Коммутаторы серии Ruby3A с поддержкой PRP/HSR

Руководство по программной части

Версия 1.1

Сайт: https://kyland-rus.ru/

Эл. почта: sales@kyland-rus.ru
support@kyland-rus.ru

KYLAND

Содержание

Предисловие

В этом руководстве в основном представлены методы доступа и функции программного обеспечения коммутаторов Ruby3A с поддержкой PRP/HSR, а также подробно описаны методы настройки через веб-интерфейс.

Структура материала

Руководство пользователя содержит следующий материал:

Основное содержание	**Пояснения**
1. Введение	Обзор Функции программного обеспечения Модели изделия
2. Доступ к коммутатору	Варианты представления Доступ к коммутатору через консольный порт Доступ к коммутатору через Telnet Доступ к коммутатору через веб-интерфейс
3. Информация об устройстве	Основные сведения о коммутаторе
4. Основная конфигурация коммутатора	Настройка пользователей Настройка IP Информация о системе Загрузка файла Обновление прошивки Выгрузка файла Перезагрузка
5. Функции	Резервирование PTP Статистика

6. Другие настройки	Аварийная сигнализация Настройка порта Настройка MAC
	Sntp Ntp IEC61850 MMS SNMPv2c SNMPv3 Файловый сервер LLDP DDMI Виртуальный кабельный тестер Radius Tacacs Plus AAA LINE
7. Обслуживание коммутатора	
8. Узлы сети	

Условные обозначения в руководстве

1. Условные обозначения в тексте

Формат	**Пояснения**
< >	Текст в угловых скобках < > – это название кнопки. Например, щелкните кнопку <Apply>.
[ ]	Текст в квадратных скобках [ ] – это название окна или меню. Например, щелкните пункт меню [File].

{ }	Текст в фигурных скобках { } – это сгруппированные элементы. Например, {IP-адрес, MAC-адрес} означает, что IP-адрес и MAC-адрес объединены в группу, и их можно настраивать и отображать совместно.
→	Элементы многоуровневых меню разделяются знаком “→”. Например, Start → All Programs → Accessories. Щелкните меню [Start], щелкните подменю [All programs], затем щелкните подменю [Accessories].
/	Выбор одного из двух или нескольких вариантов, разделенных знаком “/”. “Добавление/вычитание” означает добавление или вычитание.
~	Обозначает диапазон. Например, “1~255” означает диапазон от 1 до 255.

2. Символы

Символ	Пояснения
 **Предостережение**	На эти моменты следует обратить внимание при эксплуатации и настройке, они дополняют описание действий.
 **Примечание**	Необходимые пояснения к описанию действий.
 **Предупреждение**	Требует особого внимания. Некорректные действия могут привести к потере данных или повреждению оборудования.

Документация по изделию

Документация к коммутаторам Ruby3A включает в себя:

Наименование документа	**Содержание**
Руководство пользователя по монтажу промышленного коммутатора Ethernet Ruby3A	Описана конструкция оборудования, технические характеристики, способы монтажа и демонтажа.
Руководство пользователя по веб-интерфейсу коммутатора Ruby3A PRP/HSR	Описаны функции ПО, способы настройки через веб-интерфейс и все функции.

1 Введение

1.1 Обзор

Коммутаторы Ruby3A PRP/HSR специально разработаны для обеспечения высокой надежности промышленных сетей и реализуют протоколы PRP (протокол параллельного резервирования) и HSR (бесшовное резервирование с высокой доступностью), соответствующие стандартам IEC62439-3. Ruby3A позволяют добиться нулевой потери пакетов в случае сбоя сети, обеспечивая максимальную надежность сети. Полноценное аппаратное решение FPGA позволяет Ruby3A реализовать программное обеспечение HSR и PRP, настраиваемое на том же оборудовании с очень низкой задержкой в сети. Ruby3A поддерживает стандарт IEEE 1588v2. Синхронизацию времени высокой точности можно обеспечить через сеть HSR/PRP.

1.2 Функции программного обеспечения

Эта серия коммутаторов имеет широкий набор программных функций и может удовлетворить различные требования заказчиков.

Таблица 1 Функции программного обеспечения

Элемент	описание
HSR/PRP	Поддерживается PRP. Время восстановления при отказе 0 мс Поддерживается HSR. Время восстановления при отказе 0 мс Поддерживается совместное использование PRP/HSR
IEEE1588v2	Поддерживается режим PTPv2 (IEEE1588-2008), точность лучше 1 мкс
VLAN и Port	Скорость порта (1000M/100M/10M/auto) Дуплекс порта (full/half) 802.1Q (1~4093) VLAN на основе порта
MAC-адрес	Возможность настройки режимов Auto Learning и VLAN-aware Таблица MAC-адресов до 2K Возможность настройки таймера старения и автостарения динамических MAC-адресов

Протокол синхронизации часов	SNTP/NTP
Сетевая безопас-ность	Централизованное управление пользователями SSH SSL
LLDP	Поддерживается изучение соседей LLDP, информация о соседях, просмотр статистики сообщений
Server IEC61850 MMS	Поддерживается сервер IEC61850 MMS
Управление	клиент dhcp клиент ftp/сервер ftp/клиент sftp ping Управление с консоли клиент telnet/сервер telnet Управление через веб-интерфейс Централизованное управление SNMP (v1,v2c,v3) Работа ЦП Аварийная сигнализация по электропитанию Аварийная сигнализация по порту (LinkDown) перезагрузка устройства (перезагрузка) восстановление заводской конфигурации (настройки по умолчанию) Отображение общего времени работы устройства

1.3 Изделия, которые охватывает данное руководство

Ruby3A-3G-HV

Ruby3A-3G-L2-L2

SM6.6-HSR/PRP-GE-0.5U

SM6.6-HSR/PRP-GX-0.5U

2 Доступ к коммутатору

Доступ к коммутатору осуществляется через:

- Консольный порт
- Telnet/SSH
- Веб-браузер
- Программное обеспечение Kyvision

Программное обеспечение для управления сетью Kyvision разработано компанией Kyland. Подробная информация содержится в руководстве пользователя.

2.1 Варианты представления

При входе в интерфейс командной строки (CLI) через консольный порт или Telnet можно входить в различные представления или переключаться между представлениями с помощью следующих команд.

Таблица 2 Варианты представления

Вид меню	Вариант представления	Функция	Команда для переключения представления
Switch >	Общий режим	• Просмотр системной даты и времени. • Просмотр версии программного обеспечения.	Введите enable для входа в привилегированный режим.
Switch#	Привилегированный режим	• Настройка системных часов и даты. • Передача фала и обновление ПО. • Удаление файла коммутатора. • Настройка языка командной строки. • Просмотр настроек коммутатора и информации о системе. • Восстановление конфигурации по умолчанию.	Введите config для переключения из привилегированного режима в режим настройки. Введите exit для возврата в общий режим.

		• Сохранение текущей конфигурации.	
		• Перезагрузка коммутатора.	
Switch (config) #	Режим настройки	Настройка всех функций коммутатора.	Введите exit для возврата в привилегированный режим.

При настройке коммутатора через интерфейс командной строки для получения справки по командам можно использовать «?». В справочной информации используются различные форматы описания параметров. Например, <1, 255> означает числовой диапазон; <H.H.H.H> означает IP-адрес ; <H: H: H: H: H: H> означает MAC-адрес; word<1, 31> означает диапазон строк 1~31. Кроме того, символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.

2.2 Доступ к коммутатору через консольный порт

Доступ к коммутатору можно получить через его консольный порт и гипертерминал операционной системы Windows или другое программное обеспечение, поддерживающее подключение через последовательный порт, например, HTT3.3. В следующем примере показано, как использовать HyperTerminal для доступа к коммутатору через консольный порт.

Подключите 9-контактный последовательный порт ПК к консольному порту коммутатора с помощью консольного кабеля DB9-RJ45.

Запустите HyperTerminal на рабочем столе Windows. Щелкните [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], как показано ниже.

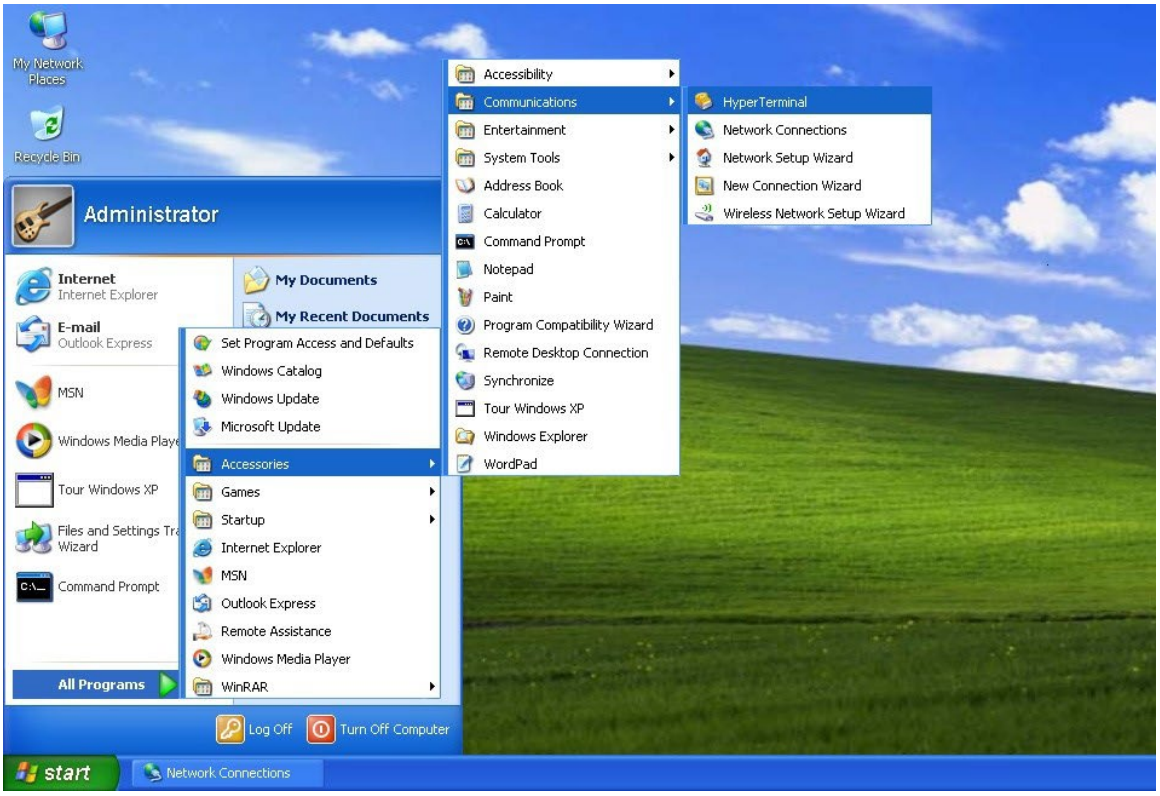


Рисунок 1 Запуск Hyper Terminal

3. Создайте новое подключение "Switch", как показано ниже.

Рисунок 2 Создание нового подключения

4. Выберите порт для подключения, как показано ниже.

Рисунок 3 Выбор порта для подключения

NOTE	**Примечание**: Чтобы убедиться, что порт выбран верно, щелкните правой кнопкой [My Computer] и щелкните [Property] → [Hardware] → [Device Manager] → [Port].

5. Настройте параметры порта (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None), как показано ниже.

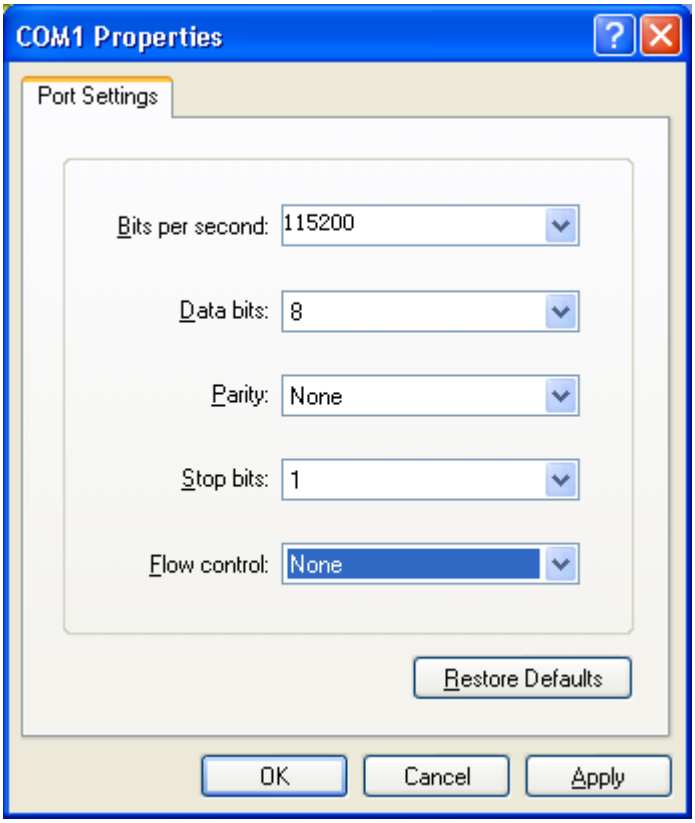


Рисунок 4 Настройка параметров порта

6. Щелкните кнопку <OK>, чтобы войти в интерфейс командной строки коммутатора. Введите пароль admin и нажмите <Enter>, чтобы войти в общий режим, как показано ниже.

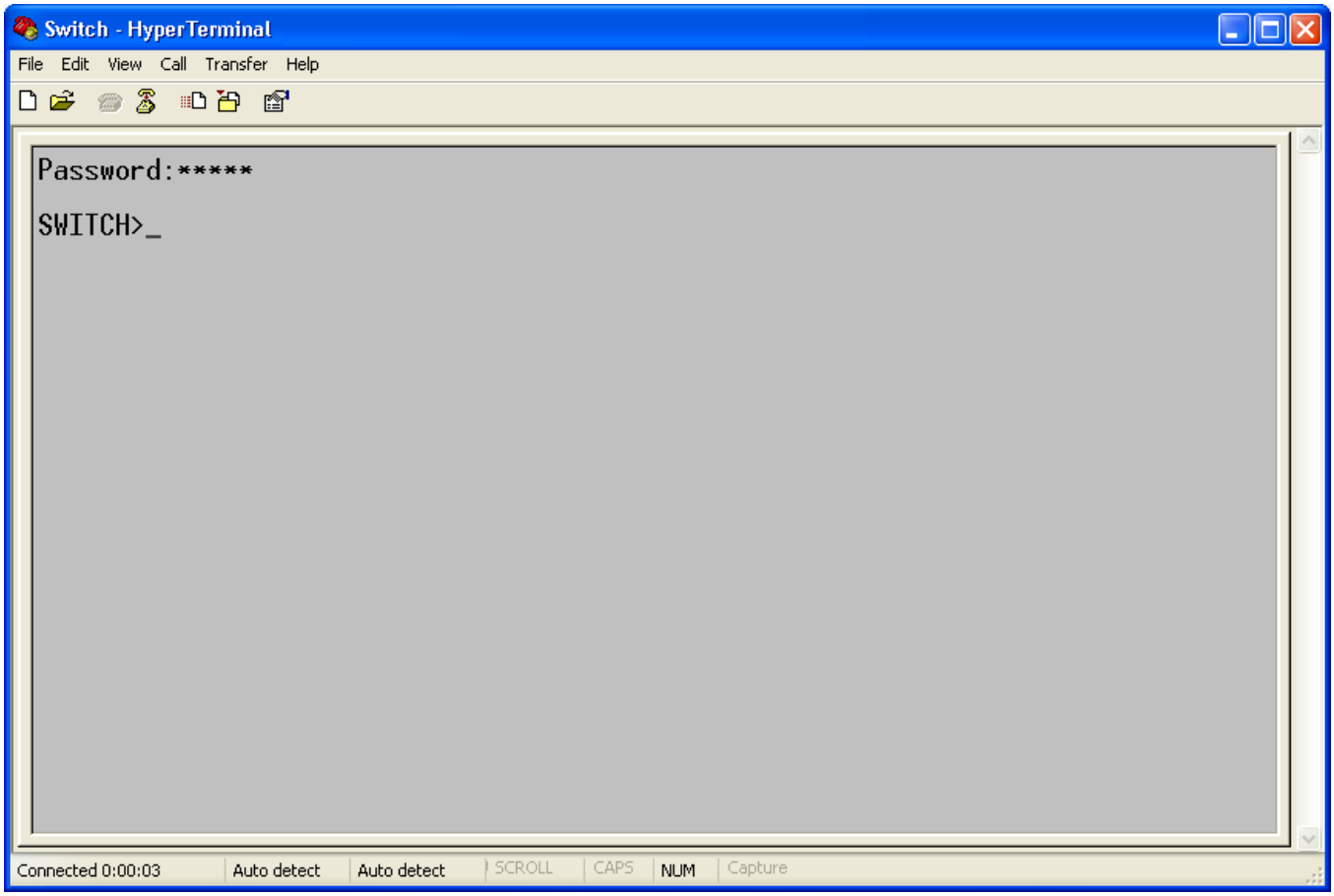


Рисунок 5 Интерфейс командной строки

7. Введите команду enable, имя пользователя по умолчанию admin и пароль 123 для входа в привилегированный режим. Можно также ввести другие созданные имя пользователя и пароль, как показано ниже.

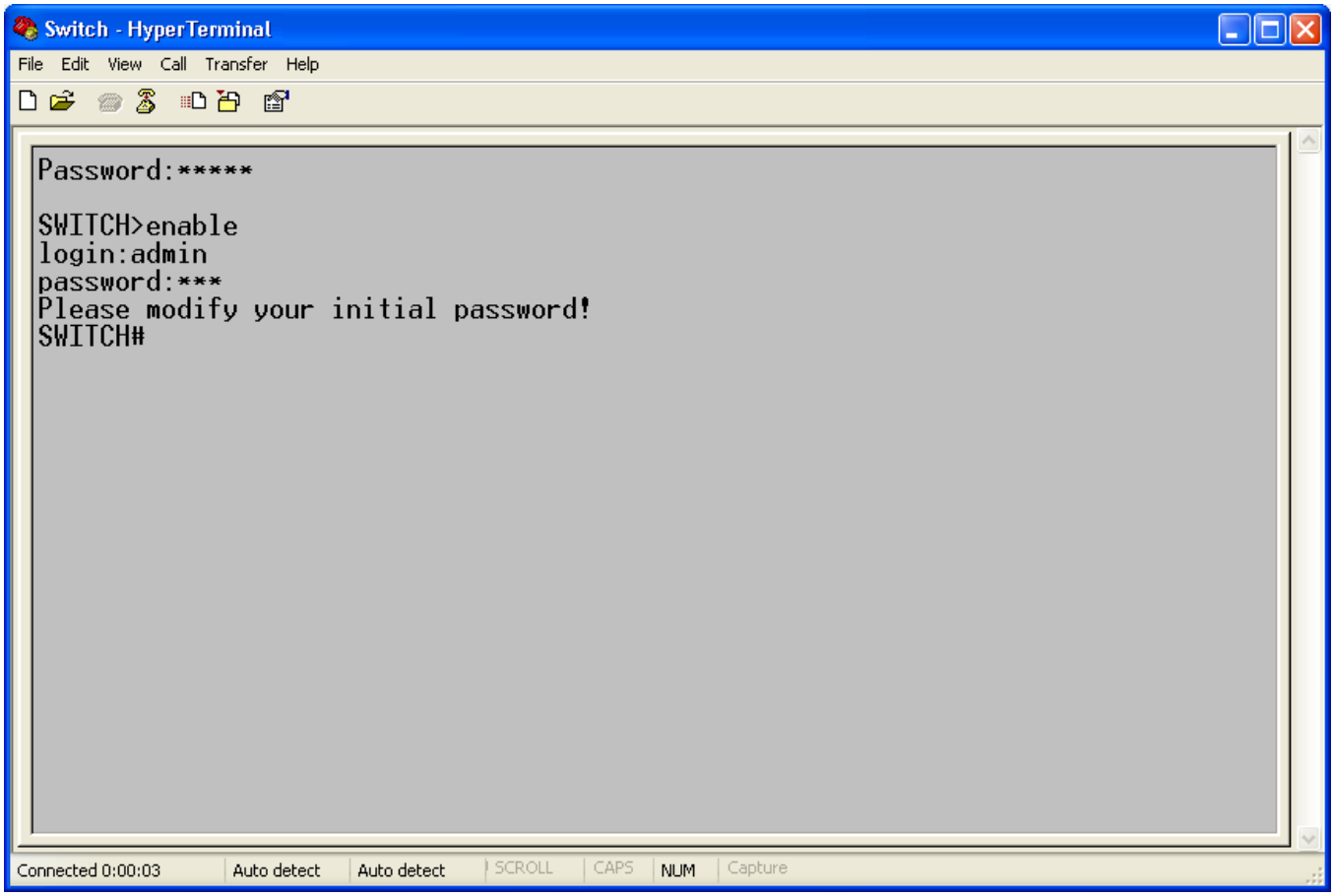


Рисунок 6 Привилегированный режим

2.3 Доступ к коммутатору через Telnet

Предварительным условием доступа к коммутатору по протоколу Telnet является нормальная связь между ПК и коммутатором.

Введите telnet IP-адрес в диалоговом окне Run, как показано ниже. IP-адрес коммутатора Kyland по умолчанию 192.168.0.2.

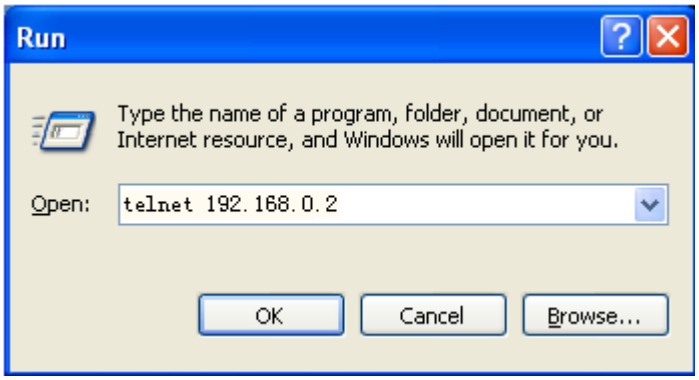


Рисунок 7 Доступ по Telnet

NOTE	**Примечание**: Чтобы подтвердить IP-адрес коммутатора, обратитесь к разделу 4.2 «Настройка IP», чтобы узнать, как получить IP-адрес.

В интерфейсе Telnet введите пароль по умолчанию admin для подключения к коммутатору. Можно также ввести другие созданные имя пользователя и пароль, как показано ниже.

Рисунок 8 Интерфейс Telnet

2.4 Доступ к коммутатору через веб-интерфейс

Предварительным условием доступа к коммутатору через веб-интерфейс является нормальная связь между ПК и коммутатором.

NOTE	**Примечание**: Для наилучшего отображения доступа через веб-интерфейс рекомендуется использовать IE8.0 или более позднюю версию.

1. Введите IP-адрес в адресной строке браузера. Отображается интерфейс для входа, как показано ниже. Введите имя пользователя по умолчанию admin, пароль 123. Щелкните <OK>. Можно также ввести другие созданные имя пользователя и пароль.

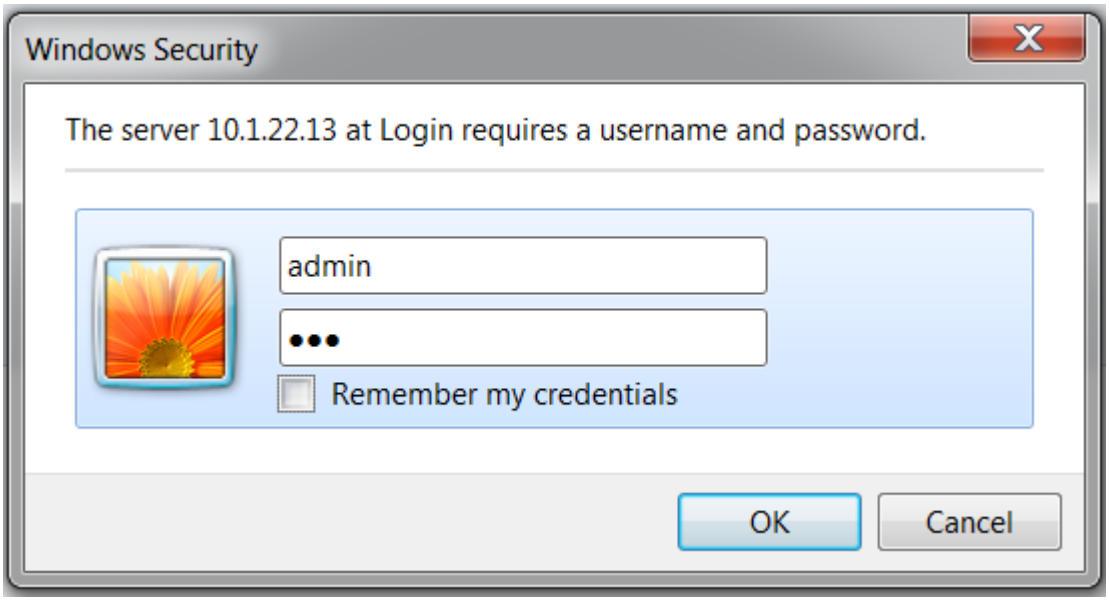


Рисунок 9 Вход через веб-интерфейс

По умолчанию отображается английский интерфейс.

NOTE	**Примечание**: Чтобы подтвердить IP-адрес коммутатора, обратитесь к разделу 4.2 «Настройка IP», чтобы узнать, как получить IP-адрес.

2. Успешный вход в систему для включения страницы управления через веб-интерфейс. Верхняя область – это дерево навигации настроек, режим настройки можно переключать в левой области, зеленый — базовый режим, красный — расширенный режим. В расширенном режиме предоставляются более высокие полномочия, чем в базовом режиме, пользователи могут настроить дополнительные модули устройства, как показано ниже.

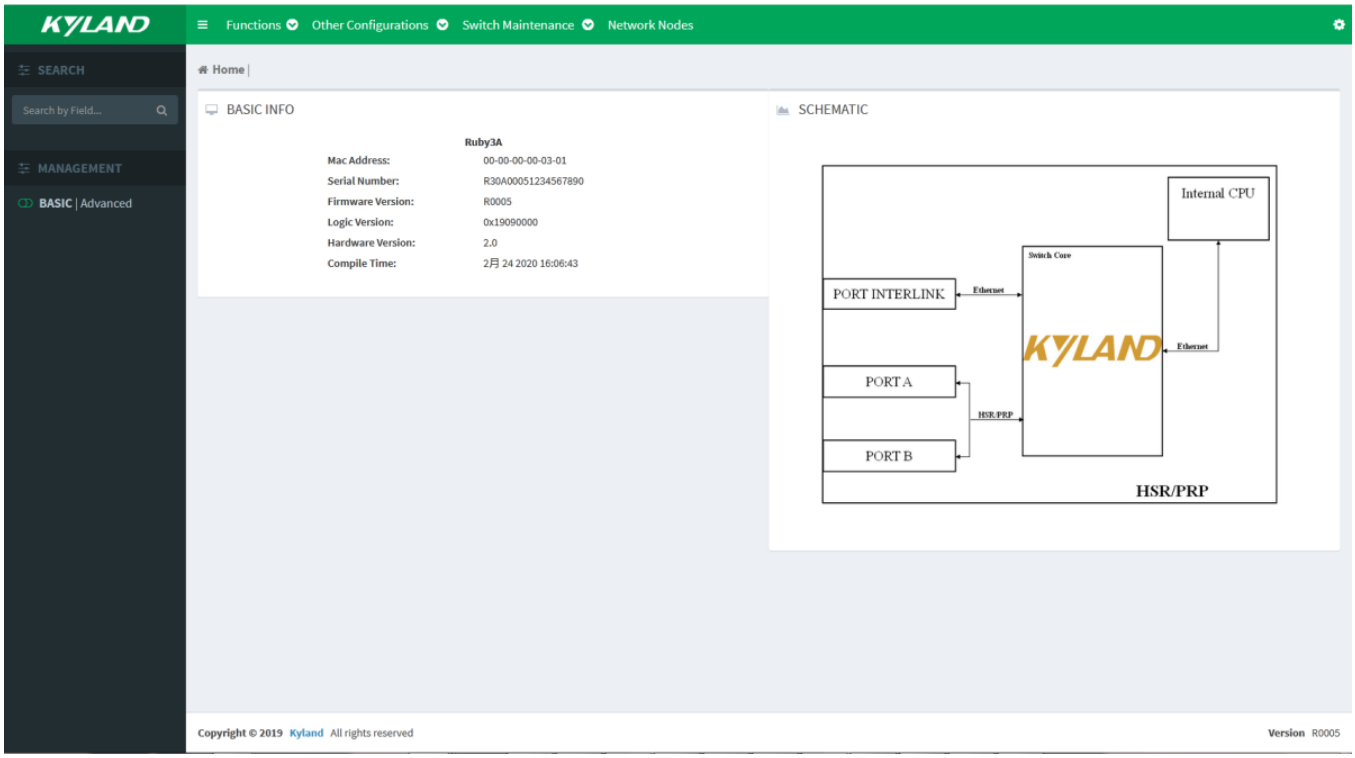


Рисунок 10 Веб-интерфейс

Щелкните значок KYLAND в верхнем левом углу, чтобы перейти к веб-интерфейсу, показанному на рисунке 10. В любом случае для переключения на веб-интерфейс щелкните значок. Щелкните значок шестеренки в правом верхнем углу и выберите Logout для выхода из веб-интерфейса. Можно настроить и другие функции коммутатора.

3 Информация об устройстве

3.1 Основные сведения о коммутаторе

1. Окно BASIC INFO

Страница BASIC INFO содержит базовую информацию о конфигурации устройства Ruby3A, включая MAC-адрес, серийный номер, версию прошивки, версию логики, версию оборудования, время компиляции, как показано ниже.

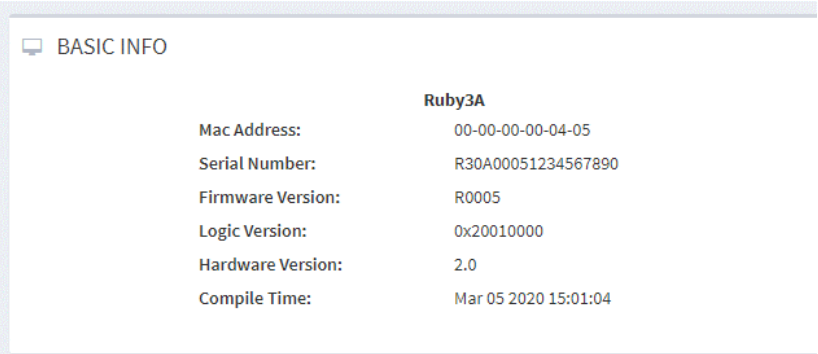


Рисунок 11 Основные сведения о коммутаторе

2. Окно SCHEMATIC

Отображается схема коммутатора, как показано ниже.

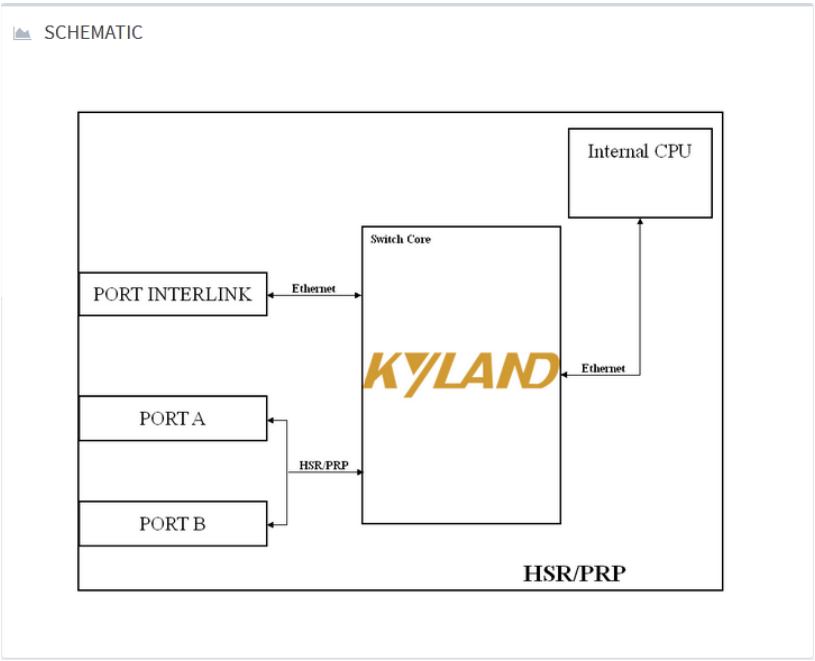


Рисунок 12 Схема коммутатора

4 Основные настройки коммутатора

Щелкните значок шестеренки в правом верхнем углу главной страницы интерфейса, чтобы настроить основную информацию о пользователе. Существует два режима: базовый и расширенный, которые имеют разные параметры базовой конфигурации. Расширенный режим дает более высокие полномочия и имеет больше настраиваемых элементов.

Настраиваемые элементы коммутатора в расширенном и базовом режиме показаны ниже.

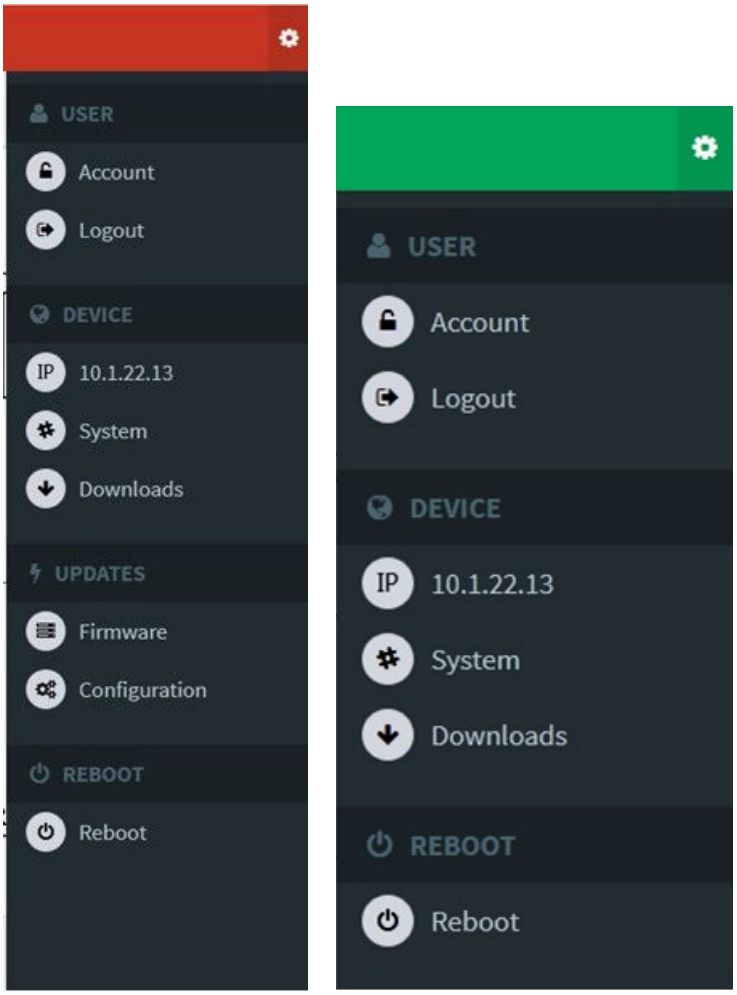


Рисунок 13 Расширенный и базовый режимы

4.1 Настройка пользователей

Пункт меню Account в разделе User предназначен для изменения пароля пользователя. Пункт Logout – выход из веб-интерфейса.

4.2 Настройка IP

1. Запрос IP-адреса коммутатора через консольный порт

Выполните вход в интерфейс командной строки через консольный порт. В режиме привилегированного пользователя введите команду show interface ip brief, IP-адрес коммутатора будет отображен, 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#
```

Рисунок 14 IP-адрес

Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите IP в разделе [DEVICE], перейдите на страницу настройки IP. Будет отображен IP-адрес портов L и M, как показано ниже.

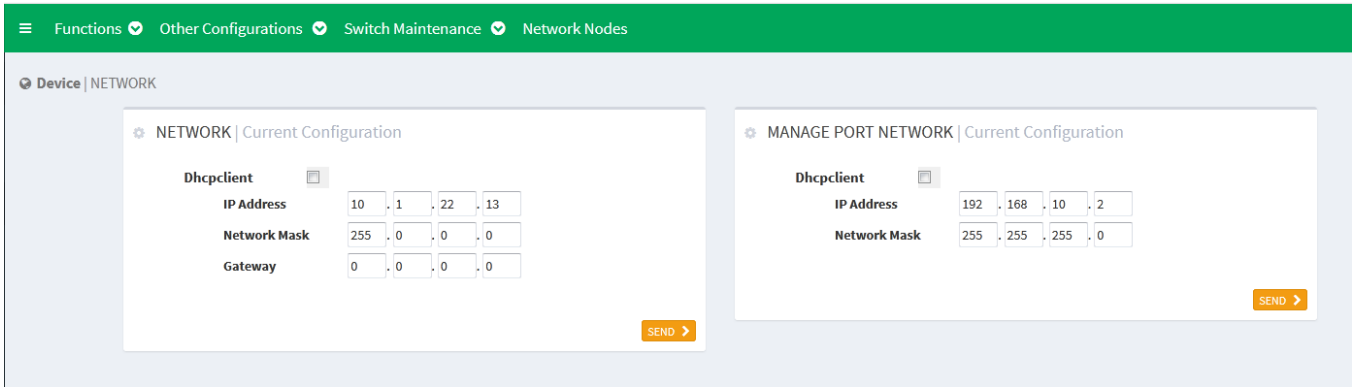


Рисунок 15 Страница настройки IP Ruby3a

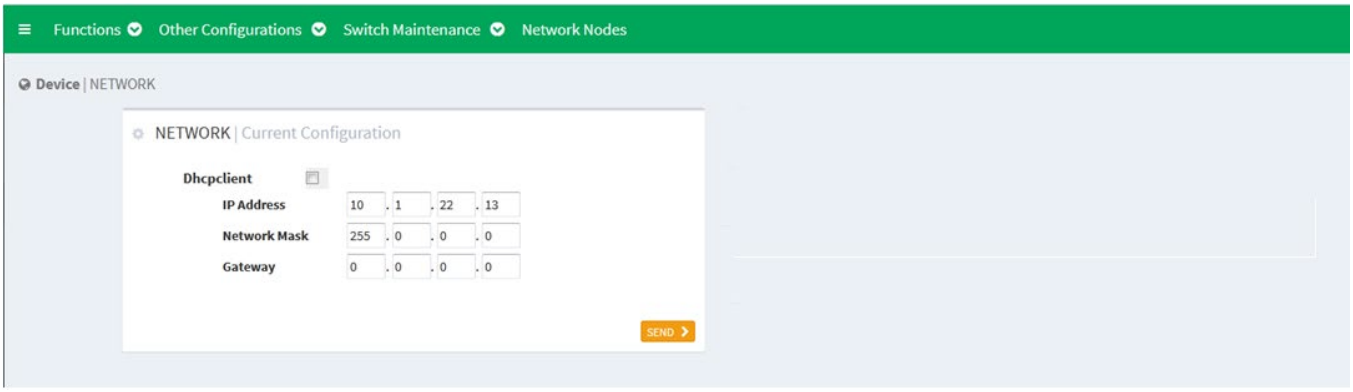


Рисунок 16 Страница настройки IP HSR/PRP

NETWORK

Функция: Настройка IP-адреса порта L.

MANAGE PORT NETWORK

Описание функции: Настройка IP-адреса порта управления

На этой странице настройки левая часть предназначена для настройки IP порта L, правая – для настройки IP порта M.

Поддерживается настройка статических и динамических IP.

CAUTION	**Предостережение**: Ruby3a имеет независимый порт управления, в SM6.6-HSR/PRP независимого порта управления нет.

4.2.1 Настройка DHCP

4.2.1.1 Введение

С непрерывным расширением масштаба и ростом сложности сети, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) и числа компьютеров, превышающего выделяемые IP-адреса, протокол BootP, специально предназначенный для статической конфигурации хоста, оказывается неспособным удовлетворить фактические потребности. Для быстрого доступа и выхода из сети и улучшения коэффициента использования ресурсов IP-адресов нам необходимо разработать автоматический механизм на основе BootP для назначения IP-адресов. Для решения этих проблем был введен DHCP (протокол динамической конфигурации хоста).

DHCP использует модель взаимодействия клиент-сервер. Клиент отправляет запрос конфигурации на сервер, а затем сервер отправляет параметры конфигурации, такие как IP-адрес, клиенту, достигая динамической конфигурации IP-адресов. Структура типичного использования DHCP показана на рисунке ниже.

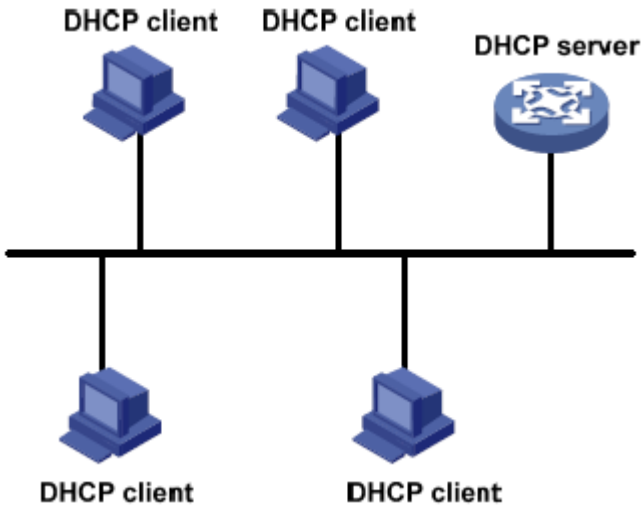


Рисунок 17 Типичное использование DHCP

CAUTION	**Предостережение**: В процессе динамического 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.

DHCP поддерживает два типа механизмов распределения IP-адресов.

Статическое распределение: сетевой администратор статически привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как WWW-сервер, и отправляет привязанные IP-адреса клиентам по DHCP.

Динамическое распределение: Сервер DHCP динамически выделяет IP-адрес клиенту. Этот механизм выделения может выделить клиенту постоянный IP-адрес или IP-адрес с ограниченным сроком аренды. Когда срок аренды истекает, клиенту необходимо повторно запросить IP-адрес.

Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента. 4.2.1.2 Настройка DHCP

CAUTION	**Предостережение**: Данное устройство не поддерживает настройку сервера DHCP, поддерживается только клиент DHCP.

На рисунке ниже показана страница настройки IP порта L.

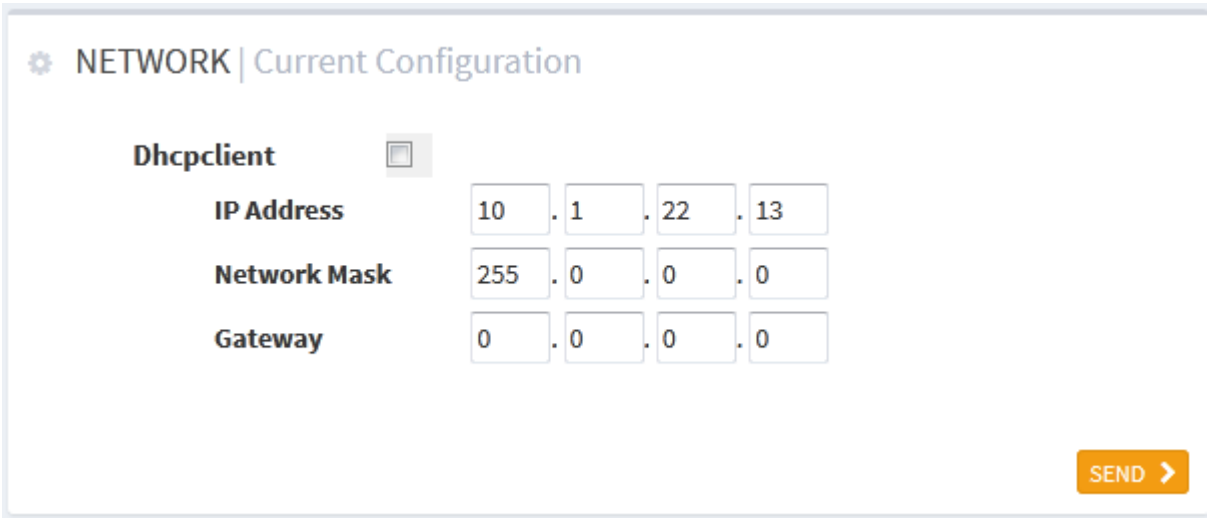


Рисунок 18 Настройка IP порта L

Когда установлен флажок Dhcpclient, клиент DHCP включен, клиент может запросить IP-адрес у удаленного сервера. Когда установлен флажок Dhcpclient, другие элементы настройки на странице остаются незаполненными. После обновления страницы можно увидеть IP-адрес, успешно полученный по DHCP. Если получить IP-адрес не удалось, предыдущий IP-адрес можно использовать в качестве текущего адреса. Значения Mask и GateWay те же самые, восстанавливается последнее значение конфигурации.

4.2.2 Настройка статического IP

Настройка IP порта L показана на рисунке 18. Настройте IP-адрес, задав вручную значения IP и маски.

IP Address

Формат: A.B.C.D

Функция: задание IP-адреса вручную

Network mask

Формат: A.B.C.D

Функция: Маску подсети можно преобразовать в число длиной 32 бита, состоящее из непрерывной строки 1 и 0. 1 соответствует полям номера сети и полям номера подсети, а 0 соответствует полям номера хоста. Длина маски — это количество 1 в маске подсети.

CAUTION	**Предостережение**: Данный коммутатор поддерживает только настройку IP порта L и порта M, каждый IP-интерфейс соответствует IP-адресу; Разные IP-интерфейсы должны быть настроены на IP-адреса с разными сегментами сети

Gateway

Формат: A.B.C.D

Функция: Задание адреса шлюза вручную.

IP-адрес и шлюз должны находиться в одном сегменте сети; в противном случае настройка будет неудачной.

4.3 Информация о системе

Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите [SYSTEM] в разделе [DEVICE], перейдите на страницу информации о системе, как показано ниже.

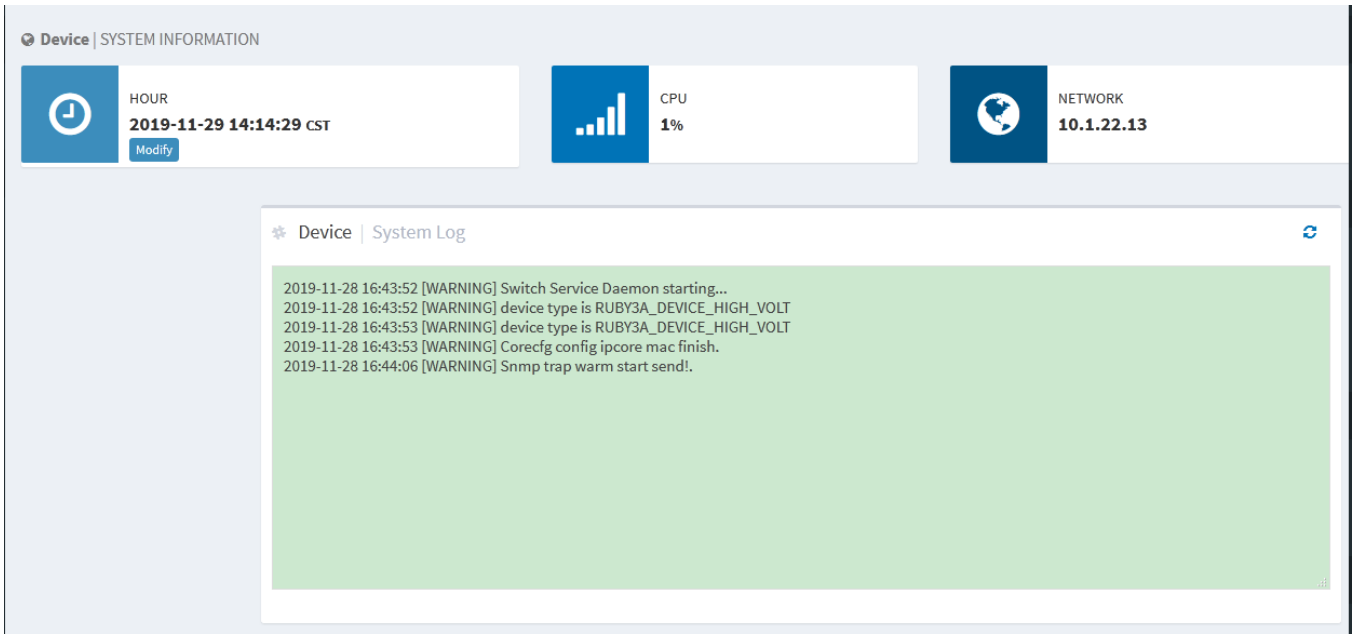


Рисунок 19 Страница информации о системе

Эта страница в основном предназначена для просмотра системной информации и настроек коммутатора, включая настройку времени, процессор, сеть и журнал.

4.3.1 Настройка часов

Для настройки системного времени и даты щелкните значок шестеренки в правом верхнем углу главной страницы, выберите [SYSTEM] и перейдите на страницу настройки часов, как показано ниже.

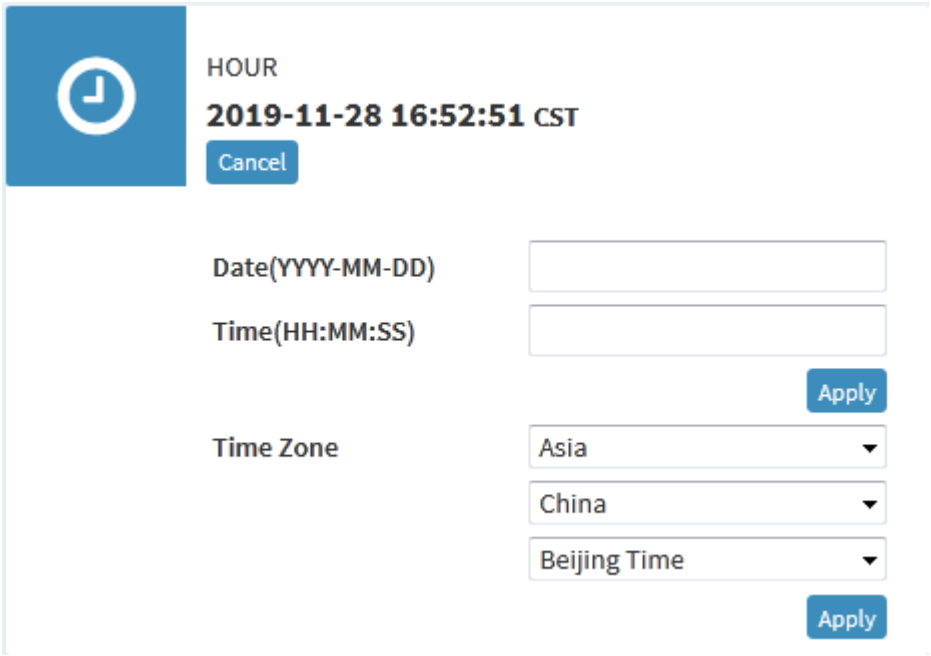


Рисунок 20 Настройка часов

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

Date (YYYY.MM.DD)

Диапазон настройки: YYYY (год) в диапазоне 1970–2099, MM (месяц) в диапазоне 1–12, DD (день)в диапазоне 1–31.

Time (HH:MM: SS)

Диапазон настройки: HH (часы) в диапазоне 0–23, MM (минуты) и SS (секунды) в диапазоне 0–59.

Time Zone

Настройка часового пояса, выберите континент, страну и город

4.3.2 Состояние ЦП

Состояние ЦП показывает текущую среднюю загрузку ЦП, как показано ниже.

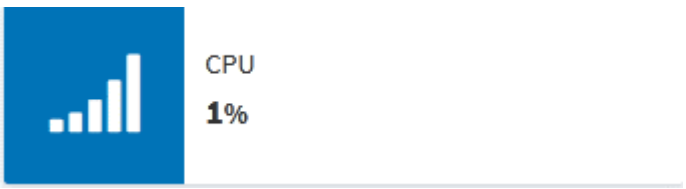


Рисунок 21 Загрузка ЦП

4.3.3 Состояние сети

Отображается IP-адрес веб-интерфейса входа в систему, демонстрируется, что интерфейс используется, как показано ниже.

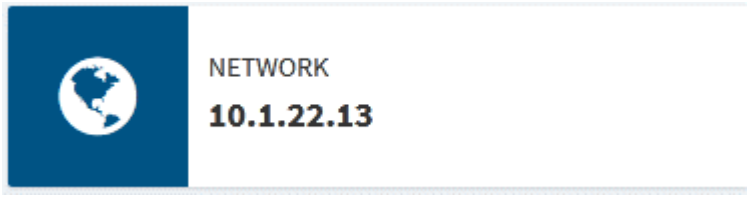


Рисунок 22 Состояние сети

4.3.4 Системный журнал

Функция журнала коммутатора записывает изменение состояния, неисправности, отладку, исключения, действия пользователя и другую информацию о системе коммутатора, что удобно для обнаружения неисправностей. Информацию журнала можно загрузить на сервер, поддерживающий протокол системного журнала, в режиме реального времени.

Сообщения в журнале включают в себя различную информацию о тревогах, широковещательных штормах, перезапуске, информацию о памяти и действиях пользователя. Информация журнала показана ниже.

Рисунок 23 Информация журнала

Щелкните кнопку обновления в правом верхнем углу, чтобы обновить информацию журнала вручную.

4.4 Загрузка файла

Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите [downloads] в разделе [DEVICE], перейдите на страницу загрузки файла. Как показано на рисунке ниже, можно загрузить MIB и файл Startup-config. Файл Startup-config — это файл запуска коммутатора, который содержит сохраненную конфигурацию коммутатора.

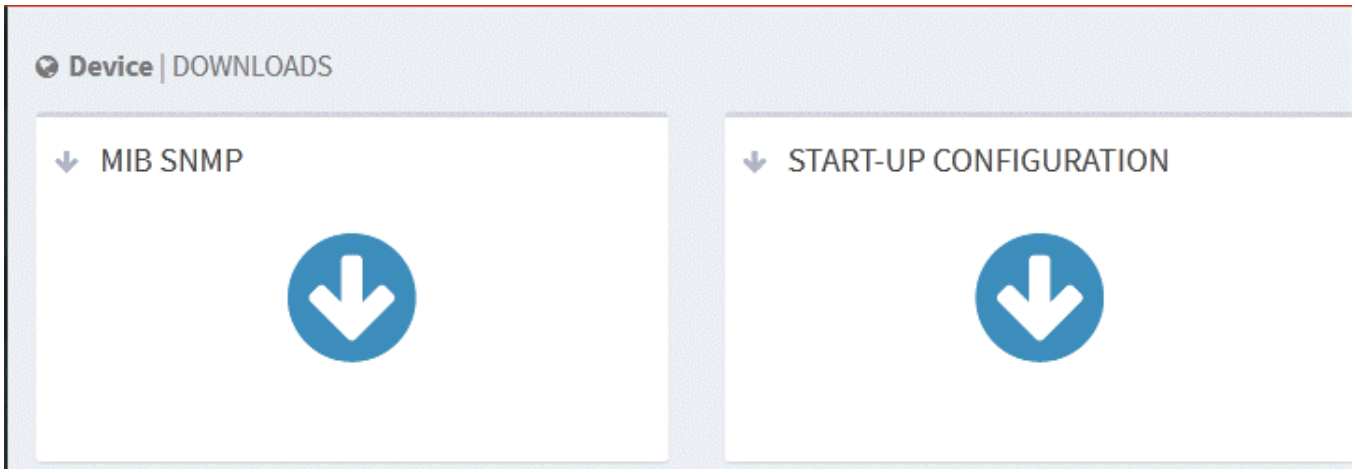
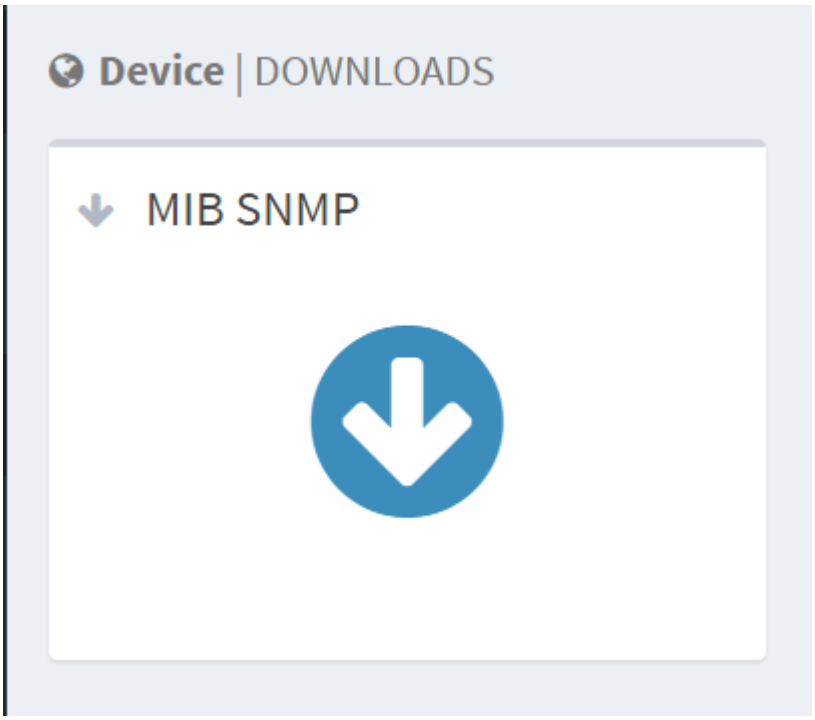


Рисунок 24 Загрузка файла

4.4.1 Загрузка файла MIB

Щелкните кнопку в MIB SNMP, во всплывающем окне щелкните ОК, чтобы загрузить файл SWITCH-DESIGN-MIB.mib по указанному пути, как показано ниже.



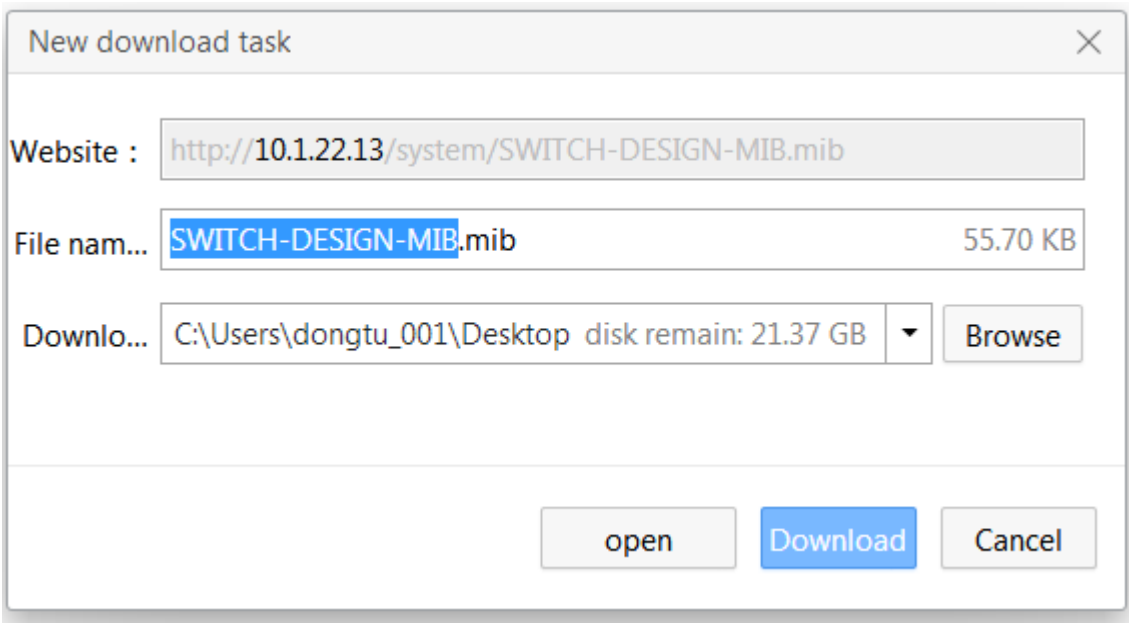
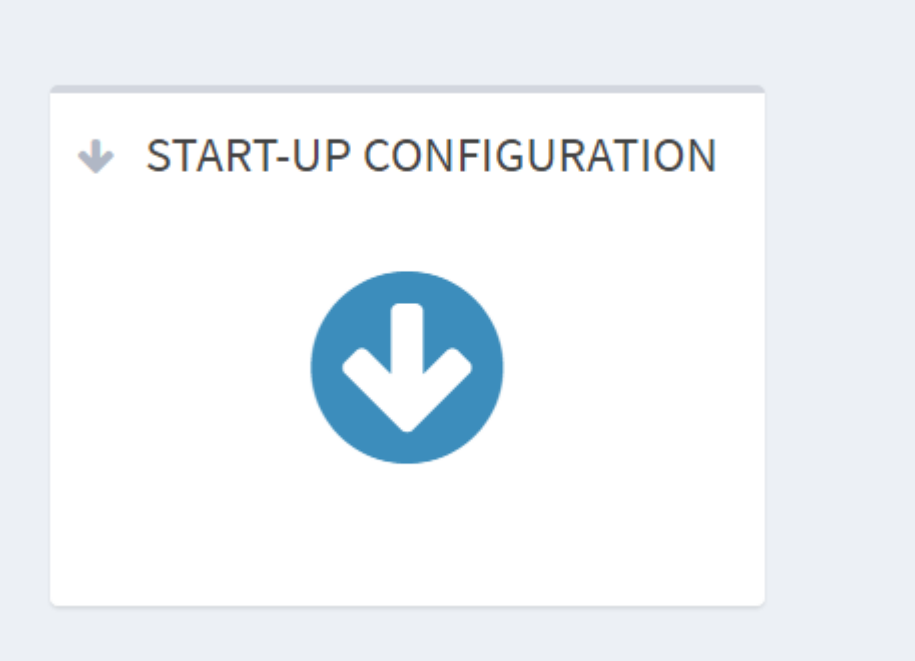


Рисунок 25 Страница загрузки файла MIB

4.4.2 Загрузка файла конфигурации

Щелкните кнопку в START-UP CONFIGURATION, во всплывающем окне щелкните ОК, чтобы загрузить файл startup_config.conf по указанному пути, как показано на рисунке ниже.



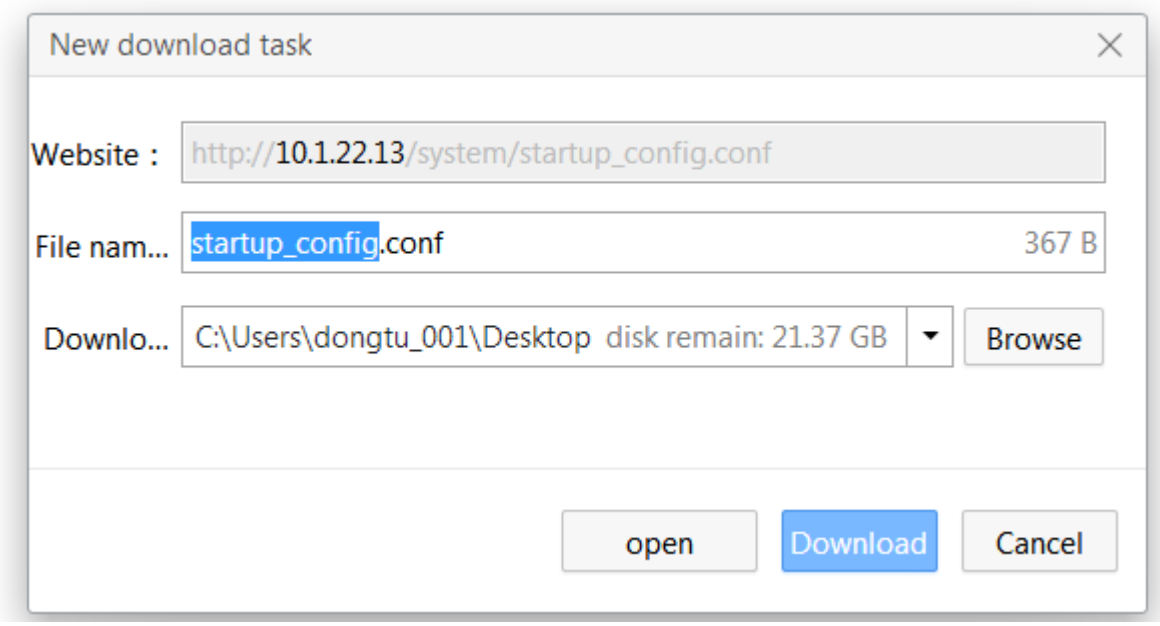


Рисунок 26 Страница загрузки файла конфигурации

4.5 Обновление прошивки

Благодаря обновлению прошивки повышается производительность коммутатора. Поддерживается обновление с сервера FTP/SFTP и локальное обновление.

4.5.1 Локальное обновление

Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите [Firmware] и перейдите на страницу обновления, как показано ниже.

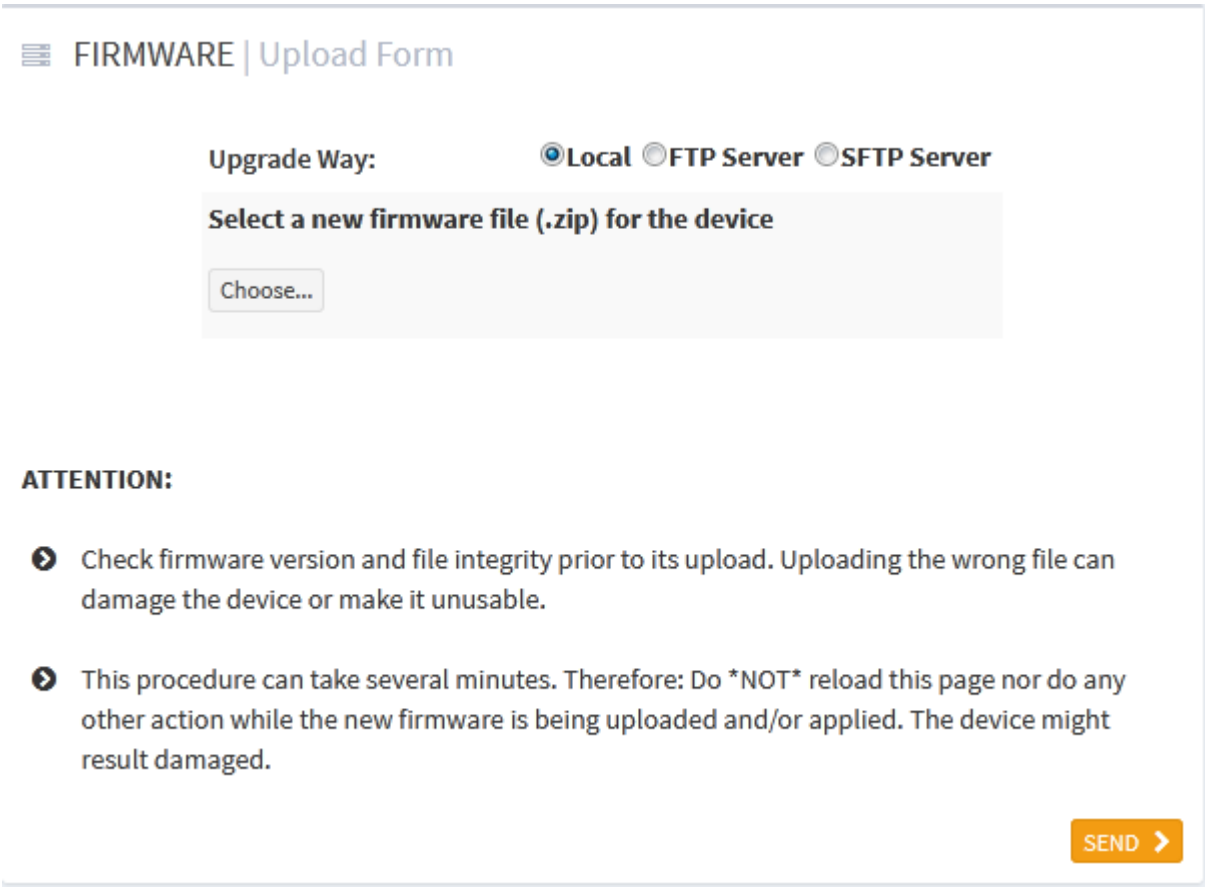


Рисунок 27 Страница локального обновления

Upgrade way

Варианты конфигурации: Local/FTP server/SFTP server

Local

Щелкните кнопку Choose для выбора нужного файла обновления, затем щелкните [SEND] для обновления.

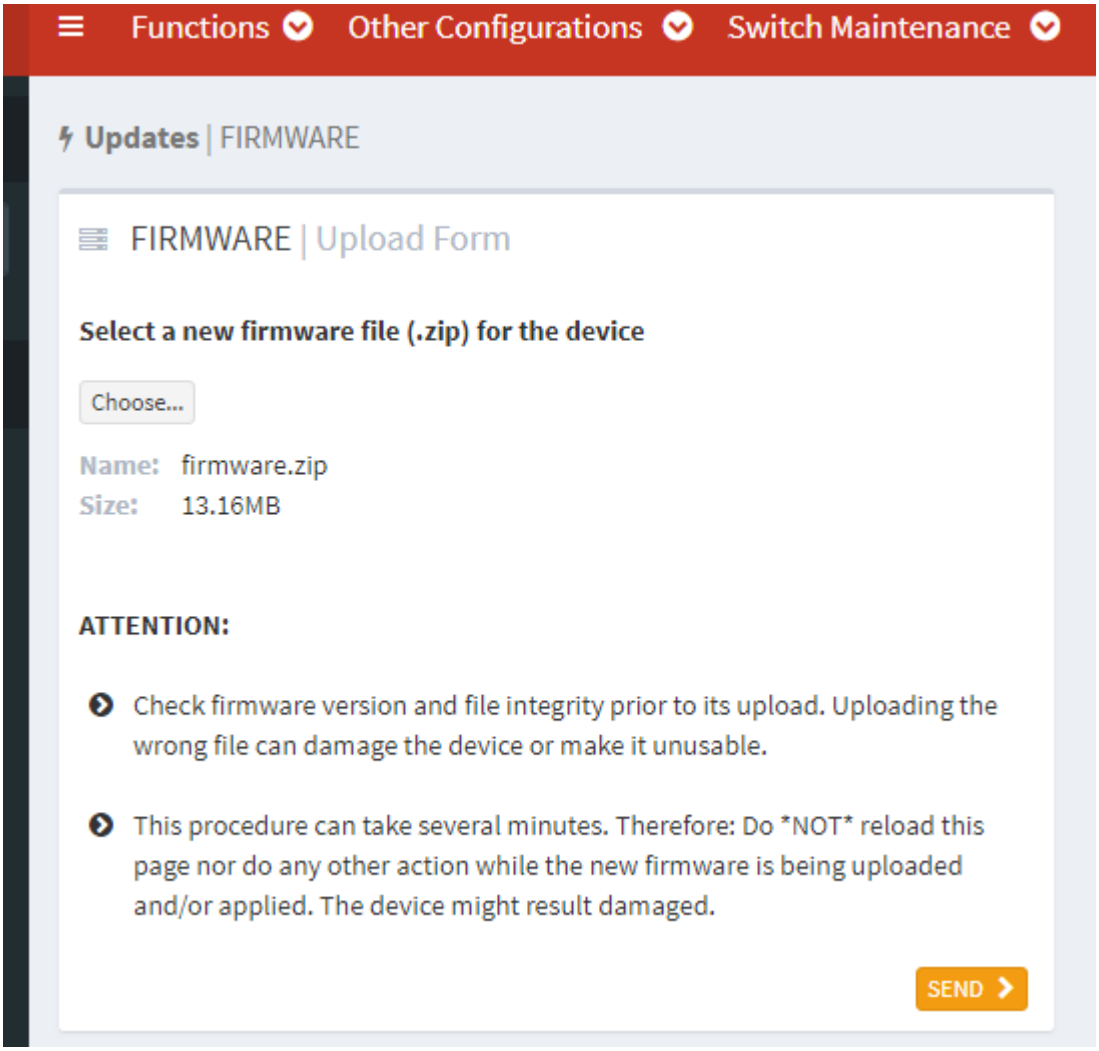


Рисунок 28 Локальное обновление/выбор файла обновления

После выбора файла щелкните <SEND> для запуска обновления. Появится страница ожидания, как показано на рисунке ниже.

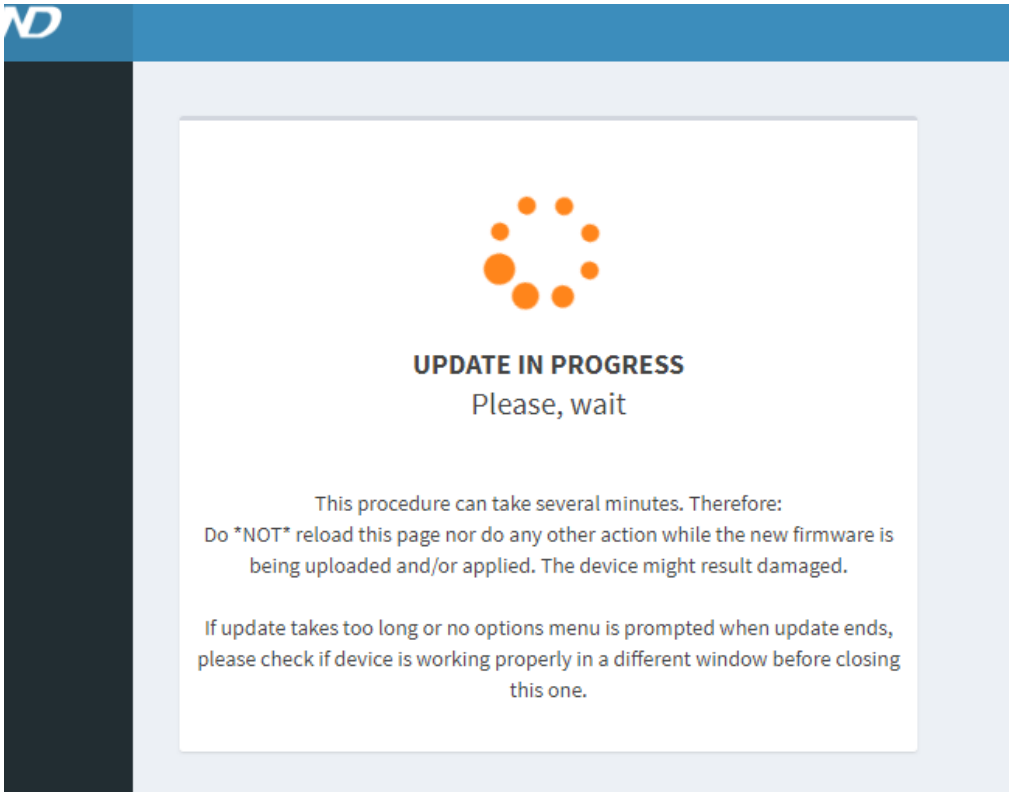


Рисунок 29 Локальное обновление/обновление прошивки

Внимание:

Не выполняйте никаких других действий, тем более не выключайте питание, это может привести к сбою обновления, даже если оно не запустится. Обновление прошло успешно, когда появляется страница, показанная на рисунке ниже.

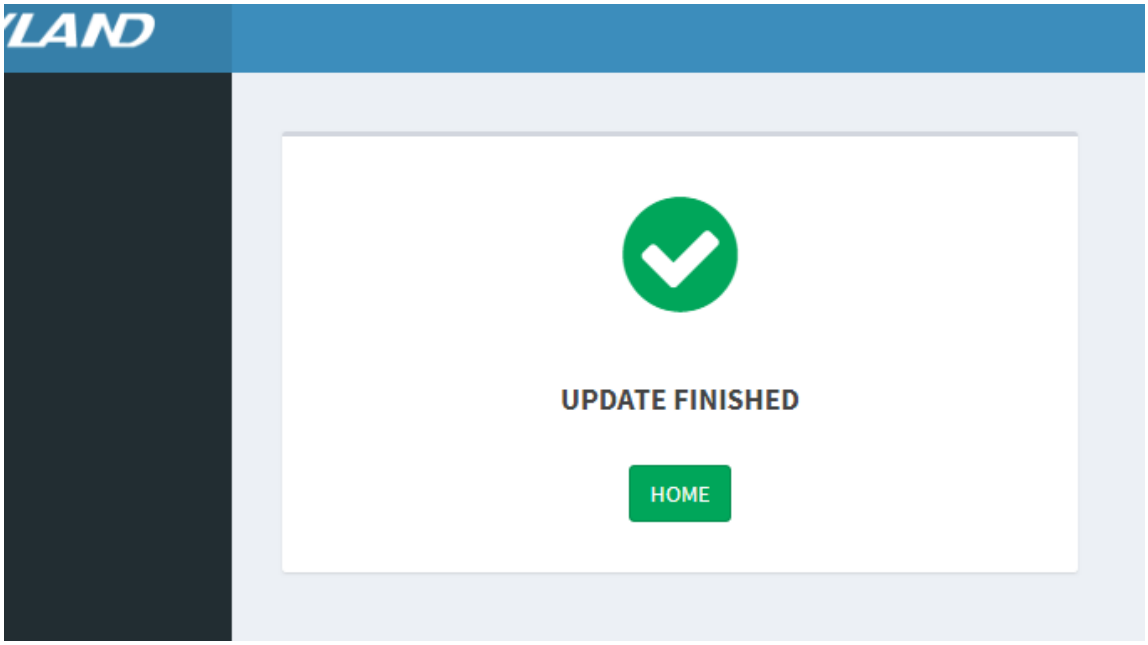


Рисунок 30 Локальное обновление/Обновление прошло успешно

Перезагрузите устройство. Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите **reboot**.

4.5.2 Обновление по FTP

Установите FTP-сервер. Ниже в качестве примера используется программное обеспечение WFTPD для ознакомления с конфигурацией FTP-сервера и обновлением программного обеспечения.

1. Щелкните [Security] → [Users/Rights]. Появится диалоговое окно Users/Rights Security Dialog. Щелкните <New User>, чтобы создать нового пользователя FTP, как показано на рисунке 31. Создайте имя пользователя и пароль, например, имя пользователя admin и пароль 123. Щелкните <OK>.

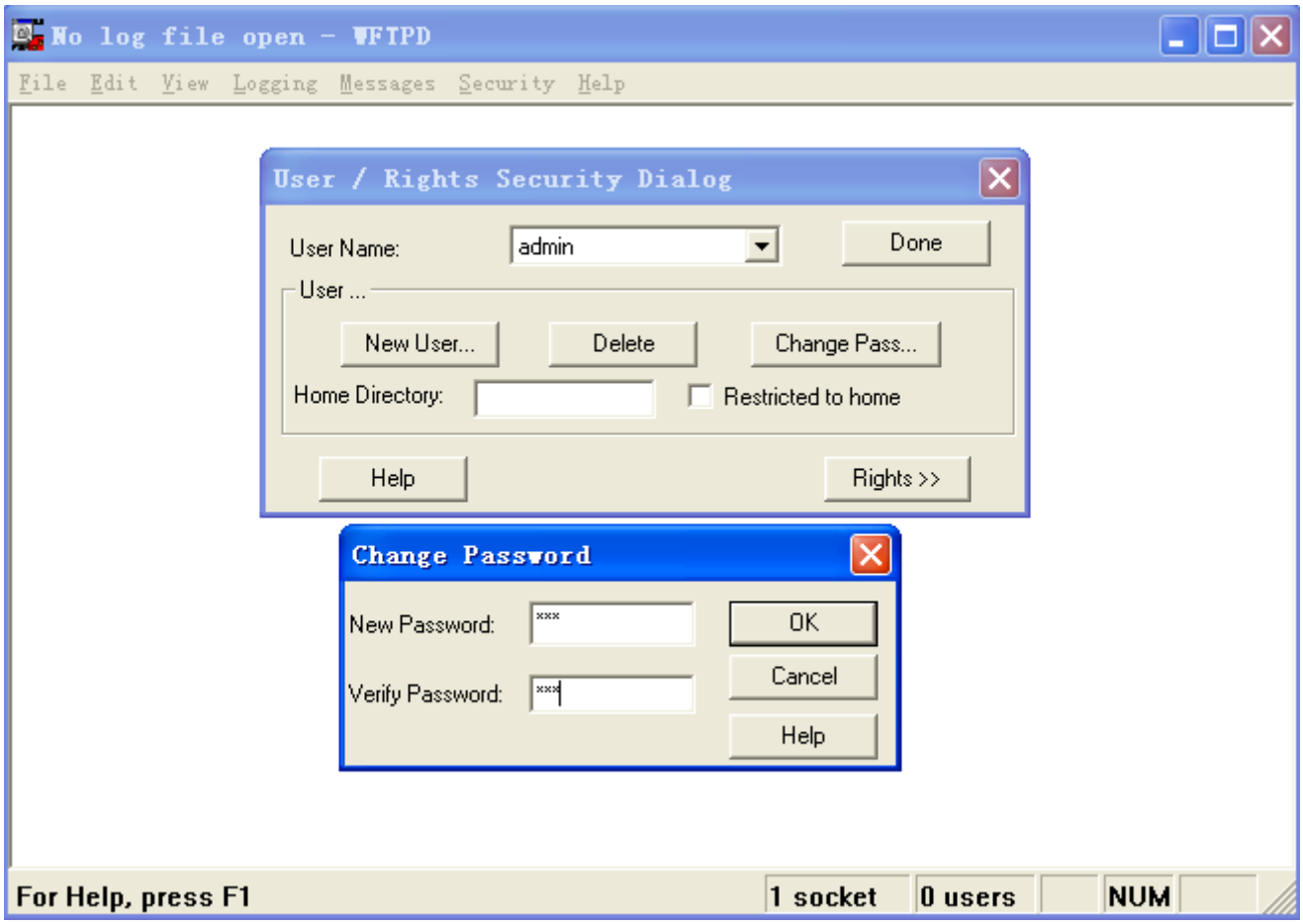


Рисунок 31 Создание нового пользователя FTP

2. Введите путь хранения файла обновления в Home Directory, как показано ниже. Щелкните <Done>.

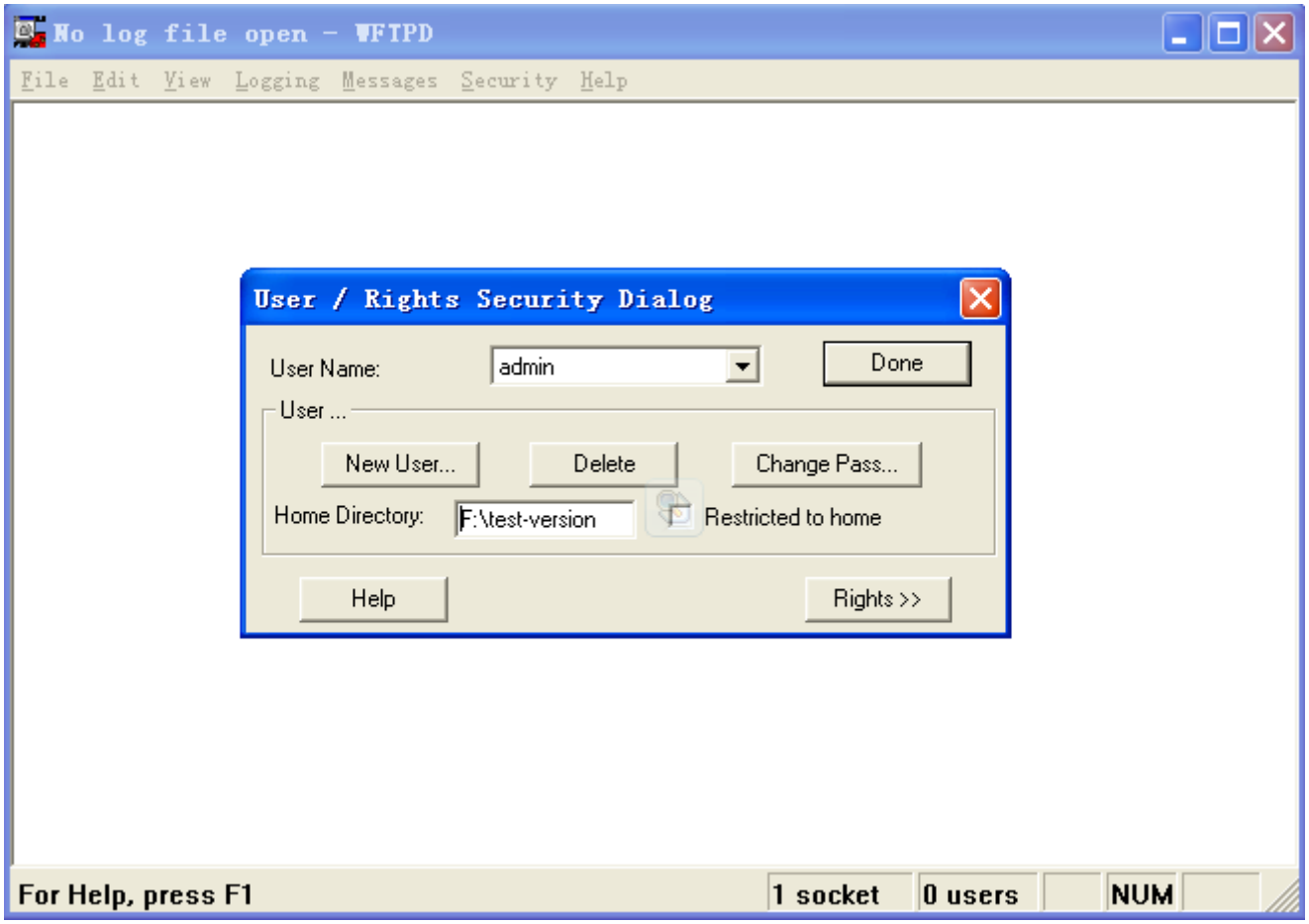


Рисунок 32 Местоположение файла

3. Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите [Firmware] и перейдите на страницу обновления. Затем выберите сервер FTP, как показано на рисунке ниже, введите IP-адрес FTP, имя пользователя, пароль и имя фала на сервере, щелкните кнопку <SEND>.

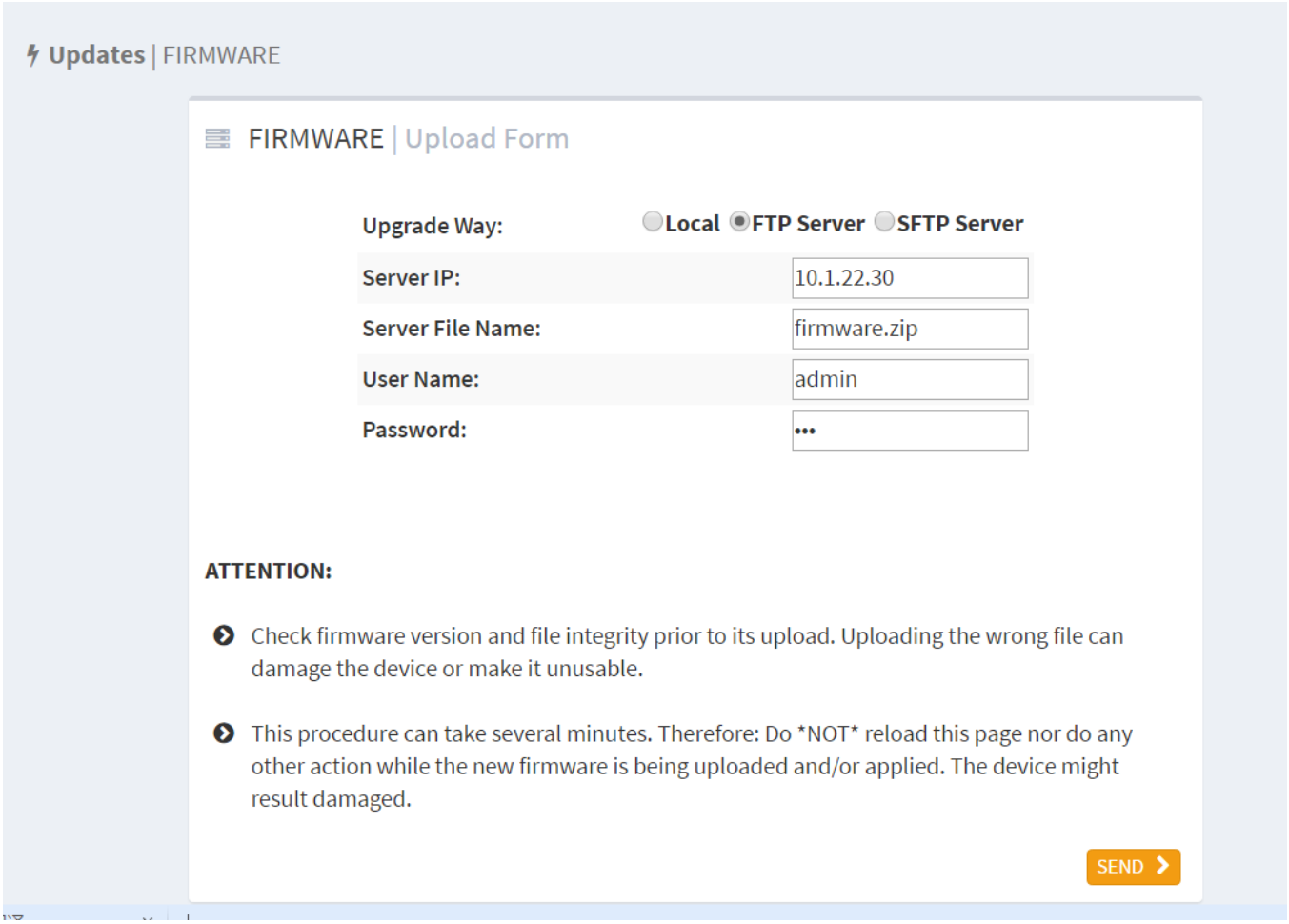


Рисунок 33 Обновление по FTP

WARNING	**Предупреждение**: Имя файла обновления по умолчанию firmware.zip, имя файла можно изменить, но расширение имени должно быть zip, в противном случае обновление не удастся.

4. Убедитесь в наличии нормальной связи между FTP-сервером и коммутатором, как показано ниже.

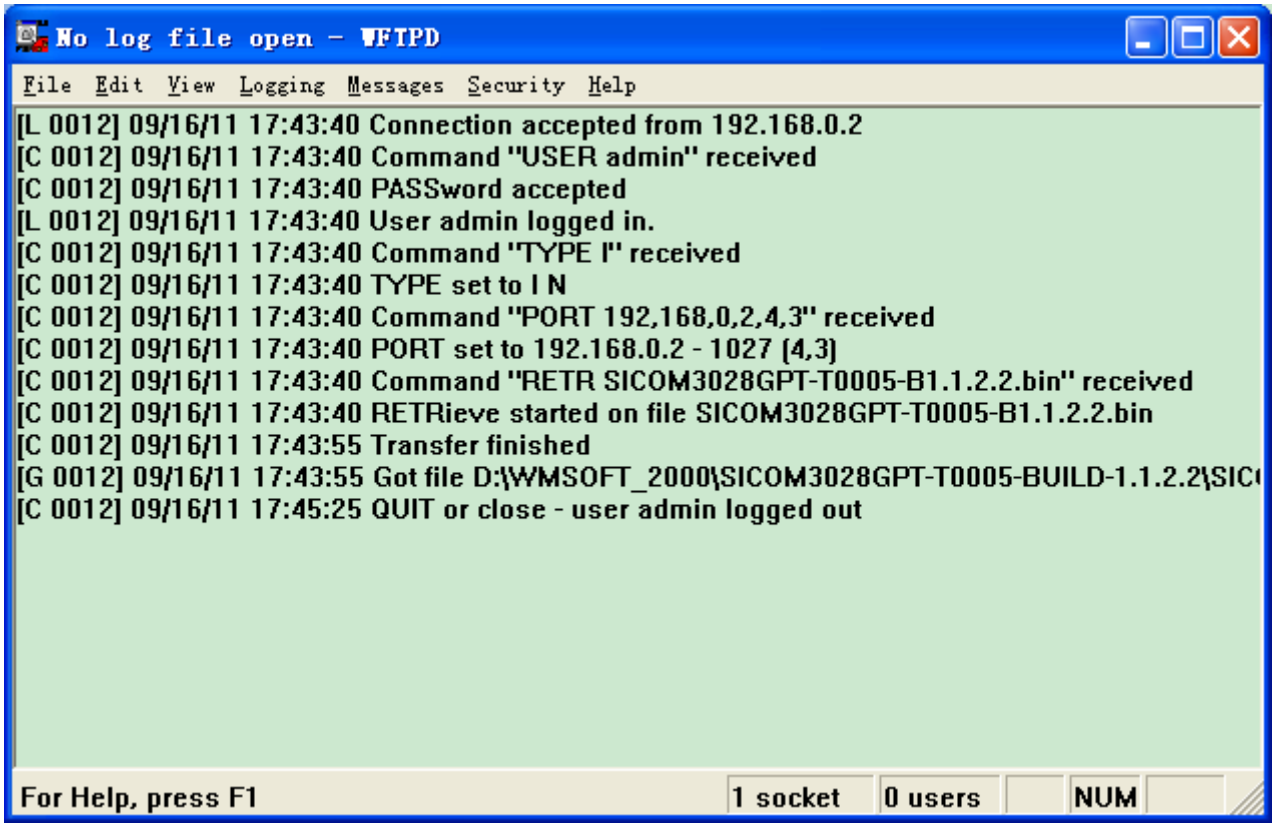


Рисунок 34 Нормальная связь между FTP-сервером и коммутатором

CAUTION	**Предостережение**: Чтобы отобразить информацию журнала обновлений, как показано на рисунке 34, нужно щелкнуть [Logging] → [LogOptions] в WFTPD и выбрать Enable Logging и информацию журнала для отображения.

5. Ход обновления показан на рисунке ниже.

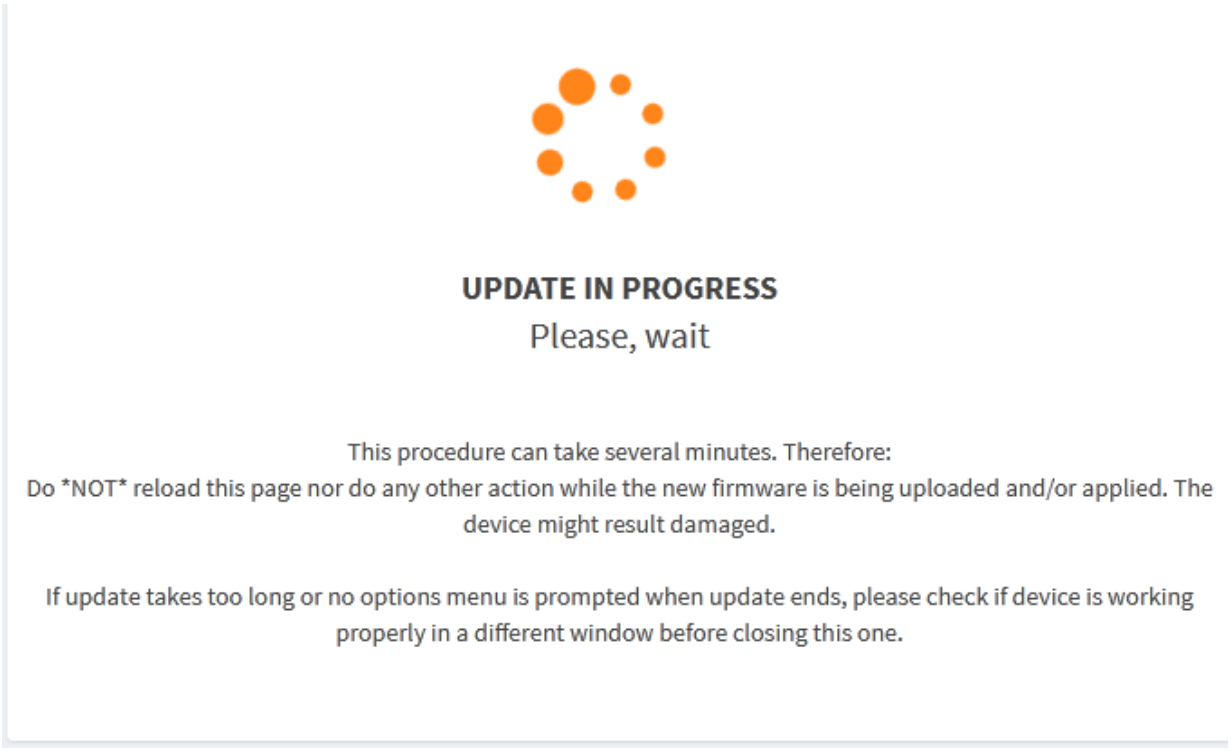


Рисунок 35 Обновление по FTP

6. Завершение обновления показано на рисунке ниже.

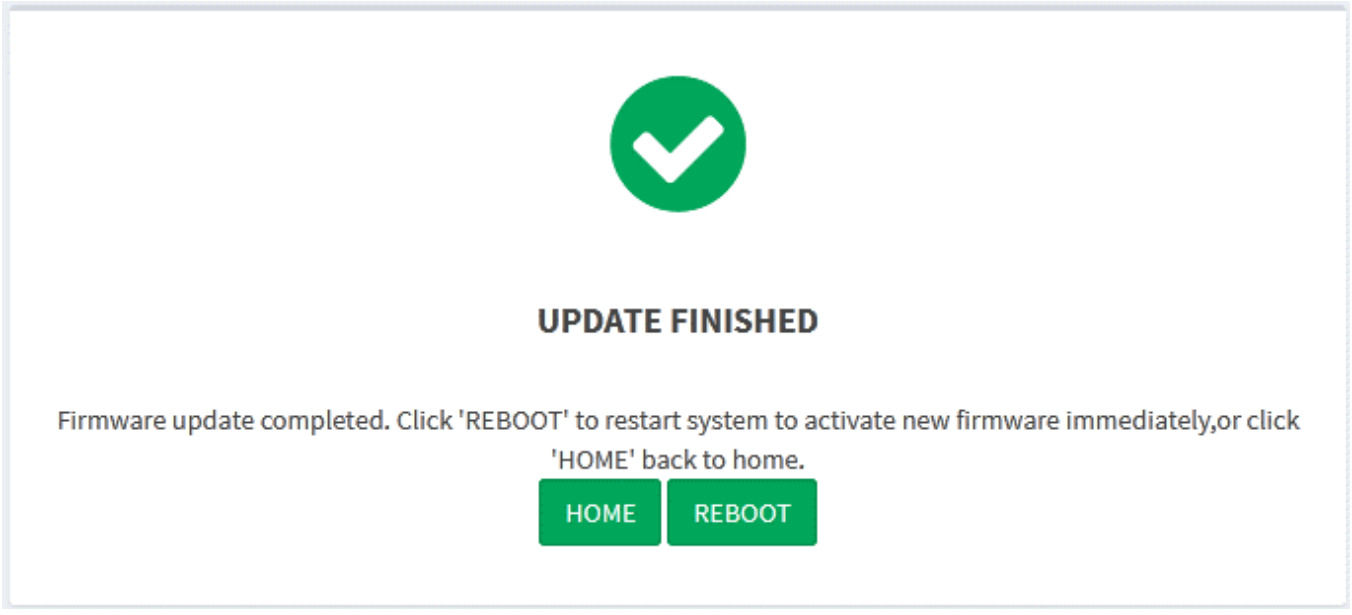


Рисунок 36 Обновление по FTP завершено

После завершения обновления можно выбрать [HOME] и [REBOOT]. Новая версия будет доступна только после перезагрузки устройства. Проверьте, является ли версия прошивки последней.

WARNING	**Предупреждение**: Во время обновления прошивки FTP-сервер должен продолжать работать. После успешного обновления прошивки необходимо перезагрузить коммутатор, чтобы новая прошивка заработала. Не перезапускайте коммутатор, если обновление не удалось, чтобы избежать потери файла, что может привести к невозможности запуска коммутатора.

4.5.3 Обновление по SFTP

Протокол безопасной передачи файлов (SFTP) — это протокол передачи файлов на основе SSH. Он обеспечивает зашифрованную передачу файлов для гарантии безопасности.

В следующем примере MSFTP используется для описания конфигурации сервера SFTP и процесса обновления прошивки.

1. Добавьте пользователя SFTP, как показано на рисунке 37. Введите пользователя и пароль, например, admin и 123. Установите номер порта 22. Введите путь для сохранения файла версии прошивки в поле Root path.

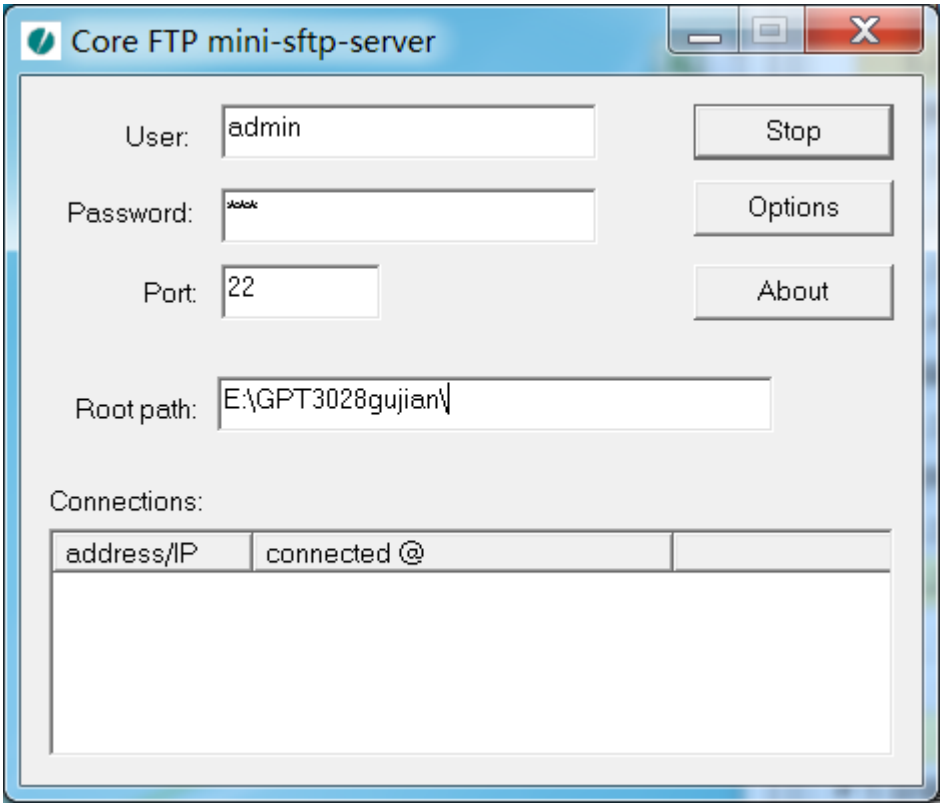


Рисунок 37 Добавление пользователя SFTP

2. Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите [Firmware] и перейдите на страницу обновления. Затем выберите сервер SFTP, как показано на рисунке ниже, введите IP-адрес SFTP, имя пользователя, пароль и имя фала на сервере, щелкните кнопку <SEND>.

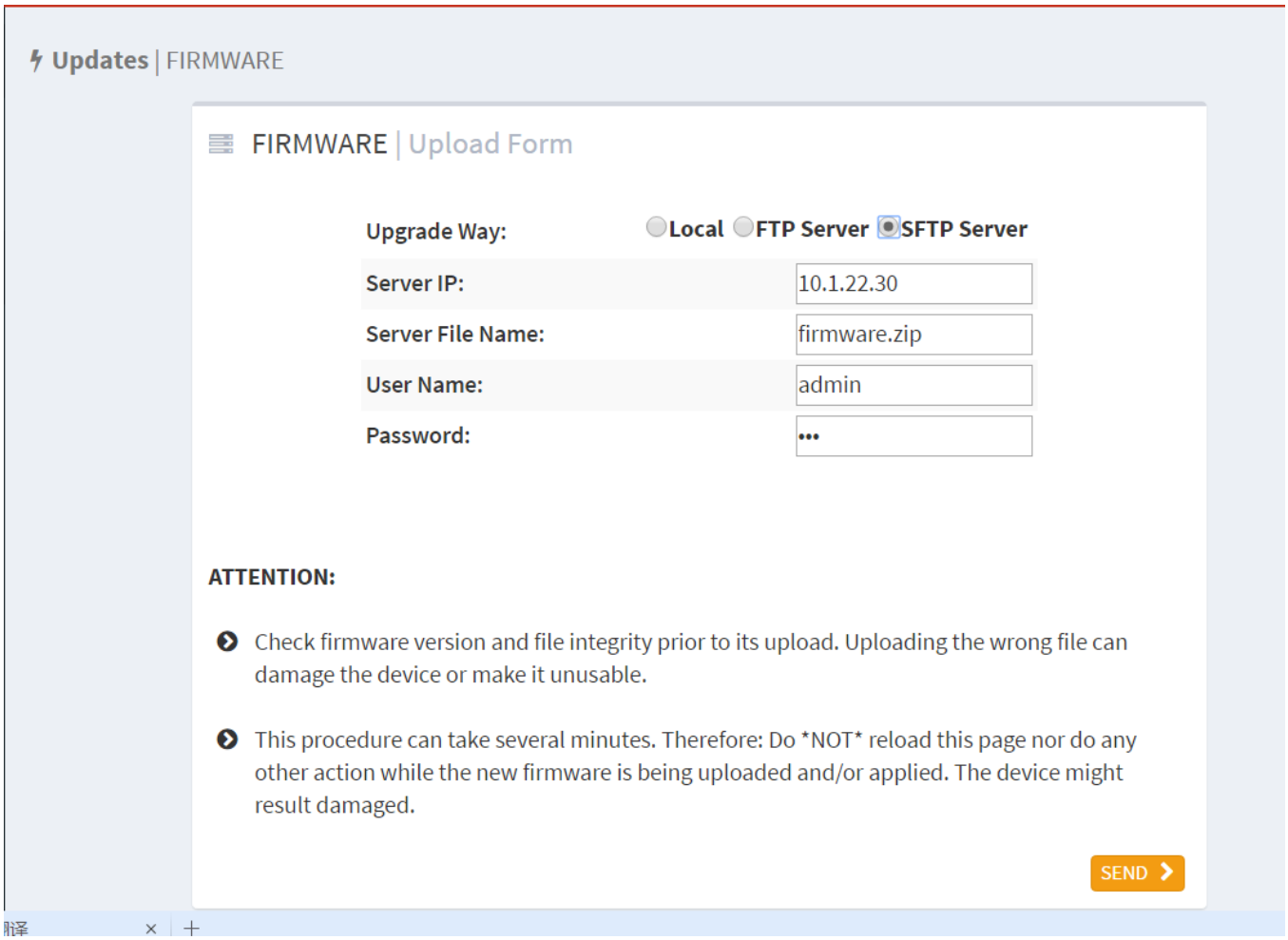


Рисунок 38 Обновление с сервера SFTP

WARNING	**Предупреждение**: Имя файла обновления по умолчанию firmware.zip, имя файла можно изменить, но расширение имени должно быть zip, в противном случае обновление не удастся.

3. Ход обновления показан на рисунке ниже.

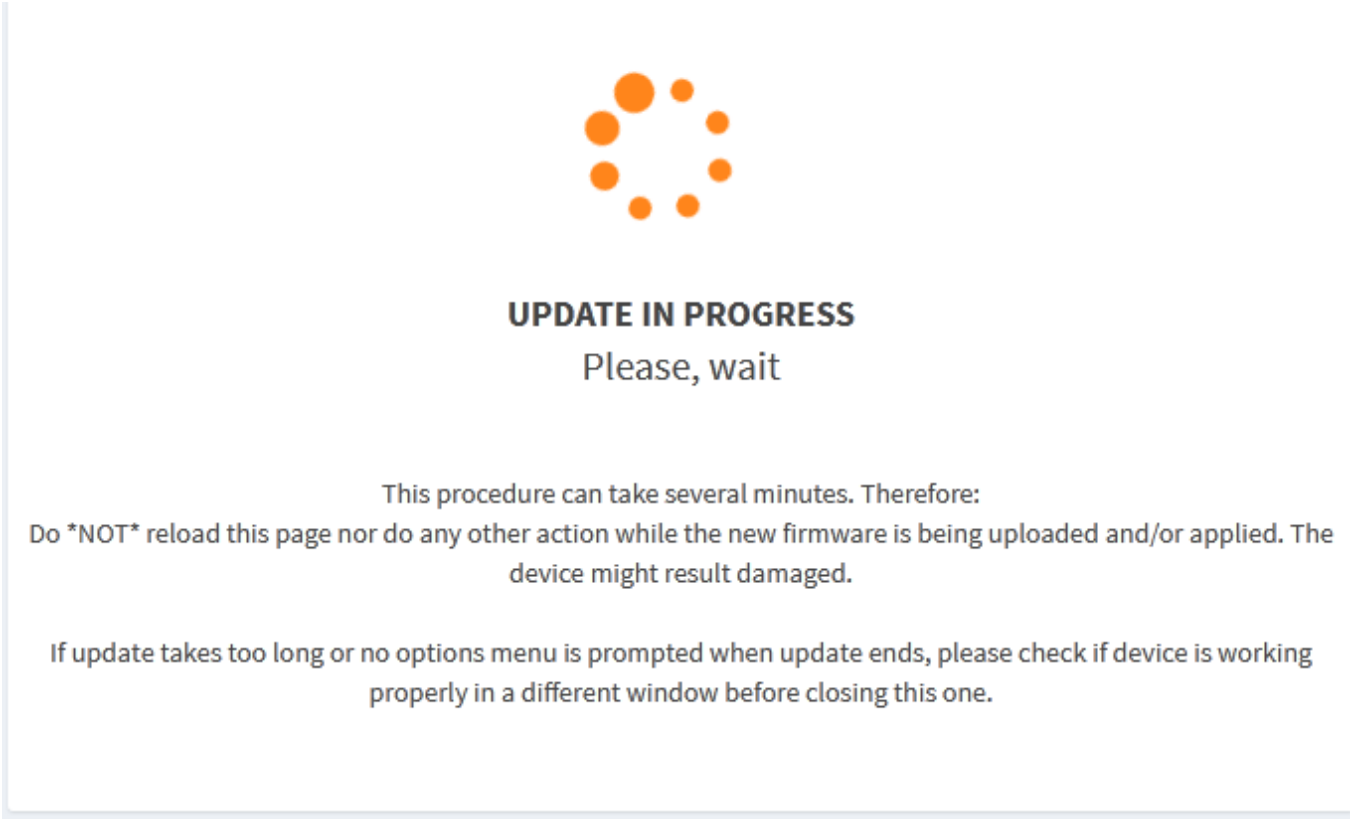


Рисунок 39 Обновление по SFTP

4. Завершение обновления показано на рисунке ниже.

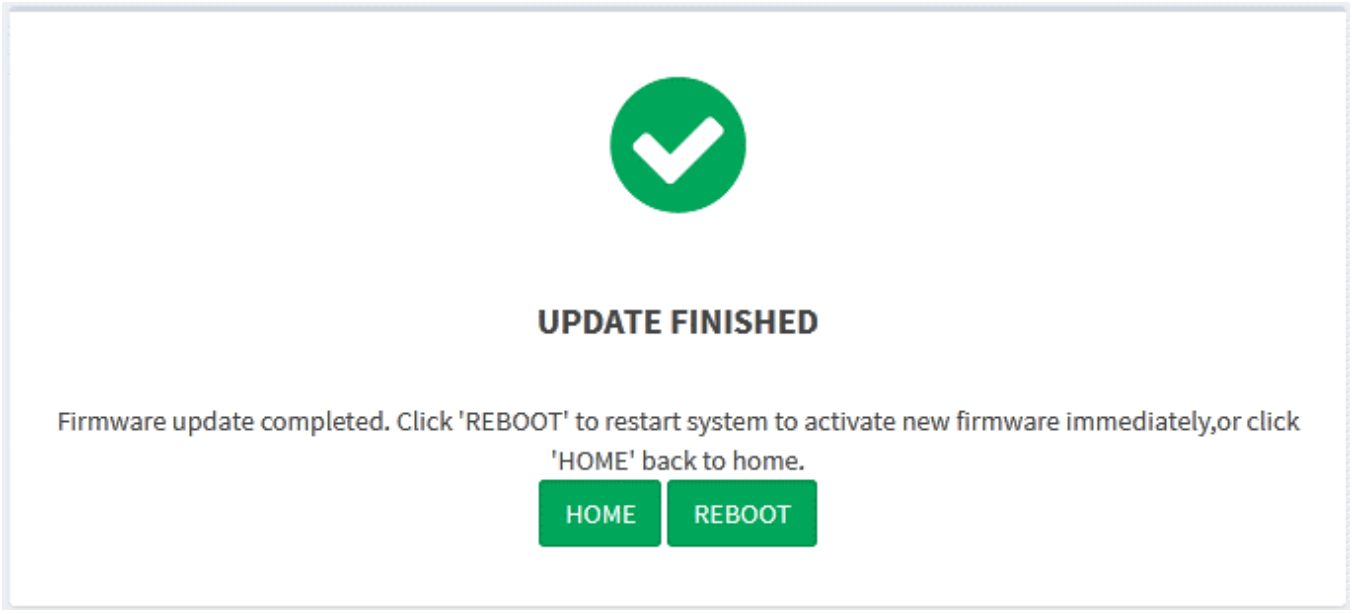


Рисунок 40 Обновление по SFTP завершено

5. После завершения обновления можно выбрать [HOME] и [REBOOT]. Новая версия будет доступна только после перезагрузки устройства. Проверьте, является ли версия прошивки последней.

WARNING	**Предупреждение**: Во время обновления прошивки FTP-сервер должен продолжать работать. После успешного обновления прошивки необходимо перезагрузить коммутатор, чтобы новая прошивка заработала. Не перезапускайте коммутатор, если обновление не удалось, чтобы избежать потери файла, что может привести к невозможности запуска коммутатора.

4.6 Выгрузка файла

Щелкните значок шестеренки в правом верхнем углу главной страницы, выберите [Configuration] в разделе [UPDATES], для выгрузки файла конфигурации локального сервера на коммутатор в качестве стартового файла коммутатора, как показано ниже.

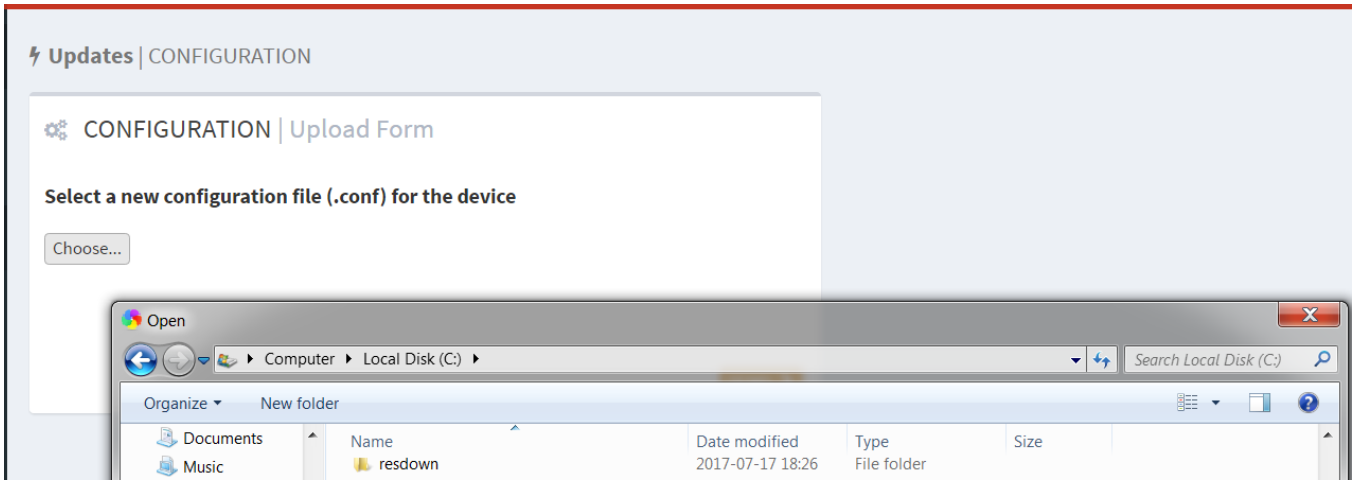


Рисунок 41 Выгрузка файла конфигурации

Выгруженный файл конфигурации сохраняется в каталоге коммутатора /etc/switch_service, и устройство запускается с файлом запуска start.conf в качестве файла запуска, включающего всю информацию о конфигурации коммутатора.

WARNING	**Предупреждение**: Выгруженный файл конфигурации должен быть текстовым файлом с расширением .conf.

4.7 Перезагрузка

При необходимости перезагрузки устройства щелкните значок шестеренки в правом верхнем углу главной страницы, выберите reboot. Устройство перезагрузится, как показано на рисунке ниже.

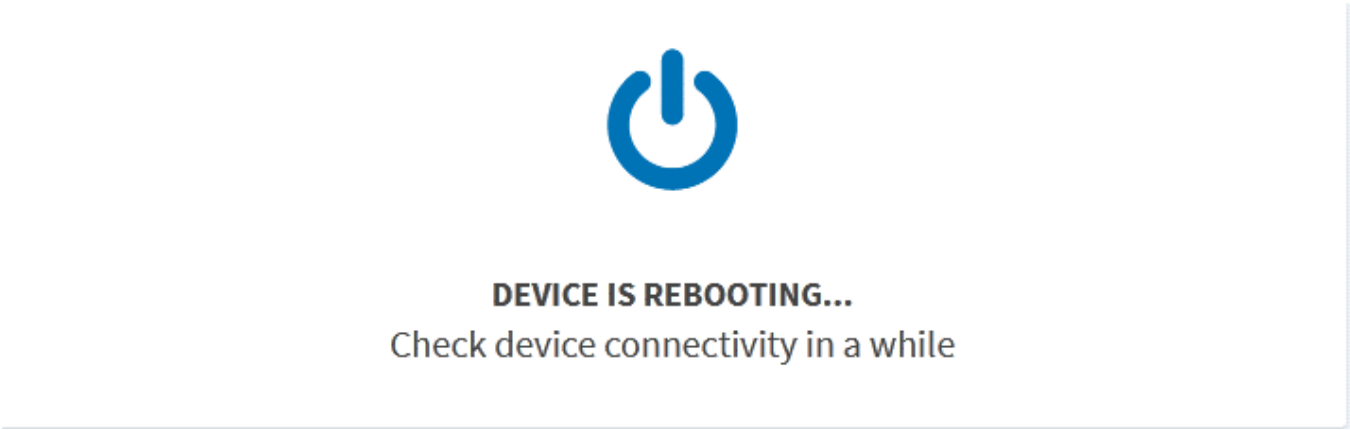


Рисунок 42 Перезагрузка

5 Функции

5.1 Резервирование

5.1.1 Принцип работы

Пояснение

SAN: singly attached node;

RedBox: Redundancy box, резервный коммутатор, который может соединять сети PRP и другие сети.

DANH: Двойной узел с HSR.

DANP: Двойной узел с PRP.

PRP

Основная идея PRP заключается в обеспечении резервирования системы через сетевые узлы, поддерживающие PRP, а основной принцип работы показан на следующем рисунке.

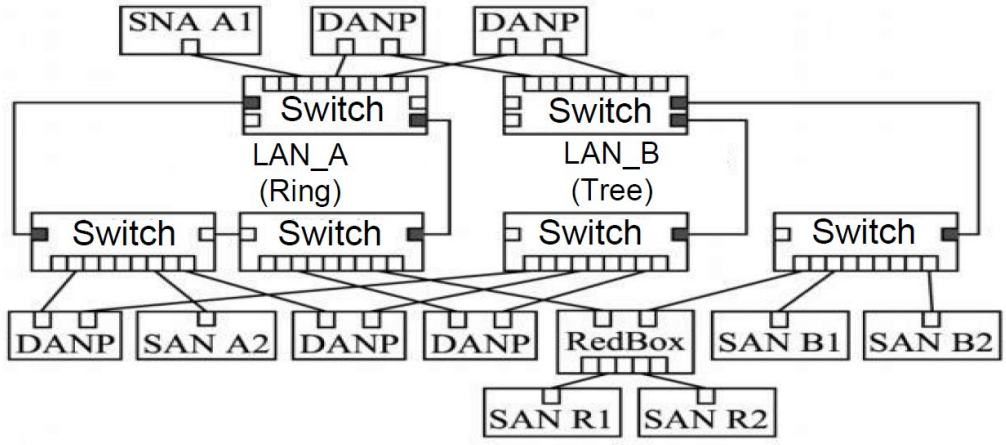


Рисунок 43 Принцип работы протокола PRP

SAN: Аббревиатура для Singly Attached Node. RedBox – это резервированный коммутатор, который может соединять сети PRP и другие сети. В схеме принципа работы протокола PRP каждый DANP подключается к двум отдельным параллельно работающим локальным сетям A и B одновременно, а сообщение копируется в 2 копии, отправляется отдельно через два полнодуплексных порта связи, а затем пересылается на DANP назначения по LAN A и B соответственно.

Кроме того, каждая независимая локальная сеть имеет различные структуры связи (например, древовидную структуру LAN B, структуру шины, кольцевую структуру LAN A, RSTP и т. д.) для улучшения резервирования системы. Узел SAN, не поддерживающий PRP, можно напрямую подключить к локальной сети (например, узел SANA1 на рисунке 43) без настройки или подключить к специальному RedBox, это также может обеспечить некоторое резервирование. Принцип работы портов PRP показан на рисунке 44. Два параллельных рабочих порта (порт A и порт B) одновременно подключаются к объекту резервирования. Когда он получает сетевые кадры из протокола UDP или протокола TCP, кадры копируются в 2 копии и отправляются одновременно из двух портов передачи (T), объект резервирования получателя отправляет пришедшие первыми кадры этих двух кадров от принимающих портов (Rx) к UDP или TCP, более поздние кадры отбрасываются. Очевидно, что этот механизм делает параллельное резервирование физического уровня прозрачным для протокола выше канального уровня, поэтому PRP совместим с другими протоколами верхнего уровня, такими как RSTP, VLAN. Кроме того, объект с резервированием канала также регулярно отправляет сообщение мониторинга сети, которое используется для обнаружения разрыва сети и других неисправностей.

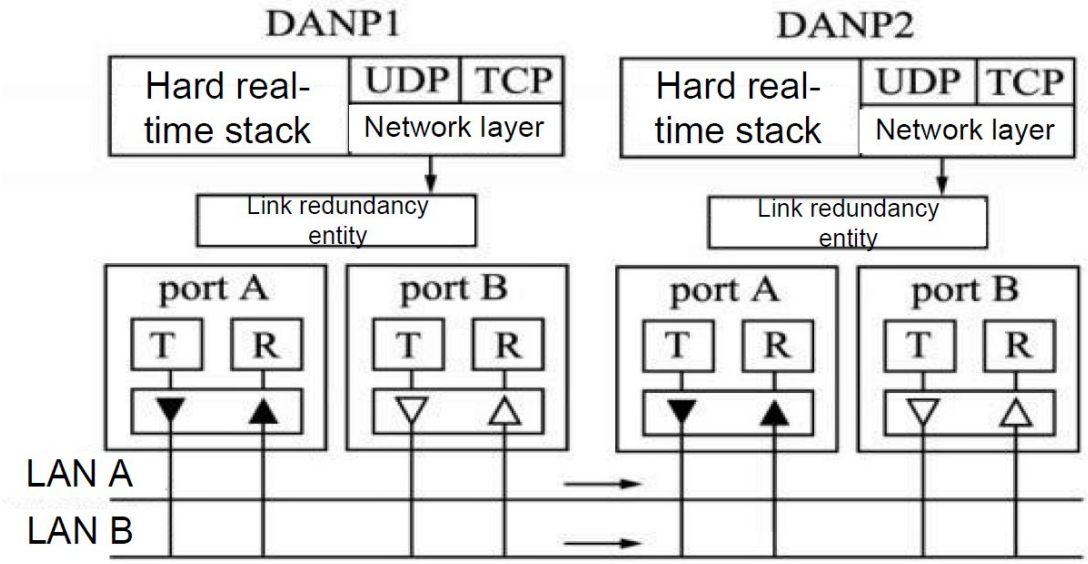


Рисунок 44 Принцип работы протокола PRP

HSR

HSR аналогичен базовой идее PRP, он также обеспечивает резервирование системы двумя независимыми физическими портами, но структура сети является кольцевой, и принцип ее работы показан ниже.

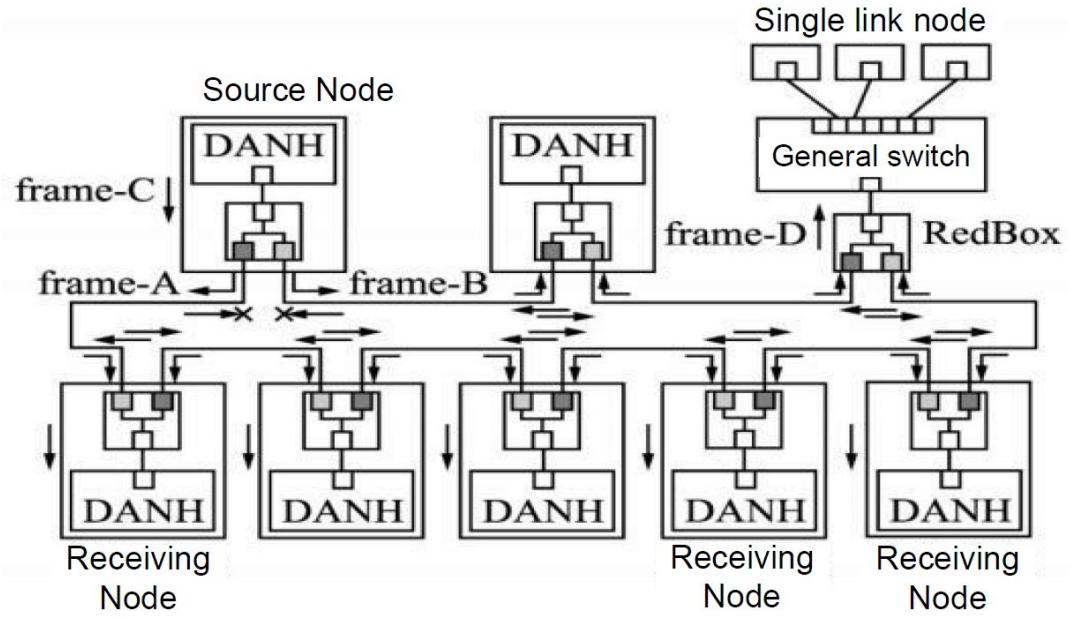


Рисунок 45 Принцип работы протокола HSR

DANH: Поддержка HSR, аббревиатура для узла с двойным присоединением с PRP; Frame A, Frame B и Frame C — это номер кадра.

Предположим, что исходный узел DANH получает один кадр из верхнего протокола как кадр C, копирует его в 2 копии, добавляет теги как кадр A и кадр B и отправляет отдельно. DANH в петле получает кадр A из порта, проверяет, является ли это широковещательным кадром, если да, то получает и пересылает, в противном случае проверяет, является ли его MAC-адрес канала назначения адресом этого узла; если нет, то он пересылается с другого порта на следующий узел, если да, то проверяется, прибыл ли кадр B первым; если приходит кадр B, то кадр A отбрасывается, в противном случае кадр A упаковывается и отправляется в верхний протокол для обработки. Когда кадр A возвращается в порт исходного узла, узел определяет, что это кадр, отправленный им самим, и отбрасывает его, избегая таким образом циклического шторма. Принцип передачи кадра B точно такой же, как и кадра A. Таким образом, каждый кадр протокола верхнего уровня копируется в 2 копии, передается в разных направлениях в цикле, разрыв в любой одна точке влияет только на передачу в одном направлении, другое направление не затрагивается, время для восстановления сети не требуется, этот механизм также полностью прозрачен для протокола верхнего уровня. HSR также отправит сообщение мониторинга сети. Если порт не получает сообщение мониторинга в течение длительного времени, определяется, что подключенная сеть повреждена. Для устройств, не поддерживающих HSR, доступ к сети HSR можно получить через RedBox.

5.1.2 Настройка через веб-интерфейс

Щелкните в дереве навигации [Functions]→[Redundancy], перейдите на страницу настройки резервирования, как показано на рисунке ниже.

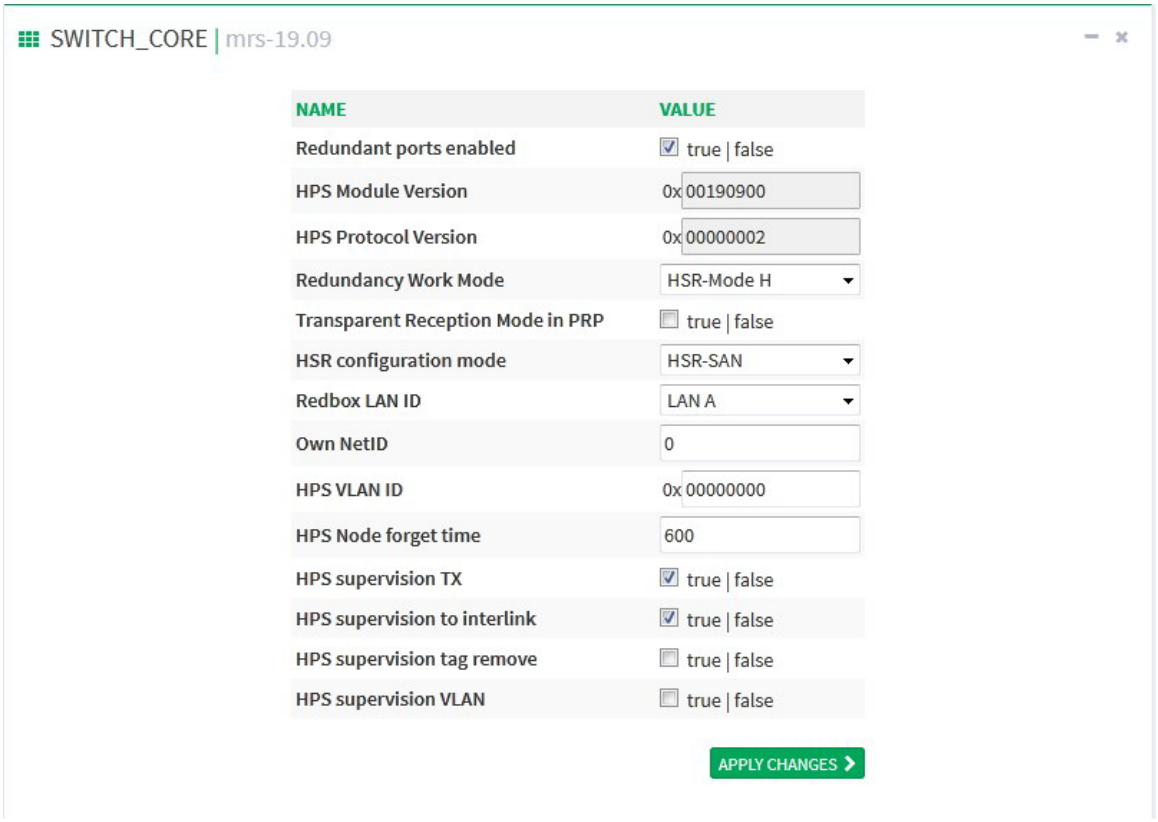


Рисунок 46 Страница настройки резервирования

Redundant ports enabled

Варианты конфигурации: true/false

Конфигурация по умолчанию: true

Функция: При включении порт работает как порт резервирования, порт не является общим портом Ethernet.

HPS Module Version

Функция: показ текущей версии модуля HPS

HPS Protocol Version

Функция: показ текущей версии протокола резервирования HSR-PRP

Redundancy Work Mode

Варианты конфигурации: PRP-Duplicate discard mode/PRP-Duplicate accept mode/HSR-Mode H/HSR-Mode N/HSR-Mode T/HSR-Mode U/HSR-Mode X

Конфигурация по умолчанию: HSR-Mode H

Функция: PRP-Duplicate discard mode: приемник в этом режиме может обнаруживать повторяющиеся элементы, передатчик LRE присоединяет шестибайтовое поле после двух кадров, оно содержит серийный номер, который является хвостом управления резервированием (RCT). Приемник LRE использует серийный номер RCT и MAC-адрес источника для обнаружения дублированных элементов. Он пересылает на верхний уровень только первый кадр в паре. Все устройства в сети PRP должны быть переведены в режим prp-duplicate-discard, как показано на рисунке 48, Конфигурация PRP.

PRP-Duplicate accept mode: этот режим используется в целях тестирования, чтобы убедиться, что повторяющиеся элементы действительно отбрасываются канальным уровнем, а не протоколом высокого уровня. В этом режиме передатчик настроен на отправку двух кадров без RCT. Приемник настроен на прием двух кадров и пересылку их (если оба приходят) на свой верхний уровень.

HSR-Mode H: этот режим является обязательной опцией и является режимом по умолчанию, в основном для пересылки кадров данных с тегом HSR. В этом режиме, за исключением кадров, отправленных самим узлом, DANH вставляет тег HSR и перенаправляет трафик кольцевой сети. Дубликат кадра и кадр, в котором узел является пунктом назначения одноадресной рассылки, не будут пересылаться. Все устройства в сети HSR должны быть переведены в режим HSR-H, как показано на рисунке 49, Типовая схема сети HSR.

HSR-Mode N: Это дополнительный режим, без переадресации. В этом режиме поведение узла аналогично режиму H, отличие состоит в том, что узел не должен пересылать сетевой трафик между портами.

HSR-Mode T: Это дополнительный режим, с прозрачной переадресацией. В этом режиме DANH должен сначала удалить тег HSR, а затем переслать кадр на другой порт и отправить кадр с хоста на оба порта без тега и без удаления дубликатов.

HSR-Mode U: Это дополнительный режим, с одноадресной переадресацией. В этом режиме поведение узла аналогично режиму H, отличие состоит в том, что узел должен пересылать трафик одноадресной рассылки в качестве пункта назначения, как при многоадресной рассылке.

Transparent Reception Mode in PRP

Варианты конфигурации: true/false

Конфигурация по умолчанию: false

Функция: После включения режима дубликат кадра не отбрасывается и RTC не стирается.

HSR configuration mode

Варианты конфигурации: HSR-SAN/HSR-HSR/HSR-PRP

Конфигурация по умолчанию: HSR-SAN

Функция: в HSR определяет режим настройки Redbox: HSR-SAN, HSR-PRP или HSR-HSR.

RedBox LAN ID

Варианты конфигурации: LAN A/LAN B

Конфигурация по умолчанию: LAN A

Функция: определяет LAN ID Redbox A или B, используемый в режиме HSR-PRP.

Own NetID

Диапазон настройки: 3 бита [0-7]

Конфигурация по умолчанию: 0

Функция: Это идентификационный номер кольцевой сети, к которой подключен узел.

HPS VLAN ID

Диапазон настройки: 12 бит[00-FFF]

Конфигурация по умолчанию: 00000000

Функция: используется для определения VLAN ID узлов Redbox.

HPS Node forget time

Диапазон настройки: 10 бит [0-1023] ед. изм. – секунда

Конфигурация по умолчанию: 600 с

Function: время, по истечении которого узел удаляется из таблицы узлов. По умолчанию задано значение 600 с.

HPS supervision TX

Варианты конфигурации: true/false

Конфигурация по умолчанию: true

Функция: включение или отключение передачи кадров контроля.

HPS supervision to interlink

Варианты конфигурации: true/false

Конфигурация по умолчанию: true

Функция: передача кадра контроля на межканальный порт.

HPS supervision tag remove

Варианты конфигурации: true/false

Конфигурация по умолчанию: false

Функция: Удаление заголовка HSR или хвоста PRP кадра контроля при передаче на межканальный порт.

HPS supervision VLAN

Варианты конфигурации: true/false

Конфигурация по умолчанию: false

Функция: Обработка кадра контроля с VLAN.

5.1.3 Пример типовой конфигурации

Три типовых конфигурации: Сеть PRP, сеть HSR и сеть QUADBOX.

Типовая сеть PRP

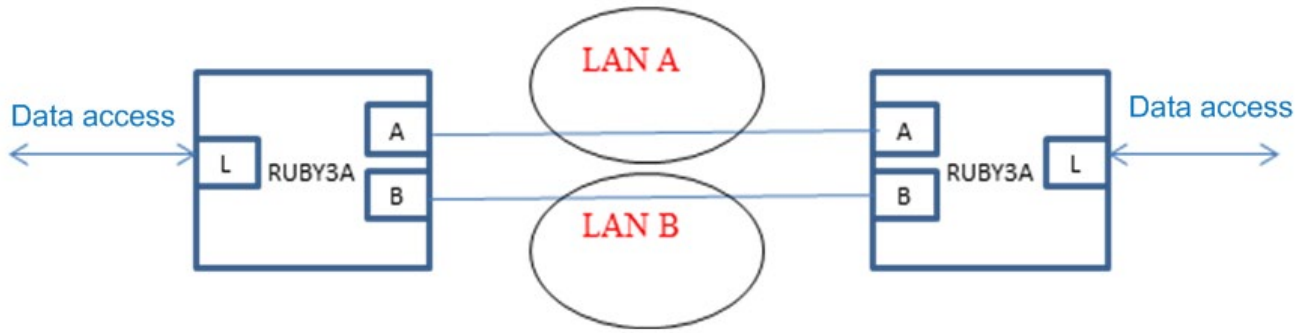


Рисунок 47 Типовая сеть PRP

Примечания в отношении сети:

Для всех устройств в сети PRP должен быть установлен режим prp-dublicate-discard. Рекомендуется, чтобы порт A подключался к порту A на другом конце, порт B подключался к порту B на другом конце. Там, где A-A может проходить через LAN A, B-B может проходить через LAN B. Обратите внимание, что LAN A и LAN B должны быть независимы.

В сети PRP данные между портами A и B не будут добавляться в другие заголовки, поэтому всеми устройствами между LAN A и LAN B можно управлять с помощью Ruby3a (в отличие от HSR). Настройка через веб-интерфейс показана ниже.

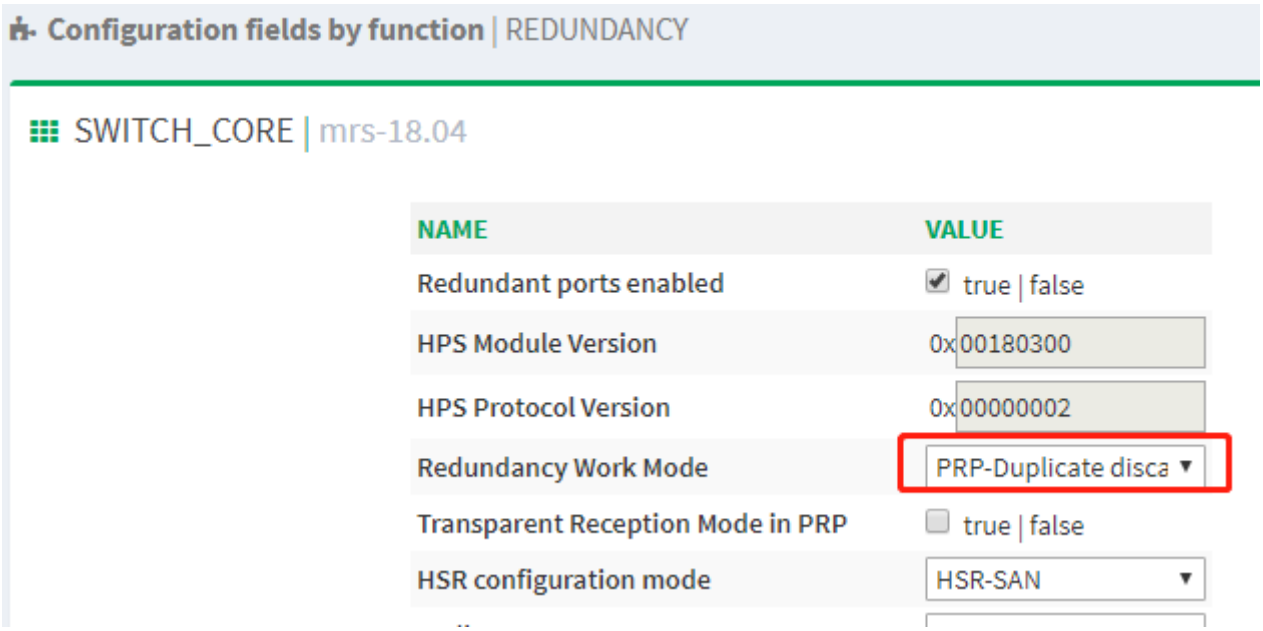


Рисунок 48 Настройка PRP

Типовая сеть HSR

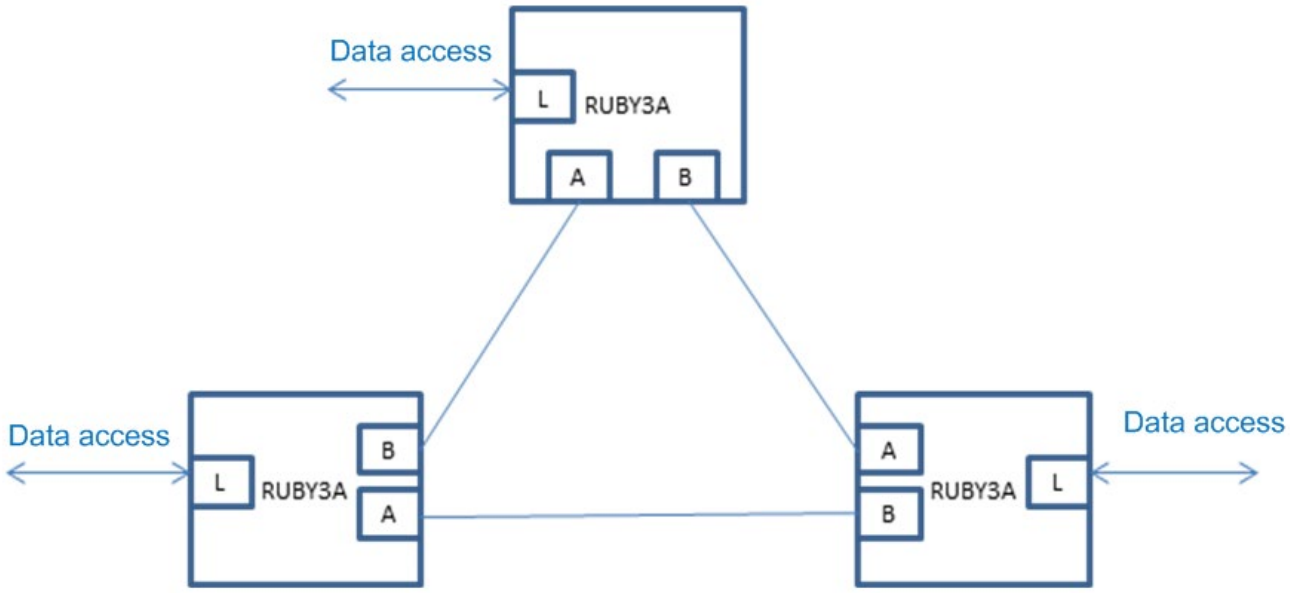


Рисунок 49 Типовая сеть PRP

Примечания в отношении сети:

Для всех устройств в сети HSR должен быть установлен режим HSR-H. Рекомендуется, чтобы порт A подключался к порту B на другом конце, а порт B подключался к порту A на другом конце по кольцу.

Примечание: Точки соединения между устройствами могут осуществлять прозрачную передачу с использованием других устройств, но учтите, что, поскольку все данные между устройствами HSR добавляются с помощью заголовков HSR, удаленное управление ими невозможно, если между устройствами добавлены устройства прозрачной передачи. Настройка через веб-интерфейс показана ниже.

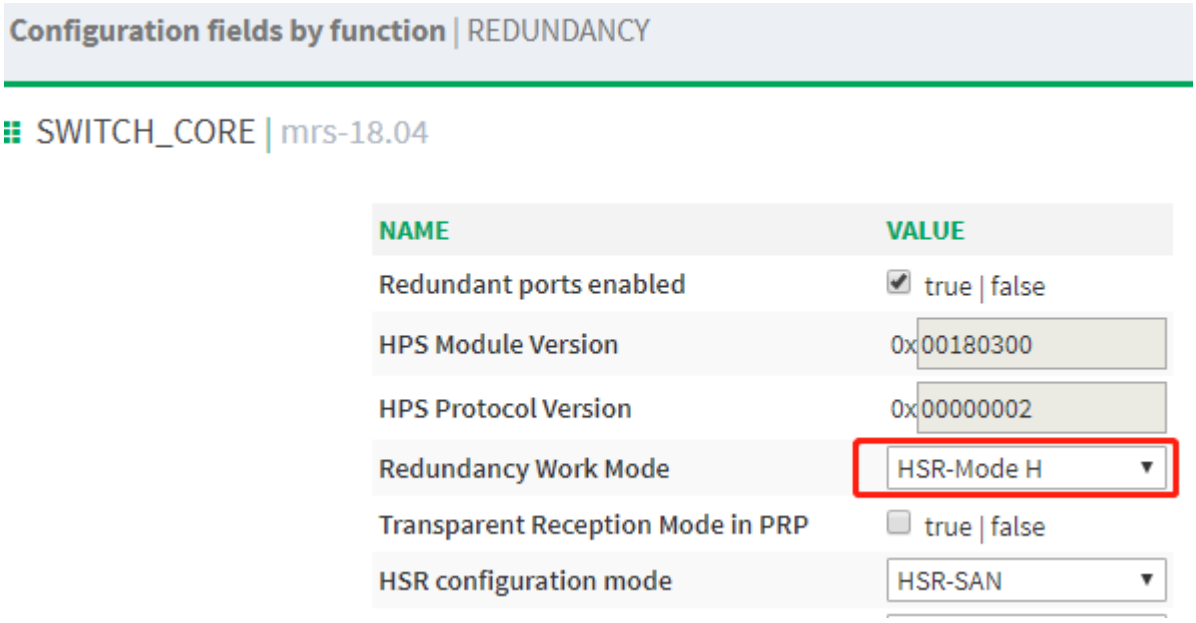


Рисунок 50 Настройка HSR

Типовая сеть QUADBOX

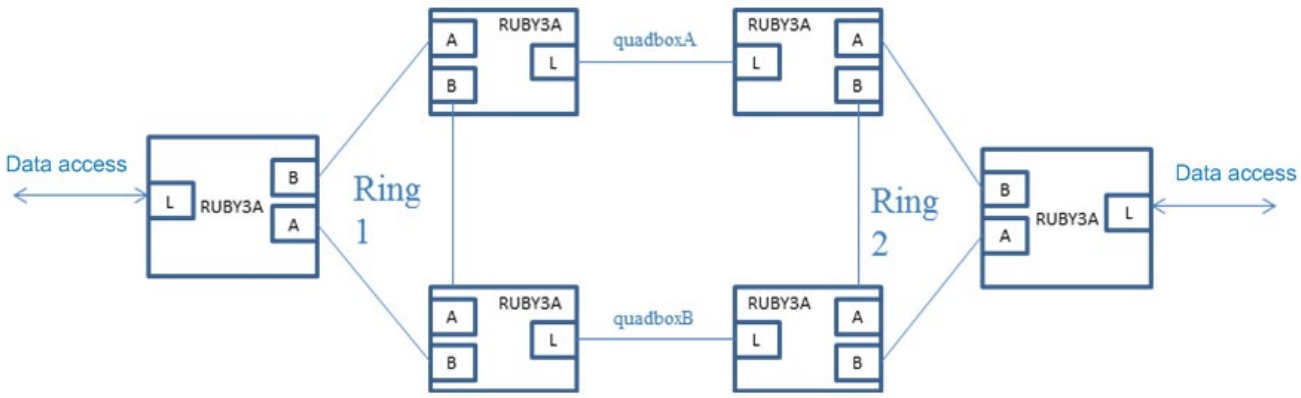


Рисунок 51 Типовая сеть QUADBOX

Примечания в отношении сети:

Преимущество сети Quadbox заключается в том, что два кольца HSR могут защищать друг друга, то есть защита 1 к 1 повышена до защиты 4 к 1. Если подключения quadboxA и quadboxB настроены на необходимость использования протокола HSR, 3 порта 4 устройств, образующих quadboxA и quadboxB, становятся резервными портами HSR.

Для всех устройств в сети Quadbox должен быть установлен режим HSR-H (режим по умолчанию), а межканальный порт, который используется для подключения QuadboxA и QuadboxB, должен быть настроен на работу в режиме HSR-HSR. Настройка через веб-интерфейс показана ниже.

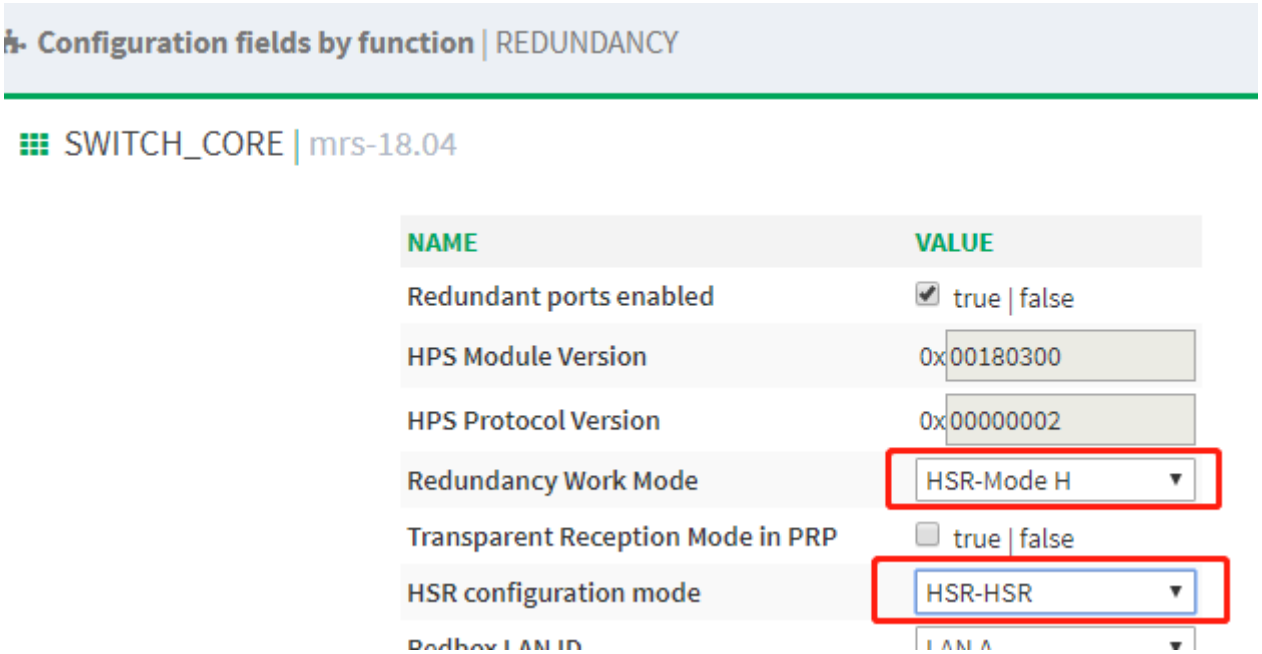


Рисунок 52 Настройка QUADBOX

5.2 PTP

5.2.1 Введение

PTP (протокол точного времени) синхронизирует часы, работающие независимо на отдельных узлах системы измерения и управления, по протоколу высокой точности. Протокол синхронизации включает как фазовую, так и частотную синхронизацию, точность синхронизации может достигать ±100 нс.

5.2.2 Основные понятия

1. Домен PTP

Сеть, применяющая протокол PTP, является доменом PTP. В домене PTP есть только одни самые современные часы, и остальные устройства в домене синхронизируются с этими часами.

2. Порт PTP

Порт, на котором включен протокол PTP, является портом PTP.

3. Узел часов

Узел в домене PTP является узлом часов, протокол PTP определяет следующие основные узлы часов:

OC (Ordinary Clock) Обычные часы

Этот узел имеет только один порт PTP в домене PTP, участвующий в синхронизации часов, и синхронизирует время от вышестоящего узла или публикует время на нисходящем узле через этот порт.

BC (Boundary Clock) Граничные часы

Этот узел имеет один или несколько портов PTP в домене PTP, участвующих в синхронизации часов.

Когда в синхронизации часов участвует только один порт PTP, время синхронизируется с вышестоящим узлом или публикуется на нисходящем узле через этот порт. Когда в синхронизации часов задействовано несколько портов PTP, время синхронизируется от восходящего узла синхронизации через один из портов, а время публикуется на нисходящем узле через оставшиеся порты. Когда граничные часы используются в качестве источника часов, время может быть опубликовано на нижестоящем узле часов через несколько портов PTP.

TC (Transparent Clock) Прозрачные часы

Этому тактовому узлу не требуется поддерживать синхронизацию с другими узлами. На TC имеется несколько портов PTP, но эти порты только пересылают сообщения протокола PTP и корректируют задержку пересылки для них без синхронизации часов через какой-либо порт.

Прозрачные часы бывают двух типов:

E2ETC (End-to-End Transparent Clock): Непосредственная пересылка отличных от P2P сообщений в сети и расчет всей задержки канала.

P2PTC (Peer-to-Peer Transparent Clock): Непосредственная пересылка сообщений Sync, сообщений Follow_Up и сообщений Announce, завершение других сообщений протокола и расчет задержки каждого канала по всему каналу.

4. Для пары синхронных тактовых узлов существуют следующие отношения главный-подчиненный: Узел, который публикует синхронные часы, является главным узлом (master), а узел, который получает синхронные часы, является подчиненным узлом (slave).

Часы узла master являются ведущими часами, а часы узла slave — подчиненными.

Порт, который публикует синхронные часы, является главным портом (master), а порт, который получает синхронные часы, является подчиненным портом (slave).

5.2.3 Принципы синхронизации

1. Выбор оптимальных часов

Используя уровень часов, ID часов и другую информацию из сообщения Announce, каждый узел выбирает узел часов в качестве оптимальных часов для домена PTP. В этот момент также определяются отношения «главный-подчиненный» между каждым узлом и портом на каждом узле. С помощью этого процесса по домену PTP устанавливается связующее дерево с оптимальными часами в качестве корня. С этого момента главные часы будут регулярно отправлять сообщение подчиненным часам. Если в течение определенного периода времени подчиненные часы не получают сообщение Announce, отправленное главными часами, главные часы будут считаться недействительными, и выбор оптимальных часов возобновляется.

Сообщение Announce содержит достаточно информации, чтобы обеспечить выбор оптимальных часов. Сообщение содержит такие важные данные, как приоритет главных часов 1, уровень часов, точность часов, приоритет главных часов 2, идентификатор часов. При выборе оптимального тактового сигнала эта информация будет сравниваться поочередно Тактовый сигнал с меньшим уровнем приоритета основного тактового сигнала 1 будет выбран в качестве оптимального тактового сигнала; тактовый сигнал с меньшим уровнем тактового сигнала выбирается в качестве оптимального тактового сигнала, когда приоритет основного тактового сигнала 1 тот же. Аналогично, если вся предыдущая информация одинакова, в качестве оптимального тактового сигнала выбирается тактовый сигнал с меньшим идентификатором тактового сигнала.

2. Принципы синхронизации

Сообщение передается и синхронизируется между ведущими и ведомыми часами, а время отправки и получения сообщения записывается. Общая задержка между ведущими и ведомыми часами рассчитывается путем расчета разницы во времени прохождения сообщения туда и обратно. Если сетевой путь симметричен, однонаправленная задержка составляет половину общей задержки. Подчиненные часы могут синхронизироваться с главными часами, регулируя местное время в соответствии с отклонением главных и подчиненных часов и односторонней задержкой.

PTP поддерживает два механизма измерения задержки:

– механизм request_response: Измерение временной задержки для сквозного соединения всего канала.

– механизм peer-to-peer delay: Измерение задержки для двухточечного соединения, по сравнению с механизмом request_response, механизм peer-to-peer измеряет задержку каждого канала на всем канале.

5.2.4 Настройка через веб-интерфейс

Щелкните в дереве навигации [Functions]→[PTP], перейдите на страницу настройки PTP, как показано на ниже.

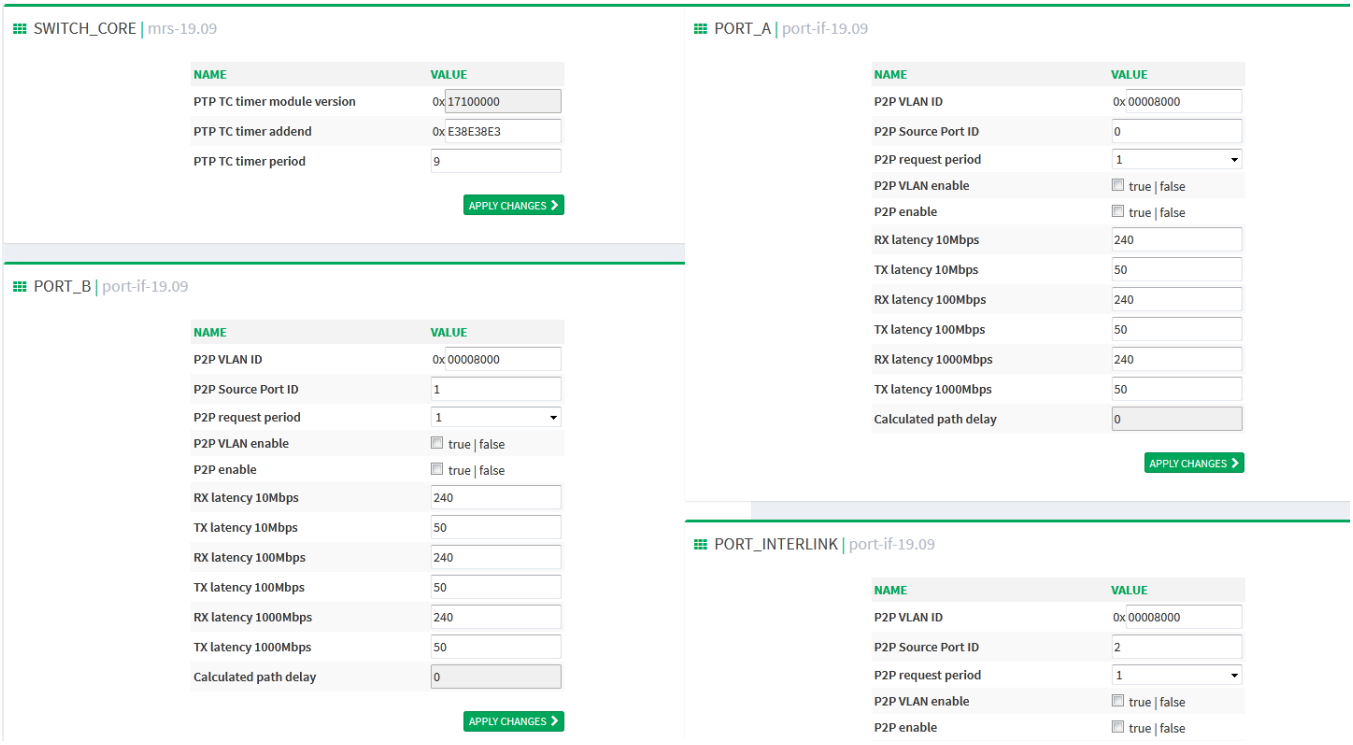


Рисунок 53 Страница настройки PTP

Как видно на рисунке 53, страница конфигурации PTP разделена на 4 части: страница конфигурации PTP TC и страница конфигурации ptp трех портов (port_a/port_b/port_interlin).

1. Настройка PTP TC

Страница настройки PTP TC показана ниже.

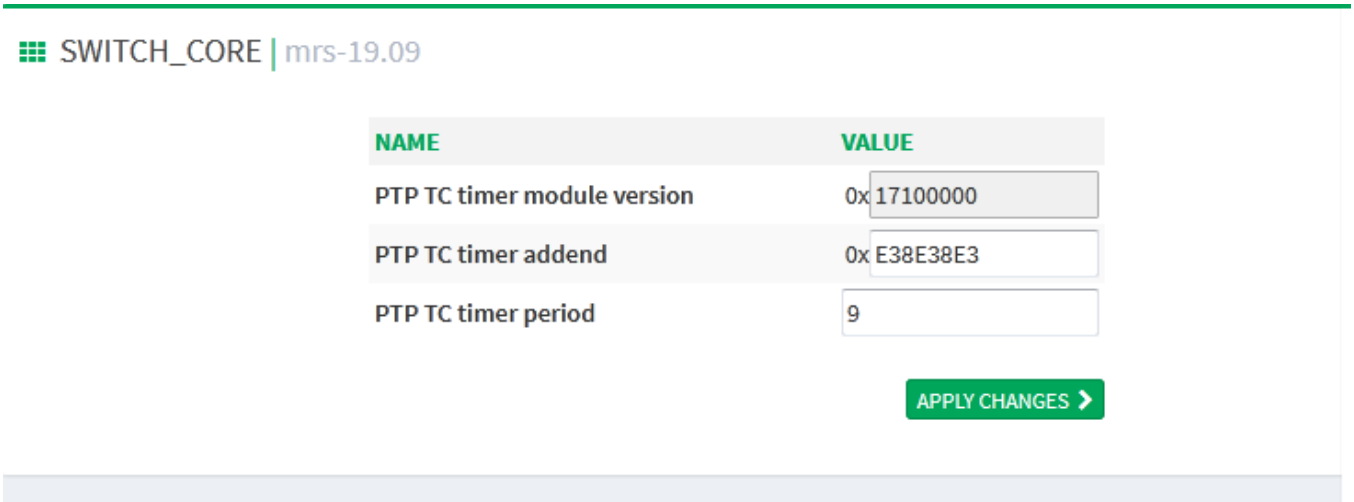


Рисунок 54 Страница настройки PTP TC

PTP TC timer module version

Описание: Версия модуля таймера TC IEEE1588.

PTP TC timer addend

Диапазон настройки: 32 бита [00-FFFFFFFF]

Конфигурация по умолчанию: E38E38E3

Функция: настройка таймера на уровне долей секунды (см. Freescale AN3423)

PTP TC timer period

Диапазон настройки: 32 бита [0-4294967295] Конфигурация по умолчанию: 9

Функция: см. Freescale AN3423.

2. Настройка порта PTP

Рассмотрим порт порт A в качестве примера. Страница настройки PTP порта A показана ниже.

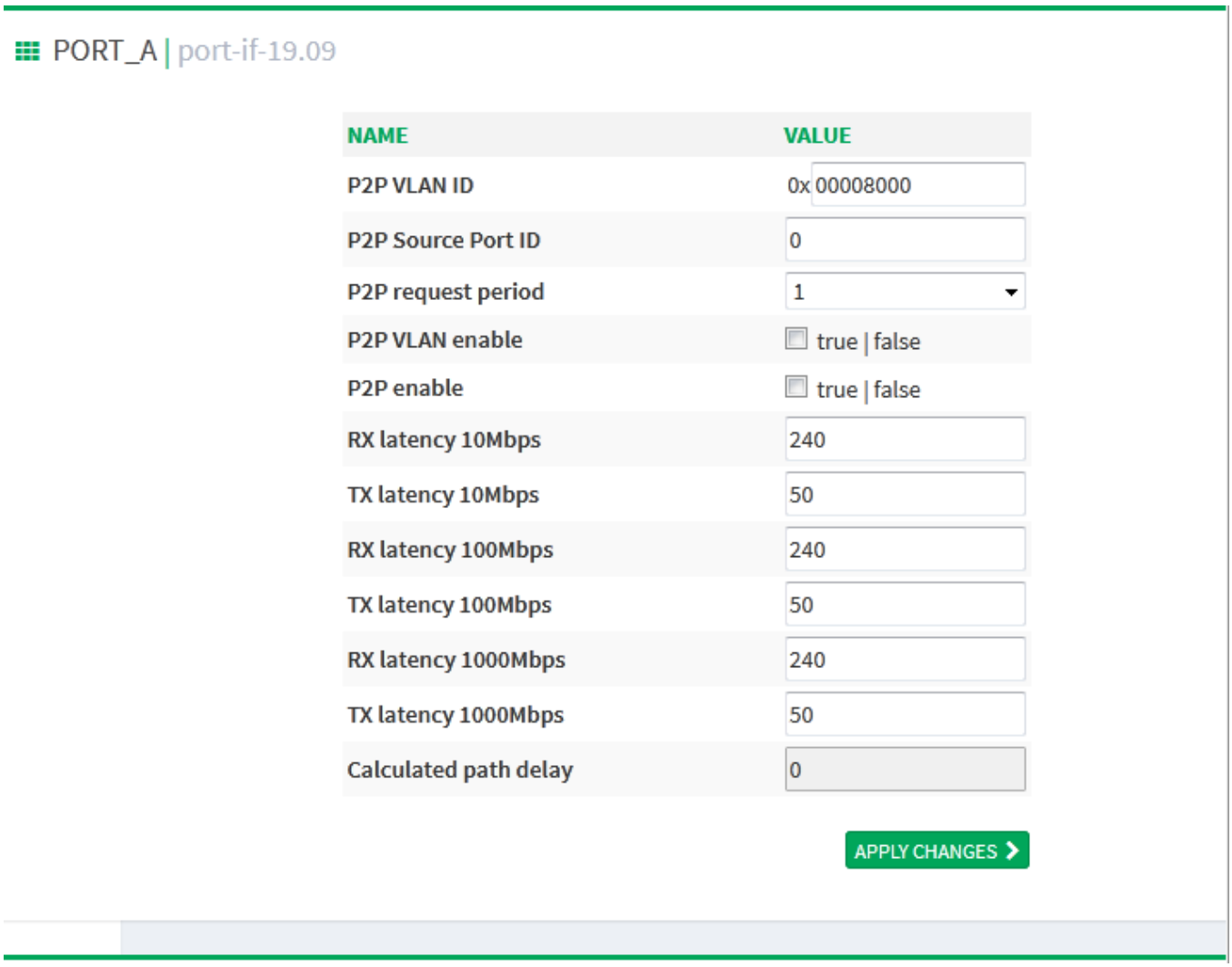


Рисунок 55 Страница настройки порта PTP

P2P VLAN ID

Диапазон настройки: 16 бит [00-FFFF]

Конфигурация по умолчанию: 00008000

Функция: Настройка тега VLAN PTP.

P2P Source Port ID

Диапазон настройки: 8 бит [00-255]

Конфигурация по умолчанию: 0

Функция: настройка ID порта-источника PTP.

P2P request period

Варианты конфигурации: 1/2/4/8

Конфигурация по умолчанию: 1

Функция: Число запросов Pdelay в секунду.

P2P VLAN enable

Варианты конфигурации: true/false

Конфигурация по умолчанию: false

Функция: добавление тега VLAN к сообщению PTP.

P2P enable

Варианты конфигурации: true/false

Конфигурация по умолчанию: false

Функция: включение или отключение механизма задержки PTP.

RX latency 10Mbps

Диапазон настройки: 16 бит [0-65535]

Конфигурация по умолчанию: 240

Функция: Логическая задержка RX (ед. изм. нс (10 Мбит/с)).

TX latency 10Mbps

Диапазон настройки: 16 бит [0-65535]

Конфигурация по умолчанию: 50

Функция: Логическая задержка TX (ед. изм. нс (10 Мбит/с)).

RX latency 100Mbps

Диапазон настройки: 16 бит [0-65535]

Конфигурация по умолчанию: 240

Функция: Логическая задержка RX (ед. изм. нс (100 Мбит/с)).

TX latency 100Mbps

Диапазон настройки: 16 бит [0-65535]

Конфигурация по умолчанию: 50

Функция: Логическая задержка TX (ед. изм. нс (100 Мбит/с)).

RX latency 1000Mbps

Диапазон настройки: 16 бит [0-65535]

Конфигурация по умолчанию: 240

Функция: Логическая задержка RX (ед. изм. нс (1000 Мбит/с)).

TX latency 1000Mbps

Диапазон настройки: 16 бит [0-65535]

Конфигурация по умолчанию: 50

Функция: Логическая задержка TX (ед. изм. нс (1000 Мбит/с)).

Calculated path delay

Функция: задержка на пути (нс), рассчитанная с использованием однорангового механизма прозрачных часов PTP.

5.3 Статистика

Щелкните в дереве навигации [Functions]→[Statistics], перейдите на страницу настройки статистики, как показано на рисунке ниже.

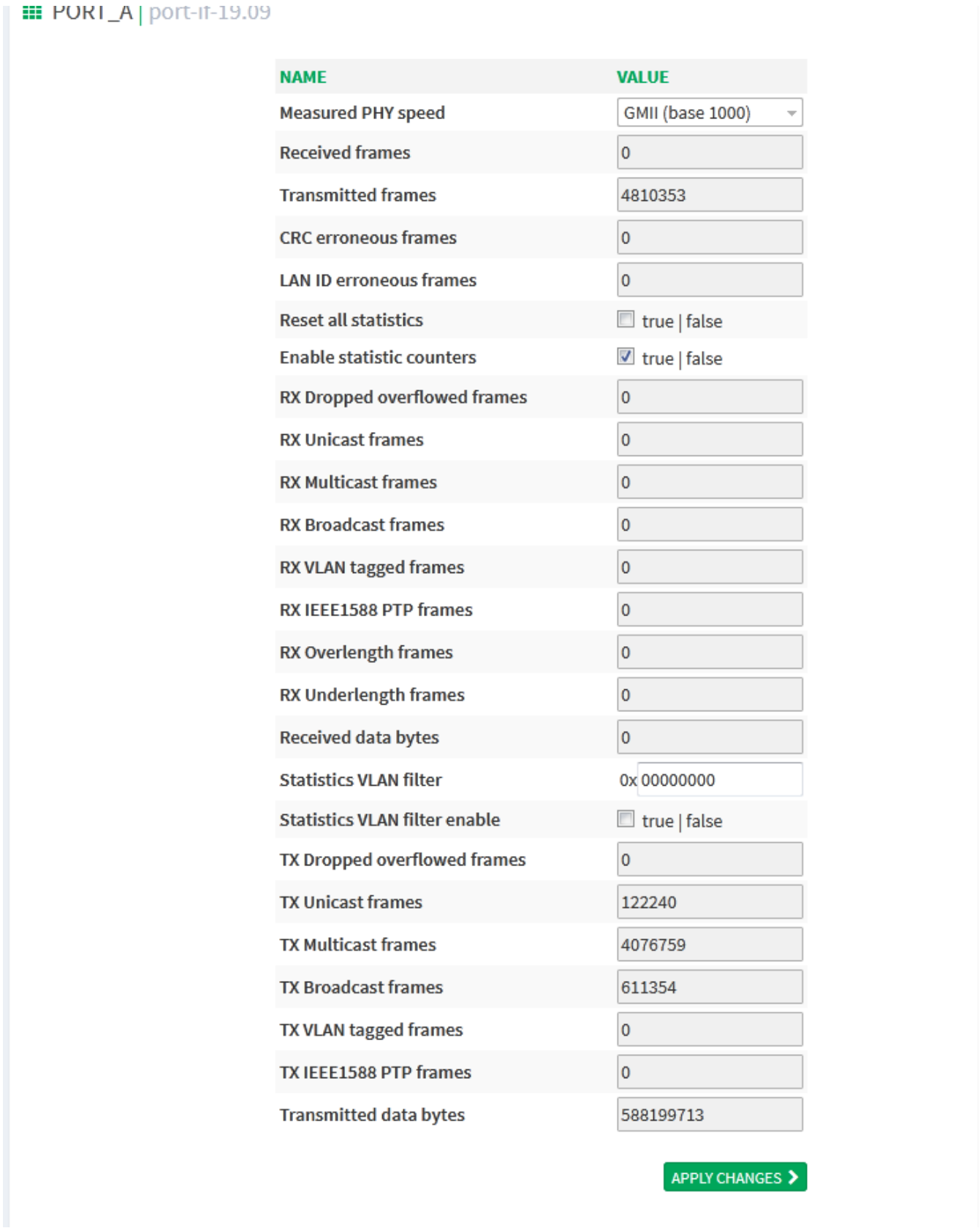


Рисунок 56 Страница настройки статистики

Measured PHY speed

Описание: Скорость PHY, измеренная с помощью модуля измерения скорости: 11 для 1000 Мбит/с, 10 для 100 Мбит/с и 01 для 10 Мбит/с.

Received frames

Описание: Количество полученных кадров. Диапазон: 32 бита [0-4294967295]

Transmitted frames

Описание: Количество переданных кадров. Диапазон: 32 бита [0-4294967295]

CRC erroneous frames

Описание: Количество кадров с ошибкой CRC. Диапазон: 32 бита [0-4294967295]

LAN ID erroneous frames

Описание: Количество кадров с ошибкой LAN ID. Диапазон: 32 бита [0-4294967295]

Reset all statistics

Описание: Сброс всех счетчиков статистики.

Enable statistic counters

Описание: Включение/выключение счетчиков статистики.

RX Dropped overflowed frames

Описание: Количество отброшенных переполненных кадров RX (на пути приема). Диапазон: 32 бита [0-4294967295]

RX Unicast frames

Описание: Количество одноадресных кадров RX Диапазон: 32 бита [0-4294967295]

RX Multicast frames

Описание: Количество многоадресных кадров RX Диапазон: 32 бита [0-4294967295]

RX Broadcast frames

Описание: Количество широковещательных кадров RX Диапазон: 32 бита [0-4294967295]

RX VLAN tagged frames

Описание: Количество тегированных кадров RX VLAN Диапазон: 32 бита [0-4294967295]

RX IEEE1588 PTP frames

Описание: Количество кадров RX IEEE1588 PTP Диапазон: 32 бита [0-4294967295]

RX Overlength frames

Описание: Количество кадров избыточной длины RX. (Действительно, когда jumbo-кадры отключены) Диапазон: 32 бита [0-4294967295]

RX Underlength frames

Описание: Количество кадров недостаточной (меньшей, чем длина минимального кадра) длины. Диапазон: 32 бита [0-4294967295]

Received data bytes

Описание: Количество полученных байтов данных (не включая ведущий байт) Диапазон: 32 бита [0-4294967295]

Statistics VLAN filter

Описание: Счетчик фильтра указанной VLAN. Диапазон: 12 бит 0X[0-00000FFF]

Statistics VLAN filter enable

Описание: Включение счетчика фильтра указанной VLAN.

TX Dropped overflowed frames

Описание: Количество отброшенных переполненных кадров TX (на пути приема). Диапазон: 32 бита [0-4294967295]

TX Unicast frames

Описание: Количество одноадресных кадров TX Диапазон: 32 бита [0-4294967295]

TX Multicast frames

Описание: Количество многоадресных кадров TX Диапазон: 32 бита [0-4294967295]

TX Broadcast frames

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

TX VLAN tagged frames

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

TX IEEE1588 PTP frames

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

Transmitted data bytes

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

6 Другие настройки

На странице настройки имеется несколько функциональных модулей с настройками коммутатора, помимо HSR/PTP, включая такие модули, как alarm, sntp, snmp, radius, tacacs.

6.1 Аварийная сигнализация

6.1.1 Введение

Коммутаторы этой серии поддерживают следующие типы аварийной сигнализации:

- Аварийная сигнализация по использованию памяти/ЦП. Если эта функция включена, аварийный сигнал генерируется, когда использование ЦП/памяти превышает указанный порог.
- Аварийная сигнализация по порту: Если эта функция включена, аварийный сигнал генерируется, когда порт находится в состоянии Link Down.

Когда функция аварийной сигнализации активна, режимы тревоги включают запись в журнал, мигание тревожного светодиода на передней панели, срабатывание клеммного блока тревоги и отправку сообщений trap SNMP.

6.1.2 Настройка через веб-интерфейс

1. Настройте и отобразите аварийную сигнализацию по использованию памяти/ЦП.

Щелкните в дереве навигации [Other Configurations]→[Alarm], перейдите на страницу настройки аварийной сигнализации, как показано ниже.

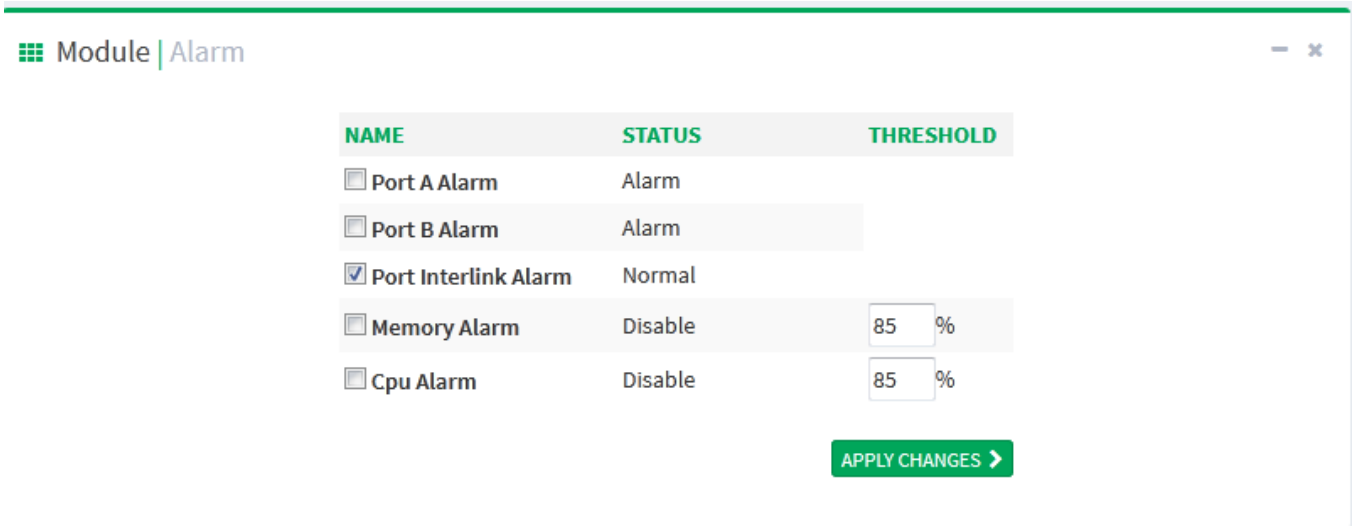


Рисунок 57 Настройка аварийной сигнализации по использованию памяти/ЦП

Memory Alarm/CPU Alarm

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение аварийной сигнализации по использованию памяти/ЦП.

Threshold (%)

Диапазон настройки: 50~100

Конфигурация по умолчанию: 85

Функция: настройка порогового значения аварийной сигнализации по использованию памяти/ЦП. Когда использование памяти/ЦП коммутатора превышает это значение, генерируется сигнал аварийной сигнализации по использованию памяти/ЦП.

Пояснение: Когда генерируется сигнал тревоги по использованию памяти/ЦП, чтобы предотвратить частые сбросы/генерацию сигнала тревоги вследствие колебаний использования памяти/ЦП вблизи порогового значения, сигнал тревоги будет сброшен только тогда, когда коэффициент использования памяти/ЦП будет на одно значение после запятой ниже, чем порог.

Alarm status

Варианты отображения: Normal/Alarm

Функция: Отображение использования памяти/ЦП коммутатора. Сигнал тревоги указывает на то, что загрузка памяти/ЦП превышает пороговое значение.

	**Предостережение**: Коэффициент использования ЦП в этом тексте относится к среднему коэффициенту использования ЦП за 5 секунд.

2. Настройте и отобразите аварийную сигнализацию по порту.

Щелкните в дереве навигации [Other Configurations]→[Alarm], перейдите на страницу настройки аварийной сигнализации, как показано ниже.

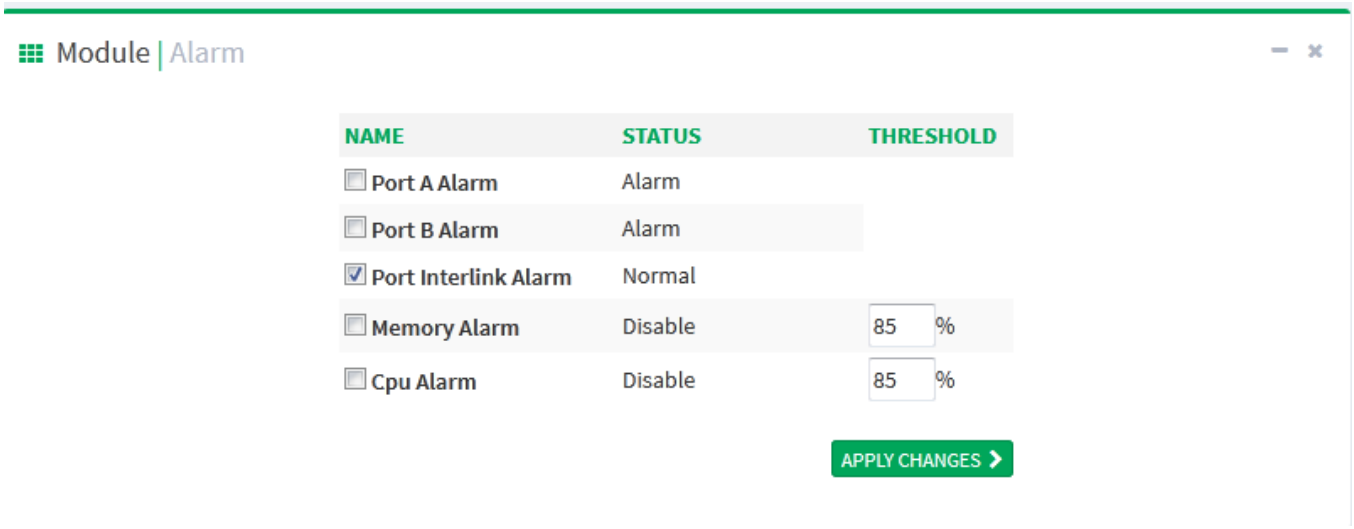


Рисунок 58 Страница настройки аварийной сигнализации по порту

Port

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: enable.

Функция: включение или отключение аварийной сигнализации по порту.

Alarm status

Варианты отображения: LinkDown/LinkUp

Функция: Состояние подключения порта. LinkUp указывает, что порт подключен и может нормально обмениваться данными; LinkDown указывает, что порт отключен или работает ненормально, будет сгенерирован сигнал тревоги.

6.2 Настройка портов

Щелкните в дереве навигации [Other Configurations]→[Port configuration], перейдите на страницу настройки портов, где можно настроить состояние, скорость и тип порта, как показано ниже.

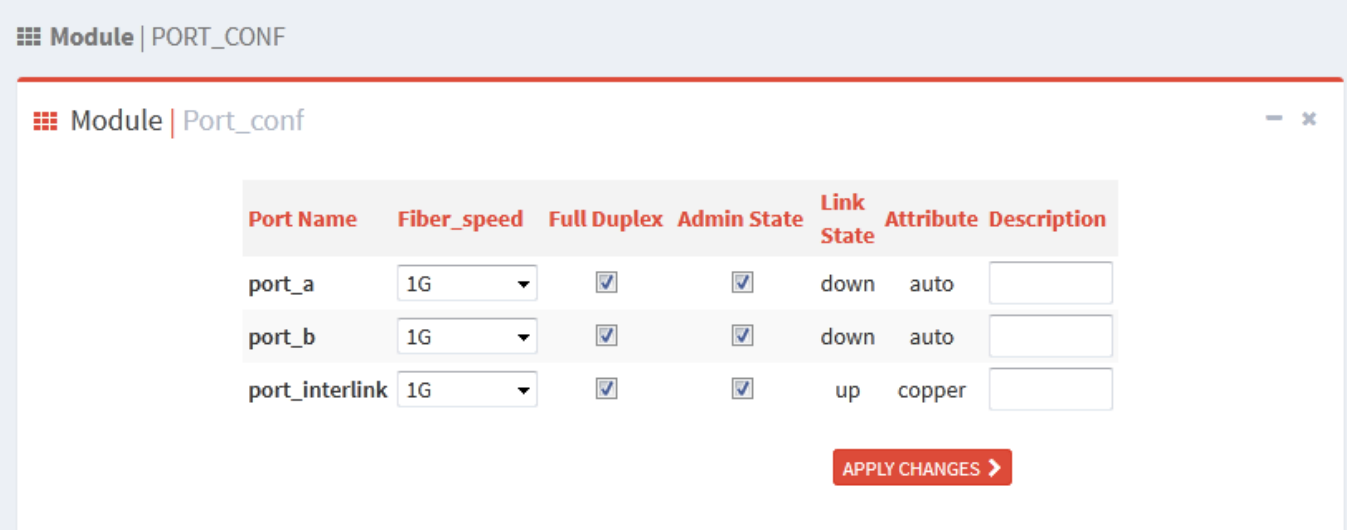


Рисунок 59 Настройка портов

Port name

Есть три порта – port_a, port_b и port_interlink

Fiber_speed

Варианты конфигурации: 100M/1G

Функция: настройка скорости автосогласования порта.

Описание: При настройке режима порта auto скорость порта по умолчанию определяется автоматическим согласованием с другим концом, а согласованная скорость может находиться в пределах диапазона скорости порта. Настраивая скорость, порт может согласовывать только частичную скорость, таким образом контролируя согласование скорости. Значение 100M можно задать только для оптического порта.

CAUTION	**Предостережение**: Настройка дуплекса и скорости доступна только в автоматическом режиме. Port_interlink субплаты SM6.6-HSR/PRP используется внутри, не настраивайте и не закрывайте его.

Full Duplex

Варианты конфигурации: Fdx/Hdx

Функция: Настройка дуплексного режима автосогласования.

Описание: Полнодуплексный режим Fdx означает, что порт может принимать данные во время передачи данных.

Полудуплексный режим Hdx означает, что порт одномоментно может или передавать или принимать данные.

При настройке режима порта auto режим дуплекса порта по умолчанию определяется автоматическим согласованием с другим концом, а согласованный режим может быть либо Fdx, либо Hdx.

При настройке дуплекса порт может согласовывать только один дуплексный режим, тем самым контролируя согласование дуплексного режима.

Admin Status

Варианты конфигурации: shutdown/no shutdown

Конфигурация по умолчанию: no shutdown

Функция: Разрешение передачи данных для порта.

Описание: no shutdown означает, что порт включен и разрешена передача данных; shutdown указывает на то, что порт отключен и передача данных не разрешена. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.

Link Status

Просмотр состояния подключения порта. Up означает, что порт находится в состоянии LinkUp и может нормально передавать данные. Down означает, что порт находится в состоянии LinkDown и не может нормально передавать данные.

Attribute

Варианты конфигурации: auto/copper

Конфигурация по умолчанию: auto

Функция: Тип среды передачи порта Ethernet.

Описание: Auto: порт автоматически обнаруживает кабели для определения типа среды передачи.

Copper: Тип среды порта – медный кабель.

Description

Диапазон настройки: 1~200 символов

Функция: Настройка псевдонима для описания порта.

6.3 Настройка MAC

При пересылке пакета коммутатор ищет порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя пакета.

MAC-адрес может быть как статическим, так и динамическим.

Статический MAC-адрес настраивается пользователем. Он имеет наивысший приоритет (не переопределяется динамическими MAC-адресами) и действует постоянно.

Динамические MAC-адреса коммутатор узнает при пересылке данных. Они действительны только в течение определенного периода. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор узнает исходный MAC-адрес кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя кадра. Если совпадение найдено, коммутатор пересылает кадр данных с соответствующего порта. Если совпадений не найдено, коммутатор передает кадр в своем широковещательном домене.

Время устаревания начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение времени, в 1-2 раза превышающего время устаревания, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки.

Статические MAC-адреса не включают понятие времени устаревания.

6.3.1 Запросы MAC

Щелкните в дереве навигации [Other Configurations]→[Mac Queries], перейдите на страницу запроса MAC-адреса, как показано ниже.

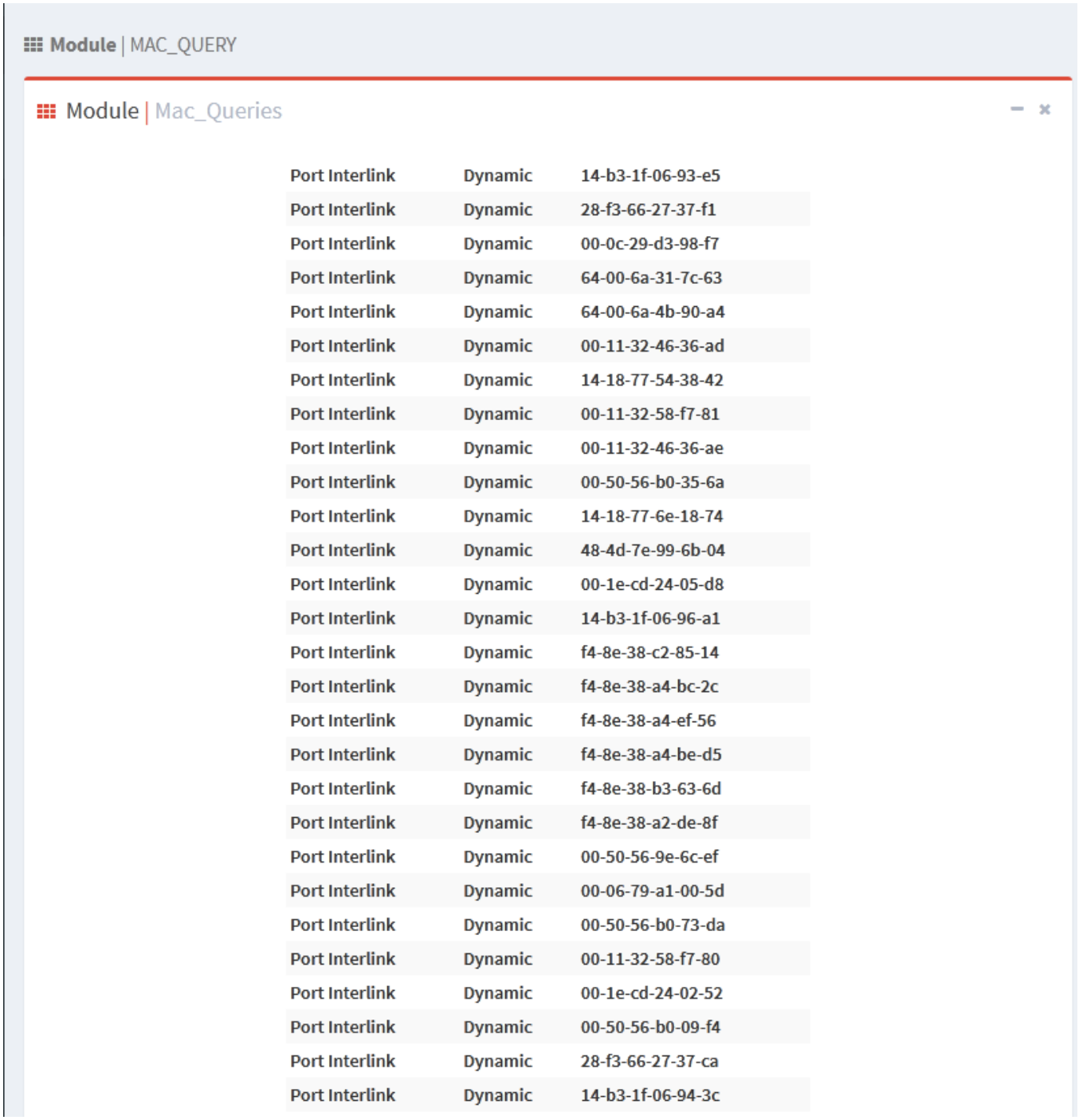


Рисунок 60 Запрос MAC-адреса

CAUTION	**Предостережение**: В режиме коммутации port_a, port_b, port_interlink соответствуют трем реальным портам. В режиме резервирования port_b представляет два резервных порта, которые не различают A и B, port_a не используется.

6.3.2 Контроль MAC-адреса

Щелкните в дереве навигации [Other Configurations]→[Mac Address Control], перейдите на страницу контроля MAC-адреса, как показано ниже.

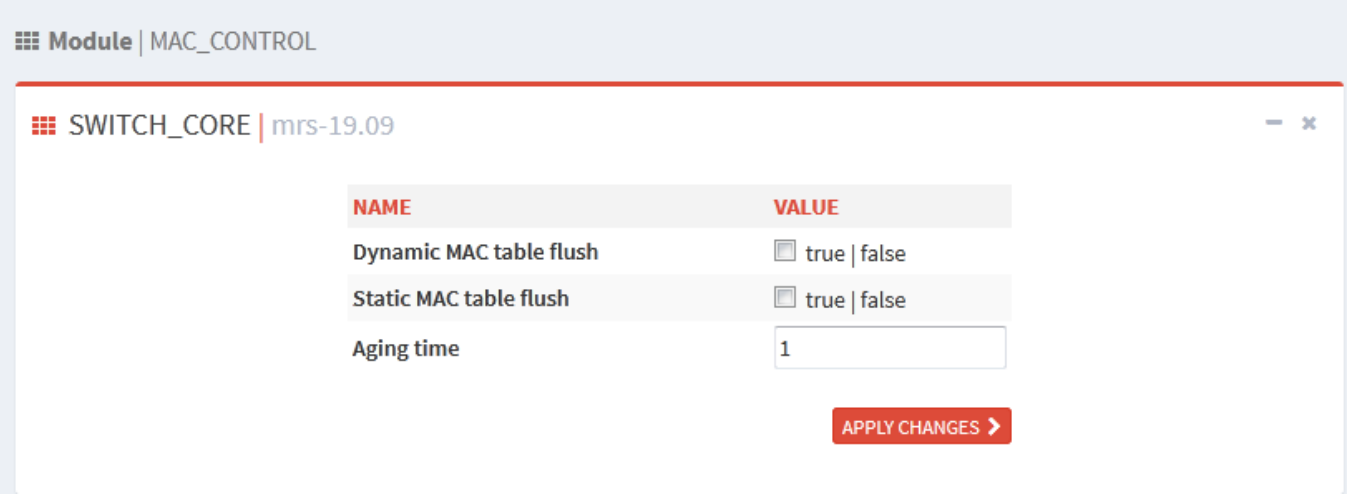


Рисунок 61 Страница контроля MAC-адреса

Dynamic MAC table flush

Варианты конфигурации: true/false

Конфигурация по умолчанию: false

Настройка обновления динамического MAC-адреса.

Static MAC table flush

Варианты конфигурации: true/false

Конфигурация по умолчанию: false

Настройка обновления статического MAC-адреса.

Aging time

Варианты конфигурации: 0-15 мин.

Конфигурация по умолчанию: 1

Настройка времени старения таблицы MAC-адресов.

6.3.3 Настройка MAC-адреса

Щелкните в дереве навигации [Other Configurations]→[Mac Address Configuration], перейдите на страницу настройки MAC-адреса, как показано ниже.

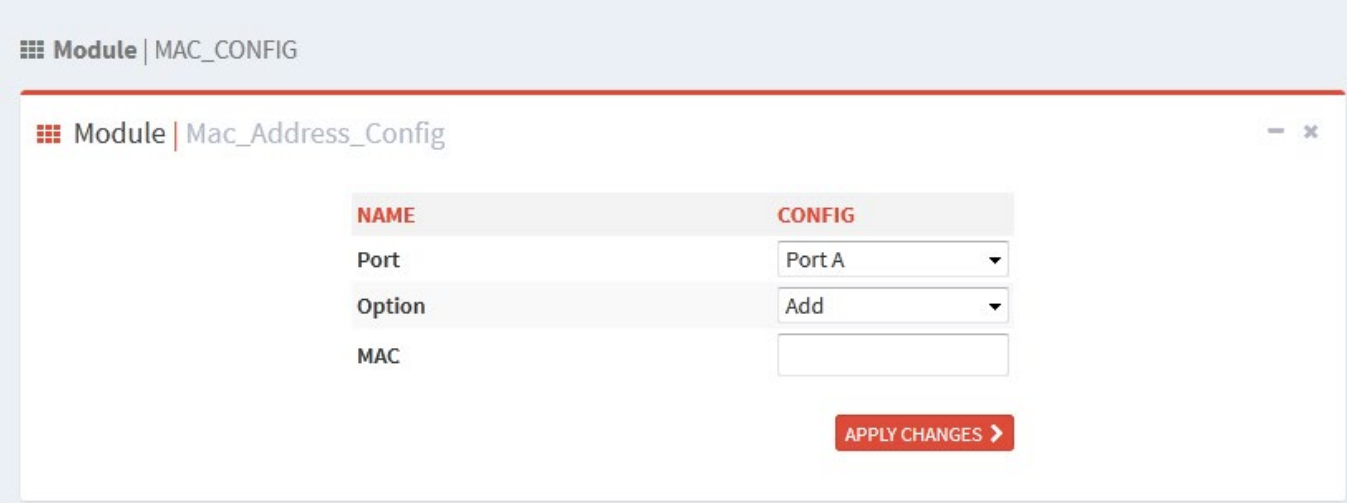


Рисунок 62 Страница настройки MAC-адреса

Port

Варианты конфигурации: port_a/port_b/port_interlink

По умолчанию: port_a

Option

Варианты конфигурации: add/delete

По умолчанию: add

Удалить или добавить MAC-адрес порта.

MAC

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число)

Функция: Настройка одноадресного MAC-адреса с младшим битом старшего байта равным 0.

6.4 SNTP

6.4.1 Введение

Протокол SNTP (простой сетевой протокол времени) калибрует время, используя запрос и ответ между сервером и клиентом. Коммутатор в качестве клиента калибрует время в соответствии с сообщением сервера.

Запрос SNTP-клиента отправляется на сервер один за другим в одноадресной форме, сервер отвечает на сообщение.

CAUTION	**Предостережение**: Когда на коммутаторе используется SNTP, сервер SNTP должен быть активен. Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени часового пояса 0.

6.4.2 Настройка через веб-интерфейс

1. Включите протокол SNTP.

Щелкните в дереве навигации [Other Configurations]→[SNTP], перейдите на страницу настройки SNTP, как показано ниже.

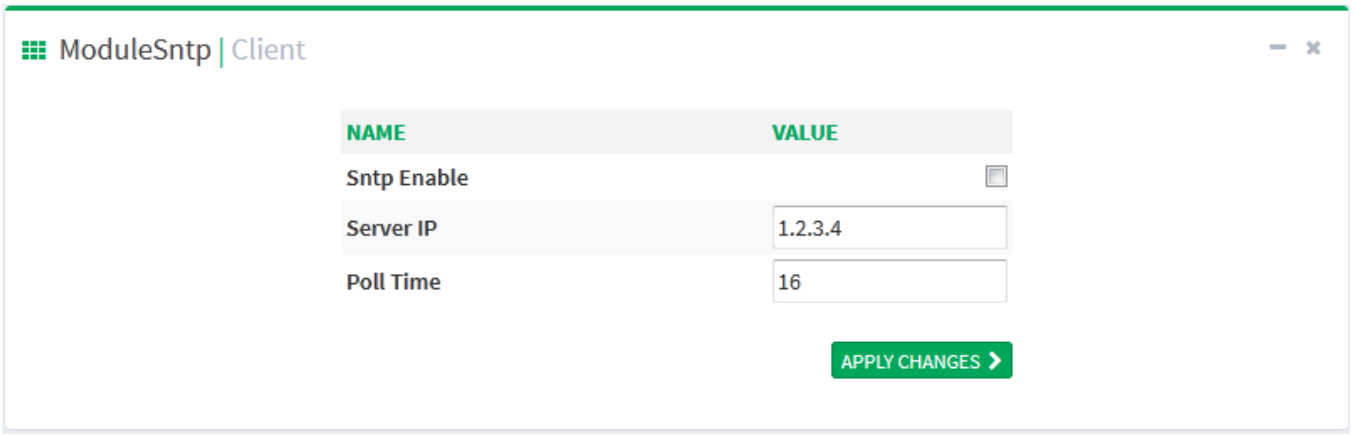


Рисунок 63 Включение протокола SNTP

SNTP Enable

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение или выключение протокола SNTP

CAUTION	**Предостережение**: Поскольку NTP и SNTP используют один и тот же номер порта UDP, их нельзя использовать одновременно.

2. Настройка IP сервера SNTP

Server IP

Формат: A.B.C.D

Функция: Настройка IP сервера SNTP, клиент будет калибровать время в соответствии с сообщением этого сервера.

3. Настройка временного интервала отправки запроса синхронизации клиентом SNTP.

Poll Time

Варианты конфигурации: 16~16284 с

Функция: Настройка временного интервала отправки запроса синхронизации клиентом SNTP серверу.

4. Проверьте, что время коммутатора синхронизировано со временем сервера.

Щелкните в дереве навигации [Network Nodes], перейдите на страницу просмотра часов, как показано ниже.

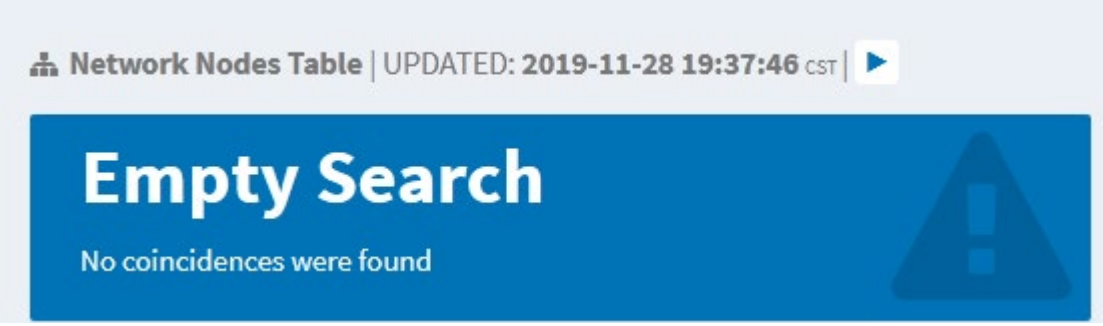


Рисунок 64 Просмотр информации о синхронизированных часах

На открывшейся странице щелкните кнопку, часы отобразятся в окне после того, как SNTP-клиент синхронизирует время с сервером.

6.5 NTP

6.5.1 Введение

Протокол сетевого времени (NTP) синхронизирует время между распределенными серверами и клиентами. NTP синхронизирует часы всех сетевых устройств, обеспечивая согласованность времени между всеми устройствами. Это позволяет устройствам предоставлять несколько приложений в одно и то же время. Локальная система с поддержкой NTP может не только синхронизировать свои часы с другими источниками часов, но и служить источником часов для других устройств.

Как показано на рисунке 65, двусторонняя задержка (T4-T1) - (T3-T2) и смещение часов ((T2-T1) + (T3-T4)) / 2 могут быть рассчитаны на основе обмена NTP-пакетами, благодаря чему достигается высокоточная синхронизация часов между устройствами.

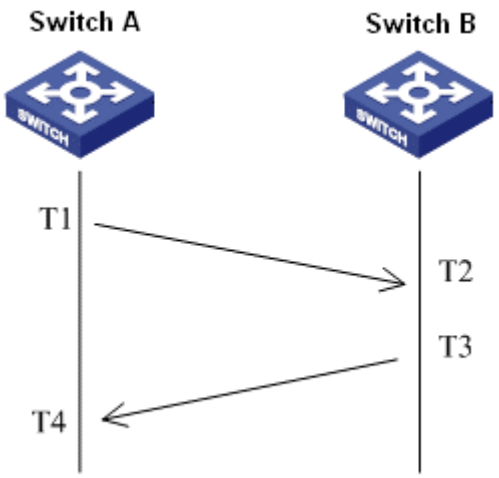


Рисунок 65 NTP

6.5.2 Рабочие режимы NTP

NTP может использовать следующие режимы для синхронизации времени. При необходимости можно выбрать соответствующий режим работы.

Режим клиент/сервер: В этом режиме клиент отправляет пакеты синхронизации часов (режим клиента) на сервер. После получения пакетов сервер автоматически работает в режиме сервера и отправляет ответные пакеты (режим сервера). После получения ответных пакетов клиент синхронизируется с оптимальными часами сервера.

Одноранговый режим: В этом режиме активный одноранговый узел отправляет пакеты синхронизации часов (режим активного однорангового узла) пассивному одноранговому узлу. После получения пакетов пассивный одноранговый узел автоматически работает в пассивном одноранговом режиме и отправляет ответные пакеты (пассивный одноранговый режим). На основе обмена пакетами устройства устанавливают одноранговый режим. Активный одноранговый узел и пассивный одноранговый узел могут синхронизировать время друг с другом. Если оба одноранговых узла синхронизировали время с других устройств, одноранговый узел с большим уровнем часов синхронизирует время с одноранговым узлом с меньшим уровнем часов.

Режим вещания: В этом режиме сервер вещания периодически рассылает пакеты синхронизации часов (режим вещания). После получения пакетов клиент широковещательной рассылки отправляет на сервер пакеты синхронизации часов (режим клиента). После получения пакетов запроса сервер отправляет пакеты ответа (режим сервера). Сервер и клиент выполняют синхронизацию часов, обмениваясь восемью пакетами запросов и ответов. Режим многоадресной рассылки Клиент многоадресной рассылки периодически отправляет пакеты запроса синхронизации многоадресной рассылки (режим клиента) на сервер многоадресной рассылки. После получения пакетов сервер отправляет

одноадресные ответные пакеты (режим сервера). Затем сервер и клиент выполняют синхронизацию часов, обмениваясь одноадресными запросами синхронизации часов и ответными пакетами.

6.5.3 Настройка через веб-интерфейс

1. Включите протокол NTP

Щелкните дерево навигации [Other Configurations]→[NTP], войдите в интерфейс глобальной настройки NTP, как показано ниже.

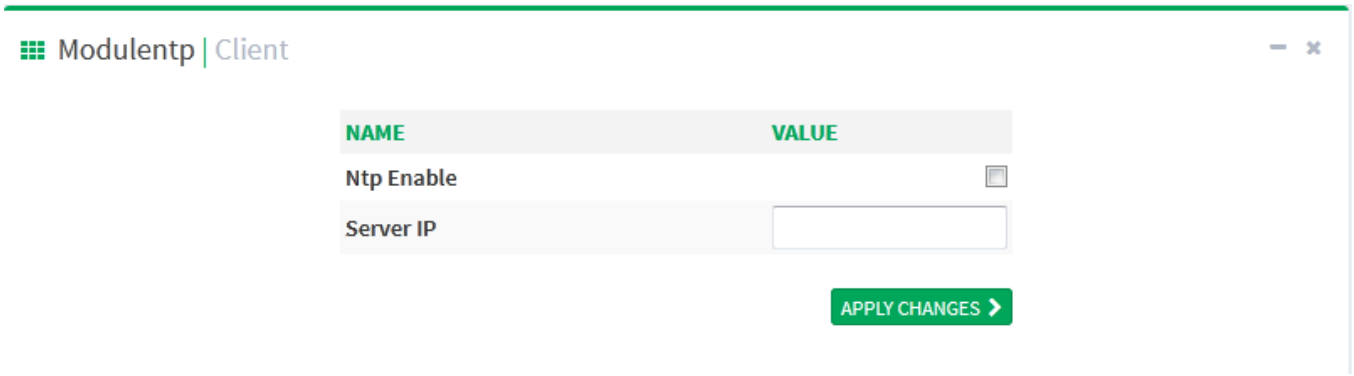


Рисунок 66 Включение протокола NTP

NTP Enable

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение глобальной службы NTP.

CAUTION	**Предостережение**: Поскольку NTP и SNTP используют один и тот же номер порта UDP, их нельзя использовать одновременно. Когда службы NTP отключены, службы NTP можно настроить и сохранить, то есть включение или отключение служб NTP не влияет на конфигурацию служб NTP.

2. Настройка сервера NTP

Server IP

Формат: A.B.C.D

Функция: Настройка IP-адреса сервера NTP. Калибровка времени клиента будет осуществляться по сообщениям сервера NTP.

6.6 IEC61850 MMS

6.6.1 Введение

В настоящее время коммутатор прозрачен по функциям трансформаторной подстанции в сети подстанции. Для мониторинга требуются отличные от IEC61850 инструменты (протоколы), такие как EMS, WEB, CLI, OPC и т. д.. Это приводит к тому, что точка наблюдения и точка настройки расходятся, становятся несогласованными и неудобными. Для решения этих проблем коммутатор спроектирован в соответствии с протоколом IEC61850 и включается в систему автоматизации подстанции (IEC61850) как интеллектуальное электронное устройство (IED, Intelligent Electronic Device). Этот подход объединяет автоматический мониторинг подстанции, удобное интегрированное планирование управления пользователем, экономию затрат на строительство и техническое обслуживание.

CAUTION	**Предостережение**: Файлы моделирования по умолчанию switch.cid, предоставленные нашей компанией, импортированы в этот коммутатор. Если заказчикам необходимо импортировать другие файлы моделирования, обратитесь к разделу «4.6 Загрузка файлов», чтобы импортировать файлы.

6.6.2 Настройка через веб-интерфейс

1. Включите функцию IEC 61850

Щелкните дерево навигации [Other Configurations]→[Iec61850mms], перейдите на страницу глобальной настройки NTP, как показано ниже.

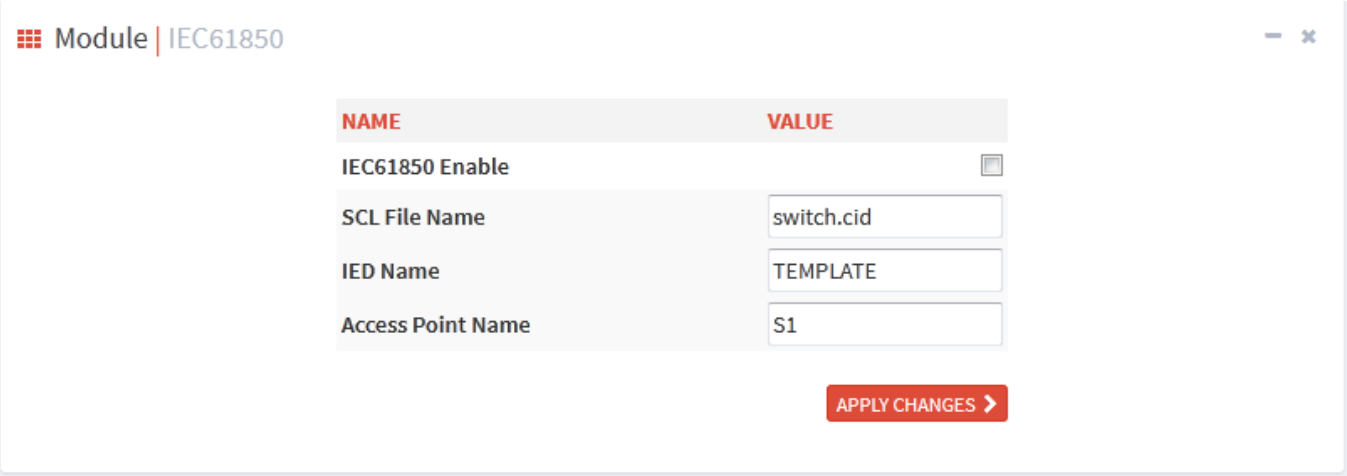


Рисунок 67 Страница настройки IEC 61850

IEC61850 enable

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение IEC61850.

SCL File Name

Диапазон настройки: 1~25 символов

Конфигурация по умолчанию: switch.cid

Функция: Задание файла моделирования, который вступит в силу при инициализации функции IEC61850.

IED Name

Диапазон настройки: 1~25 символов

Конфигурация по умолчанию: TEMPLATE

Функция: Настройка имени логического устройства для этого IED в файле моделирования.

Access Point Name

Диапазон настройки: 1~25 символов

Конфигурация по умолчанию: S1

Функция: Настройка имени точки доступа для этого IED в файле моделирования.

	**Предостережение**: Настройки имени точки доступа и имени IED должны соответствовать имени точки доступа и IED в указанном файле моделирования, в противном случае произойдет сбой запуска функции IEC 61850.

6.7 SNMPv2c

6.7.1 Введение

Simple Network Management Protocol (SNMP) — это структура, использующая TCP/IP для управления сетевыми устройствами. С помощью SNMP администратор может запрашивать информацию об устройстве, изменять настройки параметров, отслеживать состояние устройства и обнаруживать сбои в сети.

6.7.2 Реализация

SNMP использует режим станции управления/агента. Таким образом, SNMP включает в себя два типа сетевых элементов: NMS и агент.

Станция управления сетью (NMS) — это станция, на которой работает программный клиент управления сетью с поддержкой SNMP. Это ядро для управления сетью SNMP.

Агент — это процесс в управляемых сетевых устройствах. Он получает и обрабатывает пакеты запросов от NMS. Когда возникает сигнал тревоги, агент сообщает об этом в NMS.

NMS является средством управления сетью SNMP, а агент управляется сетью SNMP. NMS и агенты обмениваются пакетами управления через SNMP. SNMP включает в себя следующие основные операции:

Get-Request

Get-Response

Get-Next-Request

Set-Request

Trap

NMS отправляет пакеты Get-Request, Get-Next-Request и Set-Request агентам для запроса, настройки и управления переменными. После получения этих запросов агенты отвечают пакетами Get-Response. Когда возникает тревога, агент упреждающе сообщает об этом в NMS с помощью пакета Trap.

6.7.3 Пояснения

Коммутаторы этой серии поддерживают SNMPv2 и SNMPv3. SNMPv2 совместим с SNMPv1. SNMPv1 использует для аутентификации имя сообщества. Имя сообщества действует как пароль, ограничивая доступ NMS к агентам. Если имя сообщества, переносимое пакетом SNMP, не подтверждается коммутатором, запрос завершается неудачно и возвращается сообщение об ошибке.

SNMPv2 также использует для аутентификации имя сообщества. Он совместим с SNMPv1 и расширяет функционал SNMPv1.

Чтобы обеспечить связь между NMS и агентом, их версии SNMP должны совпадать. Для агента можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

6.7.4 Знакомство с MIB

Любой управляемый ресурс называется управляемым объектом. Management Information Base (MIB) хранит управляемые объекты. Она определяет иерархические отношения управляемых объектов и атрибутов объектов, таких как имена, разрешения на доступ и типы данных. У каждого агента есть своя MIB. NMS может читать/записывать MIB на основе разрешений. На рисунке 68 показаны взаимоотношения между NMS, агентом и MIB.

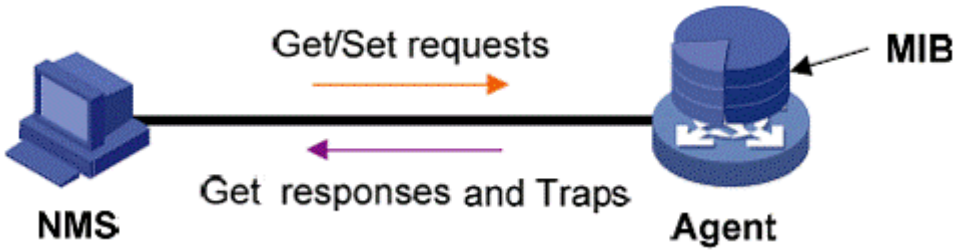


Рисунок 68 Взаимоотношения между NMS, агентом и MIB

MIB определяет древовидную структуру. Узлы дерева являются управляемыми объектами. Каждый узел имеет уникальный идентификатор Object Identifier (OID), который указывает расположение узла в структуре MIB. Как показано на рисунке 69, OID объекта A – 1.2.1.1.

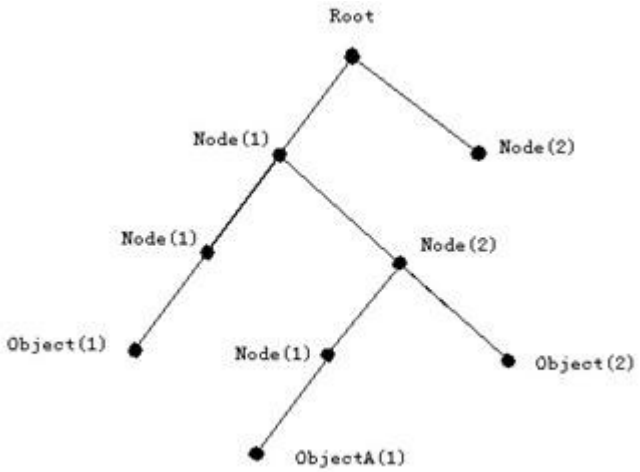


Рисунок 69 Структура MIB

6.7.5 Настройка через веб-интерфейс

1. Включите протокол SNMP, как показано ниже.

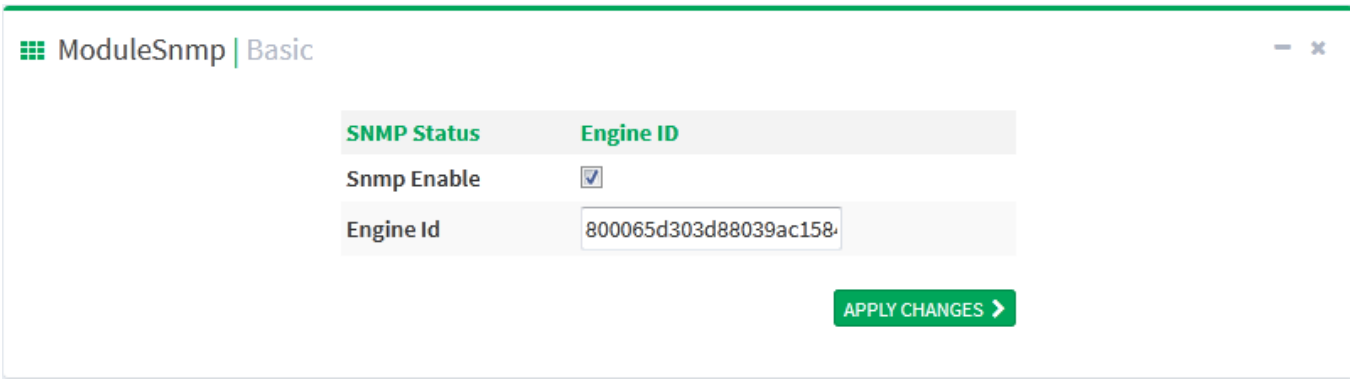


Рисунок 70 Включение протокола SNMP

SNMP Enable

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: enable.

Функция: включение или отключение протокола SNMP.

Engine ID

Диапазон настройки: четное количество шестнадцатеричных чисел, не может быть полным 0 или полным F, четное количество значений варьируется от 10 до 64.

Функция: Настройка Engine ID SNMP v3. При изменении Engine ID пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.

2. Настройте имя сообщества, как показано ниже.

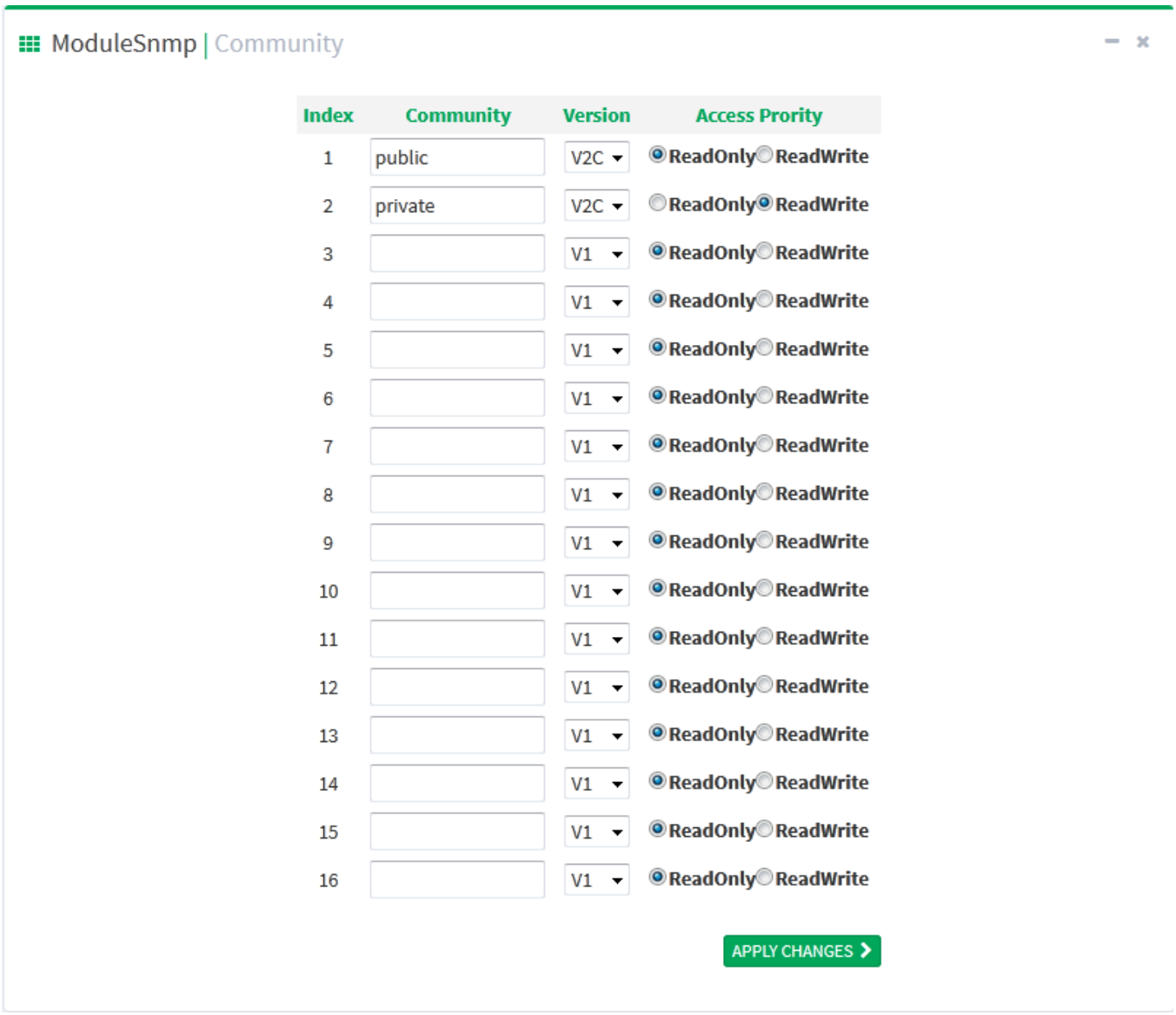


Рисунок 71 Настройка имени сообщества

Community

Диапазон настройки: 1~32 символа

Функция: Настройка имени сообщества коммутатора

Описание: Доступ к информации библиотеки MIB коммутатора возможен только в том случае, если имя сообщества в сообщении SNMP соответствует строке сообщества.

Пояснение: Можно настроить до 16 строк сообщества.

Version

Варианты конфигурации: V1/V2C

Функция: Выбор версии SNMP.

Access Prority

Варианты конфигурации: Readonly/ReadWrite

Конфигурация по умолчанию: Readonly

Функция: Настройка режима доступа MIB.

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

3. Настройте Trap, как показано ниже.

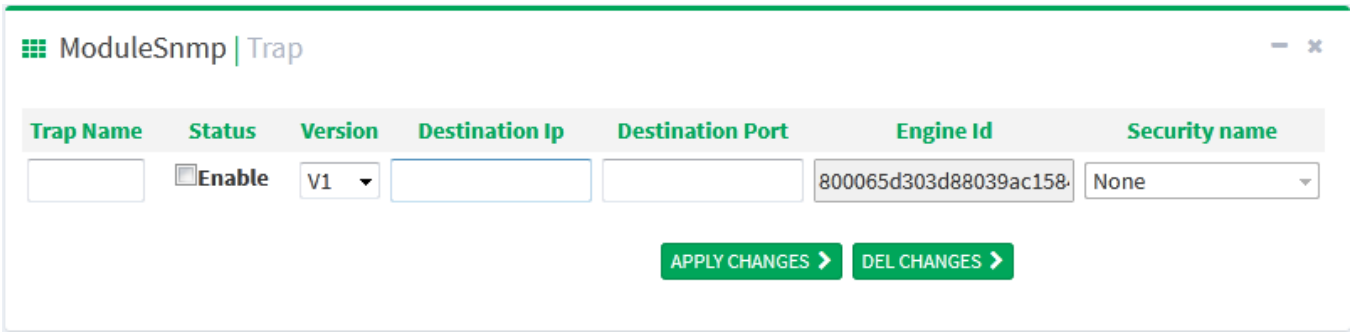


Рисунок 72 Настройка Trap

Trap name

Диапазон настройки: 1~32 символа

Функция: Настройка имени Trap.

Status

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение trap, при включении коммутатор отправляет на сервер соответствующие сообщения trap.

Version

Варианты конфигурации: SNMP v1/SNMP v2c/SNMP v3

Конфигурация по умолчанию: SNMP v1

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

Destination IP

Формат: A.B.C.D

Функция: Настройка адреса сервера для получения сообщения trap.

Destination Port

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 162

Функция: Настройка номера порта для отправки сообщений Trap.

6.7.6 Пример типовой конфигурации

Станция управления SNMP подключена к коммутатору через Ethernet, IP-адрес станции управления — 192.168.0.23, а IP-адрес коммутатора — 192.168.0.2. NMS контролирует агента через SNMPv2c, считывает и записывает информацию об узле MIB агента и отправляет отчет о сообщениях trap в NMS в случае сбоя или ошибки агента, как показано на рисунке ниже.

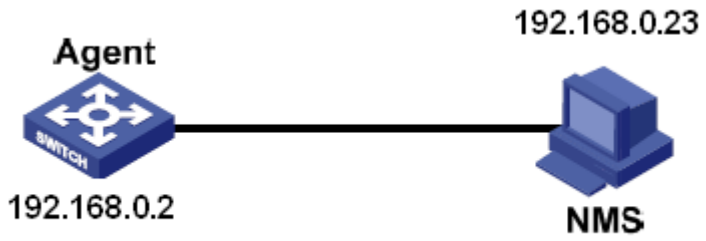


Рисунок 73 Пример настройки SNMPv2

Процесс настройки агента:

1. Включите протокол SNMP и состояние V2C, см. рисунок 70.

Настройте приоритет доступа, имя сообщества ReadOnly – public, имя сообщества ReadWrite – private, см. рисунок 71.

2. Включите состояние Trap, выберите версию V2C, IP-адрес сервера 192.168.0.23, см. Рисунок 71.

Для мониторинга и управления состоянием устройства-агента необходимо запустить в NMS соответствующее программное обеспечение для управления, например, программное обеспечение управления сетью Kyvision от Kyland.

О работе Kyvision см. в «Руководстве по эксплуатации программного обеспечения для управления сетью Kyvision».

6.8 SNMP v3

6.8.1 Введение

SNMPv3 обеспечивает механизм аутентификации модели безопасности на основе пользователей (USM). Можно настроить функции аутентификации и шифрования. Аутентификация используется для проверки подлинности отправителя пакета, предотвращая доступ незаконных пользователей. Шифрование используется для шифрования пакетов, передаваемых между NMS и агентом, во избежание перехвата. Функции аутентификации и шифрования могут повысить безопасность связи между SNMP NMS и SNMP-агентом.

6.8.2 Реализация

SNMPv3 предоставляет пять таблиц конфигурации. Каждая таблица может содержать 16 записей. Эти таблицы определяют, могут ли конкретные пользователи получать доступ к информации MIB.

Можно создать несколько пользователей в таблице пользователей. Каждый пользователь использует разные политики безопасности для аутентификации и шифрования.

Таблица групп — это совокупность нескольких пользователей. В таблице групп права доступа определяются на основе групп пользователей. Все пользователи группы имеют права группы. Таблица контекста идентифицирует строки, которые могут быть прочитаны пользователями, независимо от моделей безопасности.

Таблица просмотра относится к информации просмотра MIB, которая указывает информацию MIB, к которой могут обращаться пользователи. Представление MIB может содержать 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 одному из узлов поддерева MIB).

Можно определить права доступа MIB в таблице доступа по имени группы, названию контекста, модели безопасности и уровню безопасности.

6.8.3 Настройка через веб-интерфейс

1. Включите протокол SNMP, как показано на рисунке 115.

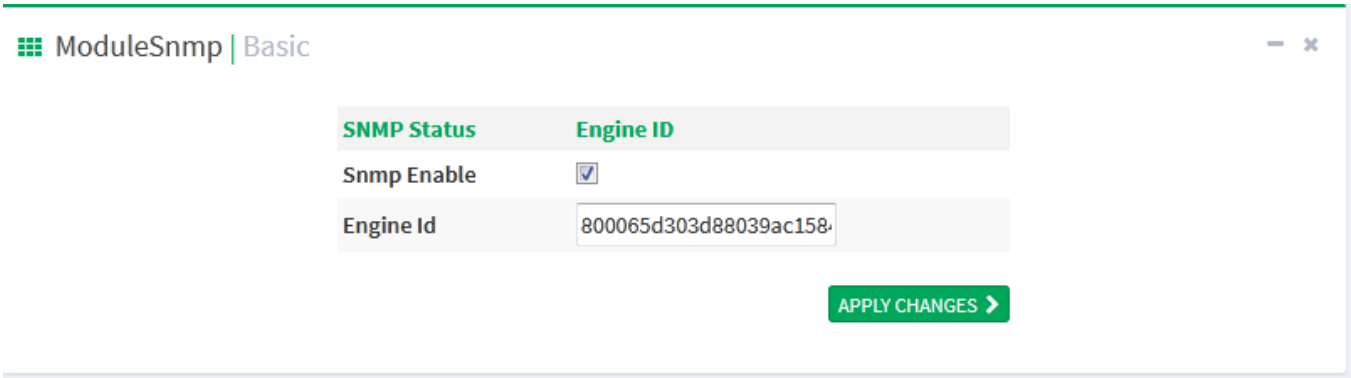


Рисунок 74 Включение протокола SNMP

SNMP Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: enable.

Функция: включение или отключение протокола SNMP.

Engine ID

Диапазон настройки: Четное количество шестнадцатеричных чисел, не может быть полным 0 или полным F, четное количество значений варьируется от 10 до 64.

Функция: Настройка Engine ID SNMP v3. При изменении Engine ID пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.

2. Настройте Trap, как показано ниже.

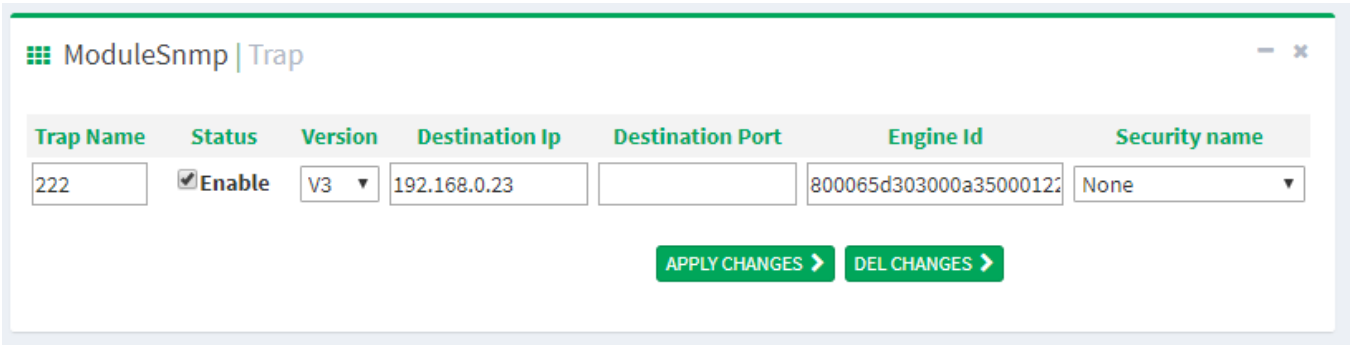


Рисунок 75 Настройка trap

Trap Name

Диапазон настройки: 1~32 символа

Функция: Настройка имени Trap.

Status

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение trap, при включении коммутатор отправляет на сервер соответствующие сообщения trap.

Version

Варианты конфигурации: SNMP v1/SNMP v2c/SNMP v3

Конфигурация по умолчанию: SNMP v1

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

Destination IP

Формат: A.B.C.D

Функция: Настройка адреса сервера для получения сообщения trap.

Destination Port

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 162

Функция: Настройка номера порта для отправки сообщений Trap.

3. Настройте таблицу пользователей, как показано ниже.

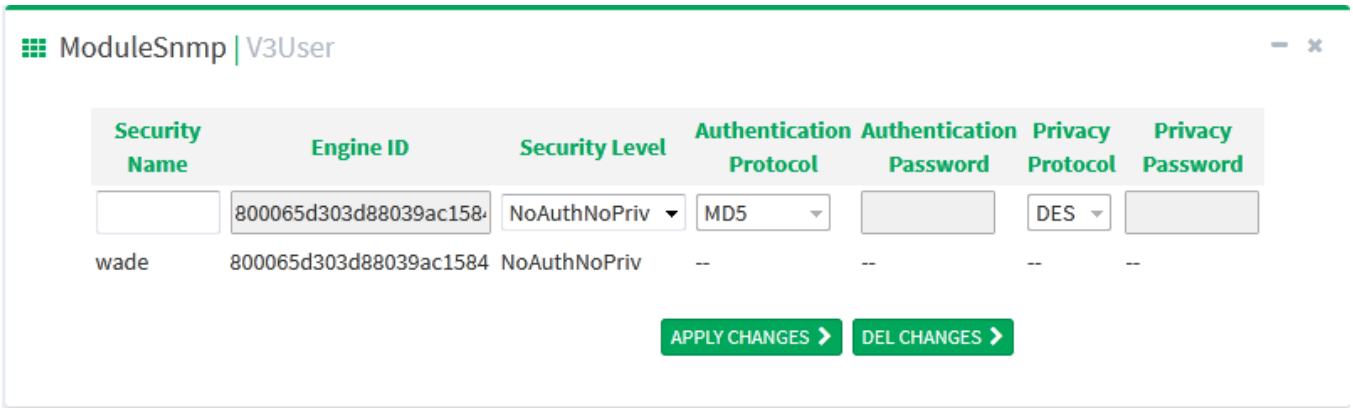


Рисунок 76 Настройка таблицы пользователей SNMPv3

Security Name

Диапазон настройки: 1~32 символа

Функция: Создание имени пользователя.

Engine ID

Диапазон настройки: Четное количество шестнадцатеричных чисел, не может быть полным 0 или полным F, четное количество значений варьируется от 10 до 64.

Функция: Настройка идентификатора механизма безопасности, передаваемого в пакетах Trap SNMP v3.

Security Level

Варианты конфигурации: NoAuthNoPriv/AuthNoPriv/AuthPriv

Функция: Настройка уровня безопасности текущего пользователя.

Описание: NoAuthNoPriv не требует ни аутентификации, ни конфиденциальности; AuthNoPriv требует аутентификацию, но не требует конфиденциальности; AuthPriv требует аутентификацию и конфиденциальность.

Authentication Protocol

Варианты конфигурации: MD5/SHA

Функция: Выбор протокола аутентификации. Протокол конфиденциальности и пароль конфиденциальности должны быть установлены, когда уровень безопасности установлен на AuthNoPriv/AuthPriv.

Authentication password

Диапазон настройки: 8~49 символов (протокол MD5) 8~32 символа (протокол SHA)

Функция: Создание пароля аутентификации.

Privacy Protocol

Варианты конфигурации: DES/AES

Функция: Выбор протокола конфиденциальности. Протокол конфиденциальности и пароль конфиденциальности должны быть установлены при выборе AuthPriv.

Privacy Password

Диапазон настройки: 8~32 символа Функция: Создание пароля конфиденциальности.

Можно настроить до 16 пользователей.

4. Настройте таблицу групп, как показано ниже.

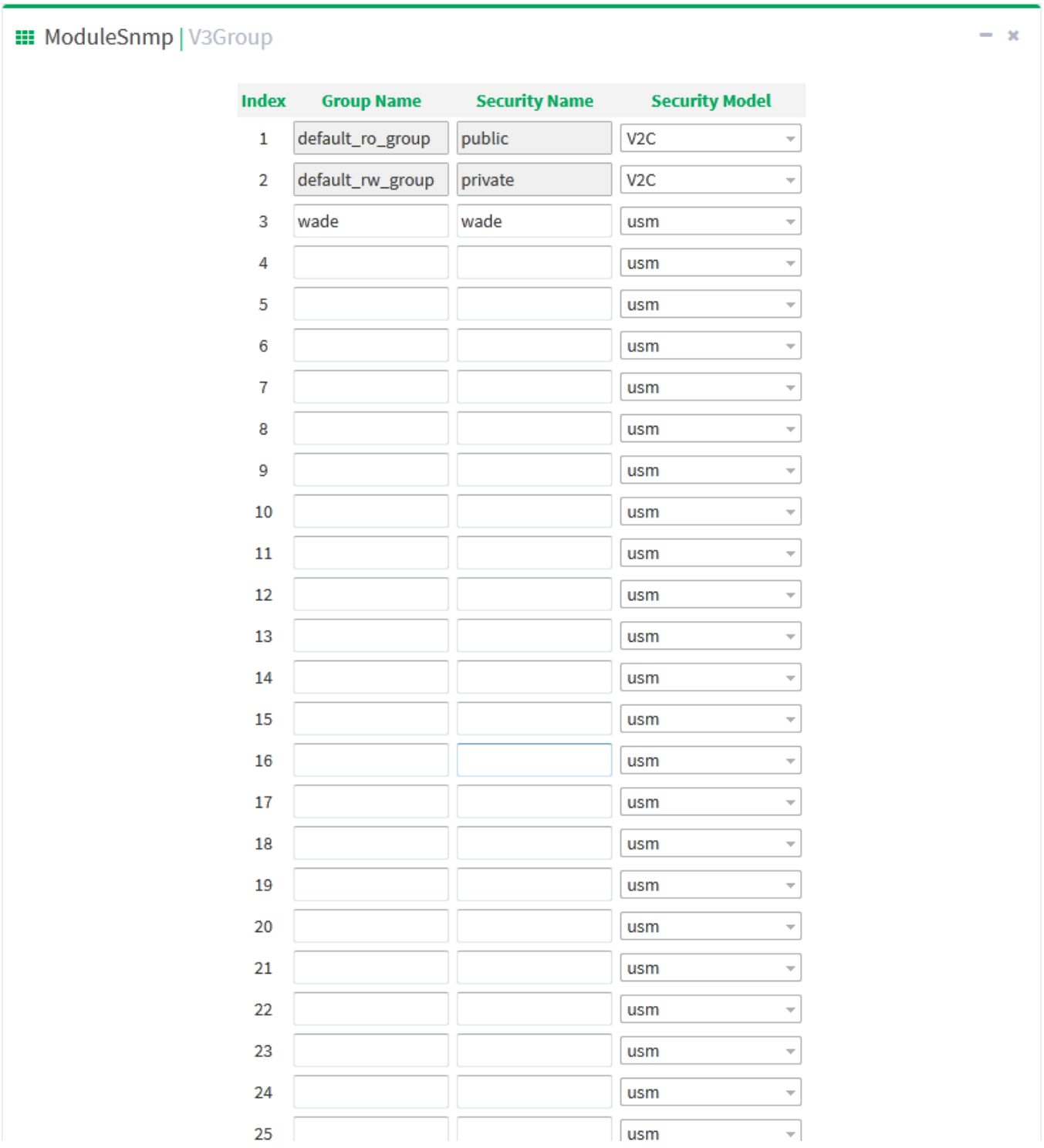


Рисунок 77 Настройка таблицы групп SNMPv3

Group Name

Диапазон настройки: 1~32 символа

Функция: Настройка имени группы. Пользователи с одинаковым именем группы принадлежат к одной группе.

Security Name

Диапазон настройки: Созданное имя пользователя, 1~32 символа

Функция: Настройка доверенного имени, доверенное имя должно совпадать с именем пользователя в таблице пользователей.

Пользователи с одинаковым именем группы принадлежат к одной группе.

Можно настроить до 32 групп.

Security Model

Конфигурация по умолчанию: SNMP v3

Функция: Выбор модели безопасности текущей группы (номер версии SNMP). SNMPv3 использует технологию USM (модель безопасности на основе пользователя), которая принудительно использует модель SNMP v3.

5. Настройте таблицу представлений, как показано ниже.

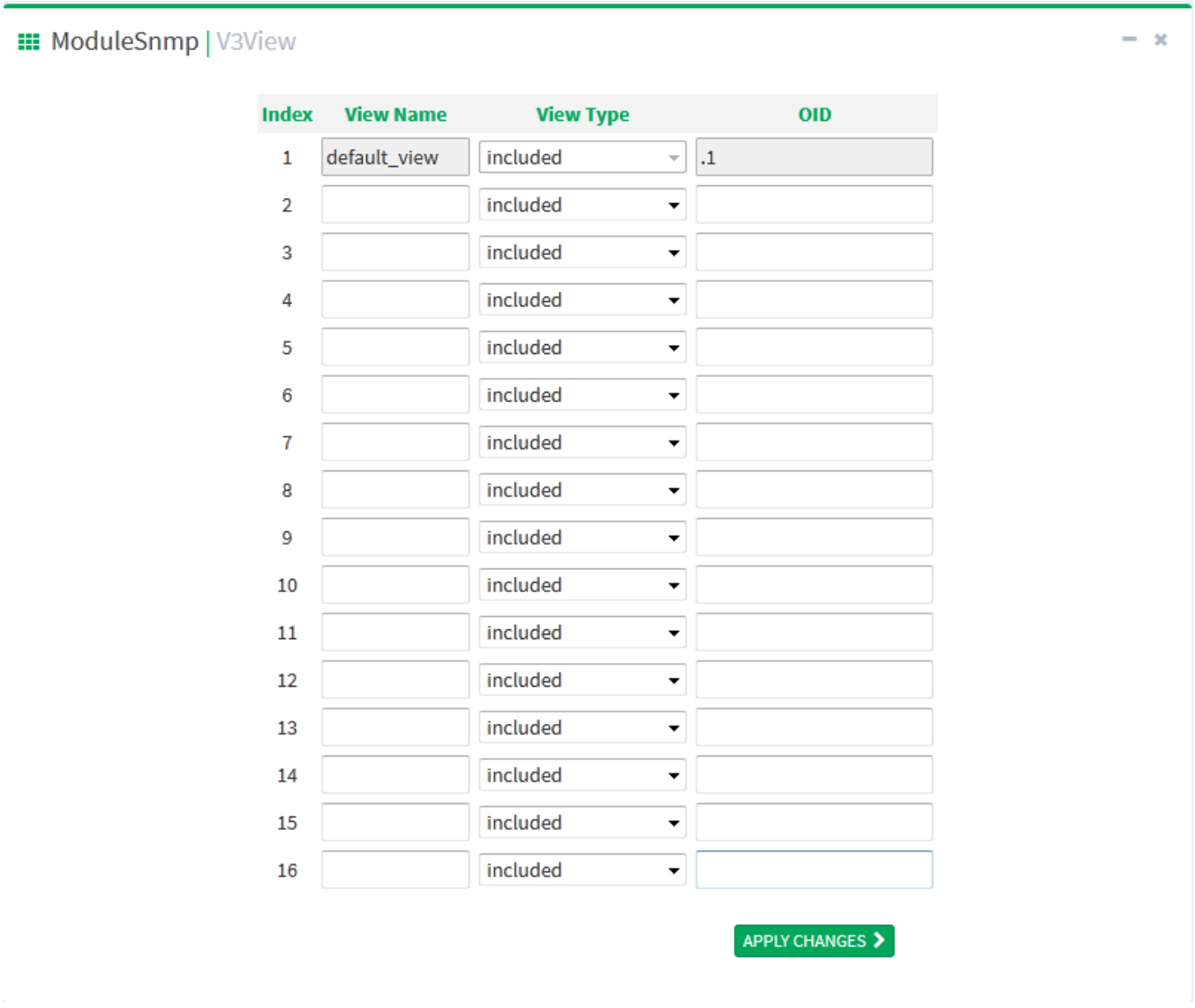


Рисунок 78 Настройка таблицы представлений SNMPv3

View Name

Диапазон настройки: 1~32 символа

Функция: Настройка имени представления.

View Type

Варианты: included/excluded

Функция: Included указывает, что текущее представление включает все узлы поддерева MIB, excluded указывает, что текущее представление не включает узлы поддерева MIB.

OID

Функция: Настройка поддерева MIB, представленного OID корневого узла поддерева.

Можно настроить до 16 представлений.

	**Примечание**: Таблица представлений по умолчанию default_view содержит все узлы поддерева 1 коммутатора.

6. Настройте таблицу доступа, как показано ниже.

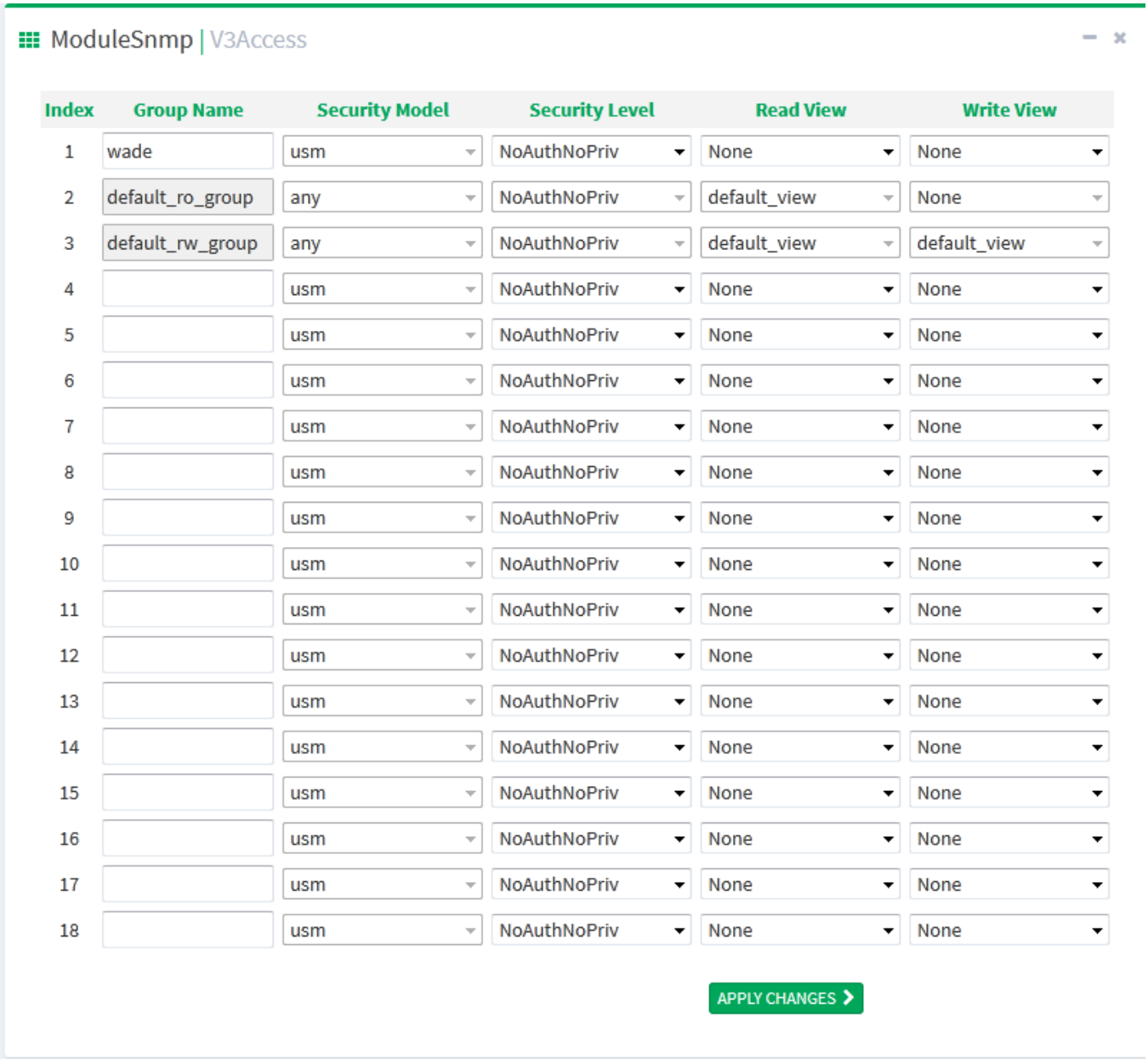


Рисунок 79 Настройка таблицы доступа SNMPv3

Group Name

Диапазон настройки: Созданное имя группы, 1~32 символа

Описание: Пользователи в группе имеют одинаковые права доступа.

Security Model

Конфигурация по умолчанию: any/v1/v2/usm

Функция: Выбор модели безопасности текущей группы (номер версии SNMP). SNMPv3 использует технологию USM (модель безопасности на основе пользователя), any означает, что можно использовать любую модель безопасности.

Имя группы и значение Security Model должны совпадать с именем группы и моделью безопасности в таблице групп.

Security Level

Варианты конфигурации: NoAuthNoPriv/AuthNoPriv/AuthPriv

Функция: Настройка уровня безопасности текущей группы.

Описание: NoAuthNoPriv не требует ни аутентификации, ни конфиденциальности; AuthNoPriv требует аутентификацию, но не требует конфиденциальности; AuthPriv требует аутентификацию и конфиденциальность. Когда требуется шифрование, протокол аутентификации/конфиденциальности, пароль аутентификации/конфиденциальности на стороне NMS должны соответствовать конфигурации таблицы пользователей, тогда можно будет успешно получить доступ к информации узла коммутатора.

Уровни безопасности NoAuthNoPriv, AuthNoPriv, AuthPriv перечислены по возрастанию. Более высокий уровень имеет доступ к более низкому уровню. Например, уровень безопасности группы настроен на AuthNoPriv. Пользователи с уровнями безопасности AuthNoPriv и AuthPriv в группе могут успешно получить доступ к коммутатору, если и протокол аутентификации/конфиденциальности, и пароль аутентификации/конфиденциальности верны; но пользователи с уровнем безопасности NoAuth,NoPriv не могут получить доступ.

Read View

Варианты конфигурации: default_view/None/Created view name

Функция: Выбор имени представления Readonly

Write View

Варианты конфигурации: default_view/None/Created view name

Функция: Выбор имени представления ReadWrite.

Можно настроить до 16 таблиц доступа.

	**Примечание**: Таблицы доступа по умолчанию {default_ro_group, any, No Auth, No Priv, default_view, None}, {default_rw_group, any, No Auth, No Priv, default_view, default_view}.

6.8.4 Пример типовой конфигурации

Станция управления SNMP подключена к коммутатору через Ethernet, IP-адрес станции управления — 192.168.0.23, а IP-адрес коммутатора — 192.168.0.2.

Пользователь 1111 и пользователь 2222 контролируют и управляют Агентом через SNMPv3, уровень безопасности AuthNoPriv, информация обо всех узлах в Агенте доступна только для чтения; Агент активно отправляет сообщение Trap v3 в NMS при возникновении тревоги, как показано на рисунке ниже.

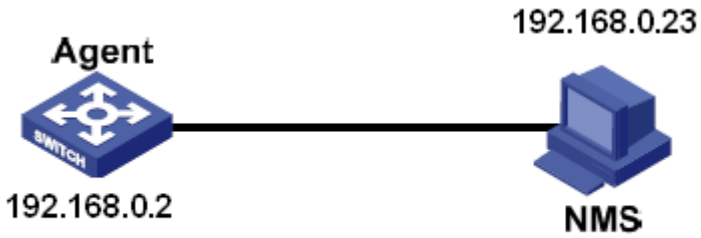


Рисунок 80 Пример настройки SNMPv3

Настройка агента показана ниже:

1. Включите протокол SNMP, см. рисунок 70.

2. Настройте таблицу пользователей SNMP v3.

User Name: 1111, security level: Auth,Priv, Authentication Protocol: MD5, authentication password: aaaaaaaa, privacy protocol: DES, privacy password: xxxxxxxx;

User Name: 2222, security level: Auth,Priv, Authentication Protocol: SHA, authentication password: bbbbbbbb, privacy protocol: AES, privacy password: yyyyyyyy; см. рисунок

76.

3. Создайте группу. security model: usm, включите пользователей 1111 и 2222, см. рисунок 77.

4. Настройте таблицу доступа SNMP v3.

Group name: group, security model: USM, security level: Auth,NoPriv, read view name: default_view, write view name: None, см. рисунок 78;

5. Включите модель Trap, см. рисунок 75.

6. Создайте элемент таблицы Trap 222 и включите модель Trap, выберите версию SNMP v3, IP-адрес назначения 192.168.0.23, выберите событие Trap для всех событий системы, интерфейса, аутентификации и коммутатора, для остальных используется конфигурация по умолчанию.

Для мониторинга и управления состоянием устройства-агента необходимо запустить в NMS соответствующее программное обеспечение для управления.

6.9 Файловый сервер

Служба передачи файлов может выполнять резервное копирование информации клиента и сервера. При изменении информации о файле клиента (сервера) файл резервной копии можно получить с сервера (клиента) посредством передачи файлов на основе протокола FTP/SFTP.

Коммутатор может служить клиентом или сервером для загрузки и выгрузки файлов через FTP/SFTP.

6.9.1 FTP

Коммутатор как клиент FTP. Сначала установите FTP-сервер, на примере программного обеспечения WFTPD познакомьтесь с процессом выгрузки и загрузки файлов конфигурации с FTP-сервера; 1. Щелкните [Security]→[users/rights], щелкните <New User> и добавьте нового пользователя FTP, как показано на рисунке ниже. Введите имя пользователя и пароль, например, имя пользователя: admin, пароль: 123, щелкните <OK>.

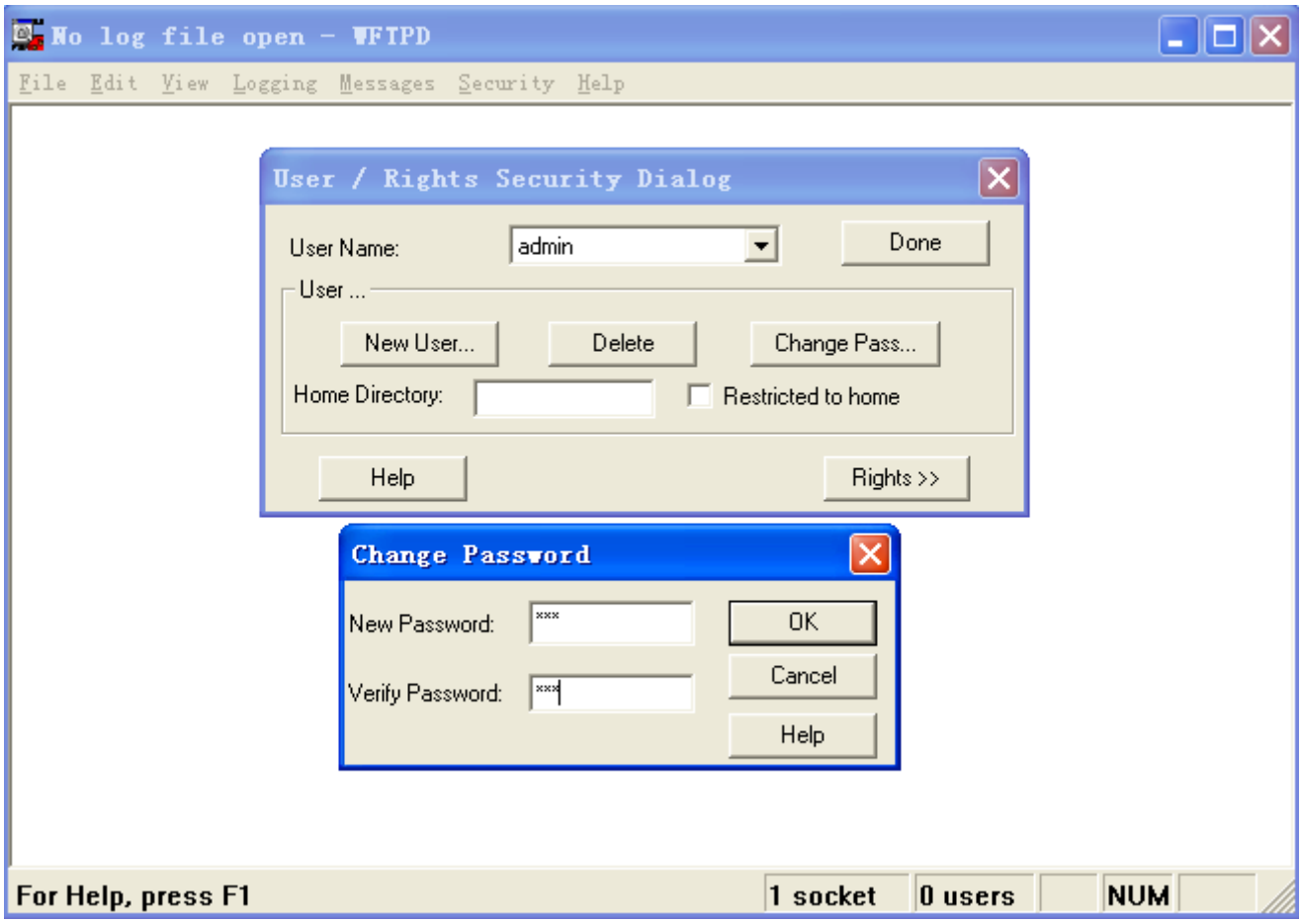


Рисунок 81 Добавление нового пользователя FTP

Введите путь хранения файла версии программного обеспечения на сервере в поле Home Directory, как показано на рисунке ниже, щелкните <Done>.

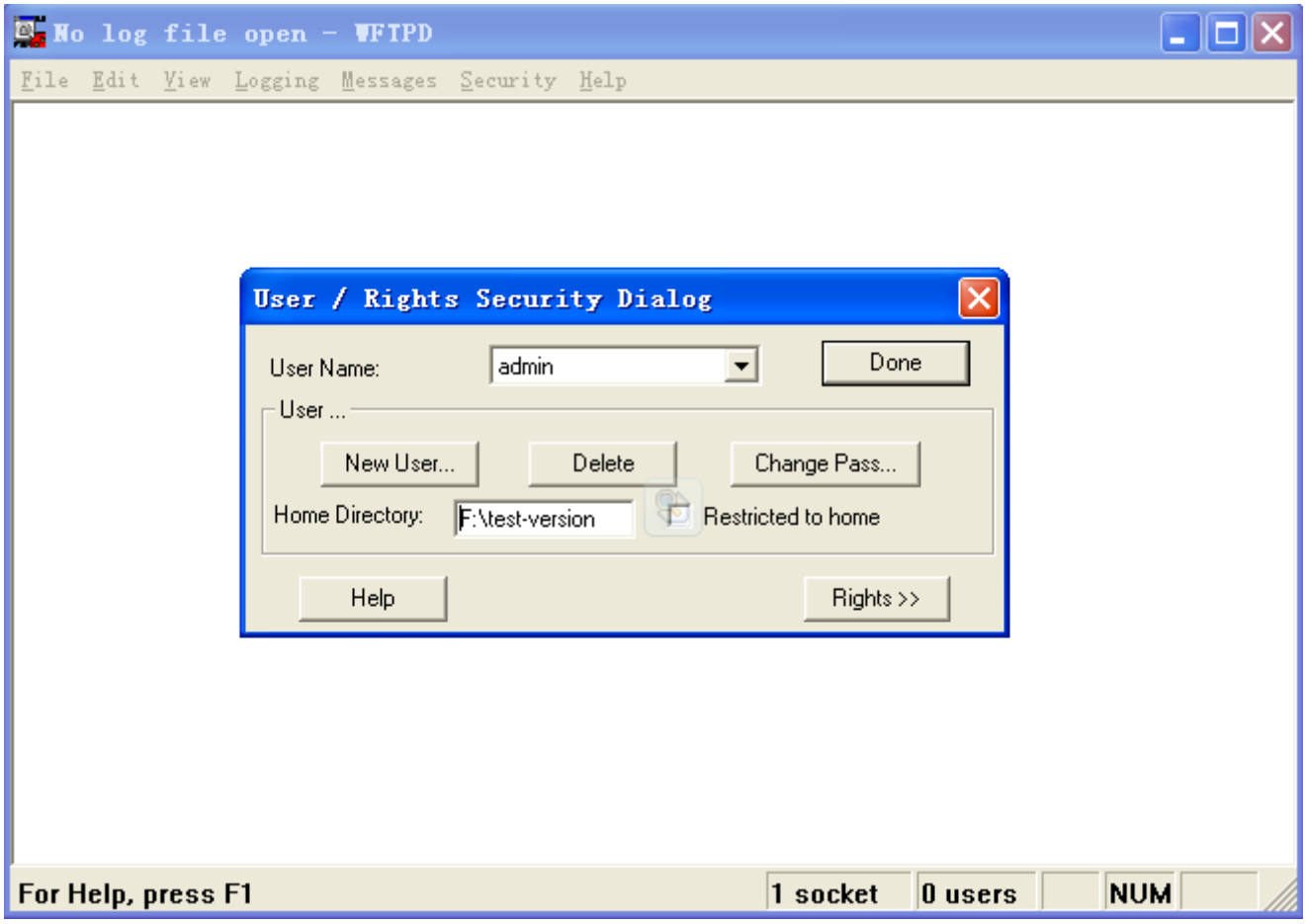


Рисунок 82 Изменение пути к файлу

Щелкните в дереве навигации [Other Configurations]→[File Server], перейдите на страницу настройки передачи файла, как показано на рисунке ниже.

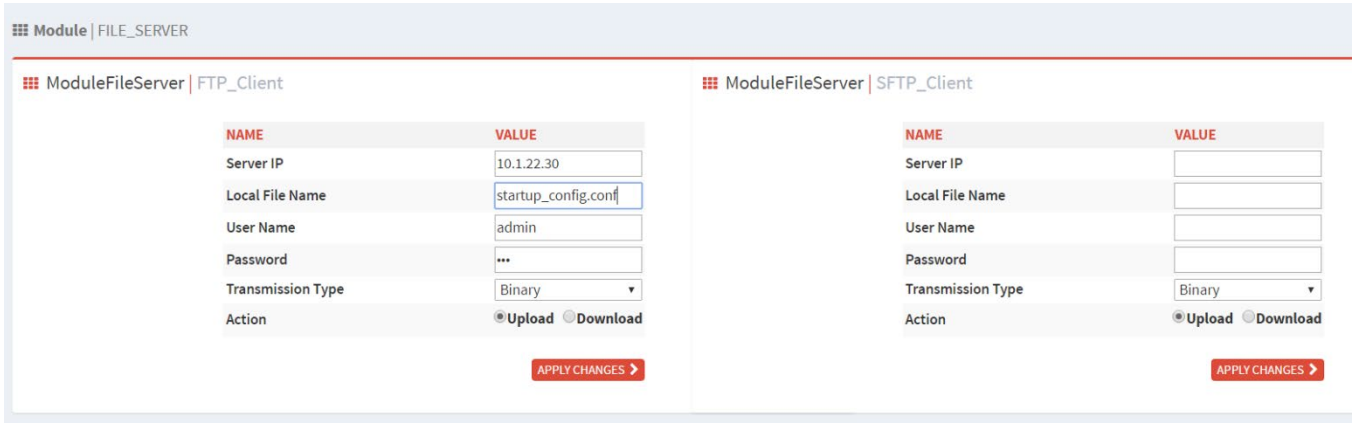


Рисунок 83 Настройка службы передачи файла

Можно настроить элементы протокола FTP или SFTP. Ниже показана настройка FTP в качестве клиента.

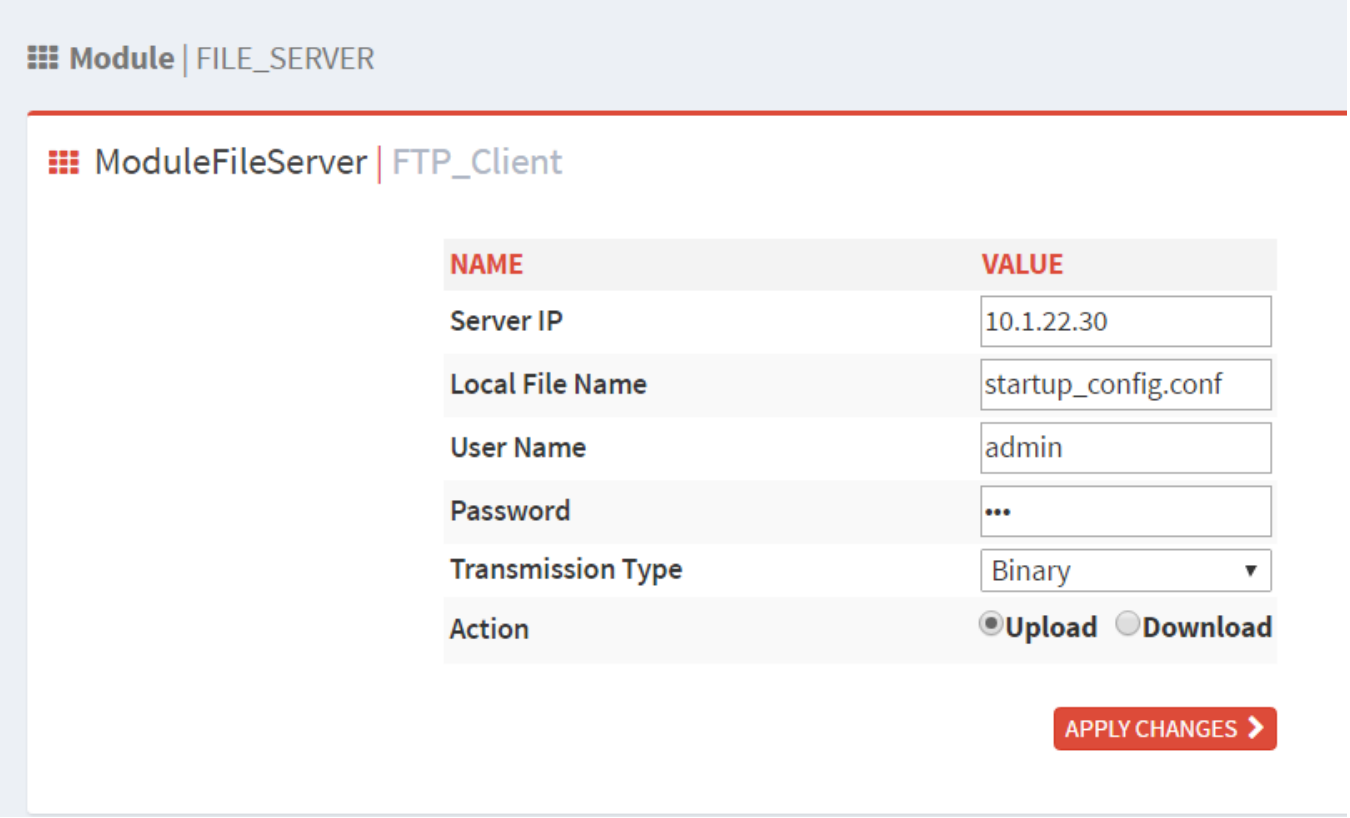


Рисунок 84 Настройка FTP

Server IP

Формат: A.B.C.D

Описание: Ввод IP-адреса сервера.

Server File Name

Диапазон настройки: 1~100 символов

Описание: имя файла на сервере

User Name

Имя пользователя на сервере

Password

Пароль пользователя

Transmission Type

Варианты конфигурации: binary/ascii

Конфигурация по умолчанию: binary

Функция: Выбор стандарта передачи файла.

Описание: ASCII указывает на передачу файла в стандарте ASCII; binary указывает на передачу файла в двоичном стандарте.

Action

Варианты конфигурации: upload/download

Функция: Upload: Выгрузка файла конфигурации коммутатора на удаленный сервер FTP.

Download: Загрузка файла конфигурации коммутатора с удаленного сервера FTP.

6.9.2 SFTP

SFTP (Secure File Transfer Protocol) — это протокол передачи файлов, основанный на SSH, который может шифровать файл и обеспечивать безопасность передачи.

Коммутатор как клиент SFTP. Сначала установите SFTP-сервер, на примере программного обеспечения MSFTP познакомьтесь с процессом выгрузки и загрузки файлов конфигурации с SFTP-сервера.

Добавьте пользователя SFTP, как показано на рисунке ниже, введите имя пользователя и пароль. User: admin, Password: 123; Port — номер порта 22 протокола SFTP; в строке Root path введите путь хранения файлов версии программного обеспечения сервера, щелкните <Start>.

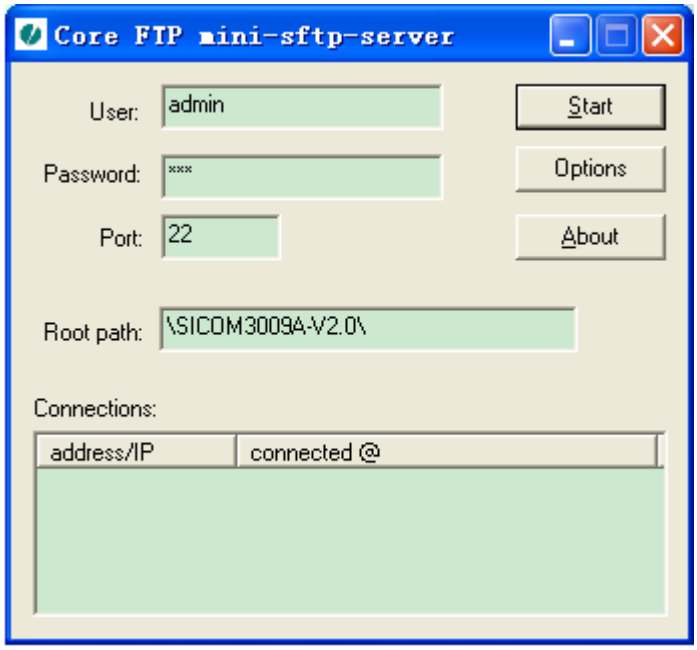


Рисунок 85 Добавление нового пользователя SFTP

Щелкните в дереве навигации [Other Configurations]→[File Server], перейдите на страницу настройки передачи файла, как показано на рисунке ниже.

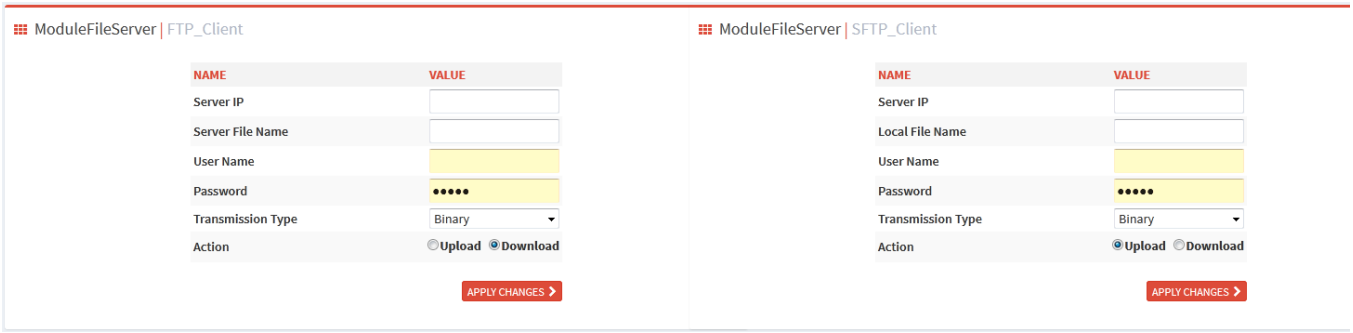


Рисунок 86 Настройка службы передачи файла

Можно настроить элементы протокола FTP или SFTP. Ниже показана настройка SFTP в качестве клиента.

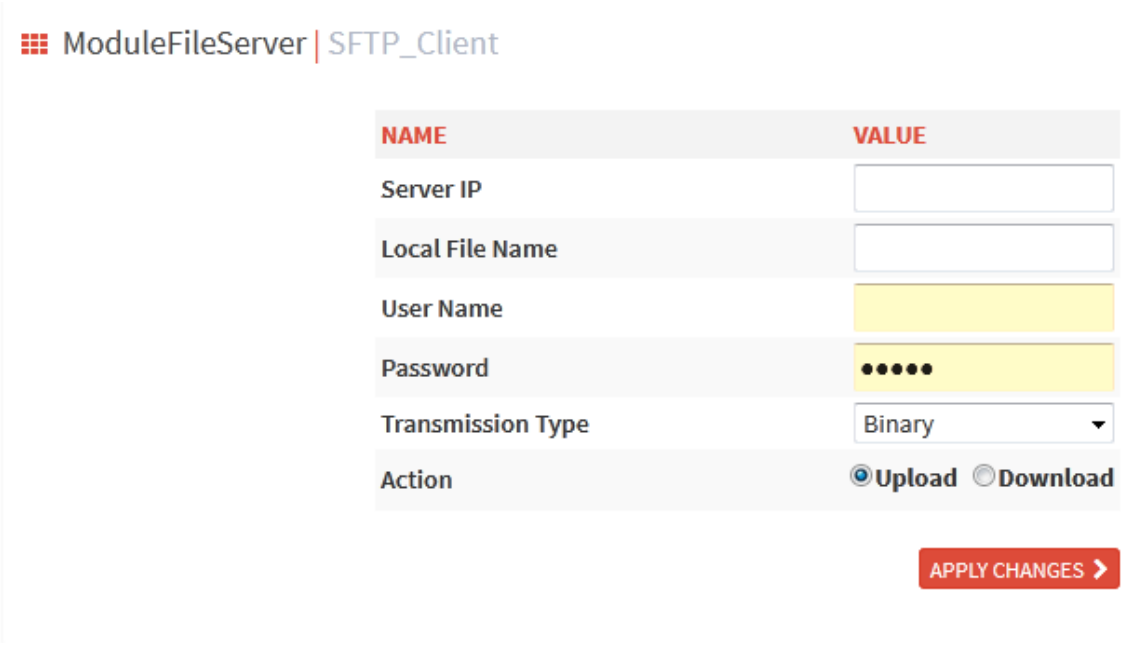


Рисунок 87 Настройка передачи по SFTP

Server IP

Формат: A.B.C.D

Описание: Ввод IP-адреса сервера.

Local File Name

Диапазон настройки: 1~100 символов

Описание: имя файла в коммутаторе.

User Name

Имя пользователя, соответствующее FTP-серверу

Password

Пароль пользователя

Transmission Type

Варианты конфигурации: binary/ascii

Конфигурация по умолчанию: binary

Функция: Выбор стандарта передачи файла.

Описание: ASCII указывает на передачу файла в стандарте ASCII; binary указывает на передачу файла в двоичном стандарте.

Action

Варианты конфигурации: upload/download

Функция: Upload: Выгрузка файла конфигурации коммутатора на удаленный сервер FTP Download: Загрузка файла конфигурации коммутатора с удаленного сервера FTP.

6.10 LLDP

6.10.1 Введение

Протокол обнаружения канального уровня Link Layer Discovery Protocol (LLDP) предоставляет стандартный механизм обнаружения канального уровня. Он инкапсулирует информацию об устройстве, такую как возможности, адрес управления, идентификатор устройства и идентификатор интерфейса, в блок данных протокола обнаружения канального уровня (LLDPDU) и объявляет LLDPDU своим непосредственно подключенным соседям. Получив LLDPDU, соседи сохраняют эту информацию в MIB для запроса и проверки состояния канала NMS.

6.10.2 Настройка через веб-интерфейс

1. Настройте LLDP

Щелкните в дереве навигации [Other Configurations]→[Lldp], перейдите на страницу настройки LLDP, как показано на рисунке ниже.

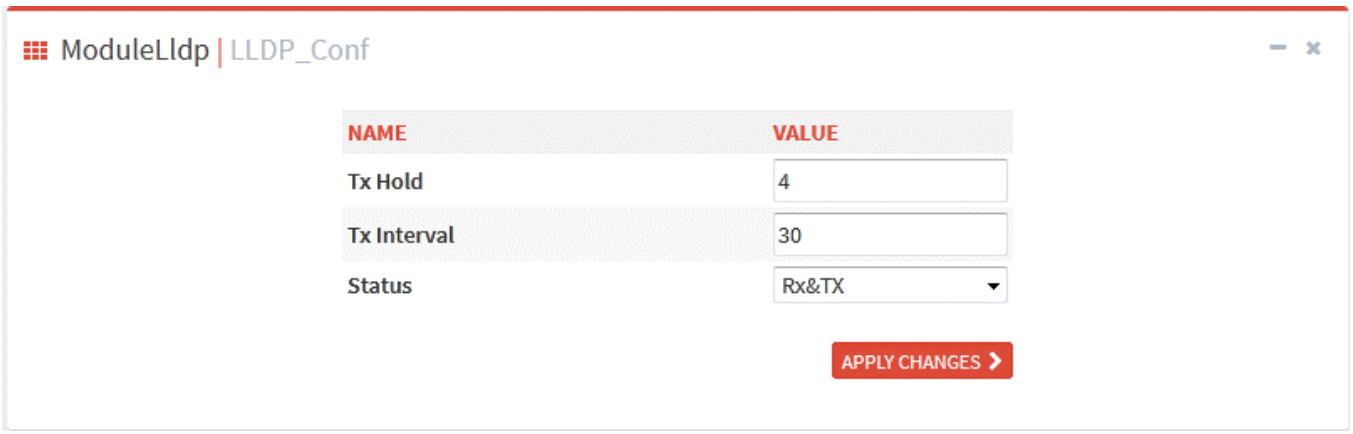


Рисунок 88 Настройка LLDP

Tx Hold

Диапазон настройки: 2~10 раз

Конфигурация по умолчанию: 4 раза

Функция: Настройка Tx Hold Допустимое время сообщения LLDP = Tx interval × Tx hold.

Tx Interval

Диапазон настройки: 5~32768 с

Конфигурация по умолчанию: 30 с

Функция: Настройка интервала времени для периодической отправки сообщений LLDP.

Status

Варианты конфигурации: Rx&Tx/Disable/RxOnly/TxOnly

Конфигурация по умолчанию: Rx&Tx

Функция: Настройка статуса сообщения LLDP. Rx&Tx означает, что коммутатор не только отправляет сообщения LLDP, но также получает и распознает сообщения LLDP. Disable указывает, что коммутатор не отправляет сообщения LLDP и не принимает сообщения LLDP; RxOnly указывает, что коммутатор только принимает и распознает сообщения LLDP; TxOnly указывает, что коммутатор только отправляет сообщения LLDP и не принимает сообщения LLDP.

2. Просмотрите информацию LLDP, как показано на рисунке ниже.

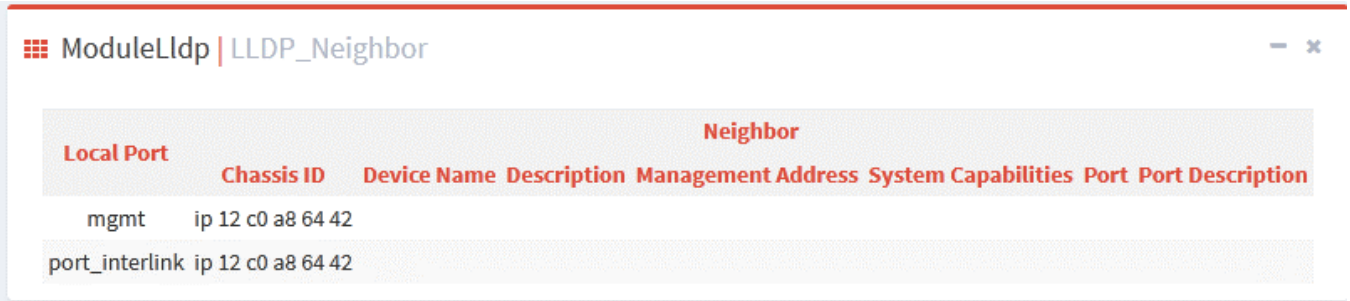


Рисунок 89 Информация LLDP

6.11 DDMI

6.11.1 Введение

Оптический модуль интерфейса цифрового диагностического монитора (DDMI) также называется интеллектуальным модулем. За счет добавления микросхемы и вспомогательной схемы блок может контролировать температуру модуля приемопередатчика, напряжение питания, ток смещения лазера, а также передавать и получать оптическую мощность в реальном времени. Эти параметры могут помочь блоку управления определить место неисправности оптоволоконной линии, упростить работы по техническому обслуживанию и повысить надежность системы.

6.11.2 Настройка через веб-интерфейс

Щелкните в дереве навигации [Other Configurations]→[Ddmi], перейдите на страницу настройки DDMI, как показано на рисунке ниже.

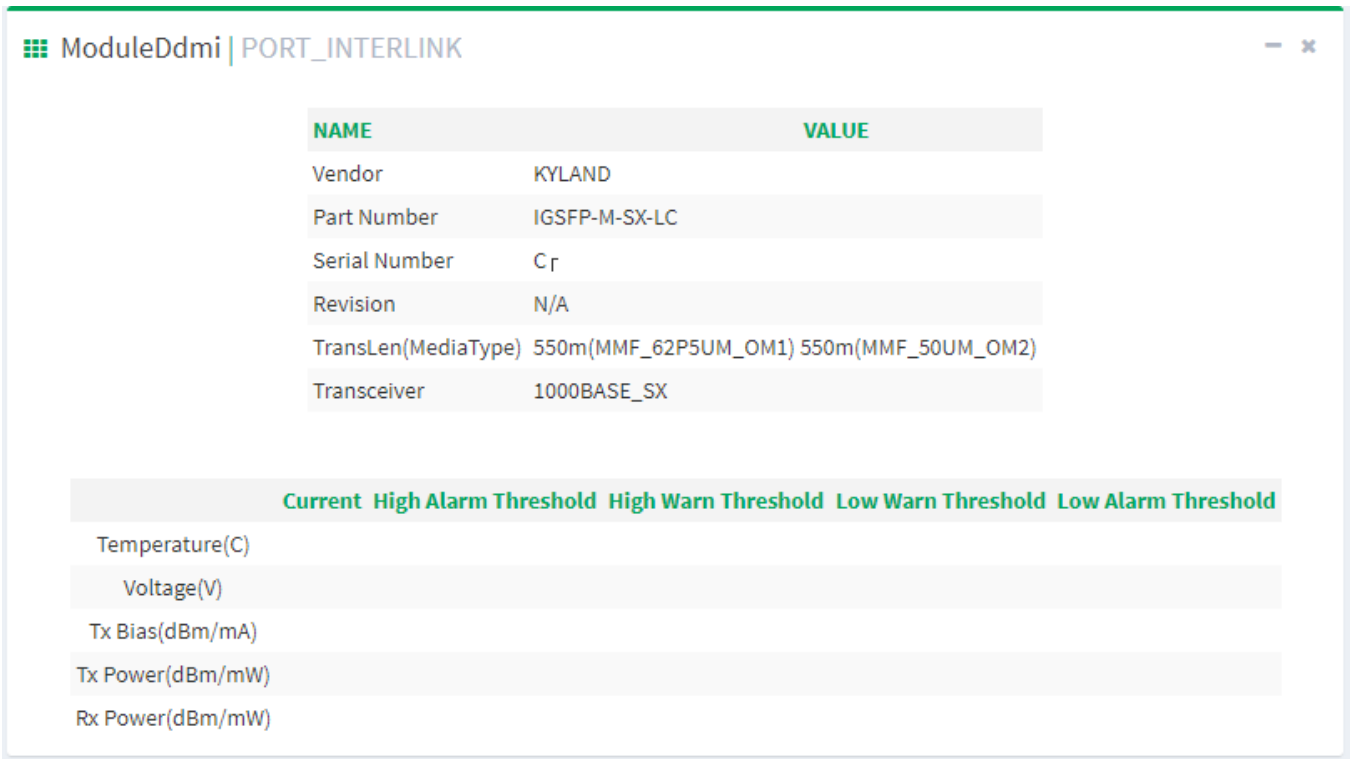


Рисунок 90 Информация оптического модуля порта L

Возьмем в качестве примера порт L: после установки оптического модуля мы можем прочитать основную информацию об оптическом модуле. Эта информация включает в себя базовую информацию: поставщик, артикул, серийный номер, версия, расстояние передачи и приемопередатчик. Некоторые подключаемые оптические модули также поддерживают более сложные информационные запросы, включая температуру, напряжение, смещение Tx, мощность Tx и мощность Rx.

6.12 Виртуальный тест кабеля

6.12.1 Введение

VCT (Virtual Cable Tester) использует технологию Time Domain Reflectometry (TDR) для определения состояния витой пары. Он передает импульсный сигнал кабелю и обнаруживает отражение импульсного сигнала для обнаружения неисправности кабеля. Если в кабеле происходит аварийное переключение, часть или вся энергия импульса будет отражаться обратно к источнику, когда передаваемый импульсный сигнал достигает конца кабеля или точки повреждения, и технология VCT может измерять время прибытия сигнала в точку повреждения и время возврата к отправителю, затем вычисляет расстояние в соответствии со временем.

Технология VCT может обнаруживать среду соединения, соединяющую медные порты Ethernet, и отправлять обратно результат обнаружения. VCT может обнаруживать следующие типы повреждений кабеля:

Short: означает короткое замыкание. Это замыкание двух и более проводов.

Open: означает разомкнутую цепь. В кабеле могут быть оборванные провода.

Normal: означает нормальное кабельное соединение.

Imped: означает несоответствие импеданса. Например, импеданс кабеля Cat.5 составляет 100 Ом, импеданс терминаторов на обоих концах кабеля должен быть 100 Ом, чтобы избежать отражения волны и ошибки данных.

Fail: означает, что тест VCT не пройден.

6.12.2 Настройка через веб-интерфейс

Щелкните в дереве навигации [Other Configurations]→[Virtual Cable Test], перейдите на страницу настройки VCT, как показано на рисунке ниже.

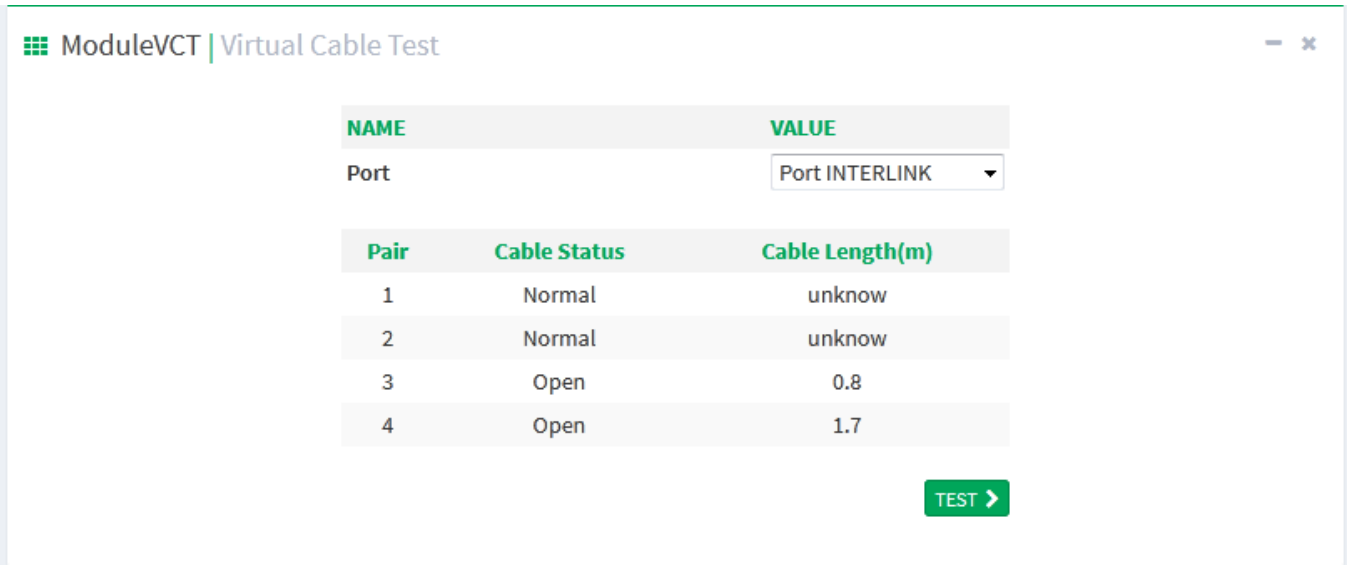


Рисунок 91 Страница настройки VCT

Port

Диапазон настройки: port_a/port_b/port_interlink

Конфигурация по умолчанию: port_a

Функция: Выбор соответствующего порта для обнаружения кабеля.

Выбрав порт, щелкните кнопку <TEST>, чтобы проверить подключение кабеля, как показано выше.

Pair

Число пар кабеля. Пара – это два медных провода.

Cable Status

Есть три состояния – Normal/Open/Short.

Normal: Нормальное подключение кабеля

Open В кабеле могут быть обрывы.

Short: Это замыкание двух и более проводов.

Cable Length (m)

Примерное расстояние точки повреждения от порта коммутатора, единица измерения — метр. Если кабель исправен, длина кабеля отображается как Unknown.

6.13 RADIUS

6.13.1 Введение

RADIUS (Remote Authentication Dial-In User Service) — это распределенный протокол обмена информацией. Он определяет формат кадра RADIUS на основе UDP и механизм передачи информации, защищая сети от несанкционированного доступа. RADIUS обычно используется в сетях, требующих высокой безопасности и удаленного доступа пользователей.

RADIUS использует режим клиент/сервер для обеспечения связи между NAS (сервером доступа к сети) и сервером RADIUS. Клиент RADIUS работает на NAS. Сервер RADIUS обеспечивает централизованное управление пользовательской информацией. NAS — это сервер для пользователей, но клиент для сервера RADIUS. На рисунке 92 показана структура.

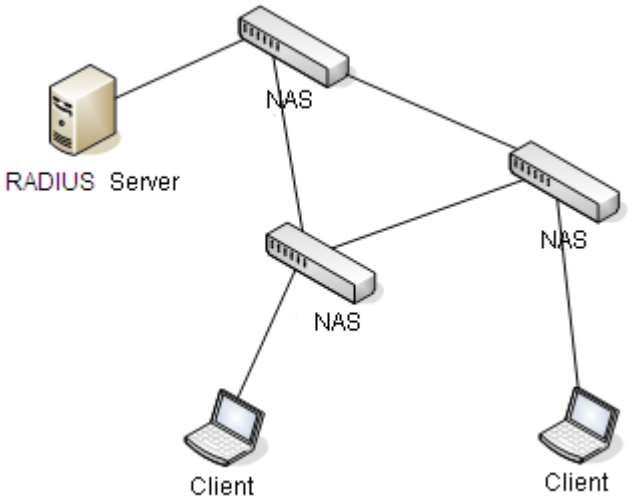


Рисунок 92 Структура RADIUS

Протокол аутентифицирует пользователей терминалов, которым необходимо войти в устройство для выполнения операций. Выступая в качестве клиента RADIUS,

устройство отправляет информацию о пользователе на сервер RADIUS для аутентификации и разрешает или запрещает пользователям входить в систему в соответствии с результатами аутентификации.

6.13.2 Настройка через веб-интерфейс

1. Настройка аутентификации RADIUS.

Щелкните в дереве навигации [Other Configurations]→[Radius], перейдите на страницу настройки RAIDUS, как показано на рисунке ниже.

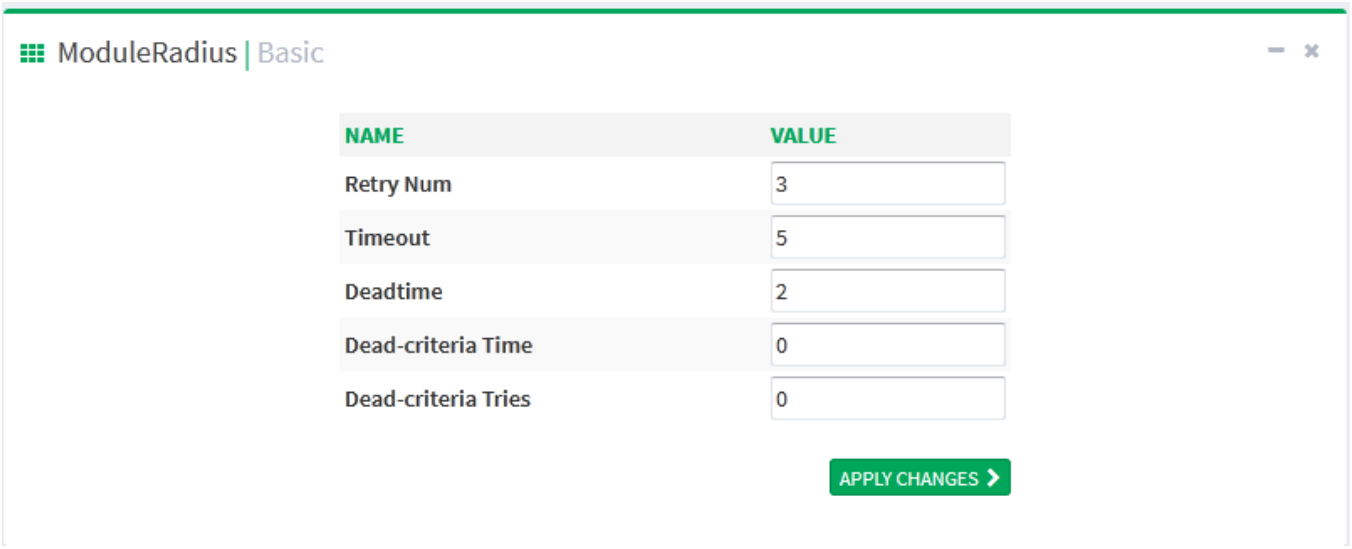


Рисунок 93 Настройка параметров аутентификации RADIUS

Retry Num

Диапазон настройки: 1~3

Конфигурация по умолчанию: 3

Функция: Настройка числа повторов RADIUS для тайм-аута сообщения. Если общее количество повторных попыток превышает значение, заданное в конфигурации, а сервер RADIUS по-прежнему не отвечает, устройство определит аутентификацию как ошибочную.

Timeout

Диапазон настройки: 1~3 с

Конфигурация по умолчанию: 3 с

Функция: Настройка таймаута ответа сервера RADIUS. Если в течение этого периода после отправки сообщения запроса RADIUS не будет получен ответ от сервера RADIUS, сообщение запроса будет отправлено повторно. Deadtime

Диапазон: 1-1440

По умолчанию: 2

Когда сервер Radius признан недействительным, необходимо закрыть его на некоторое время. По истечении времени простоя сервер Radius возвращается в допустимое состояние. Это уменьшает количество запросов к недействительному серверу.

Dead-criteria Time

Диапазон: 3-120

По умолчанию: 0

Функция: Длительность таймаута в секундах.

Описание: Задание ограничение времени ожидания сервера, чтобы определить, является ли сервер недействительным.

Dead-criteria Tries

Диапазон: 1-100

По умолчанию: 0

Функция: Число попыток

Описание: Задание предельного количества попыток, чтобы определить, является ли сервер недействительным.

2. Настройка сервера RADIUS показана на рисунке ниже.

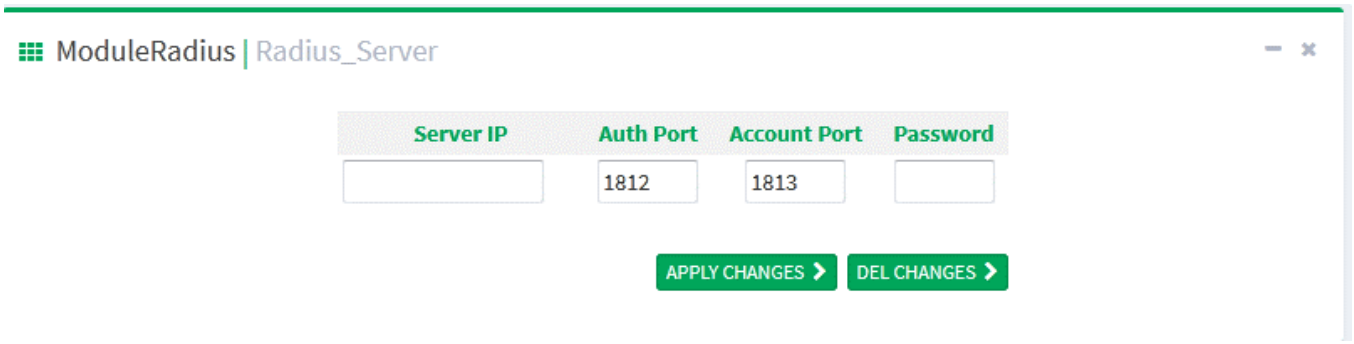


Рисунок 94 Настройка сервера RADIUS

Server IP

Формат: A.B.C.D

Функция: Настройка IP-адреса сервера RADIUS, поддерживается до 5 серверов RADIUS.

Auth Port

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 1812

Функция: Настройка номера порта UDP сервера RADIUS.

Account Port

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 1813

Функция: Настройка номера порта UDP сервера RADIUS.

Password

Диапазон настройки: 1~32 символа

Функция: Настройка пароля сервера RADIUS.

6.13.3 Пример типовой конфигурации

1. Топология

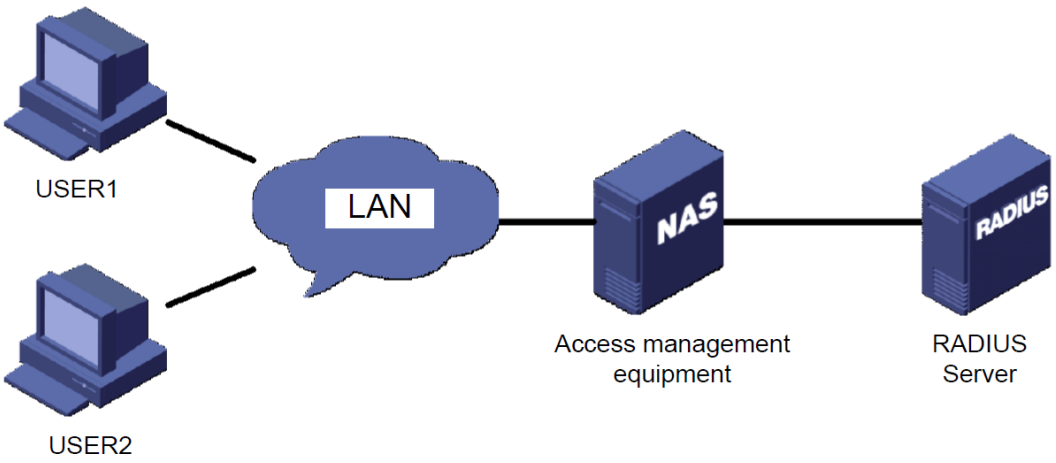


Рисунок 95 Типовая сеть

2. Требования к конфигурации

a. Вход пользователя в устройство управления через vty0 с аутентификацией AAA.

b. IP-адрес сервера аутентификации Radius и учетных записей — 192.168.1.1, порт аутентификации — 1812, порт учетной записи — 1813, ключ аутентификации test.

3. См. пример настройки через веб-интерфейс 6.13.2.

6.14 TACACS Plus

6.14.1 Введение

TACACS+ (Terminal Access Controller Access Control System) представляет собой приложение на основе TCP.

Оно использует режим клиент/сервер для реализации связи между сервером доступа к сети (NAS) и сервером TACACS+. Клиент работает на NAS, а информация о пользователях управляется централизованно на сервере. NAS — это сервер для пользователей, но клиент для сервера.

На рисунке 96 показана структура.

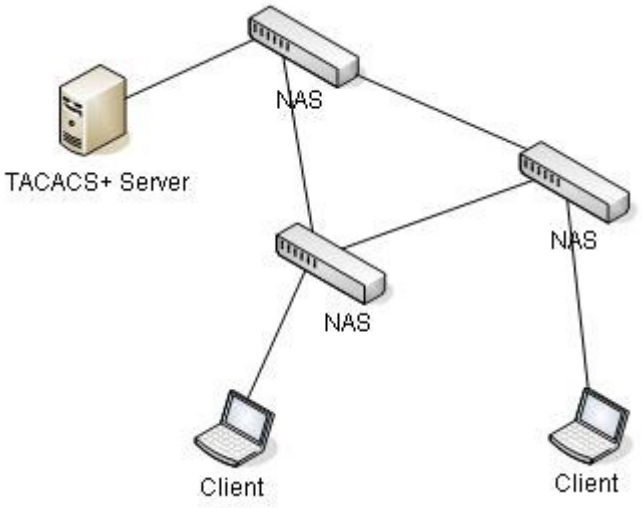


Рисунок 96 Структура TACACS+

Протокол аутентифицирует, авторизует и учитывает пользователей терминалов, которым необходимо войти на устройство для выполнения операций. Устройство служит клиентом TACACS+ и отправляет имя пользователя и пароль на сервер TACACS+ для аутентификации. Сервер получает запросы TCP-соединения от пользователей, отвечает на запросы аутентификации и проверяет легитимность пользователей. Если пользователь проходит аутентификацию, он может войти на устройство для выполнения операций.

6.14.2 Настройка через веб-интерфейс

1. Включите протокол TACACS+.

Щелкните в дереве навигации [Other Configurations]→[Tacacs plus], перейдите на страницу настройки TACACS+, как показано на рисунке ниже.

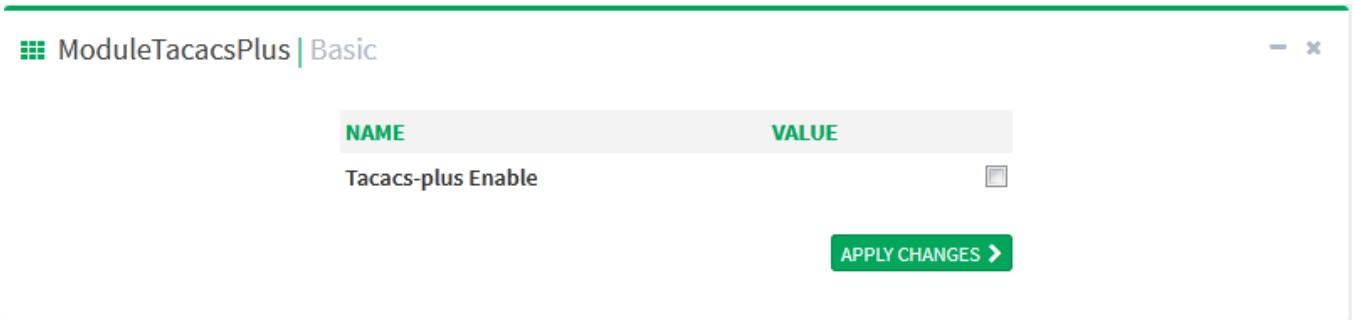


Рисунок 97 Включение протокола TACACS+

Tacacs-plus Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение протокола TACACS+.

2. Настройка сервера TACACS+ показана на рисунке ниже.

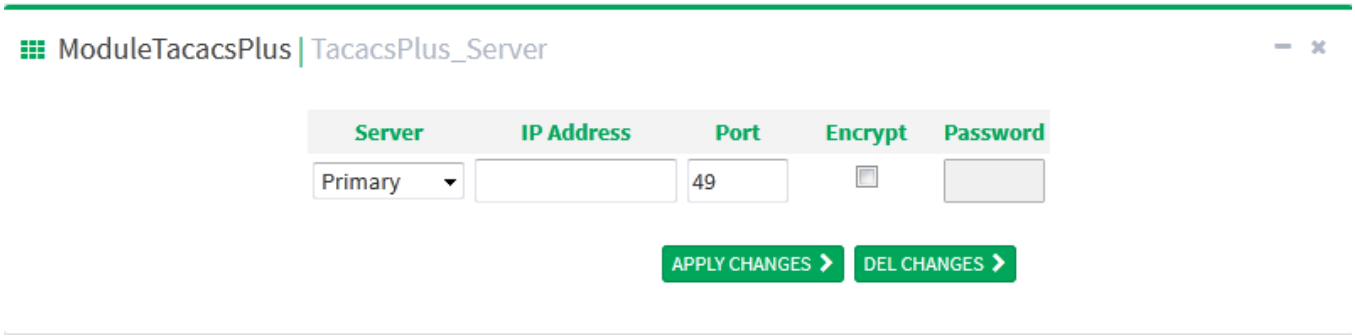


Рисунок 98 Настройка сервера TACACS+

Server

Варианты конфигурации: Master server/Slave сервер

Конфигурация по умолчанию: Master server

Функция: Выбор типа сервера текущей конфигурации.

IP-адрес

Формат: A.B.C.D

Функция: Ввод IP-адреса сервера.

Port

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 49

Функция: Номер порта, который получает запросы аутентификации NAS.

Encrypt

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или отключение шифрования. При включении необходим ввод ключа шифрования.

Password

Диапазон настройки: 1~32 символа

Описание: Настройка ключа для повышения безопасности связи клиента с сервером TACACS+. И клиент, и сервер могут проверить легитимность сообщения, совместно используя ключ устройства. Только когда ключ согласован, оба получают сообщение, отправленное другим, и отвечают друг другу, поэтому необходимо убедиться, что ключ общего доступа, настроенный на устройстве, точно такой же, как ключ на сервере TACACS+.

После завершения настройки информация о конфигурации сервера отображается в списке серверов, как показано ниже;

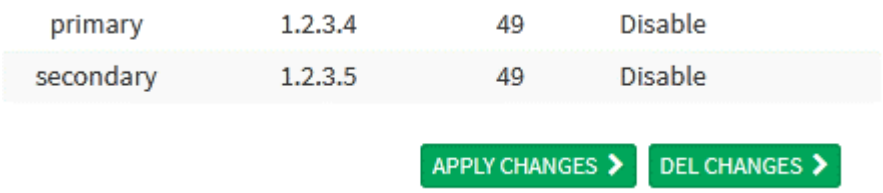


Рисунок 99 Список настроек сервера

6.14.3 Пример типовой конфигурации

Как показано на рисунке ниже, TACACS+ выполняет аутентификацию и авторизацию пользователя через коммутатор. IP-адрес сервера — 192.168.0.23, общий ключ при взаимодействии коммутатора с сервером — aaa.

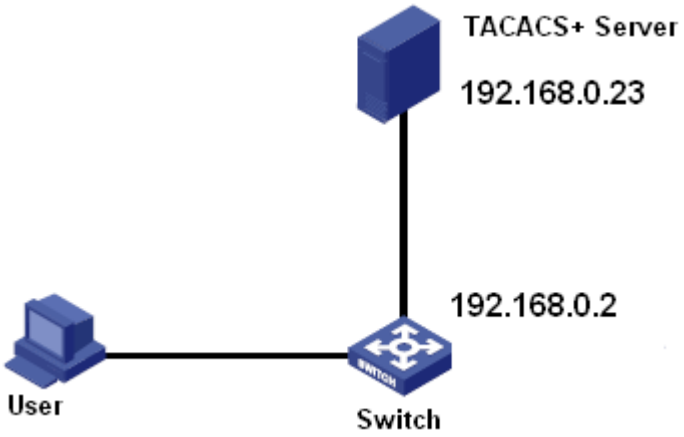


Рисунок 100 Пример аутентификации TACACS+

См. пример настройки TACACS+ через веб-интерфейс 6.14.2.

6.15 AAA

6.15.1 Введение

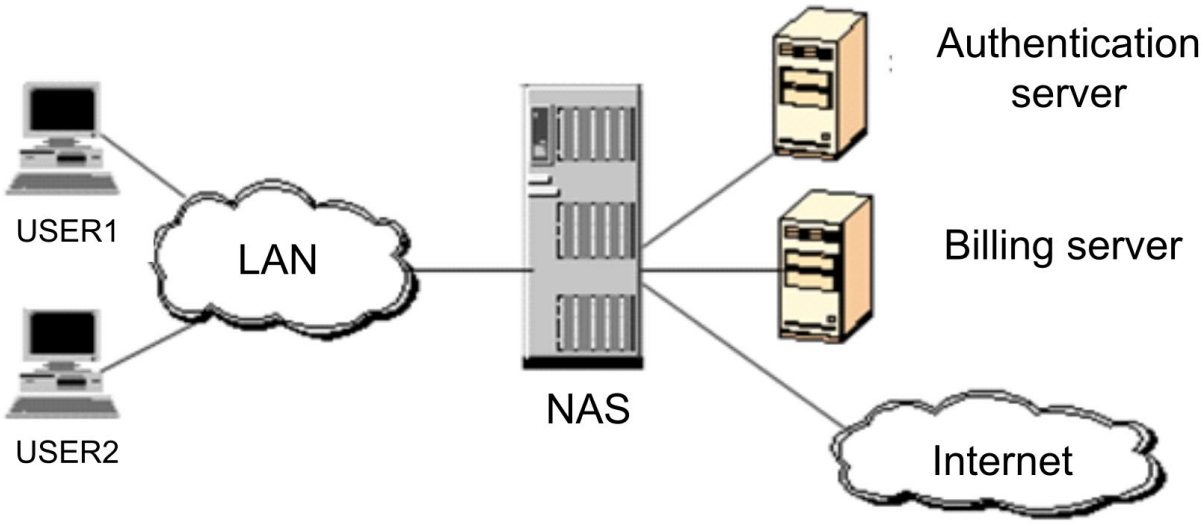


Рисунок 101 Структура AAA

Чтобы повысить безопасность сети, необходимо контролировать разрешения ресурсов в сети. Протокол AAA может предоставлять сервисы аутентификации, авторизации и учетных записей для эффективного решения проблем безопасности сетевых ресурсов и учетных записей.

AAA состоит из двух частей для реализации сервисов: Модуль AAA для обработки запросов доступа пользователя и модуль RADIUS для предоставления сервисов AAA.

AAA состоит из двух частей для реализации сервисов: Структура управления AAA для обработки запросов доступа пользователя и клиента RADIUS для предоставления сервисов AAA.

Структура управления AAA: Взаимодействует напрямую с пользователем, управляет сервисами AAA, необходимыми пользователю, и информацией запрашивающего пользователя. В то же время отправляет запросы пользователя на конкретный сервер AAA (например, RADIUS).

Структура управления AAA в процессе предоставления доступа AAA требует аутентификации для проверки легитимности пользователей. Авторизация может выполняться только после сертификации и аутентификации. Авторизация – это предоставление необходимой информации о доступе пользователей для успешного входа в сеть. Служба учетных записей (дополнительно) регистрирует успешную аутентификацию пользователей или учитывает трафик.

Клиент RADIUS: Реализует обмен данными между пользователем AAA и сервером RADIUS. Клиент RADIUS преобразует запрос AAA пользователя в сообщение протокола RADIUS, которое отправляется на сервер RADIUS; сервер RADIUS отправляет результат запроса пользователя клиенту RADIUS, клиент RADIUS обрабатывает результат запроса, отправляет обратную связь в структуру управления AAA, и, наконец, пользователь получает результат запроса.

6.15.2 Настройка через веб-интерфейс

1. Включите AAA

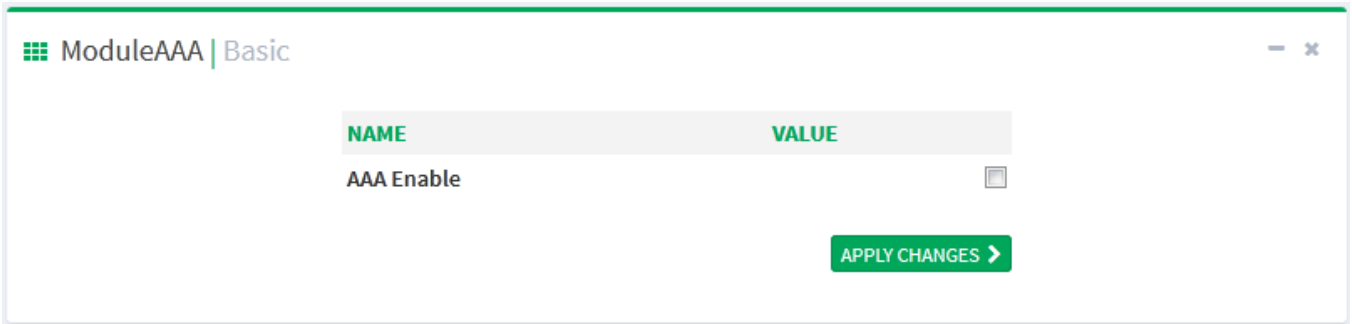


Рисунок 102 Включение AAA

Глобальное включение AAA только включает AAA, соответствующие службы можно настроить. Если отключить AA, ранее примененные службы AAA станут недействительными. Настройте режим входа в систему для доступа к коммутатору, а также режим аутентификации и последовательность аутентификации.

2. Настройка аутентификации

Щелкните в дереве навигации [Other Configurations]→[AAA], перейдите на страницу настройки входа для аутентификации, как показано на рисунке ниже.

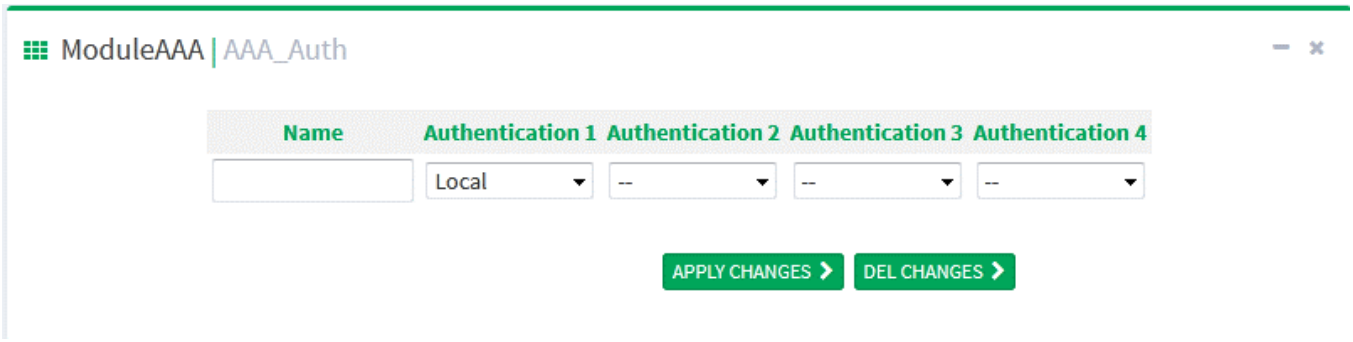


Рисунок 103 Настройка аутентификации

Authentication Name

Варианты конфигурации: Telnet/Web/dot1x/SSH

Функция: Выбор режима входа для доступа к коммутатору.

Authentication 1/ Authentication 2/ Authentication 3/ Authentication 4

Варианты конфигурации: Local/Tacacs+/Radius/None

Конфигурация по умолчанию: Local

Функция: Выбор порядка аутентификации для входа. Сначала использовать аутентификацию 1. Если она не пройдена, использовать аутентификацию 2. Если первые две аутентификации не пройдены, использовать аутентификацию. Если все предыдущие аутентификации неудачны, использовать режим аутентификации 4.

Описание: Local означает использование для выполнения аутентификаци имени пользователя и пароля, установленных в локальном компьютере. Tacacs+ означает использование для аутентификации имени пользователя и пароля, установленных на сервере Tacacs+. Radius означает использование для аутентификации имени пользователя и пароля, установленных на сервере Radius.

6.16 LINE

6.16.1 Введение

Line, как логический интерфейс управления терминалом, делится на два типа: line console и line vty. Line console соответствует входу в консоль, line vty соответствует общим протоколам входа, включая telnet. Настройки для обоих типов в основном одинаковы, оба типа поддерживаются без специальных инструкций.

6.16.2 Настройка через веб-интерфейс

Щелкните в дереве навигации [Other Configurations]→[Line], перейдите на страницу настройки Line, как показано на рисунке ниже.

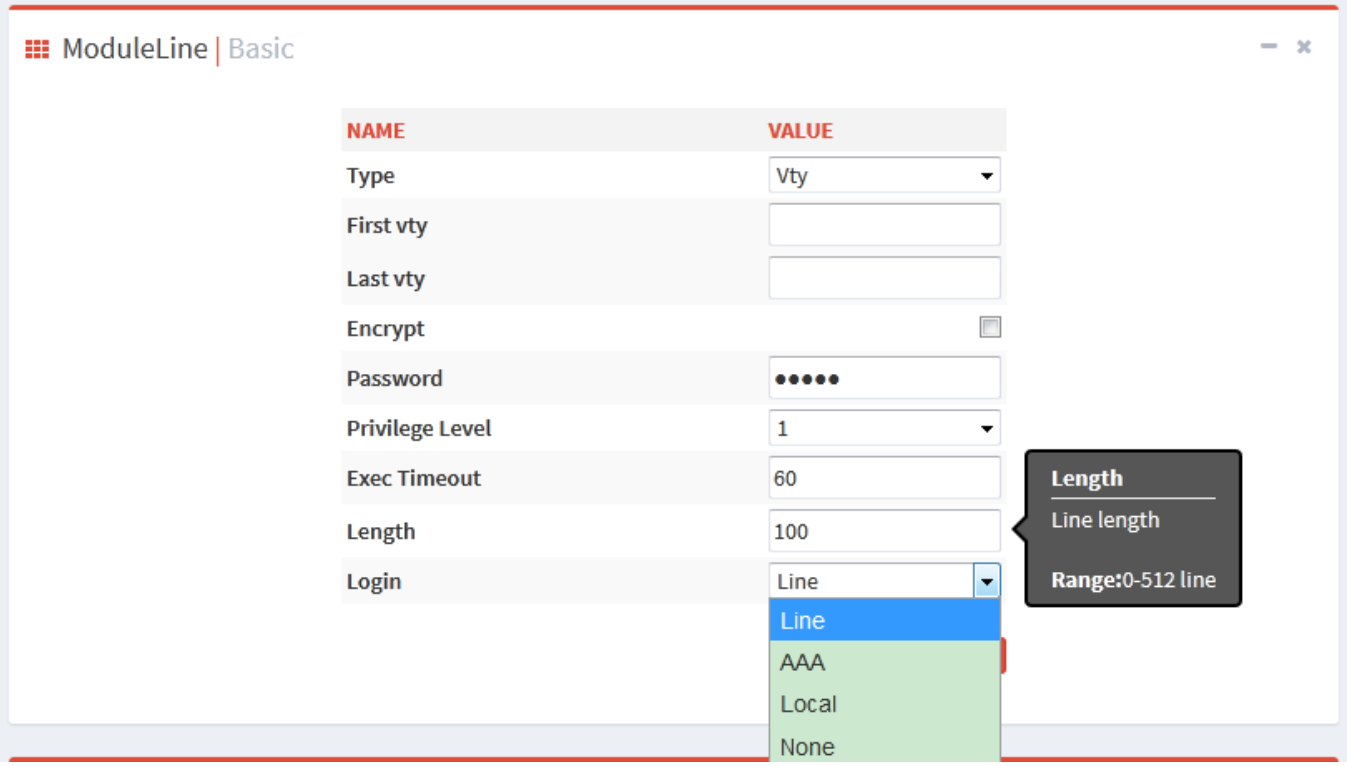


Рисунок 104 Страница настроек Line

Type

Варианты конфигурации: console/vty

Функция: Выбор режима удаленного входа в коммутатор

Console: Вход через консольный порт.

Vty соответствует общим протоколам входа в систему, включая telnet.

Vty Id

Варианты конфигурации: 0-9

Конфигурация по умолчанию: 0

Функция:

1. Тип Line – console, значение vty по умолчанию 0, настройка на консольный порт.

2. Тип Line – vty, необходимо настроить first-vty или last-vty.

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

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

Настройка только first-vty означает настройку только одной линии vty; настройка last-vty означает настройку всех линий от first-vty до last-vty.

Encrypt

Варианты конфигурации: Plaintext encryption/ ciphertext encryption

Конфигурация по умолчанию: Plaintext encryption

Функция: Пароль по умолчанию admin, снятие флажка Encrypt означает использование plaintext encryption; установка флажка Encrypt означает использование ciphertext encryption. Инструмент частного алгоритма шифрования предоставляется для генерации зашифрованного текста. Команда crypt 7.

Password

Варианты конфигурации: Plaintext password/ciphertext password

Длина пароля Plaintext password составляет 1-64 символа, длина пароля ciphertext password составляет 1-129 символов.

Конфигурация по умолчанию: plaintext password with admin

Privilege level

Варианты конфигурации: Диапазон 0-15

Конфигурация по умолчанию: 1

Функция: При настройке режима аутентификации по линии разрешение аутентификации консоли/telnet контролируется разрешением по линии.

Exec timeout

Варианты конфигурации: Диапазон: <0-86400>, ед. изм секунда

Конфигурация по умолчанию: 60

Функция: Настройка времени ожидания после входа в пользовательский терминал. При выборе значения 0 ожидания нет.

Length

Варианты конфигурации: <0-512>

Конфигурация по умолчанию: 100

Функция: Настройка максимального числа строк вывода на экран.

Login

Варианты конфигурации: line/aaa/local/none

Line: Используйте конфигурацию аутентификации с паролем в интерфейсе линии для входа в систему.

Aaa: Используйте конфигурацию аутентификации с пользователем и паролем в AAA для входа в систему.

Local: Используйте конфигурацию аутентификации с именем пользователя и паролем в локальных настройках управления пользователями для входа в систему.

None: Без аутентификации.

Конфигурация по умолчанию: line

Функция: Настройка режима аутентификации при входе в терминал.

7 Обслуживание коммутатора

Щелкните в дереве навигации [Switch Maintenance], выберите всплывающее окно для работы.

Следующие параметры позволяют устройству сохранять конфигурацию и восстанавливать заводскую конфигурацию по умолчанию.

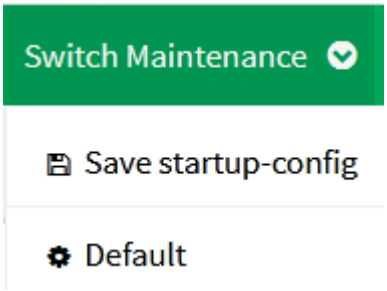


Рисунок 105 Сохранение startup-config и восстановление конфигурация по умолчанию

8 Узлы сети

Щелкните в дереве навигации [Network Nodes], перейдите на страницу информации об устройстве, как показано на рисунке ниже.

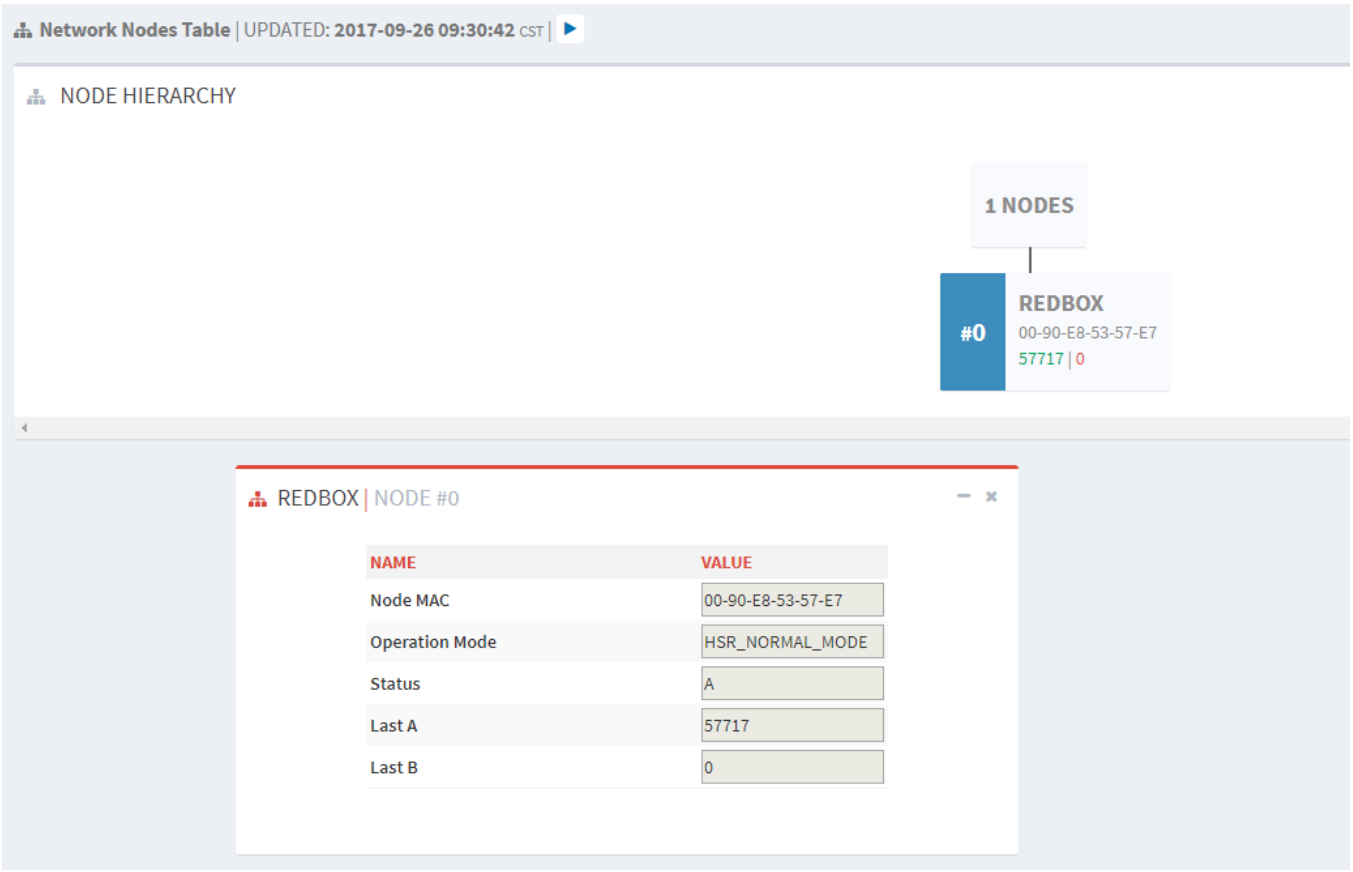


Рисунок 106 Узлы сети

Схема вверху показывает текущую сетевую ситуацию устройства, NODES — локальное устройство, REDBOX – удаленное устройство, подключение к локальному устройству осуществляется через порт A, MAC-адрес удаленного устройства и статистику полученных и переданных сообщений порта можно увидеть на схеме.

Более подробно сетевая ситуация показана в таблице REDBOX ниже.

Node MAC

Описание: MAC-адрес удаленного устройства.

Operation Mode

Описание: Режим работы устройства.

Status

Описание: интерфейс между удаленным устройством и локальным устройством, варианты A/B/A&B.

Last A

Описание: Статистика сообщений порта A

Last B

Описание: Статистика сообщений порта B

Приложение Список аббревиатур

Аббревиатура	Рашифровка
BC	Boundary Clock
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DST	Daylight Saving Time
E2ETC	End-to-End Transparent Clock
FTP	File Transfer Protocol
GPS	Global Positioning System
HTTP	Hyper Text Transfer Protocol
IED	Intelligent Electronic Device
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MIB	Management Information Base
NTP	Network Time Protocol
OC	Ordinary Clock
OID	Object Identifier
P2PTC	Peer-to-Peer Transparent Clock
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
RTC	Real Time Clock
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSL	Secure Sockets Layer

TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock

Контакты

Для получения технической поддержки пишите на наш адрес электронной почты: *support@kyland-rus.ru*

Офис продаж: *sales@kyland-rus.ru*

Для получения информации об оборудовании, документации, актуальной информации обращайтесь на сайт: *https://kyland-rus.ru/*