NetXpert NXI-3030RB

ПРОМЫШЛЕННЫЙ КОММУТАТОР С ФУНКЦИЕЙ REDBOX

Руководство по эксплуатации

Модели:

NetXpert NXI-3030RB-HV
NetXpert NXI-3030RB-DC
NetXpert NXI-3030RB-HV-HV
NetXpert NXI-3000-EM-HSR/PRP-2GE-0.5U
NetXpert NXI-3000-EM-HSR/PRP-2SFP-0.5U

Версия 1.4

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ 6
1. ОПИСАНИЕ УСТРОЙСТВА 9
1.1. Обзор 9
1.2. Функциональные возможности программного обеспечения 10
2. ДОСТУП К КОММУТАТОРУ 11
2.1. Типы режимов просмотра 11
2.2. Доступ к коммутатору через консольный порт 12
2.3. Доступ к коммутатору через Telnet 15
2.4. Доступ к коммутатору через WEB 16
3. ИНФОРМАЦИЯ О СИСТЕМЕ 17
3.1. Базовая информация о системе 17
3.2. Схема работы 17
4. БАЗОВАЯ КОНФИГУРАЦИЯ 19
4.1. Выбор режима конфигурации 19
4.2. Конфигурация пользователя 19
4.3. Конфигурация IP-адреса 20
4.4. Конфигурация DHCP 21
4.4.1. Концепция протокола DHCP 21
4.4.2. Конфигурация DHCP-клиента 22
4.4.3. Статическая конфигурация IP-адреса 22
4.5. Конфигурация системных настроек 23
4.5.1. Конфигурация часов 23
4.5.2. Состояние центрального процессора 24
4.5.3. Статус сети 24
4.5.4. Системный журнал 24
4.6. Выгрузка файлов 25
4.6.1. Выгрузка MIB-файлов 26
4.6.2. Выгрузка файла конфигурации 27
4.7. Обновление прошивки 27
4.7.1. Обновление прошивки по HTTP 28
4.7.2. Обновление прошивки по FTP 30
4.7.3. Обновление прошивки по SFTP 33
4.8. Загрузка файлов 36
4.9. Перезагрузка коммутатора 37
5. РЕЗЕРВИРОВАНИЕ 38
5.1. Принцип работы протокола параллельного резервирования PRP 38
5.2. Принцип работы протокола однородного резервирования HSR 39
5.3. Конфигурация резервирования 41
5.3.1. Пример стандартной конфигурации резервирования PRP 44
5.3.2. Пример стандартной конфигурации резервирования HSR 45

5.3.3. Пример стандартной конфигурации резервирования с Quadbox ... 46

6. PTP ... 47

6.1. Терминология и общее представление о PTP ... 47

6.1.1. Принцип работы синхронизации ... 48

6.2. Конфигурация PTP ... 49

6.2.1. Конфигурация прозрачных часов PTP TC ... 50
6.2.2. Конфигурация PTP для портов ... 51

7. СТАТИСТИКА ... 53
8. ПРОЧИЕ НАСТРОЙКИ ... 55

8.1. Аварийные сигналы ... 55

8.1.1. Конфигурация аварийных сигналов использования памяти / ЦП ... 55
8.1.2. Конфигурация аварийных сигналов порта ... 56

8.2. Конфигурация порта ... 57
8.3. Конфигурация таблицы MAC-адресов ... 58

8.3.1. Сведения о таблице MAC-адресов коммутатора ... 58
8.3.2. Просмотр таблицы MAC-адресов ... 59
8.3.3. Контроль таблицы MAC-адресов ... 59
8.3.4. Конфигурация статических MAC-адресов ... 60

8.4. SNTP ... 61

8.4.1. Конфигурация SNTP ... 61

8.5. NTP ... 63

8.5.1. Конфигурация NTP ... 64

8.6. IEC 61850 ... 65

8.6.1. Конфигурация IEC 61850 ... 65

8.7. SNMPv2c ... 66

8.7.1. Реализация SNMP ... 66
8.7.2. Информационная база управления (MIB) ... 67
8.7.3. Конфигурация SNMP ... 67
8.7.4. Стандартный пример конфигурации SNMP ... 70

8.8. SNMP v3 ... 71

8.8.1. Реализация SNMPv3 ... 71
8.8.2. Конфигурация SNMPv3 ... 72
8.8.3. Стандартный пример конфигурации SNMPv3 ... 78

8.9. Файловый сервер ... 79

8.9.1. FTP-клиент ... 80
8.9.2. SFTP-клиент ... 82

8.10. LLDP ... 84

8.10.1. Конфигурация LLDP ... 84

8.11. DDM 86
8.11.1. Конфигурация DDMI 86
8.12. Виртуальный тест кабеля 86
8.12.1. Конфигурация VCT 87
8.13. RADIUS 88
8.13.1. Общие сведения о RADIUS 88
8.13.2. Конфигурация RADIUS 89
8.13.3. Стандартный пример конфигурации RADIUS 91
8.14. TACACS+ 92
8.14.1. Общие сведения о TACACS+ 92
8.14.2. Конфигурация TACACS+ 93
8.14.3. Стандартный пример конфигурации TACACS+ 95
8.15. AAA 96
8.15.1. Конфигурация AAA 96
8.16. Конфигурация интерфейса командной строки 98
9. ОБСЛУЖИВАНИЕ КОММУТАТОРА 100
10. УЗЛЫ СЕТИ 101
11. ПРИЛОЖЕНИЕ: СОКРАЩЕНИЯ 102

ПРЕДИСЛОВИЕ

В данном руководстве пользователя описаны методы доступа и функциональные возможности программного обеспечения следующих устройств:

- промышленный Ethernet-коммутатор NetXpert NXI-3030RB с функцией RedBox (в дальнейшем NXI-3030RB);
- Модули NetXpert NXI-3000-EM-HSR/PRP-2GE-0.5U и NetXpert NXI-3000-EM-HSR/PRP-2SFP-0.5U (в дальнейшем NXI-3000-EM-HSR/PRP)

В руководстве подробно описаны методы конфигурации устройств через WEB-интерфейс.

Структура материалов

В данном руководстве пользователя содержатся следующие материалы:

Глава	*Содержание*
1. Описание устройства	Обзор Функциональные возможности программного обеспечения
2. Доступ к коммутатору	Типы режимов просмотра Доступ к коммутатору через консольный порт Доступ к коммутатору через Telnet Доступ к коммутатору через WEB
3. Информация о системе	Базовая информация о системе Схема работы
4. Базовая Конфигурация	Конфигурация DHCP Конфигурация системных параметров Выгрузка файлов Обновление прошивки Загрузка файлов Перезагрузка коммутатора
5. Резервирование	Принципы работы протокола параллельного резервирования PRP Принципы работы протокола однородного резервирования HSR Конфигурация резервирования
6. PTP	Терминология и общие представления о PTP Конфигурация PTP
7. Статистика	
8. Прочие настройки	Аварийные сигналы Конфигурация порта Конфигурация таблицы MAC-адресов SNTP NTP IEC 61850 SNMPv2c SNMPv3 Файловый сервер LLDP

	DDM Виртуальный тест кабеля RADIUS TACACS+ AAA Конфигурация интерфейса командной строки
9. Обслуживание коммутатора	
10. Узлы сети	
Приложение: словарь сокращений	

Список условных обозначений

Формат	*Описание*
< >	Текст между < > является названием кнопки. Например, необходимо нажать кнопку <Apply>.
[ ]	Текст между [ ] является названием пункта меню. Например, необходимо зайти в пункт меню [File].
{ }	Между { } указываются параметры, которые могут быть конфигурированы и отображены вместе. Например, {IP address, MAC address} обозначает, что IP-адрес и MAC-адрес можно задать одновременно.
→	Пункты многоуровневого меню разделяются знаком «→». Например, [Start] → [All Programs] → [Accessories] означает, что необходимо выбрать пункт меню [Start], затем выбрать подменю [All programs], а затем выбрать подменю [Accessories].
/	Требуется выбрать одну из нескольких опций, разделенных знаком «/». Например, «Addition/Deduction» означает, что необходимо выбрать Addition (добавление) или Deduction (удаление).
~	Обозначает диапазон. Например, «1~255» обозначает диапазон от 1 до 255.
Жирный	Пункты меню, параметры и ключевые слова написаны жирным шрифтом.
Курсив	Параметры, для которых можно подставить значения, приведены курсивом.

Документация по продукту

Документация по промышленному Ethernet-коммутатору NetXpert NXI-3030RB с функцией RedBox включает в себя:

Название документа	*Описание содержания*
Промышленный Ethernet-коммутатор NetXpert NXI-3030RB Инструкция по монтажу	Описывает структуру оборудования, технические характеристики оборудования, способы монтажа и демонтажа.
Промышленный Ethernet-коммутатор NetXpert NXI-3030RB Руководство по эксплуатации	Описывает функции программного обеспечения коммутатора, методы WEB-конфигурации и этапы настройки всех функций.

1. ОПИСАНИЕ УСТРОЙСТВА

1.1. Обзор

NetXpert NXI-3030RB (NXI-3030RB) – это серия промышленных коммутаторов с функцией RedBox с поддержкой протоколов PRP (Parallel Redundancy Protocol – протокол параллельного резервирования) и HSR (High-availability Seamless Redundancy – протокол высоконадежного бесшовного резервирования) в соответствии со стандартом МЭК 62439-3. Использование NXI-3030RB позволяет полностью исключить потерю пакетов при возникновении неисправности в сети, гарантируя высокую надежность на сетях критической инфраструктуры.

NXI-3030RB соответствует МЭК 61850-3 и обладает встроенным сервером MMS в соответствии с МЭК 61850-90-4, благодаря чему легко встраивается в системы SCADA электроэнергетики.

Аппаратная архитектура устройства построена на специальной ПЛИС, благодаря которой достигается минимальная задержка пересылки кадров с использованием PRP/HSR. NXI-3030RB так же на аппаратном уровне поддерживает протокол сверхточной синхронизации времени PTP по стандарту IEEE 1588v2 через резервируемые сети PRP/HSR. Благодаря этому устройства могут применяться на сетях, где работают протоколы реального времени.

Устройства NXI-3030RB специально разработаны для жестких условий эксплуатации с широким диапазоном рабочих температур, третьим уровнем электромагнитной совместимости, классом защиты IP40, прочным виброустойчивым креплением для монтажа на DIN-рейку. Они могут быть использованы в системах автоматизации производства, транспорта, нефтегазовой отрасли, электроэнергетике, автоматизации распределительных сетей и во многих других промышленных приложениях.

Устройство также представлено в форм-факторе модуля NXI-3000-EM-HSR/PRP. Такой модуль устанавливается в коммутаторы NXI-3040/3050-M-G, позволяя этим коммутаторам оперировать в резервируемых сетях PRP/HSR. Программные функции коммутатора NXI-3030RB и модуля NXI-3000-EM-HSR/PRP полностью совпадают.

1.2. Функциональные возможности программного обеспечения

Программное обеспечение коммутаторов NXI-3030RB обладает богатым функционалом, благодаря чему устройство способно удовлетворить различным требованиям заказчиков. Основной функционал представлен в Таблица 1.1.

Таблица 1.1. Функционал программного обеспечения NXI-3030RB.

HSR/PRP	Поддержка PTP, с нулевым временем сходимости. Поддержка HSR с нулевым временем сходимости. Поддержка двойного использования PRP и HSR (Quad Box).
IEEE1588v2	Поддержка PTPv2（IEEE1588-2008), режим Transparent Clock, точность до 1 мкс.
Настройки портов и VLAN	Настройка скорости порта (1000M/100M/10M/auto). Настройка режима дуплекса порта (full/half). Поддержка тегов 802.1Q (1…4093). Назначение VLAN ID на основе порта.
Работа с MAC-адресами	Автоматическое изучение MAC-адресов. Таблица MAC-адресов с учетом VLAN. Емкость таблицы MAC-адресов – 2K. Настройка периода устаревания MAC-адреса.
Синхронизация системных часов	Поддержка SNTP/NTP.
Сетевая безопасность	Поддержка безопасных протоколов SSH, SSL, SNMPv3.
LLDP	Поддержка LLDP: просмотр информации о соседях и статистике.
IEC61850 MMS-сервер	Поддерживается сервер MMS по стандарту МЭК 61850-90-4.
Управление и мониторинг	Поддержка DHCP-клиента. Поддержка FTP/SFTP-клиента, FTP-сервера. Поддержка встроенной диагностики Ping. Управление по консольному порту или по протоколу Telnet с помощью интерфейса командной строки. Поддержка графического WEB-интерфейса. Поддержка SNMP v1/v2c/v3 Мониторинг и отправка аварийных сигналов загрузки центрального процессора и памяти. Отправка аварийных сигналов при неисправности одного из источников питания. Отправка аварийных сигналов при пропадании линка на порте. Выделенный порт управления.

2. ДОСТУП К КОММУТАТОРУ

Доступ к коммутатору можно получить через:

- Консольный порт
- Telnet/SSH
- WEB-браузер
- SNMP

Доступ к модулю можно получить через:

- Telnet/SSH
- WEB-браузер
- SNMP

2.1. Типы режимов просмотра

В интерфейсе командной строки (CLI) устройства, доступном через консольный порт или Telnet/SSH, существует несколько режимов просмотра. Информация о режимах и способах переключения между ними представлена в Таблица 2.1.

Таблица 2.1. Типы режимов просмотра.

Режим просмотра	Тип режима просмотра	Функция режима просмотра	Переключение режима просмотра
SWITCH #	Привилегированный режим	Просмотр недавно использованных команд. Просмотр версии ПО. Просмотр ответной информации для операции ping. Загрузка/выгрузка файла конфигурации. Восстановление конфигурации по умолчанию. Перезагрузка коммутатора. Сохранение текущей конфигурации. Отображение текущей конфигурации. Обновление ПО.	Нужно ввести «configure» для перехода в режим конфигурации из привилегированного режима. Необходимо ввести «exit» для возврата в основной режим.
SWITCH (config) #	Режим конфигурации	Выполнение конфигурации функций коммутатора.	Нужно ввести «exit» для возврата в привилегированный режим.

При выполнении конфигурации коммутатора через CLI, можно использовать команду «?» для получения справки по командам. В справочной информации используются различные форматы описания параметров. Например, «1, 255» обозначает числовой диапазон; «xx:xx:xx:xx:xx:xx» обозначает MAC-адрес; «word31» обозначает текстовую строку длиной до 31 символа. Дополнительно можно использовать кнопки ↑ и ↓ для перехода между последними использованными командами.

2.2. Доступ к коммутатору через консольный порт

Получить доступ к коммутатору через консольный порт можно используя Hyper Terminal Windows или другое ПО, которое поддерживает подключение через последовательные порты. В следующем примере показано, как получить доступ к коммутатору через консольный порт с помощью Hyper Terminal.
Необходимо подключить 9-контактный последовательный порт ПК к консольному порту коммутатора с помощью кабеля DB9-RJ45.
Запустите Hyper Terminal на рабочем столе. Для этого нажмите [Start] → [Программы] → [Стандартные] → [Связь] → [Hyper Terminal], как показано на Рис. 2.1.

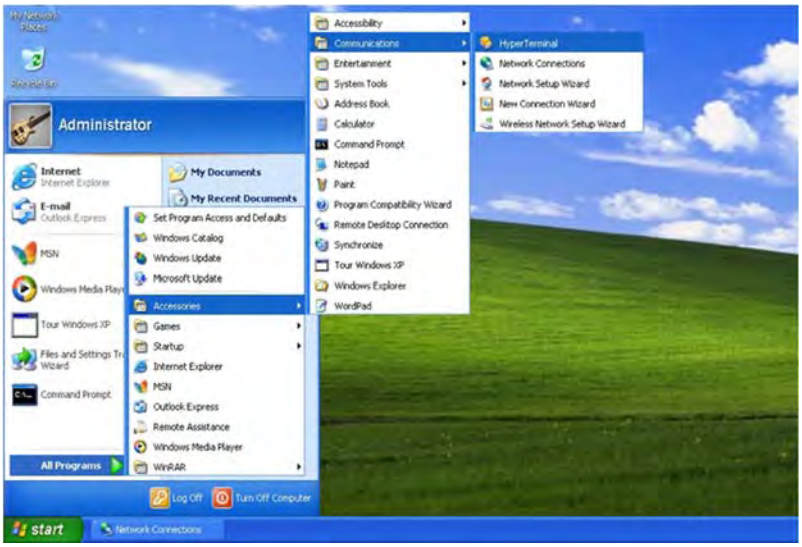

Рис. 2.1.Запуск Hyper Terminal.

Создайте новое подключение «Switch», как показано на Рис. 2.2.

Рис. 2.2. Создание нового подключения.

Подключите используемый порт связи, как показано на Рис. 2.3.

Рис. 2.3. Выбор порта связи.

Для подтверждения выбора используемого порта связи необходимо кликнуть правой кнопкой мыши [Компьютер] → [Свойства] → [Оборудование] → [Диспетчер устройств] → [Port].
Необходимо установить параметры порта Port Settings (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1 и Flow control: None), как показано на Рис. 2.4.

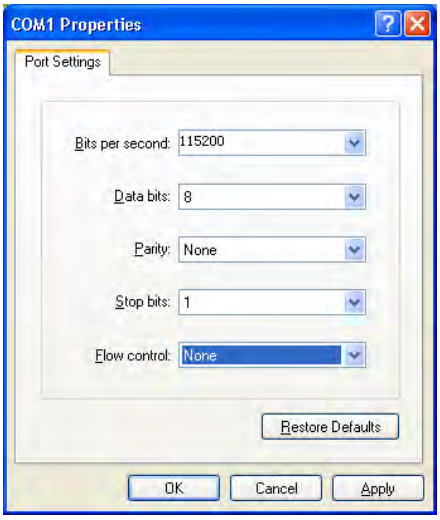

Рис. 2.4. Настройка параметров порта.

Нажмите кнопку <OK> для перехода к интерфейсу командной строки коммутатора, Рис. 2.5. Требуется ввести имя пользователя «admin» и пароль «123» для перехода к привилегированному режиму. Также можно ввести другие имена пользователей и пароли, если они настроены на коммутаторе.

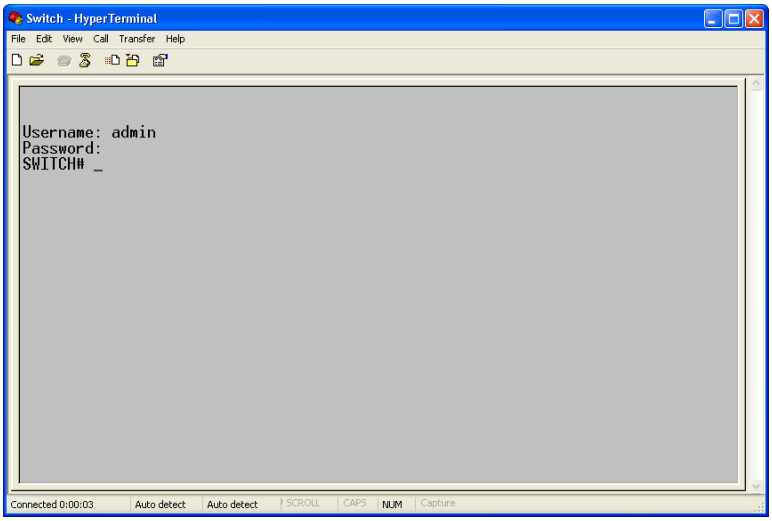

Рис. 2.5. Интерфейс командной строки.

2.3. Доступ к коммутатору через Telnet

Обязательным условием для доступа к коммутатору через Telnet является стабильная связь между ПК и коммутатором.
Введите «telnet IP address» в диалоговом окне Run операционной системы Windows, как показано на Рис. 2.6. IP-адресом по умолчанию для коммутатора является 192.168.0.2. IP-адресом по умолчанию для модуля NXI-3000-EM-HSR/PRP является 192.168.0.4. Более подробная информация о том, как задать IP-адрес коммутатора, содержится в главе 4.3. Конфигурация IP-адреса.

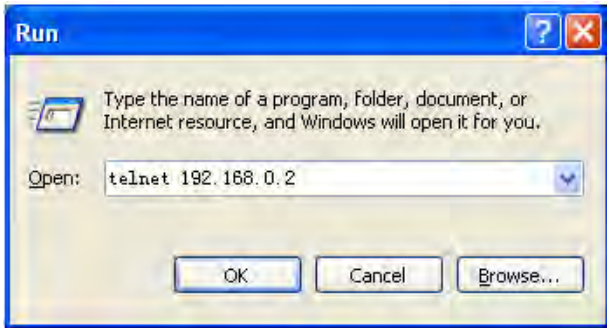

Рис. 2.6. Доступ через Telnet.

В интерфейсе Telnet необходимо ввести «admin» в поле User, и «123» в поле Password. Необходимо нажать <Enter> для подключения к коммутатору (Рис. 2.7). Также можно ввести другие имена пользователей и пароли, если они настроены на коммутаторе.

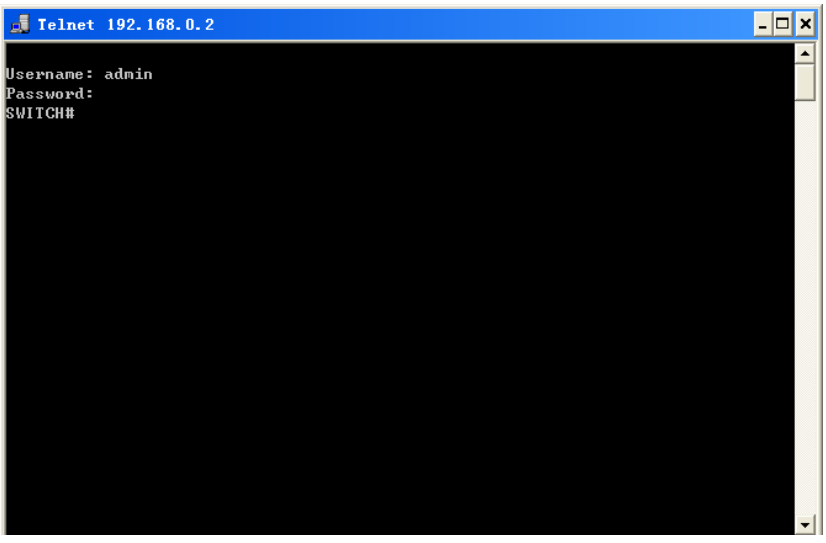

Рис. 2.7. Интерфейс Telnet.

2.4. Доступ к коммутатору через WEB

Обязательным условием для доступа к коммутатору через WEB является стабильная связь между ПК и коммутатором. Для достижения наилучших результатов отображения рекомендуется использовать браузер IE8.0 или более поздней версии.
Введите IP-адрес коммутатора в адресной строке браузера. Появится интерфейс входа в систему, показанный на Рис. 2.8. Необходимо ввести имя пользователя по умолчанию «admin», пароль «123». Далее нажать <OK>. Также можно ввести другие имена пользователей и пароли, если они настроены на коммутаторе. Более подробная информация о том, как задать IP-адрес коммутатора, содержится в главе 4.3 Конфигурация IP-адреса.

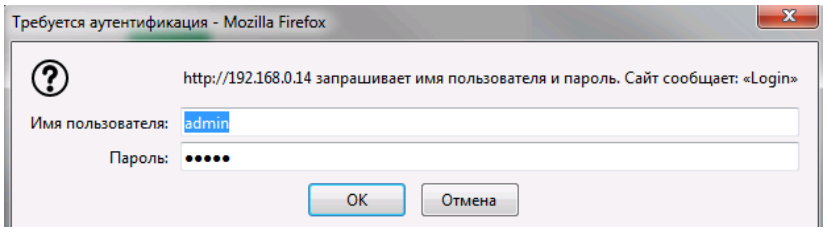

Рис. 2.8. Подключение через WEB.

После успешного входа в систему в левой части интерфейса будет отображен вэб-интерфейс устройства, как показано на Рис. 2.9. При нажатии на логотип в правом верхнем углу пользователь будет перенаправляться на стартовую страницу. В разделы управления устройством можно попасть, заходя в соответствующие раскрывающиеся меню в верхней части страницы и нажимая на шестеренку в правом верхнем углу.

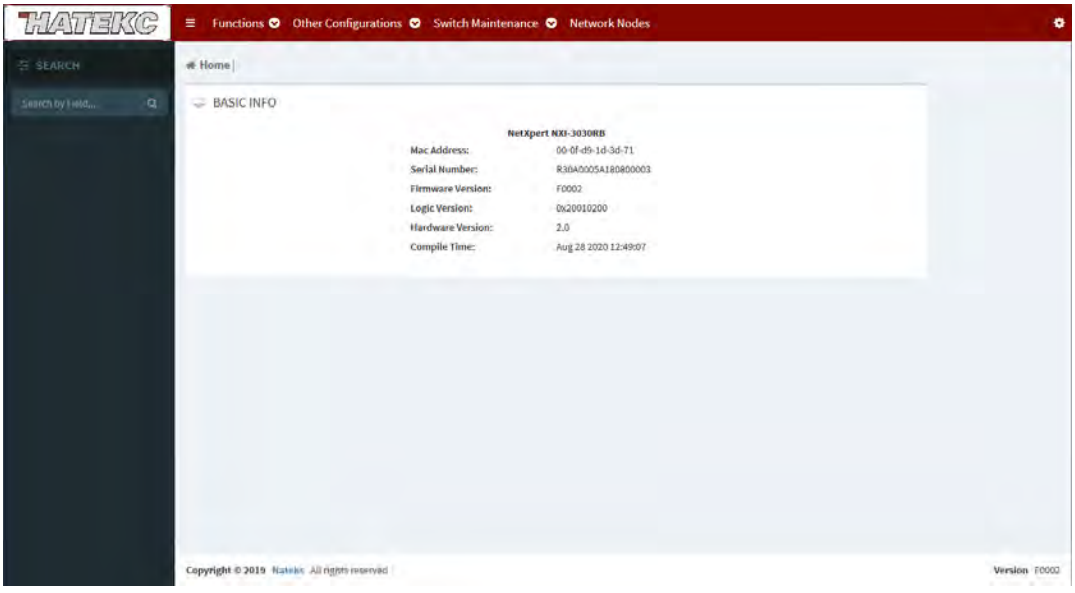

Рис. 2.9. WEB-интерфейс.

3. ИНФОРМАЦИЯ О СИСТЕМЕ

3.1. Базовая информация о системе

Для доступа к информации о системе нажмите логотип в левом верхнем углу экрана. Информация о системе коммутатора NXI-3030RB с функцией RedBox включает в себя MAC-адрес, серийный номер, информацию о версии ПО, системное время, как показано на Рис. 3.1.

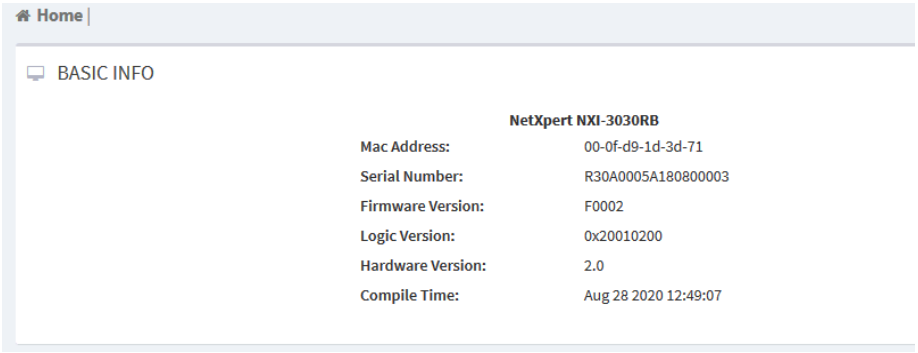

Рис. 3.1. Базовая информация о системе.

3.2. Схема работы

Принципиальная схема работы коммутатора NXI-3030RB приведена на Рис. 3.2.

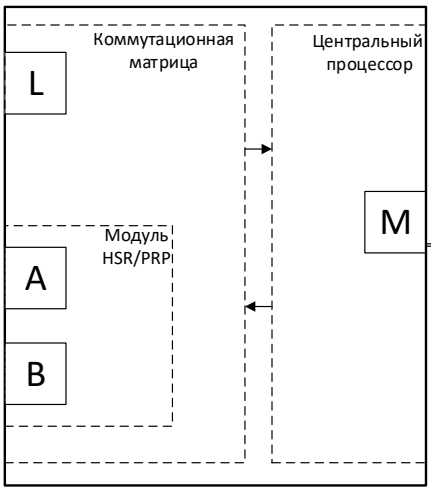

Рис. 3.2. Схема коммутатора NXI-3030RB.

Принципиальная схема работы модуля NXI-3000-EM-HSR/PRP аналогична, за исключением того, что на ней отсутствует порт M, а порт L фиксировано соединен с соответствующим слотом коммутатора, в который этот модуль установлен.

Порт L (port interlink) на NXI-3030RB – это комбо-интерфейс Ethernet для подключения конечного устройства с одним сетевым интерфейсом (SAN) к сети HSR/PRP.

Порты A и B – это комбо-интерфейсы Ethernet, которые работают в рамках модуля HSR/PRP, дублируя исходящие Ethernet-кадры и отбрасывая один из дублированных входящих кадров в соответствии с настроенным протоколом: HSR или PRP. Порты A и B по умолчанию являются единым логическим портом

в рамках матрицы коммутации устройства и образуют логический двухпортовый коммутатор вместе с портом L.

Порт M – это выделенный интерфейс управления устройством, вынесенный за пределы тракта передачи данных.

4. БАЗОВАЯ КОНФИГУРАЦИЯ

4.1. Выбор режима конфигурации

Нажмите на значок шестеренки в правом верхнем углу интерфейса, чтобы настроить основную информацию о пользователе, системе или обновить ПО либо конфигурацию устройства. Меню конфигурации устройства показано на Рис. 4.1.

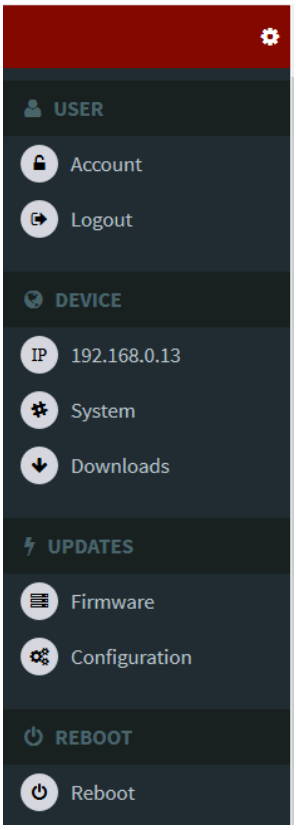

Рис. 4.1 Меню расширенной и базовой конфигурации.

4.2. Конфигурация пользователя

Кнопка <Account> в разделе User предназначена для изменения пароля пользователя. Кнопка <Logout> используется для выхода из текущего сеанса пользователя и открытия страницы входа в WEB-интерфейс.

4.3. Конфигурация IP-адреса

Для того, чтобы показать IP-адрес коммутатора через консольный порт войдите в интерфейс командной строки через консольный порт в режиме настройки привилегированного пользователя и введите команду «show interface ip brief». Результат вывода данной команды показан на Рис. 4.2.

```
RedBox# show int ip brief
Interface           Kname       IP-mode      Ipaddress          Mask              Gateway
-------------------------------------------------------------------------------------------
port_interlink      eth1        Static       192.168.100.13     255.255.255.0     0.0.0.0
mgmt                eth0        Static       192.168.0.13       255.255.255.0     --

RedBox#
```

Рис. 4.2 Просмотр IP-адреса коммутатора через консольный порт.

Для того, чтобы попасть на страницу конфигурации IP-адреса, нажмите на значок шестеренки в правом верхнем углу главной страницы WEB-интерфейса, выберите IP-адрес в разделе [DEVICE], откроется страница, показанная на Рис. 4.3. А на Рис. 4.4 показан скриншот настройки IP-адреса для модуля NXI-3000-EM-HSR/PRP

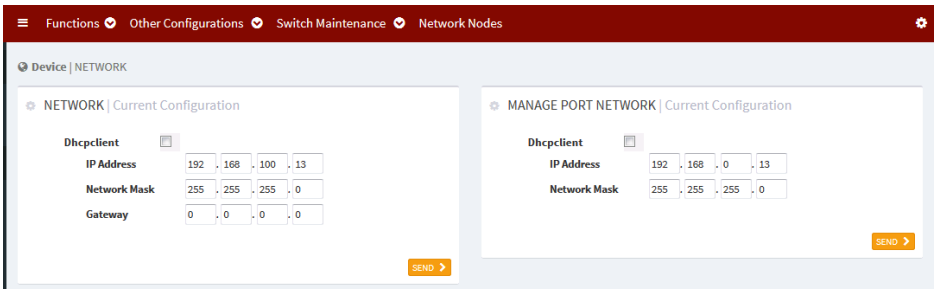

Рис. 4.3. Страница конфигурации IP-адреса для устройства NXI-3030RB.

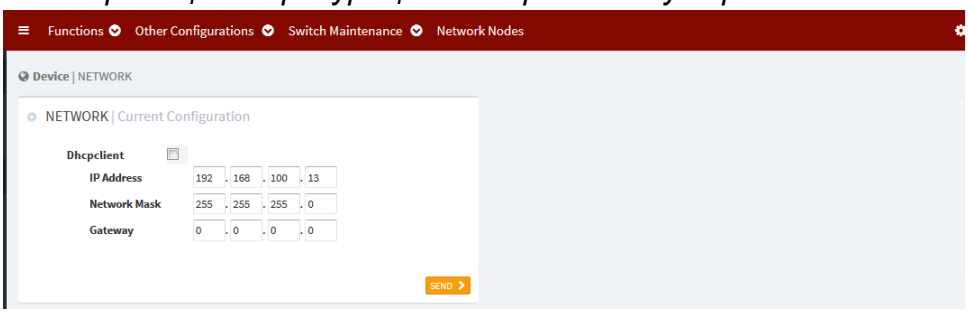

Рис. 4.4. Страница конфигурации IP-адреса модуля HSR/PRP.

При настройке нужно учитывать, что коммутатор NXI-3030RB имеет независимый порт управления, модуль HSR/PRP не имеет независимого порта управления. Описание параметров настройки меню NETWORK приведены в Таблица 4.1.

Таблица 4.1. Описание меню конфигурации IP-адреса.

Параметр	*Функция*	*Описание функции*
NETWORK	Настройка IP-адреса порта L	
MANAGE PORT NETWORK	Настройка IP-адреса порта управления	На странице конфигурации левая область предназначена для настройки IP-адреса порта L, правая область предназначена для настройки IP-адреса порта M. Есть поддержка динамической (по DHCP) и статической конфигурации IP-адреса.

4.4. Конфигурация DHCP

4.4.1. Концепция протокола DHCP

DHCP – это протокол типа «клиент-сервер». Клиент отправляет запрос конфигурации на сервер, а в ответ сервер отправляет клиенту параметры конфигурации, такие как IP-адрес, маска подсети, шлюз по умолчанию и т.п. Таким образом, можно динамически назначать IP-адреса подключаемым к сети хостам. Структура стандартного применения DHCP показана на Рис. 4.5. В процессе динамического получения IP-адресов сообщения передаются путем широковещательной рассылки, поэтому необходимо, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте сети. Если они находятся в разных сегментах, клиент может взаимодействовать с сервером только через DHCP-ретрансляцию для получения IP-адресов и других параметров конфигурации.

Рис. 4.5. Стандартное применение DHCP.

DHCP поддерживает два типа механизмов распределения IP-адресов. Статическое распределение: сетевой администратор статически привязывает фиксированные IP-адреса к нескольким конкретным клиентам и отправляет жестко привязанные IP-адреса этим клиентам по DHCP. Динамическое распределение: DHCP-сервер динамически распределяет IP-адреса для клиентов. Этот механизм распределения может предоставлять клиенту постоянный IP-адрес или IP-адрес с ограниченным сроком аренды. Когда срок аренды истекает, клиент должен повторно получить IP-адрес. Администратор сети может выбрать механизм распределения DHCP отдельно для каждого клиента.

4.4.2. Конфигурация DHCP-клиента

Коммутатор NXI-3030RB с функцией RedBox не поддерживает конфигурацию DHCP-сервера, возможна настройка только DHCP-клиента. Страница конфигурации IP-адреса порта L показана на Рис. 4.6.

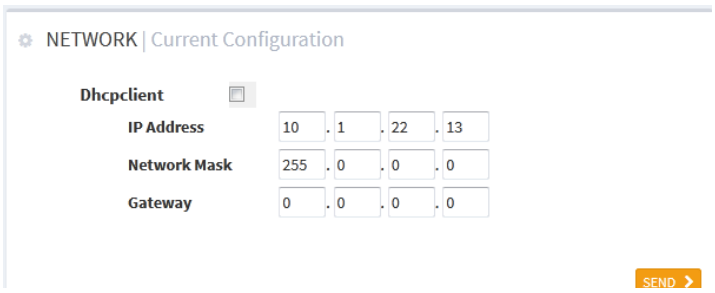

Рис. 4.6. Конфигурация IP-адреса порта L.

Для динамического получения IP-адреса и включения DHCP-клиента нужно отметить чекбокс Dhcpclient. После включения DHCP-клиент может подать заявку на получение IP-адреса на удаленный сервер. Когда включен Dhcpclient, другие элементы конфигурации на странице недоступны для выбора и настройки. Для проверки успешности получения IP-адреса по DHCP можно обновить страницу. Если получить IP-адрес не удается, предыдущий IP-адрес может использоваться как текущий, а маска подсети и шлюз так же восстанавливаются на последнее полученное значение конфигурации.

4.4.3. Статическая конфигурация IP-адреса

Страница конфигурации IP-адреса порта L показана на Рис. 4.6. Для настройки статической конфигурации IP-адреса нужно вручную заполнить поля IP Address и Network Mask. Коммутатор с функцией RedBox поддерживает только конфигурацию IP-адресов порта L и порта M, при этом каждый IP-интерфейс соответствует IP-адресу. Разные IP-интерфейсы должны быть настроены на IP-адреса из разных сегментов сети. Описание параметров настройки приведено в Таблица 4.2.

Таблица 4.2. Параметры настройки статической конфигурации IP-адреса.

Параметр	*Функция*	*Описание функции*
IP Address	Настройка статического IP-адреса	
Network Mask	Настройка маски подсети	Маска подсети может быть преобразована в двоичное число длиной 32 бита, состоящее из строки «1» и «0». «1» соответствует полю номера сети и полю номера подсети, а «0» соответствует полю номера хоста. Длина маски соответствует числу единиц в маске.
Gateway	Настройка адреса шлюза	Адрес шлюза должен находиться в том же сегменте сети, что и IP-адрес, в ином случае конфигурация не удастся.

4.5. Конфигурация системных настроек

Для перехода на страницу системных настроек нажмите на значок шестеренки в верхнем правом углу главной страницы WEB-интерфейса коммутатора с функцией RedBox, выберите пункт [SYSTEM], который расположен ниже пункта [DEVICE]. Страница системных настроек показана на Рис. 4.7. Эта страница в основном предназначена для просмотра системной информации, информации о состоянии центрального процессора, сети, просмотра журнала коммутатора и конфигурации системных часов.

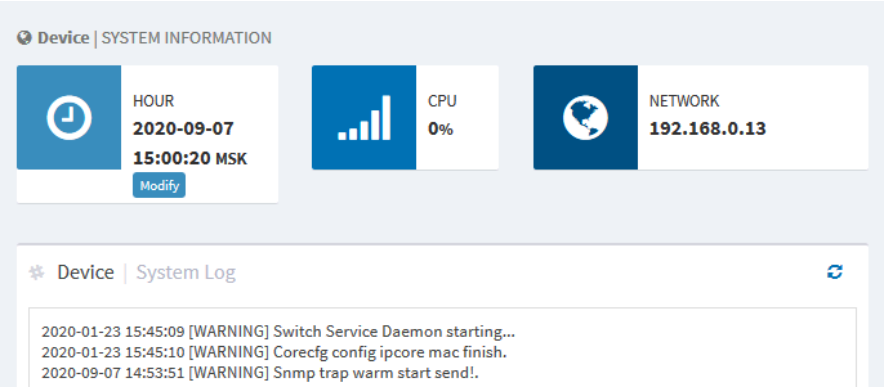

Рис. 4.7. Страница конфигурации системных настроек.

4.5.1. Конфигурация часов

Для настройки системных даты и времени нажмите на значок шестеренки в верхнем правом углу главной страницы WEB-интерфейса коммутатора, выберите пункт [SYSTEM] и зайдите на страницу конфигурации часов, показанную на Рис. 4.8. На данной странице можно посмотреть текущее время и настроить дату и время вручную.

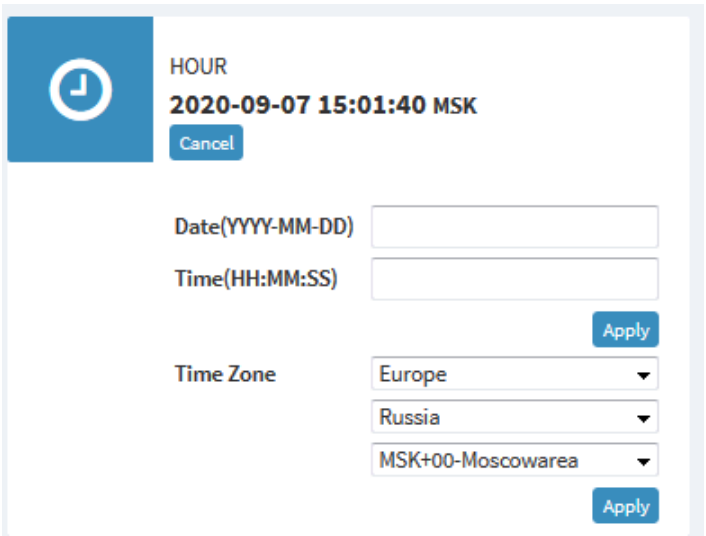

Рис. 4.8. Страница конфигурации даты и времени.

Описание параметров настройки приведено в Таблица 4.3.

Таблица 4.3. Параметры настройки даты и времени.

Параметр	*Функция*	*Значение*
Date (YYYY.MM.DD)	Настройка даты	YYYY (год) с диапазоном 1970…209, MM (месяц) с диапазоном 1…12, DD (день) с диапазоном 1…31
Time (HH:MM: SS)	Настройка времени	HH (час) с диапазоном 0…23, MM (минута), SS (секунда) с диапазоном 0…59
Time Zone	Настройка часового пояса	Нужно выбрать соответствующий континент, страну и город

4.5.2. Состояние центрального процессора

Для просмотра текущей средней загрузки центрального процессора (ЦП) нужно открыть пункт меню [CPU status], пример вывода информации показан на Рис. 4.9.

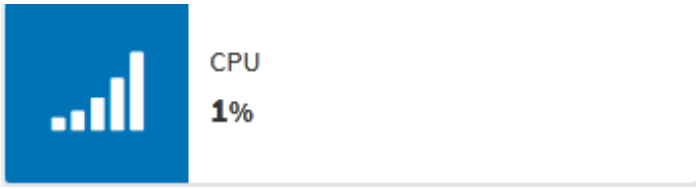

Рис. 4.9. Состояние загрузки ЦП.

4.5.3. Статус сети

Для просмотра состояния сети нужно зайти в пункт меню [NETWORK]. Пример страницы состояния сети показан на Рис. 4.10. На данной странице можно посмотреть IP-адрес WEB-интерфейса входа в систему, показывающий, что интерфейс используется.

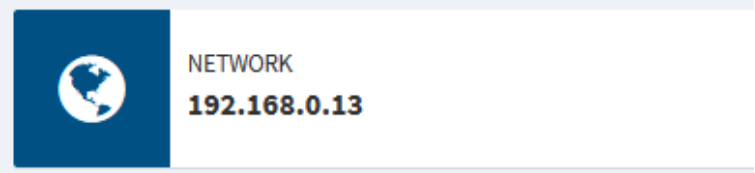

Рис. 4.10. Статус сети.

4.5.4. Системный журнал

Функция журнала коммутатора используется для записи таких событий, как изменения состояния, сбои, отладка, особые ситуации, действия пользователя и другой информацию о системе коммутатора. Записи системного журнала удобно использовать для обнаружения сбоя. Информация из журнала может быть в режиме реального времени загружена на сервер, поддерживающий протокол системного журнала Syslog.

Сообщения в журнале содержат различную информацию об авариях, широковещательных штормах, перезапусках, информацию о памяти, действиях пользователя. Пример вывода системного журнала коммутатора показан на Рис. 4.11.

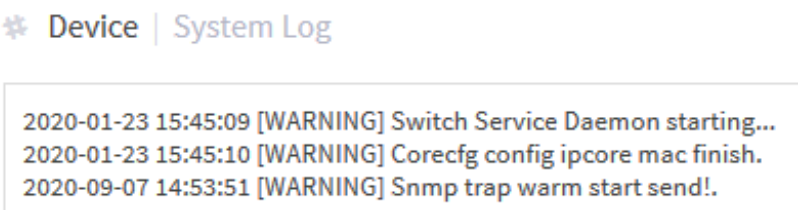

Рис. 4.11. Пример вывода системного журнала.

4.6. Выгрузка файлов

Для входа на страницу выгрузки файлов нажмите на значок шестеренки в верхнем правом углу главной страницы WEB-интерфейса коммутатора, выберите пункт [Downloads], расположенный под пунктом меню [DEVICE]. Можно выгрузить файл MIB (Management Information Base – информационная база управления SNMP) и файл конфигурации запуска коммутатора (startup-config), содержащий сохраненную конфигурацию коммутатора. Интерфейс меню выгрузки файлов показан на Рис. 4.12.

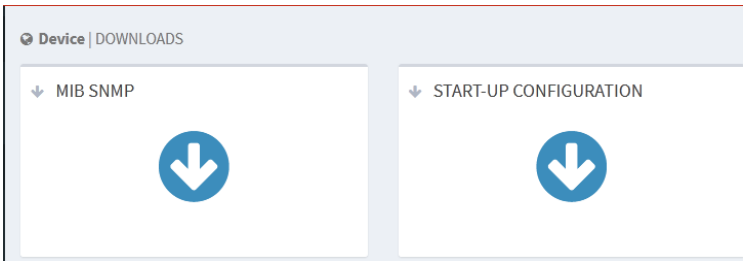

Рис. 4.12. Выгрузка файлов.

4.6.1. Выгрузка MIB-файлов

Для выгрузки MIB-файла нажмите на кнопку в поле [MIB SNMP] (Рис. 4.13), в появившемся всплывающем окне (Рис. 4.14), нажмите кнопку <OK>, чтобы сохранить файл SWITCH-DESING-MIB.mib по указанному пути сохранения.

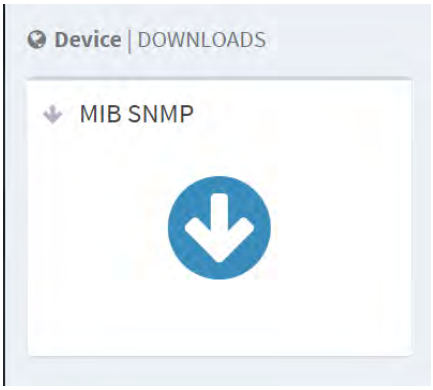

Рис. 4.13. Поле выгрузки MIB-файла.

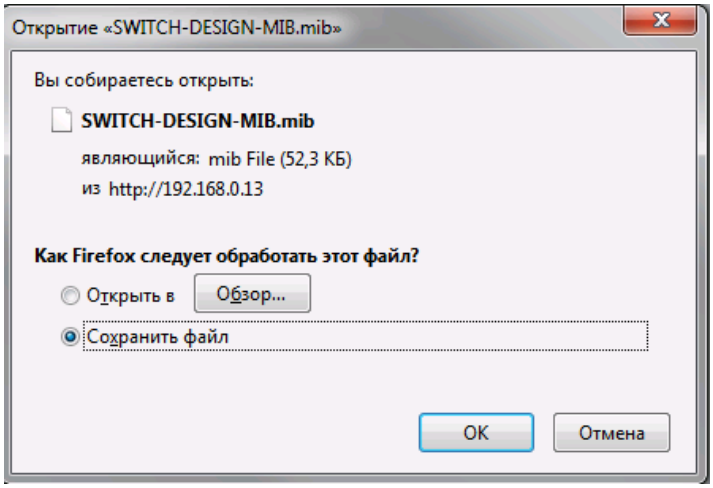

Рис. 4.14. Всплывающее окно выгрузки MIB-файла.

4.6.2. Выгрузка файла конфигурации

Для выгрузки файла конфигурации нажмите на кнопку в поле [START-UP CONFIGURATION] (Рис. 4.15), затем в появившемся всплывающем окне (Рис. 4.16) нажмите кнопку <OK>, чтобы сохранить файл startup_config.conf по указанному пути сохранения.

Рис. 4.15. Поле загрузки файла конфигурации.

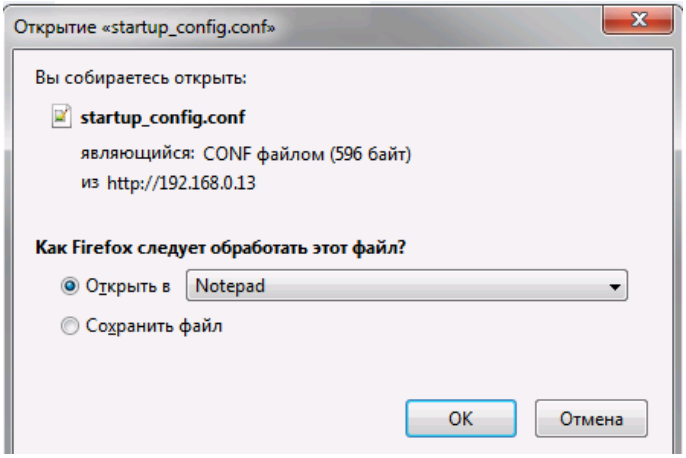

Рис. 4.16. Всплывающее окно загрузки файла конфигурации.

4.7. Обновление прошивки

Для повышения производительности коммутатора NXI-3030RB необходимо своевременно выполнять обновление прошивки. Коммутатор поддерживает обновление прошивки с локального компьютера по HTTP, а также обновление прошивки с FTP/SFTP-сервера.

4.7.1. Обновление прошивки по HTTP

Для входа на страницу обновления прошивки нажмите на значок шестеренки на главной странице WEB-интерфейса коммутатора и выберите пункт меню [Firmware]. Страница обновления прошивки показана на Рис. 4.17.

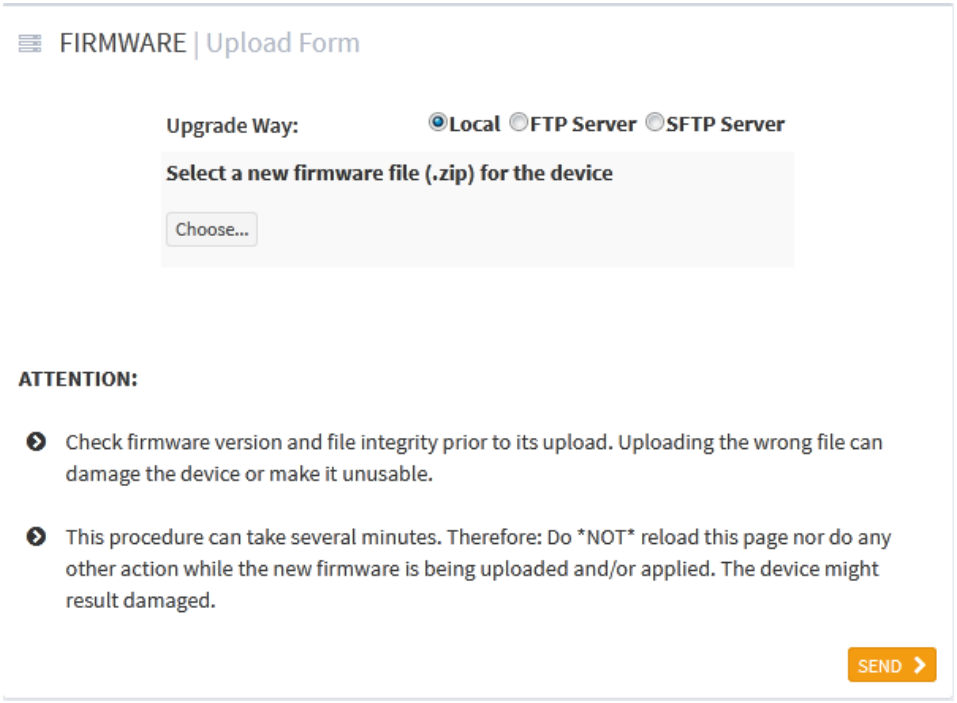

Рис. 4.17. Страница обновления прошивки.

В параметре Upgrade Way выберите значение Local, нажмите кнопку <Choose> для выбора файла прошивки, затем нажмите кнопку <Send> для выполнения обновления прошивки, как показано на Рис. 4.18.

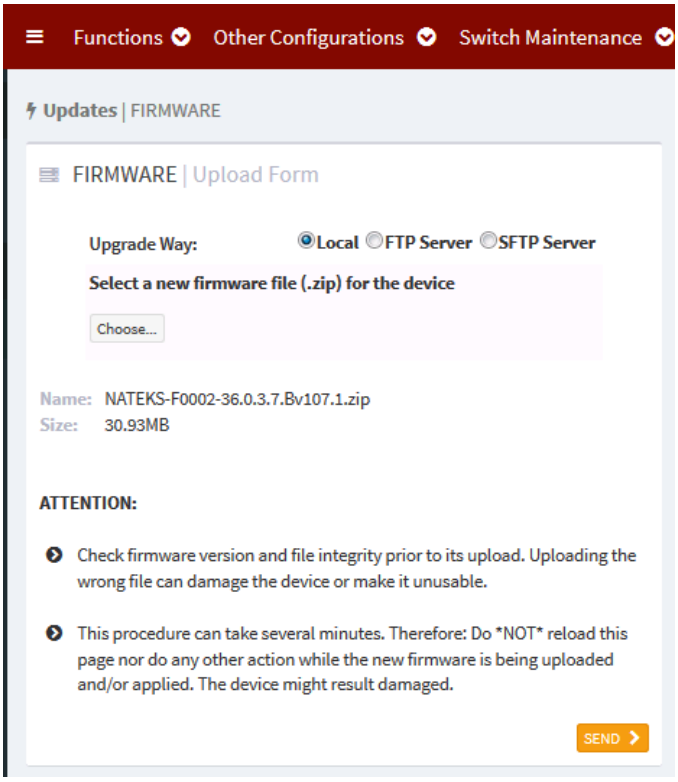

Рис. 4.18. Локальное обновление прошивки.

После нажатия на кнопку <SEND> запустится процесс обновления прошивки коммутатора, и появится страница ожидания, показанная на Рис. 4.19.

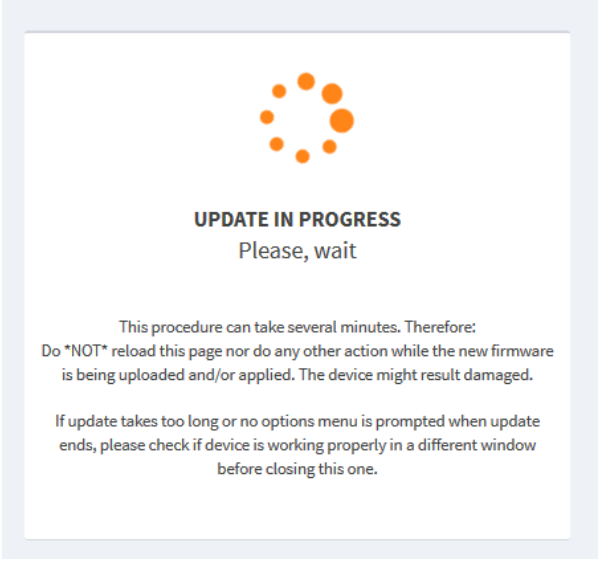

Рис. 4.19. Страница ожидания в процессе перепрошивки коммутатора.

Внимание! *До завершения обновления прошивки не выполняйте никаких других операций и не отключайте питание коммутатора, это может привести к сбою обновления и неполадкам при запуске коммутатора.*

Когда обновление успешно завершится, появится страница, показанная на Рис. 4.20.

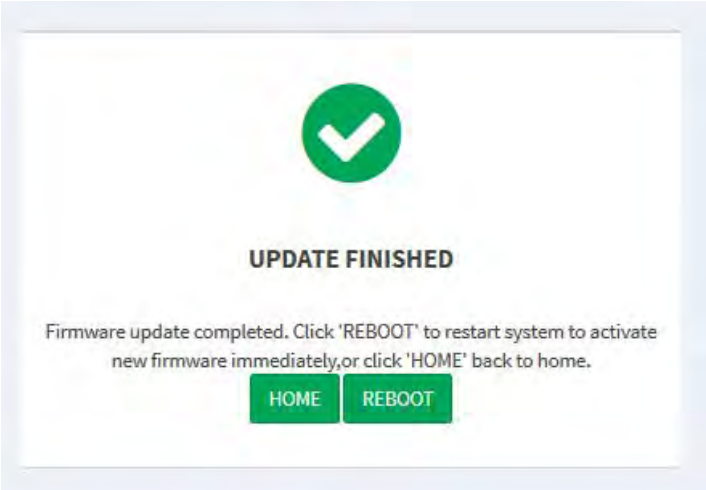

Рис. 4.20. Обновление успешно завершено.

После завершения обновления прошивки нужно выполнить перезагрузку коммутатора. Для этого нажмите на значок шестеренки в правом верхнем углу и выберите пункт меню [Reboot].

4.7.2. Обновление прошивки по FTP

Перед выполнением обновления прошивки по FTP нужно установить FTP-сервер. В качестве примера конфигурации FTP-сервера и процесса загрузки прошивки будет использоваться программное обеспечение WFTPD.

Выберите меню [Security] → [Users/Rights], откроется диалоговое окно «Users/Rights Security Dialog». Нажмите кнопку <New User>, чтобы создать нового пользователя FTP. Задайте имя пользователя (User Name) и пароль (Password), например, имя пользователя «admin» и пароль «123», нажмите кнопку <OK>. Процесс создания нового пользователя FTP показан на Рис. 4.21.

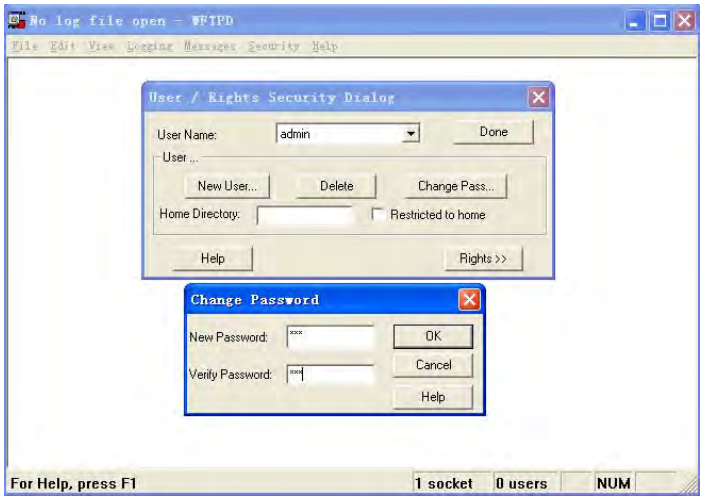

Рис. 4.21. Создание нового пользователя FTP.

Введите путь хранения файла программного обеспечения в поле Home Directory, как показано на Рис. 4.22, и нажмите кнопку <Done>.

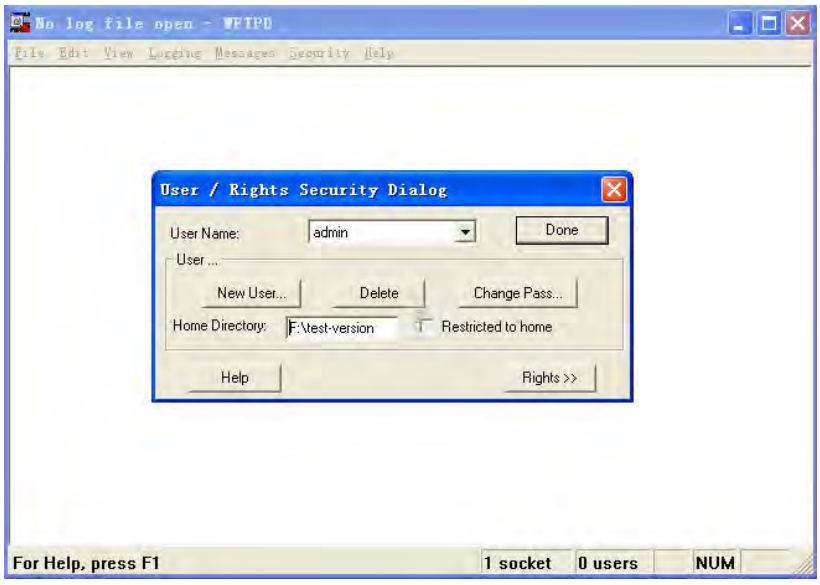

Рис. 4.22. Выбор пути хранения файла прошивки.

На главной странице WEB-интерфейса коммутатора нажмите на значок шестеренки в правом верхнем углу и выберите пункт меню [Firmware] для входа на страницу обновления прошивки коммутатора. Выберите в параметре Upgrade Way значение FTP server, в поле Server IP введите IP-адрес FTP-сервера, в поле Server File Name – имя файла прошивки на сервере, в полях User Name и Password – имя пользователя и пароль и нажмите кнопку <SEND>, как показано на Рис. 4.23.

Имя файла обновления по умолчанию – firmware.zip, имя файла может быть изменено, но расширение должно быть zip, иначе это приведет к сбою обновления.

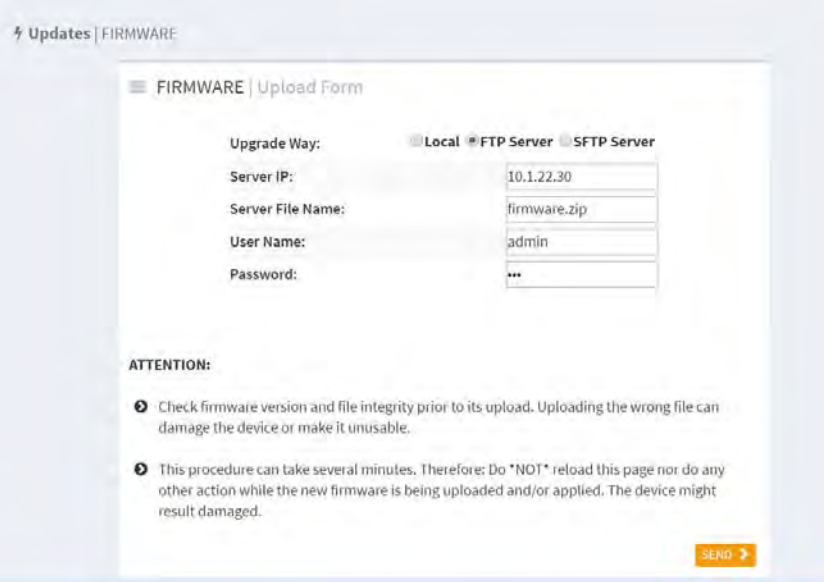

Рис. 4.23. Обновление прошивки с использованием FTP-сервера.

Убедитесь, что между FTP-сервером и коммутатором установлена нормальная связь. Для этого зайдите в программном обеспечении WFTPD в пункт меню [Logging] → [Log Options] и выберите Enable Logging. После этого будет показан журнал событий, пример записей журнала показан на Рис. 4.24.

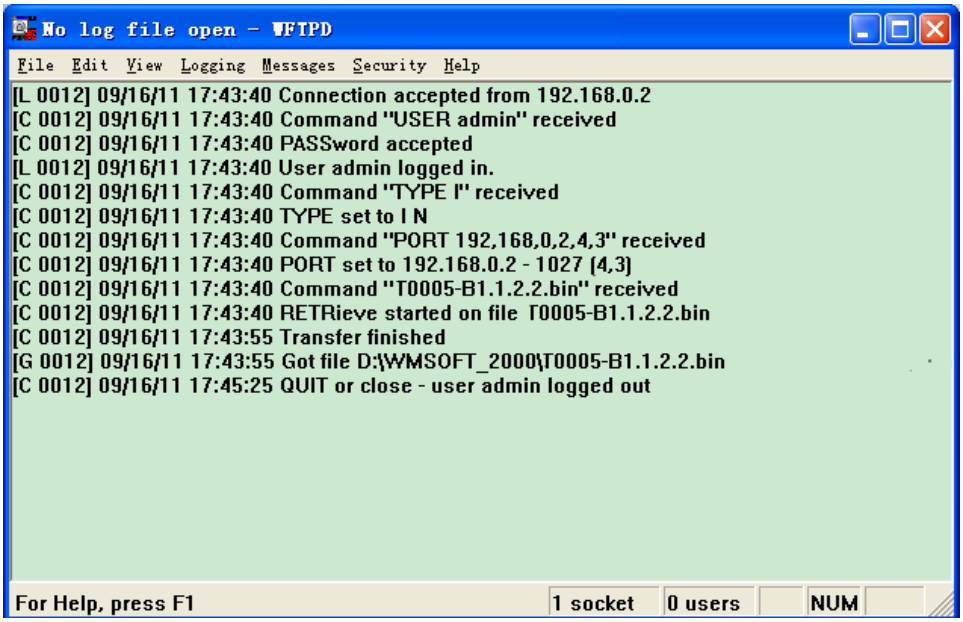

Рис. 4.24. Журнал событий при нормальной связи между FTP-сервером и коммутатором.

Во время ожидания выполнения обновления прошивки коммутатора будет выведено сообщение, показанное на Рис. 4.25. Во время выполнения обновления прошивки FTP-сервер должен оставаться в работающем состоянии.

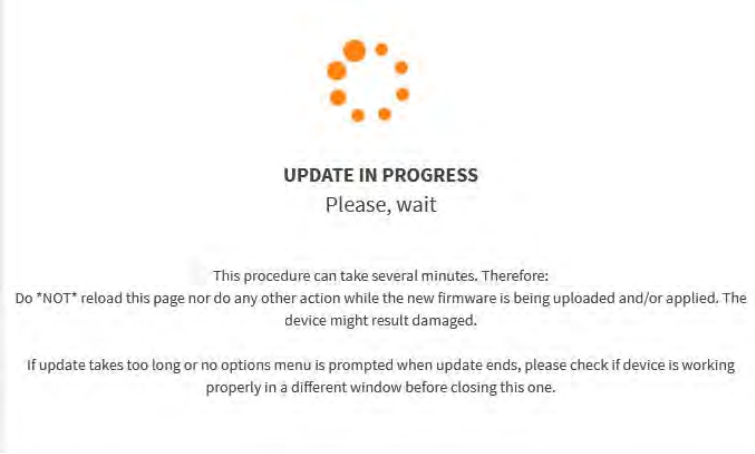

Рис. 4.25. Выполняется обновление программного обеспечения по FTP.

После успешного завершения обновления прошивки будет выведено сообщение, показанное на Рис. 4.26. Далее следует перезагрузить коммутатор, чтобы активировать новую версию, для этого нужно нажать кнопку <Reboot>.

В случае сбоя обновления не следует перезагружать устройство. Перезагрузка может привести к потере файла программного обеспечения и неполадкам при запуске коммутатора.

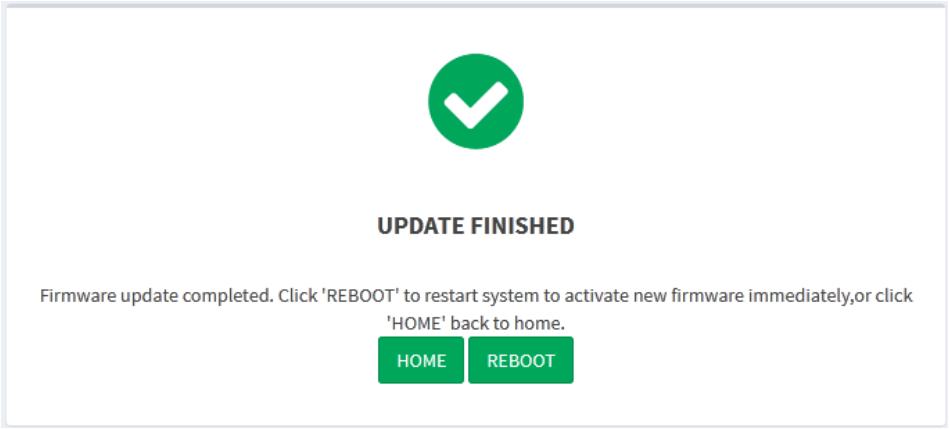

Рис. 4.26. Обновление программного обеспечения по FTP завершено.

4.7.3. Обновление прошивки по SFTP

Протокол безопасной передачи файлов (SFTP) представляет собой протокол передачи данных на основе SSH. Он обеспечивает зашифрованную передачу файлов для обеспечения безопасности.

В качестве примера конфигурации SFTP-сервера и процесса загрузки прошивки будет использоваться программное обеспечение MSFTP.

Добавьте пользователя SFTP, как показано на Рис. 4.27. Далее введите имя пользователя (User) и пароль (Password), например, «admin» и «123»; установите номер порта «22»; введите путь для файла прошивки в поле Root path.

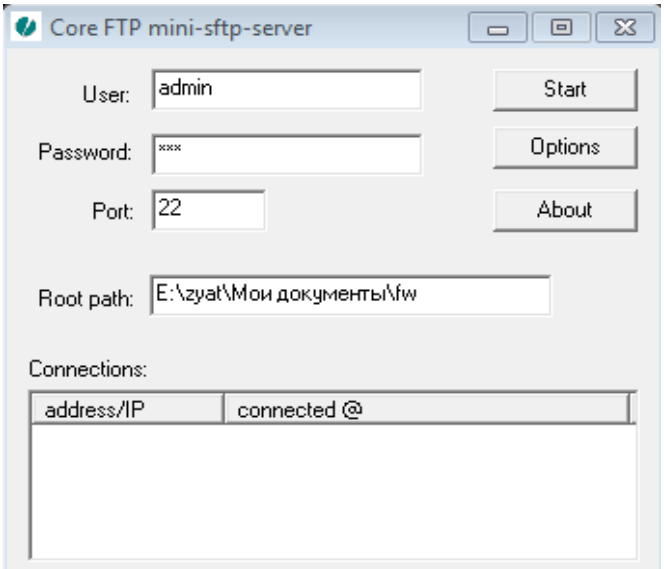

Рис. 4.27. Добавление пользователя SFTP.

На главной странице WEB-интерфейса коммутатора нажмите на значок шестеренки в правом верхнем углу и выберите пункт меню [Firmware] для входа на страницу обновления прошивки коммутатора. Выберите в параметре Upgrade Way значение SFTP server, в поле Server IP введите IP-адрес SFTP-сервера, в поле Server File Name – имя файла прошивки на сервере, в полях User Name и Password – имя пользователя и пароль и нажмите кнопку <SEND>, как показано на Рис. 4.28.

Имя файла обновления по умолчанию – firmware.zip, имя файла может быть изменено, но расширение должно быть zip, иначе это приведет к сбою обновления.

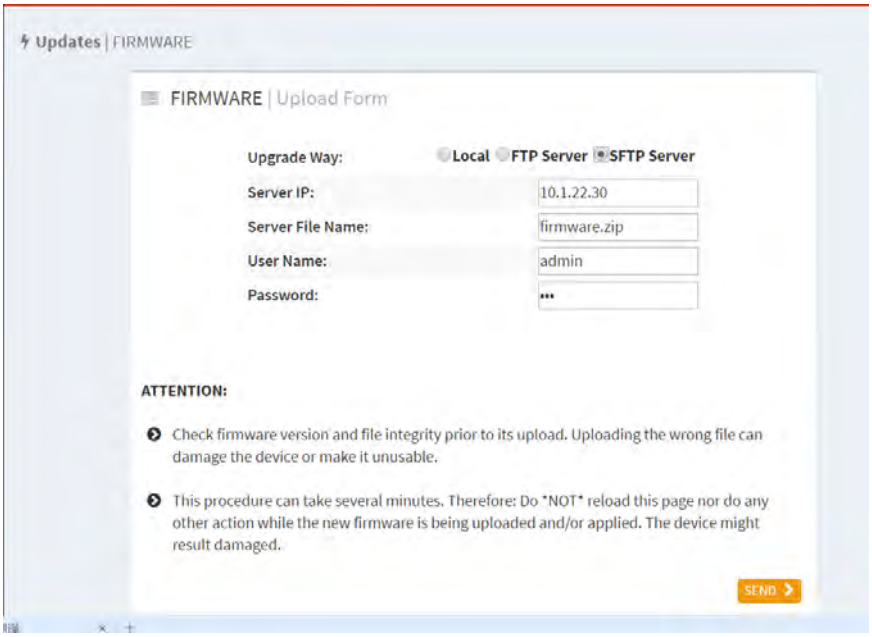

Рис. 4.28. Обновление прошивки с использованием SFTP-сервера.

Во время ожидания выполнения обновления прошивки коммутатора будет выведено сообщение, показанное на Рис. 4.29. Во время выполнения обновления прошивки SFTP-сервер должен оставаться в работающем состоянии.

Рис. 4.29. Выполняется обновление программного обеспечения по SFTP.

После успешного завершения обновления прошивки будет выведено сообщение, показанное на Рис. 4.30. Далее следует перезагрузить коммутатор, чтобы активировать новую версию, для этого нужно нажать кнопку <Reboot>.

В случае сбоя обновления не следует перезагружать устройство. Перезагрузка может привести к потере файла программного обеспечения и неполадкам при запуске коммутатора.

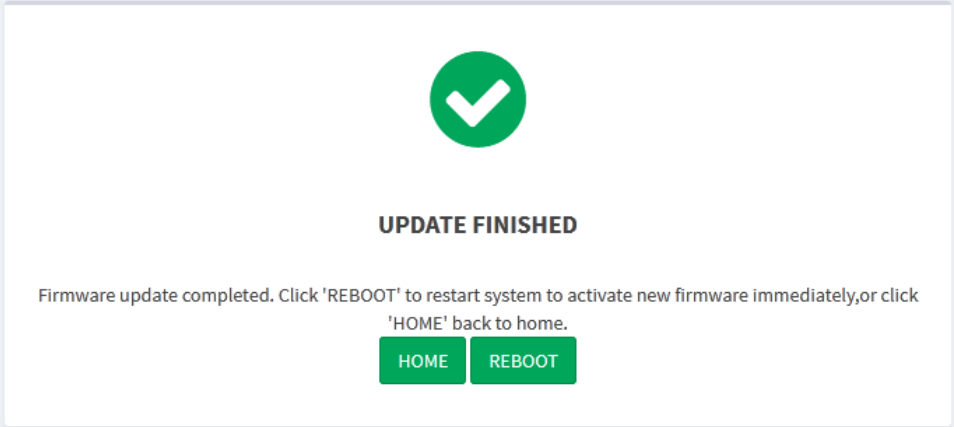

Рис. 4.30. Обновление программного обеспечения по SFTP завершено.

4.8. Загрузка файлов

На главной странице WEB-интерфейса коммутатора нажмите на значок шестеренки в правом верхнем углу и выберите пункт меню [Configuration] в меню [UPDATES] для того, чтобы загрузить файл конфигурации с локального сервера на коммутатор для использования в качестве файла запуска коммутатора. Процесс загрузки файла показан на Рис. 4.31.

Загруженный файл конфигурации должен являться текстовым файлом с расширением conf.

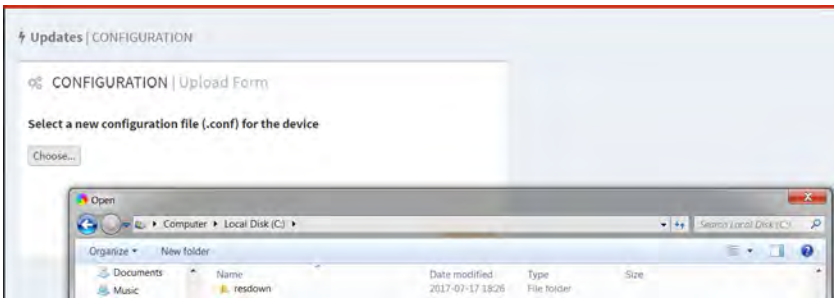

Рис. 4.31. Загрузка файла конфигурации.

4.9. Перезагрузка коммутатора

Когда необходимо выполнить перезагрузку коммутатора, нажмите на значок шестеренки в правом верхнем углу на главной странице WEB-интерфейса и выберите пункт [Reboot]. Во время перезагрузки отобразится сообщение, показанное на Рис. 4.32.

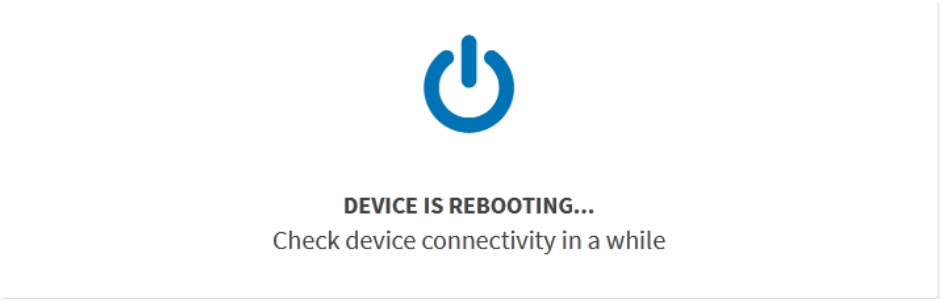

Рис. 4.32. Выполняется перезагрузка коммутатора.

5. РЕЗЕРВИРОВАНИЕ

5.1. Принцип работы протокола параллельного резервирования PRP

PRP (Parallel Redundancy Protocol) – протокол параллельного резервирования, описан в международном стандарте IEC 62439-3. PRP разработан для обеспечения в сетях Ethernet бесшовного резервирования с нулевым временем восстановления после сбоев. Для предотвращения сбоев передачи данных в сети при использовании PRP строятся две независимые сети Ethernet (LAN). Каждый пакет данных дублируется и передается по обеим сетям одновременно. Если до получателя доходят оба пакета, то отбрасывается пакет, который пришел позже. Таким образом обеспечивается бесперебойная передача данных даже в случае полного отказа одной из сетей.

Принципиальная схема работы PRP в сети передачи данных представлена на Рис. 5.1. SAN (Single Attached Node) — узел, который подключается только к одной сети (LAN A или LAN B). DANP (Doubly Attached Node implementing PRP) — узел, который подключается к обеим сетям и может посылать и принимать дублированные фреймы. NXI-3030RB – коммутатор с функцией резервирования, который соединяет PRP-сети с устройствами SAN.

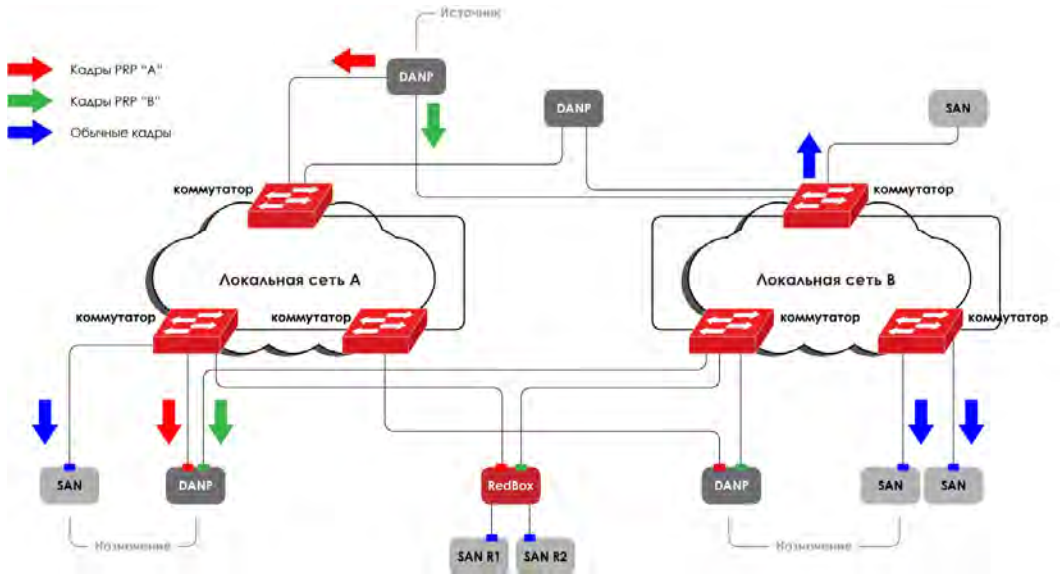

Рис. 5.1. Стандартная схема сети с использованием PRP.

На схеме, представленной на Рис. 5.1, каждый узел DAN подключается к двум параллельным независимым сетям LAN A и LAN B одновременно, кадры копируются, и 2 копии кадров отправляются отдельно через два порта коммутатора с функцией RedBox, а затем пересылаются на узлы назначения DAN по LAN A и LAN B соответственно. Для улучшения отказоустойчивости системы каждая независимая сеть может иметь различную структуру, например, LAN A имеет кольцевую структуру сети, а LAN B – древовидную. Узел SAN, который не поддерживает PRP (например, узел SAN A1), может быть напрямую подключен к LAN или подключен к специальному коммутатору с функцией RedBox.

Принцип работы PRP-порта показан на Рис. 5.2. Два работающих параллельно порта (порт A и порт B) одновременно подключены к объекту резервирования канала LRE (Link Redundancy Entity). Когда LRE принимает кадры с верхнего уровня, данные дублируются и отправляются одновременно через оба порта передачи T (Transmit ports). При этом в конец кадра добавляется трейлер, называемый стеком реального времени (Real-time Stack), в котором записывается информация о последовательном номере кадра.

Далее LRE приемника отправляет на верхний уровень первый полученный от принимающих портов Rx (Receiving ports) кадр, а пришедший позже дубль кадра отбрасывается. Дублированный кадры определяются на основании MAC-адреса источника и номера последовательности в RTS. Данный механизм является прозрачным для протоколов выше канального уровня, поэтому PRP совместим с протоколами канального уровня, такими как RSTP, VLAN и др. Кроме того, LRE регулярно отправляет сообщение мониторинга сети для обнаружения разрыва сети и других сбоев.

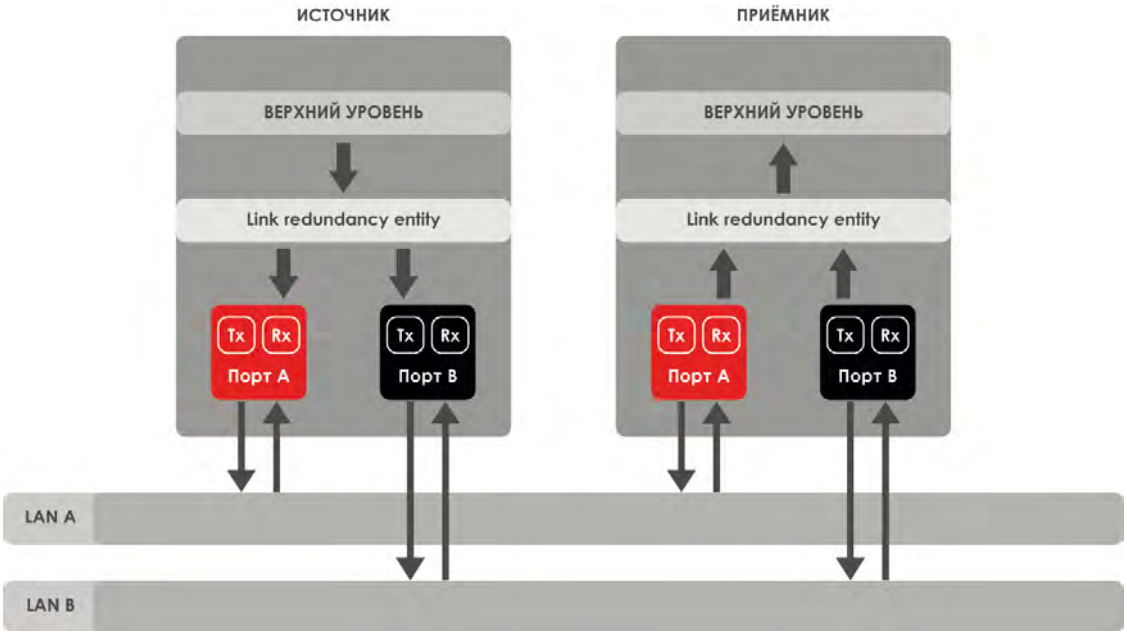

Рис. 5.2. Схема работы PRP-порта.

5.2. Принцип работы протокола однородного резервирования HSR

HSR (High-availability Seamless Redunduncy) – протокол параллельного высоконадежного однородного резервирования. В отличие от PRP, при использовании протокола HSR для резервирования используется кольцевая схема сети, все HSR-устройства имеют два Ethernet-интерфейса.

Принципиальная схема сети с использованием протокола HSR показана на Рис. 5.3. DANH (Doubly Attached Node implementing HSR) — узел, который посылает и принимает дублированные кадры внутри HSR-кольца. NXI-3030RB, позволяет подключить к HSR-сети устройство, имеющее один Ethernet-интерфейс. По сети передаются кадры: кадр A, кадр B и кадр C.

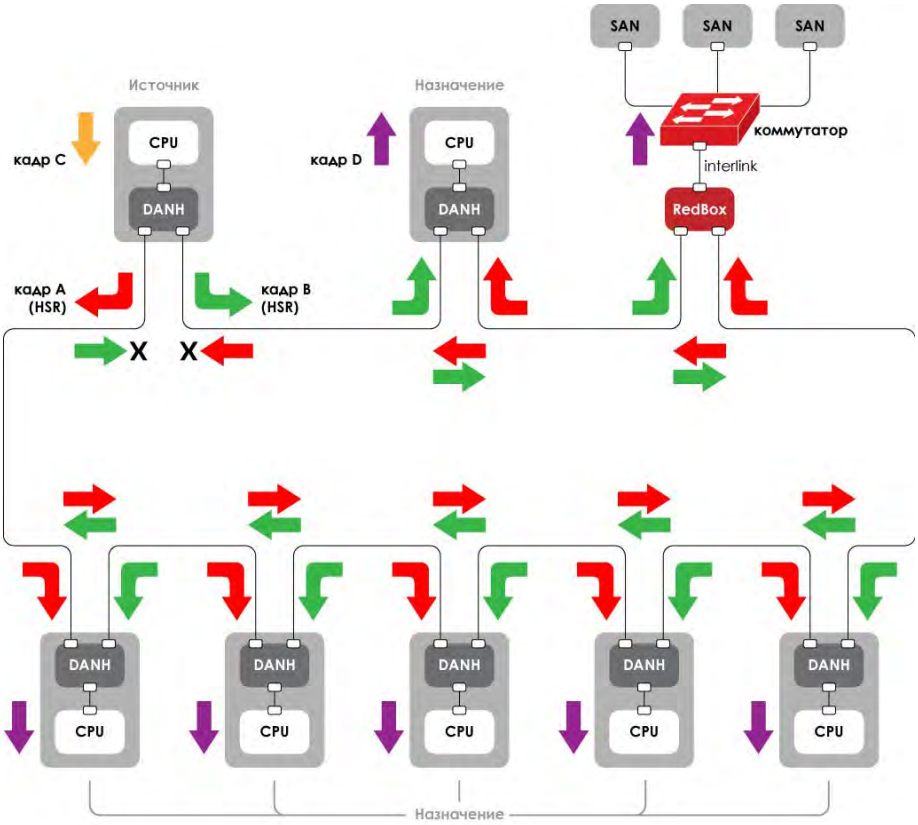

Рис. 5.3. Схема работы сети с использованием протокола HSR.

Исходный узел DAN получает с верхнего уровня кадр C, дублирует его и полученные копии – кадр B и кадр A отправляются в кольцо через разные Ethernet-интерфейсы по часовой стрелке и против часовой стрелки, соответственно. Узел-получатель DAN в кольце получает кадр A и проверяет, является ли он широковещательным кадром, если да, то принимает и пересылает кадр A; если нет, то узел-получатель DAN проверяет, является ли MAC-адрес назначения кадра A адресом данного узла DAN; если нет, то пересылает кадр A через другой порт на следующий узел DAN; если да, то проверяет, получен ли кадр B первым; если первым получен кадр B, то кадр A отбрасывается; если первым получен кадр A, то он передается на верхний уровень. Когда кадр A возвращается на порт исходного узла DAN, то узел определяет, что это отправленный им самим кадр и отбрасывает его. Принцип передачи кадра B совпадает с принципом передачи кадра A.

Так как каждый полученный с верхнего уровня кадр дублируется и передается в разных направлениях по кольцу, то любая одна точка обрыва сети влияет только на передачу в одном направлении, другое направление не затрагивается, и время для восстановления сети не требуется. При использовании протокола HSR отправляются сообщения мониторинга сети, если порт не получает сообщение мониторинга в течение длительного времени, то определяется, что подключенная сеть повреждена. Устройства, которые не поддерживают протокол HSR, могут быть к сети HSR через коммутатор NXI-3030RB.

5.3. Конфигурация резервирования

Для перехода на страницу конфигурации резервирования выберите в меню навигации пункт [Functions]→[Redundancy]. Страница конфигурации резервирования показана на Рис. 5.4.

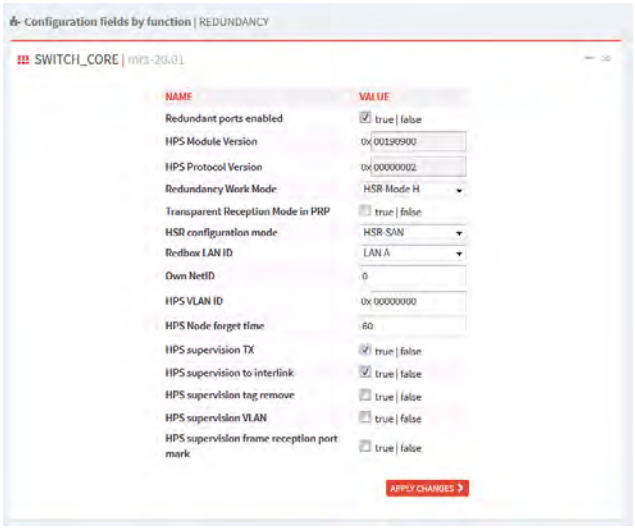

Рис. 5.4. Страница конфигурации резервирования.

Описание параметров конфигурации представлено в Таблица 5.1.

Таблица 5.1. Параметры конфигурации резервирования.

Параметр	*Значение*	*Функция*	*Значение по умолчанию*
Redundant ports enabled	true/false	Когда включено, порт работает как порт резервирования, а не как обычный Ethernet-порт.	true
HPS Module Version		Показывает текущую версию HPS-модуля.	
HPS Protocol Version		Показывает текущую версию протокола резервирования HSR-PRP.	
Redundancy Work Mode	PRP-Duplicate discard mode	Приемник LRE может обнаруживать повторяющиеся элементы, для реализации управления LRE добавляет к каждому кадру 32-битный трейлер контроля резервирования RCT (Redundancy Control Trailer). LRE приемник использует номер последовательности RCT и исходный MAC-адрес для обнаружения повторяющихся элементов и пересылает только первый кадр из двух на верхний	HSR-Mode H

		уровень. Все устройства в сети PRP должны быть установлены в режим PRP-Duplicate-discard, как показано на Рис. 5.6.	
	PRP-Duplicate accept mode	Используется в целях тестирования, чтобы убедиться, что дублирующиеся элементы действительно отбрасываются на канальном уровне, а не протоколом более высокого уровня. Передатчик LRE настроен на отправку двух дубликатов кадров без RCT. Приемник LRE настроен на прием двух кадров и пересылку их (если поступили оба) на верхний уровень.	
	HSR-Mode H	Является режимом по умолчанию, осуществляется пересылка кадров данных с HSR-тегом. За исключением кадров, отправленных самим узлом, DAN вставляет тег HSR и пересылает кольцевой сетевой трафик. Повторяющиеся кадры и кадры, в которых узел является адресатом одноадресной рассылки, пересылаться не будут. Все устройства в домене HSR должны быть настроены в одинаковом режиме для корректной работы.	
	HSR-Mode N	Режим отсутствия пересылки трафика. Узел в этом режиме ведет себя так же, как в H с тем исключением, что он не пересылает кольцевой трафик между своими портами.	
	HSR-Mode T	Режим прозрачной пересылки. В этом режиме DAN удаляет HSR-тег, а затем пересылает кадр на другой без тега и без отбрасывания повторяющихся кадров.	
	HSR-Mode U	Режим одноадресной пересылки. В этом режиме поведение узла аналогично режиму H, за исключением того, что трафик для которого данный узел – узел назначения, также пересылается дальше по кольцу.	

	HSR-Mode X	Режим отсутствия пересылки дублей. В этом режиме поведение узла аналогично режиму H, за исключением того, что узел будет отбрасывать кадры, уже полученные с противоположного кольцевого порта.	
Transparent Reception Mode in PRP	true/false	Если включен режим, то в режиме PRP дублирующийся кадр не отбрасывается, RTC не удаляется.	false
HSR configuration mode	HSR-SAN/HSR-HSR/HSR-PRP	Определяет уровень вложенности домена HSR: HSR-SAN (простой HSR), HSR-PRP (HSR-домен внутри PRP-домена) или HSR-HSR (HSR-домен внутри HSR-домена).	HSR-SAN
RedBox LAN ID	LAN A/LAN B	Определяет, в какой сети (A или B) располагается данный коммутатор с функцией RedBox в режиме HSR-PRP.	LAN A
Own NetID	3 бита [0-7]	Идентификационный номер кольцевой сети, подключенной к узлу.	0
HPS VLAN ID	12 битов [00-FFF]	Используется для определения идентификатора VLAN-узлов коммутатора с функцией RedBox.	00000000
HPS Node forget time	10 битов [0-1023] единица измерения – s (секунда)	Настройка времени устаревания соседнего узла HSR/PRP при отсутствии от него контрольных кадров.	600s
HPS supervision TX	true/false	Включение или отключение передачи контрольных кадров.	true
HPS supervision to interlink	true/false	Включение или отключение передачи контрольных кадров на порт связи.	true
HPS supervision tag remove	true/false	Включение или отключение удаления HSR-тегов или PRP-трейлеров при передаче контрольных кадров на порт связи.	false
HPS supervision VLAN	true/false	Включение или отключение обработки контрольных кадров с VLAN	false

5.3.1. Пример стандартной конфигурации резервирования PRP

Пример стандартной сети с использованием PRP показан на Рис. 5.5.

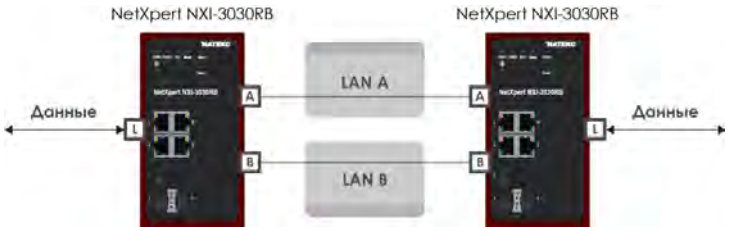

Рис. 5.5. Пример сети с использованием PRP.

Все устройства в сети PRP должны быть установлены в режим PRP-Duplicate discard mode. Рекомендуется подключать порт A коммутатора с функцией RedBox к порту A другого коммутатора с функцией RedBox, а порт B – подключался к порту B другого коммутатора с функцией RedBox. A-A может проходить через LAN A, B-B может проходить через LAN B, при этом LAN A и LAN B должны быть независимыми сетями.

В сети PRP в передаваемые через сети LAN A и LAN B кадры не будут добавляться другие заголовки второго уровня, поэтому сетевые устройства (коммутаторы) в этих сетях могут быть любыми и могут использовать другие протоколы резервирования (RSTP, ERPS и т.п.). Конфигурация коммутатора для использования PRP показана на Рис. 5.6.

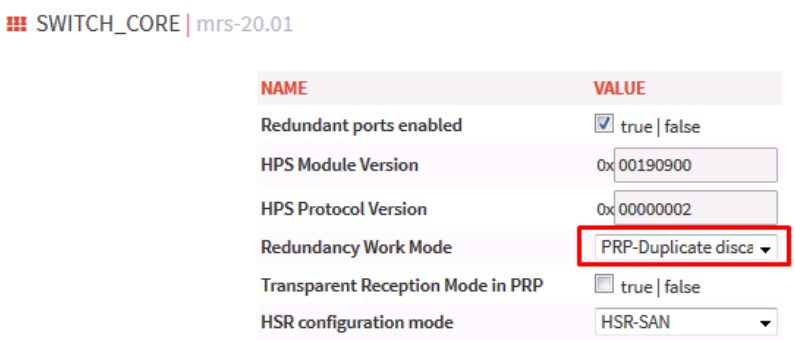

Рис. 5.6. Конфигурация коммутатора для использования PRP.

5.3.2. Пример стандартной конфигурации резервирования HSR

Пример стандартной сети с использованием протокола HSR показан на Рис. 5.7.

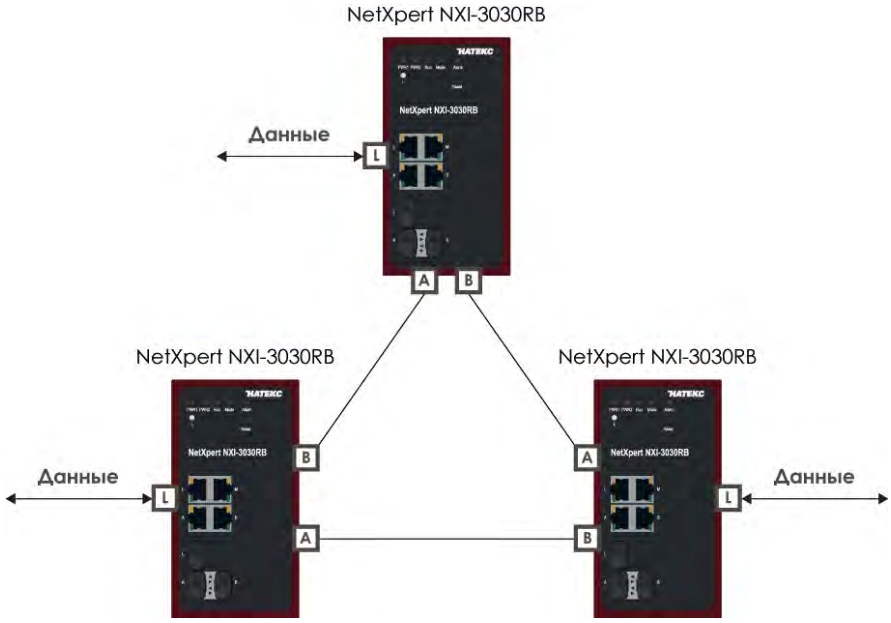

Рис. 5.7. Пример сети с использованием протокола HSR.

Все устройства в сети HSR должны быть сконфигурированы для работы в режиме HSR-mode H. Рекомендуется, чтобы порт A одного коммутатора с функцией RedBox соединялся с портом B другого коммутатора с функцией RedBox, а порт B – соединялся с портом A, как кольцо.

В точках соединения между устройствами может быть организована прозрачная передача данных с использованием других устройств. Но поскольку ко всем передаваемым между устройствами HSR-кадрам добавляются HSR-тэги, если между устройствами будут добавлены прозрачные устройства передачи данных, ими нельзя управлять удаленно. Конфигурация коммутатора для использования HSR показана на Рис. 5.8.

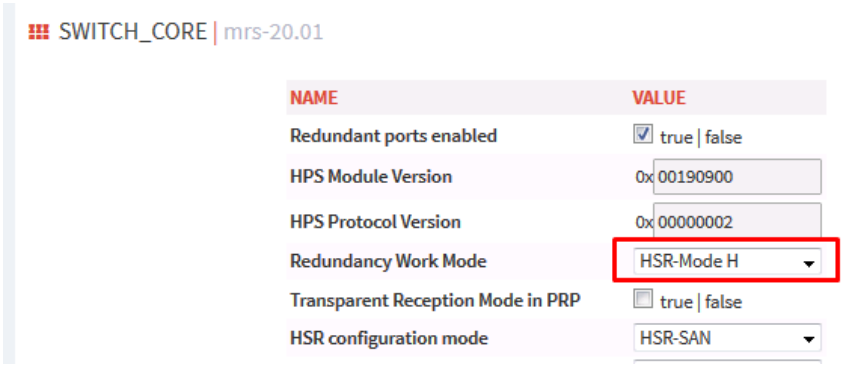

Рис. 5.8. Конфигурация коммутатора для использования HSR.

5.3.3. Пример стандартной конфигурации резервирования с Quadbox

Пример стандартной сети с использованием Quadbox показан на Рис. 5.9.

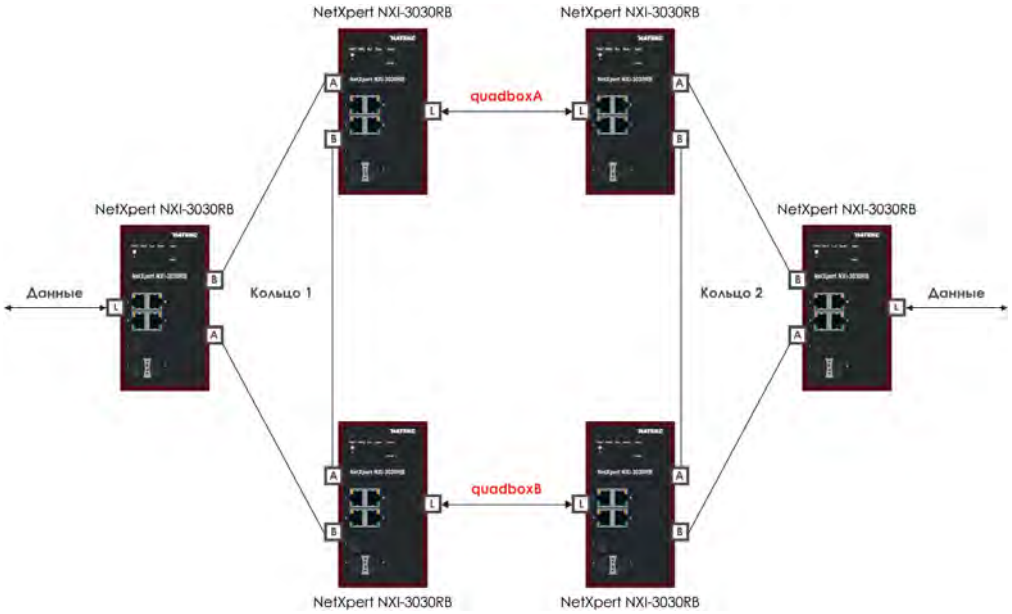

Рис. 5.9. Пример сети с использованием Quadbox.

Преимуществом сети с Quadbox является то, что она позволяет объединить два независимых HSR-кольца, повышая таким образом отказоустойчивость сети передачи данных. quadboxA и quadboxB выполняют роль DAN, являются портами резервирования HSR и могут пересылать данные из одного HSR-кольца в другое.

Все устройства в сети Quadbox должны быть установлены в режим HSR-H (режим по умолчанию), на устройствах группы quadbox должен быть настроен режим вложенности HSR-HSR. Конфигурация коммутатора для использования Quadbox показана на Рис. 5.10.

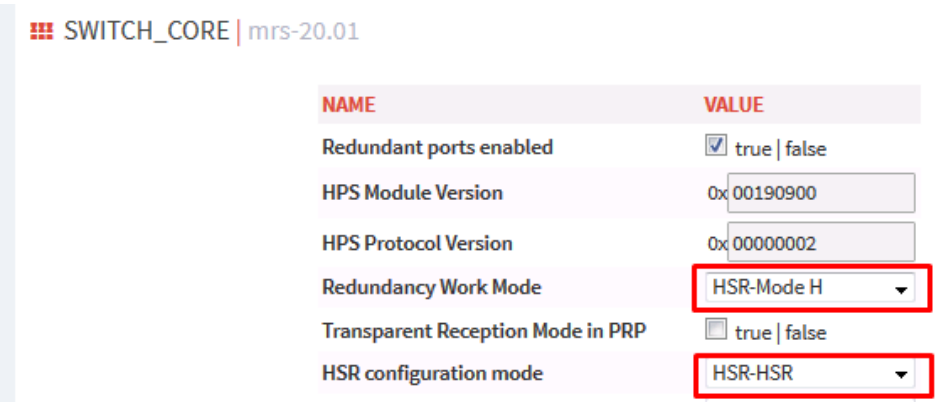

Рис. 5.10. Конфигурация коммутатора для использования Quadbox.

6. PTP

6.1. Терминология и общее представление о PTP

Протокол точного времени (PTP) синхронизирует независимые часы на распределенных узлах системы с высокой точностью и достоверностью. Протокол синхронизирует фазу и частоту с точностью до ±100 нс. Введем некоторые понятия, связанные с протоколом.

PTP-домен – это сеть, в которой применяется PTP. PTP-домен имеет только одно устройство Grandmaster (главные ведущие часы). Все остальные устройства непосредственно или косвенно синхронизируют с ним свои часы.

PTP-порт – это порт с включенной функцией PTP.

Узел часов – в контексте PTP-домена все узлы, которые так или иначе участвуют в синхронизации времени, будем называть часами. Различают следующие типы часов:

- Ordinary Clock (OC) - обычные часы
- В PTP-домене узлы OC имеют только один порт, принимающий участие в синхронизации. Порт OC получает информацию для синхронизации часов от uplink-узла.
- Boundary Clock (BC) – граничные часы
- В PTP-домене узлы BC имеют один или несколько PTP-портов, участвующих в синхронизации часов. Если только один PTP-порт принимает участие в синхронизации часов, PTP-порт получает информацию для синхронизации часов от uplink-узла или передает эту информацию downlink-узлу. Если несколько PTP-портов принимают участие в синхронизации часов, один из них получает информацию для синхронизации часов от uplink-узла, а остальные PTP-порты передают эту информацию одному или нескольким downlink-узлам.
- Transparent Clock (TC) – прозрачные часы
- Узел TC не должен сверять время с часами других узлов. PTP-порты узла TC только пересылают PTP-кадры и проверяют задержку пересылки, но не выполняют синхронизацию часов. Прозрачные часы делятся на следующие типы:
- End-to-End Transparent Clock (E2ETC): сквозные прозрачные часы, передают напрямую не PTP-пакеты и принимают участие в вычислении задержки всей линии связи.
- Peer-to-Peer Transparent Clock (P2PTC): одноранговые прозрачные часы, передают напрямую пакеты типов Sync, Follow_Up и Announce, терминируют остальные PTP-пакеты и принимают участие в вычислении задержки каждого сегмента линии связи.

Взаимоотношения между парой синхронных часов следующие:

Ведущий узел (Master Node) – узел, отправляющий информацию для синхронизации часов.

Ведомые узлы (Slave Node) – узлы, принимающие информацию, отправленную ведущим узлом.

Ведущие часы (Master Clock) – часы ведущего узла.

Ведомые часы (Slave Clock) – часы ведомого узла.

Ведущий порт (Master Port) – порт, отправляющий информацию для синхронизации часов.

Ведомые порты (Slave Port) – порты, получающие информацию для синхронизации от ведущего порта.

6.1.1. Принцип работы синхронизации

Выбор главных ведущих (Grandmaster) часов

Все узлы выбирают главные ведущие часы в домене PTP, обмениваясь Announce-пакетами с информацией об уровне часов (clock stratum) и идентификаторе часов (clock ID). Затем определяются отношения ведущий/ведомый между узлами и ведущие/ведомые порты на узлах. При этом процессе во всем домене PTP устанавливается связующее дерево с главными ведущими часами в качестве корневого узла. Затем ведущие часы периодически отправляют Announce-пакеты ведомым часам. Если ведомые часы не получают Announce-пакеты от ведущих часов в течение определенного периода времени, ведущие часы считаются не действующими, и выбор начинается заново.

Announce-пакеты содержат следующую информацию для выбора главных ведущих часов: поле 1 приоритета главных ведущих часов, уровень часов, точность синхронизации, поле 2 приоритета главных ведущих часов и идентификатор часов.

Процедура сравнения информации следующая: часы с наименьшим первым приоритетом выбираются в качестве главных ведущих часов; если у часов одинаковое значение поля первого приоритета, то в качестве главных ведущих выбираются часы с наименьшим номером уровня; аналогично, если у часов одинаковое значение поля первого приоритета, уровня, точности, второго приоритета, то в качестве главных ведущих выбираются часы с наименьшим значением идентификатора.

Принцип работы синхронизации

Ведущие и ведомые часы обмениваются пакетами синхронизации, записывают время отправки и получения пакетов, измеряют общую задержку между ведущими и ведомыми часами на основании разницы во времени. Если сетевой тракт является симметричным, задержка в одном направлении составляет половину общей задержки. Ведомые часы корректируют время в соответствии с разницей во времени между ведущими часами и ведомыми часами, и задержкой в одном направлении, осуществляя синхронизацию времени с ведущими часами.

PTP поддерживает два механизма измерения задержки:

- Механизм запрос-ответ: используется для измерения сквозной задержки (end-to-end) всей линии связи.
- Механизм Peer-to-peer: используется для измерения задержки «точка-точка» (point-to-point). В отличие от механизма запрос-ответ, механизм peer-to-peer измеряет задержку каждого сегмента линии.

6.2. Конфигурация PTP

Для перехода на страницу PTP выберите в меню навигации пункт [Functions]→[PTP]. Страница конфигурации даты и времени показана на Рис. 6.1.

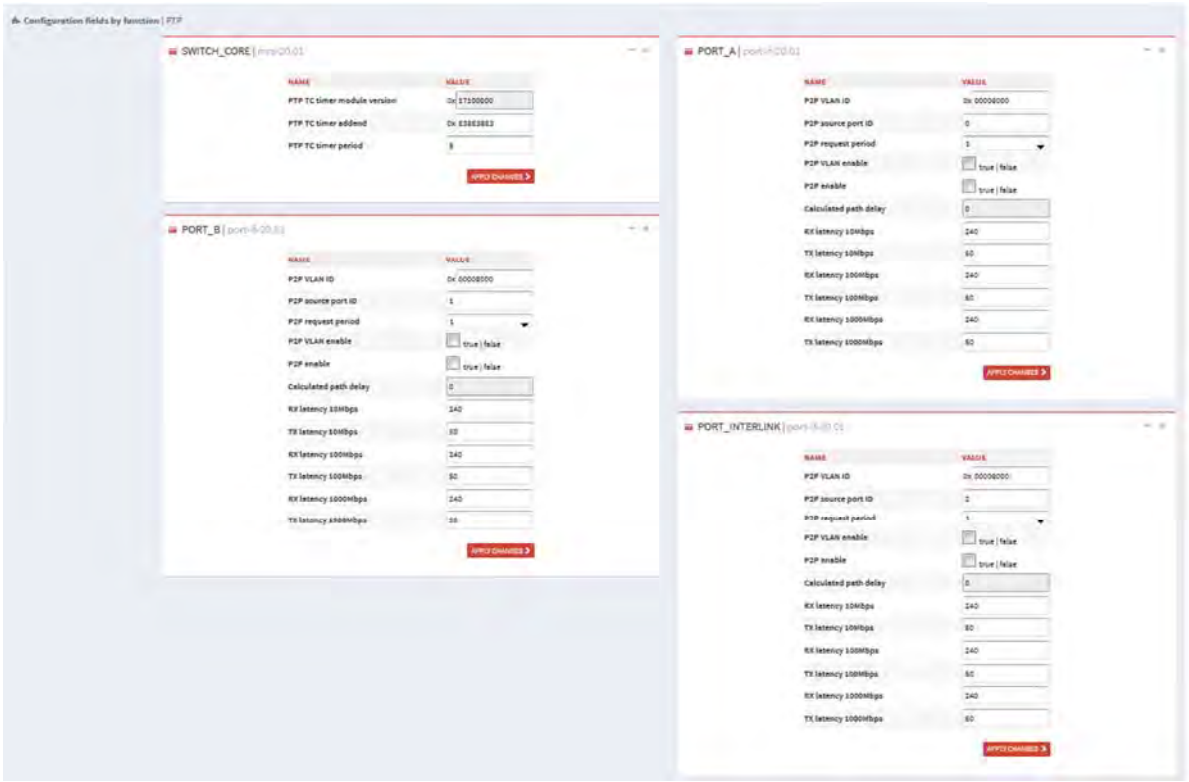

Рис. 6.1. Страница конфигурации даты и времени.

Как показано на Рис. 6.1, страница конфигурации PTP разделена на 4 части: страница конфигурации прозрачных часов PTP TC и страница конфигурации PTP для трех портов (PORT_A / PORT_B / PORT_INTERLINK).

6.2.1. Конфигурация прозрачных часов PTP TC

Конфигурация прозрачных часов PTP TC показана на Рис. 6.2.

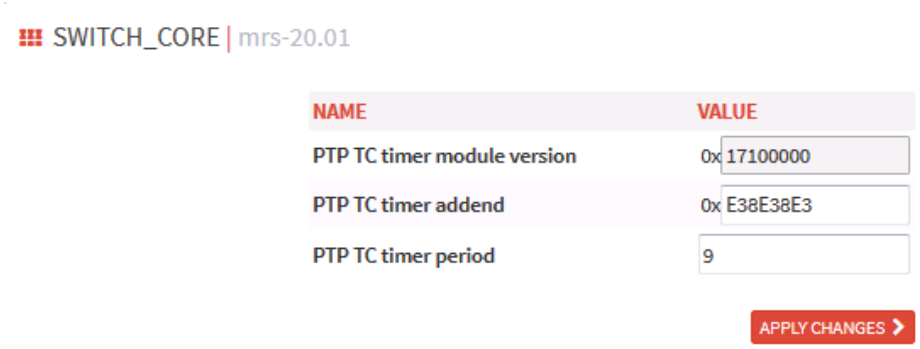

Рис. 6.2. Конфигурация PTP TC.

Описание параметров конфигурации PTP TC приведено в Таблица 6.1.

Таблица 6.1. Параметры конфигурации PTP TC.

Параметр	*Функция*	*Диапазон значений*	*Значение по умолчанию*
PTP TC timer module version	IEEE1588 версия модуля таймера прозрачных часов		
PTP TC timer addend	Регулировка таймера на субсекундном уровне (см. Freescale AN3423). Не рекомендуется менять значение по умолчанию.	32 бита [00-FFFFFFFF]	E38E38E3
PTP TC timer period	см. Freescale AN3423. Не рекомендуется менять значение по умолчанию.	32 бита [0-4294967295]	9

6.2.2. Конфигурация PTP для портов

Для примера PTP конфигурации порта рассмотрим конфигурацию порта PORT_A, показано на Рис. 6.3.

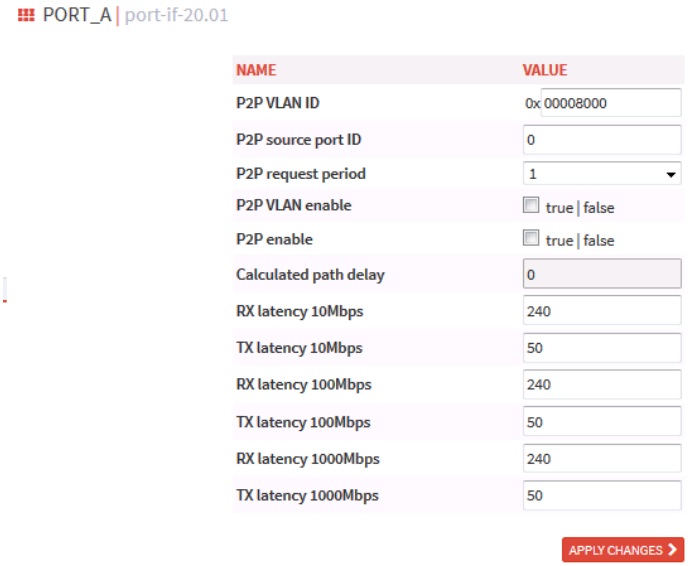

Рис. 6.3. Конфигурация PTP PORT_A.

Описание параметров PTP-конфигурации порта приведено в Таблица 6.2.

Таблица 6.2. Параметры PTP конфигурации порта.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
P2P VLAN ID	Настройка тега VLAN для кадров PTP	16 битов [00-FFFF]	00008000
P2P Source Port ID	Настройка идентификатор порта-источника для PTP	32 бита [00-FFFFFFFF]	0
P2P request period	Настройка количества запросов Pdelay в секунду	1/2/4/8	1
P2P VLAN enable	Включение добавления тега VLAN к сообщению PTP	true/false	false
P2P enable	Включение или выключение механизма задержки P2P	true/false	false
RX latency 10Mbps	Логическая задержка приема на скорости 10 Мбит/с (в наносекундах)	16 битов [0-65535]	240
TX latency 10Mbps	Логическая задержка передачи на скорости10 Мбит/с (в наносекундах)	16 битов [0-65535]	50
RX latency 100Mbps	Логическая задержка приема на скорости 100 Мбит/с (в наносекундах)	16 битов [0-65535]	240

TX latency 100Mbps	Логическая задержка передачи на скорости 100 Мбит/с (в наносекундах)	16 битов [0-65535]	50
RX latency 1000Mbps	Логическая задержка приема на скорости 1000 Мбит/с (в наносекундах)	16 битов [0-65535]	240
TX latency 1000Mbps	Логическая задержка передачи на скорости 1000 Мбит/с (в наносекундах)	16 битов [0-65535]	50
Calculated path delay	Задержка пути (в наносекундах), вычисленная с использованием однорангового механизма прозрачных часов PTP		

7. СТАТИСТИКА

Для перехода на страницу конфигурации статистики выберите в меню навигации пункт [Functions]→[Statistics]. Страница конфигурации статистики на примере порта PORT_A показана на Рис. 7.1.

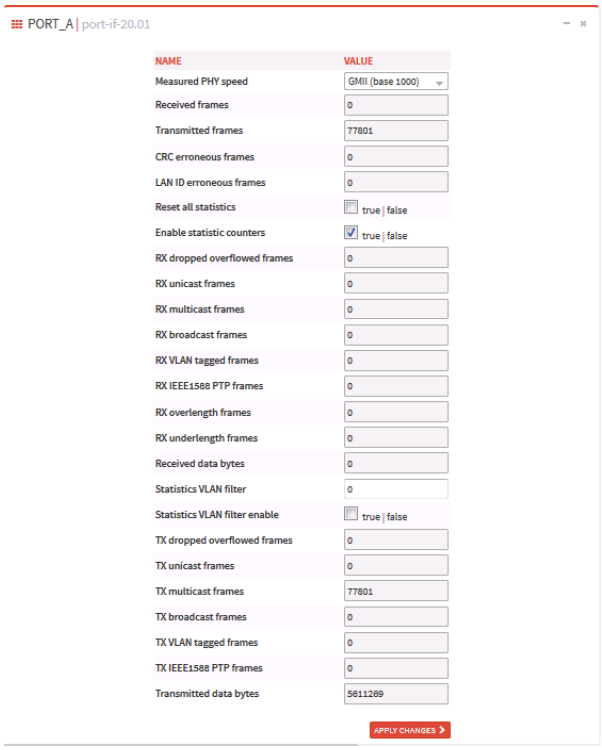

Рис. 7.1. Страница конфигурации статистики для PORT_A.

Описание параметров конфигурации статистики порта приведено в Таблица 7.1.

Таблица 7.1. Параметры конфигурации статистики порта.

Параметр	*Функция*	*Значение*
Measured PHY speed	Скорость PHY, измеренная с помощью модуля измерения скорости: «11» при 1000 Мбит/с, «10» при 100 Мбит/с и «01» при 10 Мбит/с.	
Received frames	Показывает количество полученных кадров.	32 бита [0-4294967295]
Transmitted frames	Показывает количество переданных кадров.	32 бита [0-4294967295]
CRC erroneous frames	Показывает количество кадров с ошибками CRC.	32 бита [0-4294967295]
LAN ID erroneous frames	Показывает количество кадров с ошибками идентификатора LAN.	32 бита [0-4294967295]
Reset all statistics	Сброс всех счетчиков статистики.	
Enable statistic counters	Включение или выключение счетчиков статистики.	true/false

RX Dropped overflowed frames	Количество кадров, отброшенных при приеме в связи с переполнением.	32 бита [0-4294967295]
RX Unicast frames	Количество принятых кадров одноадресной рассылки.	32 бита [0-4294967295]
RX Multicast frames	Количество принятых кадров многоадресной рассылки.	32 бита [0-4294967295]
RX Broadcast frames	Количество принятых кадров широковещательной рассылки.	32 бита [0-4294967295]
RX VLAN tagged frames	Количество принятых кадров с тегами VLAN.	32 бита [0-4294967295]
RX IEEE1588 PTP frames	Количество принятых IEEE1588 PTP кадров.	32 бита [0-4294967295]
RX Overlength frames	Количество принятых кадров превышенной длины (действительно, когда отключены jumbo-кадры).	32 бита [0-4294967295]
RX Underlength frames	Количество принятых кадров меньше минимального размера (64б).	32 бита [0-4294967295]
Received data bytes	Количество полученных байтов данных (за исключением ведущего байта).	32 бита [0-4294967295]
Statistics VLAN filter	Счетчик фильтра VLAN.	12 битов 0X[0-00000FFF]
Statistics VLAN filter enable	Включение или отключение счетчика фильтра VLAN.	true/false
TX Dropped overflowed frames	Количество кадров, отброшенных при приеме в связи с переполнением.	32 бита [0-4294967295]
TX Unicast frames	Количество переданных кадров одноадресной рассылки.	32 бита [0-4294967295]
TX Multicast frames	Количество переданных кадров многоадресной рассылки.	32 бита [0-4294967295]
TX Broadcast frames	Количество переданных кадров широковещательной рассылки.	32 бита [0-4294967295]
TX VLAN tagged frames	Количество переданных кадров с тегами VLAN.	32 бита [0-4294967295]
TX IEEE1588 PTP frames	Количество переданных кадров IEEE1588 PTP.	32 бита [0-4294967295]
Transmitted data bytes	Количество переданных байтов данных (за исключением ведущего байта).	32 бита [0-4294967295]

8. ПРОЧИЕ НАСТРОЙКИ

8.1. Аварийные сигналы

Коммутатор с функцией RedBox серии NXI-3030RB поддерживает следующие типы аварийных сигналов:

- Аварийный сигнал об использовании памяти / ЦП – если эта функция включена, аварийный сигнал генерируется, когда использование памяти / ЦП превышает указанный порог.
- Аварийный сигнал порта – если эта функция включена, аварийный сигнал генерируется, когда порт находится в отключенном состоянии.
- Сигнализация об аварийном событии может быть следующей: запись в журнале событий (Syslog), включение светодиодного индикатора Alarm, переключение реле сухих контактов и отправка трапов SNMP.

8.1.1. Конфигурация аварийных сигналов использования памяти / ЦП

Для перехода на страницу конфигурации аварийных сигналов использования памяти / ЦП выберите в меню навигации пункт [Other Configurations] → [Alarm]. Страница конфигурации аварийных сигналов использования памяти / ЦП показана на Рис. 8.1

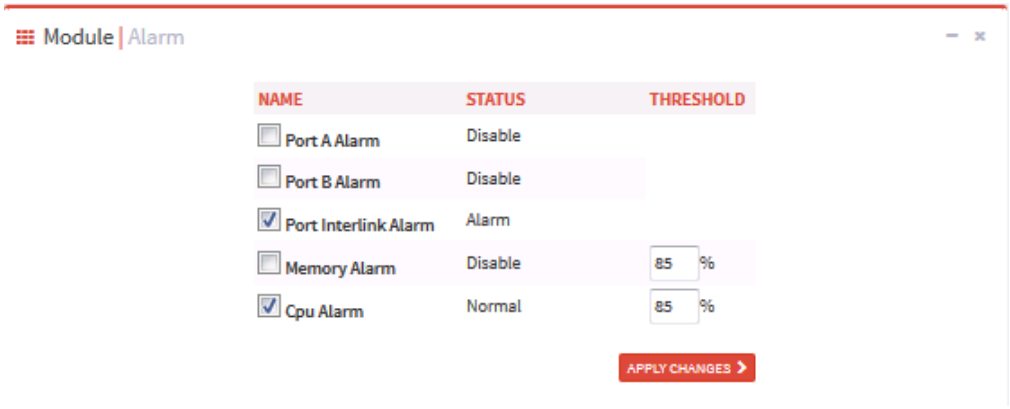

Рис. 8.1. Конфигурация аварийных сигналов использования памяти / ЦП.

Описание параметров конфигурации аварийных сигналов использования памяти / ЦП приведено Таблице 8.1.

Таблица 8.1. Параметры конфигурации аварийных сигналов использования памяти / ЦП.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Memory Alarm/CPU Alarm	Включение или выключение аварийного сигнала использования памяти / ЦП	enable/disable	disable
Threshold	Настройка порога срабатывания аварийного сигнала памяти / ЦП. Когда коэффициент использования памяти / ЦП превышает пороговое значение, генерируется аварийный сигнал памяти / ЦП.	50…100 %	85%
Alarm status	Показывает состояние использования памяти / ЦП. Значение Alarm указывает на то, что использование памяти / ЦП превышает пороговое значение. Аварийный сигнал будет прекращен, когда коэффициент использования памяти / ЦП будет ниже порогового значения. Под коэффициентом использования ЦП принимается средний коэффициент использования ЦП за 5 секунд.	Normal/Alarm	

8.1.2. Конфигурация аварийных сигналов порта

Для перехода на страницу конфигурации аварийных сигналов порта выберите в меню навигации пункт [Other Configurations] → [Alarm]. Страница конфигурации аварийных сигналов порта показана на Рис. 8.2.

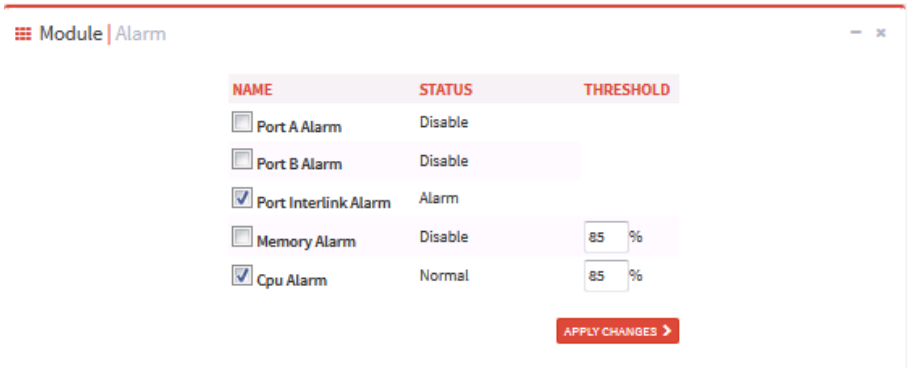

Рис. 8.2. Конфигурация аварийных сигналов порта.

Описание параметров конфигурации аварийных сигналов порта приведено в Таблица 8.2.

Таблица 8.2. Параметры конфигурации аварийных сигналов порта.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Port	Включение или выключение аварийного сигнала порта	disable/enable	enable
Alarm status	Отображение состояния подключения порта. Normal показывает, что порт подключен и может нормально обмениваться данными; Alarm указывает, что порт отключен или неисправен, будет сгенерирован аварийный сигнал.	Normal/Alarm	

8.2. Конфигурация порта

Для перехода на страницу конфигурации порта выберите в меню навигации пункт [Other Configurations] → [Port configuration]. На странице конфигурации порта можно посмотреть и настроить состояние порта, скорость, тип, как показано на Рис. 8.3.

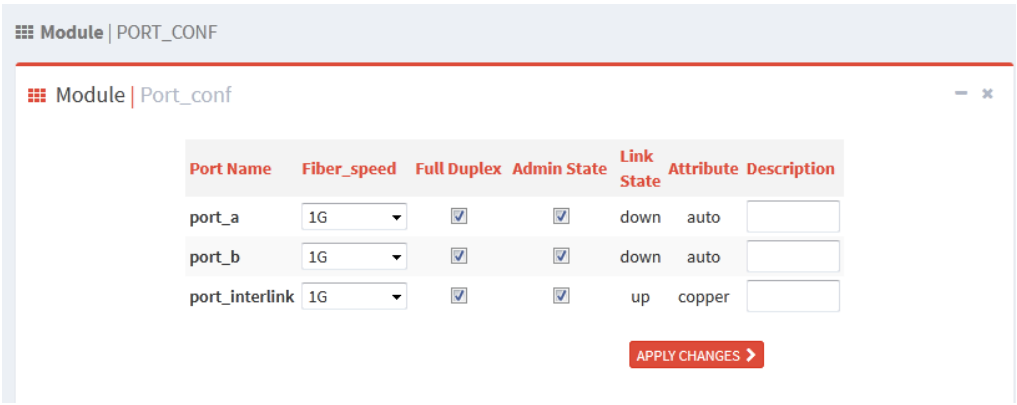

Рис. 8.3. Страница конфигурации порта.

Описание параметров конфигурации порта приведено в Таблица 8.3.

Таблица 8.3. Параметры конфигурации порта.

Параметр	*Функция*	*Значение*
Port Name	Выбор настраиваемого порта	port_a / port_b / port_interlink
Fiber_speed	Настройка скорости оптического порта. Только на оптическом порту можно установить скорость 100M. Скорость медного порта определяется автосогласованием. port_interlink модуля HSR / PRP используется для внутренних целей, не следует менять его конфигурацию.	100M/1G
Full Duplex	Конфигурация режима дуплекса. Полный дуплекс (Full Dupplex) означает, что порт может одновременно принимать данные и передавать данные. Если данная опция	Enable/disable

	отключена, порт работает в режиме полудуплекса, что означает, что порт может либо передавать, либо получать данные в конкретный момент времени.	
Admin Status	Выбор, разрешено ли порту передавать данные, значение по умолчанию – no shutdown. Enable означает, что порту разрешен прием и передача данных; disable означает, что порт отключен и передача данных не разрешена. Эта опция может напрямую влиять на состояние порта и запускать срабатывание аварийного сигнала порта.	Enable/disable
Link Status	Показывает статус линии подключения текущего порта. up указывает, что порт находится в состоянии LinkUp и может нормально взаимодействовать; down указывает, что порт находится в состоянии LinkDown и не может передавать и принимать.	up/down
Attribute	Тип носителя порта Ethernet, значение по умолчанию – auto. auto – порт автоматически обнаруживает кабель для определения типа носителя. copper – устанавливает тип носителя порта медь.	auto/copper
Description	Настройка описания порта для описания порта.	1…200 символов

8.3. Конфигурация таблицы MAC-адресов

8.3.1. Сведения о таблице MAC-адресов коммутатора

При передаче Ethernet-кадра коммутатор ищет порт назначения в таблице MAC-адресов на основании адреса назначения кадра. MAC-адрес в такой таблице может быть статическим или динамическим.

Статические MAC-адреса являются конфигурируемыми. Они имеют высший приоритет (не перезаписываемый динамическими MAC-адресами) и не удаляются автоматически.

Динамические MAC-адреса изучаются коммутатором в процессе передачи данных, они являются действующими только в течение определенного периода времени (время устаревания), после чего удаляются. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных, подлежащего передаче, коммутатор считывает MAC-адрес источника кадра, устанавливает соответствие принимающего порта и запрашивает передающий порт в таблице MAC-адресов на основании MAC-адреса назначения кадра. Если совпадение найдено, коммутатор пересылает кадр в соответствующий порт назначения. Если совпадение не найдено, коммутатор пересылает кадр в соответствующий широковещательный домен.

Отсчет времени устаревания начинается с момента, когда динамический MAC-адрес добавляется в таблицу MAC-адресов. Если ни один порт не получает кадр данных с данным MAC-адресом источника в течение от одного

до двух периодов устаревания, коммутатор удаляет эту запись MAC-адреса из динамической таблицы адресов пересылки. Статические MAC-адреса не используют концепцию времени устаревания.

8.3.2. Просмотр таблицы MAC-адресов

Для перехода на страницу просмотра таблицы MAC-адресов выберите в меню навигации пункт [Other Configurations] → [Mac Queries]. Пример страницы просмотра таблицы MAC-адресов показан на Рис. 8.4. В режиме коммутации port_a, port_b, port_interlink соответствуют трем физическим портам коммутатора. В режиме резервирования port_b представляет из себя два резервных порта, которые не делятся на A и B, port_a не используется.

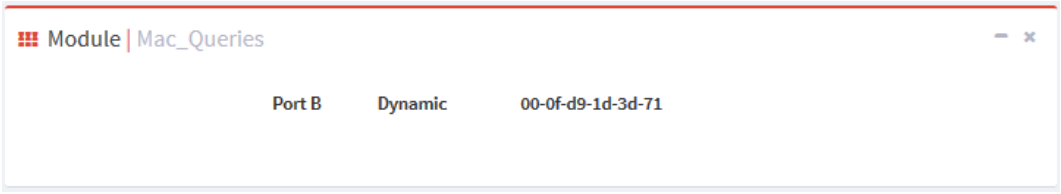

Рис. 8.4. Страница просмотра таблицы MAC-адресов.

8.3.3. Контроль таблицы MAC-адресов

Для перехода на страницу контроля таблицы MAC-адресов выберите в меню навигации пункт [Other Configurations] → [Mac Address Control]. Пример страницы контроля таблицы MAC-адресов показан на Рис. 8.5.

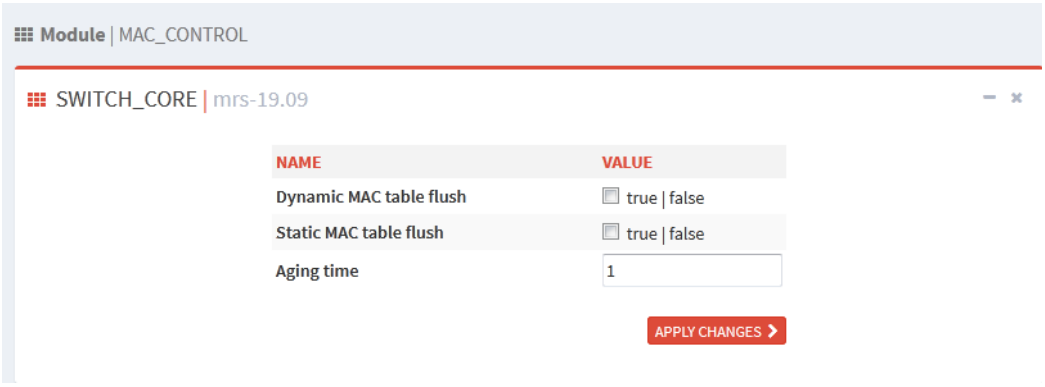

Рис. 8.5. Страница контроля таблицы MAC-адресов.

Описание параметров контроля таблицы MAC-адресов приведено в Таблице 8.4.

Таблица 8.4. Параметры контроля таблицы MAC-адресов.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Dynamic MAC table flush	Принудительная очистка динамической таблицы MAC-адресов. Для очистки нужно отметить данный чек-бокс и нажать <Apply>	true/false	false
Static MAC table flush	Принудительная очистка статической таблицы MAC-адресов. Для очистки нужно отметить данный чек-бокс и нажать <Apply>	true/false	false
Aging time	Конфигурация времени устаревания динамической таблицы MAC-адресов. Значение 0 указывает на то, что динамические записи в таблице MAC-адресов не устаревают и не удаляются автоматически.	0…15 минут	1

8.3.4. Конфигурация статических MAC-адресов

Для перехода на страницу конфигурации статических MAC-адресов выберите в меню навигации пункт [Other Configurations] → [Mac Address Configuration]. Пример страницы конфигурации MAC-адресов портов показан на Рис. 8.6.

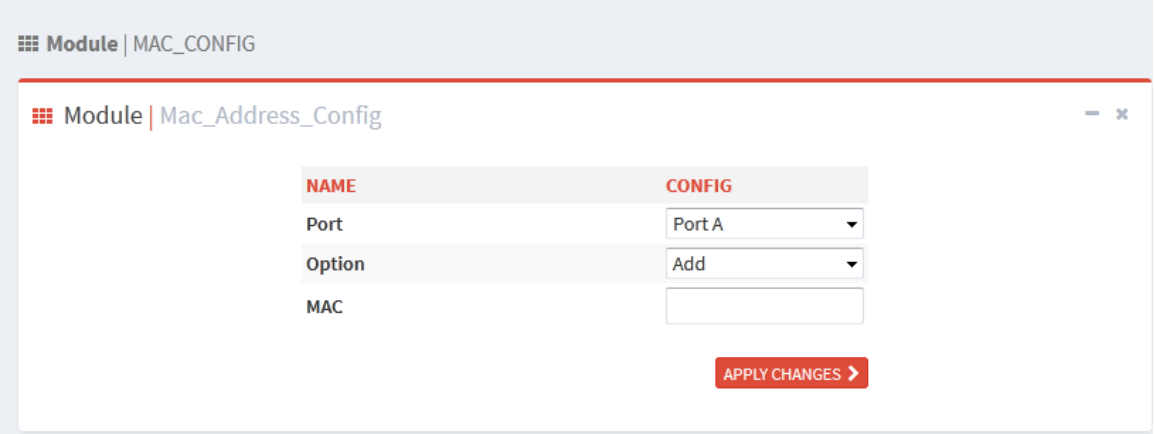

Рис. 8.6. Страница конфигурации MAC-адресов портов.

Описание параметров конфигурации MAC-адресов портов приведено в Таблица 8.5.

Таблица 8.5. Параметры конфигурации MAC-адресов портов.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Port	Выбор порта для настройки	port_a/port_b/port_interlink	port_a
Option	Добавление или удаление MAC-адреса порта	add/delete	add
MAC	Настройка одноадресного MAC-адреса.	HH-HH-HH-HH-HH-HH (HH – шестнадцатиричное число)	

8.4. SNTP

Простой протокол сетевого времени (Simple Network Time Protocol - SNTP) синхронизирует время между сервером и клиентом с помощью запросов и ответов. Являясь клиентом, коммутатор синхронизирует время с сервером в соответствии с полученными от сервера пакетами.

Для синхронизации времени по протоколу SNTP необходимо иметь активный SNTP-сервер. Вся информация о времени, передаваемая по протоколу SNTP, является информацией о стандартном времени часового пояса UTC.

8.4.1. Конфигурация SNTP

Для включения и конфигурации SNTP выберите в меню навигации пункт [Other Configurations] → [SNTP]. Страница конфигурации SNTP показана на Рис. 8.7.

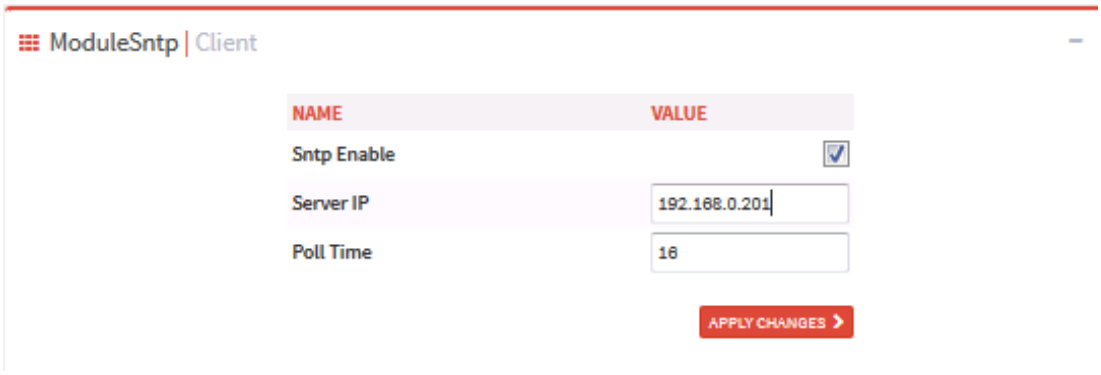

Рис. 8.7. Страница конфигурации SNTP.

Описание параметров конфигурации SNTP приведено в Таблица 8.6.

Таблица 8.6. Параметры конфигурации SNTP.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
SNTP Enable	Включение или отключение SNTP. Поскольку NTP и SNTP используют один и тот же номер порта UDP, то оба протокола не могут быть включены одновременно.	enable/disable	disable
Server IP	Нужно указать IP-адрес сервера SNTP, с которым коммутатор будет синхронизировать время	A.B.C.D	
Poll Time	Настройка временного интервала отправки SNTP-запросов на синхронизацию на сервер SNTP.	16…16284 с	

Для просмотра работы синхронизации часов с сервером SNTP выберите в меню навигации пункт [Network Nodes], как показано на Рис. 8.8. Нажмите кнопку <display clock>, часы отобразятся на странице после того, как клиент SNTP синхронизирует время с сервером SNTP.

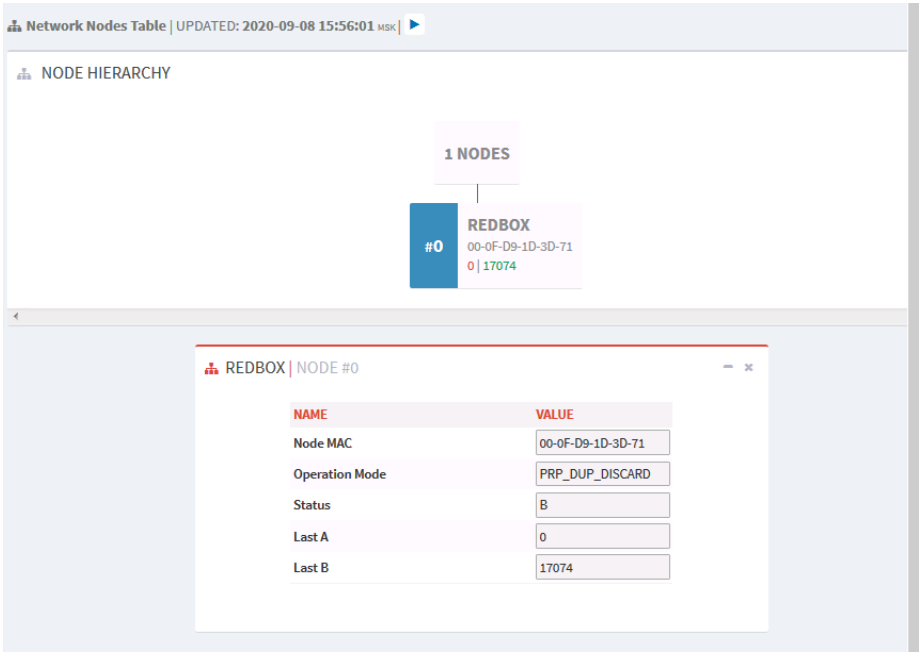

Рис. 8.8. Страница просмотра часов.

8.5. NTP

Протокол сетевого времени (Network Time Protocol - NTP) используется для синхронизации времени между распределенными серверами и клиентами. Протокол NTP применяется для синхронизации серверов точного времени. Локальная система с поддержкой NTP может не только синхронизировать свои часы с другими источниками синхронизации, но также служить сервером синхронизации времени для других устройств.

Высокоточная синхронизация часов между устройствами достигается так, как показано на Рис. 8.9. Задержка приема-передачи «(T4-T1) - (T3-T2)» и смещение часов «((T2-T1) + (T3-T4)) / 2» могут быть рассчитаны на основе обмена пакетами NTP.

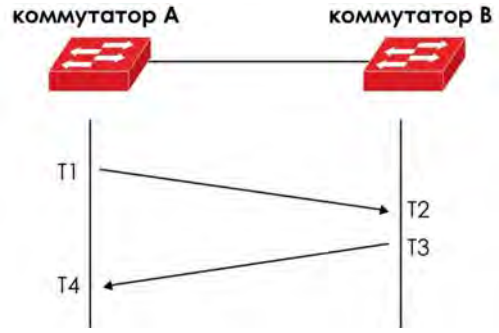

Рис. 8.9. Схема работы NTP.

При использовании NTP можно выбрать следующие режимы работы для синхронизации времени:

- Режим клиент / сервер: клиент отправляет на сервер пакеты синхронизации часов (режим клиента). После получения пакетов синхронизации сервер автоматически отправляет ответные пакеты (режим сервера). После получения ответных пакетов клиент синхронизируется с часами сервера.

- Одноранговый режим (Peer mode): активный одноранговый узел отправляет пакеты тактовой синхронизации (активный одноранговый режим) пассивному одноранговому узлу. После получения пакетов пассивный одноранговый узел автоматически отправляет ответные пакеты (пассивный одноранговый режим). На основе обмена пакетами устройства устанавливают одноранговый режим. Активный и пассивный одноранговые узлы могут синхронизировать время друг с другом. Если оба одноранговых узла синхронизировали время с другими устройствами, одноранговый узел с большим уровнем часов (clock stratum) синхронизирует время от однорангового узла с меньшим уровнем часов.

- Широковещательный режим: широковещательный сервер периодически передает пакеты синхронизации часов (режим широковещания). После получения пакетов широковещательный клиент отправляет на сервер пакеты синхронизации часов (клиентский режим). После получения пакетов запроса сервер отправляет ответные пакеты

(режим сервера). Сервер и клиент завершают синхронизацию часов обменявшись 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 пакетами запроса и ответа одноадресной синхронизации.

8.5.1. Конфигурация NTP

Для включения и конфигурации NTP выберите в меню навигации пункт [Other Configurations] → [NTP]. Страница конфигурации NTP показана на Рис. 8.10.

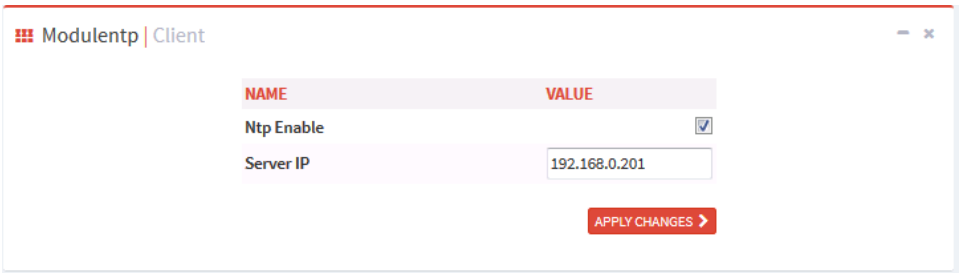

Рис. 8.10. Страница конфигурации NTP.

Описание параметров конфигурации NTP приведено в Таблица 8.7.

Таблица 8.7. Параметры конфигурации NTP.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
NTP Enable	Включение или отключение службы NTP. Поскольку NTP и SNTP используют один и тот же номер порта UDP, то оба протокола не могут быть включены одновременно. Для настройки и сохранения конфигурации NTP не требуется включение службы NTP.	enable/disable	disable
Server IP	Нужно указать IP-адрес сервера SNTP, с которым коммутатор будет синхронизировать время.	A.B.C.D	

8.6. IEC 61850

IEC 61850 – это группа стандартов, разработанная специально для использования в автоматизации подстанций. Коммутатор NXI-3030RB смоделирован в соответствии с IEC 61850 и включен в автоматическую систему подстанции (IEC 61850) как интеллектуальное электронное устройство (IED, Intelligent Electronic Device), это позволяет удобно интегрировать коммутатор в систему мониторинга и управления цифровой подстанцией.

Коммутатор поддерживает сервер IEC 61850 MMS по стандарту МЭК 61850-90-4. Файл конфигурации по умолчанию switch.cid уже импортирован на данный коммутатор. Если необходимо загрузить другой файл конфигурации, обратитесь к инструкции в разделе 4.8 – Загрузка файлов.

8.6.1. Конфигурация IEC 61850

Для включения и конфигурации IEC 61850 сервера MMS выберите в меню навигации пункт [Other Configurations] → [IEC61850MMS]. Страница конфигурации IEC61850 показана на Рис. 8.11.

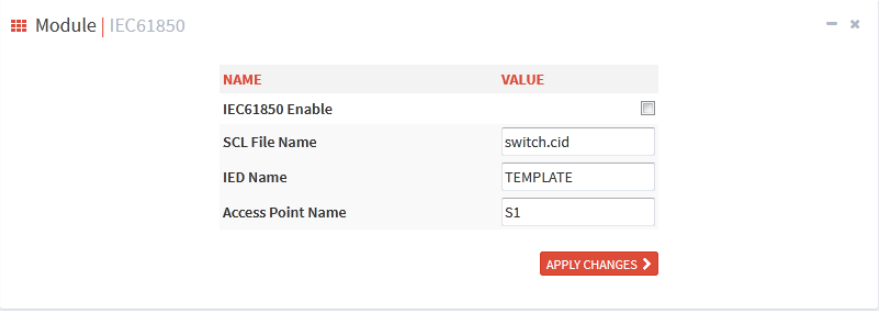

Рис. 8.11. Страница конфигурации IEC 61850.

Описание параметров конфигурации IEC 61850 приведено в Таблица 8.8.

Таблица 8.8. Параметры конфигурации IEC 61850.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
IEC61850 Enable	Включение или отключение IEC61850	enable/disable	disable
SCL File Name	Нужно указать файл конфигурации, который вступит в силу при включении функции IEC61850.	1…25 символа	switch.cid
IED Name	Настройка имени логического устройства для данного IED в соответствии с именем, указанным в файле конфигурации.	1…25 символа	TEMPLATE
Access Point Name	Настройка имени точки доступа для данного IED в соответствии с именем, указанным в файле конфигурации.	1…25 символа	S1

8.7. SNMPv2c

8.7.1. Реализация SNMP

Простой Протокол Управления Сетью (Simple Network Management Protocol – SNMP) – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. С помощью функций SNMP администратор может запрашивать информацию об устройствах в сети, изменять их настройки, просматривать состояние устройств, а также обнаруживать неисправности в сети.

SNMP предполагает два типа сетевых элементов: управляющая станция и агент.

Станция управления сетью (Network Management Station – NMS) – это станция, на которой запущено приложение управления SNMP-сетью. Управляющая станция является центром управления SNMP-сетью.

Агентом называется процесс в управляемом сетевом устройстве. Агент получает и обрабатывает пакеты с запросами от NMS. Когда возникает аварийная ситуация, агент автоматически сообщает об этом NMS.

SNMP включает в себя следующие основные операции:

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

NMS отправляет агентам пакеты Get-Request, Get-Next-Request и Set-Request для опроса состояния, конфигурации устройств и управления параметрами. После получения таких запросов, агенты отвечают пакетами Get-Response. Когда возникает аварийная ситуация, агент автоматически сообщает об этом NMS при помощи сообщения Trap (сообщение о прерывании).

Данная серия коммутаторов NXI-3030RB с функцией RedBox поддерживает версию протокола SNMPv2c (совместим с SNMPv1) и SNMPv3. SNMPv1 использует имена сообществ для проверки подлинности. Имя сообщества выступает в роли пароля, ограничивающего доступ NMS к агентам. Если коммутатор не распознает имя сообщества в составе SNMP-пакета, то такой пакет отбрасывается. SNMPv2c также использует имя сообщества для аутентификации. Для установления связи между NMS и агентом необходимо, чтобы их версии SNMP соответствовали. На агенте может быть включено несколько версий SNMP, чтобы агент мог использовать их для взаимодействия с различными NMS.

8.7.2. Информационная база управления (MIB)

Любой управляемый ресурс называется управляемым объектом. Информационная база управления (Management Information Base – MIB) содержит данные об управляемых объектах. Она определяет иерархию управляемых объектов и атрибутов объектов, таких как имена, разрешения доступа и типы данных. У каждого агента есть своя собственная база MIB. NMS имеет доступ к чтению/записи в базу MIB в соответствии с разрешениями. Взаимоотношения между NMS, агентом и MIB показаны на Рис. 8.12.

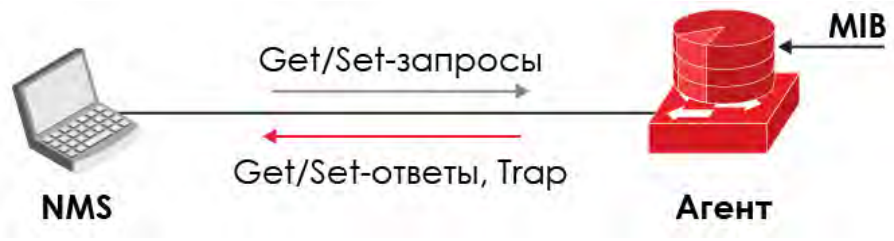

Рис. 8.12. Взаимоотношения между NMS, агентом и MIB.

MIB имеет древовидную структуру. Узлами дерева являются управляемые объекты. У каждого узла есть уникальный идентификатор объекта (Object Identifier – OID), который обозначает расположение узла в структуре MIB. Как показано на Рис. 8.13, OID объекта A – это 1.2.1.1.

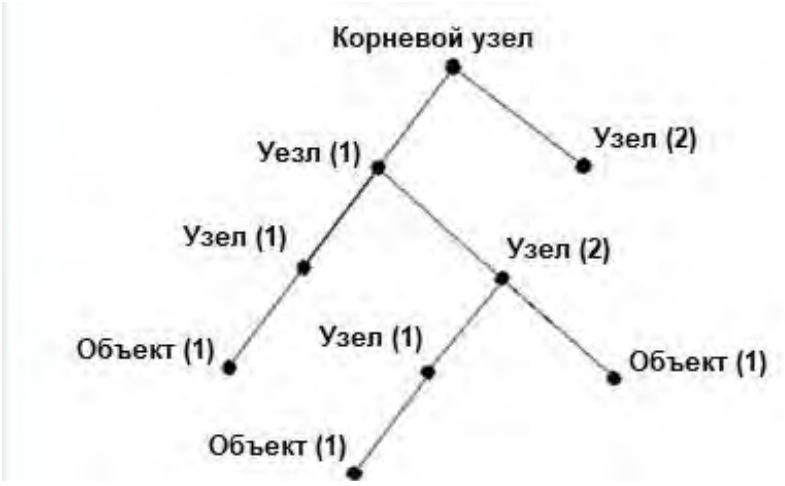

Рис. 8.13. Структура MIB.

8.7.3. Конфигурация SNMP

Для включения и конфигурации SNMP выберите в меню навигации пункт [Other Configurations] → [Snmp]. Страница включения SNMP показана на Рис. 8.14.

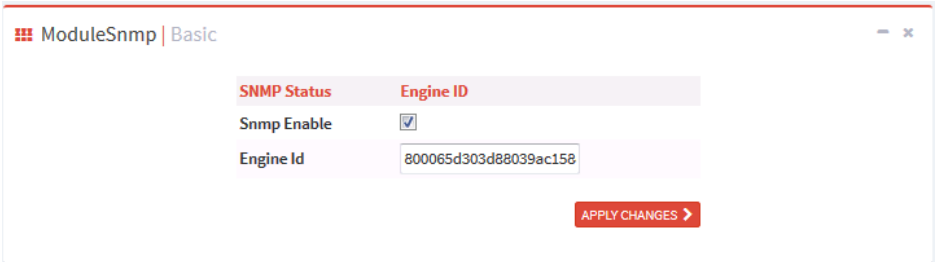

Рис. 8.14. Страница включения SNMP.

Описание параметров включения SNMP приведено в Таблица 8.9.

Таблица 8.9. Параметры включения SNMP.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
SNMP Enable	Включение или отключение SNMP	enable/disable	enable
Engine ID	Настройка идентификатора устройства SNMPv3. Когда идентификатор устройства изменяется, пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.	Четное количество (в диапазоне 10…64) шестнадцатеричных чисел. Не может состоять только из 0 или только из F	

Страница конфигурации имени сообщества показана на Рис. 8.15.

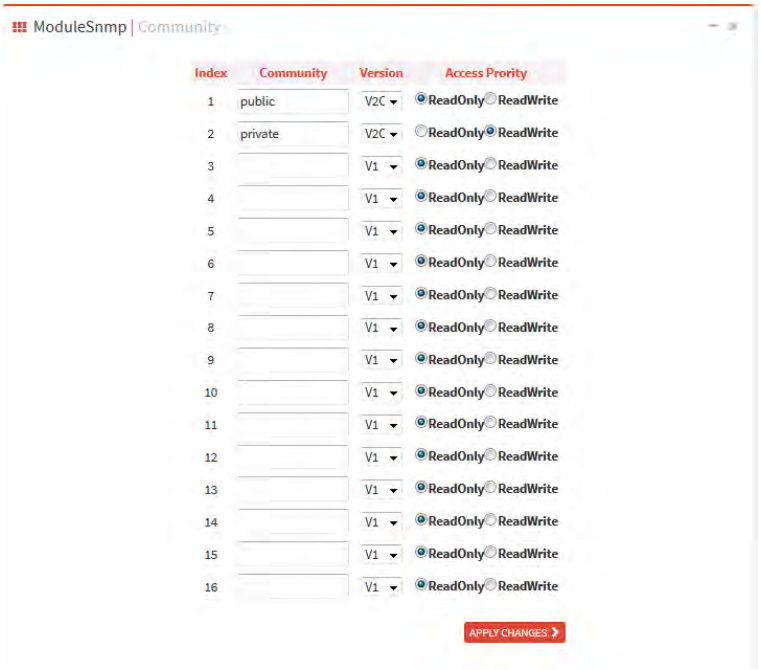

Рис. 8.15. Страница конфигурации имени сообщества.

Описание параметров конфигурации имени сообщества приведено в Таблица 8.10.

Таблица 8.10. Параметры конфигурации имени сообщества.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Community	Настройка имени сообщества коммутатора. MIB-информация коммутатора доступна для чтения и записи, только если переданное в SNMP-пакете имя сообщества совпадает с именем, заданным в коммутаторе. Можно настроить до 16 строк сообщества.	1…32 символа	
Version	Выбор версии протокола SNMP.	V1/V2C	
Access Prority	Выбор режима доступа к MIB-информации. Режим ReadOnly позволяет только читать MIB-информацию; режим ReadWrite позволяет читать и записывать MIB-информацию.	Readonly/ReadWrite	Readonly

Страница конфигурации отправки сообщения Trap показана на Рис. 8.16.

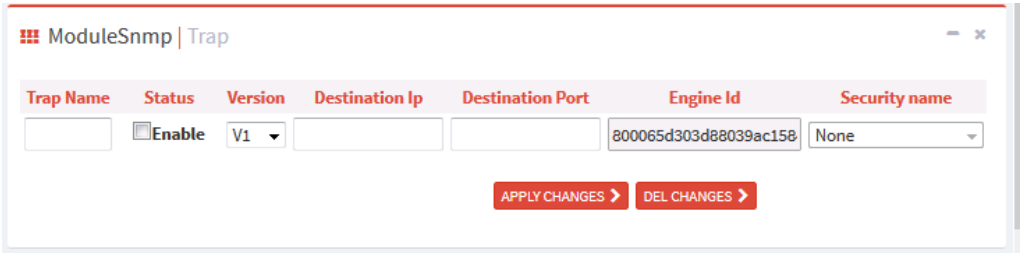

Рис. 8.16. Страница конфигурации отправки сообщения Trap.

Описание параметров конфигурации отправки сообщения Trap приведено в Таблица 8.11

.

Таблица 8.11. Параметры конфигурации отправки сообщения Trap.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Trap name	Настройка имени сообщения Trap.	1…32 символа	
Status	Включение или отключение отправки коммутатором сообщений Trap.	enable/disable	disable
Version	Выбор версии сообщения Trap, отправляемого коммутатором на сервер.	SNMP v1/ SNMP v2c/ SNMP v3	SNMP v1
Destination IP	Настройка адреса сервера для получения сообщений Trap.	A.B.C.D	
Destination Port	Настройка номера UDP-порта назначения для сообщений Trap.	1…65535	162

8.7.4. Стандартный пример конфигурации SNMP

Сервер управления SNMP соединен с коммутатором через Ethernet. IP-адрес сервера управления 192.168.0.23, а коммутатора 192.168.0.2. NMS отслеживает и управляет Агентом через SNMPv2c, и осуществляет чтение и запись информации узла MIB-Агента. При возникновении неисправностей у Агента он упреждающе отправляет сообщение Trap станции NMS. Пример стандартной конфигурации SNMPv2c приведен на Рис. 8.17.

Рис. 8.17. Пример конфигурации SNMPv2c.

Конфигурация агента:

Включить SNMP и версию v2c, как показано на Рис. 8.14; настроить права доступа для сообщества с доступом только для чтения с названием «public» и сообщества с доступом для чтения/записи с названием «private», как показано на Рис. 8.15.

Глобально включить отправку сообщений Trap; создать запись Trap111, сделать ее активной; установить версию Trap SNMPv2c, IP-адрес назначения 192.168.0.23, для остальных параметров применить значения по умолчанию, как показано на Рис. 8.16.

Для контроля и управления устройствами Агента требуется запустить соответствующее управляющее ПО в NMS, например, FlexGain View, разработанное НАТЕКС.

8.8. SNMP v3

8.8.1. Реализация SNMPv3

SNMPv3 предоставляет механизм аутентификации USM (модель обеспечения защиты на уровне пользователей) и позволяет настроить функции аутентификации и шифрования. Аутентификация используется для верификации действительности отправителя пакета, предотвращая доступ для недоверенных пользователей. С помощью же шифрования можно предотвратить перехват данных между системой управления и Агентом. Функции аутентификации и шифрования помогают повысить безопасность взаимодействия между SNMP NMS и SNMP-агентом.

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

SNMPv3 предоставляет четыре таблицы конфигурации. Эти таблицы определяют, имеет ли конкретный пользователь доступ к конкретной MIB-информации:

- в таблице пользователей создаются записи о пользователях. Каждый пользователь использует разные политики безопасности для аутентификации и шифрования;
- таблица групп представляет собой записи о совокупности нескольких пользователей. В таблице групп права доступа пользователя определяются на основе его принадлежности к заданной группе. Все пользователи в одной группе имеют одинаковые права доступа;
- таблица представлений определяет информацию MIB, к которой есть доступ у пользователей. Представление MIB может включать (запись типа include) в себя все узлы конкретного поддерева MIB (то есть пользователям разрешен доступ ко всем узлам поддерева MIB) или исключать (запись типа exclude) все узлы конкретного поддерева MIB (то есть пользователям не разрешен доступ ни к одному узлу данного поддерева MIB);
- в таблице доступа можно определить права доступа MIB по названию группы, названию контекста, модели обеспечения безопасности и уровню безопасности.

8.8.2. Конфигурация SNMPv3

Для включения и конфигурации SNMPv3 выберите в меню навигации пункт [Other Configurations] → [Snmp]. Страница включения SNMP показана на Рис. 8.18.

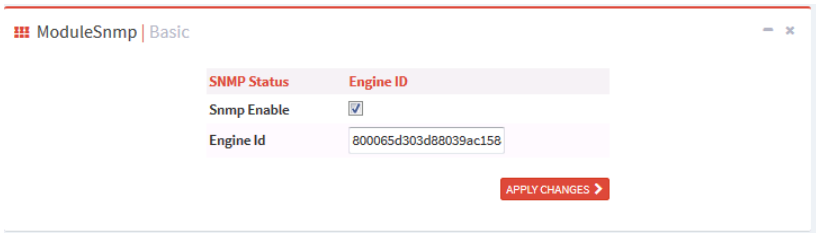

Рис. 8.18. Страница включения SNMP.

Описание параметров включения SNMP приведено в Таблица 8.9.

Таблица 8.12. Параметры включения SNMP.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
SNMP Enable	Включение или отключение SNMP	enable/disable	enable
Engine ID	Настройка идентификатора устройства SNMPv3. Когда идентификатор устройства изменяется, пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.	Четное количество (в диапазоне 10…64) шестнадцатеричных чисел. Не может состоять только из 0 или только из F	

Страница конфигурации отправки сообщения Trap показана на Рис. 8.19.

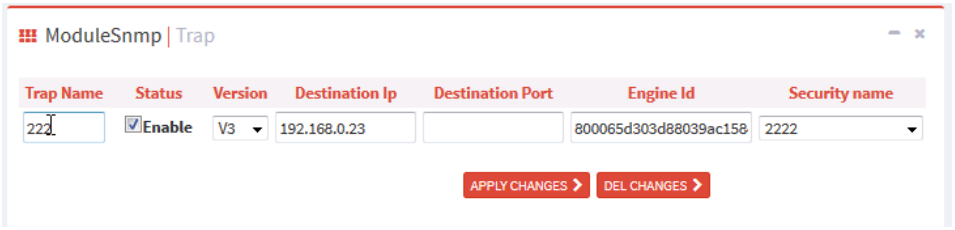

Рис. 8.19. Страница конфигурации отправки сообщения Trap.

Описание параметров конфигурации отправки сообщения Trap приведено в Таблица 8.13.

Таблица 8.13. Параметры конфигурации отправки сообщения Trap.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Trap name	Настройка имени сообщения Trap.	1…32 символа	
Status	Включение или отключение отправки коммутатором сообщений Trap.	enable/disable	disable
Version	Выбор версии сообщения Trap, отправляемого коммутатором на сервер.	SNMP v1/SNMP v2c/SNMP v3	SNMP v1
Destination IP	Настройка адреса сервера для получения сообщений Trap.	A.B.C.D	
Destination Port	Настройка номера порта для отправки сообщений Trap.	1…65535	162

Страница конфигурации таблицы пользователей SNMPv3 показана на Рис. 8.20.

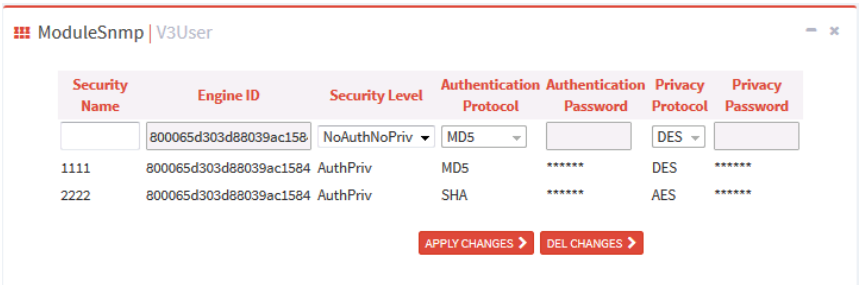

Рис. 8.20. Страница конфигурации таблицы пользователей SNMPv3.

Описание параметров конфигурации таблицы пользователей SNMPv3 приведено в Таблица 8.14.

Таблица 8.14. Параметры конфигурации таблицы пользователей SNMPv3.

Параметр	*Функция*	*Значение*
Security Name	Настройка имени пользователя	1…32 символа
Engine ID	Настройка идентификатора устройства SNMPv3 в сообщении Trap.	Четное количество (в диапазоне 10…64) шестнадцатеричных чисел. Не может состоять только из 0 или только из F
Security Level	Настройка уровня безопасности текущего пользователя. NoAuthNoPriv – не требуется ни аутентификации, ни шифрования; AuthNoPriv – требуется аутентификации, но не требуется шифрование; AuthPriv – требуется как аутентификации, так и шифрование.	NoAuthNoPriv/ AuthNoPriv/ AuthPriv
Authentication Protocol	Выбор протокола аутентификации. Настраивается, если выбраны значения AuthNoPriv / AuthPriv в параметре Security Level.	MD5/SHA
Authentication password	Настройка пароля аутентификациии. Настраивается, если выбраны значения AuthNoPriv / AuthPriv в параметре Security Level.	8…40 символов (MD5 protocol)/ 8…32 символов (SHA protocol)
Privacy Protocol	Выбор протокола шифрования. Настраивается, если выбрано значение AuthPriv в параметре Security Level.	DES/AES
Privacy Password	Настройка пароля шифрования. Настраивается, если выбрано значение AuthPriv в параметре Security Level.	8…32 символов

Страница конфигурации таблицы групп SNMPv3 показана на Рис. 8.21.

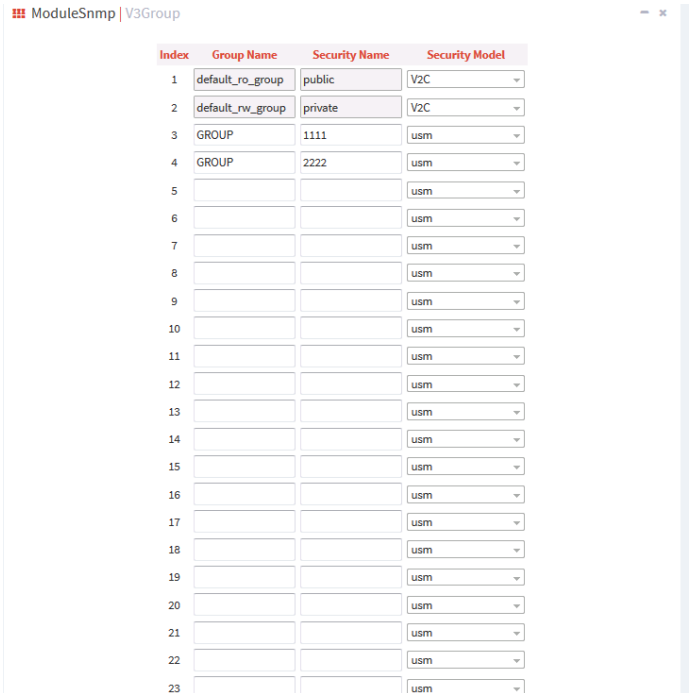

Рис. 8.21. Конфигурация таблицы групп SNMPv3.

Описание параметров конфигурации таблицы групп SNMPv3 приведено в Таблица 8.15.

Таблица 8.15. Параметры конфигурации таблицы групп SNMPv3.

Параметр	*Функция*	*Значение*
Group Name	Настройка имени группы. Пользователи с одинаковым именем группы имеют одинаковые права доступа SNMP. Можно настроить до 32 групп.	1…32 символа
Security Name	Настройка имени безопасности. Имя безопасности должно соответствовать имени пользователя в таблице пользователей.	1…32 символа
Security model	Выбор модели безопасности текущей группы (номер версии SNMP). SNMPv3 использует технологию USM (модель обеспечения защиты на уровне пользователей), принудительно используется модель SNMPv3.	SNMPv3

Страница конфигурации таблицы представлений показана на Рис. 8.22.

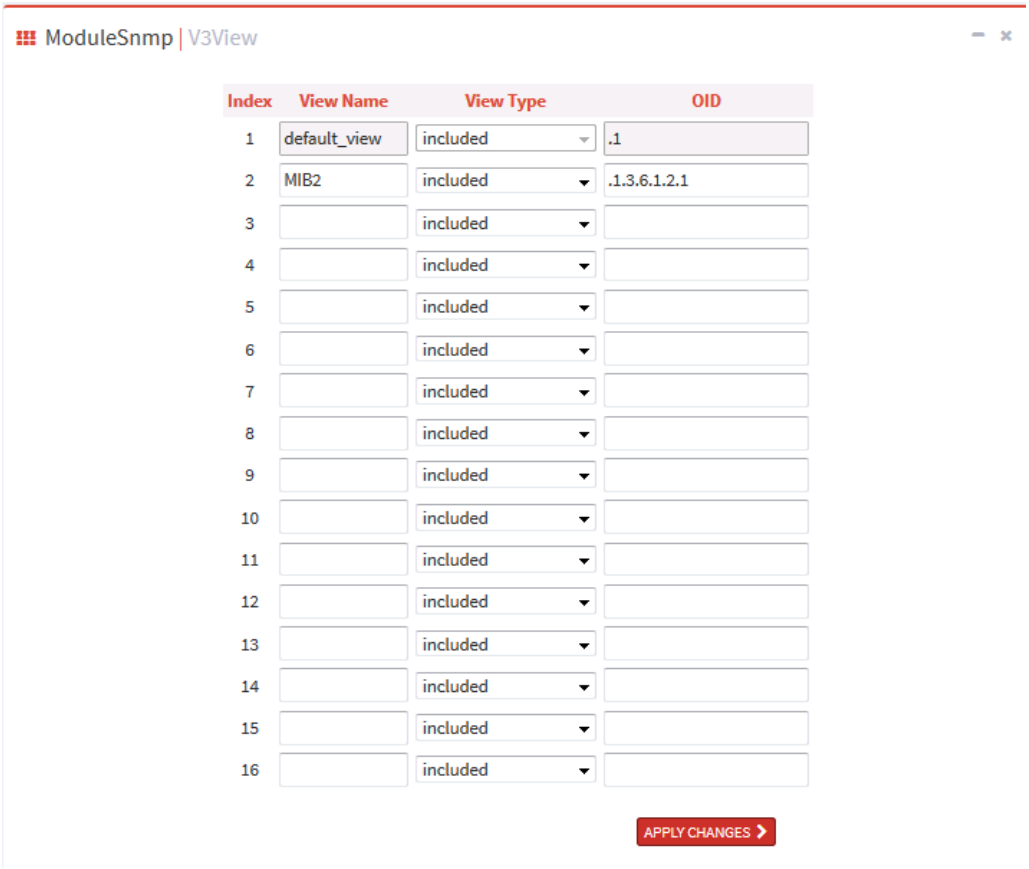

Рис. 8.22. Конфигурация таблицы представлений SNMPv3.

Описание параметров конфигурации таблицы представлений SNMPv3 приведено в Таблица 8.16.

Таблица 8.16. Параметры конфигурации таблицы представлений.

Параметр	*Функция*	*Значение*
View Name	Настройка имени представления	1…32 символа
View Type	Included означает, что текущее представление включает в себя все узлы заданного поддерева MIB. Excluded означает, что текущее представление исключает все узлы дерева MIB.	included/excluded
OID	Настройка поддерева MIB, обозначенное OID корневого узла поддерева. Может быть сконфигурировано до 16 представлений. По умолчанию на коммутаторе имеется представление default_view, включающее в себя все узлы поддерева 1.	

Страница конфигурации таблицы доступа SNMPv3 показана на Рис. 8.23.

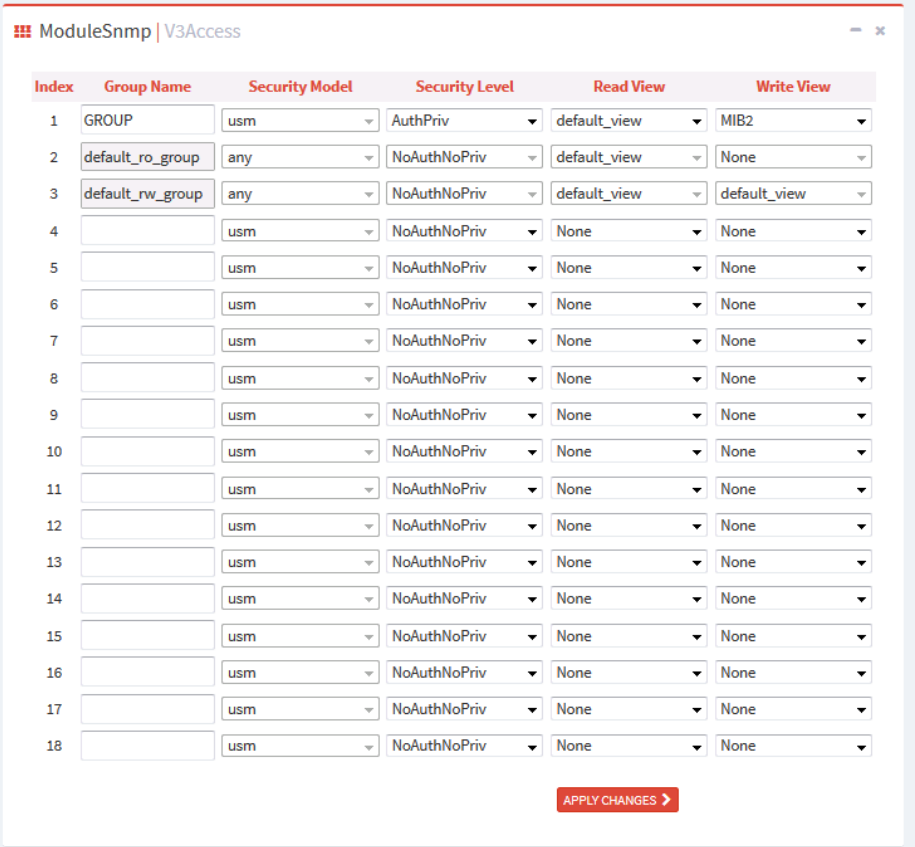

Рис. 8.23. Конфигурация таблицы доступа SNMPv3.

Описание параметров конфигурации таблицы доступа SNMPv3 приведено в Таблица 8.17.

Таблица 8.17. Параметры конфигурации таблицы доступа SNMPv3.

Параметр	*Функция*	*Значение*
Group Name	Выбор группы для настройки режима доступа. Все пользователи в группе имеют одинаковые права доступа.	Все созданные имена групп (1…32 символа)
Security Model	Настройка модели безопасности (номер версии SNMP), применяемой, когда текущая группа обращается к коммутатору. USM применяет модель обеспечения защиты на уровне пользователей (SNMPv3). Значение any обозначает, что может применяться любая модель безопасности. Имя группы и модель безопасности в таблице доступа должны совпадать с этими параметрами в таблице групп.	any/v1/v2/usm
Security Level	Настройка уровня безопасности текущего пользователя. NoAuthNoPriv – не требуется ни аутентификации, ни	NoAuthNoPriv/ AuthNoPriv/AuthPriv

	шифрования; AuthNoPriv – требуется аутентификации, но не требуется шифрование; AuthPriv – требуется как аутентификации, так и шифрование. Уровни безопасности в порядке возрастания: NoAuthNoPriv; AuthNoPriv; AuthPriv. Данные с более низким уровнем безопасности доступны для более высокого уровня безопасности. Например, если и протокол авторизации/шифрования, и пароль авторизации/шифрования введены правильно, уровень безопасности, сконфигурированный как AuthNoPriv, доступен для уровня безопасности AuthNoPriv и AuthPriv, но недоступен для уровня безопасности NoAuthNoPriv.	
Read View	Выбор имени представления, доступного только для чтения (ReadOnly).	default_view/None/ все созданные имена представлений
Write View	Выбор имени представления, доступного для записи (ReadWrite).	default_view/None/ все созданные имена представлений.

По умолчанию на коммутаторе имеются следующие таблицы доступа: {default_ro_group, any, NoAuthNoPriv, default_view, None} и {default_rw_group, any, NoAuthNoPriv, default_view, default_view}. Всего можно сконфигурировать до 16 таблиц доступа.

8.8.3. Стандартный пример конфигурации SNMPv3

Сервер управления SNMP подключен к коммутатору через Ethernet. IP-адрес сервера управления 192.168.0.23, а адрес коммутатора 192.168.0.2. Пользователь «1111» и пользователь «2222» управляют Агентом по SNMPv3. Уровень безопасности настроен как AuthNoPriv. Пользователь может выполнять только операцию чтения для всей информации узла Агента. При возникновении аварийного сигнала Агент упреждающе отправляет сообщение Trap версии 3 в NMS. Схема стандартного примера конфигурации SNMPv3 показана на Рис. 8.24.

Рис. 8.24. Пример конфигурации SNMPv3.

Настройка агента:

- Включить SNMPv3, как показано на Рис. 8.18.
- Настроить таблицу пользователей SNMPv3, как показано на Рис. 8.20:
- установить имя пользователя «1111», уровень безопасности AuthPriv, протокол аутентификации MD5, пароль аутентификации «aaaaaaaa», протокол конфиденциальности DES и пароль конфиденциальности «xxxxxxxx».
- задать имя другого пользователя как «2222», уровень безопасности AuthPriv, протокол аутентификации SHA, пароль аутентификации «bbbbbbbb», протокол конфиденциальности AES и пароль конфиденциальности «yyyyyyyy».
- Создать группу, установить модель безопасности usm, и добавить пользователя «1111» и пользователя «2222» к группе, как показано на Рис. 8.21.
- Настроить таблицу доступа SNMPv3. Задать имя группы «group», модель безопасности usm, уровень безопасности AuthPriv, параметр Read View установить default_view, параметр Write View установить None, как показано на Рис. 8.23.
- ВключитьTrap, как показано на Рис. 8.19.
- Создать запись Trap «222», активировать ее; установить версию Trap SNMPv3,
- IP-адрес назначения 192.168.0.23. Выбрать все события прерывания для системы, интерфейса, авторизации и коммутатора, а для остальных параметров применить значения по умолчанию, как показано на Рис. 8.19.
- Для контроля и управления устройствами агента требуется запустить соответствующее управляющее ПО в NMS.

8.9. Файловый сервер

Служба передачи файлов может осуществлять резервное копирование файлов конфигурации. При изменении конфигурации коммутатора NXI-3030RB файл резервной копии может быть загружен с сервера посредством протоколов передачи файлов FTP / SFTP. Таким образом требуемая конфигурация может быть легко восстановлена.

Коммутатор с функцией RedBox может использоваться как клиент для выгрузки файлов по протоколам FTP / SFTP.

8.9.1. FTP-клиент

Перед использованием коммутатора как FTP-клиента нужно установить FTP-сервер. В качестве примера конфигурации FTP-сервера и процесса загрузки прошивки будет использоваться программное обеспечение WFTPD.

Выберите меню [Security] → [Users/Rights], откроется диалоговое окно «Users/Rights Security Dialog». Нажмите кнопку <New User>, чтобы создать нового пользователя FTP. Задайте имя пользователя (User Name) и пароль (Password), например, имя пользователя «admin» и пароль «123», нажмите кнопку <OK>. Процесс создания нового пользователя FTP показана Рис. 8.25.

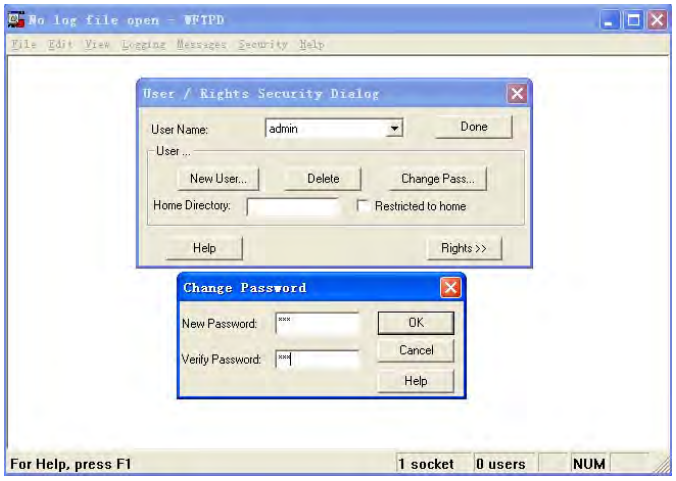

Рис. 8.25. Создание нового пользователя FTP.

Введите путь хранения файла в поле Home Directory, как показано на Рис. 8.26, и нажмите кнопку <Done>.

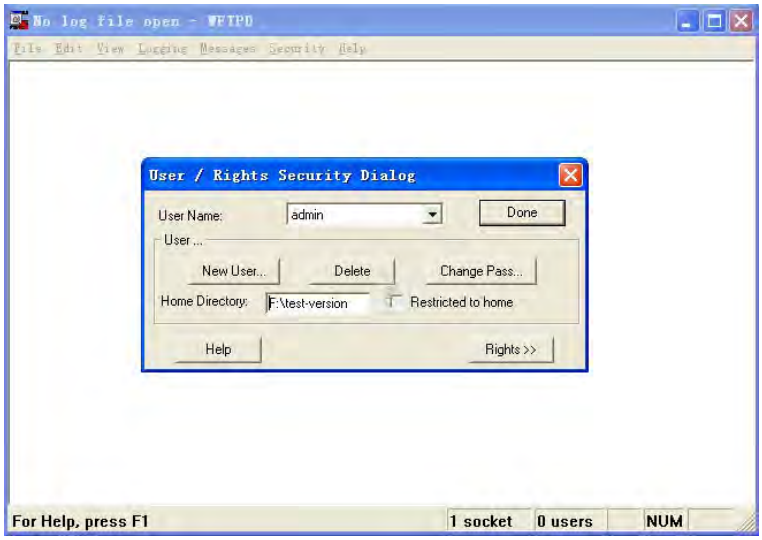

Рис. 8.26. Выбор пути хранения файла.

Для перехода на страницу конфигурации сервиса передачи файлов выберите в меню навигации пункт [Other Configurations] → [File Server]. Страница конфигурации сервиса передачи файлов показана на Рис. 8.27.

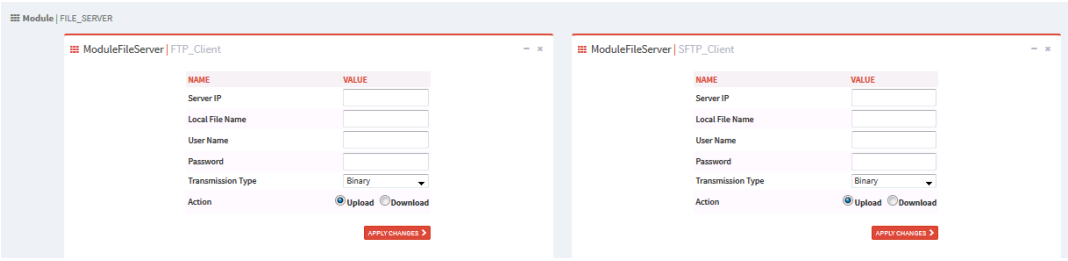

Рис. 8.27. Страница конфигурации сервиса передачи файлов.

Можно выбрать протокол FTP или SFTP. На Рис. 8.28 представлен пример конфигурации в качестве FTP-клиента.

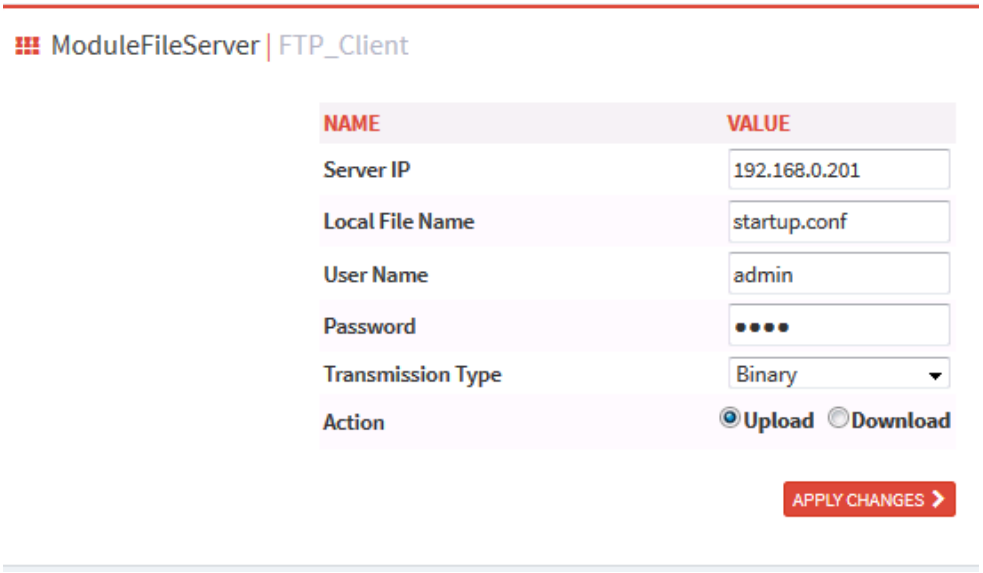

Рис. 8.28. Конфигурация FTP-клиента.

Описание параметров конфигурации в качестве FTP-клиента приведено в Таблица 8.18.

Таблица 8.18. Параметры конфигурации FTP-клиента.

Параметр	*Функция*	*Значение*
Server IP	Введите IP-адрес FTP-сервера	A.B.C.D
Server File Name	Укажите название файла на FTP-сервере	1…100 символов
User Name	Введите имя пользователя на FTP-сервере	
Password	Введите пароль пользователя	
Transmission Type	Выберите стандарт передачи файлов. Конфигурация по умолчанию: binary	binary/ascii
Action	update: выгрузите файл конфигурации коммутатора на удаленный FTP-сервер. download: загрузить файл конфигурации с удаленного FTP-сервера на коммутатор	update/download

8.9.2. SFTP-клиент

Протокол безопасной передачи файлов (SFTP) представляет собой протокол передачи данных на основе SSH. Он обеспечивает зашифрованную передачу файлов для обеспечения безопасности.

Ниже показан пример использования программы MSFTP для описания конфигурации SFTP-сервера и процесса загрузки программного обеспечения.

Добавьте пользователя SFTP, как показано на Рис. 8.29. Далее введите имя пользователя (User) и пароль (Password), например, «admin» и «123»; установите номер порта «22»; введите путь для файла прошивки в поле Root path.

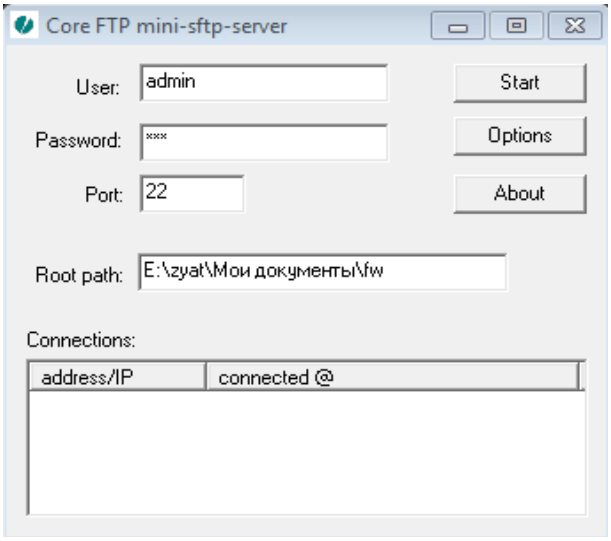

Рис. 8.29. Добавление пользователя SFTP.

Для перехода на страницу конфигурации сервиса передачи файлов выберите в меню навигации пункт [Other Configurations] → [File Server]. Страница конфигурации сервиса передачи файлов показана на Рис. 8.30.

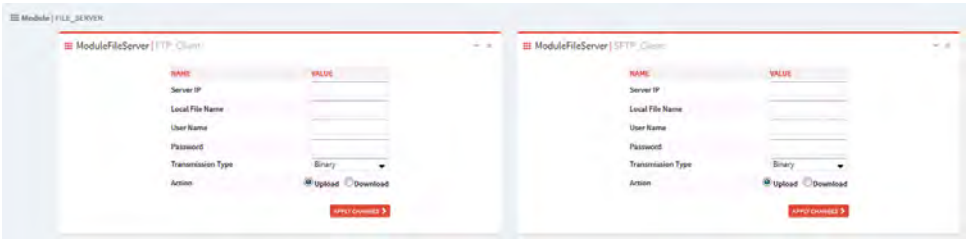

Рис. 8.30. Конфигурация сервиса передачи файлов.

Можно выбрать протокол FTP или SFTP. На Рис. 8.31 представлен пример конфигурации в качестве SFTP-клиента.

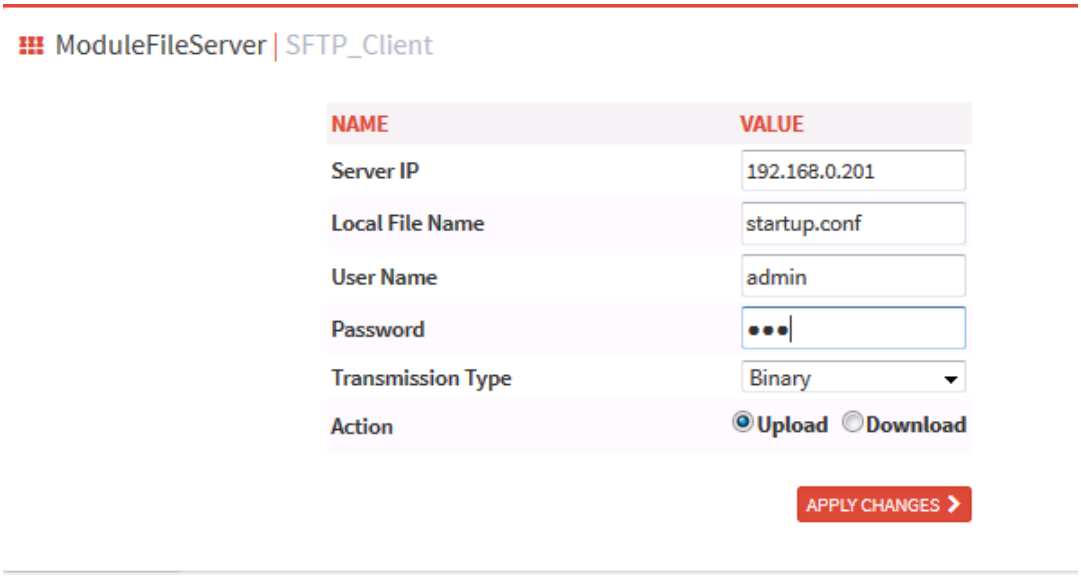

Рис. 8.31. Конфигурация SFTP-клиента.

Описание параметров конфигурации в качестве SFTP-клиента приведено в Таблица 8.19.

Таблица 8.19. Параметры конфигурации SFTP-клиента.

Параметр	*Функция*	*Значение*
Server IP	Введите IP-адрес SFTP-сервера	A.B.C.D
Local File Name	Укажите название файла на коммутаторе	1…100 символов
User Name	Введите имя пользователя на SFTP-сервере	
Password	Введите пароль пользователя	
Transmission Type	Выберите стандарт передачи файлов. Конфигурация по умолчанию: binary	binary/ascii
Action	update: выгрузите файл конфигурации коммутатора на удаленный SFTP-сервер. download: загрузить файл конфигурации с удаленного SFTP-сервера на коммутатор	update/download

8.10. LLDP

Протокол обнаружения канального уровня (Link Layer Discovery Protocol – LLDP) предоставляет стандартный механизм обнаружения соседних устройств на канальном уровне. Информация об устройстве – такая как характеристики, административные адреса, идентификатор устройства, и идентификатор интерфейса – передается в блоке данных протокола обнаружения канального уровня (Link Layer Discovery Protocol Data Unit – LLDPDU), который передается соседним устройствам, подключенным напрямую. После получения LLDPDU соседние устройства сохраняют эту информацию у себя в оперативной памяти. Такие данные можно получить посредством интерфейса управления устройствами, а также с помощью SNMP для построения в автоматическом режиме карты сети.

8.10.1. Конфигурация LLDP

Для конфигурации LLDP выберите в меню навигации пункт [Other Configurations] → [LLDP]. Страница конфигурации LLDP показана на Рис. 8.32.

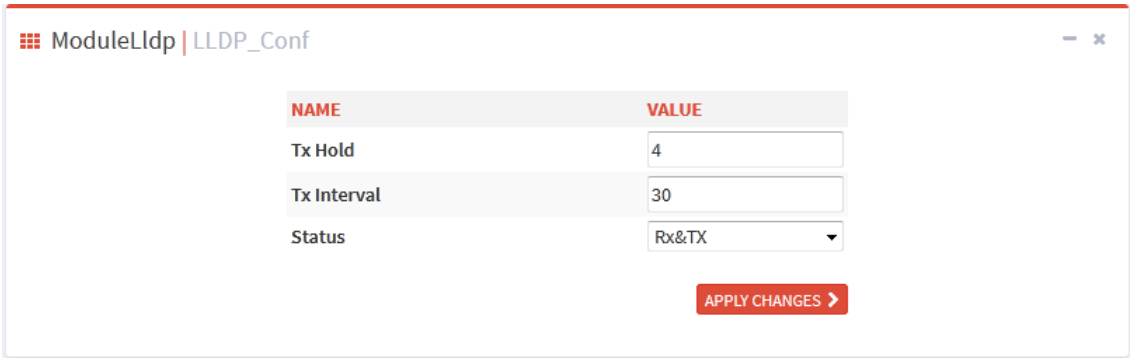

Рис. 8.32. Страница конфигурации LLDP.

Описание параметров конфигурации LLDP приведено в Таблица 8.20.

Таблица 8.20. Параметры конфигурации LLDP.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Tx Hold	Настройка числа периодов удержания Tx hold. Эффективная длительность кадра LLDP = Tx Interval * Tx Hold.	2…10 раз	4 раза
Tx Interval	Конфигурация интервала времени для отправки кадров LLDP.	5…32768 сек	30 сек
Status	Статус кадров LLDP на портах. Rx&Tx – коммутатор может отправлять кадры LLDP, а также принимать и идентифицировать кадры LLDP; Disable – коммутатор не отправляет и не получает кадры LLDP; RxOnly – коммутатор только принимает и идентифицирует кадры LLDP; TxOnly – коммутатор только отправляет кадры LLDP.	Rx&Tx/Disable/RxOnly/TxOnly	Rx&Tx

Страница просмотра информации LLDP показана на Рис. 8.33. Для отображения информации LLDP о соседнем устройстве необходимо, чтобы LLDP был включен на соответствующих соседних устройствах.

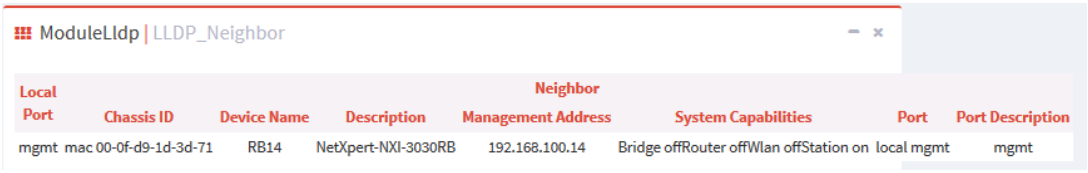

Рис. 8.33. Информация LLDP.

8.11. DDM

DDM (Digital Diagnostic Monitor) – функция цифрового контроля параметров производительности SFP-трансивера. За выполнение данного функционала отвечает интеллектуальный интерфейс оптического модуля с добавлением микросхемы и вспомогательной схемы DDMI (Digital Diagnostic Monitor Interface optical module). Интерфейс DDM может считывать температуру модуля трансивера, напряжение, ток смещения и мощность лазера (Tx) и уровень принимаемого сигнала (Rx) в режиме реального времени. Контроль данных параметров помогает выявить неисправность и определить место неисправности в волоконно-оптическом канале, упростить работы по техническому обслуживанию и повысить надежность системы.

8.11.1. Конфигурация DDMI

Для конфигурации интерфейса DDM выберите в меню навигации пункт [Other Configurations] → [DDMI]. Страница примера конфигурации DDMI для порта L показана на Рис. 8.34. После установки оптического модуля возможно посмотреть основную информацию об оптическом модуле, включающую в себя информацию о вендоре, модели, серийном номере, версии, расстоянии передачи и трансивере. Некоторые сменные оптические модули могут предоставлять расширенную информацию, включающую в себя информацию о температуре, напряжении, входящей и исходящей мощностях.

Рис. 8.34. Страница DDMI для порта L.

8.12. Виртуальный тест кабеля

Виртуальный тестер кабеля VCT (Virtual Cable Tester) использует рефлектометр для кабельных линий TDR (Time Domain Reflectometry) для определения состояния витой пары. В проверяемый кабель передаются короткие электрические импульсы и измеряется отраженный обратный сигнал для обнаружения неисправности кабеля. Если в кабеле есть повреждения, то энергия импульса будет частично или полностью отражена обратно к отправляющему источнику. Когда переданный импульс достигнет конца кабеля или точки повреждения, VCT может измерить время прибытия импульса в место повреждения и время возврата к отправителю, а затем вычислить расстояние.

VCT может выводить следующие результаты теста кабеля:

- Short – короткое замыкание; закорочены два или более проводов.
- Open – обрыв цепи; на кабеле могут быть оборванные провода.
- Normal – нормальное кабельное соединение.
- Imped – несоответствие импеданса; например, импеданс кабеля категории 5 (Cat.5) составляет 100 Ом, полное сопротивление на обоих концах кабеля должно быть 100 Ом, чтобы избежать отражения волн и ошибок данных.
- Fail – не удалось выполнить тест кабеля.

8.12.1. Конфигурация VCT

Для использования виртуального тестера кабеля VCT выберите в меню навигации пункт [Other Configurations] → [Virtual Cable Test]. Страница конфигурации виртуального тестера кабеля VCT показана на Рис. 8.35.

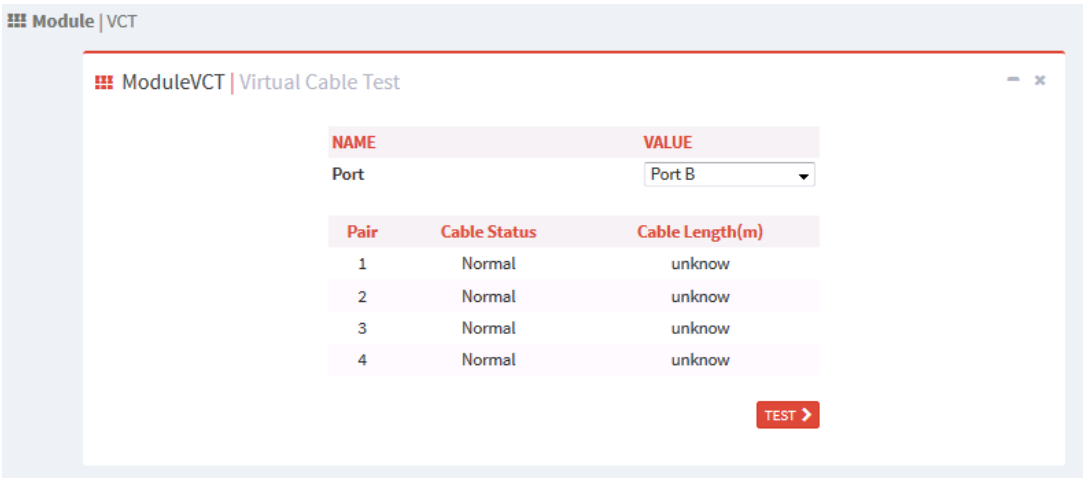

Рис. 8.35. Виртуальный тестер кабеля VCT.

Описание параметров конфигурации VCT приведено в Таблица 8.21.

Таблица 8.21. Параметры VCT.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Port	Выбор соответствующего порта для проверки кабеля. После выбора порта нажмите кнопку <TEST>, чтобы проверить подключение кабеля.	port_a/port_b/port_interlink	port_a
Pair	Номер витой пары кабеля	1–4	
Cable Status	Состояние кабеля. Normal – нормальное кабельное соединение; Open – возможен обрыв кабеля; Short – закорочены два или более провода.	Normal/Open/Short	
Cable Length (m)	Приблизительное расстояние точки повреждения от порта коммутатора, единица измерения – метр. Если кабель в норме, длина кабеля отображается как unknown.		

8.13. RADIUS

8.13.1. Общие сведения о RADIUS

RADIUS (Remote Authentication Dial-In User Service – Служба идентификации удаленных пользователей) является протоколом для аутентификации, авторизации и аккаунтинга пользователей, который использует UDP в качестве транспортного протокола.

RADIUS работает в парадигме «клиент-сервер» для реализации связи между сервером сетевого доступа (NAS) и сервером RADIUS. Клиент RADIUS работает на NAS, а учетные данные пользователей хранятся централизованно на RADIUS-сервере. В качестве NAS могут выступать различные устройства сетевой инфраструктуры: коммутаторы, маршрутизаторы, серверы приложений. NAS является сервером для пользователей, но клиентом для RADIUS-сервера. На Рис. 8.36 показан пример сети с RADIUS-сервером.

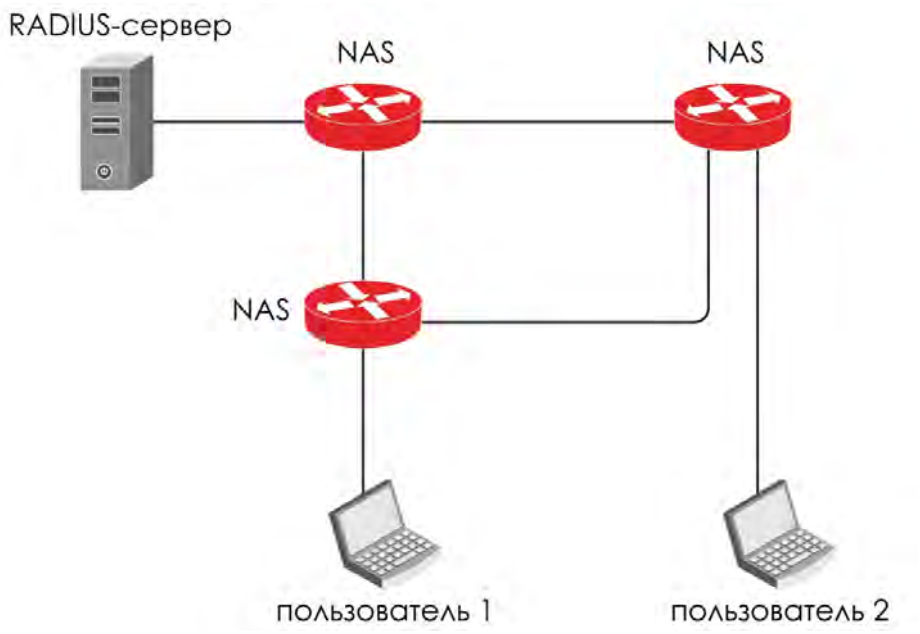

Рис. 8.36. Структура RADIUS.

Протокол авторизует пользователей терминала, которым необходимо подключиться к устройству для выполнения операций. Устройство служит клиентом RADIUS и отправляет информацию о пользователе на сервер RADIUS для аутентификации, и разрешает или не разрешает пользователям доступ к устройству в соответствии с результатами аутентификации.

8.13.2. Конфигурация RADIUS

Для конфигурации RADIUS выберите в меню навигации пункт [Other Configurations] → [Radius]. Страница конфигурации RADIUS показана на Рис. 8.37.

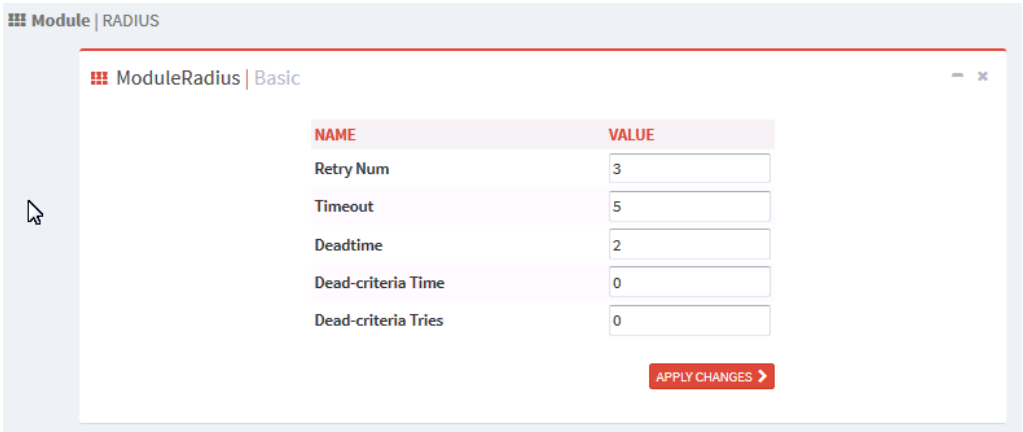

Рис. 8.37. Конфигурация аутентификации RADIUS.

Описание параметров конфигурации RADIUS приведено в Таблица 8.22.

Таблица 8.22. Параметры аутентификации RADIUS.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Retry Num	Настройка максимального числа попыток повторной отправки пакетов запроса RADIUS. Если устройство не получает ответа от сервера RADIUS после максимального числа попыток повторной отправки, аутентификация признается неудавшейся, и устройство будет считать сервер RADIUS недействующим.	1 … 3	3
Timeout	Настройка интервала времени для ответа от сервера RADIUS. После отправки пакета запроса RADIUS, если устройство не получает ответа от сервера RADIUS по истечении указанного периода времени, устройство повторно отправит пакет запроса.	1 … 3 сек	3 сек
Deadtime	Конфигурация периода, когда сервер недействителен. В течение этого периода устройство не отправляет RADIUS-сообщения запроса на сервер. После данного периода времени сервер Radius возвращается в действующее состояние. Это уменьшает количество запросов к недействительному серверу.	1 … 1440 мин	2 мин
Dead-critecria Time	Установка ограничения числа повторов запросов к серверу, чтобы определить, что сервер недействителен.	1 … 100	0

Страница конфигурации сервера RADIUS показана на Рис. 8.38.

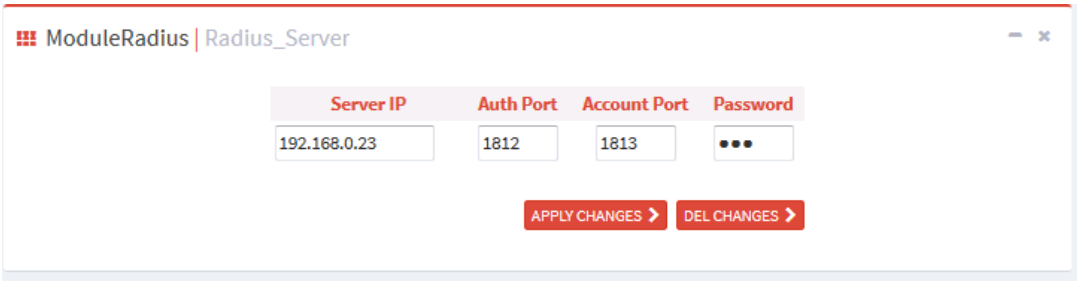

Рис. 8.38. Конфигурация сервера RADIUS.

Описание параметров конфигурации сервера RADIUS приведено в Таблица 8.23.

Таблица 8.23. Параметры конфигурации сервера RADIUS.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Server IP	Настройка IP-адреса сервера RADIUS. Можно настроить до 5 серверов RADIUS	A.B.C.D	
Auth Port	Настройка UDP-порта сервера RADIUS для аутентификации	1…65535	1812
Account Port	Настройка UDP-порта сервера RADIUS для аккаунтинга	1…65535	1813
Password	Настройка пароля сервера RADIUS	1…32 символа	

8.13.3. Стандартный пример конфигурации RADIUS

Топология показана на Рис. 8.39. сервер TACACS+ может осуществлять аутентификацию и авторизацию пользователей при доступе на коммутатор. IP-адрес сервера 192.168.0.23, а общий ключ, который используется при обмене пакетами между сервером и коммутатором, это «aaa».

Рис. 8.39. Пример аутентификации RADIUS.

Конфигурация:

- Настроить IP-адрес сервера как 192.168.0.23 и ключ как «aaa», как показано на Рис. 8.37;
- Настроить порядок авторизации для использования RADIUS для сервиса telnet, как показано на Рис. 8.45 и Рис. 8.46;
- Настроить имя пользователя и пароль на сервере RADIUS как “ccc”, ключ шифрования как “aaa”, как показано на Рис. 8.38;
- С ПК пользователя произвести попытку подключения к коммутатору с помощью telnet, используя логин и пароль “ccc”.

8.14. TACACS+

8.14.1. Общие сведения о TACACS+

Terminal Access Controller Access Control System – система управления доступом для контроллера доступа к терминалу (TACACS+) представляет собой приложение на основе TCP. Протокол работает в парадигме «клиент-сервер» для реализации связи между сервером сетевого доступа (NAS) и сервером TACACS+. Клиент TACACS+ работает на NAS, а учетные данные пользователей хранятся централизованно на TACACS-сервере. В качестве NAS могут выступать различные устройства сетевой инфраструктуры: коммутаторы, маршрутизаторы, серверы приложений. NAS является сервером для пользователей, но клиентом для TACACS-сервера. На Рис. 8.40 показан пример сети с использованием TACACS-сервера.

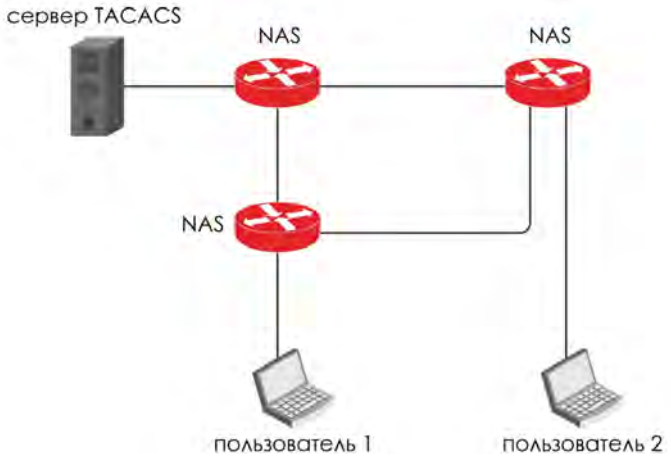

Рис. 8.40. Сеть с использованием TACACS+.

Протокол может осуществлять аутентификацию, авторизацию и аккаунтинг (Authentication Authorization Accounting – AAA) пользователей терминала, которым необходимо подключиться к устройству для выполнения операций. Устройство служит клиентом TACACS+ и отправляет имя пользователя и пароль, полученные от пользователя на сервер TACACS+ для аутентификации. Сервер получает запросы на TCP-соединение от NAS, отвечает на запросы аутентификации и проверяет правомерность действий пользователей. Если пользователь проходит аутентификацию, он может подключиться к устройству для выполнения операций.

Преимуществами протокола TACACS+ являются использование более надежного транспортного протокола TCP вместо UDP, а также возможность использовать шифрование при обмене данными между клиентом и сервером.

8.14.2. Конфигурация TACACS+

Для включения TACACS+ выберите в меню навигации пункт [Other Configurations] → [Tacacs plus]. Страница включения протокола TACACS+ показана на Рис. 8.41.

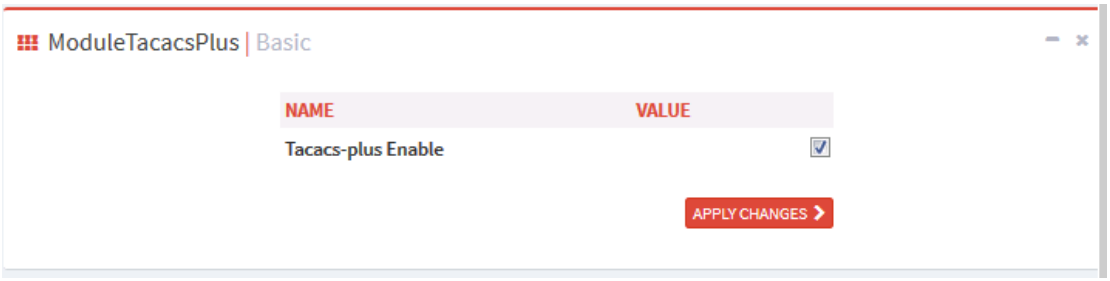

Рис. 8.41. Включение протокола TACACS+.

Описание параметров включения TACACS+ приведено в Таблица 8.24.

Таблица 8.24. Параметры включения TACACS+.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Tacacs-plus Enable	Включение или отключение протокола TACACS+	Enable/disable	Disable

Страница конфигурации сервера TACACS+ показана на Рис. 8.42.

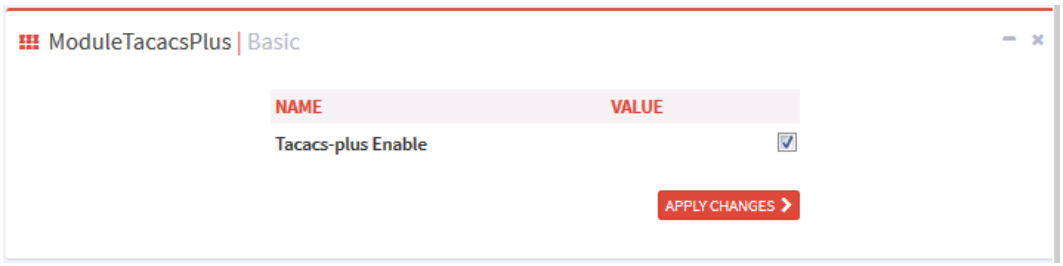

Рис. 8.42. Конфигурация сервера TACACS+.

Описание параметров конфигурации сервера TACACS+ приведено в Таблица 8.25.

Таблица 8.25. Параметры конфигурации сервера TACACS+.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Server	Выбор типа текущей конфигурации	Master server/ Slave server	Master server
IP address	Настройка IP-адреса сервера TACACS+	A.B.C.D	
Port	Настройка UDP-порта назначения сервера TACACS+	1…65535	49
Encrypt	Включение или отключение шифрования. Если включено, необходимо ввести ключ шифрования.	Enable/Disable	Disable
Password	Настройка ключа шифрования. Две стороны совместно используют ключ для проверки подлинности и шифрования пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи одинаковые. Поэтому следует убедиться, что сконфигурированный ключ совпадает с ключом на сервере TACACS+.	1…32 символа	

После завершения конфигурации будет выведена информация о конфигурации серверов TACACS+, как показано на Рис. 8.43.

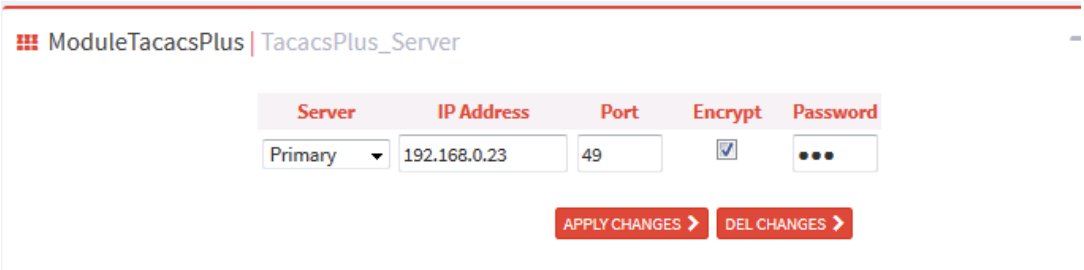

Рис. 8.43. Информация о конфигурации серверов TACACS+.

8.14.3. Стандартный пример конфигурации TACACS+

Как показано на Рис. 8.44, сервер TACACS+ может осуществлять аутентификацию и авторизацию пользователей при доступе на коммутатор. IP-адрес сервера 192.168.0.23, а общий ключ, который используется при обмене пакетами между сервером и коммутатором, это «aaa».

Рис. 8.44. Пример аутентификации TACACS+.

Конфигурация:

- Включить сервис TACACS+ на коммутаторе, как показано на Рис. 8.42;
- Конфигурация сервера TACACS+. Настроить IP-адрес сервера как 192.168.0.23 и ключ как «aaa», как показано на Рис. 8.43;
- При подключении к коммутатору через Web выбрать Tacacs+ в качестве первого метода и Local в качестве второго, как показано на Рис. 8.46;
- Сконфигурировать имя пользователя и пароль «bbb», ключ шифрования «aaa» на сервере TACACS+;
- При подключении к коммутатору через Web ввести имя пользователя и пароль «bbb» чтобы пройти аутентификацию на сервере TACACS+.

8.15. AAA

AAA (Authentication Authorization and Accounting) – это модуль, связанный с обеспечением защиты данных в информационных системах, включая обеспечение аутентификации, авторизации и аккаунтинга.

Аутентификация – это сопоставление учетной записи (пары логин-пароль) с существующей учетной записью в системе безопасности. Аутентификация считается успешной, если такое сопоставление найдено.

Авторизация – это проверка полномочий (просмотр определенных параметров RedBox или изменение определенных настроек) текущей учетной записи, сопоставление запрошенных полномочий с имеющимися в системе безопасности. Авторизация считается успешной, если запрошенные полномочия разрешены в системе безопасности.

Аккаунтинг – это учет действий пользователей, слежение за потреблением ресурсов, записи фактов получения доступа к системе.

AAA может осуществляться на основе локальной базы пользователя – т.е. аккаунтов, сконфигурированных непосредственно на коммутаторе – либо на основе базы пользователей на удаленном сервере. Удаленные серверы, как правило, работают по протоколам RADIUS (см. главу 8.13) либо TACACS+ (см. главу 8.14).

8.15.1. Конфигурация AAA

Для включения AAA выберите в меню навигации пункт [Other Configurations] → [AAA]. Страница включения AAA показана на Рис. 8.45. Глобальное включение AAA только включает AAA, соответствующие службы AAA должны быть настроены. Если отключить AAA, то ранее настроенные службы AAA станут недействительными.

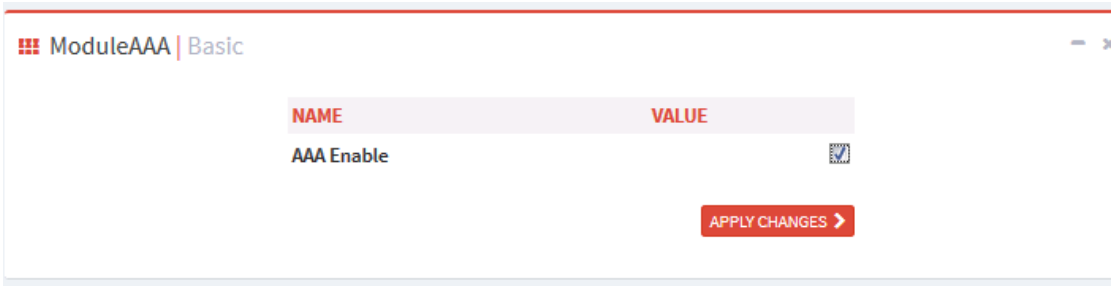

Рис. 8.45. Включение AAA.

Для настройки режима входа в систему для доступа к коммутатору, а также режима аутентификации и последовательности аутентификации выберите в меню навигации пункт [Other Configurations] → [AAA]. Страница конфигурации AAA показана на Рис. 8.46.

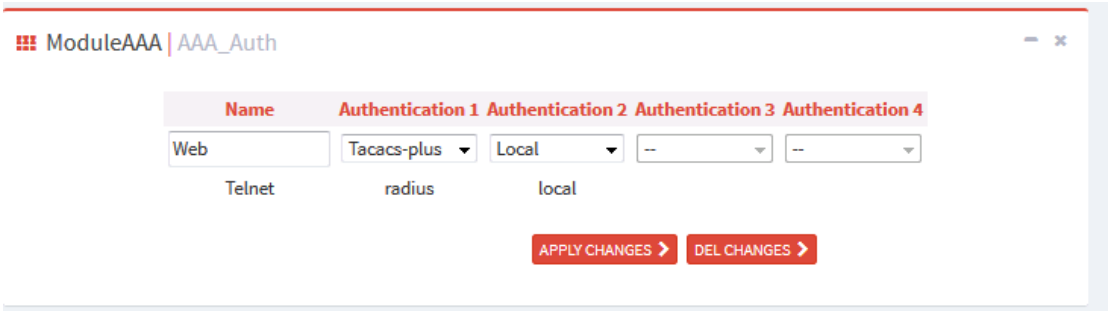

Рис. 8.46. Конфигурация AAA.

Описание параметров конфигурации сервера TACACS+ приведено в Таблица 8.26.

Таблица 8.26. Параметры конфигурации AAA.

Параметр	Функция	Значение	Значение по умолчанию
Authentication Name	Выбор режима входа в систему для доступа к коммутатору	Telnet/Web/dot1x/SSH	
Authentication 1/ Authentication 2/ Authentication 3/ Authentication 4	Выбор порядка аутентификации при входе. Сначала используется Authentication 1; если аутентификация не проходит, то используется Authentication 2; если первые две аутентификации не прошли, то используется Authentication 3; если все предыдущие аутентификации завершились неудачно, используется Authentication 4. Значение Local – использование локального имени пользователя и пароля для аутентификации; Tacacs + – использование созданного имени пользователя и пароля на сервере Tacacs+ для аутентификации; Radius – использование созданного имени пользователя и пароля на сервере Radius для аутентификации. None - аутентификация	Local/Tacacs+/Radius/ None	Local

8.16. Конфигурация интерфейса командной строки

Интерфейс командной строки (Line) коммутатора доступен через консольный порт или Telnet/SSH. Для настройки доступа к интерфейсу командной строки коммутатора выберите в меню навигации пункт [Other Configurations] → [Line]. Страница конфигурации Line показана на Рис. 8.47.

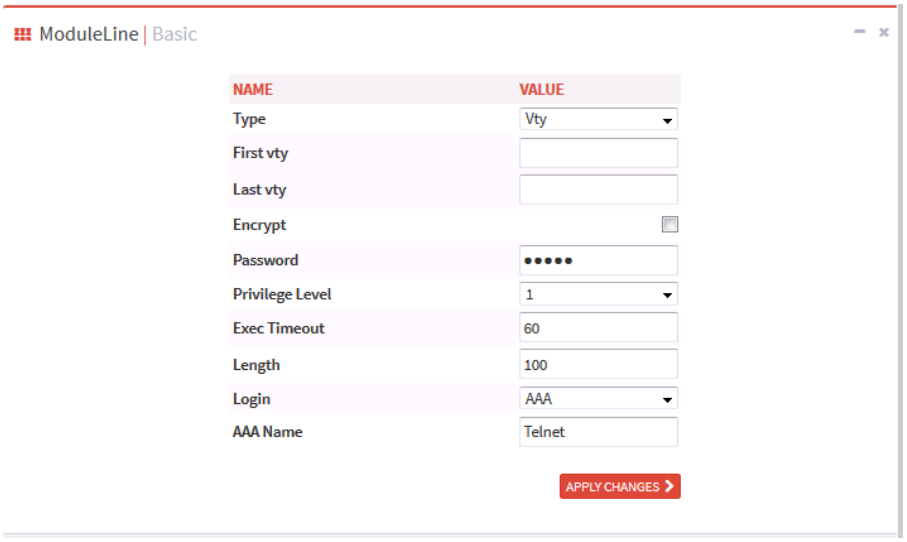

Рис. 8.47. Конфигурация Line.

Описание параметров конфигурации доступа к интерфейсу командной строки коммутатора приведено в Таблица 8.27.

Таблица 8.27. Параметры доступа к интерфейсу командной строки коммутатора.

Параметр	*Функция*	*Значение*	*Значение по умолчанию*
Type	Выбор способа доступа к интерфейсу командной строки коммутатора: console – доступ через консольный порт; vty – доступ с использованием общих протоколов входа в систему, включая telnet.	console/vty	
Vty Id (First-vty; Last-vty)	Если в параметре Type установлено значение console, значение vty по умолчанию равно 0, нужно настроить консольный порт. Если в параметре Type установлено значение vty, нужно настроить значение идентификатора First-vty или Last-vty.	0…9	0

	Настройка только First-vty означает конфигурацию только одной линии vty; настройка Last-vty означает конфигурацию линий в диапазоне от First-vty до Last-vty.		
Encrypt	Пароль по умолчанию – «admin». Не отмеченный чекбокс Encrypt означает передачу открытого текста (Plaintext encryption); отмеченный чекбокс Encrypt означает передачу зашифрованного текста (Ciphertext encryption). Используйте данный алгоритм шифрования для генерации зашифрованного текста. Команда rypt 7.	Plaintext encryption/ Ciphertext encryption	Plaintext encryption
Password	Диапазон длины пароля для открытого текста (Plaintext) составляет 1…64 символа; диапазон длины пароля для зашифрованного текста (Ciphertext) составляет 1…129 символов.	Plaintext password/Ciphertext password	
Privilege level	Уровень привилегии пользователя, авторизующегося в настраиваемых VTY.	0…15	1
Exec timeout	Интервал отсутствия активности пользователя, по прошествии которого сеанс пользователя будет принудительно завершен. Значение 0 означает отсутствие принудительного завершения сеанса по прошествии времени.	0…86400	60
Length	Длина строки виртуального терминала	0…512	100
Login	Настройка режима аутентификации для данных VTY. Line: аутентификация по паролю VTY; Aaa: использовать последовательность методов аутентификации, настроенных в модуле AAA Local: использовать локальную базу пользователей для аутентификации через данные VTY None: аутентификация отсутствует	Line/Aaa/Local/ None	Line

9. ОБСЛУЖИВАНИЕ КОММУТАТОРА

Для перехода на страницу обслуживания коммутатора NXI-3030RB выберите в меню навигации пункт [Switch Maintenance]. В появившемся всплывающем меню можно сохранить конфигурацию, нажав кнопку <Save startup-config>, или восстановить заводскую конфигурацию по умолчанию, нажав кнопку <Default>. Меню обслуживания коммутатора показано на Рис. 9.1.

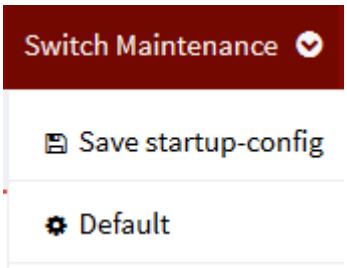

Рис. 9.1. Меню обслуживания коммутатора.

10. УЗЛЫ СЕТИ

Для просмотра информации об узлах сети выберите в меню навигации пункт [Network Nodes]. Страница вывода информации об узлах сети показана на Рис. 10.1.

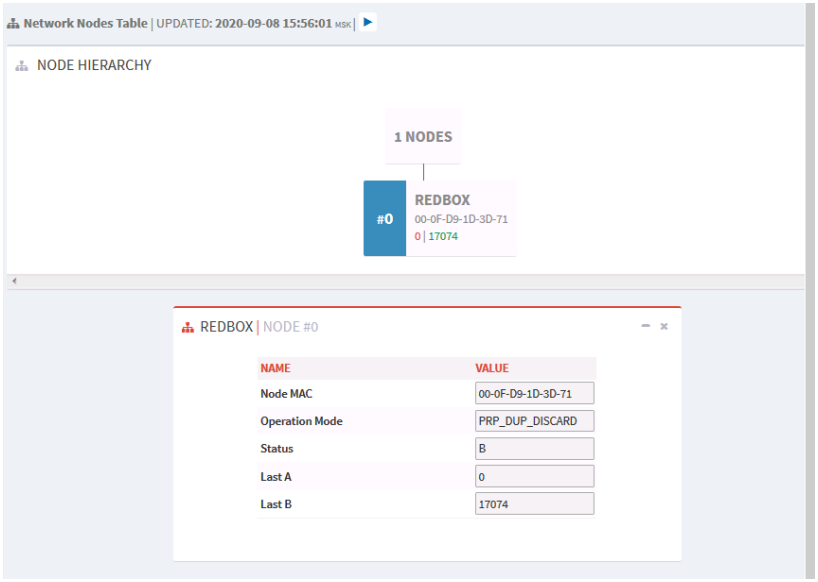

Рис. 10.1. Информация об узлах сети.

На верхней диаграмме показана текущая конфигурация сети, NODES – это локальное устройство, REDBOX – это удаленное устройство, подключенное к локальному устройству через порт B, так же указаны MAC-адрес удаленного устройства и статистика полученных и переданных портом сообщений.

Более подробная информация об узлах сети показана в таблице REDBOX. Описание параметров таблицы REDBOX приведено в Таблица 10.1.

Таблица 10.1. Параметры таблицы REDBOX.

Параметр	*Функция*
Node MAC	MAC-адрес удаленного устройства
Operation Mode	Режим работы устройства
Status	Интерфейс между удаленным устройством и локальным устройством. Возможны значения A / B / A&B
Last A	Статистика сообщений порта A
Last B	Статистика сообщений порта B

11. ПРИЛОЖЕНИЕ: СОКРАЩЕНИЯ

Сокращение	*Полное написание*
AAA	Authentication Authorization and Accounting (система аутентификации авторизации и аккаунтинга)
BC	Boundary Clock (граничные часы)
CLI	Command Line Interface (интерфейс командной строки)
DAN	Doubly Attached Node (узел двойного подключения)
DANH	Doubly Attached Node implementing HSR (узел двойного подключения, работающий по HSR)
DANP	Doubly Attached Node implementing PRP (узел двойного подключения, работающий по PRP)
DHCP	Dynamic Host Configuration Protocol (протокол динамического конфигурирования хоста)
E2ETC	End-to-End Transparent Clock (сквозные прозрачные часы)
FTP	File Transfer Protocol (протокол передачи файлов)
HTTP	Hyper Text Transfer Protocol (гипертекстовый транспортный протокол)
HSR	High-availability Seamless Redunduncy (протокол параллельного высоконадежного бесшовного резервирования)
IED	Intelligent Electronic Device (интеллектуальное электронное устройство)
LAN	Local Area Network (локальная сеть)
LLDP	Link Layer Discovery Protocol (протокол обнаружения канального уровня)
LLDPDU	Link Layer Discovery Protocol Data Unit (единица данных протокола обнаружения канального уровня)
MIB	Management Information Base (база информации управления)
MSTP	Multiple Spanning Tree Protocol (протокол множественного связующего дерева)
NAS	Network Access Server (сервер сетевого доступа)
NMS	Network Management Station (станция управления сетью)
NTP	Network Time Protocol (протокол сетевого времени)
OC	Ordinary Clock (обычные часы)
OID	Object Identifier (идентификатор объекта)
P2PTC	Peer-to-Peer Transparent Clock (одноранговые прозрачные часы)
PRP	Parallel Redundancy Protocol (протокол параллельного резрвирования)

PTP	Precision Time Protocol (протокол точного времени)
RADIUS	Remote Authentication Dial-In User Service (служба идентификации удаленных пользователей)
RMON	Remote Network Monitoring (удаленный сетевой мониторинг)
RSTP	Rapid Spanning Tree Protocol (протокол высокоскоростного связующего дерева)
SAN	Singly Attached Node (узел единичного подключения)
SFTP	Secure File Transfer Protocol (протокол безопасной передачи файлов)
SNMP	Simple Network Management Protocol (простой протокол сетевого управления)
SNTP	Simple Network Time Protocol (простой протокол сетевого времени)
SSH	Secure Shell (протокол безопасной оболочки)
SSL	Secure Sockets Layer (уровень защищенных сокетов)
STP	Spanning Tree Protocol (протокол связующих деревьев)
TACACS+	Terminal Access Controller Access Control System (система управления доступом для контроллера доступа к терминалу)
TC	Transparent Clock (прозрачные часы)
TCP	Transmission Control Protocol (протокол управления передачей данных)
UDP	User Datagram Protocol (протокол передачи датаграмм пользователей)
USM	User-Based Security Model (модель обеспечения защиты на уровне пользователей)
VLAN	Virtual Local Area Network (виртуальная локальная компьютерная сеть)