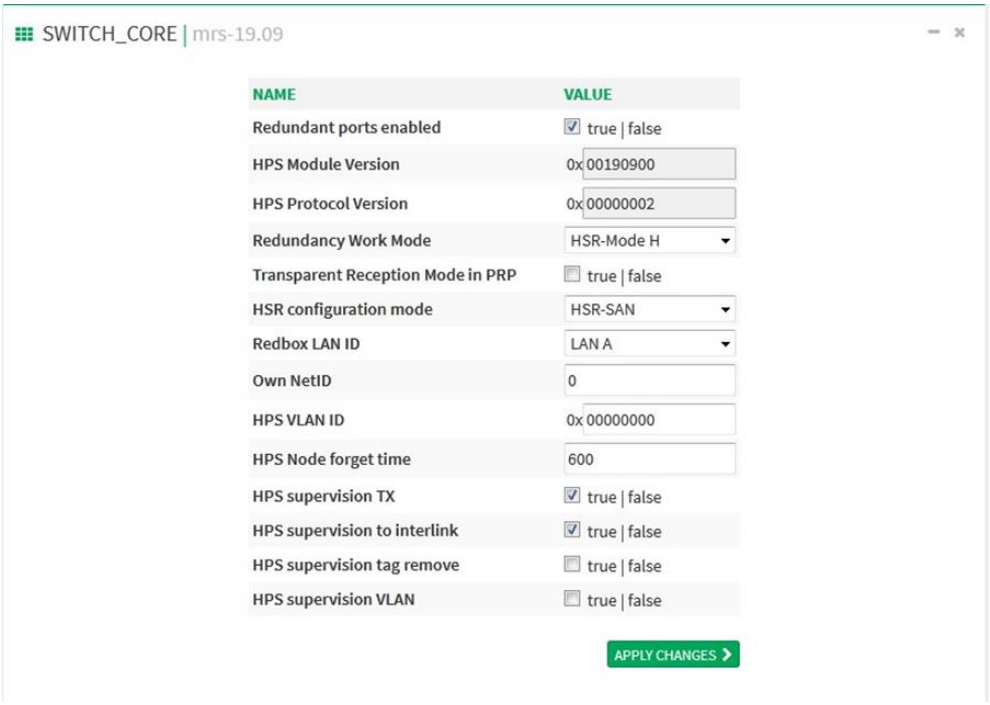


Рис. 46. Страница настроек резервирования

Активизация портов резервирования (Redundant ports enabled)
Опции: true/false (истина/ложь)
Настройки по умолчанию: true (истина)
Функция: Когда активный порт выполняет функцию порта резервирования, он не является общим портом Ethernet.
Версия модуля HPS (HPS Module Version)
Функция: отображение текущей версии модуля HPS.
Версия протокола HPS (HPS Protocol Version)
Функция: отображение текущей версии протокола резервирования HSR/PRP.

Режим работы резервирования (Redundancy Work Mode)

Опции: Режим «PRP-Duplicate discard» / Режим «PRP-Duplicate accept» / HSR-Mode H / HSR-Mode N / HSR-Mode T / HSR-Mode U / HSR-Mode X.

Настройки по умолчанию: HSR-Mode H

Функция:

Режим «PRP-Duplicate discard»: в этом режиме приемник может обнаруживать резервные копии элементов, передатчик LRE присоединяет шестибайтовое поле после двух кадров, в котором содержится порядковый номер, являющийся трейлером контроля резервирования (Redundancy control trailer, RCT). Уровень LRE использует порядковый номер RCT и исходный MAC-адрес, чтобы обнаружить дублированные элементы. Он пересылает на верхний уровень только первый кадр в паре. Все устройства в сети PRP должны быть установлены в режим prp-duplicate-discar, как показано на рисунке 48.

Режим PRP-Duplicate accept: данный режим используется для тестирования с целью подтверждения того, что резервные элементы отбрасываются именно на канальном уровне, а не протоколом верхнего уровня. В этом режиме передатчик настроен так, чтобы отправлять два кадра без трейлера RCT. Приемник настроен так, чтобы принимать два кадра и пересылать их (если оба доставлены) на свой верхний уровень.

HSR-Mode H: данный режим является обязательной опцией и режимом по умолчанию. Как правило, он относится к пересылке кадров данных с тегом HSR. В этом режиме, за исключением кадров, передаваемых самим узлом, DANH будет добавлять тег HSR и пересылать трафик по кольцевой сети. Резервный кадр и кадр, в котором узел является адресатом одноадресной передачи, пересылаться не будут. Все устройства в сети HSR должны быть установлены в режим HSR- Mode H, как показано на рисунке 49;

HSR-Mode N: этот режим не является обязательным и не предполагает пересылку. В данном режиме поведение узла аналогично режиму Mode H. Разница в том, что узел не должен пересылать трафик по кольцевой сети между портами.

HSR-Mode T: Этот режим не является обязательным; он прозрачен для пересылки. В этом режиме DANH должен сначала удалить тег HSR, а затем перенаправить кадр на другой порт и отправить кадр с хоста на оба порта без тега и без отбрасывания дублированных элементов.

HSR-Mode U: Этот режим не является обязательным; он предполагает одноадресную пересылку. В этом режиме поведение узла аналогично режиму Mode H. Отличие состоит в том, что узел должен перенаправлять одноадресный трафик в пункт назначения, как при многоадресной передаче.

Режим прозрачного приема в PRP (Transparent Reception Mode in PRP)

Опции: true/false (истина/ложь)

Настройки по умолчанию: false (ложь)

Функция: После включения режима дублированный кадр не отбрасывается, а трейлер RTC не стирается.

Режим конфигурации HSR (HSR Configuration Mode)

Опции: HSR-SAN / HSR-HSR / HSR-PRP

Настройки по умолчанию: HSR-SAN

Функция: данный режим определяет для протокола HSR вариант настройки Redbox работу в режимах HSR-SAN, HSR-PRP или HSR-HSR.

Идентификатор сети для Redbox (Redbox LAN ID)

Опции: LAN A / LAN B

Настройки по умолчанию: LAN A

Функция: определяет идентификаторы сети "A" или "B" для Redbox, которые используются в режимах HSR-PRP.

Идентификатор собственной сети (Own NetID)

Диапазон настроек: 3 бита [0-7]

Настройки по умолчанию: 0

Функция: идентификационный номер сетевого кольца, объединенного посредством узлом.

Идентификатор HPS VLAN (HPS VLAN ID)

Диапазон настроек: 12 битов [00-FFF]

Настройки по умолчанию：00000000

Функция: используется для определения идентификатора VLAN узлов Redbox.

Время забывания узла HPS (HPS Node Forget Time)

Диапазон настроек: 10 битов [0-1023], единица измерения – сек.

Настройки по умолчанию: 600 сек.

Функция: время забывания узла Redbox. По умолчанию настроено на 600 сек.

Контроль HPS TX (HPS Supervision TX)

Опции: true/false (истина/ложь)

Настройки по умолчанию: true (истина)

Функция: включить или выключить передачу управляющих кадров.

Контроль interlink-канала HPS (HPS supervision to interlink)

Опции: true/false (истина/ложь)

Настройки по умолчанию: true (истина)

Функция: передача управляющего кадра через порт interlink.

Удалить тег контроля HPS (HPS supervision tag remove)

Опции: true/false (истина/ложь)

Настройки по умолчанию: false (ложь)

Функция: удаление заголовка HSR или трейлера PRP управляющего кадра при передаче через порт interlink.

Контроль VLAN HPS (HPS supervision VLAN)

Опции: true/false (истина/ложь)

Настройки по умолчанию: false (ложь)

Функции: Обработка управляющего кадра в сети VLAN.

7.1.3. Пример типовой настройки

Для примера возьмем три типовых конфигурации: сеть PRP, сеть HSR и сеть QUADBOX.

1. Типовая сеть PRP

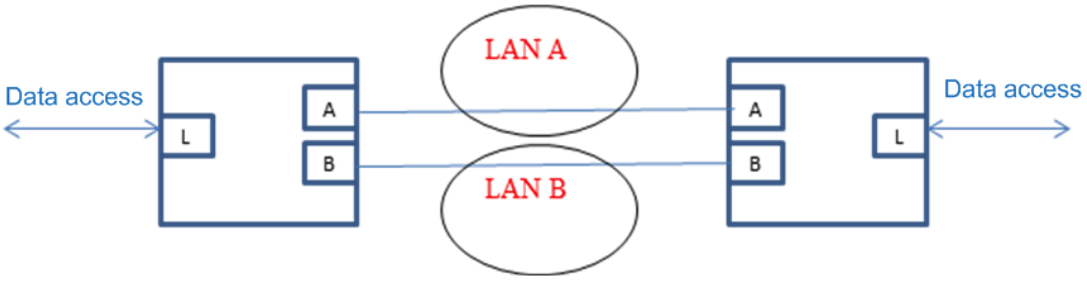


Рис. 47. Типовая схема сети PRP

Все устройства в сети PRP должны быть установлены в режим prp-duplicate-discard. Эта рекомендация обеспечить подключение порта «A» к порту «A» и порта «B» к порту «B» на другой стороне. Передача данных «A»—«A» будет проходить через LAN A, а передача данных «B»—«B» будет проходить, соответственно, через LAN B. Однако учтите, что процесс передачи должен протекать независимо между LAN A и LAN B.
При использовании PRP данные между портом A и B не будут добавляться в другие заголовки, поэтому все устройства между LAN A и LAN B могут управляться устройством серии SEWM-RB-3GC (в отличие от сети HSR). См. веб-конфигурацию ниже.

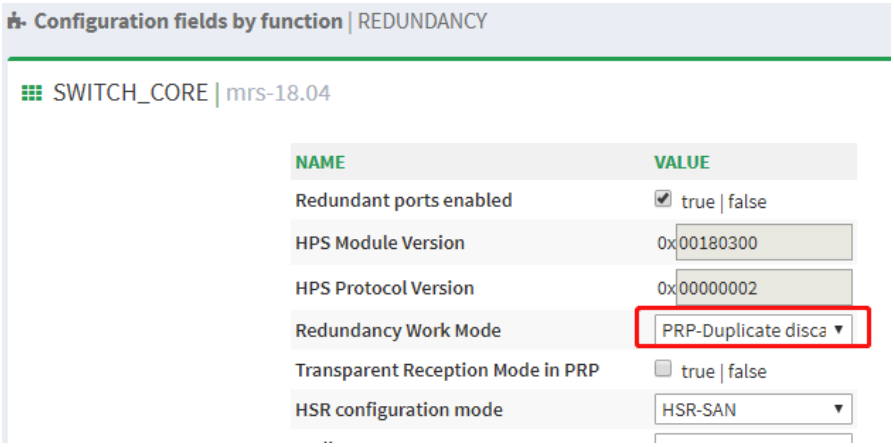


Рис. 48. Настройка PRP

2. Типовая сеть HSR

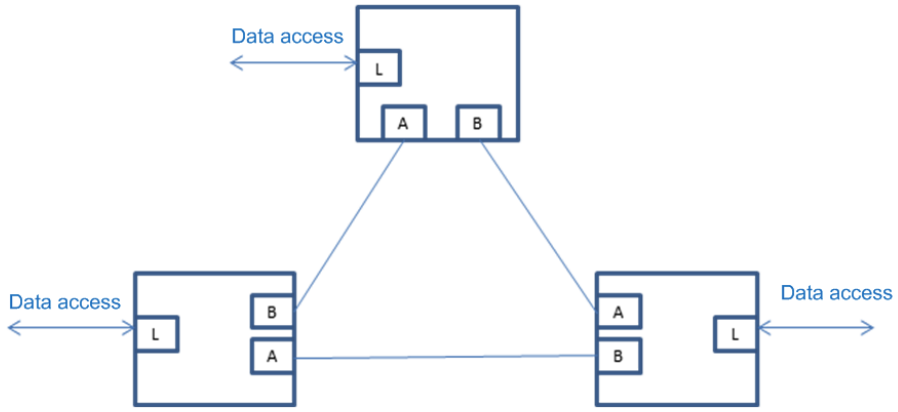


Рис. 49. Типовая схема сети HSR

Все устройства в сети HSR должны быть установлены в режим HSR-H. Рекомендуется подключение порта «A» к порту «B» и порта «B» к порту «A» на противоположной стороне кольца.

Примечание: точки соединения между устройствами могут поддерживать прозрачную передачу данных с использованием других устройств, однако учтите, что поскольку во все данные между устройствами HSR добавляются заголовки HSR, ими нельзя управлять удаленно, если между устройствами добавлены устройства прозрачной передачи. См. веб-конфигурацию ниже.

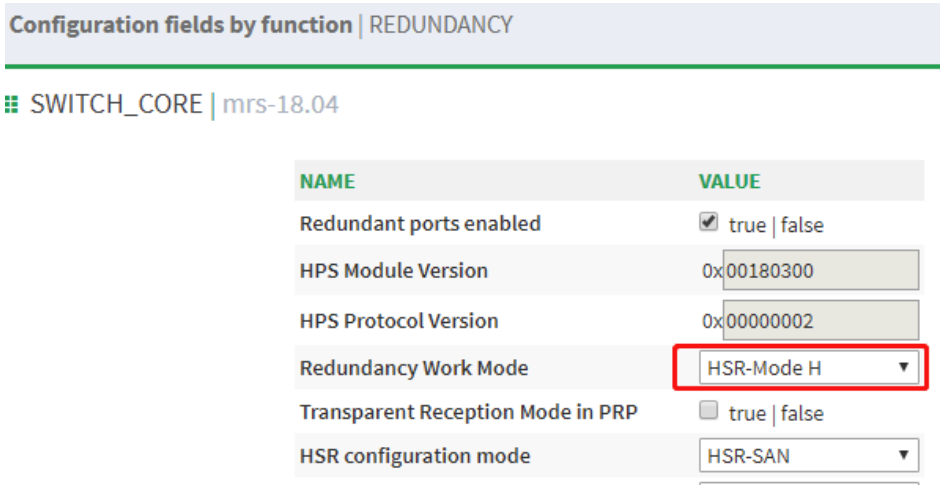


Рис. 50. Настройка HSR

3. Типовая сеть QUADBOX

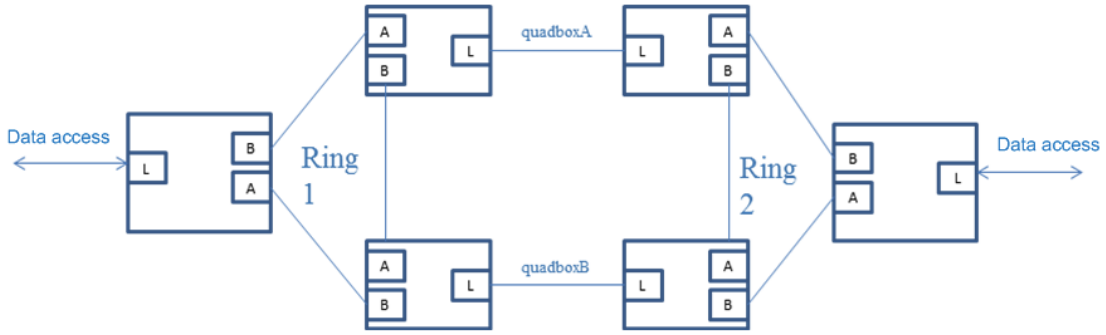


Рис. 51. Типовая схема сети QUADBOX

Преимущество сети Quadbox заключается в том, что два кольца HSR резервируют друг друга, то есть степень защиты 1:1 может быть повышена до степени 4:1. Когда соединение quadboxA и quadboxB будет установлено, необходимо запустить протокол HSR, вследствие чего 3 порта 4-х устройств, образующих quadboxA и quadboxB, становятся резервными портами HSR.
Все устройства в сети QUADBOX должны быть установлены в режим HSR-H (режим по умолчанию), а порт interlink, который используется для соединения quadboxA и quadboxB, должен быть настроен для работы в режиме HSR-HSR. См. веб-конфигурацию ниже;

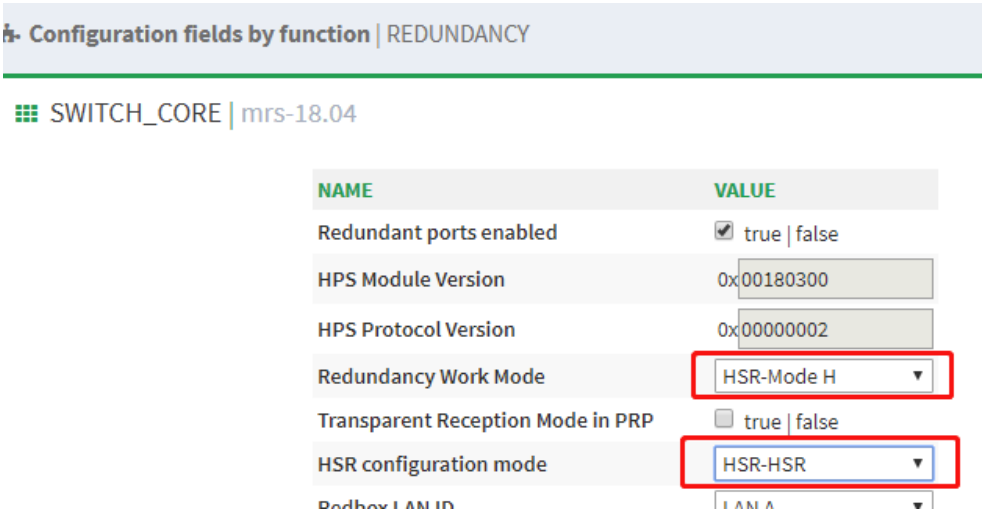


Рис. 52. Настройка QUADBOX

7.2. Протокол PTP

7.2.1. Введение

PTP (Precision Time Protocol, протокол точного времени) обеспечивает синхронизацию часов, работающих независимо на отдельных узлах, и гарантирует соблюдение высокой точности измерений. Данный протокол синхронизации включает оба вида

синхронизации: синхронизацию фаз и синхронизацию частот, а точность синхронизации может достигать ±100 нс.

7.2.2. Концепция

1. Домен PTP

Сеть, использующая протокол PTP, является доменом PTP. Домен PTP имеет только одни мастер часы, а остальные устройства в домене синхронизируются с этими часами.

2. Порт PTP

Порт, через который реализуется протокол PTP, является портом PTP.

3. Синхронизирующий узел

Узел в домене PTP – это узел синхронизации времени. В протоколе PTP определяются следующие основные узлы синхронизации:

- OC (Ordinary Clock – Обычные часы)

Устройство с одним портом, которое может быть Master (ведущими часами) или Slave (ведомыми часами). Имеет только один порт PTP в домене PTP, который участвует в синхронизации времени. Синхронизирует время от предыдущего (upstream) узла синхронизации или сообщает время следующему (downstream) узлу синхронизации через этот порт.

- BC (Boundary Clock – Граничные часы)

Эти часы имеют один и более портов PTP в домене PTP, которые участвуют в синхронизации часов.

Если в процессе синхронизации участвует только один порт PTP, время синхронизируется по предыдущему узлу синхронизации или время передается следующему узлу синхронизации через этот порт. Если в процессе синхронизации участвует несколько портов PTP, время синхронизируется по предыдущему узлу через один из портов и сообщается следующему узлу синхронизации через оставшиеся порты. В том случае, если граничные часы используются в качестве источника времени, время может передаваться следующим узлам синхронизации через несколько портов PTP.

- TC (Transparent Clock – Прозрачные часы)

Этому узлу синхронизации не требуется выполнять синхронизацию времени с другими узлами. У прозрачных часов TC есть несколько портов PTP. Эти порты обеспечивают только переадресацию сообщений протокола PTP и направляют коррекцию задержки без синхронизации часов через любой порт, т.е. измеряют время прохождения сообщения синхронизации через себя и предоставляют измеренное значение узлам, получающим сообщение синхронизации далее.

Существует два типа прозрачных часов:

E2ETC (End-to-End Transparent Clock): Прямая пересылка сообщений протокола по сети, не относящихся к типу P2P, и расчет общего времени задержки. В режиме E2E время доставки вычисляется по сообщениям, прошедшим через множество устройств, каждый из которых проставляет в поле коррекции время, на которое пакет задержался на этом устройстве.

P2PTC (Peer-to-Peer Transparent Clock): Прямая пересылка сообщений Sync (сообщения от ведущих часов, которые передают информацию о времени), сообщений Follow_Up

(содержат метку времени отправки сообщения sync и корректирующее значение) и сообщений Announce (сообщения, содержащие параметры для определения основного мастера системы по алгоритму BMC – Best Master Clock), прерывание других сообщений протокола и расчет времени задержки сообщения в каждом узле.

4. Для пары узлов синхронизации существует следующий тип отношений «ведущий-ведомый» (Master-Slave):

- Узел, передающий синхронизацию времени, это ведущий (Master) узел. А узел, принимающий синхронизацию времени, это ведомый (Slave) узел.
- Часы ведущего узла – это задающие часы (Master Clock), а часы ведомого узла – это управляемые часы (Slave Clock).
- Порт, через который синхронизация времени - это ведущий порт (Master Port). Порт, который принимает синхронизацию времени - это ведомый порт (Slave Port).

7.2.3. Принцип синхронизации

1. Выбор оптимальных часов

Посредством интерактивного взаимодействия с источником времени, идентификатора (ID) часов и других данных в сообщении Announce, каждый узел синхронизации выбирает один узел синхронизации в качестве оптимальных часов в домене PTP. В это время также определяются отношения «ведущий–ведомый» между каждым узлом и ведущим и ведомым портами на каждом узле. С помощью этого процесса в домене PTP устанавливается связующее дерево на основе оптимальных часов в качестве корня. С этих пор ведущие часы будут регулярно отправлять сообщения Announce ведомым часам. Если ведомые часы не получают сообщение Announce, отправленное ведущими часами какой-то период времени, ведущие часы будут считаться недействительными и выбор оптимальных часов будет возобновлен.

Сообщение Announce содержит достаточно информации для обеспечения выбора оптимальных часов, включая такие важные сведения, как, например, приоритет ведущих часов 1, тактовый уровень точность часов, приоритет ведущих часов 2, идентификатор часов. Данная информация сравнивается при выборе оптимальных часов. В качестве оптимальных часов обычно выбираются часы с приоритетом 1.

2. Принцип синхронизации

Сообщение передается и синхронизируется между ведущими часами и ведомыми часами. Время отправки и получения сообщения записывается. Общая задержка между ведущими и ведомыми часами рассчитывается путем вычисления разницы во времени передачи сообщения туда и обратно. Если сеть симметрична, односторонняя задержка составляет половину общей двусторонней задержки. Ведомые часы могут синхронизироваться с ведущими часами, регулируя местное время в соответствии с отклонением часов ведущий-ведомый и односторонней задержкой.

Протокол PTP предусматривает два механизма измерения задержки

Механизмы request_response (запрос_ответ): измерение задержки времени от мастера до каждого конечного устройства во всем канале связи;

Механизмы измерения задержки peer-to-peer dalay: измерение задержки от точки до точки. В сравнении с механизмом request_response, механизм измерения задержки peer-to-peer delay измеряет задержку каждого соединения всего канала связи.

7.2.4. Настройка через WEB-интерфейс

Откройте дерево навигации [Functions]→[PTP] и войдите на страницу конфигурации PTP, как показано ниже.

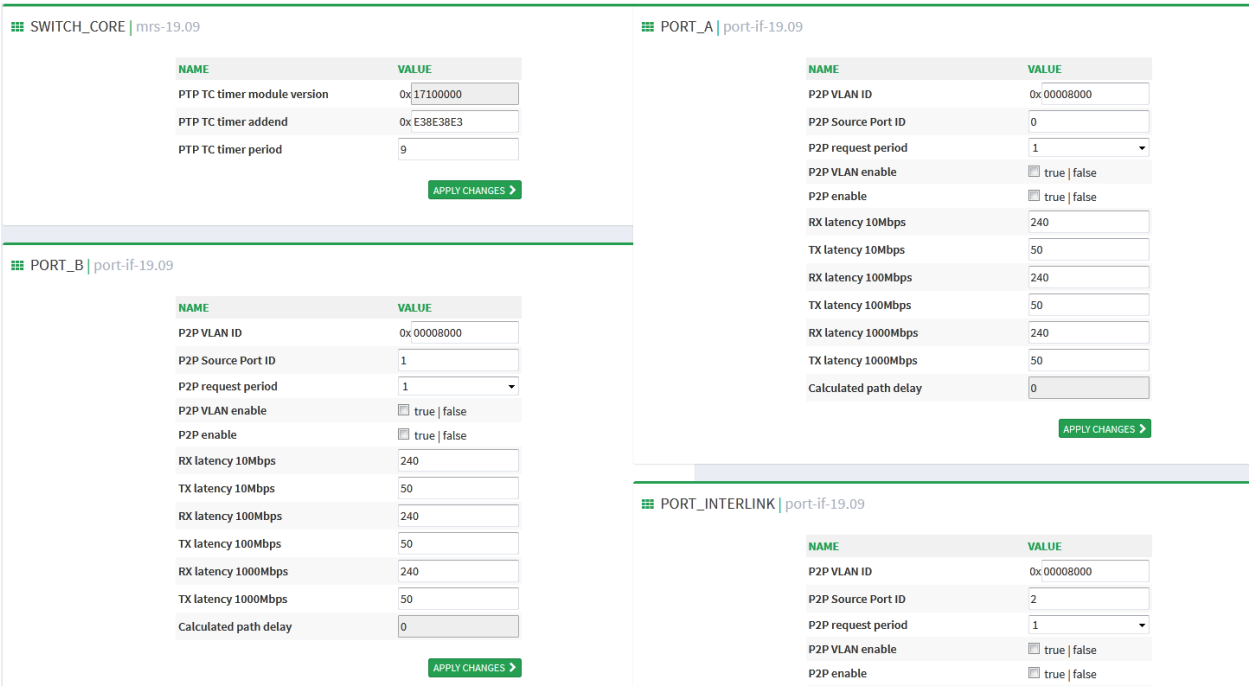


Рис. 53. Страница настройки PTP

На Рисунке 53 видно, что страница конфигурации PTP разделена на 4 части и состоит из страницы конфигурации PTP TC и страниц конфигурации PTP трех портов (port_a / port_b/ port_interlink).

1. Настройте параметры PTP TC

Страница настройки PTP TC показана на рисунке ниже:

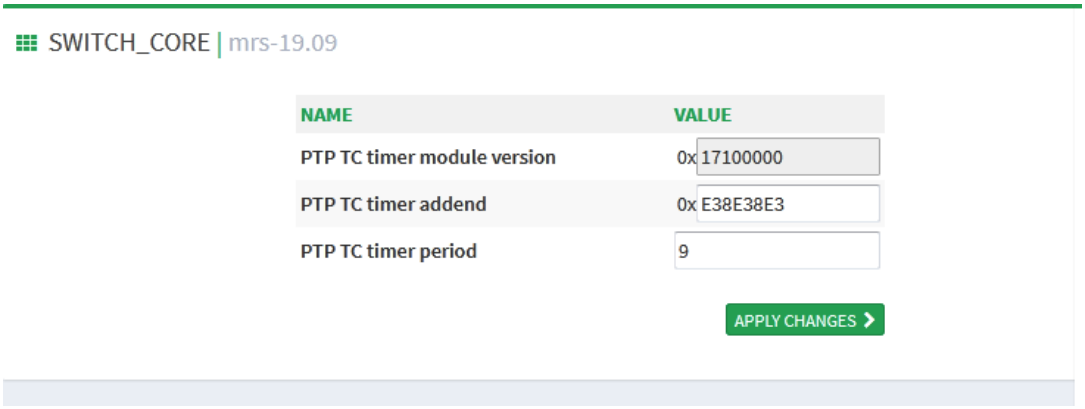


Рис. 54. Страница настройки PTP TC

Версия модуля таймера PTP TC (PTP TC timer module version)

Описание: Версия модуля таймера TC по стандарту IEEE1588.

Добавление таймера PTP TC (PTP TC timer addend)
Диапазон настроек: 32 бита [00-FFFFFFFF]
Настройки по умолчанию：E38E38E3
Функция: настройка таймера на уровне долей секунды (см. документ AN3423)
Период таймера PTP TC (PTP TC timer period)
Диапазон настроек: 32 бита [0-4294967295]
Конфигурация по умолчанию：9
Функция: см. документ AN3423.

2. Настройте параметры порта PTP
Ниже показана страница конфигурации порта port_a PTP, где порт port_a рассматривается в качестве примера:

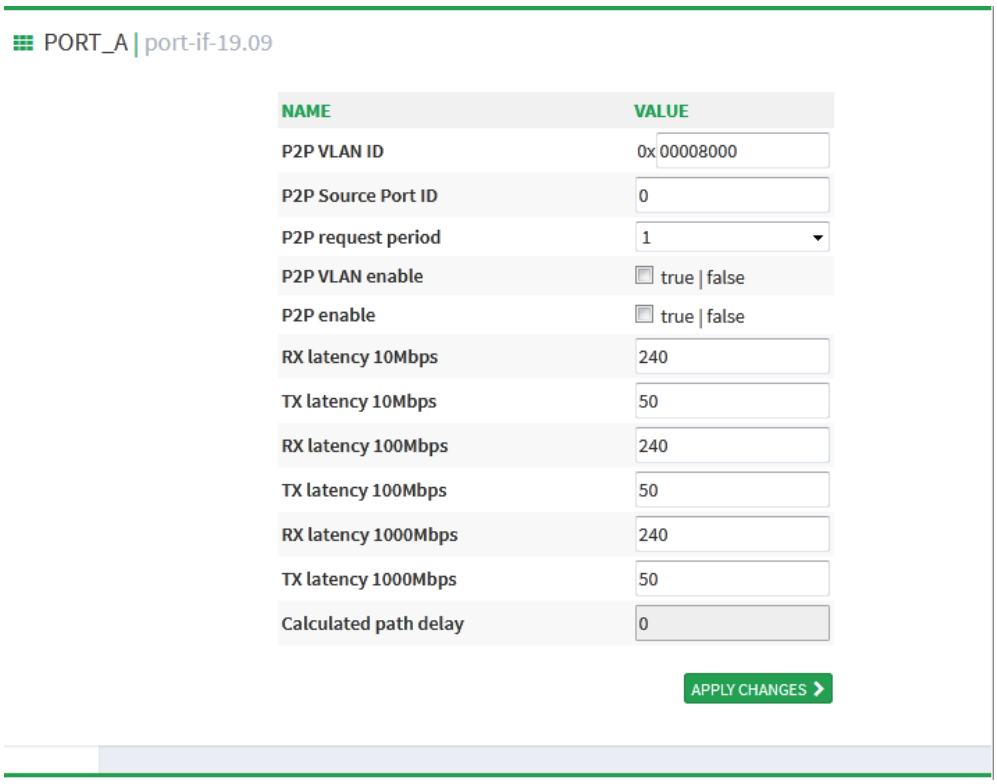


Рис. 55. Страница настройки PTP TC

Идентификатор P2P VLAN (P2P VLAN ID)
Диапазон настроек: 16 битов [00-FFFF]
Настройки по умолчанию: 00008000
Функция: настройка тега VLAN для PTP.
Идентификатор порта источника P2P (P2P Source Port ID)
Диапазон настроек: 8 битов [00-255]
Настройки по умолчанию: 0
Функция: настройка идентификатора порта источника PTP.

Период запроса P2P (P2P request period)
Опции: 1/2/4/8
Настройки по умолчанию: 1
Функция: количество задержек запросов в секунду.
Включить VLAN P2P (P2P VLAN enable)

Опции: true/false (истина/ложь)
Настройки по умолчанию: false (ложь)
Функция: добавить тег VLAN к сообщению PTP
Включить P2P (P2P enable)
Опции: true/false(истина/ложь)
Настройки по умолчанию: false (ложь)
Функция: включить или выключить механизм задержки PTP.
Время отклика RX 10 Мбит/с (RX latency 10Mbps)
Диапазон настроек: 16 битов [0-65535]
Настройки по умолчанию: 240
Функция: задержка логики RX (нс (10Мбит/с) как единица измерения).
Время отклика TX 10 Мбит/с (TX latency 10Mbps)
Диапазон настроек: 16 битов [0-65535]
Настройки по умолчанию: 50
Функция: задержка логики TX (нс (10 Мбит/с) как единица измерения).
Время отклика RX 100 Мбит/с (RX latency 100Mbps)
Диапазон настроек: 16 битов [0-65535]
Настройки по умолчанию: 240
Функция: задержка логики RX (нс (100 Мбит/с) как единица измерения).
Время отклика TX 100 Мбит/с (TX latency 100Mbps)
Диапазон настроек: 16 битов [0-65535]
Настройки по умолчанию: 50
Функция: задержка логики TX (нс (100 Мбит/с) как единица измерения).
Время отклика RX 1000 Мбит/с (RX latency 1000Mbps)
Диапазон настроек: 16 битов [0-65535]
Настройки по умолчанию: 240
Функция: задержка логики RX (нс (1000 Мбит/с) как единица измерения).
Время отклика TX 1000 Мбит/с (TX latency 1000Mbps)
Диапазон настроек: 16 битов [0-65535]
Настройки по умолчанию: 50
Функция: задержка логики TX (нс (1000 Мбит/с) как единица измерения).
Рассчитанная задержка (Calculated path delay)
Функция: задержка прохождения сигнала (единица измерения - нс), рассчитанная с применением механизма peer-to-peer прозрачных часов PTP.

7.3. Статистика

Откройте дерево навигации [Functions]→[Statistics] и войдите на страницу конфигурации статистики Statistics, которая показана ниже на примере порта port_a.

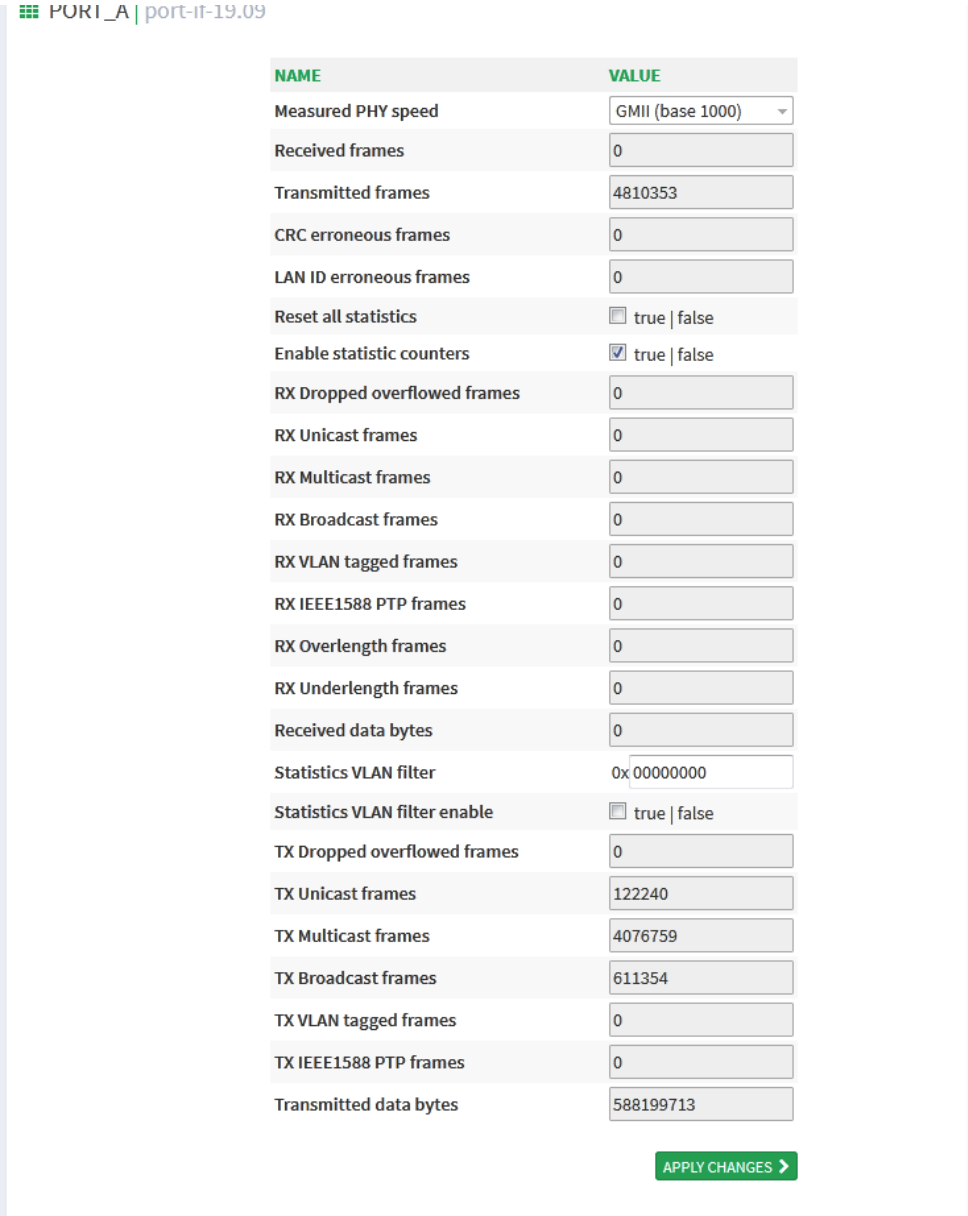


Рис. 56. Страница настройки статистики

Измеренная скорость посредством PHY (Measured PHY speed)
Описание: скорость, измеренная с помощью модуля измерения скорости: "11" при 1000 Мбит/с, "10" при 100Мбит/с и "01" при 10 Мбит/с.
Принятые кадры (Received frames)
Описание: количество принятых кадров. Диапазон: 32 бита [0-4294967295]
Отправленные кадры (Transmitted frames)
Описание: количество отправленных кадров. Диапазон: 32 бита [0-4294967295]

Ошибочные кадры CRC (CRC erroneous frames)
Описание: количество ошибочных кадров CRC. Диапазон: 32 бита [0-4294967295]
Ошибочные кадры LAN ID (LAN ID erroneous frames)
Описание: количество ошибочных кадров ID. Диапазон: 32 бита [0-4294967295]
Сброс всей статистики (Reset all Statistics)
Описание: сброс всех счетчиков статистики.
Включение счетчиков статистики (Enable statistic counters)
Описание: включить/выключить (Enable/disable) счетчики статистики.
Отброшенные кадры переполнения RX (RX Dropped overflowed frames)
Описание: количество отбрасываемых кадров переполнения RX (в тракте приема). Диапазон: 32 бита [0-4294967295]。
Одноадресные кадры RX (RX Unicast frames)
Описание: количество одноадресных кадров RX. Диапазон: 32 бита [0-4294967295]
Многоадресные кадры RX (RX Multicast frames)
Описание: количество многоадресных кадров RX. Диапазон: 32 бита [0-4294967295]
Широковещательные кадры RX (RX Broadcast frames)
Описание: количество широковещательных кадров RX. Диапазон: 32 бита [0-4294967295]
Тегированные кадры RX VLAN (RX VLAN tagged frames)
Описание: количество тегированных кадров. Диапазон: 32 бита [0-4294967295]
Кадры RX IEEE1588 PTP (RX IEEE1588 PTP frames)
Описание: количество кадров RX IEEE1588 PTP. Диапазон: 32 бита [0-4294967295]
Слишком длинные кадры RX (RX Overlength frames)
Описание: количество слишком длинных кадров RX. (значение действительно, когда отключены jumbo-кадры). Диапазон: 32 бита [0-4294967295]
Слишком короткие кадры RX (RX Underlength frames)
Описание: количество слишком коротких (кадры меньше минимальной длины) кадров. Диапазон: 32 бита [0-4294967295]
Принятые байты данных (Received data bytes)
Описание: количество принятых байтов данных (не включает ведущий байт) Диапазон: 32 бита [0-4294967295]
Фильтр статистики VLAN (Statistics VLAN filter)
Описание: назначение счетчика фильтра VLAN. Диапазон: 12 битов 0X[0-00000FFF]。
Включение фильтра статистики VLAN (Statistics VLAN filter enable)
Описание: Включение указанного счетчика фильтра VLAN.
Отброшенные кадры переполнения TX (RX Dropped overflowed frames)
Описание: количество отбрасываемых кадров переполнения TX (в тракте приема). Диапазон: 32 бита [0-4294967295]。
Одноадресные кадры TX (TX Unicast frames)
Описание: количество одноадресных кадров TX. Диапазон: 32 бита [0-4294967295]
Многоадресные кадры TX (TX Multicast frames)
Описание: количество многоадресных кадров TX. Диапазон: 32 бита [0-4294967295]
Широковещательные кадры TX (TX Broadcast frames)

Описание: количество широковещательных кадров TX. Диапазон: 32 бита [0-4294967295]

Тегированные кадры TX VLAN (TX VLAN tagged frames)

Описание: количество тегированных кадров TX VLAN. Диапазон: 32 бита [0-4294967295]

Кадры TX IEEE1588 PTP (TX IEEE1588 PTP frames)

Описание: количество кадров TX IEEE1588 PTP. Диапазон: 32 бита [0-4294967295]

Переданные байты данных (Transmitted data bytes)

Описание: количество переданных байтов данных (не включает ведущий байт). Диапазон: 32 бита [0-4294967295].

8. Другие настройки

8.1. Аварийная сигнализация

8.1.1. Введение

Данная серия коммутаторов поддерживают следующие типы аварийных сигналов:

- Memory / CPU usage alarm (Аварийный сигнал об использовании памяти / загрузке ЦП). Если данная функция включена, срабатывает аварийный сигнал, когда уровень загрузки ЦП/памяти превышает указанный порог.
- Port alarm (Аварийный сигнал о сбое порта): Если эта функция включена, срабатывает аварийный сигнал в случае, когда порт находится в нерабочем состоянии.

При включенной функции аварийной сигнализации доступны следующие аварийные режимы: запись данных, мерцание светодиодного аварийного индикатора на передней панели, срабатывание аварийного реле, подключенного к клеммной колодке, а также отправка пакетов SNMP trap.

8.1.2. Настройка через WEB-интерфейс

1. Настройка и отображение аварийных сигналов загрузки памяти и ЦП.

Откройте дерево навигации [Other Configurations]→[Alarm] и войдите в настройки Alarm (Аварийный сигнал), отобразится окно, как показано ниже:

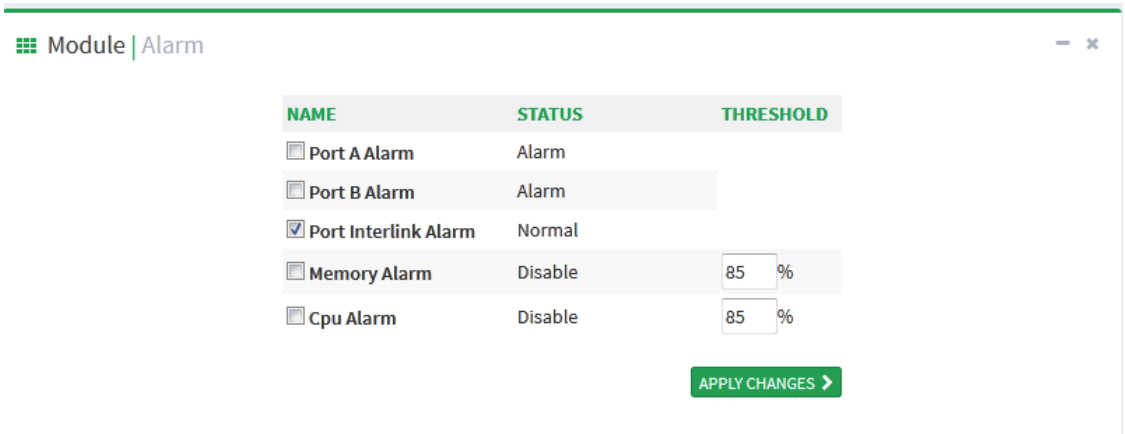


Рис. 57. Страница настройки аварийных сигналов ЦП и памяти

Аварийный сигнал» Загрузка памяти/ ЦП» (Memory Alarm/CPU Alarm)
Опции: Enable/Disable (включить/выключить)
Настройки по умолчанию: Disable (выключено)
Функция: включение или выключение аварийных сигналов загрузки памяти / ЦП.
Порог % (Threshold)
Настраиваемый дипазон: 50~100
Настройки по умолчанию: 85
Функция: настройка порога аварийного сигнала загрузки памяти/ЦП на коммутаторе. Когда уровень загрузки памяти/ЦП коммутатора выше заданного значения, формируется аварийный сигнал о превышении загрузки памяти/ЦП.
Пояснение: при формировании аварийного сигнала о превышении загрузки памяти/ЦП с целью предотвращения колебания значения загрузки памяти/ЦП около порогового значения, которые вызывают частые срабатывания аварийных сигналов и их выключение, аварийный сигнал отключается только когда процентное соотношение загрузки памяти/ЦП будет на одно плавающее значение ниже порогового.
Статус аварийного сигнала (Alarm status)
Варианты отображения: Normal/Alarm (Нормально/Авария)
Функция: отображение статуса загрузки памяти/ЦП на коммутаторе. Аварийный режим показывает, что загрузка памяти/ЦП превышает пороговое значение.

Коэффициент загрузки ЦП в данном контексте обозначает средний коэффициент загрузки ЦП за период 5 секунд.

2. Настройка и отображение аварийных сигналов сбоев порта.
Откройте дерево навигации [Other Configurations]→[Alarm] и войдите в настройки Alarm (Аварийный сигнал), отобразится окно, как показано ниже:

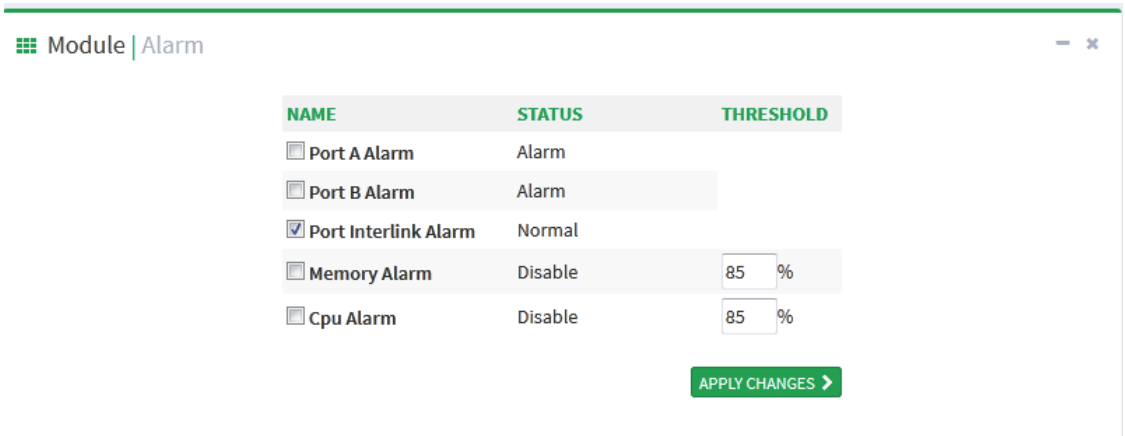


Рис. 58. Страница настройки аварийных сигналов порта

Аварийный сигнал» Загрузка памяти/ ЦП» (Memory Alarm/CPU Alarm)

Опции: Enable/Disable (включить/выключить)
Настройки по умолчанию: Enable (включено)
Функция: включение или выключение аварийного сигнала о сбое порта (включить и выключить аварийный сигнал).

Статус аварийного сигнала (Alarm status)

Варианты отображения: LinkDown/LinkUp (Работает/Не работает)
Функция: отображение статуса работы порта. LinkUp показывает, что порт подключен и может осуществлять нормальный обмен данными. LinkDown показывает, что порт не подключен, имеет неисправность и в данном случае формируется аварийный сигнал.

8.2. Настройка портов коммутатора

Откройте дерево навигации [Other Configurations]→[Port configuration] и войдите на страницу конфигурации портов. Вы можете настроить параметры канала связи, скорость передачи данных, тип порта и т.д., как показано ниже:

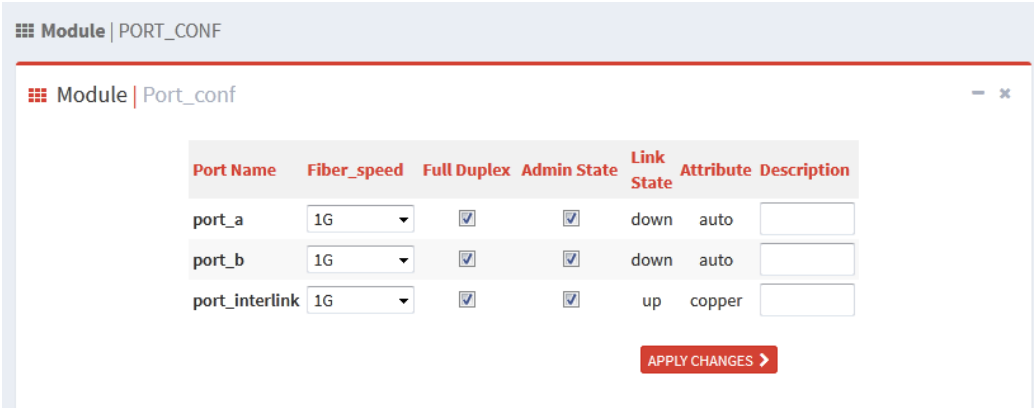


Рис. 59. Настройка портов

Имя порта (Port Name)

Существует три типа порта: port_a, port_b и port_interlink

Скорость передачи данных по оптоволокну (Fiber_speed)

Опции: 100M/1G (100 Мбит/с / 1 Гб/с)
Функция: настройка автоматического согласования скорости порта.
Описание: при установке работы порта в автоматический режим, скорость порта по умолчанию определяется путем автоматического согласования скорости портом на другой стороне канала связи. При этом согласованная скорость может быть любой в возможном диапазоне скорости порта. При настройке скорости порт может согласовать только часть скорости, таким образом, контролируя процесс согласования скорости. Только оптический порт можно устанавливать в режим 100 Мбит/с.

- Настойка дуплексной передачи и скорости доступны только в авто режиме.
- Порт port_interlink подмодуля SM6.6-HSR/PRP используется внутри сети. Не настраивайте или закрывайте его.

Настройка режима передачи (Full Duplex)
Опции: Fdx/Hdx (Full Duplex/Half Duplex, Дуплексный/Полудуплексный)
Функция: настройка автоматического согласования режима передачи порта.
Описание: Полнодуплексный режим «Fdx» означает, что порт может одновременно принимать и передавать данные. Полудуплексный режим «Hdx» означает, что одновременно порт может либо передавать, либо получать данные.
Когда настройки порта установлены в автоматический режим, по умолчанию режим работы определяется автоматическим согласованием с портом на другой стороне канала связи, при этом порт может быть либо Fdx, либо Hdx.
При настройке порт способен согласовывать только один вариант режима работы, таким образом, контролируя процесс согласования.
Admin Status (Статус Админ)
Опции: shutdown/no shutdown (отключить/не отключать)
Настройки по умолчанию: no shutdown (не отключать)
Функция: определение возможности порта передавать данные.
Описание: команда «no shutdown» активирует порт и разрешает ему передавать данные. Команда «shutdown» отключает порт и не разрешает ему передавать данные. Эта опция может напрямую влиять на состояние порта и сформировать аварийный сигнал о сбое данного порта.
Статус канала связи (Link Status)
Отображение статуса подключения текущего порта.
Режим «up» показывает, что порт находится в подключенном состоянии и может нормально передавать данные. Режим «down» показывает, что порт находится в отключенном состоянии и не может нормально передавать данные.
Определение среды передачи данных (Attribute)
Опции: auto/copper (автоматический режим / передача через «медный» порт)
Настрйки по умолчанию: auto (автоматический режим)
Функция: настройка среды передачи данных для портов Ethernet.
Описание: режим Auto автоматически определяет тип подключенного кабеля.
Copper: тип среды передачи данных для порта – «медный»
Описание (Description)
Настраиваемый диапазон: 1~200 символов.
Функция: настройка псевдонима порта для его описания.

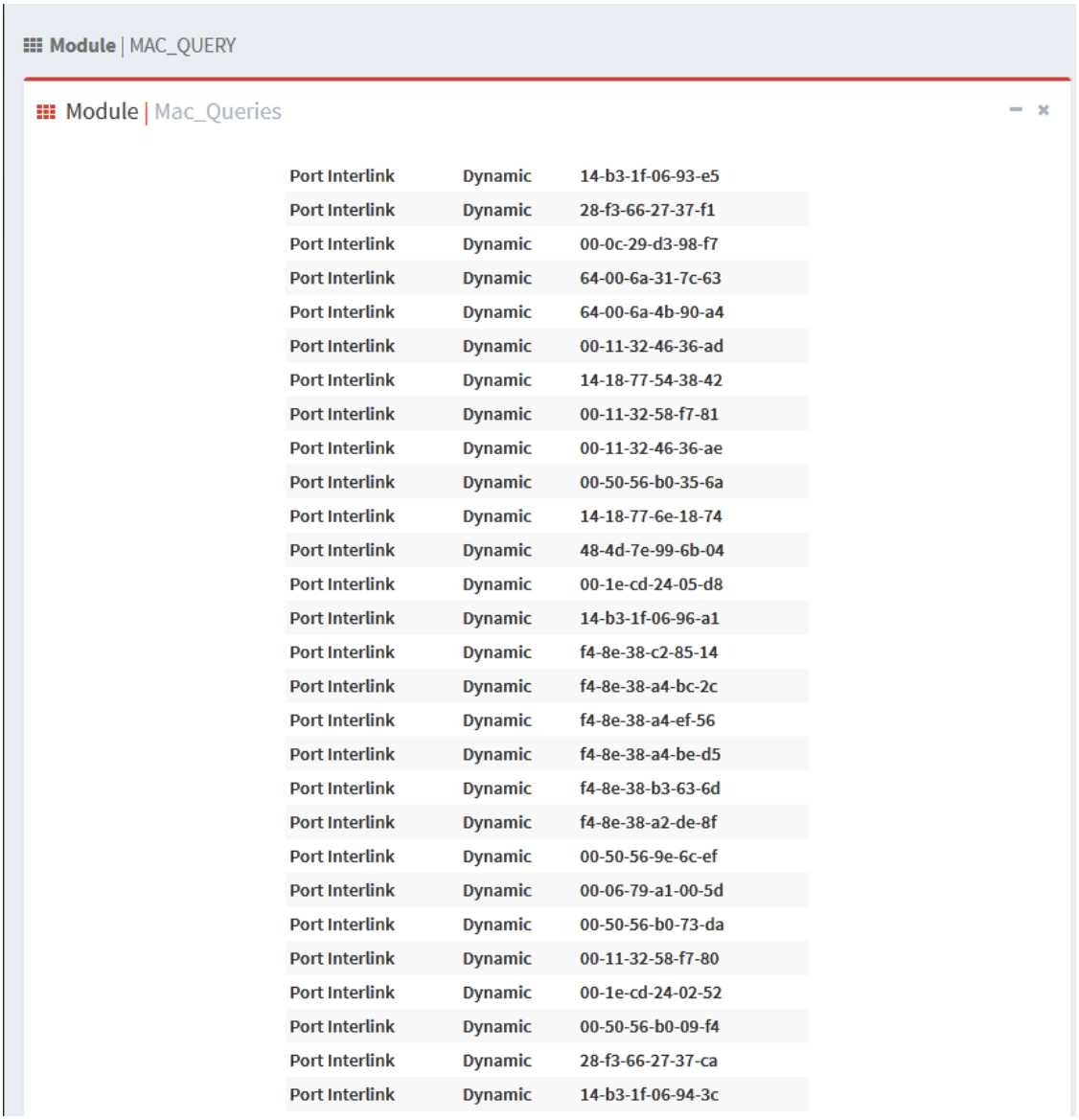
8.3. Настройка MAC-адресов

При пересылке пакета коммутатор ищет порт для переадресации в таблице MAC-адресов, имеющим MAC-адрес пункта назначения, который содержится в пересылаемом пакете.
MAC-адрес может быть статический или динамический. Статический MAC-адрес настраивается пользователем. Он обладает самым высоким приоритетом (не отменяется динамическими MAC-адресами) и действует постоянно.
Коммутатор определяет динамические MAC-адреса при переадресации данных. Они действуют только конкретный период времени. Коммутатор периодически обновляет

таблицу MAC-адресов. Получив кадр данных для переадресации, коммутатор определяет исходный MAC-адрес кадра, устанавливает соответствие с принимающим портом, запрашивает переадресующий порт в таблице MAC-адресов согласно MAC-адресу пункта назначения кадра. Если соответствие установлено, коммутатор пересылает кадр данных от соответствующего порта. Если соответствие не установлено, коммутатор транслирует кадр в своем широковещательном домене.
Время старения начинается с того момента, когда динамический MAC-адрес добавлен в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение времени, в 1-2 раза превышающего время старения, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки. Статические MAC-адреса не подразумевают понятие «время старения».

8.3.1. Запросы MAC-адресов

Откройте дерево навигации [Other Configurations] →[Mac Queries] и войдите на страницу запроса MAC-адреса, как показано ниже:



Port Interlink	Dynamic	14-b3-1f-06-93-e5
Port Interlink	Dynamic	28-f3-66-27-37-f1
Port Interlink	Dynamic	00-0c-29-d3-98-f7
Port Interlink	Dynamic	64-00-6a-31-7c-63
Port Interlink	Dynamic	64-00-6a-4b-90-a4
Port Interlink	Dynamic	00-11-32-46-36-ad
Port Interlink	Dynamic	14-18-77-54-38-42
Port Interlink	Dynamic	00-11-32-58-f7-81
Port Interlink	Dynamic	00-11-32-46-36-ae
Port Interlink	Dynamic	00-50-56-b0-35-6a
Port Interlink	Dynamic	14-18-77-6e-18-74
Port Interlink	Dynamic	48-4d-7e-99-6b-04
Port Interlink	Dynamic	00-1e-cd-24-05-d8
Port Interlink	Dynamic	14-b3-1f-06-96-a1
Port Interlink	Dynamic	f4-8e-38-c2-85-14
Port Interlink	Dynamic	f4-8e-38-a4-bc-2c
Port Interlink	Dynamic	f4-8e-38-a4-ef-56
Port Interlink	Dynamic	f4-8e-38-a4-be-d5
Port Interlink	Dynamic	f4-8e-38-b3-63-6d
Port Interlink	Dynamic	f4-8e-38-a2-de-8f
Port Interlink	Dynamic	00-50-56-9e-6c-ef
Port Interlink	Dynamic	00-06-79-a1-00-5d
Port Interlink	Dynamic	00-50-56-b0-73-da
Port Interlink	Dynamic	00-11-32-58-f7-80
Port Interlink	Dynamic	00-1e-cd-24-02-52
Port Interlink	Dynamic	00-50-56-b0-09-f4
Port Interlink	Dynamic	28-f3-66-27-37-ca
Port Interlink	Dynamic	14-b3-1f-06-94-3c

Рис. 60. Запрос MAC-адресов

- В режиме коммутации порты port_a, port_b, port_interlink соответствуют трем реальным портам.
- В режиме резервирования порт port_b представляет два порта резервирования, которые не различают порт A и B. Порт port_a не используется.

8.3.2. Управление MAC-адресами

Откройте дерево навигации [Other Configurations]→[Mac Address Control] (Управление MAC-адресом) и войдите на страницу управления MAC-адресом, как показано ниже:

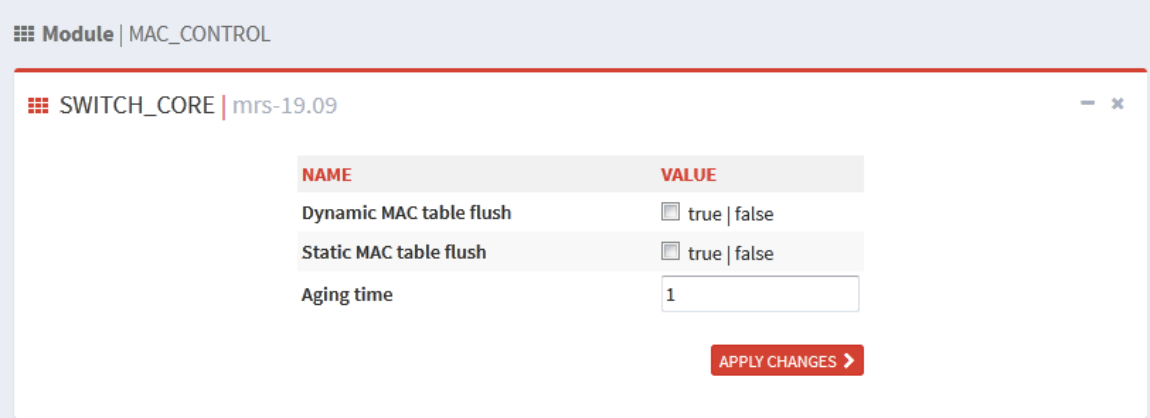


Рис. 61. Страница управления MAC-адресами

Сбросить таблицу динамических MAC-адресов (Dynamic MAC table flush)
Опции: true/false (истина/ложь)
Настройки по умолчанию: false (ложь)
Функция: настройка обновления динамических MAC-адресов.
Сбросить таблицу статических MAC-адресов (Static MAC table flush)
Опции: true/false (истина/ложь)
Настройки по умолчанию: false (ложь)
Функция: настройка обновления статических MAC-адресов.
Время старения (Aging time)
Опции: 0-15мин
Настройки по умолчанию: 1
Функция: настройка времени старения таблицы MAC-адресов.

8.3.3. Настройка MAC-адресов

Откройте дерево навигации [Other Configurations]→[Mac Address Configuration] и войдите на страницу конфигурации MAC-адресов, как показано ниже:

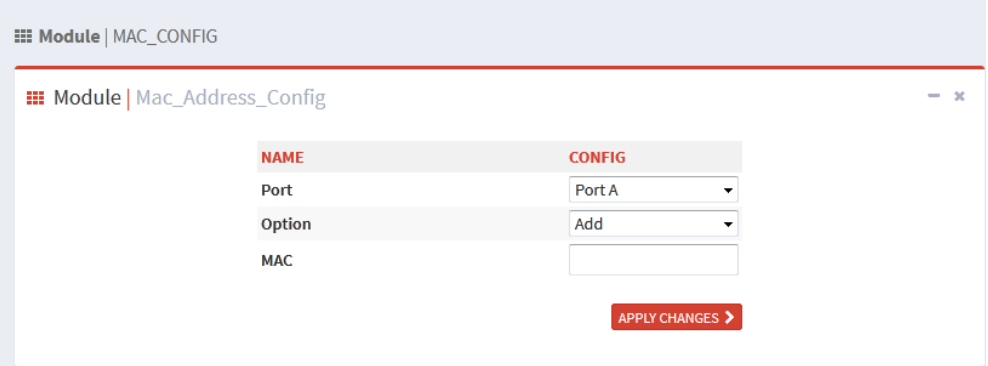


Рис. 62. Страница настройки MAC-адресов

Порт (Port)
Опции: port_a /port_b / port_interlink
Настройки по умолчанию: port_a
Опция (Option)
Опции: add/delete (добавить/удалить)
Настройки по умолчанию: add (добавить)
Функция: удалить или добавить MAC-адрес порта.
MAC-адрес (MAC)
Формат: HH-HH-HH-HH-HH-HH (H – это шестнадцатеричное число)
Функция: настройка одноадресного MAC-адреса с младшим битом старшего байта, равным 0.

8.4. Протокол SNTP

8.4.1. Введение

Протокол SNTP настраивает время, отправляя запросы и ответы между сервером и клиентом. Коммутатор играет роль клиента для калибровки времени в соответствии с сообщением сервера.
Запрос клиента SNTP отсылается на сервер один за другим путем одноадресной передачи, сервер отвечает на сообщение.

- Когда коммутатор использует протокол SNTP, сервер SNTP должен активен.
- Информация о времени в протоколе SNTP - это стандартная информация о времени для нулевого часового пояса.

8.4.2. Настройка SNTP с помощью Web-интерфейса

1. Включение протокола SNTP

Откройте дерево навигации [Other Configurations]→[SNTP] и войдите на страницу конфигурации SNTP, как показано ниже:

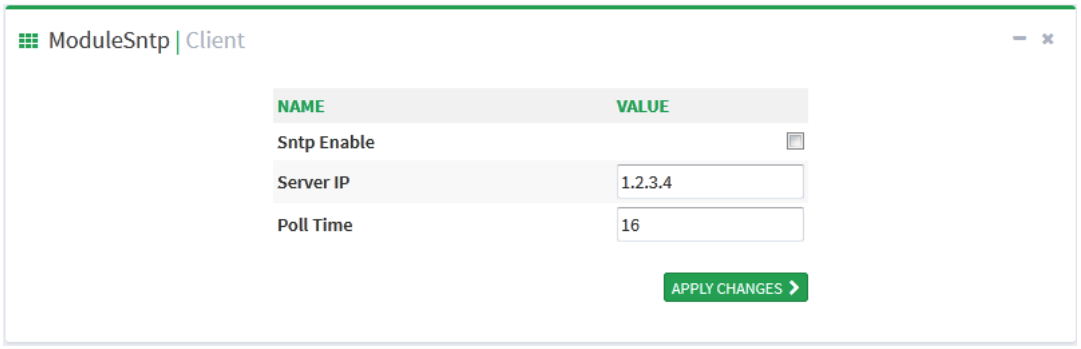


Рис. 63. Страница настройки MAC-адресов

Включить SNTP (SNTP Enable)
Опции: Enable/Disable (включить/выключить)
Настройки по умолчанию: Disable (выключено)
Функция: включение или выключение протокола SNTP

Поскольку протоколы NTP и SNTP используют один и тот же номер порта udp, оба протокола не могут быть одновременно активны.

2. Настройка IP-адреса сервера SNTP
IP-адрес сервера (Server IP)
Формат: A.B.C.D
Функция: настройка IP-адреса сервера SNTP. Клиент выполняет калибровку времени в соответствии с сообщением от этого сервера.

3. Настройка временного интервала отправки запроса на синхронизацию от SNTP-клиента
Время опроса (Poll Time)
Опции: 16~16284c
Функция: для настройки временного интервала SNTP-клиент отправляет запрос на синхронизацию серверу SNTP.

4. Просмотр информации о синхронизации часов с временем сервера
Откройте дерево навигации [Network Nodes] и войдите на страницу просмотра часов, как показано ниже:

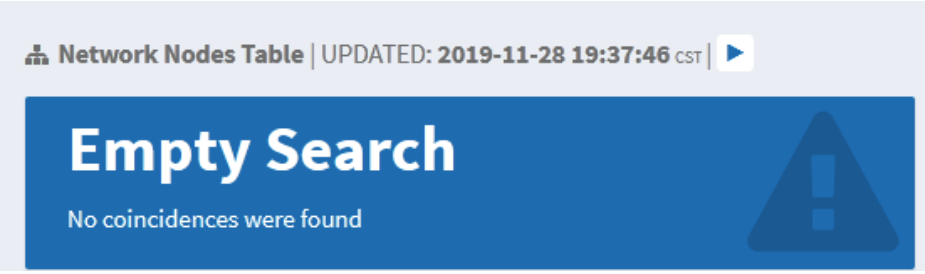


Рис. 64. Просмотр страницы синхронизации часов

Нажмите на кнопку <display clock> (отобразить часы). Часы отобразятся в окне после того, как SNTP-клиент синхронизирует время с сервером.

8.5. Протокол NTP

8.5.1. Введение

Протокол NTP выполняет синхронизацию времени между распределенными серверами и клиентами. Протокол NTP также синхронизирует часы всех сетевых устройств, обеспечивая согласованность времени на всех устройствах. Это позволяет устройствам поддерживать работу нескольких приложений в одно и то же время. Локальная система с поддержкой NTP не только синхронизирует свои часы с другими источниками времени, но также служит источником времени для других устройств.

Как показано на рисунке 65, задержка на подтверждение приёма «(T4-T1)-(T3-T2)» и сдвиг часов «((T2-T1) + (T3-T4))/2» могут быть рассчитаны с учетом обмена пакетами NTP, таким образом, обеспечив высокоточную синхронизацию времени устройств.

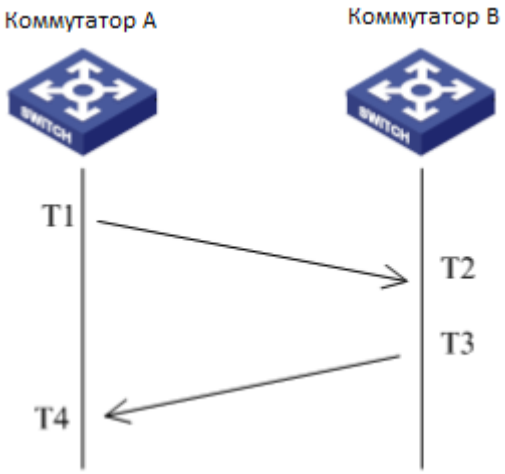


Рис. 65. Работа протокола NTP

8.5.2. Режим работы NTP

NTP может использовать различные режимы работы для синхронизации времени. При необходимости Вы можете выбрать соответствующий режим работы.

Режим Client/Server: в этом режиме клиент отправляет пакеты синхронизации времени (режим клиента) на сервер. После получения пакетов сервер автоматически начинает работать в режиме сервера и отправляет ответные пакеты (режим сервера). После получения ответных пакетов клиент выполняет синхронизацию с оптимальным временем сервера.

Режим Peer: В этом режиме активный одноранговый узел отправляет пакеты синхронизации времени (активный режим Peer) пассивному одноранговому узлу. После получения пакетов пассивный одноранговый узел автоматически начинает работать в пассивном режиме Peer и отправляет ответные пакеты (пассивный режим Peer). На основе обмена пакетами устройства устанавливают режим Peer. Активный одноранговый

и пассивный одноранговый узлы могут синхронизировать время друг с другом. Если оба одноранговых узла синхронизировали время с другими устройствами, одноранговый узел с большими тактовыми импульсами синхронизирует время с одноранговым узлом с меньшими тактовыми импульсами.

Режим Broadcast: В этом режиме широковещательный сервер периодически передает пакеты синхронизации времени (широковещательный режим). После получения пакетов широковещательный клиент отправляет на сервер пакеты синхронизации времени (режим клиента). После получения пакетов запроса сервер отправляет ответные пакеты (режим сервера). Сервер и клиент выполняют синхронизацию времени, обмениваясь восемью пакетами запроса и ответа.

Режим Multicast: Клиент многоадресной рассылки периодически отправляет широковещательные пакеты с запросами о синхронизации (режим клиента) на сервер многоадресной рассылки. После получения пакетов сервер отправляет одноадресные ответные пакеты (режим сервера). Затем сервер и клиент выполняют синхронизацию времени, обмениваясь одноадресным запросом о синхронизации времени и ответными пакетами.

1. Включение протокола NTP

Откройте дерево навигации [Other Configurations]→[NTP] и войдите в интерфейс общей конфигурации NTP, как показано ниже:

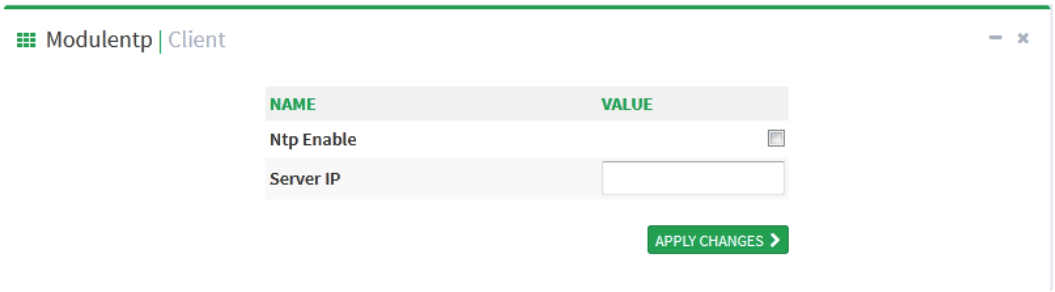


Рис. 66. Включение протокола NTP

Включить NTP (NTP Enable)

Опции: Enable/Disable (включить/выключить)

Настройки по умолчанию: Disable (выключено)

Функция: включение или выключение протокола NTP

- Поскольку протоколы NTP и SNTP используют один и тот же номер порта udp, оба протокола не могут быть одновременно активны.
- Когда сервис NTP не включен, сервис NTP можно настроить и сохранить. Это значит, что включенное или выключенное состояние сервиса NTP не влияет на настройки сервиса NTP.

2. Настройка протокола NTP

IP-адрес сервера (Server IP)

Формат: A.B.C.D

Функция: настройка IP-адреса сервера NTP. Клиент выполняет калибровку времени в соответствии с сообщением от этого сервера.

8.6. IEC61850 MMS

8.6.1. Вступление

В теории работа коммутатора на сетях передачи данных электрических подстанций является прозрачной. Для мониторинга и управления требуются обычные инструменты (протоколы), не связанные с IEC61850, такие как EMS, WEB, CLI, OPC и т.д. А для решения проблем, связанных с корректной работой коммутатора в сетях электрических подстанций он должен быть спроектирован в соответствии с требованиями протокола IEC61850 и внедрен в автоматизированную систему подстанции (IEC61850) как интеллектуальное электронное устройство (IED, Intelligent Electronic Device). Такой подход позволит обеспечить удобное интегрированное управление пользователями, экономию затрат на монтаж и экономию затрат на техническое обслуживание.

Базовые моделирующие файлы switch.cid по умолчанию, импортированы на данный коммутатор. Если Заказчику требуется импортировать другие моделирующие файлы, следует изучить информацию в Разделе «6.4 Загрузка файлов».

8.6.2. Настройка через WEB-интерфейс

1. Включение функции IEC 61850

Откройте дерево навигации [Other Configurations]→[Iec61850mms] и войдите на страницу общей конфигурации IEC 61850, как показано ниже:

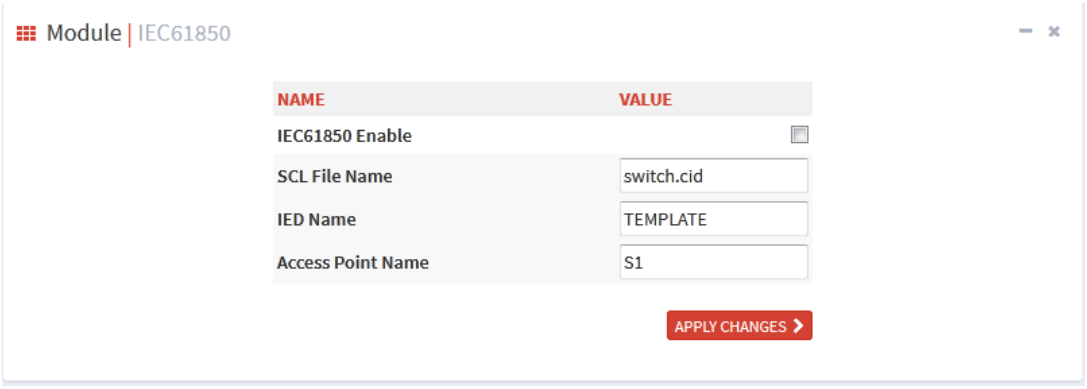


Рис. 67. Включение протокола IEC 61850

Включить IEC61850 (IEC61850 Enable)
Опции: Enable/Disable (включить/выключить)
Настройки по умолчанию: Disable (выключить)
Функция: включение или выключение IEC61850.
Имя файла SCL (SCL File Name)
Диапазон настроек: 1~25 символов
Настройки по умолчанию: switch.cid

Функция: указание имени моделирующего файла, который начинает действовать при инициализации функции IEC61850.

Имя IED (IED Name)

Диапазон настроек: 1~25 символов

Настройки по умолчанию: TEMPLATE (ШАБЛОН)

Функция: настройка имени логического устройства для этого IED в моделирующем файле.

Имя точки доступа (Access Point Name)

Диапазон конфигурации: 1~25 символов

Настройки по умолчанию: S1

Функция: настройка имени точки доступа для этого IED в моделирующем файле.

Настройки имени точки доступа и имени IED должны соответствовать именам точки доступа и IED в указанном моделирующем файле, в противном случае запуск функции IEC 61850 завершится неудачно.

8.7. Протокол SNMPv2c

8.7.1. Введение

Simple Network Management Protocol (SNMP) - протокол управления сетевыми устройствами с использованием протокола TCP/IP. Благодаря функции SNMP, администратор может запрашивать информацию об устройстве, менять настройки, следить за состоянием устройства и обнаруживать неполадки сети.

8.7.2. Реализация

Для управления устройствами, SNMP использует архитектуру «station/agent» (станция/агент). Таким образом, по функциональности он включает две составляющие: «NMS» и «Агент».

- Network Management Station (NMS) - это рабочая станция, на которой работает SNMP-приложение для управления сетью клиентов, играющая основную роль в управлении сетью с помощью протокола SNMP.
- Агент - это программный процесс на управляемом устройстве. Он отвечает за прием и обработку запросов от NMS. При возникновении аварийной ситуации агент автоматически информирует об этом NMS.

NMS является средством управления сетью SNMP, соответственно Агент управляется сетью SNMP. Обмен информацией управления между NMS и Агентом осуществляется через SNMP. Протокол SNMP обеспечивает выполнение 5 основных операций:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

NMS отправляет команды «Get-Request», «Get-Next-Request» и «Set-Request» для запроса данных, настройки и управления устройством. После получения этих запросов, Агенты отвечают командами «Get-Response». При возникновении тревоги агент автоматически

отправит сообщение «Trap» в NMS, чтобы сообщить о возникновении аномальных событий.

8.7.3. Описание

Данные серии коммутаторов поддерживают версию SNMPv2 и SNMPv3. При этом SNMPv2 совместим с SNMPv1.
SNMPv1 использует принцип аутентификации по имени сообщества (Community Name Authentication). Имя сообщества работает как пароль и используется для ограничения доступа NMS к агенту. Если имя сообщества SNMP-сообщения не может пройти аутентификацию устройства, возникает сбой запроса и в ответ отсылается сообщение об ошибке.
SNMPv2 также использует аутентификацию по имени сообщества. Он не просто совместим с SNMPv1, но и расширяет функции SNMPv1. Корректная совместная работа NMS и Агента основывается на согласованной версии SNMP. Агент может быть настроен для работы с несколькими версиями одновременно и использовать разные версии для связи с разными NMS.

8.7.4. Описание MIB (Management Information Base)

Любой управляемый ресурс можно рассматривать как объект, соответственно он называется управляемым объектом.
MIB (Management Information Base) - это совокупность всех управляемых объектов. MIB определяет иерархические отношения между управляемыми объектами и определяет основные атрибуты объектов, например, имя объекта, права доступа, типы данных и т.д. У каждого Агента есть своя MIB. NMS может читать или записывать объекты в MIB в соответствии со своими правами. Связь NMS, Агента и MIB показана на рисунке 67.

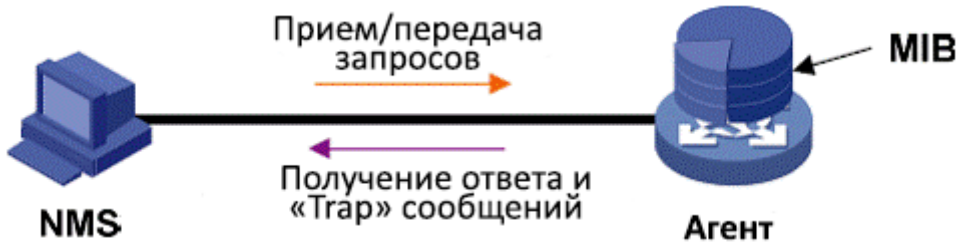


Рис. 68. Взаимосвязь NMS, Агента и базы MIB

MIB определяет древовидную структуру, где каждый узел дерева является управляемым объектом. Каждый узел дерева содержит OID (Идентификатор объекта), который может указывать позицию узла в структуре дерева MIB. OID управляемого объекта A равен 1.2.1.1 (см. рис. 157).

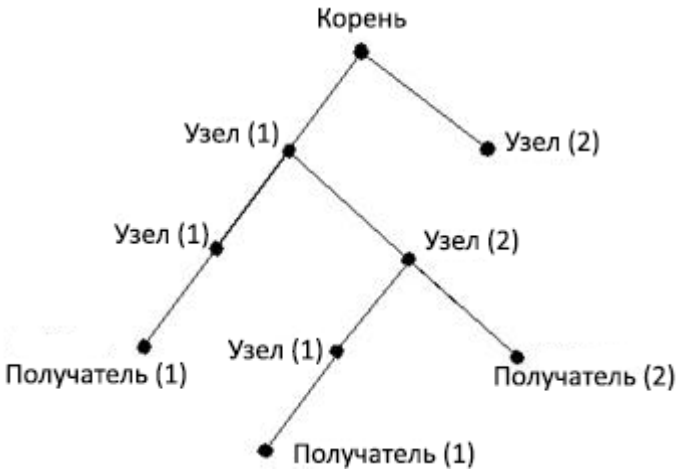


Рис. 69. Структура дерева MIB

8.7.5. Настройка через WEB-интерфейс

1. Включение протокола SNMP

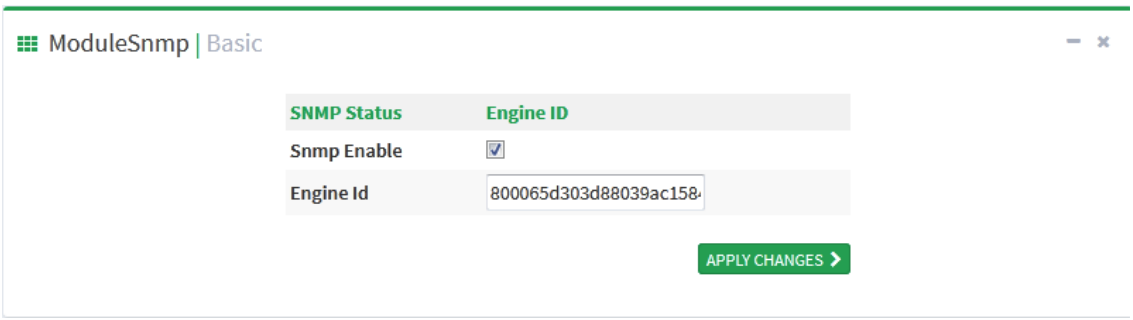


Рис. 70. Включение протокола SNMP

Включение SNMP (SNMP Enable)
Опции: Enable/Disable (включить/выключить)
Настройки по умолчанию: Enable (Включено)
Функция: Включение/Выключение протокола SNMP.
Идентификатор ядра (Engine ID)
Диапазон конфигурации: четное количество шестнадцатиричных чисел, которое не может быть полным 0 или полным F, четное количество значений в диапазоне 10~64.
Функция: настройка идентификатора системного ядра SNMPv3. Идентификатор устройства соответствующего пользователя удаляется из таблицы после внесения изменений в идентификатор ядра.

2. Настройка имени сообщества

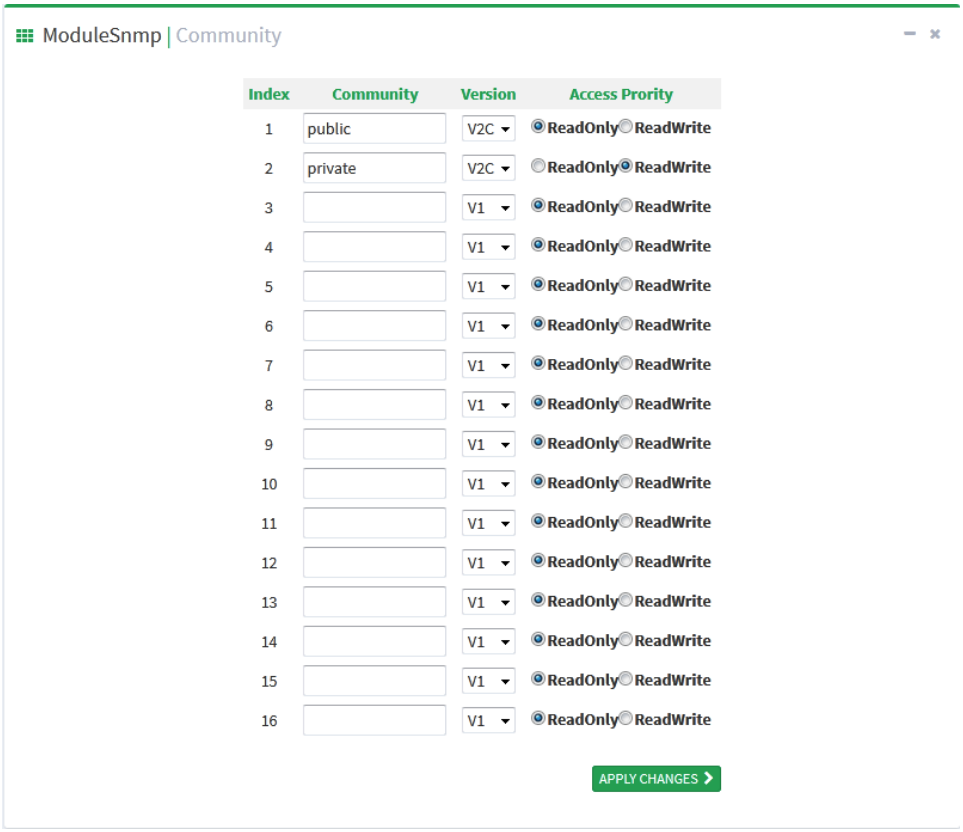


Рис. 71. Настройка имени сообщества

Сообщество (Community)

Настраиваемый диапазон: 1~32 символов

Функция: настройка имени сообщества коммутатора.

Описание: доступ к библиотеке MIB коммутатора может быть возможен только в том случае, если имя сообщества в сообщении SNMP совпадает со строками в данном обществе.

Пояснение: можно настроить до 16 строк сообщества

Версия (Version)

Опции конфигурации: V1/V2C

Функция: выбор номера версии SNMP.

Приоритет доступа (Access Priority)

Опции: Readonly/ReadWrite (только чтение / чтение-запись)

Настройка по умолчанию: Readonly (только чтение)

Функция: настройка режима доступа к библиотеке MIB.

Описание: Разрешение ReadOnly позволяет только читать информацию библиотеки MIB. Разрешение ReadWrite позволяет читать и записывать информацию в библиотеку MIB.

3. Настройка параметров передачи сообщений «Trap».

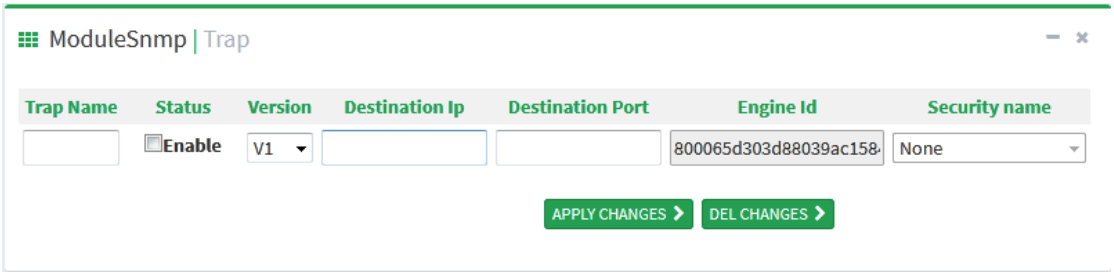


Рис. 72. Настройка «Trap»

Имя Trap (Trap name)
Настраиваемый диапазон: 1~32 символов.
Функция: Настройка имени сообщений «Trap».
Статус (Status)
Опции: Enable/Disable (включить/выключить).
Настройки по умолчанию: Disable (выключено).
Описание: включение/выключение функции отправки коммутатором сообщений «Trap».
Версия (Version)
Опции: SNMPv1/SNMPv2c/SNMPv3
Настройки по умолчанию: SNMPv1
Функция: настройка номера версии trap-сообщения, которое коммутатор отправляет на сервер.
IP-адрес пункта назначения (Destination IP)
Формат: A.B.C.D
Функция: настройка адреса сервера для получения trap-сообщений.
Порт пункта назначения (Destination Port)
Настраиваемый диапазон: 1~65535
Настройки по умолчанию: 162
Функция: настройка номера порта для отправки trap-сообщений.

8.7.6. Пример типовой настройки

NMS с SNMP подключается к коммутатору через сеть Ethernet. IP адрес NMS: 192.168.1.23, а IP адрес коммутатора: 192.168.1.2. NMS управляет и контролирует Агента с помощью протокола SNMPv2, который может читать и записывать информацию MIB узла Агента и отправляет сообщения «Trap» в NMS, когда у Агента происходит аварийная ситуация (см. рис. 73).

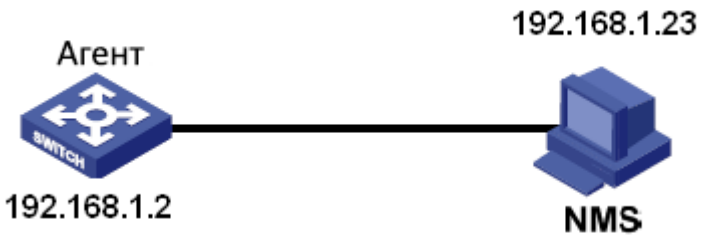


Рис. 73. Пример настройки SNMPv2

Процесс настройки Агента:

1. Включите протокол SNMP и установите статус V2 (см. рис. 64).
2. Настройте права доступа для имени сообщества «Read-Only» как «public», а для имени сообщества «Read-Write» установите значение «private» (см. рис. 71).
3. Включите режим «Trap» и установите версию V2C, настройте IP-адрес сервера как: 192.168.1.23 (см. рис. 72).

Если пользователю необходимо контролировать статус Агента, необходимо использовать соответствующее программное обеспечение, например, Symanitron NMS.

8.8. Протокол SNMPv3

8.8.1. Введение

Протокол SNMPv3 реализует механизм аутентификации на основе модели безопасности пользователя USM (User-Based Security Model). Вы можете настроить функции аутентификации и шифрования. Процесс аутентификации служит для проверки действительности отправителя пакета данных, запрещая доступ несанкционированным пользователям. Шифрование обеспечивает шифрование пакетов данных, получаемых от системы NMS и от Агента, исключая вероятность перехвата информации. Функции аутентификации и шифрования способны повысить уровень защиты соединения между системой NMS SNMP и Агентом SNMP.

8.8.2. Реализация

В протоколе SNMPv3 предусмотрено пять конфигурационных таблиц. Каждая таблица может включать 16 записей. Эти таблицы определяют право отдельных пользователей получать доступ к информации MIB.

Вы можете добавить нескольких пользователей в таблицу пользователей. Каждый пользователь следует разным политикам безопасности при аутентификации и шифровании.

Групповая таблица представляет собой совокупность нескольких пользователей. В таблице права доступа определяются согласно группам пользователей. Права группы также принадлежат всем пользователям в группе.

Контекстная таблица определяет строки, которые могут быть прочитаны пользователями независимо от моделей безопасности.

Таблица отображения относится к отображению информации MIB, в которой указывается, к какой информации MIB могут получить доступ пользователи. Отображение MIB может включать все узлы определенного поддерева MIB (то есть пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного из узлов определенного поддерева MIB (то есть пользователям не разрешен доступ ни к какому узлу поддерева MIB).

Вы можете определить права доступа к MIB в таблице доступа по имени группы, контекстному имени, модели безопасности и уровню безопасности.

8.8.3. Настройка через WEB-интерфейс

1. Включите протокол SNMP, как показано на рисунке ниже:

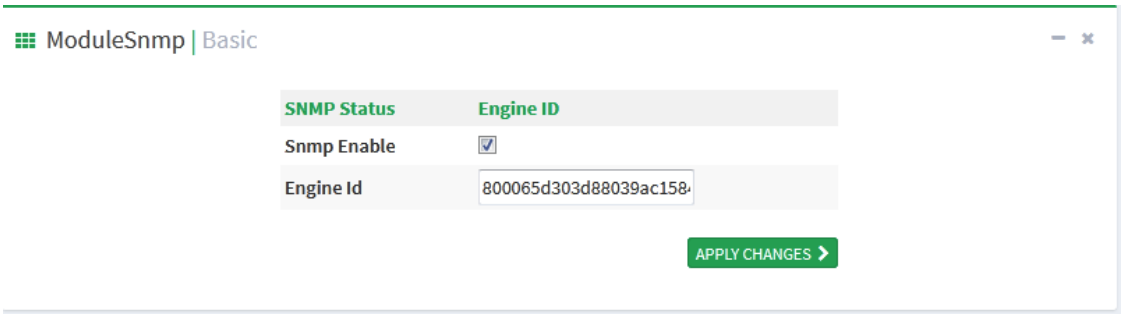


Рис. 74. Включение протокола SNMP

Включение SNMP (SNMP Enable)
Опции: Enable/Disable (включить/выключить)
Настройки по умолчанию: Enable (Включено)
Функция: Включение/Выключение протокола SNMP.
Идентификатор ядра (Engine ID)
Диапазон конфигурации: четное количество шестнадцатиричных чисел, которое не может быть полным 0 или полным F; четное количество значений в диапазоне 10~64.
Функция: настройка идентификатора системного ядра SNMPv3. Идентификатор устройства соответствующего пользователя удаляется из таблицы после внесения изменений в идентификатор ядра.

2. Настройте Trap-сообщения, как показано на рисунке ниже:

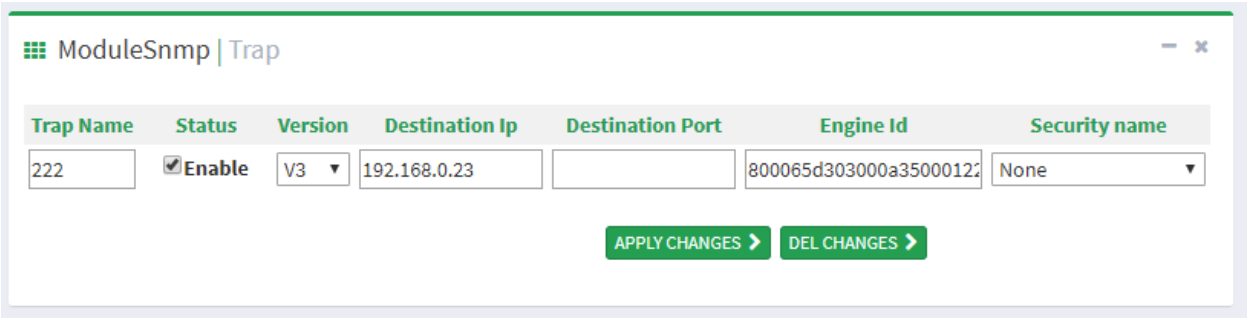


Рис. 75. Настройка Trap-сообщений

Имя Trap (Trap name)
Настраиваемый диапазон: 1~32 символов.
Функция: Настройка имени сообщений «Trap».
Статус (Status)
Опции: Enable/Disable (включить/выключить).
Настройки по умолчанию: Disable (выключено).

Функция: включение/выключение функции отправки коммутатором сообщений «Trap». Коммутатор отправляет соответствующее Trap-сообщение серверу, если функция включена.

Версия (Version)

Опции: SNMPv1/SNMPv2c/SNMPv3

Настройки по умолчанию: SNMPv1

Функция: настройка номера версии trap-сообщения, которое коммутатор отправляет на сервер.

IP-адрес пункта назначения (Destination IP)

Формат: A.B.C.D

Функция: настройка адреса сервера для получения trap-сообщений.

Порт пункта назначения (Destination Port)

Настраиваемый диапазон: 1~65535

Настройки по умолчанию: 162

Функция: настройка номера порта для отправки trap-сообщений.

3. Настройте таблицу пользователей, как показано на рисунке ниже:

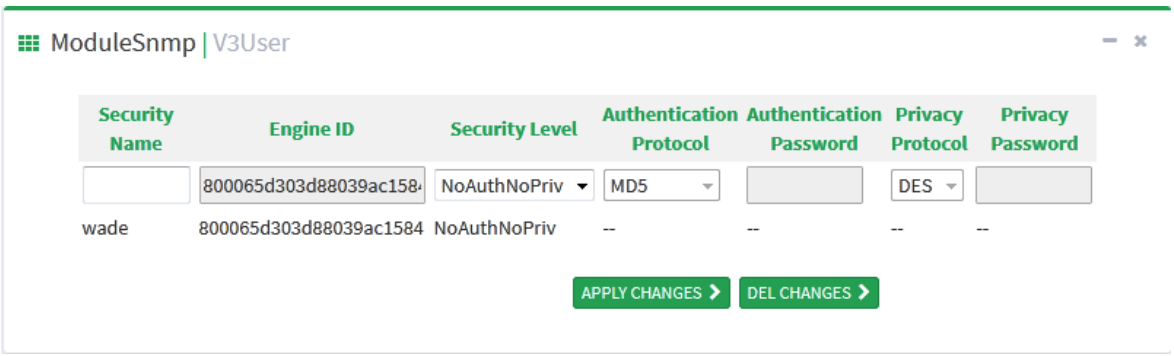


Рис. 76. Настройка таблицы пользователей SNMPv3

Имя безопасного пользователя (Security Name)

Диапазон настроек: 1~32 символов

Функция: создание имени пользователя.

Идентификатор ядра (Engine ID)

Диапазон конфигурации: четное количество шестнадцатиричных чисел, которое не может быть полным 0 или полным F; четное количество значений в диапазоне 10~64.

Функция: настройка идентификатора ядра в Trap-сообщении SNMPv3.

Уровень безопасности (Security Level)

Опции: NoAuthNoPriv /AuthNoPriv / AuthPriv

Функция: настройка уровня безопасности для текущего пользователя.

Описание: в режиме NoAuthNoPriv нет аутентификации и конфиденциальности. В режиме AuthNoPriv требуется аутентификация, но отсутствует конфиденциальность. В режиме AuthPriv требуется аутентификация и конфиденциальность.

Протокол аутентификации (Authentication Protocol)

Опции: MD5/SHA

Функция: выбор протокола аутентификации. Необходимо выполнить настройки протокола аутентификации и пароля, когда для уровня защиты выбраны режимы AuthNoPriv/AuthPriv.

Пароль аутентификации (Authentication password)
Диапазон настроек: 8~40 символов (протокол MD5), 8~32 символов (протокол SHA)
Функция: создание пароля.
Протокол конфиденциальности (Privacy Protocol)
Опции: DES/AES
Функция: Выбор протокола конфиденциальности. Необходимо выполнить настройки протокола конфиденциальности и пароля, когда выбран режим AuthPriv.
Пароль конфиденциальности (Privacy Password)
Диапазон настроек: 8~32 символов
Функция: создание пароля конфиденциальности. Можно настроить до 16 пользователей.

4. Настройте групповую таблицу, как показано ниже:

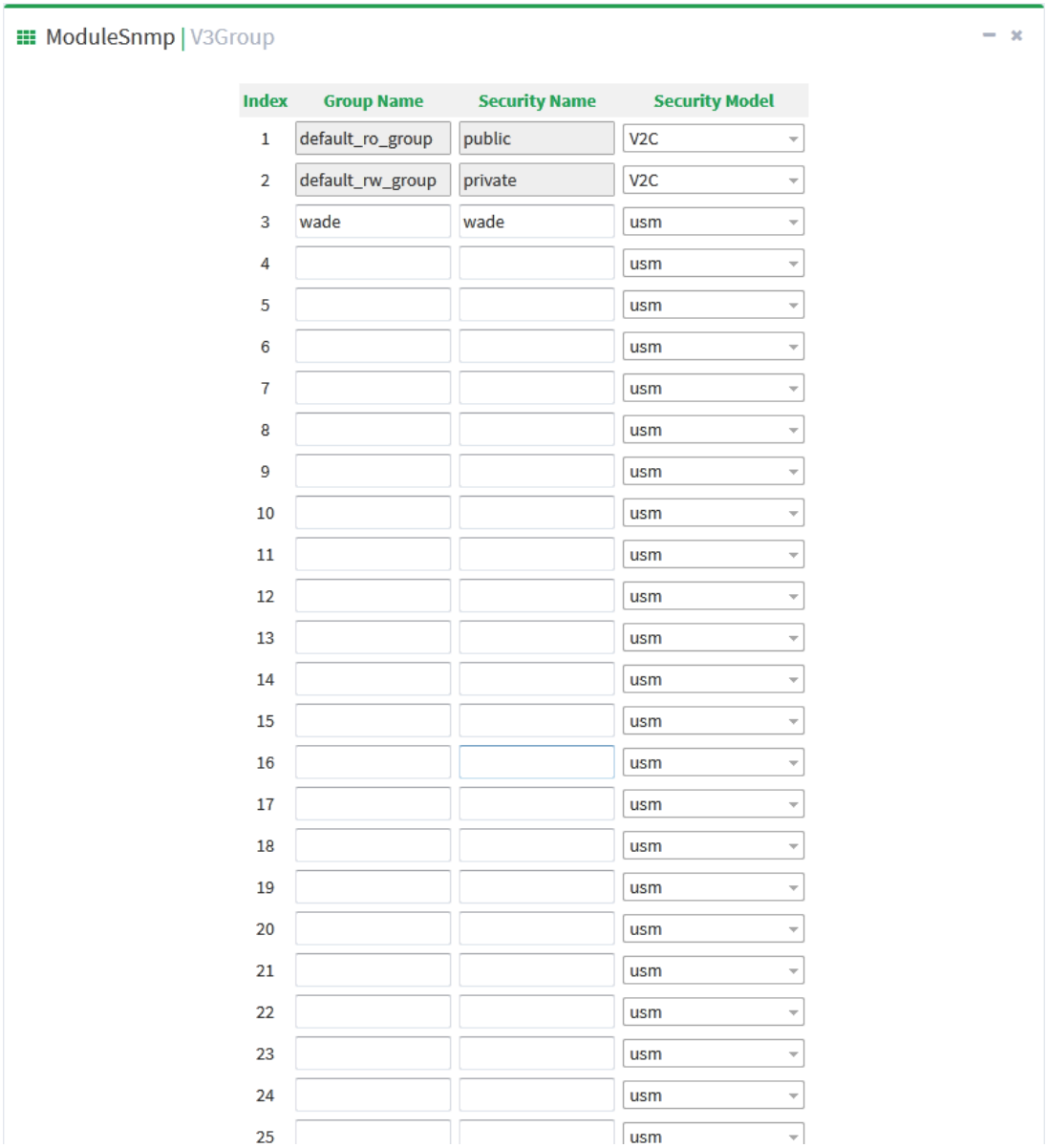


Рис. 77. Настройка групповой таблицы SNMPv3

Имя группы (Group Name)

Диапазон настроек: 1~32 символов

Функция: настройка имени группы. Пользователи с одним и тем же именем группы принадлежат к одной и той же группе.

Имя безопасного пользователя (Security Name)

Диапазон настроек: 1~32 символов

Функция: настройка имени безопасного пользователя. Имя безопасного пользователя должно соответствовать имени пользователя в таблице пользователей. Пользователи с одним и тем же именем группы принадлежат к одной и той же группе. Можно настроить до 32 групп.

Модель безопасности (Security model)

Настройки по умолчанию: SNMPv3

Функция: Выбор модели безопасности для текущей группы (номер версии SNMP). Протокол SNMPv3 использует технологию USM, что является обязательным для реализации модели SNMPv3.

5. Настройте таблицу отображения, как показано на рисунке ниже:

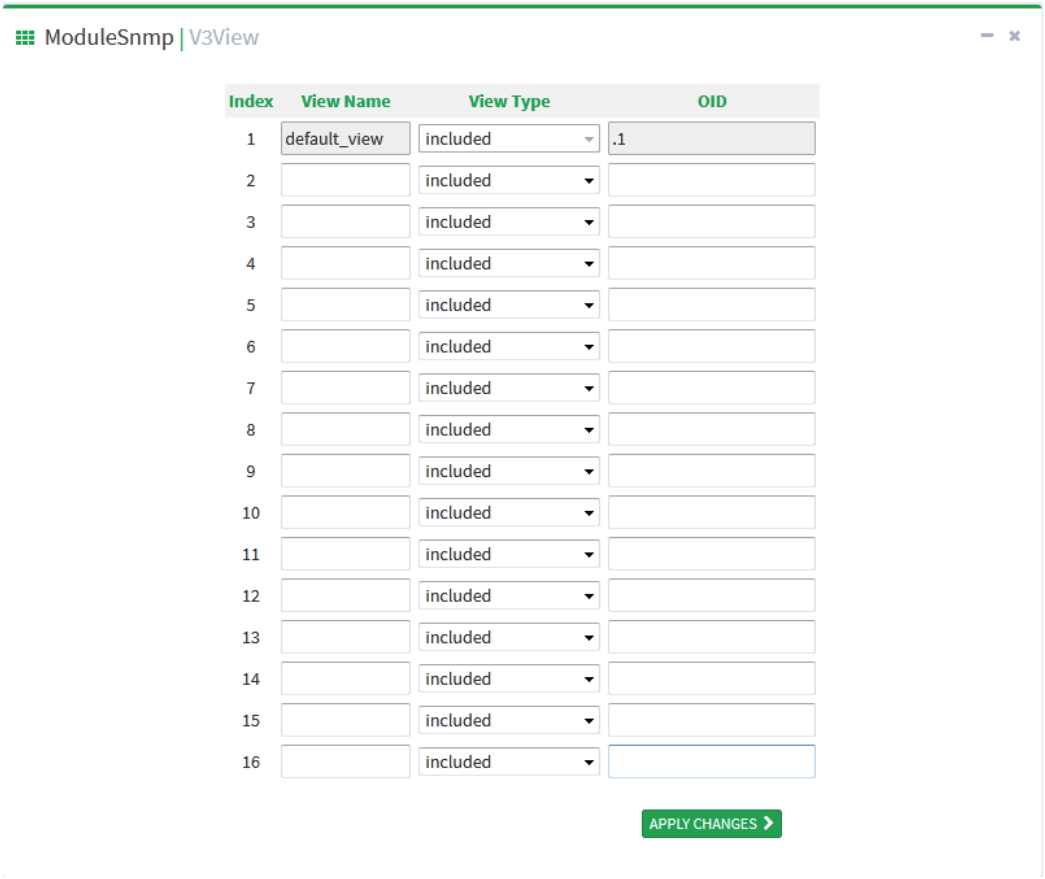


Рис. 78. Настройка таблицы отображения SNMPv3

Просмотр имени (View Name)
Диапазон настройки: 1~32 символов
Функция: настройка отображения имени.

Тип отображения (View Type)
Опции: Included/Excluded (добавлен/исключен)
Функция: опция Included обеспечивает отображение всех узлов поддерева MIB. Опция Excluded не отображает никакой из узлов поддерева MIB.
Идентификатор объекта (OID)
Функция: настройка поддерева MIB, представленного идентификатором объекта корневого узла. Можно настроить до 16 вариантов.

Таблица отображений по умолчанию default_view включает все узлы 1 поддерева на коммутаторе.

6. Настройте таблицу доступа, как показано на рисунке ниже:

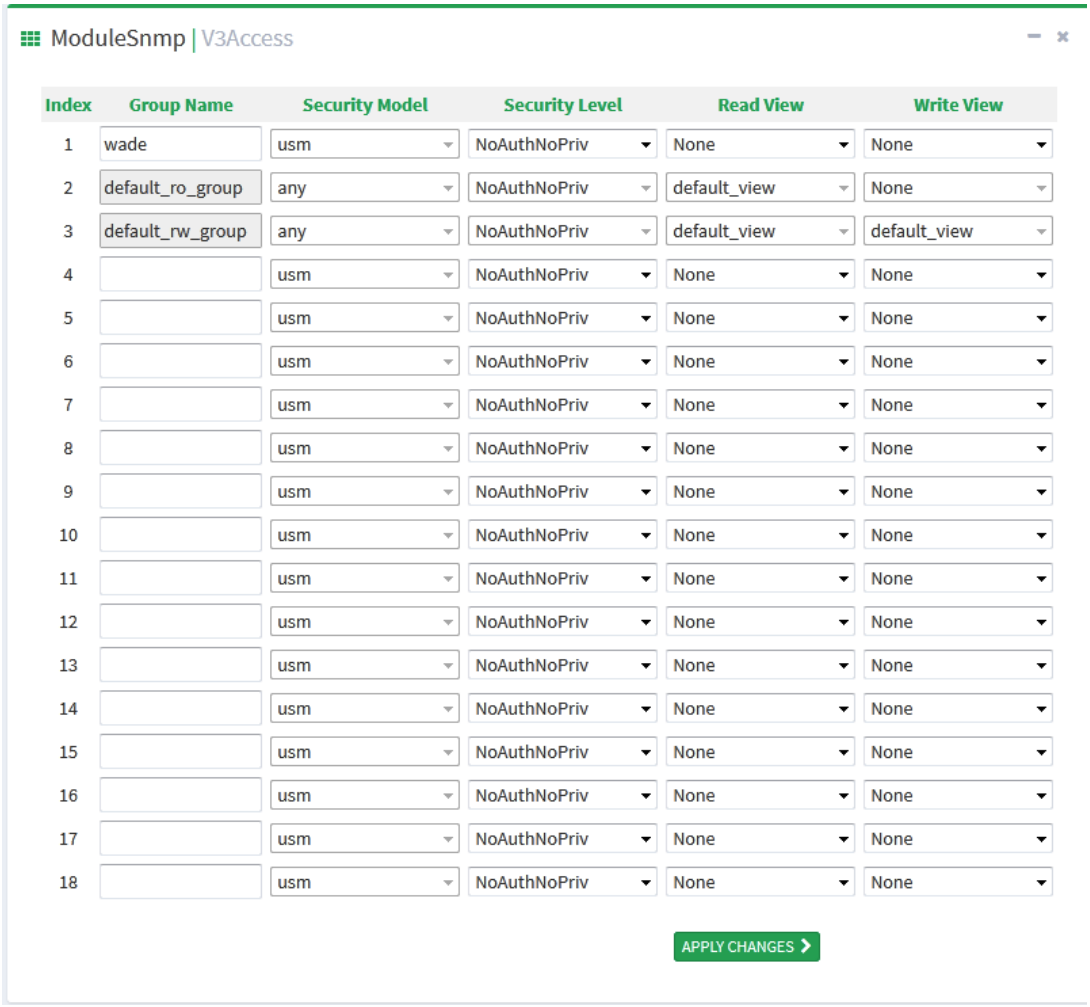


Рис. 79. Настройка таблицы доступа SNMPv3

Имя группы (Group Name)
Диапазон настроек: 1~32 символов
Описание: все пользователи группы обладают одинаковыми полномочиями доступа.

Модель защиты (Security model)
Настройки по умолчанию: any/v1/v2/usm
Функция: выбор модели защиты, которая используется, когда текущий групповой доступ к коммутатору SNMPv3 поддерживает технологию USM. Это означает, что применяться может любая модель защиты. Имя группы и модель защиты должны соответствовать имени группы и модели защиты в групповой таблице.
Уровень безопасности (Security Level)
Опции: NoAuthNoPriv/AuthNoPriv/AuthPriv
Функция: настройка уровня безопасности для текущей группы.
Описание: На уровне NoAuthNoPriv не используются ни протокол аутентификации, ни протокол конфиденциальности. На уровне AuthNoPriv требуется протокол

аутентификации без протокола конфиденциальности. На уровне AuthPriv требуется как протокол аутентификации, так и протокол конфиденциальности. Если необходимо обеспечить шифрование данных, то протокол аутентификации/конфиденциальности и пароль для аутентификации/конфиденциальности на стороне NMS должны соответствовать настройкам в таблице пользователей, чтобы успешно получить доступ к соответствующим данным о коммутаторе.

Уровни безопасности NoAuthNoPriv, AuthNoPriv, AuthPriv возрастают в соответствующем порядке. Высокому уровню безопасности разрешается доступ к низкому уровню безопасности. Например, если уровень безопасности группы установлен как AuthNoPriv, пользователи в группе с уровнями защиты AuthNoPriv и AuthPriv могут успешно получить доступ к коммутатору, если оба протокола аутентификации/конфиденциальности и пароли для аутентификации/защиты конфиденциальности соответствуют правилам. При этом пользователи с уровнями безопасности NoAuth, NoPriv доступа не имеют.

Приоритет доступа «Только чтение» (Read View)

Опции: default_view/None/Created view name

Функция: выбор имени отображения для приоритета доступа «Только чтение» (ReadOnly).

Приоритет доступа «Чтение-Запись» (Write View)

Опции конфигурации: default_view/None/Created view name

Функция: выбор имени отображения для приоритета доступа «Чтение-запись» (ReadWrite). Можно настроить до 16 таблиц доступа.

Таблицы доступа по умолчанию на коммутаторе {default_ro_group, any, NoAuth, NoPriv, default_view, None}, {default_rw_group, any, NoAuth, NoPriv, default_view, default_view}.

8.8.4. Пример типовой настройки

Станция управления SNMP подключена к коммутатору через сеть Ethernet. IP-адрес станции управления - 192.168.1.23. IP-адреса коммутатора - 192.168.1.2. Пользователь 1111 и пользователь 2222 управляют Агентом через протокол SNMPv3. Уровень защиты – «authnopriv». Информация о всех узлах, хранящаяся у Агента, доступна только для чтения. Агент активно отсылает trap-сообщение v3 в сеть NMS, когда у Агента происходит аварийная ситуация, как показано на рисунке ниже.

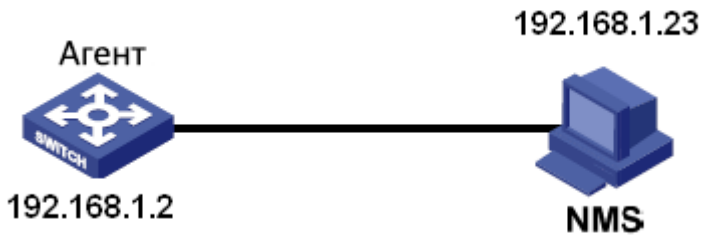


Рис. 80. Пример настройки SNMPv3

Настройте Агента, как показано ниже:

1. Включите протокол SNMP. См. рисунок 70.
2. Настройте таблицу пользователей SNMP v3.

Имя пользователя: 1111. Уровень защиты: Auth, Priv. Протокол аутентификации: MD5. Пароль аутентификации: aaaaaaaa. Протокол конфиденциальности: DES. Пароль конфиденциальности: xxxxxxxx.
Имя пользователя: 2222. Уровень защиты: Auth, Priv. Протокол аутентификации: SHA. Пароль аутентификации: bbbbbbbb. Протокол конфиденциальности: AES. Пароль конфиденциальности: yyyyyyyy. См. рисунок 76.

3. Создайте группу, модель безопасности: usm, включите пользователей 1111 и 2222. См. рисунок 77.
4. Настройте таблицу доступа SNMPv3

Имя группы: group, модель безопасности: USM, уровень защиты: Auth, NoPriv, имя режима «Read View»: default_view, имя режима «Write View»: None. См. рисунок 78;

5. Включите модель trap-сообщений. См. рисунок 75;
6. Создайте элемент таблицы trap 222 и включите модель trap. Установите версию SNMPv3, IP-адрес пункта назначения - 192.168.1.23. Выберете trap событие для всех событий системы, интерфейса, протокола аутентификации и коммутатора. Другие настройки используются по умолчанию.

Чтобы отследить и управлять статусом Агента, необходимо запустить соответствующее ПО управления системы NMS.

8.9. Файл-сервер (File Server)

Служба передачи файлов может создавать резервные копии данных файлов у клиента и на сервере. Если данные файла у клиента (сервера) меняются, резервная копия файла может быть получена с сервера (клиента) путем передачи файлов на основе протокола FTP/SFTP.
Допускается использовать коммутатор в качестве клиента или сервера для выгрузки и загрузки файлов по протоколу FTP/SFTP.

8.9.1. Описание

Переключитесь как FTP клиент. Сначала установите FTP-сервер. В нашем примере мы покажем процесс загрузки и выгрузки конфигурационных файлов на/с FTP-сервер с помощью программы WFTPD.

1. Выберете [Security]→ [users/rights] (пользователи/права). Нажмите на клавишу <New User> (Новый пользователь) и добавьте нового пользователя FTP, как показано на рисунке ниже. Введите имя пользователя и пароль. Например, имя пользователя: admin, пароль: 123. Нажмите <OK>.

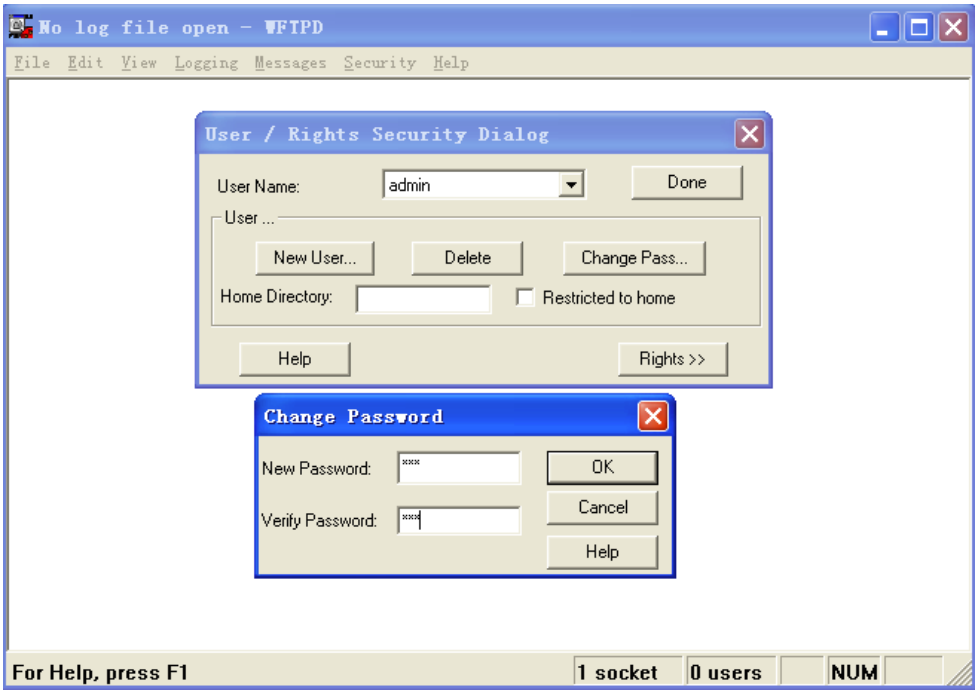


Рис. 81. Добавление нового пользователя FTP

2. Введите путь хранения файла версии программного на сервере в строке Home Directory, как показано на рисунке ниже. Нажмите <Done>.

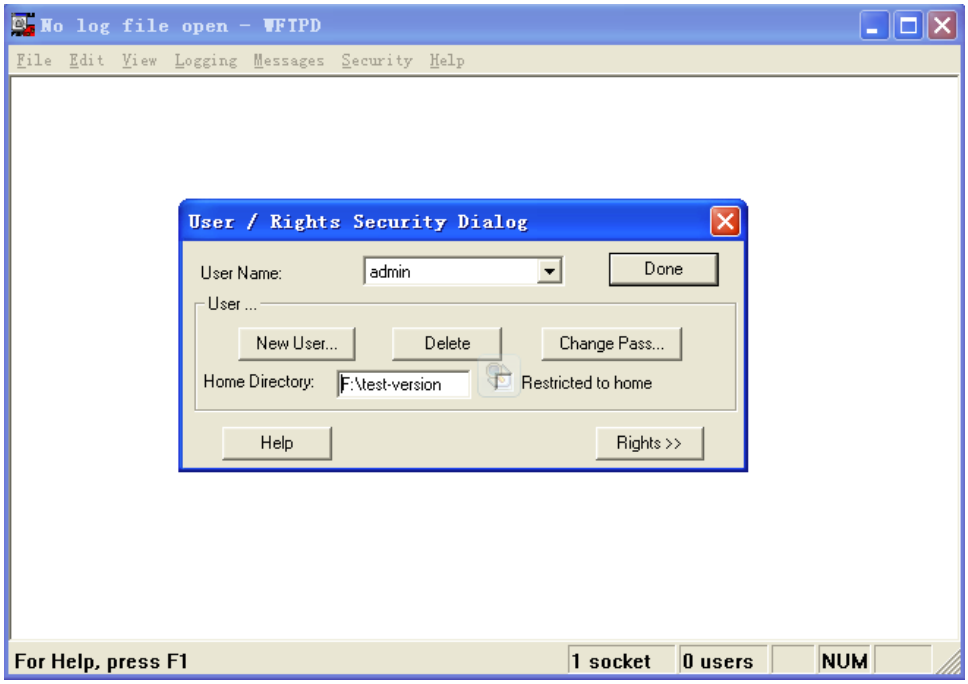


Рис. 82. Выбор месторасположение файла

3. Откройте дерево навигации [Other Configurations]→[File server]. Войдите на страницу конфигурации сервиса передачи данных, как показано на рисунке ниже:

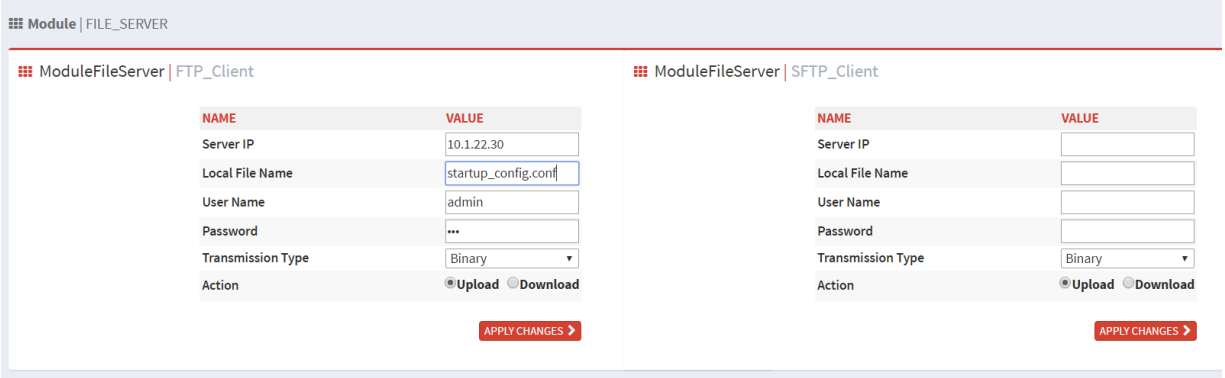


Рис. 83. Настройка сервиса передачи данных

Вы можете выполнить настройки элементов протоколов FTP или SFTP. Ниже представлены элементы конфигурации FTP на клиенте;

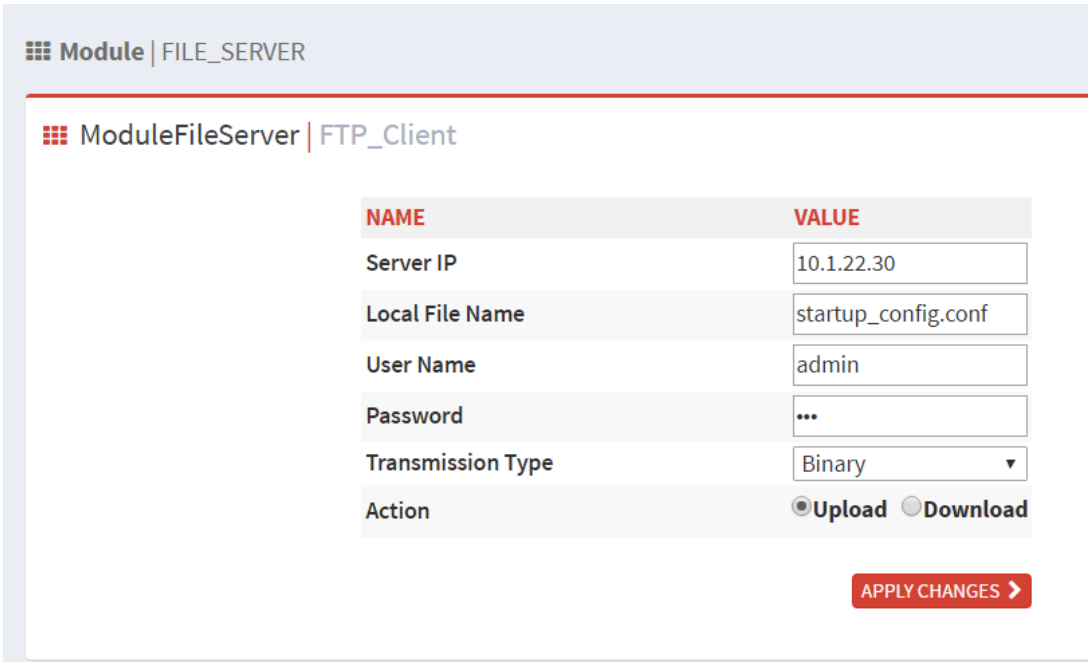


Рис. 84. Настройка FTP

IP-адрес сервера (Server IP)
Формат: A.B.C.D
Описание: ввод IP-адреса сервера.
Имя файла сервера (Server File Name)
Диапазон настроек: 1~100 символов
Описание: имя файла на сервере.
Имя пользователя (User Name)
Описание: имя пользователя на сервере/

Пароль (Password)
Описание: пароль пользователя
Тип передачи данных (Transmission Type)

Опции: binary/ascii
Настройки по умолчанию: binary
Функция: выбор стандарта передачи файлов.
Описание: ASCII – передача данных по стандарту ASCII. Binary – передача данных по стандарту двоичной передачи.
Действие (Action)
Опции: Upload/Download (загрузить/скачать)
Функция: Upload - загрузка конфигурационного файла коммутатора в каталог удаленного FTP-сервера. Download – скачивание конфигурационного файла с удаленного FTP-сервера на коммутатор.

8.9.2. SFTP

SFTP (Secure File Transfer Protocol) – это протокол передачи данных с поддержкой SSH, что обеспечивает шифрование файла и безопасность передачи.
Переключитесь как SFTP клиент. Сначала установите SFTP-сервер. В нашем примере мы покажем процесс загрузки и выгрузки конфигурационных файлов на/с SFTP-сервер с помощью программы WFTPD.

1. Добавьте пользователя SFTP, как показано на рисунке ниже. Введите имя пользователя и пароль. Например, пользователь: admin, пароль: 123. Номер порта – номер порта 22 протокола SFTP. Введите путь хранения версии ПО сервера в строке Root path. Нажмите <Start>.

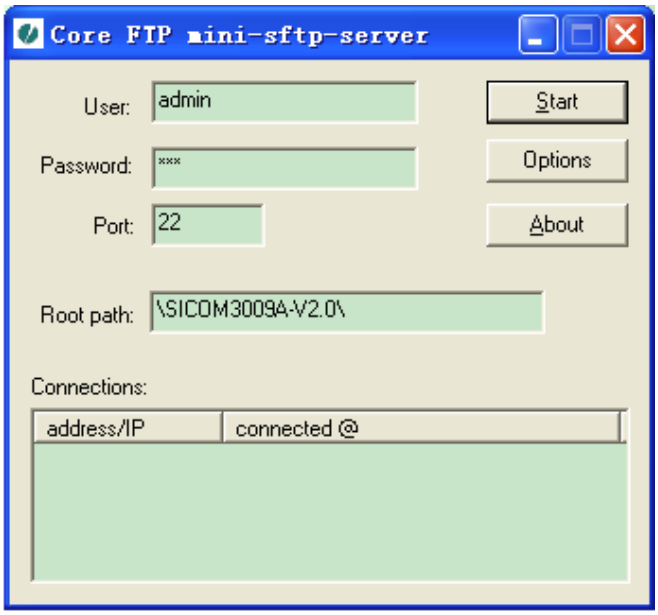


Рис. 85. Добавление нового пользователя SFTP

2. Откройте дерево навигации [Other Configurations]→ [File Server] и войдите на страницу настройки сервиса передачи данных, как показано на рисунке ниже:

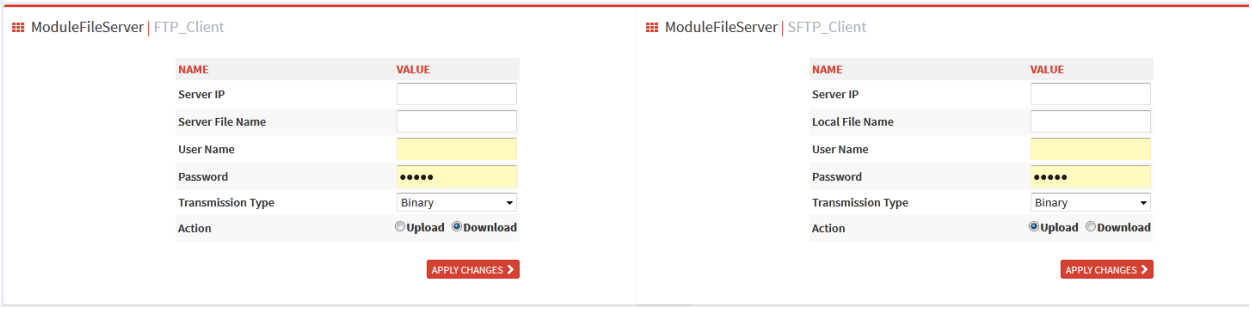


Рис. 86. Добавление нового пользователя SFTP

Вы можете настроить элементы протокола FTP или SFTP. Ниже показаны элементы настройки SFTP в меню клиента.

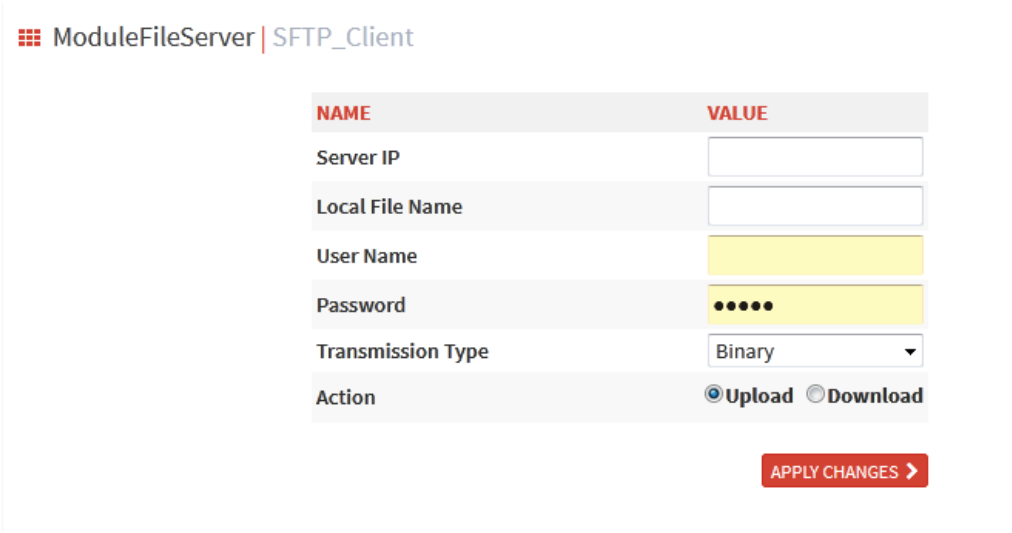


Рис. 87. Добавление нового пользователя SFTP

IP-адрес сервера (Server IP)
Формат: A.B.C.D
Описание: ввод IP-адреса сервера.
Локалное имя файла (Local File Name)
Диапазон настроек: 1~100 символов
Описание: имя файла в коммутаторе.
Имя пользователя (User Name)
Описание: имя пользователя, соответствующее SFTP-серверу.
Пароль (Password)
Описание: пароль пользователя
Тип передачи данных (Transmission Type)
Опции: binary/ascii
Настройки по умолчанию: binary
Функция: выбор стандарта передачи файлов.
Описание: ASCII – передача данных по стандарту ASCII. Binary – передача данных по стандарту двоичной передачи.
Действие (Action)
Опции: Upload/Download (загрузить/скачать)

Функция: Upload - загрузка конфигурационного файла коммутатора в каталог удаленного SFTP-сервера. Download – скачивание конфигурационного файла с удаленного SFTP-сервера на коммутатор.

8.10. Протокол LLDP

8.10.1. Вступление

Протокол Link Layer Discovery Protocol (LLDP) предоставляет собой стандартный механизм обнаружения канального уровня (2-го уровня). Он инкапсулирует различную информацию, например, возможности устройства, адрес, идентификатор устройства и интерфейса, в пакет Link Layer Discovery Protocol Data Unit (LLDPDU, блок данных протокола обнаружения уровня канала), и передаёт LLDPDU своим непосредственно подключённым соседям. При получении LLDPDU, соседи сохраняют эту информацию в MIB для предоставления NMS данной информации, а также информации о состоянии соединения между устройствами.

8.10.2. Настройка LLDP с помощью WEB-интерфейса

1. Настройка LLDP.

Откройте дерево навигации [Other Configurations)→[LLDP] и войдите на страницу настроек протокола LLDP, как показано на рисунке ниже:

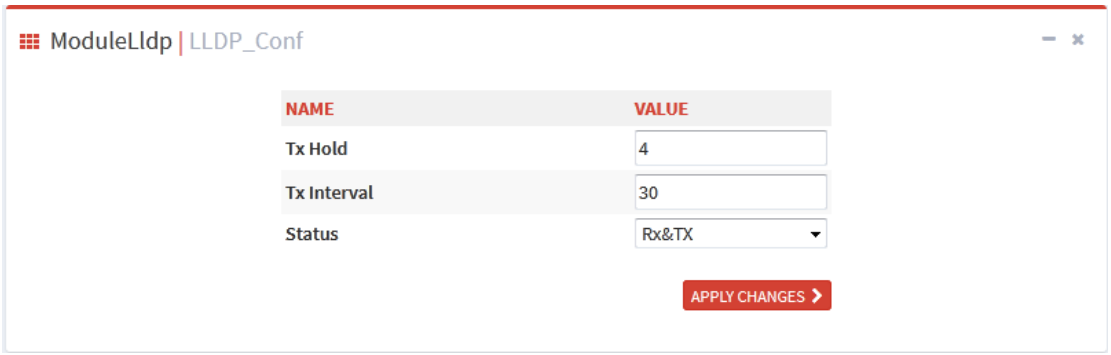


Рис. 88. Настройка LLDP

Удержание Tx (Tx Hold)
Диапазон настроек: 2~10 times (раз)
Настройки по умолчанию: 4 times (раза)
Функция: Настройка количества Tx Hold. Время действия сообщения LLDP = Tx interval × Tx hold.
Интервал Tx (Tx Interval)
Диапазон настроек: 5~32768 сек.
Настройки по умолчанию: 30 сек.
Функция: Настройка временного интервала для периодичности отсылки LLDP сообщений.
Статус (Status)
Опции: Rx&Tx/Disable/RxOnly/TxOnly
Настройки по умолчанию: Rx&Tx

Функция: Настройка статуса LLDP сообщения. Опция Rx&Tx означает, что коммутатор не только отправляет LLDP сообщения, но также принимает и распознает LLDP сообщения. Disable означает, что коммутатор не отправляет и не принимает LLDP сообщения. При выбранной опции RxOnly коммутатор только принимает и распознает LLDP сообщения, но не отсылает LLDP сообщения. С опцией TxOnly коммутатор только отправляет LLDP сообщения и не принимает их.

2. Просмотр информации о LLDP:

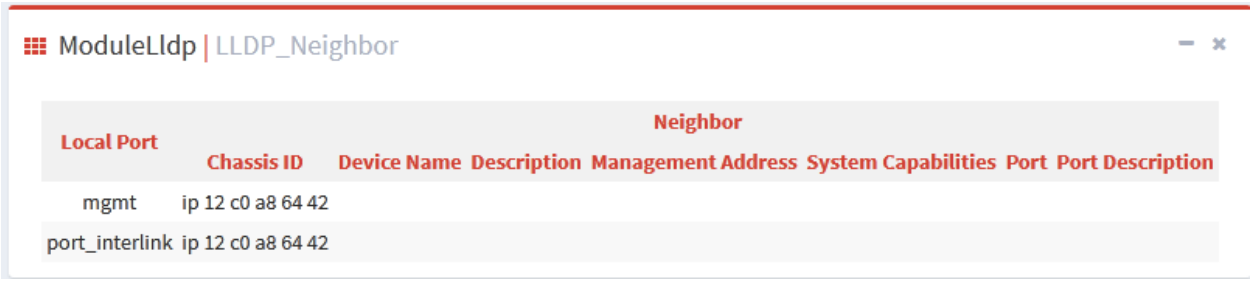


Рис. 89. Просмотр информации о LLDP

8.11. Функция DDMI

Цифровой мониторинг интерфейса трансивера SFP способен отслеживать температуру модуля, напряжение питания, ток смещения лазера, а также передавать и принимать оптическую мощность в режиме реального времени. Эти параметры помогают системе выявлять местонахождение неисправности в волоконно-оптическом канале, упрощать сервисное обслуживание и повышать уровень надежности системы.

8.11.1. Настройка с помощью WEB-интерфейса

Откройте дерево навигации [Other Configurations]→[Ddmi] и войдите на страницу конфигурации модуля DDMI, как показано на рисунке ниже:

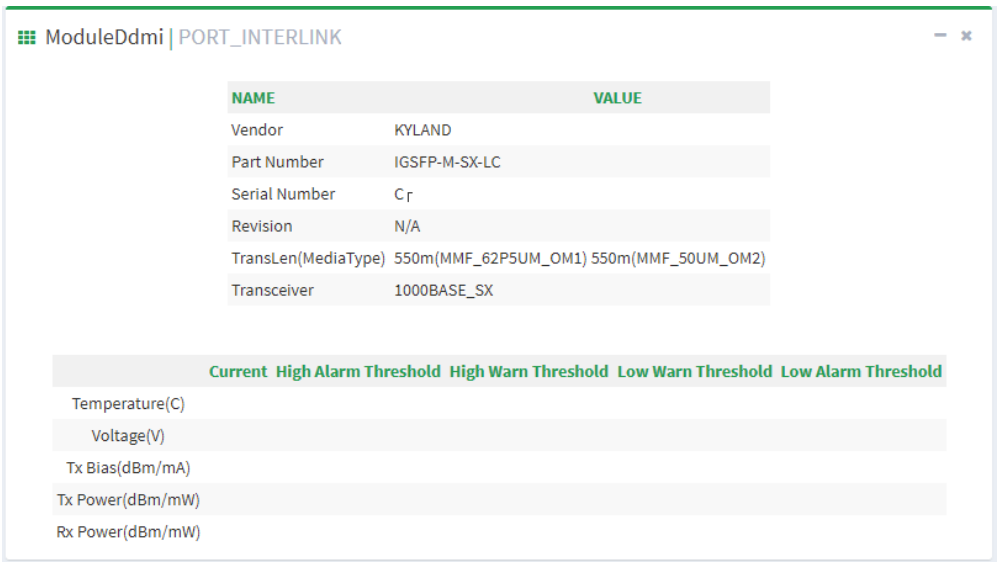


Рис. 90. Информация об оптическом модуле порта L

Порт L приведен в качестве примера. После установки трансивера SFP мы можем прочесть о нем основные сведения. Данные сведения включают такую информацию, как сведения о производителе, артикул, заводской номер, версия, дальность передачи. Некоторые трансиверы поддерживают расширенные информационные запросы, включая запросы информации о температуре, напряжении, мощности Tx и мощности Rx.

8.12. Виртуальная диагностика кабеля (Virtual Cable Test)

8.12.1. Введение

VCT (Виртуальный тестер кабеля) использует технологию рефлектометрии промежутков времени (TDR) для определения состояния кабеля витой пары. Система передает импульсный сигнал по кабелю и обнаруживает отраженный импульсный сигнал, чтобы определить неисправность кабеля. Если у кабеля обнаруживается аварийное состояние, часть или вся энергия импульса отражается обратно к источнику передачи. Когда передаваемый импульсный сигнал достигает конца кабеля или точки неисправности, VCT может измерить время прибытия сигнала в точку неисправности и время возврата к источнику передачи, а затем он производит расчет расстояния согласно времени.
VCT может обнаруживать следующие типы неисправностей кабелей:
Short: означает короткое замыкание. Когда два или более проводов закорочены.
Open: означает обрыв в цепи. В кабеле могут быть оборванные провода.
Normal: означает исправное состояние кабеля.
Imped: это означает несоответствие импеданса. Например, импеданс кабеля категории 5 составляет 100 Ом, полное сопротивление терминаторов на обоих концах кабеля должно быть 100 Ом, чтобы избежать отражения волн и ошибок данных.
Fail: означает ошибку тестирования VCT.

8.12.2. Настройка через WEB-интерфейс

Откройте дерево навигации [Other Configurations]→[Virtual Cable Test] и войдите на страницу конфигурации VCT, как показано на рисунке ниже:

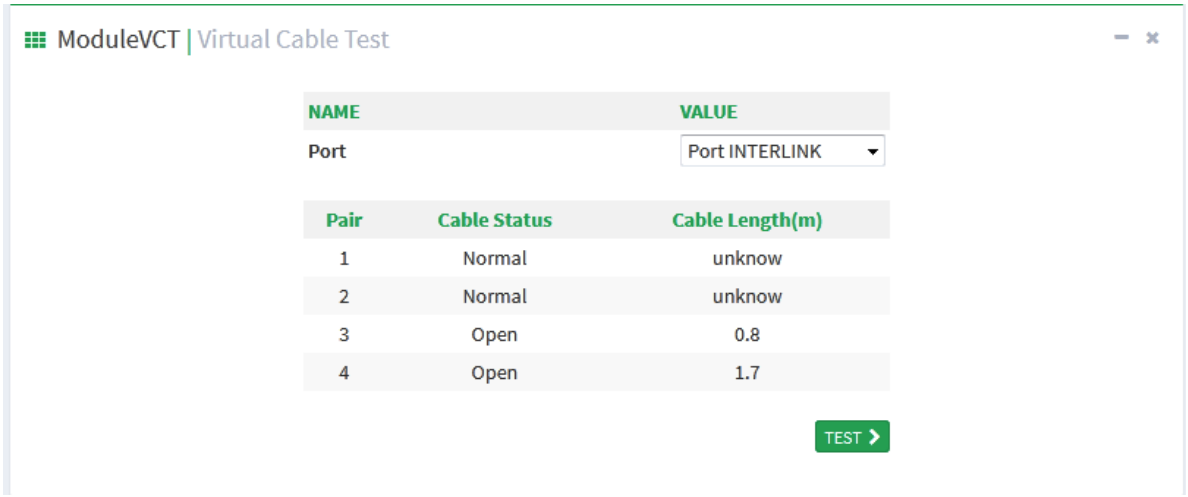


Рис. 91. Страница настройки VCT

Порт (Port)
Опции: port_a /port_b / port_interlink
Настройки по умолчанию: port_a
Функция: выбор соответствующего порта для тестирования кабеля. Выбрав порт, нажмите на кнопку [TEST] для соединения с тестируемым кабелем, как показано выше.
Пара (Pair)
Описание: количество пар кабелей. Парой считаются два медных провода.
Статус кабеля (Cable Status)
Описание: существуют три статуса – Normal /Open / Short.
Normal: нормальное соединение
Open: в кабеле могут быть обрывы.
Short: между двумя или более проводами есть короткое замыкание.
Длина кабеля (м) (Cable Length(m))
Описание: приблизительное расстояние от точки неисправности до порта коммутатора, измеряется в метрах. Если кабель исправен, длина кабеля отображается в статусе Unknown (Неизвестно).

8.13. Протокол RADIUS

8.13.1. Введение

RADIUS (Служба удаленной аутентификации пользователей) является распространенным протоколом передачи данных. Он определяет формат RADIUS кадра на основе UDP и механизм передачи данных, гарантируя защиту сетей от несанкционированного доступа. Как правило, RADIUS используется в сетях с высокими требованиями безопасности и удаленным доступом пользователей.
RADIUS поддерживает режим клиент/сервер, обеспечивая соединение между NAS (Сервером сетевого доступа) и RADIUS сервером. RADIUS клиент работает на NAS сервере. RADIUS сервер осуществляет централизованное управление информацией о пользователе. NAS сервер выполняет функции сервера для пользователей и функции клиента для RADIUS сервер. На Рисунке 92 показана структура.

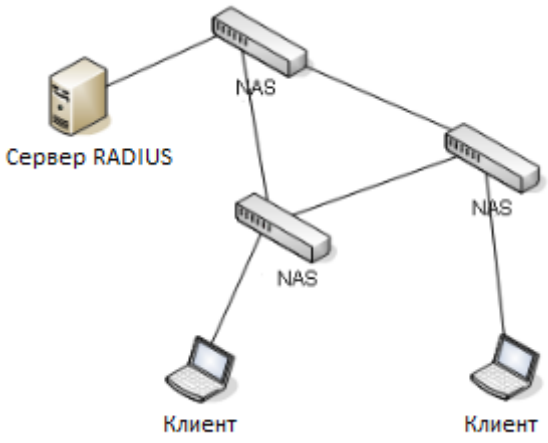


Рис. 92. Структура RADIUS

Протокол проводит аутентификацию конечных пользователей, которым необходимо авторизоваться в системе устройства для работы. Действуя как RADIUS клиент, устройство отправляет информацию о пользователе на RADIUS сервер для аутентификации и разрешает или запрещает пользователям войти в систему устройства по результатам процесса аутентификации.

8.13.2. Настройка через Web-интерфейс

1. Настройка параметров аутентификации RADIUS:

Откройте дерево навигации [Other Configurations]→[Radius] и войдите на страницу конфигурации RAIDUS, как показано на рисунке ниже:

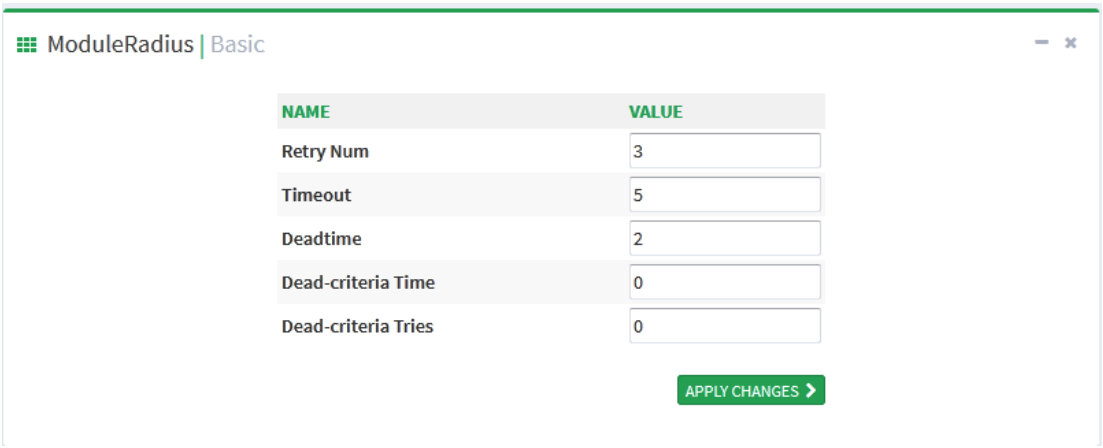


Рис. 93. Настройка параметров аутентификации RADIUS

Количество попыток (Retry Num)

Настраиваемый диапазон: 1~3

Настройки по умолчанию: 3

Функция: настройка количества попыток соединения с RADIUS сервером при настройке тайм-аута сообщений. Если общее количество попыток превышает выставленное значение и RADIUS сервер по-прежнему не отвечает, устройство определит это как сбой аутентификации.

Тайм-аут (Timeout)

Настраиваемый диапазон: 1~3 сек.

Настройки по умолчанию: 3 сек.

Функция: Настройка времени ожидания ответа от RADIUS сервера. Устройство отправляет запрос RADIUS серверу и, если RADIUS сервер не отвечает на протяжении этого времени, запрос отправляется снова.

Нерабочее время (Deadtime)

Настраиваемый диапазон: <1-1440>

Настройки по умолчанию: 2

Следует настроить сервер на закрытие в течение некоторого времени, если обнаружено, что Radius сервер не исправен. По истечении нерабочего времени Radius сервер

возвращается в рабочее состояние. Это позволяет снизить количество запросов, отправляемых на нерабочий сервер.

Время определения нерабочего состояния (Dead-criteria Time)

Настраиваемый диапазон: <3-120>

Настройки по умолчанию: 0

Функция: время ожидания в секундах.

Описание: Определение нерабочего состояния сервера с помощью настройки тайм-аута.

Количество запросов при нерабочем состоянии сервера (Dead-criteria Tries)

Настраиваемый диапазон: <1-100>

Настройки по умолчанию: 0

Функция: количество попыток

Описание: Определение нерабочего состояния сервера с помощью настройки предельного количества запросов.

2. Настройте RADIUS сервер, как показано ниже:

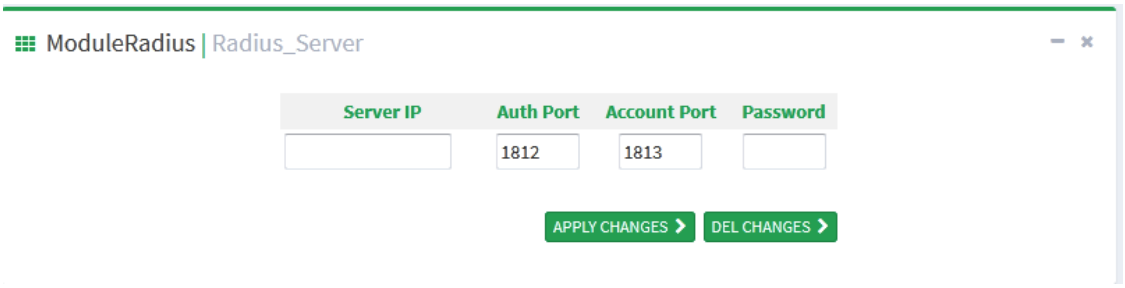


Рис. 94. Настройка RADIUS сервера

IP-адрес сервера (Server IP)

Формат: A.B.C.D

Функция: Настройка IP-адреса для RADIUS сервера. Можно настроить до 5 RADIUS серверов.

Порт аутентификации (Auth Port)

Настраиваемый диапазон: 1~65535

Настройки по умолчанию: 1812

Функция: Настройка номера UDP порта для RADIUS сервера.

Порт учетной записи (Account Port)

Настраиваемый диапазон: 1~65535

Настройки по умолчанию: 1813

Функция: Настройка номера UDP порта для RADIUS сервера.

Пароль (Password)

Настраиваемый диапазон: 1~32 символов

Функция: Настройка пароля для RADIUS сервера

8.13.3. Пример типовой настройки

1. Топология сети

Рис. 95. Типовая сеть

2. Требования к конфигурации
a. Вход пользователя в устройство управления по линии vty0 с помощью системы аутентификации AAA.
b. Аутентификация RADIUS и IP-адрес сервера учетной записи - 192.168.1.1, порт аутентификации - 1812, порт учетной записи - 1813, ключ аутентификации – test.
c. См. пример конфигурации веб-страницы в разделе 8.13.2.

8.14. Протокол TACACS+

8.14.1. Введение

Сеансовый протокол TACACS+ является приложением на основе протокола TCP. Он поддерживает режим клиент/сервер для реализации соединения между Сервером Сетевого Доступа (NAS) и TACACS+ сервером. Клиент работает на сервере NAS, а сервер осуществляет централизованное управление информацией о пользователе. NAS сервер служит сервером для пользователей и клиентом для сервера. На рисунке 96 показана структура.

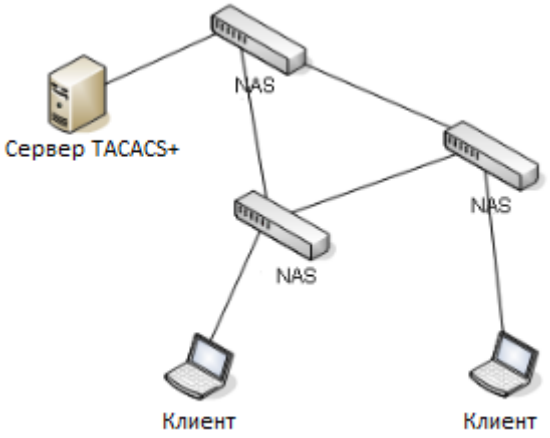


Рис. 96. Структура TACACS+

Протокол осуществляет аутентификацию, авторизацию и опрашивает конечных пользователей, которым необходимо войти в систему. Устройство пользователя действует как TACACS+ клиент и отправляет имя пользователя и пароль на TACACS+ сервер для аутентификации. Сервер получает TCP запросы о подключении от пользователей, отвечает на запросы об аутентификации и проверяет права пользователей. Если пользователь проходит процесс аутентификации, он получает доступ в систему для работы.

8.14.2. Настройка через WEB-интерфейс

1. Включение протокола TACACS+

Откройте дерево навигации [Other Configurations]→[Tacacs plus] и войдите на страницу конфигурации TACACS+, как показано на рисунке ниже:

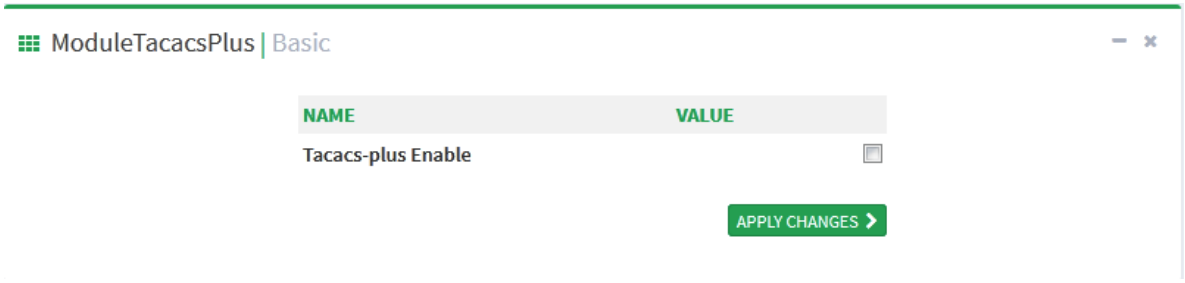


Рис. 97. Настройка протокола TACACS+

Включить TACACS+ (TACACS+ Enable)
Опции: Enable/Disable (включить/выключить)
Настройки по умолчанию: Disable (выключено)
Функция: включение или выключение протокола TACACS+ .

2. Настройте сервер TACACS+, как показано на рисунке ниже:

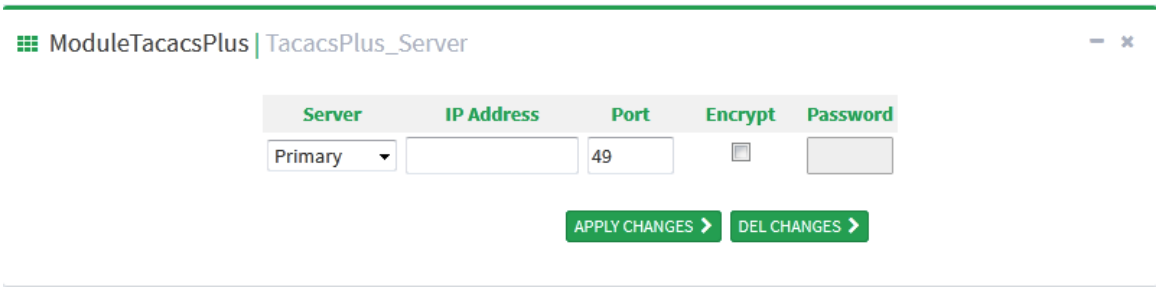


Рис. 98. Настройка сервера TACACS+

Настройка сервера (Server)
Опции: Master server / Slave server (Ведущий сервер / Ведомый сервер)
Настройки по умолчанию: Master server
Функция: выбор типа сервера для текущих настроек.
IP-адрес (IP address)
Формат: A.B.C.D
Функция: настройка IP-адреса сервера.

Порт (Port)
Диапазон настроек: 1~65535
Настройки по умолчанию: 49
Функции: настройка номера порта, принимающего запрос об аутентификации в системе NAS.
Шифрование (Encrypt)
Опции: Enable/disable (включить/выключить)
Настройки по умолчанию: Disable
Функция: включение или выключение функции шифрования. Если режим включен, потребуется ввести ключ шифрования.
Пароль (Password)
Диапазон настроек: 1~32 символов
Описание: настройка пароля (ключа) для повышения уровня безопасности соединения клиента с сервером TACACS+. Как клиент, так и сервер могут проверить легитимность сообщения, поделившись ключом устройства. Только когда ключ согласован, оба получают сообщение, отправленное другим устройством, и отвечают друг другу. Поэтому необходимо убедиться, что общий ключ, настроенный на устройстве, в точности совпадает с ключом на сервере TACACS+.
После завершения настройки информация о конфигурации сервера будет отображаться в списке серверов, как показано ниже:

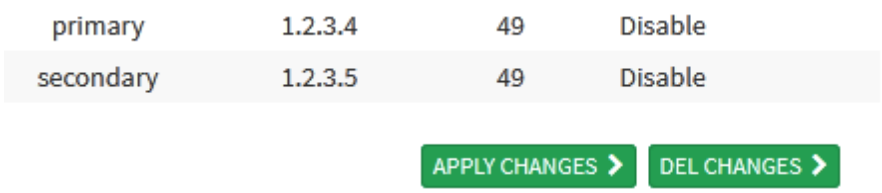


Рис. 99. Список серверов

8.14.3. Пример типовой настройки

Как показано на рисунке ниже, сервер TACACS+ выполняет аутентификацию и авторизацию пользователя через коммутатор. IP-адрес сервера - 192.168.0.23. Общий ключ – «ааа» при взаимодействии коммутатора с сервером посредством сообщений.

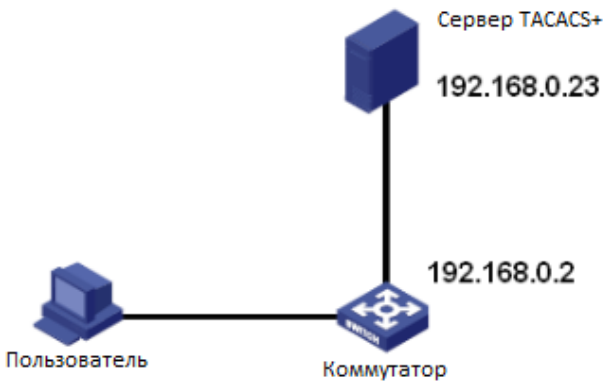


Рис. 100. Пример аутентификации TACACS+

См. настройки TACACS+ в разделе 8.14.2.

8.15. Протокол AAA

8.15.1. Введение

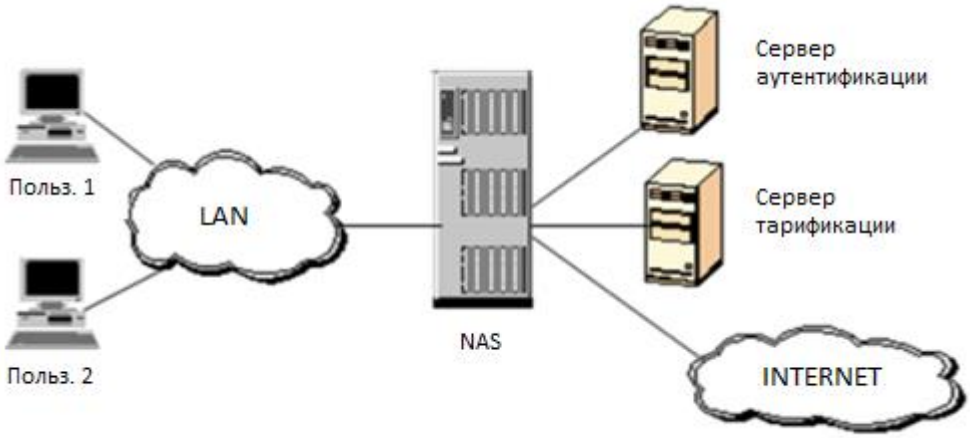


Рис. 101. Структура AAA

Чтобы повысить уровень безопасности сети, необходимо контролировать разрешение на использование ресурсов сети. Протокол AAA обеспечивает реализацию сервисов аутентификации, авторизации и учетных записей, что позволяет эффективно решать проблемы, связанные с безопасностью.

Сервисы AAA состоят из двух частей: модуля AAA для обработки запросов пользователей о получении доступа и модуля RADIUS, который поддерживает сервисы AAA и предоставляет услуги.

Платформа управления AAA взаимодействует непосредственно с пользователем, управляет сервисами AAA, необходимыми пользователю. Также платформа отсылает запросы пользователя конкретному AAA серверу (например, RADIUS).

Платформа управления AAA участвует в процессе обеспечения доступа системой AAA. Процесс аутентификации важен для подтверждения прав пользователей. Сервисы авторизации (опция) могут быть выполнены только после завершения процессов подтверждения прав доступа и аутентификации.

Именно сервер AAA предоставляет необходимую информацию о правах пользователей устройству системы NAS, чтобы пользователи могли успешно получить доступ к сети. Сервис учета (опция) регистрирует успешную аутентификацию пользователей или ведет учет трафика.

RADIUS клиент реализует обмен данными между пользователем системы AAA и RADIUS сервером. RADIUS клиент преобразовывает AAA запрос пользователя в протокольное RADIUS сообщение, которое отправляется на RADIUS сервер. RADIUS сервер, в свою очередь, отсылает результат запроса пользователя обратно RADIUS клиенту. RADIUS

клиент прорабатывает результат запроса и отправляет ответ на платформу управления AAA. В итоге пользователь получает ответ на свой запрос.

8.15.2. Настройка через Web-интерфейс

1. Включите протокол AAA

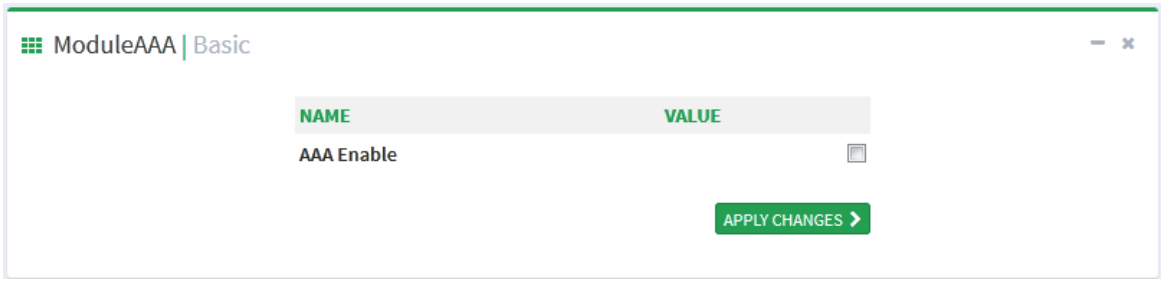


Рис. 102. Включение протокола AAA

Соответствующие сервисы AAA могут быть настроены только при глобальной активизации сервиса. При отключении сервиса AAA ранее используемые услуги будут отключены. Выполните настройки режима входа в систему для получения доступа к коммутатору, а также режима аутентификации.

2. Настройка аутентификации

Откройте дерево навигации [Other Configurations]→[AAA] и войдите на страницу настройки аутентификации, как показано на рисунке ниже:

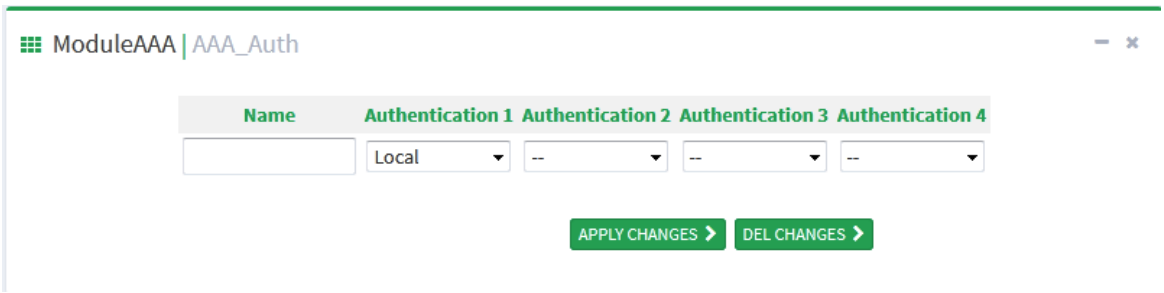


Рис. 103. Настройка аутентификации

Тип аутентификации (Authentication Name)
Опции: Telnet/Web/dot1x/SSH
Функция: выбор режима доступа к коммутатору.
Аутентификации 1-4 (Authentication 1 Authentication 2/Authentication 3/Authentication 4)
Опции: Local/Tacacs+/ Radius/None
Настройки по умолчанию: Local
Функция: выбор последовательности аутентификации. Сначала используется Authentication 1. В случае отказа выбирается Authentication 2. Если первые две аутентификации не прошли, используется Authentication 3. Если все предыдущие аутентификации завершились неудачно, используется режим аутентификации 4

Описание: Опция Local означает, что для аутентификации используются имя пользователя и пароль. Tacacs+ означает использование для аутентификации имени пользователя и пароля на сервере Tacacs+. Radius означает использование для аутентификации имени пользователя и пароля на сервере Radius.

8.16. Логический интерфейс LINE

8.16.1. Введение

LINE – это логический интерфейс терминального управления, который делится на два типа: «console» и «vty». Тип «console» соответствует входу через консоль, а тип «vty» соответствует общим протоколам входа в систему, включая telnet. Конфигурации типов LINE, в основном, одинаковые и поддерживаются без условия соблюдения особых инструкций.

8.16.2. Настройка через WEB-интерфейс

Откройте дерево навигации [Other Configurations]→[Line] и войдите на страницу настройки аутентификации при входе в систему, как показано на рисунке ниже:

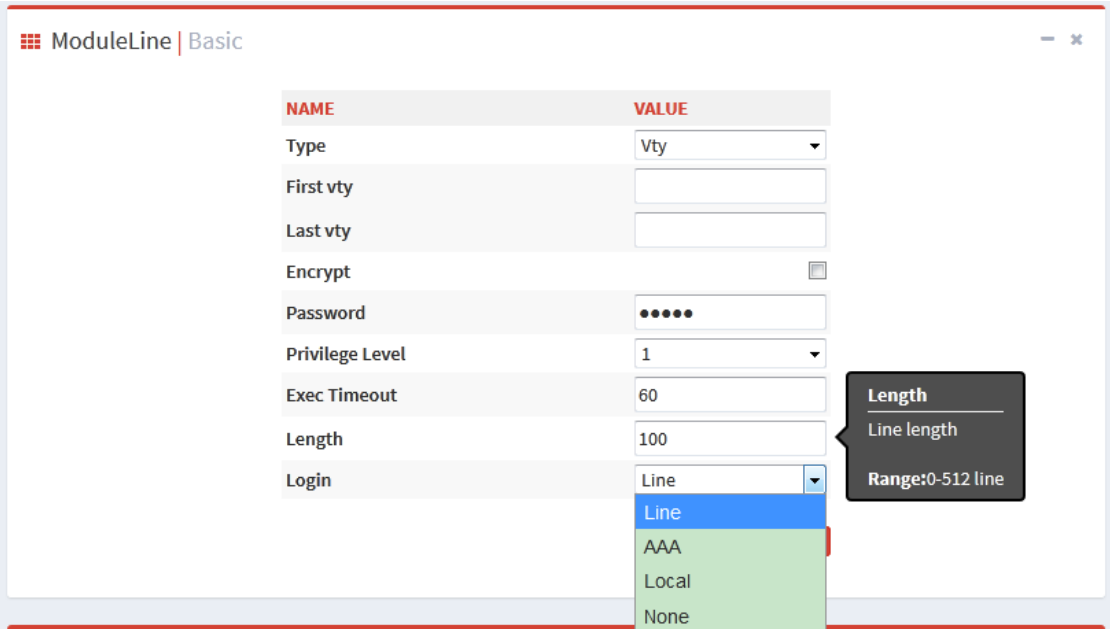


Рис. 104. Страница настройки LINE

Тип (Type)
Опции: console/vty
Функция: выбор режима входа в систему коммутатора удаленно.
Console: вход через консольный порт.
Vty соответствует базовым протоколам входа, включая протокол TELNET.
Идентификатор Vty (Vty Id)
Опции: 0-9
Настройки по умолчанию: 0

Функция:

1. Тип LINE - консоль, значение vty по умолчанию - 0, настройка на консольный порт.
2. Тип LINE - vty, необходимо настроить опции first-vty или last-vty.

first-vty: Идентификатор первой vty линии, диапазон: 0~9

last- vty: Идентификатор последней vty линии, диапазон: 0~9

При настройке только first-vty будет настроена только одна линия vty. При настройке last-vty будет настроена вся линия от first-vty до last-vty.

Шифрование (Encrypt)

Опции: Plaintext encryption/cipher text encryption (Простой текст/Зашифрованный текст)

Настройки по умолчанию: Plaintext encryption

Функция: пароль по умолчанию – admin. При снятом флажке используется простой текст. С поставленным флажком Encrypt используется зашифрованный текст. Инструмент частного алгоритма шифрования предназначен для генерации зашифрованного текста. Команда - rypt 7.

Пароль (Password)

Опции: Plaintext password / ciphertext password (Незашифрованный пароль / Зашифрованный пароль)

Длина незашифрованного пароля находится в диапазоне от 1 до 64 символов. Диапазон длины зашифрованного пароля: 1~129 символов.

Настройки по умолчанию: plaintext password with admin (незашифрованный пароль к имени admin)

Уровень привилегий (Privilege level)

Настраиваемый диапазон: 0~15

Настройки по умолчанию: 1

Функция: При настройке режима аутентификации LINE, разрешение на аутентификацию с помощью консоли/telnet контролируется разрешением LINE в определенном диапазоне.

Запрет таймаута (Exec timeout)

Настраиваемый диапазон: 0~86400 сек.

Настройки по умолчанию: 60 сек.

Функция: настройка времени таймаута неактивной сессии после входа пользователя на терминал. При установке функции в 0, таймаут отсутствует.

Длина (Length)

Опции: 0~512

Настройи по умолчанию: 100

Функция: настройка максимальное количество строк вывода на экране.

Авторизация (Login)

Опции: line/aaa/local/none

Line: для авторизации используются настройки аутентификации с паролем через интерфейс LINE.

AAA: для авторизации используются настройки аутентификации с именем пользователя и пароля через протокол AAA.

Local: для авторизации используются настройки аутентификации с именем пользователя и пароля через систему управления локальными пользователями.

None: без аутентификации.
Настройки по умолчанию: line
Функция: Установка режима аутентификации при входе в терминал.

9. Сервисное обслуживание

Откройте дерево навигации [Switch Maintenance] и выберете всплывающую опцию для продолжения работы.
Указанные ниже опции позволяют устройству сохранять настройки и восстанавливать заводские настройки по умолчанию.

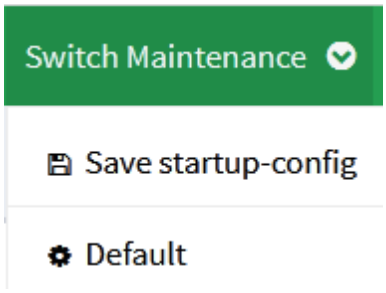


Рис. 105. Сохранение конфигурации запуска и восстановление настроек по умолчанию

10. Узлы в сети

Откройте дерево навигации [Network Nodes] для просмотра информации об узлах сети подключенных к устройству, как показано на рисунке ниже:

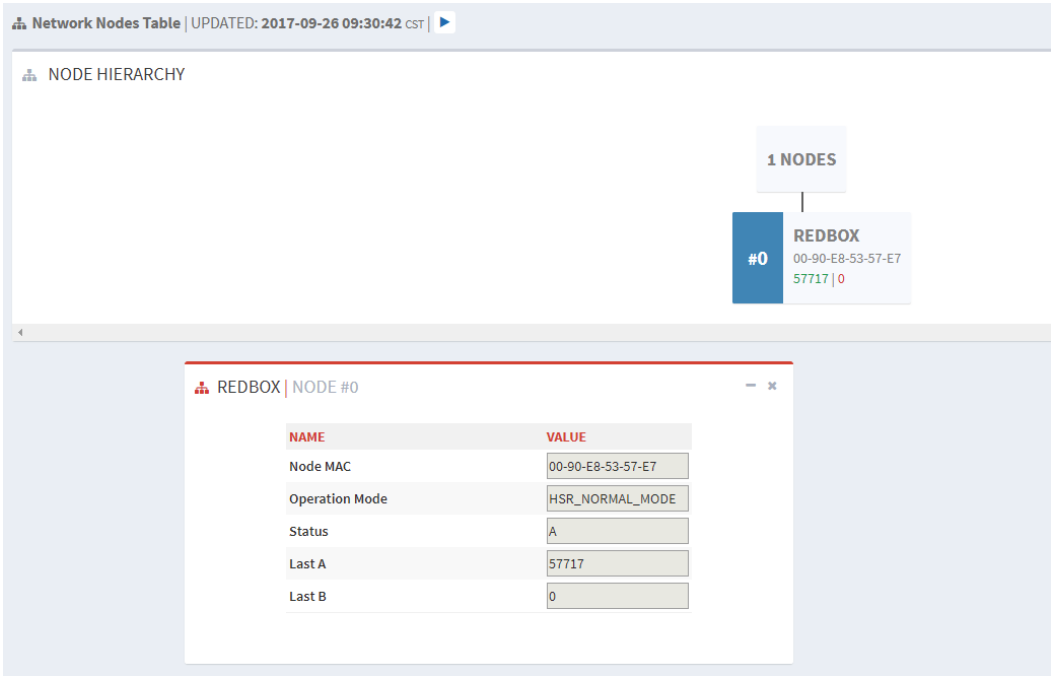


Рис. 106. Узлы в сети

На верхней диаграмме показана текущая ситуация в сети устройства. NODES - локальное устройство, REDBOX - удаленное устройство, подключение к локальному устройству через порт A. MAC-адрес удаленного устройства и статистику полученных и переданных сообщений порта можно увидеть из диаграммы.
«Сетевая ситуация» устройства более четко описана в таблице REDBOX ниже.

MAC-адрес узла (Node MAC)
Описание: MAC-адрес удаленного устройства.

Режим работы (Operation Mode)
Описание: Режим работы устройства.

Status (Статус)
Описание: интерфейс между удаленным устройством и локальным устройством. Возможные опции: A/B/A&B.

Порт A (Last A)
Описание: статистика сообщений порта A

Порт B (Last B)
Описание: статистика сообщений порта B.

11. Расшифровка аббревиатур

Аббревиатура	Полное наименование	Наименование на русском языке
BC	Boundary Clock	Граничные часы
CLI	Command Line Interface	Интерфейс командной строки
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DST	Daylight Saving Time	Летнее время
E2ETC	End-to-End Transparent Clock	Прозрачные часы, работающие в режиме End-to-End
FTP	File Transfer Protocol	Протокол передачи данных
GPS	Global Positioning System	Глобальная позиционная система
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
IED	Intelligent Electronic Device	Интеллектуальное электронное устройство
LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня
LLDPDU	Link Layer Discovery Protocol Data Unit	Блок данных протокола обнаружения канального уровня
MAC	Media Access Control	Управление доступом к среде (обеспечивает адресацию и механизмы управления доступом к каналам)
MIB	Management Information Base	База управляющей информации
NTP	Network Time Protocol	Протокол синхронизации времени в сети
OC	Ordinary Clock	Обычные часы
OID	Object Identifier	Идентификатор объекта
P2PTC	Peer-to-Peer Transparent Clock	Прозрачные часы, работающие в режиме Peer-to-Peer
PTP	Precision Time Protocol	Протокол синхронизации точного времени
RADIUS	Remote Authentication Dial-In User Service	Протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах
RTC	Real Time Clock	Часы реального времени

SNMP	Simple Network Management Protocol	Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP)
SNTP	Simple Network Time Protocol	Простой протокол синхронизации времени (является упрощённой реализацией протокола NTP)
SSL	Secure Sockets Layer	Уровень защищённых сокетов, криптографический протокол
TACACS+	Terminal Access Controller Access Control System	Усовершенствованный протокол контроля доступа к терминалам
TC	Transparent Clock	Прозрачные часы